Mobivote - Decentralized E-Voting on Android Devices

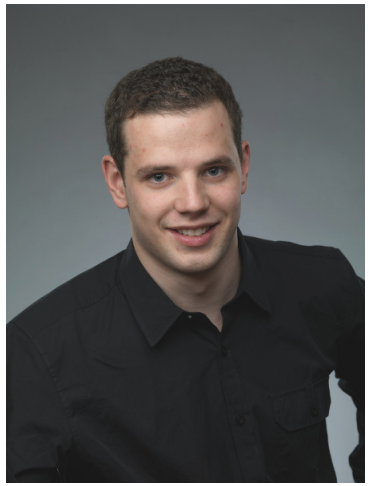
J. Ritter, P. von Bergen

Bern University of Applied Sciences

November 15, 2013

Who we are

- Jürg Ritter
  - Master student at BFH
  - part time student
  - affiliated to the BFH e-voting research group
  - employed in the industry (Swisscom)



- Philémon von Bergen
  - Master student at BFH
  - full time student
  - affiliated to the BFH e-voting research group

Who we are

- The E-Voting group belongs to the Research Institute for Security in the Information Society (RISIS) of the BFH
- Currently staffed with
  - 4 professors
  - 1 PhD student
  - 1 research assistant
  - 2 master students

Outline

Outline

Introduction

The problem

- Most current approaches for e-voting require some sort of central infrastructure
- This means we usually need to do careful planning of a voting session
- Trusted parties are required

Introduction

Idea behind the project

- Provide secure e-voting in a more spontaneous manner
  - Remove the central infrastructure
  - Participants become trustees
- Use mobile devices (tablets, smartphones)
- Use proximity as a secondary channel
  - Visual communication
  - Oral communication
- Targeted market: meetings where decisions need to be taken, for example
  - Board of directors in a company
  - General meeting of associations
  - ...

Introduction

Goal of the project

- Build a decentralized e-voting system on Android devices (smartphones and tablets)
- Uses WLAN as communication layer
- No internet access required
- Has to be usable without great knowledge about security
- Supports up to 20 participants
- Supports one-out-of-n votes
- Two master theses implementing two different cryptographic protocols

Outline

Technologies we use

- Android
- AllJoyn as messaging bus [1]
- NFC and QR-codes
- UniCrypt library for protocol cryptography [2]

UniCrypt

Outline

Live demo

- Protocols not implemented yet
- Please cross fingers for us, you are beta testers! ;-)

Outline

Cryptographic protocols

- CGS97 [3] (Jürg)
  - A Secure and Optimally Efficient Multi-Authority Election Scheme
- A Fair and Robust Voting System by Broadcast [1] (Philémon)

CGS97

Brief overview

- Protocol due to Cramer, Gennaro and Schoenmakers
- Setup
  - Administrator defines the question and the possible options of the vote
  - Trustees generate an asymmetric ElGamal keypair, where the private key is split among all trustees
  - Transcript of key generation is posted on the bulletin board
- Voting Phase
  - Voters pick an option, encrypt it using the public key and post it to the bulletin board along with a proof of validity
- Tallying
  - Using the homomorphic property of ElGamal encryption, the encrypted ballots on the bulletin board are sumed up
  - Trustees collaborate in order to decrypt the encrypted result and post the final result on the bulletin board, along with zero knowledge proofs

A Fair and Robust Voting System by Broadcast

Brief overview

- Authors: Khader, Smyth, Ryan, Hao, 2012
  - Extension of "Anonymous Voting by Two-round Public Discussion" (Hao, Ryan, Zieliński, 2008) [2]
- 3 or 4 rounds of message exchange and a tally round
- Zero knowledge proofs assure verifiability
- Uses homomorphic tallying

A Fair and Robust Voting System by Broadcast

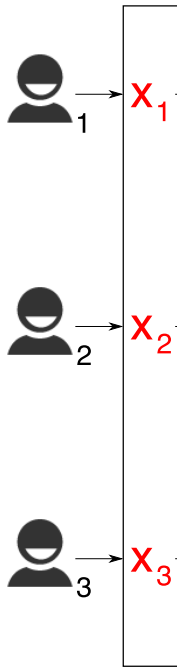
Brief overview

1

A Fair and Robust Voting System by Broadcast

Brief overview

2

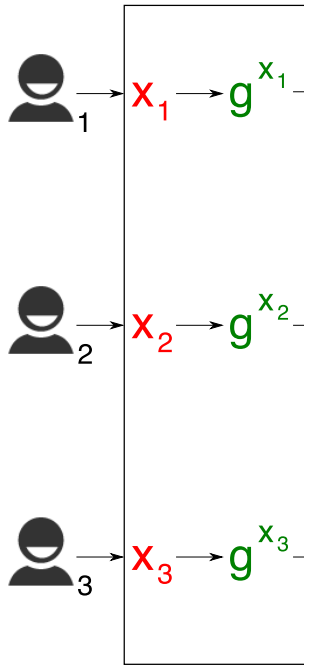


Red: private values

A Fair and Robust Voting System by Broadcast

Brief overview

3

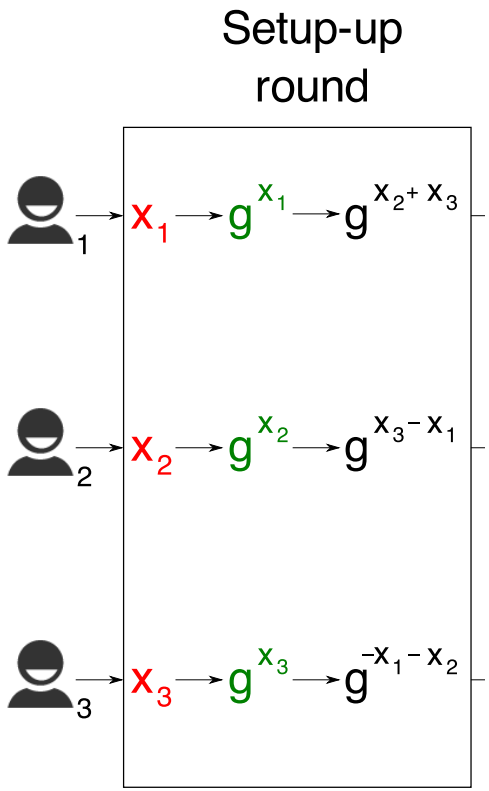


Red: private values Green: published values

A Fair and Robust Voting System by Broadcast

Brief overview

4

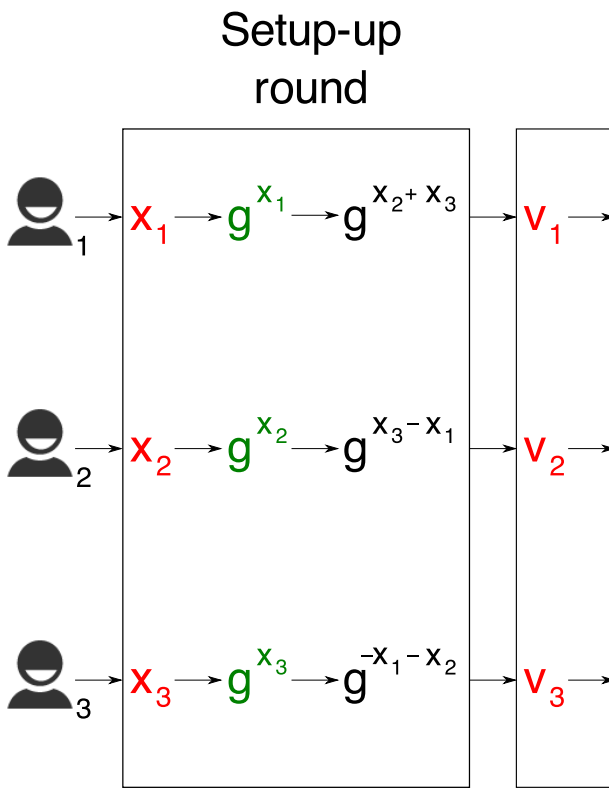


Red: private values Green: published values Black: computed values

A Fair and Robust Voting System by Broadcast

Brief overview

5

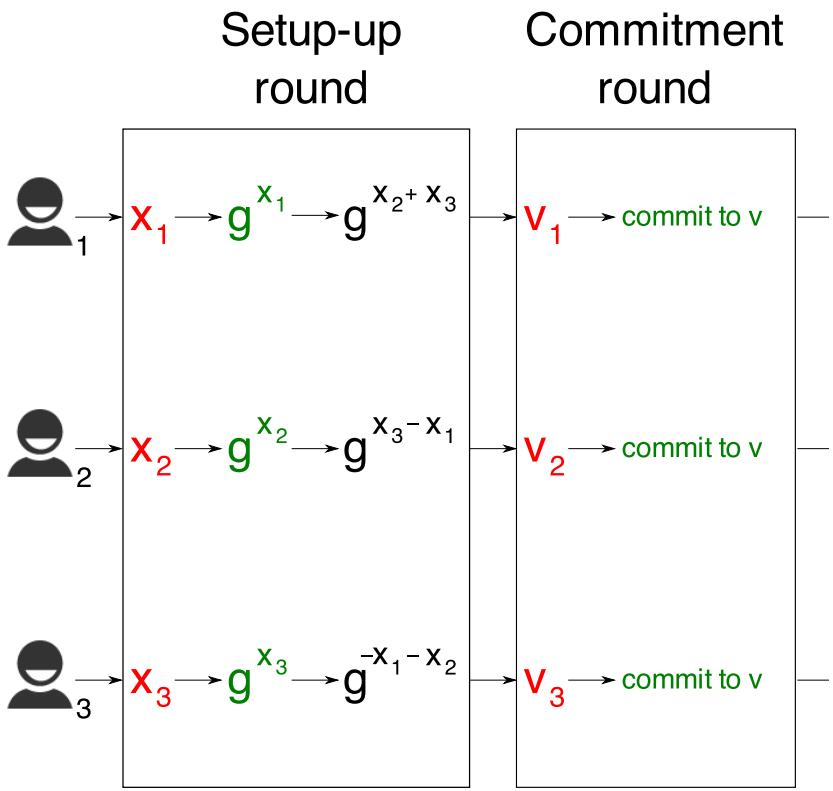


Red: private values Green: published values Black: computed values

A Fair and Robust Voting System by Broadcast

Brief overview

6

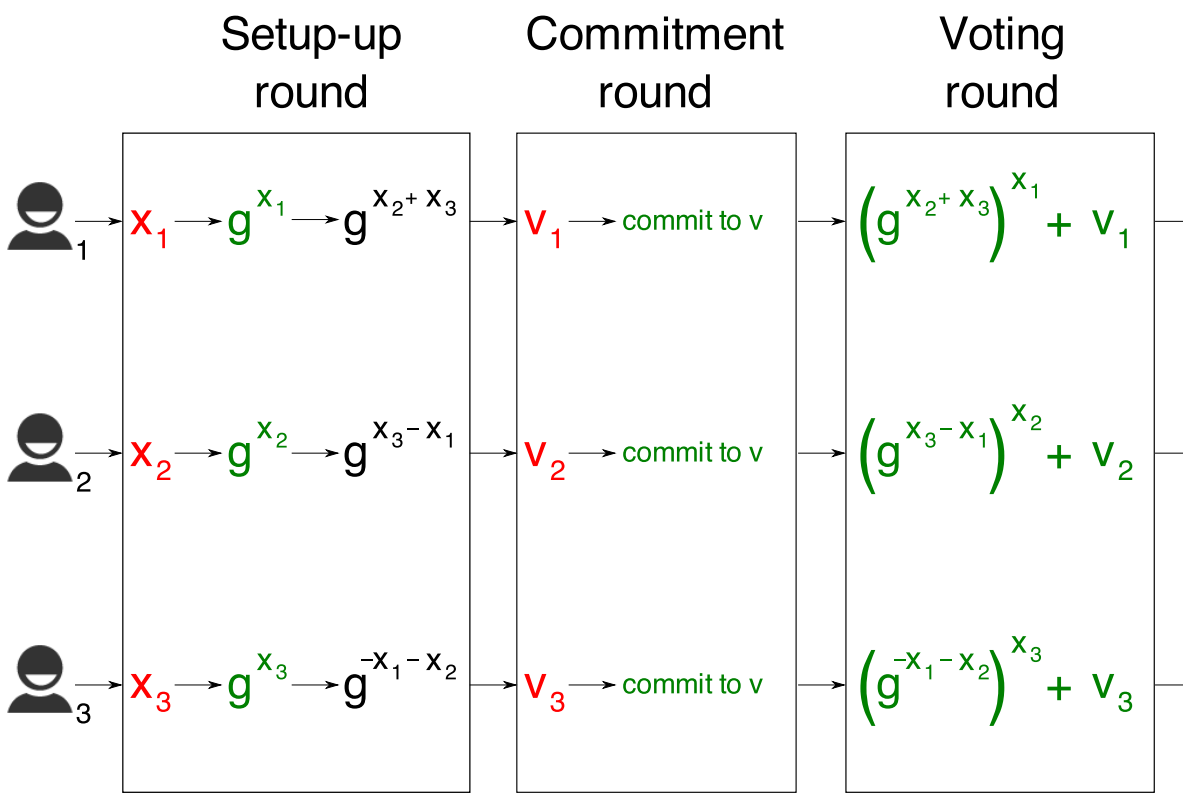


Red: private values Green: published values Black: computed values

A Fair and Robust Voting System by Broadcast

Brief overview

7

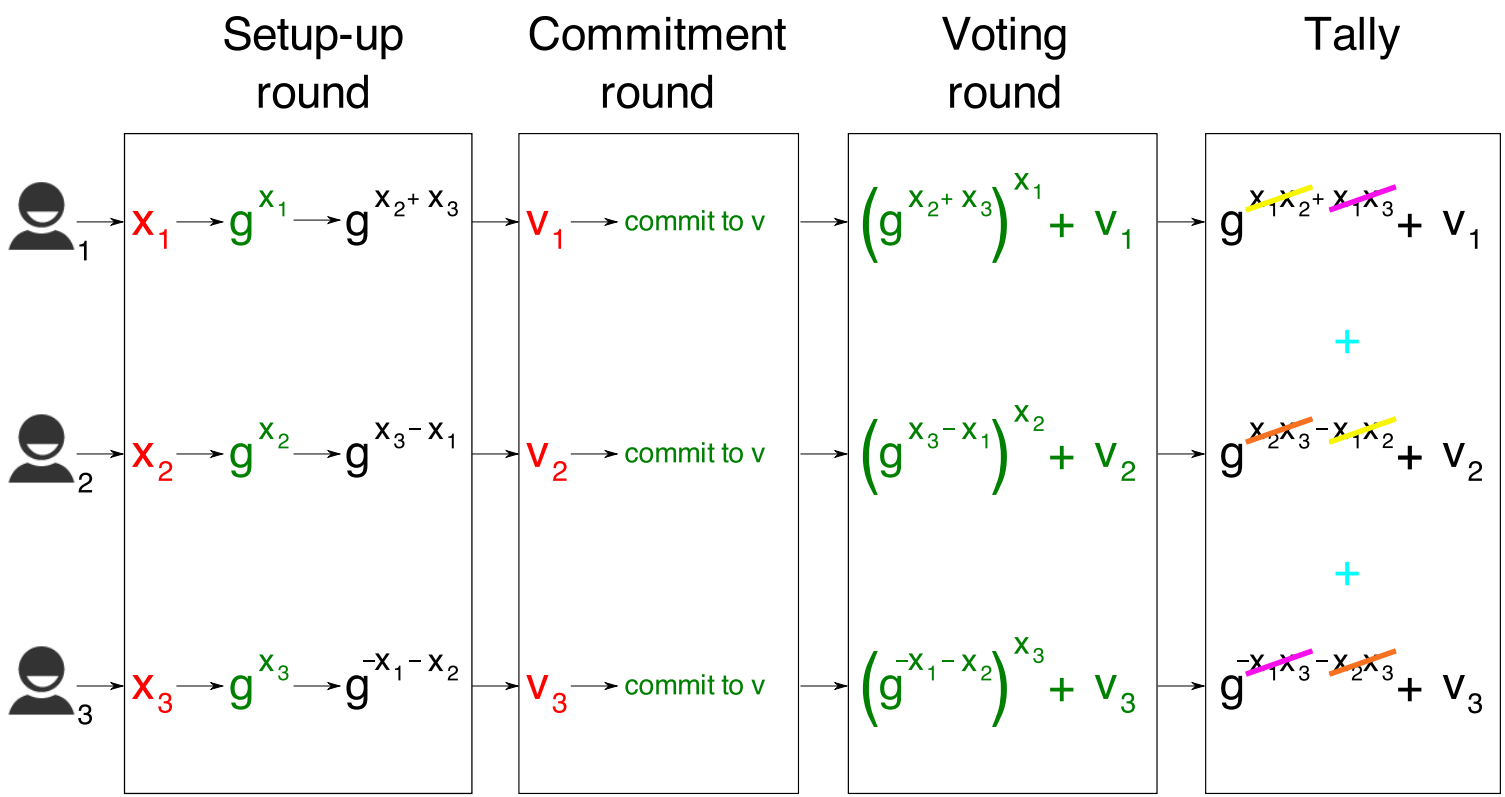


Red: private values Green: published values Black: computed values

A Fair and Robust Voting System by Broadcast

Brief overview

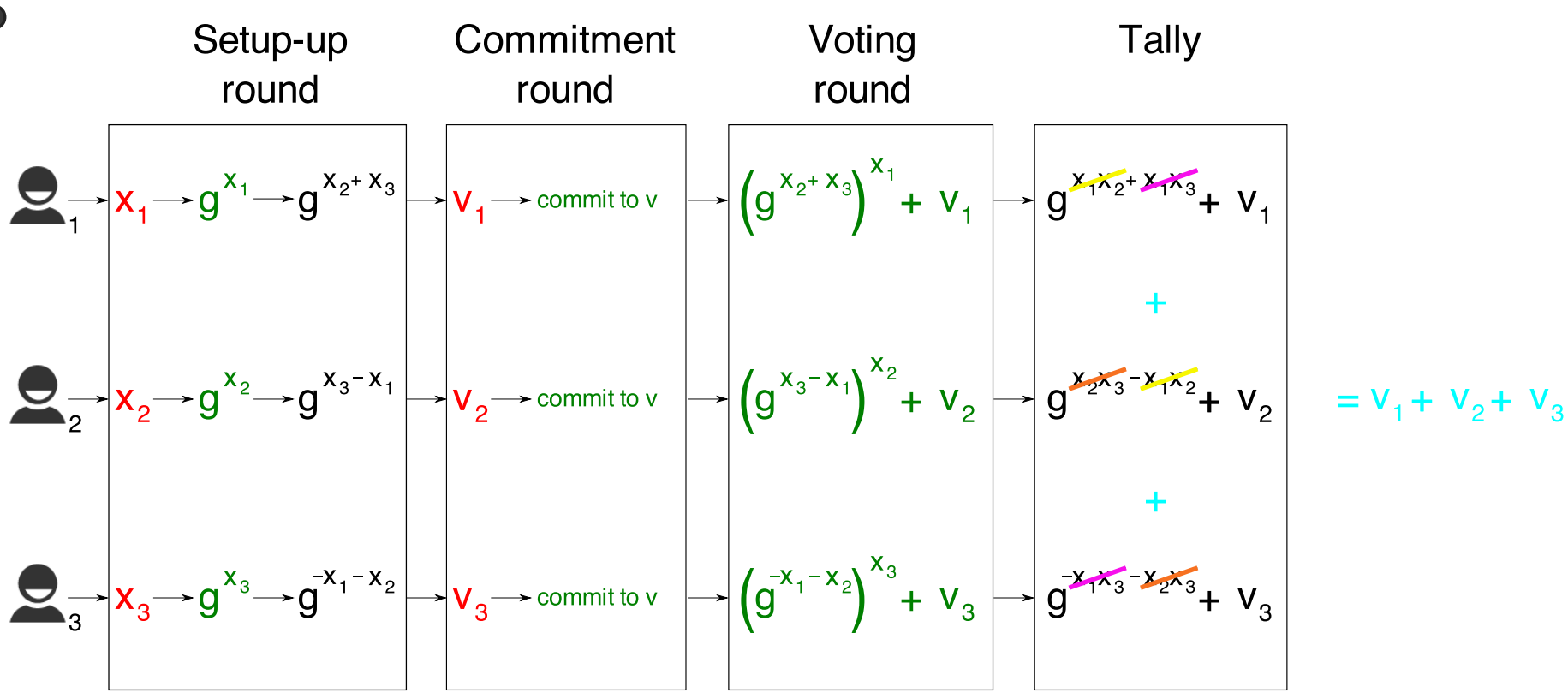
8



Red: private values Green: published values Black: computed values

A Fair and Robust Voting System by Broadcast

Brief overview



Red: private values Green: published values Black: computed values

Outline

Challenges

- Decentralized communication is not easy to set up
- Trade-off security / usability
- Robustness in many situations
- Android Wifi API
- Bootstrapping of a secure group communication

Challenges

Bootstrapping of a secure group communication

- How to check the origin of a message (authentication) ?
  - Each participant sends a RSA public key to allow others to verify the signature of the messages he sent
  - When two different public keys are received for the same participant, an error is thrown

Challenges

Bootstrapping of a secure group communication

- Communication privacy
  - AllJoyn default groups are public, so everybody can connect to a group
  - This increases the risk of impersonification or DoS attacks
  - So we use AES encryption of messages exchanged on the network
  - AES key is derived from a password that has been exchanged using a channel based on proximity
    - Visually (QR Code, display password)
    - Orally (somebody reads password)
    - Pass around a piece of hardware containing the password (NFC token)

Challenges

Bootstrapping of a secure group communication

- Key for AES encryption
  - In order to avoid rainbow table attacks on the password used for AES key derivation, we have to use a dynamic salt
  - The salt is transmitted over the network
  - An attacker could inject a different salt (DoS attack)
  - We include 3 chars of the salt's hash in the password in order to verify correctness of the salt

Outline

Discussion

Wrap-up

- We are trying to use e-voting approaches for a new use case
- Centralized component
  - to control the flow of the voting process
  - to manage the message exchange
- The e-voting protocols are still decentralized
- Protocols make some assumptions that are not always trivial to implement

Discussion

Next steps

- Next steps
  - Split up in separate projects
  - Implementation of the protocols
  - Extension to other mobile devices (future projects)

Discussion

Feedback

- Are there...
  - any questions?
  - any remarks?

Thanks

- Thank you for your attention !

References

- AllJoyn
  In the Internet of Everything, AllJoyn Enables the "Internet of Things Near You".
  Qualcomm Innovation Center
- UniCrypt
  Cryptographic library (not ready for production at this point)
  BFH E-Voting Group
- R. Cramer, R. Gennaro, B. Schoenmakers
  A Secure and Optimally Efficient Multi-Authority Election Scheme
  1997

References

- D. Khader, B. Smyth, P.Y.A Ryan, F. Hao
  A Fair and Robust Voting System by Broadcast
  2012
- F. Hao, P.Y.A Ryan, P. Zieliński
  Anonymous Voting by Two-round Public Discussion
  2008