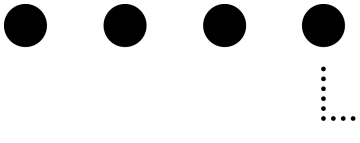


Berner Fachhochschule

Technik und Informatik

Presention of Prêt à Voter

Stephan Fischli

Introduction

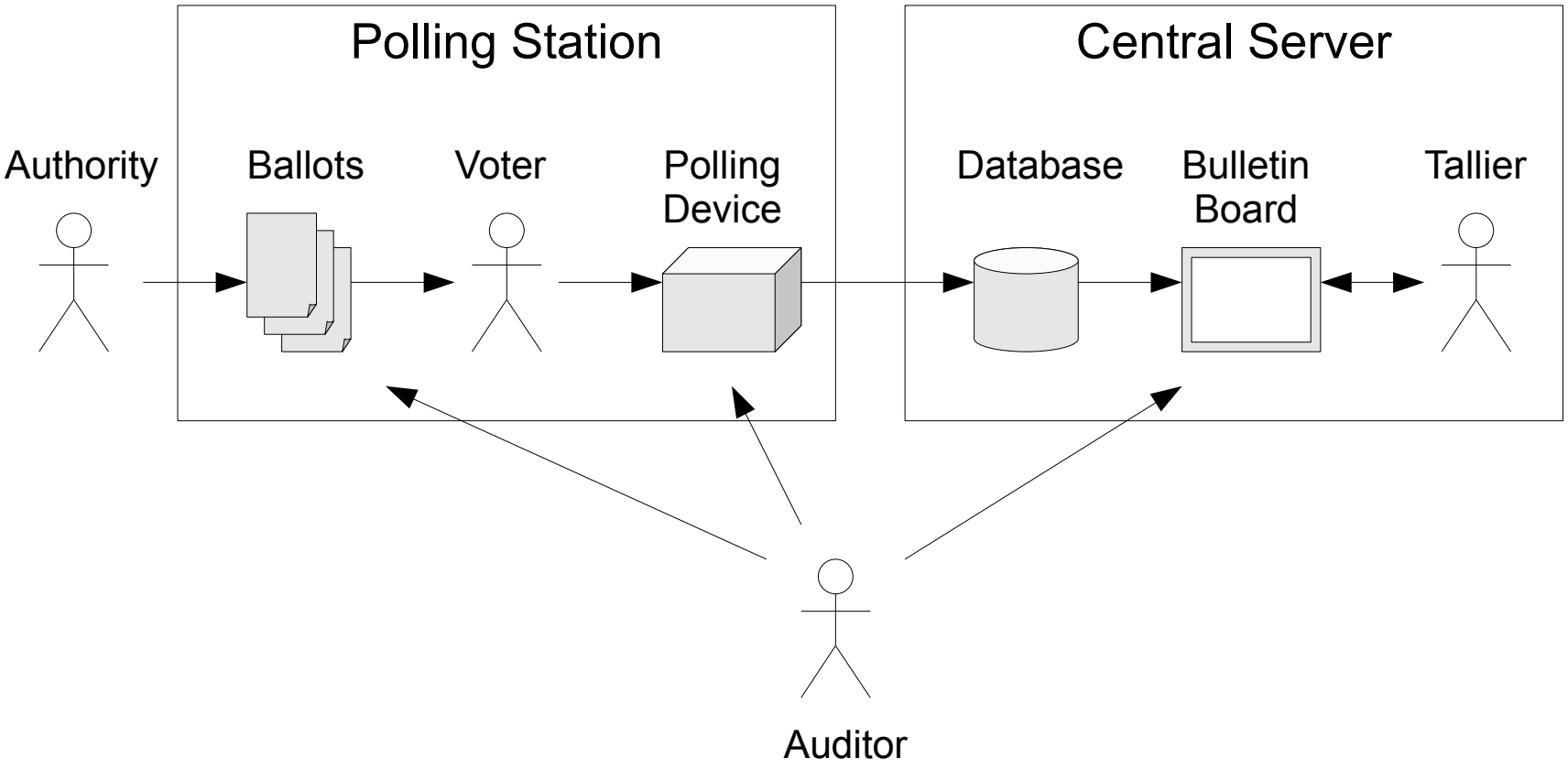
Verifiable voting scheme based on idea of Chaum

- voter gets receipt of encrypted vote for verification
- multiple tellers perform anonymising mix on encrypted votes
- all steps are published on bulletin board
- random checks guarantee correctness

Reference

- David Chaum, Peter Y. A. Ryan, Steve Schneider
  A Practical, Voter-Verifiable Election Scheme

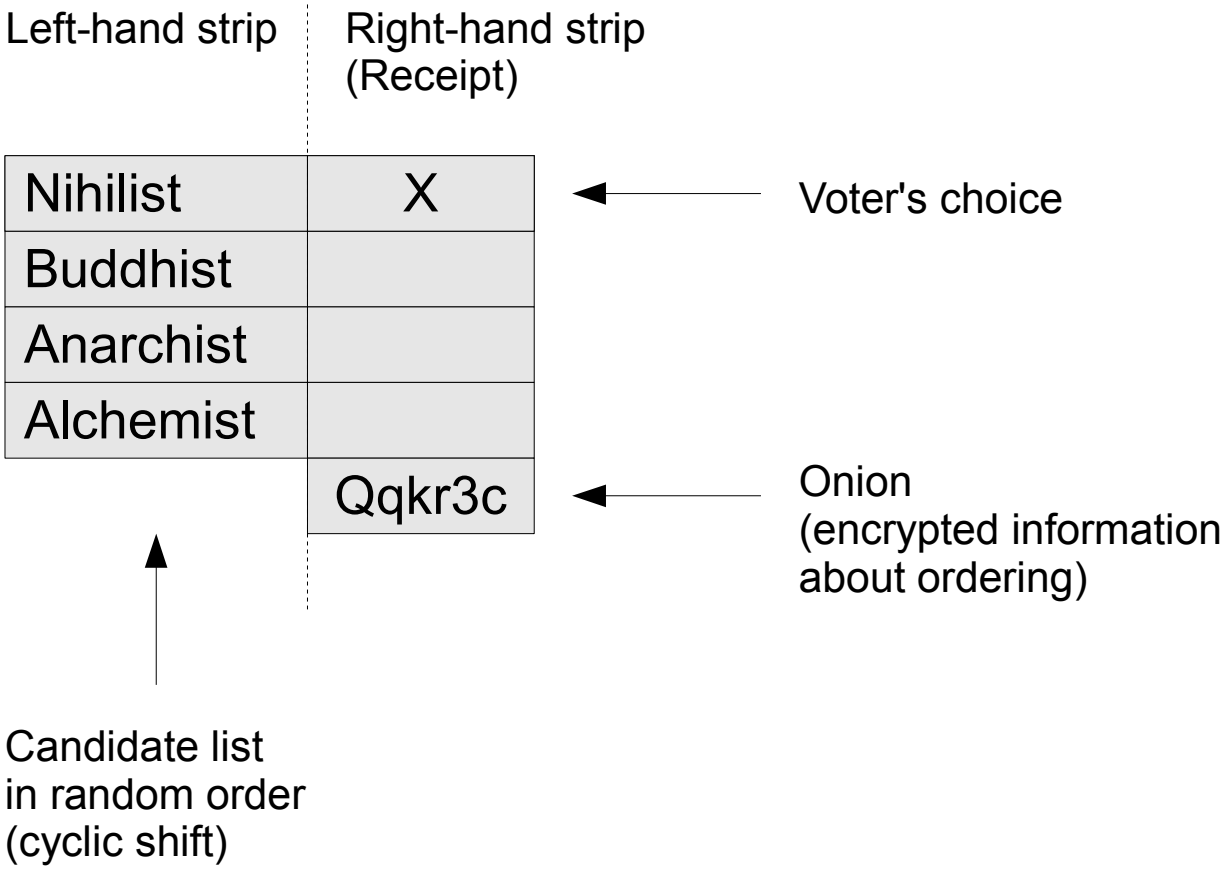
Process Overview



Election Setup

- Number of tellers (0,...,k-1) are appointed
- Each teller has two key pairs (SK_{2i},PK_{2i}) and (SK_{2i+1},PK_{2i+1})
- Authority creates large number of ballots and distributes them to the polling stations

Ballot Structure



Ballot Construction

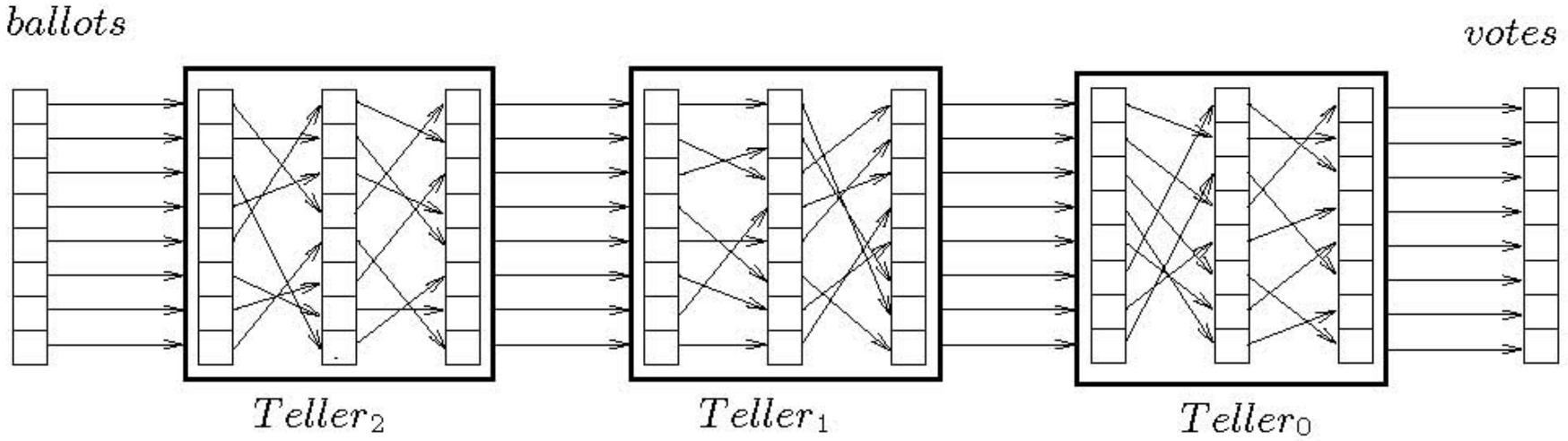
- For each ballot generate unique random
  seed = $(g_0, g_1, \ldots, g_{2k-1})$ (k number of tellers)
- Calculate cyclic offset of candidate list
  $\theta = \sum \text{hash}(g_i) \pmod v$ (v size of candidate list)
- Calculate corresponding onion
  D_0 random
  $D_{i+1} = \text{encrypt}_{PK_i}(g_i, D_i)$ (i=0,..., 2k-1)
  Onion = D_{2k}

Vote Casting

- Voter
  - authenticates and registers at polling station
  - selects a pair of ballots at random
  - chooses one to fill in her/his choice
  - destroys left-hand strip
  - feeds right-hand strip to polling device and keeps it as a receipt
- Polling device digitally sends right-hand strips to central server
- Once voting has closed, right-hand strips are posted to public bulletin board

Tallying Overview

- Talliers perform anonymising mix and decryption of the encrypted ballots on the public bulletin board
- Each tallier accepts the output column from the previous tallier as input and produces a middle and an output column
- The emerging decrypted votes cannot be linked to the encrypted ballots



Tallying Calculation

- Represent the position of the voter's choice by an integer
  $0 \leq r \leq v-1$
- Teller i-1 accepts output column (r_{2i}, D_{2i}) from teller i and
  - strips off outer layer of the onion
    $(g_{2i-1}, D_{2i-1}) = \text{decrypt}_{SK_{2i-1}}(D_{2i})$
  - calculates new r-value
    $r_{2i-1} = r_{2i} - \text{hash}(g_{2i-1}) \pmod v$
  - applies secret permutation on all pairs (r_{2i-1}, D_{2i-1}) and posts result to middle column
  - repeats process using second secret key SK_{2i-2} and posts resulting pairs to output column
- First teller obtains decrypted position of the voter's choice
  $r_0 = r - \sum \text{hash}(g_i) \pmod v = r - \theta \pmod v$

Checking on the Authority

- Voter casts a dummy vote
  → Tellers decrypt onion and return the vote
- Voter casts a ranking selection
  → Tellers return the candidate ranking
- Voter sends the onion
  → Tellers return corresponding candidate ordering
- Auditor sends the onion
  → Tellers return corresponding germs and auditor recomputes onion and offset value

Checking on the Voting Devices

- Each voter can visit the public bulltein board and compare the ballots with his/her receipt
- Digital signatures applied by the voting devices prevent fake votes

Checking on the Talliers

- Auditor assigns randomly R and L to each pair of the middle column produced by a teller
- For an R, the teller reveals the outgoing link with the corresponding germ, for an L the incoming link
- Auditor checks for any revealed link $(r_i, D_i) \rightarrow (r_{i-1}, D_{i-1})$ that

$$D_i = \text{encrypt}_{PK_{i-1}}(g_{i-1}, D_{i-1})$$

$$r_{i-1} = r_i - \text{hash}(g_{i-1}) \pmod{v}$$