NTNU
Norwegian University of
Science and Technology

Improvements in Everlasting Privacy:

Efficient and Secure Zero Knowledge Proofs

Thomas Haines Clementine Gritti
NTNU, Trondheim, Norway

October 2019

Trondheim – Gjøvik – Ålesund

Summary

- Verifiable electronic voting promises to ensure:

Summary

— Verifiable electronic voting promises to ensure:

- the correctness of elections even in the presence of a corrupt authority,

Summary

- Verifiable electronic voting promises to ensure:
  - the correctness of elections even in the presence of a corrupt authority,
  - and provide strong privacy guarantees.

Summary

— Verifiable electronic voting promises to ensure:
  - the correctness of elections even in the presence of a corrupt authority,
  - and provide strong privacy guarantees.

No ongoing privacy

However, few practical systems with end-to-end verifiability are expected to offer long term privacy, let alone guarantee it.

Summary

— Most current constructions for everlasting privacy use perfectly hiding commitment schemes and public key encryption;

Summary

- Most current constructions for everlasting privacy use perfectly hiding commitment schemes and public key encryption;
- this is made verifiable by use of Zero Knowledge Proofs (ZKPs) for correct encryption and correct shuffling of ballots.

Summary

— Various currently proposed solutions rely on unusual constructions whose security has not been established.

Summary

— Various currently proposed solutions rely on unusual constructions whose security has not been established.

— The cost of verifying the zero knowledge proofs of other solutions has only been partially analysed.

Summary

- Various currently proposed solutions rely on unusual constructions whose security has not been established.
- The cost of verifying the zero knowledge proofs of other solutions has only been partially analysed.
- Our work builds upon Moran and Naor's solution—and its extensions, applications and generalisations—to present a scheme which is additively homomorphic, efficient to verify, and rests upon well studied assumptions.

Introduction

— At present future breakthroughs in computation power, mathematics, or large-scale quantum computers will put the voters’ privacy at risk.

Introduction

- At present future breakthroughs in computation power, mathematics, or large-scale quantum computers will put the voters’ privacy at risk.
- There are schemes which provide information theoretic maximal privacy but these are impractical for most real elections.

Introduction

- At present future breakthroughs in computation power, mathematics, or large-scale quantum computers will put the voters' privacy at risk.
- There are schemes which provide information theoretic maximal privacy but these are impractical for most real elections.
- Much of the everlasting privacy literature relies on and builds upon Moran and Naor's work [MN10], which was modified as an extension to the web-based voting Helios scheme [DVDGA12].

Introduction

- At present future breakthroughs in computation power, mathematics, or large-scale quantum computers will put the voters' privacy at risk.
- There are schemes which provide information theoretic maximal privacy but these are impractical for most real elections.
- Much of the everlasting privacy literature relies on and builds upon Moran and Naor's work [MN10], which was modified as an extension to the web-based voting Helios scheme [DVDGA12].
- Moran and Naor's scheme and many others, including ours, have at least one (sometimes threshold of) authorities against which privacy holds only computationally.

Primitives

Pedersen commitments: The modified Pedersen commitment scheme Π is the triple of PPT algorithms $(\Pi.\mathrm{Setup}, \Pi.\mathrm{Com}, \Pi.\mathrm{Open})$:

- $CK \leftarrow \Pi.\mathrm{Setup}(\mathbb{G})$ s.t. $CK = \{\mathbb{G}, g, h\}$. Given a group $\mathbb{G}$ of semi-prime order n, let g be any generator of $\mathbb{G}$ and choose $h \leftarrow_r \mathbb{G}$ (with overwhelming probability h will be a generator).
- A given Commit Key $CK = \{\mathbb{G}, g, h\}$ defines the message space $\mathcal{M}_{CK} = \mathbb{Z}_n$, randomness space $\mathcal{R}_{CK} = \mathbb{Z}_n$, commitment space $\mathcal{C}_{CK} = \mathbb{G}_n$, and opening space $\mathcal{D}_{CK} = (\mathbb{Z}_n, \mathbb{Z}_n)$. The $\Pi.\mathrm{Com}_{CK}$ algorithm takes $m \in \mathbb{Z}_n, r \in \mathbb{Z}_n$ and sets $c = g^r h^m$ and $d = (m, r)$.
- The $\Pi.\mathrm{Open}_{CK}$ algorithm takes a commitment $c \in \mathbb{G}_n$ and opening $d \in (m \in \mathbb{Z}_n, r \in \mathbb{Z}_n)$. If $c = g^r h^m$ return m else return $\perp$.

Primitives

Moran-Naor (MN) encryption:

- Σ.KeyGen ouputs $PK = (n)$ and $SK = (d)$, where $n = pq$ is a RSA modulus and d is the lowest common multiple of $p - 1$ and $q - 1$. Choose k s.t. $kn + 1$ is prime, and let g, h be random generators of subgroup of order n in $\mathbb{Z}^*_{kn+1}$, denoted $\mathbb{G}_n$.
- Let $\Sigma.\mathrm{Enc}_{PK}(m \in \mathbb{Z}_n, (r \in \mathbb{Z}_n, r' \in \mathbb{Z}^*_n, r'' \in \mathbb{Z}^*_n))$ produce $CT = (c, ct_1, ct_2) = (g^r h^m \bmod kn + 1, (1 + n)^m r'^n \bmod n^2, (1 + n)^r r''^n \bmod n^2)$.
- $\Sigma.\mathrm{Dec}_{SK}(CT = (c, ct_1, ct_2))$ be the decryption function. First use the Paillier decryption function to retrieve m, r from ct_1, ct_2 respectively, then if $c = g^r h^m$ the result is m else $\perp$.

Moran and Naor's scheme (Incredible roughly)

Scheme:

- The voter submits unconditional hiding commitments to the bulletin board
- The voter, also, submits encrypted openings of these commitments to the authorities
- The authorities verifiable shuffle the unconditional hiding commitments and the openings.

Security:

- Integrity: Verifiability of the shuffle and binding property of the commitments
- Everlasting Privacy: All the information on the bulletin board in perfectly/statistically hiding

Moran and Naor’s scheme (Incredible roughly)

e encrypted votes (MN/Moran-Naor)
c commitments to votes (Pedersen)
v plaintext votes and openings

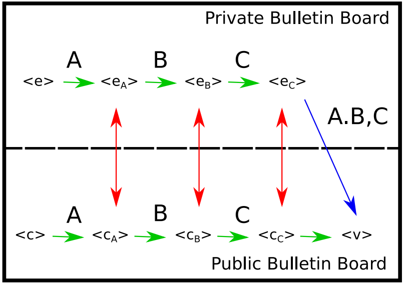

Figure: Mixing with three authorities

Moran and Naor's scheme (Incredible roughly)

Moran and Naor said "although more efficient (zero knowledge) protocols exist for these applications, for the purpose of this paper we concentrate on simplicity and ease of understanding" [MN10].

Problem

In the decade since the follow up work has continued to rely on cut-and-choose [BDvdG13, DVDGA12].

Our contribution finally closes this gap by providing efficient proofs for encryption, re-encryption and shuffling.

Related work

— Arapinis *et al.* [ACKR13] recently showed in ProVerif that various constructions achieve everlasting privacy,

Related work

— Arapinis *et al.* [ACKR13] recently showed in ProVerif that various constructions achieve everlasting privacy,
  - some of these solutions lose verifiability properties in exchange for everlasting privacy.

Related work

— Arapinis *et al.* [ACKR13] recently showed in ProVerif that various constructions achieve everlasting privacy,

- some of these solutions lose verifiability properties in exchange for everlasting privacy.

— Cuvelier *et al.* [CPP13] systematised much of the research by showing how certain types of primitives can be securely combined.

Related work

- Arapinis *et al.* [ACKR13] recently showed in ProVerif that various constructions achieve everlasting privacy,
  - some of these solutions lose verifiability properties in exchange for everlasting privacy.
- Cuvelier *et al.* [CPP13] systematised much of the research by showing how certain types of primitives can be securely combined.
  - They also present an elegant scheme called PPATC based on Abe *et al.*'s [AHO12] commitment scheme on bilinear pairings, which they show has efficient encryption on the order of 40 times faster then existing methods.

Related work

— Arapinis *et al.* [ACKR13] recently showed in ProVerif that various constructions achieve everlasting privacy,
  - some of these solutions lose verifiability properties in exchange for everlasting privacy.

— Cuvelier *et al.* [CPP13] systematised much of the research by showing how certain types of primitives can be securely combined.
  - They also present an elegant scheme called PPATC based on Abe *et al.*'s [AHO12] commitment scheme on bilinear pairings, which they show has efficient encryption on the order of 40 times faster then existing methods.

— However, Cuvelier *et al.* [CPP13] do not account for the verification complexity.

Our contribution

— We present the Sigma Protocol for re-encryption of the MN cryptosystem; we also provide the proof for this Sigma Protocol and for the protocol for correct encryption [CPP13] of the MN cryptosystem;

Our contribution

- We present the Sigma Protocol for re-encryption of the MN cryptosystem; we also provide the proof for this Sigma Protocol and for the protocol for correct encryption [CPP13] of the MN cryptosystem;
- We provide the first proof of security for the existing modified Pedersen commitment of semi-prime order;

Our contribution

- We present the Sigma Protocol for re-encryption of the MN cryptosystem; we also provide the proof for this Sigma Protocol and for the protocol for correct encryption [CPP13] of the MN cryptosystem;
- We provide the first proof of security for the existing modified Pedersen commitment of semi-prime order;
- We present an efficient variant of ballot mixing;

Our contribution

- We present the Sigma Protocol for re-encryption of the MN cryptosystem; we also provide the proof for this Sigma Protocol and for the protocol for correct encryption [CPP13] of the MN cryptosystem;
- We provide the first proof of security for the existing modified Pedersen commitment of semi-prime order;
- We present an efficient variant of ballot mixing;
- We show that Moran-Naor suggestion of Paillier encryption and Pedersen commitments—refereed as PPATP in [CPP13]—is at least as fast to verify as PPATC when using the Sigma Protocol and mix-net we will detail later.

Our contribution

- We present the Sigma Protocol for re-encryption of the MN cryptosystem; we also provide the proof for this Sigma Protocol and for the protocol for correct encryption [CPP13] of the MN cryptosystem;
- We provide the first proof of security for the existing modified Pedersen commitment of semi-prime order;
- We present an efficient variant of ballot mixing;
- We show that Moran-Naor suggestion of Paillier encryption and Pedersen commitments—refereed as PPATP in [CPP13]—is at least as fast to verify as PPATC when using the Sigma Protocol and mix-net we will detail later.
- Further, the MN system supports homomorphic tallying where PPATC does not which is a significant advantage in some situations.

Sigma protocols

The Sigma Protocol for correct encryption was proposed by Cuvelier *et al.* [CPP13], though they omit the proof. Such a protocol is used to prove that two ciphertexts encrypt the opening to a commitment.

We give a Sigma Protocol for correct re-encryption.

Pedersen commitment of semi-prime order

$\mathbb{G}_p, g_p, h_p, \mathbb{G}_q, g_q, h_q$

$\downarrow$

Challenger

$(\mathbb{G}_n, g, h)$ $\longrightarrow$

Adversary

$\longleftarrow$ (c,$(m_1, r_1), (m_2, r_2)$)

Let $\mathbb{G}_n$ be the direct product of $\mathbb{G}_p$ and $\mathbb{G}_q$

Let $g = g_p \times g_q$ $h = h_p \times h_q$

if $GCD(m_1 - m_2, n) = 1$ or $GCD(r_1 - r_2, n) = 1$ **then** WLOG

return $\gamma = (r_2 - r_1)/(m_1 - m_2)$ mod $p, \delta = (r_2 - r_1)/(m_1 - m_2)$ mod q,

if WLOG $GCD(m_1 - m_2, n) = p$ **return** $\delta = (r_2 - r_1)/(m_1 - m_2)$

$\downarrow$

γ and/or δ

Figure: Reduction from binding to discrete log

More efficient mixing

Algorithm 1: Proof of Shuffle on Private Board

Common Input: Commitment parameters $g, h, h_1, \ldots, h_N \in \mathbb{G}_n$, two ciphertexts $\mathbf{e} = (e_1, \ldots, e_N) \in \mathcal{C}_{PK}$ and $\mathbf{e}' = (e'_1, \ldots, e'_n) \in \mathcal{C}_{PK}$, and a permutation matrix commitment $\mathbf{c} = (c_1, \ldots, c_N)$.

Private Input : Permutation matrix $M = (m_{i,j}) \in \mathbb{Z}_n^{N \times N}$, randomness $\mathbf{r} = (r_1, \ldots, r_N) \in \mathbb{Z}_n^N$ s.t. $c_j = g^{r_j} \prod_{i=1}^N h_i^{m_{j,i}}$, and randomness $\mathbf{r}' = (r'_1, \ldots, r'_N) \in \mathcal{R}_{pk}$ s.t. $e'_i = \phi_{PK}(e_{\pi(i)}, r'_{\pi(i)})$, for $i, j \in [1, N]$.

1 $\mathcal{V}$ chooses $\mathbf{u} = (u_1, \ldots, u_N) \in \mathbb{Z}_n^N$ randomly and hands $\mathbf{u}$ to $\mathcal{P}$.

2 $\mathcal{P}$ defines $\mathbf{u}' = (u'_1, \ldots, u'_N) = M\mathbf{u}$ and then chooses $\hat{\mathbf{r}} = (\hat{r}_1, \ldots, \hat{r}_N)$, $\hat{\mathbf{w}} = (\hat{w}_1, \ldots, \hat{w}_N)$, $\mathbf{w}' = (w'_1, \ldots, w'_N) \in \mathbb{Z}_n^N$, and $w_1, w_2, w_3, \in \mathbb{Z}_n$ and $w_4 \in \mathcal{R}_{PK}$. $\mathcal{P}$ defines $\bar{r} = \langle \bar{1}, \mathbf{r} \rangle$, $\tilde{r} = \langle \mathbf{r}, \mathbf{u} \rangle$, $\hat{r} = \sum_{i=1}^N \hat{r}_i \prod_{j=i+1}^N u'_j$ and $r' = (\sum_{i=1}^N r'_{i,0} u_i, \prod_{i=1}^N r'^{u_i}_{i,1}, \prod_{i=1}^N r'^{u_i}_{i,2})$. $\mathcal{P}$ hands to $\mathcal{V}$, where we set $\hat{c}_0 = h$ and $i \in [1, N]$,

$$\hat{c}_i = g^{\hat{r}_i} \hat{c}_{i-1}^{u'_i} \qquad t_1 = g^{w_1} \qquad t_2 = g^{w_2} \qquad t_3 = g^{w_3} \prod_{i=1}^N h_i^{w'_i}$$

$$t_4 = \Sigma.\mathrm{Enc}_{PK}(0, w_4) \prod_{i=1}^N e_i'^{w'_i} \qquad \hat{t}_i = g^{\hat{w}_i} \hat{c}_{i-1}^{w'_i}$$

3 $\mathcal{V}$ chooses a challenge $\xi \in \mathbb{Z}_n$ at random and sends it to $\mathcal{P}$.

4 $\mathcal{P}$ then responds with:

$$s_1 = w_1 + \xi \cdot \bar{r} \qquad s_2 = w_2 + \xi \cdot \hat{r} \qquad s_3 = w_3 + \xi \cdot \tilde{r} \qquad s_4 = w_4 - \xi \cdot r'$$

$$\hat{s}_i = \hat{w}_i + \xi \cdot \hat{r}_i \qquad s'_i = w'_i + \xi \cdot u'_i$$

5 $\mathcal{V}$ accepts if and only if, for $i \in [1, N]$,

$$t_1 = \left(\prod_{i=1}^N c_i / \prod_{i=1}^N h_i\right)^{-\xi} g^{s_1} \qquad t_2 = \left(\hat{c}_N / h^{\prod_{i=1}^N u_i}\right)^{-\xi} g^{s_2} \qquad t_3 = \left(\prod_{i=1}^N c_i^{u_i}\right)^{-\xi} g^{s_3} \prod_{i=1}^N h_i^{s'_i}$$

$$t_4 = \left(\prod_{i=1}^N (e_i)^{u_i}\right)^{-\xi} \Sigma.\mathrm{Enc}_{PK}(0, s_4) \prod_{i=1}^N (e'_i)^{s'_i} \qquad \hat{t}_i = \hat{c}_i^{-\xi} g^{\hat{s}_i} \hat{c}_{i-1}^{s'_i}$$

Efficiency Encryption

Scheme	MN [MN10]	PPATC [CPP13]
$Exp_{\mathbb{Z}^*_{kn+1}}$	3.375	0
$Exp_{\mathbb{Z}^*_{n^2}}$	4	0
$Mult_{\mathbb{G}_1}$	0	9
$Mult_{\mathbb{G}_2}$	0	4
Total cost	1,024,896 multiplications	114,432 multiplications

Table: Total number of operations executed for encryption - Total cost is obtained according to the implementation setting.

Efficiency Verification

Scheme	MN [MN10]	PPATC [CPP13]
$Exp_{\mathbb{Z}^*_{kn+1}}$	1.125	0
$Exp_{\mathbb{Z}^*_{n^2}}$	0	0
$Mult_{\mathbb{G}_1}$	0	1
$Mult_{\mathbb{G}_2}$	0	0
Pairing	0	3
Total cost	79,488 multiplications	119,040 multiplications

Table: Total number of operations executed for opening verification - Total cost is obtained according to the implementation setting.

Conclusion

— Both verifiability and ongoing privacy are important.

Conclusion

- Both verifiability and ongoing privacy are important.
- There is currently a lack of well fleshed out solutions we provide verifiability, practicality, and ongoing privacy.

Conclusion

- Both verifiability and ongoing privacy are important.
- There is currently a lack of well fleshed out solutions we provide verifiability, practicality, and ongoing privacy.
- Various currently proposed solutions with everlasting privacy rely on unusual constructions.

Conclusion

— Both verifiability and ongoing privacy are important.

— There is currently a lack of well fleshed out solutions we provide verifiability, practicality, and ongoing privacy.

— Various currently proposed solutions with everlasting privacy rely on unusual constructions.

— In the decade since Moran and Naor presented their seminal work many of the gaps have been left open.

Conclusion

- Both verifiability and ongoing privacy are important.
- There is currently a lack of well fleshed out solutions we provide verifiability, practicality, and ongoing privacy.
- Various currently proposed solutions with everlasting privacy rely on unusual constructions.
- In the decade since Moran and Naor presented their seminal work many of the gaps have been left open.
- We close the gaps in the security proofs and zero knowledge proofs for schemes in the style of Moran-Naor.

Questions?

References

[ACKR13] Myrto Arapinis, Véronique Cortier, Steve Kremer, and Mark Ryan, *Practical everlasting privacy*, POST, LNCS, vol. 7796, Springer, 2013, pp. 21–40.

[AHO12] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo, *Group to group commitments do not shrink*, EUROCRYPT, LNCS, vol. 7237, Springer, 2012, pp. 301–317.

[BDvdG13] Johannes A. Buchmann, Denise Demirel, and Jeroen van de Graaf, *Towards a publicly-verifiable mix-net providing everlasting privacy*, Financial Cryptography, Lecture Notes in Computer Science, vol. 7859, Springer, 2013, pp. 197–204.

[CPP13] Edouard Cuvelier, Olivier Pereira, and Thomas Peters, *Election verifiability or ballot privacy: Do we need to choose?*, ESORICS, LNCS, 2013, pp. 481–498.