17-15 **A Chaotic Map with Variable Parameters to Design Cryptosystem**

Shuichi Aono and Yoshifumi Nishio

(Tokushima University)

1. Introduction

A chaotic map has sensitivity to a change in 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].

In this study, we propose a chaotic map that has a variable parameters. And we propose a cryptosystem using this proposed chaotic map. A characteristic of the proposed cryptosystem is that different ciphertexts are generated from the same plaintext.

2. Chaotic Map

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

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

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. Figure 1 shows the Lyapunov of the modified chaotic map that changes the value of β. We can see that the value of the Lyapunov exponent is a positive value in the range of $\beta \in [0.2, 1.0]$.

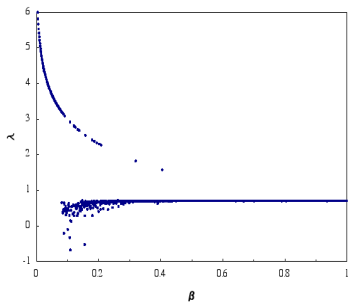

Figure 1: Lyapunov exponent of modified chaotic map.

3. Proposed Cryptosystem

We propose a cryptosystem by using the following characteristics of a chaotic map.

$$F^B_{\alpha\beta} \circ F^A_{\alpha\beta}(X_0) = F^A_{\alpha\beta} \circ F^B_{\alpha\beta}(X_0) \tag{2}$$

where A and B are the number of iterations.

The proposed cryptosystem uses three kind of keys, a public key, a private key and a shared secret key. The proposed cryptosystem is composed of the following three parts.

3.1. Key generation

A decryptor sets an initial point for X_0 and 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. $X_A = F^A_{\alpha\beta}(X_0)$, namely, A-time iterations of the modified chaotic map $F_{\alpha\beta}$ are calculated. The decryptor obtains X_0, X_A as public keys, α, β as shared secret keys and A as a private key.

3.2. Encryption process

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:

$$\begin{aligned} C_1 &= M + F^B_{\alpha\beta}(X_A) = M + X_{A+B} \\ C_2 &= F^B_{\alpha\beta}(X_0) = X_B \end{aligned} \tag{3}$$

where M is a plaintext.

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

3.3. Decryption process

In the decryption process, a decryptor calculates $C_1 - F^A_{\alpha\beta}(C_2)$ by using the shared secret keys and the private key A.

$$\begin{aligned} C_1 - F^A_{\alpha\beta}(C_2) &= M + X_{A+B} - F^A_{\alpha\beta}(X_B) \\ &= M + X_{A+B} - X_{B+A} \\ &= M \end{aligned} \tag{4}$$

The plaintext M is decrypted. An important thing is that there is no need to calculates the value of B.

4. Conclusions

In this study, we have proposed a modified chaotic map that has a variable parameters. And we have proposed a cryptosystem using this chaotic map.

As the future subject, the security of the proposed cryptosystem will be investigated in more detail.

References

[1] L. Kocarev, “Chaos-Based Cryptography : A Brief Overview, ” IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.