수축수열의 위상이동차 공격법

최언숙* · 조성진** · 황윤희*** · 김한두****

Attack using Phase Shifts of Shrunken Sequence

Un-sook Choi* · Sung-jin Cho** · Yoon-hee Hwang*** · Han-doo Kim****

요 약

높은 선형복잡도와 낮은 상관관계를 갖는 의사난수열은 통신 및 암호에 널리 사용된다. 본 논문에서는 수축생성기에의해 생성된 수축수열을 삽입수열로 해석하여 분석하고 후 위상이동차를 분석하여 수축수열의 일부 정보로부터 수축수열 모두를 알아내는 방법을 제안한다.

ABSTRACT

Pseudo-random sequences with high linear complexity and low correlation function values are widely used in communication and cryptology. In this paper, we study the properties of interleaved sequences generated by shrinking generator. And we give a method for obtaining the shrunken sequence from a partial description of the shrunken sequence by using the phase shifting of PN sequences generated by shrinking generator.

키워드

위상이동차, 수축수열, 삽입수열, 스트림암호, 선형복잡도

Ⅰ. 서 론

높은 선형복잡도와 낮은 상관관계를 갖는 의사난수열(pseudo-random sequence)은 통신 및 암호에 널리 사용된다. 이러한 품질 좋은 수열을 생성하기 위한 다양한 방법이 많은 연구자들에 의해 연구되었다[1-13]. 이런 연구결과에 의하면 생성된 수열은 영수열과 일반적으로 랜덤이 우수하다고 알려진 수열로서 하나의 특성다항식과 다양한 초기벡터에 의해 생성된 위상이동차를 갖는 의사난수열로 분해될 수 있다. 두 종류의 이러한 수열이 있다. 한 종류는 복합수열(multiplexed sequence), 시각제어수열(clock- controlled sequence)과 같이 하나의 LFSR이 다른 LFSR에 의해 출력되는 비트를 제어하여 생성시키는 수열이다[1-6]. 또 다른 종류는 m-수열, Kasami 수열, GMW 수열, No 수열 등과 같이 하나 또는 그 이상의 LFSR과 정방향 이송(feed-forward) 함수를 사용하여 생성시키는 수열이다[7-13].

스트림암호는 대규모의 데이터를 매우 빠르게 암호화하기 위해 사용되는 비밀키 암호시스템이다. 이 시스템은 긴 주기의 난수열을 발생시켜 전송하고자 하는 평문과 비트별 XOR 연산을 하여 암호문을 생성하는 방식으로서 의사 난수열을 발생시켜야 한다. 일반적으로 스트림암호의 키수열은 긴 주기, 높은 선형복

* 동명대학교 미디어공학과(choies@tu.ac.kr) ** 교신저자 : 부경대학교(sjcho@pknu.ac.kr)
*** 부경대학교 응용수학과(yhhwang@pknu.ac.kr) **** 인제대학교 컴퓨터응용과학부, 기초과학연구소(mathkhd@inje.ac.kr)
접수일자 : 2010. 12. 13 심사(수정)일자 : 2011. 01. 11 게재확정일자 : 2011. 02. 09

잡도를 가지고, 한 주기 내에서 1의 개수와 0의 개수의 차가 1이하여야 안전하다고 한다. Coppersmith 등[3]에 의해 제안된 수축생성기(shrinking generator)는 3개의 LFSR에 의해 구현된 교대단계생성기(alternating step generator)에 비해 작동 방법이 간단하고, 구현이 용이하며 고속 암호화가 요구되는 응용분야에 적합한 암호로 인식되고 있다. Gong 등[13]은 삽입수열(interleaved sequence)을 정의하고 수축생성기에 의해 생성된 수축수열(shrunken sequence)을 삽입수열로 해석하여 분석하였다. 2004년 Cho 등[14]은 최대주기 90/150 셀룰라 오토마타의 위상이동차(phase shift)를 계산하는 방법을 연구하였다. 최근 Sabater 등은 수축생성기에 의해 생성된 수축수열을 90/150 셀룰라 오토마타를 이용하여 분석하였다[4-6]. 그러나 Sabater가 제안한 방법으로는 수축수열의 일부를 알더라도 수축수열 전부를 알아낼 수는 없다.

본 논문에서는 LFSR기반의 수축수열을 삽입수열로 해석한 후 위상이동차를 분석한다. 또한 제어레지스터의 길이와 생성레지스터의 특성다항식을 알 때, 수축수열의 일부 정보로부터 이 수열과 위상이동차의 관계를 이용하여 수축수열 모두를 알아내는 방법 및 알고리즘을 제안한다.

II. 예비지식 및 기존연구

Coppersmith 등[3]에 의해 제안된 수열 생성기는 두 개의 LFSR R_1과 R_2로 구성된다. 이때 R_1은 제어레지스터로 R_2는 생성레지스터로 그 역할을 담당한다. 제어 레지스터 R_1에 의해 생성되는 수열을 이용하여 생성 레지스터 R_2에서 생성되는 수열 중 일부를 선택하여 수열을 생성하므로 제안된 수열 생성기에 의해 생성되는 수열은 R_2에 의해 생성되는 수열의 수축된 수열이다. 수축된 이 수열을 수축수열(shrunken sequence)이라 하고 이 수열의 생성기를 수축생성기(shrinking generator)라 한다. 그림 1은 수축수열을 생성하는 수축생성기의 구조이다.

수열의 생성방법은 그림 1에서 R_1과 R_2에 클럭신호가 주어질 때마다 R_1의 출력이 1이면 R_2의 출력이 키수열에 포함되고, R_1의 출력이 0이면 R_2의 출력은 배제된다. 이 수축생성기는 생성된 키수열의 비트의 위치가 고정되지 않는다는 점이 장점이고, 긴 주기, 높은 선형복잡도, 우수한 통계적 특성 등 암호학적으로 좋은 성질을 가지고 있다.

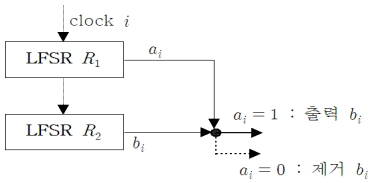

그림 1. 수축생성기의 구조
Fig. 1 The shrinking generator

<정리 1[3]> 두 개의 LFSR R_1과 R_2로 구성된 수축생성기에 대하여 R_1의 길이가 L_1이고, R_2의 길이가 L_2이면 수축생성기에 의해 생성된 수축수열의 주기 Ord와 선형복잡도 LC는 식(1)과 (2)를 만족한다.

$$Ord = (2^{L_2}-1)2^{(L_1-1)} \tag{1}$$

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

<정의 1[9]> 시간 t에서 i번째 열의 출력수열을 s_i^t라 할 때, i열에 대한 j열의 위상이동차 h는 식(3)을 만족한다.

$$s_j^{t+h} = s_i^t \tag{3}$$

특성다항식이 같은 LFSR에 의해 생성되는 수열은 초기벡터에 따라 위상 이동차만 있을 뿐 모두 같은 수열로 해석할 수 있다. 예를 들어 길이가 4이고 그 특성다항식이 x^4+x^3+1인 LFSR에 대하여 초기벡터에 따른 출력수열은 표1과 같다. 초기벡터가 '0001'일 때 생성된 수열을 s_1라 하고 초기벡터가 '0100'일 때 생성된 수열을 s_2라 할 때, $s_2^{t+2} = s_1^t$을 만족하므로 s_1에 대한 s_2수열의 위상이동차는 2이다. 마찬가지로 $s_3^{t+12} = s_1^t$이므로 s_1에 대한 s_3수열의 위상이동차는 12이다.

특성다항식 $f(x)$에 의해 생성되는 모든 수열의 집합을 $G(f)$라 하자. 예를 들어 $f(x) = x^2+x+1$이라

하면 초기벡터는 00,01,10,11로 4가지이고 이 초기벡터에 의해 생성된 수열의 집합 $G(f)$는 식(4)와 같다.

$$G(f)=\{00000\cdots,011011\cdots,110110\cdots,101101\cdots\} \quad (4)$$

표 1. 다양한 초기벡터에 의해 생성된 의사난수열
Table 1. Pseudo-random sequence generated by various initial vectors

초기벡터	생성된 수열
$0001(s_2)$	000111101011001000111101011001…
$0100(s_2)$	010001111010110010001111010110…
$1111(s_3)$	111101011001000111101011001000…
$0011(s_4)$	001111010110010001111010110010…
$0101(s_5)$	010110010001111010110010001111…

$G(f)$에서 영수열을 제외한 모든 수열은 위상이동차가 다른 모두 동일한 수열로 해석할 수 있다. 이런 수열에 대한 기준으로 트레이스(trace)를 이용한다.

<정의 2[15]> n차 원시다항식 $f(x)$에 대하여 $f(\alpha)=0$인 원시근 α의 켤레들의 합을 α의 트레이스라 하고 $Tr_1^n(\alpha)$라 쓴다. 즉 $Tr_1^n(\alpha)$는 식(5)와 같다.

$$Tr_1^n(\alpha)=\alpha+\alpha^2+\alpha^{2^2}+\alpha^{2^3}+\cdots+\alpha^{2^{n-1}} \quad (5)$$

표2는 $f(x)$에 따른 α^i의 트레이스이다. 다음 예제는 수축수열의 생성과정을 설명한다.

표 2. $f(x)$에 따른 α^i의 트레이스
Table 2. Trace of α^i associated with $f(x)$

$f(x)$	$Tr_1^n(\alpha^i)$
x^3+x+1	1001011…
x^3+x^2+1	1110100…
x^4+x+1	000100110101111…
x^4+x^3+1	011110101100100…

<예제 1> LFSR R_1의 길이가 4이고 그 특성다항식이 x^4+x^3+1이며 초기벡터가 '0001'이라 하자. 그러면 R_1에 의해 생성되는 수열 $\{a_i\}$는 최대주기수열인 000111101011001…이고 주기는 15이다. R_2의 길이가 5, 특성다항식이 x^5+x^2+1, 초기벡터가 '01001'이면 R_2에 의해 생성되는 수열 $\{b_i\}$는 최대주기수열인 0100101100111110001101110101000… 이고 주기는 31이다. 이때 수축생성기에 의해 생성되는 수축수열 $\{c_i\}$는 주기가 $2^{4-1}\times 31=248$인 수열로 01010110 11010100…이다. 그림 2는 수축수열의 생성과정을 보여준다. 그림 2에서 첫 번째 열은 $\{a_i\}$이고 두 번째 열은 $\{b_i\}$이며 두 번째 열 중 색칠된 부분이 출력수열에 포함되는 수축수열 $\{c_i\}$를 나타내며 세 번째 열은 $\{b_i\}$중 수축수열로 출력되는 수열의 위치를 나타낸다.

Sabater 등은 수축수열을 Gong이 제안한 삽입수열로 해석하여 수축생성기에 의해 생성된 수열 중 일부를 알 때 90/150 셀룰라 오토마타를 이용하여 알지 못하는 새로운 비트스트림을 재구성하는 방법을 제안하였다[6]. 이 방법은 주어진 생성기로부터 출력된 키스트림 중 일부를 알고 있을 때, 이를 이용하여 알지 못하는 새로운 비트들을 계산하는 방법으로서 90/150 CA를 합성하여 키스트림을 이용한 부분삼각형을 만들고 다시 유한체를 이용하여 새로운 비트들을 재구성한다. 이 방법은 계산이 복잡하고 무엇보다 출력수열을 일부만 알아내는 것이지 모두 알아내기는 어렵다는 문제점을 가지고 있다.

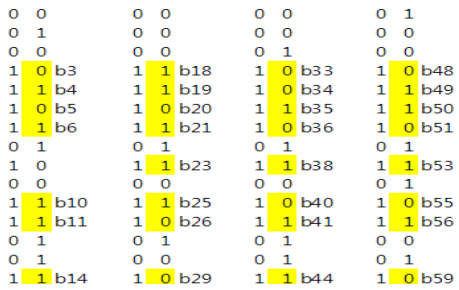

그림 2. 수축수열의 생성과정
Fig. 2. The generating process of a shrunken sequence

수축생성기에 대한 공격으로 [16]에서 위상이동차를 이용한 방법이 처음 소개되었다. 그러나 이 방법은 제어레지스터의 특성다항식과 생성레지스터의 길이를 알 때 가로챈 수열로부터 나머지 수열을 찾는 것으로

R_1에 대한 정보가 없으면 원수열을 알아낼 수 없다.

본 논문에서는 이러한 문제점을 극복하고 제어레지스터의 길이와 생성레지스터의 특성다항식을 알 때,생성되는 수열의 특성과 수축생성기에 의해 생성된 수축수열의 위상이동차를 계산하여 가로챈 키스트림의 일부를 이용하여 출력수열 전체를 알 수 있는 방법을 제안한다.

Ⅲ. 수축수열의 분석 및 위상이동차 공격법

수축 수열의 주기를 최대로 하기 위하여 LFSR R_1과 LFSR R_2의 주기는 서로 소이어야 한다. 일반적으로 n과 m이 서로 소이면 2^n-1과 2^m-1은 서로 소이다. R_1의 길이를 n, R_2의 길이를 $n+1$로 두고 각 LFSR에 대응하는 특성다항식을 원시다항식으로 두게 되면, 두 LFSR의 주기는 각각 2^n-1과 $2^{n+1}-1$이다. 그런데 $2^{n+1}-1=(2^n-1)\times 2+1$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. 따라서 두 LFSR에 의해 생성되는 수열은 수축수열의 주기 중 최대가 되는 가장 효과적인 수열이므로 본 논문에서는 R_1의 길이가 n이고 R_2의 길이가 $n+1$인 경우에 대해서만 분석하도록 한다.

<정리 2> 길이가 n인 LFSR R_1과 길이가 $n+1$인 LFSR R_2로 이루어진 수축생성기에 의해 생성되는 수축수열의 주기는 $2^{2n}-2^{n-1}$이다.

(증명) 두 LFSR의 길이가 서로 소이므로 수축수열의 한 주기가 생성되기 위해서는 R_1이 R_2의 주기인 $2^{n+1}-1$만큼 반복되고, R_1의 한 주기인 2^n-1에서 1의 개수가 2^{n-1}개 존재하므로 수축수열의 주기는 $(2^{n+1}-1)\cdot 2^{n-1}=2^{2n}-2^{n-1}$이 된다. □

수축수열을 $(2^{n+1}-1)\times 2^{n-1}$ 행렬로 표현한 것을 $\mathbb{C}_n$이라 하자. 그림 3은 예제 1에서 생성된 수축수열 $\mathbb{C}_4$이다. n차 다항식 $p_1(x)$를 특성다항식으로 갖는 R_1과 $n+1$차 다항식 $p_2(x)$을 특성다항식으로 갖는 R_2에 의하여 구성된 수축생성기에서 $p_2(\alpha)=0$ ($\alpha\in GF(2^m)$)을 만족하는 α가 존재하여 식(6)을 만족한다.

$$p_2(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})\cdots(x-\alpha^{2^n}) \quad (6)$$

이러한 수축 생성기에 의하여 생성된 수열에 의하여 생성된 수열을 2^{n-1}비트씩 끊어서 나열하였을 때 생기는 $(2^{n+1}-1)\times 2^{n-1}$ 행렬의 각 열의 특성다항식은 식(7)과 같다[4].

$$p_3(x)=(x-\alpha^E)(x-(\alpha^E)^2)(x-(\alpha^E)^{2^2})\cdots(x-(\alpha^E)^{2^n}) \quad (7)$$

여기서, $E=2^n-1$이다. 따라서 $\mathbb{C}_n$의 각 열의 특성다항식은 $p_2(x)$의 상반다항식이다.

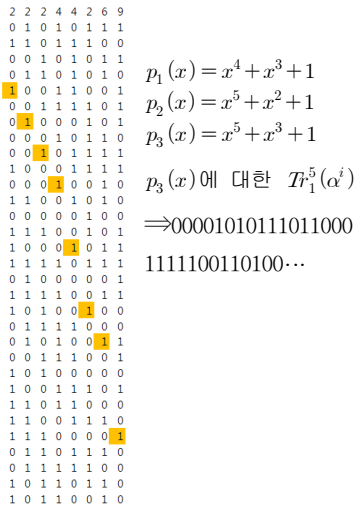

그림 3. 수축수열 $\mathbb{C}_4$

Fig. 3. The shrunken sequence $\mathbb{C}_4$

<예제 2> 그림 3의 $\mathbb{C}_4$의 각 열은 x^5+x^2+1에 의해 생성된 PN수열 중에서 x^4+x^3+1에 의해 생성된 PN수열의 1이 있는 위치에서 15칸씩 건너뛰면서 만들어진 PN수열로(그림 4), 그 특성다항식은 $p_2(x)=x^5+x^2+1$의 상반다항식인 x^5+x^3+1이다. □

길이가 n이고 초기벡터가 v인 제어레지스터 R_1에 의해 출력된 수열 $\mathbb{C}_n$을 b_i로 표현한 수열을 $B_{n,v}$라 하자. 그림 4(a)는 그림 3에서 출력된 수열 $\mathbb{C}_4$를 b_i로 표현한 수열 $B_{4,v}$의 일부이다. 또한 그림 4(b)는 예제 1의 조건에서 R_1의 초기벡터를 $v_1=\{1111\}$로 해서 얻어낸 수축수열 B_{4,v_1}의 일부이다. 그림 3과 그림 4를

통해 알 수 있듯이 $\mathbb{C}_n$의 각 열은 모두 같은 특성다항식을 가지며, 위상이동차가 있을 뿐이다. 따라서 $\mathbb{C}_n$의 i번 째 열은 $Tr_1^{n+1}(\gamma_i\alpha^i)$로 나타낼 수 있다. 이 때 α는 $p_2(x)$의 상반다항식 $p_2{}^*(x)(=p_3(x))$의 원시근이다. 또한 $B_{n,v}$의 첫 행의 b_i는 R_1에서 생성되는 수열 중 0을 제거하고 1의 위치에서만 b_i가 출력된 것으로 R_1의 초기벡터에 의해 결정된 것이다. 따라서 각 열의 위상이동차 γ_i를 결정하는 것은 $p_1(x)$와 R_1의 초기벡터이다.

b3 b4 b5 b6 b8 b10 b11 b14
b18 b19 b20 b21 b23 b25 b26 b29
b33 b34 b35 b36 b38 b40 b41 b44
b48 b49 b50 b51 b53 b55 b56 b59

(a) R_1의 초기벡터가 0001인 경우

b0 b1 b2 b3 b5 b7 b8 b11
b15 b16 b17 b18 b20 b22 b23 b26
b30 b31 b32 b33 b35 b37 b38 b41
b45 b46 b47 b48 b50 b52 b53 b56

(b) R_1의 초기벡터가 1111인 경우

그림 4. R_1의 초기벡터에 따른 $\mathbb{C}_4$

Fig. 4 $\mathbb{C}_4$ associative with initial vector of R_1

<정리 3> 차수가 n인 원시다항식과 초기벡터가 v인 LFSR R_1과 차수가 $n+1$인 원시다항식으로 구성된 LFSR R_2로 이루어진 수축생성기에 의해 생성된 수축수열 $\mathbb{C}_n$에 대하여 $\mathbb{C}_n$의 i열의 위상이동차를 γ_i라 하고, $B_{n,v}$의 첫 행의 i번 째 성분을 b_{n_i}라 하면 식(8)이 성립한다.

$$\gamma_{i+1}-\gamma_i = 2(n_{i+1}-n_i) \tag{8}$$

(증명) $\gamma_{i+1}-\gamma_i$는 $B_{n,v}$에서 i열이 $i+1$열이 $B_{n,v}$의 i열이 되기 위해 밑으로 이동하는 양이다. 즉 b_{n_i}가 $i+1$열에서 $b_{n_{i+1}}$ 다음으로 몇 번째 나타나는지를 의미한다. $B_{n,v}$의 각 열은 2^n-1만큼씩 건너 띄므로 $B_{n,v}$의 i열은 $b_{n_i}, b_{n_i+(2^n-1)}, b_{n_i+2(2^n-1)}, \cdots$이다. R_2의 길이가 $n+1$이므로 세 번째 성분은 $b_{n_i+2(2^n-1)} \equiv b_{n_i+(2^{n+1}-1)+1} \equiv b_{n_i+1} \pmod{2^{n+1}-1}$을 만족한다. 즉 식(9)와 같다.

$$b_{n_i}, b_{n_i+(2^n-1)}, b_{n_i+1}, b_{n_i+1+(2^n-1)}, \cdots \tag{9}$$

그러므로 $\gamma_{i+1}-\gamma_i = 2(n_{i+1}-n_i)$이다. □

그림 3의 $\mathbb{C}_4$는 R_1의 초기벡터가 '0001'일 때 $Tr_1^5(\alpha^i)$수열이 10000101011101100011111001101 00 이므로 γ_i는 4, 6, 8, 10, 14, 18, 20, 26이다. 여기서 $\gamma_{i+1}-\gamma_i$는 2, 2, 2, 4, 4, 2, 6 이다. b_{n_i}들에 대한 $n_{i+1}-n_i$이 (1, 1, 1, 2, 2, 1, 3, 4)이므로 $\gamma_{i+1}-\gamma_i$은 (2, 2, 2, 4, 4, 2, 6, 8)임을 확인 할 수 있다. R_1의 초기벡터가 {1111}일 때 γ_i는 29, 0, 2, 4, 8, 12, 14, 20 이다. 그러므로 $\gamma_{i+1}-\gamma_i$은 (-29(≡2), 2, 2, 4, 4, 2, 6) 이고 그림 4(b)에서 b_{n_i}에 대한 $n_{i+1}-n_i$이 (1, 1, 1, 2, 2, 1, 3, 4)이므로 정리 3을 만족함을 알 수 있다.

표 3. 가로챈 수열의 위상이동차를 찾는 알고리즘

Table 3. Algorithm for finding phase shifts of intercepted sequence

Input	R_1의 길이 n, R_2의 특성다항식 $p_2(x)$, 가로챈 수열 I
Output	$\mathbb{C}_n$의 이웃하는 열 사이의 위상이동차$\gamma_{i+1}-\gamma_i$
Step 1	I를 2^{n-1}비트씩 분할하여 2^{n-1}개의 열을 만든다.
Step 2	Stpe 1에서 얻은 2^{n-1}개의 벡터를 역순으로 하는 피봇벡터 P_i를 구한다.
Step 3	P_1으로 시작하는 길이가 $n+1$인 초기벡터를 정하여 $p_2(x)$를 특성다항식으로 하는 수열을 발생시킨다. 이 때 P_1의 길이가 $n+1$보다 작은 경우 0을 첨가하도록 한다.
Step 4	P_1부터 $P_{2^{n-1}}$까지 다음 과정을 반복하여 2^{n-1}개의 n_i값을 찾는다. (a) P_i를 품는 부분을 찾아 그 시작위치를 k_i로 두고 k_i에서부터 거리가 $2k$거리에 있는 벡터 중에서 P_{i+1}가 시작되는 위치를 찾아 $k_{i+1}-k_i$가 짝수가 되는 n_{i+1}를 찾는다. (b) 만약 그런 k_{i+1}가 존재하지 않으면 k_i의 다른 값을 찾아 (a)를 반복한다.
Step 5	2^{n-1}개의 k_i로부터 구한 $k_{i+1}-k_i$가$\gamma_{i+1}-\gamma_i$이다.

다음은 가로챈 키스트림으로부터 위상이동차를 이용한 공격법을 제안한다. Sabater는 R_1의 차수만 알고, R_2의 특성다항식을 아는 경우, 수축생성기에 의해 생성된 수축수열에서 24비트를 가로챘을 때 32비트를

더 알아내는 방법에 대하여 연구하였다[13]. 본 논문에서는 앞에서 분석한 위상이동차에 관한 정리를 이용하여 [13]과 동일한 조건인 R_1의 차수만 알고, R_2의 특성다항식을 알 때, 수축생성기에 의해 생성된 삽입수열에서 24비트를 가로챘다는 가정 하에 각 PN수열의 위상이동차를 계산해서 삽입수열을 모두 알아내는 방법에 대하여 제안한다. R_1의 길이가 n이고 R_2의 특성다항식이 $n+1$차 원시다항식 $p_2(x)$라 하자. 이 때 가로챈 수열을 I라 하자. 표3의 알고리즘을 통해 각 열에 대한 위상이동차를 알아내고 이 결과를 바탕으로 점차적으로 출력비트들을 찾아간다.

예를 들어 예제 1의 수축생성기에 대하여 $n=4$, $p_2(x)=x^5+x^2+1$의 정보만 안다고 가정하자. 그리고 24비트 수열 <001000010101100111100010>을 가로챘다고 가정하자. 이 수열을 I라 하자. I의 24비트를 8개의 열로 나열하면 그림 5(a)가 되고 주어진 5(a)의 각 열은 $p_2(x)$의 상반다항식을 따르므로 주어진 벡터를 역으로 읽은 수열의 특성다항식이 $p_2(x)$가 된다. 즉 5(b)의 각 열은 5(a)의 각 열을 역순으로 얻은 것이다. 그림 6은 첫 번째 피봇벡터를 포함하는 초기 벡터를 이용하여 $p_2(x)$에 의해 생성된 수열과 그 수열의 위치번호이다. 표 3은 가로챈 수열을 이용하여 $\mathbb{C}_n$의 이웃한 열 사이의 위상이동차인 $\gamma_{i+1}-\gamma_i$를 구하는 알고리즘이다

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

5(a)

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

5(b)

그림 5. 가로챈 수열과 피봇벡터
Fig. 5 Intercepted sequences and pivot vector

표 3의 알고리즘을 이용하면 주어진 예제의 경우 피봇벡터를 포함하는 위치는 k_i는 28, 30, 32, 36, 40, 42, 48, 56이다. 따라서 $\gamma_{i+1}-\gamma_i$는 2, 2, 4, 4, 2, 6, 8이다. 그림 7은 위 알고리즘을 이용하여 각 열에 대한 위상이동차를 바탕으로 각 열 사이의 관계를 통하여 점차적으로 새롭게 알게 되는 출력비트들을 찾아가는 과정이다.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0

30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1

그림 6. x^5+x^2+1를 특성다항식으로 갖는 PN 수열
Fig. 6 The PN sequence whose characteristic polynomial is x^5+x^2+1

그림 7에서 5, 6, 7열에서 연이은 5개의 벡터를 얻었으므로 $p_2^*(x)$를 이용하여 $\mathbb{C}_n$을 구한다.

	2	2	4	4	2	6	8
0	0	0	1	1	1	1	0
0	0	1	0	0	1	0	1
1	0	0	1	0	1	0	0
0	0	0			0		
1	1	0	0	1	0		
0	0	0	1	0			
1	1	1	0	1	1	1	
1	0	0	0		0	1	
1	1	1	0	0	1	1	1
0	1	0	0	1		0	0
1	1	1	1	0	0	0	0
1	0	1		0	1		
0	1	1		0	0	1	
0	1	0		0	0	0	
0	0	1		1	0	1	1
	0	1			0		1
	0	0			1	0	1
	1	0				1	0
	1	0				0	0
	1	1				0	
		1				0	1
		1				0	0
		1				1	1
							0
							1
							0
							0
							0
							0
							1

그림 7. 위상이동차를 이용한 $\mathbb{C}_n$의 복원과정
Fig. 7 The reconstruction process of $\mathbb{C}_n$ using phase shifts

Ⅳ. 결 론

본 논문에서는 수축생성기에 의해 생성되는 수축수열을 삽입수열로 해석한 후 위상이동차를 분석하여 가로챈 수축수열의 일부 정보인 R_1의 차수와 R_2의 특성다항식을 이용하여 제안한 알고리즘으로부터 $\mathbb{C}_n$의 이웃한 열 사이의 위상이동차인 $\gamma_{i+1}-\gamma_i$를 구하고 이를 이용하여 출력된 수축수열을 모두 알아내는 방법을 제안하였다.

감사의 글

본 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행되었습니다.
(NRF-2010-371-B00 008)

참고 문헌

[1] S. M. Jennings, "Multiplexed sequences: Some properties of the minimum polynomial," in Proc. EUROCRYPTO'82 Lecture Notes in Computer Science, vol. 149. New York: Springer_Verlag, 1983.

[2] T. Beth and F. Piper, "The stop-and-go generator" in Advances in Cryptology, Proc. EUROCRYPTO'84. New York: Springer-Verlag, 1985.

[3] D. Coppersmith, H. Krawczyk and Y. Mansour, "The shrinking generator," in; Proc. CRYPTO'93, in: LNCS 773, Springer-Verlag, pp. 22-39, 1994.

[4] A. Fuster-Sabater, P. Caballero-Gil, "Concatenated automata in cryptanalysis of stream ciphers," Proc. of ACRI 2006, LNCS 4173, Springer-Verlag, pp. 611-616, 2006.

[5] A. Fuster-Sabater and D. Guia-Martinez, "Modelling nonlinear sequence generators in terms of linear cellular automata," Applied Mathematical Modelling, 31 pp.226-235. 2007.

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

[7] S. A. Tretter, "Properties of PN2 sequences," IEEE Trans. Inform. Theory, vol. IT-20, pp. 295-297, 1974.

[8] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," Proc. IEEE, vol. 64, no. 12, pp. 1715-1729, Dec. 1976.

[9] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Sci. Lab., Univ. of Illinois, Urbana, Tech. Rep. R-285 (AD632574), 1966.

[10] R. A. Scholtz and L. R. Welch, "GMW sequences," IEEE Trans. Inform. Theory, vol. IT-30, no. 3, pp. 548-553, May 1984.

[11] A. Klapper, A.H. Chan, and M. Goresky, "Cascaded GMW sequences," IEEE Trans. Inform. Theory, vol. 39, no. 1, pp. 177-183, Jan. 1993.

[12] J. S. No and P. V. Kumar, "A new family of binary pseudo random sequences having optimal periodic correlation properties and large linear span," IEEE Trans. Inform. Theory, vol. 35, no. 2, pp. 371-379, Mar 1989.

[13] G. Gong, "Theory and applications of q-ary interleaved sequences," IEEE Trans. Inform. Theory 41(2), pp. 400-411, 1995.

[14] S. J. Cho et al., "Computing phase shifts of maximum-length 90/150 cellular automata," in: Proc. ACRI 2004, in: LNCS 3305, Springer-Verlag, pp.31-39, 2004.

[15] R. Lidi and H. Niederreiter, Finite fields, Encyclopaedia of Mathematics and its Applications, Vol. 20. Reading, MA: Addison-Wesley, 1983.

[16] 조성진, 최언숙, 김한두, 안현주, "수축생성기에 기반한 비선형 수열의 분석," 한국전자통신학회, 5(4), pp. 412-417, 2010.

저자 소개

최언숙(Un-sook Choi)

2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 대학원 응용수학과 졸업(이학박사)
2009년 부경대학교 대학원 정보 보호학과 졸업(공학박사)
현재 동명대학교 미디어공학과 전임강사
※ 관심분야 : 셀룰라 오토마타론, 정보보호

조성진(Sung-jin Cho)

1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년~현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

황윤희(Yoon-hee Hwang)

2004년 부경대학교 대학원 응용수학과 졸업(이학석사)
2008년 부경대학교 대학원 정보보호학과 졸업(공학박사)
※ 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 컴퓨터응용과학부 정교수, 기초과학연구소
※ 관심분야 : 전산수학, 셀룰라 오토마타론