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-M0 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 $\mu$. 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):

$$
\begin{align*}
    x_{n+1} & = \mu y_{n}(1-x_{n}) \\
    y_{n+1} & = \mu x_{n}(1-y_{n})
\end{align*}
$$

where $\mu$ 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.
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 $\mu=4.0$](image1)

![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 $\mu=4.0$](image2)

![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 $\mu=4.0$](image3)

**Table I**

<table>
<thead>
<tr>
<th>Initial value</th>
<th>Number of '1'</th>
<th>Number of '0'</th>
<th>$\mu$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0.523423$</td>
<td>$0.523424$</td>
<td>$995$</td>
<td>$1005$</td>
</tr>
<tr>
<td>$0.0000000001$</td>
<td>$0.000000001$</td>
<td>$1000$</td>
<td>$1000$</td>
</tr>
<tr>
<td>$0.3600000000$</td>
<td>$0.360000001$</td>
<td>$1002$</td>
<td>$998$</td>
</tr>
<tr>
<td>$0.24350000001$</td>
<td>$0.2435000001$</td>
<td>$1009$</td>
<td>$991$</td>
</tr>
<tr>
<td>$0.872400016$</td>
<td>$0.872400015$</td>
<td>$994$</td>
<td>$1006$</td>
</tr>
</tbody>
</table>

**2. Correlation Property**

The non-normalized covariance function is described by:

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

where $c_{xy}(\cdot)$ 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):

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

where $E(x)$ and $D(x)$ are the expectation and variance of the variable $x$, $E(y)$ and $D(y)$ 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.
3. The Spectrum of Lyapunov Exponents

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

$$\lambda_j = \lim_{n \to \infty} \frac{1}{n} \ln |DF^n(x_0) \cdot u_j|, \quad j = 1, 2, \ldots, n$$  \hspace{1cm} (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 $\mu$ from 3.0 to 4.0, where the Lyapunov exponents $\lambda_1$ and $\lambda_2$ 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].

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.

$$H_{XY}(\tau) = \sum_{n=0}^{N-1} h[X(n), Y(n+\tau)] \quad 0 \leq \tau \leq N - 1$$  \hspace{1cm} (5)

where

$$h[X(n), Y(n+\tau)] = \begin{cases} 1, & X(n) = Y(n+\tau) \\ 0, & X(n) \neq Y(n+\tau) \end{cases}$$  \hspace{1cm} (6)

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-M0 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).

\[ S = S_1 S_2 \ldots S_{2000} \]  

(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.

\[ B = B_1 B_2 \ldots B_{2000} \]  

(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](image)

**Table II**

<table>
<thead>
<tr>
<th>Test types</th>
<th>P-value for G-SHA-1</th>
<th>P-value for 1D logistic map</th>
<th>P-value for 2D logistic map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.604458</td>
<td>0.152717</td>
<td>0.741400</td>
</tr>
<tr>
<td>Block frequency</td>
<td>0.091517</td>
<td>0.957311</td>
<td>0.192323</td>
</tr>
<tr>
<td>Cusum-forward</td>
<td>0.451231</td>
<td>0.079565</td>
<td>0.867819</td>
</tr>
<tr>
<td>Cusum-reverse</td>
<td>0.550134</td>
<td>0.174531</td>
<td>0.863742</td>
</tr>
<tr>
<td>Runs</td>
<td>0.309757</td>
<td>0.673057</td>
<td>0.399727</td>
</tr>
<tr>
<td>Long Runs of ones</td>
<td>0.657812</td>
<td>0.034983</td>
<td>0.883440</td>
</tr>
<tr>
<td>Rank</td>
<td>0.577829</td>
<td>0.258820</td>
<td>0.875616</td>
</tr>
<tr>
<td>Spectral DFT</td>
<td>0.163062</td>
<td>0.295498</td>
<td>0.497093</td>
</tr>
<tr>
<td>Nonoverlapping templates</td>
<td>0.496601</td>
<td>0.004067</td>
<td>0.516149</td>
</tr>
<tr>
<td>Overlapping templates</td>
<td>0.339426</td>
<td>0.085687</td>
<td>0.079790</td>
</tr>
<tr>
<td>Universal</td>
<td>0.411079</td>
<td>0.905010</td>
<td>0.756507</td>
</tr>
<tr>
<td>Approximate entropy</td>
<td>0.892885</td>
<td>0.417849</td>
<td>0.286387</td>
</tr>
<tr>
<td>Random excursions</td>
<td>0.000000</td>
<td>0.256126</td>
<td>0.000000</td>
</tr>
<tr>
<td>Random excursions variant</td>
<td>0.000000</td>
<td>0.208082</td>
<td>0.000000</td>
</tr>
<tr>
<td>Linear complexity</td>
<td>0.309412</td>
<td>0.018414</td>
<td>0.197152</td>
</tr>
<tr>
<td>Serial</td>
<td>0.760793</td>
<td>0.777446</td>
<td>0.570925</td>
</tr>
</tbody>
</table>

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 the 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.

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

![Fig. 8 The correctly decrypted plain text displayed on OLED screen](image)
$P$-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 $\geq 0.01$ 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 $X$, 

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

(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


