Berner Fachhochschule - Technik und Informatik

David Chaum's Punchscan and Scantegrity

Rolf Haenni

May 12th, 2010

Outline

E2E Voting Systems

Punchscan

Randomized Partial Checking

Scantegrity

Outline

E2E Voting Systems

Punchscan

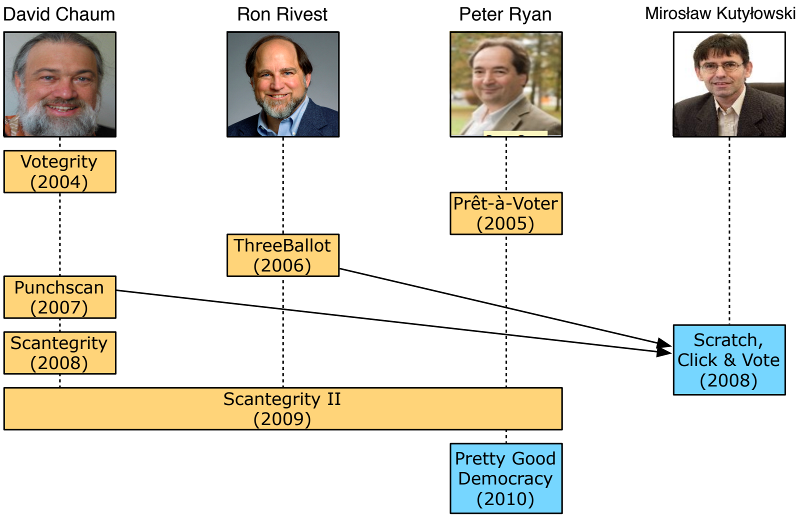
Randomized Partial Checking

Scantegrity

E2E Voting Systems

- E2E = "end-to-end voter verifiable" or "end-to-end auditable"
- Receipt-based (voter gets a receipt without revealing vote)
- Voter auditable (any voter may check that his or her ballot is correctly included in the electronic ballot box)
- Receipt-free (no voter can demonstrate how he or she voted)
- Combination of paper-based and electronic voting
- Usually, voting takes place in private voting booths at the polling station
- Often designed to be used together with optical scanners
- Allows paper recount

Overview of E2E Systems

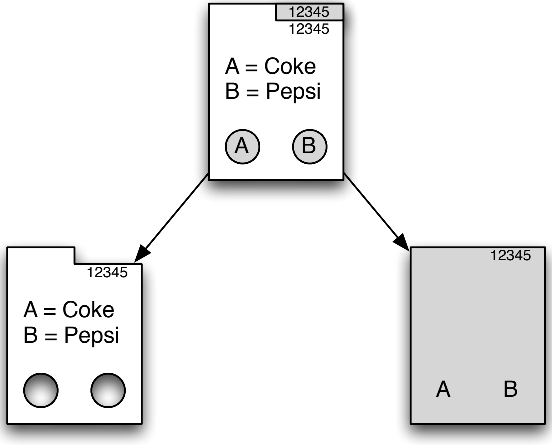


Outline

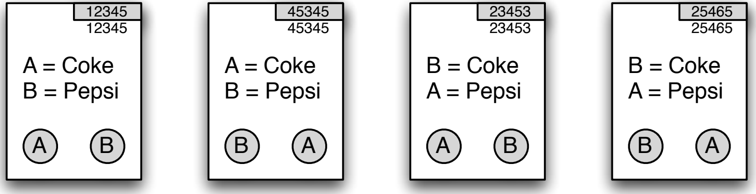
Ballots

- The pre-printed ballots consist of two-layers
- First layer
  - → Serial number
  - → List of candidates/options (e.g. in alphabetical order)
  - → Symbols attached to each list item (random order)
  - → Two holes
- Second layer
  - → Serial number
  - → Symbols to appear in holes (random order)

Ballots



Ballots

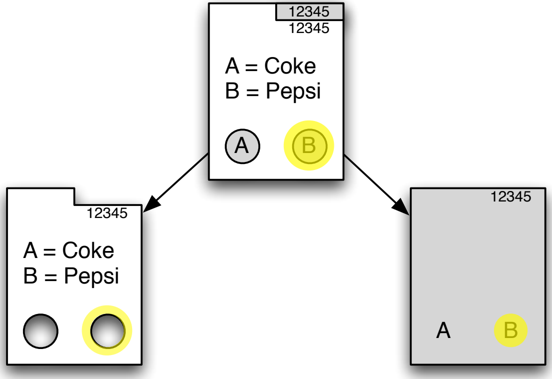


- There are two random choices $P_1 \in \{0, 1\}$ and $P_2 \in \{0, 1\}$
  - $\rightarrow$ $P_1 = 0$ means "AB on top layer"
  - $\rightarrow$ $P_1 = 1$ means "BA on top layer"
  - $\rightarrow$ $P_2 = 0$ means "AB on bottom layer"
  - $\rightarrow$ $P_2 = 1$ means "BA on bottom layer"
- Thus, we have four different ballots $(P_1, P_2) \in \{00, 01, 10, 11\}$

Voting Process

- The voter marks the hole containing the preferred choice with a translucent stamp
- The two layers are separated
- The voter choses one of the layers to be shredded
- The other layer is scanned and kept as a receipt
- Let $P_3 \in \{0,1\}$ denote the position of the mark
  - → $P_3 = 0$ means "Mark on the left"
  - → $P_3 = 1$ means "Mark on the right"
- Note that $R = P_1 \oplus P_2 \oplus P_3$ denotes the vote
  - → $R = 0$ means "1st candidate/option on the list"
  - → $R = 1$ means "2nd candidate/option on the list"

Voting Process



$$P_1 = 0,\ P_2 = 0,\ P_3 = 1$$
$$\Rightarrow R = 1 = B$$

Reconstructing the Shredding

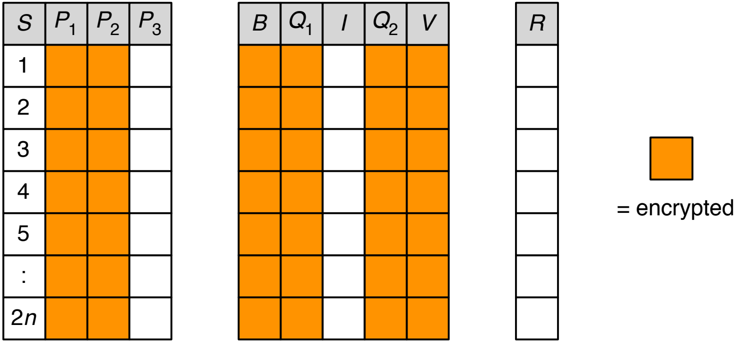
- Shredding destroys either P_1 or P_2, i.e., the paper receipt does not contain any information about R
- To reconstruct R in the final tally, two other values are defined
  - → $Q_1 \in \{0,1\}$ is chosen at random
  - → $Q_2 \in \{0,1\}$ is chosen such that $Q_1 \oplus Q_2 = P_1 \oplus P_2$ holds
- This yields $R = (P_1 \oplus P_2) \oplus P_3 = (Q_1 \oplus Q_2) \oplus P_3$
- $I = P_3 \oplus Q_1$ defines an "intermediate result" from which the vote is constructed by $R = I \oplus Q_2$

Public Board

- The public board contains three tables
- Table 1 contains four columns for
  - → S = Serial number
  - → P_1
  - → P_2
  - → P_3
- Table 2 contains five columns for
  - → B = Ballot row (1st permutation)
  - → Q_1
  - → I
  - → Q_2
  - → V = Vote row (2nd permutation)
- Table 3 contains one column for R

Public Board

- Setting up the board takes place before printing the ballots
- After the setup, the board looks as follows



Pre-Election Audit

- The goal is to verify whether $Q_1 \oplus Q_2 = P_1 \oplus P_2$ holds
- For this, half of the rows are decrypted (chosen at random)
- By inspecting the board, everybody can verify its integrity with high probability

S	P_1	P_2	P_3
1	1	0	
2			
3	0	0	
4			
5			
:			
$2n$	1	1	

B	Q_1	I	Q_2	V
3	1		1	2
1	0		1	4
$2n$	1		1	3

R

Pre-Election Audit

- After the pre-election audit, decrypted rows are deleted
- The remaining ballots are printed and distributed to the polling stations
- Every voter receives exactly one of those ballots

S	P_1	P_2	P_3
2			
4			
5			
8			
⋮			

B	Q_1	I	Q_2	V

R

Vote Casting

- After scanning the ballot, the board is updated as follows
  - → For each top layer ballot, P_1 is decrypted
  - → For each bottom layer ballot, P_2 is decrypted
  - → P_3 is posted

S	P_1	P_2	P_3
2	1		1
4		0	1
5		1	0
8	0		1
:		1	0

B	Q_1	I	Q_2	V

R

- This allows the voter to verify the correct recording of the vote

Announcing the Results

- When polling stations close, the board is enhanced as follows
  - → I is posted
  - → R is posted

S	P_1	P_2	P_3
2	1		1
4		0	1
5		1	0
8	0		1
:		1	0

B	Q_1	I	Q_2	V
		0		
		1		
		1		
		1		
		0		

R
1
1
0
0
1

- The final outcome is derived from column R

Post-Election Audit

- The goal is to verify the correct shuffling of the table rows and the correctness of I and R
- For this, half of the rows are selected at random and B and Q_1 are decrypted
- For the other half of the rows, Q_2 and V are decrypted

S	P_1	P_2	P_3
2	1		1
4		0	1
5		1	0
8	0		1
:		1	0

B	Q_1	I	Q_2	V
		0	0	4
2	0	1		
8	1	0		
		1	1	5
4	0	0		

R
1
1
0
0
1

Extensions

- 1-out-of-n elections are possible by doing the calculations modulo n (instead of modulo 2)
- Multiple public boards with different permutations (columns B and V) can be run in parallel, each of which must come out with the same result
- To protect the integrity of the ballots and the initial board, the voting authority must commit itself to the respective content (using a proper commitment scheme)

Outline

E2E Voting Systems

Punchscan

Randomized Partial Checking

Scantegrity

Randomized Partial Checking (RPC)

- Usually, mix nets provide (expensive) proofs of correct mixing
- RPC mix nets provide strong evidence of correct mixing
  - → Every mix-server must reveal half of the links between its input and output
  - → The links to be revealed are determined at random by other protocol participants
  - → If k votes are manipulated by a mix, then it remains undetected with probability $\frac{1}{2^k}$

M. Jakobsson, A. Juels, and R. L. Rivest
Making mix nets robust for electronic voting by randomized partial checking.
11th USENIX Security Symposium, 2002

Outline

Links

- White Paper (Scantegrity)
- Video presentation (Scantegrity)
- Video presentation (Scantegrity II)