Regular paper

Journal of the KIECS. pp. 319-326, vol. 15, no. 2, Apr. 30. 2020, t. 100, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2020.15.2.319

프로그램 가능 최대길이 CA기반 의사난수열 생성기의 설계와 분석

최언숙* · 조성진** · 김한두*** · 강성원****

Design and Analysis of Pseudorandom Number Generators Based on Programmable Maximum Length CA

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

요 약

PRNG(Pseudorandom number generator)는 안전한 온라인 통신을 위한 암호화 키 생성에 있어서 필수적이다. PRNG에 의해 생성되는 비트 스트림은 대칭키 암호 시스템에서 빅 데이터를 효과적으로 암호화할 수 있도록 고속으로 생성되어야 하며 또한 여러 통계적 테스트를 통과할 수준의 랜덤성을 확보해야 한다. CA(Cellular Automata) 기반의 PRNG는 하드웨어로 구현이 용이하고, LFSR기반의 PRNG보다 렌덤성이 우수하다고 알려져 있다. 본 논문에서는 대칭키 암호시스템에서 효과적인 키 수열을 생성할 수 있는 PMLCA(Programmable Maximum Length CA)기반의 PRNG를 설계한다. 제안하는 PRNG는 비선형 제어 방식을 통해 비트 스트림을 생성한다. 먼저 주기가 긴 선형 수열을 생성하는 단일 여원벡터를 갖는 (m,n)-셀 PMLCA $\mathbb{P}$ 기반의 PRNG를 설계하고 주기와 생성다항식을 분석한다. 또한 $\mathbb{P}$와 주기가 같으면서 비선형 수열을 생성하는 두 개의 여원벡터를 갖는 (m,n)-셀 PC-MLCA기반의 PRNG를 설계하고 비선형 수열이 출력되는 위치를 분석한다.

ABSTRACT

PRNGs(Pseudorandom number generators) are essential for generating encryption keys for to secure online communication. A bitstream generated by the PRNG must be generated at high speed to encrypt the big data effectively in a symmetric key cryptosystem and should ensure the randomness of the level to pass through the several statistical tests. CA(Cellular Automata) based PRNGs are known to be easy to implement in hardware and to have better randomness than LFSR based PRNGs. In this paper, we design PRNGs based on PMLCA(Programable Maximum Length CA) that can generate effective key sequences in symmetric key cryptosystem. The proposed PRNGs generate bit streams through nonlinear control method. First, we design a PRNG based on an (m,n)-cell PMLCA $\mathbb{P}$ with a single complement vector that produces linear sequences with the long period and analyze the period and the generating polynomial of $\mathbb{P}$. Next, we design an (m,n)-cell PC-MLCA based PRNG with two complement vectors that have the same period as $\mathbb{P}$ and generate nonlinear sequences, and analyze the location of outputting the nonlinear sequence.

키워드

Complement Vector, Linear sequence, Nonlinear sequence, PRNG, Programmable Cellular Automata
여원 벡터, 선형 수열, 비선형 수열, 의사 난수열 생성기, 프로그램 가능 셀룰라 오토마타

* 동명대학교 정보통신공학과 (choies@tu.ac.kr)
** 교신저자 : 부경대학교 응용수학과
*** 인제대학교 컴퓨터공학부 (mathkhd@inje.ac.kr)
**** 부경대학교 응용수학과 (jsm2371@hanmail.net)
· 접 수 일 : 2020. 01. 21
· 수정완료일 : 2020. 03. 03
· 게재확정일 : 2020. 04. 15
· Received : Jan. 21, 2020, Revised : Mar. 03, 2020, Accepted : Apr. 15, 2020
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math. Pukyong National University,
Email : sjcho@pknu.ac.kr

Ⅰ. 서 론

난수는 키 생성, 암호화, 마스킹 프로토콜 또는 인터넷 게임과 같은 많은 암호화 응용프로그램의 기본 도구이다. 비밀키 및 공개키 알고리즘에서 키 생성을 위한 시드, 암호화 및 인증에 사용되는 세션 키, 암호로 해시 될 솔트 및 식별 프로토콜에서 사용된 문제는 모두 시스템 설계자에 의해 임의으로 가정된다. 그러나 충분한 임의성을 생성하는 것은 비용이 많이 들기 때문에 대부분의 응용프로그램은 PRNG라고 하는 암호 메커니즘을 사용하여 임의의 짧은 비트 문자열을 이용하여 더 긴 무작위 비트 문자열로 확장하는 방법을 사용하고 있다[1]. 비트 스트림에 요구되는 특성은 매우 다양하다. 그 중에서 가장 흔하게 요구되는 특성은 랜덤성이다. 그리고 또 하나의 중요한 요구사항은 일반적으로 하나의 랜덤 비트 스트림이 한번 사용된 후에 폐기하는 것이 아니라 정확히 동일한 랜덤 비트 스트림을 다시 발생시켜서 재사용해야 한다는 것이다. 통신시스템의 송/수신기, 암호 시스템의 암/복호화기가 이를 요구하는 대표적인 예이다[2-5].

CA는 동역학계를 해석하는 한 방법으로 시간과 공간을 이산적으로 다룬다. 이산적 공간인 셀룰러 공간은 셀이라는 기억소자로 구성되어 있다. CA는 각 셀이 취할 수 있는 상태를 유한하게 처리하며 각 셀들의 상태가 국소적인 상호작용에 의해 동시에 업데이트되는 시스템이다. 특히 1차원 CA는 그 물리적 배열이 매우 간단하면서도 랜덤성이 좋은 의사난수열을 효과적으로 생성할 수 있는 PRNG로 응용되었다. 특히 정보화 시대에 맞추어 CA는 키 수열을 생성할 수 있는 생성기로 암호시스템에 도입되었다[6-9].

CA기반의 PRNG에 대한 설계와 분석이 지난 20여 년 간 활발히 연구되고 있다[10-16]. Cattell 등은 최대 주기 수열을 생성하는 PRNG로 LFSR보다 랜덤성이 우수한 90/150 CA 합성법을 제안하였다[10]. Sabater 와 Cho 등은 두 개의 최대길이 CA를 이용하여 출력되는 수열을 비선형적인 방법으로 제어하여, 출력수열의 랜덤성을 높이고 주기를 확장하는 PRNG를 설계하는 방법을 제안하였다[11-13]. 또한 여원 최대길이 CA 기반의 PRNG가 제안되었고 여원 최대길이에 의해 생성되는 수열에 대한 분석이 이루어졌다[14,16]. 본 논문에서는 대칭키 암호시스템에서 효과적인 키 수열을 생성할 수 있는 프로그램 가능 MLCA 기반의 PRNG를 설계한다. 제안하는 PRNG는 비선형적인 제어 방식을 통해 비트 스트림을 생성한다. 먼저 주기가 긴 선형 수열을 생성하는 단일 여원벡터를 갖는 (m,n)-셀 PMLCA $\mathbb{P}$ 기반의 PRNG를 설계하고 $\mathbb{P}$의 주기와 생성다항식을 분석한다. 또한 $\mathbb{P}$와 주기가 같으면서 비선형 수열을 생성하는 두 개의 여원벡터를 갖는 (m,n)-셀 PC-MLCA 기반의 PRNG를 설계하고 비선형 수열이 출력되는 위치를 분석한다.

Ⅱ. 배경지식 및 기존 연구

CA는 구조가 간단하고 규칙적이며 작은 단위로 확장연결이 가능하다. 이산 시간마다 한 비트 씩 출력하는 LFSR과 달리 CA는 모든 셀에서 서로 다른 이진 비트 스트림을 출력함으로 의사난수열 또는 테스트 패턴 생성기로 많이 응용되고 있다. 프로그램 가능 CA는 [7]에서 처음 소개되었는데, 각 셀의 조합 논리는 고정되어 있지 않아 다양한 전이규칙이 적용될 수 있도록 제어 신호에 의해 제어되는 CA이다. 그림 1은 프로그램 가능 90/150 CA의 간단한 구조이다. CA의 각 셀에 대한 다음 상태를 결정하는 상태전이 함수는 식(1)과 같으며, $s_i^t(\in\{0,1\})$는 시간 t에서 i번째 셀의 상태를 나타낸다.

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

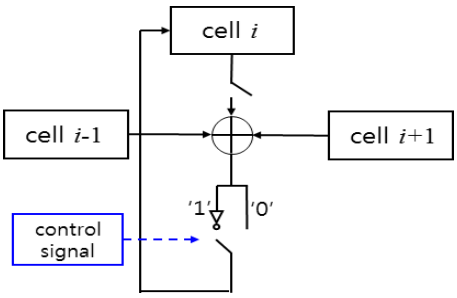

그림 1. 프로그램 가능 90/150 CA의 구조
Fig. 1 Structure of programmable 90/150 CA

본 논문에서 각 셀에 사용되는 전이규칙은 규칙 90, 105, 150, 165이고, 각 전이규칙은 표 1과 같이 부울식으로 표현할 수 있다. 표 1의 규칙 90과 150은 90/150 CA에서 적용되는 규칙으로 부울식이 모두 XOR논리로 표현되는 선형규칙이다. 선형 CA는 각 셀에 적용되는 전이 규칙이 모두 XOR로만 표현될 수 있는 선형규칙을 적용한 CA를 말한다. 또한 표 1에서 규칙 165, 105와 같이 XNOR로 표현되는 규칙을 여원규칙이라고 하며, CA의 모든 셀에 적용된 전이규칙이 선형규칙과 여원규칙으로만 이루어진 CA를 여원 CA라 한다[17].

표 1. 전이규칙 90, 105, 150, 165의 부울식
Table 1. Boolean expressions of transition rule 90, 105, 150 and 165

Rule No.	Boolean expression
90	$s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$
105	$s_i^{t+1} = \overline{s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t}$
150	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$
165	$s_i^{t+1} = \overline{s_{i-1}^t \oplus s_{i+1}^t}$

n-셀 CA의 모든 셀에 적용된 규칙이 90과 150인 경우 이러한 CA를 90/150 CA라 한다. 90/150 CA의 상태전이함수 T_n 는 $n \times n$ 행렬로 식 (2)와 같이 삼중대각 행렬로 표현되며, 이를 상태전이행렬이라 한다.

$$T_n = (t_{ij}) = \begin{cases} 1 \ , j = i-1 \text{ or } j = i+1 \\ d_i \ , i = j \\ 0 \ , o/w \end{cases} \tag{2}$$

여기서 CA의 i번째 셀에 적용되는 규칙이 90이면 $d_i = 0$, 150이면 $d_i = 1$이다. T_n을 $T_n = < d_1 d_2 \cdots d_n >$로 간단히 나타낸다.

T_n의 특성다항식은 $\Delta_n = |T_n + xI_n|$이고, 여기서 I_n는 n차 단위행렬이다. 상태전이행렬이 T_n인 임의의 n-셀 90/150 CA에 대하여 T_n의 최소다항식은 T_n의 특성다항식과 같다[15]. Δ_n이 원시다항식일 때 T_n에 대응하는 CA는 최대주기를 갖는다. 이러한 CA를 90/150 MLCA(maximum length CA)라 한다. 90/150 MLCA의 각 셀에서 출력되는 수열은 m-수열이다. n차 원시다항식에 대응하는 90/150 MLCA의 전이행렬이 T_n이고, S^t가 시간 t에서의 셀의 상태일 때 90/150 MLCA의 상태전이는 식 (3)과 같다.

$$S^{t+1} = T_n S^t \tag{3}$$

Choi와 Cho는 90/150 MLCA로부터 유도되는 여원 CA는 MLCA임을 보였고, 특히 각 셀에서 출력되는 수열은 m-수열 또는 $\overline{m}$-수열이며 $\overline{m}$-수열을 출력하는 셀의 위치를 분석하였다[16]. 90/150 MLCA로부터 유도된 여원 MLCA(C-MLCA) 상태전이는 식 (4)와 같다.

$$S^{t+1} = \overline{T_n} S^t = T_n S^t + F \tag{4}$$

정리 1은 90/150 MLCA로부터 유도된 C-MLCA의 셀 중 비선형 수열인 $\overline{m}$-수열을 출력하는 셀의 위치를 구하는 방법을 소개한다.

<정리 1[16]> n-셀 90/150 MLCA의 상태전이행렬 T_n과 여원벡터 F에 의해 유도되는 여원 MLCA $\mathbb{C}'$에 대하여 $\alpha = (v_1, v_2, \cdots, v_n)^t$ 가 $(T_n + I_n)\alpha = F$를 만족할 때, $v_i \neq 0$이면 $\mathbb{C}'$의 i번째 셀에서 출력되는 수열은 $\overline{m}$-수열이다.

III. 프로그램 가능 MLCA기반의 PRNG

본 논문에서는 (m,n)-셀 PMLCA기반의 PRNG와 (m,n)-셀 PC-MLCA기반의 PRNG를 제안한다. 이 PRNG는 m-셀 90/150 MLCA $\mathbb{C}_c$와 n-셀 여원 MLCA로 구성된다. 여기서 $n > m$이고 $\gcd(m,n) = 1$이다. n-셀 여원 MLCA는 90/150 MLCA $\mathbb{C}_g$와 여원벡터로 이루어진다. $\mathbb{C}_c$는 여원 MLCA의 여원벡터를 제어하기 위한 비트를 출력한다.

그림 2는 $\mathbb{C}_g$, 여원벡터 1개, 그리고 $\mathbb{C}_c$로 이루어진 (m,n)-셀 PMLCA 기반의 PRNG의 구조이다. 그림 2와 같이 단일 여원벡터를 갖는 (m,n)-셀 PMLCA기반의 PRNG에 의해 출력되는 수열은 주기가 $(2^m - 1)(2^n - 1)$이고 생성다항식이 $c_m(x)c_n(x)$인

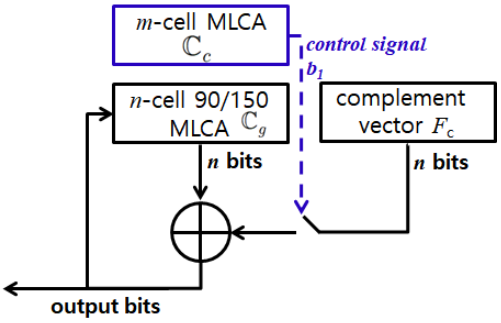

그림 2. 단일 여원벡터를 갖는 (m,n)-셀 PMLCA기반의 PRNG의 구조

Fig. 2 Structure of PRNG based on (m,n)-cell PMLCA with a single complement vector

선형수열이다[18]. 여기서 $c_{m(x)}$는 $\mathbb{C}_c$의 특성다항식이고 $c_n(x)$는 $\mathbb{C}_g$의 특성다항식이다. m-셀 $\mathbb{C}_c$에 의해 생성되는 수열 $c_0, c_1, \cdots$는 주기가 2^m-1이다. (m,n)-셀 PMLCA의 상태전이 함수를 P라 하면 시간 t에서의 상태를 S^t라고 할 때 시간 $t+1, t+2, \cdots, t+k$에서의 상태는 식(5)~(7)과 같다.

$$S^{t+1} = PS^t = T_n S^t + c_t F_c \tag{5}$$

$$\begin{aligned} S^{t+2} &= P^2 S^t = T_n(T_n S^t + c_t F_c) + c_{t+1} F_c \\ &= T_n^2 S^t + (c_t T_n + c_{t+1} I_n) F_c \\ &\vdots \end{aligned} \tag{6}$$

$$\begin{aligned} S^{t+k} &= P^k S^t = T_n^k S^t + (c_t T_n^{k-1} + c_{t+1} T_n^{k-2} + \\ &\quad \cdots + c_{t+k-2} T_n + c_{t+k-1} I_n) F_c \end{aligned} \tag{7}$$

여기서 c_t는 시간 t에서 $\mathbb{C}_c$로부터 출력된 제어비트이고 F_c은 여원벡터이다.

표 2는 $\mathbb{C}_g$의 전이규칙이 <0101>이고 $F_c=(1,0,1,1)$이고 초기 벡터가 (0,1,0,1)일 때 $\mathbb{C}_c$의 전이규칙이 <011>인 단일 여원벡터를 갖는 (3,4)-셀 PMLCA의 각 셀에서 출력되는 비트 스트림이다. 표 2에 의하면 각 셀에서 출력된 비트 스트림은 모두 생성다항식이 $x^7+x^5+x^3+x^2+1=(x^4+x+1)(x^3+x+1)$인 주기가 105인 선형 수열이다.

단일 여원벡터를 갖는 (m,n)-셀 PMLCA에 의해 출력된 수열은 비선형적 제어방식에 의해 주기는 길어졌으나 모두 선형 수열이다.

표 2. 단일 여원벡터를 갖는 (3,4)-셀 PMLCA의 출력 비트 스트림

Table 2. Output bit streams of (3,4)-cell PMLCA with a single complement vector

cell	output bit stream
1st	111111100111010101000101100110000110111011111101101001 010110110001100100100001000111000001111010000001 0100
2nd	1010000001010011111110011101010100010110011000011011 1 011111011010010101101100011001001000010001110000011 1
3rd	000111101000000101001111111001110101010001011001100 00 110111011111101101001010110110001100100100001000111 00
4th	110000011110100000010100111111100111010101000101100 11 000011011101111101101001010110110001100100100001000 01

출력되는 수열에 대하여 확장된 주기는 그대로 유지하며, 비선형 수열을 생성하는 PRNG를 설계하기 위하여 $\mathbb{C}_c$, $\mathbb{C}_g$와 여원벡터 F_x, F_c를 이용하여 $(m,n)-$셀 PC-MLCA기반의 PRNG를 설계한다. 그림 3은 본 논문에서 제안하는 두 개의 여원벡터를 갖는 $(m,n)-$셀 PC-MLCA기반의 PRNG의 구조이다. 그림 3과 같이 $(m,n)-$셀 PC-MLCA기반의 PRNG는 n-셀 여원 MLCA를 이용하여 프로그램 가능 CA를 설계함으로써 주기를 확장시킴과 동시에 비선형 수열을 생성할 수 있다.

(m,n)-셀 PC-MLCA의 상태전이 함수를 $\overline{P}$라 하면 시간 t에서의 상태를 S^t라고 할 때 시간 $(t+1)$에서의 상태를 구하는 식은 (8)과 같고, 시간 $(t+k)$에서의 상태를 구하는 식은 (9)와 같다.

$$S^{t+1} = \overline{P} S^t = T_n S^t + F_f + c_t F_c \tag{8}$$

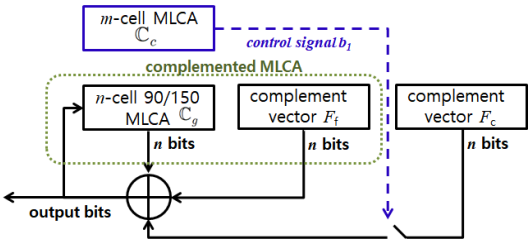

그림 3. 두 개의 여원벡터를 갖는 (m,n)-셀 PC-MLCA기반의 PRNG의 구조

Fig. 3 Structure of PRNG based on (m,n)-cell PC-MLCA with double complement vectors

$$
\begin{aligned}
&S^{t+k} \\
&= \overline{P^k} S^t \\
&= T_n^k S^t + (T_n^{k-1} + \cdots + T_n + I_n) F_f \\
&\quad + (c_t T_n^{k-1} + \cdots + c_{t+k-2} T_n + c_{t+k-1} I_n) F_c \quad (9)
\end{aligned}
$$

표 3은 $\mathbb{C}_g$의 전이규칙이 <0101>, $\mathbb{C}_c$의 전이규칙이 <011>, F_x =(0,1,1,0), F_c =(1,0,1,1), $\mathbb{C}_g$의 초기 벡터가 (0,1,0,1)일 때 두 개의 여원벡터를 갖는 (3,4)-셀 PC-MLCA의 각 셀에서 출력되는 비트 스트림이다. 표 3에 의하면 4개의 셀에서 출력되는 수열의 주기는 모두 105이다. 이 중 세 번째, 네 번째 셀에서 출력되는 비트 스트림은 생성다항식이 $x^7+x^5+x^3+x^2+1 = (x^4+x+1)(x^3+x+1)$인 선형 수열이며, 첫 번째와 두 번째 셀에서 출력되는 비트 스트림은 비선형 수열이다.

표 3. 두 개의 여원벡터를 갖는 (3,4)-셀 PC-MLCA의 출력 비트 스트림
Table 3. Output bit streams of (3,4)-cell PC-MLCA with double complement vectors

cell	output bit stream
1st	100010000010010110101010010011100110110111101110001111100001011111101011000000011000101010111010011001111100
2nd	010011001111001000100000100101101010010011101101101111011100011110000101111110101100000001100010101011 1
3rd	101000101100110000110111011111101101001010110110001100100010001110000011110100000010100111111100111010
4th	101010100010110011000011011101111101101001010110110001100100100001000111000001111010000001010011111110011

표 4. MLCA기반의 PRNG 비교
Table 4. Comparison of MLCA based PRNGs

MLCA	order	type of seq.	number of complement vectors
n-cell MLCA	2^n-1	linear	0
n-cell C-MLCA	2^n-1	nonlinear	1
(m,n)-cell PMLCA	$(2^n-1)(2^m-1)$	linear	1
(m,n)-cell PC-MLCA	$(2^n-1)(2^m-1)$	nonlinear	2

두 개의 여원벡터 F_x와 F_c를 갖는 (m,n)-셀 PC-MLCA의 상태 $Y=(y_1,y_2,\cdots,y_n)^t$가 $(T_n+I_n)Y=F_x$를 만족할 때, 정리 1에 의하여 $y_i \neq 0$ 이면 (m,n)-셀 PC-MLCA의 i번째 셀에서 출력되는 비트 스트림은 비선형 수열이다. 표 4는 MLCA 기반의 PRNG에 대한 비교 결과이다.

Ⅳ. 결론

본 논문에서는 효과적인 암호시스템 설계에 있어 중요한 요소 중 하나인 키 수열을 효과적으로 생성할 수 있는 PRNG를 설계하였다. 제안한 방법에 의하여 비선형 제어 신호에 의해 여원벡터가 제어되는 프로그램 가능 MLCA 기반의 PRNG로 트 스트림을 생성하였다. 본 논문에서는 두 가지 타입의 PRNG를 제안하였는데, 먼저 주기가 긴 선형 수열을 생성하는 (m,n)-셀 PMLCA $\mathbb{P}$기반의 PRNG를 설계하고 주기와 생성다항식을 분석하였다. 또한 $\mathbb{P}$와 주기가 같으면서 비선형 수열을 생성하는 (m,n)-셀 PC-MLCA 기반의 PRNG를 설계하고 비선형 수열을 출력하는 위치를 분석하였다. 본 논문에서 제안된 (m,n)-셀 PMLCA 기반의 PRNG와 (m,n)-셀 PC-MLCA 기반의 PRNG는 비선형 제어 방식으로 수열을 생성함으로써 보다 랜덤성이 우수하고, 주기가 긴 비트 스트림을 생성할 수 있으며 키 공간도 확장되었다. 특히 PC-MLCA 기반의 PRNG는 비선형 수열을 출력함으로써 비밀키 암호 시스템에서 효과적인 키 생성기로 응용할 수 있을 것으로 사료된다.

감사의 글

위 논문은 “2019년 한국전자통신학회 가을철 학술대회 우수논문”입니다.

이 논문은 부경대학교 자율창의학술연구비(2019년)에 의하여 연구되었음

References

[1] A. Desai, A. Hevia, and Y. L. Yin, "A Practice-Oriented Treatment of Pseudorandom Number Generators," *EUROCRYPT 2002*, Amsterdam, The Netherlands, 2002, pp. 368-383.

[2] 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.

[3] 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.

[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] 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.

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

[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] U. Choi, S. Cho, J. Kim, S. Kang, H. Kim, and S. Kim, "Color image encryption based on PC-MLCA and 3-D chaotic cat map," *2019 IEEE 4th International Conference on Computer and Communication System,* Singapore, Singapore, 2019, pp. 272-277.

[10] 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.

[11] A. Sabater and D. Martinez, "Simple Cellular Automata-Based Linear Models for the Shrinking Generator," *Proc. of IEEE Information Theory Workshop,* 2003, pp. 143-146.

[12] 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.

[13] 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.

[14] G. Y. Li, S. J. Cho, and S. T. Kim, "Complemented Maximum-Length Cellular Automata Applied on Video Encryption," *J. The Institute of Internet, Broadcasting and Communication*, vol. 17, no. 1, 2017, pp. 13-18.

[15] 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.

[16] U. Choi and S. Cho, "Analysis of Pseudorandom Sequences Generated by Maximum Length Complemented Cellular Automata," *J. of the Korean Institute of Communication Sciences*, vol. 14, no. 5, 2019, pp. 1001-1008.

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

[18] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge: Cambridge University Press, 2008.

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 정보통신공학과 교수
※ 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

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)
※ 관심분야 : 셀룰라 오토마타론, 정보보호