Light weight one-time pad RFID bidirectional authentication protocol research

Xiaohong Zhang*, **Juanfeng Xiao, Lifeng Dong**

School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China

Received 1 October 2014, www.cmnt.lv

Abstract

Today the RFID system is widely applied in the open system environment, the communication between reader and tags is easily influenced by a various kinds of interferences and attacks, so the safety performance is threatened. This paper proposes a light weight one time pad RFID security authentication protocol, associates chaotic map with hash function. In the certification process, this protocol takes a filtering operation, reduces the back-end database search calculation load, and avoids pretence, retransmission attack, tracking and so on. At the same time, takes some flag variable of the RFID system as the initial value of chaotic mapping and parameters, combines with the certification process to make the original information position scrambling, then executes XOR or encryption. Experiment simulation results show that this scheme security relies on the RFID system itself parameters and encryption process, so can solve the RFID system problem of illegal access, forge coaxing, data leakage and so on.

Keywords: RFID, light weight, bidirectional authentication protocol, hash function, chaotic map

1 Introduction

RFID (Radio Frequency Identification) is a non-contact automatic identification technology [1], its fundamental is to use transmission characteristic of space coupling of radio frequency signal (inductive coupling or electromagnetic backscatter coupling) to realize the automatic identification of identified objects. Generally, RFID system consists of RFID tags, RFID readers and back-end database [2]. The communication between tags and readers is in the wireless, non-contact channel, so it is easily affected by electromagnetic interference, reflection caused by external environment like metal, water, buildings, etc. Thus it is often caused malicious tracking and damage by attacker, and existing potential risks in the course of communication between readers and tags.

The higher working frequency of RFID system is, the faster communication speed is, but the working distance will be much longer, obviously in the process of communication, more and more interferences and attacks would be received, security threats of the system may also increase. RFID security threats mainly include two factors: one is the communication between tag and reader, which is processing in an unsafe air channel. All of data and information transmitted are exposed out of channel with plaintext, so that privacy of data is threatened. Second, the limitation of computing power and memory resources of tags and readers, especially the limitation of design cost of passive RFID tag, which makes the traditional data encryption algorithms cannot meet the RFID system security requirements very well.

RFID systems security issues include two aspects: identity authentication and privacy protection [3]. Identity authentication refers to the bidirectional recognition between tags and readers. Privacy protection mainly includes two aspects: data confidentiality and credibility. Currently, RFID security mechanism mainly has physical mechanism and password system [4]. Physical mechanism includes kill tags, blocker tags, frequency hopping communication technology, etc. Physical method will add additional physical devices or components, which causes inconvenient and increase the cost. Hash function [5] is considered to be a lightweight cryptography. Tags only need simple implements hash function and bit operation, with their advantages of less calculation and easy realization in RFID chip. Hash function’s irreversibility could guarantee RFID system security. So RFID security authentication based on hash function has been widely researched and applied. Combined sensitive of chaotic map to initial value and characteristic of generating noise-like sequence, this paper proposes a RFID data encryption bidirectional authentication protocol scheme, which meanwhile solves identity authentication between tags and readers of RFID system, authority authentication of reader-writer and privacy of data, well coordinate the problems of safety, efficiency and tags cost.

2 RFID encrypted encryption mutual secure security authentication

There are mainly 3 kinds of typical RFID security protocols based on one-way hash function: Hash-Lock protocol, random Hash-Lock protocol and Hash-Lock chain protocol [6]. Hash-Lock protocol introduces hash function to authentication, it enhances RFID message one-way characteristic. Random Hash-Lock protocol

[*] ***Corresponding author’s*** e-mail: xiaohongzh@263.net

introduces random number *R* based on Hash-Lock protocol, it realizes dynamic refresh of tag ID. But tag ID is transmitted in the form of plaintext with previous two protocols, which can be intercepted, replayed and cheated by attackers; Hash-Lock chain protocol realizes dynamic refresh of tag ID by means of secret-sharing, but it is a one-way authentication protocol and background database has a heavy computation. These 3 kind protocols all can realize database's authentication to tags which reach forward security. In frequently go in and out special systems, like access control, library book management, non-stopping toll, etc, tags need to be read and reused for many times, these 3 kind protocols don't have memory function, can not reach RFID system's fast recognition. This paper proposes a new RFID bidirectional authentication protocol based on chaotic encryption, when tags enter into read-write range of a reader, the reader will do a tag filter operation, so it can reduce tag recognition time and enhance system-running efficiency.

2.1 IMPROVED RFID MUTUAL SECURITY AUTHENTICATION PROTOCOL

RFID bidirectional authentication is a mutual identity process between tags and readers, the key of one-time pad used is random and is only used once, it is a ideal encryption scheme which unlikely to be broken. The mutual authentication between tags and readers and one-time pad can solve problems of user privacy and tag clone. A sketch of this protocol is shown in Figure 1.

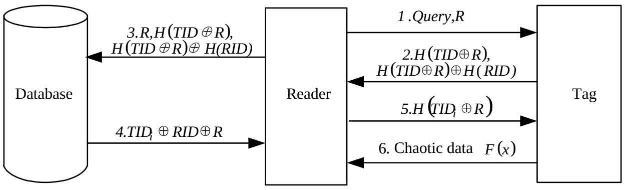

FIGURE 1 One-time pad RFID bidirectional authentication protocol

The symbols used in this paper are given as follows:

RID and *TID*: reader and tag identify;

$F(x)$: chaotic encryption data send to reader by tag;

$H(\cdot)$: one-way hash function calculation;

R: random data generated by reader;

$\oplus$: binary XOR operation;

Background database stores all tags *RID* and corresponding legal *TID*;

Reader stores itself *RID*;

Tag stores itself *TID* and corresponding legal *RID*.

Specific authentication steps are shown as below:

Step 1: Reader sends out a *query* to tags $Reader \to Tag$

The reader sends out a authentication query to tags within its working range, meanwhile generates random number *R*, and send to tags together. Then three kinds of results may happen:

1) no tag responses.

2) one tag responses.

3) multi-tags response.

When multi-tags response, a conflict will be caused, the reader will do a conflict arbitration, the reader will choose a tag to interact information after the arbitration.

Step 2: Tag response to the reader $Tag \to Reader$.

The selected tag responses the query of the reader, saves random number *R*, obtains its *TID* and its reader *RID* which with permission of read and write, calculates $H(TID \oplus R), H(TID \oplus R) \oplus H(RID)$ separately, sends to the reader as response.

Step 3: Reader filters and transmits data $Reader \to Database$

After receiving $H(TID \oplus R)$, $H(TID \oplus R) \oplus H(RID)$ of the tag, working out $H(RID)$, the reader makes a filter operation. According to its $RID^{'}$, the reader works out $H(RID^{'})$, then judges whether $H(RID)$ and $H(RID^{'})$ are equal.

If equal, the tag could go through the authentication of the reader, meanwhile data of $R, H(TID \oplus R), H(TID \oplus R) \oplus H(RID)$ will be transmit to database.

Otherwise, the reader filters the tag.

Step 4: Database filters the tag and/or the reader $Database \to Reader$.

Database will check whether exits a tag TID_i, which makes $H(TID \oplus R)$ equals to $H(TID_i \oplus R)$ after receiving the date from the reader?

If exist, the tag is legal, then checks whether exits the corresponding legal RID_i?

1) If exit, database realizes authentication for the reader, then calculates $RID_i \oplus TID_i \oplus \mathrm{R}$ and sends it to the reader;

2) Otherwise, the reader is illegal;

Otherwise, the tag is illegal.

Step 5: The reader memory the legal tag $Reader \to Tag$

After receiving data $RID_i \oplus TID_i \oplus \mathrm{R}$ from the database, according to its RID and R, the reader works out TID, updates and saves it, then calculates RID and sends to the tag.

Step 6: The tag authentication for the reader $\{x_n\}$

The tag calculates and judges whether $H(TID \oplus R)$ equals to $H(TID_i \oplus R)$ by its TID?

1) If equals, the tag realizes authentication for the reader, then the tag can send chaotic encryption data $F(x)$ to the reader;

2) Otherwise, the authentication is failure.

According to its RID, saved TID_i and random number *R*, the reader could work out the original data of the tag; otherwise, the tag fails to response.

2.2 SECURITY ANALYSIS OF IMPROVED PROTOCOL

1) Against replay, eavesdropping and position tracking attacks: in the course of communication, effective data which are used forauthentication are confused by random number R, then do the Hash function computing. Hash function's one-way and random number R make effective data can not be predictable. If an attacker intercepts the previous data, he can not predict and control the following effective data, so can effectively prevent from replay attacks. As one-way property of Hash function and co-function with random number R, attackers could not restore the true effective parameters, which could avoid effectively eavesdropping and position tracking caused by fixed output.

2) Against imitated attack, forward safety, bidirectional authentication: in step 3, the reader uses its RID' to verify the tag; In step 4, the database verify the tag and the reader, so meet the requirement of forward safety; In step 5, the tag realizes authentication of reader legality. For the chaotic encrypted data $F(x)$, only true parameter of RFID system can verify data credibility, so realize twice bidirectional authentications between the tag and the reader, so that prevent illegal or counterfeit readers or tags from participating conversation with the tag, enhance the safety and reliability of the protocol.

In order to clearly make a safety performance of authentication comparison between this paper and reference [6], specific comparison of safety function will be given in Table 1.

The notations are given as follows: √ means have this function; × means not.

3) Recognition efficiency: the protocol filters tags first in step 3, only tags which store legal reader's RID could go through tag authentication by readers, if not, the reader will ignore tags, which could avoid attackers resend data to back-end database, meanwhile reduce search computing load of back-end database, enhance the recognition efficiency of the system.

Efficiency performance of authentication protocol mainly includes calculating amount and storage capacity. Table 2 is the comparison of efficiency performance, the notations are given as follows: H stands for Hash computing, R stands for random number; N stands for tag number; L stands for length of tag's TID and reader's RID. (Generally consider lengths of TID and RID are the same.)

TABLE 1 Safety performance comparison

Safety performance index	**Forward safety**	**Against replay**	**Against eavesdropping**	**Against tracking**	**Against counterfeit**	**Bidirectional authentication**
Hash-Lock	√	×	×	×	×	×
Random Hash-Lock	√	√	√	√	×	×
Hash-Lock chain	√	×	√	√	×	×
Improved protocol	√	√	√	√	√	√

TABLE 2 Efficiency performance comparison

Protocols	**Calculated amount**			**Storage capacity**		
	Tag	Reader	Database	Tag	Reader	Database
Hash-lock	1H	/	/	2L	1L	3L
Random Hash	1H,1R	$\frac{N}{2}H$	/	1L	1L	1L
Hash chain	2H	/	$\left(\frac{N}{2}+1\right)H$	1L	1L	2L
Improved protocol	3H	1H,1R	$\frac{N}{2}H$	2L	1L	2L

From Tables 1 and 2, compared to other protocols, security provided by the protocol in this paper can be better and much completer. The reader has memory function, can store legal tag TID and realize twice security assurance of bidirectional authentication. Calculated amount of the tag in this paper is 3H, which is a bit more than other three protocols, but it realizes bidirectional authentication between tags and readers, and tags filtration from the reader. The tag does not need random number generator; it can greatly reduce the tag cost than random Hash protocol. The storage capacity is similar to other protocols, which need small storage, it is suitable for the large-scale RFID system. This protocol has high practical value to balance the tag cost, security and efficiency.

3 Chaotic encryption algorithm design

This paper designs a RFID tag security mechanism which based on chaotic encryption for TID in step 6 Figure 1, encrypting tag secret message before sending to reader. As chaos phenomenon [7] is a deterministic pseudorandom process which appears in nonlinear dynamical systems, its aperiodic, noise-like, wide-spectrum, long-term unpredictable, sensitive to initial conditional, etc, making chaotic system suitable for encryption. This paper chooses chaotic system to generate two encryption sequences, used to RFID tag secret encryption. Then send the cipher text to the reader in air channel, the reader decodes it by the same chaotic sequences, then forwards to database for decode and authentication. As the reader and the tag adopt symmetric encryption mechanism, so in this paper just do RFID tag security encryption research, the security encryption flow chart is shown in Figure 2.

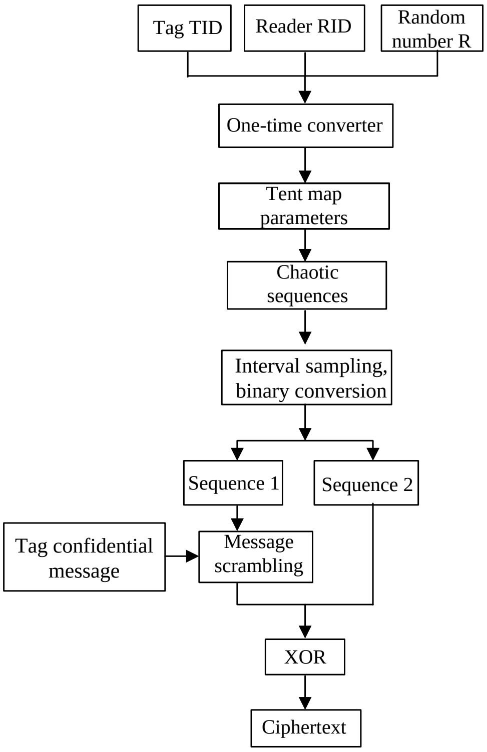

FIGURE 2 RFID tag chaotic encryption algorithm

In consideration of the limitation of RFID tag storage capacity, in this paper the simple one-dimensional Tent map [8] was adopted to generate encryption sequence, reference [9] proves that sequences which generated by this map are chaotic, this map structure is simple and its iteration speed is fast. It completely meets the requirements of characteristics that password sequence has a quick response.

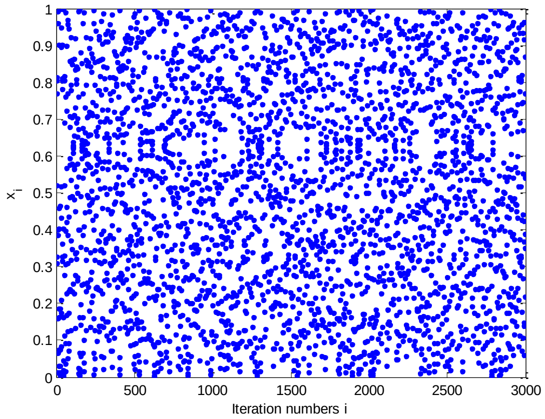

FIGURE 3 Chaotic Tent random distribution

A mathematical model of this one-dimensional Tent map is shown as below:

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

In this mathematical model: α is the parameter, $0 < \alpha < 1$, this map distributes in (0,1). Supposing that $\alpha = 0.3612, x_0 = 0.8515$, iterations $n = 1000$, Equation (1) random distribution is shown in Figure 3.

The above chart shows that this chaos sequence has well noise-like and uniform distribution performance, when initial value x_0, parameter α and chaotic sequence secret keys are unknown, it can ensure their reversibility and property of against forgery of chaos sequences [10].

3.1 ONE-TIME PAD UNIQUE PARAMETER

1) RFID system unique identification: when the manufactures delivery RFID equipments to users, the manufacture will enclose system unique identifications: tag identification TID and corresponding legal reader identification RID.

2) Chaotic map parameter definitio: this paper makes full use of RFID system unique identifications to be chaotic system secret key, which can enhance system security. Tag TID is used in Tent map initial value x_0, it corresponding legal reader RID is used in Tent map parameter α, the random number R, which generated in authentication process, is used in chaotic sequence secret key $r = 789$ ($n_1 = 837$ is the number of chaotic map iterations, $n_2 = 763$ are the value of interval sampling).

3) One-time pad converter: supposing that tag TID, reader RID and random number R are 16 bit binary number. If not, it can be calculate as the same as below method. Converting TID, RID to corresponding chaotic real number x_0, α. The range of TID, RID is $(0, 2^{16}-1)$, x_0 and α calculate factor [11] is:

$$\frac{(1-0)}{(2^{16}-1-0)} = 1.5259 \times 10^{-5} \tag{2}$$

Converting 16 bit binary number x_0 and α to corresponding decimal number, then multiply them by calculate factor, so can get chaotic map parameters x_0 and α. Secret key is $k(n,m,w) = R \oplus (2^{16}-1)$, in which n occupies the first 8 bit, interval sampling value m, w occupy 4 bit, then convert them to real number secret key k.

3.2 REALIZATION OF CHAOTIC ENCRYPTION ALGORITHM

1) Interval sampling: this step is how to get chaotic sequence. Firstly, taking sole identifications TID, RID and random number R of RFID system into one-time pad

converter, they will convert to Tent map corresponding parameters x_0, α and $k(n,m,w)$. Secondly, taking the parameters into Tent map, we can get a sequence $\{x_n\}$. Finally, do the interval sampling operation. Interval each length m,w from $\{x_n\}$ to get two chaotic sequences $\{x_m\}$, $\{x_w\}$, which have same length with tag confidential message. Interval sampling method not only gets rid of chaotic map transition state, but also makes the chaotic sequence deviate from initial value completely. It makes distribution of chaotic sequence more randomized [12] and enhances promiscuous effect of message.

2) Binary conversion: this step is how to get binary sequences. All data used in RFID system is in the format of binary, while all sequences generated by the generator of Tent map are real-value sequences, so real-value sequences have to convert to binary sequences. Real-value sequences $\{x_m\}$ and $\{x_w\}$ divided by 4, keeps three places, then converts to binary sequences 1 and 2 which could be encrypted. As sequences $\{x_m\}$ and $\{x_w\}$ distribute in (0,1), the values when they divide 4 and get three decimal places distribute in (0,250), however the largest eight binary value is 11111111 (255), so the binary sequences 1 and 2 are not overflow.

3) Message scrambling and XOR encryption: the last step is the encryption process. Chaotic sequence 1 is converted to new address of ascending order of numerical value, the tag confidential message has the same address as sequence 1 which after converting. Then XOR encryption operation is done by using scrambled tag message and sequence 2, finally cipher text could be generated.

3.3 CHAOS ENCRYPTION ALGORITHM SIMULATION

Simulation standard data selection:

1) The tag TID is 1000100010001000, its corresponding Tent map initial value is:

$$x_0 = (1000100010001000)_2 \times 1.5259 \times 10^{-5} = 0.5348;$$

2) The reader RID is 0010001000100010; its corresponding Tent map parameter is:

$$\alpha = (0010001000100010)_2 \times 1.5259 \times 10^{-5} = 0.1337;$$

3) In the process of authentication, random number R generated by the reader is 0000000000111010; According to the converted method of one-time pad introduced in the charter 2.1, secret key should be:

$$k(n,m,w) = (0000000000\ \ 111010\ )_2 \oplus (2^{16}\ \text{-}1) = \\ 1111111111\ \ 000101\ = k(512,3,10\ ) ;$$

4) If tag secret massage text is “one world one dream”, its corresponding ASCII code is:
“6f 6e 65 77 6f 72 6c 64 6f 6e 65 64 72 65 64 6d”.

Identifications of RFID system are used as initial parameters value of chaotic system in this paper. if tag TID, reader RID or random number *R* has a tiny change, the encrypted cipher text will be different largely. Table 3 makes a comparison of scrambling message and cipher text when one simulation standard data changes a bit one time.

TABLE 3 Data comparison of RFID tag chaotic encryption (symbol- is space character, bold raise is the changed bit)

	Scrambling data	Ciphertext
Index simulation data	mdn-oeel-noerwd-aro	ef 17 71 43 43 b5 c5 4c b4 b9 96 c5 51 df 47 ed 60 3 7e
Tag *TID*: **0**000100010001000	woond-enmlerad--roe	7c 97 5f 21 37 9e e9 c5 c8 f1 c7 c7 58 51 2c 7a 57 ad 6e
Reader *RID*: 0010001**1**00100010	rreloo--anoe-mwddne	f3 15 3c 7c b4 b 1a 50 64 9e 58 28 34 45 60 24 3f 7e b4
Random number *R*: 000000000011101**1**	-ddelnroo-w-eonmrea	a2 17 7b 6 40 be d2 4f fb f7 8e 80 46 c7 4d a0 73 14 70

In Chaotic encryption, sequence security main depends on chaos initial and the parameter values, tiny difference can make chaos track change a lot and the encrypted result is very different. Figure 3 shows that this algorithm not only has connection with TID, RID, but also has connection with R. When just a bit is changed, the scramble message and ciphertext completely are different, so realize one-time pad. This algorithm makes attackers can not impersonate legal tags and/or readers, Even though an attacker intercepts data in the process of communication, he can not decode RFID parameters to get the original message. Random number R ensures dynamism and unpredictability of data [13], so this algorithm can greatly enhance data security in RFID system.

4 System performance analysis

4.1 PERFORMANCE ANALYSIS OF CHAOTIC ENCRYPTED

The randomness and independence of encryption sequence are the prerequisite and foundation for the encryption algorithm security. Frequency test is also called uniformity test, it can test random sequence whether uniform distribution distributes in (0,1), if the test passes, it can prove that the sequence is random. Run test is to test the sequence run number of the sequence whether meet the requirement of random, then judge whether the sequence is independent or not. Randomness and independence of the sequence are built on an assumption that the test is past. In this paper, using above parameter values $\alpha = 0.3612, x_0 = 0.8515$ and $n = 1000$ to generate 1000 real sequences, then gets 200 sequences every 5 step, then converts them into 8 bit binary sequences and analyzes theirs performance with probabilistic [14] method.

Related symbols instrument: $erfc(x)$ is the complementary error function, P_value is the probability value at last, β is the significant level, generally pick up 1% and 5% of the significant level, 1% is very the significant level. The significant level test is also called statistical test and hypotheses test, if the calculation rate, which according to the null hypothesis, is less than the significant level, then refuses the null hypothesis; Otherwise accepts.

1) Frequency test [15]: count binary sequence, there are $t = 200 \times 8 = 1600 \quad 0,1$. The number of 0 is 837, and number of 1 is 763. Converts 0,1 to -1,1, assuming that the sequence is random:
Calculate statistic:

$$S_t = \sum_1^t x_1 + x_2 + \cdots + x_t = \quad 74\ . \tag{3}$$

Calculate statistic:

$$V = \frac{|S_t|}{\sqrt{t}} = 1.8513\ . \tag{4}$$

According to residual error formula, calculate tag P_value, taking the significant level of $\beta = 0.01$:

$$P\_value = erfc(\frac{V}{\sqrt{2}}) = 0.0643 > \beta\ , \tag{5}$$

P_value is large than β, according to the significant level criteria, if null hypothesis is acceptable, the sequence is random;

2) Run test [16]: number of runs is change times that 0 into 1 or 1 into 0, in this test number of runs $r = 789$. First the binary sequence separately subtracts from mean value 0.5, then counts the positive and negative sequence after subtracted, as the number of 0 is 837, and number of 1 is 763 so the number of negative $n_1 = 837$, and number of positive $n_2 = 763$. Assuming that sequence is an independent distribution, then.

Average:

$$E(\mathrm{r}) = \frac{2n_1n_2}{n_1 + n_2} + 0.5 = 798.789 \tag{6}$$

Variance:

$$D(\mathrm{r}) = \frac{2n_1n_2(2n_1n_2 \quad n_1 \quad n_2)}{(n_1 + n_2)^2(n_1 + n_2 \quad 1)} = 398.04 \tag{7}$$

$\underline{r}$ approximately is close to normally distribution [17], statistic:

$$Z_r = \frac{r \quad E(r)}{\sqrt{D(r)}} = \quad 0.491\ , \tag{8}$$

$\beta = 0.05$ is the significant level, checking standard normal distribution table:

$$Z_{\beta/2} = 1.96 > |Z_r| = 0.491, \tag{9}$$

$$r = 0.3121 > \beta\ . \tag{10}$$

According to the significant level criteria, assumption that the sequence is independent distribution is acceptable. At the same time in this paper, a series of test have be done such as group frequency test, max 1 run test, DFT test, cumulative sum test, random offset test, etc. Results of test verify that chaotic sequence generated by Tent map is random and of mutual independence, so it is suitable for encrypted scrambling application.

4.2 TAG STORAGE CAPACITY ANALYSIS

Internal structure of RFID chip consists of RF front end, analog front end, digital baseband processing unit and EEPROM storage cells. In Figure 4, taking a RFID tag (model No.TI2048) produced by TI company as a sample to instruct storage structure of the tag. In term of ISO18000 or EPC Class1 Generation2, only globally unique user UID 64bit could expand to 128 bit, with special packing, could expand to storage capacity around 1-2Kbit.

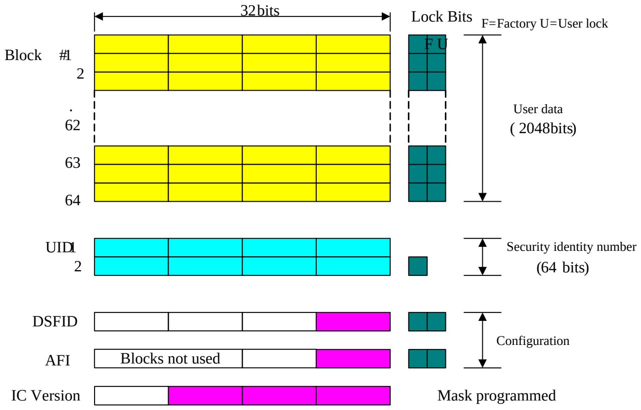

FIGURE 4 RFID tag storage unit

The improved RFID system authentication protocol base on chaotic encryption in this paper, the tag need to store non-self parameters, and they include legal reader RID, random number R and 2 encrypted keys Assuming that the tag confidential message is “one world one dream”. In term of chaotic encryption algorithm, two encrypted keys whose length is the same as length of text information will be generated. As the tag TID and random number have the same byte, both 8 bytes. Length of tag’s text message is 16 bytes, so the 2 binary numbers with 16 bytes. There are altogether 2×8+2×16=48 bytes. So this algorithm needs 48 bytes Block unit and occupies extra 18.75% tag storage capacity in 2048bit (256 bytes), this algorithm enhances privacy of RFID system data and reaches RFID system mutual authentication.

5 Conclusion

Base on chaotic system sensibility to initial value and Hash function one-way function, this paper combines them to apply in RFID identity authentication and privacy protection. Using RFID unique identifications TID , RID and R to be chaotic map initial and parameter values, it can generate two unique, unpredictable encrypted secret sequences, then encrypting tag secret message, it can realize one-time pad, and will enhance RFID data privacy and reach RFID system bidirectional authentication. In consideration of saving the cost of passive RFID tag fully, data encryption and security authentication are combined organically in this paper. This research can applied widely in the safe and secret communication of passive RFID system.

Acknowledgment

This work is jointly supported by the National Natural Science Foundation of China (No. 61363076), Scientific Research Plan Projects of Jiangxi Education Department (Nos. GJJ13435, GJJ14465).

References

[1] Zhang Y, Chen J 2012 RFID and sensor network *Beijing: China Machine Press (in Chinese)*

[2] Yang C, Zhang H 2012 RFID authentication protocol based on secret-sharing scheme *Computer Application* **32**(12) 3458-61 *(in Chinese)*

[3] Cho K 2011 Securing against brute-force attack A hash-based RFID mutual authentication protocol using a secret value *Computer Communications* **34**(3) 391-7 *(in Chinese)*

[4] Piramuthu S 2011 RFID mutual authentication protocols *Decision Support Systems* **50**(2) 387-93 *(in Chinese)*

[5] Zhang N, Zhang J 2013 Research and security analysis on open RFID mutual authentication protocol *Computer Application* **33**(1) 131-4 *(in Chinese)*

[6] Zhang X, Wang Y, Wang S 2012 Research on the cyclic shift lightweight mutual authentication protocol *Chinese Journal of Electronics* **30**(7) 20-6 *(in Chinese)*

[7] Fan J, Zang X 2009 Piecewise logistic chaotic map ad its performance analysis *Chinese Journal of Electronics* **37**(4) 720-5 *(in Chinese)*

[8] Wei Y, Dai Y, Zhang Y 2013 Adaptive chaotic embedded particle swarm optimization algorithm based on tent mapping *Computer Engineering and Application* **49**(10) 45-9 *(in Chinese)*

[9] Katz O, Ramon D A, Wagner I A 2008 A robust random number generator based on a differential current mode chaos *IEEE Transactions on very large scale integration (VLSI) systems* **16**(12) 1677-86

[10] Sheng L, Xiao Y, Sheng Z 2008 A universal algorithm for transforming chaotic sequences into uniform pseudo-random sequences *Chinese Journal of Physics* **57**(7) 4007-12 *(in Chinese)*

[11] Zhang H, Chang J, Guan H 2011 RFID security authentication protocol based on hybrid encrypting approach *Computer Engineering* **37**(1) 134-7 *(in Chinese)*

[12] Zhao Y, Fang J 2012 Research on improved pseudo random number algorithm *Computer Engineering* **38**(7) 113-5 *(in Chinese)*

[13] Gao X, Yang Y, Li Z 2013 One-time group signature model based on hash function *Application Research of Computer* **30**(1): 160-2 *(in Chinese)*

[14] Shi G, Kang F, Gu H 2009 Research and implementation of randomness tests *Journal of Electronics & Information Technology* **35**(20) 39-43 *(in Chinese)*

[15] Ryu E K, Takagi T 2009 A hybrid approach for privacy-preserving RFID tags *Computer Standards & Interfaces* **31**(4) 812-5

[16] Turan M S 2008 On independence and sensitivity of statistical randomness test *Lecture Notes in Computer Science* **5203** 18-29

[17] Zhao G, He Y 2011 RFID secure mechanism based on chaotic encryption *Computer Engineering* **37**(12) 116-8 *(in Chinese)*

Authors

Zhang Xiaohong,1966, China

Current position, grades: PhD, professor, Jiangxi University of Science and Technology.
Scientific interests: cellular neural networks, nonlinear dynamics, wireless sensor network.

Xiao Juanfeng, 1987, China

Current position, grades: master’s degree student, Jiangxi University of Science and Technology.
Scientific interests: wireless sensor network, RFID anti-collision algorithm.

Dong Lifeng, 1981, China

Current position, grades: master’s degree, instructor, Jiangxi University of Science and Technology.
Scientific interests: microelectronic technique, RFID authentication protocol.