

Zero-Knowledge Proofs for Secure and Private Voting Systems

24-25J-136

Project Proposal Report

Hussain M.R.S

BSc (Hons) in Information Technology specialized in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

August 2024

Zero-Knowledge Proofs for Secure and Private Voting Systems

24-25J-136

Project Proposal Report

Hussain M.R.S

Supervised by – Mr. Kavinga Yapa Abeywaradana

BSc (Hons) in Information Technology specialized in Cyber Security

Department of Information Technology


Sri Lanka Institute of Information Technology - Malabe

August 2024

Declaration


Declaration

We declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
Hussain M.R.S	IT21361654	

The supervisor/s should certify the proposal report with the following declaration.

The above candidate is/are carrying out research for undergraduate dissertation under my supervision.

Supervisor	Date	Signature
K.Y. Abeywardena	22 nd of August 2024	

Abstract

The rapid evolution of electronic voting systems has revolutionized the electoral process by significantly enhancing efficiency and accessibility. However, these advancements bring new challenges, particularly concerning security, privacy, and vote verification. This research addresses these challenges by proposing a novel Zero-Knowledge Proof (ZKP) protocol designed to improve electronic voting systems. The primary objective is to develop an e-voting system that ensures robust voter privacy and comprehensive verifiability while optimizing zk-SNARKs for performance and scalability in large-scale elections.

The proposed system leverages zk-SNARKs to offer cryptographic receipts that guarantee vote privacy without revealing the voter's choice. This approach aims to address significant issues such as software errors, hacking, insider threats, and the inherent difficulties in maintaining voter anonymity within electronic systems. Through a modular design, the system integrates advanced cryptographic techniques to generate and verify proofs efficiently, ensuring that votes are counted accurately and securely.

The feasibility of the proposed system is supported by its ability to handle national-scale elections, providing transparency and independent verification of results. The research highlights the need for an e-voting solution that balances privacy, security, and scalability, filling a critical gap in current systems. By addressing these challenges, the proposed ZKP protocol promises to enhance the integrity of electronic voting and restore public trust in the electoral process.

This study contributes to the field by presenting a scalable, privacy-preserving e-voting system that meets the demands of modern democratic processes, ultimately ensuring a secure and reliable electoral system.

Table of Contents

Declaration	3
Abstract	4
Table of Contents	5
1. Introduction	6
Background and Literature Survey	6
Traditional Voting Systems	7
Electronic Voting Systems	7
Avoiding Privacy Issues.....	7
Literature Review.....	8
Research Gap	9
Research Problem	9
2. Objectives	10
Primary Objective	10
Specific Objectives	10
3. Methodology	11
Components and Interactions.....	12
Overview of the Process	15
4. Project Requirements	16
Functional Requirements	16
Non-Functional Requirements	16
Expected Test Cases	16
5. Feasibility and Budget Justification.....	17
Feasibility Report.....	17
1. Technical Feasibility	17
2. Economic Feasibility (Budget)	17
3. Operational Feasibility	18
4. Legal and Regulatory Feasibility	19
5. Conclusion	19
6. References	20

1. Introduction

Electronic voting has undoubtedly reshaped the electoral process in recent years with its substantial improvements in efficiency and accessibility. However, this shift introduces new challenges concerning security, privacy, and vote verification. Addressing these challenges effectively is essential to maintaining the integrity of the electoral process and gaining public trust.

Despite their advantages, electronic voting systems are not without flaws. Issues such as software errors, hacking, and insider threats pose significant risks to the security of the election process. Moreover, safeguarding voter privacy within electronic systems is particularly challenging. Unlike traditional paper-based systems, where physical barriers generally help maintain voter anonymity, electronic systems face numerous obstacles in preserving the confidentiality of individual votes.

Recent research has investigated several cryptographic techniques to address these concerns, particularly Zero-Knowledge Proofs (ZKPs) and zk-SNARKs. These techniques hold considerable promise for enhancing privacy and security in electronic voting systems. ZKPs allow for the verification of a vote without revealing the voter's choice, thereby addressing significant privacy issues [1]. However, challenges related to scalability and efficiency remain, particularly for large-scale elections [2].

This research proposes the development of a novel ZKP protocol designed to tackle these issues in electronic voting systems. The goal is to combine maximum verifiability of the vote tally with robust privacy protections for each voter. The proposed system will focus on creating an e-voting solution optimized for national-scale elections, improving the performance and scalability of zk-SNARKs. Given the expectations for end-to-end verifiable e-voting systems in modern democratic processes, this solution aims to be both robust and privacy-preserving.

Background and Literature Survey

The integrity and fairness of any electoral process underpins democratic societies. Voting has changed over the years since the time of simple hand-counted paper ballots to the present day, which people have learned to depend on for ease and access to votes, creating complicated electronic voting systems. But with these steps forward comes a huge set of new challenges in ensuring security, privacy, and verifiability of the votes.

Traditional Voting Systems

Traditional paper-based systems, though simple, have their own set of vulnerabilities such as ballot stuffing, tampering, and human error in counting the votes. Even though, quite often, they are transparent at most times, due to the mere virtue of physicality, they are not immune to manipulations [3].

Electronic Voting Systems

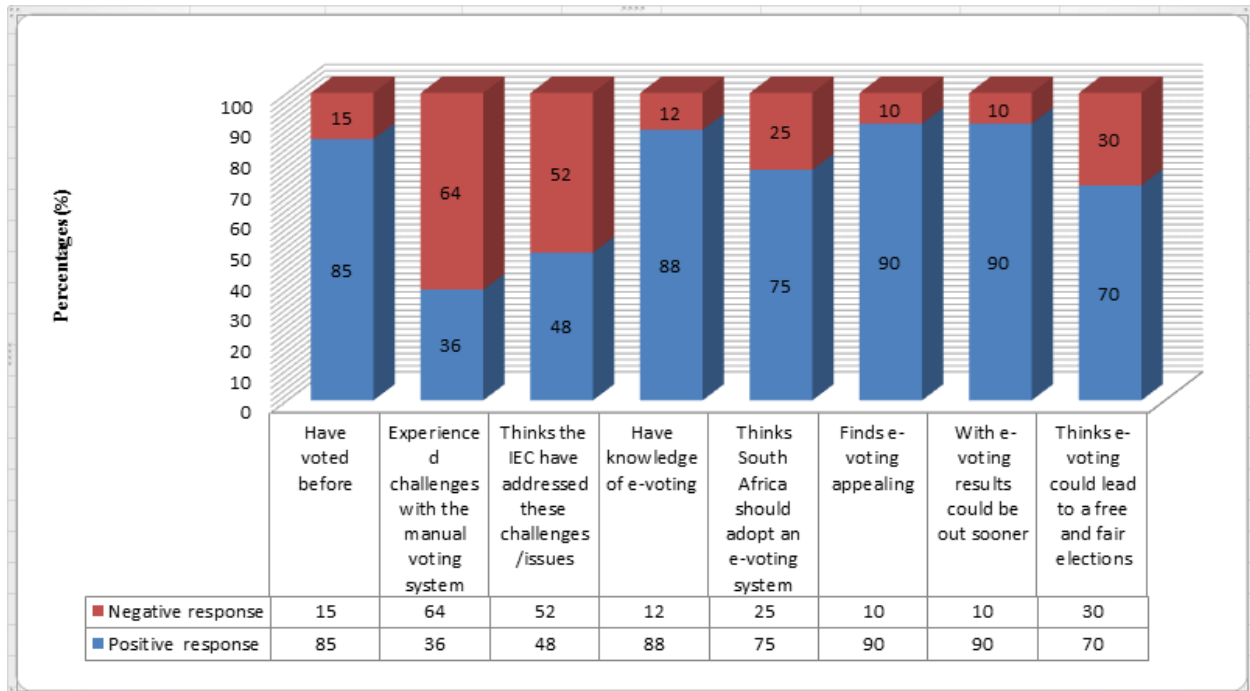
Switching the method of voting was supposed to reduce some of the problems encountered in manual counting, not to mention reducing the time it takes in ballot. The systems, though, have also brought along various risks. For instance, in the 2004 US presidential election, electronic voting machines were associated with massive criticism revealing the number recorded by them because many of these machines had software errors that lost thousands of votes [3].

Security Concerns in E-Voting: Security is one of the most critical issues and the most sensitive in e-voting. Electronic systems can be compromised in many ways, from simple hacking and random malware to rootkits, including various cyber dangers, and thus wrecking the integrity of these elections [4]. In addition to that, there may be cases of insider threats where individuals with access to the system may tamper with the results [5, 3].

Avoiding Privacy Issues

As discussed, traditional and electronic voting systems had their own share of issues, but another critical issue E-Voting faced is maintaining voter privacy. In the traditional system, some sort of physical barrier is there between the choice of the voter and the voter identity. In the Electronic System, this sort of separation is hard to execute. It is very important that the assurance of the guarantee of confidentiality with respect to a voter's choice be made sure for the fairness of the elections [6].

All things aside when it comes to voting the main focus is how many people voted, how many were counted, and how many are valid. The Security part is what needs to be done in order carry out the above mentioned processes without any hindrance or any manipulations. Most researches show that people are not wary of electronic voting as one might suspect, many welcome as an advancement in technology. The below findings were on peoples opinion on the matter of E-Voting.



This section was to understand the current stand of E-Voting, the next section will discuss how will incorporating the Novel ZKP algorithm will help with securing the E-Voting systems and meet people's needs.

Literature Review

With such respect, great research is done to counter such challenges. Homomorphic encryption and Zero-Knowledge Proofs (ZKPs) are certain cryptographic techniques proposed to solve a few of the privacy and security issues in an e-voting system. For instance, a verifiable secret-ballot election whereby the votes can be verified without uncloaking the voter's choice of an individual has been proposed by Benaloh and Tuinstra.

Zero-Knowledge Proofs, and mainly zk-SNARKs, are incredibly promising ways of preparing to control the privacy and safety in e-voting. Such proofs allow an entity to prove to another that a statement is valid without leaking any information regarding the statement except for its validity [7]. In the context of e-voting, zk-SNARKs can also be used to prove that a vote has been cast and counted without leaking the choice of the voter [1].

Research Gap

Though cryptographic techniques have greatly improved, challenges remain significant within existing e-voting systems. Most such systems either sacrifice privacy for verifiability or, as observed, turn out to be rather complex and resource-intensive, hence not practical for large-scale elections. For instance, the Helios Voting system provides end-to-end verifiability but somewhat fails to address the coercion of voters and privacy issues in the presence of a powerful adversary [3].

Besides, existing implementations of the ZKP in e-voting have a scalability and efficiency limit. These limits hamper ZKP-based voting system acceptance in realistic elections, particularly in large democracies where millions of votes need to be handled timely [8].

This research, therefore, will bridge this gap by coming up with a scalable, privacy-preserving e-voting system that makes use of zk-SNARKs in rendering full verifiability while ensuring confidentiality of the voter. The resulting system will be designed efficient enough to handle large-scale elections without compromising security or privacy.

Research Problem

The main problem addressed by this research is to have an e-voting system that satisfies voter privacy, system security, and comprehensive verifiability requirements, while being able to scale up and handle national-level elections. Most current systems sacrifice way too much for one or more of these aspects or are too complex to implement them effectively. For this gap, the solution is penned down as the development of a novel ZKP protocol for providing cryptographic receipts for private vote verification, enabling the independent audit of the vote tally without compromising privacy [9].

2. Objectives

Primary Objective

1. Ensuring Voter Privacy through ZKP Protocols:
Develop a Zero-Knowledge Proof protocol that ensures voter privacy by providing the cryptographic receipts necessary for vote verification, though not leaking the vote itself.
2. Ensuring Comprehensive Verifiability
This would ensure the existence of a system capable of not only independently verifying the vote tally but simultaneously managing to secure each voter's individual vote[6].
3. Improve Performance and Scalability:
Optimize zk-SNARKs for performance and scalability in zk-SNARK based e-voting to make it suitable for real large-scale elections[8].

Specific Objectives

- To Develop a cryptographic architecture for a secure ZKP-based voting system.
- Design of techniques for generation and verification of proofs in ZKP in an efficient manner of proof generation and verification.
- Test the system over common security threats in a simulated environment, such as replay, double voting, and collusion.
- Evaluate the scalability of the system to make it usable in any national election.
- Compare the proposed system with existing e-voting systems in terms of security, privacy, and efficiency.

3. Methodology

The project described here an e-voting system to be developed following state-of-the-art cryptographic primitives based on Zero-Knowledge Proofs, assuring that the voter's identity is not disclosed while casting and counting the ballots. More in precise terms, the system structure would have the following components:

1. **Cryptographic Primitives:** zk-SNARKs will be the setting of the zero-knowledge proof in the system. More specifically, this will be a cryptographic primitive used to allow efficient creation and verification of proof. It will be used for proving that a vote is cast correctly and that it has been included in the final tally without revealing the vote itself [10].
2. **Protocol Architecture:** Modular design of the system is ensured; it has distinctive components for the casting of voters, vote verification, and result tally. For every component, secure designs are ensured in their interaction with each other such that at any point of the voting process, no information is leaked at all [7].
3. **System Diagram:** A detailed system diagram will be provided showing how data flows from casting a vote to counting one. It will point out the ZKPs of each part of the system, and exactly relate how privacy and verifiability are taken care along the way.

VerifiedVoterDatabase

Intent: To persist data for a verified voter.

Interaction: In the case of successful verification, the voter data is saved with usage of storeVoterData().

VoterAccessesPlatform

Intent: The verified voter accesses the voting platform.

Interaction: The voter uses the voting platform to vote.

ServerReceivesVote

Intent: To receive and process the cast vote.

Interaction: The castVote() method is invoked, and the server acknowledges the vote cast with confirmVoteCast().

Security: It incorporates secure communication channels, such as HTTPS, to protect the vote data.

GeneratesZKProof

Operation: Generates a Zero Knowledge Proof for ensuring integrity and confidentiality in the vote.

Interacts: The generateZKSNARK() function makes some cryptographic computations to generate the proof, and this produced proof is then assembled using storeProof().

CryptographicReceiptCreated

Operation: It develops a cryptographic receipt that will be made out of the ZKP.

Interacts: generateReceipt() initializes the receipt, and voter receives it through receiveReceipt().

AllVotesCollected

Operation: Collected all votes for counts.

Interaction: This component enables all the votes to be stored securely and kept ready for counting.

StoredOnBlockchain

Function: Stores the vote data on a blockchain for immutability and transparency.

Interaction: Every single vote along with its proof is appended to the blockchain.

PublicVerificationInterface

Function: A public interface for independent verification.

Interaction: Verification of results is possible publicly using the method verifyResults().

ReceiptSystem

Function: Manages the issuing and storing of cryptographic receipts.

Ensures every voter that a verifiable receipt of their vote is given.

TallyingAlgorithm

Function: Securely tally the votes.

Interaction: This ensures that each vote is accounted for precisely by its proof through useProofForTally and updates the tally through addTally.

Verification: The final results are verified and made public through resultsVerified().

Overview of the Process

Voter registration: The voters register, and their identities are known.

Vote casting: The verified voters vote through a secure online portal.

Zero-Knowledge Proofs Generation: These are generated to secure the vote. Cryptographic

Receipt Issuance: Each voter will get cryptographic receipts about his/her vote. Vote Tallying:

Votes shall be securely summed up with the proofs. Verification: The final result shall be verified publicly using the blockchain.

4. **Security Measures:** The system will incorporate various security levels that will work toward protecting the system from both outside and inside attackers. This will be achieved through the encryption of all the communication to ensure its security, secure storage of the cryptographic keys, and audit at an interval specified on the integrity of the system [2].

4. Project Requirements

Functional Requirements

- The system shall allow the voters to vote without having to disclose their identity [4].
- Able to produce cryptographic evidence that the counting of votes is correct [10].
- Can be subject to independent checking on the outcome of the election.
- Allow voters to easily verify that their vote has been taken into the tally without loss of voter privacy

Non-Functional Requirements

- **Scalability:** The system should be able to handle national-level elections and handle the process of millions of votes [2].
- **Security:** The system should be robust to a majority of the security threats, including cyber-attacks, vote manipulation, and unauthorized access [3].
- **Usability:** The system should be so user-friendly that voters should be able to cast their votes without requiring advanced technical knowledge [5].
- **Performance:** The system will operate in a time-bound manner and warrant the counts of votes be done at the right time and with preciseness [7].

Expected Test Cases

- **Vote Integrity Test:** Make sure each vote is counted precisely once and that no vote is modified after it is cast.
- **Privacy Test:** Ensure that no information about who the voter chose can be known from the system.
- **Scalability Test:** Simulate mass elections to check the performance of the system under tremendous load/test.
- **Security Test:** Do pen testing to prove the possible vulnerabilities, immediate fixes, and provide mitigation for them; and to check if the system can be hacked [9].
- **Usability Test:** Gathers users' feedback to make sure that the system is friendly and easy to use.

5. Feasibility and Budget Justification

Feasibility Report

1. Technical Feasibility

1.1 Architecture of the System and Its Components

The proposed e-voting system capitalizes on modern cryptographic techniques, more specifically, zk-SNARKs, for preserving vote secrecy and ensuring the security of the system. The system architecture chiefly consists of the following components:

Voting Software: User-friendly software for voters, administrators, and auditors.

Cryptographic Engine: zk-SNARKs complexity for anonymity and verifiability .

Infrastructure for Database Management: Stacks for storing votes and cryptographic proofs .

Audit Tools: Independent tools for cross-verification to ensure transparency.

1.2 Technical Skills

This is a very confident task because it requires the knowledge of cryptography, namely zk-SNARKs, which secure voting schemes require, and the experience in developing such systems. The state of available research and current implementations creates a solid background for the development of proper cryptographic algorithms and their integration into the system.

1.3 Technology Availability

Also, all the necessary technologies are available and accessible. This includes cryptographic libraries and database management systems. Modern programming languages and their corresponding development frameworks are capable of supporting the development of secure, scalable applications, so technically, the proposed system is viable. Mainly the resources available as Open softwares and cloud servers will give the most availability and will also help in cost reduction.

2. Economic Feasibility (Budget)

2.1 Cost Estimates

The cost estimates to be incurred in the development and implementation of the e-voting system are as follows:

Software Development: Cannot confirm as this is personally developed

Cryptographic Algorithm Implementation: Personally implemented

Hardware: Personal devices and Hardly require hardware, using cloud servers

Cryptographic Key Secure Storage Devices: Cloud Databases (Around 50,000)

Testing: Done personally

Miscellaneous Costs: To be determined based on project-specific needs.

The allocation makes sure that all the fundamental development, testing, and deployment aspects fall under budget with an intense focus on security, scalability, and usability.

2.2 Return on Investment (ROI)

There are several benefits related to the investment in a strong e-voting platform:

Increased Efficiency: A process that is streamlined in nature can help reduce the cost of administration and the time taken to get it done.

Enhanced Security and Privacy: This feature will increase public confidence in the election process and lower the risk of fraud.

Scalability: Through proper design, the system can be enabled to carry out large-scale elections, hence may increase applicability in various jurisdictions.

3. Operational Feasibility

3.1 User Acceptance

The design of the e-voting system should be user-experience-centered for the system to be easy to use by all; from the voters to administrators and auditors alike. Support through user training will be important in enhancing workability.

3.2 Interaction of the System with Other International Systems

There are several challenges in the interaction of the e-voting system with other requisite already-existing international systems, namely data migration and the system compatibility that usually has to integrate with already existing systems. This is usually referred to as the legacy issue. Careful planning with phased implementation would take care of these problems.

Technical issues would be dealt with, security protocols would be upgraded, and the system's reliability would be assured through ongoing maintenance and support. Operational effectiveness can be guaranteed by a dedicated support team, coupled with regular updating of the system.

4. Legal and Regulatory Feasibility

4.1 Compliance

The e-voting system would have to be in tandem with legal and regulatory requirements for election security, privacy, and data protection. This will be achieved by going over relevant legislation and seeking collaboration with legal experts to ensure conformance to standards.

4.2 Certification

Obtaining certification from relevant authorities may be necessary to validate the system's security and reliability. This process will involve thorough testing and evaluation by independent entities.

5. Conclusion

The proposed development of ZKP algorithm for e-voting system is thus technically and economically feasible and realizable, provided the appropriate technology, expertise, and budget suitable for its development and implementation. It possesses peculiar benefits in terms of safety, privacy, and efficiency, and can therefore be used as an answer to modernization problems in the process of elections. As to operational considerations such as user acceptance and integration into the system, these will be controlled by careful planning and support. Review and certification will ensure legal and regulatory compliance.

As such, the feasibility study supports an argument for developing the proposed e-voting system: it points out all the potential advantages of this development and even suggests the ways to successfully meet the most important challenges in its implementation.

6. References

- [1] A. E. a. G. Ekbatanifard, "Z-Voting: A zero knowledge based confidential voting on blockchain," in *8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, Mashhad, Iran, 2024.
- [2] A. M. a. R. K. Dwivedi, "Designing A Secure Large Scale E -Voting System Leveraging Sharding Blockchain with Interoperability Protocol and Consensus Mechanism," in *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bangalore, India, 2024.
- [3] A. H. a. E. Teague, "Security flaws in electronic voting systems," in *USENIX/ACM Symposium on Networked Systems Design and Implementation*, 2005.
- [4] A. J. N. M. a. P. O. S. S. Chaeikar, "Security Principles and Challenges in Electronic Voting," in *IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)*, Gold Coast, Australia, 2021.
- [5] D. C. a. E. V. Heyst, "Group signatures," in *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, 1991.
- [6] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, 2015.
- [7] I. B. Y. H. M. R. Eli Ben-Sasson, "Scalable, transparent, and post-quantum secure computational," Israel Institute of Technology, Haifa, Israel, 2018.
- [8] Z. Z. W. J. H. B. Z. Xuanming Liu, "Scalable Collaborative zk-SNARK and Its Application to Efficient Proof," National University of Singapore, Singapore, 2024.
- [9] A. D. P. P. F. G. L. R. M. M. Vincenzo Agate, "SecureBallot: A secure open source e-Voting system," *Journal of Network and Computer Applications*, vol. 191, p. 103165, 2021.
- [10] S. P. Bimal Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server," *Journal of Information Security and Applications*, vol. 59, 2021.