A Quadratic Residue-Based Lightweight RFID Mutual Authentication Protocol with Constant-Time Identification

Jingxian Zhou
Information Security Evaluation Center, Civil Aviation University of China, Tianjin 300300, China
Email: jxzhou@aliyun.com

Abstract —Many RFID authentication protocols have been developed in recent years. However, most require the reader to search all tags in the system to identify a single tag. This problem makes the protocols impractical in large-scale RFID deployments. To address this problem, we propose a privacy-preserving mutual authentication protocol for RFID systems with constant-time identification, based on Quadratic Residue. Furthermore, the validity period of each tag is stored in the database so the reader can revoke an expired tag. Formal security proof shows the proposed protocol has no obvious design defects. Compared with existing approaches, the proposed protocol achieves higher efficiency.

Index Terms—Mutual authentication, quadratic residue, privacy, security

I. Introduction

Radio Frequency Identification (RFID) is a technology used for sharing stored information using electronic waves. It already pervades our daily lives: management of the supply chain (attached to goods in retail stores, car tires, etc.), inventory control, farming (tracking animals), ePassports, tracking humans (in prisons for example), etc. [1], RFID offers many benefits to society. However, there have been a number of privacy and security concerns raised regarding the proliferation and standardization of RFID together with real world examples of exploitation of the negative aspects [2], [3]. Consequently, significant efforts have been made to design RFID systems that preserve a tag's privacy. Many RFID authentication protocols have been developed in recent years. However, most of them require the reader to search all tags in the system to identify a single tag. For a large-scale RFID system, the authentication process can take a long time.

To address this issue, a number of private tag authentication protocols have been proposed with structured key management. In these approaches, a unique key and a set of group keys are assigned to each tag. The group keys are shared among several tags and used to confine the search space of the unique key corresponding to a tag's reply. Based on how group keys are managed, they are categorized into two types: tree based [4], [5] and group-based protocols [6], [7]. In a tree-based protocol, tags are mapped to leaf nodes in the tree and keys are assigned to internal nodes. Each tag has its unique key and a set of shared keys associated with the nodes from the leaf to the root. By traveling the tree, the reader can securely simulate tags. This provides high authentication efficiency, but discloses a large amount of information once tags in the system are compromised. On the contrary, in a group-based protocol, each tag has two types of keys: a unique key and a group key. Even if one of the group members is compromised, tags in other groups are intact. However, the authentication efficiency of this approach is low.

In a different approach, Alomair *et al.* [8] proposed a pre-computation strategy to allow constant-time identification. The novelty of this protocol is the architecture of the database and the utilization of off-line computations. However, as their proposed protocol makes use of an internal counter whose value is only known by the tag, it requires very large amounts of data to be pre-computed before a system can be initialized.

Chen *et al.*'s [9] proposed a scheme to achieve constant-time identification based on a quadratic residues assumption for an RFID system. This scheme utilizes direct indexing for each tag's authentication and avoids the brute search. Yeh *et al.* [10] demonstrated the weaknesses of that scheme and proposed an improved scheme to avoid them. Chen *et al.*'s authentication scheme is vulnerable to impersonation attack. Under some conditions, the scheme cannot effectively resist location privacy and replay attacks. Yeh *et al.*'s scheme supplements Chen *et al.*'s scheme by utilizing the number generated by the tags to add in the session between the tags and the server. The solution makes the scheme invulnerable to impersonation attack; however, the proposal lacks formal security and privacy analysis [11].

Furthermore, there are many cases in real life that the expired tags should be revoked. For example, expired foods in supermarket [12], cars with expired insurance [13], etc. Hence, the problem of expired tags should also be considered in any RFID authentication scheme. Even if an attacker were to obtain the information of the tag sometime later, they cannot do anything if the tag is expired, and so revocability could improve security. Therefore, a revocable secure RFID authentication scheme is desirable.

In this paper, we address the private identification problem in large-scale RFID systems, and propose a novel authentication protocol. We do not resort to

Manuscript received November 15, 2014; revised February 28, 2015.
Corresponding author email: jxzhou@aliyun.com.
doi:10.12720/jcm.10.2.117-123

expensive hash functions, nor do we incur more communication overhead. Rather, we utilize quadratic residue that is already available in RFID systems to improve identification efficiency and security. Our proposed protocol achieves authentication of the tag and reader in the RFID system and allows constant-time identification without imposing extra communication or computation overhead on the resource limited tags. The validity period of each tag is stored in the database so an expired tag can be revoked. Through detailed security analysis we show that the proposed collaborative authentication scheme achieves the required security properties of tag anonymity, reader anonymity, reader privacy, and tag untraceability. In addition, it is resistant to replay and impersonation attacks. Compared with existing approaches, our proposed protocol achieves stronger security and higher efficiency.

The outline of the paper is as follows. In section II we describe our system, adversarial, and security models. In section III, we present our proposed protocol. Section IV details the security proofs of the proposed protocol, and its efficiency is discussed in section V. We conclude the paper in Section VI.

II. Model Assumptions

A. System Model

RFID systems are typically composed of three main components: tags, readers, and a backend server. We consider that the backend server and the readers are connected online through a secure channel, and therefore form one unique entity, the reader. The RFID system consists of a larger number of tags and a single reader, as shown in Fig. 1. The tag is assumed to have limited computing power: quadratic residue computations are the most expensive operations tags can perform, whereas the reader is a computationally powerful device with the ability to perform sophisticated cryptographic operations.

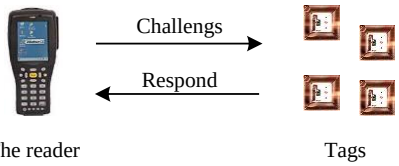

Fig. 1. The system model

B. Adversarial Model [8]

We assume adversaries with complete control over the communication channel. Adversaries can observe all exchanged messages, modify exchanged messages, block exchanged messages, replay them later, and generate messages of their own. We do not consider an adversary whose only goal is to jam the communication channel. Distinguishing tags by the physical fingerprints of their transmissions requires sophisticated devices and cannot be solved using cryptographic solutions. It is out of the scope of this work as in the majority of similar proposals.

Adversary $\mathcal{A}$ is modeled as a polynomial-time algorithm. Given a tag, T, and a reader, R, we assume $\mathcal{A}$ has access to the following oracles:

$Query(T;m_1;x_2;m_3)$: $\mathcal{A}$ sends m_1 as the first message to T; receives a response, x_2; and then sends the message $m_3=f(m_1;x_2)$. This oracle models the adversary's ability to interrogate tags in the system.

$Send(R;x_1;x_2;m_3)$: $\mathcal{A}$ receives x_1 from the reader R; replies with x_2; and receives the reader's response $m_3=f(x_1;x_2)$. This oracle models the adversary's ability to act as a tag in the system.

$Execute(T;R)$: The tag, T, and the reader, R, execute an instance of the protocol. $\mathcal{A}$ eavesdrops on the channel, and can also tamper with the messages exchanged between T and R. This oracle models the adversary's ability to actively monitor the channel between tag and reader.

$Block(\mathcal{A})$: $\mathcal{A}$ blocks any part of the protocol. This oracle models the adversary's ability to launch a denial of service attack.

$Reveal(T)$: Exposes the tags' secret parameters to $\mathcal{A}$. This oracle simulates the adversary's ability to physically capture the tag and obtain its secret information.

$\mathcal{A}$ can call the oracles *Query*, *Send*, *Execute*, and *Block* any polynomial number of times. The *Reveal* oracle can be called only once (on the same tag), after which the tag is considered compromised and, thus, there is no point calling the *Reveal* oracle on the same tag multiple times. To model tag compromise attacks, however, the adversary is allowed to call other oracles after the Reveal oracle on the same tag.

C. Security Model

The security model presented in this section does not consider the adversary's ability to perform pre-processing before engaging. In Section 4, however, we modify the security model to allow the adversary to perform pre-processing that involves calling the Reveal oracle on tags in the system. The main purpose of this modification is to allow modeling tag compromise attacks.

The two main security goals of our protocol are tag privacy and tag-reader mutual authentication. Privacy is measured by the adversary's ability to trace tags by means of their responses in different protocol runs. We define notions of untraceability [8].

Definition 1 (*Untraceability*) *In an RFID system, tags are said to be untraceable if an adversary cannot track a tag based on information gained before the tag's last authentication with a valid reader. In other words, there is no correlation between a tag's responses before and after completing a protocol run with a valid reader.*

Untraceability is modeled by the following game between the challenger, $\mathcal{C}$, (an RFID system) and a polynomial time adversary, $\mathcal{A}$.

1) $\mathcal{C}$ selects two tags, T_0 and T_1, and a valid reader, R.

2) $\mathcal{A}$ makes queries on T_0, T_1, and R using the *Query*, *Send*, *Execute* and *Block* oracles for a number of times of its choice.

3) $\mathcal{A}$ stops calling the oracles and notifies $\mathcal{C}$.

4) $\mathcal{C}$ carries out an instance of the protocol with T_0 and T_1, during which mutual authentication of both tags with R is achieved.

5) $\mathcal{C}$ selects a random bit, b, and sets $T = T_b$.

6) $\mathcal{A}$ makes queries of T and R using the *Query*, *Send*, *Execute* and *Block* oracles.

7) $\mathcal{A}$ outputs a bit, b_0, and wins the game if $b_0 = b$.

To quantify the adversary's ability to trace RFID tags, we define the adversary's advantage of successfully identifying the tag in the previous games as:

$$Adv_{\mathcal{A}} = 2(Pr[b' = b] - \frac{1}{2}) \quad (1)$$

If the adversary cannot do better than a random guess, then $Pr[b' = b] = 1/2$. Consequently, the adversary's advantage, $Adv_{\mathcal{A}}$, is zero, at which point we consider that the tags are untraceable.

The other security goal of our protocol is mutual authentication. An honest protocol run is defined as: A mutual authentication protocol run in the symmetric key setup is said to be honest if the parties involved in the protocol run use their shared key to exchange messages, and the messages exchanged in the protocol run have been relayed faithfully (without modification).

We use the formal definition of secure mutual authentication for RFID systems as appeared in [14].

Definition 2 (*Secure Mutual Authentication*): A mutual authentication protocol for RFID systems is said to be secure if and only if it satisfies all the following conditions:

- No information about the secret parameters of an RFID tag is revealed by messages exchanged in protocol runs.
- Authentication $\Rightarrow$ Honest protocol: the probability of authentication when the protocol run is not honest is negligible in the security parameter.
- Honest protocol $\Rightarrow$ Authentication: if the protocol run is honest, the tag-reader pair must authenticate each other with probability one.

To model the adversary's attempt to authenticate itself to a reader (tag), we propose the following game between the challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

1) $\mathcal{C}$ chooses a tag, T, at random, and a reader, R.

2) $\mathcal{A}$ calls the oracles *Query*, *Send*, *Execute* and *Block* using T and R for a number of times of its choice.

3) $\mathcal{A}$ decides to stop and notifies $\mathcal{C}$.

4) $\mathcal{A}$ calls the oracle *Send*(*Query*) to impersonate a tag (reader) in the system.

5) If $\mathcal{A}$ is authenticated as a valid tag (reader), $\mathcal{A}$ wins the game.

Definition 2 implies that the protocol achieves secure mutual authentication only if the adversary's probability of winning the previous game is negligible.

III. The Proposed Protocol

We propose an approach based on the quadratic residue property that can achieve the security requirements of current and emerging RFID systems/applications. Our protocol follows the challenge-response model, but the fixed information of the tag is protected using the quadratic residue function. Timestamps generated by the reader and the tag are concatenated with the *ID* to distinguish the authentication information for each session, preventing a replay attack. The validity period of each tag is also stored in the database.

A. The Quadratic Residue Theorem

If N is a positive integer, then Q is said to be the quadratic residue of N if $(N,Q) = 1$, and the congruence $x^2 \equiv Q \bmod N$ has a solution. Suppose that $N = pq$ where p and q are distinct large primes and that the congruence has a solution $x = x_0$. From the Chinese Remainder Theorem [15] there are exactly four incongruent solutions of the congruence (i.e., Q has four incongruent square roots modulo N). However, to calculate these solutions, knowledge of p and q is required. Due to the difficulty of factoring N, it is computationally infeasible to find x satisfying $x^2 \equiv Q \bmod N$ without knowing p and q [9], [16].

B. Initialization

The symbols we use are as follows:

N : The product of two large primes p and q, $N = pq$.

t, v : Random numbers generated by the tag.

l : The length of a random number.

ID_T : The identifier of a tag.

ID_R : The identifier of a reader.

$\oplus$: Exclusive-or operation.

$\overline{ID_R}$: The multiplicative inverse of ID_R, where $ID_R.\overline{ID_R} \bmod N = 1$.

R_{time} : The timestamp generated by the reader and transmitted to the tag.

$T_{time-new}$: The timestamp generated by the tag and transmitted to the reader.

$T_{time-old}$: The timestamp pre-generated in the tag.

Each tag records ID_T, N, $R_{ID} \equiv ID_R^2 \bmod N$, and $T_{time-old}$, and contains a timestamp generator, which

generates a timestamp, $T_{time-new}$, for each session. The tag stores $T_{time-new}$ by updating $T_{time-old}$ after every successful authentication.

The reader also generates timestamp R_{time} on each session. The reader stores $p, q, \overline{ID_R}, (ID_T, v_{time})$, where v_{time} is the validity time of tag ID_T.

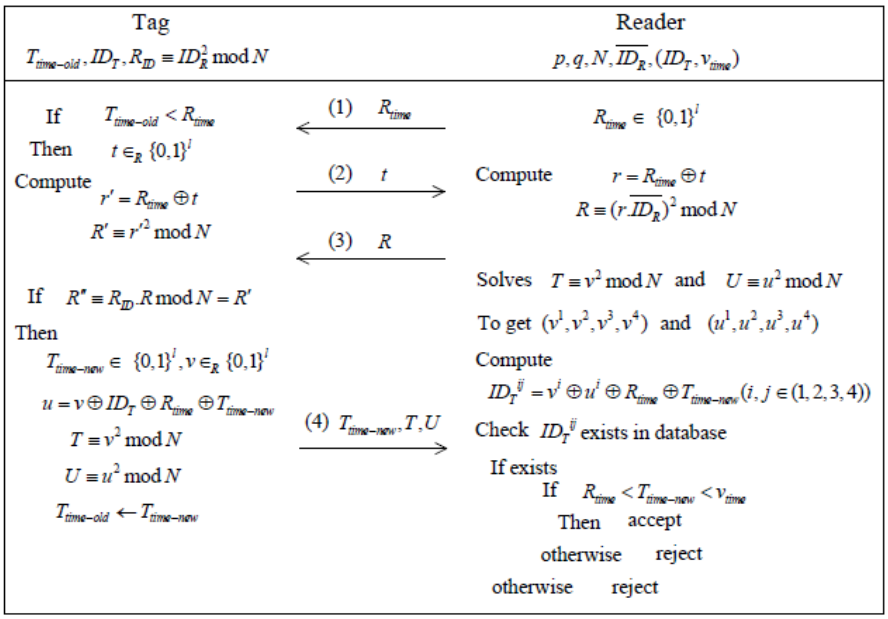

Fig. 2. The authentication process of the proposed protocol.

C. The Authentication Process

The authentication process of our proposed protocol is shown in Fig. 2.

1) The reader sends a query: The reader generates a timestamp, R_{time}, and that as a query to the tag.

2) The tag responds to the query: After the tag receives R_{time}, if $T_{time-old} < R_{time}$, it generates a random number $t \in_R \{0,1\}^l$ and sends t to the reader.

3) The reader transmits its authentication: After the reader receives t from the tag, it computes $r = R_{time} \oplus t$, $R \equiv (r.\overline{ID_R})^2 \bmod N$, and sends R to the tag.

4) Authentication of the tag: After the tag receives the information from the reader, the tag calculates $r' = R_{time} \oplus t$, $R' \equiv r^2 \bmod N$, $R'' \equiv R_{ID}.R \bmod N$. If $R'' = R'$, the authentication is successful, and the tag considers that the reader is legal.

The tag then generates a random number v, timestamp $T_{time-new}$, and calculates $T \equiv v^2 \bmod N$, $u = v \oplus ID_T \oplus R_{time} \oplus T_{time-new}$. It sends $T_{time-new}, T, U$ to the reader and updates $T_{time-old}$ as $T_{time-new}$.

5) Reader authenticates the tag. After receiving $T_{time-new}, T, U$, the reader uses T, U and the secret p, q to get the four possible v values, (v^1, v^2, v^3, v^4), and the four possible u values (u^1, u^2, u^3, u^4). It calculates $ID_T^{ij} = v^i \oplus u^j \oplus R_{time} \oplus T_{time-new}$, where $i, j \in \{1,2,3,4\}$, and checks if the tag ID_T^{ij} is in the sorted table.

If ID_T^{ij} is in the table and $R_{time} < T_{time-new} < v_{time}$, the authentication is successful, and the reader considers that the tag is legal.

On the other hand, If ID_T^{ij} cannot be found, and/or $T_{time-new} < R_{time}$, the reader concludes the tag is not legal and ignores the message.

If ID_T^{ij} is in the table, but $T_{time-new} > v_{time}$, the reader concludes the tag has expired and ignores the message.

IV. Protocol Security

We prove that our proposed protocol preserves the integrity of the tag and reader while maintaining user privacy.

Lemma 1: *In the proposed protocol, the identifier, ID_T, of a tag cannot be exposed without calling the Reveal oracle.*

Proof: In our proposed protocol, only the parameters $R_{time}, t, R, T_{time-new}, T, U$ are transmitted between the reader and the tag. The tag's identification information is wrapped into U, which can be viewed as an encryption of ID_T with the key N using the quadratic residue modulo function, and cannot be solved in polynomial time given the difficulty of factoring N.

On the other hand, an adversary, $\mathcal{A}$, can launch the *Query*, *Send*, *Execute* and *Block* oracles on the reader and the tag any number of times to obtain a set of public parameters.

Without loss of generality, assume two parameters, U_1 and U_2. Since these are generated using both a random number and the quadratic residue modulo function, they cannot be correlated with a non-negligible probability.

Therefore, unless $\mathcal{A}$ calls the *Reveal* oracle, no identifier information about a tag can be revealed.

Theorem 1: *In the proposed protocol, tags are untraceable.*

Proof: Assume challenger $\mathcal{C}$ has chosen two tags, T_0 and T_1, and a reader R. Adversary $\mathcal{A}$ calls the *Query*, *Send*, *Execute* and *Block* oracles on T_0, T_1, and R a number of times of its choice. $\mathcal{A}$ records all the outputs of the oracle calls and notifies $\mathcal{C}$.

$\mathcal{C}$ chooses a bit, b, uniformly random and sets $T = T_b$. From Lemma 1, $\mathcal{A}$ cannot infer the identifier value of the tag. $\mathcal{A}$ now calls the oracles *Query*, *Send*, *Execute*, *Block* and outputs a bit b'. Since $\mathcal{A}$ does not know the tag's identifier value, the probability that $Pr(b=b')$ will be greater than $1/2$ is negligible.

Therefore, the adversary's advantage, $Adv_{\mathcal{A}}^{trace}$, to identify the tag chosen by $\mathcal{C}$ is negligible.

Theorem 2: *The proposed protocol produces secure mutual authentication.*

Proof: Assume that $\mathcal{C}$ has given $\mathcal{A}$ a tag T and a reader R. $\mathcal{A}$ has called the *Query*, *Send*, *Execute*, and *Block* oracles a number of times of its choice, and recorded the outputs.

The first condition of Definition 2 of a secure mutual authentication is satisfied by Lemma 1.

$\mathcal{A}$ attempts to impersonate the reader, R, by sending R_{time} to the tag and receives a random number t. Since, $\mathcal{A}$ cannot infer the secret parameters, $\overline{ID_R}$, the probability of coming up with a response $r = R_{time} \oplus t$, $R \equiv (r.\overline{ID_R})^2 \bmod N$ that will be validated is negligible. Therefore, the probability of impersonating an authorized reader in the system is negligible.

On the other hand, assume that $\mathcal{A}$ attempts to impersonate the tag T. $\mathcal{A}$ must authentication itself to the reader with a response $T_{time-new}$, $T \equiv v^2 \bmod N$, $U \equiv u^2 \bmod N$, where $u = v \oplus ID_T \oplus R_{time} \oplus T_{time-new}$. Since ID_T and v remain secret, by Lemma 1, $\mathcal{A}$ can be successful with only a negligible probability. Consequently, the probability of impersonating a tag in the system is negligible.

Therefore, the probability of mutual authentication when the protocol is not honest is negligible and, hence, the second condition of Definition 2 of secure mutual authentication is satisfied.

Assume that the reader is valid, and property follows the protocol. The tag $r' = R_{time} \oplus t$, $R' \equiv r'^2 \bmod N$, $R'' \equiv R_{ID}.R \bmod N$, if $R' = R''$, the tag considers that the reader is legal. Since they are equal, only if the reader has the proper secret value R_{ID}. Similarly, if the tag is valid, and property follows the protocol, it will be always accepted. Since ID_T remain secret, by Lemma 1. Therefore, if the protocol run is honest, mutual authentication will be achieved with probability one and, consequently, the third condition of Definition 2 of secure mutual authentication is satisfied.

Hence, the conditions of Definition 2 of secure mutual authentication are satisfied. Thus, $Adv_{\mathcal{A}}^{auth}$ is negligible and the proposed protocol is shown to provide secure mutual authentication.

Theorem 3 *The proposed protocol is secure against tag compromise attacks.*

Proof The adversarial model of section II can be modified to capture the tag compromise attack. Let an adversary calling the *Reveal*(T) oracle, thus capturing the tag T, have the ability to perform multiple protocol runs with the system.

Each tag in the proposed protocol has one pieces of secret information, its identify value. Since a tag's identity value is designed to be statistically independent for different tags, compromising some tags in the system does not affect the security of other, uncompromised tags.

Furthermore, an adversary, can compromise a tag in the system and attempt to harvest a valid reader's identify value ID_R by performing multiple protocol runs with the reader. The reader's identification information is wrapping into R_{ID} and R using the quadratic residue modulo function, respectively. It is impossible that obtain ID_R any information from R_{ID} and R. However, $\mathcal{A}$ is incapable of breaking the privacy of the reader using the data of the compromised tag.

Therefore, the compromise of a tag has no practical significance.

V. Protocol Efficiency

Processing capability is limited in RFID systems, so any RFID authentication scheme should ensure not only security but also low computational cost. With the rapidly advancing techniques of the RFID tags, how to assure high efficiency for authentication and searching for the tag in the database has become a key issue. We analyze the efficiency of our protocol by evaluating the computational cost in the tag and the reader.

For an RFID system and the associated authentication protocols, let T_H, T_{OR}, T_S, T_R be the number of quadratic residue, square root derivation, hash, and random number or timestamp generation operations, respectively.

For our proposed protocol, the tag computational load (see Fig. 2) is four quadratic residue: $R' \equiv r'^2 \bmod N$, $R'' \equiv R_{ID}.R \bmod N$, $T \equiv v^2 \bmod N$, and $U \equiv u^2 \bmod N$, and three number generating operations: $t, v, T_{time-new}$. The computational load in the reader is one quadratic residue,

$R \equiv (r.\overline{ID_R})^2 \bmod N$, one number generating, R_{time} , and two square root deriving operations.

TABLE I: DIFFERENT AUTHENTICATION PROTOCOLS WITH CONSTANT-TIME IDENTIFICATION

Protocols	Rounds	Database	Reader	Tag
Alomair *et al*. [8]	5	-		$5T_H$
Yeh *et al*. [9]	5	$14T_H, 3T_S, T_R$	T_R	$4T_H, 3T_{OR}, 2T_R$
Kardas *et al*. [11]	3	-	$2T_H, 2T_S, T_R$	$2T_H, 2T_{OR}, T_R$
Fan *et al.* [13]	5	$3T_H$	T_R	
Our protocol	4	-	$4T_{OR}, 3T_R$	$T_{OR}, 2T_S, T_R$

We compare the performance of our protocols with other schemes in Table I. For those schemes proposed by Alomair *et al*. [8], Yeh *et al*. [9], Kardas *et al*. [11], and Fan *et al*. [13], the channel between the reader and the server is assumed to be secure. Hence, there is no reader-server authentication in those schemes, and tags are required to implement hash functions. Note that implementing hash functions on passive RFID tags is an open research problem [17] and does not conform to EPC standards [18]. However, even the most efficient hash function will cost approximately 1.7*k* gates [19] to implement. While Yeh's scheme [9] can achieve a complexity of $\mathcal{O}(1)$, for example, the tag and the server are required to compute 4 and 14 hash values respectively. On the other hand, our proposed protocol does not require hash functions to be implemented by either the tag or the reader.

Therefore, our protocol is more suitable for implementation on low-cost passive RFID tag.

VI. CONCLUSIONS

We proposed a protocol that enables the private identification of tags in the system with constant-time complexity based quadratic residue, and thereby addresses the problem of individual tag identification in large-scale RFID systems. By utilizing a timestamp in the system, our proposed protocol also provides revocability. Importantly, our proposed protocol is suits the computational constraints of low-cost passive RFID tags as it uses only passive RFID tag capabilities of modular squaring and *XOR* functions, and does not require implementation of hash functions on tags or readers. Future work will focus on a practical demonstration of the proposed protocol.

ACKNOWLEDGMENT

This work was supported by the National Nature Science Foundation of China (Grant No. 61303232), the Project of Civil aviation science and technology (Grant No. MHRD20140205)，the fundamental research funds for the central universities (Grant No.3122013C004), and the scientific research foundation of CAUC (Grant No. 2013QD24X).

REFERENCES

[1] J. Leung, W. Cheung, and S. C Chu, "Aligning RFID applications with supply chain strategies," *Information & Management*, vol. 51, no. 2, pp. 260-269, 2014.

[2] Y. Hou and J. Ma. "Study on security analysis of RFID," *Intelligent Data analysis and its Applications*, pp. 175-180, 2014.

[3] J. X Zhou, Y. J Zhou, F. Xiao, and X. X. Niu, "Mutual authentication protocol for mobile RFID systems," *Journal of Computational Information Systems*, vol. 8, no. 8, pp. 3261-3268, 2012.

[4] Q. Yao, Q. Qi, J. Han, J. Zhao, X. Li, and Y. Liu, "Randomized RFID private authentication," in *Proc. Pervasive Computing and Communications Conf*., 2009, pp. 1-10.

[5] T. Li, W. Luo, Z. Mo, and S. Chen, "Privacy-preserving RFID authentication based on cryptographical encoding," in *Proc. Infocom Conf*., 2012, pp. 2174-2182.

[6] G. Avoine, L. Buttyan, T. Holczer, and I. Vajda, "Group-based private authentication," in *Proc. WoWMoM Conf*., 2007, pp. 1-6.

[7] M. E. Hoque, F. Rahman, and S. I. Ahamed, "AnonPri: An efficient anonymous private authentication protocol," in *Proc. PerCom Conf*., 2011, pp. 102-110.

[8] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Scalable RFID systems: A privacy-preserving protocol with constant-time identification," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1536-1550, 2012.

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

[10] T. C. Yeh, C. H. Wu, and Y. M. Tseng, "Improvement of the RFID authentication scheme based on quadratic residues," *Computer Communications*, vol. 34, no. 3, pp. 337-341, 2011.

[11] S. Kardas, S. Celik, M. Sariyuce, and A. Levi, "An efficient and private authentication protocol for RFID systems," *Journal of Communications Software and Systems*, vol. 9, no. 2, pp. 128-136, 2013.

[12] Y. J Zuo, "Secure and private search protocols for RFID system," *Information System Front*, vol. 12, no. 5, pp. 507-519, 2010.

[13] K. Fan, J. Li, X. H Liang, X. S Shen, and Y. Yang, "RSEL: Revocable secure efficient lightweight RFID authentication scheme," *Concurrency and Computation: Practice and Experience*, vol. 26, pp. 1084-1096, 2014.

[14] B. Alomair, L. Lazos, and R. Poovendran, "Securing low-cost RFID systems: An unconditionally secure approach," *Journal of Computer Security*, vol. 19, no. 2, pp. 229-257, 2011.

[15] T. Van and C. A. Henk, "Chinese remainder theorem," *Encyclopedia of Cryptography and Security*, pp. 201-202, 2011.

[16] R. Doss, W. L Zhou, and S. Yu, "Secure RFID tag ownership transfer based on quadratic residues," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 390-401, 2013.

[17] J. S. Cho, S. S. Yeo and S. K. Kim, "Securing against brute-force attack: a hash based RFID mutual authentication protocol using a secret value," *Computer Communications*, vol. 34, no. 3, pp. 391-397, 2011.

[18] A. Juels, "Yoking-proofs for RFID tags," in *Proc. Second IEEE Annual Conf*., 2004, pp. 138-143.

[19] N. Lo, K. H. Yeh and C. Y. Yeun, "New mutual agreement protocol to secure mobile RFID-enabled devices," *Information Security Technical Report*, vol. 13, pp. 151-157, 2008.

Jingxian Zhou was born in Henan Province, China, in 1981. He received the M.S. degree in Department of Mathematics from Zhengzhou University, in 2010 and the PH. D. degree from Beijing University of Posts and Telecommunications, in 2013. Now, he works at Information Security Evaluation Center, Civil Aviation University of China. His research interests are security authentication protocol in RFID air interface and wireless sensor networks, and security architecture for the Internet of Things.