Boardroom Voting with Ballot Design Flexibility

Oksana Kulyk

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO SECURITY · USABILITY · SOCIETY

CASED Usable Security Lab Crypto Lab

Boardroom Voting - Concept

- Voters as the election authorities
- Relatively small total number of voters
- Lack of central trusted instance

TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

Boardroom Voting - Setting

- No more than 25 voters
- Portable devices (Android phones)
- Remote participation allowed
- Spontaneous elections: easy setup phase
- Flexible ballots

TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

Challenges

- Portable devices → network restrictions
  - protocols dealing with brief network shortages
  - protocols dealing with some participants going offline
- Portable devices → low computational power
  - most efficient protocols in general
  - most efficient protocols depending on ballot type
- No central trusted instance
  - non-trusted central instance for communications
  - protocols to ensure fault-tolerant communications

Boardroom Voting Stages

- PKI establishment (once for group of voters)
- Distributed key generation (once for group of voters)
- Ballot preparation (each election)
- Vote casting (each election)
- Vote anonymisation (each election)
- Verifiable distributed decryption (each election)

Preliminary Stages

- PKI establishment
  - Use existing corporate PKI, or
  - Run public keys exchange protocol
- Distributed key generation (each voter):
  - Distributively generate private key shares
  - Compute joint public key

TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

Ballot Preparation & Vote Casting

- Ballot preparation (initiator):
  - Broadcast ballot form and declared voting span
- Vote casting (each voter in turn):
  - Make a choice
  - Encrypt a chosen vote with joint public key
  - Broadcast the encrypted vote

TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

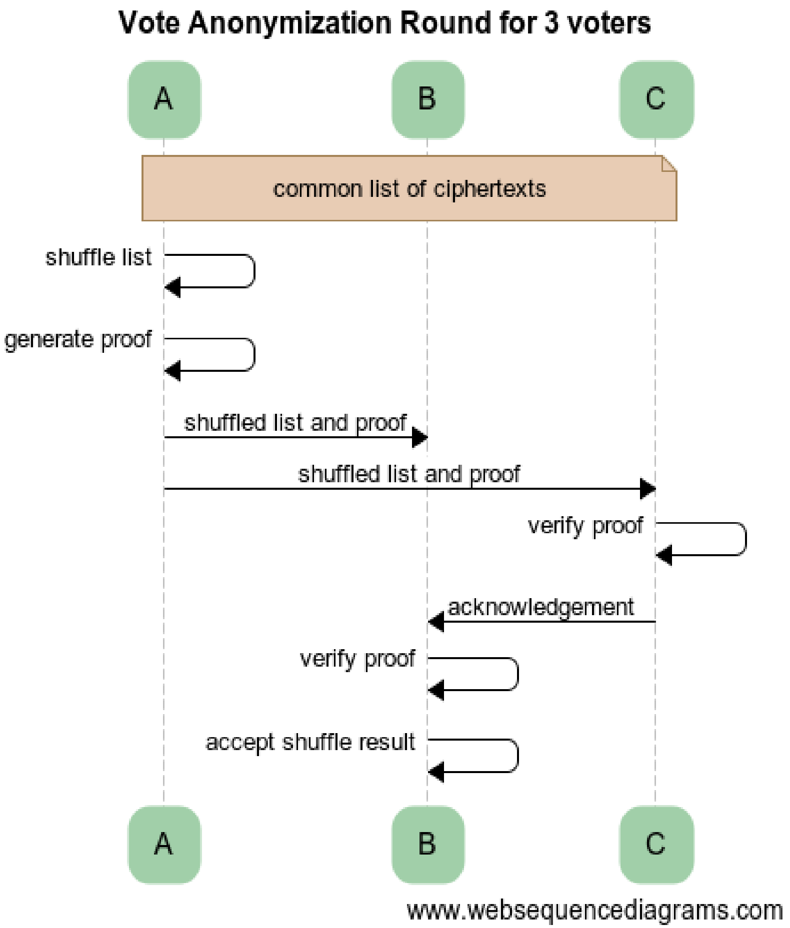
Vote anonymization

- Shuffling
  - Shuffle and permutate ciphertext list
  - Generate zero-knowledge proof of shuffle correctness
  - Broadcast the shuffled list and the proof
- Verification
  - Verify the proof of current shuffle
  - If verified, broadcast acknowledgement message
  - As next shuffler, if at least threshold acknowledgements received, take the result of current shuffle as input
  - Otherwise, take the previous list of ciphertexts as input

TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

Vote anonymization

➔Sequence example:



TECHNISCHE UNIVERSITÄT DARMSTADT
SECUSO SECURITY · USABILITY · SOCIETY

Verifiable distributed decryption

- Partially decrypt the ciphertexts using private key share
- Compute the zero-knowledge proofs of decryption correctness
- Broadcast partial decryptions and proofs
- Verify the proofs of other voters
- Reconstruct the votes from verified partial decryptions
- Display the results of voting

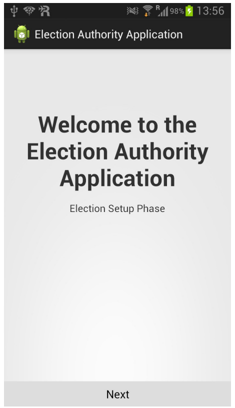
Boardroom Voting - Completed

- PKI establishment [Farb12]
- Distributed key generation [CGS97]
- Ballot preparation
- Vote casting
- Vote anonymisation
- Verifiable distributed decryption [CGS97]

Election Authority Application

- PKI establishment
- Distributed key generation
- Verifiable distributed decryption

→ **Offshot: Election Authority Application**



Boardroom Voting – Current Work

- PKI establishment [Farb12]
- Distributed key generation [CGS97]
- Ballot preparation
- Vote casting
- Vote anonymisation
- Verifiable distributed decryption [CGS97]

Boardroom Voting – Current Work

- Ballot preparation
  - ➔Different types of ballots
- Vote casting
  - Vote encoding according to ballot type
  - Vote encryption with jointly generated public key
  - Vote broadcasting to other voters
- Vote anonymisation
  - Mix net protocols
  - Homomorphic sum

Vote Anonymisation Methods

- Homomorphic sum
  - more efficient for simple ballots (-)
  - less suitable for more complex ballots (+)
- Mix net schemes
  - more complex (-)
  - more flexibility with regards to ballot type (+)

→ Decided for mix net, due to demands for ballot flexibility

Mix Net Evaluation Criteria

- Efficiency
  - Important to consider because of smartphone limitations
  - No more than total of 15 minutes for shuffle
- Security
  - No link between shuffled vote and voter's identity
  - Detection of the vote's replacement during shuffle
  - If threshold of voters is honest, no attacks with high success probability

Mix Net Evaluation Criteria

- Shuffling and reencrypting the El Gamal ciphertexts
  - ➔ Integration with other parts of protocol
- Robustness for threshold of honest mix nodes
  - ➔ Dealing with some voters misbehaving/being unavailable
- Open access
  - ➔ Legally allowed to implement in our project
- Adjustability for decentralized protocol
  - ➔ Central trusted instance not needed

Next steps

- Chose a mix net according to criteria mentioned
  - ➔ f. ex. consider [SK95], [AH01], [TW10], [BG11] etc.
- Implement and integrate all missing stages
- Integrate different protocols for various stages
  - ➔ dynamically select the best one for each specific election
- Design usable interfaces

References

- [CGS97] Cramer, Ronald, Rosario Gennaro, and Berry Schoenmakers. "A secure and optimally efficient multi-authority election scheme." European transactions on Telecommunications 8.5 (1997): 481-490.
- [BG12] Bayer, Stephanie, and Jens Groth. "Efficient zero-knowledge argument for correctness of a shuffle." Advances in Cryptology–EUROCRYPT 2012. Springer Berlin Heidelberg, 2012. 263-280.
- [AH01] Abe, Masayuki, and Fumitaka Hoshino. "Remarks on mix-network based on permutation networks." Public Key Cryptography. Springer Berlin Heidelberg, 2001.
- [Farb12] Farb, Michael, et al. SafeSlinger: Easy-to-Use and Secure Public-Key Exchange. Vol. 3. Technical Report of the CyLab, Carnegie Mellon University, 2012.
- [SK95] Sako, Kazue, and Joe Kilian. "Receipt-free mix-type voting scheme." Advances in Cryptology—EUROCRYPT’95. Springer Berlin Heidelberg, 1995.

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

References

- [TW10] Terelius, Björn, and Douglas Wikström. "Proofs of restricted shuffles." Progress in Cryptology–AFRICACRYPT 2010. Springer Berlin Heidelberg, 2010. 100-113.