Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 642425, 7 pages
http://dx.doi.org/10.1155/2015/642425

Research Article

An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System

Chin-I Lee[1] **and Hung-Yu Chien**[2]

[1] *Department of Information Management, Ling Tung University, No. 1, Ling Tung Road, Taichung 408, Taiwan*
[2] *Department of Information Management, National Chi Nan University, No. 1, University Road, Puli, Nantou 545, Taiwan*

Correspondence should be addressed to Hung-Yu Chien; hychien@ncnu.edu.tw

Received 11 September 2015; Accepted 6 December 2015

Academic Editor: Kijun Han

Mobile healthcare (M-health) systems can monitor the patients' conditions remotely and provide the patients and doctors with access to electronic medical records, and Radio Frequency Identification (RFID) technology plays an important role in M-health services. It is important to securely access RFID data in M-health systems: here, authentication, privacy, anonymity, and tracking resistance are desirable security properties. In 2014, He et al. proposed an elliptic curve cryptography- (ECC-) based RFID authentication protocol which is quite attractive to M-health applications, owing to its claimed performance of security, scalability, and efficiency. Unfortunately, we find their scheme fails to achieve the privacy protection if an adversary launches active tracking attacks. In this paper, we demonstrate our active attack on He et al.'s scheme and propose a new scheme to improve the security. Performance evaluation shows the improved scheme could meet the challenges of M-health applications.

1. Introduction

Mobile healthcare (M-health) systems can monitor the patients' conditions remotely and provide the patients and doctors with access to electronic medical records. Such a system improves both convenience and efficiency, because the patients and doctors are no longer required to be present at the same place; therefore, patients can contact their doctor at home and obtain the instant diagnosis and prescription. In the development of M-health systems, Radio Frequency Identification (RFID) technology plays an important role for identifying and accessing patients and objects. Therefore, securely accessing these RFID tags and systems is critical to the success of M-health systems [1, 2].

In a RFID system, there are three types of roles: RFID tags, RFID readers, and a back-end server. Each tag has a unique number which is used to identify a RFID-tagged product. To obtain data from a tag, a reader first issues a query to the tag and then forwards the received information provided by the tag to a back-end server. The back-end server maintains a database of the information of tags and their labelled products. However, since a tag automatically responds to any readers' queries via radio signal, the owner of the tagged product is even unaware of this action. If the tag transmits a fixed value in response to readers' queries, it raises potential privacy threats to the labelled objects and the owner's location.

Privacy protection in a RFID system is investigated in two respects. One is anonymity; the other is tracking attack resistance. The former is to provide confidentiality of tag's identity such that an unauthorized observer cannot learn the identity of the tag. The latter is to provide unlinkability of any two RFID transmission sessions; that is, given any two RFID transactions, an attacker cannot tell whether the two transactions came from the same tag or not. Tracking attack could be classified into two categories: passive tracking attack and active tracking attack. The passive tracking attack is that an adversary tries to distinguish whether two RFID transactions came from the same tag by eavesdropping only, while the active tracking attack is that an adversary can actively participate in the transactions (like eavesdropping, interrupt, replay, and modification) to get the data to tell whether two transactions came from the same tag. Both types of tracking might be used to infer users' location information or even their personal profiles.

Due to the advances of hardware development, many RFID schemes based on the public key techniques have been proposed and implemented [3]. Compared with the other cryptography mechanisms, the elliptic curve cryptography (ECC) [4, 5] is more competitive since it could provide the same security level with much smaller key size. Lee et al. [6] proposed an ECC-based RFID authentication scheme. Bringer et al. [7] and Deursen and Radomirovic [8] found that Lee et al.'s scheme is vulnerable to the tracking attack and the replay attack. Liao and Hsiao [9] proposed an ECC-based RFID authentication scheme integrated with an ID verifier transfer protocol; nevertheless, Peeters and Hermans [10] showed Liao and Hsiao's scheme cannot resist the server impersonation attack. Tan [11] proposed ECC-based RFID three-factor authentication. Arshad and Nikooghadam [12] found that Tan's scheme is not resistant to the replay attack and the denial-of-service attack.

In 2014, He et al. [13] proposed an elliptic curve cryptography- (ECC-) based RFID authentication protocol which aimed at protecting tag's anonymity and unlinkability and improving the computational complexity. Compared with the previous authentication schemes, He et al.'s scheme has better performance in terms of security, computational cost, and storage requirement. Unfortunately, we find that their scheme fails to achieve the privacy protection if an adversary launches active tracking attacks. We will show the weaknesses and propose an improved scheme. The rest of this paper is organized as follows. Section 2 gives the preliminary sketch of the elliptic curve cryptography and bilinear pairing. Section 3 reviews He et al.'s scheme and shows its security weakness. In Section 4, we propose our new scheme, which is followed by security analysis and performance evaluation in Section 5. Finally, conclusions are given in Section 6.

2. Preliminaries

We briefly introduce the elliptic curve cryptography and the bilinear pairing.

2.1. Elliptic Curve Cryptography. Koblitz [4] and Miller [5] introduced elliptic curves for cryptographic applications. Since then, elliptic curve cryptography (ECC) has played an important role in many cryptosystems. An elliptic curve E is defined over the equation $y^2 = x^3 + ax + b$ over $F(q)$, where q is a large prime and $F(q)$ is a finite field of order q. The main attraction of ECC is that ECC with 160-bit key can reach a security level the same as that of 1024-bit RSA and thereby significantly reduce the key size.

The security of He et al.'s protocol is based on the complexity of the elliptic curve discrete logarithm problem (ECDLP) [14].

Elliptic Curve Discrete Logarithm Problem (ECDLP). Given an elliptic curve E over $F(q)$ and two points P and Q on E, the elliptic curve discrete logarithm problem is to find an integer $x \in Z_q^*$ such that $xP = Q$.

2.2. The Bilinear Pairing. The bilinear pairing was initially considered as a negative property on the design of elliptic curve cryptosystems, because it reduces the discrete logarithm problem on some elliptic curves (especially for supersingular curves) to the discrete logarithm problem in a finite field [15]. Such property diminishes the strength of supersingular curves in practice [16]. However, followed by the tripartite key agreement protocol proposed by Joux [17] and the identity-based encryption scheme proposed by Boneh and Franklin [18], pairing becomes beneficial and favorable to the design of cryptographic protocols or cryptosystems [19].

Let G_1 be an additive cyclic group (which is the elliptic curve group $E(F_q)$ here) and let G_2 be a multiplicative cyclic group with the same prime order n; that is, $|G_1| = |G_2| = n$. Bilinear pairing is defined by $\hat{e} : G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties:

(1) Bilinear: for all $P, Q \in G_1$ and all $u, v \in Z_n^*$, we have $\hat{e}(uP, vQ) = \hat{e}(uvP, Q) = \hat{e}(P, uvQ) = \hat{e}(P, Q)^{uv}$.

(2) Nondegenerate: $\hat{e}(P, P) \neq 1$ for some $P \in G_1$.

(3) Computable: given $P, Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P, Q)$.

We find that He et al.'s protocol is vulnerable to active tracking attack. We will utilize the bilinear pairing to facilitate our active attacks in Section 4.

3. Weaknesses of He et al.'s Protocol

3.1. Review of He et al.'s Protocol. This section reviews He et al.'s protocol [13]. The system consists of three kinds of entities: readers, a back-end server, and a set of tags; but the RFID reader is omitted from the protocol description since it acts as an intermediate party that relays messages exchanged between a tag and the server. It is assumed that the communication between the reader and back-end server is secure. The proposed protocol comprises two phases: *setup* and *authentication*. Notations used in the protocol are defined as follows:

(i) n, q: two large primes.

(ii) $F(q)$: a finite field of order q.

(iii) E: an elliptic curve defined by the equation $y^2 = x^3 + ax + b$ over $F(q)$.

(iv) P: a generator point for a group of order n over E.

(v) x_s: the private key of the server.

(vi) P_s: the public key of the server $P_s = x_s P$.

(vii) X_T: the ID verifier of the tag.

Setup Phase. To set up the system, the back-end server performs the following tasks:

(i) Define params $= \{q, a, b, P, n\}$ as the elliptic curve domain parameters.

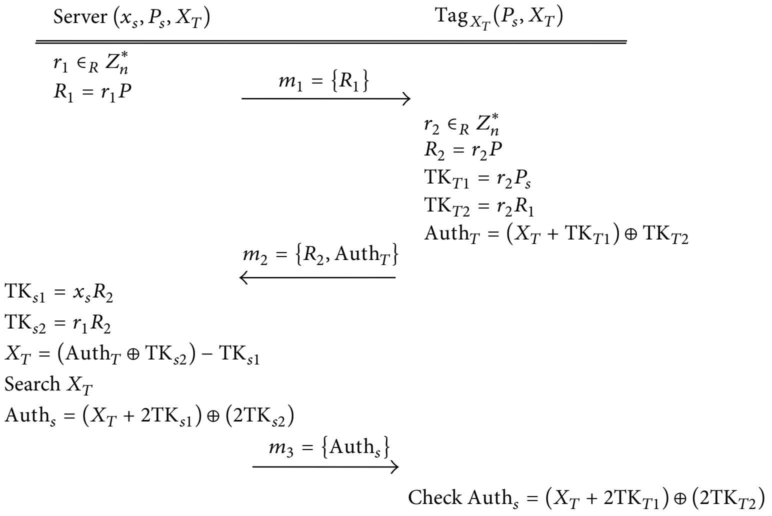

Server (x_s, P_s, X_T)
$\mathrm{Tag}_{X_T}(P_s, X_T)$
$r_1 \in_R Z_n^*$
$R_1 = r_1 P$
$m_1 = \{R_1\}$
$r_2 \in_R Z_n^*$
$R_2 = r_2 P$
$\mathrm{TK}_{T1} = r_2 P_s$
$\mathrm{TK}_{T2} = r_2 R_1$
$\mathrm{Auth}_T = (X_T + \mathrm{TK}_{T1}) \oplus \mathrm{TK}_{T2}$
$m_2 = \{R_2, \mathrm{Auth}_T\}$
$\mathrm{TK}_{s1} = x_s R_2$
$\mathrm{TK}_{s2} = r_1 R_2$
$X_T = (\mathrm{Auth}_T \oplus \mathrm{TK}_{s2}) - \mathrm{TK}_{s1}$
Search X_T
$\mathrm{Auth}_s = (X_T + 2\mathrm{TK}_{s1}) \oplus (2\mathrm{TK}_{s2})$
$m_3 = \{\mathrm{Auth}_s\}$
Check $\mathrm{Auth}_s = (X_T + 2\mathrm{TK}_{T1}) \oplus (2\mathrm{TK}_{T2})$

Figure 1: The authentication phase of He et al.'s protocol.

(ii) Choose a random number $x_s \in Z_n^*$ as the server's private key, and compute $P_s = x_s P$ as the server's public key.

(iii) Choose a random point X_T on E denoted as a tag's ID verifier.

(iv) (params, P_s, X_T) is stored at both the tag and the server's database.

(v) The server also keeps x_s secret.

Authentication Phase. To achieve mutual authentication, the server (S) and the tag (Tag_{X_T}) do the following steps. The authentication phase is illustrated in Figure 1.

Step 1 ($S \to \mathrm{Tag}_{X_T} : m_1 = \{R_1\}$). S randomly chooses $r_1 \in Z_n^*$, computes $R_1 = r_1 P$, and sends $m_1 = \{R_1\}$ as a challenge to the tag.

Step 2 ($\mathrm{Tag}_{X_T} \to S : m_2 = \{R_2, \mathrm{Auth}_T\}$). Tag_{X_T} randomly chooses $r_2 \in Z_n^*$ and computes $R_2 = r_2 P$, $\mathrm{TK}_{T1} = r_2 P_s$, $\mathrm{TK}_{T2} = r_2 R_1$, and $\mathrm{Auth}_T = (X_T + \mathrm{TK}_{T1}) \oplus \mathrm{TK}_{T2}$. Then, Tag_{X_T} sends back $m_2 = \{R_2, \mathrm{Auth}_T\}$ to S.

Step 3 ($S \to \mathrm{Tag}_{X_T} : m_3 = \{\mathrm{Auth}_s\}$). S computes $\mathrm{TK}_{s1} = x_s R_2$, $\mathrm{TK}_{s2} = r_1 R_2$, and $X_T = (\mathrm{Auth}_T \oplus \mathrm{TK}_{s2}) - \mathrm{TK}_{s1}$ and then searches the server's database for X_T. If it is not found, the server S rejects the tag; otherwise, the tag Tag_{X_T} is authenticated and thereafter S computes $\mathrm{Auth}_s = (X_T + 2\mathrm{TK}_{s1}) \oplus (2\mathrm{TK}_{s2})$ and sends back $m_3 = \{\mathrm{Auth}_s\}$ to Tag_{X_T}.

Step 4. Upon receiving the server's response, Tag_{X_T} checks if $(X_T + 2\mathrm{TK}_{T1}) \oplus (2\mathrm{TK}_{T2}) = \mathrm{Auth}_s$. If it succeeds, the server S is authenticated; otherwise, the tag stops the procedure.

3.2. The Weaknesses. We find that He et al.'s protocol is vulnerable to active tracking attack. We utilize the bilinear pairing to check whether the two transactions came from the same tag or not. We demonstrate our active attack as follows, where Adv denotes the notion that the adversary impersonates the server to get the responses for tracking. First of all, Adv randomly chooses $r_1 \in Z_n^*$, computes $R_1 = r_1 P$, and sends message $m_1 = \{R_1\}$ to probe the tags it encounters. In the following, we assume Adv encounters the same tag Tag_{X_T}.

Upon receiving the query, Tag_{X_T} randomly chooses $r_2 \in Z_n^*$ and computes $R_2 = r_2 P$, $\mathrm{TK}_{T1} = r_2 P_s$, $\mathrm{TK}_{T2} = r_2 R_1$, and $\mathrm{Auth}_T = (X_T + \mathrm{TK}_{T1}) \oplus \mathrm{TK}_{T2}$. Then, Tag_{X_T} sends back $m_2 = \{R_2, \mathrm{Auth}_T\}$ to S. Adv can compute $\mathrm{TK}_{s2} = r_1 R_2$, which equals TK_{T2}. So Adv obtains $(X_T + \mathrm{TK}_{T1}) \oplus \mathrm{TK}_{T2} \oplus \mathrm{TK}_{s2} = (X_T + \mathrm{TK}_{T1})$.

When Tag_{X_T} is probed again, it randomly chooses $\overline{r_2} \in Z_n^*$ and computes $\overline{R_2} = \overline{r_2} P$, $\overline{\mathrm{TK}_{T1}} = \overline{r_2} P_s$, $\overline{\mathrm{TK}_{T2}} = \overline{r_2} R_1$, and $\overline{\mathrm{Auth}_T} = (X_T + \overline{\mathrm{TK}_{T1}}) \oplus \overline{\mathrm{TK}_{T2}}$. Then, Tag_{X_T} responds with $m_2 = \{\overline{R_2}, \overline{\mathrm{Auth}_T}\}$. Adv computes $\mathrm{TK}_{s2} = r_1 \overline{R_2}$, which equals $\overline{\mathrm{TK}_{T2}}$. Then, it obtains $(X_T + \overline{\mathrm{TK}_{T1}}) \oplus \overline{\mathrm{TK}_{T2}} \oplus \overline{\mathrm{TK}_{s2}} = (X_T + \overline{\mathrm{TK}_{T1}})$. Now Adv performs the following steps to verify whether the two transactions came from the same tag:

(1) It computes $(X_T + \mathrm{TK}_{T1}) - (X_T + \overline{\mathrm{TK}_{T1}}) = \mathrm{TK}_{T1} - \overline{\mathrm{TK}_{T1}} = (r_2 - \overline{r_2}) P_s$ and $R_2 - \overline{R_2} = r_2 P - \overline{r_2} P = (r_2 - \overline{r_2}) P$.

(2) It checks whether the equation $\widehat{e}(R_2 - \overline{R}_2, P_S) \overset{?}{=} \widehat{e}((X_T + \mathrm{TK}_{T1}) - (X_T + \overline{\mathrm{TK}_{T1}}), P)$ holds.

If the transactions came from the same tag, the above verification equation should hold, because $\widehat{e}(X_T + \mathrm{TK}_{T1}) - (X_T + \overline{\mathrm{TK}_{T1}}), P) = \widehat{e}((r_2 - \overline{r}_2) P_S, P) = \widehat{e}((r_2 - \overline{r}_2) P, P)^{x_s} = \widehat{e}((r_2 - \overline{r}_2) P, x_s P) = \widehat{e}((R_2 - \overline{R}_2), P_S)$. That is, He et al.'s protocol cannot resist the active tracking attack.

4. The Proposed Scheme

We propose a new ECC-based scheme, which owns excellent performance in terms of security, computational complexity,

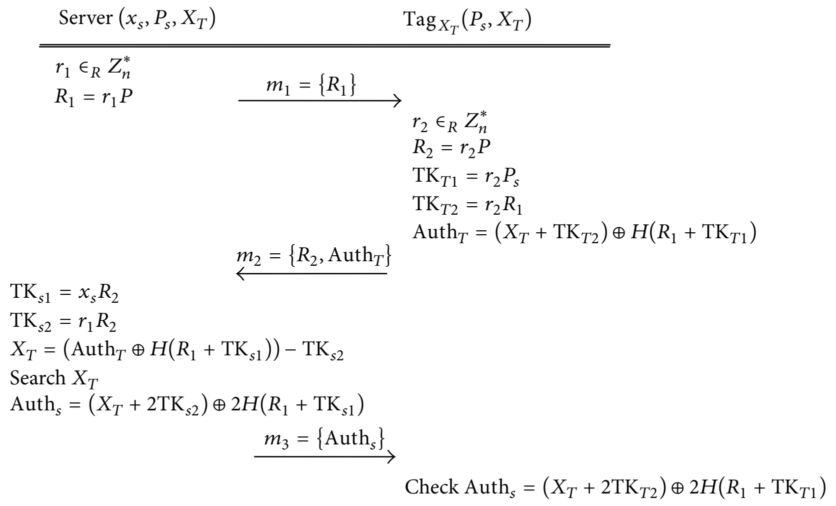

Server (x_s, P_s, X_T)
$\text{Tag}_{X_T}(P_s, X_T)$
$r_1 \in_R Z_n^*$
$R_1 = r_1 P$
$m_1 = \{R_1\}$
$r_2 \in_R Z_n^*$
$R_2 = r_2 P$
$\text{TK}_{T1} = r_2 P_s$
$\text{TK}_{T2} = r_2 R_1$
$\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$
$m_2 = \{R_2, \text{Auth}_T\}$
$\text{TK}_{s1} = x_s R_2$
$\text{TK}_{s2} = r_1 R_2$
$X_T = (\text{Auth}_T \oplus H(R_1 + \text{TK}_{s1})) - \text{TK}_{s2}$
Search X_T
$\text{Auth}_s = (X_T + 2\text{TK}_{s2}) \oplus 2H(R_1 + \text{TK}_{s1})$
$m_3 = \{\text{Auth}_s\}$
Check $\text{Auth}_s = (X_T + 2\text{TK}_{T2}) \oplus 2H(R_1 + \text{TK}_{T1})$

FIGURE 2: The authentication phase of the proposed protocol.

and communicational cost. Our scheme can resist all security threats including active tracking attack. Regarding computational complexity, we reduce the number of elliptic curve scalar multiplications, which is the most computationally expensive operation in ECC cryptography. For embedded systems like RFID and wireless sensor network, the communication operations consume the highest amount of energy of all the operations; therefore, reducing the message length is critical for saving the energy of these devices. The proposed scheme consists of two phases: setup and authentication. Since the setup phase is the same as that in He et al.'s protocol, it is omitted here. The authentication phase is described as follows.

Authentication Phase. To achieve mutual authentication, the server (S) and the tag (Tag_{X_T}) do the following steps. The authentication phase is illustrated in Figure 2.

Step 1 ($S \rightarrow \text{Tag}_{X_T} : m_1 = \{R_1\}$). S randomly chooses $r_1 \in Z_n^*$, computes $R_1 = r_1 P$, and sends $m_1 = \{R_1\}$ as a challenge to the tag.

Step 2 ($\text{Tag}_{X_T} \rightarrow S : m_2 = \{R_2, \text{Auth}_T\}$). Tag_{X_T} randomly chooses $r_2 \in Z_n^*$ and computes $R_2 = r_2 P$, $\text{TK}_{T1} = r_2 P_s$, $\text{TK}_{T2} = r_2 R_1$, and $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$. Then, Tag_{X_T} sends back $m_2 = \{R_2, \text{Auth}_T\}$ to S.

Step 3 ($S \rightarrow \text{Tag}_{X_T} : m_3 = \{\text{Auth}_s\}$). S computes $\text{TK}_{s1} = x_s R_2$, $\text{TK}_{s2} = r_1 R_2$, and $X_T = (\text{Auth}_T \oplus H(R_1 + \text{TK}_{s1})) - \text{TK}_{s2}$ and then searches the server's database for X_T. If it is not found, the server S rejects the tag; otherwise, the tag Tag_{X_T} is authenticated and thereafter S computes $\text{Auth}_s = (X_T + 2\text{TK}_{s2}) \oplus 2H(R_1 + \text{TK}_{s1})$ and sends back $m_3 = \{\text{Auth}_s\}$ to Tag_{X_T}.

Step 4. Upon receiving the server's response, Tag_{X_T} checks if $(X_T + 2\text{TK}_{T2}) \oplus 2H(R_1 + \text{TK}_{T1}) = \text{Auth}_s$. If it succeeds, the server S is authenticated; otherwise, the tag stops the procedure.

5. Security Analysis and Performance Evaluation

5.1. Security Analysis. We analyze the security of the proposed scheme as follows.

Mutual Authentication. The authentication of the tag is dependent on tag's ability to prove its knowledge of the secret X_T. In our scheme, the server receives the message $m_2 = \{R_2, \text{Auth}_T\}$, where $R_2 = r_2 P$ and $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$. The server will use its private key x_s to compute $\text{TK}_{s1} = x_s R_2$ and $\text{TK}_{s2} = r_1 R_2$ and to extract $X_T = (\text{Auth}_T \oplus H(R_1 + \text{TK}_{s1})) - \text{TK}_{s2}$. Then, the server checks whether X_T is stored in the database. Only the genuine tag that owns the secret X_T can generate valid Auth_T.

The authentication of the server is dependent on server's ability to extract X_T and generate valid Auth_s. Only the genuine server that owns the secret x_s can correctly extract X_T from Auth_T and then compute valid $\text{Auth}_s = (X_T + 2\text{TK}_{s2}) \oplus 2H(R_1 + \text{TK}_{s1})$. Without knowledge of the server's secret key x_s, the adversary cannot obtain $\text{TK}_{s1} = x_s R_2$. The tag checks the validity of Auth_s. If it is valid, then the server is authenticated.

Anonymity. In our scheme, $m_1 = \{R_1\}$, $m_2 = \{R_2, \text{Auth}_T\}$, and $m_3 = \{\text{Auth}_s\}$ are transmitted, where the tag-identity-related messages are $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$ and $\text{Auth}_s = (X_T + 2\text{TK}_{s2}) \oplus 2H(R_1 + \text{TK}_{s1})$ which are random due to two random and fresh numbers r_1 and r_2 in each session. Therefore, the adversary can learn nothing about the identity of the tag from the transmission. The randomness and freshness of the two random numbers ensure the anonymity of the proposed scheme.

Tracking Attack Resistance. The essence of the active tracking resistance of the proposed scheme is that each calculation of $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$ involves the confusion value $H(R_1 + \text{TK}_{T1})$, where the computation of TK_{T1} needs either tag's secret r_2 or the server's private key x_s; therefore,

Table 1: Performance comparison.

	Arshad and Nikooghadam [12]	Liao and Hsiao [9]	He et al. [13]	Ours
The server's computational cost	$2T_{EM} + T_M + T_{\mathrm{INV}} + 8T_H = 490.58T_{EA} + 8T_H$	$5T_{EM} + 3T_{EA} = 1208T_{EA}$	$5T_{EM} + 2T_{EA} = 1207T_{EA}$	$4T_{EM} + 4T_{EA} + 2T_H = 968T_{EA} + 2T_H$
The tag's computational cost	$2T_{EM} + T_M + 7T_H = 490.58T_{EA} + 7T_H$	$5T_{EM} + 3T_{EA} = 1208T_{EA}$	$5T_{EM} + 2T_{EA} = 1207T_{EA}$	$4T_{EM} + 4T_{EA} + 2T_H = 968T_{EA} + 2T_H$
Number of rounds/steps	3	3	3	3
Total length of transmitted message	$8\,\lvert x\rvert + 2L_{\mathrm{ECC}}$	$4L_{\mathrm{ECC}}$	$4L_{\mathrm{ECC}}$	$4L_{\mathrm{ECC}}$
The tag's transmission length	$4\,\lvert x\rvert + L_{\mathrm{ECC}}$	$2L_{\mathrm{ECC}}$	$2L_{\mathrm{ECC}}$	$2L_{\mathrm{ECC}}$
The server's storage cost	$(n+1)\,\lvert x\rvert + L_{\mathrm{ECC}}$	$(n+1)\,\lvert x\rvert + nL_{\mathrm{ECC}}$	$\lvert x\rvert + (n+1)L_{\mathrm{ECC}}$	$\lvert x\rvert + (n+1)L_{\mathrm{ECC}}$
The tag's storage cost	$5\,\lvert x\rvert + L_{\mathrm{ECC}}$	$\lvert x\rvert + 2L_{\mathrm{ECC}}$	$2L_{\mathrm{ECC}}$	$2L_{\mathrm{ECC}}$
Security weaknesses		*Server impersonation*	*Active tracking*	*No*

an active tracker has no way to derive any verifiable data from the transmissions. We can verify this by launching the same active attack on our proposed protocol as follows, where Adv denotes the notion that the adversary impersonates the server to get the responses for tracking.

First of all, Adv randomly chooses $r_1 \in Z_n^*$, computes $R_1 = r_1P$, and sends message $m_1 = \{R_1\}$ to probe the tags it encounters. In the following, we assume Adv encounters the same tag Tag_{X_T}.

Upon receiving the query, Tag_{X_T} randomly chooses $r_2 \in Z_n^*$ and computes $R_2 = r_2P$, $\text{TK}_{T1} = r_2P_s$, $\text{TK}_{T2} = r_2R_1$, and $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$. Then, Tag_{X_T} sends back $m_2 = \{R_2, \text{Auth}_T\}$ to S. Since Adv cannot compute $\text{TK}_{T1} = r_2P_s$, Adv obtains nothing except Auth_T. When Tag_{X_T} is probed again, it randomly chooses $\overline{r_2} \in Z_n^*$ and computes $\overline{R_2} = \overline{r_2}P$, $\overline{\text{TK}_{T1}} = \overline{r_2}P_s$, $\overline{\text{TK}_{T2}} = \overline{r_2}R_1$, and $\overline{\text{Auth}_T} = (X_T + \overline{\text{TK}_{T2}}) \oplus H(R_1 + \overline{\text{TK}_{T1}})$. Then, Tag_{X_T} responds with $m_2 = \{\overline{R_2}, \overline{\text{Auth}_T}\}$. Adv cannot compute $\overline{\text{TK}_{T1}} = \overline{r_2}P_s$, and Adv obtains nothing except $\overline{\text{Auth}_T}$. Adv cannot verify whether the two transactions came from the same tag. That is, our proposed protocol can resist the active tracking attack.

Tag Masquerade Attack Resistance. To impersonate a tag, the adversary must be able to generate a valid message $m_2 = \{R_2, \text{Auth}_\text{T}\}$, where $\text{Auth}_T = (X_T + \text{TK}_{T2}) \oplus H(R_1 + \text{TK}_{T1})$. However, it is difficult to generate such a message without knowing the identity of the tag X_T.

Server Spoofing Attack Resistance. To impersonate the server, the adversary must be able to generate a valid message $m_3 = \{\text{Auth}_s\}$, where $R_1 = r_1P$ and $\text{Auth}_s = (X_T + 2\text{TK}_{s2}) \oplus 2H(R_1 + \text{TK}_{s1})$. It is easy for the adversary to generate R_1, but it is difficult to generate Auth_s without knowledge of the server's secret key x_s and the tag's identity X_T.

5.2. Performance Evaluation. We compare the proposed scheme with He et al.'s protocol [13] and some related schemes [9, 12] in terms of computational cost, communicational cost, and storage cost. Let T_{EA} denote the cost of point addition over an elliptic curve E, let T_{EM} denote the cost of scalar multiplication over an elliptic curve E, let T_M denote the cost of modular multiplication over the underlying field $F(q)$, let T_{INV} denote the cost of modular inverse over the underlying field $F(q)$, let T_H denote the cost of computing a hash value, let L_{ECC} denote the bit length of one elliptic curve point, let $|x|$ denote the size of integer x, and let n denote the number of tags in the system. To evaluate the complexity, we adopt the practical figures from [20]. In [20], it lists the timing for computing kP and $g^k \bmod p$, where E is an elliptic curve defined over $F(q)$, $q \approx 2^{160}$, P is a point whose order is 160-bit prime over E, k is a random 160-bit integer, and p is a 1024-bit prime. Therefore, we can conclude that $T_M \approx (41/5)T_{EA} \approx 8T_{EA}$, $T_{EM} \approx (29/0.12)T_{EA} \approx 241T_{EA}$, and $T_{\text{INV}} \approx (3 * 8/41)T_{EA} \approx 0.58T_{EA}$ [20]. Note that the cost of executing an exclusive-or operation (XOR) is negligible when compared with other operations stated above. Since the parameters params $= \{q, a, b, P, n\}$ are stored in both the server and the tag, the storage cost of params is omitted in the following comparison. The performance comparison is summarized in Table 1. Since He et al.'s protocol [13], Liao and Hsiao's scheme [9], Arshad and Nikooghadam's scheme [12], and our proposed scheme rely on the ECDLP, the elliptic curve scalar multiplication is the most time-consuming operation in the elliptic curve cryptosystem. Although our proposed scheme has the same communicational and storage costs as He et al.'s protocol, our proposed scheme owns better computational performance by eliminating one elliptic curve scalar multiplication operation. Our proposed scheme is more efficient than Liao and Hsiao's scheme because our proposed scheme requires less cost in terms of computation, communication, and storage. Table 1 shows that Arshad and Nikooghadam's scheme requires less computational cost than our proposed scheme. However, it has been studied that communication consumes more energy than computation in embedded wireless communication systems like RFID and wireless sensor network [21, 22]. Studies in the past have shown that 3000 instructions could be executed for the same energy usage as sending a bit 100 m by radio [23]; therefore, many studies in these fields devoted lots of efforts to reducing the communication complexity [24, 25]. It is important to optimize communication and minimize energy consumption. In our proposed scheme, the tag communication requires only 50% of that of Arshad and Nikooghadam's scheme, while our scheme achieves the same security properties with slightly more computations.

6. Conclusions

Mobile healthcare systems are becoming more and more popular. Lack of protecting patient and data privacy may hinder the utility of mobile healthcare system. In this paper, we have shown the weakness of He et al.'s protocol. The protocol cannot meet privacy protection requirement since it is vulnerable to active tracking attack. We have proposed a new scheme which not only conquers the security weaknesses but also improves the computational performance.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This project is partially supported by the National Science Council, Taiwan, under Grant no. MOST 103-2221-E-260-022.

References

[1] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "User privacy in transport systems based on RFID e-tickets," in *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications*, pp. 102–122, Malaga, Spain, October 2008.

[2] Y.-C. Yen, N.-W. Lo, and T.-C. Wu, "Two RFID-based solutions for secure inpatient medication administration," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2769–2778, 2012.

[3] Y. Chen, J.-S. Chou, and H.-M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, pp. 2373–2380, 2008.

[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[5] V. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85 Proceedings*, vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, Berlin, Germany, 1985.

[6] Y. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol," in *IEEE International Conference on RFID*, pp. 97–104, Las Vegas, Nev, USA, April 2008.

[7] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Cryptology and Network Security: 7th International Conference, CANS 2008, Hong-Kong, China, December 2–4, 2008. Proceedings*, vol. 5339 of *Lecture Notes in Computer Science*, pp. 149–161, Springer, Berlin, Germany, 2008.

[8] T. Deursen and S. Radomirovic, "Attacks on RFID protocols (version 1.1)," Tech. Rep., University of Luxembourg, 2009.

[9] Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Networks*, vol. 18, pp. 133–146, 2014.

[10] R. Peeters and J. Hermans, *Attack on Liao and Hsiao's Secure ECC-based RFID Authentication Scheme Integrated with ID-Verifier Transfer Protocol*, Cryptology ePrint Archive, 2013.

[11] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, article 16, 2014.

[12] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 38, no. 12, article 136, 2014.

[13] D. He, N. Kumar, N. Chilamkurti, and J.-H. Lee, "Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol," *Journal of Medical Systems*, vol. 38, article 116, 2014.

[14] V. Miller, "Short programs for functions on curves," 1986, https://crypto.stanford.edu/miller/miller.pdf.

[15] A. J. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.

[16] C.-Y. Lin, T.-C. Wu, F. Zhang, and J.-J. Hwang, "New identity-based society oriented signature schemes from pairings on elliptic curves," *Applied Mathematics and Computation*, vol. 160, no. 1, pp. 245–260, 2005.

[17] A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *Proceedings of the 4th Algorithmic Number Theory Symposium (ANTS '00)*, pp. 385–394, Leiden, The Netherlands, July 2000.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO 2001*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, 2001.

[19] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Advances in Cryptology—ASIACRYPT 2001*, vol. 2248 of *Lecture Notes in Computer Science*, pp. 514–532, Springer, Berlin, Germany, 2001.

[20] A. Jurisic and A.-J. Menezes, "Elliptic curves and cryptography," *Dr. Dobb's Journal*, pp. 26–36, 1997.

[21] F. Zhao and L. J. Guibas, *Wireless Sensor Networks: An Information Processing Approach*, Elsevier-Morgan Kaufmann, San Francisco, Calif, USA, 2004.

[22] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[23] J. Pottie and W. J. Kaiser, "Embedding the internet wireless integrated network sensors," *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, 2000.

[24] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 2, pp. 28–36, 2002.

[25] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan, "Building efficient wireless sensor networks with low-level naming," in *Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP '01)*, pp. 146–159, Banff, Canada, 2001.

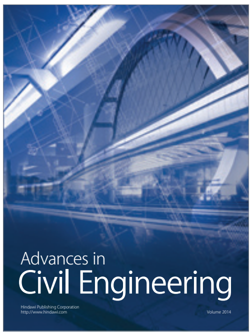
Journal of
Engineering

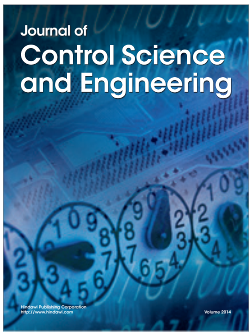
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

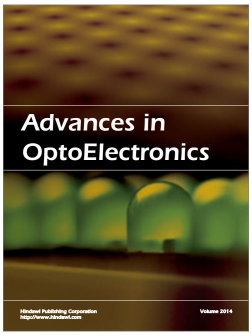
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

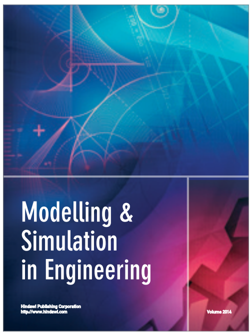
Journal of
Robotics

Journal of
Electrical and Computer Engineering

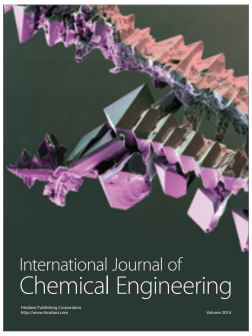

Advances in
OptoElectronics

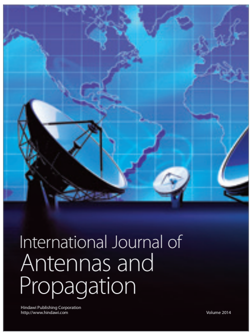
VLSI Design

International Journal of
Navigation and Observation

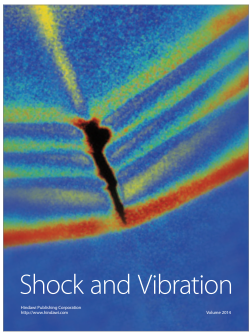

Modelling & Simulation in Engineering

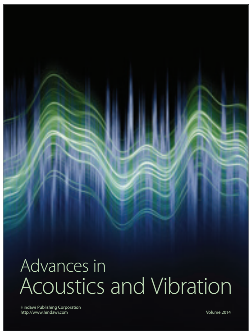
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration