2007 RISP International Workshop on Nonlinear Circuits and Signal Processing (NCSP'07)
Shanghai Jiao Tong University, Shanghai, China, Mar. 3-6, 2007

A User Authentication Protocol Using Chaotic Maps

Shuichi Aono†, Yoshifumi Nishio†

† Department of Electrical and Electronic Engineering, Tokushima University
2-1 Minami-Josanjima, Tokushima, 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 an authentication protocol by three times of the authentication interaction. This authentication protocol based on the iteration of the coupled logistic maps in a public-key cryptography. We investigate the vulnerability of this user authentication protocol.

1. Introduction

A chaotic map has various features. 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 cryptosystem using the chaos map [7][8]. There is a possibility to be linear 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 apply the public key cryptosystem. It is difficult to develop trap door in the chaotic maps. The other is that the equation form is opened to the public. A chaotic map is shown by the equation based on determinism. If the equation of the chaotic map and their parameters are opened to the public, the behavior of the sequences is known.

A simplest but important thing is authentication technology in the cryptography. An authentication technology based on public-key cryptography has two patterns. One is a digital signature. This authentication proves the correctness of the data. The other is a user authentication. This authentication proves the correctness of the user. A zero-knowledge proof is an interactive method for one party to prove to another that a statement is true, without revealing anything other than the veracity of the statement. In a user authentication, the zero-knowledge proof is an ideal in safety, but the number of the authentication interaction becomes large.

In this research, we use an authentication protocol by three times of the authentication interaction. This authentication protocol based on iterations of the logistic maps in a public-key cryptography. We investigate the vulnerability of this user authentication protocol.

2. Chaotic Map

A logistic map is one of the simplest chaotic maps. The logistic map is expressed as the following equation:

$$X_{n+1} = \alpha X_n(1 - X_n) \tag{1}$$

where α is a control parameter changing the behavior of the generated sequence.

This map is shown in Fig. 1. Figure 2 shows an example of chaotic sequences generated by the logistic map. The behavior like the uniform random number is seen in $\alpha = 4.0$.

In this research, we propose a user authentication protocol by using iterations of a chaotic map. We use coupled logistic maps as a chaotic map. The coupled logistic

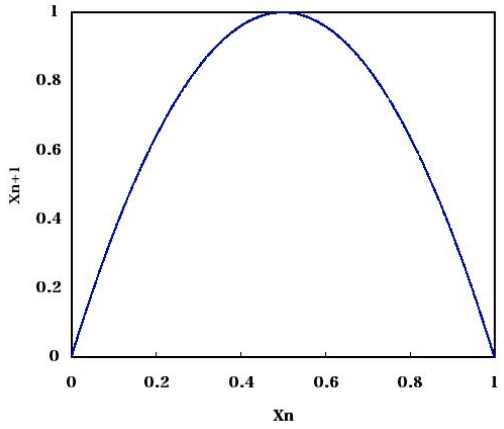

Figure 1: Logistic map. ($\alpha = 4.0$)

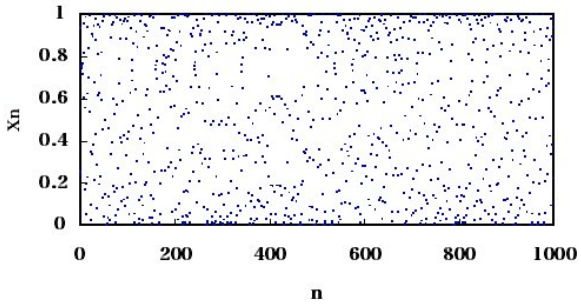

Figure 2: Chaotic sequence. ($\alpha = 4.0$)

maps are expressed as follows;

$$\begin{cases} X_{n+1} = \alpha X_n(1 - X_n) + \beta(Y_n - X_n) \\ Y_{n+1} = \alpha Y_n(1 - Y_n) + \beta(X_n - Y_n) \end{cases} \tag{2}$$

where α and β are parameters changing the behavior of the sequences.

This map is shown in Fig. 3. Figures 4 and 5 show the chaotic sequences of X_n and Y_n. The generated sequences looks like the uniform random number, though they have some bias. Figure 6 shows a relation between the value of X_n and the value of Y_n generated by the coupled logistic maps.

In this research, we use parameters $\alpha = 3.7$ and $\beta = 0.006$. This map has sensitivity to a change in initial conditions X_0 and Y_0. Therefore, a long-term forecast becomes impossible by the iterations of the maps.

The coupled logistic maps are based on easy equations.

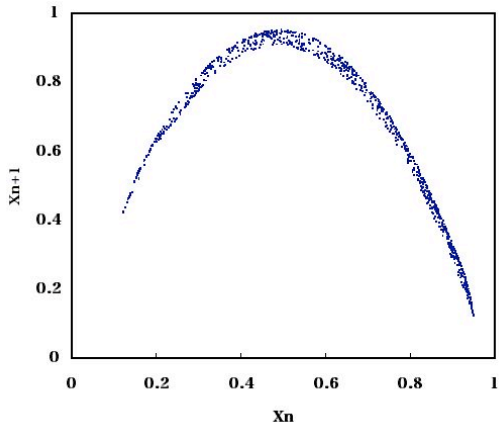

Figure 3: Coupled logistic maps. ($\alpha = 3.7, \beta = 0.06$)

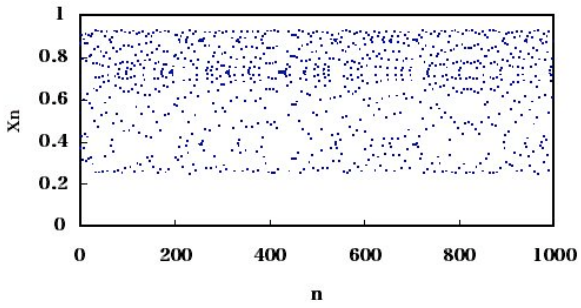

Figure 4: Chaotic sequence of X_n. ($\alpha = 3.7, \beta = 0.006$)

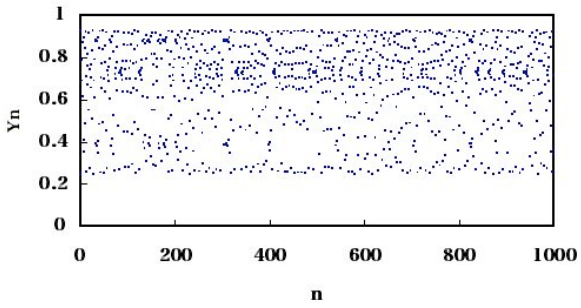

Figure 5: Chaotic sequence of Y_n. ($\alpha = 3.7, \beta = 0.006$)

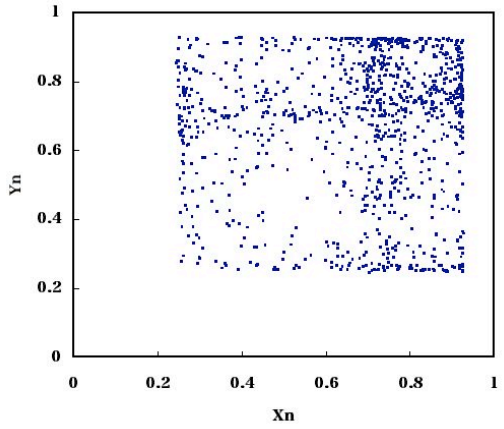

Figure 6: Relation between X_n and Y_n

It is necessary to know the number of iterations of the coupled logistic maps to obtain α and β. If the number of iterations n is unknown, it is difficult to obtain correct α and β from the value of X_0 and X_n. In a similar way, it is very difficult to obtain correct X_0 and Y_0 from the value of X_n and Y_n. Calculating the reverse-map becomes solving the polynomial equation derived from the coupled logistic maps. The polynomial equation can not be solved without knowing the correct values both of X_n and Y_n.

3. A User Authentication Protocol

The encryption technology has the function of defending information, and becomes the element of other information security technologies like the digital signature etc. A user authentication protocol is a simplest but important technology in the cryptography. In a user authentication, the zero-knowledge proof is an ideal in safety. This proof is an interactive method for one party to prove to another that a statement is true, without revealing anything other than the veracity of the statement.

However the zero-knowledge proof has a disadvantage to implement. the number of the authentication interaction becomes large. The number of the interaction of zero-knowledge proof must be four times or more. Then, the user authentication protocol of three times in the number of interactions has been proposed. This authentication protocol shown in Fig. 7.

Prover generated public key and private key, and opens the public key to the public. Prover and verifier interact three times between each other. Verifier authenticates whether to accept or to reject.

As for this protocol, safety has been proven though it is not zero-knowledge proof. The safety of this protocol is based on the difficulty of the factorization on prime numbers problem and the discrete logarithm problem. Therefore, this protocol is one of the ideal user authentication. Because this protocol is efficient and high safety. Moreover, there is an advantage that there is a method of conversion into a digital signature in the authentication protocol by three times of the authentication interaction.

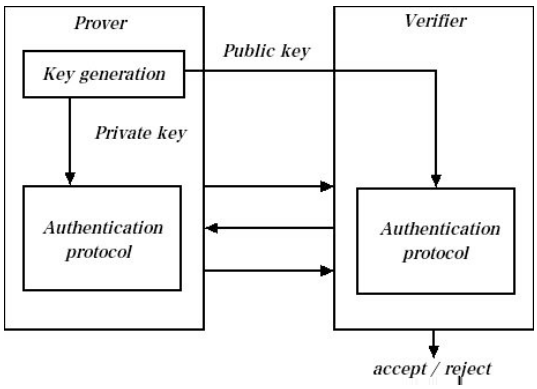

Figure 7: A user authentication protocol.

4. Proposed Authentication Protocol

In this research, we propose a user authentication protocol by using the coupled chaotic maps. This authentication protocol is composed of the following parts.

4.1. Key generation

A prover sets initial points X_0 and Y_0 of Eq. (1). In addition, set a number of iterations A_1, A_2. Here, The value of A_1 and A_2 are k bits. Calculate $(X_{A_1}, Y_{A_1}) = F^{A_1}(X_0, Y_0)$, namely A_1-time iterations of coupled logistic maps F. And calculate $(X_{A_2}, Y_{A_2}) = F^{A_2}(X_0, Y_0)$, namely A_2-time iterations of coupled logistic maps F. Also $(X_A, Y_A) = (X_{A_1} \cdot X_{A_2}, Y_{A_1} \cdot Y_{A_2})$

- private key : A_1, A_2, X_0, Y_0.
- public key : (X_A, Y_A)

4.2. Authentication protocol

A prover and a verifier interact three times in this user authentication protocol.

- step 1
  A prover selects k bits numbers B_1 and B_2.
  A relationship between B_1 and B_2 as follows :

$$\begin{cases} A_1 - B_1 = A_2 - B_2 \\ \quad or \\ A_1 - B_2 = A_2 - B_1 \end{cases} \tag{3}$$

  where, $(0 < B_1, B_2 < A_1, A_2)$

  Calculate (X_{B_1}, Y_{B_1}) and (X_{B_2}, Y_{B_2}). Send these values to the verifier.

- step 2
  A verifier chooses the $k-1$ bit value C as an arbitrary value. Send this value C to the prover.

- step 3
  A prover calculates the value of D.

$$\begin{cases} D = A_1 - B_1 - C \\ \quad or \\ D = A_1 - B_2 - C \end{cases} \tag{4}$$

  This means that the prover uses the equation selected by step 1.

- step 4
  A verifier confirms that the following equation is satisfied.

$$F^D F^C(X_{B_1}, Y_{B_1}) \cdot F^D F^C(X_{B_2}, Y_{B_2}) = (X_A, Y_A) \tag{5}$$

In this authentication protocol, the eavesdroppers can not calculate correct keys from (X_A, Y_A). But, a prover send the value of (X_{B_1}, Y_{B_1}) to the verifier. The verifier can calculate the correct time series sequences after B_1 iterations. There is a disadvantage that this authentication protocol is weak to the impersonation. Therefore, it is a future subject to develop the authentication protocol that does not send significant information.

5. Conclusions

In this research, we have proposed an authentication protocol by three times of the authentication interaction. This authentication protocol based on iterations of the coupled logistic maps.

As the future subject, we investigate security of the proposed authentication protocol in more detail. And we apply authentication protocols by using iterations of a chaotic map to the digital signature.

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.