International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:6, 2016

Radio Frequency Identification Encryption via Modified Two Dimensional Logistic Map

Hongmin Deng, Qionghua Wang

***Abstract*—**A modified two dimensional (2D) logistic map based on cross feedback control is proposed. This 2D map exhibits more random chaotic dynamical properties than the classic one dimensional (1D) logistic map in the statistical characteristics analysis. So it is utilized as the pseudo-random (PN) sequence generator, where the obtained real-valued PN sequence is quantized at first, then applied to radio frequency identification (RFID) communication system in this paper. This system is experimentally validated on a cortex-M_0 development board, which shows the effectiveness in key generation, the size of key space and security. At last, further cryptanalysis is studied through the test suite in the National Institute of Standards and Technology (NIST).

***Keywords*—**Chaos encryption, logistic map, pseudo-random sequence, RFID.

I. Introduction

RFID is being applied in many aspects, especially with the development of the internet of things (IOT) technology. However, as one of the terminal technology of IOT, the security of RFID is difficult to be ensured. Due to the limit of storage space in RFID, conventional encryption techniques are usually not so effective. On the other hand, chaos theory and technology are being increasingly applied to secure communication. This is decided by the intrinsic characteristics of chaos: aperiodicity, boundedness, sensitivity to initial conditions. In recent years, many kinds of chaotic systems are presented and employed to various situations [1]-[4]. Especially, discrete chaotic maps (such as logistic map, henon map, cat map, chebyshev map and so on) are usually simple, and it is easy to generate the PN sequences via discrete chaotic maps. For example, the sequence cipher, which is obtained from the classic logistic map, has been demonstrated the good statistical properties in the balance of 0/1 sequences, ideal properties of auto-correlation and cross-correlation. Moreover, it is not necessary to preserve the whole sequence, instead we just preserve the simple mapping function, initial value and the only parameter μ . However, the low complexity of 1D logistic map impacts on the security of encryption. In this paper, a discrete 2D logistic map is proposed and applied in the RFID communication. This 2D logistic map is different from those in prior literatures. For instance, Kanso and Smaoui combined two logistic maps by summation and modulus operations in [5]. Reference [6] proposed a 2D logistic coupled map lattice by using each map coupled with four nearest neighbors. Reference [7] studied the dynamics of coupled logistic maps with a global multiplicative coupling method in earlier literatures. In this paper, we use cross feedback control method to produce a 2D logistic map which shows more randomness. However, it is different from the system in [8] where the randomness enhancement was implemented through extending the parameter space in digitalized modified logistic map (DMLP). Generally, chaos is applied to security in two aspects: chaotic authentication and chaotic encryption algorithms [9]-[11], where an authenticated RFID security mechanism was proposed based on Chebyshev chaotic map [11]. In this paper, we do not focus on the chaotic authentication, but on the latter. As for the chaotic encryption algorithms, there are mainly two modes, namely, chaotic stream cipher mode and chaotic block cipher mode. In another category, they are also classified as symmetric encryption and asymmetric encryption. Due to the limited memory capacity, computing power in RFID system and the low encryption speed of the chaotic asymmetric cipher, the asymmetric cryptography is usually not considered in these applications. So the encryption technique based on the symmetric stream cipher is adopted in this paper.

This paper is organized as follows: Section II presents a 2D logistic map based on cross feedback control technique, and discusses its statistical properties which impact the quality of security. Section III introduces the RFID technology and encryption scheme in RFID system. In Section IV, an experiment is presented to demonstrate the chaotic RFID encryption scheme. Section V illustrates the cryptanalysis and conclusion.

II. 2D Logistic Map Based on Cross Feedback Control

A. Chaotic Model

As introduced in Section I, many chaotic systems are used in secure communication. The 2D logistic map based on cross feedback control is described in (1):

$$\begin{cases} x_{n+1} = \mu y_n (1 - y_n) \\ y_{n+1} = \mu x_n (1 - x_n) \end{cases}, \; x_n, y_n \in [0, \; 1] \tag{1}$$

where μ is the parameter of the 2D logistic map. It has been illustrated that chaos exists while $3.5699 \leq \mu \leq 4$, so this 2D map has the similar parameter space to the 1D logistic map. The phase trajectory of the 2D chaotic logistic map is shown in Figs.

This work was supported by the National Natural Science Foundation of China under Grant 61174025 and the National High Technology Research and Development Program of China under Grant 2012AA011901.

H. M. Deng is with the College of Electronics and Information Engineering, Sichuan University, Chengdu, Sichuan, 610065 China (corresponding author, phone: +86-136-7816-1961, e-mail: hm_deng@scu. edu.cn).

Q. H. Wang is with the College of Electronics and Information Engineering, Sichuan University, Chengdu, Sichuan, 610065 China (e-mail: qhwang@scu. edu.cn).

1 and 2, while that of the classic 1D logistic map is shown in Fig. 3.

Comparing Figs. 1 and 2 with Fig. 3, we see that the phase trace of the new 2D logistic map is more randomly distributed within the whole boundary, whether considering the phase trajectory between two variables (*y vs. x*) or the phase trajectory of single variable in iteration epochs ($x(i+1)$ *vs.* $x(i)$).

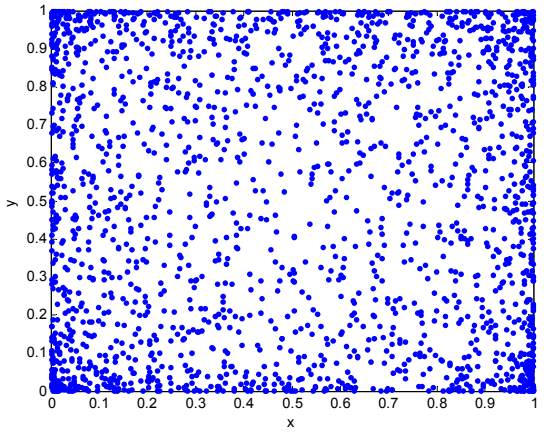

Fig. 1 The phase trajectory of the 2D logistic map (*y vs. x*), where the initial values are taken as x_0 =0.523423, y_0 =0.523424, and μ =4.0

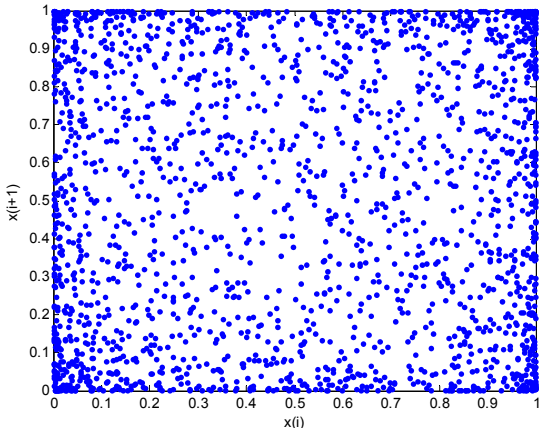

Fig. 2 The phase trajectory of the 2D logistic map ($x(i+1)$ *vs.* $x(i)$), where x_0 =0.523423, y_0 =0.523424, and μ =4.0

B. Statistical Characteristics of Sequence by the New 2D Logistic Map

Good chaotic sequences for encryption should have the following basic features: good balance property, good auto-correlationship and cross-correlationship characteristics.

1. Balance Principle

Balance principle demands that the numbers of 0 and 1 in a sequence are approximately the same. For the 2D logistic map shown in (1), we get discrete 0, 1 sequences after the real-valued chaotic sequences are discretized and quantized. Table I shows the balance property of the 0, 1 sequences with length of 2000.

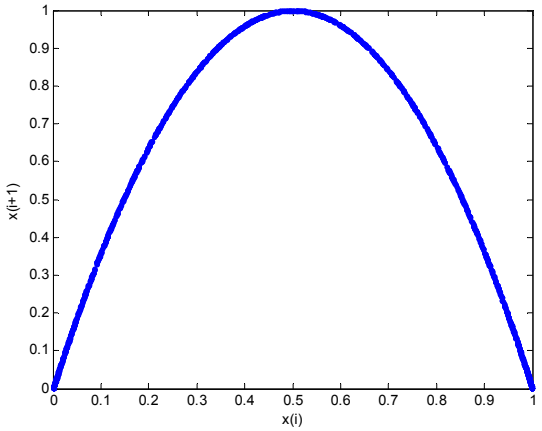

Fig. 3 The phase trajectory of the 1D logistic map ($x(i+1)$ *vs.* $x(i)$), where the initial value x_0 =0.523424, and μ =4.0

TABLE I
BALANCE PROPERTY IN ONE SEQUENCE OF THE 2D LOGISTIC MAP

Initial value		Number of '1'	Number of '0'	μ
x_0	y_0			
0.523423	0.523424	995	1005	4.0
0.000000011	0.000000001	1000	1000	4.0
0.360000000	0.360000001	1002	998	4.0
0.2435000001	0.2435000000	1009	991	4.0
0.872400016	0.872400015	994	1006	4.0

2. Correlation Property

The non-normalized covariance function is described by:

$$c_{xy}(k)=\begin{cases}\sum_{n=0}^{N-|k|-1}\left(x(n+k)-\frac{1}{N}\sum_{i=0}^{N-1}x_i\right)\left(y^*-\frac{1}{N}\sum_{i=0}^{N-1}y_i^*\right), & k\geq 0\\ c_{yx}^*(-k), & k<0\end{cases} \quad (2)$$

where $c_{xy}(.)$ is the non-normalized covariance function, and x_i, y_i are two sequences of length N in random process, respectively. And $k=1,2,...,2N-1$. And the correlation coefficient is shown in (3):

$$r_{xy}=\frac{(x-E(x))(y-E(y))}{\sqrt{D(x)D(y)}} \quad (3)$$

where $E(x)$ and $D(x)$ are the expectation and variance of the variable x, $E(y)$ and $D(x)$ are the expectation and variance of the variable y, respectively.

Fig. 4 describes the normalized auto-covariance and cross-covariance functions of the 2D logistic map. It indirectly shows the good auto-correlation and cross-correlation characteristics of this chaotic map.

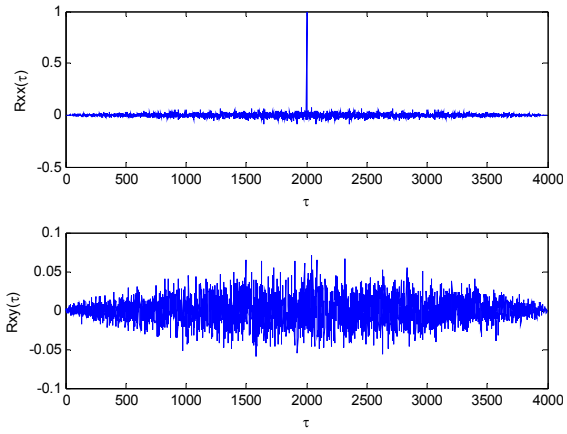

Fig. 4 The auto-covariance and cross-covariance functions of the 2D logistic map

3. The Spectrum of Lyapunov Exponents

The Lyapunov exponent function is described by (4) as in [12]:

$$\lambda_j = \lim_{n\to\infty} \frac{1}{n} \ln \left| DF^n(x_0) \bullet u_j \right|, \quad j = 1, 2, \ldots, n \tag{4}$$

where $DF^n(x_0)$ is the Jacobian matrix of the n-times iterated map with initial value x_0, and u_j is the orthonormal vector in tangent space of the map.

According to the calculating method of Lyapunov exponents from time series [13], [14], the spectrum of Lyapunov exponents for the 2D logistic map is calculated and shown in Fig. 5 with the variance of the parameter μ from 3.0 to 4.0, where the Lyapunov exponents λ_1 and λ_2 are depicted by blue curve and red points, respectively. It clearly depicts that the parameter space with chaos is similar to that of the 1D logistic map while the parameter space is spread via modulus operation in [8].

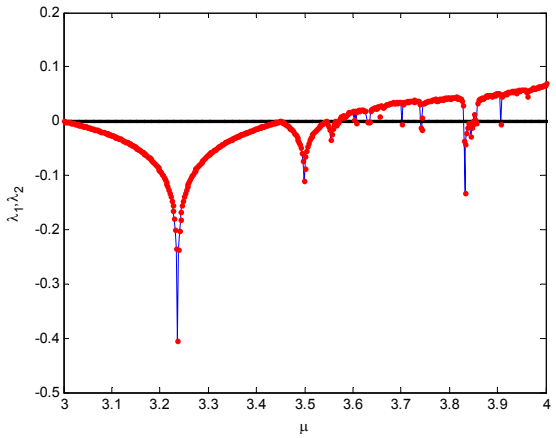

Fig. 5 The spectrum of lyapunov exponents of the 2D logistic map

4. Hamming Correlation of the Discrete PN Sequences

Fig. 4 depicts the correlation property of the chaotic real valued sequences. But the PN sequences used in secure communication are usually binary sequences. So it is important for reevaluating the property of the discrete chaotic sequences. Equations (5) and (6) denote the periodic hamming correlation of the PN sequences obtained from the 2D logistic map. Fig. 6 shows most of the hamming auto-correlation and cross-correlation values are distributed around 1000.

$$H_{XY}(\tau) = \sum_{n=0}^{N-1} h\left[X(n), Y(n+\tau)\right], \quad 0 \le \tau \le N-1 \tag{5}$$

where

$$h\left[X(n), Y(n+\tau)\right] = \begin{cases} 1, X(n) = Y(n+\tau) \\ 0, X(n) \ne Y(n+\tau) \end{cases} \tag{6}$$

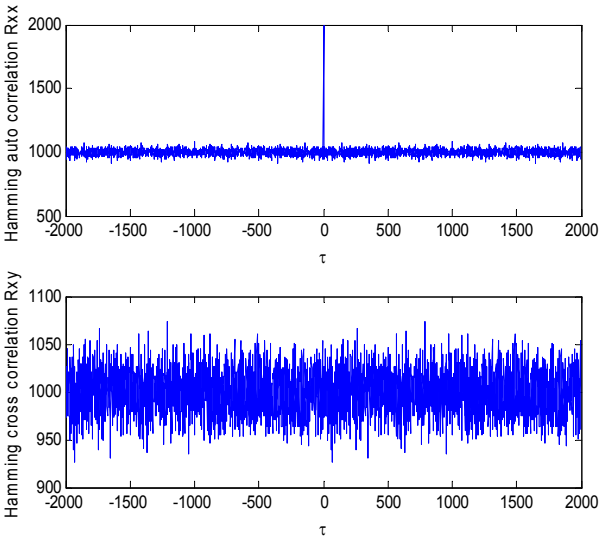

Fig. 6 The hamming auto-correlation function and cross-correlation function of the discrete PN sequences

III. RFID Technology and Encryption

RFID has been applied in many aspects: material flow, transportation, and so on. A RFID system usually consists of three parts: tag, reader, and database system. Furthermore, there are active tag and passive tag. Correspondingly, reader gets the information preserved in the tag by the tag sending actively or electromagnetic induction. The security demands of the RFID system depend mainly on the size of the potential damage and the attacker's motivation level [15].

Chaos has been increasingly applied to RFID systems for security demands. Reference [16] investigated a RFID authentication scheme based on Lorenz chaotic system in addition to the application mentioned in [11]. Reference [17] proposed a RFID encryption algorithm based on chaotic perturbation, and demonstrated its merits of high security and easiness to be implemented.

IV. Implementation of Chaotic Encryption in RFID System

In this section, an experiment is made based on the Cortex-M_0 development board, where the CPU chip is LPC11C14-301. The tag works in 13.56 MHz frequency. Due to the limited storage space, it is not suitable for using a large amount of information and complex cryptographic algorithm in RFID technology. In this experiment, we take the two valued sequence derived from the proposed 2D logistic map as the sequence cipher.

In our paper, the chaotic real valued sequence with length 2000 obtained from (1) is depicted by (7).

$$S = S_1 S_2 ... S_{2000} \tag{7}$$

For the chaotic PN sequence generator, the real-valued chaos needs to be discretized. One method is one bit quantization. Another way is the discretization by A/D conversion. In this paper, the real valued chaotic sequence S is transformed to the discrete binary sequence as in (8) by using the former method.

$$B = B_1 B_2 ... B_{2000} \tag{8}$$

Then, the shift and XOR operations are adopted between the plaintext and the key.

Example 1: the plaintext is a segment of text. "HELLO, SICHUAN". The real-valued chaotic sequence of 2D logistic map (1) is first transformed to bit sequence via quantification. It is easy to generate a lot of random sequences by this technique, so there is a large key space in this encryption algorithm.

In this experiment, the tag reader is selected to follow ISO14443A standard, the encryption algorithm is adopted based on the 2D logistic chaotic map, and the platform is the FS-11C14 development board.

The write process is shown as follows:

1) data shift;
2) chaotic encryption;
3) ciphertext transmission;
4) storage of the encrypted data in the card.

The read process of information is shown as in the four steps:

1) data read;
2) chaotic decryption;
3) data shift;
4) data is displayed on the OLED (organic light emitting diode) screen through MCU (micro-programmed control unit).

The experiment results are shown in Figs. 7 and 8. After the encryption in the write process, the received information without decryption and the plain text after the correct decryption are shown in Figs. 7 and 8, respectively.

Fig. 7 The cipher text displayed on OLED screen

Fig. 8 The correctly decrypted plain text displayed on OLED screen

V. Cryptanalysis

In the RFID system using chaotic encryption, the security of the system largely depends on the statistical property of the PN sequence. In Section II, simulation results have demonstrated the good statistical features of the 2D logistic map:

1) The enhanced random property with respect to the classic 1D logistic map. As shown in Figs. 1-3, the phase trace of the 2D logistic map is distributed randomly in the whole rectangle area, while the phase trace of the 1D logistic map is restricted in the parabola. So it is more difficult to predict the sequence for the 2D logistic map.
2) Good balance property. Among the generated chaotic sequences, the numbers of 0's and 1's are nearly equal.
3) Good hamming correlation property.

Section II not only shows the good correlation property of the 2D logistic maps (the auto-correlation function is similar to δ function and the cross-correlation function approaches zero), but also shows the optimal hamming auto-correlation and cross-correlation properties of the PN sequence got from the 2D logistic maps.

TABLE II
The Test Results of Three Binary Sequences for Randomness

Test types	P-value for G-SHA-1	*P-value* for 1D logistic map	*P-value* for 2D logistic map
Frequency	0.604458	0.152717	0.741400
Block frequency	0.091517	0.957311	0.192323
Cusum-forward	0.451231	0.079565	0.867819
Cusum-reverse	0.550134	0.174531	0.863742
Runs	0.309757	0.673057	0.399727
Long Runs of ones	0.657812	0.034983	0.883440
Rank	0.577829	0.258220	0.875616
Spectral DFT	0.163062	0.295498	0.497093
Nonoverlapping templates	0.496601	0.004067	0.516149
Overlapping templates	0.339426	0.085687	0.079790
Universal	0.411079	0.905010	0.756507
Approximate entropy	0.982885	0.417849	0.286387
Random excursions	0.000000	0.256126	0.000000
Random excursions variant	0.000000	0.208082	0.000000
Linear complexity	0.309412	0.018414	0.197152
Serial	0.760793	0.777446	0.570925

In order to further evaluate the stochastic property of PN sequence, the NIST test suite is utilized for the tests shown in Table II. Three 1,000,000-bit binary sequences based on G-SHA-1(a secure harsh algorithm), 1D logistic map and 2D logistic map are adopted. The results under fifteen types of tests are for three schemes, respectively, where the initial value x_0=0.523424 for the 1D logistic map, the initial values x_0=0.523423, y_0=0.523424 for the 2D logistic map and the

P-values for the G-SHA-1 binary sequence is cited from the SP800-22 of NIST [18]. For the tests, randomness will be accepted if a *P-value*$\geqslant$0.01 according to [18]. These tests depend on the statistical principles. For example, the *P-value* for the frequency test is computed via (9), so on and so forth.

For the frequency test of binary string X,

$$P-value = erfc\left(\frac{|S_{obs}|}{\sqrt{2}}\right) = erfc\left(\frac{\left|\sum_{i=1}^{n}(2X_i-1)\right|}{\sqrt{2n}}\right) \quad (9)$$

From Table II, the results for the 2D logistic map are similar to those for the classic G-SHA-1, with priority over 1D logistic map in some respects, simultaneously the 2D logistic map keeps the priority of easy generation and preservation.

VI. Conclusion

The chaotic encryption based on a 2D logistic map is studied in this paper. It is implemented through cross feedback control method, which is different from the prior two- dimensional logistic maps, and superior to the classic logistic map in randomness enhancement. Furthermore, the chaotic encryption algorithm in RFID system is demonstrated by experiment. At last, the cryptanalysis based on NIST test suite is presented.

Acknowledgment

The authors thank all the anonymous editors and referees for their valuable comments and suggestions.

References

[1] C. C. Hernandez, N. R. Haros, "Communicating via synchronized time-delay Chua's circuits," *Communication in Nonlinear Science and Numerical Simulation*, vol. 13, pp. 645-659, 2008.

[2] A. R. Herrera, "Chaos in predator-prey systems with/without impulsive effect," *Nonlinear Analysis: Real World Applications*, vol. 13, pp. 977-986, 2012.

[3] H. Yang, G. P. Jiang, "High efficiency differential-chaos-shift-keying scheme for chaos-based non-coherent communication," *IEEE Transactions on Circuits and Systems-II: Express Briefs*, vol.59, no.5, pp. 312-316, May 2012.

[4] T. Stojanovski, L. Kocarev, U. Parlitz, and R. Harris, "Digital chaotic encoding of digital information," in *1997 IEEE International Symposium on Circuits and Systems* Hongkong, 1997, pp.1057-1060.

[5] A. Kanso, N. Smaoui, "Logistic chaotic maps for binary numbers generations," *Chaos, Solitons and Fractals*, vol.40, pp. 2557-2568, 2009.

[6] L. Xu, G. Zhang, B. Han, L. Zhang, M. F. Li, and Y. T. Han, "Turing instability for a two-dimensional logistic coupled map lattice," *Physics Letters A*, vol. 374, pp. 3447-3450, 2010.

[7] R. Lopez-Ruiz, C. Perez-Garcia, "Dynamics of maps with a global multiplicative coupling," *Chaos, Solitons and Fractals*, vol.1, no.6, pp.511-528, 1991.

[8] S. L. Chen, T. T. Hwang, and W. W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Transactions on Circuits and Systems- II, Express Briefs*, vol.57, no. 12, pp.996-999, 2010.

[9] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters A*, vol. 309, no. 1/2, pp. 75-82, 2003

[10] A. Kanso, M. Ghebleh, "A fast and efficient chaos-based keyed hash function," *Communication in Nonlinear Science Numerical Simulation*, 18, vol.18, pp.109-123, 2013.

[11] Z. Y. Cheng, Y. Liu, and C. C. Chang, "Authenticated RFID security mechanism based on chaotic maps," *Security and Communication Networks*, vol. 6, no.2, pp.247-256, 2013.

[12] E. Ott, *Chaos in dynamical systems*. Cambridge University Press, Cambridge, Great Britain, 1993.

[13] A. wolf, J. B. Swift, H. L. Swinney and J. A. Vastano, "Determing lyapunov exponents from a time series," *Physica D*, vol.16, pp.285-317, 1985.

[14] K. Briggs, "An improved method for estimating liapunov exponent of chaotic time series," *Physics Letters A*, vol.151, pp.27-32, 1990.

[15] P. Rotter, "A framework for assessing RFID system security and privacy risks," *IEEE Pervasive Computing*, vol.7, no.2, pp.70-77, 2008.

[16] H. Chung, A. Miri, "On the hardware design and implementation of a chaos-based RFID authentication and watermarking scheme," in *the 11th International Conference on Information Sciences, Signal Processing and their Applications: Main Tracks*, *IEEE 2012*, 2012, pp. 460-465.

[17] Y. Tang, Y. Y. Lu, and Y. W. Zhang, "Chaotic dynamic disturbance algorithm based on RFID system," *Journal of Computer Applications*, vol.32, no.6, pp. 1643-1645, 1695, 2012.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh *et al*., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication 800-22 revision 1a*, *Computer security*, 2010.