Regular paper | Journal of the KIECS. pp. 533-540, vol. 16, no. 3, Jun. 30. 2021, t. 107, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2021.16.3.533

대칭 1차원 5-이웃 CA 기반의 키 수열 생성기 설계

최언숙* · 김한두** · 강성원*** · 조성진****

Design of Key Sequence Generators Based on Symmetric 1-D 5-Neighborhood CA

Un-Sook Choi* · Han-Doo Kim** · Sung-Won Kang*** · Sung-Jin Cho****

요 약

시스템의 성능을 평가하기 위하여 1차원 3-이웃 셀룰라 오토마타(Cellular Automata, 이하 CA) 기반의 의사 난수 생성기가 여러 분야에서 많이 응용되고 있다. 보다 더 효과적인 키 수열 생성을 위해 2차원 CA와 1차원 5-이웃 CA가 응용되었으나, 주어진 특성 다항식에 대응하는 대칭 1차원 5-이웃 CA를 설계하는 것은 매우 어려운 문제이다. 이를 해결하기 위해 특성 다항식의 점화식을 이용한 합성 방법, Krylov 행렬을 이용한 합성 방법과 같이 1차원 5-이웃 CA 합성에 관한 연구들이 진행되었다. 그러나 여전히 비선형 방정식을 풀어야 하는 문제점이 있었다. 이러한 문제점을 해결하기 위해, 최근 90/150 CA의 전이 행렬과 블록행렬을 이용한 1차원 5-이웃 CA 합성 방법이 제안되었다. 본 논문에서는 제안된 알고리즘의 이론적인 과정을 상세히 기술하고 그 알고리즘을 이용하여 높은 차수의 원시 다항식에 대응하는 대칭 1차원 5-이웃 CA를 구한다.

ABSTRACT

To evaluate the performance of a system, one-dimensional 3-neighborhood cellular automata(CA) based pseudo-random generators are widely used in many fields. Although two-dimensional CA and one-dimensional 5-neighborhood CA have been applied for more effective key sequence generation, designing symmetric one-dimensional 5-neighborhood CA corresponding to a given primitive polynomial is a very challenging problem. To solve this problem, studies on one-dimensional 5-neighborhood CA synthesis, such as synthesis method using recurrence relation of characteristic polynomials and synthesis method using Krylov matrix, were conducted. However, there was still a problem with solving nonlinear equations. To solve this problem, a symmetric one-dimensional 5-neighborhood CA synthesis method using a transition matrix of 90/150 CA and a block matrix has recently been proposed. In this paper, we detail the theoretical process of the proposed algorithm and use it to obtain symmetric one-dimensional 5-neighborhood CA corresponding to high-order primitive polynomials.

키워드

Cellular Automata, Primitive Polynomial, Synthesis Algorithm, Symmetric 5-neighborhood CA, State Transition Matrix
셀룰라 오토마타, 원시 다항식, 합성 알고리즘, 대칭 5-이웃 CA, 상태 전이 행렬

* 동명대학교 AI학부(choies@tu.ac.kr)
** 교신저자 : 인제대학교 컴퓨터공학부
*** 부경대학교 정보보호학과(jsm2371@hanmail.net)
**** 부경대학교 응용수학과(sjcho@pknu.ac.kr)
· 접 수 일 : 2021. 04. 06
· 수정완료일 : 2021. 05. 12
· 게재확정일 : 2021. 06. 17
· Received : Apr. 06, 2021, Revised : May. 12, 2021, Accepted : Jun. 17, 2021
· Corresponding Author : Han-Doo Kim
Dept. of Computer Engineering, Inje University,
Email : mathkhd@inje.ac.kr

Ⅰ. 서론

3-이웃 90/150 CA는 수십 년간 많은 연구자들이 연구하고 있는 분야이다[1-3]. 주어진 특성 다항식에 대응하는 90/150 CA의 합성 방법이 수학적 이론을 바탕으로 광범위하게 연구되었다[4-10]. 최근 최대 길이 CA는 이미지 암호 시스템에 적용되면서 우수한 의사난수 생성기임이 입증되었다[11,12].

[13]에서는 5-이웃 CA에 의해 생성된 이진수열의 난수성을 검증하기 위해 24비트 대칭 5-이웃 최대 주기 선형 하이브리드 CA를 사용하여 NIST 통계 테스트를 수행하였고 그 결과 5-이웃 CA가 생성하는 이진수열은 높은 난수성이 있음이 확인되었다. 또한 이들은 특성 다항식의 점화식을 이용하여 n-셀 대칭 1차원 5-이웃 CA를 구하는 기본적인 알고리즘을 제안하였다[13]. 그러나 이들이 제안한 방법은 이전 특성 다항식들을 모두 알아야만 대칭 1차원 5-이웃 CA를 구할 수 있기 때문에 비효율적인 방법이다. 이를 개선하기 위해 [5]에서는 행렬의 닮음, Krylov행렬과 90/150 CA를 이용하여 대칭 1차원 5-이웃 CA를 합성하는 알고리즘을 제안하였다. 그러나 이 알고리즘은 비선형 방정식을 풀어야 하는 문제점이 있다.

이러한 문제점을 해결하기 위해 [6]에서는 삼중블록행렬을 이용하여 비선형 문제를 일부 선형화하여 대칭 5-이웃 CA F를 효율적으로 구하는 알고리즘을 제안하였다. 본 논문에서는 [6]에서 제안한 알고리즘의 이론적인 과정을 상세히 기술하고 그 알고리즘을 이용하여 높은 차수의 원시 다항식에 대응하는 n셀 대칭 1차원 5-이웃 CA를 구한다. 특히 [4]에서 제안된 1차원 90/150 CA의 합성 알고리즘을 이용하여 상태 전이 행렬 T를 구하고, 방정식 $FQ=QT$(Q는 직교행렬)를 이용하여 구한 블록행렬의 계수, F와 $F+I$에 대한 조건을 이용하여 대칭 5-이웃 CA인 F를 구하는 과정을 제시한다.

Ⅱ. 배경 지식 및 기존 연구

n개의 셀로 이루어진 CA의 모든 셀에 적용된 전이규칙이 90 또는 150인 경우 이러한 CA를 *90/150 CA*라고 한다. n-셀 3-이웃 90/150 CA의 상태 전이 행렬 $T_n=(t_{ij})_{n\times n}$은 식(1)과 같은 삼중대각행렬이다.

$$t_{ij}=\begin{cases} d_i, & i=j \\ 1, & |i-j|=1 \\ 0, & o/w \end{cases} \tag{1}$$

T_n은 주대각성분을 이용하여 $<d_1\,d_2\,\cdots\,d_n>$로 간단히 나타낸다. 여기서 CA의 i번째 셀에 적용되는 규칙이 90이면 $d_i=0$, 규칙이 150이면 $d_i=1$ 이다. 표 1은 전이규칙 90과 150의 부울식이다.

T_n의 특성 다항식 $\triangle_n(x)$은 $|T_n\oplus xI_n|$이다. 여기서 I_n은 n차 단위행렬이다. n차 기약다항식 $f(x)$에 대하여 $f(x)$가 x^m-1의 인수가 되는 m의 최솟값이 2^n-1일 때 $f(x)$를 *원시 다항식*(primitive polynomial)이라고 한다. 예를 들어 $x^8+x^6+x^5+x^3+1$은 원시 다항식이다. T_n의 특성 다항식 $\triangle_n(x)$가 원시 다항식일 때 T_n에 대응하는 90/150 CA는 최대주기수열을 생성한다.

표 1. 전이규칙 90과 150의 부울식
Table 1. Boolean expressions of transition rule 90 and 150

Rule No.	Boolean Expression
90	$s_i^{t+1}=s_{i-1}^t\oplus s_{i+1}^t$
150	$s_i^{t+1}=s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t$

대칭 1차원 5-이웃 CA의 i번째 셀의 상태전이함수는 식 (2)와 같다.

$$s_i^{t+1}=f_i(s_{i-2}^t,s_{i-1}^t,s_i^t,s_{i+1}^t,s_{i+2}^t) \tag{2}$$

여기서 s_i^t는 시간 t에서의 i번째 셀의 상태, f_i는 i번째 셀의 조합 논리이다. 식(3)은 대칭 1차원 5-이웃 CA의 부울식이다.

$$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus u_i s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t \tag{3}$$

여기서 $u_i\in\{0,1\}$이다.

n-셀 대칭 1차원 5-이웃 CA의 상태 전이 행렬 $F_n=(v_{ij})_{n\times n}$은 식(4)와 같은 오중대각행렬이다.

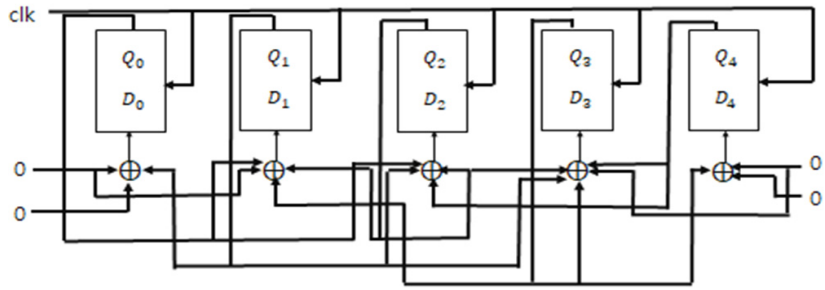

그림 1. 전이규칙이 $<00010>$, 특성 다항식이 $x^5+x^4+x^3+x+1$인 1차원 대칭 5-이웃 CA
Fig. 1 5-neighborhood null boundary CA with transition rule $<00010>$ and characteristic polynomial $x^5+x^4+x^3+x+1$

$$v_{ij}=\begin{cases}u_i, & i=j\\ 1, & |i-j|=1 \text{ or } 2\\ 0, & o/w\end{cases} \tag{4}$$

F_n은 주대각성분을 이용하여 $<u_1\,u_2\cdots\,u_n>$로 간단히 나타낸다[13]. 그림 1은 전이규칙이 <00010>, 특성 다항식이 $x^5+x^4+x^3+x+1$인 1차원 대칭 5-이웃 CA의 구조이다.

n-셀 대칭 1차원 5-이웃 CA의 상태 전이 행렬이 $F_n=<u_1\,u_2\cdots\,u_n>$일 때 F_n의 특성 다항식을 $\Gamma_n(x)$이라 하면

$$\begin{aligned}&\Gamma_1(x)=x+u_1,\ \Gamma_2(x)=(x+u_2)\Gamma_1(x)+1,\\ &\Gamma_3(x)=(x+u_3)\Gamma_2(x)+\Gamma_1(x)+(x+u_2)\Gamma_0(x),\\ &\Gamma_4(x)=(x+u_4)\Gamma_3(x)+\Gamma_2(x)+(x+u_3)\Gamma_1(x)\\ &+\Gamma_0(x).\ (\text{단 } \Gamma_0(x)=1)\\ &\vdots\end{aligned} \tag{5}$$

이므로 $\Gamma_n(x)$은 식(6)과 같다[13].

$$\begin{aligned}&\Gamma_n(x)=(x+u_n)\Gamma_{n-1}(x)+\Gamma_{n-2}(x)\\ &+(x+u_{n-1})\Gamma_{n-3}(x)+\Gamma_{n-4}(x)\ (n\geq 1)\\ &\text{단 } \Gamma_{-3}(x)=\Gamma_{-2}(x)=\Gamma_{-1}(x)=0\end{aligned} \tag{6}$$

III. 대칭 1차원 5-이웃 CA를 구하는 방법

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 특성 다항식은 동일하다[14]. 특성 다항식이 $f(x)$인 n-셀 90/150 CA의 상태 전이 행렬 T가 주어졌을 때 특성 다항식이 $f(x)$인 n-셀 대칭 5-이웃 CA의 상태 전이 행렬 F는 대칭행렬 T와 닮은 대칭행렬이므로 $FQ=QT$가 성립하는 직교행렬 Q가 존재한다. 직교행렬 Q에 대하여 방정식 $FQ=QT$ 을 이용하여 대칭 5-이웃 CA F를 구한다.

$Q=[q_1,q_2,\cdots,q_n]$ (q_i는 Q의 i번째 열벡터)라 하면 $FQ=F[q_1,q_2,\cdots,q_n]=[Fq_1,Fq_2,\cdots,Fq_n]$

이고

$$QT=[q_1,q_2,\cdots,q_n]\begin{bmatrix}t_1 & 1 & 0 & \cdots & 0 & 0 & 0\\ 1 & t_2 & 1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & t_{n-1} & 1\\ 0 & 0 & 0 & \cdots & 0 & 1 & t_n\end{bmatrix}$$

$=[t_1q_1+q_2,\ q_1+t_2q_2+q_3,\ q_2+t_3q_3+q_4,\cdots,q_{n-1}+t_nq_n]$ 이므로 식(7)이 성립한다.

$$\begin{aligned}Fq_1&=t_1q_1+q_2\\ Fq_2&=q_1+t_2q_2+q_3\\ Fq_3&=q_2+t_3q_3+q_4\end{aligned}$$

$$\vdots$$
$$F\boldsymbol{q}_{n-1} = \boldsymbol{q}_{n-2} + t_{n-1}\boldsymbol{q}_{n-1} + \boldsymbol{q}_n$$
$$F\boldsymbol{q}_n = \boldsymbol{q}_{n-1} + t_n\boldsymbol{q}_n \tag{7}$$

이를 식(8)과 같이 나타낼 수 있다.

$$(F + t_1\boldsymbol{I}_n)\boldsymbol{q}_1 = \boldsymbol{q}_2$$
$$(F + t_2\boldsymbol{I}_n)\boldsymbol{q}_2 = \boldsymbol{q}_1 + \boldsymbol{q}_3$$
$$(F + t_3\boldsymbol{I}_n)\boldsymbol{q}_3 = \boldsymbol{q}_2 + \boldsymbol{q}_4$$
$$\vdots$$
$$(F + t_{n-1}\boldsymbol{I}_n)\boldsymbol{q}_{n-1} = \boldsymbol{q}_{n-2} + \boldsymbol{q}_n$$
$$(F + t_n\boldsymbol{I}_n)\boldsymbol{q}_n = \boldsymbol{q}_{n-1} \tag{8}$$

이를 행렬방정식으로 나타내면 식(9)와 같다.

$$B(F)\,V_Q = O \tag{9}$$

단 $B(F) = (B_{ij})_{n\times n}$, $B_{ij} = \begin{cases} F + t_i I_n, & i = j \\ I_n, & |i-j| = 1 \\ O_n, & o/w \end{cases}$,

$$V_Q := \begin{bmatrix} \boldsymbol{q}_1 \\ \boldsymbol{q}_2 \\ \vdots \\ \boldsymbol{q}_n \end{bmatrix}, O := \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{10}$$

식(9)가 자명하지 않은 해 V_Q를 가져야 하므로 $|B(F)| = 0$ 이어야 한다.
주어진 T_n에 대하여 $B(F_n)$의 행사다리꼴 $ref(B(F_n))$은 식(11)과 같다.

$$ref(B(F_n)) = \begin{bmatrix} I & F_n + t_2 I & I & O & \cdots & O & O \\ O & I & F_n + t_3 I & I & \cdots & O & O \\ O & O & I & F_n + t_4 I & \cdots & O & O \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & O & O & \cdots & I & F_n + t_n I \\ O & O & O & O & \cdots & O & \Delta_n(F_n) \end{bmatrix} \tag{11}$$

여기서 $\Delta_n(x)$은 T_n의 특성 다항식이다. 따라서 T_n에 대응하는 F_n에 대하여 $\Delta_n(F_n) = O$이다.

<예제 1> 원시 다항식 $\Delta_5(x) = x^5 + x^4 + x^3 + x + 1$에 대응하는 T_5는 <00111>이므로 $B(F_5)$는 식(12)와 같다.

$$B(F_5) = \begin{bmatrix} F_5 & I & O & O & O \\ I & F_5 & I & O & O \\ O & I & F_5 + I & I & O \\ O & O & I & F_5 + I & I \\ O & O & O & I & F_5 + I \end{bmatrix} \tag{12}$$

블록행렬 $B(F_5)$의 행사다리꼴 $ref(B(F_5))$을 구하면 식(13)과 같다.

$$ref(B(F_5)) = \begin{bmatrix} I & F_5 & I & O & O \\ O & I & F_5 + I & I & O \\ O & O & I & F_5 + I & I \\ O & O & O & I & F_5 + I \\ O & O & O & O & \Delta_5(F_5) \end{bmatrix} \tag{13}$$

$B(F_5)\,V_Q = O$이 자명하지 않은 해를 갖기 위해서는 $\Delta_5(F_5) = O$이 되어야 한다. $F_5 = <00010>$인 경우 $\Delta_5(F_5) = O$이므로 T_5에 대응하는 F_5가 된다.

주어진 기약다항식 $\Delta_n(x) = x^n + \sum_{i=1}^{n-1} c_i x^i + 1$ 에 대하여 $\Delta_n(x+1)$도 기약다항식이 되므로 $|F_n| = |F_n + I| = 1$ 이다. $F_n = < u_1 u_2 \cdots u_n >$을 효율적으로 찾기 위해 $B(F_n)$의 행사다리꼴을 구하기 전에 $|F_n| = |F_n + I| = 1$, $Tr(F_n) = \sum_{i=1}^{n} u_i = c_{n-1}$인 F_n을 선택한다. 표 2는 [6]에서 제안된 주어진 원시 다항식에 대응하는 최대길이를 갖는 대칭 1차원 5-이웃 CA의 전이 행렬의 합성 알고리즘이다.

표 3은 C++프로그램을 이용하여 65차부터 128차까지 주어진 원시 다항식에 대응하는 대칭 1차원 5-이웃 CA F와 상태 전이 행렬 T를 구한 것이다. 표 3의 8차 원시 다항식에서 6, 5, 3은 $x^8 + x^6 + x^5 + x^3 + 1$을 나타낸다.

Ⅳ. 결론

본 논문에서는 [6]에서 제안한 대칭 1차원 5-이웃 CA 합성 알고리즘의 이론적인 과정을 상세히 기술하였고 그 알고리즘을 이용하여 높은 차수의 원시 다항식에 대응하는 대칭 1차원 5-이웃 CA를 구하였다. 제안된 방법은 [4]에서 제안된 1차원 90/150 CA의 합성 알고리즘과 방정식 $FQ=QT$ 로부터 블록행렬을 구성하여 블록행렬의 계수를 구함으로써 기존의 비선형의 문제를 일부 선형의 문제로 변형함으로써 보다 빠르게 대칭 1차원 5-이웃 CA를 합성할 수 있음을 보였다.

본 논문의 연구결과는 랜덤성이 우수한 의사난수열을 생성하는 생성기를 설계하는데 도움이 될 것으로 사료된다. 향후 비대칭 1차원 5-이웃 CA의 합성에 대한 연구를 진행하여 보다 다양한 1차원 5-이웃 CA를 구하고자 한다.

표 2. F의 합성 알고리즘
Table 2. Synthesis algorithm for F

Input : primitive polynomial
$$f(x)=x^n+\sum_{i=1}^{n-1}c_i x^i+1$$
Output : $F=<u_1u_2\cdots u_n>$

Step 1. Using the algorithm of [4], find the $T_n=<t_1t_2t_3\cdots t_n>$ of the 90/150 CA corresponding to $f(x)$.

Step 2. Take $F_n=\langle u_1u_2\cdots u_n\rangle$ such that $|F_n|=1$, $|F_n+I_n|=1$ and $Tr(F_n)=\sum_{i=1}^{n}u_i=c_{n-1}$.

Step 3. Construct $B(F_n)$ with T_n and F_n

Step 4. Construct $ref(B(F_n))$

Step 5. Find rank R of $ref(B(F_n))$

Step 6. If $R=n(n-1)$ Stop
else GoTo Step 2.

표 3. F와 T
Table 3. F and T

deg	primitive polynomial	F	T
8	6,5,3	<00111010>	<00001111>
16	15,13,12,11,10,9,6,4,3,2,1	<0⋯01011>	<1011101111011100>
32	30,27,26,24,22,21,20,19,18,16,15,13,12,9,8,6,5,3,2	<0⋯01111000>	<000000110101100011100001010100 10>
64	63,62,60,59,54,53,52,51,50,49,47,46,44,43,39,36,35,33,32,31,30,29,28,26,23,22,19,17,15,14,12,11,8,6,4	<0⋯01110011>	<1001001101000101011100011001000100011010111100100011001001001110>
65	61,60,59,58,57,53,51,47,45,44,43,40,37,36,35,34,33,32,31,29,26,25,24,19,15,13,12,11,8,5,4,2,1	<0⋯0101000>	<01011011101101101000010101010110100101000111001000001000110001000>
70	68,65,64,63,62,60,57,55,54,52,49,47,46,44,41,40,39,33,31,30,28,22,20,17,16,15,14,12,9,8,7,6,4	<0⋯0101101>	<0110111000100110001010100000001111000111001100011101000110011110101000>
75	74,73,70,68,67,59,58,57,50,45,42,41,40,38,35,34,33,32,29,28,26,24,22,20,19,13,11,8,4,2,1	<0⋯01100111>	<110010111111000101111001000010101101011101001000100010010100010110011111110>
80	80,79,75,74,73,71,70,67,64,62,59,57,55,54,52,51,49,46,45,42,40,37,36,35,30,27,26,23,22,19,15,14,13,11,9,8,7,6,5,4,0	<0⋯011000100>	<10101111010110001100001011000101001101101101100111110100101000110101101011010011>
85	84,83,81,80,78,76,75,71,69,68,67,66,63,62,61,60,58,56,55,51,47,46,45,44,42,37,36,34,32,31,30,29,28,26,24,23,18,17,16,15,13,11,10,7,3	<0⋯01110110>	<1110011010011010000101111111010101000001101010001000110100001110000100010011011011000>
90	89,88,85,82,80,78,76,74,72,71,70,66,64,58,57,56,55,54,53,50,49,48,42,40,37,33,26,25,24,23,22,21,14,12,7,6,5,2,1	<0⋯01010110010>	<0010110000111010110011100001111000000000110111101111011111011111110111000110001010001110 1001>
95	93,89,88,87,82,81,79,77,73,72,71,69,68,65,64,63,61,58,56,53,52,49,48,47,45,41,40,39,34,33,31,29,26,24,21,20,18,16,5,4,2	<0⋯01011100>	<10000010001001010000011110100000111001110001111011011010101110001101100000011001111011101001101>
100	98,96,95,92,91,88,87,85,83,81,78,77,71,69,68,67,64,62,61,57,56,52,46,45,39,37,35,33,30,29,25,24,20,17,16,4,1	<0⋯010111000>	<0100011010100010100100000101101110111001110010101001000001011101000001010011100101010110011111000000>
128	126,123,120,119,112,110,106,105,101,100,96,95,93,92,90,86,83,81,78,73,71,64,63,61,60,58,55,53,52,42,38,35,33,31,29,28,26,22,19,17,14,10,9,7,6,3,1	<0⋯0101010100>	<10110101010001111101000110101100011001011000000110110101000001100111001111100011010001001100100011111101111011111000101100111011>

본 논문은 2019학년도 인제대학교 학술연구조성비 보조에 의한 것임.

References

[1] J. Von Neumann, *Theory of self-reproducing automata.* Urbana and London: University of Illinois Press, 1966.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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, vol. 1, Apr. 2021. pp. 1-6.

[7] 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 Sciences*, vol. 14, no. 2, Apr. 2019, pp. 439-446.

[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] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing,* vol. 164, Nov. 2019, pp. 163-185.

[10] Z. Mehmahad and A. Latif, "A novel image encryption scheme based on reversible cellular automata and chaos," *I. J. Information Technology and Computer Science,* vol. 11, no. 1, Apr. 2019, pp. 15-23.

[11] 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.

[12] 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 Sciences*, vol. 14, no. 2, Apr. 2019, pp. 439-446.

[13] S. Maiti and D. R. Chowdhury, "Study of five-neighborhood linear hybrid cellular automata and their synthesis," ICMC 2017, CCIS 655, Apr. 2017, pp. 68-83.

[14] 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 정보통신 소프트웨어공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

1982년 고려대학교 수학과 졸업(이학사)
1984년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1989년~ 현재 인제대학교 컴퓨터공학부 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

강성원(Sung-Won Kang)

2017년 부경대학교 응용수학과 졸업(이학사)
2019년 부경대학교 대학원 수학과 졸업(이학석사)
2019년~ 현재 부경대학교 대학원 정보보호학과 박사과정 재학
※ 관심분야 : 셀룰라 오토마타론, 정보보호

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