# e-voting protocol

## A. Overview

The e-voting protocol consists of the following six phases:

### 1. Registration phase

During the registration phase, voters provide their email and password. Upon registration, each voter is assigned a unique ID (derived from their email and password combination) and a key pair for linkable ring signatures (LRS). The voter's hashed ID is securely stored on the blockchain. This hashed ID serves as a reference for verifying the identity of the voter during subsequent phases of the voting process.

### 2. Pre-election Phase

During the pre-election phase, the election parties, typically a minimum of three, participate in an election session. Together, they collaboratively generate encryption keys required for secure communication and data handling during the voting process. Additionally, these parties work together to allocate tokens to registered voters and set submission limits.

The tokens allocated to voters are used to authenticate their identity and authorize their participation in the voting process. Each voter is assigned a certain number of tokens, and these tokens are linked to their hashed IDs, ensuring a secure and verifiable connection between the voter and their allocated resources.

Submission limits are established to regulate the number of times a voter can cast their vote. These limits serve to prevent fraudulent activities such as double voting or excessive voting, thereby enhancing the integrity of the election process. By setting these limits collaboratively, the election parties ensure fairness and transparency in the allocation of voting resources.

### 3. Authentication and login phase

During the authentication phase, voters present their unique ID and key pair for linkable ring signatures (LRS). The smart contract overseeing the authentication process then utilizes a Zero-Knowledge Proof (ZKP) known as a proof of membership to verify that the voter is included in the list of registered voters without disclosing their identity.

This proof of membership protocol allows the smart contract to validate the voter's eligibility to participate in the election without revealing any additional information about the voter's identity. By employing cryptographic techniques such as ZKPs, the authentication process maintains the privacy and confidentiality of the voter's personal information while ensuring the integrity of the election.

### 4. Voting phase

During the voting phase, voters request a token for each vote they wish to cast. After receiving tokens, voters select their choices for each question on the ballot. The chosen votes are then combined into a single encrypted ballot, containing the encrypted vote, encrypted token, and a signature. A smart contract verifies the correctness of the encryption on the ballot before storing it on the blockchain. This process ensures the security and integrity of the voting process, as all votes are securely recorded and stored on the blockchain for transparency and verification purposes.

### 5. Post-election phase

During the post-election phase, all election parties engage in the filtering process to maintain vote integrity and prevent tampering. This involves downloading encrypted ballots, adding dummy ballots for anonymity, grouping them, and selecting the highest index vote for each voter. Each party independently conducts this process.

Once completed, the results from each party are compared. If a predefined number of parties agree on the same outcome, the filtering result is considered valid and stored on the blockchain. To ensure the correctness of the shuffling process, a smart contract verifies the zero-knowledge proof (zk proof) of correct shuffling.

This phase emphasizes transparency, security, and consensus among election parties, culminating in the secure storage of filtered results on the blockchain, thereby ensuring the integrity and trustworthiness of the election process.

6. Taylling phase

During the tallying phase, at least three election parties collaborate to decrypt the encrypted votes. Each party decrypts a portion of the votes using their private keys. They then exchange zero-knowledge proofs of correct partial decryption to verify the integrity and accuracy of the decryption process. Once verified, the parties collectively perform the final decryption of the votes. The concatenated bit strings are analyzed to count the number of votes cast for each question. This process determines the outcome of the election. This process ensures the accurate tabulation of votes while maintaining the privacy and security of the election.

B. Key components of the e-voting protocol

The key elements of the e-voting protocol include:

1. Encryption: Use of encryption techniques, such as Paillier and ElGamal encryption, to securely transmit and store votes, ensuring confidentiality and integrity throughout the voting process.

2. Authentication: Employing linkable ring signatures (LRS) and zero-knowledge proofs (ZKP) for authentication, allowing voters to prove their eligibility without revealing their identity.

3. Token-based Authorization: Issuance of tokens to voters for vote authorization, ensuring that only eligible voters can cast their ballots.

4. Multiple Submission Limits: Implementation of submission limits to prevent fraudulent activities, such as double voting, while allowing voters to cast multiple votes within specified limits.

5. Collaborative Filtering: Engagement of multiple election parties in the filtering phase to enhance security and prevent tampering with the election results.

6. Verification Mechanisms: Incorporation of zero-knowledge proofs and mutual verification processes to ensure the correctness of decryption and tallying procedures while preserving voter privacy.

7. Blockchain Technology: Utilization of blockchain technology for transparent and immutable storage of encrypted votes, election results, and verification proofs, enabling universal verification and ensuring the integrity of the electoral process.

These elements collectively contribute to the security, transparency, and integrity of the e-voting protocol, providing voters with confidence in the fairness and accuracy of the election outcomes.

C. Role and usage of some crucial components of the e-voting protocol

1. Linkable Ring Signatures (LRS):

- Role: LRS enables voters to authenticate themselves without revealing their identity. It allows voters to sign messages anonymously while providing the ability to link multiple signatures to the same key.
- Usage: Voters utilize LRS to prove their eligibility as registered voters during the authentication phase. This ensures that only authorized individuals can participate in the voting process.

2. Tokens:
   - Role: Tokens serve as authorization mechanisms for voters to cast their ballots. They provide a secure and verifiable way to ensure that only eligible voters can participate in the election.
   - Usage: Voters request tokens during the voting phase to authenticate themselves and obtain authorization to submit their votes. Each token is uniquely associated with a voter and encrypted to maintain privacy.

3. Lookup Table:
   - Role: The lookup table is crucial for decrypting tokens securely during the post-election phase. It contains encrypted information necessary for verifying the authenticity of tokens without compromising voter privacy.
   - Usage: During post-election processing, the lookup table is utilized to decrypt tokens securely and validate their authenticity. This ensures that only valid votes are counted while maintaining the privacy of individual voters.

4. Filtering phase
   The filtering phase in e-voting application serves several important purposes:

   - Ensuring Integrity: The filtering phase verifies the integrity of the encrypted votes and detects any tampering or manipulation that may have occurred during the voting process. By comparing results from multiple parties, the system can identify any discrepancies and ensure the accuracy of the final tally.

   - Maintaining Anonymity: During the filtering phase, the individual votes are processed in a way that maintains the anonymity of the voters. This ensures that no voter's identity is revealed during the tallying process, protecting their privacy.

   - Preventing Fraud: The filtering phase helps prevent fraudulent activities such as double voting or unauthorized modifications to the vote tally. By employing cryptographic techniques and verification mechanisms, the system can detect and reject any invalid or suspicious votes.

   - Enhancing Trust: By providing a transparent and verifiable process for tallying votes, the filtering phase enhances trust in the integrity of the election outcome. Voters, election officials, and other stakeholders can have confidence that the results accurately reflect the will of the electorate.

5. Dummy ballots

Adding dummy ballots during the filtering phase serves several important purposes in the e-voting process:

- Preserving Anonymity: Dummy ballots help protect the anonymity of voters by making it difficult to identify individual voters based on the number or pattern of

votes cast. By mixing genuine votes with dummy ballots, it becomes more challenging for observers to discern the true voting behavior of any particular voter.

- Preventing Vote Tracking: Without dummy ballots, it may be possible for malicious parties to track the votes of individual voters by observing the sequence or timing of their submissions. By introducing dummy ballots, this tracking becomes less feasible, as it is unclear which votes are genuine and which are decoys.

- Enhancing Security: Dummy ballots help thwart attempts to manipulate the voting process by injecting noise into the dataset. This makes it harder for adversaries to discern legitimate voting patterns and devise effective strategies for tampering with the results.

- Maintaining Confidentiality: Dummy ballots contribute to the overall confidentiality of the voting process by concealing the true intentions of voters. This helps mitigate the risk of coercion or intimidation, as voters can cast their ballots without fear of reprisal.

D. Open issues
   1. Develop a secure method for storing the lookup table on the blockchain without compromising privacy. Currently, the lookup table resides in the database, but our goal is to eliminate the database in the final application.

   2. Establish a mechanism for verifying the proof of correct shuffling on the blockchain while maintaining privacy. This entails ensuring that sensitive information remains confidential during the verification process.

   3. Explore strategies to optimize gas consumption when storing tokens on the blockchain. This involves finding ways to efficiently manage token storage to minimize transaction costs.