An Electronic Voting Scheme Based on ElGamal Homomorphic Encryption for Privacy Protection

Luecheng Li
Division of Science and Technology, Beijing Normal University - Hong Kong Baptist University United International College, GuangZhou, GuangDong, 511400, China
Corresponding E-mail: angela@cas-harbour.org

Abstract. Electronic voting is the product of the development of modern network technology, in view of the electronic voting system security issues. This paper puts forward a kind of electronic voting scheme based on ElGamal homomorphism encryption, the scheme using homomorphic encryption strategies to voters vote operations, to protect the identity of voters and will not be exposed, to realize the security of electronic voting, confidentiality, and fairness, eligibility, and implement the Internet security electronic voting.

1. Introduction
In 1981, for the first time David Chaum was proposed based on the Mix-net electronic voting protocol[1], electronic voting, with its high efficiency and energy saving advantages of the convenient, gradually replaced the traditional voting but as in the actual application, it has produced many new problems and requirements, some scholars constantly designed to meet the different needs of electronic voting scheme.

For the safety of electronic voting must meet the following seven properties[2]: legality, uniqueness, privacy, integrity, impartiality, veracity, verifiability. Respectively, legality means only authorized voters are eligible to vote. Uniqueness means each voter can only vote once. Privacy stands for the vote must keep secret; no institution or individual is allowed to obtain results. Integrity is explained that the vote must be safe; no one is allowed to change another’s vote and no impersonate of others. Impartiality means no one is allowed to get the result until the ballot vote is completed. Veracity stands for all the votes must be count. Verifiability means after count of votes, there must be a way to verify the results. In order to satisfy all the above properties, especially to guarantee the privacy of vote, this paper comes up with a schema based on Elgamal schemes.

Electronic voting schemes based on homomorphic encryption can be divided into Paillier schemes[4] Elgamal schemes[5, 6] and homomorphic schemes[7] on integers and LWE/RLWE schemes[8, 9] according to the different homomorphic encryption schemes. The most above-mentioned schemes except for Elgamal schemes failed to achieve more candidates to vote, although the Elgamal scheme can achieve more candidates to vote, its security is low. Therefore, this paper comes up with a scheme based on Elgamal homomorphic encryption policy to ensure the voters in votes are submitted to hide their identity information. This new scheme aims to fully guarantee the privacy of the election in the process of counting operation ballot papers.
2. Literature review

2.1. Homomorphic encryption
Homomorphic encryption by Ron Rivest et al.[3] in 1978, overturns the traditional homomorphic encryption algorithm under the form of encryption mode, different from the traditional encryption algorithm, it directly to some cipher operation to replace the clear operation, obtain and encrypt plaintext operation again the same effect, protect clear privacy homomorphism encryption generally fall into two kinds: Multiplication homomorphism and addition homomorphism early homomorphism encryption only supported multiplication homomorphism or addition homomorphism. Due to its special nature, homomorphism encryption plays an important role in many aspects, such as cloud computing and multi-party secret computing, and is an important tool to solve the privacy of electronic voting protocols.

![Information processing of homomorphic encryption algorithm](image)

2.2. ElGamal algorithm
ElGamal algorithm is a widely used homomorphic encryption algorithm, which was proposed by ElGamal[10] on the basis of public key cryptography and elliptic curve encryption system in 1985. ElGamal encryption system has a wide range of applications in practice. ElGamal algorithm can be simply described as follows.

2.2.1. Key production algorithm.
- Pick a large prime number p
  - g is the generator $Z_p^*$ of multiplication groups
  - Pick a random number $x(1 < x < p - 1)$, calculate $h = g^x \mod p$.
  - Public key is $(p, g, h)$, secret key is $x$.

2.2.2. Homomorphic encryption algorithm is as follows:
- Pick a random number $k$, where $k \in Z_p^*$
  - For the plaintext $m$, there is corresponding ciphertext:
    $$ E_k(m) = (a, b) = (g^k \mod p, \; mh^k \mod p) $$

2.2.3. Homomorphic decryption algorithm is as follows:
- For the ciphertext $c = (a, b)$, there is corresponding plaintext $m$: $D_a(a, b) = \frac{b}{a^x} \mod p = m$.

2.2.4. ElGamal homomorphic encryption algorithm. It has the following multiplicative homororphism:
$$ E_h[m_1 \cdot m_2] = (g^{r_1}, \; m_1 h^{r_1}) (g^{r_2}, \; m_2 h^{r_2}) = (g^{r_1+r_2}, \; m_1 m_2 h^{r_1+r_2}) = E_h[m_1 \cdot m_2] \quad (1) $$

3. Privacy protection electronic voting system
Participants in the electronic election process include voter, voter polling stations and authorized counting centers where voters submit their encrypted ballots through operating terminals; Polling
stations collect encrypted ballots submitted by voters and submit them to authorized counting centers; Authorization center collects all the encrypted ballot counting and counting statistics, published the results in this paper the electronic voting system using homomorphic filtering strategy to voters vote operations, to protect the identity of voters is not exposed, protect the will of the voters from the exposure, the asymmetric cryptosystem secure data in the process of information transmission election of whole process includes three parts: authorization stage, stage of voting and counting stage. Next, introduce each stage in detail.

3.1. Authorization stage
Authorization of the first stage is used to determine that the identity of voters ID is in line with the conditions of electoral voters before the vote. It is required to confirm that the identity of ID is legal. The implement method is based on the identification of biological characteristics, such as face recognition fingerprint iris recognition, or based on the magnetic card IC card identification as well as be based on RFID identification[11].

3.2. Voting stage
After voters identity check, after confirm the legitimacy of the voters, entered the stage first, voters elected operating terminals provide a blank votes to voters, voters to fill out and submit their votes in the election the operating terminal record some votes, construct a table of R * C, which R represented as the number of vote and C represented as candidate number. On this piece of R * C in the table, is as follows to record the results of the vote: If the voters approved of a candidate in the corresponding row and votes the candidate corresponds to the location of the column, record is 1, and the votes corresponding to the other columns, records of 0 then the election operation terminal for each vote records value homomorphic encryption by using encryption, forming a R * C encrypted value form and then again for the same candidates all encrypted value algebra multiply operation, to get a table in the 1 * C in the end, the election operation terminal will algebra by 1 * C in the form of the results by AES Symmetric key encryption is used to obtain the ciphertext, and then the AES symmetric key is encrypted with the RSA public key of the authorized counting center, and both are sent to the polling station server, which sends the data collected by each terminal to the authorized counting center.

3.3. Counting stage
Authorization from the central counting collect all polling stations after RSA public-key encryption cipher key, and after each operation data terminal AES encryption cipher, entered the stage first, counting authorization counting centers with their RSA private key to decrypt the cipher key for, get each operation terminal AES symmetric key, then use the AES symmetric key to decrypt the each operation from the results of the election results to decrypt the terminal is a 1 * C after algebraic multiplication computation table, the table records the real results Finally, the total number of votes for each candidate is calculated by doing the same calculation for each table received from the polling station.

4. Properties analysis

4.1. Legality
The legality depends mainly on the first stage——Authorization stage. The reliability of legality depends on the method used to identify voters. Voters are eligible to vote only if they provide an ID that matches their status and pass an audit. The cost and reliability of different authentication methods vary.

4.2. Uniqueness
During the voting period, the system's log information records the voting time corresponding to each voter ID, therefore, there are special labels in the voter database to record the voter's voting status yes or no. Hence, the same voter ID can be guaranteed to vote at most once.
4.3. Privacy
Privacy can be guaranteed during the voting stage and counting stage. Through Elgamal homomorphic encryption and encryption algorithm, the process of data operation is kept secret, so that no one knows who voted for a certain vote.

4.4. Integrality
Through the Elgamal homomorphic encryption and decryption algorithm, once a voter’s ballot is submitted, the ballot will be homomorphic encrypted algebraic multiplication, no one can modify the voter’s vote information. In addition, the label of the voter in the database shows that the voter has voted, which ensures that no one can impersonate the voter to vote.

4.5. Impartiality
Since the data flow contacted by participants in the intermediate process is all ciphertext information, if it is necessary to decipher the plaintext, the corresponding private key is required, and the storage of the private key is in the authorized counting center, which would ensure that intermediate participants could not gain access to information halfway and undermine the integrity of the election.

4.6. Veracity
Voters can only vote if they are authenticated and qualified. Once a voter has cast a ballot, homomorphism ensures that the voter's vote has been accepted. At the counting stage, the counting center is authorized to reflect the voter’s willingness to vote in the election results by reliable calculation.

4.7. Verifiability
Since the original voting data of voters is kept in each polling station, if the election results need to be verified, the authorized counting center can issue a request to collect the data from each polling station again, so that the election results can be verified.

5. Conclusion
This paper proposes a Elgama homomorphic encryption scheme to protect the privacy of voters electronic voting system design scheme of this system by homomorphic encryption, decryption and homomorphism strategy to ensure the voters information submitted at the same time, personally identifiable information will not be exposed, to ensure the voters information privacy in the operation process, through the public key encryption and asymmetric key system private key to decrypt the strategy to ensure the data security in the transmission process, will not be among participants in the process of deciphering the system satisfies the basic safety standards of electronic voting system.

References
[1] Chaum D. L. (1981) Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM, 24: 84-88. https://doi.org/10.1145/358549.358563.
[2] Fujioka A., Okamoto T. and Ohta K. (1992) A Practical Secret Voting Scheme for Large Scale Election. Advances in Crytpology-Auscrypt, pp. 224-260. https://doi.org/10.1007/3-540-57220-1_66
[3] Rivest R. L., Adleman, L., Dertouzos, M. L. (1978) On Data Banks and Privacy Homomorphisms. Foundations of Secure Computation, 169-179.
[4] Will M. A., Nicholson B., Tiehuis M., et al. (2015) Secure voting in the cloud using homomorphic encryption and mobile agents. In: Proc of International Conference on Cloud Computing Research and Innovation, Singapore. pp: 173 - 184.
[5] Cerveró M. A., Mateu V., Miret J. M., et al. (2014) An efficient homomorphic E-voting system over Elliptic curves. In: Proc of International Conference on Electronic Government and the Information Systems Perspective, Dublin. pp: 41 - 53.
[6] Xu Guang-zhi, Ye Zhen. (2008) A multi-candidate electronic voting scheme with secret tall ying.
Journal of Hefei University of Technology (Natural Science Edition), 31(9):1462 - 1464.

[7] Zhu Z. (2013) An electronic voting scheme based on fully homomorphism encryption. Guangzhou: Guangzhou University.

[8] Chillotti I., Gama N., Georgieva M., et al. (2016) A homomorphic LWE based E-voting scheme. Post-Quantum Cryptography. Berlin&Heidelberg: Springer International Publishing.

[9] Zhu Z., Liu Q., Tang C., et al. (2013) Electronic voting scheme based on LWE homomorphic encryption. NetInfo Security, 5: 8 - 11.

[10] Feng D., Pei D. (1999) Introduction to cryptography. Beijing: Beijing Science Publishing, pp: 195-204.

[11] Li X., Carlisle M.K., Aandis C. L., et al. (2007) An elementary electronic voting protocol using RFID. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy, Piscataway. pp: 234-238.