An Efficient RFID Authentication Protocol Using Dynamic Identity

Shin-Yan Chiou
(Corresponding author: Shin-Yan Chiou)
Department of Electrical Engineering, Chang Gung University
259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan
Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Tao-Yuan, Taiwan
(Email: ansel@mail.cgu.edu.tw)
(Received Feb. 20, 2018; Revised and Accepted Aug. 18, 2018; First Online July 30, 2019)

Abstract

RFID allows for automatic non-contact identification, and has been widely applied to improve everyday convenience. However, RFID suffers from significant security issues, leaving sensitive user information exposed to a range of malicious attacks. On the other hand, RFID tags have limited computing power and storage capacity, and increasing system security often further compromises system computational efficiency. Therefore, we propose a secure and efficient dynamic mutual authentication protocol for RFID. The proposed system ensures anonymity and forward privacy, and provides security against replay attacks, impersonation attacks, asynchronous attacks, and tracking attacks while significantly reducing the computational cost on RFID tags and system servers.

Keywords: Authentication; Dynamic Identity; Privacy; RFID

1 Introduction

RFID allows for automatic, wireless non-contact identification, comprising a tag, a reader and a server [7]. Electromagnetic coupling between the tag and the reader allows for the transfer of energy and data, which is then transmitted to the server. Because RFID allows for data transfer without physical contact, it can operate in harsh environmental conditions, while also allowing for data transfer from multiple tags. RFID offers simplicity and convenience and has been implemented in a wide range of applications [16, 18, 20, 30], raising the need for a secure and efficient mutual authentication protocol [2, 4, 5, 10, 24, 28].

Part of the RFID authentication protocols [3, 6, 12, 13, 22, 26] is based on Elliptic curve cryptography. This requires the tag to handle complex multiplication tasks, which is clearly inconsistent with the tag's limited computing power. In 2006, Tuyls and Batina [3] first proposed an ECC-based RFID authentication scheme which features a linear relationship between computation capacity and number of tags. Lee *et al.* [22] noted that Tuyls and Batina's protocol features problems with mutual authentication, forward privacy and impersonation attacks. To address these problems, Lee *et al.*, [22], O'Neill and Robshaw [26], and Godor *et al.* [13] proposed an improved ECC-based authentication scheme. In 2013, Chou [6] pointed out that these schemes still lack scalability, and proposed a new authentication scheme based on ECC and hash functions. Chou's scheme significantly reduces the computational cost on server, but not for the tags. In 2014, Farash [12] noted that Chou's scheme still suffered from security issues including forward privacy and mutual authentication. He proposed an improved authentication scheme based on ECC and hash functions. Although Farash's scheme improves on Chou's scheme, it does not significantly reduce tag computation loading.

In addition, another part of the RFID authentication protocols [9, 11, 14, 15, 21, 23, 27, 29, 31] is based on one-way hash function and use the one-way property of the hash function to solve the security and privacy problems of RFID systems. However, most of these schemes have serious security problems. Cho *et al.* [8] proposed a new hash-based RFID mutual authentication protocol and claimed their protocol provides the privacy [17] and forgery concerns [11, 31]. However, Kim [19] demonstrated that this protocol is vulnerable to DOS attack and Masoumeh *et al.* [29] demonstrated their protocol is vulnerable to tag and reader impersonation and desynchronization attacks.

In this paper, we propose a dynamic authentication scheme based only on hash functions to reduce the computational loading on RFID tags, and to ensure mutual authentication, forward privacy and anonymity. Our solution also provides security against replay attacks, impersonation attacks, asynchronous attacks and tracking attacks. We also provide a security analysis, and compare security and computational loading for the proposed scheme against previous schemes.

The rest of this paper is organized as follows. In Sec-

Table 1: Notations

Notation	Description
ID_i/ID_i^S	The identity of Tagi which is stored in the database of Tag_i / Server.
sn_i/sn_i^S	The dynamic serial number of Tagi which is stored in the database of Tag_i / Server.
$sTag_i/sTag_i^S$	The dynamic pseudo-random identity of Tag_i which is stored in the database of Tag_i / Server.
$bsTag_i^S$	The dynamic backup pseudo-random identity of Tag_i.
$H(\cdot)$	A one way hash function.
$a++/a--$	a=a+1/ a=a-1.

tion 2, we introduce the notations and security requirements of our protocol. The proposed scheme is demonstrated in Section 3. Section 4 provides a complete security analysis. Section 5 compares the security and computation costs of the various schemes. Finally, we draw conclusions in Section 6.

2 Preliminaries

In this section, we provide a brief introduction to the notations and security requirements of our protocol.

Table 1 shows the notations used in our protocol.

2.1 Attacker Model

In our scheme, we assume the database of the server is secure. Any identity (*i.e.* Tag_i) communicates with Server via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [1, 25].

1) An adversary may eavesdrop on all communications between protocol actors over the public channel.
2) An attacker can modify, delete, resend and reroute the eavesdropped message.
3) An attacker cannot intercept a message over a secure channel.
4) An attacker cannot be a legitimate user.
5) The attacker knows the protocol description, which means the protocol is public.

2.2 Security Requirements

The security requirements of our proposed scheme are listed as follows:

Mutual authentication. Tag and Server authenticating each other in conversation.

Forward privacy. An adversary cannot trace the tag through past conversations even if the adversary compromises a tag and obtains the data stored in tag's memory.

Anonymity. An adversary cannot know which Tag is communicating with the server through the eavesdropped data.

Resistance to impersonation attack. An adversary is prevented from impersonating any legal Tag or Server.

Resistance to replay attack. An adversary is prevented from impersonating any legal user from eavesdropped data.

Resistance to asynchronous attack. Tag and Server can process a successful mutual authentication even if the date stored in Server and Tag may be asynchronous when a session cannot be normally completed.

Resistance to tracking attack. An adversary cannot trace the tag through the eavesdropped data.

3 Proposed Scheme

In RFID system, there are three roles: Server, Reader, and Tag. The communication between Server and Reader is secure. We propose a secure and efficient RFID authentication protocol for the communication between servers and tags. Our scheme has two phases: (1) Initial Phase and (2) Authentication Phase. The protocol of each phase is described as follows.

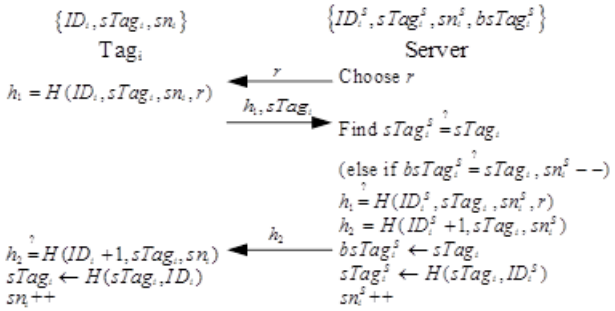

Figure 1: The proposed scheme

3.1 Initial Phase

In this phase, users proceed registration to the server, allowing them to share ID_i^S, $sTag_i^S$ and sn_i^S and offering the server to get the initial $bsTag_i^S = sTag_i$. Server chooses a secret identity ID_i and a dynamic pseudo-random identity $sTag_i$ for Tag_i, and set the serial number $sn_i = 1$. Then, Server stores ID_i, $sTag_i$, and sn_i in the database of Tag_i, and also stores ID_i^S, $sTag_i^S$, sn_i^S, and $bsTag_i^S$ in Server's database, where $ID_i^S = ID_i$, $sTag_i^S = sTag_i$, $bsTag_i^S = sTag_i$, and $sn_i^S = sn_i$.

3.2 Authentication Phase

In this phase, the server and communicate with each other to secure authentication, following the protocol illustrated in Figure 1.

Step 1. Server selects a random number r and transmits it to Tag_i.

Step 2. Tag_i receives r and then calculates $h_i = H(ID_i, sTag_i, sn_i, r)$ before sending $h_i, sTag_i$ to Server.

Step 3. Server receives $h_i, sTag_i$ and searches its database to determine whether $sTag_i^S = sTag_i$.

1) If yes, go to Step 4;
2) Otherwise continue to search to determine whether $bsTag_i^S = sTag_i$. If it exists, then calculate sn_i^S and go to Step 4. Otherwise, Tag_i is invalid and communication is terminated.

Step 4. Server verifies whether the establishment $h_1 = H(ID_i, sTag_i^S, sn_i^S, r)$ holds. If it does not, communication is terminated, otherwise continue to calculate $h_2 = H(ID_i^S + 1, sTag_i, sn_i^S)$, and perform $bsTag_i^S \leftarrow sTag_i$, $sTag_i^S \leftarrow H(sTag_i, ID_i^S)$, $sn_i^S{+}{+}$ to update $bsTag_i^S$, $sTag_i^S$ and sn_i^S in the database, before finally transmitting h_2 to Tag_i.

Step 5. Tag_i receives h_2 and verifies whether $h_2 = H(ID_i + 1, sTag_i, sn_i)$ is established. If it is not established, communication is terminated. Otherwise, perform $sTag_i \leftarrow H(sTag_i, ID_i)$, $sn_i{+}{+}$ to update $sTag_i$ and sn_i.

4 Security Analysis

In this section, we analyze the seven security requirements: mutual authentication, forward privacy, replay attack resistance, impersonation attack resistance, asynchronous attack resistance, anonymity, and tracking attack resistance.

Mutual Authentication:

The identifier ID_i of Tag_i is private, and is known only to Tag_i and Server. Thus, when Tag_i transmits h_1, Server can determine whether the sender is Tag_i via $h_1 = H(ID_i^S, sTag_i^S, sn_i^S, r)$. When Server transmits $h_2 = H(ID_i^S{+}1, sTag_i, sn_i^S)$ to Tag_i, Tag_i similarly can determine whether the sender is Server via $h_2 = H(ID_i + 1, sTag_i^S, sn_i)$.

Forward Privacy:

When an attacker accesses data $ID_i, sTag_i, sn_i$ from Tag_i, the one way nature of the hash function ensures that $sTag_i \leftarrow H(sTag_i, ID_i)$ cannot determine the old $sTag_i$ from the current $sTag_i$. Thus, our protocol satisfies Forward privacy.

Definition 1. *(Partial hashed-message problem) Let $a, b \in Z$, $T = h(a, b)$. If a can be evaluated from given T and b, then we say the Partial hashed-message problem is solved. (The probability of solving this problem is denoted as $Pr(a|T, b) = \varepsilon_1$.)*

Theorem 1. *(Forward privacy) In our scheme, if an attacker can evaluate $sTag_i^{n-1}$ from accessed data $sTag_i^{(n)}$ and ID_i from Tag_i, then the Partial hashed-message problem can be solved, where $sTag_i^{(n)}$ stands for the n^{th}-round $sTag_i$, and $sTag_i^{(n)} = h(sTag_i^{(n-1)}, ID_i)$.*

Proof. In our scheme, assume an adversary tries to track a user A from accessed data $sTag_i^{(n)}$ and ID_i. Let RO_1 be a random oracle: Input $sTag_i^{(n)}$ and ID_i to output $sTag_i^{(n-1)}$. (i.e. $RO_1(sTag_i^{(n)}, ID_i) \rightarrow sTag_i^{(n-1)}$.) In Definition 1, let $sTag_i^{(n)} \leftarrow T$ and $ID_i \leftarrow b$ be input parameters of RO_1 and obtain output $sTag_i^{(n-1)}$. Let $a \leftarrow sTag_i^{(n-1)}$, then a is evaluated. Therefore, $Pr(sTag_i^{(n-1)}|sTag_i^{(n)}, ID_i) \leq Pr(a|T, b) = \varepsilon_1$, which means the Partial hashed-message problem can be solved if ro_1 exists. □

Replay Attack Resistance:

1) Forged Tag_i: In the first step of the protocol, Server generates a random number r and sends it to Tag_i, which then uses the random number for calculating $h_1 = H(ID_i, sTag_i, sn_i, r)$. Therefore, an attacker cannot use a new random number r' and the old number h_1 to successfully forge the new number h_1', thus blocking replay attacks.
2) Forged Server: Although at the server side it is possible to use the old r to forge a new h_2, because $sTag_i$ and sn_i are different each time, it is difficult for an attacker to impersonate a legitimate server in a replay attack.

Definition 2. *(Partial joint hash problem) Let $a, b_1, b_2, c_1, c_2, d_1, d_2 \in Z$, $H_1 = h(a, b_1, c_1, d_1)$ and $H_2 = h(1, b_2, c_2, d_2)$. If H_1 can be evaluated from given H_2, c_1, c_2, d_1 and d_2, then we say the Partial joint hash problem is solved, where $c_1 \neq c_2$, $d_1 \neq d_2$. (The probability of solving this problem is denoted as $Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$.)*

Theorem 2. *(Replay attack resistance) In our scheme, if an attacker can evaluate the value of* $h_1^{(n)}$ *from eavesdropped* $h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}$ *and* $sTag_i^{(m)}$ *then the Partial joint hash problem can be solved, where* $h_1^{n)}/h_1^{(m)}$ *stands for the* n/m^{th}*-round* h_1*,* $r^{(n)}/r^{(m)}$ *means the* n/m^{th}*-round* r*,* $sTag_i^{(n)}/sTag_i^{(m)}$ *means the* n/m^{th}*-round* $sTag_i$*, and* $h_1^{(n)} = h(ID_i, sTag_i^{(n)}, sn^{(n)}, r^{(n)})$*,* $h_1^{(m)} = h(ID_i, sTag_i^{(m)}, sn^{(m)}, r^{(m)})$*.*

Proof. In our scheme, assume an adversary tries to impersonate a user i from eavesdropped $h_1^{(m)}$, $sTag_i^{(n)}$, $sTag_i^{(m)}$, $r^{(n)}$) and $r^{(m)}$). Let RO_2 be a random oracle: Input $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$ to output $h_1^{(n)}$. (i.e. $RO_2(h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \rightarrow h_1^{(n)}$.) In Definition 2, let, $h_1^{(m)} \leftarrow H_2$, $r^{(n)} \leftarrow c_1$, $r^{(m)} \leftarrow c_2$, $sTag_i^{(n)} \leftarrow d_1$ and $sTag_i^{(m)} \leftarrow d_2$ be input parameters of RO_2 and obtain output $h_1^{(n)}$. Let $H_1 \leftarrow h_1^{(n)}$, then H_1 is evaluated. Therefore, $Pr(h_1^{(n)}|h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \leq Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$, which means the Partial joint hash problem can be solved if RO_2 exists. □

Impersonation Attack Resistance:

An attacker can impersonate Tag_i or Server using either a replay attack or a false identifier ID_i.

1) In replay attack resistance, we determine that an attacker would be unable to use a replay attack to impersonate Tag_i or Server.
2) Because Server and Tag_i share a private identifier, using a false identifier to impersonate Tag_i or Server is infeasible.

Theorem 3. *(Impersonation attack resistance) In our scheme, if an attacker can evaluate the value of* $h_1^{(n)}$ *from eavesdropped* $h_1^{(m)}$*,* $r^{(n)}$*,* $r^{(m)}$*,* $sTag_i^{(n)}$ *and* $sTag_i^{(m)}$ *then the Partial joint hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to replay a user i from eavesdropped $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$. Let RO_3 be a random oracle: Input $h_1^{(m)}$, $r^{(n)}$, $r^{(m)}$, $sTag_i^{(n)}$ and $sTag_i^{(m)}$ to output $h_1^{(n)}$. (i.e. $RO_3(h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \rightarrow h_1^{(n)}$.) In Definition 2, let, $h_1^{(m)} \leftarrow H_2$, $r^{(n)} \leftarrow c_1$, $r^{(m)} \leftarrow c_2$, $sTag_i^{(n)} \leftarrow d_1$ and $sTag_i^{(m)} \leftarrow d_2$ be input parameters of RO_3 and obtain output $h_1^{(n)}$. Let $H_1 \leftarrow h_1^{(n)}$, then H_1 is evaluated. Therefore, $Pr(h_1^{(n)}|h_1^{(m)}, r^{(n)}, r^{(m)}, sTag_i^{(n)}, sTag_i^{(m)}) \leq Pr(H_1|H_2, c_1, c_2, d_1, d_2) = \varepsilon_2$, which means the Partial joint hash problem can be solved if RO_3 exists. □

Asynchronous Attack Resistance:

When an attacker uses a truncated or tampered h_2 to cause Tag_i to fail to receive h_2 or h_2 authentication, the Server-side $sTag_i^S$, sn_i^S will update (i.e., $sTag_i^S \leftarrow h(sTag_i, ID_i^S), sn_i^S++$), but the Tag_i-side $sTag_i$, sn_i will not be updated, resulting in non-synchronization. However, because we have a $sTag_i$ backup (i.e., $bsTag_i^S \leftarrow sTag_i$), when Tag_i attempts to transmit the next time, the Server-side will determine whether $bsTag_i^S = sTag_i$. If not, it will next seek to determine whether $bsTag_i^S = sTag_i$. At this time, the Tag_i-side $sTag_i$ is equivalent to the Server-side $bsTag_i^S$, and we calculate sn_i^S-- to resolve the synchronization of sn_i^S and sn_i. If the truncated or tampered h_2 appear multiple times, it will not result in non-synchronization. Thus, our scheme foils asynchronous attacks.

Anonymity:

The tag has two identifiers ID_i and $sTag_i$. ID_i takes the form of $h_1 = H(ID_i, sTag_i, sn_i, r)$ and $h_2 = H(ID_i^S+1, sTag_i, sn_i^S)$ in the transmission protocol, and $sTag_i$ is a dynamic pseudo-random ID, thus attackers attempting to intercept a particular transmission will be unable to accurately determine whether the communication is from a specific tag, thus the proposed scheme provides anonymity.

Definition 3. *(Partial hash problem) Let* $a, b, c, d \in Z$ *and* $H_1 = h(a, b, c, d)$*. If* a *can be evaluated from given* c*,* d*, and* H_1*, then we say the partial hash problem is solved. (The probability of solving this problem is denoted as* $Pr(a|H_1, c, d) = \varepsilon_3$*.)*

Theorem 4. *(Anonymity) In our scheme, if an attacker can evaluate* ID_1 *from* h_1*, then the partial hash problem can be solved.*

Proof. In our scheme, assume an adversary tries to compute ID_1 from eavesdropped h_1, r, and $sTag_i$, where $h_1 = H(ID_i, sTag_i, sn_i, r)$. Let RO_4 be a random oracle: input h_1, r and $sTag_i$ to output ID_i (i.e. $RO_4(h_1, r, sTag_i) \rightarrow ID_i$.) In Definition 3, let $r \leftarrow c$, $sTag_i \leftarrow d$ and $h_1 \leftarrow H_1$ be input parameters of RO_4 and obtain output ID_i. Let $a \leftarrow ID_i$ then a is evaluated. Therefore, $Pr(ID_i|h_1, r, sTag_i) \leq Pr(a|H_1, c, d) = \varepsilon_4$, which means the partial hash problem can be solved if RO_4 exists. □

Tracking Attack Resistance:

When an attacker intercepts Tag_i, the communications data contains $r, h_1, sTag_i, h_2$. r is a random number, $sTag_i$ uses $H(sTag_i, ID_i)$ to update, $h_1 = H(ID_i, sTag_i, sn_i, r)$ uses a different $sTag_i$, sn_i, r for each transmission, and $h_2 = H(ID_i^S + 1, sTag_i, sn_i^S)$

Table 2: Comparison of computation loadings

	Batina [3]		**Lee [22]**		**Chou [6]**		**Farash [12]**		**Our Scheme**	
	Tag	Server	Tag	Server	Tag	Server	Tag	Server	Tag	Server
Hash function	0	0	0	0	2	2	2	3	3	3
ECC Multiplication	2	3n	3	1+2n	2	3	2	3	0	0

n: The number of tags.

Table 3: Comparison of security properties

	Batina [3]	Lee [22]	Chou [6]	Farash [12]	Our Scheme
Mutual authentication	No	No	No	Yes	Yes
Forward privacy	No	Yes	No	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes	Yes
Tracking attack resistance	Yes	Yes	Yes	Yes	Yes
Replay attack resistance	Yes	Yes	Yes	Yes	Yes
Impersonation attack resistance	No	No	No	Yes	Yes
Asynchronous attack resistance	N/A$^{(*1)}$	N/A$^{(*1)}$	N/A$^{(*1)}$	N/A$^{(*1)}$	Yes

*1: No asynchronous attack issues.

uses a different $sTag_i$, sn_i^S each time. Therefore, an attacker would be unable to determine the relationship between each r, h_1, $sTag_i$, h_2 to track each Tag_i.

Definition 4. *(Partial joint-hash tracking problem) Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in Z$, $H_1 = h(a_1, b_1, c_1, d_1)$ and $H_2 = h(a_2, b_2, c_2, d_2)$. If $isEqual(a_1, a_2)$ can be evaluated from given H_1, H_2, c_1, c_2, d_1 and d_2, then we say the partial joint-hash tracking problem is solved, where $c_1 \neq c_2$, $d_1 \neq d_2$ and $isEqual(a_1, a_2)$ is 0 (if $a_1 \neq a_2$) or 1 (if $a_1 = a_2$). (The probability of solving this problem is denoted as $Pr(isEqual(a_1, a_2)|H_1, H_2, c_1, c_2, d_1, d_2) = \varepsilon_4$).*

Theorem 5. *(Tracking attack resistance) In our scheme, if an attacker can evaluate the value of $isEqual(ID_U^{(n)}, ID_V^{(m)})$ from eavesdropped $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)}$, $r^{(V)(m)}$, $sTag_U^{(n)}$ and $sTag_V^{(m)}$, then the partial joint-hash tracking problem can be solved, where $h_1^{(U)(n)}/h_1^{(V)(m)}$ stands for the n/m^{th}-round $h_1^{(U)}/h_1^{(V)}$, $r^{(U)(n)}/r^{(V)(m)}$ means the n/m^{th}-round $r^{(U)}/r^{(V)}$, $sTag_U^{(n)}/sTag_V^{(m)}$ means the n/m^{th}-round $sTag_U/sTag_V$, $h_1^{(U)(n)} = h(ID_U^{(n)}, sTag_U^{(n)}, sn^{(U)(n)}, r^{(U)(n)})$, $h_1^{(V)(m)} = h(ID_V^{(m)}, sTag_V^{(m)}, sn^{(V)(m)}, r^{(V)(m)})$, $isEqual(x, y)$ is 0 (if $x \neq y$) or 1 (if $x = y$), and $t_1 \neq t_2$.*

Proof. In our scheme, assume an adversary tries to track a user U from eavesdropped $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)})$, $r^{(V)(m)}$, $sTag_U^{(n)}$, and $sTag_V^{(m)}$. Let RO_5 be a random oracle: Input $h_1^{(U)(n)}$, $h_1^{(V)(m)}$, $r^{(U)(n)})$, $r^{(V)(m)}$, $sTag_U^{(n)}$, and $sTag_V^{(m)}$ to output $isEqual(ID_U^{(n)}, ID_V^{(m)})$. (i.e. $RO_5(h_1^{(U)(n)}, h_1^{(V)(m)}, r^{(U)(n)}, r^{(V)(m)}, sTag_U^{(n)}, sTag_V^{(m)}) \rightarrow isEqual(ID_U^{(n)}, ID_V^{(m)})$.) In Definition 4, let, $h_1^{(U)(n)} \leftarrow H_1$, $h_1^{(V)(m)} \leftarrow H_2$, $r^{(U)(n)} \leftarrow c_1$, $r^{(V)(m)} \leftarrow c_2$, $sTag_U^{(n)} \leftarrow d_1$ and $sTag_V^{(m)} \leftarrow d_2$ be input parameters of RO_5 and obtain output $isEqual(ID_U^{(n)}, ID_V^{(m)})$. Let $isEqual(a_1, a_2) \leftarrow isEqual(ID_U^{(n)}, ID_V^{(m)})$, then $isEqual(a_1, a_2)$ is evaluated. Therefore, $Pr(isEqual(ID_U^{(n)}, ID_V^{(m)})|h_1^{(U)(n)}, h_1^{(V)(m)}, r^{(U)(n)}, r^{(V)(m)}, sTag_U^{(n)}, sTag_V^{(m)}) \leq Pr(isEqual(a_1, a_2)|H_1, H_2, c_1, c_2, d_1, d_2) = \varepsilon_4$, which means the partial joint-hash tracking problem can be solved if RO_5 exists. □

5 Comparison

In this section, we analyze the performance of our proposed method from computation loadings and security properties.

Table 2 compares the computation cost between our scheme and previous schemes. The other four papers require ECC multiplication operations, whereas our scheme only requires a hash operation. The computation costs of the other three phases are far less than in other schemes. Therefore, our scheme is superior to previous schemes in terms of efficiency.

Table 3 compares the security properties between the proposed and previous schemes, and shows our proposed scheme is resistant to tracking attacks, replay attacks, impersonation attacks, and asynchronous attack resistance, and also provides mutual authentication, forward privacy,

and anonymity.

In addition, server stores $ID_i^S, sn_i^S, sTag_i^S$, and $bsTag_i^S$ for each tag. Assume each length of $ID_i^S, sn_i^S, sTag_i^S$, and $bsTag_i^S$ are is 128 bits. Then the server storage cost (for tags) is 64n bytes, where n is the number of the tags.

6 Conclusion

This paper proposes a RFID mutual authentication protocol which provides high standards of security and convenience. Our scheme is resistant to impersonation attacks, replay attacks, asynchronous attacks, and tracking attacks, and also provides mutual authentication, forward privacy, and anonymity. It also reduces the computation cost of tags and servers. Given the limited computing power in the tag, reducing the tag's calculation loading will play an important role in improving RFID efficiency.

Acknowledgments

This work is partially supported by the Ministry of Science and Technology under Grant MOST 107-2221-E-182 -052 and by the CGMH project under Grant BMRPB46. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] R. Amin and GP. Biswas, "A novel user authentication and key agreement protocol for accessing multimedical server usable in TMIS," *Journal of Medical Systems*, vol. 39, no. 3, pp. 1-17, 2015.

[2] N. Anwar, I. Riadi, and A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71-81, 2016.

[3] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 217-222, 2007.

[4] H. Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no.4, pp. 337-340, 2007.

[5] S. Y. Chiou, W. T. Ko, and 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.

[6] J. S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75-94, 2014.

[7] J. S. Chou, Y. Chen, C. L. Wu, and C. F. Lin, "An efficient RFID mutual authentication scheme based on ECC," *IACR Cryptology ePrint Archive*, p. 418, 2011.

[8] J. S. Cho, Y. S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Computers and Mathematics with Applications*, vol. 69, no. 1, pp. 58-69, 2015.

[9] J. S. Cho, S. S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Computer Communications*, vol. 34, pp. 391-397, 2011.

[10] P. Y. Cui, "An improved ownership transfer and mutual authentication for lightweight RFID protocols," *International Journal of Network Security*, vol. 18, no. 6, pp. 1173-1179, 2016.

[11] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 59-66, 2005.

[12] M. S. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 2, pp. 987-1001, 2014.

[13] G. Gódor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations," in *IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 650-657, 2010.

[14] M. H. Habibi, M. R. Aref, and D. Ma, "Addressing flaws in RFID authentication protocols," in *Progress in Cryptology (INDOCRYPT'11)*, LNCS 7107, pp. 216-235, Springer, 2011.

[15] S. Han, V. Potgar, and E. Chang, "Mutual authentication protocol for RFID tags based on synchronized secret information with monitor," in *Computational Science and Its Applications (ICCSA'07)*, LNCS 4707, pp. 227-238, Springer, 2007.

[16] H. J. Joo, M. T. Cho, and H. Y. Jeong, "RFID-based scale model freight car system allowing real-time quantity checking," *Multimedia Tools and Applications*, vol. 76, no. 4, pp. 5985–6002, 2017.

[17] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, 2006.

[18] H. Kim, "Enhanced hash-based RFID mutual authentication protocol," in *Computer Applications for Security, Control and System Engineering*, CCIS 339, pp. 70-77, Springer, 2012.

[19] H. Kim, "Desynchronization attack on hash-based RFID mutual authentication protocol," *Journal of Security Engineering*, vol. 9, no.4, pp. 357-365, 2012.

[20] J. Y. Kim, K. Y. Chung, and J. J. Jung, "Single tag sharing scheme for multiple-object RFID applications," *Multimedia Tools and Applications*, vol. 68, no. 2, pp. 465-477, 2014.

[21] S. Lee, T. Asano, and K. Kim, "RFID mutual authentication scheme based on synchronized secret information," in *Symposium on Cryptography and Information Security*, Hiroshima, Japan, 2006.

[22] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol," in *IEEE International Conference on RFID*, pp. 97-104, 2008.

[23] J. Lim, H. Oh, and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection," *Information Security Practice and Experience*, vol. 4991, pp. 278-289, 2008.

[24] L. Liu, Z. Cao, and O. Markowitch, "A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 88-92, 2016.

[25] D. Mishra, A. K. Das, A. Chaturvedi, and S. Mukhopadhyay, "A secure password-based authentication and key agreement scheme using smart cards," *Journal of Information Security and Applications*, vol. 23, pp. 28-43, 2015.

[26] M. O'Neill and M. J. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags," *IET Computers and Digital Techniques*, vol. 4, no. 1, pp. 14-26, 2010.

[27] S. Piramuthu, "RFID mutual authentication protocols," *Decision Support Systems*, vol. 50, no. 2, pp. 387-393, 2011.

[28] S. Qi, L. Lu, Z. Li, and M. Li, "BEST: A bidirectional efficiency–privacy transferable authentication protocol for RFID–enabled supply chain," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 18, no.4, pp. 234-244, 2015.

[29] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, "Cryptanalysis of the Cho *et al.* protocol: A hash-based RFID tag mutual authentication protocol," *Journal of Computational and Applied Mathematics*, vol. 259, pp. 571-577, 2014.

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

[31] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proceedings of the Workshop on RFID and Lightweight Cryptography*, pp. 17-24, 2005.

Biography

Shin-Yan Chiou received the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he worked at Industrial Technology Research Institute as a RD Engineer. Since 2009, he joined the faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. He has published a number of journal and conference papers in the areas of information security, social network security and mobile security. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.