Ad Hoc Voting on Mobile Devices

iCIS, Radboud University Nijmegen, The Netherlands

Manu Drijvers, Pedro Luz, Gergely Alpár and Wouter Lueks

Ad Hoc Voting

The security requirements of electronic voting schemes include integrity, voter authentication, and ballot secrecy. These represent a big challenge for ad hoc networks since it is easy to eavesdrop on connections or tamper with protocols by connecting extra devices wirelessly.

Kiayias and Yung define requirements for boardroom elections and propose a protocol that matches these requirements. However, their scheme becomes inefficient for elections with many candidates. Web-based implementations of electronic voting schemes like Helios, have the disavantage of requiring an external voting server to host the election.

We propose a solution that is efficient and does not require infrastructure.

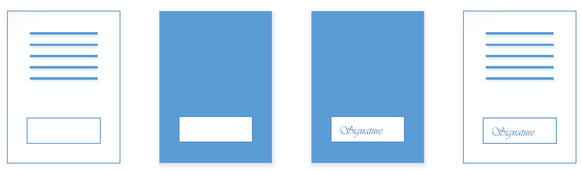
Security requirements:

- Only authorized voters can vote and at most once (*eligibility*)
- No one can determine what anyone else voted (*ballot secrecy*)
- No one can change anyone else's vote without being discovered (*integrity*)
- No one can duplicate anyone else's vote (*integrity*)
- Each voter can verify that his/her vote was counted (*verifiability*)

Building Blocks

Blind Signature

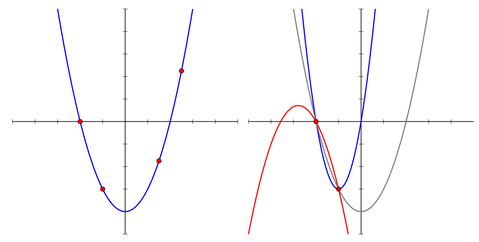
In a blind signature scheme the signer can sign a message without knowing its content. This allows us to decouple registration, where you are identifiable, from voting, where you want to be anonymous.



Example of a blind signature. The author of a document covers his document except the signature field. The signer places a signature without seeing the document. Finally the author removes the cover.

Secret Sharing

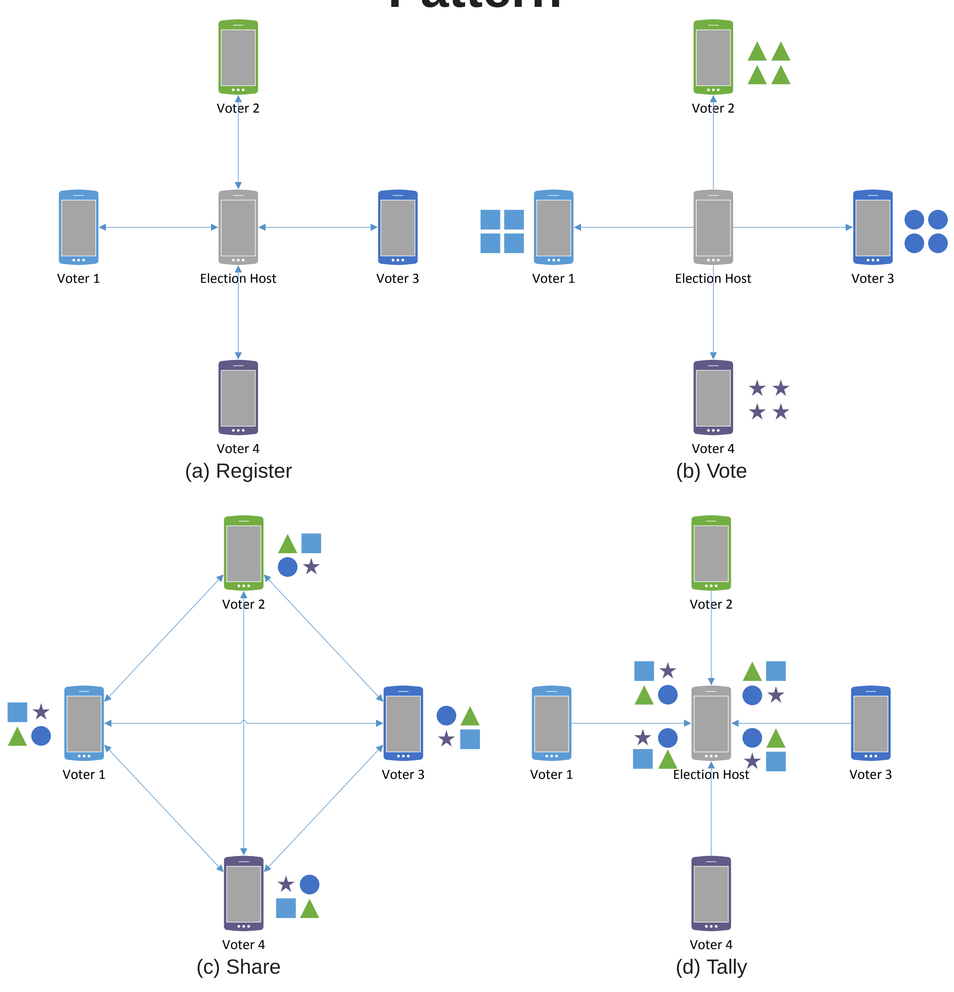
By making t-out-of-n sharing of a secret, the secret can be reconstructed by combining any t shares. Less than t shares do not give any information about the secret.



Example of 3-out-of-4 secret sharing. Given three points, one can reconstruct a polynomial of degree 2. With just two points, this is impossible, as there are many parabolas coinciding with these points.

Ad Hoc Voting Pattern

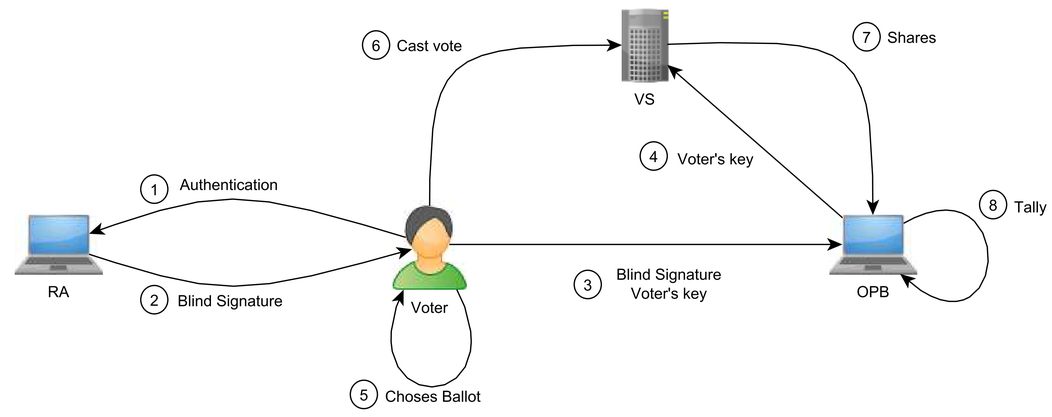
Pattern



Ad Hoc Voting Pattern can be seen as following three-stage protocol:

1. Acquire an ephemeral identity using a blind signature scheme (a)
2. Vote using this identity and distribute the secret ballot using secret sharing (b+c)
3. Combine all secret fragments to calculate the result (d)

Details



- *Voter*: casts vote
- *Voting Servers (VS)*: receives shares of ballot
- *Registration Authority (RA)*: handles registration and checks eligibility
- *Online Polling Booth (OPB)*: handles key distribution and performs the tally

References

[1] David Chaum. Blind signatures for untraceable payments. 1982.

[2] Aggelos Kiayias and Moti Yung. Self-tallying elections and perfect ballot secrecy. 2002.

[3] A. Parakh and S. Kak. Internet voting protocol based on implicit data security. 2008.

[4] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 1995.

[5] Adi Shamir. How to share a secret. 1979.

Radboud University Nijmegen