J Med Syst (2015) 39: 24
DOI 10.1007/s10916-015-0213-7



# A Secure RFID Mutual Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptography

**Chunhua Jin · Chunxiang Xu · Xiaojun Zhang · Jining Zhao**

Received: 11 September 2014 / Accepted: 23 January 2015 / Published online: 10 February 2015


**Abstract** Radio Frequency Identification(RFID) is an automatic identification technology, which can be widely used in healthcare environments to locate and track staff, equipment and patients. However, potential security and privacy problems in RFID system remain a challenge. In this paper, we design a mutual authentication protocol for RFID based on elliptic curve cryptography(ECC). We use pre-computing method within tag's communication, so that our protocol can get better efficiency. In terms of security, our protocol can achieve confidentiality, unforgeability, mutual authentication, tag's anonymity, availability and forward security. Our protocol also can overcome the weakness in the existing protocols. Therefore, our protocol is suitable for healthcare environments.

**Keywords** Radio Frequency Identification · Healthcare environments · Mutual authentication protocol · Elliptic curve cryptography · Pre-computing method

## Introduction

Radio Frequency Identification (RFID) is a technology that can automatic identify people and objects using radio waves. Its main components are a tag, a reader and a database system for handing information. Divided by power supply mode, there are three types of tags: active, passive and semi-passive tags. Active tags are more expensive since they have an internal power source and can start a connection with a reader by themselves. Passive tags are less expensive, but they do not have an internal power source and have to gain energy from the reader signal to transmit data. Semi-passive tags have a small battery which only meets the need of the internal circuit, but harvest energy from the reader signal for sending data. RFID has more advantages than the traditional barcode. It does not require line of sight to read the tag and has a longer read range than barcode reader. It allows both read and write operations. The tag can store more data than barcode and the reader can simultaneously communicate with multiple tags. These advantages make RFID suitable for healthcare environments. It has been used in the location tracking of medical assets [1, 2], new born and patient identification [3], medical treatments tracking and validation [4], patient location and process management at a wellness center [5], and surgical process management [6]. Healthcare systems are open environments and RFID utilizes radio waves for mutual communication. Personal and medical information in the tags can be read or cloned by the adversary. Thus security and privacy are the major concerns of RFID system in healthcare environments. To ensure secure communication in this application, a secure RFID mutual authentication protocol is necessary to guarantee the healthcare system safety.

In recent years, many RFID authentication protocols have been proposed. Huang and Ku [7] proposed a RFID grouping proof protocol to enhance medication safety for inpatient. Soon after, Chien et al. [8] pointed out that Huang and Ku's protocol [7] is vulnerable to Denial-of-Service(DoS) attack and replay attack. Then they gave a further improvement to overcome those attacks. Unfortunately, Peris-Lopez et al. [9] proved that Chien et al.'s protocol [8] suffers from the impersonation attack and

This article is part of the Topical on Collection on *Systems-Level Quality Improvement*

C. Jin (✉) · C. Xu · X. Zhang · J. Zhao
School of Computer Science and Engineering, UESTC, Chengdu, 611731, China
e-mail: chunhuaking@gmail.com

the replay attack. Then they gave an Inpatient Safety RFID(IS-RFID) system to enhance inpatient medication safety. However, Yen et al. [10] found that Peris-Lopez et al.'s protocol [9] does not detect the denial of proof attack and the hospital can modify the generated medication evidence. Later, Chen et al. [11] proposed a novel RFID-based tamper-resistant prescription access control protocol. However, Safkhani et al. [12] showed that Chen et al.'s protocol [11] cannon resist the impersonation attack, the traceability attack and the de-synchronization attack. In 2013, Wu et al. [13] proposed a reliable RFID mutual authentication protocol for healthcare environments. Nevertheless, Picazo-Sanchez et al. [14] pointed out that Wu et al.'s protocol [13] suffers from the traceability attack and gave an improved RFID authentication protocol.

With the development of public key cryptography, elliptic curve cryptography is receiving more and more attention. Compared with the traditional public key cryptography, elliptic curve cryptography has smaller key size with the same security level, faster speed and requires lower space. Therefore, it is especially applicable for RFID authentication protocol. In 2006, Tuyls and Batina [15] proposed the first RFID authentication protocol using ECC. Later, Batina et al. [16] proposed a very similar authentication protocol for RFID using ECC. But Lee et al. [17] found Tuyls and Batina's protocol [15] has the privacy flaw. Besides, their attack is also valid for Batina et al.'s protocol [16]. Then they proposed an improvement protocol using ECC. However, their protocol cannot provide scalability. In 2013, Liao and Hsiao [18] proposed a secure ECC-based RFID authentication protocol and claimed that their protocol can withstand various attacks. Unfortunately, Zhao [19] found that Liao and Hsiao's protocol [18] has the key comprise problem and the adversary can get the tag's private key. To address this problem, Zhao gave an improved protocol that has the same performance. Recently, Chou et al. [20] proposed a new RFID authentication protocol using ECC and demonstrated that their protocol can withstand various attacks. However, Zhang and Qi [21] pointed out that Chou et al.'s protocol [20] is vulnerable to the tag's privacy information problem, backward traceability problem and forward traceability problem. Then they gave an improved RFID authentication protocol using ECC. Very recently, He et al. [34] proposed a lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. Their protocol could provide strong security properties and overcome the weaknesses of the existing schemes.

In this paper, we propose a RFID mutual authentication protocol. As compared with existing protocols, our protocol has the following advantages:

1. our protocol has better performance since we use pro-computing method in tag's communication.
2. our protocol can achieve a lot of security properties and resist various attacks.

Therefore, our protocol is very suitable for healthcare environments.

The rest of this paper is organized as follows. We introduce the preliminary work in Section "Preliminaries". A RFID mutual authentication protocol has been proposed in Section "The proposed protocol". We give security analysis in Section "Analysis of the scheme". The conclusions are given in Section "Conclusion".

## Preliminaries

In this section, we introduce hash function [22] and the related hardness problems. The details are described as follows.

Hash function [22]

A hash function $H$ is a one-way function, which accepts an arbitrarily large input $m$, and produces a small fixed-size output $h$. we can denote as $h = H(m)$. The purpose of hash function is to generate hash value of file, message and other data blocks. It can be mainly applied in message authentication and digital signature, so that hash function has the following properties:

1. Given a message of arbitrary-length, $H$ produces a fixed-size output.
2. $H(x)$ is relatively easy to compute for any given $x$, making both hardware and software implementations practical.
3. For any given hash value $h$, it is computationally infeasible to find $y$ such that $H(y) = h$.
4. For any given block $x$, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
5. It is computationally infeasible to find any pair $(x, y)$ such that $H(x) = H(y)$.

Based on the above properties, when we employ hash function, it can guarantee the security of our protocol by preventing forgery attacks.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

ECDLP Definition: given an elliptic curve $E$ defined over a finite field $F_q$, a point $P \in E(F_q)$ of order $n$, and a point $Q = lP$ where $0 \leq l \leq n-1$, determine $l$.

Computational Diffie-Hellman Problem (CDHP)

CDHP Definition: given an elliptic curve $E$ defined over a finite field $F_q$, a point $P \in E(F_q)$ of order $n$. The computational Diffie-Hellman problem is to compute $abP$ given $(P, aP, bP)$ with $a, b \in Z_n^*$.

## The proposed protocol

In this section, our protocol has three participants: a trusted tag issuer $I$, a trusted tag $T_i$ and a trusted reader $R$ which connects with backed-end database stores identities and public keys of all legitimate tags. We assume that the channel between the tag and the reader is not secure. We also assume that the channel between the reader and backed-end database is secure. There are two phases, i.e., the setup phase and the authentication phase. Before describing the protocol, notations are presented as follows.

| | |
|---|---|
| $q, n$: | Two large prime numbers. |
| $P$: | A generator with order $n$. |
| $F(q)$: | A finite field. |
| $E$: | An elliptic curve defined over a finite field $F_q$ by the equation $y^2 = x^3 + ax + b$, where $a, b \in F(q)$. |
| $ID_{T_i}$: | The identity of the $i$th tag, where $ID_{T_i} \in \{0, 1\}^*$ . |
| $(s_R, P_R)$: | The private/public key of the reader, where $P_R = s_R P, s_R \in Z_n^*$. |
| $(s_{T_i}, P_{T_i})$: | The private/public key of the tag, where $P_{T_i} = s_{T_i} P, s_{T_i} \in Z_n^*$. |
| $H_1, H_2$: | Two secure and collision-resistant hash functions. |

*Setup phase* In this phase, the issuer generates system parameters, its private/public key and the private/public key of the tag.

1. The issuer $I$ chooses two large prime numbers $q, n$. Let $F(q)$ be a finite field and $E$ be an elliptic curve over $F(q)$ defined by the equation $y^2 = x^3 + ax + b$. Then $I$ selects a generator $P$ with order $n$.
2. $I$ chooses two secure and collision-resistant hash functions $H_1, H_2$.
3. For reader $R$, the issuer selects a random value $s_R \in Z_n^*$ as its private key and computes $P_R = s_R P$ as its public key.
4. For each tag $T_i$, the issuer chooses a random value $s_{T_i} \in Z_n^*$ as its private key and computes $P_{T_i} = s_{T_i} P$ as its public key. Scalar multiplication is the main cryptographic operation in ECC. Due to the limited computational capabilities of tag, in order to reduce the amount of computations to be performed by tag, $I$ pre-computes $r = kP, K = kP_R$ as follows. An integer $k$ has binary representation $(k_{l_q-1}, k_{l_q-2}, \cdots, k_0)_2$, $k_i \in \{0, 1\}$, then $k = \sum_{i=0}^{l_q-1} k_i 2^i$. Given an elliptic point $P$, $P_R$, $r = kP = \sum_{i=0}^{l_q-1} k_i 2^i P$, $K = kP_R = \sum_{i=0}^{l_q-1} k_i 2^i P_R$. In the same way, $I$ pre-computes $a = s_1 P, b = e_1 P_R$ as follows.Integer $s_1$ has binary representation $(s_{l_q-1}, s_{l_q-2}, \cdots, s_0)_2$, $s_i \in \{0, 1\}$, then $s_1 = \sum_{i=0}^{l_q-1} s_i 2^i$. Given an elliptic point $P$, $a = s_1 P = \sum_{i=0}^{l_q-1} s_i 2^i P$. Integer $e_1$ has binary representation $(e_{l_q-1}, e_{l_q-2}, \cdots, e_0)_2$, $e_i \in \{0, 1\}$, then $e_1 = \sum_{i=0}^{l_q-1} e_i 2^i$. Given an elliptic point $P_R$, $b = e_1 P_R = \sum_{i=0}^{l_q-1} e_i 2^i P_R$. $0 \le i \le l_q - 1$. $l_q$ denotes binary bitlength of $q$. The issuer $I$ securely stores $(s_{T_i}, P_{T_i}, P_R)$ and data values $r, K, a$ and $b$ into the tag's memory.

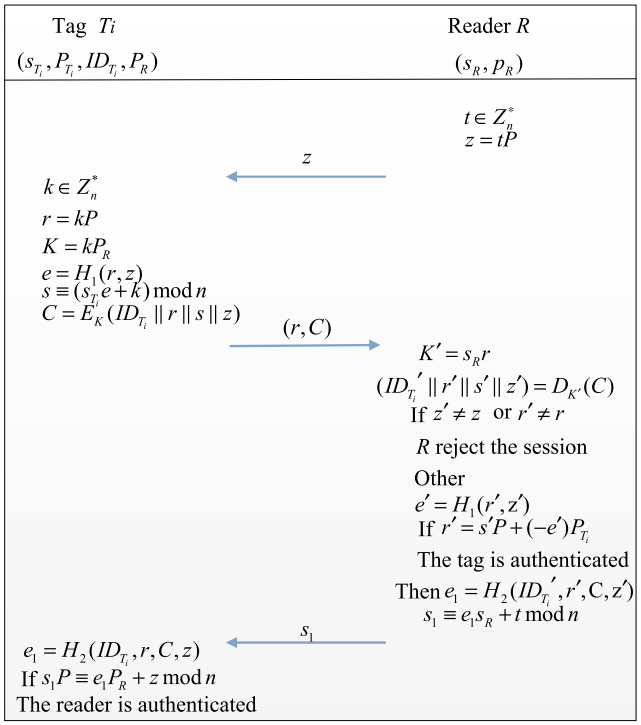


**Fig. 1** The RFID mutual authentication protocol

*Authenticated phase* In this phase, the reader and the tag can realize mutual authenticate. As shown in Fig. 1, the details are presented as follows.

1. $R$ generates a random value $t \in Z_n^*$, computes $z = tP$ and sends $z$ to $T_i$.
2. $T_i$ chooses a random value $k \in Z_n^*$, uses the binary method [23] to pre-compute $r = kP, K = kP_R$. Then $T_i$ computes $e = H_1(r, z), s \equiv (s_{T_i} e + k) \bmod n$, $C = E_K(ID_{T_i} \| r \| s \| z)$, and sends $(r, C)$ to $R$.
3. Upon receiving $(r, C)$, $R$ computes $K' = s_R r$, decrypts $C$ using $K'$, then it can get $ID'_{T_i} \| r' \| s' \| z'$. If $z' \neq z, r' \neq r$, $R$ rejects the session; otherwise, $R$ searches $ID'_{T_i}$ from its backed-end database. In this case, if $ID'_{T_i}$ is no found, $T_i$ is considered illegitimate; otherwise, $R$

obtains the corresponding item $(ID'_{T_i}, P'_{T_i})$, computes $e' = H_1(r', z')$. Then $R$ checks whether $r' = s'P + (-e')P_{T_i}$ or not. If they are equal, the tag $T_i$ is authenticated. Then $R$ computes $e_1 = H_2(ID'_{T_i}, r', C', z')$, $s_1 \equiv s_R e_1 + t \bmod n$ and sends $s_1$ to $T_i$.

4. Upon receiving $s_1$, $T_i$ first computes $e_1 = H_2(ID_{T_i}, r, C, z)$ , then it sets $a = s_1 P, b = e_1 P_R$ and uses the binary method of [23] to check whether $a \equiv b + z \bmod n$ or not. If they are equal, the reader $R$ is authenticated.

## Analysis of the scheme

In this section, we analyze the consistency and security of the proposed scheme.

### Consistency

The consistency can be easily verified by the following equations.

$$r' = s'P + (-e')P_{T_i} = (s_{T_i}e + k)P + s_{T_i}(-e')P = kP = r \tag{1}$$

$$s_1 P = (s_R e_1 + t \bmod n)P = (s_R e_1 P + tP) \bmod n = P_R e_1 + z \bmod n \tag{2}$$

### Security analysis

In this section, we will show that our protocol can provide confidentiality , unforgeability, mutual authentication, tag anonymity, availability and forward security [17, 18, 24–26]. We also show that our protocol can withstand the replay attack, the impersonation attack, server spoofing attack, DoS attack, the de-synchronization attack, the man-in-the-middle attack and cloning attack [19, 20, 27–32].

**Theorem 1** *The proposed protocol could provide confidentiality.*

*Proof* In the proposed protocol, only the random value $z$ generated by $R$ is transmitted as plaintext. While the identity of tag is transmitted as ciphertext, so the unauthorized users cannot obtain tag's identity information, only the reader $R$ which really has the private key $s_R$ can decrypt the ciphertext. Therefore, the proposed protocol could provide confidentiality. □

**Theorem 2** *The proposed protocol could provide unforgeability.*

*Proof* In the proposed protocol, only the tag $T_i$ which has the secret key $s_{T_i}$ can generate a legitimate signature $s$. In the same way, only the reader $R$ which has the secret key $s_R$ can generate a legitimate signature $s_1$. Therefore, the proposed protocol could provide unforgeability. □

**Theorem 3** *The proposed protocol could provide mutual authentication.*

*Proof* The adversary cannot produce a legitimate message $(r, C)$ without the tag's identity $ID_{T_i}$, where $r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i}e + k) \bmod n$ and $C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$. Then the reader $R$ could authenticate the tag $T_i$ by checking the correctness of tag's identity $ID_{T_i}$ and signature $s$. The adversary cannot produce a legitimate signature $s_1$ without the tag's identity $ID'_{T_i}$ and the reader's private key $s_R$, where $e_1 = H_2(ID'_{T_i}, r', C, z'), s_1 \equiv (e_1 s_R + t \bmod n)$. Then the tag $T_i$ could authenticate the reader $R$ by checking the correctness of $s_1$. Thus, the proposed protocol could provide mutual authentication. □

**Theorem 4** *The proposed protocol could provide tag's anonymity.*

*Proof* Suppose that the adversary could intercept the messages $z, (r, C)$ and $s_1$ transmitted between the reader $R$ and the tag $T_i$, where $z = tP, r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i}e + k) \bmod n, C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$, $e_1 = H_2(ID'_{T_i}, r', C, z')$ and $s_1 \equiv (e_1 s_R + t \bmod n)$. If the adversary wants to obtain the tag's identity $ID_{T_i}$ and its private key $s_{T_i}$, it has to compute $K = kP_R = ks_R P$ and $s \equiv (s_{T_i}e + k) \bmod n$. It will face the computational Differ-Hellman problem and the elliptic curve discrete logarithms problem. Thus, the proposed protocol could provide tag's anonymity. □

**Theorem 5** *The proposed protocol could provide availability.*

*Proof* In the proposed protocol, the tag's identity $ID_{T_i}$ and its private key $s_{T_i}$ are protected well, so that there is no need to update these values after the protocol execution. Therefore, the proposed protocol could provide availability. □

**Theorem 6** *The proposed protocol could provide forward security.*

*Proof* Suppose that the adversary could get the tag's identity $ID_{T_i}$ and its private key $s_{T_i}$. We also suppose that the adversary could intercept these messages $z, (r, C)$ and $s_1$ transmitted between the reader and the tag, where $z = tP, r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i}e + k) \bmod n$,

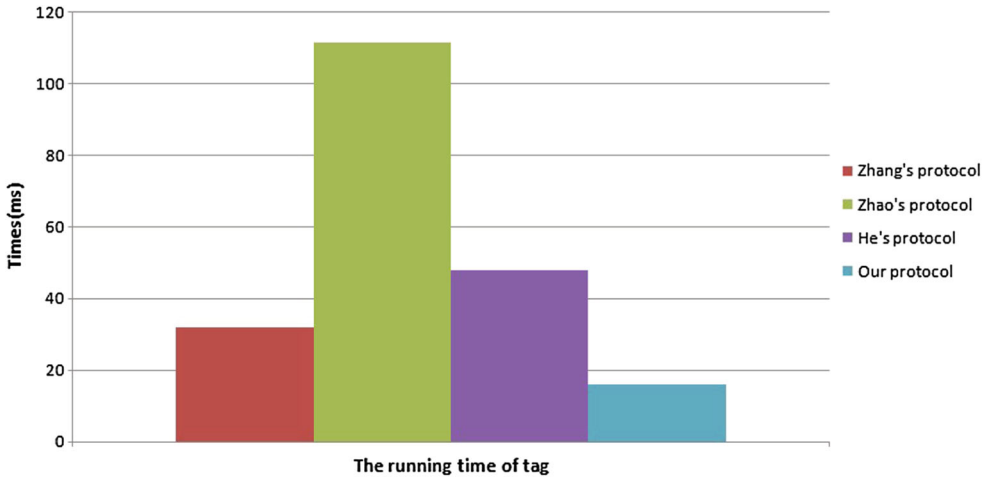


**Fig. 2** The computational cost of tag

$C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$, $e_1 = H_2(ID'_{T_i}, r', C, z')$ and $s_1 \equiv (e_1 s_R + t \bmod n)$. However, it cannot determine whether these messages $z$, $(r, C)$ and $s_1$ transmitted between the reader $R$ and the tag $T_i$ since it does not know the random numbers $t$ and $k$. Therefore, the adversary cannot trace the tag $T_i$ and the proposed protocol could provide forward security. □

**Theorem 7** *The proposed protocol could overcome the tag impersonation attack.*

*Proof* Suppose that the adversary wants to impersonation the tag $T_i$ to the reader $R$ after receiving the message $z$ sent by $R$. It has to generate a legitimate message $(r, C)$ where $r = kP$, $K = kP_R$, $e = H_1(r, z)$, $s \equiv (s_{T_i} e + k) \bmod n$ and $C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$. However, it cannot generate $(r, C)$ since it does not know the tag's identity $ID_{T_i}$ and its private key $s_{T_i}$. Thus, the proposed protocol could overcome the tag impersonation attack. □

**Theorem 8** *The proposed protocol could overcome the sever spoofing attack.*

*Proof* Suppose that the adversary wants to impersonation the reader $R$ to the tag $T_i$. It could produce a random value $t \in Z_n^*$, computes $z = tP$ and sends $z$ to the tag $T_i$. However, it cannot generate a legitimate message $s_1$ without the tag's identity $ID_{T_i}$ and the reader's private key $s_R$,

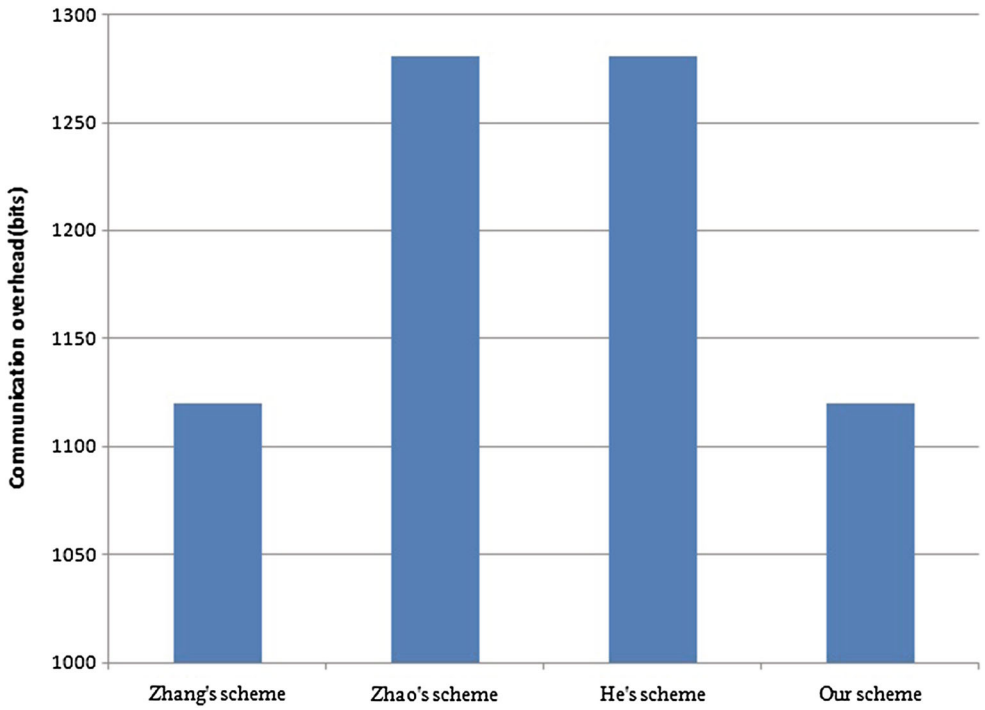


**Fig. 3** The communication overhead of RFID mutual authentication protocol

**Table 1** Performance comparison

| Scheme | [21] | [19] | [34] | Our scheme |
|---|---|---|---|---|
| Computational cost(ms) | 31.919 | 111.684 | 47.911 | 16.057 |
| Communication overhead(bits) | 1120 | 1280 | 1280 | 1120 |
| Confidentiality | Yes | Yes | Yes | Yes |
| Unforgeability | Yes | Yes | Yes | Yes |
| Mutual authentication | Yes | Yes | Yes | Yes |
| Tag anonymity | Yes | Yes | Yes | Yes |
| Availability | Yes | Yes | Yes | Yes |
| Forward security | Yes | Yes | Yes | Yes |
| Tag's impersonation attack | No | No | No | No |
| Server spoofing attack | No | No | No | No |
| Replay attack | No | No | No | No |
| Dos attack | No | No | No | No |
| Modification attack | No | No | No | No |
| Cloning attack | No | No | No | No |
| De-synchronization attack | No | No | No | No |
| Man-in-the-middle attack | No | No | No | No |

where $e_1 = H_2(ID'_{T_i}, r', C, z'), s_1 \equiv (e_1 s_R + t \mod n)$. Thus, the adversary cannot impersonation the reader $R$ to the tag $T_i$ and the proposed protocol could overcome the sever spoofing attack. □

**Theorem 9** *The proposed protocol could overcome the replay attack.*

*Proof* Suppose that the adversary intercepts the message $z$ and replays it to the tag $T_i$. However, the adversary cannot generate a legitimate signature $s_1$ after receiving the message $(r, C)$. The reason is that it does not know the tag's identity $ID_{T_i}$ and the reader's private key $s_R$ where $z = tP, r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i} e + k) \mod n$, $C = E_K(ID_{T_i} \parallel r \parallel s \parallel z), e_1 = H_2(ID'_{T_i}, r', C, z')$ and $s_1 \equiv (e_1 s_R + t \mod n)$. Then the tag $T_i$ could find the attack by checking the correctness of $s_1$.

Suppose that the adversary intercepts the message $(r, C)$ and replays it to the reader $R$ after receiving the message $z$ where $z = tP, r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i} e + k) \mod n$ and $C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$. The reader $R$ could find the attack by checking the correctness of $z$ because it produces a new random value $z \in Z_n^*$ for each session. □

**Theorem 10** *The proposed protocol could overcome DoS attack.*

*Proof* In the proposed protocol, we know that there is no need to synchronously update the tag's identity $ID_{T_i}$ after the protocol execution. Thus, the proposed protocol could overcome DoS attack. □

**Theorem 11** *The proposed protocol could overcome the modification attack.*

*Proof* Suppose that the adversary intercepts the message $z$ or $s_1$ and sends it to the tag $T_i$ when the adversary modifies it, where $z = tP, r = kP, K = kP_R, e = H_1(r, z), s \equiv (s_{T_i} e + k) \mod n$ and $C = E_K(ID_{T_i} \parallel r \parallel s \parallel z)$ and $e_1 = H_2(ID'_{T_i}, r', C, z'), s_1 \equiv (e_1 s_R + t \mod n)$. The tag $T_i$ could find the attack by checking the correctness of $s_1$. Suppose that the adversary intercepts the message $(r, C)$ and sends it to the reader $R$ when the adversary modifies it. The reader $R$ could find the attack by checking the correctness of identity $ID_{T_i}$ and the signature $s$. Thus, the proposed protocol could overcome the modification attack. □

**Theorem 12** *The proposed protocol could overcome cloning attack.*

*Proof* In the proposed protocol, we know that every tag has its own identity $ID_{T_i}$ and its own private key $s_{T_i}$, where $ID_{T_i} \in \{0, 1\}^*, s_{T_i} \in Z_n^*$. Suppose that the adversary could obtain some tags' identity and private key, but it cannot get other tags' identities and private keys since there is no relationship between these tags. Thus, the proposed protocol could overcome cloning attack. □

**Theorem 13** *The proposed protocol could overcome the de-synchronization attack.*

*Proof* In the proposed protocol, we know that the tag $T_i$ and the reader $R$ do not need to update the tag's identity $ID_{T_i}$ after the proposed execution. Thus, the proposed protocol could withstand the de-synchronization attack. □

**Theorem 14** *The proposed protocol could overcome the man-in-the-middle attack.*

*Proof* According to Theorem 3, the proposed protocol could provide mutual authentication between the tag $T_i$ and the reader $R$. Thus, the proposed protocol could overcome the man-in-the-middle attack. □

Performance analysis

In this section, we will compare the computational cost, communication overhead and security of the proposed protocol with those of existing ECC-based RFID authentication protocols [19, 21, 34] in Table 1. We denoted by A, M, the point add operation and point multiplication operation in ECC. We can omit hash function operation, XOR operation in ECC since they have fast computational speeds. We assume that $|p|$ =320 bits, $|n|$ = 160 bits, hash value = 160 bits.

We adopt the experiment on PBC library with an embedding degree 2 on an Intel Pentium(R) Dual-Core processor running 2.69GHz, 2,048MB of RAM(2,007.04MB available) using a 5MHz tag. A point add operation and a point multiplication operation need 0.065ms and 15.927ms using an ECC with 160 bits $n$, respectively. The reader has powerful computational capacity since it connects with a server, so that we do not compute its running time. While the tag has limited computational capacity, so the less tag's calculated amount the better. In this paper, we mainly compare the running time of tag. The running time of tag in [21] need 31.919ms. The running time of tag in [19] need 111.684ms. The running time of tag in [34] need 47.911ms. The running time of tag in our scheme need 16.057ms. Figure 2 shows the running time of tag in [19, 21, 34] and our scheme. As compared with [19, 21, 34], our scheme has the least computational cost of tag. Figure 3 shows the communication overhead for [19, 21, 34] and our protocol. From Figure 3, we can see that the communication overhead for [21] and our protocol have the same advantage. According to Table 1, although our protocol has the same security level with the other three protocols, our protocol has better efficiency. Therefore, our protocol is the most suitable for practical applications.

## Conclusion

The application of RFID in healthcare environments becomes more and more widespread. Therefore, many RFID authentication protocols emerge at the right moment. However, the security problems in RFID authentication protocol remain a challenge. In order to ensure security communication in healthcare environments, many RFID authentication protocols based on ECC have been proposed. In this paper, we also propose a RFID authentication protocol using ECC. We use the pre-computing concept within the tag's communication process to avoid the time-consuming scalar multiplication since the tag has limited computational capabilities. Thus, the proposed protocol has better efficiency. In terms of security, our protocol can achieve a lot of security properties and withstand many common attacks. Therefore, our protocol is more suitable for healthcare environments.

**Acknowledgments** This work is supported by the National Natural Science Foundation of China (Grant Nos.61272525 and 61370203)and Science and Technology on Communication Security Laboratory Foundation (NO.9140C110301110C1103).

## References

1. Wang, S. W., Chen, W. H., Ong, C. S., Liu, L., and Chuang, Y. W., RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. In: Hawaii International Conference on System Sciences. IEEE. pp. 184–194, 2006.
2. Najera, P., Lopez, J., and Roman, R., Real-time location and inpatient care systems based on passive RFID. *J. Netw. Comput. Appl.* 34(3):980–989, 2011.
3. Hung, Y. K., The study of adopting RFID technology in medical institute with the perspectives of cost benefit. *International Medical Informatics Symposium in Taiwan, Taiwan*, 2007.
4. Katz, J. E., and Rice, R. E., Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology. *Int. J. Med. Inform.* 78(2):104–114, 2009.
5. Leu, J. G., *The benefit analysis of RFID use in the health management center the experience in Shin Kong Wu Ho-Su Memorial Hospital*: National Taiwan University, 2010.
6. Yu, C., Chen, C., Liao, P., and Lee, Y., RFID-based operation room and medicare system for patient safety enhancement-a case study of keelung branch. *J. Inf. Manag.* 15:97–122, 2008.
7. Huang, H. H., and Ku, C. Y., A rfid grouping proof protocol for medication safety of inpatient. *J. Med. Syst.* 33(6): 467–474, 2009.
8. Chien, H. Y., Yang, C. C., Wu, T. C., and Lee, C. F., Two rfid based solutions to enhance inpatient medication safety. *J. Med. Syst.* 35(3):369–375, 2011.
9. Peris-Lopez, P., Orfila, A., Mitrokotsa, A., and van der Lubbe, J. C., A comprehensive rfid solution to enhance inpatient medication safety. I*nt. J. Med. Inform.* 80(1): 13–24, 2011.

10. Yen, Y. C., Lo, N. W., and Wu, T.. C., Two rfid-based solutions for secure inpatient medication administration. *J. Med. Syst.* 36(5):2769–2778, 2012.
11. Chen, Y. Y., Wang, Y. J., and Jan, J. K., A secure 2G-RFID-Sys mechanism for applying to the medical emergency system. *J. Med. Syst.* 37(3):1–10, 2013.
12. Safkhani, M., Bagheri, N., and Naderi, M., On the designing of a tamper resistant prescription rfid access control system. *J. Med. Syst.* 36(6):3995–4004, 2012.
13. Wu, Z. Y., Chen, L., and Wu, J. C., A reliable rfid mutual authentication scheme for healthcare environments. *J. Med. Syst.* 37:1–9, 2013.
14. Picazo-Sanchez, P., Bagheri, N., and Peris-Lopez, P., Two RFID Standard-based Security Protocols for Healthcare Environments. *J. Med. Syst.* 37:9962, 2013.
15. Tuyls, P., and Batina, L., RFID-tags for Anti-Counterfeiting. In: *Topics in cryptology-CT-RSA 2006*. pp. 115–131, 2006.
16. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I., *Public-key cryptography for RFID-tags. Fifth annual IEEE international conference on PerCom workshops' 07. IEEE*. pp. 217–222, 2007.
17. Lee, Y., Batina, L., and Verbauwhede, I., EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol. In: *2008 I.E. international conference on RFID. IEEE*. pp. 97–104, 2008.
18. Liao, Y., and Hsiao, C., A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*. doi:10.1016/j.adhoc.2013.02.004, 2013.
19. Zhao, Z. G., A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem. *J. Med. Syst.* 38(5):1–7, 2014.
20. Chou, J.-S., A secure RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *J. Supercomput.* 2014. doi:10.1007/s11227-013-1073-x.
21. Zhang, Z. Z., and Qi, Q. Q., An Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using Elliptic Curve Cryptography. *J. Med. Syst.* 38(5):1–7, 2014.
22. William S., and Stallings W., *Cryptography and Network Security, 4/E[M]*. Pearson Education India, 2006.
23. Jonsson, J., and Kaliski, B., *Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1[J]*. 2003.
24. Bringer, J., Chabanne, H., and Icart, T., *Cryptanalysis of EC-RAC, a RFID identification protocol. In:International Conference on Cryptology and Network Security–CANS'08, Lecture Notes in Computer Science*: Springer–Verlag, 2008.
25. He D., Kumar N., and Khan M. K., Robustanonymous authentication protocol for healthcare applications using wirelessmedical sensor networks. *Multimedia Systems*. doi:10.1007/s00530-013-0346-9, 2014.
26. He D., and Zeadally S., Authentication protocol for ambient assisted living system. *IEEE Commun. Mag.* 53(1):2–10, 2015.
27. Han, W., and Zhu, Z., An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem. *Int. J. Commun. Syst.* 2012. doi:10.1002/dac.2405.
28. He, D., Chen, Y., and Chen, J., Cryptanalysis and improvement of an extended chaotic maps–based key agreement protocol. *Nonlinear Dyn.* 69(3):1149–1157, 2012.
29. He, D., Kumar, N., Khan, M. K., and Lee, J.-H., Anonymous twofactor authentication for consumer roaming service in Global Mobility Networks. *IEEE Trans. Consum. Electron.* 59(4):811–817, 2013.
30. Hao, X., Wang, J., Yang, Q., Yan, X., and Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. doi:10.1007/s10916-012-9919-y, 2013.
31. He, D., and Wang D., Robust biometrics-based authenticationscheme for multi-server environment. IEEE Syst. J. doi:10.1109/JSYST.2014.2301517, 2014.
32. He, D., Zhang. Y., and Chen J., Cryptanalysis and improvementof an anonymous authentication protocol for wireless access networks. Wirel. Pers. Commun. 74(2):229–243, 2014.
33. Zhao Z., A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem. *J. Med. Syst.* 38(2):13, 2014.
34. He D., Kumar N., Chilamkurti N. and Lee J.-H., Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *J. Med. Syst.* 38(10):1–6, 2014.