2006 RISP International Workshop
on Nonlinear Circuits and Signal Processing (NCSP'06)
Waikiki Beach Marriott, Honolulu,
Hawaii, USA, March 3-5, 2006

Improvement of a Cryptosystem Using Two Chaotic Maps

Shuichi Aono[†], Masahiro Wada[*] and Yoshifumi Nishio[†]

[†] Department of Electrical and Electronic Engineering
Tokushima University
2-1 Minami-Josanjima, Tokushima 770-8506, Japan
Phone:+81-88-656-7470, Fax:+81-88-656-7471
Email: {aoichi, nishio}@ee.tokushima-u.ac.jp

[*] Konan University
8-9-1 Okamoto, Higashinada, Kobe 658-8501, Japan
Email: wada-m@konan-u.ac.jp

1. Introduction

A chaotic map has various features. A chaotic map has sensitivity to a change in initial conditions and parameters, and a long-term forecast becomes impossible by the iterations of a chaotic map. These features looks similar to the properties of the cryptology. For that reason, it is effective to use chaotic maps for cryptosystems. The chaotic cryptosystem is researched as an application of chaos in an engineering field [1-4]. On the other hand, the security of the chaotic cryptosystem is not investigated in detail. It is necessary to investigate the security and to clarify the vulnerability of the chaotic cryptosystem.

A cryptosystem using the tent map has been proposed [5]. And a cryptosystem using two chaotic maps has been proposed [6]. This system performed encryption and decryption by using two chaotic maps, a skew tent map and a logistic map, and their inverse maps.

In this research, we consider a chosen plaintext attack (CPA) for this cryptosystem. And we investigate vulnerability of the cryptosystem using two chaotic maps to CPA. We propose an effective method against this attack. The proposed method repeats the encryption process twice. We confirm that eavesdroppers cannot select the intended plaintext in the second encryption process.

2. A Cryptosystem Using the Tent Map

A cryptosystem using the tent map has been proposed [5]. A tent map is one of the most popular and the simplest chaotic maps.

2.1. Encryption and decryption function

Encryption and decryption function are described as follows,

$$F : \begin{cases} X_{k+1} = \frac{X_k}{\alpha} & (0 \le X_k \le \alpha) \\ X_{k+1} = \frac{X_k - 1}{\alpha - 1} & (\alpha < X_k \le 1) \end{cases} \tag{1}$$

$$F^{-1} : \begin{cases} X_k = \alpha X_{k+1} \\ or \\ X_k = (\alpha - 1)X_k + 1 \end{cases} \tag{2}$$

Figure 1 show the tent map and the inverse map. These maps tranform an interval [0, 1] into itself and contain only one parameter α, which presents the location of the top of the tent.

F is two to one map and F^{-1} is one to two map. Therefore, F^n is 2^n to one map and F^{-n} is one to 2^n map. Since $X = F(F^{-1}(X))$ is always satisfied, $X = F^n(F^{-n}(X))$ is always satisfied.

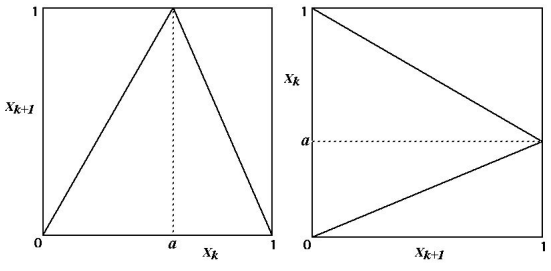


Figure 1: A cryptosystem using the tent map. (a) Tent map. (b) Inverse tent map.

2.2. Cryptosystem

1. Secret Key

The parameter α is a secret key.

2. Encryption

Set an initial point X_0 as a plaintext. Calculate n-times composite of the inverse map, $X_n = F^{-n}(X_0)$, in a recursive way, and send this value X_n to the receiver. On each computation, select one of two equations of F^{-1} in any arbitrary way. In short, one plaintext has 2^n ciphertexts and one of 2^n ciphertexts is sent to the receiver.

3. Decryption

Calculate n-times composite of the map, $X_0 = F^n(X_n)$, in a recursive way and recover the plaintext X_0. Note that only α is required for this computation. The information about which of two equations are used for each encryption process (F^{-1}), is not necessary for the decryption process.

The encryption and the decryption are achieved by repeating a simple calculation. They require n times multiplications.

2.3. Disadvantages of cryptosystem

In this cryptosystem, the tent map as a chaotic map was used. However, it had two disadvantages. One is that the map used in the system was piecewise-linear map, the other is that the ratio of the ciphertext size to plaintext size becomes vary large. The former makes the linear attack be possible and the latter makes the information efficiency be bad.

To improve these disadvantages, a cryptosystem using two chaotic maps has been proposed [6].

3. A Cryptosystem Using Two Chaotic Maps

This system performed encryption and decryption by using two chaotic maps, a skew tent map and a logistic map, and their inverse maps.

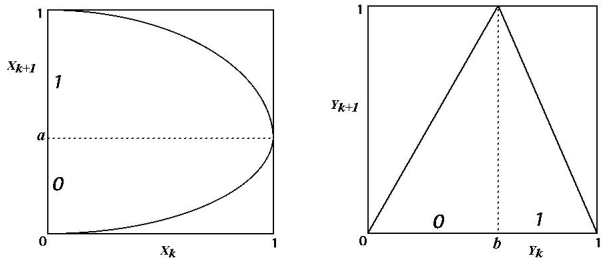
3.1. Encryption and decryption function

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

$$F : \begin{cases} X_{k+1} = a(1 - \sqrt{1 - X_k}) \\ \qquad\qquad\qquad\qquad (0 \le Y_k \le b) \\ Y_{k+1} = Y_k / b \\ \\ X_{k+1} = a + \sqrt{1 - X_k}(1 - a) \\ \qquad\qquad\qquad\qquad (b < Y_k \le 1) \\ Y_{k+1} = (Y_k - 1)/(b - 1) \end{cases} \tag{3}$$

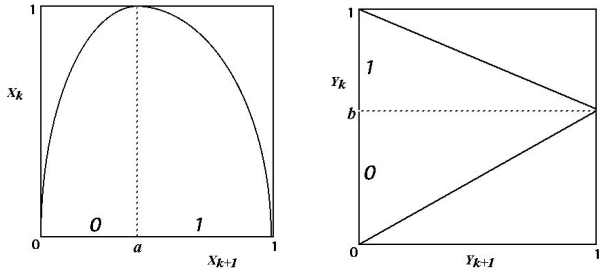
$$F^{-1} : \begin{cases} X_k = \frac{2}{a} X_{k+1}(1 - \frac{X_{k+1}}{2a}) \\ \qquad\qquad\qquad\qquad (a < X_{k+1} \le 1) \\ Y_k = bY_{k+1} \\ \\ X_k = (\frac{X_{k+1}+1-2a}{1-a})(2 - \frac{X_{k+1}+1-2a}{1-a}) \\ \qquad\qquad\qquad\qquad (0 \le X_{k+1} \le a) \\ Y_k = (b-1)Y_{k+1} \end{cases} \tag{4}$$

where F is an encryption map and F^{-1} is a decryption map. α and β are a private key in this cryptosystem. These maps are shown in Figs. 2 and 3.



(a) (b)

Figure 2: Encryption map F.



(a) (b)

Figure 3: Decryption map F^{-1}.

3.2. Cryptosystem

1. Encryption

Set an initial point Y_0 as a plaintext and X_0 as a subtext, where, $Y_0, X_0 \in (0, 1)$, and X_0 is an arbitrary value. Calculate $(X_n, Y_n) = F^n(X_0, Y_0)$, namely n-times iterations of F. Send the value X_n as a ciphertext to the receiver.

2. Decryption

Calculate $(X_0, Y_0) = F^{-n}(X_n, S)$, namely n-times it-

erations of F^{-n}, and decrypt the plaintext Y_0, where $S \in (0, 1)$ is an arbitrary value.

In the encryption process of this chaotic cryptosystem, a plaintext gives a binary sequence by the skew tent map in Fig. 2 (b). Here, the binary sequence corresponds to the branch of the skew tent map. The branch labeled 0 is used when $Y_k \in [0, b]$, and the branch labeled 1 is used when $Y_k \in [b, 1]$. Further, branches of the logistic map are selected by this binary sequence. When the branch of Y_k is 0, the branch of X_k selects 0, and when the branch of Y_k is 1, the branch of X_k selects 1. Namely, X_k includes the binary information on the value of Y_k. Because subtext X_0 is an arbitrary value, ciphertext X_n becomes the value that depends only on the binary sequence.

In the decryption process, the binary sequence given the encryption is obtained from X_k. Further, branches of the Y_k are selected by this binary sequence, where initial value of Y_k, $S \in (0, 1)$, is an arbitrary value. If X_n keeps appropriate level of precision, plaintext Y_0 will be given by calculating $F^{-1}(X_n, S)$ because F^{-1} is the reduction map.

3.3. Reduction map

We explain why arbitrary value S is correctly decrypted. In the encryption process, Y_k gives a binary sequence. Further, branches of X_k are selected by this binary sequence. So that means X_k includes the binary information on the value of Y_k. If the value of X_n is sent correctly, iterating of F^{-1} extracts the binary sequence because of the property of the inverse map. If the binary sequences are completely identical, the difference between S and Y_0 becomes small by using reduction map as shown in Fig. 4.

Figure 4 shows the state that solutions of recursive calculation starting from two different points on the inverse skew tent map. We can clearly see that the difference between S and Y_0 becomes small. If we choose number of iteration is large, the value of Y_0 becomes equal with the value of the S regardless of an initial value.

4. Chosen Plaintext Attack

In this cryptosystem, eavesdroppers needs to know the private key a to extract the binary sequence of the ciphertext X_n. It is difficult in real time for the eavesdropper who does not know the private key a to solve this cryptosystem by a round robin method. Therefore, the security of this cryptosystem was guaranteed.

In this research, we consider a chosen plaintext attack (CPA) for this cryptosystem. A CPA is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.

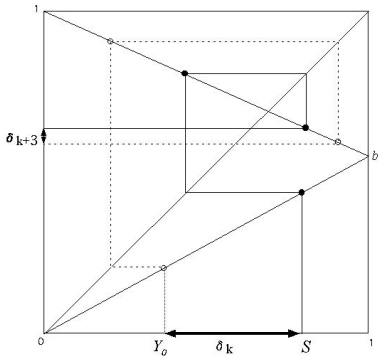


Figure 4: Reduction map.

In the encryption process, there is a possibility that the binary sequence becomes nonuniform for some plaintexts. Namely, if the initial value as a plaintext is too small, the encryption process continues to select the same branch of the skew tent map. Figure 5 shows the binary sequence for the case of $Y_0 = 10^{-40}$. Horizontal axis shows the number of the iteration, vertical axis shows the value of the binary sequence corresponding to X_k. In this simulation, two keys and the texts sizes are defined as follows.

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

where a and b are selected in the space that the distribution of ciphertext is uniform enough. And number of iteration is 144 times.

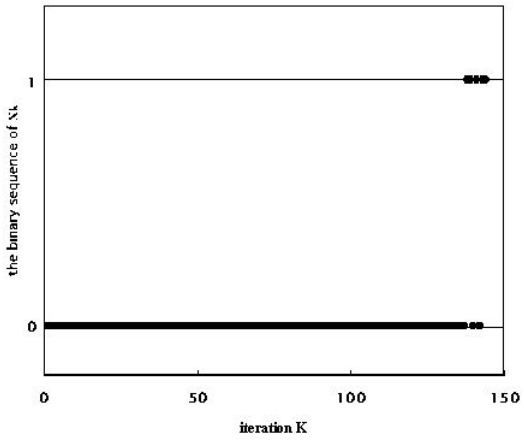


Figure 5: The binary sequence of the X_k for $Y_0 = 10^{-40}$.

From the simulated result, the encryption process continues to select the same branch until the iteration exceeds 137

times. Hence, eavesdroppers could decrypt the ciphertext by examining a limited number of combinations of the sequence, and the private key might be decrypt. This is a critical weak point of this cryptosystem.

5. Proposed Cryptosystem

We propose a simple but effective method against the CPA discussed in the previous section. The proposed method repeats the encryption process twice. We explain proposed method as follows.

1. 1st encryption process
Set an initial point Y_0 as a plaintext and X_0 as a subtext. Calculate n-times $F(X_0, Y_0)$ as described in 3.2. We can obtain X_n from $F^n(X_0, Y_0) = (X_n, Y_n)$.

2. 2nd encryption process
Set an initial point $Y'_0 = X_n$, and X'_0, where X_n is obtained by the first encryption process, and X'_0 is an arbitrary value. Calculate n-times $F(X'_0, Y'_0)$, we can obtain X'_n from $F^n(X'_0, Y'_0) = (X'_n, Y'_n)$ as a ciphertext. And send this value X'_n to the receiver.

Figure 6 shows the binary sequence for the case of $Y_0 = 10^{-40}$. Horizontal axis shows the number of the iteration, vertical axis shows the value of the binary sequence of the X'_k. The simulation condition is the same as Fig. 5.

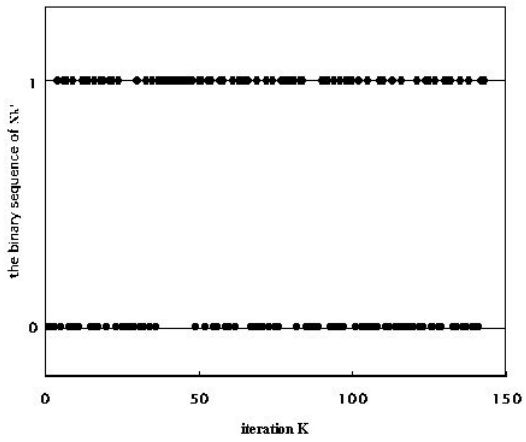


Figure 6: The binary sequence of the X'_k for $Y_0 = 10^{-40}$.

By simulated result, we can observe that there is no bias in binary sequences. An important thing is to replace X with Y in the process of the encryption. We confirm that eavesdroppers cannot select the intended plaintext in the second encryption process. Moreover, the volume of information of ciphertext has not increased though the number of iteration has increased.

6. Conclusions

In this research, we have investigated vulnerability of the cryptosystem using two chaotic maps to CPA. And we have proposed an effective method against this attack. We confirmed that eavesdroppers cannot select the intended plaintext by repeating the encryption process twice.

References

[1] L. Kocarev, "Chaos-Based Cryptography : A Brief Overview, " IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.

[2] G. Jakimoski, L. Kocarev, "Chaos and Cryptography : Block Encryption Ciphers Based on Chaotic Maps," IEEE Trans. Circuits and Systems I, vol. 48, no. 2, pp. 163-169, 2001.

[3] X. Yi, "Hash Function Based on Chaotic Tent Maps," IEEE Trans. Circuits and Systems II, vol. 52, no. 6, pp. 354-357, 2005.

[4] N. Masuda, K. Aihara, "Cryptosystems with discretized chaotic maps," IEEE Trans. Circuits and Systems I, vol. 49, pp. 28-40, 2002.

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

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