2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Qualities of the Chaotic Signal Generator for One-Time Password System

Koki Tada†, Hiroshi Kobayashi†and Hiroyuki Kamata‡

†Graduate School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571 Japan
‡School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571 Japan
Email: kamata@isc.meiji.ac.jp

Abstract—In this paper, we examine the qualities of chaotic signal modulators when the chaotic system is applied to One-Time Password(OTP) system. The One-Time Password system is an important technique in the user-authentication for the network computing. The same password cannot be used twice in the authentication system, so the masquerade by the third party can be prevented. In this study, it is verified whether the chaos modulator is effective to the One-Time Password system.

1. Introduction

In the field of network computing, the user-authentication is most important problem for maintaining the information security. In the field of the information security, many authentication techniques, which use the fingerprint, the voice, the retina and so on, have been proposed. However, these techniques, which use the medical information of human, need to append sensitive and expensive sensors. Moreover, these medical information are changed following the time elapses, so to keep the authentication system using medical information in itself is a hard task.

Besides, the authentication using the user-ID and password is still popular technique. However, the technique depends on the user's conscience; therefore the system often becomes a bottle neck of the information security.

As a technique to resolve the problem, One-Time Password(OTP) system[1] has been proposed. The system generates the password code based on the user's keyword and some parameters. The generated passwords are given to the user via the other systems, such as a mobile phone system, E-mail or a special module. Furthermore, every time the different password code is generated, and the user can never again log in the computer by the same password that is used once. Therefore, even if the password has leaked out, the information security is maintained.

Usually, the One-Time password is generated using the Hash function[2, 3]. The Hash function is a technique that converts the any-length characters into the fixed-length pseudo-random unique code. Namely, when the original characters given to the Hash function are different, the same random codes are not generated theoretically, so the technique is also applied to the investigation whether the digital data was correctly transmitted to receivers using computer networks. Moreover, the original characters can never be recovered from the generated pseudo-random code.

On the other hands, the chaotic system has also unstable orbit[4]. Namely, if the parameter is different, it is expected that the different chaotic signal can be generated. Moreover, we have proposed the chaotic modulator that uses the overflow and round-off functions[5]. These functions have properties that lose the numerical information, so the original information is never recovered as long as the parameters of the chaotic system does not leak out.

However, the generated signal becomes pseudo chaos when the finite bit-length computation is used. Therefore, even if different parameters are used, the chaotic signal is occasionally converged to the same orbit. It is extremely difficult to verify the property theoretically whether converge to the same orbit. In this study, we try to verify the characteristics of the pseudo chaos by the computer simulation, and evaluate whether the chaos modulator is suitable for the One-Time Password generator.

2. Conditions required to chaos modulators for OTP system

In this chapter, the conditions that are required to the chaos modulator are investigated when the chaos modulator is applied to OTP system[1].

Condition 1 Generated password is a pseudo random code. The chaotic signal which looks like random numbers can be generated, and this problem can be solved easily.

Condition 2 The same password is never generated twice. Because the chaotic signal that is generated by computers becomes pseudo chaos, the periodicity is included in the generated signal. Therefore, the limitation of the number of password-codes which can be used is accompanied. In this research, we suppose no problem on practical use if the period of pseudo chaos is long enough.

Condition 3 The user information cannot be estimated from the generated password.

In the case that the chaotic map is applied to the private communications[5], the synchronization of the chaotic systems both the modulator and demodulator sides becomes the most important element for realizing the perfect recov-

ery of the information. Namely, when the chaotic system is applied to the OTP generator, it is necessary to obstruct the chaos synchronization. To achieve the problem,

· The chaotic signals are decimated and transmitted.

· The bit-length of chaotic signal is shortened and transmitted.

Furthermore, when all of the internal states variables included in the chaos modulator are sent to the demodulator, the parameters of the chaotic modulator can be estimated using Lyapunov exponents analysis based on the time series data[6]. Therefore, the order of chaotic system has to be 2nd or more order system, and only a part of the internal state variables should be transmitted.

Condition 4 It is preferable to be able to set the length of the password arbitrarily.

In the case of chaos modulator, the bit-length of the generated password depends on the computation accuracy. In this study, fixed-point computation is adopted, and the bit-length of generated password is controlled by using a part of bits of the generated internal state variables.

Condition 5 When the unfounded password is given, the system does not approve the authentication.

It is necessary to limit the number of effective passwords in the total of the combination. However, it is difficult to count the number of effective passwords using personal computer. In this study, the operation accuracy is reduced, and the existence probability of the valid password is forecast.

Condition 6 When the user information is different, the generated password is also different.

True chaos has the unstable orbit and the sensitivity to the initial value, so it is impossible to forecast the behavior of the signal. However, in the case of pseudo chaotic signal, these characteristics are deteriorated. Therefore, it is needed to confirm whether there is a problem on practical use. In this research, these problems are especially examined.

3. Chaos modulator for OTP generator

The chaos modulator shown in Figure 1 is adopted in this research in consideration of these conditions. The system are structured by 2 chaotic neurons[8, 7] and 2nd-order linear digital filter[5].

$$x_1(n) = s(n) - g_1(x_1(n-1)) + \alpha x_3(n-2) + \theta_1 \quad (1)$$

$$x_2(n) = x_1(n-1) - g_2(x_2(n-1)) + \theta_2 \quad (2)$$

$$x_3(n) = x_2(n-1) - \beta x_3(n-1) - \gamma x_3(n-2) + \theta_3 \quad (3)$$

The nonlinear functions $g_1(x)$ and $g_2(x)$ are

$$g_k(x) = \begin{cases} \kappa_k x + \sigma_k & : x \le -\epsilon_k \\ \frac{\kappa_k \epsilon_k - \sigma_k}{\epsilon_k} x & : -\epsilon_k < x < \epsilon_k, k = 1, 2 \\ \kappa_k x - \sigma_k & : x \ge \epsilon_k \end{cases} \quad (4)$$

When the system is calculated by fixed-point computation, the overflow $O(x)$ and round-off $R(x)$ functions are

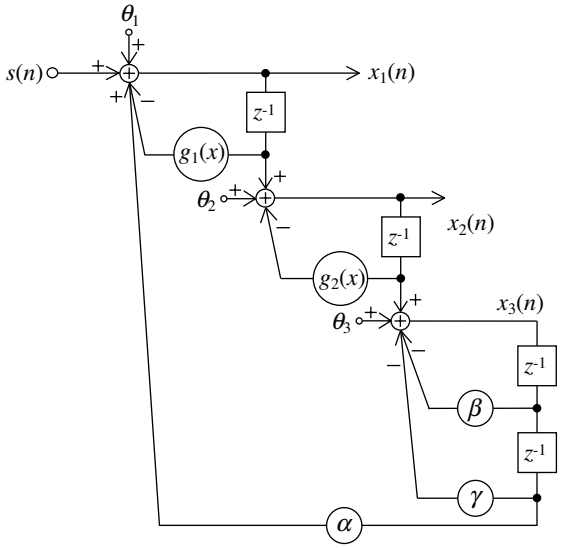

Figure 1: A block diagram of the chaos modulator for OTP generator.

appended.

$$f(x) = O(R(x)) = R(O(x)) \quad (5)$$

When $x_i(k) = f(\hat{x}_i(k))$ for $i = 1, 2, 3$ and $k = n-2, n-1, n$ are assumed, the true dynamics of the proposed system carried out by fixed-point computation are shown as follows:

$$\hat{x}_1(n) = s(n) - g_1(f(\hat{x}_1(n-1))) + \alpha f(\hat{x}_3(n-2)) + \theta_1 \quad (6)$$

$$\hat{x}_2(n) = f(\hat{x}_1(n-1)) - g_2(f(\hat{x}_2(n-1))) + \theta_2 \quad (7)$$

$$\hat{x}_3(n) = f(\hat{x}_2(n-1)) - \beta f(\hat{x}_3(n-1)) - \gamma f(\hat{x}_3(n-2)) + \theta_3 \quad (8)$$

Usually, unstable poles cannot be realized in the linear digital filter shown in Eq. (8). However, the boundness of the proposed system is given by the overflow function $O(x)$ based on the fixed-point computation, so the system which contains an unstable pole can be easily achieved.

Figure 2 shows the distribution of sign of Lyapunov exponents λ_1, λ_2, λ_3 and λ_4 of the proposed chaotic system. In this figure, 16-bit fixed-point computation is adopted, and Q10 format is used[5]. As the figure shows, λ_1 and λ_2 become plus values in all area. Namely, the generated signals by the proposed system always show the property of hyper-chaos. In addition, the area that all Lyapunov exponents show the plus value also exists. The signal with hyper-chaotic property is similar to the pseudo random sequence, so it is suitable for the password code.

4. The number of valid passwords in the total combination.

In this study, $x_1(n)$ and $x_2(n)$ of the proposed system are connected and used for the password code. As the user

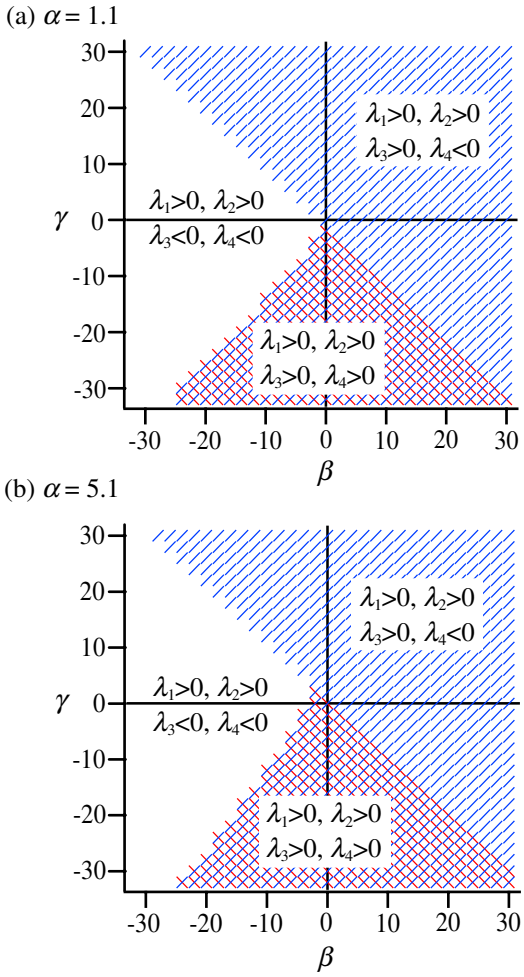

Figure 2: Distribution of the sign of Lyapunov exponents λ_1, λ_2, λ_3 and λ_4 of the proposed chaotic system. 16-bit fixed-point computation and the Q10 format are used. Parameters: $\theta_1 = \theta_2 = \theta_3 = 0.138672$, $\kappa_1 = \kappa_2 = 1.1$, $\sigma_1 = \sigma_2 = 10.1$, $\epsilon_1 = \epsilon_2 = 0.000977$.

information, we try to give the user name to the input signal $s(n)$ by ASCII codes. For examples,

$$s(n) = K, o, k, i, , T, a, d, a, 0, 0, 0, \cdots \quad (9)$$

is used in this experiment.
The format is shown in Figure 3(a). Moreover, we assume that the password is generated using $x_1(n)$ and $x_2(n)$ as shown in Figure 3(b) in this experiment. Namely, the maximum number of combination becomes $2^{24} = 16,777,216$ ways.
The tendency of the password generation is shown in Figure 4. This figure shows (i) the number of kinds of the generated passwords, (ii) the number of times that the same passwords are generated, respectively. As the figure shows, if it is within $10,000$ times, the different passwords are generated every time. The period of the signal generated by the proposed system is longer than $16,777,216$, so if all bits of

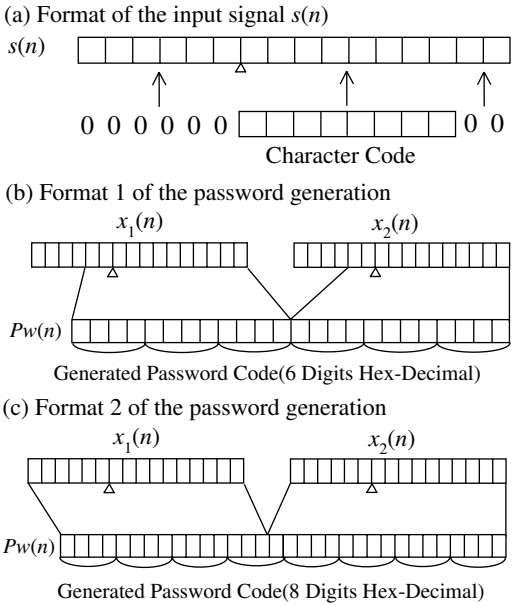

Figure 3: Format of the input signal $s(n)$.

$x_1(n)$ and $x_2(n)$ are used to the password, the valid number of times that the different passwords are generated must be increased. However, because it is difficult to verify it by using personal computer, we are groping for the verification method now, and report later.

5. Difference of generated passwords when the username is different.

In this experiment, the difference of the generated password by the difference of the username is examined. Ideally, if the user name is different, it is preferable that the same password is not generated. However, in the case of chaotic system, there is a possibility to pass the same point from various directions. In this study, if the generated time n is different enough, we assume that the system is practical even if the generated passwords are corresponding.
Figure 5 shows the time that the password $Pw_{user1}(n)$ for the $user1$ = *Koki Tada* corresponds to the password $Pw_{user2}(n)$ for the $user2$ = *Hiroshi Kobayashi*. The same parameters are used for each password generation in this experiment, and only the input signal $s(n)$ is different. Moreover, $4,194,304$ passwords are generated, and the agreement is verified by the round robin. In addition, the format shown in Figure 3(c) is used as the password generation.
The number of times that the same passwords are generated was $4,167$ times in this total iteration of $4,194,304$ times. Moreover, the minimum width of $|n2 - n1|$ that $Pw_{user1}(n1)$ is corresponding to $Pw_{user2}(n2)$ is decreased following the iteration of password-generation progresses. However, we think that the width $|n2 - n1|$ is wide, and the frequency that

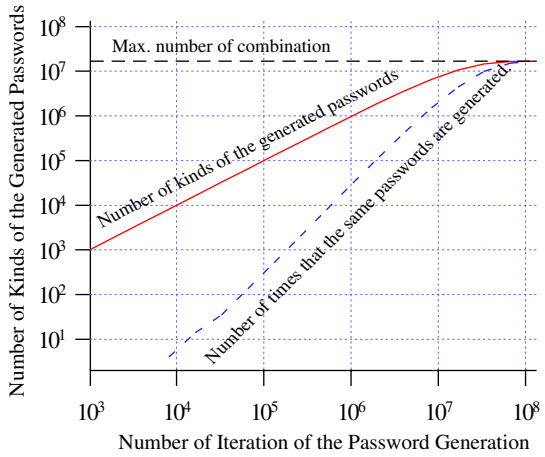

Figure 4: Number of kinds of the generated passwords. The format shown in Figure 3(b) is used for the password generation. Parameters: $\alpha = 5.1$, $\beta = 7.1$, $\gamma = -17.1$, $\theta_1 = \theta_2 = \theta_3 = 0.138672$, $\kappa_1 = \kappa_2 = 1.1$, $\sigma_1 = \sigma_2 = 10.1$, $\epsilon_1 = \epsilon_2 = 0.000977$.

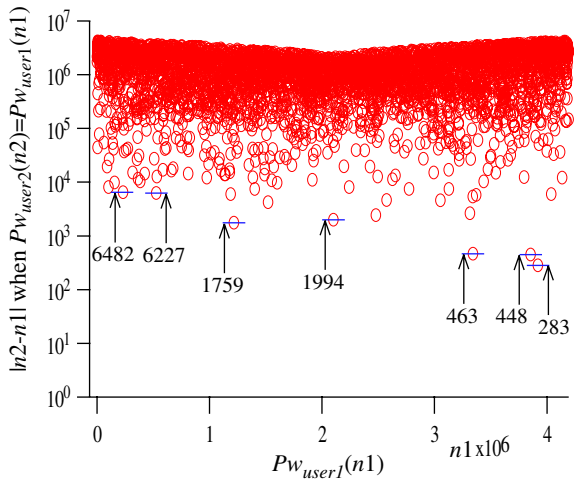

Figure 5: Difference of point $|n2 - n1|$ when the generated password $Pw_{user1}(n1)$ corresponds to the password $Pw_{user2}(n2)$. The format shown in Figure 3(c) is used for the password generation. Parameters: $\alpha = 5.1$, $\beta = 7.1$, $\gamma = -17.1$, $\theta_1 = \theta_2 = \theta_3 = 0.138672$, $\kappa_1 = \kappa_2 = 1.1$, $\sigma_1 = \sigma_2 = 10.1$, $\epsilon_1 = \epsilon_2 = 0.000977$.

the passwords are corresponded is very few in the practical scene, so the OTP generator based on the chaotic system is enough practicable.

6. Conclusions

In this study, the One-Time password generator using chaotic system has been proposed. The proposed system has 2 chaotic neurons and 2nd order linear digital filter, and the system is generated by the fixed-point computation with overflow and round-off properties. Namely, the generated chaotic signal becomes pseudo chaos. However, we think that the characteristic of the generated password is practicable enough based on some experiments. In the future, we attempt to do some examinations in addition, and to verify the reliability of the system.

References

[1] http://www.ietf.org/html.charters/otp-charter.html

[2] http://www.nist.gov/dads/HTML/hash.html

[3] Y. S. Her, K. Sakurai, "Design and Analysis of Block Cipher with Variable Word-Size Based on Dedicated Hash Functions: SHACAL-V", *Workshop on Coding, Cryptography and Combinatorics* , 2003.

[4] T. Kohda, "Discrete Dynamics and Chaos" *CORONA Pub.*, 1998.

[5] H. Kamata, Y. Umezawa, M. Dobashi, T. Endo and Y. Ishida, "Private communications with chaos based on the fixed-point computation" *IEICE, Trans. IEICE*, Vol. E83-A, No. 6, 2000.

[6] T. Sunada, K. Tsutsumi, H. Kamata and T. Endo, "Lyapunov Spectrum Estimation of the Chaotic System that the Numerical Jacobian is Unidentified Though the Dynamics is Clear.", *Proc. NOLTA2002*, pp. 789-792, 2002.

[7] M. D. Restituto, R. L. Ahumada and A. E. Vazquez, "Secure Communication Using CMOS Current-Mode Sampled-Data Circuits". *Proceedings of Nonlinear Dynamics of Electronic System*, pp. 237-240, 1995.

[8] K. Aihara, T. Takebe and M. Toyoda, "Chaotic Neural Networks", *Physical Review Letters A*, Vol. 144, pp. 333-340, Mar 1990.