**Frontiers in Computing and Intelligent Systems**
ISSN: 2832-6024 | Vol. 7, No. 1, 2024

# Research on Preventing Medical Information from Leaking based on Homomorphic Encryption

**Kangwei Rao ***

School of Intelligent Technology and Engineering, Chongqing University of Science and Technology, Chongqing, 401331, China
*** Corresponding author Email:** R759033kw@outlook.com

**Abstract:** The security and privacy protection of medical information is one of the important challenges facing today's society. Disclosure of medical information can lead to invasion of patient privacy, reputational damage to medical institutions, and potential legal liability. Therefore, it is very important to take effective measures to prevent the leakage of medical information. Information encryption is a common technical means, which can effectively protect the security and privacy of medical information. The purpose of this paper is to discuss how to prevent medical information leakage through information encryption. First, we describe the sensitivity and importance of medical information, as well as the current security challenges. Then, we discuss in detail the basic principles of information encryption and common encryption algorithms, including symmetric encryption and asymmetric encryption. Next, we explore the specific application scenarios of medical information encryption, such as electronic medical records, medical images and encryption protection during transmission. We also discuss the advantages and challenges of healthcare information encryption and propose some solutions such as key management and access control. Finally, we summarize the importance of information encryption in preventing medical information leakage and emphasize the need for further research and practice to ensure the security and privacy protection of medical information.

**Keywords:** Medical Information Security; Privacy Protection; Information Encryption; Symmetric Encryption; Asymmetric Encryption; Electronic Medical Records; Medical Images; Key Management; Access Control.

## 1. Introduction

With the rapid development of medical information technology, the security and privacy protection of medical information are becoming more and more important. This paper aims to discuss how to strengthen the security of medical information through information encryption and other measures. First, we describe the importance and sensitivity of medical information, as well as the current security challenges. Then, we discuss in detail the basic principles of information encryption and common encryption algorithms, including symmetric encryption and asymmetric encryption. Next, we explore the specific application scenarios of medical information encryption, such as electronic medical records, medical images and encryption protection during transmission. We also discuss the advantages and challenges of healthcare information encryption and propose some solutions such as key management and access control. Finally, we summarize the importance of medical information encryption and emphasize the need for further research and practice to ensure the security and privacy of medical information.

## 2. Literature Review

There have been a number of literature reviews that have helped us review the encryption techniques used to secure medical data, and there have been research papers that have explored the use of homomorphic encryption to enhance the privacy and security of electronic health records, not only introducing the basic principles of homomorphic encryption, but also discussing how it can be applied to the encryption and processing of medical information to protect patient privacy. In addition, other papers related to medical information security have also mentioned that attribute-based encryption (ABE) realizes secure and efficient medical data sharing. The purpose of this paper is to evaluate the performance and security of encryption algorithms in medical image encryption, and to provide guidance for selecting appropriate encryption algorithms. In "Secure Transmission of Medical Data Using Blockchain Technology," the authors explore the use of blockchain technology to enable the secure transportation of medical data, It also discusses how the decentralization and immutability of blockchain can be used to protect the security of medical information. Numerous literature reviews have provided important research results and relevant practical experience on preventing medical information leakage through information encryption, covering different types of encryption technologies and application scenarios, and providing valuable reference and guidance for the research and practice in the field of medical information security. Rivest et al. asked a natural question: What can one do with an encryption scheme that is fully homomorphic: a scheme E with an efficient algorithm EvaluateE that, for any valid public key pk, any circuit C (not just a circuit consisting of multiplication gates), and any ciphertexts $\psi i \leftarrow$EncryptE (pk,$\pi$i), outputs$\psi \leftarrow$EvaluateE (pk, C,$\psi$1,...,$\psi$t) , a valid encryption of C($\pi$1,...,$\pi$t) under pk? Their answer: one can arbitrarily compute on encrypted data – i. e., one can process encrypted data (query it, write into it, do anything to it that can be efficiently expressed as a circuit) without the decryption key. [1]

## 3. The Reality of Preventing Medical Information Leakage through Information Encryption

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires medical institutions and health care providers to take appropriate security measures to

protect patients' medical information. These include the use of encryption to protect the transmission and storage of medical information. The implementation of HIPAA has led to the widespread adoption of encryption technology by healthcare organizations to protect patient privacy and sensitive data.

### 3.1. Medical Information Security Urgently Needs to be Protected by Information Encryption

In 2019, the database of the National University of Singapore Hospital was hacked, resulting in the theft of personal and medical information of about 15,000 patients. This information includes name, ID number, contact information and so on. [2] Another was the 2020 Federal Labor Relations Board data breach, in which the Federal Labor Relations Board's database was hacked, resulting in the theft of personal and medical information of about 25,000 patients. This information includes names, Social Security numbers, medical records, and more. [3] And Antamos Medical Center data breach (2015): Antamos Medical Center in California was hacked, resulting in the theft of personal and medical information of approximately 45,000 patients. This information includes names, social security numbers, dates of birth, contact information and more. [4] Then there's the NHS data breach (2017): The NHS was hit by a ransomware attack that left healthcare facilities across the country unable to access patients' medical records and data. The attack affected tens of thousands of patients, resulting in disruption of medical services and loss of data. [5]

### 3.2. The Challenge of Information Encryption in Preventing Medical Information Leakage

Encryption algorithms require the use of keys for encryption and decryption operations. Effective key management is essential to ensure the security of cryptographic systems. Healthcare organizations need to establish robust key management policies, including processes for generating, storing, distributing, and updating keys. Encryption is only one part of health information security, and access control mechanisms need to be integrated. Healthcare organizations need to ensure that only authorized personnel have access to encrypted medical information and that appropriate authentication and rights management measures are in place. Implementing encryption technology requires appropriate hardware and software support. Healthcare organizations need to invest sufficient resources to select, deploy, and maintain encryption systems to ensure their efficient operation and security. Healthcare organizations need to train their staff to increase their understanding and awareness of the proper use of encryption technology. Employees should understand the importance of encryption and follow relevant security policies and operating procedures. With the continuous development of technology, new encryption algorithms and attack techniques are constantly emerging. Healthcare organizations need to keep abreast of and adopt the latest encryption technologies while remaining vigilant against new security threats

## 4. To the Knowledge of Homomorphic Encryption

Homomorphic encryption is a special encryption technique that allows calculations to be performed on data in the encrypted state without the need to decrypt the data. [6] In medical information encryption, homomorphic encryption can be used to calculate and analyze medical data without decrypting the data, thus protecting the privacy of the data.

### 4.1. About Methodology

The Gentry structure is an important structure of homomorphic encryption, proposed by Craig Gentry in 2009. It is based on the concepts of Ideal Lattice and Ideal on Rings. The algorithm composition of Gentry structure mainly includes the following key parts:

Ideal Lattice: The Gentry structure uses ideal lattices as its underlying mathematical structure. An ideal lattice is a mathematical structure that can be used to build various operations and algorithms in homomorphic encryption schemes.

Ideal on Rings: The Gentry structure uses ideal on rings to implement the basic operation of homomorphic encryption. An ideal on a ring is a mathematical concept that can be used to define addition and multiplication operations in homomorphic encryption schemes.

Key Generation Algorithm: The trap generation algorithm of the Gentry structure is used to generate public and private key pairs. The public key is used to encrypt data, and the private key is used for decryption and computation.

Encryption Algorithm: The Gentry encryption algorithm is used to encrypt plaintext data into ciphertext. The public key is used for encryption.

Decryption Algorithm: The decryption algorithm of the Gentry structure is used to decrypt ciphertext data into plain text. The private key is used for decryption.

Homomorphic Operation Algorithm: A homomorphic operation algorithm based on the Gentry structure is used to calculate ciphertext in encrypted state. These algorithms allow homomorphic addition and multiplication operations on encrypted data. [7]

### 4.2. General Principles of Homomorphic Encryption

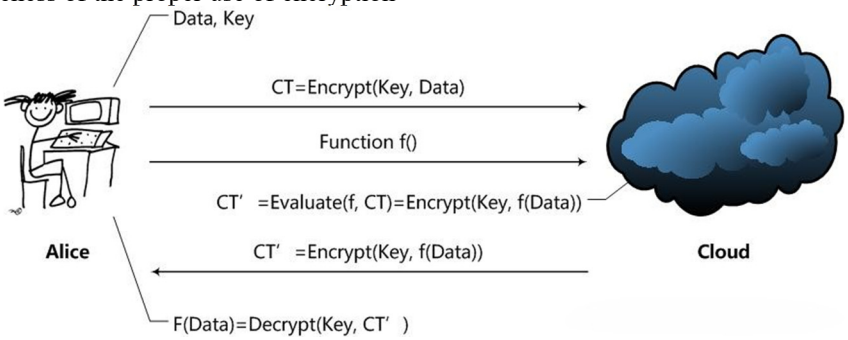


**Figure 1.** The whole process is roughly

Alice uses the Cloud to process data with Homomorphic Encryption (hereinafter referred to as HE) and the whole process is roughly like Figure 1 to show:

Alice encrypts the data and sends the encrypted data to the Cloud.

The method by which Alice submits data to the Cloud is represented here by the function f.

The Cloud processes the data in function f and sends the result to Alice.

Alice decrypts the data and gets the result.

From this, it is possible to intuitively get a function that the HE schemes should have:

KeyGen function: key generation function. This function should be run by Alice to generate the Key used to encrypt Data. Of course, there should also be some public constants PP (Public Parameter)

Encrypt function: Encrypt function. This function, which should also be run by Alice, encrypts the user Data with Key, resulting in Ciphertext CT (Ciphertext). [8]

Evaluate function: Evaluate function. This function is run by the Cloud and operates on the ciphertext under the Data processing method f given by the user, making the result equivalent to the user encrypting f(Data) with the Key.

Decrypt function: decrypt function. This function is run by Alice to get the result f(Data) of Cloud processing. [9]

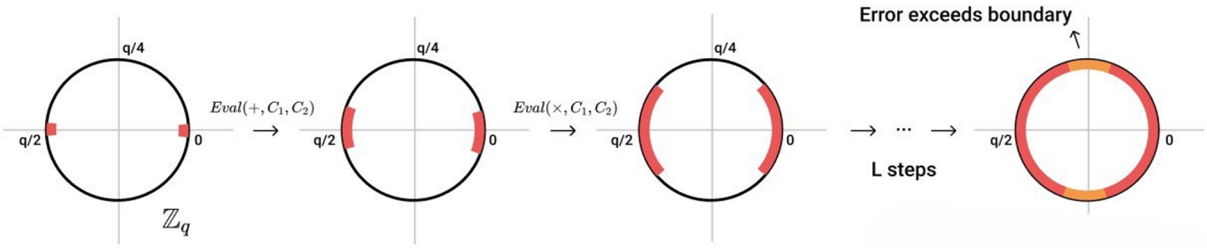


**Figure 2.** The HE schemes

# 5. Medical Information Protection Scheme based on Homomorphic Encryption

In the medical information protection scheme, it is necessary to preprocess the original medical data first. This includes steps such as data cleansing, de-identification, and data format conversion to ensure data consistency and availability. The trap generation algorithm of homomorphic encryption algorithm is used to generate public and private key pairs. The public key is used to encrypt data, and the private key is used for decryption and computation. Trap generation algorithm needs to ensure the security and randomness of the generated key pair. The preprocessed medical data was encrypted into ciphertext using an encryption algorithm. The public key is used in the encryption process to ensure that only the person holding the corresponding private key can decrypt the data. Encryption algorithms need to ensure data confidentiality and integrity. Encrypted medical data can be securely stored locally or in a storage system in the cloud. In the process of data transmission, it is necessary to adopt a secure communication protocol and encryption technology to prevent data leakage and tampering. The algorithm of homomorphic operation is used to calculate and analyze the encrypted medical data. Homomorphic operation algorithms allow homomorphic addition and multiplication operations on ciphertext in the encrypted state without decrypting the data. This makes it possible to perform complex calculations and analyses while protecting data privacy. A decryption algorithm is used to decrypt the calculated result into plain text. The private key is used for decryption. The decrypted results can be used for further data interpretation and analysis to support medical decisions and research.

## 5.1. The Feasibility and Effect of Homomorphic Encryption Scheme in Actual Medical Environment are Analyzed

Algorithm complexity: The computational complexity of homomorphic encryption algorithms is higher and may require more computing resources and time. In a real-world medical environment, the computing power and performance of the system need to be evaluated to ensure that it can meet real-time and responsive requirements.

Data scale: Healthcare data is typically large and highly dimensional. Homomorphic encryption schemes need to process a large amount of data, so it is necessary to evaluate the feasibility and efficiency of the scheme on large-scale data sets.

System integration: Homomorphic encryption schemes need to be integrated with existing healthcare information systems, including data storage, data transmission, and data processing. It is necessary to evaluate the compatibility and integration difficulty of the solution with the existing system.

## 5.2. Evaluate and Compare Medical Information Protection Schemes based on Homomorphic Encryption

Homomorphic encryption is an encryption scheme that allows calculations to be performed on encrypted data without decrypting it. This technology has important implications for the protection of medical information, as it allows sensitive data to be shared and processed securely while maintaining privacy. When evaluating and comparing medical information protection schemes based on homomorphic encryption, the following factors need to be considered: Security: The level of security provided by the encryption scheme is the most important. The scheme should be resistant to known encryption attacks and should provide strong protection against malicious adversaries. Computational efficiency: Homomorphic encryption schemes usually have significant computational overhead due to the complex mathematical operations involved. It is important to evaluate

the efficiency of the scheme in terms of computational resources and processing time required. Data privacy: The program shall ensure the privacy and confidentiality of medical information shared or processed. This includes preventing unauthorized access and ensuring that encrypted data cannot be linked back to the original patient. Usability and practicality: The program should be easy to deploy and use in existing healthcare systems. It should integrate well with existing infrastructure and workflows, and not create significant barriers or burdens for users. Scalability: The solution's ability to efficiently and effectively process large amounts of medical data is critical for real-world medical applications. Some of the popular Homomorphic Encryption schemes that have been explored for healthcare information protection include: Fully Homomorphic Encryption (FHE): FHE provides the highest level of security by performing calculations on encrypted data without any restrictions. However, FHE implementations are currently resource intensive and computationally expensive. Partial homomorphic Encryption (PHE): PHE schemes, such as the Paillier cryptosystem, allow specific types of calculations to be performed on encrypted data, such as addition and multiplication. These schemes provide a good balance between safety and efficiency. Somewhat homomorphic encryption (SHE): SHE schemes, such as BGV schemes, allow a limited number of calculations to be performed on encrypted data. While they may not support arbitrary calculations, they provide better computational efficiency compared to FHE. Each scheme has its own advantages and disadvantages. The choice of protocol depends on the specific requirements and limitations of the medical application. When comparing different homomorphic encryption schemes for medical information protection, it is important to carefully evaluate the trade-offs between security, computational efficiency, and availability.

# 6. Challenges and Limitations of Medical Information Protection based on Homomorphic Encryption

Homomorphic encryption is computationally intensive and can significantly impact system performance. The encryption and decryption operations, as well as the homomorphic computations, can be time-consuming and resource-intensive. This can pose challenges in real-time applications or scenarios with large-scale data processing requirements. Implementing and managing a homomorphic encryption system requires specialized knowledge and expertise. It involves complex cryptographic algorithms and protocols, which may be challenging for healthcare organizations to understand and implement correctly. Additionally, integrating homomorphic encryption into existing healthcare systems and workflows can be complex and time-consuming. Homomorphic encryption supports a limited set of mathematical operations, such as addition and multiplication. However, more complex operations, such as division or comparison, are not directly supported. This limitation can restrict the types of computations that can be performed on encrypted medical data, potentially impacting the usefulness of the system. Homomorphic encryption relies on secure key management practices to ensure the confidentiality and integrity of the encrypted data. Key generation, distribution, and storage are critical aspects that need to be carefully managed. Any compromise in key management can lead to the exposure of sensitive medical information. Homomorphic encryption may face scalability challenges when dealing with large volumes of medical data. As the size of the data increases, the computational and storage requirements also increase, potentially impacting the system's scalability and performance. Homomorphic encryption may face interoperability challenges when integrating with existing healthcare systems and standards. Ensuring compatibility and seamless data exchange between different systems can be complex, especially when dealing with encrypted data. Healthcare organizations must comply with various data privacy and security regulations, such as HIPAA in the United States. Implementing homomorphic encryption while ensuring compliance with these regulations can be challenging, as the regulations may not explicitly address the use of such encryption techniques

# 7. Look Forward to the Future Development Direction

By means of algorithm optimization, parallel computing, hardware acceleration, data compression and optimization, precomputation and cache technology, the algorithm efficiency of homomorphic encryption can be improved, the computational complexity can be reduced, and the algorithm is more practical and efficient.

## 7.1. Algorithm Direction Improvement Strategy

The design and implementation of homomorphic encryption algorithms can continue to be improved to improve their efficiency and performance. This includes optimizing the mathematics of the encryption algorithm, reducing the computation and storage overhead, and improving key generation and management. In addition, combining homomorphic encryption algorithm with special hardware can further improve the computing efficiency. For example, using hardware acceleration technologies such as FPgas (field Programmable gate arrays) or ASics (application-specific integrated circuits), high-performance homomorphic encryption computing can be achieved to speed up data processing. At the same time, the technique of parallel computing can be used to decompose the computation task of homomorphic encryption into multiple subtasks and process them simultaneously. By making full use of multi-core processors, distributed computing and GPU acceleration, the computational efficiency of homomorphic encryption can be improved.

## 7.2. An Improved Strategy in the Direction of Computational Complexity

By using the compression algorithm, the storage space of data can be reduced and storage resources can be saved. Common compression algorithms include lossless compression algorithms (such as GZIP, ZIP) and lossy compression algorithms (such as JPEG, MP3). Choosing the right compression algorithm can be a trade-off based on data type and compression ratio requirements. In other ways, the representation size of the data can be reduced by using more compact data encoding. For example, using variable-length encodings (such as Huffman encoding) can assign different lengths of encodings depending on the frequency of the data, thereby reducing the size of the representation of the data.

# 8. Conclusion

Homomorphic encryption is an effective technique to protect the privacy of medical information. By using homomorphic encryption, medical data can be calculated and analyzed in its encrypted state without the need to decrypt the data. Helps to protect patient privacy and comply with data protection regulations. At the same time, homomorphic encryption has potential in medical information sharing and collaboration. By using homomorphic encryption, healthcare organizations can securely share data and facilitate medical research and collaboration. This helps to increase innovation and development in the medical field. Homomorphic encryption of course has its own challenges, although homomorphic encryption provides strong data privacy protection, but its computation and processing overhead is high, may affect the performance and response time of the system. In addition, scalability in dealing with large data sets and multi-user environments is also a challenge.

# References


[1] Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 169-178.

[2] Boneh, D., & Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University.

[3] Gentry, C. (2010). Computing Arbitrary Function of Encrypted Data. Communications of the ACM, 53(3), 97-105.

[4] Stehle, D., & Steinfeld, R. (2010). Faster Fully Homomorphic Encryption. Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 377-394.

[5] Coron, J., Naccache, D., & Tibouchi, M. (2012). Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. In P. David & J. Thomas (Eds.), Advances in Cryptology-EUROCRYPT 2012, 446-464. Springer.

[6] Xia, C. (2013). Research of Homomorphic Encryption Technology and Application. Anhui University, Hefei.

[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] Coron, J. S., Mandal, A., Naccache, D., & Tibouchi, M. (2011). Fully homomorphic encryption over the integers with shorter public keys. In Annual Cryptology Conf., 487–504.

[9] Chung, K. M., Kalai, Y., & Vadhan, S. (2010). Improved delegation of computation using fully homomorphic encryption. In Advances in Cryptology—CRYPTO 2010, 483-501. Springer.