IDC-TAU

Cryptographic Voting

JUNE 2010

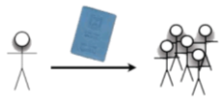
Objectives:

- **Verifiability** and **transparency**
- **Simple** and **reliable** system
- **Backward compatible** with existing (paper-based) systems
- **Unforgeability** of the results
- **Voter secrecy** and **incoercibility**
- **Software independence**:

"Undetected change in software **cannot** yield undetectable change in result "

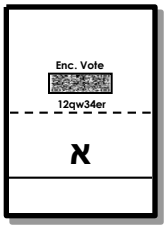
Vote Selection:

① Voter Identification

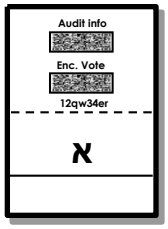


② In the Voting Booth

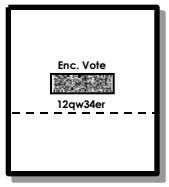
③ Option A: Approve



Option B: Audit



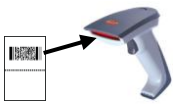
④ Fold Ballot



Vote Casting:

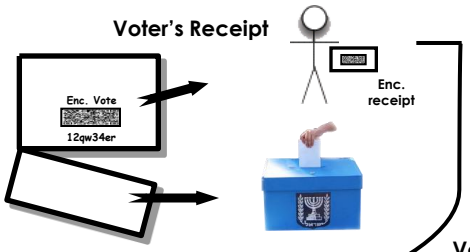
① Voter approaches Committee and:

Ⓐ Scan and Post



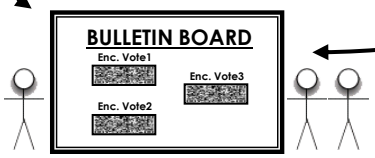
Encrypted barcode is scanned and posted on authenticated Bulletin Board

Ⓑ Voter's Receipt



Cast Physical Vote

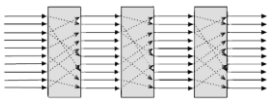
Voter verifies that vote appears on Bulletin Board



Enc. Votes, Audit info and Mix-Net Proofs posted on authenticated Bulletin Board for verification purposes

Counting and Verification:

End of the election day:
Start of verifiable Mix-Net process

① 

Vote threshold decryption:
Parties jointly decrypt the anonymized votes and compute the results of the election

② 

③ Final results are posted on Bulletin Board

Before the Elections:

- Key Generation
- Key Distribution
- Training (Voters and Voting Committee)

Cryptographic Primitives:

- Elliptic curve arithmetic
- El-Gamal based Mix-Net
- Threshold schemes
- Decentralization of trust in the form of smartcards (trusted modules) for generating randomness
- Non-Interactive Zero knowledge proofs

System Auditing:

- Verifiability is achieved by giving the different participants in election tools used for auditing
- Voter can verify that vote was counted by checking that enc. ballot is part of tally appearing on the Bulletin Board
- Auditors can verify that voting booth is not printing deviated votes by requesting audit info – randomness used in enc. operation: E_k(vote,randomness)
- Mix-Net provides Non-Interactive Zero knowledge proofs used for verifying correctness of Mix process

Project Participants:

IDC
- Dr. Alon Rosen
- Ido Bergerfroind
- Omer Davidi
- Tomer Gabai
- Assaf Inger
- Shiran Kleiderman
- Doron Sharon

TAU
- Prof. Ran Canetti
- Prof. Amnon Ta-Shma
- Jonathan Ben-Nun
- Ben Riva