Regular paper | Journal of the KIECS. pp. 593-600, vol. 13, no. 3, Jun. 30 2018, t. 89, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.3.593

90 UCA의 특성다항식과 전이규칙 블록을 이용한 CA 합성법

최언숙* · 조성진**

Characteristic Polynomial of 90 UCA and Synthesis of CA using Transition Rule Blocks

Un-Sook Choi* · Sung-Jin Cho**

요 약

효과적인 암호시스템 설계에 셀룰라 오토마타(이하 CA)가 적용되고 있다. CA는 국소적 상호작용에 의해 상태가 동시에 업데이트되는 성질이 있어서 LFSR보다 랜덤성이 우수하다. 이런 CA를 암호 시스템에 적용하기 위해 주어진 다항식에 대응하는 CA를 합성하는 방법에 대한 연구가 진행되었다. 본 논문에서는 90 UCA의 특성다항식과 전이규칙이 $<00\cdots001>$인 90/150 CA의 특성다항식의 점화관계를 분석한다. 또한 $f(x)=f(x+1)$을 만족하는 삼항다항식 $x^{2^n}+x+1$에 대응하는 90/150 CA를 90 UCA 전이규칙 블록과 특별한 전이규칙 블록을 이용하여 합성한다. 또한 $x^{2^n}+x+1$의 기약인수에 관한 성질을 분석한 후 $x^{2^n}+x^{2^m}+1$ $(n\geq 2, n-m\geq 2)$에 대응하는 90/150 CA 합성 알고리즘을 제안한다.

ABSTRACT

Cellular automata (CA) have been applied to effective cryptographic system design. CA is superior in randomness to LFSR due to the fact that its state is updated simultaneously by local interaction. To apply these CAs to the cryptosystem, a study has been performed how to synthesize CA corresponding to given polynomials. In this paper, we analyze the recurrence relations of the characteristic polynomial of the 90 UCA and the characteristic polynomial of the 90/150 CA whose transition rule is $<00\cdots001>$. And we synthesize the 90/150 CA corresponding to the trinomials $x^{2^n}+x+1\,(n\geq 2)$ satisfying $f(x)=f(x+1)$ using the 90 UCA transition rule blocks and the special transition rule block. We also analyze the properties of the irreducible factors of trinomials $x^{2^n}+x+1$ and propose a 90/150 CA synthesis algorithm corresponding to $x^{2^n}+x^{2^m}+1(n\geq 2, n-m\geq 2)$.

키워드

90/150 Cellular Automata, 90 Uniform CA, Characteristic Polynomial, Synthesis Algorithm, Transition Rule Block
90/150 셀룰라 오토마타, 90 UCA, 특성 다항식, 합성 알고리즘, 전이 규칙 블록

Ⅰ. 서 론

인터넷을 통해 이루어지는 비즈니스의 증가와 비공개 메시지 교환을 위한 네트워크 환경의 사용의 수요 증가는 통신 행위의 프라이버시 및 보안을 제공하기 위한 수단의 증가로 이어진다[1-2]. 암호화 기술은 모든 보안 통신의 필수 요소이다. 대표적인 두 가지 암호화 기술은 비밀키를 가지는 대칭키 암호시스템과

* 동명대학교 정보통신공학과 (choies@tu.ac.kr)
** 교신저자: 부경대학교 응용수학과
· 접 수 일 : 2018. 03. 22
· 수정완료일 : 2018. 05. 03
· 게재확정일 : 2018. 06. 15
· Received : Mar. 22, 2018, Revised : May. 03, 2018, Accepted : Jun. 15, 2018
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math., Pukyong National University,
Email : sjcho@pknu.ac.kr

공개키 암호시스템이다. 두 가지 유형의 시스템에 사용되는 현재 알려진 암호화 기법 또는 새로 등장하는 암호화 기법의 광범위한 개요는 [3]에서 찾을 수 있다. 이러한 유망한 기술 중 하나가 셀룰라 오토마타(Cellular Automata, 이하 CA)를 적용하는 것이다.

CA는 Guan[4]과 Kari[5]에 의해 공개키 암호 시스템에 적용되었다. 공개키 암호 시스템에서는 두 개의 키가 필요하다. 하나의 키는 암호화를 위해 사용되고 다른 하나는 복호를 위해 사용된다. 그 중 하나는 비공개로 유지되고, 다른 하나는 공개된다. CA는 국소적 상호작용에 의해 상태가 이산시간에 따라 자동적으로 업데이트된다. 이러한 CA는 LFSR보다 렌덤성이 우수하고 작은 단위로 확장 연결이 가능하다. 이러한 특성으로 인해 CA는 테스트패턴 생성기, 키수열 생성기로 적합하다. 또한 이미지 암호를 위한 기저영상 생성기, 대칭키 암호시스템에서 키수열 생성기로 사용하기에 적합하다. 대칭키 암호시스템을 위한 CA는 Wolfram에 의해 연구되었으며, 나중에 Hortensius 등, Nandi 등, Das 등에 의해 연구되었다[6-9]. Tomassini 등은 스트림 암호시스템을 위한 1차원 2차원 CA에 대하여 연구하였다[10].

이러한 CA를 모델링하기 위해서는 주어진 다항식에 대응하는 CA를 합성해야 한다. 그러나 주어진 다항식에 대응하는 CA를 구성하는 것이 LFSR보다 어렵다. 그동안 여러 연구자들에 의해 CA 합성에 관한 연구들이 진행되었다[11-18]. Cho 등은 최대 길이 90/150 CA를 갖는 90/150 CA를 합성하는 효율적인 방법을 제안하였다[14]. 이들이 제안한 방법은 Cattell 등[13]에 의해 제안된 합성 방법의 시간복잡도 $O(n^7)$을 $O(n^2)$로 감소시켰다.

Sabater 와 Cho 등은 효과적인 키수열을 생성하기 위하여 비선형적인 방법으로 키수열을 생성하는 수축수열 생성기를 CA를 이용하여 모델링 하였다[16-17]. 두 개의 LFSR을 이용하여 비선형적인 방법으로 키수열을 생성하는 수축수열 생성기에 의해 생성되는 수열의 특성다항식이 $[p(x)]^{2^a}$이라는 성질을 이용하여 이들은 가약다항식 $[p(x)]^{2^a}(a \geq 0)$ (여기서 $p(x)$는 2차 이상의 기약다항식)에 대응하는 90/150 CA의 합성 방법을 제안하였다.

Choi 등은 다항식의 계수가 모두 1인 자체 상반 다항식(self-reciprocal polynomial) $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$의 CA-다항식 여부를 결정하는 방법에 대하여 연구하였고 $f_n(x)$에 대응하는 90/150 CA의 개수를 결정하는 방법을 제안하였다[18].

본 논문에서는 90 UCA(uniform CA)와 전이규칙이 $< 00 \cdots 001 >$인 90/150 CA의 특성다항식의 점화관계를 분석한다. 이러한 결과를 이용하여 $f(x) = f(x+1)$을 만족하는 삼항다항식 $x^{2^n} + x + 1$에 대응하는 90/150 CA를 90 UCA 전이규칙 블록과 특별한 전이규칙 블록을 이용하여 합성한다. 그리고 $x^{2^n} + x + 1$의 기약인수에 관한 성질을 분석한 후 $x^{2^n} + x^{2^m} + 1$에 대응하는 90/150 CA 합성 알고리즘을 제안한다.

II. CA Preliminaries

CA 중 가장 간단한 구조를 갖는 1차원 3-이웃 CA의 각 셀의 상태전이 함수는 식 (1)과 같다.

$$s_i^{t+1} = f_i(s_{i-1}^t, s_i^t, s_{i+1}^t) \tag{1}$$

여기서 s_i^t는 시간 t에서 i번째 셀의 상태를 나타낸다. 표 1은 본 논문에서 사용되는 전이 규칙 90과 150에 대한 부울식을 나타낸다.

표 1. 전이규칙 90과 150의 부울식
Table 1. The corresponding combinational logic for rule 90 and 150

rule 90	$s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$
rule 150	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$

그림 1은 본 논문에서 사용되는 전이 규칙에 대하여 Wolfram의 표기법으로 묘사한 것이다.

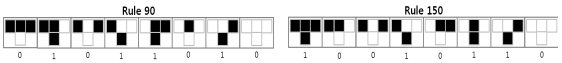

그림 1. Wolfram의 표기에서 묘사된 규칙 90과 150
Fig. 1 Rule 90 and 150 depicted in Wolfram's notation

전이규칙 90은 왼쪽 셀과 오른쪽 셀의 영향을 받아 다음 셀이 결정되고, 전이규칙 150은 왼쪽 셀과 셀 자신, 오른쪽 셀의 영향을 받아 다음 셀이 결정된다. 그러므로 n셀 90/150 CA의 상태전이행렬은 식 (2)와 같다.

$$T_n = \begin{pmatrix} d_1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & d_2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & d_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 1 & d_n \end{pmatrix} \quad (2)$$

여기서 CA의 i번째 셀에 적용되는 전이규칙이 90이면 $d_i = 0$, 150이면 $d_i = 1$이다. $T_n = < d_1 d_2 \cdots d_n >$로 간단히 나타낸다.

그림 2는 $T_4 = < 0101 >$인 90/150 CA의 구조이다.

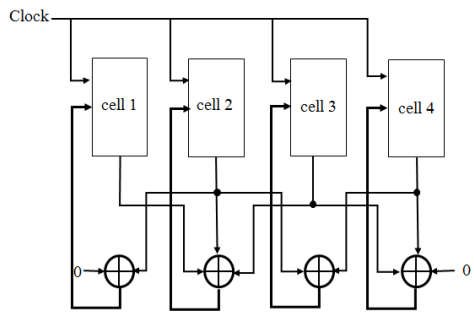

그림 2. 전이규칙 $< 0101 >$인 4셀 90/150 CA
Fig. 2 4cell 90/150 CA with rule $< 0101 >$

n셀 CA에 적용되는 규칙이 모두 같은 CA를 UCA(Uniform CA)라 한다. $T_n = < 00 \cdots 0 >$ 인 CA는 90 UCA이다. 또한 두 개 이상의 전이규칙이 적용된 CA를 HCA(Hybrid CA)라고 한다. 90/150 CA는 HCA이며, 본 논문에서는 HCA를 간단히 CA라 쓴다.

n-셀 90/150 CA의 $GF(2)$ 상의 특성다항식(characteristic polynomial) Δ_n은 $\Delta_n = |T_n \oplus x I_n|$ 이다. 여기서 I_n은 $n \times n$ 단위행렬이다. 그림 2의 4셀 90/150 CA의 특성다항식은 $x^4 + x + 1$이다.

상태전이행렬이 T_n인 임의의 n셀 90/150 CA에 대하여 T_n의 최소다항식(minimal polynomial)은 T_n의 특성다항식과 같다. 특성다항식을 구하는 계산과정은 행렬곱셈 연산에 해당되므로 계산복잡도가 크다. 그러나 90/150 CA의 전이행렬은 식 (2)와 같이 삼중대각행렬이므로 점화관계를 이용하여 효율적으로 계산할 수 있다.

Δ_n을 T_n의 특성다항식이라고 하자. 그러면 식 (3)과 같은 점화식이 성립한다[19].

$$\Delta_n = (x + d_n)\Delta_{n-1} + \Delta_{n-2} \quad (3)$$

여기서 $\Delta_1 = x + d_1$, $\Delta_0 = 1$이다.

n셀 90 UCA의 상태전이행렬 $T_n = < 000 \cdots 00 >$에 대하여 $\det(T_n) = \det(T_{n-2})$ 이고, $|T_1| = 0$, $|T_2| = 1$이다[17]. T_n의 행렬식이 1일 때, 주어진 n셀 CA는 가역 CA(invertible CA)이고, 암호시스템에서 키수열 생성기로 사용되는 CA는 가역CA이다. 특성다항식의 점화식인 식(3)에서 T_n을 90 UCA의 전이행렬이라 하면, 이에 대응하는 특성다항식 $U_n(x)$은 식 (4)와 같은 점화관계를 만족한다.

$$U_n(x) = x\,U_{n-1}(x) + U_{n-2}(x) \quad (4)$$
$$(U_1(x) = x,\ U_0(x) = 1)$$

다음 보조정리는 [20]에 의해 쉽게 얻을 수 있다.

<보조정리 1> 전이규칙이 $< 00 \cdots 001 >$인 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 할 때, $2k$ 셀 90 UCA의 특성다항식 $U_{2k}(x)$는 $U_{2k}(x) = [H_k(x)]^2$이다.

보조정리 2는 [21]의 결과이다.

<보조정리 2> k셀 90 UCA의 특성다항식이 $U_k(x)$일 때, 다음을 만족한다.

(ⅰ) $U_{2k+1}(x) = x[U_k(x)]^2 \quad (k \geq 1)$

(ⅱ) $U_{2^n-1}(x) = x^{2^n-1}$

III. 90 UCA 특성다항식 분석과 90 UCA를 이용한 CA합성

이 절에서는 전이규칙 $<00\cdots001>$인 k셀 90/150 CA의 특성다항식 $H_k(x)$과 k셀 90 UCA의 특성다항식 $U_k(x)$의 관계를 분석한다.

<보조정리 3> 전이규칙이 $<00\cdots001>$인 k셀 CA의 특성다항식을 $H_k(x)$라 하면 $H_{2^a}(x)=[H_{2^{a-1}}(x)]^2+x^{2^a-1}$이다.

(증명) k셀 90 UCA의 특성다항식을 $U_k(x)$라 하자. 식(3)에 의해 특성다항식 $H_k(x)$는 다음과 같다.

$$\begin{aligned} H_k(x) &= (x+1)U_{k-1}(x)+U_{k-2}(x) \\ &= (xU_{k-1}(x)+U_{k-2}(x))+U_{k-1}(x) \\ &= U_k(x)+U_{k-1}(x) \end{aligned} \quad (5)$$

그러므로 보조정리 1과 보조정리 2(ii)에 의해

$$H_{2^a}(x)=[H_{2^{a-1}}(x)]^2+x^{2^a-1}$$

이다. □

보조정리 1과 보조정리 3의 증명과정의 식 (5)에 의해 k셀 90 UCA의 특성다항식 $U_k(x)$와 $2k$셀 90 UCA의 특성다항식 $U_{2k}(x)$과의 관계는 식(6)과 같다.

$$U_{2k}(x)=[U_k(x)+U_{k-1}(x)]^2 \quad (6)$$

<정리 4> k셀 90 UCA 특성다항식 $U_k(x)$에 대하여 $U_{2^n-2}(x)$는 다음을 만족한다.

$$U_{2^n-2}(x)=1+\sum_{i=1}^{n-1}x^{2^n-2^i} \quad (n \geq 2)$$

(증명) $n=2$일 때, $U_2(x)=\begin{vmatrix} x & 1 \\ 1 & x \end{vmatrix}=x^2+1$ 이므로 성립한다.

$U_{2^k-2}(x)=x^{2^k-2}+x^{2^k-2^2}+\cdots+x^{2^{k-1}}+1$ 이라고 하면, $n=k+1$일 때, 식(3), (6), 보조정리 2(i)에 의해 $U_{2^{k+1}-2}(x)$는 다음과 같다.

$$\begin{aligned} U_{2^{k+1}-2}(x) &= [U_{2^k-1}(x)+U_{2^k-2}(x)]^2 \quad (\text{식}(6)) \\ &= [x\,U_{2^k-2}(x)+U_{2^k-3}(x)+U_{2^k-2}(x)]^2 \\ &= [(x+1)U_{2^k-2}(x)+x\{U_{2^{k-1}-2}(x)\}^2]^2 \\ &= (x+1)^2\left(x^{2^k-2}+x^{2^k-2^2}+\cdots+x^{2^{k-1}}+1\right)^2 \\ &\quad +x^2(x^{2^{k-1}-2}+x^{2^{k-1}-2^2}+\cdots+x^{2^{k-2}}+1)^4 \\ &= (x+1)^2\left(x^{2^{k+1}-2^2}+x^{2^{k+1}-2^3}+\cdots+x^{2^k}+1\right) \\ &\quad +x^2(x^{2^{k+1}-2^3}+x^{2^{k+1}-2^4}+\cdots+x^{2^k}+1) \\ &= x^{2^{k+1}-2}+x^{2^{k+1}-2^2}+x^{2^{k+1}-2^3}+\cdots+x^{2^k}+1 \end{aligned}$$

따라서 $U_{2^n-2}(x)=1+\sum_{i=1}^{n-1}x^{2^n-2^i}$ 이다. □

정리 4로부터 따름정리 5를 얻는다.

<따름정리 5> (i) $U_{2^{n+1}-2}(x)=x^{2^n}U_{2^n-2}(x)+1$

(ii) $U_{2^n-3}(x)=x+\sum_{i=2}^{n-1}x^{2^n-2^i+1}$ $(n \geq 2)$

90 UCA와 전이규칙 $D_4=<0101>$인 90/150 CA를 이용하여 삼항다항식 $x^{2^n}+x+1$에 대응하는 가역 CA를 합성하는 방법을 제안하기 위해 $H_{2^n}(x)$와 $H_{2^n-1}(x)$의 관계를 분석한다.

<보조정리 6> 전이규칙 $<00\cdots001>$인 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 하면 다음이 성립한다.

$$H_{2^n-1}(x)=[H_{2^{n-1}-1}(x)]^2+x^{2^n-1}$$

(증명) 보조정리 3의 식(5)와 보조정리 2(ii), 보조정리 1에 의해

$$\begin{aligned} H_{2^n-1}(x) &= U_{2^n-1}(x)+U_{2^n-2}(x) \\ &= x^{2^n-1}+[H_{2^{n-1}-1}(x)]^2 \end{aligned}$$

이다. □

<보조정리 7> 전이규칙 $<00\cdots001>$인 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 하면 $H_{2^n}(x)+H_{2^n-1}(x)=x^{2^n}$이다.

(증명) $U_{2m}(x)=[H_m(x)]^2$이고(보조정리 1), $H_k(x)=U_k(x)+U_{k-1}(x)$(식(5))이므로,

$$H_{2^n}(x)+H_{2^n-1}(x) = U_{2^n}(x)+U_{2^n-2}(x)$$
$$= [H_{2^{n-1}}(x)]^2+[H_{2^{n-1}-1}(x)]^2$$
$$= [H_{2^{n-1}}(x)+H_{2^{n-1}-1}(x)]^2$$

이다. $<10>$의 특성다항식은 $H_2(x)=x^2+x+1$이고, $<1>$의 특성다항식은 $H_1(x)=x+1$이므로

$H_2(x)+H_1(x)=(x^2+x+1)+(x+1)=x^2$이 다.

따라서 $H_{2^n}(x)+H_{2^n-1}(x)=[H_{2^{n-1}}(x)+H_{2^{n-1}-1}(x)]^2=\cdots$

$=[H_2(x)+H_1(x)]^{2^{n-1}}=x^{2^n}$ 이다. □

<보조정리 8> 전이규칙이 $<00\cdots001>$인 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 할 때, $H_{2^n}(x)H_{2^n-1}(x)=x^{2^{n+1}-1}+1$이다.

(증명) (i) $n=1$일 때

$H_2(x)H_1(x)=(x^2+x+1)(x+1)=x^3+1$이므로 성립한다.

(ii) $n=k$일 때 $H_{2^k}(x)H_{2^k-1}(x)=x^{2^{k+1}-1}+1$라 하면 $n=k+1$일 때,

보조정리 3, 보조정리 6과 보조정리 7에 의하여

$$H_{2^{k+1}}(x)H_{2^{k+1}-1}(x)$$
$$= \left([H_{2^k}(x)]^2+x^{2^{k+1}-1}\right)\left(x^{2^{k+1}-1}+[H_{2^k-1}(x)]^2\right)$$
$$= x^{2^{k+2}-2}+x^{2^{k+1}-1}\left(H_{2^k}(x)+H_{2^k-1}(x)\right)^2$$
$$+\left(H_{2^k}(x)H_{2^k-1}(x)\right)^2$$
$$= x^{2^{k+2}-2}+x^{2^{k+1}-1}x^{2^{k+1}}+\left(x^{2^{k+1}-1}+1\right)^2$$
$$= x^{2^{k+2}-1}+1$$

이다. 따라서 $H_{2^n}(x)H_{2^n-1}(x)=x^{2^{n+1}-1}+1$이다. □

<정리 9> 크기가 $m(:=2^{n-1}-2)$인 90 UCA 의 전이규칙을 O_m라 하고, 4셀 90/150 CA의 전이규칙 $D_4=<0101>$에 대하여, $T_{2^n}=<O_mD_4O_m>$인 2^n셀 90/150 CA 의 특성다항식을 $C_{2^n}(x)$라 하면 $C_{2^n}(x)=x^{2^n}+x+1$이다.

(증명) $C_{2^n}(x)=|T_{2^n}+xI_{2^n}|$에 대하여 $(2^{n-1}+1)$번째 행을 여인수 전개하면

$$C_{2^n}(x) = U_{2^{n-1}-1}(x)H_{2^{n-1}-1}(x)$$
$$+xH_{2^{n-1}}(x)H_{2^{n-1}-1}(x)+H_{2^{n-1}}(x)U_{2^{n-1}-2}(x)$$

이다. 보조정리 2(ii), 보조정리 3, 보조정리 6과 보조정리 8에 의해

$$C_{2^n}(x)$$
$$= x^{2^{2^{n-1}-1}}\left(x^{2^{2^{n-1}-1}}+[H_{2^{n-2}-1}(x)]^2\right)$$
$$+x\left([H_{2^{n-2}}(x)]^2+x^{2^{2^{n-1}-1}}\right)\left(x^{2^{2^{n-1}-1}}+[H_{2^{n-2}-1}(x)]^2\right)$$
$$+\left([H_{2^{n-2}}(x)]^2+x^{2^{2^{n-1}-1}}\right)[H_{2^{n-2}-1}(x)]^2$$
$$= x^{2^n-2}+x^{2^{n-1}-1}[H_{2^{n-2}-1}(x)]^2$$
$$+x\left(H_{2^{n-2}}(x)H_{2^{n-2}-1}(x)\right)^2+x^{2^n-1}$$
$$+x^{2^{n-1}}\left(H_{2^{n-2}}(x)+[H_{2^{n-2}-1}(x)]^2\right)^2$$
$$+\left(H_{2^{n-2}}(x)+[H_{2^{n-2}-1}(x)]^2\right)^2+x^{2^{n-1}-1}[H_{2^{n-2}-1}(x)]^2$$
$$= x^{2^n-2}+x^{2^{n-1}-1}+x^{2^n}+(x+1)\left(x^{2^{n-1}-1}+H_{2^{n-2}}(x)H_{2^{n-2}-1}(x)\right)^2$$
$$= x^{2^n}+(x+1)\left(x^{2^{n-1}-1}+H_{2^{n-2}}(x)H_{2^{n-2}-1}(x)\right)^2$$
$$= x^{2^n}+x+1$$

이다. □

Ⅳ. 삼항다항식의 성질과 전이규칙 블록을 이용한 CA합성 알고리즘

이 절에서는 크기가 $m(:=2^{n-1}-2)$인 90 UCA의 전이규칙 블록 O_m과 전이규칙 블록 $D_4=<0101>$를 이용하여 합성한 2^n셀 90/150 CA $\mathbb{C}_{2^n}=<O_mD_4O_m>$의 특성다항식을 분석한다. 정리 9에 의해 $\mathbb{C}_{2^n}$의 특성다항식은 $x^{2^n}+x+1$이다.

$F_n(x):=x^{2^n}+x+1$라 하면 $F_n(x+1)=F_n(x)$이다. 이는 $<O_mD_4O_m>$에 대응하는 특성다항식과 $<\overline{O_mD_4O_m}>$에 대응하는 특성다항식이 같다는 의미이다. 즉, 전이규칙이 90인 셀은 규칙 150으로, 규칙이 150인 셀은 90으로 모두 바꾸면 이 두 CA는 서로 다른 CA이지만 특성다항식은 같다. 예를 들어 <0000000101000000>와 <1111111010111111>의 특성다항식은 모두 $x^{16}+x+1$ 이다.

다음은 삼항다항식 $x^{2^n}+x+1$의 기약인수에 대한 분석이다.

<정리 10> $F_n(x):=x^{2^n}+x+1$일 때 $F_n(x)$는 n/d이 홀수인 각 d에 대한 $2d$차 기약다항식들의 곱이며, $2d$차 기약다항식의 인수의 수는 $2d$차 자체상반 기약다항식의 개수와 같다.

(증명) $F_n(x)$의 상반다항식 $F_n^*(x)$는

$F_n^*(x)=x^{2^n}F_n(x^{-1})=x^{2^n}+x^{2^n-1}+1$이므로

$V_n(x):=F_n^*(x+1)$라 할 때, $V_n(x)=(x+1)^{2^n}+$ $+(x+1)^{2^n-1}+1=x^{2^n}+x^{2^n-1}+\cdots+x+1$ 이다.

$V_n(x)\,|\,(x^{2^n+1}+1)\,|\,(x^{2^{2n}-1}+1)$ 이므로 $V_n(x)$은 x를 제외한 차수가 $2n$의 약수인 기약다항식들의 곱이다. 또한 $V_n(x)=(x^{2^n+1}+1)/(x+1)$이므로 정리 1[22]에 의하여 $V_n(x)$는 n/d이 홀수인 각 d에 대한 $2d$차 모든 자체상반기약다항식들의 곱이다. 기약다항식의 상반다항식이 기약이고 $g(x)$가 기약일 때 $g(x+1)$도 기약이므로 $F_n(x)$와 $V_n(x)=F_n^*(x+1)$의 기약인수의 개수는 같다[23]. 따라서 $F_n(x)$는 n/d이 홀수인 각 d에 대한 $2d$차 모든 자체상반기약다항식의 개수만큼의 $2d$차 기약다항식들의 곱이다. □

Table 2. Factorization of $x^{2^n}+x+1$ according to n
표 2. n에 따른 $x^{2^n}+x+1$의 인수분해

n	factors of $x^{2^n}+x+1$
1	(2,1,0)
2	(4,1,0)
3	(6,5,3,2,0)(2,1,0)
4	(8,6,5,3,0)(8,6,5,4,3,1,0)
5	(10,9,8,3,2,1,0)(10,9,8,6,5,1,0)(10,9,8,4,3,2,0) (2,1,0)

<예제> $F_3(x)$일 때, $3/d$가 홀수가 되는 d는 1, 3이다. 그러므로 $F_3(x)$는 6차 다항식과 2차 다항식으로 인수분해 된다. $F_4(x)$에 대하여 $4/d$가 홀수가 되는 경우는 $d=4$이다. 따라서 $F_4(x)$는 8차 기약다항식 2개로 인수분해 된다.$F_5(x)$의 10차의 기약인수의 차수는 $5/d$가 홀수이므로 $d=1,5$이므로 2차와 10차가 되어야 한다. 2차 기약인수는 x^2+x+1 뿐이다. 따라서 10차의 기약인수의 개수는 3이다. 실제로 $F_5(x)=x^{32}+x+1$ 을 인수분해하면 다음과 같다.

$$F_5(x)=(x^2+x+1)(x^{10}+x^9+x^8+x^6+x^5+x+1)\times(x^{10}+x^9+x^8+x^4+x^3+x^2+1)\times(x^{10}+x^9+x^8+x^3+x^2+x+1)$$

표 2는 $F_n(x)$의 인수분해 결과이다. 표 2에서 (6,5,3,2,0)은 인수 다항식의 계수가 0이 아닌 항 x^i의 i값이다. 즉 (6,5,3,2,0)는 $x^6+x^5+x^3+x^2+1$이다.

표3은 정리 9의 결과와 보조정리 1을 이용하여 삼항다항식 $x^{2^n}+x^{2^m}+1$에 대응하는 90/150 CA합성알고리즘이다.

Table 3. Synthesis algorithm of 90/150 CA corresponding to $x^{2^n}+x^{2^m}+1$
표 3. $x^{2^n}+x^{2^m}+1$에 대응하는 90/150 HCA 합성알고리즘

[Tri_Poly_HCA_synthesis_Algorithm]

Input : n,m $(n>m+2)$
Output : 90/150 CA transition rule

Step 1. Compute $k=n-m$.
Step 2. Generation of 90 UCA $O_{2^{k-1}-2}$.
Step 3. Generation of 90/150 CA
$T_{2^{n-m}}=<O_{2^{k-1}-2}D_4O_{2^{k-1}-2}>$ corresponding to $x^{2^{n-m}}+x+1$.
Step 4 for i from 1 to m do
(i) $r_{2^{n-m+i-1}}\leftarrow r_{2^{n-m+i-1}}+1 \bmod 2$
(ii) $T_{2^{n-m+i}}=<R_{2^{n-m+i-1}}R^*_{2^{n-m+i-1}}>$,
where, $R_{2^{n-m+i-1}}$ is the modified rule in (i)
and R^* is the symmetric transition rule of R.

Ⅴ. 결론

본 논문에서는 암호시스템에서 키수열 생성자로 사용되는 90/150 CA를 모델링하기 위해 90 UCA 전이규칙 블록과 특별한 전이규칙 블록을 이용하여 항의 수가 최소인 삼항 다항식 $F(x)=x^{2^n}+x+1(n\geq 2)$에 대응하는 가역 CA를 합성하였다. 또한 90 UCA의 특성다항식과 전이 규칙이 $<00\cdots001>$인 90/150 CA의 특성다항식의 점화관계를 분석하였다. 이러한 결과는 차수가 높은 CA의 특성다항식 계산을 매우 효율적으로 수행함으로써 CA의 특성을 파악하는데 효과적이다. 또한 $x^{2^n}+x^{2^m}+1\,(n\geq 2, n-m\geq 2)$에

대응하는 90/150 CA 합성알고리즘을 제안하였다. 이러한 연구는 CA기반의 효과적인 키 생성기를 모델링하는데 도움이 될 것으로 사료된다.

감사의 글

본 논문은 Proceedings, ICEIC 2017 논문[90/150 CA corresponding to $x^{2^n}+x^{2^a}+1$]을 확장한 논문임.

References

[1] E. Jang, "Synchronization and Secure Communication Application of Chaos Based Malasoma System," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 5, 2017, pp. 747-754.

[2] J. Saidov, B. Kim, J. Lee, and G. Lee, "Distributed Hardware Security System with Secure Key Update," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 4, 2017, pp. 671-678.

[3] B. Schneier, *Applied Cryptography.* New York: Wiley, 1996.

[4] P. Guan, "Cellular Automaton Public-Key Cryptosystern," *Complex Systems,* vol. 1, no. 1, 1987, pp. 51-56.

[5] J. Kari, "Reversibility and Surjectivity Problems of Cellular Automata," *J. Comput. System Sci.* vol. 48, no. 1, 1994, pp. 149-182.

[6] S. Wolfram, "Cryptography with Cellular Automata," *Int. Conf. on the Theory and Application of Cryptographic Techniques 1985, Lecture Notes in Computer Science 218,* California, U.S.A., Aug., 1985, pp. 429-432.

[7] P. Hortensius, R. McLeod, and H.Card, "Parallel random number generation for VLSI systems using cellular automata," *IEEE Truns. Computers,* vol. 38, no. 10, 1989, pp. 1466-1473.

[8] S. Nandi, B. Kar, and P. Chaudhuri, "Theory and Applications of Cellular Automata in Cryptography," *IEEE Truns. Computers*, vol. 43, no. 12, 1994, pp. 1346-1357.

[9] S. Das and D. Chowdhury, "On usage of cellular automata in strengthening stream ciphers," *J. Discrete Mathematical Sciences and Cryptography*, vol. 14, no. 4, 2011, pp. 369-390.

[10] M. Tomassini and M. Perrenoud, "Stream Ciphers with One- and Two-Dimensional Cellular Automata," *Int. Conf. on the Parallel Problem Solving from Nature - PPSN VI, Lecture Notes in Computer Science 1917*, Paris, France, Sep., 2000, pp. 722-731.

[11] S. Kwon, S. Cho, U. Choi, and H. Kim, "Reachable table of nonlinear cellular automata," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 10, no. 5, 2015, pp. 593-598.

[12] H. Kim and S. Cho, "Synthesis of Uniform CA and 90/150 Hybrid CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, 2016, pp. 293-302.

[13] U. Choi, S. Cho, M. Kwon, S. Kim, and H. Kim, "Synthesis of 90/102(170)/150 linear CA using 90/150 linear CA," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 9, 2016, pp. 885-892.

[14] S. Cho, U. Choi, H. Kim, Y. Hwang, J. Kim, and S. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems,* vol. 26, no. 9, 2007, pp. 1720-1724.

[15] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," *IEEE Trans. Comput-Aided Design Integrated Circuits and Systems,* vol. 15, no. 3, 1996, pp. 325-335.

[16] A. Sabater and P. Gil, "Synthesis of cryptographic interleaved sequences by means of linear cellular automata," *Applied Mathematics Letters*, vol. 22, no. 10, 2009, pp. 1518-1524.

[17] S. Cho, U. Choi, H. Kim, and H. An, "Analysis of nonlinear sequences based on shrinking generator," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 5, no. 4, 2010, pp. 412-417.

[18] U. Choi, S. Cho, H. Kim, and J. Kim, "90/150 CA corresponding to polynomial of maximum weight," *J. of Cellular Automata,* vol.13, no. 4, 2018, pp.347-358.

[19] P. Chaudhuri, D. Chowdhury, S. Nandi, and

S. Chattopadhyay, *Additive Cellular Automata Theory and Applications, vol. 1.* Los Alamitos: IEEE Computer Society Press, 1997.
[20] U. Choi, S. Cho, and G. Kong, "Analysis of Characteristic Polynomial of Cellular Automata with Symmetrical Transition Rules," *Proc. of the Jangjeon Mathematical Society,* vol. 18, no. 1, 2015, pp. 85-93.
[21] S. Cho, U. Choi, H. Kim, Y. Hwang, and J. Kim, "Analysis of 90/150 Two Predecessor Nongroup Cellular automata," *Int. Conf. on Cellular Automata for Research and Industry(ACRI) 2008, Lecture Notes in Computer Science 5191*, Yokohama, Japan, Sept., 2008, pp. 128-135.
[22] H. Meyn, "On the Construction of Irreducible Self-Reciprocal Polynomials Over Finite Fields," *Applicable Algebra in Engineering, Communication and Computing,* vol. 1, no. 1, 1990, pp. 43-53.
[23] S. Golomb, *Shift Register Sequences,* California: Aegean Park Press, 1982.

저자 소개

최언숙 (Un-Sook Choi)

1992년 성균관대학교 산업공학과 졸업 (공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 대학원 응용수학과 졸업(이학박사)
2009년 부경대학교 대학원 정보보호학과 졸업(공학박사)
2006년 ~ 현재 동명대학교 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론

조성진 (Sung-Jin Cho)

1979년 강원대학교 수학교육과 졸업 (이학사)
1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년 ~ 현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호