Application of Chaotic Encryption in RFID Data Transmission Security

Yang Jianfang
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: perfectyjf@163.com

Yao Huimin
Eighth of production plant, the company china petrdeum
Changing oilfield, Xi'an
Xi'an, 710021, China

Liu Baolong
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: liu.bao.long@hotmail.com

***Abstract*—In order to improve the security performance of data transmission in the RFID system, the sequence generated by the chaotic map is used to encrypt the data transmitted between the reader and the tag in the RFID. Based on the unpredictability, extreme sensitivity to initial conditions, and pseudo-random characteristics of chaotic sequences, the information of each electronic tag is encrypted with a unique chaotic sequence. The same operation mechanism is used to encrypt and decrypt data, and a security model based on chaotic encryption is established. At the same time, the read/write control mechanism and security issues are explained**.

Keywords-Chaotic Encryption; Chaotic Sequence; RFID System; Security Model;

I. INTRODUCTION

Radio Frequency Identification (RFID), which is a wireless non-contact automatic identification technology, automatically identifies surrounding objects through radio frequency signals, spatial coupling (including inductive coupling and electromagnetic coupling). The basic components of RFID system mainly include background server, reader and tag. In the RFID data transmission, the wired transmission between background server and reader is considered as a secure channel, while the wireless transmission between reader and tag is considered as an unsafe channel. The basic components of the RFID system are shown in the figure:

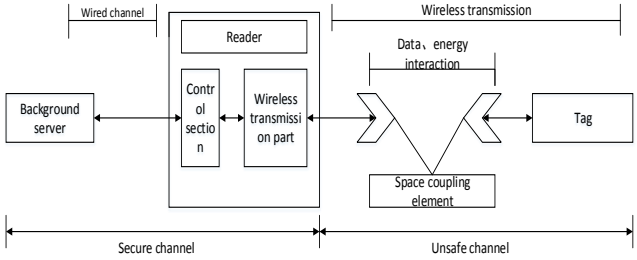

Figure 1. Diagram of the components of the RFID system.

RFID technology has been widely used in various fields due to its low cost, fast recognition speed and long service life, such as warehouse transportation management, train/car identification, baggage security inspection, access control attendance and so on. However, a lot of security problems have emerged in the process of widespread application of RFID, and it is precisely because of the remaining security problems of RFID technology that its further application and development are restricted. The security issues of RFID technology mainly come from the wireless transmission channel of readers and electronic tags, including privacy theft between authentication and data transmission. The authentication problem mainly includes the confirmation of the legality of readers and electronic tags, while the data privacy issues include tracking and leaking data information [1]. The purpose of the RFID system is to popularize the application, which requires that the cost of the reader and the electronic tag in the RFID cannot be too high, and the overly complicated security algorithm cannot be used

DOI: 10.21307/ijanmc-2019-040

in the tag, which creates a difficulty for the security solution of the RFID to some extent.

In most of the currently proposed RFID system security solutions, it can be roughly divided into physical security methods, cryptographic-based security methods, and a combination of the two. The physical security method is mainly for the protection of electronic tags, including Kill command mechanism, electrostatic shielding, blocking tags, active interference, etc [2]. Some of these methods can affect the functionality of the tag. For example, the Kill command mechanism can't respond to the reader's commands by making the tag ineffective. This prevents the corrupted tag from being activated again and cannot be used again. Although electrostatic shielding can shield the interference from illegal readers or tags, it can also make the tag unrecognizable by legitimate readers and cannot be used effectively. The blocking tag evades the legal tag by simulating a large number of tags, and the active interference is to protect the legitimate tag from being detected by sending unwanted electromagnetic signals to interfere or hinder the operation of the illegal reader. The security method based on cryptography may generally include a security protocol based on a hash function, an encryption algorithm, read and write access control and so on.

Chaos is a complex behavior controlled by nonlinear dynamic laws and is a similar random phenomenon that appears in deterministic systems. It has the characteristics of extreme sensitivity of initial values, long-term unpredictability, randomness, and similar broadband spectral noise. These characteristics make chaotic systems very suitable for information encryption [3]. Logistic mapping is one of the most typical types in chaotic systems. The content of this paper is mainly to use Logistic chaotic map to generate chaotic sequences to encrypt the data transmitted between readers and tags in RFID system, which guarantees RFID system security to some extent.

II. CHAOTIC SEQUENCE ENCRYPTS RFID TRANSMISSION DATA

A. *Introduction to chaotic mapping*

The essence of chaotic encryption is serial cipher encryption. The basic principle is to divide the plaintext data into multiple parts of continuous characters, and then use the generated chaotic key stream sequence to perform encryption calculation with the plaintext characters bit by bit, and use the synchronous generated key stream when the sequence is decrypted, and its basic schematic is shown below:

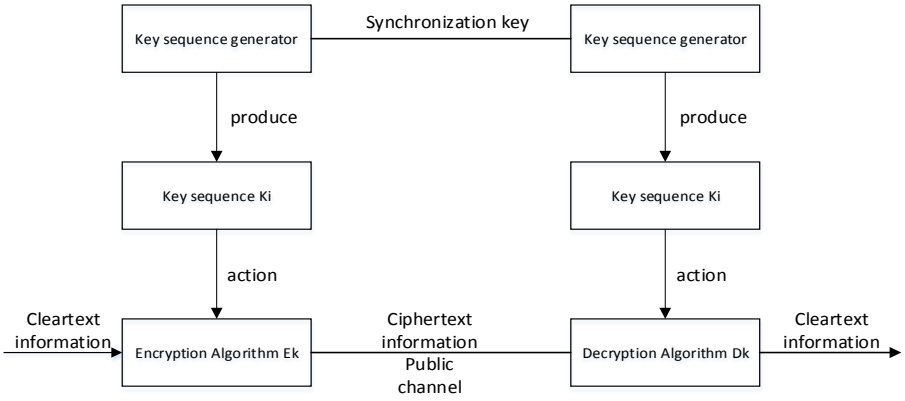

Figure 2. Data information encryption/decryption schematic.

The chaotic sequence generator is the core of chaotic encryption, which used to generate the chaotic key sequence. It then converted into an encrypted sequence for encrypting plaintext information through the conversion operation. The chaotic sequence generator can be represented by several parts in the following figure:

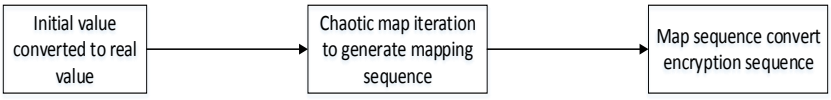

Figure 3. Chaotic sequence generator process diagram.

Chaotic map is an important part of chaotic sequence generator, and its general form can be expressed as:

$$x_{n+1} = \mu(x_n - x_n^{\,2}) \tag{1}$$

Among them, μ represents the system parameter, its value range is (0,4), x_n represents the iteration value, and takes values in the range of [0,1]. The above equation is used as a mathematical equation for chaotic mapping, and a chaotic iterative sequence for encryption is generated by multiple iterations.

Based on the purpose of deep analysis of the characteristics of Logistic mapping, this paper is simulated by matlab, and the logistic mapping bifurcation diagram obtained by taking the initial value is 0.6, while the parameter values are different, is shown in the following figure:

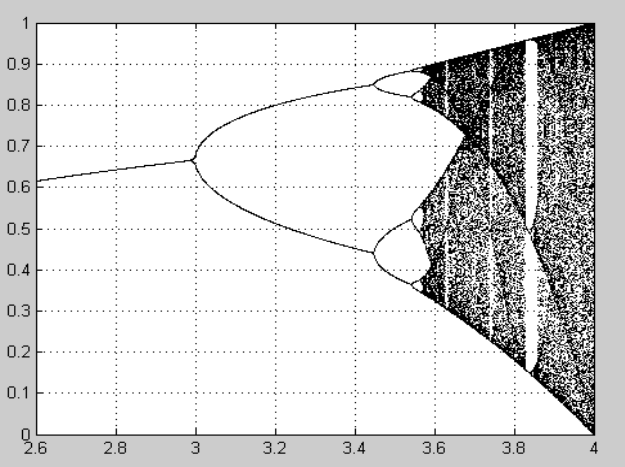

Figure 4. Logistic map bifurcation diagram.

As can be seen from the above figure, the Logistic map is from the double-period bifurcation into the chaotic state. When the value of μ is about 3.5699,the Logistic map enters the chaotic state. Therefore, the μ value range of the Logistic map in the chaotic state is (3.5699, 4), and although the Logistic map is a one-dimensional system, it can generate complex chaotic behavior.

It can be found that the Logistic mapping system only generates chaotic behavior when the initial value and the parameter value are within a certain range, and the degree and randomness of chaos are also affected by different initial values and different parameters.

B. Implementation of chaotic encryption

The chaotic sequence is a sequence of chaotic real values generated by chaotic mapping after multiple iterations, and then formed by some transformation operations. Theoretically, the chaotic sequence is a non-periodic sequence with statistical properties close to Gaussian white noise [4]. The initial value and parameter value required for chaotic mapping in the process of starting the iteration are determined by the label, The initial value x_0 is obtained by the serial number of the unique identification label, and the value of parameter μ is obtained by the read operation keyword, and it is determined according to the user's own needs. Thus, there exists a security policy that the data information of each tag uses a unique chaotic sequence to encrypt. In addition, the iterative sequence generated by the chaotic map is the real field value, and the data processed by the RFID is a binary field. Therefore, the real field value generated by the chaotic map must be converted into a binary sequence for encryption, and the corresponding domain conversion is described in the next section.

The following is a detailed explanation of the general encryption process of Logistic chaotic map. The specific process is as follows:

a) select the parameter value for μ in (3.5699,4), and design the chaotic sequence generator using (1) to generate the key stream factor sequence*;*

b) use the serial number of the tag as the initial value and enter it into the Logistic system;

c) iterate from the current position;

d) converting the iterative chaotic real value into a binary form of the key stream sequence, extracting a part as an encrypted sequence;

e) select the plaintext data of the specified location as the data to be encrypted;

f) the binary encryption sequence extracted in step d) with the plaintext information sequence to perform encryption calculation to obtain a ciphertext sequence;

g) The current operation track is used as the initial parameter of the next stage of encryption, and is reserved for use;

h) Determine whether the encryption operation is completed. If it is completed, it will enter the end state, otherwise it will return to step c).

The above process can be represented by a flow chart as follows:

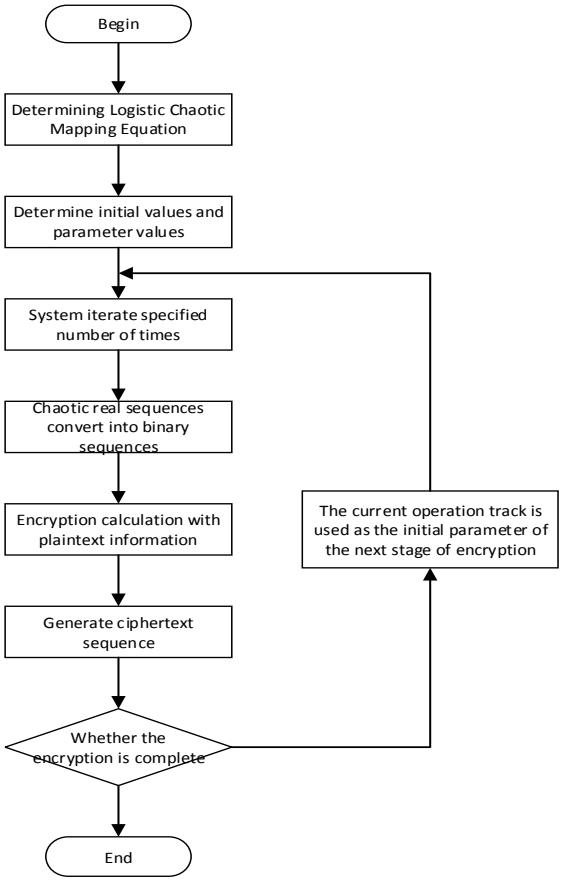

Figure 5. Logistic chaotic encryption flow chart.

It can be seen that the information is written into the electronic tag after being encrypted by the uniquely determined chaotic sequence, which greatly improves the security of the tag data to a certain extent.

C. Domain conversion of chaotic systems and encryption systems

The domain of chaotic system processing is the real number field, and the data processed by the RFID system is binary. This inevitably requires the conversion of real and binary values. The conversion mechanism between them is introduced below.

When the chaotic sequence generator iteratively generates the chaotic sequence, it is necessary to determine the initial value and the parameter value. In the process of designing, the initial value and the parameter value are associated with the label, and the serial number of the unique identification label is used as the initial value, and the user-defined read operation keyword is used as the parameter value. Here, the serial number and the read operation key are expressed in binary form. The process of converting the real value is as follows:

Initial value calculation process: Assuming that the RFID system uses a 16-bit binary number, and the range in which the serial number is converted to a decimal number is (0, 65535). The initial value x_0 of the Logistic chaotic system ranges from (0,1), First the calculation factor of x_0 is $(1-0)/65535 \approx 1.526\times10^{-5}$, The value which obtained by converting the binary number of the serial number into a decimal number and multiplying by the calculation factor is taken as the value of the initial value x_0. Listed below: the binary form of the serial number (1000 0000 0000 1010) converted to a decimal number of 32778, multiplied by the calculation factor (1.526×10^{-5}) and the initial value x_0=0.50019228.

Parameter value calculation process: In the RFID system, the read operation keyword is also a 16-bit binary number. The value of the parameter μ in the Logistic chaotic system is (3.5699456, 4). First, the calculation factor of the parameter μ is determined to be $(4-3.5699456)/65535 \approx 6.5622\times10^{-6}$, and the binary number corresponding to the parameter μ is converted into a decimal number and multiplied by the calculation factor, and finally 3.5699456 is added as the decimal value of the parameter μ. Listed below: The binary form of read operation keyword (1100 0010 0010 0100) is converted to a decimal number of 49700, which multiplied by a calculation factor (6.5622×10^{-6}) and equal to 0.32614134, parameter value μ=0.32614134+3.5699456=3.89608694.

It should be noted that the initial value x_0 is determined by the serial number of the unique identification tag, which indicates that its uniqueness determines that the chaotic sequence iterated by is also uniquely determined, and can be utilized as a private key in the encryption and decryption system. The parameter μ is determined by the read operation keyword, and the read operation keyword can be shared by the reader and the tag, and can be utilized as a public key in the encryption and decryption system.

The above is the process of converting the binary value into a real value when the chaotic sequence is started. After the chaotic encryption sequence is obtained, it needs to be binarized when encrypting the data transmitted between the reader and the tag in the RFID system. The chaotic signal $x(n)$ is converted into a binary sequence stream $b(n)$,and the quantization

function $T[x(n)]$ must be introduced in the process of conversion. The mathematical definition is as follows [5][6]:

$$T[x(n)]=\begin{cases}0 & x(n)\in\bigcup_{i=0}^{2^k-1} I_{2i}^k \\ 1 & x(n)\in\bigcup_{i=0}^{2^k-1} I_{2i+1}^k\end{cases} \quad (2)$$

Where k is an arbitrary integer greater than $0, I_0^k, I_1^k, I_2^k, \cdots$ are 2^k consecutive contiguous partitions of the initial value x_0. The above equation shows that if the chaotic signal $x(n)$ falls within the defined interval of the odd number of the quantization function as the initial bit, the corresponding binary value is 1, if it falls within the defined interval of the even number of the quantization function as the initial bit, the corresponding binary value is 0. After the conversion, because of maintaining the good randomness and unpredictability of the chaotic sequence $\{x(n)\}$, The experimental analysis proves that the above quantitative method has excellent statistical characteristics such as uniform 0-1 ratio distribution and autocorrelation [7].

III. RFID SYSTEM SECURITY MODEL AND READ/WRITE CONTROL MECHANISM, SECURITY DESCRIPTION

A. RFID system security model

The chaotic sequence generated by the above method is used to encrypt and calculate the data information written in the tag, and then sent to the wireless transmission part of the reader for transmission, and the data read back by the tag, the reader also uses the same chaos sequence to decrypte and sent to the background server for processing. In this link, the data touched by the tag, the wireless transmission and reception part and the airborne signal transmission are all chaotically encrypted data, and the ciphertext does not have any useful information. Without knowing the structure of the reader and the details of chaotic encryption, it is impossible to illegally obtain the data in the tag to be decrypted into the original data information, which greatly improves the confidentiality and security of the RFID system. The security model of the RFID system is shown below:

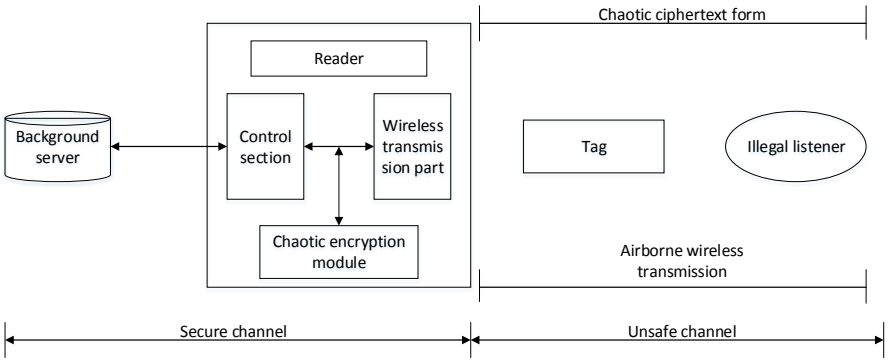

Figure 6. RFID system security model.

Based on the above RFID system security model, coupled with the read and write control mechanism of the next section, the security of RFID data is effectively guaranteed.

B. read and write control mechanism of Chaotic encryption

The legality of the reader and the tag must be verified before the RFID data transmission, which requires the establishment of a read-write control mechanism between them. This control mechanism is established in the case of chaotic encryption, which is in the unsafe communication channel between the reader and the tag. The read and write control mechanism of the RFID system is shown in the following figure:

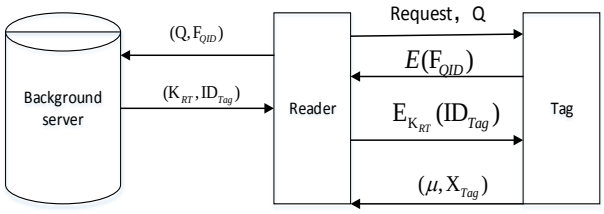

Figure 7. Read and write control mechanism after chaotic encryption.

The basic process is as follows:

K_{RT} is a shared key only by legitimate readers, tags, and servers, and ID_{Tag} is a unique number that identifies tag information.

a) The reader sends an authentication request to the surrounding tags, the tag is activated and waits for the command;

b) The tag calculates the received random number Q and its own ID_{Tag} , such as $F_{QID} = f(Q, ID_{Tag})$, the f operation is a reversible operation, then the tag encrypts F_{QID} by the shared key K_{RT} to $E(F_{QID}) = e_{K_{RT}}(F_{QID})$, and then the encrypted result $E(F_{QID})$ sent to the reader;

c) After the reader receives the $E(F_{QID})$, the decryption operation obtains F_{QID}, and then sends it to the background server together with the random number Q;

d) The background server calculates f reversible operation to get $ID_{Tag}^{'}$, and queries the local ID_{Tag} to see if $ID_{Tag} = ID_{Tag}^{'}$ exists. If it exists, it proves the validity of the label, and then sends the matching (K_{RT}, ID_{Tag}) to the Read. , otherwise the information which returned to the Reader is that the Tag is illegal;

e) After the reader receives the information (K_{RT}, ID_{Tag}) of the background server, it encrypts and calculates $E_{K_{RT}}(ID_{Tag}) = f(K_{RT}, ID_{Tag})$, and the f operation is reversible and then sent to the label;

After the tag receives $E_{K_{RT}}(ID_{Tag})$, it calculates $ID_{Tag}^{'} = f^{-1}(K_{RT}, E_{K_{RT}}(ID_{Tag}))$ to see if it is equal to its own ID_{Tag}. If it is equal, it proves the legality of the reader, so the tag will. passed the data information (μ, X_{Tag}) in the memory to the Reader. After the Reader obtains the parameter μ and the data information X_{Tag} , which generates a chaotic decryption sequence together with the initial value x_0 ,and decrypted to obtain the original correct information with the obtained data information. If they are not equal, the Reader is not legal and the Tag does not respond.

C. Safety instructions

In the RFID system security model, the data transmitted by the RFID is encrypted by using the nonlinear characteristics of the chaotic system [8],so that the encrypted RFID data ciphertext is basically similar to the white noise sequence, and there is no law at all, and it is completely impossible to find some characteristics of the original information. Even if the information in the tag is illegally obtained, the original information cannot be decrypted correctly; under the strict protection of the read/write control mechanism, the identity information of the reader and the tag can be effectively verified, and the illegal reader and the illegal tag are avoided. It ensures the legality and security of the data transmitted by the RFID system.

IV. CONCLUSION

In the context that the wireless unsecure channel between the Reader and the Tag of the RFID system may be subjected to various types of attacks, this paper uses the chaotic encryption sequence generated by the Logistic chaotic map to encrypt the data transmitted by the RFID. The generated ciphertext sequence is equivalent to the noise sequence, having the characteristic of confusion and unpredictability. As a result, the difficulty of ciphertext analysis after encryption is greatly increased. It correspondingly enhanced security and confidentiality of RFID data. In addition, the read-write control mechanism and the domain conversion of the chaotic system and the encryption system are described in detail. However, the chaotic encryption mechanism discussed in this paper still has some drawbacks and shortcomings, such as how to solve the nonlinear dynamic degradation problem of Logistic map and to ensure the randomness of chaotic sequences. These shortcomings need to be studied and solved in the future.

ACKNOWLEDGMENT

This work is partially supported by Science & Technology Program of Weiyang District of Xi'an City with project “201836".

REFERENCES

[1] ZHANG Yong-ping, WANG Feng-jian. Research of Chaotic Encryption Based RFID System Information Security[J]. Computer Security, 2010.

[2] ZHAO Yu-hua. The research of security protocol in RFID system based on theory of chaotic cryptography[D].Master's Degree Thesis of Hunan University, 2011.

[3] DENG Ai-ping, XIAO Ben. Application of Chaotic Encryption Algorithm in RFID Secure Mechanism[J].Materials Science and Information Technology, 2012.

[4] DING Xin. Hyper-chaotic Encryption Based RFID System Informaton Security[J].China Conference, 2006.

[5] ZHAO Yu-xin, WANG Wei, LIU Li-qiang. A Design and Analysis for Non-linear Combination Chaotic Stream Cipher Based on Logistic Map[J].Journal of Projectiles and Guides, 2007.

[6] QIU Yue-hong, HE Chen, ZHU Hong-wen. One Chaotic Map with Infinite Collapses and Its Quantified Sequences[J].Journal of Shanghai Jiaotong University, 2002.

[7] WU Hong, DING Qun, ZHOU Ping. Logistic Chaotic Sequence Design and Aplication in Data Encription [J].Journal of Instrumentation, 2009.

[8] Geo-Su Yim. Design of an RFID Communication Protocol Using Synchronized Chaotic Systems[J].Journal of Korea Institute of Information and Telecommunications Technology, 2016.