非予測性を重視した乱数生成器の提案*

森安 峰嗣**・森井 昌克***・笠原 正雄**

A New Type of Clock-Controlled Generator for Highly Unpredictable Pseudo-Random Sequence*

Takashi MORIYASU**, Masakatu MORII*** and Masao KASAHARA**

1. Introduction

One of the most important themes in a cryptosystem is the generating of a highly unpredictable pseudo-random sequences^{1,2)}. Recently various types of generating nonlinear pseudo-random sequence generators have been proposed. A clock-controlled generator (CCG) is one of the typical types where a linear feedback shift register (LFSR) controls the other LFSR's^{3,4)}.

In this short paper, we shall present a new type of CCG, and discuss on the linear complexity that is one of the important measures for the unpredictability of the nonlinear pseudo-random sequences.

2. A new generator

Various kinds of nonlinear pseudo-random sequence generators, which consist of some combined LFSRs only or LFSRs and logic elements, have been reported so far⁵⁾. The output function of those generators is generally nonlinear function in order not to be analyzed easily. CCG is also included in them where output of a LFSR is controlled by one of the other LFSR.

The configuration of our proposed CCG is presented in Fig. 1.

In Fig. 1, it is formed by one control LFSR (CL), some driving LFSRs (DL) and two nonlinear logic circuits, C_0 and C_1 . If a symbol from

Fig. 1 A new type of clock controlled pseudo-random generator

CL is " x ", circuit C_x is selected where x takes on 0 or 1. In other words, these two circuits making nonlinear sequences nonlinear ones are continuously varying. Furthermore the characteristic polynomial of LFSRs used in proposed CCG is primitive polynomial. It should be noted that in our proposed generator the logical circuits are controlled by LFSR, which in the conventional CCG, the constituent LFSR's are controlled by the LFSR itself.

3. Linear complexity

Let a_i be a sequence with period T . Then the sequence can be expressed by the formal power series (FPS) as follows ;

$$f(X) = \sum_{i=1}^{\infty} a_i X^{-i} = \sum_{j=0}^{\infty} \sum_{i=1}^T a_i X^{-(i+jT)} \\ = \frac{\sum_{i=1}^T a_i X^{T-i}}{X^T - 1} = \frac{n(X)}{d(X)} \quad (1)$$

where $\gcd(d(X), n(X)) = 1$. The numerator $n(X)$ is called an initial condition polynomial, and the denominator $d(X)$ is referred to as a characteristic polynomial. Furthermore the degree of a characteristic polynomial defined as

$$L = \deg[d(X)] \quad (2)$$

is called a linear complexity.

Several important measures for the unpredictability, or equivalently the randomness, of finite

* 原稿受付 1994年2月26日

** 京都工芸繊維大学 工学部 Department of Electrical and Information Science, Kyoto Institute of Technology; Matsugasaki, Sakyo ward, Kyoto city, Kyoto 606, JAPAN

*** 愛媛大学 工学部 Department of Computer Science, Ehime University; Bunkyocho 3, Matsuyama city, Ehime 790, JAPAN

Key Words : cryptography, stream cipher, pseudo-random sequence generator, linear complexity.

sequences have been proposed. The linear complexity of a sequence is one of such measures and is defined as the length of the shortest linear feedback shift register (LFSR) which can generate the sequence^{2),3)}.

We shall now analyze the linear complexity of our proposed CCG.

Let d_i be the degree of the characteristic polynomial of LFSR # i , and let d_i and d_j ($i \neq j$) be relatively prime. Moreover let $\mathcal{A}$ be a set of d_i and N be the order of it. Then all the possible product terms among arbitrary elements in $\mathcal{A}$ form a new set denoted by $\mathcal{A}$. Letting the order of $\mathcal{A}$ by Ψ , then from the definition, Ψ can be written as

$$\Psi \leq \sum_{i=1}^N \binom{N}{i} + 1 \quad (3)$$

It should be noted that Ψ depends on the circuits C_0 and C_1 in Fig. 1.

Let δ_j ($j=1, 2, \dots, \Psi$) be an element in $\mathcal{A}$. Then the characteristic polynomial $H(x)$ of the proposed CCG in Fig. 1 is given as follows :

[Theorem 1]

$$H(x) = \prod_{j=1}^{\Psi} \prod_{i=0}^{\delta_j-1} (x - \alpha_{\delta_j}^{2^i}) \quad (4)$$

where $\alpha_{\delta_j} \in \text{GF}(2^{\delta_j})$ and α_{δ_j} is a primitive root of unity (See **Appendix**).

Fig. 2 An example of proposed generator

In Fig. 2, we show an example of the proposed generator with 3 LFSRs. The linear complexity L_3 is given as follows :

$$L_3 = s + rs + st + tr + rst \quad (5)$$

where

$$\gcd(r, s, t) = 1. \quad (6)$$

Furthermore, we show another example of CCG with 3 LFSRs, so-called Geffe's generator, in Fig. 3. The linear complexity L_3^G is given as follows :

$$L_3^G = rs + st + t \quad (7)$$

Fig. 3 Geffe's generator

Fig. 4 A comparison on linear complexity

where r, s and t satisfy eq. (6)

In general the linear complexity of our proposed CCG is increasing exponentially as n grows, where n is the number of flip-flops to construct the generator. Here we compare the proposed CCG with Geffe's generator and Threshold generator¹⁾ regarding the maximum linear complexity in Fig. 4, when n flip-flops are used where n ranges from 6 to 100. The reason why these are selected is because the number of LFSRs can be set the same and the scale of generator's structures are almost similar.

References

- 1) G. T. Simmons (ed.) : Contemporary Cryptology, IEEE Press, pp. 65~134 (1992)
- 2) M. Kasahara and M. Morii : Modern Cryptography and Its Mathematical Foundations ; Technical Reports on the Second ASP Working Group in ISCIE, pp. 1~8 (1990)
- 3) M. Morii and M. Kasahara : Some Linear Complexity Profile of Finite Sequences ; Trans. of the ISCIE, Vol. 5, No. 8, pp. 325~330 (1992)
- 4) R. A. Rueppel : Analysis and Design of Stream Cipher, Springer-Verlag, pp. 5~16 (1986)
- 5) P. R. Geffe : How to Protect Data with Ciphers that are Really Hard to Break ; Electronics, pp. 99~101 (1973)
- 6) R. Lidl and H. Niederreiter : Finite Fields, Addison-Wesley, pp. 54~57 (1984)
- 7) M. K. Simons, J. K. Omura, R. A. Scholtz and B. K. Levitt : Spread Spectrum Communications, Computer Science Press, pp. 299~313 (1985)

APPENDIX

Proof of Theorem 1

First we shall give a definition of trace on finite fields⁶⁾.

【Definition 1】 Trace on finite fields is a linear mapping from an extension field to the corresponding ground field. So the following equation is called trace function :

$$\text{Tr}(a) = \sum_{i=0}^{m-1} a^{q^i}$$

where $a \in \text{GF}(q^m)$.

Moreover the following lemmas are needed to prove **Theorem 1**.

【Lemma 1】⁷⁾ Let $\{b_i\}$ be a sequence with characteristic polynomial over $\text{GF}(q)$ of degree m . Then the j -th symbol of $\{b_i\}$ is expressed by using trace function as follows :

$$b_j = \text{Tr}(Aa^j)$$

where A is an element in $\text{GF}(q^m)$.

【Lemma 2】⁷⁾ Let β and γ be elements in $\text{GF}(q^c)$ and $\text{GF}(q^d)$, respectively. Then

$$\text{Tr}(\beta) \cdot \text{Tr}(\gamma) = \text{Tr}(\beta\gamma)$$

is satisfied if $\text{gcd}(c, d) = 1$.

(Proof of Theorem 1) Supposing that $\theta_k \in \mathcal{A}$, so the j -th symbol of the proposed CCG in Fig. 1 is given by **Lemma 1** and **Lemma 2** as follows :

$$\begin{aligned} s_j &= (\text{Tr}(\alpha_{\theta_k}^j) + 1) \cdot \left(\sum_{\mathcal{A}_0} \text{Tr}(\alpha_{\mathcal{A}_0}^j) \right) + s_j \\ &= (\text{Tr}(\alpha_{\theta_k}^j)) \cdot \left(\sum_{\mathcal{A}_1} \text{Tr}(\alpha_{\mathcal{A}_1}^j) \right) \end{aligned}$$

where α_i is the element defined over $\text{GF}(2^l)$, and $\mathcal{A}_0, \mathcal{A}_1$ are content with the next connection, that is

$$\mathcal{A}_0 \cup \mathcal{A}_1 \subseteq \mathcal{A}.$$

Therefore we have eq. (4) in **Theorem 1** since the characteristic polynomial $h_{\delta_k}(x)$ generating $\hat{s}_j = \text{Tr}(B\alpha_{\delta_k}^j)$, is given as follows :

$$h_{\delta_k}(x) = \prod_{i=0}^{\delta_k-1} (x - \alpha_{\delta_k}^{2^i}).$$