Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption

Guopeng Liao
School of Energy and Power, Xi'an Jiaotong University, Xi'an, Shaanxi Province, 710000, China
Corresponding author’s e-mail: Vivian.wang@cas-harbour.org

Abstract: In recent years, multi-candidate electronic voting has attracted tremendous attention and been put into lots of practice because of its outstanding effectiveness and convenience. As a result, it has become an urgent task to achieve the anonymity and public verifiability of electronic voting. Several schemes have been proposed so far, but most of them are either inefficient or too demanding of the security of the entities involved. Focusing on this problem, a multi-candidate electronic voting scheme based on fully homomorphic encryption and digital signature algorithm is proposed in the paper. To encrypt votes efficiently and reduce the dependence of different entities, the Identity Based Full Homomorphic Encryption (IBFHE) scheme is used in the paper. A homomorphic addition ticket counter is then used to realize the homomorphism calculation of encrypted votes. To settle the problem of identity authentication in electronic voting with high efficiency and security, Elliptic Curve Digital Signature Algorithm (ECDSA) is utilized. The capability of batching votes is achieved by making use of Single Instruction Multiple Data (SIMD) technology, which is designed for improving the efficiency of the voting system. Finally, the paper makes an analysis based on six security features of e-voting, which reveals the scheme's safety and feasibility.

1. Introduction
Since human society came into being, voting has been an important part of human political life. Nowadays, with the rapid development of modern electronic information technology, e-voting is gradually taking over traditional voting and being widely used because of its superiority. However, it is the security of e-voting that has been a bottleneck restricting its development. For instance, France and Belgium have stopped using e-voting owing to its unreliable safety. What is worse, there have been serious bugs found in the e-voting system of Norway, causing bad effects on the society. Thus, to take deep research into the safety of e-voting and to design privacy preserving e-voting schemes are of great necessity [1].

Most of the modern e-voting schemes are built upon cryptography. According to the cryptography technology adopted, the existing schemes could be divided into three types: schemes based on hybrid network protocol [2, 3], schemes based on blind signature [4, 5] and schemes based on homomorphic encryption technology [6-8]. The scheme based on hybrid network protocol satisfies the demand for safety, but due to the fact that each scrambling process involving in needs a zero knowledge proof, it is inefficient when the scale of voting activities is relatively large. The scheme based on blind signature is safe and efficient, but it requires the organizers, supervisors and counters involved to be completely safe, which can be tough to satisfy.
Relatively speaking, the scheme based on homomorphic encryption technology is comparatively efficient and, thanks to its capability of direct calculation of the ciphertexts, it is able to solve the problem of trust to reduce dependence of third parties perfectly. However, most of existing schemes based on homomorphic encryption algorithm are still of low efficiency when facing large-scale voting. Some of them can not even satisfy the request of the public verifiability of the system or generate ballots for multiple candidates.

Until 2020, the IBFHE \[9\] scheme was brought out, proven to be having the characteristics of fast operation speed and small space occupation. This paper is mainly based on IBFHE scheme. Simultaneously, a homomorphic addition ticket counter \[10\] and SIMD \[11\] technology are used, which ensure the anonymity and public verifiability of the e-voting system. After consulting some references, this paper proposes a scheme for e-voting with an aim of achieving higher efficiency and reducing the dependence of the security of third parties, which could offer as an instruction for the construction of an effective e-voting system.

2. Preliminaries

2.1. Digital Signature

Digital signature is a cryptographic system constructed mainly by public key cryptography that includes two parts: signature and authentication. In most cases, private key is used for signature and public key for authentication. There have been several digital signature schemes being proposed so far, ECDSA (Elliptic Curve Digital Signature Algorithm) being one of the best and most widely used. Reference \[12\] has proven that ECDSA has the advantages of strong anti-attack, small calculation, fast processing speed, small size of secret key and system parameters, low bandwidth requirements through software running test, which shows its superiority over most other algorithms for signature. Thus in this paper, ECDSA is used to realize the public verifiability of the scheme efficiently. ECDSA is a digital signature algorithm based on ECC (Elliptic Curve Cryptography) and DSA (Digital Signature Algorithm)(Figure 1), whose safety is based on the unfeasibility of elliptic curve discrete logarithm problem \[13\].

![Figure 1. Principle of ECDSA.](image)

2.2. Fully Homomorphic Encryption Algorithm

Fully homomorphic encryption is a kink of technology that can directly operate the encrypted data. Specifically, decrypting the ciphertext that has been through some calculations, the result would be the same as applying those calculations on the plaintext, as shown in Figure 2.
Figure 2. Principle of Fully Homomorphic Encryption.

Kim, etc. (2001) [14] proposed a e-voting scheme based on ElGamal, which can only get the final winner instead of the specific number of votes for each candidate; Additionally, it is not fit for large-scale voting since its homomorphism is realized by power calculation, which is not efficient.

In 2020, IBFHE scheme was proposed, which is based on lattice cipher and matrix. By converting data to a matrix, IBFHE can encrypted multi-data simultaneously, which significantly decreases encryption time. By letting the numbers on the diagonal be the information of candidates, we can get the votes for each candidate.

Thus IBFHE is adopted, whose additive homomorphism and multiplicative homomorphism are valid for computations of matrices.

Since original IBFHE can only encrypt a single bit, SIMD technology is adopted to pack the ballots to achieve multi-bit encryption. Compared with traditional technologies of ciphertext packing, SIMD can make it possible to only encrypt the set of all the ballots once and keep one private key, which can significantly reduce the encryption time and save the space of key storage.

2.3. Homomorphic Vote Counter

Basically, the counting operations in this e-voting scheme are calculations of decimal numbers in $\mathbb{Z}^+$. However, the plaintext mentioned in the IBFHE scheme is a $\{0,1\}^{l\times l}$ matrix. In order to convert the binary addition and multiplication to decimal addition and multiplication, a proper encoding and decoding scheme should be proposed.

$$
\mathbb{Z}^+ \xrightarrow{\text{codec}} \{0,1\}^{l\times l} \xrightarrow{\text{given scheme}} \mathbb{Z}_q^{l \times (2m+1)}
$$

(1)

Intuitively, by converting $\mathbb{Z}$ to a binary $\{0,1\}^l$ and then $\{0,1\}^l$ to a diagonal matrix $\{0,1\}^{l\times l}$ would make it. However, this does not work for the counting problem in the scheme. For example, for two decimal numbers $A = a_2 a_1$, $B = b_2 b_1$, where $a_i, b_i = 0, 1$. If $a_2 = b_2 = 1$ then there is equation (2), where the “1” is the overflow problem resulted by the carry generated by modular two addition. Thus when a great amount of numbers are added, the overflow problem would occur for many times. So a ticket counter is needed, which could solve the following problems: (1) Being capable of identifying the overflow problems when one occurs. (2) Being able to count how many times it occurs. Thus, the homomorphic vote counter proposed in reference[10] is adopted.

$$
C = A + B = a_2 a_1 \oplus b_2 b_1 = 1 c_2 c_1 \neq c_2 c_1
$$

(2)
3. Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption

3.1. Description for Scheme
There are six entities involved in the scheme, each of them being voter (V), registry (R), publicity center (PC), voting center (VC), certification authority (CA) and counting center (CC). The interactions between them are shown in Figure 3.

![Figure 3. Interactions between entities.](image)

3.2. Set Up
R, VC and CC use ECDSA algorithm to generate the key pairs for digital signature. Then they use their public keys to ask for certificates from the CA, after which CA would identify these entities in accordance with the business criteria. After confirming that the public keys received are exactly owned by these entities themselves, CA makes signatures on the entities’ public keys and generates certificates using its private key. The certificates are then publicized at the publicity center, which contains the identity information and public keys of these entities.

Key pair for signature of every entity:
- R: \( p_k_R = Q_R, s_k_R = d_R \)
- VC: \( p_k_VC = Q_VC, s_k_VC = d_VC \)
- CC: \( p_k_CC = Q_CC, s_k_CC = d_CC \)

Since voters should be anonymous, the key pair for V is kept for his own without being revealed. The key pair for V is as follows:

\[
p_k_v = Q_v, s_k_v = d_v
\]  

(3)

Additionally, CA would generate the key pairs for voting according to the number of candidates and the key generation algorithm in IBFHE.

The key pairs for voting are private key (4) and public key (5), where L is the maximum depth of the circuit. CA then sends the voting public keys to R, the private keys to CC, in a safe way.

\[
\begin{align*}
  s_k &:= S_L, \cdots, S_0 \\
  p_k &:= P_L, \cdots, P_0
\end{align*}
\]  

(4)  

(5)

3.3. Registering
V sends R his identity information for registration. R then checks whether V has the right to vote and whether this is his first time voting. If both of the conditions are satisfied, R sends V a unique identification \( ID_v_i \), a unique voting identity \( B_v_i \), a blank ballot, the public key for voting \( p_k \) and the signature on \( ID_v_i, B_v_i \) using its own private key.
After that, V verifies the signature. If the signature is authenticated to be a legal signature from R, V preserves (7). Meanwhile, R sends (8) to PC, where V can check out if he has been announced as a legal voter.

\[
\begin{align*}
\text{ID}_V \| \text{B}_V \| \text{SIG}_R (\text{ID}_V \| \text{B}_V) \\
\text{ID}_V \| \text{B}_V \| \text{SIG}_R (\text{ID}_V \| \text{B}_V) \\
\text{ID}_V \| \text{B}_V \| \text{SIG}_R (\text{ID}_V \| \text{B}_V)
\end{align*}
\]

### 3.4. Voting

Assuming that there are l candidates involving, the ballot of each V will be represented in the form shown below, where the diagonal holds the voting information for each candidate, 0 for disagree and 1 for agree.

Each ballot would be represented in this form:

\[
M = \begin{bmatrix}
m_1 \\
m_2 \\
\vdots \\
m_l
\end{bmatrix} \in \{0,1\}^{l \times d}
\]

(9)

Before sent to VC, every ballot will be encrypted as follows, where P is the public key for voting received from R.

\[
C = R^T \times P + (M \mid O_{l \times 2m}) \mod q
\]

(10)

After that, V signs on his identification \( \text{ID}_{vi} \) and voting identity \( \text{B}_{vi} \) using his public key for signature. Then V sends his identification \( \text{ID}_{vi} \), voting identity \( \text{B}_{vi} \), public key for signature \( \text{pk}_{vi} \), encrypted ballot \( C_i \) and the signature \( \text{SIG}_V (\text{ID}_{vi}, \| \text{B}_{vi}) \) to VC.

\[
\begin{align*}
\text{ID}_V \| \text{B}_V \| \text{pk}_{vi} \| C_i \| \text{SIG}_V (\text{ID}_V \| \text{B}_V) \\
\end{align*}
\]

(11)

After receiving the above information, VC verifies whether the signature of the voter is legal in accordance with the signature information and public key sent by the voter. If it is legal, then VC uses R's public key to verify whether the \( \text{ID}_{vi} \| \text{B}_{vi} \) in \( \text{SIG}_R (\text{ID}_{vi} \| \text{B}_{vi} \) is the same with that in \( \text{SIG}_V (\text{ID}_{vi} \| \text{B}_{vi} \). If they are the same, then the V can be determined as a legal voter certified by the R; Besides, \( \text{B}_{vi} \) will be checked to make sure the uniqueness of this ballot. If any of these conditions is not satisfied, the ballot will be discarded. Finally, VC will send the signature of authenticated ballot to PC for publicity.

\[
\text{SIG}_V (\text{ID}_V \| \text{B}_V \| C_i)
\]

(12)

### 3.5. Counting

After the deadline for voting, CC gets all the ballots from PC and verifies the validity of every (12) using the public key of VC. If one is confirmed to be valid, then it will be taken into calculation of the homomorphic counter mentioned above. With all valid ballots being calculated, CC gets the results \( S, C^{(0)} \). After that, CC signs on \( S, C^{(0)} \) and sends (13) to PC.

\[
S \| C^{(j)} \| \text{SIG}_C (S \| C^{(j)})
\]

(13)

Finally VC decrypt \( S, C^{(0)} \) using its voting private key \( sk:=S_{L_0}...S_0 \) to get the result, which is the number of ballots of every candidate. VC then sends the result to PC for supervision.
4. Safety Analysis

Anonymity: Firstly, it is only during the registering stage when the voter's information is revealed and checked by R. After that, every voter Vi will be replaced with the identification IDVi, which is totally unrelated with the identity information about the voter. Secondly, every ballot would be encrypted using the public key for voting. In other words, except the voter, no one else could get access to the content of the ballot, nor can they match the ballot with its voter. So compared with ordinary voting scheme where VC and CC can get to know the content of ballots, the scheme proposed here can be delivered to any third party no matter it is safe or not.

Public Verifiability: At the voting stage, every valid ballot the VC collects will be publicized at PC, where every voter can compare the information on the bulletin board with the information he holds to check if his ballot has been properly counted.

Validity: Firstly, this scheme is mainly based on ECDSA and IBFHE, which ensure a higher security, correctness and efficiency over most other voting systems. Secondly, the public key of each party in the scheme is overt, any voter or third party can verify the rightness of any process. Thirdly, at each stage of the scheme, identity authentication is carried out to prevent spiteful voters from ruining the vote.

Legitimacy: At registering stage, every voter needs to send R his identity information, which would be verified by R. Only those who are authenticated can get the unique identification IDVi to participate in the following voting activity.

Uniqueness: At registering stage, a legal voter would get a unique identification IDVi as his qualification to vote. If an ID has voted once, then new ballots will be rejected. Meanwhile, R would only send an ID to a same identity information for one time.

Completeness: Ballots from illegal voters or do not satisfy the uniqueness will be discarded. Only authenticated ballot can be taken into count.

5. Conclusion

In this paper, a multi-candidate electronic voting scheme based on ECDSA and IBFHE is proposed, which achieves the anonymity and public verifiability of the voting system. Compared with most other schemes, it enhances the efficiency while reducing the dependence of third parties. But considering the time complexity of asymmetric encryption itself, there is still lots of room for improvement. More technologies and new algorithms can be integrated for further advancement of efficiency and security.

Acknowledgments
The work was supported by Prof. Ming. Deh Huang.

References
[1] Pu, H., Cui, Z., Liu, T. and Rao, J. (2020) Comprehensive Review of Secure Electronic Voting Schemes. Computer Science, pp. 1-2.
[2] Lee, B., Boyd, C., Dawson, E., et al. (2004) Providing receipt-freeness in mixnet-based voting protocols. In: Lim, J.I., Lee, D.H.(eds.). Information Security and Cryptology–ICISC 2003. Berlin, Heidelberg: Springer, pp. 245–258.
[3] Chaum, D., Ryan, P.Y.A., Schneider, S. (2005) A practical voter verifiable election scheme. In: De Capitani Di Vimercati, S., Syverson, P., Gollmann, D.(eds.) Computer Security–ESORICS. Berlin, Heidelberg: Springer, pp. 118–139.
[4] Fujioka, A., Okamoto, T., Ohta, K. (1992) A practical secret voting scheme for large scale elections. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. Queensland, Australia, pp. 244–251.
[5] Radwin, M.J. (1995) An untraceable, universally verifiable voting scheme. Seminar in Cryptology. http://www.radwin.org/michael/project/voting.pdf.
[6] Zhang, P., Yu, J., and Liu, H. (2011) A homomorphic signcryption scheme and its application in electronic voting. Journal of Shenzhen University Science and Engineering, 28(6): 489-494

[7] Rivest, R.L., Adleman, L., Dertouzos, M.L. (1978) On data banks and privacy homomorphisms. Foundations of Secure Computation, 4(11):169-180.

[8] Boneh, D., Goh, E. J., Nissim, K. (2005) Evaluating 2-DNF formulas on ciphertexts [C] / /Proc of the 2nd International Conference on Theory of Cryptography. Berlin: Springer, pp. 325-341.

[9] Chen, H., Huang, J., Chen, H.L., et al. Identity-based Matrix (level) fully homomorphic encryption scheme. Journal of Frontiers of Computer Science and Technology, pp. 1-12

[10] He, Q., Shen, W. (2019) Multi-Candidate Electronic Voting Scheme Based on Homomorphic Encryption, Computer Systems and Applications, 28(2): 146–151. http://www.c-s-a.org.cn/1003-3254/6773.html

[11] Hiromasa, R., Abe, M., Okamoto, T. (2015) Packing messages and optimizing bootstrapping in GSW-FHE. In: Katz J., ed. Public Key Cryptography (PKC 2015). Berlin, Heidelberg: Springer, pp. 699–715.

[12] Zhang, W. (2003) The Algorithm Implementation of ECDSA and Security Analysis, Information and Electronic Engineering, 1(2): 7-12

[13] Johnson, D., Menezes, A., Vanstone, S. (2001) The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1(1): 36–63. [doi: 10.1007/s102070100002

[14] Kim, K., Kim, J., Lee, B., et al. (2001) Experimental design of worldwide internet voting system using PKI. SSGRR.