

A Design Of Secure Preferential E-Voting

Kun Peng and Feng Bao

{dr.kun.peng}@gmail.com

Institute for Inforcomm Research (I²R), Singapore

Agenda

1. Preferential E-Voting
2. Coercion attack and coercion resistant
3. Italian attack
4. Existing solutions
5. The new preferential e-voting scheme
6. Conclusion

E-Voting

- ▶ Election with vote in electronic form.
- ▶ Votes are encrypted.
- ▶ The encrypted votes are collected through a digital communication network.
- ▶ The votes are tallied in electronic form by a computer system.
- ▶ The security properties of paper-based elections cannot be sacrificed.

Security Properties of E-Voting

- ▶ Correctness: all the valid votes are counted without being tampered with.
- ▶ Privacy: no information about any voter's choice in the election is revealed.
- ▶ Robustness: any abnormal situation can be detected and solved without revealing any vote.
- ▶ Flexibility: various election rules are supported.

Preferential Election

- ▶ In one-round election, it is unfair to just require that the candidate with the most votes wins.
- ▶ A candidate can hire other candidates to divert his opponent's votes.
- ▶ Multiple-round election is inconvenient and discourage voting.
- ▶ Preferential election is introduced: a vote includes a complete preferential order of all the candidates.

Course of Preferential Election

- ▶ The voters submit their complete votes in one round of communication.
- ▶ If a candidate obtains more than half of the first choices, it is the winner.
- ▶ Otherwise, the candidate with the fewest first choices is deleted and the second choices in the votes choosing him as the first choice become the first choices.
- ▶ The multi-round tallying continues until one candidate wins more than half of first choices.

Coercion Attack

- ▶ Coercion attack threatens fairness of elections.
- ▶ A candidate tries to coerce or buy over some voters to vote as he requires.
- ▶ The cheating candidate must be able to check whether a certain voter really votes as required.
- ▶ It is especially harmful to e-voting.

Coercion Resistance

- ▶ Any voter must be prevented from proving that he casts a certain vote.
- ▶ E-voting always publishes all the sealed votes for the sake of public verifiability.
- ▶ Two countermeasures: deniable encryption and re-encryption with untransferable zero knowledge proof of correctness by a third party.
- ▶ Either of them is enough for normal e-voting applications except preferential e-voting.

Italian Attack

- ▶ A special coercion attack against preferential e-voting.
- ▶ Among all the possible preferential combinations, some are rarely chosen.
- ▶ An attacker chooses a rare combination with himself as the first choice and coerces a voter to submit it.
- ▶ The attacker monitors the publicly verifiable tallying operation to see whether the special vote appears.

Current Situation

- ▶ Italian attack is effective with shuffling based election.
- ▶ Shuffling based e-voting is the default solution to preferential election.
- ▶ The existing homomorphic e-voting techniques cannot achieve security preferential election.
- ▶ Solution: secure homomorphic e-voting to handle preferential election.

The New Solution

- ▶ Applying homomorphic e-voting to preferential election.
- ▶ As the votes are tallied as a whole and no single vote is revealed, Italian attack cannot work.
- ▶ The key technique is how to adjust the votes after each round of tallying.
- ▶ The adjustment must be private and publicly verifiable.

Vote Matrix

$$\left(\begin{array}{cccc} c_{1,1} & c_{1,2} & \dots & c_{1,m} \\ c_{2,1} & c_{2,2} & \dots & c_{2,m} \\ & \dots & \dots & \\ c_{m,1} & c_{m,2} & \dots & c_{m,m} \end{array} \right)$$

where homomorphic encryption algorithm is employed.

- ▶ Rows: preferences
- ▶ Columns: candidates

Homomorphic Tallying

- ▶ Each voter has to prove that his vote is a permutation matrix.
- ▶ First choices for every candidate (the first row) are summed up exploiting homomorphism.
- ▶ If a candidate wins more than half of the first choices, he is the winner.
- ▶ Otherwise the encrypted votes must be adjusted.

Deleting the Loser

The column for the deleted candidate is deleted in every vote. A vote becomes

$$M = \left\{ \begin{array}{cccc} c_{1,1} & c_{1,2} & \dots & c_{1,t} \\ c_{2,1} & c_{2,2} & \dots & c_{2,t} \\ & \dots & \dots & \\ c_{m,1} & c_{m,2} & \dots & c_{m,t} \end{array} \right\}$$

which needs to be adjusted.

Adjustment 1

If $\sum_{j=1}^t D(c_{1,j}) = 1$, the vote does not choose the loser as the first choice, so the vote becomes

$$\left\{ \begin{array}{cccc} RE(c_{1,1}) & RE(c_{1,2}) & \dots & RE(c_{1,t}) \\ RE(c_{2,1}) & RE(c_{2,2}) & \dots & RE(c_{2,t}) \\ & \dots & \dots & \\ RE(c_{m,1}) & RE(c_{m,2}) & \dots & RE(c_{m,t}) \end{array} \right\}$$

Adjustment 2

If $\sum_{j=1}^t D(c_{1,j}) = 0$, the vote chooses the loser as the first choice, so the vote becomes

$$M' = \left\{ \begin{array}{cccc} RE(c_{2,1}) & RE(c_{2,2}) & \dots & RE(c_{2,t}) \\ RE(c_{3,1}) & RE(c_{3,2}) & \dots & RE(c_{3,t}) \\ & \dots & \dots & \\ RE(c_{m,1}) & RE(c_{m,2}) & \dots & RE(c_{m,t}) \\ RE(c_{1,1}) & RE(c_{1,2}) & \dots & RE(c_{1,t}) \end{array} \right\}$$

Adjustment 3: Implementation

M becomes $M_1 \otimes M_2 \otimes M'_1 \otimes M'_2$ where

$$M_1 = RE(M^{\times m_1})$$

$$M'_1 = RE(M'^{\times m'_1})$$

$$M_2 = RE(M^{\times m_2})$$

$$M'_2 = RE(M'^{\times m'_2})$$

- ▶ m_1, m_2 are random shares of $D(\prod_{j=1}^t c_{1,j})$.
- ▶ m'_1, m'_2 are random shares of $1 - D(\prod_{j=1}^t c_{1,j})$.

Special Operations with Matrix

$$M^{\times x} = \left\{ \begin{array}{cccc} m_{1,1}^x & m_{1,2}^x & m_{1,3}^x & \dots \\ m_{2,1}^x & m_{2,2}^x & \dots & \dots \\ m_{3,1}^x & \dots & \dots & \\ \dots & \dots & \dots & \end{array} \right\} \text{ where}$$

$$M = \left\{ \begin{array}{cccc} m_{1,1} & m_{1,2} & m_{1,3} & \dots \\ m_{2,1} & m_{2,2} & \dots & \dots \\ m_{3,1} & \dots & \dots & \\ \dots & \dots & \dots & \end{array} \right\}$$

Special Operations with Matrix

Cont

$$M_1 \otimes M_2 = \left\{ \begin{array}{cccc} m_{1,1}m'_{1,1} & m_{1,2}m'_{1,2} & m_{1,3}m'_{1,3} & \dots \\ m_{2,1}m'_{2,1} & m_{2,2}m'_{2,2} & \dots & \dots \\ m_{3,1}m'_{3,1} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{array} \right\}$$

Conclusion

- ▶ The secure e-voting scheme proposed in this paper is invulnerable against Italian attack in preferential e-voting.
- ▶ Efficiency of vote validity check and vote adjustment need improving.

Questions?