TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

TECHNISCHE UNIVERSITÄT DARMSTADT

e-voting.cc

Robert Krimmer and Melanie Volkamer (Eds.)

6th International Conference on Electronic Voting

EVOTE2014

28–31 October 2014, Lochau/Bregenz, Austria

Co-organized by

Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance

Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt

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

IEEE
Region 8 (Europe)

Gesellschaft für Informatik
German Informatics Society, SIG SEC/ECOM

PROCEEDINGS

IEEE

German Informatics Society

Robert Krimmer and Melanie Volkamer (Eds.)

6th International Conference on Electronic Voting

EVOTE2014

28–31 October 2014, Lochau/Bregenz, Austria

Co-organized by the Tallinn University of Technology, Technische Universität Darmstadt, E-Voting.CC, IEEE and Gesellschaft für Informatik

TUT PRESS

Proceedings EVOTE2014
TUT Press

ISBN 978-9949-23-685-5 (PDF)
ISBN 978-9949-23-688-6 (publication)

Volume Editors

Prof. Dr. Robert Krimmer
Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance
Akadeemia tee 3
12618 Tallinn
Estonia
E-mail: robert.krimmer@ttu.ee

Prof. Dr. Melanie Volkamer
Technische Universität Darmstadt
Hochschulstrasse 10
64289 Darmstadt
Germany
E-mail: melanie.volkamer@cased.de

Citation Recommendation: Author (2014): Title. In: Krimmer, R., Volkamer, M.: Proceedings of Electronic Voting 2014 (EVOTE2014), TUT Press, Tallinn, p. xx-yy.

printed by TUT Press, Tallinn

Printed with grateful support from the Austrian Federal Ministry of the Interior.

Preface

In 2004, the first Conference on Electronic Voting took place at Castle Hofen. Since then, the biannual EVOTE conference has become a central meeting place for e-voting researchers with different backgrounds and e-voting practitioners including vendors, observers, and election authorities. This conference is one of the leading international events for e-voting experts from all over the world. Cumulatively, over the years 2004, 2006, 2008, 2010 and 2012 more than 450 experts from over 30 countries have attended this conference to discuss electronic voting topics.

In so doing, they have established Bregenz as a regular forum and point of reference for the scientific community working with e-voting. One of its major objectives is to provide a forum for interdisciplinary and open discussion of all issues relating to electronic voting. The multidisciplinary EVOTE conference celebrate this year its tenth birthday. This year is centered on the theme "Verifying the Vote" and to review what has been accomplished since 2004. We are particularly happy to convince IEEE to publish EVOTE papers as post proceedings with them.

The diversity and multidisciplinary of EVOTE is also reflected in the program committee of EVOTE 2014 and in the 17 papers selected. These 17 papers were selected out of the 33 submissions based on a double blind-review process. 10 of the 17 accepted papers will also be published with IEEE. The program also features three invited talks:

- Yulimar Quintero Trumbo (Election Expert):
  Electoral Technology: Observations across Latin America
- Vanessa Teague (University of Melbourne):
  Trust and Verifiability in Australian E-voting
- Geo Taglione and Oliver Spycher (Swiss Federal Chancellery)
  Internet Voting in Switzerland - Where We Stand Today
-

The accepted papers represent a wide range of technological proposals for different voting settings (be it in polling stations, remote voting or even mobile voting) and case studies from different countries already using electronic voting or having conducted first trial elections.

Special thanks go to the international program committee for their hard work in reviewing, discussing and shepherding papers. They ensured the high quality of these proceedings with their knowledge and experience.

We also would like to thank the German Informatics Society (Gesellschaft für Informatik) with its ECOM working group for their partnership over several years. A big thank you goes also to the Austrian Federal Ministry of the Interior and the Regional State of Voralberg, for their continued support. Further thanks go to the platinum conference sponsor Scytl.

Tallinn, Darmstadt, October 2014 Robert Krimmer, Melanie Volkamer

This conference is co-organized by:

Tallinn University of Technology -
Ragnar Nurkse School of Innovation and Governance

Technische Universität Darmstadt -
Center for Advanced Security Research Darmstadt

E-Voting.CC GmbH -
Competence Center Electronic Voting & Participation

IEEE – Region 8 (Europe)

Gesellschaft für Informatik,
German Informatics Society, SIG SEC/ECOM

Supported by:

Federal Ministry of the Interior - Austria

Regional Government of Vorarlberg

Sponsored by:

Scytl S.A. – Platinum Sponsor

International Programme Committee

Alvarez, Michael Caltech, USA
Araujo, Roberto Universidade Federal do Pará, Brazil
Bannister, Frank Trinity College, Ireland
Barrat, Jordi EVOL2 - -eVoting Legal Lab / University of Catalonia, Spain
Benaloh, Josh Microsoft, USA
Besselar, Peter van den Vrije Universiteit Amsterdam, Netherlands
Beznosov, Konstantin University of British Columbia, Canada
Bismark, David Votato, Sweden
Bock Segaard, Signe Institute for Social Research, Norway
Braun Binder, Nadja Research Institute Public Administration Speyer, Germany
Buchsbaum, Thomas Ministry for European and Internat. Affairs, Austria
Bull, Christian Ministry of Local Government and Modernisation, Norway
Caarls, Susanne Federal Ministry of the Interior, Netherlands
DeGregorio, Paul A-Web, USA
Dittakavi, Chakrapani CIPS, India
Drechsler, Wolfgang Tallinn University of Technology, RNS, Estonia
Dubuis, Eric Bern University of Applied Science, Switzerland
Gibson, Paul Telecom SudParis, France
Gjosteen, Kristian NTNU Trondheim, Norway
Grechenig, Thomas INSO, Technical University Vienna, Austria
Grimm, Ruediger University of Koblenz, Germany
Gronke, Paul Reed College, USA
Haenni, Rolf Bern University of Applied Science, Switzerland
Hall, Joe Lorenzo CDT, USA
Hall, Thad University of Utah, USA
Imamura, Catsumi Centro Técnico Aeroespacial, Brazil
Kalvet, Tarmo Tallinn University of Technology, RNS, Estonia
Kersting, Norbert University of Muenster, Germany
Kim, Shin D. Hallym University, S.Korea
Kuesters, Ralf University Trier, Germany
Koenig, Reto Bern University of Applied Science, Switzerland
Nurmi, Hannu University Turku, Finland
Prandini, Marco DISI, University of Bologna, Italy
Pereira, Oliver Université catholique de Louvain, Belgium
Pomares, Julia CIPPEC, Argentina
Reniu, Josep Maria University of Barcelona, Spain
Rios, David Academy of Sciences, Spain
Ruggeri, Fabrizio CNR IMATI, Italy
Ryan, Mark University of Birmingham, United Kingdom
Ryan, Peter Y A University of Luxembourg, Luxembourg
Schneider, Steve University of Surrey, United Kingdom
Schuermann, Carsten ITU, Denmark
Schoenmakers, Berry TU Eindhoven, Netherlands
Serduelt, Uwe ZDA, Switzerland
Stein, Robert Federal MoI, Austria
Teague, Vanessa University of Melbourne, Australia
Tokaji, Dan Ohio State, USA
Trechsel, Alexander EUI, Florence, Italy
Wenda, Gregor Federal MoI, Austria
Wikström, Douglas KTH Royal Institute of Technology, Sweden
Zagorski, Filip University of Wroclaw, Poland
Zissis, Dimitris Aegean University, Greece

Conference Chairpersons

Krimmer, Robert Tallinn University of Technology, RNS, Estonia
Volkamer, Melanie Technische Universität Darmstadt, CASED, Germany

PhD Colloquium Chairpersons

Koenig, Reto Bern University of Applied Science, Switzerland
Barrat, Jordi EVOL2 - -eVoting Legal Lab / University of Catalonia, Spain

Organizational Committee

Traxler, Gisela E-Voting.CC, Austria (Main Contact)
Budurushi, Jurlind TUD, Germany
Meyerhoff Nielsen, Morten TUT, Estonia
Rincon Mendez, Angelica TUT, Estonia

Content

Experiences with Internet Voting

The Patchwork of Internet Voting in Canada

Nicole J. Goodman
Munk School of Global Affairs, University of Toronto
Toronto, Canada
nicole.goodman@utoronto.ca

Jon H. Pammett
Department of Political Science, Carleton University
Ottawa, Canada
jon.pammett@carleton.ca

***Abstract*— Internet voting developments in Canada are growing quickly, with activity focused in local elections, political party leadership votes and unions. In some instances, the federal structure of the Canadian state facilitates Internet voting use, while in others it inhibits it. The result of this system of divided jurisdiction is that Internet voting use in Canada resembles a patchwork, showing strong concentration in some areas and no penetration in other places. In addition to scattered geographic use, a variety of approaches to implementation are employed. In some cases online ballots are complementary to paper, while in others elections are now fully electronic. I-voting can be a two-step process requiring registration or a more direct one-step voting procedure. Likewise, Internet voting is offered in the advance portion of certain elections, whereas in others it is available for the full voting period. Finally, given that private companies administer the Internet voting portion of elections there is also a mixture of technology.**

Keywords—Internet voting; Canada; federalism; elections

I. INTRODUCTION

Canada possesses a multi-level governance structure[1], one where the various units often have effective control over their own electoral methods. This has resulted in a patchwork of Internet voting implementations within the country. Electoral Management Bodies (EMBs) with effective implementation power include Elections Canada (federal elections), provincial bodies like Elections Ontario, and offices of municipal government in hundreds of local areas. These agencies are subject to relevant legislation or regulations issued by federal and provincial parliaments, and by municipal councils. At times, this has resulted in instructions to implement trials of electronic voting methods, and in other instances specific prohibitions have been issued to prevent the use of such alternative voting methods. At other times, election agencies are left to make their own decisions, though they have usually sought approval from legislatures or councils before undertaking actual electoral trials.

This system of divided jurisdiction has resulted in the development of a substantial amount of Internet voting over the last decade. At the local level, nearly 2 million people have had opportunities to vote by Internet. These Internet elections have been concentrated in two provinces, Ontario and Nova Scotia. In Nova Scotia about one-third of communities have used Internet ballots, while in Ontario about one-quarter of the municipalities will do so in October 2014, comprising one-fifth of the provincial electorate. Supportively worded legislation in these provinces has enabled municipalities there to decide which voting methods to use. The Canadian constitution provides for overall provincial supervision (and ultimate control) of municipal governments. Municipalities are bound to carry out elections based on the framework established in *Municipal Elections Acts* written by the provinces. Providing a supportive legislative framework is in place, municipal governments have relative autonomy to implement experimental voting methods, and there is a substantial amount of local experimentation occurring.

This pattern is mirrored in another layer of Canadian governance, that of First Nations communities – bands of Aboriginal groups settled across the country. The overall system for governing First Nations elections is complex, but in many cases they are able to determine their own voting method. First Nations communities are now beginning to adopt Internet ballots in band elections and other types of votes such as referendums; to date they have been used in the provinces of Ontario and British Columbia.

Two further sets of Canadian institutions have made extensive use of Internet voting in their own internal operations. Many political parties at both the federal and provincial levels use the Internet to conduct leadership votes (local elections are nonpartisan), in keeping with the trend to choose their leaders by one person-one vote procedures involving the membership of the party [6]. Use of Internet voting for leadership votes is becoming so popular it is now the norm rather than the exception. Secondly, Canadian unions and professional/business associations have been steadily adopting Internet voting for their elections, with hundreds of these organizations making the switch to online ballots. Some Internet voting service providers report that these defined-group elections provide the bulk of their business [22].

II. INTERNET VOTING IN CANADIAN GOVERNMENTS

A. Federal Government

Federal elections in Canada are the responsibility of Elections Canada (EC). At present, EC is responsible for the administration of elections, regulating donations and campaign finances, and a variety of outreach and education initiatives. The bulk of its responsibilities surrounding the management of elections are laid out in the *Canada Elections Act* [4]. A bill recently passed in the House of Commons and now pending approval in the Senate, called the *Fair Elections Act*, made a number of changes to the role of the agency. Though Internet voting has not been trialed federally, current legislation requires that EC obtain approval from a parliamentary committee prior to moving forward. The *Fair Elections Act*, however, now requires that a provision for online ballot use be

[1] Federalism in Canada divides powers of government between national, sub-national and local levels, each which manage their own elections.

approved in both houses of the federal Parliament (including the unelected Senate), severely reducing the likelihood of Internet voting trials in federal elections.

EC has been researching Internet voting for some time and previously committed to carrying out a trial as part of its 2008-2013 Strategic Plan. Various operational considerations delayed this experiment, pushing the prospective trial back to 2015, and then again to 2019. Difficulties in relations between EC and the current Conservative government have made the agency more hesitant to undertake a trial, and it is now unclear when or if it will take place.

B. Provinces

Elections in Canada's ten provinces are administered by EMBs in each province. These are modelled on EC, led by a Chief Electoral Officer (CEO) accountable to the provincial legislature, and report to the legislative assembly either directly, through a committee, or in some cases via the Speaker of the House [15, 16, 18, 21, 23]. Various protocols surrounding the operation and management of provincial elections are outlined in pieces of legislation which typically include a primary *Elections Act*, an act pertaining to election finances, and various other regulations. In many cases EMBs have the authority to make recommendations to the provincial parliament.

No province currently has a legislative provision that would specifically permit the use of Internet voting in a general election; however, some have sections in their *Elections Act* that permit the CEO to test equipment in a by-election, which could allow an Internet voting trial. Elections Ontario, Elections Alberta, and Elections New Brunswick, for example, have such clauses in their *Elections Acts*. It is on this basis that Ontario plans to carry out an Internet voting trial in a future by-election. The introduction of these clauses has been part of a trend to support the modernization of electoral processes, perhaps triggered by declining voter turnout figures and needs to improve accessibility. Elections Alberta, for example, introduced new wording in 2008 to provide the opportunity for the CEO to test technology in hopes of modernizing the electoral process there [23]. Provinces without this section in their electoral legislation would need to have a provision added before proceeding with such a trial.

Most provincial EMBs have been researching the possibilities of Internet voting for about a decade, but trials have not occurred as early as originally expected. Elections Ontario, for example, was given a legislative mandate in 2010 to research 'network voting' and report back to the legislature, but this was pushed back due to financial considerations. Twelve interest groups were consulted in this process as well as the public through an online questionnaire. A report was issued in 2013, which suggested a test would not be as soon as expected [10]. Elections British Columbia recently issued a report that was the result of consultation with experts and some public input, whose findings recommend not proceeding with Internet voting at this time [9]. Elections Saskatchewan has taken a similar stance, issuing a public statement stating that online voting will not be implemented in the next general election (2015/2016). Smaller eastern provinces such as Prince Edward Island and New Brunswick have felt reluctant to be first to trial the technology and await the lead from a larger province. It seems Ontario has the greatest likelihood of proceeding with Internet voting in the near future. Because of online voting activity at the municipal level in Ontario, many of the province's electors have become familiar with this voting method.

Finally, we should note the lack of information and resource sharing among governments and between levels of government. There is some coordination at the top of EMB organizations, as the CEOs meet annually. Several provincial EMBs have come together in a national Electoral Voting Working Group facilitating some horizontal cooperation and information sharing regarding Internet voting, albeit the last meeting was held in 2012 [15]. At lower layers of the provincial bureaucracies, however, there is not the same institutionalized collaboration. Vertically, between national, sub-national, and local levels of government, there is not much dialogue either.[2] This lack of discourse has resulted in federal and provincial EMBs and local governments carrying out research and preparing reports in their respective silos. Even once a report is prepared, a series of internal approvals must often be sought before the document can be shared with other EMBs and governments, let alone the public. In the case of Ontario, for example, a Business Case for Internet voting was prepared, but the document was not available for sharing within the EMB community for six months, while approvals to circulate were obtained [21]. It is likely this lack of dialogue contributes to the patchwork of use and also implementation, explored below.

C. Municipalities

Municipal clerks have the responsibility to administer elections at the local level in Canada, and these local election officials have considerable independent authority to implement elections as they see fit.[3] This responsibility comes from the *Municipal Elections Act*. Clerks have the independent authority to determine how the election is administered, providing it complies with the requirements in the *Act*. However, some election aspects such as the voting method, the length of the advance voting period, and voting hours, must be approved by city councils before the administration can move forward [3]. In this sense local officials are bound not only by legislation written by the provinces, but also by the decisions of local councils when it comes to being able to implement Internet voting programmes.[4]

In their *Municipal Elections Acts,* at present, only the provinces of Ontario and Nova Scotia have clauses supporting the use of and/or experimentation with alternative voting

The authors would like to thank SSHRC for financially supporting the research.

[2] Saskatchewan started a program this year where the CEO of Elections Saskatchewan meets with six city clerks (five from larger municipalities and one from a more rural community) to discuss elections in the province. There is no standard format for how this will proceed, but it has provided a starting point for dialogue between the province and some municipalities [16].

[3] The one exception is the province of New Brunswick, which runs both provincial and municipal elections [15]. In some other areas (e.g. Prince Edward Island) the provincial EMB assists municipalities with the administration of elections [18].

[4] Municipalities are groups of communities that comprise a province. They range in population, population density, and land area and are responsible for the administration and delivery of local services.

methods. In British Columbia, municipalities including Vancouver and Nanaimo passed resolutions to enable the use of Internet voting, but were halted from moving forward when the province refused to support use of the voting method in local elections. The provincial election agency, Elections BC, assembled an independent electoral panel in September 2012 to advise on the possibility of using Internet voting for provincial and municipal elections. The panel eventually recommended to the provincial parliament that Internet voting not be implemented for local or provincial elections at this time [9]. In this way, the current structure of provinces controlling the legislation governing local Canadian elections has inhibited Internet voting as much as it has enabled it.

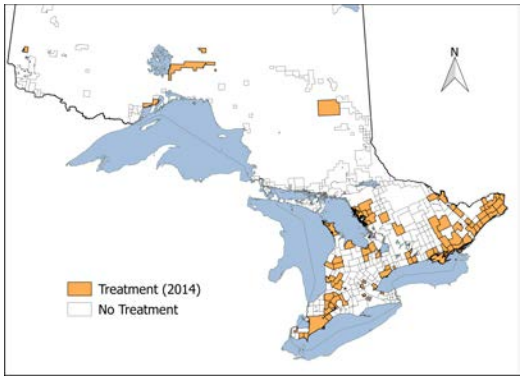
Municipalities in Alberta have been eager to pursue the use of Internet ballots in local elections. In 2012 the City of Edmonton, Alberta, conducted a mock online election (where voters cast a ballot for their favourite colour jellybean), and also conducted a public consultation through a public opinion survey and Citizens' Jury. These avenues of consultation indicated strong support for the use of Internet ballots in Edmonton's local elections, yet city council voted against the proposal. Seeing this, the provincial Ministry of Municipal Affairs declared a moratorium on Internet voting, thwarting the ability of communities still interested in its adoption, such as Grand Prairie, Wood Buffalo, and Strathcona County, from proceeding [8, 14]. In this case elected officials at both levels of government blocked the introduction of Internet voting.

In Ontario the province has put in place a legislative framework that supports the use of alternative voting methods and leaves the determination regarding types of ballots offered to the discretion of local government. A key example of cities adopting Internet voting has been the City of Markham, the first major Canadian municipality (over 100,000 electors) to use the technology. Officials in Markham supported Internet voting based on its perceived ability to enhance accessibility and convenience of the election process, improve voter turnout, focus on citizen-centered service, and to be recognized as a leader in e-government [19]. Another widely cited case involves the city of Peterborough, which has used Internet voting since 2006 [12]. Not all municipalities that consider the idea decide to implement it, however. Newmarket, Ontario is an example where the use of Internet voting was supported by city administration through research and planning and by the public through data collected from a household survey, but council voted not to allow its use in the 2014 elections. Part of this decision was due to concerns regarding security and privacy, but a lot of resistance developed from elected representatives who believed the option of Internet voting might encourage participation from electors who are not part of their voter base and typically abstain from elections (e.g. young people) [3].

In Ontario use of Internet voting in municipal elections has mushroomed. In 2003 twelve Ontario communities were the first to trial the technology. This number has increased with each round of elections growing to a potential of 98 communities out of 414 elections forthcoming in October 2014 representing about one fifth of the provincial electorate (see Fig. 1). In some cases, such as Markham, this has involved making online voting available in the advance voting period only, and included a two-step security procedure whereby electors were required to register to vote online to be able to access an Internet ballot [12]. In other situations, particularly elections in smaller municipalities (under 25,000 electors), Internet voting is offered during the entire election and does not require registration.[5] In these latter cases Internet voting is typically used in conjunction with telephone voting, making the entire election electronic. Larger municipalities (over 25,000 electors) have tended to stick with paper ballots and often only add Internet, excluding telephone. The result is a patchwork not only of adoption, but also Internet voting models.

In Nova Scotia, Internet voting use began in 2008 with four communities adopting the method, growing to fourteen in 2012. [6] Local officials have projected the number of communities offering online ballots will double in 2016, rising to 32 communities out of a potential 54 [24]. Much like Markham and other Ontario municipalities, motivations to introduce Internet voting have included becoming a leader in e-government, and improving access, convenience and electoral turnout [19]. In most Nova Scotia communities, with the exception of the provincial capital, Halifax, the Internet voting option has been kept open beyond the advance voting period to include election day. In a few cases, such as Digby Town, Truro, and Yarmouth, paper balloting on election day was done away with, and the entire election was carried out by Internet and telephone ballots

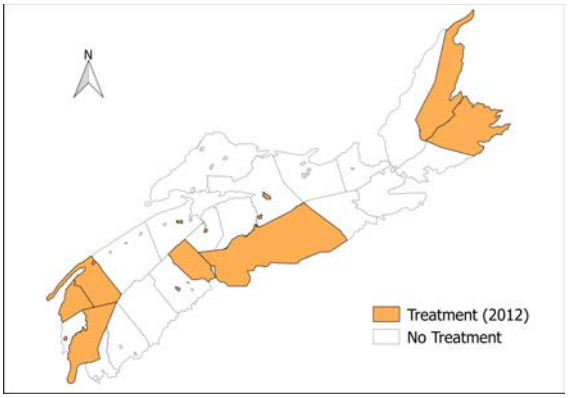
Though Internet voting has been adopted by some larger municipalities (Halifax, Markham) it is more likely to be used in smaller communities. It is especially favoured by communities that have large seasonal populations or have relied on voting by mail in the past. A majority of smaller communities use Internet voting for the full election, including election day. Fig. 1 and Fig. 2 depict Ontario and Nova Scotia municipalities that will have used Internet voting in binding local elections by October 2014, visually demonstrating the patchwork of adoption.



a. Sample Government of Ontario. Municipal Boundary - Lower and Single Tier. Ontario
b. Geospatial Data Exchange, Ministry of Natural Resources (OMNR), Peterborough, Ontario, Canada.

[5] It is important to note that 70 percent of Ontario municipalities have an electorate of 10,000 or less.

[6] Internet voting use was legally approved in sixteen Nova Scotia communities, however, only fourteen officially proceeded given that all seats in one area were acclaimed, and another determined they were unable to afford the cost at the last minute [11].



a. Sample of a Tab Government of Nova Scotia. Municipal Boundary File. GEONova, 2014.

D. First Nations

In the 617 First Nations communities in Canada, elections for Chief and band council can be governed in one of four ways (see Table 1). In 238 communities, the *Indian Act* (a federal piece of legislation) governs elections, with each participating First Nation community being responsible for carrying out their elections in accordance with the act. In April 2014, the *First Nations Elections Act* became law, providing another mechanism to govern elections in First Nations communities. This intent of this law was to create more modern electoral provisions than found in the *Indian Act:* some changes include longer terms in office, penalties for misconduct, and a common election day [13]. Communities can choose to opt-in to this legislation by passing a band council resolution, but it is presently unclear how many will do so.

A third approach to governing elections is the passage of Community or Custom Election Codes. These are election codes determined by the individual community with no interference from the federal government. Many of these codes are in fact derived from the *Indian Act*, but have been amended by communities [2]. An example of an amended provision includes the ability for off-reserve members to vote in band elections. The original wording of the *Indian Act* only allowed for First Nations members living on-reserve to cast a ballot and many communities wanted all members to be able to participate. This provision was challenged legally and the Supreme Court of Canada ruled that it violated the *Canadian Charter of Rights and Freedoms* and was unconstitutional [5]. As a consequence both on and off-reserve community members have been able to participate in Chief and council elections ever since. This change in the number, and nature of, eligible voters prompted the use of mail-in ballots in many communities. Internet voting is now appealing to many bands with large off-reserve populations that presently rely on vote by mail [2]. 2014 saw large increases in Canadian postal rates, and the beginning of a phase-out of home mail delivery, developments which will likely accelerate interest in Internet response alternatives.

Finally, 36 First Nations are considered self-governing. These communities develop their own laws to govern elections independent of any outside government and these codes are usually unique to each community based on their needs [13]. Typically, self-governing communities are distinguished by the fact that they have expanded law making authority [2].

The Indian Act and First Nations Elections Act are written to provide for paper ballots and vote by mail as methods. The ability to introduce online ballots would require a provision be added to these pieces of legislation. Communities with custom codes and those that are self-governing, however, may choose to introduce Internet voting by passing their own resolutions.

TABLE I. FRAMEWORKS FOR FIRST NATIONS ELECTIONS IN CANADA

Legislation	***# of Bands***
Indian Act and *Indian Band Election Regulations*	238
Custom and community election codes	343
Self-government agreements	36
First Nation Elections Act	*To be adopted, passed April 2014*

As the above table indicates, 379 bands could now use Internet voting methods. Overall tabulations of how many now do so, or are intending to do so, are not yet available. Some examples do exist, however. Several bands in the provinces of Ontario and British Columbia have used i-voting for various referendums and votes, although online ballots have yet to be used in a binding contest to elect band government. Nipissing First Nation, in Ontario, used Internet voting to complement paper and mail-in ballots to ratify their own constitution between November 2013 and January 2014 [7]. In British Columbia, a number of votes have taken place by Internet. Squamish First Nation used online ballots in March 2013 for a membership amendment referendum. One self-governing community in British Columbia, the Huu-ay-aht First Nation, has explicitly included a provision in their *Election Act* (Section 49(1)) to permit the use of electronic types of voting [17]. In September and April 2011 Talhtan First Nation used Internet ballots for votes regarding band member status and the introduction of power transmission lines. Talhtan will become the initial First Nation community in Canada to elect its band representatives by Internet in July 2014 [22].

Associations of First Nations are also beginning to make use of Internet ballots. The Union of Ontario Indians, an organization representing 39 First Nations communities, conducted a public consultation of all its members in early 2014 concerning a controversial piece of education legislation crafted by the federal government. Much like at the municipal level, the varied pieces of legislation governing elections provide the foundation for a relative patchwork of adoption. Providing communities have their own codes to govern elections, they are free to move forward with the implementation of digital technology with support from band council. Internet voting appeals to First Nations communities given the presence of sizable off-reserve populations (in many cases two thirds of band members live off-reserve). Even if Internet access and connectivity is an issue, online ballots may still be adopted to facilitate accessibility for those who live off the reserve lands [2].

III. INTERNET VOTING AND OTHER ACTORS

A. Political Parties & Unions

Federal and provincial political parties have been gravitating toward the method to facilitate their leadership votes. These organizations are free to use election methods as they see fit and have the power to introduce Internet voting providing it is permitted by their constitution. Internet voting is particularly attractive to parties to combine with, or replace,

TABLE II. POLITICAL PARTY LEADERSHIP VOTES USING I-VOTING

National (Canada)	Date	Overall Turnout	Methods	Use of Method
New Democratic Party	January 2003	54%	P, T, I	N/A
	March 2012	71%	P, I	
Liberal Party of Canada	April 2013	82.2%	I	82.2% I
Sub-national (province)				
Alberta Party	May 2011	58.7%	I, T	49.9% I 11.8% T
	September 2013	58.1%	I, T	50.7% I 7.4% T
Liberal Party of Alberta	September 2011	29.8%	I, T	21.2% I 8.6% T
Liberal Party of British Columbia	February 2011	62.4%	I, T	51.4% 11% T
British Columbia NDP	April 2011	71.3%	I, T	48% I 23.3% T
	September 2014	ACC	I, T	ACC
New Brunswick Liberal Party	October 2012	78.5%	I, T, M	38.8% I 15.1% T 24.5%M
Newfoundland & Labrador Liberal Party	November 2013	62.8%	I, T	30.5% I 32.3% T
Ontario NDP	March 2009	55%	I, T, M	25.4% I 4.6% T 25% M
Saskatchewan NDP	June 2009	72.4%	I, T, M	20.2% I 6.1% 46.1%M
	March 2013	77.9%	I, T, M	44.1% 7.6% T 48.3%M
TOTAL		**Avg**		**Avg i-vote**
12 parties, 8 provinces, 3 national votes	13 leadership votes	64%		41.8%

[a.] Please note "I" represents Internet voting, "T" represents telephone voting, "M" denotes vote by mail, "P" recognizes the use of paper ballots, "ACC" stands for acclaimed, and "N/A" not available.

voting by mail. To date a combination of vote by mail, Internet, and telephone ballots have been used to facilitate thirteen national and provincial leadership votes (see Table 2), with two additional e-vote elections expected in the coming months. Although first trialed in 2003, it has only been used regularly since 2009. Mostly center and left of center parties have been attracted to online voting, while comments from conservative organizations often focus on how the introduction of Internet voting may encourage participation from those who are not typically part of their membership base (e.g. young people). Two provincial conservative parties are considering Internet voting, however. The Progressive Conservatives in Prince Edward Island will likely use online ballots in their fall leadership election, and the Alberta Conservative Party is contemplating use for their upcoming leadership vote [1]. Overall, Internet voting appears to have helped improve turnout for these types of votes and seems to be the preferred method of participating for party members.

Unions representing blue and white collar workers have also embraced i-voting as a means of engaging members in elections and other votes. There are four levels of unions in Canada: international unions, national unions, regional unions, and local unions. I-voting is being explored by unions at all levels, but there is greatest interest at the local and regional levels. Online ballots have been used to date for union strike votes, ratification votes, collective bargaining, and union elections. In some cases local levels of unions are free to implement i-voting in elections, while in others they require approval from the national body [20].

B. Internet Voting Vendors

All the Canadian Internet elections held so far have been contracted to private companies, hired to carry out the electronic portion of the election. Six companies currently provide service in Canada: CanVote, Dominion Voting, Everyone Counts, Intelivote, Scytl, and Simply Voting. CanVote, Intelivote, and Simply Voting originated in Canada, while Dominion Voting and Everyone Counts are American, and Scytl is headquartered in Spain. In 2003 CanVote and an American company, Election Systems & Software, provided e-ballot service in Canada. Since then there has been an influx of companies providing a wide range of election services, including online poll training for workers, modules for candidates to track whether electors have voted (but not who they voted for) and target their get out the vote efforts. It is worrying to some that there are currently no minimum security standards in Canada for these elections, although some larger companies have been pushing for these regulations. In terms of Canadian market share Intelivote seems to lead the pack having hosted ten party leadership votes and securing 50 percent of municipal business for 2014. Scytl has carried out two leadership votes, Dominion Voting one, and each have about a quarter of the municipalities offering Internet voting subscribing to their services. The remaining companies hold less than five percent of municipal business.

IV. CONCLUSION

Canada's Internet voting deployment resembles a patchwork in a number of respects. First, most activity takes place at the local community level in two of the ten provinces, with a considerable amount in some other political organizations. The nature of divided jurisdiction and division of electoral powers has in some cases prevented the use of Internet voting, but in others the presence of supportive legislation and local autonomy has allowed its implementation. Second, the relative sovereignty of local councils to implement election changes, providing these adhere to the legislative framework written by the provinces, means that councils which have adopted Internet voting have taken a variety of approaches to implementation. This includes differences regarding the portion of the election in which i-voting is offered (e.g. advance poll or full election), and in the steps that

must be taken for an elector to cast an online ballot (e.g. whether online registration is required or not). In some cases paper ballots continue to be offered, while in others local elections have converted to being completely electronic. Limits in horizontal communication (within levels of government) and vertically (between them) has handicapped information sharing and hindered consistency in adoption and the type of model deployed.

In addition, there is a relative patchwork of technology employed given the different companies in the market and their e-voting solutions. While levels of government in other federal states considering or actively using Internet voting (such as the US and parts of Europe) have come together and implemented certification standards related to security, there is currently no such model in Canada. A lack of standards has caused concern regarding the level of security surrounding municipal elections, especially since governments with smaller budgets may be inclined to award contracts to vendors on the criterion of price. The result is a mixture of security standards regarding the Internet portion of the election.

In sum, there is a considerable amount of Internet voting in Canada. Various elements of the federal structure of authority and the decisions of local authorities have enabled Internet voting use to prosper in some areas, while in others development has been suspended. In one sense, a variety of 'policy laboratories' has allowed considerable innovation, but in another, the lack of consistency and standards provides cause for concern.

ACKNOWLEDGMENT

The authors thank SSHRC for financially supporting the research.

REFERENCES

[1] B. Anderson, Councillor, City of Edmonton. Personal interview, May 16, 2014.

[2] F. Bellefeuille, Legal Council, Union of Ontario Indians. Personal interview, May 9, 2014.

[3] A. Brouwer, Clerk, Town of Newmarket. Personal interview, February 3, 2014.

[4] *Canadian Elections Act* (Government of Canada), Act S.C. 2000, c. 9.

[5] Corbiere v. Canada (Minister of Indian Affairs), [1999] 2 S.R.C. 203.

[6] W. P. Cross and A. Blais, Politics at the Centre: The Selection and Removal of Party Leaders in the Anglo Parliamentary Democracies. Oxford University Press, 2012.

[7] S. Crutchlow, General Manager, Scytl Canada Inc. Personal communication, December 6, 2013.

[8] City of Edmonton, Report to Council – 2013 Municipal Election, 2013.

[9] Elections BC, Independent Panel on Internet Voting: Recommendations Report to the Legislative Assembly of British Columbia. British Columbia, February 2014.

[10] Elections Ontario. Alternative Voting Technologies Report: Chief Electoral Officer's Submission to the Legislative Assembly. Ontario, June 2013.

[11] N. Goodman, "Internet voting in a local election in Canada", in *Internet and Democracy in Global Perspective*, Studies in Public Choice 31, Eds. Bernard Grofman, Alex Trechsel, and Mark Franklin, Springer Verlag, 2014.

[12] N.J. Goodman, J. H. Pammett, and J. DeBardeleben, A comparative assessment of electronic voting, Elections Canada, 2010.

[13] Government of Canada, "Fact sheet – understanding First Nation elections" Department of Aboriginal Affairs and Northern Development, 2014: https://www.aadnc-aandc.gc.ca/eng/1323193986817/1323194199466 Last accessed: May 27, 2014.

[14] D. Griffiths, Minister of Municipal Affairs, Province of Alberta. Personal communication, March 6, 2013.

[15] P. Harpelle, Director of Communications & Community Outreach, Elections New Brunswick, May 9, 2014.

[16] T. Kydd, Senior Director, Outreach & Policy, Elections Saskatchewan. Personal interview, May 9, 2014.

[17] P. MacWilliam, *Online Voting in Local Government Elections*. University of Victoria, 2014.

[18] G. McLeod, Chief Electoral Officer, Elections Prince Edward Island. Personal interview, May 9, 2014.

[19] J.H. Pammett, and N. Goodman. Consultation and Evaluation Practices in the Implementation of Internet Voting in Canada and Europe. Ottawa: Elections Canada, 2013.

[20] M. Pivon, Sales Director, Western Region, Scytl Canada Inc. Personal interview, May 27, 2014.

[21] S. Pollock, Director, Technology Services, Elections Ontario. Personal interview, March 29, 2014.

[22] D. Smith, President, Intelivote Systems. Personal interview, May 13, 2014.

[23] D. Westwater, Director of Election Operations and Communications, Elections Alberta. Personal interview, May 9, 2014.

[24] B. White, Municipal Clerk and Returning Officer, Cape Breton Regional Municipality. Personal communication, December 17, 2012.

iVote.lt - a practical attempt to overcome online voting - related fears

Jonas Udris
Election Law Expert
Vilnius, Lithuania
jonas@sutartys.lt

Abstract - The paper presents the first practical attempt to introduce the advantages of online voting to the general public, offering a fully functional prototype that covers every major aspect of the online voting procedure. The authors believe that the success of this project will ease the fears and remove the doubts related to the introduction of online voting in binding elections.

Keywords—online voting, Lithuania, ivote.lt, simulator

I. THE SHORT OVERVIEW

iVote.lt is the first Lithuanian online voting simulator, which was aimed to promote and popularize online voting. The project took place prior to the official Parliamentary elections of 2012 and was hosted by www.delfi.lt, the largest Lithuanian online news portal. A total of 3566 people tested iVote.lt, which is three times as many needed for a sociological survey. More than 30 000 people at least tried the simulator; i.e., they have read the description, viewed the presentation, and downloaded the simulator software. This is more than number of voters required for one constituency. Ninety-eight percent of participants of the project voted "Yes" for introducing online voting in Lithuania.

II. INTRODUCTION

First attempts to introduce online voting in Lithuania took place in 2005, when the Concept (Draft Law) on Internet Voting was prepared by the Central Electoral Commission (CEC) and presented to Parliament [1]. Since then, multiple initiatives aimed to introduce online voting did not pass the submission stage in Parliament. Those initiatives were supported in many public, academic, and political discussions, but none led to any tangible results.

Despite the technological progress of Lithuania - where Internet speeds are among the fastest in the world, Wi-Fi hotspots grow like mushrooms in the forest after the rain, people no longer go the Tax Inspectorate in person, and banks close their offices due to the lack of visitors - online voting is still far beyond the horizon. Politicians and some part of the public believe in urban myths like "every computer system is hackable", and that online voting would lead straight to widespread electoral fraud.

To scatter these myths and increase public confidence in the idea of voting online, encourage politicians to overcome their fears, and introduce this modern way of voting, this fully-functional online voting simulator was created and introduced to the Lithuanian public in September 2012, four weeks before actual parliamentary elections. It was called the "iVote.lt project".

The goal of this paper is to present the iVote.lt project and explain how it helped increase public confidence in online voting.

III. THE IDEA

The idea was to put together the knowledge of CEC officials, the power of popular online media, and the capability of a team of programmers in order to present a working simulator that demonstrated and allowed people to try this new way of casting their vote. The simulation game invited people to try the online voting and help resolve all the myths and doubts that surrounded this way of casting a vote in real elections and referendums of the future.

The simulator had to demonstrate that online voting could be a secure and reliable voting method that fully complies with the democratic election principles set in the Constitution, the election laws, and international standards of free and democratic elections. Among those principles are the following: Free elections, Secret voting, Equal voting rights, Audibility, Reliability, Flexibility, Uniqueness, Integrity, and Convenience [2].

The project was started in January of 2012 by online voting enthusiast CEC member Jonas Udris and online media producer Justinas Vanagas. They defined the scope and aim of the project. A private IT company, UAB "EVP International", which specializes in creating online payment systems, was invited to join the project. The owner, Mr. Kostas Noreika, kindly agreed to help and appointed a team of programmers to code the software of the simulator.

The Central Electoral Commission, the Minister of Transport and Communications, and the Minister of Justice expressed their moral support for the project, and the State Enterprise Center of Registers kindly allowed the project to use their online identification system, www.ipasas.lt.

Technically, ivote.lt was based on early versions of the Estonian online voting model [3]. During the design phase many legal, information technology and election specialists contributed their knowledge and expertise to the project. The authors also tried to follow to the Recommendation Rec(2004)11 of the Committee of Ministers to member states

on legal, operational, and technical standards for e-voting [4].

The project followed exclusively informational and educational objectives. It was not part of any election campaign and did not mean to promote any political party or power. The people behind the project were not politically biased and did not belong to any political power. The project had no aim to influence election results in any way.

The simulator was not designed to imitate the real upcoming elections of 2012 or to predict their outcome. It was designed to motivate the society to show their interest in online voting as an alternative way of casting a vote.

The results of the game were completely anonymous; therefore, personal political preferences of the participants were not made public. Some statistical information was presented as additional information, such as the distribution of the voters by age, gender, and geography.

IV. The Design

The main idea behind the iVote.lt project was the "double envelope" voting principle, which is basically a digital version of traditional advanced voting by post. The voting process consisted of five major steps: 1) Generating a pair of keys; 2) Filling the ballot and encryption; 3) Casting the ballot; 4) Anonymisation; 5) Decryption and tabulation of the results.

The simulation game was designed following the principles of transparency and auditability. Therefore, only well-known and open-source libraries were used:

- The www.ivote.lt website was created using open source Symfony2 carcasus; HTTPS protocol was used.
- www.ipasas.lt of State Enterprise Center of Registers was used for user authentication.
- Java Web Start application (JRE 1.5 version and up). The source code signed by Code Signing certificate.
- Bouncy Castle Crypto (http://www.bouncycastle.org/java.html) API was used to encrypt the ballot. Data was then put to a CMS Enveloped Data package and encrypted with a 128 bit key.

The source code of the project was open for public download.

A. Generating the pair of keys

First, the pair of digital keys was generated. The Public Key was uploaded into the system and the Private Key was deconstructed and put away for safekeeping until the end of the voting. Parts of the Private Key were burned onto blank CD's and distributed among organizers of the simulator.

B. Filling in the ballot

The voting simulator was accessible either directly at www.ivote.lt or via the news portal www.delfi.lt, where it was widely advertised. The user was offered the download of a small JAVA applet, which contained an electronic "ballot" and a questionnaire, together with an encrypting algorithm and a Public Key. There was no need for any specific IT knowledge or software installation to use the simulator. The simulator worked on all JAVA-supporting operating systems, including Windows XP and higher and Mac OS X version 10.6 and higher.

Once the user finished "filling in the ballot" and the questionnaire, he or she was then asked to click a button that read "Encrypt the ballot". After the encryption was complete, the binary file containing encrypted information was generated and saved onto the user's desktop. This binary file did not contain any personal data or any other data that, when decrypted, could link the "ballot" to the voter's identity. The file name contained only the date and time of the file. The "ballot" could be opened in any text editor, but it looked like lines of random characters.

Thus, the filled out ballot and data encryption were completely anonymous; no personal or other identifying information was stored in the encrypted file. If one wanted to be sure of anonymity, he or she could transfer the encrypted file to another computer and submit it from there.

C. Casting the ballot

Once the encrypted file was generated, the user was asked to choose the "Cast the ballot" function and then they were forwarded to the www.ipasas.lt website for authentication. Here his or her identity was determined using an online banking system or a digital signature. After the authentication was complete, the user was asked to upload his or her encrypted vote. As the "ballot" file was encrypted and the private key was not accessible, no one, even the administrators, were able to disclose the persons' "vote". The user could upload as many ballots as he or she wanted, but only the last vote counted. The previous votes were destroyed (overwritten).

Some of the data, such as the voter's age, gender, and IP-based location, was collected separately for statistic purposes.

The "last vote counts" principle was achieved in a very simple way using some basic principles of computer operating systems: two files with the same name cannot exist in the same folder. When the person identified himself or herself to the system, a unique number (a long integer) was generated based on the voter's personal code using a Hash function; thus, a unique number was created for each voter but the voter could not be identified backwards. This unique number was used as a file name to the encrypted ballot. So, after the voter authenticated himself or herself and uploaded the encrypted ballot file, the ballot file got a unique name generated by "hashing" the voter's personal code. Every other vote cast by the same voter got the same file name;

thus, it automatically overwrote the previous vote. This means that only the last vote is stored in the database, with no history (unless the database is somehow duplicated or backed up before the vote update). This allowed the existence of the "cancellation vote", a special instruction that could be sent to the server to delete the vote that was previously cast.

This explanation of the "last vote counts" principle was the easiest way to convince people that the ballots were actually not linked to the voter's identity, and there really was no way to disclose the secrecy of the vote in this phase.

A Youtube video [5] was made to demonstrate how the simulator worked.

V. The process

The simulation voting was launched on the 18th of September, 2012 at 12:00 after an announcement on www.delfi.lt, the largest Lithuanian news portal. An immediate reaction followed the launch. The promotional article was read more than 40 000 times, and readers left more than 1000 comments in just the first few hours.

More than 600 people tried the simulator on the first day.

The voting lasted for 17 days – until the 5th of October, 2012. A total of 3788 electronic "ballots" were uploaded (including "re-votes"). More than 30 000 users downloaded the voting application but never uploaded the ballot.

One hundred and two participants "re-voted" at least once. A total of 3566 valid ballots were counted.

One hundred and fifty-eight users downloaded the source code.

Every voter was offered a Certificate of Participation. (This was a generated PDF file with the user's name and surname, saying that he or she had participated in the first educational online voting simulation game.) The mayor of Vilnius and several ministers and members of Parliament were among those who proudly published their certificates on their Facebook timelines.

VI. Anonymisation, decryption, and tabulation of the results

After the "voting" period was over, the collection of votes was stopped and the anonymisation process started. The server with all of the "votes" was disconnected from the Internet first.

The process worked by simply randomizing the filenames of the ballot files. As we did not store a history of the votes, we had only the last "valid" votes; thus, randomization of the filenames was sufficient to ensure voter anonymity and that only one vote per voter was counted.

The Private Key was put back together and the decryption algorithm was then launched. The votes were decrypted and the results were then tabulated. The Private Key was then destroyed so any previously made (or backed-up) copies of the votes could not be decrypted.

VII. The results overview

As this simulation was widely supported by liberal-wing politicians and youth organizations, liberal (28,86%) and conservative (26,00%) parties "won the online elections". Of course, this did not correspond to the results of the actual elections of the Parliament that took place the week after the simulator ended.

Voter distribution was as follows:

- 1130 females (30 percent) and 2638 males (70 percent),
- 679 voters ages 18-24,
- 1603 voters ages 25-34,
- 861 voters ages 35-44,
- 408 voters ages 45-54,
- and 215 voters ages 55 and above.

Although the simulator covered most aspects of online voting protocol, some important aspects were missing and should be resolved before introduction in binding elections.

Firstly, anyone with a Lithuanian electronic ID or means of internet banking authentication could participate in the ivote.lt project, regardless of their citizenship or age. Only the ones included in the electronic voters' list could vote in real online voting.

Secondly, the ballots of the iVote.lt were all the same, and the person that downloaded this was completely unknown to the system. In real voting the voter would first identify himself or herself electronically, so the ballot issuing server could determine if he or she were eligible to vote and voting constituency, and then give him or her the respective ballot.

Thirdly, it was possible to authenticate to iVote.lt not only by digital signature, but also by means of internet banking. In real online voting internet banking is not a valid method of authentication. The voter would sign in using a digital signature or other means of electronic ID, depending on the legal framework.

Fourthly, ivote.lt did not offer an option for the voter to check if his or her vote was counted, which is becoming a standard in actual working online voting systems.

All other technological and organizational methods, including "The last vote counts", "Vote cancellation", and user interface meets the requirements for online voting systems, so it is only a matter of time and political will when this voting method will be implemented in our country.

VIII. Publicity and media coverage

As noted before, the ivote.lt was not only a piece of software, but also a publicity project. More than 20 popular articles were published on the major Lithuanian news portal delfi.lt, where different people (politicians, bankers, artists, scientists, and others) expressed their support for the

introduction of online voting. There were also articles on cyber-security, digital signatures, and digital identity.

Three big rounds of discussions were held in the headquarters of the Central Electoral Commission. All three events were webcasted live on the Internet and video reviews were made after. The first round gathered representatives of the media, business, and politics. The second round brought together all the leaders of the main political parties, and the third round included IT experts, journalists, and representatives of the expatriates. These discussions revealed the growing demand of society to introduce online voting, especially among expatriates and young, active people living in Lithuania. The IT experts agreed that the current IT infrastructure is sufficient to ensure the required level of security, but some politicians still expressed a high level of mistrust and kept declaring that "our society is not ready yet".

IX. Conclusions

The project was created to promote the idea of online voting and to explain to the general public how online voting might work. The users were able to test the possibilities and advantages of online voting by themselves.

The following conclusions were made:

1. More than 3500 people participated. That was twice as many as the authors initially expected.
2. The main objective of the project was achieved completely; i.e., a fully operational online voting module was presented to the public. It scoped every aspect of online voting procedure – starting with user authentication and vote encryption, and ending with depersonalization and tabulation of the results.
3. The project proved that anonymity of the vote can be guaranteed during all stages of online voting. This was clearly explained to the public.
4. Despite the fact that results of ivote.lt do not correspond with the actual results of the Parliamentary elections of 2012, wide distribution of votes among parties show that online voting is supported by citizens of various political views.
5. The geographical distribution of ivote.lt participants showed there is a possible increase in turnout of voters living abroad.
6. The gender and age statistics showed that online voting is supported by various ages among both genders.
7. The project drew a lot of attention from various fields of society and government; politicians, businessmen, journalists, and other public figures joined the online voting–related discussions.
8. Despite a number of attempts, we do not have any information that the system was ever hacked or influenced from the outside in any way.

X. Further Steps

The online voting simulator drew enough public attention to the idea of online voting. Despite obvious Estonian success, the introduction of online voting in Norway, and online voting for expatriates in France, there is still a lot of resistance and doubt among politicians regarding the introduction of online voting in Lithuania.

However, there have been small steps made in the right direction. For the first time ever, during the presidential elections of 2014 the candidates were able to gather signatures of their supporters online. The winner - current President Dalia Grybauskaitė - collected the required minimum of 20 000 signatures just online. A total of more than 60 000 signatures were collected online. This shows growing public confidence in e-democracy.

The amendment to the Law on Municipal Governance was submitted to the Parliament, which will allow anonymous public surveys (i.e., local referendums) by means of electronic communication. This will allow the creation of a fully-functional online pilot system that technically will meet all the requirements for national elections, and could be tested and evaluated without putting national-level elections at risk.

In the spring of 2014 the Minister of Justice, together with the Minister of Transport and Communications, announced that online voting will be introduced in Lithuania some time soon.

References

[1] First Lithuanian concept for internet voting. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=287235&p_query=&p_tr2=

[2] Electronic Voting: Algorithmic and Implementation Issues, Robert Kofler, Robert Krimmer, Alexander Prosser, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

[3] http://neu.e-voting.cc/wp-content/uploads/Proceedings%202006/1.1.madise_martens_e-voting_in_estonia.pdf

[4] Recommendation Rec(2004)11, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004, was prepared by the Multidisciplinary Ad hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE).

[5] A link to a Youtube video, explaining how the simulator worked: https://www.youtube.com/watch?v=8akH1g0Iug4

[6] http://www.coe.int/t/dgap/democracy/Source/EVoting/EVotingReview06/JONAS%20UDRIS-Strasbourg2006.ppt

Verifiable Internet Voting in Estonia

Sven Heiberg*† and Jan Willemson*‡
*Cybernetica, Ülikooli 2, Tartu, Estonia
†Smartmatic-Cybernetica Centre of Excellence for Internet Voting, Ülikooli 2, Tartu, Estonia
‡Software Technology and Applications Competence Centre, Ülikooli 2, Tartu, Estonia
Email: {sven,janwil}@cyber.ee

***Abstract*—This paper introduces an extension to the Estonian Internet voting scheme allowing the voters to check the cast-as-intended and recorded-as-cast properties of their vote by using a mobile device. The scheme was used during the 2013 Estonian local municipal elections and the 2014 European Parliament elections. 3.43% and 4.04% of all Internet votes were verified, respectively. We will present the details of the protocol, discuss the security thereof and the results of implementation.**

Keywords*—*Verifiable electronic voting

I. Introduction

The first legally binding elections allowing votes to be cast over the Internet took place in 2000 at the University of Osnabrück, Germany [1], and in Arizona, USA [2]. Just five years later, Internet voting was used in the Estonian countrywide local municipal elections [20]. Since then, legally binding Internet voting has been applied by various other countries and organizations, e.g. the Austrian Federation of Students [18], Switzerland [4], Netherlands [15], Norway [27], etc.

Several of the abovementioned implementations have encountered some security issues. For example, as a response to Arizona pilot, it was recommended to delay Internet voting until suitable criteria for security are put in place [24]. The Austrian Student Federation election of 2009 was subject to a DDoS attack [10]. Both the 2011 and 2013 attempts to introduce e-voting in Norway suffered from software and physical implementation errors [27], [8]. The 2011 Estonian elections were subject to several attacks including a proof-of-concept vote manipulation malware and politically motivated attempts to revoke the results of the whole electronic vote [13].

Electronic voting can be considered inherently more dangerous compared to conventional paper-based voting, as the lack of physical evidence creates the need to trust the electronic voting device. A buggy or malicious voting device could tamper with the electronic ballot without anybody being able to detect the manipulation. If the voting device and the digital ballot box communicate over the Internet, they are exposed to geographically unbound, highly scalable attacks from the network. A security analysis for an Internet voting system provided by SERVE (Secure Electronic Registration and Voting Experiment) suggested that Internet voting should not be attempted, unless some unforeseen security breakthrough appears [16].

Verifiable voting protocols attempt to improve the situation by providing participants with the ability to check whether certain properties hold on, e.g. the electronic tally. If the protocol gives voters the means to check the properties of their individual ballots, we can refer to an *individually verifiable* voting protocol. For example, it might be possible for the voter to check whether the electronic ballot cast over the Internet was correctly accepted by the digital ballot box. There are several protocols that provide some kind of verifiability to Internet voting [26], [5], [17], [11].

In this paper, we present an individually verifiable protocol that was used in the 2013 Estonian local municipal elections and the 2014 European Parliament elections. The paper is organized as follows. Section II describes the basic Estonian Internet voting scheme and explains the need for verifiability, and Section III defines the exact objective for the verifiability extension proposed in Section IV. Section V discusses the provided security guarantees together with the residual risk vectors, and Section VI gives practical implementation results. Finally, Section VII draws some conclusions and sets out the direction of future work.

II. Estonian Internet voting in 2005–2014

The Estonian Internet voting scheme was developed in the early 2000s and is described in detail in [13]. It has been used at seven elections during 2005–2014 and the basic protocol has remained essentially unchanged.

On the conceptual level, the scheme is very simple and mimics double envelope postal voting. The central voting system generates an RSA key pair and publishes the public part s_{pub}. The voter v authenticates herself for the voting server using her ID card or mobile ID (standard identification mechanisms widely used in Estonia), and receives the candidate list. She then makes her choice c_v (which is just a candidate number in case of Estonian elections) and encrypts it with the server's public key. For encryption, RSA-OAEP is used and a random seed r is generated for the cryptosystem. Hence the anonymous ballot ("inner envelope") is computed as $b_{anon} = Enc_{s_{pub}}(c_v, r)$. The effect of the "outer envelope" is achieved by signing the ballot using the voter's ID card, and the resulting complete ballot $b = Sig_v(b_{anon})$ is sent to the voting server (see also Figure 1).

The scheme uses re-voting as an anti-coercion measure. The voter can cast a vote over Internet several times, but only the last vote will be included in the tally. This way, if a voter feels coerced, she can re-vote later. The voter can also vote on paper to cancel her electronic vote. It is assumed that uncertainty in

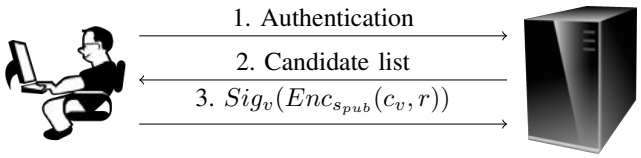


Fig. 1. The basic Estonian Internet voting protocol

the outcome of the coercion attempt makes such attempts an inefficient attack vector.

Electronic ballots are kept in the signed and encrypted form until the voting period is over. The signatures are then dropped and anonymous ballots are tallied; for that, they are decrypted with the server's private key stored in a hardware security module.

While it is rather straightforward, the system has several weaknesses, some of which were exploited during the 2011 parliamentary elections. The most severe and widely published attack was proposed by a student who made use of the fact that in its original form, the voting system gave no reliable feedback concerning whether or how the vote was actually received by the server. The student developed several versions of malware capable of blocking or even changing the vote. Due to the simple nature of the basic protocol, such manipulations would remain unnoticed by the voter [13].

After the 2011 elections, these issues were addressed in the OSCE/ODIHR report [22]. Among other suggestions, the report states:

> *The OSCE/ODIHR recommends that the NEC forms an inclusive working group to consider the use of a verifiable Internet voting scheme or an equally reliable mechanism for the voter to check whether or not his/her vote was changed by malicious software.*

The current paper can be seen as a direct consequence of this suggestion, presenting a scheme that allows the users to verify the correctness of their votes. The scheme was implemented and used as a pilot during the 2013 Estonian local municipal elections and the 2014 European Parliament elections.

However, adding vote verifiability to the system may have unexpected side effects which can violate other requirements of the election. For example, the Council of Europe has published its recommendations on legal, operational and technical standards for e-voting [3]. Recommendation number 51 reads:

> *A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.*

It can be argued that any sufficiently strong form of vote verification may be used as a proof of the content, and hence facilitate vote selling or coercion, for example [7]. In the current paper we assume the hypothesis that the truth lies somewhere in between and try to propose one possible trade-off between verifiability and coercion-resistance. See Sections V-B and V-C for a more detailed discussion.

III. Types of verifiability

There is no generally accepted definition of the verifiability of electronic voting. Various authors define it differently depending on the needs and capabilities of the community setting up the elections. We refer to [19] for a good overview and comparison of the proposed approaches. In this paper, we will rely on the definition given by Popoveniuc *et al.* [23]. They define end-to-end verifiability through the performance requirements set for the voting system. An end-to-end verifiable voting system will provide the following properties:

1) The voter is able to check that her ballot represents a vote for the candidate to whom she intended to give the vote.
2) Anyone is able to check that valid ballots do not contain over-votes or negative votes.
3) The voter can check that her ballot is recorded as she cast it.
4) Anyone is able to check that all the recorded ballots have been tallied correctly.
5) Anyone is able to check that the voters and the general public have the same view of the election records.
6) Anyone can check that any cast ballot has a corresponding voter who can perform check No. 3.

Popoveniuc *et al.* also analyze several proposed systems and conclude that some of them are fully end-to-end verifiable (e.g. Prêt à voter [25] or Scratch & vote [6]). Some other systems (e.g. Scantegrity II [9] or Helios [5]) need one of the requirements to be slightly relaxed.

We will not be requiring end-to-end verifiability in the full sense of Popoveniuc *et al.* for the Estonian voting system. We will only require the individually verifiable properties 1 (cast-as-intended) and 3 (recorded-as-cast) from the list above. There are several reasons for that. First, the 2011 parliamentary elections showed client-side weaknesses both in the preparation and transport of ballots. Cast-as-intended and recorded-as-cast properties address these weaknesses. This is similar to conventional paper-based elections that have these properties under certain assumptions, namely that:

1) The voter is capable of representing her choice correctly;
2) The ballot paper and the ballot marker pen are not tampered with and perform their function correctly;
3) The voter personally takes the ballot from the polling booth to the ballot box.

From this point on, the voter has to rely on the election officials and observers to follow the procedures correctly and to notify the public of any possible violations. The Estonian National Electoral Committee (NEC) felt that although the observability of the electronic tally can be considered in the future, the effort needed to implement end-to-end verifiability is currently not justified.

Second, achieving some additional properties would have meant implementing a completely new system with a completely new user experience compared to what the electorate is used to, and this was considered unrealistic. As we will see later in the paper, cast-as-intended and recorded-as-cast properties are achievable incrementally with respect to the current system.

IV. Verifiable Internet voting for Estonian elections

In Estonia, Internet voting makes heavy use of an existing ID card infrastructure which essentially provides one secure pre-channel between the state and the citizen in the form of certified public-private key pairs.

Since verification is something that can only happen *after* a vote is cast, we also need a post-channel that would work well together with the chosen pre-channel. During the analysis phase, a postal+SMS solution was briefly considered. It was concluded that this channel was rather expensive and still error-prone as shown by the Norwegian experience [27]. Hence another alternative was needed.

Since the basic Estonian Internet voting protocol supports vote auditing by releasing the random seed used for encryption, we decided to implement this form of verification. Of course, such a verification cannot be performed by a human alone and a computing device is required. Since verification using the same device (PC) would not address the problem of potential device corruption, we decided to introduce verification on a different platform. As of the time of the development period (2012), the prime candidates for this platform were mobile devices (smartphones, tablet computers, etc.). They provide both sufficient processing power for cryptographic operations and independent communication channels.

Verification itself requires relatively small overhead compared to the existing Estonian Internet voting system, and the entire protocol on a high level is as follows (see also Figure 2).

1) The voter authenticates herself for the server.
2) She receives a list of candidates L.
3) The voter makes her choice $c_v \in L$ and prepares the vote $b_{anon} = Enc_{s_{pub}}(c_v, r)$, encrypted with the server's public key, using randomness r. The voter sends her signed vote $b = Sig_v(b_{anon})$ to the server.
4) The server returns a unique randomly generated vote reference vr to the voter. This reference will later be used to download the correct vote to the mobile device.
5) The voter transfers r and vr from the PC to the mobile device.
6) The mobile device contacts the server over server-side authenticated HTTPS and sends vr.
7) The voter's mobile device downloads the vote b_{anon} corresponding to vr from the server together with the list of all candidates available L.
8) The mobile device computes $Enc_{s_{pub}}(c, r)$ for all $c \in L$. If for some c' the equality $Enc_{s_{pub}}(c', r) = b_{anon}$ holds, this c' is displayed to the user. If $c_v = c'$, the voter accepts the vote to have been cast as intended.

Steps 1–3 have been used since 2005 and are familiar to the general electorate. Hence, only steps 4–8 are new to voters. From the user interface point of view they can be performed rather smoothly.

The time allowed to complete steps 4–7 has been limited (30 minutes in 2013 and 60 minutes in the 2014 elections). Also, the number of times the server is ready to let the user download b_{anon} is limited (currently 3). The verifiability extension only allows for the verification of the last vote cast by the voter. Re-

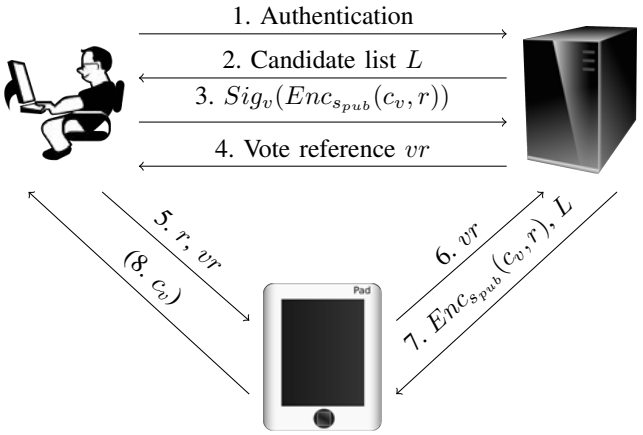


Fig. 2. The Estonian Internet voting protocol with vote verification

voting revokes both the previous ballot and the vote reference. These are largely anti-coercion measures; see Section V-B for further discussion.

The most complicated one is step 5, where the random seed r and vote reference vr need to be transferred from a PC to a mobile device. Several channels can be used for that; we chose to use QR codes, since other alternatives (like a memory card, a wired connection or Bluetooth) require extra setup. When the vote is sent to the server, a QR code containing r and vr is displayed on the PC screen. The user runs a verification application on the mobile device. The application first expects to scan the QR code, which can be done by pointing the device to the PC screen. The voter does not even need to press any buttons, as the scan is completed automatically. And assuming the network connection is open, steps 6 and 7 are also automatic. Once the vote is received from the server, the mobile device follows through with step 8.

Note that the mobile device never learns the voter's identity, it just sees random values. It finds the value c' for an anonymized encrypted vote. This prevents a malicious mobile device from breaking vote privacy. Of course, it can still lie about the value of c' found, but assuming that the PC and the mobile device are not corrupt in a coordinated manner, this lie would be detected and reported by the user with high probability. The latter assumption may or may not fully hold; see Sections V and VI for more discussion and analysis in case this assumption is relaxed.

Since step 8 assumes going through the list L, it will take some time. In practice, the candidate lists in Estonia contain up to several hundred elements in extreme cases (with the values $10 \ldots 50$ being the most common). We implemented a test application computing 400 RSA2048 encryptions with the exponent 65537. On a Samsung Galaxy Ace smartphone with an 800 MHz processor this computation took roughly 1.5 seconds. Together with the time needed to communicate with the server we estimate the total running time of the verification to be up to 5 seconds which we consider a reasonable result.

It would also be possible to implement step 8 by first asking the voter to input her choice and make the comparison with one encryption, displaying a simple yes/no answer. This

seemingly more elegant solution introduces a new potential threat vector. Namely, it would be possible for a corrupt verification application not to verify anything and just say yes. In the protocol proposed above, however, in order to manipulate the vote successfully without the voter noticing, the voting and verification applications must be corrupt in a coordinated manner. We consider the complexity of such an attack prohibitively high.

In principle, it is also possible to develop vote verification software for PC platforms and carry out a public education campaign convincing voters to verify their votes on a computer different from the one that they used to cast the vote. However, we suspect that the vast majority of voters would just run the two pieces of software on the same computer, and hence the security goals set for verification would not be achieved. At the time of writing this paper, major PC and mobile platforms are running different operating systems. Thus, the voters are forced to use separate devices for voting and verification which was one of our security goals. We acknowledge that this situation may change in the future, but at least for the elections taking place in 2013–2015 this approach should be viable.

Analyzing the voting protocol, we see that the verification device does not need and should not store anything. This means that these devices can be shared among voters, making them even more accessible.

V. Discussion

In this section we will address some specific issues about the scheme and its application.

A. Failed verifications

Individual verifiability provides NEC with an additional tool to detect possible attempts to manipulate the voting result on a large scale. Verification attempts may fail due to simple user errors or hardware/software incompatibility, but failed verifications may also indicate a manipulation attack.

Most important failures in verification can manifest themselves through the following symptoms:

- Inability to download the encrypted vote from the server,
- Failure to find the corresponding candidate from the list L,
- The candidate found does not match the voter's intention.

In case of such failures, NEC suggests that voters follow a predefined set of actions:

1) Re-vote and verify using (preferably) a different PC and mobile device.
2) In case the error persists, re-cast the vote in a polling station on paper. Notify NEC of the event.

If certain errors start repeating, this information may be used by NEC to initiate research activities and take different decisions. Failures in verification do not necessarily mean that an attack is going on. E.g. a voter who would attempt to verify her vote after the vote reference vr has expired, would get a verification failure. Similarly, a voter using the wrong QR-code would get a verification failure and possibly turn to NEC for assistance.

B. Coercion-resistance

Ben Adida, author of the verifiable Internet voting system Helios, states that his system is only suitable in low-coercion settings like student governments, local clubs, online groups such as open-source software communities, and other similar situations. The protocol is not applicable for parliamentary elections. for instance [5]. The original Helios interface actually provided a "Coerce Me!" button to remind the users about the inherent threat. A similar button could be built into the Estonian voting or verification application – anyone who gets hold of the vote $b_{anon} = Enc_{s_{pub}}(c_v, r)$ and randomness r is capable of finding out the voter's actual preference.

Coercion is more likely to occur in a remote setting. Voting in polling stations takes place in the privacy of the polling booth, and the coercer has to invent ways to maintain control over the actions of the coercee. In remote environments, the coercer can observe the voter voting for a specific candidate. Estonian Internet voting uses re-voting as an anti-coercion measure.

Verifiability seems to facilitate coercion. In the Norwegian system, the coercer may ask the voter to provide the card with the verification codes and the SMS with the code actually returned. This way the coercer can be sure that the vote for the required candidate is in the digital ballot box. In the Estonian protocol, it is enough for the coercer to control the verification application.

We argue that due to the option of re-voting, coercion is not made any easier by introducing verifiability. By observing either voting or verification, the coercer cannot be sure that the vote will actually be taken into account. We also note that a coercion attack as a manipulation attack is rather inefficient. In order to achieve an additional seat in the Parliament, a great number of people have to be coerced, and thus the probability of getting caught increases. It is also time-consuming to monitor all the coercees and their actions. (Recall that both the time the server is willing to provide a particular encrypted vote for verification, and the number of times it is ready to do so, are limited.) Nevertheless, if a society sees large-scale coercion as an existing problem, any kind of remote voting – electronic or non-electronic – should be avoided at elections.

C. The threat of false verification failure claims

Of course, introducing a new component into the system also brings along new attack vectors. Merely the possibility to claim that the verification failed can be misused by malicious voters interested in, say, a reputation attack [14]. When the proposed method of vote verification was presented to Estonian politicians, this was one of the concerns they expressed. The problem is that it is very difficult to either prove or disprove such claims without violating vote secrecy. The Norwegian experience, however, showed that a widespread reputation attack based on bogus claims did not happen [27]. On the contrary, the Norwegian electorate perceived failed verifications as a positive feature – it gave feedback that had been impossible to obtain before. After having applied the verification solution in the 2013 and 2014 Estonian elections we can say that the threat of false claims did not materialize. Considering that the

verifications made during the 2013 and 2014 elections were just pilots, the incentive of potential attackers may have been lower than for legally binding runs, and thus we still need to be ready for such an attack in the future.

D. Random factor exposure

The verification scheme leaks the randomness r used in the encryption to the mobile device. Anybody in possession of r, b_{anon} and the list of candidates L can brute-force the encrypted ballot to get the candidate number. We do not see a new threat here as anybody having access to r in the voting application also could have observed the original choice encrypted together with the randomness.

E. Diverting the verification

To provide its security properties, the verification protocol relies on some assumptions. The most important assumption made is the independence of the PC and the mobile device. If an attacker was able to install malware working on both of the devices in a coordinated manner, a potential vote manipulation could go unnoticed. The report [12] claims to have developed proof-of-concept pieces of malware for both the PC and the mobile device, using the QR code channel to make hints to the verification application about the voter's choice, whereas a compromised voting client would manipulate the vote silently.

However, the report fails to describe how to achieve a coordinated installation of the developed malware on these devices. The authors of the report also admit that if this attack were to be used on a large scale, it would carry an elevated possibility of detection, since some users may attempt verification with devices owned by others. This in turn means that the goal of introducing verification has been achieved and it is still possible to have confidence in the absence of a large-scale vote manipulation attack. See Section VI for more discussions on quantified estimates on the security guarantees obtained on the example of the 2013 Estonian elections.

Another approach to attack the scheme is based on the fact that the voter is not capable of verifying if the QR presented by the voting application contains the randomness and vote reference vr corresponding to her ballot. If the malicious voting application knows the vote reference vr_1 of an already stored ballot, which encrypted the candidate number desired by the voter, then the application could encrypt any other candidate number for vr, but show the QR code with vr_1 and r_1. This way a manipulated ballot would be stored, but the verification application would show the result expected by the voter.

The limits on the number and time of verifications and the way that the re-voting is handled make this attack difficult to execute in practice. It is not possible to acquire a set of QR codes and reuse them for a longer period of time. A more robust approach would be based on the fact that most votes are never verified and it is possible to build a QR-sharing bot-net of malicious voting applications. This would make the setup of a manipulation attack more complex, and the event of using the same QR code too many times would trigger a server-side alarm.

Vote verification is not a universal measure against all possible attacks. As discussed above, re-voting is used in Estonia as an anti-coercion measure. However, this possibility can also be abused by malware installed on the voter's PC. During the original voting session, the malware may save the PIN codes of an ID card (assuming an ID card reader without a PIN pad is used, which is mostly the case). If the ID card is inserted again later (maybe for a completely different application), the malware may also use it to submit a new vote. As there is no active feedback channel currently in use in the Estonian Internet voting protocol, most voters would never know about this occurrence even if they verified their original vote. The most efficient measure against such an attack would be to implement an active feedback channel. This is one of the possible future improvements considered for the Estonian Internet voting protocol. However, since this attack is independent of verification, further discussion remains outside the scope of the current paper.

VI. Implementation results

The described verifiable Internet voting system was first implemented for the 2013 Estonian local municipal elections. For the first pilot[1], only Android OS 2.2 and higher were supported as the mobile application platform. During the elections, 136,853 electronic votes were given (including re-votes) and 133,662 counted (which comprised 21.2% of all the votes cast). Verification was utilized on 4,696 occasions (and altogether 3.43% of all the e-votes given were verified).

For the second pilot run during the 2014 European Parliament elections, support for iOS and Windows Phone was added as well. During the elections, 105,170 electronic votes were given (including re-votes) and 103,105 votes were counted (which comprised 31.3% of all the votes cast). Verification was utilized on 4,250 occasions (and altogether 4.04% of all the e-votes given were verified).

There were no failed verifications reported in 2013. This allows us to estimate the probability that a large-scale vote manipulation went undetected. Assuming that the attacker was able to manipulate k random votes, but not tamper with the verification devices and voting devices in a coordinated manner, the probability that at least one of the manipulated votes was detected is

$$1 - \left(1 - \frac{4696}{136853}\right)^k .$$

(This corresponds well to the reasoning by Neff [21].)

In order to obtain a more realistic estimate on this probability, we have to take into account possible coordinated malware (see Section V). For illustrative purposes in this paper we assume that only half of the verifications were performed on truly independent devices. The probability that at least one of

[1]According to the current Estonian legislation, verification will have legal consequences in 2015 (and the date can be moved further if necessary). The verifications during the first two elections of 2013 and 2014 were planned as pilots to try out the new technology.

the manipulated votes was detected changes to

$$1 - \left(1 - \frac{2348}{136853}\right)^k .$$

See Figure 3 which depicts both of the graphs. We can see that even if half of the devices were compromised, the manipulation of 200 or more votes would still be detected with more than a 95% probability.

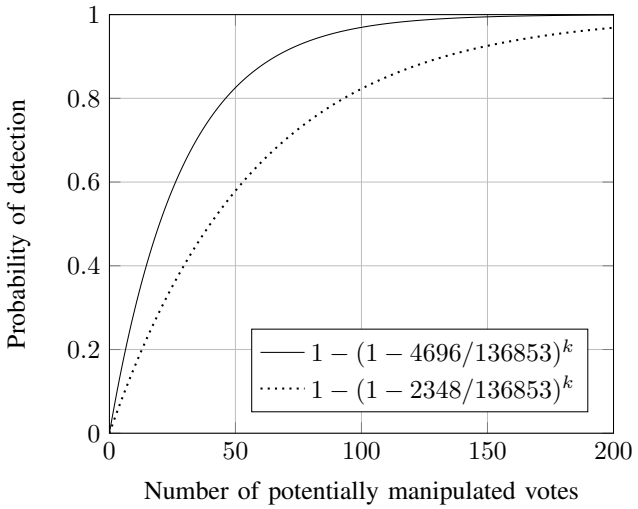


Fig. 3. Probability of large scale vote manipulation detection

The pilot in 2014 was more controversial – during the election, two software bugs were discovered in the iOS verification application. On a few occasions, the iOS application reported that it was not capable of finding the candidate number corresponding to the encrypted ballot. It appeared that binary data extracted from the QR code was interpreted as a string by the application, leading to bad encryptions under certain circumstances. The bug was fixed during the elections, the patch was successfully submitted to the iOS app store and pushed to the voters.

The second bug manifested itself when a buggy iOS verification application was accidentally used with a QR code coming from an external source (e.g. newspaper ad, online media, etc.). For the voter it looked as if her vote was not available on the server, even though it was stored correctly. This resulted in four calls to the helpdesk. The voters were instructed to cast a new vote and verify it again. No more errors were reported after this.

Hence no real vote manipulations were detected during the 2014 elections either. This allows us to estimate the probability of a large-scale attack detection exactly the same way as was done for the 2013 elections above.

VII. Conclusions and further work

In this paper, we described an extension to the Estonian Internet voting protocol, allowing users to verify that their votes are stored correctly on the server. We discussed the technical aspects and quantified the resulting security guarantees obtained during two pilot application runs.

On the one hand, Estonian democracy is rather young and all the potential weaknesses of Internet voting are aggressively used in political battles to attempt revocation or at least harm the reputation of this voting method. On the other hand, Estonian society is also very technology-oriented. For example, virtually all the eligible voters have a digital ID card capable of giving legally binding RSA signatures, and the penetration of mobile devices is growing rapidly. These considerations allowed us to propose a verifiable Internet voting scheme relying on an ID card as a pre-channel and a mobile device as a post-channel. In order to successfully and non-discoverably manipulate a vote, the attacker has to corrupt both the voter's PC and mobile device in a coordinated manner. Even if this is conceivable for a small number of votes, we consider the complexity of a corresponding successful widespread attack prohibitively high.

The system was implemented as a pilot solution for the 2013 Estonian local municipal elections and the 2014 European Parliament elections. It is expected to have legal implications in the 2015 parliamentary elections. Before legally binding conclusions can be drawn, new dispute resolution mechanisms need to be created. For example, we need to better understand how to distinguish true verification failure claims from false ones and how to deal with these false claims.

The success of the proposed system relies on the fact that currently PCs and mobile devices are independent and run different operating systems. This situation may change in the future, which means that the system will then need to be modified suitably. Also, the first pilot implementations of 2013 and 2014 are expected to give a lot of feedback, and improving the system accordingly will remain the subject of future development efforts.

Acknowledgements

This research was supported by the Estonian Research Council under Institutional Research Grant IUT27-1 and the European Regional Development Fund through the Centre of Excellence in Computer Science (EXCS) and grant project number 3.2.1201.13-0018 "Verifiable Internet Voting – Event Analysis and Social Impact".

The authors would also like to thank Arnis Paršovs for proofreading the paper and all the anonymous reviewers for their excellent comments.

References

[1] Forschungsgruppe Internetwahlen, Zweiter Zwischenbericht zum Projekt, Strategische Initiative:WahlenimInternet'nachAbschlussderWahlenzum Studierendenparlament der Universität Osnabrück am 2. Feb. 2000, 2000.

[2] Report of the National Workshop on Internet Voting: Issues and Research Agenda. Internet Policy Institute, http://verifiedvoting.org/downloads/NSFInternetVotingReport.pdf, 2001, last accessed May 6th, 2014.

[3] Legal, operational and technical standards for e-voting. http://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf, April 2005, last accessed May 6th, 2014. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum.

[4] The Geneva Internet Voting System. http://www.geneve.ch/evoting/english/doc/final-livret-anglais.pdf, last accessed May 6th, 2014.

[5] Ben Adida. Helios: web-based open-audit voting. In *Proceedings of the 17th conference on Security symposium*, pages 335–348, 2008.

[6] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, WPES '06, pages 29–40, 2006.

[7] Jordi Barrat, Michel Chevallier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. Internet Voting and Individual Verifiability: The Norwegian Return Codes. In Melanie Volkamer Manuel J. Kripp and Rdiger Grimm, editors, *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, volume 205 of *LNI – Lecture Notes in Informatics*, pages 35–45, 2012.

[8] Christian Bull and Henrik Nore. Problems encountered. Seminar on Internet voting, http://www.regjeringen.no/pages/38377245/5_problems_encountered.pdf, September 2013, last accessed May 6th, 2014.

[9] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *Proceedings of the conference on Electronic voting technology*, EVT'08, 2008.

[10] Andreas Ehringfeld, Larissa Naber, Karin Kappel, Gerald Fischer, Elmar Pichl, and Thomas Grechenig. Learning from a Distributed Denial of Service Attack against a Legally Binding Electronic Election: Scenario, Operational Experience, Legal Consequences. In Kim Andersen, Enrico Francesconi, ke Grnlund, and Tom van Engers, editors, *Electronic Government and the Information Systems Perspective*, volume 6866 of *Lecture Notes in Computer Science*, pages 56–67. Springer Berlin / Heidelberg, 2011.

[11] Kristian Gjøsteen. Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380, 2010. http://eprint.iacr.org/.

[12] J. Alex Halderman, Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer, and Drew Springall. Security Analysis of the Estonian Internet Voting System, May 2014. https://estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf.

[13] Sven Heiberg, Peeter Laud, and Jan Willemson. The Application of I-voting for Estonian Parliamentary Elections of 2011. In Aggelos Kiyaias and Helger Lipmaa, editors, *VoteID 2011*, volume 7187 of *LNCS*, pages 208–223. Springer, 2011.

[14] Sven Heiberg and Jan Willemson. Modeling threats of a voting method. In Dimitrios Zissis and Dimitrios Lekkas, editors, *Design, Development, and Use of Secure Electronic Voting Systems*, pages 128–148. IGI Global, 2014.

[15] E.M.G.M. Hubbers, B.P.F. Jacobs, and W. Pieters. RIES: Internet voting in action. In *29th Annual International Computer Software and Applications Conference (COMPSAC 2005)*, pages 417–424. IEEE Computer Society, 2005.

[16] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 2004, last accessed May 6th, 2014. http://www.servesecurityreport.org/paper.pdf.

[17] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. Veryvote: A voter verifiable code voting system. In Peter Y. A. Ryan and Berry Schoenmakers, editors, *VOTE-ID*, volume 5767 of *Lecture Notes in Computer Science*, pages 106–121. Springer, 2009.

[18] Robert Krimmer, Andreas Ehringfeld, and Markus Traxl. The Use of E-Voting in the Austrian Federation of Students Elections 2009. In Rober Krimmer and Rüdiger Grimm, editors, *4th International Conference on Electronic Voting 2010*, Lecture Notes in Informatics, pages 33–44, 2010.

[19] Lucie Langer, Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Classifying Privacy and Verifiability Requirements for Electronic Voting. In *GI Jahrestagung*, pages 1837–1846, 2009.

[20] Ülle Madise and Tarvi Martens. E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In Robert Krimmer, editor, *Electronic Voting 2006, Proceedings of the 2nd International Workshop*, LNI GI Series, pages 15–26, 2006.

[21] C Andrew Neff. Election confidence, 2003, last accessed May 6th, 2014. http://www.verifiedvoting.org/wp-content/uploads/downloads/20031217.neff.electionconfidence.pdf.

[22] OSCE/ODIHR. Estonia. Parliamentary Elections 6 March 2011. OSCE/ODIHR Election Assessment Mission Report. http://www.osce.org/odihr/77557, 2011, last accessed May 6th, 2014.

[23] Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, and Poorvi Vora. Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections*, EVT/WOTE'10, 2010.

[24] Caltech-MIT Voting Technology Project. Voting: What is, what could be. Technical report, Caltech/MIT, 2001.

[25] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

[26] Gerhard Skagestein, Are Vegard Haug, Einar Nødtvedt, and Judith E. Y. Rossebø. How to create trust in electronic voting over an untrusted platform. In Robert Krimmer, editor, *Electronic Voting*, volume 86 of *LNI*, pages 107–116. GI, 2006.

[27] Ida Sofie Gebhardt Stenerud and Christian Bull. When Reality Comes Knocking. Norwegian Experiences with Verifiable Electronic Voting. In Manuel Kripp, Melaine Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012*, Lecture Notes in Informatics, pages 21–33, 2012.

Experiences with Voting Machines

From Piloting to Roll-out: Voting Experience and Trust in the First Full e-election in Argentina

Julia Pomares
Political Institutions Program
Center for the Implementation of Public Policies Promoting Equity and Growth
Buenos Aires, Argentina
jpomares@cippec.org

Ines Levin
Department of Political Science
University of Georgia
Athens, United States

R. Michael Alvarez
Division of the Humanities and Social Sciences
California Institute of Technology
Pasadena, United States

Guillermo Lopez Mirau
Under-Secretariat for Planning of the Government of the province of Salta
Salta, Argentina

Teresa Ovejero
Electoral Secretariat
Electoral Tribunal of the province of Salta
Salta, Argentina

***Abstract*— Despite the conventional wisdom that e-voting would take place first in established democracies and later in developing countries, the speed of implementation has been higher in the developing world, especially in Latin America, with several countries such as Brazil, Venezuela, Argentina and Ecuador implementing e-voting methods. This paper looks at the experience of Salta, the first Argentine district rolling out e-voting for the entire electorate in 2013. Based on a survey of 1,000 voters in the 2013 provincial elections, the voter's experience and confidence in the election process is analyzed. Among the key findings, there is a strong effect of a voter's ability to use the voting machine without assistance on the overall support for e-voting and positive perceptions of integrity in the election process. These results have both theoretical and policy implications.**

Keywords*— *e-voting; confidence; usability; Latin America; Argentina

I. INTRODUCTION

In the 2013 elections, Salta became the first province in Argentina to implement an e-voting system for the entire electorate (about 900,000 voters). The system was used to select provincial candidates – there are compulsory primaries for voters and parties[1] – and to elect provincial legislators and council members in the municipalities throughout the province. The election took place amidst a wave of change in voting procedures at the provincial level in Argentina [1] [2] [3] [4]. Although national elections are still conducted using the ballot and envelope system (also called French system by which each party is responsible for printing and disseminating ballots), several provinces including some of the most populated ones – the autonomous City of Buenos Aires, Santa Fe, and Cordoba – have changed legislation to introduce new voting procedures. Against this background, lessons learnt from Salta – one of the few districts[2] of the country with an important proportion of indigenous people[3] – are key to informing other provinces as well as other countries in the region seeking to implement e-voting systems. For example, Ecuador has piloted the same system used in Salta in the 2014 local elections.[4]

Based on a survey of 1,000 voters conducted on Election Day (November 10, 2013), this paper analyzes two central aspects of voters' attitudes toward the voting system:

[1] Since 2009, all legislative and executive candidates must be nominated through primaries. Parties must hold primary elections, even if there is no internal competition. Candidates need to get 1.5% of votes in the primaries in order to get to the general stage. Participation in primaries (and general elections) is compulsory.

[2] Each of the 24 provinces serves as an electoral district for the national Senate and chamber of deputies.

[3] According to the last National Census (2010), 2.7% of Argentine population are indigenous. The highest proportions are to be found in four provinces, including Salta (8% of the population).

[4] See Consejo Nacional Electoral, "Simulacros de voto electrónico probarán eficacia del sistema," http://www.cne.gob.ec/index.php/Boletines-de-prensa/Articulos/simulacros-de-voto-electronico-probaran-eficacia-del-sistema.html.

perceptions and opinions about the voting experience, with a special focus on the use of the voting machine, and perceptions about the integrity of the electoral process. The paper is structured as follows. Section 2 presents our motivation for the analysis of these attitudes and the questions of the survey. Section 3 goes into detail about how e-voting is being implemented in Argentina and the context of the 2013 election under analysis. Section 4 presents the data and results of a statistical analysis of the determinants of voting experience and confidence in the integrity of the electoral process. Section 5 concludes by focusing on the policy implications of the key findings.

II. WHY FOCUS ON VOTERS' EXPERIENCES AND PERCEPTIONS OF ELECTORAL INTEGRITY?

Our interest in the voting experience is justified by the fact that voting technologies frame the voting experience in direct and indirect ways. Directly, the voting experience might affect the degree of satisfaction that people draw from that experience and opinions about the change in voting procedures. Indirectly, it might influence opinions about the transparency and integrity of elections. Also, in the context of a very diverse population, we are interested in understanding the socio-demographic determinants of evaluations of the voting system. Do differences in age and education affect voter evaluations? Does living in the urban Capital affect perceptions of ease of use and overall assessments of the new voting system? In order to answer these questions, we look at perceptions of usability and speed of the voting procedure, opinions about ease of use of different interactions with the voting machine (inserting the ballot, operating the touchscreen device and finding the candidates), as well as overall evaluations of the new voting system.

Second, we focus on confidence in elections for both theoretical and policy reasons. On the one hand, an increasing body of literature looks at trust in voting technologies in both established [5] [6] [7] [8] and developing democracies [9] [10] [11]; [12]; [13] [14]. Whereas quantitative analyses follow an inductive approach and test whether individual- or institutional-level variables shape perceptions of trust, qualitative accounts look at the *socio-cultural aspects* of the election process that are shaped by voting procedures [15]. Following previous research of the authors [1] [4], this paper places key importance on breaking down the concept of confidence into different dimensions, differentiating between perceptions of accuracy and secrecy.

At the same time, studies of trust in elections also have important policy implications. The increasing interest in e-voting technologies in developing countries is usually associated with trying to building confidence in the fairness of the electoral process. Studies of elections in Latin America [1] [16], as well as comparative studies [17], show that the focus on boosting perceptions of trust in electoral processes is an important driver of the move toward electronic voting technologies. Against this background, the Salta election is of key policy relevance since this first full implementation of e-voting might shed light on the potential consequences of introducing e-voting in other developing countries, many of which are already testing and deploying new voting procedures (such as Mexico, Ecuador and Peru).

Three questions on confidence in the election were asked. First, we distinguished between two specific dimensions of confidence in the election process: confidence that a vote will be counted as intended and confidence that the ballot will be kept secret. Whereas the former assesses perceptions of accuracy of the voting system and fairness of the counting procedure, the latter captures the ability to preclude violations of privacy and voter intimidation. Additionally, we looked at broader perceptions of the cleanness of the election.

III. E-VOTING IN ARGENTINA

The voting system traditionally used throughout the country in Argentina is the French system of ballot and envelope. Typically, a paper ballot contains party-specific candidates for multiple races that take place on the same day – which might include candidates to the presidency, national deputies, governor, provincial deputies, mayor, and local councils – and dotted lines indicate to voters how to split their vote across down-ticket races. On Election Day, voters vote in private (i.e. behind closed doors) inside a room denominated "*cuarto oscuro*" where party-specific paper ballots are displayed on several tables. Once inside the room and on their own, voters select their favorite candidates for each race – they can split their vote by picking parts of party-specific ballots, or they can vote straight-ticket by picking an unbroken party-specific ballot – and place their choices inside an envelope that they subsequently insert into a ballot box located outside the "*cuarto oscuro*."

Another important feature of the traditional voting system is that each party is responsible for printing the ballots, as used to be case in the first applications of the French system in the United States.[5] This means that once ballots are displayed in voting booths, parties are responsible for guaranteeing their supply throughout Election Day. This was not a problem under the historic two-party system in Argentina, but has increasingly come into question with the rise in political fragmentation since 1999. On the occasion of the 2007 national legislative elections, for instance, there were several claims of ballot manipulation in the province of Buenos Aires, the largest district of the country. As a consequence, the National Electoral Chamber – the highest electoral court – called for changes to the voting procedure to guarantee that all electoral options are made available to voters.

In recent years, several provinces have introduced reforms to their electoral processes, including the adoption of e-voting and of different types of the Australian ballot.[6] Salta, a province located in the northwestern part of the

[5] For a detailed analysis of the implementation of the Australian ballot in American elections, see [18].

[6] By Australian ballot, we refer to the system in which all parties are on the same official ballot, provided by the electoral authority and the voter marks her option.

country with electoral roll of about 900,000 voters, became the first province to introduce an e-voting system for general provincial elections in 2009. E-voting machines used in Salta allow voters to select candidates electronically using a touchscreen, and subsequently print choices on paper ballots that voters deposit in a ballot box. At the close of the polls, the voting machines turn into tallying machines that poll workers use to count votes. Under this new system, the relatively private act of selecting electoral options behind doors inside a "*cuarto oscuro*" is replaced with a much more public act, using a machine within sight of other voters. Although voting machines are placed inside the polling place using a layout that seeks to preserve voter privacy, the abandonment of the "*cuarto oscuro*" might induce negative perceptions of vote secrecy [3] [4].[7]

The electronic voting system was first tested in 2009 during the primaries of the Peronist party at selected polling stations in the capital of the province and suburbs. In 2011, the e-voting system was used during the primary and general elections, when the roll-out was extended to 33 per cent of the province's electoral roll. The gradual implementation of e-voting in Salta allowed researchers to learn about the impact of e-voting by comparing the voting experiences of first-time e-voters and voters who continued using the traditional voting system [3] [4]. Although the government plan was to implement the e-voting system in two more subsequent stages (66 per cent of voters in 2013 and full roll out in 2015), the provincial Executive decided to fully implement the electronic system in 2013, extending it to the entire electoral roll. In this paper, we study the impact of voting experiences on attitudes toward the e-voting system among first- and second-time e-voters, using data from a voters' survey conducted during the 2013 general election in Salta.

In 2013, the e-voting system was implemented for the whole electorate (892,000 voters in 2700 polling tables) first for compulsory open primaries (6 October) and several weeks later (10 November) for the general provincial elections. Some comments about the political context of the election are necessary. A very negative electoral campaign took place in this midterm election and the incumbents did not perform well. Whereas the governor got reelected in 2011 with 60 per cent of the votes (when e-voting was piloted for one third of the electorate), his legislative candidates got only 20 per cent of the votes in the 2013 contest. Also, it is important to add that the main opposition to the governor throughout the province came from a faction of the incumbent Peronist Party. Although these political leaders supported the change in voting procedures in 2011, they strongly opposed it in 2013. Moreover, the debate about the roll out of the e-voting system played a key role in the electoral campaign. The main provincial newspaper (*El Tribuno*) dedicated the front pages of the paper in the last week of the election to the prospect of e-voting machines functioning properly on Election Day. It was a very competitive election, especially in the Capital City. For the first time in their history, the Workers' Party (of left-wing ideology) got the first place in the election in the Capital of the province with 27 per cent of the votes.

In order to grasp the perceptions of voters and poll workers about the e-voting system, the Electoral Tribunal (part of the Judiciary), the Executive government and the Buenos Aires-based think tank CIPPEC designed and conducted a survey of 1,000 voters and 185 poll workers. Both surveys were administered on Election Day. This paper presents the results of the voters' survey, focusing on two central issues: the voting experience, and different dimensions of voter's confidence in the election process and evaluations of the voting system.

A stratified sample of 24 schools (polling stations) throughout the province was created. In all, nine municipalities were selected including the provincial Capital (concentrating 60 per cent of the provincial electorate and where most e-voting piloting took place in 2011). A team of two pollsters was assigned to each polling station. Each pollster was expected to administer at least 20 voter surveys. They were told to randomly recruit voters on their way out of the polling tables. In order to ensure a uniform socio-demographic distribution of the sample, half of their surveys had to be administered to men and they also had to follow age quotas. We present findings from the data in the next section.

IV. Voting Experience and Perpceptions of Integrity during the 2013 Elections

A. A first look at the data

When asked about perceptions of ease of use and speed of the voting system, we find very positive responses among Salta voters: 9 out of 10 voters said that voting was *very* or *somewhat* easy, and 8 out of 10 said that voting was *fast* or *very fast* (Table I). Voter opinions are also overwhelmingly positive when surveyed about the ease of interacting wit different features of the voting machine: approximately 9 out of 10 said instructions were easy to understand, and a similar number said that inserting the ballot into the machine, using the touchscreen and finding the voting option was easy (Table I). Also, voters reported very positive opinions about the qualification of poll workers: 72 per cent said that they were *very* or *somewhat* qualified to exercise their roles.

TABLE I: Perceptions of Ease of Use and Speed of Voting Procedure

Ease of Use and Speed of Voting Procedure	%
Voting was easy	88.7
Voting was fast	80.3
Machine Ease of Use	%
Instructions were easy to understand	92.3
Inserting the e-voting ballot was easy	87.5
Using the touchscreen was easy	91.3
Finding the voting option was easy	88.8

Note: summary statistics were computed excluding non-responses (N=981).

[7] Interested readers can find more description of these voting systems, and photographs of the voting devices in [3] [4].

Despite these positive evaluations of the voting experience, 1 out of 5 voters said that they experienced a problem while voting and 13 per cent of voters needed help in order to be able to cast a ballot (Table II). There are significant differences by age and education. The proportion of voters needing help doubles among least educated voters: 27 per cent of those with no formal education or only primary education needed assistance. Also, voters older than 50 years experienced more difficulties: 23 per cent of them reported having asked for help. Demanding assistance to understand the voting system is an important consideration because if poll workers are unable to help voters and preserve privacy at the same time, the secrecy of the ballot might be called into question.

TABLE II: Responses to questions about Voting Experience

Other Aspects of Voting Experience	%
Experienced a problem while voting	19.0
Thinks electoral authorities were qualified	72.2
Needed help while voting	13.1
Voter chose to split his/her ticket	34.4

Note: summary statistics were computed excluding non-responses (N=981).

Interesting insights also come out of questions inquiring about general evaluations of the system: an overwhelming majority evaluates the system in positive terms. When asked "in broad terms, how would you evaluate the voting system used today," 8 out of 10 voters said *very good* or *good*. Despite these positive opinions, a majority of voters (53 per cent) said that they would like to switch back to the traditional paper ballot system.

TABLE III: General Evaluations of the System and Voter confidence

General Evaluation of e-voting System	%
Evaluated system in positive terms	82.0
Prefers the traditional voting system	53.2
Confidence in the Election Process	%
Confident vote was correctly recorded	75.5
Confident in ballot secrecy	57.6
Believe elections in Salta are clean	35.0

Note: summary statistics were computed excluding non-responses (N=981).

Similar to previous findings on the 2011 elections, we find support for the hypothesis that perceptions of accuracy and secrecy operate differently: whereas there are high levels of trust in the ability of the system to correctly record the preferences of voters, with 75 per cent of voters reporting positive responses, voters seem more hesitant about ballot secrecy, with only 58 per cent reporting positive responses (Table III). The third question on perceptions of cleanness of the election got quite negative results: only 35 per cent of voters believe elections in Salta are clean. It is important to keep in mind that this question might capture a broader discontent with political parties and disaffection and not exclusively opinions about the voting system.

B. Statistical analysis

In order to gain a deeper understanding of the determinants of voter evaluations of the voting experience and confidence in the electoral process, we estimated a series of logistic regressions for a set of outcome variables related to: (a) voters' evaluations of ease of use and speed of the voting system; and (b) voters' confidence that their vote was recorded correctly and that ballot secrecy was preserved, together with general evaluations of the cleanness of elections in Salta. We included a set of control variables: encountering a problem while voting; perceptions of qualification of poll workers; having needed help while voting; having used the e-voting system in a previous election; whether the voter split his/her ticket; living in the Capital of Salta; age; gender; political information;[8] technology use; belief that technology simplifies life; and education.[9]

Tables IV through VII present estimates of marginal effects (i.e. changes in predicted probabilities that the binary dependent variable takes value one as a result of marginal changes in explanatory variables) and 95% confidence intervals. Results are presented in different tables based on the type of outcome variable: general evaluations of ease of use and speed of voting procedure (Table IV); ease of use of different features of the e-voting system (Table V); general evaluations of the e-voting system and preference for the previous ballot and envelope system – referred to here as "traditional voting" (Table VI); and, finally, voters' confidence in their vote being counted as intended, in ballot secrecy, and perceptions of the cleanness of elections in Salta (Table VII).

Looking at the determinants of perceptions of ease of use and speed of the voting procedure, we find a clear influence of asking for help and encountering a problem while voting, in the expected direction: asking for assistance reduces the probability of positively evaluating ease of voting by 13 percentage points. Also, encountering a problem reduces the probability of saying that voting was fast by 14.5 percentage points. Having used e-voting in the past also increases the probability of saying that voting was fast by 6 percentage points. An influence of age is also evidenced in these results: voters older than 49 years have a 3-point higher probability of saying that voting was easy. Interestingly, there is no effect of educational attainment on these perceptions (Table IV). At the same time, a strong belief in the benefits of technology (that is, strongly agreeing that technology makes life simpler) also increases the probability of holding positive perceptions of ease of use. Finally, more favorable evaluations of poll worker qualifications also have a positive influence on opinions about ease of use and speed of the voting procedure.

[8] Political information was computed as the number of correct answers among three questions measuring knowledge of persons holding salient positions in national and provincial governments.

[9] Missing values in dependent and explanatory variables were imputed using the R package *mice* [19] before estimating the regression models.

The two most direct measures of usability (encountering a problem while voting and asking for help) have considerable effects on saying that diverse actions were easily performed (Table V), including understanding instructions, inserting the ballot in the voting machine, using the touchscreen, and finding the preferred electoral option. For instance, asking for help reduces the probability of saying that inserting the ballot into the machine was easy by 20 percentage points. It is important to bear in mind that several problems had taken place during the voting process in the primary election conducted in October.[10]

Although it might be expected that experiences such as encountering a problem while voting and needing to ask for help influence perceptions of usability, it is less clear that they might affect overall evaluations of the system. We find, however, strong evidence that this is the case: asking for help increases by 15 percentage points the probability of preferring a return to the traditional means of voting with paper ballots. Perhaps not so surprisingly, those more likely to use technology in their everyday lives are less likely to prefer the old method of voting (Table VI). Voter evaluations of poll worker qualifications are also drivers of support for returning to the previous voting system. These results point to the importance of voting experience and usability issues for general evaluations of the e-voting system.

Finally, important findings can be drawn from the analysis of the determinants of confidence in the electoral process (Table VII). In line with results found for overall evaluations of the voting system, encountering a problem while voting is an important driver of negative perceptions of ballot secrecy (although not of perceptions of accuracy of the voting system). Quite remarkably, perceptions of qualification of poll workers are a strong determinant of voters' confidence in the integrity of the electoral process (favorable evaluations lead to 16.6 and 23.3 percentage point increases in perceptions of accuracy and secrecy of the voting process, respectively). Not only do these evaluations have an influence on specific dimensions of confidence in the voting process (accuracy and secrecy) but also exert considerable impact on thinking that elections in Salta are clean (a 22.1 percentage point increase). Also, after controlling for other factors, neither age, education, nor gender influence perceptions of confidence in the integrity of the electoral process. Only one demographic attribute exerts a statistically significant influence on voter confidence: living in the Capital vis-à-vis the interior of the province. Those living in the most urban areas are less likely to hold positive opinions on the secrecy of the ballot and are also less likely to believe that elections in Salta are clean. Lastly, the fact that those with more political information hold more negative opinions might indicate that negative reports about e-voting in the news media negatively influenced voters' perceptions.

V. Concluding Remarks

This paper has analyzed survey data from an important implementation of e-voting in Salta, Argentina. The primary focus has been on voter evaluations of the usability of the electronic voting system, and voter confidence in the electoral process. Since one of the main reasons for the move toward to electronic voting systems in Latin America is to improve voter perceptions of the integrity of the electoral process, it is important to evaluate voter reactions to these new means of ballot marking, casting and tabulation.

We find important results. In particular, we can conclude that voter confidence is associated with both the usability of the voting system and with the qualifications of those who assist voters when they have trouble with the system – poll workers. Both of these results shed light on dimensions of voter confidence that have not been well studied so far in the literature. Future research on evaluating new voting systems, and on voter confidence, needs to pay more attention to contextual determinants of confidence in the voting system and its integrity.

Finally, this paper has significant policy ramifications for nations in Latin America considering the adoption of new voting technologies. On one hand, the implementation of new voting systems – if accomplished with secure and usable voting technologies – may be able to improve voter confidence in the integrity of a nation's electoral process. New voting technologies, if well designed to address existing concerns with the traditional voting process, can help mitigate previous apprehensions. On the other hand, it is also seems clear that new voting systems can raise other concerns, for example, regarding voter privacy. Additionally, results discussed in this paper point to the importance of poll worker training: their job has key implications for voters' evaluations of the new system. It is only by adopting a scientific program evaluation – like that used in the recent implementations of e-voting in Salta – that the effects of adopting a new voting system can be measured and assessed.

Acknowledgements

We would like to thank the Voting Technology Project (CALTECH/MIT), Micromata, and Charles Stewart for their support to present this work at the EVOTE 2014.

[10] In the context of the primary elections, the media reported numerous cases of machines with problems reading ballots. According to informal talks with the provider, these problems were largely reduced for the general elections.

REFERENCES

[1] Alvarez, R. Michael, Ines Levin, Julia Pomares and Marcelo Leiras.. Voting Made Safe and Easy: The Impact of e-voting on Citizen Perceptions. Political Science Research and Methods 1(1), 2013, pp. 117-137.

[2] Katz, Gabriel, R. Michael Alvarez, Ernesto Calvo, Marcelo Escolar, and Julia Pomares. Assessing the Impact of Alternative Voting Technologies on Multi-Party Elections: Design Features, Heuristic Processing and Voter Choice. Political Behavior 33(2), 2011, pp. 247-270.

[3] Lopez Mirau, Guillermo, Teresa Ovejero, Julia Pomares. The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner´s Perspective. Proceedings of the 5th International Conference on Electronic Voting 2012, Kripp, M.; Volkamer, M.; Grimm, R., Eds. Bregenz, Austria, July 2012.

[4] Pomares, Julia, Ines Levin, and R. Michael Alvarez. Do Voters and Poll Workers Differ in their Attitudes Toward e-voting? Evidence From the First e-election in Salta, Argentina. USENIX Journal of Election Technology and Systems 2(2), 2014, pp. 1-10.

[5] Alvarez, R. Michael, Thad E. Hall, and Morgan H. Llewellyn. 2008. Are Americans Confident their Ballots are Counted? Journal of Politics 70(3):754–66.

[6] Delwit, Pascal, Erol Kulahci, and Jean-Benoit Pilet. 2005. Electronic Voting in Belgium: A Legitimized Choice? Politics 25(3):153–64.

[7] Stewart III, Charles. Election Technology and the Voting Experience in 2008. Caltech/MIT Voting Technology Project Working Paper #71, http://www.vote.caltech.edu/sites/default/files/ElectionTechnology_CStewart_033109.pdf. 2009.

[8] Atkeson, Lonna Rae and Kyle L. Saunders. The Effect of Election Administration on Voter Confidence: A Local Matter? PS: Political Scince & Politics 40(4): 2007, pp. 655-660.

[9] Alvarez, R. Michael, Gabriel Katz, Ricardo Llamosa, Hugo E. Martinez.. Assessing Voters' Attitudes towards Electronic Voting in Latin America: Evidence from Colombia's 2007 E-Voting Pilot. E-Voting and Identity: Lecture Notes in Computer Science Volume 5767, 2009, pp 75-91.

[10] Alvarez, R. Michael and Thad E. Hall. Electronic Elections: The Perils and Promises of Digital Democracy. Princeton: Princeton University Press. 2010.

[11] Alvarez, R. Michael, Gabriel Katz, and Julia Pomares. The Impact of New Technologies on Voter Confidence in Latin America: Evidence from E-Voting Experiments in Argentina and Colombia. Journal of Information Technology & Politics. Volume 8, Issue 2. 2011.

[12] Fujiwara, Thomas. Voting Technology, Political Responsiveness, and Infant Health: Evidence from Brazil. Unpublished Manuscript. https://www.gsb.stanford.edu/sites/default/files/documents/pe_02_11_pefujiwara.pdf. 2010.

[13] Hidalgo, F. Daniel. Digital Democratization: Suffrage Expansion and the Decline of Political Machines in Brazil. Unpublished Manuscript. http://politics.as.nyu.edu/docs/IO/17524/hidalgo.pdf. 2010

[14] McCoy, Jennifer. One Act in an Unfinished Drama. Journal of Democracy 16(1): 2005.

[15] Dompnier, Nathalie. "Les machines à voter à l'essai. Notes sur le mythe de la "modernisation démocratique"." *Genèses (Genèses)*:, pp. 69-88.

[16] Rodrigues-Filho, Jose, Cynthia J. Alexander, and Luciano C. Batista. 2006. E-voting in Brazil—The Risks to Democracy. In Electronic Voting 2006, edited by. R. Krimmer & R. Grimm, 85–94. Bonn, Germany: Gesellschaft fur Informatik.

[17] Pomares, Julia. 'Inside the Black Ballot Box. Origins and Consequences of Introducing Electronic Voting Methods'. PhD diss., London School of Economics and Political Science. 2012

[18] Ware, Alan.. The American Direct Primary: Party Institutionalization and Transformation in the North. Cambridge University Press. 2002

[19] van Buuren, S., & Groothuis-Oudshoorn, K.. MICE: Multivariate imputation by chained equations in R. *Journal of Statistical Software* 45(3), 2011, pp. 1-67.

TABLE IV: Determinants of Perceived Ease of Use and Speed of Voting Procedure

	Ease of voting			Voting speed		
	Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-12.9**	**-19.6**	**-7.5**	**-14.5**	**-22.1**	**-6.9**
Qualification of authorities: none/little to quite a lot/very	**4.0**	**1.3**	**7.2**	**12.4**	**7.1**	**18.0**
Needed help: no to yes	**-13.1**	**-21.4**	**-6.9**	**-15.9**	**-26.3**	**-7.1**
Previous e-voter: no to yes	1.9	-0.8	4.6	**6.2**	**1.5**	**10.8**
Split ticket voter: no to yes	1.6	-1.0	4.1	0.8	-4.4	5.5
Lives in Capital: no to yes	2.7	-0.4	6.0	**13.5**	**8.1**	**19.2**
Age: 24 to 49	**-2.7**	**-5.5**	**-0.3**	3.0	-1.8	7.6
Female: no to yes	-1.0	-3.5	1.7	4.1	-0.6	9.0
Information scale (0-3): 0 to 1	-0.7	-4.3	0.9	-1.4	-6.5	1.8
Technology use scale (0-6): 3 to 6	0.4	-2.4	2.9	3.1	-1.1	7.5
Belief technology simplifies life: agree to agree a lot	**3.1**	**2.1**	**4.3**	**5.6**	**2.7**	**8.2**
Education: incomplete 2ry to complete 3ry	0.9	-1.2	3.1	-1.1	-4.9	2.6

Note: Ease of voting is coded 1 if “easy” or “very easy”, and 0 if “difficult” or “very difficult”. Voting speed is coded 1 if “fast” or “very fast”, and 0 if “slow” or “very slow”. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE V: Determinants of Perceived Ease of Use of Different Features of the Voting System

	Ease of instructions			Ease of inserting ballot			Ease of using touchscreen			Ease of finding choice		
	Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-3.0**	**-6.9**	**-0.1**	**-18.4**	**-26.3**	**-11.3**	**-5.8**	**-10.7**	**-1.9**	**-14.0**	**-20.9**	**-8.1**
Qualification of authorities: none/little to quite a lot/very	1.9	-0.3	4.3	-2.2	-6.2	1.7	**4.2**	**1.4**	**7.1**	**7.3**	**3.7**	**11.2**
Needed help: no to yes	**-10.8**	**-18.9**	**-5.1**	**-19.6**	**-29.2**	**-11.4**	**-9.4**	**-17.0**	**-3.6**	**-10.3**	**-18.0**	**-3.5**
Previous e-voter: no to yes	1.8	-0.1	3.8	2.1	-1.8	5.8	-2.4	-5.6	0.2	1.4	-2.3	4.8
Split ticket voter: no to yes	0.1	-2.1	2.0	0.2	-3.7	4.1	-0.4	-3.4	2.1	-0.8	-4.7	2.4
Lives in Capital: no to yes	2.0	0.0	4.4	3.1	-0.4	7.9	-0.8	-3.4	1.9	-1.4	-4.8	2.2
Age: 24 to 49	-1.3	-3.4	0.5	0.6	-2.8	4.1	-0.5	-2.7	1.9	-1.0	-4.2	2.0
Female: no to yes	-0.7	-2.6	1.2	-2.5	-5.8	1.2	-0.6	-3.0	2.1	-0.4	-3.6	2.9
Information scale (0-3): 0 to 1	**0.4**	**0.1**	**0.8**	0.4	-3.0	1.7	**0.7**	**0.4**	**1.1**	1.2	-0.2	1.7
Technology use scale (0-6): 3 to 6	1.0	-0.9	2.7	0.6	-3.4	4.3	0.8	-1.7	3.2	-1.9	-5.8	1.5
Belief technology simplifies life: agree to agree a lot	**1.7**	**0.9**	**2.7**	0.7	-2.1	3.1	**3.0**	**2.0**	**4.0**	**2.4**	**0.2**	**4.3**
Education: incomplete 2ry to complete 3ry	0.1	-1.3	1.5	-2.2	-4.9	0.5	**-2.7**	**-4.6**	**-0.9**	-1.0	-3.6	1.5

Note: Responses to questions related to the ease of use of different features of the voting system are coded 1 if "easy" or "very easy", and 0 if "difficult" or "very difficult." Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE VI: Determinants of Overall Evaluation and Preference for Traditional Voting

	Evaluation system			**Preference for traditional voting**		
	Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-11.9**	**-19.8**	**-5.1**	**11.4**	**2.8**	**19.9**
Qualification of authorities: none/little to quite a lot/very	**14.7**	**9.9**	**20.0**	**-24.5**	**-31.7**	**-17.0**
Needed help: no to yes	**-8.4**	**-17.0**	**-1.2**	**14.7**	**3.5**	**24.5**
Previous e-voter: no to yes	-0.4	-5.4	4.0	3.6	-3.9	10.9
Split ticket voter: no to yes	-0.4	-5.2	4.1	-0.4	-7.6	7.0
Lives in Capital: no to yes	3.0	-2.0	7.5	0.2	-6.8	7.3
Age: 24 to 49	-1.9	-5.9	2.5	1.2	-4.9	7.7
Female: no to yes	0.8	-3.6	4.7	-2.1	-9.1	5.2
Information scale (0-3): 0 to 1	**-5.0**	**-11.3**	**-0.1**	4.3	-0.2	7.9
Technology use scale (0-6): 3 to 6	1.9	-2.9	6.3	**-7.8**	**-14.9**	**-0.4**
Belief technology simplifies life: agree to agree a lot	**6.6**	**4.4**	**8.5**	**-22.0**	**-27.2**	**-16.0**
Education: incomplete 2ry to complete 3ry	-2.6	-6.1	1.1	-3.3	-8.7	2.3

Note: General evaluations of the system are coded 1 if "good" or "very good", and 0 if "bad" or "very bad". Preferences for traditional voting are coded 1 if the voter reports that she/he would have preferred to vote using the traditional voting system, and 0 otherwise. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE VII: Determinants of Perceptions of Confidence in the Integrity of the Election Process

	Confidence vote recorded			Confidence ballot secrecy			Election in Salta are Clean		
	Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	-6.9	-14.8	0.2	**-11.0**	**-20.0**	**-2.0**	-1.5	-9.7	7.0
Qualification of authorities: none/little to quite a lot/very	**16.6**	**10.6**	**22.6**	**23.3**	**15.7**	**29.9**	**22.1**	**14.8**	**29.6**
Needed help: no to yes	-3.0	-12.2	5.3	-1.5	-12.2	9.5	-1.3	-10.6	8.9
Previous e-voter: no to yes	-0.1	-6.1	5.7	2.9	-4.0	9.4	3.9	-2.7	10.5
Split ticket voter: no to yes	-3.0	-8.9	2.6	-3.7	-10.3	3.5	1.1	-5.5	7.7
Lives in Capital: no to yes	0.3	-5.6	6.2	**-8.9**	**-16.2**	**-1.8**	**-9.2**	**-15.9**	**-2.6**
Age: 24 to 49	-1.4	-6.8	4.3	2.9	-3.5	9.1	4.5	-1.4	10.7
Female: no to yes	2.9	-2.7	8.7	0.4	-6.0	7.1	-2.6	-9.0	3.7
Information scale (0-3): 0 to 1	-0.2	-4.6	2.9	**-5.6**	**-9.6**	**-0.6**	-1.2	-4.9	3.3
Technology use scale (0-6): 3 to 6	-0.7	-6.6	4.6	-3.6	-10.8	3.6	-4.5	-10.7	2.5
Belief technology simplifies life: agree to agree a lot	**8.0**	**4.6**	**10.9**	**12.4**	**8.0**	**17.0**	**17.7**	**11.5**	**23.8**
Education: incomplete 2ry to complete 3ry	-2.7	-6.9	1.8	0.3	-5.1	5.4	2.8	-2.3	8.1

Note: Confidence that the vote was correctly recorded is coded 1 if “sure” or “very sure”, and 0 if “unsure” or “very unsure”. Confidence in ballot secrecy us coded 1 if “confident” or “very confident”, and 0 if “not confident” or “not at all confident”. Perceptions of cleanness of elections in Salta is coded 1 if “very clean” or “somewhat clean”, and 0 if “not very clean” or “not at all clean”. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

E-voting in the Netherlands; past, current, future?

Leontine Loeber
University of East Anglia
Norwich, UK
Leontine_loeber@xs4all.nl

***Abstract*—This paper is a case study of a country in which e-voting used to be the general norm until 2006; the Netherlands. Since the abandonment of e-voting, several attempts have been made to reintroduces some form of e-voting. This paper describes these attempts and tries to give an insight in the possible future developments of e-voting in the Netherlands.**

Keywords— e-voting, case study.

I. INTRODUCTION

The Netherlands was an early adapter of e-voting. Voting machines were introduced in 1966 in a couple of municipalities. Since then, their use grew rapidly, so that during the municipal elections of March 2006 nearly 99% of the voters cast their vote with the use of a voting machine. Both in the 2004 European Parliament elections and the national elections of November 2006, voters abroad could vote through the internet. Since 2007 this use of e-voting dramatically declined. Nowadays, elections are conducted using paper ballots, mail ballots and hand counting. The action group ´We don't trust voting machines´ raised concerns regarding the safety of both the voting machines and the internet voting system. This ultimately led to the decision to quit using these systems and to reassess e-voting in the Netherlands. [1] However, the discussions on the use of e-voting haven't stopped.

When looking at debates concerning e-voting in public elections, two key issues have to be addressed by any e-voting solution. The secrecy of the vote has to be protected, while voters, political parties and other actors have to be able to check if votes are stored and counted as they were cast. [2] The main point that the action group raised was the impossibility to check the integrity of the Direct Recording Electronic Voting Machines (DRE) that were used (Fig.1). However, the issue of secrecy of the vote got the most attention in the debate, due to the fact that this is one of the few criteria for elections that is laid down in international law.[1] Because states have to guarantee free, fair and secret elections, in court cases that the action group started against the approval of the DRE's, they had to focus on the issue of the secrecy more than on the issue of integrity.

Fig. 1. The DRE that was used in the majority of municipalities.

II. E-VOTING IN THE POLLING STATION

After the abandonment of the DRE's that were used in the polling stations a governmental committee made recommendations on the electoral process in general and on new ways of e-voting in particular. In their report 'Voting with Confidence' [3] they recommended a new form of e-voting which would consist of a voter printer and a vote counter. A voter would make its vote on the printer, which would only print the vote. The print would then be put into a ballot box and counted at the end of the day using the vote-counter, by means of scanning it. A group of technical experts were asked if this system would be feasible and how it should be tested. Their findings were that it would be hard to ensure that this new system would meet the criteria for safety and secrecy of the vote. One particular issue that would be difficult to address was the compromising radiation that vote printers would send out, which could be used in order to breach the secrecy of the vote.[2] The Secretary of State therefore informed the Parliament that she would not pursue this system. [4]

The 2009 elections for the European Parliament were the first nation-wide elections held with the use of paper ballots and hand counting. Although the hand counting process meant that it took longer for the results to be known, most municipalities finished their counts before 3 AM election night. (Fig.2).

[1] See for example article 3 of the First Protocol of the European Convention on Human Rights.

[2] In the Dutch debates the term Tempest was used. The official term for eavesdropping by means of electromagnetic emissions is Van Eck phreaking.

Fig. 2. Example of the counting process in the Netherlands.

There were also no major incidents with voters using the paper ballots. In response to question by Parliament on the duration of the counting process, the Secretary of State emphasized that the speed with which the results are known is not a goal in itself. What is important is that the voting process, including the counting of the votes is transparent and verifiable. [5] During the municipal election of March 3rd 2010, there were 15 municipalities out of the 394 that held recounts. These recounts did not lead to changes in the seat distribution. In 2010 the Parliamentary elections were observed by the Office for Democratic Institutions and Human Rights. In their report they agree with the decision to cancel e-voting as an appropriate measure in view of the challenges to electoral integrity that were identified in 2006.

Due to complaints from municipalities about the counting process and the fact that recounts were held, the government decided in April 2010 to examine if it would be feasible to introduce a form of e-counting. A bill was drafted to make experiments with e-counting possible in 2012. However, while the Minister was investigating what requirements should be met before such an experiment could take place, Parliament once again started pushing for e-voting by means of a voting computer. The Electoral Council also showed support for the reintroduction of voting machines. [6] The Minister decided to stop focusing on e-counting in order to look at e-voting again. [7]

In 2013 the government set up a new committee to investigate if e-voting could and should be used. This committee published a report called 'Every vote counts – Electronic voting and counting', in December 2013. [8] The committee concluded that it would benefit the election process to use electronic means to count votes and preferably also to cast votes. The committee presented a model using a vote printer and vote counter. This model allows voters with a physical disability to vote without help[3] while the use of the vote counter eliminated the problems with the inaccuracy of hand counting. It is possible to check the integrity of the system because the printed votes can be hand counted to verify the tally by the vote counter. This committee therefore reached the same conclusion as the committee in 2007.

The government will look into the feasibility of the advised system of a vote printer and a vote counter. The government admits that the Tempest problem which was the reason not to introduce this system after the previous committee in 2007, still exists. However the government takes the stand that if certain measures are taken to reduce Tempest as much as possible, it is acceptable to allow for a certain level of residual risk. [9]

III. INTERNET VOTING

After the discussions surrounding the internet voting for voters living abroad during the national elections of 2006, the Minister had defined criteria that all forms of e-voting should meet. Part of these criteria are the recommendations of the Council of Europe on the use of e-voting. [10] The proposed internet voting system for the waterboard elections in 2008 failed to meet these criteria. A major issue was the robustness of the cryptography that would be used. According to the testing agency, the chosen method of encryption would in the best scenario protect the secrecy of the vote until 2030, but it would be very likely that it would be possible (way) before that date to reconstruct which voter voted for which candidate. Another issue was that a voter with the right software would be able to calculate valid voting codes within 20 hours. Since the voting period was two weeks, this would mean that such a voter would be able to cast at least 16 valid votes. Finally, there were security issues with the system that would be used. [11] The government therefore decided to withhold the certification of this system. [12] The waterboard elections were then held by the use of paper ballot mail votes.

The voters living abroad also used paper ballot mail votes during the European Parliament elections of 2009 and the parliament elections of 2010 and 2012. The main issue for these voters receiving and returning their ballot paper in time. In order to solve this issue, voters were enabled in 2012 to download and print the ballot paper themselves. This eliminates the time it takes to send the ballot papers from the Netherlands to the voter (Fig. 3 and 4).

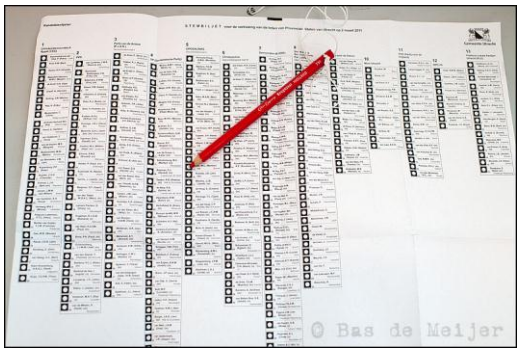


Fig. 3. Regular ballot paper.

[3] A vote printer can be equipped with audio support, making it possible for blind voters to cast their vote on their own.

Fig. 4. Ballot paper for voters living abroad.

In 2013, the Minister commissioned a market research institute to investigate the feasibility of internet voting. [13] Based on their study [14], the government informed Parliament on March 21st 2014 that they had decided that currently there are too many risks with internet voting. Combined with the large costs of internet voting and the fact that there is no evidence that internet voting raises turnout, the government will not introduce internet voting for voters living abroad in the near future. [15]

IV. Debates in Parliament

Before the Parliamentary elections in 2006 during which the controversy on e-voting arose, the Dutch Parliament was a big supporter of e-voting. Most parties were in favor of introducing nation-wide internet voting. In the first two years after the 2006 elections, the view on e-voting was dramatically different. Parliament supported the decision to cancel e-voting as long as the issues concerning secrecy and integrity were not solved. In 2007 it was Parliament who questioned the possible use of internet voting for voters living abroad. Most members felt that the internet voting system might not meet the criteria for secrecy of the vote and integrity and asked for criteria such a system should meet. [16] The decision in 2008 to cancel the use of internet voting for the waterboard elections was also supported by Parliament. In these debates, both issues; secrecy and integrity, were mentioned by members as reasons not to use e-voting. However, this attitude towards e-voting changed after the first elections conducted with paper ballots. Both after the European Parliament elections of 2009 and after the municipal elections of 2010, members asked the Secretary of State to investigate the return to e-voting, because hand counting was both inaccurate and time-consuming. [17] Where members stressed the importance of the integrity of the vote in February 2012, [18] in December 2013, nearly all political parties in Parliament were in favor of using e-voting, because that hand counting was inaccurate. [19]

V. 'Stemfies'

A question that recently got attention in the Dutch voting process is the use of smartphones by voters to make a 'stemfie' (a picture of themselves voting). During the municipal elections of March 2014, a politician posted a photo of himself on social media on which his face and the marked ballot paper were visible, showing his vote (Fig.5). His example was followed by many voters. In answer to questions about these photos, the Minister said that these kind of photos are not prohibited under Dutch law. A ngo then started a procedure against the Minister in which they demanded that he would issue a statement that 'stemfies' are not allowed and that the polling stations should act against them, because 'stemfies' breach the secrecy of the vote. On May 9th 2014, the judge ruled that although the disadvantages of 'stemfies' were in his eyes bigger than the advantages, the Election law does not prohibit them and therefore there was no reason for the Minister to withdraw his statements. During the European Parliament elections, a sign in the polling stations informed voters that they didn't have to reveal their vote to anyone.

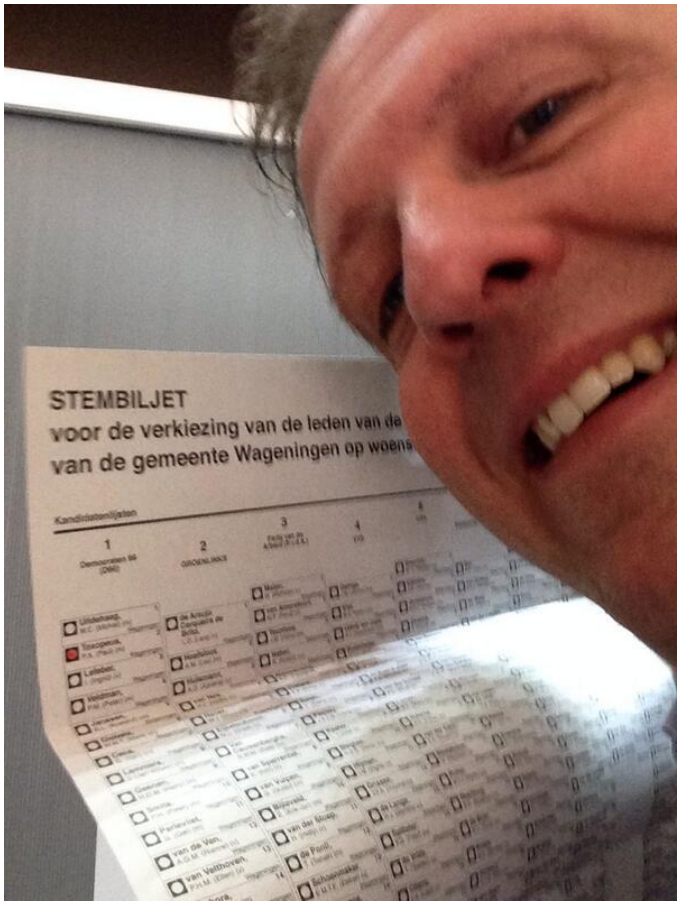


Fig. 5. 'Stemfie'.

VI. Conclusions

Although the events of 2006 led to a withdrawal of all forms of e-voting in the Netherlands and caused debates in Parliament, shortly after, Parliament once again asked for the introduction of new forms of e-voting. Both committees that looked into e-voting recommended the same: a vote printer combined with a vote counter. While government did not follow this advice in 2007 due to the concerns on secrecy of the vote and integrity of the system, nowadays it seems willing to embrace this system. Further research will be done to discover if such a system is feasible, and possible to implement in a cost-efficient manner. The government however has made the decision not to pursue internet voting for voters living abroad.

What is striking about the debate in the Netherlands on e-voting is the short time that elapsed between the decision to abandon e-voting and the renewed call for it from election officials and members of Parliament. Where the main focus was on the protection of the secrecy of the vote and the integrity of the system, it shifted to the (perceived) inaccuracy of hand counting. The arguments against e-voting seemed to have faded into the background in favor of the arguments against voting by paper ballot. One argument that is used in the debate is that paper ballot voting is old-fashioned and that in the Netherlands, where computers are a big part of daily life, it should be possible to use technology in the voting process. It is questionable if this argument should play a role in a debate that should focus on questions of secrecy of the vote, integrity of the system and accuracy of the results.

Besides the issues of e-voting and internet voting, the use of smartphones by voters to make ‘stemfies’ and post them on social media gives rise to a new debate on secrecy of the vote. Is this a right that a person can waive, or is it also a duty of a voter to protect the secrecy of the vote? At this moment, this question remains unresolved, but will undoubtedly play a role in future debates on the Dutch election process.

References

[1] L. Loeber, “E-voting in the Netherlands; from general acceptance to general doubt in two years.” Electronic voting 2008, GI lecture notes in informatics, ed. R. Krimmer and R. Grimm, 21-30. Bonn, Germany: Gesellschaft für Informatik.

[2] L. Mitrou, D. Gritzalis and S. Katsikas. "Revisiting legal and regulatory requirements for secure e-voting." Security in the Information Society. Springer US, 2002. 469-480.

[3] F. Korthals Altes et. al., “Voting with confidence”, Report by the Election Process Advisory Commission September 27, 2007, found on www.minbzk.nl.

[4] Kamerstukken II 2007/08, 31 200 VII, nr. 64.

[5] Kamerstukken II 2009/10, 31 142, nr. 16.

[6] Evaluation report of Septermber 22nd 2010, found on www.kiesraad.nl.

[7] Kamerstukken II 2013/14, 31 142, nr. 37.

[8] Committee reseach electronic voting in the polling station, “Every vote counts, Electronic voting and counting”, Kamerstukken II 2013//14 33 829, nr. 1.

[9] Kamerstukken II 2013/14, 33 829, nr. 3.

[10] Legal, operational and technical standards for e-voting, Rec(2004) 11.

[11] Fox-it, “Rapportage advisering toelaatbaarheid internetstemvoorziening waterschappen”, August 12th 2008.

[12] Kamerstukken II 2007/08, 31 142, nr. 11.

[13] Kamerstukken II 2013/14, 31 142, nr. 39.

[14] Kamerstukken II 2013/14, 33 829, nr. 2.

[15] Kamerstukken II 2013/14, 33 829, nr. 3.

[16] Handelingen II November 21st 2007, 26-2017 – 26-2023.

[17] Handelingen II 2009/10, Aanhangsel 267 and Kamerstukken II 2009/10, 31 142, nr. 22.

[18] Kamerstukken II 2011/12, 31 142, nr. 33.

[19] Kamerstukken II 2013/14, 31 142, nr. 39.

Implementation Project
Electronic Voting Azuay 2014 – Ecuador

Juan Pablo Pozo Bahamonde
National Electoral Minister
National Electoral Council (CNE)
Quito, Ecuador
juanpozo@cne.gob.ec

I. BACKGROUND

After the general elections held on February 17, 2013 , the National Electoral Council became committed to improve the electoral process through the introduction up-to-date voting and counting technologies .

A number of responsible and serious studies were carried out ever since in order to assess the feasibility of implementing the Electronic Voting by multidisciplinary teams. Given the current legislation in Ecuador and especially, the cultural reality found in Azuay province, a third-generation software solution was chosen, the same that incorporates a single ballot with an embedded chip and an electronic voting machine, all in one single system .

Generalities regarding the implementation electronic voting in the province of Azuay, local elections 2014

The project executory unit was embodied by the Provincial Delegation of Azuay. The overall objective was to implement a pilot electronic voting process in the voting and counting stages for the election of sectional authorities to be held in February 2014 in the province of Azuay.

The following specific objectives were set in order to attain this objective:

- To build knowledge base on the electronic voting in order to perform automated elections in the nation.
- To establish the regulatory framework for electronic voting and its implementation.
- To implement automatic processing in voting machines, producing results in a timely and reliable manner.
- To carry-out audits at all stages of the electronic voting.

The pilot plan was implemented in an entire province in order to measure and assess the impact of electronic voting within the voting, counting and totalization stages and to evaluate the overall results with regard to the authorities who are elected in a specific region (Prefect, vice-prefect, municipal mayors, urban and rural municipal councilors, and members of rural parish councils), It was decided to conduct the pilot project in the province of Azuay, based upon the following considerations:

- Azuay has 2.163 voting boards which is 5, 5% of the nation's total.
- The number of voters per each voting station has been kept in (300). One equipment shall be placed in each voting station (2163 equipments in total).
- Twenty per cent of the equipments were assigned to training exercises (440 equipments) whereas 10% were assigned for contingencies (220 equipments).
- The Electoral Province Delegation is skilled in the implementation of electronic voting processes.
- The mentioned Province Delegation has a high level of efficiency in the implementation of electoral processes.
- Staff in Azuay province is adequately trained for the implementation of this kind of projects.
- Adequate means of transportation (road and air) make it easy to transport the voting equipments and allow a good communication between the work teams and the CNE headquarters.
- There are good roads from Cuenca city to all the voting sites throughout the province.

TABLE I. POPULATION DATA

Population data
Azuay province presents the greatest percentage of young population: 46.7% between 15 and 44 years of age.
53.2% of the province young population are women
It is the third most densely inhabited province.

Fig. 1. Geographical location of Azuay province

Azuay is a province located south of Ecuador in the Southern Sierra Region (Andes). Its northern border meets the province of Canar, on the south the provinces of El Oro and Loja, on the east the provinces of Morona Santiago and Zamora Chinchipe, and the province of Guayas to the west. Its capital city is Cuenca, a city known as the "Athens of Ecuador" with some 330,000 inhabitants in the urban area.

II. Analysis to Determine the Best Tool

In order to decide which technology should be used to automate the voting and/or counting process, technological, legal and procedural aspects were taken into account, including the political culture in our country (both in terms of political parties and movements, and citizens in general). Within this framework (once the technology to be implemented was selected), it was possible to start making all necessary contacts throughout Latin American countries for their support with the techology solution that had been chosen. This, because variables such as language, technical support, transportation, among other aspects made it easier to locate the electronic voting method that was applied in our country.

Legal, procedural and technical aspects were taken into account in order to ensure the following conditions: *Universal Suffrage, Equal Suffrage, Free Suffrage, Suffrage Secrecy, Transparency, Verification, Reliability and Safety.* Additionally, all voting options were considered, including null and blank ballots.

As for the integral procedural standards, Calling for elections, Voters, Candidates, Voting process, Results, and Audit were taken into consideration. Also, the following technical standards were considered: Accessibility, Interoperability, Operating Systems, Security, Audit and Certification. Necessary recovery procedures were taken in case of a system failure so that the data would not be lost. The electronic voting system had restricted access levels according to the specific tasks performed by the different users.

Measures were adopted to ensure adequate system protection against intrusions from outside. Transmission of results was safeguarded through the utilization of safe transmission means that guaranteed data integrity and accuracy. The proposal was aimed at improving the quality of electoral processes in charge of the CNE by delivering accurate and verifiable results in the shortest possible time. The final objective is to improve the exercise of political rights of citizens through the implementation of automatic mechanisms within the voting and counting processes.

As per the above (as shown in the chart below), the electronic voting machine with smart ballot proved to be the most adequate for application within the Ecuadorian electoral system. Thus, it was suggested to the CNE Board that the technology that best fits the electoral process and that could deal with the number of candidates for the electoral process of February 23th, 2014, was the electronic voting equipment with smart paper ballot. However, the main problem with electronic voting is that it does not stick to Article 10 of the Organic Law of Elections and Political Organizations of the Republic of Ecuador which provides that popular voting must be publicly scrutinized.

TABLE II. COMPARISON OF VOTING TECHNOLOGY

Feature	*Electronic Ballot Box*	*Styluz*	*Smart Ballot*
Audit of voting at voting station	X	X	X
Voting secrecy	X	X	X
Counting celerity	X	X	X
Equipment portability		X	X
Electrical autonomy			X
Celerity and safety in the transmission of results gathered at each voting station	X		X
Displays candidate information on screen / ballot	X		X
Votes counted in public			X
MJRV-enabled suffrage process.	X	X	X
Accessibility for people with dissabilities.	X		X
Low propability of ballot loss (with votes /voting receipts)		X	X
Vote modifications are not possible during the counting process.	X		X
TOTAL *	8	6	12

III. COMPETITIVE ADVANTAGES OF ELECTRONIC VOTING COMPARED TO MANUAL VOTING

- Experiences in the region are favorable (in some provinces of the Republic of Argentina, this system has been used successfully in voting processeses. More than 900,000 voters from different social and cultural levels use it).
- Vote counting is public and can be observed and validated by different observers and representatives of political sectors.
- It allows to set-up the software according to the election type: It accepts blank and null ballots, votes per lists of candidates and different languages, including Quichua and Spanish. Interface designers made sure that all possibilities are available on the screen.
- 100% auditable throughout all process stages.
- The device where the vote is cast does not store any information; the choices are stored in an RFID chip on the ballot and are printed on it.
- It facilitates voting of people with disabilities including a module for the blind. One of the advantages is that the electronic equipment can be used in various voting processes, which implies an economic benefit.
- Fully portable equipment.
- It does not link the voting station with the equipment, voters can choose any free machine for your vote.
- The voter may request another ballot in case of noticing a mistake.

IV. IMPLEMENTATION OF THE ELECTRONIC VOTING PROJECT

The e-voting project was developed precisely in response to the need of obtaining agile, verifiable and transparent voting results, taking into account today's global demand for free and widespread citizen access to information, knowledge and networking, through the use of digital tools to reduce the technological gap. Moreover, the implementation of electronic voting generates a substantial change in all aspects, with politics and governance as two areas of great importance, leading to a rethinking on the proper relationship between candidates and voters as well as between representatives and citizens.

The proposal on which we based this proposal was a thorough improvement in the quality of electoral processes in charge of CNE and the generation of accurate and verifiable election results in the shortest possible time. The purpose is to improve the application of citizens' political rights by introducing automated mechanisms within voting and counting processes.

V. LEGAL FRAMEWORK

According to the constitutional mandate, the National Electoral Council shall ensure the exercise of people's political rights through their votes as provided for by the Organic Electoral and Political Organizations Law of the Republic of Ecuador, Code of Democracy, enforcing

principles of effectiveness, efficiency and quality that the public administration must observe.

Moreover, by implementing the electronic voting (which does not require the use of ballots), we will provide all aids and adequate safety levels in accordance with article 109 of the Code of Democracy. For instance, we will attain the participation of all voters and will provide the aid required by people with disabilities so that all of them will be able to vote.

The National Electoral Council may also decide to use electronic methods not only during the voting but also for the counting stage, for which purpose all rules can be modified if necessary (based upon Articles 113 and 115 of the Code of Democracy).

VI. Electronic Voting. An effective solution to a ballot counting process

Ecuador has been manually managing the processes of voting and counting of votes at polling stations and the recount in the Provincial Election Boards, with consequent problems that may arise in the manipulation of electoral kits and ballots, problems such as: ballot size, number of candidates to be elected, interpretation of some votes cast, errors in transcribing the data from vote registers, slowness in delivering results and the possibility of human errors in the counting of votes. Consequently to the above mentioned, the CNE decided that it was necessary to introduce automatic voting and counting processes. The implementation of a new computer voting system and the use of modern vote counting tools conveyed risks within the implementation and operation stages. Therefore, such implementation was programmed by stages with specialized area teams dully trained to take over project implementation.

The management team was formed with officials from the head office specialized in areas related to information, communication, finance, logistics, legal, administrative, training and electoral processes.

VII. Project's communicational dimension

A population study was carried-out in Azuay province as part of a communicational strategy. It was found that over 60% of Azuay inhabitants did not have a clear idea regarding the Electronic Voting, reason why we started an aggressive informative and training program. The campaign included visits to local communication media to spread communication products such as written newsletters, informative reports including audio interviews on the main activities undertaken by the election authorities and a monthly press conference on the progress of the project.

A massive campaign was launched in order to reach a large segment of the population. The campaign included radio, television, and print media with highly informative and emotive contents to inform people from Azuay regarding the electronic voting process. Once people were aware of the ELECTRONIC VOTING and its advantages, they rushed to the nearest training point in order to learn more about the new technology to be applied. They were also receptive to receive the training conducted at their workplaces.

The communication ELECTRONIC VOTE campaign was present on the main social networks used by people from Azuay, networks that spread positive messages on the project (always highlighting the benefits of using technology in favour of our democracy). The communications department received important feed back through this means, including many opinions issued by citizens. Additionally, the ELECTRONIC VOTE project included mobile training at a bus equipped with electronic voting machines that traveled all around the 15 cantons of the province of Azuay.

VIII. Strategies employed to promote the training process

It began with a socialization through two seminars on electoral processes that took place in the city of Cuenca with the participation of experts in the topic, experts such as Carlos María Ljubetic (Paraguay), Rui Santos (Portugal) and Amilcar Brunazo (Brazil). The workshops were aimed at the population in general and were attended by media, university representatives, representatives of the neighborhoods of Cuenca, provincial authorities and political organizations. These experts were able to share personal experiences in each of their countries.

Management of electronic voting developed the training plan that was launched in the province of Azuay. It is worth mentioning the training given to MJRV's (members of polling stations and actors involved in the event) on the management and operation of the Electronic Voting machine used in the electoral process of 23 February 2014.

Undoubtedly, we were aware on the importance of providing adequate training to voters (general public) on the voting machine.

Training started on October 1, 2013 with the first group of 100 trainers who received information about the e-voting process, voting machines, laws and hints on how to approach to people. Training to citizens started on October 15th with the 22 computers available at that time. Until 16th November 2013 a total of 100 equipments were available for the training events to citizens, including social, professional, corporate, institutional and the public in general.

In total we counted with the participation of some 200 trainers who toured throughout the province providing training at public and private companies, schools (to parents of students), universities, students from upper high school years, neighborhoods, rural communities, political organizations and at the most crowded places such as markets, parks, bus terminals, fairs and churches.

TABLE III. TRAINING

Inhabitants	Voters	% of registered voters	Number of trained citizens	Percentage of trainees
609.007	459.303	75,42%	367.441	80 %

Source: Delegation of Azuay province.

IX. SYNERGY BETWEEN TECHNOLOGY AND ELECTORAL MANAGEMENT

The Electronic Voting Project provided tools that facilitated interaction with the voting process, tools such as is the voting introduced in Azuay province on 11 December 2013, a tool that was available to citizens and political organizations at www.cne.gob.ec and www.cnezona4.ec. This tool allowed practices from home.

Functioning of the "QR Code" was explained to political organizations for them to keep quick records on the results obtained at polling stations in the province of Azuay, including details on the operation of the software's source code to allow political organizations to carry-out their own ballot counting.

Network

200 transmission links were installed with a bandwidth of 1Mbps, featuring transmission of coded information. Transmission in nationwide links reached 150 Mbps with optic fiber, which guaranteed a fast delivery of information to the ballot counting hub. XDSL technology was used in copper-based networks at rural areas. Wireless links (Radio) were established in areas lacking wire networks, as well as mobile suppliers working on 3G APN technologies. VSAT-satellite technology links were installed in areas with difficult geographical access.

X. AUDITING PROCESS: A WARRANTY OF TRANSPARENCY AND RELIABILITY

Four electronic voting audits were conducted in Azuay project. There, voters and political organizations were able to verify the results of the election process.

Audit of installation, voting and counting software - In this audit software installation, voting and counting were validated through observation, review of the application and generation of a hash code that ensures the integrity of the software used in voting and counting processes.

Audit database - This audit was performed to review the databases used as a repository of the information generated at every voting site and was used o generate the final results.

Audit of the scrutiny made at the Poll Station - This audit was conducted by the Electoral Provincial Board of Azuay and consisted of performing manual counting every vote for prefect and Vice-Prefect , Mayors, Urban - Rural Councillors and Members of the Rural Parish Boards. Once the votes counted , were compared with the results of the electronic totalizing system .

Audit of the totalization system - This audit was conducted by the Electoral Provincial Board and involved the processing of ballots for Prefect, Vice-Prefect, Mayors, Rural Councillors and Members of the Rural Parish Boards. The results were totalized and compared with the results of the electronic totalization.

XI. MUTUALITY BETWEEN THE ELECTRONIC VOTING PROJECT AND THE INCLUSION PROJECTS CENTERED AROUND HISTORICALLY EXCLUDED GROUPS.

As for the "Voting at Home" project, the National Electoral Council (CNE) developed a plan that allowed people with disabilities and older adults to vote at home by leveraging the portability of the electronic voting equipment. A database of persons with disabilities requiring special attention was elaborated before the elections. Prisoners at state jails in Azuay province were also able to vote thanks to the electronic voting machines with intelligent ballot.

XII. VARIABLES OF A COMPREHENSIVE ASSESSMENT

The following was obtained on 23 February 2014 at the Sectional Elections 2014:

1) Result reporting in less than two hours upon voting closure;
2) Reduction of absenteeism from 31.38% in 2009 to 24.80% in 2014;
3) Training given to more than 525,000 people (standing for 78% of voters).
4) Audit of 100% of voting registers and technical audits on pre-election, election and post-election phases.
5) 39 people suffering from disabilities voted at home.
6) 241 jail prisoners were given the right to vote (those who had not been sentenced).
7) Inter-cultural voting of indigenous people (in their native language).
8) Signing of the "Agreement for our Democracy and Transparency" supporting the electronic voting process (signed by political organizations participating in the electoral event).
9) Positive acknowledgements from observing missions that deem e-voting as an emblematic electoral project.

10) Permanent support given by people who became empowered of the E-voting project held in Azuay 2014.

XIII. Comparative Analysis of Participation from 2009 to 2014 (sample: province Prefect, Mayor)

The elections held on February 2014 showed an increasing participation of citizens. Comparing with the elections held in 2009, absenteeism fell from 31.38% to 25.21% in 2013 at province level, ending at 24.54% in the last elections held in February 2014. If you want to compare the amount of blank and null votes that were obtained from one election to another, it is necessary to compare two similar elections, 2009 being the last electoral process in which sectional authorities were elected. It is noteworthy that the electronic voting itself eliminates unintentional errors made by voters. It also eliminates the subjective interpretation of votes by polling station officials. Considering the results obtained in 2009 for province Prefect we can see that the number of blank votes in 2014 was smaller. A different behavior occurs in null ballots... there were fewer nulled ballots in 2014 than in 2009. (See comparison chart).

TABLE IV. Nulled Ballots 2009 – 2014 Prefect

	Election April 2009 – Prefect	Election february 2014 – Prefect
Population	551.291	609.007
Voters	378.423	459.303
Polling stations	2.319	2.163
Blank	44.041	34.716
Nulle	28.553	30.662
Total Blank and Nulle votes	72.594	65.378
Absenteeism	31.38%	24,58%

Regarding blank and null ballots for mayors, an increase in the number of blank votes was seen in 2014 compared to 2009 and a decrease of null votes from 2009 to 2014. The increase of blank and null votes from 2009 to 2014 is just 10.35 % despite the number of voters grew in that period by 16.69 %.

The total percentage of blank and null votes for Mayor with regard to the number of voters is 16.45% in 2009, whereas in 2014 such percentage dropped to 15.31 %. Participation level has also grown in Cuenca canton during the last election, going from 70.60 % in 2009 to 76.48 % this year.

TABLE V. Nulled Ballots 2009 – 2014 Mayor

‘	Election April 2009 – Mayor	Election february 2014 – Mayor
Voting sites	1.573	1.464
Voters	383.253	424.847
Persons who voted	270.682	324.918
Blank	16.044	27.016
Null	28.553	22.731
Total Blank and Nulle votes	44.597	49.747
Absenteeism	29.40%	23.52%

ANNEX. PERCEPTION OF VOTERS TOWARDS THE IMPLEMENTATION OF THE ELECTRONIC VOTING PROJECT IN AZUAY PROVINCE.

Methodology - The questionnaire was aimed at those voters who had just cast their electronic vote: A questionnaire was designed for the survey. The surveys were conducted at voting stations with the sample selected.

The questionnaire consisted of multiple choices (related to voters' socio-economic condition, variables concerning their confidence toward electronic voting, new voting technologies and scope of information campaigns and training conducted by the e-voting project weeks before the Election Day). Additionally, the questionnaire allowed respondent voters to recommend or suggest solutions to the problems derived from citizen's eagerness to know and improve the system for the next elections.

Sample design - The sample design was stratified, randomized and configured by county and urban area. Rural areas and voting sites according to the number of voters in the province of Azuay.

RESULTS FOR AZUAY PROVINCE

A total of 3,983 individuals were surveyed in Azuay province (distributed in 36 polling stations in urban and rural areas).

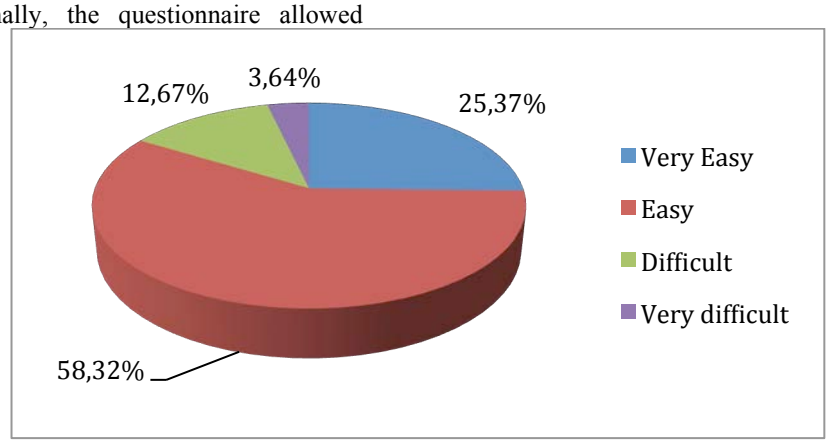


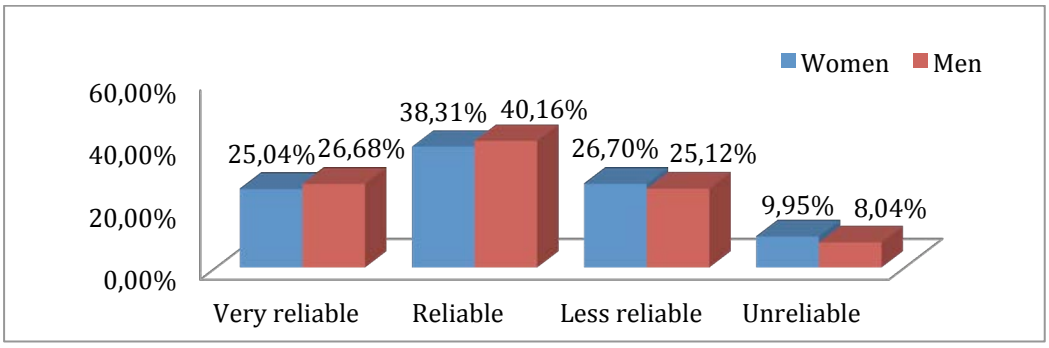
Fig. 2. Rating of Experience of Electronic Voting

1. *How do you qualify the experience of electronic voting in Azuay?*

This first rating evidence that the majority of voters surveyed (more than 80 %) felt that their experience to vote electronically was very easy or easy, which indicates a certain way that the electronic voting project Azuay was successful. Certainly, it is necessary to check that the components that formed each of the projects require adjustments, so that we can improve these processes in future projects. Below are the voters' perceptions of women and men separately.

TABLE VI. RATING OF THE EXPERIENCE OF ELECTRONIC VOTE BY SEX

AZUAY PROVINCE		
	Women	Men
Very reliable	25.04%	26.68%
Reliable	38.31%	40.16%
Less reliable	26.70%	25.12%
Unreliable	9.95%	8.04%



In conclusion it can be inferred that the fact of being a man or a woman does not affect the rating of the experience of the electronic vote; that is to say, the electronic vote was qualified in equal proportions by both voters and women voters by men.

Another key aspect of the research revolves around the voter confidence in front of the electronic voting system in Azuay. It is important to note that it is one thing that the voter has been found with a voting system friendly and easy to use; while another thing is that the voter qualifies as reliable or not the voting system as such. Hence the importance of understanding on the part of the voter, if despite having found an electronic voting system easy to use or not, the voter found reliable or not the voting system.

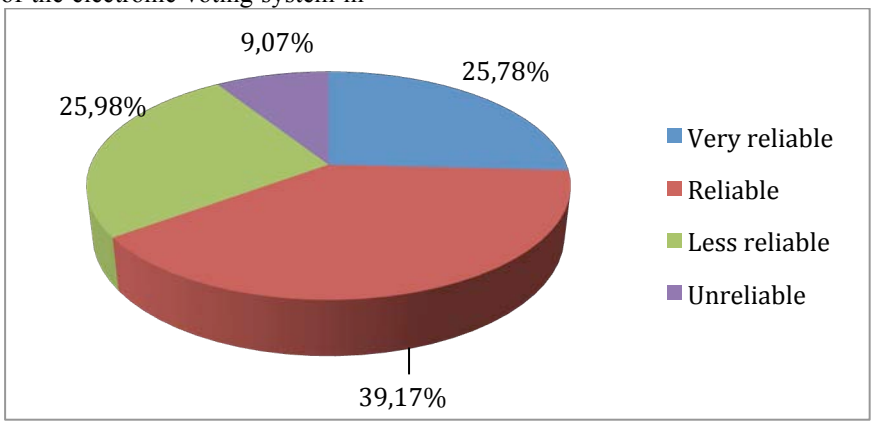
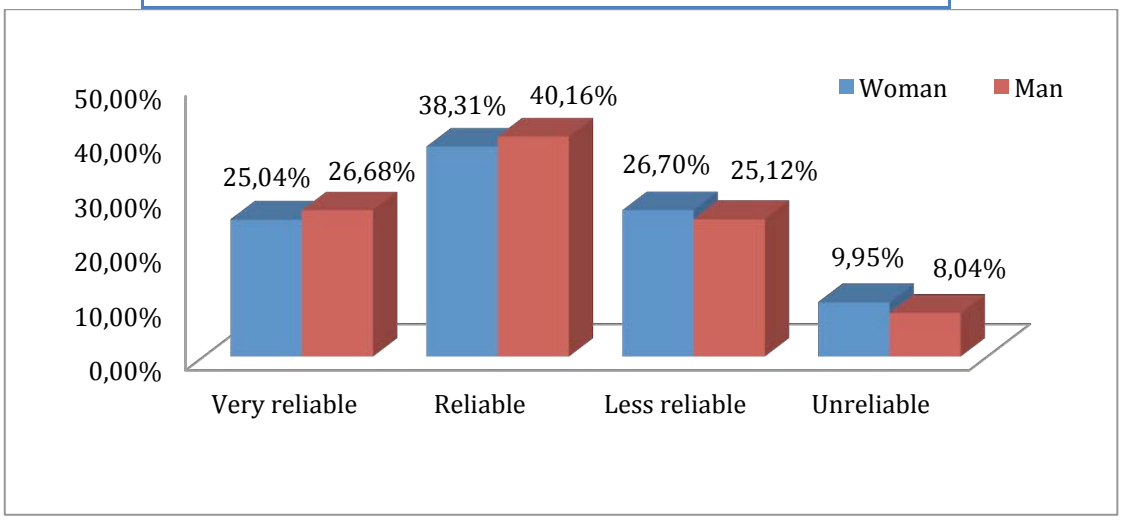


Fig. 3. Reliability in e-voting

At this point, the research i wanted to know the perception of voter with regard to this topic. The results reveal perceptions divided among voters who considered the system very reliable (25.78 %), reliable (no 39.17 %), unreliable (25.98 %) and nothing reliable (9.07 %).

TABLE VII. RELIABILITY IN E-VOTING

AZUAY PROVINCE		
	Women	Men
Very reliable	25.04%	26.68%
Reliable	38.31%	40.16%
Less reliable	26.70%	25.12%
Unreliable	9.95%	8.04%



2. *Are you willing to use this system for the upcoming elections?*

For the National Electoral Council is essential to know the opinion of citizens on whether voters would be willing to use the electronic voting system that were used in their respective provinces for the coming elections or not. Below are the results of this question along with the sex variable.

In general, eight out of ten people would be willing to vote using the electronic voting system that used the day of the election in their respective provinces. Similar results when viewed from the sex variable are presented below.

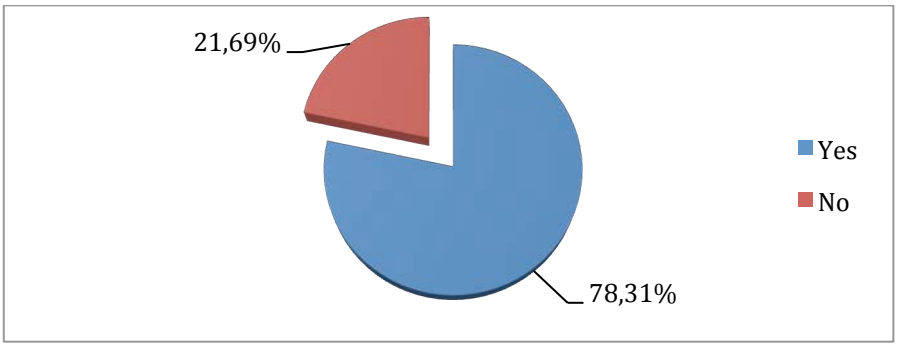
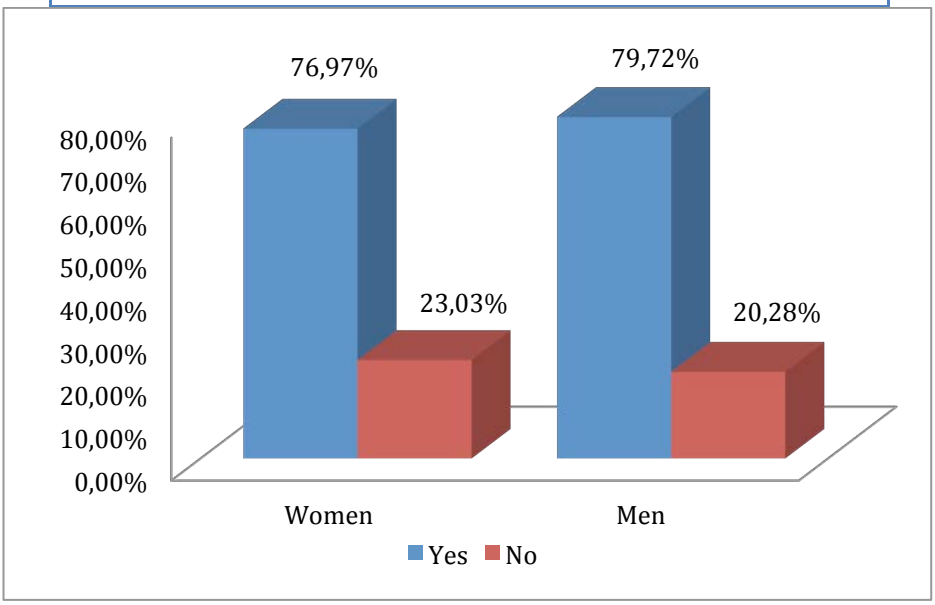


Fig. 4. Use or electronic voting in future electoral processes of the Azuay Province Reliability in electronic voting

TABLE VIII. USE OF ELECTRONIC VOTING IN THE UPCOMING ELECTIONS BY SEX

AZUAY PROVINCE		
	Women	**Men**
Yes	76.97%	79.72%
No	23.03%	20.28%

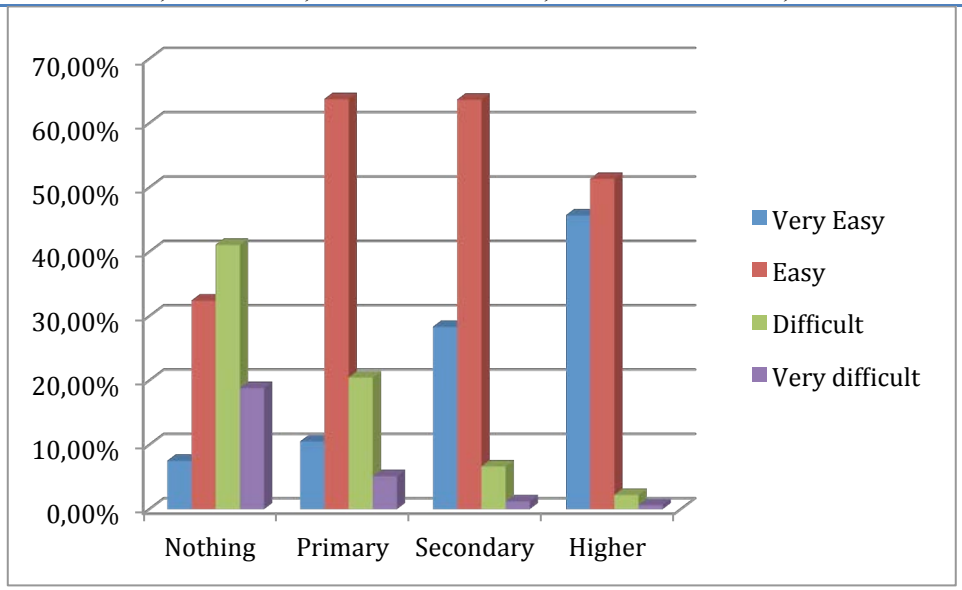


3. *Experience of electronic voting by level of education?*

In the following graphic shows how the voters felt the ease or not on the use of the voting machine depending on their level of education. In this way there is for example that a higher level of education, the easier it is considered the use of the machine.

TABLE IX. EXPERIENCE OF ELECTRONIC VOTING BY LEVEL OF EDUCATION

AZUAY PROVINCE				
	Nothing	Primary	Secondary	Highger
Very easy	7,55%	10,55%	28,38%	45,70%
Easy	32,45%	63,78%	63,69%	51,37%
Difficult	41,13%	20,50%	6,69%	2,25%
Very difficult	18,87%	5,16%	1,24%	0,68%

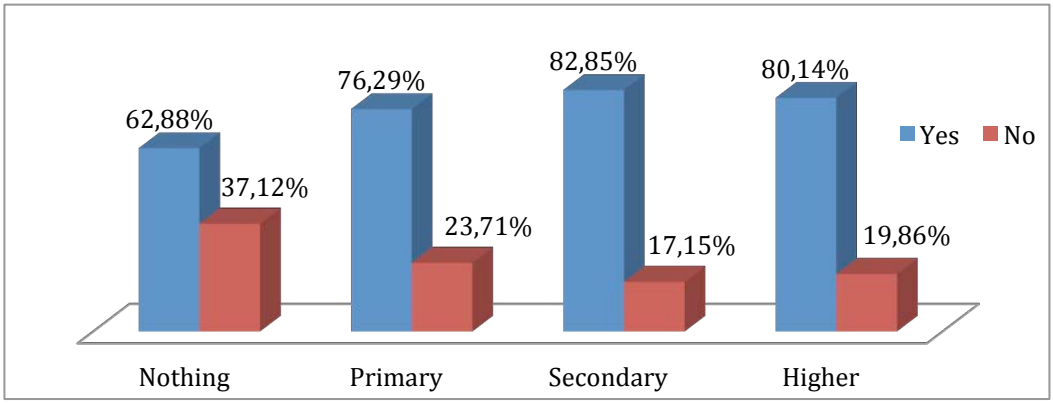


4. Confidence in the electronic voting systems by level of education?

The following graphs shows that the digital divide in terms of confidence is tied to the level of education of the electorate: the higher the level of education, the greater the confidence to the system. For the province of Azuay, the 80.14 % of people with higher education rely on the system:

TABLE X. CONFIDENCE TO THE SYSTEM ACCORDING TO LEVEL OF EDUCATION

AZUAY PROVINCE				
	Nothing	Primary	Secondary	Higher
Yes	62,88%	76,29%	82,85%	80,14%
No	37,12%	23,71%	17,15%	19,86%

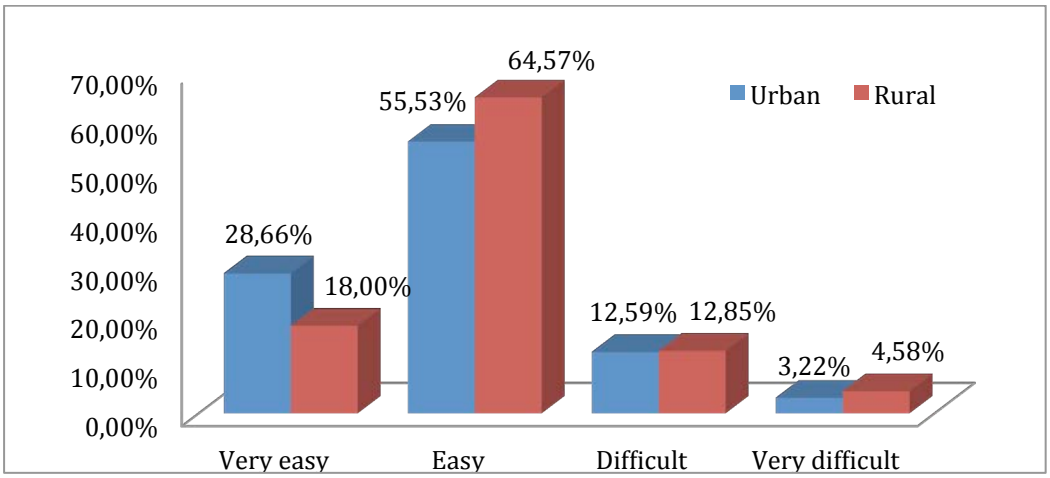


5. *Urban and rural behavior with regard to electronic voting in Azuay?*

It is important to know how the electorate of the urban and rural areas felt with regard to electronic voting. Below are results, considering primarily the variable ease of use of the machine and confidence to the system.

TABLE XI. RATING OF THE EXPERIENCE OF ELECTRONIC VOTING IN URBAN AND RURAL AREAS AZUAY

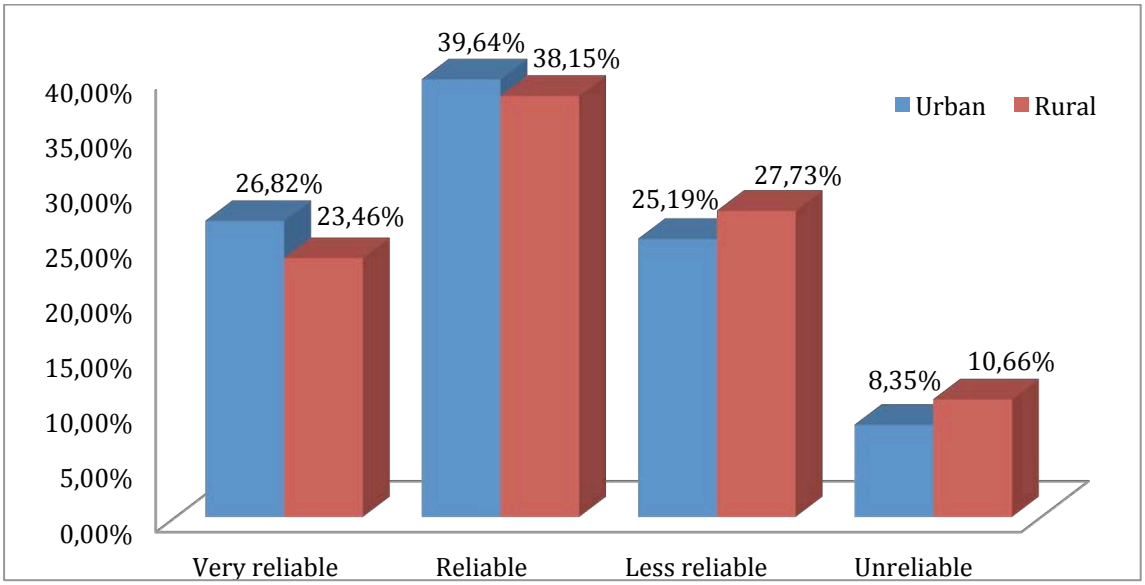
AZUAY PROVINCE				
	Very easy	Easy	Difficult	Very difficult
Urban	28,66%	55,53%	12,59%	3,22%
Rural	18,00%	64,57%	12,85%	4,58%



It can be seen that there is no significant relationship between urban or rural area and the qualification of the voter to the use of electronic voting machine. In other words, for both urban voters as to the rural was observed similar results. Below are the results based on the variable trust to the voting system.

TABLE XII. CONFIDENCE AS URBAN OR RURAL AREA

AZUAY PROVINCE				
	Very reliable	Reliable	Less Reliable	Unreliable
Urban	26,82%	39,64%	25,19%	8,35%
Rural	23,46%	38,15%	27,73%	10,66%



It should be noted that for both the variable ease of use of the machine as to the variable trust the electronic voting system, urban areas have a considerable increase on the rural areas with regard to the ease of use and the confidence to the system. On the other hand, rural areas manifested in greater numbers than urban areas, that the use of the machine is not easy and that the voting system is not reliable. These answers may have its origin in the level of education of the voters polled.

Practicality of Technical Solutions

Efficient End to End Verifiable Electronic Voting Employing Split Value Representations

Michael O. Rabin
Harvard SEAS
Columbia SEAS
Email: morabin@gmail.com

Ronald L. Rivest
MIT CSAIL
Cambridge, MA 02139
Email: rivest@mit.edu

***Abstract*—We present a simple and fast method for conducting end to end voting and allowing public verification of correctness of the announced vote tallying results. In the present note voter privacy protection is achieved by use of a simple form of distributing the tallying of votes and creation of a verifiable proof of correctness amongst several servers, combined with random representations of integers as sums mod M of two values. At the end of vote tallying process, random permutations of the cast votes are publicly posted in the clear, without identification of voters or ballot ids. Thus vote counting and assurance of correct form of cast votes are directly available. Also, a proof of the claim that the revealed votes are a permutation of the concealed cast votes is publicly posted and verifiable by any interested party. We present two versions of the method, one assuring voter privacy and proof of correctness in the presence of information leaking devices, the other achieving the same goals as well as prevention of denial of service by failing or sabotaged devices.**

Advantages of this method are: Easy understandability by non-cryptographers, implementers, and ease of use by voters and election officials. Direct handling of complicated ballot forms. Independence from any specialized cryptographic primitives. Verifiable mix nets without using public-key or homomorphic cryptography, a novel result of significance beyond e-voting. Speed of vote-tallying and correctness proving: elections involving a million voters can be tallied and proof of correctness of results posted within a few minutes.

I. Introduction and Overview

End-to-End Verifiable Voting (E2EVV) systems provide high confidence that errors and fraud can be detected and that the announced election outcome is correct. See [1]–[5] for some surveys and results about E2EVV. Cramer et al. [6] have also used secret-sharing to ensure robustness of a voting system, as we do in Section X. Recently, E2EVV systems have been used in actual elections [2] and are proposed for use in new systems such as the STAR-Vote system in in Travis County (Austin) Texas [7].

The parties and agents involved in our E2EVV scenario are:

Voters: We assume n voters V_1, V_2, ..., V_n.

Tablets: Each voter uses a tablet to compose her vote. The tablet can also print out a receipt for the voter.

Election authorities: Individuals responsible for running the election.

Election Servers: Computers performing specific functions in the election.

Secure Bulletin Board (SBB): An election server providing a secure public append-only record of election-specific data, including all cast ballots, the final election outcome, and a proof of correctness of the election outcome.

Proof Server: An election server that produces a proof of correctness of the election outcome. In our method, the proof server is implemented with a two-dimensional array of independently-controlled computers; these servers are also servers in our mix-net implementation (so we also call them "mix-servers").

Tally Server: An election server that computes the election outcome from the publicly posted list of decrypted cast votes.

Adversary: The adversary attempts to cause an incorrect election outcome to be accepted. (An accepted proof of correctness as presented here, assures correctness of announced tally outcome no matter how the adversary acted.) An adversary may also attempt to violate the privacy of voters.

An election then comprises the following steps:

1) **Setup:** The list of eligible voters is determined. The list of ballot questions is determined. (For presentation purposes we assume only one question on the ballot, which may nonetheless require a complex answer such as a preference ordering of the choices. For more questions the entire method may be repeated.) Cryptographic keys are set up as necessary for tablets and election servers.
2) **Vote Casting:** Each voter uses a tablet to enter her choice on the ballot question. The system uses some convention for providing each ballot with a unique ballot id bid. The choice is "encrypted" (more on that later), and sent to the election servers with the bid. The voter is given a printed receipt with the bid and the hash of the encryption.
3) **Posting of Vote Records:** The bid's and encrypted choices are posted on the SBB at the end of election day.
4) **Verification of Postings:** Voters may access the SBB to verify that the encryptions of their choices are correctly posted (comparing their receipt with the hash of the posted encryption for their ballot).
5) **Mixing:** The mix servers anonymize the encrypted ballots by permuting their order and dissociating the encrypted ballots from identifying meta-data such as voter names or bid's. Each of $2m$ copies of the list

of n encrypted ballots is independently mixed and re-encrypted. The resulting $2m$ permuted lists are posted on the SBB.

6) **Random Challenge:** A "random challenge" (a long string of random digits) is derived by hashing the SBB contents and/or from a public dice-rolling ceremony. The unpredictability of this challenge to an adversary prevents the adversary from undetectably manipulating the election outcome.
7) **Proving consistency with cast votes:** A random half (determined by the random challenge) of the $2m$ lists of encrypted ballots are partially decrypted, to check that the mixing was properly done. The method used here depends on properties of split-value vote representations to ensure that voter privacy is preserved. The partial decryptions are posted on the SBB for all to confirm.
8) **Posting and verification of election outcome:** The other half of the $2m$ lists are all fully decrypted and posted on the SBB. Anyone may check that they are identical lists (albeit differently permuted). The final election outcome may be determined from any one of these lists.

Adversarial model. We assume that the adversary is trying to "rig" an election by trying to force an incorrect election outcome to be accepted (because it appears to have been proven correct) or to learn how some particular voters have voted.

In Sections III–IX the adversary is assumed *not* to be interested in causing the election to fail (that is, to not produce an election outcome or proof of correctness at all). Section X deals with adversaries who attempt to deny service by failing.

Innovations re other E2E methods. The elements of our end-to-end voting method are reasonably standard, except that

- Ballots are "encrypted" in a novel manner, using commitments to secret-shared split-value representations of the voters' choices.
- No modular exponentiations or public-key operations are required, yielding substantial efficiency improvements.
- The mix-net operation is proved correct in a new manner: rather than proving each step of the mix-net to be correct, the overall operation is proved correct.
- Because ballots are fully decrypted for the final tallying operation, there is no restriction on the tallying method used. Complex tallying rules (e.g. IRV) and write-in candidates are easily handled. Furthermore, no zero-knowledge proofs are required that the encrypted ballots are valid.

We thus show how using Rabin's Split Value Representation (SVR) of integers method greatly simplifies an E2E implementation. SVR methods have been proposed for implementation of secure auctions [8], [9]; the extension to voting involves, however, further innovations.

The current paper extends our previous works [10], [11] exploring such innovations; In particular, we note that our earlier work [10] has the problem that a single election server must know how everyone voted; the present work remedies that defect.

Outline of paper. We begin in Section II with some preliminary notation and a discussion of the properties of split-value representations, including methods for securely proving equality of the values represented.

Then Sections III–IX discuss each phase of our method in detail, from initial setup to creating and verifying the final proof of correctness of the election outcome.

Section X shows how to extend the basic method to one that tolerates a certain number of failures of the mix-net servers, by using Shamir's secret-sharing method.

Finally, Section XI provides some discussion of the practical aspects of our methods, and Section XII concludes.

II. Preliminaries

A. Notation

We let $x \parallel y$ denote the concatenation of x and y.

B. Representations modulo M

For a given race, votes and values used in the system are described by values modulo a given integer M. Here M is chosen large enough so that any voter choice (including a "write-in" choice) may be represented by a unique integer modulo M. In the following, additions and subtractions of values are performed mod M.

Our methods are independent of the way such values are used to represent candidates or complex choices (as with preferential balloting).

Some of our methods (see Section X) require that M be prime.

C. Split-Value Representations

Our methods are adapted from those of [8], [9].

Definition 1: Let x be a value modulo M, so that $0 \le x < M$. A *split value representation* of x is any vector

$$X = (u, v)$$

where u and v are values modulo M such that $x = u + v \pmod M$.

Definition 2: We define the *value* of a split-value representation $X = (u, v)$ modulo M to be

$$\textsc{Val}(X) = (u + v) \bmod M \ .$$

Note that there are M different split-value representations of any given value x, since u can be arbitrarily chosen from $\{0, 1, \ldots, M-1\}$, and then the corresponding v derived via $v = (x - u) \bmod M$.

Definition 3: A *random split-value representation* of a value x modulo M is a randomly chosen split-value representation of x modulo M.

D. Commitments

Commitment to values mod M We use a commitment function $\text{COM}(K, u)$ employing a (randomly chosen) key K to commit to value u modulo M.

It is assumed that COM is computationally hiding: given the value $C = \text{COM}(K, u)$, it is infeasible to gain any information about u.

Opening a commitment $\text{COM}(K, u)$ means to reveal K and u; this opening can be verified by re-computing $\text{COM}(K, u)$.

It also assumed that it is computationally infeasible to find two pairs (K, u) and (K', u') such that $\text{COM}(K, u) = \text{COM}(K', u')$. This renders the commitment by COM to be computationally binding; no one can open a commitment in more than one way.

COM can be implemented, say, by use of AES with 256 bit keys, or with the HMAC cryptographic hash function.

We sometimes write $\text{COM}(u)$ instead of $\text{COM}(K, u)$, with the understanding that a randomly chosen K is used (which is revealed with u when the commitment is opened).

Commitment to split-value representations

Our use of a commitment to a split-value representation is analogous to the "encryption" of a choice in other E2E methods.

Definition 4: A *commitment* $\text{COMSV}(X)$ *to a split-value representation* $X = (u, v)$ is a pair of commitments, one to each component:

$$\text{COMSV}(X) = (\text{COM}(u), \text{COM}(v)) \ .$$

Note that $\text{COMSV}(X)$ denotes commitment to a split-value vector representation of a value x, $0 \leq x < M$, while $\text{COM}(u)$ is a commitment to a value u, $0 \leq u < M$.

The following fact is crucial to the security of our methods.
Fact. If just one of the two coordinates u or v in a commitment to a random split value representation X of a value x is opened, then no information about the value x is revealed.

E. Proving equality of commitments

The nice thing about commitments to split-value representations is that they can be (probabilistically) proved equal without revealing the values represented.

Suppose a Prover asserts that

$$\begin{aligned} \text{COMSV}(X) &= (\text{COM}(u_1), \text{COM}(v_1)) \\ \text{COMSV}(Y) &= (\text{COM}(u_2), \text{COM}(v_2)) \end{aligned}$$

represent the same value: $\text{VAL}(X) = \text{VAL}(Y)$. To prove this, the Prover first reveals t, where

$$t = u_2 - u_1 \pmod{M} \text{ and} \quad (1)$$
$$t = v_1 - v_2 \pmod{M} \quad (2)$$

The Verifier then picks a random value $c \in \{1, 2\}$; if $c = 1$ he asks the Prover to open $\text{COM}(u_1)$ and $\text{COM}(u_2)$. Otherwise, the Prover must open $\text{COM}(v_1)$ and $\text{COM}(v_2)$. The Verifier correspondingly checks (1) or (2). The Prover fails if the checked equation fails.

Fact. If $\text{VAL}(X) \neq \text{VAL}(Y)$, then the Prover fails with probability at least 1/2.

It is very important that a given split-value commitment should not participate in more than one such proof. Otherwise both its components may be revealed, thus revealing the value represented.

Generalization to tuples We use a generalization of the above proof method, wherein X is replaced by a tuple X_1, X_2, X_3 such that $\text{VAL}(X) = \text{VAL}(X_1) + \text{VAL}(X_2) + \text{VAL}(X_3)$, and similarly for Y and Y_1, Y_2, Y_3. (This is for our default three-row proof server arrangement; more values are used if there are more rows.)

A proof of the equality that

$$\text{VAL}(X_1) + \text{VAL}(X_2) + \text{VAL}(X_3) = \\ \text{VAL}(Y_1) + \text{VAL}(Y_2) + \text{VAL}(Y_3)$$

proceeds just as before, except that opening the first component of X is replaced by opening the first component of each of X_1, X_2, and X_3, and opening the second component of X is replaced by opening the second component of X_1, X_2, and X_3; similarly for Y. Again a value t such that $X_1 + X_2 + X_3 = Y_1 + Y_2 + Y_3 + (-t, t)$ is posted by the Prover.

The basic fact (that a cheating Prover is unmasked with probability at least 1/2) remains true.

F. Proving Equality of Arrays of Vote Values

We further generalize such proofs of equality to proofs of equality for lists of length n of commitments to vote values.

In our mechanism votes are represented by triplets $T = (X, Y, Z)$ and committed to as

$$\text{COMT}(T) = (\text{COMSV}(X), \text{COMSV}(Y), \text{COMSV}(Z)) \ .$$

By definition,

$$\text{VAL}(T) = (\text{VAL}(X) + \text{VAL}(Y) + \text{VAL}(Z)) \bmod M \ .$$

Assume that a Prover has posted in a SBB two arrays of commitments to triplet representations of values:

$$\text{COMT}(T_1), \text{COMT}(T_2), ..., \text{COMT}(T_n)$$
$$\text{COMT}(T'_1), \text{COMT}(T'_2), ..., \text{COMT}(T'_n).$$

The Prover claims that $\text{VAL}(T_j) = \text{VAL}(T'_j)$ for $1 \leq j \leq n$.

To post a proof of correctness on the SBB, the Prover posts the values $t_1, \ldots, t_n$ required for proving the claimed equalities.

Afterwards, employing appropriate randomness (see Section VIII), n random independent values $c_j \in \{1, 2\}$, $1 \leq j \leq n$, are computed and posted by the Verifier.

Now the Prover constructs and posts a corresponding proof for each claimed equality $\text{VAL}(T_j) = \text{VAL}(T'_j)$, $1 \leq j \leq n$, which can be verified as shown above.

Theorem 1: If more than k of the claimed n value equalities are false then the probability of acceptance of the claim is at most $(1/2)^k$.

Proof: If for an index j, $\text{VAL}(T_j) \neq \text{VAL}(T'_j)$, then the probability of the inequality not being uncovered is at most $1/2$. Because of the independent random choice of the challenges $c_j \in \{1,2\}$, $1 \leq j \leq n$, the probability of not uncovering at least one of the k inequalities is most $(1/2)^k$. ■

This completes our review of the mathematical preliminaries needed for our methods.

III. SETUP

We now begin our more detailed description of our method, beginning in this Section with the Setup phase.

See Figure 1 for a graphic depiction of the overall method.

A. Choice of M

We assume that there is only one race in the election. (The entire method can be replicated for additional races.)

A value of M is chosen so that each possible choice a voter can make in this race (including write-in votes, if allowed), may be uniquely represented as a value w, where $0 \leq w < M$.

If the extensions of Section X are used that use Shamir's secret-sharing method [12] to handle failing servers, then M should be prime.

B. Tablets and Servers

The voter casts her vote in a voting booth by use of a Tablet. Multiple voters may vote on a single Tablet. A representation of the vote is transferred as described below from the Tablet to various to election servers.

Some of the servers are "mix servers" that anonymize the vote by removing identifying information and shuffling them according to a secret permutation.

The mix servers also act collectively as a "proof server" (PS) that prepares a publicly verifiable proof of the correctness of the election results.

The proof of correctness will be publicly posted by the PS on an electronic Secure Bulletin Board (SBB) accessible to voters, parties involved in the election, and the general public.

In this note, to achieve high assurance of voter privacy the PS consists of nine independent devices $P_{1,j}$, $P_{2,j}$, $P_{3,j}$, $j = 1, 2, 3$ (considered as three rows of three devices each).

It will be demonstrated that as long as no more than two devices may leak out information, privacy of voters is protected. Generalizations for other parameterizations will be described later. The obvious generalization to the case of ℓ leaky devices employs $(\ell + 1)^2$ devices.

C. Secure Channels

We assume that suitable arrangements are made for secure channels between the tablets and the election servers.

For example, one may use three pairs (e_j, d_j) of a public-key encryption method (PKE), for $j = 1, 2, 3$. Here e_j is a public encryption key, and d_j is the corresponding secret decryption key. Every voter Tablet has all public encryption keys e_j, $j = 1, 2, 3$. Every $P_{j,1}$ has the secret decryption key d_j .

However, in such an implementation, the public-key decryption may become an overall computational bottleneck. Thus, we recommend using a simple hybrid encryption method to set up private symmetric keys, employing only one PKE encryption key per tablet and the corresponding PKE decryption key by the Proof Server per Tablet. This reduces the overall PKE decryption time significantly.

Each proof server also has secure channels to every other proof server in the same row or column.

IV. VOTE CASTING

We assume that the Voter's Tablet is given (or creates) a unique ballot id bid for each voter.

The Voter's Tablet takes the Voter's V vote w, where $0 \leq w < M$, and randomly represents w as a triple (x, y, z) such that

$$w = (x + y + z) \bmod M \ .$$

It then creates random split-value representations of x, y, and z as $X = (u_1, v_1)$, $Y = (u_2, v_2)$, and $Z = (u_3, v_3)$. Tablet chooses for X random keys K_1, K_2 and sends to $P_{1,1}$ the ballot representation:

$$bid, \text{COMSV}(X), PKE(e_1, (K_1, u_1) \parallel (K_2, v_1)))$$

where

$$\text{COMSV}(X) = (\text{COM}(K_1, u_1), \text{COM}(K_2, v_1)).$$

Similarly a message containing $\text{COMSV}(Y)$ is sent to $P_{2,1}$ and a message containing $\text{COMSV}(Z)$ is sent to $P_{3,1}$, using different pairs of random keys for each commitment, and using e_2 for encryption for $P_{2,1}$, and e_3 for encryption for $P_{3,1}$. In this way the Tablet sends to the first device in each row a portion of a distributed representation of vote w (each portion being a commitment to a split-value representation of a component of w, where the components add up modulo M to w).

The use of the above split value representations X, Y, Z, for x, y, z, is one of the main innovations of this paper. It is used in creating the publicly verifiable proof of correctness of the submitted votes and of the tally of the election.

As part vote-casting, the voter may participate in a "*cast-or-challenge*" protocol see Benaloh [13] to verify that her Tablet has faithfully represented her choice(s). We omit details.

V. POSTING OF VOTE RECORDS

In E2EVV each ballot is encrypted and posted on a secure public append-only Bulletin Board (SBB) [14].

All encrypted ballot information received from Tablets is publicly posted on the public Secure Bulletin Board, so that voters may confirm their correct reception. To simplify procedures, a voter is given on her receipt the ballot id bid of her vote, and the postings may be in order of ballot id.

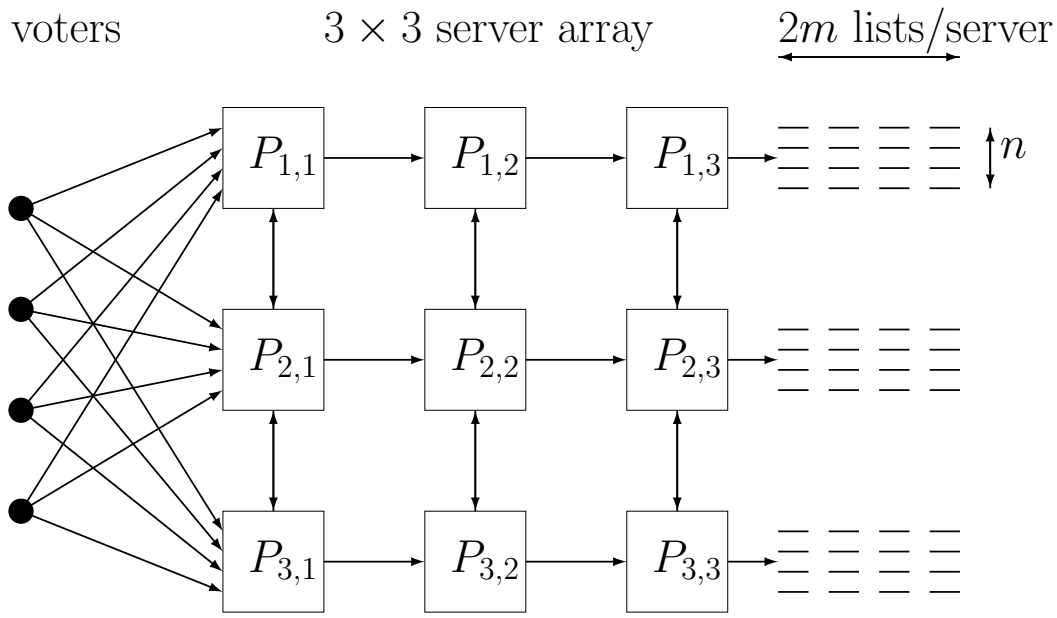


Fig. 1. An illustration of the method for $n = 4$ voters. Information flows from left to right. Each voter sends an encrypted share of his vote to each of the servers in the first column; these encrypted shares are also posted on a secure bulletin board. Each column obfuscates and reshuffles its data (each server in a column using the same random permutation) before sending it on to the next column. The information flow from the first column to the output is repeated $2m = 4$ times (with different randomness used each time). A "cut-and-choose" method randomly selects m columns of output lists to be re-routed back to be compared for consistency with the input. The other m columns are opened, checked for consistency, and posted to reveal the election outcome. A proof of the correctness of the election outcome is then prepared and posted, as described in the text.

VI. Verification of Postings

The voter was given a paper receipt from the Tablet giving a hash value of what should be posted, to enable simple verification of correct inclusion of her ballot.

Every voter can then verify that the cipher text of her ballot has been properly posted, this without her being able to convince anybody what her actual vote was. (The voter does not know how to open any commitments.)

VII. Mixing

The implementation of a fast verifiable mix-net, described in this Section, is one of the main contributions of this paper.

We emphasize that the required computational primitives are just additions mod M of integers of value at most M, and concealment of integers u of size at most M as $\textsc{Com}(K, u)$ by a fast commitment function $\textsc{Com}(\cdot, \cdot)$. These primitives are done on individual proof servers $P_{i,j}$, not in a multi-party fashion, and are executable on ordinary laptop or desktop computers at the rate of millions of operations per second.

Our mix-net, consisting of $P_{1,j}$, $P_{2,j}$, $P_{3,j}$, $j = 1, 2, 3$, creates and publicly posts $2m$ arrays of length n, each of which is a secret random permutation of the (encrypted) votes $w_1, \ldots, w_n$.

Why are $2m$ permuted lists produced, instead of a single one, as is usual for mix-nets? The answer is that we need half of them to check against the posted inputs, and half to produce the desired election outcome. Because no split-value commitment can be compared for equality more than once, we need multiple copies to make this approach work out.

The actual number $2m$ used depends on the degree of correctness assurance the system is designed to achieve; Theorem 3 in Section IX shows that $2m = 24$ provides high assurance.

Decryption. To begin, $P_{1,1}$, $P_{2,1}$, $P_{3,1}$, each using its private decryption key, opens its received commitments.

The Proof Server PS device $P_{1,1}$ has the secret decryption key d_1. It decrypts for each Ballot component X the $PKE(e_j, (K_1, u_1) \parallel (K_2, v_1))$ part. The revealed values (K_1, u_1), (K_2, v_1) are checked as the correct opening of $\textsc{ComSV}(X)$, enabling $P_{1,1}$ computes $\textsc{Val}(X) = x = (u_1 + v_1) \bmod M$.

Now $P_{1,1}$ has the sequence of X-components $x_1, \ldots, x_n$ of the n vote values $w_1, w_2, \ldots, w_n$.

Similarly $P_{2,1}$ computes $y_1, \ldots, y_n$ and $P_{3,1}$ computes $z_1, \ldots, z_n$. Here the first vote is $w_1 = (x_1 + y_1 + z_1) \bmod M$.

Even though first-column devices now have components in the clear, the distribution of a vote value w as the sum mod M of x, y and z and sending each component to a different $P_{j,1}$, $j = 1, 2, 3$, ensures that if at most two devices are leaky, the vote remains secret.

First column obfuscates and shuffles. To create an output array consisting of the n vote values concealed and randomly permuted, the servers $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ comprising the first column of the PS first *obfuscate* and then *shuffle* the list of n vote values, before passing them on to the next column.

Obfuscating: The first-column proof servers create an *obfuscation* of the list of n vote values.

Definition 5: We say that $S'_1 = (x'_1, y'_1, z'_1)$ is an *obfuscated form* of $S_1 = (x_1, y_1, z_1)$ if

$$x'_1 + y'_1 + z'_1 = x_1 + y_1 + z_1 \pmod M ,$$

that is, if S'_1 and S_1 represent the same value.

The method for $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ to obfuscate the first vote value (represented as a triple $S_1 = (x_1, y_1, z_1)$ in the three servers) is to chose three random values p_1, q_1, r_1 in the range 0 to $M - 1$, subject to $(p_1 + q_1 + r_1) \bmod M = 0$ and to compute $x'_1 = (p_1 + x_1) \bmod M$ by $P_{1,1}$, etc. Similar obfuscation is done on the components of the other $n-1$ votes w_2 , ..., w_n using different randomly chosen triplets p_j, q_j, r_j for each obfuscation.

Shuffling: $P_{1,1}$ has now the values x'_1 , ..., x'_n, $P_{2,1}$ has the values y'_1, ..., y'_n and similarly for $P_{3,1}$. Now $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ together choose a random permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Send data to next column. Then $P_{1,1}$ transmits the array $x'_{\pi(1)}, \ldots, x'_{\pi(n)}$, to $P_{1,2}$. Similarly $P_{2,1}$ transmits the array $y'_{\pi(1)}, \ldots, y'_{\pi(n)}$, to $P_{2,2}$ and $P_{3,1}$ transmits the array $z'_{\pi(1)}, \ldots, z'_{\pi(n)}$, to $P_{3,2}$.

Second column obfuscates and shuffles. The second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, repeats the same process of obfuscation and shuffling, sending the obfuscated-shuffled array to the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$.

Last column obfuscates and shuffles. Finally, $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ again obfuscate and shuffle so that $P_{1,3}$ has the array $(x'''_{\sigma(1)}, \ldots, x'''_{\sigma(n)})$. Similarly for $P_{2,3}$ and the array $(y'''_{\sigma(1)}, \ldots, y'''_{\sigma(n)})$ and for $P_{3,3}$. Here σ denotes the permutation of the original order of the ballots into the present arrays.

Posted of lists of votes. Server $P_{1,3}$ creates and posts on the SBB commitments $(\text{COMSV}(X'''_{\sigma(1)}), \ldots, \text{COMSV}(X'''_{\sigma(n)}))$ to split-value representations of the components $(x'''_{\sigma(1)}, \ldots, x'''_{\sigma(n)})$. Similarly, $P_{2,3}$ creates and posts $(\text{COMSV}(Y'''_{\sigma(1)}), \ldots, \text{COMSV}(Y'''_{\sigma(n)}))$ and so does $P_{3,3}$.

This total posted array of $3n$ commitments is one of the $2m$ lists produced by the mix-net; the whole process is repeated $2m$ times to obtain the set of all $2m$ lists.

Remark. Note that in our method of shuffling, unlike in mix-nets, components of votes are not shuffled amongst rows going from one column to the next. They rather stay within the same row obfuscated and in shuffled order.

Theorem 2: **(Maintenance of Voter Privacy.)** As long as no more than two of the nine servers $P_{i,j}$ leak out unintended data, there are at least one row and one column in the 3×3 array of servers $P_{i,j}$ that do not contain an improper server. This, combined with the obfuscation and shuffling from one column of servers to the next and the final obfuscation and shuffling by the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ of servers, results in complete secrecy of votes by individual voters, even if the above output arrays of $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ are made public and two servers of the PS leak out all their data.

We shall prove this theorem following the next remark. It is assumed that the communications between any two mix servers is secure.

Remark. If computations were properly done, then $(x'''_{\sigma(1)} + y'''_{\sigma(1)} + z'''_{\sigma(1)}) \bmod M = w_{\sigma(1)}$, etc. That is, from the output arrays of $P_{1,3}$, $P_{2,3}$, $P_{3,3}$, the votes $w_1, \ldots, w_n$ can be directly read off (in the order σ).

Proof: In first phase of obfuscation and shuffling going from the first column $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ to the second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, obfuscating a typical $S_1 = (x_1, y_1, z_1)$ into $S'_1 = (x'_1, y'_1, z'_1)$ by use of p_1, q_1, r_1. Note that $P_{1,1}$ keeps x_1 and x'_1 in its own memory. Similarly for $P_{2,1}$, $P_{3,1}$ and their components of S_1 and S'_1.

This implies that even though p_1, q_1, r_1 are known to all three of $P_{1,1}$, $P_{2,1}$, $P_{3,1}$, nothing is revealed about components of votes stored in non-leaky devices.

The same holds about obfuscation and shuffling going from the second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$ to the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$.

Once the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ is reached either it or one of the two preceding columns do not contain any leaky device. Thus third-column outputs protect voter privacy. ■

VIII. RANDOM CHALLENGE

We note that the proof servers have a need for random values of two distinct flavors:

- *Internal randomness.* The PS needs random values to create random split-value representations random permutations, etc. These values should be unpredictable to outsiders, but need not be unpredictable to the proof servers themselves. For these purposes, the proof servers may use what we call "internal randomness": truly random sources available only to each proof server.
- *External randomness (for challenges).* The proofs of correctness need random challenges (e.g. for the cut-and-choose of m lists out of $2m$, or for the proofs of equality of split-value commitments) that are unpredictable even to the proof servers (as they may be malicious). These random challenges may be obtained in either of two ways: in the Fiat-Shamir style [15] as the hash of the current SBB, or from a random external source (e.g. a dice-rolling ceremony). The former approach has the advantage that the (pseudo-)random values obtained by hashing the SBB

may be verified by anyone, but has the disadvantage that an evil proof server may try many values to be posted on the SBB until the SBB hash is to its liking. Thus, the value of $2m$ may need to be significantly larger if the Fiat-Shamir method is used. Our analyses assume that the challenges are derived from a truly random external source; appropriate adjustments to the value of $2m$ should be applied if the Fiat-Shamir method is used.

IX. Proof of Correctness

The election outcome and associated tally, as well as a proof of correctness of the announced results, are also posted on the SBB, and can be verified by anyone.

Posting of split-value representations of mix-net outputs. The device $P_{1,3}$ creates random split-value vector representations $X'''_{\sigma(i)}$ for $x_{\sigma(i)}$, $1 \leq i \leq n$, and commitments $\text{ComSV}(X'''_{\sigma(i)})$ for $1 \leq i \leq n$. Similarly for $P_{2,3}$ with the $y'''_{\sigma(i)}$, and $P_{3,3}$ with the $z'''_{\sigma(i)}$.

Using the notation of Section II-F $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ together prepare and publicly post for $1 \leq i \leq n$:

$$\text{ComT}(T_{\sigma(i)}) = (\text{ComSV}(X'''_{\sigma(i)}), \text{ComSV}(Y'''_{\sigma(i)}), \text{ComSV}(Z'''_{\sigma(i)})) \quad (3)$$

This process of obfuscation, shuffling and posting an array of the form (3) is repeated by the PS $2m$ times, where $2m$ is chosen to yield the desired assurance of correctness. Each of these posted arrays is of course created by use of a different permutation of $\{1, \ldots, n\}$.

Cut and Choose. By use of randomness extracted from all posted data together with an independent random seed, m of the posted lists (3) are randomly chosen for a proof of value-consistency with the posted concealed votes (see Introduction).

Proving consistency with cast votes: Each of these m chosen arrays (3) is rearranged by the Proof Server in the order of of bids, hence in the order of the submitted-posted concealed ballots. This is done by backtracking for the chosen arrays, the permutations used by each column.

The permutations σ for the m chosen arrays are posted, as are the values $(t_i, -t_i)$ used in the proof. For brevity we omit the simple details of how $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ compute and post the pairs $(t_i, -t_i)$, $1 \leq i \leq n$.

Now the randomness is used to open one coordinate in each of the commitments in the posted concealed ballots and the corresponding commitment in each of the m rearranged arrays (3) and prove equality of values by the method of Section II-F.

By Theorem 1, if even one of these m lists differs from the ballot list by more than k values then the probability of acceptance is at most $(1/2)^k$.

Posting and verification of the election outcome: Now all the other m permuted lists are opened and the values are revealed. Only if all opened lists are permutations of the same values is the proof of correctness accepted. The election outcome is then the result of applying the appropriate tallying function or election outcome determination function to any of the opened lists. (We assume that the election outcome does not depend on the order of the ballots.)

Level of assurance provided. We now analyze the level of assurance provided by the posted proof.

Definition 6: Call a permuted array of n values *k-good* if when re-arranged in the order of the originally concealed n ballots posted by the tablets on the PS, it differs from the concealed ballot values in fewer than k locations.

Theorem 3: The probability that the opened arrays (3) are permutations of the same values but they are not k-good, i.e. the probability of accepting an announced tally result differing from the correct tally by more than k vote values is at most

$$1/C(2m, m) + (1/2)^k \approx \sqrt{3.14m}/2^{2m} + (1/2)^k,$$

where $C(2m, m)$ is the binomial coefficient "2m choose m".

Proof: Call H the set of m lists of n ballots revealed by $P_{1,3}$, $P_{2,3}$, $P_{3,3}$. Assume that one, and therefore all, of these ballot lists is not k-good. The probability that in the cut and choose the set H is chosen to be opened is $1/C(2m, m)$. If H is not chosen then the proof of value consistency is conducted on at least one array of n concealed ballots which is not k-good. The probability of this happening and proof of correctness being accepted is at most $(1 - 1/C(2m, m))(1/2)^k$. ■

For the case of no more than 20 wrong votes we use $2m = 24$ and the probability of accepting a proof of correctness while there are more than 20 discrepancies is less than $1.38/2^{20}$.

X. Countering Denial of Service Attacks (Device Failure)

It is relatively straightforward, using well-known secret-sharing methods, to provide increased robustness against the possibility that one or more of the proof server devices may fail. As noted in the introduction, Cramer et al. [6] have also used secret sharing to improve robustness of a voting system. (Their paper employs homomorphic encryption and unlike the present work reveals only the final value of the vote count.)

These methods allow construction of systems satisfying specified robustness requirements in addition to voter privacy protection. When failures may occur, then obfuscation is done by the method of proactive secret sharing (see [16]), rather than the method described in the example of the previous sections. Because Shamir secret sharing is used, M is chosen to be a prime number, say $M = 1009$.

For example, suppose we wish to protect against one device failure and one leaky device; we'll use a PS with four rows and two columns. The votes are $(4, 3)$-shared by in the finite field F_M by the voter Tablet and the shares of each vote are securely sent to four devices $P_{1,1}, \ldots, P_{4,1}$ comprising the first column of the PS. With $(4, 3)$-secret-sharing each value is split into four shares, such that any three (but not any two) suffice to reconstruct the value.

Every first-column Proof Server device $P_{j,1}$ $(4, 3)$-shares the value 0 among the 4 devices in the first column. Every $P_{j,1}$ adds the received shares of 0 to its input share. (This is

done separately for each vote.) The first column devices shuffle the obfuscated quadruples and every $P_{j,1}$ sends its obfuscated share to $P_{j,2}$. The second column of the PS obfuscates and shuffles, produces the results as output.

Now the servers $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, $P_{4,2}$ of the second column each prepares an array of commitments to split value representations of its permuted array of shares of the n vote values w_1 , w_2 , $\ldots w_n$. These commitments are posted on the SBB. This whole process is repeated $2m$ times. Then the m permuted arrays of the (4, 3) shares of the n vote values w_1 , w_2 , $\ldots$, w_n , are posted as in Sections VII–IX.

In general, if at most f devices may fail (where $f > 0$) and at most ℓ may be leaky, then PS may have r rows and c columns, where $r \geq f + \ell + 2$ (to protect votes from leaking), use an $(r, \ell + 2)$ secret-sharing method, and choose $c \geq \ell + 1$ (to protect the shuffles). If $f = 0$, then the number of rows and the number of columns need only be $\ell + 1$, as in the example of the previous sections.

For additional protection against possibly malicious servers, one may for example employ Trusted Platform Module (TPM) technology. Work in progress (to appear) presents additional methods for countering malicious servers who attempt to actively disrupt the protocol. Of course, when paper ballots are available (as with Scantegrity or Star-Vote), one can always recover the correct election outcome by counting them.

XI. Practical Aspects

We consider some practical aspects of the proposed method, such as time and storage requirements.

Assume that the number n of ballots is 10^6, the number of tablets is 10^4, and that we use $2m = 24$. The following numbers are for a typical desktop computer or laptop, which can execute 200 private-key operations (e.g. RSA 2048-bit) per second or 8 million commitments (AES operations) per second. Assume that PS has $r = 3$ rows and $c = 3$ columns.

Time to decrypt votes from tablets: This requires 10^4 private-key operations (using a hybrid method) per first-column PS device—about 50 seconds. It also requires about 10^6 openings of pairs of commitments—under a second. The 50 seconds for the private-key operations is the major component of the running time. The last-column PS devices must prepare 24 arrays of length n with 6 commitments per vote—about 18 seconds (six seconds if the last-column processors do this in parallel). The time to create the random permutations is negligible.

Size of proof: If each commitment $\textsc{Com}(u)$ is assumed to require 30 bytes, then the overall size of the proof is about $25 \times 2 \times 3 \times 30 \times 10^6$ bytes (4.5GB), about the size of a movie; the proof can be downloaded on an typical internet connection in a few minutes at most, and checked in a couple of minutes on a typical laptop.

Code: A 2800-line python program for running simulated elections was written and tested; in experiments it performs flawlessly and rapidly. (See https://github.com/ron-rivest/split-value-voting .)

XII. Conclusion

The methods presented here provide new ways for implementing verifiable mix-nets and thus end-to-end verifiable voting. The new methods are particularly efficient since they do not require any modular exponentiations or public-key operations. We believe that the efficiency and generality of this solution render it practical for actual deployment in elections.

Acknowledgment

We thank Tal Rabin for advice on proactive secret sharing. The second author gratefully acknowledges support from his Vannevar Bush Professorship. We thank the anonymous EVOTE reviewers for numerous constructive suggestions.

References

[1] B. Adida and R. L. Rivest, "Scratch & vote: self-contained paper-based cryptographic voting," in *Proceedings of the 5th ACM workshop on privacy in electronic society*, R. Dingledine and T. Yu, Eds. ACM, 2006, pp. 29–39.

[2] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy," in *Proceedings USENIX Security 2010*, I. Goldberg, Ed. USENIX, August 11-13, 2010.

[3] A. Essex, J. Clark, U. Hengartner, and C. Adams, "Eperio: Mitigating technical complexity in cryptographic election verification," in *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'10. Berkeley, CA, USA: USENIX, 2010, pp. 1–16.

[4] H. Jonker, S. Mauw, and J. Pang, "Privacy and verifiability in voting systems: Methods, developments and trends," Cryptology ePrint Archive, Report 2013/615, 2013.

[5] S. Popoveniuc, J. Kelsey, A. Regenscheid, and P. Vora, "Performance requirements for end-to-end verifiable elections," in *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'10. Berkeley, CA, USA: USENIX, 2010, pp. 1–16.

[6] R. J. F. Cramer, M. Franklin, L. A. M. Schoenmakers, and M. Yung, "Multi-authority secret-ballot elections with linear work," Centrum voor Wiskunde en Informatica, Tech. Rep. CS-R9571, 1995.

[7] J. Benaloh, M. Byrne, P. Kortum, N. McBurnett, O. Pereira, P. B. Stark, and D. S. Wallach, "STAR-vote: A secure, transparent, auditable, and reliable voting system," *arXiv preprint arXiv:1211.1904*, 2012.

[8] S. Micali and M. O. Rabin, "Cryptography miracles, secure auctions, matching problem verification," *CACM*, vol. 57, no. 2, pp. 85–93, February 2014.

[9] M. Rabin, R. Servedio, and C. Thorpe, "Highly efficient secrecy-preserving proofs of correctness of computations and applications," in *Proceedings of 22nd IEEE Symposium on Logic in Computer Science*. IEEE, 2007, pp. 63–76.

[10] M. O. Rabin and R. L. Rivest, "Practical end-to-end verifiable voting via split-value representations and randomized partial checking," April 3, 2014, CalTech/MIT Voting Technology Project Working Paper 122.

[11] ——, "Practical provably correct voter privacy protecting end to end voting employing multiparty computations and split value representations of votes," May 12, 2014, CalTech/MIT Voting Technology Project Working Paper 124.

[12] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[13] J. Benaloh, "Ballot casting assurance via voter-initiated poll station auditing," in *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*. USENIX, 2007, p. 14.

[14] C. Cullane and S. Schneider, "Peered bulletin board for robust use in verifiable voting systems," arXiv.org/abs/1401.4151, Jan. 16, 2014.

[15] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Crypto '86*, ser. Lecture Notes in Computer Science, vol. 263. Springer, 1986, pp. 186–194.

[16] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks," in *Proc. 10th ACM Symp. Princ. Distr. Comp.* ACM, 1991, pp. 51–61.

Pretty Understandable Democracy 2.0

Stephan Neumann, Christian Feier, Perihan Sahin, and Sebastian Fach
Technische Universität Darmstadt / CASED, Germany
Email: stephan.neumann@cased.de, feier@rbg.informatik.tu-darmstadt.de,
perihansahin87@hotmail.com, info@sebastian-fach.de

***Abstract*—Technology is advancing in almost all aspects of our everyday life. One interesting aspect is the possibility to conduct elections over the Internet. However, many proposed Internet voting schemes and systems build on unrealistic assumptions about the trustworthiness of the voting environment and other voter-side assumptions. Code voting – first introduced by Chaum [Cha01] – is one approach that minimizes the voter-side assumptions. The voting scheme Pretty Understandable Democracy [BNOV13] builds on the idea of code voting while it ensures on the server-side an arguably practical security model based on a strict separation of duty, i.e. all security requirements are ensured if any two components do not collaborate in order to violate the corresponding requirement. As code voting and strict separation of duty realizations come along with some challenges (e.g. pre-auditing phase, usability issues, clear APIs), the goal of our research was to implement Pretty Understandable Democracy and run a trial election. This paper reports on necessary refinements of the original scheme, the implementation, and a trial election among the different development teams.**

I. Introduction

The advance of technology, more and more, impacts our everyday life. Shopping, banking, or chatting with friends no longer depends on physical presence but may be easily done independent of time and location by digital means. In recent years, even fundamental processes of democracy have come into the focus of technological advance. Amongst the most attractive options is the possibility to conduct elections over the Internet. Since the seminal work by Chaum [Cha81], many works addressed the challenge of voting over the Internet addressing a broad set of security requirements, see for instance [LSBV10]. It turns out, however, that most of the present schemes rely on unrealistic assumptions to ensure security: for instance, the JCJ [JCJ05] scheme relies on the voter's platform being trustworthy and the Helios voting system [Adi08] relies on the voter conducting a complex verification procedure several times. The number of infected computers[1] shows that it is not realistic to rely on voters to ensure that their platforms are trustworthy. It has also been shown (e.g. in [KOKV11]) that in particular with the Helios voting system, verifiability is not accessible to voters. Furthermore, Olembo et. al [OBV13] have shown that voters do not even see the need to verify their vote due to their trust mental models.

Code voting – first introduced by Chaum [Cha01] – is one approach that minimizes the voter-side assumptions. Since its invention several code voting schemes with different advantages and disadvantages have been proposed [HS07], [JRF09], [RT09]. Recently, Budurushi et al. [BNOV13] proposed a new code voting based Internet voting scheme, Pretty Understandable Democracy (PUD). It ensures an arguably practical security model based on a strict separation of duty, i.e. all security requirements are ensured if any two components do not collaborate in order to violate a corresponding requirement. Furthermore, the authors' goal was to keep the scheme as simple as possible. To date, PUD has not been implemented and therefore has only been considered from a purely theoretical perspective.

Contribution. As code voting and strict separation of duty realizations come along with some challenges for the implementation process, the election preparation and the vote casting (e.g. pre-auditing phase, usability issues, clear APIs), the goal of our research was to implement Pretty Understandable Democracy and run a trial election. In order to implement components by a rigorous separation of duties, we decided to implement components by group-wise student projects within a computer science class at the Technische Universität Darmstadt, Germany. In this paper, we present several improvements and refinements made to the original scheme. Thereafter, we report on our experience about the implementation of the revised scheme and running a trial election among the different development teams (each team being responsible for one component).

Related Work. Chaum's seminal work on code voting [Cha01] has motivated many researchers to build their schemes upon the same idea, e.g. [HS07], [JRF09], [RT09]. The Norwegian Internet voting system [iEGT12] also uses some kind of code voting. While their verification code approach prevents single components from undetectably violating integrity, secrecy builds upon the assumption of a trustworthy voter platform [KLH13]. The only scheme we are aware of following the distribution of trust principle as precisely as PUD is Pretty Good Democracy (PGD) [RT09][2]. As opposed to PGD, PUD is tailored towards understandability and therefore real-world applicability. A more thorough review of the related work can be found in [BNOV13].

PUD in a Nutshell. Code sheets in PUD have three parts: The first part consists of a permuted list of candidates, the second and third parts consist of random and unique codes. The code parts each hold one further code which corresponds to an acknowledgement code. Throughout the code sheet generation, the respective authorities commit on their generated code sheets by encrypting them with an additively homomorphic encryption scheme (in our case ElGamal) and publishing the code sheet parts on a bulletin board. Before randomly

[1] According to [Pan14], in 2013 31.53% of all computers were infected by malware

[2] It should be emphasized that PGD's adversary model is stronger because stored-as-cast integrity can be increased linearly with number of trustees, while PUD allows further conspiracies to violate integrity.

sending out composed code sheets to voters, a fraction of code sheets is audited by comparing the printed code sheets to the encrypted version on the bulletin board. Once, the voter casts the concatenated code (from the second and third code sheet parts) which corresponds to her preferred candidate, the code parts are forwarded to the authorities that generated the respective parts. Given the encryptions of code sheet parts, both authorities are able to re-encrypt the candidate ciphertext that corresponds to that code *without* knowing the candidate within that ciphertext. In the tallying phase, the published candidate re-encryptions are summed up homomorphically and distributively decrypted. By calculating the discrete logarithm, the final result can be obtained. The tallying process is publicly verifiable.

Remark. The full version of this paper [NFSF14] contains an extended introduction to the PUD scheme and all user interfaces. For a detailed review of PUD's security model, we refer the reader to the original PUD publication [BNOV13].

II. Preliminary Setting and Task Organization

Pretty Understandable Democracy (PUD) has been implemented within a student project as part of the lecture *Electronic Voting* in the winter term 2013/14 at the Technische Universität Darmstadt, Germany. Students participating in this course had a background in computer security and cryptography.

1) Pre-considerations: Before the course started, it has been agreed on which parts should be realized and which are not realistic within a course exercise. First, we simplified the authentication step during the election process by simply using the voter's name instead of a strong authentication method. In PUD, any communication between two components is secured by applying TLS. In contrast to a real-world system, the project management team signed the public key for each component and acted as a Certificate Authority. It was decided that the servers did not have to be protected against hackers etc.. In a real-world scenario protection against several threats, like denial of service attacks (DoS), would be necessary but was out of scope for the implementation task. However, this enabled the students to use their own laptops. Motivated by a newspaper report[3] we decided to tailor our trial election towards the *"Bürgerschaftswahl"* (which translates to State Election) of the Hanseatic City of Lübeck and implemented the respective ballot from the last state election. Furthermore, it was decided that $35 - 40$ voters (i.e. all students and supervisors) should be eligible to vote in the trial election at the end of the semester. The software development teams were free to choose any programming language, as long as they were able to provide communication interfaces for the other components. This had several advantages: First, due to the different programming skills within specific languages, students could build upon their preferred languages. Second, relying on one single programming language could result in system vulnerabilities due to the compiler. An adversary could corrupt the whole system by just corrupting the used compiler. By using different programming languages, also different compilers/interpreters are used. For distributed key generation and tallying, we extended an already existing Android application [NKMV13]. We defined a threshold of two out of three.

[3] http://www.segeberger-zeitung.de/Schleswig-Holstein/Landespolitik/Kommunalwahl-2013/Albig-erwaegt-Online-Wahl

2) Organization: There were several software development teams (each one consisted of 2 to 3 students) while each team was assigned to one component and one phase. There were the following software development teams: Voting authorities (*VA1* and *VA2*) *VA1*-setup, *VA1*-voting, *VA2*-setup, *VA2*-voting, *Trustees*-audit, *Trustees*-tallying, the registration authority *RA*-setup, *RA*-voting. In addition, there were the project management team, the bulletin board (*BB*) team, and the distribution authority (*DA*) team. Students in the software development team were explicitly told to not copy any code from other groups to ensure the required separation of duty (SoD).

3) Schedule: The lecture started on October 18, 2013. There were two sessions to discuss the PUD scheme. The group assignment was done afterwards. Correspondingly, the software development part started on November 5th, 2013 and the trial election was scheduled for February 7th, 2014. Thus, the teams had about three months time to implement and test their components.

4) Project management: The software development teams were asked to send their component design, their interfaces and their project schedule until November 15th, 2013 to the project management team. This was done in order to detect and correct design flaws in an early stage of the development process. As target date for the first integration test, the project management team proposed January 15th, 2014. During the development process the software development teams were free to organize themselves, but they were repeatedly asked to report their current status to the project management.

III. Protocol Refinements

After foundational concepts of electronic voting were introduced to the students, there were two lectures on Pretty Understandable Democracy in which the scheme was introduced and discussed with the students. During these discussions, a couple of improvements were identified. These are proposed and discussed in this section.

Candidate encoding. The original proposal was to encode candidates within one single ciphertext. Due to the fact that throughout the tallying process, all encryptions are summed up, each individual encryption of a candidate must also encode *null* encodings of all other candidates. As a consequence, computing the discrete logarithm for such a complex encoding results in a computationally-intensive task even for small-scale elections. Following the multi-candidate punch-hole vector-ballot by Kiayias and Yung [KY04], our revised scheme encodes each candidate into a separate encryption indicating whether the candidate is selected or not. Therefore C encrypted blocks are sent where C is the number of candidates. Each block has the form $\{g^x\}^r_{pk_T}$ where r is a random number and x is the number of votes for this candidate. If the voter has exactly one vote this is either 1 or 0. For example there are 3 candidates and the voter votes for candidate 1 and 3. The corresponding encodings are (g^1, g^0, g^1) and the respective encryptions are given as $(\{g^1\}^{r_1}_{pk_T}, \{g^0\}^{r_2}_{pk_T}, \{g^3\}^{r_3}_{pk_T})$. Due to this improvement the necessary number of re-encryptions is increased to C for each voter. Furthermore during the tallying process $2 \cdot C$ homomorphic sums are calculated. To overcome these drawbacks compared to the encoding in [BNOV13] the tallying performance is improved. The encrypted homomorphic sums for each candidate are given as $g^{c_1}, g^{c_2}, ..., g^{c_n}$

where c_i describes the number of votes for candidate i. To solve g^{c_i} the discrete logarithm problem has to be solved but the number of necessary modular exponentiations to find all c_i is limited to $\sum_{i=1}^{C} c_i \leq V$ modular exponentiations where V is the number of eligible voters. This is solvable by using brute-force. Compared to up to $V \cdot 10^{(C-1)\cdot\lceil\log_{10}(V)\rceil}$ modular exponentiations which are necessary to tally as described in [BNOV13] this is a significant improvement.

Cross-checking indices and positions. Originally, PUD prescribed the following procedure: After *RA* split the voting code apart and forwarded the respective parts to *VA1* and *VA2*, *VA1* and *VA2* independently re-encrypt the ciphertext related to the specific voting code (over index and position of the voting code). It turns out that a malicious voter might however prevent the computation of an election result by submitting code parts that represent different candidates, e.g. on the middle code sheet part, the voter would chose the code at position 3 and at the right code sheet part, the voter chooses the code at position 4. In such a case, *VA1* and *VA2* would re-encrypt different candidates and the computed homomorphic sum of both authorities would differ. Therefore, in addition to validity checks, *VA1* and *VA2* cross-check that they obtained codes of the same index and the same position. In case the code is invalid or a mismatch is detected, *VA1* and *VA2* log the corresponding request and inform *RA* that informs the voter.

Code length. The PUD scheme builds upon the use of voting codes to ensure the conduct of secure elections. The length of these codes plays a substantial role to the scheme because it directly impacts security and usability of the scheme. In the final part of this section, we therefore analyze which length voting codes shall have. In order to have unique codes, for C candidates and V voters, there are at least $(C+1)\cdot V$ codes per *VA* required. To allow a sufficient proportion of the code sheets to be randomly audited, a factor λ is used. Therefore $\lambda\cdot(C+1)\cdot V$ codes are needed for each *VA*. Furthermore, the codes generated by *VA1* and *VA2* are disjoint which results in a factor 2 of generated codes. Therefore $2\cdot\lambda\cdot(C+1)\cdot V$ codes are needed for both *VA*s. This means that $\log_2(2\cdot\lambda\cdot(C+1)\cdot V)$ bits are necessary for each code to ensure that all codes are different. For the trial election, we set $\lambda = 2$. With `Base32` encoding, each code consists of 3 characters.

IV. Implementation

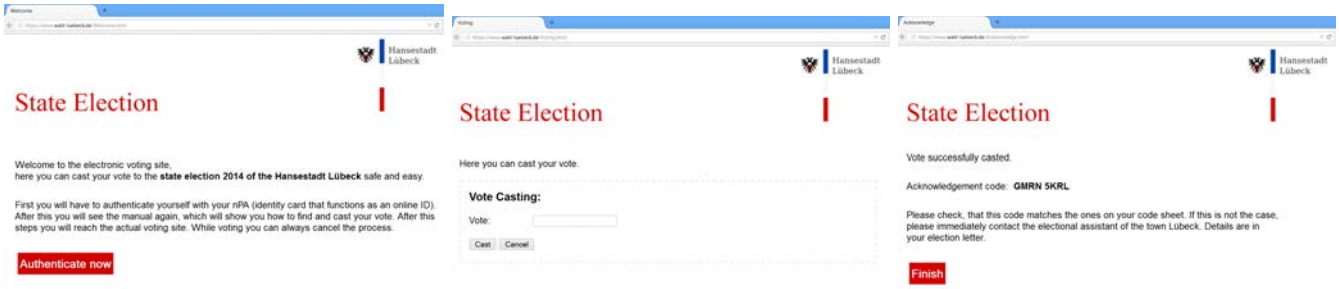
Programming Languages and Programming Interfaces. The development teams agreed on Python, Java and Scala as programming languages. Both parts of *RA* and *BB* are written in Python, both parts of *VA1* and *VA2* are written in Java and the *DA* is written in Scala. In order to ensure a smooth communication between the involved entities, the students agreed on a REST API to receive and send data. To publish the specific syntax for each command an internal Wiki was used in which each team documented all available commands for their API. Some students did never work with a REST API and had to start learning it first.

Election Material and User Interfaces. The election materials as well as the user interfaces were developed in an iterative process, i.e. members of different teams provided feedback as well as friends not being involved in the process. The election material was developed by the *DA* team in close collaboration with the *RA*-voting team. Once visited the election website, information about the Internet voting process is displayed (see Figure 1(a)). In order to proceed, the voter needs to click on 'Authenticate now'. The voter, then, authenticates himself/herself. After being authenticated, the next interface displays the election manual (similar to the election material received together with the code sheets). The voter continues by clicking on 'Vote now'. The system re-directs the voter to the next interface on which he/she casts his/her vote (Figure 1(b)). Both codes of his/her preferred candidate need to be provided in the field next to 'Vote'. Spaces will be deleted by the interface. The vote casting can either be completed by clicking on 'cast' or canceled. Once cast, the interface displays the information that the vote has been successfully cast and the respective acknowledgement code as shown in Figure 1(c). The BB provides different sectors for all phases of the election process. Every entity has read access and except the Distribution Authority also write access. All data published on the Bulletin Board is signed by the publishing authority. For example, throughout the setup phase, commitments of code sheets are published on the BB

Tests. To test their components the teams wrote their own test cases. Unfortunately, some teams did not stick to the plan on the first test, which was as announced on January 15th. Therefore, the final complete test took place at February 6th, 2014, only one day before the trial election. At the final test some problems occurred, which had to be fixed: The communication from any component to *VA1* did not work because of a TLS error. Furthermore the tallying module did not work correctly because the group did not implement homomorphic tallying properly. To fix these problems, the students worked until late night and the whole morning before the trial election. This experience shows that time schedules are even more important if (voting) systems are developed in a distributed manner.

V. Lessons Learned

The trial election was conducted on February 7th, 2014. Assembling all the needed papers (three code sheets and the election manual) took about 20 minutes (with one printer) for the small trial election with 50 voters, where ten persons in parallel took care of preparing the voting papers. This process could possibly be improved by special machines. Even without machines, the process could be organized in a way that is acceptable as in many German cities the postal voting material is also prepared manually. Auditing only five code sheets took us more than 10 minutes. It just takes time to open the envelopes and read aloud all the candidates, then all the codes from *VA1* and then all the codes from *VA2* for each audited code sheet. It even takes more time, if this is done in a transparent manner, i.e. the present observers can follow the process. When entering the codes, we noticed that some participants were confused by entering both parts of the code in the same text field. It might be worth providing two different fields in future and clearly indicating which code to enter in which field. The different views of the bulletin board were clear to the participants. However, it was also discussed that in case - due to transparency requirements - it is assumed that also voters should understand the content of the bulletin board, further information needs to be provided.



(a) Welcome Interface. (b) Vote casting interface. (c) Interface with acknowledgment.

Fig. 1. User-interface

VI. Conclusion

The present work reports about the experience of refining and implementing Pretty Understandable Democracy (PUD) and running a trial election with that scheme as part of a computer science course. The insights gained throughout the implementation and the trial election process are manifold and serve as guidelines for future research. PUD has been introduced as a theoretical concept and as such several details remained open. This gap forms the motivation for the present work. The first refinement is the multiple ciphertext encoding of single votes, which reduces the number of modular exponentiations needed throughout the tallying process significantly. In order to prevent malicious voters from blocking the calculation of the election result, the voting authorities cross-check the consistency of voting codes. Furthermore, we analyzed the required lengths of voting for different election settings. Finally, in order to conduct the trial election as close as possible to real-world elections, we proposed user interfaces tailored towards the state election of the Hanseatic city of Lübeck which currently considers introducing Internet voting. The contributions of this work builds *one* step towards PUD's real-world applicability knowing that there are many challenges open challenges before its first usage. Throughout the trial election, individual code sheet parts had to be combined into one envelope and sent out to voters. This results in significant organizational and time-intensive effort. We consider revising the code sheet distribution process, thereby lowering the organizational effort. Discussions among the students and the staff show that from a usability perspective the scheme is going into the right direction. In order to evaluate the scheme's usability in an unbiased manner, user studies will be conducted in the near future. PUD has been tailored towards a trade-off between security and transparency. Nevertheless, the scheme builds upon several cryptographic primitives. We plan to investigate the scheme's understandability by preparing information and education material and evaluating it in user-studies.

Acknowledgment. This work has been developed within the project ComVote, which is funded by CASED.

References

[Adi08] Ben Adida. Helios: Web-based open-audit voting. In Paul C. van Oorschot, editor, *USENIX Security Symposium*, pages 335–348. USENIX Association, 2008.

[BNOV13] Jurlind Budurushi, Stephan Neumann, Maina Olembo, and Melanie Volkamer. Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme. In *8th International Conference on Availability, Reliability and Security*, pages 198–207. IEEE, 2013.

[Cha81] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[Cha01] David Chaum. Sure vote: Technical overview. In *Proceedings of the Workshop on Trustworthy Elections (WOTE 01)*, 2001.

[HS07] Jörg Helbach and Jörg Schwenk. Secure Internet Voting with Code Sheets. In *VOTE-ID*, pages 166–177, 2007.

[iEGT12] Jordi Barrat i Esteve, Ben Goldsmith, and John Turner. International experience with e-voting. 2012.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *ACM Workshop on Privacy in the Electronic Society*, pages 61–70. ACM, 2005.

[JRF09] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. VeryVote: A Voter Verifiable Code Voting System. In *Proceedings of the 2nd International Conference on E-Voting and Identity*, VOTE-ID '09, pages 106–121. Springer-Verlag, 2009.

[KLH13] Reto E Koenig, Philipp Locher, and Rolf Haenni. Attacking the verification code mechanism in the norwegian internet voting system. In *E-Voting and Identify*, pages 76–92. Springer, 2013.

[KOKV11] Fatih Karayumak, Maina Olembo, Michaela Kauer, and Melanie Volkamer. Usability analysis of helios - an open source verifiable remote electronic voting system. In *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, 2011.

[KY04] Aggelos Kiayias and Moti Yung. The vector-ballot e-voting approach. In *Financial Cryptography*, pages 72–89. Springer, 2004.

[LSBV10] Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer. A taxonomy refining the security requirements for electronic voting: analyzing helios as a proof of concept. In *5th International Conference on Availability, Reliability and Security*, pages 475–480. IEEE, 2010.

[NFSF14] Stephan Neumann, Christian Feier, Perihan Sahin, and Sebastian Fach. Pretty understandable democracy 2.0. Cryptology ePrint Archive, Report 2014/625, 2014. http://eprint.iacr.org/.

[NKMV13] Stephan Neumann, Oksana Kulyk, Lulzim Murati, and Melanie Volkamer. Towards a practical mobile application for election authorities (demo). In *4th International Conference on e-Voting and Identity (VoteID13)*, 2013.

[OBV13] Maina M. Olembo, Steffen Bartsch, and Melanie Volkamer. Mental models of verifiability in voting. In *Proceedings of the 4th International Conference on E-Voting and Identity*, VoteID'13, pages 142–155, Berlin, 2013. Springer-Verlag.

[Pan14] Panda Security. Annual Report Pandalabs 2013 summary. http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf, 2014. Online; accessed 30 May, 2014.

[RT09] Peter Y. A. Ryan and Vanessa Teague. Pretty Good Democracy. In Bruce Christianson, James A. Malcolm, Vashek Matyas, and Michael Roe, editors, *Security Protocols Workshop*, pages 111–130. Springer, 2009.

Trust in Electronic Voting

Trust in Internet Election Observing the Norwegian Decryption and Counting Ceremony

Randi Markussen, Lorena Ronquillo and Carsten Schürmann
IT University of Copenhagen. Rued Langgaards Vej 7
DK-2300, Copenhagen (Denmark)
Email: {rmar, lron, carsten}@itu.dk

***Abstract*—This paper discusses the Decryption and Counting Ceremony held in conjunction with the internet voting trial on election day in the Ministry of Local Government and Regional Development of Norway in 2013. We examine the organizers' ambition of making the decryption and counting of electronic votes public in order to sustain trust in internet voting. We introduce a pragmatic approach to trust that emphasises the inseparability of truth from witnessing it. Based on this and on a description of how the event was made observable and how the complexities in the counting process were disclosed, we discuss what we term *economy of truth* from the perspective of the IT community involved in the ceremony. We claim that broadening the economy of truth by including more explicitly social and political perspectives in the ceremony, and in internet elections in general, and how witnessing is brought about, would make a more solid case for understanding how democracy is transformed.**

I. Introduction

Democratic elections in contemporary society, according to Article 21, Universal Declaration of Human Rights, shall be periodic and genuine; they shall be by universal and equal suffrage and guarantee the secrecy of the vote. Practicing elections in a manner that is compatible with these principles raises, among other things, the question of who is involved in organising, administrating and overseeing the electoral process and the voting procedures, in particular. Thus the public staging of the election, as well as public involvement in the counting, have in many countries been constitutive elements in preserving trust and legitimising a representative democracy.

Internet voting challenges these elements in a significant and profound manner, as the public engagement in counting is replaced by counting by computers that are managed by technical experts. What is rarely addressed in detail, however, is how the experts carry out their work, and how their activities may relate to the public. The internet voting trials in Norway in 2011 [2], [19], [29] and in 2013 [7], [22] stand out, as the Norwegian Ministry deliberately experimented with the idea of publicly overseeing the experts' counting activities during a public event, the so-called Decryption and Counting Ceremony. The Ministry of Local Government and Regional Development of Norway (hereafter *the Ministry*) was responsible for designing and running the ceremony. The ceremony took place on the premises of the Ministry on election day.

In this paper, we study in detail the way in which the Administration Board (employed by the Ministry) rendered the decryption and counting activities observable. The goal of the ceremony was to convince the audience that truth is produced. The Ministry argued in advance that "Observation in the *back office* combined with voter observation of return code replaces the function of the observer in the polling station" [6]. We mainly concentrate on the *back office* disclosure in order to explore how the idea of trust in this event can be addressed.

Based on a pragmatic understanding of trust in science and within science, and inspired by Shapin's framework [26, p. 6], we describe the ceremony and explore what we term *economy of truth* from the IT community's perspective. We argue that broadening the economy of truth by articulating more explicitly social and political perspectives may create a more solid understanding of how democracy is transformed. Our arguments intend to inform research communities in the area of e-governance more broadly, when trust is a key concept, as well as politicians and the public in general.

This paper is organized as follows: Section II introduces a pragmatic, philosophically motivated understanding of trust and its importance in everyday life as well as in scientific communities, and briefly presents its relevance in understanding trust in elections. Section III introduces the Decryption and Counting Ceremony and its organizational set up, including the legal bodies witnessing the event. Then, Section IV gives a high-level understanding of the decryption and counting stages of the Norwegian internet voting system as it was designed, and sketches those procedures that were executed during the actual ceremony to render parts of the system observable. The description aims by no means at being a comprehensive outline of all the details involved in the ceremony, but it serves mainly to communicate the technical complexities and challenges involved in the ceremony in a manner that is consistent with what the organizers probably intended to achieve. More technical information about the voting protocol can be found in [11]. Section V brings the insights from the various sections together by discussing the economy of truth shaped by the Decryption and Counting Ceremony from a technical perspective, as well as a social and political perspective, and finally Section VI concludes the paper.

II. How to understand trust

Over the last decades the term *trust* has received increasing academic attention. This is driven in part by our curiosity to understand how contemporary societies work, not least the role of trust in science in the making of society, as well

as the role of trust in producing knowledge within scientific communities [15], [27], [33]. Predominant perspectives tend to build on rational philosophical assumptions focusing on individual rational decision making. In contrast, pragmatic perspectives, which are the ones this paper follows, emphasize the collective aspects in the making of social orders and in knowledge production, and argue that whether actions are rational or not do not belong to the individual actor, but it also depends on how they are perceived by others [30, p. 19]. Of special interest in our context is Steven Shapin's seminal work on the origins of experimental philosophy [26]. Shapin shows that the gentlemanly culture of truth telling that Robert Boyle together with members of the Royal Society developed was consequential for trust in their new natural science. Furthermore he suggests that contemporary scientific truth claims similarly involve the witnessing by specific scientific communities [26]. In relation to elections, this argument implies that the community involved in the counting go hand in hand with the community of accounting. Where Besselaar et al. [5] argue that voters' trust in the technology is more important than the technical characteristics, we want to avoid in this paper the dichotomy between trust/subjectivity versus things/objectivity and argue that the concept of technical characteristics is closely related to the witnessing of truth claims within a specific scientific community.

Thus trust is involved in the dynamics in social ordering in everyday life, as well as in scientific knowledge production, as no single individual can constitute knowledge outside of a community. "Truth consists of the actions taken by practical communities to make the idea true, to make it agree with reality" [26, p. 6]. Shapin stresses that pragmatic philosophers reject a static understanding of truth, and emphasises the close connection between truth and trust by pointing to their etymological root in the Germanic word for tree: "Trust/truth is therefore, like a tree, something to be relied upon, something which is durable, which resists, and will support you." [26, p. 20]. The early pragmatist philosopher W. James compared the investment in trust to a credit system: "Our thoughts and beliefs *pass*, so long as nothing challenges them, just as bank-notes pass as long as nobody refuses them." [13, p. 88-91]. In connection to elections, this argument suggests that if people experience their government to be well working and find elections are held and have been held in a fair manner, they will continue trusting it until an event proves this wrong. The recent evaluation report of the Norwegian internet trial in 2013 [24] also makes this argument, suggesting that the slight reduction in trust in elections which was perceived in the municipalities involved in the internet election in 2011 had to do with its newness. But the moment people did not experience any major public scandals, the level of trust was reestablished [24].

This illustrates that trust not only involves routine interactions, it includes deliberate decisions on whether to trust or not, as well as distrust and scepticism. Trust but also distrust "presuppose a system of takings-for-granted which make this instance of distrust possible." [13, p. 19]. Thus computer scientists, especially cryptographers, share by training a specific way of addressing a situation and discussing the relevance of specific arguments. Hence the character of scepticism depends upon the extent and quality of trust in a given community. In a Scandinavian context it is often said that people trust their governments[1], meaning that if people express scepticism and distrust, it should be seen against a solid quality of trust as well. Scientific communities, or political communities to mention some, may cultivate specific language games, ways of making truth claims and discussing them. The opposite of trust in Shapin's account is "the public withdrawal of trust in another's access to the world and in another's moral commitment to speaking the truth about it (. . .). It is not just that we do not agree with them; it is that we have withdrawn the possibility of disagreeing with them." [26]. Thus trust, as well as distrust, are involved in making democratic societies work, and without them societies may fall apart.

We are especially interested in the metaphor of *economy of truth* that Shapin shortly introduces: "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behavior. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The metaphor *economy* suggests that there are interests, costs, and values involved in truth-making and hence trust-making, and that protecting certain ways of understanding the world, may be as important as producing knowledge. For instance, an economy of truth shaped by paper ballots and public involvement, is extraordinary in that it consists of all voters, including election officials who know the regulations and procedures. They perform a temporary community, distributed into several minor communities all over the countries, who have to contrive to work together locally and apply the regulations in practice. More can be said about how computers are already applied in many of their work activities. Suffice to say that the process is nonetheless in economic terms sometimes described as *people intensive* as opposed to technology intensive, following a dominant logic in our economy of replacing human labour with machines. In our context, internet voting as well as e-voting involve new scientific communities of knowledge-making and consequently other aspects of the economy of truth. Indeed, they require new equipment and machines, which in Shapin's argument, depend on specialized knowledge and a community that favours specific truth claims and ways of producing and protecting truth, as we explore in this paper. One may talk, for instance, about an economy whose monetary units includes competences, truth claims and ways of dealing with them, technologies, proofs, etc.

An important instrument for maintaining confidence in the electoral process and giving elections credibility is often expressed as transparency in every step [8], [32], meaning that the government and the organizers do not hide activities from the public. Practicing elections along these principles is a well-established habit in Norway and has no doubt inspired the Norwegian Ministry in organising the ceremony and trying to create a public space to attest to the truth produced in the counting of internet votes.

[1] According to the OECD's Better Life Index [20], 66% of people in Norway say they trust their national government, being one of the highest rates in the OECD and much higher than the OECD average of 39%.

III. The Decryption Ceremony

In June 2013 the Ministry appointed an Internet Election Committee (IEC), to ensure that the internet voting trial was conducted in accordance with the regulations, and in a manner that is open and the voters could trust [16]. The idea was to have a group of people, independent of the Ministry, to supervise the preparation, conduct verification and approve the results, besides having the authority to suspend or cancel the trial in case of irregularities. The members of this committee were also involved in the decryption event, as we will later see. The nine members covered technical and political competences, and also included a representation from the municipalities involved in the trial: one member from the Norwegian Data Protection Inspectorate, an election researcher, a cryptographer, the chairmen of the Election Boards of three of the counties, and three regular voters selected from the pilot municipalities [16]. In addition, a verification team consisting of three people with electoral and technological expertise was appointed to check the correct behaviour of the decryption and counting process [22].

The composition of the new legal institutions is noteworthy, as it suggests that political and social competences are also important in accounting for the event, besides only technical expertise. At the same time, the internet voting technology in use is based on a specialized discourse of advanced mathematics, including cryptography, and its own system of takings-for-granted, assumptions and technical challenges. Opening this black-box to convince the technically savvy audience that the system performs as expected is one thing. However, making specialized concepts such as encryption and decryption keys, secret-sharing and zero-knowledge proofs comprehensible, and therefore relevant, to a public in general that does not necessarily share this discourse, is another.

As already mentioned, many internet voting technologies are based on cryptography, and so is the Norwegian that uses, in particular, asymmetric key cryptography. During the course of the election a public and a private keys are created and used. The public key is known by everyone and used by the voter to encrypt his/her vote and make it unreadable[2], while the private key allows to decrypt the encrypted vote and hence recover the original vote. Clearly, the election private key is of special importance in the voting system when securing the privacy of votes, thus in the Norwegian context the IEC members were assigned the authority to safeguard that key. At the beginning of the election, during the so-called Key Generation Ceremony, the election keys were created and each IEC member was given a smartcard containing a unique share of the private key. Their task consisted of keeping these shares safe until the Decryption and Counting Ceremony, at the end of the election, where by putting at least 6 out of the 9 shares together [14], the key would be reconstructed and used to decrypt the electronic votes.

The Decryption and Counting Ceremony took place in an auditorium in the Ministry, two hours before the election closed. As the design of the auditorium suggests, it creates a room for an audience to watch a performance. In this context, the stage (see Fig. 1) allowed for several computers, a safety deposit box, a blender (used to destroy physical storage media) and some screens, as well as the people responsible for the internet voting system. Besides the IEC and the verifier team, the audience included election observers such as representatives from the OSCE, the Carter Center, as well as from other countries, and also the company that had built the system.

Fig. 1. The setup and the agenda [17].

The term *ceremony* underlines the formal character of a public event, and stresses the serious challenges involved in developing ways of making decryption visible, even to a mixed audience, including anybody interested in watching the online broadcast of the event [17]. However, what is shown in the ceremony is not the final counting of the election results, but a preliminary counting. As mentioned by the main spokesperson, the ceremony works as a *guided tour*, a demonstration of the virtual procedures that describe the internet counting, at the same time as the audience is invited to stay and review the final count later on.

Norway is not the only country in the world having engaged in internet elections. In Estonia, internet voting has been used for binding political elections since 2005, both local and nationwide, and other countries like Canada and Switzerland from 2003, and Australia from 2011 [2], [4] have also used it for some municipalities. However, to our knowledge, the decryption events of these elections, if any, have mostly gone unnoticed in the literature. In the case of Norway, recent reports from International Election Observation Bodies [7], [22] mention the Counting and Decryption Ceremony just as one more step taken by the Norwegian Ministry in order to make the system transparent, but do not seem to have looked into the event as such. In Estonia, Alvarez et al. [1] mention that the decryption and counting of internet votes in the election of 2007 took place before the election closed, and in order to ensure that none of the results from the internet vote tabulation could be broadcast to the media, candidates, or parties until the polls had closed, all communication devices of observers were confiscated, the doors of the room sealed, and security guards posted at the doors, while the authors do not mention any online broadcast of the event. According to the OSCE/ODIHR [21], the counting of internet votes in the Estonian parliamentary elections of March 2011 was done in the presence of the National Electoral Committee members and domestic as well as international observers, but no ceremony, as in the case of Norway, is mentioned either. In the local

[2]This encrypted vote is unreadable under certain assumptions well-known within the cryptographic community but out of the scope of this paper.

elections of October 2013, however, Halderman et al. [12] do mention in passing that the encrypted votes were decrypted and counted at an event that resembles somewhat the Norwegian Decryption and Counting Ceremony, in that there was an audience witnessing the process in a room of the Estonian Parliament building, and the event was also made available online [10]. As for other countries like Canada, Switzerland, and Australia, to our knowledge, the opening of the electronic ballot box and decryption of internet votes was not witnessed by the public, but by scrutineers and sometimes also the police, as in the case of Geneva, Switzerland.

IV. Decryption and counting

This section briefly describes the main characteristics of the Norwegian internet voting system, paying special attention to the decryption and counting stages, and then reviews some of the procedures we observed about the system working during the public ceremony.

The Norwegian internet voting system is conceived as a supplement of the traditional paper-based voting. In order to mitigate the risk of voter coercion or vote buying inherent to internet voting, and given that voters were able to vote electronically during an advance voting period of roughly one month, the system supports *repeat voting*, by which voters are able to vote multiple times, but in such a manner that only one vote will be counted. Thus if a voter casts multiple electronic ballots, the last cast ballot is the one counted, while any vote cast on paper is final and overrides previous electronic votes [11].

The system also uses return-codes, a mechanism that allows voters verify that their vote has been correctly received by the voting server and thus provides individual verifiability, usually referred to as *cast-as-intended*. This feature is not discussed further in this paper.

An important cryptographic component of the Norwegian internet voting system are *zero-knowledge proofs*, i.e. methods by which a verifier can be convinced (with negligible amounts of doubt) that a particular statement is true without learning anything else apart from the fact that the statement is true. In the case of voting, for instance, zero-knowledge proofs allow verifiers to check, among other things, that the votes have been correctly decrypted without the private key being revealed to them.

The electronic ballot box contains all internet ballots encrypted [9] and also digitally signed by the corresponding voter [11]. Once the voting phase is over, this ballot box is taken offline and handled on air gapped servers, i.e. physically isolated and not connected to the internet. The decryption and counting of internet votes thus takes place in three phases. The first phase, called *cleansing*, identifies the ballots that will be counted according to the repeat voting policy, and disregards the rest. The signature of the resulting ballots is also checked during this phase. The second phase is called *mixing*, which cryptographically anonymizes the cleansed ballots so as to prevent tracing them back to the voters who cast them. This means that the ballots are shuffled and re-encrypted at each mix-net node, so that they end up in a different order and also look different (yet still encrypt the same votes). In the final phase, the *e-counting*, the decryption key is recovered from the shares of the smartcards of the IEC [25]. The mixed ballots are then decrypted, tallied, and the electronic vote count is finally submitted to the central election administration system (EVA[3]).

In addition, every phase of the decryption and counting process generates zero-knowledge proofs showing, respectively, that the cleansing of ballots was done properly, the mix-net nodes behaved correctly and actually shuffled and re-encrypted the ballots, and that the decrypted votes accurately reflect the encrypted votes.

A. Making the decryption and counting visible

In what follows we review some of the relevant procedures we observed, carried out by the Administration Board (hereafter *the organizers*) at the Decryption and Counting Ceremony.

On the auditorium stage there is a table with three laptops, a safety deposit box, a blender and three overhead displays, showing the screen content of the laptop in use, as well as some explanatory slides giving details about what is happening during each phase. Two of the organizers are seated at the table. They will be the ones running a number of commands on the laptop corresponding to the respective phase, while a third, the spokesperson, is standing up and guides the event. In a corner of the room, a group of verifiers with a computer connected to their own big screen are sitting and waiting to come into play (see Fig. 1). Among the audience, the nine members of the IEC, equipped with their smartcards, also observe the event, awaiting to be called upon during the e-counting phase to insert their smartcards into a smartcard reader, used to reconstruct the election private key.

According to the organizers, the electronic ballot box that is about to be decrypted and counted as part of the ceremony was retrieved from the central database server some time before the ceremony in the presence of the verification team and the observers. Starting with a memory stick containing the electronic ballot box, a second one containing the electoral roll, and a third one with some other election data, the process goes through the cleansing, mixing and e-counting phases. At the same time, the overhead screens show the commands running each phase. Most of these commands are standard Linux commands, and no user interface is used but the terminal. By doing this, the organizers deliberately give the audience a glimpse into the inner details of the decryption and counting process like, for instance, which folders are being accessed at any time, what is their content, etc.

The three laptops on the table are color-coded and each connected to different servers through a cable of the same color. The audience is informed that each laptop runs one of the three phases of the decryption and counting process, thus the colors identify the components that are in use during each phase, and illustrate that the servers are apparently not connected to each other and therefore are air gapped. To confirm the latter, whenever some data (the processed ballot box) needs to be transferred from one phase to the next one, it is physically moved from one laptop to the one running the next phase by means of a new and recently unsealed memory

[3]Elektronisk Valgadministrasjonssystem.

Fig. 2. A member of the verification team taking a picture of the hash value shown in one of the big screens [17].

stick. These memory sticks are taken from the safety deposit box, for which the verifier team has the key. The organizers also show that the memory sticks are new by showing each time that they are empty. In addition, the main table of the auditorium is *kept tidy* at all times which is achieved by extracting the memory stick from the respective laptop whenever the organizers finish working with it. This aims to help the verification team and the audience to understand the movement of the data throughout the three phases. Furthermore, in order to show that the cleansed ballot box and the mixed ballot box remain unchanged when transferred from one phase to the other, and no process injects new votes into the ballot box, a well-known cryptographic tool known as *hash function* is used. The output of a hash function is unique (at least for our purposes it may be considered as such), thus it is used here to prove the equality of two files located in different machines. In the context of the ceremony, the hash value of the file to be transferred is shown both before being copied to the memory stick, and after being copied to the next machine. This enables the verifier team, as well as anyone among the audience, to take a picture of the first hash value and compare it to the second one for equality (see Fig. 2).

Because of the sensitive nature of the data contained in the two memory sticks used between the cleansing and the mixing phases, and between the mixing and the e-counting phases, as well as to illustrate that the ballots in these memory sticks should never be recovered, these memory sticks are immediately destroyed in a blender after use.

Once the mixing phase is completed, the verifier team is given two memory sticks containing, respectively, the mixed ballot box and the zero-knowledge proofs generated in the mixing phase, to check that the mixing has been conducted correctly. Later on in the ceremony, the verifiers inform that the checking has been successful. Next, as part of the e-counting phase, the organizers take a top hat in which, prior to the ceremony, they have put the name of the IEC members in small pieces of paper. One by one, the members are named at random to bring their smartcards and enter their parts of the key into the system [25], until the election private key can be recovered and finally used to decrypt the internet ballots and obtain the preliminary results. These results are then copied to a memory stick, and transferred to EVA after the public ceremony.

Finally, the verifier team is given the memory sticks containing the mixed ballot box and the zero-knowledge proofs generated in the e-counting phase, to check the decryption. The result of this check, however, is not given during the ceremony because of timing constraints.

V. Discussion

The Decryption and Counting Ceremony demonstrates that the truth in the processes involved in counting electronic votes, when internet is used to cast votes and cryptography is a prime warrantor of both the secrecy of these votes and the election's integrity, is produced very differently from the counting of paper ballots. The sketch in Section IV-A, done primarily with an eye on what we think the intention of the organizers was, points to the event as a spectacle where various elements are visualised in order to make the procedures transparent and observable to the audience and some sort of public. Following Shapin's argument that truth and trust are closely related to the witnessing of an event, we discuss the economy of truth and the ambition of accounting for the decryption to the public in various perspectives on the event.

A. The economy of truth in the IT community's perspective

Trust in the internet election, and in e-voting more generally, is mostly addressed as a question of citizens' trust. Thus the Norwegian evaluation reports of the internet voting trial in 2011 [23, p. 63] and in 2013 [24] measure the degree to which citizens trusted the technology without addressing more explicitly the ceremony and the Ministry's communication efforts as such. More broadly, the field of *e-governance* is engaged in suggesting and defining measures that should be in place for a specific technological solution to be considered trustworthy by the IT community and consequently, as we tend to hope, also by the public. E-governance also focuses on aspects that are relevant to internet voting, such as transparency, evaluation according to international standards, separation of duty, verifiability, vote updating, etc. to establish trust among the public [28], [31].

The Norwegian Decryption and Counting Ceremony adds an important element to this context, however, by opening the black-box of how decryption works, and highlighting that trust as understood by Shapin is an element within the IT community as well. As mentioned in Section II, the IT community shares a system of takings-for-granted that makes them expect certain things to take place, and this in turn makes specific ways of distrusting possible. Indeed, distrust is a hallmark of IT security with its focus on defining adversary models and estimating what might go wrong. As Shapin suggests [26], distrust is crucial in many kinds of knowledge production, and in our view the ceremony points to important aspects of the economy of truth within the IT community. Most importantly, it bears witness to the technical complexity of the Norwegian internet voting system. The IT community seems to agree that this complexity inevitably makes the system prone to risk and failures, as also mentioned in the Carter Center report [7], but it also recognises the efforts made by the organizers in managing the complexity by encouraging transparency and inviting peers to give feedback and witness the ceremony.

The ceremony attests to the idea that IT is not so much an autonomous object as a socio-technical learning process.

However, not everything that the IT community would have liked to observe, could be made visible at the ceremony. For instance, the audience could not check, and therefore needs to trust, that the correct electronic ballot box was the one used for the ceremony, or that the actual preliminary results, and no others, were transferred to EVA. While disclosing these steps could have helped in making the process more transparent, they were only shown to the verifier team. In addition to this, given that the decryption key was recovered from the IEC members during the preliminary count and before the final count, the audience has again to trust the organizers to have safeguarded and not misused it during this (even if short) period of time.

There are some other aspects in which the ceremony, probably due to time or space constraints, did not succeed in making the process more visible from a technical point of view. For instance, the use of standard Linux commands might not have given enough confidence to an IT literate about what the programs were actually doing, since it is possible to override these commands to perform a completely different task. We suspect that before the ceremony started and in front of the verifier team and the observers the organizers demonstrated the robustness of the Linux platform and that they had the right implementation of the hash function. Regarding the zero-knowledge proofs, the public has to trust the verifiers to use reliable software to check these proofs and complete checking those proofs that were not checked by the end of the ceremony. And ultimately, taking into account that what was covered by the ceremony was just a preliminary count, one wonders how the audience can be sure that the final count was indeed done in a manner similar to the simulation just observed. Besides these questions closely related to the system of takings-for-granted in the IT community, one can add the trust in the wider infrastructure in which the internet election and the ceremony depend on. Perhaps not intended as such, but to us, the top hat pointed to the ambiguities involved in keeping some things secret while making others visible, suggesting that the boundaries between science and fiction may not be necessarily as robust as we tend to think.

The organizers took also some other precautions to make the system more transparent, such as, for example, publishing the source code and the system documents in advance. This allowed for independent reviews and assessments and thus contributed to the IT community's trust in the system. The Decryption and Counting Ceremony did this to a much lesser extent because, we suspect, of those aspects that could not made visible during the event, as we have discussed above. More importantly, while the ambition to create transparency is one of the goals of the ceremony, we observe that it is reduced to trusting the work of the verification team that is responsible for approving the final result. Their position in the room as partly on the scene when checking the hashes and equipped with their own computer, and partly in the audience when they sit back and watch together with the rest of the audience, points to their role as what is increasingly termed a *proxy* in the election observation community: a stand in for the audience and the public, as the IEC appointed them. Thus the ceremony makes obvious that trust in that the votes are counted correctly ultimately is about trust in the verifiers, as well as the organizers. In this respect the ceremony relates to the idea of replacing the function of the observer in the polling station in democratic elections.

B. The economy of truth in a social and political perspective

While the ceremony makes it possible for the IT community to discuss and form an opinion on the quality of the counting of votes, it is less obvious, however, to what extent the fact of replacing the observer in the polling station is meant to be an explicit part of the ceremony. One might expect that the IEC was assigned the task to try to address questions relating to democratic legitimacy and political and social aspects of the ceremony and the internet voting trial. But their role in the decryption ceremony was apparently to focus on controlling the access to the election private key, and thus attesting to the correctness of a central albeit small part of the ceremony. They seem to fulfill the expected performance during the ceremony, but to our knowledge they have not documented their work or reflections in a publicly available form. The OSCE report points to the vague definition of their tasks and argue that "the IEC met rarely and its role appeared largely formalistic. Most IEC members with whom the OSCE/ODIHR EAM [4] met were not conversant with the system and relied entirely on the MLGRD[5]'s guidance and advice. This called into question the IEC's competence and its effectiveness as an oversight body." [22, p. 8]. It is noteworthy that this criticism stays within a technical framing of the event and the system of takings-for-granted within the IT community, which only a few members of the IEC share. However, the OSCE report does not mention the possibility of discussing the ceremony more explicitly in social and political terms, and thereby providing the politicians and the public with other kinds of arguments.

As mentioned in Section II, the term economy of truth emphasises that "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behaviour. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The above suggests that for the Norwegian trial, technologists did not include discussions about the witnessing and its quality in their economy of truth. They also did not consider other public aspects of the event, e.g. in what respect is the aforementioned replacement useful, desirable or promising. But then we beg the question why the organizers bothered to organize the Decryption and Counting Ceremony in the observed form and to make it public, if only computer scientists and other experts are considered reliable observers if not to speak of reliable witnesses? We feel strongly that it is prudent to start considering witnessing and observing as part of the economy of truth for any internet voting platform and respective ceremonies, in particular.

In broader terms, if we compare the ceremony to the democratic paper-based election in Norway, there are noteworthy differences in the kind of public that the various processes allow for. In Norway as well as in many other countries, the paper-based enactment does not only give the public the opportunity to observe the election, as the organizers of the Decryption and Counting Ceremony mention, but they are allowed to participate in the counting as volunteer election officials. If we take the distributed nature of the counting

[4]Election Assessment Mission.

[5]Ministry of Local Government and Regional Development.

process across numerous municipalities into account as well, it demonstrates the involvement of any voter who cares to participate, as well as it presumes that voters are able to count and understand the event. This means that they are accountable witnesses in the particular part of the event they take responsibility for, and it signifies a shared responsibility in terms of trusting/distrusting the counting of one's fellow citizens as the results are finally brought together in the Ministry.

The Decryption and Counting Ceremony, on the other hand, involves only computer scientists as reliable witnesses in the legitimate audience. However, there were also others in the audience, e.g. peers from the e-voting community, observers from various organizations, or representatives from other governments who want to know about the technology, and vendors. At the same time, anyone from anywhere in the world is, in principle, invited to take part via the online broadcasting. This position is strikingly different from the involvement in the local paper-based election process. The role of the audience may be described as attestive spectators[6] as opposed to active participants. Attestive spectators hardly qualify as witnesses in the way Shapin understands it, as they are not explicitly involved and accountable for the ceremony and the performance they attest to. In this respect, the verifier team is the only community that qualifies as a reliable witness. To what extent it is possible as well as acknowledged that spectators of different professional trainings may contribute to a debate is not clear. This is not so much meant as a criticism, but also as a way of exploring possible ways of making the event legible in broader terms. We believe that ordinary citizens may hardly choose to watch the online performance for entertainment, or even as a citizen duty, but perhaps engaged teachers might want to use the broadcasting in discussing democracy and technology for educational purposes. We do not know to what extent the event has had an impact for instance on politicians and their decision making, but obviously one can argue that the ceremony and the way it was presented makes it difficult for people outside of the community engaged in internet election to make sense of the performance.

J. Barrat i Esteve et al. raised the following concerns: "Internet voting was in its infancy when the Council of Europe Recommendations were written. We know now that e-enabled elections are far more complex than previously thought, not only technically, but also legally and from the procedural point of view. Yet, the recommendations say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way" [3, p. 8]. The idea that internet voting can be understood in a technically neutral way, which we see as another way of putting that it is exclusively about counting and not accounting, as if counting votes efficiently without taking the dimensions and the quality of the witnessing into account was possible, brings with it major political consequences. One of them is that when Election Observation Bodies approve of election results, for instance on the basis of the Council of Europe's Recommendation on legal, operational and technical standards for e-voting, or on the basis of the Decryption and Counting Ceremony, they implicitly also approve of the radical changes in the way witnessing takes place, but without addressing this explicitly.

[6]We owe this expression to Ingvar Tjøstheim, personal communication.

As it is well known by now, the Norwegian government decided to stop the internet trials [18], based on the arguments that the parliament disagreed on the subject, and this subject was considered too important to allow for disagreement. Besides this, they stressed that ordinary voters do not understand the mechanisms involved in internet voting [18]. This is, of course, a perfectly legitimate way of expressing a political standpoint. We do not know whether the experiences of the politicians involved in the ceremony have had a say in this argument, but common experience as well as analyses such as the OSCE report [22] certainly support the idea that ordinary citizens do not usually understand this voting mode. These arguments are indeed important from a democratic point of view. But in addition, we would like to argue that an analysis of the economy of truth that takes the new conditions of witnessing into account would provide critics, as in this case the government, with additional arguments. These arguments would in turn point to some of the conditions internet voting depends on, by opening the back-box of how the counting, and hence the accounting, take place. It would eventually make the radical changes in the way democracy is understood more obvious in terms of public involvement. The point we want to make, based on the guidelines that Shapin's idea of trust and the economy of truth provide, is that it is possible to explore political and social aspects in the process as well as sketch what the IT community is doing, and what ordinary people arguably do not understand. The argument does not so much point to missing competences among the voters, but informs about the process and the kind of public involved in the internet voting experiment. Seeing is not necessarily believing, trust and distrust go hand in hand according to Shapin, and we may reject the idea of trusting people and arrangements, if we do not know how to relate to them. The argument also suggests proponents of internet voting to be explicit about the vision of democracy that they carry with them in terms of witnessing, among other things. Currently it seems that the idea of proxy is well accepted in the community of observers, as a logical consequence of the competences and complexities involved in internet elections and deciding about the efficiency in counting votes, but less discussed within a political context: Is this what people and their representatives in Norway or elsewhere want?

VI. Concluding Remarks

The Ministry of Local Government and Regional Development of Norway organized on election day a Decryption and Counting Ceremony in the internet voting trials of 2011 and 2013. Starting from the organizers' declared perception of the ceremony in 2013, as an effort to sustain trust in internet voting, we have introduced a pragmatic approach to trust, that underlines the inseparability of truth from the witnessing of how it is brought about. We have suggested that academic or political communities can also shape the economy of truth, including their systems of takings-for-granted in how they view the world. Based on this approach as well as a description of how the event is organized in terms of an overseeing body, the IEC, and a group of appointed verifiers, this paper has examined how the organizers made the event observable to the audience and emphasised the complexities in decrypting and counting votes as well as the specific framing of the event by the IT community.

We have also discussed the limits in trying to make sense

of the event exclusively from a technical counting perspective, and explored a broader understanding of truth-making and trust-making by including a discussion of the witnessing process and the idea of making it public. We have suggested that exploring a pragmatic approach to truth and trust may be helpful in the e-governance community, as well as in other communities engaged in the idea of trust in technology. More specifically, we believe that any government considering to adopt internet voting may benefit from taking on the job of articulating social and political perspectives on internet voting. This will bring two advantages. First, it will help with refining the requirements of the internet voting architecture, by creating a space for discussing how to improve the technical performance, by mechanisms other than zero-knowledge proofs, for example advanced logging infrastructures, time stamping, distribution, redundancy, and risk-limiting audits. Second, and just as importantly, it should articulate explicitly how witnessing is brought about, to what extent a public can take shape and how those processes transform the basis for representative democracy.

ACKNOWLEDGMENT

The authors were supported in part by the DemTech grant 10-092309 from the Danish Council for Strategic Research, Program Commission on Strategic Growth Technologies. The authors would also like to thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

[1] R.M. Alvarez, T.E. Hall, A.H. Trechsel. *Internet Voting in Comparative Perspective: The Case of Estonia*. Political Science and Politics, 42, pp. 497–505, 2009.

[2] J. Barrat i Esteve, B. Goldsmith, N. Turner. *International Experience with e-voting: Norwegian E-Vote Project*. IFES, June 2012.

[3] J. Barrat i Esteve, B. Goldsmith. *Compliance with International Standards: Norwegian E-Vote Project*. Washington, DC: IFES, 2012.

[4] C. Barry, I. Brightwell, L. Franklin. *iVote, Technology Assisted Voting*. Electoral Commission of New South Wales, November 2013.

[5] P.V.D. Besselaar, A. Oostveen, F.D. Cindio, D. Ferrazzi. *Experiments with E-Voting Technology: Experiences and Lessons*. Building the Knowledge Economy: Issues, Applications, Case Studies, IOS Press, 2003.

[6] C. Bull. *Safety first! Verifiability in the Norwegian e-voting System*. Seminar on Internet Voting, Norway, September 8, 2013.

[7] Expert Study Mission Report, *Internet Voting Pilot: Norway's 2013 Parliamentary Elections*. The Carter Center, March 19, 2014.

[8] The Electoral Knowledge Network. *Elections and Technology, Guiding principles*. aceproject.org/main/english/et/et20.htm (accessed 4 August 2014)

[9] T. ElGamal. *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Trans. on Inf. Th., 31 (4), pp. 469–472, 1985.

[10] Estonian Internet Voting Committee, videos (in Estonian). www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ/videos (accessed 4 August 2014)

[11] K. Gjøsteen. *The Norwegian Internet Voting Protocol*. IACR Cryptology ePrint Archive 2013, 473.

[12] J.A. Halderman, H. Hursti, J. Kitcat, M. MacAlpine, T. Finkenauer, D. Springall. *Security Analysis of the Estonian Internet Voting System*. Technical report, May 2014. estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf (accessed 4 August 2014)

[13] W. James. *Pragmatism*. Buffalo, N.Y., Prometheus Books, pp. 88–91, (1907) 1991.

[14] Kommunal og Regionaldepartamentet. *Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities*. June 19, 2013.

[15] D. MacKenzie. *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, 2001.

[16] Ministry of Local Government and Regional Development. *Internettvalstyret er oppnemnd*. Press release. June 20, 2013. (in Norwegian) www.regjeringen.no/en/archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/Nyheter-og-pressemeldinger/pressemeldinger/2013/internettvalstyret-er-oppnemnd-.html?id=731211 (accessed 26 May 2014)

[17] Ministry of Local Government and Regional Development. *Decryption and counting ceremony of the Internet votes, video.* (English language). www.regjeringen.no/en/dep/krd/Whats-new/news/2013/dekryptering--og-opptelling-av-internett.html?id=735379 (accessed 26 May 2014).

[18] Ministry of Local Government and Regional Development. *Ikke flere forsøk med stemmegivning over Internett*. Press release. June 23, 2014. (in Norwegian) www.regjeringen.no/nb/dep/kmd/pressesenter/pressemeldinger/2014/Ikke-flere-forsok-med-stemmegivning-over-Internett-.html?id=764300 (accessed 4 August 2014)

[19] News about the Norwegian e-voting trial in 2011 (in Norwegian). www.regjeringen.no/nb/dep/kmd/prosjekter/e-valg-2011-prosjektet/nyttomevalg/nytt-om-e-valg/2011.html?id=631622 (accessed 27 May 2014).

[20] OECD's Better Life Index. oecdbetterlifeindex.org/countries/norway (accessed 31 July 2014)

[21] OSCE/ODIHR, *Estonia: Parliamentary Elections 6 March 2011*. Election Assessment Mission Report. May 16, 2011.

[22] OSCE/ODIHR, *Norway: Parliamentary Elections 9 September 2013*. Election Assessment Mission Final Report. December 16, 2013.

[23] S.B. Segaard, H. Baldersheim, J. Saglie. *E-valg i et demokratisk perspektiv* Rapport (2012:005) Institutt for samfunnsforskning, Oslo, 2012.

[24] S.B. Segaard, D.A. Christensen, B. Folkestad, J. Saglie. *Internettvalg, hva gjør og mener velgerne?*, Rapport 2014:07, Institutt for samfunnforskning, Oslo, 2014.

[25] A. Shamir. *How to share a secret*. Communications of ACM 22, November 11, pp. 612–613, 1979.

[26] S. Shapin. *The Social History of Truth. Civility and Science in Seventeenth-Century England*. The University of Chicago Press, USA, 1994.

[27] J. Simon. *Trust*. Oxford Bibliographies in Philosophy, Oxford University Press, New York, 2013. www.oxfordbibliographies.com/view/document/obo-9780195396577/obo-9780195396577-0157.xml (accessed 4 August 2014)

[28] O. Spycher, M. Volkamer, R. Koenig. *Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting*. VoteID'11, Tallin, Estonia, 2011.

[29] I.G. Stenerud, C. Bull. *When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting*. Proceedings of EVOTE2012, LNI GI Series, Bonn.

[30] A.L. Strauss. *Continual Permutations of Action*. New York, Aldine de Gruyter, 1993.

[31] M. Volkamer, O. Spycher, E. Dubuis. *Measures to Establish Trust in Internet Voting*. ICEGOV'11, Tallin, Estonia, 2011.

[32] K. Vollan. *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys*, Version 0.1 DRAFT. The Internet Voting Board Representative: Internet Voting Trial 2013, August 26, 2013.

[33] M. E. Warren. *Democracy and Trust*, Cambridge University Press, 1999.

Auditing and Verifiability

Proving the Monotonicity Criterion for a Plurality Vote-Counting Program as a Step Towards Verified Vote-Counting

Rajeev Goré
The Australian National University

Thomas Meumann
The Australian National University

***Abstract*—We show how modern interactive verification tools can be used to prove complex properties of vote-counting software. Specifically, we give an ML implementation of a vote-counting program for plurality voting; we give an encoding of this program into the higher-order logic of the HOL4 theorem prover; we give an encoding of the monotonicity property in the same higher-order logic; we then show how we proved that the encoding of the program satisfies the encoding of the monotonicity property using the interactive theorem prover HOL4. As an aside, we also show how to prove the correctness of the vote-counting program. We then discuss the robustness of our approach.**

I. Introduction

Paper-based elections consist of three main phases: printing and transporting ballot papers to polling places; collecting and transporting ballots after polling; and hand-counting ballots centrally to determine the result. Our confidence in the result is based on blind trust and scrutiny. We trust electoral officials to act honestly, but allow scrutiny by observers from political parties and independent organisations when ballots are transported, opened, and counted. That is, we rely on the difficulty of compromising all of these different non-centralised entities simultaneously. Such elections are slow to announce results, are (becoming) prohibitively expensive and impinge on the privacy of impaired voters who must be assisted by others to cast their vote. Paper ballots and hand-counting are therefore being replaced, gradually, by electronic alternatives [1], and although such vote-casting and vote-counting are very different aspects, they are often conflated into the term electronic voting.

End-to-end voter-verifiable systems attempt to provide full confidence by verifying the processed output of each phase rather than actually verifying any computer code. Such systems allow voters to verify that: their votes are cast correctly into a digital ballot; that these digital ballots are transported from the polling place to the central vote-counting authority without tampering; and that their digital ballot appears in the final tally. The methods used to guarantee these properties invariably involve sophisticated cryptographic methods, including methods for computing the sum of the encrypted votes without having to decrypt the votes themselves. But such cryptographic methods only work when the tallying process is a simple sum. No currently implemented "end to end voter-verifiable" system [2]–[5], can guarantee that votes are counted correctly using a complex preferential vote-counting method such as single transferable voting (STV). Thus there is no simple way to verify the output of the process of vote-counting using STV.

The accepted wisdom for elections that involve complex preferential vote-counting methods, such as STV, is to publish the ballots on a web page so that they can be tallied by multiple different implementations, built by interested (political) parties. That is, in e-voting, it is not the code that we should verify, but the processed output. For example. the Australian Electoral Commission (AEC) uses a computer program to count votes cast in senate elections. The program has been "certified" by a commercial certification company after conducting some testing, but has not been verified in any formal sense. The AEC makes the votes public but has refused to make the code public. Antony Green, a journalist and electoral commentator, has built his own implementation of the STV method used to count the votes. The only known "scrutiny" of the results of the previous senate election is the fact that Green's code produced the same results as those produced by the AEC computer code.

But what if the official results from the AEC differ from those of Green, or from those of the political party that loses? In particular, what if the losing party appeals to the court of disputed returns? There is no reason why the results of the AEC should be accepted over those of others. Do we resort to time-consuming and error-prone hand-counting to resolve the discrepancy? Or do we commission someone to write yet another program? Or do we enter a complex court case to argue the pros and cons of the two implementations? None of these options will engender confidence in the result, let alone e-voting itself. But if the AEC used a computer program that had been formally verified as correct, there would be a strong case to reject the conflicting results from other computer programs.

Thus, given the complexity of preferential vote-counting methods like STV, even the most secure and most sophisticated end-to-end voter-verifiable system will still fail to gain the trust of voters if it cannot guarantee that votes are not only cast correctly and transported without tampering but that they are also counted correctly.

Here, we focus on verified vote-counting where "verification" is the process of proving that an actual computer program correctly implements a formal specification of some desirable property. We first explain the various forms of software verification that are possible today and briefly explain the pros and cons of these approaches. We then describe our work on verifying that a computer program for counting votes according to a simple plurality voting scheme meets Arrow's monotonicity criterion. We also prove that the program counts votes correctly, which in this case, turns out to be relatively

simple. The case study nicely highlights the issues involved in formal verification of software.

How does our work tie into the electoral process and how does it help to improve it?

Most preferential vote-counting methods are simplified to make it possible to count the ballots by hand since humans are notoriously bad at such mechanical tasks. The greatest simplifications are usually made to the way ballots are transferred from one candidate to another even though the simplifications are known to engender some unfairness in the final tally. Simplifications are also made in tracing back through the previous rounds when breaking ties, again even though quite simple examples can be constructed which show that these approximations can lead to unfairness. Sometimes, the result can come down to a simple coin toss at some crucial juncture.

The ability to count votes using computers opens up the possibility to design new, even more complex, voting schemes which guarantee various theoretical desiderata, and to use them in real elections. How can we be sure that the new schemes enjoy the desired properties while remaining practical for counting by computer for large numbers of votes? More importantly, how can we convince voters that the safety-net provided by hand-counting is no longer necessary?

One way is to develop the voting scheme incrementally and iteratively. By starting with a simple implementation and a specification of a desired property, such as a fairness, and gradually adding complexity, we can iron out errors in the implementation and specification, and gain insights into the practicality of the desired theoretical desiderata. By involving electoral officials in this iterative process, we can ensure that they are convinced that the implementations meets the desired criteria beyond any doubt. Correctness is just one such criteria.

Our work has the potential to revolutionise elections using preferential methods of voting since it allows us to produce fairer, but necessarily complex, versions of vote-counting and produce computer programs that are guaranteed to implement these complex vote-counting methods correctly.

II. Various forms of Software Verification

Modern software verification methods can be broadly classified into two main categories which we shall call "light-weight" and "heavy-weight" for want of better terms.

Light-weight methods range from the fully automatic methods like software bounded model checking (SBMC) to full functional software verification using automatic annotation-based program verification tools such as VCC [6]. Both SBMC and annotation-based program verification tools involve adding the properties to be checked as pre and post condition annotations to the actual code, turning these annotations automatically into proof obligations by a compiler, and discharging the proof obligations automatically by some theorem prover. Their main advantage is that the proof-obligations are discharged fully automatically. Thus the user may have to learn some basics of how to annotate programs with pre- and post-conditions, and how to operate the verification tool, but the user does not have to be an expert in logic and formal proof. Their biggest disadvantage is that there is usually little that can be done when the verification tool fails to discharge the required proof obligations automatically. Even when the proof obligations are discharged automatically, there is no guarantee that the tool itself is sound or complete, lowering the trust that can be placed in the correctness of the program.

Heavy-weight verification involves encoding both the implementation and the specification into the logic of some theorem prover, and then proving that the encoding of the implementation implies the encoding of the specification using that theorem prover, usually interactively. The biggest advantage of this method is that we can trust the final proof completely. The disadvantage is that the user has to be expert in logic and formal proof.

III. Heavy-weight Verification Using HOL4

The verification process explored here falls under the rubric of heavy-weight verification. It involves producing a logical formalisation of both the program's requirements and the program itself in the HOL4 theorem proving assistant, then constructing a formal proof showing that the program matches the requirements. Why should we trust the HOL4 theorem proving assistant?

HOL4 is an (interactive) theorem prover based upon Dana Scott's "Logic for Computable Functions" (LCF), a mathematically rigorous logic engine consisting of 8 primitive inference rules which have been proven to be mathematically correct [7]. HOL4 implements this logic engine using approximately 3000 lines of ML code. This code has been scrutinised by experts in LCF to ensure that it correctly implements the 8 inference rules. Any complex inference rules must be constructed from the core primitive rules only. This means that proofs produced in HOL4 are highly trustworthy.

A side-effect of using an LCF-style proof assistant is that the program must be represented in higher-order logic. It thus becomes possible to prove various results about the program. This can be used to verify the voting scheme itself with respect to various desiderata. For example it would be possible to prove that the voting scheme in question adheres to the independence of irrelevant alternatives (see [8]). It is also possible to prove comparative results between different voting schemes: for instance that voting scheme A differs from voting scheme B in only x specific situations. The ability to reason about the program in this manner is what makes this process suited to the design of fairer voting schemes which can be rigorously tested against any desired properties.

IV. Case Study

As a case study, we implement a program for plurality vote-counting, verify that it obeys the monotonicity criterion, and also prove that it counts votes correctly.

A. Plurality Voting

First-past-the-post plurality voting is a voting scheme wherein each voter may vote for one candidate only, usually by marking a cross or a tick next to the desired candidate on the ballot paper. The number of votes for each candidate is tallied, and the candidate with the most votes (a relative majority) is declared elected. Note that the candidate does not need an absolute majority. Real-world voting systems vary in the way

they deal with a tie, but in our simple case, no candidate is elected in the case of a tie.

B. The Monotonicity Criterion (MC)

The monotonicity criterion was originally posited by Arrow as a property of social welfare functions as follows [8]:

> "If an alternative social state x rises or does not fall in the ordering of each individual without any other change in those orderings and if x was preferred to another alternative y before the change in individual orderings, then x is still preferred to y."

A social choice procedure, such as a voting scheme or a market mechanism, can be said to either satisfy this condition or not. Reducing the available social choice procedures to preferential voting schemes or a subset thereof allows us to narrow the definition and put it in more tractable language. Thus for our purpose: "social state" is the election of a particular candidate; and "x is preferred to y" refers to a societal preference and can be changed to "x is elected".

In our plurality system, voters may only vote for one candidate, ie. rank one candidate above all others (rejecting all others equally). Thus monotonicity can be rewritten as:

> If each voter either changes his or her vote to a vote for candidate x or maintains his or her vote unchanged, and x won before any votes changed, then x will still win after the changes.

C. Verification

The verification method involves producing a logical formalisation of both the program's requirements (the vote-counting legislation) and the program itself, then constructing a formal proof showing that the software matches the specification, using HOL4.

In other words, the proof procedure involves producing the following, step-by-step:

1) Implementation: An implementation in SML of the plurality vote-counting scheme.
2) Translation: A translation of the implementation into HOL4's formal logic.
3) Specification: An encoding of MC in HOL4's logic.
4) Proof: A proof acceptable to the HOL4 theorem prover that the specification (3) holds of the translation (2).

Each of these steps is explored individually below.

1) Implementation: A plurality vote-counting program has been written in StandardML (SML), a strict functional programming language. The SML code for the plurality counting program is given in Figure 1.

This implementation makes use of the `option` type operator. Specifically, `ELECT` returns a value of type `num option`. `WINNER` also makes use of the `num option` datatype. The `option` type operator is acting in both cases as a wrapper around type `num` to allow the program to return either a number (as `SOME` c) or the lack thereof (`NONE`). The statement `SOME` c is *not* shorthand for "there exists some c".

For simplicity, each candidate is represented by a number from 0 to $(C-1)$, and the set of votes by a list of numbers: each representing a vote for the numbered candidate. Let c_i be the i^{th} candidate and v_j be the j^{th} vote. A vote v_j is a vote for c_i iff the j^{th} member of the list `v` is equal to i. If $v_j < 0$ or $v_j \geq n$ where n is the number of candidates, then v_j is invalid.

Our implementation runs in $O(cv)$ time with number of candidates c and number of votes v. A $O(c+v)$ implementation is possible, but it was kept this way in order to maintain the program's functional purity and simplicity (thereby making it easier to reason about). Theoretically, the same results are provable of a $O(c+v)$ implementation but this is not explored here.

2) Translation into HOL4: Figure 1 shows the implementation translated into recursive definitions in HOL4. The translation between SML and HOL4 was done by hand, but was a purely mechanical process. Bar a few small syntactic differences, the translation clearly syntactically matches the SML implementation. Whether the HOL4 translation matches the SML implementation semantically is somewhat less clear. This issue is explored in more detail in section VI.

Note that the translation is a statement in higher order logic, not a program in the traditional sense. This is why the HOL4 function definitions consist of conjunctions (`/\` is the HOL4 syntax for logical 'and').

3) Specification: Formally stated in higher-order logic, the definition of monotonicity given on page 3 becomes:

$$\begin{aligned}
&\forall C\, w\, v\, v'.\ \Big((\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \\
&\wedge\ \big(\forall n.\, n < \texttt{LENGTH}\, v \Rightarrow (\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v')\big) \\
&\qquad\qquad \wedge\ (\texttt{ELECT}\, C\, v = \texttt{SOME}\, w)\Big) \\
&\qquad\qquad\qquad\qquad \Rightarrow (\texttt{ELECT}\, C\, v' = \texttt{SOME}\, w) \quad (1)
\end{aligned}$$

where:

- v is a list representing the set of initial votes;
- v' is a list representing the set of changed votes;
- w is a number representing the winning candidate;
- C represents the number of candidates;
- `LENGTH` l is the length of list l; and
- `EL` n l is the n^{th} element of list l, where $0 \leq n <$ `LENGTH` l.

Note that `LENGTH` and `EL` are predefined recursive functions in HOL4 and `EL` $0\ (h :: t) = h$. That is, the members of the list are numbered from 0, not 1.

The first conjunct in the antecedents of the implication (the first line) states that the number of votes cannot change. The second conjunct (second line) states that each vote in the set of changed votes must be a vote for the winner, or the same as the corresponding initial vote, or both. The third conjunct (third line) states that there is a winner from the set of initial votes. The final line states that these conjuncts together imply that the winner still wins with the changed votes.

```
local
  (* Counts the number of votes in the
     given list for candidate c. *)
  fun COUNTVOTES c []     = 0
    | COUNTVOTES c (h::t) = if h = c
                        then 1 + COUNTVOTES c t
                        else 0 + COUNTVOTES c t;

  (* Finds winner from all candidates
     numbered c or lower. *)
  fun WINNER 0 v = (SOME 0, COUNTVOTES 0 v)
    | WINNER c v =
      let
        val numvotes = COUNTVOTES c v
      in
        let
          val (w, max) = WINNER (c-1) v
        in
          if numvotes > max
            then (SOME c, numvotes)
          else if numvotes = max
            then (NONE, max)
          else (w, max)
        end
      end;
in
  (* C is the number of candidates, v is the
     list of votes *)
  fun ELECT C v = if C <= 0 then NONE
                  else #1 (WINNER (C-1) v)
end;
```

(a) SML

```
val COUNTVOTES_def = Define `
  (COUNTVOTES c []     = 0) /\
  (COUNTVOTES c (h::t) = if (h = c)
                    then 1 + COUNTVOTES c t
                    else 0 + COUNTVOTES c t)`;

val WINNER_def = Define `
  (WINNER 0 v = (SOME 0, COUNTVOTES 0 v)) /\
  (WINNER c v =
    let
      numvotes = COUNTVOTES c v
    in
      let
        (w, max) = WINNER (c-1) v
      in
        if numvotes > max
          then (SOME c, numvotes)
        else if numvotes = max
          then (NONE, max)
        else (w, max))`;

val ELECT_def = Define `
  ELECT C v = if C <= 0 then NONE
              else FST (WINNER (C-1) v)`;
```

(b) HOL4

Fig. 1: Implementation of a plurality counting algorithm (a) in SML, and (b) translated into HOL4.

4) Proof: The entire proof was completed using the HOL4 theorem prover. Rather than explaining the syntax of HOL4 and how it corresponds to higher-order logic, all of the formulae in this section are given using standard higher-order logic syntax.

Let ϕ be defined as follows:

$$\phi = \Big(\big(\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v\big) \wedge \big(\forall n.\, n < \texttt{LENGTH}\, v \Rightarrow (\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v')\big)\Big) \tag{2}$$

This allows us to rewrite the proof obligation (1) as:

$$\forall C\, w\, v\, v'.\, \big(\phi \wedge (\texttt{ELECT}\, C\, v = \texttt{SOME}\, w)\big) \Rightarrow (\texttt{ELECT}\, C\, v' = \texttt{SOME}\, w) \tag{3}$$

C is either 0 or the successor to some number (ie. $\texttt{SUC}\, x$). Examining these cases and applying some basic substitution allows us to rewrite the proof obligation (3) in terms of WINNER:

$$\forall c\, w\, v\, v'.\, \big(\phi \wedge (\texttt{FST}\, (\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \Rightarrow (\texttt{FST}\, (\texttt{WINNER}\, c\, v') = \texttt{SOME}\, w) \tag{4}$$

The new proof obligation is that at any stage of the recursion: if w beats all other candidates examined so far with the initial votes, then w beats the same candidates with the changed votes.

To get to the core of the problem, it is desirable to go one step further and rewrite the proof obligation in terms of COUNTVOTES. In order to do this, we need a formula relating WINNER and COUNTVOTES. The following lemma states that if w beats all candidates numbered c or less, then w also has more votes than all of the said candidates and vice versa. The proof of this lemma relies upon inductive proofs of various properties of WINNER:

$$\forall c\, v\, w.\, w \leq c \Rightarrow \big((\texttt{FST}\, (\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) \iff \forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v\big) \tag{5}$$

The proof obligation (4) can thus be rewritten in terms of COUNTVOTES as follows:

$$\forall c\, w\, v\, v'.\, \big(\phi \wedge (\forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v)\big) \Rightarrow (\forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v' > \texttt{COUNTVOTES}\, c'\, v') \tag{6}$$

In other words we need to prove that if w has more votes than the set of lesser-numbered candidates using the initial votes, and the conditions in ϕ hold, then w also has more votes than all the aforementioned candidates using the changed votes. A structural case analysis of v and v' can now be performed (the lists being either empty or having a head and tail).

In order to make the proof fall all the way through it is necessary to prove the following properties of `COUNTVOTES`:

$$\forall w\, v\, v'.\ \phi \Rightarrow \texttt{COUNTVOTES}\ w\ v' \geq \texttt{COUNTVOTES}\ w\ v \quad (7)$$

$$\forall w\, v\, v'.\ \phi \Rightarrow (\forall c.\ c \neq w \Rightarrow \texttt{COUNTVOTES}\ c\ v \geq \texttt{COUNTVOTES}\ c\ v') \quad (8)$$

Appendix A lists all the lemmas involved in the proof and a diagram of their inter-dependencies.

V. Correctness

The astute reader will have noticed that we have not proved the correctness of our encoding of our implementation by proving that the winner is the candidate with the most number of votes. The HOL4 formula to capture this correctness statement is:

$$\forall C\, v\, w.\ w < C \Rightarrow (\texttt{ELECT}\ C\ v = w \iff \forall c'.c' \neq w \wedge c' < C \Rightarrow \texttt{COUNTVOTES}\ w > \texttt{COUNTVOTES}\ c') \quad (9)$$

Given the lemmas proved during the proof process for the monotonicity criterion, this is a quick and easy process. It has been left out for brevity.

VI. Summary and Discussion

There are two aspects worth considering when evaluating the feasibility of our verification process: the effort involved and whether the proof actually covers everything that is required. We address each in turn.

We have proved that our recursive definitions in HOL4 match our encoding of MC. Syntactically, our SML program appears equivalent to our recursive definitions. Semantic equivalence is another matter. We have no formal guarantee that our SML implementation is equivalent to our HOL4 translation, except for their syntactic similarity.

A particularly illuminating example of this conundrum is the difference between HOL4's and SML's handling of numerical types. In both programs, the candidates are represented by numbers. SML uses integers by default, which can be positive or negative: `~1`, `0`, `1`, `2` etc. HOL4, on the other hand, uses Peano numbers, which can only be `0` or the successor to some number. That is, they can only be positive: `0`, `SUC 0`, `SUC (SUC 0)` etc. The underlying representation would not matter if the same operations were defined and those operations had the same effect. This is not the case, however. $0 - 1 = 0$ is provably correct in HOL4, whilst `0 - 1` will result in `~1` in SML (`~` is unary negation in SML so `~1` means -1). We are safe however, since our SML implementation deals only with positive integers.

One way to get around this is to execute the HOL4 definitions directly. After all, the encoding in HOL4 is itself executable using HOL4's deductive rewriting engine. Unfortunately there is a large loss in efficiency when using this method. The SML implementation takes less than 7 minutes, using less than 10.5 GiB of memory, to count 250 *million* votes with 160 candidates. By contrast, with the same number of candidates, the HOL4 translation takes 40 minutes, using 14 GiB of memory, to count 25 *thousand* votes. Also, since the logical statements must be built up using the primitive core rules of logic, it is impractical to convert a list of votes into a logical statement acceptable to HOL4.

Another way would be to write the HOL4 specification first, and automatically produce the SML implementation using a verified compiler. This is a non-trivial task. There is, in fact, a project underway aimed at automating this translation: CakeML (https://cakeml.org/) [9]. It is currently under development so is not explored here, but may in future provide the missing link required.

Currently, our confidence in the correctness of our SML program rests completely on the syntactic similarity between the SML code and its HOL4 encoding, and the assumption that syntactic similarity implies semantic equivalence. As explained above, this holds for the case study explored here. For more complex voting schemes, we envisage that an iterative process may be necessary to reduce the syntactic differences between the SML code and its encoding in HOL4 (under the assumption that syntactic similarity implies semantic equivalence). This may require extending the HOL4 theorem prover to include more complex constructs from SML which may be needed to efficiently implement more complex voting schemes.

The entire process from implementation to complete verification took 3 weeks. Bear in mind that this was a learning process, with only 1–2 months-worth of prior experience with HOL4. Ultimately, 3 weeks is a short time to spend producing a piece of fully formally verified software. How this scales to more complex problems remains to be seen.

Another measure of the effort involved is the proof-to-implementation ratio, measured in lines of code (LoC). The implemented algorithm spans 24 lines whilst the proof spans 590. This gives at least 24 lines of proof for each line of implementation. Unfortunately, the final LoC measurement does not take into account the effort expended in exploring unproductive proof strategies. This makes its applicability here questionable. Nevertheless, it may be helpful when comparing the procedure to other verification methods. Assuming the ratio can be extrapolated to larger programs, verifying a 100-line program would require 2400 lines of verification.

It is also worth noting that the methodology here is not well suited to rapid prototyping. In particular, an indeterminate amount of time can be spent attempting to prove an invalid property before realising it is impossible.

VII. Conclusion

Given the simplicity of the algorithm for plurality voting, it is questionable whether our formal proof of correctness is significant. Note, however, that the proof that our plurality voting algorithm obeys monotonicity is far from trivial. Thus our procedure for fully formally verifying complex properties of vote counting algorithms is clearly feasible for small simple

algorithms. It remains to be seen whether the procedure will scale to complex proportional representation systems.

The verification approach took roughly 10 weeks of full time work: 7 weeks of learning HOL4 and 3 weeks to specify and verify the code. Given the trustworthiness of the HOL4 proof assistant and the associated rigorousness of the proof, this seems a small price to pay. However, the following caveats apply. We verified a HOL-encoding of an SML program, not the SML program itself, so we have no proof of their equivalence. A visual comparison is compelling for the simple case we examined here, but might not be for a complex STV voting scheme used in real elections. The HOL4 encoding of plurality voting is itself executable, but is only feasible for small-scale elections. The CakeML project, currently under active development, may provide a solution that could be used to bridge this gap. Also, the interactive proof methodology does not lend itself to rapid prototyping since it does not provide counter-examples. Indeed, one can spend an inordinate amount of time trying to prove false conjectures before realising that they are indeed false.

VIII. Further Work

Our aim in the future is to extend this case study to formally verify the correctness of an SML implementation of Hare-Clark, a complex STV voting scheme used in a number of jurisdictions around the world, including Ireland, Australia and New Zealand.

Since submitting this paper, we have encoded the Hare-Clark Act which specifies the STV method used to count votes in the Australian state of Tasmania into approximately 800 lines of HOL. We have also written a matching program of approximately 200 lines of SML to count votes according to this method and have encoded the SML program into HOL. We were able to keep the syntactic similarity between the HOL encoding of the SML program and the SML program itself so we are confident that the HOL encoding captures the program correctly. Tests show that our SML program can easily count 0.5 million votes for 10 candidates in approximately 0.5 seconds. It remains to prove inside HOL4 that the HOL encoding of the SML program implies the HOL encoding of the Hare-Clark Act. We are therefore confident that the methodology outlined here will scale to allow us to formally verify complex real-world instances of STV as used in various jurisdictions around the world.

Acknowledgment

We thank Dr Jeremy Dawson for his guidance in the use of the HOL4 theorem prover.

References

[1] D. W. Jones and B. Simons, *BROKEN BALLOTS: Will Your Vote Count?* CSLI Publications, Stanford, USA, 2012.

[2] Pret-A-Voter, "Prêt à Voter," http://www.pretavoter.com/, Accessed January 28, 2013.

[3] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Security and Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[4] Helios, "Helios," http://heliosvoting.org/.

[5] D. Chaum, A. Essex, R. T. C. III, J. Clark, S. Popoveniuc, A. T. Sherman, and P. Vora, "Scantegrity: End-to-end voter verifiable optical-scan voting," *IEEE Security & Privacy*, vol. 6, no. 3, pp. 40–46, 2008.

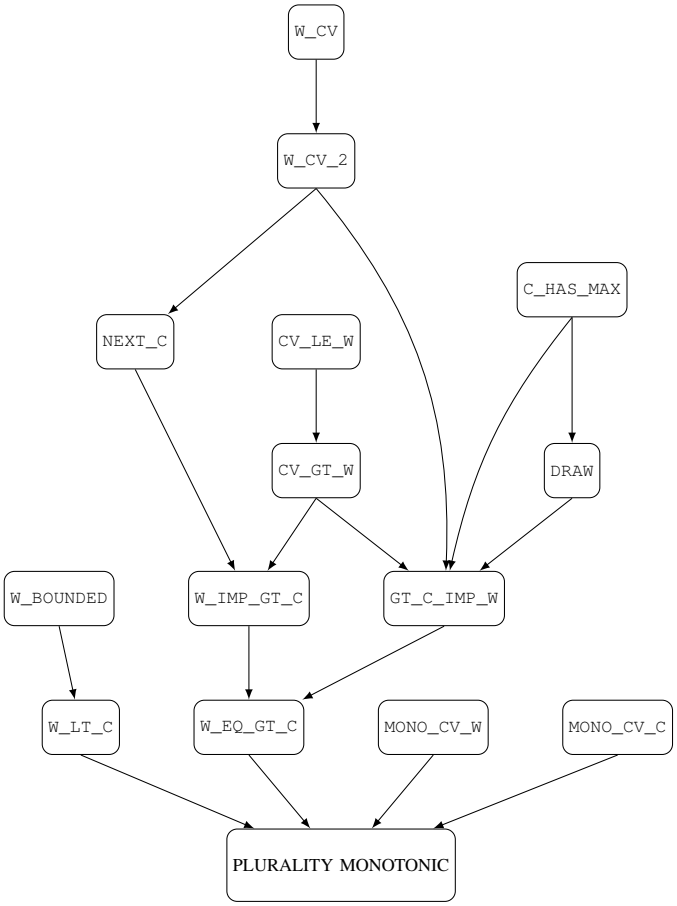


Fig. 2: Dependencies between lemmas. The proof of a lemma at the destination of an arrow relies upon the lemma at the arrow's origin.

[6] E. Cohen, M. Dahlweid, M. Hillebrand, D. Leinenbach, M. Moskal, T. Santen, W. Schulte, and S. Tobies, "VCC: A practical system for verifying concurrent C," in *Theorem Proving in Higher Order Logics*, ser. Lecture Notes in Computer Science, S. Berghofer, T. Nipkow, C. Urban, and M. Wenzel, Eds. Springer Berlin Heidelberg, 2009, vol. 5674, pp. 23–42. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03359-9_2

[7] M. J. C. Gordon and T. F. Melham, *Introduction to HOL: a theorem proving environment for higher order logic*. CUP, 1993.

[8] K. J. Arrow, "A difficulty in the concept of social welfare," *Journal of Political Economy*, vol. 58, no. 4, pp. pp. 328–346, 1950.

[9] R. Kumar, M. O. Myreen, M. Norrish, and S. Owens, "Cakeml: a verified implementation of ML," in *POPL*, 2014, pp. 179–192.

Appendix

The following is a full listing of each lemma proved during the HOL4 proof. Figure 2 shows the dependencies between the various lemmas. See Section IV-C4 for an explanation of the proof.

`CV_LE_W`:

$$\forall c\, v\, c'.\ c' \leq c \Rightarrow \texttt{COUNTVOTES}\ c'\ v \leq \texttt{SND}\ (\texttt{WINNER}\ c\ v) \quad (10)$$

CV_GT_W:

$$\forall v\, c\, c'.\ c' < \texttt{SUC}\, c \wedge \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v > \texttt{SND}\,(\texttt{WINNER}\, c\, v) \Rightarrow \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v > \texttt{COUNTVOTES}\, c'\, v \quad (11)$$

W_BOUNDED:

$$\forall c\, v\, c'.\ c' > c \Rightarrow (\texttt{FST}\,(\texttt{COUNTVOTES}\, c\, v) \neq \texttt{SOME}\, c) \quad (12)$$

W_CV:

$$\forall c\, v\, w\, m.\ (\texttt{WINNER}\, c\, v = (\texttt{SOME}\, w, m)) \Rightarrow (\texttt{COUNTVOTES}\, w\, v = m) \quad (13)$$

W_CV_2:

$$\forall c\, v\, w.\ (\texttt{SOME}\, w = \texttt{FST}\,(\texttt{WINNER}\, c\, v)) \Rightarrow (\texttt{COUNTVOTES}\, w\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \quad (14)$$

NEXT_C:

$$\forall v\, w\, c.\ (\texttt{SOME}\, w = \texttt{FST}\,(\texttt{WINNER}\, c\, v)) \wedge \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v < \texttt{SND}\,(\texttt{WINNER}\, c\, v) \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v \quad (15)$$

W_IMP_GT_C:

$$\forall c\, v\, c'\, w.\ \big((c' \neq w) \wedge (c' \leq c) \wedge (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v \quad (16)$$

C_HAS_MAX:

$$\forall v\, c.\ \exists c'.\ c' \leq c \wedge (\texttt{COUNTVOTES}\, c'\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \quad (17)$$

DRAW:

$$\forall v\, c.\ (\texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \Rightarrow \exists c'.\ c' \leq c \wedge (\texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v = \texttt{COUNTVOTES}\, c'\, v) \quad (18)$$

GT_C_IMP_W:

$$\forall c\, v\, w.\ w \leq c \Rightarrow \big((\forall c'.\ c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v) \Rightarrow (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \quad (19)$$

W_EQ_GT_C:

$$\forall c\, v\, w.\ w \leq c \Rightarrow \big((\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) = (\forall c'.\ c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v)\big) \quad (20)$$

W_LT_C:

$$\forall c\, v\, w.\ (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) \Rightarrow w \leq c \quad (21)$$

MONO_CV_W:

$$\forall w\, v\, v'.\ (\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \wedge \big(\forall n.\ (n < \texttt{LENGTH}\, v) \Rightarrow ((\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v'))\big) \Rightarrow \texttt{COUNTVOTES}\, w\, v' \leq \texttt{COUNTVOTES}\, w\, v \quad (22)$$

MONO_CV_C:

$$\forall w\, v\, v'.\ (\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \wedge \big(\forall n.\ (n < \texttt{LENGTH}\, v) \Rightarrow ((\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v'))\big) \Rightarrow \forall c.\ c \neq w \Rightarrow \texttt{COUNTVOTES}\, c\, v \geq \texttt{COUNTVOTES}\, c\, v' \quad (23)$$

Efficiently Auditing Multi-Level Elections

Joshua A. Kroll
Princeton University
Princeton, NJ 08544
kroll@cs.princeton.edu

J. Alex Halderman
University of Michigan
Ann Arbor, MI 48109
jhalderm@eecs.umich.edu

Edward W. Felten
Princeton University
Princeton, NJ 08544
felten@cs.princeton.edu

ABSTRACT

In a multi-level election, voters are divided into groups, an election is held within each group, and some deterministic procedure is used to combine the group results to determine the overall election result. Examples of multi-level elections include U.S. presidential elections and some parliamentary elections (such as those with regional groupings of voters). The results of such an election can hinge on a few votes in one group, while being insensitive to large shifts within other groups. These disparities create opportunities to focus election integrity efforts in the places where they have the highest leverage. We consider how to improve the efficiency of post-election audits, such as those that compare paper ballots to corresponding electronic records, in multi-level elections. We evaluate our proposed solutions using data from past elections.

I. Introduction

A *multi-level election* divides voters into disjoint groups, holds an election within each group, and then applies some deterministic procedure to combine the group results into an overall election result. In this paper, we discuss how to audit multi-level elections efficiently.

An important attribute of multi-level elections is that some ballots may have much more influence than others [1], [2], [3], [4]. For example, in the 2000 U.S. presidential election, a shift of 269 votes in the state of Florida would have changed the national election result, while a shift of 350,000 votes in Texas, or a shift of every vote in the most populous state, California, would not have changed the result. These non-uniformities create opportunities to focus election integrity efforts where they will do the most good. After an election, we can focus our post-election auditing resources to get the highest confidence in the overall election result, at the lowest total cost.

Post-election auditing can help to provide confidence in the integrity of an election by providing evidence that the votes were counted-as-cast. Several electronic election technologies generate redundant copies of ballot data, such as (now widely deployed) optical scan voting systems, in which voters mark paper ballots and scanned images of those ballots are tabulated electronically [5], or systems with a voter-verified paper audit trail, in which voters make a selection electronically and a copy of their selection is printed for review before being dropped automatically into a ballot box [6]. In any system with redundantly stored ballot data (e.g. electronically and on paper), we can audit by comparing the electronic record to the auxiliary record on a per-ballot basis. Generally, the electronic version of the ballot data will be much faster and cheaper to gather and tabulate and the auxiliary record will be much more costly to examine. Thus, we want to minimize the number of auxiliary records that must be examined, while also establishing high confidence that a full examination of all auxiliary records would yield the same election result as the reported electronic result. Efficient post-election auditing relies on examining a subset of the auxiliary records, comparing them to the corresponding electronic records, and relying on statistical arguments to confirm the election result to high statistical confidence.

Much prior work describes efficient approaches to ballot-based auditing in elections with simple majority or plurality rules for determining the election winner from votes cast [7], [8], [9], [10], [11], [12], [13], [14]; this work is the first to consider the case of multi-level elections and how the structure of the election's victory conditions can be used to reduce the total amount of auditing necessary to achieve a certain level of confidence.

Jones gives an overview of the need for and approaches to election auditing [15] and Dopp gives a more complete history of election auditing techniques [16].

Multi-level elections are common. One example is a U.S. presidential election, in which the voters are divided into 51 groups, one for each state.[1] Each state is assigned a certain number of electoral votes. Almost all of the states assign the state's electoral votes to the plurality winner of the state's election. (Two states, Maine and Nebraska, use a different procedure that can divide the state's electoral votes among candidates.) The states' results are combined by summing the electoral votes of each candidate. If one candidate receives a majority of electoral votes, that candidate is the winner. If no candidate receives a majority of electoral votes, then the election result is "undetermined" and the Congress holds a special vote to choose the President.

Another example is a national vote in certain parliamentary systems, where each district chooses a party representative, and representatives from the same party are assumed to act as a single coordinated bloc.[2] In such an election, the result is the identity of the party that holds a majority of seats; or lacking a single party with a majority, the result is the set of minimal coalitions, that is, a set of all of the minimal sets of parties that can form a coalition government. For example, if there are four parties, A, B, C, and D, which have 42, 29, 20, and 9 seats respectively for a total of 100 seats, then the minimal majority coalitions could be formed by parties A and B (71 seats); or by parties A and C (62 seats); or by parties A and D (51 seats); or by parties B, C, and D (58 seats).

Although the practical examples we discuss all determine the overall result by some kind of weighted counting of the individual group results, our theory is much broader than this and can handle any method for combining group results, including, for example, non-monotone systems in which winning more groups can make one's overall result worse. Our theory also extends naturally to handle elections with more than two levels.

The remainder of the paper is structured as follows. In Section II we discuss how to audit multi-level elections. In Section II-A, we work an example showing that considering an election's multi-level structure can reduce auditing costs. In Section II-B and for the rest of the paper, we develop the necessary theory to understand this phenomenon and use it to minimize overall auditing costs. We give an optimal auditing algorithm in Section II-C based on linear programming and in Section II-D, we give an approximation that is sometimes more efficient to compute. In Section II-E and Section II-F, we evaluate these methods using data from several recent elections. We finish by remarking on future work in Section III.

II. Auditing Multi-Level Elections

Post-election auditing is a statistical process for verifying, to some specified level of confidence, that the reported election result is consistent with the available evidence [15]. We assume that there is auxiliary evidence associated with each ballot which can be compared to the reported votes from that ballot, and that the auxiliary evidence is usually unexamined due to cost or time factors [8]. For example, in an optical-scan voting system, the reported results are determined by machine scanners in the polling place, and the auxiliary records are the paper ballots filled out by voters, which can be examined by hand and compared to the machine-reported results. A post-election audit will choose a sample of ballots and compare the chosen ballots with their auxiliary information. If the ballots in the sample are consistent with their auxiliary information, to within a specified tolerance, the audit succeeds; otherwise it fails and further investigation of the election is required.

The purpose of an audit is to reject by statistical means the hypothesis that a full examination of the auxiliary evidence would suggest a different overall election result than the one that was reported. This must be done to some specified level of statistical confidence (sometimes called

[1] For this purpose, the District of Columbia is treated as a state.

[2] This is not a requirement—party members may later defect on particular issues and vote with their opposition. However, we observe that when forming a government, it is especially common for parties to act as blocs (and this is generally expected), making such an assumption reasonable.

the "risk limit" [14]),[3] such as 99%. There is a rich literature on election auditing in one-level popular-vote elections (see [16], [17], [15], [7], [18], [19], [10], [9], [20], [21], [11]). Our method for multi-level auditing could be used with any method that satisfies some general assumptions, as we describe in Section II-C.

Our approach to multi-level auditing will be to assign an auditing responsibility to each group, and then argue that if all groups meet their responsibilities, the overall election result is confirmed in the necessary statistical sense. Because different groups may have a very different impact on the outcome in a multi-level election, we find that auditing to different levels of confidence in different groups can reduce significantly the cost of auditing the entire election to a specified overall level of statistical confidence, $1-\varepsilon$, as we can take advantage of choices about where to direct auditing resources.

Specifically, if the required confidence in the overall result is $1-\varepsilon$, then we will assign group i the responsibility to audit its result to a possibly different confidence level $1-\varepsilon_i$. We will assign the ε_i values such that audit success in every group implies that the overall election result is confirmed with the necessary confidence level.

If an audit in some group fails to confirm the election result, the audit will specify some escalation procedure that aims to determine the correct result in that group. If, ultimately, the election result is changed in some group, it will be necessary to re-evaluate the auditing responsibility assigned to all other groups to ensure that the required confidence level is met. This may necessitate re-auditing or the auditing of additional ballots in some locations if, for example, the auditing responsibility increases in group g' because auditing has changed the reported result in group g. The exact details of escalation will naturally depend on the nature and design of the overall election and the selection procedure that determines the overall result from the outcome in each group.

[3]We stress that, while prior work on election auditing has used the term "risk limit" to describe the acceptable bounds on confidence in the election result, we choose to call this parameter *statistical confidence*, as is done in many other fields. Nonetheless, the concepts are identical: both measure the bounds on the uncertainty in the correctness of the measured election result.

A. Election Auditing: An Illustrative Example

To illustrate the mechanics of multilevel election auditing, we will consider the case of presidential elections in the imaginary Republic of Freedonia. Freedonian voters are divided into five districts, District 1 through District 5. They vote directly for candidates for their country's highest office, President. In order to be elected President, a candidate must win a majority of the votes in at least three of the five districts. Thus, Freedonia has a multi-level election: first, candidates must win in each district and second, candidates must win across a majority of districts.

Citizens in Freedonia vote by marking a paper ballot which is scanned by an optical scanning machine that enables fully automated electronic tabulation of the paper ballots. Freedonian election officials wish to verify that the result reported by tabulation of the electronic records is consistent with the paper ballots. They will do this by a statistical procedure designed to verify consistency to 99% statistical confidence, that is, so that any discrepancy between the results will be detected with at least 99% probability. Their goal is to achieve this level of confidence at the lowest cost.

Consider now a specific election in Freedonia between two candidates for President, Alice and Bob. Table I summarizes the results of the election. How should this election be audited?

The most obvious way to audit this election is to conduct a separate audit in each district, to a confidence level of 99% within each district. Because the election within each district uses a simple majority criterion, we can use a standard auditing algorithm from the literature. Calandrino's method [8] would audit 233 ballots in District 1, and 25 ballots in each of Districts 2, 3, and 4, for a total of 308 ballots. (No audit is necessary in District 5 because District 5 did not contribute to Alice's reported victory.) The election result is be confirmed if, for every one of the audited ballots, manual reading of the ballot matches the electronic result reported for the same ballot.

In this case, it is not necessary to audit each individual district to 99% confidence. The reason for this is that Alice was reported as winning four districts when only three were required for victory, so that an incorrect result in only one district could not affect the outcome of the election. In

Candidate	District 1	District 2	District 3	District 4	District 5
Alice	51%	60%	60%	60%	35%
Bob	49%	40%	40%	40%	65%

TABLE I. RESULTS OF THE FREEDONIAN ELECTION, BY DISTRICT.

this case it is sufficient to audit to 90% confidence in Districts 1, 2, 3, and 4. To see why, suppose the election result is incorrect in two districts. If we audited the election 100 times, the audit would detect a discrepancy in the first district in 90 cases, and of the remaining ten cases, a discrepancy would be detected in the second district in nine cases. Only one case out of 100 would go undetected, which yields the required 99% detection rate. Following this procedure, we would audit 116 ballots in District 1 and 13 ballots in each of Districts 2, 3, and 4, for a total of 155 ballots.

Both of the audit strategies we have described so far spend the majority of auditing effort in District 1 (233/308 ballots in the first case, 116/155 ballots in the second case). In general, more ballots must be audited where the election result is close, because only a few miscounted ballots would be sufficient to swing the election and we need to audit more ballots to be confidence that we will randomly choose one of the few miscounted ones. By contrast, when the reported result is not close, auditing fewer ballots yields higher confidence.

This suggests a strategy in which we audit to lower confidence in District 1 and to relatively higher confidence in the other districts. The most extreme version of this strategy does no auditing at all in District 1, and audits to 99% confidence in Districts 2, 3, and 4. The logic of this approach is to establish with 99% confidence that Alice won all of Districts 2, 3, and 4, which is enough to establish that she won the election with 99% confidence, regardless of the accuracy of the reported District 1 results. In this approach we audit 25 ballots in each of Districts 2, 3, and 4, for a total of 75 ballots.

The Freedonia example shows that clever multilevel auditing strategies can reduce substantially the cost of auditing without reducing confidence in the result. It also illustrates some of the strategies that are possible. The results of analyzing this example are summarized in Table II.

The remainder of this paper presents a general mathematical theory for finding the lowest-cost strategy for auditing the result of any election conducted under a multi-level election procedure.

B. Basic Theory of Multi-Level Auditing

Intuitively, if the result of a multi-level election is incorrect, then it must be the case that the within-group result is incorrect for a sufficiently large set of the constituent groups. We define a *flipset* to be a set of groups such that changing the election results in all of these groups would have changed the overall election result. For example, in a U.S. presidential election, a flipset is a set of states which, if they all changed their results, would collectively change the total electoral college winner. We will say that F is a *minimal flipset* if F is a flipset but no proper (i.e., smaller) subset of F is a flipset. If F is a flipset, then there is some minimal flipset F^* such that $F^* \subseteq F$.

It is easy to show that if α_i are chosen so that for every minimal flipset F, $\sum_{i \in F} \alpha_i \geq 1$, and if the reported result in every group i is confirmed to confidence level $1 - \varepsilon^{\alpha_i}$, then the overall election result is confirmed to confidence level $1 - \varepsilon$. The intuition behind the proof is that if the reported overall election result is wrong, then there must be some minimal flipset F^* such that the reported group results are wrong for every group in F^*. The probability that the audits will fail to notice anything wrong anywhere in F^* is $\prod_{i \in F^*} \varepsilon^{\alpha_i} = \varepsilon^{\sum_{i \in F^*} \alpha_i}$ which by assumption is at most ε.

Cox gives a taxonomy of voting systems [22]. Our methods apply to any voting system which partitions voters into disjoint groups and holds an election in each group, subject to the constraint that the outcome at each level above the first is determined simply from the win or loss condition at the previous level (and not properties specific to the voting system used, such as vote counts).[4]

C. Optimal Auditing for Multi-Level Elections

We now turn to the question of how to minimize the cost of auditing a multi-level election.

[4] *Mixed member proportional* systems, such as the one used for parliamentary elections in Germany, do not have this property.

District	99% Confidence/District	90% Confidence/District	Optimal
District 1	233	116	0
District 2	25	13	25
District 3	25	13	25
District 4	25	13	25
Total	308	155	75

TABLE II. COST OF AUDITING THE FREEDONIAN ELECTION, IN TERMS OF NUMBER OF BALLOTS EXAMINED, BY STRATEGY EMPLOYED.

We allow the use of any known auditing scheme within each group. Our only assumption is that the expected cost C_i of auditing group i to confidence level $1-\varepsilon^{\alpha_i}$ can be expressed as $C_i = t_i \cdot \alpha_i$ for a group-specific coefficient t_i. Because t_i is the *expected* cost coefficient, our model can accommodate underlying audit methods that make adaptive decisions as to when to stop auditing, as well as schemes that have different audit costs for different ballots within a group.

We start by observing that many auditing schemes have a linear cost property, so that the expected cost of auditing a group of ballots to confidence level $1-\varepsilon^{\alpha_i}$ is proportional to α_i, with the constant of proportionality depending on the auditing scheme and the number and distribution of ballots. This constant will typically differ from group to group.

To see why linearity is a natural relation, consider that many auditing algorithms operate by performing a test (such as examining one ballot) and repeating the test, with an independent random selection, as many times as necessary until a desired confidence level is reached. If one test costs C_0 and achieves confidence $1-\varepsilon^{\alpha_0}$, then repeating the test k times (and failing if any of the k instances fails) will yield confidence $1-\varepsilon^{k\alpha_0}$ at expected cost kC_0, which satisfies the linear cost property.[5]

In the remainder of the paper, we will assume an audit scheme that has the linear cost property, that is, that the *expected* cost of auditing, *within each group* is linear *in the parameter* α_i. For schemes whose cost functions are approximately linear, our algorithm will yield a strategy that meets the required confidence level, and with cost that will typically be close to optimal. Finding the optimal-cost solution for nonlinear cost scheme will be more expensive, requiring nonlinear optimization.

If an audit scheme does not have the linear cost property, it would be fairly easy to apply our techniques using nonlinear optimization methods such as hill climbing, especially since the number of variables (i.e. the number of groups in the first-level partition of voters) is usually very small (e.g. in the U.S. Presidential election, there are 51 partitions at the lowest level). One could also approximate the cost function linearly near a proposed solution, which would lead to a correct solution (in the sense that the audit would function to guarantee the specified statistical confidence), although not necessarily a cost-optimal solution.

Because we assume the cost is linear in the α_i, we can use linear programming to find values for the α_i that minimize the total cost, subject to the constraints discussed above. For each minimal flipset F, we will have a linear constraint $\sum_{i\in F}\alpha_i \geq 1$. This will give us the optimal (lowest-cost) auditing procedure that achieves the required confidence level.

In Appendix A, we prove that two well-known ballot-based auditing methods, the Machine-assisted Election Auditing algorithm by Calandrino *et al.* [8] and the Secrecy-preserving Ballot-level Audit (SOBA) of Benaloh *et al.* [13], have the linear cost property required by our scheme.

D. Score-Based Auditing Method

In some cases, it may be difficult or inconvenient to use linear programming to find the optimal assignment of α values. As an alternative, we can approximate the solution using a score-based method that provides the required level of confidence but not a guarantee of minimal cost. To do this, we choose some method of assigning a non-negative numerical score to each group. If group i has score s_i, and if we can show that

[5] It is possible to scale to a non-integer multiple of the original α_0 and C_0 by probabilistic interpolation: if k is an integer and $0 \leq f < 1$, then an algorithm that performs the base audit k times, then with probability f performs the base audit one more time, will be linear, giving confidence $1-\varepsilon^{(k+f)\alpha_0}$ at expected cost $(k+f)C_0$.

any minimal flipset must have total score at least s_*, then we can assign $\alpha_i = \min(1, \frac{s_i}{s_*})$. (Groups that do not appear in any minimal flipset can be assigned $\alpha_i = 0$.) It is easy to show that this will be feasible, in the sense that the α values in any minimal flipset will sum to at least 1.

As an example, in a U.S. electoral vote election, we could assign each state a score equal to its number of electoral votes. If the electoral vote margin is M (that is, if at least M electoral votes would have to flip to change the election result), then it is easy to see that any minimal flipset must have total score at least $s_* = M$. Applying the score-based auditing method, a state i having e_i electoral votes gets $\alpha_i = \min(1, \frac{e_i}{M})$. The intuition is that a state's fair share of the "α burden" is proportional to its number of electoral votes.

As a refinement, we can assign $\alpha = 0$ for a subset of groups, presumably because auditing is especially expensive for these groups. We can choose a set D of groups to "drop", such that $M_D = \sum_{i \in D} \alpha_i$ is less than M. Then for every $i \in D$ we set $\alpha_i = 0$; and for every i not in D we set $\alpha_i = \min(1, \frac{e_i}{M - M_D})$. The intuition is that we don't bother to audit the groups in D, but we increase the auditing burden proportionally in the remaining groups to ensure that the total α in every minimal flipset is still large enough.

These score-based methods are likely to be useful when the number of minimal flipsets is very large. For example, in the 2008 U.S. presidential election, there are 79 841 552 minimal flipsets. Rather than enumerating them and solving a large linear programming problem, the score-based method can yield a much faster solution that we conjecture will often be close to optimal.

We observe that our score-based method is similar to the method introduced by Aslam, Popa, and Rivest [18]. That method divides votes into groups (typically precincts), but assumes that vote totals in each group are always summed to get the overall election result. We allow arbitrary aggregation rules across groups, subject to the constraint that the rules must only consider the win/loss outcome in each group. Additionally, Aslam *et al.* assume that auditing within a group is all-or-nothing: either a group is audited to 100% confidence or not at all. We admit different levels of auditing leading to different confidence intervals. Finally, our main method accounts for the bin-packing issues associated with allowing mixed confidence levels across groups, while the score-based method and the Aslam *et al.* method both ignore these issues for the benefit of ease of computation.[6]

E. Application to U.S. Presidential Elections

To illustrate the use of multi-level auditing, we can apply our method to the U.S. Presidential election from 2000 through 2012, as summarized in Figure III. As an example, the 2012 election was won by Barack Obama with 332 electoral votes, over Mitt Romney's 206. For this election, a minimal flipset would be any minimal set of states that were won by Obama and add up to at least 63 electoral votes. This calculation assumes that the expected per-ballot cost of auditing is equal in all states, so that all $c_i = 1$.

The 2000 election was very close, so there are few flipsets. Any one of the states won by Bush forms a singleton minimal flipset, so the optimal auditing strategy requires that each of these thirty states be audited to confidence level 99%. At the other extreme, the 2008 election had a larger margin of 96 electoral votes, leading to roughly 80 million minimal flipsets. Our linear program solver ran out of memory on this example, so we show a cost only for the score-based method.

F. Application to the 2010 UK Parliamentary Election

As another illustration, we applied our methods to the 2010 parliamentary election in the United Kingdom. Separate plurality elections were held in each of 565 districts. In total, members of twelve parties won seats, with the Conservative party winning 306 seats, the Labour party 258, the Liberal Democrats 57, and smaller parties winning 8, 6, 5, 3, 3, 1, 1, 1, and 1 seats, respectively. For purposes of auditing, we assume that each party's members will vote as a bloc. Since no party has a majority, a coalition of parties holding at least 326 seats in total is required to govern. We considered the set of possible governing coalitions to be the election result.

[6] While Aslam *et al.* consider linear programming as an optimal solution and give a linear program formulation of their method, they dismiss the result as necessarily too costly and complex to calculate.

Year	Electoral Vote Margin	Num. Minimal Flip Sets	Expected Number of Ballots Audited ($\varepsilon = 0.01$)			
			State-by-State	Score-Based	Score w/ Drop	Optimal (LP)
2012	63	872,775	2691.9	475.2	421.1	421.1
2008	96	79,841,552	7705.8	430.6	220.7	·
2004	17	5896	5262.6	1239.9	1239.9	1183.6
2000	2	30	64145.9	51651.1	51651.1	51651.1

TABLE III. AUDITING REQUIREMENTS FOR U.S. PRESIDENTIAL ELECTIONS 2000-2012. EXPECTED AUDITING COSTS (ASSUMING UNIT COST PER BALLOT AUDITED) REQUIRED TO ACHIEVE AN OVERALL CONFIDENCE OF 99% ($\varepsilon = 0.01$) VS. ELECTORAL VOTE MARGIN AND NUMBER OF MINIMAL FLIP SETS, AS CALCULATED USING THE OPTIMAL LINEAR PROGRAMMING METHOD, THE SCORE-BASED METHOD, THE SCORE-BASED METHODS WITH DROPS, AND A METHOD WHICH CONSIDERS AUDITING TO 99% CONFIDENCE IN EACH STATE SEPARATELY FOR THE U.S. PRESIDENTIAL ELECTIONS IN YEARS 2000-2012. FOR THE 2008 ELECTION, OUR LINEAR PROGRAM SOLVER RAN OUT OF MEMORY, SO WE SHOW ONLY THE SCORE-BASED RESULTS.

Given these assumptions, there turn out to be many possible governing coalitions that control the bare minimum number of seats. Every party can participate in such a minimum-size governing coalition. As a result, for every seat there is a minimal flipset containing only that seat, so that every seat i must be assigned $\alpha_i = 1$. Auditing to a 99% confidence level requires examining an expected 98384 ballots.

The amount of auditing required might have been much less had the election come out differently. For example, if the three major parties had gotten 256, 208, and 157 seats, and the minor parties were unchanged, then there would be only three minimal coalitions, consisting of all pairs of major parties. In this scenario the minor parties do not matter, and the smallest minimal governing coalition is a Labour-LibDem coalition with 365 seats. In this scenario, every minimal flipset involving Conservative seats contains at least 88 seats, and every minimal flipset containing Labour or LibDem seats contains at least 40 seats. Therefore we can assign every Conservative seat $\alpha_i = \frac{1}{88}$, every Labour and LibDem seat $\alpha_i = \frac{1}{40}$, and every minor party seat $\alpha_i = 0$. This would correspond to auditing every Conservative seat to a confidence level of only 0.05, and every Labour and LibDem seat to a confidence level of only 0.11. For most seats, the expected number of audited ballots would be less than one.

In general, an approach to auditing parliamentary coalition elections of this type is to compute all of the minimal coalitions (i.e., all coalitions which do not have a proper subset that is a coalition), and then to compute, for each party, the coalition containing that party which contains the smallest number of seats. Let x_i be the size (in seats) of the smallest coalition containing party i, and let x^* be the minimum number of seats needed to form a coalition (i.e., one more than half of the seats). If $w(i)$ denotes the party that won seat i, we can assign the score

$$s_i = \frac{1}{1 + x_{w(i)} - x^*}.$$

It is easy to show that any minimal flipset must have total score at least 1, so we can assign $\alpha_i = s_i$. As an additional optimization, we could consider "dropping" some seats in order to reduce the total auditing cost.

III. CONCLUSION

We introduce a novel auditing technique for examining confidence in and the integrity of real-world multi-level election systems such as the electoral college in the U.S. presidential election or coalition parliament systems in many countries.

Specifically, we describe a method for ballot-based auditing which uses the structure of the multi-level election to reduce the total amount of auditing necessary to achieve full confidence in the overall election result. We show how to use the particular structure of multi-level elections to reduce or ignore the auditing of some subgroups, reducing the cost of auditing while maintaining a defined level of overall confidence. We show both a cost-optimal approach to auditing the overall election to a specific level of statistical confidence $1 - \varepsilon^{\alpha}$ and also a score-based approximation that yields an easily computable correct, but not necessarily cost-optimal, audit strategy. We evaluate this method on real election data from the U.S. and the U.K. and show that it can significantly reduce auditing costs (in our U.S. presidential election examples, costs using our strategy were between 15.2% and 80.5% of a strategy that was independent of the election's multi-level structure; in an example drawn from

the U.K. Parliamentary election in 2010 (in which the results were highly split, allowing for many different possible coalitions), auditing to 99% confidence requires a modest cost of examining just under 100,000 ballots).

As future work, we intend to apply our frameworks to more elections and more types of election systems around the world. For example, we have only considered concretely elections where the first level in the multi-level system is decided by a majority or plurality vote. However, our results generalize readily to any selection algorithm, and we intend to consider such alternative systems in detail. For example, certain kinds of *mixed member proportional* systems (and related systems, such as those used in Germany), are not multi-level in the way we have defined. However, we believe our methods can be generalized to include such systems. We are also further refining our algorithms for determining optimal audit costs and seek to find more efficient algorithms, which are still provably cost-optimal.

APPENDIX

We give two concrete examples of multi-level election auditing using ballot-based auditing algorithms that satisfy the linear cost property. We assume in these examples for simplicity that the within-group elections are decided by a simple plurality or majority[7] and that auditing k ballots in group i has expected cost $k\ell_i$ for some group-specific expected per-ballot examination cost ℓ_i.

1) Example: Calandrino's Ballot-Based Audit: First, we give an example using election auditing algorithm of Calandrino et al. [8], which obeys the linear cost model.

Consider a group i with expected per-ballot auditing cost ℓ_i and an assigned responsibility to audit to confidence level $1-\varepsilon^{\alpha_i}$. Let m_i be the victory margin of the winning candidate. In a plurality election, $m_i = \frac{v_i^1 - v_i^2}{2}$ where v_i^1 is the winning candidate's vote count and v_i^2 is the second-place candidate's vote count. In a majority election with a winner, $m_i = v_i^1 - \frac{v_i}{2}$ where v_i is the total number of votes cast in the group. In order for the declared group winner to be wrong, at least m_i of the votes cast for the group's winning candidate must be defective, so that at least a fraction m_i/v_i^1 of the declared winner's votes must be defective. It follows that auditing n_i of the ballots cast for the group winner, without finding an error, will confirm the accuracy of the group winner with confidence level $1-(1-m_i/v_i^1)^{n_i}$, so that we can achieve the desired confidence level $1-\varepsilon^{\alpha_i}$ by setting

$$n_i = \frac{\alpha_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}.$$

(If the resulting n_i is not an integer, we can interpolate: if $n_i = k+f$ for integer k and $0 \le f < 1$, we choose k ballots with probability $1-f$ and $k+1$ ballots with probability f. Then the expected number of ballots chosen is equal to $k+f = n_i$ and the other necessary properties hold.)

Applying the same argument to all groups, we see that the total auditing cost will be

$$C = \sum_i \ell_i n_i = \sum_i \ell_i \frac{\alpha_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}.$$

Setting

$$\ell_i' = \frac{\ell_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}$$

the cost becomes

$$C = \sum_i \ell_i' \alpha_i.$$

This is consistent with the linear-cost model.

2) Example: SOBA: To emphasize that any auditing algorithm with linear expected cost could be substituted, without changing our basic analysis, we provide a second example using SOBA [13], a modern risk-limiting audit method, which also has the necessary property that the expected cost of auditing within each group i is linear in the parameter α_i.

We assume as before that subgroup elections are decided using simple plurality or majority first-past-the-post rules and that the election in each subgroup yields a well-defined result.

Consider now group i with expected per-ballot auditing cost ℓ_i and assigned responsibility to audit to confidence level $1-\varepsilon^{\alpha_i}$. Say that the winning candidate has margin m_i Then the SOBA "diluted margin" will be m_i/N_i where N_i is the number of ballots cast in group i. That means that, given numerical parameters λ and γ,

[7] A majority election might have no winner; in that case we consider the result to be $\perp$. To simplify the exposition, we will assume in the main text that $\perp$ is not the declared result in any group, although our algorithms can easily be extended to cover that case.

the "error tolerance" and "error bound inflator", respectively, the number of ballots audited in the first round of SOBA is:

$$n_i^0 = \frac{\alpha_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

SOBA proceeds by adding ballots to this sample until a specific confidence threshold is achieved. The expected additional cost from repeating the audit is negligible, scaling as C^{-2m} where C is a constant derived from the margin of victory and m is the number of misstated votes discovered [12].

The total cost C is obtained by summing over all groups gives:

$$C = \sum_i \ell_i n_i = \sum_i \frac{\alpha_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

And setting:

$$\ell_i' = \frac{\ell_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

we again obtain (consistent with the linear-cost model):

$$C = \sum_i \ell_i' \alpha_i.$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for thoughtful comments on an earlier version of this paper submitted to JETS Volume 1, Issue 1.

REFERENCES

[1] J. F. Banzhaf III, "Weighted voting doesn't work: A mathematical analysis," *Rutgers L. Rev.*, vol. 19, p. 317, 1964.

[2] L. S. Penrose, "The elementary statistics of majority voting," *Journal of the Royal Statistical Society*, vol. 109, no. 1, pp. 53–57, 1946.

[3] L. S. Shapley and M. Shubik, "A method for evaluating the distribution of power in a committee system," *American Political Science Review*, vol. 48, no. 03, pp. 787–792, 1954.

[4] K. J. Arrow, "A difficulty in the concept of social welfare," *The Journal of Political Economy*, vol. 58, no. 4, pp. 328–346, 1950.

[5] D. W. Jones, "On optical mark-sense scanning," in *Towards Trustworthy Elections*. Springer, 2010, pp. 175–190.

[6] R. T. Mercuri, "Electronic vote tabulation checks and balances," Ph.D. dissertation, University of Pennsylvania, 2001.

[7] J. A. Aslam, R. A. Popa, and R. L. Rivest, "On estimating the size and confidence of a statistical audit," in *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

[8] J. Calandrino, J. Halderman, and E. Felten, "Machine-assisted election auditing," in *USENIX/ACCURATE Workshop on Electronic Voting Technology (EVT'07)*, 2007.

[9] P. B. Stark, "Conservative statistical post-election audits," *Annals of Applied Statistics*, vol. 2, pp. 550–581, 2008.

[10] J. L. Hall, P. B. Stark, L. W. Miratrix, M. Briones, E. Ginnold, F. Oakley, M. Peaden, G. Pellerin, T. Stanionis, and T. Webber, "Implementing risk-limiting post-election audits in california," 2009.

[11] S. Checkoway, A. Sarwate, and H. Shacham, "Single-ballot risk-limiting audits using convex optimization," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT'10)*, 2010.

[12] P. B. Stark, "Super-simple simultaneous single-ballot risk-limiting audits," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT'10)*, 2010.

[13] J. Benaloh, D. Jones, E. L. Lazarus, M. Lindeman, and P. B. Stark, "Soba: secrecy-preserving observable ballot-level audit," in *Electronic Voting Technology Workship/Workshop on Trustworthy Elections (EVT/WOTE'11)*, 2011.

[14] J. Bretschneider, S. Flaherty, S. Goodman, M. Halvorson, R. Johnston, M. Lindeman, R. L. Rivest, P. Smith, and P. B. Stark, "Risk-limiting post-election audits: Why and how," Oct. 2012.

[15] D. W. Jones, "Auditing elections," *Communications of the ACM*, vol. 47, no. 10, pp. 46–50, Oct. 2004.

[16] K. Dopp, "History of confidence election auditing development (1975 to 2008) & overview of election auditing fundamentals," *National Election Data Archive*, 2008.

[17] W. R. Mebane, Jr., J. S. Sekhon, and J. Wand, "Detecting and correcting election irregularities," Stanford University, Tech. Rep., Oct. 2003. [Online]. Available: http://wand.stanford.edu/research/detecting.pdf

[18] J. A. Aslam, R. A. Popa, and R. L. Rivest, "On auditing elections when precincts have different sizes," in *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08)*, 2008.

[19] P. B. Stark, "A sharper discrepancy measure for post-election audits," *The Annals of Applied Statistics*, vol. 2, pp. 982–985, Nov. 2008.

[20] A. D. Sarwate, S. Checkoway, and H. Shacham, "Risk-limiting audits and the margin of victory in nonplurality elections," *Statistics, Politics, and Policy*, vol. 3, no. 3, pp. 29–64, 2013.

[21] R. L. Rivest and E. Shen, "A bayesian method for auditing elections," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*, 2012.

[22] G. W. Cox, "Centripetal and centrifugal incentives in electoral systems," *American Journal of Political Science*, pp. 903–935, 1990.

International Standards

The Council of Europe and e-voting:

History and impact of Rec(2004)11

Robert Stein
Austrian Federal Ministry of the Interior (BM.I)
Department of Electoral Affairs
Vienna, Austria
robert.stein@bmi.gv.at

Gregor Wenda
Austrian Federal Ministry of the Interior (BM.I)
Department of Electoral Affairs
Vienna, Austria
gregor.wenda@bmi.gv.at

***Abstract*— When the Council of Europe started to deal with the subject of electronic voting in 2002, the impact of its work was not foreseeable. What followed, however, was basically a "success story": The Recommendation on legal, operational and technical standards for e-voting (Rec(2004)11), which was adopted by the Council of Ministers on 30 September 2004, has been the most relevant international document and reference regarding e-voting for a decade. Since 2010, the role of the Council of Europe with regard to e-voting has shrunk. Nevertheless various Member States expressed the desire to further review the Recommendation in the forthcoming years. Following an informal experts' meeting in Vienna on 19 December 2013, the Committee of Ministers was confronted with the suggestion to formally update the Recommendation in order to keep up with the latest technical, legal and political developments. The forthcoming Review Meeting on 28 October 2014 may help set the course for future e-voting activities of the Council of Europe.**

Keywords—Council of Europe, e-voting, internet voting, Rec(2004)11, Recommendation, review meeting, update.

I. How it started

Using technical devices in the vote casting process is no invention of the 21st century. It already started back in the 19th century [1] and some states (have) used voting machines for several decades.[1] With the rise of the World Wide Web and e-government applications in the mid-1990s, the idea of voting over the internet was born. The first binding political online election is said to have taken place in the USA in the year 2000. [2] Originally, no sharp distinction between machine voting and internet voting was drawn when employing the new term "electronic voting" or "e-voting".[2] Around ten years ago, the term "i-voting" for "internet voting" came about. [3] The interest in information and communication technologies in elections coined politicians, scientists, and administrators alike. A British opinion paper outlined the motivation for e-voting activities in 2002: "Citizens rightly expect to be able to vote in a straightforward, accessible, and efficient way, being able to have confidence in the security and integrity of the poll. (…) Governments, therefore, are being faced with requests from their citizens to introduce new technologies in the electoral processes, in particular to make available various forms of e-voting." [4] A number of international institutions and fora could have dealt with the new phenomenon of electronic voting[3] but it was the Council of Europe which apparently developed the strongest interest and formed a "multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting" within the framework of its 2002-2004 Integrated Project "Making democratic institutions work" (IP 1). The group was supported by two subgroups dealing with legal and operational aspects as well as technical aspects. [5] Some of the driving factors were the perception that citizens lost interest in politics and the drop of participation rates in elections and referenda. [6] However, Michael Remmert already noted in 2004 that "modernising how people vote will not, per se, improve democratic participation. Failure to do so, however, is likely to weaken the credibility and legitimacy of democratic institutions." [7] The Ad Hoc Group created a set of standards on e-voting, which were eventually adopted in the form of a Recommendation by the Council of Ministers on 30 September 2004. 112 legal, operational and technical standards provided valuable guidance in the new world of electronically enabled elections and gave a better idea of principles to follow and possible risks to keep in mind. Paragraph v. of the Recommendation stipulated a first review after two years "in order to provide the Council of Europe with a basis for possible further action on e-voting". Accordingly, the first review meeting was held in Strasbourg in November 2006. Since then, repeated two-year review periods were decided by all subsequent intergovernmental meetings.

II. Recommendation Rec(2004)11

Until today Rec(2004)11 is the only international document regulating e-voting from a legal perspective. Even though these

[1] In the Netherlands, all voting machines were discontinued after suspected fraud in 2007. They had been used in polling stations nationwide since 1965 (see Loeber, E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years, in Krimmer/Grimm [Eds], 3rd international Conference on Electronic Voting 2008, Proceedings [2008] 21).

[2] The term "e-enabled voting" also became more widely used.

[3] The European Union never set sustainable steps in the area of e-voting. One of the few international events was an „eDemocracy Seminar" organized by the European Commission, which took place in Brussels on 12 February 2004 and provided an overview of European e-voting activities (including the non-EU country Switzerland) at that time. The Organization for Security and Co-operation in Europe (OSCE) appointed an expert for the observation of New Voting Technologies for the first time in 2010 and developed a "Handbook for the Observation of New Voting Technologies" in 2013.

"minimal standards" are merely voluntary and thus non-binding, the member states of the Council of Europe declared their general support and commitment with the adoption by the Committee of Ministers in 2004. The Recommendation states that "e-voting shall respect all the principles of democratic elections and referendums" and "shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means." [8] Member States were asked to "consider reviewing their relevant domestic legislation in the light of this Recommendation" [9] though a wide margin of individuality was respected since individual member states were not required "to change their own domestic voting procedures which may exist at the time of the adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums". [10] Since its adoption in 2004, Rec(2004)11 has become a unique reference for matters of e-enabled voting. [11] It has been drawn upon by various countries, scientific institutions, and even courts when evaluating plans or the actual use of electronic voting. Norway is said to be the only state that incorporated most of the Recommendation's standards into the regulatory framework for the 2011 and 2013 internet voting trials. [12] A 2007 study on e-voting in Belgium, initiated by Belgian Federal and Regional administrations, took reference of Rec(2004)11 and used it as a benchmark in its evaluation. [13] The Estonian Supreme Court considered the Recommendation when deciding about the constitutionality of e-voting. [14] The 2008 pilot in Finland, where some municipalities used voting machines in polling stations, was monitored by civil society and the Council of Europe while taking Rec(2004)11 into account. [15] Switzerland had the Recommendation, as well as other practical experiences since 2004, "on the radar" when passing recent legislative changes concerning their "vote électronique". [16] In Austria, standards of Rec(2004)11 were drawn upon for the evaluation and certification of the e-voting system used in the 2009 Federation of Students' elections. OSCE/ODIHR monitored the use of "New Voting Technologies (NVT)" in a number of states in light of the Recommendation and gave respective reference in its reports. The OSCE Handbook on the "Observation of New Voting Technologies", which was published in late 2013, calls Rec(2004)11 "the only specialized international legal document in this regard" and mentions it under "Good Practice Documents" on e-voting. [17] The publication "Introducing Electronic Voting – Essential Considerations" by the International Institute for Democracy and Electoral Assistance (IDEA) listed Rec(2004)11 among the essential international documents. [18] Even in several overseas countries such as Canada [19] or the United States, [20] elements of the Recommendation were included in different studies and reports.

Despite its worldwide recognition, the Recommendation has become a bit long in the tooth. Ten years after its adoption, numerous technical developments and new social approaches have changed the "e-world". Consequently, voices in favour of a formal update have gained strength. Ongoing innovations and technological changes were already in the states' minds when a first review after two years was demanded. The e-voting group suggested to the Committee of Ministers to "recommend to member states to keep their own position on e-voting under review and report back to the Council of Europe the results of any review that they have conducted" as "e-voting is a new and rapidly developing area of policy and technology" and "standards and requirements need to keep abreast of, and where possible, anticipate new developments." [21] In 2004, the Council of Europe established a new project, "Good governance in the information society", which would last until 2010 and continued the discussions on e-voting. It also followed new challenges posed by the broader scope of "electronic democracy" (e-democracy)[4]. The overall project aimed at providing "governments and other stakeholders with new instruments and practical tools in this field and to promote the application of existing instruments and of good and innovatory policy practice". [22]

The first review meeting in Strasbourg on 23 and 24 November 2006 concluded that the Recommendation had become accepted by member states "as a valid and currently the only internationally agreed benchmark by which to assess and evaluate e-voting systems." [23] The second review meeting was organized on the occasion of the Forum for the Future of Democracy dedicated to "e-democracy" in Madrid. It took place on 16 October 2008 and summarized the latest developments and new questions concerning e-voting. In this regard, the Recommendation was still considered useful but some aspects, particularly concerning certification and observation, were identified as topics not sufficiently covered. Hence, the Council of Europe organized a Workshop on the "Observation of e-enabled elections" in Oslo on 18 and 19 March 2010 and subsequently had experts reconvene in Strasbourg in order to work on two follow-up documents complementing Rec(2004)11 – the "Guidelines on certification of e-voting systems" and the "Guidelines on transparency of e-enabled elections". [24] Both guidelines, along with an "E-voting handbook" about the "key steps in the implementation of e-enabled elections", were presented during the third review meeting in Strasbourg on 16 and 17 November 2010. This also constituted the end of the Council of Europe's activities during the project "Good governance in the information society".

III. TOWARDS AN UPDATE?

A fourth review meeting took place in Lochau near Bregenz[5], Austria, on 11 July 2012. During this meeting, several state representatives said that Rec(2004)11 was still precious but that in light of recent practical experiences, and despite the additional guidelines of 2010, a number of issues were not dealt with any more. As a consequence, the representatives of the Member States "agreed to recommend that the 2004 Committee of Ministers' Recommendation (…) should be formally updated.". [25] They further stated "that the biennial review meetings were highly useful and should be continued (…)". [26] The Republic of Austria, one of the countries actively involved in the creation of the

[4] The Council of Europe's Ad Hoc Committee on e-democracy (CAHDE) prepared a Recommendation on e-democracy (Rec(2009)1), which was adopted by the Committee of Ministers in February 2009.

[5] The precise location was Castle Hofen in Lochau near Bregenz but all international documents bear the more widely known city name of Bregenz.

Recommendation from the start, used the opportunity during the Chairmanship of the Committee of Ministers[6] to invite e-voting experts to Vienna in order to follow up and discuss the future of Rec(2004)11 within the framework of an informal workshop. Austria had already suggested such a get-together during the 2012 review meeting. [27] Since 2010, e-voting matters have not been under the umbrella of a Council of Europe project. They are now handled by the "Directorate of Democratic Governance" belonging to the "Directorate General of Democracy". The "Division of Electoral Assistance and Census" was in charge of preparing the workshop in Vienna, which was held in co-operation with the Austrian Federal Ministry of the Interior, being Austria's primary electoral management body, on 19 December 2013 in Vienna.[7] In preparation of this meeting, the Council of Europe commissioned a report "on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting". The author was Ardita Driza Maurer, an independent lawyer/consultant and former member of the e-voting team at the Swiss Federal Chancellery. [28] Based on the findings of Ardita Driza Maurer, reasons for updating the Recommendation were debated. [29] New technological developments and concepts such as in the context of the verifiability of votes, and conclusions from studies and reports, for instance regarding certification, called for addenda or adaptions (for further details on a possible future recommendation update see the article of Ardita Driza Maurer).

More than a decade ago, developing the 112 legal, operational, and technical standards was a "rather theoretically driven exercise". [30] There is no doubt that this facilitated the intergovernmental work as not too many existing systems were influenced by the then new set of rules. However, the work on the two guidelines in 2010 already showed that this situation had changed in just a few years: Since some countries meanwhile had e-voting in use or were in the process of implementing specific solutions, discussions over specific models and paragraphs became more detailed and heated than originally expected. In the end, the guidelines remained more general in their wording than intended in the beginning. The participation of civil society and other non-governmental stakeholders was also of a different quality in the early 2000s than today's era of public participation and open government would permit. Hence, the experts' workshop in Vienna concluded that "it must be ensured that the necessary legal and technical expertise is available during the drafting process and that it must be open, with detailed mechanisms to be determined, to the full range of stakeholders, e.g. civil society actors, e-voting systems providers and possibly non-member states." [31] Another difference to the drafting work of 2002 to 2004 is the monetary perpective: While the Ad Hoc Group of 2002-2004 had sufficient resources to cover travel expenses and the input of experts within the framework of Project "IP 1", no such budget is currently available at the Council of Europe. It goes without saying that proper updates could only be realized if future budgets would allow work on Rec(2004)11.

IV. Practical use of e-voting in Europe

In contrast to 2004, a number of countries have meanwhile gained experience in the e-voting field. Some of them even provide binding, e-enabled voting channels today. Other states, however, stopped using any kind of technology in the voting process. The following overview is not meant to be exhaustive but supposed to give a better feeling of some of the recent, more note-worthy activities in the field. [32]

Albania worked on two pilot projects – one regarding the introduction of electronic voter identification means in polling station (by using the national identification card), the other concerning optical scanners in two regional counting centers during the elections in June 2013. Both pilots eventually failed. In ***Armenia***, the Central Election Commission came up with a (rather simple) system allowing Armenians working at diplomatic missions abroad and Armenian professionals working for Armenian companies abroad to vote online. The legal basis was passed before the 2012 parliamentary elections but the participation rate was small. In ***Austria***, only remote voting over the internet has been seriously discussed. The Austrian Federal Ministry of the Interior conducted an intergovernmental feasibility study presented in late 2004. [33] In order to implement internet voting, an amendment to the federal constitution (two-third majority in parliament) would be required. Some non-binding academic trials [34] in 2003, 2004[8] and 2006 and a legally binding use during the 2009 elections of the Austrian Federation of Students [35] were the only notable experiences. In 2011 the Austrian Constitutional Court suspended some provisions in the regulation for the 2009 students' elections. At the same time, the Constitutional Court emphasized that in all future deployments of e-voting the legal basis had to be clearly determined in order to allow transparency both for election commissions and individual voters. [36] ***Azerbaijan*** ran some non-binding pilots of internet voting ("shadow elections") in the past but no further steps towards e-voting have materialized. ***Belgium*** did away with voting machines in the wake of the discussions in the Netherlands but has lately looked into a new and improved paper-based machine voting system which was piloted in the regional elections in October 2012 and showed the need for various modifications. The improved system is supposed to be used in half of the country during the 2014 elections. Internet voting may only be considered for Belgian voters abroad. ***Bulgaria*** started discussing e-voting solutions in both polling stations and over the internet in 2004. A draft law allowed for internet voting pilots. In 2009, a test was run in nine electoral precincts. A legal amendment on the permission of e-voting was passed in 2012 but subsequently overturned by the Constitutional Court. The current election code stipulates the introduction of machine voting in 2015. ***Estonia*** was the first

[6] Austria assumed the chairmanship of the Committee of Ministers of the Council of Europe on 14 November 2013. The formal end was the annual meeting of the Committee of Ministers on 6 May 2014.

[7] Approximately 50 persons from about a dozen countries participated, among them almost all states actively involved in e-voting (among them being Belgium, Estonia, Norway, Russia, and Switzerland).

[8] The 2004 trial was organized along the lines of the Austrian presidential elections. For further details see Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger, E-Voting Election Test to the Austrian Federal Presidency Election 2004, Working Papers on Information Processing and Information Management 02/2004 (http://epub.wu.ac.at/194/1/document.pdf).

country to introduce internet voting as a legally binding channel during the 2005 municipal elections and the 2007 parliamentary elections. [37] Online votes have to be cast in advance of the election day. [38] During the 2013 municipal elections, 24.3% of the votes came over the internet. The i-voting system and procedure are constantly improved, for instance by installing an Electronic Voting Committee composed of IT professionals responsible for conducting the i-vote process. More transparency will be ensured by introducing a new verification system, which was tested in 2013 and will become an integral part of the law in 2015. ***Finland*** piloted voting machines based in polling stations and connected to the internet in three municipalities in 2008. Following some flaws and court decisions, the project was discontinued. A working group looked into the possibilities of internet voting and presented an internal report in June 2014. Further research on the use of the internet for participative instruments was suggested. ***France*** has been using electronic voting machines in certain municipalities though the number will not be increased after the discussions in the Netherlands and Germany. Since the early 2000s, online voting for French citizens abroad had been debated and some pilots were carried out. In 2012, select representatives for the French living abroad were elected via internet for the first time. ***Germany*** used to have voting machines in certain constituencies (for all kinds of elections) since the 1960s. Due to complaints regarding the 2005 parliamentary elections, the Federal Constitutional Court of Germany held on 3 March 2009 that the use of machines undermined the principle of publicity. [39] While electronic voting machines with a paper audit trail should suffice the requirements of the decision, Germany stopped using all kinds of machines. Internet voting is exercised on a very small scale in an academic and semi-private environment but not in any political elections. ***Ireland*** introduced electronic voting machines in 2004 but never used them due to public concerns about their reliability. The machines were stored for years and finally demolished in 2012. ***Latvia*** currently focuses on the use of ITC in scanning and counting ballots. Aside from optical scanners, ideas about internet voting are debating with the neighbouring country Estonia in mind. ***Liechtenstein*** has the legal basis for e-voting in municipal elections and, influenced by developments in Switzerland, has followed e-voting discussions for a number of years – so far, however, without any further steps. ***Lithuania*** has repeatedly tried to follow the Estonian example but proposals of the Central Election Commission to introduce e-voting have not earned sufficient support in parliament yet. The Netherlands had mechanical and electronic voting machines dating back to the 1960s and also used internet voting for certain bodies. After doubts about the security of voting machines were publicly expressed by an NGO, both voting machines and internet voting were stopped in 2008 by a ministerial decree. In late 2013, a Study Commission recommended introducing electronic voting and counting "in order to make the voting and counting process more accessible and faster". Ballot stations should use new machines with ballot printers. A nation-wide roll-out could take place after a piloting phase around 2018 or 2019. ***Norway*** conducted a feasibility study on internet voting in 2006 and carried out a first pilot on the local level (10 municipalities and 4.5 % of population) in 2011. Lessons learned from other e-voting examples, for instance the need of universal verifiability, were taken into consideration. Another use of internet voting took place during the 2013 parliamentary elections (12 municipalities and 7% of population). In June 2014 the government announced to discontinue the use of e-voting trials. [40] In ***Russia***, the Central Election Commission introduced electronic voting machines with a paper audit trail in 2005. In February 2013, the constitutional committee proposed to look into internet voting as well. In Slovenia, electronic voting machines have been used in polling stations in order to assist handicapped voters though no further expansion seems to be considered. In ***Spain***, pilots regarding electronic voting machines have been carried out since 1995. In addition, some internet voting tests were carried out on the regional (2003, Catalonia) and national level (2005). The basis for internet voting was laid down in the Basque Country electoral code in 1998. Lately, no further serious discussions have materialized. ***Switzerland*** had its first debates on internet voting in 1998 and started a pilot project on e-voting ("vote électronique") in three cantons in 2002. In the beginning, it was only used in local elections and referenda. In 2011, the first nation-wide use (for national parliamentary elections) took place. The government is still in the process of gradually expanding the use of e-voting. New legal backbones for the federal level were adopted in December 2013. In order to further extend internet voting, a new model of verifiability and new auditing routines will be required. Until the end of 2013, 12 cantons used e-voting in one way or the other. The ***United Kingdom*** was very active in testing all kinds of electronic voting methods in the early 2000s. Trials in several constituencies between 2002 and 2007 involved ballot booth voting, kiosk voting, and internet voting. After negative experiences in other countries and critical voices from the UK Electoral Commission, [41] the government has not looked into e-voting opportunities any further. In March 2014 the chair of the UK Electoral Commission called for a modernization of elections and a move to online voting. [42]

Interesting enough, the implementation of the European Citizens' Initiative[9] in all EU Member States on 1 April 2012 recently stirred up discussions about new forms of e-participation in several member states since it is possible to sign a statement of support online. [43] The future will show whether this new instrument of direct democracy in the EU really has an impact on e-voting discussions around Europe.

V. Outlook

The future of e-voting certainly looked brighter when Rec(2004) 11 was adopted ten years ago. While e-enabled elections were still in their infancy, some kind of "e-voting hype" seemed to go around, which led to legal amendments or the first pilots in a number of countries. [44] In the meantime, some kind of stagnation has emerged [45] though current international examples show that electronic voting is possible – not only in a supervised environment but also with online solutions. [46] The reasons for a decline of the e-voting euphoria are multifaceted. The economic and financial crisis of

[9] Regulation (EU) No 211/2011 of the European Parliament and the Council of 16 February 2011 on the citizens' initiative.

2008 led to budget cuts in several countries; expensive innovation programs had to be stopped. Strict court decisions concerning the use of e-enabled voting [47] as well as a growing distrust of citizens in internet solutions after data leak and hacking incidents also did their bit. Concerns about security and reliability problems inherent to online applications were already present when passing Rec(2004)11, which states "(…) that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting." [48] Today it is mainly a political decision whether countries are willing to think about e-enabled voting as computers and the internet have already influenced our daily life in an unprecedented way. Permanently excluding modern technology from voting and participative instruments does not appear realistic.[10]

The Council of Europe continues to be the only organization in Europe to set intergovernmental standards in the field of e-voting. Accordingly, the informal experts' meeting in Vienna in December 2013 (similar to the 2012 review meeting) came to the conclusion that, (…) "taking into account the issues listed in this report and the high probability that in the medium and long term, the number of electoral systems will comprise some electronic features, there are a number of strong and valid reasons for updating Recommendation Rec(2004)11." The exact terms of such an update were left to the Council of Ministers, which debated the report in the Ministers' Deputies/Rapporteur Group on Democracy (GR-DEM) on 20 May 2014 but rendered no final decision. Even the definite organization of another review meeting by the Council of Europe Secretariat in late 2014 remained uncertain at that point of time. Thus Austria, along with Belgium, Estonia, Hungary, Latvia, Poland and Switzerland, sponsored a "non-paper" for information "in view of the meeting of the GR-DEM on 17 June 2014" in order "to call for the 5th Review Meeting to take place in Autumn 2014". The delegations emphasized that such a meeting could be organized "on a costs-lie-where-they-fall basis" to keep expenses "to an absolute minimum". The non-paper also suggested that the review meeting could be held back to back with the EVOTE 2014 conference in Lochau, Austria, to take advantage of the obvious synergies.

The Council of Europe Secretariat confirmed its support of the proposal in the GR-DEM meeting on 17 June 2014 and stated that the results of such a review meeting could even feed directly into relevant discussions at the World Forum for Democracy.[11] Official invitations for the 5th meeting "to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11", scheduled for 28 October in Lochau, were sent out by the Democratic Governance Directorate of the Council of Europe on 23 June 2014. The agenda contains the points "Horizon 2016: General exchange of views on a possible update of the CM Rec(2004)11 - defining the scope of a possible update" as well as "discussion of possible first elements of the future updated Rec(2004)11 and necessary conditions for the next steps: modus operandi, terms of reference, possible timeline". There is no denial that the Council of Europe's expertise and reputation in electronic voting is internationally renowned. The Recommendation, its review, and the general objective of developing secure use of the internet in the field of democratic elections currently form part of the Council of Europe's Internet Governance Strategy 2012-2015. [49] However, future activities will largely depend on the allocation of the essential budget. It will be up to the Committee of Ministers to say which role the Council of Europe wants to play in the area of e-voting in the future. In case of a "go" for a formal Recommendation update, its outstanding role in this matter would be re-iterated.

[10] In countries with multiple voting channels such as postal voting, the free selection of polling stations or mobile election commissions, the pressure to introduce e-voting does not seem to be as strong as in those countries where the present voting system is less flexible.

[11] To be held in Strasbourg on 3 to 5 November 2014 (http://www.coe.int/de/web/world-forum-democracy).

REFERENCES

[1] Krimmer, Overview, in Krimmer (Eds), Electronic Voting 2006, 2nd International Workshop Proceedings (2006) 9.x

[2] Barrat i Esteve/Goldsmith/Turner, International Experience with E-Voting, Norwegian E-Vote Project, IFES Study (2012) 1.

[3] Inter alia, Buchsbaum, Aktuelle Entwicklungen zu E-Voting in Europa, JRP 2004, 106; Grabenwarter, Briefwahl und E-Voting: Rechtsvergleichende Aspekte und europarechtliche Rahmenbedingungen, JRP 2004, 70; Stein/Wenda, E-Voting in Österreich, SIAK-Journal 3/2005, 3.

[4] IP 1 : Exploratory Workshop on e-voting (1-2 July 2002), Proposal for a Council of Europe activity on e-voting standards - document prepared by the United Kingdom authorities (http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Work_of_e-voting_committee/03_Background_documents/98IP1(2002)11_en.asp#TopOfPage).

[5] All meeting reports are available online: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Work_of_e-voting_committee/02_Agendas_and_Reports/Default_en.asp#TopOfPage

[6] See introduction on the CoE website on the E-Voting Project: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/

[7] Remmert, M. (2004), "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, P-47, Gesellschaft für Informatik, 15.

[8] Rec(2004)11, Preamble, Paragraph i.

[9] Rec(2004)11, Preamble, Paragraph iii.

[10] Rec(2004)11, Preamble, Paragraph iv.

[11] For further details see Maurer, Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29 November 2013.

[12] http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_relating_to_trial_internet_voting_2013.pdf

[13] http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf

[14] Madise, Ü. and Vinkel, P. (2011) "Constitutionality of Remote Internet Voting: The Estonian Perspective", Juridica International. Iuridicum Foundation, Vol. 18, 4–16.

[15] Whitmore K., Congress of Local and Regional Authorities (2008) Information Report on the Electronic Voting in the Finnish Municipal Elections, https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress

[16] Concerning e-voting in Switzerland see: http://www.bk.admin.ch/themen/pore/evoting/

[17] OSCE, Handbook for the Observation of New Voting Technologies (2013) 8.

[18] http://www.idea.int/publications/introducing-electronic-voting/loader.cfm?csmodule=security/getfile&pageid=47347 (published in 2011).

[19] Schwartz, B. and Grice, D. (2013) Establishing a legal framework for e-voting in Canada, http://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf

[20] U.S. Election Assistance Commission (2011) A survey of Internet Voting, http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

[21] Remmert, M. (2004) "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, P-47, Gesellschaft für Informatik, 14.

[22] CoE website: http://www.coe.int/t/dgap/democracy/Activities/GGIS/Default_en.asp

[23] CoE website: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/

[24] Wenda, „Good Governance in the Information Society" – Der Europarat und E-Voting, in Schweighofer/Kummer (Hrsg), Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts, Tagungsband des 14. Internationalen Rechtsinformatik-Symposions IRIS 2011 (2011) 293 ff.

[25] Report Fourth Review Meeting, 4 June 2013, DGII/Inf(2013)06, 5.

[26] Report Fourth Review Meeting, 4 June 2013, DGII/Inf(2013)06, 6.

[27] Report of the Fourth Review Meeting of 4 June 2013, DGII/Inf(2013)06, 5 ("… it should be noted that a number of member states represented at the review meeting [including Austria, which will hold the Chairmanship of the Committee of Ministers from November 2013 to May 2014] might be willing to consider making some extra-budgetary voluntary contributions to facilitate and expedite this work.")

[28] Maurer, Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29.11.2013.

[29] For a summary of the whole debate see Report of 25 April 2013, DGII/Inf(2014)06, 4-6.

[30] Report of 25 April 2013, DGII/Inf(2014)06, 4.

[31] Report of 25 April 2013, DGII/Inf(2014)06, 5.

[32] Sources of this summary include the relevant OSCE/ODIHR Reports, the proceedings of the EVOTE 2012 Conference near Bregenz, Austria, the Workshop Report of 25 April 2013, DGII/Inf(2014)06, 2-6, and notes of Robert Krimmer (ODIHR's expert on New Voting Technologies from 2010-2014).

[33] http://www.bmi.gv.at/cms/BMI_wahlen/wahlrecht/E_Voting.aspx

[34] Prosser, A., Krimmer, R., Kofler, R. Electronic Voting in Austria. Current State of Public Elections over the Internet, in: Kersting, Norbert, Baldersheim, Harald (eds): Electronic voting and democracy. A comparative analysis. New York (2004).

[35] For further details, see the evaluation report: http://www.e-voting.cc/wp-content/uploads/downloads/2012/05/Evaluierungsbericht_E-Voting_Hochschuelerinnen-_und_Hochschuelerschaftswahlen_2009.pdf

[36] http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[37] Trechsel, Alexander H. et al., 2007. Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe. Strasbourg, Council of Europe (2007).

[38] http://www.vvk.ee/voting-methods-in-estonia/engindex/

[39] http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

[40] http://www.regjeringen.no/nb/dep/kmd/pressesenter/pressemeldinger/2014/Ikke-flere-forsok-med-stemmegivning-over-Internett-.html?id=764300

[41] http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/KeyfindingsandrecommendationssummarypaPer_27191-20111__E__N__S__W__.pdf

[42] http://www.theguardian.com/politics/2014/mar/26/uk-e-voting-elections-electoral-commission-voters

[43] Inter alia, Stein/Wenda, Implementing the ECI: Challenges for the Member States, in Prosser (Eds), EDEM 2011, Proceedings of the 5th International Conference on E-Democracy (2011) 45.

[44] Inter alia, Kersting, Norbert, Baldersheim, Harald (eds): Electronic voting and democracy. A comparative analysis. New York: Palgrave (2004).

[45] Inter alia, R. Michael Alvarez & Thad E. Hall, Electronic Elections: The Perils and Promises of Digital Democracy (2010).

[46] See, inter alia, Barrat i Esteve/Goldsmith/Turner, International Experience with E-Voting, Norwegian E-Vote Project, IFES Study (2012) und den Bericht des „Fourth Review Meeting" vom 4. Juni 2013, DGII/Inf(2013)06, 2 ff.

[47] See especially the German Federal Constitutional Court ruling of 3 March 2009, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html and the Austrian Constitutional Court ruling of 13 December 2011, http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[48] Rec(2004)11, Preamble.

[49] CM(2011)175 final of 15 March 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20-%202015.pdf

Ten Years Council of Europe Rec(2004)11

Lessons learned and outlook

Ardita DRIZA MAURER
Jurist, Ll.M., Consultant
Switzerland
info@electoralpractice.ch

***Abstract*— E-voting must comply with requirements for democratic votes and elections. Adopted in 2004, the Council of Europe Recommendation Rec(2004)11 is one of the first regulatory efforts in this area and so far the only one at the international level. Its ambition is to map legal principles for democratic elections with operational and technical requirements specific to e-voting. This paper presents an overview of lessons learned from the application of the Recommendation during the past ten years and discusses the need for an update.**

Keywords—Council of Europe, e-voting, regulation, Rec(2004)11, recommendations, update

I. INTRODUCTION

The Recommendation of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, also known as Rec(2004)11 [17], was adopted on 30 September 2004 by the Committee of Ministers which also took note of the Explanatory memorandum thereto [18]. Both documents were compiled by a Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting.

The Recommendation defines e-voting as an e-election or e-referendum that involves the use of electronic means at least in the casting of the vote, covering both e-voting in controlled (e.g. voting machines in polling stations) and in uncontrolled environments (e.g. internet voting from a private computer). Rec(2004)11 became rapidly a reference for Council of Europe (CoE) States that introduce or envisage introducing e-voting[1]. It remains so far the only international instrument to propose an e-voting regulation.

Two additional instruments [14][15] were adopted in 2010, however with the lower status of guidelines. They propose guidance on certification and transparency issues and are meant to complete the recommendations on these issues[2]. A formal proposal to update the Recommendation was introduced in the 2012 review meeting. The issue of an update is on the agenda of the 2014 review meeting[3].

This paper reflects on the necessity of updating Rec(2004)11 based on e-voting experiences and the use of the Recommendation in the past ten years in the CoE region. The main arguments in favour of an update include lessons learned by experimenting with e-voting or by observing it, critical assessments of the Recommendation as well as technical developments (section 2). A possible line for approaching the update is presented by way of conclusion (section 3).

The paper is based on our report to the Council of Europe on the possible update of the Recommendation [19]. The report was discussed at a CoE's organized meeting of experts in Vienna (19 December 2013). Findings are grounded mainly on the documents of the four CoE biennial review meetings that took place since its adoption, on e-voting regulations and evaluations (e.g. by countries, by international organizations, etc.) and on e-voting related work by organizations or countries beyond the CoE region. The paper focuses on e-voting regulatory issues alone.

II. LESSONS LEARNED

A. The special place of Rec(2004)11

A recent study [2] mentioned that emerging international electoral standards on e-voting are struggling to catch up with the introduction of technology into the voting and counting process. This could also apply to Rec(2004)11.

The starting point for introducing the Recommendation in 2004 was the observation that member states are already using, or considering using e-voting for a number of purposes (see the Preamble). Ten years later, OSCE/ODIHR [34] observed that today, almost all electoral processes make some use of new technologies from voter registration to tabulation of results.

Regulating e-voting is a challenging task and countries look for guidance. The Recommendation timely responded to such needs, rapidly becoming a reference (see also [27] on the

[1] Country reports presented at the CoE biennial meetings on e-voting (see http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp) reflect the implementation of the recommendations by countries. U.S. EAC 2011 report on internet voting found that in particular internet voting systems were either conceived or updated by incorporating the CoE Recommendation.

[2] Transparency is dealt in paragraphs 20 to 23 (Appendix I) and certification in paragraphs 111 and 112 (Appendix III) of the Recommendation.

[3] A fifth review meeting on the Recommendation organized by the Council of Europe will be held on 28 October 2014 in Lochau/Austria, back to back with EVOTE 2014.

role of Rec(2004)11 in fostering e-democracy). It is still the only international instrument to propose standards for regulating remote and non remote e-voting. The adoption of common standards in the Recommendation was considered key to guaranteeing the respect of all the principles of democratic elections and referendums when using e-voting [18] [37].

A number of organisations have produced guidelines on the introduction of new technologies in voting. The OSCE/ODIHR [34], IDEA [5] the Carter Center [10], the Organization of American States [33] and the National Democratic Institute for International Affairs [35] have approached the issue of standards for electronic voting and counting technologies from the perspective of election observers. IFES [24] proposes a step-by-step approach to the introduction of e-voting, including legal considerations. IFES [45], IDEA [25] or the EU [23] discuss key principles that should inform the introduction of e- voting or more generally of technology in elections. The Council of Europe also developed a Handbook [16] to provide guidance on the steps to be considered when introducing e-voting.

These documents focus on identifying good practices or formalizing procedures. They do not aim at providing an e-voting regulation and most of them are domain specific focusing on the needs of election officials, observers and so on. They need to be taken into account when updating the Recommendation but they are not equivalent to it (e.g. in their respective scopes) and no substitute to it. One explanation to that may lie in the fact that no other institution has a mandate equivalent to the CoE in setting electoral standards, at least in Europe[4].

Rec(2004)11 has also been referenced by countries and organizations beyond the CoE region when considering e-voting regulations or standards. A study commissioned by Elections Canada [39] considers the work done by CoE in this field as the most extensive while creating a legal framework for a new technology. It recommends election officials to consider referencing the Rec(2004)11 check-list. The U.S. Electoral Assistance Commission [40] has referenced the Recommendation in an effort to locate standards and requirements on internet voting utilized elsewhere in the world which include voting specific functionality, accessibility and security requirements.

B. Guiding principles or detailed requirements?

Rec(2004)11 is a pioneer effort which attempts to apply a finite but not consolidated number of legal requirements for democratic elections, dispatched in a set of international instruments only some of which are mentioned in the Preamble of the Recommendation, to e-voting.

The Recommendation is a non-mandatory instrument despite the fact that it has been accepted unanimously by the Council of Ministers and it says that member states should consider reviewing their relevant domestic legislation in the light of this Recommendation when introducing e-voting (recommendation iii). Furthermore the text of the Recommendation and of the Explanatory Memorandum itself imply that the recommendations are not exhaustive. However, in several cases, the Recommendation has been considered as a ready-to-use check-list of requirements for building and evaluating e-voting systems. Whether the Recommendation is ready for this use is questionable.

Since the first review meeting in 2006 it has been reconfirmed that the Recommendation was accepted by member States as a valid benchmark by which to assess and evaluate e-voting systems. At the same time it has been admitted that several issues, such as accreditation, certification or observation needed further research. The two guidelines on certification and transparency were endorsed as providing a common reference to be viewed, however, as work in progress since the practical experiences in the field of e-voting were in constant evolution. The last 2012 review meeting concluded that existing loopholes, ambiguities or tensions in the Recommendation justify a formal update.

Norway is the only country to have given Rec(2004)11 recommendations (with few exceptions however) the status of legal basis regulating both 2011 and 2013 internet voting trials [31][32]. However some of the recommendations were excluded and Norway also introduced verification mechanisms which are not dealt with in the Rec(2004)11 such as return codes [4].

The Norwegian system has been evaluated [1] for its conformity to Rec(2004)11 (see also [3]). The evaluation [1] concludes that as a package, the Council of Europe Recommendations represent a very comprehensive and detailed set of standards for the conduct of electronic voting. The Norwegian Internet voting system was found compliant with 85 out of the 102 relevant recommendations and non-compliant with three recommendations. This was considered a significant achievement given the exacting nature of the Council of Europe Recommendations. The difficulties encountered in applying the requirements of Rec(2004)11 prompted the authors to present a critical assessment of the recommendations.

The study [1] concluded that the Recommendation does not build on existing public international law, that it says little on the legal basis, that it aims at designing standards applicable to all circumstances and such a broad scope is problematic when it comes to their implementation, that it ignores the fact that trade-offs between standards are sometimes necessary in electronic voting (such as the need for secret voting against the need for transparency, and the need to be able to audit the function of the voting system), that the need to comply with the Recommendation as a whole is problematic, that a number of standards may appear to be overlapping or redundant, that the wording is sometimes vague (interpretation is needed) and other times too detailed and, finally, that the recommendations are technically neutral

[4] According to article 1 of the 1949 adopted Statute of the Council of Europe the organization has the aim to achieve a greater unity between its members for the purpose of safeguarding and realising principles which are their common heritage. This aim shall be pursued by agreements and common action in legal and administrative matters. Article 15 of the CoE Statue foresees that action may take the form of recommendations to the governments of members. Available: http://conventions.coe.int/Treaty/en/Treaties/Html/001.htm

in their wording, but not in their consequences when attempting to comply.

Similar critiques on the wording and structure of Rec(2004)11 were also issued earlier in two theoretical analysis of the Recommendation [26], [30]. Without considering the merits of the standards included in the Recommendation, [30] employed engineering requirements and reverse engineering techniques to show that standards are expressed in a poor way and to make a first, simple, restructuring of the Recommendation. Considering the Recommendation as a check-list of requirements for system certification purposes, the study concludes that the Recommendation as it stands makes certification against standards difficult. Several "original flaws" are identified including inconsistency, incompleteness and unclear scope, over-specification, under-specification, redundancy and repetition as well as maintainability and extensibility issues. The authors believe that a broadly applicable instrument would be genuinely useful both to governments procuring e-voting systems, and to vendors developing and maintaining such systems. So they undertake a first-step restructuring of the Recommendation, rooting out the identified original flaws.

Another study on a concrete use of the Recommendation [20] questioned the possibility for Rec(2004)11 to handle sufficiently real-world attacks against elections using e-voting. Under this perspective the Recommendation was considered as being (or ought be) specific enough as to provide detailed solutions to deal with specific threats such as skilled, creative, personally motivated and appropriately equipped students planning and executing attacks against e-voting systems. The authors propose that Rec(2004)11 be further improved by explicitly pointing out the necessity of implementing adequate countermeasures to different types of attacks and that the development of a special security strategy to deal with attacks that target voters' acceptance of e-voting should be recommended in Rec(2004)11.

The discussion on the adequacy of national regulations to cover current forms of e-voting and the required level of detail of such regulations is informative also for Rec(2004)11 given the similar challenges that all regulations face. The German Constitutional Court considered in its 2009 decision [8] that the Federal Ordinance on the Deployment of Voting Machines in Elections was unconstitutional because it did not contain provisions ensuring that only those voting machines are approved and used which comply with the constitutional preconditions of the principle of the public nature of elections (see paragraph 145 and ff. of the Court's decision) which requires that each voter, without any specific technical knowledge, is able to make sure that the system performs correctly.

The Austrian Constitutional Court in its 2011 decision [42] arrived at a similar conclusion, although based on different principles. The act regulating the elections of the Students' Union was found to be unconstitutional because it did not provide detailed requirements on the e-voting system and on the procedures to ensure that competent authorities could exercise their controlling rights. Both the German and the Austrian quashed regulations have not been updated since.

The Estonian Constitutional Judgement of the Supreme Court of 2005 [38] examined the e-voting legal basis only from the point of view of the principle of constitutionality in relation with the right to change a vote in the internet voting context alone. The Court explained that the right to change the e-vote is in accordance with the CoE Recommendation [29] and with the Estonian Constitution.

The adequacy and level of detail of national e-voting regulations have been discussed elsewhere as well. Belgium Federal and Regional Administrations commissioned a thorough study on e-voting [6] which considers Rec(2004)11 as the main benchmark for evaluating e-voting.

Finland's use of voting machines in polling stations was monitored in the light of Rec(2004)11 by both Electronic Frontier Finland [21] - a Finnish non-profit - and the Council of Europe, Congress of Local and Regional Authorities [44].

France's non-remote e-voting is regulated by specific legislation while remote internet voting, must comply with recommendations by the National Commission on Informatics and Liberties [12] whose structure and content presents many commonalities with Rec(2004)11. A recent thorough report [11] recommended that the list of legal requirements for authorizing the use of voting machines must be completed (recommendation 2).

Netherlands discontinued all forms of e-voting because, in addition to computer security problems, the embedding of the voting machines within the legal framework was considered very weak. Another lesson from the Netherlands is that technical choices made in the past to embed basic principles of elections need to be periodically reconsidered [28].

Swiss federal legislation on e-voting from uncontrolled environments introduced in 2002 presented many commonalities with Rec(2004)11 [7]. The Federal Ordinance[5] was recently modified to reflect lessons learned during the past ten years [13] and was completed with a detailed technical regulation[6].

To conclude, the scope and aim of the Recommendation need to be clarified. While Rec(2004)11 was initially intended to provide guidance, it has in several occasions been referred to as a complete and comprehensive list of requirements against which to evaluate e-voting systems. As a guiding document the Recommendation is sometimes too detailed and when considered as a take-it-or-leave-it check-list of requirements its application has proved difficult.

Furthermore the level of detail of the Recommendation requires special attention. In the light of experiences made and lessons learned so far it can be assumed that a readily implementable check-list of requirements will receive greater attention. It should be comprehensive and coherent to facilitate implementation and control. It should at least contain necessary requirements to ensure compliance of e-voting with

[5] In force since 15 January 2014, http://www.admin.ch/opc/fr/classified-compilation/19780105/index.html

[6] In force since 15 January 2014, the technical regulation is a Federal Chancellery Ordinance: http://www.admin.ch/opc/fr/classified-compilation/20132343/index.html

all international standards for democratic elections while leaving individual countries the necessary room for implementing their own electoral specificities.

C. Placing e-voting into its context

Reference [26] found it problematic that requirements (mainly security requirements) for e-voting are measured (*as secure as*) against requirements for non-electronic voting systems. As there exist no widely accepted metrics for measuring, reasoning by analogy flaws the comparison between the two. This critique needs to be addressed in a future update.

Reference [26] also draws attention to the necessary distinction between matters of public policy which affect the whole electoral system and matters of voting technology when introducing recommendations. The following example from the implementation of the Recommendation illustrates this.

In some cases, the same recommendation is implemented in opposing ways by different countries in accordance with their own specificities. This is the case with "secrecy and freedom of the vote" (recommendations 9 to 19). Norway and Estonia introduced multiple voting, or the right to change the e-vote for internet voters alone and a precedence of paper ballots over electronic ballots. This was meant to offer the voter a way to get around voting coercion and vote buying (which may arise in remote voting, because the voter can be forced to cast his or her vote in the presence of another person). Although multiple voting literally contradicts recommendation 5, [4] and [38] found that this may be interpreted to respect the Recommendation. France and Switzerland do not allow multiple voting and assign the same value to a validly issued ballot, be it on paper or electronic. Their point of view is that internet voting is just another form of distant voting from an uncontrolled environment, and that coercion will not be addressed differently for internet voting than for postal voting. ODIHR[7] encourages France and Switzerland to introduce multiple voting but says nothing of the impact this would have on the system as a whole given the inequality it will create with other channels and the fact that not all voters have access to internet voting.

The national legal context should be taken into account when regulating e-voting. Some issues may only concern e-voting. Others, although introduced in an e-voting context, are a matter of public policy (for example related to remote voting) not of voting technology. Their introduction will affect the whole system. Furthermore the technical dimension of e-voting is important and should be kept in mind when regulating it. Reasoning by analogy with postal voting has serious limits and must be used with care.

D. Same provisions for different e-voting systems?

Rec(2004)11 applies a number of legal requirements for democratic elections to an indefinite number of voting solutions, collectively known as remote and non-remote e-voting, that only share one common characteristic: the use of electronics in casting the vote. As the above mentioned analysis of the conformity of the Norwegian system showed, several recommendations are clearly written with non-remote e-voting in mind and have proved difficult to implement in an internet voting context.

Requirements and standards in the Recommendation should clearly indicate to which of the two types of e-voting they apply. Venice Commission [22] stated that e-voting in supervised environments must be treated differently from e-voting in unsupervised environments. In particular, the issues of secrecy and freedom of the vote are to be handled differently in the two cases. So, a prior determination when updating the Recommendation should be clearly to distinguish between the two categories. There is general consensus on this admitted conclusion and it was included in the report of the Rec(2004)11 review meeting of 2012 as well.

E. Technology developments, new concepts and solutions

As indicated by its title, the Recommendation is multi-disciplinary and requires combined expertise from different areas. Important work has taken place on the technical aspects of e-voting such as e-voting protocols, e-voting control and certification or e-voting increased transparency through cryptographic solutions[8]. Their consideration in the light of Rec(2004)11 goes beyond the scope of this paper. However their significance for the Recommendation needs to be examined in view of an update.

An interesting example from a regulatory perspective is work on certification [43] as it illustrates the impact legislation has on the design and control of e-voting systems. The broad principles mentioned in Appendix I of the Recommendation serve as legal background. Based on them, detailed security requirements and methods to measure and evaluate e-voting systems' security have been developed. They must be considered in view of an update of the recommendations, namely those contained in Appendixes II and III.

OSCE/ODIHR has monitored the use of e-voting in elections in different CoE countries. Its reports provide valuable information on the implementation of the Recommendation (which serves as a legal benchmark) as well as on the legal frameworks for e-voting in different countries[9]. ODIHR often gives substance to high-level requirements. Its 2013 published Handbook for the observation of new voting technologies includes a collection of such detailed recommendations. However the leap from the general OSCE and Council of Europe requirements to specific

[7] See OSCE/ODIHR'S 2012 reports on both countries' parliamentary elections, http://www.osce.org/odihr/elections

[8] Proceedings of periodical conferences such as Bregenz EVOTE, EVT/Wote, and Vote-ID give a good overview of such developments. See the respective websites: http://www.e-voting.cc/en/publications/proceedings/ ; https://www.usenix.org/conference/evtwote ; http://www.voteid13.org/

[9] OSCE/ODIHR has reported on the use of new voting technologies in several countries in the region and beyond, including Norway 2013, U.S.A. 2013, France 2012, Norway 2012, Switzerland 2012, Russian Federation 2012, Estonia 2011, Belgium 2007, Estonia 2007, Finland 2007, Kazakhstan 2007, the Netherlands 2007, Belgium (Expert Visit on New Voting Technologies) 2006, Kazakhstan 2006. All reports can be retrieved from http://www.osce.org/odihr/elections

recommendations such as those on introducing verifiability in e-enabled elections, is somewhat huge and only based on the even-less-mandatory Guidelines on transparency[10].

Several new concepts have been discussed and even introduced in the past ten years in e-voting. Most of them aim at ensuring transparency and fostering trust and confidence in the e-voting channel and are reflected in the Guidelines on transparency. Such concepts include "the use of a second medium to store the vote to improve transparency", the related "mandatory count of the second medium in a statistically meaningful number of randomly selected polling stations", specific "rules dealing with discrepancies between the mandatory count of the second medium and the official electronic results", the requirement to "gain experience in providing mechanisms that allow voters to check whether their vote was counted as intended" (paragraphs 13 to 16 of the Guidelines). Also the concept of "chain of trust in e-enabled elections" according to which voters should be able to verify if their e-vote was cast as intended, recorded as cast and counted as recorded has been implemented, introducing a new possibility for the voter to prove that their own single e-vote was cast as intended, recorded as cast and counted as recorded.

Although inspired by traditional voting, these mechanisms are new to electoral legislation. They are specific to e-voting and appear today as necessary to ensure that the public can place the same trust in e-voting as in other non-electronic voting systems. As usual with experiments, practice has so far preceded regulation. However we are now at a point where there exists a certain consensus on their use and they are being introduced in a number of countries[11]. Such new concepts and mechanisms being legally relevant, they need to be defined and their use regulated by law. The general requirements of transparency in the Recommendation and Guidelines do not regulate their implementation, operation, and control.

In addition to new concepts, our understanding of existing concepts has evolved. Experience with e-voting machines in the U.S.A. for instance shows that while voting system standards and certification against standards are useful for examining the basic aspects of voting machines, they cannot ensure secure voting systems, security being a negative quality [9]. A recent report [36] recommended reforming the certification process and conducting systematic after-election-auditing of voting equipment. Similar arguments are heard in Europe as well where the cost-efficiency of certification has been questioned and individual and universal verifiability is seen as offering better guarantees while at the same time being less costly than certification.

In the light of the previous examples and given the recognized position of the Recommendation in the regulatory field, it is necessary that Rec(2004)11 be updated to take into account technology developments and current practices.

III. UPDATE OF REC(2004)11

As with other technology related developments, e-voting regulation is being adjusted as technology advances and our understanding of it improves. In order to provide basic guidance for countries and also ensure that Council of Europe's electoral heritage is integrated in a coherent way in e-voting regulations by countries, the Recommendation needs an update in the light of recent developments and experience gained. Below we will present some thoughts on how to tackle the updating work.

A. Prior determinations

Compared to a similar document, the U.S. Voluntary Voting System Guidelines (VVSG) [41], the structure and language of Rec(2004)11 is very different. Both are voluntary. However, if adopted, VVSG provides a check-list ready for use by authorities, vendors, certifying bodies, etc., while Rec(2004)11 was intended to provide guidance, although some parts of it are too detailed for such a purpose.

Before undertaking a thorough update of the Recommendation, a decision has to be made on the kind of document we want. It can be assumed that a readily implementable (by authorities as well as by industry) check-list will receive greater attention. This decision will influence the structure, content, level of detail and wording of the entire Recommendation.

As mentioned earlier the level of detail requires attention. A detailed Recommendation may be interesting as countries look for guidance. However, the higher the level of detail, the greater the probability that the Recommendation cannot apply 100% in a specific case. A solution could be to adopt a modular approach, instead of the current situation which requires that the Recommendation be applied as "one block". The modular approach implies a mandatory layer of recommendations (minimum standards applicable everywhere in the region) on which modules of additional, optional standards would be build. Both a generic document and a more detailed one are possible choices for the Recommendation. Both require a good interleaving of legal, operational and technical requirements. Once the level of detail has been decided, it has to be applied coherently throughout the document.

Another prior determination would be clearly to distinguish recommendations dedicated to e-voting in controlled (polling stations) or in uncontrolled (remote voting) environments.

The Recommendation and the two Guidelines were developed separately (respectively in 2004 and 2010) and have different legal value. However they are closely linked to each other. Consolidating the three documents (merging, simplifying and streamlining) may be necessary.

In a second step, consideration may be given to a possible separation of hard-core requirements from more rapidly changing ones. Such a trend is observed in other similar

[10] Examples include the recommendation in 2007 that Belgium introduces legislation on voter verified paper audit trail (VVPAT) or an equivalent verification procedure and the recommendation (2012) to France and Switzerland to consider the use of a verifiable internet voting scheme or an equally reliable mechanism for voters to check whether or not their votes were cast as intended.

[11] In addition to Norway, Estonia and several Swiss cantons are introducing E2E verification mechanisms.

regulations such as the European Citizens Initiative regulatory framework[12] as well as in national regulations on e-voting as shown by the latest modification of the Swiss federal regulation on e-voting.

B. Updating policy

Experiences indicate that an update of the Recommendation is currently necessary to reflect lessons learned and new developments. Additionally, a management and maintenance policy for the Recommendation is needed. This is necessary in particular if the Recommendation is conceived as a check-list of requirements with respect to technical requirements that embed legal principles for democratic elections. Experts from different disciplines such as law, engineering, mathematics etc. must be involved in the maintenance work. Their proposals should be validated by member States' representatives before being presented to the Committee of Ministers with the request to formally update the Recommendation.

In this respect it is necessary to define an updating policy and the scope and purpose of updates. An updating opportunity cannot be used to question everything continually. An update being a further development of issues, it is up to the body responsible for mandating the update also to define and scope it.

Update rates can fit in the biennial review cycle of Rec(2004)11 which is meant for recommendations and updates to be discussed in detail. However, the bulk of the work needs to be conducted by experts who will most probably meet more frequently, physically or virtually, in between meetings. Work done by them must be presented to and validated by member States' representatives at biennial meetings.

Biennial review meetings are important and fulfil their mandate as long as they have an active role in the updating of the Recommendation. If no update is proposed, if there is no follow-up on countries' experiences and lessons learned, the Recommendation will gradually become obsolete and biennial meetings would lose their substance.

C. Final remarks

E-voting regulations are still in their infancy and have not yet reached the maturity of the rest of electoral legislation. This is also true for Rec(2004)11 whose application in the past ten years provides us with important lessons which, in return, call for an update.

If work in 2004 started from a theoretical perspective, updating work in 2014 should start by considering the practical needs of administrations, voters, industry and other stakeholders.

The initial enthusiasm for e-voting in 2004 has given way to more lucidity and maturity in the consideration of risks and opportunities. Today's understanding of IT and e-voting should be duly taken into account in the updating process.

The aim is to ensure that the Recommendation is up-to-date, balanced and responsive to ongoing developments. A revised Recommendation would allow the Council of Europe to maintain its position as a recognised and cutting-edge actor in the field of e-voting.

[12] See Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative, (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:065:0001:0022:en:PDF) and the Commissions' implementing regulation of 17 November 2011 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF)

All internet sources cited in this paper were accessed end August 2014

[1] Barrat, J. and Goldsmith, B. (2012) *Compliance with International Standards, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

[2] Barrat, J., Goldsmith, B. and Turner, J. (2012) *International Experience with Internet Voting, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf

[3] Barrat, J., Goldsmith, B. and Turner, J. (2012) *Speed and Efficiency of the Vote Counting Process, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic4_Assessment.pdf

[4] Barrat, J., Chevallier, M., Goldsmith, B., Jandura, D., Turner, J. and Sharma, R. (2012) "Internet voting and individual verifiability: the Norwegian return codes", in Kripp, M., Volkamer, M., Grimm, R. (Eds.) *Electronic Voting 2012, Proceedings of the 5th Conference on Electronic Voting 2012 (EVOTE2012)*

[5] Barrat, J. (2012) *Observing e-enabled elections: how to implement regional electoral standards*, http://www.idea.int/democracydialog/upload/Observing-e-enabled-elections-how-to-implement-regional-electoral-standards.pdf

[6] BeVoting, (2007) *Study of electronic voting systems, Part I, 15 April 2007 and Part II, 12 October 2007*, Part I http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf, Part II http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections2011/fr/presentation/bevoting-2_gb.pdf

[7] Braun, N. (2004) 'E-Voting: Switzerland's Projects and their Legal Framework – in a European Context' in Prosser, A. and Krimmer, R. (Eds.) *Electronic Voting in Europe. Technology, Law, Politics and Society*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-47, pp. 43-52.

[8] Bundesverfassungsgericht (2009), Decision *2 BvC 3/07, 2 BvC 4/07, of 3 March 2009*, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.htm

[9] CALTECH/MIT Voting Technology Project (2012) *Voting, What has changes, What hasn't & What needs improvement* http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement

[10] (The) Carter Center (2012) *The Carter Center Handbook on observing electronic voting, second edition*, http://www.cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf

[11] Commission des lois constitutionnelles du Sénat français/Anziani, A. and Lefèvre A. (2014) *Rapport d'information no 445 (2013-2014) sur le vote électronique*, http://www.senat.fr/rap/r13-445/r13-445.html

[12] Commission Nationale de l'Informatique et des Libertés/France (CNIL) (2010), *Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique*, http://www.cnil.fr/documentation/deliberations/deliberation/delib/249/

[13] Conseil fédéral/Suisse (2013) *Rapport du Conseil fédéral sur le vote électronique. Evaluation de la mise en place du vote électronique (2006-*

2012) et bases de dévelopment, du 14 juin 2013, http://www.bk.admin.ch/themen/pore/evoting/07977/index.html?lang=fr

[14] Council of Europe (2011) *Certification of e-voting systems, Guidelines for developing processes that confirm compliance with prescribed requirements and standards*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf.

[15] Council of Europe (2011) *Guidelines on transparency of e-enabled elections*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf

[16] Council of Europe/Susanne Caarls (2010) *E-voting handbook, Key steps in the implementation of e-enabled elections*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting2010/Biennial_Nov_meeting/ID10322 GBR 6948 Evoting handbook A5 HD.pdf

[17] Council of Europe (2004) *Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, adopted by the Committee of Ministers on 30 September 2004, https://wcd.coe.int/ViewDoc.jsp?id=778189

[18] Council of Europe (2004) *Explanatory Memorandum to the Draft 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

[19] Driza Maurer, A. (2013) *Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29 November 2013*, http://www.electoralpractice.ch/wp-content/uploads/2014/01/REPORT-DRIZA-MAURER-20131129.pdf

[20] Ehringfeld, A., Naber, L., Grechenig, T., Krimmer, R., Traxl, M. and Fischer, G. (2010) "Analysis of Recommendation Rec(2004)11 based on the experiences of specific attacks against the first legally binding implementation of e-voting in Austria", in Krimmer, R. and Grimm, R. (Eds.) *Electronic Voting 2010 (EVOTE10)*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-167, pp. 225-237

[21] Electronic Frontier Finland, Vähä-Sipilä, A. (ed.) (2009) *A report on the finish e-voting pilot*, http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf

[22] European Commission for Democracy through Law (Venice Commission)/Grabenwarter, Ch. (2004) *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*, http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx

[23] European Commission (2006) *Methodological Guide on Electoral Assistance*, http://ec.europa.eu/europeaid/multimedia/publications/documents/thematic/ec_methodological_guide_on_electoral_assistance_en.pdf

[24] Goldsmith, B. (2011) *Electronic Voting & Counting Technologies, A Guide to Conducting Feasibility Studies*, IFES Election Technology Series, http://www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf

[25] IDEA (2011) *Introducing electronic voting, Essential Considerations. Policy paper*, http://www.idea.int/publications/introducing-electronic-voting/

[26] Jones, D. (2004) *The European 2004 Draft E-Voting Standard: Some critical comments*, http://homepage.cs.uiowa.edu/~jones/voting/coe2004.shtml

[27] Krimmer, R. (2012) "The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy", *Tallinn University of Technology Doctoral Theses Series I: Social Sciences, No. 19*

[28] Loeber, L. (2008) "E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years" in Krimmer, R. and Grimm, R. (Eds.) (2008) *Electronic Voting 2008 (EVOTE08)*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-131

[29] Madise, Ü. and Vinkel, P. (2011) "Constitutionality of Remote Internet Voting: The Estonian Perspective", *Juridica International. Iuridicum Foundation*, Vol. 18, pp. 4–16.

[30] McGaley, M. and Gibson, J.P. (2006) *A Critical Analysis of the Council of Europe Recommendations on e-voting*, https://www.usenix.org/legacy/event/evt06/tech/full_papers/mcgaley/mcgaley.pdf

[31] Norway (2013) *Regulations relating to trial internet voting during advance voting and use of electronic electoral rolls at polling stations on election day during the 2013 parliamentary election in selected municipalities*, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_relating_to_trial_internet_voting_2013.pdf

[32] Norway (2011) *Regulations relating to trial electronic voting during advance voting, use of electoral roll at polling stationsand use of new ballot papers at the 2011 municipal and county council elections in the selected municipalities of Bodø, Bremanger, Hammerfest, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn and Ålesund, and the county municipalities of Møre og Romsdal, Hedmark, Vestfold, Vest-Agder, Rogaland, Hordaland, Sogn og Fjordane, Nordland and Finnmark*, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/E-valgsforskriften_endelig_versj_230611_engelsk.pdf

[33] Organisation of American States (2010) *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*, http://www.oas.org/es/sap/docs/Technology English-FINAL-4-27-10.pdf

[34] OSCE/ODIHR (2013) *Handbook for the observation of new voting technologies*, http://www.osce.org/odihr/elections/104939

[35] Pran, V. and Merloe, P. (2008) *Monitoring electronic technologies in electoral processes: an NDI guide for political parties and civic organizations*, http://www.ndi.org/node/14616

[36] Presidential Commission on Election Administration (2014) *The american voting experience: Report and Recommendations of the Presidential Commission on Election Administration*, https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

[37] Remmert, M. (2004) "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), *Electronic Voting in Europe - Technology, Law, Politics and Society*, P-47, Gesellschaft für Informatik, pp. 13–16.

[38] Republic of Estonia, Supreme Court, *Judgment of the Constitutional Review Chamber of the Supreme Court, Decision 3-4-1-13-05, 1st September 2005*, http://www.nc.ee/?id=381

[39] Schwartz, B. and Grice, D. (2013) *Establishing a legal framework for e-voting in Canada*, http://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf

[40] U.S. Election Assistance Commission (EAC) (2011) *A survey of Internet Voting*, http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

[41] U.S. Election Assistance Commission (EAC) (2005) *2005 Voluntary Voting System Guidelines*, http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

[42] Verfassungsgerichtshof (2011) Decision *V 85-96/11-15, 13 December 2011*, http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[43] Volkamer, M. (2009) *Evaluation of Electronic Voting, Requirements and Evaluation Procedures to Support Responsible Election Authorities*, Springer-Verlag Berlin Heidelberg 2009

[44] Whitmore K., Congress of Local and Regional Authorities (2008) *Information Report on the Electronic Voting in the Finnish Municipal Elections observed on 26 October 2008, 1 December 2008*, https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress

[45] Yard, M. (Ed.) (2010) *Direct Democracy: Progress and Pitfalls of Election Technology*, IFES Election Technology Series, http://www.ifes.org/Content/Publications/Books/2010/Direct-Democracy-Progress-and-Pitfalls-of-Election-Technology.aspx

Electronic Voting in Polling Stations

Implementation and Evaluation of the EasyVote Tallying Component and Ballot

Jurlind Budurushi
and Melanie Volkamer
Computer Science Department
Technische Universtität Darmstadt
Darmstadt, Germany
Email: name.surname@cased.de

Karen Renaud
School of Computing Science
University of Glasgow, UK
Email: karen.renaud@glasgow.ac.uk

Marcel Woide
Psychology Department
Technische Universtität Darmstadt
Darmstadt, Germany
Email: marcel.woide@cased.de

***Abstract*—The German federal constitutional court ruled, in 2009, that elections had to have a public nature. EasyVote, a promising hybrid electronic voting system for conducting elections with complex voting rules and huge ballots, meets this requirement. Two assumptions need to hold, however. The first is that voters will verify the human-readable part of the EasyVote ballot and detect discrepancies. Secondly, that electoral officials will act to verify that the human-readable part of the ballot is identical to the machine-readable part, and that they, too, will detect discrepancies. The first assumption was tested in prior work, so in this paper we examine the viability of the second assumption.**

We developed an EasyVote tallying component and conducted a user study to determine whether electoral officials would detect discrepancies. The results of our user study show that our volunteer electoral officials did not detect all of the differences, which challenges the validity of the second assumption.

Based on these findings we proceeded to propose two alternative designs of the EasyVote ballot: (1) In contrast to the original EasyVote ballot, the human-readable part highlights only the voter's direct selections in orange, i.e. votes that are automatically distributed by selecting a party are not highlighted; (2) The second alternative includes only the voter's direct selections and highlights them in orange. Both alternatives reduce the number of required manual comparisons and should consequently increase the number of discrepancies detected by election officials. We evaluated both alternatives in an online survey with respect to ease of verification and understandability of the cast vote, i.e. verifying that the human-readable part contained the voter's selections and understanding the impact (distribution of votes) of the corresponding selections.

The results of the online survey show that both alternatives are significantly better than the original EasyVote ballot with respect to ease of verification and understandability. Furthermore, the first alternative is significantly better than the second with respect to understandability of the cast vote, and no significant difference was found between the alternatives with respect to ease of verification of the cast vote.

I. Introduction

The German saying "different countries, different customs" holds true for elections, which can be very different between and even within countries. Some elections, like parliamentary elections in Estonia or Germany have very simple voting rules and small ballots. Voters can select 1 out of n-candidates, where n is a relatively small number between two and 20. Other elections, like parliamentary and European elections in Luxembourg, parliamentary elections in Belgium and local elections in Germany (e.g. Bavaria, Bremen, Hamburg, Hesse), have very complex voting rules and huge ballots. In this paper we focus on the local elections in Hesse, because we were able to access original materials, e.g. ballots, tallying software and training presentations, used in the 2011 elections. In these elections voters can cast up to 93 votes[1] depending on the size of the district; usually more than ten parties and more than 450 candidates participate, which results in huge ballots, nearly the size of an A0[2] sheet of paper (Size: 27" x 35"). Furthermore, voters can select a party (votes are automatically assigned to the candidates of the selected party according to the list order), and cross out candidates they do not like. They can perform vote splitting (cast votes for candidates of different parties) and cumulative voting (cast up to three votes for each candidate). Such complexity introduces challenges regarding both vote casting and tallying processes. In the vote casting process, voters might unintentionally spoil their vote, due to the complex voting rules. Furthermore, the tallying process is very time intensive and likely to be error prone, because of the combination of complex voting rules and huge ballots.

In order to address these challenges and improve the situation for both voters and poll workers, in particular for local elections in Hesse, Volkamer *et al.* [2] proposed an electronic voting system, called EasyVote. The EasyVote system can be briefly described as follows: 1) Voters prepare their ballots on a voting device, which prints their selections. The printed ballot contains voters' selections in a human- and machine-readable (a plaintext QR-Code) format. 2) Voters deposit their ballots into the ballot box. 3) Ballots are tallied automatically, by scanning the QR-Codes on the printouts.

Budurushi *et al.* [3] evaluated a number of electronic voting systems with respect to their feasibility for use in elections with complex voting rules and huge ballots. They report that, with respect to the *public nature of elections*[3] and

[1]This number depends on the the number of available seats, which also limits the number of candidates nominated by a party.

[2]A0 according to [1].

[3]This principle was introduced by the Federal Constitutional Court of Germany in 2009, and states that it must be possible for the citizen to verify the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge, i.e. each election step must be transparent for the voter.

secrecy legal requirements, the EasyVote system supported the complex local elections in Hesse better than the other systems. Henning *et al.* [4] analysed the EasyVote system from a legal perspective and showed that it complied with German requirements for local elections in Hesse.[4] Both analyses [3], [4] rely on the following assumptions being true: (1) Voters will act to verify the correctness of the human-readable part of their ballots; (2) Voters will detect discrepancies; (3) Electoral officials will verify that the human-readable matches the machine-readable part (QR-Code); (4) Electoral officials will detect discrepancies. However, before EasyVote can be used in practice, the validity of these assumptions has to be verified. With respect to the first and second assumptions, Budurushi *et al*. [5] showed that the number of voters that verified their printouts and detected discrepancies could be increased significantly if voters were provided with pre-printed, "just-in-time" verification instructions.

Thus, in the first part of this paper we focus our attention on the actions of electoral officials during the tallying process. We implemented a tallying component prototype based on the EasyVote system. The tallying process itself could, in general, be achieved using different techniques: (1) by scanning the printouts with different scanners manufactured by different manufacturers (trust distribution), or (2) by scanning printouts and performing either risk-limiting audits described in [6] and [7], or the Bayesian method described in [8], or (3) by scanning each ballot and comparing the human-readable printout with the details on the screen (generated from the QR-Code). We implemented the latter process, as this complies with the legal requirements [4]. We do not know whether the other techniques are aligned with the public nature of elections, because, to the best of our knowledge, no legal analysis has been conducted yet. Since electoral officials have to scan a large number of individual ballots, one after the other, the accuracy of the process becomes important and therefore should be evaluated. Accuracy is particularly important, because it relies on human attention, which is notoriously unreliable [9], [10]. This is especially the case when the prevalence of the target to be noticed is low [11], [12], when the searcher has to look for multiple different targets at the same time [13] and when the size of the area to be searched is large [14]. All of these are true for the EasyVote ballots so it seems important to test the impact of this well-known human limitation on the checking required during the EasyVote tallying process. Therefore in a user study, we evaluated the *accuracy* of the EasyVote tallying component by intentionally introducing manipulated printouts, i.e. printouts where the human-readable part did not match the machine-readable part (the data stored in the QR-Code). Note that the goal was to evaluate the *accuracy* of the actions of electoral officials during the implemented tallying process, thus we assumed a compromised vote casting component and an honest and correctly implemented EasyVote tallying component. The results of this study show that this way of effecting the tallying in EasyVote is not fully accurate as we rely on human ability to detect differences and our participant "electoral officials" did not detect all the manipulations we introduced during their scanning and verification process. The study also revealed that it will be necessary either to improve the EasyVote system or to relax the legal requirements.

Based on these findings, in the second part of this paper we focused on improving the process and proposed two alternative EasyVote ballot designs: (1) In contrast to the original EasyVote ballot, the human-readable part highlights the voter's direct selections in orange, i.e. votes that are automatically distributed by selecting a party are not highlighted; (2) The second alternative includes only the voter's direct selections and highlights them in orange. Both alternatives reduce the number of required manual comparisons and should consequently increase the number of discrepancies detected by the poll workers. We evaluated the alternatives in an online survey with respect to *ease of verification* and *understandability* of the cast vote, i.e. verifying that the human-readable part contains the voter's selections and understanding the impact (distribution of votes) of the corresponding selections. The results of the online survey show that the alternatives are significantly better than the original EasyVote ballot with respect to ease of verification and understandability of the cast vote. Furthermore, the first alternative is significantly better than the second with respect to understandability of the cast vote, and no significant difference was found between the alternatives with respect to ease of verification of the cast vote.

II. Background

We first explain the traditional tallying process in the local Hesse elections. The paper ballots used in the traditional local elections in Hesse are shown and elaborated on in Figure 1. The traditional tallying process in the local elections in Hesse comprises two phases. Both phases are led by an electoral official who gives instructions to other electoral officials and observes the process. In the first phase, at the end of the election day, electoral officials perform the following steps:

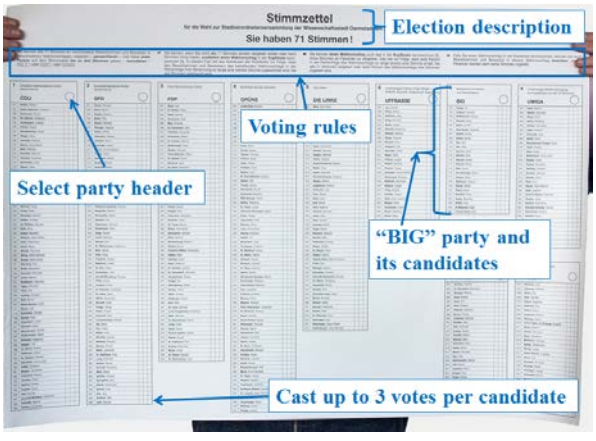


Fig. 1: Paper ballot of the local elections in Hesse in 2011. (Size: 27" x 35")

- Open the ballot boxes, count the total number of cast ballots and compare it with the total number of marked voters in the electoral register.

[4]As the legal evaluation is in German, we outline here the most important conclusions: (1) Voters can verify their vote without any specialist knowledge. (2) Voters are not required to rely on the system's integrity. (3) The system enables an automatic tally of single votes, and also a full manual tallying of votes, similar to the traditional one. (4) The human-readable part is the deciding factor regarding the tallying process. (5) The system strengthens the principle of the "public nature of elections", since on the one hand voters can better understand the impact of their selections, and on the other hand the tallying process might be faster and more accurate than the traditional one.

- Divide the ballots into four categories: 1) Only party header is marked 2) Candidates and/or a party header are marked 3) Invalid 4) Not assignable to 1), 2) or 3).
- Check that ballots are assigned to the correct category.
- Divide and count the 1st category by parties (first intermediate result).
- Discuss and assign each single ballot of the 4th to the 1st, 2nd or 3rd category.
- Manually recompute the intermediate election result, based on the 1st and 3rd category.

The second phase of the tallying process takes place the day after the election. This phase is supported electronically by special purpose software. The software used by traditional local elections in Hesse is called PC-Wahl.[5] During this phase only ballots from the 2nd category, i.e. ballots that contain marked candidates and/or a party header, are tallied. Electoral officials perform the following steps:

- Electoral officials enter the intermediate result from the first phase.
- First five ballots are entered and recorded into the PC-Wahl interface (Figure 2).
- Manually tally the first five ballots.
- Compare the electronic result with the manual result.[6]
- Enter and record the rest of the ballots into the corresponding PC-Wahl interface.
- Electronically compute the final election result, and sign the printed disposition.

The process of entering and recording ballots via the corresponding PC-Wahl interface is performed by three electoral officials. One electoral official narrates the marks from the ballot and a second enters them into the PC-Wahl interface. A third electoral official verifies that the first and second electoral officials have performed this correctly.

Note that electoral officials who participate in the second phase of the tallying process are employees of the corresponding electoral office and/or municipality. Hence, they have relatively high technical expertise. Furthermore, they participate in a theoretical training workshop regarding the PC-Wahl software. The workshop lasts approximately 30 minutes, and electoral official can practice if they wish to, in order to ensure their competence.

III. Implementation

In this section we introduce and describe the different steps of the implemented EasyVote tallying process. The EasyVote ballots that need to be tallied are shown in Figure 3. Afterwards, we present the interfaces of the implemented prototype.

[5]http://www.pcwahl.de/.

[6]This check only serves as a self-control for electoral officials, rather than checking the correctness of PC-Wahl.

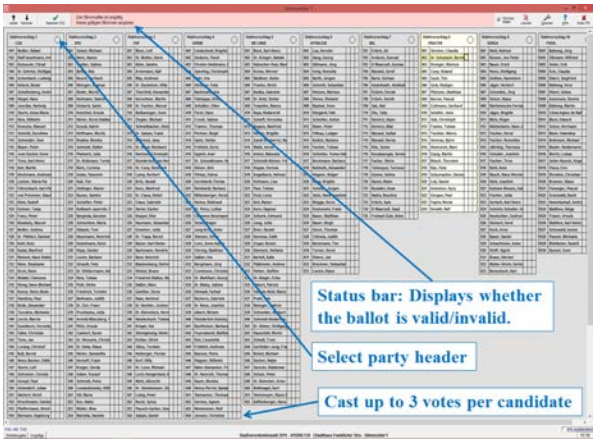


Fig. 2: Ballot entering and recording interface of PC-Wahl.

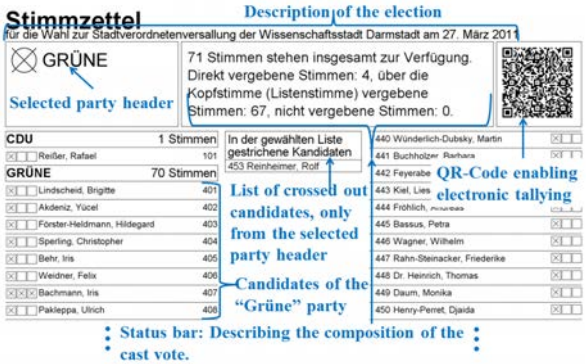


Fig. 3: The EasyVote paper ballot.

A. Tallying Process

The implemented EasyVote tallying process comprises the following steps: (1) Open the ballot boxes, count the total number of cast ballots and compare it with the total number of marked voters in the electoral register. (2) Scan each individual ballot. (3) Electronically compute the final election result, and sign the printed disposition.

Since the EasyVote ballots are electronically prepared and printed in a pre-defined layout, format and font, the ballots could feasibly be scanned by using Optical Character Recognition (OCR) scanners. However, for scanning each individual ballot we decided to use QR-Codes scanners, as originally proposed by Volkamer *et al.* [2], based on the following general advantages of QR-Code scanners:

- QR-Code scanners provide a much higher error correction level and therefore are more accurate.
- QR-Code scanners can be used for all type of ballots (universal encoding), while OCR scanners need to be configured and maintained for each type of ballot.

Hence, the process of scanning and counting an individual ballot, shown in Figure 4, consists of the following steps: (1) Pick up a ballot. (2) Scan the QR-Code. (3) Verify and confirm

that the scanned information matches the human-readable part of the ballot. (4) Repeat process with the next ballot.

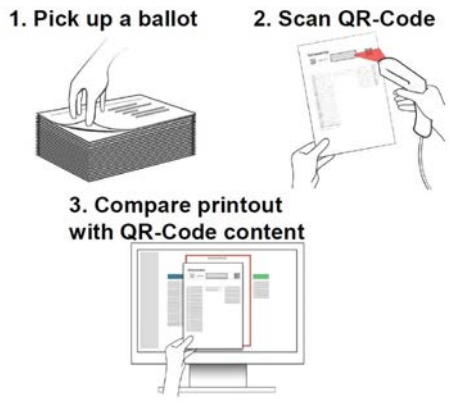


Fig. 4: Scanning and counting ballots with EasyVote.

Note that if we used OCR scanners the human-readable part is also the machine-readable part. This prevents the vote casting component from manipulating the machine-readable part, because voters would be able to detect the manipulation. However, in order to ensure the correctness of the scanning/counting process, electoral officials are still required to fully verify/examine the scanned ballot against the printout (EasyVote ballot). If we assume that electoral officials are required to detect *all* possible discrepancies, it makes no difference whether these are introduced by the vote casting or tallying components.

B. Interfaces of the Prototype

The EasyVote tallying component proposed by Volkamer *et al.* [2] uses two monitors (two different interfaces) for the tallying process. The first monitor, presented in step three on Figure 4, displays and enables the verification of each individual scanned ballot. The second monitor displays intermediate election results after scanning, verifying and confirming each individual ballot. This enables electoral officials and the general public to verify that each individual ballot is correctly added to the election result.

Figure 5 presents the implemented interface for the first monitor, while Figure 6 presents the implemented interface for the second monitor.

IV. User Study - Accuracy Evaluation

In this section we describe the user study, in which we evaluated the prototype with respect to accuracy. The goal of the study was to find out if the implemented EasyVote tallying component is 100% accurate, i.e. that discrepancies where the QR-Code does not match the human-readable part can always (in any case and by any participant) be detected. We intentionally introduced manipulated printouts, in order to check if participants detected the discrepancies.

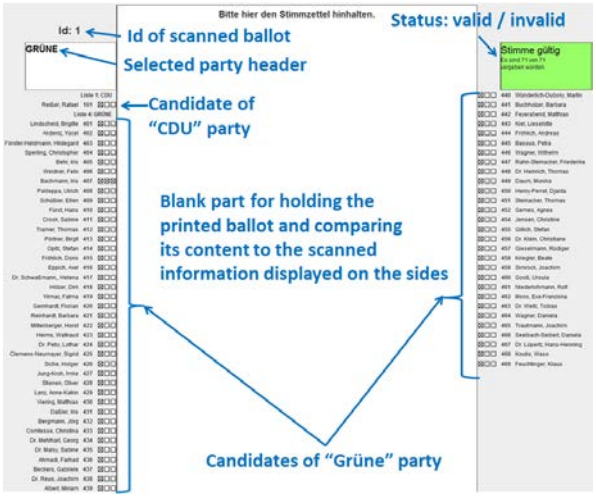


Fig. 5: Scanning and verifying the content of the current ballot.

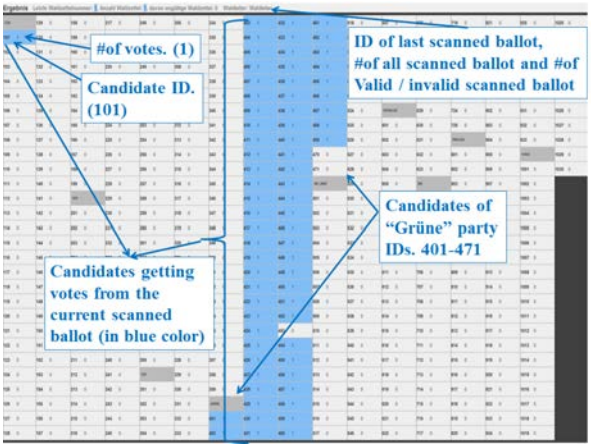


Fig. 6: Overview on the intermediate election result.

A. Preliminary Considerations and Materials

In the user study we only focused on the process of scanning an individual ballot and verifying that the human-readable part matches the machine-readable part. Although by verifying intermediate results we might also be able to detect discrepancies, we assume that if participants cannot detect all discrepancies during the scanning and verifying process, they will also not detect further discrepancies while verifying intermediate results. Thus, for this study we assumed a compromised vote casting component and, an honest and correctly implemented EasyVote tallying component. Note that in practice the tallying component is not assumed trustworthy, as different mechanisms can be used to detect a malicious tallying component, for instance the tallying component provides a cryptographic commitment after each scanned ballot or a hash chain, or by videotaping both monitors at the same time. Afterwards, random checks can be performed to ensure the correctness of the election result.

Furthermore, one of the most well-known challenges in the area of usable security is that you cannot communicate

the primary goal of the study to participants without biasing them [15]. If participants know the primary goal of the study, they may act in a manner perceived as appropriate, and change their behaviour [16]. Therefore we told all participants in the user study that the goal was to evaluate the usability of the EasyVote tallying component. This was necessary so that the participants would not be biased in their behaviour.

The materials required to conduct the user study are listed here. For the materials from the local elections in Hesse we collaborated with the local authorities.

- Training workshop presentations for the PC-Wahl software.
- 189 original electronically filled in ballots from the local elections in Hesse 2011. They were split as follows: 94 from the 1st, 89 from the 2nd and 6 from the 3rd category.[7]
- The implemented EasyVote tallying component.
- Training workshop presentations for the EasyVote system. We created these presentations based on those for the PC-Wahl software.
- 189 EasyVote ballots. These ballots were electronically created, and duplicated the 189 traditional ballots.
- Five EasyVote test ballots to be used during the training phase: Three ballots with candidates and party header marked, and two ballots that also contained crossed out candidates. Two of the five ballots required corresponding corrections by the participants.

B. Study Design

In order to evaluate the accuracy of the implemented EasyVote tallying component we manipulated the QR-Codes of the EasyVote ballots. Hence, when scanning the QR-Code of a manipulated ballot participants should detect a discrepancy between the EasyVote ballot and the data displayed on the screen. As we do not aim to change, but rather to improve the tallying process for local elections in Hesse, participants were required to tally only ballots of the 2nd category, i.e. a total of 89 ballots that contain votes assigned to candidates and/or a selected party header.

C. Manipulations: Introducing Discrepancies

While manipulating the QR-Codes of the EasyVote ballots is technically trivial, we first had to solve the following challenges: 1) Identify all possible manipulations that lead to a difference between the printed human-readable part on the ballot and the data displayed on the monitor; 2) Select an adequate set of manipulations; 3) Introduce an adequate number of manipulations, in order to not directly reveal the study goal; 4) Decide how to randomly add manipulations to ballots; 5) Decide how to introduce the manipulations into the ballot set randomly.

By performing a systematic analysis we identified 36 possible manipulations that we classified in the following five manipulation categories: 1) Changing only vote distribution (7 manipulations); 2) Change candidate names (14 manipulations); 3) Changing party, including its candidates (11 manipulations); 4) Invalidating a valid ballot (2 manipulations); 5) Validating an invalid ballot (1 manipulation).

In order to select a reasonable set of manipulations, we defined the following criteria: 1) Detecting the manipulation requires a full and careful comparison of the EasyVote ballot and monitor; 2) Manipulation should be hard to detect. This led us to the following adequate manipulation set:

- Remove votes from a candidate and assign them to another candidate (1st manipulation category).
- Remove votes from a candidate and do not re-assign them (1st manipulation category).
- Remove a candidate and insert another candidate instead (2nd manipulation category).
- Remove a candidate (2nd manipulation category).
- Remove a party, including its candidates (3rd manipulation category)

This set also covers the manipulations used in previous studies, refer to [17] and [18].

Furthermore, since we were restricted by the number of ballots used in this study we manipulated only 5 out of the 89 ballots. In this way we covered all manipulation categories and introduced a reasonable number of manipulations relative to the number of ballots, such that participants would not guess the primary study goal. We randomly selected 5 ballots and introduced the manipulations according to a random permutation. Finally, we randomly introduced the manipulated ballots into the set of all ballots. Note that each group was confronted with the same manipulations, but in a different random order.

D. Experimental Design and Procedure

11 participants were randomly allocated to four different groups. Three groups consisted of three participants, and one group of two. Each group had to perform the following steps:

- Read and sign the agreement form for participating to the study.
- Participate in the training workshop.
- Tally the 2nd category ballots with the implemented prototype.
- Debrief.

Furthermore, we randomly assigned participants of a group the following tasks: 1) Scanning (one participant had to scan the ballot); 2) Verifying (two participants had to verify that the human-readable part matches the machine-readable part). As the last group consisted only of two participants, one of the participants was randomly assigned to perform both tasks.

Note that the EasyVote tallying process proposed by Volkamer *et al.* [2] requires only two electoral officials. However, we used the same setting as in the traditional local elections in Hesse, thus assigning three instead of two participants (electoral officials) to each group. The last group consisted

[7] Refer to section II for the description of the different categories.

only of two participants, because one of them did not show up.

E. Experimental Setup and Ethical Considerations

All experiments took place in our department. The venue was equipped with tables, chairs and a projector. The projector was used during the presentations in the training workshops. All groups were provided with the necessary hardware equipment, monitor(s), a computer on which the tallying software was installed, and a printer.

An ethics commission at our university provides ethical requirements for research involving humans. These requirements were met. All participants were told that all data would be stored anonymously and used only for the purposes of the experiment.

F. Recruiting and Sampling

The participants were recruited via e-mail, advertising in social networks and flyers. The experiment had 11 randomly selected participants (6 female, 5 male), age 19-57 years: 7 students from different subject areas and 4 employees of our university. All participants were naïve, with respect to the content, since none had worked as an electoral official before. Three different incentives encouraged participation: First, the employees of our university were interested in science and wanted to support our research. Second, 3 were psychology students, who are required by their department to participate in 30 hours of research studies. We compensated them with the appropriate amount of hours. For the rest of the participants we provided €10 per participant.

It is important to note that most of the participants were university students who are very familiar with technology. While they may not be representative of the larger "electoral officials" population, they probably serve a best-case scenario for what tallying performance could be.

G. Results

In this section we report the results regarding the dependent variable "detected" that reflects the accuracy of the implemented EasyVote tallying component. Table I summarises the results of the study. "True" means that the discrepancy was detected and corrected by the participants, while "False" means that the discrepancy was not detected.

TABLE I: Summary of the accuracy evaluation.

Manipulation categories*	Group 1 / Position	Group 2 / Position	Group 3 / Position	Group 4** / Position
1	False / 1	True / 34	True / 6	True / 59
2	True / 83	False / 75	True / 68	True / 8
3	True / 51	False / 36	True / 88	False / 89
4	False / 9	True / 67	True / 25	False / 3
5	True / 87	True / 46	False / 54	True / 36

* Refer to section II for the description of the different categories.
** This group consisted only of two participants.

The results of the accuracy evaluation show that none of the groups detected all introduced discrepancies. Furthermore, the results indicate that detecting a discrepancy does not depend on the position, or on whether others have previously been detected, or on the specific manipulation category.

Note that due to these results, which already show that the implemented EasyVote tallying component does not achieve 100% accuracy, we decided not to continue the user study, i.e. not to include further groups (participants) enabling us to achieve an adequate sample size that would allow to perform various statistical tests.

V. Online Survey - EasyVote Ballot Design

In this section we describe our online survey and present the results. This survey is motivated by the results of the user study reported in the first part of the paper. Hence, the goal was to identify an alternative EasyVote ballot design. On the one hand it ought to reduce the number of required manual comparisons and consequently increase the number of discrepancies detected by poll workers. On the other hand it enables voters easily to verify their cast vote. We also report on recruitment and sampling of participants.

A. Alternative EasyVote Ballots

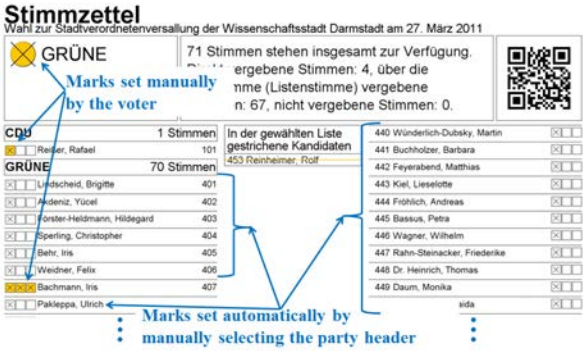
In the survey we presented participants with two possible EasyVote ballot designs (see Figure 7). In contrast to the original EasyVote ballot, both alternatives introduce colour as a new dimension. According to Braun and Silver [19], the colour red conveys the highest level of perceived hazard followed by orange, black, green and blue. Furthermore, Young and Wogalter [20] found that with respect to memory times print highlighted with orange was better remembered than non-highlighted text. Moreover, since red is problematic for a significant percentage of the male population due to colour blindness, orange seemed the best choice.

The first alternative, in contrast to the original EasyVote ballot, highlights the voter's manual selections in orange. The second alternative simplifies things even further, since it eliminates everything except the voter's manual selections and these are still highlighted in orange. Hence, automatically distributed votes, i.e. remaining votes that are assigned to the candidates of a party by selecting the party header, are not printed. The size of the printout remains the same, independent of the voter's selections.

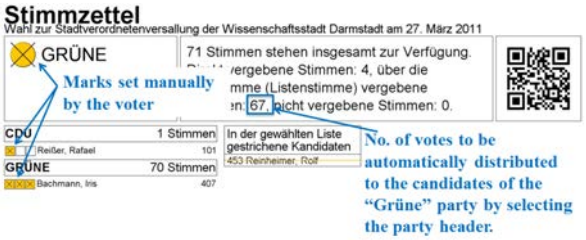
Furthermore, in contrast to the original EasyVote ballot, the machine-readable part (QR-Code) encodes only the voter's manual selections. Thus, the "adapted" EasyVote tallying component implements the algorithm to automatically distribute votes independently of the voter's manual selections, rather than only relying on the data stored in the QR-Code. Both alternatives reduce the number of required manual comparisons for both voters and electoral officials. However, in order to ensure the correctness of the election result, we suggest that electoral officials check the automatic distribution of votes for a random set of ballots, i.e. verify the complete ballot displayed/interpreted by the tallying component, rather than only voter's manual selections.

B. Design and Procedure

The survey consisted of four parts and was structured as follows: (1) Participants were introduced to the local elections



(a) The first alternative.



(b) The second alternative.

Fig. 7: The alternative EasyVote ballot designs

in Hesse. They were asked whether they had previously cast a vote in local Hesse or similar elections, and how often they participated in local elections. (2) Participants were told how many invalid votes were cast in the local elections in Hesse in 2011. This percentage, (5.5%)[8] was much higher than the German federal elections in 2013 (on avarage 2.7%)[9]. Then they were introduced to the EasyVote vote casting process. (3) They were asked some general questions to assess the comprehensibility of the EasyVote vote casting process. (4) Participants were given a textual description of a cast vote, and confronted with the original and the two alternative ballots. All reflected the cast vote described in the text. Participants were asked to rank the ballot types (original and alternatives) with respect to ease of verification and understandability of the cast vote, i.e. verifying that the human-readable part contains the voters selections and understanding the impact (distribution of votes) of the corresponding selections. We also collected some demographic data (nationality, age, gender and education).

C. Recruiting and Sampling

The participants were recruited via e-mail, advertising in social networks, flyers and by personal contact. 87 subjects participated (35 female, 48 male, 4 others) between the ages of 19-75 years. We removed 14 participants (3 female, 9 male, 2 others) aged 22-75, because they did not answer all questions with respect to the vote casting process with the EasyVote voting system. The remaining 73 subjects (32 female, 39 male, 2 others) aged 19-65 comprised one participant with apprenticeship, four with a Ph.D. degree, five with middle school qualification, seven with a B.Sc. degree, seven with a technical college qualification, eight with a vocational education, 15 with a Diploma/M.Sc. degree and 26 with a high school qualification. Most (63) were Germans, four were Austrians, 2 were Turkish, one Swiss and one did not provide information about nationality. No incentives were provided, thus participation was purely voluntary.

[8]http://www.statistik-hessen.de/K2011/EK1.htm, last accessed 10.08.2014 (in German).

[9]http://www.bundeswahlleiter.de/en/bundestagswahlen/BTW_BUND_13/ergebnisse/landesergebnisse/l06/, last accessed 10.08.2014.

D. Results

Table II summarises the results with respect to understandability of cast vote and Table III with respect to ease of verification.

TABLE II: Understandability of cast vote.

	Times of ranking		
EasyVote Ballot	**First place**	**Second place**	**Third place**
Original	5	27	41
First alternative	41	30	2
Second alternative	27	16	30

TABLE III: Ease of verification of cast vote.

	Times of ranking		
EasyVote Ballot	**First place**	**Second place**	**Third place**
Original	6	18	49
First alternative	32	40	1
Second alternative	35	15	24

In order to measure the difference between the original and the alternative designs of the EasyVote ballot we used the Wilcoxon non-parametric test. The test shows a significant difference between the first alternative and the original EasyVote ballot with respect to understandability, Z=-6.722; $p < 0.01$ and ease of verification, Z=-6.722; $p < 0.01$. A significant difference is also found between the second alternative and the original EasyVote ballot with respect to understandability, Z=-2.891; $p < 0.01$ and ease of verification, Z=-4.205; $p < 0.01$. Additionally, the first and second alternatives differ significantly regarding understandability, Z=-3.673; $p < 0.01$ with a higher rank sum for the first alternative (1993.50). No significant difference was found between both alternatives regarding ease of verification.

Furthermore, we evaluated participants' statements, on a five-point Likert scale, concerning the advantages of the EasyVote system compared to the traditional elections in Hesse. Approximately 92% of the participants agreed or fully agreed that the EasyVote system would support voters in such complex elections, such as the local elections in Hesse. 64% of the participants would be happy to use the EasyVote system at the next local elections in Hesse. Around 80% of the participants recognised or fully recognised the advantages of the EasyVote system compared to traditional local elections in Hesse, and think that the EasyVote system is a first step in the right direction to introduce technology in the context of legally-binding elections. Only one participant did not perceive any advantages with respect to using the EasyVote system.

VI. Conclusion and Future Work

The focus of our research is on electronic voting systems for elections with complex voting rules and huge ballots that

meet the German constitutional requirements, including the principle of the public nature of elections. This principle requires that voters should be able to verify all essential steps of the election without technical knowledge. Therefore, in this paper we considered the EasyVote [2] hybrid voting system, which is supposed to meet those requirements. Because of the public nature of elections, we focused on the tallying process in which ballots are scanned individually and each ballot is verified as correct before being tallied.

In the first part of this paper, we reported the results of a user study carried out to evaluate the accuracy of the implemented EasyVote tallying process. The main finding is that the implemented tallying process cannot guarantee a 100% accurate election result since participants did not notice all manipulations. Such human errors could be avoided by automatically scanning all EasyVote ballots, i.e. implementing a different tallying process. Furthermore, trust could be increased either by risk-limiting audit techniques or by using several independent scanners/tallying components. However, this would decrease the extent to which the public nature principle is implemented. This result shows that just because a voting system meets the public nature requirement it does not mean that discrepancies are detected or that underlying fraud is necessarily revealed.

In the second part we reported the results of an online survey, which evaluated two alternative EasyVote ballots designs. Both alternatives were shown to reduce the number of manual comparisons required and can be expected to increase the number of discrepancies detected by the election officials. The results of the online survey show that the first alternative design, where voters' manual selections are additionally highlighted in orange, differs significantly with the original EasyVote ballot with respect to understandability and ease of verification of the cast vote. Furthermore, the first and second alternatives differ significantly regarding understandability. No significant difference was found between the alternatives with respect to ease of verification.

Thus, for future interdisciplinary research we will study the reliability of mechanisms which comply with the principle of the public nature of elections. We plan to repeat the user study with the new EasyVote ballot design (first alternative), and also to propose different techniques to improve detection accuracy. Another open research question is to discover what an acceptable rate of errors is, if indeed we have to accept that some errors will remain undetected.

ACKNOWLEDGMENT

This paper has been developed within the project 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen - which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation). We would like to thank Paul Gerber for helpful comments and suggestions.

REFERENCES

[1] International Organization For Standardization, *ISO 216:2007: Writing paper and certain classes of printed matter – Trimmed sizes – A and B series, and indication of machine direction*. ISO, 2007.

[2] M. Volkamer, J. Budurushi, and D. Demirel, "Vote casting device with VV-SV-PAT for elections with complicated ballot papers," in *International Workshop on Requirements Engineering for Electronic Voting Systems*. Proceedings of the IEEE, 2011, pp. 1–8.

[3] J. Budurushi and M. Volkamer, "Feasibility analysis of various electronic voting systems for complex elections," in *International Conference for E-Democracy and Open Government 2014*, May 2014.

[4] M. Henning, M. Volkamer, and J. Budurushi, "Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen," *Die Öffentliche Verwaltung (DÖV)*, no. 20, October 2012.

[5] J. Budurushi, M. Woide, and M. Volkamer, "Introducing precautionary behavior by temporal diversion of voter attention from casting to verifying their vote," in *Workshop on Usable Security (USEC)*, Feb. 2014.

[6] M. Lindeman and P. B. Stark, "A gentle introduction to risk-limiting audits," *IEEE Security and Privacy*, vol. 10, no. 5, p. 42, 2012.

[7] M. Lindeman, P. S. B, and V. Yates, "Bravo: Ballot-polling risk-limiting audits to verify outcomes," in *Electronic Voting Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*. Bellevue, WA: USENIX, 6-7 August 2012.

[8] R. Rivest and E. Shen, "A Bayesian method for auditing elections," in *Proceedings of the 2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*. Bellevue, WA: USENIX, 6-7 August 2012.

[9] D. J. Madden and S. R. Mitroff, "Aging and top-down attentional control in visual search," 2010, institute for Homeland Security Solutions Research Brief. https://www.ihssnc.org.

[10] J. M. Wolfe, T. S. Horowitz, and N. M. Kenner, "Cognitive psychology: Rare items often missed in visual searches," *Nature*, vol. 435, no. 7041, p. 439440, 2005.

[11] A. N. Rich, M. A. Kunar, M. J. Van Wert, B. Hidalgo-Sotelo, T. S. Horowitz, and J. M. Wolfe, "Why do we miss rare targets? Exploring the boundaries of the low prevalence effect," *Journal of Vision*, vol. 8, no. 15, p. 15, 2008.

[12] J. M. Wolfe, T. S. Horowitz, M. J. Van Wert, N. M. Kenner, S. S. Place, and N. Kibbi, "Low target prevalence is a stubborn source of errors in visual search tasks." *Journal of Experimental Psychology: General*, vol. 136, no. 4, p. 623, 2007.

[13] T. Menneer, K. R. Cave, and N. Donnelly, "The cost of search for multiple targets: Effects of practice and target similarity," *Journal of Experimental Psychology: Applied*, vol. 15, no. 2, pp. 125–139, 2009.

[14] B. Zenger and M. Fahle, "Missed targets are more frequent than false alarms: A model for error rates in visual search." *Journal of Experimental Psychology: Human Perception and Performance*, vol. 23, no. 6, p. 1783, 1997.

[15] C. Kuo, A. Perrig, and J. Walker, "Designing an evaluation method for security user interfaces: lessons from studying secure wireless network configuration," *Interactions*, no. 3, pp. 28–31, 2006.

[16] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "'I did it because I trusted you': Challenges with the study environment biasing participant behaviours," in *SOUPS Usable Security Experiment Reports (USER) Workshop*, Microsoft in Redmond, WA, July 14-16 2010.

[17] S. P. Everett, *The usability of electronic voting machines and how votes can be changed without detection*, Std., 2007, doctoral dissertation, Rice University, Houston, TX.

[18] B. A. Campbell and M. D. Byrne, "Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability," in *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 1–1. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855491.1855492

[19] C. C. Braun and N. C. Silver, "Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance," *Ergonomics*, vol. 38, no. 11, pp. 2207–2220, 1995.

[20] S. L. Young and M. S. Wogalter, "Comprehension and memory of instruction manual warnings: Conspicuous print and pictorial icons," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 32, no. 6, pp. 637–649, 1990.

Pressing the button for European elections

Verifiable e-voting and public attitudes toward internet voting in Greece

Alex Delis[†], Konstantina Gavatha[‡], Aggelos Kiayias[†], Charalampos Koutalakis[‡], Elias Nikolakopoulos[‡], Lampros Paschos[‡], Mema Rousopoulou[†], Georgios Sotirellis[‡], Panos Stathopoulos[‡], Pavlos Vasilopoulos[†]*, Thomas Zacharias[†], Bingsheng Zhang[†]

[†]Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens, Greece
[‡]Department of Political Science and Public Administration, National and Kapodistrian University of Athens, Athens, Greece
*CEVIPOF, SciencesPo, Paris, France
www.demos-voting.org

***Abstract*— We present the initial set of findings from a pilot experiment that used an Internet-based end-to-end verifiable e-voting system and was held during the European Elections 2014 in Athens, Greece. During the experiment, which took place on May 25th 2014, 747 people voted with our system in special voting stations that were placed outside two main polling places in Athens, Greece. The election mimicked the actual election that was taking place which included a great number of parties. After casting their ballot, voters were invited to complete online a post-election questionnaire that probed their attitudes towards e-voting. In total, 648 questionnaires were collected. We present a description of the experiment and a regression analysis of our results. Our results suggest that acceptance of the e-voting system was particularly high especially among the most educated, the technologically adept but also –somewhat surprisingly– older generations.**

Keywords—e-voting; public opinion; Greece

I. INTRODUCTION

One of the most significant challenges in the development of electronic voting is its acceptance by voters. Issues of public trust and support are often at the center of the debate on the adaptation or rejection of electronic voting systems, regardless of their technical characteristics. Even though the issue of electronic voting has attracted increased scholarly attention during the last decade, studies over the acceptance of such as system by the mass public and the factors behind individual-level variance in acceptance remain scarce. In this paper, we aim to advance the relevant literature by presenting individual-level correlates of attitudes toward electronic voting from Greece. Greece is an ideal case for testing attitudes toward e-voting in environments with low familiarity with internet use, as the country ranks quite low in internet penetration. What is more, using Greece as an example adds to the literature by evaluating attitudes toward electronic voting in Europe where such research remains very scarce, with the notable exception of [1]. In particular, this paper investigates the impact of socio-demographic and familiarity with technology on three key components of acceptance of an e-voting system, namely: a) the perceived easiness of the e-voting system b) participants' willingness to see the system being adopted for national elections and c) participants' attitudes to cast their vote remotely using an e-voting system. The trial was conducted in polling stations during the 2014 European Elections. These elections are held every four years across all EU members for the election of the European parliament. The test was not binding for participants: Upon their exit from the polling booth, electors were asked to vote again through an e-voting system should they agreed to do so. Our results suggest that acceptance of the e-voting system was particularly high especially among the most educated, the technologically adept but also –somewhat surprisingly– older generations.

II. E-VOTING EVALUATIONS

Available evidence on the public reception of an electronic voting system mainly come from the United States and Latin America (but see [1] for an application in Europe): Past research has shown that e-voting systems are viewed rather favorably by citizens who participate in the trials [2, 3]. As for individual level-factors, Sherman et al. [3] investigated the impact of a number of characteristics for the case of the US in a convenience sample consisting of 105 volunteers who replied on advertisements. Their results illustrate that acceptance of the electronic voting system depends significantly on the extent to which participants had a basic understanding of the e-voting system. On the other hand, Alvarez et al. [2] studied acceptance of different e-voting devices in the case of Colombia using a non-representative yet extended sample consisting of 2294 respondents coming from three cities. Their results showed that acceptance of the system was particularly high, exceeding 80 percent of positive responses in perceived reliability of the system and 90 percent in perceived easiness. Nonetheless, according to their findingshighly educated and –surprisingly- the eldest age groups were more likely to regard the system as more reliable.

III. PRESENTATION OF E-VOTING SYSTEM DEMOS

Demos is a remote e-voting system that supports end-to-end verifiability (i.e. the voter verifies that her vote was tallied properly) and voter privacy. The system employs code-voting as introduced by Chaum [4] with a number of

modifications both in terms of usability as well as in terms of verifiability. In code-voting based systems, the voters obtain a ballot that contains a list of the candidates, each of them associated with a unique vote-code, and vote by submitting the vote-code that corresponds to the candidate of their choice. Tallying takes place by combining cryptographic elements that relate to the submitted vote-codes. The system utilizes a number of cryptographic elements that include *perfectly binding commitments* and suitably designed *zero-knowledge (ZK) proofs*.

For brevity we do not present here all the cryptographic details of Demos, which are independent of our experiment. The front-end of Demos, which is the most relevant to our experiment and explained in detail below, could have been fitted with any other code-voting system in the back-end and provide the same voting experience.

A. Setup

In the pre-election phase, an *election authority* (EA) generates ballots that have a unique serial number and consist of two equivalent parts (**A** and **B**) containing all information needed to vote. Namely, in each part, every candidate is associated with a randomly generated vote-code, which is cryptographically paired with a *vote-code recording receipt* (Fig. 1). This ballot format is called a *double ballot*. The double ballots are randomly distributed to the voters by EA or another distribution authority. Next, the EA uses the commitment scheme to create a table **T** where all ballot information is committed via the perfectly binding commitments (the candidates are first encoded and then committed). The committed ballots are sorted according to their serial numbers and the parts **A** and **B** (e.g. 100**A** , 100**B**, 101**A**, 101**B**, 102**A**, etc.). In addition, **T** includes information for verifying that the committed values correspond to well-formed ballots. The verification is done by incorporating a novel ZK protocol. Then, EA posts **T** on a *public bulletin board* (BB) and provides a *keyholder* (KH) with the de-commitment information and a *bulletin board authority* (BBA) with the list of pairs of vote-codes andvote-code recording receipts. At the end of the pre-election phase, the working tape of EA is destroyed, for privacy preserving reasons. Note that the KH functionality is distributed to a number of parties via standard secret-sharing to ensure better privacy.

B. Vote-Casting

Vote secrecy in Demos is ensured by the random distribution of the ballots, so that the serial numbers are in no way linked with the voters. When each voter receives a double ballot, she chooses a random side for voting. After the election result is announced, the other part of the ballot will be used for auditing. The double ballot idea for ensuring voting integrity was used in a number of previous systems (e.g., in the Scantegrity system [5]). Then, she sends to BBA the vote-code for the candidate of her choice. This can be done by clicking a button in a user-friendly environment, or manually by typing the vote-code in case the voter does not trust her voting client. The BBA reads the vote-code and if it is valid, it produces the vote-code recording receipt that this vote-code is paired with. It provides the voter with the vote-code recording receipt who can check in her ballot that her vote was correctly recorded by the system. In more detail (refer to Fig. 1 for terminology), the voter can compare the vote-code recording receipt provided by the system to the vote-code receipt appearing next to the party and vote-code of his choice on the ballot's used facet and, thus, if both are identical, be certain that his vote was properly cast through the electronic voting system. An important feature of Demos is that choosing (randomly) one of the two ballot parts for voting, the voter generates (ideally) 1 bit of randomness that is posted on the BB.

We note that after the voter submits the vote-code (using the tablet driven front-end), the system will respond with a vote-code recording receipt as feedback. For example, in Fig. 1, in case the voter votes for party "ΕΛΛΑΣ" the vote-code that will be submitted will be "OIJJ-AGFN-4AUY" while the vote-code recording receipt will be "V605E4". This receipt will appear in the voting interface after the vote-code has been remotely recorded by the system. The voter may check that her vote was received properly by visually verifying that the six digit vote-code recording receipt matches the corresponding receipt for the political party of her choice.

C. Election result computation and verification

After the voting phase has ended, the tally is computed as follows:

1. The KH provides BBA with the de-commitment information and ZK proof information.
2. BBA marks all commitments to the corresponding encoded options (see also Fig. 2 for screenshot of this view).
3. BBA adds (homomorphically) all the marked commitments and opens their sum, which is the election result in encoded form. Finally, it publishes the encoded election result. We note that the result can be efficiently decoded by any party, without the possession of a secret key.
4. Additionally, BBA opens all information for the ballot parts that were used for auditing (Fig. 2), thus revealing the correspondence between vote-codes and parties.

E2E verifiability in Demos is achieved (with high probability)[1] :

1. Because any party can compute the election result and verify the ZK proofs.

[1] We note that the complete security analysis of the system is not the objective of the present paper. However we do present some elements from the analysis in order to give an overview of the system operation. For more information of the demos system please see the web-site http://www.demos-voting.org

2. By the auditing of the ballots: the voter can verify that her ballot was not altered by a malicious party by checking that the perfectly bound opening of the ballot part used for auditing matches the part that the voter obtains. Observe that the malicious EA cannot know in advance which part of the ballot the voter is going to use to vote. Therefore, the EA can guess only with 1/2 probability, which is going to be the part that the voter will choose for auditing. This implies that the probability of altering *t* votes without being detected decreases exponentially in *t*.

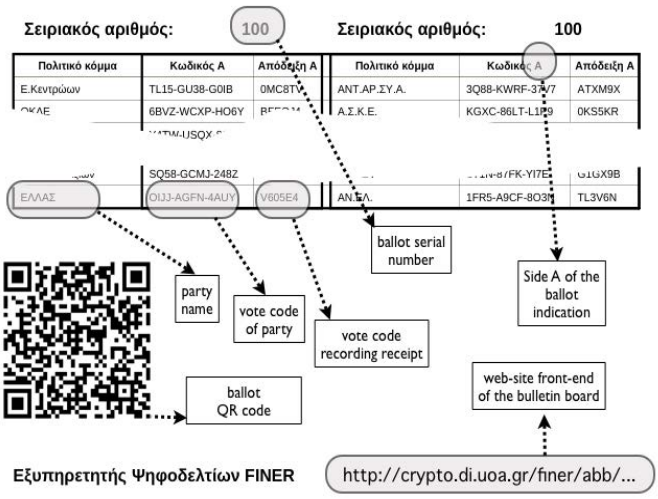


Figure 1. Facet (A) of paper ballot

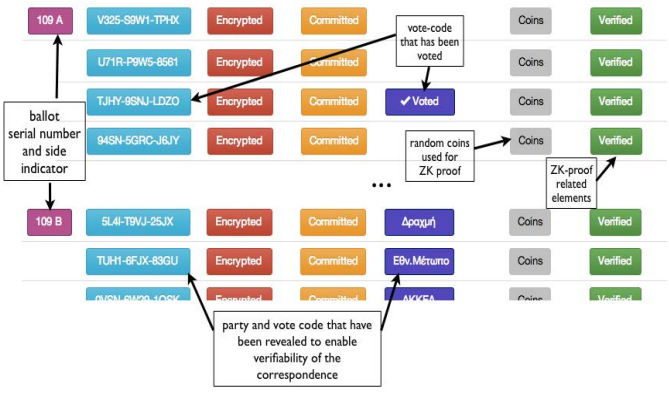


Figure 2. The Bulletin Board at the verification phase

IV. THE PILOT IMPLEMENTATION OF DEMOS

In the pilot implementation of Demos, each participant received a paper ballot where in each facet, besides the lists of candidates, vote-codes and vote-code recording receipts, there was a *QR code* (Fig. 1), which, if scanned, lead to a web rendering of the ballot, with an easy to use interface, where candidate parties appeared in buttons the user can click on. In the trial of the system presented below, voters used tablets with cameras to scan paper ballots and voted electronically through the interface described above. The privacy concerns that have been raised when sensitive ballot information is encoded in non-plaintext form, as QR codes, (see [6] for this topic) do not affect our implementation. This is because Demos supports voting by directly typing the vote-codes so that the voter is able to sidestep QR scanning when she does not trust her client. This alternative that our system provides was explained in the participants both on site and via handouts. Furthermore, since all voters voted on site, issues of vote-selling or coercion that are typically linked with remote voting were not raised or examined[2].

As mentioned above, by using their ballot's unique serial number, voters could trace their ballot and check (a) that their vote was properly marked as "voted" and (b) that in the unused version of the ballot all selection codes correspond to the proper candidate parties that were shown in the paper version of the ballot. This covers one of the two parts of the E2E verifiability check of Demos. Note that the complete check requires also the verification of zero-knowledge proofs that may be done by any external observer (including any voter if they wish to do so). This aspect was not tested in our trial (i.e., no third party zero-knowledge verifiers were commissioned), as involving the participants in the technical details of Demos was out of the scope of our experiment.

THE PILOT EXPERIMENT

The trial was conducted on two different polling stations for the 2014 European Elections in the premises of two public schools in highly populated municipalities in the greater Athens metropolitan area. While the actual election procedure was being held inside the school buildings, a set of desks was placed right outside within the guarded courtyard and next to them there were banners that informed the public regarding the trial that was taking place. In each site, two tablets were placed on the desks supported by an elevated Plexiglas stand that allowed for the insertion of the A4 paper ballot underneath (containing the serial number of the "electronic envelope", the codified candidate parties, the *vote-codes* corresponding to them, their *vote-code recording receipts* and the QR code).

[2] Still voters were informed about the functions of the pilot system and its potential application for remote i-voting and, as presented further in the analysis of the distributed questionnaire findings, they were asked whether they would use it to vote from home for national elections. Our system accepts further enhancements to (partially) deal with the issue of coercion that are out of scope for the present exposition.

Four assistants in each site conducted the trial. Assistant A was responsible for calling one out of every four voters that had already participated in the conventional elections, to participate in the e-voting procedure. In case of refusal, Assistant A called the next one and took note of the refusal. Assistant B accompanied the participants to the desks with the tablets, where the other two Assistants were handing them the ballot and explaining them how they could vote via our setting. Only when asked, (in cases where the participants where unfamiliar with scanning a paper) the Assistants would help the participant to scan the ballot under the tablet. Then, keeping a distance to ensure privacy, Assistants C and D, would, if asked to by the participant, offer clarifications or guidance on the use of the e-voting system. Upon submitting their vote, the participants were prompted to a website where they could (optionally) complete the questionnaire online using the same device. The completion of the questionnaire included questions on respondents' socio-demographic backgrounds as well as a number of attitudinal items, measured in five-point Likert scales regarding electronic voting.

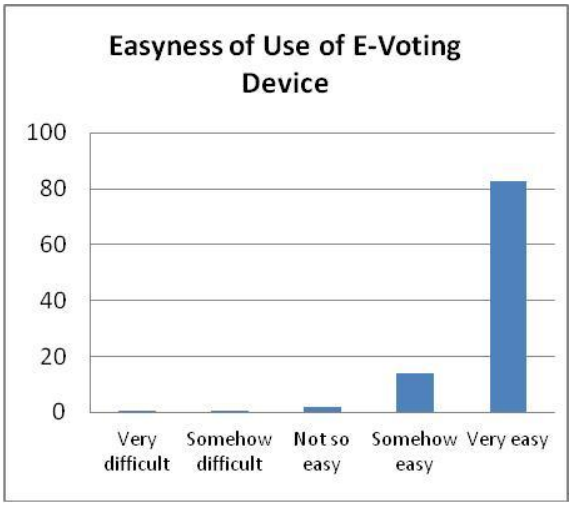
Before leaving, participants were given two leaflets, one containing information about the e-voting system function and features, with emphasis on its procedural safeguards for transparency, verifiability, reliability and security, and another containing a set of simple directions for the successful completion of the verification procedure. A total of 747 people participated in the e-voting trial, while 648 of them filled in the online questionnaire that followed the actual e-voting procedure. Table 1 reports the demographic details of the sample. The sample is skewed in terms of age but mainly in terms of levels of education. Even though this is a typical characteristic of any public opinion survey (e.g. Pew 2012), this means that the aggregate level distribution of attitudes toward e-voting may be higher than what they would appear in the broader Greek population and should be interpreted with caution. The average participation rate was 61.5% in both sites, i.e., about 6 out of 10 voters of the actual voting procedure agreed to participate in the e-voting pilot. The website of the project, (whose address was only publicized in the paper ballots), received 231 unique visits (i.e., a rate of about 30% of the total people that participated) during the next two days. In addition, 21 participants (about 2.8%) chose to make use of the verifiability process and actually locate their ballot assigned to them. It is worth noting that while the verifiability turnout may seem small we consider it satisfactory for our experiment as the verifiability aspect was very briefly explained to each voter (none of which showed any familiarity with this level of secure e-voting design) and the voters were aware of the fact that the pilot election was not binding in any way (and hence one would expect a lower interest in verification than it would have been in case the election was binding). Furthermore, the actual election results were available through other means to all voters (e.g. via regularly conducted exit polls with results broadcasted in the national TV). It is also worth noting that even with as little as 21 verification checks (if done properly) our system would have been capable of providing a reasonable level of election integrity.

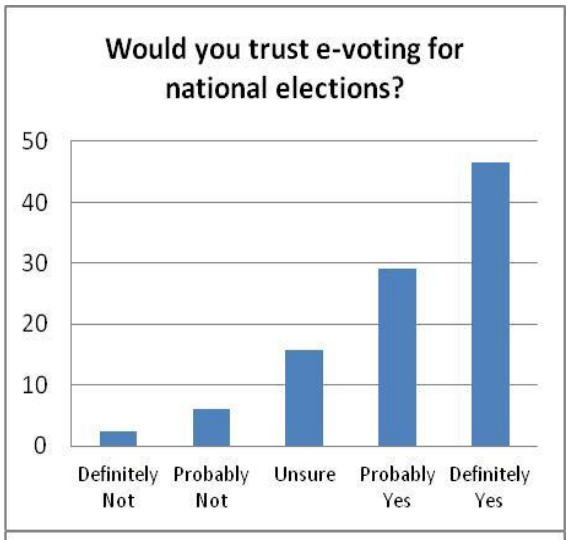
Gender	Percent
Male	50.9
Female	49.1
Age	
15-24	12.8
25-34	16
45-54	24.5
55-64	22.8
65+	7.8
Level of Education	
Up to six years	2
Six to Nine years	3.3
High school graduate	19.3
Some college	13.3
Higher education graduate	41.5
Postgraduate	20.7

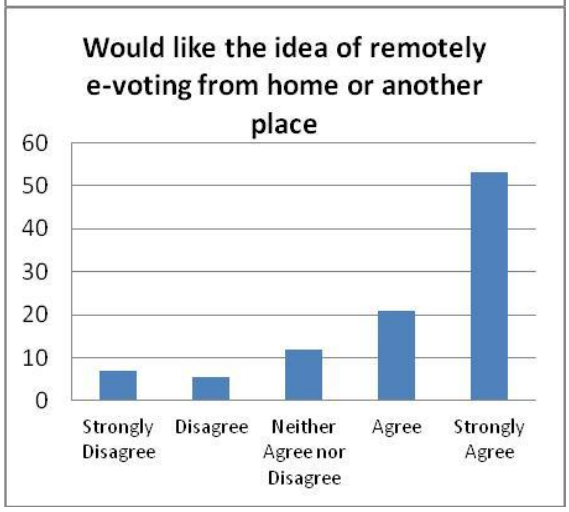
TABLE 1: Demographic Composition of Sample

A. RESULTS

We measured respondents' attitudes toward e-voting through a number of items. Attitudes toward the device were highly positive (Graphs 3-6). Starting with overall satisfaction, nearly 90 percent of respondents answered that they were "somewhat" and "very" satisfied with the electronic voting experience. Moving on to the perceived difficulty of using the e-voting device, 82.7 percent of respondents found its use "very easy", while only 1.2 percent answered that they faced problems using the device. Apart from easiness of use and satisfaction, we measured trust and attitudes toward the adoption of remote electronic voting for national elections. Respondents' attitudes were again very positive: 47 percent of the sample said they would trust an e-voting device such as the one they used for the conduction of European elections, while less than one in ten (8.6 percent) appeared negative toward such an implementation. As for attitudes toward remote electronic voting, roughly three out of four respondents were somehow or very positive toward the prospect of being able to vote in national elections from home with a use of a similar device, while only 12.4 percent appeared dismissive toward this prospect.







Figures 3-6: Distribution of Post-test Respondent Attitudes toward E-Voting

Even though the acceptance of e-voting was quite high in the sample we have reasons to expect that the aggregate distribution masks significant individual-level variation. A number of scholars have argued that the use of electronic voting could possibly create a turnout gap between technologically adept and novices [7-9]. Hence, the argument goes, as the old and less educated are least adept in using technology these population segments will be less likely to vote using an electronic voting device and consequently they may be more skeptical toward the introduction of e-voting devices, and especially remote e-voting devices. Drawing on an e-voting pilot study conducted in the UK in 2003, Norris [7] illustrated that while the option to cast a vote electronically could moderately boost turnout among young voters, it eventually may lead to the suppression of participation among older generations of voters. What is more, since the elder participate in higher rates compared to younger voters, Norris [8] argued that the introduction of electronic voting could lead to an overall decline in electoral turnout.

In order to investigate whether these trends are evident *after* respondents have used electronic voting devices we construct three linear regression models[3], measuring the impact of socio-demographic characteristics (age cohort, gender, level of education) and Internet use (through a dummy variable separating non-Internet users from the rest of the sample) on (a) difficulty using the e-voting device (Model A) (b) trust in e-voting for national elections (Model B) and (c) attitudes toward the prospect of voting from home or another place using a remote electronic voting device (Model C).

[3] In order to ensure that the statistical analysis was not hampered by the discrete nature, nor the non-parametric distribution of the dependent variables all models were re-estimated using complementary log-log regression, an appropriate statistical technique for dealing with highly skewed discrete variables [10]. Results were identical to those reported in the paper in terms of levels of significance and coefficient signs. Same is the case when education is entered as a dummy variable separating those who have attended university from the rest of the sample, with the exception of "easiness of use" where while the education coefficient although positive, falls short of achieving statistical significance.

	Model A		Model B		Model C	
	Easiness of use		Trust		Attitude toward Remote Electronic Voting	
	b	S.E.	b	S.E.	b	S.E.
Male	0,00	0,04	0.01	0.08	-0.07	0.09
Age cohort						
15-24						
25-34	-0,05	0,08	0,50***	0,14	0,53**	0,17
35-44	0,05	0,07	0,73***	0,13	0,60***	0,16
45-54	-0,09	0,07	0,79***	0,13	0,66***	0,16
55-64	-0,08	0,08	1,02***	0,14	0,67***	0,18
65 plus	-0,30**	0,11	1,17***	0,20	0,83**	0,24
Education	0,03**	0,02	-0,01	0,03	-0,01	0,04
No internet access	-0,42***	0,10	-0,07	0,18	-0,09	0,22
Easiness of Use			0,59***	0,07	0,69***	0,09
Adj. R_2	0.12		0.16		0.11	
N	624		620		618	

TableABLE 2: OLS Regression of Easiness of Use, Trust toward E-Voting and Attitudes toward remote e-voting. *(Entries are unstandardized OLS coefficients. Standard errors are reported in the second column.* **: $p < 0.05$; ***: $p < 0.01$)

Beginning with variation in individual-level variation in the difficulty of using the e-voting device, results suggest that educated respondents found it easier to use the device. On the other hand, perceived difficulty was significantly increased for participant categories that are less likely to be familiar with technology, namely respondents aged over 65 years and those who do not use the Internet. Model B reports the respective OLS regression results on trust of e-voting for national elections, using the same independent variables as Model A plus the item measuring perceived difficulty. Results suggest that, all else equal, facility with the e-voting device is associated with general trust toward e-voting, as those who found the use of the electronic voting device easy were more likely to trust the implementation of an electronic voting for general elections. What is striking however is that, all else equal, older aged cohorts appear significantly more trustful toward electronic voting compared to younger age cohorts. This finding that seems paradoxical at first has also appeared in other countries [2] and can be attributed to the fact that younger respondents who are more knowledgeable on issues of technology are more likely to be aware of possible security threats than older and less technologically familiar respondents [2]. Surprisingly, level of education[4] on the other hand is not associated with trust toward electronic voting. The lack of impact of the level of education is against previous findings [2] and needs to be further investigated. Moving on to Model C, which measures variation in attitudes toward remote electronic voting, results suggest that the extent to which one finds remote electronic voting a good idea mainly depends on age and perceived difficulty of using the electronic voting device. Again, as was the case with trust toward e-voting, older respondents appear more positive toward remote electronic voting. What is more, participants who found the use of the e-voting machine easy were significantly more likely to respond that they would like to be able to vote remotely with an e-voting device. Yet it should be noted that the explanatory power of all three models, as indicated by the adjusted R^2 is rather low, meaning that there exist additional latent factors that account for variation in attitudes toward electronic voting in Greece.

CONCLUSION

Electronic voting systems are deemed as a cost-effective alternative for conducting elections, having a promising potential for the quality of democratic representation especially among distinct social groups that may face difficulties accessing polling stations. Yet studies investigating the acceptance of e-voting by the general public remain scarce. This paper advanced the literature on electronic voting by presenting evidence on attitudes toward electronic voting from Greece. Three main conclusions can be drawn from the analysis. First, our results point to the conclusion that acceptance of electronic voting could be fairly high in the general population, bringing additional evidence to confirm previous research by [2] and [3]. This finding however should be interpreted with caution as the sample was skewed in regard with age and level of education, compared to the general Greek population. An additional parameter that may have boosted positive responses is that respondents took part in the trial after having tried the e-voting device. Second, the aggregate distribution of preferences toward e-voting masks significant individual-level variation: Citizens who are already familiar with technology, those who found e-voting easy and older age cohorts were significantly more likely to be supportive of its implementation in national elections. These results appear to substantiate the worry that the advent of electronic voting could possibly create a gap between segments of the population who are familiar with technology and those who are not. On the other hand gender and education were unrelated to e-voting preferences. Third, sociodemographic characteristics and familiarity with technology account only for a small portion of the total variation in acceptance of electronic voting. Future research

[4] It should be noted that the insignificance of education persists with alternative codings as well as when perception of e-voting difficulty and internet use are removed from the model.

could shed more light to the pattern of attitudes toward e-voting from a comparative perspective and further investigate latent parameters that may have an impact on attitudes toward e-voting.

Acknowledgements. The authors gratefully acknowledge the support of the Greek Secretariat of Research & Technology through project FINER, Excellence Programme/ARISTEIA1.

V. REFERENCES

[1] Baldersheim, H., Saglie, J., and Segaard, S. B.. Internet Voting in Norway 2011: Democratic and Organisational Experiences. communication présentée au Congrès mondial de l'Association internationale de science politique, Madrid, 2012.

[2] Alvarez, R. M., Katz, G., Llamosa, R., and Martinez, H. E.. Assessing voters' attitudes towards electronic voting in Latin America: Evidence from Colombia's 2007 e-voting pilot. In E-Voting and Identity Springer Berlin Heidelberg. 2009, p. 75-91.

[3] Sherman, A. T., Carback, R., Chaum, D., Clark, J., Essex, A., Herrnson, P. S. and Vora, P. L. "Scantegrity Mock Election at Takoma Park". In Electronic Voting, 2010, July, p. 45-61.

[4] Chaum, D."Surevote: Technical overview". In Proceedings of the Workshop on Trustworthy Elections, *WOTE*, 2001.

[5] Chaum, D. A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. T. Sherman, and P. Vora. "Scantegrity: End-to-end voter verifiable optical-scan voting". In *IEEE Security and Privacy*, volume May/June, 2008.

[6] Budurushi, J. Stockhardt, S. Woide, M. and Volkamer, M. " Paper Audit Trails and Voters' Privacy Concerns". In Tryfonas, T. and Askoxylakis, I.: LNCS, Human Aspects of Information Security, Privacy and Trust, vol. 8533, p. 400-409, Springer International Publishing Switzerland, June 2014.

[7] Norris, P. "Will new technology boost turnout? Experiments in e-voting and all-postal voting in British local elections". In: Kersting, N., Baldersheim, H., (eds.) *Electronic Voting and Democracy*, New York, 2003, pp. 193–225.

[8] Norris, P. "E-voting as the magic ballot for European Parliamentary elections? Evaluating e-voting in the light of experiments in UK local elections". In Trechsel, A.H. and F. Mendez (eds.) *The European Union and E-voting.* London: Routledge, 2005, pp. 60-90.

[9] Gibson, R. "Internet voting and the European Parliament elections: Problems and prospects". In Trechsel, A.H. and F. Mendez (eds.) *The European Union and E-voting.* London: Routledge, 2005, p. 29-59.

[10] Powers, D. A., Xie, Y. "Statistical methods for categorical data analysis*"*. San Diego, CA: Academic Press, 2000.

Mobile Voting

Electronic Voting with Fully Distributed Trust and Maximized Flexibility Regarding Ballot Design

Oksana Kulyk, Stephan Neumann, Melanie Volkamer, Christian Feier, Thorben Köster
Technische Universität Darmstadt / CASED, Germany
Email: firstname.lastname@cased.de

***Abstract*—One common way to ensure the security in voting schemes is to distribute critical tasks between different entities — so called trustees. While in most election settings election authorities perform the task of trustees, elections in small groups such as board elections can be implemented in a way that all voters are also trustees. This is actually the ideal case for an election as trust is maximally distributed. A number of voting schemes have been proposed for facilitating such elections. Our focus is on a mix net based approach to maximize flexibility regarding ballot design. We proposed and implemented a corresponding voting scheme as an Android smartphone application. We believe smartphones are most likely to be used in the election settings that we consider in the paper. Our implementation also enables voters to remotely participate in the voting process. The implementation enables us to measure timings for the tallying phase for different settings in order to analyze whether the chosen mix net based scheme is suitable for the considered election settings.**

I. Introduction

Recently there has been an increased interest in remote electronic voting, with a focus on large scale elections. However, there are also many smaller scale elections, such as polls in private associations, university environments, committees, and boards with 20 to 30 voters. These boards used to conduct their elections during meetings on paper. Some are planned in advance and others are spontaneous, some use simple yes / no ballots, others more complex options including write in ballots. Elections and polls during meetings are challenging because they happen frequently and people people's mobility has increased. This means that voters are sometimes not present to vote on paper in person. So far technology enables them to participate in public discussions (e.g., over video conference), but they are then either excluded from the voting process or they have to sacrifice the secrecy of their vote in order to participate.

Remote electronic voting would enable them to participate in secret elections, even when they are not physically present. However, well known remote electronic voting schemes such as Civitas/JCJ [1] and Helios [2], [3] are not appropriate as these schemes distribute the duties of registration, voting and tabulation among a number of entities, in advance, requiring a long and time-consuming preparation phase. All this imposes a financial and administrative burden on the election authorities which seems not to be adequate for small scale board elections, in particular spontaneous board elections.

Thus, what is required is a distributed voting scheme, without central servers utilising only the voter's own devices, be it their laptops or smartphones. Note, besides not relying on central servers and not requiring lengthy preparation processes, distributed voting schemes have a further advantage: trust is distributed amongst all voters as all act as trustees.

Correspondingly, our contribution is the proposal of a voting scheme that meets all the above-mentioned requirements of secret elections and polls. The proposed voting scheme is based on existing cryptographic components used in centralized voting schemes such as verifiable mix nets, verifiable secret sharing and threshold decryption.

Furthermore, we implemented the corresponding scheme as an Android smartphone application, allowing voters to participate remotely. Note that we selected smartphone applications as smartphones are most likely to be used in the contemplated election setting and are, as such, the worst-case scenario regarding limitations with respect to computation and network capacity. The implementation enables us to measure timings for the tallying phase for different settings in order to analyze whether the chosen mix net based scheme is acceptable for the considered election settings.

The remainder of this paper is structured as follows: Section II outlines the requirements that were determined to be of relevance for the present election setting. In Section III, we present the design decisions and components selected throughout the voting scheme development process. In Section IV, we describe the composition of these components in terms of a scheme description and evaluate the scheme's security in Section V. In Section VI, we report on the implementation process. Section VII analyzes the scheme's efficiency. Section VIII reviews the related work and Section IX concludes.

II. Requirements

Based on discussions with potential boards (i.e. customers), we identified the following general and security requirements for a suitable voting scheme. Note, these requirements should be considered from a practical perspective since different (often unclear) legal requirements hold in such election settings than for national elections.

A. General requirements

The following general requirements were identified:

Ballot flexibility: It should be possible to conduct elections with ballots of any complexity due to the high spontaneity of corresponding polls:

- Yes/No election
- Multiple candidate selection ("k out of L" election)
- Priority voting (ranking of the candidates)

- Write-in ballots.

Voter flexibility: It should be possible to change the list of eligible voters for each new vote.

Spontaneity: Conducting the election should require as little preparation as possible.

Mobility: The application should run on everyday mobile devices.

Remote participation: It should be possible to cast a vote without being physically co-present with the other voters.

Usability: The system should be usable by non-experts.

Efficiency: The tallying phase should not take more than 15 minutes for 25 participating voters.

Furthermore, it cannot be assumed that it is possible to use PKI.

B. Security requirements

The following security requirements have been identified:

Eligibility: The system should only accept votes from eligible voters.

Uniqueness: Only one vote should be accepted from each voter.

Fairness: The voter should be unable to see the election results, complete or partial, before she casts her own vote.

Vote secrecy: It should be impossible link a voter to his or her individual vote.

Integrity: It should be impossible to replace a cast vote with a vote for another option.

Verifiability: The voter should be able to verify, that the vote she intended to cast is included in the final tally (*individual verifiability*). Furthermore, any third party should be able to verify, that all the cast votes have been tallied correctly (*universal verifiability*).

Robustness: After the votes have been cast, the system should be able to fulfil its functions and tally the votes despite minor errors.

These security requirements should be ensured in the following security model. It is assumed that:

1) More than the half of all the voters are honest and available during the whole voting process i.e. vote casting and tallying. This assumption is justified due to the fact that it would be unreasonable to conduct an election where the majority is corrupt.
2) The devices belonging to honest voters are also reliable and trustworthy, and are not affected maliciously by faults in hardware or software (operating system and voting application). This assumption is justified for the same reason as the previous one. Honest voters without honest devices cannot feasibly run the protocol in an honest way. Note, that in certain settings this assumption might be difficult to ensure. Namely, the smartphones are obviously used privately for other purposes, and might be at risk of infection with malware, especially when the owner is not an expert in mobile security and does not take security precautions. For example, if the OS version on the smartphone is not up-to-date, and the owner often installs apps from untrusted sources, the risks of running the election on such smartphones might be too high, and the application should not be used.
3) Honest users' devices are able to communicate with each other. Similar to the previous assumption this assumption enables honest voters to run the election.
4) No coercion takes place.

To facilitate the second assumption, it is important to embrace diversity in software and hardware. There are several manufacturers of the Android smartphones, thus, there is at least some degree of diversity. The diversity in software can be ensured, if there are different sources and a number of software developers, where the voters can download the voting application from.

Note that we can only guarantee the security requirements for honest voters. However, this holds true for traditional elections as well. For instance, a malicious voter cannot be prevented from forwarding her mail voting material to another person, thus breaking the uniqueness property.

III. Design Decisions

In this section we discuss the cryptographic primitives we used in the proposed voting system.

A. Public Key Infrastructure

As we cannot assume that PKI is in place, part of the voting application is to establish one. We do this by first exchanging the voters' RSA public keys for message authentication, and then exchanging the voters' AES keys for message encryption. One must provide protection against the man-in-the-middle attacks while exchanging the RSA public keys. One way to do this, without relying on certificate authorities and other rather complex preparations, is to use the key exchange based on short authentication strings, as described in [4]. The scheme relies on the existence of an out-of-band channel — namely, the voters should be able to communicate with each other either via physical proximity, or via video or telephone call. This channel is then used to perform manual verification of short strings over such a channel in order to frustrate man-in-the-middle attacks. In order to improve the **usability** of this verification, according to the proposition in [5], the strings have 24-bit length, and are represented as passphrases of three words from the from the PGP Word List [6]. Note, that the communication channels between eligible voters have to be established beforehand in order to execute this scheme; other preparations are not needed, thus increasing **spontaneity**.

After we use the scheme for exchanging the RSA public keys between the voters, thus providing means for message authentication, these keys are then being used to securing communications while establishing symmetric AES keys between each pair of voters via Diffie-Hellman key exchange. For generating the secret parameters in the Diffie-Hellman exchange, the SHA-256 is used as the key derivation function. Thus, means for securing end-to-end encryption are provided.

B. Verifiable secret sharing and threshold decryption

Almost all proposed electronic voting schemes rely on a distributed verifiable secret sharing scheme to generate the election key in a distributed manner and a verifiable threshold

decryption scheme to decrypt individual votes or the sum of all votes in a distributed manner.

A number of secret sharing schemes have been proposed in the literature ([7], [8], [9], [10]), while some of them do not have the means to verify the correctness of the secret sharing, or require the existence of a single trusted instance for key distribution. The scheme that does not have these disadvantages is the one described by Pedersen in [11], [12] and is proven to be IND-CPA secure if used in conjunction with the ElGamal cryptosystem, as shown in [13]. Thus, we decided to use this approach in our application. The corresponding verifiable threshold decryption scheme, which relies on the keys being generated as in [11] is described in [14].

C. Homomorphic tallying versus mix net approach

The approaches most commonly used in electronic voting schemes for preserving the vote secrecy are the homomorphic tallying (e.g. in [15], [14]) and mix net schemes (e.g. in [16], [17]). The first approach relies on homomorphic properties of a crypto system used to encrypt the votes, most commonly, the exponential ElGamal. The homomorphic property is used to multiply the encrypted votes, and then to decrypt the resulting sum. This approach is inefficient for complex kinds of ballots such as priority ranking, and is unsuitable for write-in ballots. Therefore, for ensuring **ballot flexibility** in our application we chose to use the mix net approach.

Two types of mix nets have been proposed: decryption mixnets (e.g. in [18], [16]) and re-encryption mix nets (e.g. in [17], [19]). In order to ensure **robustness** of the scheme, we decided to implement one of the re-encryption mix net schemes. Note, in case of a decryption mix net, one dishonest note can violate robustness.

These schemes also rely on the homomorphic property of an underlying crypto system. A number of entities called the *mix nodes*, the role of which is taken by the voters in our setting, participate in the scheme, whereby each mix node in turn shuffles the list of encrypted ciphertexts $C = (c_1 = Enc_h(v_1, s_1), ..., c_N = Enc_h(v_1, s_1))$ using a secret permutation π and secret randomness values $r = (r_1, ..., r_N)$, outputting the shuffled list $C' = (c'_1, ..., c'_N)$ so that holds:

$$c'_i = Enc_{pk}(1, r_i) \cdot c_{\pi(i)}$$

D. Verifiable mix net schemes

In order to ensure **integrity** and to provide **verifiability**, however, each note has to prove that the input and output set contain the same votes (without revealing π and r). A number of schemes for providing a so called non-interactive zero-knowledge proof of shuffle have been developed ([20], [21], [22], [23], [24]) which mainly differ in their efficiency, degree of vote secrecy, integrity/verifiability as well as robustness. In order to decide which of the proposed proofs is the most appropriate one for our setting, we compare them wrt. efficiency, vote secrecy and integrity/verifiability. For the comparison we apply the following considerations:

- For the efficiency considerations, we consider the number of modular exponentiations E needed for computing the proof of shuffle and for verifying it.
- In order to measure the degree of secrecy of the proposed mix net schemes, we consider the size of *anonymity group* $|A|$. Let $C = \{c_1, ..., c_N\}$ be the list of ciphertexts that results from the final shuffle. Let $A \subseteq C$ be a group of ciphertexts, whereby it is known that the vote of some given voter is in A. Ideally, this group would be the group of all votes cast within the election ($|A| = N$), in which case it is said that a mix net provides *complete* secrecy. Otherwise, if $|A| < N$, the mix net's secrecy is *incomplete*.
- In order to measure the degree of integrity/verifiability of a mix net scheme, we consider the probability p, that the attacker can successfully prove the correctness of an incorrect shuffle. Note, in case p is negligible, the mix net scheme provides *overwhelming* integrity.
- In order to measure the degree of robustness, we consider
  the minimal number of voters t, that should participate and behave correctly during the mixing, in order for it to provide a valid result.

The result of the evaluation according to these considerations is proposed in Table I. As one can see, the schemes that provide the best efficiency, such as the schemes in [20], [21], are seriously lacking in either secrecy or integrity, in particular, for small values of N. As such, the proof of shuffle with the best trade-off between security (secrecy, integrity/verifiability, robustness) and efficiency is the one proposed in [23]; however, since it is covered by patent - to the best of our knowledge, we chose to use the method proposed by Wikström in [24], [25] in our implementation.

TABLE I: Comparison of mix net schemes

PoS	$\|A\|$	E	p	t
[20]	$N/2$	$2N$	50%	$(N/2+1)$
[21]	$complete$	$6\sqrt{N}$	$(\sqrt{N}-1)/N$	1
[22]	$complete$	$12N$	$overwhelming$	1
[23]	$complete$	$2N \log k + 4N$	$overwhelming$	1
[24], [25]	$complete$	$20N + 19$	$overwhelming$	1

k is a divisor of N

E. Proof of Correctness

As shown in [26], ensuring vote secrecy also depends on whether ballot independence is assured: namely, a malicious voter should be unable to cast a vote which is both valid and meaningfully related to a cast vote of another voter. In particular, a group of malicious voters of size f can attempt to break vote secrecy by taking a vote cast by another voter, and casting it as their own vote. Then, after looking at a final result, they could see which vote has been cast at least $f + 1$ times, thus figuring out how the attacked voter has voted. A simple way to prevent this attack is to make the voters prove that they know a corresponding plaintext for a ciphertext message they cast as their vote. For the ElGamal encryption, this can be done by using the non-interactive proof of knowledge of discrete logarithm (described in [27]). Thus, for $c = (a, b) = (g^r, v \cdot h^r)$

with g, h being the ElGamal public keys, the voter has to prove the knowledge of r given a.

IV. Voting Scheme Description

The voting scheme consists of following basic components: verifiable secret sharing, re-encryption mix net, and verifiable distributed decryption. As a crypto system used in encrypting the votes, we chose ElGamal due to its homomorphic properties and its wide use in the selected schemes. Let p, q, g be the corresponding ElGamal parameters, that are publicly available.

1) Ballot initialization: The initiator of the voting composes a ballot that, according to the election type, may consist of the voting question, possible answers, voting rules etc. The empty ballot is then broadcast to all the voters chosen by the initiator, whereby each voter has an option either to agree to participate in the voting, or decline. As a result, the group of voters that is about to participate in this election is formed. In case a set of keys for the election (see Section III-B) has already been generated for this group, the voting proceeds with the *vote casting* stage; otherwise, it proceeds with the *key exchange* stage.

2) Key exchange: This phase consists of generating keys for the election via a verifiable decentralized threshold secret sharing scheme described in [11] with threshold value of $\lfloor N/2 \rfloor + 1$: x_i, the shares of private key that each voter holds, and the jointly computed public key h. The participants also exchange commitments h_i to x_i, which are calculated as $h_i = g^{x_i}$, that are later used for verifiable decryption. The key exchange phase only needs to be performed once for each group of voters; in any further elections conducted by the same group, the previously generated keys can be securely reused.

3) Vote casting: The voters are given a certain time limit, during which they are supposed to cast their vote. The vote v_i is encoded so that it could be used as a plaintext in ElGamal encryption, and e_i is calculated as $Enc_h(v_i, r_i)$ for a random $r_i \in_R \mathbb{Z}_q$. Furthermore, the proof of correctness is used to demonstrate the knowledge of v_i to prevent ballot-copying attacks, as shown in III-E. After (c_i, p_i) have been broadcast by all voters, each voter possesses the initial list of all votes $C_0 = (c_1, ..., c_N)$.

4) Tallying: At the beginning of the tallying phase, the votes are anonymized (Figure 1): this process is divided into N rounds, with fixed execution times. In each round, the voter i applies a mix net scheme to the list C_{i-1} using a random vector $r = (r_1, ..., r_N)$ and a permutation π in order to get a shuffled list $C_i = Enc_h(1, r) \cdot (C_{i-1})_\pi$. She also computes a non-interactive proof of shuffle P_i as described in Section III-D, in order to demonstrate that the shuffle has been executed correctly. After that she communicates the values (C_i, p'_i) to other voters. Then, each one of the remaining voters verifies p'_i, and if it is verified, accepts C_i; if p'_i is not verified, or if the voter i does not send any shuffle result within a round time, sets $C_i := C_{i-1}$. At the end, after all the voters have performed the shuffling, the list C_N is accepted as the final list of anonymized votes. The verifiable decryption scheme is then being executed as described in [14] (Figure 2): for each encrypted vote $c_i \in C_N, c_i = (a_i, b_i)$ each voter j computes the partial decryption share $d_{i,j} = a_i^{x_j}$ using her private key share x_j. (S)he then also computes the non-interactive zero-knowledge proof $p''_{i,j}$ to prove that the secret value x_i used for partial decryption is the same value, that was committed to during key exchange phase. The voters then broadcast their computed values (d_j, p''_j) with $d_j = (d_{1,j}, ..., d_{N,j})$, $p''_j = (p_{1,j}, ..., p_{N,j})$. As soon as any voter gets a threshold amount of partial decryptions and proofs of its correctness $(d_{i,j}, p''_{i,j})$, whereby $p''_{i,j}$ is verified successfully, she can reconstruct the decryption of c_i from the collected values of partial decryption shares. In this way, all the votes in C_N are being decrypted, resulting in values of $V = (v_1, ..., v_N)$. The final result is then tallied according to election rules: as such, for example, if each vote represents a candidate from the given list $v_i \in \{C_1, ..., C_L\}$, the result is the sum of the votes cast for each candidate, $S = (s_1, ..., s_L),\ s_i = |v_j : j = 1, ..., N, v_j = C_i|$.

V. Security Analysis

This section is dedicated to an informal security argument on the presented scheme. To evaluate its security, we identify threats against the security requirements (see Section II-B) and show that the scheme defends against these threats under given assumptions. Note, that the scheme can only provide defence against these threats for the voters with uncorrupted devices, as otherwise the application would just behave according to the attacker's commands, instead of following the scheme.

Eligibility A non-eligible voter can cast the vote in the system, in case there is no authentication in place, or the voter can fake her identity and impersonate an eligible voter. This is not the case if the list of all voters is known in advance, which is ensured in the ballot initiation stage, and if reliable PKI exists, providing means for message authentication and thus preventing identity impersonation. Therefore, it should be impossible for the attacker to impersonate an eligible voter and cast a vote instead of her.

Uniqueness In case no votes from non-eligible voters are accepted, which is ensured via eligibility, a voter can break uniqueness and cast more than one vote, if she can fake her identity and pretend to be another eligible voter. This is impossible due to existing PKI. Thus, it can be ensured that during the vote casting stage, only the voter's first vote (alternatively, only the last one) is accepted.

Fairness In the scheme the fairness property can be broken if a voter is able to reveal others' votes during vote casting. To do this, s/he must be able to decrypt the votes that are broadcast. This is only possible, if at least $\lfloor N/2 \rfloor + 1$ voters collaborate and use their secret keys for decryption. This is impossible according to the assumptions 1-2 in Section II-B; therefore, there is no way for any voter to know the intermediate result at vote casting.

Vote Secrecy The possible ways to break secrecy in the scheme is to either decrypt the cast votes before they are anonymized, or to prevent them from being anonymized. The first way is possible if at least $\lfloor N/2 \rfloor + 1$ voters cooperate maliciously and use their secret key shares for

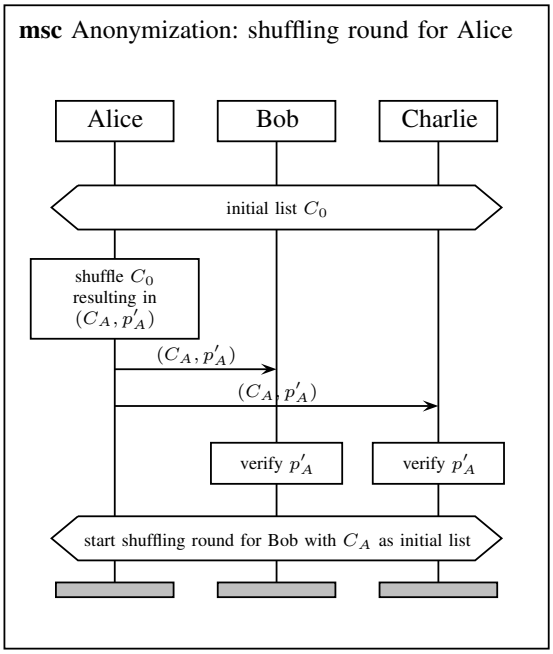


Fig. 1: Anonymization round for $N = 3$

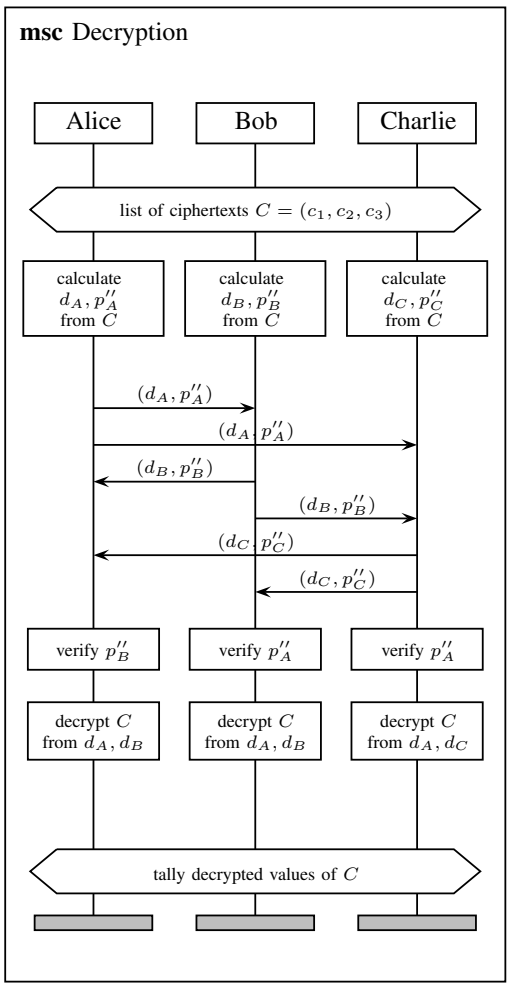


Fig. 2: Decryption for $N = 3$

decryption. The second way is possible if all but one[1] voter decline to perform the anonymization or to keep the correspondences between input and shuffled ciphertexts a secret. Thus, according to assumptions 1-2 in Section II-B, vote secrecy is ensured.

Integrity A way to break integrity and replace some cast vote with another vote, would be either to replace the ciphertext during anonymization stage, or to provide a manipulated partial decryption during tallying stage. This attempts will be detected, however, due to the employment of zero-knowledge proofs during decryption and anonymization, which each voter has to verify before accepting. Therefore, everyone should have the possibility to verify the correctness of the tallying. Thus, any manipulation with the election result will be noticed.

Verifiability Similarly to ensuring integrity, universal verifiability of the correctness of election result is ensured due to non-interactive zero-knowledge proofs that could be verified by anyone using publicly available information. Given universal verifiability, the only way to break individual verifiability would be for the application to cast a vote that is different from the voter's intention. However, due to the assumption 2 in Section II-B, individual verifiability is ensured.

Robustness The result of the voting cannot be decrypted and thus tallied, if only less then $\lfloor N/2 \rfloor + 1$ voters are available and can communicate with each other during decryption. Additionally, the result cannot be tallied without necessarily breaking vote secrecy, if the anonymization of the votes has not been performed correctly, which is possible, as described above, if all but one voter are unable to shuffle the ciphertexts and keep the correspondences between the input list and the shuffled list secret. Therefore, according to assumptions 1-3 in Section II-B, robustness of the system is ensured.

[1] If only one voter is honest, then the public will not know the correspondences between the voter's identity and the vote; however, if all the other voters are dishonest, and each dishonest voter i reveals the correspondences between the ciphertexts in lists C_{i-1} and C_i to the public, the honest voter will be the one who knows how each one has voted. Thus, vote secrecy during anonymization could be ensured only if at least two voters perform their shuffling correctly and do not reveal the correspondences between the ciphertexts.

VI. Implementation

In this section we describe the implementation details of the voting scheme, as well explain particular design decisions

we made.

A. Design Decisions

1) Android app: We developed an application to implement the described voting scheme for Android smartphones. Android is based on a Linux Kernel and is the most widely used mobile operating system. It runs on many different machines which differ in many respects like, for example, screen resolution, CPU power and available memory. The application is designed to support all machines which run Android 4.0 or higher and have more than 512 RAM available.

2) Communication: To establish the communication channels between the voters' smartphones, we had to choose between several options, such as BlueTooth, WiFi-Direct, SMS or instant messaging protocols such as MSN or ISQ. We chose to use XMPP, which is an open-source instant messaging protocol. In advantage to other options, it allows for communications over the network without being in physical proximity to each other, does not place substantial restrictions on message length, and can be extended thus making it easier to adjust for our implementation. To establish a connection to other participating smartphones the Smack API[2] which builds upon XMPP is used. In order for the voters to communicate with each other, the XMPP server has to be available, either as a public server, or as a private server, established by the company. The voters then use their account data on this server to log in the application. As the XMPP protocol communicates via network, **remote participation** is ensured, by enabling every eligible voter to participate in the voting, as long as she has access to network connection, for example, to the mobile internet on her smartphone.

For establishing the PKI we prepared a central server that is used as a "bulletin board" where the initial list of voters is stored. The bulletin board is needed for establishing the PKI only, and is not required on any other stage of voting. This initial list of voters is required in order to enable the initial communication between voter's devices, as voter could send the messages to others only knowing their XMPP account IDs.

This server is relied on with regards to availability only, and does not hold any sensitive information. We use the scheme described in III-A in order to exchange the RSA keys and the AES keys between the voters.

3) Libraries: For implementing the mix net, we did not use the Verificatum implementation by Wikström[3] due to licence restrictions. Instead, the application uses the open-source `unicrypt`[4] library for the mix net implementation. We used the `guava-library`[5] as a utility library e.g. for Base64 encoding. Android ships with a cut-down bouncycastle implementation for cryptographic primitives which only allows symmetric encryptions up to 128 Bit. To support better encryption schemes like 256 Bit symmetric encryption an external library called `spongycastle`[6] is used. Spongycastle is a derivation of Bouncycastle[7], the most popular and extensive Java library for cryptography, which is optimized for Android and renames the packages to avoid classloader conflicts.

B. Walkthrough

We have attempted to make the user interface as simple as possible, requiring only the minimum amount of interaction from the users. We also iteratively improved them due to feedback from colleagues and friends. Note, we plan as future work to evaluate the usability within a user studies.

When starting the application, the voter arrives at the welcome page and logs herself in using her XMPP account. After logging in, the user is referred to the Main Menu (see Figure 3). There, the PKI establishment process can be launched, which concludes when all the voters comparing and verify the passphrases displayed on their screens (see Figure 4). Note, that the PKI establishment scheme is only performed once for each set of voters. It is only repeated when new persons (i.e. new employers, or new boardroom members) are added to the list of eligible voters.

After the PKI has been established, the elections can be conducted. The person who wants to start the election composes and broadcasts the ballot as seen in Figure 5. As all other participants see the invitation and agree to participate, the election starts: if this group of voters starts an election for the first time, the key exchange is being run first. Otherwise, the voters can start with the vote casting, whereby each voter selects her vote and confirms the vote as seen in Figure 6.

After all votes are received the mix net starts anonymizing the votes. As this is the most computationally intensive part of the process, it may take some time. Afterwards the votes are decrypted and tallied and the result shown as seen in Figure 7.

A flow diagram which explains the PKI establishment process (Figure 8), ballot initiation (Figure 9), and voting process (Figure 10) are given, while the captions in bold on the diagrams refer to the steps where the interaction of the voter with the user interface is needed.

C. Fault Handling

We have identified the steps of the voting process, whereby some faults might be present. Most commonly some voters not being present or being unable to communicate with the others might occur. We have already shown, in Section IV, how some of these faults are handled. Furthermore, as shown in Section V, some of these faults, such as the voters failing to produce valid partial decryptions of a vote, could be ignored under the assumptions that we make.

Other faults are the ones that occur during voting phases, that preclude the tallying stage: namely, faults could occur during PKI establishment (i.e. the adversary trying to execute a man-in-the-middle attack), ballot initialization stage (such as voters not responding to the invitation to vote), or vote casting. The diagrams in figures 8,9,10 show the way the application is supposed to handle these faults. As such, for example, the voter who wishes to initiate the election has the option to decide, whether she still wants to start the election if not all of the invited voters respond to her invitation, or to wait some more for the missing voters to respond, or to cancel the election.

[2]http://www.igniterealtime.org/projects/smack/
[3]http://www.verificatum.org/
[4]https://github.com/bfh-evg/unicrypt/
[5]https://code.google.com/p/guava-libraries/
[6]http://rtyley.github.io/spongycastle/
[7]https://www.bouncycastle.org/

Fig. 3: Main Menu

Fig. 4: Establishment of the PKI

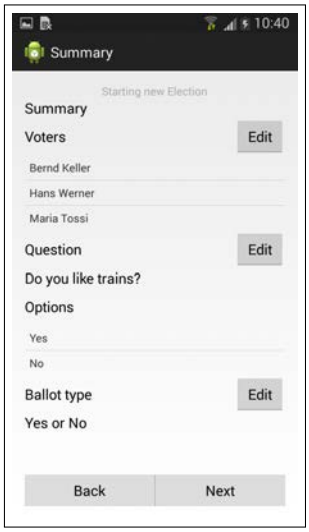


Fig. 5: Summary of the ballot for the new election

Fig. 6: Overview of a cast vote

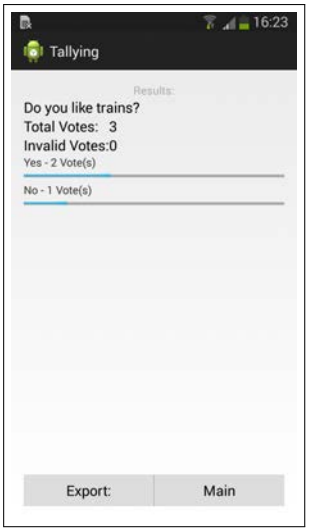


Fig. 7: Election result

Another source of faults during the voting, is the inconsistency of message broadcast. In order to broadcast a message using XMPP, the message has to be sent separately to each receiver. Thus, it makes the system vulnerable to Byzantine faults, whereby a malicious voter can send different messages to different receivers (for example, during broadcasting a cast vote), thus endangering robustness of the voting. One way to solve this problem is to make the voters manually compare the result of each stage (for example, by comparing hash values of a complete list of cast votes at the end of vote casting). Another solution is to implement additional communication schemes that ensure Byzantine Fault Tolerance, such as the schemes described in [28], [29][8].

[8]Note, that some of the methods to implement BFT provide more efficiency at the cost of requiring additional assumptions regarding the amount of faulty nodes f out of total N, most commonly, $f < \lfloor N/3 \rfloor$.

VII. Efficiency evaluation

Without counting the costs of the communication (i.e. signing and verifying the communicated messages, as well as encrypting/decrypting them when needed), the cost of the execution of the scheme in number of required modular exponentiations, with the anonymization stage being the most computationally extensive part, is as follows:

$$26N^2 + 22N + \lfloor N/2 \rfloor + 1 + N(\lfloor N/2 \rfloor + 1) - 1$$

Thus, the efficiency of the voting scheme is $\mathcal{O}(N^2)$. Note that it only depends on the number of the voters, and not on ballot complexity, such as number of candidates or possible options.

As additional computational and communication costs arise in the implementation, which depend on programming tech-

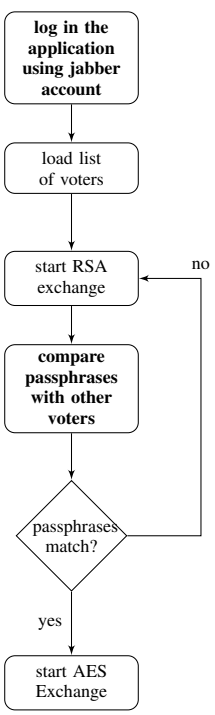


Fig. 8: Establishment of the PKI

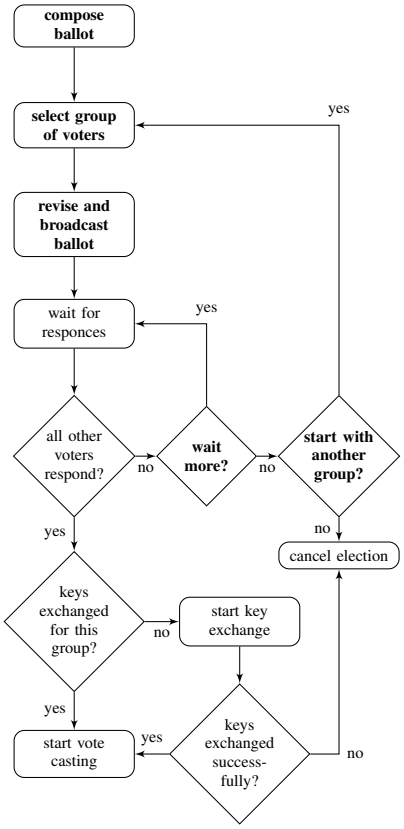


Fig. 9: Ballot Initiation

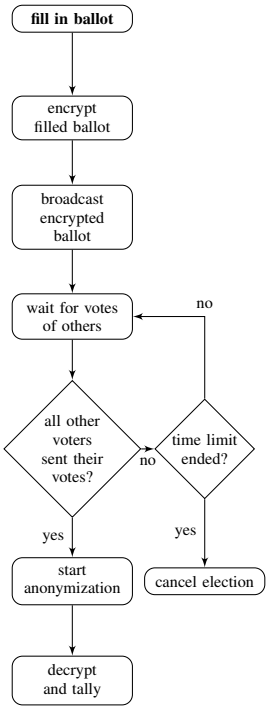


Fig. 10: Vote Casting

niques and network capabilities, we evaluated the performance of the application, by measuring the time it takes to calculate and display the result of voting after the votes have been cast. The application was run on several S3 Samsung smartphones, all in the same room. The "voters" were represented by Gmail accounts with GTalk as the XMPP server for communication, created for test purposes. We did not count the time taken for the PKI establishment stage, since it is only conducted once initially, nor the key exchange stage, since it only has to be executed once for a group of voters. We also did not record the time elapsed during ballot initialization and vote casting, since the time spent on this stage depends mostly on how long the voters take to make their decisions and cast their votes. The key length is as follows: the RSA keys used for message authentication have 2048-bit length, as well as the ElGamal parameters g, p. The ElGamal secret keys, as well as random values used in exponentiations, have 256-bit length.

The resulting times from running the election between $2-5$ voters are given in table II. The times seem linear because of how the cryptographic schemes with several rounds have been implemented in order to achieve synchronization: each round is given a fixed amount of time, during which it is expected for all computations to be complete. Thus, this time is chosen as an upper limit for the computations - namely, for the mix net scheme, the duration of one shuffling round is set such as one should be able to complete the shuffling of 25 ciphertexts, which includes calculating and verifying the corresponding proofs of shuffle. Thus, the time spent on anonymizing the votes is $\mathcal{O}(N)$ for $N \leq 25$. The time for decrypting the votes is $\mathcal{O}(N^2)$, but it is relatively small compared to the anonymizing stage. Thus, extrapolating the times for 25 voters[9], we can assume that the election will last slightly less then 12 minutes on such devices.

TABLE II: Execution times of tallying stage

Number of voters	Average execution time (ms)	Average execution time (min)
2	65764.5	1.10
3	85152.7	1.42
4	109375	1.82
5	129702.6	2.16

VIII. Related Work

A number of schemes for decentralized voting with distributed trust has been proposed in the literature. Among them are the works in [15], [30] and [14], which were implemented in the *MobiVote* application. The security model of these schemes is similar to the one that we describe in this paper, namely, the security of the scheme depends on the majority of the voters and their voter devices being uncorrupted. However, the schemes in question employ homomorphic tallying, thus being less suitable for complex ballots. An Android application for spontaneous decentralized voting in classroom setting has been proposed in [31]; the approach, however, does not ensure verifiability. A scheme for decentralized voting

[9]We used the polynomial trend line function in Excel.

has been described in [16], and then expanded in [32]. The scheme uses mix net scheme for anonymizing the votes; however, it relies on all the voters being uncorrupted during the anonymization stage for ensuring robustness and integrity, which is a disadvantage compared to our approach.

IX. Conclusion and Future Work

We have presented a scheme for decentralized voting with distributed trust, and an application that implements this scheme, thus enabling secure elections in small groups. We have shown that this application fulfills the security requirements of eligibility, uniqueness, fairness, vote secrecy, integrity, verifiability, robustness, as well as the general requirements of ballot flexibility, voter flexibility, spontaneity, mobility, remote participation that we have set as our goal. As a future task, we will work on the usability of the application, conducting user studies and improving the user interfaces. As part of improving usability, we will work on further improving efficiency of the application. This includes (1) using the fact, that the mix net scheme developed in [24] is specifically designed with an "offline" and "online" phase, whereby the offline phase is the computationally extensive one, and can be executed before the election actually starts. Currently, these two phases are executed one directly after another during vote anonymization. The offline phase, however, could be completed in advance, during the idle time of the protocol, when no other extensive computations are being executed, thus making the tallying phase substantially faster. Furthermore, (2) efficiency of the vote anonymization will be further improved by only requiring a subset of all voters to participate as mix nodes. We have shown that at least two honest voters are needed to ensure vote secrecy during vote anonymization. Thus the set of shufflers must contain at least two honest voters. According to our assumptions, at most $\lceil N/2 \rceil - 1$ voters are dishonest. Adding two honest honest voter upon $\lceil N/2 \rceil - 1$ results in the fact that the minimal number of voters that need to act as mix nodes is $\lceil N/2 \rceil + 1$. In order to determine the shufflers for each election, a common reference string to generate randomness can be used. One could instantiate the common reference string by a cryptographic hash value of all the votes cast in the election, then using it as an input in a deterministic function that outputs a sequence of shufflers. Another way would be to sort the list of all voters in the election according to canonical order, and choose the first $\lceil N/2 \rceil + 1$ from the sorted list. Another way to improve efficiency will be to use elliptical curves instead of integer groups, in which case additional considerations on how to encode votes are necessary.

Another direction of future work is to discuss the issue of people using same or similar smartphones as well as people all installing the software from the same vendor or download it from the same platform.

Finally, we will also have a closer look to the robustness of the application. In particular, we will implement the Byzantine Fault Tolerance scheme in order to make communication more reliable. An efficient way to do this, that requires more than two thirds of honest nodes, is described in [28]. Another, way to implement the Byzantine Agreement is described in [29]. Although this way is less efficient, it does not require changes in security model, and can be applied if more than half of all the voters are honest, provided that the means of message authentication are in place.

Acknowledgment

This paper has been developed within the project 'BoRoVo' Board Room Voting - which is funded by the German Federal Ministry of Education and Research (BMBF) under grant no. 01IS12054 and within the project ComVote, which is funded by the Center for Advanced Security Research Darmstadt (CASED), Germany. The authors assume responsibility for the content. We also thank the reviewers for their valuable comments that helped to considerably improve the quality of this work.

References

[1] Clarkson, M.R., Chong, S., Myers, A.C.: Civitas: Toward a secure voting system. In: IEEE Symposium on Security and Privacy, IEEE Computer Society 354–368

[2] Adida, B.: Helios: Web-based open-audit voting. In van Oorschot, P.C., ed.: USENIX Security Symposium, USENIX Association 335–348

[3] Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability analysis of helios-an open source verifiable remote electronic voting system. In: Proceedings of the 2011 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. USENIX. (2011)

[4] Nguyen, L.H., Roscoe, A.: Efficient group authentication protocol based on human interaction. In: Proceedings of Workshop on Foundation of Computer Security and Automated Reasoning Protocol Security Analysis. (2006) 9–31

[5] Farb, M., Burman, M., Chandok, G., McCune, J., Perrig, A.: Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, Technical Report CMU-CyLab-11-021, Carnegie Mellon University (2011)

[6] Zimmermann, P.R.: Pgpfone: Pretty good privacy phone owner's manual. MIT, http://web. mit. edu/network/pgpfone/manual (1995)

[7] Shamir, A.: How to share a secret. Communications of the ACM **22**(11) (1979) 612–613

[8] Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: Foundations of Computer Science, 1987., 28th Annual Symposium on, IEEE (1987) 427–438

[9] Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Foundations of Computer Science, 1985., 26th Annual Symposium on, IEEE (1985) 383–395

[10] Benaloh, J.C.: Secret sharing homomorphisms: Keeping shares of a secret secret. In: Advances in CryptologyCRYPTO86, Springer (1987) 251–260

[11] Pedersen, T.P.: A threshold cryptosystem without a trusted party. In: Advances in CryptologyEUROCRYPT91, Springer (1991) 522–526

[12] Pedersen, T.P.: Distributed provers and verifiable secret sharing based on the discrete logarithm problem. DAIMI Report Series **21**(388) (1992)

[13] Cortier, V., Galindo, D., Glondu, S., Izabachene, M.: A generic construction for voting correctness at minimum cost-application to helios. IACR Cryptology ePrint Archive **2013** (2013) 177

[14] Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. European transactions on Telecommunications **8**(5) (1997) 481–490

[15] Khader, D., Smyth, B., Ryan, P.Y., Hao, F.: A fair and robust voting system by broadcast. In: EVOTE'12: 5th International Conference on Electronic Voting. (2012)

[16] DeMillo, R.A., Lynch, N.A., Merritt, M.J.: Cryptographic protocols. In: Proceedings of the fourteenth annual ACM symposium on Theory of computing, ACM (1982) 383–400

[17] Benaloh, J.: Simple verifiable elections. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, USENIX Association (2006) 5–5

[18] Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM **24**(2) (1981) 84–90

[19] Jakobsson, M., Juels, A., Rivest, R.L.: Making mix nets robust for electronic voting by randomized partial checking. In: USENIX security symposium, San Francisco, USA (2002) 339–353

[20] Jakobsson, M., Juels, A., Rivest, R.: Mix nets robust for electronic voting by randomized partial checking. USENIX security symposium (2002)

[21] Demirel, D., Jonker, H., , Volkamer, M.: Random block verification: Improving the norwegian electoral mix-net. In Manuel J. Kripp, M.V., Grimm, R., eds.: 5th International Conference on Electronic Voting 2012 (EVOTE2012). Volume 205 of LNI - Series of the Gesellschaft für Informatik (GI)., Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, Gesellschaft für Informatik (July 2012) 65–78

[22] Groth, J.: A verifiable secret shuffle of homomorphic encryptions. Journal of Cryptology **23**(4) (May 2010) 546579

[23] Bayer, S., Groth, J.: Efficient zero-knowledge argument for correctness of a shuffle. In: Advances in Cryptology EUROCRYPT. (2012)

[24] Terelius, B., Wikström, D.: Proofs of restricted shuffles. In: Progress in Cryptology–AFRICACRYPT 2010. Springer (2010) 100–113

[25] Wikström, D.: A commitment-consistent proof of a shuffle. In: Information Security and Privacy, Springer (2009) 407–421

[26] Smyth, B., Bernhard, D.: Ballot secrecy and ballot independence coincide. In: Computer Security–ESORICS 2013. Springer (2013) 463–480

[27] Schnorr, C.P.: Efficient signature generation by smart cards. Journal of cryptology **4**(3) (1991) 161–174

[28] Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI. Volume 99. (1999) 173–186

[29] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) **4**(3) (1982) 382–401

[30] Hao, F., Ryan, P.Y., Zieliński, P.: Anonymous voting by two-round public discussion. IET Information Security **4**(2) (2010) 62–67

[31] Esponda, M.: Electronic voting on-the-fly with mobile devices. ACM SIGCSE Bulletin **40**(3) (2008) 93–97

[32] Alkassar, A., Krimmer, R., Volkamer, M.: Online-wahlen für gremien. DuD Datenschutz und Datensicherheit **8**(29) (2005)

Scroll, Match & Vote: A Coercion-Resistant Mobile Voting Interface

Carlos Ribeiro
Inesc-id and
Instituto Superior Técnico
Universidade de Lisboa
Email: carlos.ribeiro@tecnico.ulisboa.pt

Rui Joaquim
SnT
University of Luxembourg
Email: rui.joaquim@uni.lu

Gonçalo Pereira
Inesc-id and
Instituto Superior Técnico
Universidade de Lisboa
Email: goncalo.pereira@tecnico.ulisboa.pt

***Abstract*—Mobile Internet elections are appealing for several reasons: they promise voter convenience, lower abstention rates, and reduce costs. However, there are a number of trust issues that prevent them from becoming ubiquitous, the most relevant of which is the possibility of voter coercion at the time of the vote. Other issues, such as the trustworthiness of both the services running the election and the mobile voting platform (usually the voter's computer or smartphone), are also major barriers to mobile Internet elections adoption.**

The proposed "Scroll, Match & Vote" (SM&V) interface aims to overcome these trust issues, while attempting to ensure the usability required for wide adoption. The SM&V interface may be coupled with previous e-voting solutions to ensure end-to-end verifiability and collusion resistance [1], while adding coercion resistance to a degree similar to that of several coercion-resistant e-voting systems. The SM&V interface requires the use of a device with Internet connection and multitouch screen.

Prior to voting, the voter is required to register in a controlled precinct sometime between several months before the voting phase to immediately preceding the vote. In the voting phase, the voter is shown two lists side by side on the device. One list contains all the candidates' names and the other list shows voting codes. One of the voting codes is correct; the others are false. The voter casts her vote by scrolling one or both lists and matching her chosen candidate with the correct code. The voting phase may take place anywhere with an Internet connection, even in the presence of coercers.

I. Introduction

Internet elections have been a research subject for many years with a number of interesting results, several of which are being piloted worldwide [2], including on actual binding elections [3], [4]. The arguments in favor of Internet elections are obvious: i) increased voter convenience and participation, ii) greater tally accuracy and speed, and iii) reduced costs, among others. However, the arguments against Internet elections are also pertinent: i) the insecure voting-platform problem, which results from the use of multipurpose devices owned and managed by the voter [5]; ii) the lack of transparency resulting from the nonexistence of physical votes and the possibility of collusion between the digital devices participating in the election; and iii) the nonexistence of private voting precincts paving the way for several coercion scenarios.

Carlos Ribeiro was supported by Suspect, PTDC/EIA-CCO/122542/2010
Rui Joaquim was supported by the Fonds National de la Recherche, Luxembourg (grant INTER/SNF/11/11).

The widespread use of smartphones with ubiquitous Internet access has emphasised some of these advantages and disadvantages. While it is even more convenient for the voter to vote on her own smartphone, it is also easier for the coercer to influence her vote, given that the voter may vote anywhere. In spite of this, one of the most common reasons for the failure of voting experiments is the lack of usability; voting systems that are too complex are doomed to fail, even if they are able to overcome all the security problems noted above [6].

Scroll, Match & Vote (SM&V) is a coercion-resistant interface that may be coupled with an end-to-end verifiable and collusion-resistant voting protocol, like MarkPledge3 (MP3) [7], to build an Internet voting system that compares advantageously with other Internet voting systems [1], [8].

Elections are usually constrained in time and space, i.e. they must be conducted on the specified election day and in controlled precincts. This double constraint is one of the sources of abstention, given that not everyone is available to be at a specific place on a set date during certain hours. Removing either of these constraints is highly problematic. If the election takes too long (i.e. several months), the democracy suffers because some voters vote with much less information than others. Early voting and postal voting are seen as exceptions rather than as the rule. Removing the space constraint is also difficult because it usually means loosing coercion resistance [8]. The current proposal follows the path of JCJ/Civitas [9], [8] and splits the two constraints such that the space constraint and the time constraint do not apply to the same action. The voter must register at a private booth without tight time constraints (within a span of one or two months) and must vote on election day without any space constraints (with the exception of having an Internet connection).

The SM&V interface assumes that the voter owns a mobile Internet device with a multitouch screen (hereafter referred to the voter's smartphone).

The next section describes the complete voting process, while section III states and discusses the security properties of the system and section IV discusses usability properties. We conclude in section V.

II. SM&V Voter Interaction

From a voter's perspective, the voting machine is her smartphone, although, as described below, the actual ballot creation may be performed by an applet running inside a

UICC, a secure SDCard, or any other secure element (SE) in order to ensure confidentiality of the vote (cf. [10]).

The voter process is divided into three phases: the registration phase, the voting phase, and the verification phase.

The **registration** phase is the most complex phase of the voting process. It begins following the election initialization by the electoral commission and ends just before votes are cast, i.e. it can be done even on election day.

When SM&V is coupled with MP3, the voter is required to challenge the voting machine during registration using random values. These can be generated prior to the registration in the form of printed 2D codes by the voter herself, by an online helper organization, or even by a coercer, provided that he is not colluding with the voting machine (i.e. the UICC or the SDCard). Other end-to-end verifiable voting protocols will require slightly different interactions. The following describes the registration process for SM&V coupled with MP3.

To register, the voter should takes her smartphone to a private booth prepared especially for this purpose and presses register on her smartphone voting application (screen I in Figure 1). She will then be asked to: choose the election (screen II); read one of the 2D codes with her smartphone camera (screen III) and, tap her phone against a special device, within the private booth, dubbed "Pledge Display Device" (PDD) (screen V), whose only purpose is to build an untappable channel between the voter and the voting machine, in order to display a short secret voting code to the voter: the "pledge".

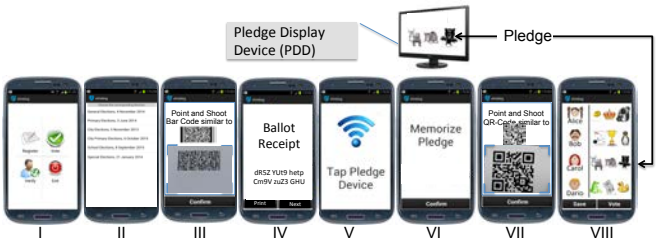


Fig. 1. Registration procedure.

The PDD owes its existence to the untrustworthiness of the voter's smartphone. Being a multipurpose device with many different applications running, it is assumed that anything displayed on its screen may be leaked to a coercer. The PDD's only purpose is to receive, decrypt, and display the "pledge". It does not know anything else about the voter; therefore, it cannot compromise the voter's privacy. Still, to ensure that using false PDDs is impossible, the "pledge" is sent to the PDD encrypted with the PDD's key, which is provided for the voting machine in a certificate signed by the electoral commission.

After tapping the smartphone on the PDD, the voter is asked to memorize the "pledge" showed in the PDD (screen VI), and read the second 2D code (screen VII). For usability purposes, the two 2D codes should be different types (e.g. a PDF417 and a QR code).

In the final step of the registration phase the voter's smartphone displays two scrollable lists side by side (screen VIII). The list on the left displays the names of the candidates, while the list on the right displays an equal number of sequences of symbols, one of which is the "pledge" shown in the PDD. To prevent coercion, the voter should also memorize a few other sequences of symbols to be used as false voting codes in case of coercion. The registration ends either by saving the generated ballot or by engaging immediately in the voting phase.

Voting is accomplished by sliding one or both lists on the screen so that the chosen candidate and the sequence of symbols with the "pledge" become aligned (they can be visible or not, provided that they are aligned), and pressing "VOTE". Without knowing the "pledge", no one next to the voter will able to tell which candidate the voter has chosen. Given that the voter is able to mislead the coercer about the sequence encoding the "pledge", a coercer will not be able to tell which candidate the voter is voting for.

In the **verification** phase, the voter checks to see if her vote was counted as she intended by verifying that her signed vote is in the poll, the 2D codes published match the printed ones, and that the vote is counted for the chosen candidate, which is done by checking a copy of her ballot. The copy of the ballot shown is similar to screen VIII of Figure 1, with the difference that it cannot be changed (the rotation is signed); the voting codes become verification codes for the end-to-end protocol and the voter may verify that the "pledge" is next to the chosen candidate. This verification process can be done using the mobile voting app, but it is recommended that the voter use another Internet device with a simple web browser connected to a Helper Organization (HOs) that she trusts. In addition to showing the vote to the voter, HOs run the necessary cryptographic checks to ensure that the verification code next to each candidate was not tampered with, and that the overall tally is correct [10].

III. Security Properties and Trust Model

The purpose of the proposed interface is to add coercion resistance to an "end-to-end verifiable" protocol, thus building a system that ensures both properties simultaneously. We have chosen the MP3 protocol for its high degree of soundness and performance, although the same exercise may be done with other end-to-end verifiable protocols. The connection between the SM&V interface and the MP3 protocol requires a slight change in the voting process (the voter casts her vote only after the generation of the MP3 receipt, which is different from the standard MarkPledge protocol usage), and MP3 verification codes are also used as voting codes, but it can be demonstrated that the overall system maintains the MP3 security properties [10].

MP3 ensures the integrity of votes cast, even if every entity is compromised, provided that there is at least one honest HO and, that, at the very least, a subset of the trustees are honest. However, it does not ensure confidentiality of the vote unless the voting machine is not compromised. Coercion resistance is not possible without vote confidentiality; therefore, SM&V ensures coercion resistance only if the voting machine is not compromised, which in our case requires that the SDCard or UICC is not compromised.

In addition to the voting machine's integrity requirement, SM&V also requires that PDDs do not disclose the "pledges" to anyone but the voters, and that only legitimate registration precincts own certified PDDs, i.e. PDDs with a certificate

signed by the election committee for that specific election. Finally, the channel between the PDD and the voter cannot be tappable, which is the most difficult requirement to satisfy, given that any one with a camera is able to record and transmit what is being displayed by the PDD within the voting booth. In spite of the difficulty, this is a common assumption of most voting protocols, including the traditional paper-based voting.[1]

With the satisfaction of the above requirements, SM&V is able to ensure simultaneous "end-to-end verifiability" and limited coercion resistance. In particular, an SM&V system is vulnerable to the following coercion attacks:

- **Randomization** - An attacker may force a voter to vote randomly, preventing the voter from voting for her the chosen candidate.
- **Forced-Abstention** - An attacker may obtain a proof of abstention by looking at the tally and verifying whether there is a vote for the coerced voter. Therefore, anyone may force a voter to abstain and then verify wether she has complied.
- **Pre-attack surveillance** - A coercer may learn with some probability the "pledge" of a voter by checking the cast ballot and learning the code next to the voter's likely chosen candidate. After learning the "pledge", the coercer may force the voter to revote for another candidate. The coercer does not know, for sure, however, wether the learned "pledge" is the correct "pledge". This vulnerability is shared with Civitas [8].

The only mitigation mechanism provided by SM&V in response to any of these attacks is to allow the voter to override her e-vote by voting physically at a voting booth.

IV. Usability Discussion

Usability is a major issue in any voting system but assumes a specific relevance in end-to-end voting systems, where the voter distrusts her voting machine and is, therefore, required to handle a more complex voting interface.

SM&V requires the voter to be able to memorize the "pledge" for a long period (sometimes over a month) and to be able to distinguish it from the remaining voting codes. From a usability perspective, a short sequence of symbols simplifies memorization; however, the length of the sequence depends on both the number of different voting codes and the number of different symbols. The number of different voting codes is set accordingly with the level of security required and the size of the ballot; more voting codes imply a lower probability of guessing the "pledge". Therefore, using short and memorable sequences implies the use of large sets of symbols, which complicate distinguishability, unless the chosen set of symbols is carefully designed so that each symbol is clearly distinguishable from the others.

According to Bertin [11] there are eight visual variables that are used by humans to distinguish symbols: shape, size, color, brightness, pattern, orientation and horizontal and vertical positions. Symbols that differ in more variables are easier to distinguish from each other; therefore it is possible to use large sets of symbols provided that they differ in as many of these variables as possible. On the other hand, long-term memory in humans beings works better with semantic information [12] rather than with abstract information, which seems to indicate that symbols representing concrete concepts are preferred over abstract ones.

TABLE I. Distribution of subjects by age and gender

	Gender			
Age	Male		Female	
15-24	5	(11.4%)	8	(18.2%)
25-49	22	(50%)	6	(13.6%)
50-64	2	(4.5%)	1	(2.3%)
> 64	0	(0%)	0	(0%)

TABLE II. Memorization techniques reported by the voters

Memorization technique	Number	
Sequence of symbols of the "pledge"	15	(29.4%)
Non-repeating symbol of the "pledge"	12	(23.5%)
Candidate in front of the "pledge"	8	(15.6%)
"Pledge" position within the ballot	7	(13.7%)
History with the symbols of the "pledge"	3	(5.88%)
Other	6	(11.8%)

We have run tests with a set of 128 different symbols, varying in both color and shape, representing 128 different objects and animals[2]. Both the "pledge" and the voting codes in the ballot are shown as combinations of three of these symbols (with a maximum of 2^{21} combinations), which results in a highly sound election (cf. [1] for soundness proofs).

The quality of the chosen set of symbols was tested by performing an experiment with 45 different subjects, with the distribution of age and gender shown in Table I. Two-thirds of the subjects were university students or had university degrees; one-fifth had only a basic education and the remaining subjects had completed secondary education. Each of the subjects was shown a sequence of three symbols similar to the "pledge" and a list of sequences of three symbols similar to the ballot. Then the subjects were asked to find the "pledge" in the ballot and memorize both the "pledge" and the position where it appears in the ballot. A copy of the ballot was given to the subjects, who were also instructed not to make any mark or written annotation about the "pledge". Finally, a month later, the subjects were asked to point to the "pledge" in the ballot.

The results were promising, although there is still some margin for improvement; only three of the 45 subjects (6.7%) were not able to point to the "pledge" within the ballot, resulting in $93.3\% \pm 6\%$ correctness for a confidence level of 0.9. However, the reasons for these errors were completely unrelated to gender, age or education level. Of the three subjects who forgot the "pledge", two mistakenly identified one symbol for another in their "pledge" (the same pair of symbols which were too much similar) and the third mistakenly identified a voting code similar to the "pledge" of a previous experiment. These two types of mistakes confirmed the relevance of carefully thought-out choice of symbols and

[1] Notice the official warnings against selfies taken inside the booth in the 2014 European elections.

[2] Taken from the popular game *Categories*.

revealed that consecutive elections should not share the same set of symbols. Both problems may be easily solved.

The voters who chose the correct "pledge" reported using several techniques in order to memorize it (Table II). While some reported to have memorized all three symbols in the "pledge" (29.4%), others memorized just one symbol that they found was not repeated in any other position in the ballot (23.5%). Still others memorized the name of the candidate that was in front of the "pledge" when the ballot was saved (15.6%). Finally, some memorized the position of the "pledge" in the ballot (13.7%). Note that a few voters used several memorization techniques.

Another interesting result was the subjects' perceptions of the level of difficulty of the task; the task was perceived to be much more difficult than it actually is. While 28.9% of the subjects stated, at the beginning of the experience, that they were expecting to fail (i.e. forgetting the "pledge"), the reality is that only 6.7% (three subjects) forgot, and the mistake was due more to an error in the experiment than to the inability of the voters. This error in subjects' perceptions of the difficulty of the task may result from modesty, i.e. the voter may not want to boast about her ability to memorize the code without testing how difficult it is. However, it may also result from not correctly perceiving the task they were asked to perform. In fact, several voters showed surprise when they were told that they could keep the "pledge" written in the ballot together with the other codes and would just have to memorize which of them it is the "pledge", and that they could even refresh their memory from time to time, if they want to do so.

Some subjects also reported that they would prefer a different set of symbols, such as numbers or letters. In fact, SM&V may be adapted to use several sets of symbols in the same election, provided that the voter chooses the set of symbols to use prior to seeing the "pledge" (to avoid a covert channel). With such an option, one of the sets of symbols could be specifically designed for color-blind voters. Nevertheless, it is expected that some voters will forget the "pledge" or be uncertain of it, yet they should not be prevented from voting. In SM&V, a voter may register again and receive another "pledge" or may even decide to invalidate her Internet registration and vote using the traditional paper-based ballot or any other voting methods, i.e. SM&V may coexist with other voting methods, leaving to the voter the choice of which method to use.

The experiment also demonstrated that using SM&V for simultaneous election and multiple-choice elections has additional usability challenges. It is clear that asking voters to memorize one "pledge" for each election will result in a major usability problem. On the other hand, using one "pledge" for every simultaneous elections will result in a security problem. One solution is to create a ballot with every possible combination of choices and ask the voter to choose one combination of candidates. Such large ballot would not only require a different interface to be shown and manipulated by the voter but also a huge number of different verification codes. Finding a large-enough distinguishable set of symbols is a challenge by it self. A possible solution is to use a combination of nouns and verbs, creating random sentences like "Tickets Flood Chicken". Such verification codes can easily reach 10^9 combinations ($10^3 nouns \times 10^3 verbs \times 10^3 nouns$), and can be alphabetically ordered, which is enough for most elections ($\mathrm{O}\left(10^6\right)$) but not all (e.g. Chicago voters in 2000 had 78 choices to make).

V. Conclusion

Although secure mobile Internet elections are a difficult goal to achieve, and there is still a long way to go until all relevant properties are attained simultaneously, particularly resistance to *surveillance attacks*, we believe that SM&V is a step in that direction.

SM&V leaves room for further development in terms of both security and usability. From a security point of view, the most important evolution would be the resistance to surveillance attacks within the voting booth. While eliminating these attacks may be difficult, it might be possible to raise the bar for the attacker by incorporating touch sensitive channels (e.g. cold and hot surfaces) between the voter and the Secure Element generating the vote. From a usability point of view, it is also possible to envision several developments. The current interface is not able to manage multiple-choice and simultaneous elections. Both problems may be solved by the same solution, given that multiple-choice elections can mimic multiple simultaneous elections, and several solutions are currently being tested.

References

[1] R. Joaquim, C. Ribeiro, and P. Ferreira, "Eviv: an end-to-end verifiable internet voting system," *Computers & Security*, vol. 32, pp. 170–191, 2012.

[2] R. Krimmer, S. Triessnig, and M. Volkamer, "The development of remote e-voting around the world: A review of roads and directions," in *E-Voting and Identity*, ser. LNCS. Bochum, Germany: Springer Berlin / Heidelberg, October 2007, vol. 4896, pp. 1–15.

[3] G. Schryen and E. Rich, "Security in large-scale internet elections: a retrospective analysis of elections in estonia, the netherlands, and switzerland," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 4, pp. 729–744, 2009.

[4] Ministry of Local Government and Regional Development, "e-vote 2011 - project web site," September 2012, http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658.

[5] A. D. Rubin, "Security considerations for remote electronic voting," *Commun. ACM*, vol. 45, no. 12, pp. 39–44, Dec. 2002. [Online]. Available: http://doi.acm.org/10.1145/585597.585599

[6] A.-M. Oostveen and P. Van den Besselaar, "Security as belief: user?s perceptions on the security of electronic voting systems," *Electronic voting in Europe: Technology, law, politics and society*, vol. 47, pp. 73–82, 2004.

[7] R. Joaquim and C. Ribeiro, "An efficient and highly sound voter verification technique and its implementation," in *E-Voting and Identity*. Springer, 2012, pp. 104–121.

[8] M. Clarkson, S. Chong, and A. Myers, "Civitas: Toward a secure voting system," in *IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE Computer Society, May 2008, pp. 354–368.

[9] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proc. of the 2005 ACM workshop on Privacy in the electronic society*. Alexandria, VA, USA: ACM, November 2005, pp. 61–70.

[10] C. Ribeiro, Joaquim, and G. Pereira, "Scroll, match & vote: An e2e coercion resistant mobile voting system," INESC-ID, https://www.inesc-id.pt/ficheiros/publicacoes/10160.pdf, Tech. Rep. 14, May 2014.

[11] J. Bertin, *Semiology of graphics: diagrams, networks, maps*. Wisconsin: University of Wisconsin press, 1983.

[12] F. I. Craik and R. S. Lockhart, "Levels of processing: A framework for memory research," *Journal of verbal learning and verbal behavior*, vol. 11, no. 6, pp. 671–684, 1972.

Proceedings EVOTE2014
TUT Press

ISBN 978-9949-23-685-5 (PDF)
ISBN 978-9949-23-688-6 (publication)

This conference is one of the leading international events for e-voting experts from all over the world. One of its major objectives is provide a forum for interdisciplinary and open discussion of all issues relating to electronic voting. Cumulatively, over the years 2004, 2006, 2008, 2010, 2012 and 2014 more than 550 experts from over 35 countries have attended this conference to discuss electronic voting and related topics. In so doing, they have established Bregenz as a regular forum and point of reference for the scientific community working with e-voting. This is the proceedings volume of the tenth anniversary of the first conference and contains 17 papers accepted for presentation at the conference.

printed by TUT Press, Tallinn