Forward Private RFID Authentication Protocol Based on Universal Hash Function

Shujing Gao\textsuperscript{a,b,*}, Hongjun Wang\textsuperscript{a}

\textsuperscript{a}School of Information Science and Engineering, Shandong University, Jinan 250100, China
\textsuperscript{b}College of Information Science and Technology, Qingdao University of Science and Technology Qingdao 266061, China

Abstract

Privacy of RFID systems is receiving increasing attention with the progress of Internet of Things. There are a number of challenges in providing privacy and security in the RFID tag due to the limited computation ability of low-cost RFID tags. Many research works have already been conducted using hash functions and pseudorandom numbers to design the RFID protocol. But few of them involve the detail implementation methods of hash functions that can be used. The paper proposes a universal hash function $H_{M\text{-hash}}$ that is suitable for low-cost RFID tags. A mutual and forward private authentication protocol MFPA is designed based on $H_{M\text{-hash}}$. Finally, the security proofs of MFPA are provided under standard model instead of random oracle model. For the first time, the security of the protocol is proofed based on hardware circuit which makes the result more credible.

Keywords: Radio Frequency Identification; Universal Hash Function; Multiple Input Shift Register; Forward Privacy; Internet of Things

1 Introduction

Although it was originally introduced to be used in supply chain, RFID (Radio Frequency Identification) technology today is employed in a great number of applications, such as agriculture [1], toll administration [2], e-passport [3], etc.. With the pervasive of Internet of Things, RFID will intrude the life of end-users.

The RFID systems are vulnerable to many security attacks and privacy disclosure [4] threats due to the restricted computation ability of low-cost RFID tags from which it is very difficult to implement a complicated and safe cryptosystem. In addition, the insecure wireless communication environment also paves the way for new privacy threats in RFID-based systems.

Although some researchers think that advanced cryptographic algorithms, such as ASE, ECC [5, 6], can be used in RFID tags with the progress of design and manufacturing technology of semiconductor, But it is very difficult for users to gain high security at the expenses of cost.

\textsuperscript{*}Corresponding author.

\textit{Email address:} shujing.g@126.com (Shujing Gao).
We focus on two main questions about the requirement of RFID protocol.

The first is the design of hash functions that suitable for RFID tag. There are so many RFID protocols that based on hash functions, such as hash-lock [7, 8], randomized hash-lock [9, 10], hash chain [11], etc. But few of such protocols involve the implementation of hash functions. Efficient Toeplitz [12] hash function is proposed to be used in RFID tag in [13]. But there are no further explanations about the implementation of universal hash function. Hash functions can be divided into cryptographically hash functions and universal hash functions and the former is with higher computation requirement. The protocol in [14] and others proposed base on it [15, 16] are all need cryptographically hash functions which with high hardware complexity and not fit for RFID tag.

The second question is the design and proof of authentication protocol with forward privacy. Low hardware complexity and high security is a pair of contradiction, especially for passive tags. The trade-off between security and computation ability should be considered in the mind in RFID protocol designing. The requirement of security is different according to different domain. Framework for evaluating domain risks is proposed in [17]. As can be seen from the framework, the applications about human, such as e-passport, human implantations and Medical information system, have the highest security and privacy requirement.

There are three classes of privacy depending on the capability of the adversary [18]:

- **Weak privacy**: The adversaries can’t tamper with a tag.
- **Forward privacy**: The adversaries can destroy a tag but cannot uncover any past action of the tag.
- **Strong privacy**: The adversaries can access the tags’ secrets.

Clearly, weak privacy, assumes that adversaries can’t tamper with a tag, can be acquired with simple operation, such as XOR, CRC, etc. [19, 20]. But the systems with weak privacy are easy to be attacked for the same reason. Strong privacy can only be achieved by advanced cryptographic mechanisms which are not fit for RFID tag. Forward privacy can be viewed as the highest level of user-privacy and do not need complex calculation method. Considering the trade-off between security and computation complexity, a lot of efforts have already been put in developing RFID authentication protocols with forward privacy.

One of the most appealing proposals that provide such a high level of user privacy was made by Ohkubo, Suzuki, and Kinoshita [21, 14]. The authors rely on two one-way functions: one to update the internal state of the tag and the other to produce an identification value that does not allow a passive attacker to recover the internal state of the tag. But it is discovered to be vulnerable to DoS attack [13]. The OSK protocol and others that based on it [15, 16] have the same problem of needing cryptographically strong hash functions which is too complex to be implemented in RFID tags.

Building on the previous work of OSK, two protocols, PFP [13] and EFPP [22], are proposed based on universal hash functions. The PFP is a one-way authentication protocol that only considers the authentication of readers to tags. The tags may alter the internal states on the query of impersonating readers and cause the desynchronizations of tags and readers. Furthermore, in the discussion of implementation methods of the PFP, the authors only put forward using Toeplitz,
but hesitate to make further explanation about the construction and the related properties of universal hash functions based on Toeplitz.

**Contributions.** The paper firstly proposes a universal hash function family $H_{M-hash}$ based on $M-hash$ [23]. $M-hash$ is a hash function with low hardware complexity that can be used in low-cost RFID tags like EPC C1G2. $H_{M-hash}$ is proved to be almost strong universal hash function family.

Secondly, we propose Mutual and Forward Private Authentication (MFPA) RFID protocol based on $H_{M-hash}$. The MFPA is proved to be with security, correctness, forward privacy under the standard model. This is in contrast with previous work on forward private protocols which were only proven secure in the random oracle model.

**Organization of the paper.** The paper is organized as follows: In Section 2, we describe the security model and some definitions. In Section 3, we construct the universal hash function family $H_{M-hash}$ and prove it to be $\epsilon-$ almost strong universal hash function family. The mutual and forward private authentication protocol MFPA is described in Section 4. We prove the security of MFPA under the standard model in Section 5. Finally, we conclude in Section 6.

# 2 Securities and Privacy Model

The RFID system includes a backend database, a reader and several tags. Each tag $T_i$ has a secret internal state initialized with a secret $k_{i^0}$. This secret is also known from the backend database to which readers are connected.

We assume that the initial secrets $k_{i^0}$ of the tags are uncorrelated, i.e. independently and randomly chosen. During its lifetime, an initialized tag can enter authentication exchanges with a reader, following a protocol that specifies which messages are to be computed and exchanged and how the internal states of the tag and the back-end system are to be updated. An authentication exchange between a tag and a reader either results inside the reader in an authentication success together with a tag identity or in an authentication failure.

The RFID protocol should satisfy:

(a) Correctness: legal tags should not be refused. This means the scheme can resist against denial of service (DoS) attack.

(b) Security: illegal tags (readers) should not be accepted. This means the scheme can resist against replay, impersonation, man-in-the-middle attacks.

(c) Forward privacy: the user of the tags should not be traced. This means the scheme can resist against tracing attacks.

1. Security

An RFID authentication protocol is said secure if it resists impersonation attacks. The one-way authentication protocols always only consider the authentication of readers to tags but ignore the authentication of tags to readers. Lack of mutual authentication may infer various attacks, such as DoS, track, man-in-the-middle, etc. We will give the mutual security definition in this section.
An impersonation attack proceeds in two phases. During the first phase, an adversary interacts both with a legitimate reader and a legitimate tag $T_i$ and is allowed to trigger, observe, and disturb the communication between the tag $T_i$ and the reader, and to access the outcome of the authentication (success or failure). During the second phase, the adversary only interacts with the reader or the tag $T_i$ to initiate an authentication exchange to impersonate the tag $T_i$ or the reader. The impersonation succeeds if the authentication is successful and the adversary is identified as the tag $T_i$ or the reader.

**Definition 1** An RFID authentication protocol is said to be $\varepsilon_s$—mutual security if for any adversary, the probability that the tags and readers impersonation attack be successful are all at most $\varepsilon_s$.

2. Correctness

The adversary may attack the RFID system and causes a legitimate tag to be “desynchronized” with the system, rendering it unable to successfully pass some or all subsequent authentications.

**Definition 2** An RFID authentication protocol is said to be $\varepsilon_c$—correct if for any adversary, the probability that a legal tag cannot be identified is at most $\varepsilon_c$.

3. Privacy

A privacy attack also proceeds in two phases. During a first phase, $A$ interacts with any two legitimate tags $T_{i_0}, T_{i_1}$ and a legitimate reader. The adversary is allowed to trigger, observe, and disturb authentication exchanges involving $T_{i_0}$ and (possibly) the reader and authentication exchanges involving $T_{i_1}$ and (possibly) the reader. During a second phase, $A$ again interacts with a tag $T_{i_b}$ randomly selected among the two tags $T_{i_0}$ and $T_{i_1}$, and $b$ is concealed to $A$. First, $A$ is allowed to trigger, observe, and disturb authentication exchanges involving $T_{i_0}$ and is given access to the corresponding authentication outcome (success or failure). Then, $A$ is given access to the internal state value of $T_{i_b}$. Eventually, $A$ outputs a guess $b'$ for the value of $b$, and succeeds if $b'$ is equal to $b$.

**Definition 3** An RFID authentication protocol is said to be $\varepsilon_p$—forward privacy if for any adversary, the probability that the privacy attack be successful is at most $\varepsilon_p$.

### 3 Security Mechanism

#### 3.1 Universal Hash Function Family

A universal hash function family [24] $H$ is a finite set of hash functions. Any hash function $h \in H$ is a mapping from a finite set $X$ with size $|X|$ to a finite set $Y$ with size $|Y|$. For a pair $(M \in X, M' \in X)$ with $M \neq M'$, the following function is defined:

1. Collision probability $\delta$: $\delta_h(M, M') = 1$ if $h(M) = h(M')$, and $\delta_h(M, M') = 0$ otherwise.
(2) For a universal hash function family $H$, $\delta_H(M, M')$ is defined as $\sum_{h \in H} \delta_h(M, M')$ counts the number of functions in $H$ for which $M$ and $M'$ collide.

The definition of $\varepsilon-$ almost universal hash function family is given in [25]. In this paper, we will define $\varepsilon-$ almost strong universal hash function family.

**Definition 4** A finite set of hash functions $H = h : X \rightarrow Y$ is $\varepsilon-$ almost strong universal if for all $M, M' \in X$ with $M \neq M'$: $|h \in H : h(M) = h(M')| = \delta_H(M, M') < \varepsilon|H|.$

### 3.2 $H_{M-hash}$

MISR (Multiple-Input-Shift-Register) takes LFSR as main structure and is mainly used in test response compaction of IC self-test [26]. Using the irreversibility of “compaction” of MISR, we will construct the hash function. MISR with bits based on internal LFSR is shown in Fig. 1.

![Fig. 1: structure of n bits MISR](image_url)

The $c_1$ through $c_{n-1}$ are feedback tabs of the LFSR and $d_1$ through $d_n$ are the parallel input data. It would take $\lceil m/n \rceil = L$ cycles to compact one $m$ bits input vector $D$. Let $D_i$ represent $n$ bits input data in the $i$th cycle. That is:

$$D = \begin{bmatrix} D_1 \\ D_2 \\ \vdots \\ D_L \end{bmatrix}, \quad D_t = \begin{bmatrix} d_1(t) \\ d_2(t) \\ \vdots \\ d_n(t) \end{bmatrix}$$

If the initial state of MISR is $Y(0)$, and $Y(t+1)$ and $Y(t)$ represent the states of $(t+1)$th and $t$th cycle of MISR respectively, then the operation of the LFSR can be described as $Y(t+1) = AY(t)$, with $A$ the transition matrix of LFSR. As we can see from Fig. 1, the operation of MISR can be described as:

$$Y(t + 1) = AY(t) + D_t$$  \hspace{1cm} (1)
The matrix representation of Eq. (1) is shown below.

\[
\begin{bmatrix}
  y_1(t+1) \\
  y_2(t+1) \\
  y_3(t+1) \\
  \vdots \\
  y_{n-1}(t+1) \\
  y_n(t+1)
\end{bmatrix} =
\begin{bmatrix}
  c_1 & c_2 & c_3 & \cdots & c_{n-1} & c_n \\
  1 & 0 & 0 & \cdots & 0 & 0 \\
  0 & 1 & 0 & \cdots & 0 & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  0 & 0 & \cdots & 1 & 0 & 0 \\
  0 & 0 & \cdots & 0 & 1 & 0
\end{bmatrix}
\times
\begin{bmatrix}
  y_1(t) \\
  y_2(t) \\
  y_3(t) \\
  \vdots \\
  y_{n-1}(t) \\
  y_n(t)
\end{bmatrix}
+ 
\begin{bmatrix}
  d_1(t) \\
  d_2(t) \\
  d_3(t) \\
  \vdots \\
  d_{n-1}(t) \\
  d_n(t)
\end{bmatrix}
\]

The hash function M-hash can be constructed base on Eq. (1):

\[
h(D) = Y(L) = A^L Y(0) + \sum_{j=1}^{L} A^{L-j} D_j
\]

The register state at the end of \(L\)th cycle, i.e. \(Y(L)\), is the hash value of input vector \(D\).

A set of \(M - \text{hash}\) with different initial state can be used to construct a universal hash function family \(H_{M-hash}\). There are \(2^n\) different initial states for \(n\) bits \(M - \text{hash}\), we get \(|H_{M-hash}| = 2^n\).

The security of this kind of universal hash function depends on the probability of collision [24]. It is proved that the collision probability of \(n\) bits \(M - \text{hash}\) is \(\varepsilon < \frac{1}{2^n}\).

**Theorem 1** \(n\) bits \(H_{M-hash}\) is \(\varepsilon\)-almost strong universal hash function family, with \(\varepsilon < \frac{1}{2^n}\).

**Proof** For \(\delta_H(M, M') = \sum_{h \in H} \delta_h(M, M') = |H| \delta_h(M, M')\), we should only prove \(\delta_h(M, M') < \varepsilon\). In other words, the collision probability of each hash functions satisfies \(P_{colli} < \frac{1}{2^n}\) which is true from the prove of [23].

### 3.3 Pseudo-random Number Generator

The security of Pseudo-random Number Generator (PRNG) depends on the difficulty level of distinguishing the sequence of the PRNG from a perfect random sequence.

Consider a Pseudo-random Number Generator (PRNG) \(G : \{0, 1\}^n \rightarrow \{0, 1\}^L\) with input and output lengths \(n\) and \(L > n\). We define the advantage of a distinguisher \(A\) for distinguishing \(G\) from a perfect random generator as: \(\text{Adv}_G^{\text{PRNG}}(A) = |\text{Pr}[A(G(x)) = 1] - \text{Pr}[A(y)] = 1|\), where \(x \in \{0, 1\}^n\)is the random value input to \(G\) and \(y \in \{0, 1\}^L\) is a true random sequence.

**Definition 5** A PRNG \(G\) is said to be \(\varepsilon_r\)-secure if \(\text{Adv}_G^{\text{PRNG}}(A) \leq \varepsilon_r\).

Supposing the PRNG \(G\) used in the protocol proposed in this paper is \(\varepsilon_r\)-secure.
4 The MFPA Protocol

The MFPA is a three-round authentication protocol. The protocol uses a $\varepsilon$-almost strong universal hash function family $H_{M-hash}$ and a $\varepsilon_r$-secure pseudo-random number generator $G$ to protect the RFID system from adversary attacks.

The notations used are listed as follows:

- $T_i$: A tag
- $R$: Reader
- $D$: Database attached to reader
- $a_j$: Random numbers generated by Database in first round of the $j$th authentication
- $r_j$: Random numbers generated by tag in the $j$th authentication
- $a_j'$: Random numbers generated by Database in third round of the $j$th authentication
- $k_{i0}^j$: The initial state of tag $T_i$
- $k_{ij}^j$: The state of tag $T_i$ in the $j$th authentication
- $k_i^j$: The new internal state of tag $T_i$ after the $j$th authentication
- $k_0^j$: The initial state of tag $T_i$

Initially, the internal state of every tag $T_i$ is randomly set to be $k_0^j \in \{0, 1\}^n$. Fig. 2 shows the $j$th session of the protocol. The current state of the tag is $k_{ij}^j$.

![Fig. 2: The MFPA protocol](image)

**First round**: Challenge. The reader sends a random number $a_j$ as query.

**Second round**: Authentication of reader to tag.

1. The tag generates a pseudo-random number $r_j$ on receiving $a_j$. Hash function $h_j$ is selected from $H_{M-hash}$ taking $k_{j-1}$ as the initial state. The tag calculates $h_j(a_j \oplus r_j) || r_j$ and sends the result to the reader.

2. The reader verifies the answer of the tag by searching through the backend database: for each tag $T_i$ in the system, the reader fetches the last known state $k_{i}^{j-1}$ and runs through the set of possible values $h_j(a_j \oplus r_j) || r_j$. If a match is found for the tag with last known state $k_{i}^{j-1}$, the reader then complete the authentication to the tag successfully.

**Third round**: Authentication of tag to reader.
(1) Hash function $h_j$ is selected from $H_{M\text{-hash}}$ taking $k_{j-1}$ as the initial state. The reader calculates $k_j = h_j(a_j || r_j)$ and generates random number $a'_j$ at the same time. Hash function $h_{j+1}$ is selected from $H_{M\text{-hash}}$ taking $k_j$ as the initial state. The reader calculates $h_{j+1}(a'_j)$ and sends $h_{j+1}(a'_j) || a'_j$ to the tag.

(2) The tag, using the same method, calculates $h_{j+1}(a'_j)$. The authentication of tag to reader is succeed if the result matches to the date received. The internal state of the tag changed from $k_{j-1}$ to $k_j$.

5 MFPA Protocol Analyses

The attacks proceed in two phases. During the first phase, an adversary learns from the authentication exchanges between a legitimate reader and one or two legitimate tags. During the second phase, he carries out the attacking process depending on the information gained from the first phase. The protocol is deemed to be secure if the probability of attacking success is negligible.

Assuming the information set that the adversary learned during the first phase is $I$, the attacking game is $A(I)$. $A(I) = 1$ if the attack is successful, and $A(I) = 0$ otherwise. The probability of adversary be successful can be defined as $Pr[A(I) = 1]$. The system is secure if $Pr[A(I) = 1]$ is negligible. The game $A(I)$ can be security game $A_s(I)$, correctness game $A_c(I)$ and privacy game $A_p(I)$.

Theorem 2 MFPA protocol is $\varepsilon_s$-mutual secure with $\varepsilon_s \leq \varepsilon_r + \frac{1}{2^n}$.

Proof According to [27], we should construct a blinder $A^{\text{sim}}$ for adversary $A$. $A^{\text{sim}}$ is itself an adversary which can interact with reader and the tags in the RFID system but do not have access to the reader tapes so does not know the secret key nor the database. The system is secure if the success probability of $A$ and $A^{\text{sim}}$ is indistinguishable.

It means that there are no privacy losses through the communication channel. In other words, the adversary makes no effective use of the messages as their simulation (without using the secret values) leads to the same probability of success. Thus the scheme can be considered secure.

The blinder $A^{\text{sim}}$ depends on random guess to attack the scheme. The attacking game and the success probability of $A^{\text{sim}}$ can be defined as $A^{\text{sim}}(R)$ and $Pr[A^{\text{sim}}(R) = 1]$ respectively, with $R$ represent “random guess”.

We define the advantage of $A(I)$ over $A^{\text{sim}}(R)$ for attacking the scheme as: $Adv^A_{A^{\text{sim}}} = Pr[A(I) = 1] - Pr[A^{\text{sim}}(R) = 1]$.

Two directions of security should be proved according to Definition 1.

1) The probability of illegal tag successfully authenticated by the reader.

We define the tag impersonation game as $A_s^R(I)$. The system can resist tag impersonation attack when $Pr[A_s^R(I) = 1] \leq \varepsilon_r + \frac{1}{2^n}$.

The impersonation attack occurs during the second round when reader authenticating the tag. The adversary $A$ will make a counterfeit message $C'$ that can be accepted by the reader.

The advantage of $A(I)$ over $A^{\text{sim}}(R)$ for impersonating the tag is $Adv^A_{A^{\text{sim}}} = Pr[A(I) = 1] - Pr[A^{\text{sim}}(R) = 1]$. The information $I$ consists of two pats: one comes from $G$ and the other comes
from $H_{M-hash}$. Thus, let’s consider another worse circumstance: $H_{M-hash}$ has been compromised by $A$ successfully. We define advantage of $A(I)$ over $A^{sim}(R)$ under this circumstance as $Adv_{A^{sim}} = Pr[R^A(Y(I)) = 1] - Pr[A^{sim}(R) = 1]$. Obviously, we can see that $Adv_{A^{sim}} < Adv_{A^{sim}}$. Now, the advantage of $A$ over $A^{sim}$ is equal to Definition 5: advantage of $A$ for distinguishing $G$ from a perfect random generator $Adv_{G}^{PRNG}(A)$. It is easy to see that $Adv_{A^{sim}} < Adv_{G}^{PRNG}(A)$. Because $G$ is $\varepsilon_r-$ secure, then we get $Adv_{A^{sim}} < Adv_{G}^{PRNG}(A) \leq \varepsilon_r$ and $Pr[R^A(Y(I)) = 1] < \varepsilon_r + Pr[A^{sim}(R) = 1]$. 

The $A^{sim}$ will successfully make an impersonation attack by randomly guess the correct $n$ bits internal state of the tag with the probability of $\frac{1}{2^n}$. That is to say $Pr[A^{sim}(R) = 1] = \frac{1}{2^n}$. We get $Pr[R^A(Y(I)) = 1] \leq \varepsilon_r + Pr[A^{sim}(R) = 1] \leq \varepsilon_r + \frac{1}{2^n}$.

(2) The probability of illegal reader successfully authenticated by the tag.

We define the reader impersonation game as $A^T_s(I)$. The system can resist reader impersonation attack when $Pr[A^T_s(I) = 1] \leq \varepsilon_r + \frac{1}{2^n}$.

The impersonation attack occurs during the third round when reader authenticating the tag. The adversary $A$ will make a counterfeit message $C''$ that can be accepted by the reader. The proof process is the same as (1). We can get $Pr[A^T_s(I) = 1] \leq \varepsilon_r + Pr[A^{sim}(R) = 1] \leq \varepsilon_r + \frac{1}{2^n}$.

From (1) and (2) we can draw the conclusion that MFPA is $\varepsilon_s-$ mutual secure with $\varepsilon_s \leq \varepsilon_r + \frac{1}{2^n}$.

**Lemma 1** After the compaction of a same vector, the probability of $n$ bits MISR, starting from different state but going back to a same state is $\frac{1}{2^n}$.

**Proof** The universal hash function family $H_{M-hash}$ is composed of $2^n$ $M-hash$ functions with different initial states. So, Lemma 1 can also be stated as: for two different $M-hash$ functions $h, h' \in H_{M-hash}$, the probability of $h(D) = h'(D)$ is $\frac{1}{2^n}$.

After the compaction of a same vector, the probability of of $n$ bits MISR, starting from different state but going back to a same state is $\frac{1}{2^n}$.

Suppose the hash values of $m$ bits input vector $D$ with different initial state, $Y(0)$ and $Y'(0)$ are $h(D)$ and $h'(D)$, respectively. The matrix $Y'(0)$ is the modulo-2 sum of $Y(0)$ and another matrix $Y_e$, that is $Y'(0) = Y(0) \oplus Y_e$.

$$h(D) = A^L Y(0) + (\sum_{j=1}^{L} A^{L-j} D)$$

$$h'(D) = A^L Y'(0) + (\sum_{j=1}^{L} A^{L-j} D) = A^L Y(0) + A^L Y + (\sum_{j=1}^{L} A^{L-j} D)$$

Without loss of generality, suppose the situation of $D = 0$, then:

$$h'(D) = A^L Y(0) + (\sum_{j=1}^{L} A^{L-j} D) + A^L Y_e + (\sum_{j=1}^{L} A^{L-j} D) = h(D) + A^L Y_e + (\sum_{j=1}^{L} A^{L-j} D) = h(D) + h_e(D)$$

The collision occurs when $h_e(D) = 0$ and $h'(D) = h(D)$. $h_e(D) = 0$ means starting from the initial state $Y_e$ and return all-zero state after input vector $D = 0$.

When input a vector $D = 0$, that is $p = 0$ and $1 - p = 1$, there are only one 1 in each line and each row of Markov probability transition matrix. That is to say, starting from any state, the endpoint is exclusive and be all-zero state with the probability of $P = \frac{1}{2^n}$.
So the probability of \( h'(D) = h(D) \) is \( P = \frac{1}{2^n} \).

**Theorem 3** MFPA protocol is \( \varepsilon_c \)-correct with \( \varepsilon_c \leq \frac{1}{2^n} \).

**Proof** According to Definition 2, we should proof that \( Pr[A_c(I) = 1] \leq \frac{1}{2^n} \).

The legal tags will be refused by tag when the backend database has updated its state with respect to this tag but the tag did not update its internal state in second round, or vice versa. This only happens through an impersonation attack by the attacker or because of a hash function collision.

(1) Impersonation attack. The adversary will impersonate the tag or reader successfully and only change the state in the reader or in the tag. From Theorem 2, the success probability of impersonation attack is \( \varepsilon_s \leq \varepsilon_p + \frac{1}{2^n} \).

(2) Hash function collision. When reader authenticating the tag in the second round by calculating \( h_j^i(a_j \oplus r_j) \parallel r_j \) for every tag \( T_i \) in the system and searching the mach. The tag \( T_y \) will be authenticated as \( T_x \) when \( h_j^x(a \oplus r) = h_j^y(a \oplus r) \). The state in the backend database with respect to \( T_y \) will be undated but the tag \( T_y \) did not update its internal state. Then a desynchronization occurs.

\( h_j^x(a \oplus r) \) and \( h_j^y(a \oplus r) \) are two functions from \( H_{\text{M-hash}} \) with different initial states and same input vector \( a \oplus r \). From Lemma 1, the probability of \( h_j^x(a \oplus r) = h_j^y(a \oplus r) \) is \( \frac{1}{2^n} \).

From (1) and (2), we can get that MFPA is \( \varepsilon_c \)-correct with \( \varepsilon_c \leq \frac{1}{2^n} \).

**Theorem 4** MFPA protocol is \( \varepsilon_p \)-forward privacy with \( \varepsilon_p \leq \frac{1}{2^n} \).

**Proof** Let’s suppose that \( A \) has acquired \( \alpha \) authentication exchanges between two tags \( T_x, T_y \) and the reader. It also has compromised the internal state of \( T_b \) after the \( \gamma \)th authentication, with \( \gamma > \alpha \). The probability of \( A \) successfully guess the correct value of \( b \) is defined as \( Pr[A_p(I)] = Pr[A_p(\gamma = \alpha + 1)] \).

We need only consider the worst case when \( \gamma = \alpha + 1 \). That is \( A \) compromises the internal state of the tag just after the \( \alpha + 1 \)th authentication exchanges. Because of the dependency of two consecutive authentication sessions, \( Pr[A_p(I)] < Pr[A_p(\gamma = \alpha + 1)] \), obviously.

The information \( A \) acquires in the first phase is \( a_i^x, h_i^x(a_i^x \oplus r_i^x \oplus k_i^x) || r_i^x \) and \( h_{i+1}^x(a_i^x \oplus k_i^x) || a_i^x \) from \( T_x \) and \( a_i^y, h_i^y(a_i^y \oplus r_i^y \oplus k_i^y) || r_i^y \) and \( h_{i+1}^y(a_i^y \oplus k_i^y) || a_i^y \) from \( T_y \), with \( i = 1, 2, ..., \alpha \). \( A \) can give the correct guess of \( T_b \) on finding out the value of \( k_a \).

The internal state of \( T_b \) that \( A \) has compromised is \( k_{\alpha+1} \).

Because \( k_{\alpha+1} = h_{\alpha+1}(a_{\alpha+1} || r_{\alpha+1} \oplus k_a) \) and \( a_{\alpha+1}, r_{\alpha+1} \) can all be acquired through monitoring. \( A \) can get \( k_a \) by solve the above function.

We can get the function \( k_{\alpha+1} = A^L Y(0) + (\sum_{j=1}^{L} A^{L-j} D_j) \) with \( n \) bits \( Y(0) \) and \( D = a_{\alpha+1} || r_{\alpha+1} \oplus k_a \) as unknown number. So, a set of \( 2^{(2n-n)} = 2^n \) solutions can be obtained on average, among which only one is the correct. Then the probability of the \( A \) guessing the tag \( T_b \) correctly is \( \frac{1}{2^n} \).
6 Conclusions

The contribution of the paper lies in two aspects. Firstly, we design a universal hash function family $H_{\text{M-hash}}$ with low hardware complexity that can be used in low-cost RFID tags like EPC C1G2. Secondly, we design a mutual and forward private authentication RFID protocol MFPA based on $H_{\text{M-hash}}$. The proof result under standard model indicates that MFPA is secure, correct and privacy and can resist DoS, replay, impersonation, man-in-the-middle and tracing attacks. The security proof of the MFPA, based on standard model and taking hardware circuit into account, is more credible when compared with other protocols that proofed under the random oracle model and only considering the mechanism of the protocols.

References

[23] Shujing Gao, Hongjun Wang, Design and analysis of pseudorandom number generator compatible with EPC C1G2 tag, Journal of Information and Computational Science, Vol. 9, Iss. 10, 2865-2876