A Cryptosystem Using Chaotic Map with Variable Parameter

Shuichi AONO
Dept. Electrical and Electronic Eng.,
Tokushima University
Email: aoichi@ee.tokushima-u.ac.jp

Yoshifumi NISHIO
Dept. Electrical and Electronic Eng.,
Tokushima University
Email: nishio@ee.tokushima-u.ac.jp

SUMMARY

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][2]. A chaotic cryptosystem is researched for the application of chaos in engineering field [3]-[7].

In our previous research, we have proposed a modified chaotic map that has a parameter changing the shape of the map and have proposed a cryptosystem using the modified chaotic map [8]. A characteristic of this cryptosystem is that different ciphertexts are generated from the same plaintext.

The modified chaotic map is expressed as the following equation:

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

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. Namely, the feature of the generated sequences is determined by these parameters.

In this research, we investigate features of the modified chaotic map when the parameters α and β was changed. We use parameters α and β as a shared secret keys in the cryptosystem in [8]. Hence, it is important for the security of the proposed cryptosystem to investigate the correlation between the generated sequences and the parameters. It influences the vulnerability of the cryptosystem.

REFERENCES

[1] L. Kocarev, "Chaos-based cryptography : a brief overview, " IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.
[2] K. Kelber and W. Schwarz, "Some design rules for chaos-based encryption systems," International Journal of Bifurcation and Chaos, vol. 17, no. 10, pp. 3703-3707, 2007.
[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] M. Harada, Y. Nishio and A. Ushida, "A cryptosystem using two chaotic maps," Proceedings of NOLTA'99, vol. 2, pp. 609-611, 1999.
[5] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," IEEE Trans. Circuits and Systems I, vol. 49, pp. 28-40, 2002.
[6] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps, " Proceedings of ISCAS'03, vol. 3, pp. 28-31, 2003.
[7] X. Yi, "Hash function based on chaotic tent maps," IEEE Trans. Circuits and Systems II, vol. 52, no. 6, pp. 354-357, 2005.
[8] S. Aono and Y. Nishio, "Chaotic map with parameter changing shape of the map for a cryptosystem, " Proceedings of NOLTA'08, 2008 (printing).