2004 RISP International Workshop on Nonlinear
Circuit and Signal Processing (NCSP'04)
Hawaii, USA, Mar. 5-7, 2004.

Analysis of a Cryptosystem Using a Chaotic Map Extended to Two Dimensions

Toru Hiraoka and Yoshifumi Nishio

Dept. of Electrical and Electronics Engineering
Tokushima University
2-1 Minami-Josanjima, Tokushima, Japan
Phone:+81-88-656-7470, Fax:+81-88-656-7471
Email: {hiraoka, nishio}@ee.tokushima-u.ac.jp

1. Introduction

A cryptosystem using a simple one-dimensional chaotic map has been proposed [1]. This system performed encryption and decryption by using a skew tent map and its inverse map. However, the weaknesses of the system have been already reported, especially against a chosen ciphertext attack or a linear attack [2]. In order to overcome the weaknesses, a cryptosystem using two chaotic maps has been proposed by the authors' group [3].

In this research, we make clear the encryption and the decryption processes of the system and analyze the relation between the key and digit of the recoveredtext. Further, we discuss the chosen plaintext attack.

2. Construction of a Cryptosystem Using Two Chaotic Maps

In this research, we use two chaotic maps, a skew tent map and a logistic map, and their inverse maps.

2.1. Encryption and Decryption Function

In the system of this research, the encryption function and the decryption function are described as follows.

$$F : \begin{cases} X_{k+1} = \dfrac{a + \sqrt{1 - x_k}(2-a)}{2} \\ \qquad\qquad\qquad\qquad (0 \le Y_k \le b) \\ Y_{k+1} = Y_k / b \\ \\ X_{k+1} = a\dfrac{(1 - \sqrt{1 - X_k})}{2} \\ \qquad\qquad\qquad\qquad (b < Y_k \le 1) \\ Y_{k+1} = (Y_k - 1)/(b-1) \end{cases}$$

$$F^{-1} : \begin{cases} X_k = 4\left(\dfrac{X_{k+1} + 1 - a}{2-a}\right)\left(1 - \dfrac{X_{k+1} + 1 - a}{2-a}\right) \\ \qquad\qquad\qquad\qquad (a/2 < X_{k+1} \le 1) \\ Y_k = bY_{k+1} \\ \\ X_k = \dfrac{4}{a}X_{k+1}\left(1 - \dfrac{X_{k+1}}{a}\right) \\ \qquad\qquad\qquad\qquad (0 \le X_{k+1} \le a/2) \\ Y_k = (b-1)Y_{k+1} + 1 \end{cases}$$

Where F is an encryption map and F^{-1} is a decryption map. a and b are parameters that are a private key in this system. These maps are shown in Figs. 1 and 2.

2.2. Cryptosystem

1. Encryption

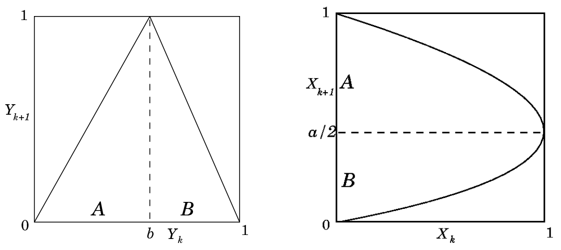
(i) Set an initial point Y_0 as a plaintext and X_0 as a subtext, Y_0, $X_0 \in (0,1)$ where X_0 is an arbitrary value.

(ii) Calculate n-times F, we can obtain X_n from $F^n(X_0, Y_0) = (X_n, Y_n)$. X_n is the ciphertext and is sent to the receiver.

2. Decryption

Calculate n-times $F^{-1}(X_n, S)$ and decrypt the plaintext Y_0 where $S \in (0,1)$ is an arbitrary value. This value becomes the plaintext after n-times calucation.

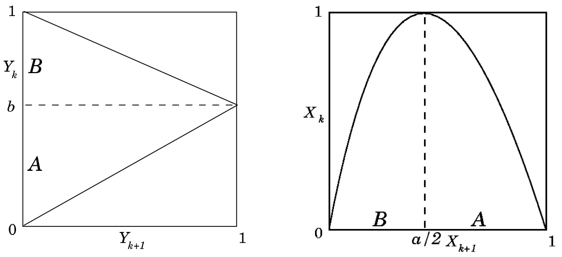
Two symbols (A, B) are used to explain the process of the mapping. In the encryption process, the branch labeled A is used when $Y_k \in [0, b]$, and the branch labeled B is used when $Y_k \in (b, 1]$. This decides which branch is used in the map of X_k. Namely, when the label is A, the branch $X_k \in (a/2, 1]$ is used. While, when the label is B, the branch $X_k \in [0, a/2]$ is used. By this process the information of Y_0 is mapped to the sequence of the labels A and B and further the sequence of the labels is mapped to the value of X_n.



(a)

(b)

Fig. 1: Encryption map (F).



(c)

(d)

Fig. 2: Decryption map (F^{-1}).

In the decryption process, the inverse process is perfomed. The information of X_n is mapped to the sequence of the labels and the sequence is mapped to the value of Y_0.

3. Discussions

3.1. Requirement for Parameters

The key and the plaintext size are required over 64bit (about 20 digits) for the defense against a brute force attack. The ciphertext needs a sufficient size that it can be decrypted correctly. In this system, two keys and the texts sizes are defined as follows.

· keys $a \in [0.8, 1.2]$ and $b \in [0.4, 0.6]$: 21 digits
· plaintext $Y_0 \in (0, 1)$: 40 digits
· subtext X_0 and $S \in (0, 1)$: 40 digits
· ciphertext : 50 digits

Where a and b are selected in the space that the distribution of ciphertexts is uniform enough. Figure 3 shows the distribution of X_k to the parameter a. Besides, deciding b and digits of the plaintext are explained in detail in 3.4. According to [3], when more than 80 times mapping is satisfied independence of χ^2 test. However, in this research, we iterate moreover 64 times against brute force attack and hence the iteration number becomes 144.

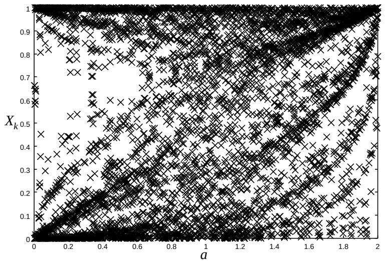


Fig. 3: Distribution of X_k to parameter a.

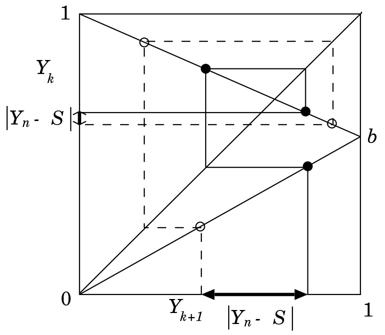


Fig. 4: Reduction of difference between S and Y_n.

3.2. Recover Process

We explain why S chosen arbitrarily becomes to the exact plaintext after the decryption process. As we described in 2.2, in the encryption process, the information of Y_0 is mapped to the sequence of the labels. Further, the sequence of the labels is mapped to the value of X_n. If the value of X_n is sent correctly, the iteration of F^{-1} gives the exact sequence of the labels because of the propoerty of the inverse map. If the sequence of the labels is completely identical, the difference between S and Y_n becomes smaller as the mapping is iterated. This is because the Y part of F^{-1} is reduction map as shown in Fig. 4. If we choose the iteration number as large enough, the difference becomes smaller than the minimum precision and the values are regarded as identical.

3.3. χ^2 test for Uniformness

From a viewpoint of safety, when the same ciphertext is decrypted with some different keys, there is a problem if the recovered texts are not uniform enough. We investigate whether the plaintext would be uniform or not for some different keys, when a ciphertext is decrypted. We use χ^2 test for the uniformness. The consept of the method is as follows.

(i) Divide the interval [0,1] into l class intervals.

(ii) Calculate plaintexts to a ciphertext with 1000 different keys, count the frequencies ($f_i : i = 1, 2, 3, \ldots, l$) in the class intervals.

(iii) Compute

$$\chi^2 = \sum_{k=1}^{l} \frac{(f_i - f_i^{'})^2}{f_i^{'}}$$

This value approach χ^2 distribution of degree of freedom $l - 1$. If this value is smaller than the upper 5% point of χ^2, the uniformness is not rejected. Table 1 shows χ^2 test for some ciphertexts, where $l = 10$ and $f_i = 1000/l = 100$. The uniformness is satisfied because the upper 5% point of χ^2 in degree of freedom 9 is 16.9. Figure 5 shows the distribution of the recovered texts when $\chi^2 = 12.46$.

Table. 1: χ^2 test for uniformness.

Ciphertext	χ^2
C_1	12.46
C_2	10.78
C_3	8.42
C_4	11.9
C_5	11.48
C_6	7.86
C_7	10.82
C_8	9.56
C_9	13.68
C_{10}	11.16

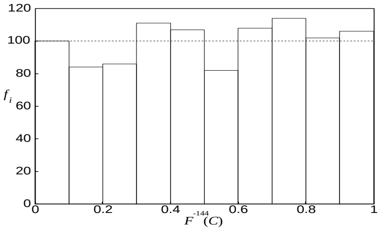


Fig. 5: Histogram of the recovered texts for 1000 keys.

($C_1 = 0.3109587238573985739875938759833475383534 5979878.$)

3.4. Key and Text Size

In order to investigate the range of the key b, we carry out computer simulations for different 1000 plaintexts. Figure 6 shows the number of the success which means that the plaintext is recovered correctly. Further, Fig. 7 shows the relation between the recovered digits and the value of b. We can say that when the value of b is in $[0.4, 0.6]$, all plaintexts are recovered correctly. However, as the key approaches to the edges, the success rate becomes smaller. This is bacause the reduction of the difference between S and Y_n in the decryption process becomes slower.

This can be explained theoretically as follows. If $b = 0.4$, the choosing of the labels A and B of the map $F^{-1}(Y_k)$ in 144 times is estimated as $A : 58$ and $B : 86$, respectively. Because

$$144 \cdot \frac{4}{10} = 57.6, \quad 144 \cdot \frac{6}{10} = 86.4.$$

Therefore, the relation between the reduction of $|S - Y_n|$ and the precision P is as follows.

$$\left(\frac{4}{10}\right)^{58} \cdot \left(\frac{6}{10}\right)^{86} \cdot |d| \leq 10^{-P}$$

where d is the difference between S and Y_n which must be smaller than 1. By taking a logarithm of the both sides.

$$\log \left(\frac{4}{10}\right)^{58} \cdot \left(\frac{6}{10}\right)^{86} \simeq -42.16 \leq \log 10^{-P}$$

$$P \leq 42.16$$

Similarly, the values for other cases are calculated and are summarized in Table 2. Hence, we define that b is in $[0.4, 0.6]$ and that the size of the plaintext is 40 digits.

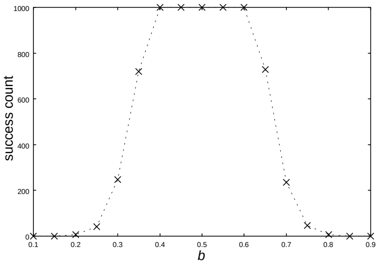


Fig. 6: Success number versus b.

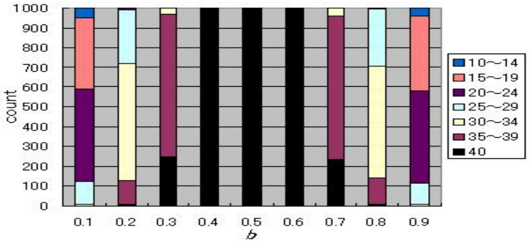


Fig. 7: Recovered digit versus b.

Table. 2: Relation between b and the recovered digit.

b	the recovering digit
0.1, 0.9	19
0.2, 0.8	31
0.3, 0.7	38
0.4, 0.6	42
0.5	43

3.5. Chosen Plaintext Attack

We consider a chosen plaintext attack. It is supposed that a plaintext with the value of $Y_0 = 10^{-40}$ is chosen. In the encryption process, until the value of $F(Y_{k+1})$ exceed the value of key b, the value increases about twice by the iteration of the mapping. However, because the initial value is too small, it takes about 135 times as shown in Fig. 8. This means that the sequence of the labels mapped from Y_0 is $AAAAAAAA\cdots$. Hence, eavesdroppers could decrypt the ciphertext by examining only a limited number of combinations of the sequence after 135 times.

Though this could be the critical weakness of this cryptosystem, limiting the range of the plaintext is one of the easy way to avoid this attack.

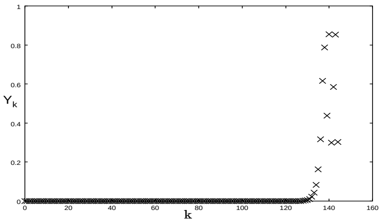


Fig. 8: Series of Y_k for $Y_0 = 10^{-40}$.

4. Conclusions

We have made clear the encryption process and the decryption process of the cryptosystem using a chaotic map extended to two dimensions. We have analyzed the relation between the key and the digit of the recovered text, and a chosen plaintext attack has been investigated.

Acknowledgement

This work was partly supported by The Telecommunications Advancement Foundation's Research Grant.

References

[1] T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A Secret Key Chaotic Map," *Trans. IEICE*, vol. E73, no. 7, pp. 1041-1044, 1990.

[2] E. Biham, "Cryptanalysis of the Chaotic-map Cryptosystem Suggested at EUROCRYPT'91," *Proc. Eurocrypt'91*, pp. 532-534, 1991.

[3] M. Harada, Y. Nishio and A. Ushida, "A Cryptosystem Using Two chaotic Maps," *Proceedings of NOLTA'99*, vol. 2, pp. 609-611, 1999.