1-1-2013

On RFID authentication protocols with wide-strong privacy

Nan Li
University of Wollongong, nl864@uowmail.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Vijay Varadharajan
Macquarie University

On RFID authentication protocols with wide-strong privacy

Abstract

Radio frequency identification (RFID) tag privacy is an important issue to RFID security. To date, there have been several attempts to achieve the wide-strong privacy by using zero-knowledge protocols. In this paper, we launch an attack on the recent zero-knowledge based identification protocol for RFID, which was claimed to capture wide-strong privacy, and show that this protocol is flawed. Subsequently, we propose two zero-knowledge based tag authentication protocols and prove that they offer wide-strong privacy.

Publication Details

Li, N., Mu, Y., Susilo, W., Guo, F. & Varadharajan, V. (2013). On RFID authentication protocols with wide-strong privacy. Cryptology and Information Security Series, 11 3-16.

On RFID Authentication Protocols with Wide-Strong Privacy [1]

Nan Li [a], Yi Mu [a], Willy Susilo [a,2], Fuchun Guo [a] and Vijay Varadharajan [b]

[a] *Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, Australia*

e-mail: {nl864,ymu,wsusilo,fuchun}@uow.edu.au

[b] *Information and Networked Systems Security Research, Department of Computing, Faculty of Science, Macquarie University, Sydney,Australia*

e-mail: vijay.varadharajan@mq.edu.au

Abstract. Radio frequency identification (RFID) tag privacy is an important issue to RFID security. To date, there have been several attempts to achieve the wide-strong privacy by using zero-knowledge protocols. In this paper, we launch an attack on the recent zero-knowledge based identification protocol for RFID, which was claimed to capture wide-strong privacy, and show that this protocol is flawed. Subsequently, we propose two zero-knowledge based tag authentication protocols and prove that they offer wide-strong privacy.

1. Introduction

Radio frequency identification (RFID) tags have very limited computation and storage resources and are usually not tamper-resistant. For example, an attacker could physically access the RFID tag and collect its internal state. The RFID tag communicates with the RFID reader via a wireless interaction, and hence, there is a security concern. The attacker could be able to identify a tag by using the information collected from tag-reader communication. Therefore, the privacy of RFID tags has become an issue in RFID applications.

Vaudenay [22] introduced the strong privacy model which captures a number of RFID privacy cases, which are corresponding to eight classes with respect to eight different privacy levels from weak to strong. The strongest level is the wide-strong privacy. Later, Ng, Susilo, Mu and Safavi-Naini [16] refined the Vaudenay's model and claimed that the wide-strong privacy is possible. Based on the Bohli-Pashalidis' model [2,3] and Vaudenay's model, Hermans, Pashalidis, Vercautern and Preneel [10] proposed a new practical RFID privacy model which relies on the indistinguishability of tags.

[1] This work is supported by the Australian Research Council Discovery Project DP110101951.

[2] This work is supported by ARC Future Fellowship FT0991397.

Wide-strong privacy is achievable by using the public key cryptography (PKC) [22,16]. An RFID authentication protocol based on the IND-CCA2 secure public key encryption scheme is strong private for wide adversaries [10]. Deursen and Radomirović [7] proposed the wide-strong private authentication protocol by employing the Cramer-Shoup encryption scheme.

The digital signature is an alternative cryptographic primitive in PKC. However, a traditional digital signature is hard to preserve the tag's privacy as the signature is publicly verifiable. Fortunately, we found that digital signatures, such as strong designated verifier signatures [11], can be obtained by applying IND-CCA2 encryption schemes. Thus, it is possible to construct a wide-strong private identification protocol based on strong designated verifier signature schemes. The elliptic curve cryptography (ECC) based RFID authentication protocols are acceptable by low-cost RFID tags [9,15]. Many ECC based RFID authentication protocols [21,12,13,14,1] were proposed. Most of them are the variants of the Schnorr signature scheme. However, these schemes have been unfortunately broken later in [8,12,5,6,4]. Recently, a new and interesting protocol was proposed by Peeters and Hermans [18]. They claimed that the protocol achieves the wide-strong privacy.

Our Contributions

The contribution of this paper is twofold. First, in contrast to the claim made in [18][3], we demonstrate that Peeters and Hermans' [18] protocol is vulnerable to our attack, which makes the tag traceable. Second, we propose two wide-strong private protocols based on zero-knowledge. The proposed protocols offer provable wide-strong privacy in the model described in [10]. As features of our protocols, the reader can convince a third party, such as a client in the supply chain, the presence of the tag by signature which is extracted from a successful authentication and our (second) optimized protocol eliminates the modular operations in the prime field.

Paper Organizations

The rest of this paper is organized as follows. In Section 2, we describe some mathematical preliminaries and review the underlying privacy model. Section 3 demonstrates an attack launched by the wide-strong adversary against Peeters and Hermans' protocol. We proposed a basic protocol and prove the privacy in Section 4 and Section 5, respectively. An optimized protocol is presented in Section 6. Section 7 concludes the paper.

2. Preliminaries

In this section, we give the definitions of some mathematical preliminaries and present the adopted privacy model of this paper.

[3]The authors updated their paper [18] in eprint and the new version does not suffer from the attack.

2.1. Bilinear Maps

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three additive cyclic groups of same prime order q. P and V are generators of group $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear mapping (pairing) and $(P, V, q, e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ is a bilinear group. Let ψ be a computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ that $\psi(V) = P$. We say it is a symmetric bilinear group if $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$. A bilinear pairing satisfies the properties as follows:

- **Bilinearity**: for all $P \in \mathbb{G}_1$, $V \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_q^*$, we have the equation $e(P^a, V^b) = e(P, V)^{ab}$.
- **Non-Degeneracy**: for all $P \in \mathbb{G}_1$, $V \in \mathbb{G}_2$, if P, V are generators respectively, we have $e(P, V) \neq 1$ is a generator of $\mathbb{G}_T$.
- **Efficiency**: There is an efficient algorithm to calculate $e(P, V)$ for all $P \in \mathbb{G}_1$, $V \in \mathbb{G}_2$.

2.2. Complexity Assumptions

Definition 1 (Computational Diffie-Hellman (CDH) assumption) *Given a tuple $< P, aP, bP >$, where $a, b \in_R \mathbb{Z}_q^*$, P is a generator of the group $\mathbb{G}$, there is no PPT adversary can find abP with advantage at least ϵ.*

2.3. Privacy Model

In this paper, we use the privacy model defined in [10]. The oracles defined in the model are as follows.

- $\mathsf{CreateTag}(\mathsf{ID}) \to T_i$: Taking as input a tag's identifier ID, the oracle sets up and registers a new tag to server. Then, it outputs the reference T_i of the tag.
- $\mathsf{Launch}() \to \pi, m$: It launches a new session π and returns the first message m sent by the reader.
- $\mathsf{DrawTag}(T_i, T_j) \to vtag$: Taking as input a pair of tag references (T_i, T_j), it outputs $vtag$ which is a virtual tag reference linked to either T_i or T_j according to the value of g, where $g \in \{0, 1\}$. The oracle outputs $\perp$, if T_i or T_j is already drawn.
- $\mathsf{Free}(vtag)$: Taking as input a virtual tag $vtag$, it retrieves the tuple $(vtag, T_i, T_j)$ and moves (T_i, T_j) to the set of free tags and resets T_i's (if $g = 0$) or T_j's (if $g = 1$) volatile memory.
- $\mathsf{SendTag}(vtag, m) \to m'$: Taking as input a virtual tag $vtag$ and a message m, the oracle retrieves $(vtag, T_i, T_j)$ and sends m to the tag T_i (if $g = 0$) or T_j (if $g = 1$). It outputs the tag's response m'.
- $\mathsf{SendReader}(\pi, m) \to m'$: Taking as input an instance π and a message m, the oracle sends m to the reader in session π and outputs the reader's response m'. If the session π is not activated, the oracle outputs $\perp$.
- $\mathsf{Result}(\pi) \to c$: Taking as input an instance π, the oracle outputs the result c of the authentication if π exists, otherwise outputs $\perp$.
- $\mathsf{Corrupt}(T_i) \to s$: Taking as input a reference T_i of the tag, the oracle outputs the state s of the tag if T_i is not drawn, otherwise outputs $\perp$.

The model defined eight different classes of privacy and adversary. In each class, the adversary is restricted by the capability of oracle access. The strongest adversary in the model is the wide-strong adversary who can access the all above oracles as many times as he needs in polynomial time. The privacy experiment $\mathbf{Exp}_{\mathcal{A},\mathcal{S}}^{ws-private}$ for the wide-strong adversary is as follows:

1. Setup: The system $\mathcal{S}$ sets up the system depending on the security parameter k and chooses a random bit $g \in \{0,1\}$.
2. Learning: The adversary $\mathcal{A}$ can interact with $\mathcal{S}$ in polynomial time and queries all above oracles.
3. Guess: The adversary outputs a bit g'. If $g' = g$, the experiment outputs 1, 0 otherwise.

We say that the adversary $\mathcal{A}$ wins the wide-strong privacy game if and only if the experiment outputs 1.

Definition 2 *A RFID authentication protocol is privacy-preserving if there is no adversary $\mathcal{A}$ who wins the wide-strong privacy game in polynomial time t with the advantage $Adv_{\mathcal{A}}$ at least ϵ, where*

$$Adv_{\mathcal{A}} = \left| \Pr[\mathbf{Exp}_{\mathcal{A},\mathcal{S}}^{ws-privacy} = 1] - \frac{1}{2} \right| \geq \epsilon.$$

3. A Simple Attack

In RFID privacy models [22,10], the adversary is classified to "narrow" and "wide" according to whether allowed to query Result oracle during the simulation. A wide adversary can query the Result oracle to check whether a session is valid. Our attack exploits the capabilities of wide-strong adversaries where they can forge new sessions by using the tag's private key and verify the validity of the forgery.

In the attack, the adversary can query all oracles defined in Section 2.3. He chooses two tags T_0 and T_1 and queries the Corrupt oracle to both of them. Upon receiving the internal state of T_0 and T_1, the adversary issues SendTag query to a virtual tag T_g which is either linked to T_0 or T_1. The adversary generates a new response $\mathcal{I}^{*\prime}$ by using the tag's state and $\mathcal{I}^*$ which is the response of the tag. Then, the adversary submits $\mathcal{I}^{*\prime}$ to the Result oracle. Based on the output of the Result oracle, the adversary can output a correct link between the virtual tag and the target tag. The attack is depicted as in Fig.1.

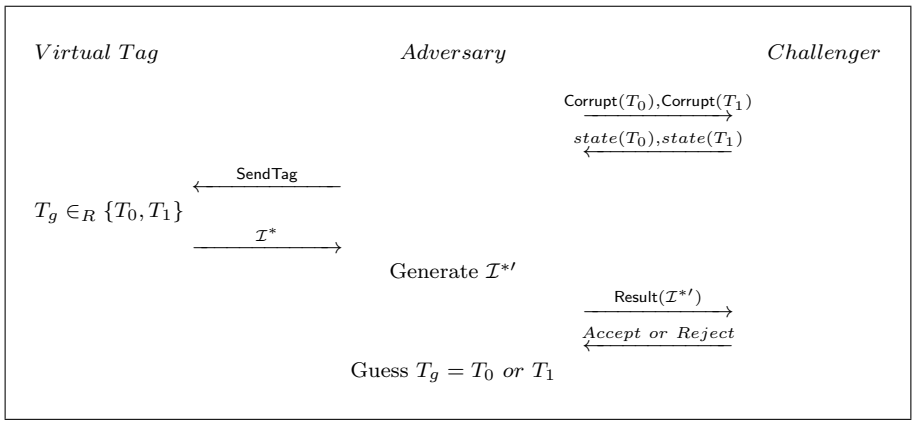

Figure 1. Our attack.

3.1. Peeters and Hermans' Protocol

Recently, Peeters and Hermans [18] proposed an interesting RFID identification protocol based on zero-knowledge. They presented two protocols where the second one is an efficient optimized version. Here, we review their improved protocol. In the protocol, both tag and reader have a pair of public/private keys $(x, X = xP)$ and $(y, Y = yP)$, respectively. The public keys X and Y are mutually known to the reader and the tag. The protocol initiated with the tag generating a random number $r \in \mathbb{Z}_q^*$. The tag sends the reader $R = rP$ and receives the reader's response e, where $e \in \mathbb{Z}_q^*$. The tag computes

$$d = xcoord(rY),\ s = x + er + d,$$

where $xcoord$ is a function which returns the value of x-coordinate of the input point, and sends s to the reader. Upon receiving the response, the reader computes

$$d' = xcoord(yR),\ X' = (s - d')P - eR,$$

and accepts the tag if X' appears in the database. The protocol is depicted as in Fig. 2.

The authors claimed that their protocol is wide-strong private, while we show that the protocol is vulnerable to our attack.

Theorem 1 *In Peeters and Hermans' protocol (Figure 2), a wide-strong adversary is able to break the tag's private with advantage* $\Pr[\bar{E}] = 1 - \frac{n}{q}$.

Proof 1 *Suppose that the public system parameters* (P, Y)*, where* P *is a generator of a goup* $\mathbb{G}$ *and* Y *is the reader's public key, are known to the adversary. Given an instance of the protocol execution of the tag* T_0 *or the tag* T_1*, the wide-strong adversary* $\mathcal{A}$ *aims to decide which tag involves the session.*

The adversary $\mathcal{A}$ *issues two oracle calls, which are* $\mathsf{Corrupt}(T_0)$ *and* $\mathsf{Corrupt}(T_1)$ *to the challenger. The challenger respectively returns* T_0 *and* T_1*'s private keys* x_0

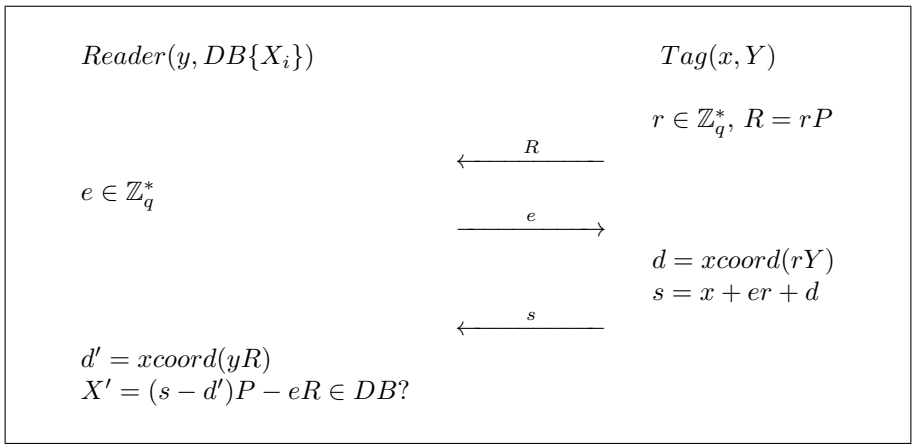

Figure 2. Peeters and Hermans' protocol.

and x_1 to the adversary. In the challenge phase, the challenger gives an instance $\mathcal{I}^*$ of the protocol execution, where $\mathcal{I}^* = (R^*, e^*, s^*)$. The instance is generated by using the tag T^*'s private key x^*, where $x^* = x_0$ or $x^* = x_1$. Hence, we have

$$s^* = x^* + e^* r^* + d^*,$$

where $d^* = xcoord(r^*Y)$. Then, $\mathcal{A}$ generates a new instance $\mathcal{I}^{*\prime} = (R^{*\prime}, e^{*\prime}, s^{*\prime})$ as follows,

$$R^{*\prime} = R^*,\ e^{*\prime} = e^*,\ s^{*\prime} = s^* - x_0 + x_1.$$

Since $\mathcal{A}$ is a wide adversary, it queries the Result *oracle on input a session $\mathcal{I}^{*\prime}$. The challenger then returns whether it accepts the session. If the challenger's output is* 1*, it means that $\mathcal{I}^{*\prime}$ is valid and $\mathcal{A}$ has*

$$s^{*\prime} = s^* - x_0 + x_1 = (x^* - x_0 + x_1) + e^* r^* + d^*.$$

Then, we have three cases:

- Case 1 *($x^* - x_0 + x_1 = x_0$): With the new session wrt tag T_0, $\mathcal{A}$ has the solution that $x^* = 2x_0 - x_1$.*
- Case 2 *($x^* - x_0 + x_1 = x_1$): With the new session wrt tag T_1, $\mathcal{A}$ has the solution that $x^* = x_0$.*
- Case 3 *($x^* - x_0 + x_1 = x_2$): With the new session wrt another tag T_2, where x_2 is the private key of T_2, $\mathcal{A}$ has the solution $x^* = x_2 + x_0 - x_1$.*

According to the knowledge that x^* is either x_0 or x_1 and assuming tags have individual keys, Case 1 *is impossible as it indicates $x_0 = x_1$. $\mathcal{A}$ can deduce from* Case 2 *and* Case 3 *that*

$$x^* = x_0 \text{ or } x^* = x_2 + x_0 - x_1 = x_1.$$

Then, $\mathcal{A}$ can guess the session $\mathcal{I}^*$ is related to the tag T_0 with a high probability. If the challenger rejects the session $\mathcal{I}^{*\prime}$, $\mathcal{A}$ can decide $\mathcal{I}^*$ is related to the tag T_1. Therefore, the protocol is vulnerable to our attack.

Let E be the event that there exists the tag T_2 with the private key

$$x_2 = 2x_1 - x_0.$$

Since a tag's private key is randomly chosen from $\mathbb{Z}_q^*$, it can be considered that $2x_1 - x_0$ is also a random value. Event E occurs with a negligible probability $\frac{n}{q}$, where n is the number of tags except T_0 and T_1. Hence, the adversary outputs a correct guess with the probability

$$\Pr[\bar{E}] = 1 - \frac{n}{q}.$$

□

4. Proposed Protocol

Many ECC-based RFID identification protocols employ Diffie-Hellman keys to preserve the privacy of the tag. Usually, there are two approaches to generate the Diffie-Hellman key: 1) The tag uses its private key and the nonce(s) to compute with the reader's public key (e.g., [1,12,13]); 2) The tag chooses a random number to compute with the reader's public key (e.g., [18]). However, a strong adversary can compromise the tag and obtain the tag's private key. Hence, the two ways provide the equal level of privacy protection under the strong attack. In this paper, we adopt the second approach.

To withstand the attack described in Section 3, the tag's response should not be transferable to another valid response even if the tag's private key is known to the adversary. In our protocol, we protect the tag's private key by using two random values. Given a valid tag's response, anyone who does not have the tag's temporary key or the reader's private key cannot output a new valid tag's response.

Our protocol is a variant of the Schnorr identification protocol [19]. The identification process consists of two passes where the reader initiates the session. Prior to identifying the tag, both of the reader and the tag are required to store particular states. Let $\mathbb{G}$ is an additive group with the prime order p and P is a generator of the group. The public/private key pairs of the tag and the reader are $(x, X = xP)$ and $(y, Y = yP)$, respectively, where $x, y \in_R \mathbb{Z}_q^*$. Initially, the backend server inserts the tag's public key X into the database DB as the tag's identifier. The server sets the tuple (x, Y, P) as the tag's state and stores it into the tag. The reader receives its pair of public/private keys and it is allowed to access the database.

To identify a tag, the reader randomly chooses $C \in \mathbb{G}$ and sends C as a challenge to the tag. Upon receiving the challenge, the tag firstly picks a random number $r \in \mathbb{Z}_q^*$ and computes $R = rP$. Let $h : \mathbb{G} \times \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_q^*$ be a cryptographic hash function. The tag generates a signing message

$$v = h(R, rY, C),$$

where rY is a temporary Diffie-Hellman key. The signing message is computable if and only if either the tag's choice r or the reader's private key y is known. It is significant to preserve the tag's privacy. Then the tag computes

$$s = xv + r \pmod{q},$$

and sends (R, s) to the reader. On receiving the tag's response, the reader extracts the tag's identity as

$$v' = h(R, yR, C),\ X' = (sP - R){v'}^{-1}.$$

If X' exists in the database, the tag is identified, otherwise it is rejected. The proposed basic RFID identification protocol is depicted as in Fig. 3.

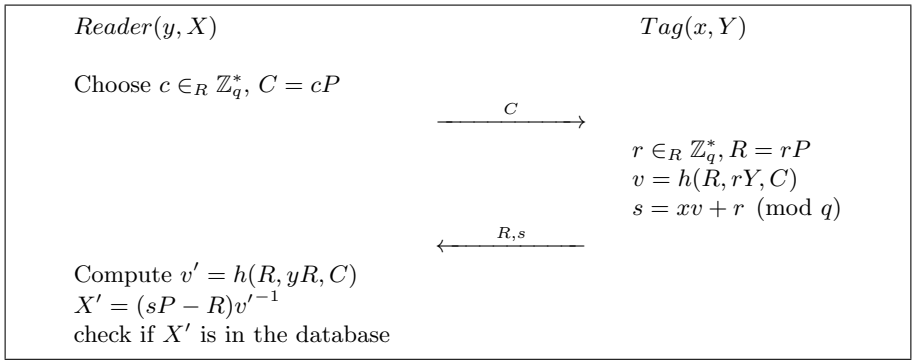

Figure 3. Baisc protocol.

The reader can extract the tag's signature after a successful tag authentication. Given yR and C, anyone who has the tag's public key X can verify the validity of the signature (R, s). It is an important difference between the encryption based protocols and the zero-knowledge based protocols.

5. Privacy Analysis

We analyse the privacy of the proposed basic protocol and show that it is wide-strong private under the model [10].

Theorem 2 *The proposed basic RFID authentication protocol is private against the wide-strong attack if the CDH problem is hard.*

Proof 2 *Suppose that there is an adversary $\mathcal{A}$ who can (ϵ, q_h, t)-distinguish the 'left' and 'right' world in the wide-strong privacy experiment. Let $\mathcal{A}$ has an advantage ϵ' to solve the CDH problem. We can construct an algorithm $\mathcal{B}$ run by*

the challenger to solve the CDH problem using the adversary $\mathcal{A}$. Given the CDH instance (P, aP, bP), algorithm $\mathcal{B}$ aims to output abP. On behalf of the system $\mathcal{S}$, $\mathcal{B}$ interacts with the adversary $\mathcal{A}$ as follows.

- Setup*: $\mathcal{B}$ sets P as the generator of the additive cyclic group $\mathbb{G}$. Let the public key of the reader be $Y = aP$ and the private key of the reader be $y = a$, which is unknown to $\mathcal{B}$. $\mathcal{B}$ maintains the lists $L_h = \{< R, rY, C, v > \}$, $L_{Ref} = \{< vtag, T_i, T_j >\}$, $L_S = \{< T, \pi, z >\}$ and a database of tags $\mathcal{T} = \{< ID, T, X, x >\}$, which are initially empty. $\mathcal{B}$ tosses a coin and sets $g = 0$ or $g = 1$, where $\Pr[g = 0] = \Pr[g = 1] = \frac{1}{2}$. The virtual tag reference $vtag$ is an incremental counter starts from 0.*
- h Query*: $\mathcal{A}$ issues $h_{\mathcal{E}}$ query on input (R_i, r_iY, C_i) at most q_h times. $\mathcal{B}$ outputs v_i if (R_i, r_iY, C_i) is in the list L_h. Otherwise, $\mathcal{B}$ randomly selects $v_i \in \mathbb{Z}_q^*$ and sets $h(R_i, r_iY, C_i) = v_i$. Then, $\mathcal{B}$ outputs v_i and adds $< R_i, r_iY, C_i, v_i >$ into the list L_h.*
- CreateTag Query*: $\mathcal{A}$ issues the oracle query on input a tag identity ID_i. If ID_i is not in $\mathcal{T}$, $\mathcal{B}$ sets up a new tag T_i and generates the tag's pubic/private key pair (x_i, X_i), where $x_i \in \mathbb{Z}_q^*$, $X_i = x_iP$. $\mathcal{B}$ outputs the reference T_i and adds $< ID_i, T_i, X_i, x_i >$ into the database $\mathcal{T}$. If ID_i exists, $\mathcal{B}$ ignores the query.*
- DrawTag Query*: $\mathcal{A}$ issues the oracle query on input a pair of tag references (T_i, T_j). If any of the issued tags is not free, which is currently referenced, the oracle outputs $\perp$. If $g = 0$, $\mathcal{B}$ references $vtag$ to T_i, T_j otherwise. $\mathcal{B}$ outputs $vtag$ and adds $< vtag, T_i, T_j >$ into the list L_{Ref}.*
- Free Query*: $\mathcal{A}$ issues the oracle query on input a reference $vtag$. If $vtag$ is in the list L_{Ref}, $\mathcal{B}$ deletes the entry $< vtag, T_i, T_j >$ and erases the volatile memory of the referenced tag, which is T_i or T_j.*
- Corrupt Query*: $\mathcal{A}$ issues the oracle query on input a tag reference T_i. If T_i is not in $\mathcal{T}$, $\mathcal{B}$ firstly creates a new tag by using* CreateTag Query*. $\mathcal{B}$ then outputs the tag's secret key x_i.*
- SendTag Query*: $\mathcal{A}$ issues the oracle query on input $vtag$ and a message C_i. If the entry $< vtag, T_i, T_j >$ is not in the list L_{Ref}, $\mathcal{B}$ outputs $\perp$. Otherwise, $\mathcal{B}$ retrieves the the referenced tag T_g's secret key x_g and computes as follows.*

  * *Randomly selects $z_i \in \mathbb{Z}_q^*$ and let $r_i = b + z_i$. Then, $\mathcal{B}$ computes $R_i = bP + z_iP$.*
  * *$\mathcal{B}$ randomly picks $w_i \in \mathbb{Z}_q^*$ and lets $v_i = w_i - \frac{b}{x_g}$.*
  * *Computes $s_i = x_gw_i + z_i$ and sets $m_i = (R_i, s_i)$, $\pi_i = (C_i, m_i)$.*

  $\mathcal{B}$ outputs m_i and adds $< T_i, \pi_i, z_i >$ into the list L_S. We show that the simulation is perfect as

$$\begin{aligned} s_i &= x_gw_i + z_i \\ &= x_g(w_i - \frac{b}{x_g}) + (b + z_i) \\ &= x_gv_i + r_i \end{aligned}$$

- SendReader Query*: Since there is no reply message from the reader, $\mathcal{B}$ ignores the query to this oracle.*
- Result Query*: $\mathcal{A}$ issues the oracle query on input a session π_i. $\mathcal{B}$ responses as follows.*
  - *If π_i is in the list L_S, $\mathcal{B}$ accepts the session and outputs 1.*
  - *If π_i,is not in the list L_S, $\mathcal{B}$ looks up the list L_h. If $< R_i, \cdot, C_i, v_i >$ is not in L_h, $\mathcal{B}$ outputs 0 and rejects the session.*
  - *$\mathcal{B}$ Computes $X_i = (s_i P - R_i)v_i^{-1}$ and verifies it by checking if X_i in the the database $\mathcal{T}$. $\mathcal{B}$ outputs 1 if it exists, 0 otherwise.*

Eventually, the adversary has to output a bit $g' \in \{0, 1\}$ in the guess phase. That is, to determine which world ('left' or 'right') the simulation has encountered. If the adversary successfully outputs $g' = g$, he wins the experiment and $\mathcal{B}$ can use it to solve the CDH problem. Since $\mathcal{A}$ has to query the hash oracle to determine which tag is referenced during the experiment, there is at least one query input $(R_i, r_i Y, c_i)$ to the Hash Query *is correct. $\mathcal{B}$ retrieves $r_i Y$ from the list L_h and computes $abP = r_i Y - z_i Y$, where $z_i \in L_S$, to be a solution of the given CDH problem.*

The simulation fails when $\mathcal{B}$ rejects a valid session. It occurs when $\mathcal{A}$ issued a valid session π to Result *while $< R_i, \cdot, C_i, v_i >$ is not in the list L_h. A valid session which is not generated by $\mathcal{B}$ implies that the adversary could find the Diffie-Hellman key $r_i Y$ or guess the correct s_i. Let the event E be that the simulation fails. We have the negligible probability $\Pr[E] \leq \epsilon + \frac{n}{q}$, where n is the number of tags in $\mathcal{T}$.*

□

6. Optimisation

RFID tags are resource-constrained devices which have limited gates to implement protocols. The increase of the tag's gates costs more in production. In terms of the hardware implementation of our basic protocol, the tag is required to do the modular in both of the prime field and the binary field. Although the modular is an efficient operation, it consumes large number of gates for the hardware implementation [17,20]. Unfortunately, most of RFID identification protocols which are based on public key cryptography need modular calculations in both of the prime field and the binary field.

In this section, we propose an optimized protocol and show that the number of required gates are reduced. As a feature, there is no modular operation in the prime filed required to the tag. Instead, only the modular in the binary field is needed.

6.1. Protocol 2

The optimized protocol also consists of two passes where the reader initiates the session. Let $\mathbb{G}$ be an additive group with the prime order q and e be a bilinear pairing, where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. P_1 and P_2 are two generators of the group $\mathbb{G}$.

The public/private key pairs of the tag and the reader are $(xP_2, X = e(P_1, xP_2))$ and $(y, Y = yP_2)$, respectively, where $x, y \in_R \mathbb{Z}_q^*$. The backend server inserts the entry of the tag into the databse and stores the tuple (xP_2, Y, P_1, P_2) into the tag. The reader receives its pair of public/private keys and it is allowed to access the database.

To identify a tag, the reader randomly selects $C \in \mathbb{G}$ and sends C as a challenge to the tag. Upon receiving the challenge, the tag chooses a random number $r \in \mathbb{Z}_q^*$ and computes $R = rP_1$. Then, the tag generate a signing message v as in the basic protocol, where $v = h(R, rY, C)$. The tag computes

$$S = vxP_2 + rP_2,$$

and sends (R, S) to the reader. On receiving the tag's response, the reader extracts the tag's identity as

$$v' = h(R, yR, C),\ X' = \left(\frac{e(P_1, S)}{e(R, P_2)}\right)^{v'-1}.$$

If X' exists in the database, the tag is identified, otherwise it is rejected. The optimized RFID identification protocol is depicted as in Fig.4.

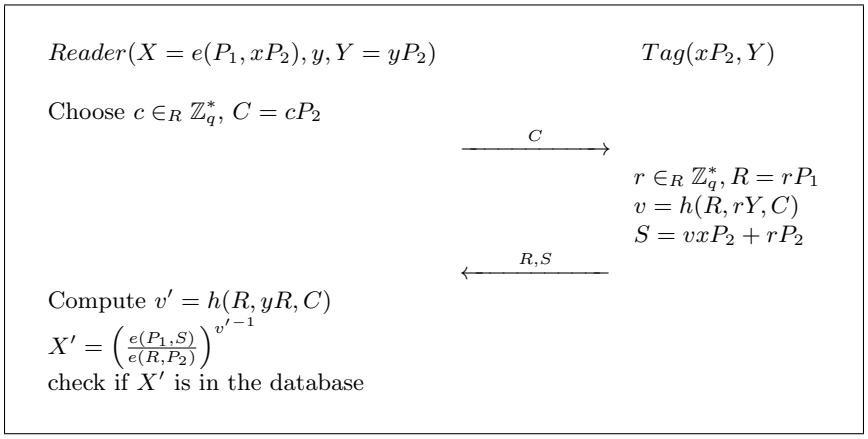

Figure 4. Optimized protocol.

6.2. Privacy Analysis

Theorem 3 *The proposed optimized RFID identification protocol is private against the wide-strong adversary if the CDH problem is hard.*

Proof 3 *Suppose that there is an adversary $\mathcal{A}$ who can (ϵ, q_h, t)-distinguish the 'left' and 'right' world in the wide-strong privacy experiment. Let $\mathcal{A}$ has an advantage ϵ' to solve the CDH problem. Given an instance (P, aP, bP), we can construct an algorithm $\mathcal{B}$ to find the solution abP of CDH problem using the adversary $\mathcal{A}$. $\mathcal{B}$ interacts with the adversary $\mathcal{A}$ as follows.*

- Setup*: $\mathcal{B}$ selects k, where $k \in \mathbb{Z}_q^*$ and sets P_1, P_2, where $P_1 = kP, P_2 = P$, as two generators of the additive cyclic group $\mathbb{G}$. Let the public key of the reader be $Y = aP$ and the private key of the reader be $y = a$, which is unknown to $\mathcal{B}$. $\mathcal{B}$ maintains the lists $L_h = \{< R, rY, C, v >\}$, $L_{Ref} = \{< vtag, T_i, T_j >\}$, $L_S = \{< T, \pi, z >\}$ and a database of tags $\mathcal{T} = \{< ID, T, X, xP >\}$, which are initially empty. $\mathcal{B}$ tosses a coin and sets $g = 0$ or $g = 1$, where $\Pr[g = 0] = \Pr[g = 1] = \frac{1}{2}$. The virtual tag reference vtag is an incremental counter starts from 0.*
- h Query*: $\mathcal{A}$ issues $h_{\mathcal{E}}$ query on input (R_i, r_iY, C_i) at most q_h times. $\mathcal{B}$ outputs v_i if (R_i, r_iY, C_i) is in the list L_h. Otherwise, $\mathcal{B}$ picks $v_i \in \mathbb{Z}_q^*$ and sets $h(R_i, r_iY, C_i) = v_i$. Then, $\mathcal{B}$ outputs v_i and adds $< R_i, r_iY, C_i, v_i >$ into the list L_h.*
- CreateTag Query*: $\mathcal{A}$ issues the oracle query on input a tag's identity ID_i. $\mathcal{B}$ ignores the query if ID_i exists. Otherwise, $\mathcal{B}$ randomly chooses $x_i \in \mathbb{Z}_q^*$ and computes $X_i = e(kP, x_iP)$. Then, $\mathcal{B}$ creates a new tag and sets (X_i, x_iP) as its public and private key pair. $\mathcal{B}$ outputs the reference T_i and adds $< ID_i, T_i, X_i, x_iP >$ into the database $\mathcal{T}$.*
- DrawTag Query*: $\mathcal{A}$ issues the oracle query on input a pair of tag references (T_i, T_j). If any of the issued tags is not free, the oracle outputs $\perp$. Depending on the value of g, $\mathcal{B}$ references vtag to T_i (if $g = 0$) or T_j (if $g = 1$). $\mathcal{B}$ outputs vtag and adds $< vtag, T_i, T_j >$ into the list L_{Ref}.*
- Free Query*: $\mathcal{A}$ issues the oracle query on input a reference vtag. If vtag is in the list L_{Ref}, $\mathcal{B}$ removes the entry $< vtag, T_i, T_j >$ and erases the volatile memory of the referenced tag.*
- Corrupt Query*: $\mathcal{A}$ issues the oracle query on input a tag reference T_i. If T_i is not in $\mathcal{T}$, $\mathcal{B}$ creates a new tag by running* CreateTag Query*. $\mathcal{B}$ then outputs the tag's secret key x_iP.*
- SendTag Query*: $\mathcal{A}$ issues the oracle query on input vtag and a message C_i. $\mathcal{B}$ outputs $\perp$ If $< vtag, T_i, T_j >$ is not in the list L_{Ref}. Otherwise, $\mathcal{B}$ retrieves the the referenced tag T_g's secret key x_gP and randomly selects $z_i, w_i \in \mathbb{Z}_q^*$. Then, $\mathcal{B}$ computes*

$$R_i = kbP + z_ikP,\ S_i = w_ix_gP + z_iP,$$

and sets $m_i = (R_i, S_i)$, $\pi_i = (C_i, m_i)$. $\mathcal{B}$ outputs m_i and adds $< T_i, \pi_i, z_i >$ into the list L_S.
- SendReader Query*: Since there is no reply message from the reader, $\mathcal{B}$ ignores the query to this oracle.*
- Result Query*: $\mathcal{A}$ issues the oracle query on input a session π_i. $\mathcal{B}$ outputs 1 if π_i is in the list L_S, otherwise $\mathcal{B}$ outputs 0 if $< R_i, \cdot, C_i, v_i >$ is not in the list L_h. If $< R_i, \cdot, C_i, v_i >$ exists, $\mathcal{B}$ computes $X_i = (\frac{e(P_1, S_i)}{e(R_i, P_2)})^{v_i^{-1}}$ and outputs 1 if X_i appears in $\mathcal{T}$, 0 otherwise.*

Eventually, if the adversary outputs a guess g', where $g' = g$, $\mathcal{B}$ has at least one correct value of r_iY in the list L_h. $\mathcal{B}$ can find the solution of CDH problem as $abP = r_iY - z_iY$, where $z_i \in L_S$. The simulation fails when $\mathcal{B}$ outputs a false rejection with the negligible probability at most $\epsilon + \frac{n}{q}$, where n is the number of tags in $\mathcal{T}$. □

7. Conclusion

In this paper, we demonstrated an attack which is launched by the wide-strong adversary on the Peeters and Hermans' identification protocol. Given a valid session, the adversary can make a new session and distinguish the tag based on the output of the result oracle. We proposed two zero-knowledge based RFID authentication protocols which are wide-strong private. The proposed protocols have been formally proved to be wide-strong private. Moreover, the reader can obtain the tag's signature after a successful tag authentication. The optimized protocol eliminates the modular computations in the prime field.

Acknowledgments
We thank the anonymous reviewers for their fruitful comments of improving this work.

References

[1] Batina, L., Seys, S., Singelée, D., Verbauwhede, I.: Hierarchical ecc-based RFID authentication protocol. In: Juels, A., Paar, C. (eds.) RFIDSec. LNCS, vol. 7055, pp. 183–201. Springer (2011)
[2] Bohli, J.M., Pashalidis, A.: Relations among privacy notions. In: Dingledine, R., Golle, P. (eds.) Financial Cryptography. LNCS, vol. 5628, pp. 362–380. Springer (2009)
[3] Bohli, J.M., Pashalidis, A.: Relations among privacy notions. ACM Trans. Inf. Syst. Secur. 14(1), 4 (2011)
[4] Bringer, J., Chabanne, H., Icart, T.: Cryptanalysis of ec-rac, a RFID identification protocol. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS. LNCS, vol. 5339, pp. 149–161. Springer (2008)
[5] van Deursen, T., Radomirović, S.: Untraceable RFID protocols are not trivially composable: Attacks on the rvision of ec-rac. IACR Cryptology ePrint Archive 2009, 332 (2009)
[6] van Deursen, T., Radomirović, S.: Ec-rac: Enriching a capacious RFID attack collection. In: Yalcin, S.B.O. (ed.) RFIDSec. LNCS, vol. 6370, pp. 75–90. Springer (2010)
[7] van Deursen, T., Radomirović, S.: Insider attacks and privacy of RFID protocols. In: Petkova-Nikova, S., Pashalidis, A., Pernul, G. (eds.) EuroPKI. LNCS, vol. 7163, pp. 91–105. Springer (2011)
[8] Fan, J., Hermans, J., Vercauteren, F.: On the claimed privacy of ec-rac iii. In: Yalcin, S.B.O. (ed.) RFIDSec. LNCS, vol. 6370, pp. 66–74. Springer (2010)
[9] Hein, D.M., Wolkerstorfer, J., Felber, N.: Ecc is ready for RFID - a proof in silicon. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) Selected Areas in Cryptography. LNCS, vol. 5381, pp. 401–413. Springer (2008)
[10] Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B.: A new RFID privacy model. In: Atluri, V., Díaz, C. (eds.) ESORICS. LNCS, vol. 6879, pp. 568–587. Springer (2011)
[11] Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: Maurer, U.M. (ed.) EUROCRYPT. LNCS, vol. 1070, pp. 143–154. Springer (1996)
[12] Lee, Y.K., Batina, L., Verbauwhede, I.: Ec-rac (ecdlp based randomized access control): Provably secure RFID authentication protocol. In: RFID, 2008 IEEE International Conference on. pp. 97 –104 (2008)
[13] Lee, Y.K., Batina, L., Verbauwhede, I.: Untraceable RFID authentication protocols: Revision of ec-rac. In: RFID, 2009 IEEE International Conference on. pp. 178 –185 (2009)
[14] Lee, Y.K., Batina, L., Singelée, D., Verbauwhede, I.: Wide-weak privacy-preserving RFID authentication protocols. In: Chatzimisios, P., Verikoukis, C.V., Santamaría, I., Laddomada, M., Hoffmann, O. (eds.) MOBILIGHT. LNCS, Social Informatics and Telecommunications Engineering, vol. 45, pp. 254–267. Springer (2010)

[15] Lee, Y.K., Sakiyama, K., Batina, L., Verbauwhede, I.: Elliptic-curve-based security processor for RFID. IEEE Trans. Computers 57(11), 1514–1527 (2008)
[16] Ng, C.Y., Susilo, W., Mu, Y., Safavi-Naini, R.: RFID privacy models revisited. In: ESORICS. LNCS, vol. 5283, pp. 251–266. Springer (2008)
[17] Oren, Y., Feldhofer, M.: A low-resource public-key identification scheme for RFID tags and sensor nodes. In: Basin, D.A., Capkun, S., Lee, W. (eds.) WISEC. pp. 59–68. ACM (2009)
[18] Peeters, R., Hermans, J.: Wide strong private RFID identification based on zero-knowledge. IACR Cryptology ePrint Archive 2012, 389 (2012)
[19] Schnorr, C.P.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) CRYPTO. LNCS, vol. 435, pp. 239–252. Springer (1989)
[20] Shamir, A.: SQUASH - a new MAC with provable security properties for highly constrained devices such as RFID tags. In: Nyberg, K. (ed.) FSE. LNCS, vol. 5086, pp. 144–157. Springer (2008)
[21] Tuyls, P., Batina, L.: RFID-tags for anti-counterfeiting. In: Pointcheval, D. (ed.) CT-RSA. LNCS, vol. 3860, pp. 115–131. Springer (2006)
[22] Vaudenay, S.: On privacy models for RFID. In: ASIACRYPT. LNCS, vol. 4833, pp. 68–87. Springer (2007)