Anonymous Voting by 2-Round Public Discussion

A decentralized solution to the e-voting problem

Speaker: Feng Hao

Thales E-Security, Cambridge, UK

WISSEC '09

Acknowledgment

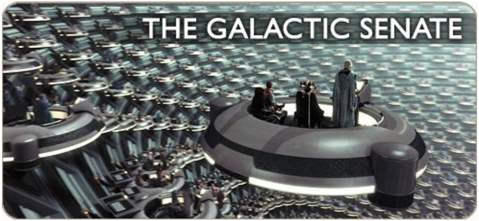
- Joint work with
  - Peter Ryan – Faculty of Science, University of Luxembourg
  - Piotr Zieliński – Google Inc, UK

- F. Hao, P. Ryan, P. Zieliński, "Anonymous Voting by 2-Round Public Discussion," to appear on *IET Information Security*, 2010.

Outline

1. Problem statement
2. Past solutions
3. New solution
4. Conclusion

A Crypto Puzzle



The chancellor is seeking re-election in the senate. Some delegates do not want to vote for him, but worry about the revenge. The dark-side force is strong; surveillance is everywhere. In addition, no trusted third parties exists. How to arrange a voting such that the voters' privacy will be best protected?

Constraints in the scenario

1. There are no private channels.
   - All communication is public and traceable to the sender.
2. There are no trusted third parties.
   - A TTP is someone who can break your security policy.

Kiayias-Yung solution

- Kiayias and Yung first proposed a solution in 2002.
- The protocol executes in 3 rounds.
- Each voter publishes $O(n)$ ephemeral public keys.
- And performs $O(n)$ public key operations.
- System complexity $O(n^2)$: too complex.

Groth's solution

- Groth improved Kiayias-Yung's solution in 2004.
- His solution trades round efficiency off system complexity.
- Its system complexity $O(n)$ vs Kiayias-Yung's $O(n^2)$.
- Its round efficiency $O(n)$ vs Kiayias-Yung's 3.
- Too many rounds.

Our solution - Open Vote Network

- Generalization of Anonymous Veto Network (SPW'06).
- Only two rounds.
- Linear system complexity.
- As secure as Kiayias-Yung and Groth's.
- But much more efficient than both.

The Open Vote Network protocol: 2-round Referenda

Round-1 Every participant P_i publishes g^{x_i} and a zero knowledge proof for x_i, and computes:

$$g^{y_i} = \frac{\prod_{j<i} g^{x_i}}{\prod_{j>i} g^{x_i}}$$

Round-2 Every participant publishes $g^{x_i y_i} \cdot g^{v_i}$ and a zero knowledge proof showing that v_i is one of $\{1,0\}$.

$$v_i = \begin{cases} 1 & \text{for ``yes''} \\ 0 & \text{for ``no''} \end{cases}$$

To tally, anyone can compute $\prod_i g^{x_i y_i} g^{v_i} = \prod_i g^{v_i} = g^{\sum_i v_i}$.

Cancellation formula - the magic

Proposition

For the x_i and y_i as defined in the protocol, $\sum_i x_i y_i = 0$.

Proof.

By definition $y_i = \sum_{j<i} x_j - \sum_{j>i} x_j$, hence

$$
\begin{aligned}
\sum_i x_i y_i &= \sum_i \sum_{j<i} x_i x_j - \sum_i \sum_{j>i} x_i x_j \\
&= \sum\sum_{j<i} x_i x_j - \sum\sum_{i<j} x_i x_j \\
&= \sum\sum_{j<i} x_i x_j - \sum\sum_{j<i} x_j x_i \\
&= 0.
\end{aligned}
$$

□

Cancellation formula - an example

Example

Assume $n = 4$.

$$\begin{aligned}\sum_i x_i y_i = \quad & \qquad\qquad\quad - x_1x_2 - x_1x_3 - x_1x_4 \\ & + x_2x_1 \qquad\quad - x_2x_3 - x_2x_4 \\ & + x_3x_1 + x_3x_2 \qquad\quad - x_3x_4 \\ & + x_4x_1 + x_4x_2 + x_4x_3 \qquad\qquad = 0.\end{aligned}$$

Security properties

1. **Maximum ballot secrecy**
   - Each cast ballot is indistinguishable from random.
2. **Self-tallying**
   - Anyone can tally the votes without external help.
3. **Dispute-freeness**
   - Anyone can verify all voters act according to the protocol.

Comparison

Protocols	Year	Round	Exp	KP for exp	KP for equality	KP for 1-of-k
Kiayias-Yung	2002	3	$2n+2$	$n+1$	n	1
Groth	2004	$n+1$	4	2	1	1
–	2009	2	2	1	0	1

- Our protocol requires only 2 rounds.
- One const public key operation per voter in each round.
- One const knowledge proof per voter in each round.
- Overall, the efficiency has been very close to the best possible.

Centralized vs decentralized

- Decentralized e-voting, e.g., Open Vote Network
  - No trusted parties
  - Maximum protection of the voters' privacy
  - However, weak against DoS attacks
  - Suitable for small-scale election like boardroom
- Centralized e-voting
  - More robust against DoS attacks
  - More scalable
  - However, involve trusted third parties
  - Suitable for large-scale election like countrywide

Conclusion

- Presented the Open Vote Network protocol.
- A decentralized solution to the e-voting problem.
- It requires only two rounds.
- Minimum computation load and bandwidth usage.
- Compared favorably to past solutions.
- Close to the best efficiency possible.