A Lightweight RFID Security Protocol Based on Elliptic Curve Cryptography

Quan Qian, Yan-Long Jia, Rui Zhang

(Corresponding author: Quan Qian)

School of Computer Engineering & Science, Shanghai University
99 Shangda Rd., Baoshan District, Shanghai, China
(Email: qqian@shu.edu.cn)

(Received Nov. 12, 2013; revised and accepted Mar. 13 & Nov. 6, 2014)

Abstract

Radio Frequency Identification (RFID) is a promising new technology that is widely deployed for object tracking and monitoring, ticketing, supply-chain management, contactless payment, etc. However, RFID related security problems attract more and more attentions. This paper has studied a novel elliptic curve cryptography (ECC) based RFID security protocol and it shows some great features. Firstly, the high strength of ECC encryption provides convincing security for communication and tag memory data access. Secondly, the public-key cryptography used in the protocol reduces the key storage requirement and the backend system just store the private key. Thirdly, the new protocol just depends on simple calculations, such as XOR, bitwise AND, and so forth, which reduce the tag computation. Finally, the computational performance, security features, and the formal proof based on BAN logic are also discussed in detail in the paper.

Keywords: BAN logic, elliptic curve cryptography, RFID security protocol

1 Introduction

Internet of Things (IoT) refers to uniquely identifiable objects and their virtual representations in an Internet-like structure [30]. In IoT, each kind of sensor equipment, such as RFID (Radio-frequency identification), barcodes, two-dimension code, QR codes, GPS, etc. can integrate with Internet to get a huge network. Among them, RFID was seen as a prerequisite for the Internet of Things. If all objects and people in daily life were equipped with identifiers, they could be managed and interacted effectively. IoT has been regarded as the another technological revolution after Internet. For instance, the Intelligent Earth, Sensing China, U-Japan, IT839 of Korea has been pushed the IoT to a unprecedented level whether in application or research field [4]. However, with the fast development of IoT, the security issues have brought some negative influence, which has attracted the industry or scientific research to this hot area. Among them, the RFID security is the at the top list of primary concerns and RFID systems must need severval security requirements [7, 19, 32]. So far, there are some research results in this area.

Sarma proposed a Hash-lock RFID security protocol, which has been the basis for research on challenge-response hash encryption based RFID protocols [23, 24]. [27] is another hash function based mutual authentication protocol. Lin presented a random sequence based RFID protocol, which use hash function and random sequences to guarantee the freshness of the authentication message [13]. But to some extent, the security strength largely depends on the random sequence length. And because of the cost limit of tag, the sequence length is not very long, which limits the security. Molnar proposed a David Library RFID protocol [17]. Although this protocol has almost no security vulnerability in design, but it requires the tag has the function of generating random numbers, which limits the protocol use in low cost tags. Wu et al. improved the digital library RFID security protocol, and changed the security assumptions of the original protocol which can be compatible with the original one but resists new attacks [31]. Some light weight and low cost RFID authentications are provided in [18, 20, 29]. Similar to [1], the protocol's security heavily relies on the synchronous update between the back end database and the tag. Once there occurs abnormal in authentication (e.g. power interruption), the information will appear not synchronous, resulting in the tag not available. Moreover, the protocol is too computation complicated, facing challenges in terms of reliability. Khan and Moessner use a light weight computation and the protocol provide the synchronization and security by timestamp [10]. The main feature of the protocol lies in the back end database, which use a special Key-Class data structure, can find the target ID efficiently. But the protocol also has some disadvantages. Firstly, the mutual authentication is not too ideal. Secondly, the tag should not only generate random number, but also save a certain amount of privacy data, which make it not applicable for low cost tags. Khedr proposed an authentication scheme for passive RFID tags combining a random key scheme with a strong cryptography [11]. And Wei et al. provided a improved authentication protocol for mobile agent device for RFID privacy protection [28]. Sun et al presents a RFID protocol based on cryptographic hash function, which mainly focuses on preventing an attacker tracking a target tag by observing unsuccessful previous session, that is the forward privacy service [26]. Moreover, the proposed RFID protocol is evaluated according to both the privacy attribute and the implementation performance.

Concerning about the ECC based RFID protocols, Martinez focuses on the protocol's scalability [15]. The protocol combines ECC and zero knowledge authentication, and the forward security is quite reliable. Martinez proposed an elliptic curve and zero knowledge based forward secure RFID protocol [14], which can resist some common attacks, but there is a higher demand on tag computation ability. [9] also make use of ECC, but the key synchronization policy is not perfect. Besides that, the protocol, similar to [15], requires the tag to generate the random key and can do scalar multiplication. Batina et al. put forward a public-key cryptography for RFID tags [5], which provides online and offline, the two ways of authentication. However, at the online phase, the tag use plaintext communication and at the offline phase, the tag need to do some complicated computations. It is not suitable for those low cost tags. Kumar et al introduce some implementation details of ECC hardware and discuss the performance factors on the chip size, memory and computation time [12]. Babaheidarian et al analyze the ECC-based RFID authentication protocols known as EC-RAC [3]. It mainly focuses on the reasons why some versions of EC-RAC protocols are exposed to privacy and/or security threats.

As mentioned above, some research have been conducted in RFID security protocols, as space limited we cannot described them one by one. In this paper, we propose an ECC based RFID security protocol. The contributions of the protocol are: (1) all sensitive information are encrypted by ECC, which ensure the confidentiality of transmitted information. (2) The computations involved are not too complicated that can been applied to low cost tags. (3) Due to the random number generated by the reader constantly updated, the corresponding authentication messages change continuously, which increase the difficulties for adversaries to decode them.

The organization of the paper are as follows. Section 2 presents the main idea of our ECC based RFID security protocol, including the protocol description and authentication process. Section 3 discusses the correctness from the points of tag and reader authentications. The protocol security will be discussed in section 4 and the formal proof with BAN logic in Section 5. Finally, the Section 6 gives a conclusion and the future work.

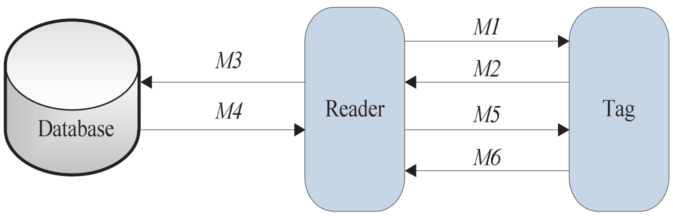

Figure 1: An ECC based RFID secure protocol model. Here, $M1 : \{Query, R\}$; $M2 : \{ECC(M(id)) + R, P_t + R\}$; $M3 : \{ECC(M(id)) + R, P_t + R, R\}$; $M4 : \{H(id) \oplus K_x, (K_x + R_x) \oplus H(id^{'})\}$; $M5 : \{H(id) \oplus K_x, (K_x + R_x) \oplus H(id^{'})\}$; $M6 : \{ECC(M(data)) + R, P_t + R\}$.

2 ECC-based RFID Security Protocol

Generally speaking, the designing goal of RFID security protocol is to implement the authentication and secure communication, which includes ensuring the integrity, confidentiality and security of the user secret information. At the same time, the protocol itself can resist the adversary sniffing, deleting, tampering or other malicious operation on the tag data. In addition, the protocol can resist the RFID common attacks, such as replaying, location tracking, denial of service, etc. The procedure of our protocol is illustrated in Figure 1.

In Figure 1, there are six messages interacted among three participants, the tag, reader and the backend database. Among different messages, $P_s = n * G$, P_s is the database public key and n is the database private key. Similarly, in $P_t = t * G$, t is the tag's private key, and P_t is the tag's public key. In $K = r * G$, r is the database temporary communication key, and K is the temporary public key. K_x, R_x is the x-coordinate of point K and R on ecliptic curve.

Furthermore, in Figure 1, $M(x)$ refers to encode information x to a point on ecliptic curve. $ECC(m) = m + r \times P$, where r is the private key of sender, m the message to be sent, P the public key of the receiver. The backend database need to choose a private key n ($n < m$, n is a big integer) and to create the public key $P = n \times G$. The sensitive date of tag, for instance, the tag ID and the privacy data, are encoded to a point (x, y) on the ecliptic curve.

2.1 Protocol Description

ECC is an approach to public-key cryptography based on algebraic structure of elliptic curves over finite fields. For current cryptographic purposes, suppose choosing a ecliptic curve in the finite field F_q, any point in F_q, $(x, y) \in F_q * F_q$ must satisfy the following equation:

$$y^2 \equiv x^3 + ax + b(mod\, q)$$

where, the elliptic curve group is made up of non-negative integer solutions P less than q, $P = (x, y)$ and infinite point 0. a and b are constants that satisfy $4a^3 + 27b^2 \neq 0(mod\, q)$ and $F_q(q > 3)$. To choose a base point $G = (x, y)$ in $E_q(a, b)$, and this base point satisfy the condition that exists a minimum positive integer m (m is a big prime number), let $mG = O_\infty$(m is regarded as the $G's$ order).

In our protocol, hash function is very important, where some lightweight algorithms can be used [2, 25]. SQUASH is a quite simple hash method [25], and it has great encryption performance without random number creation. In addition, the security of SQUASH is almost equal to public-key approach. The QUARK [2], is another lightweight encryption scheme, also can be used for message authentication, stream encryption, with great identification, anti-collision and security.

2.2 Procedure of Protocol Authentication

1) Authentication Request. First of all, the reader starts a authentication request and sends a **Query** and a random number R to the tag. And the R is a point coordinate in the elliptic curve.

2) The Tag Authentication. Once the tag has received the reader's authentication request, it sends $M_0 = \{ECC(M(id)) + R, P_t + R\}$ to the reader, where $ECC(M(id)) = id + t \times P_t$, and t is the private key of the tag. When the reader has received $M2$, forwards $M2$ and sends its own random number R to the backend database at the same time.

When the database has received $M3$, computes $ID = M_0 - R - n \times P_t$, and then searches the database's index table to determine whether there exists $id^{'} = ID$. If it finds successfully, the tag authentication succeeds. Otherwise, the tag authentication fails and the database keeps silence.

3) The Reader Authentication. Once the tag has authenticated successfully, the database creates the random key $r(2 \leq r \leq n)$, and gets the temporary public key $K = r \times G$. Using the point K and R's x coordinate K_x and R_x, the tag sends the server's id. After that, the database, using its saved tag's $id^{'}$, computes $H(id) \oplus K_x, (K_x + R_x) \oplus H(id^{'})$, and then sends M4 to the reader.

After the reader receiving M4, sends M5 to the tag. Once the tag receive M5, computes the result according to the tag's $H(id)$, R and the data in M5. If the M4 is expressed as M1 and M2, where $M1 = H(id) \oplus K_x$ and $M2 = (K_x + R_x) \oplus H(id^{'})$, then we can get $H(id^{'}) = (H(id) \oplus M1 + R_x) \oplus M2$. At the same time, if $H(id^{'}) = H(id)$, then the reader authenticated successfully; otherwise, unsuccessfully. And if the authentication fails, the tag keep silence.

4) The Data Transmission. When the reader is authenticated successfully, the tag send M6 to the reader. $M6 = \{ECC(M(data)) + R, P_t + R\}$ and $ECC(M(data)) = data + t \times P_t$ (t is the tag private key). After that, the tag clear R from its memory. Once the reader receives M6, calculates $Data = M3 - R - n \times P_t$, and $Data$ is the confidential information that the tag will send. As $Data$ has been encoded as a point in the elliptic curve, so we can verify its correctness by computing whether it is really on the curve.

3 The Protocol Correctness Verification

3.1 Verification for Tag Authentication

When tag has received $M2$, does pre-judgment, only those messages being accordance with the predefined criteria, can be sent to the database. First of all, the reader receives $M3$, and then determines whether the tag information has been saved in the database.

The known facts are the database has been saved the private key n and tags' ID list $ID_1, ID_2, ..., ID_n$. The database receives the message sent by a reader, which contains $M^{'} = ECC(M(id)) + R, P_t + R, R$. From $M^{'}$, we can get R,P_t,and $m^{'} = ECC(M(id)) + R$. Moreover, we can get $ECC(M(id)) = m^{'} - R$, and $ID = ECC(M(id)) - n \times P_t$.

Using the ID to search in the ID list $ID_1, ID_2, ..., ID_n$ from the database, if finds successfully, then it says the validity of the tag and the authentication is successfully; otherwise, fails.

3.2 Verification for Reader Authentication

As mentioned above, supposing we have a secure communication between the reader and the backend database, for instance, a secure wired communication. And the backend database saves each tag's ID. When the tag has received $M5$, depending on its own saved related information, the tag verifies the reader's validity. Supposing the tag has received $M5$ and got $H(id)$ and R_x. Given $m_1 = H(id) \otimes K_x$ and $m_2 = (K_x + R_x) \otimes H_{id'}$, then we can get: $K_x^{'} = m_1 \otimes H(id)$, then: $H_{id'} = (K_x^{'} + R_x) \otimes m_2$.

So, if $H(id^{'}) = H(id)$, then it indicates the reader's validity. The reason is only the valid reader has the correct $H(id^{'})$. And if $H(id^{'}) \neq H(id)$, then the reader's authentication fails.

4 The Protocol Security Verification

1) Tag Authentication and Reader Authorized Access. Through the above analysis, it shows that the tag's validity can be verified uniquely by its ID. Meanwhile, the reader's validity can be verified through the correctness of $H(id^{'})$, which guarantees the reader's authorized access to the tag.

2) Tag Anonymity. In the above protocol, the confidential information, for instance, the tag's ID and data, are not transmitted in plaintext. All of the sensitive data are encrypted by ECC, e.g. $ECC(M(id))$ and $ECC(M(data))$. So, even the adversary sniffed the secret information, it is very difficult to decipher them, that is, the tag anonymity.

3) The Backward Security. A major security concern in every cryptosystem is the protection of secret information from exposure. In general, the backward security is designed to prevent the compromise of a long-term secret key from affecting the confidentiality of future conversations.

The RFID backward security is what the adversary got the secret information at time $t1$ cannot be used for future $t2$ authentication, which can prevent the replay attack. In order to satisfy the backward security, it should require the secret information are changing each time, furthermore, the information after changed cannot be deduced by the previous ones. In our protocol, we embedded random number R in authentication, which can ensure the freshness and backward security. The detailed proof are as follows.

Supposing at time t_1, the tag sent message $M_{t_1-1} = ECC(M(id)) + R_1$, $M_{t_1-2} = P_t + R_1$. At time t_2, the random number in the reader is R_2. When the data of t_1 has been transferred to the database, then $P_t^{'} = M_{t_1-2} - R_2$. As R_1 and R_2 are random numbers, there are very low probability that the two are equal. So, the low equal probability is for $P_t, P_t^{'}$. In other words, we cannot solve the tag's ID by P_t and $P_t^{'}$, and the authentication fails.

4) The Forward Security. Similar to the backward security, the forward security for RFID security that is to say, even if the adversary acquires the current state t_2, he/she cannot create any relationships between t_2 and any past state t_2, which can prevent the malicious tracking or tag privacy leakage.

In our mentioned protocol, all the messages in authentication have utilized random number R or variant of R, which ensure the freshness of each message and can protect the privacy as a result.

5 The Protocol Formal Analysis

Security protocol generally refers to a sequence of operations that ensure providing secure delivery of data between different communication parties. Security protocols must achieve certain goals when an arbitrary number of sessions are executed concurrently or an adversary may use information acquired in one session to compromise the security of another. Since security protocols form the basis of modern secure networked systems, it is important to develop formal, accurate and applicable methods for finding errors and proving that the target protocols meet their expected security requirements. In order to guide the security protocol designing and debugging, to discover the security flaws as soon as possible, the formal verification method is regarded as an effective way. Currently, there are three kinds of formal methods: modal logic of knowledge and belief, theorem proof, and process calculus [22, 8, 33]. Next, we will use BAN, a kind of logical method, to prove that our proposed protocol is correct.

5.1 The BAN Logic

The BAN (named after its inventors Burrows, Abadi, and Needham) logic is a modal logic of belief, and it has been widely used for security protocol formal verification [6, 21, 16]. Specially, BAN logic has a set of rules for defining and analyzing information exchange protocols, which can help its users determine whether the exchanged information are trustworthy and secure against eavesdropping.

5.1.1 Basic Operators of BAN Logic

The main objects in BAN contains communication participants(P and Q), session $key(K)$ and some operators. And X represents any statements. BAN has 10 basic modal operators including: P believes $X(P|\equiv X)$; P sees $X(\mathrm{P}\lhd X)$; P once said $X(P|\sim X)$; P has jurisdiction over $X(P \Rightarrow X)$; X is fresh $(\#(X))$; P and Q share key $K(P \overset{K}{\longleftrightarrow} Q)$; P has a published public key $K(\overset{K}{\longrightarrow} P)$, and corresponding private key K^{-}; P and Q share secret $X(P \overset{X}{\rightleftarrows} Q)$; Message encryption $(\{X\}_K)$ and Message combination $(<X>_Y)$. The detailed introduction can be found in [6].

5.1.2 Main Inference Rules of BAN Logic

(1) Message meaning: If P believes K is Q's public key and P sees $\{X\}_{K^-}$, then P believes Q said X.

$$\frac{P|\equiv \overset{K}{\longrightarrow} Q, P \lhd \{X\}_{K^-}}{P|\equiv Q|\!\sim X}$$

For sharing key case, the similar rule is:

$$\frac{P|\equiv P \overset{K}{\longleftrightarrow} Q, P\lhd <X>_Y}{P|\equiv Q| \sim X}$$

(2) Jurisdiction: If P believes Q has jurisdiction over X and P believes Q believes X, then P believes X.

$$\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$$

(3) Nonce verification: If P believes X is fresh and P believes Q believes once said X, then P believes Q believes X.

$$\frac{P\mid\equiv \#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$$

(4) Belief: If P believes X, and P believes Y, then P believes the combined (X, Y).

$$\frac{P\mid\equiv X, P\mid\equiv Y}{P\mid\equiv (X, Y)}$$

If P believes the combined (X, Y), then P believes X.

$$\frac{P\mid\equiv (X, Y)}{P\mid\equiv X}$$

If P believes Q believes the combined (X, Y), then P believes Q believes X.

$$\frac{P\mid\equiv Q\mid\equiv (X, Y)}{P\mid\equiv Q\mid\equiv X}$$

(5) Freshness: If P believes X is fresh, then P believes the combined (X, Y) is fresh.

$$\frac{P\mid\equiv \#(X)}{P\mid\equiv \#(X, Y)}$$

(6) Message receiving: If P believes K is the public key of P, and P sees $\{X\}_{K^-}$, then P sees X.

$$\frac{P\mid\equiv \xrightarrow{K} P, P \lhd \{X\}_{K^-}}{P \lhd X}$$

Since BAN logic is based on knowledge and belief, we can add another message meaning rule for our protocol inference.

(7)Complex message meaning: If P believes K is the public key of P and R is public key of Q, and P sees the encrypted message $\{\{X\}_K\}_{R^-}$, then P believes Q said X.

$$\frac{P\mid\equiv \xrightarrow{K} P, P\mid\equiv \xrightarrow{R} Q, P \lhd \{\{X\}_{K^-}\}_{R^-}}{P\mid\equiv Q \sim X}$$

5.2 The Protocol Formal Analysis

There are three participants in the protocol: the tag A, the reader B, and the backend database S. Further, A and B share the public key of the database S. Supposing there is a secure communication channel between the reader B and database S, for instance, using a wired secure communication. $data$ represents the secret data that the tag saved.

5.2.1 The initial assumption

1) The assumptions trusted by all participants:

- $S\mid\equiv \#(R)$: the backend database S believes the reader's random number R is fresh;
- $A\mid\equiv \#(R)$: the tag A believes the reader's random number R is fresh.

2) The initial keys trusted by all participants:

- $S\mid\equiv \xrightarrow{P_t} A$: the database S believes P_t is the tag A public key;
- $S\mid\equiv \xrightarrow{P_s} S$: the database S believes P_s is his own public key;
- $A\mid\equiv S \overset{id}{\rightleftarrows} A$: the tag A believes it shares the secret id with the database S.

3) The controlled services provided by all participants:

- $S\mid\equiv A\mid\Rightarrow id$: the database S believes the tag A has jurisdiction over id;
- $A\mid\equiv S\mid\Rightarrow id^{'}$: the tag A believes the database S has jurisdiction over its own saved $id^{'}$.

5.2.2 The Ideal Model of the Protocol

In order to formally analyze the protocol, the abstracted ideal model of the original protocol are as follows:

① $A \rightarrow B$: $\{R, P_t, \{\{id, R\}_{P_s}\}_{P_t^-}\}$: That is the tag send message $\{R, P_t, \{\{id, R\}_{P_s}\}_{P_t^-}\}$ to the reader.

② $B \rightarrow S$: $\{R, P_t, \{\{id, R\}_{P_s}\}_{P_t^-}\}$: That is the reader forward the $\{R, P_t, \{\{id, R\}_{P_s}\}_{P_t^-}\}$ to the backend database.

③ $S \rightarrow B$: $\lhd id^{'}, R, K \rhd_{id}$: That is the database send the combined secret $\lhd id^{'}, R, K \rhd_{id}$ to the reader.

④ $B \rightarrow A$: $<id^{'}, R, K>_{id}$: That is the reader forward the combined secret $\lhd id^{'}, R, K \rhd_{id}$ to the tag.

⑤ $A \rightarrow B$: $\{P_t, R, \{\{data, R\}_{P_s}\}_{P_t^-}\}$: That is the tag send the final secret information $\{P_t$, R, $\{\{data, R\}_{P_s}\}_{P_t^-}\}$ to the reader.

5.2.3 The Expected Goal of the Protocol

Supposing the communication between the reader and the backend database is secure and the database saves each tag's ID in advance. So, the expected goal of the proposed protocol includes: ① $S\mid\equiv id$, that is the backend database believes the id that the tag send. ② $A\mid\equiv id^{'}$, that is the tag believes the $id^{'}$ that the backend database send.

Table 1: Performance comparison among several public-key encryption based RFID secure protocols

Protocol Goals	**Sub-goals**	**[15]**	**[9]**	**[5]**	**Ours**
Authentication	Tag	○	○	○	○
	Reader	○	○	○	○
Forward security	User Privacy	○	○	○	○
	Position Tracking	○	○	○	△
Backward security	Replay Attacking	○	○	○	○
Data Security	Confidentially	○	○	○	○
	Integrity	△	△	△	○
Performance	Random number?	*Y*	*Y*	*Y*	*N*
	Point multiplication?	*Y*	*Y*	*N*	*N*
	Simple calculation	*P*	*P*	*P*	*Y*

5.2.4 BAN Logic Inference

1) From message ①, we can get $B \triangleleft \{R,\ P_t,\ \{\{id, R\}_{P_s}\}_{P_t^-}\}$, but cannot understand the encrypted message and forward it to S.

2) From message ②, we can get $B \triangleleft \{R,\ P_t,\ \{\{id, R\}_{P_s}\}_{P_t^-}\}$. Then, according to the initial assumption $S|\equiv \xrightarrow{P_t} A$ and $S|\equiv \xrightarrow{P_s} S$, using Rule(7) can yield: $S|\equiv A \backsim \{id, R\}$. Next, by initial assumption $S|\equiv \#(R)$ and Rule(5), can get $S|\equiv \#(id, R)$. After that, using Rule(3), can get $S|\equiv A|\equiv \{id, R\}$. Next, using Rule(4), can obtain $S|\equiv A|\equiv id$. After that, according to the initial assumption $S|\equiv A|\Rightarrow id$, can get $S|\equiv id$. Finally, S send message ③.

3) Once B receive message ③, forward and send message ④. Once A received message ④, it says $A \triangleleft < id^{'}, R, K >_{id}$. According to the initial assumption $A|\equiv S \overset{id}{\rightleftarrows} A$ and Rule(1), can yield $A|\equiv S \backsim \{id^{'}, R, K\}$. Then, by initial assumption $A|\equiv \#(R)$ and Rule(5), can get $A|\equiv \#\{id^{'}, R, K\}$. After that, using Rule(3), can yield $A|\equiv S|\equiv \{id^{'}, R, K\}$. Next, using Rule(4), can get $A|\equiv S|\equiv id^{'}$. Finally, using Rule(2), we can get the goal $A|\equiv id^{'}$, that is what the protocol expected.

From the above inference, it shows that the protocol obtains the final belief goal, $S|\equiv id$ and $A|\equiv id^{'}$. That is to say the protocol reaches its security goal and the authentication succeeds.

6 The Comparison of Relative RFID Protocols

Our proposed protocol is based on ECC, which can provide strong encryption only by a short length of key. Furthermore, the protocol only use some simple operators, reducing the tag computational complexity, which is suitable for those low cost tags. Next, we will give a comparison between our protocol and some typical public-key based protocols from the point of security and performance. It is shown in Table 1.

In Table 1, [15] and [9] are two ECC-based RFID security protocols, and [5] is a public-key based one. And the notation "○" represents the protocol implements well or provides this service. " △ " means partially provided or not well implemented. "*Y*" means yes, "*N*" means no, and "*P*" means partial.

From Table 1, it shows that from the point of security, our protocol is almost equivalent to the existing protocols. However, concerning the computation compared with other related protocols, ours has great advantages, especially for those ECC based protocol, the point multiplication requires considerable computing capacity. So, our protocol is suitable for those low cost, low computational ability tags.

7 Conclusion and Future Work

RFID as the core technology of IoT, the security issues have been emerged widely. It is meaningful to develop lightweight RFID security protocols for those low cost and low computation capability tags. In this paper, we proposed a elliptic curve cryptography based protocol, analyzed its security, performance, and verified using BAN logic. From the analysis, it shows that the protocol can provide mutual authentication for the tag and the reader. Meanwhile, it can resist some common RFID related attacks. Moreover, our proposed protocol just use some simple operators, such as XOR, bitwise AND, etc., reducing the computation complexity for those low cost tags.

The future directions we can do further are: simulating the protocol in some real IoT environments to evaluate its real performance; using more factors not only random number to improve the forward security; developing our own lightweight hash function to balance the tradeoff between the computation pressure and security requirements.

Acknowledgments

This study was supported by the Shanghai Municipal Natural Science Foundation under grant No.13ZR1416100. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] P. D. Arco and A. D. Santis, "On ultralightweight RFID authentication protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 4, pp. 548–563, 2011.

[2] J. P. Aumasson, L. Henzen, W. Meier, and M. N. Plasencia, "Quark: A lightweight hash," *Journal of Cryptology*, vol. 26, no. 2, pp. 313–339, 2013.

[3] P. Babaheidarian, M. Delavar, and J. Mohajeri, "On the security of an ECC based RFID authentication protocol," in *9th International ISC Conference on Information Security and Cryptology (ISCISC'12)*, pp. 111–114, Tabriz, Sept. 2012.

[4] Baidu Encyclopedia, *Intelligent Earth*, July 24, 2015. (http://baike.baidu.com/view/2168958.htm)

[5] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Proceedings of PerCom'07*, pp. 217–222, White Plains, NY, Mar. 2007.

[6] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *ACM Transaction on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[7] T. J. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, no. 1, pp. 95–100, 2009.

[8] M. L. Deng, J. F. Ma, and L. H. Zhou, "Design of anonymous authentication protocol for RFID," *Journal of Communications*, vol. 30, no. 7, pp. 20–26, 2009.

[9] G. Godor, P. Szendi, and S. Imre, "Elliptic curve cryptography based authentication protocol for small computational capacity RFID systems," in *Proceedings of the 6th ACM Workshop on QoS and Security for Wireless and Mobile Networks*, pp. 98–105, Bodrum, Turkey, Oct. 2010.

[10] G. N. Khan and M. B. Moessner, "Secure authentication protocol for RFID systems," in *20th International Conference on Computer Communications and Networks (ICCCN'11)*, pp. 1–7, Hawaii, USA, July 2011.

[11] W. Khedr, "On the security of moessner and KHAN authentication scheme for passive EPCglobal C1G2 RFID tags," *International Journal of Network Security*, vol. 16, no. 5, pp. 369–375, 2014.

[12] E. S. Kumar and C. Paar, "Are standards compliant elliptic curve cryptosystems feasible on RFID?," in *Proceedings of RFIDSec'06*, New York, USA, 2006.

[13] G. B. Lin, Y. H. Wang, and Y. J. Zhan, "RFID security protocol based on random sequence," *Computer Engineering*, vol. 34, no. 20, pp. 151–153, 2008.

[14] S. Martnez, M. Valls, C. Roig, F. Gin, and J. M. Miret, "An elliptic curve and zero knowledge based forward secure RFID protocol," in *3rd conference on RFID-Sec*, pp. 42–52, Malaga,Spain, July 2007.

[15] S. Martnez, M. Valls, C. Roig, J. M. Miret, and F. Gin, "A secure elliptic curve-based RFID protocol," *Journal of Computer Science and Technology*, vol. 24, no. 2, pp. 309–318, 2009.

[16] J. L. Meng and Z. Wang, "A RFID security protocol based on hash chain and three-way handshake," in *Fifth International Conference on Computational and Information Sciences (ICCIS'13)*, pp. 1463–1466, Shiyang, June 2013.

[17] D. Molnar and D. Wagner, "Privacy and security in library RFID issues, practices, and architectures," in *11th ACM Conference on Computer and Communications Security (CCS'04)*, pp. 210–219, Washington, DC, USA, Oct. 2004.

[18] M. Naveed, W. Habib, U. Masud, U. Ullah, and G. Ahmad, "Reliable and low cost RFID based authentication system for large scale deployment," *International Journal of Network Security*, vol. 14, no. 3, pp. 173–179, 2012.

[19] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: a research survey," in *2011 International Conference on Communication Systems and Network Technologies (CSNT'11)*, pp. 115–119, Katra, Jammu, June 2011.

[20] P. Peris-Lopez, J.C. Hernandez-Castro, J.M.E. Tapiador, and A. Ribagorda, "Lmap: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Workshop on RFID Security (RFID-SEC'06)*, pp. 1–6, Graz, Austria, July 2006.

[21] Q. Qian, X. Guo, and R. Zhang, "RFID protocol based on random number and encryption hash," in *IET International Communication Conference on Wireless Mobile and Computing (CCWMC'11)*, pp. 169–174, Shanghai, China, Nov. 2011.

[22] S. H. Qing, "Design and logical analysis of security protocols," *Journal of Software*, vol. 14, no. 7, pp. 1300–1309, 2003.

[23] S. E. Sarma, S. A. Weis, and D. Engels, "Radio-frequency identification: Secure risks and challenges," *CryptoBytes*, vol. 6, no. 1, pp. 2–9, 2003.

[24] S. E. Sarma, S. A. Weis, and D. W. Engels, "Rfid systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems (CHES'02)*, pp. 454–469, CA, USA, Aug. 2002.

[25] A. Shamir, "SQUASH - A new mac with provable security properties for highly constrained devices such as RFID tags," *Fast Software Encryption*, LNCS 5086, pp. 144–157, Springer, 2008.

[26] D. Z. Sun and J. D. Zhong, "A hash-based RFID security protocol for strong privacy protection," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1246–1252, 2012.

[27] C. H. Wei, M. S. Hwang, and A. Y. Chin, "A mutual authentication protocol for RFID," *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, 2011.

[28] C. H. Wei, M. S. Hwang, and A. Y. Chin, “An improved authentication protocol for mobile agent device in RFID,” *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[29] C. H. Wei, M. S. Hwang, and A. Y. Chin, “An authentication protocol for low-cost RFID tags,” *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[30] Wikipedia, *Internet of Things*, July 24, 2015. (`http://en.wikipedia.org/wiki/Internet-of-Things`)

[31] H. W. Wu, S. H. Qing, and H. L. Li, “Security analysis and improvement to digital library RFID protocol,” in *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet'12)*, pp. 2834–2837, Yichang, China, Apr. 2012.

[32] X. L. Zhang and B. King, “Security requirements for RFID computing systems,” *International Journal of Network Security*, vol. 6, no. 2, pp. 214–226, 2008.

[33] Y. B. Zhou and D. G. Feng, “Design and analysis of cryptographic protocols for RFID,” *Chinese Journal of Computers*, vol. 29, no. 4, pp. 581–589, 2006.

Quan Qian is a Professor in Shanghai University, China. His main research interests concerns computer network and network security, especially in cloud computing, IoT and wide scale distributed network environments. He received his computer science Ph.D. degree from University of Science and Technology of China (USTC) in 2003 and conducted postdoc research in USTC from 2003 to 2005. After that, he joined Shanghai University and now he is the lab director of network and multimedia.

Yan-Long Jia is a master degree student in the school of computer science, Shanghai University. His research interests include IoT, computer and network security.

Rui Zhang received her B.E. and Ph.D. degree from Department of Electronic Engineering & Information Science, University of Science and Technology of China, in 2003 and 2008, respectively. After that, she joined the School of Computer Engineering and Science, Shanghai University. Now, she is an associate professor and her main research interests include computer networks, network coding for wireless networks and wireless communication, etc.