World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-11, Issue-4, October 2021 Pages 12-18

Design of A Coercion-Resistant Electronic voting Protocol Using Homomorphic Encryption

Chizalum E. Echeta, Moses O. Onyesolu

***Abstract*— With the relevance of elections to democratic governance, it is imperative that voters have full confidence in the electoral process. By eliminating the risks of vote buying, voter coercion and increasing voter inclusion, people can have more confidence in elections and this study proposes an electronic voting scheme that achieves this. The electronic voting scheme proposed here draws its security properties from a cryptographic voting protocol based on homomorphic encryption. The additively homomorphic properties of the Paillier cryptosystem are combined with a multi-party election authority to receive and tally votes in encrypted form. Furthermore, this electronic voting scheme is implemented as a web-based app, using the JavaScript programming language, allowing users to vote from any geographical region with the aid of a computing device and an Internet connection. The proposed voting scheme is suitable for multi-candidate elections with any number of voters and achieves vote confidentiality, reliability and efficiency.**

CCS CONCEPTS

• Security and privacy → Privacy-preserving protocols.

***Index Terms*— Privacy-preserving, Homomorphic encryption, electronic voting, Data security.**

I. INTRODUCTION

Democracy is one of the five forms of government existent in the world today. One major characteristic of a democratic government is the possession of the power and civic responsibility, by all adult citizens, to elect their representatives by means of an electoral process, otherwise known as voting. In the history of mankind, voting procedures and technologies have undergone various phases of evolution, from clay balls put in clay pots in ancient Greek society;to paper ballots used in more recent democratic societies, to the use of electronic devices in modern polling stations. With each evolution, the goal has been to make voting an inclusive, well-structured and trustworthy process. This process should have an appropriate amount of participation by the governed, with results accurately reflecting the wishes of the voters/general population.

According to Treshel et al. [31], many countries are currently considering the introduction of e-voting systems with the aim of improving various aspects of the electoral process. E-voting is often seen as a tool for advancing democracy, building trust in electoral management, adding credibility to election results and increasing the overall efficiency of electoral processes. The technology is evolving fast and election managers, observers, international organizations, vendors and standardization bodies are continuously updating the methodologies and approach taken to achieve efficiency. Properly implemented e-voting solutions can eliminate certain common avenues of fraud, speed up the processing of results, increase accessibility and make voting more convenient for citizens.

In some cases where it has been implemented and used over a series of electoral events, a reduction in the cost of elections or referendums have been recorded in the long term. For instance, Alvarez et al. [2] states that Estonia became the first country in the world to have nationwide local elections where people could cast binding votes over the Internet in October 2005. This world premiere was then followed by its use in the nation's parliamentary elections in 2007, in which the number of Internet voters reached 3.4% of the total number of eligible voters. Internet voting has also been trialed in a bunch of developed countries such as the Netherlands, France, Switzerland, the United Kingdom and the United States of America, Haynes [12].

With the Internet being an integral part of everyone's lives these days, coupled with the relative success which electronic voting has achieved thus far, it is quite easy to predict that we will see higher mass adoption levels of electronic voting going forward. Also, higher preference will be given to remote voting over the Internet, carried out using personal computers or portable devices.

For all the benefits which Internet voting offers, a critical factor which would play a role in its acceptance and adoption as a credible means of voting, capable of replacing manual systems is security. The millions of voters, who are eligible to cast votes in order to elect their chosen leaders need to be confident that the election process being participated in is democratic and fair. Consequently, the conversations to be had about Internet voting include the pitting of potential rewards against the security risks involved. In order to mitigate these risks, diverse researchers have come up with varied cryptographic functions to be used in achieving secure Internet voting systems. One of such cryptographic functions involves the use of homomorphic encryption, which shall be used in this study to construct a cryptographically secure voting protocol, which achieves coercion resistance.

Encrypting data has become widespread lately and is seen to be used in the technology stacks for emails, instant messaging applications such as WhatsApp and Telegram as well as in online banking applications. The introduction of encryption to these technology stacks has helped build trust in them and made them commonplace. In the same vein, there is need for encryption to be applied to voting systems, albeit in a different manner.

Ideally, when encrypting data, a conventional encryption

Chizalum E. Echeta, Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria
Moses O. Onyesolu, Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria

algorithm is used to convert the data from plaintext to a ciphertext. The ciphertext is then sent across to the receiving party. The receiver has to decrypt this data before computations can be performed on it. If a reply has to be sent to the original sender, the data has to be encrypted once more, before re-sending. Flemming (2020) posits that static data, such as just described cannot be used for so much. But then, if there was a way to perform calculations on that data without first decrypting it, a whole new world of possibilities begin to present themselves. While the only computation you can perform on regular encrypted data is to decrypt it, with homomorphic encryption you can perform various algebraic computations on encrypted data without having to decrypt beforehand.

Even though homomorphic encryption provides provable security based on some computationally hard problem, it is usually associated with huge computational overheads when compared to other privacy enhancing technologies. The choice of implementing a homomorphic scheme depends on the specific problem scenario and how much utility can be traded in for the privacy guarantees. In this case, election votes can be reduced to ones and zeros. For a case where a voter has selected a particular candidate, this case can be likened to a 1, and a case where a voter has not selected a particular candidate, the case can be likened to 0. Tallying said election votes would simply imply performing an addition operation on all the cases which have selected 1 for individual candidates.

In this study, homomorphic encryption will be used together with the Paillier cryptosystem to tally encrypted votes. The Paillier cryptosystem is an additively homomorphic scheme and can be used to perform addition operations. The construction designed in this work will have a multi-party election authority to collate and tally the votes in order to achieve a redundant and robust system.

Internet voting should be the holy grail of voting during elections because it has the potential to increase voter participation, convenience and create a sense of trust and belief in the authenticity and purity of electoral processes. However, this is seen to not be the case as voters have fears of interference from influential parties, voter coercion, vote rigging, buying and vote manipulation by the electoral authorities. In order to mitigate these risks, votes have to be properly secured. To this end, many researchers have conducted research into ways of securing Internet voting systems using methods such as biometric authentication, hardware tokens and more recently cryptographic functions.

The use of cryptographic functions such as homomorphic encryption has been proposed but, in most cases, research carried out has not been implemented using prototypes. In other cases, the methods used to construct the cryptographic protocols have computational times that are higher than average. The protocol construction used in this study, will use homomorphic encryption in a multi-party setting to create a protocol that is computationally light and efficient. Furthermore, this protocol will be implemented using a web-based voting system built from the ground up. This system will be able to secure votes by encrypting them, tallying the encrypted votes and publish the encrypted votes.

Contribution: In this work, we design and implement a coercion-resistant electronic voting protocol using homomorphic encryption. Our motivation is drawn from a need to obtain a highly efficient web based electronic voting system that can be applied in a real-world scenario. In order to achieve this, firstly we develop a cryptographically secure electronic voting protocol. Then apply the cryptographic voting protocol that has been developed, in the design of a web based electronic voting system. The implementation of this web based electronic voting system will be built using the JavaScript programming language

II. RELATED WORKS

Gritzalis [11] believed that an electronic voting scheme should be run as a complementary scheme to traditional voting systems. The paper pointed out the functional security requirements of an electronic voting system as well as the non-functional security requirements of the system. According to the study, electronic schemes should respect generality, freedom, equality, secrecy and directness. In the Internet voting proposal by Querejeta-Azurmendi et al. [25], a re-voting approach was put forward as a means of achieving coercion-resistance. A voter is not expected to own any public or private keys and only authentication credentials are used. The proposed scheme leveraged on the Millionaire's protocol to satisfy the four requirements of a remote voting scheme which are universal verifiability, ballot secrecy, eligible verifiability and coercion resistance. The concept of everlasting privacy for achieving receipt freeness was proposed by Phillip Locker in Locher and Haenni [20]. This new voting protocol was the first to offer verifiability, everlasting privacy and receipt-freeness. If privacy is neither based on computational intractability like the impossibility of computing discrete logarithms or factoring large numbers nor on the availability of Tallying authority (TA), then the privacy is said to be everlasting in an information theoretical sense. This feature is a desirable property that can be used to avoid vote privacy violations by much more powerful computers, as computers keep growing in computational capability. The TA in this scheme is only required during the casting and tallying of votes, to prevent the casting of invalid ballots but not to guarantee vote privacy. In the same year, a new cryptographic protocol was presented by Locher, Haenni and Koenig [21], which achieved coercion resistance and everlasting privacy. This protocol was designed to have public verifiability, everlasting privacy and coercion-resistance as its security properties. The adversary/ coercer in this scheme is assumed to have an infinite amount of time and computational power to break vote privacy. The voters are authenticated anonymously using Zero Knowledge Proof by perfectly hiding commitments. Coercion-resistance is achieved based on a new mechanism for deniable vote updating. To evade coercion by submitting a final secret vote update, the voter needs not to remember the history of all precedent votes. The protocol uses two types of mix networks to guarantee that vote updating is not detectable by the coercer. Rønne, Atashpendar, Gjøsteen and Ryan [26] 's approach to election tallying is simply a version of the Juels et al. [16] protocol in linear- time using Fully Homomorphic Encryption primitives such as hashing, Zero Knowledge Proof of correct decryption and threshold cryptography. The proposed scheme tried to replace the Juels et al. protocol which runs in quadratic time with a solution that runs in

linear time. The scheme achieved better individual verifiability but a security analysis was not done on the protocol therefore protocol security was not deemed a guarantee. The scheme is claimed to be a novel application of fully homomorphic encryption to electronic voting. Ruan and Zou [27] carried out a survey of existing remote e-voting systems to see whether these systems satisfied three major security properties needed for a secure electronic voting scheme. The properties tested for were receipt-freeness, the ability to resist vote selling and voter-coercion resistance. The study is basically a comparison of the most prominent electronic voting protocols with respect to how the critical security properties required for large scale adoption of remote electronic voting systems are satisfied. Concerning the Hirt and Sako [14] voting scheme, it is seen to not be coercion-resistant. This is because the deceit tactic employed by the voter to evade coercion can be detected by the coercer. For the Lee and Kim [19] protocol, the tamper resistant device is seen to improve vote privacy but it is not coercion-resistant as the voters are not able to disguise themselves and are distinguishable by the coercer. The Juels, Catalano and Jakobsson [17] scheme submitted credentials and passed votes through a mixnet for anonymity. The scheme is coercion-resistant and efficient, but not entirely secure. Work done by Smyth [23] is another survey that explored the various definitions of coercion resistance and its applications in electronic voting. The survey discovered that only one of the schemes that had been developed so far is considered to not be a weak coercion resistant scheme. A weak system is defined as one that is not coercion-resistant. The survey results show that the existing electronic voting protocols have not met the definition of the security requirements for such systems. The study claims that a new and formalized definition of coercion resistance should be invented. The survey discovered that only the definition given by Küsters, Truderung and Vogt [18] satisfied the conditions to be called coercion resistant. This implies that, either all the other voting systems are not secure based on the definition, or the definition is too strong and overshoots the requirements for a coercion resistant system. By this discovery, the conclusion is that coercion resistance has not been formally defined and perhaps, a new definition should be found. This is proposed as a possible direction for future research. The paper by Augoye and Tomlinson [3] viewed electronic voting from a different perspective
– the real world issues and threats it is up against. It identified a few threats, then followed up with an analysis of voting schemes which have been trialed in Australia and Estonia. Recommendations are subsequently proffered on how to mitigate threats to the voting schemes upon deployment in real-world environments which are not trustworthy. Identified threat analysis of voting schemes fingers socio-economic factors such as religion, poverty, insider threats, cybersecurity and influence from foreign governments as capable of hampering the security and credibility of voting schemes. The paper recommends that electronic voting schemes be end-to-end verifiable from the authentication of voters down to the tallying of votes so that the votes can be deployed successfully in adverse environments. Cetinkaya [6]'s paper proposed a formal definition of the security requirements for cryptographic voting protocols as well as an elaborate checklist for each and every security requirement. PreFote was suggested as a building block to be used in the design of voting protocols. PreFote otherwise known as predefined vote, uses an intentionally prepared fake vote list where each PreFote possesses a unique code and an associated candidate from the list of candidates. The voter has a unique code and a set of PreFotes. At the end of the election, a voter uses a unique code for individual verifiability and checks if the vote is published on the list. According to Xia, Tong, Xiao and Chang [32], existing electronic voting schemes are designed either for high coercion environments or for high security. However, these schemes generally have one thing in common – they require ordinary voters to perform cryptographic functions. By definition, a practical voting scheme should be one in which voters need neither a trusted device, nor some special knowledge to be able to use the system. The paper proposed a new generic framework which is both practical and achieves receipt-freeness. It also meets three privacy requirements defined as: coercion-resistance, no vote buying and verifiability. The protocol uses a 2 number system that works in a similar way to the Maskballot scheme. Florentine square is applied in the voting stage to prevent adversaries from coercion and vote buying. Jamroga and Tabatabaei [15] provided a game theory-based approach to coercion resistance. No new protocol or old voting scheme was discussed in this paper. Instead, the focus was on the costs and benefits associated with parties involved in electronic voting. Consideration was given to whether a society should invest in protecting itself against coercion, if so, in what way and to what extent. The assumption being made is that all coercers are mumped into one entity. Elections are viewed as a 2-player game between the coercers and the society. The paper sheds light on the economic and social aspects of elections and deserves further work seeing as not much work has been done on it. Sampigethaya and Poovendran [29] viewed electronic voting as an emerging social application of cryptographic protocols. The study provided a framework which can serve as a reference sheet when designing or selecting voting schemes. The framework is illustrated in the analysis of existing electronic voting schemes. Schemes are classified into i. Hidden voter: voters submit votes anonymously; split into the token based and bulleting based system. Chaum [7] ii. hidden vote: voters openly submit encrypted votes [8] iii. hidden voter with hidden votes: voters anonymously submits encrypted votes [19] After comparing the schemes, there was no clear leader. The paper paints a clear picture of what conditions are satisfied by various schemes and influences what scheme are chosen for particular implementation needs. Selene is an end-to-end verifiable voting scheme by [28]. In conventional cryptographic E2E voting schemes, voters use encrypted ballots for vote verifiability. For all the transparency it provides, it requires voters and election officials to have some technical knowledge of cryptography. This scheme however, uses a unique, tracking number provided to each voter to achieve vote verifiability. The votes are published on a bulletin board alongside the tracking numbers assigned to voters. A few rules apply here: (1) no two voters have the same tracking number (2) a secure link is provided between voter and tracker. In order to avoid coercion resistance, the

voter only gets his tracking number after the votes have been published on the bulletin board. This scheme aims to put all the cryptographic technicalities of an electronic voting system under the hood and let the voter have a seamless voting experience while having no prior knowledge of cryptography. [9] described and analyzed the electronic voting protocol which was used in the Norwegian government in 2011 when Internet voting was trialed for local government elections. The protocol was designed by Scytl. The protocol is coercion-resistant and uses a multiple ballot system where the last submitted ballot counts as the valid vote. [16] defined an electronic voting scheme as coercion resistant if it is not feasible for an adversary to determine whether a coerced voter complied with their demands. The proposed scheme provides the first formal security definition for electronic elections of any kind. Fair degree of efficiency with an unusual lack of structural complexity models real life threats such as vote buying and vote cancelling. The scheme uses an anonymous channel during ballot casting and an untappable channel during the registration phase. To ensure vote privacy, a mixnet is used. Encrypted votes are posted to the bulletin board, signatures are checked then the cipher text is run through a mixnet. The scheme however is found to be vulnerable to three types of attack: the randomization attack, forced absentation attack and the simulation attack. In Schweisgut [30], the distinguishing factor of the proposed scheme is the use of pseudonomynisation of cipher texts to achieve permanent vote secrecy. The scheme achieves coercion resistance based on work done by Juels et al. (2005). The credentials used to authenticate voters are encrypted. A MIX-cascade is then used to omit the one time-consuming plaintext equivalence test (PET). [22] presented the minimal requirements for receipt-free elections without untappable channels between the voter and election authorities. Based on this requirement, a solution is proffered which is based on an encryption black box. Votes encrypted by an encryption black box are verifiable and also implemented using smartcards. The protocol is suitable for Internet voting. The requirements for receipt-freeness are (1). Use of private and authenticated channels, (2). Voter having no knowledge of the decryption key and (3) knowledge of the randomness used during the voting process. Receipt-freeness is achieved as it is impossible for the coercer to tamper with the encryption black box to access its randomness. To obtain both receipt freeness and efficiency in [1], the authors modified the voting scheme of [19] while improving on the optimistic mix net proposed by [10]. The scheme has an administrator tasked with providing randomization. This is similar to ballot encryption and then mixing at the voting stage. The protocol is lightweight as it uses single encryption. [13] proposed a receipt free voting scheme based on a third-party randomizer. The final ballot is generated by randomizing the first ballot and generating a proof of validity interactively with the voter. The randomizer generates the re-encryption proof in designated-verifier way and uses a divertible zero-knowledge proof technique to generate the proof of validity. Recently [4] proposed an efficient multicandidate electronic voting scheme based on the Paillier Cryptosystem in which the tallying stage is seen to be more efficient. [22] proposed a receipt-free electronic voting protocol using a tamper-resistant smartcard. The study pointed out the difficulty of implementing an untappable channel and introduced the necessity of using a tamper resistant device. While voting, the protocol smartcard plays the role of a mixer. The re-encryption proof is given in an interactive way, so the same attack applied to [19] is possible. The re-encryption proof should be given in a non-interactive way, with a designated verifier, such that it cannot be transferred to third parties. The voter should also not be able to construct a receipt. According to [14], the existence of an untappable channel from the authority to the voter is the weakest physical assumption for receipt-freeness. In contrast, implementing an untappable channel in a real world distributed environment is very difficult to achieve. If a physically isolated voting booth in a dedicated computer network is used to achieve receipt-freeness, it will cost a lot more and inconvenience voters since they have to be physically present at a particular voting booth. If the overall voting system is inconvenient, voter participation in electronic voting will yield little to no advantage. In order to increase participation in electronic voting, Internet voting has been earmarked as the most viable solution. A larger number of voters can participate in electronic voting via the Internet while being in any geographical location. For all the convenience which Internet voting offers, achieving receipt-freeness is considered difficult because the Internet is a ‘tappable’ channel open to eavesdropping and denial of service attacks amongst many more.

III. ELECTRONIC VOTING PROPERTIES AND BENEFITS

The electronic voting system being proposed is expected to offer the following important benefits

Increasing the level of participation: The convenience that an Internet voting system offers has the tendency to maximize user participation, by allowing them to vote from anywhere. The possibility of accessing the system using various computer systems and mobile devices equipped with Internet connection increases voter turnout for elections.

Auditability: The design of the system allows administrators to guarantee users that their votes are correctly issued and accounted for according to the intention to vote. In addition, votes cast are verifiable both on an individual level and by external observers.

Efficiency: The system offers the capacity to significantly cut down on organizational and implementation costs of organizing and running a manual based voting system. The efficiency in collation and publication of election results dwarfs that of the traditional paper voting system in comparison.

Precision: Using an electronic voting system eliminates errors encountered in manual based systems. The system offers accuracy and quick publication of results.

Reliability: The encryption protocol developed in this work allows the participation of independent observers that can verify the absence of election fraud and manipulation. Results are posted to a public bulletin board and equivalence algorithms can be used to verify that every vote is counted and accounted for on the bulletin board

- Faster result collation time: The primary advantage of an electronic voting machine is its speed. With

traditional paper methods, ballots must be collected and counted from polling stations. This process is time-consuming and delays the final result. With electronic voting, results are available almost instantly because votes are counted as they are cast. To calculate the final result, all the polling stations report their votes and they're all added together. By using e-voting, the results of elections could be available in a matter of hours rather than days, meaning elections could have a more instantaneous impact.

- Increase in voter turnout and participation: One other major plus of electronic voting is voter engagement. Many people fail to take advantage of their right to elect their officials. Electronic voting also allows for greater accessibility to people with disabilities. Currently, if a voter is unable to mark a paper ballots, an assistant is required to vote for them. This process compromises the person's right to cast an anonymous ballot. By bringing voting into the digital space, people who are unable to visit or use a polling booth can vote from home. This maintains voter anonymity and encourages the disabled and elderly to make their voices heard.
- Comparatively cost effective in the long run: Finally, the last major advantage associated with e-voting is a long-term decrease in expenses. Paper votes require electoral officers that count and transport votes, which can add up as stations around the country tally up the results. These expenses could put a major strain on an entity like a small, underfunded local government. Electronic ballot-counting machines can cut the cost of human counters, while Internet voting can also cut out polling location employees. The infrastructure can be re-used every election, so it would be a one-time purchase.

IV. PRELIMINARIES

In this sections, the cryptographic building blocks and the settings used in the construction of this protocol will be introduced.

A. *Homomorphic Encryption*

Homomorhpic Encryption (HE) allows for an arbitrary operation to be performed on ciphertexts, such that the resulting ciphertext would decrypt to the same value as would be obtained if a targeted algebraic operation were to be performed on the plaintext values. Let $EncP_k(\cdot)$ and $DecS_k(\cdot)$ represent encryption and decryption functions respectively. (m_1, m_2) are two messages and k is a scalar value, while $\boxplus$, $\boxdot$ and $\boxtimes$ are arbitrary operations on the ciphertexts. Then, homomorphism is defined in Equations (1) to (3) as adopted from [33]

$$DecS_k\left(EncP_k(m_1) \boxplus EncP_k(m_2)\right) = m_1 + m_2 \quad \textbf{(1)}$$

$$DecS_k\left(EncP_k(m_1) \boxdot EncP_k(m_2)\right) = m_1 \cdot m_2 \quad \textbf{(2)}$$

$$DecS_k\left(EncP_k(m_1) \boxtimes k\right) = m_1 \cdot k \quad \textbf{(3)}$$

B. *Paillier Scheme*

Paillier cryptosystem is an additively homomorphic scheme which is secure under the computational composite residuosity assumption as shown in Equations (1) to (3).

Given a public key, private key pair (*pk*, *sk*) respectively. *pk* := (*g*, *n*) and *sk* := $\Pi(n)$.

where $\Pi(n)$ is the Carmichael's function on *n*, defined as $\Pi(n) := lcm(p-1, q-1)$.

$$Encryption:\ c := Encpk(m, r) := g^m . r^n \bmod n^2 \quad \textbf{(1)}$$

where $\in Z^*_{n^2}$ *;* $n := p.q$*, such that p and q are distinct large primes,* $r \leftarrow Z^*_n$ *, g is generator of order n.*

Decryption: Given ciphertext c,

$$m := \frac{L_n\,(c^{\Pi} \bmod n^2)}{L_n(g^{\Pi} \bmod n^2)} \bmod n \text{ and } L_n(a) := \frac{a-1}{n} \quad \textbf{(2)}$$

Additive Homomorphism*:* Given two ciphertexts of messages m_0 *and* m_1, we can compute the sum as follows:

$$Enc_{pk}(m_0, r_0)\ x\ Enc_{pk}(m_1, r_1) := (g^{m_0} . r_0^n\ x\ g^{m_1} . r_1^n)$$
$$:= (g^{m_0+m_1} . (r_0 . r_1)^n \bmod n^2)$$
$$:= Enc_{pk}(m_0 + m_1) \quad \textbf{(3)}$$

C. *Commitment scheme*

Commitment scheme is a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later. Commitment schemes are designed so that a party cannot change the value or statement after they have committed to it: that is, commitment schemes are binding. Commitment schemes have important applications in a number of cryptographic protocols including secure coin flipping, zero-knowledge proofs, verifiable secret sharing and secure computation.

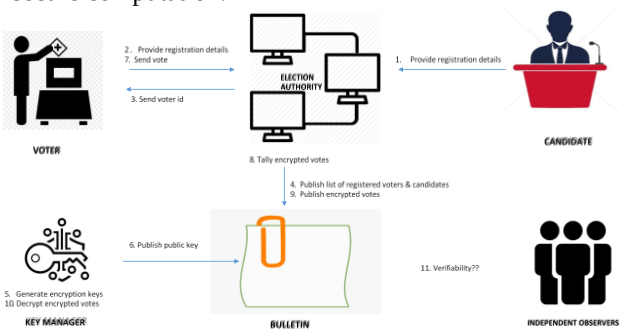

Figure 1: Architectural design of the cryptographic voting protocol.

D. *Bulletin Board*

The bulletin board model, introduced by Benaloh [5], specifies the communication model for the election process, enabling broadcast communication and universal verifiability. A bulletin board is a public readable communication channel with memory. Writing to a bulletin board is append-only, data already written cannot be altered or deleted anymore and its content can be read by anyone. The communication channels in all described protocols are implemented by means of a bulletin board. It can be used to

realize a broadcast channel and private channels, using additional public key encryption.

4.5 Parties Involved

a. The candidate: The candidate sends registration details to the election authority, registers and then gets relegated to having only voting rights.

b. The voter The voter sends registration details to the election authority. If registration details are valid, a unique voter ID is issued to the voter. On Election Day, the voter authenticates with the election authority, the voting software obtains a public key published on the bulletin board and encrypts the vote using this encryption key. The encrypted vote is then sent to the election authority.

c. The Election authority The election authority in this protocol performs three functions - register voters, tally the votes and publish votes upon completion of the election. In the registration phase the election authority serves as one entity, handling all the registration requirements. However, a switch is made to a multi party mode in the tallying and results publishing phase of the election. In the tallying, the election authority is designed in amulti-party setting. A minimum of three servers are setup such that each election authority is located in a different geographical region. Votes are transmitted from the voters to each election authority simultaneously. An independent tally of the votes on is computed on each server, with the results using a commitment scheme to the bulletin board. The commitment scheme ensures that all published values cannot be altered. This setting helps to create redundant and robust system. In order to manipulate the election results at any time, a majority of the servers have to be compromised, with all the compromised servers publishing the exact same result. The election is deemed conclusive only if a majority of the servers publish the same result. d. Bulletin Board This is presented in section 4.1 e. Key manager A key manager in a cryptosystem is charged with the management of cryptographic keys. Key managers handle the generation, storage, exchange, replacement and use of keys

4.6 Protocol Description

Here we provide details of the various steps in the voting protocol

- Step 1: Candidate sends registration details to the Election Authority. The details include personally identifying information
- Step 2: Voter sends personally identifying details, for registration, to the Election Authority
- Step 3: Election authority screens all registration details received. Voter IDs are sent to all registered voters with acceptable data
- Step 4: The list of registered voters is published to the bulletin board. This list is immutable and will not be altered under any circumstance as soon as the registration phase is over
- Step 5: A public key and private key is generated here by the key manager. The public key will be used by the voters to encrypt the votes. This process is handled automatically by the voting software such that the voter does not have to manually retrieve the keys. The key manager retains the private key which can only be assessed by authorized personnel.
- Step 6: The key manager publishes the public key to the bulletin board
- Step 7: This step covers the voting phase. In order to vote, each voter has to authenticate using the voter_ID received in step 3. Upon authentication, a session is opened for the voter. The voter retrieves the public key from the bulletin board. With the keys retrieved, the vote is encrypted and sent in an encrypted format (ciphertext) to the Election authority.
- Step 8: The Election authority tallies the encrypted votes. The total votes for each candidates is calculated using the additive properties of the Paillier cryptosystem and stored as a ciphertext.
- Step9: The Election authority publishes the ciphertext which represents the the total votes tally to the bulletin board.
- Step 10: The key manager decrypts the encrypted votes using the private key
- Step 11: Decrypted results can now be viewed in plaintext, indicating the winner of the election

V. CONCLUSION

Having established the relevance and importance of adopting electronic Internet voting as a viable alternative to physical voting, this study proposes a cryptographic voting protocol which makes it possible for voters to participate remotely in elections over the Internet. This protocol uses the homomorphic encryption scheme to achieve coercion resistance. Votes are cast in encrypted form, tallied and encrypted results are generated. When decrypted, the results default to the candidate with the most votes. The protocol is simple, robust and can be scaled to accommodate any number of voters. The voting system guarantees the integrity, confidentiality and robustness of votes as additional security properties.

REFERENCES

[1] Riza Aditya, Byoungcheon Lee, Colin Boyd, and Ed Dawson. 2004. An efficient mixnet-based voting scheme providing receipt-freeness. In *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 152–161.

[2] R Michael Alvarez, Thad E Hall, and Alexander H Trechsel. 2009. Internet voting in comparative perspective: the case of Estonia. *PS: Political Science & Politics* 42, 3 (2009), 497–505.

[3] Voke Augoye and Allan Tomlinson. 2018. Analysis Of Electronic Voting Schemes In The Real World.. In *UKAIS*. 14.

[4] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. 2001. Practical multi-candidate election system. In *Proceedings of the twentieth annual ACM symposium on Principles of distributed computing*. 274–283.

[5] Josh Benaloh and Dwight Tuinstra. 1994. Receipt-free secret-ballot elections. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*. 544–553.

[6] Orhan Cetinkaya. 2008. Analysis of security requirements for cryptographic voting protocols. In *2008 Third International Conference on Availability, Reliability and Security*. IEEE, 1451–1456.

[7] David Chaum. 2004. Secret-ballot receipts: True voter-verifiable elections. *IEEE security & privacy* 2, 1 (2004), 38–47.

[8] Josh D Cohen and Michael J Fischer. 1985. *A robust and verifiable cryptographically secure election scheme*. Yale University. Department of Computer Science.

[9] Kristian Gjøsteen. 2010. Analysis of an internet voting protocol. *IACR Cryptol. ePrint Arch.* 2010 (2010), 380.

[10] Philippe Golle, Sheng Zhong, Dan Boneh, Markus Jakobsson, and Ari Juels. 2002. Optimistic mixing for exit-polls. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 451–465.

[11] Dimitris A Gritzalis. 2002. Principles and requirements for a secure e-voting system. *Computers & Security* 21, 6 (2002), 539–556.
[12] P Haynes. 2014. Online Voting: Rewards and Risks. Atlantic Council, Intel Security, Washington DC.
[13] Martin Hirt. 2001. Receipt-freeness in Electronic Voting. In *Proceedings of Workshop on Trustworthy Elections (WOTE'01)*.
[14] Martin Hirt and Kazue Sako. 2000. Efficient receipt-free voting based on homomorphic encryption. In *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 539–556.
[15] Wojciech Jamroga and Masoud Tabatabaei. 2016. Preventing coercion in Evoting: be open and commit. In *International Joint Conference on Electronic Voting*. Springer, 1–17.
[16] Ari Juels, Dario Catalano, and Markus Jakobsson. 2005. Coercion-Resistant Electronic Elections: In WPES'05. In *4th Workshop on Privacy in the Electronic Society*. 61–70.
[17] Ari Juels, Dario Catalano, and Markus Jakobsson. 2010. Coercion-resistant electronic elections. In *Towards Trustworthy Elections*. Springer, 37–63.
[18] Ralf Kusters, Tomasz Truderung, and Andreas Vogt. 2010. A game-based definition of coercion-resistance and its applications. In *2010 23rd IEEE Computer Security Foundations Symposium*.
[19] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. 2003. Providing receipt-freeness in mixnet-based voting protocols.
[20] In *International conference on information security and cryptology*. Springer, 245– 258.
[21] Philipp Locher and Rolf Haenni. 2016. Receipt-free remote electronic elections with everlasting privacy. *Annals of Telecommunications* 71, 7 (2016), 323–336.
[22] Philipp Locher, Rolf Haenni, and Reto E Koenig. 2016. Coercion-resistant internet voting with everlasting privacy. In *International Conference on Financial Cryptography and Data Security*. Springer, 161–175.
[23] Emmanouil Magkos, Mike Burmester, and Vassilis Chrissikopoulos. 2001. Receiptfreeness in large-scale elections without untappable channels. In *Towards The E-Society*. Springer, 683–693.
[24] Maxime Meyer and Ben Smyth. 2019. Exploiting re-voting in the Helios election system. *Inform. Process. Lett.* 143 (2019), 14–19.
[25] Pascal Paillier. 1999. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology?EUROCRYPT?99*. Springer, 223–238.
[26] Iñigo Querejeta-Azurmendi, David Arroyo Guardeño, Jorge L Hernández-Ardieta, and Luis Hernández Encinas. 2020. NetVote: A Strict-Coercion Resistance Re-
[27] Voting Based Internet Voting Scheme with Linear Filtering. *Mathematics* 8, 9 (2020), 1618.
[28] Peter B Rønne, Arash Atashpendar, Kristian Gjøsteen, and Peter YA Ryan. 2019. Coercion-resistant voting in linear time via fully homomorphic encryption: towards a quantum-safe scheme. *arXiv preprint arXiv:1901.02560* (2019).
[29] Yefeng Ruan and Xukai Zou. 2017. Receipt-freeness and coercion resistance in remote E-voting systems. *International Journal of Security and Networks* 12, 2 (2017), 120–133.
[30] Peter YA Ryan, Peter B Rønne, and Vincenzo Iovino. 2016. Selene: Voting with transparent verifiability and coercion-mitigation. In *International Conference on Financial Cryptography and Data Security*. Springer, 176–192.
[31] Krishna Sampigethaya and Radha Poovendran. 2006. A framework and taxonomy for comparison of electronic voting schemes. *computers & security* 25, 2 (2006), 137–153.
[32] Jörn Schweisgut. 2006. Coercion-resistant electronic elections with observer. In *Electronic Voting 2006–2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting. CC*. Gesellschaft für Informatik eV.
[33] Kristjan Vassil, Mihkel Solvak, Priit Vinkel, Alexander H Trechsel, and R Michael Alvarez. 2016. The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly* 33, 3 (2016), 453–459.
[34] Zhe Xia, Zheng Tong, Min Xiao, and Chin-Chen Chang. 2018. Framework for practical and receipt-free remote voting. *IET Information Security* 12, 4 (2018), 326–331.
[35] Chibuike Ugwuoke, Zekeriya Erkin, and Reginald L. Lagendijk. 2018. SecureFixed-Point Division for Homomorphically Encrypted Operands. InProceedingsof the 13th International Conference on Availability, Reliability and Security(Ham-burg, Germany)(ARES 2018). Association for Computing Machinery, New York,NY, USA, Article 33, 10 pages. https://doi.org/10.1145/3230833.3233272