2007 International Symposium on Nonlinear Theory and its Applications
NOLTA'07, Vancouver, Canada, September 16-19, 2007

A Cryptosystem Using Expansion of Chaotic Map

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 a change in initial conditions and parameters, and a long-term forecast becomes impossible by 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 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.

I. Introduction

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 cryptosystems using the chaotic map [7][8]. There is a possibility to be linearly 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 realize the public key cryptosystem. It is difficult to develop trap door in the chaotic map. The other is that the system equation is opened to the public. If the equation of the chaotic map and its parameters are opened to the public, the behavior of the sequences is known. Recently some researchers proposed a public-key cryptography based on the chaotic map [9].

In this research, we propose a cryptosystem 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.

II. 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:

$$\begin{cases} X_{n+1} = \dfrac{2}{\alpha} X_n \left(1 - \dfrac{X_n}{2\alpha}\right) & (0 \le X_n \le \alpha) \\ X_{n+1} = \left(\dfrac{X_n + 1 - 2\alpha}{1-\alpha}\right)\left(2 - \dfrac{X_n + 1 - 2\alpha}{1-\alpha}\right) & (\alpha < X_n \le 1) \end{cases} \tag{1}$$

where α is a parameter changing the top of the map. This map is shown in Fig. 1. The generated sequences look like uniform random numbers. Figure 2 shows an example of chaotic sequences generated by the modified logistic map. The behavior like the uniform random number is seen in $\alpha = 0.5$.

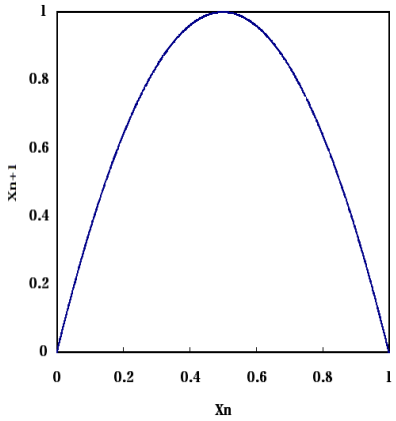

Fig. 1. Modified logistic map F. ($\alpha = 0.5$)

This map has sensitivity to a change in parameter α. Therefore, a long-term forecast becomes impossible by iterations of a map. However, the modified logistic map is based on an

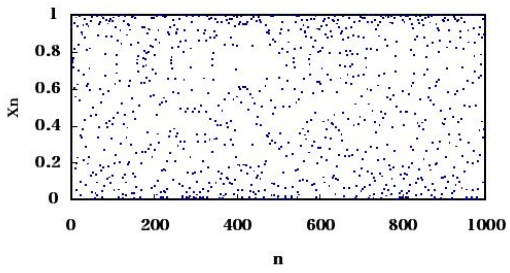

Fig. 2. Chaotic sequence. ($\alpha = 0.5$)

easy equation. If the number of iterations n and values of X_n and X_{n+1} are known, it is easy to calculate the value of α. In other words, it is necessary to know the number of iterations to obtain the correct value α. If the number of iterations n is unknown, it is difficult to calculate correct α from the value of X_0 and X_n. We propose the chaotic cryptosystem using this feature.

III. 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.

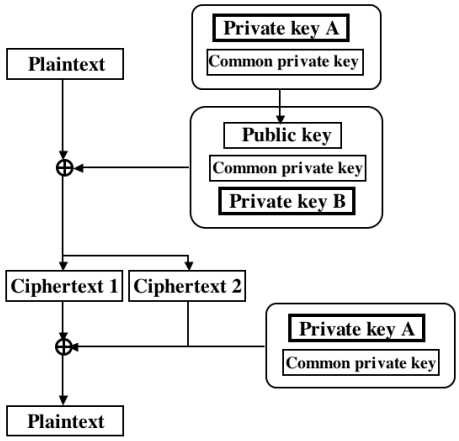

Fig. 3. Block diagram of the cryptosystem.

A. 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.

A 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 for the decryptor. The decryptor keep a private key A to himself.

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

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

- X_0, X_A : public keys.
- α : common private key.
- A : private key.

B. 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 :

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

where, M is a plaintext.

Send these values (C_1, C_2) as a ciphertext to the receiver.

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

C. Decryption Process

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

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

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 a private key A for decryption.

IV. Requirements for Cryptosystem

A. 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. We use a GNU Multiple Precision Arithmetic Library (GMP) [10] to implement. GMP is a library for arbitrary precision arithmetic, operating on signed integers, rational numbers, and floating point numbers.

In this cryptosystem, a public key, a common key and a plaintext size are defined as follows :

- α 40 digits.
- X_0, $X_A \in [0, 1]$ and M 40 digits.

B. Ciphertext Size

In this cryptosystem, it is not necessary to consider the effect of rounding error of the sequences generated by the modified logistic map. Because only the direction of the expansion is used. Therefore, we truncate a number to 40 decimal places by the iteration of the map. The ciphertext sizes are defined the same as the plaintext.

- C_1 and C_2 40 digits.

C. Range of Parameter α

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

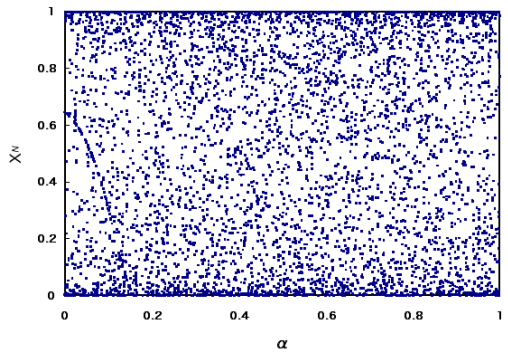

Fig. 4. Distribution of X_N for $N = 10$.

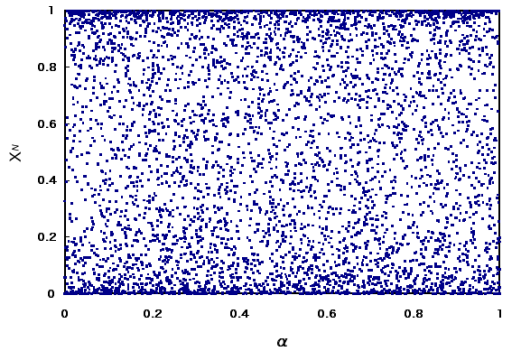

Fig. 5. Distribution of X_N for $N = 100$.

From Fig. 4, we can see that the bias is caused at the value of α close to 0 and 1.

We use χ^2 test for the uniformity to determine the range of α. χ^2 test for the uniformity is expressed 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, and make $l \times l$ contingency table f_i.
3) Calculate

$$\chi^2 = \sum_{i=1}^{l} \frac{(f_i - f_i')^2}{f_i'} \tag{4}$$

where f_i' is an ideal value.

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 different keys and the number of iterations are shown in Table 1.

TABLE I
χ^2 TEST FOR THE UNIFORMITY.

Range of α	$N = 10$	$N = 100$
$0 \sim 0.1$	82.1	35.7
$0.1 \sim 0.2$	15.6	13.5
$0.2 \sim 0.3$	14.2	15.8
$0.3 \sim 0.4$	16.4	6.8
$0.4 \sim 0.5$	13.5	16.2
$0.5 \sim 0.6$	11.9	16.8
$0.6 \sim 0.7$	4.8	12.0
$0.7 \sim 0.8$	10.5	9.8
$0.8 \sim 0.9$	9.6	15.2
$0.9 \sim 1.0$	21.2	23.4

From this table, we determined that the range of the common private key is $\alpha \in [0.1, 0.9]$.

- $\alpha \in [0.1, 0.9]$ 40 digits.

D. Number of Iterations

We investigate numbers of iterations A and B. A and B are arbitrary value as private keys. The cipher-breaking becomes difficult by increasing this value. 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 6 shows the difference of the generated value X_N between the case of $\alpha = 0.49$ and the case of $\alpha = 0.49 + 10^{-40}$. The horizontal axis shows the number of iterations N, and the vertical axis shows the difference between the generated sequences.

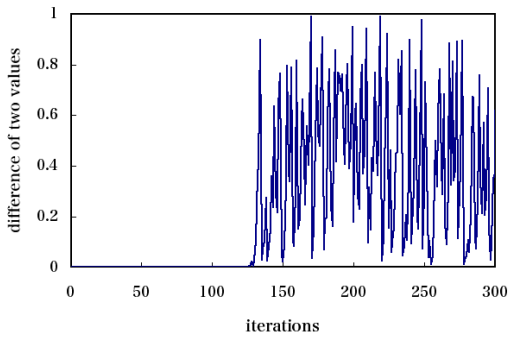

Fig. 6. Difference of two values.

From this figure, there are no large differences of two values until the iteration exceeds 150 times. It is undesirable to use

the range of $N < 150$ as the key. We can see the difference of two values that have changed nonuniformity for $N > 150$. Therefore, we determine that the number of iterations are arbitrary value over 150 times.

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

V. Security Analysis

A. Public Key

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

We investigate the security of the proposed cryptosystem that the public keys $X_0 = 0.41234$ and $X_A = 0.24739$ are attacked by the eavesdroppers with the brute force attack. Table 2 shows results of the brute force attack for the limited case of $N < 50$ and $\alpha = 5$ $digits$.

TABLE II
Results of the brute force attack.

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

This results are solutions of keys in limited case, however the eavesdropper can detect a lots of values. An important thing is that the all of values are correct keys for the eavesdroppers who knows only $X_0 = 0.41234$ and $X_A = 0.24739$. If the eavesdroppers chooses a really correct key in Table 2, it is necessary to know the value of the α or the value of the A. Those parameters are known to only the decryptor and the encryptor. Moreover, 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 modified logistic map are a long-term sequences.

For that reason, 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. And we used X_0 and X_A as public keys.

B. 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 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} 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 iterations to calculate the parameter α.

In addition, the encryptor can easily change the number of 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.

VI. Conclusions

In this research, we have proposed a cryptosystem using iterations of a modified chaotic map. And we have investigated vulnerability of this cryptosystem. This cryptosystem is a symmetric-key cryptography that has a characteristic of a public-key cryptography. The number of the delivery of the keys has decreased to using this cryptosystem.

As the future subject, we investigate security of the proposed 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.

[10] "The GNU MP Bignum Library," http://gmplib. org/