World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:6, No:11, 2012

Study on the Chaotic Cipher Combined with Mersenne Twister

Daiki Yoshida, Ariyoshi Nakayama, Hirotaka Watanabe,Taichi Sato,
Syuhei Kuriyama, and Hiroyuki Kamata

***Abstract*—**In this study, we propose the chaotic cipher combined with Mersenne Twister that is an extremely good pseudo-random number generator for the secure communications. We investigate the Lyapunov exponent of the proposed system, and evaluate the randomness performance by comparing RC4 and the chaotic cipher.

In these results, our proposed system gets high chaotic property and more randomness than the conventional ciphers.

***Keywords*—**Chaos, chaotic property, cipher, Mersenne Twister, Randomness.

I. Introduction

In recently year, informational communication technology has evolved. At the same time, the demand of the information security has also risen. The stream cipher with chaos is the effective method that has low computational cost. And the encryption method using the initial value sensitive dependence of chaos has been proposed [1,2]. These chaotic properties are the Sensitive Orbital Instability and Long-term Unpredictability and so on. By these properties, the transfer of correct information becomes possible only when the parameters and the initial values are perfectly corresponding between the modulator and the demodulator. In conventional system, the chaotic cipher has been comprised of the nonlinear map and another nonlinear filter for synchronization between the modulator and the demodulator [3]. The conventional chaotic cipher has been added to Volterra filter [8] that is a kind of nonlinear digital filter. This filter increases the number of parameters for the encryption key, and the chaotic characteristics. However the conventional system has the problem to improve randomness.

In this study, we propose the chaotic cipher combined with Mersenne Twister [5] that is an extremely good pseudo-random number generator to improve randomness. In our proposed system, we change the nonlinear map to Mersenne Twiseter.

In this study, we reassemble a cipher system at first, and evaluate the performance as secret code of that system randomness, based on Lyapunov experiments, and the coefficient sensitivity against the parameter mismatching.

D. Yoshida is with Graduate School of Science and Technology, Meiji University 1-1-1 Higashi-mita, Tama-ku, Kawasaki, 214-8571 Japan (E-mail:ce11096 @meiji.ac.jp).

H. Kamata is with School of Science and Technology, Meiji University 1-1-1 Higashi-mita, Tama-ku, Kawasaki, 214-8571 Japan (E-mail: kamata@isc.meiji.ac.jp).

A. Nakayama, H. Watanabe, T. Sato and S. Kuriyama are with Graduate School of Science and Technology, Meiji University 1-1-1 Higashi-mita, Tama-ku, Kawasaki, 214-8571 Japan.

II. Calculation Method

This Chaotic modulator is assuming the use of 16bit fixed-point arithmetic [1]. Thereby necessary bounded ness for chaos can be generated. In 16bit fixed-point arithmetic, the addition, subtraction and multiplication can be executed with 32-bit accumulator. We move the decimal point 10 places to the left. We call it Q10 Format. Therefore, the white areas mean integer zones. The light grey areas mean decimal zones. And the dark grey area, the most significant bit is used for signed bit.

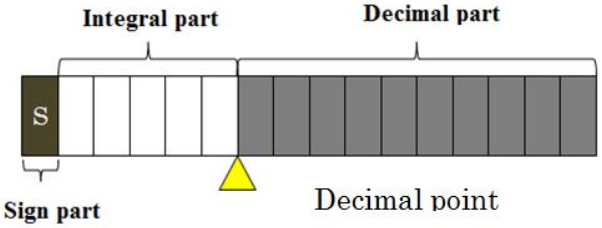

Fig. 1 Q10 Format

Q10unit represents the smallest unit, Q10min represents the minimum, Q10max represents the maximum.

Minimum unit of $Q10$ Format

$$Q10_{unit} = 2^{-10} \cong 0.000977 \quad (1)$$

Minimum value of $Q10$ Format

$$Q10_{\min} = -2^{16-10-1} = 32.0 \quad (2)$$

Maximum value of Q10 Format

$$Q10_{\max} = 2^{16-10-1} - Q10_{\min} \cong 31.999023 \quad (3)$$

III. Chaotic Modulator

In this section, we explain the conventional system and the proposed system.

A. Conventional System

The chaotic modulator is comprised of the nonlinear map and another nonlinear filter for synchronization. (4)〜(6) are encrypted part, (7) is Transfer part, (8)〜(10) are Decryption part.

Encrypted part

$$\begin{aligned} x_1(n) &= s(n) + g_1\{x_1(n-1)\} \\ &\quad + g_2\{x_1(n-1)\} \\ &\quad + g_3\{x_1(n-1)\} + \theta \end{aligned} \quad (4)$$

$$x_2(n) = h_0 + \sum_{i=1}^{3} h_i x_i(n-1) + \sum_{i=1}^{3}\sum_{j=1}^{3} h_{ij} x_i(n-1) x_j(n-1) + h_{123}\prod_{i=1}^{3} x_i(n-1) \quad (5)$$

$$x_3(n) = x_2(n-1) \quad (6)$$

Transfer part

$$x_4(n) = x_1(n) \quad (7)$$

Decryption part

$$r(n) = x_4(n-1) - g_1\{x_1(n-1)\} - g_2\{x_2(n-1)\} - g_3\{x_1(n-1)\} - \theta \quad (8)$$

$$x_5(n) = h_0 + \sum_{i=1}^{3} h_i x_{i+3}(n-1) + \sum_{i=1}^{3}\sum_{j=1}^{3} h_{ij} x_{i+3}(n-1) x_{j+3}(n-1) + h_{123}\prod_{i=1}^{3} x_{i+3}(n-1) \quad (9)$$

$$x_6(n) = x_5(n-1) \quad (10)$$

where, the $s(n)$ shows the information signal that should be encrypted, the $r(n)$ shows the signal that should be decrypted, $x_1(n)$, $x_2(n)$, $x_3(n)$, ・・・ are the internal state variables of the system, and parameter h_i, h_{ij}, ・・・ are coefficients that are the keys of the cipher. $g_n\{x\}$ is a nonlinear function.

Nonlinear function

We have been examining the chaotic modulator by using the next expression for the function.

$$g_n(x) = \begin{cases} \kappa_n x + \sigma_n : x \le -\epsilon_n \\ \dfrac{\kappa_n - \sigma_n}{\epsilon_n} x : -\epsilon_n < x < \epsilon_n \\ \kappa_n x - \sigma_n : x \ge \epsilon_n \end{cases} \quad (n = 1,2,3) \quad (11)$$

We have been using the next expression for the function.

The form of the (11) is shown in Fig. 2.

The form shows that the value varies sharply around 0.

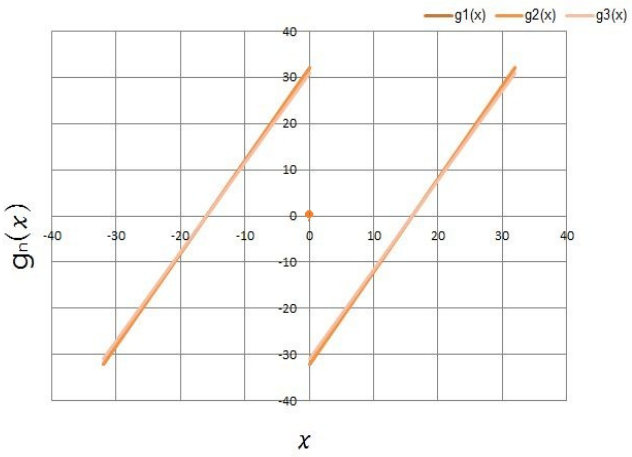

Fig. 2 Nonlinear map

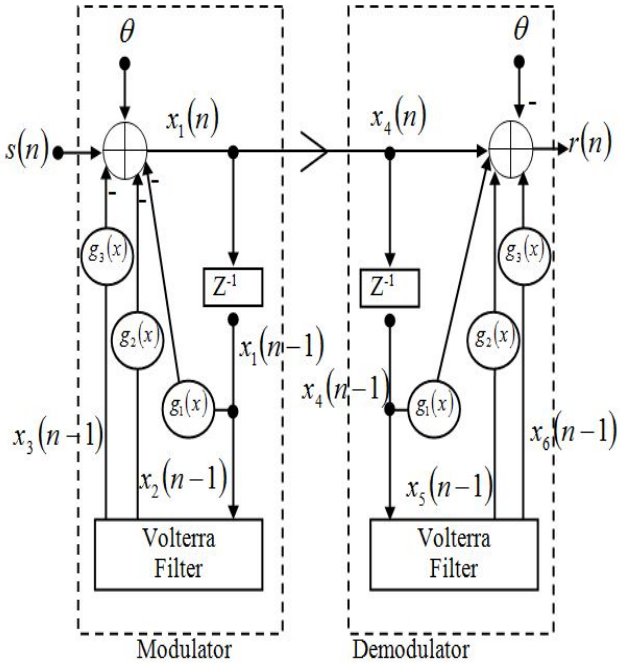

Fig. 3 The block diagram of the conventional chaotic cipher

The Fig. 3 shows the block diagram of the conventional chaotic cipher.

Jacobian

The Jacobian matrix J_{old} of the conventional system's dynamics is shown as:

$$J_{old}(n) = \begin{bmatrix} \dfrac{\partial}{\partial x_1} g_1(x_1(n)) & \dfrac{\partial}{\partial x_2} g_2(x_2(n)) & \dfrac{\partial}{\partial x_3} g_3(x_3(n)) \\ J_{10} & J_{11} & J_{12} \\ 0 & 1 & 0 \end{bmatrix} \quad (12)$$

$$J_{10} = h_1 + 2h_{11}x_1(n) + (h_{12} + h_{21})x_2(n) + (h_{13} + h_{31})x_3(n) + h_{123}x_2(n)x_3(n) \quad (13)$$

$$J_{11} = h_2 + 2h_{22}x_2(n) + (h_{12} + h_{21})x_1(n) + (h_{23} + h_{32})x_3(n) + h_{123}x_1(n)x_3(n) \quad (14)$$

$$J_{12} = h_3 + 2h_{33}x_3(n) + (h_{13} + h_{31})x_1(n) + (h_{23} + h_{32})x_2(n) + h_{123}x_1(n)x_2(n) \quad (15)$$

B. Proposed System

This is our proposed system.(17)～(19) are encrypted part, (20) is Transfer part, (21)～(23) are decryption part. The proposed system is adopted Mersenne Twister in (17) and (21).

The Mersenne Twister is a very fast random number generator of period 219937 −1 introduced by Makoto Matsumoto and Takuji Nishimura [5]. Despite the fact that the Mersenne Twister is an extremely good pseudo-random number generator, it is not cryptographically secure by itself for a very simple reason. Because, it is possible to determine all future states of the generator from the state the generator has at any given time. Therefore, we combine Random number generated by the Mersenne Twister and Random number generated by the Chaotic Neuron Type Nonlinearity.

In this system, MT represents the Mersenne Twister.

Encrypted part

$$x_1(n) = s(n) + MT_1(n)x_1(n-1) + MT_2(n)x_2(n-1) + MT_3(n)x_3(n-1) + \theta \quad (17)$$

$$x_2(n) = h_0 + \sum_{i=1}^{3} h_i x_i(n-1) + \sum_{i=1}^{3}\sum_{j=1}^{3} h_{ij}x_i(n-1)x_j(n-1) + h_{123}\prod_{i=1}^{3} x_i(n-1) \quad (18)$$

$$x_3(n) = x_2(n-1) \quad (19)$$

Transfer part

$$x_4(n) = x_1(n) \quad (20)$$

Decryption part

$$r(n) = x_4(n) - MT_1(n)x_4(n-1) - MT_2(n)x_5(n-1) - MT_3(n)x_6(n-1) + \theta \quad (21)$$

$$x_5(n) = h_0 + \sum_{i=1}^{3} h_i x_{i+3}(n-1) + \sum_{i=1}^{3}\sum_{j=1}^{3} h_{ij}x_{i+3}(n-1)x_{j+3}(n-1) + h_{123}\prod_{i=1}^{3} x_{i+3}(n-1) \quad (22)$$

$$x_6(n) = x_5(n-1) \quad (23)$$

The Fig. 4 shows the block diagram of the proposed chaotic cipher.

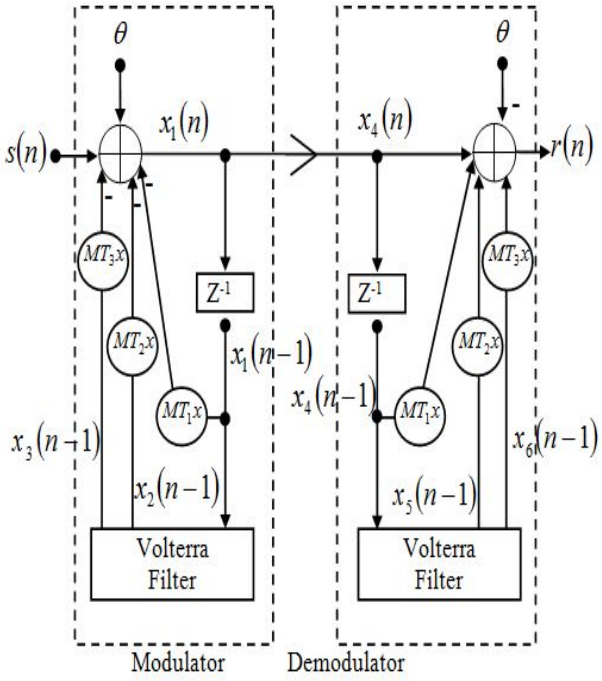

Fig. 4 The block diagram of the proposed chaotic cipher

The Jacobian matrix J_{new} of the proposed system's dynamics is shown as:

$$J_{new}(n) = \begin{bmatrix} MT_1(n) & MT_2(n) & MT_3(n) \\ J_{10} & J_{11} & J_{12} \\ 0 & 1 & 0 \end{bmatrix} \quad (24)$$

$$J_{10} = h_1 + 2h_{11}x_1(n) + (h_{12} + h_{21})x_2(n) + (h_{13} + h_{31})x_3(n) + h_{123}x_2(n)x_3(n) \quad (25)$$

$$J_{11} = h_2 + 2h_{22}x_2(n) + (h_{12} + h_{21})x_1(n) + (h_{23} + h_{32})x_3(n) + h_{123}x_1(n)x_3(n) \quad (26)$$

$$J_{12} = h_3 + 2h_{33}x_3(n) + (h_{13} + h_{31})x_1(n) + (h_{23} + h_{32})x_2(n) + h_{123}x_1(n)x_2(n) \quad (27)$$

IV. Lyapunov Exponent of the Chaotic Modulator

In this section, we investigate the Lyapunov exponent of the chaotic cipher. The Lyapunov exponent is the most basic indicator of deterministic chaos. When the maximum Lyapunov exponent is bigger than 0, it can be called chaos.

Each Lyapunov exponent is calculated by the Jacobian matrix in (16), (24).When the chaotic cipher takes Lyapunov experiment, each parameter h2, h3 of the chaotic cipher moves from -32.0 to 31.0 in units of 1.0. Normally, these systems should move all parameters. However, it is quite time consuming. So we test in this way.

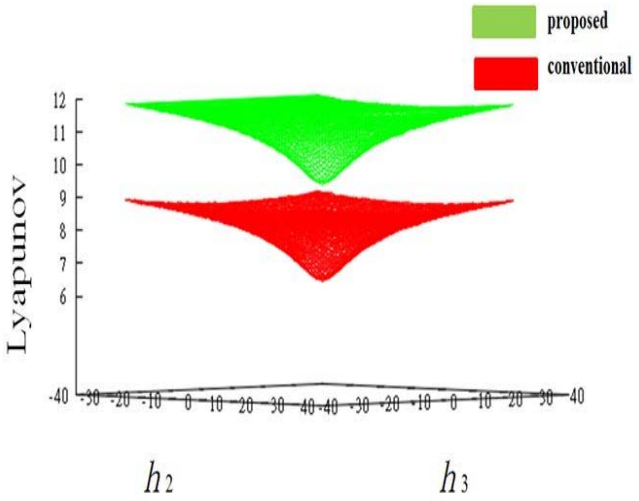

Fig. 5 Maximum Lyapunov Exponents

As the Fig. 5 shows, the conventional system is approximately from 6.0 point to 9.0 point; the proposed system is approximately from 9.5 point to 11.5 point. The proposed system is approximately 3.5 point higher than conventional system.

In this result, the presumption of the parameters based on the calculation result of the Lyapunov spectrum becomes more difficult.

V.RANDOMNESS TEST

We use Diehard Tests to randomness test. Diehard Tests are the tests which check the randomness of the sequence signal. Diehard Tests consist of 18 kinds of test. The signal which passed all tests has a high possibility which is a random signal.

In this validation, an initial value of parameters of the chaotic cipher that play a key part is 1.0. When the chaotic cipher takes randomness tests two parameters of the chaotic cipher moves from -32.0 to 31.99 in units of 1.0. Also, we compare chaotic cipher and RC4 cipher. RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography.

We verify the validity of chaotic cipher by compare existing cipher and chaotic cipher. When the RC4 cipher takes randomness tests, two parameters move to minimum size from maximum size in units of 1.0. Normally, these systems should move all parameters. However, it is quite time consuming. So we test in this way.

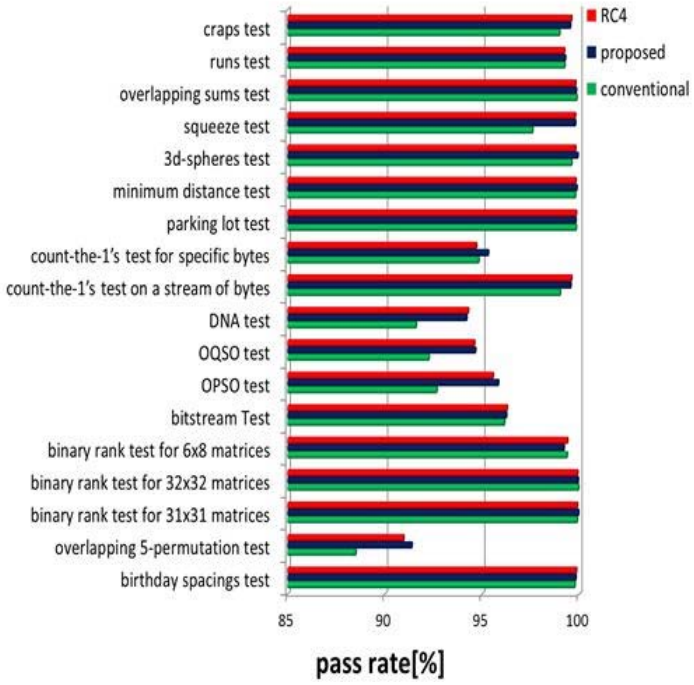

Fig. 6 Each test's result of Diehard Tests

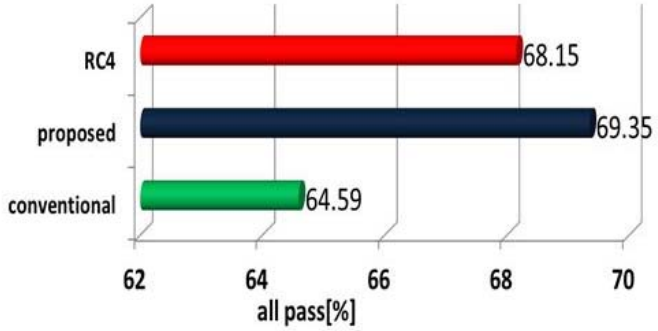

Fig. 7 All pass's result of Diehard Tests

As the Fig. 7 shows, the conventional system is 64.40[%], the proposed system is 69.35[%], the RC4 is 68.15[%]. The proposed system gets more randomness than conventional system. Furthermore, the proposed system is shown high value by RC4.

VI. Sensitivity Against the Parameter Mismatching

In this research, we evaluate the sensitivity against the parameter mismatching of these Modulation and demodulation.

If these parameters of the proposed system's modulation and demodulation are match, the given signal must be decoded. In reverse, if these parameters of the proposed system's modulation and demodulation are not match, the given signal must not be decoded.

This test investigates the effect of the decoded signal, when there is error in the parameter. On the demodulated given values of all possible parameters, we calculate the errors of the original signal and the demodulated signal.

$$D = -\frac{1}{L}\sum_{i=0}^{L-1}\left|u(t) - s(t)\right| \tag{28}$$

(28) is seek the error D. Where, the $s(t)$ shows signal that should be decrypted, the $u(t)$ shows the information signal that should be encrypted, L shows number of samples. When the D become 0, this point could be demodulated. We performed this validation as L = 1000. In this validation, an initial value of parameters of the chaotic cipher that play a key part is 1.0.

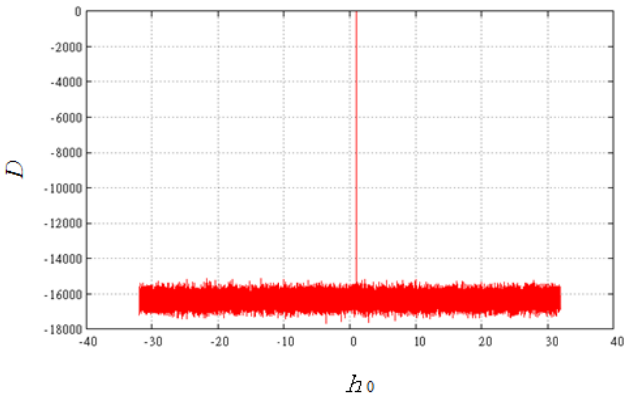

Fig. 8 Result of the parameter mismatching

This Fig. 8 shows result of the parameter mismatching, when parameter $h0$ moves. In this result, when the values do not match the parameter, the value is not decoded. And, the value is decoded when the values match the parameter.

Also, other parameters are as same as this result. The proposed system can be decrypted without error. Therefore, all parameters of the proposed system are these valid encryption keys.

VII. Conclusion

In this paper, we proposed the chaotic cipher combined with Mersenne Twister. In this attempt, our proposed system gets more randomness than conventional system. And the maximum Lyapunov exponent of the proposed system becomes bigger than the maximum Lyapunov exponent of the conventional system. And all parameters of the proposed system are these valid encryption keys.

In these result, the proposed system gets better secure communications than the conventional system.

References

[1] H. Kamata, T. Endo and Y. Ishida, "Secure communication using chaos via DSP implementation" IEEE, Proc. ISCAS'96, Vol.3, pp.112-115, 1996.Authors, Title, Journal, Publisher, Location, pages, year.

[2] M.D.Restituto, R.L.Ahumada and A.R.Vasques, "Secure communication using CMOS current-mode sampled-data circuits" Proc. Nonlinear Dynamics of Electronic.

[3] K.Iwata,T.Nakamura and H.kamata,"chaotic Modulator with Volterra Filter for Cipher" IEICE, Proceedings of NOLTA ,pp.216-219, 2007.

[4] K. Aihara, "Chaotic neural Netowork" Bifurcation Phenomena in Nonlinear Systems and Theory of Dynamical System, pp. 143-161, 1990.

[5] M.Matumoto and T. Nishimura, "MersenneTwister:a 623-dimensionally equidistributed uniform pseudo-random number generator" ACM Transactions on Modeling and Computer Simulation , Volume 8 Issue 1, Jan. 1998 .

[6] M. Sano and Y. Sawada, "Measurement of the Lyapunov Spectrum from a Chaotic Time Series" Phys. Rev. Lett , No.55, 1082-1085 1985.

[7] S.Watanabe, K.ABE,"A VLSI Design of Mersenne Twister" 2005-CSEC-9, IPSJ SIG Technical Report, pp.1-6,May,2005(in Jpanese)

[8] M. Schetzen,"The Volterra and Wiener Theories of Nonlinear System" Wiley, 1980.