





Robert Krimmer, Rüdiger Grimm (Eds.)

**Electronic Voting 2010 (EVOTE2010)**

**4<sup>th</sup> International Conference**  
**Co-organized by**  
**Council of Europe, Gesellschaft für Informatik**  
**and E-Voting.CC**

**July 21<sup>st</sup> - 24<sup>th</sup>, 2010**  
**in Castle Hofen, Bregenz, Austria**

Gesellschaft für Informatik e.V. (GI)

## **Lecture Notes in Informatics (LNI) - Proceedings**

Series of the Gesellschaft für Informatik (GI)

Volume P-167

ISBN 978-3-88579-261-1

ISSN 1617-5468

### **Volume Editors**

Mag. Robert Krimmer

E-Voting.CC gGmbH

Competence Center for Electronic Voting and Participation

Pyrkergergasse 33/1/2, A-1190 Vienna, Austria

Email: [r.krimmer@e-voting.cc](mailto:r.krimmer@e-voting.cc)

Prof. Dr. Rüdiger Grimm

Universität Koblenz-Landau

Institut für Wirtschafts- und Verwaltungsinformatik

Universitätsstraße 1, D-56016 Koblenz, Germany

Email: [grimm@uni-koblenz.de](mailto:grimm@uni-koblenz.de)

### **Series Editorial Board**

Heinrich C. Mayr, Universität Klagenfurt, Austria (Chairman, [mayr@ifit.uni-klu.ac.at](mailto:mayr@ifit.uni-klu.ac.at))

Hinrich Bonin, Leuphana-Universität Lüneburg, Germany

Dieter Fellner, Technische Universität Darmstadt, Germany

Ulrich Flegel, SAP Research, Germany

Ulrich Frank, Universität Duisburg-Essen, Germany

Johann-Christoph Freytag, Humboldt-Universität Berlin, Germany

Thomas Roth-Berghofer, DFKI

Michael Goedicke, Universität Duisburg-Essen

Ralf Hofestädt, Universität Bielefeld

Michael Koch, Universität der Bundeswehr, München, Germany

Axel Lehmann, Universität der Bundeswehr München, Germany

Ernst W. Mayr, Technische Universität München, Germany

Sigrid Schubert, Universität Siegen, Germany

Martin Warnke, Leuphana-Universität Lüneburg, Germany

### **Dissertations**

Dorothea Wagner, Universität Karlsruhe, Germany

### **Seminars**

Reinhard Wilhelm, Universität des Saarlandes, Germany

### **Thematics**

Andreas Oberweis, Universität Karlsruhe (TH)

© Gesellschaft für Informatik, Bonn 2010

printed by Köllen Druck+Verlag GmbH, Bonn

## **Preface**

Castle Hofen has been the meeting place for e-voting specialists working in academia, administration, politics and industry since 2004. This interdisciplinary setting has brought many fruitful discussions and influenced the further development of the topic in many ways.

The continued interest is best reflected in the over 30 papers which we received following our call for papers. To make the conference again as attractive as in the past, we had to select the best papers for presentation based on a double blind review process. Special thanks go to the Council of Europe and the working group ECOM - Ecommerce, E-Government and Security of the Gesellschaft for Informatik for their support in organizing this conference.

Further thanks go again to the Gesellschaft for Informatik and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Ministries for Science and Research (BMWF), for Interior (BMI), and the Regional Government of Vorarlberg for their continued support. Without the help of the programme committee, who were always available with their advice, the conference would not have reached the level it has today.

Finally we would like to thank Thorbjørn Jagland, general secretary of the Council of Europe that the conference can take place under their auspices.

Vienna, Koblenz, July 2010

Robert Krimmer, Rüdiger Grimm

## Co-Organizers



E-Voting.CC gGmbH  
Competence Center for Electronic Voting and Participation



Council of Europe



Gesellschaft für Informatik  
Working Group for E-Commerce, E-Government and Security

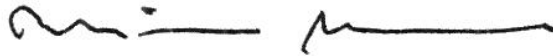
## **Introductory Words**

The far-reaching changes made by the technological revolution help people to communicate instantly with others regardless of their respective locations. People travel around the globe more frequently and millions engage in social networks and use new forms of internet-based communication systems to share their thoughts and ideas. Electronics and social systems are blending into each other to create new communication channels.

These developments present democracy with an opportunity: information and communication tools can be used to foster greater participation in political processes, regardless of time and place. For example, using electronic voting systems to cast one's vote via the internet has become a real option.

But what are the political implications of e-voting and what are the socio-cultural issues? What are the technical challenges and the limitations to e-voting systems? These are just some of the questions which need to be debated and answered.

International sharing of current research, standards and practices is vital if e-voting is to gain public confidence as a reliable and democratic voting tool. With this in mind, the Council of Europe welcomes the Fourth International Conference on Electronic Voting as a unique occasion for representatives of governments and international organisations, academia and businesses to exchange their views and expertise in the field of e-voting.



Thorbjørn Jagland  
Secretary General of the Council of Europe

## Supporters





## **Introductory Words**

Dear Conference Participants,

This year is the fourth time that the renowned international EVOTE conference will take place in Austria, on the shores of the beautiful Lake Constance. Since 2004, when this biennial conference was held for the first time, much progress has been made all over the world in the field of electronic voting. In this respect, 2004 was a turning point in many ways: it was not only the birth of the EVOTE conference in Bregenz, Austria, it was also the year in which the Recommendation of the Committee of Ministers of the Council of Europe to Member States on Legal, Operational, and Technical Standards for E-voting was passed—and the Federal Ministry of the Interior published its first detailed report on the feasibility of e-voting.

However, six years is a long time in the world of technology. Modern citizens of today use computers and other means of modern communication in a much wider way than they did in 2004. The Internet as well as mobile phones and other handheld devices influence our daily lives in an unprecedented way. Austria is fully aware of this phenomenon and is internationally known as a forerunner in terms of e-government applications. My Ministry, being the competent administrative authority for electoral matters in Austria, has been very active in doing research in the area of e-voting for a number of years.

I consider it crucial to keep track of new technological developments in the field of democratic participation. Learning more about national and international experiences in e-voting, especially concerning remote Internet voting, is fruitful and essential for election officials, governments, policy makers, and legislators when discussing possible future solutions to make more people participate in elections and other instruments of direct democracy.

Elections in Austria enjoy the solid trust of society and have a high degree of transparency. It will be indispensable to keep these high standards when implementing new technologies in future elections. Finding the balance between accessibility, user-friendliness, and the highest degree of security in any kind of electronic voting system is the top challenge which has to be tackled. The secrecy of the vote, as an indispensable value in a free world, must never be compromised.

In a rapidly advancing field such as e-voting, new issues are constantly brought to the discussion table and require input from the "best of the best." The EVOTE2010 conference is the ideal forum for this task. E-voting experts from around the globe, both practitioners and representatives from academia, are gathered here and prove how much responsibility and credibility is attached to the discussions.

I wish this conference the very best, and I look forward to the results and products of the presentations and debates.

Dr. Maria Fekter  
Federal Minister of the Interior

## Sponsors



Bundesrechenzentrum GmbH, Austria



Micromata GmbH, Germany



Scytl, Spain

## **Programme Committee**

- Mike Alvarez, USA
- Frank Bannister, Ireland
- Jordi Barrat, Spain
- Josh Benaloh, USA
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Chantal Enguehard, France
- Simon French, UK
- Thomas Grechenig, Austria
- Ruediger Grimm, Germany
- Thad Hall, USA
- Catsumi Imamura, Brasilia
- Norbert Kersting, South Africa
- Monique Leyenaar, Netherlands
- Robert Krimmer, Austria
- Laurence Monnoyer-Smith, France
- Hannu Nurmi, Finland
- Wolfgang Polasek, Austria
- Michael Remmert, France
- Peter Ryan, Luxembourg
- Josep Reniu, Spain
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Kazue Sako, Japan
- Berry Schoenmakers, Netherlands
- Robert Stein, Austria
- Dan Tokaji, USA
- Alexander Trechsel, Switzerland
- Melanie Volkamer, Germany
- Dan Wallach, USA
- Gregor Wenda, Austria

## **Organization Committee**

- Daniel Botz
- Manuel Kripp
- Nicole Lundeen
- Gisela Traxler
- Felix Wendt



## Content

### Overview

*Robert Krimmer, Rüdiger Grimm* ..... 15

**Session 1: Recent Developments in E-Voting** ..... 17

#### **Voting Technology and the Election Experience:**

##### **The 2009 Gubernatorial Races in New Jersey and Virginia**

*Charles Stewart, R. Michael Alvarez, Thad E. Hall* ..... 19

##### **The Use of E-Voting in the Austrian Federation of Students Elections 2009**

*Robert Krimmer, Andreas Ehringfeld, Markus Traxl* ..... 33

##### **Scantegrity Mock Election at Takoma Park**

*Alan T. Sherman, Richard Carback, David Chaum, Jeremy Clark,  
Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc,  
Ronald L. Rivest, Emily Shen, Bimal Sinha, Poorvi Vora* ..... 45

**Session 2: Sociocultural Issues of E-Voting** ..... 63

##### **The Role of Trust, Participation and Identity in the Propensity to e- and i-vote**

*Letizia Caporusso* ..... 65

##### **The Virtual Polling Station - Transferring the Sociocultural Effect of Poll Site Elections to Remote Internet Voting**

*Philipp Richter* ..... 79

**Session 3: Certification and Evaluation of E-Voting Systems** ..... 87

##### **A Formal IT-Security Model for the Correction and Abort Requirement of Electronic Voting**

*Rüdiger Grimm, Katharina Hupf, and Melanie Volkamer* ..... 89

##### **Compliance of POLYAS with the Common Criteria Protection Profile - A 2010 Outlook on Certified Remote Electronic Voting**

*Niels Menke and Kai Reinhard* ..... 109

##### **A Survey: Electronic Voting Development and Trends**

*Komminist Weldemariam and Adolfo Villaflorida* ..... 119

**Session 4: Operation and Evaluation of E-Voting Systems** ..... 133

##### **An Evaluation and Certification Approach to Enable Voting Service Providers**

*Axel Schmidt, Melanie Volkamer, Johannes Buchmann* ..... 135

**Session 5: End to End Verifiability and Protocol Improvements** ..... 149

##### **Verifiability in Electronic Voting - Explanations for Non Security Experts**

*Rojan Gharadaghy and Melanie Volkamer* ..... 151

##### **Verification Systems for Electronic Voting: A Survey**

*Jordi Pujol-Ahulló, Roger Jardí-Cedó, and Jordi Castellà-Roca* ..... 163

##### **Sigma Ballots**

*Stefan Popoveniuc and Andrew Regenscheid* ..... 179

<b>Session 6: E-Voting Experiences</b> .....	191
<b>Electronic Elections in a Politicized Polity</b>	
<i>Thad Hall and Leontine Loeber</i> .....	193
<b>Double-entry Accounting Provides Software-Independent Algorithm for Confirming the Integrity of Automated Election Tallies</b>	
<i>Roberto S. Verzola</i> .....	213
<b>Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria</b>	
<i>Andreas Ehringfeld, Larissa Naber, Thomas Grechenig, Robert Krimmer, Markus Traxl, Gerald Fischer</i> .....	225
<b>Session 7: Discussion of E-Voting Protocols</b> .....	239
<b>Universally Verifiable Efficient Re-encryption Mixnet</b>	
<i>Jordi Puiggalí Allepuz and Sandra Guasch Castelló</i> .....	241
<b>Why Public Registration Boards are Required in E-Voting Systems Based on Threshold Blind Signature Protocols</b>	
<i>Reto E. Koenig, Eric Dubuis, and Rolf Haenni</i> .....	255
<b>Session 8: Theoretical and Practical Implications of E-Voting</b> .....	267
<b>Coercion-Resistant Hybrid Voting Systems</b>	
<i>Oliver Spycher, Rolf Haenni, Eric Dubuis</i> .....	269
<b>E-voting in Japan: A developing case?</b>	
<i>Masahiro Iwasaki</i> .....	283

## Overview

Robert Krimmer<sup>1</sup>, Rüdiger Grimm<sup>2</sup>

<sup>1</sup>E-Voting.CC gGmbH  
Competence Center for Electronic Voting and Participation  
Pyrkerlgasse 33/1/2, A-1190 Vienna, Austria  
[r.krimmer@e-voting.cc](mailto:r.krimmer@e-voting.cc)

<sup>2</sup>Universität Koblenz-Landau  
Institute for Information Systems Research  
Universitätsstraße 1, D-56016 Koblenz, Germany  
[grimm@uni-koblenz.de](mailto:grimm@uni-koblenz.de)

This fourth proceedings volume of the EVOTE conference series features an impressive set of papers dealing with various aspects of electronic voting. It is the task of this conference series to enable the discourse amongst specialists working in academia, administration, politics and industry so that understanding, cooperation and future research can emerge. The conference includes discussions of practical work, its evaluation and theoretical foundation. In particular, it takes up the most urgent challenges that came up during the past two years. Therefore, special topics include end-to-end verifiability and certification of electronic voting systems. The papers are presented in the following.

The **first session** deals with the recent experiences made in the United States and Austria. First *Thad Hall, Charles Stewart, and R. Michael Alvarez* present the connexion between voting technology and voter experience in the gubernatorial races in New Jersey and Virginia. Then *Robert Krimmer, Andreas Ehringfeld and Markus Traxl* present findings from the evaluation of the contested 2009 federation of students election, which offered electronic voting via the Internet for the first time in Austria. Thirdly the large and designated team consisting of *Alan Sherman, Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald Rivest, Emily Shen, Bimal Sinha, and Poorvi Vora* report from a mock election using an end-to-end verifiable electronic voting system.

In the **second session** the socio-cultural dimension of electronic voting is discussed. Here *Letizia Caporusso* discusses the role of trust, participation, and identity. Then *Philipp Richter* presents how the voter experience with Internet-based voting could be made as similar as voting in the polling station.

The **third topic** is dealing with certification and evaluation of electronic voting. Here *Rüdiger Grimm, Katharina Hupf, and Melanie Volkamer* start an extension of the formal model presented at EVOTE08. *Niels Menken* and *Kai Reinhard* show to which degree the remote e-voting system POLYAS is compliant with the common criteria protection profile. *Komminist Weldemariam* and *Adolfo Villafiorita* go on from there and present the current state in the development of e-voting systems.

**Session four** will host the presentation of *Axel Schmidt, Melanie Volkamer and Johannes Buchmann* on an evaluation approach for voting service providers.

In the **fifth session** *Rojan Gharadaghy and Melanie Volkamer* try to explain end-to-end verifiability to the non expert. In a different approach *Jordi Pujol-Ahulló, Roger Jardí-Cedó, Jordi Castellà-Roca* will classify these systems. Then *Stefan Popoveniuc and Andrew Regenscheid* will present a practical approach of a end-to-end-verifiable voting system.

In **session six** we will come back to e-voting experiences, where *Thad Hall and Leontine Loeber* will discuss the political environment and how it influences the discussion around e-voting. *Roberto Verzola* will show an innovative way on how to input voting results based on basic booking-keeping principles. *Andreas Ehringfeld, Larissa Naber, Thomas Grechenig, Robert Krimmer, Markus Traxl, and Gerald Fischer* discuss the Council of Europe Recommendation Rec(2004)11 how the experiences with the attacks on the federation of students' election in 2009 could be reflected.

In the **seventh session** e-voting protocols are discussed. Here *Jordi Puiggali and Sandra Guasch* present an universally verifiable efficient re-encryption mixnet. Then *Reto Koenig and Eric Dubuis* discuss how blind signature based internet voting systems can be made more secure using bulletin boards.

In the **final session** on theoretical and practical implications of e-voting *Oliver Spycher and Rolf Haenni* discuss how hybrid voting systems can be made coercion-resistant. *Masahiro Iwasaki* closes with a description of e-voting in Japan.

These papers give a good overview on the fast developments in the past two years. It also shows the necessity and importance of interdisciplinary research. Further we hope Castle Hofen will for long be home to these fruitful discussions.



## **Session 1: Recent Developments in E-Voting**



# **Voting Technology and the Election Experience: The 2009 Gubernatorial Races in New Jersey and Virginia**

Charles Stewart III<sup>1</sup>, R. Michael Alvarez<sup>2</sup>, Thad E. Hall<sup>3</sup>

<sup>1</sup>Kenan Sahin Distinguished Professor of Political Science,  
Massachusetts Institute of Technology  
77 Massachusetts Avenue  
Room E53-470  
Cambridge, MA 02139-4307 USA

<sup>2</sup>Professor of Political Science, California Institute of Technology  
1200 E. California Blvd. MC 228-77  
Pasadena, CA 91125 USA

<sup>3</sup>Associate Professor of Political Science, University of Utah  
260 S. Central Campus Drive, Room 252  
Salt Lake City, UT 84112 USA

**Abstract:** In this paper, we examine the attitudes of voters regarding the voting experience in the 2009 gubernatorial elections in New Jersey and Virginia. We focus especially on the way in which voting technology experiences that voters have had **affect** their confidence in the voting process, their attitudes toward fraud and reform, and other aspects of the voting process. We find that voters are sensitive to the voting mode they use—in person voting compared to absentee voting—as well as to whether they get to vote on the technology they prefer (paper versus electronic). Finally, the privacy that voters feel in the voting process is also important in shaping the voter's confidence.

## 1 Introduction

In the aftermath of the 2000 presidential election in the United States, groups like the Caltech/MIT Voting Technology Project (VTP) began studying the voting technology and the process of voting in American elections [VTP 2001].<sup>1</sup> Many of the early studies like the work of the VTP, though, focused either on survey data collected for other purposes (like the Census Bureau's Current Population Survey) or on the analysis of aggregated election returns [AI09]. These studies, while important, were unable to study in detail the voting experience --- and they were unable to relate the voting experience directly to the technology used by the voter to cast his or her ballot.

However, in recent years, the situation has changed, as detailed survey data on the voting experience has begun to be collected in earnest. In the 2007 gubernatorial elections in three states, in the Super Tuesday presidential primary races in 12 states, and then in the 2008 presidential election, the VTP conducted surveys in the appropriate states to determine the quality of the voting process across all modes of voting—early voting, absentee voting, and election day voting. The goal of these studies was to determine the way in which voters experienced the election process. In this paper, we use data from the most recent study by the VTP of voting experiences in New Jersey and Virginia in each state's 2009 gubernatorial elections. These studies built, in part, on earlier work designed to study the voting process as experienced by the voter. Scholars have studied the confidence of voters in the voting process [AH08; AHL08, AHL2009; AS05; BHC05], experience voters have had with their poll workers [HMP09; Ha09], and combinations of these experiences [AAH07; CMMP08]. However, most of these studies have been state-specific studies and many have focused on Election Day voting experiences, not considering the fastest growing part of the voting experience. These studies have also all focused on federal elections.

In this study, we consider a different type of American election, the off-year gubernatorial election. Five states have off-year gubernatorial elections; Virginia and New Jersey are on one cycle (e.g., 2009, 2005, 2001) and Kentucky, Louisiana, and Mississippi are on a different cycle (e.g., 2007, 2003, 1999). Our data analysis allows us to consider voter confidence in this slightly different context. In this study, we also specifically focus on how voters' experiences were affected by the voting technology they used to cast their ballots and the voting technology – paper or electronic – that is their preference.

---

<sup>1</sup> This paper uses data from the *2009 Survey of the Performance of American Elections*, which was funded by The Pew Charitable Trusts *Make Voting Work* Initiative. All findings are based on the analysis of the authors and do not reflect the views or opinions of the Pew Charitable Trusts.

## 2 Data and Analysis

The data in this analysis come from the *2009 Survey of the Performance of American Elections* (SPAE), and builds on the *2008 Survey of the Performance of American Elections*, which was the first nationwide effort to gauge the quality of the election experience from the perspective of voters [AAB09]. The data presented here come from the 2009 Survey of the Performance of American Elections (SPAE). The 2009 SPAE was an Internet survey that involved 1,200 interviews of registered voters in New Jersey and 1,300 interviews of registered voters in Virginia. The survey was in the field the week following the election, beginning Thursday, November 5 (two days after the election), with 98% of interviews completed by Monday, November 9. *YouGov/Polimetrix* conducted this survey entirely on the Internet using state-level matched random samples in each of the states. The respondents were recruited through a variety of techniques and the resulting sample matched the state populations on important demographic characteristics, such as education, income, race, and partisanship. The survey questionnaires were pilot tested in the November 2007 gubernatorial elections in Mississippi, Kentucky, and Louisiana and in the February 2008 Super Tuesday presidential primary. The main body of the survey asked a series of items about the experience of voters on Election Day, in early voting centers or during postal voting.

We checked the validity of the results by comparing the self-reported vote for governor in each state against the actual election returns. The results were very close and easily within sampling error.<sup>2</sup> We also compared some simple cross-tabulations within our survey with similar cross-tabulations from the network exit polls. We do not report those results here, but there is very close agreement between our results and the exit polls when we break the results down by sex, party, and reported 2008 presidential vote.<sup>3</sup>

## 3. Voting Experience

The voting experience is an important part of the democratic process. It is through voting that individuals express their preferences for policy, either through the election of representatives or directly through voting on referenda and initiatives [Pi67]. The act of voting has changed dramatically over the past 200 years [Be04; Ke00] and voters have certain expectations about the voting process, including about voter privacy and voting experiences [e.g., KMN10; GHD09]. We also know that variations in the voting experience can affect voter confidence and their attitudes about the voting experience. For example, voters who rate their poll worker-voter interaction higher are more likely to be confident that their votes were counted accurately [HMP09]. Likewise, we know that absentee voters are less confident that their votes are cast correctly compared to voters

---

<sup>2</sup> For example, in New Jersey the unofficial return results/survey results were Corzine (D) 44.4/42.1, Christie (R) 49.0/48.4, and Daggett (I) 5.7/8.6. In Virginia, the results were McDonnell (R) 58.6/59.4 and Deeds (D) 41.3/39.9.

<sup>3</sup> In the interest of brevity, we do not report standard errors in this paper. In general, in an analysis of 1,200 observations and a mean proportion at 50%, the 95% confidence interval is  $\pm 2.9\%$ .

who vote in person in a precinct (either on election day or early) [AHL08]. We also know that problems at the polls – long lines, machine problems, and the like – all serve to lower evaluations of the voting experience at the polling place.

Our analysis here considers the voting experience in New Jersey and Virginia in November 2009 and focuses on the role that technology plays in the voting experience. We not only consider the role of voting technology, but also the use of electronic media prior to the election to learn more about the voting process. We start our discussion with this pre-election information search process and then consider the election process itself. We conclude by examining voter evaluations of election fraud.

	New Jersey	Virginia
Candidate position statements	74%	75%
News about the election	64%	62%
Polling place location	17%	23%
Sample ballots	15%	15%
Instructions on how to vote absentee	7%	8%
Instructions on how to vote at a polling place	5%	3%
Other	4%	5%

**Table 1:** Use of the Internet for Political Use

One critical part of the Internet and society is that individuals can now use the Internet to collect information about the voting process prior to voting. Voters can use the Internet to find out more about where they can vote, how to vote, and about the candidates for whom they can vote. Interestingly, we find that only 34% of respondents in New Jersey and 47% of those in Virginia reported that they had gone “online to find out information about the November 2009 election.” In Table 1, when we examine the reasons why individuals visited the websites that they did, we find that most people used the Internet to find information about the candidates or track news about the election. Fewer than 1 in 5 respondents who went online did so to get information about their polling place, sample ballots, or information regarding how to vote. Respondents generally used the Internet for news about the election and the candidates, relying on the Internet only a little to understand the mechanics of voting.

Once voters get to the polling place, they may or may not have to wait in a line to vote. The 2008 SPAE found that African Americans wait in line to vote significantly longer than do Whites. For instance, in November 2008, African Americans waited twice as long to vote (27 minutes, on average) than did Whites (13 minutes). Although some of this difference may be attributed to the excitement generated by the Obama campaign

and a surge in African-American turnout in November 2008, examples of this pattern in other elections suggests the need for a richer explanation of this pattern. One important explanation may be that some individuals arrive at the polls before they open, or there is a clustering of voting at specific times.

We find that time of voting does explain some of the wait time problem. African Americans did report waiting longer to vote in both New Jersey and Virginia. In New Jersey, the estimated average wait was 1.7 minutes for Whites and 3.2 minutes for Blacks; in Virginia, the averages were 2.8 and 8.2 minutes, respectively. However, when we exclude early-arrivers (people who arrive before the polls are open) from the calculations, average wait times in Virginia were 2.7 minutes for Whites and 6.4 minutes for Blacks. The racial disparity remains, but it has been reduced. The racial differences are also explained by the fact that African Americans are more likely to live in large cities where lines are longer, regardless of race, compared to smaller towns and suburbs. Even so, *within community types*, African Americans still waited longer. For instance, within big cities, African Americans reported waiting 11 minutes to vote, compared to 5.9 minutes for Whites; within the outer suburbs, the reported waits were 3.4 minutes for Blacks and 2.0 minutes for Whites.

		Precinct Voting Technology			
		New Jersey		Virginia	
		DRE	DRE	OPSCAN	MIXED
No Line	N	660	372	170	103
	Percent	70.66%	62.42%	68.55%	68.67%
Less than 10 Min Line	N	247	185	59	40
	Percent	26.45%	31.04%	23.79%	26.67%
10- 30 Min Line	N	24	29	13	6
	Percent	2.57%	4.87%	5.24%	4.00%
30 or More Line	N	3	10	6	1
	Percent	0.32%	1.68%	2.42%	0.67%

**Table 2:** Lines and Voting Technology

When we consider line length and voting technologies, we see that, in Virginia, voters were more likely to encounter some line than in New Jersey, although roughly two-thirds of voters in Virginia encountered no line. We do see that voters in precincts with DREs were more likely to wait in a line of any length to vote compared to precincts with optical scan voting or a mix of both technologies. However, voters in optical scan precincts were more likely than voters in DRE precincts (7.66% to 6.55%) to wait in a line that was 10 minutes or longer. Voters in precincts that had a mix of both technologies were least likely to wait in a line 10 minutes or longer.

## 4 Voter Confidence

One summary measure of the voting experience is whether the voter thinks that his or her vote was counted correctly. The standard metric for evaluating voter confidence has been to ask: “How confident are you that *your vote* in the General Election was counted as you intended?” In addition, some scholars have also begun to probe voter confidence in the count at higher levels of government; in this survey, we asked about confident in “your county or city” and in “your state as a whole.” The purpose of asking all three questions is that one taps into a voter’s confidence their the votes in their precinct will be counted, and the other two tap into confidence in the location where the votes are aggregated (in their city or county, where elections are administered in the United States) and were the final results are certified (at the state level).

Table 3 presents the percentages of respondents stating they were “very confident” in each state. The results are broadly consistent with other surveys of experience with government services, in which respondents generally report high ratings for their personal experience and lower ratings when asked about the experience of other people, or the system in general. In the November 2008 general election, 72% of New Jersey voters and 74% of Virginia voters said they were “very confident” their votes were counted as cast. The results for 2009 are very similar to those in 2008, with Virginia voters becoming slightly more confident and New Jersey voters slightly less confident. This might just be due to random variability, though the direction of the movements is consistent with the pattern that voters for winning candidates tend to express greater confidence than people who vote for the losers.

The New Jersey gubernatorial race was much closer than Virginia, which may explain some of the shift across the past year. Furthermore, when we look at how the confidence of partisans shifted between 2008 and 2009, the pattern is consistent with the “winners are more confident” theme. The next table reports the percentage of respondents saying they were “very confident” their own vote was counted as cast, by state and by party, across 2008 and 2009.

	Democrats			Republicans			Independents		
	2008	2009	Diff.	2008	2009	Diff	2008	2009	Diff
New Jersey	78%	62%	-16%	70%	76%	+6%	69%	66%	-3%
Virginia	81%	66%	-15%	71%	81%	+10%	68%	76%	+8%

**Table 3:** Change in Confidence, 2008 to 2009

In Table 4, when we consider confidence across various levels of government, we see that there is a clear decline in confidence as we move from the precinct to county to state levels. Over thirty percent of respondents were less confident in the overall state vote count than in how their own vote was counted. In Virginia, which has a non-partisan Board of Elections, 29% of Democrats and 25% of Republicans were less confident in the overall state vote count. In New Jersey, elections are run by an elections division that is located in the Secretary of State’s office; the Secretary of State was associated with the unpopular Democratic governor. In New Jersey, 29% of Democrats and 39% of Republicans were less confident in the statewide count. In both states, roughly 35% of Independents were less confident in the statewide count.



	New Jersey	Virginia
Your Vote	68%	75%
Your City/County	54%	63%
Your State	41%	51%

**Table 4:** Voter Confidence Across Levels of Government

## 5 Voter Confidence and Technology

We also examined voter confidence across the various voting technologies used. Here, we see first that voter confidence varies across modes of voting. Absentee voters have the lowest level of personal confidence and Election Day voters have the highest levels of confidence. In Virginia, the personal confidence gap between Election Day and absentee voters is approximately 8 percentage points and in New Jersey, it is 14 percentage points. In New Jersey, the gap remains, but becomes smaller as we move to county-level and state-level confidence. In Virginia, the gap actually reverses at the state level, with absentee voters more confident than precinct voters. This reversal in Virginia largely occurs because precinct voters have more of a decline in confidence between personal and state confidence levels; the decline is much less for absentee voters.

In Table 5, we also see differences across the voting technologies used. In Virginia, some voters vote on DREs and some vote on optical scan. Most counties use only one technology or the other, but a small number of counties—including one of the most populous counties in the state, use a mix of optical scan and DREs in the precincts in the county. In Virginia, we see that DRE and optical scan voters have similar levels of confidence at all three levels and that individuals in counties with mixed technology are slightly less likely to be confident.

		New Jersey			Virginia		
		Not/Not Too Confident	Somewhat Confident	Very Confident	Not/Not Too Confident	Somewhat Confident	Very Confident
Mode of Voting	Election Day	4.17%	25.91%	69.92%	3.51%	20.02%	76.47%
	Early	20.00%	20.00%	60.00%	2.94%	23.53%	73.53%
	Absentee	10.13%	34.18%	55.70%	8.57%	22.86%	68.57%
Congruence: Technology Used and Wanted	Incongruence	11.01%	33.03%	55.96%	3.01%	26.42%	70.57%
	Congruence	3.94%	25.79%	70.27%	3.92%	17.84%	78.24%
Preferred Voting Method	Hand Count Paper	6.90%	37.93%	55.17%	2.33%	34.88%	62.79%
	Opscan	5.00%	41.67%	53.33%	6.14%	22.81%	71.05%
	DRE	3.85%	24.67%	71.48%	2.55%	16.41%	81.05%
Precinct Voting Technology	DRE	4.62%	26.61%	68.78%	3.99%	19.65%	76.36%
	Opscan				3.49%	17.44%	79.07%
	Mixed				3.18%	27.39%	69.43%

**Table 5:** Voter Confidence by Various Technology Factors

We also asked voters about their preferred method of voting. DREs were the top choice in both states, with 90% of New Jersey residents and 74% of Virginia residents making this choice. Optical scan was the choice of 6.7% in New Jersey and 21.2% in Virginia; hand counted paper ballots are the choice of 3.1% in New Jersey and 4.7% in Virginia. Some voters have congruence between their voting preference and the technology on which they vote; voters who want to vote on a DRE and vote in a precinct in New Jersey have such congruence, but voters who want to vote on a paper ballot that is counted via optical scan can only have such congruence if they vote absentee. A lack of such congruence could affect voter confidence, given that the voter would rather use a different technology.

When we examine confidence by preferred voting technology, we see that DRE voters are most confident that their vote will be counted accurately in both states. In Virginia, there is a monotonic decline in confidence from DREs (81% very confident) to optical scan (71%) to hand counted paper ballots (62.8% very confident). In New Jersey, the decline is roughly 15 percentage points from DREs to either optical scan or hand counted paper ballots. When we examine the issue of congruence, we see that voters who are congruent are more confident in both states, with the gap much larger in New Jersey than in Virginia. This is likely the result of it being difficult to vote using an alternate method in New Jersey, where absentee voting policies are not very liberal.

## 6 Voter Privacy and Problems at the Polls

The voting process is one that, since the turn of the 20<sup>th</sup> century, has been a private process with secret ballots. There is a normative idea that voting will be private, with ballots being secret. There is also an expectation that the voting experience will be problem-free and that voting technologies will work correctly. However, we have increasingly read of voters complaining that the in-person voting process is not private, either because voting booths are too small and exposed to wandering eyes, or because voters often have to hand a ballot to a poll worker to have it cast.<sup>4</sup>

In order to identify problems with the voting process and with privacy, we asked voters in both states the following question: “Do you agree or disagree that you were able to vote in private?” Overall, 91% of voters in New Jersey and 81% of voters in Virginia “strongly agreed” with this statement. It is not obvious why Virginia voters expressed less satisfaction with their voting privacy. The difference is not due to the presence of optical scanners in Virginia, since the percentages are virtually identical for users of DREs (80.6%) and optical scanners (81.4%). These differences persist across racial groups and types of communities. The robustness of the difference across the two states, regardless of controls for community and demographic factors, suggests that the explanation lies in the details of how precincts are configured in the two states.

We also asked voters, “Have you ever had a problem when you tried to vote that kept you from voting?” In Table 6, we see that, in New Jersey, 4.6% of voters said that they had had a problem that had prevented them from voting before and 3.6% of Virginians gave the same answer.<sup>5</sup> As we see in the table below, having a past problem voting or having concerns about voter privacy both affect voter confidence in a very negative manner. In New Jersey, privacy concerns lowered confidence by 19 percentage points; in Virginia, those with privacy concerns were 9.5 percentage points less confident than those who had no such concerns. Individuals who had encountered previous problems that kept them from voting were 25 and 20 percentage points less likely to be very confident in New Jersey and Virginia, respectively.

---

<sup>4</sup> For instance, see “New N.Y. Voting System Raises Privacy Concerns,” [pressconnects.com, http://www.pressconnects.com/article/20091130/NEWS01/911300341/New+N.Y.+voting+system+raises+privacy+concerns](http://www.pressconnects.com/article/20091130/NEWS01/911300341/New+N.Y.+voting+system+raises+privacy+concerns)

<sup>5</sup> Voting machine problems were rather rare in this election, occurring in less than 1% of cases in either state.

	New Jersey			Virginia		
	Not/Not too Confident	Somewhat Confident	Very Confident	Not/Not too Confident	Somewhat Confident	Very Confident
Felt Privacy	4.02%	25.03%	70.95%	3.26%	19.59%	77.15%
Felt Lack of Privacy	11.63%	37.21%	51.16%	5.19%	27.27%	67.53%
No Past Problems	4.02%	26.03%	69.95%	3.40%	19.80%	76.80%
Past Problem Voting	20.00%	35.56%	44.44%	13.51%	29.73%	56.76%

**Table 6: Confidence and Privacy**

## 7 Voting Technologies and Voting Fraud

The role of computers in casting and counting votes has been a controversial issue since at least 2002 (AH04, AH08; HNH08; St06, St09]. The controversy over electronic voting centers, in part, over a debate as to whether paper ballots or electronic ballots are easier to count, easier to use for voting, and easier to steal. We asked these questions in New Jersey and Virginia with great interest because both states have substantial DRE usage. DREs are the sole technology used for in-precinct voting in New Jersey and approximately 75% of Virginia voters use DREs in the precincts.

	New Jersey			Virginia, DRE users			Virginia, OpScan users		
	OpScan	DRE	Paper	OpScan	DRE	Paper	OpScan	DRE	Paper
Easy to steal votes	59%	24%	80%	53%	23%	79%	30%	28%	75%
Easy for disabled	51%	70%	53%	54%	74%	56%	69%	63%	66%
Easy for non-disabled	69%	86%	69%	74%	89%	74%	84%	83%	84%
Easy to count	42%	77%	24%	51%	78%	28%	67%	68%	35%

**Table 7: Concern About Voting Technology, by Voting Technology Used**

We asked respondents their opinions of the three major voting technologies: (1) “paper ballots that are scanned and counted by a computer,” (2) “electronic voting machines, that is, voting machines with a touch screen, like an ATM machine,” and (3) “paper ballots that are counted by hand.” For each of these technologies, we asked respondents to agree or disagree with the following statements about each technology:

1. It is easy for dishonest people to steal votes;
2. It is easy for people *with* disabilities to vote on;
3. It is easy for people *without* disabilities to vote on; and
4. It is easy for election officials to count votes accurately.

Responses to these questions are summarized in the previous table. The numbers in the cells are the percentage of respondents saying they *agree* with the statements. (Individuals saying they “don’t know” are included in the denominator.)

Compare, first, the New Jersey respondents, all of whom used DREs if they voted in-precinct, with the Virginia respondents in DRE jurisdictions.<sup>6</sup> The attitudes toward the three technologies are strikingly similar. Virginians may be a little more favorably inclined toward all three technologies, but only slightly. For DRE users in both states, the superior technology is clearly DREs, followed by optical scanners and then hand-counted paper.

Type of In-Precinct Equipment	New Jersey	Virginia	
	DRE	DRE	Optical Scan
Paper ballot	3.0%	4.1%	4.4%
Optical Scan	6.3%	13.6%	40.0%
DRE	82.2%	76.7%	48.0%
Don’t know	4.3%	2.9%	5.4%
Other	4.2%	2.8%	2.2%

**Table 8:** Preferred Voting Technology, by Voting Technology Used

When we compare the Virginia respondents who live in counties/cities that use DREs for in-precinct voting with those who live in municipalities that use optical scanners, we see that optical scan users have a better opinion of optical scanning than the DRE users, but except for the “vote stealing” item, the differences are surprisingly small. The same can be said for opinions about hand-counted paper ballots, as well. Similarly, optical scan users have a lower opinion of DREs than the DRE users, but the differences are surprisingly small, especially given the controversy over DRE machines. These findings lead us to conclude that voters are largely supportive of what they are currently voting on, with little nostalgic pining for the lowest-tech solution, hand-counted paper ballots.

We also asked the respondents “Which kind of voting machine or method would you most prefer to use?” Table 8 gives the responses to this question, broken down by state and by type of equipment use in Virginia. Again, users of DREs are happy to be using them, with New Jersey DRE users a bit more pleased with this technology than Virginians. In Virginia, the optical scan users are surprisingly split in their preference for the two major forms of voting.

Further analysis can be performed on these responses. The well-known divisions over machine choice show up in the data. For instance, liberals and highly educated respondents are more likely to oppose DREs. African Americans, interestingly enough, are more supportive of DREs in both states than are Whites.

<sup>6</sup> In New Jersey, 91% of voters in our sample report voting in a precinct on Election Day. In Virginia, the percentage was 93%.

## 8 Conclusion

Only quite recently have scholars begun to collect and analyze individual-level data on the voting experience in the United States. The availability of detailed individual data on a voter's experience, coupled with knowledge of what voting technologies are being used by these same voters when they cast their ballots, constitutes a rich new area for research and will no doubt generate new ideas for future improvement of election administration in the United States. We clearly see that voters are sensitive to the voting experience that they have and their attitudes about the electoral process are shaped in part by the experience that they have voting.

One of the most interesting results in our analysis concerns the confidence that voters state they have that their ballot is being counted as they intended. Consistent with earlier studies of voter confidence, we find that those who cast their ballot in person on Election Day express the most confidence that their ballot is being counted as they intended; those who vote before Election Day, especially those who vote by mail, consistently report lower levels of confidence that their ballots are counted as intended. Exactly why these differences exist in our analysis and in previous studies is a question that requires additional research, since increasing numbers of voters are choosing to cast their ballots before Election Day.

We also found that when voters were asked which voting technology they would prefer to use, we found that those who currently use DRE machines to vote would like to continue using them. Interestingly, we found that optical scan voters in Virginia were deeply divided about whether they would like to continue the use of optical scan voting technology, which indicates another area for future research.

The methodology used in this study—of surveying voters about their voting experience immediately after the election—is one that can be replicated in other countries and in all electoral environments. For instance, in the 2010 parliamentary elections in the United Kingdom, there were many reports of electoral problems, such as understaffed polling places, polls that ran out of ballots, and long lines.<sup>7</sup> A survey of voter attitudes can determine how such problems affect voter confidence and also identify the breadth of the problem nationwide, without having to rely solely on the media to know what occurred. For public managers of elections and for political principals, having these data can improve public management of election without having to rely solely on hearsay and media reports that are not validated with more systematic data.

---

<sup>7</sup> <http://www.timesonline.co.uk/tol/news/politics/article7118998.ece>

## Bibliography

- [AI09] Alvarez, R. M. 2009. Measuring Election Performance. Caltech/MIT Voting Technology Project Working Paper 94, <http://vote.caltech.edu/drupal/node/325>.
- [AH08] Alvarez, R. M., & Hall, T. E. 2008. *Electronic elections: The perils and promise of digital democracy*. Princeton, NJ: Princeton University Press.
- [AAB09] Alvarez, R. M., Ansolabehere, S., Berinsky, A., Lenz, G., Stewart III, C., and Hall, T. E. 2009. *2008 Survey of the performance of American elections*. Boston/Pasadena: Caltech/MIT Voting Technology Project.
- [AHL08] Alvarez, R. M., Hall, T. E., and Llewellyn, M. 2008. Are Americans confident their ballots are counted? *Journal of Politics* 70 (3):754-766.
- [AHL09] Alvarez, R. M., Hall, T. E., and Llewellyn, M. 2009. *The winner's effect: Voter confidence before and after the 2006 elections*. Working Paper. Pasadena, CA, <http://vote.caltech.edu>.
- [AS07] Atkeson, L. R., and Saunders, K. L. 2007. Voter confidence: A local matter? *PS: Political Science & Politics* (40), 655-660.
- [Be04] Bense, R. 2004. *The American ballot box in the mid-nineteenth century*. New York: LOCATION: Cambridge University Press.
- [BHC05] Bullock III, C. S., Hood III, M., and Clarke, R. 2005. Punch cards, Jim Crow, and Al Gore: Explaining voter trust in the electoral system in Georgia, 2000. *State Politics & Policy Quarterly* 5 (3):283-294.
- [VTP01] Caltech/MIT Voting Technology Project. 2001. Voting: What is, what could be. <http://vote.caltech.edu/drupal/node/10>.
- [CMM08] Claassen, R. L., Magleby, D. B., Monson, J. Q., and Patterson, K. D. 2008. At your service: voter evaluations of poll worker performance. *American Politics Research*, 36: 612-634.
- [GHD09] Gerber, A., Huber, G., Doherty, D., & Dowling, C. 2009. Is there a secret ballot? Ballot secrecy perceptions and their implications for voting behavior. Paper presented at the annual meeting of the *American Political Science Association*, . Toronto, Canada, September 3-9, 2009.
- [Ha09] Hall, T. E. 2009. *Voter attitudes toward poll workers in the 2008 election*. Pasadena, CA: Caltech/MIT Voting Technology Working Paper 77.
- [HMP09] Hall, T. E., Monson, Q., and Patterson, K. 2009. The human dimension of elections: How poll workers shape public confidence in elections. *Political Research Quarterly* 62 (3):507-522.
- [HNH08] Herrnson, P. S., Niemi, R. G., Hanmer, M. j., Bederson, B. B., Conrad, F. C., and Traugott, M. W. 2008. *Voting technology: The not-so-simple act of casting a ballot*. Washington, D.C.: Brookings Institution Press.
- [KMN10] Karpowitz, C. F., Monson, J. Q., Nielson, L., Patterson, K. D., and Snell, S. A. 2010. *Political norms and the private act of voting*. Working Paper. Provo, UT: Brigham Young University.
- [Ke00] Keyssar, A. 2000. *The right to vote*. New York: Basic.
- [St09] Stewart III, C. 2009. Election technology and the voting experience in 2008. Paper presented at the annual meeting of the *Midwest Political Science Association*, Chicago, IL,; April 2-5, 2009.
- [St06] Stewart III, C. 2006. Residual vote in the 2004 election. *Election Law Journal* 5 (2):158-169.





## **The Use of E-Voting in the Austrian Federation of Students Elections 2009**

Robert Krimmer<sup>1</sup>, Andreas Ehringfeld<sup>2</sup>, Markus Traxl<sup>3</sup>

<sup>1</sup>E-Voting.CC gGmbH

Competence Center for Electronic Voting and Participation

1190 Vienna, Austria

[r.krimmer@e-voting.cc](mailto:r.krimmer@e-voting.cc)

<sup>2</sup>Vienna University of Technology

Industrial Software (INSO)

1040 Vienna, Austria

[andreas.ehringfeld@inso.tuwien.ac.at](mailto:andreas.ehringfeld@inso.tuwien.ac.at)

<sup>3</sup>Institut für Verwaltungsmanagement

6020 Innsbruck, Austria

[markus.traxl@verwaltungsmanagement.at](mailto:markus.traxl@verwaltungsmanagement.at)

**Abstract:** The use of e-voting for the elections to the Austrian Federation of students (Hochschülerinnen und Hochschülerschaftswahlen) was one of the most sophisticated Austrian e-government projects in 2009. The task was to complement the paper based voting with an electronic voting channel in order to create new opportunities to vote. Together with the implementation of e-voting the legal basis of the federation of students was adapted to include an electronic election administration. The discussion around e-voting was rather controversial with clear pro and contra positions.

This first of a kind implementation of e-voting in Austria was technically successful. Almost 1% (2.161) of the eligible students cast their votes electronically between 18<sup>th</sup> and 22<sup>nd</sup> of May 2009. For identification and authentication, they used the citizen card (the Austrian model of a smart card with digital signature) and a suitable smartcard-reader device, which was handed out for free. The anonymity was performed by using a cryptographic protocol in the post-voting phase, similar to a paper based postal voting procedure. The e-voting servers were placed in two data centers of the Federal Computing Centre (Bundesrechenzentrum) to allow for fail-safe operation.

While the discussion around e-voting was rather controversial with clear pro and con positions, and marked a first nation-wide discussion around remote voting in general. For future uses of e-voting in Austria the penetration of identification and authentication means has to be raised as well as a more positive atmosphere amongst the stakeholders has to be reached.

## 1 Background

The first legally binding election offering a voting channel through the Internet in Europe took place at the University of Osnabrück (Germany) on February 2nd and 3rd of 2000 [FoIn00]. This served as the initial starting point for concrete thoughts around the use of electronic means in the elections to the Austrian federation of students. In May of that year the chairman of the federation of students took this as a reason to request the introduction of remote voting (either postal or Internet voting) to its elections in a public consultation process on the Hochschulrinnen- und Hochschülerschaftsgesetz (law on the federation of students) [Fais00]. Following this request a project group was installed consisting of members of the Federal Ministry of Science and the federation of students. This group decided to foster the development around electronic voting by piloting it at the Vienna University of Economics and Business Administration (WU). In the following months the legal grounds were laid for a first use in the federation of students elections (Hochschulrinnen- und Hochschülerschaftswahlen) taking place in spring 2001.

However in March of 2001 the project was stopped due to a continuous delay in the distribution of smart cards bearing a digital signature to the students of the WU [WUFI01].

Two years later the research group E-Voting.at at the Institute of Information Processing and Management at WU developed an E-Voting prototype for a shadow election in parallel to the paper-based federation of students elections in May of 2003 [PKKU03]. 978 students participated in this test where they cast an additional electronic to the paper vote. For the 2004 election to the Federal President this setup was repeated and a shadow election was conducted where all 20.000 students at WU could participate [PKKU04]. In the same year the then Federal Minister for Interior, Ernst Strasser, started an inter-ministerial working group to evaluate the constitutional, technical and international questions around a potential introduction of e-voting in Austria. This group recommended to first making experiences in elections to self-governing bodies like the chamber of commerce or the federation of students. Furthermore it came to the conclusion, in order to introduce e-voting on federal level it would need to be included in the constitution [AG04]. In 2007 a research assignment to the Federal Ministry of Interior was agreed in the coalition paper of the XIII. Government to investigate e-voting.

On May 11th 2007 the Federal Minister of Science Johannes Hahn announced publicly at a speech at University of Linz to offer e-voting for the first in the 2009 elections to the federation of students [Hahn07]. This was the basis for the first legally binding e-voting project in Austria.

## **2 The Project**

The first step in this project was a feasibility study conducted in summer of 2007 [Krim07]. The main task was to integrate e-voting without compromising the existing paper-based voting in the polling station. To do so, an additional voting channel via the Internet was to be offered, from Monday 8:00 through Friday 18:00 in the week before the paper-based election days. During these days, all students of Austrian universities should have the possibility to participate in an Internet election without pre-registration. For identification purposes the Austrian citizen card (a smart card bearing a digital signature) in accordance with section 2 nr 10 of the Austrian E-Government law 2004 was to be used. After the end of the Internet-based vote casting, the votes were to be stored in an encrypted way until the general counting of votes at the end of the last voting day. Students, who had voted through the Internet, would be marked “voted” in the voter register and thereby guaranteeing the one-man-one-vote principle. The next step was then to adapt the legal framework.

## **3 Legal Basis**

The Federation of Students law 1998 (HSG) and the corresponding decree Federation of Students Election Regulations 2005 (HSWO) are the two legal texts forming the grounds for this project.

In Austrian self-governing bodies are regulated by national law passed by the parliament. In the course of the initial discussion around e-voting the national parliament passed an amendment to the Federation of students law in 2001 [HSG01]. It followed the principal of technology neutrality and only regulated certain corner stones. In section 34 paragraph 4 HSG 1998 the use of electronic signatures for identification purposes in accordance with the Austrian signature law, as well as the data protection law 2000 (DSG) were regulated. This led to the fact that for the e-voting system had to be approved by the Austrian data protection commission as it handles sensible data by interpretation of section 18 paragraph. 2 DSG. Furthermore the voting system has to provide technical means for the control of the electoral process to the election commissions.

The law also enabled the minister of science to introduce e-voting by the way of a decree, which included more detailed regulations for the e-voting system, like

- A definition of terms
- Change of time periods and mile stones for the electoral processes of the federation of students election
- Introduction of an additional voting channel
- Introduction of an election administration system

## 4 Diffusion of Smart Cards

A major challenge in the project was to distribute the Austrian citizen card amongst the students, as penetration with this technology was limited at the start of the project. For this the Austrian chancellery, the Federal Ministries for Finance and Science initiated the project [studi.gv.at](http://studi.gv.at) to foster the adoption of this new technology in fall of 2008. The project took place in parallel to the e-voting project due to synergies and both projects benefitting from each other. The main focus was to raise the public awareness amongst students for the citizen card itself as well as to promote services accessible with it.

The Austrian citizen card is an integral part of the social security card which every member of the Austrian social security system possesses<sup>1</sup>. To activate one's citizen card, a 10 minute procedure has to be done where a qualified person checks the activator's identity and then he/she can freely enter two PIN codes.

To raise the number of activations several activities were started

- The website [studi.gv.at](http://studi.gv.at): this website provided information on the digital signature, the smart card itself as well as how students can make use of it. While in fall semester the focus was on general applications, the summer semester made a complete turn towards electronic voting as an application for the smart card.
- Distribution of free-of-charge card readers: Every student, who activated his/her citizen card, got a card reader for free.
- Posters and flyers promoted the project.
- Tutors: As the activation required a qualified person, 22 tutors coming from different universities around the country who would then activate as many students as possible using a laptop with 3G data cards and explain the new technology to the potential users.
- As the project moved on, the tutors were trained to train other students for this activation procedure so that a snow-ball-effect could take place.

In general the project [studi.gv.at](http://studi.gv.at) was very successful as the number of citizen card users on paper reached 14.000. While in the beginning the numbers were rather low, the closer it got to the e-voting taking place in May 2009, the more students activated their smart cards. The project could be divided into four phases:

- Initial phase:                    October to December 2008
- Pre voting phase:                January to April 2009
- Voting phase:                    May 2009
- Post voting phase:                June 2009

---

<sup>1</sup> The citizen card basically is a functionality available not only to the social security card but also Austrian bank cards, credit cards etc.

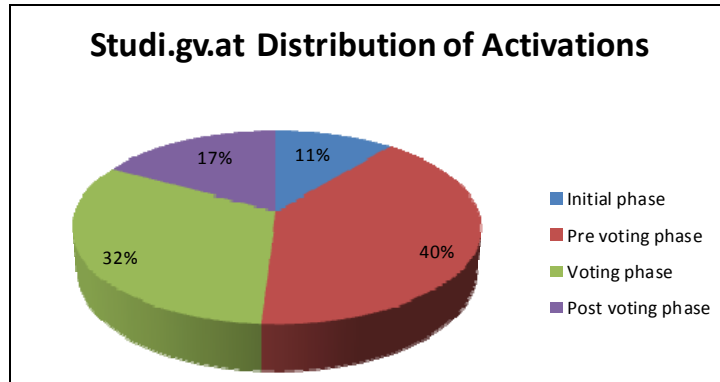


Figure 1: Distribution of Citizen Card Activations

#### 4 The E-voting Process

The e-voting process from the point of the voter - amending it with certain steps happening in the e-voting application – took place as follows:

1. First the website <https://www.oeh-wahl.gv.at> was opened and then the voter chose the field “To the electronic vote”
2. Then the students selected the university at which he/she wanted to vote electronically. In case one wanted to vote for more than one university this step had to be repeated each time.
3. After the selection of the university the voter got concrete descriptions how to use his/her citizen card
  - a. First the card reader had to be connected to the computer and the citizen card inserted
  - b. Then the voter could either use a locally installed or a web-browser-based solution of the so-called citizen card environment, which basically is a driver set for web applications to access the smart card.
  - c. Then the voter had to input a four-digit PIN-code which released his/her identity to the voting application
  - d. This identification procedure was concluded with the authentication using the digital signature on the smart card which was activated by entering a six-digit PIN-code.

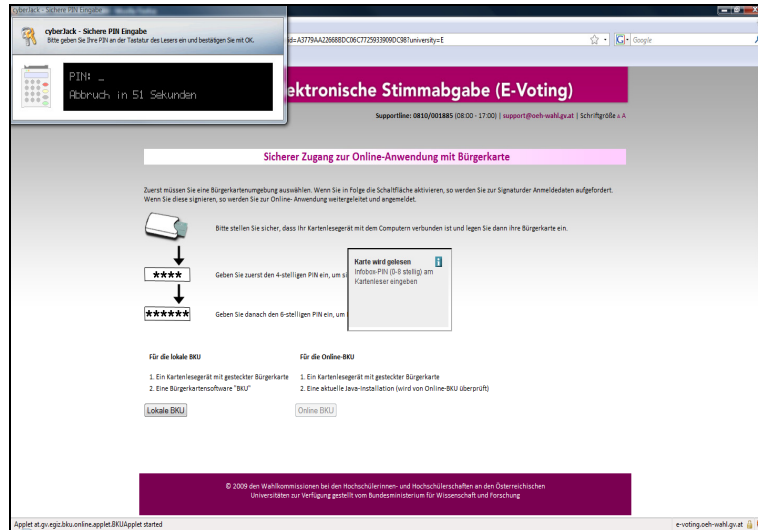


Figure 2: E-voting screenshot with PIN-code

4. After successful identification and authentication a ballot sheet was displayed for every race the voter was eligible to vote in. Normally an average student would cast two ballots
  - a. The first ballot sheet was for the university board of the federation of students. Here one group could be elected.
  - b. The second and more ballot sheets were for the study board representation. Here up to five student representatives could be elected.
5. Invalid votes could be cast by either not selecting any choice or by selecting too many.
6. After all ballots were cast an overview with all choices was displayed to the voter and had to be confirmed. This should prevent junk votes.
7. The confirmation took place with an affidavit where the voter confirmed to have cast the ballot in person and not have been influenced by a third person. This had to be signed digitally again with his/her six digit PIN-code.
8. The voting system showed after the successful vote a confirmation code. This code could be used after the end of the election to check whether one's vote was counted.

In the following figure we tried to amend this process with the cryptographic steps taking place similar to the process when filling out a postal vote.

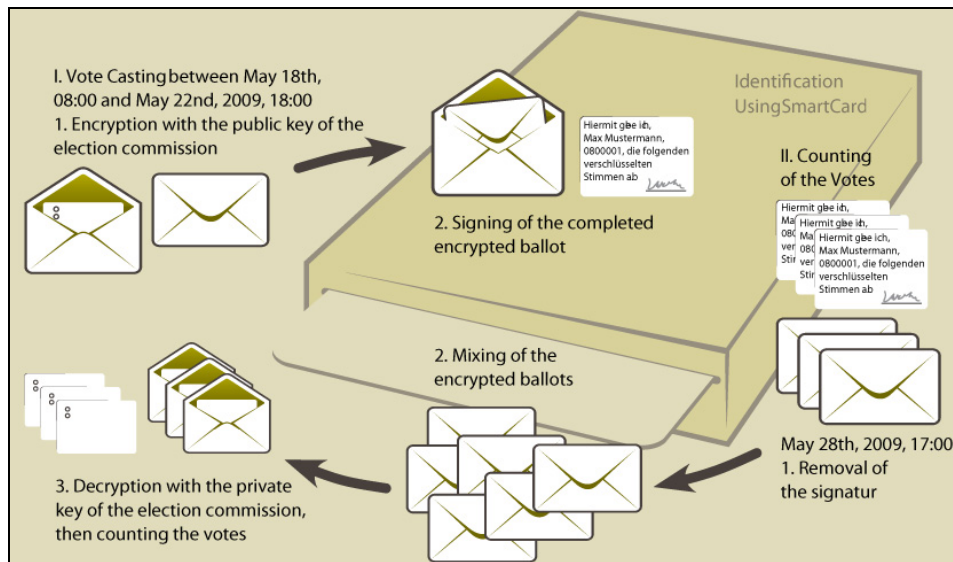


Figure 2: Overview of the E-voting Process

## 5 Pre Voting Phase

The project can be divided into three phases – (i) the pre voting, (ii) the voting, and (iii) the post voting phase. While the voting phase was the most intense period, the preparatory steps were manifold. A first step was the certification process.

### 5.1 Certification

The components of the e-voting system, which were used for vote casting and verification of the voters' identity, had to be certified 60 days before the first day of use by the independent certification body A-Sit established by the Austrian signature law<sup>2</sup>. The standard against which the e-voting system is checked against was the Council of Europe recommendation on legal, operational and technical standards for electronic voting [CoE04].

<sup>2</sup> The legal basis is laid down in section 64 paragraph 3 HSWO 2005 and section 34 paragraph 6 HSG 1998.

The certification lasted from December 1 2008 till March 25 2009 and was conducted using the source code as well as technical documents written by the e-voting provider. A-Sit checked whether the security architecture of the software was able to fulfill the requirements in the law. Furthermore the source code was used to verify if the described architectural protection methods were also implemented correctly. On March 27 2009 A-Sit published the certification [ASit09].

### **5.2 Usability Test**

On March 18 2009 two universities<sup>3</sup> conducted a usability test. Aim was to verify the actual ease of use of the e-voting system and to collect feedback from the students. These comments were reviewed critically and implemented in the final version of the software.

### **5.3 Vote Eligibility Check**

The vote eligibility check was offered from 23<sup>rd</sup> to 30<sup>th</sup> of April 2009. This was the first possibility to use the citizen card within this project. Here a single voter could check his/her own eligibility to vote. Around 370 persons made use of this opportunity. It was noted that a number of people had problems remembering their PIN-codes for the citizen card. During the whole time of the eligibility check a support hotline was offered.

In case a voter found an error with his/her personal voting rights, he/she had the possibility to appeal against it with the election commission at the respective university. On the basis of these appeals missing voting rights were corrected after decision by the election commissions.

### **5.4 Review of Certification Report by Members of the Election Commissions**

The minister has to provide members of the election commissions following section 64 paragraph 3 and 7 HSWO 2005 with the possibility to review the certification report and the source code of the e-voting system software.

This review took place on 8<sup>th</sup> of May 2009. The participants had to sign up for this occasion. Based on the regulation only members of the elections commissions were allowed to participate, which count for 250 persons.

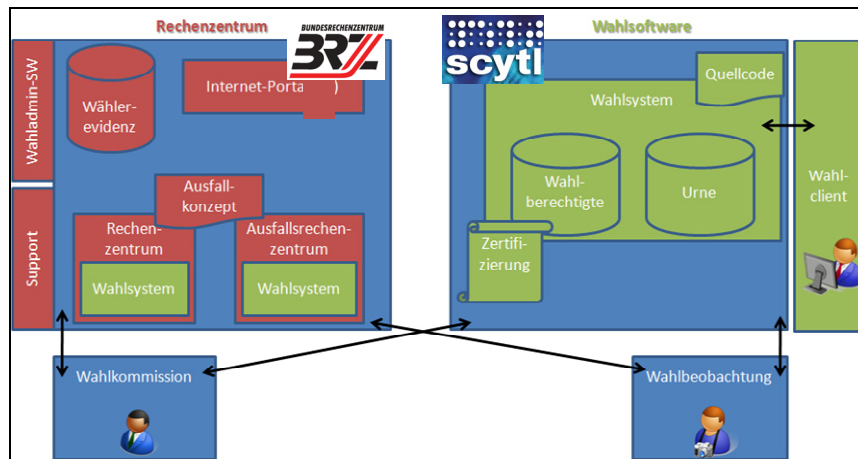
The review meeting was designed to accommodate all of them, however only 28 took part in the event. At the beginning the agenda was discussed with the participants. It was arranged in sessions, where experts – including the developers of the system – presented the underlying principles. In parallel the certification report and the source code could be reviewed and questions asked to the experts.

---

<sup>3</sup> Vienna University of Economics and Business Administration and University of Leoben



## 5.5 Fail-safe Operation of the E-voting Servers



**Figure 3:** Overview Infrastructure

The servers were operated at two separate locations:

- Federal Computing Center (Bundesrechenzentrum GmbH)
- Parallel Computing Center

The two computing centers were about five kilometers apart from each other. Both locations met highest international standards regarding physical security, energy supply, fire protection, access control systems, recording systems (real time video surveillance, access logging).

The e-voting system was classified as highly critical system and was underlying special security mechanisms within the federal computing center (BRZ).

All components were put in a security rack in each computing center location. Access to the protected zone around the security rack in the server room was only possible for authorized personnel. Access of any kind was logged and controlled by the security control center.

Additionally both security racks were secured using steel cables and cable seals from the point of installation till the secure data destruction. Each single cable seal was registered using a unique number.



**Figure 4:** Sealed security rack

### **5.6 Ethical Convention on E-voting**

In the field of e-voting the Council of Europe has developed with the 2004 recommendation on legal, operational and technical standards [CoE04] a very important instrument. Since then it has observed the developments in its member countries on this issue. In communication with the federal election commission of the federation of students elections, the Council of Europe recommended them to publish an ethical convention on e-voting based on the experiences in Estonia [TSBA07]. The commission developed an initial version and forwarded it to the commissions at the respective universities. For future elections it deems necessary to make a broad discussion process on this convention in a timely distance to the election days (on a political level and also in the public sphere).

## **6 The Voting Phase**

230.479 students were eligible to vote at the 21 Austrian universities where the federation of students elections 2009 took place. A total 375 races had to be decided, consisting of 21 university body elections and 354 study body elections. 2,411 candidates campaigned for 1,633 mandates.

On Monday, 18<sup>th</sup> of May 2009 at accurately 8:00 the electronic voting was started. The system automatically opened the vote casting which was observed by several representatives of the media. Shortly afterwards the first legally binding vote was cast successfully.

The electronic voting ended technically successful on Friday, 22<sup>nd</sup> of May 2009 at 18:00. Until then 2,161 students participated in the elections.

During the electronic voting the servers and the number of participants at the 21 universities could be watched in a 24hrs accessible observation room at the federal computing center. There a screen was directly attached at the database server to allow for election observation.

On the first two days of the e-voting the Austrian Federal Ministry of European and International Affairs had organized an international seminar on voting from abroad. The participants watched the whole process and concluded that e-voting election observation must allow for an end-to-end observation of all process steps. An observation solely on election day allows only for limited assessment [VEVS09].

After the e-voting voting channel was closed, the voter directories at the universities were updated in accordance with which voting rights were used by participants in the e-voting. The paper based election took place from Tuesday, 26<sup>th</sup> to Thursday 28<sup>th</sup> of May 2009. Here for the first time an election administration system was offered to all election commissions at the 21 universities, including the approximately 50 sub-commissions.

## **7 Post Voting Phase**

In the post voting phase the counting of the votes was started right after each polling station had closed. While the paper-based votes were counted right at the respective polling stations, the electronic votes got counted at the Federal Computing Center where representatives of the federal election commission of the federation of students elections were present, as well as from certification body A-Sit, and the operational team from the Federal Computing Center, after the last polling station had closed at 17.00. After detailed security and documentation procedures were completed it took only 1.5 hours in total to come up with the final e-voting results. A special challenge was the aggregation of the electronic and paper-based results, as some election commissions had problems to operate the election administration system which was used for this purpose. This was especially unfortunate as this led to a disappointment with the media for whom e-voting mainly is a tool for faster results calculation.

Three weeks after the election days all data – but the votes and protocols – were destroyed using physical and then thermal destruction.

## 8 Conclusions

In this Austrian premiere with a the first implementation of a remote electronic voting channel in a legally binding election it was shown successfully how a participation via the Internet is possible in a political decision making process. Hereby many experiences – common to pilot projects – were made. This includes especially the adaptation of paper election processes to the requirements of processing electronic votes as well as the intensive public discussion. Especially the public discourse had to be led and was very important especially to the topic of e-voting as well as to the discussion remote voting channels in Austria in general.

## Bibliography

- [AG04] Arbeitsgruppe ‚E-Voting‘ (2004): Abschlussbericht zur Vorlage an Dpr. Ernst Strasser, Bundesminister für Inneres, Wien, [http://www.bmi.gv.at/wahlen/wahldownloads/E-Voting/Abschlussbericht\\_E-Voting\\_2004\\_11\\_29.pdf](http://www.bmi.gv.at/wahlen/wahldownloads/E-Voting/Abschlussbericht_E-Voting_2004_11_29.pdf)
- [ASit09] A-Sit Certification, published at [http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen\\_hsg/index.php](http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_hsg/index.php)
- [CoE04] Council of Europe: Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11, Council of Europe, Strasbourg 2004.
- [Fais00] Faißt, Martin: Stellungnahme der Österreichischen Hochschülerschaft anlässlich der Änderung des Bundesgesetzes über die Vertretung der Studierenden an den Universitäten – Hochschülerschaftsgesetz 1998, May 15 2000.
- [FoIn00] Forschungsgruppe Internetwahlen, Zweiter Zwischenbericht zum Projekt ‚Strategische Initiative: Wahlen im Internet‘ nach Abschluss der Wahlen zum Studierendenparlament der Universität Osnabrück am 2. Feb. 2000, Osnabrück, 2000.
- [Hahn07] APA: Wissenschaftsminister Hahn will E-Voting bereits bei ÖH-Wahl 2009. Aussendung APA0431, May 11 2007, Vienna.
- [HSG01] Hochschülerinnen- und Hochschülerschaftsgesetz 1998, passed on Feb. 1, 2001.
- [Krim07] Krimmer, Robert: Machbarkeitsstudie – Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektr. Abstimmungsverfahren, Vienna, 2007.
- [TSBA07] Trechsel, A., Schwerdt, G., Breuer, F., Alvarez, M.(2007): Internet Voting in the March 2007 Parliamentary Elections in Estonia, Florenz, [http://www.vvk.ee/public/dok/Coe\\_and\\_NEC\\_Report\\_E-voting\\_2007.pdf](http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf)
- [PKKU03] Prosser, Alexander; Kofler, Robert; Krimmer, Robert; Unger, Martin-Karl (2003): Die erste Internet-Wahl Österreichs. Working Papers of the Institute for Information Processing and Management, Nr. 04/2003, [http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01\\_574.pdf?ID=epub-wu-01\\_574](http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01_574.pdf?ID=epub-wu-01_574)
- [PKKU04] Prosser, Alexander; Kofler, Robert; Krimmer, Robert; Unger, Martin Karl (2004): E-Voting Wahltest zur Bundespräsidentchaftswahl 2004, Working Papers of the Institute for Information Processing and Management, Nr. 01/2004, [http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01\\_714.pdf?ID=epub-wu-01\\_714](http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01_714.pdf?ID=epub-wu-01_714)
- [VEVS09] Bundesministerium für europäische und internationale Angelegenheiten: E-voting seminar. <http://www.bmeia.gv.at/botschaft/auslandsoesterreicher/ratgeber/wahlen/e-voting-workshop-2009.html>
- [WUF101] Hochschülerinnen- und Hochschülerschaft an der Wirtschaftsuniversität Wien (2001): WU-Flash, Ausgabe 025, Newsletter May 5 2001, <http://flash.oeh-wu.at/pipermail/wu-flash/2000-May/000037.html>

# Scantegrity Mock Election at Takoma Park

Alan T. Sherman (UMBC)<sup>1</sup>, Richard Carback (UMBC),  
David Chaum, Jeremy Clark (UWaterloo),  
Aleksander Essex (UOttawa), Paul S. Herrnson (UMCP),  
Travis Mayberry (UMBC), Stefan Popoveniuc (GWU),  
Ronald L. Rivest (MIT), Emily Shen (MIT),  
Bimal Sinha (UMBC), Poorvi Vora (GWU)

<sup>1</sup>Contact author: Cyber Defense Lab  
University of Maryland, Baltimore County (UMBC)  
Baltimore, MD 21250, USA  
[sherman@umbc.edu](mailto:sherman@umbc.edu)

**Abstract:** We report on our experiences and lessons learned using Scantegrity II in a mock election held April 11, 2009, in Takoma Park, Maryland (USA). Ninety-five members of the community participated in our test of this voting system proposed for the November 2009 municipal election. Results helped improve the system for the November binding election.

## 1 Introduction

On April 11, 2009, ninety-five voters cast ballots on the Scantegrity II voting system during a mock election held at the Community Center in Takoma Park, Maryland, coinciding with Takoma Park’s celebration of Arbor Day. The purpose of this exercise, which we call Mock1, was to demonstrate and tune Scantegrity’s capability in preparation for the Takoma Park municipal election in November 2009 [Car10]. The November election was historic — the first time any end-to-end (E2E) cryptographic voting system with ballot privacy has been used in a binding governmental election. This paper, a short summary of which appears as [She09], describes our experiences using Scantegrity in Mock1 and presents and interprets data collected through questionnaires, unobtrusive observations, and independently-administered focus groups.

Scantegrity [Cha09] is a software-independent cryptographic audit system that overlays a traditional optical-scan voting process. Voters mark paper ballots with revealing ink, exposing a randomly chosen confirmation code in each marked oval, which the voter may choose to write down on a detachable ballot chit. After polls close, each voter has the option of checking her confirmation codes online, to verify that her vote has been recorded as intended. Furthermore, Scantegrity is universally verifiable: using special software of his or her choice, anyone can verify online that the tally was computed correctly from the official data (and during the actual election, two auditors even wrote their own software for this purpose and made it public).

There has been some debate within the voting systems' community about how easily cryptographic end-to-end systems could be understood, used, and administered, but there is little evidence from which to draw any conclusions.

Mock1 is part of a larger research project to measure how easy Scantegrity is for voters to use and poll workers to administer. The research also studies how well voters and poll workers accept this revolutionary system. Mock1 only tested the Scantegrity voting system and was required to mimic a binding election. We closely followed procedures that were later used in November's binding election. These requirements constrained research methodologies, but were needed to assess viability of Scantegrity in the binding election. We plan to carry out a second mock election, Mock2, and expert review, which will be a field test comparing Scantegrity with a commercial optical scan voting system.

Our hypothesis is: Voters and election officials will accept and have confidence in Scantegrity as a viable practical high-integrity voting system. They will find it reasonably easy to use and administer, compared with traditional optical scan voting. A statistically significant number of voters will verify their votes online, and a statistically significant number of them will detect errors, if present, to produce high assurance in the election outcome.

At Mock1 we measured Scantegrity's performance through surveys, observations, and focus groups. Eighty voters and all six Takoma Park poll workers filled out questionnaires about their experiences with Scantegrity, including questions about how easy the system was to use and administer and how well they understood and accepted the system. Two unobtrusive observers watched and timed fifty-three of the voters as they voted. A professional moderator led two focus groups: one for all six poll workers and one attended by four voters. After polls closed, twenty-nine of the voters (31%) verified their votes online, using a privacy-preserving receipt on which each voter copied confirmation codes exposed during the voting process for their ballot choices.

In the rest of this paper, we briefly review selected previous work, explain our election and research methods, present and discuss our results, state recommendations, and explain our conclusions. The Scantegrity website [Scan] lists additional details about Mock1, including questionnaires and the agreement with the City of Takoma Park.

## **2 Previous Work**

There have been several usability studies on voting systems and vote-verification systems, but no major usability study has been conducted on any E2E voting system. The only previous usability studies on E2E systems have been the preliminary studies mentioned above and a few student projects at UMBC (on Punchscan), MIT (on ThreeBallot), and Univ. of Surrey, England (on Prêt à Voter). Scantegrity and its predecessor Punchscan [Punch] were exercised by running student elections, organizational elections, mock elections, the 2007 VoComp International Voting System Design Competition [Voc07], and surveys [Scan]. Scantegrity has been used at the following events: Mock Presidential Elections at MIT and George Washington

University (November 4, 2008, Cambridge, MA, and Washington, DC); Mock Board of Directors Election for the Ottawa Canadian Linux Users Group (April 1, 2008, Ottawa, Canada); and a survey at the Claim Democracy Conference (November, 2007, Washington, DC). Essex *et al.* [Ess07] document their use of Punchscan in the 2007 student elections at the University of Ottawa.

RIES [OSCE07, Hub05] was used twice in 2004 in the Netherlands in a government Internet election. This system is voter verifiable and universally verifiable, but allows voters to prove how they voted. Helios [Adi09] was used in March 2009 to elect the President of the Université catholique de Louvain using remote voting. This system neither protected against undue influence nor compromise of the voter's computer. Byrne *et al.* [Byr07] experimentally compared the usability of punch cards, lever machines, and paper ballots; they found that voters made fewer errors with paper ballots.

Using expert review, laboratory studies, and a field experiment with 1540 participants, Herrnson *et al.* [Her08, Bed03, Con09, Her06] found that voting system interface and ballot styles had an impact on voter satisfaction, the need for help, and voters' abilities to cast their ballots as intended. They also demonstrated that the most frequent error made by voters was voting for a candidate other than the one they intended to support, usually a candidate listed on the ballot immediately before or after the intended candidate. This type of error is more serious than the errors associated with the residual vote because, in addition to denying an intended candidate a vote, it gives a vote to a candidate's opponent. They found that results of this experiment varied by voter demographics and voting experience. They also found that design issues and voter backgrounds influenced not only the voters' evaluations of different voting systems, but also their voting accuracy. Laskowski [Las04] offers practical metrics for voting system usability, and draft voluntary guidelines [EAC07] address usability.

There is a large body of knowledge about the usability of both computer systems [Shn05] and security [Cra05], but none of this work addresses how well and easily voters and election officials will be able to use Scantegrity.

Alvarez *et al.* [Alv08] and Newkirk [New08] frame public opinion about voting technologies. Newkirk finds that public opinion about voting systems has remained remarkably stable between 2004 and 2008. Direct Recording Electronic (DRE) systems were the top-rated systems in terms of voter trust throughout most of this period, followed closely by precinct count optical scan (pcos) systems. Fewer voters trusted vote-by-mail, central count optical scan systems, and Internet voting. There were some variations by background characteristics, but the overall stability in levels of trust and the near parity of DRE and pcos systems are remarkable given questions raised about these systems by serious scholars, political activists, and conspiracy theorists on the blogosphere. Indeed, public confidence in election count accuracy was ranked only second to public trust in banks and financial institutions. More confidence was voiced for elections than medical providers (including hospitals and clinics), universities and schools, large corporations, and the government.

Given the impact of public opinion on the decisions of policymakers who purchase voting systems and oversee other matters related to the administration of elections, it is important to study public reactions to voting systems. The fact that no such study has been conducted on any E2E system to date is a significant shortcoming. The Mock1 test of Scantegrity is a first step in addressing this shortcoming.

### **3 Methods**

We now describe the voting and research procedures used in Mock1. Our research protocols and questionnaires were approved by UMBC's Institutional Review Board, as required for experiments with human subjects. Polls were open from 10 AM to 2 PM

#### **3.1 Voter Experience**

Each voter first approached a welcome table located outside the polling room. After signing a consent form, the voter proceeded to an adjacent check-in table. There, a poll worker looked up the voter's name in a poll book and issued a voter authority card. The voter then entered the polling room and presented the voting authority card to poll workers at the ballot issue table, who issued a Scantegrity ballot secured to a locked clipboard with privacy sleeve (see Appendix B).

The voter proceeded to one of three voting areas, each with a cardboard privacy shield. Using a special pen with revealing ink, the voter marked her ballot choices by marking the selected ovals with the pen. The revealing ink exposed a two-character confirmation code in each marked oval. Optionally, while also using the special pen, the voter could write down these confirmation codes on a detachable ballot chit, treated with reactive ink. As required by Takoma Park for municipal elections, Instant Runoff Voting (IRV) [Pou08] was used, so each voter was asked to rank each candidate in order of preference.

Appendix A shows the Mock1 ballot, which featured four questions about trees. To avoid possible confusion, Takoma Park officials required that races on our Mock1 ballot not resemble those on official ballots. November's official ballot had two races (mayor and ward council member) per ward. The municipal election can also have ballot questions.

Instead of voting on the issued ballot, each voter had the option of performing a "print audit" to verify that the ballot had been correctly printed. To do so, the voter walked to a voter assistance table and followed instructions from a poll worker. The poll worker marked the ballot spoiled and exposed all confirmation codes. The voter was permitted to copy information from the ballot to take home. A poll worker then escorted the voter back to the ballot issue table to receive another ballot. Each voter was allowed to receive up to three such ballots. We used a similar procedure if the voter unintentionally spoiled a ballot (e.g., by marking the wrong choice).



After marking the ballot, the voter proceeded to the scanning table. A poll worker unlocked the ballot from the locked clipboard and scanned the ballot. Looking at a touch-screen display connected to the scanner, the voter confirmed that the ballot was scanned. Without showing the voter's ballot choices, the touch-screen display warned the voter if the scanner detected any over- or under-voted questions. At this point, the voter could either return to the voting area with the ballot or cast the ballot by pressing the cast button on the display. The poll worker then tore off the chit and gave it to the voter, and dropped the ballot into the ballot box. Throughout the scanning process, a privacy sleeve hid the ballot choices. The chit provided instructions on how the voter could optionally verify her vote online after polls closed.

### **3.2 Research Protocols**

Any consenting adult who showed up was permitted to vote. At the request of Takoma Park, to encourage children to become involved in voting and new voting technology, assenting children twelve to seventeen years old were also permitted to vote, with parental consent. We advertised the event through e-mail, Web pages, local TV, and in the Takoma Park Newsletter [TPN09]. Despite the rain, 105 people signed consent forms.

Sitting in the polling room in the place reserved for official observers, two unobtrusive observers watched as many voters as possible, filling out voter observation sheets. Each observer recorded the time an observed voter spent from receiving a ballot to casting it. Each observer also noted how many times the voter spoiled a ballot, requested or received assistance from a poll worker, or appeared confused.

As each voter left the polling room, a researcher asked the voter if she would be willing to fill out a questionnaire. If yes, the researcher handed the voter a conventional clipboard with two two-sided questionnaires: a voter field test questionnaire and a demographics questionnaire. Form numbers linked the field test and demographics questionnaires filled out by the same voter.

As the voter returned the clipboard, the researcher asked the voter if she would be willing to return at 3 PM that day for a one-hour focus group. For each such willing voter, the researcher wrote down a telephone number and the demographics form number. The plan was to call eight of the willing voters, reflecting a diverse sample of voters as determined solely from the demographics form. However, given that only twelve of the 80 voters filling out questionnaires agreed to participate in a focus group, we invited all twelve willing voters, of whom four showed up.

We also conducted a separate one-hour focus group for all six poll workers as soon as possible after polls closed. Each poll worker also filled out a poll worker field test questionnaire and demographics form.

Voters could visit the online verification web site after polls closed. After providing consent and verifying their votes online, they were invited to fill out an online verification questionnaire and a short demographics form.

Aside from the consent form and list of telephone numbers on the focus group sign-up sheet, we did not collect any personal identifying information.

Originally, we had planned to link each voter's demographics questionnaire to her observation sheet and ballot (and thereby to her verification questionnaire). Ultimately, we decided not to do so, to avoid interfering with the election process, and to avoid creating the appearance of violating ballot privacy. Instead, we added a second short demographics questionnaire to the online verification experience.

For Mock1, Takoma Park poll workers and Scantegrity team members worked side-by-side to help the poll workers learn how to operate the system. By contrast, in the binding election in November, poll workers operated the system entirely by themselves.

## **4 Results**

This section summarizes data collected from our research instruments, including the voter demographics questionnaire, observations sheets, voter field test questionnaires, online voter demographics and verification questionnaires, and the voter and poll worker focus groups.

### **4.1 Unobtrusive Observations**

Figure 1 summarizes observations made by two unobtrusive observers watching fifty-three of the voters. The main difficulty was the length of time it took to vote, averaging about eight minutes from the time a voter received a ballot to the time the voter cast the ballot (not including time for check-in or instructions given before voter received a ballot). Much of the time was observed to be at the scanner table.

When voters asked for assistance and/or poll workers intervened, it was typically either because the voter did not know what to do after marking the ballot, or because the voter did not know what to do upon spoiling a ballot.

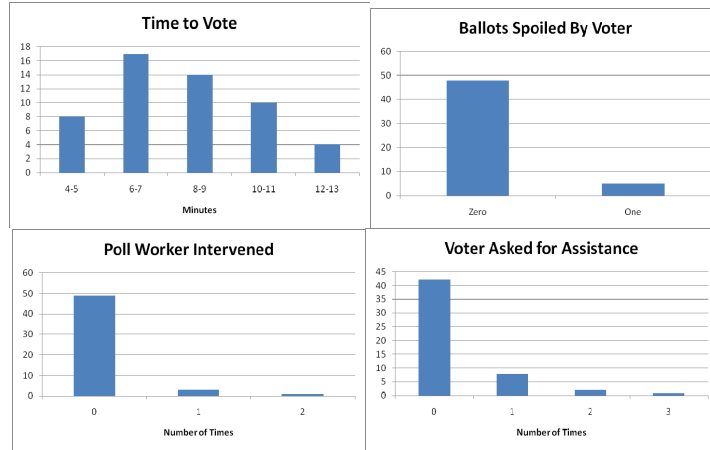


Figure 1: Summary of data from unobtrusive observations of 53 voters.

#### 4.2 Voter Demographics

Figure 2 summarizes voter characteristics of the eighty voters who filled out paper demographics questionnaires. These voters were not representative of the Takoma Park voting population. They had high family incomes and were highly educated, frequent computer users, mostly fifty to sixty years old, motivated, and able to get to the mock election on their own.

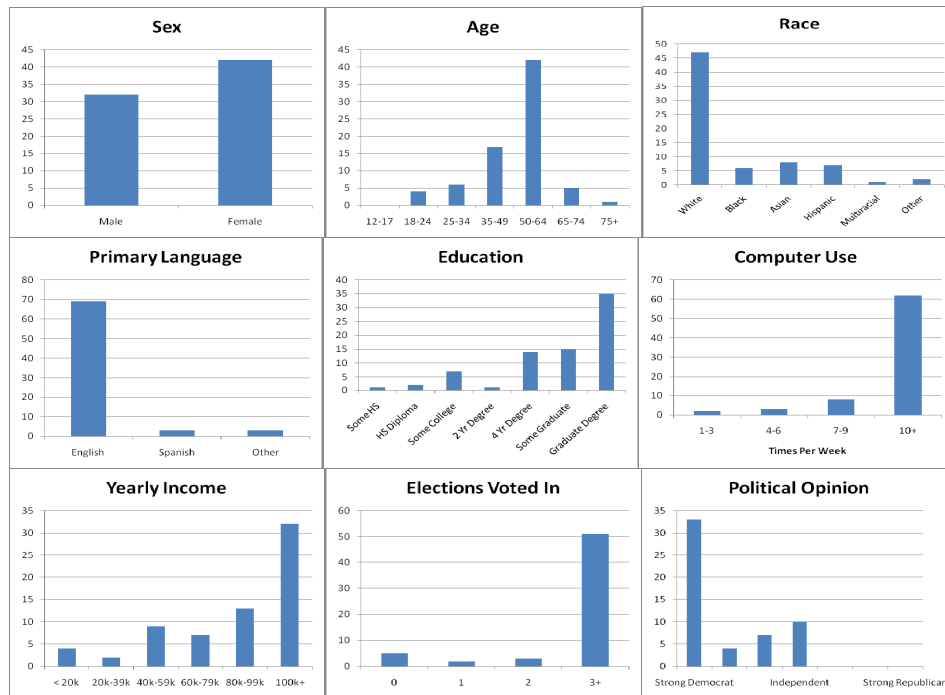
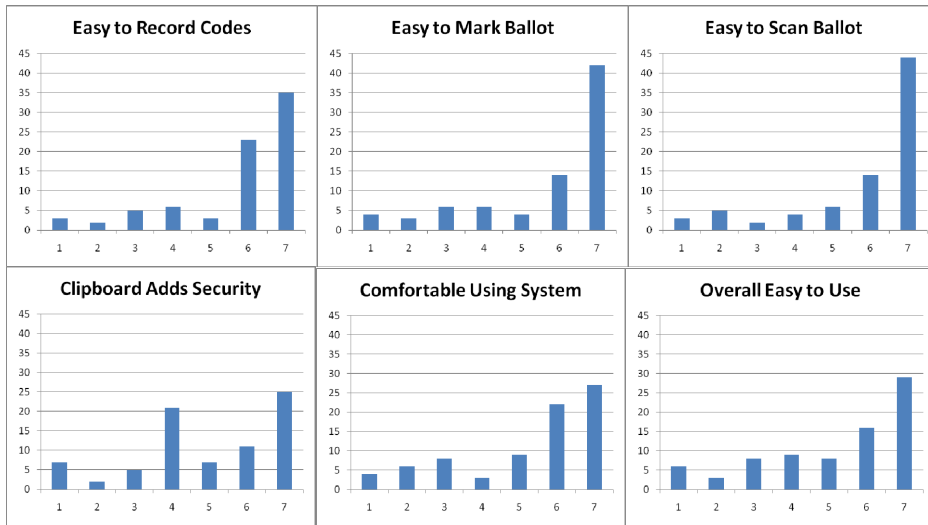


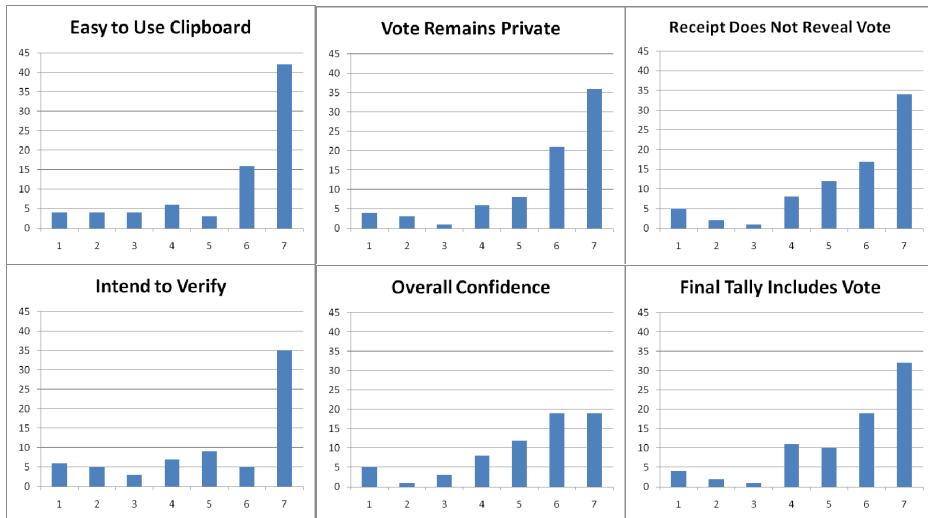
Figure 2: Summary and comparison of voter demographics from 80 responses to a paper questionnaire filled out by voters immediately after voting.

### 4.3 Voter Field Test Survey

Figures 3 through 6 summarize data collected from eighty field test questionnaires filled out by voters immediately after casting their ballots. We include all responses, even though it was apparent (from implausible answers to questions about ease of correcting errors and understanding of cryptographic details) that three respondents had likely reversed the seven-point Likert scale.



**Figure 3:** Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting.



**Figure 4:** Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting.

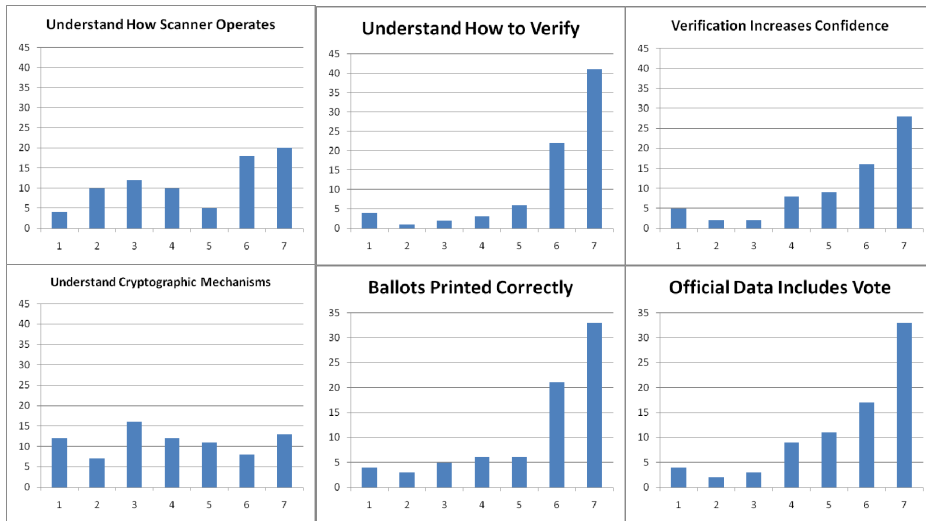


Figure 5: Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting

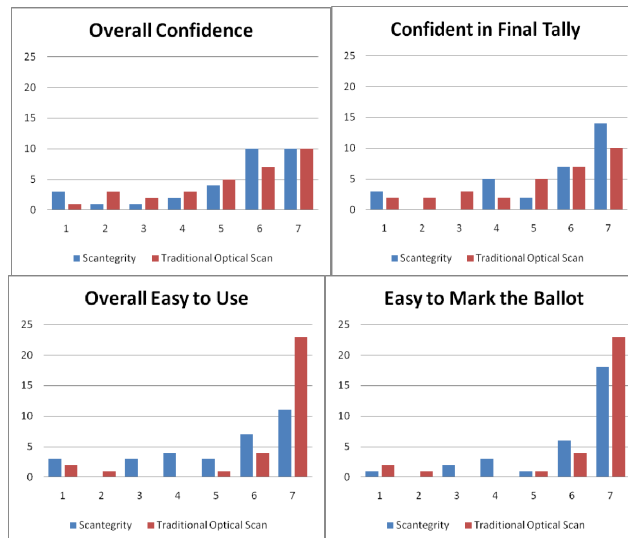


Figure 6: Summary of 31 responses to questions about Scantegrity and a comparison to answers from those same responders about traditional optical scan systems based on their recollection of their last experience with an optical scan system (1 = strongly disagree, 7 = strongly agree)

#### 4.4 Online Voter Verification Survey

As of April 15, thirty-one voters verified their votes online. Seven of these voters completed the associated online questionnaire. Table 1 summarizes the responses from these seven voters.

Q		1	2	3	4	5	6	7
1	I was able to complete the verification process.	0	1	0	0	0	2	4
2	I verified that my votes were correctly recorded as cast.	1	1	0	0	0	2	3
3	The verification system was easy to use.	1	0	0	0	0	1	5
4	I feel comfortable using the verification system.	1	0	0	0	0	3	3
5	I am confident the official data includes my intended vote.	0	1	0	2	1	1	2
6	I am confident the final tally includes my intended vote.	0	1	0	3	0	1	2
7	I am confident my vote is and will remain private.	0	1	0	1	2	2	1
8	Online verification increased my confidence in the results.	1	2	1	1	1	0	1
9	I understand how the online verification system works.	0	3	1	0	0	1	2
10	I have confidence in the online verification system.	0	1	0	4	1	0	1
11	Overall, I have confidence in Scantegrity.	0	0	1	3	2	0	1

**Table 1.** Summary of all 7 responses from the online verification questionnaire (1 = strongly disagree, 7 = strongly agree).

#### 4.5 Voter and Poll Worker Focus Groups

Four voters participated in the voter focus group. These came from the twelve voters who stated they might be available to participate, all of whom were invited. These four voters were not representative of the Takoma Park voting population: they were involved with municipal functions and some had helped bring voters to previous elections.

All six Takoma Park poll workers participated in the poll worker focus group. Each was experienced and had worked previous elections in Takoma Park. None are part of the Scantegrity Team. Because both groups expressed similar thoughts, we now summarize the main comments from both groups together, as reported by the moderator [Bau09]:

1. The process took too much time.
2. Providing instructions in one chunk at beginning was overwhelming.
3. The instructions were too complex, and there was too much explaining.
4. Although the voters in the focus group did not experience difficulties voting, some wondered if other voters in Takoma Park might experience difficulties writing down confirmation codes and verifying their votes online.
5. Vote casting at the scanning table took too much time.
6. Some poll workers disliked that a poll worker handled the ballot during scanning.
7. The scanner was finicky.
8. During scanning, the poll workers liked the feedback of seeing light on a flash drive blink, suggesting that the ballot was read.

9. The locked clipboard added time and complexity, but did not increase security.
10. Make the special pens available only in the voting area.
11. Poll workers felt that they should have been more in charge, especially of the flow of voters around the room.
12. Poll workers felt that the process could be sped up to make it viable for the binding election.

Finally, the moderator [Bau09] emphasized, “It is critical that all instructions are tested ahead of time on a range of people representative of the wider Takoma Park population to ensure they are clear and understandable” and that “[t]ranslations into other languages must also be tested.”

## 5 Discussion

The main two issues were that the process was too slow (taking about eight minutes to vote on average) and many voters found the instructions somewhat complicated. Much of the delay was caused by the scanning process and lengthy instructions given to voters. Fortunately, these problems are solvable through process simplification and improvement, better scanners, and careful human-factors testing.

Although there has been tremendous simplification of Chaum’s ideas from SureVote, through Punchscan to Scantegrity, the team had spent relatively little effort on testing and perfecting the human-factors details of the voting process, especially when carried out by typical voters. Some Mock1 voters were enthusiastic about the security features of Scantegrity, but most seemed not to care much about security, focusing primarily on the physical process of receiving a ballot, marking the ballot, and scanning the ballot. While such voter reactions are well known from the social science literature, it was nevertheless a dramatic learning experience to witness these reactions first-hand.

Although the Mock1 voters and participants in the voter survey group were not typical Takoma Park voters (many were self-selected as having an interest in the voting system to be used by the city, and some were just there to participate in the Arbor Day celebration), they provided useful feedback and expressed awareness of potential issues that might affect other voters. Factors affecting the slow voting process included lengthy instructions, redundant instructions, instructions for optional steps, use of the locked clipboard, writing down confirmation codes, tearing off the ballot chit, difficulty of correcting mistakes (for the few who unintentionally spoiled ballots), checking for over- and under-votes at the scanner touch screen, and a slow, finicky scanner.

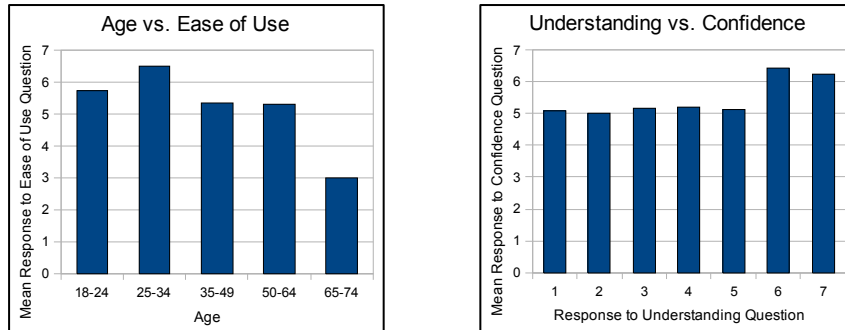
Our scanner caused significant problems. Ballots had to be inserted in a particular orientation. If they went in at too much angle, a corner could be unread. Some voters seemed confused that the touch screen did not show how they voted, but only for each race whether the race was over- or under-voted. After the voter pressed “cast,” feeding the scanned ballot into a privacy sleeve and dropping the ballot into a large ballot box was clumsy. Although these equipment, implementation, and process problems can be fixed, they would have created severe difficulties in an election with over 2,000 voters.

The locked clipboard worked poorly. It complicated and slowed down the process, made it difficult to drop ballots into the scanner, and added weight. Most voters felt it did not enhance security, despite its purpose of making it difficult to steal or swap ballots. At the scanning table, several voters mistakenly ripped their ballots off the locked clipboard. Technically, any ballot with torn locking hole was supposed to be invalid, but for simplicity this rule was not enforced.

Some elderly voters commented that they had difficulty reading the confirmation codes. Three voters reported that some confirmation codes blurred, especially if rubbed heavily, and one reported that the ballot paper deteriorated. On a positive note, marking the ballot with revealing ink produced perfectly darkened ovals: because there was no reactive ink outside the ovals, no darkening appeared there. Although this outcome was not the motivation for printing Scantegrity ballots with invisible ink, it appears evident that invisible ink yields a superior method for marking optical scan ballots. We supplied pointed “bullet” style special pens, to facilitate writing down the confirmation codes. Wider “chisel” style special pens, however, seem to work better for marking ovals.

Figure 7 shows correlations between survey responses on age and ease of use, and between understanding of Scantegrity and overall confidence in the system. As expected, overall, older voters found Scantegrity harder to use than did younger voters. Interestingly, most voters still had high confidence in Scantegrity, even if they felt they understood the system poorly. This finding runs contrary to a widely asserted notion that voters will not accept a system that they do not understand.





**Figure 7.** Correlation between age and overall ease of use, and between understanding and overall confidence in system. Voters under 65 years of age found Scantegrity easier to use. Voters who felt they understood the system very well had slightly higher confidence in the system, yet even those who felt they had a poor understanding of the system had a moderately high confidence in the system. Pearson correlation coefficients: age vs. ease of use: -0.20, understanding vs. confidence: 0.28. (1 = strongly disagree, 7 = strongly agree)

## 6 Recommendations

To simplify and streamline the process, we recommend the following:

1. Eliminate the locked clipboard.
2. Eliminate redundant instructions. At beginning of process, do not provide instructions for optional steps.
3. Use high-quality, fast, robust scanners—preferably of the type that automatically drops the ballot into the ballot box when the voter signals to cast the ballot. The scanner should accept ballots inserted in any orientation.
4. Add a printer to the scanner to provide a digitally signed receipt with the confirmation codes. Great care must be taken to ensure that this printer does not violate ballot privacy (Fink and Sherman [Fin09] suggest one approach).
5. Eliminate the tear-off chit. Instead, provide a separate sheet of paper to any voter who wishes to write down confirmation codes or other ballot information by hand.
6. Print confirmation codes with a restricted character set to avoid easily confused letters.
7. Use “chisel” style special pens for ease of marking ovals, selecting a small enough chisel width to permit writing down confirmation codes and write-in candidates.
8. Thoroughly analyze and test the voting process with many diverse voters.

## 7 Conclusions

The mock election demonstrated that Scantegrity can be effectively used in elections and is well accepted by voters. Survey data show that voters feel comfortable with the system and have confidence in it.

Mock1 revealed though that the flow of people through the voting process must be greatly improved. The implementation, procedures, voter instructions, and equipment of Scantegrity used in this election need to be simplified and streamlined. Although Scantegrity significantly simplifies the voting process from its predecessors SureVote and Punchscan, additional attention is needed to improve and fine tune the voter experience, including the physical processes of receiving, marking, and scanning the paper ballot.

After polls closed, thirty-one of the ninety-five voters verified their votes online, demonstrating that a sufficient number of voters will likely take advantage of the verification option in E2E systems. This percent of voters verifying their votes is consistent with that observed in our other Punchscan and Scantegrity trials. We conjecture, however, that in binding elections, the percentage will also depend on the degree of interest in and contention of the races.

Our findings include that the locked clipboard added complexity, but did not enhance security, and that revealing ink provides a superior technology for marking optical scan ballots with perfectly darkened ovals.

Even though many voters do not care much about security and tend to trust voting systems, a small and vocal group of political activists is very concerned about this issue. Deploying systems like Scantegrity fundamentally enhances outcome integrity and directly addresses those activists concerns.

Accessibility for voters with disabilities was not a focus of this study. In separate projects, our team is seeking better solutions for the vital challenge of making high-integrity voting truly accessible to differently-abled voters, including the blind.

Learning from Mock1, we implemented the following changes for the subsequent binding election: eliminated the locked clipboard, designed a new privacy sleeve, eliminated the monitor check at scanning, added a second scanner, built ballot feeders for the scanners, used a double-ended pen with chisel and bullet points, eliminated redundant instructions, improved signage and instructions at registration and in the voting booths, and used a separate receipt card rather than a tear-off chit.

Mock1 helped pave the way for Scantegrity's successful deployment in the November 2009 binding governmental election in Takoma Park [Car10]. Lessons learned from this feasibility demonstration helped streamline voter flow, reduce average voting time (from 8 min to 2.5 min), and improve instructions to voters.

## **8 Acknowledgments**

We are grateful to the many people who made this pilot study of Scantegrity possible, especially Anne Sergeant (Chair, Takoma Park Board of Elections), other members of the Board, Jessie Carpenter (City Clerk), and the Mock1 voters. Lynn Baumeister led the focus groups and offered numerous practical suggestions. Brian Strege and Fahad Alduraibi observed voters. Russell Fink, Douglas Jones, Sharon Laskowski, and Svetlana Lowry provided useful feedback. Esther Haynes offered editorial suggestions.

Sherman was supported in part by the Department of Defense under IASP grant H98230-09-1-0404.

Vora and Popoveniuc were supported in part by National Science Foundation under SGER grant NSF-CNS-0831149.

## Bibliography

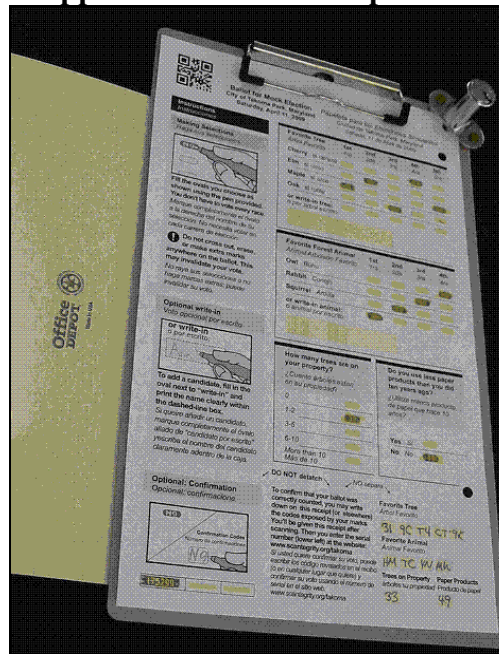
- [Adi09] Adida, B. *et al.* 2009. Electing a university president using open-audit voting: analysis of real-world use of Helios. In *Online proceedings of EVT 2009* [http://www.usenix.org/event/evtwote09/tech/full\\_papers/adida-helios.pdf](http://www.usenix.org/event/evtwote09/tech/full_papers/adida-helios.pdf)
- [Alv08] Alvarez, R. M., and E.T. Hall: 2008. *Electronic elections: The perils and promises of electronic democracy*. Princeton, NJ, USA: Princeton University Press.
- [Bau09] Baumeister, L. 2009. Mock election notes: Mock election, April 11. Takoma Park.
- [Bed03] Nederson, B. *et al.* 2003. Electronic voting system usability issues. In *Proceedings of the SIGCHI conference on human factors in computing systems*, 145-152.
- [Ben04] Bensel, R. F. 2004. *The American ballot box in the mid-nineteenth century*. New York: Cambridge University Press.
- [Byr07] Byrne, M. D., K. K. Greene, and S. P. Everett. 2007. Usability of voting systems: Baseline data for paper, punch cards, and lever machines. In *Human factors in computing systems: Proceedings of CHI 2007*, 171-180. New York: ACM.
- [Car10] Carback, R. *et al.* 2010. Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy, USENIX security 2010. <http://www.usenix.org/events/sec10/>
- [Cha09] Chaum, D., *et al.* 2009. Scantegrity: End-to-end verifiability for optical scan elections. In *IEEE Transaction on Information, Forensics, and Security - special issue on voting* 4 (4): 611-627.
- [Con09] Conrad, F., *et al.* 2009. Electronic voting eliminates hanging chads but introduces new usability challenges. In *International Journal of Human-Computer Studies* 67 (1): 111-124.
- [Cra05] Cranor, L.; and S. Garfinkel S. 2005. *Security and usability: Designing secure systems that people can use*. O'Reilley.
- [Ess07] Essex, A. *et al.* 2007. Punchscan in practice: An E2E election case study. Proceedings of the IAVoSS workshop on trustworthy elections (WOTE 2007).
- [Fin09] Fink, R., and A. T. Sherman A. T. 2009. Combining end-to-end voting with trustworthy computing for greater privacy, trust, accessibility, and usability (summary). In *Proceedings of the NIST workshop on end-to-end voting systems*, October 13-14.
- [Her06] Herrnson, P. S. *et al.* 2006. The importance of usability testing of voting systems. In *Proceedings of the USENIX/accurate electronic voting technology on USENIX/Accurate electronic voting technology workshop*. [http://www.usenix.org/events/evt06/tech/full\\_papers/herrnson/herrnson.pdf](http://www.usenix.org/events/evt06/tech/full_papers/herrnson/herrnson.pdf)
- [Her08] Herrnson, P. S. *et al.* 2008. *Voting technology: The not-so-simple act of casting a ballot*. Washington, DC: Brookings Institution Press.
- [Hub05] Hubbers, E., B. Jacobs, and W. Pieters. 2005. RIES: Internet voting in action. In *Proceedings of the COMPSAC*.
- [Las04] Laskowski, S. 2004. Improving the usability and accessibility of voting systems and products. NIST Special Publications SP 500-256.
- [New08] Newkirk, G. M. 2008. Trends in American trust in voting technology, March 17, white paper. InfoSENTRY Services.
- [OSCE07] Office for Democratic Institutions and Human Rights. 2007. The Netherlands parliamentary elections, 22 November 2006, OSCE/ODIHR election assessment mission report. Warsaw.
- [Pou08] Poundstone, W. 2008. *Gaming the vote: Why elections aren't fair (and what we can do about it)*. New York: Hill and Wang.
- [Punch] Punchscan. <http://www.punchscan.org/>
- [Scan] Scantegrity. <http://www.scantegrity.org/>
- [ScaT] Takoma Park Election Day Scantegrity Website. <http://www.scantegrity.org/takoma/>

- [She09] Sherman, A. T. 2009. Scantegrity mock election at Takoma Park (summary). In *Proceedings of the NIST workshop on end-to-end voting systems, October 13-14.*
- [Shn05] Shneiderman, B., and C. Plaisant. 2005. Designing the user interface, 4th edition. Addison Wesley.
- [Tako] City of Takoma Park. <http://www.takomaparkmd.gov/>
- [TPN09] Takoma Park Newsletter. 2009. This Arbor Day: Plant the seeds for election verifiability. April.
- [EAC05] United States Election Assistance Commission. 2005. Voluntary voting system guidelines. December.
- [Voc07] VoComp. <http://www.vocomp.org/>

### Appendix A: Ballot

Ballot shown smaller than actual size.

### Appendix B: Locked Clipboard



Locked clipboard resists chain voting.



## **Session 2: Sociocultural Issues of E-Voting**





# The role of trust, participation and identity in the propensity to e- and i-vote

Letizia Caporusso

Dipartimento di Sociologia e Ricerca Sociale  
Università degli Studi di Trento  
Via Verdi, 26  
38122 Trento, Italy  
[letizia.caporusso@unitn.it](mailto:letizia.caporusso@unitn.it)

**Abstract:** The paper analyzes the issue of citizens' propensity to deploy automated elections as a dependent of several ascribed and attitudinal factors. Data are drawn from a computer-assisted telephone survey carried out in the Autonomous Province of Trento, which through project ProVotE sponsors the largest program of touchscreen-based voting in Italy. Alongside socio-demographic variables such as sex, age, education, and occupation, we describe how socio-political attitudes such as trust, participation, and identity affect the propensity to vote by automated means. We conclude that, based on the binomial and multinomial logistic models we implemented, our data support the hypothesis of existing divides between those who are favourable to automation in elections and those who are not, the main cleavages being age and level of education. Furthermore, a greater degree of trust in the generalised other is needed in e-voting but not perceived in i-voting, while both voting procedures appeal those who are already politically mobilized but less attached to traditions.

## 1 Introduction and research hypotheses

To the eyes of an external observer, the European electoral legislation landscape appears as a colourful and assorted patchwork of requirements, procedures, and technical tools. Some countries revoked e-voting as soon as they loss support from the electoral basis, no matter whether it was a novelty, as in Ireland [Co04a; Co04b; Co06; Lu07] or a long established habit, as in the Netherlands [Go06; Oo07]. Others are more cautious and promote trials and experimentations with or without legal value, but always on a limited scale: this is the case in Switzerland [Br04; BB06], Great Britain [FR03], Spain [Fe07], Portugal [Fa08], and Italy [Ca08]. Some countries, such as Belgium and France, currently deploy electronic machines, while a few Baltic explorers are adopting more and more innovative channels: i-voting, successfully deployed in Estonia [MM06] and debated in Lithuania [Ud06], and even m-voting, i.e., voting from a mobile phone, as recently approved in Estonia [Wo08].

For the purposes of this paper, it is necessary to distinguish between paper-and-pencil polling-place voting, which is the traditional solution adopted by the Italian legislation; electronic voting by means of a computer installed in voting booths that are not connected to any network, generally labelled as *e-voting*; and internet voting from unsupervised environments, known as RIV (Remote Internet Voting) or just *i-voting*.

E-voting generally reproduces the features of the paper ballot on a more advanced technological artefact, allowing for quicker tabulation of the results and preventing some kinds of clerical mistakes in filling in the different measures [Re04]. I-voting can be regarded as a form of absentee ballot involving a further evolutionary step of technological development and reproducing dynamics similar to those faced in mail-in balloting [PS08].

Though more and more salient in Europe and in the rest of the world, the sociological debate pro and versus automated voting rests primarily on theoretical basis. Some authors underline how electronic voting will revolutionize democracy for the better by reducing costs, by limiting errors made by voters and electoral administrators, but above all by allowing for uniform standards in the ballot format [SC05]. Besides, thanks to an immediate access to online sources of information, i-voters could express a more documented and informed choice [AH04]. Conversely, other commentators believe that by making voting too easy and convenient, one would actually diminish the percentage of voters who really care about a certain policy; therefore e- and i-voting do not substantially revolutionize democracy [Bu01]. What is more, casting a ballot online is an individual business, which might deprive balloting of its symbolic value, which is intrinsically communitarian: all men and women—regardless of their age, status, education—walk as equals into anonymous polling booths and, as equals, decide to participate in the nation's destiny. Authors wonder whether democracy as we know it can be thus individualised and removed from its public expression. Opinions, again, are divided: some believe citizens are ready to give up the liminal phase of walking into the booth [Mo06], others see it as a betrayal of the democratic traditions and standpoints [MS04; Or01], the use of the internet apparently increasing social isolation [NE00]. In addition to this, as we already anticipated, the overall quality of democracy might be seriously affected by the divide in the access to automated voting facilities, which tend to be preferred by already mobilized social groups [Ke05], though this viewpoint is being fiercely debated [PS08]. Overall, electronic and internet voting appear as a promising challenge as much as a deceitful means supported by politicians to represent themselves as “modern” [FR03].

As a consequence, an oft debated topic is, at the time being, whether electronic and internet voting might change the socio-demographic and ideological profile of the electorate by facilitating some already advantaged social groups and discriminating the minorities. Some characteristics of the population have been proved to be associated with the ability of voting with different technologies: for instance, the amount of residual votes on ballot measures is linked to the voting technologies alongside the income and the percentage of black people living in a given county, whereas age and the percentage of Latinos appear to be not significantly associated to the chosen procedure [KK08]. Similar considerations might apply to the introduction of an electronic medium to replace a long-established habit of voting by paper and pencil.

Legally binding i-voting experiences show contradictory results: surveys conducted after the Arizona democratic primary in 2000 converge on finding a significant impact of age and level of education, whereas sex should not play a role in the choice to vote online [Ke05; So01]. On the other side, they substantially diverge in their interpretation of the effect of income, which is significant at the bivariate level [Ke05; So01] or when crossing ecological rather than individual data [Gi01], but loses its power when pooled in a multivariate model [So01]. Location (urban/rural) would not exert a statistically

significant effect [So01], as well as party identification [Ke05]. While some authors insisted on the existence of a digital divide between different social classes, sex and age groups [Gi05], individual level turnout data from the 2004 Michigan democratic primaries allowed researchers to signally address campaigners' concerns. Race and class were not found to be significant and a two-step decision model clarified that their impact is limited to the choice of voting absentee: once this decision has been taken, they play no role on the selection of the preferred method (by mail or by internet) to cast the ballot [PS08].

We can therefore expect sex, age, occupation, and education to be associated with the propensity to vote over the internet or on-site, by electronic means.

Furthermore, potential disparities might be observed not just in terms of the socio-demographic composition of the e-/i-electorate, but also in its quality: sociologists and political scientists are interested in observing how much an individual is linked to her socio-political community, and whether different modes of relation between a citizen and the society might affect her interest in e- and i-voting.

As pointed out by Guerra et al. [Gu03], trust in the other is crucial in establishing relations, and it has been argued that the trust flow starts with trust in the institutions delivering the elections [XM05]. It has also been underlined that i-voting will advantage citizens of areas where political participation is higher [Bi05], i.e., will appeal those who are already mobilized [KK08]. The bivariate association between political efficacy and willingness to vote over the internet has been established by Solop [So01], though he did not specify how the index is calculated, nor control for socio-demographic variables. A further condition supporting the deployment of automated means is the sense of belonging to the community, a concept which has been referred to as "social identity" [OV05], though not implying the identification of the individual by others, as intended by Guerra et al. [Gu03], but rather the feeling of describing oneself as part of a meaningful social group.

Given these premises, we might expect that trusting institutions and the generalised other, feeling as a member of one's community, and taking part in political activities beyond voting might increase the chances of being in favour of electronic and internet balloting.

The analysis that follows will then address the following question: what circumstances—socio-demographic characteristics and political attitudes—are associated with the (un)willingness to cast one's ballot from a terminal?

## 2 Data and methods

Since December 2004, the Autonomous Province of Trento has sponsored a research plan aimed at investigating and supporting the transition to automated means of casting and counting ballots in local elections. Pilots took place in 2005, 2006, and 2008 within the largest project of electronic voting carried out in Italy so far. The local government deployed a phased-in approach as suggested, among others, by the European Commission [Ve04], with the goal of gradually substituting paper and pencil with touchscreens. At the time this paper was being written, the multi-disciplinary *équipe* working on the ProVotE project provided local authorities with detailed evaluations of the field trials and recommendations on the conditions under which the switch-over

should take place, but no final decision has been taken yet. As none of the pilots could be legally binding, and individual-level data of voters and non-voters are not available, we relied on surveys to monitor the propensity to vote electronically in a supervised environment and over the internet (as done previously, amongst others, by Gibson [Gi01] and Kenski [Ke05]). Although i-voting is not on the agenda of either the Italian government or of the local one, the growing salience of this topic in the international arena suggested that we should start a preliminary investigation in order to highlight the conditions underlying the support for and the opposition against it.

Data that will be presented in this contribution are drawn from computer assisted telephone interviews carried out at the beginning of December 2007 on a sample of 1603 adult citizens. The sample was stratified in order to be representative of sex, age, and town of residence.

The three dependent variables reflect:

- the interviewee's propensity to deploy ProVotE e-voting machine (model a),
- the general stereotype towards automated voting, i.e., whether it has more advantages or more risks (model b), and
- the propensity to vote over the internet (model c).

These three variables were dichotomized by collapsing answers that expressed favor in the new technology and those that did not, as shown in Table 1.

As independent variables, we considered a set of socio-demographic characteristics (sex, age, level of education, and type of occupation) but also some indexes<sup>1</sup> of social and the political attitudes that the above summarized literature review held as theoretically or empirically crucial.

Specifically, an index of *trust in the generalised other* was computed from three dichotomous items following the Survey Research Center's rephrasing of Rosenberg's Faith in People scale [RS85], which is still being deployed in its ten point version in the European Social Survey. Given the limited number of items available, we did not compute a quasi-cardinal measure but rather aggregated the answers in order to separate those who tend to trust others (60.5% of valid cases) from those who offer no positive answer (39.5%). Bivariate analysis showed that education is the most significant factor related to this attitude: people in their adult age tend to trust others more than youth and the elderly. Bourgeois are more confident than interviewees of the working class, whereas sex has no significant impact.

In order to tap beliefs about politicians and the political process, we computed an index of *political cynicism*<sup>2</sup> by adapting Agger, Goldstein, and Pearl's scale [AGP61]. This quasi-cardinal measure is positively correlated to age and negatively correlated to the level of education, whereas there is no significant difference between sexes and occupations.

---

<sup>1</sup> A full list of the items enclosed in the survey is available upon request.

<sup>2</sup> Given the nature of the data gathering method (CATI), we offered just five modes of response instead of the original six. The standardised index has been computed using five of the six items, thus obtaining good internal consistency (Cronbach's  $\alpha = 0.63$ ). The median is 0.24, skewness is -0.566, kurtosis is 0.720 and range is 6.266.

A further index of *trust in the local institutions*<sup>3</sup> was computed by translating Craig, Niemi, and Silver's incumbent-based trust scale [CNS90], supplementing it with two items from Bennett's governmental attentiveness scale and ANES studies [RSW91], and adapting their wording for the local dimension. This attitude is actually cross-sectional and unrelated to sex, age, education, and occupation.

A second crucial dimension, *political participation*<sup>4</sup>, is represented by political activities: an index was computed from nine dichotomous items deployed within the Italian National Election Study [It06] and Verba and Nie's Participation in America Survey [Br99].

*Voting in the last general election* was retained as a separate control variable: 86.7% of the respondents declared they voted, an estimate which is consistent with the turnout of 2006 political elections in the region Trentino-Alto Adige, where the recorded participation rate was 87% [Mi09].

The third social dimension taken into consideration is the feeling of *territorial identity*, the sense of belonging to a local community that shares the same heritage and identifies itself in both symbols and actions. The indicators chosen to elicit this concept were only in part inspired by ANES studies and adapted to the local reality, so the resulting typology is original and not yet tested for external validity. We distinguished five types of interviewees:

- enthusiastic (26.4%) are proud of whatever concerns their land, possibly even edging toward chauvinism. Within this group women are more represented than men, as well as lower grades of education and people over their fifties;
- un-socialised (17.0%), though they define themselves as "trentini", they do not know the anthem, which is usually taught at school and sung at local festivities. As just one out of four was born outside the province, it is likely that people within this group are less integrated than those providing on-average or even enthusiastic answers. More women than men belong to this type, and seven out of ten are below fifty years of age;
- disillusioned (10.2%) said they feel little attached to at least one of the symbols taken into consideration. Disillusion is more common amongst young men and higher-grade white collars;
- strangers (11.0%) declared they do not feel themselves to be citizens of the Autonomous Province of Trento, or didn't answer to the identity-related questions. Interestingly, this attitude is more common amongst middle-aged professionals and those with higher education level: no surprise that just one out of four was born in the province;
- the remaining 35.4% gave intermediate answers and were labelled as "middlemen".

Given the nature of the dependent variables, we deployed multinomial and binary logistic regression and report the regression parameters (B), their Wald test significance

---

<sup>3</sup> In its original version this scale was deployed with dichotomous items, while our version has five possible answers. The index is standardised, with median of 0.08, skewness -0.007, kurtosis -0.302, and range 6.002.

<sup>4</sup> The summation index has been standardised and has a median of 0.13, skewness 0.683, kurtosis 0.052, range 4.654. The resulting Cronbach's alpha is 0.64.

and their standard errors. Odds ratios can be easily computed by raising the base of the natural log to the  $B^{\text{th}}$  power.

**Table 1 – Propensity towards the automation of voting procedures**

<b>a. Propensity to e-vote</b>		<b>b. Electronic voting has...</b>		<b>c. Propensity to i-vote</b>	
	%		%		%
very much in favour	25.8	more advantages than risks	36.3	very much in favour	16.0
quite in favour	30.0	more risks than advantages	35.7	quite in favour	23.9
neither in favour nor against	11.6			a little/not much in favour	17.5
quite against	14.7			not at all in favour	36.6
very much against	11.8				
<i>Total valid cases</i>	93.9	<i>Total valid cases</i>	72.0	<i>Total valid cases</i>	93.9
did not answer	0.4	did not answer	0.3	did not answer	0.2
did not know	5.7	did not know	27.7	did not know	5.9
<i>Total</i>	100.0	<i>Total</i>	100.0	<i>Total</i>	100.0
<i>N</i>	1603	<i>N</i>	1603	<i>N</i>	1603

### 3 Discussion of the results

Consistently with the reviewed literature on cyber-trust, remote i-voting elicits less support than polling-place e-voting: the latter is approved by 55.8% of the interviewees, whereas the former by 39.9% [Table 1]. The data support the hypothesis of an incremental deployment of technology, which sees e-voting as a step in an evolutionary process in which paper and pencils yield to remote internet voting: there is just a limited amount of respondents who would accept i-voting but not e-voting (3.7%), likely because of the added value of voting remotely rather than by the deployment of technology [Table 2].

But what is the profile of voters who would support automated elections? How much do socio-demographic characteristics affect the propensity to vote on a touchscreen or over the internet? Is there an impact of socio-political attitudes on this choice?

**Table 2 – Attitudes towards different solutions for voting automation**

% <b>Electronic voting has...</b>	<b>a. Propensity to e-vote</b>			<b>b. Propensity to i-vote</b>		
	no	yes	Total	no	yes	Total
more advantages than risks	29.7	17.0	46.7	38.1	12.1	50.1
more risks than advantages	3.5	49.8	53.3	16.9	32.9	49.9
Total	33.2	66.8	100.0	55.0	45.0	100.0
	<i>r = .603 (sig=.000) N=1021</i>			<i>r = .422 (sig=.000) N=1111</i>		

% <b>Propensity to i-vote</b>	<b>c. Propensity to e-vote</b>		
	no	yes	Total
no	29.0	25.3	56.4
yes	3.7	42.0	43.6
Total	32.7	67.3	100.0
	<i>r = .482 (sig=.000) N=1260</i>		

### 3.1 Socio-demographic characteristics

The analysis carried out by means of a multivariate logistic regression model allows us to compare the characteristics of those who answered favourably, those who are against, and those who provided no opinion on the subject matter, which gives us some insight into the potential non-response bias affecting surveys on e- and i-voting [Table 3]. We thus observe that interviewees who do not take a stand on the issues are also less likely to provide personal details, especially with regard to their occupation, while missing information on age is related to missing information on i-voting.

The model also shows that sex impacts significantly on the chances to see more risks than advantages in automated voting, but women are more sceptical than men also with reference to the ProVotE stand-alone machine and to i-voting. Age has a non-linear effect: consistently with previous research (e.g., Gibson [Gi05]) we find that automated elections are more supported by people in their middle age than by the youngsters and the elderly. The level of education contributes to the interest for these innovations in the electoral procedures: all factors being equal, the chances that a graduate supports i-voting are nearly twice as much as those of a person with a lower degree. Finally, there is no direct effect from occupation, which nonetheless is retained in the following analysis as a control variable.

**Table 3: Effects of socio-demographic characteristics on the propensity to automation in electoral procedures**

	a. Propensity to e-vote				b. Electronic voting has more advantages				c. Propensity to i-vote			
	yes		indifferent / DA / DK		yes		DA / DK		yes		DA / DK	
	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE
<b>Sex</b>												
male	0.15	0.123	-1.08	0.788	0.46***	0.122	0.13	0.132	0.20	0.112	0.13	0.224
female <sup>a</sup>												
<b>Age</b>												
missing	1.06	0.671	1.08	0.788	1.02	0.770	1.31	0.697	1.63*	0.641	2.17*	1.063
age	0.07***	0.020	0.02	0.025	0.05**	0.021	-0.01	0.021	0.08***	0.020	0.05	0.036
age <sup>2</sup> /age	-0.01***	0.001	-0.01	0.001	-0.00**	0.000	0.01	0.001	-0.01***	0.000	-0.01	0.000
<b>Education</b>												
missing	0.02	0.864	0.20	0.978	0.40	1.049	0.45	0.934	0.07	0.902	-0.30	1.197
min. 4 yrs univ. degree	0.64*	0.301	0.36	0.402	0.82**	0.310	-0.61	0.342	1.26***	0.303	-1.48	0.812
high school / BA	0.75**	0.234	0.76**	0.288	0.57*	0.256	-0.09	0.242	0.90***	0.255	-0.40	0.386
mid. school / prof. educ	0.39	0.214	0.65*	0.257	0.22	0.243	0.11	0.217	0.37	0.247	0.01	0.330
no title / elem. school <sup>a</sup>												
<b>Occupation</b>												
missing	-0.01	0.212	0.50*	0.251	0.26	0.225	0.48*	0.218	-0.13	0.214	0.67*	0.326
bourgeoisie	0.27	0.277	-0.56	0.448	-0.22	0.264	-0.41	0.325	0.53*	0.252	0.01	0.645
petite bourgeoisie	0.37	0.221	0.41	0.278	0.22	0.214	0.26	0.227	0.30	0.195	-0.09	0.423
white collars. high skilled	0.16	0.193	0.32	0.250	-0.14	0.190	0.32	0.201	0.08	0.172	0.36	0.353
white collars. low skilled	-0.07	0.184	0.16	0.238	0.28	0.184	0.22	0.202	0.26	0.170	0.53	0.320
working class <sup>a</sup>												
<b>Constant</b>	-1.27*	0.492	-1.87**	0.632	-1.81	0.508	-0.90	0.524	-2.25***	0.490	-3.52***	0.944

<sup>a</sup> reference category. Multinomial logistic regression models. DA = does not answer; DK = does not know. \* $p < .05$  \*\* $p < .01$  \*\*\* $p < .001$   
 model a.: N=1603. Model  $\chi^2(df)^{sig} = 122.192(26)^{***}$ . -2LL = 2530.168; Pseudo R<sup>2</sup> Cox&Snell = 0.073, Nagelkerke = 0.085, McFadden 0.039.  
 model b.: N=1603. Model  $\chi^2(df)^{sig} = 140.702(26)^{***}$ . -2LL = 2628.343; Pseudo R<sup>2</sup> Cox&Snell = 0.084, Nagelkerke = 0.095, McFadden 0.040.  
 model c.: N=1603. Model  $\chi^2(df)^{sig} = 224.639(26)^{***}$ . -2LL = 1976.318; Pseudo R<sup>2</sup> Cox&Snell = 0.131, Nagelkerke = 0.159, McFadden 0.081.

### 3.2 Social and political attitudes

To ascertain the role of the three socio-political dimensions described in section 2 (trust, participation, identity), we ran different binomial logistic models and found that the sign, the magnitude, and the significance of the coefficients did not substantially differ from what we observed in a single all-encompassing model, which is presented in Table 4.

Within the first dimension, we expected that *trust in the generalised other*—as a feeling that contrasts with, for instance, complot theories—would enhance the chances to accept automated elections. All other factors being held constant, this index was found to be relevant as long as voting in a supervised environment is concerned (model a and b) but negligible in the i-voting model. A possible interpretation of this result might take into account the relative safety of the voting environment as perceived by the elector: whereas automated voting as presented in the first two questions can be easily prefigured as quite similar to the present way of casting a ballot—where the computer takes over the paper and pencils—the third question suggests a totally different and much individualised location. The generalised other then is not the technician, the programmer, distant, invisible and perhaps even transparent to the eyes of the voter, but she is rather the returning officer, the member of the board of the scrutinizers, who support the elector in exerting her right to vote.

*Political cynicism* does not have much impact on the prejudice against automated voting (does it have more risks or more advantages) nor on the imaginary of remote voting, but rather it does on its practical application: interestingly enough, the cynical elector welcomes ProVotE, likely as a possible solution to potential frauds at the very local level. A large scale complot, as envisioned by activists in other countries with regard to i-voting, seems not to be foreseen by our interviewees.

Finally, we found no support for the common rhetoric that holds automated voting as better accepted by citizens who trust the local government. Controlling for all other socio-demographic and socio-political factors, *trust in the local administration* appears to be cross sectional: the coefficients are weak and non significant, though the sign of the relationship is consistent with our research hypothesis.

The second dimension we considered is *political participation*, which encompasses a set of political actions, such as signing up for a petition or a referendum, writing to candidates, trying to convince someone to vote for a party and so on. Our data bring further evidence to an already consolidated literature stressing how e- and i-voting appeal to citizens who are already politically mobilized. But we also found a small effect related to voting in past elections: those who did not cast a ballot have more chances to be in favour of automated means and especially remote voting appears significantly attractive. These results support what we already anticipated: the attraction of this innovation is given by the possibility to vote comfortably from an individually chosen location rather than by the deployment of technology *tout court*.



**Table 4:** Effects of socio-political attitudes on the propensity towards voting automation

	a. Propensity to e-vote		b. Electronic voting has more advantages		c. Propensity to i-vote	
	B	SE	B	SE	B	SE
<b>Sex</b>						
male	0.17	0.127	0.47***	0.125	0.20	0.114
female <sup>a</sup>						
<b>Age</b>						
missing	1.03	0.706	1.12	0.845	1.64*	0.664
age	0.07**	0.021	0.05*	0.022	0.07***	0.021
age*age	-0.01***	0.001	-0.01*	0.001	-0.01***	0.000
<b>Education</b>						
missing	-0.31	0.895	0.22	1.178	-0.11	0.913
min. 4 yrs university degree	0.56	0.317	0.76*	0.321	1.02**	0.311
high school / BA	0.69**	0.243	0.53*	0.263	0.75**	0.260
middle school / professional edu no title / elementary school <sup>a</sup>	0.35	0.221	0.20	0.248	0.30	0.250
<b>Occupation</b>						
missing	-0.01	0.220	0.29	0.234	-0.19	0.220
bourgeoisie	0.14	0.283	-0.30	0.273	0.49	0.258
petite bourgeoisie	0.29	0.228	0.14	0.221	0.24	0.199
white collars. high skilled	0.11	0.200	-0.22	0.196	0.05	0.177
white collars. low skilled	-0.13	0.189	0.27	0.189	0.26	0.173
working class <sup>a</sup>						
<b>Trust</b>						
missing trust in the other	0.34	0.180	0.42*	0.183	0.01	0.165
trust in the other	0.53***	0.141	0.65***	0.141	0.248	0.132
missing political cynicism	-0.11	0.160	-0.03	0.166	0.15	0.149
political cynicism	0.15*	0.073	0.05	0.071	0.06	0.066
missing trust in local gov.	-0.08	0.142	-0.02	0.144	-0.21	0.133
trust in local government	0.08	0.078	0.05	0.074	0.06	0.069
<b>Political participation</b>						
missing political activities	0.81**	0.276	0.45	0.253	0.28	0.215
political activities	0.18*	0.070	0.06	0.069	0.27***	0.063
missing voting	-0.33	0.480	-1.15	0.638	0.12	0.441
voting in last elections	-0.14	0.209	-0.20	0.203	-0.35	0.189
<b>Territorial identity</b>						
enthusiastic	-0.11	0.233	-0.15	0.227	-0.35	0.208
middlemen	-0.20	0.224	-0.14	0.217	-0.30	0.197
disillusioned	-0.50	0.272	0.27	0.268	-0.25	0.241
un-socialised	0.12	0.248	0.16	0.237	-0.06	0.217
strangers <sup>a</sup>						
<b>Constant</b>	-1.28*	0.563	-1.94**	0.578	-1.71**	0.543

<sup>a</sup> reference category. Binomial logistic regression models.

\* $p < .05$  \*\* $p < .01$  \*\*\* $p < .001$

- model a.: N=1319. Model  $\chi^2(df)_{90} = 119.025(27)***$ . -2LL = 1537.538;  
Cox&Snell  $R^2 = 0.086$ , Nagelkerke  $R^2 = 0.121$ . Overall % of predictability = 70.7%
- model b.: N=1154. Model  $\chi^2(df)_{90} = 84.499(27)***$ . -2LL = 1515.616;  
Cox&Snell  $R^2 = 0.071$ , Nagelkerke  $R^2 = 0.094$ . Overall % of predictability = 59.1%
- model c.: N=1505. Model  $\chi^2(df)_{90} = 228.520(27)***$ . -2LL = 1822.873;  
Cox&Snell  $R^2 = 0.141$ , Nagelkerke  $R^2 = 0.199$ . Overall % of predictability = 65.7%

The last dimension under analysis concerns the operationalization of identity according to the typology described in section 2. Though not statistically significant (which might be due, amongst other reasons, to the sample size), the sign and the magnitude of the coefficients suggest us some ideas about the effect of identity on the propensity to deploy automated means for voting. Quite interestingly, people who are more integrated in their community are less inclined to e- and i-voting: a conservative or traditionalist attitude, the pride of belonging to the community (though the same one which crafted the voting device) do not reinforce the willingness to vote automatically, but rather inhibit it. This finding goes in the opposite direction of our initial research hypothesis, according to which we expected that being a protagonist of such an innovation would be associated with a higher propensity to deploy the ProVotE machinery, in a sort of Hawthorne

factory effect [Ma33]. We can try to interpret this tendency in the light of the Durkheimian notion of community, which requires the members' co-presence in order to elicit, through rituals, that feeling of effervescence that recalls and forwards the shared values and norms.

## 4 Conclusions

The governments' preoccupation with the increasing disenfranchisement of the electorate brought about numerous attempts to restore citizens' participation in elections. Alongside reforms in the traditional paper-based electoral systems, many countries show a growing interest in automated means for casting ballots and tabulating the results. Automated elections promise a simplification of procedures, thus eliminating voters' fatigue (which is one of the causes of undervoting), clerical mistakes, and, possibly, low turn-out [KK08]. Nonetheless at the time being, empirical evidence is scarce if not anecdotal: literature draws on different sources of data and contexts that do not allow generalization.

Rather than on certainties on the feasibility and the advantages of e- and i-voting, most national experiences converge on the preoccupations advanced by pressure-groups and by some researchers: do automated elections change the composition of the electorate and thus the quality of democracy?

Our data showed that age and education level are significant predictors of the propensity to vote remotely or in electronic booths, the effect of age being actually non-linear, thus suggesting that youth, as well as the elderly, will not be attracted to polls, should e-voting be introduced, neither will people with low levels of education.

But we also considered how the voters' profile will change according to their socio-political attitudes, signally with reference to trust, political participation, and identity.

We found further evidence to Xenakis' and Macintosh's [XM05] suggestion that in the chain of inherited trust, citizens do not realize they implicitly give credit to someone who is unknown, not just to them, but even to the same authorities delivering the elections. I-voting propensity is actually unrelated to both trust in the local government and trust in the generalised other; in other words prospect i-voters experience different kinds of concerns than those sensed in other e-transactions, while trust in the other is significant when voting in a supervised environment. Our data therefore support Oostveen's and Van den Besselaar's statement, according to which "people should not just have to trust in the integrity of a voting system or the people who designed, developed and implemented it" [OV04], thus implying that more observation opportunities might be introduced to enhance the feeling of security. It is then advisable that on one side citizens should be enabled and encouraged to observe procedures at the polling booths, but on the other side they should also be made aware of the role of technology (and of the people in charge of designing and managing it) should i-voting be introduced.

Furthermore, as participation in political activities proved significant for both e- and i-voting, our data suggest that in the Italian context, and signally in Trentino, the conclusions drawn by Prevost and Schaffner [PS08] cannot be totally corroborated: if mobilization only influences the choice to vote remotely, but not the medium through which the ballot is cast, we should not have found political participation to be a

significant predictor in the e-voting model as well. We can therefore conclude that there is a substantial divide in the propensity to deploy automated means of elections: people who are already politically mobilized are more in favour of automated elections—as suggested, amongst others, by Kimball and Kropf [KK08], Kenski [Ke05], Birdsall [Bi05]—no matter whether voting takes place from a remote location or in a supervised environment. Nonetheless, we also found evidence that automated voting, especially in its i-form, might appeal those who did not participate in the last political elections. Finally, we learnt that even though most i-voting initiatives have been developed at the local level by local contractors [Kr08], pride for belonging to the same community that crafted this innovation does not enhance the chances of being in favour of deploying the i-voting mechanisms, but on the contrary, a higher degree of integration inhibits the propensity to i-vote. We tried to interpret this attitude with reference to the Durkheimian theory of collective effervescence, which is elicited by ritual events such as elections. The seeming contradiction between the positive impact of political participation and the negative, though not significant, impact of integration is a paradoxical finding that calls for further research. It is likely that mobilization is not disjoined from progressive individualization of conventional political behaviours, which would account for both the positive effect of participation and the irrelevant effect of integration, but a more complex model is needed to account for these relations, which goes far beyond the scope of this paper. Further investigations are also needed in the direction of the feeling of security and privacy that different media convey: for instance, how i-voting will eventually overcome the tension between the need for privacy and the requisite of identity recognition is still to be ascertained. We also acknowledge the limitations related to the method of data gathering we deployed: should similar data be available in real experimental settings, we will be able to confirm whether attitudes towards e- and i-voting match with actual behaviours or not. The next steps of our analysis will signally address the effect of the technological artefact and take into consideration the voters experience with current voting procedures and with technology in general, through scales that can be computed within the same dataset presented here. At the time being, our research suggests that greater attention should be paid to the quality of the electorate that e- and i-vote engage: based on the binomial and multinomial logistic models we implemented, our data support the hypothesis of existing divides between those who are favourable to automation in elections and those who are not, the main cleavages being represented by age and education, but also by socio-political attitudes.

## 5 Acknowledgements

The author acknowledges that the research presented in this contribution was carried out within the project ProVotE, financed by the Autonomous Province of Trento, and wishes to thank the director of the Electoral Bureau, Patrizia Gentile, and the members of the sociological *équipe*—Carlo Buzzi, Francesca Sartori, Pierangelo Peri, and Giolo Fele—for their constant support and encouragement.

## Bibliography

- [AGP61] Agger, R. E., M. N. Goldstein, and S. A. Pearl. 1961. Political cynicism: Measurement and meaning. *Journal of Politics* 23: 477–507.
- [AI06] Allen, P. L. 1906. Ballot laws and their workings. *Political Science Quarterly* 21: 38–58.
- [AH04] Alvarez, R. M., and T. E. Hall. 2004. *Point, click, and vote. The future of Internet voting*. Washington, DC: Brookings Institution.
- [Bi05] Birdsall, S. 2005. The democratic divide. *First Monday* 10. [http://131.193.153.231/www/issues/issue10\\_4/birdsall/index.html](http://131.193.153.231/www/issues/issue10_4/birdsall/index.html)
- [Br99] Brady, H. E. 1999. Political participation. In *Measures of political attitudes*, ed. J. P. Robinson, P. R. Shaver, and L. S. Wrightsman, 737–801. San Diego, California: Academic Press.
- [Br04] Braun, N. 2004. E-voting: Switzerland's projects and their legal framework. In *Electronic voting in Europe: Technology, law, politics and society*, ed. A. Prosser and R. Krimmer. 43-52. Bonn: GI.
- [BB06] Braun, N. and D. Brändli 2006. Swiss e-voting pilot projects: Evaluation, situation analysis and how to proceed. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer. 27-36. Bonn: GI.
- [Bu01] Buchstein, H. 2001. Modernisierung der Demokratie durch e-Voting? *Leviathan: Zeitschrift für Sozialwissenschaft* 29: 147–155.
- [Ca08] Caporusso, L. 2008. There is more to e- than meets the eye: Towards automated voting in Italy. In *E-voting: The last electoral revolution*, ed. J. M. Reniu. 27-44. Barcelona: ICPS.
- [Co04a] Commission on Electronic Voting. 2004. *First report of the Commission on Electronic Voting on secrecy, accuracy and testing of the chosen electronic voting system*. [http://www.cev.ie/htm/report/download\\_first.htm](http://www.cev.ie/htm/report/download_first.htm)
- [Co04b] Commission on Electronic Voting. 2004. *Interim report of the Commission on electronic voting on secrecy, accuracy and testing of the chosen electronic voting System*. <http://www.cev.ie/htm/report/V02.pdf>
- [Co06] Commission on Electronic Voting. 2006. *Second report of the Commission on electronic voting on secrecy, accuracy and testing of the chosen electronic voting system*.
- [CNS90] Craig, S. C., R. G. Niemi, and G. E. Silver. 1990. Political efficacy and trust: A report on the NES pilot study items. *Political Behavior* 12: 289–314.
- [FR03] Fairweather, B., and S. Rogerson. 2003. Internet voting—Well at least it's modern. *Representation* 39: 182–195.
- [Fa08] Falcão, J. et al. 2008. Auditing e-voting pilot processes and systems at the elections for the European Parliament and for the Portuguese Parliament. In *E-voting: The last electoral revolution*, ed. J. M. Reniu. 93-114. Barcelona: ICPS.
- [Fe07] Fernández Rodríguez, J. J. et al. 2007. *Voto electrónico. Estudio comparado en una aproximación jurídico-política (desafíos y posibilidades)*. Santiago de Querétaro, Mexico: Fundación Universitaria de Derecho, Administración y Política.
- [Gi01] Gibson, R. 2001-2. Elections online: Assessing internet voting in light of the Arizona democratic primary. *Political Science Quarterly* 16: 561–583.
- [Gi05] Gibson, R. 2005. Internet voting and the European Parliament elections: Problems and prospects. In *The European Union and e-voting: Addressing the European Parliament's internet voting challenge*, ed. A. Trechsel and F. Mendez. London: Routledge.
- [Go06] Gongrijp, R. et al. 2006. Nedap/Groenendaal ES3B voting computer. A security analysis, Stichting "Wij vertrouwen stemcomputers niet", Amsterdam. <http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf>

- [Gu03] Guerra, G. A. et al. 2003. *Economics of trust in the information economy: Issues of identity, privacy and security*. Oxford: Oxford Internet Institute.
- [It06] Itanes. 2006. <http://www.itanes.org/>.
- [Ke05] Kenski, K. 2005. To i-vote or not to i-vote? Opinions about internet voting from Arizona voters. *Social Science Computer Review*.23:293-303
- [KK08] Kimball, D. C., and M. Kropf. 2008. Voting technology, ballot measures, and residual votes. *American Politics Research* 36: 479–509.
- [Kr08] Krimmer, R. 2008. The development of remote electronic voting in Europe. In *E-voting: The last electoral revolution*, ed. J. M. Reniu, 13–26. Barcelona: ICPS.
- [Lu07] Lundell, J. 2007. Second report of the Irish Commission on electronic voting. *Voting Matters* 23: 13–17.
- [MM06] Madise, Ü., and T. Martens. 2006. E-voting in Estonia 2005. The first practice of country-wide binding internet voting in the world. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer. 15-26. Bonn: GI.
- [MS04] Marvin, C., and P. Simonson. 2004. Voting alone: The decline of bodily mass communication and public sensationalism in presidential elections. *Communication and Critical/Cultural Studies* 1: 127–150.
- [Ma33] Mayo, E. 1933. *The human problems of an industrial civilization*. New York: MacMillan.
- [Mi09] Ministero dell'Interno, Archivio Storico delle Elezioni, 2009. <http://elezionistorico.interno.it/>
- [Mo06] Monnoyer-Smith, L. 2006. How e-voting technology challenges traditional concepts of citizenship: An analysis of French voting rituals. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer, 61–68. Bonn: GI.
- [NE00] Nie, N. H., and L. Erbring. 2000. *Internet and society. A preliminary report*. Standford: Stanford Institute For The Quantitative Study Of Society. [http://www.stanford.edu/group/siqss/Press\\_Release/Preliminary\\_Report.pdf/](http://www.stanford.edu/group/siqss/Press_Release/Preliminary_Report.pdf/).
- [Oo07] Oostveen, A.-M. 2007. Context matters. A social informatics perspective on the design and implications of large-scale e-government systems. Amsterdam: Universiteit van Amsterdam.
- [OV04] Oostveen, A.-M., and P. Van den Besselaar. 2004. Security as belief. User's perceptions on the security of electronic voting systems. In *Electronic voting in Europe: Technology, law, politics and society*, ed. A. Prosser and R. Krimmer, 73–82. Bonn: GI.
- [OV05] Oostveen, A.-M., and P. Van den Besselaar. 2005. Trust, identity and the effects of voting technologies on voting behavior. *Social Science Computer Review*.23: 304-311.
- [Or01] Ornstein, N. 2001. What does the law require? Panel 4: Perspectives of political parties, 3rd public hearing of the national commission on election reform, held on May 24, 2001, in Austin, Texas.
- [PS08] Prevost, A. K., B. F. Schaffner. 2008. Digital divide or just another absentee ballot?: Evaluating internet voting in the 2004 Michigan democratic primary. *American Politics Research* 36: 510–529.
- [Re04] Remmert, M. 2004. Toward European standards in electronic voting. In *Electronic voting in Europe: Technology, law, politics and society*, ed. A. Prosser and R. Krimmer. 13-16. Bonn: GI.
- [RS85] Robinson, J. P. and P. R. Shaver, eds. 1985. *Measures of social psychological attitudes*. Ann Arbor, Michigan: University of Michigan, Institute for Social Research.
- [RS91] Robinson, J. P., P. R. Shaver, and L. S. Wrightsman, eds. 1991. *Measures of personality and social psychological attitudes*. San Diego, California: Academic press.

- [SC05] Smith, A. D., and J. S. Clark. 2005. Revolutionising the voting process through online strategies. *Online Information Review* 29: 513–530.
- [So01] Solop, F. I. 2001. Digital democracy comes of age: Internet voting and the 2000 Arizona democratic primary election. *PS: Political Science & Politics* 34: 289–293.
- [Ud06] Udris, J. 2006. The Lithuanian concept of voting via internet for elections and referenda. Presentation held at the Council of Europe on account of the Central Electoral Commission of the Republic of Lithuania, November 16, in Strasbourg, France.
- [Ve04] Venice Commission. 2004. Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe. In *European Commission for democracy through law*. <http://venice.coe.int/>
- [Wo08] World E-Democracy Forum. 2008. Estonia to vote by mobile phone in 2011. <http://www.edemocracy-forum.com/2008/12/estonia-to-vote-by-mobile-phone-in-2011.html>
- [XM05] Xenakis, A., and A. Macintosh. 2005. Trust analysis of the UK e-voting pilots. *Social Science Computer Review* 23: 312-325..

# **The Virtual Polling Station**

## **Transferring the Sociocultural Effect of Poll Site Elections to Remote Internet Voting**

Philipp Richter

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)  
Universität Kassel  
Wilhelmshöher Allee 64-66  
34109 Kassel  
Germany  
[prichter@uni-kassel.de](mailto:prichter@uni-kassel.de)

**Abstract:** Public voting in polling stations is believed to have a socioculturally-integrative effect, conveyed through the symbolic and ritualistic character of the election process. Remote internet voting is believed to not be able to provide this effect, because it omits the corporeal appearance at the polling station. The following contribution aims at indicating how such a sociocultural effect could be transferred from the real world polling station to remote internet elections.

### **1 The Public Nature of the Polling Station and Internet Elections**

All forms of electronic voting, including internet voting, have been criticized for not fulfilling the Principle of the Public Nature of the Election which was declared as a constitutional principle in the Voting-Machine-Judgment of the German Federal Constitutional Court [BVerfG09] and which requires verifiability of the election for every citizen without special technical knowledge. Remote internet voting has additionally been accused of another shortcoming which the German legal literature has also located in the sphere of the Principle of the Public Nature of the Election. It has been brought forth that remote internet voting is not able to substitute the sociocultural integrative effect of public elections in real world polling stations, conveyed through the symbolic and ritualistic form of the election process. The corporeal act of voting at the polling station is described as the conscious exercise of a civil liberty as well as the perceptible expression of affiliation with the community to which is attested an identity-causing and ritualistic impact which politically integrates the voter and conveys to him a sense of the significance of the election [Ha04]. The "...polling station with its naked walls and shabby ballot boxes..." is described in contrast to the surroundings of the internet as a dramatization-free zone of political rationality [Me04]. The citizen is believed to experience himself through the ritual of the public election as sovereign and to gain the chance to identify with the state. This "symbolic-ritualistic character," which is attested to create a constituting effect in democratic elections, is believed to be "trivialized" and to dwindle in remote internet voting [Ka05]. Votes cast via the internet

are described as an unreflected act which is inadequate to the significance of an election and are even called “junkvote” [Bu01].

This criticism would mainly also be applicable to postal voting in which the corporeal appearance at the polling station is also omitted. In the Voting-Machine-Judgment this aspect of the public nature of elections was not addressed. The democratic-integrative effect of the election was based on the possibility for every citizen to fully monitor compliance with the election principles laid down in Article 38 of the German Constitution (GG). On the other hand, the Court was not called upon to say anything on this aspect, since the ruling only examined the use of on-site voting machines. It therefore remains unsettled, if a sociocultural effect as described is constitutionally required as part of the Principle of the Public Nature of the Election or if it is merely an effect caused by the established voting technique.

It shall not however be disputed here that such a symbolic-ritualistic effect of elections, aside from its dogmatic justification, is able to accomplish considerable integrative processes in democratic states. The abstract construct of the state becomes perceptible in symbols and rituals. By ritualistic participation of the citizens in matters which unite them and by establishing symbols for the display of common meaning, the community gains form, security and constancy [He83, p. 97]. Such symbols and rituals are widely known. The state, as a union of meaning and a body capable of acting, is perceptible in flags and emblems, in anthems, in the public meetings of parliaments and among many others also in the act of voting in public, in which moreover every eligible voter is able to take part actively. An election in a parliamentary democracy is the fundamental tool by means of which the citizens unite into a public body which is able to act. By active participation the citizens gain the possibility to take part in the installation of the organization called state and thus to perceive it as something of their own making, not as something ordered from above. Unity in meaning and unity in action by forming a public body are the two factors which in combination give the societal alliance its constancy [He83, p. 106 ff.]. In an election, they are exercised side-by-side and become perceptible by the symbolism and the ritual of the public act of voting.

It is however a misconception to believe that the described effect could only be conveyed by the corporeal act of voting in the real world, a misconception which overlooks that the sociocultural effect of public voting could be conveyed in new ways by a medium like the internet [Ne02]. It has not been proved by which actions or symbols exactly the described effect is conveyed. Is it interaction and communication with other voters? Is it the reputable surrounding of the polling station? Is it the slowness of the process? Is it all of them together? Is it something else for each voter? The question would be very hard to answer.

However in the following, it shall be indicated how the central aspects of the act of voting in the real world polling station could be transferred to remote internet voting.



## 2 The Virtual Polling Station

Concepts for internet voting systems in respect to user interfaces up to now have usually aimed at offering a login and a digital ballot paper. Internet remote voting is therefore rightly sometimes called electronic postal voting [Ta99]. In this form, it uses only part of the potential of the IT-surroundings: the mobility of the voter in comparison with elections in polling stations, the speed of the transmission in comparison to postal voting, and the speed of the counting in comparison to both.

It does not, however, use the possibility to create virtual reality and thus to simulate the act of voting as a perceptible exercise. The polling station could be displayed graphically and entered by the voters via avatars.<sup>1</sup> Voters could enter the polling station simultaneously and thus interact as in the real world. This user interface could become the frame into which established internet voting concepts such as authentication, digital ballot paper, encryption, etc. could be embedded and which could extend them by the sociocultural effect of the public election.<sup>2</sup>

### 2.1 The Polling Station and the Voting Avatar

The polling station could be displayed as a three-dimensional graphical space. It could be designed following the model of a typical polling station in the real world, for example a school building. It could even imitate the real polling station for each electoral district. The virtual polling station thus could convey a reputable impression like real world polling stations are believed to do. Creating one virtual polling station for every polling station in the real world would mean higher expenses than creating only one virtual polling station for all absentee voters. It might however convey a high level of identification with the electoral district.

The voting avatar represents the voter graphically in the virtual world and allows him to move in the polling station and carry out the necessary steps of the election. It could look like the actual voter and thus make him visible to the other voters like in the real world polling station. If it would indeed be sensible to shape the avatar as the real voter, should be further discussed. At least the design of the avatar should stay within the scope of what is possible in the real world, so that it would be adequate to the significance of the election and not give the voting process the character of a game.

### 2.2 Chat

If one sees an important trigger for the sociocultural effect in interaction and communication with other voters, as possible in the real world polling station, this could be arranged in the virtual polling station by means of a general chat, a display by which text messages may be sent and read by all participants. Whoever would misemploy this application in order to disturb orderliness in the polling station, for example by polemic statements or molestation of other voters, could, exactly like in the real world, be expelled from the polling station, § 31 S. 2 *Bundeswahlgesetz* (BWG). The name of each voter or alias should be shown above the avatar so that chat messages can be linked to it.

---

<sup>1</sup> The use of 3D-surroundings and avatars in internet voting has also been proposed in order to attract younger people to internet voting in [MP04].

<sup>2</sup> Established concepts might also be extended at crucial points by the virtual polling station. Such aspects shall only be experimentally hinted at in this contribution, however.

### 2.3 Electoral Assistants

If one sees an important trigger for the sociocultural effect in communication with electoral assistants, who embody the state, even this could be arranged in the virtual polling station. Electoral assistants could also take part in the election process by means of avatars. By means of audio and video transmission as in VoIP-communication, they could even get in direct contact with voters and exercise classic duties of electoral assistants, for example identity controls and voting instructions. Maybe they might even monitor by video transmission that the secrecy of the vote is not broken by persons gazing at the voter's computer display.<sup>3</sup>

Internet voting is often seen as a way to make election assistants obsolete. This approach is however in conflict with the democratic ideal of a public citizen election, in which citizens take part on both sides of the ballot. It furthermore disregards the communicative potential of the internet. Also, a democratic monitoring of the election by citizens on both sides of the virtual ballot might be facilitated in this way.

### 2.4 Casting of Votes

The actual casting of the votes could be conducted classically by use of a digital ballot paper, which the voting avatar optically receives from the assistant avatar. The ballot paper could be filled out by the voter at a voting table and be dropped into the graphical ballot box. All IT-based concepts for the protection of the voting principles could and should be brought to bear in the vote casting. The virtual polling station cannot replace them. It would only convey the symbolic and ritualistic framework for the casting of votes.

### 2.5 Possible Election Procedure

The possible procedure of an election in the virtual polling station will now be outlined in order to make the specific chances and risks accessible to further analysis. Additionally the design of the virtual surroundings and their functional interaction can be described vividly in this way.

Every voter might be handed the necessary software and be assigned a temporary or permanent voting account, which would grant to him access to his avatar and to an instantiated<sup>4</sup> polling station. After logging in to his account, he might gain access to his avatar and might be given information on the voting procedure, the code of behavior in the polling station, and the possibilities for monitoring the election. He then might enter the virtual world with his avatar and appear, for example, on the street in front of the polling station.

---

<sup>3</sup> This idea would of course have to be designed as to be in compliance with the Privacy of the Home (Art. 13.1 GG) and the Informational Self-Determination (Art. 2. 1, Art 1. 1 GG).

<sup>4</sup> Instances in virtual worlds are closed areas, which may for example be entered only by certain users.

Here he might chat with other voters, exactly like in the real world. He might enter the polling station and, if one sees another trigger for the sociocultural effect of the election in the slowness of the procedure, get in line and wait for his turn. He might then approach an assistant avatar and interact with it. An audio-visual window might pop up by means of which voter and voting assistant might communicate directly. The voting assistant might brief the voter, check his identity, and eligibility. He might then hand over the digital ballot paper to the voter. This might be visualized by the assistant avatar handing a graphical ballot paper over to the voting avatar. The voter might walk his avatar over to a voting table and fill out the ballot paper.<sup>5</sup> During the act of casting the vote, nobody must be able to interfere with the voter or his avatar. The voter might then again interact with an assistant avatar or directly drop the graphical ballot paper into the ballot box. He then might leave the polling station and log out or, as in the real world, might chat with other voters on the street in front of the polling station.

## 2.6 Sociocultural Effect

The advocates of a symbolic-ritualistic effect, which can only be conveyed by the corporeal act of voting in the real world polling station, present triggers for this effect. These triggers are stimuli from the real world, like seeing other voters, the optical impression of the polling station, corporeal movement on the way to the polling station, etc. The described effect is a pattern-based reaction to these stimuli.

Stimuli from the real world may however be transferred into virtual worlds and the other way around [Fr05, para. 15 ff.]. By means of graphical simulation of procedures in real world polling stations, the stimuli of public voting may, to a large extent, be transferred into the process of remote internet voting and trigger correspondent pattern-based reactions in the voter.

During transfer, stimuli are subject to transformation processes. Transfers from one world to another, as would be the case here, are not complete [Fr05, para. 28 ff.]. Driving a car in the virtual world is only an abstraction of driving a car in the real world, different actions are necessary to succeed. This transformation is necessary to transfer a stimulus and the correspondent learned pattern from the real world into the natural laws of the virtual world [Fr05, para. 30 ff.]. In a successful transfer, the virtual world does not employ the same stimuli as in the real world, but an abstract version of the stimulus which is able to suggest a reaction pattern from the real world [Fr05, para. 32 ff.].

It is thus in principle possible to trigger the described sociocultural effect of public voting by a virtual version of the procedure in the real world polling station. How successful this transfer would be in respect to every single voter would depend on the quality of the stimuli which are used to simulate stimuli from the real world, which are believed to trigger the desired reaction pattern. These relations would have to be analyzed thoroughly.

---

<sup>5</sup> A graphical polling booth might also be installed. It would however fulfill no other function than the visual one and might lead the voter to the misconception that it would grant the secrecy of his digital vote.

Graphical depiction of the polling station, the voters, and of the vote casting however appear to be functional suggestions of the voting procedure in the real world with a relatively low effort of transfer. Direct audio-visual communication with election assistants would demand an especially low effort of transfer, namely that from an authentic live portrayal to a real person, a transfer exercised by humans for ages.

The virtual polling station might slow down the remote internet vote casting and remove from it the feeling of cursoriness. The voter would not switch back and forth between browser windows, between the election, commercials and videos, but his senses would be focused on the election process.

Experiences in virtual worlds, especially communication and interaction in three-dimensional graphical surroundings leave behind memories. Nobody who has ever exposed himself to this technology would dispute this. The possibility of stimulus transfers from real to virtual and the effectuality of virtual experiences for the real world has furthermore been widely proven and accepted in education and training. Pilots learn real aviation in simulators. Doctors exercise physiological training by means of computer simulations instead of test animals [Mü96] and train surgical operations on humans in virtual surroundings [MHB10].

## **2.7 Difficulties**

The process of stimulus transfer and transformation from the real world polling station will only work, if stimuli from the real world are known. The reaction pattern of the public election can only be suggested by virtual stimuli, if people still exercise and thus learn the pattern in the real world. For people who know only the virtual polling station, different reactions might be triggered. In order to convey the same reaction to these possible future citizens, the patterns would either have to be trained in the real world or virtual stimuli would have to be found, which trigger the same reaction originally.

By graphically depicting the public election of the real world, the aspect of monitoring the election and the sociocultural effect of the election would no longer be made possible by the same means. When an avatar casts a vote, this act visualizes the election. The visualization however does not grant certainty of the successful vote cast. For verification other mechanisms would have to be applied, which would allow monitoring for everybody without special technical knowledge. Voters would have to be advised not to rely on graphic visualizations, which are not designed to convey trust, but symbolic and ritualistic effects.

Remote internet voting and especially the virtual polling station would demand a certain amount of skill in respect to computers and the internet as well as access to hardware and software. Since these are not given for all citizens, the described technology may not fully replace established voting techniques, but rather be an additional voting channel.

Virtual realities have up to now become commonly known mainly through entertainment, especially gaming. The concept of the virtual polling station might thus be attacked on the ground that it would further trivialize the act of voting and change it into a game. Such criticism would however oversee that technology, especially information technology, triggers specific effects only by its specific application [Ro93]. The virtual polling station would have to be designed in a way that would be adequate to the fundamental significance of elections in parliamentary democracies and must not be designed following the aesthetics of entertainment.

### **3 Conclusion**

By means of a virtual polling station as described above, remote internet voting could trigger the sociocultural effect of corporeal voting in the real world. Remote internet voting would not remain in the stage of electronic postal voting, but develop into an absentee election with virtual attendance. In comparison to postal voting, remote internet voting including a virtual polling station could thus considerably facilitate the sociocultural effect of absentee voting.

## Bibliography

- [Bu01] Buchstein, H.: Modernisierung der Demokratie durch e-Voting?, *Leviathan* 2/2001, p.147 (155).
- [BverfG09] Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 123, p. 39.(68 ff.) [http://www.bverfg.de/entscheidungen/cs20090303\\_2bvc000307.html](http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html).
- [Fr05] Fritz, J: Wie virtuelle Welten wirken, Bundeszentrale für politische Bildung, 2005, [http://www1.bpb.de/themen/OI6VDV,2,0,Wie\\_virtuelle\\_Welten\\_wirken.html](http://www1.bpb.de/themen/OI6VDV,2,0,Wie_virtuelle_Welten_wirken.html)
- [Ha04] Hanßmann, A.: Möglichkeiten und Grenzen von Internetwahlen, 2004, p. 185.
- [He83] Heller, H.: Staatslehre, 6. Auflage, 1983.
- [Ka05] Karpen, U.: Elektronische Wahlen?, 2005, p. 31.
- [Me04] Meinel, F.: Öffentlichkeit als Verfassungsprinzip und die Möglichkeit von Onlinewahlen, *KJ* 2004, p. 414 (428).
- [MHB10] Maschuw, K.; Hassan, I.; Bartsch, D.K.: Chirurgisches Training am Simulator, *Der Chirurg* 1 2010, p. 19.
- [MP04] Maidou, A.; Polatoglou, H.M.: E-Voting and the architecture of virtual space, *Electronic Voting in Europe –Technology, Law, Politics and Society*, Workshop of the ESF TED Programme, 2004 in Bregenz, Lake of Constance, Austria, pp. 133. ff.
- [Mü96] Müllges, K: Vom Brüllfrosch zur Computermaus, *Deutsches Ärzteblatt* 93, Heft 42, 18. Oktober 1996, p.69.
- [Ne02] Neymanns, H.: Online-Wahlen, Buchstein/ Neymanns (Hrsg.), 2002, p. 36.
- [Ro93] Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung, 1993, pp. 72 f.
- [Ta99] Tauss, J.: Die elektronische Briefwahl als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten, *Jahrbuch Telekommunikation und Gesellschaft* 1999, pp. 285 – 292.

## **Session 3: Certification and Evaluation of E-Voting Systems**





# A Formal IT-Security Model for the Correction and Abort Requirement of Electronic Voting<sup>1</sup>

Rüdiger Grimm<sup>1</sup>, Katharina Hupf<sup>1</sup>, and Melanie Volkamer<sup>2</sup>

<sup>1</sup>Institute of Information Systems Research  
Universität Koblenz-Landau  
Universitätsstraße 1  
56070 Koblenz  
Germany  
[\\_{grimm,hupf}@uni-koblenz.de](mailto:{grimm,hupf}@uni-koblenz.de)

<sup>2</sup>Center for Advanced Security Research Darmstadt  
Technische Universität Darmstadt  
Mornewegstraße 32  
64293 Darmstadt  
Germany  
[volkamer@cased.de](mailto:volkamer@cased.de)

**Abstract:** This paper addresses a basic security requirement of electronic voting, namely that a voter can correct or abort his vote at any time prior to his final vote casting. This requirement serves as a protection against voter precipitance (haste). We specify rules for a reset and cancel function that implement the correction and abort requirement. These rules are integrated in an extended version of the formal IT security model provided in [VG08]. We show that these rules do respect the requirements covered in this model namely that each voter can cast a vote, that no voter loses his voting right without having cast a vote and that only eligible voters can cast a vote. This paper formally describes and mathematically proves the model and finally shows at which places of a voting process the formal rules apply.

---

<sup>1</sup> This paper is developed within the project “ModIWA – Modellierung von Internetwahlen” which is funded by DFG, and carried out at the Universities Kassel (Roßnagel, Richter) and Koblenz-Landau (Grimm, Hupf)

## 1 Introduction

Security is an elementary property of electronic voting systems and is thus fundamental for the trust of the voters in the system. Security objectives for electronic voting were first collected in an informal way, for example by a European-wide accepted recommendation adopted by the Council of Europe [CE04]. Later the semi-formal method of the Common Criteria [CC06] was used to specify a Protection Profile (PP) for a basic set of security requirements for online voting products [VV08]. There are good reasons to specify the security objectives of an IT system in a formal way, i.e., by mathematical calculus which states and proves properties clearly [Wa05]. The formalization of security objectives is a way to gain unambiguous and clearly understood

Requirements for electronic voting. Due to its formal base, it can be mathematically proven that a specification or implementation conforms to these formal security requirements. For example, the mandatory access model of Bell and LaPadula [BP73] strengthens the trust in a secure centrally controlled multi-user computer system, such that in the early days of computer system security evaluation it used to define the highest assurance level of the Orange Book Criteria [DD85]. Thus a formal IT security model on electronic voting defining security requirements from [CE04] and [VV08] in a formal language can create large amounts of trust in the effect of the security functions implemented in the electronic voting system.

However, the Common Criteria Protection Profile for online voting products [VV08] requires an evaluation according to evaluation assurance level EAL2+ on a scale from 1 to 7. This level does not require any formal proof. This evaluation level seems to be acceptable as this PP only claims to define basic requirements. Parliamentary elections, however, demand a higher evaluation level, probably EAL 6 or 7. At this level, the application of formal methods and the definition of a formal security model [CC06] are mandatory for the Common Criteria evaluation.

To enable a Common Criteria evaluation according to these levels, the authors of [VG08] provide an IT security sub-model for electronic voting. However, this model only covers a small subset of security objectives namely that each voter can cast a vote, that no voter loses his voting right without having cast a vote and that only eligible voters can cast a vote. This model needs to be extended to meet the remaining security objectives. The aim of this paper is to extend the protection against errors by haste (precipitation). Moreover, in extending the model in [VG08] we have found a weakness in the model which is corrected in this paper, as well.

Protection against errors by haste is a basic legal requirement well established in private and public law [Ba06]. This requirement is expressed by two security objectives in [VV08], “O.Correction” and “O.Abort,” as well as by the security objectives 10 and 11 in [CE04]. To meet these two security objectives, we will propose two functions “reset” and “cancel” of a voting process. The abortion of a voting process protects not only against precipitation, but it also protects the secrecy of voting against unwanted external events like the appearance of another person during the voting process. Thus reset and cancel are important for the support of the freedom of vote.

The paper is organized as follows: In the subsequent section 2 we quote those security objectives, from the Protection Profile on basic requirements for online voting products [VV08], that we are going to formalize in this paper. In section 3 we enhance the existing formal IT security model in [VG08] according to our findings and provide a full proof of its correctness. In section 4 we formalize the “reset” and “cancel” functions, which have been introduced in section 2. In section 5 we prove that this extended security model is correct and, thus, provides a smooth extension of the original security model [VG08]. To complete the picture, in section 6 we show (informally) at which points in a voting process our security rules of the formal model are applied. Finally, in section 7 we draw some conclusions from our work and point to further research.

## 2 Security Objectives

Security models start with the identification of security objectives [CC06, Gr08]. In the protection profile of a basic set of security requirements for online voting [VV08], a set of thirty-two security objectives for online voting products are specified. The following two of these have been used as a first step towards a formal model for remote electronic voting systems in [VG08]<sup>2</sup>:

**O.OneVoterOneVote:** It is ensured that (a) each voter can cast one vote and (b) no voter loses his voting right without having cast a vote.

**O.UnauthVoter:** Only eligible voters who are unmistakably identified and authenticated are allowed to cast a vote that is stored in the ballot box.

These two objectives are met by specifying properties that define “secure system states” and rules to be applied on any function that securely transfers a system state into another system state. Therefore, these rules are called transition rules. After specifying the related security state properties and transition rules of these two security objectives, we will extend the model by including two more security objectives from [VV08], namely:

**O.Abort:** The voter can abort his voting process at any time prior to the final casting of the vote without losing his right to vote.

**O.Correction:** There is no limit on the number of corrections a voter can make to his vote until the final casting of the vote.

These objectives will not be met by security properties, but by a further transition rule. We propose that “reset” and “cancel” functions are the appropriate prototype functions of this rule, whereby “cancel” will be a repetition of “reset” until the initial state of a voter’s voting process. We will prove (in section 5) that these rules preserve the security properties of **O.OneVoterOneVote** and **O.UnauthVoter**.

---

<sup>2</sup> We refer to [VV08] as well. This paper formally models some basic security requirements for electronic voting, which apply to both voting machines and online voting.

The rules for allowed state transitions are to be implemented by voting products as functions for data processing. However, the rules do not determine appropriate places for these functions within a voting process. Strictly speaking, it is not the purpose of an IT security model to design processes or protocols. Although we are not going to design the voting process, we will show (in section 6) informally at which points in a voting process our rules (and especially the “reset” and “cancel” functions) would be applied.

### 3 The Basic Model

#### 3.1 The original model of [VG08]

We quote the basic model from [VG08] in that we take the security objectives **O.OneVoterOneVote** and **O.UnauthVoter** and associate them with properties of a secure state and allowed state transitions. Before we define the security properties, we define (general) system states of a voting process:

**Definition 1 (voting system state)**

A system state  $S := \langle W, V, voter \rangle$  is represented by a triple of the following three entries:

1.  $W$  – Set of eligible voters (those who are listed in the electoral register and have not yet cast a vote).
2.  $V$  – Set of (encrypted) votes stored in the e-ballot box.
3.  $voter: V \rightarrow M$  – Mapping of (encrypted) votes to their electors.

$W_{total}$  is the set of all eligible voters registered by the responsible voting officials before the voting system is started.  $M$  is a superset of  $W_{total}$  that contains any user who tries to access the remote electronic voting system, whether or not this particular user has the right to cast a vote. The function  $voter$  assigns each (encrypted) vote to its producer (voter).

The initial state is defined as the triple  $S_0 := \langle W_{total}, V_0 = \{\}, voter_0 = \{\} \rangle$ .

We assume that state transitions  $t_1, t_2 \dots$  that carry the system from state to state are stimulated by events such as the login of a voter into the system, the request of an empty voting ballot, the filling out of the ballot, the casting of a vote, etc.

$$S_0 \xrightarrow{t_1} S_1 \xrightarrow{t_2} \dots \xrightarrow{t_i} S_i$$

Now we follow the basic model in [VG08] and proceed to defining secure system states, and then we state the rules for allowed state transitions.

### Definition 2 (secure voting system state, basic version)

A state  $S_i$  is a secure state iff (all of) the following constraints hold:

$$\begin{aligned} \text{OneVoterOneVote (A)} & \quad \forall v, v' \in V_i : \text{voter}(v) = \text{voter}(v') \Rightarrow v = v' \\ \text{OneVoterOneVote (B)} & \quad \forall w \in W_{total} \setminus W_i : \exists v \in V_i : \text{voter}(v) = w \\ \text{UnauthVoter} & \quad \forall v \in V_i : \text{voter}(v) \in W_{total} \end{aligned}$$

### Definition 3 (rules for permitted state transitions)

A state transition from state  $S_i$  to state  $S_{i+1}$  stimulated by event  $t_{i+1}$  is permitted,  $\text{permitted}(S_i \xrightarrow{t_{i+1}} S_{i+1})$ , if one of the following rules holds:

$$[\text{Rule 1}] \quad W_i = W_{i+1} \wedge V_i = V_{i+1} \wedge \text{voter}_i = \text{voter}_{i+1}$$

$$[\text{Rule 2}] \quad \exists v \in V_{i+1} : (\text{voter}_{i+1}(v) \in W_i \wedge W_{i+1} = W_i \setminus \{\text{voter}_{i+1}(v)\} \wedge V_i = V_{i+1} \setminus \{v\})$$

[Rule 1] represents a state transition in which no vote is cast whereas [Rule 2] models a state transition during which an eligible voter casts a vote into the ballot box. This voter is eliminated from the list of eligible voters and his vote is stored in the ballot box.

### 3.2 Discussion of the original model

The security theorem in [VG08] proves that “for all permitted state transitions starting with the initial state [...] holds that any reachable state is secure.” This security theorem is correctly proven. But it doesn't regard those secure states that are reached by an illegal state transition. Any state reachable by a permitted state transition from a secure state is obliged to be secure, even if the initial state (which is secure) has been reached for any reason by a non-permitted state transition. The following example shows that this isn't fulfilled for the formal security model in [VG08]:

Assume an eligible voter casts a vote into the ballot box, but –due to erroneous system implementation– the voter isn't eliminated from the list of eligible voters. The succeeding system state remains secure because *OneVoterOneVote(B)* doesn't specify properties of  $W_i$ , but only of  $W_{total} \setminus W_i$ . Suppose this voter casts a vote again. Since this voter is still eligible, his vote is stored in the ballot box and he is eliminated from the list of eligible voters. This represents a permitted state transition according to [Rule 2]. But the ballot box now contains two votes from the same voter. Thus an insecure system state is reached from a secure state by a permitted state transition.

To avoid this situation the definition of secure states needs to be extended such that a voter who has cast a vote into the ballot box is removed from the list of eligible voters. This can be incorporated into the formal model of [VG08] by extending definition 2 by an additional requirement for secure states:

$$\text{OneVoterOneVote (C)} \quad \forall w \in W_i : \forall v \in V_i : \text{voter}(v) \neq w$$

Still, this extension isn't sufficient yet. Let  $S_i$  be a secure state. Furthermore, assume that an eligible voter  $x$  who hasn't yet cast a vote wants to vote. Let the system be in a state where the voter's eligibility is provable, i.e.,  $x \in W_i$ . Due to an incomplete or incorrect list of registered voters, let  $x \notin W_{total}$ . This situation and  $x \in W_i \setminus W_{total}$  are not forbidden by the definition of a secure state. Therefore, the system would follow [Rule 2] and let  $x$  cast a vote  $v$ , such that  $V_{i+1} = V_i \cup \{v\}$  holds. Even though state  $S_i$  was secure and the state transition from  $S_i$  to  $S_{i+1}$  was permitted, state  $S_{i+1}$  isn't secure since  $x = \text{voter}(v) \notin W_{total}$  violates the security property *UnauthVote*.

To avoid this situation, we add one more requirement for secure states, namely, that the system allows only registered voters ( $x \in W_{total}$ ) to cast a vote ( $x \in W_i$ ):

$$\text{EligibleVoters} \quad W_i \subseteq W_{total}$$

This leads our enhanced security model's definition of a secure state.

### 3.3 The enhanced model

We now include the additional security properties *OneVoterOneVote (C)* and *EligibleVoters* from our discussion in section 3.2 above to the three security properties *OneVoterOneVote (A and B)* and *UnauthVoter* from definition 2 in section 3.1 above and thus we get the final definition of a secure state by these five security properties:

#### Definition 4 (secure voting system state, advanced version)

A voting system state  $S_i$  is a secure state if (all of) the following constraints hold:

<i>OneVoterOneVote (A)</i>	$\forall v, v' \in V_i : \text{voter}(v) = \text{voter}(v') \Rightarrow v = v'$
<i>OneVoterOneVote (B)</i>	$\forall w \in W_{total} \setminus W_i : \exists v \in V_i : \text{voter}(v) = w$
<i>OneVoterOneVote (C)</i>	$\forall w \in W_i : \forall v \in V_i : \text{voter}(v) \neq w$
<i>EligibleVoters</i>	$W_i \subseteq W_{total}$
<i>UnauthVoter</i>	$\forall v \in V_i : \text{voter}(v) \in W_{total}$

Obviously, the five properties above are equivalent to the two following properties:

**(ap.1)**  $voter$  is an injective function (equivalent to *OneVoterOneVote* ( $A$ )),

**(ap.2)**  $W_{total} = W_i + voter(V_i)$  (“direct sum”, equivalent to the other four properties). The direct sum means that both hold,  $W_i \cup voter(V_i) = W_{total}$ , and  $W_i \cap voter(V_i) = \emptyset$ .

The proof that (ap.1) and (ap.2) are equivalent to definition 4 is straight forward and left as an exercise to the reader. It is also easy to see that the initial state  $S_0$  is secure, because the voter function is empty, and hence injective; and  $W_0 \cup voter(V_0) = W_{total} \cup \emptyset = W_{total}$ ; and  $W_0 \cap voter(V_0) = W_{total} \cap \emptyset = \emptyset$ .

### Security Theorem

Permitted state transitions of definition 3 carry secure states into secure states according to definition 4.

**Proof:** In [VG08] we proved the security theorem in the weaker version that starting with  $S_0$  any sequence of allowed state transitions would always lead to a secure state. We had to prove this by mathematical induction. Here we prove a stronger version that starting from any secure state (regardless of how this state was reached) an allowed state transition according to [Rule 1] or [Rule 2] will always reach a secure state. That is, we have to prove directly: For any  $i \geq 0$ , if we assume that  $S_i$  is secure, i.e., it has properties (ap.1) and (ap.2), and that  $permitted(S_i \xrightarrow{t_{i+1}} S_{i+1})$ , i.e.,  $t_{i+1}$  follows [Rule 1] or [Rule 2], then we have to show that properties (ap.1) and (ap.2) also hold for  $S_{i+1}$ .

Let  $t_{i+1}$  follow [Rule 1]. Then  $V_{i+1} = V_i$  and  $W_{i+1} = W_i$  and  $voter_{i+1} = voter_i$ , thus  $S_{i+1}$  simply inherits the security properties (ap.1) and (ap.2) from  $S_i$ .

Let  $t_{i+1}$  follow [Rule 2]. Then exactly one eligible voter casts a vote  $v$  into the ballot box during state transition  $t_{i+1}$ . Thus,  $W_{i+1} = W_i \setminus \{voter_{i+1}(v)\}$  and  $V_{i+1} = V_i \cup \{v\}$  holds.

(ap.1) Then  $voter_{i+1}$  is injective on  $V_i \cup \{v\}$ , because  $voter_{i+1}$  restricted on  $V_i$  is, by definition, equal to  $voter_i$ , which is injective, and  $voter_{i+1}(v)$  does not match with any other image of  $voter_i$ , because  $voter_{i+1}(v) \in W_i \setminus W_{i+1} \subset W_i$  and hence cannot have been in  $voter_i(V_i)$  since  $W_i \cap voter(V_i) = \emptyset$ .

(ap.2) (i)  $W_{i+1} \cup voter(V_{i+1}) = (W_i \setminus \{voter(v)\}) \cup voter(V_i \cup \{v\}) = (W_i \setminus \{voter(v)\}) \cup (voter(V_i) \cup \{voter(v)\}) = W_i \cup voter(V_i) = W_{total}$ .  
The last equality holds because  $S_i$  has property (ap.2).

(ii)  $W_{i+1} \cap voter(V_{i+1}) = (W_i \setminus \{voter(v)\}) \cap voter(V_i \cup \{v\}) = (W_i \setminus \{voter(v)\}) \cap (voter(V_i) \cup \{voter(v)\}) = W_i \cap voter(V_i) = \emptyset$ .  
The last equality holds because  $S_i$  has property (ap.2).

## 4 An additional transition rule for “reset” and “cancel”

In this section we incorporate the security objectives  $O.Abort$  and  $O.Correction$  into the enhanced formal model. For this purpose we introduce an additional transition rule [Rule 3], which meets these objectives and will, therefore, be associated with a secure “reset” and “cancel” function.

### 4.1 Informal description of “reset” and “cancel”

While  $O.Abort$  is correlated with the sending and receiving of “cancel,”  $O.Correction$  is associated with the sending and receiving of “reset.” With “reset” we mean that during a voting process a voter can go back one step just before the last message that he sent to the server. With “cancel” we mean, that a voter can repeat reset events back to the initial state so that he can restart his individual voting process. On the receiving side, after a voter’s “reset” the voting server must filter out all events that were stimulated by messages exchanged with this voter just before the last message received from this voter. However, all other events stimulated by messages with other voters must be kept by the voting server. On receiving a “cancel” message from a voter, the voting server must forget all events by messages exchanged with this voter, but keep all events stimulated by other voters. The sending and receiving of a “reset” and “cancel” message must be carefully synchronized between voters and their voting server. As a security rule, the “reset” must not create or delete voting rights or cast votes

### 4.2 Formal basics

The formalization of the “reset” and “cancel” functions requires some formal basics on lists and list operations and a communication function on events. Readers who are familiar with the formal specifications can skip to section 4.3.



Let  $M$  denote the set of all communication partners. Then we assume communication partners  $a, b, \dots \in M$  who observe events that are correlated by a communication function  $com$ . Partner  $a$  will be a model for a voter and partner  $b$  will be a model for a voting server. Each partner observes events on his side that are stimulated by the sending and receiving of messages. Events are communicated via messages. If  $a$  sends a message of type  $e$  to  $b$ , then  $a$  observes the event of type  $e$  that he sends to  $b$ , and  $b$  would observe this event with the label  $e$  as a message of type  $e$  that he receives from  $a$ . In the following we will use the terms “message” and “message type” with the same meaning as “event” and “event label”, respectively. We will sometimes say, “sending event” and “receiving event” instead of “sent message” or “received message.” The following event labels (=message types) are useful for the modeling of electronic voting, e.g., [VV08]. Note that they are just an example which we will take up in section 6. They are not exhaustive. For example, message types “error” or “verify” are ignored throughout this paper’s model.

$$Eventlabels = \{\pm login, \pm requestBallot, \pm vote, \pm reset, \pm cancel, \pm confirmBallot, \pm castVote, \pm feedback, \pm logout\}$$

Let  $e \in Eventlabels$  then  $sig(e)$  denotes the algebraic sign of  $e$ . A negative sign of an event label  $e$  indicates that the associated event is being sent, e.g.,  $e = -login$ . A positive sign indicates the associated event is being received, for example,  $e = confirmBallot$ .

*Events* are event labels associated with their sender and recipient. We denote the set of all possible events as

$$Events \subseteq Eventlabels \times M \times M$$

Let  $a, b \in M$  and  $e \in Eventlabels$ . Events are defined as triples, but for convenience we will use the following notation for events instead (cf. [Gr09]):

$$\begin{array}{ll} a(e:b) & \text{a receives a message e from b} \\ a(-e:b) & \text{a sends a message e to b} \end{array}$$

Let for  $1 \leq k \leq n$   $\pi_k$  denote the set-theoretic projection of a Cartesian product of  $n$  sets on its  $k$ -th component. Let  $x = a(\pm e:b)$  be an event and  $\pi_i$  the projection of a tuple to its  $i$ -th element, then

$\pi_1(x)$  returns the event label  $e$  of  $x$ , which may carry a positive or negative sign.

$\pi_2(x)$  returns  $a \in M$ . Note that  $a$  is the sender of the message  $e$  if  $sig(e)$  is positive, and  $a$  is the recipient if  $sig(e)$  is negative.

$\pi_3(x)$  returns  $b \in M$ . Note that  $b$  is the recipient of the message  $e$  if  $sig(e)$  is positive, and  $b$  is the sender if  $sig(e)$  is negative.

For the synchronization of events that are stimulated by messages between  $a$  and  $b$ , we need a way to express that a message is observed by both sides. Let  $Events$  be the set of all possible events,  $a, b \in M$  and  $e \in Eventlabels$ . The function  $com$  is defined as in [Gr09] and maps the sending and receiving of a message on the corresponding event on the partner's side:

$$com: Events \rightarrow Events$$

$$com(a(e:b)) := b(-e:a)$$

$$com(a(-e:b)) := b(e:a)$$

We are going to collect events in ordered lists of events which allow us to operate on sequences of events and on identified events within the list. The algebra of ordered lists is a standard formalism used in theoretical computer science, see for example [MG08]. As usual, a list of events is understood as a finite sequence (or n-tupel) of these events. If  $op$  is a function on lists, for example the deletion of its head element, then the  $k$ -times repetition of the operation is denoted as  $op^k(L) = op_k(op_{k-1}(\dots(op_1(L))\dots))$ .

Useful list functions are [MG08]:

- For any list  $L$  of elements of a set  $Q$ ,  $set(L) \subset Q$  denotes the (unordered) set that consists of all elements of  $L$ .
- $head(L)$  and  $tail(L)$  return the last element of  $L$ , and the rest of the list  $L$  without the last element, respectively. In contrast,  $\overline{tail}$  is complementary to  $tail$  and returns the remaining list without the first element of  $L$ .
- Let  $q \in Q$ , then  $L||q$  appends the element  $q$  at the end of the list  $L$ .
- $|L|$  returns the number of elements in  $L$ .
- Assume  $n \in \mathbb{N}$  a natural number and  $q \in Q$ .  $L[n]$  returns the element at the  $n$ -th position in the list and  $pos(L, q)$  returns the position of the last occurrence of the element  $q$  in the list  $L$ .
- $del(L, l)$  with  $l \in \mathbb{N}$  a natural number returns the list  $L$ , from that the  $l$ -th and all succeeding elements are removed.
- Especially for lists  $L$  of events, we define a filter function, a remove function and a select function. For an event  $x$  and  $k \in \{1, 2, 3\}$ ,  $filter_k(L, x)$  removes all events with event label  $x$  from the list  $L$  if  $k=1$ , or it removes all events whose first or second actor is  $x$  from the list  $L$  if  $k=2, 3$ , and then returns the remaining list. For a communication partner  $a$ ,  $rmv(L, a)$  returns the list  $L$  from which all events that were sent or received by  $a$  are removed. The function  $select_k(L, x)$  returns the list of events where only those events with the event label  $x$  are contained if  $k=1$ , or only those events whose first or second actor is  $x$  are contained if  $k=2, 3$ .

### 4.3 Formalized “reset” and “cancel”

We are now ready to formally define the “reset” and “cancel” event and prove the important synchronization theorem. For simplicity we assume in the following that  $a$  communicates solely with  $b$ , while  $b$  communicates with  $a$  and other partners as well. Thus in the model,  $a$  represents a voting client and  $b$  represents the voting server.

#### Definition 5 (Reset)

Let  $a, b \in M$  and  $X_i$  be the list of events on the side of communication partner  $a$ , i.e.,  $\forall x \in X_i : \pi_2(x) = a$ . Furthermore, let  $Y_j$  denote the list of events on the side of communication partner  $b$ . Let  $sent(X_i)$  denote the list of events that contains the send-events of  $X_i$  only, and let  $received(Y_j)$  denote the list of events that contains the receive-events of  $Y_j$  only, then we define:

$$X_i \parallel a(-reset : b) := \begin{cases} X_0 & \text{if } set(sent(X_i)) = \emptyset \\ del(X_i, l) & \text{else, where } l = \max\{n \in N \mid x_n \in set(sent(X_i))\} \end{cases}$$

$$Y_j \parallel b(reset : a) := \begin{cases} del(Y_j, k) \parallel rmv(\overline{tail}^k(Y_j, a)) & \text{if } C_2 \\ filter_3(Y_j, a) & \text{else} \end{cases}$$

where  $C_2$  is  $\exists k > 0 : k = \max\{n \in N \mid y_n \in set(received(filter_3(Y_j, a)))\}$

Explanation: If a communication partner  $a \in M$  executes a “reset” then the last event  $x_l \in X_i$  which is sent by  $a$  and all successive events to  $x_l$  are deleted. If there is no event in  $X_i$  that is sent by  $a$  (i.e.,  $X_i$  is empty or contains only received events), then  $X_i$  is set to its initial state.

If a communication partner  $b \in M$  receives a “reset” then the last event  $y_k \in Y_j$  that is received by  $b$  from  $a$  is deleted as well as all successive events to  $y_k$ , which are sent to or received from  $a$  by  $b$ . Remark that all events successive to  $y_k$ , which are exchanged with other communication partners, are preserved in the state of communication partner  $b$ . If there is no event in  $Y_j$  that is received from  $a$  by  $b$  (i.e.,  $Y_j$  is empty, doesn't contain any events exchanged with  $a$  or contains only events sent to  $a$ ), then all messages sent by  $b$  to  $a$  are deleted from the list  $Y_j$ , i.e.,  $b$  is set to initial state with respect to  $a$ . All events that are exchanged with different communication partners are preserved.

### General Assumptions:

The reset and cancel functions are to be synchronized between voters and server. They wouldn't work properly if the system is interrupted. Therefore, availability is a security requirement for all communication functions. For the purpose of our security considerations, we assume that our systems are available and work correctly. Therefore, we assume secure communication channels in the following sense:

$$(A1) \exists i \geq 0 : x \in \text{set}(X_i) \Leftrightarrow \exists j \geq 0 : \text{com}(x) \in \text{set}(Y_j)$$

If a communication partner  $a$  exchanges a message  $x$  with  $b$  then there exists a state such that this message is observable on the partner's side.

$$(A2) \forall i > 0 : \forall x_n, x_m \in \text{set}(\text{sent}(X_i)) : \text{pos}(X_i, x_n) < \text{pos}(X_i, x_m) \Leftrightarrow \\ \forall j \geq i : \text{pos}(Y_j, \text{com}(x_n)) < \text{pos}(Y_j, \text{com}(x_m))$$

If a communication partner  $a$  sends two messages in a particular order then the communication partner  $b$  receives them in exactly that order.

### Theorem (Synchronization property of “reset”)

In a secure communication environment (i.e., A1, and A2 hold) the sending and receiving of “reset” events are well synchronized. Formally:  $\text{com}(\text{head}(\text{sent}(X_i \parallel a(\text{-reset}:b)))) = \text{head}(\text{received}(\text{select}_3(Y_j \parallel b(\text{reset}:a), a)))$ .

**Proof:**

Given the two assumptions (A1) and (A2). Furthermore, we denote  $C_1: \text{set}(\text{sent}(X_i)) \neq \emptyset$ , i.e.,  $a$  hasn't sent anything so far and  $C_2: \text{set}(\text{received}(\text{filter}_3(Y_j, a))) \neq \emptyset$ , i.e.,  $b$  hasn't received any message from  $a$ . According to definition 5 of "reset," the following four possibilities exist:

1. *Neither  $C_1$  nor  $C_2$  holds.*

Then  $X_i \parallel a(-\text{reset}:b) = \emptyset$  and  $\text{select}_3(Y_j \parallel b(\text{reset}:a)) = \text{select}_3(\text{filter}_3(Y_j, a)) = \emptyset$ . Obviously, Theorem 1 is true.

2.  *$C_1$  does not hold, but  $C_2$  holds.*

This directly contradicts assumption (A1). If there was no message sent by communication partner  $a$ , then there can't be any message received from  $a$  by  $b$ .

3.  *$C_1$  hold and  $C_2$  does not hold.*

This is a direct contradiction to assumption (A1) as well. If there was no message received by  $b$  from  $a$ , then there can't be any message sent from  $a$  to  $b$ .

4.  *$C_1$  and  $C_2$  hold.*

Let  $x_i$  be the last event sent by  $a$  before executing reset. Due to premise (A2),  $\text{head}(\text{received}(\text{select}_3(Y_j, a))) = \text{com}(x_i)$  holds. On the side of communication partner  $a$ , the event  $x_i$  and all successive events to  $x_i$  are eliminated during the execution of reset. On the side of communication partner  $b$ , the event  $\text{com}(x_i)$  and all successive events to  $\text{com}(x_i)$  that are exchanged with the communication partner  $a$  are eliminated during the execution of reset. All events successive to event  $x_i$  that are exchanged with different communication partners are preserved.

If  $\text{set}(\text{sent}(X_i \parallel a(-\text{reset}:b))) = \emptyset$  holds, then due to premise (A1)  $\text{set}(\text{received}(\text{select}_3(Y_j \parallel b(\text{reset}:a), a))) = \emptyset$  holds as well. Thus Theorem 1 holds.

Assume  $\text{sent}(X_i \parallel a(-\text{reset}:b)) \neq \emptyset$  and let  $x_m = \text{head}(\text{sent}(X_i \parallel a(-\text{reset}:b)))$  be the last sent event after the execution of "reset." Given precondition (A1) there exists a state on the partner's side such that  $\text{com}(x_m) \in Y_j \parallel b(\text{reset}:a)$ . Furthermore, in accordance to premise (A2)  $\text{com}(\text{head}(\text{sent}(X_i \parallel a(-\text{reset}:b)))) = \text{head}(\text{received}(\text{select}_3(Y_j \parallel b(\text{reset}:a), a)))$  holds.

**Definition 6 (“Cancel”)**

Let  $a, b \in M$  and  $X_i$  be the list of events on the side of communication partner  $a$ , i.e.,  $\forall x \in X_i : \pi_2(x) = a$ . And let  $Y_j$  be the list of events on the side of communication partner  $b$ , respectively. Then we define:

$$X_i \parallel a(-cancel : b) := X_0$$

$$Y_j \parallel b(cancel : a) := filter_3(Y_j, a)$$

Explanation: If a communication partner  $a$  executes a “cancel”, then he is set back to his initial state with an empty event list  $X_0$ . If a communication partner  $b$  receives a “cancel” from communication partner  $a$ , then all events sent to or received from  $a$  by  $b$  are eliminated from his event list.

**Remark:**

According to definition 6 the following holds: Let  $k := |sent(X_i)| + 1$  be one more than the number of all sending events in the list of events on the side of  $a$ , and let  $l := |received(filter(Y_j, a))| + 1$  be one more than all events that  $b$  has received from  $a$ , then

$$X_i \parallel a(-cancel : b) = X_i \parallel^k a(-reset : b) = X_0$$

$$Y_j \parallel b(cancel : a) = Y_j \parallel^l b(reset : a) = filter_3(Y_j, a)$$

The execution of “cancel” by a communication partner  $a$  can be expressed by means of the event “reset”. Communication partner  $a$  executes  $a(-reset : b)$  for each event sent by him, until there are no events left or only events that are received by  $a$ . By executing an additional  $a(-reset : b)$ ,  $a$  is set to its initial state with empty event list  $X_0$ .

The execution of “cancel” on the partner’s side can be specified by the means of the event “reset” as well. Communication partner  $b$  receives  $b(reset : a)$  for each event received from  $a$ . The remaining events are all either sent from  $b$  to  $a$  or are messages exchanged with other communication partners different than  $a$ . The remaining events sent to  $a$  are deleted by the execution of an additional  $b(reset : a)$ .

In the next step we must make sure that “reset” cannot produce insecure states, i.e., we have to specify a transition rule for “reset”.

#### 4.4 Transition rule for “reset”

A state transition from state  $S_i$  to state  $S_{i+l}$  stimulated by event  $t_{i+l}=a(-reset:b)$  is permitted,  $permitted(S_i \xrightarrow{t_{i+l}} S_{i+l})$ , if the following rule holds:

[Rule 3] Let  $T_i$  be the list of events observed by  $a$  before the execution of “reset,” and let  $T_{i+l}$  be the list of events observed by  $a$  after the execution of reset, and let  $l := |T_{i+l}|$  be the length of list  $T_{i+l}$ . Furthermore, let  $T := \overline{tail}^l(T_i)$  be the list of reverted events. Then  $t_{i+l}=a(-reset:b)$  is permitted iff

$$(a \in W_i \cap W_{i+l}) \wedge (\forall 1 \leq j \leq |T|: permitted(S_{i+j} \xrightarrow{T[j]} S_{i+j+1}))$$

Explanation: According to [Rule 3], a state transition from state  $S_i$  to state  $S_{i+l}$  stimulated by event  $t_{i+l} = a(-reset:b)$  is an allowed state transition if the voter is eligible and has not yet cast his vote, both, before and after, the execution of “reset” ( $a \in W_i \cap W_{i+l}$ ) and all reverted state transitions were permitted ( $permitted(S_{i+j} \xrightarrow{T[j]} S_{i+j+1})$ ).

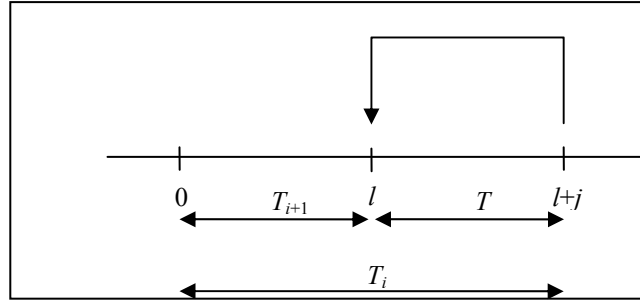


Figure 4.1: Relation between the list of events before and after the execution of “reset.”

Remark: [Rule 3] is compatible with both rules, [Rule 1] and [Rule 2], because it resets only permitted transitions. [Rule 3] conforms to [Rule 1] because by the reverted state transitions no vote had been cast into the ballot box. [Rule 3] is compatible with [Rule 2] because the resetting voter would not be one of those voters who had cast votes into the ballot box. Due to the definition of the “reset” function (the filter function in definition 5 makes sure that actions of other participants remain untouched!), the ballots of the other voters would not be reverted, of course.

## 5 The extended model

In this section, we show that [Rule 3] complies with the security properties (ap.1) and (ap.2) which are equivalent to definition 4.

The specification of an IT security model requires first the specification of secure system states and of permitted state transitions [Gr08]. As a definition for secure system states, we use the definition 4 of section 3.3 above in the version with the two properties (ap.1) and (ap.2), namely that “*voter* is an injective function” (ap.1) and that “ $W_{total}=W_i+voter(V_i)$ ” (ap.2).

### Extended security theorem

Permitted state transitions according to [Rule 1] and [Rule 2] of definition 3 as well as according to [Rule 3] from section 4 carry secure states into secure states according to definition 4. Formally, if a state  $S_i$  is secure and  $permitted(S_i \xrightarrow{t_{i+1}} S_{i+1})$ , then  $S_{i+1}$  is also a secure state.

**Proof of the security theorem:** For [Rule 1] and [Rule 2] we have proven the security theorem already in section 3. We have only to prove the security theorem with respect to [Rule 3] of secure “resets.” To simplify the proof, we first prove the following lemma:

**Lemma 1:** If a state  $S_i$  is secure and  $permitted(S_{i-1} \xrightarrow{t_i} S_i)$ , then  $S_{i-1}$  was a secure state.

**Proof of Lemma 1:** If  $S_i$  is a secure state and  $t_i$  was a permitted state transition, then the state transition  $t_i$  was performed according to [Rule 1] or by [Rule2]:

[Rule 1]: Then  $V_i = V_{i-1}$  and  $W_i = W_{i-1}$  hold. Since  $S_i$  is secure,  $S_{i-1}$  was secure as well.

[Rule 2]: Then there exists exactly one vote  $v$  that has been put into the ballot box during state transition  $t_i$  such that  $V_{i-1} = V_i \setminus \{v\}$  and  $W_{i-1} = W_i \cup \{voter(v)\}$ . It has to be proven that the properties (ap.1) and (ap.2) hold for  $S_{i-1}$ .

(ap.1) Firstly, *voter* is injective on  $V_{i-1}$  because  $V_{i-1} = V_i \setminus \{v\} \subset V_i$ , and *voter* is assumed to be injective on the full  $V_i$  already.

(ap.2) Secondly, it must be shown that  $W_{i-1}+voter(V_{i-1})=W_{total}$ :

(i)  $W_{i-1} \cup voter(V_{i-1}) = W_{total}$  holds because *voter* is injective, and therefore

$$W_{i-1} \cup voter(V_{i-1}) = W_i \cup \{voter(v)\} \cup voter(V_i \setminus \{v\}) = W_i \cup \{voter(v)\} \cup (voter(V_i) \setminus \{voter(v)\}) = W_i \cup voter(V_i) = W_{total}.$$

The last equality holds because  $S_i$  is assumed to be secure.



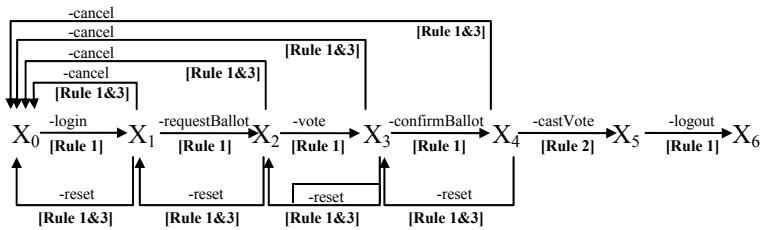
- (ii)  $W_{i-1} \cap voter(V_{i-1}) = \emptyset$  is true because:  
 $W_{i-1} \cap voter(V_{i-1}) = (W_i \cup \{voter(v'')\}) \cap voter(V_i \setminus \{v''\})$ . Since  $S_i$  is a secure state such that  $W_i \cap voter(V_i) = \emptyset$  holds, it is sufficient to prove that  $\{voter(v'')\} \cap voter(V_i \setminus \{v''\}) = \emptyset$  holds. And this is true because *voter* is injective.

This completes the proof of Lemma 1.

Given the Lemma 1 above, the proof of the security theorem with respect to [Rule 3] is trivial: If  $t_{i+1}$  follows [Rule 3] and  $S_i$  was secure, then all reverted state transitions were permitted according to [Rule 3], and hence  $S_{i+1}$  is a secure state according to our Lemma 1 above.  $\square$

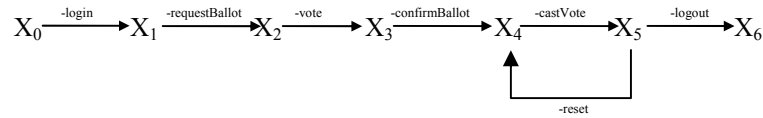
## 6 Transition rules in a voting process

In the previous sections we have specified conditions for allowed state transitions. In this section we show, at which points in a voting process these rules are to be applied. There are several variants conceivable for each voter's polling process [VV08]. Since we are not going to discuss process designs, we have chosen one process variant with login at start of the voting process.



**Figure 6.1:** Mapping of transition rules on a (simple version of a) voting process

A sequence of transitions of the polling process is exemplarily shown in figure 6.1 where only the client side of the electronic voting process is considered. The voter identifies and authenticates himself by sending his data to the voting server (*-login*). If the voter is unmistakably identified and authenticated on the server's side, the voter is able to request the ballot form (*-requestBallot*). The ballot form is displayed on the voter's client and the voter makes his voting decision (*-vote*). The voter has to confirm his ballot (*-confirmBallot*) to protect against errors by haste. Afterwards he casts a vote into the ballot box (*-castVote*), where the casting of the vote follows [Rule 2]. The voter is allowed to correct his vote (*-reset*) or abort (*-cancel*) his voting process any time prior to the final casting of the vote, where "reset" and "cancel" follow [Rule 1] and [Rule 3].



**Figure 6.2:** Example of an illegal placing of “reset” in the voting process

But the voter should not be allowed to correct or abort his vote after the final casting of his vote, as shown in figure 6.2. If he could do that, he would obtain the possibility to cast a vote into the ballot box for a second time. Note that our recommendation for the placement of “reset” and “cancel” complies with the security transition [Rule 3] which states that the voter is eligible, both, before and after the execution of “reset” and that all reverted state transitions were permitted.

## 7 Conclusion

In this paper an IT security model formalizes some basic security requirements for electronic voting: one voter one vote, eligible voters, the correction of a vote, and the abortion of a voting process. The corresponding security properties are specified as secure system states. The voting functions are controlled by state transition rules. We prove mathematically that a function following the rules would transfer a secure state into a secure state.

This contribution demonstrates how security requirements for electronic voting can be formalized and how an existing IT security model can be extended by adding gradually security objectives. However, we have not yet included anonymity or verifiability in our model. For a complete formalization of the security requirements for electronic voting, the IT security model presented in this paper needs to be extended by the remaining security objectives defined in the Protection Profile [VV08] and [GH09] step-by-step. Our next research step is to incorporate voter anonymity.

## Bibliography

- [Ba06] Bachmann, Gregor: Private Ordnung („Private Regime“). Jus Privatum 112, Mohr Siebeck, Tübingen 2006. Esp. S. 293 on precipitance and legal certainty of promises, also in the Anglo-Saxon legal domain.
- [BP73] D. E. Bell and L. J. LaPadula. Secure Computer Systems: Mathematical Foundations, and A mathematical model. ESD-TR-73-278, MTR-2547, Vols 1&2. The MITRE Corporation, Bedford, MA, Nov 1973.
- [CC06] Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, Version 3.1, 2006
- [CE04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation rec(2004)11 adopted by the committee of ministers of the Council of Europe and explanatory memorandum. Strassburg, 2004.
- [DD85] US Department of Defense: Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Dec 1985, <http://csrc.nist.gov/publications/history/dod85.pdf> [25 Feb 2010]
- [GH09] Grimm, R., Hupf, K.: Sicherheitsanforderungen an Onlinewahlen, In: Pichler (Hrsg.), Österreichischer Workshop über Elektronische Wahlen, Salzburg, Dezember 2009.
- [Gr08] Grimm, R.: IT-Sicherheitsmodelle. Technical Report 03/2008, Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, 2008
- [Gr09] Grimm, R.: A Formal IT-Security Model for a Weak Fair-Exchange Cooperation with Non-Repudiation Proofs. In SECURWARE 2009, The Third International Conference on Emerging Security Information, Systems and Technologies, Athens, 18-23 June 2009. IEEE Computer Society Press, 2009
- [MG08] MIT/GNU Scheme 7.7.90+, Chap. 7 Lists, MIT, Boston Massachusetts, 2008, <http://www.gnu.org/software/mit-scheme/documentation/mit-scheme-ref/> [25 Feb 2010]
- [VG08] Volkamer, M., Grimm, R.: Development of a Formal IT Security Model for Remote Electronic Voting Systems. In Electronic Voting, pages 185-196, 2008.
- [VV08] Volkamer, M., Vogt, R.: Common Criteria Protection Profile For Basic Set of Security Requirements for Online Voting Products. BSI-CC-PP-0037, Version 1.0, 18. April 2008. <http://www.bsi.bund.de/> [visited Feb 8, 2010]
- [Wa05] Wang, Andy Ju An: Information Security Models and Metrics. Proceedings of the 43rd ACM Southeast Regional Conference, Vol 2, Security Session, 2005, pp. 178 - 184.



# Compliance of POLYAS with the Common Criteria Protection Profile - A 2010 Outlook on Certified Remote Electronic Voting

Niels Menke and Kai Reinhard

Micromata GmbH  
Marie-Calm-Str. 1-5  
34131 Kassel  
Germany  
[n.menke@micromata.de](mailto:n.menke@micromata.de), [www.polyas.de](http://www.polyas.de)

**Abstract:** In 2008, the German Federal Office for Information Security issued the common criteria protection profile for Online Voting Products (PP-0037). Accordingly, we evaluated the Polyas electronic voting system, which is used for legally binding elections in several international organizations (German *Gesellschaft for Informatik*, GI, among others), for compliance with the common criteria protection profile and worked toward fulfilling the given requirements. In this article we present the findings of the process of creating a compliant security target, necessary restrictions and assumptions to the system design as well as the workings of the committee, and architectural and procedural changes made necessary.

## 1 Introduction

The remote electronic voting system Polyas has been in use since 1996 in international remote electronic voting projects like the elections of the German Society for Informatics (GI), the *Deutsche Forschungsgesellschaft* (DFG), Swiss Life Group Elections, and Finnish as well as German youth elections [RJ07]. As of 2010, about a million legally binding votes have been cast using the Polyas system, supporting different methods of authentication as well as rigorous documentation while maintaining a high level of anonymity and integrity.

In 2008, the German Federal Office for Information Security and its advisory board released and certified the common criteria protection profile for remote electronic voting systems [PP08]. Since then, it has been the ambition of Polyas' developers to certify the compliance of its system and architecture with the common criteria. Toward this goal we completed a security target for the existing Polyas system based on the protection profile and adjusted the system as well as defining restrictions where necessary.

In this paper we will present the workings of Polyas and the changes made necessary to achieve compliance with the requirements of the common criteria at large and the protection profile in particular, thereby showing possible solutions to typical problems when building electronic voting systems to be evaluated against the existing common criteria protection profile.

## **2 The Polyas voting process, revised**

### **2.1 Overview**

Polyas, among the electronic voting systems available on the market, is classified as a remote electronic voting system aka Internet voting system [VK06].

The most common variant of Polyas, which is to be discussed in this paper, uses a secret-based authentication by a common username/password process (see also [PP08] p. 16f.). While other variants of voter-authentication, namely, OpenID or Smartcard, exist and can be deployed on top of the core system, they are considered experimental at this point of time and therefore not yet to be evaluated against the common criteria protection profile.

Polyas ensures anonymity in the voting phase by means of a separation of duty among its components (see also [RJ07]). Voting with Polyas takes place by means of a Web browser (thin-client). While rich-client architecture is also available and can be used on demand of the voting committee, it is not yet subjected to common criteria evaluation.

### **2.2 Polyas general architecture—Achieving a separation of duty**

The general concept of Polyas' architecture is inspired by real world ballot box voting sites (see figure 1). An electoral registry holds the authentication details and provides the point of entry for the voter who is going to cast his vote. The voter will hand his authentication credentials to the registry server, which will verify these credentials.

To ensure that the registry has not been compromised, the credentials are signed with a validation signature that resides on a third, separate validation server, and will be verified in case of authentication. Following a Two-Man-Rule, both the validation server and the electoral register will need to approve the credentials' authenticity before the voter will be issued a temporary voting token, and, with it, the opportunity to cast his vote.

To ensure that the same credentials are not used more than once for different voters (or voters unknown at the time of signing) the validator stores the signature after the first successful authentication attempt and together with the electoral register, will reject any credentials that are not eligible to cast a vote (see figure 2).

Once the voter has received his voting token, he is passed to the ballot box server, which presents one or more virtual ballot papers for the voter to cast his vote. Once the voter has successfully cast his vote, the temporary voting token is deleted from the system, thereby destroying any link between the voter's identity and his then-cast vote.

The election process from pre-voting phase to post-voting phase is to be electronically managed and overseen by the voting committee by means of a separate system. This system will, for example, allow the committee to monitor how many votes have been cast, how many voters have been marked as having voted, oversee the system health and functionality of the other components as well as starting, stopping, and finally counting the entire vote once a configurable number of committee members has authorized each of these respective processes.

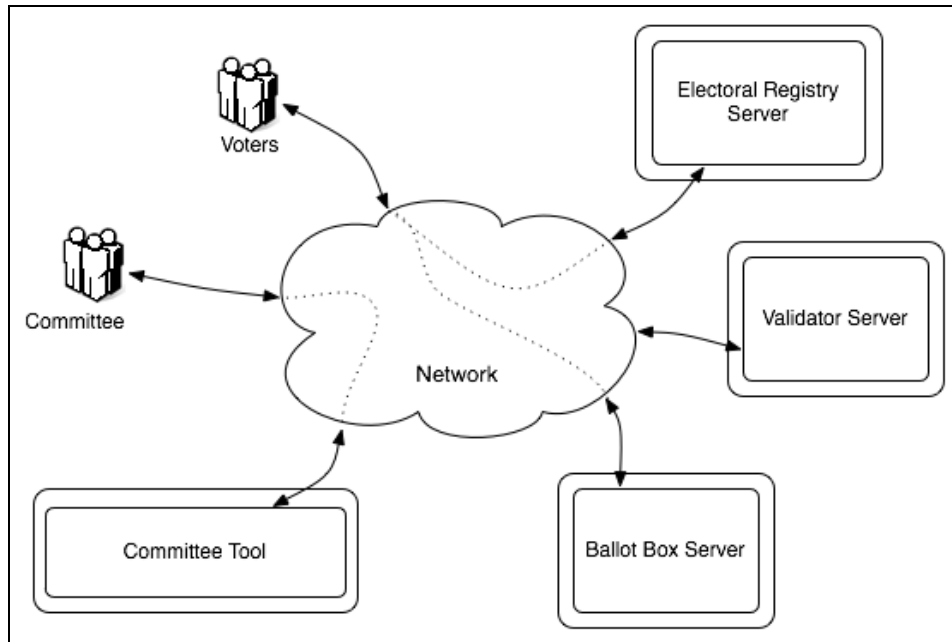


Figure 1: Polyas Architecture

### 2.3 Process Overview

**Pre-Voting** There are six steps that need to be undertaken before an election can be started (See also [RJ07]):

- Installing the Polyas software on each individual server. The software should be signed to recognize software manipulation in the post-voting process.
- Generating the authentication credentials, signing them with the validators' signature, and storing them in the registry.
- Sending the authentication credentials to each respective voter. Credentials will be sent under cover and need to be revealed (a one-way-process) by the voter in order to view it.

- For each of the four Polyas components, an https, a communication, and a database key pair must be generated. The https public keys will be shared. The private communication and database keys shall be encrypted, and one pass phrase for each of the keys must be entered. These pass phrases may form an additional layer of separation of duty for the vote-starting process as they can be handed out to different members of the committee and entered separately into the committee-tool.
- The private communication keys of the ERS and VS are used to sign the hashed credentials of each respective voter. Let  $sk_{VS}$  be the validators' communication key and  $sk_{ERS}$  be the electoral registry's communication key. Further, let  $hash$  be the SHA-256 hashing function and  $sig$  be the RSA signature function.

Then each column will contain:

$$ID - hash(Pw) - sig_{ERS} - sig_{VS}$$

where

$$sig_{ERS} \equiv sig(sk_{ERS}, hash(Pw)) \quad \text{and} \quad sig_{VS} \equiv (sk_{VS}, sig_{ERS}).$$

The thus a signed electoral register shall be installed on the register system. The whole electoral register is further signed with  $sk_{ERS}$ . This signed register should then be stored in case the need for validation arises.

- Once all components are online, the election is waiting to start. A configurable number of committee members must approve the start of the election in the committee-tool under their respective logins. Once this has happened, the system is awaiting passphrase authorization.
- For each of Polyas' components there will now be two remote access tokens (passphrases) in existence, which will have to be entered before the respective system will be operational. For the committee-tool, these shall be entered separately. When the committee tool is online and the start has been authorized, the tool will provide an interface for the committee to enter the respective passphrases of each other component.
- Once the last passphrase has been entered, the election enters the voting phase.

**Voting** The high level protocol of a voter casting a vote is described in figure 2. It is distinctive in several ways: For one, the vote is already sent to the ballot box server after the first acknowledgment. Then, the exact sent vote is sent back to the voter for verification. Thus the voter can be sure the ballot box server has interpreted his vote correctly. Votes are generally stored in an encrypted and signed manner.

Moreover, the tokens are also stored, encrypted using the public key of the involved database. Note that, according to the requirements of the protection profile, the token is explicitly not stored in the database when it is first sent to the ballot box server. It is only after the voter has confirmed his vote to be cast that the vote is finally written to the database.



Aside from the requirements of the protection profile and the signing and encryption of each individual vote, each block of thirty votes (whilst thirty is a variable) will be stored alongside with a signature of this block, factoring in the signature of the previous block, in the case that more than thirty votes have already been stored, providing a further layer of protection against any possible manipulation.

The voting token represents the authentication of the voter to the ballot box, so the ballot box cannot link the incoming or already cast vote to the credentials of the voter who issued the vote. An attacker attempting to break Polyas' anonymity would have to have unencrypted access to both of the fully separated systems (electoral register and ballot box) to establish such a link. Additionally, the vote token is encrypted via RSA, so the attacker would have to know the private key of the ballot box and/or electoral registry server in order to intercept it. Note that at no time will the token be written to the database. After the voting token is marked as invalid, its acquired memory is overwritten with pseudorandom values to ensure secure deletion.

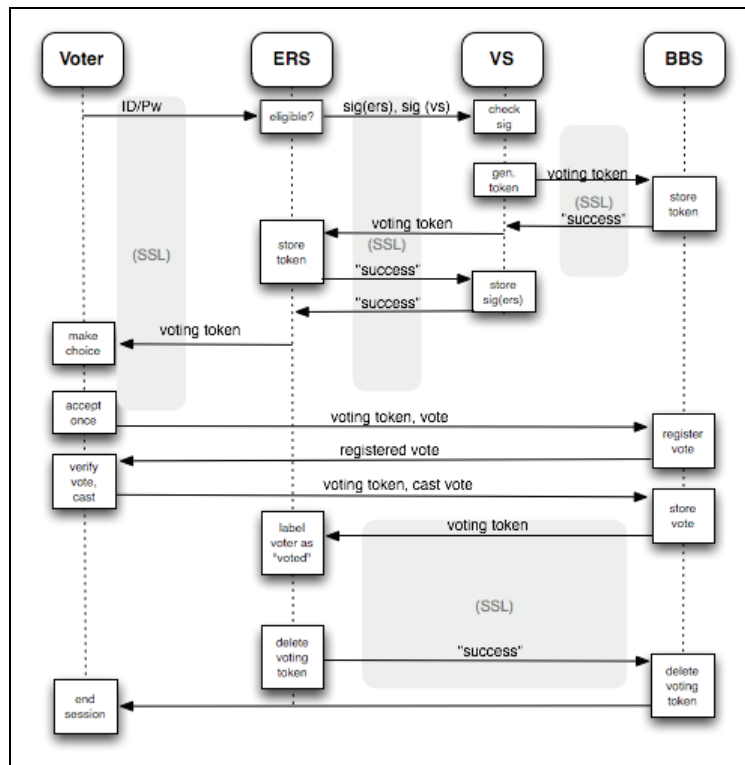


Figure 2: Polyas Protocol

To provide a means of defense against so-called phishing attacks, Polyas uses a module based on Image-Maps, presenting the user with a virtual, clickable keyboard on screen. There, the user can enter his credentials and the browser will only submit X/Y-coordinates. Because these are randomized with every different login-attempt, the risk of password phishing is drastically reduced.

The protection profile requires a voter be able to cancel his voting process as well as be able to intentionally cast an invalid vote. Both requirements are fulfilled. If the voting process is intentionally cancelled or technically interrupted before the vote is committed, no vote will be stored in the database, and the voter will be able to vote again. If the process is interrupted once the vote has been finally cast, the voter will be notified of his cast on his next login-attempt.

We consider the protocol to be safe against the voter trying to sell his vote. The possibility of selling would imply there being proof of his vote (and its content). Aside from the so far not solvable dilemma of remote voting, namely, that the voter can be observed throughout the entire voting process (see [KV05]), it is not possible for the voter to review his vote once cast. Therefore, it is also not possible to prove the contents of his vote to a third party after having submitted the vote and/or before submitting, since the voter might always change his choice shortly before finally casting his vote. Once the vote is cast, the voter will only be presented with the message that he has indeed voted, but for said reason no further details on his vote will be given.

**Post-Voting** To close the election, the committee has to issue the command to stop in the committee-tool. Once a sufficient number of “stop election” commands to satisfy the separation of duty has been cast, the committee-tool automatically walks through the process of stopping the election (see also [Me08]). For this purpose the validator server is first taken offline; thus disabling the possibility of further logons but not disturbing any possibly still ongoing vote processes.

After a certain amount of time to allow any remaining logged on voters to cast their votes, e.g., ten minutes, has expired, the electoral registry server is also taken offline, thus cancelling any eventually ongoing vote processes.

The ballot box server is then issued a command to count the votes and store the result along with a signature as a certificate of authenticity. The signed result can be retrieved by the committee from the ballot box server and is also displayed in the committee-tool. The committee-tool further generates a post-voting documentation including the results of the count, the log files of all involved systems, an image of each respective database, and the electoral register. All of this data will be stored in a signed archive.

As the software has been signed in the pre-voting process, it should be verified in the post-voting process that the software is still carrying the same signature to exclude the possibility of unauthorized modifications.

### **3 Achieving and maintaining compliance**

#### **3.1 Assessing the challenges**

The Polyas architecture and process as described in 2.2 and 2.3 already fulfilled many of the objectives presented by the common criteria protection profile [PP08], as was already suggested in [RJ07]. The practicality of the implemented solutions for non-political remote electronic voting had been proven as mentioned in the introduction and in [VK06].

For one example, the protocol used by Polyas offers a natural way of achieving secrecy and anonymity when voting by fully separating the systems responsible for authenticating the voter and receiving/tallying his vote and only maintaining linkage in the form of a secure token that will be deleted at the very moment the voter has cast his vote. Simultaneously, the objective to only allow legit voters, who are unmistakably identified, had already been achieved, as was the secrecy and integrity of messaging, and the so-called overhaste protection that ensures that a voter will not cast an irreversible vote in error.

There were however, unfulfilled requirements given by [PP08] concerning the handling of the committee's tasks and its separation of duty, as well as preventing the tallying of intermediate results by members of the committee.

### **3.2 Assumptions and strict conformance**

The common criteria protection profile for remote electronic voting does make certain conditions about the operation of the voting system that may not be circumvented for the certificate to remain valid. These conditions include, among others (for a complete list, please see [PP08]):

- The initial data in the electoral registry is that which the committee has approved. No additional data is entered by any means.
- Every registered voter has successfully received his credentials.
- The surrounding technical environment and network will function correctly for the time of the election.
- The voter will not be observed while voting (see 2.3 on vote buying).
- The committee can be trusted and will only use the functionality provided by the target of evaluation.
- The voter will verify he is connected to the correct voting system before voting.
- Data that is not under the control of the target of evaluation will be deleted once the vote has been successfully cast.

These assumptions reduce the functionality to be implemented to achieve compliance to a subset that is provided exclusively by the Polyas system as the target of evaluation.

Additionally, the protection profile demands strict conformance, which essentially means that all of the requirements have to be fulfilled by the target of evaluation itself (here: Polyas) and not by any organizational means 'on top' of the actual software.

### **3.3 Achieving separation of duty for the committee**

One of the main challenges presented by the protection profile was the implementation of strict separation of duty for the election committee. This has been achieved in Polyas by introducing a fourth system to the original three systems in [RJ07], encapsulating the full functionality that the election committee can and may use to administer and oversee the election. This is supported by the assumption that the committee is to be trusted to not use any other knowledge or method to manipulate the election (see 3.2).

The aforementioned system, the Polyas committee-tool, integrates smoothly into the Polyas election lifecycle. It allows for the committee to safely, easily, and traceably start and stop as well as count and archive the complete election. In addition, it allows the committee to oversee the election, monitor the state of every involved system, run self-tests, view the logging of all involved systems, and see how many votes have been cast up to the point of examination as well as how many voters have been marked as having voted. Anomalies in this case can thus easily be detected even while the election is still in an ongoing state, so the committee could decide upon measures to be undertaken in case of any discrepancies.

When the election is to be counted, the committee-tool provides the option of warning the committee if the number of cast votes falls below a configurable amount, thereby possibly endangering the anonymity of the cast votes.

The most prevalent feature of the committee-tool, though, is its rigorous enforcing of the separation of duty for the committee. For every election, the separation of duty count variable  $S$  with  $S > 1$  may be configured to a size appropriate for the specific committee.

The system will then only execute the functions of starting, stopping and/or counting the vote once  $S$  different committee members have authorized this particular function with their respective credentials.

Once a committee member has given his or her authorization for a task (i.e. starting the voting phase), the committee-tool will inform him on the number of additional authorizations needed until the requested action will be carried out by the committee-tool. Every committee member may, of course, authorize each action once and only once.

### **3.4 System Safety and Self-Testing**

The protection profile states that the election officers must be notified of malfunctions of the network connection or of storage of data. In such cases, the election officers should carry out a test sequence provided by the target of evaluation as demonstration of the correct operation (self-test) [PP08].

This requirement was achieved by including an already mentioned self-test routine in the committee-tool. This routine can either be carried out manually on request of an election officer, whereby it is ensured that only one self-test routine can be issued at once in case of multiple logged in election officers at the same time, or can be configured to run on a time-based schedule. In case of any detected faults at the levels of each system's hardware, storage integrity, system-time, anomalies in number of cast votes or network connection, the committee will immediately be notified of the fault and any possible consequences for the election and be asked to take appropriate counter-measures.

Any noticeable problems during the aforementioned self-test routine will be logged alongside with timestamps and therefore be included in the election archive documents.

### **3.5 Prevention of intermediate results**

The protection profile requirement that no information flow between the committee and the ballot box server may result in intermediate results to be extrapolated in any way ([PP08]). Because the protection profile is formulated under the assumption that (see 3.1) the committee will only use the means provided by the target of evaluation itself, and because the committee usually will not have any direct access to the ballot box server, restricting the acting possibilities of the committee during the voting phase can solve this.

Once the vote has been started, there is no possibility offered in Polyas for the vote to be tallied unless the election is also stopped in the process. While the committee may oversee how many votes have been cast at every point in time during the voting phase, no disclosure on the content of these votes is ever given before the vote is finally stopped. Note that once stopped, in accordance to the protection profile, the election may not be resumed. Restarting a stopped election will unavoidably require the ballot box server to be cleared of any votes that had so far been cast.

Further, the stopping of the election as well as an assumed restart would have to be authorized by each of the  $S$  members of the committee, hence would not go unnoticed by at least  $S$  members of the committee as well as the voters who will be trying to vote during the—should such an attempt be made—inevitably resulting down-time of the voting system.

### **3.6 Audit records for the committee**

The protection profile requires the committee to be able to read the audit information (successful identification and authentication of election officers, starting and stopping of the polling phase, starting of the tallying with determination of the election result, performance and results of every self-test and identified malfunctions) from the audit records of each involved system [PP08]. This information is made available in Polyas by means of the committee-tool, where each committee member can inspect the logs of each of the four Polyas component-systems in an easily readable and comprehensible format. Note that these audit files explicitly do not contain any information on the voters' logins, the identities of voters who have or have not cast their vote nor any vote content so no conflict arises with the given security objectives, particularly the secrecy of voting.

## **4 Conclusion**

In this paper, we presented possible solutions to the challenges presented by the common criteria protection profile for remote electronic voting systems using the example of the Polyas system. The first look in respect to the then upcoming protection profile in 2007, [RJ07], still presented some challenges to overcome regarding the compliance of a state-of-the-art electronic voting system to the requirements of the common criteria protection profile. Additionally, there was no proof of the practicality of [PP08] so far.

The final version of the protection profile, by implying strict conformance, made organizational solutions a non-option. Instead, each requirement of the protection profile had to be directly implemented into the voting system. To achieve compliance for the Polyas system, certain minor adjustments to the protocol were necessary; as was a new tool for the committee to restrict its action options, its monitoring of the voting system's health, its view of the audit records, to enforce a separation of duty among committee members, and to prevent the tallying of intermediate results. As has been described, all of those objectives could be fulfilled while still maintaining strict conformance as well as preserving the advantages of the originally implemented protocol concerning secrecy of voting and the one-voter one-vote principle. An architectural balance between anonymity and security is still maintained in a sufficient manner for non-political remote electronic voting.

At present, we consider the described system to be compliant with the current protection profile and are looking toward qualified evaluation to achieve independently certified remote electronic voting. Therefore, we are confident that we have shown that it is possible to implement an electronic voting system for non-political voting systems that fulfill the criteria given by [PP08].

The [PP08] certification will be the first of its kind in the world of pc-based remote voting. The common criteria process will assure consistent and trusted evaluation, as well as opening up possibilities to further build upon attained knowledge and extend the acquired solutions. We look forward to additional challenges presented by the certification and publishing the first practical common criteria security target based on the protection profile.

## Bibliography

- [Gr06] Grimm, R., R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, and M. Weinand. 2006. Security requirements for non-political Internet voting. In *Electronic voting 2006. Proceedings of the 2nd international workshop on electronic voting*, ed. Robert Krimmer, 203–212. Bonn, Germany: Gesellschaft für Informatik.
- [Me08] Menke, N. 2008. Sicherheit elektronischer Wahlsysteme am Beispiel des Online-Wahlsystems Polyas. Master's thesis, University of Kassel, Germany.
- [PP08] Bundesamt für Sicherheit in der Informationstechnik. 2008. *Common Criteria Schutzprofil—Basisansatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, BSI-CC-PP-0037*
- [RJ07] Reinhard, K., and W. Jung. 2007. Compliance of POLYAS with the BSI protection profile. Basic requirements for remote electronic voting systems. In *E-voting and identity. First international conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, revised selected papers*, ed. Ammar Alkassar and Melanie Volkamer, 62-75. Springer.
- [KV05] Krimmer, R., and M. Volkamer. 2005. Bits or paper? Comparing remote electronic voting to postal voting. In: *EGOV (Workshops and Posters)*, 225–232.
- [VA07] Volkamer, M., and A. Alkassar (eds.). 2007. *E-voting and identity. First international conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, revised selected papers*. Springer
- [VK06] Volkamer, M., and R. Krimmer. 2006. Die Online-Wahl auf dem Weg zum Durchbruch. *Informatik Spektrum* 29 (2): 98–113.

# A Survey: Electronic Voting Development and Trends

Komminist Weldemariam and Adolfo Villafiorita

Fondazione Bruno Kessler,  
Center for Scientific and Technological Research (FBK-IRST)  
via Sommarive 18  
I-38050 Trento, Italy  
([sisai\\_adolfo.villafiorita@fbk.eu](mailto:sisai_adolfo.villafiorita@fbk.eu))

**Abstract:** Any practitioner working on electronic voting (e-voting) seems to have different opinions on the main issues that seem to affect the area. On the one hand—given the criticality and the risk e-voting systems potentially pose to the democratic process—e-voting systems are permanently under a magnifying glass that amplifies any glitch, be it significant or not. On the other hand, given the interest e-voting raises within the general public, there seems to be a tendency to generalize and oversimplify. This tendency leads to attributing specific problems to all systems, regardless of context, situation, and actual systems used. Additionally, scarce know-how about the electoral context often contributes to make matters even more confused. This is not to say all e-voting systems show the security and reliability characteristics that are necessary for a system of such a criticality. On the contrary, a lot of work still has to be done. Starting from previous experiences and from a large-scale experiment we conducted in Italy, this paper provides some direction, issues, and trends in e-voting. Getting a clearer view of the research activities in the area, highlighting both positive and negative results, and emphasizing some trends could help, in our opinion, to draw a neater line between opinion and facts, and contribute to the construction of a next generation of e-voting machines to be safely and more confidently employed for elections.

## 1 Introduction

The advantages that e-voting systems can bring cannot be achieved without an observable cost (e.g., risks). One of which is opening up security vulnerabilities to attackers [Mer01, GGR07, BBC+08, BBC+10]. In that respect, recently we have seen that most currently deployed e-voting systems share critical failures in their design and implementation, which render their technical and procedural controls insufficient to guarantee trustworthy voting [LKK+03, KSRW04]. The lack of trust can also render even more secure and more reliable e-voting systems completely useless.

Clearly, the abundance of security threats in e-voting systems and their increasing popularity make a strong case for the need to propose new designs, protocols/schemes, techniques and tools for their design, development as well as their security assessment. The application and use of known techniques such as business process modeling and formal techniques and tools in voting, in general and in the development of an e-voting solution in particular, however are very limited and unsatisfactory. Additionally, work to

rigorously define e-voting properties and attack models and languages to describe the counter-measurements is still more preliminary.

Although some progress has been made in understanding and supporting the better development of e-voting systems, e.g., [MN03, XM05b, XM07, WVM07, VWT09, DKR09], there is no classification to understand the common characteristics, objectives, and limitations of these approaches. Thus the lack of a comprehensive comparative study provides little or no direction on choosing the appropriate development techniques for particular needs.

In this paper, we classify the most important development approaches for e-voting systems and compare them with respect to motivations, methods, and logic. More specifically, we have classified them in four major categories, according to what we believe to be their major contributions to the development of e-voting systems: UNDERSTANDING (the risks posed by the introduction of e-voting systems in the polling stations), REQUIREMENTS (developing requirements for e-voting), IMPLEMENTATION (designing voting schemes, protocols, and/or techniques), and ASSURANCE (using techniques and tools to analyze the security of existing systems, by giving lower-level and higher-level assurances). We hope the work contributes to the work done by designers, developers, certification authorities, as well as technical election officials.

The paper is organized as follows. In Section 2 we review the use of (business) process modeling and redesigning to understand the context and risks caused by the introduction of electronic solutions in the polling stations. In Section 3, we briefly survey the progress made in developing requirements for e-voting systems. We continue, in Section 4, by briefly surveying progress made in designing and implementing voting schemes. In Section 5, we focus on the application of formal methods and techniques and tools to assess the security of e-voting systems. We conclude, in Section 6, by presenting some conclusive considerations and viewpoints.

## **2 Understanding Risks**

Understanding the “context” of elections is very important prior to introducing e-voting solutions. The obvious reason is that this helps to understand and discuss the possible risks that can result through the introduction of a new system. Previous work in this area focused on the understanding, representation, and effective implementation of e-voting procedures. That is, using business process reengineering (BPR) to understand what changes could be introduced to the conventional voting procedures to allow a safe and secure transition to electronic elections.

The BPR concept pertains to the redesign in the context of existing business rules, such that the introduction of e-voting solution can be evaluated. As it is critical to define roles and responsibilities within the e-voting process which could furnish a better understanding of who is responsible for doing what during the different process stages to



produce election results, it is also equally important to provide systematic methodology to deduce what could go wrong during this procedural rich workflow, instead of detecting the weaknesses well after attacks have already been taken.

As far as we are aware, the first use of BPR to evaluate the transition to e-voting is that proposed by Xenakis and Macintosh in [XM05b, XM07]. The authors investigated the need for business process reengineering to be applied to electoral process in order to propose a possible transition to an e-voting system. Risks and difficulties while introducing e-voting solutions are discussed, in more detail, in [XM04a, XM04b]. Furthermore, the same authors in [XM04c, XM05a] discussed the need for procedural security in electronic elections and provided various examples of procedural risks which occurred during trials in the UK. The approach can obviously highlight some of the security implications of the administrative workflow in e-voting, such as those discussed in [LKK+03]. However, these approaches do not provide techniques to systematically model and analyze procedural alternatives for better electronic solutions. Additionally, they do not provide ways to analyze the security aspect of these procedures. In other words, a systematic analysis of procedures is absent.

In references [Mat06, WVM07], the authors developed a UML-based methodology for modeling and analyzing electoral processes. The methodology is supported by a tool named VLPM [CMV09] that helps in the modeling, analysis and structuring of electoral procedures as business process models. Beyond that, the VLPM tool helps to assist a lawmaker to link laws with the process models, and a process engineer to analyze the effects of the changes due to the introduction of a new law (or law modification) on the models to maintain the “*synchronization*” of laws with models, as the same time by fostering collaboration between them, i.e. lawmaker and the process analyst. The methodology and the tool have been demonstrated for the development of an e-voting system named ProVotE [VWT09]. An approach to reason on security properties of the “*to-be*” models (which are derived from “*as-is*” model) in order to evaluate procedural alternatives in e-voting systems is presented [BDF+09]. In particular, using Datalog and the underlying analysis tool the authors expressed and analyzed security concerns, such as delegation of responsibility among untrusted parties and trust conflict. The aim is that of understanding problematic trust/delegation relationships and eventually finding ways to adopt a solution to the detected security properties violations.

### **3 Developing Requirements for E-voting**

There are various international documents such as the recommendations from the European Union (EU) Venice Commission [Cou04] and the U.S. Federal Election Commission (FEC) Voting Systems Standard (VSS) [Fed02, Fed05], which describe a set of principles for voting systems. These documents mainly specify principles about the behaviors of each component of a voting system that should be respected, as well as the related procedures. The FEC-VSS, for instance, provides details about the standards to be used for performance and tests of voting machines. It also describes non-functional requirements (e.g., audits log features) and specifications for various hardware components. However, these kinds of requirements often make the development and

implementation of the actual system difficult. Moreover, the way these documents describe (security) requirements is hard to understand, and sometimes they contain contradicting/conflicting requirements —specifically, the conflict between the requirements for secrecy and accuracy. If the e-voting system needs to be developed in a safe and secure way, there must be an appropriate requirements definition. We have surveyed dozen works in this area. Because of the limited space, however, we are able to present but a few of those that we think are the most important and complete.

Reference [Mer01] presents a thorough discussion on three gaps that must be comprehended prior to developing (security) requirements for e-voting systems. These gaps are the *technological gap* —that is, between hardware and software, the *socio-technical gap* —that is, between social and computer policies, and the *social gap* —that is, between social policies and human behavior. The same author also coined the term audit trails, which is often used in DRE machines. Namely, the type of DRE equipped with printed audit trails is often called DRE-VVPAT. That is, a touch-screen-based machine that produces a printout of each vote, verified directly by the voter, to maintain a physical and verifiable record of the votes cast. Thus an essential activity to ensure e-voting system behaves correctly is to lay down what behaving correctly means for that system. This cannot be achieved without a proper engineering approach, such as requirements engineering techniques.

The author in [McG08] presented an approach to address the mentioned problems by proposing a methodological approach for analyzing the root causes of the conflicts, organizational barriers (or procedural barriers), and requirements of a critical election. The approach comprises of two strategies for the development of requirements, namely, top-down and bottom-up. The first one is aimed at developing a set of requirements from an existing catalogue. The latter, instead is aimed at developing a new catalogue.

Subsequent to [McG08], Volkamer has provided, “*a standardized, consistent, and exhaustive list of requirements for e-voting systems*” [Vol09]. Specifically, these requirements are mostly for standalone DRE and remote e-voting systems. Such requirements not only describe requirements that the system should meet, but also specify the corresponding laws or regulations for the evaluation of the systems themselves. The author developed a methodology for the requirement development process. The results of the methodology include system requirements (divided into functional, security, and usability requirements), organizational requirements, and assurance requirements for both stand-alone DRE voting machines and remote e-voting systems. Furthermore, the methodology comprises of crosschecks, existing catalogues, election principles, and the possible threats. This could allow software engineers and developers to easily understand how their systems meet these requirements. Following that, the author proposed an evaluation and certification procedure mostly for remote voting systems by complementing the Common Criteria common evaluation methodology and also developing a protection profile for remote voting.

In reference [WMV09], the authors showed the management and structuring of requirements using finite state machines (FSMs). That is, by defining relationships between requirements and system architecture based on FSMs. More specifically, the

methodology they followed allowed them to understand the election processes, identify constraints, and distinguish both common and event specific requirements from various requirements sources, e.g. from those mentioned above. These are then refined into fine-grained requirements using FSMs. The decomposition from high-level to low-level requirements and the logical dependencies among them have been demonstrated. Additionally, the separation between generic and election or configuration specific requirements is concrete and detailed enough to function as a general reference schema that could be adopted by other solutions. In other words, this approach is fairly general to be used for other e-voting systems and, possibly, to provide a roadmap —rough and draft as it might be— for bridging the gap between higher-level principles and lower level system specifications.

#### 4 Designing Voting Schemes and/or Protocols

Prior works with respect to this area focused on the design of cryptographic schemes, protocols, and/or techniques to improve the design of voting machines. The ultimate goals of these approaches include ensuring a voter can be certain that her/his vote has been recorded correctly and accurately (*voter verifiability*), no voter can prove to anyone else how s/he voted (*receipt freeness*), and an independent body can verify that the recorded votes match exactly with the published tally after the election [Ive91, CFSY95, Cha04]. What is most common to all these approaches is that they rely on the underlying cryptographic principles to various degrees of complexity.

PunchScan [CPS+07, ECCP07] is a cryptographic voting system that is easy to use by the voter as well as by election officials, while at the same time providing a transparent and reliable process. It also provides public verifiability, election integrity and enhanced voter privacy. Scantegrity [CEC+08, CCC+09] is a successor of PunchScan that meets industrial standard by providing end-to-end verifiability of the integrity of critical steps in the voting process and election results. Prêt à Voter (verifiable electronic elections) [RBH+09] is a type of electronic voting system that uses paper based ballot forms that are converted to encrypted receipts to provide security and “auditability”, at the same time remaining coercion resistant and easy to use. The Scratch & Vote is another cryptographic voting method proposed in [Adi06]. It provides public election “auditability” using simple, immediately deployable technology. The method combines a variety of existing cryptographic voting ideas such as homomorphic encryption —e.g., which allows votes to be tallied without decrypting individual votes, the cut-and-choose at the precinct approach, and so on. Additionally, works like [FOO93, BT94, RRN01, SCM08] attempt to provide (maximum) secrecy and/or anonymity for the vote and voter.

We cannot, however, say that cryptographic schemes and/or protocols address the current situation in the democratic process for several reasons. For example, the protocols that have been proposed so far do not yet overcome all of the barriers to their use in critical elections [McG08]; although DRE machines are very popular in public elections in some U.S. states, the applicability and scope of the proposed schemes are very limited in these machines. Moreover, as noted in [KSW05], some cryptographic

protocols have some security holes, such that sensitive information about the election can be leaked in one way or another. Therefore, we must analyze their security by considering the system in its entirety since these protocols are only one part of a larger system composed of voting machines, software design and implementations, and complex election procedures [KSW05].

In reference [Sas07], the author presents the concept of “*designing voting machines for verification*,” aimed at providing techniques to help vendors, independent testing agencies, and others verify the critical security properties of DRE voting machines. The basis idea of the approach consists of two interesting techniques. The first focuses on creating a trustworthy vote confirmation process, where the author proposed an architecture that splits the vote confirmation code into separate modules whose integrity are protected using hardware isolation techniques. The second focuses on helping to ensure a very important property in voting, that is, “*None of a voter’s interactions with the voting machine, including the final ballot, can affect any subsequent voter’s sessions.*” In order to do that, the author used a hardware resets technique that restores the state of modules components to a consistent initial value between consecutive voters. With this, it could be possible to eliminate the risk of privacy breaches and ensure that all voters are treated equally by the systems.

Other works, such as [SKW06, Yee07] apply techniques used in other domains —like pre-rendering user interface and hardware separation— to build higher assurance with accessible, verifiable and secure e-voting systems. The design of a trustworthy DRE-based voting system by exploring the TPM (Trusted Platform Module) infrastructures (e.g., PKI, hardware protection of cryptographic keys) is presented in [PT09]. Additionally, the authors present a scheme that improves registration integrity, and introduces a design that prioritizes election integrity. Their voting system has nine steps as a whole, from an election’s inception to its final conclusion.

## **5 Providing Assurances**

With respect to the assurance of e-voting systems, existing works focus on two main areas to assess the security of e-voting systems. While the first one focuses on providing lower-level assurances, the other focuses on providing higher-level assurances; both use powerful techniques and tools.

### **5.1 Applying formal methods to e-voting**

The use of formal methods in the specification and verification of e-voting systems is relatively new. Existing works in this area present formal specification and verification of an e-voting system at different levels of abstraction. These works aim to demonstrate how feasible the formal verification of voting machine logic, thereby providing a higher level of assurance about the security of the system. In this area the trends focus on three

closely related aspects, mainly according to the aim of the verification. These are verifying cryptographic protocols, system behavior, and procedures.

The references [DKR09, KR05] present a framework for formal specification and verification of three privacy-type e-voting protocol properties. These properties are vote-privacy, receipt-freeness, and coercion-resistance. The authors used applied  $\pi$ -calculus [AF01] to formalize these properties as observational equivalence, after formalizing the voting protocol as a set of processes using the same machinery. In [CFM+08], the authors used a CCS (Calculus of Communicating Systems)-like process algebra with cryptographic primitives to specify and analyze some properties of the e-voting system they built. More specifically, they presented a small mobile implementation of an e-voting system named M-SEAS (Mobile Secure E-voting Applet System) and used formal verification technique to validate the security properties of the system.

The authors in [VWT09] demonstrate the integration of formal methods in the development process of a voting system. In particular, the authors specified the behaviors of voting control logic using a UML finite state machine and developed a tool named FSMC<sup>1</sup> that automatically generates NuSMV [CCG+02] code corresponding to the specified FSM (this helped the requirements discussed in [VWT09]). Then they performed the verification using the NuSMV model checker. The results of the model checker, presented in the form of counter-measurement, are then analyzed. This enabled the authors to incorporate the analysis results of the verification into the actual development process of the core application.

In references [WKV09, WKV10], the authors show how formal methods can be used to reverse synthesize existing e-voting systems (named ES&S voting systems). They used the ASTRAL language to specify the ES&S voting process and used the PVS analysis tool. A number of critical security requirements that the machines should respect have been specified and analyzed against the specification. Subsequently, the authors specified known attacks against the system (as demonstrated in [MBV07]) using the same machinery and extended the original specifications, and then performed the analysis on the extended model with the same set of critical security requirements that the original specifications should respect. The two main lessons drawn from their work are: formal methods help gain a better understanding of the security “boundaries” of e-voting systems, and the role that open specifications play in the development of more secure e-voting systems.

The reference [SJSW09] presents an approach for designing and analyzing of an e-voting machine based on a combination of formal verification and systematic testing. They formally verify the correctness of each of the individual components of the voting machine, as well as verify some of the crucial correctness properties of their composition. Their work is targeted to the following verification goals: ensuring that each individual component of the voting machine and their composition should meet the specification of the individual components and their composition respectively; voting machine should be structured to enable sound systematic system testing; ensuring that

---

<sup>1</sup> <http://ict4g.fbk.eu/fsmcp/last/>

the voting machine must behave and store votes according to the voters selection when configured with a particular election definition file. For each module, they construct a formal specification that fully characterizes the intended behavior of that component. A number of properties related to the structural and functional aspects that the machine should satisfy are identified and specified. They used Verilog [TM91] for the implementation of their specification and SMV<sup>2</sup> analysis tool and “satisfiability” solving (especially, the SMT solver) to verify that their Verilog implementation meets the specifications.

Finally, in reference [WV08], the authors proposed an approach to formally analyze procedures. Namely, they proposed a methodology based on the NuSMV [CCG+02] machine to analyze procedures systematically.

## 5.2 Assessing exiting e-voting systems

Some e-voting systems currently deployed in elections have recently undergone a thorough and independent scrutiny to evaluate their security and quality. This is because, in recent years, the DRE machines raised serious security concerns. These machines make the election process less verifiable and greatly expand the aspects of an election for which voters must rely solely on trust. Security vulnerabilities have been reported in each aspect of security—that is, technological, socio-technical, and social aspects, as noted prior in [Mer01]. These vulnerabilities have been systematically investigated and proved by various academic studies. This creates an enigma in the trustworthiness of the machine and the voting process as well.

In line with this, we mention the following academic researches [Jon03, KSRW04, GGR07, BBC+08, ASH+08]. These works assess both hardware and software of different forms of e-voting machines (e.g., Diebold/Premier, ES&S, InterCivic), mostly used in some U.S. states. The studies identified serious design and implementation flaws, which are notable for their level of egregiousness. More specifically, these analyses have showed that the current e-voting systems are vulnerable to very serious attacks. In addition, they have produced a catalogue of vulnerabilities and possible attacks. Some analyses also suggested a drastic change in the way in which e-voting systems are designed, developed, and tested (e.g., by identifying procedures to eliminate or mitigate the discovered issues, by developing a precise methodology and toolsets for the assessment). The assessment methodology presented in [BBC+08, MBV07] is particularly astonishing as it provides various insights on each individual and in-depth step of the analysis. The software testing community can use it for the evaluation of other complex-security critical systems and evaluation.

---

<sup>2</sup> <http://www.kenmcml.com/>

## 6 Discussions and Conclusion

There are a number of established approaches for modeling, specifying, and verifying a system satisfies a set of properties. One important contributor to the security of any system is the way in which the software is designed and developed. Standards for software engineering developed over the last forty plus years require that a system undergo a rigorous process of requirements definition, structured design and review, and careful programming and testing [Som95]. Like proper engineering leads to cars of higher quality, so too does better software engineering lead to more secure, robust software computer systems. Systems that are designed without this kind of careful design and implementation are almost certain to have flaws and security issues.

BPR techniques help to understand, model, and analyze the high-level context of the electoral processes. This provides information about the context of the business architecture (*as-is*) and software delivery (*to-be*) prior to the subsequent development activities for the introduction of an e-voting solution. It also helps in assessing the effectiveness of the processes as experienced and evaluated by the citizens outside the development and support organizations. However, it is not always possible to transform a business solution into an e-voting solution [AO05]. This is because, unlike business processes, the electoral processes are tightly bounded by legal frameworks and are usually more regulated than business processes. Thus, we need a proper methodology and tools that abet such reengineering activities. However, some approaches such as the one given in [CMV09] can be a starting point to extend and reuse in the reengineering process of e-voting projects.

The use of formal methods has been shown to improve the security and quality of complex systems. These approaches allow designers to prove, test, or otherwise examine interesting properties of a complex process whose behavior is specified abstractly, and then interactively refine the behavioral specification to be as close to an implementation as appropriate for a given assurance level. In practice, moreover, the technique has been recognized as a powerful and effective mechanism for improving the security and quality of complex systems (e.g., in avionics). Thus, drawing a direct connection to this can help to improve the current development trends of e-voting machines.

Moreover, the studies of experimental data about the e-voting machines' security, performance and their evolution with respect to the social and technical aspects are still unsatisfactory. This limits their use on a larger scale. For example, data sets based on observing security threats to voters' anonymity by following standard procedures that illustrate each machine's behavior during elections can help raise the transparency in elections using electronic devices and increase the confidence of voters in the democratic system. Data sets related to the process of setting up experiments, running an election, and performing security evaluations across various voting machines (e.g., as in Diebold and ES&S) provide information about the behavior of machines under malicious circumstances, whether they are designed carefully or not, and provide recommendations that need to be considered for design alternatives.

Developing and deploying e-voting systems in a safe and secure manner requires ensuring the technical and procedural levels of assurance with respect to social and regulatory frameworks. In this paper, we have presented techniques mainly in three areas (namely, BPR, formal methods, and security) and showed how these techniques are effectively exercised for correct design and implementation of e-voting systems. Therefore, the success of the next generation of e-voting machines depends upon being able to capitalize on the lessons learned from different disciplines. The work we have presented in this paper is one way in which we can get a better understanding of the strengths and the weaknesses of existing techniques and thus lay the foundations for engineering, designing, implementing, as well as deploying a new generation of more secure and robust technologies for polling stations.

## Bibliography

- [Adi06] Adida, Ben 2006. Advances in cryptographic voting systems. PhD diss., Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology..
- [AF01] Abadi, Martin, and Cédric Fournet. 2001. Mobile values, new names, and secure communication. *SIGPLAN Not* 36(3):104–115. New York, NY, USA: ACM.
- [AO05] Alpar, Paul, and Sebastian Olbrich. 2005. Legal requirements and modelling of processes in e-government. *Electronic journal of e-government*, 3.
- [ASH+ 08] Ansari, Nirwan, Pitipatana Sakarindr, Ehsan Haghani, Chao Zhang, Aridaman K. Jain, and Yun Q. Shi. 2008. Evaluating electronic voting systems equipped with voter-verified paper records. *IEEE Security and Privacy* 6(3):30–39: IEEE Computer Society.
- [BBC+ 08] Balzarotti, Davide, Greg Banks, Marco Cova, Viktoria Felmetzger, Richard Kemmerer, William Robertson, Fredrik Valeur, and Giovanni Vigna. 2008. Are your votes really counted?: Testing the security of real-world electronic voting systems. In *ISSTA '08: Proceedings of the 2008 international symposium on software testing and analysis*, 237–248. New York, NY, USA: ACM.
- [BBC+10] Balzarotti, D., G. Banks, M. Cova, V. Felmetzger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna. 2010. An experience in testing the security of real-world electronic voting systems. *IEEE transactions on software engineering*.
- [BDF+09] Bryl, Volha, Fabiano Dalpiaz, Roberta Ferrario, Andrea Mattioli, and Adolfo Villafiorita. 2009. Evaluating procedural alternatives: A case study in e-voting. *EG* 6(2):213–231.
- [BT94] Benaloh, Josh, and Dwight Tuinstra. 1994. Receipt-free secret-ballot elections (extended abstract). In *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on theory of computing*, 544–553. New York, NY, USA: ACM.
- [CCC+ 09] Chaum, D., R.T. Carback, J. Clark, A. Essex, S. Popoveniuc, R.L. Rivest, P. Ryan, E. Shen, A.T. Sherman, and P.L. Vora. 2009. Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE transactions on information forensics and security* 4(4):611–627.
- [CCG+02] Cimatti, Alessandro, Edmund Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella. 2002. NuSMV 2: An open source tool for symbolic model checking. In *Computer aided verification, lecture notes in computer science*, 241–268. Berlin / Heidelberg: Springer.
- [CEC+ 08] Chaum, David, Aleksander Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, and Poorvi L. Vora. 2008. Scantegrity: end-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46: IEEE Computer Society.



- [CFM+08] Campanelli, Stefano, Alessandro Falleni, Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli. 2008. Mobile implementation and formal verification of an e-voting system. In *Proceedings of the 2008 Third International Conference on Internet and Web Applications and Services*, Washington, DC, USA: IEEE Computer Society.
- [CFSY95] Cramer, Ronald J.F., Matthew Franklin, L. A.M. Schoenmakers, and Moti Yung. 1995. Multi-authority secret-ballot elections with linear work. Technical report, CWI (Centre for Mathematics and Computer Science).
- [Cha04] Chaum, David. 2004. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy* 2:38–47: IEEE Computer Society
- [CMV09] Ciaghi, Aaron, Andrea Mattioli, and Adolfo Villafiorita. 2009. VLPM: a tool to support BPR in public administration. In *Proceedings of the Third International Conference on Digital Society (ICDS2009)*, 289–293: IEEE Computer Society.
- [Cou04] Council of Europe. 2004. Recommendation on legal, operational and technical standards for e-voting. Council of Europe, September. [Available online at <https://wcd.coe.int/ViewDoc.jsp?id=778189>]
- [CPS+ 07] Carback, Richard T., Stefan Popoveniuc, Alan T. Sherman, and David Chaum. 2007. Punchscan with independent ballot sheets: Simplifying ballot printing and distribution with independently selected ballot halves. In *Proceedings of the 2007 LAVoSS workshop on trustworthy elections (WOTE 2007)*. [Available online at [http://punchscan.org/papers/ibs\\_carback.pdf](http://punchscan.org/papers/ibs_carback.pdf)]
- [DKR09] Delaune, Stéphanie, Steve Kremer, and Mark Ryan. 2009. Verifying privacy-type properties of electronic voting protocols. *J. Computer Security* 17(4):435–487.
- [ECCP07] Essex, Aleks, Jeremy Clark, Richard Carback, and Stefan Popoveniuc. 2007. Punchscan in practice: An E2E election case study. In *Proceedings of the 2007 LAVoSS Workshop on trustworthy elections (WOTE 2007)*, held in conjunction with 7<sup>th</sup> workshop on Privacy Enhancing Technologies, Ottawa, Canada.
- [Fed02] Federal Election Commission. 2002. Voting system standards. USA: United States Election Assistance Commission, <http://www.eac.gov/>.
- [Fed05] Federal Election Commission. 2005 Voluntary voting system guidelines (VVSG). USA: United States Election Assistance Commission, <http://www.eac.gov/>.
- [FOO93] Fujioka, Atsushi, Tatsuaki Okamoto, and Kazuo Ohta. 1993. A practical secret voting scheme for large scale elections. In *ASIACRYPT '92: Proceedings of the workshop on the theory and application of cryptographic techniques*, 244–251. London, UK, 1993: Springer-Verlag.
- [GGR07] Gardner, Ryan, Sujata Garera, and Aviel Rubin. 2007. On the difficulty of validating voting machine software with software. In *EVT'07: Proceedings of the USENIX/accurate electronic voting technology on USENIX/accurate electronic voting technology workshop Berkeley, CA, USA*: USENIX Association.
- [Ive91] Iversen, Kenneth R. 1991. A cryptographic scheme for computerized elections. In *CRYPTO '91: Proceedings of the 11th annual international cryptology conference on advances in cryptology*, 405–419. London, UK: Springer-Verlag.
- [Jon03] Jones, Douglas W. 2003. The evaluation of voting technology, chapter 1. In *Advances in Information Security*, 3–16. Ed. Dimitrius Gritzalis: Kluwer Academic Publisher
- [KR05] Kremer, Steve, and Mark D Ryan. 2005. Analysis of an electronic voting protocol in the applied pi-calculus. In *Proceedings of the 14th European symposium on programming (ESOP'05), lecture notes in computer science*, 186–200. Edinburgh, U.K.: Springer.
- [KSRW04] Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. 2004. Analysis of an electronic voting system. IEEE Symposium on security and privacy, 0:27: IEEE Computer Society
- [KSW05] Karlof, Chris, Naveen Sastry, and David Wagner. 2005. Cryptographic voting protocols: a systems perspective. In *Proceedings of the 14th conference on USENIX security symposium Berkeley, CA, USA*: USENIX Association.
- [LKK+ 03] Lambrinouidakis, Costas, Spyros Kokolakis, Maria Karyda, Vasilis Tsoumas, Dimitris Gritzalis, and Sokratis Katsikas. 2003. Electronic voting systems: Security implications of the administrative workflow. In *Proceedings of the 14th international workshop on database and expert systems applications*, 467, Washington, DC, USA: IEEE Computer Society.

- [Mat06] Mattioli, Andrea 2005-2006. Analisi dei processi in ambito di voto elettronico per le elezioni in Provincia di Trento. Master's thesis, University of Trento.
- [MBV07] McDaniel, P., M. Blaze, and G. Vigna. 2007. EVEREST: Evaluation and validation of election-related equipment, standards and testing. Ohio Secretary of State's EVEREST project report. [available online at [www.cs.ucsb.edu/~vigna/publications/2007\\_mcdaniel\\_blaze\\_vigna\\_voting.pdf](http://www.cs.ucsb.edu/~vigna/publications/2007_mcdaniel_blaze_vigna_voting.pdf)]
- [McG08] McGaley, Margaret. 2008. E-voting: An immature technology in a critical context. PhD diss., Department of Computer Science, National University of Ireland, Maynooth.
- [Mer01] Mercuri, Rebecca T. 2001. Electronic vote tabulation checks and balances. PhD diss., University of Pennsylvania.
- [MN03] Mercuri, Rebecca T., and Peter G. Neimann. 2003. Verification for electronic balloting systems, chapter 3. In *Advances in information security*, 31-42: Kluwer Academic Publishers.
- [PT09] Paul, Nathanael, and Andrew S. Tanenbaum. 2009. The design of a trustworthy voting system. *Annual computer security applications conference (ACSAC)*, 507-517: IEEE Computer Society.
- [RBH+ 09] Ryan, P.Y.A., D. Bismark, J. Heather, S. Schneider, and Zhe Xia. 2009. Prêt à Voter: A voter-verifiable voting system. *IEEE transactions on information forensics and security* 4(4).
- [RRN01] Ray, Indrajit, Indrakshi Ray, and Natarajan Narasimhamurthi. 2001. An anonymous electronic voting protocol for voting over the internet. In *WECWIS '01: Proceedings of the third international workshop on advanced issues of e-commerce and web-based information systems*, 188. Washington, DC, USA: IEEE Computer Society.
- [Sas07] Sastry, Naveen K. 2007. Verifying security properties in electronic voting machines. PhD diss., EECS Department, University of California, Berkeley.
- [SCM08] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. 2008. A three-ballot-based secure electronic voting system. *IEEE Security and Privacy* 6(3):14–21: IEEE Computer Society
- [SJSW09] Sturton, Cynthia, Susmit Jha, Sanjit A. Seshia, and David Wagner. 2009. On voting machine design for verification and testability. ACM conference on computer and communications security (CCS'09), Chicago, Illinois, USA, November 9-13 , 463-476: ACM
- [SKW06] Sastry, Naveen, Tadayoshi Kohno, and David Wagner. 2006. Designing voting machines for verification. In *Proceedings of the 15th conference on USENIX security symposium*, volume 15. Berkeley, CA, USA: USENIX Association.
- [Som95] Sommerville, Ian. 1995. Software engineering (5th ed.). Addison Wesley Longman Publishing Co., Inc. Redwood City, CA, USA.
- [TM91] Thomas, Donald E., and Philip R. Moorby. 1991. The VERILOG hardware description language. Norwell, MA, USA: Kluwer Academic Publishers.
- [Vol09] Volkamer, Melanie. 2009. Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities. Springer Publishing Company, Incorporated: Springer.
- [VWT09] Villafiorita, Adolfo, Komminist Weldemariam, and Roberto Tiella. 2009. Development, formal verification, and evaluation of an e-voting system with VVPAT. *IEEE transaction on information forensics and security* 4(4) 651--661.
- [WKV09] Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. 2009. Formal analysis of attacks for e-voting system. In *CRiSIS '09: Fourth international conference on risks and security of internet and systems*: IEEE.
- [WKV10] Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. 2010. Formal specification and analysis of an e-voting system. In *The 5th international conference on availability, reliability and security (ARES 2010)*: IEEE Computer Society.
- [WMV09] Weldemariam, Komminist, Andrea Mattioli, and Adolfo Villafiorita. 2009. Managing requirements for e-voting systems: Issues and approaches motivated by a case study. In *Proceedings of the first international workshop on requirements engineering for e-voting systems*: IEEE Computer Society.

- [WV08] Weldemariam, Komminist, and Adolfo Villafiorita. 2008. Modeling and analysis of procedural security in (e)voting: The Trentino's approach and experiences. In *Proceedings of the conference on Electronic voting technology (EVT)*. Berkeley, CA, USA: USENIX Association.
- [WVM07] Weldemariam, Komminist, Adolfo Villafiorita, and Andrea Mattioli. 2007. Assessing procedural risks and threats in e-voting: Challenges and an approach. In *VOTE-ID, lecture notes in computer science*, 38–49: Springer.
- [XM04a] Xenakis, Alexandros, and Ann Macintosh. 2004. G2G collaboration to support the deployment of e-voting in the UK: A discussion paper. In *EGOV, lecture notes in computer science*, 240–245: Springer.
- [XM04b] Xenakis, Alexandros, and Ann Macintosh. 2004. Levels of difficulty in introducing e-voting. In *EGOV*, 116–121: Springer.
- [XM04c] Xenakis, Alexandros, and Ann Macintosh. 2004. Procedural security analysis of electronic voting. In *ICEC '04: Proceedings of the 6th international conference on electronic commerce*, 541–546. New York, NY, USA: ACM Press.
- [XM05a] Xenakis, Alexandros, and Ann Macintosh. 2005. Procedural security and social acceptance in e-voting. In *HICSS '05: Proceedings of the 38th annual Hawaii international conference on system sciences (HICSS'05) - Track 5*, 118.1. Washington, DC, USA: IEEE Computer Society.
- [XM05b] Xenakis, Alexandros, and Ann Macintosh. 2005. Using business process re-engineering (BPR) for the effective administration of electronic voting. *The electronic journal of e-government* 3(2) 91-98. [available online at [www.ejeg.com](http://www.ejeg.com)]
- [XM07] Xenakis, Alexandros, and Ann Macintosh. 2007. A methodology for the redesign of the electoral process to an e-electoral process. *International journal electronic governance* 1:4–16.
- [Yee07] Yee, Ka-Ping. 2007. Extending prerendered-interface voting software to support accessibility and other ballot features. In *EVT'07: Proceedings of the USENIX workshop on accurate electronic voting technology*, 5. Berkeley, CA, USA: USENIX Association.



## **Session 4: Operation and Evaluation of E-Voting Systems**



# An Evaluation and Certification Approach to Enable Voting Service Providers

Axel Schmidt<sup>1</sup>, Melanie Volkamer<sup>2</sup>, Johannes Buchmann<sup>1</sup>

<sup>1</sup>Cryptography and Computer Algebra

Technische Universität Darmstadt

Hochschulstr. 10

D-64289 Darmstadt

Germany

[{axel,buchmann}@cdc.informatik.tu-darmstadt.de](mailto:{axel,buchmann}@cdc.informatik.tu-darmstadt.de)

<sup>2</sup>Center for Advanced Security Research Darmstadt (CASED)

Morneuegstr. 32

D-64293 Darmstadt

[melanie.volkamer@cased.de](mailto:melanie.volkamer@cased.de)

**Abstract:** In this paper we provide an evaluation and certification approach for Voting Service Providers (VSPs) which combines the evaluation of the electronic voting system and the operational environment for the first time. The VSP is a qualified institution which combines a secure voting system and a secure operational environment to provide secure remote electronic elections as a service [La08]. This centralized approach facilitates legal regulation and evaluation. So far, a legal regulation framework for VSPs has been developed which demands evaluation and certification of the VSP [Sc09a]. Therefore the VSP is required to provide a security concept in which it demonstrates satisfaction of the security requirements defined in the legal regulation. However neither the content of this security concept nor an adequate evaluation methodology has been specified so far. We therefore developed a security concept template and a comprehensive evaluation methodology for the VSP, which includes both the voting system and operational environment of VSPs. Our proposal incorporates existing evaluation methodologies to facilitate evaluation and certification. With this paper and the legal regulation a realistic approach to enable the VSP concept is accomplished.

## 1 Introduction

Security is one of the most important goals in the field of electronic voting. A lot of research has been done to develop sophisticated e-voting protocols with complex cryptographic mechanisms to improve security. An additional approach to strengthen security and trustworthiness is the evaluation and certification of e-voting systems.

Here the security functionality of a system is analyzed for compliance with a predefined and approved set of requirements. In 2008 the first evaluation standards for online voting systems were published—the “Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products” [*sic*] [VV08].

However, in [Sc09b] the authors showed that the security of the operational environment, in which the voting system is implemented, has to be considered as well. One attempt to combine the security of a voting system with a secure operational environment is the Voting Service Provider (VSP) concept [La08]. The VSP is a qualified and professional institution which provides secure remote electronic elections as a service on behalf of the election host. Therefore the VSP provides the secure hardware and software, the voting system, the secure infrastructure as well as the specialist knowledge and the skilled personnel needed to operate electronic elections securely. The VSP is a centralized approach and thereby can be regulated and evaluated easily. Legal regulation is an important means to provide a basis for security, trustworthiness and correct behavior. A corresponding evaluation and certification procedure can verify the compliance with such legal regulation. In [Sc09a] the authors therefore introduced a legal framework for the regulation of VSPs. The framework defines requirements for VSPs and demands their evaluation and certification. The legal regulation stipulates that the evaluation and certification of VSPs is based on a 'security concept.' In this security concept, the VSP needs to demonstrate how the requirements of the legal framework are satisfied. The evaluation authority appointed in the statute uses the security concept as the basis for evaluation and certification of the VSP. The security concept comprises technical and organizational aspects, which have to be addressed by the voting system and/or the operational environment. Concluding, the centralized VSP concept and the legal framework provide an ideal basis for a combined evaluation of the voting system and operational environment.

However neither the content of the security concept for VSPs nor an adequate evaluation methodology has been specified so far. Therefore we developed a comprehensive template for such a security concept for VSPs. Further we propose a combined evaluation approach incorporating existing evaluation methodologies for both the voting system and operational environment. We expand the Common Criteria evaluation for online voting systems [VV08] by including an evaluation approach for the operational environment based on the approved *IT-Grundschrift/ISO27001*<sup>1</sup> methodology [G08d]. In this way we facilitate a fully comprehensive evaluation of VSPs and thereby enable the VSP to be put into practice. Our approach is practical since already existing certificates can be included in the evaluation thereby reducing costs and efforts of the VSP evaluation.

We consider related work in Section 2. In Section 3 we develop a security concept template as the basis for evaluation of VSPs. The template specifies which requirements need to be considered. In Section 4 we introduce the Common Criteria and *IT-Grundschrift/ISO27001* certification methodologies and show how they can be used in a security concept based VSP evaluation. In Section 5 we discuss the applicability of these certification methodologies to the VSP scenario and conclude the paper.

---

<sup>1</sup> eng.: IT Basic Protection/ISO27001



## 2 Related Work

In the area of e-voting, evaluation is mainly considered in the Common Criteria Protection Profile for online voting products [VV08], which we incorporated in our work. Its development has been discussed in [VKG07]. Several companies are striving to have their e-voting software certified accordingly, e.g. the Polyas voting software by Micromata [RJ07].

Regarding the operational environment, there exist several methodologies. For example, ITIL is a collection of best practices concentrating on IT service management and the optimization of service quality<sup>2</sup>. However, ITIL is less security-oriented. A Swiss project in Geneva is working on the implementation and evaluation of an e-voting system<sup>3</sup>. The coordinators specified security requirements for their voting system<sup>4</sup> and used the ISO27001 methodology for evaluation which is a standard for Information Security Management Systems (ISMS) [Re07, Tr09, Is08]. Our evaluation approach is more comprehensive since it builds on a specialized legal regulation and incorporates the Common Criteria Protection Profile [VV08], being the current evaluation standard for online voting systems, which we expand by using the *IT-Grundschatz/ISO27001* methodology for evaluation of the operational environment. Thereby we extend the basic ideas of the Swiss approach. Weldemariam et al. provided a more theoretical approach to assess the operational environment of e-voting systems [WVM07]. In contrast, our work focuses on the practicability of the evaluation in real-world scenarios.

In Germany, the evaluation of Certification Authorities (CAs) is based on an approach similar to the VSP evaluation. The “German Signature Ordinance” legally regulates CAs and requires them to provide a security concept (see [G01] § 2). However profound information on the content of the security concept is missing thereby complicating the CA evaluation. To improve the situation for VSPs, we therefore developed a detailed security concept template facilitating VSP evaluation.

## 3 A Security Concept Template for Voting Service Providers

The legal framework introduced in [Sc09a] specifies only the basic structure of the security concept for VSPs. We therefore developed a detailed security concept template which contains all requirements a VSP must satisfy in order to comply with the legal regulation. We point out that the legal framework for VSPs was developed in Germany and therefore might need adjustment in order to be applied in other countries. This is considered future work.

---

<sup>2</sup> [http://www.ogc.gov.uk/guidance\\_itil.asp](http://www.ogc.gov.uk/guidance_itil.asp)

<sup>3</sup> <http://www.ge.ch/evoting/english/welcome.asp>

<sup>4</sup> <http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN022422.pdf>

### 3.1 Methodology

To identify the requirements, which have to be considered by the VSP in the security concept to comply with the legal regulations [Sc09a], we deeply analyzed the legal framework including the act and ordinance. In order to facilitate the interpretation of the requirements by VSPs, we adapted these requirements to the technical field of application. To this end, we analyzed the corresponding preambles of the legal frameworks. They contain additional information which is relevant for implementation and thereby facilitate concretizing the legal requirements. Moreover we incorporated existing technical standards and requirements catalogs in order to further concretize and supplement the requirements from the legal framework. Therefore we utilized recent standards including the “Legal, Operational and Technical Standards for E-voting” from the Council of Europe [Co04], which define comprehensive requirements for electronic elections, as well as the catalog of requirements for the operational environment of electronic elections presented in [Sc09b], which is based on a multitude of existing literature on e-voting security. We used applicable requirements from these sources for adapting the legal requirements to the technical field and integrated them in our template. As a result many requirements from the catalog [Sc09b] and [Co04] have been included in the template. We structured the resulting requirements based on the provisions from the legal framework. Our approach and especially the incorporation of existing technical standards are inspired by the interdisciplinary KORA<sup>5</sup> methodology [Ha92]. KORA describes a procedure to derive technical requirements and implementation proposals from legal stipulations for the similar scenario of information and communication systems. It has been tried and tested many times (see for example [Ha94] and [Id00]).

### 3.2 Template Structure and Content

The legal framework provides a basic structure for the security concept. For our template we adjusted the structure slightly in order to merge related requirements. Due to space limitations, we cannot present the complete security concept template in this paper<sup>6</sup>. We present the structure and an overview of the included requirements. We provide detailed examples in Section 4.3.

*Technical, structural and organizational safeguards:* The VSP shall describe all technical, structural and organizational measures essential for the operation of a VSP according to the legal regulations. Here we incorporated the majority of requirements from the catalog [Sc09b]. The section includes requirements for secure communication channels that provide unaltered and confidential communication between the voter and election server. Secure storage media must provide integrity, availability, and sufficient capacity. Secure erasure of sensible data as well as archiving and system cleansing measures must be provided.

---

<sup>5</sup> *Konkretisierung Rechtlicher Anforderungen*, eng.: Implementation of legal requirements

<sup>6</sup> The complete template will be published as a technical report shortly.

The VSP must realize the management of cryptographic keys and certificates and correct time for all system components. The VSP shall prevent attacks and unauthorized access to the voting server. The VSP must ensure correct setup of the voting system, set and publish time tables and register the voters correctly.

*Technical products for remote electronic elections:* The VSP shall list the technical products used for its electronic voting services, e.g., electronic voting software or election server hardware. If a product is certified this should be indicated here.

*Setup and operation of remote electronic elections:* The VSP shall demonstrate how it achieves availability; confidentiality and integrity of the voting services and election data; and how it realizes the operation of the election, the briefing of voters, and election host. The VSP's voting services must fulfill the election principles of the particular type of election. It must achieve the secure identification and authentication of the voters. The VSP must demonstrate how the legal requirements for ballot casting are satisfied [Sc09a]. Integrity and verifiability of tallying must be accomplished. The VSP must show how the election and adherence to law are documented and how integrity protection and archiving of such data are achieved. The secure system state must be ensured. This includes correct initial state, secure system interruption, and closure of the voting phase. The VSP must ensure the secure delivery of authentication means to the voters and correct representation of the electronic ballot.

*Warranty of data protection:* The VSP is required to prove that the applicable legal data protection provisions, i.e., the German Federal Data Protection Act, the German State Data Protection Act, and the German Teleservices Act, were observed. This can be achieved by a data protection audit, e.g., by the German Independent Centre for Privacy Protection Schleswig-Holstein<sup>7</sup> or *IT-Grundschutz*, which provides a data protection module<sup>8</sup>.

*Guarantee and maintenance of operation:* The VSP shall demonstrate the precautions taken to guarantee and maintain the operation of the electronic voting service, especially in case of emergencies.

*Personnel:* The VSP shall demonstrate that the employed personnel have the reliability (i.e., guarantee that the legal provisions regarding the VSP's operation are observed) and the specialist qualifications (i.e., the knowledge, experience and skills necessary for their work).

*Residual security risks:* The VSP must assess and value remaining security risks in order to evaluate its reliability. This relates to the residual risk of system failure or interruption in particular with regard to deployed technology. The VSP may refer to valuation from evaluation authorities or manufacturers of deployed products. We discuss this in Section 4.4.

---

<sup>7</sup> [https://www.datenschutzzentrum.de/faq/quetesiegel\\_engl.htm](https://www.datenschutzzentrum.de/faq/quetesiegel_engl.htm)

<sup>8</sup> [https://www.bsi.bund.de/cae/servlet/contentblob/475580/publicationFile/31090/moduleb01005\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/475580/publicationFile/31090/moduleb01005_pdf.pdf)

## 4 Combined Evaluation Approach

The legal framework [Sc09a] for VSPs does not demand a specific methodology for evaluating the security concept. However the incorporation of existing evaluation certificates is explicitly allowed. The intention is to facilitate the evaluation process and avoid double checking. We show how this approach can be realized by applying two approved evaluation methodologies for both voting system and operational environment to the security concept evaluation. We analyzed the requirements contained in our security concept template and found that many requirements are satisfied by either a voting system certified according to the Common Criteria Protection Profile [VV08] or by safeguards for the operational environment from the *IT-Grundschrift/ISO27001* catalogs [G05]. To this end we compared both the ‘objectives’ of the Protection Profile and the ‘modules’ and safeguards from the *IT-Grundschrift/ISO27001* catalogs with the requirements from our template. We describe this in more detail in the following sections. By utilizing an accordingly certified voting system and a certified operational environment, the security concept evaluation effort is reduced to evaluating only a few remaining requirements not covered by those certificates. We therefore propose to combine these methodologies for the security concept based evaluation of VSPs. Thereby we enable the combined evaluation and make it usable for the VSP evaluation. We introduce the methodologies in the following sections. While the *IT-Grundschrift* methodology originates in Germany, we point out that the “*IT-Grundschrift* based on ISO27001” certification is internationally accepted, as is Common Criteria.

### 4.1 Common Criteria

The “Common Criteria for Information Technology Security Evaluation” (CC) is an international standard (ISO/IEC 15408) for computer security evaluation and certification<sup>9</sup>. CC focuses on the evaluation of IT products like hardware or software components. Besides the evaluation of concrete products, CC allows specifying generalized security requirements for a family of products in a ‘Protection Profile’ (PP). Manufacturers thereby are enabled to develop corresponding products. An evaluation authority then evaluates and certifies the compliance of the product’s security functionality with the PP. In 2008, the German Federal Office for Information Security certified and published the “Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products” [*sic*] [VV08]. This PP specifies basic security requirements for online voting system software for non-political elections with low attack potential. The included requirements represent the essential foundation upon which voting systems for all election scenarios can build. It is an important step towards the certification of e-voting systems and is therefore planned to be mandatory for such systems in Germany. For our evaluation approach, the PP ‘objectives’ and ‘assumptions’ are relevant. The objectives specify the security goals which certified voting software is able to achieve.

In order to achieve these security objectives several assumptions are assumed to be realized, which cannot be achieved by the voting software. These assumptions must be satisfied by the operational environment. We show how PP-certified voting software can

---

<sup>9</sup> <http://www.commoncriteriaportal.org/>

facilitate the evaluation of a VSP. Our analysis revealed that many requirements included in the VSP's security concept can be fulfilled by such certified voting software and therefore do not need to be evaluated again in the VSP evaluation (see Section 4.3). Moreover we expanded the PP approach: since we incorporated the requirements from the catalog [Sc09b] into the security concept template (see Section 3.1), we especially included the assumptions towards the operational environment from the PP because these are contained in the catalog. Consequently a certified VSP realizes the secure operational environment assumed necessary in the PP to achieve the security objectives of the voting software. We discuss the applicability of the PP to the VSP scenario in Section 5. For further details on PP evaluation we refer to [VV08] and [VK07].

## 4.2 IT-Grundschatz/ISO27001

*IT-Grundschatz* (eng.: IT Basic Protection) provides a methodology to ensure and certify the security of complex 'information domains' which consist of infrastructural, organizational, personnel and technical components. *IT-Grundschatz* includes a comprehensive catalog of safeguards which can be implemented in order to satisfy protection requirements [G05]. The evaluation and certification methodology of *IT-Grundschatz* has been adapted to incorporate the methodology and the generic requirements on information security management systems from ISO27001 [Is08]. ISO27001 is an approved international standard that specifies requirements for the introduction, operation and improvement of information security management systems (ISMS) [KRS08]. It includes a sophisticated risk management methodology. ISO27001 is the first international standard for information security management that allows certification [G08a]. While ISO27001 specifies requirements, it only provides a very limited number of rather indefinite safeguards to fulfill those requirements. *IT-Grundschatz* can fill this gap by providing a multitude of concrete safeguards which can be used to satisfy the generic requirements from ISO27001. A synthesis of *IT-Grundschatz* and ISO27001 therefore seems plausible [KRS08]. Moreover, *IT-Grundschatz* includes predefined risk assessment to avoid a complex risk analysis at least in scenarios with normal protection levels. Concluding, the *IT-Grundschatz/ISO27001* approach facilitates implementation of the ISO27001 methodology by providing an immense set of safeguards and decreases efforts by reducing the need for costly risk analysis. Compared to classical risk analysis the *IT-Grundschatz* approach is more cost-effective and has been tested in practice for many years [G08a]. An *IT-Grundschatz/ISO27001* certification always includes an official ISO27001 certification, but, due to the additionally audited technical aspects, is more informative. The evaluation is performed by an external auditor certified by the German Federal Office for Information Security. In order to prove the achieved security level, *IT-Grundschatz* includes a certification methodology. There are three certification levels; the most comprehensive one is the 'ISO27001 certification based on *IT-Grundschatz*,' which incorporates the procedures and requirements of ISO27001 certification based on *IT-Grundschatz* safeguards.

The certification procedure comprises inspections of the reference documents, on-site inspection, and the generation of audit reports. For lower security level certification, *IT-Grundschatz* provides the less comprehensive and less costly 'entry level' (lowest level) and the 'continuation level' (intermediate level). The certification level is reflected

in according to safeguard categories. While the entry level certification only requires the implementation of safeguards of category A, the continuation level requires A and B. The ISO27001 certificate based on *IT-Grundschutz* requires all safeguards –A, B, and C– to be implemented. The additional ‘Z’ safeguards present supplements that can be used in case of higher security requirements.

#### **4.2.1 *IT-Grundschutz* procedure**

We describe the procedure an institution has to perform in order to secure its information domain according to the *IT-Grundschutz* methodology [G08a, G08b].

At first, the architecture, components, and processes of the information domain must be identified and documented. This is done in the *structure analysis*. Subsequently, the *determining of protection requirements* assesses the level of protection that is appropriate for the particular objects specified in the structure analysis. All objects are analyzed in regard to the potential damage that could result from an impairment of the protective goals of confidentiality, integrity or availability. Then the protection requirement for each object of the structural analysis is classified as “normal,” “high,” or “very high.” Next, the *selection and adaptation of safeguards* must be accomplished. In this modeling process, the prior identified objects of the information domain are associated with respective *IT-Grundschutz* modules. The modules are comprised of generic aspects (e.g., personnel, contingency planning), infrastructure (e.g., server room), IT systems (e.g., laptop), networks (e.g., WLAN), and applications (e.g., database). Each module is associated with specific safeguards suitable to protect the module from typical threats. The safeguards are classified in the categories *A (entry level)*, *B (continuation level)*, *C (certificate)* and *Z (additional)* in accordance with the targeted certification level. All safeguards must be examined and adapted to the specific scenario to ensure the appropriate function. Adaptations must be documented. The result of the procedure is an *IT-Grundschutz* model for use as a test plan for an existing information domain or as a development plan for an information domain in planning. Next, the *basic security check* is performed to provide an overview over the existing security level by comparing current state and target state. Therefore applicability and current implementation status of each selected safeguard are checked. The basic security check reveals where additional steps have to taken in order to implement the *IT-Grundschutz* safeguards.

#### **4.2.2 Handling special requirements**

For efficiency reasons, *IT-Grundschutz* uses a two-stage approach. In the first stage, a normal protection level and a typical application scenario are assumed. Here, the *IT-Grundschutz* safeguards provide an adequate security level. These safeguards can be determined quickly and efficiently allow for increases in the security level of the information domain.

However, in some scenarios, especially in an electronic election scenario, some objects might require safeguards at a higher security level. Therefore *IT-Grundschutz* provides the *supplementary security analysis* in the second stage. At first, it is applied to objects whose protection requirement was classified “high” or “very high” in regard to at least one of the protective goals of confidentiality, integrity or availability in the preceding

analysis. Secondly, a supplementary security analysis is indicated, if a very specific object cannot be modeled appropriately due to the lack of respective *IT-Grundschutz* modules. At last, objects which can be modeled with *IT-Grundschutz* modules, but which are deployed in an untypical way or in an untypical environment shall undergo a supplementary security analysis as well. *IT-Grundschutz* provides several options on how to handle such special requirements. First, the before mentioned additional ‘Z’-safeguards can be implemented to achieve a higher protection level. If not sufficient, an additional *risk analysis* needs to be performed. *IT-Grundschutz/ISO27001* recommends a risk analysis approach described in [G08c]. The intention is to determine threats to the information domain that are not considered sufficiently by the regular *IT-Grundschutz* safeguards and to find appropriate safeguards. We sketch the basic steps. For all target objects the basic *IT-Grundschutz* threats are listed. Additional threats are determined by analyzing the specific protection requirements and the operating scenario for the target objects. Threat probability and potential damage are assessed. The protection level of implemented safeguards is checked. Next, measures are determined to handle the risks—risks can be reduced by additional safeguards, risks can be avoided (e.g., by restructuring business processes), risks can be transferred (e.g., by insurance policies) and under certain circumstances (e.g., low threat probability upon extremely costly safeguards), risks can be accepted and therefore remain. Such residual risks must be assessed and documented. Next a second basic security check is performed to check whether the security level has been improved. At last, *IT-Grundschutz* allows for adaptation by adding new modules to describe threats and safeguards for specific components which are not included in the *IT-Grundschutz* catalog so far. We discuss the applicability of *IT-Grundschutz/ISO27001* to the VSP scenario in Section 5.

### **4.3 Incorporating Protection Profile and *IT-Grundschutz***

We demonstrate how the proposed PP and *IT-Grundschutz/ISO27001* evaluation methodologies can be incorporated in the security concept based VSP evaluation. In our security concept template we linked respective requirements to corresponding PP objectives, meaning that these requirements are covered by the referenced objectives and therefore satisfied by PP-certified voting software. Respectively, to each requirement that has to be satisfied by the operational environment, we linked suitable *IT-Grundschutz* safeguards. To this end, we assumed a generalized VSP architecture and components and mapped them to *IT-Grundschutz* modules. Our results thereby also show how utilizing PP-certified voting software and incorporating existing *IT-Grundschutz/ISO27001* can reduce costs and efforts in the VSP evaluation. Due to space limitations, we are restricted to presenting examples from our security concept template. In the first example a PP-certified voting system would significantly reduce the extent of evaluation. We list the applicable PP objectives that are achieved by a certified voting system. For their complete description, we refer to [VV08].

## *BALLOT CASTING*

*References:* VSP act § 8, VSP ordinance § 3

*PP objectives:* O.Abort (b), O.OneVoterOneVote (b), O.Correction (c),  
O.Acknowledgement (d), O.Proof (e)

The VSP must ensure that the voters

- a) are able to cast an invalid vote,
- b) are able to abort the voting procedure without losing elective franchise,
- c) are able to correct their vote any number of times until the final voting,
- d) receive a confirmation for their vote,
- e) are not enabled by the voting system to show their voting decision to others.

Besides a), all aspects are completely satisfied by a PP-certified voting system. The evaluation authority only needs to ensure that a) is fulfilled.

The next example shows how PP assumptions are integrated into the security concept template and how they can be satisfied by *IT-Grundschutz* safeguards [G05].

## *SYSTEM TIME*

*References:* Operational environment requirements catalog [Sc09b]

*PP assumption:* A.SystemTime

*IT-Grundschutz safeguards:* B 3.3 Network components (S 4.227 Use of a local NTP server for time synchronization), B5 Security of applications (S 5.67 Use of a time stamp service)

The VSP must make the correct time and time stamps available to the voting system, conforming to the actual time. The required exactness is defined by the election host. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.



In this case, the referenced *IT-Grundschrift* safeguards satisfy the assumption. *IT-Grundschrift* safeguards can also be used to satisfy many other requirements from the security concept; e.g., “Guarantee and maintenance of operation” (see Section 3.2) can be realized by implementing the modules “B 1.3 Contingency planning concept” and “B 1.8 Handling security incidents” [G05].

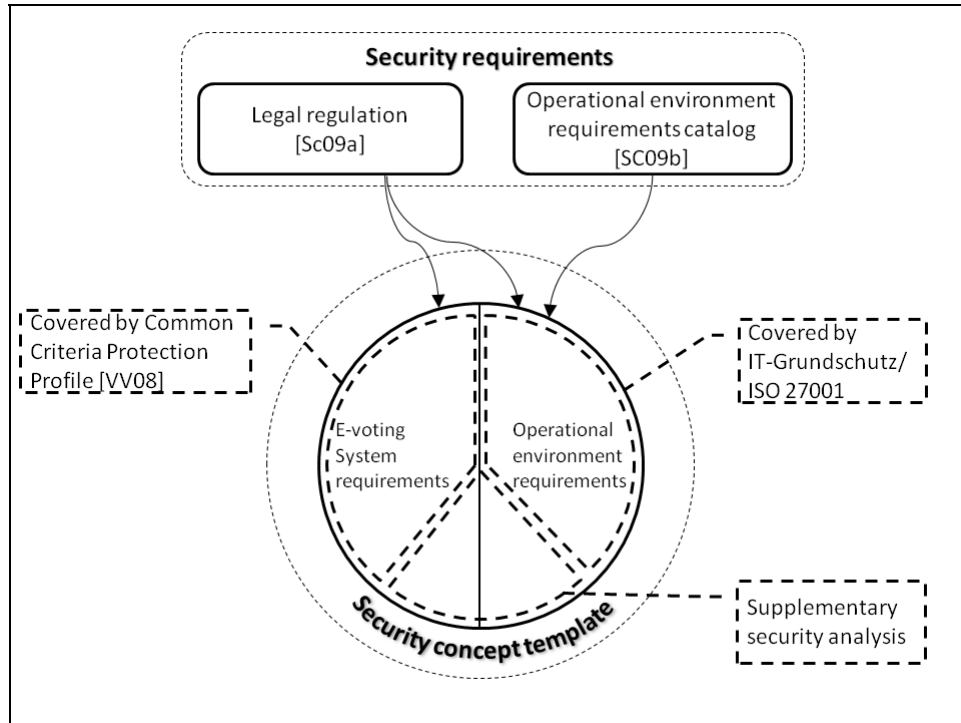
However, our findings revealed that *IT-Grundschrift* safeguards cannot cover all of the requirements in the template. For example, the voter registration or secure delivery of authentication means cannot be described appropriately by *IT-Grundschrift*. Availability or integrity safeguards from the *IT-Grundschrift* might not be sufficient for all election scenarios. We explain how to proceed in the next section.

#### **4.4 Application guideline**

To apply the security concept template we recommend that the VSP performs the *IT-Grundschrift* procedure described above in order to define the specific protection requirements of its system and to analyze to what extent the *IT-Grundschrift* safeguards referenced in the template fulfill these requirements. If certain requirements cannot be covered, a supplementary security analysis and, based on its result, a risk analysis should be performed. Remaining risks identified in this analysis have to be noted in the Section “Residual security risks” in the security concept (see Section 3.2).

If the VSP already has an *IT-Grundschrift* certificate which includes the respective safeguards noted in the template, the particular requirements are satisfied and do not need to be evaluated again. Otherwise the linked safeguards serve as a recommendation on how to satisfy the requirements. However, the operational environment is no plug-in component with exactly defined functional properties; *IT-Grundschrift* safeguards must always be adjusted to the specific local conditions. Therefore the applicability of an existing *IT-Grundschrift* certificate to the security concept and the election scenario always must be checked by the evaluation authority.

If PP-certified voting software is utilized, the VSP can skip the implementation of safeguards for the requirements which are already satisfied by the certified voting software. The evaluation authority only must evaluate whether the remaining requirements have been satisfied. This reduces the costs and effort of conducting a VSP evaluation. To optimize the evaluation, voting software manufacturers could include the fulfillment of these remaining requirements for the voting software from our template to their CC certification to prove not only PP-compliance, but additional ‘VSP-suitability.’



**Figure 1:** Application of evaluation methodologies

We illustrate our evaluation approach and the incorporation of the PP and *IT-Grundschutz/ISO27001* as well as the legal framework and the security concept template in Figure 1.

## 5 Discussion and Conclusion

We discuss the pros and cons of *IT-Grundschutz/ISO27001* and its applicability to the VSP scenario. Alternative certification methodologies like pure ISO27001 are mostly based on a general risk analysis approach. Threats and safeguards have to be determined from scratch. These are complex and costly tasks. In *IT-Grundschutz*, these steps are already integrated in every module of the *IT-Grundschutz* catalog. The large number of *IT-Grundschutz* safeguards simplifies implementation and can support the design process of VSPs. Hence, *IT-Grundschutz* evaluation is practicable. This supports the VSP approach. Basically, these safeguards ensure a normal security level for typical threats. This might not be sufficient for particular e-voting scenarios. However, *IT-Grundschutz* provides supplementary security analysis and risk analysis to adapt to special scenarios with higher protection requirements. Moreover new specific e-voting modules may be added to the *IT-Grundschutz* catalog. Consequently *IT-Grundschutz* seems applicable to the e-voting scenario and is a good choice for the certification of the operational environment of VSPs. Moreover, since many computer centers or similar IT

service providers already have *IT-Grundschutz* certificates, it facilitates their evaluation in case they want to provide electronic voting services as VSPs.

However, in the case of already existing *IT-Grundschutz/ISO27001* certification the implemented safeguards need to be checked during the VSP evaluation for their suitability in the e-voting scenario. The effort should be determined and assessed in practical tests. Furthermore *IT-Grundschutz* is mostly used in Germany. This might reduce acceptance abroad. However, since the legal framework for VSPs is built for the German context, this does not affect the integration of *IT-Grundschutz* in the security concept evaluation.

The applicability of the PP to the VSP scenario is obvious. To develop a state-of-the-art evaluation approach, we need to incorporate this important evaluation concept for voting software. Admittedly, the PP is intended only for non-political election scenarios with low attack potential. However, it represents a foundation of requirements all other election scenarios build upon. Furthermore, since the legal framework for VSPs includes non-political elections as well, the PP perfectly fits into the VSP scenario. Regarding the incorporation of the PP into the VSP evaluation, this is an improvement on both sides; from the VSP perspective, using PP-certified voting software significantly facilitates the VSP evaluation. From the PP perspective, our VSP evaluation approach closes the gap of the PP evaluation because now the VSP is certified to achieve all open PP assumptions towards the operational environment. Thereby an overall evaluation is achieved. A VSP certified according to the security concept template complies with the legal framework, it represents the required operational environment for voting systems certified according to the PP, and it achieves the state-of-the-art in operational environment security as demanded in [Sc09b]. We point out that our combined evaluation approach of voting system and operational environment might be adapted to other e-voting scenarios outside the VSP context. However the existing legal framework, the security concept and the centralized design make the VSP scenario an ideal basis.

In this paper we presented a security concept template for VSPs and a corresponding evaluation methodology. By incorporating existing evaluation methodologies into the security concept evaluation, we presented a realistic approach which reduces the costs and effort of an evaluation. Concluding our work helps to enable the VSP concept and improves e-voting evaluation by combining the evaluation of voting systems and operational environment.

## Bibliography

- [Co04] Council of Europe. 2004. Legal, operational and technical standards for e-voting, Recommendation Rec(2004)11, Council of Europe Publishing, Strasbourg.
- [G01] German Ordinance on Electronic Signatures (Signaturverordnung). 2001. [http://bundesrecht.juris.de/sigv\\_2001/index.html/](http://bundesrecht.juris.de/sigv_2001/index.html/).
- [G05] German Federal Office for Information Security. IT-Grundschutz Catalogues. 2005. [http://www.bsi.de/english/gshb/download/it-grundschutz-kataloge\\_2005\\_pdf\\_en.zip/](http://www.bsi.de/english/gshb/download/it-grundschutz-kataloge_2005_pdf_en.zip/).
- [G08a] German Federal Office for Information Security. 2008. BSI-Standard 100-1 Information Security Management Systems (ISMS), Version 1.5.
- [G08b] German Federal Office for Information Security. 2008. BSI-Standard 100-2 IT-Grundschutz Methodology, Version 2.0.

- [G08c] German Federal Office for Information Security. 2008. BSI-Standard 100-3 Risk analysis based on IT-Grundschutz, Version 2.5.
- [G08d] German Federal Office for Information Security. 2008. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits.
- [Ha92] Hammer, V., Pordesch, U., Roßnagel, A.: 1992. KORA - eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Arbeitspapier 100. provet, Darmstadt.
- [Ha94] Hammer, V., Pordesch, U., Roßnagel, A., Schneider, M.J. 1994. Vorlaufende Gestaltung von Telekooperationstechnik - am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235. Sankt Augustin.
- [Id00] Idecke-Lux. 2000. Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz. Nomos. Baden-Baden.
- [Is08] ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems Requirements Specification, ISO/IEC JTC1/SC27, 2008.
- [KRS08] Kersten, H., Reuter, J., Schröder, K.-W. 2008. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg, Wiesbaden.
- [La08] Langer, L., Schmidt, A., Buchmann, J. 2008. Secure and Practical Online Elections via Voting Service Provider. In *Proceedings of ICEG 2008*, 255-262. ACI.
- [RJ07] Reinhard, K.; Jung, W. 2007. Compliance of POLYAS with the BSI Protection Profile-Basic Requirements for Remote Electronic Voting Systems. In *VOTE-ID*, Lecture Notes in Computer Science vol. 4896, ed. A. Alkassar and M. Volkamer, 62-75. Springer.
- [Re07] Republic and Canton of Geneva State Chancellery. Report by the Geneva government to the Geneva parliament on the internet voting project. 2007. [http://www.ge.ch/evoting/english/doc/rapports/EN\\_RD\\_639\\_and\\_Annex.pdf/](http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf/).
- [Sc09a] Schmidt, A., Heinson, D., Langer, L., Opitz-Talidou, Z., Richter, P., Volkamer, M., Buchmann, J. 2009. Developing a legal framework for remote electronic voting. In *Proceedings of VOTE-ID 2009 Second international conference on E-voting and Identity, Luxembourg, LNCS 5767*, 92-105. Springer.
- [Sc09b] Schmidt, A., Volkamer, M., Langer, L., Buchmann, J. 2009. Towards the impact of the operational environment on the security of e-voting. In *Proceedings of INFORMATIK 2009, LNI 154*, 1814-1826. GI.
- [Tr09] Tranchard, S. 2009. The State of Geneva designs a secure Internet voting system. In *ISO Focus* 6:38-39.
- [VKG07] Volkamer, M., Krimmer, R., Grimm, R. 2007. Independent Audits of Remote Electronic Voting - Developing a Common Criteria Protection Profile. In *Proceedings of Elektronische Demokratie in Österreich - EDEM '07*, 115-126. Vienna: OCG Verlag.
- [VV08] Volkamer, M., Vogt, R. 2008. Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte. Common Criteria Protection Profile BSI-PP-0037. [https://www.bsi.bund.de/eln\\_156/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0037/](https://www.bsi.bund.de/eln_156/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0037/).
- [WVM07] Weldemariam, K., Villafiorita, A., Mattioli, A. 2007. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In *Proceedings of the First Conference on E-Voting and Identity (VOTE-ID), LNCS 4896*.

## **Session 5: End to End Verifiability and Protocol Improvements**



# Verifiability in Electronic Voting Explanations for Non Security Experts

Rojan Gharadaghy and Melanie Volkamer

CASED—Center for Advanced Security Research Darmstadt  
Technische Universität Darmstadt  
Mornewegstraße 32, 64293 Darmstadt  
Germany  
[rojan.gharadaghy, melanie.volkamer}@cased.de](mailto:{rojan.gharadaghy,melanie.volkamer}@cased.de)

**Abstract:** Scientists have requested verifiable electronic voting schemes for many years. These schemes offer individual and universal verifiability by applying and combining complex cryptographic primitives and protocols. Electronic voting systems in use provide less or even no verifiability. Thus election authorities and voters need to trust the provider and developer of the voting system regarding the integrity of the election. Due to arising critiques and the voting computer decision of the Federal Constitutional Court in Germany, the future electronic voting systems will probably need to implement verifiability. Therefore, this paper presents an overview and analysis of approaches to implement verifiability. We mainly address non-security experts like the average election authority and the average voter. Thus, the paper supports election authorities in their decision making process for a verifiable electronic voting system and the voter in making use of the verifiability.

## 1 Introduction

Electronic voting and in particular remote electronic voting offers many advantages compared to traditional paper based elections: like lower costs, faster tallying, improved accessibility and flexibility to the voter, greater accuracy of the result, lesser unintended invalid votes, and lower risk of human errors. However, an election can only profit from these advantages if the electronic voting system used ensures the four election principles of an equal, universal, secret, and free election. From an IT security point of view, these principles mainly mean that an electronic voting system has to ensure the secrecy of the vote and the integrity of the election result. Both must not be vulnerable to an outside attacker (i.e., hackers) nor to an inside attacker (i.e., developers, server/system hosts and administrators, and voters). Electronic voting systems used so far (e.g., in Estonia, the Netherlands, Austria, and Germany) have been evaluated by security experts. These evaluations mainly intended to check the system's robustness against outside threats while the election authorities and the voters have to trust that the developer and provider of the electronic voting system are not corrupt nor do they violate the election principles.

The problem is that once these systems are installed and the election is started, it is very difficult, if not impossible, to check whether the evaluated system and only this system is running<sup>1</sup> (for the entire voting period). As malicious providers could effect the system in several ways, (e.g., change the voting software undetected, log additional data, implement backdoors, change entries in databases in order to modify the election result or break the secrecy of the vote) verifiability mechanisms are necessary to run secure and trustworthy electronic elections. With these mechanisms voters and the public are able to audit the integrity of the election and thus the election result is ensured. Thus one can trust the provider, but the trust can also be audited. Note, even in traditional elections, trust in the people running the election (e.g., poll workers in the polling station) is not unlimited because observation in polling stations and other relevant places (e.g., central tallying) are allowed—sometimes required (compare [BWahlG, NRW]).

Due to the fact that (a) the trustworthiness of a system rises if the system implements verifiability in addition to a security evaluation [Vo09]; (b) critiques have increased against the so-called black box voting systems; and (c) the German Federal Constitutional Court demanded verifiability for (electronic) voting in its voting computer decision [BFG09], the future electronic voting systems will probably need to implement verifiability mechanisms. The decision for a particular verifiability electronic voting system is made by the election authority, and the verifiability mechanisms themselves need to be applied by voters and observers. The problem is that verifiability approaches are based on complex cryptographic primitives and protocols. These approaches are only understandable to those with a background in cryptography. This is not the case for the average election authority or voter. Therefore, this paper presents an overview and analysis of existing technologies to implement verifiability from a non-security expert perspective. A couple of “important to know” statements have been identified and are labeled correspondingly. We point out the advantages and disadvantages of different approaches. The paper supports election authorities in their decision making process for a verifiable electronic voting system. It further helps voters to understand the advantages and boundaries of verifiable voting systems as well as to apply verifiability mechanisms in a future electronic election.

The remaining part of this paper is structured as follows: First, in Section 2, we give a short introduction on verifiability in general. The focus of Section 3 is individual verifiability and how this can be realized, while Section 4 concentrates on different aspects of and different approaches for universal verifiability. Section 5 concludes this paper.

## 2 Verifiability

In the electronic voting literature, verifiability addresses the security requirement of the integrity of the election result. First of all, this means that it is possible for the voter to audit that his/her vote has been properly created (in general encrypted), stored, and

---

<sup>1</sup> Trusted computing techniques could help here, but would require special hardware and software at the voter’s PC. Therefore, these approaches cannot be applied to voting.



tallied (the so-called *individual verifiability*). Further, this means that everyone can audit the fact that only votes from eligible voters are stored in a ballot box, and that all stored votes are properly tallied (the so-called *universal verifiability*<sup>2</sup>) [La09]. Systems providing both forms are called End-to-End (E2E) verifiable [Be09].

**(Important to know 1)** Even with a verifiable electronic voting system, it is still possible for malicious providers and system developers to manipulate the (integrity of the) election result, but due to the verifiability, it will be detected. Thus it is not necessary anymore to trust them (regarding the integrity of the election result<sup>3</sup>).

**(Important to know 2)** It is not required that each voter makes use of the individual verifiability or that all voters, candidates, parties, and observers make use of the universal verifiability. As a malicious provider does not know who verifies his/her vote and who does not, the provider cannot manipulate single votes without being detected with a very high probability. Regarding universal verifiability, it would even be sufficient if one trustworthy entity verifies the tallying.

Implementing verifiability in general would be easy. For instance a doodle<sup>4</sup> poll is perfect verifiable as everyone can go to the doodle web page after having cast a vote and verify that the vote next to his/her name has not been altered. Further he/she can verify that the result is correct by tallying each vote next to the voters' names (if the corresponding person is eligible to vote). But, if an electronic voting system needs to ensure the secrecy of the vote (which a doodle poll does not), it is necessary to apply and combine complex cryptographic primitives and protocols<sup>5</sup>.

**(Important to know 3)** Even with these cryptographic techniques, it is not possible to provide unconditional<sup>6</sup> verifiability and unconditional secrecy of the vote at the same time. Protocols ensure either unconditional verifiability and computational<sup>7</sup> secrecy of the vote or vice versa (compare [Ad08]).

Bulletin Boards (BB) have been invented in order to implement verifiability in electronic voting (for both remote electronic voting and electronic voting devices). BBs are public broadcast channels like web pages in the Internet, which have special properties: Data is published only by authorized parties and, once published, cannot be deleted or modified anymore. Such a Bulletin Board can be accessed (with read access) by everyone for verifiability purposes—including the voter and the election authority. The Bulletin

---

<sup>2</sup> Other terms are public auditable or open audit [La09].

<sup>3</sup> Ideally, an electronic voting system would also provide the possibility to verify that the secrecy of the vote and maybe also other requirements are ensured (see [Vo09]). This is not covered in this paper.

<sup>4</sup> <http://www.doodle.com/>

<sup>5</sup> For electronic voting devices, it is also possible to realize verifiability without cryptography by using voter verifiable paper audit trails, printed by the devices and stored in a traditional ballot box. As the authors do not see a real benefit in these systems, this is not further addressed here.

<sup>6</sup> Unconditional means perfectly verifiable; even very powerful attackers cannot violate the integrity of the election result without been detected.

<sup>7</sup> Computational means that it depends on the solvability of a mathematical problem, which is classified as hard to solve. However, very powerful attacks would be able to break it. In general these problems are hard to solve today, but this might change in future.

Board contains and displays at least a list of cast votes (in encrypted form) together with voters' IDs or pseudonyms, and a couple of proofs used for verifiability (see Figure 1). The concrete content depends on the implemented verifiability approach. With the help of the Bulletin Board, verifiability can be done from any place at any time over the Internet—independent of whether the vote casting took place at an electronic voting system or over the Internet. Thus verifiability becomes possible for everyone not only those observing the process in the polling station. This is a main advantage compared to traditional paper based elections.

**(Important to know 4)** Bulletin Boards are a necessary concept to implement verifiability in electronic voting.

Verifiability can be achieved either “by hand” (by those who understand the underlying cryptography and are able to program their own verifiability) or by verifiability tools provided by independent institutes (for average voters and election authorities to run the verifiability). These could be downloadable or accessible through corresponding web pages. Moreover, the voter could also ask institutes like a university to run the verifiability on his/her behalf.

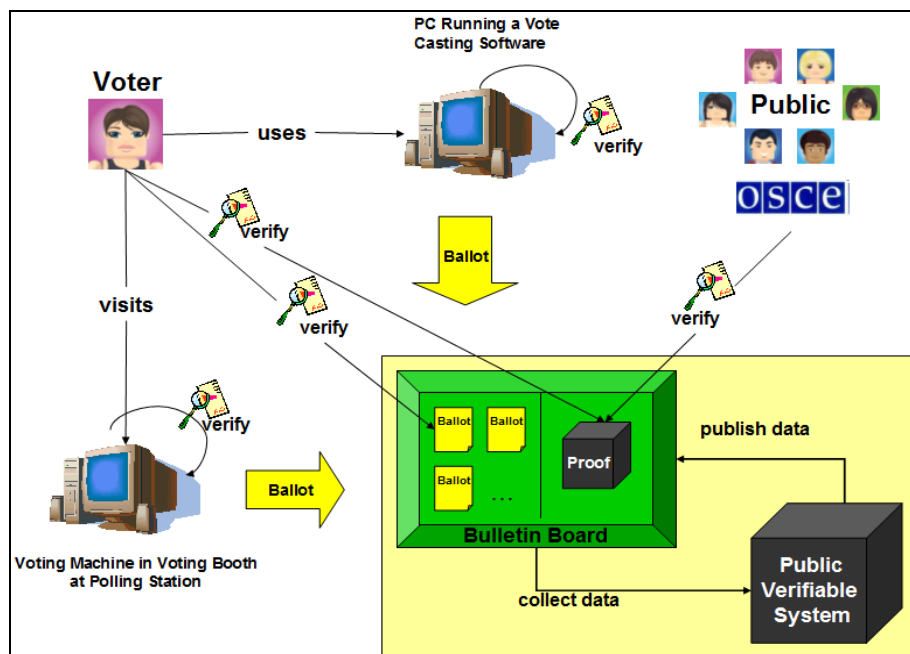


Figure 1: Overview on verifiability in electronic voting

**(Important to know 5)** Verifiability tools/software needs to be available from independent institutes so that the voter can choose the one he/she trusts.

## 2.1 Individual verifiability

Individual verifiability addresses the voter. The goal of individual verifiability is that the voter can verify that

- (a) his/her vote is properly encrypted (during vote casting), i.e., if he/she chooses candidate  $A$  then candidate  $A$  is also encrypted and not candidate  $B$  [cast as intended];
- (b) his/her encrypted vote is sent and stored unaltered at the Bulletin Board (after vote casting), i.e. if candidate  $A$  has been encrypted to  $enc(vote_A)$  then  $enc(vote_A)$  must appear on the Bulletin Board next to the voter's ID/pseudonym and not  $enc(vote_B)$  [stored as cast];
- (c) his/her encrypted vote is properly included in the election result (after tallying), i.e., in general properly decrypted and properly added to the other decrypted votes [tallied as stored].

Part (c) is only covered indirectly by universal verifiability. The idea is that if it is verifiable for all encrypted votes on the BB that they are properly included in the tally then this also holds for a particular vote [La09].

**(Important to know 4)** Individual verifiability ensures that the vote is cast as intended and stored (on the BB) as cast (part (a) and (b)).

**(Important to know 5)** Due to part (b), there exist a link between the voter/pseudonym and his/her encrypted vote on the Bulletin Board. Consequently, once the encryption scheme is broken the secrecy of the vote is violated, if there is a link between voter and encrypted vote.

## 2.2 Main idea and first approach

Implementing individual verifiability can be realized relatively easy in the following way: votes are encrypted probabilistic, that is, votes are concatenated with a random number and then encrypted<sup>8</sup>  $enc(vote\#R)$ <sup>10</sup>. In general, knowing the values  $vote$  and  $R$  means that it is possible to “decrypt” this term without the knowledge of the decryption key: just by encrypting the value  $vote\#R$  again and comparing the output with the encrypted term  $enc(vote\#R)$ . Based on this, the individual verifiability can be implemented in the following way:

- The voter uses an individual verifiability tool.
- This tool gets as input from the voting application the encrypted vote  $enc(vote\#R)$  and the random value  $R$  used for the encryption plus from the voter the value  $vote$ .
- This tool audits whether *the vote has been encrypted properly*.

---

<sup>8</sup> Public-key encryption is used, which means that a message is encrypted with the public key of the receiver, and the encrypted message can only be decrypted with the corresponding secret key, which is only known by the receiver.

<sup>9</sup> The symbol # is used for concatenations.

<sup>10</sup> Without this value  $R$  the encryption does not really protect the confidentiality of the vote as an attack could easily encrypts all possible votes and compares the output with  $enc(vote)$ .

- If this is the case, the encrypted vote is transferred to the Bulletin Board and stored.
- In order to later verify that the vote is properly stored on the BB, the random number is stored on the voter's PC.
- After having completed the vote casting, a voter can use the individual verifiability tool again to verify whether *his/her encrypted vote is properly stored* on the Bulletin Board.
- This time, the tool takes as input the stored random value  $R$  and from the voter, his/her choice and some personal information to identify the voter's entry on the BB.
- With this information the tool computes  $enc(vote\#R)$  and verifies whether this value is on the Bulletin Board. Note, both verifiability checks can be repeated with arbitrary individual verifiability tools.

The described approach provides unconditional individual verifiability. But, it violates the secrecy of the vote because it is not receipt-free<sup>11</sup>. A voter could use his/her knowledge of the randomness  $R$  as a receipt to prove to himself/herself that he/she cast his/her vote.

### 2.3 Advanced approach

In order to avoid such a receipt and thus be receipt-free, the above described mechanism for individual verifiability needs to be modified in the following way (see, e.g., [Ad09, Ad08]):

- Here, after the voting application has encrypted the vote, the voter needs to decide whether he/she wants to verify that the *vote has been properly encrypted* or whether the voter wants to cast the vote (which means the encrypted vote is sent to and stored on the Bulletin Board while the encrypted vote is stored on the voter's PC<sup>12</sup>).
- Only, if the voter decides to verify the encrypted vote, the random value  $R$  is revealed as input for the individual verifiability tool.
- If the voter decides to cast the vote, the value  $R$  is not revealed to ensure receipt-freeness.
- In this approach, the *second part* of the individual verifiability works as follows: The voter uses the individual verifiability tool again.
- This tool takes as input the stored encrypted vote and from the voter some personal information to identify his/her entry on the Bulletin Board. It verifies whether the encrypted vote appears on the BB.

The consequences for the individual verifiability in this approach are the following:

- [cast as intended] The voter cannot verify whether the cast encrypted vote contains his/her candidate choice. After having successfully verified a couple of (test) votes,

<sup>11</sup> Receipt-free means that the voter does not get a receipt to prove which candidate he/she chose.

<sup>12</sup> In this approach, the randomness  $R$  is neither leaked to the voter nor stored on his/her PC.

the voter has good evidence that his/her cast vote is also properly encrypted. The idea is that the voting application does not know how the voter will decide and thus does not know when (in case it would be malicious) to encrypt a different vote.

- [stored as cast] While in the previously described approach the voter could verify that the encrypted vote on the BB contains his/her candidate choice, in this approach he can only check whether the stored encrypted vote is properly stored on the Bulletin Board. However in combination with the evidence from the first part of the individual verifiability (cast/encrypted as intended), this is acceptable.

**(Important to know 6)** In order to verify that his/her vote is cast, the voter needs to verify his vote twice: once during vote casting and once after vote casting/after tallying. Thus there are two additional steps compared to black box voting systems if the voter wants to apply individual verifiability.

**(Important to know 7)** In order to provide receipt-freeness, a voter gets only evidence with high probability but no formal proof for the individual verifiability because the vote he/she finally cast cannot be verified, but only arbitrary votes before.

### 3 Universal verifiability

Universal verifiability is more complex than individual verifiability. At least two comparable (cryptographic) approaches exist. This section is structured into the following subsections: In the subsection 3.1, the main idea is proposed as well as its high level implementation and challenges in realizing it. The two main cryptographic approaches (one based on so called MIX networks and the other one based on the homomorphic property of encryption schemes) are introduced and explained in subsection 3.2.

#### 3.1 Idea and Challenges

After the voting period for each voter who cast a vote, a corresponding encrypted vote is stored and published on the Bulletin Board<sup>13</sup>.

**(Important to know 8)** The universal verifiability needs to ensure that all of these stored votes are properly tallied<sup>14</sup>. This usually also includes that the decryption is done properly.

The easiest way to implement universal verifiability would be to decrypt each vote on the Bulletin Board and publish all decrypted votes and the decryption/secret key. These data enable everyone to tally the votes him/herself or by using a universal verifiability tool and to verify that the votes are properly decrypted with the decryption/secret key. However, this would violate, in the worst case, the secrecy of the vote (if the encrypted

---

<sup>13</sup> Each encrypted vote can be unambiguously linked to a voter or his/her pseudonym. This is necessary to enable the individual verifiability.

<sup>14</sup> [Ry09] also recommends verifying that all votes are cast by eligible voters. We agree that this is necessary. However, due to time and space constraints this is not covered by universal verifiability in this paper.

votes are linked to the voters ID), and in any case, the system would not be receipt-free. Thus the Bulletin Board would contain either the information: *voter ID – encrypted vote – decrypted vote* or at least *voter’s pseudonym – encrypted vote – decrypted vote*. Obviously, it is challenging to compute the election result without violating the secrecy of the vote and being receipt-free. Therefore, one of the following two cryptographic techniques is applied to meet this challenge with corresponding cryptographic protocols (compare to [Sc08, Sm05])<sup>15</sup>:

- Cryptographers have developed encryptions schemes (so called homomorphic schemes), which allow the encrypted sum of all encrypted votes to be computed. Decrypting this sum is equal to the sum of all decrypted votes, i.e.,  $dec(enc(vote1) + enc(vote2) + \dots + enc(voten)) = dec(enc(vote1)) + dec(enc(vote2)) + \dots + dec(enc(voten))$ . The main advantage of this approach is that it is not necessary to decrypt single votes. The decryption/secret key is only used once to decrypt the result. Therefore, the secrecy of the vote is ensured at the same time (see also Figure 2 and compare to Section 3.2.1).
- The second approach is based on the idea that the encrypted votes are first anonymized and then decrypted. To do so, the encrypted votes are first of all separated from the voter’s ID/pseudonym. This set of encrypted votes is then anonymized by using a so called MIX net (compare to [Ch81]). A MIX net contains several nodes (so called MIX nodes which are general servers, running a particular software) while each MIX node takes as input the set of encrypted votes, shuffles this set and outputs a list of anonymized encrypted votes. This is done by each MIX node. Finally after shuffling the votes several times, the anonymized votes are decrypted and tallied. Several MIX nodes are used to increase the trust in the secrecy of the vote; although it is enough if one MIX node is trustworthy and anonymized the set of encrypted votes by shuffling the encrypted votes (see also Figure 3 and compare to Section 3.2.2).

**(Important to know 9)** Two different approaches are distinguished for a tallying procedure that ensures the secrecy of the vote: (a) Either only the encrypted sum is decrypted (while single votes are never decrypted) or (b) the encrypted votes are anonymized by randomized shuffling and only the anonymized votes are decrypted.

A *universal* verifiability tallying procedure needs to ensure the secrecy of the vote while providing proofs of the election result’s integrity, that is, proving that the tallying procedures ran appropriately. Thus proofs need to be created during the tallying. This makes the tallying more complex and also a little bit slower. Although it becomes more complex and involves more entities in the tallying, the robustness of the tallying needs to be ensured, i.e., running the tallying should not rely on single entities. No single (malicious) entity should be able to block the computation of the election result, e.g., by claiming to having lost the decryption/secret key.

---

<sup>15</sup> Actually in [Sm05], two more approaches are named. However, these are not very popular and thus not included in this paper. They are “heterodox schemes” and “schemes based on secret sharing among several mutually distrustful election authorities.”

**(Important to know 10)** A universal verifiability approach needs to ensure the secrecy of the vote and needs to be robust while providing proofs of the election result's integrity.

In order to get a universal verifiable voting scheme, it is necessary to extend the above described approaches (homomorphic encryption function / MIX nets) with corresponding proofs.

### 3.2 Two main approaches

The main idea of universal verifiability is to ensure that the tallying is done properly. Thus for both approaches, we explain what can go wrong in terms of where manipulations of the election results' integrity can occur and which techniques can be used to provide universal verifiability, i.e., make such manipulations detectable.

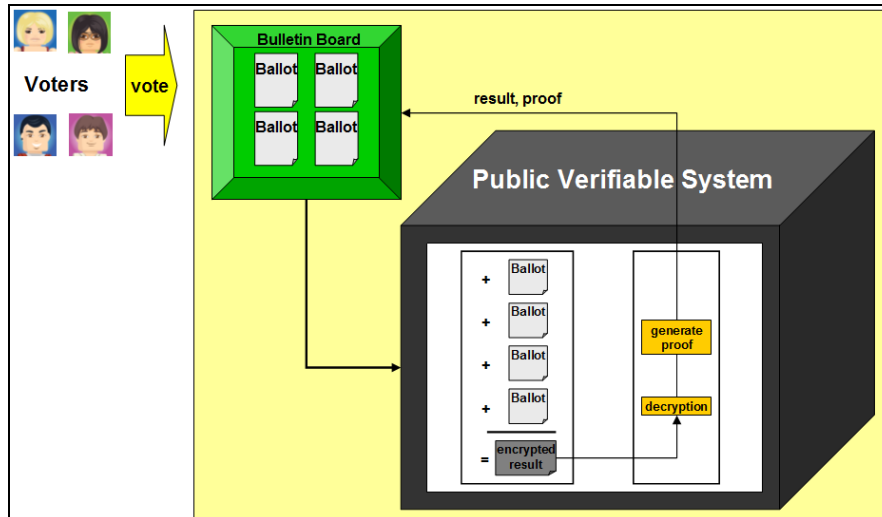
#### 3.2.1 Approach based on homomorphic encryption

In a universal verifiably scheme based on homomorphic encryption, the following two manipulations must be detectable with corresponding proofs:

- The system provides an arbitrary result as output for the decryption of the encrypted sum.
- The key holder(s) get the wrong decryption/secret key. This wrong key is used for decryption. The corresponding output is not equal to the sum of decrypted votes. Thus the integrity of the election result is not ensured.

Further, the robustness of the tallying procedure should not depend on the one key holder of the decryption/secret key.

To improve the robustness, the secret key is shared by several authorities with a so-called secret sharing scheme [Sh79]. This can be done in a way that  $k$  out of  $n$  authorities are already able to decrypt a message (in this scheme the encrypted sum of all votes). Thus if some authorities lose their key shares, the result can still be determined. To overcome the problem of the key holders receiving the wrong keys, so called verifiable secret sharing schemes are applied [Ch85]. Here it can be proven that the shares are properly distributed. Cryptographers also developed methods to prove that a message was properly decrypted without revealing the secret key (this is necessary to ensure the secrecy of the vote). One possibility of proving the correctness of a decryption is to use the Chaum-Pedersen protocol [CP92]. Using all three techniques the tallying is universal verifiable and at the same time proofs are provided in two situations: one after the key distribution and the other one with the decryption of the election result. Correspondingly, in both situations the proofs need to be verified. Moreover, it needs to be verified that the encrypted sum has been calculated correctly. An overview of the universal verifiability approach based on homomorphic encryption is shown in Figure 2.



**Figure 2:** Universal verifiability based on homomorphic encryption

### 3.2.2 MIX-based approach

In a universal verifiability scheme based on homomorphic encryption, the following three manipulations must be detectable:

- The output of a MIX node does not correspond to the shuffled input because encrypted votes have been modified. (1)
- The component finally decrypting the votes provides an arbitrary result for the decryption of each vote. (2)
- The key holder(s) got the wrong decryption/secret key. This key is used to decrypt votes. The corresponding output is not equal to the cast vote. (3)

Further, the robustness of the tallying procedure should not depend on the one key holder of the decryption/secret key and not on each MIX node. To increase the robustness of the MIX net so called re-encryption MIX nets are used. This means that arbitrary MIX nodes can fail and arbitrary new MIX nodes can be added to increase the trust in the secrecy of the vote. To increase the robustness with respect to the key holder and to ensure (2) and (3), the same techniques as for the homomorphic approach are used (namely: verifiable secret sharing and a proof of correct decryption). In addition, it needs to be ensured that each MIX node cannot manipulate the election result by altering the votes from the input to the output. To do so, cryptographers either use Zero Knowledge Proofs or Randomized Partial Checking [JJR02]. The first provides a real proof while the second approach only provides high evidence. However, the second approach is much more efficient than the first one.



Using all these techniques, the tallying is universal verifiable, and proofs/evidences are provided in three situations: (similar to the homomorphic approach) one after the key distribution and the other one with the decryption of the election result; plus the proofs/evidence provided by each MIX node. Correspondingly, in all three situations the proofs/evidence needs to be verified. The universal verifiability approach based on MIX nets is shown in Figure 3.

**(Important to know 11)** While there is less effort involved in the tallying and verifiability of homomorphic schemes, not all election schemes can be run using this approach because for some schemes (e.g., with write-in ballots) a corresponding homomorphic encryption scheme does not exist.

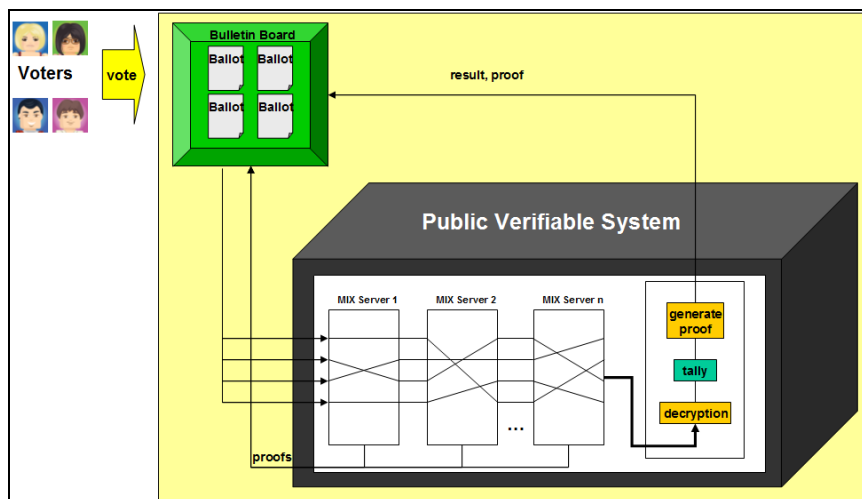


Figure 3: Universal verifiability based on a verifiable MIX net

## 4 Conclusion

Verifiability (both universal and individual) in electronic voting is becoming more and more important. After having discussed these techniques for years in the research community, this now needs to be implemented in future electronic voting schemes. Due to the fact that these techniques need to ensure the secrecy of the votes, the approaches are rather complicated and suffer from different constraints. The most important one is the theorem that an electronic voting system can either ensure unconditional secrecy or unconditional verifiability. Further, the election authority has to decide which verifiability approach they are in favor of.

This paper explains the different approaches from a high level perspective to also enable non-security experts to decide which technique to use and what its advantages and disadvantages are. Further, this paper addresses voters to help them understand what the advantages of verifiable voting schemes are and how to use them.

However, even if this paper helps to understand verifiability in the context of electronic voting, in order to use these techniques for legally binding elections, there are two open issues: First of all, the user friendliness has to be increased to enable average voters to use the verifiability mechanisms. Second, it is necessary to develop technical and/or organizational mechanisms and policies to handle those cases in which the result of any verifiability is negative.

## Bibliography

- [Ad08] Adida, B. 2008. Web-based open audit voting. In *Proceedings of the 17th symposium on security*, pp. 335–348. Berkeley, CA, USA: USENIX Association.
- [Ad09] Adida, B. et al. 2009. Electing a university President Using Open-Audit voting: analysis of real-world use of Helios. In *EVT'09. Proceedings of electronic voting technology workshop*. USENIX Association.
- [Be09] Benaloh, J. 2006. Simple verifiable elections. In *EVT'06. Proceedings of the USENIX/accurate electronic voting technology workshop*. Berkeley CA, USA: USENIX Association.
- [Ch81] Chaum, D.. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM 24, February, Nr. 2*, pp. 84–90..
- [CP92] Chaum, D. and T. P. Pedersen. 1992. Wallet databases with observers. In *CRYPTO, volume 740 of LNCS*, 89–105. Springer.
- [Ch85] Chor, B. et al. 1985. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *FOCS85*, pp. 383-395.
- [BWahlG] *Bundeswahlgesetz in der Fassung der Bekanntmachung vom 23. July 1993 (BGBl. I S. 1288, 1594), last change 17. March 2008 (BGBl. I S. 394).*
- [NRWO] *Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 – NRWO) BGBl. Nr. 471 idF BGBl. I Nr. 28/2007.*
- [BFG09] *BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1–163), Urteil des Zweiten Senats. [http://www.bverfg.de/entscheidungen/cs20090303\\_2bvc000307.html/](http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html/).*
- [JJR02] Jakobsson, M., A. Jueles, and R. L.Rivest. 2002. Making mix nets robust for electronic voting by randomized partial checking. In *Proceedings of the 11th symposium on security*, pp. 339–353. Berkeley, CA, USA: USENIX Association.
- [La09] Langer, L. et al. Unpublished. Towards a framework on the security requirements for electronic voting protocols. In *Post Proceedings of RE-Vote09*.
- [Ry09] Ryan. M. 2009. *Verifying electronic voting protocols in the applied pi calculus*. Slides presented at the 3rd workshop on security and electronic voting (VETO 09). [http://www-veto2009.imag.fr/Material/Mark\\_Ryan.pdf/](http://www-veto2009.imag.fr/Material/Mark_Ryan.pdf/).
- [Sc99] Schoenmakers, B. 1999. *A simple publicly verifiable secret sharing scheme and its application to electronic voting*. Technical report. Eindhoven, NL: Department of Mathematics and Computing Science, Eindhoven University of Technology.
- [Sc08] Schoenmakers, B. 2008. Voting schemes. Draft book chapter. To appear in *Algorithms and theory of computation handbook*, <http://www.win.tue.nl/~berry/papers/ChVotingSchemesJuly2008.pdf>
- [Sh79] Shamir, A. 1979. How to share a secret. *Communications of the ACM* 22 (11): 612–613.
- [Sm05] Smith, W. D. 2005. Cryptography meets voting. <http://www.math.temple.edu/~wds/homepage/cryptovot.pdf>
- [Vo09] Volkamer, M. et al. 2009. Elektronische Wahlen. Verifizierung vs. Zertifizierung. *Proceedings of INFORMATIK 2009, volume 154 of LNI*, 1827-1836. Bonn, Germany: Gesellschaft für Informatik.

# Verification Systems for Electronic Voting: A Survey

Jordi Pujol-Ahulló, Roger Jardí-Cedó, and Jordi Castellà-Roca

Departament d'Enginyeria Informàtica i Matemàtiques  
UNESCO Chair in Data Privacy  
Universitat Rovira i Virgili  
Av. Països Catalans 26  
E-43007 Tarragona, Spain  
[{firstname.lastname}@urv.cat](mailto:{firstname.lastname}@urv.cat)

**Abstract:** Voting is an important part of the democratic process. The electorate makes a decision or expresses an opinion that is accepted for everyone. Some parts could be interested in the election results deviation without anyone else noticing it. However, ensuring that the whole voting process is performed correctly and according to current rules and law is, then, even more important. We present in this work a review of existing verification systems for electronic voting systems, from both academia and the commercial world. To do so, we realize a fair comparison against a set of representative voting verification systems, by using an evaluation framework. We define this framework to be composed of several properties and covering important system areas, ranging from the user interaction to security issues. We then model the natural evolution of verifiability issues on electronic voting systems, which are influenced by restrictions on current laws and by technological advances.

## 1 Introduction

From the birth of democracy in Athens in sixth century BC and the first form of electoral laws, electoral systems have been designed and developed according to country particularities in democratic governments worldwide.

An election process consists of choosing a person or party, namely *candidate*, to represent all members of the community (e.g., a company, a state, or a country). For a candidate, winning an election represents a big responsibility, but it is also very attractive in many ways for other reasons (e.g., funds, ability to change existing rules and laws). Therefore, synergies could appear to deviate from election results to have a certain candidate (not) win.

However, it is a difficult task to check whether the election results correspond to the voters' preferences, since *votes are commonly private and anonymous*. That is, if voter Alice votes for candidate A, any another person must not know or extract Alice's preferences from the election process and results.

In other words, *elections must be verifiable*, even though voters' preferences are linked in no way to them. Therefore, *verifiability* comes to light as the most important election property to provide *trustfulness* to the election results to both candidates and voters.

Verifying that election results correspond to voters' preferences depends on the voting system. From a location viewpoint, most of the existing systems are based on *poll sites*, where voters go to specific places to vote. Remote voting systems (such as mail voting or lastly internet voting systems) are also an alternative.

From a ballot perspective, traditional voting systems use ballots in paper format. They were firstly introduced in the state of Victoria, Australia, in 1856 [Be10]. Paper ballots contain all the necessary information to vote for a specific candidate, in a human-readable format. Thus in the vote counting or *tally*, any person can verify whether the ballot is correct and, if so, to which candidate it is related to. However, the main drawbacks of traditional voting systems are that all operations are manual, as well as their high economic and logistic costs. In addition, the tally process where votes are counted can turn into a long procedure susceptible to human errors, especially when the voting system is complex.

More modern voting solutions incorporate electronic devices to mainly accelerate the tally process and overcome the problems induced by human errors, and also increment accessibility for disabled and illiterate voters. First initiatives appeared in 1964 in some states of the USA, which used punchcards and computer tally machines [Be10]. These kinds of solutions can use different technologies, ranging from punchcards, optical scanners (to scan ballots), to cryptographic techniques. Electronic voting (e-voting) systems thus pose other kinds of challenges to election *verifiability*, whilst at the same time ensuring voter privacy and anonymity.

To put all of this in words, we can differentiate three different types of *verifications*: *individual*, *universal* and *end-to-end*. Briefly speaking, *individual verification* permits voters to check that their individual ballots are correctly cast and counted.

From a system viewpoint, *universal verification* allows poll workers to inspect that the election results correspond to the cast ballots. The aim is to ensure that the whole voting process is performed correctly, what leads to *trustful* election results. In traditional voting systems, both verifications are achieved by a set of *procedures* (i.e., manual operations addressed by election officials, or also by independent entities and observers from candidates). Contrariwise, a mix of *procedures and technologies* usually addresses them in e-voting systems.

A later enhanced property is the *end-to-end (E2E) verifiability*. Seen from a voter's point of view, in an E2E verifiable voting system, a voter can check during the voting process that both her ballot is correctly cast and counted in the final tally. The goal is then to

increase the voters' *reliability* in the election results. Note that this property was hardly supportable in traditional voting systems, since the voter Alice concluded her interaction with the voting system when casting the ballot into the ballot box. However, new designs of voting systems and modern technologies facilitate an E2E voter-verifiable voting process.

In this survey, we present a fair comparison on the verifiability of electronic voting systems based on poll sites. We also name them *voting verification systems* (VVSs). The motivation is that poll-site-based voting systems are the most common ones nowadays. Besides, we specialize our study on e-voting systems since they are the most recent trend in democratic voting systems [Ev09]. The systems included in this analysis are remarkable commercial and academic solutions of the last decade. Thus the contribution of this work is twofold: (i) definition of a *common evaluation framework* to fairly compare all systems and (ii) *study and comparison* of remarkable e-voting systems.

**Document structure** The next section introduces the necessary background for the present work. Sec. 3 presents the evaluation framework and Sec. 4 the analysis of all voting verification systems (VVS). In Sec. 5, we perform the analysis of all the systems and pinpoint the technological trends. Finally, Sec. 6 presents the concluding remarks of this work and some future work.

## 2 Background

We consider in this study the standard voting process composed of the following phases: (i) *voter registration* and identification, (ii) *vote casting* using ballots and (iii) *vote tally*, where all ballots are securely *tabulated* and unbiased results are made *public*. The voting process also includes all *procedures* and *technologies* to trustfully address the consultations or elections. In addition, we present the system classification of the voting models and voting verification systems, according to the voting location and the U.S. HAVA classification, which will be used later in this work to organize the analyzed voting systems.

### 2.1 Voting models

We present two classifications of the voting models, according to the place where voters have to attend to vote (see Sec. 2.1.1), as well as according to the U.S. HAVA classification (see Sec. 2.1.2).

#### 2.1.1 Location-based classification

According to the place voters have to go to vote, voting systems are broadly classified into **poll-site-based** and **remote** voting systems. The former type is the most used nowadays, and it is characterized by having voters go to specific buildings, namely poll sites, to cast their votes. Conversely, voters may remotely cast their vote in *remote voting systems*. The most important examples are **vote-by-mail** and **internet voting**.

Recently, a new kind of systems has been proposed: **presential remote**. Such systems allow the casting of votes in a controlled environment (i.e., poll sites) although the tally is electronically conducted at a centralized site, dedicated to securely count all votes. Therefore, this kind of systems benefits from both existing modes, poll-site-based and remote, since they are very helpful when voters are abroad (e.g., the military), whilst at the same time reducing the tally time.

As mentioned earlier, our *focus* is put on *verification systems of poll-site-based systems*, which also allow us to take presential remote voting systems into consideration.

### 2.1.2 HAVA classification

This classification has been promulgated by the Election Assistance Commission (EAC), an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). Appendix C of the 2005 VVSG [E105] separates the VVSs into four types: (i) **process separation-based** VVSs have a modular architecture split into two independent, totally isolated systems dealing with the *generation* and *casting processes, respectively*; (ii) **evidence-based** VVSs are based on capturing *all actions* performed during the voting phase of voters; (iii) **direct** VVSs generate a *parallel* registry of votes, which permits a direct verification of the vote to be cast; lastly, (iv) **end-to-end cryptography-based** VVSs employ cryptographic methods to craft receipts which allow voters to verify that their votes were not modified, without revealing the voting preferences of the voters. We will classify the evaluated electronic VVSs using this classification system.

## 3 Common Evaluation Framework

In this section, we introduce the classification and properties that we will extract from the set of systems under consideration. All of them constitute the single, structured *evaluation framework* that we will use to ease their fair comparison and analysis.

### 3.1 Classification of VVSs

We employ the following classification to *percolate* the systems through, respectively, in order to obtain their natural organization. The publication year of the academic publication or system is the last organizational property used.

1. From **electronic-** and **paper-based systems**, we only consider electronic VVSs, which require voting in an *electronic* (instead of a *paper*) format.
2. We use the aforementioned **HAVA classification** to separate them into *process separation-*, *evidence-*, *end-to-end (E2E) cryptography-based* and *direct* VVSs.

3. We further organize them into **integral** or **independent systems**. *Integral* ones perform the whole voting process, while *independent* VVSs are designed solely to verify independently that another voting system's operations can be trusted.

### 3.2 Evaluated properties from VVSs

We present in this section the characteristics considered against which all systems are to be evaluated. We have classified them into these voting process concerns: *user interaction*, *security*, *integrability* (with an existing voting system), as well as *technical issues*. Note that any property definition is such that a *positive answer* corresponds to a *positive feature*.

**User interaction** The *user interaction* greatly determines the voters' impression and *reliability* of the voting system:

1. **Accessibility** Whether the system *does not* prevent a disabled user to vote.
2. **Use impact** Whether the system *does not* create a more complex (even longer) process to cast a vote.
3. **Reliability** Trust in the whole voting process from a *voter's viewpoint*.

**Security** The security issues are broadly categorized into these two big sets, namely *voter* and *voting process*:

#### **Voter-related:**

4. **Ballot secrecy** The system *prevents* a third entity from seeing the contents of the ballot.
5. **Voter anonymity** The system *prevents* the ballot from being linked to the voter.
6. **Coercion resistant** A coercer *cannot* verify nor demonstrate how the voter voted.
7. **Individual verification.** A voter *can* verify that her vote was accounted for *properly*.

**Voting-related:**

- **Universal verification:**

8. **Ballot box integrity** Only registered voters' votes *appear* at the end of the voting process (before the tally process) and are unmodified.
9. **Tally accuracy** The tally process *counts* all of the cast votes and not before the end of the voting process (i.e., no partial results are allowed).
10. **Auditability** The e-voting system (with no paper trails) *allows* a third party to analyze what happened before, during, and after the vote was cast, without compromising other security properties, in order to certify the final tally and election results.

**Integration** Regardless of whether the VVSs are *integral* or *independent*, we will consider the feasibility and effectiveness of adapting/integrating the evaluated system with other voting systems. In particular, briefly speaking, we consider the synchronization of operations, especially when votes are being cast, between a given voting system and the evaluated system *acting as an independent VVS* (as issued in [Sh06]).

11. **Integration** *Ease* of implementing/adapting the evaluated system as an independent verifier system for other voting infrastructures.
12. **Data management** Whether the vote cast subsystem of the voting systems and the evaluated system *guarantee* atomicity, as well as whether this integration is resistant to failures (e.g., user errors, cable disconnections).

**Technical issues** We also analyze the VVS performance from a *technical viewpoint*:

13. **Simplicity** Whether the verification solution *is* straightforward and simple.
14. **Availability** A suitable voter *must be able to* cast her vote, within the established time period, and be prevented from voting multiple times (if not otherwise allowed).
15. **Scalability** The verifier system computationally *scales*.
16. **Flexibility** This measures the level of freeness *allowed* by the verifier system (e.g., number of candidates, write-in mode).



**Properties representation** For brevity, when summarizing these sixteen properties for all the evaluated systems, we will use the following notation:

User interaction	↑/↓/~: Good/Weak/Acceptable.
Security	Y/N/~: Yes/No/Partially.
Integration	NT: No additional Technical requirements (on voting consoles, etc). T: Additional Technical requirements. NSW: No additional SoftWare requirements (on voting consoles, etc). SW: Additional SoftWare requirements.
Data management	NA: There is No operation Atomicity. A: There is operation Atomicity. DL: There is Data Loss. NDL: There is No Data Loss.
Technical Issues	↑/↓: High/Low
At any property	"N/A": When the property is <i>not addressed</i> .

**Table 1:** Value representation of the considered evaluation properties

## 4 Presentation and classification of VVSs

We present here all the evaluated *electronic VVSs*. The idea behind them is that they depend primarily on e-voting procedures, even though some of them may have paper *receipts* to provide E2E verifiability. From the HAVA classification, we present solutions on three out of the four types: *process separation-*, *evidence-*, and *end-to-end cryptography-based* (E2E).

### 4.1 Process separation-based VVSs

As we have presented before, a process-separated VVS is divided into two independent and isolated subsystems: *ballot generation* and *casting*. In this class of systems, the security constraints are mainly applied to the casting process. We present below the most representative one: Modular Voting Architecture, namely "Frog" [BJR01].

#### 4.1.1 Modular voting architecture ("Frog")

S. Bruck, D. Jefferson, and R. Rivest presented this system in 2001 [BJR01]. It is the example *par excellence* of separation process and, therefore, it implements an integral e-voting solution that emphasizes and standardizes a separation between vote *generation* and vote *casting* components.

On the day of the election, the voter identifies himself to a poll worker, who takes a blank *ballot* (ballots are named *frogs*), initializes it and, then, returns the ballot to the voter. Afterwards, the voter inserts his ballot into the *vote generation equipment*; she selects her options through a direct-recording electronic (DRE) voting machine, and her

choices are introduced onto her ballot. The second phase starts here. The voter introduces her ballot into the *vote-casting equipment* and *checks* the content of her ballot. When the voter agrees with the content, her ballot is digitally *signed* (using a single key for all votes), then *frozen* (the frog is blocked against writing), and finally *deposited* into the *frog bin*. At this moment, an electronic copy of her vote is randomly stored in a data unit memory and replicated in other memories for reliability. Once the elections are over, election officials publish the results for each precinct in a Web as two separated, unlinked lists: one with the voters' names and the second one with all cast ballots with a system-wide digital signature. Therefore, anyone can verify the digital signature and compute the election results.

## 4.2 Evidence-based VVSs

These systems capture the actions performed by voters when casting their votes, independently of the voting system and invisible by the voter. In addition, to ensure information integrity, all recorded events are stored outside of the vote terminal. Under this type of VVSs, we consider VVAATT and VVVAT.

### 4.2.1 Voter verified audio audit transcript trail (VVAATT)

VVAATT is an *audio verification* system, introduced by T.Selker and S.Cohen in 2004 [Se04, SC05]. This system records the *audio* of all events during the voting process into a physical medium (in a cassette tape or in a CD-W media), at the same time this is complemented by the *visual* verification from the DRE. In the same line, there exists Voter Verified Video Audit Trail (VVVAT), which instead, captures the sequence of screenshots on the DRE terminal (see [Cr07] for an example).

## 4.3 End-to-end verifiable VVSs

We present in this section the E2E cryptographic-based VVSs, which among other capital properties have an end-to-end (E2E) verifiability. To do so, some of them generate *paper receipts* to allow voters to check that their votes were counted in the tally process. The following solutions are the selected systems under analysis: VoteHere [Ne01], VoteBox [SDW08], Three-Ballot-Based Secure Electronic Voting System [SCM08], and the last ErgoGroup/Scytl proposal [No09b].

### 4.3.1 VoteHere

VoteHere is an integral solution introduced by C. Andrew Neff and VoteHere, Inc. in 2001 [Ne01, Va01]. This system is based on the use of DRE terminals. It is built considering receipt- and cryptography-based verifications in order to cover both *individual* and *universal* verifications.

For each voter, the voting system builds a *code* for each electable candidate before the election starts. Once the voter has chosen her preferences on the DRE, the DRE shows

the codes related to each candidate. If they correspond with those pre-built codes, the voter confirms her vote and a *receipt* is printed with her *verification codes*. Once the election ends, the *encrypted votes* are made publicly available (guaranteeing ballot secrecy), and then the voter can *check* if her vote was counted (or complain to election officials otherwise).

#### 4.3.2 VoteBox

VoteBox is an integral solution and was developed by D. Sandler, K. Derr, and D. Wallach in 2008 [SDW08]. The VoteBox system uses a technique adapted from Benaloh's work on voter-initiated auditing [Be07] to gain *end-to-end verifiability*. In other words, the voting system actually is an audit system that records everything that happened. Its main properties are as follows:

- **Pre-rendered user interface** The user interface is built from *pre-rendered* graphics, a closed sequence of pages (screens) containing text, and graphics that reduce runtime code size. The only interactive elements are buttons, rectangular regions of the screen (VoteBox supports touch screens), and other assistive technologies (computer mice, keyboards or audio feedback to state transitions).
- **Tamper-evidence and replication** A *permanent, tamper-evident* audit system records the events along the voting process and provides resistance to data loss in case of failure or tampering. VoteBox consists of two parts: the supervisor console and VoteBox booths (i.e., voting terminals). A broadcast network connects both parts, so that events from both parts (including ballot casts or supervisor commands) are replicated on all voting terminals and entangled with a hash chaining to provide *immutable* logs.
- **End-to-end verifiability** To encrypt ballots, VoteBox uses the ElGamal cryptosystem and its *additive homomorphic* property. Any cast ballot is encoded in a binary format and encrypted by a public key for the election. Therefore, the tally is addressed by (i) the multiplication of all ballots and (ii) the multiplication result decryption in order to obtain the election results.

#### 4.3.3 A three-ballot-based secure electronic voting system

This system [SCM08] is based on the original, paper-based Three-Ballot system [Ri06], but is completely redesigned to provide a full electronic solution. The idea behind the Three-Ballot approach is that a *ballot* consists of three single *parts*, with a list of candidates in the same order on the three parts. In order to vote for a candidate, the voters mark *any two parts* for the corresponding candidate (marking only one part means no vote is cast). When casting the vote, the three parts are separated from each other and mixed with the rest of parts from other voters. The tally operation is done by a simple calculation on the number of marks for each candidate on all the parts. One out of the three parts is randomly chosen by the voter to *copy* and to take home as a *receipt*. The same approach is maintained in this electronic version of Three-Ballot [SCM08].

#### 4.3.4 E-valg 2011

The Norwegian Ministry of Local Government and Regional Development initiated in 2008 a selection process of e-voting technological providers, which finished on December 2009. ErgoGroup<sup>1</sup> and Scytl<sup>2</sup> [No09b] will provide the e-voting solution for the Norwegian municipal elections in 2011 [No09c].

The ErgoGroup/Scytl's solutions provide all the security requirements by using cryptographic techniques. Until now, the ErgoGroup/Scytl consortium has designed various systems to support two types of voting: *poll-site-based* (compatible with DREs) [Sc04] and *remote voting* [PM07]. Moreover, the latter allows a presential remote voting model, which suits the system requirements specification of the E-valg 2011 project [No09d].

ErgoGroup/Scytl's proposal [No09b] is based on a *hybrid scheme* that combines mixing techniques and ElGamal homomorphic properties [Pe09]. The homomorphic cryptography uses a *multiplicative* property [Pe04, Pe09] so that the system performs partial multiplications of the votes. The election private key, used to open the encrypted votes, is generated using a *threshold scheme* [Sh79]. Lastly to retain all desirable security properties, this system uses digital signatures, zero knowledge proofs, and the generation of return codes (i.e., *receipts*).

## 5 Study and comparison of VVSs

In this section we introduce the analysis of the considered VVSs (Sec. 5.1) and the study of the synergies on voting systems and cryptographic technologies (Sec. 5.2).

### 5.1 Analysis and comparison of VVSs

We follow the properties considered in our common evaluation framework to compare and analyze all evaluated VVSs. See Tab. 3 for the complete elaboration.

**User interaction** Given that all VVSs use DREs to emit votes, all of them provide a certain degree of **accessibility**. However, some of them improve it by using audio guides (VVAATT), or indeed with other assistive technologies (such as mice or keyboards) (VoteBox and E-valg). For the E-valg case, this is proved by the studies [Sh06], [No09a]. As for the **use impact**, systems like Frog, VoteBox and Three-Ballot present a more complex and likely longer voting process. For instance, in Frog there exists a strict separation of the generation and cast processes (even though a voter can bring a filled ballot from home); VoteBox allows voters to perform an "immediate ballot challenge" [Be07]; and Three-Ballot uses a multi-ballot composed of 3 parts. Further, in order to increase the **reliability** of the voting system, they provide three kinds of augmented features: (i) frogs (Frog) and *receipts* (VoteHere, VoteBox, Three-Ballot and E-valg)

---

<sup>1</sup> <http://www.ergogroup.no/default.aspx?path={2A1C0F50-F200-43C8-98C6-36CD82F7A587}>

<sup>2</sup> <http://www.scytl.es>

tangible elements for the voter, (ii) audio guides (VVAATT), and (iii) public web bulletins (all except VVAATT).

**Security** VVAATT/VVVAT do not ensure vote confidentiality, given that all (audio or video) recordings show the *sequential* voting order. In addition, VVAATT/VVVAT suffer from *weak* recording equipment protection (given that they must be accessed often) and *untrustworthy* information extraction techniques. In conclusion, even though the recording support provides audit means, VVAATT/VVVAT are not reliable. Next, we only will focus on the rest of the systems.

**Voter-related security** Except for Frog, all of the systems use a public key infrastructure (PKI), most of them ElGamal, to ensure **ballot secrecy**. However, these VVSs use very different techniques to guarantee **voter anonymity**. While Frog uses a simple randomization algorithm, Three-Ballot separates each of the three parts of a ballot and stores them using their hash values. More complex techniques also appear: mixing (VoteHere), additive homomorphism (VoteBox) or a hybrid scheme (multiplicative homomorphism and mixing in E-valg). VoteBox, Three-Ballot and E-valg are **resistant to coercion and vote selling**. The same is not true for VoteHere, since it may have a flaw given that it shows both encrypted ballots and receipts with return codes [Ba04]. Lastly, except for Frog, all systems render *augmented individual verification* with *E2E voter verifiability* through receipts.

		Security Techniques			
		ZKPs	Digital Signatures	Threshold Scheme	Audit System
VVS	Frog	No	Yes	No	No
	VoteHere	Yes	Yes	Yes	No
	VoteBox	Yes	Yes	Yes	Yes
	Three-Ballot	No	Yes	No	No
	E-valg	Yes	Yes	Yes	Yes

**Table 2:** Security techniques used by voting verification systems

**Voting-related security** Except for Frog, all of the systems ensure **ballot box integrity** through different technologies (like ZKPs, digital signatures or threshold schemes). The use of a threshold scheme prevents security attacks against the electoral system. See Tab. 2 for more details. Thus, VoteHere, VoteBox, Three-Ballot and E-valg guarantee **tally accuracy**. Homomorphic algorithms make a more efficient tally than mixing techniques [Pe04, Pe09]. As for **auditability**, Three-Ballot creates logs for any voter-related operation, even though it creates none about the tally process. The evaluated strongest audit systems appear in VoteBox and E-valg, which use *immutable* logs. VoteBox, however, builds a distributed total audit system, while E-valg only centrally audits the critical system elements.

**Integration** In order to be **integrated**, the evaluated VVSs have some software or technological dependences (see Tab. 3 for more details). However, only VoteBox and E-valg [Sh06] ensure vote atomicity, loss resistant, and tamper evident solutions.

**Technical issues** VoteBox and Frog are more **complex** than the rest of the systems, given that the former has a distributed infrastructure, and the latter is strictly tied to the separation of processes. However, VoteBox is the only system that structurally provides distributed *replication* of sensible information, which leads to a high degree of system **availability**. Another of VoteBox's good properties is its **scalability**, given that it uses homomorphic cryptography, and thus makes the tally process easier. This property is also shared by E-valg. However, both of them should carefully address presential remote voting, guaranteeing the necessary infrastructure in order not to overload the voting system. Finally, only Frog, VoteHere and E-valg render **flexible** on vote type and format. Notice that VoteBox, by using additive homomorphic cryptography, only supports simple types of votes. Lastly, Three-Ballot is only suitable for multi-ballot formats composed of 3 single parts, even though that the ballot content is flexible.

## 5.2 Study of trends in VVSs

From the above analysis we can extract *three clear trends* in regard to the following issues: (i) voting location, (ii) voting technology, and (iii) degree of verifiability.

**Voting location study** We have evaluated *poll-site-based* VVSs. All of them use DREs as voting terminals. Clearly, DREs are very helpful in order to manage votes electronically. It is worth noting the demonstrated trend away from *poll-site-based* toward presential remote voting systems. For instance, VVAATT/VVVAT, Frog, VoteHere and Three-Ballot are of the first type, and VoteBox and E-valg are presential remote voting systems. This trend is a consequence of not only the technology, but also the natural evolution in the democratic rules. However while VoteBox was *adapted* to support presential remote voting schemes, E-valg was *structurally* designed to do so.

**Voting technology study** We consider here the voting technology used from the ballot cast to the tally and, therefore, VVAATT/VVVAT-based systems are not considered. The idea behind this technology is to address security issues such as voter anonymity, ballot box integrity, and tally accuracy among others. These systems present a clear evolution in this issue. We detail them from simpler to more complex and reliable solutions.

While Frog uses only a simple *randomization* algorithm to anonymize votes, VoteHere uses a more reliable mixing technique to address *voter anonymity*. VoteBox and Three-Ballot use (computationally hard) *additive homomorphic* cryptography to guarantee *voter anonymity* and to perform the *tally*. The most complex, but flexible and reliable technology is used by E-valg, the *hybrid scheme*, which is composed of multiplicative homomorphic cryptography (computationally less hard than additive ones [Pe04, Pe09]) and mixing mechanisms. Clearly, the technology used presents a *trade-off* between ensuring (i) more secure, trustful, and reliable voting technologies, and at the same time guaranteeing (ii) fast and resource-efficient ones. This trend from simple randomization techniques to hybrid schemes is a direct consequence of the continuous permeability of voting systems with regard to the latest cryptographic advances.

**Verifiability study** We can organize the analyzed systems as follows: (i) VVAATT/VVAT-based and Frog systems provide deficient or basic verifiability in voting processes, respectively. They mainly guarantee at some degree the individual verifiability, yet the same is not true for universal or E2E verifiability. (ii) VoteHere and Three-Ballot VVSs offer an acceptable degree of verifiability (individual, universal, and E2E). Finally, (iii) E-valg and VoteBox ensure a good level of verifiability, while at the same time they define a tough audit system. To sum up from all of these remarkable VVSs, VoteBox and E-valg are the best alternatives for voting systems. However, E-valg is a better voting system candidate, which should be followed closely. This is because it provides commercial applications, a high degree of verifiability, and a smooth transition from traditional voting systems to electronic ones, not to mention its accessibility and ease-of-use.

VVS	USER INTER.			SECURITY							INTEGR.		TECHNICAL ISSUES			
	Accessibility	Use Impact	Reliability	VOTER-RELATED				VOTING-RELATED			Integration	Data Management	Simplicity	Availability	Scalability	Flexibility
				Ballot Secrecy	Voter Anonymity	Coercion Resistant	Individual Verification	UNIVERSAL VERIFICATION		Audability						
								Ballot Box Integrity	Tally Accuracy							
Frog	↓	~	↑	N	Y	N	~	~	N	N	SW/T	N/A	↓	N/A	↓	↑
VVAATT	~	↑	↑	N	N	N	N	N	N	~	T	DL/NA	↑	N/A	↓	↓
Vote Here	↓	↑	↑	Y	Y	N	Y	Y	Y	N	SW	N/A	↑	N/A	~	↑
Vote Box	↑	↓	↑	Y	Y	Y	Y	Y	Y	Y	SW/T	N/DL/A	↓	↑	↑	↓
Three-Ballot	N/A	↓	↑	Y	Y	Y	Y	Y	Y	Y	N/A	N/A	↑	N/A	~	↓
E-valg	↑	↑	↑	Y	Y	Y	Y	Y	Y	Y	N/A	N/DL/A	↑	N/A	↑	↑

**Table 3:** Detailed properties of the Voting Verification Systems.

## 6 Conclusions

In this paper, we have presented an evaluation framework, common for all systems, in order to conduct a fair study of the different electronic voting verification systems (VVSs). The strong point of the present study is threefold: (i) we define the common evaluation framework, (ii) we present academic and commercial VVSs, and (iii) we conduct a fair study and comparison among them, having the verifiability analysis as a connecting thread.

Even though the origin of e-voting systems was to accelerate the tally process, the trend is clear and firm towards not only electronic tally, but also electronic vote casting

[Ba06]. Since the introduction of the DREs, more and more initiatives are addressing electronic casting in elections. This trend is also visible in our study.

As we have seen, good designs of e-voting systems may be significantly helpful for disabled and also for illiterate citizens. At the same time, the use of electronic voting technologies may reduce the economic and logistic costs of elections and consultations, while facilitating geographically distributed citizens to vote. Even though there are no conclusive studies, the tally accuracy on e-voting systems is higher than in paper-based voting systems [Ba06]. However, e-voting systems should not be massively introduced – education and increasing the sensibility toward democracy is necessary beforehand– in a society where there exists a high ratio of abstention.

As demonstrated by the technologies used in the latest e-voting systems, we foresee that the future trend in the use of electronic voting will be *remote e-voting*. In this line, there were some first *remote presential* and *internet voting* experiences. The global acceptance of these remote e-voting schemes will empower citizens with new democratic participation tools, which will likely lead to direct and binding citizen consultations and elections.

## Bibliography

- [Ba04] Barnes, Richard. 2004. VoteHere VHTi. A verifiable e-voting protocol. Cryptography applications bistro. <http://www.cs.virginia.edu/crab/VoteHere.pdf/>. (accessed Feb. 2010).
- [Ba06] Barrat Esteve, Jordi. 2006. A preliminary question. Is e-voting actually useful for our democratic institutions? What do we need it for? In *Proc. of 2nd international conference on electronic voting (E-VOTE '06)*, 51–60. GI, Bregenz, Austria.
- [Be10] Bellis, Mary. 3<sup>rd</sup> November 2009. The history of voting machines. <http://inventors.about.com/library/weekly/aa111300b.htm/>. (accessed Feb. 2010).
- [Be07] Benaloh, Josh. 2007. Ballot casting assurance via voter-initiated poll station auditing. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07)*, 14–14, Berkeley, CA, USA: USENIX Association.
- [BJR01] Bruck, Shuki, David Jefferson, and Ronald Rivest. 2001. *A modular voting architecture ("Frogs")*. In *Proceedings of the Workshop on Trustworthy Elections (WOTE '01)*, California, USA. URL: <http://vote.caltech.edu/backup/wote01/pdfs/amva.pdf>
- [Cr07] Cross, E.V., G. Rogers, J. McClendon, W. Mitchell, K. Rouse, P. Gupta, P. Williams, I. Mkpog-Ruffin, Y. McMillian, E. Neely, J. Lane, H. Blunt, and J.E. Gilbert. 2007. Prime III: One machine, one vote for everyone. In *(On-line) proceedings of 2007 voting competition conference*. <http://vocomp.org/papers/primeIII.pdf/>. (accessed Feb. 2010)
- [El05] Election Assistance Commission (USA). 2005. Voluntary voting system guidelines. [http://www.eac.gov/voting%20systems/docs/vvsgvolume1.pdf/attachment\\_download/file/](http://www.eac.gov/voting%20systems/docs/vvsgvolume1.pdf/attachment_download/file/).
- [Ev09] E-voting.cc (competence center for electronic voting and participation). 2009. Map of electronic democracy. *Modern Democracy* 2(1):8–9.
- [Ne01] Neff, C. Andrew. 2001. A verifiable secret shuffle and its application to e-voting. In *CCS '01. Proceedings of the 8th ACM conference on computer and communications security*, 116–125. New York, NY, USA: ACM.



- [No09a] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Accessibility and usability evaluation of e-vote prototypes. [http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e\\_valg\\_system\\_losning/report\\_evoting\\_usability\\_accessibility\\_eval\\_nr\\_iter2\\_final.pdf/](http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_system_losning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf/). (accessed Feb. 2010).
- [No09b] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Contractor solution specification. [http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e\\_valg\\_systemlosning/Tilbud\\_ergogroup/SSA-U\\_Appendix\\_2A\\_Contractor\\_Solution\\_Specification.pdf/](http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_ergogroup/SSA-U_Appendix_2A_Contractor_Solution_Specification.pdf/). (accessed Feb. 2010).
- [No09c] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Project directive for e-valg 2011. [http://www.regjeringen.no/upload/KRD/Vedlegg/KOMM/Evalg/Project\\_directive\\_evalg2011\\_v101\\_english.pdf/](http://www.regjeringen.no/upload/KRD/Vedlegg/KOMM/Evalg/Project_directive_evalg2011_v101_english.pdf/). (accessed Feb. 2010).
- [No09d] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. System requirements specification. [http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System\\_Requirements\\_Specification1.pdf/](http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf/). (accessed Feb. 2010).
- [Pe04] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee. 2004. Multiplicative homomorphic e-voting. In *Proceedings of 5th international conference on cryptology in India (INDOCRYPT '04)*, 61–72. Kolkata, India. Springer.
- [Pe09] Peng, Kun. 2009. A hybrid e-voting scheme. In *Proceedings of the 5th international conference on information security practice and experience (ISPEC '09)*, 195–206, Berlin, Heidelberg: Springer-Verlag.
- [PM07] Puiggali, Jordi, and Vitor Morales-Rocha. 2007. Independent voter verifiability for remote electronic voting. In *Proceedings of international conference on security and cryptography (SECRYPT '07)*, 333–336. Barcelona, Spain. Springer.
- [Ri06] Rivest, Ronald L. 2006. The three-ballot voting system. Unpublished draft.
- [Sc04] Scytl Online World Security S. A. 2004. Auditability and voter verifiability for electronic voting terminals. [http://www.scytl.com/a\\_home/PNYX.VM\\_White\\_Paper.pdf](http://www.scytl.com/a_home/PNYX.VM_White_Paper.pdf). (accessed Feb. 2010).
- [SC05] Selker, Ted, and Sharon Cohen. 2005. An active approach to voting verification. [http://vote.caltech.edu/drupal/files/working\\_paper/vtp\\_wp28.pdf](http://vote.caltech.edu/drupal/files/working_paper/vtp_wp28.pdf). (accessed Feb. 2010).
- [SCM08] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. 2008. A three-ballot-based secure electronic voting system. *IEEE Security and Privacy* 6(3):14–21.
- [SDW08] Sandler, Daniel, Kyle Derr, and Dan S. Wallach. 2008. Votebox. A tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th conference on security symposium (SS'08)*, 349–364. Berkeley, CA, USA: USENIX Association.
- [Se04] Selker, Ted. 2004. The voter verified audio audit transcript trail. [http://www.dos.state.pa.us/election\\_reform/lib/election\\_reform/VVAATT\\_CalTech.pdf](http://www.dos.state.pa.us/election_reform/lib/election_reform/VVAATT_CalTech.pdf). (accessed Feb. 2010).
- [Sh79] Shamir, Adi. 1979. How to share a secret. *Commun. ACM* 22(11):612–613.
- [Sh06] Sherman, Alan T., Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, Donald F. Norris, John Pinkston, Andrew Sears, and Dongsong Zhang. 2006. An examination of vote verification technologies: findings and experiences from the Maryland study. In *Proceedings of the USENIX/accurate electronic voting technology workshop 2006 on electronic voting technology workshop (EVT'06)*, 10–10. Berkeley, CA, USA: USENIX Association.
- [Va01] Varner, Philip E. 2001. Vote early, vote often, and vote here. A security analysis of VoteHere. PhD diss., University of Virginia.



# Sigma Ballots

Stefan Popoveniuc<sup>1</sup> and Andrew Regenscheid<sup>2</sup>

<sup>1</sup>KT Consulting  
Gaithersburg, MD, USA  
[stefan@popoveniuc.com](mailto:stefan@popoveniuc.com)

<sup>2</sup>Computer Security Division  
National Institute of Standards and Technology  
100 Bureau Drive  
Gaithersburg, MD, USA.  
[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)

**Abstract:** We present Sigma ballots, a new type of ballot designed to be used in secure elections. Sigma ballots use the random order of candidates introduced by Prêt à Voter, combined with the confirmation codes of Scantegrity II. These ballots can be produced by a DRE machine with a slightly modified VVPAT, or can be similar to optical scan ballots. Sigma ballots work in conjunction with existing publicly verifiable tallying schemes to allow for end-to-end verifiability. The advantages of Sigma ballots include an easy check for correct printing, the possibility of keeping a fixed order of candidates when selections are made, automated creation of receipts, no extra marks added to the ballot after it is cast, the ability to be hand counted, and voters only needing to know a valid confirmation code to file a complaint.

## 1 Introduction

A new class of voting systems was developed in the last couple of years which allows for a unique level of public scrutiny of the declared totals. These systems, known as *end-to-end verifiable voting systems*, allow voters to check that their ballots were cast and recorded as they intended, and allow anyone to check that all the recorded ballots have been correctly tallied. They offer security properties radically different from any voting system used in elections today.

While, in theory, many end-to-end verifiable voting systems have great properties, in practice, they suffer from known weaknesses. Some of them may be difficult to use by voters [PH06], others may be difficult to implement in practice [CD04], some may be too slow for very large elections [CRS05], while others may be vulnerable to attack [CD08].

Recently, binding elections have been run using end-to-end verifiable systems [EA07, AB09]. Scantegrity II [CD08] has been used in a public election, to elect the mayor and city council of Takoma Park, MD. While Scantegrity II has many desirable security properties, it suffers from a series of problems, many of them being acknowledged after the Takoma Park election.

In this paper, we present Sigma ballots, a new type of ballot which can be used in conjunction with existing publicly verifiable tallying schemes to create end-to-end verifiable voting systems that are not vulnerable to many attacks faced by existing systems.

### 1.1 Motivation and Related Work

A number of end-to-end verifiable voting systems have been proposed [EA07, AB09, CD08, AR06, CRS05]. Many of these systems have known vulnerabilities.

A well-known attack on Scantegrity II is to misprint the ballots. For example, if we assume that a certain voter is going to vote for Alice, but the inside attacker is a supporter of Bob, then the attacker may print next to Alice the confirmation code that corresponds to Bob. The voter fills in the oval next to Alice's name and gets a confirmation code that she thinks is for Alice, when in fact it is for Bob. The tallying mechanism is going to correctly transform this confirmation code into a vote for Bob. This attack is possible because voters are not able to directly distinguish improperly printed Scantegrity II ballots from correctly printed ones.

The typical way of mitigating this attack is to allow the voter to choose two ballots, one to vote, and one to spoil and audit the printing on it. This approach is theoretically sound, but in practice there are multiple disadvantages. First, the approach adds time and complexity to the voting process. Second, voters need to take the fully marked ballots home, and check them against the data on a bulletin board. This potentially violates current election practices, as ballot accounting procedures in many jurisdictions prevent voters from leaving the polling place with a ballot, even spoiled ballots. Third, the approach is highly dependent on procedures followed both by the voter and election officials [KJ07].

Another option is to have a designated auditor that comes and chooses a random set of ballots to be audited for correct printing. This solution requires a trusted auditor, as well as a secure chain of custody for the audited ballots.

The same print audit problem exists in other voting systems, e.g., Prêt à Voter [CRS05], Scratch&Vote [AR06], or, more generally, voting systems in which the ballot does not consist of two or more symmetrical parts, such as PunchScan [PH06].

Another issue with Scantegrity II is that voters are asked to create their receipts by hand. They have to write down the serial number of the ballot along with the confirmation codes for each ballot question. This task can be time consuming and error-prone.

A third security problem identified with Scantegrity II is the possibility of the voting system transforming a no-vote into a valid vote, or a valid vote into an over-vote, by adding extra marks to the ballot after it was cast. Since the voter cannot prove that she does not know the codes for the marks she did not make, the voter cannot prove that she was not the one that made the marks which were in fact added by the system afterwards. This security issue is unique to end-to-end verifiable voting systems where the voting receipt is a proof of knowledge, rather than a partial copy of a cast ballot.

## **1.2 Contribution**

This paper presents Sigma ballots, a new type of ballot to be used to create secure voting systems. Sigma ballots use the random order of candidates introduced by Prêt à Voter, combined with the confirmation codes of Scantegrity II. These ballots can be produced by a DRE machine with a slightly modified Voter Verifiable Paper Audit Trail (VVPAT) printer, or can be similar to optical scan ballots. For illustration purposes this paper provides an example (see section 5) for how to implement verifiable ballot tallying using techniques from Scantegrity II [CD08].

Similar to PunchScan, but without suffering from its indirection problems, the proposed Sigma ballots are two parts symmetrical ballots, with any of the parts containing the same amount of information. The voter may use any of the parts to check for correct printing, without being able to prove how she voted.

Sigma ballots can be used to automatically create a receipt, without the voter needing to write down anything by hand.

Sigma ballots also solve the problem of improperly invalidating cast ballots by giving the voter a digitally signed receipt, covering all and only the selection on the voter's ballot. The voter can now prove that extra marks have been added to her ballot after it was cast by presenting her signed receipt.

## **2 Description of Sigma ballots**

We start by describing what a Sigma ballot looks like. In section 3, we detail how the Sigma ballot can be created using either a DRE with a VVPAT printer, or an optical scan system.

The design of the Sigma ballot uses ideas from the Prêt à Voter ballot and the Scantegrity II confirmation codes. Sigma ballots are filled-in ballots, clear text, with marks next to the candidates the voter selected. Voters can inspect a Sigma ballot to verify that their choices are correctly represented, by checking the names next to the marks. Also, Sigma ballots can be counted by hand.

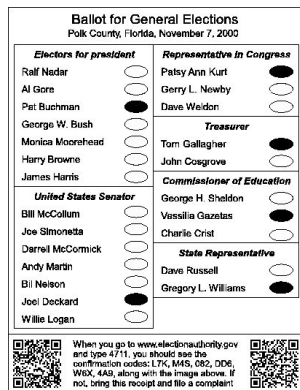
Figure 1 shows a Sigma ballot. On the left side of the ballot is a list of candidates, in a permuted order on each ballot<sup>1</sup>. The order of the candidates on each ballot is publicly committed to before the election and may be different for different ballots. On the right, there is a mark for each candidate the voter selected.

The voter can check that the marks appear only next to the candidates she voted for. If not, the voter can start creating another Sigma ballot (no harm was done). This check is similar to asking the voter to verify that the Voter Verified Paper Audit Trail (VVPAT) contains her choice in a DRE+VVPAT system.

Each mark that appears next to the candidates has a confirmation code assigned to it. All the confirmation codes are printed at the bottom of the ballot. A public commitment ties the confirmation code to the marks next to the candidates, i.e., to the position where marks appear at.

Instructions are printed at the bottom of the ballot about how the voter can check that her vote was correctly recorded. There are also two bar codes containing digital signatures. One signature covers the confirmation codes and the order of the candidates (the left side); the other covers the confirmation codes and the position where marks appear at (the right side).

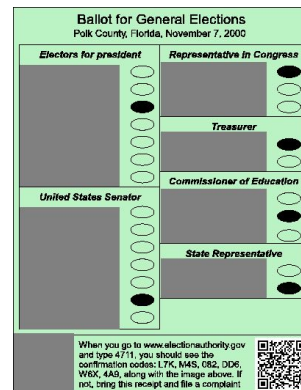
Like in Scantegrity II, the voter only sees the confirmation codes for the candidates she selected, creating a knowledge-based receipt. If the voter notices that her confirmation codes are not correctly posted on the public bulletin board, knowledge of a valid confirmation codes is sufficient to file a complaint.



**Figure 1:** A Sigma ballot. The order in which the candidates are printed may be different on different ballots. The confirmation codes are not associated with candidates or marks.



**Figure 2:** Receipt produced by photocopier 1. The order of the candidates is visible, but no marks are visible, so an observer cannot tell how the voter voted.



**Figure 3:** Receipt produced by photocopier 2. The marks are visible, but the order of the candidates is hidden, so an observer cannot say which candidates the marks correspond to.

<sup>1</sup> The name “Sigma ballot” comes from having a permutation represented by the Greek letter  $\sigma$ .

There are two photocopiers in the polling place, which are used to produce a receipt from a Sigma ballot. On her way out, the voter may choose one of the two photocopiers and place her ballot in it. The scanning portion of the photocopiers is partially blackened out by an opaque template (i.e., black tape), such that, for the first photocopier, the template hides (i.e., does not allow to be copied) the portion with the marks (Figure 2). For the second photocopier, the template hides the portion with the order of the candidates (Figure 3). The copy produced by the photocopier becomes the voter's receipt, while the Sigma ballot is deposited into a ballot box.

If the voter chooses the first photocopier, she obtains the order in which the candidates appeared on the voted ballot along with the confirmation codes (see Figure 2). Since no marks for any of the candidates are visible, and since the confirmation codes may be different for different ballots, inspecting this receipt does not reveal the choices the voter made. If the voter chooses the second photocopier, the voter obtains the position of the marks along with the confirmation codes (see Figure 3). Since the order of the candidates may be different on different ballots, the positions where the marks appear do not reveal the chosen candidates. Therefore, no matter which photocopier the voter uses, she gets a receipt that does not reveal how she voted.

The bar code at the bottom of the ballot contains a digital signature of the receipt to avoid voters being able to manufacture fake receipts, and to avoid having the system adding more marks after the ballot is cast. The verification of the correctness of the digital signature is part of future work.

To simplify things, two digital signatures are on the initial Sigma ballot. Depending on which photocopier is used, one of them is covered, such that the receipt only contains the appropriate digital signature.

All the receipts are posted on a public bulletin board and the voter may check it and compare her receipt to the posted one. If the receipt does not appear on the bulletin board, or if it is not correctly posted (e.g., different confirmation codes, different order of the candidates, or different position of the filled-in marks), the voter can show her physical receipt, which is irrefutable proof that the bulletin board contains invalid information. The posted receipts can be used by a publicly verifiable tallying scheme (see section 5) to produce vote totals which are proven to come from the posted receipts, and thus from the choices the voters made.

## 2.1 Pre-election setup

Before the election, a set of commitments is published for each ballot. For each confirmation code, a commitment that ties the confirmation code to a coded vote is made. The coded vote is the input to a verifiable tally mechanism (can be a mixnet [PH06] or homomorphic tallier [AR06]).

For each ballot, a commitment to the order of the candidates is published before the election. If the voter uses the first photocopier getting her receipt with the order of the

candidates, this commitment is opened, and anybody (not just the voter), can check that the receipt posted on the public bulletin board is consistent with the commitment that ties each candidate with the position it appears at.

Commitments that tie marks at certain marked positions to confirmation codes are also published for each possible marked position. For each confirmation code on each ballot, the system publishes a commitment that ties the confirmation code to the position that should be marked when this confirmation code is printed on the chit. If the voter uses the second photocopier, the system opens the commitment that binds the confirmation code on the receipt to the position of the mark on the receipt. Anybody can check that, on the posted receipts, the marks appear at the positions indicated by the opened commitments and that the confirmation codes do correspond to these positions.

We assume that the system that produces the Sigma ballot does not know a priori which photocopier is chosen by the voter. If, on a particular ballot, the system modifies either the order of the candidates, or the confirmation codes, then the system has a 50% chance of not getting caught (because there is a 50% chance that the voter chooses the photocopier that makes a copy of the part that was not cheated on). Assuming the voters' choices of photocopiers are independent, the probability of not detecting any misprinted ballots decreases exponentially with the number of misprinted ballots.

## **2.2 Advantages of Sigma ballots**

Sigma ballots have three major advantages. First, it should be relatively easy for the voters to check if the paper ballot contains a vote for the candidate that they voted for: locate a mark and simply read the name of the candidate to the left of the mark. Second, by giving the voters the choice to put their ballot in any of the two photocopiers, the voter performs an automatic print audit of their ballot. In some cases the voters check that the order of the candidates is correct, and in the other cases the voters check that the confirmation codes correspond to the marked positions. Third, the voter does not have to create a receipt by hand, since the confirmation code is already printed on the stub of the ballot, which is photocopied and included in the receipt.

Voters that are not interested in getting a receipt can simply ignore the photocopiers and walk out, but not before depositing the Sigma ballot into the ballot-box. To ensure that the ballots are correctly printed, it is not necessary that all voters get a receipt from one of the photocopiers, but only that a statistically significant, unpredictable fraction do.

Depending on the predictability of the confirmation codes, the lack of a paper receipt may *not* prevent the voter from checking the public bulletin board, just like in Scantegrity II. If correct confirmation codes on any given ballot are difficult to guess by voters, then the voter's knowledge of the confirmation codes may be sufficient to file a complaint if the confirmation code is not correctly posted on the bulletin board. A voter that provides a confirmation code that is unpredictable, and that was previously committed to, has probably discovered that her correctly cast ballot is not correctly posted on the bulletin board.



### **3 Producing the Voted Ballot**

Sigma ballots are ballots that are already filled-in; they already contain the will of the voter. In this section, we present a few ways in which Sigma ballots can be created. One option is to use a DRE connected to a printer (VVPAT). A second option is to have an optical scan paper ballot that is a combination of Prêt à Voter and Scantegrity II ballots.

#### **3.1 Ballot Marking Devices—DREs with VVPAT**

Probably the easiest way to produce Sigma ballots is to use a ballot marking device. This device can look like a DRE, where voters can make their selection using a touch screen and have the liberty to choose the ballot language, font size, contrast, etc. The same device can serve multiple ballot styles.

The order in which the candidates are presented to the voter can be standardized and can be the same for all ballots (such that it is consistent with local electoral law). After the voter made all her selections and inspected the review screen, she presses the “Print Sigma Ballot” button. The DRE has a regular office printer attached to it which prints a Sigma ballot. The voter inspects the print-out to see if marks appear next to the candidates she voted for. If this is not the case, she spoils the Sigma ballot and uses the DRE again to make her selections and to produce another Sigma ballot. Otherwise, the voter walks over to the area where the photocopiers are, following the process described in section 2.

The Sigma ballot can be viewed as a Voter Verifiable Paper Audit Trail (VVPAT). But the VVPAT is not printed under glass and the voter can photocopy part of it. The DRE always prints the Sigma ballot, just like it always prints a VVPAT, regardless if the voter will take the Sigma ballot to the photocopier or not. As soon as the Sigma ballot is out of the printer and is inspectable by the voter, the voter can simply memorize the confirmation codes next to the selected candidates. Later, if the voter does not see the confirmation codes on the public bulletin board, she may still file a complaint, and knowledge of the codes may be sufficient. The voter only knows the confirmation codes for the candidates she selected, thus knowing some other valid confirmation code would mean that either the vote guessed the code (which should be difficult if the codes are unpredictable), or the bulletin board contains an incorrect confirmation code.

By looking at the Sigma ballot, the voter gets a receipt based on “something you know,” i.e., the confirmation codes. The voter may also get a “something you have” receipt, a paper receipt, if she uses one of the photocopiers. The extra check that the paper receipt allows the voter to do is to ensure that the association between candidates and confirmation codes on her Sigma ballot is correct. This association has two parts: candidates to positions and positions to confirmation numbers. The voter can check that either the order of the candidates is correct, or that the marks are correctly assigned to the confirmation codes.

Because of the digital signature, neither the voting system nor the voter can add more marks to the receipt after it comes out of the photocopier. Having a physical receipt (as opposed to a “something you know”) precluded the voting system from adding more marks to the cast ballots, which may be used as an attack to transform a blank ballot into a voted one, or a voted one into an over-voted one (as is the case in Scantegrity II).

At the end of the voting day, the DREs can provide tallies for fast reporting. Moreover, the Sigma ballots can be used in a hand recount, since each Sigma ballot is a clear text ballot. A third count is provided by an existing publicly verifiable tallying mechanism such as the ones used by Scratch&Vote [AR06], PunchScan [PH06] or the Scantegrity II [CD08] (presented in section 5).

### 3.1 Optical Scan

A Scantegrity II [CD08] ballot is an optical scan ballot in which, next to each candidate there is an oval printed in invisible ink. The voter fills in the oval next to her desired candidate, and the chemicals in the pen react with the invisible ink printed in the oval, such that the ovals turns mostly black, except for a confirmation code that stays white, and thus becomes visible. The voter can record the confirmation code, in essence creating a receipt for her vote. The paper ballots can be scanned or counted by hand.

A practical problem with a Scantegrity II ballot is ensuring that codes are printed next to the correct candidates. Scantegrity II allows the voter to receive two ballots, one to fully mark and audit the printing on it, and the other one to cast. In practice, since performing the print audit is an extra burden, voters do not perform print audits. In this case, a designated auditor is needed for performing the print audit, which may be problematic.

A Sigma ballot is a Scantegrity II ballot with candidates in randomized order. This solves the print audit problem by allowing the voter to choose one of the two photocopiers to create her receipt and check the correctness of half the printing on her ballot.

Another shortcoming of the Scantegrity II ballots is that voters must create their own receipts, by writing down the confirmation numbers revealed when marking the ovals, or remembering them. Sigma ballots address this too. Assume the voter is allowed to place her Sigma ballot in one of the photocopiers, get her copy, but also get back the Sigma ballot. The voter then deposits the ballot she got back into an optical-scan system, which has a printer attached to it. The voter places the copy she got from the photocopier in the paper feed of this printer, such that the printer will print on this copy. The optical scanner detects the marks from the ballot and prints the confirmation codes on the copy that is in the printer. Therefore the voter does not need to write down the confirmation codes by hand.

The above technique is based on the assumption that the scanner does not know if the voter used the first or the second photocopier (i.e., the photocopier cannot signal the scanner). If the voter used the second photocopier, the copy already contains the confirmation codes, since in a Scantegrity II ballot the codes are revealed when the oval is filled-in by the voter. If the scanner would produce different confirmation codes, then the voter would have irrefutable proof that the scanner printed incorrect confirmation codes. If the voter used the first photocopier, the copy contains the order of the candidate, but without any confirmation codes. In this case the scanner can print incorrect confirmation codes without being detected. But since it is assumed that the scanner does not know what information is already printed on the voter's copy, the chance of printing incorrect confirmation codes and not getting caught decreases exponentially with the number of ballots cheated on.

One can also envision a system in which the scanner is used before the photocopiers: the voter puts the Sigma ballot in a scanner that checks for under-votes and over-votes and also prints the confirmation codes at the bottom of the ballot (a copy of the ballot can also be produced instead of printing at the bottom of the original ballot). Then the voter gets back the ballot and goes to one of the photocopiers, like in the DRE setting. The voter always gets the confirmation numbers, since they were printed by the scanner at the bottom of the ballot. The voter can also check that the scanner wrote the confirmation codes correctly (i.e., it detected the marks correctly), by simply inspecting the output of the optical scanner.

#### 4 Formalization of Sigma Ballots

We present a formal model of Sigma ballots. For simplicity, we model a single race and we assume that there is a candidate “No Vote,” which is selected by default if the voter does not select any candidate. Let  $C$  be the set of candidates. Let  $c$  be the cardinality of the set  $C$ , and let  $Z_c$  be the set of numbers from zero to  $c-1$ . Let  $N$  be the set of all possible confirmation codes, and let  $E$  be the set of coded votes that a publicly verifiable tallying scheme takes as input. We assume that the cardinality of  $N$  is large.

A Sigma ballot is defined by three functions:

1.  $\sigma : C \rightarrow Z_c$  representing the association between the candidates and the position they appear at.  $\sigma$  is a bijective function.
2.  $\pi : Z_c \rightarrow N$  representing the association between positions and confirmation codes.  $\pi$  is an injective function. We assume that it is difficult to guess  $y \in N$  such that  $\exists! x \in Z_c$  such that  $\pi(x)=y$ .
3.  $\phi : \pi(Z_c) \rightarrow E$  representing the association between confirmation codes and coded votes.  $\phi$  is an injective function.

A Sigma ballot transforms a clear text vote (a candidate) into a coded vote by composing the three functions  $\phi \circ \pi \circ \sigma$ .

---

<sup>2</sup> We abuse the  $Z_c$  notation to simply mean the set of numbers from zero to  $c-1$  instead of the set of residues modulo  $c$ .

The protocol follows the following steps, for each ballot:

1. The election authority computes in secret  $\phi$ ,  $\pi$  and  $\sigma$ .
2. The election authority computes and publishes:
  - a. A commitment to the entire function  $\sigma$ .
  - b. For each  $x \in \mathbf{Z}_c$ , a commitment to  $(x, \pi(x))$
  - c. For each  $x \in \pi(\mathbf{Z}_c)$  a commitment to  $x$
  - d. For each  $x \in \pi(\mathbf{Z}_c)$  a commitment to  $(x, \phi(x))$
3. The election authority prepares a publicly verifiable tallying function  $\mathbf{D}$  such that  $\forall x \in \mathbf{C}, \mathbf{D} \circ \phi \circ \pi \circ \sigma(x) = x$ . The preparation may involve publishing commitments, keys, etc. depending on the particular  $\mathbf{D}$ . One can say that a sigma ballot encrypts a clear text vote  $x$  into a coded vote  $y$  and  $\mathbf{D}$  decrypts  $y$  back to  $x$ . A sample  $\mathbf{D}$  is described in section 5.

To check that  $\forall x \in \mathbf{C}, \mathbf{D} \circ \phi \circ \pi \circ \sigma(x) = x$ , a public auditor chooses a statistically significant number of ballots and asks the election authority for the information such that the equation  $\mathbf{D} \circ \phi \circ \pi \circ \sigma(x) = x$  can be publicly checked. This is the very first step of the protocol and is done before Election Day, before ballots are printed.

The next step is to produce Sigma ballots and receipts, using one of the protocols described in section 3.

After the voter obtains her receipt, the following commitments are opened:

1. If the receipt contains the order of the candidates, the commitment to the entire function  $\sigma$  is opened.
2. If the receipt contains the position  $x$  of the marks, the commitment to  $(x, \pi(x))$  is opened.
3. For the confirmation code  $x$  which is always on the receipt, the commitment  $(x, \phi(x))$  is opened.

If a voter complains that she does not see the correct confirmation codes posted on the public bulletin board, she is asked to provide the confirmation codes that she thinks should be on the bulletin board. Then the election authority opens all commitments to  $x$ ,  $\forall x \in \pi(\mathbf{Z}_c)$ . If the confirmation code provided by the voter is not among the opened ones, then the voter must be wrong. If it is among the revealed ones, and since the confirmation codes are difficult to simply guess, then, if a statistically significant fraction of voters provide confirmation codes that are among the committed ones, this becomes an indication of malfunction.

If the voter does not see her paper receipt correctly posted on the public bulletin board, i.e., the order of the candidates or the position at which the marks appear is not the same, then the voter can bring her paper receipt as irrefutable proof of malfeasance.

Anybody can inspect the bulletin board and check that the commitments are consistent with the posted receipts, i.e., with the order of the candidates or with the association between confirmation codes and the marked positions. Also, anyone can check the commitments to the confirmation codes themselves or the commitments to the association between confirmation codes to coded votes.

## 5 One way to produce the tally

Inspired by Scantegrity II [CD08], we briefly describe an example of a function  $\mathbf{D}$  that allows everyone to check that all the receipts have been correctly tallied. This scheme is not a contribution of this paper, and it is presented only for completeness.

Let  $N$  be the number of ballots in an election and let  $c$  be the number of candidates on a ballot. Consider three tables (see Figure 4): table  $R$  contains coded votes, table  $T$  contains clear text votes that are countable by anyone and table  $D$  connecting  $R$  with  $T$ .  $R$  is a matrix with  $N$  rows and  $c$  columns, each row represents the coded votes of a ballot.  $R$  is a matrix with  $c$  rows and  $N$  columns, each row representing a candidate. An element  $(i, j)$  is either marked or not marked in  $R$  and  $T$ . A mark in  $T$  corresponds to a vote for a candidate.  $D$  is a set with  $N * c$  elements. Figure 4 gives an example of the three tables for an election with six ballots and two candidates.

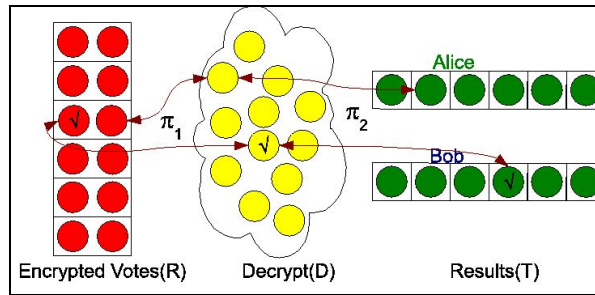


Figure 4: Pointer-based mixnet

The tables are connected by two permutations,  $\pi_1$  and  $\pi_2$ .  $\pi_1$  connects  $R$  with  $D$ :  $D_k = R_{\pi_1(k)}$ , where  $k$  is some canonical representation of  $(i, j)$ , e.g.,  $k = (c-1)*i + j$ . Similarly,  $\pi_2$  connects  $D$  with  $T$ :  $T_k = D_{\pi_2(k)}$ .

The properties of the permutations may be formalized as follows: let  $\pi_1: \mathbf{Z}_{n \times c} \rightarrow \mathbf{Z}_{n \times c}$  be bijective and let  $\pi_2: \mathbf{Z}_{n \times c} \rightarrow \mathbf{Z}_{n \times c}$  be bijective such that no two coded votes belonging to the same ballot initially (in the same row in table  $R$ ) are mapped to two elements belonging to the same candidate (the same row in table  $T$ ):

$$\forall i, j, i \neq j \text{ having } [i / c] = [j / c] \rightarrow [\pi_2(\pi_1(i)) / b] \neq [\pi_2(\pi_1(j)) / b] \quad \text{Equation 1}$$

where  $[x]$  represents the greatest integer less or equal to  $x$ . The function  $\mathbf{D}$  that provides a universally verifiable tally function is  $\mathbf{D} = \pi_2 \circ \pi_1$ .

Initially, the election authority publishes commitments to each mapping done by  $\pi_1$  and  $\pi_2$ , along with the commitments needed for the Sigma ballots, including the commitments that tie in the confirmation coded to the coded vote (the indexes in the  $R$  table). To check the correctness of this step, an auditor can request some statistically significant number of ballots to have their commitments opened. When a cast ballot is received, the election authority opens the commitment that ties the confirmation code to the coded vote in the  $R$  table. After the polls close and the index in the  $R$ ,  $D$  and  $T$  are marked, the final audit checks that one of the two properties hold, at random:  $D_i = R_{\pi_1(i)}$  or  $D_i = T_{\pi_1(i)}$  and that the properties of the two permutations  $\pi_1$  and  $\pi_2$  hold, i.e., it checks

that both  $\pi_1$  and  $\pi_2$  are injective functions and that Equation 1 holds for each of the revealed pairs of  $\pi_1$  or  $\pi_2$ . Because the voting system cannot predict which permutation will be checked, a successful audit implies that the coded votes have been correctly transformed into clear text votes with high probability. Privacy is preserved, since no complete link is revealed from the R table to the T table, but only links from either R to D, or from D to T.

## 6 Conclusions

We have presented a new type of filled-in ballot which has confirmation codes like Scantegrity II and the order of the candidates permuted like Prêt à Voter. The advantages of Sigma ballots combine the ability to easily check that they have been correctly printed with the ability to file a complaint without the need for the voter to present physical evidence. At the same time, Sigma ballots solve some of the issues of Scantegrity II, such as adding marks after the ballots have been cast, or needing to create receipts by hand. Sigma ballots produce a “something you know” receipt to check the correct recording of the cast ballot and a “something you have” receipt to check the correctness of printing.

We described two ways in which Sigma ballots can be produced: using a DRE+VVPAT or using an optical scan Scantegrity II ballots. The DRE+VVPAT approach seems to be the most promising one, since it combines the advantages of having a robust and precise interface with the availability of hand countable paper ballots, and on top of that, the publicity verifiable tallying method.

## Bibliography

- [AR06] Adida, B, and R. Rivest. 2006. Scratch & vote. Self-contained paper-based cryptographic voting. In *WPES '06. Proceedings of the 5th ACM workshop on privacy in electronic society*, 29–40. New York, NY, USA: ACM Press.
- [AB09] Adida, B. et al. 2009. Electing a university president using open-audit voting. Analysis of real-world use of helios. In *Electronic voting technology workshop/workshop on trustworthy elections*. Usenix.
- [CD04] Chaum, D. 2004. Secret-ballot receipts. True voter-verifiable elections. *IEEE Security and Privacy* January/February: 38–47.
- [CRS05] Chaum, D., P. Y. A. Ryan, and S. Schneider. 2005. A practical voter-verifiable election scheme. In *ES-ORICS, volume 3679 of lecture notes in computer science*, ed. Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, 118–139. Springer (<http://www.springerlink.com/content/ebrbl9kc81bhx98j/>).
- [CD08] Chaum, D. et al. 2008. End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *EVT'07. Proceedings of the USENIX/accurate electronic voting technology workshop*. USENIX Association.
- [EA07] Essex, A. et al. 2007. Punchscan in practice. An e2e election case study. In *IAVoSS workshop on trustworthy elections (WOTE 2007)*. University of Ottawa, Canada.
- [KJ07] Kelsey, J. et al. 2007. Some random attacks on paper-based e2e systems. <http://kathrin.dagstuhl.de/files/Materials/07/07311/07311.KelseyJohn.Slides.pdf/>. (accessed 17 November 2008).
- [PH06] Popoveniuc, S., and B. Hosp. 2006. An introduction to PunchScan. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*. Robinson College, Cambridge.

## **Session 6: E-Voting Experiences**





## **Electronic Elections in a Politicized Polity**

Thad Hall<sup>1</sup> and Leontine Loeber<sup>2</sup>

<sup>1</sup>Associate Professor of Political Science, University of Utah  
260 S. Central Campus Drive, Room 252  
Salt Lake City, UT 84112  
USA

<sup>2</sup>University of Leiden, Netherlands  
Professor Paul Scholtenlaan 48  
1181 ME Amstelveen  
The Netherlands

**Abstract:** Since the 2000 presidential elections, the evolution of electronic technologies in American elections—from voting machines to computerized voter registries—has occurred within the context of a highly partisan, polarized, and politicized environment. The decision about the type of voting systems to use within a given state has become especially political and these debates have affected the confidence and attitudes of voters toward various voting technologies. In the Netherlands, the debate even led to abolishing the use of all electronic technologies in elections. In this paper, we consider the evolution of voter confidence over this period and the evolution of the political debate that relates to electronic voting. We note that confidence in voting systems is affected by several factors, including race, partisanship, voting for a winning candidate, and the mode of voting (i.e., voting in person or voting via absentee ballot). During this time, certain factors, such as partisanship, have changed in importance based on previous election outcomes. On the issue of the importance of partisanship on confidence, we compare the United States and the Netherlands and the evaluation of electronic voting.

## 1 Introduction

A polity is a geographic area with a corresponding government. The term is also used to refer to a state or a lower level government such as a province, municipality or district. A polity can become politicized when different political factions appear. This may lead to changing policies with regard to electronic elections. A policy is a set of decisions to achieve a rational outcome. In this paper we look at different factors that may influence policies concerning electronic voting in politicized polities. The study of confidence in the electoral process—especially the process of counting ballots—in the United States has become a major field of research since the disputed 2000 presidential election. In that election, the decision regarding who won the race for president, between Al Gore and George Bush, became a tangled legal issue, largely because of the difficulties associated with determining how to count and recount ballots in the State of Florida. The decision of the United States Supreme Court in *Bush v. Gore* determined that recounts in the election would end, making George Bush the victor, but the controversies surrounding election administration and voting technologies continued. Throughout 2001 and 2002, several research groups and blue-ribbon commissions examined the elections in the United States and made recommendations that informed the passage of the Help America Vote Act (HAVA) of 2002 [VTP01, CF02]. Given that the most visible problem from the 2000 presidential election was the issue of how to count ballots, it is not surprising that the centerpiece of HAVA was providing funding to states to purchase modern voting technologies, with the intent of solving the vote-counting problem through the acquisition and implementation of new voting systems.

However, the contentiousness of the 2000 election was not just the result of the debate over the way votes were counted and the closeness of the election in the state of Florida. As many scholars have noted, the 2000 election occurred in a period when the American electorate had become increasingly polarized [AS08]. The highly politically engaged are especially polarized and there is evidence of strong partisan polarization in America as well. Liberals and conservatives, and Democrats and Republicans, view the political world quite differently; their issue preferences are highly bifurcated across an array of policy issues. In addition, the electorate is becoming divided geographically, with more states becoming uncompetitive and relatively few states serving as battlegrounds for electoral competition at the presidential level [AS08; Bi08]. These divisions in America have become much more pronounced than they were in the 1960s, with polarization increasing throughout the 1970s, 1980s, and 1990s.

One key issue for voting is how polarization and having a polarized electorate affects the confidence of voters in the voting process. Given the problems that existed in the 2000 election, it is reasonable to ask whether the partisan polarization—combined with issues with election administration—affects the willingness of losers to “consent” to the outcome of the election. The question of consent among losers is critical for the legitimacy of election administration because, although winners always find the election to have been fair, losers have to think and feel that the process that resulted in their loss was fair [ABB05]. This consent is needed not just from the candidates and parties; voters themselves must be confident that election administration is not being manipulated for partisan reasons.

In the Netherlands, electronic voting was introduced in 1966 and was for a long time no subject of debate. The confidence in the system was very high, which led to more and more municipalities making the choice for voting machines. During the municipal elections of 2006, 99% of the voters voted on a direct recording electronic (DRE) voting machine. In the summer of 2006, an action group called “We don’t trust voting computers” was founded, which started a media campaign against the voting machines in use. This led to several debates in Parliament and ultimately to the abolishment of all forms of electronic voting. After the parliamentary elections of 2006, voters were asked whether they had confidence in different forms of electronic voting. This research, done in the National Voters Study 2006, is the first major study done in the Netherlands concerning voter confidence.

In the United States, there has been an effort since 2004 by political scientists to measure voter confidence in the electoral process. This effort has examined confidence generally in the electoral process, but also with specific methods of voting, such as electronic voting or voting with machine-counted paper ballots. In this paper, we review the findings in this literature and present new analyses that show how Americans remain divided in their confidence levels in the voting process generally and with specific voting technologies. We discuss how a simple measure of confidence can be used to evaluate the attitudes of voters and election officials in various aspects of the electoral process. We then consider how voter confidence has changed over time in the electoral process and how partisanship, ideology, and the voting technology used all affect the confidence of individuals participating in the electoral process.

The American context for studying voter confidence and considering the effects of voting technologies on confidence has occurred in the shadow of the 2000 presidential election controversy. In order to disentangle the issue of voter confidence and voting technology, we compare the findings of the United States with results from the Netherlands. There, there was a great controversy over the security and efficacy of electronic voting in 2008, which led the government to disallow the use of these machines in elections in the Netherlands. We can compare confidence in the American context with the Netherlands to see how partisanship and attitudes toward voting technology are treated in both contexts. We can then see how the American experience may be unique in some ways, but not others, regarding voter confidence.

## **2 Measuring Confidence in the Electoral Process**

Although discussions of voter confidence have existed in the United States for some time—the term “confidence” was used in the report of the National Commission on Federal Election Reform (Carter and Ford 2002)—the systematic measurement of voter confidence in the voting process has been a more recent phenomenon. In 2004, Alvarez and Hall conducted one of the first studies to use what has become a standard voter confidence question. The question they used was, “How confident are you that your vote was [or will be] counted as intended in [the election]?” with the response options “very confident,” “somewhat confident,” “not too confident,” or “not at all confident.” As

Alvarez, Hall, and Llewellyn (2008, 755) discuss, this measure “define[s] trust in the electoral process as the confidence that the voters have that their ballot was counted as intended.” As Gronke and Hicks (2009) note, several scholars have used voter confidence as a metric for studying voter attitudes toward election reforms [Ha08] and Stewart (2009) has referred to this voter confidence metric as “a summary judgments of the voting experience.”

Scholars have also broadened this concept in a small number of surveys to ask voters not just “how confident are you that *your vote* will be counted as intended,” but also “how confident are you that *all votes in your county* will be counted as intended” and “how confident are you that *all votes in your state* will be counted as intended” [AAH09; AS07]. These broader measures are designed to determine if voters have different levels of confidence across varying levels of government—their vote, votes administered by a process in their county, and votes administered by various processes and various officials across the state—and various levels of abstraction in the process (your vote, votes in a county, votes in the state).

A key question that has emerged regarding the use of this metric is whether the metric is merely a reflection of the respondent’s trust in government or the respondent’s expectation of their candidate winning the election. Alvarez, Hall, and Llewellyn (2008) make the claim that there is no *a priori* reason to think that vote confidence and trust in government are the same. They argue, “Voters may not possess confidence in the voting technology used to cast a ballot, but trust their elected officials completely. Alternatively, voters may believe that the electoral process is fair and accurate, but simultaneously hold the belief that all politicians are crooks” [AHL08, 755]. They put the question of voter confidence within the literature on trust, but note how the two concepts are different.

Recently, Atkeson, Alvarez, and Hall (2009) and Gronke and Hicks (2009) independently tested the validity of this construct, explicitly examining whether voter confidence and voter trust are truly distinct concepts. Atkeson et al. (2009) compare three types of voter confidence—personal vote, the votes in a county, and votes in a state—with a measure of trust in government and a measure of political efficacy. They find that the confidence questions load differently in a principal-component analysis compared to the trust and efficacy questions; they are not part of the same dimension. In addition, trust, efficacy, and confidence have different correlation relationships; the confidence questions are highly inter-correlated, but these questions in turn are not as correlated with either trust or efficacy. Importantly, when used as dependent variables in a regression model, different factors predict voter confidence when compared to either efficacy or trust. For the confidence questions, a voter’s experience voting affects voter confidence, but is unrelated to either trust in government or efficacy.

Gronke and Hicks (2009) use a different methodology to come to the same result. Specifically, they run a series of regression analyses to determine if voter confidence is explained by trust in government, confidence in social or political institutions, current economic-political factors, or by election administration experiential factors. They determine that, although trust in government and confidence in election officials do help

to shape voter confidence, election experience is a strong predictor as well. If voter confidence were merely another measure of trust in government, these other factors would be washed out by the high correlation between trust and confidence. This adds weight to arguments that the voter confidence metric is a sound one to use as a “summary measure” for determining a voter’s confidence in the electoral process, at least in the American context.

In the Netherlands, the study of voter confidence has been done in the context of the National Election Survey. This survey is conducted before, during, and after elections for Parliament. It studies a wide range of subjects and contains nearly 700 questions. Different questions are asked before and after the election. During the Parliamentary Elections of 2006 a series of questions was added to the survey conducted after the election on voter confidence, both in the outcome of the election in general and in different voting methods. These questions were asked in light of the discussion on voting machines. Around 2800 participants answered these questions.<sup>1</sup>

### **3 Experiential Influences on Voter Confidence**

Research on voter confidence has generally focused on three sets of attributes that affect confidence in the voting process. First, there have been studies examining the way in which the voting experience—especially during in-person election-day voting—affects voter confidence [e.g., AAB09; CMM08; GH09; Ha09; HMP09]. These studies have found that voter confidence is affected by voter experiences at the polls. Voter confidence is sensitive to the experience that voters have with their poll workers; poll workers that are not seen as competent can negatively affect voter confidence. This is not surprising, given the important role that poll workers play in ensuring that votes are counted and counted accurately.

Second, there have been relatively consistent findings that voter confidence varies across modes of voting. This finding has been made by numerous scholars and the one consistency of these findings is that voter confidence is predicated on the mode by which voters cast their ballot [e.g., AH04, AH08A, AHL08, AHL09, AS07, AAH07, Ha09, St09, AAB09]. In the American context, there are three modes by which voters can cast their ballots, although these laws do vary by state [AAB09]; voters can cast a ballot (1) in person in a polling place on Election Day, (2) in person in a polling place during a period prior to Election Day (often the two weeks prior) in an “early voting” location, or (3) remotely, using a paper ballot that is mailed back to their election office (absentee or postal voting).<sup>2</sup> In the Netherlands, voters can vote in person in a polling place on Election Day. However, unlike in the United States, Dutch voters cannot vote absentee. They can give a proxy vote to a voter of their choice. A proxy vote can be given by a

---

<sup>1</sup> For more information about the survey and its methodology, see <http://www.dpes.nl/>, last accessed on 10 May 2010.

<sup>2</sup> The rules for absentee voting vary by country and can (as in the case of the United States) vary by subdivision within the state. In the United States, absentee voting occurs by the election official mailing the ballot to the voter and the voter mailing the ballot back. By contrast, in Estonia absentee voting is done using the Internet and in the Dutch case, the voters choose someone to cast a ballot for them.

voter who cannot vote in person at the polling station on Election Day to any other voter. The voter who receives the proxy vote is allowed to cast the vote for the other person. A voter can only cast proxy votes for two voters. Even though the system allows voters who cannot vote in person to use their vote, they have no guarantee that the person they give their proxy vote to will cast their vote as intended. Voters who live abroad can vote either by postal ballot or, in the 2006 elections, by Internet. For all voting methods, it is possible to cast a blank vote.

	Mode of Voting		
Confidence	In Person Election Day	In Person Early	Absentee
Not Confident	1.92%	1.62%	2.52%
Not too Confident	3.02%	2.61%	5.63%
Somewhat Confident	20.16%	22.87%	31.76%
Very Confident	74.91%	72.90%	60.09%
	Mode of Voting		
Trust in Elections	Proxy Voter	Voted In Person	
Very Much	31.56%	31.17%	
Much	49.78%	49.87%	
Not Too Much or Too Little	12.89%	13.29%	
Little	3.11%	4.89%	
Very Little	2.67%	0.77%	

**Table 1:** Confidence and Trust by Vote Mode

The research on voter confidence shows that voters who cast ballots using absentee voting are much less confident than voters who vote in-person, either early or on Election Day. In the top half of Table 1, we show the confidence of voters across various vote modes using data from the *2008 Survey of the Performance of American Elections* [AAB09]. These data illustrate the large gap in confidence between in-person and absentee voters. Absentee voters have many potential reasons for being less confident that their vote will be counted accurately, which may arise largely because these voters are less confident that their vote will be counted at all. In absentee voting, voters typically surrender their ballots to a third party—a postal service—and typically have to guess as to whether their ballot was received in the time frame required for ballots to be counted. These concerns are well founded; a small but significant percentage of ballots are rejected because they are received at the local election office after the deadline for including such ballots in the vote count [AHS08]. Even among ballots that were received in a timely manner, another cluster of ballots contains errors that result in the ballots being disqualified and not included in the ballots counted. Even after this hurdle is eclipsed, the vote on the ballot may still have an error that results in the vote not being counted for a given race.

In the bottom half of Table 1, we show data on voter confidence that uses a slightly different question than the one used in the American context. Here, we examine trust in the elections process generally by voting mode in the Dutch context. Here, we see that there are no significant differences in trust between voters who cast a vote in person and voters who gave a proxy vote. Both groups have the same levels of trust in the voting process.

Finally, there has been research on voter confidence and how it is related to the voting technology the individual used to cast her ballot [AH04, AHL08, AL08, AS07, HNH08, St09]. In these studies, the primary analysis has been whether voting technologies affect voter confidence. The findings of these studies have been relatively consistent; in the United States, voters using DREs tend to be less confident than voters who vote on paper ballots. For example, Alvarez, Hall, and Llewellyn (2008) found that voting on a DRE lowered the predicted probability that an individual would have their vote counted accurately by sixteen percentage points compared to a voter who voted using a paper ballot. Interestingly, this decline in confidence is the same as the decline in confidence for individuals who vote absentee. The confidence was even lower if an individual had low levels of trust in electronic voting generally.

In his study of the 2008 election, Stewart (2009) extended the work of Alvarez, Hall, and Llewellyn to determine if their results held in the 2008 election. Using a variety of statistical analyses, including ordered probit and ordinary least squares regressions (with state fixed effects and without), he found that voting technology was an important part of the confidence equation. Specifically, voters who cast ballots using electronic voting technologies were less confident than voters who cast ballots using optical scan voting. In addition, important for the discussion of voter confidence and polarization in the next section, Stewart found that liberal voters who used DREs were much less confident than were other voters who used DREs. In fact, conservative voters who use DREs are especially confident that their vote is counted accurately.

In the Netherlands however, in the 2006 Parliamentary elections, more voters expressed confidence in the DREs than in paper ballot voting; 80% of the voters expressed high levels of confidence in voting by DRE but the confidence level for paper ballot voting was 74%. When asked what type of voting method a voter preferred, DRE or paper ballot, 50% of the voters preferred voting by DRE and only 14% paper ballots. The 2006 election was the last election before the decision to terminate use of DREs in the Netherlands. During the 2006 election, out of around 400 municipalities, only 35 municipalities used paper ballot voting, the rest used DREs made by the Nedap Company.

## 4 Voter Confidence and Political Polarization in the United States

The fact that there are variations in confidence across voting technologies and voting modes—early, absentee, and Election Day—leads to questions regarding the political and ideological factors that also may affect voter confidence. There is a strong rationale for thinking that liberals and Democrats would be less confident overall compared to conservatives and Republicans, as well as thinking that liberals and Democrats would be less confident in electronic voting. The issue of overall confidence in this political and ideological context can be explained as resulting from two factors. First, Democrats were on the losing end of the 2000, 2002, and 2004 elections—elections that were generally very close and very polarizing. The close and controversial aspects of the 2000 election in Florida and the 2004 presidential election in Ohio—where both Secretaries of State were Republicans who had endorsed President Bush—led many Democrats to view these elections as being one where partisan decision making had made the playing field unfair [AH08a].

Second, there were linkages made between the outcomes of these elections and the use of electronic voting. The concerns about electronic voting arose because of research that found problems associated with the Diebold DRE) voting machines that were used in several states, including Georgia and Maryland [KSR04]. These technical concerns became and remain a contentious source of debate, which centers primarily on whether DREs can be secured using standard methods for securing election materials through chain of custody procedures (AH08b).

These technical concerns became politicized when various advocates attempted to make links between electronic voting and pro-Republican election outcomes, starting with claims that the election in the state of Georgia in 2002 was potentially fraudulent. As Alvarez and Katz (2008) note,

The allegations and concerns about the potential for election fraud in the trial use of these “touchscreen” voting systems in Georgia's 2002 election only worsened when the chairman and chief executive of Diebold, Inc., the corporation that produced the “touchscreen” voting machines used in Georgia was quoted in a Republican fundraising letter that he was “committed to helping Ohio deliver its electoral votes to the president next year.”<sup>3</sup>

Alvarez and Katz (2008) review the claims of irregular outcomes in the 2002 senatorial and gubernatorial elections in Georgia—which introduced DREs statewide the same year—and use statistical analyses to refute these claims of fraud associated with electronic voting. However, questions continued to be raised about the accuracy and validity of elections conducted using DREs through the 2006 elections, as various issues have come up in jurisdictions that use electronic voting. Ironically, the same polarization has not occurred with similar problems with electronically counted paper ballots

---

<sup>3</sup> Schwartz, John. 2004. Executive calls vote-machine letter an error. *New York Times*, May 12, section A, column 6, page 19.



[AH08a]. The debate over electronic voting has also failed to consider the important issue of usability and effective interaction between the voter and the voting technology—the issue that was the original concern of reformers after the 2000 presidential election. Work in this area has examined the usability of various voting equipment and the evaluation that voters have of these technologies [HNN08]. These data show that voters have varying attitudes toward specific voting technologies and that it is incorrect to view all electronic voting as being the same. Voters differentiate between various types of DREs and between DREs and paper ballots in ways that are much more subtle than would normally be thought.

We see evidence of the difference in attitudes toward electronic voting among political partisans in survey data where voters are asked the following: “I’m going to read you some statements about electronic voting and want to know whether you agree or disagree with each statement, or if you have no opinion. ‘Electronic voting systems increase the potential for fraud.’”<sup>4</sup> Table 2 shows data for this question from surveys conducted 25–29 August 2004, 9–15 March 2005, and 26–31 October 2006 by International Communications Research

		Agree	Disagree	No Opinion
Oct-06	Republican	32	40	26
	Democrat	46	21	29
	Independent	39	21	37
Mar-05	Republican	33	37	28
	Democrat	47	23	28
	Independent	36	31	32
Aug-04	Republican	34	32	30
	Democrat	40	23	35
	Independent	40	31	29

**Table 2:** Electronic Voting and the Potential for Fraud

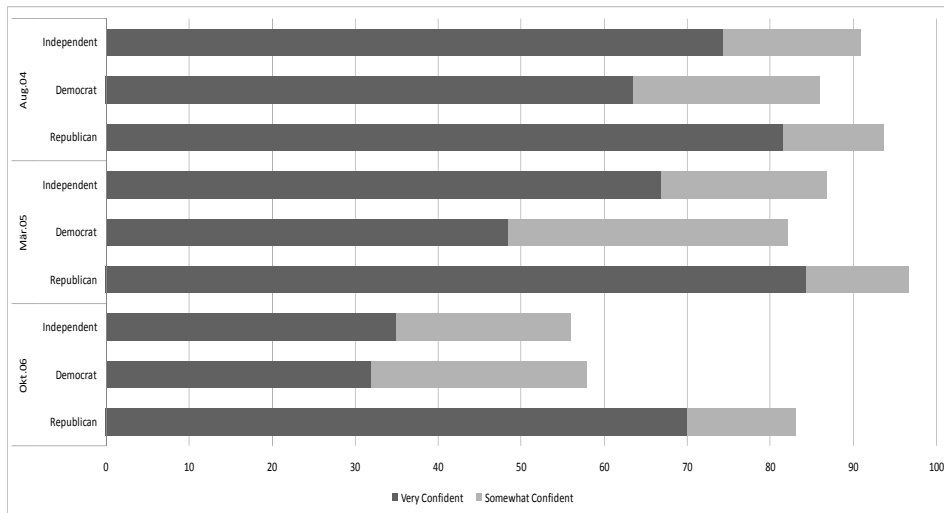
In each case, we see that Democrats are more likely to think that electronic voting increases the potential for fraud compared to Republicans and that the Democrat/Republican gap on this issue widens from six percentage points before the 2004 election to thirteen points after the 2004 election. This widening gap comes from Democrats becoming more sure that electronic voting increases the potential for fraud; the attitudes of Republicans stays the same on the agree side of the question, but five percentage points more Republicans disagree with this statement between the three surveys.<sup>5</sup> The data from the 2006 wave is shown in the top third of the table; it closely

<sup>4</sup> A detailed discussion of these survey data and the methodology for their collection can be found in Alvarez and Hall 2008a and Alvarez, Hall, and Llewellyn 2008.

<sup>5</sup> The survey marginals presented in Figure 3 do not show the “don’t know/no response” category. In the first survey, 4.6 percent of Republicans answered, “don’t know” compared to 1.6 percent of Democrats. In the second wave, Republicans and Democrats were almost equal in this category (1.9 percent Republicans, 2.3 percent Democrats).

mirrors the 2005 survey data and suggests a relative stability in attitudes about electronic voting and the likelihood of it increasing the potential for fraud during this period.

There are also differences between Democrats and Republicans in their confidence that their vote will be counted accurately. If we look at data from before the 2006 election in the three waves of surveys, we see that there are marked differences between Democrats and Republicans who are very confident—Republicans are much more confident than Democrats are that their votes will be accurately counted. Prior to the 2006 election, we see that, even combining the very confident and somewhat confident categories for Democrats, more Republicans are very confident than Democrats are very or somewhat confident.



**Figure 1: Voter Confidence by Party Affiliation**

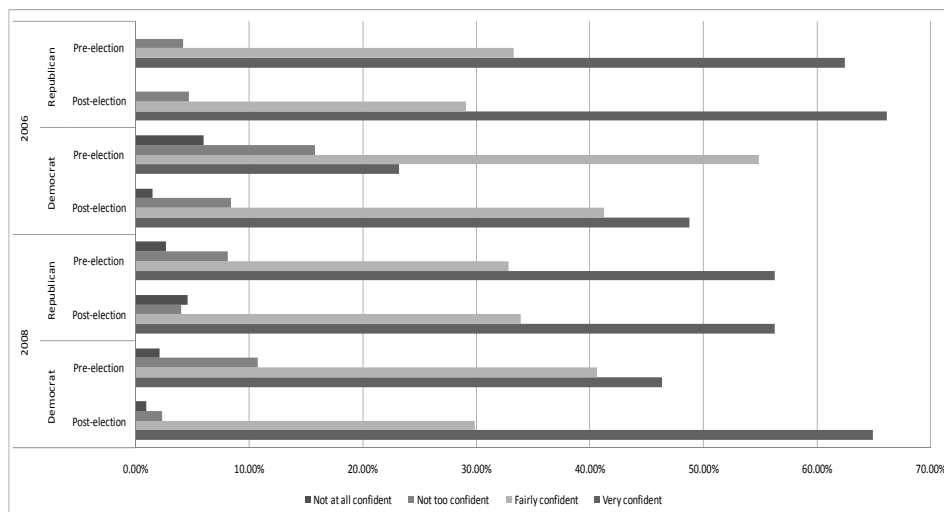
If we consider the context of the 2000 and 2004 elections—where Democrats lost close elections for the presidency and suffered losses in the Senate in 2002—it is not surprising that Democrats expressed little confidence in the electoral process. For many, it was likely easier to blame the electoral process than blame voters and the candidates for these losses. However, in 2006 and 2008, the Democrats were on the winning side of the elections. In 2006, Democrats nationally recaptured control of the Congress and, in 2008, they recaptured control of the Presidency. So how did these wins affect voter confidence?

We can examine this by using data from the Cooperative Congressional Election Study (CCES), which is a national survey conducted by Polimetrix in which individuals were surveyed before and after the 2006 congressional elections and the 2008 presidential elections.<sup>6</sup> Before the election, individuals were asked about their confidence that their

<sup>6</sup> For more information about the survey and its methodology, see <http://web.mit.edu/polisci/portl/cces/index.html> (last accessed 1 June 2009).

vote *would be* counted accurately, and after the election, they were asked their confidence that their vote *was* counted accurately. Figure 2 shows the pre- and post-election confidence for Democrats and Republicans after each of these elections. In 2006, we see that the percentage of Democrats who were very confident doubled between the pre- and post-election surveys and the percentages of Democrats who stated being not too confident or not at all confident declined by half as well. Republicans—who were much more confident to begin with—saw little change in their confidence in the pre- to post-election surveys. In 2008, we see a similar pattern; Republicans have a relatively stable level of confidence between the pre- and post-election surveys and Democrats have a sharp increase in the percentage reporting being very confident in the post-election survey compared to the pre-election survey.

As Alvarez, Hall, and Llewellyn (2009a, 2009b) have argued, this result can be viewed as a form of “winner’s effect” that is conditional on an election outcome being different from the outcome that was expected for one of the parties. In the case of the 2006 and 2008 elections, Republicans expressed relatively high levels of confidence in the system before the election, but were not surprised by losing, given the level of polling on these elections and the amount of conservative punditry that had predicted—even welcomed the idea of—Republican losses. Democrats, on the other hand, had a more “believe it when I see it” attitude, which led them to have lower baseline levels of confidence pre-election and a relatively strong surge in overall confidence after the election.



**Figure 2:** Pre- and Post-Election Confidence 2006 and 2008

In their work on a winner’s effect in the 2006 elections, Alvarez, Hall, and Llewellyn (2009a) found that, in the pre-election voter confidence model, Democratic voters, and Independent voters, had significantly lower levels of confidence compared to Republicans. Specifically, the first differences in an ordered logit model show that “hypothetically changing the voter’s party identification from Republican to Independent decreases the likelihood of a very confident response by 21 percentage points and from Republican to Democrat lowers confidence by 28 percentage points.” They also found

that individuals who lived in an area that the respondent felt was not dominated by one political party was more confident, pre-electoral confidence may be increased through a belief in the existence of a politically balanced or non-partisan local government [AHL09a].

By contrast, they found that post-election voter confidence was driven by both partisan and election administration factors. There was a winner's effect—Democrats did have a marked increase in confidence after the election. In addition, voters who think that there is congruence between their party identification and the party that controls the local government are significantly more likely to be confident compared to voters who have incongruence. This finding supports previous research [AS07] regarding the link between confidence and local government politics. The post-election voter confidence was also affected by the voting technology the voter used. Specifically, voters who used electronic voting were significantly less confident than were voters who cast ballots using paper ballots. The negative effects of electronic voting, however, were made up for if voters voted on an electronic voting machine that had a paper audit trail (PAT) that allowed the voter to review a printed copy of their ballot before casting their electronic vote. In fact, voting on an electronic voting machine with a PAT made voters 14 percentage points more likely to be very confident compared to paper ballot voters [AHL08].

Alvarez, Hall, and Llewellyn (2009b) have also examined voter confidence in partisan primary elections, specifically the “Super Tuesday” presidential primaries held on 5 February 2008. These primary elections are interesting because they bring out the most committed partisan voters, who may have different views about the voting process compared to more casual voters. However, they find that the same factors that have been identified previously—a partisan difference in confidence between Democrats and Republicans (Republican primary voters have a higher base level of confidence compared to Democrats), lower confidence among absentee voters, and a “winner's effect” (voters in a primary who voted for a winner are more confident than those who voted for a loser)—all are significant in primary elections as well.

## **5 Voter Confidence and Political Polarization in the Netherlands**

Because we only have data on voter confidence in the Netherlands for one election, it is not possible to see whether there are changes in voter confidence within supporters of the same party over time. It is however possible because of the multi-party system to look at the difference in voter confidence between voters of several parties, some of which were winners in the 2006 elections and some of which were losers. However, because of the Dutch proportional representation system coupled with coalition government, even parties that lose seats can still end up in government. In 2006, for example, this happened with the Labor Party (PvdA). Winning or losing in the Netherlands is therefore more relative than in the US. In the elections of 2006, the big winners were the Socialist Party (SP), the ChristenUnie, the Party for Animals (Partij voor de Dieren), and the party led by Wilders (PVV). Big losers were the Labor Party (PvdA), the Liberals (VVD), the Democrats 66 (D66), and the former party of Fortuyn (LPF).

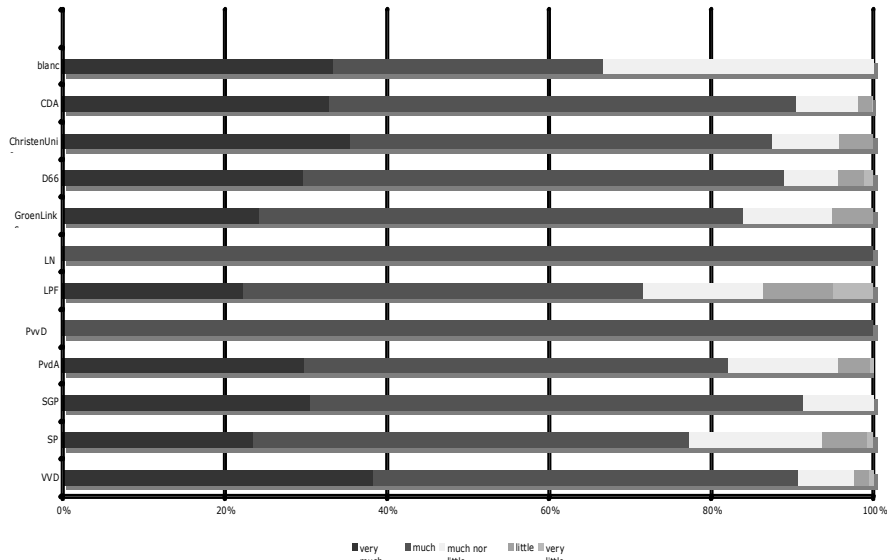


Figure 3a: Confidence in Voting machines

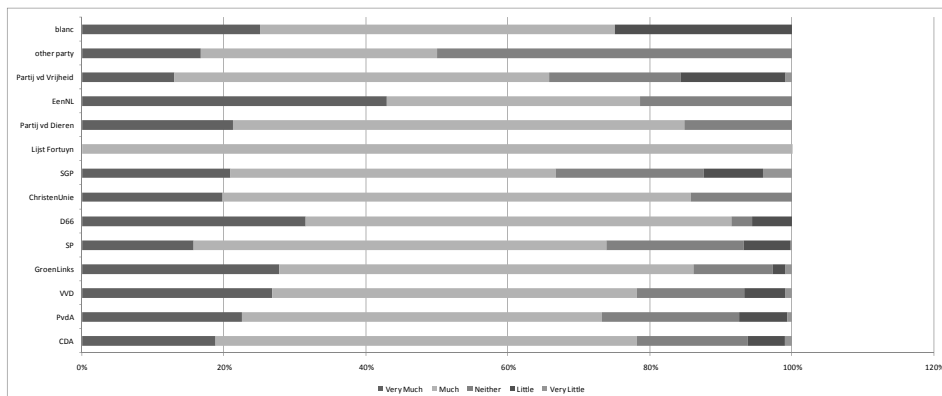


Figure 3b: Confidence in Paper Ballots

Figure 3a shows the confidence level in voting by voting machine of the voters of all the parties. In general, the trust in voting machines is very high, both with voters of parties that won compared to 2003 and parties that lost. One party that was actually a winner, the Socialist Party shows lower levels of trust. Two losing parties, the Liberals and the LPF have high levels of trust, compared to the other parties. The only voters that seem to have relatively low levels of trust in the DREs are the voters who voted blank. The same picture appears when looking at confidence levels with regard to paper ballot voting, as shown in Figure 3b. Again, one of the winning parties, the SP shows lower levels of confidence. The LPF, which lost all its seats, has a high level of trust. These figures do suggest that there is no winner or loser effect on voter trust in voting technology apparent in Dutch elections.

## 6 Reforms and Voting Technology: Reforms in a Polarized Electorate

The partisan differences that exist in voting technology in the United States may continue into the future, given the polarized views of Americans and the fact that Americans are “well sorted” both ideologically and geographically [e.g., AS08, Bi08]. This sorting makes politics in the United States self-reinforcing; individuals tend to be involved in self-referential worlds, interacting primarily with individuals who share their views. The debate over election fraud in the United States, for example, has a strong partisan bent as do debates over making voter registration and voting easier [AAB09, AHH08]. Given this partisan dynamic, how does the future debate over electronic voting look going into the future?

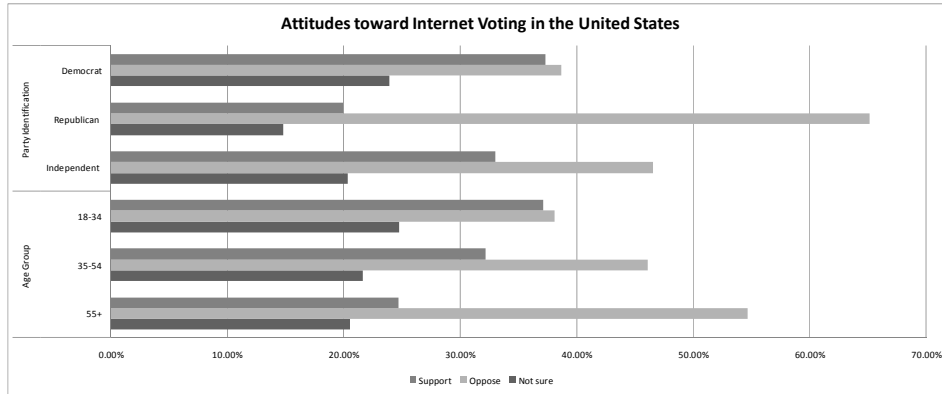
We can begin to see the potential future debate over electronic voting in recent survey data that asked 32,800 individuals who participated in the 2008 CCES survey conducted by Polimetrix. The survey asked individuals the following question: “States have tried many new ways to run elections in recent years. Do you support or oppose any of the following ways of voting or conducting elections in your state?” One reform the individuals were asked about was “Allow absentee voting over the Internet.” Respondents were given the following response options: “Support,” “Oppose,” and “Not Sure.”<sup>7</sup> Given the movement toward Internet voting that is currently either ongoing or under consideration across western countries, it is interesting to consider the attitudes of Americans toward these reforms and how the partisan nature of the debate over this reform might shape up.<sup>8</sup>

In Figure 4, we see that overall support for Internet voting in the United States is not tremendously high; 31.0 percent support Internet voting, 46.9 percent oppose this reform, and 22.1 percent are undecided. However, there are clear differences in attitudes between Democrats, Republicans, and Independents and between younger and older voters on this issue. First, Republicans are much more opposed to Internet voting than are Democrats. Only 20 percent of Republicans support the idea of Internet voting and 65.2 percent of Republicans oppose it. By contrast, Democrats have a more diverse set of viewpoints and are more undecided on it; 37.4 percent of Democrats support Internet voting and a roughly equal percentage (38.7 percent) of Democrats oppose it. In addition, almost 24 percent of Democrats are undecided about Internet voting compared to only 14.9 percent of Democrats. There are also differences in attitudes toward these reforms vary across age cohorts as well. Younger individuals have more positive views toward Internet voting than do older individuals, who are more negatively inclined toward this reform.

---

<sup>7</sup> Individuals could also skip the question. There were 26,066 valid responses to the survey question. The data in Figure 6 have 26,066 as the total number of cases analyzed, except for the partisan question, where individuals who did not state a party identification were excluded. For that table, 23,330 is the denominator.

<sup>8</sup> For a review of these reforms, see AH04, AH08a, MT04, TM05, TSB07.



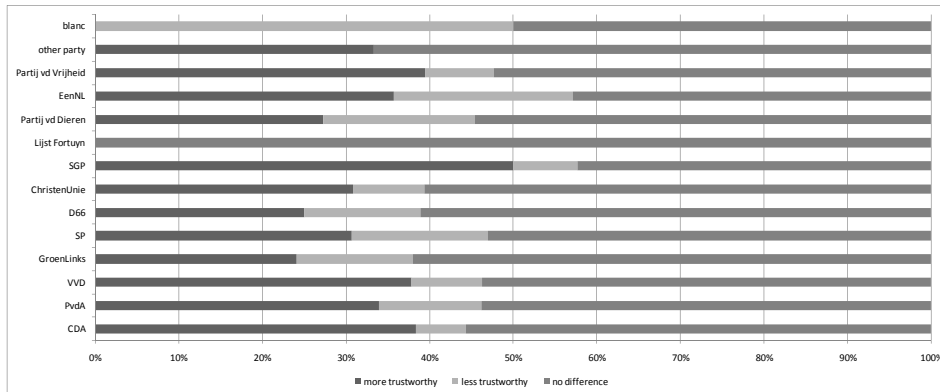
**Figure 4:** Internet Voting Attitudes in the United States

These partisan differences are not surprising, given that Democrats have used Internet voting in primary elections more than have Republicans, including the 2000 Arizona Democratic Presidential primary elections, the 2004 Michigan Presidential caucus, and the 2008 Presidential primary held by overseas voters. In addition, work internationally has shown differences in attitudes and in the use of Internet voting, especially in Estonia, across age groups. The key question is whether this reform will become one that has a partisan component, like the debate over electronic voting does in the United States, or whether Internet voting will be a reform that is debated without partisan suspicions. In Table 4, we see that there is not strong support for Internet voting in the Netherlands either.

Trust in Internet Voting	
Very Much	4,3%
Much	27,3%
Not Too Much or Too Little	21,2%
Little	33,7%
Very Little	13,4%

**Table 4:** Trust in Internet Voting

In the Netherlands, the debate on the use of voting technology led to an abandonment of all electronic forms of voting [JP09, Lo08]. These decisions were made after the 2006 parliamentary elections. Almost all parties in Parliament, whether they won or lost seats during this election, supported the return to paper ballot voting. This is remarkable, since most voters did express a higher trust in voting machines than in paper ballots as shown in Figure 5.



**Figure 5:** Trustworthiness of Voting Machine Compared to Paper Ballot

After the municipal elections of March 2010, the question whether or not to use electronic voting again became a topic of debate. During these elections, in which everybody voted with paper ballot, the results of the count were subject of discussion in a number of municipalities. There were problems with the proxy votes, in some cases two people were in the voting booth together and the votes were not always counted correctly.<sup>9</sup> Fifteen municipalities, including Rotterdam, the second largest city in the Netherlands, decided to do a recount of all the votes. This led to some cases of a seat being awarded to a different party. Parties that felt they had been ‘cheated’ out of seats raised the issue of trustworthiness. Some parties even demanded a revote. In Rotterdam, the two biggest parties, the PvdA and a local party, Leefbaar Rotterdam, achieved the same number of seats. Since by custom, the largest party is the first to try to form a coalition to govern, the exact number of votes that either party received became of importance. The PvdA had the most votes. Leefbaar claimed that a lot of the poll workers in Rotterdam were supporters of the PvdA and that this had helped them to become the biggest.<sup>10</sup> After the recount, which was done by different people and under scrutiny of the parties and the press, the PvdA still received the most votes.<sup>11</sup>

The municipal elections did show a more politicized debate on the use of certain voting techniques. The abandonment of the voting machines apparently did not mean that the same pathologies did not occur. On the contrary, where the use of voting machines had not raised issues on politicization of the voting process, with the paper ballot elections, there were politicized recounts. The security of the proxy voting system was questioned and issues were raised with regard to the accuracy of the results when paper ballots are used. This led to a strong call from the poll workers and the local election boards to return to a form of electronic voting. So far however, the government has stated that they have no intentions to do so.<sup>12</sup> Parliament has agreed to this course of action. Apparently,

<sup>9</sup> <http://www.nd.nl/dossiers/politiek/gemeenteraadsverkiezingen-2010> (in Dutch only, May 23, 2010).

<sup>10</sup> <http://www.deweekkrant.nl/pages.php?page=1112223> (in Dutch only, accessed May 23, 2010).

<sup>11</sup> <http://www.ad.nl/ad/nl/1038/Rotterdam/article/detail/469496/2010/03/12/Hertelling-Rotterdam-PvdA-blijft-grootste-partij.dhtml> (in Dutch only, accessed May 23, 2010).

<sup>12</sup> [http://www.telegraaf.nl/binnenland/6223820/\\_Rood\\_potlood\\_niet\\_ter\\_discussie\\_.html](http://www.telegraaf.nl/binnenland/6223820/_Rood_potlood_niet_ter_discussie_.html) (in Dutch only, accessed May 23, 2010).



the decisions made by government and parliament in 2007 and 2010 were not solely based on confidence in electronic voting, but also on other factors. Because electronic voting was in the past uncontroversial in the Netherlands, until now, there are hardly any studies that have focused on the motives of political parties to favor certain types of voting technology. More research is therefore needed to find out what motivated parties to abandon electronic voting.

## **7 Conclusions and Implications**

Voter confidence in election results is of the utmost importance for the legitimacy of the chosen legislators. When the trustworthiness of the techniques and methods that are used during the elections become subject of a debate, this can have a negative impact on the confidence of voters. Voters or NGOs can raise the question of trustworthiness, as was the case in the Netherlands, but losing candidates can also be tempted to use the voting system as a scapegoat, as seems to happen in the United States and even in the 2010 municipal elections in the Netherlands. In the United States, the 2000 election raised critical questions about the performance of the nation's voting system and these questions have continued to resonate through the polity. Most troubling, they are creating questions among some voters about the security and accuracy of various voting technologies. These concerns have polarized characteristics in some cases, especially in regards to voting modes—voters tend to be less confident in by-mail voting compared to in-person voting—and across voting technologies, with liberals and Democrats less confident in DREs compared to conservatives and Republicans. In controversial elections, such as in 2000, 2002, 2004, and in certain specific races in 2006, voting technology has been the focus of media and political scrutiny, used to explain election losses and to question the voting process.

In the United States, one reason why confidence is so important is that losers are just that, losers. There is no proportional representation in Congress or in the Executive, so voting for a losing candidate can mean that your preferences will not be represented in the political debate. Obviously, there are people who vote for losing candidates, but the party they support may control the Congress or one chamber therein. However, in proportional systems, a voter's party can finish third or fourth and still get a plum portfolio in a coalition government. In the American context, losing can be a more bitter experience. The evidence points toward a clear loser effect on confidence in voting technology.

The Dutch case seems to support this thesis. In the proportional system that is used in the Netherlands, losing parties can be part of government. The data from the 2006 elections shows that the level of voter confidence in voting technology is not noticeably influenced by the fact of whether or not the party a person voted for won or lost in the elections. There are differences between parties in the level of voter confidence, but more research is needed to find what factors cause this. The March 2010 elections did show an increasing politicization of the debate on voting techniques. It remains to be seen whether or not this trend will continue.

As electronic voting technology use expands, debates over its efficacy have expanded as well. The Dutch experience with electronic voting is a case in point, where electronic voting technologies came under sharp scrutiny and were eventually removed from use [Lo08]. In the Netherlands, the advocates and opponents of electronic voting were not divided on party lines. Neither were they following the preferences of the voters, since these voters even expressed more confidence in electronic voting than in paper ballot voting. However, if such debates become politicized, they can undermine trust and confidence in the voting process. As advocates and politicians link to address concerns about certain voting technologies, the pro and con sides of these debates can take on partisan dimensions, with one party or set of parties associated with liking or disliking one voting technology or mode of voting over another. In the American context, such linkage has occurred with electronic voting, as Democrats and liberals associate DREs with pro-Republican interests. After the 2008 elections, these positions may have shifted. If positions in the debate on the use of electronic voting depend solely on partisan dimensions, other objectives of electronic voting, such as the improvement of voter accessibility may be overlooked. Other countries (e.g., Estonia) have much clearer core ideals about the efficacy of electronic voting and these core ideals make confidence in the system higher [TSB07]. The American example is a cautionary one; when voting technologies are politicized, they can undermine confidence in the voting process.

## Bibliography

- [AS08] Abramowitz, A. I., and K. L. Saunders. 2008. Is polarization a myth? *Journal of Politics* 70 (2): 542–555.
- [AH04] Alvarez, R. M., and T. E. Hall. 2004. *American attitudes about electronic voting*. Salt Lake City: Center for Public Policy and Administration at the University of Utah.
- [AH08b] Alvarez, R. M., and T. E. Hall. 2008b. Building secure and transparent elections through standard operating procedures. *Public Administration Review* Sept/Oct.: 827–837.
- [AH06] Alvarez, R. M., and T. E. Hall. 2006. Controlling democracy: The principal-agent problems in election administration. *Policy Studies Journal* 34 (4): 491–510.
- [AH08B] Alvarez, R. M., and T. E. Hall. 2008a. *Electronic elections: The perils and promise of digital democracy*. Princeton, NJ: Princeton University Press.
- [AH04] Alvarez, R. M., and T. E. Hall. 2004. *Point, click, and vote: The future of Internet voting*. Washington, DC: Brookings Institution Press.
- [AAB09] Alvarez, R. M., S. Ansolabehere, A. Berinsky, G. Lenz, C. Stewart III, et al. 2009. *2008 survey of the performance of American elections*. Boston/Pasadena: Caltech/MIT Voting Technology Project.
- [AHL08] Alvarez, R. M., T. E. Hall, and M. Llewellyn. 2008. Are Americans confident their ballots are counted? *Journal of Politics* 70 (3): 754–766.
- [AHL09a] Alvarez, R. M., T. E. Hall, and M. Llewellyn. 2009a. *The winner's effect. Voter confidence before and after the 2006 elections*. Working Paper. Pasadena, CA. <http://vote.caltech.edu/>.
- [AHL09b] Alvarez, R. M., T. E. Hall, and M. Llewellyn 2009b. Voter confidence in partisan primary elections. Working Paper. Pasadena, CA. California Institute of Technology.
- [AHS08] Alvarez, R. M., T. E. Hall, and B. Sinclair. 2008. Whose absentee votes are returned and counted: The variety and use of absentee ballots in California. *Electoral Studies*. 27: 673-683.
- [ABB05] Anderson, C. J., A. Blais, S. Bowler, T. Donovan, O. and Listhaug. 2005. *Losers' consent: Elections and democratic legitimacy*. Oxford: Oxford University Press.
- [AS05] Ansolabehere, S., and C. Stewart III. 2005. Residual votes attributable to technology. *Journal of Politics* 67 (2): 365–389.
- [AS07] Atkeson, L. R., and K. L. Saunders. 2007. Voter confidence: A local matter? *PS: Political Science and Politics* 40: 655-660.
- [AAH09] Atkeson, L. R., R. M. Alvarez, and T. E. Hall. 2009. Government trust and voter confidence: How similar are they? Paper presented at the annual meeting of the *Midwest Political Science Association*, Chicago, IL: April 2-5, 2009.
- [AAH07] Atkeson, L. R., R. M. Alvarez, and T. E. Hall. 2007. *The New Mexico election administration report: The 2006 November general election*. Albuquerque: University of New Mexico.
- [Bi08] Bishop, B. 2008. *The big sort*. New York: Houghton Mifflin.
- [VTP01] Caltech/MIT Voting Technology Project. 2001. *What is/what could be*. Boston/Pasadena: VTP.
- [CF02] Carter, J., and G. Ford. 2002. *To assure pride and confidence in the electoral process*. Washington, DC: Brookings Institution Press.
- [CSED08] Center for the Study of Elections and Democracy. 2008. *Evaluating the quality of the voting experience*. Provo, Utah: Brigham Young University.
- [CMM08] Claassen, R. L., D. B. Magleby, J. Q. Monson, and K. D. Patterson, K. D. 2008. At your service: voter evaluations of poll worker performance. *American Politics Research* 36: 612–634.

- [Fo06] Fortier, J. C. 2006. *Absentee and early voting. Trends, promises, and perils.* Washington, DC: AEI Press.
- [GH09] Gronke, P., and J. Hicks. 2009. Re-examining voter confidence as a metric for election performance. Paper presented at the annual meeting of the *Midwest Political Science Association*, Chicago, IL: April 2-5, 2009
- [Ha09] Hall, T. E. 2009. Voter attitudes toward poll workers in the 2008 election. Paper presented at the annual meeting of the *Midwest Political Science Association*, Chicago, IL: April 2-5, 2009.
- [HMP09] Hall, T. E., J. Q. Monson, and K. Patterson, K. 2008. Poll workers and American democracy. In *Democracy in the States: Experiments in Election Reform*, ed. B. Cain, T. Donovan, and C. Tolbert. Washington, DC: Brookings Institution Press, 35-54.
- [HMP09] Hall, T. E., Q. Monson, and K. Patterson, K. 2009. The human dimension of elections. How poll workers shape public confidence in elections. *Political Research Quarterly*. 62, No. 3, 507-522
- [HNH08] Herrnson, P. S., R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. C. Conrad, and M. W. Traugott. 2008. *Voting technology. The not-so-simple act of casting a ballot.* Washington, D.C.: Brookings Institution Press.
- [JP09] Jacobs, B., and W. Pieters. 2009. Electronic voting in the Netherlands. From early adoption to early abolishment. In *Foundations of security analysis and design V: FOSAD 2007/2008/2009 tutorial lectures, lecture notes in computer science, vol. 5705*, ed. A. Aldini, G. Barthe, and R. Gorrieri. Berlin: Springer-Verlag. 121-144.
- [KSR04] Kohno, T., A. Stubblefield, A. D., Rubin, and D. S. Wallach. 2004. Analysis of an electronic voting system. In *IEEE symposium on security and privacy*. IEEE Computer Society Press. 1-23.
- [Lo08] Loeber, L. 2008. E-voting in the Netherlands; from general acceptance to general doubt in two years. In *Electronic voting 2008, GI lecture notes in informatics*, ed. R. Krimmer and R. Grimm, 21–30. Bonn, Germany: Gesellschaft für Informatik.
- [MT04] McNeal, R., and C. Tolbert. 2004. Support for Internet voting in the United States. In *Electronic voting and democracy. A comparative analysis*, ed. N. Kersting and H. Baldersheim. London: Palgrave.
- [St09] Stewart III, C. 2009. Election technology and the voting experience in 2008. Paper presented at the annual meeting of the *Midwest Political Science Association*, Chicago, IL: April 2-5, 2009.
- [St06] Stewart III, C. 2006. Residual vote in the 2004 election. *Election Law Journal* 5 (2): 158–169.
- [TV03] Tomz, M., and R. P. Van Houweling. 2003. How does voting equipment affect the racial gap in voided ballots? *American Journal of Political Science*, 47, 1: 347-361.
- [TM05] Trechsel, A. H., and F. Mendez. 2005. *The European Union and e-voting. Addressing the European Parliament's Internet voting challenge.* London: Routledge.
- [TSB07] Trechsel, A. H., G. Schwerdt, F. Breuer, R. M. Alvarez, and T. E. Hall. 2007. *Report for the Council of Europe, Internet voting in the March 2007 parliamentary elections in Estonia.* Strasbourg: Council of Europe.

# Double-entry Accounting Provides Software-Independent Algorithm for Confirming the Integrity of Automated Election Tallies

Roberto S. Verzola

Institute of Mathematics  
University of the Philippines  
Diliman Campus, Quezon City  
Philippines  
[rverzola@gn.apc.org](mailto:rverzola@gn.apc.org)

**Abstract:** This paper proposes the use of double-entry accounting to maintain the integrity of election data as they go through the processes of counting, canvassing, consolidation, and reporting. Double-entry accounting brings to election tallies its well-known benefits of minimizing errors, deterring fraud, and maintaining the integrity of large collections of numeric data. Its superiority to single-entry methods, which are currently in use in the electoral tallies of most countries, is universally acknowledged in business and is increasingly appreciated by governments. This paper describes how double-entry accounting can be applied to election tallies, proposes the equations that govern the accounting of ballots and votes, and discusses the advantages that this brings. It also responds to arguments that the method is not appropriate for election tallies.

## 1 Introduction

Persistent concerns about the integrity of electronic voting (e-voting) systems have slowed down their adoption in many countries.

One response to this concern is the suggestion to make e-voting systems “software-independent.” For instance, the U.S. National Institute of Standards and Technology (NIST), with the support of the U.S. Association of Computing Machinery (ACM), had recommended to the Technical Guidelines Development Committee (TGDC) that only software-independent e-voting systems be certified. The TGDC adopted this recommendation and, in turn, proposed it to the U.S. Election Assistance Commission.

Thus the TGDC Voluntary Voting Systems Guidelines (VVSG) now include software independence as a voting system requirement: “Software independence (Rivest06) means that an undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results. All voting systems must be software independent in order to conform to the VVSG” [TG07].

One way to make an e-voting system software independent is to retain a paper ballot as the original document expressing voter intent. Since errors due to software cannot alter the paper ballot, these errors can be detected in a ballot-based recount. Thus in their paper cited in the VVSG, Rivest and Wack call the paper ballot approach “strongly software-independent” [RW06].

This paper proposes the use of the double-entry accounting method to provide a simple, robust, and time-tested way to detect errors in voting machine counts that is also software-independent.

## 2 Data items as equalities

Double-entry accounting is based on an algorithm that detects errors in real-time from a numeric data set, regardless of its size, by imposing a consistency check on every data item that goes in and comes out of the data set. This consistency check is implemented by requiring every data item to be recorded *as an equality*. As data items are accumulated, recorded, totaled, reported, and rerecorded at various levels of data consolidation, equal amounts are being manipulated all the time. Thus the totals of the left and right hand sides of the equality (henceforth, LHS and RHS) must remain equal *at all times*.<sup>1</sup> Most errors in recording, arithmetic, and reporting will cause the equality to fail. So if the consistency check is done in real-time, errors will be automatically detected in real-time too. This method can detect errors in the original data set—as submitted by optical ballot scanners or human counters, for instance—as well as errors in the data set introduced by the machines, software, or human operators that update, manipulate, and report this data set. As long as the raw data sets are made available, this method can be implemented independently of the specific software or hardware platform used in an e-voting system. The accounting profession implements this automatic checking by recording the two sides of the equality in two corresponding columns, and regularly ensuring that the two columns are “balanced,” i.e., their totals are equal.

Over the centuries, businesses and the accounting profession have developed and standardized systems and procedures—familiar to managers, auditors, accountants, and bookkeepers worldwide—for maintaining a generally high level of data integrity using this method, which can be implemented manually or in software. When businesses shift from manual to computerized data operations, more sophisticated means of ensuring data integrity become possible. Still, this highly-robust, time-tested, and standardized double-entry method is invariably retained as a way to keep data operations machine- and software-independent. So it remains a universal workhorse of businesses.

First described in the late fifteenth century, the superiority of the double-entry system to single-entry methods has made it the standard system of business accounting for several hundred years throughout the world.

---

<sup>1</sup> Accountants call the left-hand side (LHS) of the equality debit (Dr), and the right-hand side of the equality credit (Cr).

Increasingly, double-entry accounting has made inroads in governments too, although they have been slower in recognizing its benefits. It was only in the nineteenth century when it saw widespread use in the public sectors of France (1815) and Great Britain (1829) [Ni01]. Some countries adopted the system only in the late twentieth century. In the first few years of the twenty-first century, the European Commission was still using single-entry accounting [Kh02], shifting to the double-entry system only on 1 January 2005 [EU06]. In other countries, especially among local governments, its introduction is still in the planning stages, as part of public sector financial reform.

It is therefore understandable if election authorities have not yet made the conceptual leap to adopt double-entry accounting in vote tabulations.

### **3 Election tallies today: single-entry**

Most election tallies today still use the single-entry accounting method of recording and accumulating individual isolated numbers, not equalities. This method is susceptible to undetected errors that can be passed on to intermediate levels of vote consolidation up to the final tabulation. The common practice of recording, maintaining, and reporting vote totals at every level of consolidation is *not* double-entry accounting. Few election authorities strictly enforce a requirement that blanks (or undervotes) and invalid votes (such as overvotes) be counted, recorded, reported, and included in the totals at every consolidation level, in the same way that votes for candidates are. If small unexplained discrepancies arise which are deemed immaterial to the final outcome, local voting officials tend to simply agree to “clean up” the figures. Few, if any, set aside special accounts to keep track of small discrepancies that could not be reconciled in time. Since special accounts such as blanks, invalids, missing, and excess votes are necessary to implement a true double-entry election accounting system, there cannot be many countries, municipalities or election jurisdictions, if indeed there is even one, that use this system in vote tabulations and election accounting today.

### **4 Every vote counts**

It is sometimes argued that the requirements are more stringent in accounting for money than in accounting for votes. According to this argument, a win by a small margin is no different from a win by a large margin. Hence, the argument goes, accuracy to the last vote is not as important as accuracy to the last cent.

On the contrary, accuracy to the last vote is also important for the following reasons:

- A single vote may not make a difference to an election outcome, just as a single cent hardly makes a difference to a businessman’s bottom line. But a one-vote or one-cent discrepancy may hide larger, but undetected discrepancies in the system. Worse, they may indicate procedural or system flaws or loopholes that can result in more serious errors in the future. Businesses take one-cent discrepancies seriously not because one

cent matters to them, but to make sure that the discrepancy does not hide more serious problems in their accounting system. Just as banking automation made possible large-scale fraud through the accumulation of fractional cents and round-off errors, election automation makes possible fraudulent election outcomes through the accumulation of small discrepancies in many voting precincts. Through its simple consistency check of equalities, the double-entry algorithm can detect even single-vote discrepancies, as soon as they occur. This imposes, at very low cost, a high-quality standard for election data sets and voting machines, which can only enhance the public perception of e-voting systems.

- The size of a winning margin is significant as far as a winner's mandate is concerned. Thus, vote discrepancies may not affect the final outcome, but they may still affect the publicly-perceived mandate or lack of mandate of an election winner. In the 2004 Philippine election for president, for instance, the winner who was eventually proclaimed was secretly caught in taped telephone conversations, subsequently made public, as she instructed a senior election official in manipulating election results to ensure herself a winning margin of at least one million votes.

- In many countries, the sanctity of the ballot is enshrined in their constitution, which emphasizes that every single vote—and voter—counts. To win public trust, it is best that e-voting system vendors adopt a similar attitude.

## 5 Basic features of a double-entry election tabulation system

This paper describes the basic features of a double-entry election tabulation system for a one-slot position (e.g., president) and for a multiple slot position (e.g., senator, where twelve slots are available in the Philippine case). The examples given are also applicable to other single- or multi-slot positions. It is assumed that voter-prepared paper ballots are used, for scanning by optical ballot scanners.

In business accounting, the fundamental equalities are **Assets = Capital + Liabilities** and **Revenue = Expenses + Profit**. In double-entry election accounting, the fundamental equalities are discussed below.

Ballots are the heart of the election process, because they represent a permanent record of voter intent, the “will of the people.” In keeping track of ballots, the following **ballot equation** can be used:

**Received Ballots + Excess Ballots = Cast Ballots + Spoiled Ballots + Unused Ballots + Missing Ballots**

**Received Ballots** record the number of ballots allotted to the voting jurisdiction. Ballots end up as either **Cast** (i.e., given to the voter and filled out), **Unused**, or **Spoiled**. The total ballots cast, unused or spoiled should equal the number received, which accounts for every single ballot, at every level of consolidation. The **Excess** and **Missing** accounts are used to force a balance and transparently record anomalous situations where some ballots could not be accounted for, even after repeated efforts to do so.



## 6 The ballot status report

Table 1 shows a sample ballot status report for one precinct, based on the ballot equation:

Table 1. Ballot Status Report		
Ballot type	LHS (Dr)	RHS (Cr)
Received	200	
Excess	0	
<b>Cast</b>		45
<b>Spoiled</b>		3
<b>Unused</b>		152
<b>Missing</b>		0
Column Total	200	200

Under Ballot Type, the RHS accounts (Cast, Spoiled, Unused, and Missing) are indented, in accordance with common accounting practice. The LHS of the two numeric columns represents the total number of ballots received by the polling center. The RHS breaks down how these ballots ended up. The LHS total is equal to the RHS total and the report is balanced. If an imbalance exists, the reason for the discrepancy must be identified and corrected. If it persists—which is anomalous—and time does not permit another round of double-checking, the discrepancy should be recorded on the side that is smaller, as Excess or as Missing. This balances the report in a transparent manner, which allows for a subsequent audit later if the Excess/Missing accounts appear abnormally high.

In every ballot are the votes, the key to the whole process. Two equations govern the accounting of votes:

**No. of Slots for Position x Cast Ballots = Available Votes**

**Available Votes + Excess Votes = Valid Votes + Invalid/Blank Votes + Missing Votes**

For executive positions like president or vice-president, there is only one slot for the winner. Hence, the number of validly cast ballots is also the number of total available votes. For legislative positions like senator or councilor, there are usually several slots, fixed by law. Then, the number of total **Available Votes** is the number of validly **Cast** ballots multiplied by the **number of slots** available for the position being contested. Available votes can end up three ways. They can be cast as **Valid** and counted in favor of a particular candidate. They can be deemed **Invalid**; for example, a non-candidate is voted in or if two names or more are listed or marked (also called an “overvote”), or for any other reason as defined by law. Finally, an available vote can remain **Blank** (also called an “undervote”). The total votes counted in favor of each candidate plus the

Invalid/Blank votes should equal the Available Votes. The Caltech/MIT Voting Technology Project lumps together all Invalid/Blank votes that did not go to any candidate under the term “residual” votes, and studied the role of variations in county, technology, demography, and other factors that tend to increase or decrease them [AS04].

The vote equation was separately proposed in 2004 by Saltman as well as by Jones. Saltman suggested that “for each contest, the total number of ballots cast multiplied by the number of legitimate votes cast per ballot should equal the sum of votes assigned to each candidate plus the number of overvotes plus the number of undervotes”: [Sa04]. Jones proposed essentially the same equation  $B = C + O + U$ , where B is the number of “ballots found in the ballot box,” C is the “sum of votes for specific candidates,” O is the “number of overvotes,” and U the “number of undervotes” [Jo04]. Writing about e-voting systems, both authors also referred to double-entry methods, but in the context of financial transactions and business accounting. Saltman wrote: “As in accounting, where double-entry bookkeeping has been standard for about a century, there needs to be cross-checking that distributes the total responses possible with each ballot to each category that could have been used by each user” [Sa04]. And Jones wrote: “Thus, we issue carbon copies of the paper receipt for a financial transaction to both parties in the transaction, and we develop systems such as double-entry bookkeeping” [Jo04]. Neither author, however, proposed setting up special Excess or Missing Accounts, which are essential to an auditable double-entry accounting system in election tallies.

## 7 Vote status report: single-slot positions

Table 2. Vote Report, for President		
No. of Slots: 1	Cast Ballots: 150	
Votes	LHS (Dr)	RHS (Cr)
Available	150	
Excess	0	
<b>Invalid/blank</b>		12
<b>Candidate 1</b>		70
<b>Candidate 2</b>		50
<b>Candidate 3</b>		18
<b>Missing</b>		0
Column Total	150	150

Table 2 is a sample vote report for a single-slot position in one precinct, where candidates 1, 2 and 3 are hypothetical candidates.

Available Votes is equal to the No. of Slots times the Cast Ballots in the Ballot Report (taken from Table 1). Invalid/Blank Votes are the slots which have been left blank, which contain unrecognizable names, or which were not counted for one reason or another.

Procedure-wise, the main difference between the double-entry and single-entry methods is the extra work, throughout the consolidation process at every level, of keeping track of invalid/blank votes—votes in a validly cast ballot that did not go to any candidate. This extra work is equivalent to an additional candidate in every position. *This data is essential in a double-entry election accounting system, to make possible a balanced vote report.*

As in standard accounting practice, the LHS and RHS column totals (debits and credits in accounting parlance) must balance before the next step in the process can proceed. The Excess/Missing accounts can be used to force a balance in a transparent way, to document unexplained discrepancies in the count. These should also be recorded, added up, and reported throughout the process, at every level of consolidation.

## **8 Vote status report: multiple-slot positions**

In multi-slot positions, voters may write several names on the ballot for the same position. In this case, Available Votes is equal to Cast Ballots (this number is taken from the Ballot Status Report, Table 1) times the No. of Slots (1,800 equals 150 times 12). Table 3 below is a sample vote report for a multi-slot position in one precinct.

Counting the invalid/blank votes in a multi-slot contest is only slightly more complicated, because each ballot may hold a mix of valid and invalid/blank votes. Aside from the valid votes per candidate in the contest, the number of invalid/blank votes in the ballot must also be counted and recorded. Note that for each position, the total of the valid votes per candidate plus the Invalid/Blank Votes should always equal the number of slots available for the position (12, in the example given).

Table 3. Vote Report, for Senator		
No. of Slots: 1	Ballots cast: 150	
Votes	LHS (Dr)	RHS (Cr)
Available	1800	
Excess	0	
Invalid/blank		640
Candidate 1		110
Candidate 2		105
Candidate 3		100
Candidate 4		95
Candidate 5		90
Candidate 6		85
Candidate 7		80
Candidate 8		75
Candidate 9		70
Candidate 10		65
Candidate 11		60
Candidate 12		55
Candidate 13		50
Candidate 14		45
Candidate 15		40
Candidate 16		35
Missing		0
Column Total	1800	1800

## 9 Special accounts: the Excess/Missing accounts

Election officials point out that a vote count at the precinct level often ends up with a few extra or missing ballots or votes which could not be accounted for. Then they simply agree among themselves to sweep these small discrepancies under the rug and send in a report with consistent totals.

Under a true double-entry system, separate accounts (often called “errors and omissions”) are created and maintained, so that discrepancies which cannot be explained within the time available to the election authorities are transparently recorded under such accounts, thus maintaining the required balance between the two columns. These accounts can be called Excess (a LHS account) and Missing (a RHS account). The following algorithm will force a vote report to balance:

- compute the difference between the two column totals;
- record the difference under the column with the smaller total, as Excess if the LHS-column total is smaller or as Missing if the RHS-column total is smaller;
- recompute the column totals, which should now balance.

The Excess/Missing accounts record a potential vote padding/shaving problem, which election officials are unable to resolve immediately. Documenting the forced balance in such a transparent manner facilitates a subsequent audit should it prove to be necessary.

These accounts should be maintained, recorded and reported at every level of consolidation, together with vote and ballot counts.

## 10 Advantages of double-entry election accounting

If governments are slow to recognize the superiority of double-entry election accounting, the private sector, including the e-voting industry, can take the initiative in its advocacy, citing their current business accounting practices. The latter, for one, should welcome the strict consistency check on the data, which facilitates machine and software testing, helps improve software quality, and gives them more confidence in the internal consistency of their system, a clear marketing advantage. For governments, election authorities and the ordinary voter, double-entry election accounting will bring the following specific advantages:

- The double-entry method is a simple, easy-to-understand, highly standardized, and widely-known algorithm for enforcing data consistency that has withstood the test of time. Its universal use in the business sector and widespread use in the government sector attests to its superiority over the single-entry election tabulation method that is used today in most countries and localities. Failure to balance is an automatic warning about problems in the election data set. It can flag clerical errors such as recording or addition mistakes that often creep in and stay undetected when single-entry methods are used, or errors introduced into the data set by the machine or its software. It can also locate errors more easily by testing which section of the data set fails to balance.

- It provides a logical step-by-step upgrade path for electoral reform and modernization. In countries like the Philippines, where the manual system of election tabulation itself suffers from substantial flaws [Ca04], undertaking automation before existing systemic flaws themselves are corrected seems foolhardy. Introducing a new level of complexity on a shaky foundation of uncorrected systemic and procedural defects is a formula for expensive failure. Automating a flawed single-entry system could result in an equally flawed automated system that would sooner or later have to be redone. Given the costs and risks associated with any automation project, it would make sense for countries which are considering election automation to first modernize their tabulation system by adopting double-entry accounting. This simple, low-cost step can tap existing pools of expertise that even the least developed countries already have and immediately provide dramatic improvements in minimizing clerical errors, maintaining the integrity of election data, and deterring fraud.
- On the stable platform of a modern election accounting system, countries may choose to upgrade to an intermediate hybrid system that uses spreadsheet software to implement the modernized method with computers, or they can skip this step and proceed directly to full automation, using the same double-entry system. In each upgrade step towards automation, the double-entry system provides a built-in check during the period of conversion that facilitates the process, in a way that is independent of vendors, machines, and software. Existing voting machines outputs in standard formats like Comma Separated Values (CSV) or Election Markup Language (EML) can be fed to third-party software to check for consistency using the double-entry system. Later, vendors may add an accounting module in their software to tally votes using double-entry methods, as an option or as a standard feature. Whether the election only covers one position (typical in the European context) or many (as in the U.S. and Philippine context), implementing the double-entry method involves the equivalent of accounting for the votes of an additional candidate. At worst, this means 50% more work if there are only two candidates vying for a position. In jurisdictions that are required to keep track of invalid/blank votes anyway, then this is not additional work at all.
- Strictly enforcing the requirement that reports balance will instill among election officials the discipline of providing necessary information which may not relate directly to the question of who won or lost the elections, but which is essential in detecting errors and other anomalies. This information includes the number of invalid/blank votes, the number of ballots cast (or voters who actually voted), the number of excess/missing ballots, and the number of precincts tallied. Under single-entry methods, the discipline of submitting such information may be imposed through instructions and administrative orders, but local election officials may simply ignore the requirement. In the Philippines, for instance, one-third (thirty-three out of ninety-eight) of the cities and provinces submitting their reports to the National Canvassing Board in the May 2007 elections did not provide the number of precincts tallied or the number of voters who actually voted [Ha97]. Under double-entry accounting rules, officials have no option, but to provide this information or the reports will not balance. Election officials may still force a balance by using special accounts specifically meant for this purpose, but doing so will make such moves transparent and subject to subsequent audit.

- The data consistency imposed by the double-entry system sets high-quality standards among e-voting vendors, forcing them to seriously check every single vote discrepancy in their machines and their software. In so doing, it enhances the public perception of the integrity of e-voting systems. While voting machines today do incorporate their own internal data checks, these checks may vary from one vendor to another, from one software to another, and from one model to another. A change of vendor, model or software version can introduce new problems that may not be detected in time, allowing errors to creep to higher levels of vote consolidation. By adopting an election tabulation platform that is independent of vendor, machine or software, mistakes and errors can be detected as soon as they are made.
- The additional information requirement to implement double-entry election accounting facilitates fraud control. The number of invalid/blank votes and the number of ballots cast set an upper-bound on the fraudulent votes that a dishonest candidate may accumulate and help detect ballot stuffing or its electronic equivalent. The number of excess/missing ballots, if significant, can trigger deeper investigation. The number of precincts tallied enables the computation of per-precinct averages and other statistics, which are useful indicators for detecting abnormal events, such as highly improbable or even impossible statistics as well as wild swings in some averages.

## 11 Limitations

Double-entry accounting should not be seen as a magic bullet that will eliminate election fraud. Even in business, where double-entry methods have been in use for several hundred years, fraudulent business practices continue to be uncovered and business owners as well as consumers must remain vigilant. For instance, double-entry methods will have no effect on electioneering with government resources, election overspending, or vote-buying. It cannot prevent the suppression of votes caused by fouling up voters' lists, precinct assignments or precinct locations. It cannot prevent goons from taking over voting precincts and operating the voting or counting machines directly. For best effect, it needs to be used together with other tools for fraud detection, investigation, and control.

In particular, two common errors will not be detected. If two erroneous, but offsetting errors are recorded, preserving the equality in the two columns, the errors are not detected. Thus, the double-entry method will not detect a vote padding/shaving operation where votes are subtracted from one candidate and the same number of votes is added to another candidate. If two entries in one column are switched, the column total will also stay the same. Thus vote switching between two candidates will not be detected either.

Despite its limitations, double-entry accounting will catch most clerical errors and a number of intentional errors, as every business will testify. It will make it more difficult for fraudulent entries to enter the system, and will save time that would otherwise be spent in detecting, locating, and correcting the errors that managed to creep in. Thus the double-entry approach is still recognized as an enormous advance compared to single-entry systems in minimizing errors, improving auditability, and reducing fraud.

## 12 Conclusion

Ballot and vote tabulation can benefit significantly from standard double-entry business accounting methods, which involve the recording of equal values at all times. By replacing the single-entry election tally methods practiced today in most countries with double-entry methods, slow election counts due to endless disputes over errors can be avoided and canvassing fraud can be detected more easily.

## Bibliography

- [AS04] Ansolabehere, S., and C. Stewart. 2004. Voting technology and uncounted votes in the United States. *Journal of Politics*.
- [Ca04] Carlos, C. et.al. 2004. *Electoral reform in the Philippines. Issues and challenges*, 89-92.
- [EU06] EU Committee of the UK House of Lords. 2006. *Financial management and fraud in the European Union. Perceptions, facts and proposals (Vol. II: Evidence)*.,61. <http://www.publications.parliament.uk/pa/ld200506/ldselect/ldecom/270/270ii.pdf/>.
- [Jo04] Jones, D. 2004. Auditing elections. *Communications of the ACM*, 47 10: 46-50. <http://portal.acm.org/citation.cfm?id=0922594.1022622/>.
- [Kh02] Bashir K. 2002. The European Union fails on financial accountability. *Contemporary Review*.
- [Ha07] Halalang Marangal. 2007. *A citizens' Audit of the 2007 senatorial elections. Report #4*. July 19: 3.
- [Ni01] Nikitin, M. 2001. The birth of a modern public sector accounting system in France and Britain and in the influence of Count Mollien. *Accounting History* May.
- [RW06] Rivest, R.; Wack, J. 2006. *On the notion of "software independence" in voting systems (draft version)*. July 28, 2006.
- [Sa04] Saltman, R. 2004. *Requirements for the evaluation of voting system security*. (presented to the Technical Guidelines Development Committee of the Election Assistance Commission of the U.S. National Institutes of Standards and Technology). Sep. 20. <http://vote.nist.gov/NISTpaper%20040920.pdf/>.
- [TG07] Technical Guidelines Development Committee. 2007. *Voluntary voting system guidelines recommendations to the election assistance commission*.



# **Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria**

Andreas Ehringfeld<sup>1</sup>, Larissa Naber<sup>1</sup>, Thomas Grechenig<sup>1</sup>,  
Robert Krimmer<sup>2</sup>, Markus Traxl<sup>3</sup>, Gerald Fischer<sup>1</sup>

<sup>1</sup>Vienna University of Technology  
Industrial Software (INSO)  
1040 Vienna, Austria  
 [{firstname.lastname}@inso.tuwien.ac.at](mailto:{firstname.lastname}@inso.tuwien.ac.at)

<sup>2</sup>E-Voting.CC gGmbH  
Competence Center for Electronic Voting and Participation  
1190 Vienna, Austria  
[r.krimmer@e-voting.cc](mailto:r.krimmer@e-voting.cc)

<sup>3</sup>Institut für Verwaltungsmanagement  
6020 Innsbruck, Austria  
[markus.traxl@verwaltungsmanagment.at](mailto:markus.traxl@verwaltungsmanagment.at)

**Abstract:** This paper discusses the recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting in light of the various attacks against the 2009 Austrian federation of students election. This election was the first instance of e-voting being implemented in a legally binding election in Austria. The question is if the recommendation published in 2004 is sufficient to handle real-world attacks against elections using e-voting. Based on the experience gained, several amendments to the recommendation are described.

## **1 Introduction**

According to [BSSL01] and [SZKK88] regular re-evaluation and re-assessment are fundamental security principles. The recommendation Rec(2004)11 on legal, operational and technical standards for e-voting [Rec04] of the Committee of Ministers to member states was developed by [CEIP04] between 2002 and 2004 and remained unchanged so far.

The effectiveness of Rec(2004)11 is analyzed based on the experience of a recent e-voting election, which suffered from various different attacks such as the first Denial of Service attack (DoS) against a legally binding electronic election worldwide.

## 1.1 Case Study: 2009 Austrian Federation of Students Elections

The Austrian federation of students elections (*Hochschülerinnen- und Hochschülerschaftswahlen*) takes place every two years. Of the 240,000 eligible voters only about 30% participate in the voting (average for the past thirty-six years). The voting period is three days long during which students at all universities in Austria can cast their votes. Prior to the 2009 election, paper-based voting was the only channel.

The idea using electronic voting for the federation of students election was first introduced in May 2000 by the national federation of students. As a consequence of [OeH00], the federation of students law was adapted to allow for the possibility of remote voting like e-voting or postal voting. This amendment led to an evaluation project [EV07] with the heads of the national federation of students and members of the Austrian ministry for science, focusing on e-voting at the University of Economics in Vienna.

In May 2007, the minister for science and research announced that e-voting would be an additional voting channel in the 2009 federation of students election. The project's goal was to enable students (such as students currently abroad) to cast their votes from home.

Four months later, the national federation of students published a statement in [OeH07] summarizing their objections to e-voting and concluding that the technology conflicts with the idea of a free and secret ballot. Despite the fact that the threats concerning e-voting are similar to those in almost all other modes of voting, especially all modes of remote voting (e.g., [AH04] and [AH08]), e-voting (and the risks involved) became a very controversial topic and thus one of the major topics of most election campaigns [OHER10].

Other than federation of students' resistance, the federation of students election made for a very good field study because it has a very high organizational complexity, despite the small number of potential voters (260,000), with more than 400 individual voting options across the twenty-one participating universities. The required technical skill and in-depth knowledge of the election process can rival any other Austrian election.

## 1.2 Methodology

The Edwards Deming Plan-Do-Check-Act Cycle (PDCA Cycle) [ED50] can be employed to improve upon Rec(2004)11.

*Plan (Hypothesis):* The question is whether the recommendations in Rec(2004)11 are sufficient to handle state-of-the-art real world attacks.

*Do (Experiment):* The 2009 Austrian federation of students election was chosen for this analysis because it is a recent example of a legally binding e-voting election, which used the Rec(2004)11 as a benchmark in the certification process and caused much controversy, which guarantees a high number of skilled attacks. The voter base - students - are skilled, creative, personally motivated, and equipped with both technical resources and enough time to plan and execute attacks. This makes them a force to reckon with.

*Check (Evaluation):* The various attacks during the electronic voting period are described; countermeasures are explained and related to the recommendations in Rec(2004)11. Identified gaps are analyzed and conclusions drawn. Potential amendments for further improvement of Rec(2004)11 are presented.

*Act:* The final step in the Deming Cycle lies within the biennial review cycle of Rec(2004)11 where additional recommendations and updates are discussed in detail.

### **1.3 Related Work**

Related work deals with security relevant aspects of e-voting from different views. The legal bearings of e-voting at the Austrian federation of students election are discussed in [KLSV09; LC10]. Papers like [SLBV09] show technical requirements while [XAMA05] deals with the procedural security and social acceptance in e-voting.

## **2 Recommendation Rec(2004)11 for E-Voting**

As part of the project [CoED04] the Committee of Ministers established an expert committee to prepare recommendations on legal, operational, and technical standards for e-voting in the years 2002–2004. The standards were adopted as Rec(2004)11 on 30 September 2004.

The measures included in the Recommendation are grouped into legal standards (thirty-five measures), operational standards (twenty-five measures), and technical requirements (fifty-three measures).

A continuous improvement process over a biennial cycle forms an integral part of the Recommendation. Currently additional recommendations derived from the experiences gained in recent projects are in discussion (see [CoEO10]). These amendments pertain to election observation and the certification processes of e-voting systems.

## **3 Certification of the E-Voting System of the 2009 Federation of Students Election Based on the Recommendation Rec(2004)11**

The timeline, activities, and responsibilities of the federation of students election are defined in the federation of students law [HSG98] and the election regulations [HSWO05]. Concerning e-voting this means that although the specifications are technology neutral and non-discriminatory, they shape how e-voting is implemented. The legal framework stipulates - among other aspects - that the e-voting system has to be approved by the Austrian data protection commission. Furthermore a certification process based on Common Criteria and the recommendation Rec(2004)11 has to be passed.

The technical components to be used—especially those related to the vote casting and the voters' authentication—have to be certified sixty days before the election by a certification authority according to the laws [Sig10], [HSG98] and election regulation [HSWO05].

The e-voting software (documentation, development process descriptions, architecture, security descriptions, threat analysis, technical descriptions, and source code) was audited between December 2008 and March 2009. On 27 March, the certification process ended successfully with the publishing of a certification [ASC09]. The published certificate stipulated key types and length, the compliance of processes for compilation, installation, configuration and operation of the software as well as operating conditions and security information to be released to the voters.

#### **4 Technical Attacks during the E-Voting Period**

E-voting, as a new voting channel in the 2009 Austrian federation of students election, was scheduled to be completed before the traditional on-site paper-based vote. Thus voters were able to cast their vote electronically between 18 May at 8:00 AM and 22 May at 6:00 PM. Students could choose whether they wanted to cast their votes electronically or vote in the traditional paper-based election between 26–28 May.

During the e-voting period, different attacks against the e-voting system, voters' acceptance, and the elections were discovered. Several of those attacks are described in the following sections.

##### **4.1 Distributed Denial of Service Attack**

Three days before the electronic election started preparations of a distributed Denial of Service (dDoS) attack were detected by the e-voting provider's security staff. An Austrian organization, registered as an organization working toward the use of information technology and telecommunication in a humane, socially responsible and private way, published a web tool which was touted as a harmless server availability checking tool. It was stated that everyone has the right to stress test (check the availability of) the e-voting system, and therefore it was absolutely legal, and practically mandatory, for as many people on as many PCs as possible, to do so, preferably day and night.

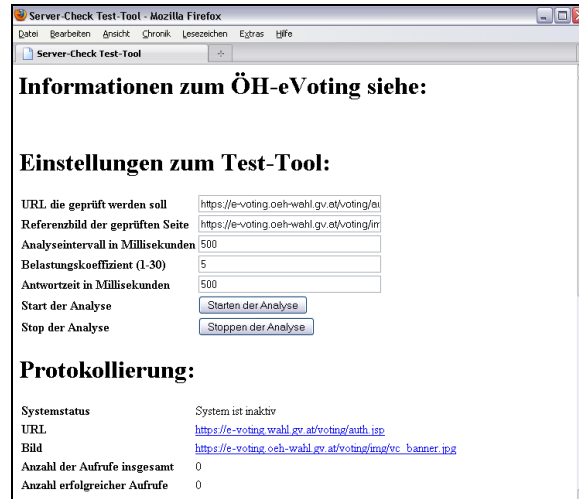


Fig. 1: GUI of the dDoS attack tool

The tool was written in javascript and opened a certain URL in invisible iframes as specified within a form textbox on the webpage (per default prefilled with the e-voting website). To avoid browser caching, random characters were added at the end of the URLs opened by the iframes. The other parameters defined how many iframes were opened/refreshed at the same time and at which interval. As the Austrian Computer Emergency Response Team (CERT.at) analyzed the potential danger of the script, even a brief analysis showed that a single PC using commonplace ADSL connectivity produced a permanent load of 10 Mbit/s on the web server.

The most interesting aspect of this attack is that although it was managed centrally, the attackers were distributed using their local resources and their local IP, which made the detection of attackers and possible blocking harder. Unlike most dDoS, this attack did not require a bot-net to be in place; the attackers participated willingly, even if sometimes unwittingly, to the potential problems caused.

An effective technical countermeasure to stop the attack was to include code written in javascript on every webpage of the e-voting system, which checked if the site was opened within a frame and reopened the site within the parent window, thus effectively stopping the tool.

This attack highlighted several of the practical problems stemming from denial of service attacks on e-voting systems. Even though dDoS attacks are not limited to e-voting systems, the ramifications of dealing with them in an e-voting setup are different. Blocking all incoming traffic from the source IP is a common measure. In an e-voting situation, this might deprive an unknown number of other voters of their legal voting rights. Configuration changes and parameter, or even software, adaptations are other popular counter measures. Again in the case of an e-voting system, it has to be considered whether these measures invalidate the existing certification and thus disqualify the whole election. The problem might be compounded by several adaptations

on the attackers' side forcing even more adaptations on the e-voting systems. These questions mostly belong in the realm of law and likely will keep legal practitioners occupied for years.

In case of the Austrian federation of students election, configuration changes were not necessary as the javascript code was already part of the e-voting system and certified months before. The original intention of the existing codes was to keep political parties and others from directly including the voting system via frames as part of their webpages. The same code was added to the gateway pages to also protect those pages from being attacked. As these pages were not part of the certified voting system, no conflicts resulted.

The most important countermeasure however was that e-voting was an additional voting channel scheduled before the paper-based election. According to the law, the election commission can—in the case of specific problems—decide to annul the e-vote, and the students who already voted electronically would be advised to vote again during the paper-based voting period. Consequently not even a successful dDoS attack can effectively harm the election. We suggest to amend the existing paragraph within Rec(2004)11 (art. 45) to not only state that “*remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations...*” but also to include a statement that ending the remote election period before the opening of the polling stations and establishing a process for informing all remote voters in case of annulment due to technical problems may be a way to countermeasure the effect of a dDoS attack.

#### 4.2 Phishing Attack with Mock E-Voting System

To successfully cast a vote students using their own personal computer had to use an Austrian citizen card [BK10], a card reader, and an internet browser with java support. To access the voting system the students had to visit the official federation of students election website, <http://www.oeh-wahl.gv.at> [OeW10], where they received all relevant information concerning the election. The e-voting system was only linked to the official federation of students election website during the actual e-voting period. The link to the voting system was not published in advance. By clicking a link marked “to the electronic voting,” the students were transferred to the voting system.

During the voting period, a political party published a website similar to the official website to mislead the voters. Even a voting process was simulated. The URL used was easily mistaken for the official URL:

Official URL:	<a href="http://www.oeh-wahl.gv.at">www.oeh-wahl.gv.at</a>
Attacker's URL:	<a href="http://www.oeh-wahlen.at">www.oeh-wahlen.at</a>
Differences:	election vs. elections (translated) and missing government (gv) subdomain.

This attack could be considered as a phishing attack to gain sensitive information or, at the least, to irritate and mislead the voters. Phishing attacks are not e-voting specific so there are many anti-phishing approaches like [MP08] in banking or [QRYM07] in e-mail systems.

From the technical point of view, this attack could be counteracted by a combination of several measures. First of all, an official website of the election has to be established. It should be the single point of official information concerning everything related to the election. This especially includes the time the election takes place, the description of the voting process, the locations of the polling stations, the names of the candidates and political parties, results of previous elections, and the final results of this election. Furthermore this official website should be the portal to the e-voting system during the e-voting period. The website should be announced through multiple channels such as posters, links from other trustful websites, and much more which reflects Rec(2004)11 Art. 46 which states, *“For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.”*

Evaluation of the referrer HTTP header in the portal server logs showed that about 42 percent of the visitors directly navigated the website by entering the official URL manually into the browser. Most other visitors searched for the name of the election using their favorite search engine (keywords: “federation of students election, information, e-voting” before the election, “federation of students election, e-voting” during the election period, “federation of students election, results” after the election). Consequently active monitoring of search engine results on typical queries and decisive action against phishers are essential countermeasures against such phishing attacks. Buying domains easily mistaken for the real URL and therefore likely targets for phishers is another appropriate countermeasure.

As described in [QSM07], proofing the integrity of the website is very important which concludes to the recommendation to use extended validation certificates (EV) which add verified identity to SSL as described in [CF11]. Furthermore, official websites and internet voting systems related to legally binding elections should be hosted within the government domain space (in Austria e-voting.oeh-wahl.gv.at).

From the organizational point of view, the political party’s fake website conflicts with the principles of honest e-voting based on the experience of internet voting in the Estonian parliamentary elections [TSBA07]. In the Austrian federation of students election all election commissions and political parties were made aware of the principles, which were recommended by the Council of Europe, however, never accepted.

Different studies have shown that server-side security indicators and client-side mechanisms like browser warnings do not guarantee prevention of phishing attacks [DHC06] [DTH06] [SDOF07] [WIFE05] [WMG06]. This is due to the fact that if phishers can convincingly imitate the appearance of legitimate web sites, users tend to ignore security warning or do not interpret security cues appropriately [YWAP08]. As an

additional technical countermeasure, the security layer of the Austrian citizen card used for authentication per default only allows access to the personal data stored on the card if the connection is based on HTTPS and the requested data is either sent to a .gv.at domain or a domain identified by a special certificate denoting the URL as a government related resource. Naturally neither .gv.at domains nor a government OID certificate are freely obtainable. For further details on the security architecture of the Austrian citizen card, please refer to [LHP02].

From the operational point of view, before and during the election period the registration and use of domain names similar to the official domain name have to be strictly monitored. Any suspicious activity should be brought to the attention of the election commission as soon as possible to allow for enough time to instigate counter measures.

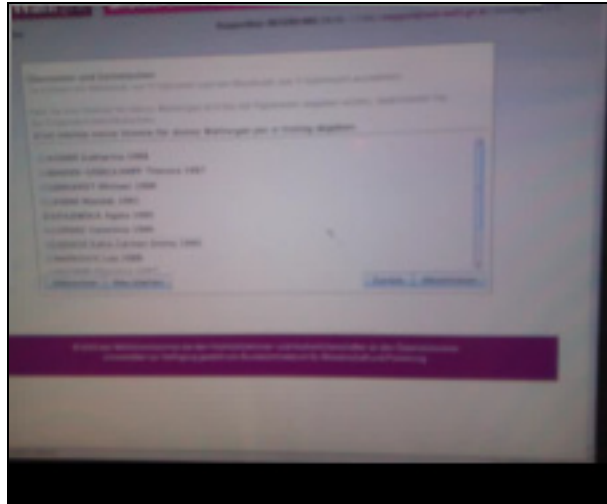
Even though this advice is not explicitly included within Rec(2004)11, it is addressed by article 103: “*The audit system shall record times, events and actions, including: [...] any attacks on the operation of the e-voting system and its communications infrastructure [...] malfunctions and other threats to the system.*” Nevertheless, considering the danger of such an attack, a paragraph denoting the importance of preventing and handling phishing attacks in remote elections would lead to further improvement.

### **4.3 Vote Flipping Video**

E-voting systems are susceptible to a class of attacks that usually does not feature in other web-based attacks: campaigns to discredit, or smear campaigns. The aim of these attacks is not to disturb or subvert the voting process as such, but to foster the rejection of e-voting as a viable voting channel by alluding that the e-voting process was either not secure or even subverted. Most of the arguments brought against e-voting can be used against any form of remote voting. However, there is one class of arguments that only pertains to e-voting systems and that is the inherent lack of transparency in computerized systems. The technology involved is usually beyond the grasp of the average citizen, and the fact that the same technology powers everything from banking to telecommunications, does not stop people from believing, that this technology will be subverted to nefarious purposes once applied to e-voting.

A vote flipping video was used in a campaign to discredit the federation of students election. This video tried to prove that a voter could select one candidate while on the electronic ballot sheet a different candidate would be marked. The video was released to the media during the election phase.





**Fig. 2:** Fake vote flipping video

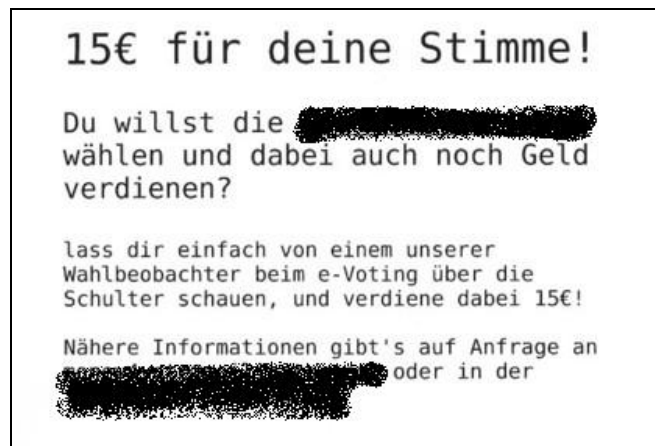
Although the video was quite blurry and of bad quality, it was identified as a fake by experts after some investigation. Nevertheless, this experience of the 2009 Austrian federation of students election demonstrates several important aspects. First of all, an incident response team has to be established to react to such events and support the election commission with the analysis as stated in Rec(2004)11 (art. 76): *“Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.”*

Furthermore to allow the timely reaction to attacks, a public communication channel has to be established and announced beforehand. The communication channel should also serve as a contact point for the press in the case of suspicious materials offered to the media. It should be made clear that proof of failure or other reproaches addressed to the media should be handed in for validation before publishing.

Based on this experience it is advisable to declare an official communication channel for announcing possible security relevant incidents. This can be reflected in the appropriate manner in the recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.

#### 4.4 Vote Buying Campaign

The federation of students election suffered from a second campaign to discredit it, this one a case of alleged vote buying. On the first e-voting day, flyers were found in several lecture rooms at a university asking students to cast their votes using the e-voting system in front of a specific political party's election observers to receive a payment of fifteen euros.



**Fig. 3:** Flyer for vote buying

Translation:

15 € for your vote!  
Do you want to vote for [XXXXXXXX] and at the same time earn money for it?  
Let one of our election observers watch you vote electronically and earn 15€ at the same time.  
Per request, more information is available at [XXXXXXXX]  
or at [XXXXXXXX].

Please note that the names of political parties have been removed.

Although not absolutely proven, it seems relatively certain that the flyers were a fake. The intention of the vote buying flyers could have been not only to discredit the political party named on the flyers, but also to irritate and discourage students eligible to vote from using the e-voting system. However, the e-voting system might not have been the primary target in that case.

Vote buying is the most regular form of violation according to [CAPA07]. If votes are cast in secret, there is no way for candidates and party organizers to be certain that the vote was cast according to the agreement between the voter and the briber. Vote buying is possible for all forms of remote elections and thus not unique to the e-voting process. Rec(2004)11 includes this requirement by several recommendations that have to be

combined to be effective. (art. 80) *“The e-voting system shall restrict access to its services, depending on the user identity. User authentication shall be effective before any action can be carried out.”* And (art. 51) *“A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.”* In the 2009 Austrian federation of students election, the voter had to confirm with the digital signature of her/his citizen card that she/he votes free and in secret. This confirmation was an integral part of the authentication process in which the voter’s identity was proven by verifying the digital signature. As with any security related system, it is necessary to balance security with usability. The benefit of enforcing such a confirmation at the beginning of the voting process is that the voter’s awareness is improved and confirmed before filling out the ballot sheets.

In general Rec(2004)11 should include the recommendation of establishing the voter’s awareness that votes should be freely cast and in secret in remote elections.

#### **4.5 Unknown Social Engineering Attacks**

During the e-voting period, user-support was handled by the Federal Computing Centre of Austria (BRZ). Voters could contact user-support by e-mail, phone or by an online contact form. A self diagnosis tool, which was integrated within the website, turned out to be very helpful in debugging problems on the user/client side.

As stated in Rec(2004)11 (art. 79), *“The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.”* A technical monitoring system was established to ensure that during the polling period, the voting equipment and its use satisfied the requirements. A traffic light display showed the operations team the functional status of the system without having physical or virtual access to the sealed system. The user-support team was well-trained, especially against social engineering attacks. Processes had been established to identify and counter such malicious attempts.

## **5 Conclusion**

The recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting was published in 2004. Since then there have been periodic iterations by means of biennial review meetings to revisit the impact of the recommendations and to identify necessary amendments.

The focus of this paper was the question of whether the described recommendations are sufficient to handle these state-of-the-art attacks. The basis of this analyze was a discussion of the various attacks that occurred during the 2009 Austrian federation of students election with conclusions regarding suggested improvements for Rec(2004)11.

Based on the distributed denial of service attack, it is a possibility that if e-voting is an additional voting channel, mechanisms could be put in place to recast the vote on election day on paper.

The danger of phishing attacks turned out to be very critical. Therefore Rec(2004)11 could be further improved by explicitly pointing out the necessity of implementing adequate countermeasures.

The acceptance of e-voting as a new voting channel is a key success factor in every project. Various attacks don't target the election directly, but rather target the voters' acceptance by publishing, for example, fake videos of vote flipping as happened during the 2009 Austrian federation of students election. Dealing with such attacks is very difficult and demands the development of a special security strategy, which should be recommended in Rec(2004)11.

Counteracting attack attempts against the e-voting system by social engineering methods demands awareness programs, trained staff, and well-designed processes as requirements that could be included in the recommendation.

The recommendation Rec(2004)11 has been reviewed in 2006, 2008 and will undergo a third review in fall of 2010. The experiences of the Austrian federation of students election can provide interesting insights for this continuous improvement process.

## Bibliography

- [AH04] Alvarez, R., and T. Hall. 2004. Point, click, and vote. The future of internet voting. Washington, DC.: Brookings Press.
- [AH08] Alvarez, R., and T. Hall. 2008. Electronic elections. The perils and promise of digital democracy. Princeton NJ, USA: Princeton University Press.
- [ASC09] Certificate according to §34 (6) HSG 1998 for the federation of students election 2009. <http://www.a-sit.at/>.
- [BK10] Austrian Citizen Card and Specification of the Austrian Citizen Card Technology. <http://www.buergerkarte.at/en/>.
- [BSSL01] Schneier, Bruce. 2001. Secret and Lies. IT-Sicherheit in der vernetzten Welt. dpunkt.verlag/Wiley.
- [CAPA07] Parliamentary Assembly Council of Europe. 2007. Secret ballot. European code of conduct on secret balloting, including guidelines for politicians, observers and voters.
- [CEIP04] Integrated Project "Making Democratic Institutions work" (2002 – 2004), Conference on The future of democracy in Europe 17-19 November 2004, Barcelona (Spain)
- [CF11] Extended Validation Certificates Add Verified Identity to SSL. <http://www.cabforum.org/>.
- [CoED04] Council of Europe. 2002-2004. Integrated Project "Making Democratic Institutions work." <http://www.coe.int/t/dgap/democracy/activities/Previous%20Projects/>.
- [CoEO10] Council of Europe. 2010. Workshop on the "Observation of e-enabled elections", Oslo, 18-19 March. [http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Evoting\\_Oslo\\_Seminar/](http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Evoting_Oslo_Seminar/).
- [DHC06] Downs, J.S., M. B. Holbrook, and L. F. Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the SOUPS*, 79–90.
- [DTH06] Dhamija, Rachna, J.D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the CHI*, 581–590.
- [ED50] Deming, W. Edwards. Deming Circle PDCA, Presented during lectures in Japan during World War II
- [EV07] Krimmer, R. 2007. *Machbarkeitsstudie. Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektronischer Abstimmungsverfahren.*
- [HSG98] Federation of students law. 1998. Hochschülerinnen- und Hochschülerschaftsgesetz 1998 (HSG 1998).

- [HSWO05] Election regulations. 2005. Hochschulinnen- und Hochschülerschaftswahlordnung 2005 (HSWO 2005).
- [KLSV09] Krimmer, R., C. Lehner, S. Stangl, B. Varga, R. Stein, G. Wenda, J. Kozlik 2009. E-Voting im Rahmen der Wahlen zur Österreichischen Hochschulinnen- und Hochschülerschaft 2009, in Hauser, W., M. Kostal: *Hochschulrecht 09*, Wien, NWV, 539-551.
- [LC10] Lehner, C. 2010. Die Wahlen zur Österreichischen Hochschulinnen- und Hochschülerschaft, Doctoral Dissertation at the University of Vienna.
- [LHP02] Leitold, H., A. Hollosi, and R. Posch. 2002. Security architecture of the Austrian citizen card concept. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, 391–400.
- [MP08] San Martino, Antonio, and Xavier Perramon. 2008. Defending e-banking services. Antiphishing approach. Universität Pompeu Fabra, The Second International Conference on Emerging Security Information, Systems and Technologies.
- [OeH00] Head of Federation of students 2000. Statement concerning federation of students law.
- [OeH07] Head of federation of students 2007. Bedenken der ÖH Bundesvertretung zu e-voting bei Hochschulinnen- und Hochschülerschaftswahlen, September 2007
- [OeW10] Informational website of the federation of students election by the election commissions. <http://www.oeh-wahl.gv.at/>.
- [OHER10] E-Voting Evaluation Report. 2010. E-Voting bei den Hochschulinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht.
- [PKK04] Prosser A., R. Krimmer, and R. Kofler. 2004. Implementing an internet-based voting system for public elections. Project experience. In *Enterprise information systems V*, ed. O. Camp, J.B.L. Filipe, S. Hammoudi, and M. Piattini, 294–299. Boston, USA/Dordrecht, Netherlands: Kluwer Academic Publishing.
- [QRYM07] Qiong Ren Yi Mu Susilo, W. 2007. SEFAP. An email system for anti-phishing. In *Univ. of Wollongong, Wollongong, Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference*, 782–787.
- [QSM04] Quasthoff, Matthias, Harald Sack, and Christoph Meinel. 2007. Why HTTPS is not enough. A signature-based architecture for trusted content on the social web. Hasso Plattner Institute, University of Potsdam, IEEE/WIC/ACM International Conference on Web Intelligence.
- [Rec04] Council of Europe. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. <https://wcd.coe.int/ViewDoc.jsp?id=778189/>.
- [SDOF07] Schechter S. E., R. Dhamija, A. Ozment, and I. Fischer. 2007. The emperor's new security indicators. An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the IEEE symposium on security and privacy*, 51–65.
- [SLBV09] Schmidt, A., L. Langer, J. Buchmann, M. Volkamer 2009. Specification of a Voting Service Provider. In: *Requirements Engineering for E-Voting Systems (RE-VOTE)*.
- [Sig10] Austrian Government. Electronic signature law. Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG).
- [SZKK88] Sunzu. 1988. *Die Kunst des Krieges*. Droemersch Verlaganstalt.
- [TSBA07] Trechsel, A., G. Schwerdt, F. Breuer, and M. Alvarez. 2007. *Internet voting in the March 2007 parliamentary elections in Estonia*. European University Institute. [http://www.vvk.ee/public/dok/Coe\\_and\\_NEC\\_Report\\_E-voting\\_2007.pdf/](http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf/).
- [WIFE05] Whalen, T., and K. M. Inkpen. 2005. Gathering evidence. Use of visual security cues in web browsers. In *Proceedings of the conference on graphics interface*, 137–144.
- [WMG06] Wu, M., R. C. Miller, and S. L. Garfinkel. 2006. Do security toolbars actually prevent phishing attacks? In *Proceedings of the CHI*, 601–610.
- [XAMA05] Xenakis A., A. Macintosh 2005. Procedural Security and Social Acceptance in E-Voting. In: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*.
- [YWAP08] Yue, Chuan, and Haining Wang. 2008. Anti-phishing in offense and defense. In The College of William and Mary, annual computer security applications conference, 345–354.



## **Session 7: Discussion of E-Voting Protocols**





# Universally Verifiable Efficient Re-encryption Mixnet

Jordi Puiggali Allepuz and Sandra Guasch Castelló

Scytl Secure Electronic Voting  
Tuset 20, 1-7, 08006 Barcelona, Spain  
[jordi.puiggali@scytl.com](mailto:jordi.puiggali@scytl.com), [sandra.guasch@scytl.com](mailto:sandra.guasch@scytl.com)

**Abstract:** Implementing a transparent audit process when an election is conducted by electronic means is of paramount importance. Universally verifiable mixnets are focused on providing such a property by means of cryptographic proofs verifiable by any auditor. While some of these systems require high amount of computing resources that make them inefficient for real elections, others proposals reduce the computation cost by sacrificing audit accuracy or reducing the voter privacy protection level. In this paper, we propose an efficient mixnet verification system that combines the advantages of the RPC and Optimistic Mixing techniques, achieving a high audit accuracy level while fully preserving voters' privacy.

## 1 Introduction

When developing an election by electronic means, the main problem that arises is how to implement a transparent audit process. In traditional elections, independent auditors and observers can directly oversee the election process while it is happening. An important objective of this audit process is to verify that the opening of the ballot boxes and the counting of the votes is accurately and honestly implemented. When the counting process is done by electronic means (i.e., decryption and counting of the votes), overseeing the logical process while it is executed in the machine is practically impossible: this process is a logical entity that cannot be monitored by human means as in traditional elections. Therefore, it is of paramount importance that the electronic voting system provides transparent audit means of its correct behavior.

With electronic voting, results can be verified the same way as in traditional voting: making a parallel recount of the votes. Therefore, the difficulty of the audit process relies on the proper opening of the votes: the vote decryption process.

One possible approach is to allow auditors or observers to install programs in the system to monitor the voting platform. The problem is that auditor programs should be also monitored, since the decryption process becomes also vulnerable to these programs. Therefore, the solution introduces an infinite loop that has no easy solution (who watches the watchmen?).

Alternatively, the decryption process can be audited by means of monitoring the log information generated during its execution. However, assuming that the decryption process is compromised, the log information could be also manipulated to hide any

malicious practice. Furthermore, the information provided by the decryption process should be limited, since it must preserve voter's privacy (e.g., it cannot register the relationship between a decrypted content and an encrypted vote if the later can be correlated to a voter).

In 1995, Sako and Kilian [SK95] introduced the concept of "universal verifiability" for their proposal of a vote decryption process based on a mixnet approach. This verifiability is focused on providing means for any auditor or observer to verify the correct decryption of the votes, using cryptographic proofs that are generated by the decryption process.

A mixnet or *mix network* is composed of one or various nodes that shuffle the input messages using a secret permutation. Since mix-nodes also perform a transformation process that modifies the values of the set of input encrypted votes, it is important to be able to verify the mixing and decryption procedures in such a way that privacy and integrity are preserved.

Since Chaum introduced the first mixnet in 1981 [Ch81], the search for efficient verification methods that do not break the anonymization process (i.e., revealing the secret permutation or the re-encryption factors) has been a fertile area of research. Specifically, the universal verifiability property has been the main purpose of the mixnets designed in the last fifteen years.

In this paper, we introduce a universally verifiable efficient verification method for re-encryption mixnets that achieves high correctness while preserving voters' privacy. The paper is structured as follows: in section 2 we explain our motivation to design a new mixing verification system, in section 3 the underlying cryptosystem is defined, the new verification method is presented in section 4, and the paper concludes in section 5.

## 2 Motivation

Providing cryptographic proofs for the universal verification of a mixing process can be complex, computationally costly, and can involve a risk of reducing the voters' privacy.

Some mixing systems ([SK95], [FS01], [Ne01]) achieve a high correctness while preserving voters' privacy at the cost of performing a great number of proofs and verifications. Since these proofs and verifications have a high computational cost, it makes them inadequate in real election environments with a large number of votes. One of the motivations for the introduction of electronic voting is to speed up the vote counting process. For this reason, there are proposals that use them to make a parallel tallying of the votes while a faster method (less accurate) is used to give faster provisional election results, as proposed in [BG02].

To improve the efficiency of the mixing process (i.e., increase the speed of the mixing and audit process), other mixing systems focused the design of their audit mechanisms on reducing the cost of their cryptographic audit mechanisms by sacrificing to some

degree the strength of the voter's privacy or reducing the accuracy of the audit process (i.e., correctness) to an acceptable level. For instance, Random Partial Checking (RPC) [JJR02] trades-off mainly privacy, while the proposal in [Go02] preserves voters' privacy, but at the expense of sacrificing some correctness and efficiency: it performs more proofs that slow down the audit process. Another method that sacrifices some privacy and correctness on behalf of efficiency is [BG02], achieving results that can be considered good enough for an electronic process when large amounts of votes are counted.

The mixing verification system presented in this paper has a high degree of efficiency (comparable to the fastest proposals) while completely preserves voter privacy, and at the same time achieves a high level of correctness for small-medium and large elections.

### 3 Underlying Cryptosystem

In our scheme, voters use the ElGamal cryptosystem properly parameterized for semantic security [Pf94], [TY98] to encrypt the votes. The cryptosystem is composed by three public parameters:  $p$ ,  $q$ ,  $g$ , a public key  $h$ , and a private key  $x$  defined in the following way:

- The modulo  $p$  is chosen as a large safe prime, that is  $p=2q+1$  and  $q$  is a prime number.
- $g$  is a generator of  $Gq$ , the  $q$ -order subgroup of  $Zp^*$ .
- The private key  $x$  is selected from  $Zq$ , and the public key  $h$  is calculated as  $h=g^x \text{ mod } p$ .

In order to make the encrypted votes indistinguishable, the voting options  $v$  are configured to be all from the quadratic residue or quadratic non-residue modulo  $p$  set. In case a voting option does not fit in the set, a padding string could be added.

The voting options are encrypted using random exponents  $r$  in  $Zq$ :

$$c = (v \cdot h^r \text{ mod } p, g^r \text{ mod } p) = (c_1, c_2)$$

Therefore, an encrypted voting option can be recovered as

$$v = c_1 \cdot c_2^{-x} \text{ mod } p.$$

There are some interesting properties of the cryptosystem that are used in our mixing verification process, such as re-encryption and homomorphic operation of the encrypted votes.

#### 3.1 Re-encryption of the encrypted votes

Thanks to the properties of the ElGamal cryptosystem, an encrypted message can be re-encrypted using a new randomization value without changing the decryption process.

Being the encrypted vote

$$c = (v \cdot h^r \bmod p, g^r \bmod p) = (c_1, c_2),$$

The re-encryption can be performed as

$$c' = (c_1 \cdot h^{r'} \bmod p, c_2 \cdot g^{r'} \bmod p) = (v \cdot h^{r+r'} \bmod p, g^{r+r'} \bmod p) = (c_1', c_2').$$

The re-encrypted vote can be decrypted as usual:

$$v = c_1' \cdot c_2'^{-x} \bmod p.$$

### 3.2 Homomorphic operation of the encrypted votes

Being two votes  $v_1$  and  $v_2$ , an encryption operation  $E$ , and two algebraic operations  $\Phi$  and  $\Theta$ , the homomorphic property can be defined as

$$E(v_1) \Phi E(v_2) = E(v_1 \Theta v_2).$$

Since ElGamal is a cryptosystem with homomorphic properties, the product of  $n$  encrypted votes  $c_i$  generates an equivalent encrypted information  $Ec$  whose content  $Ev$  is the product of the plaintext voting options and the encryption exponent  $r_e$  is the sum of the individual encryption exponents:

$$\begin{aligned} \prod_{i=1}^n c_i &= \left( \prod_{i=1}^n v_i \cdot h^{r_i}, \prod_{i=1}^n g^{r_i} \right) = \left( \left( \prod_{i=1}^n v_i \right) \cdot h^{\sum_{i=1}^n r_i}, g^{\sum_{i=1}^n r_i} \right) = \\ &= (Ev \cdot h^{r_e}, g^{r_e}) = Ec \end{aligned}$$

## 4 Mixing process and verification

### 4.1 Overview

The universal verification method for re-encryption mixnets presented in this paper combines the advantages of the RPC technique [JJR02] and the ‘‘Optimistic Mixing’’ proposal [Go02]: the partial disclosure of information is combined with proofs calculated from homomorphically aggregated groups of votes to achieve greater levels of privacy, robustness and soundness than these methods.

In the first step, each mix-node shuffles and re-encrypts the input encrypted votes, storing in a secret and secure way the permutation and re-encryption values applied for each vote. When the last node has mixed and re-encrypted its inputs the anonymized votes are ready to be decrypted, but before disclosing any significant information, the correct performance of the mixnet is universally verified.

In the verification process, the input encrypted votes of each node are divided into several independent groups following a random organization proposed by a verifier (i.e., an auditor). As said before, this group organization is done at the end of the mixing process (i.e., before decrypting the votes), preventing the disclosure of sensitive

information to any mixing node in order to cheat the verification process. Then each prover—the mix-node—provides information to the verifier about the global location in the mix-node’s output of the votes belonging to each group in the input.

The global location of the votes of one output group does not disclose the individual position of each vote related to its original input group in the mix-node. For instance, disclosed output group positions are sorted by numerical value instead of their position in the mix-net input group.

When the verifier divides the input encrypted votes into groups, it also multiplies the votes in each group to obtain an *Input Integrity Proof* using the homomorphic properties explained in section 3.2. After the prover indicates which votes in the output of the node belong to each input group, the verifier can multiply the votes belonging to each output group to obtain an *Output Integrity Proof*. For each pair *Input-Output Integrity Proof* at each node, the prover provides a Zero-Knowledge Proof to demonstrate that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof*.

Since the integrity proofs can be calculated and verified by any auditor, this method achieves the universal verifiability objectives. Furthermore, this proposal allows the verification of the mixing process without disclosing information about the position of individual votes in the output node after the shuffling process, preserving voters’ privacy.

The next sections provide the details of vote group generation, the integrity proofs, and their related ZKPs.

## 4.2 Creating the groups

When the verification process starts, the verifier randomly defines how the input votes in the first mix-node are grouped by sending an array with the indexes of the position of the votes to be grouped:

For  $m$  input votes:  $\{v_1, v_2, v_3, \dots, v_m\}$ .

An example of a grouping array is:  $\{v_3, v_{m-1}, v_5, \dots, v_2\}$ .

Since the size of the groups is pre-defined (explained at the end of this section), the prover organizes the input votes following the grouping array order to define each vote group contents. Then, using the mixing permutation information, the prover indicates to the verifier for each mix-node output vote the group to which it belongs to. Since this information is provided following the order of the mix-node output votes, it is not possible to individually correlate input and output votes (only group affiliation).

For the next nodes of the mixnet, input vote groups are re-defined using as reference the output vote groups of the previous mix-node. We do not propose the reorganization of the groups at random, as in the first mix-node, to prevent disclosing information that could be used to correlate mixnet last output votes with first input ones: an attacker could analyze the votes belonging to each new grouping at each mix-node and identify

intersections of the groups that could facilitate the tracing of output votes with a reduced set of input votes (or in the worst case, an individual vote) of the first mix-node. If so, the probability of an input vote being connected to a specific final output vote would be different from  $1/m$ , opening the door to privacy issues.

In order to prevent this attack, the new input groups are created by taking votes from different output groups of the previous mix-node. This is done in such a way that the groups in the last mix-node are composed of at least one vote from each group defined in the first mix-node. A proposal to redefine the groups consists of creating a new group by selecting votes belonging to different groups in the previous node in a consecutive way, like it is shown in figure 3. In this figure, the first group of the second node (G1,2) is formed by a vote from the first group of the first node (G1) and by one of the second (G2); the group of the second node (G3,4) is formed by a vote of the third group of the first node (G3) and one of the fourth (G4), and so on.

In order to preserve voter privacy, the size of the group also matters (e.g., if the size of the groups is too small, maybe the votes are not equally distributed at the last node of the mixnet). Furthermore, the probability of detecting manipulations of the votes during the mixing process also depends on the size of the groups (the smaller the group is, the higher the probability of detecting the manipulation of any vote is). For this reason, the groups need to be set up in a proper way to achieve the highest detection ratio without compromising voter privacy.

Being  $t$  the number of mixnet nodes (at least two) and  $m$  the total number of votes, the number of  $n$  votes inside a group should be at least:

$$n = \sqrt[t]{m} \quad [1]$$

This formula preserves the privacy and optimizes manipulation detection rates of the votes. As shown in the formula, in our proposal the number of mixnet nodes also contributes to the correctness of the verification process. However, this optimization should be evaluated carefully, since the addition of new mixnet nodes reduces the efficiency of the proposal: increases the number of cryptographic operations required by the mixing and verification processes.

In the possible case of one or more nodes disclosing information about the individual permutations applied to the votes, they would not be taken into account in the formula 1. Therefore, privacy would still be maintained.

### 4.3 Generation of the ZKP of the Integrity Proofs

The integrity check of the votes grouped at each node is based in the homomorphic properties of the ElGamal encryption scheme. We call the result of multiplying a group of votes *Integrity Proof*.

The result of the multiplication of  $n$  votes of the same group in the input of a node, or *Input Integrity Proof* can be defined as:

$$\prod_{i=1}^n c_i = \left( \prod_{i=1}^n v_i \cdot h^{r_i}, \prod_{i=1}^n g^{r_i} \right) = \left( \left( \prod_{i=1}^n v_i \right) \cdot h^{\sum_{i=1}^n r_i}, g^{\sum_{i=1}^n r_i} \right) = (Ev \cdot h^{r_e}, g^{r_e})$$

The multiplication of the same group of votes in the output of the node (i.e., the same votes after being re-encrypted), is called *Output Integrity Proof* and it is equal to:

$$\begin{aligned} \prod_{i=1}^n c_i' &= \left( \prod_{i=1}^n v_i \cdot h^{r_i+r_i'}, \prod_{i=1}^n g^{r_i+r_i'} \right) = \left( \left( \prod_{i=1}^n v_i \right) \cdot h^{\sum_{i=1}^n r_i+r_i'}, g^{\sum_{i=1}^n r_i+r_i'} \right) = \\ &= (Ev \cdot h^{r_e+r_e'}, g^{r_e+r_e'}) \end{aligned}$$

Since the mix-node knows all the individual re-encryption factors of the votes of each group, it can calculate the accumulated re-encryption factor  $r_e' = \sum_{i=1}^n r_i'$ . Having this

accumulated factor, the mix-node can make a Non-Interactive Zero Knowledge Proof of Re-encryption (NIZKP-RE), proving that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof* using the re-encryption factor  $r_e'$ . This proof can be based on the Schnorr Identification Protocol like in [MA99] or the Chaum-Pedersen proof of equality of discrete logarithms [CP93].

Therefore, any auditor, after calculating by herself the *Input Integrity Proof* and *Output Integrity Proof* of the groups of a node, can use the NIZKP-RE to check that both proofs are based on the same contents. In other words, the global contents of the votes in a group still remain the same. Since the integrity proofs are based on the homomorphic product of the votes, there is still a possibility that a rogue mix-node could cheat the system. However, as explained in section 4.5.1, the way the groups are modeled in our proposal makes the probability of detecting such manipulation very high (e.g., it has a probability of 99.91% of detecting a manipulation of 2 votes in an election with 10,000 votes).

If the proof is successfully verified, the node is believed to behave correctly. This NIZKP-RE is done for each group of votes at each node.

#### 4.4 Verification Protocol Summary

To summarize, the verification protocol implements the following steps after the mixing process:

1. For the first mix-node, the verifier divides at random the input votes in groups using a grouping array that is sent to the prover.
2. Then, the verifier calculates an *Input Integrity Proof* for each group.

3. The verifier asks the prover for the output destination of the votes belonging to each group and calculates an *Output Integrity Proof* for each group.
4. The prover calculates a NIZKP based on the re-encryption factor in order to demonstrate that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof* of the same group.
5. For the next node, the groups are redefined in such a way that each new group is composed of votes from different output groups in the previous node, and the steps 2–5 are repeated until the correct behavior of the last mix-node is verified.

An example of the procedure is shown in Fig. 1. The figure also shows the group configuration at each mix-node:

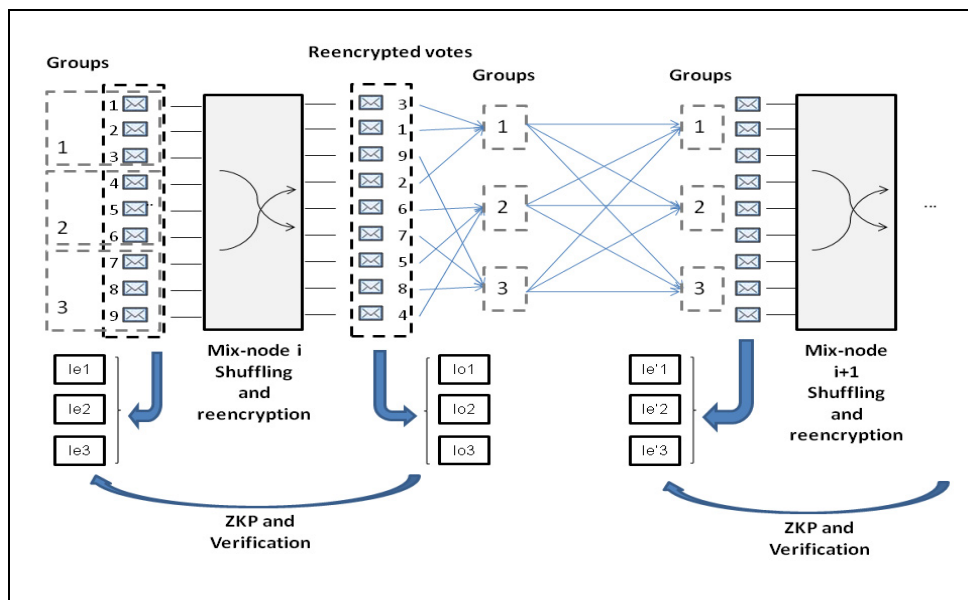


Fig. 1: Mixing verification process

## 4.5 Properties of the new system

We analyze the new verification method proposed from four points of view: soundness, efficiency, privacy, and universal verifiability.

### 4.5.1 Soundness

Since the verification process is based on the *Integrity Proofs* that are calculated by multiplying groups of votes, an attacker could take advantage of the cryptosystem's homomorphic properties in order to modify the votes in the mixnet without being detected. In fact, if several votes in the same group are modified in such a way that the



modifications are cancelled when the *Integrity Proof* is calculated, these changes are not detected in the verification process. However, since the group configuration is unknown until the mixing process finishes, the probability of an attacker changing a significant amount of votes without being detected is negligible.

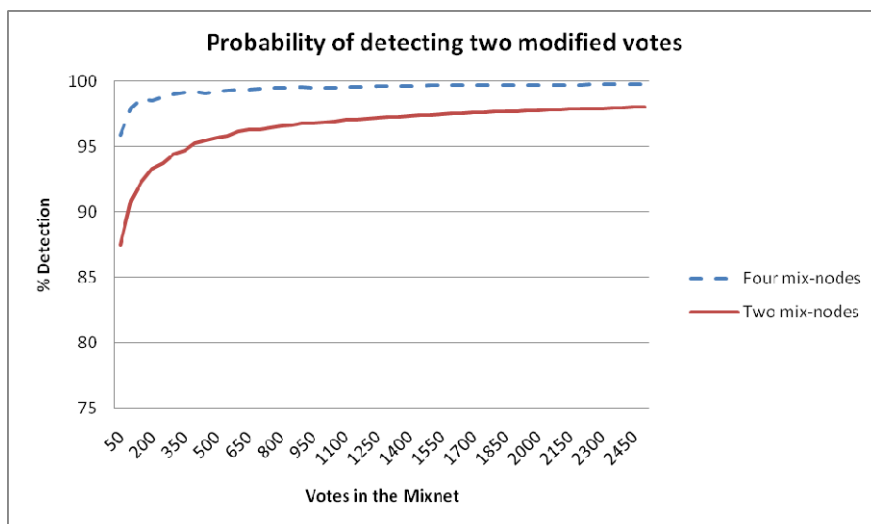
The chance of an attacker not being detected depends on the amount of votes in the mixnet, the number of groups in which the votes are divided, and the number of manipulated votes. Since the probability of being undetected decreases with the number of modified votes, we can define the most successful scenario for the attacker as the one where only two votes are manipulated, they are in the same group, and the modifications cancel out when the *Integrity Proof* is calculated.

The probability of detecting a pair of manipulated votes is:

$$P_{\text{success}} = 1 - \frac{n-1}{m-1}, \quad [2]$$

where  $m$  is the total number of votes and  $n$  is the number of votes in each group.

It is important to maintain a convenient relationship between the total number of votes processed by the mixnet and the size of the groups: the smaller the groups are, the higher the probability of detecting an attacker is. Otherwise, the larger the groups are, the faster the verification process becomes.



**Fig. 2:** Graphic showing the probability of detecting two modified votes when two mix-nodes and four mix-nodes are used.

Formula 1 gives an optimized relationship between the size of a group of votes and the total number of votes that are processed by the mixnet to meet the efficiency, soundness, and privacy requirements.

For example, in an election with 10,000 votes and a mixing of two nodes, the minimum size of the groups in order to preserve the voter privacy is 100 votes. With this configuration the probability of detection of two modified votes is 99%. If the mixing is performed with four nodes, the minimum size for each group is ten votes, which gives a probability of detection of 99.91%.

The probability of detecting two modified votes in a mixnet composed of two mix-nodes (bigger groups) or of four mix-nodes (smaller groups) is shown in Fig. 2. In both cases the probability of detection tends toward 100%, but when more mix-nodes are used and smaller groups are configured, the probability of detection increases faster.

#### 4.5.2 Privacy

Following the procedure described in section 4.2., groups at the input of each node contain votes from different groups of the previous node's output, in such a way that it is impossible for an attacker to track back the output votes to the groups defined in the first mix-node. Therefore, the privacy level of the verification method does not compromise the original privacy provided by the re-encryption mixnet.

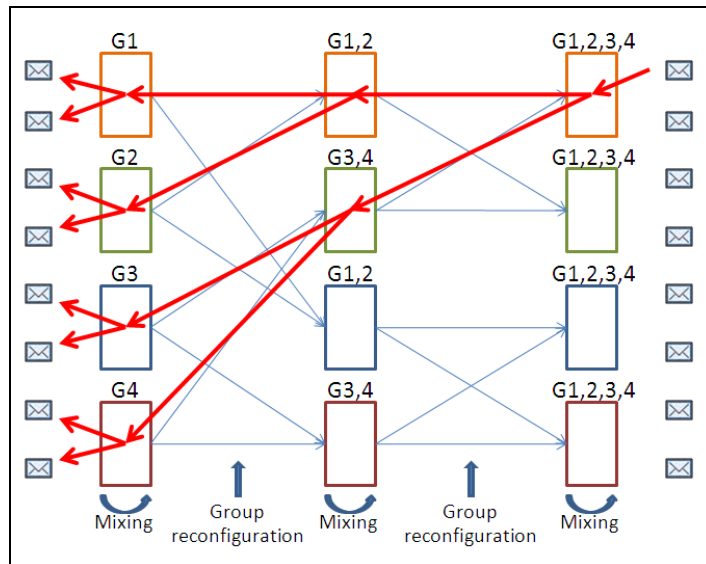


Fig. 3: Traceability of a message in the mixnet.

Fig. 3 shows how privacy is maintained due to the group reconfiguration at each node. An attacker choosing any encrypted vote of the mixnet output cannot successfully track it back to an individual encrypted vote in the input or any subset of input votes.

Therefore, all the votes in the input have the same probability of being in a specific output.

Formula 1 defines the group size depending on the number of mix-nodes for a fixed amount of votes in the mixnet. In the case that it is desirable to use small groups to increase the probability of detecting manipulated votes (the soundness of the proofs), more nodes in the mixnet are needed to preserve voter privacy.

### 4.5.3 Efficiency

Preserving voters' privacy and audit soundness by dividing the votes into small non-overlapping groups has an odd behavior: it reduces the efficiency of the mixnet. The computation costs of the verification method depend on the number of votes in the system and the amount of groups created for the verification process, since the proofs of correct behavior are done over them. Therefore, for a fixed number of votes in the mixnet, the more groups there are, the more the computation costs are consumed. On the other hand, the probability of detecting manipulated votes increases since there are less votes in each group.

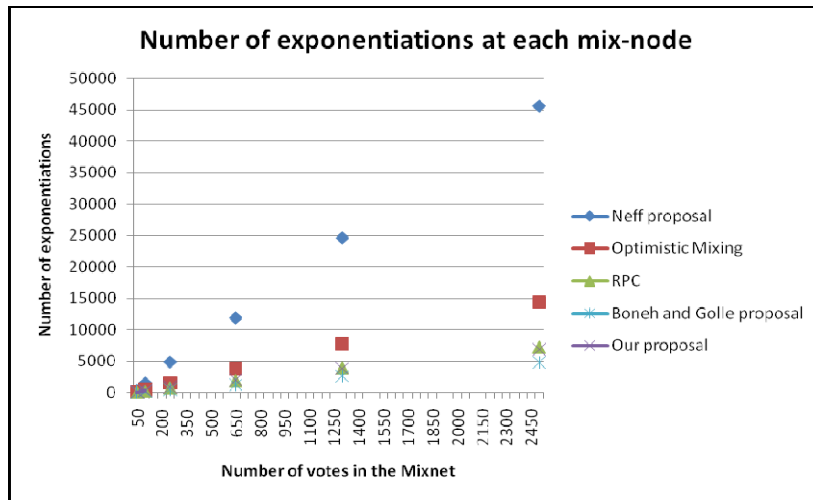


Fig. 4: Comparison of the number of exponentiations required at each mix-node in some mixing verification systems

We have estimated the cost of performance of our method based on the number of exponentiations done at each phase:

- Mixing: the re-encryption of the votes at each mix-node requires  $2m$  exponentiations, where  $m$  is the total number of votes in the mixing.
- Proof of correct mixing: calculating the zero-knowledge proofs of correct performance at each node requires  $2(m/n)$  exponentiations, where  $(m/n)$  is the

number of groups in which the total number of votes is divided at each node, and  $n$  is the number of votes per group.

- Verifying correct mixing: the verification of correct mixing at each node requires  $4(m/n)$  exponentiations.

In the Fig. 4, a comparison of our method with other mixing verification systems in terms of the number of exponentiations is provided, showing that our system is one of the fastest for large amounts of votes.

#### 4.5.4 Universal verifiability

A universally verifiable mixnet provides a proof of correct mixing that any observer can verify. For this purpose, some information is stored to let any auditor check the verification process after the mixing. Since the verification is made in zero knowledge, there is no need for the auditor to have any special or private data (i.e., private key of the election) to perform this check. The information collected during the mixing process for further verification consists of the set of encrypted votes in the mixing input and the re-encrypted votes at the output of each mix-node. During the verification process, the configuration of the votes in (input/output) groups and the zero-knowledge proofs performed by each node are also stored. Therefore, any auditor can check the verification process later using this information: the *Input* and *Output Integrity Proofs* can be calculated from the input/output sets at each node and the zero-knowledge proofs between them can be verified.

## 5 Conclusions

In this paper we described a new proposal of a universally verifiable and efficient method for re-encryption mixnets that achieves high correctness while preserving voters' privacy. Specifically, our proposal achieves an efficiency level comparable to the current faster existing systems, while our capacity of detecting manipulated votes is closer to the most accurate methods without compromising the voters' privacy.

Assuming an implementation of four nodes and setting the vote group size of the verification process to optimize the relationship between full voter privacy, efficiency, and fraud detection (using the formula 1 described in section 4.2), we can achieve the following conclusions.

From the point of view of efficiency, the computation cost of our proposal is close to the Boneh and Golle method [BG02]: the fastest one as shown in the figure 4. Regarding RPC method [JJR02], this is more efficient only for small batches of votes (less than 1500), but when the amount of votes increases, our system becomes faster. Considering the other methods [Go02][Ne01], the efficiency improvements are clear.

In terms of privacy, compared with our proposal, the original RPC proposal offers a weaker privacy level, since the input votes could be connected with some specific output

votes with a probability higher than  $1/m$ . An improvement proposed by Chaum [Ch02] solves this privacy issue by grouping pairs of mix-nodes in a special way during the verification and requiring at least four nodes. However, the problem still remains if the information from intermediate nodes is disclosed. On the other hand, in the method explained in [BG02], full voter privacy is difficult to achieve: each verification round done to increase the accuracy of the verification process discloses sensitive information that could be used to increase the probability of correlating input and output votes. In our proposal, we keep full voter privacy.

In terms of accuracy, our proposal achieves a high level of cheating detection for a small number of manipulated votes (i.e., 2 votes). This probability is closer to 100% when the number of votes is near 300 votes (99%). The other methods, except [Ne01], have similar or lower accuracy levels.

In summary, compared with the current verification methods, our solution is the most well-balanced in terms of efficiency, privacy, and accuracy, while providing universal verification properties.

## Bibliography

- [BG02] Boneh, D., and P. Golle. 2002. Almost entirely correct mixing with applications to voting. In *Proceedings of the 9th ACM conference on computer and communications security (Washington, DC, USA, November 18–22, 2002) CCS '02*, ed. V. Atluri, 68–77. New York NY: ACM.
- [Ch02] Chaum, D. Secret ballot receipts and transparent integrity. Better and less-costly electronic voting at polling places. White Paper. <http://www.vreceipt.com/article.pdf/>.
- [Ch81] Chaum, D. L. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (February): 84–90.
- [CP93] Chaum, D., and T. P. Pedersen. 1993. Wallet databases with observers. In *Proceedings of the 12th annual international cryptology conference on advances in cryptology (August 16–20, 1992). Lecture notes in computer science, vol. 740*, ed. E. F. Brickell, 89–105. London: Springer-Verlag.
- [FS01] Furukawa, J., and K. Sako. 2001. An efficient scheme for proving a shuffle. In *Proceedings of the 21st annual international cryptology conference on advances in cryptology (August 19 - 23, 2001). Lecture notes in computer science, vol. 2139*. ed. J. Kilian, 368–387. London: Springer-Verlag.
- [Go02] Golle, P., S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. 2002. Optimistic mixing for exit-polls. In *Proceedings of the 8th international conference on the theory and application of cryptology and information Security. Advances in cryptology (December 01 - 05, 2002). Lecture notes in computer science, vol. 2501*, ed. Y. Zheng, 451–465. London: Springer-Verlag.
- [JJR02] Jakobsson, M., A. Juels, and R. L. Rivest. 2002. Making mix nets robust for electronic voting by randomized partial checking. In *Proceedings of the 11th USENIX security symposium (August 05–09, 2002). USENIX Security Symposium*, ed. D. Boneh, 339–353. Berkeley CA, USA: USENIX Association.
- [MA99] Markus, J., and J. Ari. 1999 *Millimix. Mixing in small batches*. Technical Report 99-33. Center for Discrete Mathematics & Theoretical Computer Science.

- [Ne01] Neff, C. A. 2001. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM conference on computer and communications security (Philadelphia, PA, USA, November 05 - 08, 2001)*. CCS '01, ed. P. Samarati, 116–125. New York, NY: ACM.
- [Pf94] Pfitzmann, B. 1994. Breaking efficient anonymous channel. In *Advances in cryptology (Eurocrypt '94), volume 950 of LNCS*, ed. A. D. Santis, 332–340. Berlin: Springer-Verlag.
- [SK95] Sako, K., and J. Kilian. 1995. Receipt-free mix-type voting scheme. A practical solution to the implementation of a voting booth. In *Advances in cryptology - EUROCRYPT '95. Lecture notes in computer science*, ed. C. Guillou and J. Quisquater, 393-403. Berlin: Springer-Verlag.
- [TY98] Tsionis, Y. and M. Yung. 1998. On the security of ElGamal based encryption. In *Proceedings of the first international workshop on practice and theory in public key cryptography. Public key cryptography (February 05 - 06, 1998). Lecture notes In computer science, vol. 1431*. ed. H. Imai and Y. Zheng, 117–134. London: Springer-Verlag.

# Why Public Registration Boards are Required in E-Voting Systems Based on Threshold Blind Signature Protocols

Reto E. Koenig<sup>1</sup>, Eric Dubuis<sup>2</sup>, Rolf Haenni<sup>2</sup>

<sup>1</sup>University of Fribourg  
Department of Computer Science  
CH-1700 Fribourg, Switzerland  
reto.koenig@unifr.ch

<sup>2</sup>Research Institute for Security in the Information Society  
Bern University of Applied Sciences  
Quellgasse 21, Postfach  
CH-2501 Biel, Switzerland  
{eric.dubuis,rolf.haenni}@bfh.ch

**Abstract:** In this paper, we demonstrate that e-voting protocols based on threshold blind signatures from multiple authorities allow a coalition of  $m$  eligible voters to cast more than  $m$  votes. This property presents a serious violation of the principles of democracy in the voting process. We analyze the applicability of this violation and provide a generic solution using a public registration board and modified threshold signature schemes.

## 1 Introduction

Threshold blind signature schemes provide several highly desired properties in cryptography: privacy, security, robustness through redundancy, and avoidance of single points of failure. Many existing threshold blind signature schemes allow independent signature requests from multiple signers, i.e., no communication among the signers has to take place. Exactly this property applied in an e-voting protocol results in a severe violation of the principles of democracy in the voting process. To the best of our knowledge, no protocol design based on threshold blind signature has ever been analyzed regarding this fact.

### 1.1 Related Work

One of the central technical challenges of designing an e-voting protocol is to simultaneously authenticate voters unequivocally while preserving the anonymity of their votes. One approach is to define the system based on *blind signatures* [Ch82], [Ch83]. The development of such systems is stimulated by the fact that blind signature schemes are simple to understand and implement, flexible enough to be adjusted to all sorts of settings, and suitable for large-scale elections.

Applying blind signatures to e-voting was first proposed in [FOO92]. In the suggested protocol, known as FOO92, the voter first encrypts the vote and then requests a blind signature from the voting authority. The blind signature ensures that the content of the vote remains entirely disguised from the voting authority during the authorization process. The encrypted vote, together with the blind signature, is then sent over an anonymous channel to a public board. To open the votes for counting, the voter supplies the encryption key at the end of the voting period, again over an anonymous channel.

One of the major drawbacks of FOO92 is its potential for single points of failure, e.g., it allows the authority to introduce votes for voters who abstain from casting their votes. This and other drawbacks have been addressed in the literature, and hence, many variations of the FOO92 protocol exist today [CC96], [Ok97], [Ba94], [Oh99], [RRN01], [CC97], and [He97].

One aspect, which is common for presentday protocols, is the replication of entities having the property of single point of failure. This replication allows the distribution of power as only a certain number of instances is needed in order to keep the protocol from failing, see for example [Du99], [Ki02], [JZF03], [Ba0], [AFT07], [AW07], and [CCM08].

## 1.2 Contribution and Overview

In Section 2, we will briefly illustrate the above-mentioned class of protocols. We will demonstrate a generic e-voting protocol based on threshold blind signature, where entities with the property of single point of failure are replicated. We will then analyze the attack on the provided generic scheme where any coalition of  $m$  eligible voters can cast more than  $m$  votes. Our analysis will provide us with some qualitative and quantitative results.

In Section 3, we present a generic counter-measure against the above-mentioned attack, which is applicable to many existing e-voting schemes of that class. Section 4 gives a security analysis on the revisions made in Section 3, and Section 5 provides our conclusions.

## 2 E-Voting Protocol using Threshold Blind Signature Scheme

In the following we present a generic template e-voting protocol using threshold blind signatures. This protocol shall serve as the representative for various state-of-the-art e-voting protocols of this class. For the sake of readability, certain aspects of the protocol will be omitted whereas a more detailed view will follow in a proceeding section. Even though other protocols are different in detail, they carry the same threshold properties.



## 2.1 Threshold Blind Signature

To avoid an entity becoming a single point of failure, the entity is replicated  $N$  times where it is assumed that at least  $t$  replicates work in the sense of the protocol. The threshold  $t$  must be greater than 1 and smaller than  $N$ . To maximize the robustness and reliability of the protocol, the choice of  $t$  should make it unlikely that  $t$  or more replicates of an entity collude, or that  $N - t$  replicates fail. For e-voting protocols,  $\frac{2}{3}N \leq t \leq \frac{3}{4}N$  is often mentioned as a reasonable choice in multi-party computation [Hi01].

### Concrete Examples of Blind Signature Schemes

**RSA Based Blind Signature.** A *blind signature*, as introduced by Chaum [Ch82], is a form of digital signature, where the signer  $A$  is not supposed to see the real message to be signed, nor can the signer trace back the signature to the voter  $V$  (i.e., an unknown signature to an unknown message for a known requester). In order to achieve this goal, the data  $x$  to be signed is disguised before it is given to the signer using a blinding function. This function usually involves a public key  $e$  of the signer and a random number  $r$ :

1.  $V \rightarrow A: x' = \text{blind}_e(x, r)$ .

After the signer has signed the blinded data  $x'$  with the private key  $d$ , the resulting blind signature  $s'$  can be transformed into an ordinary digital signature  $s$  using a corresponding unblinding function:

2.  $A \rightarrow V: s' = \text{sign}_d(x')$ ,
3.  $A: s = \text{unblind}(s', r)$ .

In the classical RSA scheme, the blinding and unblinding functions consist of multiplying  $x$  with the blinding factor  $r^e$  and  $s'$  with the unblinding factor  $r^{-1}$ , respectively.

**Schnorr Based Blind Signature.** Blind signature schemes based on discrete logarithms were first introduced by Schnorr [Sc90]. In this scheme, the blinding and unblinding function consists of a typical  $\Sigma$  communication scheme:

1.  $A \rightarrow V: r' = g^k \bmod p$ , where  $k \in_R Z_q$ ,  $e = g^{-c} \bmod p$ , and  $g, p, q$  are setup parameters.
2.  $V \rightarrow A: x' = \varepsilon - \beta$  where  $\varepsilon = H(x, r)$ ,  $r = r'g^{\alpha e \beta} \bmod p$ , and  $\alpha, \beta \in_R Z_q$ .
3.  $A \rightarrow V: s'_i = k + x'c \bmod q$ .

The resulting blind signature  $(r, s')$  for the blinded data  $x'$  can be transformed to a signature  $(r, s)$  for the data  $x$  by applying the corresponding unblinding function  $s = s' + \alpha \bmod q$ .

## Threshold Blind Signatures

A *threshold blind signature* scheme is a combination of a threshold signature scheme with blind signatures such that the data to be signed is not revealed to the signers, nor can the signers trace back the signature to the corresponding voter.

A threshold blind signature scheme can be defined as a  $(t, N)$ -*threshold signature* scheme. This scheme lets  $N$  parties sign some common data, such that the outcome is a valid signature, if at least  $t$  parties have contributed to the signature [Bo03]. We can simply realize such a scheme by having each party sign the data  $x$  individually and then count the number of valid signatures, in order to decide if the threshold has been reached. In the following we will use a generic description of blind signatures which can be adapted to any blind signature scheme: If  $\mathbf{s} = (s_1, \dots, s_k)$  with  $t \leq k \leq N$  denotes the individual signatures and  $\mathbf{e} = (e_1, \dots, e_N)$  the public keys of the signers, we denote the corresponding verification function by

$$\text{verify}_{\mathbf{e},t}(\mathbf{s}, x) \in \{true, false\}.$$

## 2.2 The Protocol

The common e-voting protocol for such systems involves five entity types (voter, administration, the registration authority, the key authority, voting board) and consists of five consecutive phases:

**Phase 1: Initialization.** The administration initiates the voting process by distributing the empty ballots, and the set of identities of legitimate voters together with their public keys to all necessary entities.

The key authorities create the public-key / secret-key pair for a randomized asymmetric cryptography used during the voting process. In order to dissolve power, the key generation process is done in a distributed way, by using a threshold scheme such as [Ge03] whose description is beyond the scope of this paper.

**Phase 2: Voter Preparation** The voter fills in the empty ballot and randomly encrypts the resulting vote by the public key provided by the key authorities. The resulting message is called the vote. At the end of this phase, the voter is ready to start the registration process.

**Phase 3: Registration** The purpose of the registration phase is to authorize legitimate voters to cast their votes. For this, the voter requests a signature for the blinded vote from at least  $t \leq N$  registration authorities. The blinding of the vote has to be generated for each replicated registration authority separately, as each replicate uses its own private key for signing. The voter sends the blinded vote to each registration authority where it will be signed and returned if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not previously requested another signature during the

voting process. Upon reception, the voter obtains the signatures for the vote by unblinding. If at least  $t$  signatures have been received then the voter is ready to start the vote casting process.

**Phase 4: Vote Casting** The voter sends the vote together with the authorities' signatures anonymously to the public voting board. The board accepts the vote if and only if there are at least  $t$  valid signatures associated to it.

**Phase 5: Counting** The last phase of the e-voting protocol involves the opening of the votes to make them available for counting. For this, the key authorities publicly decrypt the cast votes using the secret part of the key pair. The votes are now ready to be counted by everyone.<sup>1</sup>

### 2.3 Violation of Democracy

We will now demonstrate the attack on democracy by exploiting the properties of the described threshold blind signature protocols.<sup>2</sup>

**Definition 1 (Democracy)** A system is democratic if authorized voters can vote (*eligibility*), and if eligible voters can vote only once (*uniqueness*).

Let us first analyze Phase-3 in more detail where the voter has to address a signing request to at least  $t$  replicates of the registration authority. The voter generates a blinded message for each signer, whereas each blinded message consists of the same vote. Each signer will sign the received message and returns it to the voter. The vote will be declared valid if at least  $t$  different and valid signatures for the vote are provided.

This protocol implicitly violates democracy and therefore can be used as an attack on the e-voting system. As only  $t$  signatures are needed in order to render a vote valid,  $N - t$  signatures can be used for another vote. One voter cannot get more than one valid vote, but a group of voters can. The following example shall demonstrate a possible attack:

- available registration authorities:  $N = 4$
- authority signature threshold:  $t = 3$

A *fair* voter  $V_i$  generates four blinded messages (one blinded message  $w'_{ji}$  per authority  $A_j$ ,  $1 \leq j \leq 4$ ) containing the same vote  $w_i$ :

$$V_i \quad \begin{matrix} A_1 & A_2 & A_3 & A_4 \\ w'_{1i} & w'_{2i} & w'_{3i} & w'_{4i} \end{matrix}$$

---

<sup>1</sup> This phase can be adapted in manifold ways, such as re-encryption to gain receipt freeness or homomorphic counting instead of individual decryption. Since these adoptions distract from the intended focus of this paper and, hence, will not be followed any further.

<sup>2</sup> Many to our colleague Emmanuel Benoist for pointing this out.

Each authority signs the blinded message and returns the signature  $s_{ji}'$  to the voter. To cast the vote  $w_i$ , the voter sends it together with three out of four unblinded signatures  $s_{ji}$  anonymously to the voting board. The voter discards the remaining signature.

A *malicious voter group* consisting of three colluding voters  $V_k, V_l, V_m$ , where  $k, l, m \in \{1, \dots, N\}$  and  $k \neq l \neq m$  can generate an additional vote  $w_x$  resulting in four independent votes:

	$A_1$	$A_2$	$A_3$	$A_4$
$V_k$	$w'_{1k}$	$w'_{2k}$	$w'_{3k}$	$w'_{4x}$
$V_l$	$w'_{1l}$	$w'_{2l}$	$w'_{3x}$	$w'_{4l}$
$V_m$	$w'_{1m}$	$w'_{2x}$	$w'_{3m}$	$w'_{4m}$

The following holds true:

- $w_k$  is rendered valid by the signatures  $s_{1k}, s_{2k}, s_{3k}$  of authorities  $A_1, A_2,$  and  $A_3$ ;
- $w_l$  is rendered valid by the signatures  $s_{1l}, s_{2l}, s_{4l}$  of authorities  $A_1, A_2,$  and  $A_4$ ;
- $w_m$  is rendered valid by the signatures  $s_{1m}, s_{3m}, s_{4m}$  of authorities  $A_1, A_3,$  and  $A_4$ ; and
- $w_x$  is rendered valid by the signatures  $s_{2x}, s_{3x}, s_{4x}$  of authorities  $A_2, A_3,$  and  $A_4$ .

This is possible as the different registration authorities operate independently from each other and, hence, no synchronization takes place amongst them. Even though the attack is not possible on an exponential scale, it is still significant. The quantitative impact of the attack is proportional to the number of colluding voters.

Due to the nature of threshold there always exists a subset of size  $N - t$  authorities not needed in order to get sufficient signatures for a valid vote. Let  $V_c$  be the size of a malicious colluding voter group. Hence, the maximum number of additional votes  $v_+$  that can be rendered valid by the malicious voter group, is:

$$v_+ = \left\lfloor \frac{N - t}{t} V_c \right\rfloor$$

For the threshold values  $N, t$  such that  $\frac{2}{3}N \leq t \leq \frac{3}{4}N$  (see Section 2.1),  $v_+$  is in the range of:

$$\frac{V_c}{3} \leq v_+ \leq \frac{V_c}{2}$$

The violation of democracy shown above is present in all protocols based on threshold blind signature where the blinding procedure results in a different message for every individual signer. Therefore, a common registration board must be used as knowledge base for synchronization amongst the registration authorities.

### 3 E-Voting Protocol Using a Public Registration Board

A public board is a broadcast channel with memory. Data can be broadcast by anyone. By using a guard,<sup>3</sup> the accepted data can be restricted to authorized participants only. Once published, the data can be read by everyone but cannot be altered anymore. The concept of the public board has been introduced by Benaloh et al. [CF85] and [Be87] and brings verifiability to e-voting schemes.

To prevent the violation of democracy, we introduce a public registration board. We assume that the guard of the board guarantees the following properties:

- Only eligible voters can append an entry (using the public key for identification).
- Each eligible voter can append only once.
- Only eligible registration authorities can append signatures (using the public key for identification).
- Each eligible registration authority can append only one signature per eligible voter entry.

#### 3.1 Revised Voting Protocol

By introducing a public board for the registration process, the voter no longer communicates to the registration authorities. Instead, the blinded hash of the encrypted vote is broadcast to the public registration board. In addition, the registration authorities no longer communicate to the voters. Instead, the registration authorities read the public registration board entries and broadcast the signed voter entries back to it. Therefore, the initial Phase 3 of the generic protocol in Section 2.3 needs the following revision:

**Phase 3: Registration** The purpose of the registration phase is to authorize legitimate voters to cast only their votes. For this, the voter requests a signature for the blinded hash of the encrypted vote from at least  $t \leq N$  registration authorities. The voter does so by broadcasting the blinded hash of the encrypted vote along with the public voter key to the public registration board. The registration board will accept the message if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not yet requested another signature during the voting process. These conditions also prevent the public registration board from being flooded. Each registration authority will sign one blinded hash per voter and broadcasts this signature back to the public registration board. Then, the voter can obtain the signatures for the hash by unblinding them. If at least  $t$  signatures have been added to the public registration board then the voter is ready to start the vote casting process.

---

<sup>3</sup> A guard is a predicate on a candidate entry and on the board's state. The predicate must evaluate to true for the entry being added to the board. If the predicate evaluates to true then we call the candidate entry to be *valid*, and it is added. Otherwise, if the predicate evaluates to false then the candidate entry is discarded.

The following revision of the Phase 4 prevents the board from being flooded:

**Phase 4: Vote Casting** The voter sends the encrypted vote, the vote hash, and the authorities' signatures anonymously to the voting board. The board accepts the vote if and only if there are at least  $t$  valid signatures associated to the vote hash.

### 3.2 Public Registration Board Collective

The public registration board presented at the beginning of Section 3 may suffer from some catastrophic failure that prohibits it from fulfilling its duty. It may no longer be able to service its regular clients, or it may be victim of a denial of service attack, with the same effect that prevents regular clients to communicate successfully with the board.

In [HL09], a scheme for a collective of public boards is presented being based on  $N$  peers of identical public boards. As long as a threshold set of  $t$  out of  $N$  public boards function correctly, the integrity of the entries on the boards can be guaranteed by the collective. Each peer accepts and stores the same information as outlined in the beginning of Section 3. In order to write information onto the board, voters and authorities send their messages to one peer of their choice. The peer in turn will then form a threshold set  $t$  of peers to guarantee (in terms of a receipt) the publishing of the message.

There are two versions of the collective: The first one having a *synchronized history*, all peers maintain the same order among the accepted messages. The second version supports the concept of an *unsynchronized history* which satisfies our requirements. To read all messages previously published, however, clients need to consult  $N - t + 1$  peers.

### 3.3 Revised Threshold Blind Signature Schemes

The revision of Phase-3 requires a property which is not present in the normal schemes as defined in Section-2.1. It requires that each signing party (registration authority) is given the *same* blinded data  $x'$  such that the very same data is signed by all parties. Therefore, a new assumption has to be introduced: The blinding and the unblinding function,

$$\begin{aligned}x' &= \text{blind}_{\mathbf{e}}(x, r), \\ \mathbf{s} &= \text{unblind}_{\mathbf{e}}(\mathbf{s}', r),\end{aligned}$$

depend on the public keys  $\mathbf{e}$  of all signing parties.

### RSA Based Threshold Blind Signature

To realize such a scheme based on RSA, we use a common blinding factor  $r^{e_1 \cdots e_N}$  and individual unblinding factors  $r^{-(e_1 \cdots e_{i-1} e_{i+1} \cdots e_N)}$  to obtain classical RSA signatures  $s_i = x^{d_i}$ . Note that if  $m_i$  denotes the modulus for the public key  $e_i$ , then  $m_1 \cdots m_N$  will be an appropriate modulus for  $r^{e_1 \cdots e_N}$ . The individual modulus  $m_i$  can then be used by the  $i$ -th signer to sign the common blinded data  $x'$  and by the recipient of the blind signatures to do the unblinding.

### Schnorr Based Threshold Blind Signature

To realize such a scheme based on Schnorr, we can use the threshold blind signature scheme introduced by Jinho Kim et al. [KKL02]. The original scheme describes the following message flow for the message signing procedure:<sup>4</sup>

1.  $V \rightarrow A_i: \omega_i = \prod_{k=1, k \neq i}^t \frac{k}{k-i}$
2.  $A_i \rightarrow V: e_i = g^{t_i} h^{u_i} \bmod p$  where  $t, u \in_R Z_q$  and  $g, h, p$  setup parameters
3.  $V \rightarrow A_i: x' = \varepsilon - \delta$  where  $\varepsilon = H(x, \hat{e})$ ,  $\hat{e} = e g^\beta h^\gamma y^\delta \bmod p$ ,  $e = \prod_{i=1}^t e_i$  and  $\beta, \gamma, \delta \in_R Z_q$
4.  $A_i \rightarrow V: (R_i, S_i)$  where  $R_i = t_i - x' r_i \omega_i \bmod q$ ,  $S_i = u_i - x' s_i \omega_i \bmod q$  with  $r_i, s_i$  public key of  $A_i$ .

However, even this protocol is still prone to the attack, if used without public registration board, and hence the message flow has to be adapted<sup>5</sup> in order to gain democracy using this protocol:

1.  $A_i \Rightarrow board: (e_i, id_V)$  for each eligible voter
2.  $V \Rightarrow board: (\omega_i, x', id_{A_i})$  for at least  $t$  authorities
3.  $A_i \Rightarrow board: (R_i, S_i, id_V)$

Each authority calculates the commitment for each eligible voter in advance and places them on the public board next to the voter id. Any voter can then start the blinding and signature process. The voter is allowed to present one and only one blinded data  $x'$  on the public registration board.

## 4 Security Analysis

The question whether the attack presented in Section-2 is still possible, can be denied rather intuitively. Every voter can send only one message (a commitment to the voters vote) to be signed to the public registration board. Every registration authority provably

<sup>4</sup> For the sake of readability, the protocol steps presented are stripped down to the signing process. Please refer to the original paper for a more detailed view of the complete protocol.

<sup>5</sup>  $\Rightarrow$  indicates that each message has to be signed by the sender.

signs the very same message per voter. Therefore, no threshold attack can be executed any more, and democracy is established under such circumstances.

We now have to prove that the revision does not introduces other security issues for the whole e-voting process.

**Anonymity:** The introduction of the public registration board seems to raise an anonymity issue. But this is not the case as the only information that can be learned through the public registration board is the fact that some voter initiated the e-voting process. But nothing can be learned of the vote itself nor its containing data. Furthermore, it is not possible to trace the voter's vote. This results in the inability to know if a voter really finished the e-voting process by casting the vote.

**Democracy:** In the revised protocol the registration authorities do not sign the blinded encrypted vote any more but its blinded hash-value. The consequence of this refinement comes into operation only during the vote casting process. As a blindly signed message is a valid message, the public voting board accepts it as being authorized. As a consequence of this, the voting board could be tainted by receiving signed messages from the public registration board. These votes, however, would be invalid and would not affect the final tally. On the other hand, this is a serious issue, and it can be addressed by letting the voting board to accept only the following tuple: Encrypted vote, and the signatures of the hash-value of the encrypted vote.

**Persistence:** The use of the public registration board implies the permanent storage of the signatures. Hence, the voter does not need to keep them anymore. The only information the voter needs to keep at a safe place is the blinding factor.

**Privacy:** If all involved registration authorities collude against a single voter, the voter's privacy is still warranted by the blinding factor the voter has chosen, since finding the correct blinding factor is considered hard [Be01], [KKL02].

## 5 Conclusion

In this paper we demonstrated that any blind signature protocol with threshold bears an intrinsic weakness on democracy and unforgeability of votes, if no public registration board is in use. The public registration board acts as a point of synchronization, where each voter has to give the commitment to only one single blinded message, ready to be signed by all signing authorities. Therefore, a public board not only serves as a means for individual and universal verifiability. The public registration board is an imperative instrument of communication to multiple authorities within a threshold system. Furthermore, we showed that the special requirement, the provably signing the same data, by multiple signers within the threshold signature scheme based on RSA or on Schnorr can be achieved by a refinement of the blinding/unblinding process.



## Bibliography

- [AW07] Aeby, A., and M. Wiget. 2007. On-Line Meinungsumfragen. Diploma thesis, Bern University of Applied Sciences. Biel, Switzerland.
- [AFT07] Anane, R., R. Freeland, and G. Theodoropoulos. 2007. E-voting requirements and implementation. In *CEC '07, 9th IEEE Conference on E-Commerce Technology*, 382–392. Tokyo, Japan.
- [Ba94] Baraani-Dastjerdi, A., J. Pieprzyk, and R. Safavi-Naini. 1994. A practical electronic voting protocol using threshold schemes. Technical report. Wollongong, Australia: University of Wollongong, Department of Computer Science.
- [Ba05] Baiardi, F., A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli. 2005. SEAS, a secure e-voting protocol. Design and implementation. *Computers & Security* 24(8): 642–652.
- [Be01] Bellare, M., C. Namprempre, D. Pointcheval, and M. Semanko. 2001. The one-more-RSA-inversion problems and the security of Chaum’s blind signature scheme.
- [Bo03] Boldyreva, A. 2003. Threshold signatures, multi-signatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In *PKC'03, 6th international workshop on theory and practice in public key cryptography, LNCS 2567*, ed. Y. Desmedt, 31–46. Miami, FL USA.
- [CC96] Cranor, L. F., and R. K. Cytron. 1996. Design and implementation of a practical security-conscious electronic polling system. Technical report WUCS-96-02. St. Louis, MO USA: Washington University.
- [CC97] Cranor, L. F., and R. K. Cytron. 1997. Sensus: A security-conscious electronic polling system for the internet. In *HICSS-30, 30th Hawaii international conference on system sciences, volume 03*, 561–570. Maui, HI USA.
- [CCM08] Clarkson, M. R., S. Chong, and A. C. Myers. Civitas. 2008. Toward a secure voting system. In *SP'08, 29th IEEE symposium on security and privacy*, 354–368. Oakland, CA USA.
- [CF85] Cohen, Josh D., and Michael J. Fischer. 1985. A robust and verifiable cryptographically secure election scheme. In *SFCS '85: Proceedings of the 26th annual symposium on foundations of computer science*, 372–382. Washington, DC USA: IEEE Computer Society.
- [Ch82] Chaum, D. 1982. Blind signatures for untraceable payments. In *CRYPTO'82, 2nd international cryptology conference*, 199–203. Santa Barbara, CA USA.
- [Ch83] Chaum, D. 1983. Blind signature system. In *CRYPTO'83, 3rd international cryptology conference*, 153–156. Santa Barbara, CA USA.
- [Be87] Daniel, J., and Benaloh, C. 1987. Verifiable secret-ballot elections. PhD diss., New Haven, CT, USA.
- [Du99] DuRette, B. W. 1999. Multiple administrators for electronic voting. Bachelor thesis, Massachusetts Institute of Technology. Boston, MA USA.
- [FOO92] Fujioka, A., T. Okamoto, and K. Ohta. 1992. A practical secret voting scheme for large scale elections. In *ASIACRYPT'92, workshop on the theory and application of cryptographic techniques, LNCS 718*, ed. J. Seberry and Y. Zheng, 244–251. Gold Coast, Australia.
- [Ge03] Gennaro, Rosario, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. 2003. Revisiting the distributed key generation for discrete-log based cryptosystems.
- [He97] Herschberg, M. A. 1997. Secure electronic voting using the world wide web. Master’s thesis, Massachusetts Institute of Technology. Boston, MA USA.
- [Hi01] Hirt, M. 2001. Multi-party computation. Efficient protocols, general adversaries, and voting. PhD diss., ETH Zürich. Zürich, Switzerland.

- [HL09] Heather, James, and David Lundin. 2003. The append-only web bulletin board. In *Formal aspects in security and trust, LNCS 5491*, ed. Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, 242–256.
- [JZF03] Joaquim, R., A. Zuquete, and P. Ferreira. 2003. REVS—a robust electronic voting system. In *IADIS international conference e-society 2003*, 95–103. Lisbon, Portugal.
- [Ki02] Kim, K. 2002. Killer application of PKI to Internet voting. In *IWAP'02, 2nd international workshop for Asia public key infrastructures*. Taipei, Taiwan.
- [KKL02] Kim, J., K. Kim, and C. Lee. 2002. An efficient and provably secure threshold blind signature. In, *ICISC'01, 4th international conference on information security and cryptology, LNCS 2288*, ed. K. Kim, 318–327. Seoul, South Korea.
- [Ok97] Okamoto, T. 1997. Receipt-free electronic voting schemes for large scale elections. In *5th international security protocols workshop, LNCS 1361*, ed. B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, 25–35. Paris, France.
- [Oh99] Ohkubo, M., F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. In *ISW'99, 2nd international workshop on information security, LNCS 1729*, ed. M. Mambo and Y. Zheng, 225–234. Kuala Lumpur, Malaysia.
- [RRN01] Ray, I., I. Ray, and N. Narasimhamurthi. 2001. An anonymous electronic voting protocol for voting over the internet. In *WECWIS'01, 3rd international workshop on advanced issues of e-commerce and web-based information systems*, 188–191. San Jose, CA USA.
- [Sc90] Schnorr, Claus-Peter. 1990. Efficient identification and signatures for smart cards. In *CRYPTO '89: proceedings of the 9th annual international cryptology conference on advances in cryptology*, 239–252. London, UK: Springer-Verlag.

**Session 8: Theoretical and Practical Implications of  
E-Voting**



# Coercion-Resistant Hybrid Voting Systems<sup>1</sup>

Oliver Spycher<sup>1</sup>, Rolf Haenni<sup>2</sup>, and Eric Dubuis<sup>2</sup>

<sup>1</sup>Department of Computer Science  
University of Fribourg  
Boulevard de Pérolles 90  
CH-1700 Fribourg, Switzerland  
oliver.spycher@unifr.ch

<sup>2</sup>Research Institute for Security in the Information Society  
Bern University of Applied Sciences  
Quellgasse 21, Postfach  
CH-2501 Biel, Switzerland  
{rolf.haenni,eric.dubuis}@bfh.ch

**Abstract:** This paper proposes hybrid voting systems as a solution for the vote buying and voter coercion problem of electronic voting systems. The key idea is to allow voters to revoke and overrule their electronic votes at the polling station. We analyze the potential and pitfalls of such revocation procedures and give concrete recommendations on how to build a hybrid system offering coercion-resistance based on this feature. Our solution may be of interest to governments, which aim at integrating paper-based and electronic voting systems rather than replacing the former by the latter.

---

<sup>1</sup> Research supported by the Hasler Foundation, project No. 09037.

## 1 Introduction

In consideration of the complexity and manifold vulnerabilities of today's computers and networks, most governments pursue a cautious strategy in introducing electronic means into processes that are so fundamental to running their democracies. Their reservation is particularly distinctive if the technology involves components that are not under their control. The number of countries experimenting with electronic voting over the Internet is therefore still marginal. Estonia and Switzerland, two of the few pioneering countries in Internet elections and referendums (we shall use the general term *voting*), follow the strategy of slowly increasing the number of electronic votes over the years [CH02]. The idea behind keeping this shift at a slow pace is to limit the risk and consequences of fraud in the early stages of the respective project.<sup>2</sup> In the foreseeable future, traditional and electronic voting systems are therefore expected to live side-by-side for quite some time.

Running two or more different voting systems in parallel requires some care. For example, the possibility must be excluded for voters to cast more than one vote, for instance one in each subsystem. The respective systems in Estonia and Switzerland have their own mechanisms to avoid this. The Swiss Canton and Republic of Geneva, for example, issues a voting card that contains a scratch-off panel with a hidden PIN to access the electronic system [CWS06]. Voters that know their PIN can cast their vote electronically. However, a voter needs to show an untouched scratch-off panel to get access to the ballot box or voting booth at the polling station.

Another problem of running more than one voting system in parallel is the fact that the overall voting system is at most as secure as each of its subsystems. If we consider traditional paper-based systems as almost perfectly secure, the security of the overall voting system is directly determined by the security of its electronic subsystem. Every possible weakness of the electronic system automatically poses a security threat to the overall voting system. If for instance the electronic system issues a receipt to the voters that allows them to prove a coercer or vote-buyer how they voted, the overall voting system is subject to fraud. Indeed, *receipt-freeness* and *coercion-resistance* are two of the most difficult properties to achieve in electronic voting systems [BT94, JCJ05, SKR06].

---

<sup>2</sup> The legitimacy of such concerns has been demonstrated by the negative e-voting experience of several countries. In the Netherlands, for example, all nationwide e-voting activities were stopped in 2007 after the vulnerability of the deployed voting machines had been exposed in public [Lo08].

In this paper, we introduce the concept of a *hybrid voting system*, which is more than just running a traditional paper-based and an electronic voting system in parallel to form what we would call an *integrated voting system*. The idea is to exploit the properties of the paper-based voting infrastructure to overturn the weaknesses of the electronic system. In particular, we suggest hybrid voting systems as integrated voting systems extended by a *vote revocation* mechanism, which allows voters to overrule their electronic votes by casting an additional paper vote at the polling station. The idea is thus similar to the re-voting feature of the Estonian Internet voting system, in which voters can to cast multiple votes electronically, but such that only the last vote is taken into account [MM06]. The principle and possible benefits of counting only the “last ballot” has first been mentioned in [Sk02]. It is our proposed counter-measure against the vote buying and voter coercion problem, which is difficult to avoid in pure e-voting systems.

To motivate and define our concept of a hybrid voting system, we start in Section 2 with a general discussion of the vote buying and voter coercion problem in electronic voting systems. Then we present our understanding of a hybrid voting system and explain why they offer coercion-resistance. In Section 3, we give concrete recommendations of how to build a hybrid system with the vote revocation feature. To make our analysis as generic as possible, we first develop a classification of different e-voting systems by looking at the properties of the underlying electronic ballot boxes. We will argue that a hybrid system that prevents vote buying and voter coercion can always be constructed, if the enclosed electronic voting system guarantees that each voter can unambiguously identify his vote in the electronic ballot box. In Section 4, we summarize the main conclusions of our analysis and refer to some of the open problems.

## 2 Hybrid Voting Systems

New voting mechanisms will not find acceptance unless they evidently preserve the security level of traditional paper-based voting. This requirement is inherently difficult to fulfil with e-voting systems and it seems that it is not fulfilled to a satisfactory degree by many of the proposed models or existing systems. Two serious types of fraud that are particularly difficult to prevent and which are largely scalable in electronic systems are *vote buying* and *voter coercion*. In the first part of this section, we describe the challenge of building trustworthy e-voting systems that inherently prevent such types of fraud. Then we show how hybrid voting systems may offer voters a means of voting electronically while keeping the possibilities of such types of fraud as scarce as in traditional paper-based systems.

## 2.1 Vote Buying and Voter Coercion

Whether or not a system has actually implemented required security features is not necessarily transparent to the voters. If they feel that their votes may not even reach the final tally, they might fully restrain from voting electronically and tend to cast their votes in the traditional way, a means of casting votes still likely to be available in the near future. By doing so, they witness the vote reaching the body of the possibly transparent ballot box. Some countries even allow voters to attend the tallying procedure and thus witness the consideration of their votes in the final outcome. To establish a similar level of voters' trust in e-voting systems, it is imperative to give them access to some information that confirms the correct casting of their votes in a convincing way. This confirmation is meant to provide *individual verifiability*, a precondition to trustworthiness of voting systems. The existence of such a confirmation may thus seem like a feature, but since it will generally also convince any third party that a particular vote was cast, it disallows voters to deceive others about their votes. Such information is thus called a voter's *receipt* [BT94]. Its existence is a violation of the voter's privacy, because it opens the door to the following two types of fraud, in which the adversary gets the voter to vote in a prescribed way [Sk02].

**Vote Buying** The voter will be rewarded by the *vote buyer* for voting in a particular manner. To receive the reward, the voter may actively co-operate with the vote buyer, e.g. by deviating from the normal voting procedure to construct a receipt.

**Voter Coercion** The voter is put under pressure or threatened by a *coercer* to vote in a particular manner. Here, the voter may only consent to co-operate with the vote buyer as long as the threat is perceived as real.

Note that both forms of exploiting a voting system are largely scalable in an electronic environment. A vote buyer could simply set up a web site explaining the conditions for making easy money, while a coercer could easily post his threats to thousands of voters. In both cases, the attack is only interesting to potential adversaries as long as voters are able to prove them how they voted. Without a receipt, a corrupted voter could simply lie about the vote cast, i.e., the motivation of an adversary even launching such an attack in the first place is likely to be as low as with paper-based votes.

Clearly, it must be a primary objective to establish an e-voting system that is immune to all sorts of vote-buying and voter-coercion attacks, including those in which the adversary gets the voter to abstain from voting or to vote at random. Systems blessed with that immunity are called *coercion-resistant* [JCJ05, SKR06]. Note that coercion-resistance is stronger than mere *receipt-freeness* [BT94, JV06], which alone does not prevent adversaries from getting voters to abstain from voting. In the literature, there are many suggestions for receipt-free or coercion-resistant systems, but most of them rely on unrealistic technical assumptions such as untappable communication channels [BT94, Ok97, HS00, MBC01, LBD03, SKR06, XS06, MN06, CLW08].

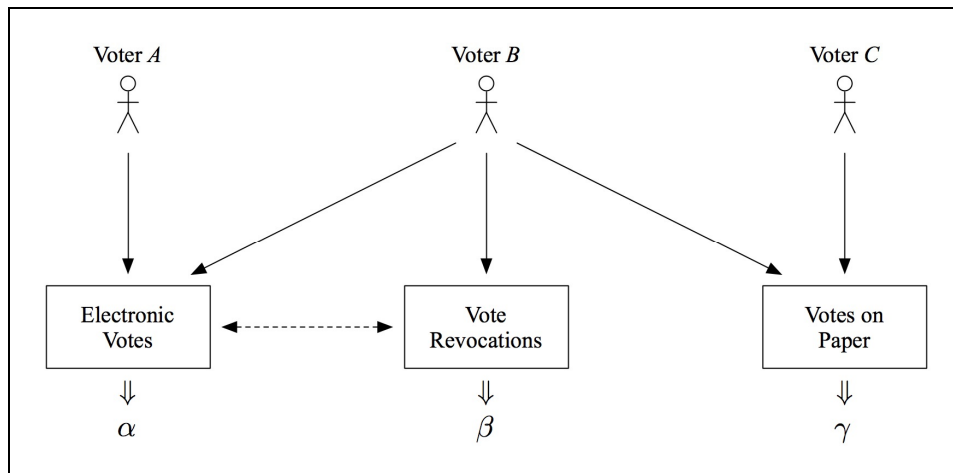


## 2.2 Hybrid Systems

A hybrid voting system offers every voter the choice between either casting a vote electronically or casting a traditional paper vote at the polling station. The key to undermining the possibility of exploiting the electronic subsystem for the above-mentioned types of fraud is to allow the voters to revoke their electronic votes at the polling station and then to let them cast the vote of personal choice in the traditional way, i.e., inside the (presumably) coercion-free environment of the polling station. Clearly, the revocation mechanism must be designed in a way that an adversary cannot find out which votes have been revoked. In Subsection 3.2, we will propose two different solutions to that problem. Both solutions include three different ballot boxes: the  $\alpha$ -box for the electronic votes, the  $\beta$ -box for the vote revocations, and the  $\gamma$ -box for the paper votes. The final outcome  $\Sigma$  of the voting can then be calculated as

$$\Sigma = \alpha - \beta + \gamma,$$

where  $\alpha$ ,  $\beta$ , and  $\gamma$  denote the individual results of the respective ballot boxes.<sup>3</sup> This model with three ballot boxes is illustrated in Figure 1. Depending on the revocation mechanism, the  $\beta$ -box may contain revocations either in electronic form or on paper. Clearly, each vote in the  $\beta$ -box must reflect the corresponding vote from the  $\alpha$ -box.



**Figure 1:** Three types of ballot boxes and voters in a hybrid voting system: Voter *A* votes electronically; Voter *B* first votes electronically, but then overrules it by a paper vote; Voter *C* votes on paper.

<sup>3</sup> We do not further specify here whether the ballot boxes contain simple yes/no-votes or more complicated 1-out-of- $n$  or  $k$ -out-of- $n$  selections. In the latter cases,  $\Sigma = \alpha - \beta + \gamma$  must be applied component-wise to each of the  $n$  options.

**Coercion-Resistance** In a hybrid system with a vote revocation procedure, even if an adversary is contently convinced that the voter cast the electronic vote as told, there is still the possibility that the vote will be overruled by the voter's personal choice and thus not be considered in the final tally. Only by witnessing the voter entering the polling station, it becomes apparent to the coercer that the voter's intention is most likely to revoke the vote. However, monitoring the entrance of a polling station is not easily scalable to a large number of corrupted voters. Furthermore, since the possibility of hindering voters from going to the polling station is also given in traditional, well-accepted paper-based systems, it does not prevent hybrid systems from reaching the same level of coercion-resistance as their traditional counterparts.

We conclude that if adversaries must assume that corrupted voters will usually revoke their votes, a hybrid system is clearly coercion-resistant: an attack would simply seem too expensive. We believe that it is possible for governments to invoke that perception among adversaries, for instance by explicitly allowing voters to cooperate with vote buyers and coercers, however only as long as they revoke their biased vote.

**Prerequisites** Remarkably, pure electronic voting systems and the electronic subsystems of hybrid voting systems do not necessarily share the same prerequisites. For example, the great challenge of removing receipts from pure e-voting systems does no longer apply to the electronic components of a hybrid voting system. Not only are receipts admitted, their guaranteed presence may even be a prerequisite in the design of a hybrid system. One of the proposed methods in Subsection 3.2 requires such guaranteed receipts. In general, we are less restrictive by imposing the following two basic prerequisites for the e-voting component of a hybrid voting system:

1. The system guarantees the presence of a vote identifier to ensure that the voters can identify the votes in the  $\alpha$ -box that were generated using their credentials. Receipts are special cases of such vote identifiers.
2. The system provides some mechanism that allows voting officials at the polling station to check whether or not a registered voter has already cast an electronic vote.

Voting systems complying with the second prerequisite form an integrated voting system. Note that in general the guaranteed existence of a vote identifier (first prerequisite) is insufficient for the voting officials to verify whether someone has cast an electronic vote or not (second prerequisite). Because if such an identifier is secret to the voter, the existence of the electronic vote could be concealed by simply withholding the identifier. Complying with the first prerequisite alone does not therefore imply the property of an integrated voting system. Similarly, the existence of a mechanism to check if somebody has already voted electronically (second prerequisite) is in general not enough to identify that person's vote in the  $\alpha$ -box (first prerequisite), because the system may provide a list of voters that is completely disconnected from the list of votes. Thus, hybrid voting systems form a stronger notion than mere integrated voting systems.

In the absence of a receipt, the first prerequisite can be met by leaving the encrypted vote attached to information that publicly identifies the voter. In order to preserve the voters' privacy, the individual votes clearly may never be decrypted in this case, not even at the time of tallying. Instead, homomorphic methods for tallying exist, where only the result of the tally needs to be decrypted [CGS97, HS00]. By applying this method, even the second requirement is inherently met. We thus conclude that the prerequisites we impose on the electronic subsystem of a hybrid system do not form obstacles that are particularly hard to overcome.

### 3 Vote Revocations in Hybrid Systems

We now consider the construction of a coercion-resistant hybrid voting system. To prevent vote buying and voter coercion, we need to define a secure vote revocation mechanism that allows voters to update their electronic votes at the polling station. For the solution presented in this section, we assume that the electronic subsystem provides the two key prerequisites discussed at the end of the previous section. We assume thus the existence of an electronic ballot box, in which the electronic votes are collected (the  $\alpha$ -box). Additionally, we suppose that the traditional voting infrastructure satisfies the following three minimal requirements.

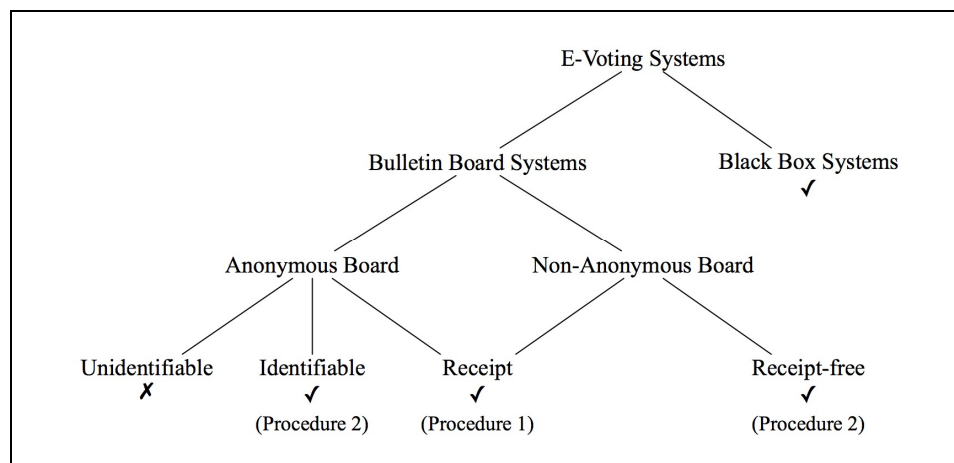
1. The traditional voting infrastructure consists of a polling station, where the paper votes of registered voters are anonymously collected in a physical ballot box (the  $\gamma$ -box).
2. The traditional voting procedure at the polling station (checking the identity of voters, opening the ballot box, counting the votes, etc.) is sufficiently secure, in particular coercion-resistant, and the voting officials are reliable and trustworthy.
3. The official voting period at the polling station chronologically succeeds the electronic voting period.

To understand the applicability of the proposed vote revocation procedures, we first need to get an overview of the different types of electronic ballot boxes in e-voting systems. The result of this discussion in Subsection 3.1 is a classification of e-voting systems, from which two fundamentally different situations emerge. For each of these cases, we propose in Subsection 3.2 a corresponding vote revocation procedure that fits into the proposed counting scheme of a hybrid system.

### 3.1 Classification of E-Voting Systems

A common core component of all existing e-voting systems is an electronic ballot box, in which votes are collected during the voting period. One can think of it as a database with two basic operations for adding new entries and reading its content. To ensure the availability and the correctness of these operations, and to guarantee the integrity and consistency of the database, a variety of security measures need to be implemented. Some of these measures aim at avoiding so-called single points of failure, i.e., critical components capable of causing the entire system to fail.

Depending on the chosen configuration and properties of the electronic ballot box and the structure of its entries, different e-voting systems emerge. In the remainder of this subsection, we will make a distinction between black box and bulletin board systems, anonymous and non-anonymous boards, identifiable and non-identifiable board entries, and the presence or absence of a receipt. In Figure 2, we give a first overview of this classification and indicate where vote revocations are possible.



**Figure 2:** Classification of existing e-voting systems with different types of electronic ballot boxes. The check marks indicate where vote revocations are possible.

**Black Box vs. Bulletin Board Systems** E-voting systems mainly differ in the type of database access they provide. There are two extreme cases, one in which the access is restricted to a few authorized persons only and one in which everybody can add new entries to the database and read its contents (while deleting entries is always prohibited). E-voting systems of the first category are sometimes called black box voting systems [HA03, KKW06]. They are very popular in commercial solutions and in existing political e-voting projects. An advantage of black box systems is that from a cryptographic point of view, they are relatively simple to understand and implement. On the other hand, they are often criticized as not providing enough transparency, i.e., neither providing individual verifiability nor allowing the outcome to be publicly verified.

The second major category comprises systems with a public bulletin board, through which all cast votes are visible to everybody [Pe05]. To ensure the secrecy of the votes and the fairness of the voting process, the board's entries need to be encrypted (at least during the official voting period). The purpose of the public board is to allow all voters to verify the inclusion of their votes in the electronic ballot box and the correctness of the counting. Most system proposals in the scientific e-voting literature are based on such bulletin boards.

**Anonymous vs. Non-Anonymous Boards** In bulletin board systems, there are two opposed subcategories, each defined by whether the entries on the board are anonymous or not. In the case of anonymous boards, there must be an additional mechanism to exclude votes from unauthorized voters or multiple votes from the same voter. Examples of such mechanisms are mix nets [Ch81] or blind signatures [Ch82]. If the board entries are not anonymous, for example if they contain a unique voter ID that attributes them unambiguously to the respective voters, there must be a mechanism that prevents the decryption of single votes. Systems of that type are usually based on homomorphic encryption schemes with a shared public key [CGS97, HS00]. Clearly, in those systems, the publicly known voter ID serves as the vote identifier.

**Vote Identifiers vs. Receipts** Another distinguishing feature of bulletin board systems concerns the board entries themselves. There are three basic types: those which can be identified and disclosed with a receipt, those which can only be identified with a vote identifier (but not disclosed), and those which are completely unidentifiable. In the case of a non-anonymous board, where the identification of the votes is given intrinsically, only two types of board entries remain, those with a receipt and those without. These cases are depicted at the bottom of the tree shown in Figure 2.

### 3.2 Vote Revocation

In the classification tree of the previous subsection, four cases are tagged with a check mark and one is crossed out. The cross means that the case of an anonymous board with unidentifiable board entries is not compatible with any vote revocation procedure. The missing vote identifier makes it impossible to either remove the vote from the electronic ballot box or to subtract it from the final tally. Note that by explicitly requiring the existence of vote identifiers at the end of Section 3, we had already ruled out this case from the beginning.

In black box systems, it is possible to install a vote revocation mechanism as long as the electronic votes in the ballot box remain identifiable. Due to the lack of transparency offered by such systems, the correct application of a potential revocation mechanism cannot be verified by the public. We therefore leave revocations using a black box approach undiscussed.

**Procedure 1: Revocations on Paper** The first procedure we propose assumes that every voter owns a receipt for his vote in the  $\alpha$ -box. It does not matter whether the board is anonymous or not, but it is crucial that the voter (and not the coercer or vote buyer alone) is in possession of the receipt. The payoff of this restriction is a revocation procedure that is particularly appealing in its simplicity.

The following points define the procedure. We start off when the voter at the polling station is about to revoke the electronic vote in the  $\alpha$ -box, i.e., we assume that the voting officials have already successfully checked the voter's identity and right to vote.

1. The voter uses the receipt to locate the encrypted vote in the  $\alpha$ -box and reveal it to the voting officials.
2. The voting officials prepare a revocation paper ballot containing the same vote and hand it over to the voter.
3. The voting officials verify that the voter drops the revocation paper ballot into the  $\beta$ -box.
4. The voter is granted access to the  $\gamma$ -box to cast the final paper vote.

In this procedure, the  $\beta$ -box is thus a physical ballot box similar to the  $\gamma$ -box. At the end of the official voting period, it is opened and tallied according to the same tallying procedure.

In the scheme as it is proposed, it is crucial to assume that the voting officials will not allow the voters to cast a paper ballot that differs from their electronic votes in the  $\alpha$ -box. If not all voting officials are fully trustworthy, then several voting officials should be involved in each step of the procedure. In other words, before the voter gets access to the  $\gamma$ -box, a sufficient number of voting officials would have to give their approval, for instance by signing the revocation ballot. Thus, we merely need to assume that among the group of involved voting officials, there is at least one that would refuse the signature to an incorrect revocation ballot.

A drawback of this procedure is the fact that the content of the electronic vote must be revealed to the voting officials. One could argue that this violates the anonymity of the vote, because in a simple yes/no-type of voting, evoking a yes-vote implies that the update will be a no-vote, and vice versa. But since such conclusions will always remain speculative, i.e., it cannot be excluded that the original and the updated votes are identical, we think that this is an unpleasant, but acceptable side effect.

Note that by requiring instead of avoiding a receipt, we sharply depart from the mainstream approach of taking additional measures to make electronic voting systems receipt-free. Yet, the following procedure shows how vote revocations can be realized even without receipts.

**Procedure 2: Electronic Revocations** Let the e-voting component of the hybrid system now be a system that provides a mere vote identifier, not necessarily a receipt. The idea then is to leave the votes encrypted throughout the whole revocation procedure. To guarantee the anonymity of those who decide to revoke their votes, and thus to ensure the overall system remains coercion-resistant, we define the  $\beta$ -box as an anonymous bulletin board to which re-encryptions of the original votes are posted. The adversary is then unable to make out which votes from the  $\alpha$ -box have been revoked. The electronic voting environment must therefore comply with the following additional requirements.

- The  $\beta$ -box must be an anonymous bulletin board.
- The encryption scheme used to generate the encrypted votes in the  $\alpha$ -box must allow re-encryption<sup>4</sup> and the generation of non-transferable proofs of correct re-encryption.<sup>5</sup>

---

<sup>4</sup> Let  $w = E(v, r)$  be the encrypted vote, where  $E$  is a randomized encryption function with randomization factor  $r$ . Then  $w' = R(w, r')$  denotes the re-encryption of  $w$ , such that the decryptions of  $w$  and  $w'$  are identical, i.e.,  $v = D(w) = D(w')$ .

<sup>5</sup> A proof of correct re-encryption allows a prover to convince a verifier that  $w'$  is indeed a re-encryption  $R(w, r')$  of  $w$ , without revealing the randomization factor  $r'$ . A proof constructed as an *interactive  $\Sigma$ -protocol* is inherently non-transferable, i.e., only the involved verifier will be convinced of its correctness [BG92]. Corresponding non-interactive protocols are transferable, but there is a general way of extending them to be convincing to a designated verifier only [JS196].

The following steps define the proposed procedure:

1. The voter generates a re-encryption of the encrypted vote in the  $\alpha$ -box.
2. A corresponding non-transferable proof of correct re-encryption is generated, designated to the voting officials at the polling station. Optionally, this step can be done remotely in a non-interactive manner.
3. The voter approaches the voting officials and uses the vote identifier to identify the encrypted vote in the  $\alpha$ -box.
4. The voter hands the re-encryption and the corresponding non-transferable proof over to the voting officials.
5. If the delivered proof is valid, the voting officials post the re-encrypted vote to the  $\beta$ -box.
6. The voter is granted access to the  $\gamma$ -box to cast the final paper vote.

The electronic  $\beta$ -box is tallied according to the tallying procedure defined for the  $\alpha$ -box.

Similarly to Procedure 1, we can enhance the scheme by requiring a sufficient number of voting officials to approve the correctness of the voter's re-encryption, i.e., a voter would only be granted access to the  $\gamma$ -box if sufficiently many voting officials have posted their electronic signatures of the re-encryption to the bulletin board.

Clearly, the randomization factor used for the re-encryption may serve as a receipt. The voter can therefore always prove to an adversary that the electronic vote has been revoked, but he or she will never be interested in doing so. On the other hand, the receipt does not help to prove to an adversary that the electronic vote has *not* been revoked. It thus does not reduce the security level of the overall system.

## 4 Conclusion

Governments around the world intend to offer their citizens e-voting as a comfortable way to express their political preferences. Yet, it seems that the traditional paper-based schemes are not likely to disappear for some decades. Defining procedures that integrate both means of casting votes to an overall voting system clearly poses an inherent necessity. We propose our understanding of hybrid voting systems as a solution to this challenge. By introducing the anonymous  $\beta$ -box and by exploiting the traditional polling station as a protective environment, we allow voters to revoke their electronically casted votes. We argue why such an approach yields coercion-resistance, even if the electronic subsystem were indeed subject to coercion. In a hybrid system, we are therefore given the freedom to have an e-voting subsystem that grants receipts to satisfy individual verifiability, without introducing the risk of vote buying or voter coercion.



## Bibliography

- [BG92] M. Bellare and O. Goldreich. On defining proofs of knowledge. In E. F. Brickell, editor, CRYPTO'92, 12th Annual International Cryptology Conference on Advances in Cryptology, LNCS 740, pages 390–420, Santa Barbara, USA, 1992.
- [BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In STOC'94, 26th Annual ACM Symposium on Theory of Computing, pages 544–553, Montréal, Canada, 1994.
- [CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. *European Transactions on Telecommunications*, 8(5):481–490, 1997.
- [Ch81] D. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
- [Ch82] D. Chaum. Blind signatures for untraceable payments. In CRYPTO'82, 2nd International Cryptology Conference, pages 199–203, Santa Barbara, USA, 1982.
- [CLW08] S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In NDSS'08, 15th Network and Distributed System Security Symposium, pages 81–94, San Diego, USA, 2008.
- [CWS06] M. Chevallier, M. Warynski, and A. Sandoz. Success factors of Geneva's e-voting system. *Electronic Journal of e-Government*, 4(2), 2006.
- [Di02] Die Bundesbehörden der Schweizerischen Eidgenossenschaft. Bericht über den Vote Electronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte. *Bundesblatt*, 154(5):645–700, 2002.
- [DKR06] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In CSFW'06: 19th IEEE workshop on Computer Security Foundations, pages 28–42, Venice, Italy, 2006.
- [HA03] B. Harris and D. Allen. *Black Box Voting: Ballot Tampering in the 21st Century*. Plan Nine Publishing, 2003.
- [HS00] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, EUROCRYPT'00, International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 1807, pages 539–556, Bruges, Belgium, 2000.
- [JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In V. Atluri, S. De Capitani di Vimercati, and R. Dingledine, editors, WPES'05, 4th ACM Workshop on Privacy in the Electronic Society, pages 61–70, Alexandria, USA, 2005.
- [JSI96] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In U. Maurer, editor, EUROCRYPT'96, International Conference on the Theory and Application of Cryptographic Techniques, LNCS 1070, pages 143–154, Saragossa, Spain, 1996.
- [JV06] H. L. Jonker and E. P. Vink. Formalizing receipt-freeness. In ISC'06, 9th Information Security Conference, LNCS 4176, pages 476–488, Samos, Greece, 2006.
- [KKW06] A. Kiayias, M. Korman, and D. Walluck. An internet voting system supporting user privacy. In ACSAC'06, 22nd Annual Computer Security Applications Conference, pages 165–174, Miami Beach, USA, 2006.
- [LBD03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, ICISC'03, 6th International Conference on Information Security and Cryptology, LNCS 2971, pages 245–258, Seoul, Korea, 2003.

- [Lo08] L. Loeber. E-voting in the Netherlands: from general acceptance to general doubt in two years. In R. Krimmer and R. Grimm, editors, 3rd International Workshop on Electronic Voting, Lecture Notes in Informatics, pages 21–30, Bregenz, Austria, 2008. Gesellschaft für Informatik E.V.
- [MBC01] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In B. Schmid, K. Stanoevska-Slabeva, and V. Tschammer, editors, I3E'01, 1st IFIP Conference on towards the E-Society, volume 202, pages 683–694, 2001.
- [MM06] Ü. Madise and T. Martens. E-voting in Estonia 2005: The first practice of country-wide binding internet voting in the world. In R. Krimmer, editor, 2nd International Workshop on Electronic Voting, number P-86 in Lecture Notes in Informatics, pages 15–26, Bregenz, Austria, 2006. Gesellschaft für Informatik E.V.
- [MN06] T. Moran and M. Naor. Receipt-free universally-verifiable voting with everlasting privacy. In C. Dwork, editor, CRYPTO'06, 26th Annual International Cryptology Conference on Advances in Cryptology, LNCS 4117, pages 373–392, Santa Barbara, USA, 2006.
- [Ok97] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, 5th International Security Protocols Workshop, LNCS 1361, pages 25–35, Paris, France, 1997.
- [Pe05] R. A. Peters. A secure bulletin board. Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, The Netherlands, 2005.
- [Sk02] J. Skripsky. Minimal models for receipt-free voting. Semester project, ETH Zürich, 2002.
- [XS06] Z. Xia and S. Schneider. A new receipt-free e-voting scheme based on blind signature. In WOTE'06, IAVoSS Workshop on Trustworthy Elections, pages 127–135, Cambridge, U.K., 2006.

# **E-voting in Japan: A developing case?**

Masahiro Iwasaki

College of Law  
Nihon University  
2-3-1 Misaki-cho, Chiyoda-ku,  
Tokyo 101-8375  
JAPAN  
[iwasaki@mtj.biglobe.ne.jp](mailto:iwasaki@mtj.biglobe.ne.jp)

**Abstract:** This paper aims to introduce the current situation of electronic voting (e-voting) in Japan and discuss its challenges. E-voting has gradually spread in Japan. It has been used a total of twenty times by ten local governments since it was first introduced in 2002. Under the current law, e-voting can be used only for the election of the head of local government or council members. The paper first introduces the actual state of e-voting in Japan. Then the current status and challenges of the electronic voting system are analyzed based on data obtained from the experiences of Japanese cases. Finally, the paper discusses what challenges the Japanese e-voting has, and what could be given as prescriptions for them.

## **1 Current Status of E-voting in Japan**

In 2002, the first electronic voting (e-voting) was realized in Japan. Since then, ten local governments conducted a total of twenty cases of e-voting. In Japan, after “e-Japan Strategy<sup>1</sup>,” which aims to build an electronic government (e-government<sup>2</sup>), was published in January 2001 many efforts toward an electronic government (e-democracy) and electronic democracy have been attempted<sup>3</sup>. E-voting can be considered within this trend<sup>4</sup>.

This paper aims to introduce the current status of e-voting in Japan and to discuss its challenges. The paper first introduces the actual state of e-voting in Japan. Then the current status and challenges of the electronic voting system are analyzed based on data obtained from experiences of Japanese cases<sup>5</sup>. Finally, the paper discusses what challenges Japanese e-voting has, and what could be given as prescriptions for them. In Japan, the “Act on Special Provisions Concerning Voting Method by Means of

---

<sup>1</sup> <http://www.kantei.go.jp/jp/singi/it2/kettei/010122honbun.html>

<sup>2</sup> See [An07], [Ha99], [Ho08], [Kh09], and [No01].

<sup>3</sup> The concept of “electronic democracy” is vague and it has various meanings. See [Fe00], [Gi04], [Ha99], [Hi98], [Iw05], [To98], and [Ts98].

<sup>4</sup> <http://www.kantei.go.jp/jp/singi/it2/index.html>

<sup>5</sup> See [Iw04] and [Iw09].

Electromagnetic Recording Voting Devices Used for Election of Council Members and Heads of Local Governments (hereafter ‘E-voting Act’)” was enacted in the 153<sup>rd</sup> extraordinary Diet session on November 30, 2001<sup>6</sup>. The Act was issued on 7 December and put into effect on 1 February 2002, which enabled e-voting for local elections. The E-voting Act is intended only for elections of a local government head or a member of a local council. Each local government is required to establish its own ordinance before holding any e-voting.

For example, in the case of Niimi City, Okayama Prefecture, Niimi City Council enacted the “Ordinance Concerning Voting by Means of Electromagnetic Recording Voting Devices Used for Elections of Council Members and Mayor of Niimi City” in March 2002<sup>7</sup>. This enabled e-voting in the double election of Niimi City Mayor and the Council members on 23 June of the same year<sup>8</sup>. Since then, there have been total of twenty cases of e-voting by ten local governments<sup>9</sup>. This number indicates that the dawn of e-voting in Japan is over and the country is now in the phase of establishment.

## 2 Introductory Phase of E-voting

According to the E-voting Act, e-voting is defined as a means of voting that uses a device. The current procedures for such an electronic voting method in Japan are as follows:

- First, an elector goes to a designated polling station on an election day.
- The elector is required to bring an admission ticket to his/her polling station, which s/he has received in the mail in advance.
- When the elector hands the admission ticket to the reception at the polling station, a staff person checks his/her identification by comparing the name of the elector with the register of electors.
- When the personal identification has been confirmed, a voting card is issued from a voting card issuing device by the staff, which is handed to the elector.
- The elector stands in front of a voting device and inserts the voting card; this initiates the device.

---

<sup>6</sup> [http://www.soumu.go.jp/senkyo/senkyo\\_s/news/touhyou/denjiteki/pdf/houritsu.pdf](http://www.soumu.go.jp/senkyo/senkyo_s/news/touhyou/denjiteki/pdf/houritsu.pdf)

<sup>7</sup> We can experience a demonstration of e-voting on the website of Niimi City.

<http://www.city.niimi.okayama.jp/?ID=10973>

<sup>8</sup> <http://www.city.niimi.okayama.jp/?ID=9901>

<sup>9</sup> A total of twenty cases of e-voting by ten local governments are as follows: (1) Niimi City, Okayama Prefecture, (2) Hiroshima City, Hiroshima Prefecture, (3) Shiroishi City, Miyagi Prefecture, (4) Sabae City, Fukui Prefecture, (5) Kani City, Gifu Prefecture, (6) Otama Village, Fukushima Prefecture, (7) Ebina City, Kanagawa Prefecture, (8) Rokunohe Town, Aomori Prefecture, (9) Kyoto City, Kyoto, Prefecture, and (10) Yokkaichi City, Mie Prefecture.

- The elector selects a candidate of his/her choice from a list of candidates shown on the touch-panel screen by touching the appropriate name, using his/her finger or a touch pen (if not voting for any candidate, the elector touches a display that says, “Complete without Voting;” this will allow the elector to complete his/her vote without choosing any candidate).
- The elector confirms the selected candidate.
- The voting result is recorded in an electromagnetic recording medium inside the electronic voting device.
- The elector removes the voting card from the voting device.
- The voting process is now complete; the elector returns the voting card at the exit, and leaves the polling station.

Contrary, the current procedures for a traditional paper ballot voting method in Japan (which is called “self-write voting”) are as follows:

- First, an elector goes to a designated polling station on an election day.
- The elector is required to bring an admission ticket to his/her polling station, which s/he has received in the mail in advance.
- When the elector hands the admission ticket to the reception at the polling station, a staff person checks his/her identification by comparing the name of the elector with the register of electors.
- When the personal identification has been confirmed, a ballot paper is handed to the elector by the staff.
- The elector writes the name of a candidate from a list of candidates (if not voting for any candidate, the elector does not write any name; this will allow the elector to complete his/her vote without choosing any candidate).
- The elector casts the ballot paper into the ballot box.
- The voting process is now complete; the elector leaves the polling station.

Therefore, e-voting in Japan is considered an evolved form of self-write voting, rather than a method completely different from the conventional self-write voting. The Study Group describes this aspect in detail in a report on “Election Systems Using Electronic Devices within the Ministry of Internal Affairs and Communications<sup>10</sup>.”

---

<sup>10</sup> [http://www.soumu.go.jp/menu\\_news/s-news/2002/pdf/020201\\_2.pdf](http://www.soumu.go.jp/menu_news/s-news/2002/pdf/020201_2.pdf)

On 30 July 1999, the former Ministry of Home Affairs established the Study Group on Election Systems Using Electronic Devices. The Group released the final report on 1 February 2002, indicating that the introduction of e-voting has three phases as described below. In Japan, the implementation of the first phase has been the focus.

- The first phase is when an elector votes using an electronic voting device at a designated polling station.
- The second phase is when an elector can vote at a polling station other than a designated one.
- The third phase is when voting at a polling station is not required, and an elector votes using a privately-owned computer terminal.

The first phase is the form that has been implemented in Japan. In this phase, electronic voting devices are not connected to any network; they are individually installed both in polling stations and vote-counting stations. An elector has to go to a designated polling station as one has always done.

The only difference from the conventional method is that an elector votes by using a voting device, not self-write voting, at a polling station.

When counting votes, the challenge is to find a method to deliver voting data to a vote-counting station. The recording medium that stores voting data is removed from the voting device at the polling station, and delivered to the vote-counting site. This is the same procedure as the one in self-write voting, where the ballot box holding ballot paper is delivered to the vote-counting station.

Currently, the recording medium that stores data is hand-delivered from the polling station to the vote-counting station by election staff. The other possible delivery method is to send the data over a network connecting the polling station and vote-counting site. This method has not been adopted in the first phase since it still contains various issues, including security.

The second phase networks includes voting devices installed at polling stations with a dedicated line. The line used in this phase is to be closed for security issues. The register of electors needs to be networked for the personal identification of electors at polling stations. The network is also necessary to share information about the candidates.

In the second phase, voting at a polling station other than a current designated one becomes possible. In this case, either of the following will be chosen: (1) voting at any polling station within the same electoral district; (2) voting at any polling station within all the electoral districts of the same election; and (3) voting at any site including areas not having an election.

The voting at any polling station within the same electoral district enables an elector to vote at a nearby polling station in an area where s/he lives, rather than a current designated polling station. For example, an elector can vote at the closest polling station when s/he goes out for shopping.

The voting at any polling station within all the electoral districts of the same election enables, for example, an elector to vote at any polling station within a prefecture, if it is for a prefectural election. For the election of Tokyo Metropolitan Mayor, an elector can vote in any ward other than Chiyoda Ward even if it is not his/her designated polling station.

The voting at any site including areas not having an election enables an elector to vote in Kyoto Prefecture, if there is a polling station, even when the election is for Tokyo Metropolitan. Also, an elector can vote at a site other than a polling station if it is authorized for voting.

For all of the above three scenarios in the second phase, establishing a network for the register of electors or for sharing candidate information will be necessary. The register of electors is used for identifying if a person who comes to vote is a particular elector, and the list will be operable depending on the status of the Basic Resident Registers Network and Local Government Wide Area Network.

In the third phase, instead of requiring electors to vote at polling stations as a conventional system does, it is assumed that a computer owned by each elector would be used for voting. If all elections are conducted by the third phase method, a polling station itself may become unnecessary. In this phase, a standard internet connection, not a dedicated line, would be utilized as each individual's computer is used. Thus security issues are unavoidable. Also, the issue of the Digital Divide—including whether an elector can use a computer and whether s/he has a computer, or not—becomes crucial.

The problem of identification at the time of voting also emerges. Since identification based on a register of electors at a polling station is not performed in the third phase, as the current system does, it is difficult to identify if a person sitting in front of a computer is a particular elector. Therefore, it is necessary to prevent impersonation by identity verification with public key cryptography as well as biometrics using fingerprints and irises.

In addition, since third parties such as observers at a polling station do not exist in the third phase, it becomes unclear if a voting individual is voting based on his/her true free will. For example, there could be a possibility that an elector is forced to vote for a particular candidate under abduction/confinement. Considering that the existence of observers at polling stations in the current system guarantees the transparency of elections, it is crucial how to resolve the transparency issue in the third phase voting.

Judging from the evolution of ICT, it could be possible to implement the third phase e-voting. However, from the perspective of operating an election, the third phase is quite unrealistic. E-voting is still in the first phase in Japan, and it seems more likely that the situation will continue as it is now. There are many issues to be resolved in order to shift to the second phase, and those issues are not easy to solve. It is crucial to steadily accumulate the experiences of e-voting in the first phase<sup>11</sup>.

---

<sup>11</sup> Cf. [Ke04].

### 3 Characteristics of E-voting in Japan

The intrinsic changes are overlooked if e-voting is viewed as a mere change from self-write voting to a method using devices. In fact, if one focuses only on e-voting, one's perspective would be that it is just a change of voting methods. However, e-voting indicates a new form of election in an ICT-prevailing society<sup>12</sup>. The newness of e-voting can be described by four aspects: voting, tallying, communication and vote-counting methods.

	Self-write voting	E-voting
Voting method	Using a ballot paper	Using a voting device
Tallying method	Using a ballot box	Using a voting device
Method of communicating voting data	Delivery of the ballot box from the polling station to the vote-counting station	Delivery of the recording medium from the polling station to the vote-counting station
Vote-counting method	Staff	Computer

**Table 1:** Self-write voting and e-voting in contemporary Japan

First, the voting method differs significantly from conventional self-write voting in using a voting device, and the newness lies in voting with a device instead of voting by a paper ballot. A voter casts a ballot by operating a voting device at a polling station, and the vote is stored as it is in the device. Containing a recording medium that stores voting data, the device plays the double role of writing down the vote onto a paper ballot and accumulating ballots in a ballot box, as it was done in self-write voting. That is in e-voting, the device itself has the double function of casting ballots and storing voting data. This brings both advantages and disadvantages.

The advantages include the simplification of voting for voters due to the use of a device. As the currently-used voting device adopts a touch-panel, the act of voting is done with only a light touch on a screen. For example, it is easier for physically challenged voters to touch a device than self-write voting. It is clear that e-voting makes voting simpler than self-write voting does.

The second advantage is the accuracy of voting, which is related to the first advantage. In e-voting, as a voter chooses a candidate to vote from a list of candidates displayed on

<sup>12</sup> Cf. [Fe00], [Gi03], [Gi04], [Ha00], [Ha99], and [Oa06].



a screen, s/he can only vote for those on the list. However, in self-write voting, voters often write a name other than that of a candidate, or misspell a name, which results in invalid ballots. Voters may also write down only the last name or the first name. In self-write voting, a typical problem is when there are more than one candidate with the same last name; in such a case, votes are equally divided among both candidates. On the contrary, e-voting ensures the accuracy of voting by avoiding the above issue since a voter has no choice, but to vote for candidates displayed on a screen for a certain election.

The third advantage is that of being barrier-free. E-voting leads to a barrier-free system by making it easy for the elderly and the physically-challenged to vote. There are voters who have difficulty writing on ballots with a pencil, and it is easy for them to vote using a device. For those who are optically challenged, voting with audio guidance becomes available by using an appropriate voting device. Such voters can vote at their own pace since they operate the device by listening to audio guidance with headphones and can adjust audio speed. Such voting devices have already been developed in Japan. Although the current voting device supports optical challenges, promoting a barrier-free device for those who are both optically and aurally challenged, or those who are intellectually challenged is an issue to be resolved.

The disadvantages include the failure of a voting device, errors in device operation, and distrust in a voting device such as the leakage of privacy, and the cost issue of a device. In other words, issues related to a device become the disadvantages. If a device fails, voting itself becomes impossible. While bringing many advantages by using a device, e-voting could cause disadvantages exactly because it uses a device.

In fact, there were several cases where voting discontinued due to the failure of a voting device or a device failed due to errors in operation. In the case of Kani City, Gifu Prefecture, the election itself became invalid as it was determined that the failure of their voting devices affected the result.

The possibility of privacy leakage can be noted in terms of distrust of a device. Voters often have a variety of distrust such as: A device might record who voted for whom upon voting; or it is unclear if a ballot was truly cast for the candidate whom the voter has chosen. There is no other solution to clear up as much distrust as possible other than to improve the reliability of e-voting. It can be time consuming; however, it is indispensable to make efforts in establishing reliability.

Additionally, there is the issue that the cost of a voting device is high. Indeed, the E-voting Ordinance was abolished in Sabae City, Fukui Prefecture, due to the high cost<sup>13</sup>. However, a special local grant tax measure is applied when implementing e-voting, and financial support is available according to the number and size of polling and vote-counting stations. More specifically, the amount provided is based on a calculation that multiplies designated unit price depending on the number of polling and vote-counting stations. The special local grant tax amount is the sum of polling station expenses and vote-counting station expenses.

---

<sup>13</sup> See [Iw04].

Although there exists an image that e-voting is costly, assistance is actually available. It is necessary to provide information about the actual operational status, including the fact that the previous cases adopted rental devices instead of purchased ones. It is not necessarily reality that it takes a tremendous cost and high risks in order to introduce e-voting from scratch.

Next, a tallying method is related to one that stores voting data in an electronic voting device. So far, there are two data recording methods for electronic voting devices: a standalone method and a client-server method. Most of the cases in Japan have adopted the standalone method, although there were two cases that used the client-server method. The two differ in the tallying methods of electronic voting devices. In simple terms, the standalone method is equipped with one recording medium per voting device, while the client-server method uses one recording medium per polling station. In the case of the standalone method, if there are five electronic voting devices at one voting station, five recording media will be delivered from the polling station to the vote-counting station, since each device has one recording medium. The client-server method uses one recording medium per polling station. Thus there is one recording medium however many voting devices are installed at one polling station. One server is set up for each polling station, connecting multiple voting devices, and voting data is collected in the server. In delivering data from the polling station to a vote-counting station, the collected data on the server is transferred to a magneto-optic disk (MO), which will be delivered to the vote-counting station.

Although the two collection methods have their own advantages and disadvantages, there is a reason that the standalone method is more likely to be adopted when considering issues in reality. This method can minimize any damage in case trouble occurs. Even if one voting device fails in a polling station, it can be immediately replaced with a back-up device. In this way, there will be almost no influence on voting that follows. As the recording medium equipped in the failed machine has the voting data up to the time of the failure, it is delivered to the vote-counting station. Obviously, the voting data reflects the will of voters, thus it cannot be made invalid or destroyed. The standalone method provides two recording media; one is original and the other is a duplicate. Therefore, if the original recording medium did not store data properly, or the medium was damaged, the duplicate can serve in place of the original.

On the other hand, since the client-server method collects voting data in one recording medium by a server regardless of the number of voting devices at a polling station, there is a possibility that all of the voting devices at the polling station would be unusable if the server fails. Even if each voting device is operable, voting is no longer possible as voting data cannot be recorded. In fact, trouble due to server failure occurred in the e-voting in Kani City in July 2003. Later, a lawsuit was initiated regarding the e-voting in Kani City, and the election itself was determined invalid.

Based on such history, the standalone method is more widely adopted<sup>14</sup>. The collection method for e-voting employs a voting device that stores voting data in a recording medium, which leads to a question: An indication that paper medium should also be used

---

<sup>14</sup> Exceptionally, two of twenty cases of e-voting in Japan adopted a client-server method. Otama Village and Ebina City used it.

since recording voting data only in a voting device would cause difficulty if the device or its recording medium fail. This is the notion that self-write voting be applied, for use in an emergency, along with e-voting. It is true that this would prevent the loss of voting data at the time of any trouble.

Also, there is a proposal for countermeasures suggesting that paper ballots be prepared in case of device failure and that self-write voting using the paper ballots replace e-voting, if there is any device failure. This proposal would result in higher costs since costs for providing voting devices and preparing paper ballots are both necessary for one election. This leads to a discussion about whether e-voting should be introduced with such costs.

At this moment, there are two methods for tallying, and no alternative method has been proposed or considered to be put into practice. It is worth examining the various methods. However, voting methods or tallying methods that are significantly different from the implementation of e-voting would never facilitate any discussion, even if they were proposed.

Next, methods of communicating voting data are discussed. They are the delivery methods from a polling station to a vote-counting station. What is necessary, when voting time on an election day is over and a polling station is closed, is the delivery of voting data to the vote-counting station. In the case of self-write voting, ballot boxes are delivered to vote-counting stations as they are. In e-voting, a recording medium is removed from the e-voting device, sealed, stored, and locked in a strong container, and delivered to a vote-counting station. Basically the delivery of voting data from a polling station to a vote-counting station is the same as the conventional method. The only difference is whether it is a ballot box with paper ballots inside or a recording medium storing voting data.

At this moment, the delivery of voting data is handled in the same way as the conventional method, since the implementation of e-voting is still in the first phase as it is defined in the report issued by the Ministry of Internal Affairs and Communications' Study Group of Election Systems Using Electronic Devices<sup>15</sup>. When voting time is over, a ballot box is closed and delivered to a vote-counting station by car. Thus the most important factor in e-voting is to deliver a recording medium quickly and safely to a vote-counting station. When e-voting is implemented in the second and third phases in the future, it is unnecessary to maintain the current delivery method. For example, in the second phase, each polling station would have a dedicated network. If security issues such as intrusion by hackers are resolved, voting data can be delivered to a vote-counting station through such network. Then the communication method of voting data will see a dramatic change. In the third phase, voting would be done from a work place or a computer at home. There will be security issues, but it will be significantly different from the current first phase in terms of data delivery. In this phase, further study is needed to determine whether polling stations should be set up, and whether a means of collecting voting data from all voters and delivery it to polling stations is necessary. Also, it is possible to collect all the voting data at each polling station and send them to a vote-counting station, or to send the data accordingly to a vote-counting station through a network.

---

<sup>15</sup> [http://www.soumu.go.jp/menu\\_news/s-news/2002/pdf/020201\\_2.pdf](http://www.soumu.go.jp/menu_news/s-news/2002/pdf/020201_2.pdf)

If the second and third phases are implemented, the method of communicating voting data could be transformed significantly while maximizing the advantages of ICT. Although there are mountains of issues to resolve before that, there are various possibilities for future communication methods. Since the current e-voting follows the same conventional method, the advantage of e-voting is not yet very clear in terms of its communication method. In other words, there will be more advantages depending on how communication methods are utilized in e-voting.

The fourth notable point is the vote-counting method. In e-voting, the important task is to read a recording medium delivered to a vote-counting station by a computer, not to take out paper ballots from a ballot box. The reading itself is the vote-counting process. In the standalone method, the more voters an area has, the more recording media there will be, since one electronic voting device has one recording medium. Those who are in charge of vote-counting process would be one staff person who operates the recording media on a computer, and the other who checks and confirms the computer operation, which means that only two people are necessary. Compared to self-write voting, this is a significant cutback in labor, and leads to the reduction of labor costs. When a recording medium is read by a computer, the data is quickly calculated and the voting result is displayed on the screen. The vote-counting result is revealed when the displayed result is printed.

The E-voting Act defines that an electronic voting device shall not be connected to an electric communication line. Thus, this is the limit to reducing vote-counting time. It is because the data must be delivered from the polling station to the vote-counting station, and the current method cannot shorten this delivery time. In the future, if a polling station and a vote-counting station are networked and the delivery of voting data is done in a second over the network, even further reduction of time will be possible. The reasons for prohibiting the connection to electric communication circuits include security issues. Since there is the possibility of unauthorized access from outside, such as by hackers, security measures must be thorough. One option for security measures is use a closed, dedicated network. By doing so, it is possible to prevent unauthorized access.

The advantages of vote-counting methods in the current first phase are as follows: There are no illegible ballots there is no equal division of ballots; there is a reduction of vote-counting time; and a reduction of labor in vote-counting tasks. All of these are significantly different from the conventional self-write voting. The voting, tallying, communication, and vote-counting methods of e-voting have completely different features from those in the conventional self-write voting, thus could achieve significant effect depending on how they are used<sup>16</sup>.

---

<sup>16</sup> See [Iw04] and [Iw09].

## 4 Issues in E-voting

In order to popularize e-voting, it is most important to prevent troubles due to mechanical failure. Some solutions have been gradually proposed, and the current measures are discussed below.

In November 2005, the Ministry of Internal Affairs set up the Research Committee on E-voting System<sup>17</sup> as a “permanent research entity that provides advisory functions from a professional standpoint regarding a way of an e-voting system, bringing new structure for improving reliability of the system into view.” In March 2006, the Committee put together a report, “Basic Policy Regarding a Measure for Improving Reliability of E-voting System.” The report stresses measures for trouble prevention in E-voting, addressing technical requirements of electronic voting devices and certification systems of technical requirements for improving reliability. It notes that there were three factors in past troubles: First, the contents defined by technical requirements themselves were inappropriate or insufficient; second, prior confirmation of whether an individual electronic voting device complied with technical requirements was not sufficient; and third, there were issues in operating the voting devices. Solutions to the first factor include the analysis of troubles from the past and a thorough investigation of the validity of the technical requirements, as well as the reinvestigation into the necessity of the legal binding power of technical requirements. For the second factor, it was suggested that the necessity of introducing a certification system should be examined in order to confirm compliance with technical requirements by third parties. For the third factor, it is important to follow through on improvement measures and to create manuals for those in charge of conducting the e-voting.

Traditionally, confirming compliance with technical requirements only involved self-inspection by manufacturers and joint inspection with an election committee at delivery to an implementing municipality. For self-inspection, manufacturers only had to submit a self-inspection certificate at the time of delivery. Thus the report noted that “instead of commissioning inspections to manufacturers and local public agencies, it is necessary to introduce a system of confirming compliance by third parties in order to prevent further occurrence of mechanical troubles and ensuring the reliability of E-voting system.” The municipalities that have already conducted e-voting also suggested the necessity of a certificate system by third parties.

In response to the above report, on 18 December 2006, the Ministry of Internal Affairs and Communications issued the revised technical requirements and “Implementation Guideline for Confirming Compliance Regarding the Technical Requirements of E-voting System.” Upon request for inspection by a manufacturer, a private inspection agency under contract with the Ministry is to confirm the compliance with technical requirements, and the result is to be publicized. It is an advantage for manufacturers to have e-voting devices with confirmed compliance as defined by the certification system. It is also true for each election committee or each municipality, since they can use devices of a certain technological level when choosing devices and implementing

---

<sup>17</sup> [http://www.soumu.go.jp/main\\_sosiki/kenkyu/denshi\\_touhyo/index.html](http://www.soumu.go.jp/main_sosiki/kenkyu/denshi_touhyo/index.html)

E-voting. Basically, it is not only that a certification system can prevent unnecessary trouble, but also that it is indispensable. An inspection agency reports the results to the Ministry after the inspection and submits a “Report on Inspection and Verification of Electromagnetic Recording Voting System” to the Minister of Internal Affairs and Communications. The Ministry publishes the verification results upon receiving the report of the inspection results.

After the certification system was introduced in December 2006, Shiroishi City and Rokunohe Town held elections using e-voting on 22 April 2007. It was the third implementation of E-voting for both municipalities. The certification system was put into practice for those two cases, and E-voting devices that complied with technical requirements were used in the two elections. Until today, a couple of other cases of elections using E-voting have been held, and no significant cases of trouble have occurred.

Although the introduction of the certification system is useful for preventing troubles, what kind of and when an incident would happen will always remain unknown as E-voting involves devices. Thus manufacturers and governments are required to make constant efforts in the research and development of e-voting, as well as measures that envision various situations. Work is not completed once a system is established; revisions and improvements are required in e-voting, as in any other systems.

Lastly, the introduction of e-voting to national elections is mentioned here. As of December 2007, the Liberal Democratic Party and the New Komeito, which are the ruling parties, and the Democratic Party of Japan agreed on the introduction of E-voting to national elections. They worked to enact the bill in the Diet, and it passed the House of Representatives. However, it was withdrawn as an unfinished bill in the House of Councilors. At that time, the bill suggested that E-voting in national elections would be allowed only for municipalities with E-voting ordinances. However, the deliberation proceeded with difficulty around measures against the failure of voting devices, and time eventually ran out. Although the bill was withdrawn, it is notable that the introduction of E-voting was discussed officially. Furthermore, the fact that the bill passed the House of Representatives implies that there is some possibility of implementing E-voting in national elections. In Japan, the possibility of putting E-voting into reality seems to have been expanding gradually from local elections to national elections.

## Bibliography

- [An07] Anttiroiko, A. et al. 2007. *Encyclopedia of digital government, 3 Vols.* Hershey: Idea Group Reference.
- [Be06] Benz, A, et al. 2006. *Governance and democracy. Comparing national, European and international experiences.* London: Routledge.
- [Co09] Contini, F. et al. 2009. *ICT and innovation in the public sector. European studies in the making of e-government.* New York: Palgrave Macmillan.
- [Da08] Dai, X. et al. 2008. *The internet and parliamentary democracy in Europe. A comparative study of the ethics of political communication in the digital age.* London: Routledge.
- [Dr05] Driike, H. et al. 2005. *Local electronic government. A comparative study.* London: Routledge.
- [Fe00] Ferdinand, P. et al. 2000. *The internet, democracy and democratization.* London: Frank Cass.
- [Gi03] Gibson, R. et al. 2003. *Political parties and the internet. Net gain?* London: Routledge.
- [Gi04] Gibson, R. et al. 2004. *Electronic democracy. mobilisation, organization and participation via new ICTs.* London: Routledge.
- [Ha00] Hacker, K. L. et al. 2000. *Digital democracy. Issues of theory and practice.* London: Sage, 2000.
- [Ha99] Hague, B. et al. 199. *Digital democracy. Discourse and decision making in the information age.* London: Routledge.
- [Hi98] Hill, K. et al. 1998. *Cyberpolitics. Citizen activism in the age of the internet.* Lanham: Rowan & Littlefield Publishers.
- [Ho08] Homburg, V. 2008. *Understanding e-government. Information systems in public administrations.* London: Routledge.
- [Iw04] Iwasaki, M. 2004. *E-voting* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.
- [Iw05] Iwasaki, M. et al. 2005. *E-democracy* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.
- [Iw09] Iwasaki, M. 2009. *E-democracy and e-voting* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.
- [Ke04] Kersting, N. et al. 2004. *Electronic voting and democracy. A comparative analysis.* New York: Palgrave Macmillan.
- [Kh09] Khosrow-Pour, M. 2009. *E-government diffusion, policy, and impact. Advanced issues and practices.* Hershey: Information Science Reference.
- [Mä04] Mälkiä, M. et al. 2004. *eTransformation in governance. New directions in government and politics.* Hershey: Idea Group Publishing.
- [No01] Norris, P. 2001. *Digital divide. Civic engagement, information poverty, and the internet worldwide.* Cambridge: Cambridge University Press.
- [Oa06] Oates, S. et al. 2006. *The internet and politics. Citizens, voters and activists.* London: Routledge.
- [Pi00] Pierre, J. et al. 2000. *Governance, politics and the state.* New York: Palgrave Macmillan.
- [Sh04] Shane, P. et al. 2004. *Democracy online. The prospects for political renewal through the internet.* New York: Routledge.
- [To98] Toulouse, C. et al. 1998. *The politics of Cyberspace.* New York: Routledge.
- [Ts98] Tsagarousianou, R. et al. 1998. *Cyberdemocracy. Technology, cities and civic networks.* London: Routledge.