ECC-Based Untraceable Authentication for Large-Scale Active-Tag RFID Systems

Yalin Chen · Jue-Sam Chou

Abstract Radio frequency identification (RFID) tag authentication protocols are generally classified as non-full-fledged and full-fledged, according to the resource usage of the tags. The non-full-fledged protocols typically suffer de-synchronization, impersonation and tracking attacks, and usually lack scalability. The full-fledged protocols, supporting cryptographic functions, are designed to overcome these weaknesses. This paper examines several elliptic-curve-cryptography (ECC)-based full-fledged protocols. We found that some still have security and privacy issues, and others generate excessive communication costs between the tag and the back-end server. Motivated by these observations, we construct two novel protocols, PI and PII. PI is designed for secure environments and is suitable for applications, including E-Passport and toll payment in vehicular ad-hoc networks. PII is for hostile environments and can be applied in pseudonymous payment and anti-counterfeiting services. After analysis, we conclude that PII can resist many attacks, outperform previous ECC-based proposals in communication efficiency, and provide mutual authentication function and scalability.

Keywords RFID, identification protocol, untraceability, location privacy, scalability, Elliptic Curve Cryptography

1 Introduction

Yalin Chen
Institute of information systems and applications, National Tsing Hua University, Taiwan
e-mail: yalin78900@gmail.com

Jue-Sam Chou (✉)
Department of Information Management, Nanhua University, Taiwan
Tel: 886-5-2721001-56536, Fax: 886-5-2427137
e-mail: jschou@mail.nhu.edu.tw

For some time, commercial products have been identified by attached barcodes. The barcodes, however, must be read one by one through an optical reader with a line-of-sight pathway. Nowadays, radio frequency identification (RFID) tags can be scanned hundreds at a time in a contactless manner, and thus potentially could become a replacement for barcodes. A typical RFID system is composed of tags, readers, and a back-end server. Tags are of two types: passive and active. A passive tag does not carry a battery, has a short communication range, is equipped with extremely simple hardware, and is very low cost. Conversely, an active tag has a battery, has a larger communication range, can accommodate more complex computing components, and costs more. Low-cost tags are adapted for general merchandise identification. High-cost active tags can be used for personal identification or luxury goods.

RFID applications, however, also raise new challenges of security and privacy. For example, data passing through the air could allow the product information disclosure. Tags attached to goods carried by people could expose their location and thus violate their privacy. Privacy can be considered into three concepts: *anonymity* in which the real ID of a tag must be unknown, *untraceability* in which the (in)equality of two tags must be impossible to determine [40], and backward/forward privacy, which indicates, even if the internal state of a tag is exposed, a tag remains *untraceability* for its previous/subsequent activities [45]. Besides these privacy issues, literature [13] has identified other potential threats with RFID systems.

- Replay attack: An attacker intercepts the data transmitted between a tag and a reader and reuses it to spoof the tag.
- De-synchronization attack: An attacker merely intercepts and drops the communication between a tag and a reader, or sends spoofed messages in order to cause the data updated in the tag site and the server site to be out of synchronization. This makes the tag permanently unidentifiable.
- Impersonation attack: An attacker uses a message eavesdropped earlier to impersonate a legitimate tag (or server) to pass a server's (or tag's) authentication.
- Man-in-the-middle attack: An attacker modifies a message transmitted between a tag and a server, creating a false impression that they are communicating with the intended party, when in fact, they are communicating with the attacker.
- Physical attack: An attacker corrupts a tag, extracts the confidential data, and then uses it to launch various attacks on other tags.

Facing the above-mentioned new challenges and threats, researchers have proposed many secure and privacy-preserving RFID authentication protocols [6, 10, 13, 15, 18, 26, 35, 41–43, 58, 61, 65, 66, 69, 73, 77, 78, 83, 84]. According to the computation capability and operations supported on the tags, these protocols can be categorized into four basic classes: (1) full-fledged, (2) simple, (3) lightweight and (4) ultra-lightweight [14]. Class (1) supports cryptographic functions such as hashing, encryption [4, 36, 37, 52, 55, 82], and even a public key algorithm [3, 6, 20–22, 24, 38, 39, 46–48, 51, 53, 56, 57]. Class (2) supports a random number function and a hash function, but not encryption or a public key algorithm

[7, 64, 75, 80, 81, 85]. Class (3) supports a Pseudo Random Number Generator (PRNG) and Cyclic Redundancy Code (CRC), but has no hashing function [12, 27, 33, 34, 44, 49, 60, 68, 71, 74]. Finally, class (4) contains only simple bit-wise operations like XOR, AND, OR and modular addition [11, 14, 17, 59, 72, 76].

The most frequently used standard for the non-full-fledged tags is the electronic product code (EPC) global UHF Class 1 Generation 2, denoted as Gen2. Gen2 adopts CRC and PRNG components only. Although this tag type is low cost [65], it has considerable privacy issues. This is because the Gen2 protocol transmits unprotected tag identity through the air and allows for information leakage and traceability of the carrier's location. While the other non-full-fledged RFID tag authentication proposals do focus on privacy issues, they are sometimes accompanied by other problems such as de-synchronization. In the following document, we use several recent proposals to illustrate the typical challenges associated with these non-full-fledged approaches.

Study [15] presented a Gen2-conforming RFID authentication protocol which tried to address Gen2 privacy problems. However, it suffers impersonation and de-synchronization attacks [26]. Later, a remedy against these defects was proposed in [84]. Nevertheless, this remedy exposes tag locations because the tag's response to the reader's query always contained an unchanged index (C_i). Thus, anyone could use this index to distinguish and trace the tag. Meanwhile, another Gen2-comforming solution, named TRAP-3, was proposed by the authors in [10]. However, a de-synchronization attack was found, and an improvement was presented in [83]. This improvement still suffered the same vulnerability; we will show the details in Section 3.1. Study [58] presented an ultra-lightweight RFID protocol to address de-synchronization problems. Two reports [73, 83], however, showed that the protocol failed in its attempt, and each further offered a refinement. Unfortunately, both refinements kept the tags' pseudonyms unchanged before being successfully identified. This fixed data could still jeopardize location privacy.

Several non-full-fledged schemes in [18, 67, 69] tried to provide scalability. However, the scheme in [18] still requires a server to perform a linear search for the tag identification when the tags suffer successive interrogation attacks. The cost of a linear search can be denoted as O(N), where N is the number of the tags in an RFID system. Study [67] introduces a great many of readers (each reader shares a key with a set of tags, and therefore, the tags are divided into different searching groups) to reduce the searching cost to O(N/α), where α is the number of readers. We think the scalability of study [67] is still unsatisfactory since deploying too many readers in a site seems impractical. In addition, it suffers tracking problems because the dynamic tag identity (ID_i) remains the same when the last pass of the previous session is intercepted. This also causes a de-synchronization problem since the server has updated the tag identity, but the tag has not. We will show this in Section 3.1. Thus far, the most efficient non-full-fledged proposal to ensure scalability is the scheme in [12], which reduces the server's searching cost to O($N^{1/2}\log N$). This may still be insufficient when applied in a large-scale environment such as E-Passport or specific industry products, because the database would have to be sorted before the protocol execution.

Motivated by these unsatisfactory non-full-fledged RFID authentication proposals, we consider that a full-fledged approach using a public key cryptosystem could be an attractive solution [6, 35, 78]. Of the available public key cryptosystems, elliptic curve cryptography (ECC) offers the same security level as the others, using shorter keys. This makes ECC a suitable component to embed in resource-limited tags [77]. Many low-cost implementations of ECC primitives have been proposed [3, 6, 20–22, 24, 38, 39, 46–48, 51, 53, 56, 57]. We have reviewed several recent ECC RFID authentication protocols and found that all need at least three passes when active tags are applied. This paper, therefore, constructs two novel two-pass ECC RFID authentication protocols, PI and PII. PI is for secure environments and PII for hostile environments. Both can be applied for large-scale object identification. The potential applications of our proposals are E-Passport [1, 2, 30, 31, 79], public transportation tickets, pseudonymous credit cards [9, 63], payment or targeted re-calls in vehicular ad-hoc networks (VANETs) [28, 29], and anti-counterfeiting for luxury goods [19].

The remainder of this paper is organized as follows. Section 2 introduces the background of the protocols. Section 3 reviews some recent RFID protocols, both non-full-fledged and full-fledged. Section 4 presents our protocols and their security analyses. The discussions are demonstrated in Section 5. Finally, we present our conclusion in Section 6.

2 Preliminaries

This section introduces the elliptic curve cryptography in Section 2.1. Then, a privacy model used to examine the robustness of the traceability for an RFID scheme is described in Section 2.2.

2.1 Elliptic Curve Cryptography (ECC)

We show the concept of ECC [50, 70] below. Suppose a and b are two integers that define the curve of the equation $y^2 = x^3 + ax + b$. Points (x, y) satisfying the elliptic curve equation along with an infinite point O and an addition operation form a cyclic additive group G. The operations of group G are defined below.

- $P = (x, y)$ is a Group element, then define $-P = (x, -y)$ and $P + (-P) = O$.
- If P and Q are two distinct elements and $P \neq -Q$, define $P + Q$ as follows: Draw a line through P and Q, then the line will intersect with the curve, the intersected point is denoted as $-R$, and define $P + Q = R$.
- If a group element $P = (x, 0)$, then $P + P = O$. Otherwise, draw a tangent line through P, the intersected point is defined as $-R$, afterwards $P + P = 2P = R$.

In addition, for the group G, there exists a base point P, also called generator or primitive root, and it can generate the group G. That is $G = \{P, 2P, 3P, \ldots. (n-1)P, nP = O\}$, where n is the order (size) of G. The security of ECC builds on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). That is, when the order of G is sufficiently large, given a random group element Q, outputting an

integer α such that $Q = \alpha P$ is computationally infeasible. In practice, the security level of ECC with the key size (i.e. the order of group G) of 160 bits is approximately equal to the security level of RSA cryptosystem with key size of 1024 bits.

2.2 RFID privacy model

For an RFID authentication protocol, Untraceable Privacy and Backward/Forward Privacy are desirable properties. Untraceable Privacy, i.e. *untraceability*, indicates that given any two *uncorrupted* tags and their communication transcripts, it is impossible to determine which transcript belongs to which tag. Backward Privacy means even given all the internal states of a target tag at time t, an attacker cannot identify the target tag's transcripts that occur at time t', $t' < t$ [45]. Likewise, Forward Privacy is defined in the same manner, except for that t' should be greater than t. In the following, we refer [25, 32, 54] to define these privacy notions formally. We first model the capability of an adversary A through the following queries, where R indicates a reader and T a tag.

- **Execute** (R, T, i) query: A eavesdrops on the protocol running between the two communicating parties, R and T, in session i of the protocol execution. This query models a passive attack.
- **Send** (R, T, m, i) query: A impersonates some reader R (or tag T) in session i of the protocol by sending message m to a tag T (or a reader R). This query will be sent to the victim T (or R), and models an active attack.
- **Corrupt**(T) query: A physically accesses tag T's memory to obtain all its stored keys and memory data. This query also models an active attack.
- **Test**(T_0, T_1) query: This query generates a random bit $b \in \{0, 1\}$ and returns T_b to adversary A. A wins if he guesses b correctly.

Then we have the following definitions.

Definition 1: (**Untraceable Privacy**) An adversary A and a challenger C are involved in the following game.

> ***Learning phase***: A issues above Execute, Send, Corrupt queries to any readers and tags in a given RFID system.
>
> ***Challenge phase***: A chooses two uncorrupted tags, T_0 and T_1, and sends **Test**(T_0, T_1) query to C. C flips a coin to select bit $b \in \{0, 1\}$ and gives T_b to A. A then makes any **Execute** and **Send** queries to T_b. Finally, A outputs b'.

The probability of A wins the game is denoted by $Adv_A^{Upriv}(k) = |\ \mathrm{pr}(b' = b) - \mathrm{pr}(\text{random flip coin}) = |\ \mathrm{pr}(b' = b) - 1/2\ |$, where k is the security parameter (usually the key size). We say the given RFID authentication scheme possesses the property of Untraceable Privacy if $Adv_A^{Upriv}(k)$ is negligible.

Definition 2: (**Backward Privacy**) An adversary A and a challenger C are involved in the following

game.

Learning phase: A issues above Execute, Send, Corrupt queries to any readers and tags in a given RFID system.

Challenge phase: A chooses two uncorrupted tags, T_0 and T_1, and sends **Test**(T_0, T_1) query to C. C flips a coin to select bit $b \in \{0, 1\}$ and gives T_b to A. A then makes Corrupt(T_b) query to obtain all keys and data in T_b's memory. Finally, A outputs b'.

The probability of A wins the game is denoted by $Adv_A^{Bpriv}(k) = |\ \mathrm{pr}(b' = b) - \mathrm{pr}(\text{random flip coin}) = |\ \mathrm{pr}(b' = b) - 1/2\ |$, where k is the security parameter (usually the key size). We say the given RFID authentication scheme possesses the property of Backward Privacy if $Adv_A^{Bpriv}(k)$ is negligible.

Definition 3: (**Forward Privacy**) The definition is the same as the Forward Privacy except that, after A making Corrupt (T_b) query in the challenge phase, A_is allowed to make Execute and Send query to both tags T_0 and T_1. Similarly, we say the given RFID authentication scheme possesses the property of Forward Privacy if $Adv_A^{Fpriv}(k)$ is negligible.

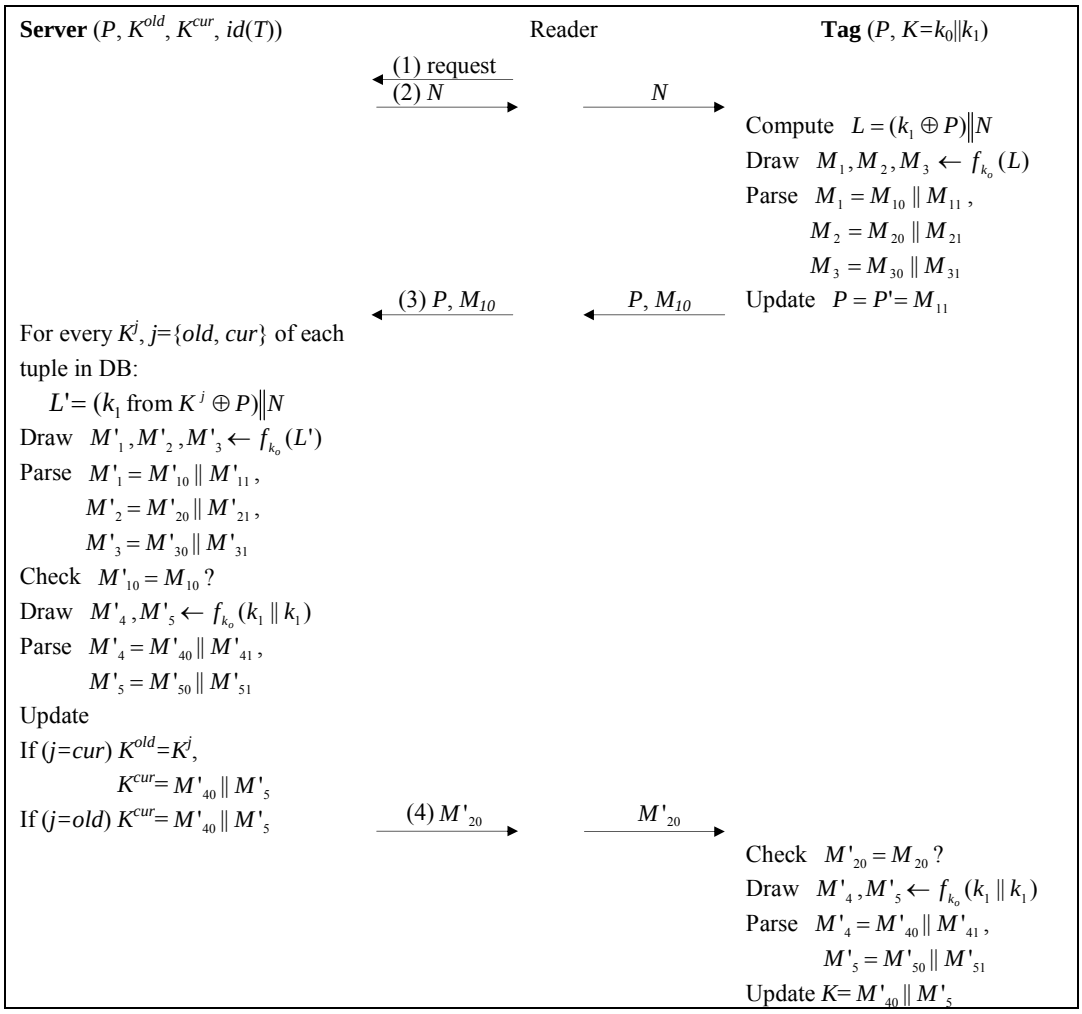

Fig. 1 A TRAP-3 improvement [83]

3 Review of RFID authentication protocols

In this section, we review two non-full-fledged and several recently proposed full-fledged RFID authentication protocols in Section 3.1 and 3.2, respectively.

3.1 Non-full-fledged RFID authentication protocols

As mentioned in the Introduction, study [83] shows an improvement of TRAP-3, but it still has a de-synchronization problem. Fig. 1 illustrates the improved protocol. To demonstrate the de-synchronization attack on this improvement, we assume that there exists an attacker X interacting with two legal readers R_A and R_B, as shown in Fig. 1(a) through Fig. 1(c). At time T_0, a server and tag pair communicated via R_A in session A. Supposes X intercepts M'_{20A} and suspends the session. X then waits until time T_1, and when the same pair communicates via another legal reader R_B in session B, X intercepts M'_{20B} and abandons session B.

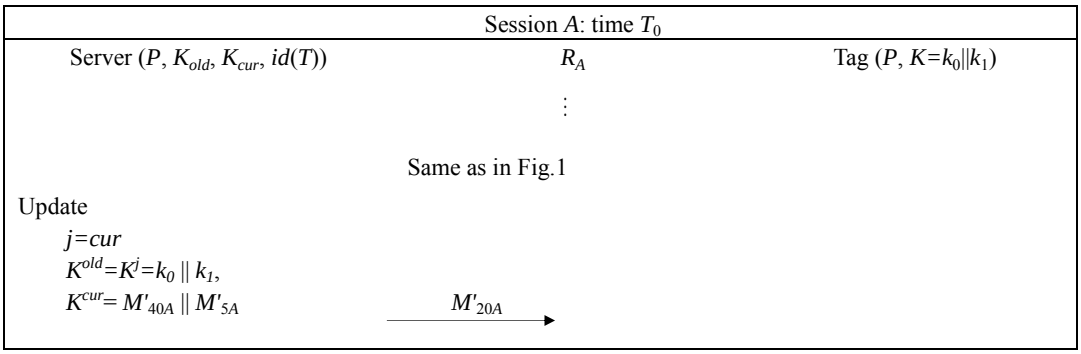

Fig. 1(a) A intercepts M'_{20A} and suspends this session

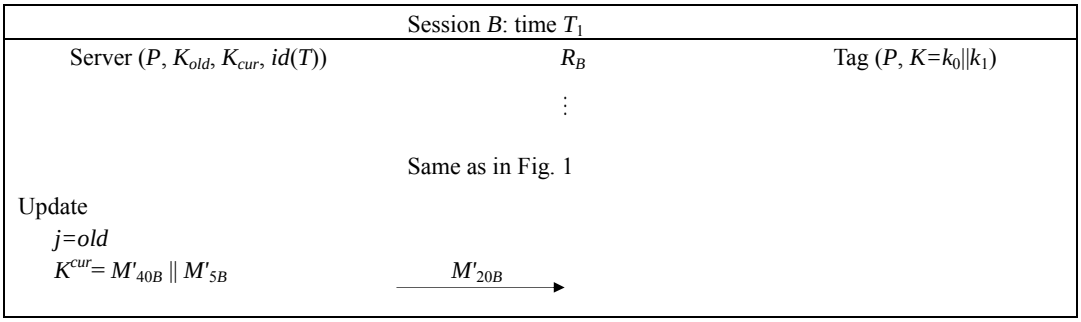

Fig. 1(b) A intercepts M'_{20B} and abandons this session

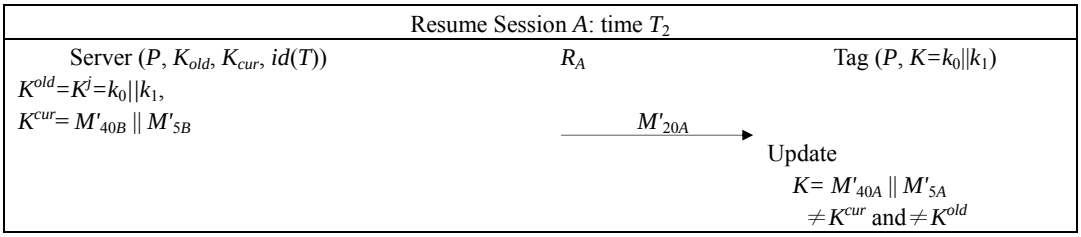

Fig. 1(c) A sends M'_{20A} to the tag

Subsequently, X resumes session A at time T_2 and sends M'_{20A} to the tag. As a result, the keys

stored in both the server ($K^{old} = K^{j} = k_0 \| k_1$, $K^{cur} = M'_{40B} \| M'_{5B}$) and the tag ($K = M'_{40B} \| M'_{5A}$) are different. Thus, we demonstrate that Yeh *et al.*'s improved version of TRAP-3 is still vulnerable to the de-synchronization attack.

Study [69] was designed to resist a de-synchronization attack, but we found it cannot attain the goal still. We depict their protocol in Fig. 2 and demonstrate the attack as follows.

In cases 2 and 3 (confidential update) of their protocol, as shown in Fig. 2, server S sends (r, M_s) to tag T, where r is a random number generated by S and M_s $(= g_k(r \| M_T) \oplus (s \| k' \| m'))$ is a $(2l + |m'|)$-bit string. Upon receiving (r, M_s), T computes $(s \| k' \| m') = M_S \oplus g_k(r \| M_T)$ and checks, whether $h(s) = k$ holds. If it holds, T updates its key k to k' and its counter c to m'. However, if the adversary modifies the second l bits of string M_s to obtain M'_s and sends it to T. When T uses M'_s to compute $(s \| k' \| m')$, its second l bits would be different from the value k' owned by S. Hence, T will have a distinct key from k'. This is why we say that Song *et al.*'s protocol could not resist the de-synchronization attack.

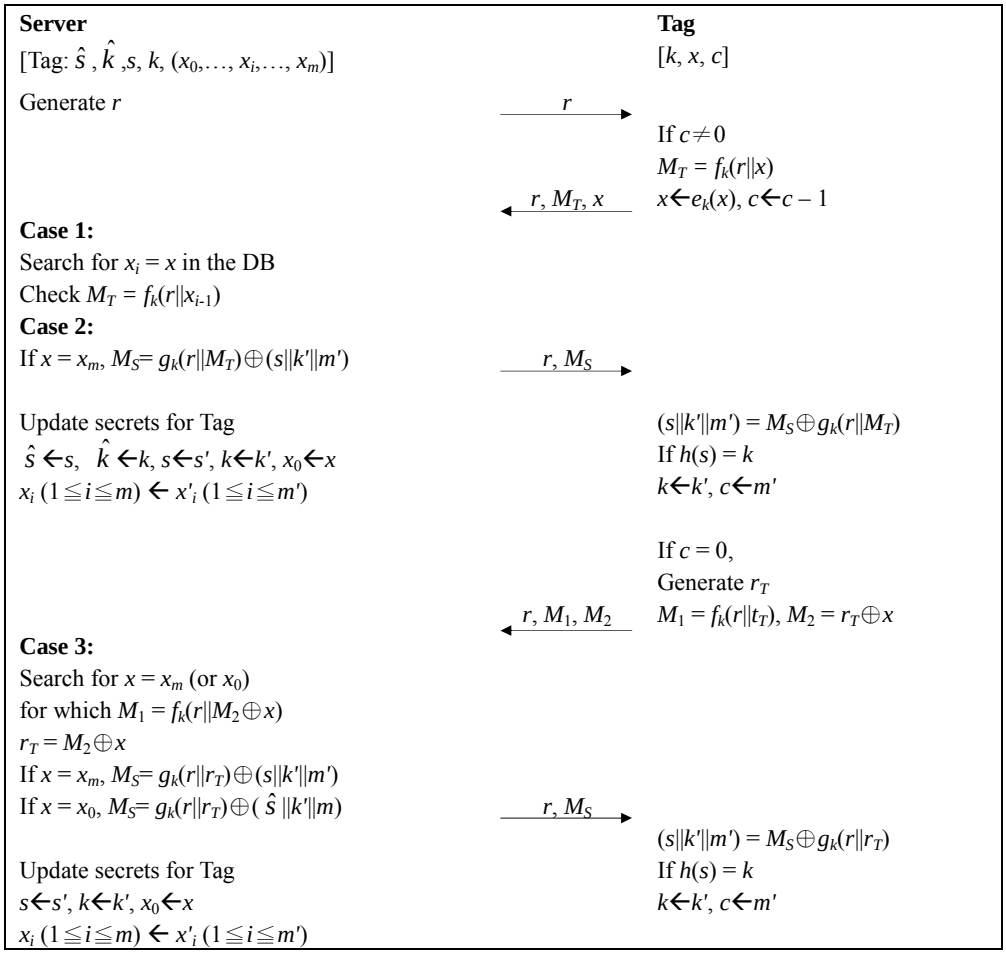

Fig. 2 An RFID authentication and secret update protocol [69]

3.2 Full-fledged RFID authentication protocols

This section reviews several recent ECC RFID authentication protocols. An RFID protocol was

proposed in [77], which uses ECC Schnorr identification technique to resist passive attacks and counterfeiting. We depict the protocol in Fig. 3.

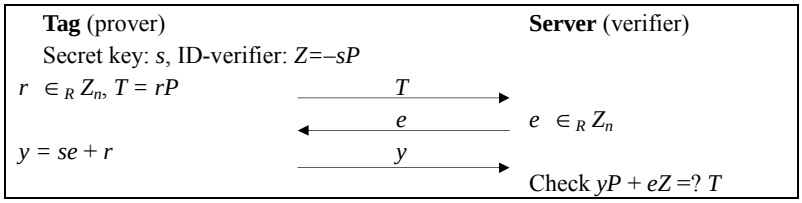

Fig. 3 An ECC-Schnorr-identification-based RFID protocol [77]

However, this protocol has a tracking problem [42]. When an adversary eavesdrops tag and server's communications and obtains a transcript, $\{T, e, y\}$, he can use e^{-1} to obtain the tag ID-verifier, Z ($= -sP$) by computing $e^{-1}(T - yP)$. Then, the adversary can track the tag with Z. We show another way to track a specific tag. An adversary A first eavesdrops a transcript $\{T_1 = r_1P, e, y_1 = se+r_1\}$. A then pretends a legitimate reader to interrogate a target tag. After receiving T_2 ($= r_2P$) from a tag, A sends a challenge e' ($= e$) back to the tag, and obtains y_2 ($= ae+r_2$). A then can recognize the specific tag by checking whether $(y_2 - y_1)P$ is equal to $T_2 - T_1$.

In addition to the tracking problem, this protocol is vulnerable to man-in-the-middle attacks because the data of a communication transcript are linearly related to the tag ID-verifier (refer to the note in Fig. 4). In the Fig. 4, an adversary E stands between a tag and a server to communicate with each by tampering original transmitted messages. The server and the tag eventually complete the identification process but do not know at all that they connect with E indeed.

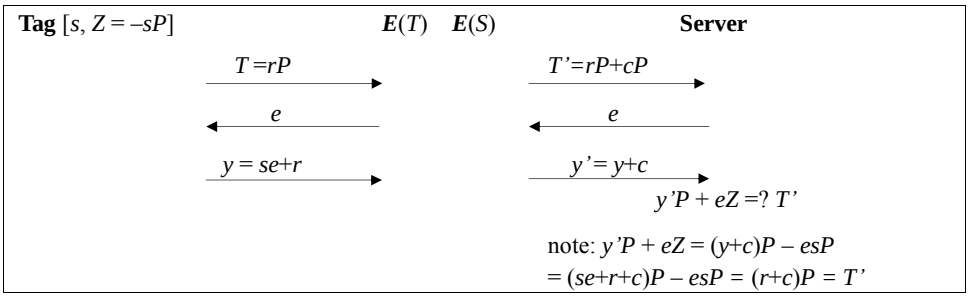

Fig. 4 A man-in-the-middle attack to the protocol [77]

Regarding the scalability, we let the server compute $Z^* = e^{-1}(T - yP)$ and then directly look up a tag in server's DB with Z^*. Tuyls *et al.*'s protocol, therefore, provides scalability.

An improvement of [77] uses ECC Okamoto's identification technique to resist active attacks was proposed in [6]. However, the protocol in [6] like the one in [77] also has a tracking problem and a man-in-the-middle vulnerability.

Study [42] presented an Elliptic Curve Based Randomized Access Control (EC-RAC) protocol to address the tracking problem. Unfortunately, EC-RAC protocol later was found not to resist tracking and replay attacks by the authors in [43]. Therefore, a revised version EC-RAC II was proposed. However, this revised version exposes to the risk of man-in-the-middle threats [41]. Accordingly, study

[41] presented EC-RAC IV to overcome both tracking and man-in-the-middle vulnerabilities through eliminating the possibility of linear operations on the communication transcripts. Fig. 5 illustrates the scheme EC-RAC IV, where $x(eP)$ indicates the x-coordinate of the elliptic curve point eP. Another variant of EC-RAC IV [40] is shown in Fig. 6 allows an additional password transfer. These two schemes eventually achieved their security and privacy goals.

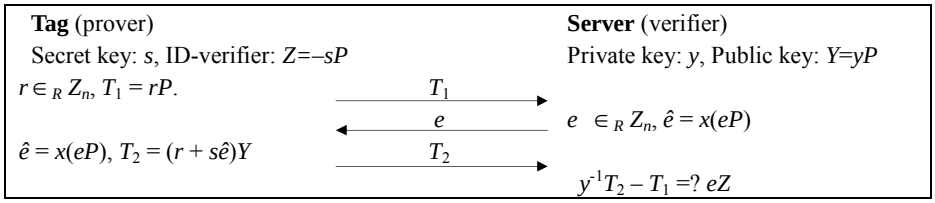

Fig. 5 EC-RAC IV RFID identification protocol

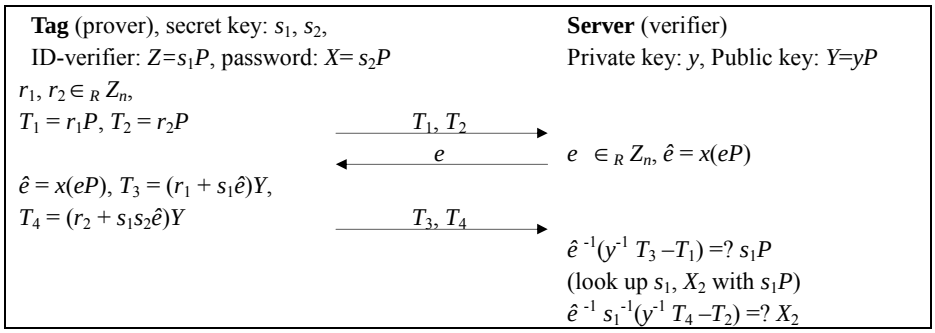

Fig. 6 EC-RAC IV variant with password transfer

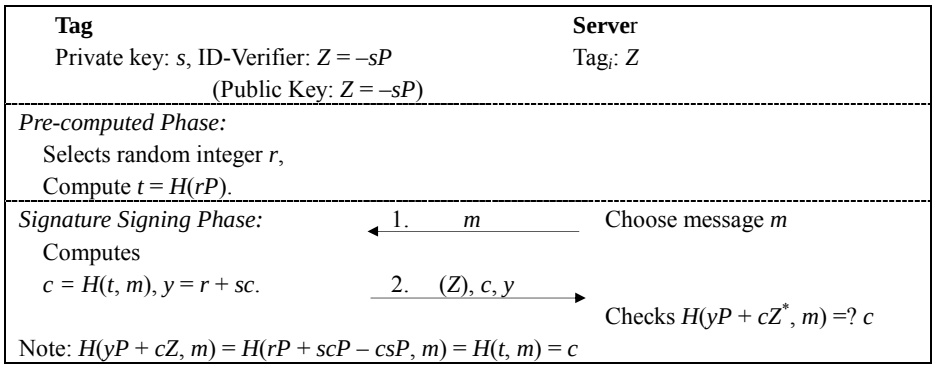

Fig. 7 An RFID signature scheme [53]

Study [53] employed CryptoGPS primitives [23, 62] to design an ECC digital signature scheme for low-cost RFID tags, as shown in Fig. 7. The study also presented a low-cost hardware implementation. Its goal is to prevent tag cloning, and for data authentication to prevent transmission forgery. As a digital signature scheme, the scheme in this study causes tag traceability in essence, because the tag should claim who it is, i.e. presents its public key Z to a server in the second transmitted message (see Fig. 7). Alternatively, the scheme could be treated as a privacy-preserving scheme which turns the tag's public key Z into a secret ID-Verifier shared with the server only. Under this case, it can resist possible deduction of an ID-Verifier from a communication transcript due to the one-way property of the hash function. However, the tag still can be tracked by an attacker who replays an earlier eavesdropped message m to a tag and observes whether the tag response is the same as the earlier eavesdropped

response $\{c, y\}$. Another problem is a brute searching for server identifying a tag with the ID-Verifier Z. Thirdly, the Forward and Backward Privacy cannot be preserved when the stored data (i.e., s, Z, and $t = H(rP)$) in a tag are exposed to an adversary.

The above-mentioned so far are protocols in which a tag initiates the first message and therefore, cannot be applied for passive RFID tags without battery embedded. All of them could serve for passive tags if the additional hello message is first initiated from a server to a tag and makes the tag charged. Nevertheless, this result in a three-pass protocol into a four-pass protocol and generate excessive communication costs. In contrast, the scheme [16] can be applied for both active and passive tags without any adjustment, as shown in Fig. 8. Moreover, it provides mutual authentication and scalability, and resists many threats, including tracking and man-in-the-middle attacks.

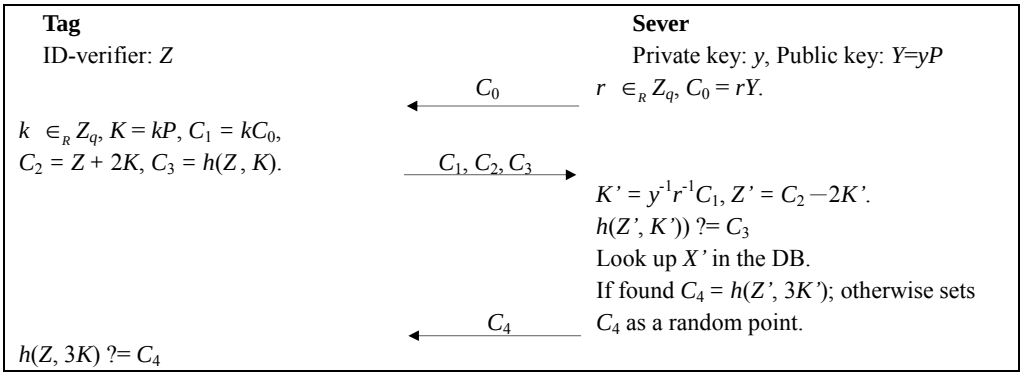

Fig. 8 An RFID mutual authentication protocol [16]

4. Proposed protocols

Our goal of this research aims to propose a two-pass ECC-based RFID authentication protocol while considering privacy protection, scalability and various attack prevention. We propose two such kinds of protocols, PI and PII. PI is for secure environments and PII for hostile ones. As usual, we assume that the server and the readers communicate via secure channels. Therefore, we use "server" to represent "server/reader" for short. Each of our protocols consists of two phases, namely, an initialization phase and an authentication phase. Before describing PI and PII, we first define the used notations.

G: an additive group of order q on an elliptic curve,

P: a primitive element of G,

ID_i: tag_i's identity,

s: server's private key,

Y: server's public key,

H: a one-way hash function mapping from $\{0, 1\}^*$ to $\{0, 1\}^{q'}$,

H_1: a one-way hash function mapping from G to $\{0, 1\}^{q'}$,

H_2: a one-way hash function mapping from $Z_q \times G$ to $\{0, 1\}^{q'}$,

q': the hash output length, and

k, r: two random numbers in Z_q.

4.1 Protocol PI for secure environments

A secure environment assumes that the reader is trusted and there is no attacker exists around the reader and the tag, for example, an E-Passport gateway in the airport. That is, a reader in the gateway checks each E-Passport passing, which is always guarded against by the police. In practice, a secure environment may be fulfilled by setting a detector to monitor possible intruders periodically. Thus, the proposed PI scheme does not need to consider the eavesdropping or other threats around the reader and the tag, but only focus on the security of a distant back-end server. For example, the tag communication transcripts logged on server's DB could leak due to server insider attacks or outsider intrusions. The following is the proposed PI scheme.

4.1.1 Initialization Phase

In this phase, server S generates an elliptic-curve group G with a base point P and order q, and the ECDLP on G is computationally infeasible. S also generates a random number s as its private key and computes $Y = sP$ as its public key. In addition, S defines two secure hash functions: H: $\{0, 1\}^* \rightarrow \{0,1\}^q$. Then, S starts to initialize all tags in the system. It produces a database containing two fields, ID_i and $H(ID_i)P$, and sorts it by $H(ID_i)P$ for each tag. Finally, S distributes ID_i, $H(ID_i)P$ and Y to each Tag_i, over a secure channel, where i = 1 to N and N is the number of tags in the system.

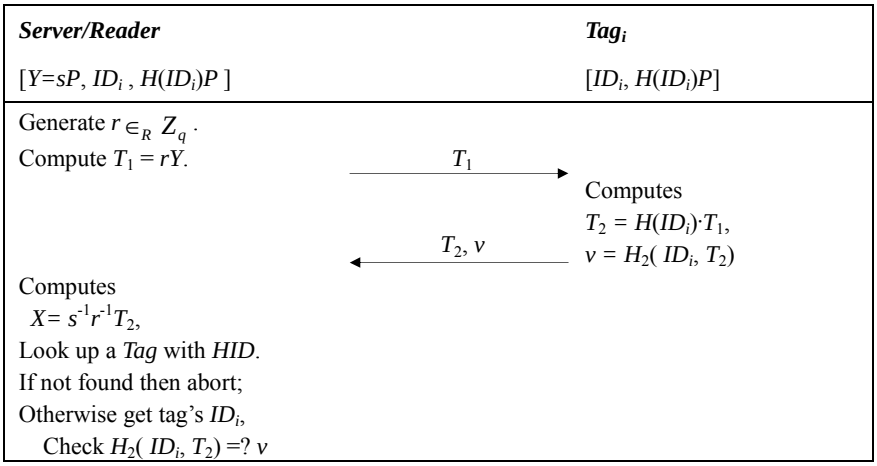

Fig. 9 Proposed RFID authentication protocol PI

4.1.2 Authentication Phase

In this phase, server S and Tag_i perform the following steps, also depicted in Fig. 9.

Step1: S chooses a random number r, computes $T_1 = rY$, and broadcasts T_1.

Step2: Upon receiving T_1, Tag_i computes $T_2 = H(ID_i)\cdot T_1$ and $v = H_2(ID_i, T_2)$, and sends the message $\{T_2, v\}$ back to the server.

Step3: Upon receiving $\{T_2, v\}$, S applies its private key s and the one-time secret r to compute $X = s^{-1}r^{-1}\cdot T_2$, which is supposed to be $s^{-1}r^{-1}\cdot H(ID_i)\cdot T_1 = s^{-1}r^{-1}\cdot H(ID_i)\cdot rY = H(ID_i)P$. Then it looks up a tag record with X. If the corresponding tag not found, S aborts the message and terminates. Otherwise, S gets the tag's ID from the found record and verifies whether $H_2(ID_i, T_2)$ is equal to

the received v. If the verification passes, S accepts Tag_i.

4.1.3 Security and Privacy Analysis

Since the PI protocol is performed in a secure environment, only an authorized reader is allowed to interrogate a tag. In other words, the interrogation message T_1 must be a randomly generated message from the legal reader. In addition, T_1 is not impossibly replayed in a secure environment. Therefore, the communication transcript $\{T_1, T_2, v\}$ is always different and looks random. From the theoretical viewpoint, the probability of the occurrence of two identical interrogation messages is $1/q$. This is negligible since q must be sufficiently large to make ECDLP infeasible. Due to the randomness of communication transcripts, the anonymity and untraceability privacy can be preserved even when the server's DB is intruded by hackers.

Regarding the scalability, the proposed PI allows the server to directly look up a possible tag record by using the computed X which is supposed equal to Tag_i's identifier $H(ID_i)P$ (also see the Step 3 above). We emphasize that the identifier $H(ID_i)P$ can be correctly computed simply when Tag_i's response $\{T_2, v\}$ is not tampered by any attackers, i.e. only a secure environment can achieve this circumstance. Therefore, the server searching cost O(1) can be ensured.

Other threats like eavesdropping, impersonation, man-in-the-middle and replay can be easily avoided due to the guarantee of the secure environments.

4.2 Protocol PII

PII is designed for any environments, secure or hostile. In this case, a tag cloud be interrogated by a malicious reader; a man in the middle or an eavesdropper cloud around a tag or a reader. Therefore, all kinds of possible threats should be taken into account. The following is the details of the proposed PII.

4.2.1 Initialization phase

In this phase, server S first generates system parameters like PI does. Thus we have G, q, P, s and $Y=sP$. In addition, S defines three secure hash functions, H: $\{0, 1\}^* \rightarrow \{0, 1\}^{q'}$, H_1: $G \rightarrow \{0, 1\}^{q'}$, and H_2: $\{0, 1\}^q \times G \rightarrow \{0, 1\}^{q'}$. Secondly, S starts to initialize all tags in the system. S generates a random number ID_i, computes $H(ID_i)$ for each tag, and produces a database containing two fields, ID_i and $H(ID_i)$, and sorts it by $H(ID_i)$. Finally, S distributes $H(ID_i)$, ID_i and server's public key Y to each Tag_i over a secure channel. Each tag then stores them into its memory.

4.2.2 Authentication phase

In this phase, when authenticating Tag_i, S carries out the following steps, also depicted in Fig. 10.

Step 1: S generates a random number r, computes $C_1 = rP$ and $C_2 = rY$, and uses its private key to produce a signature $sn = r + s \cdot H_1(C_2)$. Then it broadcasts C_1, C_2 and sn.

Step 2: Upon receiving the broadcast message, Tag_i uses the server's public key to verify the received signature, i.e. $sn \cdot P =? C_1 + H_1(C_2) \cdot Y$. If the equation does not hold, Tag_i aborts the message and

stops. Otherwise, Tag_i accepts the server's interrogation message and then prepares authentication data. Tag_i computes $C_3 = kC_2$, $c = H(ID_i) + H_1(kC_1)$ and $d = H_2(ID_i, kC_1)$, and answers C_3, c and d to the server.

Step 3: Upon receiving Tag_i's response, S computes $H(ID)^* = c - H_1(s^{-1}C_3)$, which is supposed that $H(ID_i)^* = c - H_1(s^{-1}T_3) = H_1(ID_i) + H_1(kC_1) - H_1(s^{-1}kC_2) = H_1(ID_i)$. S then uses $H(ID_i)^*$ to look up a tag in the DB. If it does not find the corresponding tag, S aborts the response and terminates. Otherwise, S gets the tag's identity ID^* from the found record, and verifies whether $H_2(ID_i, s^{-1}C_3)$ is equal to the received d (=$H_2(ID_i, kC_1)$), where $s^{-1}C_3 = s^{-1}kC_2 = s^{-1}krY = krP = kC_1$. If the verification passes, S identifies Tag_i.

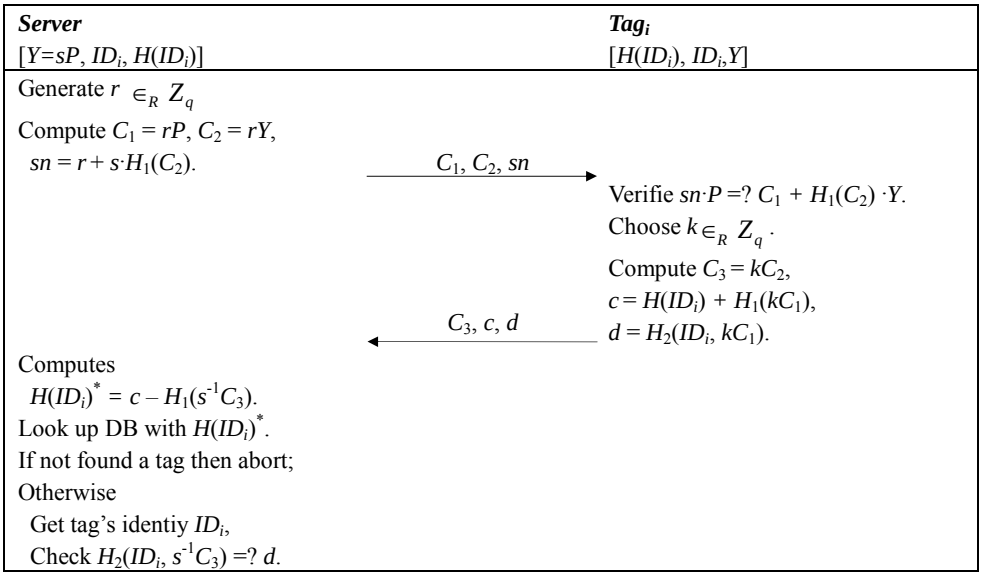

Fig. 10 Proposed RFID authentication protocol PII

4.2.3 Security and Privacy Analysis

In the following, we first discuss some attacks, (1) through (3), on our protocol PII, which often occur in RFID systems. Then, we show that our protocol has scalability and mutual authentication at items (4) and (5). Finally, we apply the formal privacy model to analyze the Untraceable Privacy and Backward/Forward Privacy of the proposed PII.

(1) Replay attack

When an attacker replays an old message flow, says $\{C_1^{(old)}, C_2^{(old)}, sn^{(old)}\}$, to a *Tag*. Although the *Tag* cannot recognize the message as a replayed one, it answers a random response, says $\{C_3^{(new)}, c^{(new)}, d^{(new)}\}$, based on *Tag*'s randomly chosen integer k. In other words, the random response $\{C_3^{(new)}, c^{(new)}, d^{(new)}\}$ cannot be distinguished from any other response e.g., $\{C_3^*, c^*, d^*\}$ due to the randomness of $k^{(new)}$ and $k^{(*)}$. As a result, the attacker gains no advantage of the response, i.e. it cannot be used for identifying or tracking any tags. On the other hand, if an old flow $\{C_3^{(old)}, c^{(old)}, d^{(old)}\}$ is replayed as a response to a new interrogation $\{C_1^{(new)}, C_2^{(new)}, sn^{(new)}\}$, the server will reject $\{C_3^{(old)}, c^{(old)}, d^{(old)}\}$. This is because the server cannot obtain the corresponding tag's ID due to the different $k^{(new)}$ and $k^{(old)}$, i.e.

the probability of $s^{-1}T_3^{(old)} = k^{(new)}T_1^{(new)}$ is sufficiently small to be negligible. Therefore, replaying an aged response $\{C_3^{(old)}, c^{(old)}, d^{(old)}\}$ cannot cause any effect.

(2) Man-in-the middle attack

Assume that an adversary A launches a man-in-the-middle attack (MIMA) between a server and a tag. He pretends to be the real server to the tag and vice versa. We now detail this attack prevention of our scheme as follows and also illustrate it in Fig. 11.

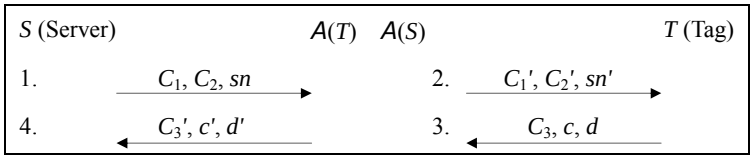

Fig. 11 Man-in-the-middle attack on PII

Step 1: The server chooses a random number r, prepares $\{C_1 = rP, C_2 = rY, sn = r + s \cdot H_2(T_2)\}$ and sends them to the tag.

Step 2: A intercepts the message and chooses a random number r' to compute $C_1' = rP + r'P$ and $C_2' = rY + r'Y$. The value of sn' should be equal to $(r + r') + s \cdot H_2(C_2')$. However, without the knowledge of s, A cannot generate valid sn' to be successfully verified by the tag.

Step 3: Assume that A succeeded in step 2, i.e. valid $sn' = (r + r') + s \cdot H_2(T_2')$ were produced. The tag will accept $\{C_1', C_2', sn'\}$ and then prepare an autnetication message. It chooses a random k, computes $C_3 = kC_2'$, $c = H(ID) + H(kC_1')$ and $d = H_2(ID, kT_1')$, and sends $\{C_3, c, d\}$ to the server.

Step 4: A intercepts $\{C_3, c, d\}$ and tries to produce valid $\{C_3', c', d'\}$. A can randomly select an integer k' and computes $C_3' = k'C_2$. Then, to produce a valid c', A should know tag's $H(ID)$ from the intercepted c $(= H(ID) + H(kC_1'))$. However, without the knowledge of k (a one-time secret generated by the tag), it is hard to extract $H(ID)$ and produce valid c'.

From the above analysis, we can see such an MIMA attack cannot work.

(3) Physical attack

Supposing that an adversary A uses physical means to obtain Tag_i's secrets ID_i and $H(ID_i)$, the proposed PII scheme can still keep the Backward and Forward Privacy, i.e., the previous and subsequent communication scripts of the Tag_i cannot be recognized. This is because any transcript $\{C_1, C_2, sn, C_3, c, b\}$ of PII is uniformly random due to the random integers r and k. Any transcript of PII therefore, cannot be computationally linked to the specific ID_i. A formal analysis of Backward and Forward Privacy of PII will be presented in (7).

(4) Scalability

It is obviously that server takes O(1) to search for a tag by using the computed $H(ID_i)^*$. Therefore, the proposed PII provides scalability.

(5) Mutual authentication

In our scheme, a server computes $\{C_1 = rP, C_2 = rY, sn = r + sH_1(C_2)\}$, where sn is server's signature related both C_1 and C_2, and sends them to a tag. Then, the tag verifies the signature Sn by applying server's public key Y. On the other hand, the tag which has identity ID_i computes $C_3 = kC_2$, $c = H(ID_i)+ H_1(kC_1)$ and $d = H_2(ID_i, kC_1)$ to be checked by the server. We know that only legal Tag_i has valid ID_i embedded to let the server find it in its DB. Thus, our protocol can achieve mutual authentication.

(6) Anonymity

From the transmitted data of the proposed PII, $\{C_1 = rP, C_2 = rY, sn = r + sH_1(C_2), C_3 = kC_2, c = H(ID_i)+ H_1(kC_1), d = H_2(ID_i, kC_1)\}$, only c and b contain tag's ID. However, the tag ID be shuffled through one-way hash functions. One-way property indicates obtaining a pre-image (e.g., ID_i) from a hash result (e.g., $H(ID_i)$) is very hard. Thus, our scheme has anonymity.

(7) Untraceable Privacy and Backward/Forward Privacy

We use the formal notions described in Section 2.2 to show that the proposed PII possesses Untraceable Privacy and Backward Privacy and Forward Privacy.

Lemma 1: ***According to Definition 1, we claim our RFID identification protocol PII possesses Untraceable Privacy.***

Proof: We prove this lemma using the following reduction. In the adversary game, if A could differentiate two uncorrupted tags $\{T_b, T_{1-b}\}$, where b = 0 or 1, from a tag response $\{C_3, c, d\}$ to a query $\{C_1, C_2, sn\}$. This implies that A knew $H(ID_b)$, without the knowledge of server's secret s and could derive rkP, when giving $C_3 = krsP$, $c = H(ID_b) + H_1(rkP)$ and $d = H_2(ID_b, krP)$. However, this is computationally infeasible. If this happened, we could use A to construct an algorithm B to extract rkP from C_3, and then use algorithm B to solve the ECDLP. This is a contradiction. The design of algorithm B is shown in Fig. 12. We prove this lemma.

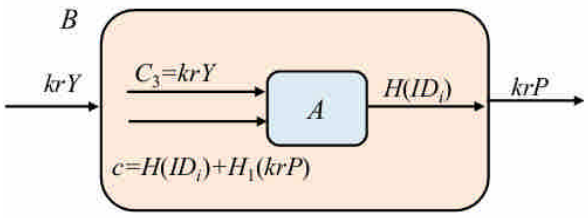

Fig. 12 B's construction of solving ECDLP

Lemma 2: According to Definition 2, we claim our RFID identification protocol PII possesses Backward Privacy.

Proof: We prove this lemma using the following reduction. In the adversary game, A is given the corrupted T_b's secret $\{ID_b, H(ID_b)\}$, where b = 0 or 1, and two historic communication transcripts $\{C_1^{(0)}, C_2^{(0)}, sn^{(0)}, C_3^{(0)}, c^{(0)}, d^{(0)}\}$ and $\{C_1^{(1)}, C_2^{(1)}, sn^{(1)}, C_3^{(1)}, c^{(1)}, d^{(1)}\}$. If A could

determine which transcript belongs to T_b, this implies A must be able to deduce $krP^{(b)}$ from $H_1(krP^{(b)})$ to confirm $d^{(b)}$ for assuring the right tag. However, again this is impossible. Since, if it were true, the one-way property of hash function H_1 is violated. We thus prove this lemma.

Lemma 3: According to Definition 3, we claim our RFID identification protocol PII possesses Forward Privacy.

Proof: As this property is similar to Forward Privacy and the proof of this lemma can refer to Lemma 2.

5. Discussions

In this section, we compare our work PII with recent ECC RFID authentication schemes, including ECRAC IV, ECRAC IV variant, the scheme (with secret ID-verifier) in [53], and the scheme in [16], all of which are reviewed in Section 3.2.

As we know, ECC-based RFID protocols belong to the full-fledged class and are believed to attain *scalability* and avoid *de-synchronization* more easily than the non-full-fledged protocols. Our scheme, EC-RAC IV, EC-RAC IV variant and the scheme in [16] do achieve these two aims, but the scheme in [53] does not have scalability if it makes the tag ID-verifier secret for the *anonymity* (see Section 3.2). A recent ECC RFID protocol [24] has de-synchronization issue because it adopts a dynamic ID as the non-full-fledged protocols did, which need a server and a tag synchronously update the dynamic ID. Therefore, we can see that inadvertent designed ECC proposals could cause scalability and de-synchronization problems.

Mutual authentication is another important feature that many RFID schemes aimed at. This feature allows a tag and a server to confirm that the received messages are sent by the intended party. It thus can avoid malicious probing or wrong data updating. The schemes, EC-RAC IV, EC-RAC IV variant and [53], provide only tag-to-server authentication but not server-to-tag authentication. Our scheme provides server-to-tag authentication by letting a server sign the transmitted data, and also provides tag-to-server authentication through a hash result generated with the tag identifier (see Section 4.3 for details). The scheme in [16] uses two hash results for tag-to-server and server-to-tag authentications respectively. Both our scheme and scheme [16] require a hash function calculator embedded on tags. This increase the hardware cost of a tag, although the computation cost of an ECC point multiplication (e.g., $rP = P + P \ldots + P$, which is $r - 1$ times of point additions) is about 500 times a hash value generating [24]. In other words, the increase of hash computations is trivial but the increase of hash hardware for an RFID tag should be carefully considered. For a high-cost tag, additional hash hardware may be not a burden. We will discuss more tag hardware cost in a later paragraph.

Regarding the MIMA, earlier ECC solutions based on Schnorr identification schemes [6, 42, 43, 77] suffer this attack, but EC-RAC IV terminates this weakness. The scheme in [53] also based on Schnorr identification, but it takes advantage of the one-way property of a hash function to prevent the MIMA. Our scheme and scheme [16] both employ the signature technique and the one-way hash results for

authenticating entities. Such strategies seem work for prevention the MIMA by eliminating the possibility of linear composition from the communication transcripts.

Privacy-preserving is always an important issue in RFID identification study. Except the basic requirements of *anonymity* and *untraceability*, *Backward Privacy* and *Forward Privacy* are stronger privacy notions that we have mentioned. Recently, privacy notions of *wide* (or *narrow*) and *strong* (or *weak*) have been introduced in [78, 40]. *Weak* privacy is equivalent to *untraceability* while *strong* privacy is equivalent to both *Backward* and *Forward Privacy* in our study. The *wide* (or *narrow*) indicates that an attacker has knowledge of the verification result (accept or reject) from a side channel, e.g., the question, whether a door opens or not. Another example as shown in [5] demonstrated that if tags emit a distinctive "radio fingerprint," then no protocol-level countermeasures can prevent privacy infringement. Therefore, when focusing only on protocol-level privacy, we can see that EC-RAC IV, EC-RAC IV variant, scheme [16] and our work do have the *strong* privacy, i.e., the *Backward* and *Forward Privacy*. In addition, scheme [53] (without publicly transmitting tag ID-verifier) can preserve *untraceability* if it applied in a secure environment, e.g., E-Passport.

Communication efficiency is another important goal for this study. Our RFID authentication protocol is very efficient. It uses only two passes to achieve the same security and privacy requirements as EC-RAC IV, EC-RAC IV variant and scheme [16] do (these schemes need at least three passes). Although, scheme [53] is a two-pass protocol, their design does not focus on privacy preserving. To be as competitive as our proposal, we try to reduce EC-RAC IV to a two-pass protocol as shown in Fig. 13. However, we found the reduced version is vulnerable to tag impersonation attack. In the attack, an adversary A eavesdrops two successful protocol runs between the server and a specific tag, obtaining the transcripts of $\{e, T_1 = rP, T_2 = (r + s\hat{e})Y\}$ and $\{e', T_1' = r'P, T_2' = (r' + s\hat{e}')Y\}$. A can then compute $e'' = e' - e$, $\hat{e}'' = x(e''P)$, $T_1'' = T_1' - T_1 = (r' - r)P$, and $T_2'' = T_2' - T_2 = (r' + \hat{e}''s)Y - (r + \hat{e}s)Y = (r' - r)Y + (\hat{e}'' - \hat{e})sY$. We found that T_1'' and T_2'' satisfy $\hat{e}''^{-1} \cdot (y^{-1}T_2'' - T_1'') = \hat{e}''^{-1} \cdot ((r' - r)P + (e' - e)sP - (r' - r)P) = (e' - e)^{-1}(e' - e)sP = sP$. This means that by using $\{e'', T_1'', T_2''\}$, the tag will be successfully authenticated by the server. In this way, A can generate any legitimate authentication messages at his will to impersonate any specific tag successfully. Therefore, the attempt to convert EC-RAC IV to a protocol with fewer passes fails.

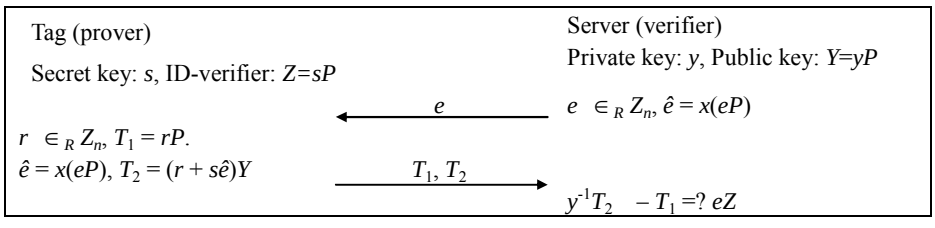

Fig. 13 Reduced EC-RAC IV

The tag hardware cost for the compared schemes is a combination of three factors (which all are measured in gates): typical ECC implementation (with point multiplication), CryptoGPS (without point multiplication), and hash function. An efficient typical ECC implementation [6] takes 8214 gates for

160-bit key size, attaining about the 80-bit security level. CryptoGPS identification technique [23, 62] adopted by [53] takes only 1967 gates to compute modular multiplications and modular additions with respect to ECC point coefficients (e.g., $y = r + sc$). In addition, an implementation of SHA-1 proposed by the authors in [53] takes 5527 gates. Due to the high cost of SHA-1 implementation, we think it might be too expensive for the tags of our proposal PII and therefore, consider another cheaper hash implementation, such as the low-cost hash function study [8] which transforms symmetric block cipher schemes into low-cost hash function. In the study, a DM-PRESENT-80 hash function (Davies-Meyer mode, 80-bit block length, 64-bit hash length, 64-bit security), focusing on one-way property only, takes about 2000 gates. While a DM-AES-128 hash function (Davies-Meyer mode, 128-bit block length, 128-bit hash length, 80-bit security), focusing on both collision-resistance and one-wayness, takes about 4400 gates. In summary, scheme [53] requires the lowest tag hardware cost, because it uses of CryptoGPS and a hash implementation. Scheme [16] and our PII require tag hardware about 10K gates; it is still believed to be acceptable for a high-cost RFID tag. Besides, for low-cost consideration, PII tag can adopt only one hash function, *Hash*(.), for all hash computations of $H(.)$, $H_1(.)$ and $H_2(.)$. More precisely, the input of the function *Hash*(.) can be any input of $H(.)$, $H_1(.)$ and $H_2(.)$; the output of *Hash*(.) is a 64-bit random string. The low-cost DM-PESENT-128 can be a candidate *Hash*(.).

Table 1 shows the comparison result that we discussed above.

Table 1 Comparisons of recent ECC RFID authentication protocols

	EC-RAC IV [41]	EC-RAC IV var. [40]	Scheme [53]	Scheme [16]	PII	Reduced PII
Scalability	yes	Yes	no	yes	yes	yes
Against De-Sync.	yes	Yes	yes	yes	yes	yes
Against MIMA	yes	Yes	yes	yes	yes	yes
Mutual Authentication	No	No	no	yes	yes	no
Untraceability	yes	Yes	no	yes	yes	yes
Strong Privacy	yes	Yes	no	yes	yes	yes
Protocol Passes	3	3	2	3	2	2
Tag Hardware (gates)	ECC (8214)	ECC (8214)	CryptoGPS+ Hash (3967)	ECC+ Hash (10214)	ECC+ Hash (10214)	ECC+ Hash (10214)
Tag Computation Load	3M	5M	1H	2M+2H	4M+3H	2M+2H
Transmission Size (bits)	480	800	480	608	768	608

Hash: adopts DM-PRESENT-80 hash function

We further examine the tag computation load and transmission size. As we know, in the ECC-based RFID schemes, the point multiplication is the heaviest computations. According to [53], it takes about 500 times of time cost than a hash computation. In Table 1, we show only the number of point multiplications and hash computations the protocols need but ignore the other minor computations like

random number generating and modular operations. It is obvious that scheme [53] has the best performance taking only one hash. Our PII, requiring four point multiplications and three hashing, takes a little higher computation overhead. To save it, we reduce the PII protocol by eliminating the signature verification for the tag which takes two point multiplications and one hashing (But the reduced PII will lose the server-to-tag authentication function). As a result, the reduced PII is competitive with EC-RAC IV. Regarding the transmission size, we adopt an ECC point as 160 bits and a hash value as 64 bits. Then EC-RAC IV and scheme [53] have the smallest size with 480 bits. While our PII has the biggest size with 748 bits, but the reduced PII has a moderate size with 608 bits.

To sum up, compared to EC-RAC IV the proposed PII takes only two passes and possesses mutual authentication but requires more cost in tag hardware, computation overhead and transmission size. Reducing the cost that the tag authenticates the server (i.e., the signature verification takes two point multiplications and one hashing) or finding other authentication approaches could be the aim of the future work.

6. Conclusion

In this paper, we reviewed several recent lightweight and ECC-based RFID authentication protocols and showed that they either have a certain security deficiency or are less efficient. We, therefore, based on ECC proposed two novel RFID authentication protocols, PI and PII, to overcome the drawbacks. We showed that PI works correctly and PII can resist various attacks and has scalability, untraceability, and forward and backward privacy. From the comparison results among PII and various ECC-based RFID authentication protocols, we conclude that the proposed protocol PII (the reduced version), which requires only two passes, and uses just two point multiplications and two hash operations on the tag side, not only had the same security level as EC-RAC IV but also was more efficient than the recently proposed solutions. We, therefore, conclude that PII is suitably applied in a real mobile world which needs high security and large-scale deployment, such as E-Passport.

Reference

1. Abid, M., & Afifi, H. (2008). Secure E-passport protocol using elliptic curve Diffie-Hellman key agreement protocol. In *International Conference on Information Assurance and Security*, 99–102.
2. Abid, M., Kanade, S., Petrovska-Delacrétaz, D., Dorizzi, B., & Afifi, H. (2010). Iris based authentication mechanism for E-passports. In *International Workshop on Security and Communication Networks (IWSCN'10)*, 1–5.
3. Ahamed, S.I., Rahman, F., & Hoque, M.E. (2008). ERAP: ECC based RFID authentication protocol. In *IEEE International Workshop on Future Trends of Distributed Computing Systems*, 219–225.
4. Alomair, B., Clark, A., Cuellar, J., & Poovendran, R. (2012). Scalable RFID systems: A

privacy-preserving protocol with constant-time identification. *IEEE Trans. On parallel and distributed systems, 23*(8), 1536–1550.

5. Avoine, G., & Oechslin, P. (2005). A scalable and provably secure hash based RFID protocol. In *IEEE Pervasive Computing and Communication Security (PerSec'05)*, 110–114.
6. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. In *IEEE International Conference on Pervasive Computing and Communications Workshops (Per'07)*, 217–222.
7. Bianchi, G. (2011). Revisiting an RFID identification-free batch authentication approach. *IEEE Communication Letters, 15*(6), NO. 6, 632–634.
8. Bogdanov, A., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., & Seurin, Y. (2008). Hash functions and RFID tags: Mind the gap. In *CHES 2008, LNCS#5154*, 283–299.
9. Buccafurri, F., & Lax, G. (2011). Implementing disposable credit card numbers by mobile phones. *Electronic Commerce Research 11*(3), 271–296.
10. Burmester, M., & Medeiros B. (2008). The security of EPC Gen2 compliant RFID protocols. In *International conference on applied cryptography and network security (ACNS'08)*, 490–506.
11. Cao, T., Bertino, E., & Lei, H. (2009). Security analysis of the SASI protocol. *IEEE Trans. on Dependable and Secure Computing, 6*(1), 73–77.
12. Cheon, J.H., Hong, J., & Tsudik, G. (2012). Reducing RFID reader load with the meet-in-the-middle strategy. *Journal of Communications and Networks, 14*(1), 10–14.
13. Chen, Y., Chou, J.S., & Sun, H.M. (2008). A novel mutual authentication scheme based on quadratic residues for RFID systems. *Computer Networks, 51*(12), 2373–2380.
14. Chien, H.Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Trans. on Dependable and Secure Computing, 4*(4), 337–340.
15. Chien, H.Y., & Chen, C.H. (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces, 9*(2), 254–259.
16. Chou, J.S., Chen, Y., Wu, C.L., & Lin, C.F. (2011). An efficient RFID mutual authentication scheme based on ECC, *Cryptology ePrint Archive*: Report 2011/418.
17. D'Arco P., & Santis, A.D. (2011). On ultralightweight RFID authentication protocols. *IEEE Trans. on Dependable and Secure Computing, 8*(4), 548–563.
18. Deng, R.H., Li, Y., Yung, M., & Zhao, Y. (2010). A new framework for RFID privacy. *Computer Security – ESORICS, LNCS# 6345*, 1–18.
19. Eurich, M., Oertel, N., & Boutellier, R. (2010). The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain. *Electronic Commerce Research 10*(3-4), 423–440.
20. Fan, J., Batina, L., & Verbauwhede, I. (2009). Light-weight implementation options for curve-based cryptography: HECC is also ready for RFID. In *International conference for Internet technology and secured transactions*, 1–6.

21. Fürbass, F. (2006). ECC signature generation device for RFID Tags.
22. Fürbass, F. & Wolkerstorfer, J, (2007). ECC processor with low die size for RFID applications. In *IEEE international symposium on Circuit and systems (ISCAS'07)*, 1835–1838.
23. Girault, M. (1991). Self-certified public keys. In *Eurocrypt '91, LNCS# 547*, 490–497.
24. 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 symposium on wireless pervasive computing (ISWPC)*, 331–336
25. Habibi, M.H., Aref, M.R., & Ma, D. (2011). Addressing flaws in RFID authentication Protocols. In *INDOCRYPT 2011, LNCS#7107*, 216–235.
26. Han, D. & Kwon, D. (2009). Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces, 31*(4), 648–652.
27. Huang, Y.J., Lin, W.C., & Li, H.L. (2012). Efficient implementation of RFID mutual authentication protocol. *IEEE Trans. on Industrial Electronics, 59*(12), 4784–4791.
28. Isaac, J.T., Zeadally, S. & Sierra, J.C. (2010). Implementation and performance evaluation of a payment protocol for vehicular ad hoc networks. *Electronic Commerce Research 10*(2), 209–233.
29. Isaac, J.T., Zeadally, S. & Sierra, J.C. (2012). A lightweight secure mobile Payment protocol for vehicular ad-hoc networks (VNETs). *Electronic Commerce Research 12*(1), 97–123.
30. Jeng, A.B., & Chen, L.Y. (2009). How to enhance the security of E-passport. In *Proc. International Conference on Machine Learning and Cybernetics*, 2922–2926.
31. Juels, A., Molnar, D., & Wagner, D. (2005). Security and privacy issues in E-passports. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 1–12.
32. Juels, A., & Weis, S. (2006). Defining strong privacy for RFID. *Cryptology ePrint Archive*, Report 2006/137.
33. Kapoor, G., & Piramuthu, S. (2010). Vulnerabilities in some recently proposed RFID ownership transfer protocols. *IEEE Communication Letters, 14*(3), 260–262.
34. Kapoor, G., & Piramuthu, S. (2012). Single RFID tag ownership transfer protocols. *IEEE Trans. on Systems, Man, and Cybernetics—Part C, 42*(2), 164–173.
35. Kaya, S.V., Savas, E., Levi, A., & Ercetin, O. (2009). Public key cryptography based privacy preserving multi-context RFID infrastructure. *Ad Hoc Networks, 7*(1), 136–151.
36. Kim, H.W., Lim, S.Y., & Lee, H.J. (2006). Symmetric encryption in RFID authentication protocol for strong location privacy and forward-security. In *International Conference on hybrid information technology (ICHIT'06)*, 718–723.
37. Kinoshita, S., Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O., & Kanai, A. (2005). Privacy enhanced active RFID tag. In *Proc. International Workshop on Exploiting Context Histories in Smart Environments*, 1–5.
38. Ko, W.T., Chiou, S.V., Lu, E.H., & Chang, H.K. (2011). An improvement of privacy-preserving ECC-based grouping proof for RFID. In *Cross Strait Quad-Regional Radio Science and Wireless*

Technology Conference, 1062–1064.

39. Kumar, S. & Paar, C. (2006). Are standards compliant elliptic curve cryptosystems feasible on RFID? In *Workshop on RFID Security*, 1–19.
40. Lee, Y.K., & Batina, L. (2010). Low-cost untraceable authentication protocols for RFID. In *ACM conference on Wireless Network Security (WiSec'10)*, 55–64.
41. Lee, Y.K., Batina, L., Singelee, D., Preneel, B., & Verbauwhede, I. (2010). Anti-counterfeiting untraceability and other security challenges for RFID Systems- public-key-based protocols and hardware. *Information Security and Cryptography, Part 5*, 237–257.
42. Lee, Y.K., Batina, L., & Verbauwhede, I. (2008). EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In *IEEE International Conference on RFID*, 97–104.
43. Lee, Y.K., Batina, L., & Verbauwhede, I. (2009). Untraceable RFID authentication protocols: Revision of EC-RAC. In *IEEE International Conference on RFID*, 178–185.
44. Lehtonen, M.O., Michahelles, F.M., & Fleisch, E.F. (2007). Trust and security in RFID-based product authentication systems. *IEEE System Journal, 1*(2), 129–144.
45. Lim, C.H., & Kwon, T. (2006). Strong and robust RFID authentication enabling perfect ownership transfer. In *ICICS'06, LNCS#4307*, 1–20.
46. Liu, H., & Ning, H. (2011). Zero-knowledge authentication protocol based on alternative mode in RFID systems. *IEEE Sensors Journal, 11*(12), 3235–3245.
47. Liu, H., Ning, H., Zhang, Y., He, D., Xiong, Q., & Yang, L.T. (2012). Grouping-proofs based authentication protocol for distributed RFID systems. *IEEE trans. on parallel and distributed systems, 24*(7), 1321–1330.
48. Luo, P., Wang, X., Feng, J., & Xu, Y. (2008). Low-power hardware implementation of ECC processor suitable for low-cost RFID tags. In *International conference on solid-state and integrated-circuit technology*, 1681–1684.
49. Maimut, D., & Ouai, K. (2012). Lightweight cryptography for RFID tags. *IEEE Security & Privacy, 10*(2), 76–79.
50. Mao, W. (2003). *Modern Cryptography - Theory and Practice*, 196–203, Prentice Hall.
51. Nathan, B.T., Meenakumari, R., & Usha, S. (2011). Formation of elliptic curve using finger print for network security. *In International conference on process automation, control and computing (PACC)*, 1–5.
52. 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.
53. O'Neill, M., & Robshaw, M.J.B. (2010). Low-cost digital signature architecture suitable for radio frequency identification tags. *IET Comput. Digit. Tech., 4*(1), 14–26.
54. Ouafi, K., & Phan, R.C.-W. (2008). Traceable privacy of recent provably-secure RFID protocols. In *International Conference Applied Cryptography and Network Security (ACNS), LNCS#5037*, 479–489.

55. Oyarhossein, S., & Mohammadi, S. (2009). Cryptography and authentication processing framework on RFID active tags for carpet products. In *International Conference on Communications Technology and Applications, (ICCTA'09)*, 26 – 31.
56. Peeters, R., Singelée, D., & Preneel, B. (2012). Toward more secure and reliable access control. *Pervasive computing, 11*(3), 76–83.
57. Pendl, C., Pelnar, M., & Hutter, M. (2012). Elliptic curve cryptography on the WISP UHF RFID tag. *RFID Security and Privacy, LNCS#7055*, 32–47.
58. Peris-Lopez, P., Hernandez-Castro, J.C., Tapiador, J.M.E., & Ribagorda, A. (2009). Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. *Information Security Applications, LNCE#5379*, 56–68.
59. Phan, R.C.-W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol - SASI. *IEEE Trans. on Dependable and Secure Computing, 6*(4), 316–320.
60. Piramuthu, S. (2008). Lightweight cryptographic authentication in passive RFID-tagged systems. *IEEE Trans. on Systems, Man, and Cybernetics—Part C, 38*(3), 360–376.
61. Piramuthu, S. (2011). RFID mutual authentication protocols. *Decision Support Systems*, *50*(2), 387–393.
62. Poupard, G., & Stern, J. (1998). Security analysis of a practical 'On the Fly' authentication and signature generation. In E*urocrypt'98, LNCS#1403*, 422–436.
63. Rennhard, M., Rafeli, S., Mathy, L., Plattner. B., & Hutxhison, D. (2004). Towards pseudonymous e-commerce. *Electronic Commerce Research 4*(1-2), 83–111.
64. Rizomiliotis, P., Rekleitis, E., & Gritzalis, S. (2009). Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags. *IEEE Communication Letters, 13*(4), 274–276.
65. Roberti, M. (2007). A 5-cent breakthrougha. In *International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT'07)*.
66. Sadeghi, A.R., Visconti, I., & Wachsmann, C. (2010). Enhancing RFID security and privacy by physically unclonable functions. *Information Security and Cryptography, Part 5*, 281–305.
67. Seo, Y., Lee, H., & Kim, K. (2006). A scalable and untraceable authentication protocol for RFID. In *International conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06)*, 252–261.
68. Song, B., Hwang, J.Y., & Shim, K.A. (2011). Security improvement of an RFID security protocol of ISO/IEC WD 29167-6. *IEEE Communication Letters, 15*(12), 1375–1377.
69. Song, B., & Mitchell, C.J. (2011). Scalable RFID security protocols supporting tag ownership transfer. *Computer Communications, 34*(1), 556–566.
70. Stinson, D. R. (1995). *Cryptography – Theory and Practice*, CRC Press Inc.
71. Sun, H.M., & Ting, W.C. (2009). A Gen2-based RFID authentication protocol for security and privacy. *IEEE Trans. on Mobile Computing, 8*(8), 1052–1062.
72. Sun, H.M, Ting, W.C., & Wang, K.H. (2011). On the security of Chien's ultralightweight RFID authentication protocol. *IEEE Trans. on Dependable and Secure Computing, 8*(2), 315–317.

73. Tagra, D., Rahman, M., & Sampalli, S. (2010). Technique for preventing DoS attacks on RFID systems. *Software, Telecommunications and Computer Networks, 23*(25), 6–10.
74. Tan, C.C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Trans. on Wireless Communications, 7*(4), 1400–1407.
75. Tan, C.C., Sheng, B., & Li, Q. (2010). Efficient techniques for monitoring missing RFID tags. *IEEE Trans. on Wireless Communications, 9*(6), 1882–1889.
76. Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. *IEEE Communication Letters, 6*(5), 702–705.
77. Tuyls, P., & Batina, L. (2006). RFID-tags for anti-counterfeiting. *Topics in Cryptology – CT-RSA, LNCE#3850*, 115–131.
78. Vaudenay, S. (2007). On privacy models for RFID. *Advances in Cryptology, LNCS#4822*, 68–87.
79. Vaudenay, S. (2007). E-passport threats. *IEEE Security and Privacy, 5*(6), 61–64.
80. Wang, B., & Ma, M. (2012). A server independent authentication scheme for RFID systems. *IEEE Trans. on Industrial Informatics, 8*(3), 689–696.
81. Wei, C.H., Hwang, M.S., & Chin, A.Y. (2011). A mutual authentication protocol for RFID. *IT Professional, 13*(2), 20–24.
82. Yamada, I., Shiotsu, S., Itasaki, A., Inano, S., Yasaki, K. & Takenaka, M. (2005). Secure active RFID tag system. In *International Workshop on UbiComp Privacy*, 1–5.
83. Yeh, K.H., & Lo, N.W. (2010). Improvement of two lightweight RFID authentication protocols. *Information Assurance and Security Letters*, *1*, 6–11.
84. Yeh, T.C., Wang, Y.J., Kuo, T.C., & Wang, S.S. (2010). Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications, 37*(2), 7678–7683.
85. Zuo, Y. (2012). Survivability experiment and attack characterization for RFID. *IEEE Trans. on Dependable and Secure Computing, 9*(2), 289–302.

Yalin Chen received her bachelor degree in the department of computer science and information engineering from Tamkang University, her MBA degree in the department of information management from National Sun-Yat-Sen University (NYSU), and her Ph.D. degree from the Institute of Information Systems and Applications of National Tsing-Hua University (NTHU) in Hsinchu, Taiwan. She is now a Research Assistant for projects of the National Science Council. Her primary research interests are data security and privacy, protocol security, authentication, key agreement, electronic commerce security, wireless communication

	security, RFID authentication protocol, electronic cash.
	**Jue-Sam Chou** received his Ph.D. degree in the department of computer science and information engineering from National Chiao Tung University (NTCU) in Hsinchu, Taiwan, ROC. He is an associate professor and teaches at the department of Information Management of Nanhua University in Chiayi, Taiwan. His primary research interests are electronic commerce security, data security and privacy, protocol security, authentication, key agreement, sensor network security, RFID authentication protocol, electronic cash, electronic voting.