

A Homomorphic E-Voting Protocol Based on El-Gamal Cryptosystem

Hamed Mousavi

Ph.D. Student, School of Mathematics
Georgia Institute of Technology

Women In STEM 2019, Georgia State University, Atlanta, Georgia

April 5, 2019

Outline

1 E-Voting Protocols

2 Algorithms of Protocols

3 Numerical Results

Steps

Steps of a Typical E-Voting Protocol

- 1 Set Up
- 2 Vote Casting
- 3 Tally Computing

Categories

Main categories of E-Voting Protocols

- 1 Blind Signature: Using Token, Proof of Authentication for the Ballots.
- 2 Mixers: blind the name and vote of a voter by permutating the ballots.
- 3 Homomorphic: Sum of Encrypted votes is equal to the Encryption of Sum of Votes (i.e. Encrypted Tally is equal to Tally of Encrypted).

Properties

Main Properties of E-Voting Systems

- 1 **Fairness:** The result of voting should not be announced before the end of vote casting.
- 2 **Privacy:** Ensures that no one links the ballot to the voter. (i.e. there is no difference for C , if A votes V_1 and B votes V_2 or A votes V_2 and B votes V_1).
- 3 **Eligibility:** Only the eligible voters, who pass the authentication process, can be allowed to vote once.
- 4 **Robustness:** If the protocol can recover from the faulty or betray of any (reasonably sized) subset of parties.
- 5 **Coercion-resistant:** If an adversary cannot force a voter to behave as he/she wants.

Discrete Logarithm Problem

Let G be a group. Finding k where $y = g^k$ and $g, y \in G$ are known.

El-Gamal Cryptosystem

- 1 Step one: Alice and Bob with private keys $a, b \in \mathbb{F}_p$ send their public keys aP, bP and compute a table of all $\{vP \mid v \text{ is plaintext}\}$.
- 2 Step two: Then Bob chooses random number $k \in \mathbb{F}_p$ and sends $(x, y) = (kP, vP + kaP)$.
- 3 Step three: Alice can compute $y \hat{=} ax$ and checks vP in the table in order to find v .

Outline

- 1 E-Voting Protocols
- 2 Algorithms of Protocols
- 3 Numerical Results

Protocol

- ① Step Up: center chooses s, p, E_p and P where $s \in \mathbb{F}_p$ as its secret key and P as a primitive point on E_p . The center announced $h = sP$ as its public key in the bulletin board. Voters are registered and are given a secret key in order to prove their authentication.
- ② Vote Casting: voter i chooses random number $a_i \in \mathbb{F}_p$ and $v_j \in \{1, \hat{1}\}$. Then he/she sends $B_i = (B_{i,1}, B_{i,2}) = (a_i P, v_j P + a_i s P)$ with some proofs of authentication.
- ③ Tally Computing: The center computes and announces $s \sum_{j=1}^N B_{j,1}$ with a proof of authentication. So it can compute $(\sum_{j=1}^N a_j) s P$ and finally $(\sum_{j=1}^N v_j) P$ from $\sum_{j=1}^N B_{j,2} - s \sum_{j=1}^N B_{j,1}$. Next, $\sum_{i=1}^N v_i$ can be found according to the table $\{-NP, \dots, -P, 0, P, \dots, NP\}$ which is formed by the tallier.

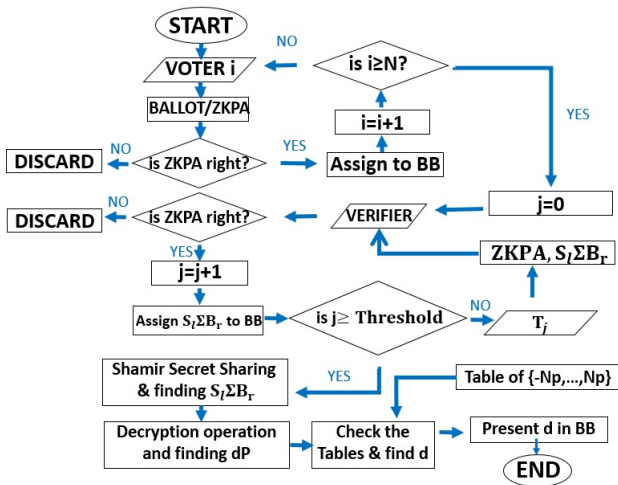


Figure: The flowchart of the protocol proposed in [2].

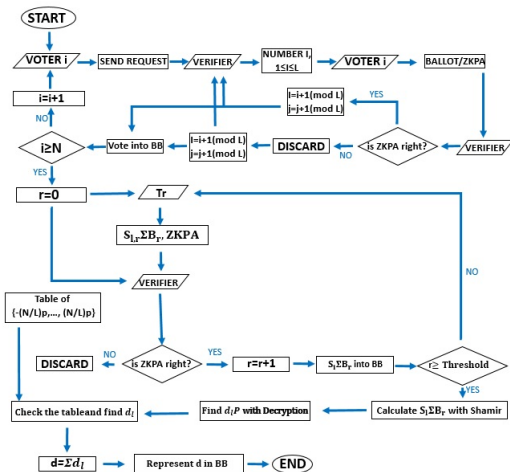


Figure: The flowchart of the proposed protocol.

Outline

- 1 E-Voting Protocols
- 2 Algorithms of Protocols
- 3 Numerical Results**

	Foo	Kim	Radwin	porkodi	Lee , Boyd	Weber	Proposed	Cramer	Hirt	JCJ	Meng
Fairness	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y
Eligibility	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Privacy	Y	Y	P	Y	Y	Y	Y	P	Y	Y	Y
Communication complexity	H	M	M	M	H	VH	M	M	H	M	VH
Random integer number	H	M	M	M	H	H	M	M	H	H	VH
Individual verifiability	Y	Y	N	Y	N	N	Y	Y	Y	N	N
Global verifiability	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Receipt-freeness	N	Y	N	N	Y	Y	N	N	Y	Y	Y
Robustness	N	N	N	Y	Y	Y	Y	Y	P	Y	Y
Coercion-resistant	N	N	N	N	Y	Y	N	N	N	N	Y
Efficiency	M	L	L	L	M	M	M	L	M	L	L

Y : Yes, N : No, L : Low, M : Medium , H : High, VH : Very High, P : Partially,

Table: The result of a voting for $M = 2$, $N = 200$, $L = 5$.

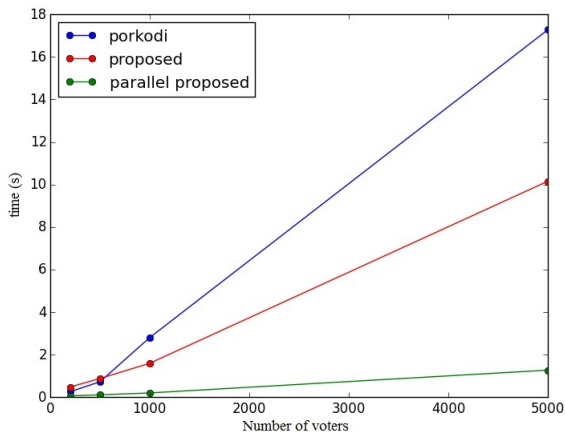


Figure: Time consuming of the proposed protocol with one server and multiple servers (parallel) and the protocol in [2] with $200 \leq N \leq 5000$.

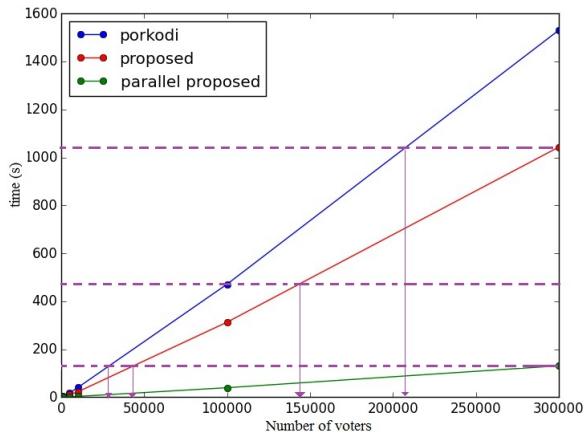





Figure: Estimated number of voters in the same time consuming in the proposed protocol with one server, multiple servers (parallel) and protocol in [2].

	192 bits	224 bits	256 bits	384 bits	521 bits
The proposed protocol	18.23 K	24.77 K	32.31 K	72.46 K	133.18 K
The protocol in [6]	20.35 K	27.23 K	35.12 K	76.69 K	138.90

Table: Memory consumption with 10 subsystems, 200 voters, and different prime numbers.

References

-  Cramer R, Gennaro R, Schoenmakers B. 1997. *A secure and optimally efficient multi-authority election scheme*. European transactions on Telecommunications. 8(5). pp. 481-490.
-  Porkodi C. Arumuganathan R. Vidya K. 2011. *Multi-authority Electronic Voting Scheme Based on Elliptic Curves*. IJ Network Security. 12(2). pp. 84-91.
-  Mousavi H., Ahmadi B., and Rahimi S. *A New Approach to Decrease The Computational Complexity of E-voting Protocols*. Transactions on Emerging Telecommunications Technologies 28.7 (2017): e3140.

Thank You

HMOUSAVI6@GATECH.EDU