The 15th IEEE International Workshop on Nonlinear Dynamics of Electronic Systems
NDES'07, Tokushima, Japan, July 23-26, 2007

A Chaotic Cryptosystem Using Lyapunov Exponent

Shuichi Aono†, 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 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 using Lyapunov exponent of a chaotic map. This cryptosystem is a symmetric-key cryptography that has a public key. We investigate the vulnerability of this cryptosystem.

1. 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 the Lyapunov exponent of a chaotic map. And we investigate the vulnerability of this cryptosystem. This cryptosystem uses the Lyapunov exponent until convergence 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:

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

where α is a parameter changing the top of the map. This map is shown in Fig. 1. The generated sequences looks like the 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 $\alpha = 0.5$.

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 relation of two successive numbers. In

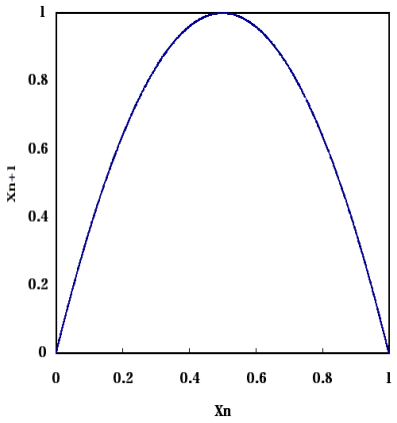

Figure 1: Modified logistic map F. ($\alpha = 0.5$)

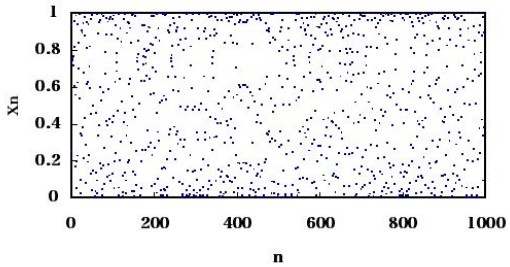

Figure 2: Chaotic sequence. ($\alpha = 0.5$)

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.

The Lyapunov exponent of this map is expressed as the following equation.

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \log |F'(X_k)| \tag{2}$$

Figure 3 shows the Lyapunov exponent generated by the modified logistic map. Horizontal axis shows the value of α, vertical axis shows the value of the Lyapunov exponent. We can see that the Lyapunov exponent depends on the value of α.

The Lyapunov exponent converges to a constant value without depending on an initial value. In this research, we use the Lyapunov exponent until convergence. The finite Lyapunov exponent is expressed as the following equation.

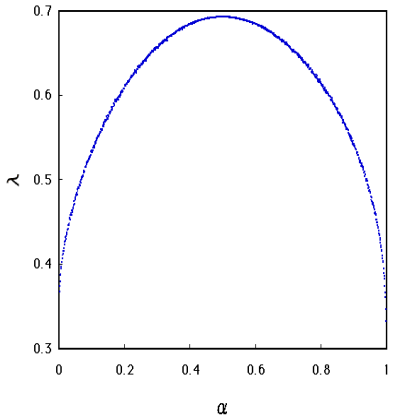

Figure 3: Lyapunov exponent of the modified logistic map.

$$\lambda_L(X_k) = \frac{1}{L} \sum_{k=0}^{L-1} \log |F'(X_k)| \tag{3}$$

This function has sensitivity to a change in initial value X_0 and a value of L. Figure 4 shows the relation between λ_L and L. We can see that the range of the value of λ_L is changing with the values of L.

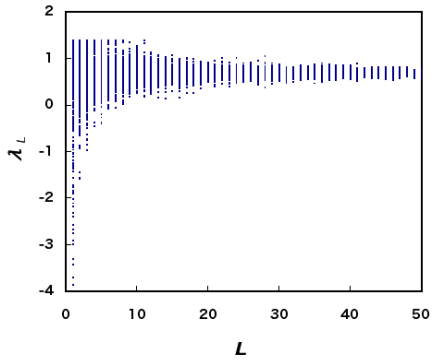

Figure 4: Relation between λ_L and L.

3. A Chaotic Cryptosystem

We propose a cryptosystem by using the Lyapunov exponent of a modified logistic map. The simplified block diagram of the cryptosystem is shown in Fig. 5. This cryptosysytem is composed of the following three parts. Key generation, encryption process and decryption process.

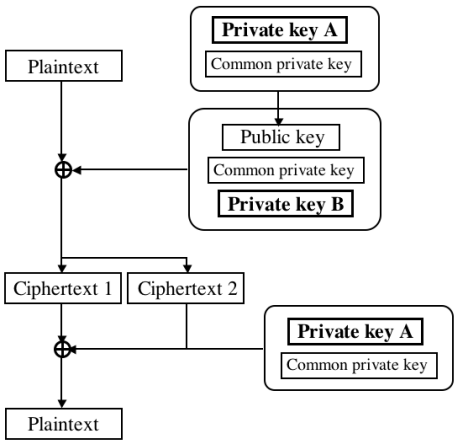

Figure 5: Block diagram of the cryptosystem.

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, parameters α and L, here α and L are common private keys. 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 public keys, α, L as common private keys and A as a private key.

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

3.2. Encryption Process

We explain an 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 :

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

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 $C_1 - \lambda_L(F^A(C_2))$ by using a private key A.

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

And decrypt the plaintext M. An important thing is that there is no need to calculates the value of B. The decryptor uses only common private keys and private key A for the decryption.

3.4. Requirements for Cryptosystem

The key space size and plaintext size are required over 128 bits (40 digits) for the defense against brute force attack. It is not necessary to consider the effect of rounding error of the sequences generated by the modified logistic maps. Because only the direction of the expansion is used. Therefore, we truncate a number to 40 decimal places by the iteration of the maps. And the ciphertext sizes are defined the same as the plaintext.

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

- α 40 digits.
- X_0, $X_A (\in 0, 1)$ and M 40 digits.
- C_1 and C_2 40 digits.

Next, we investigate the numbers of iterations A and B. The cipher-breaking becomes difficult by increasing this value. The calculation time of the 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 $X_0 = 0.2$ and the case of $X_0 = 0.2 + 10^{-40}$. The horizontal axis shows the number of the iterations, and the vertical axis shows the difference between the generated sequences.

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 keys. 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.

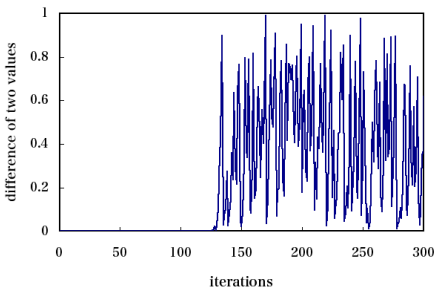

Figure 6: Difference of two values for $X_0 = 0.2$ and $X_0 = 0.2 + 10^{-40}$.

4. Security Analysis

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_A. Therefore, we open X_0 and X_A to the public as public keys. Moreover, there is a possibility that all of the parameter α generates the value of X_A after the 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.

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. When this cryptosystem is attacked by a CPA, and encryptor selects the same value B, the eavesdroppers can easily obtain two values as $\lambda_L(X_{A+B})$ and X_B. However, it is difficult for eavesdroppers to obtain correct A, B and α from the value of X_0, X_A, X_B and $\lambda_L(X_{A+B})$. 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 private key at the encryption.

5. Conclusions

In this research, we have proposed a cryptosystem using the Lyapunov exponent 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 investigate security of the proposed cryptosystem in more detail. And we apply the proposed cryptosytem 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.