DOI: https://doi.org/10.36910/6775-2524-0560-2023-53-09
UDC 004.9:614.2

Radchenko Kostiantyn, assistant
https://orcid.org/0000-0002-1282-6307
Li Bai, graduate student
https://orcid.org/0009-0000-3408-348X
Potapova Ekaterina, Ph.D., Associate Professor
https://orcid.org/0000-0002-3347-6350
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», c. Kyiv, Ukraine

RESEARCH OF CRYPTOGRAPHIC INFORMATION PROTECTION TECHNOLOGY IN HEALTH AND MEDICAL CARE FIELD OF CHINA

Radchenko K., Li Bai, Potapova E. Research of Cryptographic Information Protection Technology in Health and Medical Care Field of China. Cryptography technology based on domestic algorithms for the use of informatization in the health and medical care field of China is classified and researched in the paper. In the trend of medical services gradually transitioning from "closed" to "open", the medical information security environment is not optimistic. It is emphasized that with the correct settings and selection of the necessary cryptographic stability of the encryption algorithm, the technology is safe and independent, ensures the safety of medical data and facilitates the circulation of medical services. Cryptography technology service realizes the identity authenticity of medical data access subjects, the confidentiality and integrity protection of medical health information in the process of sharing and storage, the protection of sensitive information in the process of access, query and use, and the secure data cochain in the whole process, and ensures that the cryptographic application is secure, independent and controllable, truly achieves the security of medical health data and promotes the open sharing of health services.

Keywords: cryptography technology, trusted identity, transmission encryption, privacy protection, domestic algorithm.

Радченко К.О., Лі Бай, Потапова К. Р. Дослідження технології криптографічного захисту інформації в галузі охорони здоров'я та медичної допомоги Китаю. У роботі класифіковано та досліджено технологію криптографії на основі вітчизняних алгоритмів для використання інформатизації у сфері охорони здоров'я та медичного обслуговування Китаю. У тенденції поступового переходу медичних послуг від «закритості» до «відкритості» середовище безпеки медичної інформації поки ще не є оптимальним. Наголошується, що при правильному налаштуванні та підборі необхідної криптографічної стійкості алгоритму шифрування технологія є безпечною та незалежною, забезпечує безпеку медичних даних та полегшує обіг медичних послуг. Служба технології криптографії реалізує автентичність ідентифікації суб'єктів доступу до медичних даних, захист конфіденційності та цілісності медичної інформації про здоров'я в процесі обміну та зберігання, захист конфіденційної інформації в процесі доступу, запиту та використання, а також безпечний коланцюг даних у всьому процесі та гарантує, що криптографічна програма є безпечною, незалежною та керованою, дійсно забезпечує безпеку медичних даних про здоров'я та сприяє відкритому обміну послугами охорони здоров'я.

Ключові слова: технологія криптографії, довірена особа, шифрування передачі, захист конфіденційності, вітчизняний алгоритм.

Statement of a scientific problem. The vigorous development of "internet plus healthcare" [1], the continuous improvement of smart medical applications, the growing number of big data applications in the health field, and the continuous emergence of new businesses and application methods have brought a variety of data security challenges to health big data at all stages of the whole life process of health diagnosis and treatment, data use, including identity counterfeiting, privacy disclosure, secret theft, data tampering, ultra vires access, etc. The country attaches great importance to data security and has successively promulgated the Personal Information Protection Law and the Data Security Law in 2021. Among them, the Data Security Law clearly states that carrying out data activities must fulfill data security protection obligations and assume social responsibility. In the field of medical and health, data security is related to the safety of patient life, personal privacy, and public interests. In order to better protect medical data security and standardize medical data sharing, the National Information Security Standardization Technical Committee officially released the "Information Security Technology Health and Medical Data Security Guidelines" at the end of 2020, which proposed confidentiality for health and medical data controllers The security goals of integrity and availability. In 2022, the National Health Commission issued the "Management Measures for Network Security of Medical and Health Institutions", which clearly stated that "all medical and health institutions should strengthen data collection, storage, transmission, processing, use, exchange, and destruction throughout their lifecycle security management work, adopt prevention and control measures such as data desensitization, data encryption, and link encryption to prevent data leakage during the data collection process" [1,4]. Passwords are the foundation and core of network information security, It is an important component of the national network information construction. This article will discuss the application of cryptographic technology based on domestic algorithms in the field of healthcare to ensure the security of medical data.

Research analysis. The hospital information system covers various functional departments, and its construction has the characteristics of central deployment, distributed application, and hierarchical management. It is aimed at all doctors, nurses, physicians, operation and maintenance personnel and other different types of staff, with different identity roles and management permissions. To ensure effective access control for users, it is necessary to ensure the authenticity and trustworthiness of personnel identities, Ensure the orderly conduct of relevant business and work. Therefore, based on the unique information environment of the hospital, it is necessary to establish a set of identity authentication management system for the entire hospital. Based on password technologies such as dynamic passwords, message authentication codes, and digital certificates, trusted identity authentication credentials for the user network world should be established to achieve secure, reliable, and trustworthy identity login authentication, ensuring the authenticity and trustworthiness of the identities of users with different roles.

The confidentiality and integrity requirements of medical data during transmission ensure the secure transmission of medical and health data between the user end and the server end in business processes such as internet healthcare and remote work outside the hospital; Ensure the transmission security of medical and health data between hospital systems and regional platform systems in business processes such as direct reporting of infectious disease information and sharing of electronic medical records. During the transmission process, verify the integrity and confidentiality of the data to prevent theft or tampering of medical data [6].

Medical data involves a large amount of privacy information such as patients and medical records. Privacy protection is applied to privacy data, important information, and sensitive information, with dynamic desensitization. Differential data display can be performed based on user permissions to prevent the leakage of personal or sensitive information such as user identity information, phone numbers, and medical records.

As the various functions of hospital information systems gradually replace traditional medical diagnosis and treatment methods, both doctors and patients have shifted from recognition of a paper diagnosis book to recognition of the description content of a data message. Whether the responsibility attribution of data messages is clear directly related to whether the information technology process can completely replace traditional paper processes. Therefore, on the premise of the authenticity and credibility of the identities of both doctors and patients, it is necessary to combine reliable electronic signature technology to establish a responsibility recognition mechanism in the hospital information system, ensure clear responsibility attribution of medical data, achieve a truly paperless diagnosis and treatment process, and fully leverage the high efficiency advantages of informatization.

The goal of the work. The main objective of the research is to present a method by which cryptographic technology in the field of health care to ensure the security of medical data.

Implementation of the method could involves the provision for medical and health institutions strengthen data collection, storage, transmission, processing, use, exchange, and destruction throughout their lifecycle security management work, adopt prevention and control measures such as data desensitization, data encryption, and link encryption to prevent data leakage during the data collection process.

Presentation of the main material and substantiation of the obtained research results. Basic cryptographic technology mainly includes domestic commercial cryptographic algorithms such as SM2, SM3, and SM4, as well as digital signatures, digital envelopes, encryption and decryption, integrity calculations, SSL protocols, etc. based on these algorithms.

Symmetric cryptographic algorithm, where the encryption key and decryption key are "symmetric", and the encryption process and decryption process use the same key. There are two main forms of symmetric ciphers for different data types and application environments: for example, block ciphers using the SM4 cryptographic algorithm, and stream ciphers using the ZUC cryptographic algorithm [2].

The public key cryptographic algorithm, also known as asymmetric cryptographic algorithm, differs from symmetric cryptographic algorithms in that encryption and decryption use different keys, solving the problem of key management in symmetric cryptographic algorithms. This includes fields such as encryption and decryption algorithms based on public keys, digital signature verification technology, and key negotiation. China has issued the standard commercial public key cryptographic algorithm, SM2 cryptographic algorithm. The public key encryption algorithm uses different keys for encryption and decryption, becoming the public key and private key. The public key is made public, while the private key is kept confidential. Digital signature algorithms, also known as electronic signature algorithms, can achieve functions similar to handwritten signatures, but with the help of mathematical methods, they are more secure and functional than handwritten signatures. The public key encryption algorithm, combined with a key negotiation algorithm of a specific cryptographic protocol, is used to negotiate keys that are commonly used by both communication parties.

The hash algorithm is a function that can compress any length of information into a fixed length of short information according to a certain algorithm. It has properties such as tamper resistance and irreversibility, and the output of the function becomes a summary value, also known as a summary. The hash algorithm has many functions, and it can be used for digital signatures: first compress the message, then sign the digest value; It can detect the integrity of messages and determine whether the message has been tampered with based on the digest value; It can be used for password storage, taking advantage of the unidirectional nature, even if the digest value is exposed, the password will not be exposed. The SM3 algorithm is a cryptographic hash algorithm in China's commercial cryptographic standards (Fig.1).

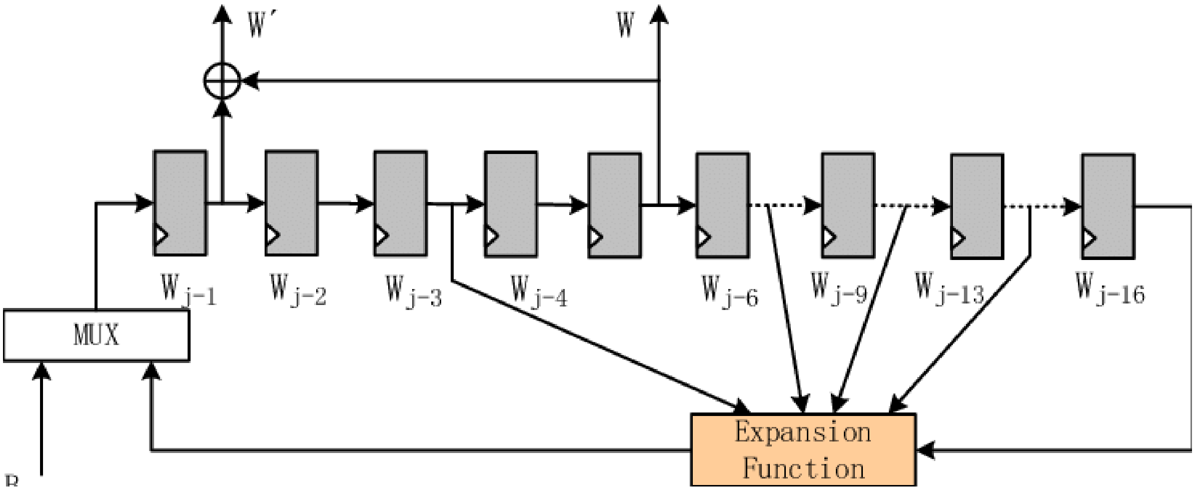

Fig.1. The SM3 message expansion structure [7]

Applying cryptographic algorithms to achieve specific security functions is very complex, and different usage environments require different cryptographic protocols. Different security functions are also implemented by different cryptographic protocols. Therefore, there are various cryptographic protocols in cryptography, such as key agreement protocols, identity authentication protocols, etc. The security of password protocols is crucial for password applications. Password protocols are not secure, and even if password algorithms are secure, password applications are still insecure.

Building a certificate storage blockchain based on judicial applications, using medical institutions, CA institutions, relevant notary offices, judicial appraisal centers, internet courts, arbitration and other institutions as blockchain nodes. Utilizing the characteristics of multi-party consensus, distributed storage, traceability, and tamper resistance of blockchain, it is deeply integrated with domestic cryptographic technology, combined with digital signature technology, trusted timestamp, identity authentication technology, etc., to ensure the authenticity and integrity of electronic data.

The National Cryptography Algorithm is a series of cryptographic standards designated by the Office of the State Administration of Commercial Cryptography, which have been recognized by the National Cryptography Administration as domestically produced cryptographic algorithms to ensure the security of information transmission in fields such as finance and healthcare.

National Cryptography refers to the domestically produced cryptographic algorithm recognized by the National Cryptography Bureau. There are mainly SM1, SM2, SM3, and SM4. The key length and packet length are both 128 bits [3].

SM1 is symmetric encryption. Its encryption strength is equivalent to AES. This algorithm is not publicly available, and when calling it, it needs to be called through the interface of the encryption chip.

SM2 is asymmetric encryption based on ECC. The algorithm has been made public. Due to its ECC based algorithm, its signature speed and key generation speed are both faster than RSA. ECC 256 bit (SM2 uses a type of ECC 256 bit) has higher security strength than RSA 2048 bit, but faster computation speed than RSA.

SM3 message summary. MD5 can be used as a comparative understanding. The algorithm has been made public. The verification result is 256 bits.

The packet data algorithm for the SM4 wireless local area network standard. Symmetric encryption, with a key length and packet length of 128 bits.

SM2 algorithm: The SM2 elliptic curve public key cryptography algorithm is a public key cryptography algorithm independently designed in China, including the SM2-1 elliptic curve digital signature algorithm, the SM2-2 elliptic curve key exchange protocol, and the SM2-3 elliptic curve public key encryption algorithm, which are used to achieve functions such as digital signature key negotiation and data encryption. The difference between the SM2 algorithm and the RSA algorithm is that the SM2 algorithm is based on the discrete logarithmic problem of point groups on elliptic curves. Compared to the RSA algorithm, the strength of the 256 bit SM2 password is already higher than that of the 2048 bit RSA password.

SM3 algorithm: SM3 hash algorithm is a password hash algorithm independently designed in China, suitable for the generation and verification of digital signature and verification message authentication codes in commercial password applications, as well as the generation of random numbers. It can meet the security requirements of various password applications. To ensure the security of the hash algorithm, the length of the hash value generated should not be too short. For example, MD5 outputs a 128 bit hash value, and the output length is too short, which affects its security. The output length of SHA-1 algorithm is 160 bits, while the output length of SM3 algorithm is 256 bits. Therefore, the security of SM3 algorithm is higher than that of MD5 algorithm and SHA-1 algorithm (Fig.2).

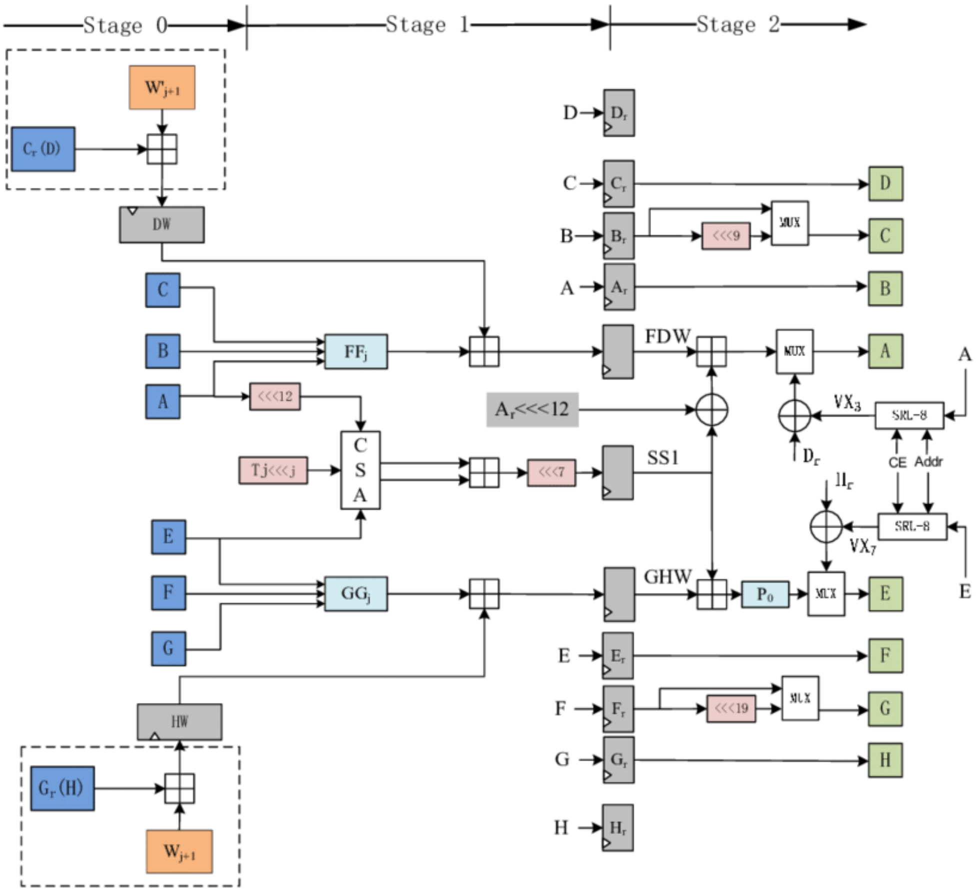

Fig.2. The high-throughput round architecture of SM3 [8]

SM4 algorithm: The SM4 block cipher algorithm is a group symmetric cipher algorithm independently designed in China, used to encrypt/decrypt data to ensure the confidentiality of data and information. The basic condition for ensuring the security of a symmetric cryptographic algorithm is that it has sufficient key length. The SM4 algorithm has the same key length as the AES algorithm, with a group length of 128 bits, thus outperforming the 3DES algorithm in terms of security.

Based on password technologies such as dynamic passwords, message authentication codes, and digital signatures, the authenticity of digital identities of individuals, devices, institutions, and other entities is ensured through diversified identity credentials. Doctors, nurses, and pharmacists have professional qualifications, and their online identities correspond to their professional identities, achieving consistency between their online identities and industry identities; For personnel entering and exiting important areas such as computer rooms, as well as operation and maintenance personnel, ensure their identity is trustworthy and effectively intercept unauthorized personnel from entering.

For all medical staff in hospitals, a unified and compliant digital certificate service system based on national secret digital certificates can be established to solve the problem of identity credentials and credential authentication for actors in the hospital information system. If it is based on PC access, the national secret digital certificate in the USBKey can be verified by using the USBKey digital certificate based on the national secret algorithm and calling identity authentication based on the national secret browser Verification, achieving identity authentication in application and data aspects; If it is based on mobile access, integrate a mobile intelligent terminal security password module that meets the GM/T 0028-2014 "Password Module Security Technical Requirements" [5] on the mobile terminal, call the collaborative signature function, issue a mobile digital certificate based on the national security algorithm, and achieve identity authentication in terms of application and data through collaborative signature authentication between the terminal and the server.

Medical information systems include various roles such as medical and nursing technology users, patients, office workers, operation and maintenance personnel, researchers, etc., which access business applications through terminals such as PC and APP through local area networks and the internet. Network communication transmission often exists in scenarios such as online registration, internet healthcare, and remote office work outside the hospital.

At the network layer, secure data transmission channels are established using National Security SSL technology to achieve identity authentication at the network layer, while protecting the integrity and confidentiality of data during communication, preventing medical data from being tampered with, leaked, or stolen. Usually, gateways based on national security algorithms and compliant with commercial password product authentication requirements are deployed in the DMZ area of hospitals, without the need to integrate with application systems to build a national security transmission channel.

At the application layer, password devices based on national security algorithms and meeting the certification requirements of commercial password products are usually deployed in the service area. Important data such as personal privacy information and patient reports are protected for confidentiality through the SM4 national security algorithm, and digital signature integrity is protected through the SM2 national security algorithm, ultimately achieving the confidentiality and integrity protection of important data transmission at the application layer.

Conclusions. Therefore, in the field of medical and health, data security is related to the safety of patient life, personal privacy, and public interests. In order to better protect medical data security and standardize medical data sharing, it was suggested to pay special attention confidentiality for health and medical data controllers. The security goals of integrity and availability. Passwords are the foundation and core of network information security, and one are an important component of the national network information construction.

References

1.Yang F., Shu H., Zhang X. Understanding “Internet Plus Healthcare” in China: Policy Text Analysis / J Med Internet Res 2021;23(7):e23779 / Mode of access: https://www.jmir.org/2021/7/e23779 – doi: 10.2196/23779

2.Basic crawler reverse engineering, understanding SM1-SM9, ZUC national secret algorithm [Electronic resource] / Mode of access: https://segmentfault.com/a/1190000040933093/en – Access date: appeal 05.11.2023.

3.SM3 cryptographic hash algorithm [Electronic resource] / Mode of access: https://gmbz.org.cn/main/viewfile/20180108023812835219.html – Access date: appeal 05.11.2023.

4.Dong, K.N. & Wang, N. (2017). The dawn of intelligent medical era: an overviewof theapplication of artificial intelligence + health care. Big data era, 000 (004), p.26-37.

5.Titir, S. (2010) Mobile Health Care System for Patient Monitoring. Information and Communication Technologies, (101):695-700.

6.Zheng, W. Z. & Liu, Q. L. (2016). Changes and governance of China's Internet in 21years. Xinmin weekly, 000 (019), 16-19.

7.Ma, Y., Xia, L., Lin, J., Jing, J., Liu, Z., Yu, X. (2012). Hardware Performance Optimization and Evaluation of SM3 Hash Algorithm on FPGA. In: Chim, T.W., Yuen, T.H. (eds) Information and Communications Security. ICICS 2012. Lecture Notes in Computer Science, vol 7618. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34129-8_10

8.Suo, S., Xi, W., Cai, T., Jian, G., Yao, H., Li, J. Encryption Technology in Information System Security / Advances in Computer Science Research, volume 87 // 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019). https://doi.org/10.2991/icmeit-19.2019.80