ISSN 1392 – 124X, ISSN 2335 – 884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2013, Vol.42, No.2

Secure Indefinite-Index RFID Authentication Scheme with Challenge-Response Strategy

Wen-Chung Kuo[1], Bae-Ling Chen[2,*], Lih-Chyau Wuu[3]

[1] *Department of Computer Science and Information Engineering, National Yunlin University of Science &Technology No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan e-mail: simonkuo@yuntech.edu.tw*

[2] *Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan e-mail: chenbl@yuntech.edu.tw*

[3] *Institute of Computer Science and Information Engineering, National Yunlin University of Science and Technology No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan wuulc@yuntech.edu.tw*

crossref http://dx.doi.org/10.5755/j01.itc.42.2.1615

Abstract. In 2011, Chen, Tsai, and Jan proposed a radio frequency identification (RFID) access control protocol for a low-cost RFID system (CTJ-scheme for short). They claimed that their scheme not only guarantees mutual authentication and location privacy but also resists man-in-the-middle, spoofed reader, and spoofed tag attacks. However, in late 2011, Chen *et al.* pointed out that CTJ-scheme is vulnerable to a spoofed reader attack and did not provide any protection against denial-of-service (DoS) attacks. In addition, our research also found that under Chen *et al.*'s spoofed reader attack, tag contents can be surreptitiously altered by replaying message. In this paper, we analyze the weaknesses of CTJ-scheme and propose an enhanced scheme. According to our analyses, the proposed scheme is secure against the aforementioned DoS, spoofed reader, and modification attacks, while maintaining the merits of the original scheme..

Keywords: radio frequency identification (RFID), access control, mutual authentication, security, privacy.

1. Introduction

RFID is a contactless technology using radio signals to exchange data between a tagged object, and a reader for the purpose of identifying and tracking the object. A basic RFID system consists of RF tags, RF readers, and a backend database server. To start the identification, a reader broadcasts a radio frequency signal for querying the data stored on the tags. After receiving this request signal, each tag responds by transmitting the corresponding data back to the reader. The reader then forwards the received tag response to its backend server for further processing, including tag identification and corresponding information retrieval. Since the radio channel is open and insecure, information security is a fundamental problem that impacts RFID system applications. The most important security issue of an RFID system is how to protect the content of a tag from unauthorized accesses.

Access control is used to authenticate a user who is able to interact with resource. In terms of the security of current RFID systems, many access control protocols have been proposed in last decade [1-11] with the aim to provide secure communication between a server/reader and a tag. Due to the limitations of a passive RFID tag, such as, computational ability, storage space, and power constraints, designing an efficient and secure authentication protocol is still a great challenge.

* Corresponding author

1.1. CTJ-scheme

In 2011, Chen, Tsai, and Jan proposed an indefinite-index access control protocol with a challenge-response strategy for a low-cost RFID system (CTJ-scheme) [4] as shown in Figure 1. In CTJ-scheme, since tags are issued by the backend database server, a serial number $index_i$ and a s ecret value Key_i are stored in both the tag i and the backend database server. When a reader tries to access the tag i, it emits a random number Q to i. Then i chooses a random number R and then generates a message γ from Q, R, and its stored Key_i. The serial number $index_i$ will be pre-converted to a point by a number-to-point process. Therefore, a matrix π is organized by using Q, R, and the information of points. Finally, the tag performs $\pi \cdot \omega$ to protect π and emits tag's response $\{\gamma, \pi \cdot \omega\}$ back to the reader. So, the reader forwards the received tag's response and Q to the backend database server. With $index_i$ and Key_i, the server can verify the tag's response. If the tag is authenticated, the server computes the corresponding message $\{Key_i, \alpha, R\}$ and sends the message back to the reader. After the reader forwards the correct α to the tag, the tag can verify it. If the reader is authenticated, the tag's content can be accessed or modified by the authenticated reader.

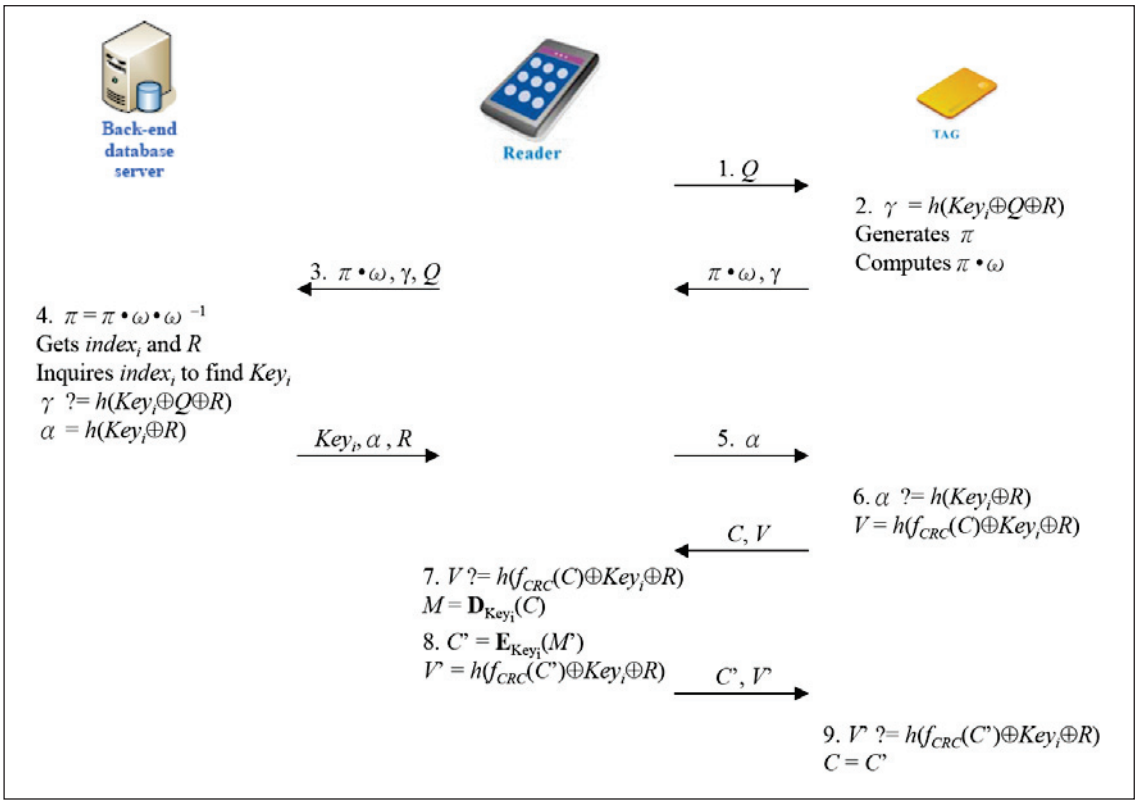

Figure 1. CTJ-scheme access control protocol

1.2. Flaws of CTJ-scheme

Chen *et al.* claimed their proposed scheme not only guarantees mutual authentication and location privacy but also resists various attacks. However, there are still flaws in their scheme.

1.2.1. Spoofed reader attack

In later 2011, Chen, Kuo, and Wuu indicated that CTJ-scheme is vulnerable to a spoofed reader attack [2] as shown in Figure 2. That is to say, when an adversary emits a particular $Q = 0$ by a spoofed reader, the message γ of the tag's response is equal to the correct α since $\gamma = h(Key_i \oplus Q \oplus R) = h(Key_i \oplus R) = \alpha$. Therefore, the reader can bypass the tag's verification and be authenticated by the tag.

1.2.2. DoS attack

In addition, Chen *et al*. also pointed out that CTJ-scheme does not provide any protection against DoS or resource exhaustion attacks [2]. An adversary can send large amounts of requests to a tag and cause the tag to be unavailable to legitimate readers since it is busy with replay message computation during the attack period. Successively, since CTJ-scheme does not provide any verification mechanism for a legitimate reader to verify a tag, after appending Q to the tag's response, the reader forwards the response to the backend server. It means that the reader the backend server. It means that the reader

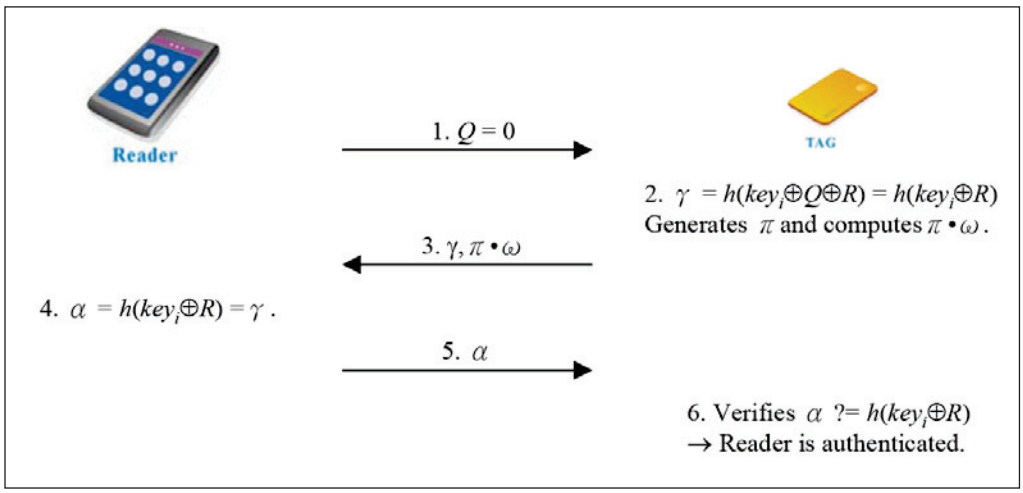

Figure 2. Chen *et al.*'s spoofed reader attack on CTJ-scheme

the backend server. It means that the reader becomes an accomplice in the DoS attack. Moreover, the backend server will try to recover $index_i$ and find the corresponding Key_i after receiving the reader's message. Note that the server needs to scan through its whole database in order to determine if $index_i$ is not usable. This attack thus abuses the computational resources of the server. Trivially, all of the tag, the reader, and the backend server will be fooled by the attacker.

1.2.3. Modification attack

Under Chen *et al.*'s spoofed reader attack scenario in [2], our research found that the content of a tag can be altered by replaying communication message from an unauthorized adversary. The attack is demonstrated in Figure 3. At the end of step 6 of CTJ-scheme, the tag sends a ciphertext C and check value V back to the authenticated (spoofed) reader, and the received message $\{C, V\}$ can be replayed and be sent back to the tag by the reader. Since the message $\{C, V\}$ is qualified, the content of the tag will be updated by the reader/adversary in the end of the step 9 of CTJ-scheme.

In this paper, we propose an enhanced protocol and demonstrate our proposed scheme is secure against DoS, spoofed reader, and modification attacks, while maintaining the merits of CTJ-scheme. The structure of this paper is organized as follows: Section 2 describes the preliminaries of our scheme. In Section 3, an enhanced RFID access control protocol is proposed. The security analysis and comparison of the proposed protocol is presented in Section 4. Finally, our conclusions are given in Section 5.

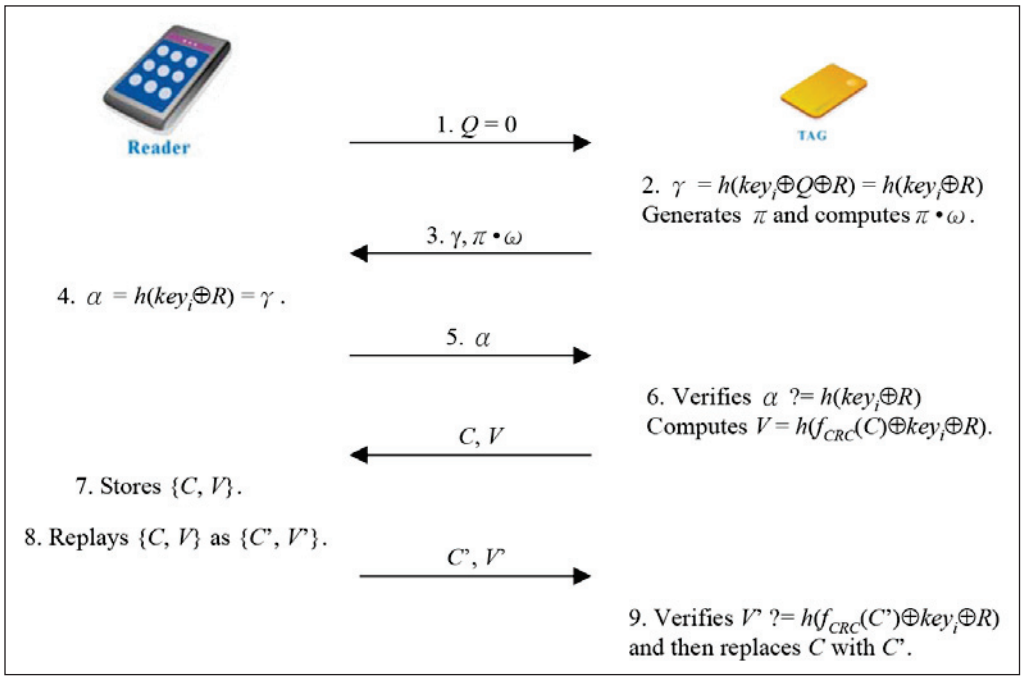

Figure 3. Modification attack under Chen et al.'s spoofed reader attack scenario

2. Preliminaries

2.1. Shared secret key

If there is a mechanism for a reader to verify the legitimacy of a tag, the reader will play the role of doorkeeper to control the entrance of the backend server. Only the response of the verified tag can be forwarded to the server for authentication, and the server does not need to spend resources for authenticating an unauthorized tag. Therefore, in practice, a reader can use a pre-shared key to filter out the responses issued from unauthorized tags. In other words, a tag can be verified by using a key, and this key can be common for all tags. Thus, a tag is verified by using the following two steps: first, a reader verifies that the tag is registered with the backend server; then the server identifies and authenticates the verified tag.

2.2. Redundant information

The reason the spoofed reader in CTJ-scheme is able to mount a modification attack to alter the content of a tag is because there is redundant information in the communications between the reader and the tag. In other words, the formula to calculate V is identical to calculating V'. To remove this flaw, we need to change the dependency of $\{C, V\}$ or $\{C', V'\}$. An authentication scheme should ensure that only authenticated readers can modify tag contents.

2.3. Design goals

An enhanced protocol will be proposed in this paper. There are two major design goals in this protocol:
(I) It should provide a protection mechanism against DoS attack.
(II) It should not only protect a tag's stored data from unauthorized access but also to maintain the security merits in [4].

3. Our enhanced scheme

In this section, the enhanced RFID access control protocol is discussed.

3.1. Notations

The notations used throughout this paper are as follows:

- sk a shared secret key between the reader and all tags.
- indexi a serial number in both the tag i and the backend database server.
- Keyi a secret value in the tag i also known by the backend database server.
- $\oplus$ an exclusive-or operation.
- h a one-way hash function.
- fCRC a cyclic redundancy check function.
- EKeyi an encryption function using the secret value Keyi to encrypt the message.
- DKeyi a decryption function using the secret value Keyi to decrypt the message.
- ω a square matrix in all tags issued by the backend database server.
- $\omega-1$ the inverse matrix of ω, $\omega \cdot \omega-1 = In$, in the backend data-base server.
- ε a critical response time.

3.2. Proposed scheme

The proposed scheme consists of three components: tag, reader, and backend database server, shown in Fig. 4.

3.2.1. Steps

1) The reader generates a random number Q and emits it to the tag.
2) After receiving Q, the tag selects a random number R and computes β and γ as follows:

$$\beta = h(sk \oplus Q) \quad (1)$$

$$\gamma = h(sk \oplus Key_i \oplus R). \quad (2)$$

The messages β and γ will be used for DoS filtering by the tag and authentication by the reader and server, respectively. For the purpose of keeping the tag's location private, a number-to-point process is performed on tag's serial number $index_i$ as in CTJ-scheme, and such transformation will be pre-processed to be different for each access. Then, a matrix π is organized by using Q, R, and the information of points. Finally, the tag replies β, γ, and $\pi \cdot \omega$ to the reader.

3) After the reader receives the response, the message β is verified as follows:

$\beta \stackrel{?}{=} h(sk \oplus Q)$.

If it holds, the reader forwards γ, $\pi \cdot \omega$, and Q to the backend database server; otherwise, the reader drops the tag's response and stops the session. Note that similar to CTJ-scheme, we presume a secure channel between the reader and the backend database server.

4) Since server receives messages from the reader, π can be obtained by:

$$\pi = (\pi \cdot \omega) \cdot \omega^{-1}. \quad (3)$$

Then, the four points (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) and $Q \oplus R$ can be obtained, allowing the server to easily figure out the coordinate (x_i, y_i) and R. The server possesses the tag's $index_i$ and searches it in the database to get Key_i. Therefore, the message γ can then be verified as follows:

$\gamma \stackrel{?}{=} h(sk \oplus Key_i \oplus R)$.

If the equality fails, this signifies the tag is issued

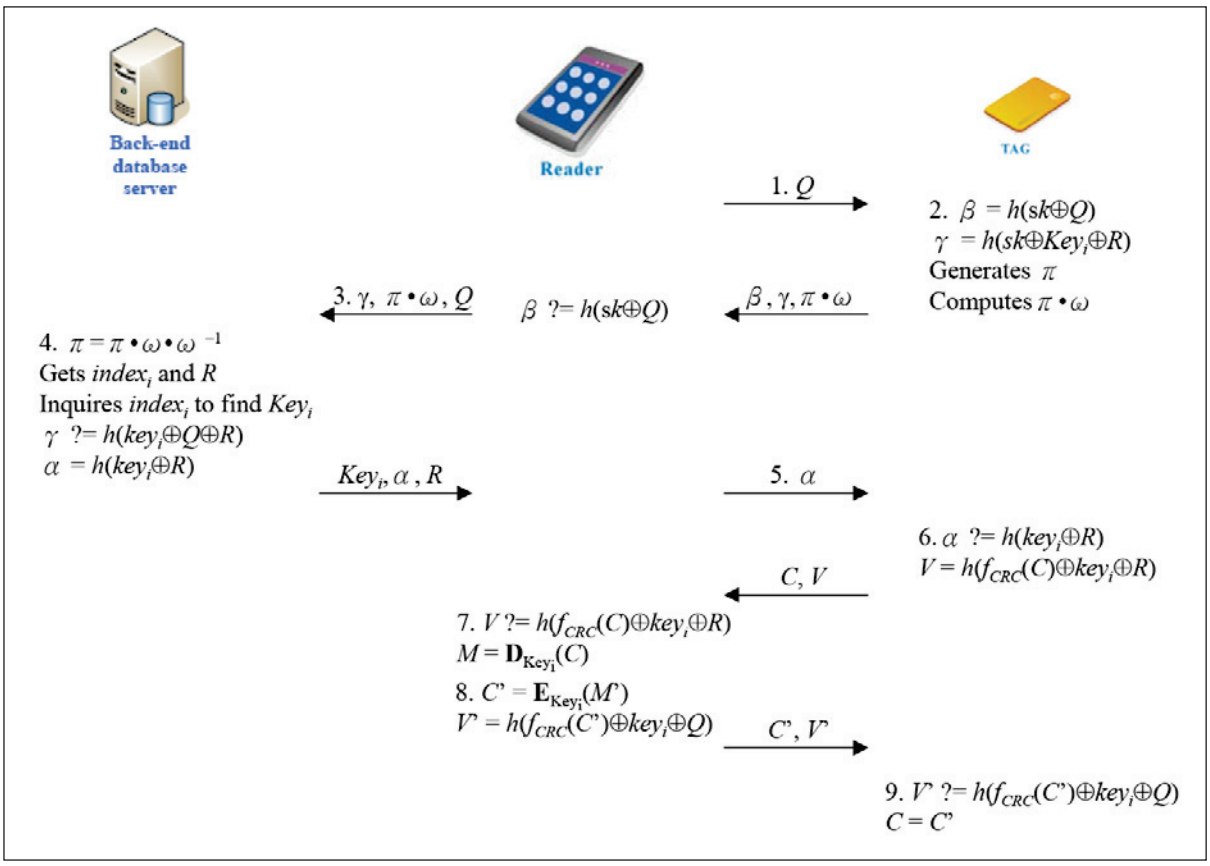

Figure 4. Our proposed enhanced RFID authentication scheme

by the server, but does not have the correct Key_i and/or R. Thus the server should take appropriate measures, e.g., stop the authentication session, examine the tag in a physically secure location, and ensure that there is a s tolen card attack. Otherwise, if the equality holds, it means the tag has the correct credentials and then server provides the following message α to the reader for mutual authentication.

$$\alpha = h(Key_i \oplus R). \quad (4)$$

Then, Key_i, R, and α are sent to the reader.

5) From the backend database server messages, the reader holds Key_i and R for the following access session and forwards α to the tag.
6) The tag receives α from the reader, and verifies it as follows:

$$\alpha \stackrel{?}{=} h(Key_i \oplus R).$$

If the equality holds, it means the reader has proved itself trustworthy since the message α is embedded with the correct Key_i and R. Now, the reader is authorized to access the ciphertext C in the tag. For assuring transmission integrity, the check value V is generated as follows:

$$V = h(f_{CRC}(C) \oplus Key_i \oplus R). \quad (5)$$

Then, C and V are sent to the reader.

7) As the reader receives the message from the tag, the ciphertext integrity check is performed as follows:

$$V \stackrel{?}{=} h(f_{CRC}(C) \oplus Key_i \oplus R).$$

Afterwards, the reader can use Key_i to decrypt C as follows:

$$M = \mathbf{D}_{Key_i}(C). \quad (6)$$

8) If it is necessary to send modified data M' to the tag, it should be encrypted by the reader in advance.

$$C' = \mathbf{E}_{Key_i}(M'). \quad (7)$$

For assuring transmission integrity, the check value V' is generated as follows:

$$V' = h(f_{CRC}(C') \oplus Key_i \oplus Q). \quad (8)$$

Then, C' and V' are transmitted to the tag.

9) When the tag receives the messages from the reader, the ciphertext integrity check can be performed as follows:

$$V' \stackrel{?}{=} h(f_{CRC}(C') \oplus Key_i \oplus Q).$$

Therefore, the ciphertext in the tag is updated from C to C'.

4. Security analysis and comparison

The proposed enhanced scheme is a modified form of CTJ-scheme. Parts of the security analyses have been already discussed and demonstrated in [4]. In this section, we focus our discussion on the enhanced security features of the proposed scheme.

4.1. DoS attack

In the proposed scheme, when a reader receives a tag's response, it verifies the legitimacy of the tag. Only tag responses that pass the reader's verification will be forwarded to the server for authentication. Therefore, the server does not waste resources for authenticating unauthorized tags. In other words, the proposed scheme can prevent fake tags from consuming the server's computational resources by verifying the integrity of shared secret key. In case the server fails to locate a tag in its database, it means that an attack is detected. In the proposed scheme, the server will take appropriate measures. The fact that the server tries to search a tag's serial number with all the available serial numbers in its database is simply to make the protocol complete.

4.2. Spoofed reader attack

Assume that an adversary wants to attempt the spoofed reader attack and bypass the authentication of a tag. The adversary emits $Q = 0$ using a spoofed reader and the reader then receive tag's response $\{\beta, \gamma, \pi \cdot \omega\}$. However, both β and γ are not equal to α. Therefore, the spoofed reader cannot bypass the tag's verification by using received message. Though brute-force attack can be used to guess the shared secret key *sk*, the adversary needs to make another guess of ($Key_i \oplus R$). If both brute-force attacks can be done in the critical response time ε, the expected response $\alpha = h(Key_i \oplus R)$ can be generated to fool the tag. However, for implementation, the critical response time will be defined to be less than the expected running time of a brute-force attack.

4.3. Spoofed tag attack

Suppose there is an adversary without the knowledge of tag's secret key *sk* and secret value Key_i trying to impersonate a tag. According to the design of the proposed scheme, without the correct shared secret key *sk*, the fake tag cannot generate the correct authentication token β to pass the reader's verification. Without the correct secret value Key_i, the fake tag cannot generate the correct authentication token γ and pass the server's authentication. Therefore, the fake tag fails the reader's and the server's authentications in the proposed scheme.

4.4. Modification attack

From our discussion in Section 4.2, the proposed scheme has mitigated the flaw where a spoofed reader can bypass the tag's authentication and receive both the ciphertext C and check value V from a tag. Assume an adversary eavesdrops the ciphertext C and check value V and tries to modify the content of a tag by replaying $\{C, V\}$. The adversary transmits the eavesdropped message $\{C, V\}$ to the tag. However, Eq.(5) and Eq.(8) are not equal, and the ciphertext integrity check cannot be done. Note that only an authenticated reader, providing the correct secret value Key_i and random number R, with the random number Q can modify the content of the tag. Therefore, the spoofed reader cannot mount the modification attack.

4.5. Man-in-the middle attack

By our discussions in Section 4.2 ~ 4.4, we can conclude that without the knowledege of the correct shared secret key *sk* and the correct secret value Key_i, an eavesdropper may only passively monitor the communication and not glean any information from it. Therefore, our proposed scheme withstands the man-in-the middle attack.

4.6. Mutual authentication

The mechanisms to provide mutual authentication in the CJT-scheme and the proposed scheme are essentially the same. Specifically, the tag authentication token β is composed of a shared secret key *sk* and a random nonce Q, and the tag authentication token γ is composed of a shared secret key *sk*, a secret value Key_i, and a random nonce R. The reader authentication token α is composed of a secret value Key_i and a random nonce R. All three tokens β, γ, and α are different. By using the "challenge-response" strategy three times in the proposed scheme, the scheme achieves mutual authentication between the reader and the tag.

4.7. Location privacy

There is a number-to-point pre-processing mechanism providing location privacy in the CJT-scheme. By using the same approach, the proposed scheme also provides location privacy.

4.8. Comparisons

We evaluated the performance of the proposed scheme with CTJ-scheme. Tables 1 and 2 illustrate the computation overhead and the functionality comparison between CTJ-scheme [4] and the proposed scheme.

4.8.1. Time complexity

Compared to CTJ-scheme, the proposed scheme adds two hashes and one comparison: one hash and one comparison on the reader, and one hash operation on the tag, for the "Reader authenticates tag" requirement. In general, hash and comparison require lower computation computational complexity than

Table 1. Computation overhead

Authentication / Scheme	CTJ-scheme [4]			Ours		
	Server	Reader	Tag	Server	Reader	Tag
Reader authenticates tag	–	–	–	–	t_h+t_c	t_h
Server authenticates tag	t_h+t_c	–	t_h	t_h+t_c	–	t_h
Tag authenticates reader	t_h	–	t_h+t_c	t_h	–	t_h+t_c
Tag's content access	–	$2t_h+t_c+t_e+t_d$	$2t_h+t_c$	–	$2t_h+t_c+t_e+t_d$	$2t_h+t_c$

t_h is the time complexity of a hash.
t_c is the time complexity of a comparison.
t_e is the time complexity of an encryption.
t_d is the time complexity of a decryption.
"–" means there is no relative processing.

decryption/encryption. It is a reasonable tradeoff for minimizing the risk of DoS attack.

4.8.2. Functionality

The functionality of the proposed scheme is compared with CTJ-scheme, and we summarize the comparisons in Table 2.

Table 2. Functionality comparison

Functionality / Scheme	CTJ-scheme [4]	Ours
Resists DoS attacks	No	Yes
Resists reader impersonation attacks	No	Yes
Resists tag impersonation attacks	Yes	Yes
Resists tag modification attacks	No	Yes
Resists replay attacks	No	Yes
Resists man-in-the-middle attacks	No	Yes
Server authenticates tag	Yes	Yes
Reader authenticates tag	No	Yes
Tag authenticates reader	No	Yes
Achieves mutual authentication	No	Yes
Provides location privacy	Yes	Yes

5. Conclusions

In this paper, we show that CTJ-scheme is vulnerable to DoS, spoofed reader, and replay attacks. We then present an enhanced secure RFID access control protocol based on CTJ-scheme. The proposed scheme not only withstands DoS, spoofed reader/tag, man-in-the middle, and replay attacks, but also provides mutual authentication and location privacy. In other words, the proposed scheme retains all the advantages of CTJ-scheme while being robust against DoS, spoofed reader, and replay attacks, and also provides the same security properties. According to our analysis on both computation overhead and functionality, our scheme is more secure than CTJ-scheme and is suitable for applications in open and insecure environments.

Acknowledgment

This research was supported by NSC 100-2221-E-150-068.

References

[1] **G. Avoine, P. Oechslin.** A scalable and provably secure hash based RFID protocol. In: *2nd IEEE International Workshop on Pervasive Computing and Communication Security, IEEE Computer Society Press*, 2005, pp. 110–114.

[2] **B. L. Chen, W. C. Kuo, L. C. Wuu**. Security on the Design of RFID Access Control Protocol using the Strategy of Indefinite-index and Challenge-response. In: *The 5th International Conference on Genetic and Evolutionary Computing (ICGEC2011), Taiwan*, 2011, pp. 9-12.

[3] **B. L. Chen, W. C. Kuo, L. C. Wuu.** A Secure Password-Based Remote User Authentication Scheme without Smart Cards. *Information Technology and Control*, 2012, Vol. 41, No. 1, pp. 53-59.

[4] **Y. Y. Chen, M. L. Tsai, J. K. Jan.** The design of RFID access control protocol using the strategy of indefinite-index and challenge-response. In: *Computer Communications*, Vol. 34, No. 3, Special Issue of Computer Communications on Information and Future Communication Security, March 2011, pp. 250–256.

[5] **H. Y. Chien.** Secure access control schemes for RFID systems with anonymity. In: *Proceedings of the 7th International Conference on Mobile Data Management (MDM 2006)*, 2006, p. 96.

[6] **T. Dimitriou.** A lightweight RFID protocol to protect against traceability and cloning attacks. In: *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005, pp. 59–66.

[7] **L. He, Y. Gan, N.-N. Li, Z.-Y. Cai**. A security-provable authentication and key agreement protocol in RFID system. In: *International Conference on Wireless Communications, Networking and Mobile Computing 2007 (WiCom 2007)*, September, 2007, Vol. 21, No. 25, pp. 2078–2080.

[8] **S. M. Lee, Y. J. Hwang, D. H. Lee, J. I. Lim**. Efficient authentication for low-cost RFID systems. In: *International Conference on Computational Science and its Applications – ICCSA 2005*, 2005, pp. 619–627.

[9] **S. Weis, S. Sarma, R. Rivest, D. Engels**. Security and privacy aspects of low-cost radio frequency identification systems. In: *1st International Conference on Security in Pervasive Computing (SPC)*, March, 2003, Vol. 12, No. 14, pp. 201-212.

[10] **Y. Xiao, X. Shen, B. Sun, L. Cai**. Security and privacy in RFID and applications in telemedicine. *IEEE Communication Magazine*, 2006, Vol. 44, No. 4, pp. 64–72.

[11] **J. Yang**. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, A Thesis for the Degree of Master of Science, School of Engineering Information and Communications University, 2005.

Received April 2012.