International Journal of Innovative Computing, Information and Control
Volume **8**, Number **12**, December **2012**

 ISSN 1349-4198
pp. 8341–8354

ADVANCED CONSTANTLY UPDATED RFID ACCESS CONTROL PROTOCOL USING CHALLENGE-RESPONSE AND INDEFINITE-INDEX

Zi-Yao Cheng[1], Yun Liu[1], Chin-Chen Chang[2,3,*] and Shih-Chang Chang[4]

[1]Key Laboratory of Communication and Information Systems
Beijing Municipal Commission of Education
Department of Electronic and Information Engineering
Beijing Jiaotong University
No. 3, Shang Yuan Cun, Hai Dian District, Beijing 100044, P. R. China
{ 09111024; liuyun }@bjtu.edu.cn

[2]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
*Corresponding author: alan3c@gmail.com

[3]Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan

[4]Department of Computer Science and Information Engineering
National Chung Cheng University
No. 168, University Rd., Minhsiung Township, Chiayi County 62102, Taiwan
chang.coby@gmail.com

Received September 2011; revised January 2012

Abstract. *Radio Frequency Identification (RFID), which can be implemented in various applications, has become one of the most popular technologies for remote, automatic identification. Currently, many scientific researchers are focused on this issue with the goal of achieving high security and privacy protection. Recently, Chen et al. proposed an RFID access control protocol that can satisfy the practical requirements of the authentication mechanism and infrastructure for access authorization. In this paper, we demonstrate that Chen et al.'s protocol cannot validate the legitimacy of tag when replay attacks occur. Moreover, our analysis indicated that location privacy and forward secrecy are not well protected in this protocol. To surmount the above weaknesses, we propose an advanced RFID access control protocol based on challenge-response, and its novel improvements make the proposed protocol more secure, efficient, practicable, and suitable for limited-power RFID systems.*
Keywords: RFID, Access control, Security, Privacy, Authentication

1. **Introduction.** Radio Frequency Identification (RFID) is an emerging technology that makes practical use of radio frequency for identifying objects and tracking items automatically. This kind of contact-free, automatic identification system [1-5] includes three main components, i.e., a radio frequency (RF) tag, an RF reader and a back-end database server. The objective item with an attached tag can be interrogated by the RF reader, allowing the reader to access the tag information via radio communication. According to the resident data as an index, the secret record of the corresponding tag can be inquired automatically by the reader from the database of the back-end server. RFID can be used in many applications. Specifically, a tag can be affixed to any object and used to track

and manage inventory, assets, human activity, etc. It can also be affixed to vehicles, computer equipments, books, mobile phones, etc. Meanwhile, the healthcare industry has been equipped with RFID to reduce counting, looking for things and auditing items. Many financial institutions utilize the relevant RFID technologies to track key assets and automate compliance. With recent advances in social media, RFID is being used to tie the physical world with the virtual world.

In general, RFID infrastructure contains two inherent communication channels, with one channel providing a secure connection between the reader and the back-end database server and the other channel serving as an insecure channel for the tag negotiation with the reader. From this knowledge, it is extremely possible to eavesdrop, intercept, and modify information that is transmitted over an insecure channel. Hence, the essential requirements of RFID systems focus on making an adaptive mechanism for information security [6-9]. More specifically, the mechanism must guarantee that 1) there is adequate access control so that only authorized readers can read tag secrets; 2) no one can use independent communications among the RFID components to trace the tag owner, which is the essential part for location privacy; and 3) forward secrecy protection is provided even if the secret information of the tag is compromised, i.e., the tag owner's previous locations cannot be revealed by tracking the tag's past communications. However, many previous research efforts [10-15] have distinct security and privacy drawbacks for designing RFID systems.

Originally, Weis et al. [10] proposed two simple RFID access control protocols, in which one operated as a hash-lock oriented RFID system, and the other was based on the randomized hash-lock RFID system. Another RFID hash-based access control protocol was proposed by Chien [11]. However, Chen et al. [16] discovered that there were some disadvantages for all of the above research findings. For instance, it is easy for an adversary to spoof the reader by replaying the tag response, since the insecure channel is inherently in favor of purposive eavesdropping and intercepting. So, in all probability, the adversary who eavesdrops on the information transmitted from the reader can spoof the tag in accordance with the previously explained rule. Moreover, the protection of location privacy cannot be guaranteed due to the interception of the tag response. Meanwhile, Chen et al. determined that many previous research developments [12-15] were insecure against man-in-the-middle attacks [12], spoofing attacks [12,13], and privacy violations [12,14,15]. The weak spots of these schemes were due to the fact that they were unable to protect mutual authentication [13] in view of the above situation. To fill the gaps, Chen et al. proposed a new method for RFID access control using a strategy of challenge-response and indefinite-index. They claimed that this proposed scheme protected mutual authentication and location privacy and that it also effectively prevented man-in-the-middle attacks and spoofing attacks.

However, although Chen et al.'s protocol [16] has an attractive merit with its novel strategy, in fact, it cannot achieve the security requirements as claimed. In our cryptanalysis, we can show that Chen et al.'s protocol is still vulnerable to the replay attack, in which an adversary can retransmit an intercepted message to dupe the reliable server. In addition, Chen et al.'s challenge-response approach can only guarantee the protection of mutual authentication, and, unfortunately, it has difficulty withstanding RFID privacy violation due to its tag access leakage. Also, it is impossible for the approach to make use of forward secrecy when tag uniform operations remain linkable by setting up a constant secret value.

In this paper, we propose an advanced RFID access control protocol that can remedy the aforementioned security weaknesses and decrease the overhead of the RFID system. Our significant system features can be summarized as follows:

1. Security requirements. We demonstrate that our proposed protocol can resist replay attacks, man-in-the-middle attacks, and spoofing attacks. In addition, this protocol protects location privacy such that no adversary can eavesdrop on the communication and trace the tag owner. Also, it exhibits forward secrecy in that the leakage of data stored in the tag cannot cause the compromise of past communications before the leakage occurred.
2. Constantly updated mechanism. In order to avoid the interception and modification of information transmitted via radio communication, we constructed a secure RFID mechanism for secure connection. This mechanism allows the legal tag and the valid server to update their respective secret values synchronously. This means that each access session can be performed securely, since the shared secret is updated concurrently.
3. Higher efficiency. To compare with Chen et al.'s protocol, our proposed protocol has been proven to be more efficient and its overhead decline is extremely adequate for RFID limited energy consumption.
4. Practicability. The significance of the challenge-response approach is that it makes sure that mutual authentication can be achieved between an authenticated tag and an authorized reader, thereby supporting secure access to future tags. In addition, the different representations of index provide security protection against baleful attacks for tag tracking.

The rest of this paper is organized as described below. In Section 2, we briefly review the original protocol and discuss its weaknesses. The proposed RFID access control protocol is presented in Section 3. In Section 4, we provide our security analysis, and the discussions are described in Section 5. Our remarkable conclusions are provided in Section 6.

2. Original RFID Access Control Protocol.

Chen et al. proposed a new design of the RFID access control protocol [16], and they emphasized that their novel strategy was based on indefinite-index and challenge-response. Below, we present all the details of Chen et al.'s protocol, and the specific procedures are depicted in Figure 1. In addition, we demonstrate our cryptanalysis according to the original protocol.

The following notations are used throughout all of the procedures of Chen et al.'s protocol, and introduce them first to ensure better understanding of the context:

- $index_i$: the ith tag's serial number
- key_i: the ith tag's secret value
- $h(\cdot)$: a one-way hash function
- $f_{CRC}(\cdot)$: a cyclic redundancy check function
- $E_{Key_i}(\cdot)$: an encryption of message with the secret value Key_i
- $D_{Key_i}(\cdot)$: a decryption of message with the secret value Key_i
- ω: a square matrix that is stored in all tags and issued by the back-end database server
- ω^{-1}: the inverse matrix of ω that is stored in the back-end database server
- ε: the critical response time
- $\oplus$: the exclusive-or operation

2.1. Review of Chen et al.'s RFID access control protocol.

Chen et al.'s protocol includes several steps described as follows:

Step 1: The reader generates a random number Q and transmits it to the tag.

Step 2: After receiving the random number Q, the tag selects another random number R and computes $\gamma = h(Key_i \oplus Q \oplus R)$ by utilizing its secret key Key_i and received random number Q. The tag's serial number is the key of authentication execution

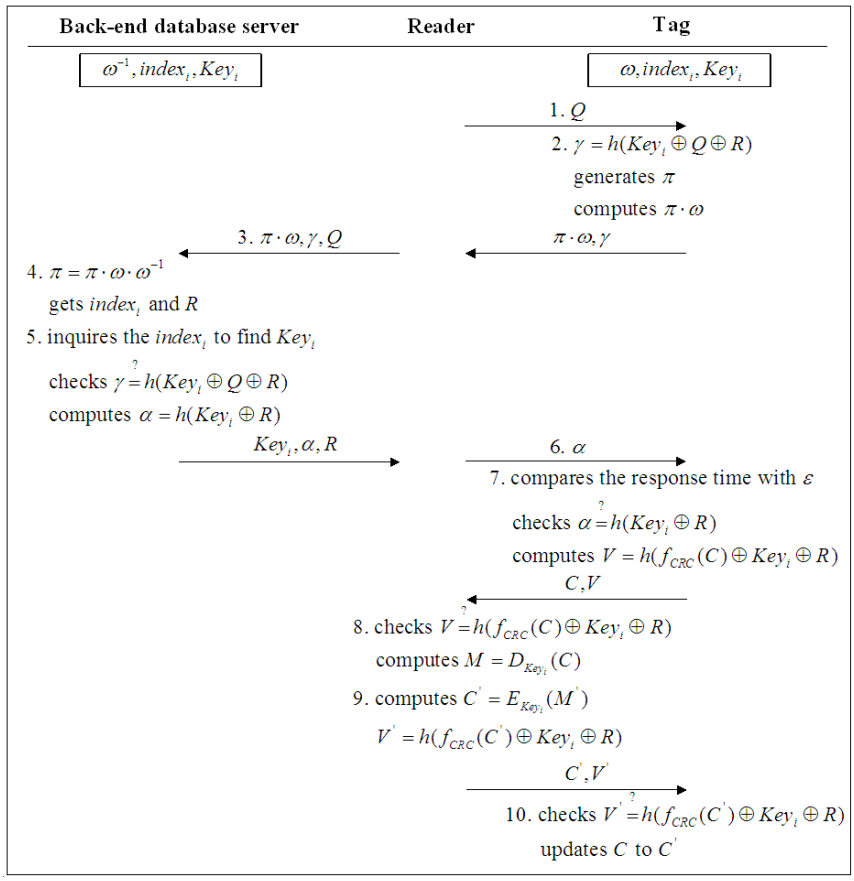

FIGURE 1. Chen et al.'s protocol

between the tag and the back-end database server. The serial number must be represented differently in each session in order to keep the tag's location privacy, and it cannot be sent over an insecure channel directly. Hence, the tag's serial number $index_i$ can be protected with a matrix π as follows:

a) Design the $index_i$ as a coordinate (x_i, y_i), and it can be randomly represented, since there are indefinite possibilities to select two un-parallel lines, where the two un-parallel lines intersect at the coordinate (x_i, y_i) and each line can be determined by two assured points.
b) Randomly select two points on the first line, termed (x_1, y_1) and (x_2, y_2), respectively. Similarly, the other two points, (x_3, y_3) and (x_4, y_4), are also selected freely on the second line.
c) The matrix π consists of all these four points and the two random numbers, such as:

$$\pi = \begin{bmatrix} x_1 & y_1 & x_2 \\ y_2 & x_3 & y_3 \\ x_4 & y_4 & Q \oplus R \end{bmatrix}.$$

d) To protect the matrix π, the tag calculates a matrix product $\pi \cdot \omega$ and forwards the tag's response message $\{\pi \cdot \omega, \gamma\}$ to the reader.

Step 3: After receiving the tag's response message, the reader passes it along with its selected random number Q to the back-end database server.

Step 4: When the message $\{\pi \cdot \omega, \gamma, Q\}$ has been received by the back-end database server, the server can derive the matrix π by utilizing the following function such that $\pi = (\pi \cdot \omega) \cdot \omega^{-1}$. Thus, the four pre-determined points (x_1, y_1), (x_2, y_2), (x_3, y_3)

and (x_4, y_4), can be obtained, and it is easy to derive the pair of values (x_i, y_i) intersected by the two un-parallel lines and the random number R from the matrix π.

Step 5: Upon obtaining the tag's $index_i$, the back-end database server can retrieve the corresponding secret value Key_i from its database and verify that $\gamma \stackrel{?}{=} h(Key_i \oplus Q \oplus R)$. If it is, the tag is validated and truly issued by the server. After that, the back-end database server computers $\alpha = h(Key_i \oplus R)$ and forwards the message $\{Key_i, \alpha, R\}$ to the reader.

Step 6: After receiving the message from the back-end database server, the reader must forward the parameter α to the tag.

Step 7: When the tag receives the parameter α, it first checks whether the response time is less than the critical response time ε. If it is satisfied, the tag can verify that $\alpha \stackrel{?}{=} h(Key_i \oplus R)$ to check the validity of the reader. In case of equality, the reader has been authenticated to access the ciphertext C stored in the tag, where the ciphertext is associated with a check value $V = h(f_{CRC}(C) \oplus Key_i \oplus R)$. Next, the tag sends the message $\{C, V\}$ to the reader.

Step 8: Once the message $\{C, V\}$ is received, the reader checks the ciphertext integrity by comparing whether the received V is equal to the value of $h(f_{CRC}(C) \oplus Key_i \oplus R)$. If it is, the reader can decrypt the ciphertext C with the secret value Key_i such that $M = D_{Key_i}(C)$.

Step 9: When the reader attempts to modify data M' to the tag, it encrypts the plaintext M' with the secret value Key_i such that $C' = E_{Key_i}(M')$. Then, the reader sends the message $\{C', V'\}$ to the tag, where $V' = h(f_{CRC}(C') \oplus Key_i \oplus R)$.

Step 10: Upon receiving the message $\{C', V'\}$, the tag checks the ciphertext integrity by comparing whether the received V' is equal to the value of $h(f_{CRC}(C') \oplus Key_i \oplus R)$. If it is, the record of ciphertext in the tag is updated from C to C'.

2.2. **Weaknesses of Chen et al.'s RFID access control protocol.** Compared with previous protocols [10,11], Chen et al. claimed that their new protocol provided technical RFID access control by incorporating a challenge-response mechanism to avoid replay attacks. However, Safkhani et al. [17] recently discovered that Chen et al.'s RFID access control protocol is still vulnerable and can be attacked easily. In the following subsections, our cryptanalysis further illustrates that their protocol cannot withstand the replay attack and also cannot satisfy the requirements for location privacy and forward secrecy in the RFID security mechanism. Hence, we introduce the weaknesses of Chen et al.'s RFID access control protocol below.

2.2.1. *Replay attack.* In Chen at al.'s RFID access control protocol, an adversary can successfully intercept a message and replay the message to impersonate the tag. The detailed procedures refer to [17]. As an adversary eavesdrops on an independent session between the tag and the reader, he or she can store the tag's response message $\{\pi \cdot \omega, \gamma\}$ transmitted in Step 2 and then dupe the reader into believing her or his validity by replaying this message to act as the expected message $\{\pi' \cdot \omega, \gamma'\}$ in the next session. With the expect of the adversary, when a new session begins, the back-end database server will receive a message $\{\pi' \cdot \omega, \gamma', Q'\}$ in Step 3, where γ' indeed is still the value of γ and $\pi' = \pi$. Upon deriving the matrix π' in Step 4 such that $\pi' = (\pi' \cdot \omega) \cdot \omega^{-1} = \pi$, the back-end database server can derive $index_i$ correctly to acquire the related Key_i from the database and compute the random number $R' = R \oplus Q \oplus Q'$. Since each tag's shared secret Key_i is defined in advance and always has a definite value, γ' can be verified that $\gamma' = h(Key_i \oplus Q' \oplus R') = h(Key_i \oplus Q' \oplus R \oplus Q \oplus Q') = h(Key_i \oplus Q \oplus R) = \gamma$. Therefore,

the adversary can intercept the message transmitted in Step 2 and replay it to make the back-end database server believe her or his validity.

2.2.2. *Location privacy.* Chen et al.'s RFID security infrastructure cannot protect location privacy, since the data transmitted in their approach can be used to trace the tag. If we assume that an adversary intercepts the message $\{C', V'\}$ transmitted in Step 9 and replaces it with a fake message $\{C^*, V^*\}$, after that, the tag can check that V^* is not equal to $h(f_{CRC}(C^*) \oplus Key_i \oplus R)$. In other words, the ciphertext integrity check cannot be done, which leads to the inability to update the ciphertext in Step 10, whereby the tag will have to take the original ciphertext C to execute the protocol for the reader's access. Thus, the adversary has the opportunity to trace the tag when it forwards the ciphertext C again.

2.2.3. *Forward secrecy.* In fact, RFID security requirements must include the protection of forward secrecy even if the tag has been compromised by an adversary, so the adversary cannot use the compromised secret data or information to eavesdrop or trace the tag's operations established previously. However, we discovered that the secret value Key_i for the ith tag is always definite in Chen et al.'s protocol, which does not offer a security mechanism for each legal tag and the back-end database server to update their respective shared secret synchronously. This simply means that, if the secret value Key_i stored in the ith tag is compromised, the adversary has the ability to trace the tag's preceding operations and communications.

3. **Proposed RFID Access Control Protocol.** The proposed protocol performs the challenge-response approach to guarantee mutual authentication without the aforementioned drawbacks, and we also utilized the same RFID structure and components as Chen et al.'s protocol. In order to further improve the security and efficiency of the original protocol, our design has an evident merit in that each tag is allowed to update its own secret value for individual private communication, and the corresponding server is able to accomplish the same process synchronously. The proposed protocol is presented as follows, and the specific steps are depicted in Figure 2. In the figure and throughout the paper, we utilize the same notations that were used in Chen et al.'s protocol.

Before describing the following protocol steps, we distinguish the significance of our additional notations involved in the protocol below:

- Key_i: the current secret value shared between the tag and the back-end database server, which was stored initially in the found database and the tag memory.
- Key_{i-old}: the old secret value shared between the tag and the back-end database server for the last access session, which was recorded initially by the server, where $Key_{i-old} = Key_i$ at beginning in the found database.
- ACK: the acknowledgment message, which allows the reader to announce that the tag access has been accomplished.

Next, we introduce the specific steps of our proposed protocol as follows:

Step 1: The reader generates a random number Q and transmits it to the tag.

Step 2: After receiving the random number Q, the tag selects another random number R and computes $\gamma = h(Key_i \oplus Q \oplus R)$ by utilizing its secret key Key_i and the received random number Q. The tag's serial number is the key of authentication between the tag and the back-end database server. In order to keep the tag's location private, the serial number must be represented differently in each session, and it cannot be sent over an insecure channel directly. Hence, the tag's serial number $index_i$ can be protected with a matrix π as follows:

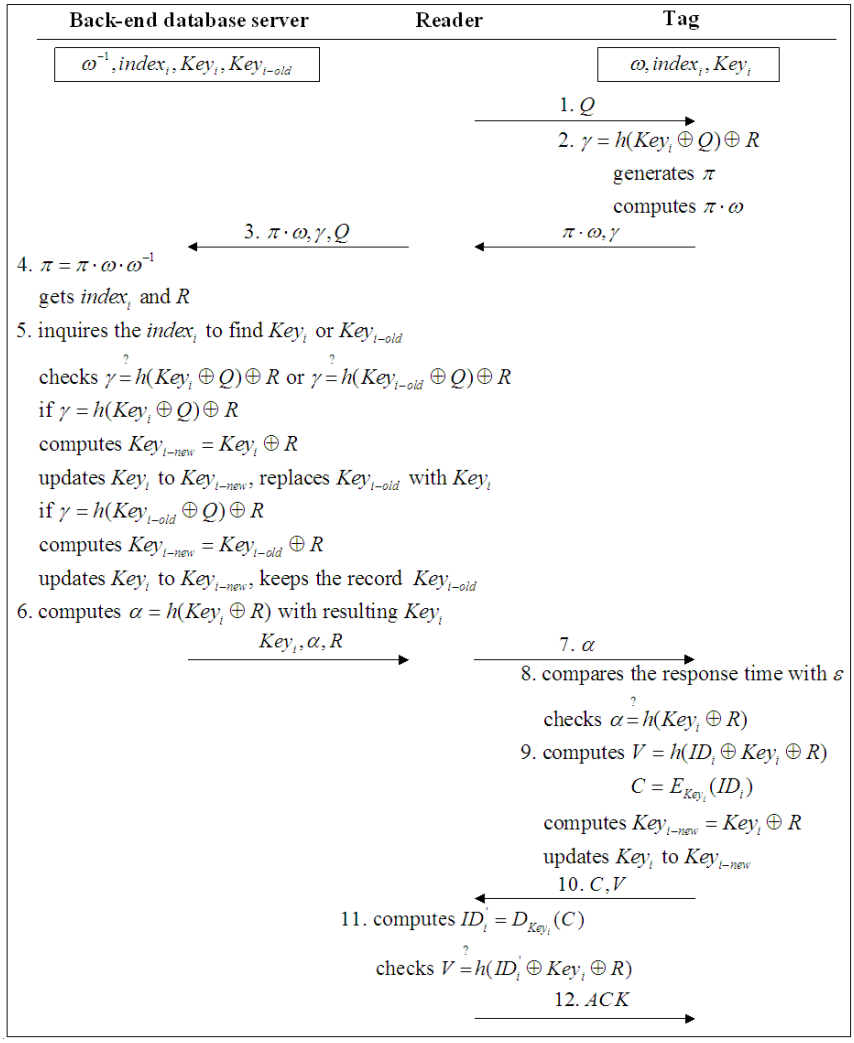

FIGURE 2. Our proposed scheme

a) Design the $index_i$ as a coordinate (x_i, y_i), and it can be randomly represented, since there are indefinite possibilities to select two un-parallel lines, where the two un-parallel lines intersect at the coordinate (x_i, y_i) and each line can be determined by two assured points.
b) Randomly select two points on the first line, termed (x_1, y_1) and (x_2, y_2), respectively. Similarly, the other two points, (x_3, y_3) and (x_4, y_4), are also selected freely on the second line.
c) The matrix π consists of all these four points and the two random numbers, such as:

$$\pi = \begin{bmatrix} x_1 & y_1 & x_2 \\ y_2 & x_3 & y_3 \\ x_4 & y_4 & Q \oplus R \end{bmatrix}.$$

d) To protect the matrix π, the tag calculates a matrix product $\pi \cdot \omega$ and forwards the tag's response message $\{\pi \cdot \omega, \gamma\}$ to the reader.

Step 3: After receiving the tag's response message, the reader passes it along with its selected random number Q to the back-end database server.

Step 4: When the message $\{\pi \cdot \omega, \gamma, Q\}$ has been received by the back-end database server, the server can derive the matrix π by utilizing the following function such that

$\pi = (\pi \cdot \omega) \cdot \omega^{-1}$. Thus, the four pre-determined points (x_1, y_1), (x_2, y_2), (x_3, y_3) and (x_4, y_4), can be obtained, and it is easy to derive the pair of values (x_i, y_i) intersected by the two un-parallel lines and the random number R from the matrix π.

Step 5: Upon obtaining the tag's $index_i$, the back-end database server can retrieve the corresponding secret value Key_i or Key_{i-old} stored in its database and verify that $\gamma \stackrel{?}{=} h(Key_i \oplus Q) \oplus R$ or $\gamma \stackrel{?}{=} h(Key_{i-old} \oplus Q) \oplus R$. Thus, we demonstrate the two cases as follows:

I. If it complies with the equation $\gamma = h(Key_i \oplus Q) \oplus R$, the server will compute $Key_{i-new} = Key_i \oplus R$ to be the next session secret recorded by itself. Meanwhile, in the found database, the server will update Key_i to Key_{i-new} and replace Key_{i-old} with Key_i.

II. If it complies with the equation $\gamma = h(Key_{i-old} \oplus Q) \oplus R$, the server will compute $Key_{i-new} = Key_{i-old} \oplus R$ to be the next session secret recorded by itself. Meanwhile, in the found database, the server will update Key_i to Key_{i-new} and cannot replace the record Key_{i-old}, which should be kept for authentication in the next session.

Step 6: If either case can be done, the tag is validated and truly issued by the server. This means that the resulting Key_i has already been identified as Key_i or Key_{i-old}. Hence, the back-end database server computes $\alpha = h(Key_i \oplus R)$ by using the resulting Key_i and forwards the message $\{Key_i, \alpha, R\}$ to the reader.

Step 7: After receiving the message from the back-end database server, the reader must forward the parameter α to the tag.

Step 8: When the tag receives the parameter α, it first checks whether the response time is less than the critical response time ε. If it is satisfied, the tag can verify that $\alpha \stackrel{?}{=} h(Key_i \oplus R)$ to check the validity of the reader. In case of equality, the reader can prove its validity for the tag access.

Step 9: Until now, mutual authentication has been done between the tag and the back-end database server. After that, since the reader has been authorized to access the data and information stored in the tag, the tag computes $V = h(ID_i \oplus Key_i \oplus R)$ with its identity ID_i, and encrypts the plaintext ID_i with the secret value Key_i such that $C = E_{Key_i}(ID_i)$. Then, the tag computes $Key_{i-new} = Key_i \oplus R$ and updates its secret value from Key_i to Key_{i-new}.

Step 10: After the shared secret value has been updated synchronously, the tag sends a message that contains the ciphertext C and the plaintext check value V to the reader.

Step 11: Upon receiving the message $\{C, V\}$, the reader can decrypt the ciphertext C by using the secret value Key_i, such that $ID_i' = D_{Key_i}(C)$, and then the reader checks whether the received V is equal to the value of $h(ID_i' \oplus Key_i \oplus R)$. If it is, the reader has truly received the identity of the tag, and the correct access authorization has been done.

Step 12: As the reader achieves the tag access, it publishes the acknowledgment message ACK to the tag.

4. **Security Analysis.** A basic problem in the design of RFID systems is formal security proof for specific cryptographic protocols. Without a constantly updated RFID security mechanism, Chen et al.'s protocol [16] cannot protect the security requirements as they claimed. In this section, we provide an in-depth analysis, which is necessary for understanding the security and functionality requirements, and we discuss how our proposed

protocol fixes the above-mentioned security weaknesses. Therefore, we present six claims to demonstrate our security concerns, as follows:

Claim 1. In this proposed protocol, all the procedures can be performed securely provided by the authentication proof based on BAN logic.

Proof: In our proposed protocol, we use BAN logic, a logical analysis proposed by Burrows et al. [18] to verify authentication operations. Owing to the analytical procedures of BAN logic, each round of the protocol must be transformed into idealized form. In the following, we first introduce the basic notation of BAN logic.

$M \overset{X}{\Leftrightarrow} N$: Formula X is a secretly known only to M and N. Only M and N may use X to prove their identities to one another.

Next, we provide the logical postulates to demonstrate that the tag T and the back-end database server S can mutually authenticate as follows.

T **believes fresh** (Q).
S **believes fresh** (R).
T **believes** $T \overset{Key_i}{\Leftrightarrow} S$.
T **believes** S **believes** $T \overset{Key_i}{\Leftrightarrow} S$.
S **believes** $T \overset{Key_i}{\Leftrightarrow} S$.
S **believes** T **believes** $T \overset{Key_i}{\Leftrightarrow} S$.

In the proposed protocol, there are four messages that used to achieve the mutual authentication. And we use BAN logic to analysis our protocol, illustrated in Figure 2, there are three components involved such as the tag T, the reader B and the back-end database server S. Next, we idealize the protocol as follows.

Message 1. $T \to B$: $\pi \cdot \omega$, $h(Key_i \oplus Q) \oplus R$.
Message 2. $B \to S$: $\pi \cdot \omega$, $h(Key_i \oplus Q) \oplus R$, Q.
Message 3. $S \to B$: Key_i, $h(Key_i \oplus R)$, R.
Message 4. $B \to T$: $h(Key_i \oplus R)$.

Before starting to analyze our protocol, we first make the following assumptions:

$A1$. T **believes** $T \overset{h()}{\Leftrightarrow} S$.
$A2$. T **believes** (B **controls fresh** (Q)).
$A3$. T **believes** (T **controls fresh** (R)).
$A4$. T **believes** (S **believes** $T \overset{Key_i}{\Leftrightarrow} S$).
$A5$. S **believes** $T \overset{h()}{\Leftrightarrow} S$.
$A6$. S **believes** (T **controls fresh** (R)).
$A7$. S **believes** (T **controls** ω^{-1}).
$A8$. S **believes** (B **controls fresh** (Q)).
$A9$. S **believes** (T **believes** $T \overset{Key_i}{\Leftrightarrow} S$).

Then, we analyze the idealized form of our proposed protocol using the above assumptions and rules of BAN logic. Details of the logic proof are presented as follows.

B receives *Message* 1. The rules show that

B **sees** $\{\pi \cdot \omega, h(Key_i \oplus Q) \oplus R\}$. (Statement 1)

We break conjunctions and produce

B **believes** T **said** $\pi \cdot \omega$, (Statement 2)
B **believes** T **said** $h(Key_i \oplus Q) \oplus R$. (Statement 3)

Next, B forwards Message 2 to S. The rules show that

S **sees** $\{\pi \cdot \omega, h(Key_i \oplus Q) \oplus R, Q\}$. (Statement 4)

We break conjunctions and produce:

S **believes** B **said** $\pi \cdot \omega$, (Statement 5)

S **believes** B **said** $h(Key_i \oplus Q) \oplus R$, (Statement 6)
and
S **believes** B **said** Q. (Statement 7)
By $A8$ and Statement 7, we utilize the nonce-verification rule to deduce
S **believes** Q. (Statement 8)
By Statement 2 and Statement 5, the message-meaning rule works out that
S **believes** T **said** $\pi \cdot \omega$. (Statement 9)
By $A7$ and Statement 9, we apply the message-meaning rule to derive
S **believes** T **said** π. (Statement 10)
By$A6$, $A8$ and Statement 10, we employ the nonce-verification rule to deduce
S **believes** π. (Statement 11)
By Statement 3 and Statement 6, the message-meaning rule is used to obtain
S **believes** T **said** $h(Key_i \oplus Q) \oplus R$. (Statement 12)
By $A6$ and Statement 12, we apply the message-meaning rule to derive
S **believes** T **said** $h(Key_i \oplus Q)$. (Statement 13)
By $A5$ and Statement 13, the message-meaning rule can be used to obtain
S **believes** T **said** $Key_i \oplus Q$. (Statement 14)
By Statement 8 and Statement 14, we apply the message-meaning rule to deduce
S **believes** T **said** Key_i. (Statement 15)
By $A9$ and Statement 15, the nonce-verification rule applies and yields
S **believes** Key_i. (Statement 16)
After that, B receives *Message* 3. The annotation rule yields that
B **sees** $\{Key_i, h(Key_i \oplus R), R\}$. (Statement 17)
We break conjunctions and produce below:
B **believes** S **said** Key_i, (Statement 18)
B **believes** S **said** $h(Key_i \oplus R)$, (Statement 19)
and
B **believes** S **said** R. (Statement 20)
Then, B forwards Message 4 to T. The rules show that
T **sees** $\{h(Key_i \oplus R)\}$. (Statement 21)
In the following, we produce that:
T **believes** B **said** $h(Key_i \oplus R)$. (Statement 22)
By Statement 19 and Statement 22, we utilize the message-meaning rule to deduce
T **believes** S **said** $h(Key_i \oplus R)$. (Statement 23)
By $A1$ and Statement 23, the message-meaning rule works out that
T **believes** S **said** $Key_i \oplus R$. (Statement 24)
By $A3$ and Statement 24, we employ the message-meaning rule to obtain
T **believes** S **said** Key_i. (Statement 25)
By $A4$ and Statement 25, the nonce-verification rule applies and yields
T **believes** Key_i. (Statement 26)

Based on Statement 16 and Statement 26, we prove that this proposed protocol can achieve the mutual authentication requirement correctly.

Claim 2. Assume an adversary, named $\boldsymbol{A}$, replays the intercepted message in the cryptographic system. The proposed protocol can resist the replay attack.

Proof: Suppose that $\boldsymbol{A}$ monitors the tag's communication and intercepts the message $\{\pi \cdot \omega, \gamma\}$ in Step 2 for replaying intention. Without loss of generality, the back-end database server will receive a message $\{\pi' \cdot \omega, \gamma', Q'\}$ in Step 4 when the next access session starts, in which $\pi' = (\pi' \cdot \omega) \cdot \omega^{-1} = \pi$ makes $\boldsymbol{A}$ derive the correct serial number $index_i$ to find Key_i or Key_{i-old} stored in the found database. To surmount the aforementioned

weaknesses in Chen et al.'s protocol, we refer to our enhanced operations whereby $\boldsymbol{A}$'s replaying intention can be discovered in Step 5, as described in the two cases that follow.

In the first case, due to our constantly updated mechanism, the current secret value Key_i has been updated. Moreover, the replaying message consists of the old secret value Key_{i-old} and original random number R. It is clear that the back-end database server can check that $\gamma' \neq h(Key_i \oplus Q') \oplus R'$.

In the second case, since the old record Key_{i-old} is still stored in the found database, $\boldsymbol{A}$ seems to be able to make such a replay attack. However, since the random number R' complies with the equation $R' = R \oplus Q \oplus Q'$, the back-end database server can also check that $\gamma' \neq h(Key_{i-old} \oplus Q') \oplus R'$.

Thus, the replaying intention will fail in this RFID security mechanism. Our proposed protocol truly can prevent such a replay attack.

Claim 3. If adversary $\boldsymbol{A}$ monitors the private connection between the tag and the back-end database server, the proposed protocol still can withstand the risk of the man-in-the-middle attack.

Remark 4.1. *In order to facilitate understanding, the emphasis on the man-in-the middle attack is in terms of an eavesdropping attack in which the adversary makes independent connections with the parties, intercepts all messages, and publishes different messages between the related parties, making them believe that they are communicating securely with each other. The proof is given below.*

Proof: Suppose that $\boldsymbol{A}$ obtains the message $\{\pi \cdot \omega, \gamma\}$ by eavesdropping on the tag's communication; although the random number Q can be intercepted easily by $\boldsymbol{A}$ in Step 1, $\boldsymbol{A}$ still cannot guess any correct information from the obtained message. The reason is that the parameter γ entirely contains a one-way hash function $h(Key_i \oplus Q)$ and a random number R which is transformed to be hidden in the matrix product $\pi \cdot \omega$, so the corresponding value of each individual is changeable due to the randomly selected number R and constantly updated secret value Key_i. Without knowing the above details of the legal tag's communication message, $\boldsymbol{A}$ cannot pass the back-end database server's specific verification in Step 5. Similarly, $\boldsymbol{A}$ also cannot imitate a dependable message based on the response α to dupe the tag into believing her or his trustworthiness since he or she cannot pass the verification in Step 8, because the related one-way hash function $h(Key_i \oplus R)$ can protect security reliability against $\boldsymbol{A}$'s hostile attack. In essence, adversary $\boldsymbol{A}$ cannot completely control the entire conversation between the two parties. Thus, in our proposed protocol, a man-in-the-middle attack can be prevented, as indicated in the above proof.

Claim 4. Assume adversary $\boldsymbol{A}$ attempts to pretend to be a legal participant in order to make a spoofing attack on the RFID system; in such a case, the proposed protocol can resist this kind of spoofing attack.

Proof: In our RFID security protocol, the legal tag and the valid reader can negotiate with each other based on mutual authentication with the shared secret value Key_i and the random number Q or R. Since our system is constantly updated, only the legal tag can protect its serial number $index_i$ with a matrix product $\pi \cdot \omega$ and calculate the correct γ to pass the back-end database server's verification with valid Key_i and R in Step 4. Meanwhile, only the legal reader can acquire the correct message $\{Key_i, \alpha, R\}$ to pass the tag's verification within the response time ε in Step 8. No matter how $\boldsymbol{A}$ obtains communication messages such as $\{\pi \cdot \omega, \gamma\}$ and $\{\alpha\}$, he or she still cannot deceive the other endpoint in this RFID security mechanism without knowing the current and formal Key_i and R. As just mentioned, adversary $\boldsymbol{A}$ has no way to make a fake tag or reader to spoof the other side in this proposed protocol.

Claim 5. If adversary $\boldsymbol{A}$ collects the tag's different message on purpose, he can keep

track of the tag's owner in terms of the history record. However, the proposed protocol can protect the tag's location privacy effectively.

Proof: As we know, our challenge-response based RFID infrastructure still uses the significant design of indefinite-index in Chen et al.'s protocol. It is implied that the tag's serial number $index_i$ can be represented differently in each session, since there are infinite possibilities to freely select two un-parallel lines that intersect at the coordinate (x_i, y_i) with four randomly chosen points in Step 2. Hence, for each session, the matrix is changeable by rearranging these four points and random numbers Q and R. Furthermore, the weakness of location privacy in Chen et al.'s protocol is evident in that, when adversary $\boldsymbol{A}$ replaces the message $\{C', V'\}$ with a fake message $\{C^*, V^*\}$ to interrupt the connection between the tag and the reader, the reappearance message for reader's access can be used to trace the tag's owner. On the contrary, in the proposed protocol, the tag's secret identity is encrypted by the secret value Key_i. Moreover, the secret value Key_i is always updated for each access session so that the message $\{C, V\}$ becomes uninterpretable for $\boldsymbol{A}$'s monitor. Whenever the message transmitted in this security mechanism is intercepted and modified, adversary $\boldsymbol{A}$ still cannot use it to trace the tag's owner. Therefore, in the proposed protocol the protection of the tag's location privacy can be guaranteed successfully.

Claim 6. The proposed protocol can achieve the protection of forward secrecy.

Proof: The messages transmitted by the tag and the back-end database server are well protected against compromising secret information. Thus, adversary $\boldsymbol{A}$ cannot retrieve the secret information from the messages such that $\{\pi \cdot \omega, \gamma\}$, $\{\alpha\}$ and $\{C, V\}$. Moreover, although the secret value Key_i can be compromised by $\boldsymbol{A}$, he or she cannot utilize the current secret Key_i to derive the old secret Key_{i-old} for obtaining the tag's past communications. This is because that the tag's secret value can be updated, and the random number Q and R are freely generated by the legal tag and reader, respectively for each access session. Hence, it is impossible for adversary $\boldsymbol{A}$ to trace the tag's preceding communications by using the compromised current secret knowledge.

5. **Discussions.** In this section, we present the advantages of efficiency and functionality that the proposed protocol has over the previously published protocol [16]. More precisely, the merit of efficiency is by virtue of the performance comparison, in which we show the detailed computation cost in Table 1. It is obvious that the computation cost contains four different operations, i.e., the exclusive-or operation (xor), the one-way hash function ($hash$), the symmetric encryption operation (enc), and the symmetric decryption

Table 1. Comparison of computation cost

Items	Computation cost		
	Components	Chen et al.'s protocol [16]	Ours
Reader authenticates tag	Tag	2*xor*+1*hash*	2*xor*+1*hash*
	Reader	0	0
	Server	3*xor*+1*hash*	4*xor*+1*hash*
Tag authenticates reader	Tag	1*xor*+1*hash*	1*xor*+1*hash*
	Reader	0	0
	Server	1*xor*+1*hash*	1*hash*
Tag access	Tag	2*xor*+2*hash*	1*xor*+1*hash*+1*enc*
	Reader	4*xor*+2*hash*+1*dec*+1*enc*	2*xor*+1*hash*+1*dec*
	Server	0	0
Total	Three components	13*xor*+8*hash*+1*dec*+1*enc*	10*xor*+6*hash*+1*dec*+1*enc*

TABLE 2. Comparison of security requirements and functionality

Items	Chen et al.'s protocol [16]	Ours
Withstanding the replay attack	No	Yes
Withstanding the spoofing attack	Yes	Yes
Withstanding the man-in-the-middle attack	Yes	Yes
Protection of location privacy	No	Yes
Protection of forward secrecy	No	Yes
Mutual authentication	Yes	Yes
Challenge-response approach	Yes	Yes
Strategy of indefinite-index	Yes	Yes

operation (*dec*). Moreover, we introduce the security and functionality merits by making comparison with the related protocol in Table 2.

As stated earlier, we also utilize the challenge-response based cryptographic system similar to Chen et al.'s protocol to confirm the mutual authentication and the execution of access control. From the view of efficiency, it can be seen in Table 1 that the computation cost of our protocol includes seven exclusive-or operations and four hashing operations after the mutual authentication has been done, which is the same energy consumption as Chen et al.'s protocol. However, when performing the tag access, our protocol utilizes only three exclusive-or operations, two hashing operations, one symmetric encryption operation and one symmetric decryption operation. The result is that the total computation cost of our protocol is less than that for Chen et al.'s protocol. This means that our protocol is more efficient and has lower energy consumption than the protocol produced by previous research efforts.

In Table 2, it is evident that our protocol has the same functionality characteristics as Chen et al.'s protocol, i.e., it achieves mutual authentication, exploits the challenge-response approach, and uses the strategy of indefinite-index. In addition, we have shown that our protocol remedies the corresponding weaknesses by withstanding the replay attack, protecting location privacy, and protecting forward secrecy. Compare with the related protocol, the proposed protocol is more efficient and practical for the implementation of RFID systems. In addition, it can be performed easily in such a security RFID mechanism for which we developed an advanced method to ensure its compliance.

6. **Conclusions.** In this paper, we propose an advanced, constantly-updated RFID access control protocol based on challenge-response and indefinite-index. In our protocol, we have achieved the goal of proposing both an RFID authentication protocol and a security access control mechanism. The evident merit of our protocol that its security mechanism can protect transmitted information against vicious eavesdropping, intercepting, and modification, since an adversary who attempts to attack the RFID system will fail no matter what approach he or she uses. Our protocol enhances the security and privacy of tag identification and access reading operations, which are still vulnerable in Chen et al.'s protocol. The security analysis demonstrates that our protocol can withstand the spoofing attacks and the man-in-the-middle attacks; in addition, it has security improvements, including withstanding replay attacks, protecting location privacy, and protecting forward secrecy.

Also, we presented a performance analysis to show that our protocol has higher efficiency than the previous protocol [16]. Due to its lower computation cost and energy consumption, the proposed protocol is very suitable for RFID systems that are necessarily equipped with light-weight devices. Hence, the proposed protocol can be applied to practical and secure RFID mechanisms that have high safety and performance requirements.

Acknowledgment. This work is partially supported by National High Technology and Development Program (863 Program) of China under Grant No. 2011AA010104-2, National Natural Science Foundation of China under Grant 61071076, the Academic Discipline and Postgraduate Education Project of Beijing Municipal Commission of Education, the Fundamental Research Funds for the Central Universities under Grant 2012YJS023. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Y. Xiao, X. Shen, B. Sun and L. Cai, Security and privacy in RFID and applications in telemedicine, *IEEE Communication Magazine*, vol.44, no.4, pp.64-72, 2006.

[2] C. M. Roberts, Radio frequency identification (RFID), *Computers & Security*, vol.25, no.1, pp.18-26, 2006.

[3] 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.

[4] C. C. Tan, S. Bo and L. Qun, Secure and serverless RFID authentication and search protocols, *IEEE Transactions on Wireless Communications*, vol.7, no.4, pp.1400-1407, 2008.

[5] A. X. Liu and L. A. Bailey, PAP: A privacy and authentication protocol for passive RFID tags, *Computer Communications*, vol.32, no.7-10, pp.1194-1199, 2009.

[6] T. Cao and P. Shen, Cryptanalysis of some RFID authentication protocols, *Journal of Communications*, vol.3, no.7, pp.20-27, 2008.

[7] S. Y. Kang, G. G. Lee and I. Y. Lee, A study on secure RFID mutual-authentication scheme in pervasive computing environment, *Computer Communications*, vol.31, no.18, pp.4248-4254, 2008.

[8] E. K. Ryu and T. Takagi, A hybrid approach for privacy-preserving RFID tags, *Computer Standard & Interfaces*, vol.31, no.4, pp.812-815, 2009.

[9] T. C. Yeh, C. H. Wu and Y. M. Tseng, Improvement of the RFID authentication scheme based on quadratic residues, *Computer Communications*, vol.34, no.3, pp.337-341, 2011.

[10] S. Weis, S. Sarma, R. Rivest and D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, *Proc. of the 1st International Conference on Security in Pervasive Computing*, Boppard, Germany, pp.50-59, 2004.

[11] H. Y. Chien, Secure access control schemes for RFID systems with anonymity, *Proc. of the 7th International Conference on Mobile Data Management*, Nara, Japan, pp.96-96, 2006.

[12] T. Dimitriou, A lightweight RFID protocol to protect against traceability and cloning attacks, *Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp.59-66, 2005.

[13] J. Yang, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, *Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp.149-153, 2004.

[14] G. Avoine and P. Oechslin, A scalable and provably secure hash based RFID protocol, *Proc. of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security*, pp.110-114, 2005.

[15] S. M. Lee, Y. J. Hwang, D. H. Lee and J. I. Lim, Efficient authentication for low-cost RFID systems, *Proc. of International Conference on Computational Science and Its Applications*, pp.619-627, 2005.

[16] Y. Y. Chen, M. L. Tsai and J. K. Jan, The design of RFID access control protocol using the strategy of indefinite-index and challenge-response, *Computer Communications*, vol.34, no.3, pp.250-256, 2011.

[17] M. Safkhani, N. Bagheri and M. Naderi, Cryptanalysis of Chen et al.'s RFID access control protocol, *Cryptology ePrint Archive*, 2011.

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