Regular paper | Journal of the KIECS. pp. 235-242, vol. 14, no. 1, Feb. 28. 2019, t. 93, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.1.235

90/150 HCA를 이용한 MWCA 판정법

최언숙* · 조성진** · 김한두*** · 김진경** · 강성원**

MWCA Test using 90/150 HCA

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

요 약

유한체 상에서 자기상반다항식은 역방향읽기 성질을 갖는 가역 부호를 설계하는 데 유용하다. 본 논문은 자기상반다항식 중 하나인 최대무게 다항식을 특성다항식으로 갖는 90/150 CA에 관한 연구이다. 전이규칙이 $<100\cdots0>$인 n-셀 90/150 CA를 이용하여 $2n$차 최대무게 다항식에 대응하는 90/150 MWCA가 존재하는지에 대한 판정법을 제안한다. 제안하는 방법은 실험을 통하여 검증한다.

ABSTRACT

Self-reciprocal polynomials over finite fields are useful in several applications, including reversible codes with read-backward properties. This paper is a study on 90/150 CA with characteristic polynomials of maximal weight polynomials, which is one of the self-reciprocal polynomials. In this paper, we propose a decision method for determining the existence of 90/150 MWCA corresponding to the maximum weight polynomial of degree $2n$ using n-cell 90/150 CA with transition rule $<100\cdots0>$. The proposed method is verified through experiments.

키워드

Cellular Automata, Maximum Weight Polynomial, 90/150 MWCA, Characteristic Polynomial, CA-Polynomial
셀룰라 오토마타, 최대무게 다항식, 90/150 MWCA, 특성다항식, CA 다항식

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 물리적, 생물학적 및 계산 시스템을 위해 단순한 결정론적 수학 모델을 제공한다. CA는 간단한 구조임에도 불구하고 복잡한 행동을 할 수 있고, 복잡하고 무작위적인 패턴을 생성할 수 있다. CA는 셀이라는 기본 단위 메모리가 일정한 배열로 이루어지며, 그 상태가 이산시간에서 전이규칙에 따라 상태가 전이되는 동적인 시스템이다. 1차원 3-이웃 CA는 CA중 가장 간단한 구조로, 셀이 선형으로 배열되어 있으며 각 셀의 다음 상태는 자기 자신과 왼쪽과 오른쪽의 인접한 두 셀의 상태에 의해 정해진 규칙에 따라 갱신된다. 이러한 CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다. CA에 대한 연구가 시작된 이래로 암호화를

* 동명대학교 정보통신공학과 (choies@tu.ac.kr)
**부경대학교 응용수학과(sjcho@pknu.ac.kr, 5892587@hanmail.net, jsm2371@hanmail.net)
*** 인제대학교 컴퓨터공학부 (mathkhd@inje.ac.kr)
** 교신저자 : 부경대학교 응용수학과
· 접 수 일 : 2018. 12. 04
· 수정완료일 : 2019. 01. 09
· 게재확정일 : 2019. 02. 15
· Received : Dec. 04, 2018, Revised : Jan. 09, 2019, Accepted : Feb. 15, 2019
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math., Pukyong National University,
Email : sjcho@pknu.ac.kr

위해 CA를 이용하려는 끊임없는 시도가 이루어지고 있다. CA는 Wolfram에 의해 처음 암호시스템에서 응용되었고, 이미지 암호를 위한 기저영상 생성기, 대칭키 암호시스템에서 키수열 생성기 등에 응용되었다[1-5].

Wang 등은 카오스와 가역 CA를 사용하여 보안수준이 높은 이미지 암호 알고리즘을 제안하였다[6]. 또한 Bakhshandeh등은 이미지 변조를 검출할 수 있는 이미지 암호시스템을 카오스 함수와 CA를 사용하여 설계하였다[7]. Ping 등은 가역 CA와 비가역 CA를 모두 이용하여 암호 시스템을 설계하였는데 가역 CA는 혼돈과 확산과정을 위해 사용되었고, 비가역 CA는 의사난수열 생성을 위해 사용되었다. 또한 이들은 보안성을 높이기 위해 비아핀 및 균형규칙을 CA에 적용하였다[8]. Nandi 등은 탄력적이고 안전한 생체인식 시스템을 구축하기 위하여 CA를 기반으로 하는 ECG 해시코드를 설계하였다[9].

선형 CA는 상태전이 함수를 행렬을 이용하여 나타낼 수 있으므로, 주어진 CA의 상태전이 행동에 관하여 수학적으로 분석이 용이하다. 그러나 역으로 원하는 성질을 가지는 CA를 설계하는 것은 매우 어려운 문제이다.

CA기반의 여러 가지 응용에 관한 연구와 함께 응용분야에 적합한 CA를 모델링하는 연구도 계속적으로 이루어지고 있다. 이는 주어진 특성다항식에 대응하는 CA를 합성하는 것이 LFSR(Linear Feedback Shift Register)에 비해 어렵기 때문이다. 그동안 여러 연구자들에 의해 CA 합성에 관한 연구들이 진행되었다[10-16]. Cho 등은 최대 길이 90/150 CA를 갖는 90/150 CA를 합성하는 효율적인 방법을 제안하였다[12]. 이들이 제안한 방법은 Cattell 등에 의해 제안된 합성 방법의 시간복잡도 $O(n^7)$을 $O(n^2)$로 감소시켰다[12, 13].

Sabater 와 Cho 등은 효과적인 키수열을 생성하기 위하여 비선형적인 방법으로 키수열을 생성하는 수축수열 생성기를 CA를 이용하여 모델링하였다[14, 15]. 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 최대무게 다항식 $f_n(x)$의 CA 다항식 여부를 결정하는 방법에 대하여 연구하였고 $f_n(x)$에 대응하는 90/150 CA의 개수를 결정하는 방법을 제안하였다[16]. 또한 90 UCA(uniform CA)와 전이규칙이 $<10\cdots00>$인 90/150 CA의 특성다항식의 점화관계를 분석하여 삼항다항식에 대응하는 CA 합성법을 제안하였다[17, 18]. 그리고 삼항다항식 $x^{2^n}+x^{2^n-1}+1(n \geq 2)$에 대응하는 90/150 HCA를 이용하여 2^n차 최대무게 다항식에 대응하는 90/150 CA를 합성하는 알고리즘을 제안하였다[19].

본 논문은 양방향으로 읽기가 가능한 부호를 설계하는데 적용되는 자기상반다항식 중 하나인 최대무게 다항식을 특성다항식으로 갖는 90/150 CA에 관한 연구이다. 전이규칙이 <100…0>인 n-셀 90/150 HCA(Hybrid CA)를 이용하여 $2n$차 최대무게 다항식에 대응하는 90/150 MWCA가 존재하는지에 대한 판정법을 제안한다. 제안한 알고리즘을 이용하여 최대무게 다항식에 대응하는 90/150 MWCA의 존재에 대해 판정을 내리고 실제 존재하는 경우에 대하여 90/150 MWCA를 합성한다.

II. CA Preliminaries

CA의 다음 상태는 각 셀에 적용되는 전이 함수에 의해 결정된다. CA 중 가장 간단한 구조를 갖는 1차원 3-이웃 CA의 각 셀의 상태전이 함수는 식 1과 같다.

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

여기서 s_i^t는 시간 t에서 i번째 셀의 상태를 나타낸다. $f_i(s_{i-1}^t, s_i^t, s_{i+1}^t)$를 부울함수로 표현했을 때, XOR논리로만 표현되는 규칙을 선형규칙이라고 하며 선형규칙으로만 이루어진 CA를 선형 CA라고 한다. 본 논문에서 사용되는 90/150 CA는 모든 셀에 적용되는 전이규칙이 90 또는 150인 CA를 말한다. 표 1은 전이규칙 90과 150에 대한 부울식을 나타낸다.

표 1. 전이규칙 90과 150의 부울식
Table 1. Boolean equation for transition rule 90 and 150

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

n-셀 90/150 CA의 상태전이 함수는 선형 CA이므로 다음 상태를 구하는 함수를 행렬로 표현할 수 있다. 이러한 행렬을 상태전이행렬이라고 하며 식 2와 같이 삼중대각행렬이 된다. 여기서 CA의 i번째 셀에 적용되는 전이규칙이 90이면 $d_i = 0$, 150이면 $d_i = 1$이다.

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

식 2는 $T_n = < d_1 d_2 \cdots d_n >$로 간단히 나타낸다. 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. 상태전이행렬이 T_n인 임의의 n셀 90/150 CA에 대하여 T_n의 최소다항식(minimal polynomial)은 T_n의 특성다항식과 같다. T_n은 삼중대각행렬이므로 T_n의 특성다항식 Δ_n은 식 3과 같은 점화관계가 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.

그림 1은 $T_4 = < 0001 >$인 90/150 CA의 구조이다. 그림 1의 4셀 90/150 CA의 특성다항식은 $x^4 + x^3 + x^2 + 1$이다.

III. 90/150 HCA를 이용한 MWCA 판정법

n차 최대무게 다항식은 n차 다항식의 모든 계수가 1인 다항식으로 $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$이다. $f_n(x)$는 $f_n(x) = f_n^*(x)$를 만족하는 자기상반다항식

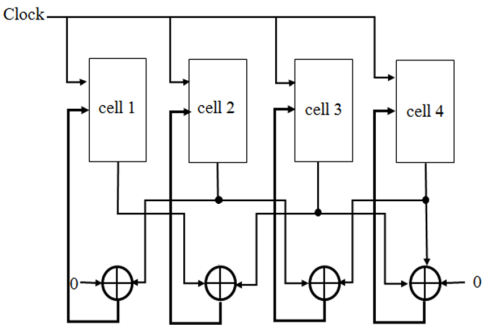

그림 1. 전이규칙 <0001>인 90/150 CA의 구조
Fig. 1 Structure of 90/150 CA with transition rule <0001>

이다. 여기서 $f_n^*(x) = x^n f_n\left(\frac{1}{x}\right)$이다. 그리고 $f_n(x)$를 특성다항식으로 갖는 90/150 CA를 90/150 MWCA(Maximum Weight CA)라 한다.

예를 들어 $f_4(x)$에 대하여 4-셀 90/150 MWCA는 $R_4 = < 0010 >$이다. 그리고 $f_6(x)$에 대하여 6-셀 90/150 MWCA는 존재하지 않는다.

표 2는 $f_1(x)$부터 $f_{200}(x)$까지 대응하는 90/150 MWCA의 존재여부에 대한 결과이다. 표 2에 의하면 1차에서 200차까지 90/150 MWCA가 존재하지 않는 차수는 모두 59개이다.

$(2n+1)$-셀 90/150 MWCA는 n-셀 90/150 MWCA로부터 합성할 수 있다[16]. 예를 들어 $f_4(x)$에 대응하는 90/150 MWCA는 R_4이므로 이를 이용하여 $f_9(x)$에 대응하는 90/150 MWCA를 합성할 수 있고 그 결과는 $< R_4 1 R_4^* >$이다. 여기서 R_4^*는 R_4의 대칭전이규칙 $< 0100 >$을 역순으로 나타낸 것이다. 반면에 n-셀 90/150 MWCA가 존재하지 않으면 $(2n+1)$-셀 90/150 MWCA 역시 존재하지 않는다. 표 2에서 6-셀 90/150 MWCA가 존재하지 않으므로, 크기가 13, 27, 55, 111,…인 90/150 MWCA가 존재하지 않는다. 따라서 $n = 2m$인 짝수차 $f_n(x)$에 대하여 90/150 MWCA가 존재하는 지에 대한 판정기준이 필요하다. 다음 보조정리는 식 3으로부터 유도할 수 있다[19].

<보조정리 1> 전이규칙이 $<100\cdots0>$인 $k(\geq 2)$-셀 90/150 HCA의 특성다항식을 $h_k(x)$라 하면 식 4를 만족한다.

$$h_k(x)=xh_{k-1}(x)+h_{k-2}(x) \quad (4)$$

여기서 $h_1(x)=x+1$이고 $h_0(x)=1$이다.

정리 2는 n-셀 90/150 HCA로부터 $2n$-셀 90/150 MWCA를 판단하는 기준을 제시하는 근거이다.

<정리 2> 전이규칙이 $<100\cdots0>$인 90/150 CA의 특성다항식 $h_m(x)$에 대하여 식 5가 성립한다.

$$x^m h_m(x+1/x)=f_{2m}(x) \quad (5)$$

표 2. $f_1(x)$부터 $f_{200}(x)$까지 90/150 MWCA가 존재하지 않는 차수

Table 2. The degree of the polynomials for which there is no 90/150 MWCA from $f_1(x)$ to $f_{200}(x)$

Range of degree	The degree in which MWCA does not exist
$f_1(x)\sim f_{50}(x)$	6, 13, 20, 22, 27, 30, 34, 41, 45, 46, 48
$f_{51}(x)\sim f_{100}(x)$	55, 61, 62, 68, 69, 70, 72, 76, 78, 83, 88, 90, 91, 92, 93, 97
$f_{101}(x)\sim f_{150}(x)$	102, 104, 111, 114, 118, 123, 125, 126, 132, 137, 139, 140, 141, 145, 146, 150
$f_{151}(x)\sim f_{200}(x)$	153, 154, 157, 160, 166, 167, 174, 177, 181, 183, 185, 187, 188, 190, 195, 198

(증명) 수학적 귀납법으로 증명할 수 있다. $h_1(x)=x+1$이므로 $xh_1(x+1/x)=x(x+x^{-1}+1)=x^2+x+1=f_2(x)$이다. 그러므로 $n=1$일 때 성립한다. $n=2$일 때, 보조정리 1에 의해 $h_2(x)=x^2+x+1$이고,

$$\begin{aligned}x^2h_2(x+1/x)&=x^2((x+x^{-1})^2+(x+x^{-1})+1)\\&=x^4+x^3+x^2+x+1\\&=f_4(x)\end{aligned}$$

이므로 식 5를 만족한다.

$m\leq k$ 일 때, $x^kh_k(x+1/x)=f_{2k}(x)$라고 가정하면,

$$\begin{aligned}&x^{k+1}h_{k+1}(x+1/x)\\&=x^{k+1}\{(x+x^{-1})h_k(x+x^{-1})+h_{k-1}(x+x^{-1})\}\\&=(x^{k+2}+x^k)h_k(x+x^{-1})+x^2x^{k-1}h_{k-1}(x+x^{-1})\\&=(1+x^2)x^kh_k(x+x^{-1})+x^2f_{2(k-1)}(x)\\&=f_{2k}(x)+x^{2k+2}+x^{2k+1}\\&=f_{2k+2}(x)\end{aligned}$$

이므로 $m=k+1$일 때도 성립한다.

다음은 m-셀 90/150 HCA기반의 $2m$-셀 90/150 MWCA의 존재 여부에 대한 판정기준을 제안한다. m-셀 90/150 HCA $<10\cdots0>$의 특성다항식을 $h_m(x)$이라 할 때, $f_{2m}(x)$에 대응하는 $2m$-셀 90/150 MWCA의 존재여부에 대한 판정기준은 다음과 같다.

(ⅰ) $h_m(x)$가 기약이고 x의 계수가 1이면 $f_{2m}(x)$는 기약다항식이다. 따라서 $f_{2m}(x)$는 CA 다항식이다.

(ⅱ) $h_m(x)$가 기약이고 x의 계수가 0이면 $f_{2m}(x)$는 가약다항식이며 CA 다항식이 아니다.

(ⅲ) $h_m(x)$가 가약일 때, 기약인수가 모두 짝수 차이면 $f_{2m}(x)$는 CA 다항식이다.

(ⅳ) $h_m(x)$가 가약일 때, x의 계수가 0인 홀수차 기약 인수가 존재하면 $f_{2m}(x)$는 CA다항식이 아니다.

(ⅴ) $h_m(x)$가 가약일 때, 홀수차 기약 인수의 x항의 계수가 모두 1이면 $f_{2m}(x)$는 CA 다항식이다.

표 3은 제안한 판정기준을 이용하여 90/150 MWCA의 존재 여부를 결정하는 알고리즘이다.

표 3. 90/150 MWCA 판정 알고리즘
Table 3. 90/150 MWCA decision algorithm

Input : Degree n of $f_n(x)$
Output : $f_n(x)$ is a CA-polynomial or not a CA-polynomial
Step1 : If (n is odd) $m=\lfloor n/4 \rfloor$ else $m=n/2$
Step2 : Compute $h_m(x)$ using eq. (4) $h_k(x)=xh_{k-1}(x)+h_{k-2}(x)$ $(k=2,3,\cdots m)$
Step3 : If ($h_m(x)$ is irreducible) { If (coefficient of x term = 1) $f_n(x)$ is a CA-polynomial STOP else $f_n(x)$ is not a CA-polynomial STOP }
Step4 : Factor $h_m(x)$
Step5 : If (the degree of all irreducible factors is all even) $f_n(x)$ is a CA-poly. STOP else if (the coefficient of x term of all odd-degree irreducible factor is 1) $f_n(x)$ is a CA-polynomial STOP else $f_n(x)$ is not a CA-polynomial STOP

표 4는 제안한 90/150 MWCA 판정 알고리즘을 이용하여 $f_{2m}(x)$에 대응하는 90/150 MWCA의 존재 판정의 결과이다. 표 4에서 $h_m(x)$의 인수분해의 개수 목록은 기약인수의 각 항에 대하여 계수가 1인 x의 차수를 의미한다. 예를 들어 (2,1,0)은 x^2+x+1을 나타낸다. 또한 편의상 항의 수가 6이상인 기약인수에 대하여는 내림차순으로 정리하여 최고차항의 차수와 하위 3개항의 x의 차수만 나타낸다.

	(15,⋯,5,4,0)(15,⋯,6,2,0)
110	(4,1,0)(4,3,2,1,0)(6,5,4,1,0)(24,⋯,3,2,0)(24,⋯,8,7,0)(24,⋯,4,2,0)(24

본 연구에서는 $m=6000$까지 $h_m(x)$을 구하여 Maple 13을 이용하여 $h_m(x)$의 인수분해를 하였다. 또한 제안된 알고리즘에 의해 CA-다항식인 경우 $2m$셀 90/150 MWCA를 합성하였다. 이때 90/150 MWCA 합성은 [12]에서 제안된 90/150 CA합성알고리즘을 이용하였다.

Ⅳ. 결론

본 논문에서는 양방향으로 읽기가 가능한 부호어를 생성하는 자기상반다항식 중 최대무게 다항식에 대응하는 90/150 MWCA의 존재 여부에 대한 판정법을 제안하였다. 전이규칙이 <100⋯0>인 m-셀 90/150 HCA의 특성다항식을 구한 후 인수분해 한 결과를 5가지 부류로 나누어 $f_{2m}(x)$가 CA 다항식인지 아닌지 판단하였다. 이러한 방법은 전이규칙이 일정한 작은 크기의 90/150 CA의 특성다항식을 이용하여 큰 크기 셀의 90/150 MWCA의 존재에 대한 판정이 가능하므로 제안한 판정법은 셀의 크기가 커졌을 때, 매우 효율적일 것으로 사료된다.

표 4. 90/150 MWCA 판정 알고리즘을 이용한 $h_m(x)$의 인수분해와 $f_{2m}(x)$의 판정 결과
Table 4. Results of $f_{2m}(x)$ and factorization of $h_m(x)$ using 90/150 MWCA decision algorithm

m	Factorization $h_m(x)$	Output ($f_{2m}(x)$ is...)	case
54	(18,⋯,4,1,0)(18,⋯,2,1,0)(18,⋯3,1,0)	a CA-polynomial	iii
57	(2,1,0)(11,⋯,3,2,0)(44,⋯,6,5,0)	not a CA-polynomial	iv
60	(5,4,2,1,0)(55,⋯,2,1,0)	a CA-polynomial	v
65	65,⋯,33,1,0	a CA-polynomial	i
83	83,⋯,3,2,0	not a CA-polynomial	ii
108	(3,2,0)(5,2,0)(5,3,0)(5,4,3,2,0)(15,⋯,54,0)(15,⋯,6,3,0)(15,⋯,4,2,0)(15,⋯,9,3,0)	not a CA-polynomial	iv

감사의 글

본 논문은 "2018년 한국전자통신학회 가을철학술대회 우수논문"임.

References

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

[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] 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.

[4] 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.

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

[6] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation,* vol. 18, no. 11, 2013, pp. 3075-3085.

[7] A. Bakhshandeh and Z. Eslami1, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Optics and Lasers in Engineering*, vol. 51, no. 6, 2013, pp. 665-673.

[8] P. Ping, F. Xu, and Z. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Processing*, vol. 105, no. 1, 2014, pp. 419-429.

[9] S. Nandi, S. Roy, J. Dansana, W. Karaa, R, Ray, S. Chowdhury, S. Chakraborty, and N. Dey, "Cellular Automata based Encrypted ECG-hash Code Generation: An Application in Inter-human Biometric Authentication System," *I. J. Computer Network and Information Security,* vol. 6, no. 11, 2014, pp. 1-12.

[10] H. Kim, S. Cho, U. Choi, and M. Kwon, "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.

[11] 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.

[12] 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.

[13] 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.

[14] A. Sabater and P. Gil, "Synthesis of cryptographic interleaved sequences by means of linear cellular automata," *Applied Mathematics Letters*, vol. 22, 2009, pp. 1518-1524.

[15] 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.

[16] U. Choi, S. Cho, H. Kim, and J. Kim, "90/150 CA corresponding to polynomial of maximum weight," *J. of Cellular Automata,* vol. 13, 2018, pp.347-358.

[17] 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, 2018, pp. 383-390.

[18] 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*, vol. 13, no. 3, 2018, pp. 593-600.

[19] U. Choi and S. Cho, "90/150 RCA corresponding to Maximum Weight Polynomial with degree 2^n," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 4, 2018, pp. 819-826.
[20] P. Chaudhuri, D. Chowdhury, S. Nandi, and S. Chattopadhyay, *Additive cellular automata theory and applications.* Los Alamitos; IEEE Computer Society Press, 1997.

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

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

김진경(Jin-Gyoung Kim)

2008년 부경대학교 대학원 응용수학과 졸업(이학석사)
2013년 부경대학교 대학원 응용수학과 졸업(이학박사)
※ 관심분야 : 셀룰라 오토마타론, 유한체

강성원(Sung-Won Kang)

2017년 부경대학교 응용수학과 졸업(이학사)
2017년~ 현재 부경대학교 대학원 응용수학과 석사과정 재학
※ 관심분야 : 셀룰라 오토마타론, 유한체