J Supercomput (2014) 70:987–1001
DOI 10.1007/s11227-014-1272-0

Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography

Mohammad Sabzinejad Farash

Published online: 27 July 2014

Abstract Radio frequency identification (RFID) is a wireless technology for automatic identification and data capture. Security and privacy issues in the RFID systems have attracted much attention. Many approaches have been proposed to achieve the security and privacy goals. One of these approaches is RFID authentication protocols by which a server and tags can authorize each other through an intracity process. Recently, Chou proposed a RFID authentication protocol based on elliptic curve cryptography. However, this paper demonstrates that the Chou's protocol does not satisfy tag privacy, forward privacy and authentication, and server authentication. Based on these security and privacy problems, we also show that Chou's protocol is defenseless to impersonation attacks, tag cloning attacks and location tracking attacks. Therefore, we propose a more secure and efficient scheme, which does not only cover all the security flaws and weaknesses of related previous protocols, but also provides more functionality. We prove the security of the proposed improved protocol in the random oracle model.

Keywords RFID · Elliptic curve · Authentication protocol · Untraceable privacy · Random oracle model

1 Introduction

Radio frequency identification (RFID) technology is rapidly becoming ubiquitous, gradually replacing barcodes as the means of product or item identification [1]. A typical RFID system consists of three components: tags, readers, and a back-end server. An RFID tag is a radio transponder that is composed of an integrated circuit for storing

M. S. Farash (✉)
Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran
e-mail: m.sabzinejad@gmail.com; sabzinejad@khu.ac.ir; sabzinejad@tmu.ac.ir

and processing identification information, as well as an antenna for communicating with RFID readers [2,3]. When a back-end server wants to identify one or more tags, a reader emits an interrogation signal via its antenna. Any tag within range of the signal responds with certain stored data, such as a tag identifier. The reader then passes the received tag data to the back-end server for further processing, including tag identification and information retrieval [4]. The radio interface between the tags and reader is generally insecure, while the channel between the reader and back-end server is a fixed infrastructure and can be generally assumed to be secure. The insecure wireless communication channel between the tags and reader will induce some serious security and privacy problems. The possible security threats to RFID systems include denial of service, man in the middle, counterfeiting, spoofing, eavesdropping, traffic analysis, traceability, de-synchronization etc. One of the most important way to assure privacy and security in RFID systems is authentication protocol [5,6].

Many efficient and private RFID authentication schemes have been proposed in the literature. Most attempts to design RFID authentication protocols rely on the use of symmetric key cryptography (e.g., [7–12]). The main reason why most RFID authentication protocols use symmetric-key primitives, lies in the common perception of public-key cryptography being too slow, power-hungry and too complicated for such low-cost environments. However, recent works proved this concept to be wrong, as for example the smallest published elliptic curve implementations [13,14] consume less area than the candidate cryptographic hash algorithms proposed in the SHA-3 competition [15]. Moreover, symmetric-key solutions usually suffer from scalability problems, that is, the back-end server requires a linear search to identify a tag [16–19]. These have led to the introduction of public-key based RFID authentication protocols using elliptic curve cryptography (ECC). This approach solves the scalability issues, prevents cloning attacks and offers advanced privacy protection [20,21].

In 2006, the first ECC-based RFID authentication protocol was proposed by Tuyls and Batina [22] using the Schnorr identification scheme [23]. In 2007, Batina et al. [24] proposed a similar ECC-based solution by applying Okamoto identification scheme [25]. But, Lee et al. [26] pointed both Tuyls and Batina's protocol, and Batina et al.'s protocol suffer from privacy problems. To address these privacy problems, Lee et al. [26], O'Neill and Robshaw [27] and Godor et al. [28] separately proposed improved ECC-based RFID authentication protocols. However, Chou [21] recently indicated that the three schemes [26–28] still have no scalability. Chou then designed a novel ECC-based RFID authentication protocol, to avoid these issues.

In this paper, we show that Chou's protocol [21] does not achieve tag (forward) privacy, tag authentication, server authentication, and mutual authentication. As such the protocol is susceptible to impersonation attacks, location tracking attacks and tag cloning attacks. Then, we propose an improved protocol to enhance the security of Chou's protocol. Our improved protocol does not only maintain the merits and cover the demerits of the Xie's protocol, but also meets all the requirements of such protocols. Finally, the security of the proposed protocol is proved in the random oracle model.

The rest of this paper is organized as follows. Section 2 introduces the definitions of elliptic curves and security model of RFID authentication protocols. In Sect. 3, we review the Chou's RFID authentication protocol. In Sect. 4, we describe the weaknesses of the Chou's protocol. An improved protocol is proposed and analyzed in

Sect. 5. In Sect. 6, we make a comparison between our protocol and some related protocols. In Sect. 7 we make a comparison between security and performance. Finally 8 concludes the paper.

2 Preliminaries

2.1 Elliptic curves

An elliptic curve E over a field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$ and $\Delta \neq 0$ where Δ is the discriminate of E. The above equation is called the Weierstrass equation. The condition $\Delta \neq 0$ ensures that the elliptic curve is smooth, that is, there are no points at which the curve has two or more distinct tangent lines. Also included in the definition of an elliptic curve is a single element denoted by $\mathcal{O}$ and called the *point at infinity*. The *chord and tangent rule* is used for adding two points to give a third point on an elliptic curve. Together with this addition operation, the set of points denoted as $E(\mathbb{F}_p)$ forms a commutative group $\mathbb{G}$ under addition with $\mathcal{O}$ serving as its identity and P as its generation.

Elliptic curves have been widely used to construct cryptographic primitives including encryption functions, signature scheme, cryptographic protocols and so on (e.g., [29–34]).

2.2 Computational assumptions

Let $\mathbb{G}$ be a cyclic additive group generated by P, whose order is a prime p.

Definition 1 (*Discrete Logarithm Problem (DLP)*) Given $P, aP \in \mathbb{G}$, find $a \in \mathbb{Z}_p^*$.

Definition 2 (*Computational Diffie–Hellman Problem (CDHP)*) For $a, b \in \mathbb{Z}_p^*$, given $P, aP, bP \in \mathbb{G}$, find $abP \in \mathbb{G}$.

Definition 3 (*Decision Diffie–Hellman Problem (DDHP)*) For $a, b, c \in \mathbb{Z}_p^*$, given $P, aP, bP, cP \in \mathbb{G}$, find if $cP = abP$.

2.3 Security requirements

Several security requirements for RFID systems were described in the literature [35].

– *Anonymity* The most important information of a tag which need to be kept secure is tag's identifier. This identifier is used in the authentication procedures between the tag and the server. Disclosure the tag's identity makes the RFID system vulnerable to various attacks including cloning attack and tracking attack. Thus, it is needed for a RFID system to provide the tag anonymity.

Table 1 Notations

Notation	Description
$\mathbb{G}$	An additive group of prime order q on an elliptic curve
P	A generator of $\mathbb{G}$
X_i	The identifier of ith tag which is a random point in $\mathbb{G}$
y	The private key of the server
Y	The public key of the server which is $Y = yP$
h	A one-way hash function

- *Location privacy* In a RFID system, the location of users should be kept private as well as tags' identifier. Location privacy means that, an adversary cannot distinguish two messages sent from a particular tag. This property guarantees that the adversary cannot track or monitor the tags.
- *Mutual authentication* This property means that the tags and the legal reader/server can successfully authorize each other. In the other words, an attacker cannot masquerade as a legal tag or the reader/server.
- *Forward privacy* This property means that, an adversary who compromises a tag and obtains the stored data in the tag's memory cannot trace the tag through past conversations the tag involved in.
- *Resistant to replay attack* In a replay attack, an adversary who eavesdropped and captured the conversation between a tag and the server replays the obtained messages to the legitimate destination as being authentic. It is necessary for a RFID system to resist this attack.

3 Review of Chou's scheme

There are two roles: server/reader and tag in Chou's RFID system. The server is used to stand for server/reader and the communication between the server and tag is assumed to be insecure. Chou's system consists of two phases: setup phase and authentication phase. The notations used to describe the system are listed in Table 1.

3.1 Setup phase

In this phase, the server chooses a random number $y \in \mathbb{Z}_q$ as its private key and computes $Y = yP$ as its public key. It also chooses a random point $X_i \in \mathbb{G}$ as the identifier of ith tag and then stores each tag's identifier and related information in its database, where the information includes the name of the tag and production number, and so on. Finally, the server stores $\{X_i, Y, P\}$ in each tag's memory.

3.2 Authentication phase

When interrogating a set of tags, the server broadcasts a random point. Each tag in the range of the interrogation signal performs the authentication protocol shown in Fig. 1 as follows:

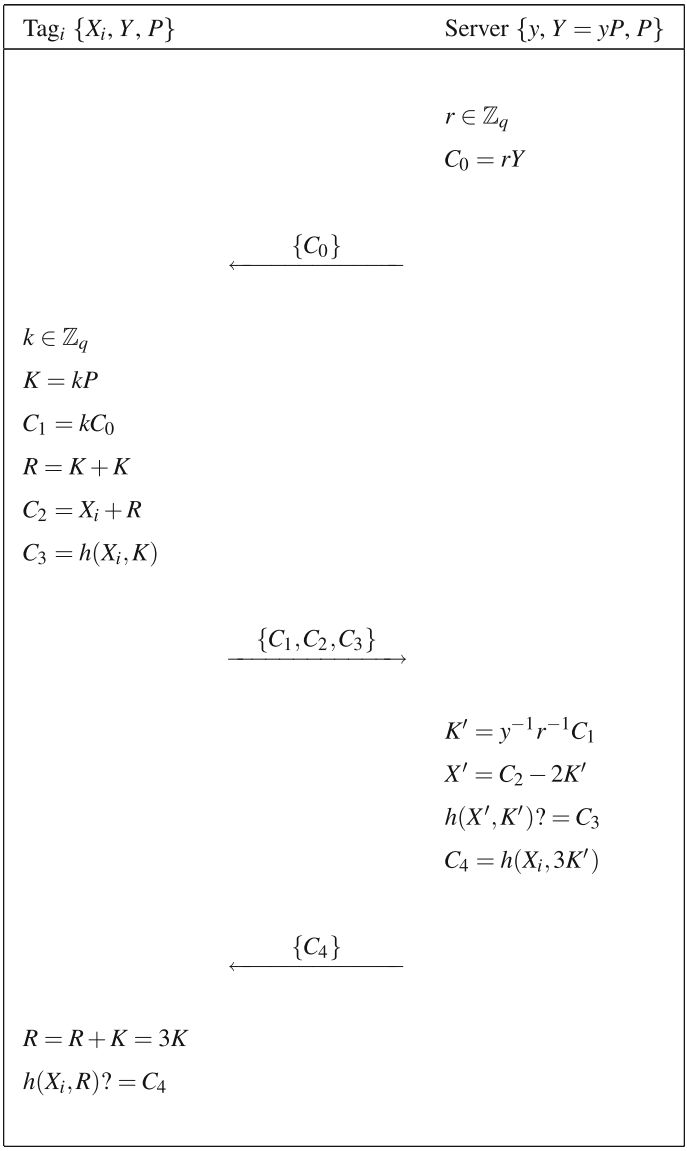

Fig. 1 Chou's RFID mutual-authentication scheme

Step 1: The server chooses a random integer $r \in \mathbb{Z}_q$, computes $C_0 = rY$ and broadcasts interrogation message C_0 to the Tag$_i$.
Step 2: On receiving the interrogation, Tag$_i$ picks a random integer $k \in \mathbb{Z}_q$ and computes $K = kP$ and $C_1 = kC_0$. Tag$_i$ then sets a register R as $K + K$ and computes $C_2 = X_i + R$ and $C_3 = h(X_i, K)$. Then Tag$_i$ sends $\{C_1, C_2, C_3\}$ to the server.
Step 3: On receiving the message $\{C_1, C_2, C_3\}$, the server extracts $K' = y^{-1}r^{-1}C_1$ and computes candidate tag identifier $X' = C_2 - 2K'$. The server then computes

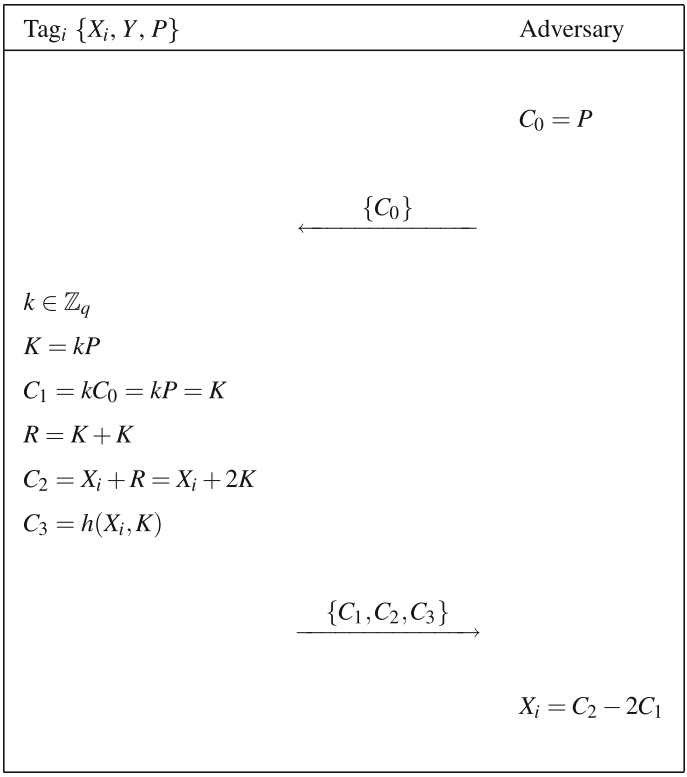

Fig. 2 Breaking the privacy of Chou's scheme

a hash value, $h(X', K')$ and compares it with the received C_3. If they are equal, the server directly fetches X' from its database. If succeeds, the Tag$_i$'s identity is authenticated, and the server will authenticate itself to the Tag$_i$ by making a hash value $C_4 = h(X_i, 3K')$. If the candidate X' is not found in the server's database, the server sets C_4 as a random integer u to prevent possible location privacy leakage. Finally, the server returns C_4 to the Tag$_i$.
Step 4: On receiving C_4, the Tag$_i$ increments the register R by K (now the value in register R is $3K$) and computes a hash value $h(X_i, R)$. Then Tag$_i$ compares the hash result with the received C_4. If they are equal, Tag$_i$ believes that the counterpart is the true server.

4 Weaknesses of Chou's scheme

4.1 Lack of tag privacy

Tag privacy relies on the inability of the adversary to learn the tag's identifier X_i. However, the tag's identifier can easily be obtained from the tag in Chou's scheme, without physical attacks. To do so, the adversary $\mathcal{A}$ performs the following steps with Tag$_i$ as shown in Fig. 2):

Step 1: The adversary $\mathcal{A}$ generates and sends the message $C_0 = P$ to the Tag_i.
Step 2: On receiving the interrogation, Tag_i picks a random integer $k \in \mathbb{Z}_q$ and computes $K = kP$ and

$$C_1 = kC_0 = kP = K.$$

Tag_i then sets a register R as $K + K$ and computes

$$C_2 = X_i + R = X_i + 2K$$
$$C_3 = h(X_i, K).$$

Then Tag_i sends $\{C_1, C_2, C_3\}$ to the server.
Step 3: The adversary $\mathcal{A}$ intercepts the message $\{C_1, C_2, C_3\}$. Since $C_1 = K$ and $C_2 = X_i + 2K$, the adversary $\mathcal{A}$ can obtain the Tag_i's identifier X_i as follows:

$$\begin{aligned} C_2 - 2C_1 &= (X_i + 2K) - 2K \\ &= X_i. \end{aligned}$$

4.2 Lack of forward privacy

Forward privacy relies on the inability of the adversary to track Tag_i by knowing the identifier X_i. Chou's scheme obviously lacks forward privacy. This is because when an adversary performs above-mentioned steps and obtains the identifier X_i of a specific tag Tag_i, he/she can use this X_i to determine whether a past conversation, $\{C_0^*, C_1^*, C_2^*, C_3^*\}$, belongs to the specific tag by computing $K^* = 2^{-1}(C_2^* - X_i)$, and evaluating the equation $h(X_i, K^*)? = C_2^*$. Therefore, Chou's scheme is vulnerable to location tracking attacks.

4.3 Lack of mutual authentication

After obtaining the Tag_i's identifier X_i, the adversary $\mathcal{A}$ can impersonate not only Tag_i but also the server. To impersonate Tag_i, the adversary $\mathcal{A}$ performs same as the actual tag because he/she know the secret identifier X_i. To impersonate the server, the adversary $\mathcal{A}$ can continues the attack described in Sect. 4.1 by sending $C_4 = h(X_i, 3C_1) = h(X_i, 3K)$ to Tag_i's. On receiving C_4, Tag_i's compares it with $h(X_i, 3K)$, and accepts it because they are equal. Therefore, the adversary $\mathcal{A}$ have succeeded to masquerade as the legal server. Therefore, Chou's protocol does not achieve tag authentication, server authentication, and mutual authentication.

5 Our improved scheme

To solve the security problems of RFID authentication protocols, we propose an improved ECC-based protocol.

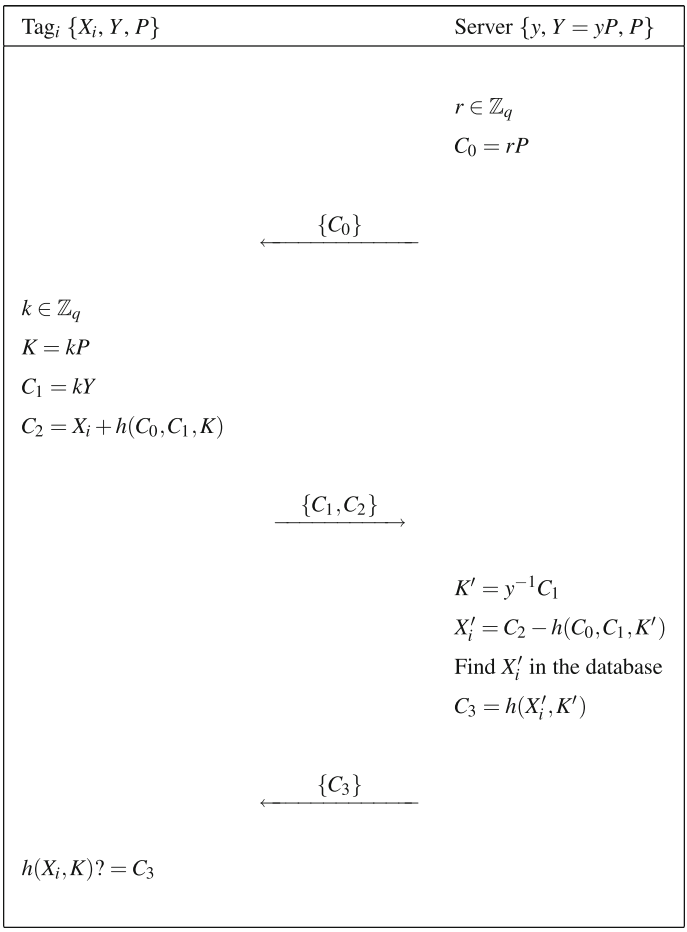

Fig. 3 Improved RFID mutual-authentication scheme

5.1 Protocol description

When interrogating a set of tags, the server broadcasts a random point. Each tag in the range of the interrogation signal performs the authentication protocol shown in Fig. 3 as follows:

Step 1: The server chooses a random integer $r \in \mathbb{Z}_q$, computes

$$C_0 = rP, \tag{1}$$

and broadcasts interrogation message C_0 to the Tag$_i$.
Step 2: On receiving the interrogation message C_0, Tag$_i$ picks a random integer $k \in \mathbb{Z}_q$ and computes

$$K = kP, \tag{2}$$
$$C_1 = kY, \tag{3}$$
$$C_2 = X_i + h(C_0, C_1, K). \tag{4}$$

Tag_i then sends $\{C_1, C_2\}$ to the server.
Step 3: On receiving the message $\{C_1, C_2\}$, the server extracts

$$K' = y^{-1}C_1 \tag{5}$$

and computes candidate tag identifier

$$X_i' = C_2 - h(C_0, C_1, K'). \tag{6}$$

The server then directly fetches X_i' from its database. If succeeds, the server makes a hash value

$$C_3 = h(X_i', K'). \tag{7}$$

Finally, the server returns C_3 to the Tag_i.
Step 4: On receiving C_3, the Tag_i checks if

$$h(X_i, K)? = C_3. \tag{8}$$

If it holds, Tag_i believes that the counterpart is the true server.

6 Security analysis of our improved protocol

In this section, we prove the correctness and the privacy of the improved authentication RFID scheme in the random oracle model.

6.1 Security model of RFID authentication protocols

6.1.1 Participants

A RFID authentication protocol is run in a network of a number of interconnected participants where each participant is either a tag $T \in \mathcal{T}$ or a trusted server $S \in \mathcal{S}$. The set $\mathcal{S}$ is assumed to involve only a single server for simplicity. Each of the participants may have several instances called oracles involved in distinct executions of the protocol Π. We refer to ith instance of T (resp. S) in a session as Π_T^i (resp. Π_S^i). Every instance Π_T^i (resp. Π_S^j) has a partner identifier pid_T^i (resp:pid_S^j), a session identifier sid_T^i (resp:sid_S^j), and an output decision $output_T^i$ (resp:$output_S^j$). pid_T^i (resp:pid_S^j) denotes the set of the identities that are involved in this instance. sid_T^i (resp:sid_S^j) denotes the flows that are sent and received by the instance Π_T^i (resp. Π_S^j). $output_T^i$ (resp:$output_S^j$) is either $Accept$ or $Reject$; if the instance Π_T^i (resp. Π_S^j) feels the protocol has been normally executed outputs $Accept$, otherwise it outputs $Reject$.

Definition 4 (*Accepted Instance*) An instance Π_T^i (resp. Π_S^i) is said to be *Accepted* if and only if it holds (1) a session identifier sid_T^i (resp:sid_S^j), (2) a partner identifier pid_T^i (resp:pid_S^j), and (3) an output decision $output_T^i = Accept$ (resp:$output_S^j = Accept$).

Definition 5 (*Partnered Instances*) Two instances Π_T^i and Π_S^j are *partners* if and only if: (1) $pid_T^i = pid_S^j$; (2) $sid_T^i = sid_S^j$.

6.1.2 Long-lived keys

Each tag $T \in \mathcal{T}$ holds a secret identifier X_T. The server S holds a vector $\langle X_T \rangle_{T \in \mathcal{T}}$ with an entry for each tag, and a public/privat key pair $\langle y_S, Y_S = y_S P \rangle$.

6.1.3 Adversary model

The communication network is assumed to be fully controlled by an adversary $\mathcal{A}$, which schedules and mediates the sessions among all the parties. The adversary $\mathcal{A}$ is allowed to issue the following queries in any order:

Execute(Π_T^i, Π_S^j): This query models passive attacks in which the attacker eavesdrops on honest executions among the tag instance Π_T^i and the trusted server instance Π_S^j. The output of this query consists of the messages that were exchanged during the honest execution of the protocol.
Send(Π_T^i (resp. Π_S^j), m): The adversary makes this query to intercept a message and then modify it, create a new one, or simply forward it to the instance Π_T^i (resp. Π_S^j). The output of this query is the message that the instance Π_T^i (resp. Π_S^j) would generate upon receipt of message m. Additionally, the adversary is allowed to initiate the protocol between the tag T and the server S by invoking Send(Π_T^i, (Π_S^i, $Start$)) (resp. Send(Π_S^i, (Π_T^i, $Start$))).
Corrupt(T): This query returns to the adversary the secret identifier X_T of the tag T.
Test(T): Only one query of this form is allowed to be made by the adversary to an uncorrupted T. To respond to this query, a random bit $b \in \{0, 1\}$ is selected. If $b = 1$, then a Execute(Π_T^i, Π_S^j) query is made and the messages that were exchanged during the honest execution of the protocol are respond to the adversary. Otherwise, uniformly chosen random values are returned.

6.1.4 Untraceable privacy

To model the untraceable privacy of an authentication RFID protocol, a game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ as follows:

Learning Phase: $\mathcal{A}$ can issue any Execute, Send, and Corrupt queries.
Challenging Phase: In this phase, $\mathcal{A}$ issues a Test query on an uncorrupted tag. The Challenger tosses a random bit $b \in \{0, 1\}$ and responses according to the Test query. $\mathcal{A}$ then continues making any Execute, Send, and Corrupt queries.

Guessing Phase: Eventually, $\mathcal{A}$ outputs a prediction (b') on b. $\mathcal{A}$ wins the game if $b' = b$, and we define $\mathcal{A}$'s advantage (l is the security parameter) in winning the game as

$$Adv^{\mathcal{A}}(l) = |\Pr[b' = b] - 1/2|. \tag{9}$$

Definition 6 (*Negligible Function*) A function $\epsilon(l)$ is called negligible (in the parameter l) if for every $c \geq 0$ there exists an integer $k_c > 0$ such that for all $l > k_c$, $\epsilon(l) < l^{-c}$.

Definition 7 (*Untraceable Privacy*) An authentication RFID protocol has untraceable privacy if:

1. *Correctness*: In the presence of a benign adversary, which faithfully conveys messages, both partner instances Π_T^i and Π_S^j output Accept decisions (i.e., $output_T^i = output_S^j = Accept$).
2. *Privacy*: For any polynomial time adversary $\mathcal{A}$, the advantage $Adv^{\mathcal{A}}(l)$ in winning the above game is negligible.

6.2 Security proof

Lemma 1 (Correctness) *In the presence of a benign adversary, which faithfully conveys messages, both partner instances Π_T^i and Π_S^j in the improved authentication RFID scheme output Accept decisions (i.e., $output_T^i = output_S^j = Accept$).*

Proof According to the protocol description, the server S accepts tag_i if the parameter X_i' computed by S is equal to the Tag_i's identifier X_i. This equality holds, since according to the Eqs. (1), (3), (4), (5) and (6):

$$\begin{aligned}
X_i' &= C_2 - h(C_0, C_1, K'). \\
&= (X_i + h(C_0, C_1, K)) - h(C_0, C_1 r y^{-1} C_1) \\
&= (X_i + h(C_0, C_1, K)) - h(C_0, C_1, y^{-1} k Y) \\
&= (X_i + h(C_0, C_1, K)) - h(C_0, C_1, y^{-1} k y P) \\
&= (X_i + h(C_0, C_1, K)) - h(C_0, C_1, kP) \\
&= (X_i + h(C_0, C_1, K)) - h(C_0, C_1, K) \\
&= X_i.
\end{aligned}$$

Moreover, the server is accepted by Tag_i if the Eq. (8) holds. We show that it holds as follows:

$$
\begin{aligned}
C_3 &= h(X_i', K') \\
&= h((C_2 - h(C_0, C_1, K')), y^{-1}C_1) \\
&= h((C_2 - h(C_0, C_1, y^{-1}C_1)), y^{-1}C_1) \\
&= h((C_2 - h(C_0, C_1, kP)), kP) \\
&= h(((X_i + h(C_0, C_1, K)) - h(C_0, C_1, kP)), kP) \\
&= h(((X_i + h(C_0, C_1, kP)) - h(C_0, C_1, kP)), kP) \\
&= h(X_i, kP) \\
&= h(X_i, K).
\end{aligned}
$$

□

Lemma 2 (Privacy) *In the improved authentication RFID scheme, for any polynomial time adversary $\mathcal{A}$, the advantage $Adv^{\mathcal{A}}(l)$ in winning the game with a challenger is negligible.*

Proof For a contradiction, assume that there is an adversary $\mathcal{A}$ against our scheme that has a non-negligible advantage $\epsilon(l)$. Using this adversary, we show how to construct a challenger $\mathcal{C}$ that can solve the DDH problem with non-negligible advantage $\epsilon'(l)$. Suppose the challenger $\mathcal{C}$ is given an instance $(P_1 = P, P_2 = aP, P_3 = bP, P_4 = cP) \in \mathbb{G}$ of the DDH problem for $a, b, c \in \mathbb{Z}_q^*$, and is faced to find if $P_4 = abP$.

Assume that the game between $\mathcal{C}$ and $\mathcal{A}$ involves $n_t(l)$ tags where l is the security parameter. The challenger $\mathcal{C}$ works by interacting with the adversary $\mathcal{A}$ as follows:

Setup Phase: $\mathcal{C}$ simulates the system setup to the adversary $\mathcal{A}$ and defines the system public parameters $\{\mathbb{G}, P, h\}$. $\mathcal{C}$ then sets the public key of the server as $Y = P_2 = aP$ which is the input of DDH problem and gives it to $\mathcal{A}$; hence $\mathcal{C}$ does not know the long-term private key of the server. $\mathcal{C}$ then randomly chooses $I \in \{1, \ldots, n_t(l)\}$ to assign Tag_I as the target of Test query.

Learning Phase: $\mathcal{A}$ can issue any Execute, Send, and Corrupt queries.

- Execute(Π_T^i, Π_S^j): $\mathcal{C}$ returns the tuple $\{C_0, C_1, C_2, C_3\}$ to $\mathcal{A}$, which are the exchanged message between to instances Π_T^i and Π_S^j.
- Send(Π_T^i (resp. Π_S^j), m): $\mathcal{C}$ returns to the adversary the message that the instance Π_T^i (resp. Π_S^j) would generate upon receipt of message m.
- Corrupt(Tag_t): $\mathcal{C}$ returns to the adversary the secret identifier X_t of Tag_t.

Challenging Phase: In this phase, $\mathcal{A}$ issues a Test query on an uncorrupted tag Tag_t. If $\text{Tag}_t \neq \text{Tag}_I$, $\mathcal{C}$ aborts the simulation. Otherwise, $\mathcal{C}$ chooses random numbers $r, s \in \mathbb{Z}_q^*$ and sets $C_0 = rP$ and $K = rP$. Since b and b are unknown, $\mathcal{C}$ can not compute the real parameters C_1 as abP, thus it sets $C_1 = P_4 = cP$ and computes $C_2 = X_I + h(C_0, C_1, K)$ and $C_3 = sP$. Then, $\mathcal{C}$ returns $\{C_0, C_1, C_2, C_3\}$ to $\mathcal{A}$.

Guessing Phase: Eventually, $\mathcal{A}$ outputs a guess with a non-negligible advantage $\epsilon(l)$ to indicate that whether the received response in the challenging phase is a valid tuple or not. If the guess is YES, then $C_1 = abP$; if NO, $C_1 \neq abP$.

Table 2 Performance comparison

	Tuyls's [22]		Batina's [24]		Lee's [26]		Chou's [21]		Ours	
	Tag	Server	Tag	Server	Tag	Server	Tag	Server	Tag	Server
Hash functions	0	0	0	0	0	0	2	2	2	2
Scaler multiplications	1	2n	2	3n	3	1+2n	2	3	2	3

n The number of tags

Therefore, $\mathcal{C}$ can find if $C_1 = abP$ using $\mathcal{A}$ and resultantly can compute the DDH problem. In the following we compute the success probability of $\mathcal{C}$ to solve DDH problem within this game.

Success Probability: $\mathcal{C}$ aborts the simulation only if $\mathcal{A}$ issues a Test query on an tag Tag_t other than the chosen tag Tag_I. Therefore, the success probability that $\mathcal{C}$ solves DDH problem is

$$\epsilon'(l) \geq (\frac{1}{n_t(l)})\epsilon(l),$$

which is a non-negligible function.

□

Theorem 1 *The improved authentication RFID scheme has untraceable privacy, provided the DDH assumption holds. Specifically, suppose an adversary $\mathcal{A}$ wins the game with non-negligible advantage $\epsilon(l)$. Then there exists a polynomial-time algorithm $\mathcal{C}$ to solve the DDH problem with non-negligible advantage $\epsilon'(l) \geq (\frac{1}{n_t(l)})\epsilon(l)$.*

Proof From Lemma 1 and Lemma 2. □

7 Security and performance comparison

In this section, we evaluate the performance and functionality of our proposed protocol and make comparisons with some related ECC-based RFID authentication protocols. Table 2 shows the performance comparisons of our proposed protocol and some other related protocols. It can be seen that the computation cost of the proposed protocol is same as the Chou's scheme.

Table 3 lists the security comparisons among our proposed protocol and other related protocols. It demonstrates that our protocol has many excellent features and is more secure than other related protocols.

8 Conclusion

In this paper, we briefly reviewed the Chou's ECC-based RFID authenticated protocol. We Showed that the Chou's protocol does not satisfy tag (forward) privacy, tag authentication, server authentication, and mutual authentication. As such the protocol was

Table 3 Security comparison

	Tuyls's [22]	Batina's [24]	Lee's [26]	Chou's [21]	Ours
Reply attack	Secure	Secure	Secure	Secure	Secure
Man-in-the-middle attack	Insecure	Insecure	Insecure	Secure	Secure
Impersonation attack	Insecure	Insecure	Insecure	Insecure	Secure
Mutual authentication	Not-provided	Not-provided	Not-provided	Not-provided	Provided
Location privacy	Not-provided	Not-provided	Provided	Not-provided	Provided
Forward privacy	Not-provided	Not-provided	Provided	Not-provided	Provided

susceptible to impersonation attacks, location tracking attacks and tag cloning attacks. To overcome the security weaknesses, we proposed an improved protocol. In comparison to the related schemes, the proposed scheme not only is secure against well-known cryptographical attacks, but also provides more security features. However, the total computation of the improved protocol seems to be high for a RFID system. Therefore, reducing the computational cast especially for tag side is our future work. It can be achieved by using pre-computing technics.

References

1. Burmester M, Le TV, Medeiros BD, Tsudik G (2009) Universally composable RFID identification and authentication protocols. ACM Trans Inf Syst Secur (TISSEC) 12(4):21
2. Juels A, Weis S (2006) Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137
3. Cai S, Li Y, Li T, Deng RH (2009) Attacks and improvements to an RIFD mutual authentication protocol and its extensions. In: Proceedings of the second ACM conference on wireless network security, pp 51–58
4. Song B, Mitchell CJ (2011) Scalable RFID security protocols supporting tag ownership transfer. Comput Commun 34(4):556–566
5. Niu B, Zhu X, Chi H, Li H (2014) Privacy and authentication protocol for mobile RFID systems. Wirel Pers Commun. doi:10.1007/s11277-014-1605-6
6. Shao-hui W, Zhijie H, Sujuan L, Dan-wei C (2013) Security analysis of two lightweight RFID authentication protocols. Ann Telecommun. doi:10.1007/s12243-013-0361-z
7. Dehkordi MH, Farzaneh Y (2013) Improvement of the hash-based RFID mutual authentication protocol. Wirel Pers Commun. doi:10.1007/s11277-013-1358-7
8. Safkhani M, Peris-Lopez P, Hernandez-Castro JC, Bagheri N (20174) Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol. J Comput Appl Math 259(1):571–577
9. Alagheband MR, Aref MR (2013) Simulation-based traceability analysis of RFID authentication protocols. Wirel Pers Commun. doi:10.1007/s11277-013-1552-7
10. Chen CL, Huang YC, Shih TF (2012) A novel mutual authentication scheme for RFID conforming EPCglobal class 1 generation 2 standards. Inf Technol Control 41(3):220–228
11. Kuo WC, Chen BL, Wuu LC (2013) Secure indefinite-index RFID authentication scheme with challenge-response strategy. Inf Technol Control 42(2):124–130
12. Alagheband MR, Aref MR (2013) Unified privacy analysis of newfound RFID authentication protocols. Secur Commun Netw 6(8):999–1009
13. Hein D, Wolkerstorfer J, Felber N (2009) ECC is ready for RFID—a proof in silicon. Sel Areas Cryptogr LNCS 5381:401–413
14. Lee YK, Sakiyama K, Batina L, Verbauwhede I (2008) Elliptic curve based security processor for RFID. IEEE Trans Comput 57(11):1514–1527
15. N.N.I., Technology of Standards: Cryptographic hash algorithm competition. http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

16. Ning H, Liu H, Mao J, Zhang Y (2011) Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. IET Commun 5(12):1755–1768
17. Alomair B, Clark A, Cuellar J, Poovendran R (2012) Scalable RFID systems: a privacy-preserving protocol with constant-time identification. IEEE Trans Parallel Distrib Syst 23(8):1536–1550
18. Alomair B, Poovendran R (2010) Privacy versus scalability in radio frequency identification systems. Comput Commun 33(18):2155–2163
19. Song B, Mitchell CJ (2011) Scalable RFID security protocols supporting tag ownership transfer. Comput Commun 34(4):556–566
20. Batina L, Lee YK, Seys S, Singele D, Verbauwhede I (2012) Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Pers Ubiquitous Comput 16(3):323–335
21. Chou JS (2013) An efficient mutual authentication RFID scheme based on elliptic curve cryptography. J Supercomput. doi:10.1007/s11227-013-1073-x
22. Tuyls P, Batina L (2006) RFID-tags for anti-counterfeiting. In: Topics in Cryptology (CT-RSA'06), LNCS 3860, pp 115–131
23. Schnorr CP (1990) Efficient identification and signatures for smart cards. In: Advances in cryptology (CRYPTO'89), pp 239–252
24. Batina L, Guajardo J, Kerins T, Mentens N, Tuyls P, Verbauwhede I (2007) Public-key cryptography for RFID-tags. In: Fifth annual IEEE international conference on pervasive computing and communications workshops, 2007. (PerCom Workshops'07), pp 217–222
25. Okamoto T (1993) Provably secure and practical identification schemes and corresponding signature schemes. In: Advances in Cryptology (CRYPTO'92), pp 31–53
26. Lee YK, Batina L, Verbauwhede I (2008) EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol. In: IEEE international conference on RFID, pp 97–104
27. O'Neill M, Robshaw MJ (2010) Low-cost digital signature architecture suitable for radio frequency identification tags. Comput Digital Tech IET 4(1):14–26
28. Godor G, Giczi N, Imre S (2010) Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations. In: IEEE international conference on wireless communications, networking and information security (WCNIS), pp 650–657
29. Farash MS, Bayat M, Attari MA (2011) Vulnerability of two multiple-key agreement protocols. Comput Electr Eng 37(2):199–204
30. Farash MS, Attari MA, Bayat M (2012) A certificateless multiple-key agreement protocol without one-way hash functions based on bilinear pairings. IACSIT Int J Eng Technol 4(3):321–325
31. Farash MS, Attari MA, Atani RE, Jami M (2013) A new efficient authenticated multiple-key exchange protocol from bilinear pairings. Comput Electr Eng 39(2):530–541
32. Farash MS, Attari MA (2013) Provably secure and efficient identity-based key agreement protocol for independent PKGs using ECC. ISC Int J Inf Secur 5(1):1–15
33. Farash MS, Attari MA (2014) A pairing-free ID-based key agreement protocol with different PKGs. Int J Netw Secur 16(2):143–148
34. Farash MS, Attari MA (2014) An enhanced and secure three-party password-based authenticated key exchange protocol without using server's public-keys and symmetric cryptosystems. Inf Technol Control 43(2):143–150
35. Niu B, Zhu X, Chi H, Li H (2014) Privacy and authentication protocol for mobile RFID systems. Wirel Pers Commun. doi:10.1007/s11277-014-1605-6