셀룰라 오토마타 기반의 수축-삽입 수열의 분석

최언숙* · 조성진**

Analysis of Shrunken-Interleaved Sequence Based on Cellular Automata

Un-Sook Choi* · Sung-jin Cho**

요 약

스트림 암호시스템에 사용되는 불규칙 시각 제어 생성기인 수축수열 생성기는 두 개의 LFSR(Linear Feedback Shift Register)로 구성되며 이 생성기에 의해 생성되는 수열은 비선형수열임이 알려져 있다. 두 개의 최대길이를 갖는 90/150 셀룰라 오토마타 기반의 비선형수열 생성기는 각 셀에서 동일한 특성다항식을 갖는 의사 난수열을 효과적으로 생성할 수 있으므로 LFSR에 의해 생성되는 수열에 비하여 주기와 선형복잡도가 높은 비선형수열을 생성할 수 있다. 본 논문은 이러한 비선형수열에 대한 분석으로 90/150 셀룰라 오토마타 기반의 수축-삽입수열(shrunken-interleaved sequence)을 다룬다. 셀룰라 오토마타 기반의 비선형수열 생성기에 의해 생성되는 수축-삽입수열을 삽입수열로 분석이 가능함을 보이고 출력 수열의 일부를 알 때 알려지지 않은 새로운 출력 수열의 일부를 효과적으로 재구성하는 알고리즘을 제안한다.

ABSTRACT

The shrinking generator which is one of clock-controlled generator is a very simple generator with good cryptographic properties. A nonlinear sequence generator based on two 90/150 maximum length cellular automata can generate pseudorandom sequences at each cell of cellular automata whose characteristic polynomials are same. The nonlinear sequence generated by cellular automata has a larger period and a higher linear complexity than shrunken sequence generated by LFSRs. In this paper we analyze shrunken-interleaved sequence based on 90/150 maximum length cellular automata. We show that the sequence generated by nonlinear sequence generator based on cellular automata belongs to the class of interleaved sequence. And we give an effective algorithm for reconstructing unknown bits of output sequence based on intercepted keystream bits.

키워드

수축생성기, 삽입수열, 비선형수열, 셀룰라 오토마타, 수축-삽입수열

Keywords

Shrunken genrator, interleaved sequence, nonlinear sequence, cellular automata, shrunken-interleaved sequence

* 동명대학교
** 부경대학교 (교신저자, sjcho@pknu.ac.kr)

접수일자 : 2010. 05. 13
심사완료일자 : 2010. 07. 05

Ⅰ. 서 론

스트림암호는 구현의 용이성, 높은 속도, 좋은 신뢰성과 같은 실제적인 장점 때문에 안전한 통신에서 중요한 역할을 한다. 이러한 암호는 매우 긴 주기의 난수열을 발생시켜 평문과 더함으로써 암호문을 생성하는 방식으로, 생성된 수열이 난수와 구별이 불가능해야만 안전하다고 할 수 있다. LFSR기반의 스트림 암호는 유한상태기계로 생성할 수 있는 최대 주기의 수열을 얻을 수 있으며, 수학적인 분석이 용이하다. 특히 선형복잡도라는 측도를 사용하면 다음에 출력될 값을 예측하기 위해 필요한 수열의 양을 계산할 수 있는 장점이 있다. 최대길이 LFSR은 입증할 만한 긴 주기성 및 좋은 통계적 특성을 가지고 있지만, 자체적으로는 선형이기 때문에 출력수열 중 적당한 길이의 연속한 출력 값을 알면 그 다음에 출력될 값을 알 수 있다. 따라서 LFSR을 단독으로 사용하는 것은 문제가 있다. 이러한 이유로 스트림 암호로 사용하기 위해서 LFSR수열에 비선형 논리가 도입되었다[1].

키 스트림에 비선형성을 내재시킬 수 있는 불규칙 시각 제어 생성기(clock-controlled generator)는 두 개의 레지스터로 구성된 생성기이다. 첫 번째 레지스터는 제어레지스터(control register)로 규칙적으로 클럭된다. 두 번째 레지스터는 생성레지스터(generator register)로 제어레지스터의 상태 값을 입력으로 하는 함수에 의해 클럭 수가 결정된다. 생성레지스터에 의해 생성된 출력 비트는 키스트림 비트로 출력된다. 시각 제어 생성기 중 하나인 수축생성기(shrinking generator)는 1993년 Coppersmith 등에 의해 제안되었고 이 생성기는 세 개의 LFSR에 의해 구현된 교대단계 생성기(alternating step generator)에 비해 그 작동방식이 간단하고 또한 구현이 용이하여 고속의 암호화가 요구되는 응용분야에 적합한 스트림 암호로 인식되고 있다[2]. 이후 LFSR기반의 수축생성기로 Meier 등[3]에 의해 자기수축생성기(self-shrinking generator)가 제안되었다. Choi 등은 [4]에서 제어 LFSR의 출력비트가 생성 LFSR의 출력비트를 제어하는 역할 뿐 아니라 키스트림에도 영향을 주는 균형 잡힌 수축생성기 (balanced shrinking generator)를 제안하였다.

Sabater 등은 LFSR기반의 수축 생성기에 의해 생성되는 수축수열과 같은 수열을 생성하는 생성기를 한 개의 90/150 셀룰라 오토마타(이하 CA)를 이용하여 고안하였다[5]. 그러나 제안된 방법은 CA가 LFSR과 달리 각 셀에서 동일한 특성다항식을 가지는 수열을 출력할 수 있음을 고려하지 않고 있으며 90/150 그룹 CA[6]의 주기와 수축생성기에 의해 생성되는 수축수열의 주기가 같을지라도 초기 수열벡터에 따라 주기보다 훨씬 짧은 길이의 수열을 생성할 수 있음을 간과하였다. 이런 문제점을 극복하기 위해 Choi 등은 [7]에서 90/150 최대길이를 갖는 CA 두 개로 이루어진 수축-삽입 생성기 (shrinking -interleaving generator, 이하 SI 생성기)를 제안하였다.

본 논문에서는 [7]에서 제안된 SI 생성기를 분석한다. 제안된 방법은 SI 생성기에 의해 생성된 수축-삽입수열 (shrunken-interleaved sequence, 이하 SI 수열)을 삽입수열로 해석함으로 생성된 수열의 일부를 알 때 유한체론을 바탕으로 하여 출력된 수열의 새로운 비트를 알아내는 방법이다. 또한 가로챈 부분수열로부터 새로운 비트뿐 아니라 떨어진 위치까지 정확히 알 수 있는 알고리즘을 제안한다.

Ⅱ. 연구배경 및 기존 연구

Coppersmith 등에 의해 제안된 수축생성기는 그림 1과 같이 두 개의 LFSR로 구성된다. 두 개의 LFSR R_1과 R_2가 이용되며 R_1은 제어 LFSR로 R_2에 의해서 생성되는 수열의 일부분을 선택하기 위한 목적으로 사용된다. 따라서 수축생성기에 의해서 생성되는 키스트림은 R_2에 의해서 생성되는 수열의 수축된 형태가 된다. 즉, R_1과 R_2에 클럭신호가 가해짐에 따라서 R_1의 출력이 '1'이면 R_2의 출력이 키스트림의 일부가 되고, 반면에 R_1의 출력이 '0'이면 R_2의 출력이 무시된다. 이 생성기는 생성된 키 스트림비트의 정확한 위치가 고정되어 있지 않다는 장점을 가지고 있으며, 긴 주기, 높은 선형복잡도, 좋은 통계적 특성 등 암호학적으로 좋은 성질을 지니고 있다. 수축수열의 주기 T와 선형복잡도 LC는 식 (1), (2)와 같다[1].

$$T = (2^{L_2} - 1)2^{(L_1 - 1)} \quad (1)$$

$$L_2 2^{(L_1 - 2)} < LC \leq L_2 2^{(L_1 - 1)} \quad (2)$$

여기서 L_1은 R_1의 길이이고, L_2은 R_2의 길이다.

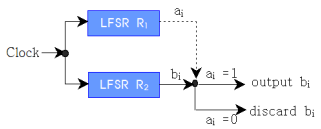


그림 1. 수축생성기
Fig. 1. The shrinking generator

<예제 1> LFSR R_1의 길이가 3이라 하자. 특성다항식이 x^3+x+1 이고 초기 수열벡터가 '001'이라고 하면 R_1에 의해 생성되는 수열 $\{a_i\}$는 '0010111…'이고 주기는 7이다. 그리고 LFSR R_2의 길이가 4이고 특성다항식이 x^4+x+1 이며 초기 수열벡터가 '0001'이라고 하면 R_2에 의해 생성되는 수열 b_i 는 '000100110101111…'이고 주기는 15이다. 이때 얻어지는 수축수열 $\{c_i\}$는 주기가 15×4=60인 수열로 (3)과 같다.

$$
\begin{aligned}
a_i &: 0010111001011100101110010111001011\cdots \\
b_i &: 000100110101111000100110101111 0001\cdots \\
c_i &: 0001111101000011001\cdots
\end{aligned} \tag{3}
$$

Meier 등[3]에 의해 제안된 자기수축생성기(self-shrinking generator)는 수축생성기에서 사용하는 두 개의 LFSR의 동작을 한 개의 LFSR로 구현하고자 하는 발상을 기반으로 설계되었다(그림 2).

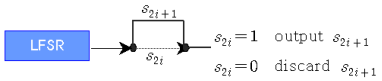


그림 2. 자기수축생성기
Fig. 2. The self-shrinking generator

한 개의 LFSR에서 출력되는 출력수열의 짝수 번째 비트는 수축생성기의 제어레지스터의 역할을 하고, 홀수 번째 비트는 생성레지스터의 역할을 한다. 즉, 우선 LFSR 2회의 동작으로 얻어진 비트 쌍 (s_{2i}, s_{2i+2})에서 $s_{2i}=1$이면 s_{2i+1}을 키스트림으로 출력하고 $s_{2i}=0$이면 키스트림의 출력 없이 다시 LFSR을 2회 동작한다.

Choi 등은 [4]에서 제어 LFSR의 출력비트는 생성 LFSR의 출력비트를 제어하는 역할 뿐 아니라 생성 LFSR의 출력비트와 XOR되어 키스트림을 생성하는 균형 잡힌 수축생성기(balanced shrinking generator)를 제안하였다. 균형 잡힌 수축생성기의 구조는 그림 3과 같다.

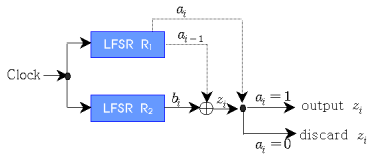


그림 3. 균형 잡힌 수축생성기
Fig. 3. The balanced shrinking generator

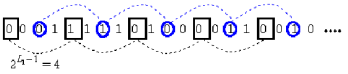
스트림 암호의 가장 대표적인 분석기법인 상관공격(correlation attack)은 Seigenthaler[8]에 의해 제안되었고, 이후 Meier 등[9]에 의해 공격알고리즘이 제안되었다. 이 공격기법은 LFSR 기반 스트림암호 뿐만 아니라 일반적인 스트림 암호의 안전성 분석에 기본적인 분석방법으로 활용되고 있다. 수축생성기와 자기수축생성기에 대한 고속 상관공격이 Zhang 등[10]에 의해 제안되었다. 이후 최근 까지 많은 연구자들에 의해 수축생성기와 자기수축생성기에 대한 다양한 분석이 활발히 진행되고 있다[11,12]. Sabater 등은 수축생성기와 자기수축생성기에 의하여 생성된 수열의 일부를 알 때, 90/150 CA를 이용하여 분석하는 방법을 제안하였다[13-15]. Sabater 등은 [13]에서 수축생성기에 의해 생성된 수축수열을 삽입수열로 분석하였다. 예제 1에서 생성된 키스트림 $\{c_i\}$에서 $c_0, c_4, c_8, \cdots$은 수열 $\{a_i\}$의 한 주기인 '0010111'에서 첫 번째 1인 a_2에 의해 출력된 b_i출력비트이다(그림 4). 마찬가지로 $c_2, c_6, c_{10}, \cdots$는 세 번째 1인 a_5에 의해 출력된 $\{b_i\}$의 출력비트이다. 길이가 L_1인 R_1에서 출력되는 수열 $\{a_i\}$중 한 주기 안에서 1의 개수는 2^{L_1-1}개이다[16]. 따라서 식 (1)에 의해 주기가 $(2^{L_2}-1)\cdot 2^{L_1-1}$인 수축수열을 2^{L_1-1}개씩 끊어 행으로 나열하면 각 열은 주기가 $2^{L_2}-1$인 의사난수열(pseudorandom sequence, 이하 PN수열)이 된다. R_2의 특성다항식이 $f(x)$이라 하면 각 열에서 생성되는 PN수열의 특성다항식 $p(x)$은 (4)와 같다[13].

$$p(x)=(x-\lambda^q)(x-\lambda^{2q})(x-\lambda^{2^2q})\cdots(x-\lambda^{2^{L_2-1}q}) \tag{4}$$

여기서 $q=2^{L_1}-1$이고 λ는 $f(\lambda)=0$를 만족하는 $f(x)$의 원시근이다. 따라서 주어진 수축수열의 특성다

항식 $P(x)$은 (5)와 같다.

$$P(x) = p(x^{2^{L_1-1}}) = [p(x)]^{2^{L_1-1}} \tag{5}$$



- $L_1 = 3$, $L_2 = 4$
- R_2의 특성다항식 : $x^4 + x + 1$
- 각 열의 특성다항식 :
  $p(x) = x^4 + x^3 + 1$
- 수축수열의 특성다항식:

$P(x) = p(x^4) = x^{16} + x^{12} + 1$

u_1	u_2	u_3	u_4
0	0	0	1
1	1	1	1
0	1	0	0
0	0	1	1
0	0	1	0
1	1	0	1
1	0	0	1
1	0	1	0
1	0	0	0
0	1	0	1
1	1	0	0
0	1	1	0
1	1	1	0
1	0	1	1
0	1	1	1

그림 4. $L_1 = 3,\ L_2 = 4$인 수축수열
Fig. 4. The shrunken sequence for $L_1 = 3,\ L_2 = 4$

다음은 Sabater 등에 의해 제안된 수축수열의 분석법이다[13]. 그림 4에서 생성된 수축수열의 일부인 $\{s_i\}=\{0,0,1,1,0,0,1,0,1,1\}$을 안다고 하자. 얻어진 10개의 비트로 표 1과 같은 부분 삼각형을 구한다.

표 1. 10개 비트로 재구성한 수열
Table 1. Sequences reconstructed from 10 shrunken bits

Δ_1 v_1	v_2	v_3	Δ_2 v_1	v_2	v_3	Δ_3 v_1	v_2	v_3	Δ_4 v_1	v_2	v_3
0	0	1	1	1	0	0	0	0	0	1	1
0	1	1	1	1	0	0	0	1	1	1	1
1	1	1	1	1	0	0	1	1	1	0	
1	0	1	1	1	1	1	1	0	0		
0	0	1	1	0	1	1	1				
0	1	0	0	0	1	1					
1	0	0	0	1							
0	1	1	1								
1	1										
1											

수축수열과 동일한 특성다항식을 갖는 90/150 CA를 합성할 수 있으므로 부분 삼각형을 만들 때 전이규칙이 <90, 90, ⋯>인 경우에 대하여 표 1의 부분 삼각형을 얻는 방법은 Δ_1에서 v_1은 얻은 10개 비트이고 이 수열을 $z_0, z_1, z_2, \cdots$라 할 때, Δ_1에서 v_2는 $z_1, z_2, z_3, \cdots$이다. Δ_1에서 v_3은 $z_0 + z_2,\ z_1 + z_3, z_2 + z_4, \cdots$와 같이 구성한다. $\Delta_j\,(j \geq 2)$에서 각 v_1은 Δ_{j-1}의 v_3와 같고 $\Delta_j\,(j \geq 2)$에서 v_2와 v_3를 얻는 방법은 Δ_1의 방법과 동일하다. 이렇게 재구성한 수열에 대하여 Δ_j의 세 번째 열 v_3은 (6)을 만족한다.

$$\begin{aligned} v_3 &= z_0 + z_2 && (\Delta_1) \\ v_3 &= z_0 + z_4 && (\Delta_2) \\ v_3 &= z_0 + z_2 + z_4 + z_6 && (\Delta_3) \\ v_3 &= z_0 + z_8\ (\Delta_4) \end{aligned} \tag{6}$$

Δ_2에서 v_3 수열은 성분이 $z_0 + z_4,\ z_1 + z_5,\ z_2 + z_6, \cdots$이고, 이 때 z_4를 $p(x) = x^4 + x^3 + 1$의 원시근 α라 두면 $1 + \alpha = \alpha^{12}$를 만족하므로 v_3 수열은 $z_{4 \cdot 12}(= z_{48}), z_{49}, z_{50}, \cdots$이다. 또 Δ_4에서 v_3 수열은 $z_0 + z_8, z_1 + z_9$이고 $1 + \alpha^2 = \alpha^9$이므로 v_3 수열은 $z_{4 \cdot 9}(= z_{36}), z_{37}$이다. 합성된 90/150 CA의 전이규칙이 <150, 150, ⋯>인 경우는 <90, 90, ⋯>인 경우와 동일하므로 전이규칙이 <90, 150, ⋯>인 경우에 대하여 부분 삼각형을 만든다. 이때 v_1, v_2는 <90, 90, ⋯>인 경우와 동일하고 Δ_1에서 v_3은 $z_0 + z_1 + z_2,\ z_1 + z_2 + z_3,\ z_2 + z_3 + z_4, \cdots$와 같이 구성한다. 이러한 규칙으로 재구성한 수열에 대하여 Δ_j의 세 번째 열 v_3은 (7)을 만족한다.

$$\begin{aligned} v_3 &= z_0 + z_1 + z_2 && (\Delta_1) \\ v_3 &= z_0 + z_2 + z_4 && (\Delta_2) \\ v_3 &= z_0 + z_1 + z_3 + z_5 + z_6 && (\Delta_3) \\ v_3 &= z_0 + z_4 + z_8 && (\Delta_4) \end{aligned} \tag{7}$$

Δ_4에서 $z_0 + z_4 + z_8$은 $1 + \alpha + \alpha^2 = \alpha^7$이므로 $z_0 + z_4 + z_8,\ z_1 + z_5 + z_9$는 z_{28}, z_{29}이다. 따라서 예제 1의 수축생성기에서 생성된 수축수열의 일부인 10개의 비트를 알 때 [13]에서 제안된 방법에 의하여 새로운 10비트를 알 수 있다. 그러나 이 방법은 새로운 비트를 알기위하여 90/150 CA를 합성하는 과정이 필요하며 계산절차가 복잡하다. 본 논문에서는 이러한 분석방법을 유한체를 바탕으로 하여 효율적으로 계산하는 알고리즘을 제안하며 알려진 k개의 비트에 대하여 새로 알게 되는 비트수를 계산하며 무엇보다 두 개의 90/150 CA로 구성된 SI 생성기에 의해 생성되는 SI 수열을 분석한다.

Ⅲ. SI 생성기

국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃 CA(3- neighborhood CA)라 한다. 본 논문에서는 다루는 90/150 CA는 각 셀이 다음상태로 전이될 때 사용되는 전이규칙이 규칙 90과 150의 조합으로만 이루어진 CA를 의미하며 전이규칙 90과 150은 (8), (9)와 같다.

$$\text{규칙 } 90 : q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t) \quad (8)$$

$$\text{규칙} 150 : q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \quad (9)$$

전이규칙 90과 150은 XOR논리로 이루어져 있으므로 CA의 다음 상태를 구하는 전이함수는 행렬로 표현된다. 이 행렬을 상태전이행렬(state transition matrix)이라 하며 90/150 CA의 상태전이행렬은 (10)과 같은 삼중 대각행렬이다.

$$T = \begin{pmatrix} d_1 & 1 & 0 & \cdots & 0 \\ 1 & d_2 & 1 & \cdots & 0 \\ 0 & 1 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \quad (10)$$

여기서 d_i는 i번 째 셀에 적용된 전이규칙으로, 규칙 90이면 '0'이고 규칙 150이면 '1'이다. 또한 $t_{i,i+1} = t_{i-1,i} = 1\ (i = 1, 2, \cdots, n)$을 만족한다. 이를 간단히 $T = < d_1, d_2, \cdots, d_n >$로 나타낸다.

Gong에 의해 제안된 삽입수열(interleaved sequences) [5]은 같은 특성다항식을 갖는 수열을 초기수열벡터를 각각 달리하여 얻어진 각각의 수열을 사이사이에 끼워 넣어 얻어지는 수열을 말한다. 그림 5는 삽입수열 생성기이다.

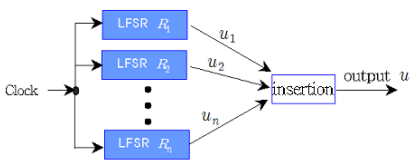


그림 5. 삽입수열 생성기
Fig. 5. The interleaving generator

SI 생성기[7]는 두 개의 CA $\mathbb{C}_1$과 $\mathbb{C}_2$가 이용되며 $\mathbb{C}_1$은 $\mathbb{C}_2$에 의해서 생성되는 수열의 일부분을 선택하기 위한 목적으로 사용된다. 주어진 SI 생성기에 의해서 생성되는 키수열은 $\mathbb{C}_2$에 의해서 생성되는 각 셀의 PN 수열의 수축된 형태가 되며 동시에 각 셀에서 출력되는 비트를 순차적으로 출력하기 때문에 수축과 삽입이 동시에 일어나는 수열이 된다. 즉, CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 클럭신호가 가해짐에 따라서 CA $\mathbb{C}_1$의 출력이 '1'이면 CA $\mathbb{C}_2$의 각 셀의 출력이 키 수열의 일부가 되고, 반면에 CA $\mathbb{C}_1$의 출력이 '0'이면 CA $\mathbb{C}_2$의 출력이 무시된다. 이러한 SI 생성기를 수학적으로 모델링하자. 최대길이를 갖는 두 개의 90/150 CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 대하여 $\mathbb{C}_1$의 길이가 m이고 $\mathbb{C}_2$의 길이가 n일 때 $\gcd(m,n) = 1$이라 하자. 각 상태전이행렬이 T_1, T_2이고 $\mathbb{C}_1$의 초기상태를 u_0, $\mathbb{C}_2$의 초기상태를 v_0라 하면 (T_1, u_0)를 이용하여 $2^m - 1$번 상태를 전이시켜 $(2^m - 1) \times m$행렬 A와 (T_2, v_0)를 이용하여 $2^n - 1$번 상태를 전이시켜 $(2^n - 1) \times n$행렬 B를 얻는다. A의 m개의 열 중 j번째 열 A_j를 선택하여 (11)과 같은 $(2^n - 1)(2^m - 1) \times (n+1)$행렬 $S = (s_{ij})$를 구한다.

$$S = \begin{pmatrix} B & A_j \\ \vdots & \vdots \\ B & A_j \end{pmatrix} \quad (11)$$

임의의 A_j에 대하여 0의 개수는 $2^{m-1} - 1$이고, 1의 개수는 2^{m-1}이다. 그러므로 식 (11)에서 $n+1$열 중 0의 개수는 $(2^{m-1} - 1)(2^n - 1)$이다. 행렬 S에서 $s_{i,n+1} = 0$이면 i번 째 행을 제거한 후 $n+1$열을 제거하여 얻은 행렬 S_I는 (12)와 같다.

$$S_I = \begin{pmatrix} k_0 & k_1 & \cdots & k_{n-1} \\ k_n & k_{n+1} & \cdots & k_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ k_{(2^{m-1}(2^n-1)-1)n} & k_{(2^{m-1}(2^n-1)-1)n+1} & \cdots & k_{2^{m-1}(2^n-1)n-1} \end{pmatrix} \quad (12)$$

S_I의 각 열은 $\mathbb{C}_2$의 각 셀에서 출력된 PN수열의 수축된 형태이다. (13)의 수열 $\{K\}$를 SI수열(shrunken-interleaved sequence)라 한다.

$$\{K\}=[k_0, k_1, \cdots, k_{2^{m-1}(2^n-1)n-1}] \tag{13}$$

<정리 1> 두 개의 CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 대하여 $\mathbb{C}_1$의 특성다항식이 m차 원시다항식이고, $\mathbb{C}_2$의 특성다항식이 m과 서로소인 n차 원시다항식 $f(x)$ 라 하면 SI 수열의 주기는 $2^{m-1}(2^n-1)n$와 같다.

(증명) $\mathbb{C}_1$과 $\mathbb{C}_2$의 길이 m과 n이 서로소이므로 $\mathbb{C}_1$과 $\mathbb{C}_2$의 주기 2^m-1과 2^n-1도 서로소이다. 따라서 식 (11)은 (2^n-1)개의 B와 (2^m-1)개의 A 를 붙여서 만들게 되므로 S의 크기는 $(2^n-1)(2^m-1)\times(n+1)$이다. A의 임의의 한 열 A_j에는 1의 개수가 2^{m-1}개 이므로 S로부터 얻어진 S_I의 행 수는 $2^{n-1}(2^{m-1}-1)$이다. 또 열의 수가 n이므로 SI 수열의 주기는 $2^{m-1}(2^n-1)n$이다.

<정리 2> 두 개의 CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 대하여 $\mathbb{C}_1$의 특성다항식이 m차 원시다항식이고, $\mathbb{C}_2$의 특성다항식이 m과 서로소인 n차 원시다항식 $f(x)$ 라 하면 SI 수열의 최소다항식은 (15)와 같고 선형복잡도 LC는 (16)과 같다.

$$[f^*(x^n)]^{2^{m-1}} \tag{14}$$

$$LC=2^{m-1}\cdot n^2 \tag{15}$$

여기서 $f^*(x)$는 식(4)의 $p(x)$이다.

(증명) $\mathbb{C}_1$과 $\mathbb{C}_2$에 의해 생성된 SI 수열 $\{K\}$를 n개씩 나누어 행으로 나열하면 (12)와 같고 이 때 $k_0, k_n, k_{2n}, \cdots$는 $\mathbb{C}_2$의 각 셀에 의해 출력된 PN 수열의 수축된 형태로 수축생성기에 의해생성된 수축수열과 같은 형태이다. 그러므로 $\mathbb{C}_2$의 각 셀에서 생성된 PN 수열의 특성다항식이 $f(x)$ 이므로 $f(x)$ 의 원시근을 α라 할 때, $k_0, k_n, k_{2n}, \cdots$의 최소다항식은 (4)와 (5)에 의해 $[f^*(x)]^{2^{m-1}}$ 이고 이런 수축수열이 n가 삽입된 형태이므로 $[f^*(x^n)]^{2^{m-1}}$ 를 만족한다. 또한 선형복잡도는 주어진 수열의 최소다항식의 차수이므로 $f(x)$ 가 n차이므로 $[f^*(x^n)]^{2^{m-1}}$ 의 차수는 $2^{m-1}\cdot n^2$이다.

<예제 2> 3-셀 $\mathbb{C}_1$의 상태전이행렬 T_1와 4-셀 $\mathbb{C}_2$의 상태전이행렬 T_2가 $T_1=<0,1,1>$, $T_2=<0,1,0,1>$라 하면 T_2의 특성다항식은 x^4+x+1이다. 초기 상태벡터를 $u_0=(001)$, $v_0=(0001)$라 하면 SI수열 생성 과정은 그림 6과 같다.

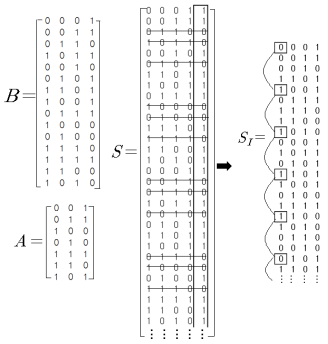


그림 6. SI 수열생성 과정
Fig. 6. The process of generation of SI sequence

그림 6에서와 같이 S_I의 각 열은 $\mathbb{C}_2$의 각 셀에서 생성되는 PN수열의 수축형태이다. 따라서 SI 생성기에 의해 얻은 SI수열의 주기는 정리 1에 의해 240이다. S_I의 첫 열을 $c_{01}, c_{11}, c_{21}, \cdots$라 할 때 $c_{01}, c_{41}, c_{81}\cdots$이 A_j의 같은 1에 대해 영향을 받은 성분이므로 A_j에 1의 개수가 2^{m-1}개 이므로 A_j에서 같은 성분 1에 대해 영향을 받는 비트끼리 열로 나열하면 그림 7과 같다. 그림 7의 각 열의 특성다항식은 x^4+x^3+1으로 모두 동일하다. 즉 SI 수열 역시 삽입수열의 관점으로 해석할 수 있는데 수축수열과 달리 복합된 삽입수열로 해석할 수 있다.

그림 7. SI 수열
Fig. 7. The SI sequence

$\mathbb{C}_2$의 특성다항식이 $f(x)$일 때, 각 열의 특성다항식은 $f(x)$의 상반다항식 $f^*(x)$이며 같은 특성다항식을

가지며 다양한 초기벡터에 의해 생성된 $2^{m-1} \cdot n$개의 PN 수열이 삽입된 형태이다. 그러므로 생성된 SI 수열의 특성다항식은 $f^*(x^{2^{m-1} \cdot n})$으로 예제 2에서 생성된 SI 수열의 특성다항식은 (16)과 같다.

$$f^*(x^{2^{m-1} \cdot n}) = (x^{16})^4 + (x^{16})^3 + 1 = x^{64} + x^{48} + 1 \qquad (16)$$

Ⅳ. SI 수열의 분석

SI 생성기에 의해 생성된 SI 수열의 일부를 알 때, 이를 이용하여 알려지지 않은 다른 비트를 알아내는 방법을 제안한다. 두 개의 CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 대하여 $\mathbb{C}_1$의 길이가 m이고 $\mathbb{C}_2$의 길이가 n이며 $\mathbb{C}_2$의 특성다항식이 n차 원시다항식 $f(x)$ 인 SI 생성기로부터 k개의 비트 $z_0, z_1, \cdots, z_{k-1}$(= z)을 알고 있다고 하자. 주어진 SI수열을 삽입수열로 생각할 수 있으므로 식 (4)에 의해 z는 $f^*(x)$ 에 의해 생성되는 수열로 (17)과 같이 $2^{m-1} \cdot n$개의 쌍으로 나눌 수 있다.

$$\begin{array}{l} (z_0, z_l, z_{2l}, \cdots) \\ (z_1, z_{l+1}, z_{2l+1}, \cdots) \\ \quad\vdots \\ (z_{l-1}, z_{2l-1}, z_{3l-1}, \cdots) \end{array} \qquad (17)$$

여기서 $l = 2^{m-1} \cdot n$이다. 이 때 $z_0, z_l, z_{2l}, \cdots$ 를 적당히 선택하여 유한체를 이용하여 새로운 비트를 알 수 있으며 식 (17)의 모든 쌍에 대해 할 필요 없이 $z_0, z_l, z_{2l}, \cdots$ 만 고려하면 된다. 만약 $k = 2^{m-1} \cdot n^2$이면 식 (17)의 모든 순서쌍이 각 n개의 성분으로 이루어지므로 각 순서쌍에 대하여 n개의 성분을 초기 상태로 하여 $f^*(x)$ 을 통해 모든 비트스트림을 알 수 있으므로 k는 $2^{m-1} \cdot n^2$보다 작은 경우에 대하여 다루도록 한다. 예를 들어 그림 7의 SI 수열 중 일부인 연이은 40($=k$)개의 비트열'10001110111111000011 10110010010101110 100'(= z)를 알고 있다고 하자. 그림 8은 주어진 z를 이용하여 새로운 비트열을 생성하는 과정을 나타낸다. 그림 8에서 z_0는 40개 비트 z를 나타낸다. z_{16}은 z에서 z_{16}부터 z_{39}까지 24개 비트를 나타내며, z_{32}은 z에서 z_{32}부터 z_{39}까지 8비트를 나타낸다.

즉 $l = 2^{m-1} \cdot n = 16$일 때 $\lceil k/l \rceil$ 개의 부분 수열 $z_0, z_l, z_{2l}, \cdots z_{pl}$를 만든다. 여기서 $p = \lceil k/l \rceil - 1$을 만든다. $z_l, z_{2l}, \cdots z_{pl}$중 한 개 이상의 수열을 선택하여 XOR하고 그 결과와 z_0를 XOR하여 수열을 재구성한다.

```
z0: 1000111011111110000111101100 ......
z16: 0011101100100101011110100
z32: 01110100
-------------------------------------
z0 ⊕ z16: 1011010111011001010011 11
z0 ⊕ z32: 11111010
z0 ⊕ z16 ⊕ z32: 11000001
```

그림 8. SI 수열의 재구성
Fig. 8. Reconstruction of SI sequence

그림 8에서 $z_0 \oplus z_{16} = z_0 \oplus z_l$에 대하여 z_0는 1, $z_l = \alpha$이라 하면 $1 + \alpha = \alpha^{12}$이다. 이 때 α는 $f^*(x)$의 원시근이다. $\alpha^{12} = z_{192}$이므로 따라서 $z_0 \oplus z_{16}$열은 z_{192}부터 연이은 24 비트를 의미한다. 같은 방법으로 $1 + \alpha^2 = \alpha^9$이므로 $z_0 \oplus z_{32}$은 z_{144}부터 연이은 8 비트를 나타낸다. $1 + \alpha + \alpha^2 = \alpha^7$이므로 $z_0 \oplus z_{32}$은 z_{112}부터 연이은 8 비트를 나타낸다. 따라서 주어진 연이은 40개의 비트들로부터 새로운 38 비트를 알 수 있다. 표 2는 정리 2를 기초로 한 SI수열의 일부를 알 때 이를 이용하여 새로운 비트를 재구성하는 알고리즘이다.

<정리 3> 두 개의 CA $\mathbb{C}_1$과 $\mathbb{C}_2$에 대하여 $\mathbb{C}_1$의 길이가 m이고 인 $\mathbb{C}_2$의 길이가 n이고 $\mathbb{C}_2$의 특성다항식이 $f(x)$인 SI 생성기에 의해 생성된 SI수열의 일부인 k비트를 알 때 가로챈 k개의 비트로부터 재구성할 수 있는 수열의 최대 비트수(NK)는 $NK = 2^p(k-(p-1) \cdot l) - (k+l)$ 이다.

여기서 $l = 2^{m-1} \cdot n$이고, $p = \lceil k/l \rceil - 1$이다.

(증명) k개의 비트로 p개의 부분수열 $z_0, z_l, z_{2l}, \cdots z_{pl}$를 만들면 각 부분수열의 비트수는 $k, k-l, k-2l, \cdots, k-pl$이다. z_0를 반드시 선택하고, 재구성된 수열의 비트수가 $k-l$인 경우는 $z_0 \oplus z_l$에 의해 재구성하는 경우이다. 일반적으로 재구성된 수열의 비트수가 $k-hl$인 경우는 z_0와 z_{hl}이 선택되고 $0 < i < h$인 z_{il}이 선택되거나 그렇지 않은 경우로 나누어지기 때문

에 경우의 수는 2^{h-1}가지이다. 따라서 재구성할 수 있는 최대비트수는 식 (18)과 같다.

$$\sum_{h=1}^{p}(k-hl)\cdot 2^{h-1}=2^{p}(k-(p-1)l)-(k+l) \qquad (18)$$

표 2. SI 수열 재구성 알고리즘
Table 2. The Algorithm for reconstruction of SI sequence

Input : $\mathbb{C}_1$의 길이 m, $\mathbb{C}_2$의 길이 n과 특성다항식 $f(x)$, k비트의 SI수열의 일부(z)
Output : 새롭게 재구성된 SI수열과 시작위치(po)
Step 1. $l=2^{m-1}\cdot n$, $p=\lceil k/l \rceil-1$를 계산한다.
Step 2. 주어진 z를 이용하여 p개의 부분수열 $z_0, z_l, z_{2l}, \cdots z_{pl}$를 구한다.
Step 3. for h=1 to p
(a) 부분수열 $z_0 \oplus a_1 z_l \oplus a_2 z_{2l} \oplus \cdots \oplus a_{h-1} z_{(h-1)l} \oplus z_{hl}$를 구한다. ($a_i \in \{0,1\}$)
(b) $1+a_1\alpha+a_2\alpha^2+\cdots+a_{h-1}\alpha^{h-1}+\alpha^h=\alpha^T$를 만족하는 T를 계산한다. 여기서 α는 $f^*(x)$의 원시근이다.
(c) po=$l\cdot T$를 계산한다.

V. 결론

본 논문에서는 두 개의 LFSR로 이루어진 수축생성기에 비하여 훨씬 효과적으로 긴 주기를 생성하면서 비선형성을 잃지 않는 SI 수열을 생성할 수 있는 생성기로 90/150 최대길이를 갖는 CA 두 개로 이루어진 SI 생성기를 분석하였다. 수축생성기에서 생성된 수축수열이 삽입수열로 분석할 수 있는 것과 같은 원리로 이를 확장하여 SI 수열을 삽입수열로 분석할 수 있음으로 보이고 SI 생성기에 의해 생성된 수열의 일부를 알 때 출력된 수열의 새로운 비트를 알아내는 효과적인 알고리즘을 제안하였으며 유한체론을 바탕으로하여 가로챈 부분수열로부터 떨어진 위치까지 정확히 계산할 수 있음을 보였다.

참고문헌

[1] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1997.

[2] D. Coppersmith, H. Krawczyk, and Y. Mansour, “The shrinking generator,” Lecture Notes in Computer Science 773, pp. 22-39, 1993.

[3] W. Meier and O. Staffelbach, "The self-shrinking generator," Lecture Notes in Computer Science, Advanced in Cryptology Eurocrypt ’94, pp. 205-214, 1995.

[4] S.A. Choi and K.C. Yang, "Balanced Shrinking Generator," Lecture Notes in Computer Science 2587, pp. 213-226, 2003.

[5] A.F. Sabater and D.G. Martinez, “Modelling nonlinear sequence generators in terms of linear cellular automata,” Applied Mathematical Modelling, Vol. 31, pp. 226-235, 2007.

[6] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, “New synthesis of one-dimensional 90/150 linear hybrid group cellular automata” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 26(9), pp. 1720-1724, 2007.

[7] U.S. Choi, S.J. Cho, H.D. Kim, Y.H. Hwang and S.T. Kim, "Nonliear Pseudorandom Sequences Based on 90/150 LHGCA," Lecture Notes in Computer Science 5192, ACRI 2008, pp. 471-477, 2008.

[8] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext-only," IEEE Transactions on Computers, Vol. C-34, pp. 81-85, 1985.

[9] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," Journal of Cryptology, Vol. 1(3), pp. 159-176, 1989.

[10] B, Zhang, H. Wu, D. Feng and F. Bao, "A Fast Correlation Attack on the Shrinking Generator," CT-RSA 2005, Lecture Notes in Computer Science 3376, pp. 72-86, 2005.

[11] M. Hell and T. Johansson, "Two new attacks on the self-shrinking generator," IEEE Transactions on INformation Theory, Vol. 52(8), pp. 3837-3843, 2006.

[12] B. Zhang and D. Feng, "New Guess-and-Determine Attack on the Self-Shrinking Generator," Lecture Notes in Computer Science 4284, Advances in Cryptology – ASIACRYPT 2006, pp. 54-68, 2006.
[13] A.F. Sabater and P.C. Gil, "Concatenated Automata in Cryptanalysis of Stream Ciphers," Lecture Notes in Computer Science 4173, ACRI 2006, pp. 611-616, 2006.
[14] A.F. Sabater and P.C. Gil, "Cryptanalytic Attack on Cryptographic Sequence Generators: The Class of Clock-Controlled Shrinking Generators," Lecture Notes in Computer Science 5073, Computational Science and Its Applications – ICCSA 2008, pp. 668-679, 2008
[15] A.F. Sabater, M.E. Pazo-Robles and P.C. Gil. "A simple linearization of the self-shrinking generator by means of cellular automata," Neural Networks Vol. 3. pp.461-464, 2010.
[16] R.J. McEliece, "Finite Fields for Computer Scientists and Engineers" Kluwer Academic Publishers, 1987.
[17] G. Gong, "Theory and applications of q-ary interleaved sequences," IEEE Transactions on Information Theory, Vol. 41, pp. 400-411, 1995.

저자소개

최언숙(Un-Sook Choi)

1992년 2월: 성균관대학교 산업공학과 학사
2000년 2월: 부경대학교 응용수학과 석사
2004년 2월: 부경대학교 응용수학과 박사
2004년 3월～2006년 2월: 영산대학교 자유전공학부 단임교수
2009년 8월: 부경대학교 정보보호협동과정 박사
2006년 3월～현재:동명대학교 미디어공학과 전임강사
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년 ～ 현재 : 부경대학교 응용수학과 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론