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.

A Cryptosystem Based on Iterations of Chaotic Map

Shuichi AONO† and Yoshifumi NISHIO†

† Dept. of Electrical and Electronic Eng., 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 a change in initial conditions and parameters, and a long-term forecast becomes impossible by the iterations of a chaotic map. These features look similar to the properties of the cryptology. For that reason, it is effective to use chaotic maps for cryptosystems. In this research, we propose a cryptosystem by using iterations of a chaotic map. This cryptosystem uses expansion map for encryption and decryption. This cryptosystem is a symmetric-key cryptography that has a public key. We investigate the vulnerability of this cryptosystem.

Key words chaotic cryptosystem, logistic map

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 look 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].

A lot of chaotic cryptosystems that use the expansion and the reduction of the chaotic map for the encryption and decryption are reported [5][6]. On the other hand, many researchers are reported about the disadvantages of cryptosystem using the chaos map [7][8]. There is a possibility to be linear attacked when the piecewise-linear map is used in the cryptosystem. In addition, the advantages of the chaotic map is demonstrated when the direction of the expansion is used for the encryption. It is undesirable to use reduced map for cryptosystem.

Moreover, a symmetric-key cryptography has the problem of the delivery of the key distribution. This problem can be solved by using a public-key cryptography. However, there are two problems in the application of the chaotic map to the public-key cryptography. One is that the trap door is necessary to apply the public key cryptosystem. It is difficult to develop trap door in the chaotic maps. The other is that the equation form is opened to the public. A chaotic map is shown by the equation based on determinism. If the equation of the chaotic map and their parameters are opened to the public, the behavior of the sequences is known. Recently some researchers are proposed a public-key cryptography based on chaotic maps [9].

In this research, we propose a cryptosystem by using iterations of a chaotic map. And we investigate the vulnerability of this cryptosystem. This cryptosystem uses expansion map for encryption and decryption. The decryptor and the encryptor have each private key, and they encrypts to ciphertext and decrypts to plaintext with each private key and a common private key. This cryptosystem is a symmetric-key cryptography that has characteristic of a public-key cryptography.

2. A Chaotic Map

In this research, we use a modified logistic map. The modified logistic map is one of the simplest chaotic maps. The modified logistic map is expressed as the following equation:

$$\begin{cases} X_{k+1} = \frac{2}{\alpha} X_k (1 - \frac{X_k}{2\alpha}) & (0 \leqq X_k \leqq \alpha) \\ X_{k+1} = (\frac{X_k + 1 - 2\alpha}{1-\alpha})(2 - \frac{X_k + 1 - 2\alpha}{1-\alpha}) & (\alpha < X_k \leqq 1) \end{cases} \tag{1}$$

Here, α is a parameter changing the top of the map. This map shown in Fig. 1. The generated sequences looks like the uniform random number. Figure 2 shows an example of chaotic sequences generated by the modified logistic map. The behavior like the uniform random number is seen in $\alpha = 4.0$.

This map has sensitivity to a change in parameter α. Therefore, a long-term forecast becomes impossible by the iterations of a map. However, the modified logistic map is based on an easy equation. Even if eavesdroppers does not know the value of α, parameter α can be obtained from the

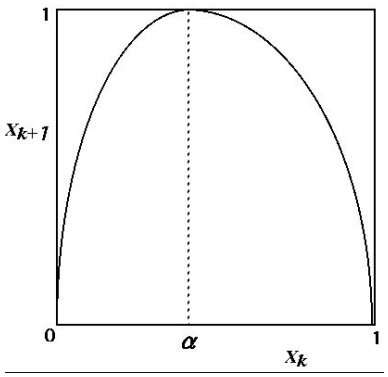

Fig. 1 A modified logistic map F.

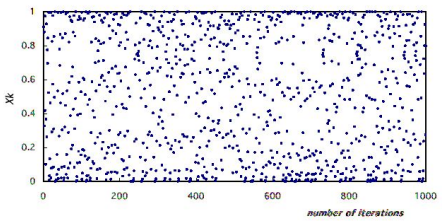

Fig. 2 Chaotic sequence generated by the modified logistic map.

relation of two successive numbers. In other words, it is necessary to know the number of iterations of the modified logistic map to obtain α. If the number of iterations k is an unknowns, it is very difficult to obtain correct α from the value of X_0 and X_k. We propose the chaotic cryptosystem using this feature.

3. Cryptosystem

We propose a cryptosystem by using iteration of a modified logistic map. The simplified block diagram of the cryptosystem is shown in Fig. 3. This cryptosysytem is composed of the following three parts. Key generation, encryption process and decryption process.

3.1 Key Generation

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

The decryptor set an initial point X_0 and a parameter α, here α is a common private key. In addition, set a number of iterations A. This value A is a private key of the decryptor. The decryptor keep a private key A to himself.

Calculate $X_A = F^A(X_0)$, namely A-time iterations of a modified logistic map F.

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

- X_0, X_A : public keys.

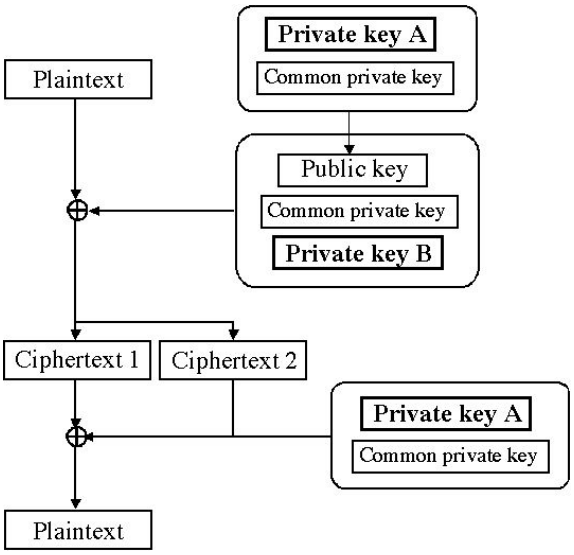

Fig. 3 Block diagram of the cryptosystem.

- α : common private key.
- A : private key.

3.2 Encryption Process

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

The encryption functions are described as follows :

$$\begin{aligned} C_1 &= M + F^B(X_A) = M + X_{A+B} \\ C_2 &= F^B(X_0) = X_B \end{aligned} \tag{2}$$

here, M is a plaintext.

Send this value (C_1, C_2) as a ciphertext to the receiver.

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

3.3 Decryption Process

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

$$\begin{aligned} C_1 - F^A(C_2) &= M + X_{A+B} - F^A(X_B) \\ &= M + X_{A+B} - X_{B+A} \\ &= M \end{aligned} \tag{3}$$

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 common private key α and private key A for decryption.

4. Requirements for Cryptosystem

4.1 Key and Plaintext Sizes

The key space size and plaintext size are required over 128 bits (40 digits) for the defense against brute force attack. In this cryptosystem, a public keys, a common key and plaintext size are defined as follows :

- α 40 digits.
- X_0, $X_A (\in 0, 1)$ and M 40 digits.

4.2 Range of Parameter α

Next, we investigate the range of parameter α. There is a possibility that the distribution of the generated sequences has bias for some chosen value of the key and chosen initial value. Figure 4 and 5 shows the distribution of the value of the X_N in changing the α the case of $N = 10$ and the case of $N = 100$.

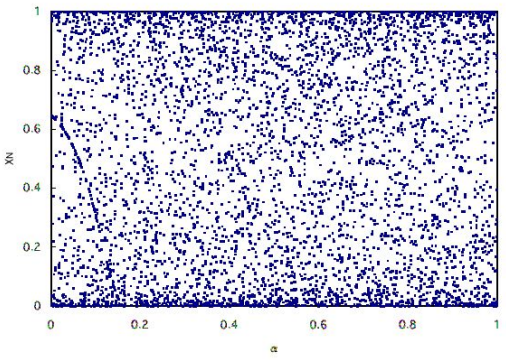

Fig. 4 The distribution of the X_N the case of $N = 10$.

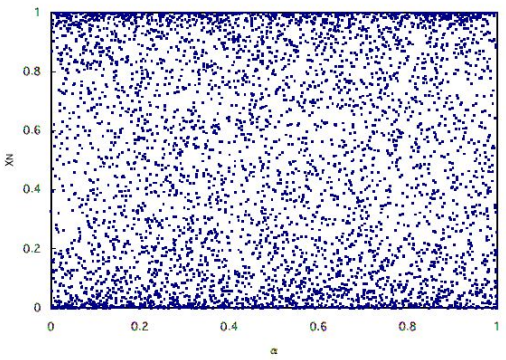

Fig. 5 The distribution of the X_N the case of $N = 100$.

From Fig. 4, we can see that the bias is caused at the value of α close to 0 and 1. This bias decreases according to increasing the iterations of map. If the generated sequences has some bias, the eavesdroppers does not calculate correct keys. Because the decryptor can set an arbitrary the common private key α and arbitrary the private key A. In this research, we defined $\alpha (\in 0.1, 0.9)$.

- $\alpha (\in 0.1, 0.9)$ 40 digits.

4.3 Ciphertext Size

In this cryptosystem, we do not expanse and reduce the value of the plaintext. We have to think only about the effect of rounding error of the sequences generated by a modified logistic map. And so, we truncate a number to 40 decimal places by the iteration of the map. Therefore, the ciphertext sizes are defined the same as the plaintext.

- C_1 and C_2 40 digits.

4.4 Number of Iterations

We investigate the number of iterations as a private keys A and B. A and B are arbitrary value. The cipher-breaking becomes difficult by increasing this value. However, if this value becomes longer, The computation time increases.

In order to determine the number of iterations, we simulated the sequences with slight different keys. Figure 6 shows the difference of the value between the case of $\alpha = 0.49$ and the case of $\alpha = 0.49 + 10^{-40}$. Horizontal axis shows the number of the iterations N, vertical axis shows the difference between the generated sequences.

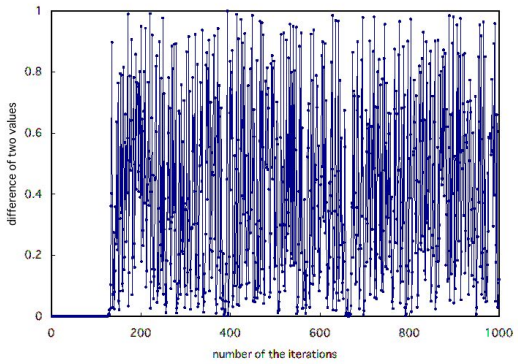

Fig. 6 The difference of two value.

From this figure, we can see the difference of two values that have changed nonuniformity in the case of $N > 150$. There are not so many differences of two values until the iteration exceeds 150 times. It is undesirable to use the key for cryptosystem. Therefore we determine that the number of iterations are arbitrary value over 150 times.

- A and $B > 150$ *times*.

5. Security of The Propose Cryptosystem

5.1 A Public Keys

This cryptosystem uses the public-key cryptography for a part of the cryptosystem, and the number of the delivery of the keys are decreased. It is very difficult for eavesdroppers to obtain correct α and A from the value of X_0 and X_k. So, we open the X_0 and the X_A to the public as a public keys.

We explain that reason giving examples. When the public keys are $X_0 = 0.41234$ and $X_A = 0.24739$, the eavesdroppers are attacked by the brute force attack. Table 1 shows the results of the brute force attack for the limited case of $N < 50$ and $\alpha = 5$ *digits*.

This results are solutions in limited case, however eavesdropper can detect a lots of a values. An important thing

Table 1 The results of the brute force attack.

Private key α	Iterations A	Private key α	Iterations A
0.04439	19	0.51144	8
0.04719	44	0.51929	45
0.06094	15	0.52547	25
0.10328	2	0.54957	19
0.13988	21	0.55229	27
0.15702	17	0.62369	9
0.15839	24	0.64520	12
0.18736	46	0.64959	35
0.19175	40	0.67215	24
0.24723	21	0.74644	46
0.30044	47	0.74863	22
0.33086	3	0.79956	45
0.37352	35	0.82766	34
0.43097	17	0.83572	38
0.44703	39	0.85982	34
0.45617	7	0.88199	49
0.47851	23	0.95105	23
0.48088	27	0.97876	38
0.50042	36		

is that the all of the values are correct keys for the eavesdropper who knows only $X_0 = 0.41234$ and $X_A = 0.24739$. But a really correct private keys are only one in their values. When the eavesdroppers chooses a really correct key in this Table 1, it is necessary to know the value of the α or the value of the A. Only the decryptor and the encryptor knows that parameters. Moreover, there is a possibility that all of the parameter α generates the value of the X_A after the N-times iterations. Because the generated sequences by the modified logistic map are a long-term sequences. It is difficult to establish the value of the X_0 does not becomes the value of the X_A by repeating N times of the map with a certain α.

For that reason, we thought that the value of α and the value of A did not calculate even if the value of the X_0 and the value of the X_A were opened to the public. And we used X_0 and X_A as a public keys.

We can think about the ciphertexts C_1 and C_2 in a similar way the above. In actuality, the sequences generated by the modified logistic map has period. If the generated sequences becomes true random number, here is a possibility that all of the parameter α that shown in Table 1 generates the value of the X_B as a C_2 after the N-time iterations.

5. 2 A 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.

This propose cryptosystem is a simple but effective system against the CPA. When this cryptosystem is attacked by a CPA, and encryptor selects the same value B, the eavesdroppers can easily obtain two values as X_{A+B} and X_B. Because, 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 value of X_0, X_A, X_B and X_{A+B}. 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 the iterations to calculate the parameter α.

In addition, the encryptor can easily change the number of the iterations B at the every encryption, also same for the decryptor. The security of the cryptosytem becomes more safety by setting the different key at the encryption.

6. Conclusions

In this research, we have proposed a cryptosystem by using iterations of a modified chaotic map. And we have investigated vulnerability of this cryptosystem. The proposed cryptosystem is a symmetric-key cryptography that looks like a public-key cryptography that has both of a private key and a common private key. The number of the delivery of the keys has decreased to using this cryptosystem.

As the future subject, we would like to investigate security of the cryptosystem in more detail. And we apply the cryptosytem by using iterations of a chaotic map to the system of the personal authentication.

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] E. Biham, “Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT’91,” Proc. Eurocrypt ’91, pp. 532-534, 1991.

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

[9] L. Kocarev, Z. Tasev, “Public-key encryption based on Chebyshev maps, ” Proceedings of ISCAS’03, vol. 3, pp. 28-31, 2003.