IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"Electronic Voting System using Paillier Cryptosystem"

[1]Sheeba P. S., [2]Sakshi Kamble

[1]Associate Professor, [2]Undergraduate Student

[1]Computer Science & Engineering (IoT & Cyber Security Including Blockchain Technology),

[1]Lokmanya Tilak College of Engineering, Navi Mumbai, India

Abstract: The homomorphic encryption approach enables computations to be carried out on ciphertexts, which is crucial as sharing data with untrusted parties during communication can expose it to potential attacks. Over time, researchers have proposed various methods for achieving homomorphic encryption, each demonstrating different levels of effectiveness and limitations in developing a secure system. This study aims to explore the theoretical foundations, practical applications, and implications of the Paillier cryptosystem in electronic voting systems. Through a comprehensive analysis and evaluation, we seek to elucidate the role of Paillier encryption in addressing the challenges and limitations of existing electronic voting systems, paving the way for more secure, transparent, and inclusive democratic practices.

Index Terms – Paillier Cryptosystem, homomorphic encryption, electronic voting.

I. INTRODUCTION

In the digital age, the advent of electronic voting systems has revolutionized democratic processes by offering increased accessibility, efficiency, and convenience to voters worldwide. However, alongside these advancements come significant challenges in ensuring the security, privacy, and integrity of the voting process. Traditional electronic voting systems often rely on centralized architectures and conventional cryptographic techniques, which may introduce vulnerabilities and undermine public trust in electoral outcomes.

Addressing these challenges requires innovative cryptographic solutions that can provide robust security guarantees while preserving the privacy and anonymity of voters. One such solution is the Paillier cryptosystem, a pioneering advancement in the field of cryptography that offers unique homomorphic properties ideal for secure electronic voting applications.

Developed by Pascal Paillier in 1999, the Paillier cryptosystem is a probabilistic asymmetric encryption scheme based on the computational difficulty of the Decisional Composite Residuosity Assumption (DCRA). Unlike traditional cryptosystems, Paillier encryption supports additive homomorphism, allowing for secure computations on encrypted data without the need for decryption. This property enables operations such as addition and multiplication to be performed on encrypted values, making it well-suited for secure aggregation and tallying of votes in electronic voting systems.

At its core, the Paillier cryptosystem consists of a public-private key pair, where the public key is used for encryption and the private key is used for decryption. Encryption involves the transformation of plaintext messages into ciphertexts using modular exponentiation and modular multiplication operations, while decryption requires the use of the private key to recover the original plaintexts.

The use of Paillier encryption in electronic voting systems offers several advantages:

Confidentiality: Votes are encrypted before transmission, ensuring the privacy and anonymity of individual voters.
Integrity: Homomorphic properties enable secure aggregation and tallying of encrypted votes, preserving the integrity of the voting process.
Verifiability: End-to-end verifiability mechanisms allow voters and election authorities to independently verify the correctness of election results without compromising voter privacy.
Transparency: The use of cryptographic techniques enhances the transparency and auditability of the voting process, fostering trust and confidence in electoral outcomes.

This paper aims to explore the theoretical foundations, practical applications, and implications of the Paillier cryptosystem in electronic voting systems. Through a comprehensive analysis and evaluation, we seek to elucidate the role of Paillier encryption in addressing the challenges and limitations of existing electronic voting systems, paving the way for more secure, transparent, and inclusive democratic practices.

II. Literature Survey

In recent years, the development of secure electronic voting systems has become a focal point in both academic research and practical implementation. Various cryptographic techniques have been explored to enhance the security and privacy of electronic voting processes. Among these techniques, the Paillier cryptosystem [1] has emerged as a prominent solution due to its unique homomorphic properties, allowing for secure computations on encrypted data.

According to a study by Rivest [3], the Paillier cryptosystem offers a robust and efficient solution for electronic voting systems, ensuring both the confidentiality and integrity of the voting process. This sentiment is echoed by [6], who conducted a comprehensive analysis of cryptographic schemes for secure electronic voting, concluding that Paillier encryption stands out for its security guarantees and computational efficiency.

Furthermore, a research [2] explores the application of the Paillier cryptosystem in practical electronic voting scenarios, highlighting its versatility and adaptability to various voting schemes and requirements. Additionally, a study by Benaloh [4] proposes enhancements to the Paillier cryptosystem specifically tailored for electronic voting applications, addressing potential vulnerabilities and improving the overall security of the voting process.

While these studies provide valuable insights into the theoretical foundations and practical applications of the Paillier cryptosystem in electronic voting systems, ongoing research efforts are necessary to address emerging challenges and further optimize the implementation of secure electronic voting protocols.

This literature survey underscores the significance of the Paillier cryptosystem in the realm of secure electronic voting, citing reputable research studies that attest to its efficacy and suitability for ensuring the confidentiality, integrity, and efficiency of electronic voting processes.

III. Limitations in Current System

Despite notable advancements, current electronic voting systems are plagued by persistent limitations that undermine their effectiveness and trustworthiness. These limitations encompass various vulnerabilities and shortcomings, hindering the realization of truly secure and transparent voting processes.

One of the primary challenges faced by existing electronic voting systems is the prevalence of vulnerabilities such as vote tampering and coercion. Traditional systems, particularly those utilizing centralized architectures, are susceptible to malicious attacks and unauthorized manipulation. The reliance on a single server for storing and processing votes creates a single point of failure, exposing the entire system to potential security breaches.

Furthermore, the cryptographic techniques employed in many electronic voting systems may fall short in providing adequate assurances of privacy and integrity. While methods like blind signatures and mixnets have been proposed to enhance security, their implementation often introduces complexities and performance

overheads that impede practical adoption. As a result, ensuring the confidentiality and integrity of votes remains a significant challenge in electronic voting.

Moreover, the absence of standardized protocols and frameworks exacerbates the complexity of developing and deploying secure electronic voting systems. Interoperability issues and compatibility constraints across different voting platforms hinder seamless integration and exacerbate concerns regarding transparency and trustworthiness. Without robust and universally accepted standards, achieving consensus on the verifiability and accuracy of electoral outcomes becomes increasingly challenging.

In essence, the limitations of existing electronic voting systems stem from a combination of technical vulnerabilities, architectural flaws, and regulatory gaps. Addressing these limitations requires comprehensive solutions that prioritize security, privacy, and transparency while promoting accessibility and usability for all stakeholders involved in the electoral process.

IV. Research Objective

The current landscape of electronic voting systems is fraught with challenges, including security vulnerabilities and privacy concerns, which undermine the integrity and trustworthiness of electoral processes. In response to these limitations, the primary objective of this research is to develop a robust and privacy-preserving electronic voting system that leverages the advanced cryptographic capabilities of the Paillier cryptosystem. By addressing the inherent shortcomings of existing systems, the research aims to establish a foundation for secure, transparent, and verifiable voting practices.

The specific objectives of the research are as follows:

Design and Implementation: Develop a prototype electronic voting system that utilizes the Paillier cryptosystem to ensure the confidentiality and integrity of votes cast by voters. The system should incorporate mechanisms for voter authentication, secure transmission of votes, and end-to-end verifiability.

Security and Performance Evaluation: Conduct comprehensive testing and analysis to evaluate the security properties and performance characteristics of the proposed electronic voting system. This assessment will involve assessing the system's resistance to various types of attacks, as well as its efficiency and scalability in handling large-scale elections.

Usability and User Experience: Assess the usability and user experience of the electronic voting system to ensure accessibility and ease of use for voters from diverse backgrounds. This evaluation will focus on user interface design, navigation flow, and clarity of instructions to facilitate a seamless voting experience.

Scalability and Robustness: Investigate the scalability and robustness of the electronic voting system to accommodate different election scenarios and stakeholder requirements. This analysis will consider factors such as system performance under varying load conditions, adaptability to evolving technological environments, and resilience against potential disruptions.

V. Proposed System

The proposed electronic voting system represents a paradigm shift in electoral practices, offering a comprehensive solution that addresses the shortcomings of existing systems. Central to the proposed system is the integration of the Paillier cryptosystem, which provides a solid foundation for ensuring the security, privacy, and verifiability of the voting process.

Key features of the proposed system include:

Voter Authentication Mechanisms: Implement robust authentication mechanisms to verify the identity of voters and prevent unauthorized access to the voting platform. This may involve the use of multi-factor authentication, biometric verification, or other secure authentication protocols.

Secure Transmission Protocols: Employ advanced encryption techniques to protect the integrity of votes during transmission from voters to the central server. Secure communication channels, such as encrypted protocols and digital signatures, will be utilized to safeguard against eavesdropping and tampering.

End-to-End Verifiability: Incorporate mechanisms that enable voters and election authorities to independently verify the integrity of the voting process. This includes providing cryptographic proofs of vote casting, encryption, and decryption, as well as enabling transparent audit trails for accountability and transparency.

Auditability and Transparency Features: Integrate auditability and transparency features into the electronic voting system to ensure accountability and trustworthiness in the electoral process. This may involve real-time monitoring tools, logging mechanisms, and reporting functionalities to enable stakeholders to audit and scrutinize the voting process.

Here's an explanation of the key components and properties of the Paillier scheme:

1. *Key Generation:*
   - The Paillier cryptosystem involves the generation of a public key and a private key.
   - The public key consists of two large prime numbers pp and qq, and a composite number $n=p\times q$n=p×q.
   - Additionally, it includes a public parameter gg, which is typically chosen such that gg is a generator of the multiplicative
   - group $Zn*$Zn∗ (the set of integers modulo nn that are coprime to nn).
   - The private key consists of the prime factors pp and qq.
2. *Encryption:*
   - To encrypt a message mm, a random value rr is chosen such that $0\leqslant r<n$0⩽r<n and gcd⁡(r,n)=1gcd(r,n)=1.
   - The ciphertext cc is computed as $c=gm\cdot rn \bmod n^2$c=gm·rnmodn2.
3. *Decryption:*
   - To decrypt the ciphertext cc, the recipient uses the private key.
   - The original message mm can be recovered as $m=L(c\lambda \bmod n^2)\cdot\mu \bmod n$m=L(cλmodn2)·μmodn, where $L(x)$L(x) is the least significant bits of xx, $\lambda=\text{lcm}(p-1,q-1)$λ=lcm(p−1,q−1), and μμ is the modular inverse of $L(g\lambda \bmod n^2)$L(gλmodn2) modulo nn.
   - Note: The function $L(u)$L(u) computes $(u-1)/n$(u−1)/n.
4. *Homomorphic Properties:*
   - The Paillier cryptosystem supports additive homomorphic properties, meaning that operations performed on ciphertexts result in the same operations on the plaintexts when decrypted.
   - Specifically, given ciphertexts $c1$c1 and $c2$c2 representing plaintexts $m1$m1 and $m2$m2 respectively, multiplying $c1$c1 by $c2$c2 results in a ciphertext that represents the plaintext $m1+m2$m1+m2.
   - This property enables computations on encrypted data without the need for decryption.
5. *Security:*
   - The security of the Paillier cryptosystem is based on the difficulty of factoring the composite number nn into its prime factors pp and qq.
   - When the modulus nn is sufficiently large, the scheme is considered secure against attacks such as integer factorization.

VI. IMPLEMENTATION/ METHODOLOGY

Purpose of the Program:

The program simulates an electronic voting system, allowing users to cast their votes for different candidates in an election. It

also tallies the votes and displays the results.

Candidate List:

The program starts by defining a list of candidates who are running in the election. In this example, we have three candidates:

"Candidate A", "Candidate B", and "Candidate C".

Key Generation:

The program generates a pair of encryption keys: a public key and a private key. These keys are used for encrypting and decrypting

the votes, respectively. This is done using a cryptographic technique called Paillier encryption, which provides a form of

homomorphic encryption.

Authentication Function:

There's a function called authenticate_voter() that simulates the process of authenticating voters. In a real system, this function

would verify the identity of voters based on their usernames and passwords.

Voting Function:

The cast_vote() function simulates the process of casting a vote. When a voter selects a candidate, their vote is encrypted using

the public key. This ensures that the vote remains confidential and cannot be tampered with during transmission.

Tallying Votes Function:

The tally_votes() function simulates the process of tallying the encrypted votes. It counts the number of votes received by each

candidate without decrypting the individual votes. This is achieved using the homomorphic properties of Paillier encryption,

which allow mathematical operations to be performed on encrypted data.

Main Program:

The main program prompts the user to enter the number of voters participating in the election. It then simulates the voting process

for each voter, prompting them to authenticate and select a candidate to vote for. After all votes are cast, the program tallies the

votes and displays the results.

Homomorphic Encryption:

Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without

decrypting it first. In this program, Paillier encryption is used, which supports additive homomorphic properties. This means that

mathematical operations (such as addition) performed on encrypted data result in the same operations on the plaintexts when

decrypted.

Result Generation:

The program generates the result by tallying the encrypted votes for each candidate. Since the votes are encrypted, they remain

confidential throughout the process. The result is then displayed, showing the number of votes received by each candidate.

The Paillier cryptosystem is partially homomorphic, specifically supporting additive homomorphism.

1. *Partially Homomorphic:*
   - Paillier encryption supports additive homomorphism, which means that it allows for addition operations to be performed on encrypted data. Specifically, given two ciphertexts representing plaintexts m1m1 and m2m2, when the ciphertexts are multiplied together, the resulting ciphertext represents the sum of the plaintexts (m1+m2m1+m2).
   - However, Paillier encryption does not support multiplication of encrypted values directly.
2. *Key Generation:*
   - In the Paillier cryptosystem, a public-private key pair is generated.
   - The public key consists of a composite number nn and a public parameter gg.
   - The private key consists of the prime factors of nn.
3. *Encryption:*
   - To encrypt a plaintext mm, a random value rr is chosen such that $0 \leqslant r < n 0 \leqslant$ r<n and gcd(r,n)=1gcd(r,n)=1.
   - The ciphertext cc is computed as $c=(gm \cdot rn) \bmod n$2c=(gm·rn)modn2.

4. *Decryption:*
   - To decrypt a ciphertext cc, the recipient uses the private key.
   - The original plaintext mm can be recovered as follows: $m=L(c\lambda \bmod n2)L(g\lambda \bmod n2)\cdot\mu \bmod n$m=L(gλmodn2)L(cλmodn2)·μmodn where λλ is the least common multiple of $p-1$p−1 and $q-1$q−1, and μμ is the modular inverse of $L(g\lambda \bmod n2)$L(gλmodn2) modulo nn.
   - The function $L(x)$L(x) extracts the least significant bits of xx, effectively rounding it down to the nearest multiple of nn.
5. *Additive Homomorphism:*
   - When two ciphertexts $c1$c1 and $c2$c2 are multiplied together (i.e., $c1\cdot c2$c1·c2), the resulting ciphertext represents the sum of the plaintexts ($m1+m2$m1+m2).
   - This property allows computations on encrypted data without the need for decryption, preserving the confidentiality of the data.
6. *Working of Paillier Encryption:*
   - When a plaintext mm is encrypted, the Paillier encryption scheme incorporates randomness (represented by rr) to ensure semantic security.
   - The encrypted value cc is computed using modular exponentiation and modular multiplication operations, which are computationally efficient.
   - Decryption involves a series of modular exponentiations and modular multiplications, followed by a division operation to recover the original plaintext.

VII. Results and Conclusion

Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without decrypting it first, which is crucial as sharing data with untrusted parties during communication can expose it to potential attacks. The simulation results are shown in Figure 1. The program generated the result by tallying the encrypted votes for each candidate. Since the votes are encrypted, they remain confidential throughout the process. The result is then displayed, showing the number of votes received by each candidate.

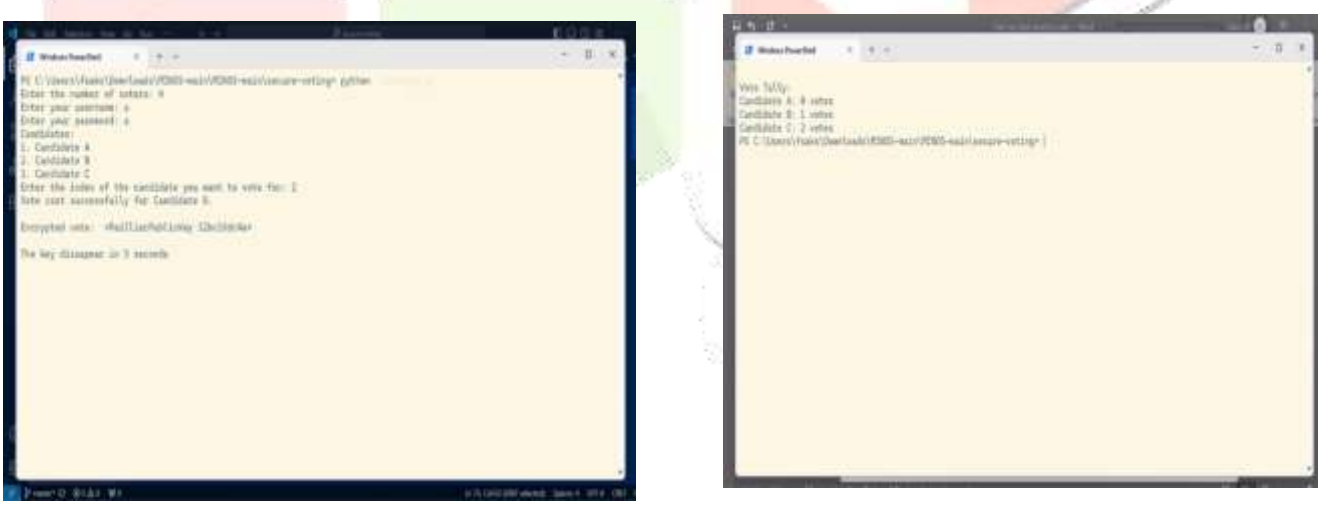

Fig 1. Simulation Results

In this work, Paillier encryption is used, which supports additive homomorphic properties. This means that mathematical operations (such as addition) performed on encrypted data result in the same operations on the plaintexts when decrypted. The new approach offers stronger encryption for homomorphic computation in the e-voting system, making it more reliable than existing single cryptographic methods.

REFERENCES

[1] Paillier, Pascal (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes" (PDF). Advances in Cryptology – EUROCRYPT '99. EUROCRYPT. Springer.

[2] Martin HirtKazue Sako, Efficient Receipt-Free Voting Based on Homomorphic Encryption, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000.

[3] Rivest, R., Adleman, L., and Dertouzos, M. 1978. On data banks and privacy homomorphisms. Foundations of secure computation 4, no. 11: 169-180.

[4] Josh Benaloh, Tal Moran, Lee Naish, Kim Ramchen, Vanessa Teague, Shuffle-Sum: Coercion-Resistant Verifiable Tallying for STV Voting, IEEE Transactions on Information Forensics and Security, Volume: 4, Issue: 4, December 2009, pp. 685-698.

[4] Golle, P., Jakobsson, M., Juels, A., Syverson, P. (2004). Universal Re-encryption for Mixnets. In: Okamoto, T. (eds) Topics in Cryptology, Lecture Notes in Computer Science, vol 2964. Springer, Berlin, Heidelberg.

[6] Yun-Xing Kho, Swee-Huay Heng, andJi-Jian Chin, A Review of Cryptographic Electronic Voting, Symmetry 2022, 14(5), 858.

[5] Coron, J., Mandal, A., Naccache, D., and Tibouchi, M. 2011. Fully homomorphic encryption over the integers with shorter public keys, Advances in cryptology. Lecture Notes in Comput. Sci., vol. 6841, Springer, pp. 487–504.

[6] Yi, X., Paulet, P. and Bertino, E. 2014. Homomorphic Encryption and Applications, Springer Briefs in Comp. Sci.

[7] Gentry, C., Halevi,S., and Smart N. 2012. Fully homomorphic encryption with polylog overhead, Advances in cryptology—EUROCRYPT 2012, Lecture Notes in Comput. Sci., vol. 7237, Springer, Heidelberg, pp. 465–482.