Study on Chaotic Cipher with Robustness and Its Characteristics

Takashi Arai[1(✉)], Yuta Kase[1], and Hiroyuki Kamata[2]

[1] Graduate School of Science and Technology, Meiji University,
1-1-1 Higashi-mita, Tama-ku, Kawasaki, Kanagawa, Japan
cel81004@meiji.ac.jp
[2] School of Science and Technology, Meiji University,
1-1-1 Higashi-mita, Tama-ku, Kawasaki, Kanagawa, Japan

Abstract. In this paper, we propose a robustness cryptosystem with a small amount of computation. By adopting a stream cipher not but block cipher like AES, the processing speed is improved. Furthermore, it has chaotic properties and improved randomness. Moreover, since an expression for synchronizing the encryption system and the decryption system is not used in the proposed method, even when a bit error occurs, it is correctly decrypted. In general, nonlinear signals such as chaotic map, Jacobian can be estimated from time series signals by Sano-Sawada method. In the chaotic cipher, the parameters in the expression are used as cryptography keys. Therefore, if Jacobian is a constant, the cryptographic key will be estimated. In the proposed system, we formulate the expression so that each element of Jacobian becomes time-variant as much as possible. Thereby the safety of the system is secured.

Keywords: Cryptosystem · Chaotic map · Stream cipher

1 Introduction

In recent years, with the spread of personal computers and smartphones, IT has advanced and movements toward IoT are progressing. Therefore, a lightweight and robust cryptosystem that can be installed in electric appliances, such as microwave ovens and air conditioners, that are not always good at computational performance. In this research, we propose a chaotic stream cipher using fixed-point arithmetic and evaluate its characteristics in order to realize cryptosystem with a small amount of computation which can handle high speed processing.

2 Methods

2.1 Cipher

Ciphers are roughly divided into block ciphers and stream ciphers. The block cipher has a high cryptographic strength, and the stream cipher has a feature that the processing speed is high. As an example of the block cipher, RSA cryptography is cited.

L. Li et al. (Eds.): AsiaSim 2018, CCIS 946, pp. 414–424, 2018.
https://doi.org/10.1007/978-981-13-2853-4_32

The stream cipher has RC4. This time, we adopt stream encryption method and are striving to improve processing speed.

2.2 Fixed-Point Arithmetic

Fixed-point arithmetic is a computational method that fixes the number of bits of the decimal part and the integer part in advance. It is an arithmetic method suitable for a low computational resource environment compared with floating-point arithmetic. Generally, in fixed-point arithmetic, the overflow occurs in some cases and the width of expressible values is limited. However, in this research, we are actively use to represent the boundedness of chaos. Figures 1 and 2 show the calculation methods of addition/subtraction and multiplication in fixed-point arithmetic, respectively. Addition and subtraction can be performed in the same way as ordinary arithmetic, however, multiplication involve a process of doubling the bit-length of data. In this research, division is not used, it is omitted here. In this research, we adopt 16 bit format with decimal part as 10 bits, integer part as 5 bits and most significant bit as sign bit [1].

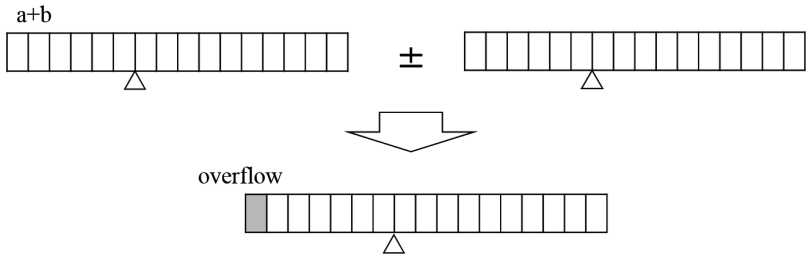

Fig. 1. Addition and subtraction in the fixed-point arithmetic.

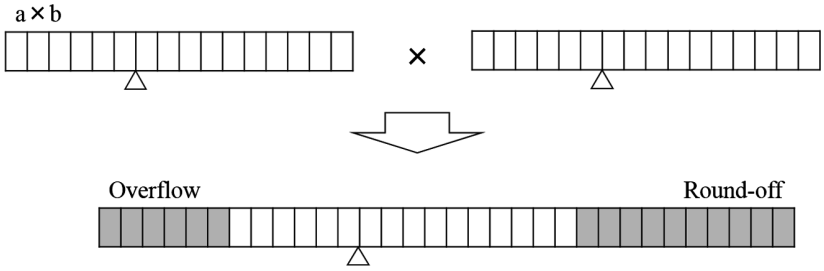

Fig. 2. Multiplication in the fixed-point arithmetic.

2.3 Chaotic Property

Chaos is a deterministic phenomenon due to nonlinearity that exhibits a complex behavior equivalent to a stochastic system [2]. Chaotic property are mainly the following items. These properties are suitable for encryption. In the system, randomness is

improved by incorporating the chaotic phenomenon into the stream cipher. However, these characteristics are obtained when chaos is generated in an environment of infinite digit operation. Therefore, in a finite digit operation like a general-purpose computer, characteristics degrade a little. Hence, it is important to evaluate the robustness of signal generated through the system.

- orbital instability
  The error of a small initial value is exponentially elongated and finally expanded to the maximum distance of the attractor. The elongation percentage of the initial displacement is quantified by Lyapunov exponent.
- long-term unpredictability
  Due to orbital instability, the error increases unless the initial state is observed with infinite precision. Therefore, long-term prediction is realistically impossible although it can make short-term predictions.
- nonperiodicity
  When observed as a time series signal, it shows aperiodic behavior.
- boundedness
  With the orbital instability alone, the error of the initial value variation continues to increase exponentially and eventually diverges. In order to maintain the asymptotic stability as an attractor, it is necessary to exist in the bounded region by recursive motion by nonlinear folding.

3 Chaotic Cipher

The flow of transmission and reception of the chaotic encryption system will be described. The sender encrypts the plain text $\boldsymbol{s}(\boldsymbol{n})$ with the modulation system and sends the cipher $\boldsymbol{r}(\boldsymbol{n})$ to the recipient via the network. The receiver demodulates the received cipher $\boldsymbol{r}(\boldsymbol{n})$ with the demodulation system and obtains the original information. Since the cryptosystem in this study employs common key cryptosystem, it is necessary to deliver the key to the receiver in advance.

3.1 Conventional Method

The modulation and demodulation systems are represented by three expressions. $s(n)$ is plaintext and $x_1(n)$ is encrypted signal. The first expression contains a nonlinear function $f(x)$, which creates system nonlinearity. This first expression is called "chaotic neuron" [1]. The second expression uses a second-order Volterra filter. This filter contains many parameters. These parameters are cryptography keys. In addition, the elements of Jacobian are time-variant not but constant because this expression contains the second power term. Therefore, it is difficult to estimate the parameter value from the time series signal. The output of this second expression becomes the input of the third expression, and the output of the third expression becomes the input of the first expression. In the demodulation system, the first expression is the inverse function of the modulation system. The second and third expressions are same as that of modulation system. Thereby taking the synchronization of the system [3].

- Encryption part

$$\begin{aligned} x_1(n) &= \mathrm{s}(n) - f(x_1(n-1)) + \alpha x_3(n-1) + \theta_1 \\ x_2(n) &= \sum_{i=1}^{3} h_i x_i + \sum_{i=1}^{3} \sum_{j=1}^{3} h_i h_j x_{ij} + \mathrm{h}_{123} \prod_{i=1}^{3} x_i(n-1) + \theta_2 \\ x_3(n) &= x_2(n-1) \end{aligned} \tag{1}$$

- Transfer part

$$\boldsymbol{r}(\boldsymbol{n}) = \boldsymbol{x}_1(\boldsymbol{n}) \tag{2}$$

- Decryption part

$$\begin{aligned} s(n) &= r(n) + f(r(n-1)) - \alpha x_3(n-1) - \theta_1 \\ x_2(n) &= \sum_{i=1}^{3} h_i x_i + \sum_{i=1}^{3} \sum_{j=1}^{3} h_i h_j x_{ij} + \mathrm{h}_{123} \prod_{i=1}^{3} x_i(n-1) + \theta_2 \\ x_3(n) &= x_2(n-1) \end{aligned} \tag{3}$$

- Nonlinear Function

$$\boldsymbol{f}(\boldsymbol{x}) = \begin{cases} \boldsymbol{x} - \mathbf{16}(\boldsymbol{x} < 0) \\ -\boldsymbol{x} + \mathbf{16}(\boldsymbol{x} \geq \mathbf{0}) \end{cases} \tag{4}$$

3.2 Proposed Method

The proposed method consists of three expressions as well. In the conventional method, the value of the first equation was transmitted as an encrypted signal, however in the proposed method, the value of the third equation is transmitted. In this research, the value of the previous time is used for calculation of encryption and decryption. Therefore, if one value is rewritten, subsequent decryption may be affected Therefore, in the proposed method, the synchronous formula is eliminated so that even if the transmission signal is rewritten in the middle, it will not affect subsequent decryption [4].

- Encryption part

$$\begin{aligned} x_1(n) &= s(n) - f_1(x_1(n-1), x_2(n-1), x_3(n-1)) + \theta_1 \\ x_2(n) &= x_1(n-1) - f_2(x_2(n-1), x_3(n-1)) + \theta_2 \\ x_3(n) &= x_2(n-1) - f_3(x_3(n-1)) + \theta_3 \end{aligned} \tag{5}$$

- Transfer part

$$\boldsymbol{r}(\boldsymbol{n}) = \boldsymbol{x}_3(\boldsymbol{n}) \tag{6}$$

- Decryption part

$$\begin{aligned} x_2(n-1) &= r(n) + f_3(r(n-1)) - \theta_3 \\ x_1(n-1) &= x_2(n) + f_2(x_2(n-1), r(n-1)) - \theta_2 \\ s(n) &= x_1(n) + f_1(x_1(n-1), x_2(n-1), r(n-1)) - \theta_1 \end{aligned} \tag{7}$$

- Nonlinear function

$$\begin{aligned} f_1(x_1, x_2, x_3) &= \textstyle\sum_{i=1}^{3} h_i x_i^3 + h \prod_{i=1}^{3} x_i \\ f_2(x_1, x_2) &= \textstyle\sum_{i=1}^{2} h_i x_i + \sum_{i=1}^{2} \sum_{j=1}^{2} h_{ij} x_i x_j + h_{31} x_1^3 + h_{32} x_2^3 \\ f_3(x_1) &= h + \textstyle\sum_{i=1}^{3} \left(h_i x_1^i + (h_i \oplus x_1^i) \right) \end{aligned} \tag{8}$$

4 Evaluation of the Characteristic

4.1 Key Length

The effective number of encryption keys is judged from the coefficient sensitivity by parameter mismatching as to whether or not it will be correctly decoded when trying to decrypt with the wrong key. The value of D in Eq. 9 is the average of the error between the plaintext and the demodulated signal. The number of samples L is calculated at

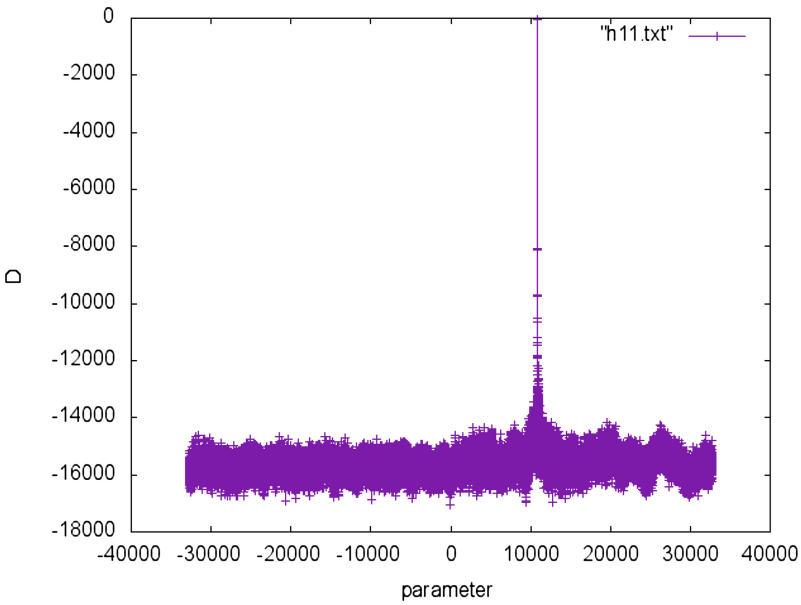

Fig. 3. h_{11} coefficient sensitivity.

1000. If the point at which D shows 0 is one parameter value used for encryption, and if the value of D is evenly distributed around the point, the target parameter is judged to be a valid key. This evaluation is calculated for each parameter.

$$\mathrm{D} = -\frac{1}{L}\sum_{t=0}^{L-1} |u(t) - s(t)| \tag{9}$$

The results of $h_{11}, h_{12}, h_{13}, h_{14}, c_1$ and c_2 indicate the waveform shown in Fig. 3. This figure shows that it can be demodulated to some extend with a parameter of near value, therefore, these are not valid keys. For other parameters, the error is evenly distributed even in the vicinity of the correct value as Fig. 4, hence these are effective keys. Thus valid key size is $16\,\mathrm{bit} \times 16 = 256\,\mathrm{bit}$. This value is equivalent to the maximum key length of AES.

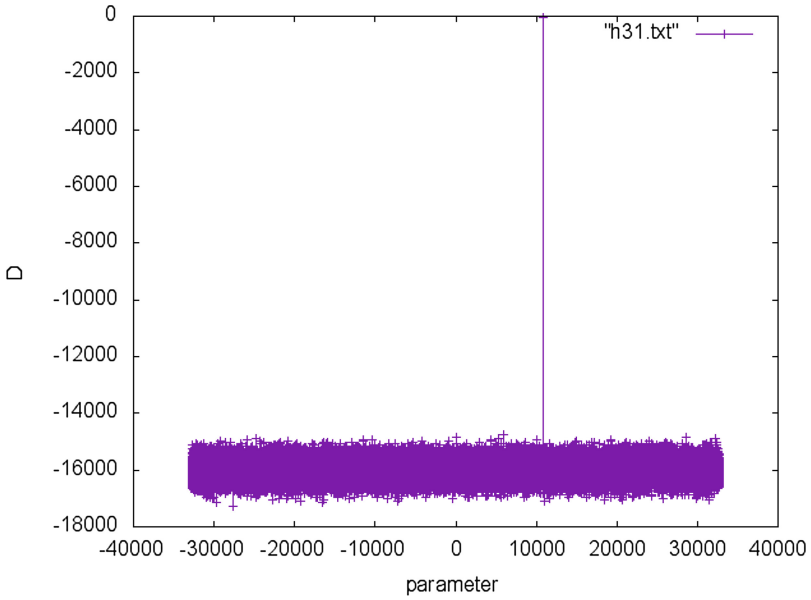

Fig. 4. h_{13} coefficient sensitivity

4.2 Processing Speed

We measure the processing time for encrypting 100 Mbytes of data. The processing speed is calculated by Eq. 10. Bps [bit per second] is used as the processing speed unit. Show operating environment in Table 1.

$$\begin{aligned}&\text{Encryption processing speed[Mbps]}\\ &\quad = 100[\text{Mbyte}] \times 8 \div \text{Encryption processing time[second]}\end{aligned} \tag{10}$$

Table 1. Operating environment.

OS, IDE	Microsoft, Windows 10 Education, Visual Studio 2015 Community
CPU	Intel, Core(TM)i7-7700 CPU @ 4.20 GHz
Memory	16.0 GB

Table 2 shows the result of processing speed. According to the table, the proposed method has slightly faster processing speed than the conventional method. It was possible to increase the number of effective encryption keys without impairing the processing speed. It is thought that it is caused by not using conventional nonlinear function.

Table 2. Processing rate.

	Conventional method	Proposed method
Processing speed [Gbps]	6.154	7.272

4.3 Randomness

To verify the randomness of the encrypted time series signal, we adopt the tool called NIST SP 800-22b tests [5]. It is a pseudo random number evaluation method published by National Committee of the US Department of Commerce (NIST). It consists of 16 tests. The evaluation value p-value is calculated in each test. If the value exceeds

Table 3. Results by NIST800-22b tests

	p-value results
Frequency	0.86343753
Block Frequency	0.61174483
Cumulative Sums forward	0.45199095
Cumulative Sums reverse	0.59484914
Runs	0.24360247
Longest Run	0.90019117
Rank	0.68858998
FFT	0.12093755
NonOverlappingTemplate	0.86055195
Overlapping Template	0.2613284
Universal	0.91720385
Approximate Entropy	0.2977884
Random Excursions	0.53397883
RandomExcursionsVariant	0.24597552
Serial	0.67040924
Linear Complexity	0.26375071

0.0001, it is stipulated that the test is acceptable. We test using the parameter values selected by the random number generation function of C language.

Table 3 shows the measurement results of NIST SP800-22b. P-value exceeds 0.0001 in all items. Therefore, it can be said that randomness is satisfactory.

4.4 Lyapunov Exponents

We try to confirm whether or not it has orbital instability by calculating Lyapunov exponent. The Lyapunov exponents are the values obtained by quantifying the elongation rate of the space. Since the system is three dimensional in this time, three Lyapunov exponents are calculated, and judging that it shows chaotic property because it spreads to that dimension if at least one of the three becomes positive value. The Lyapunov exponent is calculated by estimating Jacobian from the encrypted time series signal by Sano-Sawada method [6]. The change of the Lyapunov exponent when changing one parameter was evaluated for each parameter.

Figure 5 shows the result of parameter h_1. The first (maximum) Lyapunov exponent is positive in all areas. Therefore, in the parameters used this time, the system has orbital instability. There was no significant difference in comparison with the results of the conventional method. All three Lyapunov exponents are positive. It means that it spreads to all dimensions. If we do not calculate with a finite digit, the value diverges. Since this study uses fixed-point arithmetic, a system with such characteristics can also be realized.

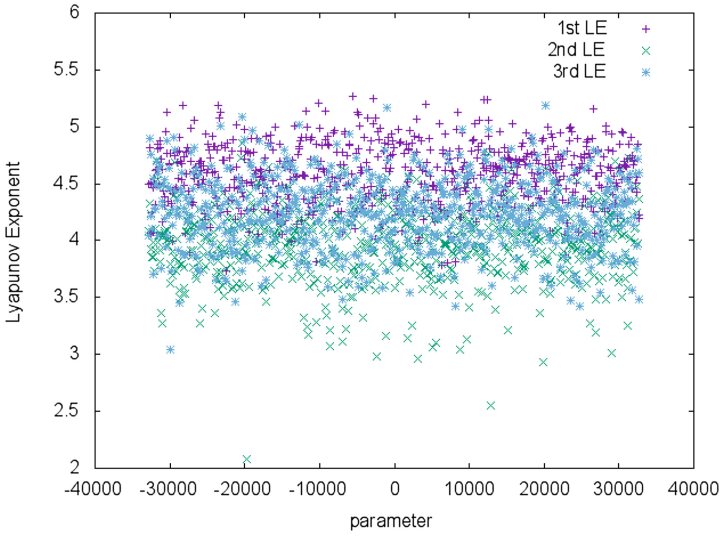

Fig. 5. h_{31} Lyapunov exponents

4.5 Characteristics of Jacobian

The matrix obtained by differentiating the dynamics with the parameters of each dimension is called Jacobian. It is possible to estimate Jacobian from the time series signal by the Sano-Sawada method. Hence, if Jacobian is a constant, the parameter value may be estimated. Therefore, it is desirable that each element of Jacobian is time-variant.

Equations 11 and 12 show the Jacobian of the system of the conventional method and the proposed method, respectively. In the conventional method, four out of nine elements were time-variant. In the proposed method six elements are time-variant. Thus it became harder to guess the parameter value by the Sano-Sawada method.

$$\begin{pmatrix} \frac{\partial f(x_1)}{\partial x_1} & 0 & \alpha \\ \frac{\partial f_{volterra}(x_1,x_2,x_3)}{\partial x_1} & \frac{\partial f_{volterra}(x_1,x_2,x_3)}{\partial x_2} & \frac{\partial f_{volterra}(x_1,x_2,x_3)}{\partial x_3} \\ 0 & 1 & 0 \end{pmatrix} \tag{11}$$

$$\begin{pmatrix} \frac{\partial f_1(x_1,x_2,x_3)}{\partial x_1} & \frac{\partial f_1(x_1,x_2,x_3)}{\partial x_2} & \frac{\partial f_1(x_1,x_2,x_3)}{\partial x_3} \\ 1 & \frac{\partial f_2(x_2,x_3)}{\partial x_2} & \frac{\partial f_2(x_2,x_3)}{\partial x_3} \\ 0 & 1 & \frac{\partial f_3(x_3)}{\partial x_3} \end{pmatrix} \tag{12}$$

4.6 Bit Error

We have found a new property in the proposed method. The finding is that even though one sample erroneous data is transmitted, if the data thereafter is correct, it can be correctly decoded. As described above, conventionally, the second and third expression is used as a synchronous expression. Hence when these expressions calculate different values at the time of encryption and decryption, correct decoding is not able to be

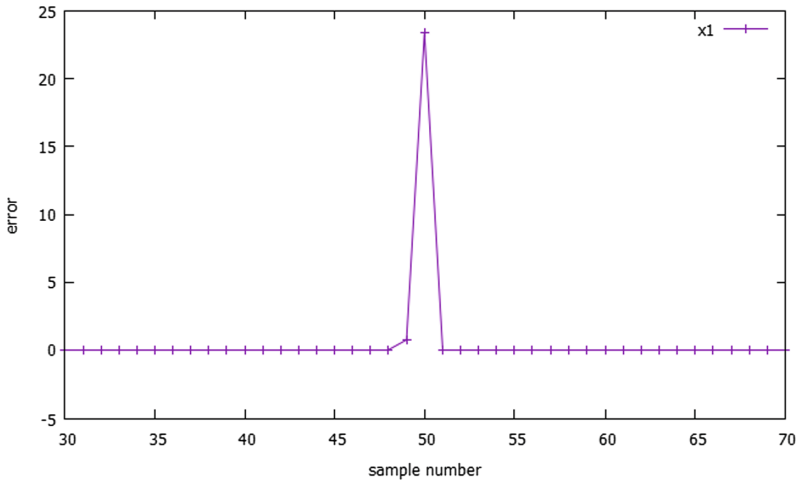

Fig. 6. Error in decoding of x_2

performed. Therefore, in the proposed method, the expression for synchronizing is not used. The first, second, and third expressions decode with the inverse function of the encryption expression. This property has been confirmed by the following method. First, 100 sample was encrypted and transmitted. At the time of transmission, the 50th sample is shifted by 1 bit. Decryption is performed using the data.

Figures 6, 7 and 8 show the error circumstances between the encrypted signal and the demodulated signal of each expression. The signals $x_2[49], [50]$ are not able to

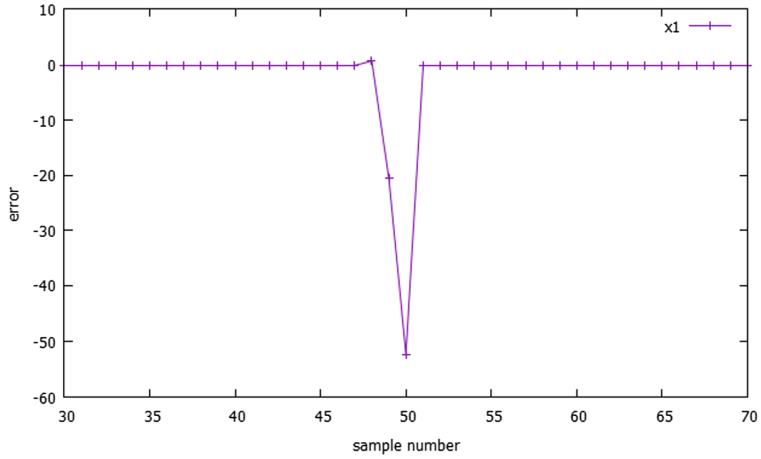

Fig. 7. Error in decoding of x_1

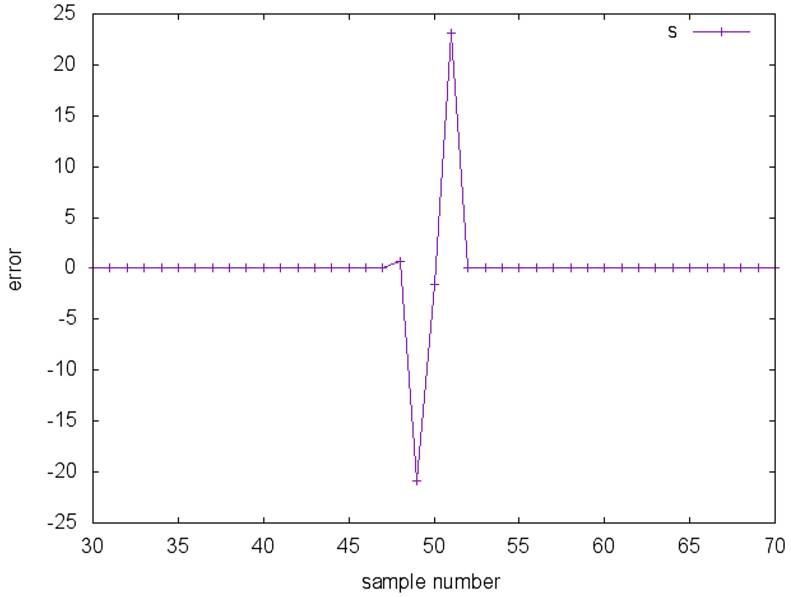

Fig. 8. Error in decoding of s

decode correctly because the demodulation is performed using the transmission signal ($r[50]$) that give the bit error. Similarly, The signals $x_1[48], [49], [50]$ which are performing demodulation using samples containing error ($x_2[49], [50], r[50]$) are not able to decode correctly. The same is true for the final demodulated signals. For this reason, an erroneous signal is decoded from the 48th to the 51st sample, however the correct value is decoded from the 52th sample onward. Though we change the number of samples and how bit errors occur we could decode correct value. Due to this nature, it can be considered that redundant bits during transmission such as error correction can be reduced.

5 Conclusions

In the system proposed this time, it was possible to improve the number of effective encryption keys and robustness without losing randomness, processing speed. Although the expression was constructed in three stages this time, it is possible to increase the number of stages according to the calculation resource. The processing speed was measured by software, however comparison with hardware (number of gates) will also be conducted in the future. Also, Jacobian's future objective is to make all elements time-variant.

References

1. Tsuruoka, Y., Nakasone, T., Kamiyama, K., Kamata, H.: The development of the chaotic block cipher. In: Proceeding to JSST 2015, pp. 125–128 (2015)
2. Abarbanel, H.D.I.: Analysis of Observed Chaotic Data. Springer, New York (1996). https://doi.org/10.1007/978-1-4612-0763-4
3. Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Phys. Rev. Lett. **64**(8), 821–824 (1990)
4. Restituto, M.D., Ahumada, R.L., Vazquez, A.R.: Secure communication using CMOS current-mode sampled-data circuits. In: Proceedings of Nonlinear Dynamics of Electronics System, pp. 237–240 (1995)
5. Koh, T., Powers, E.J.: Second-order Volterra filtering and its application to nonlinear system identification. IEEE Trans. Acoust. Speech Sig. Process. **33**(6), 1445–1455 (1985)
6. Kawanishi, Y., Yoshida, D., Watanabe, H., Nakayama, A., Sato, T., Kamata, H.: Chaotic modem system using nonlinear map with simultaneous Volterra filter. In: Proceedings of JSST 2011, pp. 456–459 (2011)
7. Murphy, S.: The power of NIST's statistical testing of AES candidates. In: The Third AES Candidate Conference (2000)
8. Sano, M., Sawada, Y.: Measurement of Lyapunov spectrum from a chaotic time series. Phys. Rev. Lett. **55**(10), 1082–1085 (1985)