e-voting

- Introduction
- Authentication in Electronic Elections
- Security Aspects
- Bullet Points From Paper
  - Authentication with Weaker Trust Assumptions for Voting Systems (Quaglia & Smyth)
Introduction
e-voting

- Decision making process

- Hard, conflicting security requirements for remote voting:
  - Integrity
  - Confidentiality
World Map of Electronic Voting
Authentication in Electronic Elections
**External Authentication**

\[ \Gamma_{\text{Ext}} = (\text{Setup}, \text{Vote}, \text{Tally}, \text{Verify}) \]

Identities: Tallier (T), Voter (V)

\[ \begin{align*}
T: & \quad (pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa) \\
V: & \quad b \text{ or } \bot \quad \leftarrow \text{Vote}(pk, nc, v, \kappa) \\
T: & \quad (V, pf) \quad \leftarrow \text{Tally}(sk, nc, bb, \kappa) \\
\therefore & \quad s \quad \leftarrow \text{Verify}(pk, nc, bb, V, pf, \kappa)
\end{align*} \]

**Internal Authentication**

\[ \Gamma_{\text{Int}} = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \]

Identities: Tallier (T), Registrar (R), Voter (V)

\[ \begin{align*}
T: & \quad (pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa) \\
R: & \quad (pd, d) \quad \leftarrow \text{Register}(pk, \kappa) \\
V: & \quad b \quad \leftarrow \text{Vote}(d, pk, nc, v, \kappa) \\
T: & \quad (V, pf) \quad \leftarrow \text{Tally}(sk, nc, bb, L, \kappa) \\
\therefore & \quad s \quad \leftarrow \text{Verify}(pk, nc, bb, L, V, pf, \kappa)
\end{align*} \]


*Helios (via Facebook, Google), Yahoo (via OAuth) ** Voting system by Juels, Catalano & Jakobsson via cryptographic primitives
Correctness

\[(pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa)\]

for \(1 \leq i \leq nb\) do

\[(pd_i, d_i) \leftarrow \text{Register}(pk, \kappa)\]

\[b_i \leftarrow \text{Vote(<d_i>, pk, nc, v_i, \kappa)}\]

\[V[v_i] \leftarrow V[v_i] + 1\]

\[(V', pf) \leftarrow \text{Tally}(sk, nc, \{b_1, \ldots, b_{nb}\}, <\{pd_1, \ldots, pd_{nb}\}>, \kappa)\]

\[
\text{prob}(V = V' \mid nb \leq mb \land nc \leq mc) > 1 - \text{negl}(\kappa)
\]
Security Aspects
Security Aspects
Security Aspects

- Ballot secrecy
- Election verifiability
  - Individual verifiability
  - Universal verifiability
- Eligibility verifiability
Security Aspects

- Ballot secrecy
- Election verifiability
  - Individual verifiability
  - Universal verifiability
- Eligibility verifiability
External Ballot Secrecy Game $G^{\text{Bal-Sec-Ext}}$

- Run election setup $(pk, sk, mb, mc) \leftarrow \text{Setup}(k)$.
- Call the attacker $A$ with input $1^k$ and $pk$. Await a number $nc$.
- Set $B \leftarrow \emptyset$.
- Choose a hidden bit $h \leftarrow \{0,1\}$ randomly.
- Prepare a secrecy oracle $O^{\text{Sec}}$. When called with $v_0, v_1 \in \{1, \ldots, nc\}$, the oracle creates ballot $b \leftarrow \text{Vote}(pk, nc, v_h, k)$, adds it to $B \leftarrow B \cup \{(b, v_0, v_1)\}$ and returns $b$.
- Call the attacker $A$ with $O^{\text{Sec}}$. Await a $bb$.
- Run tally $(V, pf) \leftarrow \text{Tally}(sk, nc, bb, k)$.
- Call the attacker $A$ with input $V$ and $pf$. Await a guess $h' \in \{0,1\}$.
- If $h = h' \land \text{balanced}(bb, nc, B) \land 1 \leq nc \leq mc \land \|bb\| \leq mb$ then ACCEPT else REJECT.

\[\text{balanced}(bb, nc, B):\]
\[
\forall v \in \{1, \ldots, nc\} \text{ we have} \]
\[
|\{b | b \in bb \land \exists v_1. (b, v, v_1) \in B\}| = |\{b | b \in bb \land \exists v_0. (b, v_0, v) \in B\}|
\]

**Definition**

An electronic election scheme with external auth. $\Gamma^{\text{Ext}} = (\text{Setup}, \text{Vote}, \text{Tally}, \text{Verify})$ satisfies Ballot-Secrecy-Ext iff for each ppt attacker $A$ the advantage

\[
\text{adv}^{\text{Bal-Sec-Ext}}(A) = |\text{prob } (G^{\text{Bal-Sec-Ext}}(A) = \text{ACCEPT}) - \frac{1}{2}| 
\]

is at most $\text{negl}(k)$. 

---

13
Internal Ballot Secrecy Game $G^{\text{Bal-Sec-Int}}$

- Run election setup $(pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa)$.
- **Call the attacker $A$ with input $1^\kappa$ and $pk$.** Await a number $nv$.
  
  **for** $1 \leq i \leq nv$ **do**
  
  $(pd_i, d_i) \leftarrow \text{Register}(pk, \kappa)$.

- Call the attacker $A$ with input $\{pd_1, \ldots, pd_n\}$. Await a number $nc$.
- Set $B \leftarrow \emptyset$, $R \leftarrow \emptyset$.
- Choose a hidden bit $h \leftarrow \{0,1\}$ randomly.
- **Prepare a secrecy oracle $O^{\text{Sec}}$.** When called with $i$, adds $i$ to $R$ and returns $d_i$ if $i \notin R$. When called with $i \in R$ and $v_0, v_1 \in \{1,\ldots,nc\}$, the oracle creates ballot $b \leftarrow \text{Vote}(d_i, pk, nc, v_h, \kappa)$ and adds it to $B \leftarrow B \cup \{(b,v_0,v_1)\}$, adds $i$ to $R$ and returns $b$.

- Call the attacker $A$ with $O^{\text{Sec}}$. Await a $bb$.
- Run tally $(V, pf) \leftarrow \text{Tally}(sk, nc, bb, \{pd_1, \ldots, pd_n\}, \kappa)$.
- Call the attacker $A$ with input $V$ and $pf$. Await a guess $h' \in \{0,1\}$.
- If $h = h' \land \text{balanced}(bb, nc, B) \land 1 \leq nc \leq mc \land \|bb\| \leq mb$ then ACCEPT else REJECT.

**Definition**

An electronic election scheme with internal auth. $\Gamma_{\text{int}} = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify})$ satisfies Ballot-Secrecy-Int

iff for each ppt attacker $A$ the advantage

$$\text{adv}^{\text{Bal-Sec-Int}}(A) = |\text{prob } (G^{\text{Bal-Sec-Int}}(A) = \text{ACCEPT}) - \frac{1}{2}|$$

is at most $\text{negl}(\kappa)$. 
Security Aspects

- Ballot secrecy
- Election verifiability
  - Individual verifiability
  - Universal verifiability
- Eligibility verifiability
External Individual Verifiability Game

$G^{IV-Ext}$

- Call the attacker $A$ with input $1^\kappa$. Await $pk$, $nc$, $v$, $v'$. 
- Run vote algorithm for $v$ and $v'$:
  - $b \leftarrow \text{Vote}(pk, nc, v, \kappa)$
  - $b' \leftarrow \text{Vote}(pk, nc, v', \kappa)$
- If $b = b'$ and $b \neq \perp$ and $b' \neq \perp$ then ACCEPT
  else REJECT.

Definition

An electronic election scheme with external auth.
$\Gamma^\text{Ext}_v = (\text{Setup}, \text{Vote}, \text{Tally}, \text{Verify})$

satisfies IV-Ext

iff

for each ppt attacker $A$ the advantage

$\text{adv}^{IV-Ext}(A) = |\text{prob}(G^{IV-Ext}(A) = \text{ACCEPT})|$ is at most $\text{negl}(\kappa)$. 

---

16
Internal Individual Verifiability Game

\( G_{\text{IV-Int}} \)

- Call the attacker A with input 1\(^\kappa\). Await \( pk \) and \( nv \).

- for 1 ≤ i ≤ \( nv \) do
  \[(pd_i, d_i) \leftarrow \text{Register}(pk, \kappa).\]

- Let \( L \leftarrow \{pd_1, \ldots, pd_{nv}\} \) and Crypt \( \leftarrow \emptyset \).

- Prepare oracle \( O^{\text{IV}} \). When called with \( i \in \{1, \ldots, nv\} \), adds \( d_i \) to Crypt and returns \( d_i \).

- Call the attacker A with \( L \) and \( O^{\text{IV}} \). Await \( nc, v, v', i, j \).

- Run vote algorithm for \( v \) and \( v' \):
  \[ b \leftarrow \text{Vote}(d_i, pk, nc, v, \kappa) \]
  \[ b' \leftarrow \text{Vote}(d_j, pk, nc, v', \kappa) \]

- If \( b = b' \land b \neq \bot \land b' \neq \bot \land i \neq j \land d_i \in \text{Crypt} \land d_j \notin \text{Crypt} \) then ACCEPT else REJECT.

Definition

An electronic election scheme with internal auth.
\( \Gamma_{\text{Int}} = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \)
satisfies IV-Int
iff
for each ppt attacker A the advantage
\[ \text{adv}^{\text{IV-Int}}(A) = |\text{prob} (G^{\text{IV-Int}}(A) = \text{ACCEPT})| \]
is at most \( \text{negl}(\kappa) \).
Security Aspects

- Ballot secrecy
- Election verifiability
  - Individual verifiability
  - Universal verifiability
- Eligibility verifiability
Algorithm Verify is required to accept iff the election outcome is correct.

- The outcome vector length must be $nc$.
- Component $\beta$ of Tally outcome vector equals $\ell$ iff there exist $\ell$ unique ballots on the bulletin board that are votes for candidate $\beta$.
- The output represents the choices used to construct the recorded ballots.
Algorithm Verify is required to accept iff the election outcome is correct.

Injectivity

Ballots interpreted only for one candidate.

(v≠v' => b≠b')
Algorithm Verify is required to accept iff the election outcome is correct.

- **Injectivity**: Ballots interpreted only for one candidate.
- **Completeness**: Tally produces election outcomes that will be accepted by Verify.

\[
\Pr[|bb| \leq mb \land nc \leq mc \implies \text{Verify}()=1] > 1-\text{negl}()
\]
Algorithm Verify is required to accept iff *the election outcome is correct*.

- **Injectivity**: Ballots interpreted only for one candidate.
- **Completeness**: **Tally** produces election outcomes that will be accepted by **Verify**.
- **Soundness**: The probability to conduct a scenario where **Verify** accepts although the election outcome is not correct is negligible.

\[
\Pr[V^* \neq V \Rightarrow \text{Verify}(V^*) = 1] \leq \text{negl}()
\]
\( \Gamma_{\text{Ext/Int}} = (\text{Setup}, <\text{Register}>, \text{Vote}, \text{Tally}, \text{Verify}) \) satisfies Universal Verifiability (UV-Ext/Int) if Injectivity, Completeness and Soundness are satisfied.
Security Aspects

- Ballot secrecy
- Election verifiability
  - Individual verifiability
  - Universal verifiability
- Eligibility verifiability
Eligibility Verifiability Game \( G^{EV-Int} \)

- Call the attacker \( A \) with input \( 1^k \). Await \( pk \) and \( nv \).
- for \( 1 \leq i \leq nv \) do
  - \((pd_i, d_i) \leftarrow \text{Register}(pk, k)\).
- Let \( L \leftarrow \{pd_1, \ldots, pd_{nv}\} \), \( \text{Crpt} \leftarrow \emptyset \), and \( \text{Rvld} \leftarrow \emptyset \).
- Prepare oracle \( O^{EV} \). When called with \( i, v, nc \); computes \( b \leftarrow \text{Vote}(d_i, pk, nc, v, k) \), adds \( b \) to \( \text{Rvld} \) and outputs \( b \).
- Prepare oracle \( O^{IV} \). When called with \( i \in \{1, \ldots, nv\} \), adds \( d_i \) to \( \text{Crpt} \) and returns \( d_i \).
- Call the attacker \( A \) with \( L, O^{EV} \) and \( O^{IV} \). Await \( nc, v, i, b \).
- If \( b \neq \perp \land b \notin \text{Rvld} \land d_i \notin \text{Crpt} \land \exists r: b = \text{Vote}(d_i, pk, nc, v, k; r) \) then \( \text{ACCEPT} \) else \( \text{REJECT} \).

### Definition

An electronic election scheme with internal auth. \( \Gamma_{\text{int}} = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \) satisfies \( EV-Int \) iff for each ppt attacker \( A \) the advantage

\[ \text{adv}^{EV-Int}(A) = |\text{prob } (G^{EV-Int}(A) = \text{ACCEPT})| \]

is at most \( \text{negl}(k) \).
Authentication with Weaker Trust Assumptions for Voting Systems*

(*)

Elizabeth A. Quaglia and Ben Smyth (2018)
Ext2Int

• $\Gamma_{\text{Ext}} \rightarrow \Gamma_{\text{Int}}$
  +digital signature
  + NIPS

• Relation $R(\Gamma, \Omega)$ such that
  $((pk, b, \sigma, nc, \kappa), (v, r, d, r')) \in R(\Gamma, \Omega)$
  $\iff b = \text{Vote}(pk, nc, v, \kappa; r) \land \sigma = \text{Sign}_\Omega(d, b; r')$

• $FS(\Sigma, H) = (\text{Prove}_\Sigma, \text{Verify}_\Sigma)$

• $\Omega = (\text{Gen}_\Omega, \text{Sign}_\Omega, \text{Verify}_\Omega)$

• Ext2Int($\Gamma, \Omega, \Sigma, H$)
  where
  $\Gamma$ : Underlying election scheme
  $\Omega$ : Signature Scheme
  $\Sigma$ : Sigma Protocol for $R$
  $H$ : Hash Function

Construction

Ext2Int($\Gamma, \Omega, \Sigma, H$) = (Setup, Register, Vote, Tally, Verify)
  such that:

Setup($\kappa$): $(pk, sk, mb, mc) \leftarrow \text{Setup}_\Gamma(\kappa)$

Register($pk, \kappa$): $(pd, (pd, d)) \leftarrow \text{Gen}_\Omega(pk)$

Vote($d', pk, nc, v, \kappa$): if parse($d'$) = (pd, d) fails then $\bot$ else
  pick $r, r'$ at random and compute:
  $b \leftarrow \text{Vote}_\Gamma(pk, nc, v, \kappa; r)$
  $\sigma \leftarrow \text{Sign}_\Omega(d, b; r')$
  $\tau \leftarrow \text{Prove}_\Sigma((pk, b, \sigma, nc, \kappa), (v, r, d, r'), \kappa)$
  and outputs $(pd, b, \sigma, \tau)$.

Tally($sk, nc, bb, L, \kappa$): $(V, pf) \leftarrow \text{Tally}_\Gamma(sk, \text{auth}(bb, L), nc, \kappa)$

Verify($pk, nc, bb, L, V, pf, \kappa$): $s \leftarrow \text{Verify}_\Gamma(pk, \text{auth}(bb, L), nc, V, pf, \kappa)$
Ext2Int

auth(bb, L) =
\{b | (pd, b, σ, τ) ∈ bb ∧
Verify_Ω(pd, b, σ) = 1 ∧
Verify_Σ((pk, b, nc, κ), τ, κ) = 1 ∧
pd ∈ L ∧
(pd, b', σ', τ') ∉ bb \{(pd, b, σ, τ)} ∧
Verify_Ω(pd, b', σ') = 1\}.

OR

One cannot vote more than once. (Vote once or never)

Ω : Signature Scheme
Σ : Sigma Protocol for R
H : Hash Function

Construction

Ext2Int(Γ, Ω, Σ, H) = (Setup, Register, Vote, Tally, Verify) such that:

Setup(κ): (pk, sk, mb, mc) ← Setup_Γ(κ)

Register(pk, κ): (pd, (pd, d)) ← Gen_Ω(pk)

Vote(d', pk, nc, v, κ): if parse(d') = (pd, d) fails then ⊥ else
pick r, r' at random computes:
b ← Vote_Γ(pk, nc, v, κ; r)
σ ← Sign_Ω(d, b; r')
Prove_Σ((pk, b, nc, κ), (v, r, d, r'), κ)
and outputs (pd, b, σ, τ).

Tally(sk, nc, bb, L, v, pf, κ): (v, pf) ← Tally_Γ(sk, auth(bb, L), nc, κ)

Verify(pk, nc, bb, L, v, pf, κ): s ← Verify_Γ(pk, auth(bb, L), nc, v, pf, κ)
Lemma:

Let $\Gamma$ be an election scheme with external authentication, $\Omega$ be a digital signature scheme, $\Sigma$ be a sigma protocol for relation $R(\Gamma, \Omega)$, and $H$ be a random oracle. 

If $\Omega$ satisfies strong unforgeability, then $\text{Ext2Int}(\Gamma, \Omega, \Sigma, H)$ is an election scheme with internal authentication.
Security of Ext2Int

- Let $\Gamma$ be an election scheme with external authentication, $\Omega$ be a digital signature scheme, $\Sigma$ be a sigma protocol for relation $R(\Gamma, \Omega)$, and $H$ be a random oracle.

  If
  $\Gamma$ satisfies $\text{Ballot-Secrecy-Ext}$, $\Sigma$ satisfies $\text{special soundness}$ and $\text{special honest verifier zero-knowledge}$, and $\Omega$ satisfies $\text{strong unforgeability}$

  Then
  Election scheme with internal authentication $\text{Ext2Int}(\Gamma, \Omega, \Sigma, H)$ satisfies $\text{Ballot-Secrecy-Int}$.

  Pf. Sketch: ...
Security of Ext2Int

- Let $\Gamma$ be an election scheme with external authentication, $\Omega$ be a digital signature scheme, $\Sigma$ be a sigma protocol for relation $R(\Gamma, \Omega)$, and $H$ be a random oracle.

If $\Omega$ satisfies strong unforgeability, $\Sigma$ satisfies special soundness and special honest verifier zero-knowledge, and $\Gamma$ satisfies $UV$-Ext Then
Election scheme with internal authentication $Ext2Int(\Gamma; \Omega; \Sigma; H)$ satisfies IV-Int, EV-Int, and UV-Int.

Pf. Sketch: ...