A Mobile RFID Authentication Protocol Based on Self-assembling Cross-bit Algorithm

Dao-Wei Liu[1], Sheng-Hua Xu[2], and Wen-Tao Zuo[1]
(Corresponding authors: Dao-Wei Liu)
Engineering College, Guangzhou College of Technology and Business[1]
Guangzhou 510006, China
Email: 995565519@qq.com
Network Information Center, Guangdong Polytechnic Normal University[2]
(Received Dec. 8, 2021; Revised and Accepted June 11, 2022; First Online July 3, 2022)

Abstract

The wired communication between the fixed reader and database in traditional RFID systems is considered a safe channel. However, the mobile reader and the database communicate wirelessly in mobile RFID systems, so the channel is no longer safe and reliable. Therefore, the traditional RFID authentication protocol cannot be applied to mobile RFID systems. An ultra-lightweight mobile-wireless bidirectional authentication protocol MAP-SKBO based on a shared private key and bitwise operation, is proposed to solve this problem. MAP-SKBO is based on the bitwise operation mechanism, which adopts ultra-lightweight bit replacement and self-combined cross-bit operation to encrypt the transmitted information and uses random numbers to maintain the transmission information's freshness and the shared information private key. During the communication process, the tag, the reader, and the database authenticate each other to resist sabotage by an attacker. Security analysis shows that MAP-SKBO can achieve tasks such as the dynamic update of the shared private key and desynchronization-attack resistance. The formal mathematical reasoning of MAP-SKBO by GNY logic proves the correctness of MAP-SKBO. A performance analysis indicates that MAP-SKBO has low computational complexity and is suitable for low-cost mobile RFID systems.

Keywords: Internet of Things; Mutual Authentication; RFID; Sac; Shared Key

1 Introduction

Radio frequency identification (RFID) is a non-physical contact using object recognition and data exchange technology. RFID arose in the last century, and large-scale applications were implemented in the late nineties [3, 15].

Current RFID systems typically consist of three parts, the tag, the reader and the database. In a traditional RFID system, the reader is generally fixed, so the communication between the reader and the database is based on a wired channel, which is considered to be safe [10, 18]. The reader is embedded in a mobile intelligent terminal to form a mobile RFID system. In a mobile RFID system, the reader is no longer fixed but mobile. Therefore, information transmission between the reader and the database can only be accomplished wirelessly. A wireless channel can easily be eavesdropped by attackers, which makes information transmission between the reader and database unreliable [8, 16].

Based on the above description, the traditional RFID authentication protocol is clearly not suitable for mobile RFID systems. In view of these problems, this paper proposes a two-way authentication protocol MAP-SKBO based on shared private key and bitwise operation in a mobile RFID system. MAP-SKBO applies ultra-lightweight bit replacement and self-combination of cross-bit operation to encrypt the transmitted information, thereby reducing the calculations on the tag side. Each round of the authentication process uses random numbers to maintain the freshness of the communication information and then updates the shared private key's freshness after the authentication process. During the communication process, the authenticity of the side that sends the message is verified first; then, the response information is verified to realize authentication among the three parties of the tag, the reader and the database.

The first section of this article provides an introduction to describe the limitations of the traditional RFID authentication protocol and the security flaws in mobile RFID systems, leading to the focus of this paper. The second section introduces the authentication protocol proposed in recent years for mobile RFID systems. The third section introduces the mathematical knowledge and defines the computational symbols required in the MAP-SKBO design process. The fourth section establishes a security model for the authentication protocol applicable to mobile RFID systems and gives an abstract descrip-

tion of the authentication protocol. The fifth section systematically describes the MAP-SKBO design steps. The sixth section analyzes the security of MAP-SKBO with respect to identity authentication, desynchronization attacks, track attacks and replay attacks. The seventh section adopts the formal logic of GNY to perform rigorous mathematical reasoning for MAP-SKBO. The eighth section analyzes the performance of MAP-SKBO in terms of the computational complexity, storage capacity, etc. of the tag, the reader and the database. The ninth section summarizes the full text and provides directions for future research.

2 Related Research Works

Reference [13] proposes an RFID one-way authentication protocol based on PRF, but the analysis finds that the protocol cannot completely resist denial-of-service (DoS) attacks. If an attacker constantly sends a message c to the tag, the tag continually updates the value of its own counter ctr, causing the reader to spend more time traversing the query. Reference [11] proposes a PFP protocol based on a hash function and pseudo-random generator, but the protocol has some drawbacks. If the internal state chain length w is too small, it cannot resist DoS attacks. If the value of w is too large, the reader will pay a large cost to calculate the internal state chain. The authentication scheme proposed in Reference [19] cannot resist desynchronization attacks. The attacker makes the shared private key stored between the tag and the reader inconsistent by means of replay attack and information forging and then destroys the subsequent authentication between the tag and the reader. The authentication scheme proposed in Reference [4] cannot resist active attack. An attacker can gradually derive the private key stored in the tag by continuously interrogating the tag and analyzing the reply information of the tag. Although the scheme proposed in Reference [9] is resistant to common attacks, the tag side needs to generate five random numbers during the authentication process, which makes the computational complexity of the tag excessive. All the above authentication protocols have a common feature that they are designed for traditional RFID systems. However, they are not applicable to mobile RFID systems.

Reference [17] proposes a one-way mobile authentication protocol but found that the agreement cannot resist man-in-the-middle attacks and replay attacks. A mobile authentication protocol based on elliptic curve is proposed in Reference [7]; however, this scheme cannot ensure the privacy of the reader and the computational complexity of the tag is also high. An ultra-lightweight mobile authentication protocol is proposed in Reference [2]. The analysis shows that the protocol cannot resist replay attacks on the tag. The mobile authentication protocol proposed in Reference [12], which is based on a hash function, cannot prevent tag forgery, man-in-the-middle attacks and replay attacks. Reference [6] proposes a tripartite authentication of the mobile protocol. However, the protocol burdens the database with a heavy workload and also cannot resist DoS attacks. The Edwards curve-based mobile protocol proposed in Reference [20] does not implement authentication from the reader side to the tag in the authentication process, which makes the protocol vulnerable to impersonation attack. Reference [14] proposes a mobile authentication protocol based on a shared private key. However, the protocol, in which the tag authenticates the reader, does not achieve full authentication, which makes the protocol vulnerable to impersonation attacks.

Considering the shortcomings of many existing schemes, this paper proposes a mobile authentication system, MAP-SKBO, based on shared private key and bitwise operation for a mobile RFID system. The MAP-SKBO authentication process involves first verifying the authenticity of the message source and then conducting follow-up operations, which can resist the deliberate destruction of the attacker. Encrypting information by bitwise operation enables MAP-SKBO to achieve an ultra-lightweight level, which can effectively reduce the computational load of the RFID system. From the perspective of safety and performance, MAP-SKBO is suitable for low-cost mobile RFID systems.

3 Related Knowledge

To facilitate the description, we use "Sac(Z)" to represent self-assembling cross-bit operation. Let X, Y, and Zbe three binary numbers of l bits, $X = x_1x_2\cdots x_L$, $Y = y_1y_2\cdots y_L$, and $Z = z_1z_2\cdots z_L$, where $X \in \{0,1\}^l$, $Y \in \{0,1\}^l$, $Z \in \{0,1\}^l$. X undergoes bitwise XOR with Y to obtain Z. $Sac(Z)$ is a new binary number W with l bits formed by the combination of the high and low bits of Z, that is, $Sac(Z) = z_1z_L/2 + 1z_2z_L/2 + 2\cdots z_L/2z_L$.

The self-assembling cross-bit operation can be implemented in the tag and reader as described below. Introduce two pointers, one for P_1 and one for P_2, where P_1 points to the head of binary number Z and P_2 points to the end of binary number Z. When P_1 traverses from the head of Z, P_2 simultaneously starts traversing from the end of Z. The numbers traversed by pointer P_1 are sequentially placed in the odd bits of the new binary number W, and the numbers traversed by pointer P_2 are sequentially placed in the even bits of the new binary number W. Finally, through combination we can obtain the new binary number W, that is, $Sac(Z)$ [5].

The self-assembling cross-bit operation requires only shift and bitwise OR operation and the final combination, thereby reducing system throughput and storage capacity to achieve an ultra-lightweight level. Different orders of pointer assignment will produce different values, thereby increasing the difficulty of cracking. For example, if $l = 8$, $X = 11011001$ and $Y = 01100101$, then $X \oplus Y = Z$ and $Sac(Z) = 11011010$. The specific process is shown in Figure 1.

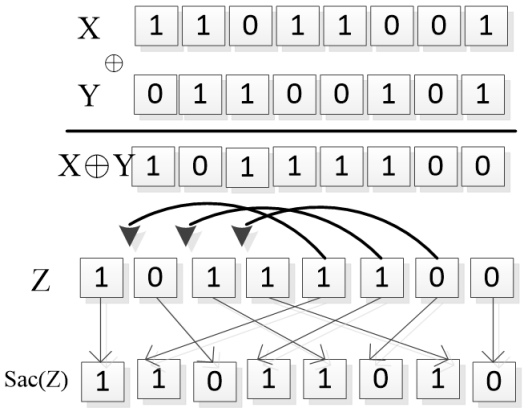

Figure 1: Self-assembling cross-bit operation flow chart

4 RFID Security Model

The goal of a mobile RFID authentication protocol is not only to ensure the safety of the tag's private information but also to ensure that both the tag and the mobile reader cannot be tracked. This paper uses MySQL query mode to model the attack ability of Attacker-A while establishing the non-traceable model of a mobile RFID system. T represents the tag, R represents the reader, DB represents the database, and P represents the protocol that the tag, the mobile reader, the database are involved in. The participants in the protocol can initiate several instances of P, where M_T represents the instance initiated by the tag, M_R represents the instance initiated by the mobile reader, and M_{DB} represents the instance initiated by the database. Attacker-A can perform the following query operation:

1) Execute (M_T, M_R, M_{DB}, n) Query Operation: This query operation describes an instance where Attacker-A executes protocol P. Simultaneously, all the two-way transferring communication information between tag T and mobile reader R or between mobile reader R and database DB is acquired during the n-th round of communication. The query operation modeling is equivalent to a static attack.

2) Send $(M_T, message, n)$ Query Operation: In this query operation, Attacker-A sends a message to tag T during the n-th round of communication, and the query operation is modeled as a dynamic attack. Through this query operation, tag T will return a value as a response message based on the protocol and the stored data.

3) Send $(M_R, message, n)$ Query Operation: In this query operation, Attacker-A sends a message to mobile reader R during the n-th round of communication, and the query operation modeling is equivalent to a dynamic attack. Through this inquiry operation, mobile reader R will return a value as a response message according to the protocol and the stored data.

4) Corrupt (M_T) Query Operation: This query operation describes the ability of Attacker-A to bribe tag T so that T will actively leak the private information stored by itself. This query operation modeling is equivalent to a dynamic attack.

5) Corrupt (M_R) Query Operation: The query operation describes the ability of Attacker-A to buy a mobile reader R so that R will actively leak the private information stored by itself. The query operation modeling corresponds to a dynamic attack.

5 Design of MAP-SKBO

5.1 Initinal Conditions and Symbols

Before MAP-SKBO is executed, all entities in the mobile RFID system must initialize the memory unit as follows.

The tag stores Key_L, Key_R and ID_T, forming the triple (Key_L, Key_R, ID_T). The mobile reader stores Key_L, Key_R and ID_R to form the triple (Key_L, Key_R, ID_R). The database stores Key_L, Key_R, ID_T and ID_R to form the four-tuple $(Key\_L, Key\_R, ID_T, ID_R)$. The definitions and descriptions of the symbols used in MAP-SKBO are shown in Table 1.

Table 1: Symbol definitions

Symbol	Description
T	The tag
R	The mobile reader
DB	The database
ID_T	Identifier ID of the tag
ID_R	Identifier ID of the reader
Key	The private key shared among the reader, the tag and the database
Key_L	The left half of the shared private key
Key_R	The right half of the shared private key
Key_old	The shared private key of the last round of authentication
Key_new	The shared private key of the current round of authentication
r_T	The random number generated by the tag
r_R	The random number generated by the reader
r_{DB}	The random number generated by the database
$\oplus$	Bitwise XOR operation
&	Bitwise AND operation
$Sac(X)$	Self-combined cross-bit operation

5.2 MAP-SKBO Authentication Process

The MAP-SKBO authentication process is shown in Figure 2. The following gives a description of the specific meanings of formulas M0 to M12 in Figure 2, as shown in Table 2. Then, in combination with Figure 2, a description of the specific steps of the MAP-SKBO authentication is given.

Table 2: Formula descriptions

Symbol	Description
M0	$r_R \oplus Key\_R$
M1	$r_R \oplus Key\_L$
M2	$r_R \oplus r_T$
M3	$r_T \oplus ID_T$
M4	$Sac(r_T \& Key\_L, r_T \oplus Key\_R)$
M5	$Sac((r_T \& r_R) \oplus (r_T \& Key\_L))$
M6	$r_R \oplus ID_R$
M7	$Sac(r_R \& ID_R \& Key\_L, r_R \& ID_R \& Key\_R)$
M8	$r_R \oplus r_{DB} \oplus ID_R$
M9	$r_T \oplus r_{DB} \oplus ID_T$
M10	$Sac(r_R, r_{DB})$
M11	$Sac(r_T, r_{DB})$
M12	$r_R \& r_{DB}$

The MAP-SKBO authentication process is shown in Figure 2.

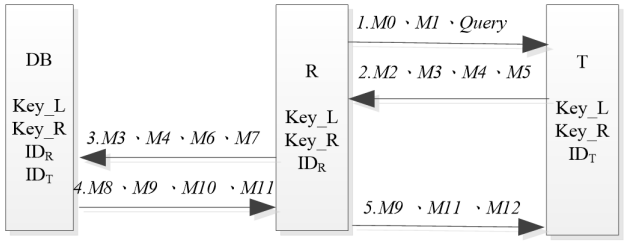

Figure 2: MAP-SKBO authentication flow chart

The detailed steps of the MAP-SKBO authentication process are as follows.

Step 1. The mobile reader generates a random number $r_R \in 0,1^l$; then, the reader calculates the values of M0 and M1 and sends M0, M1 and the authentication request command query to the tag.

Step 2. After the tag receives the information, the values of $M0 \oplus Key\_R$ and $M1 \oplus Key\_L$ are calculated and compared to determine if they are the same.

If they are equal, the tag verifies that the mobile reader has passed and proceeds to step three; otherwise, the tag indicates that the mobile reader is forged and MAP-SKBO terminates immediately.

Step 3. The tag calculates random number r_R and generates a random number $r_T \in 0,1^l$. Then, the tag calculates M2, M3, M4, and M5 and transmits (M2, M3, M4, M5) to the mobile reader.

Step 4. After the mobile reader receives the message, it first calculates the values of $M2 \oplus r_R$ and M5' and determines whether the values of M5' and M5 are equal. If they are equal, then the mobile reader verifies that the tag has passed and proceeds to Step 5; otherwise, the reader indicates that the tag is forged and MAP-SKBO terminates immediately, where $M5' = Sac(((M2 \oplus r_R) \& r_R) \oplus ((M2 \oplus r_R) \& Key\_L))$.

Step 5. The mobile reader calculates random number r_T and the values of M6 and M7 and transmits (M3, M4, M6 and M7) to the database.

Step 6. The database authenticates the mobile reader.

1) After the database receives the information, it first calculates the values of $M6 \oplus ID_R$ and M7‘ and determines whether the values of M7‘ and M7 are equal. If they are equal, the database verifies that the mobile reader has passed and proceeds to Step 3; otherwise, the process proceeds to Step 2, where $M7' = Sac((M6 \oplus ID_R) \& ID_R \& Key\_L, (M6 \oplus ID_R) \& ID_R \& Key\_R)$.
2) The database uses Key_old instead of Key_new to perform the calculation in Step 1. If they are equal, the database verifies that the reader has passed and goes to Step 3; otherwise, the mobile reader is forged and MAP-SKBO terminates immediately.
3) The database calculates random number r_R and goes to the seventh step.

Step 7. The database authenticates the tag.

1) After the database verifies that the mobile reader has passed, it calculates the values of $M3 \oplus ID_T$ and M4‘ and determines whether M4 ’ and M4 are equal. If they are equal, the database verifies that the tag has passed and Step 3 is performed; otherwise, Step 2 is performed, where $M4' = Sac((M3 \oplus ID_T) \& Key\_L, (M3 \oplus ID_T) \oplus Key\_R)$.
2) The database uses Key_old instead of Key_new to perform the calculation in Step 1. If they are equal, then the database verifies that the tag has passed and goes to Step 3; otherwise, the tag is forged and MAP-SKBO terminates immediately.
3) The database calculates random number r_T and proceeds to the eighth step.

Step 8. The database generates a random number $r_{DB} \in 0,1^l$, calculates the values of M8, M9,

M10 and M11, starts to update the information of the shared private key, that is, Key_old=Key and Key=Key_new, and transmits (M8, M9, M10, M11) to the mobile reader, where $Key\_new = Sac((r_{DB} \oplus r_T \oplus r_R) \oplus (r_{DB}\&r_T\&r_R))$.

Step 9. After the mobile reader receives the message, it calculates the values of $M8 \oplus r_R \oplus ID_R$ and M10‘ and compares the values of M10‘ with M10. If they are equal, the mobile reader verifies that the database is authentic and proceeds to Step 10; otherwise, it indicates that the database is forged and MAP-SKBO terminates immediately, where $M10‘ = Sac(r_R, (M8 \oplus r_R \oplus ID_R))$.

Step 10. The mobile reader calculates the value of M12, updates the information of the shared private key, that is, Key_old=Key and Key=Key_new, and transmits (M9, M11, M12) to the tag, where $Key\_new = Sac((r_{DB} \oplus r_T \oplus r_R) \oplus (r_{DB}\&r_T\&r_R))$.

Step 11. The tag authenticates the mobile reader.

1) After the tag receives the information, the tag calculates the values of $M9 \oplus r_T \oplus ID_T$ and M12‘ and compares M12‘ with M12 for equality. If they are equal, then the tag verifies the mobile reader and proceeds to Step 2; otherwise, it indicates that the mobile reader is forged and MAP-SKBO terminates immediately, where $M12‘ = r_R\&(M9 \oplus r_T \oplus ID_T)$. The tag authenticates the database.
2) The tag calculates the value of M11‘ and determines whether M11‘ and M11 are equal. If they are equal, then the tag verifies the database and proceeds to Step 3; otherwise, it indicates that the database is forged and MAP-SKBO immediately terminates, where $M11‘ = Sac(r_T, (M9 \oplus r_T \oplus ID_T))$.
3) The tag starts to update the information of the shared private key, that is, $Key = Sac((r_{DB} \oplus r_T \oplus r_R) \oplus (r_{DB}\&r_T\&r_R))$. The authentication process among the tag, the mobile reader and the database terminates.

6 Safety

1) Replay Attack: The tag generates a random number r_T in each authentication process, and the authentication message (M2, M3, M4, M5) contains r_T in each calculation. If the attacker adopts the old message, the tag will use the newly generated random number r_T when verifying the authentication message (M9, M11, M12). This will cause the tag to fail when validating the mobile reader and the database, and the MAP-SKBO will terminate immediately, preventing attackers from completing the follow-up authentication process. Therefore, MAP-SKBO can resist replay attacks.
2) Asynchronous Attack: In an asynchronous attack, during the authentication process, due to the deliberate sabotage of the attacker, the shared private key of the mobile reader (or the database) and the tag becomes asynchronous. An asynchronous attack is also known as a desynchronization attack. To resist asynchronous attacks, MAP-SKBO stores the shared private key, Key_old, used in the previous authentication process to recover synchronization with the tag. When the database authenticates the tag and the mobile reader through (M3, M4, M6, M7), it first calls Key_new. If the verification fails, Key_old is called to resist the attacker's desynchronization attack. Therefore, the existence of Key_new and Key_old makes MAP-SKBO resistant to asynchronous attacks.
3) Man-in-the-middle Attack: Replacing the message and tampering with the news are the most common forms of man-in-the-middle attacks. According to the protocol application scenario, an attacker can obtain all communication message sets of the tag, the mobile reader and the database among all three MS=M0, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12. Because the above message is encrypted, even if the attacker acquires the above message, he cannot derive any useful information from it. Although an attacker can modify or tamper with one of the messages, MAP-SKBO will verify the message at each step and find that the message has been tampered with. Meanwhile, the calculation of the above messages is associated with random numbers r_R, r_T and r_{DB}, and the random numbers are randomly generated and unpredictable, making it harder for an attacker to modify the message. Thus, MAP-SKBO can resist man-in-the-middle attacks.
4) Forward Security: Due to the database storing the shared private key of the previous round of the authentication process, here only the forward security of the tag is discussed. If the attacker wants to obtain the current shared private key value of the tag, the attacker needs to decrypt the previous authentication message from the last received message. However, the attacker cannot succeed for the following reasons. First, the attacker cannot crack the message encrypted by the bitwise operation because at least two quantities in the ciphertext are unknown to the attacker. Second, after the authentication, MAP-SKBO immediately updates the value of the shared private key, and there is no correlation between the initial and updated values. Furthermore, the calculation of the value is dependent on three random numbers r_R, r_T and r_{DB}, which are impossible for the attacker to obtain. Therefore, MAP-SKBO can ensure the forward safety of the tag.
5) Bidirectional Authentication: In the mobile RFID system, because the communication between the

tag and the reader or between the reader and the database is performed through a wireless channel, which is not secure, each message transmission requires authentication.

The tag authenticates the reader. The reader sends the message to the tag for the first time, and the tag completes the first authentication of the reader in the second step. In the tenth step, the reader transmits a message to the tag a second time, and the tag completes the second authentication of the reader in the eleventh step. The reader authenticates the tag. The tag sends a message to the reader in the third step, and the reader completes the authenticity verification of the tag in the fourth step.

The reader authenticates the database. The database transmits the message to the reader in the eighth step, and the reader completes the authenticity verification of the database in the ninth step.

The database authenticates the reader and the tag. To ensure resistance to desynchronized attacks, the database simultaneously stores the values of Key_new and Key_old. In the fifth step, after the reader sends the message to the database, the database authenticates the reader in the sixth step and authenticates the tag in the seventh step. Through these processes, the tag, the reader, and the database can achieve mutual authentication, so MAP-SKBO can achieve bidirectional authentication.

7 GNY Logical Formal Proof

In this paper, the formal analysis and proof of the WKGA-BO protocol are performed by using GNY [1] formal logic analysis.

1) Formal Description of the Protocol: The following conventions are used to simplify the application of the GNY formal logic language description to the MAP-SKBO. R represents the mobile reader, T represents the tag, and DB represents the database. The flow of the MAP-SKBO protocol is as follows:

Msg1: $R \rightarrow T : \{M0, M1, Query\}$

Msg2: $T \rightarrow R : \{M2, M3, M4, M5\}$

Msg3: $R \rightarrow DB : \{M3, M4, M6, M7\}$

Msg4: $DB \rightarrow R : \{M8, M9, M10, M11\}$

Msg5: $R \rightarrow T : \{M9, M11, M12\}$

After using GNY formal logic language to standardize the above protocol, the process can be described as follows:

Msg1: $T < *\{M0, M1, Query\}$

Msg2: $R < *\{M2, M3, M4, M5\}$

Msg3: $DB < *\{M3, M4, M6, M7\}$

Msg4: $R < *\{M8, M9, M10, M11\}$

Msg5: $T < *\{M9, M11, M12\}$

2) The Initalization Assumption of the Protocol: The MAP-SKBO protocol assumptions are as follows: the combination of R, DB, T represent the body, where R represents the mobile reader, T represents the tag, and DB represents the database.

Sup1: $T \ni (Key\_R, Key\_L, ID_T r_T)$

Sup2: $R \ni (Key\_R, Key\_L, ID_R, r_R)$

Sup3: $DB \ni (Key\_R, Key\_L, ID_R, ID_T, r_{DB})$

Sup4: $R| \equiv \#(r_R, r_T, r_{DB})$

Sup5: $T| \equiv \#(r_R, r_T, r_{DB})$

Sup6: $DB| \equiv \#(r_R, r_T, r_{DB})$

Sup7: $T \models R \overset{Key\_R, Key\_L}{\longleftrightarrow} T$

Sup8: $R \models T \overset{Key\_R, Key\_L}{\longleftrightarrow} R$

Sup9: $DB \models R \overset{Key\_R, Key\_L, ID_R}{\longleftrightarrow} DB$

Sup10: $R \models DB \overset{Key\_R, Key\_L, ID_R}{\longleftrightarrow} R$

Sup11: $DB \models T \overset{Key\_R, Key\_L, ID_T}{\longleftrightarrow} DB$

Sup12: $T \models DB \overset{Key\_R, Key\_L, ID_T}{\longleftrightarrow} T$

3) The Proof Target of the Protocol: There are five main proof targets of the MAP-SKBO protocol, namely, mutual trust of the freshness of the information exchanged among the tag, the mobile reader and the database. The proof formulas of the target are as follow:

Goal1: $T \models R| \sim \#(M0, M1)$

Goal2: $R \models T \sim \#(M2, M3, M4, M5)$

Goal3: $DB \models R| \sim \#(M3, M4, M6, M7)$

Goal4: $R \models DB| \sim \#(M8, M9, M10, M11)$

Goal5: $T \models R| \sim \#(M9, M11, M12)$

4) The Protocol Proving Process: The proof of the MAP-SKBO protocol is based on the initialization hypothesis, which proves that the process follows the rules of logical reasoning in Reference [1], and the notification rules, fresh rules, procession rule and the rules of message interpretation follow the GNY logic inference rules in Reference [1], which are, respectively, represented as T, P, F and I.

Because the protocol proves that the processes of proving Goal 2: $R \mid\equiv T| \sim \#(M2, M3, M4, M5)$, Goal 3: $DB \mid\equiv R| \sim \#(M3, M4, M6, M7)$, Goal 4: $R \mid\equiv DB \sim \#(M8, M9, M10, M11)$, Goal 5: $T \mid\equiv R| \sim \#(M9, M11, M12)$ are similar to the proof process of Goal 1: $T \mid\equiv R| \sim \#(M0, M1)$, this section proves only Goal 1: $T \mid\equiv R| \sim \#(M0, M1)$ as an example. The proof process is given below.

Proof.
$\because$ Rule P_1: $\frac{P<X}{P \ni X}$ and Msg 1: $T < *\{M0, M1\}$,
$\therefore T \ni \{M0, M1\}$.

$\because$ Rule: F1: $\frac{P \ddagger (X)}{P \ddagger (x,y), P \ddagger \#F(X)}$ and Sup 4: $R \mid \equiv \#(r_R, r_T, r_{DB})$,

$\therefore T = \#\{M0, M1\}$.

$\because$ Rule P_2: Sup 1: $T \ni (Key\_R, Key\_L, ID_T, r_T)$ and Sup 2: $R \ni (Key\_R, Key\_L, ID_R, r_R)$,

$\therefore T \ni \{M0, M1\}$.

$\because$ Rule F10: $\frac{P \ddagger (X), P \ni X}{P \ddagger \#(H(X))}$ and the formula derived: $T = \#\{M0, M1\}$, $T \ni \{M0, M1\}$,

$\therefore T \models \#\{M0, M1\}$.

$\because$ Rule I3: $\frac{P \ddagger H(X, <S>) >, P \ni (X,S), P \ddagger P \longleftrightarrow Q, P \ddagger \#(X,S)}{P \ddagger Q \mid \sim (X,S), P \ddagger Q \sim H(X, <S>)}$

Then, $\because$ Sup 7: $T \mid \equiv R \overset{Key\_R, Key\_L}{\longleftrightarrow} T$, Sup 8: $R \mid \equiv T \overset{Key\_R, Key\_L}{\longleftrightarrow} R$ and Msg 1: $T < *\{M0, M1\}$,

$\therefore T \models R \sim \{M0, M1\}$.

$\because$ freshness definition and its derivation: $T = \#\{M0, M1\}, T \models R \sim \{M0, M1\}$,

$\therefore$ Goal 1: $T \mid \equiv R \mid \sim \#(M0, M1)$ has been proved. □

8 Performance Analysis

A mobile RFID system includes a tag, mobile reader, and database. Because the latter two have strong computing power and large storage capacity, they have little effect on the performance of the protocol. Therefore, the computation power and storage capacity of only the tag are analyzed. The performance analysis of the RFID authentication protocol is conducted from four main perspectives: the computational load of the tag, the storage of the tag, the number of conversations, and protocol traffic. Table 3 shows the performance comparison results of MAP-SKBO and other authentication protocols.

In Table 3, H represents a hash function operation, M represents scalar multiplication, S represents a random number calculation, and Sac represents a combination of self-cross-bit operation. As described in the third section of the article, H, M and S are lightweight operations, whereas Sac is ultra-lightweight operations. That is, the former require much more computation than the latter. Because the bitwise XOR operation and bitwise AND operation require less computation, their computation is ignored in the performance analysis. The lengths of the shared private key Key, the identifier ID and the result of each operation (i.e., H, M, S, Sac) are set to l.

1) Storage and Computation Load of the Tag: In this paper, the MAP-SKBO tag needs to store only two values, the shared privates key Key and the identifier of the tag ID_T. According to the previous convention, the required storage capacity of the tag is 2l. Compared with the References [12, 17, 20], the storage capacity of the tag of this protocol is reduced; compared with the References [6, 7, 14], the storage capacity of the tag in this paper is equivalent.

Table 3: Performance comparison of authentication protocols

Reference	Computational Load	Storage Capacity	Protocol Traffic
Reference [17]	H	3l	10l
Reference [7]	4M+ H	2l	22l
Reference [12]	3H	3l	14l
Reference [6]	2H	2l	13l
Reference [20]	3M+2H	6l	17l
Reference [14]	3S+H	2l	12l
This protocol	S+4Sac	2l	17l

In terms of the computation load of the tag, the bitwise XOR operation and bitwise AND operation have small computational cost, so their costs are not considered. Therefore, the computational cost is much less than that of other studies. In this paper, we do not encrypt the message using a hash function or scalar multiplication, which are computationally intensive. Instead, we encrypt the message by ultra-lightweight bitwise operation to reduce the computational load. In summary, the protocol in this paper has some improvements compared to other protocols in terms of the storage and computational load of the tag.

2) Communication and the Number of Conversations: The communication traffic of this protocol is slightly larger than those in References [6,12,14,17], but there are some security risks in the previous protocols. The proposed protocol overcomes the defects of previous protocols. This protocol is equivalent to those in References [7, 20] in terms of communication traffic and solves their security problems.

The number of conversations in most of the protocols is five. The proposed protocol has no advantage in terms of the number of conversations. In summary, this protocol achieves little improvement with respect to overall communication traffic and the number of conversations but solves the security flaws in other protocols. Therefore, this protocol still has some practical value.

9 Conclusion

This paper describes the differences between traditional RFID systems and mobile RFID systems and notes that the traditional RFID system authentication protocol cannot be applied to mobile RFID systems. Therefore, an MAP-SKBO authentication protocol is proposed for mobile RFID systems. The paper expounds the defects and deficiencies in some current authentication protocols applicable to mobile RFID systems and then proposes an improved authentication scheme. The proposed MAP-

SKBO protocol abandons the hash function encryption method and instead uses bitwise operations to encrypt the information, making the protocol achieve an ultra-lightweight level. The use of bit replacement operations and self-combined cross-bit operations increases the difficulty of the attacker in cracking the protocol. A security analysis and performance analysis illustrate the security and advantages of the protocol. GNY logic formally proves the correctness of MAP-SKBO; MAP-SKBO is not only suitable for mobile RFID systems but also for traditional RFID systems. Future potential research directions include the following: Optimize the MAP-SKBO protocol to reasonably reduce the traffic of the whole communication; and implement a MAP-SKBO mobile RFID system prototype to determine the total number of gates, the time needed to achieve complete communication and other issues to achieve the combination of theory and practice.

Acknowledgments

This paper is supported by the 2021 Guangdong Education Science Planning Project (Special Project for Higher Education) (China) (2021GXJK).

References

[1] M. Burrows, M, Abadi, R. M. Needham, "A logic of authentication," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, pp. 233-271, 1989.

[2] Z. Cao and O. Markowitch, "Analysis of Shim's attacks against some certificateless signature schemes," *International Journal of Network Security*, vol. 23, no. 3, pp. pp. 545-548, 2021.

[3] S. Y. Chiou, "An efficient RFID authentication protocol using dynamic identity," *International Journal of Network Security*, vol. 21, no. 5, pp. 728-734, 2019.

[4] S. Y. Chiou, W. T. Ko, E. H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and its application," *International Journal of Network Security*, vol. 20, no. 2, pp. 396-402, 2018.

[5] J. F. Chong, Z. Zhuo. , "Constructions of balanced quaternary sequences of even length," *International Journal of Network Security*, vol. 22, no. 6, pp. 911-915, 2020.

[6] Y. P. Duan, "Lightweight RFID group tag generation protocol," *Control Engineering of China*, vol. 27, no. 4, pp. 751-757, 2020.

[7] K. Fan, W. Jiang, H. Li, *et al.*, "Lightweight RFID protocol for medical privacy protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656-1665, 2018.

[8] M. S. Hwang, E. F. Cahyadi, S. F. Chiou, C. Y. Yang. , "Reviews and analyses the privacy-protection system for multi-server," *Journal of Physics: Conference Series*, vol. 1237, pp. 022091, June 2019.

[9] K. Li and R. Huang, "A CKKS-based privacy preserving extreme learning machine," *International Journal of Network Security*, vol. 24, no. 1, pp. 166-175, 2022.

[10] D. W. Liu, J. Ling, "An improved RFID authentication protocol with backward privacy," *Computer Science*, vol. 43, no. 8, pp. 128-130, 2016.

[11] L. H. Liu and X. Y. Cao, "A note on one privacy-preserving centralized dynamic spectrum access system," *International Journal of Network Security*, vol. 23, no. 6, pp. 1074-1077, 2021.

[12] 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.

[13] S. Sundaresan, R. Doss, S. Piramuthu, *et al.*, "A secure search protocol for low cost passive RFID tags," *Computer Networks*, vol. 122, pp. 70-82, 2017.

[14] J. Q. Wang, Y. F. Zhang, D. W. Liu, "Provable secure for the ultra-lightweight RFID tag ownership transfer protocol in the context of IoT commerce," *International Journal of Network Security*, vol. 22, no. 1, pp. 12-23, 2020.

[15] Y. Wei, J. Chen, "Tripartite authentication protocol RFID/NFC based on ECC," *International Journal of Network Security*, vol. 22, no. 4, pp. 664-671, 2020.

[16] H. Xia and W. Yang, "ID-authentication based on PTPM and certificateless public-key cryptography in cloud," *International Journal of Network Security*, vol. 23, no. 6, pp. 952-961, 2021.

[17] R. Xie, B. Y. Jian, D. W. Liu, "An improved ownership transfer for RFID protocol," *International Journal of Network Security*, vol. 20, no. 1, pp. 149-156, 2018.

[18] R. Xie, J. Ling, D. W. Liu, "A wireless key generation algorithm for RFID system based on bit operation," *International Journal of Network Security*, vol. 20, no. 5, pp. 938-950, 2018.

[19] Y. Xue, "Research on network security intrusion detection with an extreme learning machine algorithm," *International Journal of Network Security*, vol. 24, no. 1, pp. 29-35, 2022.

[20] X. Zhao, "Attack-defense game model: research on dynamic defense mechanism of network security," *International Journal of Network Security*, vol. 22, no. 6, pp. 1037-1042, 2020.

Biography

Dao-wei Liu received a master's degree in School of Computers from Guangdong University of Technology (China) in June 2016. His current research interest fields include information security.

Sheng-hua Xu received a master's degree in School of Computers from Guangdong University of Technology (China) in June 2009. He is now a lecturer, working in Guangdong Polytechnic Normal University. At present,

his research interests mainly include information security.

Wen-tao Zuo received a master's degree in School of Computers from South China Agricultural University (China) in June 2010. He is now a lecturer, working in Guangzhou College of Technology and Business. His current research interest fields include information security.