A Mutual Authentication Protocol Based on Hash Function for RFID

Chia-Hui Wei², Min-Shiang Hwang¹, Augustin Yeh-hao Chin²

Department of Management Information Systems¹
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Computer Science²
National Tsing Hua University
101, Section 2, Kuang Fu Road, Hsinchu 300, Taiwan, R.O.C.
Email: chwei@cs.nthu.edu.tw, yhchin@cs.nthu.edu.tw
A Mutual Authentication Protocol Based on Hash Function for RFID

Abstract
Security and privacy problems are important issues for developing the RFID system. Designing a security protocol for these systems is difficult since the tag has small power consumption with a limited memory capability. Inappropriate use of the traditional encryption methods in RFID systems is a result of those limitations. Therefore, much research is based on hash function and mutual authentication; however, these protocols perform weakly under the attacks of tracking and forward security. In this paper, we propose a protocol of mutual authentication with the ability to resist tracking attacks and forward security attacks. The protocol can reduce the weaknesses and strengthen the security requirements in RFID systems.

Keywords: Hash Function, Privacy, RFID, and Security

1. Introduction
The barcode is the most widely adopted identification system. However, the barcode cannot add other descriptive information due to its limited space, and requires laser scanning devices at close range to read and process information. Therefore, Radio Frequency Identification (RFID) will gradually replace the traditional barcode in various applications and gain popularity in logistics [11][18], hospitals [1][4], and education [9][10]. The main characteristic of the RFID is that its small size allows it to be embedded in any product, and to be traced and located by radio frequency. The RFID system is composed of three different parts: tags, readers, and backend database. The tags contain processing units and limited memory, and it can perform simple arithmetic operations. The tag transfers data through radio frequency to the reader; the reader then transfers data back to the backend database. The backend database can authenticate the legitimacy of the tags.

Each tag has its own ID. The tag is installed in an open environment for identification of trade items, logistic units, assets and locations. When a customer buys the item and takes it home, the tag is still available, so an attacker may be able to track the customer or learn what this customer carrying in his/her bags by scanning the RFID tags; and results in private violation. Another problem is security; anyone can scan tag's ID because the tag is in an open environment. An attacker with the tag's ID can cheat the database in order to be verified as legal. Under this situation, the security problem results in a privacy violation. Many research works reported such attacks [2][3][20]. For example, the purpose of the RFID Kills Web site
Although RFID has many advantages, it still faces several challenges. The privacy and security are major issues. Many protection mechanisms are proposed [2][3][20]. None of these mechanisms is secure enough to prevent the attacker from retrieving secure information [5]. Most related works that aim to protect the security and privacy in RFID systems are divided into two groups; namely, (1) physical methods such as kill command [14], [15], faraday cage [7], active jamming [7], and blocker tag [7]; and (2) cryptographic methods such as hash-based protocol etc [2][3], [8][19][20]. The former method is not suitable in RFID because a killed tag cannot be reused and cannot solve after-sale service problem for kill command or the limited of size in faraday cage. Therefore, physical methods cannot be used in various applications in the RFID system such as [4][6][10]. In cryptographic methods, the traditional encryption methods are not suitable for RFID systems because the tag is limited by processing units and memory. The hash chain is basically a cryptography approach used in micro payment systems and RFID systems. Lamport [8] describes that a hash chain could be constructed by applying a one-way hash function to generate an initial value. Much research has been focused on improving Lamport's protocol to protect privacy and security. We propose a protocol called the hash function based authentication protocol that can be used on low-cost RFID systems. Our protocol uses the hash function to achieve mutual authentication and data security between the tag and the backend database.

The rest of this paper is organized as follows. We describe the requirements of RFID system in Section 2. Section 3 presents the proposed protocols. Concluding remarks are finally made in Section 4.

2. Requirements of RFID System
As stated in Section 1, the characteristic of radio frequency results in many research issues about security and privacy in implementing a RFID system. In addition, efficiency is another concern when the reader would be identified by multiple tags simultaneously. We propose the following criteria for evaluating a good protocol.

2.1. Mutual authentication
An item’s data is delivered through a channel between the reader and the tag by radio frequency. Therefore, a malicious reader could get information from a tag without authorization, resulting in security and privacy problems. In order to mend this problem, the protocol needs to ensure the mutual authentication between the reader and the tag, and it is an essential function of the security protocol. Such a mutual authentication can be divided into two subtasks, namely (1) reader identification of a
tag and (2) tag identification of a reader. The former subtask occurs when a reader must confirm its legal identity for a tag so a reader can be confident of the tag's identity before sending information. The later subtask occurs when a tag must confirm its legal identity for a reader so a tag can be confident of the reader's identity before updating its data by itself.

2.2. Basic security and privacy

To build a trusted information system and to enhance its security are both crucial to the future of RFID technology. There are two challenges: one is personal privacy protection and the other is security problem [2][12] [20]. The personal privacy intruding models are described as the following. The tag's data are stored in a store for identification and management of the inventory. Nevertheless, an attacker can still trace what consumers buy and their locations if the store has not disabled the tag. This is serious privacy information invasion when a consumer buys a product, which stores the tag's ID. An attacker can surreptitiously steal all the communications between the reader and the tag if they communicate via radio frequency, which is easy to be sniffed or eavesdropped. Therefore, we need to design a protocol to solve security and privacy problems; even if an attacker can eavesdrop and get data, he or she still does not know the useful information.

We suggest that all of the RFID systems need to attain basic security. The basic security is essential for RFID system in order to prevent tag tracking, cloning, and replay attack.

- **Tag Tracking:** A tag always broadcasts a fixed serial number to nearby readers. Therefore, the attacker could identify the fixed serial number of the tag from different locations or transaction records. The attacker could know what items that the consumer bought from the store or what books the consumer borrowed from the library by eavesdropping. Furthermore, when a consumer makes a purchase and pays by credit/debit card, this transaction will establish a link between the customer’s identity and the serial numbers of the tags for this customer. Marketer could identify the serial number of the tag and profile transaction records from different branches. Marketer could analyze what items the customer prefers. The problem of clandestine tracking is not only tracking tag but also linking personal information with the credit/debit. This is serious privacy problem and should be prevented.

- **Cloning:** A cloning tag is the copying data from one tag onto another tag. The tag is installed in open environments, such as supermarkets, hospitals, schools, and other public places; so any attacker can read the tag's ID at anytime. Then, an
attacker clones the same tag by writing all the obtained data onto other tags. Consequently, cloning tag becomes a serious security problem when a cloned RFID passport cannot be prevented.

- **Replay Attack**: The attacker repeats or delays the same message when valid data are transmitted; and tries to intercept the data and retransmits them. The attacker then can cheat or spoof either the reader or the tag in order to obtain the accessed data. For example, when the tag sends an ID to the reader for recognition of its identity; meanwhile, the attacker is also able to eavesdrop and keeps the ID. After the tag and the reader have finished all the communications, the attacker retransmits ID to the reader and the item can be passed the verification illegally. Replay attack not only occurs between the tag and reader but also occurs between the reader and the backend database. In this situation, an illegal tagging attempt to be verified by the reader or backend database results in a security problem.

2.3. Additional security and privacy
We propose the threats model not only including basic security but also providing additional security. The additional security occurs under certain assumption. Such an additional security would not occur, if the assumption does not exist. Therefore, the additional security is not always required in every RFID system.

- **Forward Security**: The attacker can compromise a tag, obtain its current data, and possibly trace future transaction record. For example, when the tag is attached in a passport, the reader verifies the tag’s ID, and an attacker compromises the tag to obtain the ID. Hence, the attacker can trace that user's future boarding information depending on whether the ID is matched or not. Forward security will not occur if the tag updates its ID each session.

- **Denial of Service (DOS)**: An attacker could send massive messages to the backend database and then attempt to crash the backend database; consequently, the unavailability of resource for its intended users occurs. In this situation, the data is stored in both the tag and the backend database, and they become inconsistent so the protocol cannot identify the data. The backend database also could not respond to other validation requests since the backend database is still unavailable. Denial of Service will not occur if the backend database and the tag will not update the common data.

2.4. Efficiency
The tag, which can perform simple arithmetic operations, is limited in processing
units and memory. Therefore, efficiency of traffic cost, computation cost, and memory cost are concerned, if multi-tags are read simultaneously.

- **Traffic cost**: The tag transfers the data through radio waves, thus the number of traffic is critical. Lower traffic will reduce the communication time.
- **Computational cost**: The capability and power of the tag is limited, thus it cannot calculate complicated computational operations. The simple arithmetic is adopted in RFID system.
- **Memory cost**: The memory space is needed to store values in the tag and the reader, thus the storage cost is low, if less values are being stored.

3. **The Proposed Protocol**

In this section, we propose a mutual authentication protocol based on hash function in detailed steps, and then we evaluate the proposed protocol in analysis requirements of a RFID system. All symbols are listed in Table 1.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A =? B$</td>
<td>whether $A$ equal $B$ or not</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>exclusive-or operator</td>
</tr>
<tr>
<td>$h()$</td>
<td>one-way hash function ${0, 1}^* \rightarrow {0, 1}^t$</td>
</tr>
<tr>
<td>$S_{old}$</td>
<td>old secret value</td>
</tr>
<tr>
<td>$S_{new}$</td>
<td>new secret value</td>
</tr>
<tr>
<td>$N_{R(old)}$</td>
<td>old random number</td>
</tr>
<tr>
<td>$N_{R(new)}$</td>
<td>new random number</td>
</tr>
<tr>
<td>$ID$</td>
<td>unique identifier of tag</td>
</tr>
<tr>
<td>$RID$</td>
<td>unique identifier of reader</td>
</tr>
</tbody>
</table>

3.1 **The proposed protocol**

In order to solve the privacy and security problems, most research assumes that the reader and the connection between the backend databases are treated as one entity and share one secure channel when the reader and the backend database are at a fixed location, regardless of the reader's location in reality. In the real world, a storekeeper always has irregular patterns of movement to make an inventory of the goods in stock. Therefore, the mobility of the reader is necessary. However, the reader could be counterfeited if the reader combined mobile device to communicate with the database anywhere and anytime in a wireless environment. In this situation, the communication channel between the reader and the database should be assumed as insecure. In our proposed protocol, two insecure channels are considered between (1) the backend database and the reader, and (2) the reader and the tag. In the following paragraphs, we will describe our protocol shown in Figure 1. The tag stores an identification $ID$.
and a secret value $S$; and the reader stores its identifier number $RID$ and the backend
database will maintain $S_{new}$, $S_{old}$, $ID$, $RID$, plus the new and old random numbers $N_{R(old)}$ and $N_{R(new)}$. In the initial phase, each tag and backend database has the same secret
value $S$.

1. The reader generates a random number $N_R$ and then sends a request message
and $N_R$ to the tag. After receiving the message, the tag generates a random
number $N_T$ and computes $M_1 = h(S \oplus N_R \oplus N_T)$; and then the tag must send
$N_T$ and $M_1$ to the reader.

2. The reader computes $M_2 = h(RID \oplus N_R)$ and sends these messages, $(M_1, M_2,$
$N_R, N_T)$, to the backend database.

3. After receiving these messages, $(M_1, M_2, N_R, N_T)$ from the reader, the
detailed steps are listed in the following:

(a) The backend database compares whether $N_R$ is matched with $N_{R(old)}$ or
not. The backend database goes to the next step if the $N_R$ and $N_{R(old)}$ are
not matched; otherwise, the check fails.

(b) The backend database computes $h(S \oplus N_R \oplus N_T)$ from its database and
receives the random numbers $N_R$ and $N_T$. Next, the backend database
compares $M_1 = h(S \oplus N_R \oplus N_T)$ to verify whether the tag is genuine or
not.

(c) The backend database computes $h(RID \oplus N_R)$ from its database and
receives a random number $N_R$. The reader is legal, if the comparison of
$M_2 = h(RID \oplus N_R)$ is successful.

(d) The backend database generates a random number $N_{DB}$ and computes
$M_3 = h(ID \oplus N_{DB})$ and $S_{new} = h(S \oplus N_{DB} \oplus N_T)$. Next, the backend
database sends $M_3$ and $N_{DB}$ to the reader.

(e) The backend database updates $S_{new} = h(S \oplus N_{DB} \oplus N_T)$.

4. After the reader receives the messages $M_3$ and $N_{DB}$, the reader forwards it to
the tag.

5. Upon receiving message $M_3$ and $N_{DB}$, the tag computes $M_3 = h(ID \oplus N_{DB})$.
The mutual authentication will be done if the tag has successfully verified
this message. When the transaction is finished, the tag will update the value
$S_{new} = h(ID \oplus N_{DB} \oplus N_T)$.

In order to prevent tag's $ID$ being read by an attacker, the tag sends a secret value
$S$ to replace the sent $ID$ to the backend database. The secret value $S$ is updated in each
session so an attacker cannot track tag and replay the message. The backend database
stores $S_{new}$ and $S_{old}$ to prevent a DOS attack.
3.2 Evaluation of the proposed protocol

We provide the requirements of RFID system and a comparison of security characteristics in our protocol in Section 2. We summarized all of the evaluation of the proposed protocol in terms of privacy, resist attack model, and efficiency.

- The mutual authentication process.
  
  Only a legitimate tag and reader can generate the valid values, $M_1 = h(S \oplus N_R \oplus N_T)$ and $M_2 = h(RID \oplus N_R)$, because the value $S$ and $RID$ are private. In the last step, the backend server is authenticated by the tag through checking $M_3 = h(ID \oplus N_{DB})$. The backend database and the tag do all of the processes, if the mutual authentication is successfully validated.

- Resistance towards tag tracking.
  
  The tag sends messages $M_1 = h(S \oplus N_R \oplus N_T)$. The secure value $S$, random numbers $N_T$, and $N_R$ are updated in each session. Even if an attacker obtains $M_1$ it still cannot be tracked the tag since $S$, and $N_R$ are both changed; and $N_T$ is not published. Therefore, the attacker cannot trace the tag.
• Resistance towards cloning.
  For cloning of a tag, an attacker needs to forge the messages $M_1$ and $M_2$. However, the attacker cannot compute them because the attacker cannot obtain the secret value $S$ from the tag and $RID$ from the reader. As a result, cloning the tag would eventually fail.

• Resistance towards replay attacks.
  An attacker can intercept the message $M_1$, $M_2$, $NR$, and $NT$ to the database from the reader, and then replay it to the backend database. However, the authentication would fail since the attacker replays the previous $NR$, and the backend database stores the $NR_{(old)}$ equal to the previous $NR$. The backend database is stopped, if $NR_{(old)}$ is equal to the $NR$. Therefore, the attacker would fail in the attempt to be identified as valid.

• Resistance towards forward security.
  The secret value $S$ is stored in both the backend database and the tag, and will be updated in next session. Therefore, forward security attack cannot be successful, since the secret value $S$ is independent in each session and has no relationship with the previous session. Therefore, forward security attack can be avoided.

• Resistance towards denial of service attacks.
  Although an attacker can drop the message, our protocol would still be valid. The attacker can drop Steps 4 and 5, causing the value $S$ not being updated from the tag. The proposed protocol can fix it in the next section since the tag will send an old value $S$ to the backend database, therefore this tag would find that $S = S_{old}$ value and still passes the verification.

• Computation cost.
  Three hashes, $M_1$, $M_2$, and $M_3$, are needed to compute the tag, reader and the backend database.

• Traffic cost.
  In order to guarantee that the reader is legitimate, the reader should send four values, $M_1$, $M_2$, $NR$, and $NT$ to the backend database for identification. The traffic cost between the tag and the reader needs two values, $M_1$, and $NR$.

• Storage cost.
  The storage cost of the tag is $ID$ and $S$. The storage cost of the backend database is $ID$, $RID$, $S_{new}$, $S_{old}$, $NR_{(old)}$, and $NR_{(new)}$.

4. Conclusions
RFID system is popular and widely used in various applications. As stated in [16], [19], world's largest retailer Wal-mart announced that their products should be embedded RFID tags by 100 main suppliers at 2005. A global trade organization of
air transport, the International Air Transport Association (IATA) [13], [17], uses RFID to improve the baggage identification of the global airline industry. However, some organizations oppose RFID systems on the base of invasion of personal privacy (STOP RFID http://www.stoprfid.de/en/problem.html).

Using hash function and random number generator techniques, the former generates different hashed values for distinct inputs; therefore, security and privacy are achieved. The later is to ensure that the message is dynamically changed in each session in order to prevent message from being resubmitted. Consequently, the message flown among reader, tag, and database is **unreadable and changeable**; hence, the goals of security and privacy are both achieved. Conceptually, secret value S, random number N, and hash function M are used as both **static** and **dynamic** lockers within the protocol. Only a legal transaction can recognize the right values of these numbers and be able to generate the hashed value correctly. Semantically, S and N play as the first line defender and hash function M plays as the secondary defender as shown in Figure 1. Under the protocol, an attacker cannot intrude a RFID system, even if he/she can get the initial S and N; since the values of S, N, and M are subsequently changed during different sessions of a transaction dynamically.

**References**


Biography

Chia-Hui Wei received the M.S. degree in Information Management from Chaoyang University of Technology, Taiwan. Currently, she is pursing her Ph.D. degree in Computer Science from National Tsing Hua University, Taiwan. Her current research interests include RFID security, information security, and mobile communications.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC). He received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984–1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999–2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002–2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published over 100 articles on the above research fields in international journals.

Augustin Yeh-hao Chin reeived the the Ph.D. degree from University Texas at Austin. Currently, he is a professor with the Department of Computer Science from the National Tsing Hua University, Hsinchu County, Taiwan. His current research interests include database systems, algorithm design, system programming, and software engineering.