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 \textit{in the future}
  - Extensive data collection \textit{in the present}
- Contemporary adversary (privacy)
  - Corrupt voters
  - Monitor & store communications
  - Computationally bounded
- Future adversary
  - Examine past \textit{public} data
  - Potentially has \textit{insider access} to past \textit{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 form of verifiability

Aleksander Essex @aleksessex · Nov 4, 2019
Electronic voting is like betting on a coin toss where you can’t inspect the coin, you can’t toss the coin, you can’t call it in the air, and you most certainly can’t see how it landed. I tell you when you lose, and you hand over the money. What? Don’t you trust me? 😊
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
  \[\text{CFSY96, Adio8, KZZ15}\]

- Anonymity: Mixnets \[\text{Cha81}\] & Blind signatures \[\text{Cha82}\]

- Computational & trust assumptions

- Flavors:
  - Receipt Freeness \[\text{BT94}\]
  - Coercion Resistance \[\text{JCJo5}\]
  - Perfect Ballot Secrecy \[\text{KYo2}\]
  - Everlasting Privacy \[\text{MNo6}\]
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 [MNo6]
  ▶ integrity matters until the loser is convinced
Encryption becomes obsolete
  ▶ Gradually (e.g. Moore’s Law, better attacks)
  ▶ Spectacularly (e.g. practical quantum computing)

Verifiability $\rightarrow$ 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
Formal study initiated in [MNO6]

More concrete in [MN10]

Previously hinted in: [CFSY96]: Perfectly hiding Pedersen commitments & verifiable secret sharing through private channels [FOO92]

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 = 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 Bulletining Boards
- [BDV13] Encapsulate as a mixnet
- [ACKR13] Formalization as *practical* everlasting privacy in the applied pi-calculus
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
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
(params, \(sk_{\mathcal{E}A}, pk_{\mathcal{E}A}\)) := Setup(1^\lambda)

(pk_i, (sk_i, pk_i)) := Register(\(\mathcal{E}A(sk_{\mathcal{E}A}), V_i()\))

(I, C) :=

SetupElection(\(sk_{\mathcal{E}A}, n, m, \text{params}, \text{Election-information}\))

(⊥, (b_i, \(\pi_{b_i}\))) :=

Vote(\(\mathcal{E}A(sk_{\mathcal{E}A}), V_i(c_i, sk_i), \text{params}, pk_{\mathcal{E}A}, pk_i, I, C, BB\))

BB \leftarrow \text{Cast}(BB(), V_i(b_i, \pi_{b_i}))

\{0, 1\} = \text{Valid}(BB, b)

(T, \(\pi_T\)) := Tally(\(sk_{\mathcal{E}A}, \text{params}, C, BB\))

\{0, 1\} = \text{Verify}(T, \text{params}, pk_{\mathcal{E}A}, BB, C, I, b_i, \pi_{b_i}, \pi_T)
\[(\text{params, } sk_{\mathcal{E}_A}, pk_{\mathcal{E}_A}) \coloneqq \text{Setup}(1^\lambda)\]

- The EA generates the cryptographic parameters and its credentials
Each voter registers with some identifying information and obtains some form of credentials.

\[(pk_i, (sk_i, pk_i)) := \text{Register}(\mathcal{E}A(\mathcal{E}A(sk_{\mathcal{E}A})), V_i())\]
\((I, C) := \text{SetupElection}(sk_{\mathcal{E}A}, n, m, \text{params}, \text{Election-information})\)

- \(\mathcal{E}A\) creates the election by publishing the list of eligible voters and candidates
Voting: Vote and Cast functionalities

\[(\bot, (b_i, \pi_{b_i})) := \text{Vote}\langle E.A(sk_{E.A}), \mathcal{V}_i(c_i, sk_i), \text{params, pk}_{E.A}, pk_i, I, C, BB\rangle\]

\[BB \leftarrow \text{Cast } \langle BB(), \mathcal{V}_i(b_i, \pi_{b_i})\rangle\]

- 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
\((T, \pi_T) := \text{Tally}(sk_{\mathcal{E}}, \text{params}, C, BB)\)

- 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
- $A$ sees two Bulletin Boards
- $C$ executes Setup, Register in both Boards
- $A$ chooses the eligible voters and candidates to setup the election
- $A$ dynamically corrupts voters and schedules voting
- Corrupted ballots go to both BBs
- Challenge phase: $A$ chooses two options $c_0, c_1$ for honest in $BB_0, BB_1$
- $C$ performs tally
- $A$ must guess board
Algorithm 1: Privacy Experiment $\text{Exp}^{\text{priv,} \beta}_{A, \Pi, t}(1^\lambda, n, m)$

$$(\text{params}, \text{sk}_A, \text{pk}_A) \leftarrow \Pi.\text{Setup}(1^\lambda)$$

$BB_b \leftarrow (\text{params}, \text{pk}_A) \quad b \in \{0, 1\}$

$$\text{for } i \in [n] \text{ do}$$

$$\text{(sk}_i, \text{pk}_i) \leftarrow \Pi.\text{Register}(\mathcal{E}A(\text{sk}_A), \mathcal{V}_i)$$

$$BB_b \leftarrow \text{pk}_i \quad b \in \{0, 1\}$$

$$\text{Aux} \leftarrow \text{Aux}_{\text{Register}}$$

$$\text{end}$$

$$(I, C') \leftarrow A^{\Pi.\text{SetupElection}}(n, m, BB_b) \quad b \in \{0, 1\}$$

$V_c \leftarrow A(I, \text{corrupt})$

$V_h := I \setminus V_c$

$$\text{for } i \in I \text{ do}$$

$$\text{if } i \in V_c \text{ then}$$

$$c_i \leftarrow A(\text{choose})$$

$$\text{(b}_i, \pi_{b_i}) \leftarrow A^{\Pi.\text{Vote}}(c_i, \text{sk}_i, BB_b) \quad b \in \{0, 1\}$$

$$\text{else}$$

$$(c_0, c_1) \leftarrow A(\text{choose})$$

$$(b_{i_0}, \pi_{b_{i_0}}) \leftarrow$$

$$\text{Vote}(((\mathcal{E}A(\text{sk}_A), \mathcal{V}_i(c_0, \text{sk}_i), BB_0)$$

$$(b_{i_1}, \pi_{b_{i_1}}) \leftarrow$$

$$\text{Vote}(((\mathcal{E}A(\text{sk}_A), \mathcal{V}_i(c_1, \text{sk}_i), BB_1)$$

$$\text{end}$$

$$\text{end}$$

$$(T, \pi_T) \leftarrow A^{\Pi.\text{Tally}()}$$

$$\beta' \leftarrow A(T, \pi_T, BB_\beta, \text{guess})$$

$$\text{if } \beta = \beta' \wedge |V_c| \leq t \text{ then}$$

$$\text{return } 1$$

$$\text{else}$$

$$\text{return } 0$$

$$\text{end}$$
Weak everlasting privacy

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

- $(c_0, c_1) \leftarrow \mathcal{A}'()$
- $(BB_\beta, T) \leftarrow \mathcal{A}'_{\Pi}()$
- $\beta' \leftarrow \mathcal{A}'(T, \pi_T, BB_\beta, \text{guess})$
- **if** $\beta = \beta'$ **then**
  - **return** 1
- **else**
  - **return** 0
- **end**

**Weak Everlasting Privacy for $\Pi$**

$\forall \mathcal{A}', \exists$ negligible function $\mu : \forall n, m :$

$\Pr[\text{Exp}_{\mathcal{A}', \Pi, t}^{w\text{-ever-priv}, 0}(1^\lambda, n, m)] -$

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

- Parameterization by voting scheme $\Pi$ and future adversary $\mathcal{A}'$
- $\mathcal{A}'$ selects the voting choices
- $\mathcal{A}'$ uses only the public view $(BB)$ to distinguish voting behaviour
- Game-based version of practical everlasting privacy of [ACKR13]
Algorithm 3: $\text{Exp}_{A', A, \Pi, t}^{\text{ever-priv}, \beta}(1^\lambda, n, m)$

$c_0, c_1, V_c \leftarrow A'()$
$(BB_\beta, \text{view}_A, T) \leftarrow A'_{\Pi, A}()$
$\beta' \leftarrow A'(T, \pi_T, BB_\beta, \text{view}_A, \text{guess})$
\text{if } \beta = \beta' \land |V_c| \leq t \text{ then}
\quad \text{return 1}
\text{else}
\quad \text{return 0}
\text{end}

Everlasting Privacy for $\Pi$

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

- Parameterization by voting scheme $\Pi$ and current and future adversaries $A, A'$
- $A'$ selects the voting choices and corruption strategies
- $A'$ uses the public view $(BB)$ and $A$ corruption information view $\text{view}_A$ to distinguish voting behaviour
**Strong Everlasting Privacy**

**Algorithm 4: \( \text{Exp}^{s\text{-ever-priv}, \beta}(1^\lambda, n, m) \)**

\[
\begin{align*}
(c_0, c_1, V_c) &\leftarrow A'(()) \\
(BB_\beta, \text{view}_A, \text{Aux}, T) &\leftarrow A'^\Pi, A(c_0, c_1) \\
\beta' &\leftarrow A'(T, \pi_T, BB_\beta, \text{view}_A, \text{Aux, guess}) \\
\textbf{if} \ \beta = \beta' \land |V_c| \leq t \ \textbf{then} \\
& \quad \text{return} \ 1 \\
\textbf{else} \\
& \quad \text{return} \ 0 \\
\textbf{end}
\end{align*}
\]

**Strong Everlasting Privacy for \( \Pi \)**

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

- Parameterization by voting scheme \( \Pi \) and current and future adversaries \( A, A' \)
- \( A' \) selects the voting choices and corruption strategy
- \( A' \) uses the public view \((BB)\) and \( A \) corruption information \( \text{view}_A \) to distinguish voting behaviour
- combines comms insider information \( \text{Aux} \)
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
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
REFERENCES

MYRTO ARAPINIS, VÉRONIQUE CORTIER, STEVE KREMER, AND MARK RYAN. PRACTICAL EVERLASTING PRIVACY. 2013.


DAVID BERNHARD, VÉRONIQUE CORTIER, DAVID GALINDO, OLIVIER PEREIRA, AND BOGDAN WARINSCHI. SOK: A COMPREHENSIVE ANALYSIS OF GAME-BASED BALLOT PRIVACY WITHOUT INDIVIDUAL VERIFIABILITY. 2018.

ÉDOUARD CRUVELIER, OLIVIER PEREIRA, AND THOMAS PETERS. ELECTION VERIFIABILITY OR BALLOT PRIVACY: DO WE NEED TO CHOOSE? volume 8134 LNCS, 2013.


DANIEL JUELS. UNTRACEABLE ELECTRONIC MAIL, RETURN ADDRESS PRIVACY, AND BEST-WORST-EVENTS. 2012.

ZACHARIAS, AND BINGSHENG ZHANG. END-TO-END VERIFIABLE ELECTIONS IN THE STANDARD MODEL. 2015.

PHILIPP LOCHER AND ROLF HAEJNI. VERIFIABLE INTERNET ELECTIONS WITH EVERLASTING PRIVACY AND MINIMAL TRUST. 2015.

PHILIPP LOCHER, ROLF HAEJNI, AND RETO E. KOENIG. COERCION-RESISTANT INTERNET VOTING WITH EVERLASTING PRIVACY. 2015.