2023 International Symposium on Nonlinear Theory and Its Applications
NOLTA2023, September 26-29, 2023, Catania and Online

Study on Advancement of Chaotic Stream Cipher including Rabin Cipher.

Masaki Onoue† and Hiroyuki Kamata‡

†Graduate School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki, Kanagawa, 214-8571, Japan
‡School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki, Kanagawa, 214-8571, Japan
Email: ce231018@meiji.ac.jp, kamata@meiji.ac.jp

Abstract– We have investigated robust cryptosystems that can be implemented in electronic devices with low computational power, such as IoT devices. The conventional chaos stream cipher with the built-in Rabin cipher in this research has the problem that the randomness of the ciphertext was low and the ciphertext information is larger than the plaintext information. Then, we propose a novel method to improve the randomness by incorporating polynomials, and to improve the increase in encrypted information by Jacobi symbols. This paper describes the two proposed systems and their verification results.

1. Introduction

With the spread of IoT devices, it has become common to use home appliances connected to networks. However, the CPUs installed in IoT devices have limitations in processing speed and usable memory, which poses a problem in terms of security maintenance. In such a low-computing resource environment, various methods are being investigated to maintain high security and reduce resource consumption [1].

The chaotic stream cipher proposed in this research [2] consists of three formulas, the first of which transmits the internal state variable. The second and third equations are used for synchronization on both sides of the transmitter and receiver, using a 2nd order Volterra filter. In this research, these operations are realized using fixed-point arithmetic to achieve the boundedness required for chaos and to improve suitability for environments with low-computing resources.

To increase the randomness of the generated cipher and to improve its robustness as a cipher, transmitting the internal state variable in the Volterra Filter has been investigated. However, there are problems that the Volterra Filter is a quadratic equation and the overflow in fixed-point arithmetic makes it difficult to identify unique solutions, and thus true-value decryption cannot be obtained [3].

In this study, we are comparing the processing structure of the Rabin cipher with the problem of multiple solutions due to overflow. The Rabin cipher has a characteristic that four solutions can be obtained by solving. Focusing on this point, a method has been proposed in which $x_1(n)$ is processed by the Rabin cipher before transmission [3].

In addition, while the conventional chaotic stream cipher is a common key cryptography, the Rabin cipher is a public key cryptography. Therefore, by applying the Rabin cipher, it is expected that the chaotic stream cipher will be developed into a public key cryptography.

While chaotic stream cipher incorporating the Rabin cipher is effective in realizing public-key cryptography, they have several drawbacks compared to conventional methods. One of them is that the randomness of the generated ciphertext is often inferior to that of the conventional method. Also, the ciphertext information may increase nearly four times more than the plaintext information [3]. A method [4] has also been proposed to suppress the increase by a factor of 2, however this method may not decrypt correctly.

In this study, we propose a novel method of incorporating polynomials into cryptographic schemes that incorporate the Rabin cipher, and show that the randomness of the cipher can be improved. Furthermore, we propose a method to suppress the increase of cryptographic information compared to plaintext information by using Jacobi symbols and conditional branches.

2. Principle

2.1. Computational Format

An unsigned fixed-point format with a total of x bits and a decimal part of y bits is called the UxQy format in this paper. The structure of U16Q10 is shown in Fig. 1.

In this study, we used three multiple precision arithmetic formats:

- U256Q160
- U512Q320
- U1024Q640

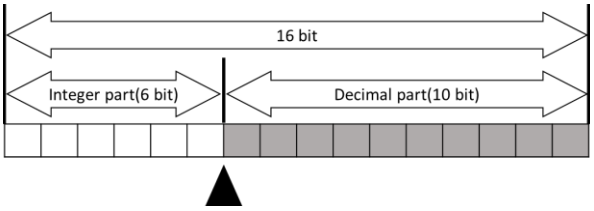


Fig1: U16Q10 format

ORCID iDs First Author: 0009-0005-4917-0486,
Second Author: 0009-0004-0598-4210.

2.2. Rabin cipher

The cipher is a type of public-key cryptography, in which prime numbers $p\,and\,q$ that satisfy $p \equiv q \equiv 3\,mod\,4$ are used as private keys, and $u = p, q$ as public keys [5].

Modulation system

$$y = x(x + B)\ mod\ u\ (B \text{ is even}) \quad (1)$$

Demodulation system

$$x_p = \left\{\left(y - \frac{B^2}{4}\right)^{\frac{p+1}{4}} - \frac{B}{2}\right\} mod\ p \quad (2)$$

$$x_q = \left\{\left(y - \frac{B^2}{4}\right)^{\frac{q+1}{4}} - \frac{B}{2}\right\} mod\ q \quad (3)$$

$$\begin{cases} z = a\,mod\,p \\ z = b\,mod\,q \end{cases}$$

$$(a,\ b) = \begin{cases} (x_p,\ x_q) \\ (p - x_p,\ x_q) \\ (x_p, q - x_q) \\ (p - x_p,\ q - x_q) \end{cases} \quad (4)$$

Although there exist four z that satisfy Eq. (4), only one solution that satisfies $z = x$. There are various ways to identify the solution. For example, if $B = 0$, it can be uniquely obtained as shown in Table 1.

Table 1: Unique identification of solutions ($B = 0$)

	$0 \leq x < \frac{u}{2}$	$\frac{u}{2} \leq x$
$\left(\frac{x}{u}\right) = 1$	x_1	x_2
$\left(\frac{x}{u}\right) = -1$	x_3	x_4

3. Proposed methods

3.1. Basic form of evaluation formula

The Volterra Filter function used in each method is shown in Eq. (5) and the nonlinear function $f(x)$ is shown in Eq. (6), where Y is half of the maximum value of the fixed-point arithmetic format U512Q320.

$$f_v(x_1, x_2, \cdots, x_n,\ \theta) = \sum_{i=1}^{n} h_i x_i + \sum_{i=1}^{n}\sum_{i=1}^{n} h_i x_i x_j$$
$$+ h_{123}\prod_{i=1}^{n} x_i + \theta \quad (5)$$

$$f(x) = \begin{cases} \kappa x + Y + \sigma\ (\varepsilon + Y \leq x) \\ \kappa x + Y - \sigma\ (x \leq Y - \varepsilon) \\ 0\ (otherwise) \end{cases} \quad (6)$$

In this study, $\kappa = 10, \sigma = \frac{Y}{5}, \varepsilon = \frac{Y}{25}$.

3.2. Proposed method1

We introduce a method that incorporates the Rabin cipher into the chaotic stream cipher proposed in this laboratory as a conventional method [3]. Four solutions are obtained by decryption in the Rabin cipher. The correct solution is obtained by preparing two sets of encryption keys and finding the common term for each. For a plaintext $s(n)$, the public key u_i must always satisfy $s(n) < u_i$, so that u_i is $2M$ bits when $s(n)$ is M bits.

The problem with the conventional method is that the randomness becomes low. Therefore, we prepared polynomials $C_1(n)$ and $C_2(n)$ and added them to the ciphertext $r_i(n)$ during modulation and subtracted them during demodulation to improve randomness. We refer to this method as proposed method 1. The polynomials are

$$C_1(n) = \alpha h_1 x_2(n-1)^2, \quad (7)$$
$$C_2(n) = \theta_1 h_{123} x_3(n-1)^2. \quad (8)$$

Since they must be random, it uses internal state variables $x_2(n-1)$ and $x_3(n-1)$. In order not to become a constant even when differentiated by internal state variables, their squares were incorporated. To validate α and θ_1, which are not traditionally valid keys, we also included them. In case of the conventional method, $C_1(n) = C_2(n) = 0$.

Modulation system

$$x_1(n) = s(n) - f(x_1(n-1))$$
$$+ \alpha x_3(n-1) + \theta_1 \quad (9)$$
$$x_2(n) = f_v(x_1(n-1), x_2(n-1), x_3(n-1), \theta_2) \quad (10)$$
$$x_3(n) = x_2(n-1) \quad (11)$$
$$y_i = \{C_i(n) + x_1(n)(x_1(n) + B(n))\}$$
$$mod\ u_i\ (i = 1,\ 2) \quad (12)$$
$$A(n) = h_1 + h_{12}x_2(n-1) + h_{13}x_3(n-1)$$
$$+ h_{21}x_2(n-1) + h_{31}x_3(n-1)$$
$$+ h_{123}x_2(n-1)x_3(n-1) \quad (13)$$
$$B(n) = \begin{cases} A(n)\ (A(n) \text{ is even}) \\ A(n) - 1\ (otherwise) \end{cases} \quad (14)$$

Transmission information (4 Mbit)

$$r_1(n) = y_1 \quad (15)$$
$$r_2(n) = y_2 \quad (16)$$

Demodulation system

$$x_{pi} = \left\{\left(r_i(n) - C_i(n) + \frac{B(n)^2}{4}\right)^{\frac{p_i+1}{4}} - \frac{B(n)}{2}\right\}$$
$$mod\ p_i \quad (17)$$

$$x_{qi} = \left\{\left(r_i(n) - C_i(n) + \frac{B(n)^2}{4}\right)^{\frac{q_i+1}{4}} - \frac{B(n)}{2}\right\}$$
$$mod\ q_i \quad (18)$$

$$\begin{cases} z_i = a \bmod p \\ z_i = b \bmod q \end{cases}$$

$$(a,\ b) = \begin{cases} (x_{pi},\ x_{qi}) \\ (p - B(n) - x_{pi},\ x_{qi}) \\ (x_{pi}, q - B(n) - x_{qi}) \\ (p - B(n) - x_{pi},\ q - B(n) - x_{qi}) \end{cases} \tag{19}$$

There exist four z_i each satisfying Eq. (19) for $i = 1, 2$, with $x_1(n)$ as their common term, and solve the following equation.

$$s(n) = r(n) + f\big(x_1(n-1)\big)$$
$$-\alpha x_3(n-1) - \theta_1 \tag{20}$$
$$x_2(n) = f_v(x_1(n-1), x_2(n-1), x_3(n-1), \theta_2) \tag{21}$$
$$x_3(n) = x_2(n-1) \tag{22}$$

3.3. Proposed method2

In the proposed method 1, the transmission information was four times larger than the plaintext. This is because that two sets of encryption keys are prepared to select the correct one from the four plaintext candidates m_i. If $B(n) = 0$, m_i is uniquely distinguished by the conditions shown in Table 1.

We refer to this method as proposed method 2. Furthermore, the following polynomial $C_3(n)$ is given and evaluated to ensure randomness as in the proposed method 1. $C_3(n)$ has more terms than $C_1(n)$ and $C_2(n)$ to ensure sufficient randomness.

$$C_3(n) = h_{13}h_{12}h_1 + \alpha x_1(n-1)x_2(n-1)$$
$$+\theta_1 x_2(n-1)x_3(n-1) \tag{23}$$

Modulation system

Eqs. (1) ~ (3) are the same with Eqs. (5) ~ (7) in the conventional method.

$$y = \{C_3(n) + x_1(n)^2\} \bmod u \tag{24}$$

Transmission information ($2M$ + 1bit)

$$r_1(n) = y \tag{25}$$
$$r_2(n) = \left(\frac{x_1(n)}{u}\right) \tag{26}$$

Demodulation system

$$x_p = (r_1(n) - C_3(n))^{\frac{p+1}{4}} \bmod p \tag{27}$$
$$x_q = (r_1(n) - C_3(n))^{\frac{q+1}{4}} \bmod q \tag{28}$$
$$\begin{cases} z = a \bmod p \\ z = b \bmod q \end{cases}$$
$$(a,\ b) = \begin{cases} (x_p,\ x_q) \\ (p - x_p,\ x_q) \\ (x_p, q - x_q) \\ (p - x_p,\ q - x_q) \end{cases} \tag{29}$$

Although there exist four z that satisfy Eq. (29), $z < u/2$ and $r_2(n) = (z/u)$ is the solution to be found and is $x_1(n)$. Using this, Eqs. (20) ~ (22) similar to the conventional method 1 are solved.

4. Verification

4.1. Randomness

The tool "NIST SP800-22" [6], a pseudorandom number evaluation method published by NIST, was used to verify randomness. It has 16 tests, and a parameter called $p - value$ is calculated for each test. If the significance level is α, the test is considered to have passed when $p - value \geq \alpha$ is satisfied. In this study, $\alpha = 0.01$, $N = 1000$ tests were conducted and the passing rate was calculated.

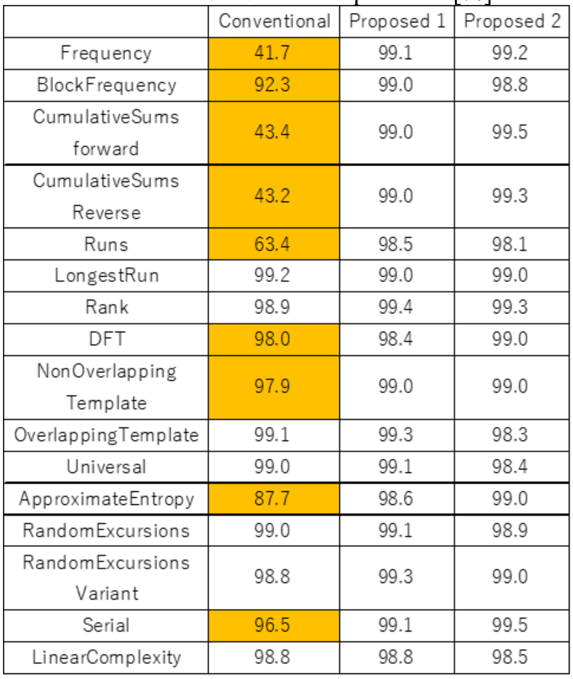
Since the passing rate m of the test should fall within the range shown by the following equation,

$$(1-\alpha) \pm 3\sqrt{\frac{(1-\alpha)\alpha}{N}} \approx 0.980561, 0.999439 \tag{30}$$

Randomness was considered sufficient if it fell within.

The results are shown in Table 2. From the same table, it can be seen that the conventional failed to pass some of the tests. On the other hand, the proposed method 1 and 2, which incorporate the polynomial, passed the all tests. Therefore, the polynomial improved the randomness as expected.

Table 2: NIST SP800-22 pass rate [%]



	Conventional	Proposed 1	Proposed 2
Frequency	41.7	99.1	99.2
BlockFrequency	92.3	99.0	98.8
CumulativeSums forward	43.4	99.0	99.5
CumulativeSums Reverse	43.2	99.0	99.3
Runs	63.4	98.5	98.1
LongestRun	99.2	99.0	99.0
Rank	98.9	99.4	99.3
DFT	98.0	98.4	99.0
NonOverlapping Template	97.9	99.0	99.0
OverlappingTemplate	99.1	99.3	98.3
Universal	99.0	99.1	98.4
ApproximateEntropy	87.7	98.6	99.0
RandomExcursions	99.0	99.1	98.9
RandomExcursions Variant	98.8	99.3	99.0
Serial	96.5	99.1	99.5
LinearComplexity	98.8	98.8	98.5

4.2. Valid encryption key

Evaluate whether the variables used in the cipher are suitable as cipher keys. Use Eq. (31) to find the coefficient sensitivity of all the cipher keys. where L is the number of samples, and $u(t)$ is the output of the demodulation system. In the case of correct decryption, $D = 0$.

$$D = -\frac{1}{L}\sum_{t=0}^{L-1}|u(t) - s(t)| \qquad (31)$$

We create the graph for the above equation with the key value x on the horizontal axis and D on the vertical axis. If the waveform of this graph is irregular, it can be considered to be a valid encryption key.

The variables α, θ_1, which were not effective in the conventional method, are effective for the proposed method 1 and 2. The reason is considered that the variables are incorporated into the polynomials $C_1(n) \sim C_3(n)$.

5. Conclusion

In this study, we improve a chaotic stream cipher incorporating the Rabin cipher, improving its randomness and reducing the redundancy of the ciphertext information content with respect to the plaintext.

On the other hand, since quantum computers, which have been developed in recent years [7], will be able to solve prime factorization at high speed, it is necessary to consider the Rabin cipher on the assumption that the secret key can be deduced from the public key. Since the method proposed in this study does not use Rabin cipher in all phases of encryption, but rather considers the chaotic stream cipher to be inherent, it is not necessarily possible to immediately apply a quantum computer without the cipher structure being deciphered.

In the future, it will be necessary to consider methods that increase the system complexity and robustness as a cipher even if the private key is guessed by a quantum computer compared to conventional methods.

References

[1] T. Arai, T. Sato, H. Kamata, “Study on Chaotic Cipher with robustness and its characteristics”, Proc. On AsiaSim 2018, pp.414-424, 2018.

[2] K. Iwata, T. Nakamura, T. Ikeue, H. Irikura and H. Kamata, Chaotic Modulator with Volterra Filter for Cipher, IEICE, Proceeding of NOLTA, 2007, pp.216-219.

[3] T. Sato, T. Arai, H. Kamata, “Study on the Chaotic Stream Cipher including Rabin Cipher.”, The Workshop on Circuits and Systems, pp.25-29, 2019. (In Japanese)

[4] T. Sato, T. Arai, and H. Kamata, “Study on a Chaotic stream cipher applying a Rabin cipher”, NCSP20, p.2, 2020.

[5] Michael O. Rabin, “Digitalized Signatures and Public Key Functions as Intractable as Factorization”, MIT/LCS/TR-212, Massachusetts Institute of Technology Cambridge, 1979.

[6] NIST, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, Special Publication 800-22, 2010.

[7] NIST, “NISTIR 8105: Report on Post-Quantum Cryptography”, p.6, 2016.