University of Fribourg

Bern University of Applied Sciences

Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting

Oliver Spycher

Bregenz, July 12th, 2012

Outline

Challenge

Underlying scheme - JCJ 2005

New scheme

Assessment and Conclusion

Outline

Verifiability vs. Coercion-Resistance

A voting protocol is coercion-resistant, if the adversary cannot tell whether a subject complied or applied a counter-strategy.

Verifiability despite

1. privacy
2. receipt-freeness
3. coercion-resistance

- → JCJ proposal in 2005
- → how can we render tallying efficient?

The JCJ model

Voters

- honest voters cast their vote
- corrupted voters follow the coercer's instructions
- the voter under coercion chooses compliance or counter-strategy (hand out fake voting credential)

Authorities (registrars, talliers)

- verifiability: no trusted authorities
- coercion-resistance: trustworthy registration
- coercion-resistance: at least 1 trusted registar and tallier each

$\rightarrow$ *Assume adversarial uncertainty regarding Σ (result) and Γ (number of votes cast with fake credential)*

Degree of Coercion-Resistance δ

δ relates to the voter's average expected loss when applying the counter strategy.

Example (taken from Kuesters 2009)

- 2 candidates c_1, c_2, 2000 honest participating voters
- $P = (void = 0.3, c_1 = 0.35, c_2 = 0.35)$ probability distribution of Σ
- Coercer offers 50.–

- $\delta = 0.021$, assuming voter wants c_1
- $E(money|complying) - E(money|notcomplying) = \delta \times 50.-$
- **In average the voter will loose 1.05** Should he comply?

Contribution of the proposed scheme

Schemes with a parameter β to reduce tallying time of JCJ

- Big β implies small δ
- Meaningful computation time still scales over a parameter β

In the new scheme

1. β is small for given δ
2. no meaningful computation time scales over β

Outline

Primitives

Primitives used in JCJ and the new scheme

- Multiparty ElGamal Cryptosystem (homomorphic, IND-CPA)
- Re-encryption Mix-Nets
- (Designated verifier) Non-interactive Zero-Knowledge Proofs
- Anonymous channel
- Authenticated, untappable channel
- Plaintext equality test (PET) $\rightarrow$ explained later

Setup in JCJ

Registration:

1. Voting credential σ obtained from registrars
2. Voter ID associated with encrypted credential $\mathrm{E}_e(\sigma, \alpha_R)$ on Public Bulletin Board (PB)

$\rightarrow$ Only the collusion of all registrars or talliers can elicit σ
$\rightarrow$ Voter can lie about his credential (make up a σ).

Casting votes

Voter posts to PB:

1. $\mathrm{E}_e(\sigma, \alpha_A)$
2. $\mathrm{E}_e(v, \alpha_B)$ (encrypted vote)
3. Proofs of knowledge of α_A, α_B and v is a valid vote

$\rightarrow$ How do we perform tallying based on $\mathrm{E}_e(\sigma, \alpha_A)$?

PET - Plaintext Equivalence Test

Given $\mathrm{E}_e(p_1)$, $\mathrm{E}_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

1. Compute $\mathrm{E}_e(\frac{p_1}{p_2}) = \frac{\mathrm{E}_e(p_1)}{\mathrm{E}_e(p_2)}$
2. Compute $\mathrm{E}_e((\frac{p_1}{p_2})^z) = \mathrm{E}_e^z(\frac{p_1}{p_2})$, $z \in_R \mathbb{Z}_q$, fresh unknown
3. Compute $(\frac{p_1}{p_2})^z = \mathrm{Dec}_d(\mathrm{E}_e((\frac{p_1}{p_2})^z))$
4. Return *true* if $(\frac{p_1}{p_2})^z = 1$, *false* otherwise.

Tallying: Talliers perform the following steps

Check Proofs

Remove duplicates

- Compare all $< \mathrm{E}_e(\sigma, \alpha_A) >$ with eachother using PET

Authorize votes

- Apply mix-net on all $< \mathrm{E}_e(\sigma, \alpha_A), \mathrm{E}_e(v, \alpha_B) >$
- Apply mix-net on all $< \mathrm{E}_e(\sigma, \alpha_R) >$
- Compare all $< \mathrm{E}_e(\sigma, \alpha_A) >$ with all $< \mathrm{E}_e(\sigma, \alpha_R) >$ using PET

Decrypt and count

Outline

Setup

Pre-registration

1. Registrars prepare $< \sigma, i >$ and publish $< \mathrm{E}_e(\sigma, \alpha_R), \mathrm{E}_e(i) >$
2. They apply a mix-net on all $< \mathrm{E}_e(i) >$ and talliers decrypt the output

$\rightarrow$ There are $\beta \times N_+$ credentials in the credential-pool.

Registration

1. Voting credential (σ, i) obtained from registrars
2. Voter ID associated with encrypted credential components $(\mathrm{E}_e(\sigma, \alpha_R), \mathrm{E}_e(i))$

$\rightarrow$ Voter can lie about his credential (make up a σ and choose a random valid i).

Casting votes

To cast a vote - voter posts to PB:

1. $\mathrm{E}_e(\sigma, \alpha_A)$
2. i
3. $\mathrm{E}_e(v, \alpha_B)$ (encrypted vote)
4. Proofs of knowledge of α_A, α_B and v is a valid vote

$\rightarrow$ What would be a coercion strategy?
$\rightarrow$ How do we authorize votes based on $\mathrm{E}_e(\sigma, \alpha_A)$ and i?

M-PET - Modified Plaintext Equivalence Test

Given $\mathrm{E}_e(p_1)$, $\mathrm{E}_e(p_2)$, decide whether $p_1 = p_2$, without revealing plaintexts.

Algorithm

1. Compute $\mathrm{E}_e(p_1^z) = \mathrm{E}_e(p_1)^z$, $\mathrm{E}_e(p_2^z) = \mathrm{E}_e(p_2)^z$
2. Decrypt both
3. Return *true* if $p_1^z = p_2^z$, *false* otherwise.

$\rightarrow$ This reveals nothing about plaintexts, if the logarithm of one plaintext is unknown in the base of the other

Tallying: Talliers perform the following (1)

Check Proofs

Remove duplicates

- Compare all $< \mathrm{E}_e(\sigma, \alpha_A) >$ with eachother using M-PET

Authorize votes (1)

- Finalise post-registration (1): Apply mixnet on credentials of the credential-pool $< \mathrm{E}_e(\sigma, \alpha_R), \mathrm{E}_e(i) >$, decrypt i-component
- Apply mix-net on all $< \mathrm{E}_e(\sigma, \alpha_R), \mathrm{E}_e(\sigma, \alpha_A), \mathrm{E}_e(v, \alpha_B) >$ (i is used to form these tuples)
- Compare $\mathrm{E}_e(\sigma, \alpha_R)$ with $\mathrm{E}_e(\sigma, \alpha_A)$ for each tuple using PET

Tallying: Talliers perform the following (2)

Authorize votes (2)

- Finalise post-registration (2): Apply mixnet on the σ-components of the assigned credentials of the credential-pool $< \mathrm{E}_e(\sigma, \alpha_R) >$
- Compare all remaining $< \mathrm{E}_e(\sigma, \alpha_A) >$ with all $< \mathrm{E}_e(\sigma, \alpha_R) >$ using M-PET

Decrypt and count

Outline

Challenge

Underlying scheme - JCJ 2005

New scheme

Assessment and Conclusion

Conclusion

Verifiability

- As in JCJ

Coercion-resistance

- $\delta < \frac{1}{\beta}$ can be shown with JCJ attacker and JCJ trust-assumptions
- $\delta < \frac{2}{\beta}$ can be shown when assuming multi-coercion
- what about if...

Efficiency

- Scales over β only at pre-registration and post-registration
- No-one is kept waiting...

Efficiency vs. Coercion-resistance

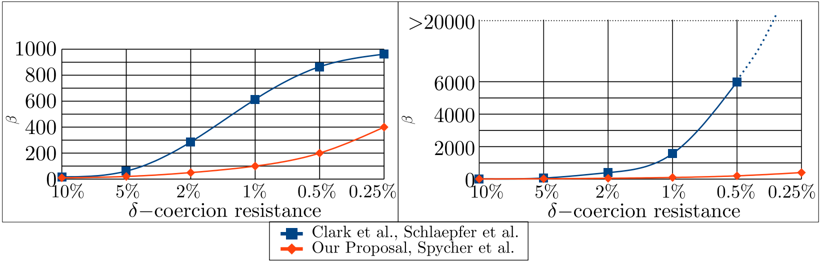

Figure: The two drawings show the parameter β in dependence of the degree of coercion-resistance δ. The diagram on the left shows the case for 1000 voters and 1000 votes on the voting board, the one on the right 100000 voters and 100000 votes on the voting board.

Thank You!

Questions / Remarks

e-voting.bfh.ch contacts, projects, events