2008 International Symposium on Nonlinear Theory and its Applications
NOLTA'08, Budapest, Hungary, September 7-10, 2008

Chaotic Map with Parameter Changing Shape of the Map for a Cryptosystem

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 propose a chaotic map with parameter changing the shape of the map. And we propose a cryptosystem using a chaotic map. A characteristic of the proposed cryptosystem is that different ciphertexts are generated from the same plaintext. The ciphertext depends on the private key of the encryptor. This cryptosystem is a symmetric-key cryptography that has an advantage of public-key cryptography. We investigate the vulnerability of this cryptosystem.

1. Introduction

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[1][2]. A chaotic cryptosystem is researched for the application of chaos in engineering field [3]-[9].

Some 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 its 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 this research, we propose a chaotic map that has a parameter changing the shape of the map. And we propose a cryptosystem using this proposed chaotic map. A characteristic of the proposed cryptosystem is that a different ciphertexts are generated from the same plaintext. The ciphertext depends on the public key of the 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.

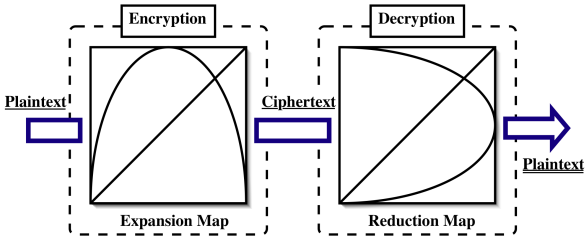


Figure 1: Basic chaotic cryptosystem

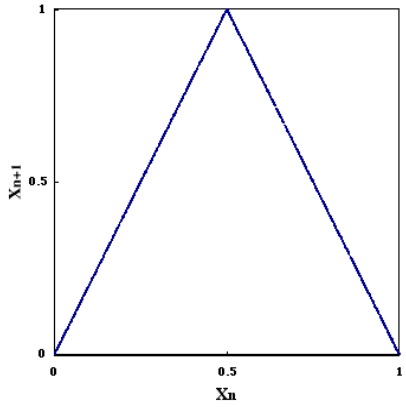
2. Chaotic Map

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

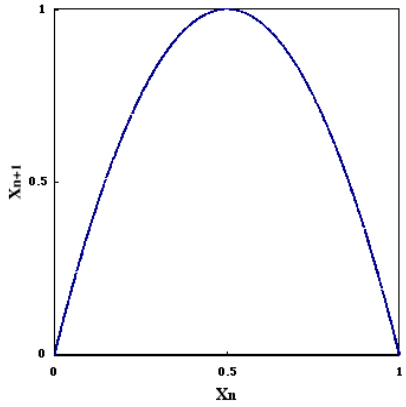
$$F : \begin{cases} X_{n+1} = 1 - (1 - \dfrac{X_n}{\alpha})^{\frac{1}{\beta}} & (0 \le X_n \le \alpha) \\ X_{n+1} = 1 - (\dfrac{X_n - \alpha}{1 - \alpha})^{\frac{1}{\beta}} & (\alpha < X_n \le 1) \end{cases} \tag{1}$$

where α and β are parameters changing the central coordinate and shape of the map.

The shape of the modified chaotic map is changed by combinations of α and β. Therefore, the feature of the generated sequences is determined by these parameters. For example, the modified chaotic map becomes a tent map at the case of $\alpha = 0.5$ and $\beta = 1.0$. In the case of $\alpha = 0.5$ and $\beta = 0.5$, the modified chaotic map becomes a logistic map. These maps are shown in Fig. 2.



(a)



(b)

Figure 2: Modified chaotic map ($\alpha = 0.5$, (a) $\beta = 1.0$, (b) $\beta = 0.5$)

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

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

Figure 3 shows the Lyapunov of the modified chaotic map that changes the value of β. The horizontal axis shows the value of β, and the vertical axis shows the value of the Lyapunov exponent. We can see that the value of the Lyapunov exponent is a positive value in the range of $\beta \in [0.2, 1.0]$.

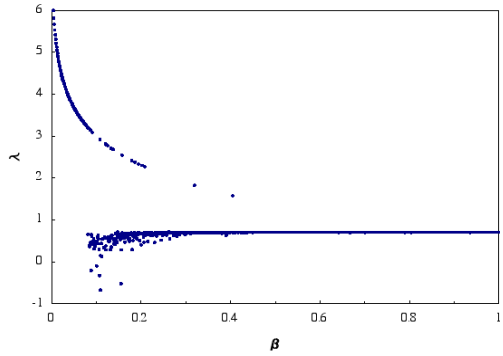


Figure 3: Lyapunov exponent of modified chaotic map.

The modified chaotic map has sensitivity to a change in parameters α, β and the initial state X_0. Therefore, a long-term forecast becomes impossible by iterating the map. However, the modified chaotic map is expressed by simple equations. If the number of iterations n and parameters α and β are known, it is easy to calculate X_n from initial value X_0. In other words, it is necessary to know both the number of iterations and parameters to calculate the correct X_n. Similarly, it is difficult to calculate parameters α, β and n from X_0 and X_n. In this research, we use parameters α and β as a shared secret keys.

3. Proposed Cryptosystem

We propose a cryptosystem by using iteration of the modified chaotic map. In order to adopt the private key for symmetric-key cryptography, the chosen private key must be negated by the decryptor in the decryption process. We use the following characteristics of a chaotic map to solve this problem.

$$F^B \circ F^A(X_0) = F^A \circ F^B(X_0) \tag{3}$$

where A and B are the number of iterations.

The proposed cryptosystem is composed of the following three parts. The key generation, the encryption process and the decryption process.

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 a 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 sets an initial point for X_0, parameters α and β. Here, α and β are shared secret keys. In addition, set the number of iterations A. This value A is a private key for the

decryptor. The decryptor keeps a private key A secretly. $X_A = F^A(X_0)$, namely, A-time iterations of the modified chaotic map F are calculated.

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

- X_0, X_A : public key.
- α, β : 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 :

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

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.

3.3. Decryption process

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

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

The plaintext M is decrypted. In this cryptosystem, we use only the expansion map for encryption and decryption by adopting the private keys. An important thing is that there is no need to calculates the value of B. The decryptor uses only the shared secret keys α, β and the private key A for decryption.

4. Security Analysis

4.1. Shared secret key space size

The shared secret key space size 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. We determined the key space sizes as follows :

- $\alpha \in [0, 1] : 40\ digits, \beta \in [0.2, 1.0] : 10\ digits.$

In the proposed cryptosystem, the modified chaotic map is changed by combinations of α and β. Namely, the key space size of this cryptosystem equals the key space of α times the key space of β. If there is no effective shortcut attack, the key space size is computationally-secure key space. Next, we consider the rounding error by the discrete chaotic map. We truncate X_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. We use a GNU Multiple Precision Arithmetic Library (GMP) [10] to implement the proposed cryptosystem. GMP is a library for arbitrary precision arithmetic, operating on signed integers, rational numbers, and floating point numbers.

4.2. Private key space size

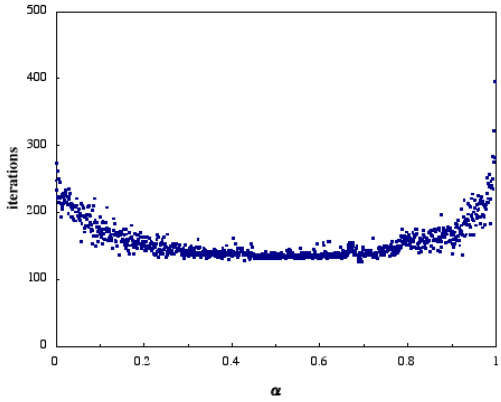
We investigate the numbers of iterations A and B as the private keys. The security of the proposed cryptosystem depends on the parameters α and β. Hence, it is not necessary to ensure the large key space for A and B against the brute force attack. However, the number of iterations should be large enough to ensure α and β sensitivity. The modified chaotic map has a sensitivity to a change in the parameter. Small variations of the parameter produce large variations by iterating the map. Therefore, cipher-breaking becomes difficult by increasing the numbers of iterations. However, if the number of iteration is small, there are no large differences between the variations of the parameters. It is undesirable to use as small number of iterations as keys.

In order to determine the number of iterations, we simulated the sequences generated with slightly different keys. Figure 4 (a) shows the difference of the generated values X_n between the case of α and the case of $\alpha + 10^{-40}$. The horizontal axis shows the value of α, and the vertical axis shows the first number of iterations when the difference between two values becomes larger than 0.5. And, the difference of the two values between the case of β and the case of $\beta + 10^{-10}$ is shown in Fig. 4 (b). From this figure, we determine that the number of iterations is larger than 500.

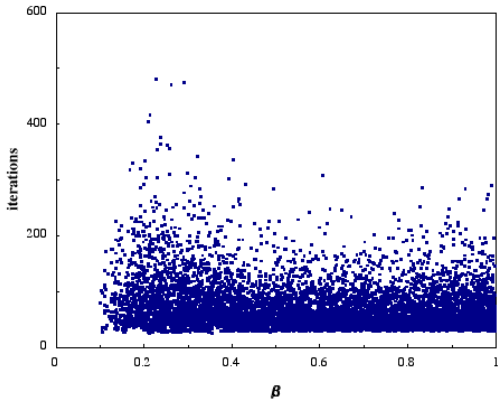
4.3. Public key consideration

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 pair of parameters α and β generates the value of X_A after N-times iterations. Because the generated sequences by the modified chaotic map are a long-term sequences. Surely, we secure enough key space size in consideration of brute force attack. The eavesdropper cannot decide the correct key and does not know whether the obtained key is correct key or not, even if the eavesdroppers search all of the keys by brute force attack.

For that reason, It is difficult for eavesdroppers to obtain correct α, β and A from the value of X_0 and X_A. We



(a)



(b)

Figure 4: Difference between two values for (a) α and $\alpha + 10^{-40}$, (b) β and $\beta + 10^{-10}$

thought that the values of α, β 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.

4.4. 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. Though an eavesdropper can easily obtain two values X_{A+B} and X_B from a pair of plaintext and its ciphertexts by using the difference between the two ciphertexts, it is difficult for the eavesdropper to obtain correct A, B, α, β from X_A, X_B and X_{A+B}. For this reason, we consider that the CPA is not effective compared with the brute force attack.

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. We think that this feature is an advantage compared with the conventional chaotic symmetric-key cryptosystem. The security of the cryptosystem becomes safer by setting the different private key at the encryption.

5. Conclusions

In this research, we have proposed a modified chaotic map with parameter changing the shape of the map. And we have proposed a cryptosystem using this 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. In particular, independent and identically distributed of the generated sequences. The sequences generated by the modified chaotic map is not uniform for some parameter β. Therefore, we need to adopt the protocol such as using the lower bit of generated sequences. 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] 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.

[3] G. Jakimoski and 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.

[4] X. Yi, "Hash function based on chaotic tent maps," IEEE Trans. Circuits and Systems II, vol. 52, no. 6, pp. 354-357, 2005.

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

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

[9] K. Y. Cheong and 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] "The GNU MP Bignum Library," http://gmplib. org/