Abstract
In our project, we have explored various schemes for conducting online elections, assessing them based on their feasibility and fulfillment of a number of criteria for a secure and accurate election.

We have constructed an implementation modeled on one scheme that we found to best satisfy the desired properties.

Online Voting Scheme Criteria

- **Eligibility**: Only eligible voters can vote, and they are only able to vote once.
- **Fairness**: No party can gain information about any intermediate results during the election.
- **Privacy**: The secrecy of each voter's vote should be maintained throughout the election.
- **Soundness**: Faulty or dishonest behavior by any participants does not cause any unreasonable delay or invalidation of the whole election.
- **Verifiability**: The announced result of the election can be checked by voters, and possibly any observers.
- **Receipt-freeness**: voters are unable to construct any receipt that can convince anybody of how they voted, so coercers or vote-buyers have no means of confirming that voters acted as they were instructed.
- **Coercion-resistance**: Extends upon receipt-freeness to prevent a number of additional coercion attacks.

Cryptographic Primitives

- **Mix Net**: Multiple participants each randomly re-encrypt and permute a list of data in sequence, in such a way that no observer, including the mixers themselves, can form any associations between the original and final lists.
- **Zero-Knowledge Proofs**: Proofs which demonstrate to a very high probability the truth of a statement, without revealing any other meaningful information.
- **Secret Sharing**: A method for distributing shares of data among multiple parties such that only a certain subset of the parties can combine their shares to recover the data.
- **Threshold El Gamal Cryptosystem**: Based on the difficulty of the discrete log problem. Secret key shared between multiple parties so that a certain subset must cooperate to successfully decrypt. Public and private keys generated in a distributed manner.
- **Threshold RSA Cryptosystem**: Based on difficulty of factoring large integers. Secret key shared between multiple parties.

Main Election Components

- **Bulletin Board**: Public information, proceedings and results of election are posted and can be seen and verified by any observer.

Conclusion
Our application provides a demonstration implementation of the Acquisti scheme that satisfies a majority of required criteria. There is still a great amount of work that would have to be done to provide a fully developed system for conducting online elections, such as implementing a more robust bulletin board system and a distributed RSA key generation protocol. Still, our implementation has given us a clear idea of what the main remaining challenges are to providing secure online elections.

Election Timeline

**Setup Phase**
- El Gamal key generation for both Votes and Credential key pairs
- RSA keys distributed
- Ballot and credential shares are posted to the BB

**Voting Phase**
- Administrators send credential shares to voters
- Voters download ballots from the BB
- Voters homomorphically combine their shares with the ballot of their choice and post it to the BB

**Tallying Phase**
- List of credentials is passed through a mix net
- RSA decryption of posted votes
- List of posted votes is passed through a mix net
- El Gamal decryption of mixed votes
- List of valid credentials is matched against the list of votes and tally is increased for corresponding vote choices

Application Screenshots

- **Voter Interface**
- **Administrator Interface**
- **Bulletin Board Interface**