Practical Provably Correct Voter Privacy Protecting End to End Voting Employing Split Value Representations of Votes

Michael O. Rabin
Columbia University SEAS
Harvard University SEAS

Ronald L. Rivest
MIT CSAIL

Presenter Prof. Douglas Wikstrom

EVOTE 2014 Bergenz
October 29th, 2014

RRV (Rabin Rivest Voting) Properties

- Voter Privacy Preserving
- Vote Values Publicly Posted
- Publicly Verifiable Proof of Correctness
- Supports Complicated Voting Forms
- Resistant to Gossipy and Failing Servers
- Highly Efficient
- Not Dependent on Specialized Encryptions Such as Homomorphic Encryptions
- Employs Novel Highly Efficient, Verifiable, Mix-Net Using Just Any Commitment Functions and Split-Value Representation

Structure

- Voter Uses Tablet
- Secure Bulletin Board (SBB) for Posting Concealed Votes, Eventually Clear Vote Values, Proof of Correctness
- Proof Server (PS) Consisting of (For Example) 11 Interconnected Servers
- In Example, Tolerates Up To Two Gossipy Servers, Two Failing Servers
- Correctness Proof, If Accepted, Assures Absolute Correctness of Vote Tally Irrespective of Server Misbehavior

Split-Value Representations [Rabin et al., 2007], [Rabin et al., 2009]

- Let M be an integer, $0 \leq x < M$ a value. A Split-Value (SV) representation of x is $X = (u,v)$ where

$$\text{Val}(X) = (u+v) \bmod M = x$$

- Random SV representation is obtained by $u \leftarrow_R [0, M-1]$, and
$v = (x-u) \bmod M$
- Let COM$(,)$ be a commitment function so that a value u is committed by choosing key K and setting COM(u) = COM(K, u)

Split-Value Representations Continued

- Opening / Decommitting COM(u) done by revealing K, u. Checking correctness by computing COM(K, u) and verifying equality with COM(u).
- COMSV(X) (COM Split-Value X) for $X = (u, v)$ obtained by choosing random keys K_1, K_2 and setting COMSV$(X) = ($COM$(K_1, u),$ COM$(K_2, v))$

Proving Correctness of Equality and of Addition of Concealed Values

- Let $X=(u_1, v_1), Y=(u_2, v_2)$. Assume COMSV$(X)$, COMSV($Y$) posted. Prover who knows to open commitments, claims to Verifier that Val(X)=Val(Y)
- Note: Val(X)=Val(Y) iff exists $t \in [0, M-1]$ s.t. $X = Y + (t, -t)$ i.e. $(u_1, v_1) = (u_2 + t, v_2 - t)$ (all ops. $mod\ M$)
- Proof: Prover posts t

Proving Correctness of Equality and of Addition of Concealed Values (Continued)

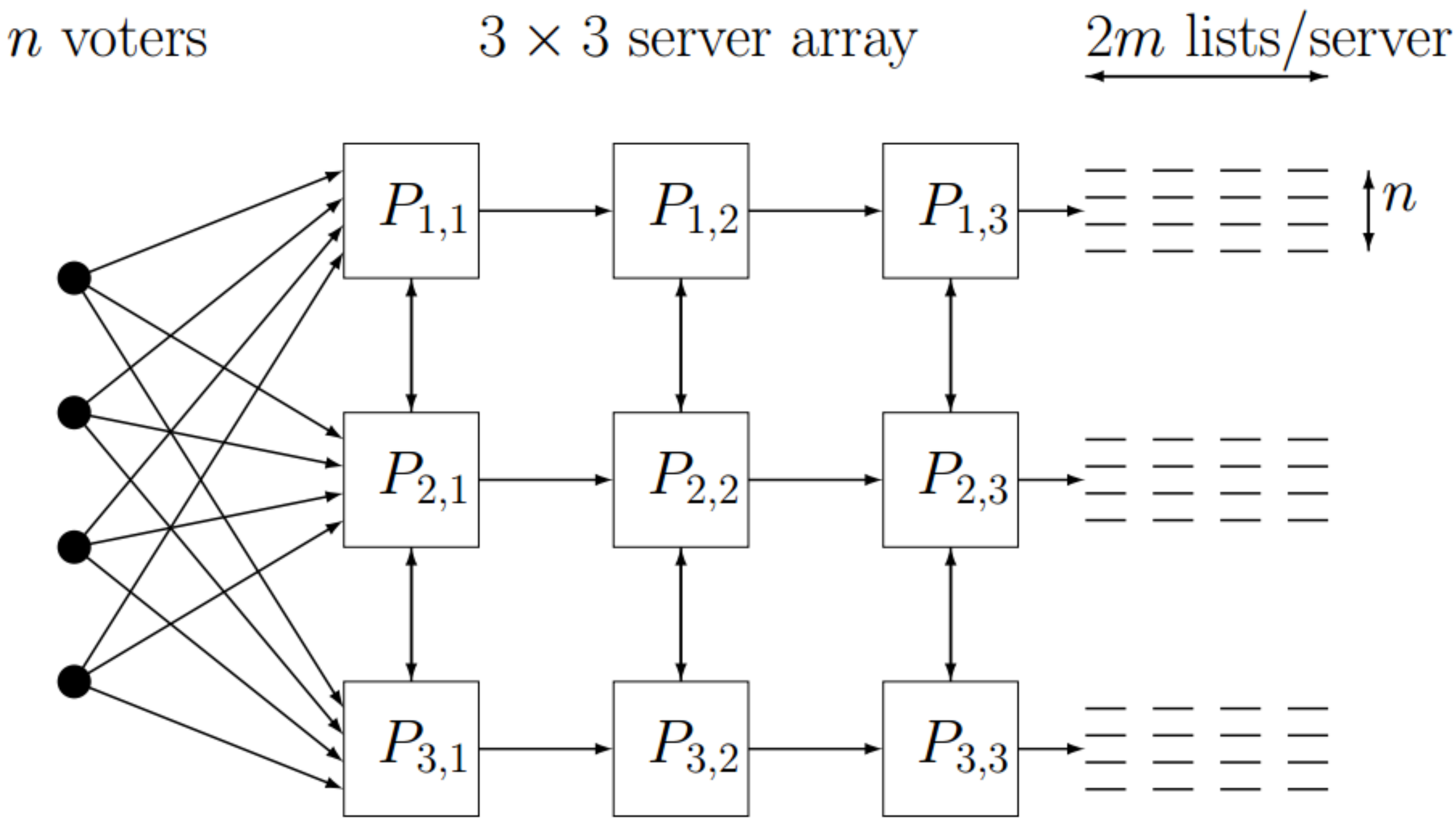
- Verifier randomly chooses $c \in \{1, 2\}$
- If $c=1$, Prover reveals u_1, u_2. Verifier checks $u_1 = u_2 + t$
- If $c=2$, Prover reveals v_1, v_2. Verifier checks $v_1 = v_2 - t$
- PROB(Verifier Accepts False Claim of Val(X) = Val(Y)) ≤ ½
- Assume COMSV(X), COMSV(Y), COMSV(Z) posted. Prover who knows to open commitments claims to Verifier that Val(X)+Val(Y) = Val(Z)

Proving Correctness of Addition (Continued)

- Again, addition holds iff exists $t \in [0, M-1]$, s.t. $X + Y = Z + (t, -t)$. I.e. $(u_1, v_1) + (u_2, v_2) = (u_3 + t, v_3 - t)$
- Again Verifier randomly chooses $c \in \{1, 2\}$.
- If $c = 1$, Prover reveals u_1, u_2, u_3.
- Verifier accepts claim if $u_1 + u_2 = u_3 + t$
- Similarly if $c = 2$
- PROB(Verifier accepts false claim)$\leq 1/2$
- Note that these proofs REVEAL NOTHING about Val(X), Val(Y), Val(Z)!!

Structure of System

- Proof Server comprises 9 servers arranged in 3 rows and 3 columns



Structure of System (Continued)

- System employs standard PKE, say RSA. Three instances EN_1, EN_2, EN_3 with public encryption keys en_1, en_2, en_3 and private / secret decryption keys dc_1, dc_2, dc_3 are used.
- Every Voter Tablet has all public encryption keys en_1, en_2, en_3
- In Proof Server PS first server $P_{1,1}$ in first column gets decryption key dc_1, second server $P_{2,1}$ in first column gets dc_2, third server $P_{3,1}$ in first column gets dc_3.

Voting

- Voter gets a Voter Tablet. Vote represented by some values

  $w \in [0, M-1]$. M, say, $= 2^{32}$
- Tablet randomly breaks voter vote value w into components $w = x + y + z \ (Mod\ M)$
- Tablet creates random split-value representations X, Y, Z for x, y, z. Tablet selects random keys $K_1, K_2, \ldots, K_5, K_6$. Creates COMSV($X$), COMSV($Y$), COMSV($Z$)
- Voter is assigned vote id vid. Voter Ballot is $vid, COMSV(X), COMSV(Y), COMSV(Z)$

Voting (Continued)

- Not mandatory. Voter gets receipt $R = vid,$ Hash of his Ballot
- Tablet collects all ballots, orders by voter ids and posts on SBB

Voter Tablet: Randomly chooses AES key $ktab$

AES($ktab$, list of all X comp. of its vote values) —send→ $P_{1,1}$

AES($ktab$, list of all commitment keys K_1, K_2 of COMSV(X)) —send→ $P_{1,1}$

$EN_1(en_1, ktab)$ —send→ $P_{1,1}$

- Similarly for $P_{2,1}$ and $P_{3,1}$ with Y and Z

Creation of Proof

- Proof Server chooses $2m$ (say $2m=24$)
- Proof Server repeats $2m$ times a net-mixing of cast votes
- Mixing done along the three rows of PS, see diagram
- In each PS column, Proof Servers jointly agree on a permutation of vote values to next column
- Proof Servers in column agree on obfuscation of vote value components, see paper for obfuscation

Creation of Proof (Continued)

- Proof Server $P_{1,3}$ of rightmost column creates COMSV(X) of its obfuscated components. Posts in the permuted order. Similarly, for $P_{2,3}$ creating COMSV(Y) and $P_{3,3}$ creating COMSV(Z)
- Now there are posted $2m$ permutations of commitments to obfuscated components of all the vote values
- Cut-And-Choose: Using strong source of randomness, m permuted lists are chosen and PS rearranges by vote ids and using Split-Value proves equality to posted concealed votes

Creation of Proof (Continued)

- Remaining m permuted lists of commitments to components of votes are opened in permuted form
- Vote values are computed by addition of components
- Assuming fewer than three gossipy servers, voter votes remain private
- Dealing with failures requires two additional servers. Details in full paper.
- Further work deals with fully malicious servers

Probability of Accepting False Proof

- Theorem: The probability that the revealed arrays of vote values are permutations of same values but differ from actually cast value by more than k locations and accepting the tally as correct is at most

$$1/C(2m,m)+(1/2)^k \approx \sqrt{(3.14m)}/2^{2m}+(1/2)^k$$

- Speed. Tallying and posting proof of correctness for one million votes requires less than ten minutes!

Extra slides below

Illustration of the Method

- Addition
  - M=17
  - x=7, y=7, x+y=z=14
  - X=(3,4), Y=(15,9), Z=(8,6)
  - CLAIM: val(X)+val(Y) = val(Z)

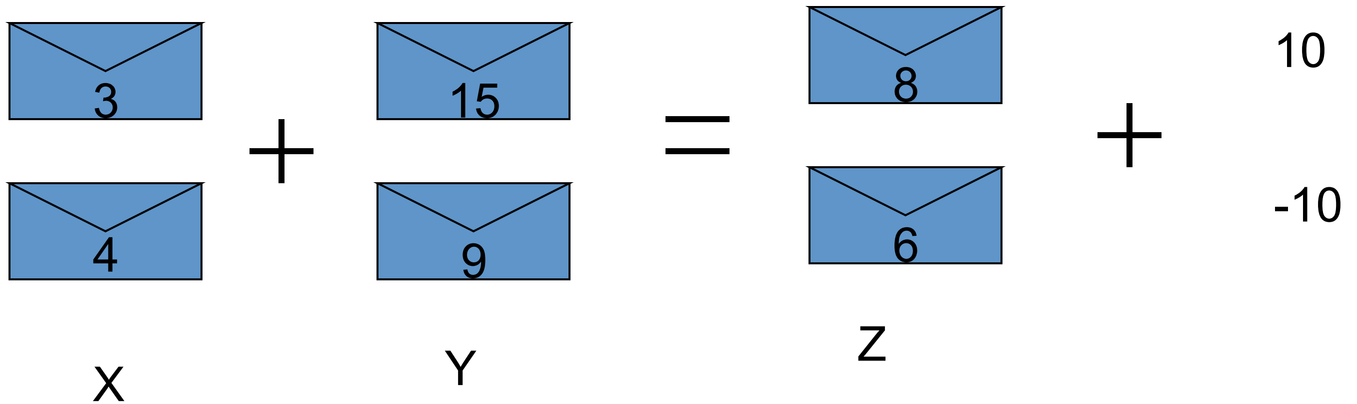


Illustration of the Method

- Addition
  - M=17
  - x=7, y=7, x+y=z=14
  - X=(3,4), Y=(15,9), Z=(8,6)

Prover posts (10,-10). Verifier: $c \xleftarrow{R} \{1,2\}$