Homomorphic Encryption in Ballot Casting in the Election System

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Yufei Zhou

Fall, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Yufei Zhou, Department of Computer Science

Homomorphic Encryption In Ballot Casting In The Election System

CS4991 Capstone Report, 2022
Yufei Zhou
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
yz5zys@virginia.edu

ABSTRACT

Ever since the United States was founded, the election system has been the essence of this country. However, as cyber threats become more severe, more widespread and harder to detect, intensifying citizen distrust of election results, the voting system needs to be improved to better defend against foreign attacks during elections and annihilate the public's worry.

Homomorphic encryption, an encryption method that can maintain the nature of the original text, would address the election transparency issue. I propose testing different implementations of homomorphic encryption schemes such as RSA, El Gamal Encryption, and Paillier Encryption to search for the most suitable and reliable method for encrypting ballots. The ballots after the encryption can be displayed to the public. Meanwhile, encryption would allow ballot-counting institutions to add up the ballots for the final result in a way that the entire process can be traced and records kept for future reference. Further testing based on simulating real vote-casting scenarios is needed to determine the stability and adaptability of the model. In addition, security protocol should be employed with the encryption scheme to ensure the system works at an optimal security level.

1 INTRODUCTION

"Governments are instituted among Men, deriving their just Powers from the Consent of the Governed."—Thomas Jefferson (1776), Declaration of Independence.[2] Ever since the United States was founded, the election system has been the essence of this country. Elections give the public the right to select their representatives. The inclusiveness of the individuals who are eligible to vote symbolizes the improvement in U.S. social structure and the advancement of equality. The concept of equality rooted in U.S. history and the fairness of the elections is an externalization of the values of U.S. citizens. Given their importance, election standards have been gradually refined and improved, along with advancements in technology and social structure.

However, as cyber threats become more severe, more widespread, and harder to detect, intensifying citizen distrust in the result of the elections, voting system defenses need to be improved. Specific concerns include foreign attacks during elections. It is critical to building trust bonds within the community to encourage more voters to vote. And as more voters get involved in the elections, the authority and the representativeness of the elections will be elevated. Therefore, a more transparent voting process that is both secure and reliable is urgently needed.

2 RELATED WORK

Discussion on applying cryptographic algorithms to election systems has already been initiated in recent decades. In fact, the National Institute of Standards and Technology (NIST, 2011)[4] proposed the use of cryptographic algorithms to "protect the confidentiality of information in transit or in storage" and discussed the value of "message authentication codes or digital signatures for establishing trust in the authenticity and integrity of information." Also, Benaloh, a senior cryptographer at Microsoft, mentioned the concept of homomorphic encryption in an interview for The New Yorker in 2020. [1] However, no specific implementation was detailed in these documents.

The performances of different e-voting cryptographic schemes, including Mix-Net Based, Homomorphic, Blind Signature-Based, Blockchain-Based, and Post-Quantum e-Voting, were compared and evaluated in parallel by Kho, et. al. (2022). [7] Although relevant ideas regarding homomorphic encryption were already well-established by experts in cryptography, voting systems based on homomorphic encryption are not yet adopted by the election institutions.

3 PROPOSED PROCESS DESIGN

3.1 Model Selection

The selection of appropriate encryption algorithms is critical to the stability and efficiency of the election system. In this section, RSA [5], El Gamal encryption[6], and Pillier encryption[3] are evaluated based on practicality in the context of large-scale national elections. According to the analysis, El Gamal encryption suits best. Therefore, RSA and Pillier encryption will only be briefly introduced—the encryption process will be omitted.

3.1.1 RSA Encryption and Pillier Encryption.

The generation of RSA and Pillier encryption key pairs both rely on large prime numbers and modular multiplicative inverse. In the following, the steps shared by both encryption schemes are marked with ①; steps of RSA are marked with ②; steps of Pillier are marked with ③.

① Generate 2 large prime number p, q and compute their products n
① Generate $\lambda(n) = lcm(p-1, q-1)$ where lcm stands for least common multiplier.
② Generate integer e such that $1 < e < \lambda(n)$
② Determine the multiplicative inverse of e in $\mathbb{Z}_{\lambda(n)} \rightarrow d$
② Produce key pair: public key (n, e) and private key (n, d)
③ Generate integer $g \in \mathbb{Z}_{n^2}$
③ Ensure n divides the order of g, $(o(g))$ and compute $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$ where $L(x) = \dfrac{x-1}{n}$ and division is defined as field division.
③ Produce pub key (n, g) and priv key (λ, μ)

Both encryptions are time and computation consuming due to the incorporation of large prime numbers and the calculation of large powers. Due to their lack of efficiency, these two schemes are not suitable to be applied into the election system.

3.1.2 ElGamal Encryption.

ElGamal Encryption scheme is a symmetric encryption algorithm developed based on Diffie-Hellman key exchange. It takes advantage of the properties of finite fields. Specifically, the key is generated within a randomly selected cyclic group. The key generation process is described as following:

① Generate a cyclic group $\mathbb{G}$ with order q and generator g.
② Select an integer x randomly from $\{1, 2 \ldots q-1\}$.
③ Compute $h := g^x$.
④ Produce pub key h and priv key x

Since ElGamal encryption makes use of field operations, it avoids the computation of large powers of large numbers. When applied to a larger scale,

the computation will be more efficient compared with previous two encryption schemes.

3.2 Homomorphic Property

Homomorphic property of the encryption algorithms allows mathematical operations, such as addition, subtraction, or multiplication, to be performed on the cipher text. However, different key generation processes of different algorithms support different mathematical operations.

3.2.1 *Homomorphic Multiplication.*

El Gamal supports homomorphic multiplication. It means that the product of plain texts can be retrieved from the multiplication operation of the cipher texts.

Given a public key $y = g^x$ and two plain texts m_1, m_2, we have $Enc(m_1; r_1) \cdot Enc(m_2; r_2)$ $= (g^{r_1}, m_1 y^{r_1}) \cdot (g^{r_2}, m_2 y^{r_2}) = (g^{r_1+r_2}, (m_1+m_2) y^{r_1+r_2})$ $= Enc(m_1 \cdot m_2)$ where r_1, r_2 are two random number chosen within the cyclic group $\mathbb{G}$.

3.2.2 *Homomorphic Addition.*

However, the addition of plain texts is more useful for a voting system. Therefore, a modified version of El Gamal encryption—exponential El Gamal, supports homomorphic addition.

Given a public key $y = g^x$ and two plain texts m_1, m_2, we have $Enc(m_1; r_1) \cdot Enc(m_2; r_2)$ $= (g^{r_1}, g^{m_1} y^{r_1}) \cdot (g^{r_2}, g^{m_2} y^{r_2}) = (g^{r_1+r_2}, g^{m_1+m_2} y^{r_1+r_2})$ $= Enc(m_1 + m_2)$ where r_1, r_2 are two random number chosen within the cyclic group $\mathbb{G}$.

3.3 Ballot Encryption

The ballots need to be converted to numbers before encryption. I propose that each candidate in the election is assigned to an integer, with each vote converted to a 24-bit binary number, or 3-byte hexadecimal number. Then the result of the addition would not cause any overflow since $2^{25} - 1 = 33554431$, which is much larger than the maximum possible vote an individual can get from a single state. To illustrate the encryption more clearly, consider the following example: suppose there are two candidates in an election with index 0 and 1 and two voters. The first voter votes for both of candidates and the second voter votes for the candidate with index 1. Then, the plain text of the first voter's vote would be 00000000000000000000000100000000 0000000000000001 in binary, or $0x000001000001$ in hexadecimal. The plain text of the second voter's vote would be 00000000000000000000000000000000 0000000000000001 in binary, or $0x000000000001$ in hexadecimal. Therefore, after the addition operation on the cipher text, the result would be 00000000000000000000001000000000000000000000 0010 in binary, or $0x000001000002$ in hexadecimal. Therefore, the first (most significant) 24-bit represents the number of votes of the candidate with index 0 and the second (last significant) 24-bit represents the number of votes of the candidate with index 1.

3.4 Challenge and Mitigation

The original El Gamal encryption is vulnerable to chosen cipher text attack. Given an encrypted cipher text $Enc(m; r) = (g^r, g^m y^r)$, it is easily to modify another valid cipher text $Enc(2m; r) = (g^r, g^{2m} y^r)$. However, the exponential El Gamal encryption is safe against chosen cipher text attack since if the cipher text $g^m y^r$ can only be safely modified knowing m or r. To further secure the safety of cipher text during transmission, a signature scheme can be applied to cipher text for the ballot counting entities to verify that the received cipher text is from the voter without modification by a third party. Here, I propose a simple signature scheme based on RSA [5].

① Generate a random number α that is between 1 and the length of cipher text.

② Generate a RSA key pair and encrypt the random number with private key.

③ Compute the hash of the first α bits of the cipher text.

④ Append the encryption of the random number and the hash to the original cipher text.

The encryption of a 3-digit(at most) number would greatly reduce the workload in both encryption and decryption. Also, the signature scheme would guarantee that a valid ballot is not modified in the transmission process.

4 ANTICIPATED OUTCOMES

If the proposed model works properly, the ballot casting process during the election will become transparent. The voters would be able to trace their ballots on an interactive online platform. The transparency will enhance the authoritativeness of the election system as well as the trust bond within communities. Meanwhile, citizens who used to hold a skeptical perspective would be motivated to participate in the elections. As a result, the turnout rate will be elevated.

The new system would also help to improve the efficiency and accuracy of absentee ballot. Instead of sending and receiving absentee ballots by mail, citizens abroad from the United States would be able to vote online.

5 CONCLUSION

In this proposal of electronic voting system, I adopt exponential El Gamal encryption as a basis, and integrate RSA signature scheme as an additional security protection. In addition, the design of the encryption model takes the computational resource limitation into consideration to fit the scale of the elections, especially national elections. Specifically, since field computation is based on modulo operation, the complexity of calculation would be restricted, and thus avoid the computation of large numbers.

6 FUTURE WORK

Limited by undergraduate knowledge, I think the practicality of the model needs further testing and evaluation. For example, the security of the model is not supported by theoretical evidence. A zero-knowledge proof of the encryption scheme would be needed. Moreover, the performance and effectiveness of the model when applied to real elections should be examined to check whether it improves computational efficiency as stated in this proposal. Last, the promotion of this system requires support from governments and citizens since its primary purpose is to better serve the democratic system of the country and improve the authoritativeness and transparency of the election system.

REFERENCES

[1] Sue Halpern. 2020. Can Our Ballots Be Both Secret and Secure? (July 7 2020). Retrieved November 30, 2022 from https://www.newyorker.com/news/the-future-of-democracy/can-our-ballots-be-both-secret-and-secure

[2] Thomas Jefferson. 1997. *Declaration of Independence*. Applewood Books, Jackson, MS, USA.

[3] Paillier Pascall. 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes *(Advances in Cryptology — EUROCRYPT '99.)*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_16

[4] Andrew Regenscheid and Beier Geoff. 2011. Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. (September 2011). Retrieved November 30, 2022 from https://www.nist.gov/system/files/documents/itl/vote/nistir7711-Sept2011.pdf

[5] Rivest Ron, Shamir Adi, and Adleman Leonard. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* 21, 2 (Feburary 1978), 120–126. https://doi.org/10.1145/359340.359342

[6] ElGamal Taher. July 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 31, 4 (July 1985), 469–472. https://doi.org/10.1109/TIT.1985.1057074

[7] Kho Yun-Xing, Heng Swee-Huay, and Chin Ji-Jian. 2022. A Review of Cryptographic Electronic Voting. *Symmetry* 14, 858 (April 21 2022). https://doi.org/10.3390/sym14050858