Encrypted Ballot

Rachit Kumar Pandey
IIT (ISM) Dhanbad

Description

The project aims to develop a secure voting system that ensures voters can cast their votes both anonymously and without the possibility of being traced back. It also uses partial trustees to ensure there is no single point of failure.

Stakeholders

Organizer

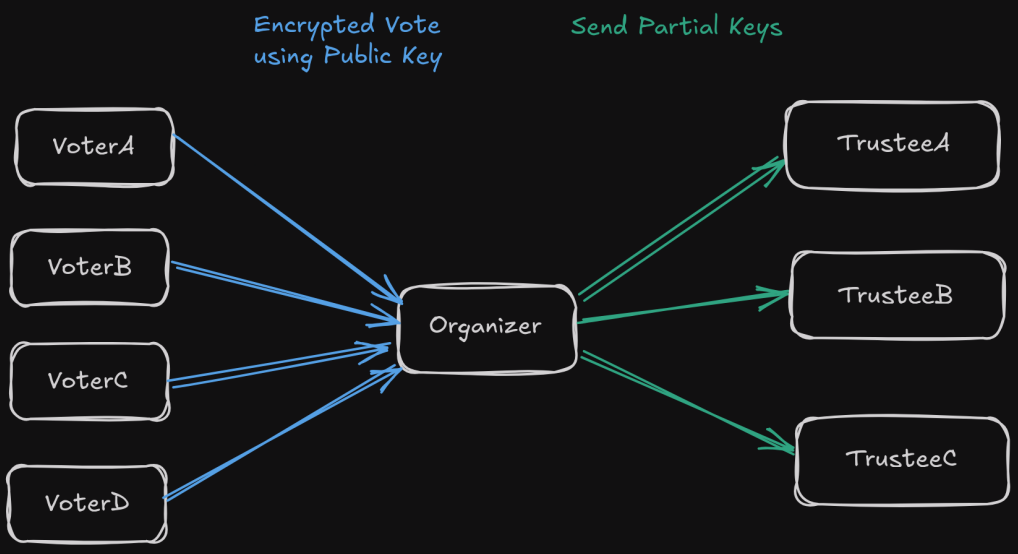
Role: Initiates and manages the election process. Distributes partial private keys to trustees.

Trustees

Role: Custodians of the election's partial private keys. Provide partial decryptions.

Voters

Role: Cast their votes in the election securely and anonymously



The Plan

Generate Public and Private Keys

Use a key generation algorithm (RSA) to create:

- Public Key: Used by voters to encrypt their votes.
- Private Key: Used for decryption, split into fragments for trustees.

Stage 0: Generate Election

- Set up the election by defining its options and securely generating partial keys for trustees to ensure decentralization.

Split the Private Key

- Use Shamir's Secret Sharing cryptography method to divide the private key into multiple fragments:
- Distribute fragments securely to trustees.

Registration Portal

- Make a portal to allow users to enter their information and password for registration.

Stage 1: Voter Registration

- Making a voter list based on user registrations using email and password.
- Hashing the email and password and storing them so private information is not leaked.

Password storage

- Hash the email and password (with a salt), and store them in a databse.

Login

- Authenticate the voter using their email and password
- Grant access to the voting interface if authentication is successful.

Stage 2: Casting Votes

- Allow the voter to securely login to the portal and choose their preferred candidate.
- Encrypt the vote using systems public key.
- Generate a receipt for the user.

Voter Anonymyzation

- Link votes to voter ID through a one-way hashing (SHA-256) ensuring vote anonymity while retaining the ability to audit voter participation.

Partial Decryption by Trustees

- Decrypt the encrypted result using the partial keys.
- Partial decryptions are combined to fully decrypt the result without exposing individual private keys or votes.

Stage 3: Tally and Result

- Use homomorphic encryption to tally the results without revealing individual votes.
- Publish the final tally.

Publish Final Results

- Publish the decrypted final tally.
- Publish the anonymized list of encrypted votes (and their hashes) so voters can verify their vote was included in the tally.

Tech Stack

Timeline

7th Dec - 11th Dec

Setup

Implement public/private key generation and Shamir's Secret Sharing.
Design a database for users, elections, and votes.

12th Dec - 18th Dec

Voter Registration

Build voter registration website with authentication (email/password).
Store hashed and salted user data in database.
Test registration.

17th Dec - 22nd Dec

Voting

Create a voting portal with encryption using the public key.
Implement vote anonymization.
Test the voting process and receipt generation.

23rd Dec - 24th Dec
1st Jan - 4th Jan
*see footnote [1]

Tally and Result

Perform partial decryption with trustee keys and publish results.
Make Dashboard to display results.
Conduct final tests.

About Me

Just a guy curious about tech.

My dive into this world began when I was around 15 years old. I wanted to understand how computers work, which led me to start learning basic digital electronics.

As I explored further, I discovered a completely different operating system that was said to be much closer to the hardware. Intrigued, I decided to wipe my hard drive clean and install Linux and fell down the rabbithole. I haven't gone back to Windows ever since.

I also had some experience with cryptography while learning about email encryption and hash verification. However, I never explored it much further, which is exactly why I chose this project.

Why Me?

I truly love this field and I'm really passionate about it.
I'm confident I can learn, grow, and contribute in the club effectively in the club.

Due to my impulsive nature, I can't commit any daily goal but I will commit about 30-35 hours per week. I'll also try to maintain and keep updated a Github repository linked here.

[1] I'll be going on a trip from 25th-31st Dec, I'll be taking my laptop along but I don't believe I'll be able to get any significant work done. Hence I've excluded that period from the timeline.