A Multi-party Secure E-commerce Voting Scheme Based on SDGHV Algorithm

Jiahui Deng¹, Jing Lin², Jiayun Hu³ and Jiawei Qian¹ ⁴*,b

¹ International Investment and Finance, Jiangxi University of Finance and Economics, Nanchang, Jiangxi Province, 330013, China
² CIMA, Jiangxi University of Finance and Economics, Nanchang, Jiangxi Province, 330013, China
³ Econometrics, University of Sydney, Sydney, 2050, Australia
⁴ Software engineering, East China Normal University, Shanghai, 200062, China

aemail: fionanguyen1113@163.com
bCorresponding author's email: jwqian@stu.ecnu.edu.cn

Abstract. In the era of continuous development of e-commerce, the selection of e-commerce affects the development of e-commerce business and management efficiency. Based on the multi-party secure computing technology, this paper designs a set of the electronic voting scheme based on SDGHV multi-party secure data platform for the feedback on customers' opinions after the goods are sold, which provides a useful reference for the selection of e-commerce products.

1. Introduction

Secure multi-party computing can solve the collaborative computing problem of privacy protection between a group of parties that do not trust each other under the condition of ensuring the independence of input information, the correctness of calculation and confidentiality. At present, the theoretical research on the privacy protection function of secure multi-party computing mainly focuses on the aspects of Secret Key Management, Privacy-protected Electronic Auctions, Online Voting, which has achieved many positive results. However, due to the imperfect theoretical research, lack of essential research tools and low operational efficiency, the improvement of its degree of practicality needs to be further realized. MPC's fundamental task is to calculate the contract function without a trusted third party. In this process, the authenticated homomorphic encryption enables users to analyze and retrieve specific data even in case of data encryption, thus improving the data processing efficiency and the security of delivery while ensuring correct decryption results.

The essence of electronic voting is a multi-party security protocol, which is the first electronic voting protocol proposed by Chaum[1] in 1981 based on hybrid network and RSA public key. The application of MPC in Electronic Voting can realize two-way verification without a third party's interference, thus protecting participants' privacy to the greatest extent. Meanwhile, it can distinguish dishonest voters and counting managers, which can better guarantee voting security and fairness. The original electronic voting protocol based on blind signature technology is the FOO protocol proposed by Fujioka[2]. This protocol can realize large-scale Electronic Voting based on the blind signature, but it does not have anti-forgery and anti-collusion aggression. With the development of homomorphic...
encryption technology, the application of homomorphic encryption technology in electronic voting can ensure the secrecy, anonymity and encryption. Ihsan Jabbar[3] et al. realized two essential requirements of Electronic Voting through the ElGamal cryptography system, the security of electronic voting equipment and voters' ability to voluntarily or involuntarily choose. Wang[4] et al. proposed an electronic voting scheme of free receipt based on blockchain, which ensures Blockchain distribution creditability. Li[5] et al. used the multi-secret sharing scheme with multi-level access structure to enable the public to verify the final election results; Baudier Patricia[6] et al. proposed to use qualitative methods and blockchain technology to reduce the abstention rate of electronic voting and strengthen democracy during the outbreak of COVID-19.

In the context of the continuous development of information technology, how to efficiently use big data analysis and information technology to help the scientific implementation of cross-border e-commerce product selection has become an urgent problem to be solved at present. Seo Min-Kyo adopted emotion analysis method to measure the valid integer of user polarity and subjectivity and explored the reliability of Google application score, but this method lacked relevant privacy protection. Soma[7] adopted k-means clustering algorithm to combine the characteristics of products purchased by customers, generate product keys unique to the business, and build models to subdivide products according to the quantity and revenue of products sold, as well as the price and revenue of products sold, but large communication overhead would occur.

Therefore, based on the current research results, this paper designs a multi-party privacy voting system based on SDGHV password scheme by combining electronic voting based on secure multi-party computation with the selection of e-commerce, which innovates the application scenario. After the goods are sold, the system will input the encrypted feedback data into the multi-party secure computing platform for calculation, and the obtained results will be sent to the merchants in the form of "recommended" or "not recommended". In this process, users' basic information will be fully protected, and merchants will have no way to know the specific preference data of consumers. In this way, not only the privacy of users will be protected to a great extent, but also the abnormal commodity data caused by merchants' purchase reviews, rebates and other illegal operations will be reduced at the same time.

Therefore, the scheme proposed in this paper has important practical significance for the comprehensive application of e-commerce.

2. The application architecture design of multi-party secure computing e-commerce selection

With the rise of internet-based B2C and B2B E-commerce, privacy protection in this environment has become increasingly prominent. At present, there are many privacy protection measures and schemes in the field of E-commerce. However, in the actual operation process, especially in the evaluation field of commodities, on the one hand, there are problems such as too many authorized functions, invasion of privacy, and difficulty in securing security for the platform, on the other hand, there is the problem of feedback information distortion.

The confidentiality, verifiability, and complete performance of the multi-party secure computing platform and blockchain technology can protect consumers' feedback from being corrupted by illegal operations, and reduce the inauthenticity of malicious or false evaluations. At the same time, each participant's voting information will not be disclosed to others, ensuring users' privacy and improving their trust in the platform. Also, businesses can take the voting results as a reference for product selection and marketing, and other consumers can also get the real evaluation results of the products if they need them.

2.1. From the Perspective of Multi-party Security Computing, Design of Electronic Voting System for E-Commerce Commodity Selection

This scheme's voting model is divided into four roles. The detailed description is as follows:
1) E-merchant: The main initiator of electronic voting, responsible for setting the parameters of voting time, voting questions, voting options, determining the whitelist of voters (only authenticated voters can join the whitelist), and managing the voting process.

2) Voter: The participant who has passed the identity authentication in the electronic voting is responsible for the login stage and voting stage in the voting process.

3) Multi-party Secure Computing Platform: Statistics and analysts in the process of electronic voting, carry out modeling analysis of the votes and send the results to e-commerce companies.

4) Blockchain: Data protector in electronic voting to ensure that consumer information will not be disclosed, the password algorithm in the voting process is correctly executed and acts as a bulletin board for electronic voting (some data can be publicly queried on the blockchain).

Table 1. Design of Electronic Voting System for E-Commerce Commodity Selection

2.2. The application structure of e-commerce commodity selection

2.3. Within a complete application framework (as shown in Figure 2), businesses can get the information they need efficiently, quickly, and uniquely. Businesses will first create questionnaires that meet their goals and set expectations and then send them to their research platforms and multi-party secure computing platforms, respectively. After the voters log in, the survey platform will automatically distribute the questionnaire. Then, after completing the questionnaire, the data will be automatically imported into the multi-party secure computing platform for calculation and generation of results according to the expected value. Later, the platform will send the calculated results to the merchant who can never access the original data’s input source in the whole process. The MPC platform, which is the core of the whole process, can combine multiple computer mathematical models to obtain the data needed to achieve users' goals, avoid interference from third parties, and achieve two-way authentication, which can better guarantee voting security and fairness. Simultaneously, the whole process will be escorted by blockchain technology, strictly ensuring data integrity, non-tampering and non-disclosure.
2.4. Case study

Step 1. Assume that an e-commerce company A wants to investigate the customer feedback of products B in 2019, and a total of N different customers have purchased B products in this year.

Step 2. A designed the questionnaire and the corresponding threshold (agreed by The T party) and imported into the multi-party secure computing platform.

Step 3. The e-commerce platform will randomly distribute questionnaires to the signed customers in the group sampling survey.

Step 4. The questionnaire results filled in by customers are only presented as to whether or not. The key generator will automatically generate public-private key pairs and two random number vectors with the sum of 0, among which the public key is given to N participants with one random number given to MPC platform, and the private key and another random number vector are sent to the merchants.

Step 5. The feedback information is encrypted and submitted to the MPC platform for analysis and calculation.

Step 6. The MPC platform will compare the calculated result with the threshold value set before calculation, and then the company will get the decision result of "this product is worthy of promotion" or "this product is not worthy of promotion", and then announce it publicly as they wish.

Step 7. A will carry out the next stage of commodity marketing planning according to the results.

Step 8. Feedback the results to customers according to their needs to facilitate their future consumption decisions.

3. Homomorphic Cryptographic Scheme Algorithm Based on Integer

| KeyGen: The four parameters involved control the number of elements in the public key and the bit lengths of different integers. We use $\tau$ for the number of elements in the public key, $\gamma$ for their bit length, $\eta$ for the bit length of private key $P$, $\rho(p0$ respectively) for the bit length of noise in the public key (the new ciphertext respectively). Note that all of the above parameters are polynomials in the security parameter. |
|---|
| Select the security parameter $\eta$, and randomly select a bit of odd $p$ as the private-key form $(2\mathbb{Z}+1)\cap(2^{\eta-1},2^{\eta})$. Then a $q_0$ is selected at random from $\mathbb{Z}\cap[1,\frac{2^\gamma}{p}]$ and $x_0 = q_0 \cdot p$ |
will be calculated, and the public-private key pair is denoted as \((pk, sk) = (x_0, p)\).

It randomly selects one noise \(r \in \mathbb{Z} \cap (-2^\nu, 2^\nu)\) and one noise \(q \in \mathbb{Z} \cap \{1, \frac{2^\nu}{p}\}\) and sends the calculation of \(l = q \cdot p + 2r\) to the encryption party.

Enc: The binary encrypted message is denoted as \(m = (m_1, \ldots, m_r)\), and the cypher party computes \(c_i = [l + m_i]_p\) to obtain a ciphertext of \(c = (c_1, \ldots, c_r) [z]_p\), the remainder of \(z\) respect to \(P\).

Dec: Calculate \(m_i = [c_i \mod p]_2\) to get \(m = (m_1, \ldots, m_r)\).

Since sdghv is a fully homomorphic algorithm on binary, setting the appropriate model can complete the operation properly. For example, if at least two votes are passed by three people, the voting vector of three people is \(m_1, m_2, m_3\), and the calculation model is \(f (m_1, m_2, m_3) = (m_1 \cap m_2) \cup (m_2 \cap m_3) \cup (m_1 \cap m_3)\).

4. The verification process of the algorithm

See reference [8] for the correctness and safety proof of DGHV algorithm. The correctness of SDGHV algorithm is verified as follows: The public key \(x_0 = q_0 \cdot p\) (unknown parameter, \(p\) is private key), \(m \in \{0, 1\} \cdot 2^{-\frac{\eta}{2}}\), \(q_0 < p\), \(p\) is an odd number of \(\eta\) bits.

\[
\text{Encrypt } c_i = [(l + m_i) \mod x_0 = (q \cdot p + 2r + m_i) \mod q_0 \cdot p] \\
\text{and decrypt } m_i' = c_i \mod p \mod 2 \quad m_i' = (q \cdot p + 2r + m_i) \mod q_0 \cdot p \mod p \mod 2.
\]

So there is \(t\) such that:

\[
0 \leq (q \cdot p + 2r + m_i) - t \cdot q_0 \cdot p < q_0 \cdot p = ((q \cdot p + 2r + m_i) - t \cdot q_0 \cdot p) \mod p \mod 2 = (2r + m_i) \mod 2 = m_i
\]

The homomorphism properties are verified as follows:

\[
(q \cdot p + 2r + m_j) + (q \cdot p + 2r + m_j) \mod q_0 \cdot p \mod p \mod 2 = (m_i + m_j + 4r) \mod 2 = (m_i + m_j) \mod 2
\]

\[
(q \cdot p + 2r + m_j)(q \cdot p + 2r + m_j) \mod q_0 \cdot p \mod p \mod 2 =

((q \cdot p + 2r)^2 + (q \cdot p + 2r)(m_i + m_j) + m_i \cdot m_j) \mod q_0 \cdot p \mod p \mod 2
\]

So there is \(t\) such that:

\[
0 \leq (q \cdot p + 2r)^2 + (q \cdot p + 2r)(m_i + m_j) + m_i \cdot m_j - t \cdot q_0 \cdot p < q_0 \cdot p = 4r^2 + 2r(m_i + m_j) + m_i \cdot m_j \mod 2 = m_i \cdot m_j \mod 2
\]

Its security assurance comes from the computation of \(m_i' = c_i \mod p\).

Moreover, \(p\) is not deterministic. When \(P\) is fixed, and \(L\) is continually updated, there will be a tricky problem approximating the multiple \(L\)'s greatest common divisor.

5. Conclusion

Under the background of the increasing maturity of multi-party security technology, this paper focuses on the analysis of the application of multi-party security computing technology based on electronic
voting in the field of e-commerce selection. Moreover, the increasing improvement of people's living standard and the increasing diversification and richness of commodity selection, a useful commodity feedback mechanism has a specific reference for consumers' selection. Also, it has universality for the daily operation of e-commerce.

At present, the application of e-commerce based on the combination of blockchain and MPC technology is still under constant exploration, and too large data scale, low computing efficiency, high-cost problems are still waiting to be solved. Simultaneously, the standard threshold that is difficult to establish, the randomness of consumer feedback data and the uncertainty of future scientific and technological development all lead to the exploration state that the application of MPC technology in E-commerce Selection still needs to be further summarized in theory and practice.

All in all, the application of Multi-party Secure Computing and BlockChain technology to E-commerce can further promote E-commerce's excellent development, but it will also be a long-term process of exploration. Only through continuous learning in practice can E-commerce achieve the goal of better service for consumers.

References
[1] Untraceable electronic mail, return addresses, and digital pseudonyms[J]. David L. Chaum. Communications of the ACM. 1981 (2)
[2] FUJIOKA A., OKAMOTO T., OHTA K. A practical secret voting scheme for large scale elections [C]. Advances in Cryptology-AUS-CRYPT '92 Workshop on the Theory and Application of Cryptographic Techniques Proceedings. 1993: 244-251.
[3] Ihsan Jabbar, Saad Najim Alsaad. Design and Implementation of Secure Remote e-Voting System Using Homomorphic Encryption. 2017, 19(5):694-703.
[4] Baocheng Wang, Jiawei Sun, Yunhua He, et al. Large-scale Election Based On Blockchain. 2018, 129:234-237.
[5] Jing Li, Xianmin Wang, Zhengan Huang, et al. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. 2019, 130:91-97.
[6] Baudier Patricia, Kondrateva Galina, Ammi Chantal, et al. Peace engineering: The contribution of blockchain systems to the e-voting process. 2021, 162
[7] Soma Bandyopadhyay, S. S. Thakur, J. K. Mandal. Product recommendation for e-commerce business by applying principal component analysis (PCA) and K -means clustering: benefit for the society. 2020, :1-8.
[8] Dian-Hua T , Yun-Fei C , Hao-Miao Y . Compactly-Optimized DGHV Fully-Homomorphic Encryption Scheme[J]. Communications Technology, 2013