International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.369-382
http://dx.doi.org/10.14257/ijsia.2016.10.3.32

# RFID Bi-Directional Authentication Protocol Based on Dynamic Coupled Integer Tent Map

Liu Jiandong, Zhang Xiao, Wang Yequan, Shang Kai

*School of Information Engineering,*
*Beijing Institute of Petro-chemical Technology, Beijing 102617, China*
*liujiandong@bipt.edu.cn*

***Abstract***

T*o meet the special needs of RFID, it is proposed to use a coupled dynamic integer tent map lattices model (DCML) to implement a Hash function and a random number generation scheme. The scheme is featured with fast operation. Based on this， this paper proposes RFID bi-directional authentication protocol. This has strictly proved by BAN logic. This protocol can resolve eavesdropping, illegal access, location tracking, impersonation and replay attack.*

***Keywords****: RFID; Dynamic coupled integer tent map lattice; Random number; Hash function; Authentication protocol*

## 1. Introduction

RFID is a non-contact automatic identification technology, which can automatically identify an object and obtain relevant data through radio-frequency signal without human intervention. It can also work under various severe environments. RFID technology not only can identify a high-speed moving object, but also can simultaneously identify multiple labels. It is easy to operate and has been widely applied in various industries. However, RFID featured with non-contact also brings a lot of insecurity factors [1-2], mainly including unauthorized read, location tracking, eavesdropping, spoofing, replay attack, *etc*.

In order to solve security problems of RFID, scholars both at home and abroad have conducted intensive researches[3-7]， including Hash Lock Protocol[5] proposed by Sarma *et al*., Randomized Hash-lock Protocol [6] proposed by Weis *et al*., and Hash Chain Protocol proposed by Ohkubo *et al*. [7]. All of above three classical protocols are realized based on one-way Hash function. Due to unidirectionality of Hash function, these protocols can solve some insecure problems, but there are still insecure factors.

(1) Problems of Hash Lock Protocol：IDs of the labels are transmitted in an open form；metaID, Key, and ID are transmitted as fixed values, which are easy to be positioned by attackers；once a shared key is set, it can not be changed, and the metaID of the labels is static and can not be refreshed dynamically；An attracter can gain the trust of reader through intercepting metaID and ID, and thus conduct replay attack and spoofing towards backend database.
(2) Problems of randomized Hash Lock Protocol: IDi of label returned by reader is transmitted in an open form; attackers can gain the trust from the reader by intercepting IDi and R，so as to simulate (H(ID‖R),R), and thus conduct replay attack and spoofing; Attackers can effectively track labels by tracing IDi ; if the quantity of labels in the database is very large, the communication traffic between reader and database will be very large, and data are likely to be lost.
(3) Problems of Hash Chain Protocol: this protocol is a one-way authentication protocol

ISSN: 1738-9976 IJSIA

and a reader can authenticate a label but a label can not authenticate a reader; Two Hash functions are integrated in a label, so that the costs and calculated quantities of the label are improved; since labels can not authenticate readers, an attacker can pretend to be an reader, to constantly send Query requests to labels, and thus to constantly refresh secret values of labels, which leads to too big computation burden of database during later legitimate authentication. When the label refreshing frequency (t) is larger than the maximum length m of Hash Chain Protocol, the label becomes invalid; computation burden of backend database is not only related to the number (n) of labels, but also related to the label refreshing frequency (t), which causes the increase of computation burden of backend database.

Above analysis shows that, to solve the security problems of RFID, design of secure authentication protocol must meet the following two conditions:

(1) Hash value is used to replace information when conveying it in insecure channels and the important information shall be accompanied with random numbers;
(2) Bi-directional authentication function shall be placed between labels and readers. At present, the study of RFID secure authentication protocol is mainly focusing on the design of unipolarity of Hash function. Wen [8] proposed a RFID two-way authentication protocol based on Hash function, and Wen [9] proposed a RFID secure authentication protocol based on Hash function. Randomized Hash-lock Protocol and Hash Chain Protocol have achieved higher security performance than that of Hash Lock Protocol, but the authentication protocol algorithms proposed by above two papers still have serious security flaws.

RFID bidirectional authentication protocol proposed by Literature [4] based on Hash function. Protocol authentication process:

(1) A Reader sends a Query request to a label;
(2) After receiving the request, the label takes out its $ID_T$ value and reader's $ID_R$ value with read and write access, generates a random number R and timestamp $t_T$，and then sends $H(ID_T)\|H(ID_R,R)\|K_{Key}(R)\|H(t_T)$ to the reader;
(3) The reader will send the received $H(ID_T)\|H(ID_R,R)\|K_{Key}(R)$ to the database;
(4) Database will make a query to check whether there is a $ID_t$，which makes $H(ID_t)= H(ID_T)$. If yes, then a reader label $ID_r$ corresponding to $ID_t$ and the shared key of the label are taken out; R is obtained by decoding $K_{key}(R)$, and $H(ID_r,R)\|H(IDt,R)$ is sent to the reader. Meanwhile, R is used to update new secret key;
(5) After receiving message, the reader will check whether $H(IDr,R)= H(ID_R,R)$; if yes, then the reader sends $H(ID_t,R)\|H(t_T)\|H(t_R)$ to a label.
(6) After receiving message, the label checks whether $H(ID_T,R)=H(ID_t,R)$; if yes, it passes the authentication. R is used to update secret key, and $H(t_R)$ is sent to the reader.

The protocol has the following problems:

(1) Since the label conducts two Hash computations and one encryption operation, it has too big operation burden with very high costs.
(2) When a reader sends $H(ID_t,R)\|H(t_T)\|H(t_R)$ to a label，if an attacker falsifies the $H(ID_t,R)$，then the reader can not pass the label authentication, and the label secret key will not be updated. Now, the secret key of the database has been updated. In the next authentication, the legitimate labels will become illegitimate.
(3) When a label sends $H(ID_T)\|H(ID_R,R)\|K_{Key}(R)\|H(t_T)$ to a reader，if an attacker falsifies the $H(ID_R,R)$，then the label can not pass the database authentication but the database can not pass the reader authentication. As a result, the database secret key is updated but the label secret key is not updated. The next authentication will face some problems;
(4) An attacker can position and track a label through $H(ID_T)$.

 

Literature [5] proposed a RFID secure authentication protocol based on Hash function. The protocol authentication processes are described as follows:

(1) A reader generates a random number R，and sends a Query request and R to a label；
(2) After receiving the request，the label calculates $H(ID_t)$ and $H(ID_t \| R)$，and sends $H(ID_t)$ and $H(ID_t \| R)$ to the reader；
(3) The reader calculates $H(ID_r)$ and $H(ID_r) \oplus H(ID_t \| R)$，and sends R, $H(ID_t)$, $H(ID_r) \oplus H(ID_t \| R)$ to the database；
(4) The database checks whether there is a label equal to $H(ID_t)$. If yes，then it passes the authentication, otherwise, the authentication fails. The database works out $H(ID_r)$ according to $H(ID_t)$，R and $H(ID_r) \oplus H(ID_t \| R)$, finds the corresponding $ID_r$, and sends $ID_r \oplus ID_t \oplus R$ to the reader；
(5) the reader works out the label identification $ID_t$ from $IDr \oplus ID_t \oplus R$，R and its identification $ID_r$, calculates $H(ID_t \| R)$，and then sends it to the label;
(6) After receiving the calculation result, the label calculates $H(ID_t \| R)$ through stored $ID_t$ and R. Meanwhile, it is compared with the one sent from the reader. If they are equal, then it passes the authentication, otherwise, the authentication fails.

The protocol has the following problems:

(1) Since the $H(ID_t)$ sent from the label is a fixed value, an attacker can position and track the label through $H(ID_t)$；
(2) The reader uses $H(ID_t \| R)$ to verify the label, and the label also uses $H(ID_t \| R)$ to verify the reader in the same way. An attacker can intercept $H(ID_t)$ and $H(ID_t \| R)$，and then send $H(ID_t \| R)$ to a label so that it can gain the trust from the label and thus conduct spoofing；
(3) The computation burden of both labels and readers is huge. Once putting into operation, it may cause slow operation of the system.
(4) The paper starts from b implementing a Hash function and random number generator suitable for RFID, to fundamentally solve the problems of RFID bi-directional authentication protocol, and designs a RFID bi-directional authentication protocol with practical value.

## 2. Coupled Dynamic Integer Tent Map Lattices

### 2.1 Dynamic Integer Tent Map [10]

Tent map is an extremely simple chaotic dynamics model, which controls the two straight lines of the tent through parameter *a*. The expression of tent map is illustrated in the formula (1):

$$x_{i+1} = \begin{cases} \dfrac{x_i}{\alpha}, & 0 \le x_i \le \alpha \\ \dfrac{1-x_i}{1-\alpha} & \alpha \le x_i \le 1 \end{cases} \tag{1}$$

The size of *a* determines the location of mapping center. when $a$=0.5，it is called standard tent map. The expression of standard tent map is illustrated in the formula (2):

$$x_{i+1} = \begin{cases} 2x_i & 0 \le x_i \le 0.5 \\ 2(1-x_i) & 0.5 \le x_i \le 1 \end{cases} \quad (2)$$

One of the excellent characteristics of tent map is its uniformly distributed functions. Since tent map is featured with high ergodic property, random moments, and initial value sensitivity, it can meet the requirement of cryptographic algorithm on diffusion property.

The standard tent map (formula 2) is equally converted from real number field operations to integer operation (Given that binary digits of integer are n).

$$F_\alpha : \quad x_{i+1} = \begin{cases} 2x_i + 1, & x_i \in [0, \quad 2^{n-1}) \\ 2(2^n - 1 - x_i), & x_i \in [2^{n-1}, 2^n - 1] \end{cases} \quad (3)$$

Formula (3) is integer tent map, and map $F_a$ could be expressed by broken lines, and is uniformly distributed on [0, $2^n$-1]. Integer tent map maintains the elongation and folding properties of real number field tent map. Its stretching property leads to exponent separation of consecutive points, and its folding property maintains a bounded generation sequence and leads to the mapping irreversible.

Since the map $F_a$ is defined within the finite field, the generated iterative sequence inevitably enters into periodic states and even some periodic points with small length occur.

In order to avoid short cycle of integer tent map, the tent map and modular operation are combined, and the integer tent map is dynamically extended, to get new map model, which is illustrated as follows:

$$F_\beta : \quad x_{i+1} = \begin{cases} 2g_i + 1, & g_i \in [0, \quad 2^{n-1}) \\ 2(2^n - 1 - g_i), & g_i \in [2^{n-1}, 2^n - 1] \end{cases} \quad (4)$$

therein，

$$g_i = (x_i + k_i) \bmod 2^n \quad (5)$$

In $F_\beta$ map (Figure 1), dynamic parameter $k_i$ controls the horizontal migration of the "tent". $k_i$ stands for the distance of the migration of the "tent" along horizontal axis.

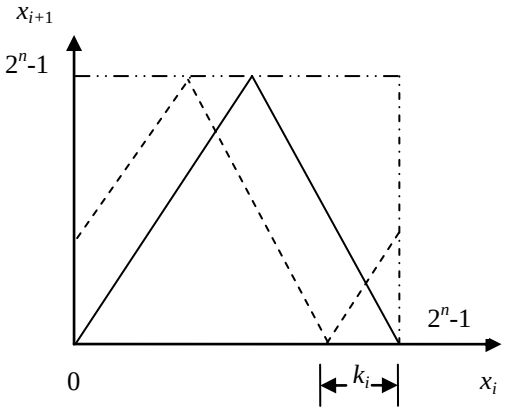


**Figure 1. Dynamic Integer Tent Map**

In iterative operation, $k_i$ will have different values along with the change of iteration step number $i$. In each iterative operation, the "tent" in the Figure 2 is moving and changing, so it is called dynamic integer tent map. Definitional domain of the dynamic integer tent map is [0, $2^n$-1].

Figure 2 shows the mapping sequence distribution after changing the step-

 

size of the dynamic parameter $k_i$. The dynamic parameter $k_i$ of each iteration is $4*i$ ($i$ is the current iteration step number).

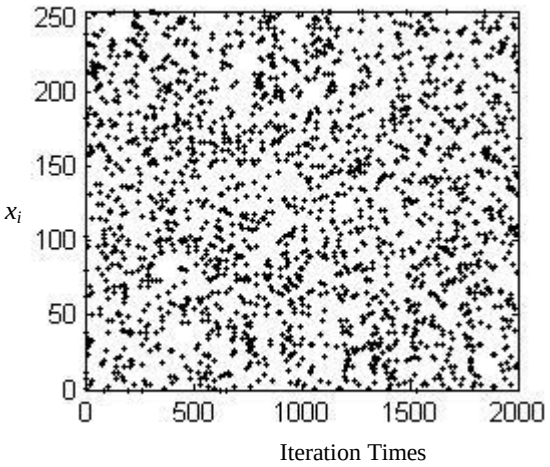


**Figure 2. Time Sequence Generated by Dynamic Integer Tent Map**

### 2.2 Dynamic Coupled Integer Tent Map Lattices Model (*DCML*)

Coupled Map Lattice (*CML*) is an extremely important model type for studying nonlinear space-time chaotic behaviour, and the selected nonlinear function, size of the system lattice, coupling coefficients, and nonlinear function parameters will affect the complexity of sequence generated from *CML* and thus affect the security of its constructed cryptosystem. In order to keep the uniform distribution of time sequence generated by the system, the *CML* structure is improved, namely, by taking dynamic integer tent map as the nonlinear function of *CML*. The coupled mode is expressed as formula (6) [11].

$$x_i(n+1) = (f(x_i(n) + f(x_{i-1}(n)) + f(x_{i+1}(n))) \bmod 2^k \quad (6)$$

In the formula, $x_i(n+1)$ stands for the status value of the $(n+1)^{th}$ step iteration of the $i^{th}$ lattice, and $f(\cdot)$ stands for nonlinear function of lattice. Here it is the dynamic integer tent map (formula (4)), and mod stands for modular operation; $2^k$ is the status number of lattice value. Each lattice point value is determined by three lattice points of previous step iteration, and each lattice point can affect the three lattice points of the next step iteration, which realizes the coupling between lattice points, and is conductive to the confusion and diffusion of information.

Spatiotemporal chaos behaviour of *DCML* is illustrated in the Figure 3. There are 32 lattice points, and each lattice point value is an 8 digital unsigned integer. Namely, the maximum value of lattice points is 255. Lattice point initial value $x_0 = [1\ 2\ 3\ 4\ \ldots\ldots\ 32]^T$.

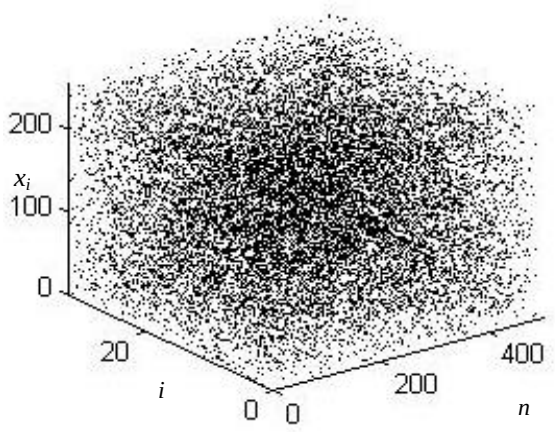


**Figure 3. Spatiotemporal Series of Dynamic Coupled Integer Tent Map**

### 2.3 DCML is used to Build Hash Function and Generate Random Numbers

RFID is featured with low computation capacity, limited storage resources, short wireless communication distance, large number of nodes, low costs, and small size.

Limited by computation resources, the conventional Hash functions and random number generation algorithms suitable for Internet are not universally applicable. Currently, many RFID chips employ a single-byte computing model (word length is a byte). Therefore, it is necessary to build a light weight Hash function and random number generator, which takes a single byte as its processing unit, so as to meet the special requirements of RFID.

The general process of building a one-way Hash function based on DCML is described as follows:

1) The original data M is divided into single-byte message blocks of $M_0$, $M_1$,…,$M_{t-1}$. If the original data size is few than 8 bytes, then 1010……sequences are supplemented, making their length t=8.
2) Given that L=t, single-byte message blocks ($M_0$, $M_1$,…,$M_{t-1}$) are assigned to initial vectors($x_0(0)$, $x_1(0)$, …, $x_{L-1}(0)$) of DCML model.
3) The DCML model (formula(6)) is iterated for (t+10) rounds，the last iteration result is taken out, and the first 8 components are connected as the last 64bit Hash values.

Above algorithm uses dynamic coupled tent map lattices to conduct massage confusion and diffusion. Since it is featured with even distribution, with good unipolarity and strong collision resistance, it is conductive to improve the balance degree of Hash function. Simple operations are employed within the limited integer set, which facilitates the hardware and software implementation in the RFID system and has high implementation efficiency.

The general process of random number generation based on DCML is described as follows:

1) Initial value vectors ($s_0(0)$, $s_1(0)$, …, $s_7(0)$)：

i. 0x01,0x89,0x32c,0xba,0x02,0xfd,0x45,0xcd.

2) Disturbance vectors：Any Hash result will be taken as a disturbance vector ($r_0(0)$, $r_1(0)$, …, $r_7(0)$)。
3) The relationship between initial value vector and disturbance vector is xor，as the initial vector of iterative operation ($x_0(0)$, $x_1(0)$, …, $x_7(0)$).
4) The DCML model (formula(6)) is iterated for 10 rounds，the last iteration result is taken out, and the 8 components are connected as the last 64bit random numbers.

 

Above function is recorded as **H**(·), and the generated random number is recorded as **r**. A RFID bi-directional authentication protocol is built based on this.

## 3. RFID Bi-Directional Authentication Protocol based on Random Numbers and Hash Function

Random numbers and Hash function are employed to build secure RFID bi-directional authentication protocol. Before being generated, each label needs to have a secret value S shared with backend database in addition to store its identification ID. A built-in random number generator is placed in the reader, and all of identification $ID_i$ as well as secret value $S_i$ corresponding to $ID_i$ are stored in the backend database. The protocol process flow is illustrated in the Figure 4.

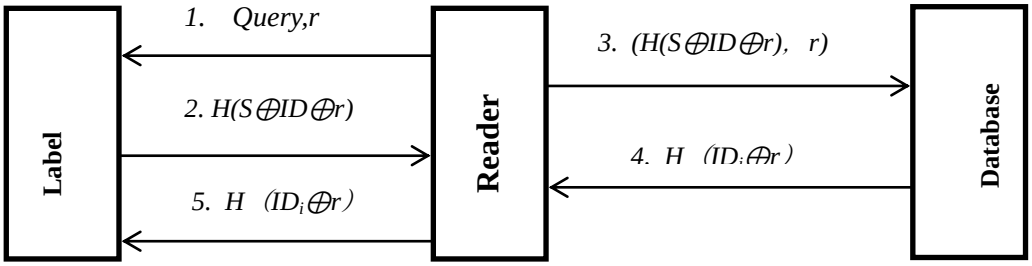


**Figure 4. The Flow Chart of a Randomized RFID Bi-Directional Authentication Protocol based on Hash Function**

### 3.1 Authentication Process

(1) *R-T*： reader generates a random number *r,* and sends the r and a Query authentication request to a label；

(2) *T-R*：After receiving the request, the label calculates the $H(S \oplus ID \oplus r)$，and sends the result to the reader and stores *r*；

(3) *R-D*：after receiving $H(S \oplus ID \oplus r)$ from the label，the reader will send it and r to database；

(4) *D-R*：database query is conducted and the calculation is made to identify whether there is a data pair$(ID_i,S_i)$, which allows $H(S_i \oplus ID_i \oplus r)= H(S \oplus ID \oplus r)$; If it does not exist, the authentication fails；If it exists，then the calculation is made in database and the $H(ID_i \oplus r)$ is sent to the reader；

(5) *R-T*：after receiving the $H(ID_i \oplus r)$ from database，the reader will forward it to the label. After receiving $H(ID_i \oplus r)$，the label will calculate $H(ID \oplus r)$，and verify whether $H(ID \oplus r)$ is equal to $H(ID_i \oplus r)$. if yes, then it passes the verification, otherwise, it fails to pass the verification.

### 3.2 Performance Analysis

(1) Confidentiality: the Hash value acquired from Hash computation is transmitted during the interaction between reader and label. Even if an attacker intercepts transmitting information, he/she is not able to get the real message.

(2) Integrity：due to unidirectivity of *Hash* function，if transmitting data are falsified，they can not pass authentication, so that the integrity of the transmitting data is ensured；

(3) Security：Since the random numbers of each authentication are different, each Hash value is also different. Therefore, even if attracter intercepts the current information, it can not be used during next authentication.

(4) Database computation burden is small：Assuming that labels with the number of N are stored in the database, then the average computation burden of the database is *(1+N/2)H* (*H* stands for *Hash* computation) and some simple exclusive-or operation. Therefore, the database is more efficient with small computation load.
(5) Bi-directional authentication between label and database is achieved. The validity of labels is verified by database through *H(S ⊕ID ⊕r), and the* validity of database is verified by label through $H(ID_i \oplus r)$;
(6) It has effectively solved many insecure problems.

1) Preventing unauthorized read： The data on labels can only be read through authenticated reader, so that the unauthorized read is effectively avoided.
2) Preventing location tracking: during the process of each authentication, Hash value is different due to different random numbers, and the last authentication information is different with the current one, so that location tracking is effectively avoided.
3) Preventing eavesdrop：Since message is transmitted through Hash computation, and the Hash value cannot reversely derive the real message, attackers are not able to get real information, and thus it can effectively prevent the eavesdrop;
4) Preventing counterfeit：both *ID* and *S* are confidential information of the system， attackers are not able to forge *H(S ⊕ID ⊕r)* and $H(ID_i \oplus r)$， and thus they can not forge label and reader;
5) Preventing replay; due to different random number r, even though attacker intercepts the *H(S ⊕ID ⊕r)* this time, they are not able to simulate the *H(S ⊕ID ⊕r)* of the next time, and thus the replay attack is effectively prevented.

### 3.3 Performance Comparison

This protocol has overcome the safety defects existing in hash lock protocol, randomized Hash locking protocol and Hash chain protocol, as well as in *RFID bi-directional authentication protocol and RFID security authentication protocol based on Hash function.* Its performance comparison is illustrated in the Table 1, and the efficiency comparison is illustrated in the Table 2. In Table 1, √ stands for secure, × stands for insecure; In Table 2, L stands for the length of the ID, secret and secret key, r stands for the random number and timestamp, and H stands for Hash function.

**Table 1. Security Comparison**

| | *Hash* Locking *protocol* | random *Hash* Locking protocol | *Hash* Chain protocol | RFID Mutual Authentication Protocol Based on Random Number and Hash Function | RFID Security Authentication Protocol Based on Random Number and Hash Function | Protocol in this paper |
|---|---|---|---|---|---|---|
| Anti tracks | × | × | √ | × | × | √ |
| Anti-hacking | × | × | √ | √ | √ | √ |
| Replay attack prevention | × | × | × | √ | √ | √ |
| Security equipment coaxing | × | × | × | √ | × | √ |
| Mutual authentication | √ | √ | × | √ | √ | √ |
| A distributed environment | √ | √ | √ | √ | √ | √ |

 

**Table 2. Protocol Efficiency Comparison**

| | *Hash* Locking *protocol* | random *Hash* Locking protocol | *Hash* Chain protocol | RFID Mutual Authentication Protocol Based on Random Number and Hash Function | RFID Security Authentication Protocol Based on Random Number and Hash Function | Protocol in this paper |
|---|---|---|---|---|---|---|
| Label Computation | *1H* | *1H,1r* | *2H* | *3H,2r, 1L* | *3H,1r* | *2H* |
| reader computation | — | *(n/2)H* | — | *1H, 1r* | *2H, 1r* | *1r* |
| database computation | — | — | *(tn/2)H* | *(2+n/2)H, 1L, 1r* | *(1+n/2)H* | *(1+n/2)H* |
| Label storage space | *2L* | *1L* | *1L* | *2L* | *1L,1r* | *2L, 1r* |
| reader storage space | — | — | — | *1H* | *1L, 1r* | *1r* |
| database storage space | *3nL* | *nH* | *2nL* | *3nL* | *2nL* | *2nL* |

## 4. The Proof of BAN Logic

BAN logic is the logic used for formalized analysis of authentication protocol proposed by scientists of DEC of USA, Burrows, Abadi and Needham, and it is based on the belief logic reasoning mode[12]. During the reasoning process, the principal belief of the protocol changes along with thechange of message. The break of cryptographic algorithm adopted by the protocol is not considered during the BAN logical proof; the protocol is firstly "idealized" and transformed into BAN logical formula, and then we make reasoning according to reasonable hypothesis and inference rules, so as to figure out whether the protocol will realize its expected objective [13].

### 4.1 Primary Inference Rule

(1) Rule of message meaning reasoning

The inference rule of message means of shared key:

$$\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q, P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$$

If P believes K is the session key between P and Q, and P has received the X encrypted by K, then P believes that Q has sent message to X at a time.

Rule of asymmetrical secret key message meanings:

$$\frac{P|\equiv \overset{K}{\longrightarrow}Q, P\triangleleft\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$$

If P considers K is the public key of Q, and P has received message X encrypted by private key of Q at a time, then P believes that Q has sent message X.

Rule of shared secret message meaning:

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

If P believes Y is the shared secret between P and Q, and P has received message X encrypted by K, then P believes that Q has sent message X at a time.

(2) Rule of fresh reasoning

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

If P believes that Q possesses arbitration right to X, and P believes that Q believes X, then P believes X.

(3) Rule of arbitration

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

If P believes that Q possesses arbitration right to X, and P believes that Q believes X, then P believes X.

(4) Rule of reception

$$\frac{P\triangleleft(X,Y)}{P\triangleleft X,P\triangleleft Y}$$

If P has received the cascade of X and Y, then P has received both X and Y.

$$\frac{P\triangleleft(X)_Y}{P\triangleleft X}$$

If P has received message X encrypted by secret Y, then P has received message X.

$$\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,P\triangleleft\{X\}_K}{P\triangleleft X}$$

If P believes K is the shared secret key of P and Q, and P has received message X encrypted by K, then P has received message X.

$$\frac{P|\equiv\overset{K}{\longrightarrow}Q,P\triangleleft\{X\}_{K^{-1}}}{P\triangleleft X}$$

If P believes K is a public key of Q, and P has received message X encrypted by private secret key of Q, then P has received or seen message X.

$$\frac{P|\equiv\overset{K}{\longrightarrow}P,P\triangleleft\{X\}_K}{P\triangleleft X}$$

If P believes K is its public key, and P has received ciphertext of message X, which is encrypted by K, then P has received message X.

(5) Rule of fresh judgment

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

If P believes that message X is fresh, then P believes that the message, which is cascaded by X and Y, is fresh.

### 4.2 Proof of Protocol

**4.2.1 Protocol Idealization:** We know that the channel between reader and database is secure, so it is taken as the R as a whole.

$$M1: R\rightarrow T: Query, r$$
$$M2: T\rightarrow R: H(S\oplus r\oplus ID), r$$
$$M2: R\rightarrow T: H(r\oplus ID)$$

In the idealized model of the protocol, M1 can be removed as it has no meaning to the analysis of protocol.

$$M2: T\rightarrow R: H(S\oplus r\oplus ID), r$$
$$M2: R\rightarrow T: H(r\oplus ID)$$

 

**4.2.2 The Primary Hypothesis of Protocol and its Objective:** The primary hypothesis of the protocol:

1) $R|\equiv \#(r)$ 2) $T|\equiv \#(r)$ 3) $R|\equiv R\overset{r}{\longleftrightarrow}T$ 4) $T|\equiv T\overset{r}{\longleftrightarrow}R$

5) $R|\equiv T|\Rightarrow ID$ 6) $T|\equiv R|\Rightarrow ID_i$ 7) $R|\equiv R\overset{S}{\rightleftarrows}T$

Objective of the establishment of protocol:

1) $R|\equiv ID$ 2) $T|\equiv ID_i$

**4.2.3 Proof of Authentication Protocol**

(1) Prove: $R|\equiv ID$

By $R|\equiv R\overset{S}{\rightleftarrows}T$ *and* Inference rules $\dfrac{P|\equiv P\overset{Y}{\rightleftarrows}Q, P\lhd <X>_Y}{P|\equiv Q|\sim X}$ available:

$\dfrac{R|\equiv R\overset{S}{\rightleftarrows}T, R\lhd\{r, ID\}_S}{R\lhd(r, ID)}$ deduced $R \lhd (r, ID)$

By $R|\equiv \#(r)$ *and* Inference rules $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$ available:

$\dfrac{R|\equiv \#(r)}{R|\equiv \#(r, ID)}$ deduced $R|\equiv \#(r, ID)$

By $R|\equiv R\overset{r}{\longleftrightarrow}T$ *and* Inference rules $\dfrac{P|\equiv P\overset{K}{\longleftrightarrow}Q, P\lhd\{K\}_K}{P|\equiv Q\sim X}$ available:

$\dfrac{R|\equiv R\overset{r}{\longleftrightarrow}T, R\lhd\{ID\}_r}{R|\equiv T\sim ID}$ deduced $R|\equiv T\sim ID$

By $R|\equiv \#(ID), R|\equiv T|\sim ID$ and Inference rules $\dfrac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$ available:

$\dfrac{R|\equiv \#(ID), R|\equiv T|\sim ID}{R|\equiv T|\equiv ID}$ deduced $R|\equiv T|\equiv ID$

By $R|\equiv T|\Rightarrow ID, R|\equiv T|\equiv ID$ and Inference rules $\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$ available:

$\dfrac{R|\equiv T|\Rightarrow ID, R|\equiv T|\equiv ID}{R|\equiv ID}$ deduced $R|\equiv ID$

(2) Prove: $T|\equiv ID_i$

By $T|\equiv \#(r)$ and Inference rules $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$ available:

$\dfrac{T|\equiv \#(r)}{T|\equiv \#(r, ID_i)}$ deduced $R|\equiv \#(r, ID_i)$

By $T|\equiv R\overset{r}{\longleftrightarrow}T$ and Inference rules $\dfrac{P|\equiv P\overset{K}{\longleftrightarrow}Q, P\lhd\{K\}_K}{P|\equiv Q\sim X}$ available:

$\dfrac{T|\equiv R\overset{r}{\longleftrightarrow}T, T\lhd\{ID_i\}_r}{T|\equiv R\sim ID_i}$ deduced $T|\equiv R\sim ID_i$

By $T \mid\equiv \#(ID_i)$ 和 $T \mid\equiv R \sim ID_i$ and Inference rules $\dfrac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$ available：

$\dfrac{T\mid\equiv\#(\mathrm{ID}_i),T\mid\equiv R\mid\sim\mathrm{ID}_i}{T\mid\equiv R\mid\equiv\mathrm{ID}_i}$ deduced $T \mid\equiv R \mid\equiv ID_i$

By $T \mid\equiv R \mid\Rightarrow ID_i$ 和 $T \mid\equiv R \mid\equiv ID_i$ and Inference rules $\dfrac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$

available：

$\dfrac{T\mid\equiv R\mid\Rightarrow\mathrm{ID}_i,T\mid\equiv R\mid\equiv\mathrm{ID}_i}{T\mid\equiv\mathrm{ID}_i}$ deduced $T \mid\equiv ID_i$

## 5. Conclusion

RFID is replacing traditional barcode, but its application is limited because the data transfer between label and reader is vulnerable to external attack. This paper, after having analyzed the security problems of RFID technology, has designed and strictly proved a safer and more efficient bi-directional authentication protocol of RFID based on Dynamic Coupled Integer Tent Map, which can be widely applied in military, aviation, transportation, manufacture, medical and logistics sectors.

## Acknowledgements

This work described in this paper was supported by the Beijing Natural Science Foundation Project, China (No.4112018).

## References

[1] D. Ranasinghe, D. Engels, P. Cole, “Low-cost RFID systems: Confronting security and privacy [C]”, Proc of the Auto- ID Labs Research Work shop. Cambridge, MA: Auto-ID Labs, (**2004)**.
[2] J Kwak, K. Rhee, S Oh, *et al*. “RFID system with fairness within the framework of security and privacy [C]”.,Proc of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks. Berlin: Springer, (**2005)**, pp. 142-152.
[3] D Zhenhua ,L Jintao , F Bo ., “RFID authentication protocol Based on Hash functions[J]”.Computer research and development, vol. 46, no. 4, **(2009)**, pp. 583- 592.
[4] C Keli, G Chunsheng, “A two-layer / Mutual authentication of the random Hash Lock RFID Security Protocol [J]”. Application of electronic technology . no. 11, **(2008)**, pp. 46-149.
[5] S. Sarma, S. WEIS S, ENGELS D. RFID systems and security and privacy implications[C]. Proc of CHES’02 Springer, (**2002)**, pp. 454-469.
[6] S WEIS, S SARMA, R RIVEST R. Security and privacy aspects of low-cost radio frequency identification systems[C]. Proc of Security in pervasive Computing’04, (**2004)**, pp. 201- 212.
[7] M OHKUBO, K SUZUKI, S KINOSHITA, “Cryptographic approach to privacy-friendly tags[C]”. Proc of RFID Privacy Workshop, USA MIT, (**2003)**.
[8] Z Nan , Chen Jianying , Fu Chun . RFID mutual authentication protocol Based on Hash functions [J]. Journal of Southwest University for nationalities, vol. 38, no. 6, (**2012)**, pp. 969-972.
[9] L Mingsheng , Wang Yan, Xin sheng Zhao. RFID research of security authentication protocol Based on Hash functions[J]. Chinese Journal of sensors, vol. 24, no. 9, (**2011)**, pp. 1317-1321.
[10] L Jiandong. One-way Hash Function based on Integer Coupled Tent Maps and Its Performance Analysis[J]. Journal of Computer Research and Development, **2008,** no.3, pp. 563-569 (in Chinese)
[11] L Jiandong, Yang Kai, Yu Youming. Improved Coupled Tent Map Lattices Model and Its Characteristic Analysis[J]. Journal of Computer Research and Development, vol. 48, no. 9, **(2011)**, pp. 1667-1675 (in Chinese).
[12] M. Burrows , A. Abadi M, Needham R. Logic of Authentication [J]. ACM Transactions on Computer Systems, vol. 8, no. 1, **(1990)**, pp. 18-36.
[13] Needham, “Using encryption for authentication in large networks of computers [J]”. Communications of the ACM, vol. 21, no. 12, **(1978)**, pp. 993- 999.

 

## Authors

**LIU Jiandong**, born in 1966. He has been professor of Beijing Institute of Petrochemical Technology since 2008. His main research interest is chaos cryptography.

**ZHANG Xiao**, born in 1991. He has been postgraduate student of Beijing University of Chemical Technology since 2010.His main research interest is hash function.

**WANG Yequan**, born in 1991. He has been postgraduate student of Beijing University of Chemical Technology since 2009. His main research interest is chaos cryptography.

**SHANG Kai**, born in 1992. He has been postgraduate student of Beijing University of Chemical Technology since 2011.9.His main research interest is chaos cryptograph.