Security Models For Everlasting Privacy

Athecrypt 2020

Panagiotis Grontas
Aris Pagourtzis
Alexandros Zacharakis

National Technical University
Of Athens

07.01.2020

https://eprint.iacr.org/2019/1193

TL;DR

- Game-based definitions for everlasting privacy
- A new adversarial model
  - Powerful computational capabilities *in the future*
  - Extensive data collection *in the present*
- Contemporary adversary (privacy)
  - Corrupt voters
  - Monitor & store communications
  - Computationally bounded
- Future adversary
  - Examine past public data
  - Potentially has insider access to past private data (surveillance - breaking of trust assumptions)
  - Computationally powerful
- Everlasting privacy variations

Electronic Voting Properties:Verifiability

- Voters vote in an adversarial environment (bugs, malice)
- Election authorities and voter devices are not trusted

Checks:

- Cast as intended
- Recorded as cast
- Tallied as recorded

Verifiability: voters and auditors check the process

- Individual
- Universal
- Eligibility

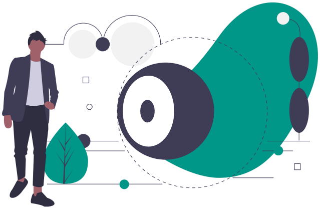
Accountability: a stronger from of verifiability

Electronic Voting Properties:Privacy

Standard feature of elections since the 19th century encoded into law

Privacy is not absolute: The result reveals information but no more should leak

- Secrecy: Encryption & Commitment schemes [CFSY96, Adi08, KZZ15]
- Anonymity: Mixnets [Cha81] & Blind signatures [Cha82]
- Computational & trust assumptions
- Flavors:
  - Receipt Freeness [BT94]
  - Coercion Resistance [JCJ05]
  - Perfect Ballot Secrecy [KY02]
  - Everlasting Privacy [MN06]



Relation of privacy and verifiability

- To enable verifiability the system must generate evidence
  - without compromising secrecy
  - without functioning as a receipt
- Does verifiability without privacy make sense?
  - Does it really matter if the vote is dictated by a coercer or changed by a corrupted authority?
- You can't have (computational) privacy without individual verifiability [CL18]
  - Replace votes in order to learn how a targeted voter voted
  - Voters that check their votes protect the privacy of others
- Integrity is ephemeral, privacy should be everlasting [MN06]
  - integrity matters until the loser is convinced

Everlasting privacy = Post Snowden Privacy

- Encryption becomes obsolete
  - Gradually (e.g. Moore's Law, better attacks)
  - Spectacularly (e.g. practical quantum computing)
- Verifiability $\longrightarrow$ election data widely available
- Voting data can be valuable to a future authoritarian regime
- Resources in Snowden's world:
  - Advanced computational power
  - Collected data (e.g. mass surveillance)
  - Insider data (e.g. political parties)
- Indirect coercion attempt

Everlasting Privacy: Previous work I

Formal study initiated in [MN06]

Receipt-Free Universally-Verifiable Voting with Everlasting Privacy*

Tal Moran and Moni Naor**

Department of Computer Science and Applied Mathematics,
Weizmann Institute of Science, Rehovot, Israel

More concrete in [MN10]

Split-Ballot Voting:
Everlasting Privacy With Distributed Trust

TAL MORAN
Weizmann Institute of Science, Israel
and
MONI NAOR
Weizmann Institute of Science, Israel

Previously hinted in:
[CFSY96]: Perfectly hiding

Pedersen commitments & verifiable secret sharing through private channels [FOO92]

Theorem 3 (Privacy). *Even if the administrator and the counter conspire, they cannot detect the relation between vote v_i and voter V_i.*

Sketch of Proof. The relation between the voter's identity ID_i and the ballot x_i is hidden by the blind signature scheme. The ballot x_i and the key k_i are sent through the anonymous communication channel. So no one can trace the communication and violet the privacy of the voters. It is unconditionally secure against tracing the voting.

Made practical in [HG19]

Blind signatures & anonymous channels

Everlasting Privacy: Previous work II

Split ballot voting [MN10]

- Two election authorities
- Votes cast protected using a perfectly hiding commitment scheme
- To tally, the openings are required
- Exchanged computationally protected
- Tallying: Parallel shuffling of commitments and openings between the authorities
- Casting is not anonymous

- Everlasting privacy
  - the authorities are honest
  - they do not collaborate
  - the openings are not made public
- One corrupted authority: computational privacy
- Two corrupted authorities: correctness

Everlasting Privacy: Previous work III

Everlasting privacy = information theoretic security against the public view

- [DGA12] Replace Helios exp. ElGamal with Pedersen commitments (openings sent through private channels)
- [CPP13] Commitment Consistent Encryption - use of public/private Bulleting Boards
- [BDV13] Encapsulate as a mixnet
- [ACKR13] Formalization as *practical* everlasting privacy in the applied pi-calculus

Everlasting Privacy: Previous work IV

Revisiting the anonymous channel idea [FOO92] for casting

[LH15] & [LHK16]:

- Public credentials to the Bulletin Board
- (Un)encrypted vote to the Bulletin Board
- Commitment to 1 out of *n* voting credentials with ZKPoK
- Follow up: Deniable vote updating for coercion resistance

Anonymous channel: helps with coercion resistance by thwarting forced abstention attack

Everlasting Privacy: Previous work V

[GPZZ19]

- Coercion resistance using real-fake credentials
- All valid credentials posted to BB
- During voting attach a (fake) credential to a blinded ballot
- Election authority marks validity by signing
- All checks are embedded into a variation of blind signatures (PACBS)
- Include ZKPoK for EA's actions provide verifiability

All voting interactions are auditable in the BB

A Generic Voting System - Participants

Participants:

- Election Authority
- *n* voters
- *m* candidates
- Bulletin Board to store all voting related data in a publicly accessible manner

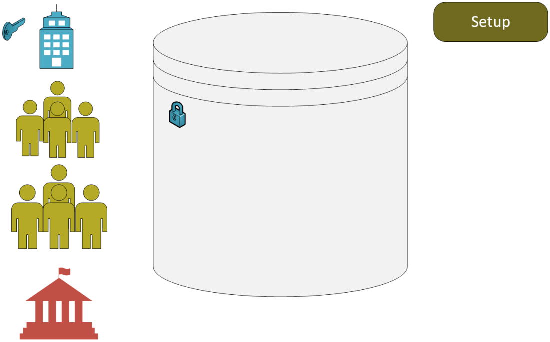
A Generic Voting System - Functionalities

- $(\text{params}, sk_{\mathcal{EA}}, pk_{\mathcal{EA}}) := \text{Setup}(1^{\lambda})$
- $(\text{pk}_i, (\text{sk}_i, \text{pk}_i)) := \text{Register}\langle \mathcal{EA}(\text{sk}_{\mathcal{EA}}), \mathcal{V}_i() \rangle$
- $(\mathrm{I}, \mathrm{C}) :=$ $\text{SetupElection}(sk_{\mathcal{EA}}, n, m, \text{params}, \text{Election-information})$
- $(\perp, (\mathrm{b}_i, \pi_{\mathrm{b}_i})) :=$ $\text{Vote}\langle \mathcal{EA}(\text{sk}_{\mathcal{EA}}), \mathcal{V}_i(\text{c}_i, \text{sk}_i), \text{params}, \text{pk}_{\mathcal{EA}}, \text{pk}_i, \mathrm{I}, \mathrm{C}, \mathcal{BB} \rangle$
- $\mathcal{BB} \Leftarrow \text{Cast}\langle \mathcal{BB}(), \mathcal{V}_i(\mathrm{b}_i, \pi_{\mathrm{b}_i}) \rangle$
- $\{0, 1\} = \text{Valid}(\mathcal{BB}, \mathrm{b})$
- $(\mathbf{T}, \pi_{\mathbf{T}}) := \text{Tally}(\text{sk}_{\mathcal{EA}}, \text{params}, \mathrm{C}, \mathcal{BB})$
- $\{0, 1\} = \text{Verify}(\mathbf{T}, \text{params}, \text{pk}_{\mathcal{EA}}, \mathcal{BB}, \mathrm{C}, \mathrm{I}, \mathrm{b}_i, \pi_{\mathrm{b}_i}, \pi_{\mathbf{T}})$

Operation I

$(\text{params}, sk_{\mathcal{EA}}, pk_{\mathcal{EA}}) := \text{Setup}(1^\lambda)$

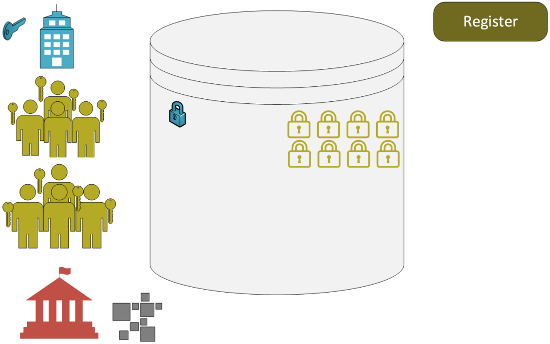
- The EA generates the cryptographic parameters and its credentials



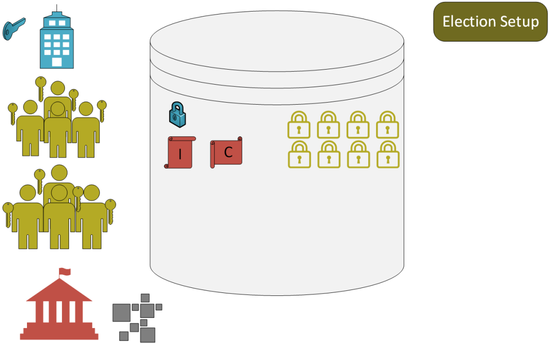
Operation II

$$(\mathsf{pk}_i, (\mathsf{sk}_i, \mathsf{pk}_i)) := \mathsf{Register}\langle \mathcal{EA}(\mathsf{sk}_{\mathcal{EA}}), \mathcal{V}_i() \rangle$$

- Each voter registers with some identifying information and obtains some form of credentials



$(\mathrm{I}, \mathrm{C}) :=$ SetupElection($sk_{\mathcal{EA}}, n, m$, params, Election-information)



- $\mathcal{EA}$ creates the election by publishing the list of eligible voters and candidates

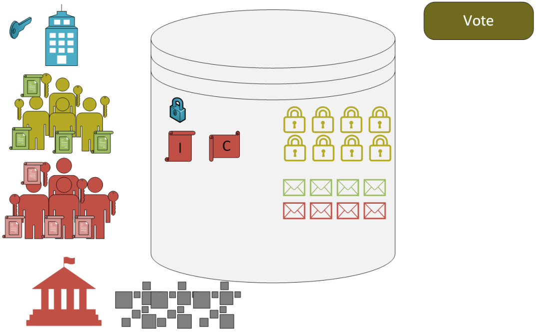
Operation- IV

Voting: Vote and Cast functionalities

$$(\perp, (\mathrm{b}_i, \pi_{\mathrm{b}_i})) := \mathsf{Vote}\langle \mathcal{EA}(\mathsf{sk}_{\mathcal{EA}}), \mathcal{V}_i(\mathsf{c}_i, \mathsf{sk}_i), \mathsf{params}, \mathsf{pk}_{\mathcal{EA}}, \mathsf{pk}_i, \mathrm{I}, \mathrm{C}, \mathcal{BB}\rangle$$

$$\mathcal{BB} \Leftarrow \mathsf{Cast}\ \langle \mathcal{BB}(), \mathcal{V}_i(\mathrm{b}_i, \pi_{\mathrm{b}_i})\rangle$$

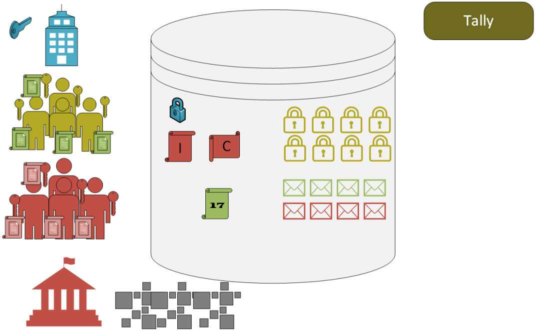
- The voter presents a credential and commits to a voting choice
- The EA verifies the right to vote
- The voter casts the ballot
- The validity of the ballot is checked



Operation - V

$$(\mathbf{T}, \pi_{\mathbf{T}}) := \text{Tally}(\text{sk}_{\mathcal{EA}}, \text{params}, \mathrm{C}, \mathcal{BB})$$

- The EA tallies the votes
- Releases the result along with a proof of correctness
- Verification takes place



Adversarial capabilities

Motivation

The everlasting privacy adversary is not only confined to the public view of the election. It also has access to ‘insider‘ information.

Contemporary Adversary $\mathcal{A}$

- Computationally Constrained
- Active participation (through voter corruption)

Future Adversary $\mathcal{A}$’

- Computationally Unbounded
- Weak Everlasting Privacy: Public protocol transcript
- Everlasting Privacy: Cooperate with $\mathcal{A}$
- Strong Everlasting Privacy: communication and ‘insider’ data

The security game

- An extension of [BCG+15] for privacy
- $\mathcal{A}$ sees two Bulletin Boards
- $\mathcal{C}$ executes Setup, Register in both Boards
- $\mathcal{A}$ chooses the eligible voters and candidates to setup the election
- $\mathcal{A}$ dynamically corrupts voters and schedules voting
- Corrupted ballots go to both BBs
- Challenge phase: $\mathcal{A}$ chooses two options c_0, c_1 for honest in $\mathcal{BB}_0, \mathcal{BB}_1$
- $\mathcal{C}$ performs tally
- $\mathcal{A}$ must guess board

The security game II

Algorithm 1: Privacy Experiment $\mathsf{Exp}^{\mathsf{priv},\beta}_{\mathcal{A},\Pi,t}(1^\lambda, n, m)$

$(\mathsf{params}, \mathsf{sk}_{\mathcal{EA}}, \mathsf{pk}_{\mathcal{EA}}) \leftarrow \Pi.\mathbf{Setup}(1^\lambda)$
$\mathcal{BB}_b \Leftarrow (\mathsf{params}, \mathsf{pk}_{\mathcal{EA}}) \quad b \in \{0,1\}$
for $i \in [n]$ **do**
    $(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathbf{Register}\langle \mathcal{EA}(\mathsf{sk}_{\mathcal{EA}}), \mathcal{V}_i \rangle$
    $\mathcal{BB}_b \Leftarrow \mathsf{pk}_i \quad b \in \{0,1\}$
    $\mathsf{Aux} \Leftarrow \mathsf{Aux}_{\mathsf{Register}}$
end
$(\mathrm{I}, \mathrm{C}) \leftarrow \mathcal{A}^{\Pi.\mathsf{SetupElection}}(n, m, \mathcal{BB}_b) \quad b \in \{0,1\}$
$V_c \leftarrow \mathcal{A}(I, \mathbf{corrupt})$
$V_h := I \backslash V_c$
for $i \in \mathrm{I}$ **do**
    if $i \in V_c$ **then**
        $c_i \leftarrow \mathcal{A}(\mathbf{choose})$
        $(\mathrm{b}_i, \pi_{\mathrm{b}_i}) \leftarrow \mathcal{A}^{\Pi.\mathsf{Vote}}(c_i, \mathsf{sk}_i, \mathcal{BB}_b) \quad b \in \{0,1\}$
    else
        $(c_0, c_1) \leftarrow \mathcal{A}(\mathbf{choose})$
        $(\mathrm{b}_{i0}, \pi_{\mathrm{b}_{i0}}) \leftarrow \mathbf{Vote}\langle(\mathcal{EA}(\mathsf{sk}_{\mathcal{EA}}), \mathcal{V}_i(c_0, \mathsf{sk}_i), \mathcal{BB}_0\rangle$
        $(\mathrm{b}_{i1}, \pi_{\mathrm{b}_{i1}}) \leftarrow \mathbf{Vote}\langle(\mathcal{EA}(\mathsf{sk}_{\mathcal{EA}}), \mathcal{V}_i(c_1, \mathsf{sk}_i), \mathcal{BB}_1\rangle$
    end
end
$\mathsf{view}_{\mathcal{A}} \Leftarrow \mathsf{view}_{\mathsf{Vote}}$
$\mathsf{Aux} \Leftarrow \mathsf{Aux}_{\mathsf{Vote}}$
for $i \in \mathrm{I}$ **do**
    if $i \in V_c$ **then**
        $\mathcal{BB}_b \Leftarrow \mathcal{A}^{\Pi.\mathsf{Cast}}(\mathrm{b}'_i, \mathcal{BB}_b) \quad b \in \{0,1\}$
    else
        $\mathcal{BB}_0 \Leftarrow \Pi.\mathbf{Cast}(\mathrm{b}'_{i0}, \mathcal{BB}_0)$
        $\mathcal{BB}_1 \Leftarrow \Pi.\mathbf{Cast}(\mathrm{b}'_{i1}, \mathcal{BB}_1)$
    end
end
$\mathsf{view}_{\mathcal{A}} \Leftarrow \mathsf{view}_{\mathsf{Cast}}$
$\mathsf{Aux} \Leftarrow \mathsf{Aux}_{\mathsf{Cast}}$
$(\mathbf{T}, \pi_{\mathbf{T}}) \leftarrow \mathcal{A}^{\Pi.\mathsf{Tally}}()$
$\beta' \leftarrow \mathcal{A}(\mathbf{T}, \pi_{\mathbf{T}}, \mathcal{BB}_\beta, \mathbf{guess})$
if $\beta = \beta' \wedge |V_c| \leq t$ **then**
    return 1
else
    return 0
end

Weak everlasting privacy

Algorithm 2: $\mathsf{Exp}^{\text{w-ever-priv},\beta}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)$

$(c_0, c_1) \leftarrow \mathcal{A}'()$
$(\mathcal{BB}_\beta, T) \leftarrow \mathcal{A}'^{\Pi}()$
$\beta' \leftarrow \mathcal{A}'(\mathbf{T}, \pi_{\mathbf{T}}, \mathcal{BB}_\beta, \mathbf{guess})$
if $\beta = \beta'$ **then**
  return 1
else
  return 0
end

Weak Everlasting Privacy for Π

$\forall \mathcal{A}'$, $\exists$ negligible function $\mu : \forall n, m :$
$\Pr[\mathsf{Exp}^{\text{w-ever-priv},0}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] -$
$\Pr[\mathsf{Exp}^{\text{w-ever-priv},1}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] \leq \mu(\lambda)$

- Parameterization by voting scheme Π and future adversary $\mathcal{A}'$
- $\mathcal{A}'$ selects the voting choices
- $\mathcal{A}'$ uses only the public view ($\mathcal{BB}$) to distinguish voting behaviour
- Game-based version of practical everlasting privacy of [ACKR13]

Everlasting privacy

Algorithm 3: $\mathrm{Exp}^{\text{ever-priv},\beta}_{\mathcal{A}',\mathcal{A},\Pi,t}(1^\lambda, n, m)$

$(c_0, c_1, V_c) \leftarrow \mathcal{A}'()$
$(\mathcal{BB}_\beta, \mathsf{view}_\mathcal{A}, T) \leftarrow \mathcal{A}'^{\Pi,\mathcal{A}}()$
$\beta' \leftarrow \mathcal{A}'(\mathbf{T}, \pi_\mathbf{T}, \mathcal{BB}_\beta, \mathsf{view}_\mathcal{A}, \mathbf{guess})$
if $\beta = \beta' \wedge |V_c| \leq t$ **then**
  return 1
else
  return 0
end

Everlasting Privacy for Π

$\forall \mathcal{A}, \mathcal{A}'$, $\exists$ negligible function $\mu : \forall n, m :$
$\Pr[\mathrm{Exp}^{\text{ever-priv},0}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] -$
$\Pr[\mathrm{Exp}^{\text{ever-priv},1}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] \leq \mu(\lambda)$

- Parameterization by voting scheme Π and current and future adversaries $\mathcal{A}, \mathcal{A}'$
- $\mathcal{A}'$ selects the voting choices and corruption strategies
- $\mathcal{A}'$ uses the public view ($\mathcal{BB}$) and $\mathcal{A}$ corruption information $\mathsf{view}_\mathcal{A}$ to distinguish voting behaviour

Strong Everlasting privacy

Algorithm 4: $\mathrm{Exp}^{\text{s-ever-priv},\beta}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)$

$(c_0, c_1, V_c) \leftarrow \mathcal{A}'()$
$(\mathcal{BB}_\beta, \mathrm{view}_\mathcal{A}, \mathrm{Aux}, T) \leftarrow \mathcal{A}'^{\Pi,\mathcal{A}}(c_0, c_1)$
$\beta' \leftarrow \mathcal{A}'(\mathbf{T}, \pi_\mathbf{T}, \mathcal{BB}_\beta, \mathrm{view}_\mathcal{A}, \mathrm{Aux}, \mathbf{guess})$
if $\beta = \beta' \wedge |V_c| \leq t$ **then**
  return 1
else
  return 0
end

Strong Everlasting Privacy for Π

$\forall \mathcal{A}, \mathcal{A}'$, $\exists$ negligible function $\mu : \forall n, m :$
$\Pr[\mathrm{Exp}^{\text{s-ever-priv},0}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] -$
$\Pr[\mathrm{Exp}^{\text{s-ever-priv},1}_{\mathcal{A}',\Pi,t}(1^\lambda, n, m)] \leq \mu(\lambda)$

- Parameterization by voting scheme Π and current and future adversaries $\mathcal{A}, \mathcal{A}'$
- $\mathcal{A}'$ selects the voting choices and corruption strategy
- $\mathcal{A}'$ uses the public view ($\mathcal{BB}$) and $\mathcal{A}$ corruption information $\mathrm{view}_\mathcal{A}$ to distinguish voting behaviour
- combines comms insider information Aux

Everlasting privacy with perfectly hiding commitments

- The problem: decommitments exchanged through private channels
- An insider will have access to them
- Commitment opening exchanged through private channel = encrypted ballot
- Strong everlasting privacy cannot be attained (in principle)
- At most weak everlasting privacy

Everlasting privacy with anonymous channel

The anonymous channel can:

- Nullify leaked information & casting order
- by disconnecting votes from voters
- can help achieve strong everlasting privacy
- must maintain other voting properties (verifiability, eligibility)

- Are we trading a problem for a different one?
- Information theoretical anonymity vs lack of central control
- Implementation on a large scale with such compromises

Discussion

References

Myrto Arapinis, Véronique Cortier, Steve Kremer, and Mark Ryan. **Practical everlasting privacy.** 2013.

Ben Adida. **Helios: Web-based open-audit voting.** 2008.

David Bernhard, Véronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. **SoK: A comprehensive analysis of game-based ballot**

Josh Benaloh and Dwight Tuinstra. **Receipt-free secret-ballot elections (extended abstract).** 1994.

Ronald Cramer, Matthew Franklin, Berry Schoenmakers, and Moti Yung. **Multi-authority secret-ballot elections with linear work.** 1996.

David Chaum. **Untraceable electronic mail, return**

privacy without individual verifiability. 2018.

Édouard Cuvelier, Olivier Pereira, and Thomas Peters. **Election verifiability or ballot privacy: Do we need to choose?** volume 8134 LNCS, 2013.

Denise Demirel, J Van De Graaf, and R Araújo. **Improving Helios with everlasting privacy towards the public.** 2012.

Zacharakis, and Bingsheng Zhang. Towards everlasting privacy and efficient coercion resistance in remote electronic voting. 2019.

Thomas Haines and Clémentine Gritti. **Improvements in everlasting privacy: Efficient and secure zero knowledge proofs.** 2019.

Ari Juels, Dario Catalano, and Markus Jakobsson.

Zacharias, and Bingsheng Zhang. **End-to-end verifiable elections in the standard model.** 2015.

Philipp Locher and Rolf Haenni. **Verifiable internet elections with everlasting privacy and minimal trust.** 2015.

Philipp Locher, Rolf Haenni, and Reto E. Koenig. **Coercion-resistant internet voting with everlasting**