A Lightweight Authentication Protocol for Mobile RFID

Tao Pan[1], Kai-Zhong Zuo[2,3], Tao-Chun Wang[2,3], and Chun-Hong Deng[1]
(Corresponding author: Tao Pan)

College of Internet and Communication, Anhui Technical College of Mechanical and Electrical Engineering[1]
No.16, Wenjin West Rd., Yijiang Dist., Wuhu City 241002, Anhui Province, China
College of Computer and Information, Anhui Normal University[2]
Anhui Key Laboratory of Network and Information Security[3]
No.1, Beijing East Rd., Jinghu Dist., Wuhu City 241000, Anhui Province, China
Email: ahjdpt@126.com
(Received Apr. 24, 2023; Revised and Accepted Nov. 23, 2023; First Online Feb. 23, 2024)

Abstract

Recently, Radio Frequency Identification (RFID) has been widely used. A lightweight security authentication protocol for mobile RFID is proposed to aim at the problems of high complexity and system security in existing mobile RFID authentication protocols. The tag identity is encrypted by the matrix's arrangement and combination of column vectors based on column pseudonyms, which can effectively reduce tag computational complexity. The tag is required to mainly store its identity and shared keys, which can effectively reduce tag storage complexity. During the authentication process, the proposed protocol generates dynamic authentication keys without changing shared keys, which are different in each session. The protocol uses XOR operation to transfer privacy data based on the dynamic authentication keys. This method can effectively reduce the computational complexity of the protocol while protecting privacy data. The protocol requires the receiver to verify the random number in time after receiving information, which can effectively solve the system security problem. Formal proof and analysis results show that the proposed protocol has good security and can resist attacks. The experimental results indicate that the protocol has low complexity, which can effectively reduce the burden of tag operation and storage. It has good value for mobile RFID systems.

Keywords: Arrangement and Combination; Authentication Protocol; Dynamic Authentication Key; Mobile RFID; Random Number

1 Introduction

RFID is a non-contact automatic identification technology which was born in the 20th century. In recent years, Internet of Things (IoT) technology has attracted extensive attention, because it can greatly improve the quality of people's lives. RFID is becoming more and more popular as one of the key technologies of IoT. As the RFID system has low cost and high reliability, it is now widely used and combined with everyday life [1], such as health, agriculture, and so on. Its market capitalization is expected to rise to $ 16.23 billion by 2029 [5, 6].

RFID uses radio signals to identify a product, animal or person. In addition to identifying objects, RFID system also plays an important role in tracking and managing objects [3]. RFID authentication technology is the basis of its applications. A typical RFID system consist of three parts: RFID tag, reader and database. When RFID authentication begins, RFID tag responses to the incident RF energy transferred from the reader. Then the tag sends out the identity information. After receiving the information, the reader can decode and modulate it. Then the reader transmits it to the database. Finally, the database verifies the legitimacy of the tag identity. Through identity authentication, we can confirm whether the tag is a legitimate user registered in the system. As the increasing demand on privacy protection and system security, RFID security authentication technology has become particularly important, and it has more and more attention [23].

Generally, the traditional RFID authentication is regarded as fixed RFID authentication and the RFID reader cannot be moved, which is not suitable for mobile application scenarios. It has been unable to meet people's need. Thus, the mobile RFID authentication is recommended. For example, in animal husbandry, people used to count the growth information of animal artificially in the past. This method cannot feedback growth information in time making it difficult to guide business improvement. The mobile RFID authentication can realize automatic registration and identification of multiple objects. People only need to hold the mobile reader within the specified

range. Then the mobile reader can quickly receive the information and identify a large amount of tag identity. As a result, it greatly improves management level. Mobile RFID authentication brings convenience to people's life and the production of industry and agriculture. However, it brings new challenges. Mobile RFID authentication puts forward new requirements for protocol complexity and system security.

This paper proposes a lightweight authentication protocol for mobile RFID. The rest of the paper is organized as follows. The second section introduces the characteristics of mobile RFID authentication mode and analyzes the challenges of the mode. The third section briefly reviews the typical RFID authentication protocols and analyzes that the current protocols, which are not suitable for mobile RFID system. The fourth section defines some prior knowledge of data encryption required in the authentication process. The fifth section describes detail authentication process of the protocol. The formal proof based on BAN logic of protocol security performance are provided in the sixth section, alongside with the security comparison with existing protocols. The seventh section compares and analyzes the complexity of the protocol through experiments. Finally, the eighth section gives the conclusion of the paper.

2 Authentication Mode of Mobile RFID

In the mobile RFID system, there are three entities, including the database, the mobile reader and the tag. Both the database and the reader have strong computing power and large storage space. They can perform a variety of complex operations. Unlike traditional RFID reader, the mobile RFID reader can be moved randomly. The RFID tag chip has small area and simple hardware structure [2]. Thus, the storage space of the tag is limited, and the computing power is poor. The traditional encryption algorithms with high complexity are not suitable for the tag [9]. The authentication mode of mobile RFID is shown in Figure 1.

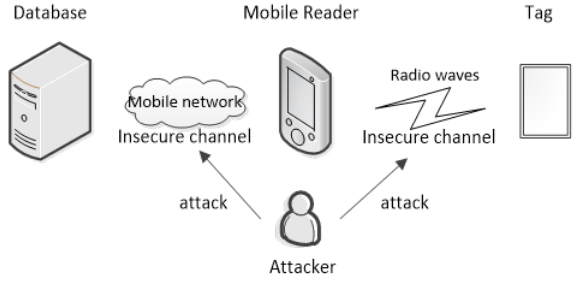

Figure 1: Authentication mode of mobile RFID

At present, there are two modes to authenticate the legitimacy of tag identity. One mode is that the database authenticates the tag identity. When receiving the tag identity, the mobile reader sends it to the database. Then the database authenticates the tag identity. The other mode is that the reader directly authenticates the tag identity. This scheme does not require too much participation of the database. The reader completes the tag identity authentication. It can reduce the number of wireless communications and the risk of communication. However, the mobile reader still needs a small amount of communication with the database in the second mechanism, while increasing the amount of computation of the mobile reader. People usually use the first mode to authenticate the tag identity, rather than using the second mode.

Since the mobile reader is removable, the wired communication channel is no longer suitable for mobile RFID system. The mobile reader communicates with the tag through radio waves. The communication between the database and the reader is based on mobile network. All communication channels are wireless. Due to the weakness of wireless channel, mobile RFID is more vulnerable to illegal attacks than fixed RFID. The attacker can perform signal interference on the channel, which interrupts normal communication. Sometimes, the attacker monitors the channel, intercepts and restores the encrypted data to the plaintext data. System security and privacy protection are the primary problems to be solved.

In fact, the rapid movement of the tag in mobile application scenarios will inevitably affect the efficiency of information reading [19]. It is also difficult to solve the low complexity computing problem of the protocol in mobile RFID system effectively.

3 Related Research Works

In recent years, a variety of RFID security authentication protocols have been proposed. Xu *et al.* proposed an ID-updated mutual authentication protocol for mobile RFID system in Reference [22]. In the protocol, the one-way hash function protects privacy data, and the identity update operation solves the tracking attacks of the tag. Due to the insecure channel of mobile system, it is likely that the data will be out of synchronous. Besides, the identity of the reader is transmitted on the insecure channel. This would suffer information leakage. Shen *et al.* proposed an improved anti-counterfeit complete RFID tag grouping proof generation protocol in Reference [18]. The protocol adopts a one-way pseudo-random function as the basic encryption method. Later, Reference [12] points out that it cannot prevent tag forgery and replay attacks. Tewari *et al.* proposed secure timestamp-based mutual authentication protocol in Reference [20]. The protocol uses timestamps and bitwise operation to provide security against disclosure. The subsequent identity authentication is performed after the initial judgment of whether the communication is legal according to the timestamp value. As the pseudonym information of tag identity is transmitted on the channel directly, the attacker can send

query signal for many times to obtain tag responses. And then, the attacker can obtain timestamp data easily to obtain legitimate authentication of the database. The protocol cannot prevent replay attacks. The reader does not verify the correctness of the information sent by the tag. It is vulnerable to denial-of-service attacks. Besides, the protocol assumes that the channel between the reader and the server is secure. It is not suitable for mobile RFID system. Chegeni *et al.* proposed a lightweight RFID mutual authentication protocol based on hybrid cryptography in Reference [8]. In the protocol, the data is encrypted by advanced encryption standard (AES) and the AES secret key is encrypted by Elliptic-curve (ECC). Since the ECC algorithm is asymmetric cryptography, the secret key is much secure. As reader's identity is not verified, the protocol is prone to replay attacks and denial of service attacks. Liu et al. proposed a mobile RFID authentication protocol in Reference [12]. The protocol adopts bitwise operation to encrypt the information, and requires tag to perform bit-wise operations multiple times, which increase the tag operation cost. It seems that the attacker can easily crack the database identity. The protocol cannot prevent impersonation attacks. The attacker can implement asynchronous attacks by signal interference. Other similar protocols, such as the literature [4, 11, 15, 17, 21].

Through the above analysis, it can find that the public key cryptography and the hash function cryptography are widely used for the current authentication protocols. These encryption methods increase computational cost and reduce the computational efficiency. It is particularly unsuitable for the low-cost RFID tag. Meanwhile, the current protocols face various security problems, such as replay attacks, tag forgery, and so on. All the above protocols are not applicable to the mobile RFID system. Therefore, it is an urgent problem to design a secure and low complexity authentication protocol for the mobile RFID system.

4 Preliminaries

We start to describe some prior knowledge of data encryption, which will be used in the proposed protocol.

4.1 Tag Identity Encryption

To ensure that the sensitive information of the tag cannot be decoded by the attacker, it is necessary to encrypt the identity of the tag. To facilitate the description, we use $Mvp(\ )$ to represent the arrangement and combination of column vectors of matrix. There are two parameters in $Mvp(\ )$, matrix X and parameter a, that is $Mvp(X,\ a)$. Assume that X is the binary number of length L, and the value of column parameter a is known. We first calculate the value of b and d, where b=L/a, d=L mod a, and judge whether d is equal 0. If d is equal 0, X can be expressed as the following equation,

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1a} \\ x_{21} & x_{22} & \cdots & x_{2a} \\ \vdots & \vdots & \cdots & \vdots \\ x_{b1} & x_{b2} & \cdots & x_{ba} \end{bmatrix}.$$

$Mvp(\ )$ encrypts the data in this way that arranges the column vectors in a sequential order. It is easy to get new data Y, that is, Y=$Mvp(X,\ a)$=$(x_{11}, x_{21}, \cdots, x_{b1}, x_{12}, x_{22}, \cdots, x_{b2}, \cdots, x_{1a}, x_{2a}, \cdots, x_{ba})$. If d is not equal 0, a certain number of binary number 0/1 is filled into X. In this way, the data after X transformation can be expressed as $(x_{11}, x_{12}, \cdots, x_{1a}, x_{21}, x_{22}, \cdots, x_{2a}, \cdots, x_{b1}, x_{b2}, \cdots, x_{ba}, x_{(b+1),1}, \cdots, x_{(b+1),d}, \varphi)$, where $\varphi = \{0,1\}^{(b+1)*a-L}$. Then it gets new data $Y = Mvp(X, a) = (x_{11}, x_{21}, \cdots, x_{b1}, x_{(b+1),1}, x_{12}, x_{22}, \cdots, x_{b2}, x_{(b+1),2}, \cdots, x_{1d}, x_{2d}, \cdots, x_{bd}, x_{(b+1),d}, x_{1,(d+1)}, x_{2,(d+1)}, \cdots, x_{b,(d+1)}, \theta, \cdots, x_{1a}, x_{2a}, \cdots, x_{ba}, \theta)$, where θ is 0 or 1.

Give an example, let X=(11110000) and a=4, then L=8, b=2, d=0. Finally, Y=$Mvp(X,\ a)$=(10101010). It is shown in Figure 2.

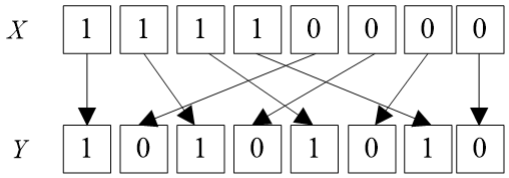

Figure 2: Encryption operation of Mvp()

4.2 Dynamic Authentication Key

In the authentication process, to protect the privacy data, the protocol generates dynamic authentication keys without changing the shared key.

Suppose K_u is a shared key whose binary length is S, it can conveniently use K_{uL} and K_{uR} to represent the dynamic authentication key, where u is a natural number.

Select m-bit binary numbers from the key K_u in order from left to right. The selected numbers are used as the high-bit numbers of K_{uL}. The remainder of K_{uL} is filled with 0. In a similar way, select n-bit binary numbers from the key K_u in order from right to left. The selected numbers are used as the low-bit numbers of K_{uR}. The remainder of K_{uR} is filled with 1.

For example, if K_u = (111001111111), m = 2, n = 6, then the dynamic authentication keys are K_{uL} = $(11\{0\}^{10})$, $K_{uR} = (\{1\}^{6}111111)$. It is shown in Figure 3.

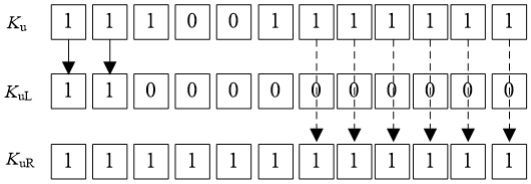

Figure 3: Dynamic authentication key

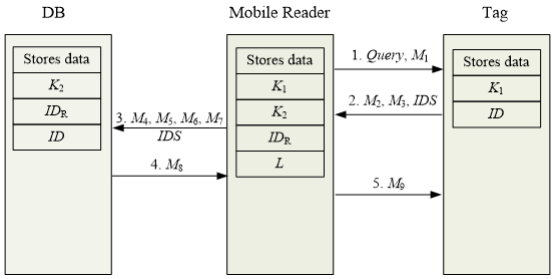

Figure 4: A lightweight authentication protocol for mobile RFID

5 The Proposed Authentication Protocol

5.1 Initial Conditions and Symbols

The tag is usually embedded in products. Sometimes it will be pasted on the object. The tag has low computing power and small storage space. It stores ID and K_1. The mobile reader has strong computing power and large storage space. It stores the binary length of ID, K_1, K_2 and its identity ID_R. The database stores ID, ID_R, K_2. It can verify the legitimacy of tag identity.

The definitions of the symbols used in protocol are shown in Table 1.

Table 1: Symbol definitions

Symbol	Description
ID	Identity of the tag
IDS	Encrypted ciphertext of ID
ID_R	Identity of the reader
L	The binary length of ID
K_1	Private key shared between the reader and the tag
K_2	Private key shared between the database and the reader
K_{1L}	The left part of K_1
K_{1R}	The right part of K_1
K_{2L}	The left part of K_2
K_{2R}	The right part of K_2
r_1	A random number generated by the reader
r_2	A random number generated by the tag
r_3	The other random number generated by the reader
$Mvp()$	The arrangement and combination of column vectors of matrix
$\oplus$	XOR operator
$\|\|$	Connection operator
$\triangleq$	Comparison operator

5.2 Authentication Process

The protocol authentication process is shown in Figure 4.

The authentication steps are described as follows.

Step 1. The reader generates a random number r_1, where $r_1 \in (2, L-1)$. It calculates $M_1 = (K_1 \oplus (r_1/2))||(L \oplus r_1)$. M_1 is divided into two parts. The value of $K_1 \oplus (r_1/2)$ can be marked as M_{1F}. And the value of $L \oplus r_1$ can be marked as M_{1S}. The reader sends query signal and M_1 to active the tag.

Step 2. After receiving the query signal from the reader, the tag performs the following operations.

1) The tag calculates $u_1 = M_{1F} \oplus K_1$ based on the private key, and calculates $u_2 = M_{1S} \oplus L$. It compares the values of u_1 and $u_2/2$ to determine whether they are equal. If they are equal, the tag gets r_1. Otherwise, RFID system suffers from counterfeiting attacks.
2) The tag calculates $p = L/r_1$, $q = Lmodr_1$. Then it uses K_1 and r_1 to calculate the value of a dynamic authentication key K_{1L}. It uses K_1 and p to calculate K_{1R}.
3) The tag calculates $IDS = Mvp(ID, r_1)$.
4) The tag ID is divided into p modules. Each module contains r_1-bit binary numbers. The remaining numbers are stored in the variable δ, if $L > p * r_1$. Then it performs odd check on each module to obtain check bits. These check bits are combined with variable δ to get a new number m.
5) The tag generates a random number r_2 and calculates $M_2 = K_{1R} \oplus r_1$, $M_3 = K_{1L} \oplus (m||r_2)$. Finally, it sends M_2, M_3 and IDS to the reader.

Step 3. After receiving the tag response, the reader performs the following operations.

1) The reader calculates $u_3 = L/r_1$. It uses K_1 and r_1 to calculate the value of a dynamic authentication key K'_{1L}. It also can use K_1 and u_3 to calculate K'_{1R}.
2) The reader calculates $u_4 = M_2 \oplus K'_{1R}$ and compares it with r_1, $u_4 \triangleq r_1$. If they are not equal, the reader determines that the information has been changed by the attacker.

3) The reader calculates $u_5 = M_3 \oplus K'_{1L}$. It is divided into two parts, one of which can be marked as m and the other as r_2. The reader stores r_2 to prevent replay attacks.

4) The reader generates a random number r_3, where $r_3 \in (2, L-1)$, and calculates $u_6 = L/r_3$. Then it uses K_2 and r_3 to calculate the value of a dynamic authentication key K_{2L}. It uses K_2 and u_6 to calculate K_{2R}.

5) The reader calculates $M_4 = K_2 \oplus r_3$, $M_5 = K_{2L} \oplus ID_R$, $M_6 = r_1 \oplus r_3$, $M_7 = r_1 \oplus m$, and sends the message IDS, M_4, M_5, M_6, M_7 to the database.

Step 4. The database verifies the legitimacy of the tag identity and sends response to the reader.

1) The database calculates $u_7 = M_4 \oplus K_2$, and stores it. Next time, it checks whether u'_7 is equal to u_7. If both are equal, the database terminates the authentication. The system suffers replay attacks.

2) The database uses K_2 and r_3 to calculate the value of a dynamic authentication key K'_{2L}. It uses K_2 and L/r_3 to calculate K'_{2R}.

3) The database calculates $u_8 = M_5 \oplus K'_{2L}$ and checks whether u_8 is equal to ID_R to verify the legitimacy of the reader identity.

4) The database calculates $u_9 = M_6 \oplus u_7$ and then calculates $u_{10} = M_7 \oplus u_9$.

5) First, the database gets plaintext of ID using the corresponding decryption, that is $ID = Mvp'(IDS, u_9)$. Later, it verifies the correctness of ID by m. If ID is incorrect, the authentication is terminated. Otherwise, the database verifies the legitimacy of tag identity by matching data ID in the database.

6) If the authentication is success, the received data are correct and legal. The database calculates $M_8 = K_{2R} \oplus (r_3||m)$ and sends it to the reader.

Step 5. The reader verifies the response information from the database at first, and then sends the latest reply about the legitimacy of the tag identity.

1) The reader calculates $u_{11} = M_8 \oplus K_{2R}$. The value of u_{11} is divided into two parts, u_{11F} and u_{11S}.

2) Verify the correctness of u_{11F} and u_{11S}. If there is $u_{11F} = r_3$, it indicates that the information is a reply to the request which is sent by the reader just now. And if there is $u_{11S} = m$, it indicates that the information is a response to the authentication of the current tag identity.

3) The reader calculates $M_9 = K_{1R} \oplus (u_3||r_2)$ and sends it to the tag.

Step 6. The tag calculates $u_{12} = M_9 \oplus K_{1R}$. The value of u_{11} is divided into two parts, u_{12F} and u_{12S}. The tag compares u_{12F} with p, $u_{12F} \triangleq p$. If it is the same, the tag determines that the received information is a reply to the current query. Then the tag compares u_{12S} with r_2, $u_{12S} \triangleq r_2$. If it is the same, the authentication is successful. Otherwise, the authentication fails.

6 Security Analysis and Comparisons

6.1 Formal Proof

BAN logic uses knowledge and belief to describe and reason authentication protocol. It is a kind of modal logic reasoning rule, which can effectively prove the security of the protocols [7]. In this paper, the security of the protocol is proved by using BAN logic formal proof. The proof of BAN logic has four steps. Firstly, establish the idealized protocol model. Secondly, give a reasonable protocol initial assumption. Thirdly, give expected safety objectives of protocol. Finally, proof the security of the protocol according to reasoning rules.

For the convenience of proof, we make the following provisions. The database, mobile reader and tag are represented by DB, R and T respectively. $a \oplus b$ can be seen as $\{a\}_b$ or $\{b\}_a$. $Mvp(ID, a)$ can be seen as $\{ID\}_a$. The inference rules of BAN logic used in the proof are introduced as follows.

Message-meaning rule R1: $\frac{P|\equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$

Nonce-verification rule R2: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

Jurisdiction rule R3: $\frac{P|\equiv Q \Longrightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

Seeing rule R4: $\frac{P \lhd (X,Y)}{P \lhd X}$

Session-key rule R5: $\frac{P|\equiv \#(K), P|\equiv Q|\equiv X}{P|\equiv P \overset{K}{\leftrightarrow} Q}$, and X is a necessary factor of K.

1) An Idealized Protocol Model

Through analysis, the idealized model of the protocol can be expressed as follows.

$M\_1 : R \rightarrow T : (\{r_1\}_{K_1}, \{r_1\}_L)$

$M\_2 : T \rightarrow R : \{r_1\}_{K_1}, \{(m, r_2)\}_{K_1}, \{ID\}_{r_1}$

$M\_3 : R \rightarrow DB : \{r_3\}_{K_2}, \{ID_R\}_{K_2}, \{r_1\}_{r_3}, \{m\}_{r_1}, \{ID\}_{r_1}$

$M\_4 : DB \rightarrow R : \{(r_3, m)\}_{K_2}$

$M\_5 : R \rightarrow T : \{(r_1, r_2)\}_{K_1}$

2) Original Hypothesis

Initial assumptions of the protocol can be expressed as follows.

P1: $DB \mid\equiv DB \overset{K_2}{\leftrightarrow} R$. It means that DB believes DB and R use the shared key K_2 to communicate each other.

P2: $DB \mid\equiv \#(r_1)$. It means that DB believes r_1 is fresh.

P3: $DB \mid\equiv \#(r_3)$. It means that DB believes r_3 is fresh.

P4: $DB \mid\equiv \#(ID)$. It means that DB believes ID is fresh.

P5: $DB \mid\equiv R \Longrightarrow D$. It means that DB believes R has jurisdiction over ID.

P6: $R \mid\equiv T \mid\Longrightarrow r_1$. It means that R believes T has jurisdiction over r_1.

P7: $R \mid\equiv (\#r_1)$. It means that R believes r_1 is fresh.

P8: $R \mid\equiv T \overset{K_1}{\leftrightarrow} R, T \mid\equiv R \overset{K_1}{\leftrightarrow} T$. It means that R and T may use the shared key K_1 to communicate each other.

P9: $T \mid\equiv R \mid\Longrightarrow r_2$. It means that T believes R has jurisdiction over r_2.

P10: $T \mid\equiv (\#r_2)$. It means that T believes r_2 is fresh.

3) The expected safety objectives

G1: $DB \mid\equiv ID$. It means that DB believes ID is correct. That is to say, the tag identity authentication is successful.

G2: $R \mid\equiv r_1$. It means that R believes r_1 is correct. That is to say, the reader receives the legitimate data from the tag.

G3: $T \mid\equiv r_2$. It means that T believes r_2 is correct. That is to say, the tag receives the successful authentication responses from the reader.

4) Formal proof

With massage M_4, using seeing-key rule R4:$\frac{DB \lhd \{(r_3,m)\}_{K_2}}{DB \lhd \{r_3\}_{K_2}}$. With initial assumptions P1, using message-meaning rule R1: $\frac{DB \mid\equiv DB \overset{K_2}{\leftrightarrow} R, DB \lhd \{r_3\}_{K_2}}{DB \mid\equiv R \mid\sim r_3}$. With initial assumptions P3, using nonce-verification rule R2: $\frac{DB \mid\equiv \#(r_3), DB \mid\equiv R \mid\sim r_3}{DB \mid\equiv R \mid\equiv r_3}$. With initial assumptions P3, using session-key rule R5: $\frac{DB \mid\equiv \#(r_3), DB \mid\equiv R \mid\equiv r_3}{DB \mid\equiv DB \overset{r_3}{\leftrightarrow} R}$. With massage M_3, using message-meaning rule R1:$\frac{DB \mid\equiv DB \overset{r_3}{\leftrightarrow} R, DB \lhd \{r_1\}_{r_3}}{DB \mid\equiv R \mid\sim r_1}$. With initial assumptions P2, using nonce-verification rule R2:$\frac{DB \mid\equiv \#(r_1), DB \mid\equiv R \mid\sim r_1}{DB \mid\equiv R \mid\equiv r_1}$. With initial assumptions P2, using session-key rule R5:$\frac{DB \mid\equiv \#(r_1), DB \mid\equiv R \mid\equiv r_1}{DB \mid\equiv DB \overset{r_1}{\leftrightarrow} R}$. With massage M_3, using message-meaning rule R1: $\frac{DB \mid\equiv DB \overset{r_1}{\leftrightarrow} R, DB \lhd \{ID\}_{r_1}}{DB \mid\equiv R \mid\sim ID}$. With initial assumptions P4, using nonce-verification rule R2:$\frac{DB \mid\equiv \#(ID), DB \mid\equiv R \mid\sim ID}{DB \mid\equiv R \mid\equiv ID}$. With initial assumptions P5, using Jurisdiction rule R3:$\frac{DB \mid\equiv R \Longrightarrow ID, DB \mid\equiv R \mid\equiv ID}{DB \mid\equiv ID}$. we can obtain result $DB \mid\equiv ID$.

Using a similar method, we can obtain results $R \mid\equiv r_1, T \mid\equiv r_2$. All objectives are proved.

6.2 Security Analysis

1) Brute force attack. The attacker can acquire communication data via eavesdropping. Then it implements a brute force attack on the data stolen. Most information is encrypted using XOR operation based on the shared key. The key K_1 and K_2 are privacy keys, which are not disclosed to anyone. Even if the attacker gets M_1, M_2, M_3 and M_9, it is impossible to obtain any plaintext data because there is no K_1. Even if the attacker gets M_4, M_5 and M_8, it is impossible to obtain any plaintext data because there is no K_2. If M_6, M_7, IDS are obtained, the attacker cannot get plaintext data because of the lack of a random number r_1. M_6, M_7, IDS are encrypted by XOR operation. If a number has 128 bits, the guessed probability is 2^{128} which is very small. Based on the above analysis, the proposed protocol can prevent brute force attack.

2) Impersonation attack. The attacker can masquerade as the reader or the tag to pass legal authentication [13]. In the protocol, the attacker fakes the tag and sends M_2, M_3, IDS to the reader. After receiving the information, the reader first verifies the correctness of the number r_1 generated by itself. Since K_{1R} and r_1 are random numbers, the number M_2 sent by the attacker cannot be the same as the value of $K_{1R} \oplus r_1$. The attacker failed to fake the tag.

Later, the attacker fakes the reader and sends query signal and M_1 to the tag. The tag verifies the correctness of the number r_1 after receiving the query. The number r_1 is a random number, which is different in each session. The attacker cannot obtain the values of K_1 and L by analyzing the previous M_1. The attacker failed to fake the reader.

In the mobile RFID system, the attacker may impersonate the reader to send information to the database. The protocol requires the database to use dynamic authentication key K_{2L} to detect the reader identity ID_R. It can effectively prevent fake reader attack initiated by the attack.

Based on the above analysis, it is found that the proposed protocol can effectively resist impersonation attack.

3) Replay attack. The attacker collects data through listening channels, then it uses them to obtain legal identity authentication. In the protocol, the attacker acquires M_2, M_3, IDS, and sends them to the reader. When receiving the information, the reader first verifies the correctness of r_1. After that, the reader verifies r_2. Since r_1 and r_2 are random numbers, their values are different for each authentication. The attacker failed to replay the tag information.

In the mobile RFID system, the attacker may attempt to replay the reader request information IDS, M_4, M_5, M_6, M_7 to the database. The database first

calculates $u_7 = M_4 \oplus K_2$. Then it compares u_7 with the stored r_3 to determine whether the information is replayed. So, the protocol can resist replay attack.

4) Asynchronous attack.The encryption operation in the protocol is mainly based on the private keys $K_1, K_2, K_{1L}, K_{1R}, K_{2L}, K_{2R}$. The value of the keys K_1, K_2 are not update after each authentication. K_{iL}, K_{iR} are obtained by transforming K_i, where $i \in (1, 2)$. They are set up temporarily during the execution of the protocol. There will be no asynchronous update of the shared key. So, the protocol can resist asynchronous attack.

5) Forward security. If the secret key is exposed or leaked during current session, the attacker can predict the secrets of previously exchanged messages [14]. In the protocol, suppose that the attacker obtains the encrypted data M_1, M_4, M_6, M_7, IDS is the number by using XOR operation based on the random number, and M_2, M_3, M_5, M_8, M_9 are the numbers by using XOR operation based on the dynamic authentication key. The random number and the dynamic authentication key can prevent forward security attack.

6) Denial of service (Dos). The attacker overloads the reader by transmitting interference signals. The reader cannot respond to the request for the legitimate tag. In the protocol, when receiving the information, the reader first verifies the correctness of r_1. Since r_1 is a random number, it is different in each session. The reader can quickly determine whether the signal comes from a legitimate tag. The protocol can effectively resist denial of service attack.

6.3 Security Comparisons

The security comparison between the proposed protocol and the existing protocols is shown in Table 2. It is obvious that the proposed protocol has the best security performance compared with the existing protocols.

7 Complexity Performance Evaluation

Due to the strong computing power and large storage space of the database and the reader, the performance advantages of the protocol are mainly reflected in the storage complexity and computational complexity of the tag.

7.1 Storage Complexity

The storage complexity of the protocol is mainly reflected by storage performance of the tag. Considering the limited storage space of the tag, the tag storage overhead should be reduced when designing the protocol. Generally, the storage space is divided into basic storage space and temporary storage space. The basic storage space is set by the manufacturer when the tag is delivered. The temporary storage space is the additional space that the tag needs to temporarily allocate according to its own calculation.

We make the following assumptions, L_{ID} is the length of the tag identity, L_K is the length of the private key, L_F is the length of the encryption function, L_N is the length of the number, and L_{bit} is the length of the bitwise operation. Generally, the key and the number have the same length. They are also operation objects of bitwise operation. That is $L_N = L_K = L_{bit}$. The tag storage space comparison is shown in Table 3.

In Table 3, we find that the basic storage space of the tag in the proposed protocol is equivalent to that of Reference [20]. But with the authentication processing development, the temporary auxiliary storage space is significantly reduced. We observe that the tag total storage space of the proposed protocol is the smaller than other protocols listed in Table 3.

7.2 Computational Complexity

The database and mobile reader have strong computing power in mobile RFID system. The primary factor affecting the computational complexity of the protocol is the efficiency of tag operation. The paper evaluates the computational complexity of the protocol based on experiment of authenticating the legitimacy of tag identity. The experiment is done on the real scene.

Hardware and software environment configuration used in the experiment are as follows.

Upper computer configuration: Intel Core i7-11800H CPU @ 4.2GHZ, 512G Memory, Win10 OS, Visual Studio 2022 as a development environment, MYSQL database.

Hardware of the reader and the tag: Magic RF M100 reader, nRF24LE tag.

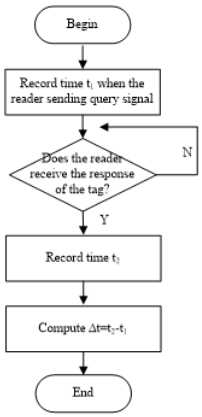

Figure 5: Design flow chart

The efficiency of tag operation is evaluated by the tag computing time. The length of tag identity is generally within 512 bits in EPC and ISO/IEC standard RFID system [10, 16]. Figure 5 shows the design flow chart of

Table 2: Comparison of security features

Protocol	Brute force attack	Impersonation attack	Replay attack	Asynchronous attack	Forward security	Denial of service
Reference [22]	N	Y	Y	N	N	Y
Reference [18]	Y	N	N	Y	Y	Y
Reference [12]	Y	N	Y	N	Y	Y
Reference [20]	N	Y	N	Y	N	N
Reference [8]	Y	Y	N	Y	Y	N
Proposed protocol	Y	Y	Y	Y	Y	Y

$Y: yes, N: no$

Table 3: Comparison of the tag storage space

Protocol	Basic storage space	Temporary storage space
Reference [22]	$2L_{ID}+L_K$	$L_F+5L_N+L_K$
Reference [18]	$L_{ID}+2L_K$	$2L_F+5L_N+L_K+L_{bit}$
Reference [12]	$L_{ID}+2L_K$	$2L_F+6L_{bit}$
Reference [20]	$L_{ID}+L_K$	$2L_F+L_N+4L_{bit}$
Reference [8]	$L_{ID}+L_K$	$2L_F+5L_N$
Proposed Protocol	$L_{ID}+L_K$	$L_F+2L_N+2L_{bit}$

obtaining the tag computing time. Figure 6 shows the experimental scene of tag authentication.

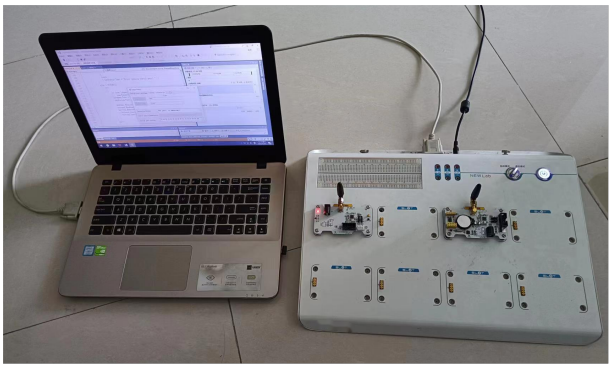

Figure 6: Experimental scene

In the upper computer, the application program is designed by C # language, which can record and display the computing time of the tag. It is shown in Figure 7 and Figure 8.

In References [22] and [8], the tag needs to perform hash function or symmetric encryption function with high complexity for many times. In References [12, 18, 20], the tag performs bitwise operation and bit operation function for many times. However, the proposed protocol only needs to perform one permutation and combination operation, as well as less bitwise operation and arithmetic operation.

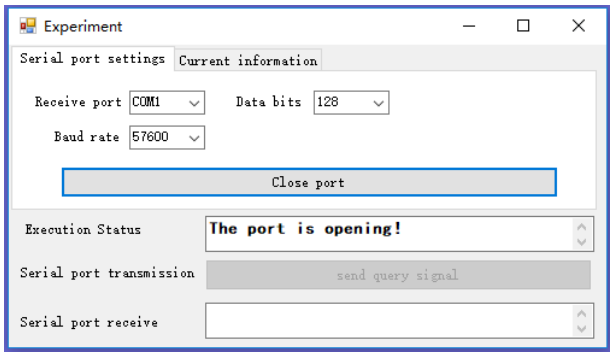

Figure 7: Serial port settings

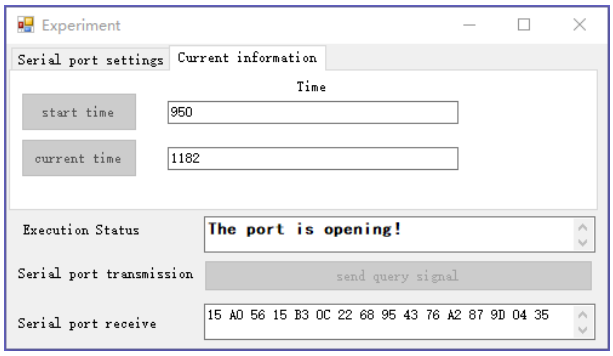

Figure 8: Current information

We assume that the results of all functions in each protocol have same length. Figure 9 shows a comparison of the tag computing time between the proposed protocol and other protocols. As the length of tag identity increases, the computing time of tag of the proposed protocol is significantly reduced.

Although the mobile reader has strong computing power, the low complexity operation of the reader has great value for mobile scenario applications of the protocol. For example, in the electronic toll collection (ETC) system, the low complexity operation of the reader can not only improve the detection efficiency of vehicles, but also prevent car collisions caused by slow detection.

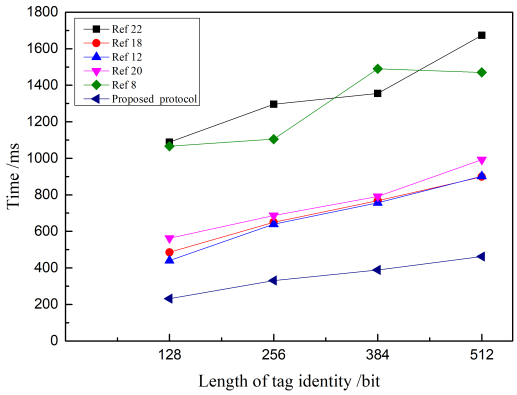

Figure 9: Comparison of tag computing time

In the experiment, we can record time t_0 when the authentication process begins. Record time t_1 when the reader sending query signal. Record time t_2 when the reader receiving the data from the tag. Record time t_3 when the reader sending the data to the database. Record time t_4 when the reader receiving the data from the database. Record time t_5 when the reader sending the data to the tag. Clearly, we can simply to calculate the result, $\Delta t_0 = t_1 - t_0$,$\Delta t_1 = t_3 - t_2$, $\Delta t_2 = t_5 - t_4$. The computing time of the reader is $\Delta t_0 + \Delta t_1 + \Delta t_2$.

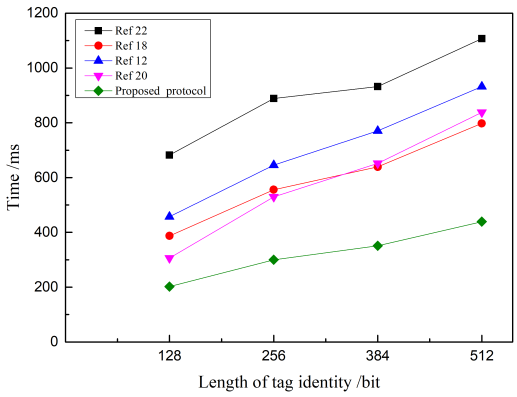

Figure 10: Comparison of reader computing time

References [8] doesn't participate in the comparative experiment, because the reader only performs forwarding operations. In References [22], the reader needs to perform hash function several times. In References [12, 18, 20], the reader performs bitwise operation and bit operation function for many times. In the proposed protocol, the reader uses XOR operation to transfer privacy data, which can reduce the computational complexity. Figure 10 shows a comparison of the reader computing time. As the length of tag identity increases, the computing time of reader of the proposed protocol is reduced significantly.

In summary, the computational complexity of the protocol has obvious advantages. The protocol is suitable for mobile RFID system.

8 Conclusion

In this paper, we have presented a lightweight security authentication protocol for mobile RFID. The tag performs the operation of arrangement and combination of column vectors based on column pseudonym to encrypt its identity. The protocol uses XOR operation to transfer privacy data based on the dynamic authentication keys. Meanwhile, it requires the receiver to verify the random number in time after receiving the information. Formal proof and analysis results show that the proposed protocol has good security and can resist various attacks. Furthermore, the proposed protocol has the low complexity, and it can be well used in the field of production and life.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61972438), Anhui Natural Science Foundation (2108085MF219), the Key Program of Universities Natural Science Research of the Anhui Provincial Department of Education (KJ2020A1112), Special Project of Science and Technology Development Center of the Ministry of Education of china (2021ALA04004).

References

[1] A. Abuzneid, S. A. Mellouki, Z. Siraj, et al., "Low-cost rfid authentication protocol based on elliptic curve algorithm," *International Journal of Interdisciplinary Telecommunications and Networking*, vol. 13, no. 2, pp. 1–11, 2021.

[2] M. B. Ahmad and F. A. Nababa, "The need of using a radio frequency identification system," *International Journal of New Computer Architectures and their Applications*, vol. 11, no. 2, pp. 22–29, 2021.

[3] H. L. Alaoui, A. E. Ghazi, M. Zbakh, et al., "A highly efficient ecc-based authentication protocol for rfid," *Journal of Sensors*, vol. 2021, no. 4, pp. 1–16, 2021.

[4] U. Ali, M. Y. I. B. Idris, M. N. B. Ayub, et al., "Rfid authentication scheme based on hyperelliptic curve signcryption," *IEEE Access*, vol. 9, pp. 49942–49959, 2021.

[5] S. Anandhi, R. Anitha, and V. Sureshkumar, "An authentication protocol to track an object with multiple rfid tags using cloud computing environment," *Wireless Personal Communications*, vol. 113, no. 2, pp. 2339–2361, 2020.

[6] A. Arslan, S. A. Colak, and S. Erturk, "A secure and privacy friendly ecc based rfid authentication

protocol for practical applications," *Wireless Personal Communications*, vol. 120, no. 4, pp. 2653–2691, 2021.

[7] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[8] V. Chegeni, H. Javadi, M. Goudarzi, et al., "Providing a hybrid cryptography algorithm for lightweight authentication protocol in rfid with urban traffic usage case," *The ISC International Journal of Information Security*, vol. 13, no. 1, pp. 73–85, 2021.

[9] N. Dinarvand and H. Barati, "An efficient and secure rfid authentication protocol using elliptic curve cryptography," *Wireless Networks*, vol. 25, no. 1, pp. 415–428, 2019.

[10] B. Fatemeh and C. K. Nemai, "Hybrid chipless rfid tags-a pathway to epc global standard," *IEEE Access*, vol. 6, pp. 67415–67426, 2018.

[11] T. F. Lee, K. W. Lin, Y. P. Hsieh, et al., "Lightweight cloud computing-based rfid authentication protocols using puf for e-healthcare systems," *IEEE Sensors Journal*, vol. 23, no. 6, pp. 6338–6349, 2023.

[12] D. W. Liu, S. H. Xu, and W. T. Zuo, "A mobile rfid authentication protocol based on self-assembling cross-bit algorithm," *International Journal of Network Security*, vol. 24, no. 5, pp. 975–983, 2022.

[13] M. Mehrabani and S. Sadegha, "Security analysis and improvement of wei-chi ku and yi-han chen's rfid protocol," *International Journal of Innovation in Engineering*, vol. 1, no. 2, pp. 73–83, 2021.

[14] M. Naeem, S. A. Chaudhry, K. Mahmood, et al., "A scalable and secure rfid mutual authentication protocol using ecc for internet of things," *International Journal of Communication Systems*, vol. 33, no. 7, pp. 1–13, 2019.

[15] I. Sarah, B. Mustapha, and D. Karim, "An enhanced scalable and secure rfid authentication protocol for wban within an iot environment," *Journal of information security and applications*, vol. 58, no. 86, pp. 1–15, 2021.

[16] G. Saxl, M. Ferdik, M. Fischer, et al., "Uhf rfid prototyping platform for iso 29167 decryption based on an sdr," *Sensors*, vol. 19, no. 10, pp. 1–12, 2019.

[17] M. Shariq, K. Singh, M. Y. Bajuri, et al., "A secure and reliable rfid authentication protocol using digital schnorr cryptosystem for iot-enabled healthcare in covid-19 scenario," *Sustainable Cities Society*, vol. 75, pp. 1–13, 2021.

[18] G. F. Shen, S. M. Gu, and D. W. Liu, "An anti-counterfeit complete rfid tag grouping proof generation protocol," *International Journal of Network Security*, vol. 21, no. 6, pp. 889–896, 2019.

[19] J. Su, Z. Sheng, and A. X. Liu, "Capture-aware identification of mobile rfid tags with unreliable channels," *IEEE Transactions on Mobile Computing*, vol. 14, no. 8, pp. 1182–1195, 2020.

[20] A. Tewari and B. B. Gupta, "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," *International Journal on Semantic Web and Information Systems*, vol. 16, no. 3, pp. 20–34, 2020.

[21] G. H. Wei, Y. L. Qin, and W. Fu, "An improved security authentication protocol for lightweight rfid based on ecc," *Journal of Sensors*, vol. 2022, pp. 1–6, 2022.

[22] Y. Xu and J. S. Yuan, "Design and analysis of an id-updated mutual authentication protocol for mobile rfid system," *Photonic Network Communications*, vol. 37, no. 2, pp. 204–211, 2019.

[23] Z. G. Zhao, "A secure rfid authentication protocol for healthcare environments using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, pp. 46–47, 2014.

Biography

Tao Pan was born in 1986. He is a lecturer at Anhui Technical College of Mechanical and Electrical Engineering. His major research interests include RFID technology and information security.

Kai-Zhong Zuo was born in 1974. He received his Ph.D. from Shanghai University. He is currently a professor and a supervisor of Master's student at Anhui Normal University. His major research interests include data security and privacy preservation.

Tao-Chun Wang was born in 1979. He received his Ph.D. from Nanjing University of Aeronautics. He is currently a professor and doctoral tutor at Anhui Normal University. His major research interests include sensor technology and crowd sensing.

Chun-Hong Deng was born in 1970. He is currently a professor at Anhui Technical College of Mechanical and Electrical Engineering. His major research interests include internet of things.