위상이동차를 이용한 수축 생성기의 분석

황윤희* · 조성진**· 최언숙***

Analysis of Shrinking Generator Using Phase Shifts

Yoon-Hee Hwang* · Sung-Jin Cho** · Un-Sook Choi***

요 약

원시다항식을 특성다항식으로 갖는 두 개의 LFSR로 구성된 수축 생성기를 삽입 생성기로 해석하고, 생성된 수열들 간의 위상이동차(phase shift)에 대하여 분석한다. 또한 위상이동차를 이용하여 수축 생성기에 의하여 생성된 수열의 부분수열을 알 때 나머지 수열을 구하는 방법을 제안한다.

ABSTRACT

In this paper, we show that the shrinking generator with two LFSR whose characteristic polynomials are primitive is an interleaving generator and analyze phase shifts in shrunken sequence. Also for a given intercepted sequence of shrunken sequence, we propose the method of reconstructing some deterministic bits of the shrunken sequence using phase shifts.

키워드

키스트림 생성기, 수축 생성기, 삽입 생성기, 위상이동차

Key word

keystream generator, shrinking generator, interleaving generator, phase shift

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

접수일자 : 2010. 06. 25
심사완료일자 : 2010. 08. 24

Ⅰ. 서 론

대부분의 키스트림 생성기는 PN 수열을 출력하는 LFSR에 수축이나 삽입 또는 시각 제어 등과 같은 비선형적 요소를 결합하여 난수열을 발생한다. 이러한 키스트림 생성기는 높은 선형 복잡도와 긴 주기 그리고 좋은 통계적 성질을 가진 키 수열을 생성하고 구현한다[1]. 이렇게 비선형적 요소를 결합한 수열 생성기에는 수축 생성기, 삽입 생성기, 시각 제어 생성기, 자기 수축 생성기 등이 있으며, 이들 생성기들은 여러 연구자들에 의하여 제안되고, 분석되어졌다[2-10]. Sabater 등은 LFSR 기반의 수축 생성기에 의하여 생성되는 수축 수열과 같은 수열을 생성하는 생성기를 하나의 90/150 셀룰라 오토마타(Cellular Automata)를 이용하여 고안하였다[2]. 그러나 제안된 방법은 셀룰라 오토마타가 LFSR과 달리 각 셀에서 동일한 특성다항식을 가지는 수열을 출력할 수 있음을 고려하지 않고 있으며 90/150 그룹 셀룰라 오토마타의 주기와 수축 생성기에 의하여 생성되는 수축 수열의 주기가 같다고 해도 초기 수열벡터에 따라 주기보다 훨씬 짧은 길이의 수열을 생성 할 수 있음을 간과하였다. 이런 문제점을 극복하기 위하여 Choi 등은 [9]에서 두 개의 90/150 최대 길이를 갖는 셀룰라 오토마타로 이루어진 수축-삽입 생성기를 제안하였다.

또한 스트림 암호의 공격 알고리즘이 Meier 등[11]에 의하여 제안되었다. 이 공격기법은 최근 LFSR 기반 스트림 암호 뿐만 아니라 일반적인 스트림 암호의 안정성 분석에 기본적인 분서방법으로 활용되고 있다. 수축생성기와 자기 수축 생성기에 대한 고속 상관공격이 Zhang 등[12]에 의하여 제안되었다. 이후 Sabater 등은 수축 생성기에 의하여 생성된 수열의 일부를 알 때, 90/150 셀룰라 오토마타를 이용하여 분석하는 방법을 제안하였다[1].

본 논문에서는 이러한 키스트림 생성기들 중 하나인 수축 생성기(shrinking generator)를 삽입 생성기(interleaving generator)와 관련하여 분석하고, 이를 이용하여 수축 생성기를 공격한다.

Ⅱ. 수축 생성기 분석

2장에서는 수축 생성기와 삽입 생성기에 대하여 간단히 소개하고, 수축 생성기를 삽입 생성기로 해석한다.

삽입 생성기는 두 개 이상의 LFSR에 의하여 생성된 수열을 생성될 때 마다 순서별로 삽입함으써 각각의 수열에서 생성된 선형성을 없애는 수열 생성기이다. 이 때, 보다 긴 주기를 생성하기 위하여 각각의 LFSR은 원시다항식을 특성다항식으로 가진다. 예를 들어 다음과 같은 두 개의 LFSR로 이루어진 삽입 생성기로 키스트림 수열을 생성하여 보자.

표 1. 삽입 생성기에 사용되는 LFSR-1과 LFSR-2
Table 1. LFSR-1 and LFSR-2 of shrinking generator

	특성다항식	초기값
LFSR-1	x^3+x+1	001
LFSR-2	x^3+x+1	100

LFSR-1에 의하여 생성된 수열 $\{a_i\}$와 LFSR-1에 의하여 생성된 수열 $\{b_i\}$에 의하여 생성된 삽입 수열 $\{c_i\}$는 다음과 같다.

$$\{a_i\} : 0010111 = a_1 a_2 \cdots$$
$$\{b_i\} : 1001011 = b_1 b_2 \cdots$$
$$\{c_i\} : 01001001101111 = a_1 b_1 a_2 b_2 \cdots$$

다음으로 수축 생성기는 두 개의 LFSR에 결합으로 이진 수열을 생성한다. 이 때, 보다 긴 주기를 생성하기 위하여 각각의 LFSR은 원시다항식을 특성다항식으로 가지며 각각의 주기는 서로소가 되게 구성한다.

두 LFSR 중에 제어를 하는 LFSR-1은 수열 $\{a_i\}$를 생성하고, LFSR-1에 의하여 LFSR-2에 의해 생성된 수열 $\{b_i\}$가 출력 수열 $\{c_i\}$를 생성한다고 하자. 그러면 $a_i = 1$이면 $c_j = b_i$이고, $a_i = 0$이면 b_i를 삭제함으로써 수축 수열 $\{c_i\}$가 생성된다. 그림 1은 수축 생성기의 구조이다.

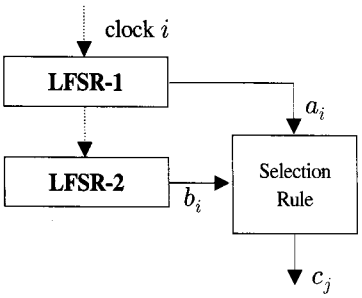

그림 1. 수축 생성기의 구조
Fig. 1. The structure of shrinking generator

예제 1] 수축 생성기의 두 LFSR을 다음과 같이 두자.

표 2. 삽입 생성기에 사용되는 LFSR-1과 LFSR-2
Table 2. LFSR-1 and LFSR-2 of shrinking generator

	특성다항식	초기값
LFSR-1	x^3+x+1	001
LFSR-2	x^4+x^3+1	0001

그러면 $\{a_i\}$, $\{b_i\}$에 의하여 생성되는 $\{c_i\}$는 다음과 같다.

$\{a_i\}$: 0010111001011100101110010111⋯
$\{b_i\}$: 0001111010110010001111010110⋯
$\{c_i\}$: 0111010001111110⋯

이 때 생성되는 수축 수열의 한 주기를 생성하기 위해서 LFSR-1의 주기 $7(=2^3-1)$과 LFSR-2의 주기 $15(=2^4-1)$가 서로 소이므로 LFSR-1이 15번 반복되어야 하며 이 때 길이 7인 한 주기 안에 1이 4번 생성되고 이것에 의하여 LFSR-2에서 4개의 비트가 15번 출력되어 수축 수열의 주기는 $4\times15=60$이다. 이 때 수축 수열의 주기를 최대로 하기 위하여 LFSR-1와 LFSR-2의 주기는 서로 소여야 한다. 이에 대하여 다음 정리가 성립한다.

일반적으로 n과 m이 서로 소이면 2^n-1과 2^m-1은 서로소이므로 다음 정리를 만족한다.

정리 1] 특성다항식을 원시다항식으로 가지는 n차 LFSR-1의 주기와 $n+1$차 LFSR-2의 주기는 서로 소이다.

증명) 특성다항식을 원시다항식으로 가지므로 두 LFSR의 주기는 각각 2^n-1과 $2^{n+1}-1$이다.

$2^{n+1}-1=(2^n-1)\times2+1$이므로 유클리드 알고리즘에 의하여 $2^{n+1}-1$와 2^n-1의 최대공약수는 2^n-1와 1의 최대공약수와 같으므로 $2^{n+1}-1$와 2^n-1의 최대공약수는 1이다. 따라서 두 LFSR의 주기인 2^n-1과 $2^{n+1}-1$은 서로 소이다.

즉, LFSR-1의 차수가 n이면 LFSR-2의 차수를 $n+1$로 하여 각각의 주기가 서로 소가 되게 할 수 있다. 그러면 이 두 LFSR에 의하여 생성되는 수축 생성기의 주기는 LFSR-1이 LFSR-2의 주기 $2^{n+1}-1$만큼 반복되고, 반복될 때 마다 LFSR-1의 1의 개수인 2^{n-1}만큼 출력되므로 $2^{n-1}\times(2^{n+1}-1)$이 된다.

다음으로 이렇게 생성되는 수열의 특징을 살펴보자.

n차 특성다항식 $C_1(x)$를 특성다항식으로 갖는 LFSR-1과 m차 특성다항식 $C_2(x)$을 갖는 LFSR-2에 의하여 구성된 수축 생성기에서 $C_2(\alpha)=0$ (여기서, $\alpha\in GF(2^m)$)을 만족하는 α가 존재하여 다음을 만족한다.

$$C_2(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})\cdots(x-\alpha^{2^{m-1}}) \tag{1}$$

그러면 이러한 수축 생성기에 의하여 생성된 수열에 의하여 생성된 수열을 2^{n-1}비트씩 끊어서 나열하였을 때 생기는 $(2^m-1)\times2^{n-1}$ 행렬의 각 열의 특성다항식은 다음과 같다[1].

$$C_3(x)=(x-\alpha^E)(x-(\alpha^E)^2)(x-(\alpha^E)^{2^2})\cdots(x-(\alpha^E)^{2^{m-1}}) \tag{2}$$

여기서, $E=2^n-1$이다.

예제 1에서와 같이 $\{a_i\}$는 주기가 7이며 0010111이 반복된다. LFSR-2에 의하여 생성된 수열 $\{b_i\}$를 $b_1b_2b_3\cdots b_{15}b_1b_2\cdots$이라 두면 $\{c_i\}$는

$c_1c_2c_3 \cdots c_{60} \cdots$
$= b_3b_5b_6b_7b_{10}b_{12}b_{13}b_{14}b_2b_4b_5b_6b_9b_{11}b_{12}b_{13} \cdots$

이다. 이렇게 수축된 수열 $\{c_i\}$를 LFSR-2의 차수인 4비트 씩 끊어서 나열하면 다음과 같다.

$$\begin{array}{c} c_1c_2c_3c_4 \\ c_5c_6c_7c_8 \\ \vdots \\ b_3\ b_5\ b_6\ b_7 \\ b_{10}b_{12}b_{13}\ b_{14} \\ b_2\ b_4\ b_5\ b_6 \\ b_9\ b_{11}b_{12}\ b_{13} \\ \vdots \end{array}$$

위 각 열은 특성다항식이 $c_2(x) = x^4 + x^3 + 1$이 주어진 LFSR-2가 생성한 수열에서 7칸 씩 띄어가며 생성하는 수열이므로 $c_2(\alpha) = 0$을 만족하는 α에 대하여 그 수열을 생성하는 LFSR의 특성다항식은 다음과 같다.

$$\begin{aligned} & c_2(\alpha^7) \\ & = (x-\alpha^7)(x-(\alpha^7)^2)(x-(\alpha^7)^{2^2})(x-(\alpha^7)^{2^3}) \\ & = x^4 + x + 1 \end{aligned} \tag{3}$$

다시 말해 $\{c_i\}$를 4비트 씩 끊어서 나열하면 다음과 같고 각 열은 특성다항식이 $x^4 + x + 1$인 LFSR에 의하여 생성된 PN 수열인 0001001101011111이고, 특히, 각각은 위상이동차를 가지고 있다. 즉, 생성된 수축 수열을 삽입 수열로 해석한다면 특성다항식을 $x^4 + x + 1$로 가지는 LFSR을 이용한 삽입 생성기가 됨을 알 수 있다.

0111
0100
0111
1110
0011
0011
1001
1101
0000
1010
0100
1101
1010
1110
1001

위 각 열들의 위상이동차는 수축 생성기의 LFSR-1에서 생성된 수열과 관련이 있다. 위 열들의 위상이동차를 i 열이 $i+1$ 열이 되기 위해 밑으로 이동하는 양이라고 하자. 예를 들어 1열이 2열이 되기 위하여 4칸을 밑으로 이동하여야 하므로 1열에 대한 2열의 위상이동차는 4이고, 2열이 3열이 되기 위하여 2칸을 밑으로 이동하여야 하므로 2열에 대한 3열의 위상이동차는 2이다. 같은 방법으로 3열에 대한 4열의 위상이동차는 2이다.

LFSR-1에서 생성된 수열이 0010111…이므로 첫 번째 1인 위치가 3번째이므로 1열은 LFSR-2에서 생성된 수열에서 세 번째 비트인 b_3을 출력하고 LFSR-1에서 생성된 수열의 주기가 7이므로 7칸씩 띄어가면서 $b_3b_{10}b_2 \cdots$의 순서로 출력하고, 같은 방법으로 2열은 LFSR-1에서 생성된 수열 0010111…에 의하여 $b_5b_{12}b_4 \cdots$의 순서로 출력하고 있다. 따라서 1열에 대한 2열의 위상이동차는 세 번째 원소인 b_3가 2열에서 b_5 다음으로 몇 번째 만에 나오는가를 구하는 것이다. 이는 LFSR-1의 주기인 7씩 건너 띄어가는 수열임을 알고 있으므로 다음을 만족하는 n을 구하는 문제가 된다.

$$3 \equiv 5 + (2^3 - 1) \times n \pmod{2^4 - 1} \tag{4}$$

여기서 k을 구하기 위하여 식을 정리하면

$$\begin{aligned} & (2^3-1) \times k \equiv 3 - 5 \equiv -2 \pmod{2^4-1} \\ & \Rightarrow (2^3-1) \times k \equiv 2^4 - 1 - 2 \equiv 13 \pmod{2^4-1} \\ & \Rightarrow 7k \equiv 13 \pmod{2^4-1} \end{aligned} \tag{5}$$

이고, $k = 4$이며 이것이 1열에 대한 2열의 위상이동차가 된다. 이를 이용하여 각 열의 위상이동차를 구하는 것을 일반화하면 다음 정리를 얻는다.

정리 2] n차 원시다항식을 특성다항식으로 가지는 LFSR-1과 m차 원시다항식을 특성다항식으로 가지는 LFSR-2로 구성된 수축 생성기에 의하여 생성된 수열을 $2^n - 1$비트씩 잘라서 나열한 행렬을 A라 하면, A의 각 열은 같은 수열이며 위상이동차를 갖는다. (단, $n < m$)

증명) n차 원시다항식을 특성다항식으로 가지는 LFSR-1과 m차 원시다항식을 특성다항식으로 가지는

LFSR-2로 구성된 수축 생성기의 수열 생성과정은 LFSR-1에 의해 생성된 수열의 1의 위치에서 LFSR-2에 의해 생성된 수열을 출력하는 것이다. 따라서 LFSR-1에 의하여 생성된 수열의 주기가 2^n-1이므로 LFSR-1에 의하여 생성된 수열에서 첫 번째 1이 j_1번째 존재한다면 j_1+2^n-1번째에도 1이 존재한다. 이를 일반화하면 i 번째 1이 j_i번째 존재한다면 j_i+2^n-1번째에도 1이 존재한다. 여기서 i는 LFSR-1에 의해 생성된 수열의 한 주기 동안 1의 개수가 2^{n-1}개 이므로 $1 \le i \le 2^{n-1}$이다. 따라서 LFSR-2에 의하여 생성된 수열을 $b_1b_2\cdots$라 하면, 수축 생성기에 의하여 생성된 수열은 $b_{j_1}b_{j_2}\cdots b_{j_{2^{n-1}}}b_{j_1+2^n-1}b_{j_2+2^n-1}\cdots b_{j_{2^{n-1}}+2^n-1}\cdots$이다.

한편, 수축생성기에 의하여 생성된 수열을 2^{n-1}비트씩 끊어서 나열하면 다음과 같다.

$$\begin{matrix} b_{j_1} & b_{j_2} & \cdots & b_{j_{2^{n-1}}} \\ b_{j_1+2^n-1} & b_{j_2+2^n-1} & \cdots & b_{j_{2^{n-1}}+2^n-1} \\ & \vdots & & \end{matrix} \tag{6}$$

위의 각 열에서 k번째 원소와 $k+1$번째 원소는 LFSR-2에 의하여 생성된 수열 $b_1b_2\cdots$에서 2^n-1칸씩 건너 띄어 가며 출력하게 되므로 각 열은 위상이동차를 갖지만 같은 수열임을 알 수 있다.

정리 3] n차 원시다항식을 특성다항식으로 갖는 LFSR-1과 m차 원시다항식을 특성다항식으로 갖는 LFSR-2로 구성된 수축 생성기에 의하여 생성된 수열을 2^n-1비트씩 잘라서 나열한 행렬을 A라 하자. (단, $n<m$)

LFSR-1에 의하여 생성된 주기가 2^n-1인 수열에서 i 번째 1이 있는 위치가 수열의 j_i번째일 때 i 번째 수열에 대한 $i+1$번째 수열의 위상이동차는 다음 식을 만족하는 k 이다.

$$j_i \equiv j_{i+1}+(2^n-1)\times k \pmod{2^m-1} \tag{7}$$

증명) n차 원시다항식을 특성다항식으로 가지는 LFSR-1과 m차 원시다항식을 특성다항식으로 가지는 LFSR-2로 구성된 수축 생성기에 의하여 생성된 수열을 2^{n-1}비트씩 끊어서 나열하면 식(6)과 같고 정리 2에 의하여 각 열은 같은 수열이다. 여기서 i 번째 열에 대한 $i+1$번째 열의 위상이동차를 k 라 하면 $i+1$번째의 첫 번째 원소 $b_{j_{i+1}}$가 2^n-1씩 띄어 갈 때 k 번만에 b_{j_i}와 같아지는 것을 의미한다. 이 때 LFSR-2에 의해 생성되는 수열의 주기가 2^m-1이므로 다음을 만족하는 k가 위상이동차가 된다.

$$j_i \equiv j_{i+1}+(2^n-1)\times k \pmod{2^m-1} \tag{8}$$

예제 2] 3차 원시다항식 x^3+x+1을 특성다항식으로 가지는 LFSR-1과 4차 원시다항식을 특성다항식으로 가지는 LFSR-2로 구성된 수축 생성기에 의하여 생성된 수열을 4($=2^{3-1}$)비트씩 잘라서 나열한 행렬을 A라 하면 A 의 각 열의 위상이동차는 LFSR-1에 의하여 생성된 수열은 0010111…이므로 정리 2에서 i 와 j_i는 다음과 같다.

표 3. i번째 1의 위치 j_i
Table 3. ith position of 1 (j_i)

	1	2	3	4	5	6	7
	0	0	1	0	1	1	1
i			1		2	3	4

여기서, $j_1=3, j_2=5, j_3=6, j_4=7$이다. 그러면 정리 3에 의하여 3번째 수열에 대한 4번째 수열의 위상이동차 k는 다음 식을 만족한다.

$$\begin{aligned} 6 &\equiv 7+(7)\times k \pmod{15} \\ -1 &\equiv 7k \pmod{15} \\ 14 &\equiv 7k \\ k &= 2 \end{aligned} \tag{9}$$

따라서 3번째 열에 대한 4번째 열의 위상이동차가 2임을 알 수 있다.

특히, 본 논문에서 가능한 긴 주기를 생성하기 위하여 조건으로 n차 원시다항식을 특성다항식으로 가지는 LFSR-1과 $n+1$차 원시다항식을 특성다항식으로 가지

는 LFSR-2로 구성된 수축 생성기의 경우 특별한 형태를 가진다.

즉, n차 원시다항식을 특성다항식으로 가지는 LFSR-1과 $n+1$차 원시다항식을 특성다항식으로 가지는 LFSR-2로 구성된 수축 생성기에 의하여 생성된 수열을 $n+1$비트씩 잘라서 나열한 행렬을 A라 하자. 그러면 A의 각 열의 위상이동차는 다음을 만족한다. LFSR-1에 의하여 생성된 주기가 2^n-1인 수열에서 i번째 1이 있는 위치가 수열의 j_i번째일 때 i번째 수열에 대한 $i+1$번째 수열의 위상이동차 k는 다음 식을 만족한다.

$$\begin{aligned} & j_i \equiv j_{i+1} + (2^n-1)\times k \pmod{2^{n+1}-1} \\ & \Rightarrow -(2^n-1)\times k \equiv j_{i+1} - j_i \pmod{2^{n+1}-1} \\ & \Rightarrow (2^{n+1}-1-2^n+1)\times k \equiv j_{i+1} - j_i \pmod{2^{n+1}-1} \\ & \Rightarrow 2^n \times k \equiv j_{i+1} - j_i \pmod{2^{n+1}-1} \end{aligned} \tag{10}$$

따라서 다음 표가 성립한다.

표 4. 위상이동차 k
Table 4. phase shift k

$j_{i+1}-j_i$	k
1	2
2	4
3	6
⋮	⋮
l	$2\times l$

다시 말하면, LFSR-1에서 1의 위치가 연이어 있으면 대응하는 두 열의 위상이동차가 2이고 1의 위치가 1001로 세 비트가 띄어져 있으면 대응하는 두 열의 위상이동차가 6이 됨을 바로 알 수 있다.

Ⅲ. 수축 생성기 공격

3장에서는 2장에서 수축 생성기를 삽입 생성기로 재해석하고 위상이동차를 분석한 내용을 이용하여 수축 생성기의 LFSR-1의 원시다항식이 주어지고 수축 생성기에 의하여 생성된 수열의 일부를 알 때 나머지 수열을 알아낼 수 있음을 예를 들어 보인다.

예제 3] 어떤 수축 생성기의 LFSR-1의 원시다항식이 x^3+x+1이고 LFSR-2의 차수가 4라 할 때, 수축 생성기에 의하여 생성된 수열의 주기가 $(2^4-1)\times 2^{3-1}=60$이고, 여기서 이 수열의 일부인 011101000111임을 안다면 수축 생성기에 의하여 생성된 수열의 나머지를 알 수 있다. LFSR-1이 원시다항식에 의하여 수열 0010111을 생성함을 알 수 있으므로 정리 2에 의하여 위상이동차가 다음과 같음을 알 수 있다.

1열에 대한 2열의 위상이동차 = 4
2열에 대한 3열의 위상이동차 = 2
3열에 대한 4열의 위상이동차 = 2

생성된 수열의 일부를 다음과 같이 나열하면

0	1	1	1
0	1	0	0
0	1	1	1
1	1	1	0

이고 이를 위상이동차를 이용하여 빈 칸을 채워나가면 다음과 같이 짙은 숫자의 비트를 알아낼 수 있다.

0	1	1	1
0	1	0	0
0	1	1	1
1	1	1	0
	0	**1**	**1**
	0	**1**	**1**
	0	**0**	**1**
	1	**0**	**1**
		0	**0**
		1	**0**
			0
			1

Ⅳ. 결 론

원시다항식을 특성다항식으로 갖는 두 개의 LFSR-1과 LFSR-2에 의하여 구성되는 수축 생성기를 두 개 이상

의 LFSR에 의하여 생성된 수열을 생성될 때마다 순서별로 삽입하여 선형성을 없애는 삽입 생성기로 재해석하고, 생성된 수열들 간의 위상이동차를 LFSR-1에서 생성되는 수열의 1의 위치를 이용하여 분석하고 위상이동차를 구하였다. 또한 이를 이용하여 수축 생성기에 의하여 생성된 수열의 부분수열을 알 때 나머지 수열을 구할 수 있음을 보였다.

참고문헌

[1] A.F. Sabater and P.C. Gil, "Concatenated Automata in Cryptanaysis of Stream Ciphers," ACRI 2006, LNCS 4173, pp. 611-616, 2006.

[2] A.F. Sabater and D.G. Marinez, "Modelling Nonlinear Sequence Generator in terms of Linear Cellular Automata," Applied Mathematical Modelling, Vol. 31, pp. 226-235, 2007.

[3] D. Coppersmith, H. Krawczyk and Y. Mansour, "The Shrinking Generator", LNCS 733, pp. 22-39, 1994.

[4] J.D. Golic, "Correlation Analysis of the Shrinking Generator," LNCS 2139, pp. 440-457, 2001.

[5] A. Kanso, "Clock-Controlled Shrinking Generator of Feedback Shift Registers, LNCS 2727, pp. 443-451, 2003.

[6] T. Johnasson, "Reduced Complexity Correlation Attacks on Two Clock-Controlled Generators," LNCS, 1514, pp. 342-356, 1998.

[7] J.D. Golic and L. O'Connor, "Embedding and Probabilistic Correlation Attacks on Clock-Controlled Shift Registers," LNCS 950, pp. 230-243, 1995.

[8] J.D. Golic, "Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers," LNCS 921, pp. 248-262, 1995.

[9] U.S. Choi, S.J. Cho, H.D. Kim, Y.H. Hwang and S.T. Kim, "Nonlinear Pseudorandom Sequense Based on 90/150 LHGCA," LNCS 5192, ACRI 2008, pp. 471-477, 2008.

[10] W. Meier and O. Staffelbach, "The Self-Shrinking generator," LNCS, Advanced in Cryptology Eurocrypt '94, pp. 205-214, 1995.

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

[12] B. Zhang, H. Wu, D. Feng and F. Bao, "A Fast Correlation Attacts on the Shrinking Generator," CT-RSA 2005, LNCS 3376, pp. 72-86, 2005.

저자소개

황윤희(Yoon-Hee Hwang)

2002년 2월 : 부경대학교 통계학과 학사
2004년 2월 : 부경대학교 응용수학과 석사
2008년 8월 : 부경대학교 정보보호학과 박사
※관심분야 : 셀룰라 오토마타론, 정보보호, 유한체, 컴퓨터 구조론, VLSI

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
988년 2월: 고려대학교 수학과 박사
1988년 ~ 현재 : 부경대학교 수리과학부 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론, VLSI

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 학사
2000년 부경대학교 응용수학과 석사
2004년 부경대학교 응용수학과 박사
2004년~2006년 2월 영산대학교 자유전공학부 단임교수
2006년 3월~현재 동명대학교 멀티미디어공학과 전임강사
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론, VLSI