社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Chaotic Map with Chaotically Changing Parameter for a Cryptosystem

Shuichi AONO† and Yoshifumi NISHIO†

† Department of Electrical and Electronic Engineering, Tokushima University
2-1 Minami-Josanjima, Tokushima 770-8506, Japan
E-mail: †{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 propose a two-dimensional chaotic map with a chaotically changing parameter for a cryptosystem. And we propose a cryptosystem using a two-dimensional chaotic map. A characteristic of the proposed cryptosystem is that a different ciphertext is generated from the same plaintext. The ciphertext becomes the value that depends on an encryptor. This characteristic is one of the important features in public-key cryptography. This cryptosystem is symmetric-key cryptography that has a characteristic of public-key cryptography. We investigate the vulnerability of this cryptosystem.

Key words chaotic map, 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. 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 other advantage. A different ciphertext is generated from the same plaintext. An encryptor select 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 this research, we propose a two-dimensional chaotic map with a chaotically changing parameter for a cryptosystem. This chaotic map has a changing parameter generated by the logistic map. And we propose a cryptosystem using this two-dimensional chaotic map. A characteristic of the proposed cryptosystem is that a different ciphertext is generated from the same plaintext. The ciphertext becomes the value that depends on an encryptor. This characteristic is one of the important features in public-key cryptography. This cryptosystem is symmetric-key cryptography that has a characteristic of public-key cryptography. We investigate the vulnerability of this cryptosystem.

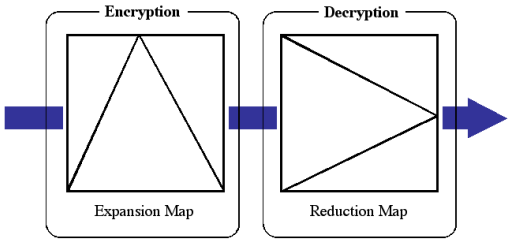


Fig. 1　Chaotic cryptosystem

2. Two-dimensional Chaotic Map

In this research, we use an expansion map for encryption and decryption. By using only an expansion map, even if reverse-map turns into n-to-one map, it is possible to decrypt a correct plaintext. Therefore, we can use a more complex chaotic map that the calculation of the reverse-map becomes difficult for eavesdroppers.

In order to make calculation of the reverse-map difficult, we propose a two-dimensional chaotic map. The proposed two-dimensional chaotic map is expressed as the following equation:

$$F : \begin{cases} X_{n+1} = \dfrac{2}{Y_n} X_n (1 - \dfrac{X_n}{2Y_n}) & (0 \leqq X_n \leqq Y_n) \\ X_{n+1} = (\dfrac{X_n + 1 - 2Y_n}{1 - Y_n})(2 - \dfrac{X_n + 1 - 2Y_n}{1 - Y_n}) & (Y_n < X_n \leqq 1) \end{cases} \quad (1)$$

where

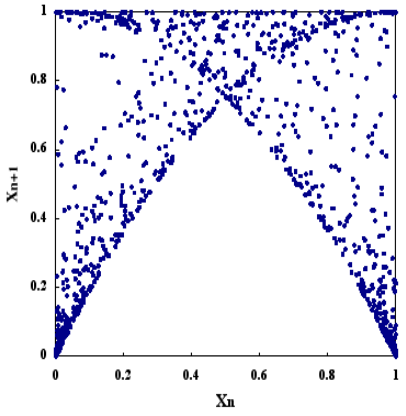
$$\begin{cases} Y_{n+1} = \dfrac{2}{\alpha} Y_n (1 - \dfrac{Y_n}{2\alpha}) & (0 \leqq Y_n \leqq \alpha) \\ Y_{n+1} = (\dfrac{Y_n + 1 - 2\alpha}{1 - \alpha})(2 - \dfrac{Y_n + 1 - 2\alpha}{1 - \alpha}) & (\alpha < Y_n \leqq 1) \end{cases} \quad (2)$$

This chaotic map is changed in the parameter α by chaotic sequences generated by the logistic map. We consider that the cipher-breaking and long-term forecast become more difficult by changing a parameter α in chaos. This maps are shown in Fig. 2. We can see that the chaotic attractor becomes more complex as compared to the logistic map. Figure 3 shows the chaotic sequences of X_n. This map has sensitivity to a change in parameters α and initial states. Therefore, a long-term forecast becomes impossible by iterating a chaotic map.

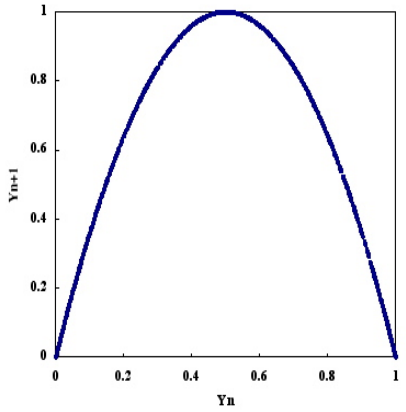
However, the proposed two-dimensional chaotic map is expressed by simple equations. If the number of iterations n and the parameter α are known, it is easy to calculate X_n and Y_n from initial values X_0 and Y_0. In other words, it is necessary to know both the number of iterations and parameter α to obtain the correct X_n and Y_n. If the number of iterations n or parameter α are unknown, it is difficult to calculate X_n and Y_n.

3. Proposed Cryptosystem

We propose a cryptosystem by using iteration of a two-dimensional chaotic map. This cryptosystem is composed of the following three parts. The key generation, the encryption process and the decryption process. In order to combine the concept of the private key and symmetric-key cryptography, the chosen private key must be negated by the decryptor in the decryption process. We use the following characteristics of a chaos map to solve this problem.



(a)



(b)

Fig. 2 Chaotic maps ($\alpha = 0.5$) (a) X_n, (b) Y_n

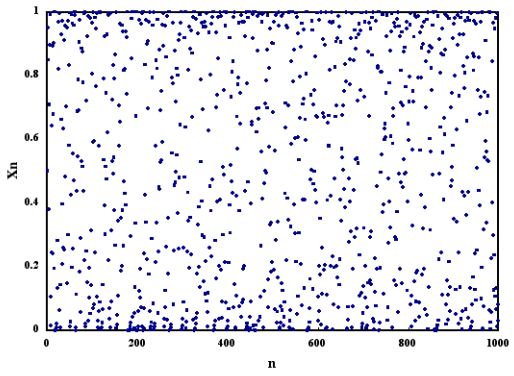


Fig. 3 Chaotic sequences generated by proposed chaotic map

$$F^A \circ F^B(X_0) = F^B \circ F^A(X_0) \quad (3)$$

3.1 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 points for X_0, Y_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. $(X_A, Y_A) = F^A(X_0, Y_0)$, namely, A-time iterations of the two-dimensional chaotic map F are calculated.

The decryptor can obtain X_0, X_A, Y_0, Y_A as public keys, α as a shared secret key and A as a private key.

- X_0, X_A, Y_0, Y_A : public key.
- α : shared secret key.
- A : private key.

3. 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 :

$$\begin{aligned} C_1 &= M + F^B(X_A) = M + X_{A+B} \\ C_2 &= F^B(X_0) = X_B \\ C_3 &= F^B(Y_0) = Y_B \end{aligned} \tag{4}$$

where M is a plaintext.

(C_1, C_2, C_3) are calculated. These values are sent to a receiver as ciphertexts.

- C_1, C_2, C_3 : ciphertext.
- B : private key.

3. 3 Decryption process

In the decryption process, a decryptor calculates $C_1 - F^A(C_2)$ by using C_3 and a private key A.

$$\begin{aligned} C_1 - F^A(C_2) &= M + X_{A+B} - F^A(X_B) \\ &= M + X_{A+B} - X_{B+A} \\ &= M \end{aligned} \tag{5}$$

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 α and a private key A for decryption.

4. Security Analyses

4. 1 Brute force attack

The key space size α is required over 128 bits (40 digits) for the defense against brute force attack. A brute force attack is a method of defeating a cryptographic scheme by trying all possible keys. If there is no effective shortcut attack, the key space size with 128 bits is computationally-secure key space.

We consider the range of the parameter α. We investigate the correlation of α and X_n. We use χ^2 test for the uniformity to determine the range of α. χ^2 test for the uniformity is performed as follows.

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

(2) Calculate X_n with the different key α. Here, X_0 is a fixed value. Make an $l \times l$ contingency table f_i.

(3) Calculate

$$\chi^2 = \sum_{i=1}^{l} \frac{(f_i - f_i')^2}{f_i'} \tag{6}$$

where f_i' is an ideal value. However, the two-dimensional chaotic map does not pass the χ^w test. Because this map has some bias in the distribution of the generated sequence. In this research, we use the frequency of X_n with the random α as ideal.

The upper 5% of this χ^2 test is 16.9. If the value of χ^2 test is 16.9 or less, the uniformity of the generated sequence is guaranteed. The simulated results for 10 different keys and the number of iterations are shown in Table 1. From this table, we confirm that all the distributions of X_n are uniform. In other words, we can use any parameter α as a shared secret key because the distribution of X_n is independent on the parameter α of the two-dimensional chaotic map. We determined that the range of the shared secret key is $\alpha \in [0, 1]$.

Table 1 χ^2 test for uniformity

Range of α	$N = 50$	$N = 100$	$N = 150$
$0 \sim 0.1$	16.75	16.77	8.03
$0.1 \sim 0.2$	7.95	8.72	16.25
$0.2 \sim 0.3$	10.17	16.01	13.11
$0.3 \sim 0.4$	14.03	6.45	9.51
$0.4 \sim 0.5$	9.83	14.70	14.68
$0.5 \sim 0.6$	7.38	9.78	5.46
$0.6 \sim 0.7$	11.46	14.56	15.91
$0.7 \sim 0.8$	10.76	8.31	10.86
$0.8 \sim 0.9$	16.90	11.53	13.27
$0.9 \sim 1.0$	13.28	15.87	3.74

Next, we investigate numbers of iterations A and B. Cipher-breaking becomes difficult by increasing these parameters. The calculation time of the proposed cryptosystem depends on the number of iterations. In order to determine the number of iterations, we simulated the sequences with slightly different keys. Figure 4 shows the difference of the generated value X_n between the case of $\alpha = 0.51$ and the case of $\alpha = 0.51 + 10^{-40}$. The horizontal axis shows the number of iterations, and the vertical axis shows the difference between the generated sequences.

From this figure, there are no large differences between the two values unless the iteration exceeds 150 times. It is undesirable to use the range of $N < 150$ as keys. We can see the difference between the two values that have changed

nonuniformity for $N > 150$. Therefore, we determine that the number of iterations is arbitrary but exceeds 150.

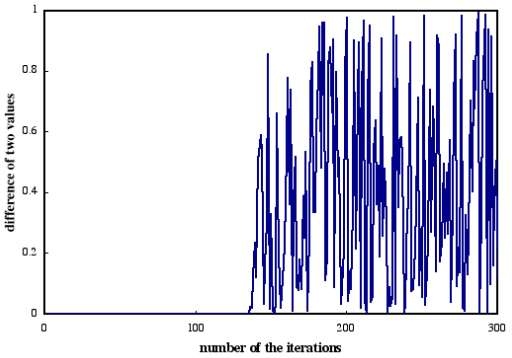


Fig. 4 Difference of two values

Next, we consider the rounding error by the discrete chaotic map. We truncate X_n and Y_n to 40 decimal places by iterating of the map. Therefore, the chaos space is certainly reduced. However, the reduction of the chaos space does not affect the key space. We secure enough key space in consideration of rounding error.

The proposed cryptosystem uses the public-key cryptography for a part of the cryptosystem, and the number of the delivery of keys are decreased. There is a possibility that all of the parameter α generates the value of X_A after N-times iterations. Because the generated sequences by the two-dimensional chaotic map are a long-term sequences and there are no bias for the range of parameter. For that reason, It is difficult for eavesdroppers to obtain correct α and A from the value of X_0, Y_0, X_A and Y_A. We thought that the value of α and the value of A did not be calculated even if the value of X_0 and the value of X_A were opened to the public.

4. 2 Chosen plaintext attack

Next, 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.

The proposed cryptosystem is a simple but effective system against the CPA. If the proposed cryptosystem is attacked by the CPA, and the encryptor selects the same value B, the eavesdroppers can easily obtain two values X_{A+B}, Y_B and X_B. Because, the proposed cryptosystem is considered to be sort of stream cipher. Namely the value of the plaintext is not changed and expanded it in this cryptosystem. However, it is difficult for eavesdroppers to obtain correct A, B and α from the public keys and the ciphertexts. Even if a discrete-valued of the chaotic sequences are known to the eavesdroppers, the eavesdroppers have to detect two successive numbers or the number of iterations to calculate the parameter α.

In addition, the encryptor can easily change the number of iterations B at the every encryption. The encryptor can generate a different ciphertext from the same plaintext. This feature is an advantage compared with the conventional chaotic symmetric-key cryptosystem. The security of the cryptosystem becomes more safety by setting the different key at the encryption.

5. Conclusions

In this research, we have proposed a two-dimensional chaotic map with a chaotically changing parameter. And we propose a cryptosystem using the two-dimensional chaotic map. A characteristic of the proposed cryptosystem is that a different ciphertext is generated from the same plaintext. We have investigated vulnerability of this cryptosystem.

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 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.