Georgia Tech Shenzhen | GTSI Sustainability Expo Day

Secure Electronic Voting System Based on Zero-Knowledge Proof & Homomorphic Encryption

Haotian Chen[1], Xi Wang[2]
h.chen@gatech.edu[1] xwang3234@gatech.edu[2]

1. Introduction

Electronic voting(e-voting) is voting that uses electronic means to either aid or take care of casting and counting ballots . We designed and create a secure electronic voting system based on zero-knowledge proof and homomorphic encryption. The electronic voting system archieved crucial attributes include:

- **Security & Anonymity**: We employ cryptographic protocols like Zero-Knowledge Proofs and Paillier encryption, along with Shamir's Secret Sharing, to verify voter identity without revealing private information. This ensures both security and anonymity.
- **Auditability & Transparency**: Our protocol maintains meticulous documentation and uses cryptographic techniques (such as Zero-Knowledge Proofs and Homomorphic Encryption) for public verification while keeping votes confidential.

2. Overview

2.1 Role Definition

There are three roles in our evoting system.

- **Voter, also User:** The user represents an eligible voter who participates in the electronic voting process. Users cast their votes using the system.
- **Local officer, also Authentication Server(AS):** AS acts as an Local officer responsible for verifying the identity of voters, generate key pairs and and issue the unique ballot to the valid users.
- **Voting Center, also Counting Server(CS):** CS is responsible for collecting and counting votes.

2.2 Relaxation

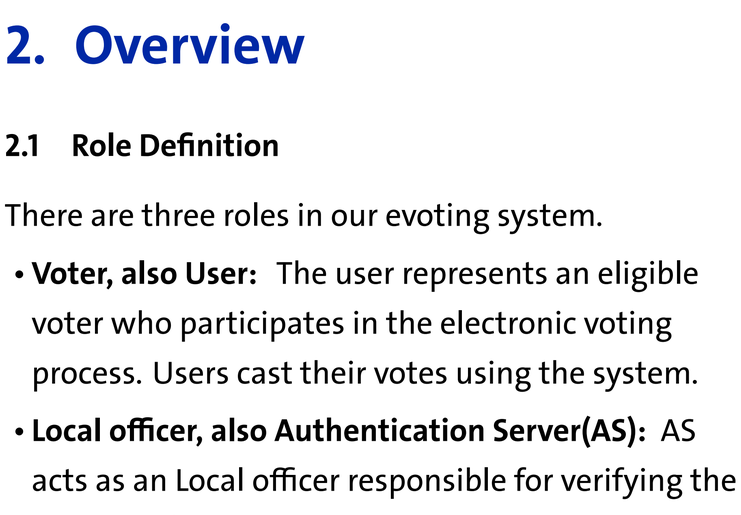

Figure 1: Process of the system

It is presumed that the AS is reliable, and the communication between the user, the CS, and the AS is secure.

2.3 Process

The system are mainly divided into three major phase:

2.3.1 Registration Phase

1. Users register using their email addresses.
2. Utilizing the Fiat-Shamir heuristic for non-interactive Zero-Knowledge Proofs (ZKPs), users generate a private key (x) and a public key ($h = g^x$).
3. The public key is transmitted to the CS.

2.3.2 Voting Phase

1. The registration process is terminated.
2. The AS employs Paillier encryption to produce a public key (e) and a private key (d).
3. The public key is documented, while the private key is distributed into secret shares corresponding to the number of valid users via Shamir's Secret Sharing.
4. Unique forms are created for each user, and these forms, along with the secret shares and public key information, are dispatched to the users.
5. Upon completing the form, users encrypt their voting information (m_{id}) using the public key (d) with Paillier encryption, resulting in the ciphertext (c_{id}).
6. A commitment for the ciphertext (c_{id}) is generated using the Fiat-Shamir heuristic for non-interactive ZKPs to validate the user's identity, and the ciphertext (c) is sent to the CS.

2.3.3 Tallying Phase

1. Voting is prohibited during this phase
2. The CS ascertains the legitimacy of each ballot.
3. Operations are conducted directly on the amassed ciphertexts ($C = c_1, c_2, \ldots$), with the sum ($s = \sum_{c \in C} c$) being computed.

2.3.4 Publication Phase

1. Users must input the key previously acquired from the AS. If a majority exceeding a specified ratio inputs their secret shares, the vote is deemed successful
2. The decryption key (d) is reconstructed using the gathered secret shares, the results are decrypted, and subsequently announced.

3. Applied Method

3.1 Zero-Knowledge Proof

We Use Fiat-Shamir Heuristic Zero-Knowledge Proof(Fiat-Shamir Heuristic ZKP) to validate the every collected ballot. The Fiat-Shamir heuristic is a method used to convert an interactive zero-knowledge proof (ZKP) into a non-interactive one. In a ZKP, one party (the prover) convinces another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself.

3.2 Homomorphic Encryption

Homomorphic Encryption: Encrypted computations with *Paillier's cryptosystem* allow secure vote tallying, leveraging the property $E(a + b) \equiv E(a) + E(b)$.
This property enables us to directly manipulate ciphertexts and count the ballots.

3.3 Secrete Sharing

We use Shamir's Secret Sharing to split a secret key(for decrypting the ballot) into multiple the number of valid voter parts and distribute it to voters. To be more specifically, We shard the key into shares equal to the number of users and distributed a key share to each user, attached in their unique ballot.

4. Conclusions

Our system exemplifies the integration of **Zero-Knowledge Proofs** and **Homomorphic Encryption** to fortify the security and preserve the anonymity of the electronic voting process. It upholds the pillars of democracy by ensuring a transparent and verifiable approach to e-voting, showcasing the efficacy of cryptographic protocols in safeguarding electoral integrity.

References

[1] Uriel Fiege, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 210–217, 1987.

[2] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 59–68, 1986.

[3] Mahmood Khalel Ibrahem. Integrated security protocol for electronic election system. *Journal of Information Engineering and Applications*, 7(1), 2017.