Regular paper

Journal of the KIECS. pp. 819-826, vol. 13, no. 4, Aug. 31 2018, t. 90, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.4.819

2^n차 최대무게 다항식에 대응하는 90/150 RCA

최언숙* · 조성진**

90/150 RCA Corresponding to Maximum Weight Polynomial with degree 2^n

Un-Sook Choi* · Sung-Jin Cho**

요 약

일반화된 해밍무게는 선형부호의 중요한 파라미터의 하나로써 암호시스템에 적용할 때 부호의 성능을 결정한다. 그리고 격자도를 이용하여 블록부호를 연판정으로 복호할 때 구현에 필요한 상태복잡도를 평가하는 척도가 되기도 함으로써 그 중요성이 한층 부각되고 있다. 특별히 삼항다항식을 기반으로 하는 유한체 상의 비트-병렬 곱셈기에 대한 연구가 진행되어왔다. 셀룰라오토마타(Cellular Automata, 이하 CA)는 국소적 상호작용에 의해 상태가 동시에 업데이트되는 성질이 있어서 LFSR보다 랜덤성이 우수하다. 본 논문에서는 효과적인 암호시스템 설계에 있어 중요한 요소 중 하나인 의사난수열 생성기의 효과적 합성에 관하여 다룬다. 먼저 간단한 90/150 전이규칙 블록의 특성다항식의 성질을 분석하고, 이 규칙블록을 이용하여 삼항다항식 $x^{2^n}+x^{2^n-1}+1(n\geq 2)$ 에 대응하는 가역 90/150 CA와 2^n 차 최대무게다항식에 대응하는 90/150 가역 CA(RCA)의 합성알고리즘을 제안한다.

ABSTRACT

The generalized Hamming weight is one of the important parameters of the linear code. It determines the performance of the code when the linear codes are applied to a cryptographic system. In addition, when the block code is decoded by soft decision using the lattice diagram, it becomes a measure for evaluating the state complexity required for the implementation. In particular, a bit-parallel multiplier on finite fields based on trinomials have been studied. Cellular automata(CA) has superior randomness over LFSR due to its ability to update its state simultaneously by local interaction. In this paper, we deal with the efficient synthesis of the pseudo random number generator, which is one of the important factors in the design of effective cryptosystem. We analyze the property of the characteristic polynomial of the simple 90/150 transition rule block, and propose a synthesis algorithm of the reversible 90/150 CA corresponding to the trinomials $x^{2^n}+x^{2^n-1}+1(n\geq 2)$ and the 90/150 reversible CA(RCA) corresponding to the maximum weight polynomial with 2^n degree by using this rule block.

키워드

90/150 Reversible Cellular Automata, Reversible CA, Maximum Weight Polynomial, Minimum Weight Polynomial, Synthesis Algorithm
90/150 가역 셀룰라 오토마타, 가역 CA, 최대 무게 다항식, 최소 무게 다항식, 합성 알고리즘

* 동명대학교 정보통신공학과 (choies@tu.ac.kr)
**교신저자: 부경대학교 응용수학과
· 접 수 일 : 2018. 05. 21
· 수정완료일 : 2018. 07. 03
· 게재확정일 : 2018. 08. 15
· Received : May. 21, 2018, Revised : Jul. 03, 2018, Accepted : Aug. 15, 2018
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math., Pukyong National University,
Email : sjcho@pknu.ac.kr

Ⅰ. 서 론

스마트폰, 태블릿 PC등과 같은 스마트기기의 확산과 클라우드 서비스를 비롯한 관련 기술의 발달로 가정/업무환경을 비롯하여 사회 전 분야에 걸쳐 큰 혁신이 일어나고 있다. 원격으로 가사활동 뿐만 아니라 학습, 진료 등이 가능해지고, SNS를 통한 광범위한 정보공유와 새로운 사회적 관계가 형성되고 있다. 특히 최근에는 기존의 한계를 뛰어넘어 언제 어디서나 편리하면서도 효율적으로 업무에 종사할 수 있도록 스마트 워크 환경이 정착되어 가고 있다. 그러나 이러한 컴퓨팅 환경은 그 특성상 기존의 서버환경과는 다르게 데이터를 클라우드 서버라 불리는 중앙 서버로 위탁하는 방식이기 때문에 서비스 제공자는 사용자의 데이터들을 위탁 받는다. 이러한 환경 환경으로 인해 사용자들의 민감한 개인정보가 유출될 가능성이 더욱 높아지게 되었다[1]. 이로 인해 발생하는 개인정보 유출사건은 사회적 개인적 큰 손실을 초래한다. 따라서 이러한 환경에서 정보를 안전하게 보호하는 문제는 매우 중요한 문제이다[2,3].

부호를 암호시스템에 응용하는 과정에서 도입된 개념인 일반화된 해밍무게는 격자도를 이용하여 블록부호를 연판정(soft decision)으로 복호할 때 상태 복잡도(state complexity)와 등가임이 입증됨으로써 중요성이 한층 부각되고 있다. 특별히 삼항다항식을 기반으로 하는 유한체 상의 비트-병렬 곱셈기에 대한 연구가 진행되어왔다[4].

셀룰라 오토마타(Cellular Automata, 이하 CA)는 동역학계를 해석하는 한 방법으로 시간과 공간을 이산적으로 다룬다. 이산적 공간인 셀룰러 공간은 셀이라는 기억소자로 구성되어있다. CA는 각 셀이 취할 수 있는 상태를 유한하게 처리하며 각 셀들의 상태가 국소적인 상호작용에 의해 동시에 업데이트되는 시스템이다. 더욱이 CA는 인접한 이웃들과 결합논리로 서로 연결되어 있고 그 형태가 규칙적인 배열로 구성되기 때문에 랜덤성이 좋은 랜덤 패턴을 효과적으로 생성할 수 있다. 이러한 이유로 CA는 Wolfram에 의해 처음 암호시스템에서 응용되었고[5], 이미지 암호를 위한 기저영상 생성기, 대칭키 암호시스템에서 키수열 생성기 등에 응용되었다[6-9]. CA는 Guan에 의해 공개키 암호시스템에 적용되었으며[10] 암호시스템 뿐만 아니라 CA는 테스트패턴 생성기, 오류정정부호 등 다양한 분야에서 응용되고 있다.

이러한 CA의 응용에 관한 연구와 함께 응용분야에 적합한 CA를 모델링하는 연구도 계속적으로 이루어지고 있다. 이는 주어진 특성다항식에 대응하는 CA를 합성하는 것이 LFSR에 비해 어렵기 때문이다. 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[15]에 의해 제안된 합성 방법의 시간복잡도 $O(n^7)$을 $O(n^2)$로 감소시켰다.

Sabata 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[18,19]. Kim 등은 삼항 다항식에 대응하는 90/150 CA의 상태전이행렬 구성에 대하여 연구하였고, Choi 등은 90/150 CA중 그 규칙이 서로 반전이 되어도 특성다항식이 변화가 없는 특별한 CA의 특성다항식의 점화관계를 분석하고, 합성하는 알고리즘을 제안하였다[13,19].

본 논문에서는 효과적인 암호시스템 설계에 있어 중요한 요소 중 하나인 의사난수열 생성기의 효과적 합성에 관하여 다룬다. 먼저 간단한 90/150 전이규칙 블록 $<10\cdots0>$의 특성다항식의 다양한 점화관계를 분석한다. 그리고 규칙블록과 4셀 90/150 전이규칙 블록 $<0100>$을 이용하여 최소무게 다항식 $x^{2^n} + x^{2^n-1} + 1$ $(n \geq 2)$에 대응하는 90/150 RCA의 합성알고리즘을 제안한다. 또한 최소무게 다항식 $x^{2^n} + x^{2^n-1} + 1 (n \geq 2)$

에 대응하는 가역 90/150 CA를 이용하여 2^n차 최대 무게다항식에 대응하는 90/150 가역 CA의 합성알고리즘을 제안한다.

II. CA Preliminaries

CA의 최소 단위인 셀이 선형으로 배열되어 있고, 셀의 다음 상태를 결정할 때 영향을 주는 이웃 셀이 좌우로 r개씩 인 CA를 1차원 r-이웃 CA라 한다. 1차원 r-이웃 CA의 상태전이 함수는 부울함수로 식 (1)과 같다.

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

여기서 $s_i^t (\in \{0,1\})$는 시간 t에서 i번째 셀의 상태를 나타낸다. 본 논문에서 다루는 90/150 CA는 가장 간단한 1차원 3-이웃 CA이며 간단히 CA라 한다. 각 셀에 적용되는 상태전이 함수가 XOR로 표현되는 규칙을 선형규칙이라고 하며 CA의 모든 셀에 적용된 전이규칙이 선형규칙일 때, 선형 CA라 한다. 그림 1은 Wolfram의 표기법으로 전이규칙 30과 150을 묘사한 것이다. 1차원 3-이웃 CA 전이규칙은 $2^{2^3} = 256$가지이며, 다음 상태의 값을 이진수로 하며 십진수로 표현한 것이 전이규칙 번호이다.

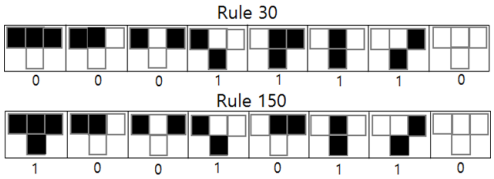

그림 1. Wolfram의 표기에서 묘사된 규칙 30과 150
Fig. 1 Rule 30 and 150 depicted in Wolfram's notation

표 1은 본 논문에서 사용되는 전이 규칙 90과 150에 대한 부울식이다. 전이규칙 90은 왼쪽 셀과 오른쪽 셀의 영향을 받아 다음 셀이 결정되고, 전이규칙 150은 왼쪽 셀과 셀 자신, 오른쪽 셀의 영향을 받아 다음 셀이 결정되는 선형규칙이다. 그러므로 n셀 90/150 CA의 상태전이행렬은 식 (2)와 같다.

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

여기서 CA의 i번째 셀에 적용되는 전이규칙이 90이면 $d_i = 0$, 150이면 $d_i = 1$이며 (2)는 간단히 $T_n = < d_1 d_2 \cdots d_n >$로 간단히 나타낸다. T_n의 행렬식 $\det(T_n)$이 1일 때 T_n은 가역행렬이며, 가역행렬에 대응하는 CA는 가역 CA(reversible CA, RCA)는 암호시스템에서 키수열 생성기로 많이 응용된다.

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 2는 $T_4 = < 0100 >$인 90/150 CA의 구조와 상태전이행렬 T와 T의 특성다항식이다. n-셀 90/150 CA의 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 $x^4 + x^3 + x^2 + x + 1$은 기약다항식이다.

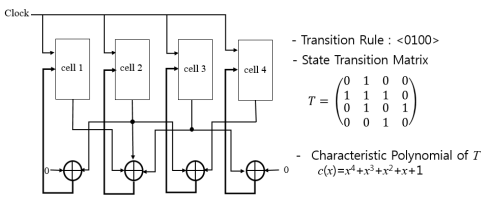

그림 2. 4셀 90/150 CA $< 0100 >$의 구조와 특성다항식
Fig. 2 The structure of 4cell 90/150 CA with rule $< 0100 >$ and the characteristic polynomial

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 삼중 대각행렬이므로 점화관계를 이용하여 효율적으로 계산할 수 있다. Δ_n을 T_n의 특성다항식이라고 하자. 그러면 식 (3)과 같은 점화식이 성립한다[20].

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

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

III. 최대무게 다항식에 대응하는 90/150 RCA

다항식 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 에 대하여 다항식의 무게 $\mathrm{w}(f)$는 계수가 0이 아닌 항의 수이다. 따라서 2차 이상의 기약다항식의 무게 $\mathrm{w}(f)$는 $\mathrm{w}(f) \geq 3$ 이다. 예를 들어 삼항 다항식 $x^{2^n} + x^{2^n-1} + 1$은 최소무게 다항식이며, $x^{2^n} + x^{2^n-1} + \cdots + x + 1$ 는 2^n차 최대 무게 다항식(maximum weight polynomial)이다. 본 논문에서는 $x^{2^n} + x^{2^n-1} + 1$에 대응하는 90/150 RCA를 이용하여 $x^{2^n} + x^{2^n-1} + \cdots + x + 1$ 에 대응하는 90/150 RCA합성 알고리즘을 제안한다.

전이 규칙이 $T_n = < d_1 d_2 \cdots d_n >$ 에 대하여 $T_n^* = < d_n \cdots d_2 d_1 >$ 를 대칭전이규칙(symmetric transition rule)이라 한다[21]. 다음의 성질은 [21,22]의 결과이다.

성질 1. T_n의 특성다항식 Δ_n과 T_n^*의 특성다항식 Δ_n^*에 대하여 $\Delta_n = \Delta_n^*$이다.

성질 2. T_n과 T_n^*의 규칙블록을 이용하여 합성한 $2n$셀 90/150 CA $R_{2n} = < T_{\overline{n}} T_n^* >$의 특성다항식은 Δ_n^2이다. 여기서 $T_{\overline{n}} = < d_1 d_2 \cdots d_{n-1} \overline{d_n} >$이다.

성질 3. $(2n+2)$셀 90/150 CA $R_{2n+2} = < T_n a_1 a_2 T_n^* >$ 의 특성다항식 U_{2n+2}는 식(4)와 같다.

$$U_{2n+2} = D_2 \Delta_n^2 + (a_1 + a_2)\Delta_n \Delta_{n-1} + \Delta_{n-1}^2 \quad (4)$$

여기서 D_2는 $< a_1 a_2 >$의 특성다항식이고, Δ_{n-1}은 $< d_1 d_2 \cdots d_{n-1} >$ 의 특성다항식이다.

본 논문에서 사용하는 규칙블록 $< 10 \cdots 00 >$에 대응하는 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 할 때, $H_k(x)$의 점화관계를 분석하고, 이 결과를 이용하여 삼항 다항식 $x^{2^n} + x^{2^n-1} + 1$에 대응하는 90/150 CA를 합성한다. 정리 1은 식(3)을 이용하여 쉽게 얻을 수 있다.

<정리 1> 전이규칙이 $< 10 \cdots 0 >$인 $k(\geq 2)$셀 90/150 CA의 특성다항식을 $H_k(x)$라 하면 $H_k(x) = xH_{k-1}(x) + H_{k-2}(x)$ 이고, $H_1(x) = x+1$, $H_0(x) = 1$이다.

정리 2와 3은 [19]의 결과이다.

<정리 2> 전이규칙이 $< 10 \cdots 0 >$인 k셀 90/150 CA의 특성다항식을 $H_k(x)$라 하면 $H_{2^n}(x) + H_{2^n-1}(x) = x^{2^n}$이다.

<정리 3> 전이규칙이 $< 100 \cdots 00 >$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.

<정리 4> 전이규칙 $V_k = < 10 \cdots 0 >$, $V_k^* = < 0 \cdots 01 >$와 $D_4 = < 0100 >$를 합성한 2^n셀 90/150 CA $R_{2^n} = < V_k D_4 V_k^* >$의 특성다항식은 $x^{2^n} + x^{2^n-1} + 1$이다. 여기서 $k = 2^{n-1} - 2$이다.

(증명) $R_{2^n} = < V_k D_4 V_k^* >$의 특성다항식을 $h_{2^n}(x)$라 하자. D_4에서 $d_1 = d_4$이므로 $R_{2^n} = < V_{k+1} D_2 V_{k+1}^* >$이다. 여기서 $D_2 = < 10 >$이다. V_k에 대응하는 특성다항식을 $H_k(x)$라 할 때, 성질 3의 식(4)에 의해 $h_{2^n}(x)$은 식(5)와 같다.

$$\begin{aligned} h_{2^n}(x) &= (x^2+x+1)[H_{2^{n-1}-1}(x)]^2 \\ &\quad + H_{2^{n-1}-1}(x)H_{2^{n-1}-2}(x) + [H_{2^{n-1}-2}(x)]^2 \\ &= (xH_{2^{n-1}-1}(x) + H_{2^{n-1}-2}(x))^2 \\ &\quad + H_{2^{n-1}-1}(x)[xH_{2^{n-1}-1}(x) + H_{2^{n-1}-2}(x)] \\ &\quad + [H_{2^{n-1}-1}(x)]^2 \end{aligned} \quad (5)$$

정리 1, 2, 와 정리 3 에 의하여 $h_{2^n}(x)$는 다음을 만족한다.

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

2^n셀 90/150 CA $R_{2^n} = < V_k D_4 V_k^* >$의 특성다항식 $h_{2^n}(x) = x^{2^n} + x^{2^n-1} + 1$에 대한 상반다항식과

$h_{2^n}(x+1)$의 성질을 살펴본다. 먼저 $h_{2^n}(x)$의 상반다항식은 $h^*_{2^n}(x)=x^{2^n}h_{2^n}(1/x)=x^{2^n}+x+1$이다. $h^*_{2^n}(x)$에 대응하는 CA는 $<O_k0101O_k>$이며 $h^*_{2^n}(x+1)=h^*_{2^n}(x)$이다[19]. 다음은 최소무게 다항식인 $h_{2^n}(x)$으로부터 최대무게 다항식의 유도과정이다. $R_{2^n}=<V_kD_4V_k^*>$에 대하여 $<\overline{V_kD_4V_k^*}>$의 특성다항식은 $h_{2^n}(x+1)$이며, $h_{2^n}(x+1)$은 식(6)을 만족한다.

$$h_{2^n}(x+1)=(x+1)^{2^n}+(x+1)^{2^n-1}+1$$
$$=x^{2^n}+x^{2^n-1}+x^{2^n-2}+\cdots+x+1 \quad (6)$$

식 (6)은 2^n차 최대무게다항식이다. 그러므로 R_{2^n}을 이용하여 최대무게다항식을 특성다항식으로 갖는 90/150 RCA를 유도할 수 있다.

표 2. 삼항다항식과 최대무게 다항식에 대응하는 90/150 RCA 합성알고리즘
Table 2. Synthesis algorithm of 90/150 CA corresponding to trinomial and maximum weight polynomial.

[Min_n_Max_weight_Poly_RCA_synthesis_Algorithm]
Input : n $(n>2)$
Output : (1) Rm : 90/150 CA of trinomial
(2) RM : 90/150 CA of maximum weight polynomial

Step1.Compute $k=(2^n-2)/2$.
Step2. Generation of 90/150 CA $V_k=<10\cdots0>$.
Step 3. Generation of 90/150 CA $Rm_{2^n}=<V_k10V_k^*>$ corresponding to $x^{2^n}+x^{2^n-1}+1$, where V_k^* is the symmetric transition rule of V_k.
Step 4 Generation of 90/150 CA $RM_{2^n}=<W_k01W_k^*>$ corresponding to maximum weight polynomial, where $W_k=\overline{V_k}$.

표 2는 삼항 다항식 $h_{2^n}=x^{2^n}+x^{2^n-1}+1$와 최대무게다항식 $f_{2^n}=x^{2^n}+x^{2^n-1}+\cdots+x+1$ 에 대응하는 90/150 RCA합성알고리즘이다.

<정리 5> 2^n셀 90/150 CA $R_{2^n}=<V_kD_4V_k^*>$의 특성다항식 $h_{2^n}(x)$은 n/d가 홀수가 되는 d에 대하여 $2d$차 기약다항식으로 인수분해 되고, $2d$차 기약인수의 개수 $S(d)$는 식(7)과 같다.

$$S(d)=\frac{1}{2d}\sum_{d/r\,:\,odd}\mu(r)2^{d/r} \quad (7)$$

여기서 $\mu(r)$은 뫼비우스 함수로 $r=1$인 경우는 1이며, r이 서로 다른 k개의 소수로 소인수분해 되면 $(-1)^k$이다. 또한 r이 소수의 제곱으로 나누어지는 경우는 0이다.

(증명) $(x+1)h_{2^n}(x+1)=x^{2^n+1}+1$이다.

$f_{2^n}(x):=h_{2^n}(x+1)$ 라 두면, $f_{2^n}(x)\,|\,(x^{2^n+1}+1)\,|\,(x^{2^{2n}-1}+1)$가 성립한다. $f_{2^n}(x)\,|\,(x^{2^{2n}-1}+1)$이므로 $f_{2^n}(x)$는 x를 제외한 $2n$의 약수인 기약다항식들의 곱이다. 또한 $f_{2^n}(x)\,|\,(x^{2^n+1}+1)$이므로 정리 1[23]에 의하여 $f_{2^n}(x)$는 자체 상반다항식인 $2d$차의 기약인수들의 곱이다. 단, n/d는 홀수이다. h_{2^n}에서 f_{2^n}의 변환에 의하여 인수들의 차수는 변하지 않는다[24]. 그러므로 $h_{2^n}(x)$의 모든 기약인수는 $2d$차의 기약인수들의 곱이다. 단, n/d는 홀수이다. 또한 기약인수의 개수도 서로 같다. 따라서 $h_{2^n}(x)$의 기약인수의 개수 $S(d)$는 한 $2d$차 자체상반다항식의 개수와 같다.

표 3. 삼항다항식 $x^{2^n}+x^{2^n-1}+1$의 인수분해
Table 3. Factorization of trinomial $x^{2^n}+x^{2^n-1}+1$

n	irreducible Factors of $x^{2^n}+x^{2^n-1}+1$
3	(6,4,3,1,0)(2,1,0)
4	(8,7,5,4,3,2,0)(8,5,3,2,0)
5	(10,9,5,4,2,1,0)(10,9,8,7,2,1,0)(10,8,7,6,2,1,0)(2,1,0)
6	(12,10,9,6,4,3,0)(12,11,10,8,7,3,0)(12,7,4,3,0)(12,11,8,7,4,3,0)(12,10,7,3,0)(4,3,0)
7	(14,13,9,7,6,4,3,1,0)(14,12,10,9,7,4,3,1,0)(14,13,12,11,10,9,7,5,3,1,0)(14,10,9,7,6,4,3,1,0)(14,12,8,7,6,5,3,1,0)(14,8,7,5,3,1,0)(14,12,11,10,8,7,6,4,3,1,0)(14,13,12,10,8,7,6,5,3,1,0)(14,13,11,8,7,4,3,1,0)(2,1,0)

<예제> $n=9$일 때, $9/d$가 홀수가 되는 d는 1, 3, 9이다. 따라서 $x^{512}+x^{511}+1$의 기약인수는 2차, 6차, 18차 기약다항식이다. 2차 기약다항식의 개수는 $(\mu(2)\cdot 2^{2/2})/2=1$ 이고 6차 기약인수의 개수는 $(\mu(1)\cdot 2^3+\mu(3)\cdot 2^1)/6=(8-2)/6=1$ 이다. 그리고 18차 기약인수의 개수는 $(\mu(1)\cdot 2^9+\mu(3)\cdot 2^3+$

$+\mu(9)\cdot 2^1)/18=28$이다.

표 3은 2^n셀 90/150 CA $R_{2^n}=<V_kD_4V_k^*>$의 특성다항식 $h_{2^n}(x)(3\le n\le 8)$ 의 인수분해 결과이다. 표 3에서 (6,4,3,1,0)은 $x^6+x^4+x^3+x+1$을 나타낸 것이다. 표 4는 $h_{2^n}(x)$의 기약인수의 차수와 해당 차수의 기약인수의 개수를 나타낸다. 표에서 k_i차 인수의 개수가 N_i일 때 $k_i(N_i)$로 나타낸다. 즉, $n=5$일 때, $x^{2^5}+x^{2^5-1}+1$은 2차 기약인수 1개와 10차 기약인수 3개로 인수분해 된다는 의미이다.

표 4. $x^{2^n}+x^{2^n-1}+1$의 인수의 차수와 개수

Table 4. The degree of factors of $x^{2^n}+x^{2^n-1}+1$ and the number of factors

n	$k_i(N_i)$	n	$k_i(N_i)$
3	2(1),6(1)	18	4(1),12(2),36(13797)
4	8(2)	19	2(1),38(13797)
5	2(1),10(3)	20	8(2),40(26214)
6	4(1),12(5)	21	2(1),6(1),14(9),42(49929)
7	2(1),14(9)	22	4(1),44(95325)
8	16(16)	23	2(1),46(182361)
9	2(1),6(1),18(28)	24	16(16),48(349520)
10	4(1),20(51)	25	2(1),10(3),50(671088)
11	2(1),22(93)	26	4(1),52(1290555)
12	8(2),24(170)	27	2(1),6(1),18(28),54(2485504)
13	2(1),26(315)	28	8(2),56(4793490)
14	4(1),28(585)	29	2(1),58(9256395)
15	2(1),6(1),10(3),30(1091)	30	4(1),12(5),20(51),60(17895679)
16	32(2048)	31	2(1),62(34636833)
17	2(1),34(3855)	32	64(67108864)
- k_i : The degree of factors of $h_{2^n}(x)$ - N_i : The number of factors for degree k_i			

Ⅳ. 결론

본 논문에서는 효과적인 암호시스템 설계에 있어 중요한 요소 중 하나인 의사난수열 생성기의 효과적 합성법을 제안하였다. 전이규칙이 $<10\cdots 0>$인 90/150 CA와 최대주기를 갖는 4셀 90/150 CA $<0100>$을 이용하여 최소무게 다항식 중 하나인 삼항다항식 $x^{2^n}+x^{2^n-1}+1\,(n\ge 2)$ 에 대응하는 90/150 RCA를 합성하는 방법과 삼항다항식의 특별한 성질을 이용하여 2^n차 최대무게다항식에 대응하는 90/150 RCA를 합성하는 방법을 제안하고 알고리즘화 하였다. 이러한 결과는 최대무게 다항식을 90/150 CA를 합성하는 연구에 도움이 될 것이며 CA기반의 의사난수열 생성기를 모델링하는데 도움이 될 것으로 사료된다.

References

[1] J. Kim and J. Chon, "Decoding problem of random linear codes and its cryptographic application," *J. of the Korean Institute of Communication Sciences*, vol. 32, no. 6, 2015, pp. 30-38.

[2] 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.

[3] 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.

[4] N. Jang, C. Kim, S. Hong, and Y. Park, "Efficient Bit-Parallel Shifted Polynomial Basis Multipliers for All Irreducible Trinomial," *J. of the Korea Institute of Information Security & Cryptology*, vol. 19, no. 2, 2009, pp.49-61.

[5] S. Wolfram, "Cryptography with Cellular Automata," *in Advances in Cryintology: Crypto '85 Proceedings, Lecture Notes in Computer Science 218*, Springer, 1986, pp. 429-432.

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

[7] S. Nandi, B. Kar, and P. Chaudhuri, "Theory and

Applications of Cellular Automata in Cryptography," *IEEE Trans. on Computers*, vol. 43, no. 12, 1994, pp. 1346-1357.

[8] 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.

[9] M. Tomassini and M. Perrenoud, "Stream Ciphers with One- and Two-Dimensional Cellular Automata," *Parallel Problem Solving from Nature - PPSN VI, Lecture Notes in Computer Science 1917, Springer,* 2000, pp. 722-731.

[10] P. Guan, "Cellular Automaton Public-Key Cryptosystern," *Complex Systems I*, 1987, pp. 51-56.

[11] 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.

[12] 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.

[13] H. Kim, S. Cho, and U. Choi, "On the Construction of the 90/150 State Transition Matrix Corresponding to the Trinomial $x^{2^n-1}+x+1$," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 2, 2017, pp. 383-389.

[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] U. Choi and S. Cho, "Characteristic Polynomial of 90 UCA and Synthesis of CA using Transition Rule Blocks," *J. of the Korea Institute of Electronic Communication Sciences, J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 3, 2018, pp. 593-600.

[20] P. Chaudhuri, D.RChowdhury, S. Nandi and S. Chattopadhyay, *Additive Cellular Automata Theory and Applications.* Los Alamitos, California: IEEE Computer Society Press, 1997.

[21] U. Choi, S. Cho, and G. Kong, "Analysis of Characteristic Polynomial of Cellular Automata with Symmetrical Transition Rules," *Proceedings of the Jangjeon Mathematical Society*, vol. 18, no. 1, 2015, pp. 85-93.

[22] H. Kim, S. Cho, U. Choi, and M. Kwon, "Analysis of 90/150 Cellular Automata with Extended Symmetric Transition Rules." *Proceedings of the Jangjeon Mathematical Society*, vol. 20, no. 2, 2017, pp. 193-201.

[23] 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.

[24] S. Golomb, *Shift Register Sequences.* Los Alamitos, 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