Remote Electronic Voting can be Efficient, Verifiable and Coercion-Resistant

Roberto Araújo, Amira Barki, Solenn Brunet and Jacques Traoré

1st Workshop on Advances in Secure Electronic Voting Schemes – VOTING'16
February 26th, 2016

orange™

Content

1. Previous Work
2. Building Blocks
3. Our Electronic Voting Scheme
4. Conclusion

Previous Work
(Juel, Catalano and Jakobsson, WPES 2005)

- JCJ formally defined the property of coercion-resistance, by considering possible attacks:
  - constrain a voter to cast given or random votes
  - force her to reveal her private data
  - vote on her behalf
  - force her to abstain

- Main idea: a coercer must be unable to distinguish a fake credential from a valid one.

⇒ for N ballots, the tallying complexity is in $\mathcal{O}(N^2)$

Motivations

	Linear complexity	Multiple elections	Practical for real polls	Completely anonymous
AFT07	✓	✗	✓	✓
AT13	✓	✓	✗	✓
CH11	✓	✓	✓	✗
SKHS11	✓	✓	✓	✗

Building Blocks

- Designated Verifier Proof (DVP) which cannot be transferred:

  Only the designated verifier can be convinced by this proof

- Non-Interactive Zero-Knowledge Proof of Knowledge (NIZKP):

  Enable a prover to convince a verifier that he knows some secret

- ElGamal Cryptosystem

- Algebraic MAC Scheme

- Sequential Aggregate MAC Scheme

ElGamal Cryptosystem

- Given $\mathbb{G} = \langle g \rangle$ cyclic group of prime order p
  - private key x, public key $pk = g^x$
  - encryption of m: $E_{pk}[m] = (g^r, mh^r)$
  - decryption of $E_{pk}[m]$: $mh^r(g^r)^{-x}$
- Properties:
  - multiplicatively homomorphic: $E_{pk}[m_1] \times E_{pk}[m_2] = E_{pk}[m_1 \times m_2]$
  - distribution of the private key (i.e. the decryption)
  - comparison of two ciphertexts via Plaintext Equivalence Test (PET):

    $PET\left(E_{pk}[m_1], E_{pk}[m_2]\right) = 1$ if $m_1 = m_2$ and 0 otherwise
  - easy re-encryption:

    $E_{pk}[m] = (g^r, mh^r)$ can be transformed in $E_{pk}[m]' = (g^{r+r'}, mh^{r+r'})$

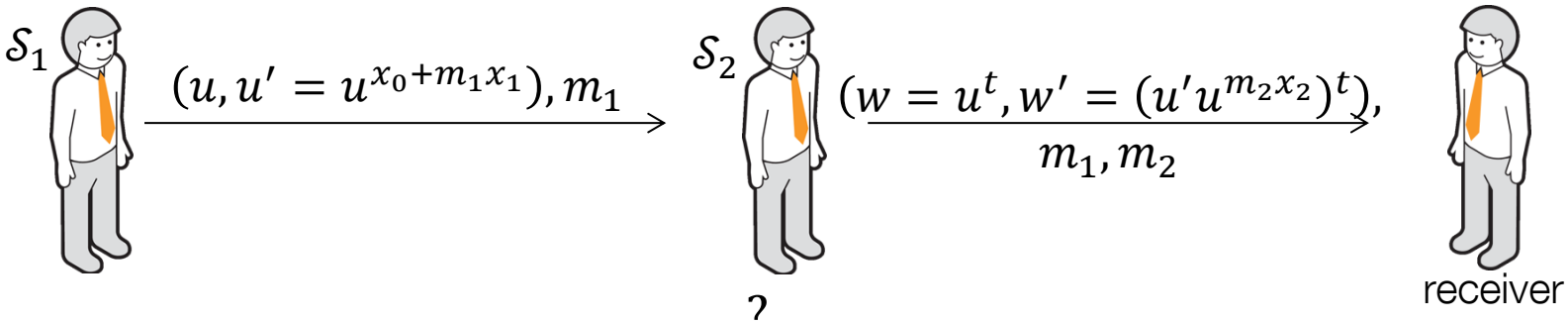
Algebraic MAC Scheme
(Chase, Meiklejohn, Zaverucha, ACM CCS2014)

- Setup(1^k): Generate $pp = (\mathbb{G}, p, g, h)$ such that
  - $\mathbb{G}$ cylic group of prime order p, where DDH is hard
  - g, h two of its generators
- KeyGen(pp):
  - secret key $sk = (x_0, x_1, x_2)$
  - optionally, the public parameters $(C_{x_0} = g^{x_0}h^x, X_1 = h^{x_1}, X_2 = h^{x_2})$
- MAC(sk, m_1, m_2):
  - choose u randomly
  - generate $\sigma = (u, u')$ where $u' = u^{x_0 + m_1 x_1 + m_2 x_2}$
- Verify(sk, m_1, m_2, σ): $u \neq 1$ and $u^{x_0 + m_1 x_1 + m_2 x_2} \stackrel{?}{=} u'$

Deciding whether $(m, u, u' = u^{x_0 + m x_1})$ is a valid MAC on m is equivalent to the DDH problem.

Our Sequential Aggregate MAC Scheme

- Setup: $pp = (\mathbb{G}, p, g, h)$
  - $sk_1 = (x_0, x_1)$, secret key of the first signer $\mathcal{S}_1$
  - $sk_2 = x_2$, secret key of the second signer $\mathcal{S}_2$
  - $C_{x_0} = g^{x_0}h^x, X_1 = h^{x_1}, X_2 = h^{x_2}$, associated public parameters
- Computation of MAC on m_1 by $\mathcal{S}_1$ and m_2 by $\mathcal{S}_2$:



- Verification: w ≠ 1 and $w' \stackrel{?}{=} w^{x_0+m_1x_1+m_2x_2}$

existentially unforgeable

Our eVote Scheme

1. Setup
2. Registration
3. Voting
4. Tallying

voters

Receive credential in order to cast a vote

registration authorities

Issue credentials in a distributed manner during the registration step

coercers

Force voters to make a particular vote and try to verify it

tallying authorities

Jointly manage the tallying phase

Security Model

- Registration occurs through an untappable channel
  ⇒ no adversaries at this step
- Votes may be posted anonymously
- Bulletin Board is universally accessible
- Attacker may:
  - access to all public information
  - corrupt a subpart of the election authorities
  - coerce voters: requests secrets, forces a particular vote…

Voters trust their voting client.

Set-Up

- Set-Up:
  - g, h, o generators of a cyclic group $\mathbb{G}$ of prime order p
  - registrars $\mathcal{R}$: share $sk = (x_0, x_1)$, $pk = (C_{x_0} = g^{x_0}h^x, X_1 = h^{x_1})$
  - talliers $\mathcal{T}$: share sk and an ElGamal keypair $(T, \hat{T})$
- Registration:
  - credential (s, u, u'):
    - s and u chosen randomly by $\mathcal{R}$
    - $u' = u^{x_0 + sx_1}$ computed by $\mathcal{R}$
  - in case of coercion, fake credential: (s', u, u') (DDH assumption)

Registration

- $\mathcal{R}$ jointly compute $(u, u' = u^{x_0 + s x_1})$ with s, u cooperatively selected and prove its validity through a DVP:

$(s, u, u'), \mathrm{DVP}$

- If a coercer asks to her credential, she can send a fake one:

(s', u, u')

The DVP can only convince the designated voter!

More about our Ballot

- Credential: (s, u, u') where $u' = u^{x_0 + s x_1}$

- Ballot: $\langle E_T[v], w, w', E_T[w^s], o^s, P \rangle$
  - (w, w') is a randomized credential s.t. $w = u^l$ and $w' = (u')^l$
  - P is a pair of NIZKPs of validity:
    - $E_T[v]$ is an encryption of a valid vote
    - the voter knows:
      - the plaintext of $E_T[w^s]$
      - the secret s, common both to $E_T[w^s]$ and o^s

Voting (first election)

- Vote under coercion:

$$\langle E_T[a], w, w', E_T[w^{s\prime}], o^{s\prime}, P \rangle \longrightarrow$$

- Revote:

$$\langle E_T[b], w, w', E_T[w^{s}], o^{s}, P \rangle \longrightarrow$$

Bulletin Board
$\langle \dots \rangle$
$\langle E_T[a], w, w', E_T[w^{s\prime}], o^{s\prime}, P \rangle$
$\langle \dots \rangle$
$\langle \dots \rangle$
$\langle \dots \rangle$
$\langle \dots \rangle$
$\langle E_T[b], w, w', E_T[w^{s}], o^{s}, P \rangle$
$\langle \dots \rangle$
$\langle \dots \rangle$

Tallying Phase [1/5]

1. Discard ballots with invalid proofs

Bulletin Board (offline)
$\langle E_T[b], w_1, w_1', E_T[{w_1}^r], o^r, P\rangle$
$\langle E_T[b], w_2, w_2', E_T[{w_2}^s], o^s, P\rangle$
$\langle E_T[a], w_3, w_3', E_T[{w_3}^t], o^t, P\rangle$
$\langle E_T[b], w_4, w_4', E_T[{w_4}^{s'}], o^{s'}, P\rangle$
~~$\langle E_T[a], z_1, z_1', E_T[{z_1}^r], o^{r'}, P\rangle$~~
$\langle E_T[a], z_2, {z_2}', E_T[{z_2}^s], o^s, P\rangle$

Tallying Phase [2/5]

2. Remove duplicates votes
   ⇒ ballots published using the same secret s

Bulletin Board (offline)
$\langle E_T[b], w_1, w_1', E_T[{w_1}^r], o^r \rangle$
~~$\langle E_T[b], w_2, w_2', E_T[{w_2}^s], o^s \rangle$~~
$\langle E_T[a], w_3, w_3', E_T[{w_3}^t], o^t \rangle$
$\langle E_T[b], w_4, w_4', E_T[{w_4}^{s'}], o^{s'} \rangle$
$\langle E_T[a], z_2, {z_2}', E_T[{z_2}^s], o^s \rangle$

Possible policy: keep the last one

Tallying Phase [3/5]

3. Reconstruction and checking of credentials

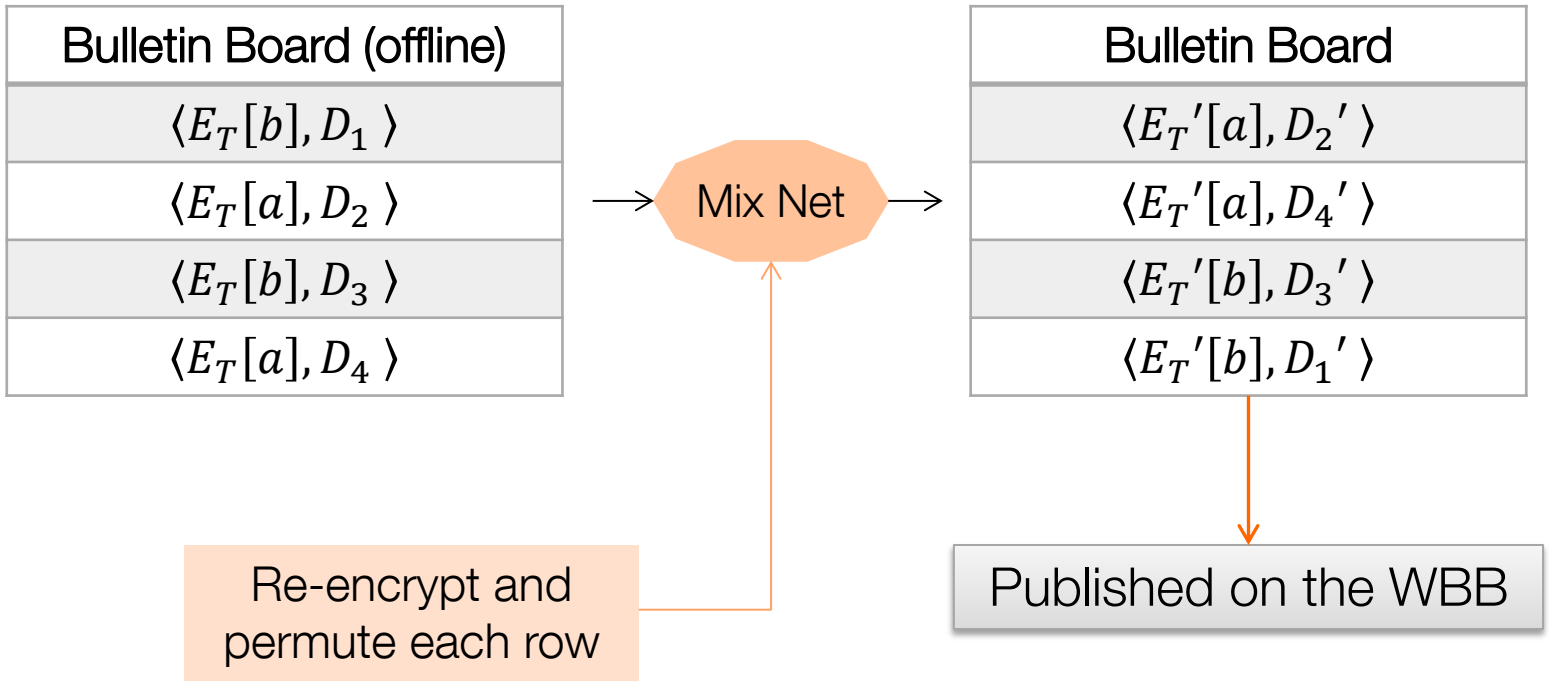
Bulletin Board (offline)
$\langle E_T[b], w_1, w_1', E_T[{w_1}^r] \rangle$
$\langle E_T[a], w_3, w_3', E_T[{w_3}^t] \rangle$
$\langle E_T[b], w_4, w_4', E_T[{w_4}^{s'}] \rangle$
$\langle E_T[a], z_2, {z_2}', E_T[{z_2}^s] \rangle$

1. The authorities cooperatively compute $E_T[w]$, $E_T[w^{x_0}]$, $E_T[w^s]$, $E_T[(w^s)^{x_1}]$ in order to obtain:
   $\mathrm{E_T}[w^{x_0}] \times E_T[w^{sx_1}] = E_T[w^{x_0+sx_1}]$

2. Then, power $C = E_T[w^{x_0+sx_1}]/w'$ to a fresh random α for the PET:
   $D = C^{\alpha}$ should be equal to $E_T[1]$

Tallying Phase [4/5]

4. Mix the ballots



Tallying Phase [5/5]

5. Identify valid votes by jointly decrypting D_i:
   - If the plaintext is equal to 1, the ballot is valid and thus decrypted

Bulletin Board (offline)
$\langle E_T'[a], D_2' \rangle$
$\langle E_T'[a], D_4' \rangle$
~~$\langle E_T'[b], D_3' \rangle$~~
$\langle E_T'[b], D_1' \rangle$

Distributed decryption →

Results
a
a
b

Multiple Elections and Credentials Revocation

- For a second election, registrars $\mathcal{R}$:
  - jointly generate an election identifier e_I
  - compute a new pair of keys $(x_2, X_2 = h^{x_2})$, shared with the talliers $\mathcal{T}$
  - publish an updated credential (w, w') for each eligible voter:

    $(u, u' = u^{x_0 + s x_1})$ associated to the secret s

    becomes $(u^t, (u' u^{e_I x_2})^t) = (w, w' = w^{x_0 + s x_1 + e_I x_2})$

⇒ voting and tallying phases are unchanged

Security

- A voter cannot prove her vote:

  false and real credentials are indistinguishable
- No forced abstention:

  votes cast using anonymous channel
- No forced randomization and impersonation:

  voter can use fake credential for false vote and cast another one later
- Resistance to shoulder-surfing:

  Re-vote policy: only the last might count

Our voting scheme satisfies:
- eligibility requirement through security properties of the MAC,
- coercion-resistance property under DDH assumption.

Conclusion

- a Sequential Aggregate MAC Scheme existentially unforgeable

- Our new voting scheme for remote elections is:
  - publicly verifiable
  - efficient (linear time complexity)
  - coercion-resistant
  - allowing multiple elections and credentials revocation

Thank you