IWVCC'08
@ Xian
Nov. 1-3, 2008

A Cryptosystem Based on Iterations of Chaotic Map with Variable Parameter

Shuichi AONO 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

Abstract— A chaotic map has sensitivity to changes in the initial conditions and parameters, and a long-term forecast becomes impossible by iterating a chaotic map. These features look similar to the features of cryptology. For this reason, it is effective to use chaotic maps for cryptosystems. In this research, we investigate features of the modified cut map when the parameters α_i are changed. We use the parameter α_i as shared secret key in the cryptosystem. Hence, it is important for the security of the proposed cryptosystem to investigate the relation between the generated sequences and the parameters. It influences the vulnerability of the cryptosystem.

1. Introduction

A chaotic map has sensitivity to a change in the initial conditions and parameters, and a long-term forecast becomes impossible by iterating a chaotic map. These features look similar to the features of cryptology. For this reason, it is effective to use chaotic maps for cryptosystems. A chaotic cryptosystem is researched for the application of chaos in engineering field [1-4].

Many chaotic cryptosystems that use the expansion and the reduction of chaotic maps for encryption and decryption are reported [5][6]. Figure 1 shows the basic chaotic cryptosystem. An encryptor encrypts plaintext by using the expansion map, and a decryptor decrypts ciphertext by using the reduction map as a reverse-map. If we use one-to-n map as the expansion map, the plaintext cannot be uniquely decrypted, because calculating the reverse-map becomes n-to-one map. Namely, it is necessary to propose the cryptosystem that one-to-one mapping is realized between the plaintext space and the ciphertext space in the decryption [7]. By using only an expansion map for encryption and decryption, one-to-one mapping is realized simply. In addition, the advantages of the chaotic map is demonstrated when the direction of the expansion is used for encryption. It is undesirable to use reduced map for cryptosystems.

Recently, some researchers have proposed public-key cryptography based on chaotic maps [8][9]. The delivery of the key distribution can be solved using public-key cryptography. Though this is an important advantage of public-key cryptography, public-key cryptography has another advantage. A different ciphertext is generated from the same plaintext. An encryptor selects an arbitrary value as a private key. The plaintext becomes the ciphertext that depends on this private key. We consider that this feature is the interesting feature for the development of the chaotic cryptosystem. Because, this feature means that the slightly different condition has to change in a randomly different. It may be no exaggeration to say that this is a characteristic of the chaotic map.

In our previous research, we have proposed a modified chaotic map that has a parameter changing the shape of the map and have proposed a cryptosystem using the modified chaotic map [10]. A characteristic of this cryptosystem is that different ciphertexts are generated from the same plaintext.

In this research, we investigate features of the modified cut map when the parameters α_i are changed. We use the parameter α_i as a shared secret key in the cryptosystem. Hence, it is important for the security of the proposed cryptosystem to investigate the relation between the generated sequences and the parameters. It influences the vulnerability of the cryptosystem.

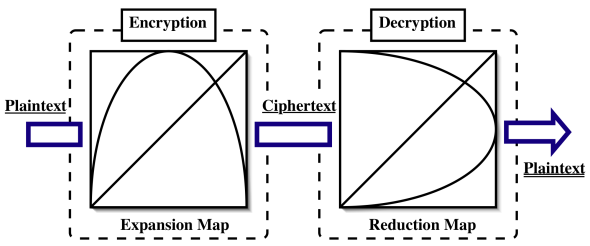


Figure 1: Basic model of chaotic cryptosystem

2. Cryptosystem Based on Iterations of Map [10]

We have proposed a cryptosystem by using iteration of the chaotic map. The simplified block diagram of the cryptosystem is shown in Fig. 2. The proposed cryptosystem is composed of the following three parts. The key generation,

the encryption process and the decryption process.

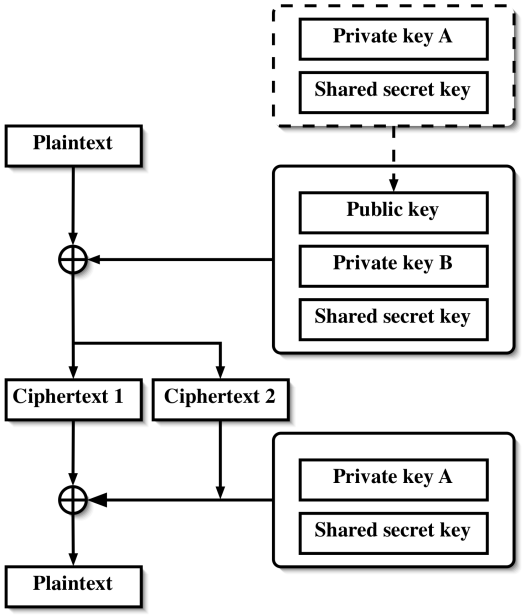


Figure 2: Block diagram of cryptosystem

2.1. Key generation

This cryptosystem uses three kind of keys, a public key, a private key and a shared secret key. A shared secret key means private key between the decryptor and the encryptor. And, the keys are decided by the decryptor. The process of key generation is as follows.

A decryptor sets an initial point for X_0 and a parameter α. Here, α is a shared secret key. In addition, set the number of iterations A. This value A is a private key for the decryptor. The decryptor keep a private key A to himself. $X_A = F^A(X_0)$, namely, A-time iterations of the modified chaotic map F are calculated.

The decryptor can obtain X_0, X_A as public keys, α as a shared secret key and A as a private key.

- X_0, X_A : public key.
- α : shared secret key.
- A : private key.

2.2. Encryption process

We explain an encryption process of this cryptosystem. A encryptor chooses the value B as a number of iterations, where B is an arbitrary value. The encryptor encrypts by using a private key B.

The encryption functions are described as follows :

$$\begin{aligned} C_1 &= M + F^B(X_A) = M + X_{A+B} \\ C_2 &= F^B(X_0) = X_B \end{aligned} \tag{1}$$

where M is a plaintext.

(C_1, C_2) are calculated. These values are sent to a receiver as ciphertexts.

- C_1, C_2 : ciphertext.
- B : private key.

2.3. Decryption process

In the decryption process, a decryptor calculates $C_1 - F^A(C_2)$ by using a private key A.

$$\begin{aligned} C_1 - F^A(C_2) &= M + X_{A+B} - F^A(X_B) \\ &= M + X_{A+B} - X_{B+A} \\ &= M \end{aligned} \tag{2}$$

And decrypt the plaintext M. An important thing is that there is no need to calculates the value of B. The decryptor uses only a shared secret key and a private key A for decryption. By adopting the private, one-to-one mapping between the encryption and the decryption is achieved.

3. Chaotic Map

In this research, we use a modified cut map. The modified cut map is expressed as the following equation:

$$F : \begin{cases} X_{n+1} = \dfrac{1}{\alpha_1} X_n & (0 \le X_n \le \alpha_1) \\ X_{n+1} = \dfrac{1}{\alpha_2 - \alpha_1} X_n - \dfrac{\alpha_1}{\alpha_2 - \alpha_1} & (\alpha_1 < X_n \le \alpha_2) \\ \quad \vdots & \quad \vdots \\ X_{n+1} = \dfrac{1}{\alpha_k - \alpha_{k-1}} X_n - \dfrac{\alpha_{k-1}}{\alpha_k - \alpha_{k-1}} & (\alpha_{k-1} < X_n \le \alpha_k) \\ X_{n+1} = \dfrac{1}{1 - \alpha_k} X_n - \dfrac{\alpha_k}{1 - \alpha_k} & (\alpha_k < X_n \le 1) \end{cases} \tag{3}$$

where $\alpha_{i(i=1,\ldots,k)}$ is a parameter changing the shape of the map.

The shape of the modified chaotic map is changed by α_i. Therefore, the feature of the generated sequences is determined by this parameter. The modified cut map becomes a original cut map at the case of $k = 1$ and $\alpha_1 = 0.5$. This map is shown in Fig. 3.

Next, we investigate the Lyapunov exponent of the modified cut map. The Lyapunov exponent is expressed as the following equation.

$$\lambda = \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \log |F'(X_k)| \tag{4}$$

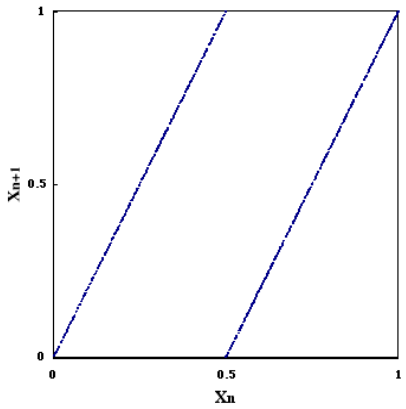


Figure 3: Modified cut map ($k = 1$, $\alpha_1 = 0.5$)

Figure 4 shows the Lyapunov of the modified cut map that changes the value of k. The horizontal axis shows the value of k, and the vertical axis shows the value of the Lyapunov exponent.

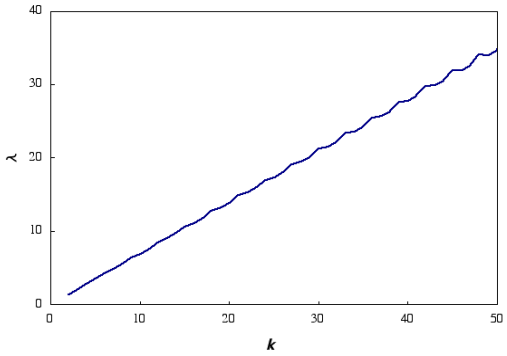


Figure 4: Lyapunov exponent of modified cut map

4. Simulated Results

In this research, we investigate the characteristic of the modified cut map. It is important for the security of the chaotic cryptosystem to investigate the relation between the generated sequences and the parameter.

4.1. Uniformity of generated sequences

We investigate the correlation of X_0 and X_n. We use the χ^2 test for the uniformity. The χ^2 test for uniformity is performed as follows.

1. Divide the interval $[0, 1]$ into l class intervals.

2. Calculate X_n with different initial values. Make an $l \times l$ contingency table f_i.

3. Calculate

$$\chi^2 = \sum_{i=1}^{l} \frac{\left(f_i - f_i'\right)^2}{f_i'} \tag{5}$$

where f_i' are ideal.

The upper 5% of this χ^2 is 16.9. If χ^2 is 16.9 or less, the uniformity of the generated sequence is guaranteed. The simulated result with changing the parameter k is shown in Fig. 5. From this figure, we confirm that almost the distributions of X_n are uniform. In other words, we can use any combination numbers k for the proposed cryptosystem because the distribution of X_n is uniform and independent on the initial values of the modified cut map.

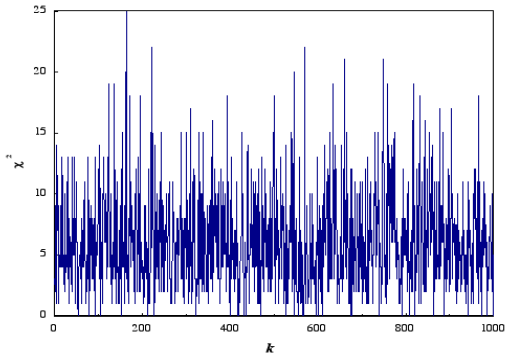


Figure 5: χ^2 test for uniformity

4.2. Number of iterations

Next, we investigate numbers of iterations A and B. The numbers of iterations correspond to the key sensitivity. The modified cut map has sensitivity to changes in parameters α_i. Small variations of the keys produce large variations by iterating the map. Therefore, cipher-breaking becomes difficult by increasing numbers of iterations. However, if the number of iteration is small, there are no large differences between the variations of the keys. It is undesirable to use as keys.

In order to determine the number of iterations, we simulated the sequences with slightly different keys. Figure 6 (a) shows the difference of the generated value X_n with $k = 1$ between the case of X_0 and the case of $X_0 + 10^{-40}$. The horizontal axis shows the number of iterations, and the vertical axis shows the vertical axis shows the difference between the generated sequences. And, the difference of the two values cases of $k = 2$ and $k = 3$ are shown in Fig. 6 (b)(c).

From these figures, there are no large differences unless the number of iteration is small. It is undesirable to use this

range as keys. We can see the difference between the two values that have changed nonuniformity after several iterations. In addition, we can see that there is inverse relationship between the number of k and the number of iterations. Namely, we can easily obtain diffused sequences by iterating a simple chaotic map and the fast diffusion is realized by using the combination map.

5. Conclusions

In this research, we have investigated features of the modified cut map when the parameters α_i are changed. We have confirmed that there is inverse relationship for diffusing the plaintext between the number of k and the number of iterations.

As the future subject, the security of the proposed cryptosystem will be investigated in more detail. We will develop the secret sharing scheme by using iterations of a chaotic map.

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, G. Jakimoski, K. Aihara and L. Kocarev, "Chaotic Block Ciphers : From Theory to Practical Algorithms," IEEE Trans. Circuits and Systems I, vol. 53, no. 6, pp. 1341-1352, 2006.

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

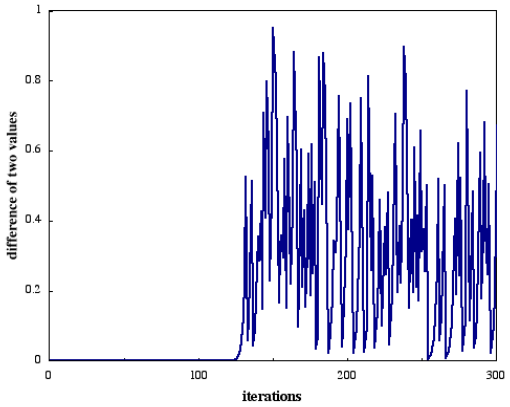
[6] M. Harada, Y. Nishio and A. Ushida, "A Cryptosystem Using Two Chaotic Maps," Proceedings of NOLTA'99, vol. 2, pp. 609-611, 1999.

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

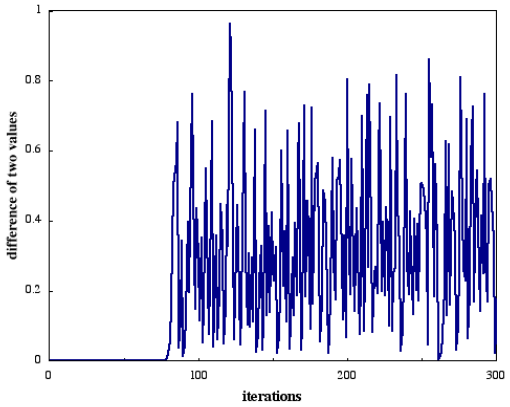
[8] L. Kocarev, Z. Tasev, "Public-key encryption based on Chebyshev maps, " Proceedings of ISCAS'03, vol. 3, pp. 28-31, 2003.

[9] K. Y. Cheong, T. Koshiba, "More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials," IEEE Trans. Circuits and Systems II, vol. 54, no. 9, pp. 795-799, 2007.

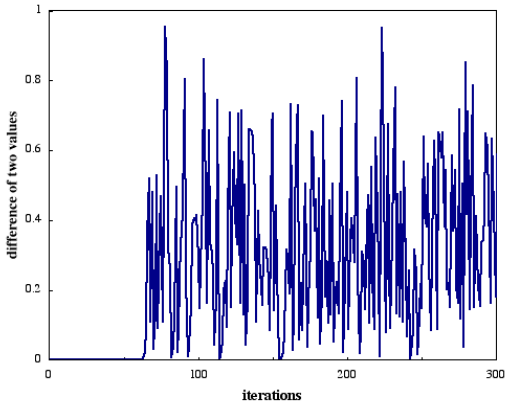
[10] S. Aono and Y. Nishio, "Chaotic map with parameter changing shape of the map for a cryptosystem, " Proceedings of NOLTA'08, pp. 384-387, 2008.



(a)



(b)



(c)

Figure 6: Difference between two values for (a) $k = 1$, (b) $k = 2$, (c) $k = 3$