AURAPUB

Deep Learning and Pattern Recognition
2024 Volume1,Issue1

DLPR

Design and implementation of the electronic label authentication protocol based on digital signature

Peilin Wang[1*], Tianyu Hu[1],

1 School of Computer Science and Technology, Hainan University, Haikou, 570100, China

Abstract. RFID technology plays a critical role in item identification, tracking, asset management, anti-counterfeiting, and wireless communication, significantly enhancing productivity. However, the security of the wireless communication link between electronic tags and readers is a growing concern, limiting wider adoption. Ensuring secure electronic tag authentication is essential.

This paper focuses on implementing a system to encrypt electronic tags using digital signature algorithms like Elliptic Curve Cryptography (ECC) and RSA. It compares these methods in terms of signature computation time, memory usage, and key length, highlighting their advantages and limitations. The paper begins by detailing the components, principles, applications, and security challenges of RFID systems. It then delves into ECC, which provides high-security strength with shorter keys, and RSA, which relies on large prime factorization and is widely used. Experimental results reveal that ECC offers advantages in encryption speed and key efficiency, especially in resource-constrained environments, while RSA remains suitable for specific scenarios. This study demonstrates the implementation of these algorithms in RFID systems and provides insights into their comparative strengths and constraints.

Keywords: Digital signature; Electronic tag; ECC algorithm; RSA algorithm

1 Introduction

1.1 Background and significance of the paper

Background of the paper

With the rapid development of the information society, the Internet of Things (IOT) technology has been widely penetrated into various fields. In the Internet of Things technology, radio frequency identification (RFID) technology has been widely used with its unique advantages (such as long-distance reading, fast processing of large amounts of data, etc.). As an important part of RFID technology, electronic tag [1] is not only applied in the fields of supply chain management, logistics, traffic management and other fields, but also plays an important role in medical care, retail, public security and other fields.

The wide application of electronic tags has also brought some new problems and challenges, among which the most critical issue is the security and privacy protection of electronic tag data. Since the information interaction between readers and tags is [2] in an open wireless communication environment in a challenge-response way, the data is likely to be illegally read and tampered with, which not only poses a threat to personal privacy, but also poses the risk of leaking trade secrets and national security. Even if the RFID system is simple and convenient, it is difficult to be promoted on a large scale. Therefore, how to effectively protect the data security and privacy of electronic labels has become an important topic of current research.

At present, there are many mature encryption algorithms and security authentication protocols in cryptography, but due to the limitations of RFID tags in computing and storage capacity, [3], most of them cannot be directly applied in RFID systems. As a means of authentication based on public key encryption technology, digital signature can effectively solve the problem that the traditional cryptography technology is difficult to achieve in passive electronic labels, and ensure the authenticity and integrity of electronic data. At the same time, the advantage of not requiring readers and tags to jointly maintain the key pair can also guarantee the lightweight [4] of the tag end operation. By applying digital signature technology to electronic label authentication, the data security and privacy protection of electronic label can be effectively solved.

Therefore, the design and implementation of electronic label authentication protocol as the research topic. Through this study, a system implements authentication on RFID tags using different digital signature algorithms, while comparing the performance of different encryption algorithms from three different aspects.

Research significance of the paper

RFID technology with its low cost and convenience advantages to bring huge productivity benefits, but also exposed the greater security risks, such as data leakage, information forgery, illegal access, location tracking, etc., these security.

Full hidden dangers have become the main reason for hindering the further development of RFID technology. The authentication protocol of tags and readers in electronic tags can solve the associated hazards and secondary hazards caused by information leakage [5], which is to protect electronics The key link of label information security. Because label resources are limited and cannot support strong encryption, information security of low-cost RFID tags is a challenging task [6], and the design of algorithms and protocols need to consider tags The limitation of. In the case of common electronic labels with limited storage and computing power, it is necessary to realize security authentication and ensure the lightweight of label end operation.

Digital signatures can provide security services such as authentication, data integrity and anti-denial. The electronic label authentication protocol based on digital signature can effectively protect the security and integrity of the electronic label data, prevent the data from being illegally tampered with and forged, and help to protect the privacy of users. As a kind of asymmetric encryption technology, digital signature is easier to realize secure authentication in passive passive electronic label in wireless open system.

This study will design and implement an electronic label authentication system based on digital signature. The significance of this study is that it applies different digital signature algorithms to RFID labels and shows, more intuitively shows the realization of digital signature on electronic labels; the significance is to show different algorithms in different aspects by comparing different digital signature algorithms and the combination of electronic labels; the significance is to guarantee the security application of security in various fields of electronic labels, enhance the public trust and acceptance of Internet of Things technology, and promote the social application of Internet of Things technology.

1.2 Research status at home and abroad

Due to the limitations of RFID tag equipment resources, although it is difficult to design a cheap and safe and efficient safety mechanism, many safety methods have been proposed through the unremitting efforts of domestic and foreign researchers.

For RFID system security requirements, in the beginning is achieved through hardware protection, namely the security method based on physical mechanism, the security mechanism can be implemented in some specific occasions to protect data privacy, such as security requirements, but the security mechanism usually need third party equipment, high cost, and poor flexibility, cannot play to the advantages of RFID low cost, also cannot meet the market demand. Therefore, the security authentication protocol based on the password mechanism has gradually become the mainstream of the security mechanism.

Crygraphy-based security protocols are more flexible, less costly and more applicable than physical methods. The security mechanism can be divided into three kinds: authentication protocol based on simple logic operation, authentication protocol based on symmetric cryptosystem and authentication protocol based on asymmetric cryptosystem [7]. For the authentication protocol based on simple logic operations, such as LMAP protocol, RAPP protocol, EMAP protocol, SASI protocol, HB protocol, etc.

The calculation and storage cost is small, but the failure of two-way authentication cannot meet the security requirements of RFID system. The authentication protocol based on the symmetric cryptography system mainly includes the authentication protocol based on DES and the authentication protocol based on AES. The symmetric cryptography mechanism needs to manage the key. Once the key is leaked, the attacker can get all the data. For authentication protocols based on asymmetric cryptography system, such as RSA, ECC, DSA, etc., although they have higher security, they also need more computational costs. However, the lightweight label side can be ensured by putting the more expensive operations on the server side.

At home and abroad, research in related fields is progressing, and various new protocols and algorithms are proposed to deal with changing needs and threats. However, due to the characteristics of electronic labels, the field still faces many challenges, such as how to further reduce the computing and storage requirements while ensuring security, and how to improve the efficiency of authentication while protecting privacy.

1.3 Research content of the thesis

The paper aims to design and implement a system that can simulate the encryption of RFID tags, using two different digital signature algorithms, ECC (elliptic curve cryptography) and RSA (Rivest-Shamir-Adleman) [8].

First, this paper introduces the RFID technology and its wide application in various fields. With the popularity and large-scale application of RFID tags, the security and privacy protection of data have become an important focus. In order to ensure the secure transmission and integrity of RFID tag data, digital signature algorithm has become a common and effective encryption means.

Second, this paper details ECC and RSA in terms of performance. The analysis of existing algorithms reveals their advantages and disadvantages, made improvements, and remaining security problems. Finally, the system is implemented and the experimental and performance evaluation is performed, verifying that the two algorithms are compared on performance indicators such as response time, memory footprint and key length to evaluate their performance in electronic label encryption.

Overall, this paper provides an in-depth study of the field of RFID tag encryption by implementing a system that can encrypt RFID tags using different digital signature algorithms and making a comprehensive comparison of their performance. The research results of this paper aim to improve the security of RFID tag encryption system and contribute to RFID security and privacy protection in practical application, and provide valuable reference for further research in related fields.

1.4 Organizational structure of the paper

This article is divided into five chapters, and each chapter is arranged as follows:

Chapter 1: introduces the research background and research significance of the paper and the development status at home and abroad. Through the development and application of electronic tags, the current challenges of RFID system, the advantages of digital signatures and other aspects of the background and significance. According to the different mechanisms of RFID to deal with security problems, and different security protocol.

Chapter 2: expounds the related theory and technology of RFID system, introduces the model of RFID system, the working principle of RFID and the workflow of RFID system. It also explains the current security risks of the RFID system, and details the measures to be taken to deal with various security threats.

Chapter 3: It mainly introduces the two digital signature algorithms, ECC algorithm and RSA algorithm. The research and analysis of the proposed algorithms, explain the process in the electronic label authentication, and introduce the advantages and improvements made from many aspects, as well as the existing security problems and defects.

Chapter four: introduces the function and implementation method of the system, and analyzes the conclusions of the system. The advantages and disadvantages of ECC and RSA are explained in terms of signature time consuming, memory footprint, public and private key length.

Chapter 5: Summarize the work carried out in this paper, and put forward further work prospect in combination with the functions that the system can realize but have not been realized theory and techniques of RFID

1.5 RFID, system overview

The RFID system model

Electronic tag is a new generation of small device [9] used for identity identification. The traditional RFID system model generally consists of [10]: electronic tag (Tag), reader (Reader) and background server (Server). The system structure diagram is shown in Figure 2.1. When the system is working, for passive electronic labels, the reader and writer first sends a specific frequency RF signal to the electronic label, so that the electronic label generates induced current and obtains energy, sends the stored information back to the reader, and then the background server operates the information obtained by the reader and writer. For active electronic tags, it can directly send a frequency signal to the reader, and then operated by the background server.

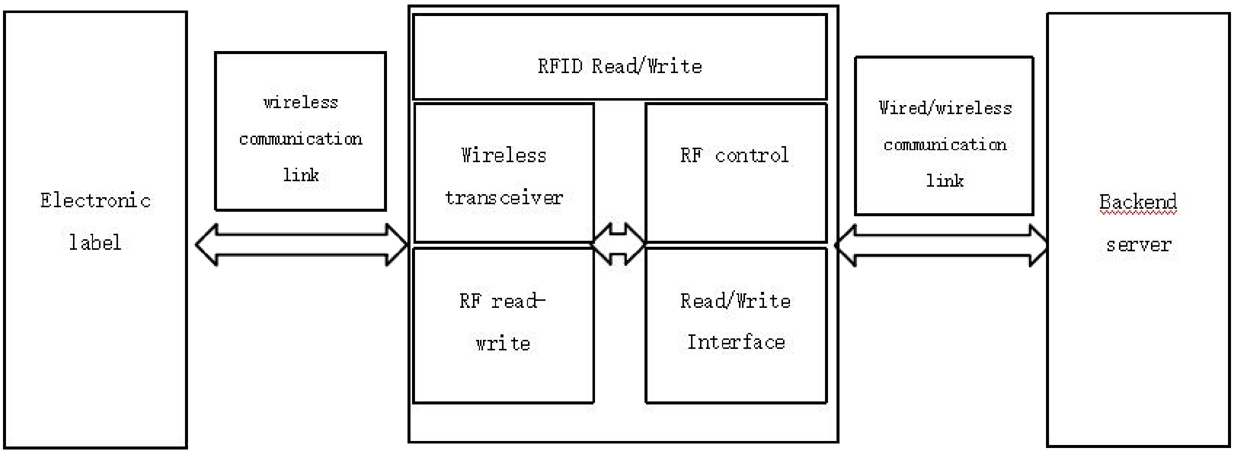


Figure 2.1 Structural diagram of the RFID system

(1) Electronic label

The electronic tag (Tag) has a unique electronic code, is a unique fixed identity symbol of the electronic tag, attached to the object to identify the target object [11]. The electronic tag is composed of an internal circuit and a chip coupling element, integrating multiple modules, such as an antenna module, a power supply module, a memory module, a control module, etc., as shown in Figure 2.2. Electronic labels can be divided into active and passive labels according to the way the energy is provided. For passive labels, this kind of label can only be consumed by the induced current generated by the reader and writer, so the calculation power is weak and unable to achieve complex calculation, but it has the advantage of low cost. At the same time, the passive label has a simple structure, a small volume, and a relatively long life span. The active label can actively send a signal to the reader, which can provide the energy needed for calculation, so it has strong computing power, high performance, large storage capacity, but the cost is relatively high. Due to the limited life of the own power supply, the life of the active label is relatively short.

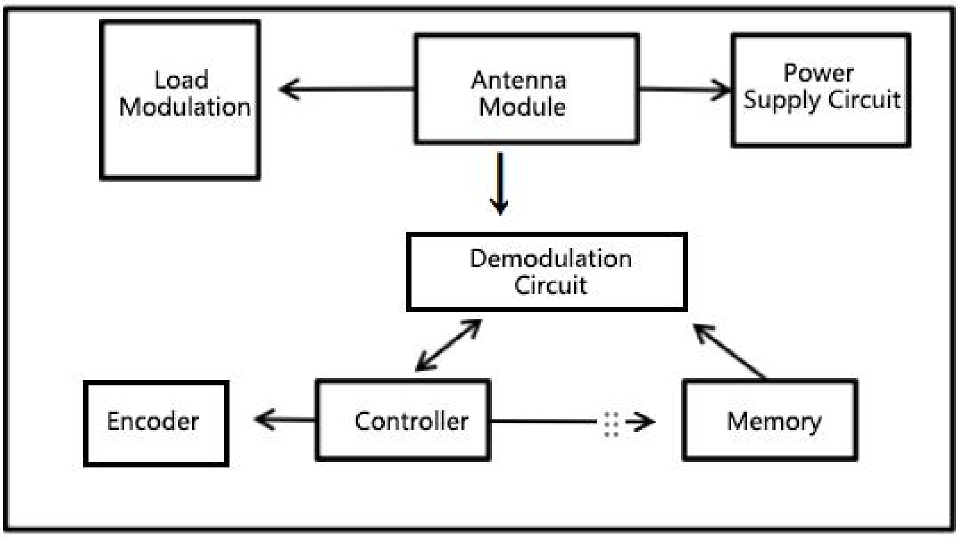


Figure 2.2 Internal structure diagram of the electronic tag

Electronic labels can be divided into low frequency (LF), high frequency (HF), ultra-high frequency (UHF) and microwave (MV) according to their operating frequency. For low-frequency electronic labels, the more common operating frequencies are 125 kHz and 134 kHz [12]. This kind of electronic label read range is short, generally between a few centimeters to dozens of centimeters. The advantage of low frequency electronic label is that it can better penetrate non-metallic objects without being susceptible to electronic interference. It is often used in animal tracking, car anti-theft and access control systems. The operating frequency of the high-frequency electronic labels is generally 13.56MHz. Its reading range is relatively far, and can reach about one meter. The labels are widely used in ticketing, payment, document tracking, and biometrics. UHF electronic tags work between 860 MHz and 960 MHz, and their read range is a few meters or even ten meters. In addition, their data transmission rates are also relatively higher. However, the UHF electronic tags are less adaptable to environmental conditions, especially for liquid and metallic environments. Such labels are widely used in logistics and supply chain management, baggage handling, warehouse management and other scenarios. Microwave electronic tags usually work at a frequency of 2.4GHz or 5.8GH z, and they have longer read distances, up to tens of meters, and higher transmission rates. But its hardware costs are also similarTo be higher, and are more sensitive to environmental factors. Microwave electronic tags are often used in highway toll stations and other applications that require long-distance reading.

According to different reading and write methods, electronic labels are mainly divided into read-only labels, read and write labels, read-only labels and read and write labels with data protection function. The read-only label writes data at one time, then the internal data cannot be modified and can only be read; the read and write label can repeatedly read and write the internal data of the label; after the write, the read-only label is allowed to write data once, and the data cannot be modified, but can be read several times; the read and write label with data protection function can read and write, but also pair.

The data is locked to prevent being modified or deleted.

(2) Reader and writer

The main function of the reader is to communicate with the RFID tag by the radio frequency, and to read or write the information in the tag. It mainly consists of antenna, RF module, controller, data interface and power supply of [13]. The reader structure is shown in Figure Figure 2.3. The reader sends a radio signal through the antenna to motivate the RFID tag within its working range, where the radio signal motivating the RFID tag is generated by the RF module, and the task of receiving the signal reflected by the label is also responsible by the RF module. The controller is the core part of the reader, which is responsible for controlling the workflow of the reader, such as sending read or writing instructions, processing the received data, etc. The data interface is used to transfer the data obtained by the reader to the upper computer or other devices. The common data interfaces are serial interfaces (such as RS232, RS485), parallel interface, USB interface, Ethernet interface, etc. Depending on the type of reader and the environment, it may be DC, AC, or battery powered.

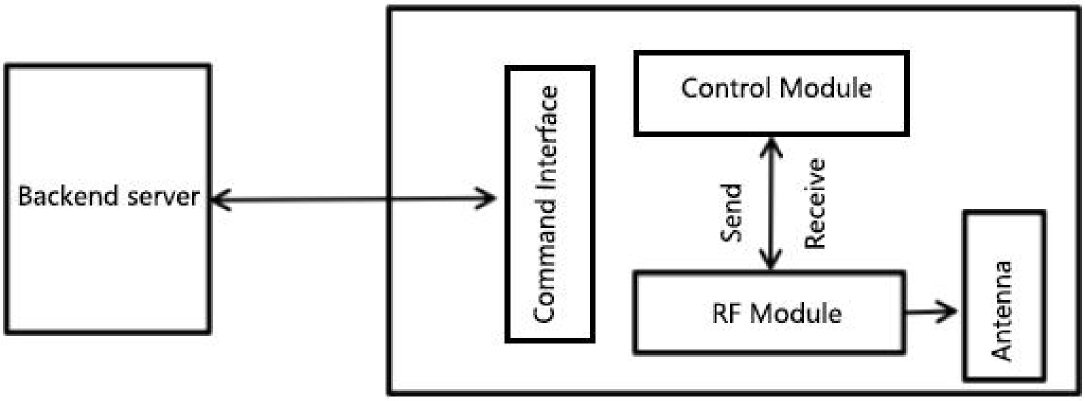


Figure 2.3 Structure diagram of the reader and writer

(3) Background server

Background server, also known as background data management system, including database, application server and middleware, is the data center of the whole RFID system, which is responsible for processing the data obtained from readers and writers, and executing the corresponding business logic. These data generally contain the unique identifier of the electronic label, and possibly other label-related data, while the background server can also write the data into the allowable electronic label through the read and writer. In addition, it also has the functions of data analysis, system management and data sharing. Overall, the background server is a core part of the RFID system that connects the RFID system with a specific business.

RFID, working principle

When the RFID system works, the RFID tag is first activated, and the reader transmits radio energy through its antenna. When the electronic tag enters the operating range of the reader [14], the tag receives the radio energy and passes through this.

Energy activates itself. For passive RFID tags, this energy is used for power. Once the electronic tag is activated, it sends back the information stored inside it (such as a unique identifier) to the reader. Data transmission is achieved through the transmission of radio signals (reflection modulation). For writable electronic labels, the reader can also write data. Then, the data receiving and processing, that is, the reader receives the data from the electronic label, and performs preliminary processing, such as decoding and checking. The processed data is then transmitted to the background server through the data interface.

Finally, the background server conducts subsequent processing of the received data, such as storage, analysis, display, etc.

Since readers can usually read multiple electronic labels at the same time, anti-collision processing is also needed to avoid conflicts of label data. In addition, the RFID system may do some other processing, such as data filtering, data encryption and decryption.

1.6 Security issues of the RFID system

RFID system security risks

Several types of security threats of RFID system are as follows:

(1) Illegal reading

Because RFID tags can be read wirelessly at a certain distance, an attacker may use an illegal RFID reader to illegally read information from an electronic tag. This will lead to the disclosure of private data, such as personal identity information, location information, etc.

(2) Fraud attack

A spoofing attack is also known as counterfeit attacks, and an attacker may forge electronic tags or readers to trick the system for illegal access or operation. For example, forge a label with a specific authority to illegally enter a restricted area.

(3) Replay the attack

For such attacks, the attacker captures a legitimate RFID communication process and then replay the process when appropriate. By this means, an attacker may be able to bypass some security controls, such as authentication.

(4) Tracking and positioning

Since the reading of electronic labels does not require the participation of the label subject, the attacker may use this feature to track the holder of the label and conduct illegal positioning or behavior analysis.

(5) Physical attack

RFID tags may also be subject to physical attacks, which can directly affect the function of the tags and lead to data loss. There are also attackers through some illegal means to obtain customer information directly from the label surface, and even to obtain the label internal information.

Security requirements for the RFID system

(1) Data confidentiality

A kinds of sensitive privacy information may be stored in RFID tags, and usually need to be implemented through encryption to prevent illegal reading. Encrypt at write and then decrypt at read and retrograde. Using this method, even if the attacker can capture the data in the transmission, it cannot interpret their true meaning.

(2) Data integrity

Data in RFID tags may be maliciously modified or damaged during the process of transmission, so some means are needed to ensure the integrity of the data. If you use a hash function or a digital signature to check whether the data has been modified, the hash function can generate a unique fingerprint of the data, even if the data only changes slightly, the hash value will change significantly. Digital signature uses the private key to encrypt the hash value, so that when reading the data, the public key can be used to decrypt, and compare the decryption results with the recalculated hash value, to verify whether the data has been modified.

(3) Authentication

To prevent spoofing and replay attacks, both readers and tags require authentication. Authentication is usually achieved in a challenge-response manner, where the reader sends a random challenge to the label, and then the label needs to use an internal key to generate a correct response. Only a verified reader can read or write the labels, and only a verified label will respond to the reader request.

(4) Prevent tracking and positioning

With the use of electronic tag reading, the attacker may also track the tag holder. In order to prevent this, various technologies are needed to protect the anonymity of labels, such as dynamic identification and anonymous authentication. Dynamic identification means that the label will use different identification codes each time, while anonymous authentication means that the label does not need to expose its true identity during the authentication process.

(5) Prevent physical attacks
Damage to the label can be resolved by using wear-resistant materials. For the acquisition of label surface information or internal information, there are blocking label method and active interference method. The blocking tag method activates the RFID "block" command through a specific password, after which the RFID tag will no longer read any request accordingly.host

Dynamic interference method refers to the specific device to transmit RF signals to interfere with the work of RFID readers.

1.7 Summary of this chapter

This chapter first mainly introduces the RFID system model, elaborated the internal composition, work tasks and work methods from three parts of electronic tags, readers and background server, which elaborated the various classifications of electronic tags, and different application fields for different specifications. Secondly, the security risks of RFID system are analyzed from the multiple attacks adopted by attackers, which shows that the security problem of wireless link communication between RFID tag and readers is the most important problem. Finally, the response methods of different security risks are analyzed and explained.

2 Research on the electronic label authentication protocol based on digital signature

2.1 ECC certification protocol analysis

Digital signature is mainly used to realize the integrity of data, the authentication of data source and the non-deniability. Compared with the digital signature scheme based on RSA, the ECC-based digital signature scheme is more efficient and more suitable for the resource-limited wireless sensor network [15].

Analysis of the EC-RAC protocol.EC-RAC is a protocol based on elliptic curve cryptography for authentication [16] between electronic tags and readers. It combines the functions of encryption and authentication, ensuring the confidentiality, integrity, and authentication of the communication.

(1) The meaning of the symbols in the agreement
The meaning of the symbols in the agreement is shown in Table 3.1.

Table 3.1 Meaning of symbols in the agreement

symbol	meaning
Reader	reader-writer
Tag	RFID
P	Elliptic curve generates the element
r 1， r 2	Random numbers generated by the background server and the electronic tags
(y, Y)	The private key and the public key of the background server

(2) Agreement execution process

First, the reader and writer store the private key and public key {y, Y = yP} in the background server, and the public key {x_2, X_2 = x_2P}and the identification information {x_1, X_1 = x_1P}. The RFID tag stores the public key {x_2, x_2 = x_2P} and its own identification information {x_1, x_1 = x_1P}.

Then the reader generates a random number r_2 zn and generates a request to send to the label, after the label is received, ready to perform subsequent computation and response.

After the label receives the random number, it first judges whether the random number r_2 is zero. If it is zero, the protocol is directly terminated, and the output authentication fails [17]. If not zero, the electronic label generates a random number $r_{2\in}z_n$ and performs the following calculations:

$$T_1 = r_1P \qquad （3.1）$$

$$T_2 = (r_1 + x_1)Y \tag{3.2}$$

$$v = r1x1 + r2x2 \tag{3.3}$$

reader decrypts the encryption results with the private key and verifies the received signature with the public key of the label.

The specific calculation is:

$$X_1 = y^{-1}T_2 - T_1 \tag{3.4}$$

Finally, whether the equation vp x 1 T 1= X 2 is valid. If so, the signature verification is passed, indicating that the identity authentication of the label is successful. The compumethod is tested as follows:

$$y^{-1}T_2 - T_1 = y^{-1}(r_1 + x_1)y - r_1p = (r_1 + x_1)p - r_1p = r_1x_1 = X_1 \tag{3.5}$$

$$(vp - x_1T_1)r_2^{-1} = [(r_1x_1 + r_2x_2)p - x_1r_1p]r_2^{-1} = r_2x_2pr_2^{-1} = x_2p = X_2 \tag{3.6}$$

(3) Agreement security performance analysis.

The EC-RAC protocol uses digital signature technology to ensure the integrity of the communication data. Through the verification of the signature, it can ensure that the received data comes from the label, and there is no malicious modification in the process of transmission. Meanwhile, it can also confirm the identity of the label and prevent the forged label from communicating as a legal label. In addition, the EC-RAC protocol also prevents replay attacks by using random numbers and challenges, with new random numbers and challenges being used per communication, making the old communication data unable to be reused in subsequent communications.

Elliptic curve cryptography, relative to traditional encryption algorithms such as RSA, can achieve shorter key length at the same level of security, reduce the cost of storing and transmitting keys, and reduce the probability of the key being cracked. Because side channel attacks are usually based on the physical characteristics of analytical computing equipment under different operations, such as power consumption, electromagnetic radiation, etc., and the elliptic curve operation in EC-RAC protocol usually has low power consumption and execution time, thus reducing the risk of side channel attacks.

The EC-RAC protocol also has certain security defects. Because EC-RAC protocol can only by the reader to verify the legitimacy of label identity, can not judge whether the random number is sent by legitimate readers, the attacker can launch a denial of service attack (DOS), by continuously generate random number to electronic tags RFID tag calculation, consume a lot of computing resources, makes the RFID system produces a large number of redundant information, readers and tags cannot normal authentication, thus can not work.

Moreover, the EC-RAC protocol can only realize the authentication of the RFID tag by the background server, but does not realize the authentication of the RFID tag to the reader, so this protocol is a one-way authentication protocol [18] without label anonymity.

Analysis of the protocol modified by Liao et al.*(1) The meaning of the symbols in the agreement*

The meaning of the symbols in the agreement is shown in Table 3.2.

Table 3.2 Meaning of symbols in the agreement

symbol	meaning
Reader	reader-writer
Tag	RFID
P	Elliptic curve generates the element
(X R , X R)	The public and private key of the reader
(X T , X T)	The public and private key of the electronic label

(2) *Agreement execution process.*

The private key XRzn is first generated by the reader, from which the public key XR = XRP is calculated and generated. Similarly, the RFID tag should also generate the private key XTzn and the calculation tag public key XT = XTP, and then send the tag public key and its own private key to the reader, which is stored in the background server.

Then a random number r 2 zn is generated by the reader, calculated R 2= r 2 P, and generated a challenge sent to the label, simultaneously sending R 2. After the electronic label receives the challenge, the random number r 1 zn is generated and the following calculation is completed:

$$\mathrm{R}_1 = \mathrm{r}_1\mathrm{P} \tag{3.7}$$

$$\mathrm{TK}_{\mathrm{T}1} = \mathrm{r}_1\mathrm{R}_2 \tag{3.8}$$

$$\mathrm{TK}_{\mathrm{T}2} = \mathrm{r}_1\mathrm{X}_\mathrm{R} \tag{3.9}$$

$$\mathrm{Aut}h_\mathrm{T} = \mathrm{S}_\mathrm{T} + \mathrm{TK}_{\mathrm{T}1} + \mathrm{TK}_{\mathrm{T}2} \tag{3.10}$$

is calculated and sent(Aut*h*T, R1)to the reader. After the reader receives the data returned by the electronic tag, calculate it TK R 1= r 2 and TK R 2= X R R1, and then verify the equation Aut*h*T TK R1 TK R2 = XT. If the equation holds, the reader authenticates the label successfully. Then the background server calculates Aut*h* R= X T R1 + r 2 X T and sends the results to the RFID tag.

After the label receives the Aut*h* R, the equation Aut*h* R= r 1 X T + X T R 2 is verified. If the equation is established, the electronic label is also verified successfully.

(3) Agreement security performance analysis

This agreement further improves the EC-RAC protocol and realizes the two-way authentication protocol. The server ensures the legitimacy of the tag by verifying the received signature, and the label can also confirm the legitimacy of the server. Since the two random numbers (r 1, r 2) are different each time, Aut*h* T and Aut*h* R are unpredictable in each session, and the attacker cannot track the position of the target by intercepting the exchanged messages,

Even if an attacker sends a malicious request to the RFID tag, the attacker cannot track the owner of the RFID tag by analyzing the exchanged messages. Therefore, this agreement has anonymity and the ability to resist tracking attacks, which is the most important security requirement for privacy.

As for the forward security of the protocol, we assume that the attacker has obtained the key of the label, but the attacker cannot get the temporarily generated random number, so the protocol can not know the previous communication content, so this protocol also has the forward security.

2.2 RSA certification protocol analysis

(1) The meaning of the symbols in the agreement

The meaning of the symbols in the agreement is shown in Table 3.3.

Table 3.3 Meaning of symbols in the agreement

symbol	meaning
M	proclaimed in writing
H(M)	The clear hash value
S	digital signature
N	modulus
e	Public key index
d	Private key index

(2) Agreement execution process

A pair of RSA keys is first generated by the reader, including the public and private keys. The public key consists of modulus N and public key exponent e, and the private key consists of modulus N and private key exponent d.

Htext M hhhelectronic the text abstract H (M). Later, the private key index d is used by the electronic label to obtain the signature s=H (M) d modN. Then the plaintext M and the digital signature S are sent together to the reader side.

Then, the reader end is authenticated. After receiving the plaintext M and the digital signature S, the public key index e and analog N sent by the label end are used to decrypt the digital signature S, and the decrypted plaintext summary H(M) = se modN is obtained. The reader hashes the received plaintext and obtains the explicit summary H (M)

Later, compare whether H (M) and H (M) are equal. If equal, if the same, the authentication is passed, the message integrity is verified, and the reader can trust the tag end. If not equal, the authentication fails, indicating that there may be message modification or forgery the risk of.

As shown above, RSA signature algorithms generally require combining hash functions to realize the generation and comparison of explicit summaries. The choice of hash function can be decided according to the specific requirements and safety requirements. The common hash functions include [19] including MD5, SHA-1 and SHA-256.

(3) Agreement security performance analysis

First of all, the RSA signature algorithm itself does not provide anonymity. Since the signature is generated using a private key, the reader can verify the authenticity of the signature through the public key and identify the sender of the signature. At the same time, RSA algorithm does not have forward security. If the senders private key is leaked or cracked, the previously generated signature is still valid, so the protection of forward security requires other measures, such as changing the key regularly or using the encryption algorithm with forward security. In addition, the RSA algorithm itself does not have special protection for tracking attacks. If the signature information is intercepted, the attacker can track the sender of the signature. In order to resist tracking attacks, it can consider using anonymous communication protocol, confusing technology or using confusing agents to communicate. For side channel attacks, the RSA signature algorithm is very vulnerable, especially those based on side channel information such as execution time and power consumption analysis. To resist side channel attacks, side channel resistance techniques can be used, such as RSA varieties using anti-side channel algorithms or isolation and protection measures of the physical layer can be used. Similarly, the RSA signature algorithm is not directly involved in anti-denial-of-service attacks, but some measures can be taken to mitigate the impact of denial-of-service attacks when using signatures, such as using traffic restrictions, authentication, and accessControl strategies and others [20]

RSA algorithm is usually used to ensure the integrity of information and authenticate the identity of the sender. In the application scenarios of electronic tags, in order to meet different security requirements, a variety of technologies and security measures may need to be used, such as encryption algorithm, hash function, access control, physical layer security, etc.

2.3 Summary of this chapter

The main research content of this chapter is the analysis of the existing ECC algorithms and RSA algorithms. First of all, the specific authentication process of different ECC algorithms and RSA algorithms on the electronic label is introduced. Through the analysis of the calculation process, the security performance of the protocol and the security risks are mainly analyzed from the aspects of anti-denial of service attack ability, anonymity, forward security, anti-channel attack, anti-channel attack and anti-tracking attack. Then the improved protocol and the previous protocol are compared and analyzed, and the improved safety performance and the problems still exist. Finally, how to improve some security risks of RSA from other ways besides improving the algorithm itself.

3 System implementation and result analysis

3.1 System implementation

System environment

The system is written in the python language and implemented by using the PyCharm Community Edition 2022.1 development platform under the Windows operating system. Two windows were built to communicate via the TCP / IP protocol, with one analog tag end and the other analog reader end.

The system represents the label ID by entering the clear text at the label end, and simulates the label end and the reader end to implement the authentication protocol using different algorithms. The hardware computer configuration processor uses the AMD (R) R5-460 0H@3.00GHz.

Key code

(1) Communication implementation of the key code

A new thread is created with the server_thread function, which is a continuously running server that can listen for new connections and accept the data sent through these connections. Call the receive_instructions function, accepting a string list argument. In TCP / IP communication, all data is transmitted in the form of byte flow, so it is necessary to combine all parameters into one string on the sender and decompose the string back to the original parameter on the receiver. The key codes are as follows:

```
# Create a TCP socket

with socket.socket(socket.AF_INET,socket.SOCK_STREAM) As s:s.bind ((HOST,

    PORT)) # bind the host name and port number

    The s. listen() # starts listening for the connections

    Conn, addr = s. accept() # Accept the connection
    request with conn: # Establish the connection

        The print (Connected by, addr) # Print connection
        information while True:

            Data = conn.recv (1024) # The received data

            ifnot data: # End the cycle break if no data is received
```

(2) Calculate the signature time key code

In this paper, we record the time spent to measure the performance of different algorithms by recording the time between the execution and the execution of the signature, as the time spent by the algorithm. Taking ECC encryption algorithm as an example, the key code is as follows:

```
start = time.time() # Record the signature start time
self.signatureA = self.sign_message(self.instructionA) # signature end = time.time() # Record the end
time of the signature
self.encryption_time = end-start # Calsignature takes time self.encryption_time_label.config (
Text = f Time taken to encrypt:{self.encryption_time} seconds) # Export signature to take time
```

As the code shows, the signature takes time to output in the tag side window for more intuitive understanding.

(3) Key code for calculating the key length

For the password length has been determined when the algorithm selection, there are mainly 1024 bit and 2048bit for RSA algorithm, while the public and private key lengths for ECC algorithm are 19 2bit, 256bit and 384bit. The RSA key length selected by the system is 1024bit and ECC, and the key length used by the algorithm is 192bit, because they have basically the same security strength [21], which is easier to measure their performance in other aspects. Taking the ECC algorithm as an example, the key code is as follows:

```
# Generate the ECC key pair
private_key = ec.generate_private_key(ec.SECP192R1())public_key = private_key.public_key()
# Get the ECC key length
private_key_length = private_key.key_sizepublic_key_length = public_key.key_size
# Output the ECC key length
self.private_key_label.config (Text = f private key length: {private_key_length}
bit)self.public_key_label.config (text=f public key length: {public_key_length} bit) As shown in the
above code, the public key and the private key length are displayed on the label end.
```

(4) Key code of computing memory usage

The system uses the psutil library to get the memory usage of the current process in MB. Its key Code is as follows:

```
process = psutil.Process() # Get memory footprint
memory_usage = process.memory_info(). The rss / 1024 / 1024 # computing memory footprint
The print ("Memory usage:", memory _ usage, "MB") # output memory usage as shown in the above
code, obtain the memory usage is converted to MB before output.
```

3.2 Analysis of the results

The analysis of the experimental results consists of three parts, namely, ECC certification, RSA certification and comparative analysis of the performance of the two. As shown in Figure 4.1 and Figure 4.2, the system is divided into two interfaces, representing the tag end and the reader end, which simulate the communication between the electronic tag and the reader in the RFID system through TCP / IP communication.

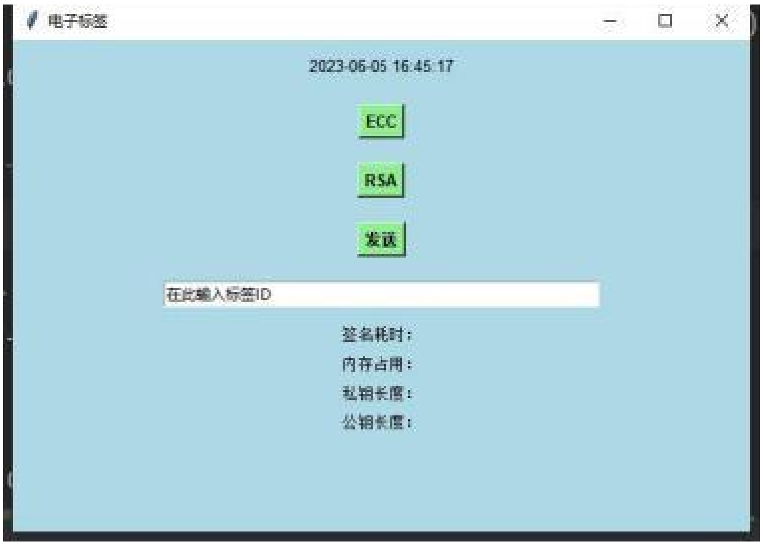


Figure 4. 1 Schematic diagram of the electronic tag end

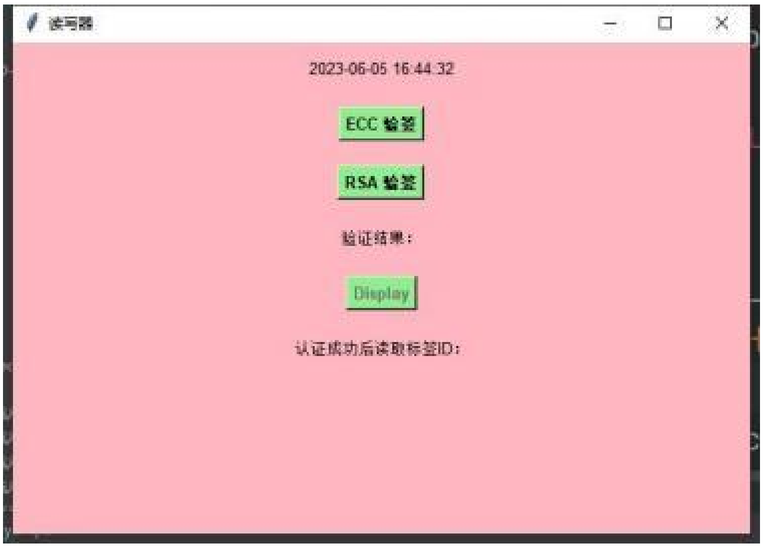
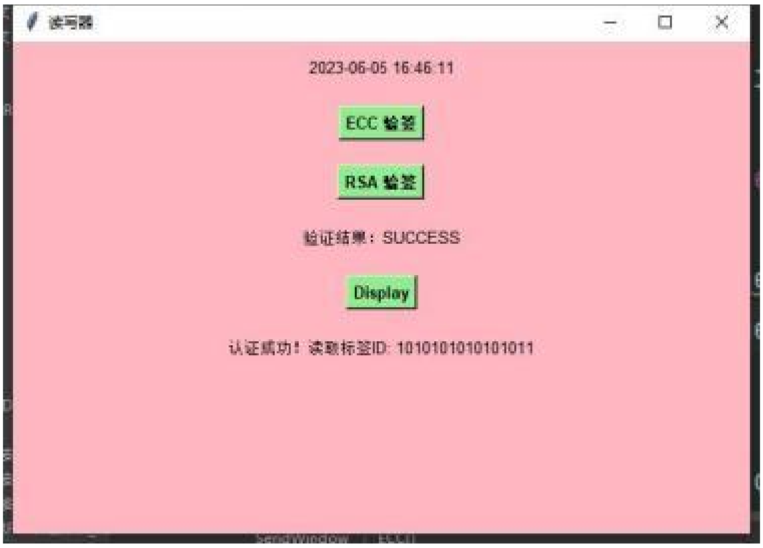


Figure 4.2 Schematic diagram of the reader end

ECC certification implementation

For the authentication process of ECC, the 16-bit plaintext is first input manually in the set plaintext input box to simulate the electronic label ID. Then click the ECC button to indicate that you can use the ECC algorithm to implement the authentication protocol. The background will automatically generate the private key, public key and random number and calculate it. The calculation process has been explained in Chapter 3. Then click to send all the calculated data sent to the reader, then click the ECC check button, the background will calculate from the label data, the specific calculation process also as shown in chapter 3, automatic authentication after calculation, after authentication is successful, will successfully receive electronic tag ID, click the D isplay button display electronic tag ID. The final certification of successful results are shown in Figure 4.3



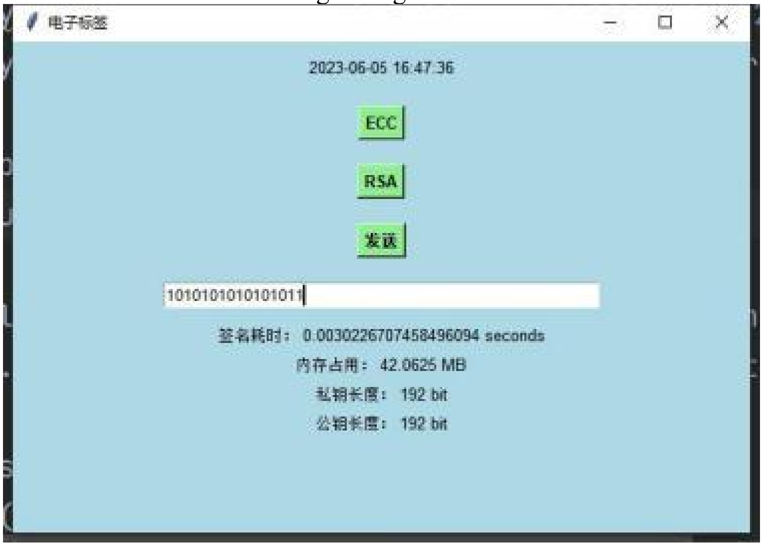
2023-06-05 16:46:11

验证结果：SUCCESS

认证成功！读取标签ID: 1010101010101011

Figure 4.3 Schematic diagram of ECC authentication

In addition, the time and memory footprint and key length of the encryption have been described and will be displayed on the label side. As shown in Figure Figure 4.4.



2023-06-05 16:47:36

1010101010101011

签名耗时： 0.0030226707458496094 seconds

内存占用： 42.0625 MB

私钥长度： 192 bit

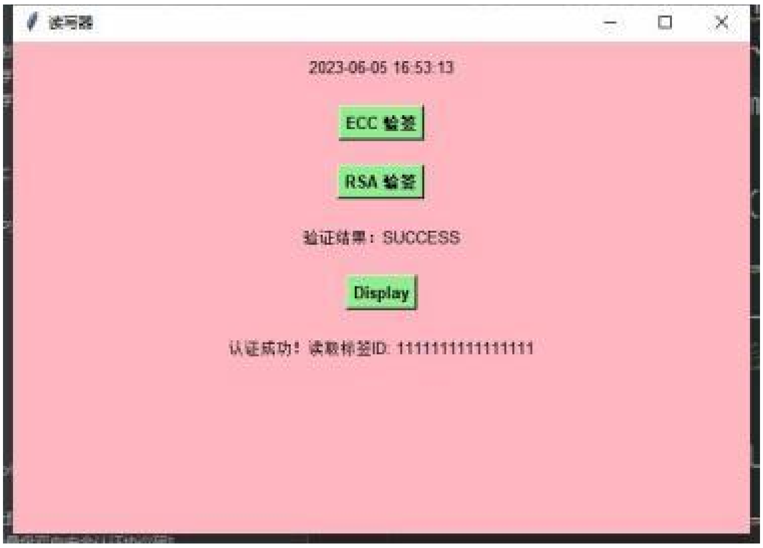
公钥长度： 192 bit

Figure 4.4 Schematic diagram of the ECC algorithm tag end

It can be seen that the 192-bit ECC algorithm is used to implement the authentication protocol. The execution time of the 16-bit tag ID signature is only about 3 milliseconds, and after many tests, each execution time is basically in milliseconds, indicating that the protocol is able to achieve lightweight and meet the market demand for lightweight RFID tag certification protocol. Because the memory usage can only calculate the memory usage of the entire process, it cannot separate the memory usage of the signature, so the ECC algorithm authentication alone, and the memory usage can not be analyzed after comparing with the RSA encryption algorithm.

RSA certification implementation

The RSA algorithm authentication protocol is basically the same as the authentication with ECC algorithm. First, input 16-bit plaintext at the label end to represent the label ID. Then click the RSA button, and the background will first encrypt it through the hash algorithm, and then sign the encrypted summary and send it to the tag end for verification. After the verification, click the Display button will display the tag ID. The certification results are shown in Figure 4.5.



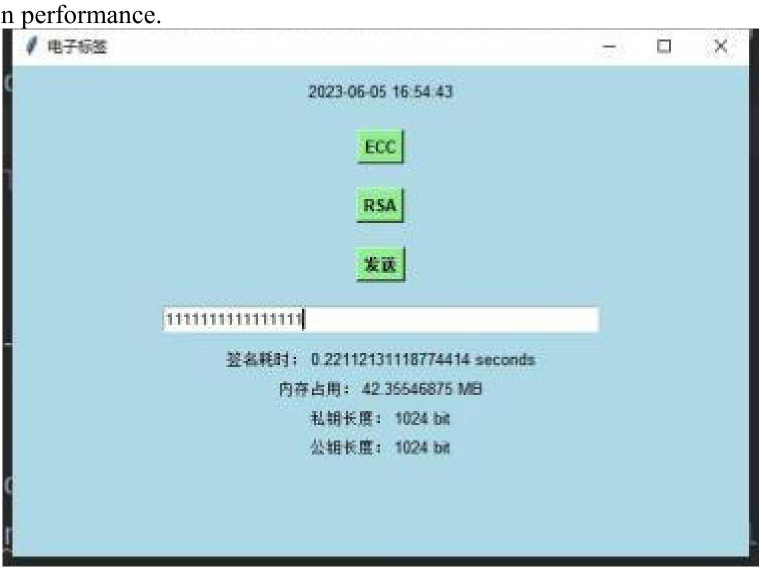
2023-06-05 16:53:13

验证结果：SUCCESS

认证成功！读取标签ID: 1111111111111111

Figure 4.5 Schematic diagram of the RSA successful authentication reader end

The signature time-consuming, memory footprint and the length of public and private key of RSA algorithm authentication are also displayed on the label end, as shown in Figure 4.6. It is obvious that for the authentication of the electronic tag ID of the same length, the signature time of the 1024-bit RSA algorithm with basically the same safety strength [22] as the 192-bit ECC algorithm is up to about 22 1 ms, and the results are basically near this level after many experiments, close to more than 70 times the signature time of the ECC algorithm. Similarly, because the memory usage is the memory usage of the whole program, it is impossible to directly obtain the accurate memory usage of the algorithm. However, after many RSA algorithm authentication experiments and comparison with ECC algorithm authentication, it is not difficult to find that RSA algorithm is also slightly higher in memory usage than ECC algorithm. Therefore, it can be judged that under the same conditions, the ECC algorithm has a higher encryption performance.



2023-06-05 16:54:43

1111111111111111

签名耗时： 0.22112131118774414 seconds

内存占用： 42.35546875 MB

私钥长度： 1024 bit

公钥长度： 1024 bit

Figure 4.6 The label end diagram of the RSA algorithm

Comparative analysis

Although RSA algorithm is lower than ECC in terms of unit security strength, it is still the mainstream digital signature scheme [24] because of its relatively simple [23] and has been widely used and studied for decades, which has been proved to be safe and reliable. Due to the late emergence of ECC algorithm, and the implementation and use of ECC algorithm require specific mathematical knowledge and professional skills, which limits its application in some fields. At the same time, the application scope and compatibility are worse than that of RSA algorithm, so the penetration rate is lower than that of RSA. However, with the rise of the resource-limited environment and the Internet of Things, the requirements for data security are becoming higher and higher, and the demand for signature algorithms is also increasing. With its advantages of fast encryption speed and higher efficiency, ECC algorithm has been even more widely used in recent years, and its own development has become more rapidly.

Compared with RSA algorithm, the differences between ECC algorithm are mainly reflected in the following aspects:

(1) Key length
The ECC algorithm is able to use a shorter key length to provide a security [25] comparable to the RSA algorithm. In contrast to RSA requiring a longer key (typically 1024bit or longer), ECC, the algorithm can use a shorter key length (typically 256 bit) to achieve the same security level [26], which makes the ECC algorithm more applicable in resource-constrained environments, such as RFID tags, with limited computing and storage resources.

(2) Operation speed
According to the experimental results, ECC algorithm is usually faster than RSA algorithm in encryption and decryption operations, because ECC algorithm is based on elliptical curves. In contrast, the RSA algorithm uses the factorization problem [27] with large prime numbers, which has a higher computational complexity. Speed is an important factor in the communication between RFID tags and readers, as tags usually need to be used in a short period of time responses to the readers request.

(3) Storage requirements
The ECC algorithm requires less storage space than the RSA algorithm. This is due to the ECC algorithm can use a shorter key length while ensuring security and requiring less storage space. This is particularly important for RFID tags, which usually have very limited storage capacity and minimize the storage space occupied by the algorithm.

(4) Safety
The ECC algorithm is based on the elliptic curve discrete logarithmic problem [28], which is considered a relatively difficult mathematical problem. Although the security of the ECC algorithm also depends on the chosen elliptic curve and parameter settings, the ECC algorithm is widely accepted and considered safe and reliable under correct selection and implementation.

3.3 Summary of this chapter

This chapter first describes the main functions of the system, which mainly simulates the ECC algorithm and RSA algorithm on the RFID system authentication, explicit transmission and from the aspects of signature time, memory usage, public key length and private key length shows the basic performance of the different algorithm, and explains the environment of the system. Then show the operation process of the system and the function and significance of the controls, analyze and explain the conclusions of the system, explain the advantages of ECC algorithm over RSA algorithm in terms of key length, operation speed, storage requirements and security, and explain why although ECC algorithm in many aspects due to RSA algorithm, its widespread adoption in practical application is relatively low. However, ECC algorithms have become increasingly attractive in specific scenarios and are expected to be more widely used.

4 Summary and Outlook

4.1 Work summary

Based on the advantages of RFID technology, including fast data transmission speed, batch read and write labels, non-line-of-sight identification and strong environmental adaptability, it has been widely used in many fields. With the rapid promotion of RFID technology, its safety problems are also gradually obvious, which has become an important factor hindering the development of RFID technology. Because the communication between tags and readers in the RFID system is completed in the open environment, it also becomes a weak link in the whole RFID system. Based on the deep understanding of the working principle of RFID system, this paper focuses on the safety issues between RFID tag and readers.

Firstly, according to the working principle and application scenario of RFID system, this paper analyzes the security risks and security requirements of the system, and discusses the possible attack means and corresponding security strategies. Then, how the existing security protocols are applied to the authentication between RFID tags and readers is expounded, and all aspects of security are analyzed. We know that the original EC-RAC protocol has been able to complete the basic authentication, preventing unauthorized third parties from obtaining the communication content, ensuring the integrity of the data, and confirming the identity and credibility of the label, ensuring that the information comes from the legal label. At the same time, it can also effectively prevent the replay attack and the side channel attack.

However, EC-RAC protocol still has defects such as inability to resist denial of service attacks and anonymity. Liao et al later improved this, achieve anonymity, anti-tracking attacks and forward security. For RSA algorithm, in addition to ensuring the integrity of the information and the identity of the sender, it itself can not meet other security needs, and needs to integrate a variety of technologies and security measures to achieve.

Finally, a system is implemented to simulate the communication between readers and tags, and to use the most widely used ECC algorithm and RSA algorithm for interstate authentication, which more intuitively shows the implementation of the security protocol based on encryption algorithm in the RFID system. In addition, the different authentication protocols are compared in terms of encryption time, key length, and memory footprint to measure their performance.

4.2 Work Outlook

Through the analysis and research of the existing protocols, this paper designs a system that simulates the RFID tag end and the reader end authentication. In the future work, it can also be improved and deepened from the following aspects:

(1) To achieve more agreements, the development of the agreement has actually experienced a long process, and only after continuous improvement can it be widely used at present. The system can be made more intuitive by implementing more protocols

Improvement process of the protocol.

(2) Use different key digits of the same algorithm for authentication, which can not only measure the performance of different algorithms, but also help to understand and compare the performance and function of different key digits.

(3) Realize the simulated attack. By simulating various attack methods used by the attacker, the security requirements of the protocol can be tested from more aspects and the security performance can be measured more reasonably.

(4) The design of the new protocol, with the further development of RFID technology, the demand for its security will be more and more high, the design of a new security protocol is still an important topic, can be more lightweight, can also have more powerful security.

Reference

1. Dong Zhenjie. RFID Lag Ownership Transfer Protocol Research in the Internet of Things [D]. Xidian University, 2021.
2. Liu Yali. RFID Security Certification Protocol Research [D]. Nanjing University of Aeronautics and Astronautics, 2014.
3. Lu Wenna, Wang Genying, Liu Yun. Research based on a low-cost RFID mid-magnitude security certification protocol [J]. Railway Communication Signal, 2010,46 (12): 32-35.
4. Liu Yali, Qin Xiaolin, Zhao Xiangjun, etc.. Lightweight RFID authentication protocol based on digital signature [J]. Computer Science, 2015,42 (02): 95-99 + 107.
5. Shen Shuai. Research on the lightweight two-way security authentication protocol based on RFID [D]. Guilin University of Technology, 2019.
6. Vajda I,Buttyán L. Lightweightauthentication protocols forlow-cost RFI D tags.[C]. Second Workshop on Security in Ubiquitous Computing – Ubicomp,2003:2003.
7. Xia Yongxiang, Shi icai, Zhang Yu, et al. An RFID authentication protocol based on the light power encryption system [J]. Computer Engineering, 2014,40 (07): 69-72.
8. Cao Shuiren, Longhua, Liu Yun, etc. Performance analysis of digital signatures based on elliptic curves and RSA [J]. Modern electronic technology, 2006 (17): 29-31.
9. S. I. Ahamed, F. Rahman, E. Hoque.ERAP: ECC Based RFID Authentication Protocol.[J]. 2008 12th IEEE International Works hop on FutureTrends o fDistributed ComputingSystems, Kunming, China, 2008,pp:219-225
10. Gan Yong, Xu Yunqian, He Lei, etc. Review of the security and privacy of RFID systems [J]. Network Security Technology and Applications, 2015, No.180 (12): 69-71.
11. Ma Liqiong, Gao Daqing, Zhang Yumei. Research on RFID technology [J]. Information and Computer (theoretical edition), 2019,31 (20): 150-151 + 157.
12. Li Fuyu, Li Zhekun. Analysis of frequency band characteristics and application status of radio frequency identification (RFID) system [J]. Guide, 2007, No.45 (09): 1 + 3.
13. Liu Kai, Bi Yanbo, Guo Guowei. Analysis of the composition and characteristics of RFID technology [J]. Chinese and foreign entrepreneurs, 2015, No.484 (02): 128.
14. Wang Juan. RFID authentication protocol study based on hash function [D]. Nanjing University of Posts and Telecommunications, 2012.

15. Ayaz H M, Ummer I, G. M B. MutualEntity Authentication Pro tocol Based on ECDSAfor WSN.[J]. Procedia ComputerScience, 2016,89:187-192.

16. Li Hongzhang. Overview of the application of RFID read-write RFID technology in intelligent manufacturing systems [J]. Information and Computer (theoretical edition), 2021,33 (03): 173-175.

17. Tian Haowei. An RFID security protocol study based on ECC [D]. Yanshan University, 2022.

18. Zhang Wenli, Zhao Feng. Design and analysis of the RFID two-way security authentication protocol [J]. Smart Computer and Application, 2013,3 (05): 91-93.

19. Yang Wenqing. On the digital signature and the digital certificate [J]. Computer Products and Circulation, 2020 (11): 286.

20. Sun Yue. Research on the blockchain-based key generation and negotiation scheme [D]. Nanjing University of Posts and Telecommunications, 2020.

21. Chen Xianglin, Liu Runtao, Yu Cunguang. Hybrid data encryption algorithm based on DES and ECC [J]. Journal of Harbin University of Science and Technology, 2007 (01): 58-61.

22. Pang Wen. Application of the ECC algorithm in the digital signature [J]. Journal of Weinan Normal University, 2006 (02): 41-43.

23. Zhao Lijuan. Design and implementation of the licensing system based on ECC signature [J]. Microcomputer Information, 2010,26 (33): 54-55 + 60.

24. Song Shujun. Application of the RSA algorithm in the digital signature [D]. China University of Petroleum, 2007.

25. Li Qing, Chen Liang, Feng Mei, etc. Some typical data encryption algorithms [J]. Information System Engineering, 2017, No.287 (11): 148-149.

26. Liu Chun, Zhang Fengyuan, Zhang Qishan. Comparison and implementation of RSA and ECC algorithms based on smart cards [J]. Computer Engineering and Application, 2007, No.563 (04): 96-98 + 118.

27. Hu Nengfa. A message recovery signature based on elliptic cryptography [J]. Journal of Yangtze University (Natural Science Edition), Polytechnic Volume, 2008 (01): 190-192.

28. Zhao Jie. Analysis of the Internet of Things Security Technology [J]. Information Technology and Informatization, 2020, No.248 (11): 155-157.