Regular paper | Journal of the KIECS. pp. 1105-1112, vol. 15, no. 6, Dec. 31. 2020, t. 104, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2020.15.6.1105

Krylov 행렬을 이용한 대칭 1차원 5-이웃 CA의 합성

조성진* · 김한두** · 최언숙*** · 강성원****

Synthesis of Symmetric 1-D 5-neighborhood CA using Krylov Matrix

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

요 약

1차원 3-이웃 셀룰라 오토마타(Cellular Automata, 이하 CA) 기반의 의사난수 생성기는 시스템의 성능을 평가하기 위한 테스트 패턴 생성과 암호 시스템의 키수열 생성기 등에 많이 응용되고 있다. 본 논문에서는 더 복잡하고 혼돈스러운 수열을 생성할 수 있는 CA기반의 키 수열 생성기를 설계하기 위해 각 셀의 상태전이에 영향을 주는 이웃을 5개로 확장한 1차원 대칭 5-이웃 CA에 대해 연구한다. 특히 대칭 5-이웃 CA를 합성하기 위해 Krylov 행렬을 이용하는 대수적인 방법과 Cho et al.의 알고리즘을 기반으로 한 1차원 n셀 대칭 5-이웃 CA 합성 알고리즘을 제안한다.

ABSTRACT

One-dimensional 3-neighborhood Cellular Automata (CA)-based pseudo-random number generators are widely applied in generating test patterns to evaluate system performance and generating key sequence generators in cryptographic systems. In this paper, in order to design a CA-based key sequence generator that can generate more complex and confusing sequences, we study a one-dimensional symmetric 5-neighborhood CA that expands to five neighbors affecting the state transition of each cell.

In particular, we propose an n-cell one-dimensional symmetric 5-neighborhood CA synthesis algorithm using the algebraic method that uses the Krylov matrix and the one-dimensional 90/150 CA synthesis algorithm proposed by Cho et al. [6].

키워드

Primitive Polynomial, 5-neighborhood CA, Cellular Automata, State Transition Matrix
원시 다항식, 5-이웃 CA, 셀룰라 오토 마타, 상태 전이 행렬

Ⅰ. 서론

1차원 3-이웃 셀룰러 오토마타(CA)는 그 구조가 간단하면서 작은 단위로 확장 연결이 용이하고, LFSR보다 랜덤성이 우수하여 우수한 의사난수열 생성기로 알려져 있고 오류정정부호, 테스트 패턴 생성, 암호시스템의 키 수열 생성기 등과 같은 여러 분야에 광범위하게 응용되고 있다[1]. 특히 1차원 3-이웃 90/150 CA는

* 부경대학교 응용수학과(sjcho@pknu.ac.kr)
** 교신저자 : 인제대학교 컴퓨터공학부
*** 동명대학교 정보통신공학과(choies@tu.ac.kr)
**** 부경대학교 정보보호학과(jsm2371@hanmail.net)
· 접 수 일 : 2020. 09. 08
· 수정완료일 : 2020. 10. 28
· 게재확정일 : 2020. 12. 15
· Received : Sep. 08, 2020, Revised : Oct. 28, 2020, Accepted : Dec. 15, 2020
· Corresponding Author : Han-Doo Kim
Dept. of Computer Engineering, Inje University,
Email : mathkhd@inje.ac.kr

수십 년간 많은 연구자들이 연구하고 있는 분야이다[2,3]. 주어진 특성다항식에 대응하는 90/150 CA의 합성 방법이 연구되었고, 또한 그 행동이 수학적 이론을 바탕으로 분석되었다[4-7]. 최근 최대 길이 CA는 이미지 암호 시스템에 적용되면서 우수한 PRNG임이 입증되었다[8]. 본 논문에서는 90/150 CA의 확장으로 한 셀이 다음 상태로 전이되는데 영향을 주는 이웃 셀의 개수를 5개로 증가시킨 1차원 5-이웃 선형 CA를 모델링하고 그에 따른 성질들을 분석하고자 한다. 5 이상의 이웃 2차원 CA의 응용분야가 있지만 하드웨어 복잡도가 커진다는 단점이 있다. CA 셀의 인접 반경의 크기에 따라 난수성과 확산 특성이 증가할 수 있다. CA의 확산성이 좋을수록 스트림 암호를 빠르게 초기화할 수 있다[9,10]. 본 논문에서는 높은 확산성을 가지면서 랜덤성이 우수한 의사난수열을 생성할 수 있는 5-이웃 CA를 연구한다. 특성다항식 $f(x)$가 원시다항식일 때 Cho et. al [6]의 알고리즘을 이용하여 대응하는 3-이웃 90/150 CA를 구한 후, $f(x)$에 대응하는 5-이웃 CA를 대수적인 방법을 이용하여 효율적으로 찾는 방법을 제안한다.

II. 배경 지식 및 기존 연구

1980년대 초 Wolfram은 셀이라는 기본 단위 메모리의 배열로 이루어진 1차원 3-이웃 선형 CA를 제안하였다. 배열된 각 셀의 상태는 주어진 CA의 전이규칙에 따라서 이웃하는 두 셀과 자기 자신의 상태에 의존하여 이산시간이 경과 함에 따라 다음 상태로 전이된다. 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 상태전이행렬 T_n는 식 (1)처럼 표현할 수 있다.

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

이때 상태전이행렬 T_n는 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. T_n의 특성다항식 $c_{T_n}(x)$은 $c_{T_n}(x) = |T_n \oplus x I_n|$ 이다. 여기서 I_n은 n차 단위행렬이다. $c_{T_n}(x)$가 원시다항식일 때 T_n에 대응하는 CA는 최대 주기수열을 생성한다.

n차 기약다항식 $f(x)$에 대하여 $f(x)$가 $x^m - 1$의 인수가 되는 m의 최솟값이 $2^n - 1$일 때 $f(x)$를 *원시다항식*(primitive polynomial)이라고 한다. 예를 들어 $x^6 + x^5 + 1$은 원시다항식이다. 표 1은 이 논문에서 사용하는 전이규칙 90과 150의 부울식이다.

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

5-이웃 CA의 i번째 셀의 상태전이함수는 식 (2)와 같다.

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

여기서 s_i^t는 시간 t에서의 i번째 셀의 현재 상태, s_i^{t+1}는 시간 $t+1$에서의 i번째 셀의 다음 상태, f_i는 i번째 셀의 조합 논리이다.

식 (3)은 대칭형 1차원 5-이웃 CA의 부울식이다.

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

여기서 $u_i \in \{0,1\}$이다.

n-셀 5-이웃 CA의 상태전이행렬 F_n은 식 (4)처럼 표현할 수 있다.

$$F_n = \begin{pmatrix} u_1 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & u_2 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & u_3 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & u_{n-1} & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 & u_n \end{pmatrix} \quad (4)$$

이때 상태전이행렬 F_n은 주대각성분을 이용하여 $< u_1\, u_2 \cdots\ u_n >$로 간단히 나타낸다[10].

1차원 n-셀 대칭 5-이웃 CA의 상태전이행렬이 $F_n = < u_1\, u_2 \cdots\ u_n >$일 때 F_n의 특성다항식을 ∇_n이라 하면 식 (5)와 같은 식이 성립한다.

$$\begin{aligned}
&\nabla_1 = x + u_1\,,\ \nabla_2 = (x+u_2)\nabla_1 + 1\,,\\
&\nabla_3 = (x+u_3)\nabla_2 + \nabla_1 + (x+u_2)\nabla_0\,,\\
&\nabla_4 = (x+u_4)\nabla_3 + \nabla_2 + (x+u_3)\nabla_1 + \nabla_0 \qquad (5)\\
&\text{단 } \nabla_0 = 1 \text{ 이다.}
\end{aligned}$$

정리 1은 1차원 n-셀 대칭 5-이웃 CA를 분석하기 위해 필요한 특성다항식을 구하는 점화식이다[10].

<정리 1> 1차원 n-셀 대칭 5-이웃 CA의 상태전이행렬이 $F_n = < u_1\, u_2 \cdots\ u_n >$일 때 F_n의 특성다항식을 ∇_n이라 하면 식 (6)과 같은 점화식이 성립한다.

$$\begin{aligned}
\nabla_n &= (x+u_n)\nabla_{n-1} + \nabla_{n-2} + (x+u_{n-1})\nabla_{n-3}\\
&\quad + \nabla_{n-4}\ (n \geq 1). \qquad (6)\\
&\text{단 } \nabla_{-3} = \nabla_{-2} = \nabla_{-1} = 0, \nabla_0 = 1 \quad \text{이다.}
\end{aligned}$$

Maiti et al. [11]은 1차원 n-셀 5-이웃 CA의 특성다항식 ∇_n이 주어졌을 때 다항식 나눗셈 알고리즘을 이용하여 $\nabla_{n-1}, \nabla_{n-2}, \nabla_{n-3}$이 주어졌다는 전제하에 1차원 n-셀 대칭 5-이웃 CA를 구하는 알고리즘을 제안하였다. Maiti et al. 의 이런 방법은 이전 특성다항식들을 사용해야 하는 비효율적인 방법이므로 이 논문에서는 Krylov 행렬을 이용하는 대수적인 방법과 [6]에서 제안된 1차원 90/150 CA의 합성 알고리즘을 이용하여 1차원 n-셀 대칭 5-이웃 CA를 구하는 효율적인 방법을 제안하고자 한다.

III. 5-이웃 CA를 구하는 방법

정사각행렬 A, B에 대하여 $B = P^{-1}AP$를 만족하는 가역행렬 P가 존재할 때 B는 A와 *닮음*(similar) 행렬이라고 한다. 닮음 행렬의 특성다항식은 같다. 그리고 특성다항식이 동일한 기약다항식인 두 행렬은 닮음 행렬이다[12]. 특성다항식이 $f(x)$인 n-셀 90/150 CA의 상태전이행렬 T가 주어졌을 때 특성다항식이 $f(x)$인 n-셀 5-이웃 CA의 상태전이행렬 F는 T와 닮음 행렬이므로 $FQ = QT$가 성립하는 가역행렬 Q가 존재한다. 직교행렬 Q에 대하여 $FQ = QT$ 를 만족하는 5-이웃 CA에 대응하는 F를 찾고자 한다. 예를 들어 원시다항식 $f(x) = x^4 + x + 1$에 대응하는 3-이웃 90/150 CA에 대응하는 T는 $< 0101 >$이다. 이때 $F = < 0011 >$ 이고 $Q = \begin{bmatrix} 1&1&0&1\\ 0&1&1&1\\ 1&1&1&0\\ 1&0&1&1 \end{bmatrix}$ 는 $Q^TQ = I$를 만족한다. 이 경우 $FQ = QT$가 성립한다.

주어진 n차원 열벡터 $\boldsymbol{x}$와 n차 정사각행렬 M에 대하여

$$K(M, \boldsymbol{x}) = [\boldsymbol{x}, M\boldsymbol{x}, M^2\boldsymbol{x}, \cdots, M^{n-1}\boldsymbol{x}] \qquad (7)$$

를 *Krylov 행렬*(Krylov matrix)이라고 한다[13].

$Q = [\boldsymbol{q_1}, \boldsymbol{q_2}, \cdots, \boldsymbol{q_n}]$ ($\boldsymbol{q_i}$는 Q의 i번째 열벡터)라 하면 $H := K(F, \boldsymbol{q_1})$ 와 $R := K(T, \boldsymbol{e_1})$ 에 대하여 $F^{\boldsymbol{n}}\boldsymbol{q_1}$을 식 (8)과 같이 구할 수 있다. 여기서 $\boldsymbol{e_1} = [1, 0, \cdots, 0]^T$ 이다.

$$\begin{aligned}
&F\boldsymbol{q_1} = (QTQ^T)(Q\boldsymbol{e_1}) = Q(T\boldsymbol{e_1})\\
&F^{\boldsymbol{2}}\boldsymbol{q_1} = F[Q(T\boldsymbol{e_1})] = (QTQ^T)[Q(T\boldsymbol{e_1})] = Q(T^2\boldsymbol{e_1})\\
&F^{\boldsymbol{3}}\boldsymbol{q_1} = F[Q(T^2\boldsymbol{e_1})] = (QTQ^T)[Q(T^{\boldsymbol{2}}\boldsymbol{e_1})] \qquad (8)\\
&= Q(T^3\boldsymbol{e_1})\\
&\qquad\qquad \vdots
\end{aligned}$$

이와 같이 계속하면 식 (9)가 성립한다.

$$\begin{aligned}
H &= [\boldsymbol{q_1}, F\boldsymbol{q_1}, \cdots, F^{n-1}\boldsymbol{q_1}]\\
&= [Q\boldsymbol{e_1}, Q(T\boldsymbol{e_1}), Q(T^2\boldsymbol{e_1}), \cdots, Q(T^{n-1}\boldsymbol{e_1})]\\
&= Q[\boldsymbol{e_1}, T\boldsymbol{e_1}, T^2\boldsymbol{e_1}, \cdots, T^{n-1}\boldsymbol{e_1}] \qquad (9)\\
&= QK(T, \boldsymbol{e_1}) = QR\,.
\end{aligned}$$

따라서 $H = QR$이다.

예제 1> 원시다항식 $f(x)=x^5+x^2+1$ 에 대응하는 3-이웃 90/150 CA에 대응하는 T를 [6]에서 제안된 합성 알고리즘을 이용하여 구하면 $<11110>$이다. $H=QR$ 을 이용하여 $f(x)$에 대응하는 1차원 대칭 5-이웃 CA의 전이행렬 F를 식 (10)과 같이 구한다.

$$H=\left[\boldsymbol{q}_1, F\boldsymbol{q}_1, F^2\boldsymbol{q}_1, F^3\boldsymbol{q}_1, F^4\boldsymbol{q}_1\right] = \left[\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_3, \boldsymbol{q}_4, \boldsymbol{q}_5\right]\begin{bmatrix}1&1&0&0&1\\0&1&0&1&0\\0&0&1&1&1\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix} = QR \tag{10}$$

을 풀면 $(F^4+F^3+F^2+I)\boldsymbol{q}_1=[1,1,1,1,1]^T$이다.
$F=<u_1u_2u_3u_4u_5>$라 두면

$$F^2=\begin{bmatrix}u_1 & u_1+u_2+1 & u_1+u_3+1 & 0 & 1\\ u_1+u_2+1 & u_2+1 & u_2+u_3 & u_2+u_4+1 & 0\\ u_1+u_3+1 & u_2+u_3 & u_3 & u_3+u_4 & u_3+u_5+1\\ 0 & u_2+u_4+1 & u_3+u_4 & u_4+1 & u_4+u_5+1\\ 1 & 0 & u_3+u_5+1 & u_4+u_5+1 & u_5\end{bmatrix} \tag{11}$$

F^3의 1열과 2열은 식 (12)와 같다.

$$\begin{bmatrix}u_1+u_2+u_3\\ u_1u_2+u_3+1\\ u_1u_3+u_2\\ u_2+u_3+1\\ u_1+u_3+u_5+1\end{bmatrix}, \begin{bmatrix}u_1u_2+u_3+1\\ \sum_{i=1}^{4}u_i\\ u_2u_3+\sum_{i=1}^{4}u_i+1\\ u_2u_4+u_3+1\\ u_3+u_4+1\end{bmatrix} \tag{12}$$

또한 F^4의 1열과 2열은 식 (13)과 같다.

$$\begin{bmatrix}u_1+u_2+u_3+1\\ u_1u_2+u_1u_3+u_2u_3+u_1+1\\ u_1u_2+u_1u_3+u_2u_3+u_5+1\\ u_1u_2+u_1u_3+u_2u_4+u_3u_4+u_1+u_2+u_4+u_5\\ u_1u_3+u_1u_5+u_3u_5+u_3+1\end{bmatrix}, \begin{bmatrix}u_1u_2+u_3+1\\ u_1+u_2+u_3+u_4\\ u_2u_3+u_1+u_2+u_3+u_4+1\\ u_2u_3+u_2u_4+u_3u_4+u_3\\ u_2u_3+u_2u_4+u_3u_5+u_4u_5+u_1+u_2+u_4+u_5+1\end{bmatrix} \tag{13}$$

주어진 F에 대하여 $\boldsymbol{q}_1$를 얻기 위해 방정식 $(F^4+F^3+F^2+I)\boldsymbol{q}_1=[1,1,1,1,1]^T$을 풀어야 한다. 방정식의 해가 있으면 주어진 F의 특성다항식 $c_F(x)$을 구한다.

$H=QR$을 만족하는 Q가 $FQ=QT$에 대한 필요충분조건이 아니므로, 구한 $\boldsymbol{q}_1$에 대응하는 F에 대하여 $c_F(x)=f(x)$ 인지 확인해야 한다.
만약, $c_F(x)\neq f(x)$ 이면 또 다른 F에 대하여 위의 과정을 반복한다. 그러므로 $FQ=QT$를 만족하는 $\boldsymbol{q}_1$을 구하는 것이 매우 어렵다. 실제로 위 방법을 통해 해를 구하면 $F=<00011>$이다.

F를 구할 때 조건 $|F|=1$ 과 $|F+I_n|=1$ 을 이용하면 구하는 시간이 짧아진다. 표 2는 주어진 n차 원시다항식 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+1$ 에 대하여 $H=QR$을 이용하여 5-이웃 CA F를 구하는 알고리즘이다.

표 2. 주어진 원시다항식에 대응하는 1차원 5-이웃 CA의 전이행렬 F의 합성 알고리즘
Table 2. Synthesis algorithm for an 1-D 5-neighborhood CA F corresponding to a given primitive polynomial

5-neighborhood 90/150 CA generation method
Step 1. Using the algorithm of [6], find the $T=<t_1t_2t_3\cdots t_n>$ corresponding to the 3-neighborhood 90/150 CA corresponding to to the given $f(x)$.
Step 2. Using T, we get the Krylov matrix $R:=K(T,e_1)$.
Step 3. Take $F=\langle u_1u_2\cdots u_n\rangle$ such that $\lvert F\rvert=1$ and $\lvert F+I_n\rvert=1$. Take F such that $u_1+u_2+\cdots+u_n=1$ (or $u_1+u_2+\cdots+u_n=0$) if the coefficient of the $(n-1)$st term of the polynomial $f(x)$ is 1 (or 0).
Step 4. Using $H=QR$, we get the equation $U:=F^{n-1}+a_{n-2}F^{n-2}+\cdots+a_1F+a_0I_n$, $U\boldsymbol{q}_1=\boldsymbol{E}_n$, where $a_0,a_1,\cdots,a_{n-2}\in\{0,1\}$ and

$\boldsymbol{E_n}=[1,\cdots,1]^T$. Find the solution $\boldsymbol{q_1}$ of the system of equations $U\boldsymbol{q_1}=\boldsymbol{E_n}$. If the sum of the components of the column of $\boldsymbol{q_1}$ is 1, then the characteristic polynomial $c_F(x)$ of F is calculated.

Step 5. If $c_F(x)=f(x)$, then given F is the 5−neighborhood 90/150 CA we want to find. If $c_F(x)\neq f(x)$, go back to step 3 and examine repeatedly until F satisfies $c_F(x)=f(x)$.

표 3은 주어진 알고리즘을 이용하여 Maple 2019를 이용하여 6차부터 10차까지 원시다항식에 대한 1차원 5-이웃 CA F를 구한 것이다. 표 3의 8차 원시다항식에서 3, 5, 6은 $x^8+x^6+x^5+x^3+1$을 나타낸다.

표 3. 주어진 원시다항식에 대응하는 1차원 5-이웃 CA F

Table 3. A 1-D 5-neighborhood CA F corresponding to a given primitive polynomial

F corresponding to a given primitive polynomial		
deg	primitive polynomial	F
6	1,4,5	<000010>
	2,3,5	<001011>
	1,2,5	<010110>
	5	<100101>
7	1	<0010001>
	3	<0000101>
	4	<0000011>
	1,2,5	<0101110>
	1,3,6	<1000101>
	2,4,6	<0001011>
	4,5,6	<0101111>
	1,2,3,4,5	<0010111>
	1,2,3,5,6	<0011111>
	2,3,4,5,6	<0111011>
8	3,5,6	<00111010>
		<01101001>
		<10100011>
9	3,5,6,7,8	<000000100>
	4,5,8	<000011100>
	1,2,3,5,6	<000100010>
	1,2,3,4,5,6,8	<000100011>
	5,6,8	<000110010> <001010010>
	1,2,4,5,7	<000110101>
	3,5,6,7,8	<001000000>
	3,4,5,6,7	<001001011> <001100110>
	1,5,8	<001001100>
	1,3,4,5,8	<001010001>
	2,7,8	<001011011> <100110011>
	⋮	⋮
10	2,3,4,5,6,7,9	<0000001011>
	1,6,9	<0000001101>
	1,2,6,7,8	<0000101011>
	2,3,4,5,8	<0000101101>
	5,7,8	<0000111010> <0011000110>
	2,3,8	<0000111100>
	1,5,6,8,9	<0001100111> <0010101011>
	3,4,5,6,7,8,9	<0001101101>
	5,8,9	<0010001111>
	4,5,8	<0010011100>
	2,3,4,8,9	<0010011110>
	2,3,7,8,9	<0011011100>
	2,3,5	<0011011101>
	2,3,4,5,6,8,9	<0011100110>
	⋮	⋮

Ⅳ. 결론

본 논문에서는 Krylov 행렬을 이용하는 대수적인 방법과 Cho et al. [6]의 알고리즘을 이용하여 n-셀 대칭 1차원 5-이웃 CA를 구하는 효율적인 방법을 연구하였다. 이 알고리즘의 수행시간을 향상시키는 한 방안으로 F를 구하는 시간복잡도를 개선하기 위하여 비선형방정식을 선형방정식으로 바꾸어 방정식의 해를 구하는 방법을 연구할 필요가 있다.

본 논문은 2019학년도 인제대학교 학술연구조성비 보조에 의한 것임.

References

[1] J. V. 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, vol. 1.* Los Alamitos, California: 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] U. Choi and S. Cho, "Analysis of Pseudorandom Sequences Generated by Maximum Length Complemented Cellular Automata," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 5, 2019, pp. 1001-1008.

[5] U. Choi, S. Cho, H. Kim and S. Kang, "Design and Analysis of Pseudorandom Number Generators Based on Programmable Maximum Length CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 15, no. 2, 2020, pp. 319-326.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] J. Jose and D. R. Chowdhury, "Four neighborhood cellular automata as better cryptographic primitives," *IACR Cryptology ePrint Archive 2015*, vol. 700, 2015, pp. 74-82.

[11] S. Maiti and D. R. Chowdhury, "Study of five-neighborhood linear hybrid cellular automata and their synthesis," *International Conference on Mathematics and Computing, vol. 655,* 2017, pp. 68 - 83.

[12] R. A. Horn and C. R. Johnson, M*atrix Analysis.* Cambridge, U. K.: Cambridge Univ. Press, 1985.

[13] M. Serra and T. Slater, "A Lanczos algorithm in a finite field and its application," *J. Comb. Math. Comput., vol. 7,* 1990, pp. 11-32.

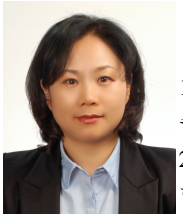
저자 소개

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

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



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

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