Advanced Science and Technology Letters
Vol.145 (NGCIT 2017), pp.60-63
http://dx.doi.org/10.14257/astl.2017.145.12

Synthesis of CA using Linear Rule Blocks

Sung Won Kang[1] , Un Sook Choi[2], Sung Jin Cho[1], Han Doo Kim[3],
Min Jeong Kwon[1] and Jin Gyoung Kim[1]

[1]Department of Applied Mathematics, Pukyong National University, 48513, Daeyeon 3-Dong, Nam-Gu, Busan, South Korea, jsm2371@hanmail.net(Sung Won Kang: *Presenter*)
sjcho@pknu.ac.kr(Sung Jin Cho: Corresponding author), mjblack02@pknu.ac.kr(Min Jeong Kwon), 5892587@hanmail.net(Jin Gyoung Kim)
[2] Department of Information and Communications Engineering, Tongmyong University, Busan 48520, South Korea, choies@tu.ac.kr
[3] Department of Applied Mathematics and Institute of Basic Science, Inje University, 50834, Inje-ro, Gimhae-si, Gyeongnam, South Korea, mathkhd@inje.ac.kr

Abstract. The key sequence generation method in symmetric key cryptosystems is a very important problem. The shrinking generator is a binary sequence generator composed by two LFSRs: one register produces a sequence and the other is a control register to decimate the sequence.

The linear complexity (LC) of the shrunken sequence generated by this generator is $2^{L_1-2}L_2 < LC \le 2^{L_1-1}L_2$, where L_1 and L_2 are the lengths of the registers. Since the characteristic polynomial of the shrunken sequence is of the form $\{f(x)\}^k$ $(k \in \square)$, it can be modeled as a linear CA.

In this paper, we synthesize 90/150 CA corresponding to $\{f(x)\}^k$ using linear rule blocks and analyze the properties of those CA.

Keywords: Cellular Automata, Characteristic Polynomial, Inverse Symmetric Transition Rule, Linear Rule Blocks, Key Sequence, Shrinking Generator.

1 Introduction

CA has a simple, regular, modular and cascadable structure with logical neighborhood interconnection. The simple structure of CA with logical interconnections is ideally suited for hardware implementation [1]. The characteristics of these CAs are suitable for key sequence generators in symmetric key cryptosystems. For this reason, many researchers have proposed methods to synthesize CA suitable for cryptography etc. Cho et al. proposed efficient methods of synthesis of 90/150 maximal-length CA [2]. Sabater et al. [3] proposed classes of cryptographic interleaved sequences generated by linear 90/150 CA obtained by concatenating the basic automata.

The LC of the shrunken sequence generated by this generator is $2^{L_1-2}L_2 < LC \le 2^{L_1-1}L_2$, where L_1 and L_2 are the lengths of the registers. Since the characteristic polynomial of the shrunken sequence is of the form $\{f(x)\}^k$ $(k \in \square)$, it can be modeled as a linear CA. Sabater et al. [3] synthesized a 90/150 CA with a

ISSN: 2287-1233 ASTL

characteristic polynomial $\{f(x)\}^{2^a}$ $(a \in \square)$ by shrinking generator. However, in order to model various shrunken sequence generators, it is necessary to focus on the problem of synthesizing 90/150 CA corresponding to $\{f(x)\}^k$.

In this paper, to solve this problem, we synthesize 90/150 CA with linear rule blocks and analyze the properties of those 90/150 CA.

2 90/150 CA Preliminaries

Hereafter we use 90/150 CA. Since 90/150 CA is a linear CA, it can be represented as a matrix referred to as the *state transition matrix* over the finite field *GF*(2). An n-cell 90/150 CA is characterized by an $n \times n$ state transition matrix. The state transition matrix T_n is constructed as

$$T_n = \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_n \end{pmatrix}$$

, where $a_i = 0$ (resp. 1) if cell i uses rule 90 (resp. 150). We briefly represent T_n as $< a_1, a_2, \cdots, a_n >$.

Cho et al. [2] proposed a new efficient method for the synthesis of one-dimensional 90/150 linear hybrid group CA for any CA-polynomial as well as irreducible polynomial. This method is efficient and suitable for all practical applications. Sabater et al. [3] and Cho et al. [4] proposed a method of constructing a linear 90/150 CA with characteristic polynomial $f(x)^2$ by concatenating the basic automata whose characteristic polynomial is $f(x)$ which is irreducible.

3 90/150 CA using Linear Rule Blocks

The characteristic polynomial Δ_n of an n-cell 90/150 CA satisfies the following recurrence relation [5]:

$$\Delta_n = (x + a_n)\Delta_{n-1} + \Delta_{n-2}$$

where $\Delta_1 = x + a_1$, $\Delta_0 = 1$.

For the state transition matrix $T_n =< a_1, a_2, \cdots, a_n >$ of an n-cell 90/150 CA, $T_n^* =< a_n, \cdots, a_2, a_1 >$ is called the *symmetric transition rule* of T_n [6], and $\overline{T_n^*} =< \overline{a_n}, \cdots, \overline{a_2}, \overline{a_1} >$ is called the *inverse symmetric transition rule* of T_n [7].

If $\Delta_n = C_n(x)$ is the characteristic polynomial of T_n and $\overline{\Delta_n^*}$ is the characteristic polynomial of $\overline{T_n^*}$, then $\overline{\Delta_n^*} = C_n(x+1)$. Now we investigate the properties about concatenation of the 90/150 CA using the inverse symmetric transition rule blocks.

Theorem 1. Let T_n be the state transition matrix of an n-cell 90/150 CA. Then the characteristic polynomial $V_{2n}(x)$ of $<T_n\overline{T_n^*}>$ is $V_{2n}(x) = \Delta_n\overline{\Delta_n^*} + \Delta_{n-1}\overline{\Delta_{n-1}^*}$.

Since $\Delta_n(x+1)$ $=$ $\overline{\Delta_n^*}(x)$ and $\Delta_{n-1}(x+1)$ $=$ $\overline{\Delta_{n-1}^*}(x)$, $V_{2n}(x)$ $=$ $V_{2n}(x+1)$ in Theorem 1. Let $F(x) = x^{2^n} + x + 1$. Then the degree of every irreducible factor of $F(x)$ over *GF*(2) divides $2n$ [8]. Since $F(x+1) = F(x)$, every irreducible factor of $F(x)$ is one of $V_{2n}(x)$.

For example, for $x^{2^4} + x + 1 = (x^8 + x^6 + x^5 + x^3 + 1)(x^8 + x^6 + x^5 + x^4 + x^3 + x + 1)$, 90/150 CA corresponding to $x^8 + x^6 + x^5 + x^3 + 1$ is <00001111> and 90/150 CA corresponding to $x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$ is <00110011>.

We extend the transition rules by the 2-cell CA $<d_1, d_2>$ as follows.

Theorem 2. Let T_n be the state transition matrix of an n-cell 90/150 CA. Then the characteristic polynomial $V_{2n+2}(x)$ of $<T_n, d_1, d_2, \overline{T_n^*}>$ is

$$V_{2n+2}(x) = D_2\Delta_n\overline{\Delta_n^*} + (x+d_1)\Delta_n\overline{\Delta_{n-1}^*} + \Delta_{n-1}\overline{\Delta_{n+1}^{*\ l_{d_2}}}$$

, where D_2 is the characteristic polynomial of the 2-cell 90/150 CA $<d_1, d_2>$ and $\overline{\Delta_{n+1}^{*\ l_{d_2}}}$ is the characteristic polynomial of rule vector $<d_2, \overline{a_n}, \cdots, \overline{a_2}, \overline{a_1}>$.

Choi et al. proposed 90/150 CA of synthesizing method corresponding to $\{f(x)\}^{2m}$ using symmetric rule [6]. Using symmetric transition rule blocks and inverse symmetric transition rule blocks of basic 90/150 CA, we propose synthesis method of 90/150 CA corresponding to $\{f(x)\}^k$ $(k > 2m)$ such that $f(x+1) = f(x)$ with an example.

For example, assume that R_{30} is a rule of 90/150 CA corresponding to $(x^6 + x^5 + x^3 + x^2 + 1)^5$. We use the rule R_{30} to synthesize 90/150 CA corresponding to $(x^6 + x^5 + x^3 + x^2 + 1)^{40}$. Fig. 1 shows the process of synthesizing 90/150 CA corresponding to $(x^6 + x^5 + x^3 + x^2 + 1)^{40}$ using the method proposed by [6] and Theorem 1.

4 Conclusion

In this paper, we proposed synthesis method of 90/150 CA corresponding to $\{f(x)\}^k$ to model shrunken sequence generator as CA. We gave the synthesis method of the 90/150 CA with the inverse symmetric transition rule and analyzed the characteristic polynomial of the CA. For a given transition rule, a 90/150 CA corresponding to $\{f(x)\}^k$ was synthesized using symmetric transition rule blocks and inverse symmetric transition rule blocks.

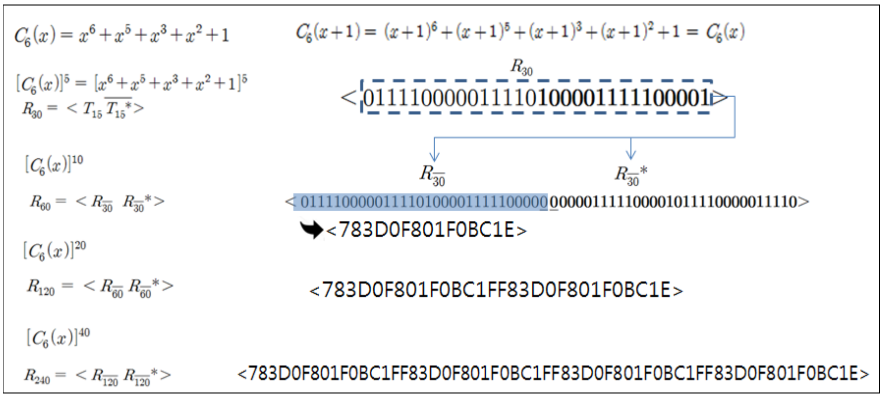
$C_6(x) = x^6+x^5+x^3+x^2+1$
$C_6(x+1) = (x+1)^6+(x+1)^5+(x+1)^3+(x+1)^2+1 = C_6(x)$
$[C_6(x)]^5 = [x^6+x^5+x^3+x^2+1]^5$
$R_{30} = < T_{15}\, \overline{T_{15}}^* >$
R_{30}
<011110000011110100001111100001>
$[C_6(x)]^{10}$
$R_{\overline{30}}$
$R_{\overline{30}}^*$
$R_{60} = < R_{\overline{30}}\ R_{\overline{30}}^* >$
< 011110000011110100001111100000000001111100001011110000011110>
<783D0F801F0BC1E>
$[C_6(x)]^{20}$
$R_{120} = < R_{\overline{60}}\ R_{\overline{60}}^* >$
<783D0F801F0BC1FF83D0F801F0BC1E>
$[C_6(x)]^{40}$
$R_{240} = < R_{\overline{120}}\ R_{\overline{120}}^* >$
<783D0F801F0BC1FF83D0F801F0BC1FF83D0F801F0BC1FF83D0F801F0BC1E>

Fig. 1. The process of synthesizing 90/150 CA corresponding to $(x^6+x^5+x^3+x^2+1)^{40}$.

References

1. Wolfram, S.: Statistical mechanics of cellular automata. Rev. Modern Physics. 55, 601--644 (1983)
2. Cho, S.J., Choi, U.S., Kim, H.D., Hwang, Y.H., Kim, J.G., Heo, S.H.: New synthesis of one-dimensional 90/150 linear hybrid group cellular automata. IEEE Trans. Comput-Aided Design Integr. Circuits Syst. 26(9), 1720--1724 (2007)
3. Sabater, A.F., Gil, P.C.: Synthesis of cryptographic interleaved sequences by means of linear cellular automata. Applied Mathematics Letters. 22, 1518--1524 (2009)
4. Cho, S.J., Choi, U.S., Kim, H.D., Hwang, Y.H., Kim, J.G.: Analysis of 90/150 two predecessor nongroup cellular automata. ACRI 2008, LNCS, 5191, 128--135 (2008)
5. Chaudhuri, P.P., Chowdhury, D.R., Nandi, S., Chatterjee, S.: Additive cellular automata, theory and applications, vol. 1. Los Alamitos, California: IEEE Computer Society Press. (1997)
6. Choi, U.S., Cho, S.J., Kong, G.T.: Analysis of characteristic polynomial of cellular automata with symmetrical transition rules. Proceedings of the Jangjeon Mathematical Society. 18(1), 85--93 (2015)
7. Kim, J.G., Choi, U.S., Cho, S.J., Kim, H.D., Kwon, M.J., Kang, S.W., Pyo, Y.S.: Irreducibility of CA with Inverse Symmetric Transition Rule. Proceedings of the Korea Institute of Electronic Communication Sciences. 11(1), 62--63 (2017)
8. Lidl, R., and Niederreiter, H.: Finite Fields. Cambridge Univ. Press, Cambridge. (1997)