Regular paper | Journal of the KIECS. pp. 333-342, vol. 17, no. 2, Apr. 30. 2022, t. 112, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2022.17.2.333

비대칭 1차원 5-이웃 선형 MLCA의 합성

최언숙*

Synthesis Of Asymmetric One-Dimensional 5-Neighbor Linear MLCA

Un-Sook Choi*

요 약

셀룰라 오토마타(이하 CA)는 이산적이고 추상적인 계산 모델로 다양한 분야에서 적용되고 있다. 우수한 의사 난수열 생성기로 적용 가능한 CA는 최근에 암호 시스템의 기본 요소로 발전했다. CA 기반 스트림 암호에 대한 여러 연구가 수행되었으며 적절한 CA 규칙이 사용되는 경우 CA의 이웃의 반경이 증가될 때, 암호화 강도가 증가됨이 관찰되었다. 본 논문에서는 1차원 의사 난수열 생성기(PRNG)로 응용될 수 있는 CA 중 1차원 5-이웃 CA를 이웃의 연결 상태에 따라 분류하고, 특성다항식의 점화관계를 구한다. 또한 1차원 3-이웃 90/150 CA의 상태 전이행렬을 이용하여 이웃의 반경을 2로 증가시킨 비대칭 5-이웃 선형 MLCA를 합성 알고리즘을 제안한다.

ABSTRACT

Cellular Automata (CA) is a discrete and abstract computational model that is being applied in various fields. Applicable as an excellent pseudo-random sequence generator, CA has recently developed into a basic element of cryptographic systems. Several studies on CA-based stream ciphers have been conducted and it has been observed that the encryption strength increases when the radius of a CA's neighbor is increased when appropriate CA rules are used. In this paper, among CAs that can be applied as a one-dimensional pseudo-random number sequence generator (PRNG), one-dimensional 5-neighbor CAs are classified according to the connection state of their neighbors, and the ignition relationship of the characteristic polynomial is obtained. Also this paper propose a synthesis algorithm for an asymmetric 1-D linear 5-neighbor MLCA in which the radius of the neighbor is increased by 2 using the one-dimensional 3-neighbor 90/150 CA state transition matrix.

키워드

Primitive Polynomial, Asymmetric 5-Neighborhood CA, Cellular Automata, State Transition Matrix, MLCA
원시 다항식, 비대칭 5-이웃 CA, 셀룰라 오토마타, 상태 전이 행렬, MLCA

Ⅰ. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 이론적인 특성과 실제 응용으로 많은 연구자들에 의해 연구되어오고 있다. 특히 가장 간단한 구조로 이루어진 1차원 3-이웃 CA는 작은 단위로 확장 연결이 용이하다. Wolfram은 1차원 3-이웃 CA를 난수 생성에 처음 적용한 후 오류정정부호, 검사패턴 생성, 암호시

* 교신저자 : 동명대학교 AI학부
• 접 수 일 : 2022. 01. 13
• 수정완료일 : 2022. 03. 01
• 게재확정일 : 2022. 04. 17
• Received : Jan. 13, 2022, Revised : Mar. 01, 2022, Accepted : Apr. 17, 2022
• Corresponding Author : Un-Sook Choi
School of Artificial Intelligence, Tongmyong University
Email : choies@tu.ac.kr

스템의 키 스트림 생성기, 이미지 암호 알고리즘 등에 적용되었다[1-5]. CA는 자연에서 일어나는 많은 일들을 더 쉽게 이해할 수 있게 해 주었으며 단순하고 규칙적인 CA의 구조 및 특성은 다양한 분야의 연구자들과 실무자들의 관심을 받기에 충분했다. 지난 20년간 1차원 CA기반의 PRNG가 광범위하게 연구되었다[2,4-7]. 많은 연구자들이 다양한 분야에 적용 가능한 CA를 합성하기 위해 CA 다항식에 대한 연구를 수행하였다. PRNG에 적합한 최대 주기 CA(: Maximum Length CA, 이하 MLCA)에 해당하는 CA 다항식의 연구가 Cattell 등에 의해 처음 연구되었다[6]. 그들은 모든 기약 다항식이 CA 다항식이며, 특히 기약 다항식에 해당하는 두 개의 선형 CA가 있음을 보였다. 그들은 차수가 1600인 원시 다항식에 해당하는 선형 CA가 Maple 프로그램을 사용하여 합성될 수 있다고 주장했다. 여기서 원시 다항식에 해당하는 CA는 MLCA이다. Cho 등은 참고문헌[6]에서 제안한 알고리즘을 개선하기 위해 LT(: Lanczos Tri-diagonalization) 방법을 기반으로 하는 새로운 합성 방법을 제안하였다[7]. 제안된 방법은 기존의 알고리즘의 계산 복잡도인 $O(n^7)$를 $O(n^2)$으로 크게 줄였다. LT기반의 90/150 MLCA 합성 알고리즘을 이용하여 90/150 MLCA를 합성했으며, 원시다항식 $x^{9689}+x^{4187}+x^{2444}+x^{1836}+x^{471}+x^{84}+1$에 대응하는 9689-셀 90/150 MLCA를 합성했다. 주어진 특성다항식에 대응하는 90/150 CA의 합성 방법이 수학적 이론을 바탕으로 광범위하게 연구되었다[8-10].

최근 2차원 CA PRNG가 관심을 받고 있다[4]. 그러나 무작위성은 1차원 CA PRNG보다 나은 것으로 보이지만 설계의 복잡성과 계산 효율성을 고려할 때 어느 것이 낫다고 단정 짓기는 어렵다.

Maiti 등은 5-이웃 CA에 의해 생성된 이진수열의 난수성을 검증하기 위해 24비트 대칭 5-이웃 최대 주기 LHCA를 사용하여 15개의 검사로 구성된 NIST 통계 검증을 수행하였으며 높은 난수성이 있음을 확인하였다[11]. Cho 등은 원시다항식 $f(x)$에 대응하는 대칭 5-이웃 CA를 구하기 위해 Krylov 행렬을 이용하여 합성하였다[12]. Choi 등은 참고문헌[12]에서 제안된 비선형 방법을 개선한 대칭 5-이웃 합성법을 제안하였다[13].

본 논문에서는 1차원 의사 난수열 생성기(PRNG)로 응용될 수 있는 CA 중 1차원 5-이웃 CA를 이웃의 연결 상태에 따라 분류하고, 특성다항식의 점화관계를 구한다. 또한 1차원 3-이웃 90/150 CA의 상태 전이행렬을 이용하여 이웃의 반경을 2로 증가시킨 비대칭 5-이웃 선형 MLCA를 합성법을 제안한다.

II. 1차원 선형 CA

1차원 CA는 기본 CA로 각 셀이 1비트 메모리 요소인 셀의 1차원 셀 스트링으로 구성되며 가장 가까운 이웃 간의 상호작용에 의해 이산 시간 단계에서 상태가 전이된다. 기본 CA는 1차원 3-이웃 CA이다. 집합 N_i를 i번째 셀 c_i의 이웃에 대한 집합이라고 할 때, 기본 CA의 N_i는 $N_i=\{c_{i-1},c_i,c_{i+1}\}$이다. c_i^t를 시간 t에서 기본 CA의 i번째 셀의 상태라 하고, g_i를 i번째 셀의 상태전이 함수라 할 때 다음상태 c_i^{t+1}는 상태는 식 (1)과 같다.

$$c_i^{t+1}=g_i(c_{i-1}^t,c_i^t,c_{i+1}^t) \tag{1}$$

3개의 셀(즉, 주어진 셀과 가장 가까운 이웃)에 대해 총 $2^3(=8)$개의 이진 상태가 있기 때문에 표준 규칙에 따라 0에서 255까지 레이블이 지정된 총 $2^8(=256)$개의 가능한 규칙이 존재한다. g_i가 XOR논리로 표현될 때 g_i를 선형 규칙이라 한다[14]. 주어진 CA의 모든 셀에 적용되는 규칙이 선형 규칙으로만 이루어진 CA를 선형 CA라 한다. 식 (2)는 선형규칙을 부울식으로 나타낸 것이다.

$$c_i^{t+1}=p\cdot c_{i-1}^t\oplus q\cdot c_i^t\oplus r\cdot c_{i+1}^t \tag{2}$$

여기서 $p,q,r\in\{0,1\}$이다. 1차원 선형 3-이웃 CA의 각 셀에 적용할 수 있는 전이규칙의 수는 7개이다. 그림 1은 7개의 선형규칙에 대한 3개의 이웃의 상태에 대해 다음상태 전이를 보여준다. 그림 1에서 규칙 60에 대해 3개의 이웃 상태 $c_{i-1}^t, c_i^t, c_{i+1}^t$가 각각 111, 110, 101, 100, 011, 010, 001, 000에 대해 다음 상태 c_i^{t+1}은 0, 0, 1, 1, 1, 1, 0, 0 이다. 다음 상태 8개 비트를 십진수로 표현하면 규칙 번호인 60(=00111100)이 된다. 선형 CA의 상태전이 함수는 행렬로 나타낼

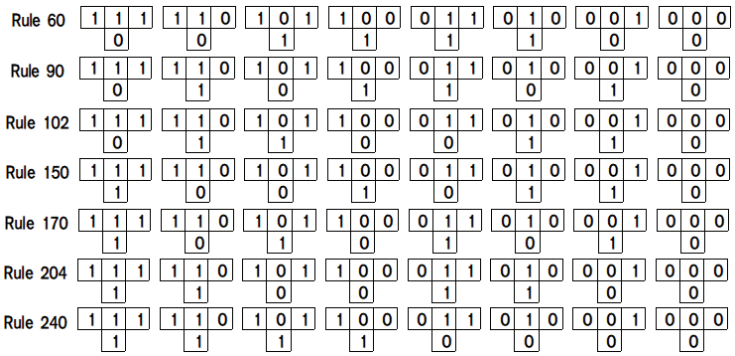

그림 1. 기본 CA의 이웃의 상태에 대한 셀의 다음 상태 전이
Fig. 1 Next state transition of a cell relative to the state of the neighbor of the elementary CA

수 있으며 이 행렬을 상태전이행렬이라고 하면 기본 CA의 상태전이행렬은 삼중 대각행렬로 표현된다. 선형 기본 CA중 각 셀에 적용된 규칙이 규칙 90과 150으로만 이루어진 CA를 90/150 CA라 한다. n개의 셀로 이루어진 90/150 CA의 상태전이행렬 T_n은 식 (3)과 같다.

$$T_n=(t_{ij})_{n\times n}=\begin{cases}d_i\,, i=j\\ 1\ \ , i=j+1 \text{ or } i=j-1\\ 0\ \ , otherwise\end{cases} \tag{3}$$

여기서 $d_i\in\{0,1\}$이고 i번째 셀에 적용된 전이규칙이 90인 경우 $d_i=0$ 이고 전이규칙이 150인 경우 $d_i=1$이다. T_n을 주대각선 성분을 이용하여 간단히 $<d_1d_2\cdots d_n>$로 표현한다.

전이규칙이 $<d_1d_2\cdots d_n>$인 n-셀 90/150 CA의 T_n에 대하여 특성다항식 $|T_n+xI_n|$을 C_n이라 할 때 C_n에 대한 점화식은 식 (4)와 같다. I_n은 n차 단위행렬이다[14].

$$C_n=(x+d_n)C_{n-1}+C_{n-2}\,(n\geq 1) \tag{4}$$

여기서 C_{n-i}은 $<d_1d_2\cdots d_{n-i}>$로 이루어진 부분 90/150 CA의 특성다항식이고, $C_0=1, C_{-1}=0$이다. C_n이 원시다항식일 때 C_n에 대응하는 90/150 CA는 MLCA이다. 예를 들어 $p(x)=x^9+x^6+x^5+x^4+x^2+x+1$는 원시다항식이고 90/150 MLCA합성 알고리즘에 의해 얻어진 T_9은 <011111111> 이다.

90/150 CA는 비밀키 암호 시스템에서 효과적인 PRNG로 응용된다[3,5]. 키공간과 상태 전이의 무작위성을 증가시키기 위해 1차원 CA의 이웃의 반경을 1에서 2로 확장하여 이웃의 수를 3에서 5로 확장시킨다. 이웃의 반경을 넓혀 이웃의 수를 5개 증가시키면 N_i는 $N_i=\{c_{i-2},c_{i-1},c_i,c_{i+1},c_{i+2}\}$이 된다. 이는 2차원 CA의 설계의 복잡성과 분석의 어려움을 해소하면서 각 셀에 적용할 수 있는 전이규칙의 수가 1차원 90/150 CA보다 4배 이상 커지게 됨으로 키 공간의 확장과 무작위성을 높일 수 있다. 1차원 5-이웃 CA의 i번째 셀의 상태전이함수는 식 (5)와 같다.

$$c_i^{t+1}=f_i(c_{i-2}^t,c_{i-1}^t,c_i^t,c_{i+1}^t,c_{i+2}^t) \tag{5}$$

여기서 c_i^t는 시간 t에서의 i번째 셀의 현재 상태, c_i^{t+1}는 시간 $t+1$에서의 i번째 셀의 다음 상태, f_i는 i번째 셀의 조합 논리이다. 1차원 5-이웃 CA의 모든 셀에

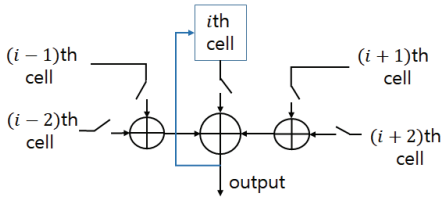

그림 2. 선형 5-이웃 CA의 구조
Fig. 2 Structure of Linear 5-Neighbor CA

적용되는 $f_i(i=1,2,\cdots)$ 가 XOR논리로 표현될 때 주어진 선형 5-이웃 CA이다. 그림 2은 선형 5-이웃 CA의 구조이다. 1차원 선형 5-이웃 CA의 i번째 셀의 시간 $(t+1)$에서의 상태 c_i^{t+1}는 식 (6)과 같다.

$$c_i^{t+1}=pc_{i-2}^t\oplus qc_{i-1}^t\oplus sc_i^t\oplus uc_{i+1}^t\oplus vc_{i+2}^t \quad (6)$$

여기서 $p,q,s,u,v\in\{0,1\}$이다. $n-$셀 1차원 선형 5-이웃 CA의 상태전이함수는 크기가 $n\times n$인 5중 대각행렬 M으로 표현할 수 있으며 특성다항식은 $g(x)=\det(M-xI)$ 이다. 식 (6)에서 $s=r_i$, $p=v=0, q=u=1$이면 3-이웃 90/150이다.

III. 비대칭 1차원 선형 5-이웃 CA

3.1 1차원 선형 5-이웃 CA의 분류와 특성다항식의 점화관계

1차원 3-이웃 CA의 효과적 합성을 위해 전이규칙을 90과 150으로 제한한 것과 같이 선형 5-이웃 CA의 효과적 합성을 위해 이웃의 의존도를 몇 가지로 제한한다. 이때 셀의 상태전이를 위해 참여하는 이웃의 수를 3-이웃 90/150 CA보다는 크거나 같게 둔다. 표 1은 선형 5-이웃 CA의 이웃의 의존도에 따른 분류와 셀의 수에 따른 MLCA의 수이다. 표 1에서 유형 II는 90/150 CA이다.

전이규칙이 $<r_1,r_2,r_3,\cdots,r_n>$인 n-셀 선형 5-이웃 CA의 특성다항식 $g(x)$를 Γ_n라 하고 Γ_i를 $<r_1,r_2,r_3,\cdots,r_i>$까지 부분 선형 5-이웃 CA의 특성다항식이라고 하자.

유형 II의 선형 5-이웃 CA $\mathbb{F}_n$는 90/150 CA이므로 특성다항식 Γ_n은 $\Gamma_n=(x+u_n)\Gamma_{n-1}+\Gamma_{n-2}$ 이다.

유형 III의 선형 5-이웃 CA는 대칭 1차원 5-이웃 CA로 상태전이행렬 $M_n=(v_{i,j})_{n\times n}$은 식 (7)과 같다.

$$v_{ij}=\begin{cases}u_i, & i=j\\ 1, & |i-j|=1\text{ or }2\\ 0, & o/w\end{cases} \quad (7)$$

n-셀 대칭 1차원 5-이웃 CA의 특성다항식의 점화관계는 식 (8)과 같다[13,15].

$$\Gamma_n=(x+u_n)\Gamma_{n-1}+\Gamma_{n-2}+(x+u_{n-1})\Gamma_{n-3}+\Gamma_{n-4}\ (n\geq 1) \quad (8)$$

단, $\Gamma_{-3}=\Gamma_{-2}=\Gamma_{-1}=0$,$\Gamma_0=1$ 이다.

본 논문에서는 9가지 유형 중 유형 IV, V의 의존도를 가지는 비대칭 1차원 선형 5-이웃 CA에 대해 다룬다. 먼저 특성다항식 점화 관계를 유도하고 3-이웃 90/150 MLCA의 상태전이행렬 T_n을 이용하여 유형 IV, V의 n-셀 비대칭 1차원 선형 5-이웃 CA $\mathbb{A}_n$합성법을 제안한다. 유형 IV와 유형 V의 의존도를 가지는 n-셀 CA는 사실상 서로 구조가 같다. 즉 동형사상이다. 상태전이행렬 $M_n=(a_{i,j})_{n\times n}$은 식 (9)와 같고, M_n을 간단히 $<r_1,r_2,r_3,\cdots,r_n>$라 나타낸다.

$$a_{ij}=\begin{cases}r_i, & i=j\\ 1, & j=i+2\text{ or }j=i\pm 1\\ 0, & o/w\end{cases} \quad (9)$$

전이규칙이 $<r_1,r_2,r_3,\cdots,r_n>$이고, 이웃 의존도가 유형 IV인 n-셀 비대칭 1차원 5-이웃 CA $\mathbb{A}_n$의 특성다항식을 구해보자.

먼저 $n=1$일 때, $\Gamma_1=x+r_1$ 이다. $n=2$일 때, $\Gamma_2=(x+r_2)(x+r_1)+1$이므로 $\Gamma_0=1,\Gamma_{-1}=0$라 두면 $\Gamma_2=(x+r_2)\Gamma_1+\Gamma_0+\Gamma_{-1}$이다. 같은 방법으로 $\Gamma_3,\Gamma_4,\cdots$ 를 정리하면 식 (10)을 만족한다.

$$\begin{aligned}\Gamma_3&=(x+r_3)\Gamma_2+(x+r_1)+1\\&=(x+r_3)\Gamma_2+\Gamma_1+\Gamma_0\\\Gamma_4&=(x+r_4)\Gamma_3+\Gamma_2+\Gamma_1\\&\vdots\\\Gamma_n&=(x+r_n)\Gamma_{n-1}+\Gamma_{n-2}+\Gamma_{n-3}\\&(n\geq 3,\Gamma_0=1,\Gamma_{-1}=0)\end{aligned} \quad (10)$$

3.2 비대칭 1차원 선형 5-이웃 CA 합성법

주어진 원시다항식을 특성다항식으로 갖는 비대칭 1차원 선형 5-이웃 CA $\mathbb{A}$를 찾기 위해서 가장 간단한 방법은 전수조사이다.

표 1. 1차원 선형 5-이웃 CA의 이웃에 따른 분류와 최대길이 CA의 개수
Table 1. Number of n-cell one-dimensional linear five-neighbor MLCAs

Type	(p,q,s,u,v)	Number of n-cell one-dimensional linear five-neighbor MLCAs			
		$n=9$	$n=10$	$n=11$	$n=12$
Ⅰ	$(1,0,*,0,1)$	-	-	-	-
Ⅱ	$(0,1,*,1,0)$	96	120	352	288
Ⅲ	$(1,1,*,1,1)$	52	66	188	174
Ⅳ	$(0,1,*,1,1)$	57	106	242	206
Ⅴ	$(1,1,*,1,0)$	57	106	242	206
Ⅵ	$(1,0,*,1,1)$	49	46	160	102
Ⅶ	$(1,1,*,0,1)$	49	46	160	102
Ⅷ	$(1,0,*,1,0)$	101	88	160	210
Ⅸ	$(0,1,*,0,1)$	101	88	160	210

그러나 이 방법은 복잡도가 $O(2^n)$이므로 암호화에 사용되기 위해 셀의 크기가 큰 MLCA를 합성하기 위해 많은 시간이 소요된다. 따라서 3-이웃 90/150 MLCA를 합성하는 방법은 $O(n^2)$이므로 LT기반의 90/150 MLCA 합성 알고리즘을 이용하여 상태전이행렬 T를 구한 후 이를 이용하여 MLCA $\mathbb{A}$를 합성한다. 표 2는 원시다항식 $g(x)$에 대응하는 90/150 MLCA를 합성하는 알고리즘이다[7].

정사각행렬 C,D에 대하여 $D=P^{-1}CP$를 만족하는 가역행렬 P가 존재할 때 D는 C와 닮은 행렬(similar matrix)이라고 한다. 두 행렬이 닮은 행렬일 때, 두 행렬의 특성다항식은 동일하다[16].

표 2. 90/150 MLCA 합성알고리즘
Table 2. Synthesis algorithm of 90/150 MLCA

Input: Primitive Polynomial
$g(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+1$
Output: 90/150 CA $<d_1,d_2,\cdots,d_n>$

Step 1: Make the matrix B from
$x^{i-1}+x^{2i-1}+x^{2i} \bmod g(x)\ (i=1,2,\cdots,n)$
Step 2 : Solve the equation $Bv=(0,0,\cdots,0,1)^t$
Step 3: Construct a Krylov matrix $H=K(C^t,v)$
by the seed vector v, which is a solution
of the equation in Step 2.
Step 4: Compute the LU factorization $H=LU$
Step 5: : Compute CA for f(x) by the matrix U
using $d_1=a_1,\ d_i=a_{i-1}\oplus a_i (i=2,3,\cdots,n-1),\ d_n=a_{n-1}\oplus c_{n-1}$.

원시다항식이 $g(x)$에 대응하는 90/150 CA의 상태전이행렬 T는 특성다항식이 $g(x)$인 $\mathbb{A}$의 상태전이행렬 M는 T와 닮은 대칭행렬이므로 $MQ=QT$가 성립하는 Q가 존재한다. Q에 대하여 방정식 $MQ=QT$을 이용하여 $\mathbb{A}$에 대응하는 M을 구한다.

$Q=[\boldsymbol{q_1},\boldsymbol{q_2},\cdots,\boldsymbol{q_n}]$ ($\boldsymbol{q_i}$는 Q의 i번째 열벡터)라 하면

$$MQ=M[\boldsymbol{q_1},\boldsymbol{q_2},\cdots,\boldsymbol{q_n}]=[M\boldsymbol{q_1},M\boldsymbol{q_2},\cdots,M\boldsymbol{q_n}]$$

이고

$$T=\begin{pmatrix} d_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}$$ 일 때,

$QT=[d_1\boldsymbol{q_1}+\boldsymbol{q_2},\ \boldsymbol{q_1}+d_2\boldsymbol{q_2}+\boldsymbol{q_3},\ \boldsymbol{q_2}+d_3\boldsymbol{q_3}+\boldsymbol{q_4},\cdots,\boldsymbol{q_{n-1}}+d_n\boldsymbol{q_n}]$ 이다.

$MQ=QT$의 각 식을 정리하면 식 (11)과 같다.

$$\begin{cases}(M+d_1I_n)\,\mathbf{q_1}=\mathbf{q1}\\(M+d_2I_n)\,\mathbf{q_2}=\mathbf{q_1}+\mathbf{q_3}\\(M+d_3I_n)\,\mathbf{q_3}=\mathbf{q_2}+\mathbf{q_4}\\\vdots\\(M+d_{n-1}I_n)\,\mathbf{q_{n-1}}=\mathbf{q_{n-2}}+\mathbf{q_n}\\(M+d_nI_n)\,\mathbf{q_n}=\mathbf{q_{n-1}}\end{cases} \quad (11)$$

식 (11)의 M이 $< r_1, r_2, r_3, \cdots, r_{n-1}, r_n >$ 이면 Q를 구하기 위한 행렬 방정식은 $A\mathbf{V_Q}=\boldsymbol{O}$ 이다. 이때 A는 다음과 같은 블록행렬이다.

$$A=\begin{pmatrix}T+r_1I & I & I & O & \cdots & O & O & O\\ I & T+r_2I & I & I & \cdots & O & O & O\\ O & I & T+r_3I & I & \cdots & O & O & O\\ O & O & I & T+r_4I & \cdots & O & O & O\\ O & O & O & I & \cdots & O & O & O\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ O & O & O & O & \cdots & T+r_{n-2}I & I & I\\ O & O & O & O & \cdots & I & T+r_{n-1}I & I\\ O & O & O & O & \cdots & O & I & T+r_nI\end{pmatrix}$$

여기서 $V_Q:=\begin{bmatrix}q_1\\q_2\\\vdots\\q_n\end{bmatrix}, O:=\begin{bmatrix}0\\0\\\vdots\\0\end{bmatrix}$ 이다.

$A\mathbf{V_Q}=\boldsymbol{O}$ 가 자명하지 않은 해 V_Q 를 가져야 하므로 $\det(A)=0$ 이어야 하며, 주어진 T에 대한 A의 식 (12)의 A_E와 같은 행사다리꼴로 변형할 수 있다.

$$A_E=\begin{pmatrix}I & T+r_2I & I & I & \cdots & O & O\\ O & I & T+r_3I & I & \cdots & O & O\\ O & O & I & T+r_4I & \cdots & O & O\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ O & O & O & O & \cdots & I & T+r_nI\\ O & O & O & O & \cdots & O & \Gamma_n(T)\end{pmatrix} \quad (12)$$

여기서 Γ_n은 $\mathbb{A}$의 특성다항식이고 $\mathbb{A}$의 M과 T는 닮음이므로 $\Gamma_n(T)=O$이다.

<예제> 원시다항식 $g(x)=x^5+x^4+x^3+x+1$을 특성다항식으로 가지는 90/150 CA는 표 2의 알고리즘에 의해 T=<00111>이다. $A\mathbf{V_Q}=\boldsymbol{O}$ 에서 A는

$$A=\begin{pmatrix}T+r_1 & I & I & O & O\\ I & T+r_2I & I & I & O\\ O & I & T+r_3I & I & I\\ O & O & I & T+r_4I & I\\ O & O & O & I & T+r_5I\end{pmatrix} \quad (13)$$

이고, A의 $A_E=(\mathbf{a_{ij}})_{n\times n}$에 대하여 $\mathbf{a_{5,5}}=\Gamma_5(T)$ 이며 $\Gamma_5(T)=O$이 되어야 한다. 이를 만족하는 M은 $<01100>, <00110>, <10001>$ 이다. 90/150 CA는 하나의 원시다항식에 대해 대응하는 전이규칙이 2개 존재하나, 비대칭 5-이웃 선형 CA는 2개 이상 존재할 수 있음을 알 수 있다. 따라서 더 많은 MLCA를 합성할 수 있으므로 비대칭 5-이웃 선형 CA를 PRNG로 응용할 때 더 넓은 키공간을 확보할 수 있음을 의미한다.

표 3. 비대칭 1차원 선형 5-이웃 MLCA의 합성 알고리즘
Table 3. Synthesis algorithm for an asymmetric 1-D linear 5-neighbor MLCA

Input : primitive polynomial $g(x)=x^n+\sum_{i=1}^{n-1}c_ix^i+1$ Output : $\mathbb{A}=<r_1r_2\cdots r_n>$
Step 1. Using the algorithm of Table 1, find the $T=<d_1d_2d_3\cdots d_n>$ of the 90/150 CA corresponding to $g(x)$.
Step 2. Take $R=\langle u_1u_2\cdots u_n\rangle$ such that $\lvert R\rvert=1$, $\lvert R+I\rvert=1$ and $Tr(R)=\sum_{i=1}^{n}u_i=c_{n-1}$.
Step 3. Construct A with T and R
Step 4. Construct A_E
Step 5. Find rank $r(A_B)$ of A_E
Step 6. If $r(A_B)=n(n-1)$ Stop and $\mathbb{A}\leftarrow R$ else GoTo Step 2.

표 3은 비대칭 1차원 선형 5-이웃 MLCA $\mathbb{A}$의 합성 알고리즘이다. 표 4는 제안된 알고리즘을 이용하여 다양한 크기의 비대칭 1차원 선형 5-이웃 MLCA를 구한 결과이다. 표 4에서 deg.는 다항식의 차수이자 CA의 셀의 수를 나타내며, 9차 원시다항식 9,8,4,3,2,1,0은 $x^9+x^8+x^4+x^3+x^2+x+1$을 의미한다.

표 4. 주어진 원시다항식에 대응하는 90/150 MLCA와 비대칭 1차원 5-이웃 MLCA
Table 4. A 90/150 MLCA and a asymmetric 5-neighbor linear MLCA corresponding to a given primitive polynomial

deg.	Primitive Polynomial	90/150 MLCA T	Asymmetric 1D 5-neighbor linear MLCA $\mathbb{A}$
9	9, 8, 4, 3, 2, 1, 0	<111010001>	<101011010>
10	10, 8, 7, 6, 5, 4, 3, 1, 0	<0000001111>	<0000110011>
16	16, 13, 11, 6, 5, 4, 3, 1, 0	<0000101010100101>	<0100000101100101>
24	24, 23, 20, 19, 17, 12, 8, 3, 0	<000010101010010100000000>	<000101101100001001111010>
32	32, 30, 24, 21, 20, 14, 13, 6, 4, 3, 2, 1, 0	<01110010010101101110011011111110>	<11111011010111100111000101101001>
40	40, 39, 38, 36, 29, 26, 22, 17, 14, 12, 10, 9, 4, 3, 0	<1010001011000110110000100000100001000100>	<0000100111000110111110101011010011000111>
64	64, 63, 61, 58, 57, 55, 51, 49, 46, 45, 43, 42, 39, 37, 36, 33, 31, 28, 27, 25, 23, 22, 21, 19, 18, 17, 15, 12, 10, 8, 7, 6, 4, 3, 0	<100111111111111110011100010111011010110100010010000110101000011100>	<100001001010110000001100001011011111101100000000000000000000000000>
80	80, 77, 76, 75, 73, 72, 71, 68, 67, 64, 61, 60, 59, 58, 57, 54, 51, 48, 47, 46, 43, 39, 38, 36, 35, 34, 33, 31, 27, 24, 22, 18, 17, 16, 14, 13, 11, 9, 8, 7, 6, 4, 2, 1, 0	<11010111011111010011011001000011110010110100000000111001010101011111110100100110010>	<11100111001011100001110000111101011100000000000000000000000000000000000000000000>
100	100, 99, 96, 94, 90, 89, 88, 87, 86, 84, 81, 80, 76, 75, 73, 69, 63, 58, 57, 55, 53, 51, 49, 46, 45, 43, 40, 39, 37, 31, 27, 24, 23, 21, 16, 14, 13, 11, 10, 4, 2, 1, 0	<1000111011010010001111010111110101110000110100100000111010100111001000001101100100100111001110011011>	<0110000101100001110011011100101110010010000000000000000000000000000000000000000000000000000000000000>
128	128, 125, 123, 122, 120, 119, 118, 115, 113, 109, 107, 106, 105, 103, 102, 101, 100, 95, 92, 87, 82, 81, 78, 77, 75, 74, 72, 70, 69, 68, 65, 62, 61, 60, 58, 56, 53, 51, 45, 44, 42, 41, 40, 38, 36, 33, 32, 31, 29, 26, 25, 24, 22, 21, 20, 19, 18, 17, 15, 14, 12, 9, 8, 4, 3, 2, 0	<0110100000000000111111010010011010100101000111011110001111000001010001000000110111001011000000000111011110001010100100011111010111>	<11001011101101010000011001000100011110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000>
160	160, 158, 157, 154, 153, 150, 148, 147, 146, 141, 140, 139, 138, 129, 128, 125, 121, 119, 116, 111, 110, 108, 107, 106, 103, 102, 100, 99, 98, 96, 94, 92, 85, 81, 80, 79, 77, 75, 74, 73, 72, 71, 70, 68, 67, 65, 63, 62, 57, 56, 54, 53, 51, 50, 49, 46, 45, 44, 40, 37, 36, 33, 30, 29, 28, 23, 22, 21, 19, 18, 17, 15, 14, 7, 6, 5, 3, 2, 0	<1000111100110100011101010100111111101101111101011101100110110100111110000010111111000011011100001011101101010101001010101100001010000000001110000110011101011010 0>	<1111100011001000011111111010010011101011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000>
200	200, 199, 195, 192, 190, 189, 187, 186, 185, 183, 182, 179, 176, 175, 174, 173, 170, 169, 168, 164, 163, 161, 159, 157, 155, 154, 152, 150, 147, 146, 145, 144, 143, 142, 141, 140, 138, 137, 136, 135, 134, 129, 127, 126, 121, 120, 117, 116, 115, 114, 113, 112, 110, 109, 106, 105, 100, 98, 93, 92, 91, 90, 87, 85, 82, 78, 76, 74, 72, 69, 67, 66, 65, 62, 61, 59, 58, 57, 55, 54, 53, 52, 51, 45, 43, 41, 37, 36, 33, 31, 28, 24, 22, 20, 17, 15, 14, 12, 10, 4, 0	<110000101000011000101010000101101000010010111010100011000111101011001010101100110101100101010111010011010100101011101011111011111111111101000101000001111111110000001000001101011001011010111010101000101>	<010101100000100000001001010010101101001100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000>

IV. 결론

본 논문에서는 2차원 CA와 같은 무작위성의 수준을 가지며 설계의 복잡성을 줄일 수 있는 1차원 선형 5-이웃 CA를 이웃의 연결 상태에 따라 분류하고 이웃의 의존관계가 비대칭인 유형 IV와 V인 경우에 대하여 CA의 전이 행동 분석에 핵심이 될 수 있는 특성다항식의 점화관계를 구하였다. 이는 특성다항식을 계산 할 수 있는 시간 복잡도를 효과적으로 줄였다. 또한 90/150 MLCA의 합성알고리즘을 기반으로 하여 주어진 원시다항식에 대응하는 5-이웃 MLCA를 합성할 수 있는 알고리즘을 제안하였다. 향후 이웃의 의존관계에 따라 분류된 다양한 5-이웃 CA 중 유형 I, VI, VII, VIII, IX의 특성을 분석하고 합성하는 방법에 대해 연구하고자 한다.

본 논문은 2021년 한국전자통신학회 추계 학술대회 우수논문으로 선정된 "1차원 5-이웃 선형 셀룰라 오토마타의 특성"을 수정 및 확장한 것이며 이 연구는 Tongmyeong University Research Grants 2021(2021A025)의 지원에 의한 것임.

References

[1] S. Wolfram, "Theory and Applications of Cellular Automata," *IEEE Transactions on Computers,* vol. 43, no. 12, Jan. 1995, pp. 1346-1357

[2] M. Matsumoto, "Simple cellular automata as pseudorandom m-sequence generators for built-in self-test," *ACM Trans. Model. Comput. Simul.* vol. 8, no. 1, 1998, pp. 31-42.

[3] H. Jeong, S. Cho, and S. Kim, "Medical image encryption based on C-MLCA and 1D CAT," *J. of the Korea Institute of Electronic Communication Science*s, vol. 14, no. 2, Apr. 2019, pp. 439-446.

[4] M. Tomassini, M. Sipper, and M. Perrenoud, "On the generation of high-quality random numbers by two-dimensional cellular automata," *IEEE Trans. Comput.* vol. 49, no. 10, Oct. 2000, pp. 1146-1151.

[5] S. Roy, J. Karjee, U. Rawat, D. Pratik, and N. Dey, "Symmetric key encryption technique: A cellular automata based approach in wireless sensor networks," *Comput. Sci.*, vol. 78, 2016, pp. 408-414.

[6] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, vol. 19, no. 3, Mar. 1996, pp. 325-335.

[7] 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, Sept. 2007, pp. 1720-1724.

[8] 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.

[9] U. Choi, S. Cho, H. Kim, and M. Kwon, "Analysis of 90/150 CA corresponding to the power of irreducible polynomials," *J. of Cellular Automata,* vol. 14, no. 5-6, 2019, pp. 417-433.

[10] H. Kim, S. Cho, U. Choi, M. Kwon, and G. Kong, "Synthesis of uniform CA and 90/150 hybrid CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, Mar. 2016, pp. 293-302.

[11] S. Maiti and D. Chowdhury, "Study of five-neighborhood linear hybrid cellular automata and their synthesis," *2017 the 3rd Int. Conf. on Mathematics and Computing,* Haldia, India, Jan. 2017, pp. 68-83.

[12] S. Cho, H. Kim, U. Choi, and S. Kang, "Synthesis of Symmetric 1-D 5-neighborhood CA using Krylov Matrix," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 15, no. 6, Dec. 2020, pp.1105-1111.

[13] U. Choi, H. Kim, S. Kang, and S. Cho, "Design of Key Sequence Generators Based on Symmetric 1-D 5-Neighborhood CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 16, no. 3, June 2021, pp. 533-540.

[14] P. Chaudhuri, D. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive cellular automata, Theory and applications, vol. 1.* Los Alamitos: IEEE Computer Society Press, 1997.

[15] U. Choi, S. Cho and S. Kang, "1-D symmetric 5-neighbor MLCA based color image encryption," *2021 IEEE the 6th Int. Conf. on Computer and Communication Systems*, Chengdu, China, Apr. 2021, pp. 1-6.

[16] R. A. Horn and C. R. Johnson, *Matrix Analysis.* Cambridge, Cambridge Univ. Press, 1985.

저자 소개

최언숙(Un-Sook Choi)

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