Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/135/2025.21090

Data Privacy Protection Utilizing Homomorphic Encryption Techniques

Zongwei Li[1,a,*]

[1]*School of Information and Intelligent Engineering, Zhejiang Wanli University, Ningbo, 315000, China*
a. 2022014439@zwu.edu.cn
**corresponding author*

Abstract: In the current era with the rapid development of the Internet, although a variety of technologies have offered convenience to people's lives, numerous problems have arisen regarding the security of individual and collective data, Problems such as data privacy leakage occur continuously. The content of this review is data privacy protection based on homomorphic encryption. Firstly, the basic principle and formula of homomorphic encryption are briefly introduced. Then, the homomorphic encryption-based data privacy protection approach is developed in response to the importance of safeguarding data privacy. In the case of partially homomorphic encryption, the article refers to such homomorphic encryptions as PPDM, STHE, and ECC. In fully homomorphic encryption, such as DBMS, HTM-FHE, and MKFHE, are mentioned. Under the current homomorphic encryption technology, the performance of data protection has witnessed a remarkable improvement; however, there exist numerous deficiencies. The majority of algorithms are relatively complex and consume a considerable number of resources. The aim of this review lies in facilitating readers' prompt comprehension of the existing technologies and development status in this domain, as well as the merits and demerits of current technologies.

Keywords: Homomorphic encryption, data privacy, privacy protection.

1. Introduction

In the current era of rapid advancement in information technology, data privacy protection has emerged as a critical issue that demands urgent resolution. With the extensive utilization of technologies like cloud computing, big data, and artificial intelligence, the collection, storage, and processing of data have become increasingly prevalent, and the consequent privacy leakage and data security problems have grown increasingly severe. Traditional data protection approaches often rely on encryption and access control. Nevertheless, in practical applications, the encryption of data frequently results in the inability to conduct direct computations on the ciphertext, thereby restricting the efficient utilization of data. To solve this problem, homomorphic encryption technology came into being [1]. It allows for direct computations on encrypted data, and the computational results remain correct after decryption, thereby achieving effective data processing while safeguarding data privacy.

Homomorphic encryption technology can be categorized into multiple types in accordance with different algorithms, such as Partial Homomorphic Encryption (PHE) [2], Fully Homomorphic

DOI: 10.54254/2755-2721/135/2025.21090

Encryption (FHE) [3], etc. These distinct homomorphic encryption algorithms possess unique features and are applicable to diverse application scenarios, offering flexible solutions to satisfy the ever-increasing demand for data privacy protection. Although remarkable advancements have been achieved in the theoretical research and technical realization of homomorphic encryption, it still confronts challenges like computational efficiency, algorithmic complexity, and security in practical applications. Secondly, it is known from literature [4], the current status of data protection in the domestic context. Hence, an in-depth study on the application of homomorphic encryption based on different algorithms in data privacy protection not only contributes to understanding its technical characteristics but also offers significant theoretical support and practical guidance for future research and application. This paper will undertake a classified overview of the principles, strengths and weaknesses of various homomorphic encryption algorithms and their practical applications in data privacy protection, with the expectation of offering references for researchers and developers in related domains.

2. Homomorphic Encryption

2.1. A Simple Outline of Homomorphic Encryption

Homomorphic encryption is an encryption method that allows direct computation on ciphertexts without the need for prior decryption, thus ensuring the privacy and security of the data. The fundamental principle lies in the mathematical construction, such that specific operations executed on the ciphertext can correspond to the identical operations on the plaintext. For example, if a homomorphic encryption scheme supports addition, carrying out an addition operation on the ciphertexts and then decrypting will result in the sum of the two plaintexts. By this means, users can conduct data processing and analysis while safeguarding sensitive information, and it is extensively utilized in domains like cloud computing, financial services, and medical data analysis. Whether it be partially homomorphic encryption (supporting a single type of operation) or fully homomorphic encryption (supporting arbitrary operations), homomorphic encryption offers a potent tool for realizing secure computing. The formulas of homomorphic encryption primarily pertain to the encryption and decryption processes, along with the nature of homomorphic operations. Herein are some prevalent homomorphic encryption formulas, encompassing the fundamental notions of additive homomorphic encryption (PHE) and multiplicative homomorphic encryption (FHE).

Additive homomorphic encryption enables the performance of addition operations on ciphertexts without decryption. Supposing there exist an encryption function E, a decryption function D, and it supports addition operations. Homomorphic encryption allows for addition operations on encrypted data. Supposing there exist an encryption function E, a decryption function D, and it supports addition operations.

For the plaintexts m1 and m2, they are encrypted as ciphertexts:

$$c1 = E(m1) \tag{1}$$

Property of Additive Homomorphism:

$$c1 = E(m1) \tag{2}$$

Decrypt the encrypted sum:

$$E\big(m1\big) + E\big(m2\big) = E(m1 + m2) \tag{3}$$

Multiplicative homomorphic encryption permits multiplication operations on encrypted data. Let there be the same encryption function E and decryption function D.

DOI: 10.54254/2755-2721/135/2025.21090

$$D\left(E(m1)+E(m2)\right)=D(c1+c2)=m1+m2 \tag{4}$$

For the plaintexts m1 and m2, they are encrypted as ciphertexts:

$$c1=E(m1) \tag{5}$$

$$c1=E(m1) \tag{6}$$

Property of Multiplicative Homomorphism:

$$E(m1)\times E(m2)=E(m1\times m2) \tag{7}$$

Decryption of Multiplication:

$$D\left(E(m1)\times E(m2)\right)=D(c1\times c2)=m1\times m2 \tag{8}$$

2.2. The Classification of Homomorphic Encryption

Homomorphic encryption can be categorized into three classes according to the types of operations it supports: Partially Homomorphic Encryption (PHE), Fully Homomorphic Encryption (FHE), and Somewhat Homomorphic Encryption (SHE). Partially homomorphic encryption merely supports a single operation (such as addition or multiplication), allowing particular computations to be performed on ciphertexts without the need for decryption. Fully homomorphic encryption supports an arbitrary number of addition and multiplication operations and is capable of performing complex computations on encrypted data. Somewhat homomorphic encryption lies between the two, supporting a finite number of addition and multiplication operations and being applicable to some specific application scenarios. Via these classifications, the homomorphic encryption technology is capable of fulfilling the security computing demands in diverse scenarios. In this review, it is mainly divided into two parts: partial homomorphic encryption and full homomorphic encryption for discussion, summarizing the data privacy protection methods depend on homomorphic encryption.

2.2.1. Partial Homomorphic Encryption

Partially Homomorphic Encryption (PHE) constitutes an encryption technique that enables specific types of operations on encrypted data without the necessity of decryption, thereby safeguarding the privacy and security of the data. Contrary to fully homomorphic encryption, partially homomorphic encryption merely supports one category of operations, for instance, addition or multiplication, rather than both concurrently. By this means, users are capable of conducting computations when the data is encrypted, guaranteeing the confidentiality of the original data. It is extensively utilized in domains such as secure data processing, cloud computing, and privacy protection. Partially homomorphic encryption, while offering data security, is still capable of attaining a certain extent of data processing capacity and constitutes a significant part of modern privacy protection technology.

Partially Homomorphic Encryption (PHE) has manifested its crucial value in numerous practical application scenarios. Firstly, within a cloud computing context, users are capable of uploading their sensitive data to the cloud after encrypting it. Cloud service providers can undertake specific operations (such as addition) on the encrypted data without accessing the original data, thereby effectively safeguarding user privacy. Secondly, in the domain of financial services, partially homomorphic encryption can be employed to compute a customer's credit score or risk assessment securely without disclosing their personal financial information. Moreover, in medical data analysis, researchers are able to carry out statistical analysis on patients' encrypted health data, guaranteeing the privacy of the data and facilitating data sharing and collaboration. In summary, partially

DOI: 10.54254/2755-2721/135/2025.21090

homomorphic encryption provides a flexible and pragmatic solution for data privacy protection, facilitating secure data processing and analysis in diverse industries.

2.2.2. Fully Homomorphic Encryption

Fully homomorphic encryption is an advanced encryption technique that permits any sort of computation, including addition and multiplication,to be performed on encrypted data without needing to decrypt it. This means that users can perform complex data processing and analysis while maintaining data confidentiality. Fully homomorphic encryption is founded upon profound mathematical theories, typically encompassing domains such as polynomial rings and lattice theory. The core concept thereof lies in constructing a specific encryption schema that allows encrypted data to retain its structure and properties when performing operations, thereby yielding the correct plaintext outcome after decryption. Although fully homomorphic encryption holds immense potential in theory and offers a comprehensive solution for secure computing and privacy protection, the problems of computational complexity and efficiency still constitute the principal challenges in current research.

Fully Homomorphic Encryption (FHE) is progressively manifesting its potential in contemporary practical applications, particularly in data processing scenarios where a high degree of privacy protection is demanded. For example, in cloud computing, users are capable of uploading sensitive data after encryption. Cloud service providers can conduct computations directly on such data without decryption, like data analysis and machine learning model training, thereby safeguarding user privacy. Additionally, fully homomorphic encryption has applications in the field of medical and health. Researchers can undertake analyses of the encrypted medical records of patients to derive statistical results without exposing individual information. Furthermore, the financial sector is also exploring the utilization of fully homomorphic encryption for conducting secure risk assessment and credit scoring, further propelling the demand for privacy computing technologies. Notwithstanding the considerable computational cost of fully homomorphic encryption, its superiority in guaranteeing data security and privacy has gradually garnered attention and experimentation in numerous domains.

3. The Significance of Data Privacy

In the digital era, the significance of data[5] privacy has become ever more salient. With the prevalence of the Internet and smart devices, a considerable amount of information, such as personal information, behavioral data, and consumption habits, is collected, stored, and analyzed. The leakage or misuse of these data may not only result in the violation of personal privacy but also give rise to more extensive social problems. Firstly, data privacy is directly associated with an individual's fundamental rights. Every person has the right to control their own information and determine when, where and in what manner to share personal data. In the absence of effective privacy protection mechanisms, personal information may be utilized by lawbreakers, resulting in criminal acts such as identity theft and fraud, and bringing about economic losses and psychological harm to the victims. Secondly, data privacy is of paramount importance for the reputation and trust of enterprises. When collecting and processing user data, enterprises must adhere to relevant laws and regulations and guarantee the privacy and security of users. If an enterprise is undermined by a data leakage incident, it will not merely lose the trust of its clients but also might encounter legal lawsuits and substantial fines. This renders data privacy a crucial element for the sustainable development of enterprises. Moreover, data privacy is pertinent to the stability and security of society. In the context of the continuous advancement of big data and artificial intelligence technologies, the misuse of personal data may give rise to problems such as social discrimination, surveillance and manipulation, thereby influencing social justice and democratic values. Hence, ensuring data privacy is not merely the

DOI: 10.54254/2755-2721/135/2025.21090

protection of individuals but also a crucial link in maintaining the overall interests of society. On the whole, the importance of data privacy is manifested in multiple domains such as safeguarding individual rights, preserving corporate reputations, and facilitating social security. In this era characterized by the rapid advancement of information technology, all parties should jointly exert efforts to enhance the protection of data privacy and raise public awareness regarding privacy, with a view to constructing a safer and more trustworthy digital environment.

4. Approaches to Data Privacy Protection

4.1. Partial Homomorphic Encryption

Internet giants employ modern technologies to amass copious amounts of data and apply the same to data mining for the purpose of prediction and decision-making in a multitude of domains such as healthcare, network analysis, insurance, market basket analysis, and bioinformatics. However, the extensive repository gathers a wide variety of data types, and it inevitably accumulates a considerable amount of private and sensitive data related to users.The exposure of such private and sensitive information could potentially compromise users' privacy. In the past few years, in various data mining applications, the issue of privacy is growing in importance. Privacy-Preserving Data Mining (PPDM) [6] has evolved as a solution to privacy problems. PPDM is committed to safeguarding personal data without undermining data utility. Literature [7] proposed a homomorphic encryption scheme based on privacy chain, using a statistical transformation method that incorporates weights based on evidence and information value, for protecting users' privacy and confidential information. The introduced Statistical Transformation of Homomorphic Encryption (STHE) algorithm will modify the numerical and categorical values within the adult income, bank marketing, and lung cancer datasets while preserving the utility of the data. In STHE, the quasi-identifiers are initially modified using IV, then the homomorphic encryption based on the privacy chain is applied via RSA for protecting data privacy. The performance of the STHE algorithm is compared with the state-of-the-art algorithms of classifier models, decision trees, random forests, extreme gradient boosting, and support vector machines. The experimental outcomes show that the proposed STHE algorithm surpasses current methods in multiple dimensions, such as precision, efficiency, data conversion, information retrieval, privacy preservation, and data utility.

Among the aforementioned data protection approaches based on PPDM and STHE, STHE safeguards personal information through methods such as homomorphic encryption and privacy swapping, thereby lowering the risk of data leakage. Regarding data utility, this method, while protecting privacy, does not impact the usability of the data, ensuring that the data can still be utilized for effective analysis and decision-making. Regarding compatibility, STHE can be employed in conjunction with multiple classifier models, such as decision trees, random forests, and so forth, exhibiting considerable flexibility and superior adaptability to diverse application scenarios. Although the approach mentioned in literature [7] has delivered remarkable performance in data privacy protection, it also presents certain shortcomings. In terms of computational overhead, homomorphic encryption typically has a high computational complexity, which might result in slower processing speeds, particularly when handling large-scale datasets. Secondly, with respect to key management, homomorphic encryption demands a more refined key management mechanism. The security and storage of keys also constitute a considerable challenge for the privacy and security of data. Furthermore, regarding data perturbation, although the objective of STHE is to preserve data utility, the perturbation of data during the implementation of statistical transformations might result in information loss, influencing the accuracy of certain specific analytical tasks. Overall, the STHE algorithm exhibits remarkable performance and privacy protection capabilities in privacy-preserving data mining. Nevertheless, during the implementation process, matters such as computational

DOI: 10.54254/2755-2721/135/2025.21090

expenses, complexity, and compliance need to be contemplated. How to achieve a favorable equilibrium between safeguarding privacy and preserving data utility constitutes a crucial direction for the further advancement of this approach.

Concerns about data security and privacy protection are increasingly prominent, presenting substantial challenges to the advancement of cloud computing. In order to enhance the existing homomorphic encryption technology, reference [8] put forward the ECC homomorphic encryption algorithm and designed and implemented it. Based on this, an aggregation model for data privacy protection was established, and the efficacy of secure operations on ECC homomorphic encrypted data was analyzed. In comparison with the conventional RSA encryption algorithm, the ECC homomorphic encryption algorithm exhibits greater security. When the key length gradually increases, the security of ECC with over 300 bits is significantly superior to that of RSA with over 2000 bits. Concurrently, the ECC homomorphic encryption algorithm excels RSA in aspects of encryption time and cipher size. The ECC homomorphic encryption algorithm possesses merits such as low computational complexity and favorable security performance. The ECC homomorphic encryption algorithm referred to in literature [9] has made considerable contributions to the protection of data security and privacy. Regarding security, the security provided by ECC is higher than that of RSA at shorter key lengths. For example, the security offered by a 300-bit ECC key can surpass that of a 2000-bit RSA key. This allows ECC to strike a superior balance between security and computational efficiency. Furthermore, ECC homomorphic encryption possesses a smaller key size, capable of reducing storage and transmission costs while guaranteeing the same level of security. This is of great significance for resource-constrained devices, such as common Internet devices. Finally, the computational complexity of ECC is relatively low and it is typically faster than RSA. This implies that when handling large-scale data, ECC homomorphic encryption can markedly enhance the extraction performance of the system. Although ECC boasts numerous advantages, it exhibits a certain degree of dependence in terms of implementation complexity as well as the selection of algorithms and parameters. In the aspect of implementation, the realization of ECC is relatively intricate, particularly in the selection of different curves and parameter configuration, demanding more specialized knowledge and experience. If the parameters are selected inappropriately, it could result in security loopholes.

4.2. Full Homomorphic Encryption

In recent years, as the concern for privacy protection has grown, encrypted database management systems (DBMS) based on fully homomorphic encryption (FHE) have garnered greater research attention. FHE permits the outsourcing of DBMS to cloud servers without divulging plaintext data, effectively guarding against internal malicious divulgation and external illegal theft. Nevertheless, the DBMS based on FHE confronts challenges of high computational latency and low query processing capability in practical deployment. To this end, the literature [10] put forward an efficient ciphertext database system based on the Confused Modulus Component Fully Homomorphic Encryption algorithm (CMP-FHE), designing ciphertext indexes through the sign function and modulo operation to lower computational costs and enhance query efficiency. Meanwhile, rapid ciphertext indexing is accomplished based on N-ary N-form homogeneous equation systems, greatly reducing the number of operations. This solution only requires 54 seconds to conduct keyword queries in a ciphertext dataset of 10,000 rows, verifying the practicability of the fully homomorphic ciphertext database.

The protection approach based on fully homomorphic encryption mentioned in Literature [10] exhibits relatively good performance in privacy protection, particularly outstanding in terms of efficacy. The system designs ciphertext indexes through the sign function and modulo operation, thereby reducing computational costs. This implies that when handling ciphertext data, resource

DOI: 10.54254/2755-2721/135/2025.21090

consumption can be significantly reduced, and the overall efficiency of the system can be enhanced. This approach also embodies its full homomorphic nature. Employing full homomorphic encryption technology permits computations on encrypted data without the necessity of decryption, safeguarding the privacy and security of the data. This is of crucial significance for safeguarding users' sensitive information. Furthermore, with regard to practicality, owing to its superior query performance and security, this scheme possesses a high degree of feasibility in practical applications and is applicable to scenarios demanding high security and rapid access. Nevertheless, the DBMS of FHE does have certain deficiencies. In terms of the complexity of computation, it is comparable to some other approaches, featuring a relatively elevated computational complexity. Fully homomorphic encryption algorithms are typically more intricate than traditional encryption algorithms, potentially resulting in augmented difficulties in implementation and maintenance. This might demand professional expertise and techniques to guarantee the correctness and security of the system. Secondly, with respect to the consumption of computing resources, despite the fact that this approach reduces the computational cost, fully homomorphic encryption per se might still demand more computing resources than other encryption methods, particularly when handling more complex queries. Finally, in terms of cost, owing to the technical intricacy of fully homomorphic encryption, the implementation cost (including development time, hardware requirements, etc.) could be rather high, which might constrain its extensive application in certain scenarios. Overall, the DBMS of FHE possesses remarkable advantages in enhancing data query efficiency and data privacy protection; however, it also confronts formidable challenges such as complexity, development costs, and resource consumption.

Fully Homomorphic Encryption (FHE) enables performing computations on ciphertexts without the need for decryption, thereby supporting the secure outsourcing of computational tasks to untrusted cloud platforms. Subsequently, to address application scenarios involving private information provided by multiple data owners, researchers developed multi-key fully homomorphic encryption (MKFHE) and threshold fully homomorphic encryption (ThFHE). These advancements followed the need for enhanced encryption methods in multi-party data environments. However, both MKFHE and ThFHE come with specific limitations. For example, MKFHE necessitates the participation of all involved parties during decryption and does not allow for decryption by a partial group of members. whereas ThFHE requires pre-fixed participants and does not support dynamic joining or leaving. To address these limitations, the literature [10] put forward a novel concept termed Hierarchical Threshold Multi-Key Fully Homomorphic Encryption (HTM-FHE), which combines the characteristics of MKFHE and ThFHE and integrates the merits of both. Subsequently, [11] offered the first lattice-based HTM-FHE construction, designated as HTM-TFHE. The scheme presented in Literature [11] is capable of evaluating binary gates on ciphertexts encrypted under public keys of different groups and then conducting bootstrapping. The semantic properties and simulation security of HTM-TFHE have been validated based on the LWE assumption. Additionally, HTM-TFHE facilitates granular access management for encrypted data, offering a substantial benefit in practical applications.

The hierarchical threshold multi-key fully homomorphic encryption scheme described in Literature [11] offers several notable advantages. Regarding security, the semantic and simulation security of HTM-FHE has been verified under the LWE assumption. It is capable of effectively safeguarding data privacy and is suitable for conducting secure computations in untrusted environments. Secondly, with respect to flexibility, the flexibility of HTM-FHE has been conspicuously enhanced. HTM-FHE supports fine-grained access control over encrypted data and is capable of processing data in accordance with the permissions of different users, thereby enhancing the security and efficiency of data management. Finally, HTF-FHE possesses highly efficient computing capabilities. This approach permits complex computations on encrypted data and is

capable of effectively outsourcing computing tasks to the cloud, thereby reducing the burden of local computing. However, HTM-FHE also presents certain shortcomings. Like some other algorithms, although a remarkable improvement has been achieved in computational efficiency, there still exist significant challenges in terms of computational complexity. Secondly, with regard to key management, the management and distribution of multiple keys might augment the complexity of the system, particularly in cases where participants fluctuate frequently. The secure management of keys demands extra attention. Finally, in the aspect of application scenarios, this approach has certain constraints. Despite the fact that HTM-FHE holds extensive application potential, in certain specific circumstances, adjustments and optimizations might still be needed in accordance with actual demands. Overall, HTM-FHE, as an emergent encryption technology, demonstrates an auspicious development prospect. It is capable of safeguarding data privacy while facilitating the secure application of information technology. Researchers ought to actively focus on and support the research and development in this domain, contributing to the advancement of science and technology as well as social development.

5. Conclusion

The discursive content of this review mainly pertains to data privacy protection based on homomorphic encryption, and homomorphic encryption is expounded from two aspects: fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE). The article elicits data privacy protection based on homomorphic encryption by virtue of the significance of data privacy. The purpose lies in assisting beginners in this aspect to have a quicker understanding of what homomorphic encryption and data privacy protection are, offer references for methods of data privacy protection, establish a foundation for learning in this regard, and make contributions to future research in the area of data privacy protection utilizing homomorphic encryption.

References

[1] *Qian, P., Wu, M., Liu, Z. (2015). A Method on Homomorphic Encryption Privacy-Preserving for Cloud Computing // East China University of Science and Technology, Henan University of Science and Technology, Northeastern University, Shanghai University of Engineering Science, Engineering and Industry Technology Institute (EITI). Proceedings of the 2nd National Conference on Information Technology and Computer Science (CITCS 2015). School of Computer Science, Nanjing University of Posts and Telecommunications; School of Computer Science and Technology, Jiangsu University of Science and Technology; School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications; 8.*

[2] *Kvetny, N. R., Titarchuk, A. Y., Kotsiubynskyi, Y. V., et al. (2018). Partially homomorphic encryption algorithm based on elliptic curves//Vinnytsia National Technical Univ. (Ukraine); Lublin Univ. of Technology (Poland); Almaty Univ. of Power Engineering and Telecommunications (Kazakhstan).*

[3] *Wang, D., Guo, B., Shen, Y., et al. (2017). A Faster Fully Homomorphic Encryption Scheme in Big Data//IEEE Beijing Section, Xi'an Jiaotong-Liverpool University. Proceedings of 2017 IEEE 2nd International Conference on Big Data Analysis(ICBDA 2017).College of Computer Science Sichuan University; School of Control Engineering Chengdu University of Information Technology; School of Automation Engineering University of Electronic Science and Technology of China; School of Software Chengdu Polytechnic; 2017:5.*

[4] *Ma, H. X., Bai H. X. (2025). Research on Privacy Protection Edge Computing Architecture in the Big Data Environment. Journal of Shanxi University (Natural Science Edition), 1-10. https://doi.org /10.13451/j.sxu.ns.2024146.*

[5] *Zhang, F. C., Wu, J. Y., Chen L. Z., et al. (2024). Research on Trusted Computing Scheme for Cloud Computing Data Privacy Protection// China Computer Federation. Proceedings of the 39th National Computer Security Academic Exchange Conference. China Southern Power Grid Co., Ltd.; Beijing Trustworthy Huatai Information Technology Co., Ltd.; Beijing University of Technology; 4. DOI: 10.26914/c.cnkihy.2024.043767.*

[6] *Du, P. Y., Xiong, J., Zhang, L. P. & Li, Y. Y. (2024). Research on Privacy Protection Methods for Data Mining in Large-scale Massive Data. Electronic Product Reliability and Environmental Testing (01), 1-7.*

DOI: 10.54254/2755-2721/135/2025.21090

[7] *Sathish Kumar, G., Premalatha, K., Uma Maheshwari, G. & Rajesh Kanna, P. (2023). No more privacy Concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user's private and sensitive data. Expert Systems With Applications.*

[8] *Lv, Y. R. (2021). Data privacy protection based on homomorphic encryption. Journal of Physics: Conference Series(1),*

[9] *Tan, T., Zhang, L. M., Yan, H. W., et al. (2024). Asymmetric and Lossless Encryption Algorithm for Vector Maps Based on RSA. Geography and Geo-Information Science, 40(06): 45 - 50.*

[10] *Li, X. D., Zhao, C. Y., Zhou, S. Y., Li, H., & Jin, X. (2024). An Efficient Ciphertext Database System Scheme Based on Fully Homomorphic Encryption. Information Security Research, 10(9), 811 - 817.*

[11] *Wan, X. H. Lin, H. Wang, M. Q. & Shen, W. T. (2025). Hierarchical Threshold Multi-Key Fully Homomorphic Encryption. Journal of Information Security and Applications103919-103919.*