17 - 22

Uniformity of Ciphertext Generated by Two Chaotic Maps

Shuichi Aono†, Yoshifumi Nishio†

† Department of Electrical and Electronic Engineering
Tokushima University

1. Introduction

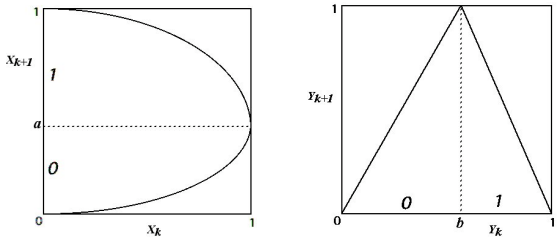
A chaotic map has sensitivity to a change in initial conditions and parameters, and a long-term forecast becomes impossible by the iterations of a chaotic map. For that reason, it is effective to use chaotic maps for cryptosystems. The chaotic cryptosystem is researched as an application of chaos in an engineering field. On the other hand, the security of the chaotic cryptosystem is not investigated in detail. It is necessary to investigate the security and to clarify the vulnerability of the chaotic cryptosystem.

A cryptosystem using the tent map has been proposed [1]. A cryptosystem using two chaotic maps has been also proposed [2]. This system performed encryption and decryption by using two chaotic maps, a skew tent map and a logistic map, and their inverse maps. The method of repeating the encryption process twice has been proposed [3]. This method used the same map as the first encryption and the second encryption.

In this research, we propose the method of repeating the encryption process twice by using different chaotic maps, and investigate the uniformity of the generated ciphertext.

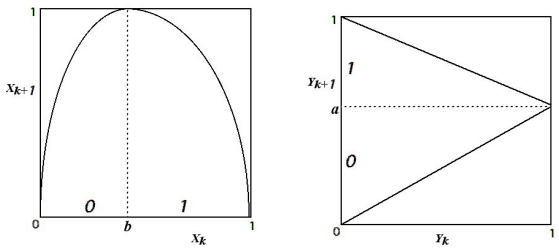
2. Proposed Cryptosystem

The proposed method repeats the encryption process twice. The encryption maps are shown in Figs. 1 and 2.



(a) (b)

Figure 1: 1st encryption map F_1.



(a) (b)

Figure 2: 2nd encryption map F_2.

where F_1 is the first encryption map and F_2 is the second encryption map. a and b are private keys in this cryptosystem.

In the first encryption process, set an initial point Y_0 as a plaintext and X_0 as a subtext, where, X_0 is an arbitrary value. Calculate $(X_n, Y_n) = F^n(X_0, Y_0)$, namely n-times iterations of F_1.

In the second encryption process, set an initial point $X'_0 = X_n$, where X_n is obtained by the first encryption process. Calculate n-times $F(X'_0, Y'_0)$, we can obtain Y'_n from $F^n(X'_0, Y'_0) = (X'_n, Y'_n)$ as a ciphertext. And send this value Y'_n to the receiver.

The decryption function F^{-1} is a function that replaces a with b of the encryption function F.

3. Simulated Results

In this research, we investigate the correlation of the plaintext and the ciphertext. We use χ^2 test for the uniformity. This χ^2 test examines the distribution of ciphertext encrypted with different keys. The upper 5% of this χ^2 is 16.9. If the value of χ^2 test is 16.9 or less, the uniformity of the ciphertext is guaranteed.

The simulated results for 5 different plaintexts are shown in Table 1.

Table 1: The results of the χ^2 test.

Plaintext	Conventional method	Proposed method
P_1	464.70	7.90
P_2	435.08	7.28
P_3	489.06	11.20
P_4	451.06	13.82
P_5	544.06	10.50

4. Conclusions

In this research, we have investigated the uniformity of the ciphertext. By simulated results, we confirmed that the distribution of the ciphertext is uniformity.

References

[1] T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A Secret Key Chaotic Map," Trans. IEICE, vol. E73, no. 7, pp. 1041-1044, 1990.

[2] M. Harada, Y. Nishio and A. Ushida, "A Cryptosystem Using Two Chaotic Maps," Proceedings of NOLTA'99, vol. 2, pp. 609-611, 1999.

[3] S. Aono, M. Wada and Y. Nishio, "Improvement of a Cryptosystem Using Two Chaotic Maps," Proceedings of RISP International Workshop on Nonlinear Circuits and Signal Processing (NCSP'06), pp. 349-352, 2006.