I.J. Modern Education and Computer Science, **2014, 1, 17-24**
Published Online January 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.01.02

A Novel Mutual RFID Authentication Protocol with Low Complexity and High Security

Samad Rostampour
Department of Computer Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: s.rostampour@srbiau.ac.ir

Mojtaba Eslamnezhad Namin
Department of Computer Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: m.eslamnezhad@srbiau.ac.ir

Mehdi Hosseinzadeh
Department of Computer Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: hosseinzadeh@srbiau.ac.ir

Abstract — Radio Frequency Identification (RFID) is a method for automated identifying objects. One of the problems of this technology is its security. RFID tags include resource limitation; therefore, the system designers cannot implement complex circuits to enhance their security. Usually the symmetric and asymmetric encryption methods increase resources and cost. Because it is believed to increasing security is inconsistent with the simplicity, the researchers mostly use one-way encryption methods. In this paper, we propose a mutual authentication protocol based on public key cryptography. The used encryption method includes high security and low complexity. This protocol performs in few steps and is suitable for portable devices with power limitation. In terms of security, the proposed protocol is robust against known attacks. In addition, we prove the protocol is secure by an analytical method.

Index Terms — RFID, Mutual Authentication, Security, Encryption, Public key.

I. INTRODUCTION

Objects Automatic identification is currently growing. Researchers have presented different technologies in recent years. One of these is barcode, which was very popular for its cost and efficiency. Some barcode restrictions, such as requiring line-of-sight and the operator caused that the other technologies emerged. Radio Frequency Identification (RFID) is one of the methods that has been impressive during the past decade and overcame many limitations. RFID does not require an operator and can detect many objects simultaneously. Because RFID relates to some issues such as identification and privacy, it requires highly secure structure. One of the security parameters of RFID is an appropriate authentication method for preventing unauthorized access. The first step in the communication between a tag and a reader is a device is sure that the other side is legitimate. The purpose of this paper is to provide a mutual authentication method, which includes high security, low computational cost and easy implementation. During the recent years, many different methods are presented for authenticating that most of them have suffered from security flaws. The most of primary researches have presented one-way authentication method. Because of Inventing various penetration approaches the security models have been turned into mutual methods. The methods confirm the validity of a tag and a reader simultaneously. Increasing applications of RFID and enter it into the different categories such as healthcare, agriculture, food supply chain, transportation and other services cause to increase the importance of secure access. On the other hand, the different attacks, such as traceability, Do's and replay have shown that RFID systems are vulnerable. In this paper, a method is presented which provide different aspects of security. The one-way hash model could not solve all security problems, but searchers persisted to use this model for reducing complexity. This matter proved that only reducing the weight of authentication methods is not the main criterion. The system designers require to tradeoff between weight and security. The encryption method in this paper is based on public key encryption, so it has a high security level. Unlike most strong encryption methods as ECC (Elliptic Curve Cryptography) and RSA, this method provides less complexity that is suitable for portable systems, such as RFID, tag and Smart Card

We organize this paper as below: in the next section, we describe some related works in this area. The III section discusses about the proposed encryption technique and its mathematical analysis. Section IV presents the new protocol. Efficiency and security of the proposed protocol are evaluated in Section V. Finally, will be conclusions.

II. RATED WORKS

In recent years, the much research has been done about RFID security. Many researchers have attempted to present a secure authentication method and claimed that it is robust against various attacks.

Some other researchers initially found the weakness of previous protocols and then, solved it or offered a new protocol. Today, many protocols are used to justify the attack and their security will be rejected. In [1] an Ultra-light weight protocol was presented which used permutation method for exchanging information. This method performed a series of simple logical operations such as shift and xor and they transform the data. In the period shortly after the introduction of this paper, three papers were presented that they penetrated to this approach. In [2] traceability attack is carried out. In [3] Disclosure attack was carried out and [4] proved RAPP protocol is not resistance against DE synchronization attack. Paper [5] designed a new attack on RFID systems and introduced a new protocol called ACSP. It claimed that ACSP is resistant against the new attack and other known attacks. Paper [6] attacked to the ACSP protocol and proved that it is not strong. It implemented impersonation and traceability attacks on ACSP protocol. In 2007, Konidala et al. presented a lightweight authentication protocol [7]. The authors tried to use simple operation for sending data such as access password. This protocol was based on ISO-18000-6C standard. About 5 years later, Huang et al. demonstrated the proposed protocol included weaknesses and can be penetrated to ISO-18000-6C [8]. Because the used encryption method was weak, the authors showed that this protocol is weak against correlation attack and the attacker can recover data by eavesdropping some of the information. Hence, Huang presented a new mutual authentication protocol that removed some of the problems and utilized simple functions such as xor or mod.

Paper [9] presented a one-way hash method based on low-cost methods. This protocol was based on mutual authentication and claimed that, because of the updating TID in each step of the connection, it prevent many attacks.

III. CRYPTOGRAPHY MODEL

In this section, we introduce the method of encryption. First, the mathematical concept is defined. Then, how to apply it in the field of cryptography is described.

A. Mathematically defined

It is assumed $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{n} \in \mathbb{R}^\mathrm{m}$ is a set of linearly independent vectors. L lattice is a set of linear combinations of $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{n}$ with coefficients in $\mathbb{Z}$:

$$L = \{a_1\mathrm{v}_1 + a_2\mathrm{v}_2 + \cdots + a_n\mathrm{v}_n \;:\; a_1, a_2, \ldots, a_n \in \mathbb{Z}\} \quad (1)$$

A basis for L is any set of linearly independent vectors, which makes L. Both of arbitrary bases of L have the same number of elements. A dimension of a lattice L is the number of vectors in any basis of L.

Suppose that $\mathrm{v}_1, \ldots, \mathrm{v}_\mathrm{n}$ are the bases for L and $\mathrm{w}_1, \ldots, \mathrm{w}_\mathrm{n} \in \mathrm{L}$ are the set of vectors for L. Can be written any wj for lattice as follows:

$$\begin{aligned} \mathrm{w}_1 &= \mathrm{a}_{11}\mathrm{v}_1 + \mathrm{a}_{12}\mathrm{v}_2 + \cdots + \mathrm{a}_{1\mathrm{n}}\mathrm{v}_\mathrm{n} \\ \mathrm{w}_2 &= \mathrm{a}_{21}\mathrm{v}_1 + \mathrm{a}_{22}\mathrm{v}_2 + \cdots + \mathrm{a}_{2\mathrm{n}}\mathrm{v}_\mathrm{n} \\ \mathrm{w}_\mathrm{n} &= \mathrm{a}_{\mathrm{n}1}\mathrm{v}_1 + \mathrm{a}_{\mathrm{n}2}\mathrm{v}_2 + \cdots + \mathrm{a}_{\mathrm{nn}}\mathrm{v}_\mathrm{n} \end{aligned} \quad (2)$$

In above equation all coefficients a_{ij} are the integer number. Both available bases of L lattice are interrelated and interdependent with a matrix has integer numbers elements and ± 1 determinant. One of the fundamental computational problems related to the lattice is finding the shortest nonzero vector in it. Another main problem is finding a vector in a lattice, which is the closest to arbitrary external vector. In this section, we describe same problems and analyze them in terms of mathematic and cryptography.

The shortest vector problem (SVP): The goal of this problem is, finding the shortest nonzero vector in L lattice; it means to find a nonzero vector $\mathrm{v} \in \mathrm{L}$, so that Euclidean norm $\|\mathrm{v}\|$ is minimal.

The closest vector problem (CVP): by having $\mathrm{w} \in \mathbb{R}^\mathrm{m}$ which is not in L, the aim is to find the vector $\mathrm{v} \in \mathrm{L}$ is closest to w. It means to find the minimum $\mathrm{v} \in \mathrm{L}$ so that Euclidean norm $\|\mathrm{w} - \mathrm{v}\|$ is minimal. SVP and CVP are deep problems. In addition, their computational complexity is increased when the lattice dimension grows. Even finding approximate solutions for the CVP and SVP, is used even in many different fields of pure and applied mathematics. CVP and SVP are members of NP-hard problems. In 1998, in [10] has been shown to solve such problems is not simply possible. In practice, CVP is a little more difficult than SVP because CVP often convert to SVP with slightly more dimensions. To view the proof of solving SVP is not more difficult than CVP see [11]. In mid-90s, several cryptographic systems were introduced that they are based on difficult problems such as SVP and CVP in a lattice with a large dimension N that their security were not acceptable. Ultimately, by resolving some problems, designing secure cryptographic systems based on lattice problems was provided. Motivation for introducing these cryptosystems has been two matters. First, insomuch breaking the inverse computational one-way algorithms had been easier; so new cryptosystems were required that there are based on other kinds of difficult mathematical problems. For example, two decades ago many people thought factorization 384-bit numbers were impossible; today, not only 384-bit numbers were dissolved but also 512-bit numbers have been factorized. Attending the number of scientists of cryptosystem to break public key encryption systems, could not led to collapse encryption methods but it was caused these systems became less safe, more fragile and slower.

The second reason is that encryption systems based on the lattice are faster than systems based on discrete logarithms or factorization numbers like RSA or ECC. Generally, to obtain the k-bit security, encryption and decryption operations of RSA and ECC algorithms are required to $\mathcal{O}(\mathrm{k}^3)$ operation whereas this rate is $\mathcal{O}(\mathrm{k}^2)$ in a system based on lattices. Furthermore, the implementation of simple linear algebra operations in systems based on lattice in terms of hardware and software is very simple. A point that should be noted is that analyzing methods for encryption systems based on the lattice are not well known as systems based on factorization numbers or discrete logarithm. Thus, despite systems based on the lattice are the subject of ongoing researches, but their practical implementations are very low compared with older systems. Some of the required parameters in cryptography are described as follows. Lattices with even dimension as $\mathrm{n} = 2\mathrm{N}$ that include all $(\mathrm{x}, \mathrm{y}) \in \mathbb{Z}^{2\mathrm{N}}$ vectors. For every positive integer constant q which is a public parameter and it’s order is(n) :

$$y \equiv xH \quad (mod\ q) \tag{3}$$

Matrix H is a public key and $\mathrm{N} \times \mathrm{N}$ matrix where each its row is obtained by performing a permutation of the previous row. Therefore, for showing H, its first row is sufficient, so, the length of the public key is $\mathcal{O}(\mathrm{n} \log \mathrm{n})$ and it will be significantly smaller than the key of GGH.

Private key is only a short vector of $(\mathrm{f}, \mathrm{g}) \in \mathrm{L}$. This set with its partial rotations include $\mathrm{N} = \frac{1}{2}\dim(\mathrm{L})$ independent short vector in L. This matter allows the owner of (f, g) to solve the certain cases of CVP in L and extract plain text from cipher text. Security of the original text is based on the difficulty of solving the CVP in lattice. Moreover, vector (f,g) and its turns are approximately shortest nonzero certain vectors in L. Now by this method sending secure information is as follows.

B. *Encryption method*

This operation starts by selecting an integer $\mathrm{N} \geq 1$ and two modulo p and q. It is assumed R, Rp and Rq are shortened form of polynomial rings (4):

$$\begin{aligned} \mathrm{R} &= \frac{\mathbb{Z}[\mathrm{x}]}{(\mathrm{x}^{\mathrm{N}}-1)} \\ \mathrm{R}_{\mathrm{p}} &= \frac{(\mathbb{Z}/\mathrm{p}\mathbb{Z})[\mathrm{x}]}{(\mathrm{x}^{\mathrm{N}}-1)} \\ \mathrm{R}_{\mathrm{q}} &= \frac{(\mathbb{Z}/\mathrm{q}\mathbb{Z})[\mathrm{x}]}{(\mathrm{x}^{\mathrm{N}}-1)} \end{aligned} \tag{4}$$

Several assumptions about the parameters N, p and q are considered, N must be a prime number and $\gcd(\mathrm{N}, \mathrm{q}) = \gcd(\mathrm{p}, \mathrm{q}) = 1$.

In this system, at first, recipient chooses its general parameters N, p, q and d with terms mentioned earlier. Recipient's private key consists of two-elected random polynomial:

$$\mathrm{f(x)} \in \mathcal{T}(\mathrm{d}+1, \mathrm{d}), \mathrm{g(x)} \in \mathcal{T}(\mathrm{d}, \mathrm{d}) \tag{5}$$

It calculates the inverse of a polynomial f in Rp and Rq and called them Fp and Fq:

$$\mathrm{F}_q(x) = \mathrm{f}(x)^{-1} \ \text{ in } R_q \ , \mathrm{F}_p(x) = \mathrm{f}(x)^{-1} \ \text{ in } R_p \tag{6}$$

If any of the inverses does not exist, the receiver must select a new f(x). If a polynomial has the form $\mathcal{T}(\mathrm{d}, \mathrm{d})$, means it has equal number of 1 and -1, then it is not never reversible in R_{q}. So, the receiver chooses f(x) in term $\mathcal{T}(\mathrm{d}+1, \mathrm{d})$ not to $\mathcal{T}(\mathrm{d}, \mathrm{d})$. The receiver calculates polynomial (7) as:

$$\mathrm{h(x)} = \mathrm{F}_{\mathrm{q}}(\mathrm{x}) * \mathrm{g(x)} \ \text{ in } \mathrm{R}_{\mathrm{q}} \tag{7}$$

Polynomial h(x) is the recipient's public key and its private key is pair $\left(\mathrm{f(x)}, \mathrm{F}_{\mathrm{p}}(\mathrm{x})\right)$. Furthermore, the receiver can only save f(x) and when needed calculates $\mathrm{F}_{\mathrm{p}}(\mathrm{x})$ byf(x).

The main message is the polynomial $\mathrm{m(x)} \in \mathrm{R}$ that its coefficients are in the range$\left(-\frac{\mathrm{p}}{2}, \frac{\mathrm{p}}{2}\right]$. The Sender selects random polynomial $\mathrm{r(x)} \in \mathcal{T}(\mathrm{d}, \mathrm{d})$ as one-time key and calculates (8) as:

$$\mathrm{e(x)} \equiv \left(\mathrm{ph(x)} * \mathrm{r(x)} + \mathrm{m(x)}\right) \ (\mathrm{mod}\, \mathrm{q}) \tag{8}$$

Encrypted text of sender is the polynomial e(x) in the ring Rq.

C. *Decryption method*

Receiver for encrypting first calculates polynomial a(x) byf(x):

$$\mathrm{a(x)} \equiv \mathrm{f(x)} * \mathrm{e(x)} \ \ (\mathrm{mod}\, \mathrm{q}) \tag{9}$$

Then $\mathrm{F}_{\mathrm{p}}(\mathrm{x})$ multiply with a(x) modulo p:

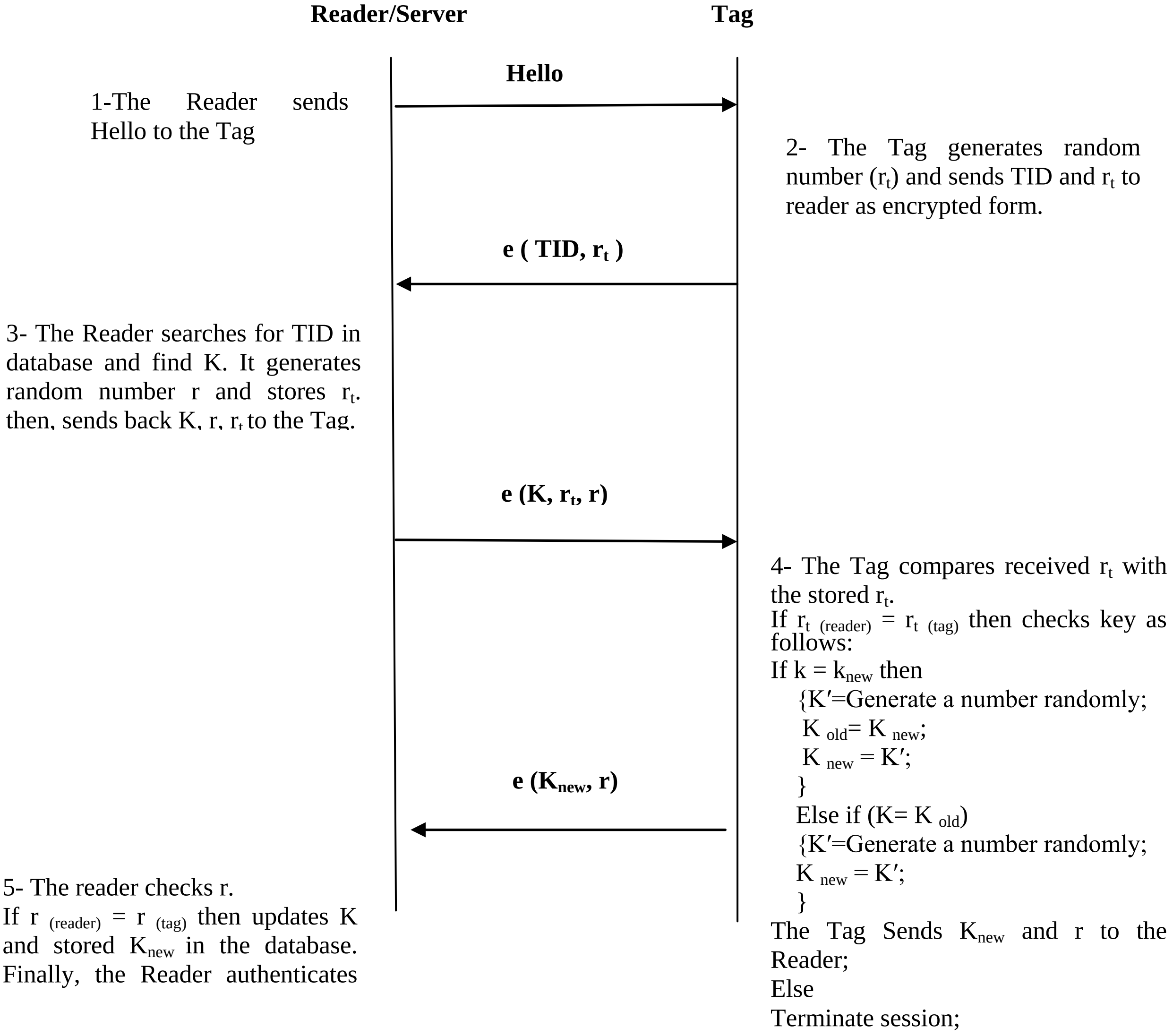
$$\mathrm{b(x)} \equiv \mathrm{F}_{\mathrm{p}}(\mathrm{x}) * \mathrm{a(x)} \ \ (\mathrm{mod}\, \mathrm{p}) \tag{10}$$

Assume that all the parameters are chosen properly, is shown that the polynomial $\mathrm{b}(x)$ which indeed is the original message $\mathrm{m}(x)$ [12].

IV. THE PROPOSED PROTOCOL

Encryption method was described in the previous section. This method uses simple operations such as addition and multiplication; so, it has high speed and low complexity. It is based on NP-hard problems. We describe the proposed protocol in this section. We have used the introduced encryption method in this protocol and provided a mutual authentication. We assume the reader and back-end server have been combined together although they can be separate. We implement it in five phases and denote some parameters as below:

1. TID: it is the ID number of the tag that is assigned to it.
2. Kold: it is the primary authentication key.
3. Knew: it is the new authentication key after updating K.
4. r: it is a random message that the reader generates it.
5. rt: it is a random message that the tag generates it.



1-The Reader sends Hello to the Tag

2- The Tag generates random number (r_t) and sends TID and r_t to reader as encrypted form.

3- The Reader searches for TID in database and find K. It generates random number r and stores r_t. then, sends back K, r, r_t to the Tag.

4- The Tag compares received r_t with the stored r_t.

```
If $r_{t\ (reader)} = r_{t\ (tag)}$ then checks key as follows:
If $k = k_{new}$ then
    {K′=Generate a number randomly;
    $K_{old} = K_{new}$;
    $K_{new} = K′$;
    }
    Else if ($K = K_{old}$)
    {K′=Generate a number randomly;
    $K_{new} = K′$;
    }
The Tag Sends $K_{new}$ and r to the Reader;
Else
Terminate session;
```

5- The reader checks r.
If $r_{(reader)} = r_{(tag)}$ then updates K and stored K_{new} in the database. Finally, the Reader authenticates

Figure 1. The proposed protocol

The first phase: In this phase, the reader sends a request message (Hello) to the tag.

The second phase: tag immediately after receiving Hello and activating, generates a random number (r_t). Then it encrypts r_t and TID with the public key of the reader. It sends the encrypted message shows as e(TID, r_t) to the reader.

The Third phase: the reader decrypts received information from the tag. After that, it searches TID in the database. If the server finds some equivalent, the operation will continue. In the row of TID field, a key is stored. The server also generates a random number r. Then all this information sends to the tag in an encrypted message. The contents of this message are r_t, k and r.

The fourth phase: after taking information, the tag compares received r_t with stored r_t in its memory. If they are equal, it will compare the value of K. In the tag, there are two fields K: K_{New} and K_{old}. Compare operation is simple. Therefore, storing two values is not expensive for the tag. At the first, K is compared with K_{new}. If they are equal, K is updated; otherwise, K is compared with K_{old} and if they are equal, then K is updated. The operation will be terminated if the received K is different with two fields. If the value of K is correct and updates, it means the tag authenticated the server. Because the protocol is mutual, the server must be able to authenticate the tag, too. The Tag sends K_{New} and r to the server as an encrypted form.

The Fifth phase: the server compares the received r with stored r in its database. If they are equal, value of K will be changed, and the authentication process will be completed.

V. SECURITY ANALYZES

Analysis of security of the proposed protocol will be discussed in this section. First, we test the protocol resistance against some known attacks. Then the protocol is evaluated by BAN logic.

Mutual Authentication: In the proposed protocol, at first, the tag authenticates the reader. When it received the desired information, such as k and r_t properly, it can verify the reader, then sends r and k_{new} to the reader, and if the information is correct, the reader confirms the tag. Therefore, both devices authenticate the other, and protocol is a mutual authentication.

DE synchronization: The aim of DE synchronization attack is not establishing a connection between the tag & the reader. Because the proposed protocol uses two fields K and both new and old values are stored, there is not the possibility of the attack. If at any stage of the connection sending information to be prevented, there will not be still the risk of attack.

Replay: This group of attacks usually occurs when the attacker makes fail in the exchange of information, by using the submitted information in the previous phases, to create a successful relationship with them. For two reasons encrypted form of the message is unused:

1) All data are sent in encrypted form, and the attacker cannot decrypt the data.
2) In each phase, there is a random number in the information. Therefore, Replay attack is not possible on this protocol.

Traceability: This attack occurs when the tag always sends a constant message in response to a reader; in this case, there is the possibility of tracking tags. This protocol is robust against traceability attack. The encryption method changes form of a message, and it uses a random value for generation new message in each time encoding. Therefore, the attacker cannot detect unique form message for tracing a tag.

DoS: In DoS attack, attacker intends to create multiple sessions to damage shared information on the tag and the reader. This protocol uses two key fields. Using two key fields causes if an adversary disconnects session in one of the connections is re-established successfully based on the old value of K. Therefore, the protocol is not vulnerable.

Eavesdropping: During all stages, the attacker can eavesdrop the information but none of this information would be helpful for him. All parameters as K, r and TID will be sent on the communication channel. Encrypting all data before sending, causes if the attacker obtains them he cannot break them.

Forward Secrecy: One of the security parameters is forward secrecy. Forward secrecy that means if an adversary penetrates to the system, he cannot retrieve the previous data based on the current information that is available. Because all information is encrypted by an asymmetric method, this is not possible in this algorithm and protocol is resistant against this threat.

Man-in-the-middle: In this protocol, the attacker cannot implement a MITM attack and presents itself as a party of the connection. Because of the exchanged information includes a random number (r) that is generated by each party, data is changed in each step. Therefore, a fake device cannot control the process.

Data confidentiality: The main advantage of the used encryption method is the cost to strength ratio. Because the encryption method is NP-hard problem, its breaking is more difficult. Therefore, the data will be confident in all stages of the process.

Impersonation: For impersonation attack, an attacker needs to know that some authentication parameters; so it can impersonate itself to others. There is no such possibility in this protocol. The protocol uses random value and encrypts all information. An adversary cannot find useful data for impersonation attack. He cannot create a session with unauthorized access. This protocol checks fresh information in each step of the process.

BAN Logic: In this section, we analyze the proposed authentication protocol with BAN logic. BAN logic is an important tool for evaluating protocols. This logic analyzes different parts of a system. There are some tools in this area, but we choose BAN logic because it is strong and simple. We describe it and prove the validation of the protocol with BAN logic [13, 14].

BAN logic performs protocol analyzing in four steps: Idealizing the protocol, Initiative premises, Establishment of security goals and Protocol Analysis. BAN logic consists of nineteen rules. Here we use only five principle rules as below:

Message-meaning Rule (R1):

$$\frac{P |\equiv \xrightarrow{K} Q, P \triangleleft \{X\}_k}{P |\equiv Q |\sim X} \tag{11}$$

Nonce-verification Rule (R2):

$$\frac{P |\equiv \#(X\ ), P |\equiv Q |\sim X}{P |\equiv Q |\equiv X} \tag{12}$$

Jurisdiction Rule (R3):

$$\frac{P |\equiv Q |\Rightarrow X\ , P |\equiv Q |\equiv X}{P |\equiv X} \tag{13}$$

Freshness Rule (R4):

$$\frac{P |\equiv \#(X)}{P |\equiv \#(X, Y)} \tag{14}$$

First step: Idealizing the protocol The aim of this step is converting the proposed protocol to favorable form, for implementing BAN logic on it. TID is unique for each tag. For clearly explaining, we denote TID in the tag TID_t and in the reader TID_r. By eliminating unencrypted messages of the proposed protocol, we have an ideal form as follows:

TABLE I: Security level comparison proposed algorithm with others algorithms

	Protocols					
Attack	Han et al.[15]	Qingling et al.[16]	Chen & Deng[17]	ACSP	RAPR	Proposed
Traceability	✓	✓	✓	✗	✗	✓
Desynchronization	✓	✓	✓	✗	✗	✓
DoS	✗	✓	✗	✓	✓	✓
Impersonation	✗	✗	✗	✗	✓	✓
Replay	✗	✓	✗	✓	✓	✓
✗: weak against attack ✓: strong against attack						

First message:

$$R \to T_X : \ \{IDS, r_t\}_{K_R^{-1}} \tag{15}$$

Second message:

$$T_x \to R: \ \left\{K, R \overset{r_t}{\longleftrightarrow} T, r\right\}_{K_T^{-1}} \tag{16}$$

Third message:

$$R \to T_X : \ \left\{K_{new}, R \overset{r}{\longleftrightarrow} T\right\}_{K_R^{-1}} \tag{17}$$

Second step: Initiative premises In this step, we denote the initial premises of the proposed protocol briefly as follows:

$$A_1 : R|\equiv T_X |\Rightarrow k_{new} \qquad A_2 : T_X |\equiv R \overset{r_t}{\longleftrightarrow} TID_i$$
$$A_3 : \mathrm{R} |\equiv R \overset{r_t}{\longleftrightarrow} T_X \qquad A_4 : R|\equiv k$$
$$A_5 : R|\equiv \#(r) \qquad A_6 : T|\equiv \#(r_t)$$
$$A_7 : T|\equiv IDS$$
$$A_8 : T \Big|\equiv \xrightarrow{K_T} T_X \qquad A_9 : R \Big|\equiv \xrightarrow{K_R} R$$
$$A_{10} : T \Big|\equiv \xrightarrow{K_R} R \qquad A_{11} : R \Big|\equiv \xrightarrow{K_t} T_X \tag{18}$$

Third step: Establishment of security goals The Goals of the proposed protocol include $R|\equiv T|\equiv k_{new}$ and $T|\equiv R|\equiv k$. It is meant that each major component of the system guarantees the validation of the other part of system in mutual authentication.

The fourth step: protocol Analysis In this step, by applying logical rules to the initial premises and the idealized messages in the first step, we discover the final opinion of the protocol**.** If the final opinion includes the certain goals in the previous step, the proposed authentication protocol can meet the necessary security requirements; otherwise, the proposed protocol is not secure. Proof of the protocol is as follows:

Based on first message:

$$T \lhd \{K, r_t, r\}_{K_T^{-1}} \tag{18}$$

Using the Message-meaning rule (R1) and assumption A9:

$$T\, |\equiv R| \approx \{K, r_t, r\}_{K_T^{-1}} \tag{19}$$

Using the Freshness rule (R4) and assumption A2:

$$B|\equiv \#\{IDS, K, r_t\}_{K_T^{-1}} \tag{20}$$

Using Nonce-verification rule (R2) and the following equations (20) and (21) can be claimed:

$$T\, |\equiv R|\equiv \{K, r_t, r\}_{K_R^{-1}} \tag{21}$$

Therefore, based on (22), we can conclude that:

$$T \mid\equiv R \mid\equiv k \tag{22}$$

Similarly, by the second message can be proved that:

$$R \mid\equiv T \mid\equiv k_{new} \tag{24}$$

As shown above, the final opinions result of the proof are $R \mid\equiv T \mid\equiv k_{new}$ and $T \mid\equiv R \mid\equiv k$. Therefore, we claim that the proposed protocol includes very high security and low overhead. In addition, it addresses many of the problems in the previous methods. It is a secure mutual RFID authentication. Table I presents the security level comparison the proposed protocol against other protocols.

VI. CONCLUSIONS

In this paper, we presented a mutual authentication method. There are several limitations for designing RFID systems. Because the tag resources are limited, we cannot use the complicated and expensive circuits in it. Usually increasing security causes increasing cost and complexity. The goal is to design simple circuits with proper security. Introduced protocol uses a public key encryption method. This method is defined in the lattice space. The encryption system has appropriate security because it is NP-Hard problem. In addition, its breaking probability is minimal. The used mathematical operations include simple operations such as addition and multiplication and its circuit are simple. The protocol performs authentication operation in few number stages and high-speed rate. Finally, we evaluated protocol and shown that it is resistant against known attacks. In addition, its performance was analysed by BAN logic and its safety was confirmed.

REFERENCES

[1] Y. Tian, G. Chen, J. Li. *A new ultralightweight RFID authentication protocol with permutation*, IEEE Communications Letters, 2012, 16 (5), pp702–705.

[2] G. Avoine, X. Carpent, Yet another ultralightweight authenticationprotocol that is broken, in pre-proceeding of RFIDsec, 2012.

[3] W. Shao-hui, H. Zhijie, L. Sujuan, C. Dan-wei, Security analysis of RAPP an RFID authentication protocol based on permutation, Cryptology ePrint Archive, Report 2012/327, 2012.

[4] Z.Ahmadian, M.Salmasizadeh, M.R. Aref Desynchronization attack on RAPP ultra-lightweight authentication protocol, Information Processing Letters, 2013, 113, pp 205–209.

[5] Zhu Zhong Qian, Ce Chen, Ilsun You, Sanglu Lu. ACSP: a novel security protocol against counting attack for UHF RFID systems, Computers & Mathematics with Applications, 2012, 63 (2), pp 492–500.

[6] M. Safkhani et al., on the security of RFID anti-counting security protocol (ACSP), Journal of Computational and Applied Mathematics, 2013.

[7] M. Konidala, Z. Kim, and K. Kim, A simple and cost effective RFID tag–reader mutual authentication scheme, in Proc. Int. Conf. RFIDSec, Jul. 2007, pp. 141–152.

[8] Y.Huang, W.Lin, and H.Li, Efficient Implementation of RFID Mutual Authentication Protocol, IEEE Transactions on Industrial Electronics, Vol. 59, No. 12, Dec 2012.

[9] J.Cho, S.Yeo, S.Kim, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, Computer Communications, 34, 2011, pp 391–397.

[10] M. Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions, in Proceedings of the thirtieth annual ACM symposium on Theory of computing, 1998, Dallas, Texas, United States: ACM.

[11] Goldreich O, Micciancio D, Safra S, Seifert J.P, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. Inform. Process. Lett., vol 71, 1999, pp. 55–61.

[12] Hoffstein J, Pipher J, Silverman J.H, NTRU: A Ring Based Public Key Cryptosystem, in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423 (J.P. Buhler, ed.), Springer-Verlag, Berlin, 1998, pp.267-288.

[13] Michael Burrows, Martin Abadi, Roger Needham. A Logic of Authentication. DEC SRC, 1989, Research Report 39.

[14] Zhen Zhang, Shijie Zhou, Zongwei Luo. Design and Analysis for RFID Authentication Protocol, IEEE International Conference on e-Business Engineering, 2008, Xian, china.

[15] S. Han, V. Potgar, E. Chang, Mutual authentication protocol for RFID tags based on synchronized secret information with monitor, Proceedings of ICCSA, 4707, LNCS, 2007, pp. 227–238.

[16] C. Qingling, Z. Yiju, W. Yonghua, A minimalist mutual authentication protocol for RFID system and BAN logic analysis, ISECS International Colloquium on Computing, Communication, Control, and Management, 2008, pp. 449–453.

[17] Chen, C.-L., Deng, Y.-Y., 2009. Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection. Engineering Applications of Artificial Intelligence 22, 1284–1291.

Samad Rostampour received B.S degree in computer hardware engineering form Shahid Bahonar University, Kerman, Iran in 2005 and M.S. degree in Computer Architecture, Iran in 2008. He is Ph.D candidate in computer system Architecture in Science and Research

Tehran branch, Islamic Azad University since 2012. Since 2008, he is faculty member of Islamic Azad University, Ahvaz branch and a lecturer of Computer Engineering Department. His research interests include Computer Networks, Information Security, Cryptography, and System Design.

Mojtaba Eslamnezhad Namin received his B.Sc. degree in Computer Engineering from Ardebil Branch, Islamic Azad University, Ardebil, Iran, in 2008. In addition, he received his M.Sc. degree in Computer Engineering from Tabriz Branch, Islamic Azad University, Tehran, Iran, in 2011. He has been a Ph.D. student at Science and Research Branch, Islamic Azad University, Tehran, Iran since 2012. His research interests include Security of RFID and WSN.

Mehdi Hosseinzadeh received B.Sc. in Computer Hardware Engineering from Islamic Azad University, Dezful branch, Iran in 2003. He also received the M.Sc. and Ph.D. degree in Computer System Architecture from the Science and Research Branch, Islamic Azad University, Tehran, Iran in 2005 and 2008, respectively. He is currently Assistant Professor in Department of Computer Engineering of Science and Research Branch of Islamic Azad University, Tehran, Iran. His research interests are Computer Arithmetic with emphasis on Residue Number System, Cryptography, Network Security and E-Commerce.