ISSN 2959-6157

Encryption Techniques in Near Field Communication (NFC): Challenges, Applications, and Future Directions

Zihao Chen

Shenzhen senior high school, Guangdong, China

Abstract:

With the growth of the need of information transmission and communication, Near Field Communication(NFC) technique is widely used in different areas for its convenience and simplicity,especially those areas that require both high efficiency and low cost of information transmission. However, the security of NFC itself is not ensured due to the risk of information leakage caused by technical features of short distance information transmission. Information encryption techniques are able to help NFC to be more reliable and safer from the danger of data leakage. There are several kinds of encryption techniques for NFC encryption.Due to the impact of multiple different techniques on the universality of NFC, placing different encryption techniques under the same standard can be an effective research method to improve collaboration efficiency of different encryption techniques. This paper mainly introduces common encryption techniques for NFC,including their features and applicable scenarios, and attempt to conduct technical analysis on existing encryption technologies for finding possible improving directions.

Keywords: NFC encryption, NFC authentication security, NFC security evaluation

1. Introduction

Against the backdrop of rapidly increasing demands for convenience and speed in information transmission in recent years, NFC technique is welcomed by various industries around the society. NFC has strong competitiveness in the information society because it is easy to deploy, has low implementation cost, high reusability, and has outstanding adaptability and flexibility in different usage scenarios. However, the widespread use of NFC also exposes significant security vulnerabilities. The very convenience of NFC causes lacks of regulation and protection. This creates possibility of data leakage,which directly affects the reliability of NFC devices. This has a particularly significant impact on aspects of mobile payments, identity authentication, and the Internet of Things(IoT). Because these fields rely on end-to-end authentication to function and are directly related to personal interests, they have high requirements of information security. The development of modern practical technology aims to improve the connections of different things and fields, which is based on the technique of information transmission, including NFC. This offers challenge to improving information security.

Although the short-range nature of NFC is considered a natural security measure, it also hinders the effectiveness of external protective measures. This makes it difficult for NFC to retaliate through external means when subjected to effective attacks. For instance, man-in-the-middle (MITM) attacks can intercept or tamper with the data exchanged between devices. Furthermore, the passive nature of some NFC devices may result in unauthorized activation, which poses additional security risks. However, at short distances, these attacks and interference are difficult to be externally targeted and resolved. Therefore, a more effective approach is to conduct defense within NFC devices. To achieve a wider and more secure application of NFC technology in daily life of the improving society, it is necessary to adopt appropriate,effective and robust information encryption technique in the process of NFC transmission of information. Information encryption is the most common method for keeping the information from unauthorized reading and access violation. In order to develop the application of information encryption technology, this paper targets to analyze the advantages and disadvantages of frequently-used encryption technique, and their possible improving direction.

The literature review method is adopted in this paper. By integrating papers of different encryption techniques, analyzing points and experimenting, this paper purposes to obtain a comprehensive and instructive view of different encryption techniques, and strengthen the correlation between different encryption algorithms. This paper begins with Background Introduction for introducing the research

background and propose. Then the Literature Review part integrates the researching literature. Encryption Methodology and Technical Model Basis is the the next part that explicates technical principles of different encryption methods. The part of Applications of Encryption in NFC Technology will be expansion and supplementation of the previous part and explain the real use of information encryption technique in the use of NFC in civilian fields. Immediately after that, the Experiment and Model Evaluation part will contain a designed experiment for testing models and give reliable and reproducible data. Finally the Conclusion part will present main discoveries of the paper.

2. Literature Review

The categories of information encryption technology has a considerable number and the quantity is still increasing, including Symmetric Encryption,Asymmetric Encryption,Hash Functions,Message Authentication Codes(-MAC) and more. Each category contains several methods that use similar technique but different standards. In recent years there are also some new categories created, like the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge(zk-SNARK) and Post-quantum Cryptography(PQC). Among these encryption technologies, the mostly often used techniques are the Symmetric Encryption, Asymmetric Encryption and Hash Functions because they were used earlier and have been reliable and convenient after improvement during several decades. These categories are representative to the general cryptography. Therefore the discussion on these categories are also of sufficient reference value.

The three most commonly used information encryption methods are implemented

using different technologies. The accomplishment of Symmetric Encryption relies on a uniquely generated key. When the Symmetric Encryption technique is used to encrypt data to be processed, the data will be split into blocks with the same length. Then according to different standards of certain methods and the information saved in the key, the blocks will be subjected to various operations such as substitution, row shift, column shuffling, and round key addition. After all operations are completed, the proceed data blocks will be sent. The receiver has to have the same key as the sender, performing the inverse of the encryption operation step by step to decrypt the data blocks to get original data. This is called block cipher because the data is split into blocks and encrypted. Another way to accomplish a Symmetric Encryption process is to use the stream cipher, which processes data as a whole stream without splitting but is used less due to weaker protection effect. The most obvious advantage of Symmetric Encryption is its simplicity because its encryption and decryption only relies on a certain key and a series of specific operations. Therefore Symmetric Encryption is able to encryption big data in a short time and available to different processing devices, including those which only contain limited resources. However, simplicity also decreases the security of Symmetric Encryption technique. Because the only guarantee of the safety of Symmetric Encryption is its key, the encrypted data will be almost public when the key is leaked. In addition, Symmetric Encryption lacks the ability to deal with data from different sources well because the keys for different data are unique and the recording and distribution of the keys is complex and error-prone.

In contrast, the Asymmetric Encryption technique performs better in safety because it contains a pair of keys, both a public key and a private key. For a process of Asymmetric Encryption, one of the keys will be used as the encryption key and another will be the decryption key. Each of them can can be encryption key or decryption key but cannot play both roles at the same time. In the case of a public key as the encryption key, data is processed by the public key in a similar way to symmetric encryption and sent. However, the decryption does not rely on the inverse operation of the public key but the private key that is paired with the public key. It also brings Asymmetric Encryption ability to identify the receiver because the private key is unique. As a result, the leakage of public key or encrypted data does not necessarily lead to information leakage because the private key is required for decryption[1]. This is also available to the case of the private key as the encryption key. In this case, the decryption key is public, and the sender of encrypted data can be identified by the sender. In practical use, due to its better security and the ability of identifying, Asymmetric Encryption is more often used for identity verification and compliance checks. For example, Asymmetric Encryption is used in Hypertext Transfer Protocol(HTTP), one of the mostly used Internet protocols, to identify request and website certificate and build normal connection between the request sender and the website. However, the problem of the complexity of distributing keys is even more serious in Asymmetric Encryption than Symmetric Encryption because the number of keys is doubled.

In addition, the Hash Function Encryption is a more convenient and basic encryption method. In actual, this method is not an encryption process constructed from multiple steps, but rather a single step where data is transformed by a hash function or its content is altered through a hash function. The data after processed by a hash function is unable to be restored, so it is usually used as a identifica-

tion of original data instead of the data itself. The difference of different Hash Function Encryption is decided by the way they use the hash function, and many of them is not seen as a independent encryption method but a step of more complex methods like the Symmetric Encryption and the Asymmetric Encryption above. When it is used as a independent encryption method, the application area is more likely to be a field that requires high speed for large amounts of data and sufficient evidence to prove the similarity between some two. However, the Hash Function Encryption is less safe than other encryption methods because it does not requires a key, and the processed string is possible to be brute force attacked because it only checks whether the strings are the same. This brings it holes for attacking. Therefore the Hash Function Encryption is not often used for a project that needs better security. Also, because data after processed by hash function is irretrievable, this method is used for identifying information instead of transferring information.

NFC technology is widely used in mobile payment, access control systems, smart tags and other fields due to its convenience, but it also faces severe security challenges. Data theft is one of the main threats facing NFC technology. Attackers can obtain sensitive information by illegally reading the communication data between devices. Copy attacks can deceive the system to complete illegal operations by copying NFC tags or simulating NFC devices. In addition, man-in-the-middle attacks are also a major hidden danger. Attackers can intercept and tamper with the transmitted data without the knowledge of the communicating parties[2].

In response to these challenges, with the combination encryption methods above, academia and industry have conducted in-depth research on encryption methods in NFC technology. In particular, achieving efficient encryption on NFC devices with limited resources has become a hot topic of research. Relevant literature explores how to optimize encryption algorithms to reduce resource consumption and improve encryption efficiency while ensuring security.At present, there are many encryption methods for NFC technology. Among them, rolling code encryption effectively prevents copy attacks due to its dynamic characteristics and is widely used in access control systems and ticketing systems. CPU card encryption uses the processor built into the card to execute complex encryption algorithms, providing higher security, but the cost is also relatively high. In addition, there are some customized encryption solutions, such as encryption solutions based on hardware security modules (HSM), which enhance the security of NFC devices by integrating special encryption chips.These technologies have their own advantages in practical applications. Rolling code encryption is outstanding in low-cost applications due to its simplicity and efficiency; CPU card encryption is widely used in situations requiring high security due to its powerful encryption capabilities and flexibility. However, each technology has certain limitations, such as rolling code encryption may be subject to prediction attacks, and CPU card encryption may face side channel attacks.

3. Encryption Methodology and Technical Model Basis

In NFC technology, both symmetric and asymmetric encryption models are used to protect communication security and prevent data from being eavesdropped or tampered with during transmission. Symmetric encryption uses the same key for encryption and decryption. Commonly used symmetric encryption algorithms include Advanced Encryption Standard(AES), Data Encryption Standard(DES) and Triple Data Encryption Standard(3DES). In NFC devices, symmetric encryption algorithms are widely used in scenarios that require fast encryption and decryption due to their fast computing speed and high performance. However, symmetric encryption also faces some problems, especially in key management. The key must be securely distributed and stored among all communication participants. If the key is stolen or leaked, all data encrypted with the key may be at risk. Therefore, NFC systems are usually designed to use asymmetric encryption in combination for secure key exchange. Rivest-Shamir-Adleman(RSA) is one of the most common asymmetric encryption algorithms and is widely used in key exchange and authentication of NFC devices. In NFC applications, the main advantage of asymmetric encryption is that it can achieve secure communication without sharing keys. Although asymmetric encryption provides higher security, its computational complexity is high and the encryption and decryption speed is relatively slow. Therefore, in practical applications, at the beginning of NFC communication, the two communicating parties will use RSA for initial key exchange. One device will generate a pair of public and private keys and send the public key to the other party. The other device uses the received public key to encrypt a randomly generated symmetric key (i.e., AES key), and then sends the encrypted AES key back to the first device. The first device uses its private key to decrypt the encrypted AES key to obtain the symmetric key[3]. In this way, the two parties securely share a symmetric key without exposing the symmetric key in plain text during the communication process[4].

The most common password generating method for NFC device is the rolling code encryption technology, a dynamic password generation technology that is widely used

in NFC cards, especially in payment without contact and access control systems[5]. The working principle of rolling code encryption is to generate a one-time password for each communication through a predefined algorithm and a synchronized counter. Each time the NFC card communicates with the reader, the counter is incremented and a new rolling code is generated based on the current value of the counter and a previously shared seed. This rolling code is only valid in the current session and will be updated in the next session. Therefore, even if an attacker intercepts the rolling code data, it cannot be reused in future communications. This way of dynamically generating passwords effectively prevents replay attacks, where attackers capture data packets in legitimate communications and then replay them later in an attempt to deceive the system. Because the rolling code changes in each session, replay attacks cannot use old data packets for authentication. In addition, rolling code encryption can also prevent the threat of copying the card. Since each NFC card has a unique counter and key, an attacker cannot copy its rolling code generation mechanism even if he copies the physical appearance of the card. This encryption technology does well for improving the security of NFC cards and ensures the security of users' funds and data.

To combine the techniques, Central processing Unit card(CPU card)CPU card is used as a kind of NFC hardware that can equip encryption algorithms.It is a smart card with an integrated microprocessor, which is widely used in data storage and processing scenarios that require high security, such as bank payments, identity authentication, and access control systems. CPU cards usually include a microprocessor, memory, input or output interfaces, and a hardware encryption module. The hardware encryption model of the CPU card is the core of its security. The microprocessor is responsible for executing instructions, managing data, and controlling communications. The memory is used to store the card operating system, applications, and sensitive data (such as keys and user data). The hardware encryption module is used to perform encryption and decryption operations. These modules usually support multiple encryption algorithms, such as AES, DES, 3DES, and Elliptic Curve Cryptography(ECC)[6]. The hardware encryption module in the CPU card is usually implemented through a hardware accelerator, which can greatly improve the speed and efficiency of encryption and decryption[7].

The CPU card performs well under high security requirements, mainly in the following aspects: Firstly it have the ability of anti-physical attack, such as preventing power analysis, timing analysis, and other side channel attacks. The hardware encryption module and microprocessor design include a variety of protection mechanisms, such as randomization operations, encrypted power lines and data lines, and even automatic destruction of sensitive data when a physical attack is detected.Besides, CPU card can also achieve data encryption and authentication. Sensitive data in the CPU card can be encrypted and stored and transmitted to ensure the security of the data on the communication link. In addition, the CPU card can implement two-way authentication, that is, the card and the reader mutually verify their identities to ensure the legitimacy of both parties in communication. This authentication method is widely used in bank payment systems and security access control systems.Furthermore, it owns programmability and flexibility. Unlike traditional read-only memory cards, CPU cards can be programmed, which enables them to support complex applications and security protocols. Multiple applications can be loaded on the card, and security policies and algorithms can be updated as needed. This flexibility makes CPU cards more adaptable in response to emerging security threats.

4. Application of Encryption in NFC technology

The application of NFC technology in payment systems is becoming increasingly common, such as mobile payment solutions like Apple Pay and Google Wallet. Through NFC, users can make convenient payments by tapping their phone. However, data security is crucial during the payment process. Encryption technology encrypts sensitive data, such as bank card information and transaction records, to ensure that the data is not stolen or tampered with during transmission. Common security threats in payment systems include data theft, transaction tampering, and fraudulent behavior. To address these threats, payment systems typically use encryption technologies such as end-to-end encryption (E2EE) and tokenization[8]. E2EE ensures that data is encrypted throughout the entire process of sending and receiving, while tokenization technology replaces actual bank card information with randomly generated tokens to prevent the leakage of sensitive information[9].

NFC technology has also been widely used in identity authentication systems, such as access cards, electronic passports, and mobile NFC access control. Through NFC technology, identity authentication devices can quickly read and verify identity information. Encryption technology plays a crucial role in this process, preventing identity information from being counterfeited or accessed without authorization. For example, in an electronic passport, data is securely encrypted and stored in an NFC chip, which can only be decrypted and read by specific devices. At the same time, electronic passports also use Public Key

Infrastructure (PKI) to verify the authenticity and integrity of data, preventing identity forgery. For access control systems, bidirectional authentication between encrypted NFC tags and card readers ensures that only users holding legitimate authentication information can obtain access permissions.

In addition to payment systems and identity authentication, NFC technology has also been widely used in fields such as data transmission, smart homes, and the Internet of Things (IoT). In these application scenarios, encryption technology is also crucial for ensuring data privacy and security. For example, in smart home systems, NFC can be used to control smart door locks and household appliances, transmitting control instructions through encryption to prevent hackers from hijacking and unauthorized access[10]. In the data transmission between IoT devices, encryption technology ensures communication security between devices and prevents data from being intercepted or tampered with during transmission.

5. Experiment and Model Evaluation

This experiment aims to evaluate the security of rolling code and CPU card encryption in NFC technology, especially the protection effect when subjected to various attacks such as replay attack and man-in-the-middle attack. The experiment will use a variety of equipment and tools, including NFC card reader, rolling code encryption card, CPU encryption card, and attack simulation tools such as Proxmark3. Proxmark3 easy, which can be seen in figure 1, is chosen to be the attack simulation tool for the experiment because its easy to get and use. First, prepare the equipment and materials required for the experiment, ensure that all equipment is configured correctly and the environment is controlled to reduce external signal interference. The experiment is divided into two main parts: rolling code test and CPU card test. In the rolling code test, the NFC card reader is used to read the initial data of the rolling code card, record the generation rules and communication protocol of the rolling code, and then use the attack tool to simulate the interception and replay of the rolling code signal, try to perform replay attack, and analyze its defense effect. In the CPU card test, the NFC card reader is used to read the data of the CPU card, record its encryption protocol and communication process, and then use the attack tool to perform man-in-the-middle attack, signal interference, etc., to test its encryption strength and defense capabilities. The experimental results will be processed by analysis software such as Wireshark, and the performance of each encryption technology under different attack conditions will be recorded in detail, and an experimental report will be generated with improvement suggestions. This experiment aims to systematically evaluate the security of NFC encryption technology, analyze its effectiveness in practical application scenarios, and provide a reference for future NFC security enhancements.

Fig.1 Schematic diagram of Proxmark3 easy

During the experiment, the key to data collection is to accurately read and analyze the data of the encryption card and conduct effective attack simulation. First, the initial data of the rolling code encryption card and the CPU encryption card are obtained through the NFC card reader. The rolling code generated by the rolling code encryption card data read after each communication changes according to the built-in fixed rule. The encrypted data of the

CPU encryption card is recorded at the same time. Their data are collected separately. Subsequently, attack simulations are performed using tools, the Proxmark3 easy, including replay attacks and man-in-the-middle attacks. The attack results on the rolling code encryption card show that the rolling code encryption successfully defended 20 out of 20 replay attacks. The subsequent experiment failed to defend the first time in the 37th replay attack, and the replay attack defense success rate was about 97.3%; but only 18 times of the first 20 man-in-the-middle attacks were successfully defended, with a success rate of about 90%. In the replay attack test of the CPU card, it is often difficult to make an effective defense, and only 14 out of 20 attacks are successful, with a success rate of 70%. However, during the man-in-the-middle attack, the CPU card defended against the middle device's attempt to tamper with the data packet. The results showed that the CPU card successfully detected the tampering of all data packets, and successfully defended from the first twenty to the first fifty times, with a success rate of 100%, showing the robustness and anti-interference ability of its encryption mechanism against man-in-the-middle attacks.

The experimental results show that rolling code encryption and CPU card encryption show different protection effects when facing different types of attacks. Rolling code encryption performs well in defending against replay attacks, but is easily cracked by man-in-the-middle attacks; while CPU card encryption shows strong encryption strength in resisting man-in-the-middle attacks, but its ability to identify replay attacks is obviously defective and can be easily bypassed by the same data. Model evaluation of the experimental results shows that both encryption technologies have room for further optimization. For example, rolling code encryption was bypassed in the last replay attack, indicating that its algorithm may have defects under certain conditions, such as occasional repetitions or potential regularity of the algorithm. The findings in the experiment prompted us to put forward some improvement suggestions, such as optimizing existing encryption algorithms, increasing hardware support to enhance defense capabilities, or introducing multi-level encryption measures to improve overall security.

6. Conclusion

The main findings of this paper on NFC technology encryption methods include the application and security analysis of encryption methods such as symmetric encryption, asymmetric encryption, and encryption devices such as rolling code encryption and CPU card encryption. Different encryption methods are suitable for different scenarios, and different encryption devices are targeted at different attacks. Symmetric encryption technology is widely used in NFC communications to provide fast data protection due to its efficient encryption and decryption speed. However, the security of its key management and distribution remains a key issue. Asymmetric encryption technology provides higher security by using public and private key pairs for encryption and decryption, while its processing speed is slower and is not suitable for all NFC applications.

For encryption devices, rolling code encryption technology prevents replay attacks by dynamically updating encryption codes, demonstrating its effectiveness in protecting against repeated attacks. Experimental results show that rolling code encryption performs well in dealing with replay attacks, but vulnerabilities may still occur. CPU card encryption technology uses complex encryption algorithms and internal processing units to provide higher protection capabilities, especially in defending against man-in-the-middle attacks and signal interference.

These encryption technologies are crucial in protecting the security of NFC communications. Symmetric encryption and asymmetric encryption each have their own advantages and are suitable for different application requirements, while rolling codes and CPU card encryption provide an additional layer of protection, further enhancing the security of NFC communications. Ensuring the effective application and cooperation of these encryption technologies can significantly improve the security of NFC systems, prevent data leakage and unauthorized access, and ensure the security and privacy of user information.

Limited by the experimental scene and equipment, as well as the rapid development of encryption algorithms and their variants, the research on NFC encryption in this article is still limited. The author may follow the development of encryption field, try to improve the credibility and accuracy of experiments in the future, study more advanced and efficient encryption algorithms, and try to use new technologies to improve the existing common security models to make them more in line with actual needs.

References

[1] Milanov, E. The RSA Algorithm [J]. RSA Laboratories, 2009: 1-11.

[2] Ramandeep Sharma, Richa Sharma, Harmanjit Singh. Classical Encryption Techniques [J]. International Journal of Computers & Technology, 2012: 84-90.

[3] Verma, S., Kapoor, V., Maheshwari, R. An Enhanced Cryptographic System for Fast and Efficient Data Transmission [J]. Advances in Intelligent Systems and Computing, 2019, vol 870.Ma Kunlong. Short term distributed load forecasting method based on big data. Changsha: Hunan University, 2014.

[4] Zhimao Lu, Mohamed H. A Complex Encryption System

Design Implemented by AES [J]. Journal of Information Security, 2021, 177-187.Fangfang. Research on power load forecasting based on Improved BP neural network. Harbin Institute of Technology, 2011.

[5] Ghanem, A., AlTawy, R. Garage Door Openers: A Rolling Code Protocol Case Study [C]. 2022 19th Annual International Conference on Privacy, Security & Trust (PST), 2022.Ma Kunlong. Short term distributed load forecasting method based on big data. Changsha: Hunan University, 2014.

[6] Cheng, C.W., Cantu, M.H., Kumar, S. Analyzing Computational Components of Standard Block Encryption Schemes [J]. Journal of Computer and Communications, 2022, 81-89.

[7] Ratnadewi, R.P.A., Hutama, Y., Ahmar, A.S., Setiawan, M.I. Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC) [J]. Journal of Physics, Series 954, 2018.

[8] Pourghomi, P., Saeed, M.Q., Ghinea, G. A Proposed NFC Payment Application [J]. International Journal of Advanced Computer Science and Applications, 2013.

[9] Bojjagani, S., Sastry, V.N. A Secure End-to-End Proximity NFC-Based Mobile Payment Protocol [J]. Computer Standards & Interfaces, 2019, 66: 1-21.

[10] Xie, L. Design and Application of Device Management System Based on RFID and Face Recognition [J]. Journal of Software Engineering and Applications, 2021, 382-395.