論文96-33A-2-2

초기조건과 비선형 함수와의 상관관계를 이용한 스트림 암호시스템 분석

(Analysis of stream cipher system with initial condition and nonlinear function)

金 志 弘 *, 李 晩 榮 **

(Ji Hong Kim and Man Young Rhee)

요 약

비선형 함수를 도입한 선형귀환 치환레지스터로 구성된 키스트림 생성기에 대하여, 기존의 방법인 상관공격에 의하여 비선형 결합함수의 형태를 찾고자 하는 노력과는 달리, 본 논문에서는 원래의 키스트림 생성기의 출력중 일부를 알고 있는 상태에서, 키스트림 생성기를 구성하고 있는 LFSR의 귀환결합 형태와 사용된 비선형 결합함수의 최고차수를 알고 있으면, 원래의 키스트림 생성기의 출력계열과 동일한 출력계열을 생성시킬 수 있는 등가시스템과, 이때 필요한 출력비트의 최소갯수에 대하여 논한다.

Abstract

Key stream generator consisting of several linear feedback shift registers with a nonlinear combining function have been applied in stream cipher system. Most of the papers until now have been focusing on correlation attack and analysis of key stream generator with nonlinear combining function. Given some part of key stream sequences, we can generate identical output sequences with original key stream sequences if the feedback connection and the maximum order of nonlinear combination function are known.

Ⅰ. 서 론

스트림 암호시스템의 키스트림 생성기(key stream generator)에 의해 생성되는 계열이나 CDMA(Code Division Multiple Access)방식이 도입된 이동통신 시스템에서 사용되는 파이럿계열 혹은 긴부호계열들은 모두 선형귀환 치환레지스터(LFSR: Linear Feedback Shift Register)를 사용하여 생성한다. 이러한 LFSR을 이용하여 생성되는 스트림 암호시스팀의 최대 단점은 출력계열이 이진(modulo 2) 연산에 의해 생성되기 때문에 귀환결합구조를 알지 못하는 경우에도 2N (N:LFSR의 단수)비트의 출력문을 알면, N개의 선형 방정식을 해석함으로서, 시스팀을 분석할 수 있기 때문에, 완벽한 랜덤 특성을 얻을 수 없다는 점이다. 따라서 이러한 단점을 해결하기 위하여 선형귀환 치환레지스터 계열들에 비선형 배치구조를 도입하여 출력계열들이 훌륭한 의사난수(pseudorandom)특성과 높은 선형복잡도(linear complexity) [6,8]를 얻기 위한 수많은 연구가 수행되어 졌으며, 그 중에서 선형귀환 치환레지스터에 의해 생성되는 최대장계열에 대하여, 선형복잡도(linear complexity)와 무작위 특성(randomness property)를 높이기 위하여 비선형 결합함수를 도입한 Rueppel의 방법[7]에 대하여 논한다.

비선형 결합함수를 적용한 경우에 대하여 지금까지의 연구는 비선형 함수에 의한 상관관계에 의하여 시

* 正會員, 世明大學校 電子工學科
(Dept. of Electronic Eng., Semyung Univ.)
** 正會員, 漢陽大學校 電子通信工學科
(Dept. of Elec. Comm., Hanyang Univ.)
接受日字:1994年2月21日, 수정완료일:1996年1月11日

스템의 구조를 파악하는 방법[2,9,10]이 대부분이었으나, 본 논문에서는 선형시스템에서의 출력계열의 특성과 비선형 결합함수를 도입한 경우의 출력계열의 특성을 분석하고, 키스트림 생성기의 귀환결합 방정식과 비선형 결합함수의 최대 차수만을 알면, 원래의 키스트림 생성기의 출력계열과 동일한 출력계열을 생성할 수 있는 등가키스트림 생성기를 구하고, 등가시스템을 구하기 위해 요구되는 출력계열의 최소 비트수에 대하여 구한다.

Ⅱ. 선형 시스템 해석

1. 의사난수계열

일반적으로 난수계열이란 유한계열에 의해서는 생성이 불가능하기 때문에 이와 유사한 무작위 계열을 LFSR 시스템에 의해 생성하고, 이를 의사 난수계열(pseudorandom sequence)라고 한다. 이러한 의사 난수계열은 평형성(balance), 연속성(run), 상관(correlation), 중첩(superposition), 데시메이션(decimation) 특성[3,14]을 가지며,원시다항식을 귀환탭계수로 하는 LFSR에 의해 생성될 수 있다. 또한 이러한 계열은 유한체상에서 최대주기를 가지므로 이를 최대장 계열(maximum length seuence)이라고 한다. 일반적으로 유한체상에서의 최대장 계열의 갯수는 (정리-1)에 의해 주어진다.

(정리-1) 유한체 $GF(2^N)$에서의 요소는 N단 LFSR의 내용(contents)에 의해 생성될 수 있으며, 이때 생성되는 최대장 계열을 생성하는 귀환결합의 갯수는 식(1)과 같다[3].

$$\lambda_p(N) = \frac{\phi(2^N-1)}{N} \qquad (1)$$

예로서 N=5인 경우에는 $GF(2^5)$에서의 최대장 계열을 생성할 수 있는 귀환 결합의 갯수는 Euler's ϕ function $\phi(2^5-1) = \phi(31) = 30$ 이므로 $\lambda_p(5) = 6$ 이며, 귀환결합방정식을 8진법으로 표시하면 45, 51, 57, 67, 73, 75 가 된다[3].

2. trace 함수

trace 함수는 식(2)과 같이 정의되며, n이 m으로 나누어 질때, $GF(p^n)$의 원소 α를 부속장(subfield)인 $GF(p^m)$으로 매핑시킬 수 있는 함수이다[11,12].

$$tr_m^n(a) = \sum_{i=0}^{n/m-1} a^{p^{mi}} \qquad (2)$$

또한 trace 함수는 다음과 같은 특성을 갖는다.

- $tr_m^n(a) = tr_m^n(a^{p^{mi}})$, $a \in GF(p^n)$, $0 \le i \le (n/m)-1$
- $tr_m^n(a\alpha+b\beta) = a\, tr_m^n(\alpha) + b\, tr_m^n(\beta)$,
  all $a, b \in GF(p^m)$, and $\alpha, \beta \in GF(p^n)$
- $tr_m^n(a) = (n/m)a$, $a \in GF(p^m)$
- $tr_m^n(a) = b$, $b \in GF(p^m)$ 을 만족하는 해는
  $a \in GF(p^n)$에서 p^{n-m} 개의 해를 갖는다.
- 만일 $GF(p) \subset GF(p^m) \subset GF(p^n)$이면
  $tr_1^n(a) = tr_1^m(tr_m^n(a))$, $a \in GF(p^n)$ 가 된다.

(정리-2) 유한체 $GF(2^N)$에서 정수 r과 s가 동일한 cyclotomic coset에 속하면 식(3-a)의 관계가 성립되며, 이때 생성되는 출력계열(식 3-b)들은 동일한 초기상태하에서 발생되는 동일한 출력에 해당된다.[3,13]

$$tr(a^r) = tr(a^s), \quad a \in GF(2^N), \quad r,s \text{ 는 정수} \qquad (3\text{-a})$$

$$tr(a^r)^n = tr(a^s)^n, \quad a \in GF(2^N), \qquad (3\text{-b})$$

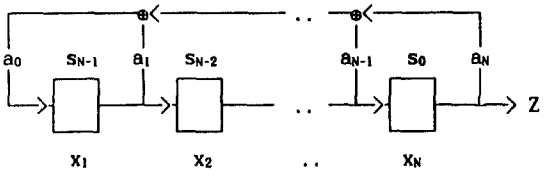

그림 1. 일반적인 LFSR 생성기
Fig. 1. General LFSR generator.

일반적으로 그림 1과 같은 N단의 선형귀환 치환레지스터에 의해 생성되는 순환계열 s_n 는 지연자(Delay Operator) D로 표시할 수 있다.

$$s_n + \sum_{j=1}^{N} a_j s_{n-j} = 0, \qquad n \ge N \qquad (4)$$

$$(D^N + \sum_{j=1}^{N} a_j D^{N-j})\, s_n = 0, \qquad n \ge 0 \qquad (5)$$

좌측의 괄호안의 식을 $f(D)$라 하면, 이는 최대 N개의 근을 갖는 특성방정식이다. 이러한 특성방정식에 의해 해당되는 계열을 발생시킬 수 있다.[5,12]

$$s_n = \sum_{i=1}^{N} A_i (a_i)^n \qquad (6)$$

식(6)에서 A_i는 선형귀환 치환레지스터의 초기치에 의해 결정되는 $GF(2^N)$의 요소(element)이며, α_i 는 특성방정식 $f(D)$의 서로 다른 근(root)에 해당한다.

식(6)에서 N차 원시다항식 $p(x)$를 귀환결합 방정식으로 사용하는 N단 LFSR 시스템에서의 근 α_i 는 α, α^2, α^4, α^8 .. $\alpha^{(2^{N-1})}$ 으로 표시된다. 그러므로 만약 어떤 일정한 초기상태($A_1=A_2=\ ..=A_N=1$)인 경우에 대하여, 생성되는 출력계열 s_n은 식(7)과 같이 trace 함수에 의해 표시될 수 있다.

$$s_n = \sum_{i=0}^{N-1} (\alpha^2)^n = tr(\alpha^n) \qquad (7)$$

만약 이러한 초기상태에서 d번 천이된 후의 LFSR의 출력계열은 다음과 같다.

$$s_{n+d} = \sum_{i=0}^{N-1} (\alpha^{2^i})^{n+d}$$

따라서 $tr(\alpha^n)$은 $A_1=A_2=..=A_N=1$ 로서, 초기상태 "0001"인 경우의 출력계열 s_n을 의미한다면, $tr(\alpha^{n+d})$ 는 $A_1=\alpha^d$, ... $A_N=(\alpha^{2^{N-1}})^d$ 로서, 초기상태 "0001"에서 d번 천이된 상태에서의 출력계열 s_{n+d}를 의미한다.

Ⅲ. 비선형 시스템 해석

1. 비선형 결합함수를 도입한 시스템

일반적으로 생성다항식을 귀환 결합계수로 하는 LFSR 시스템의 출력계열은 최대주기를 갖는 최대장 계열이 된다. 이러한 최대장 계열의 출력에 대하여 선형 복잡도와 비예측성을 높히기 위하여 그림 2와 같이 비선형 함수을 사용한 키스트림 생성기를 사용한다.

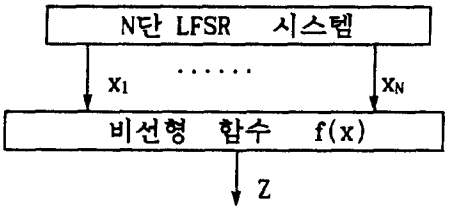

그림 2. 비선형 함수를 이용한 키스트림 생성기
Fig. 2. Key stream generator with nonlinear function.

N단 LFSR에 의해 생성된 각 단의 출력계열에 대하여 비선형 함수를 적용하기 위하여, LFSR의 첫번째 단의 출력계열을 x_1, 두번째 단의 출력계열을 x_2, ... N번째 단의 출력계열을 x_N 이라 한다. N단 키스트림 생성기에 사용된 비선형 결합함수의 형태는 식(8)과 같이 일반식으로 표시할 수 있다.

$$\begin{aligned} f(x) = \ & a_1x_1 + a_2x_2 + a_3x_3 + .. + a_Nx_N \\ & + a_{12}x_1x_2 + a_{23}x_2x_3 + a_{24}x_2x_4 \ldots \\ & + a_{123}x_1x_2x_3 + a_{124}x_1x_2x_4 + a_{125}x_1x_2x_5 \ldots \\ & + a_{1234}x_1x_2x_3x_4 + a_{1235}x_1x_2x_3x_5 \ldots \\ & + \ \ldots\ldots \\ & + a_{123\ldots N}x_1x_2x_3x_4 \ldots x_N \end{aligned} \qquad (8)$$

이때 출력계열의 계수 $a_{i_1}\ldots_{i_k}$ 는 식(9)와 같이 표현될 수 있다[10].

$$a_{i_1}\ldots_{i_k} = \sum_{x \in S_{i_1}\ldots_{i_k}} f(x) \qquad (9)$$

$$S_{i_1}\ldots_{i_k} = \{ x \mid x_j=0,\ \forall_j \notin I_{i_1}\ldots_{i_k} \}$$

$1 \le i_1 < i_2 < i_3 .. < i_k \le N$인 정수들의 집합을 $I_{i_1}\ldots_{i_k} = \{ i_1, i_2, .. i_k \}$ 라 정의한다.

이러한 비선형 결합함수를 도입한 LFSR 시스템(이하 키스트림 생성기라 함)의 첫번째 주기동안의 출력계열 Z는 키스트림 생성기의 각 단들 간의 자체 곱들의 항에 대한 선형결합 형태로 표시할 수 있다. N단 키스트림 생성기의 출력계열에 대한 최대 주기 $T=2^N-1$로 표시하면, 출력계열 Z는 식(10)과 같이 T ×T 형태의 곱행렬 P와 이들에 대한 계수행렬 A = $(a_1, a_2, a_3, \ldots, a_{123\ldots N})$ 의 곱형태로 표시될 수 있다.

$$\mathbf{Z} = \mathbf{P}^{\mathrm{T}} \cdot \mathbf{A} \qquad (10)$$

$$\mathbf{A} = (\mathbf{P}^{\mathrm{T}})^{-1} \cdot \mathbf{Z} \qquad (11)$$

식(11)은 임의의 출력계열 행렬과 주어진 초기상태를 이용하여 생성된 곱행렬의 역행렬을 곱하면, 주어진 초기상태하에서 키스트림 생성기에서 사용된 비선형 결합함수를 찾을 수 있음을 나타낸다. N단 LFSR 시스템의 각 단에서 출력을 취하면, 한주기동안 출력계열의 weight는 2^{N-1} 이며, LFSR 시스템의 2개의 단의 출력에 대하여 하나의 항으로 구성된 2차 비선형 결합함수를 적용하여 출력을 취하면, 한주기동안 출력계열의 weight는 2^{N-2} 이다. 또한 LFSR 시스템의 k개의 단의 출력에 대하여 하나의 항으로 구성된 k차 비선형 결합함수를 적용하여 출력을 취하면, 한주기동안 출력계열의 weight는 2^{N-k}가 된다. 따라서 다음과 같은 정

리가 성립한다.

(정리-3) 최대장계열을 생성할 수 있는 N단 LFSR 시스템에서 하나의 항으로 구성된 k차 비선형 결합함수를 적용하면 한주기 동안의 출력계열의 weight는 2^{N-k} 이다.

N차 원시다항식에 의해 구성되는 LFSR 시스템의 출력계열의 주기는 2^N-1이다. 비선형 결합함수의 차수가 1일때, 즉 선형시스템의 경우에 대한 출력계열의 갯수는 ${}_NC_1$ 이며, 비선형 결합함수의 차수가 2일때의 출력계열의 갯수는 ${}_NC_2$ 이며... 비선형 차수가 N인경우의 출력계열의 갯수는 ${}_NC_N$ 이다. N단 LFSR 시스템에 대한 전체 비선형 결합함수의 형태는 ${}_NC_1 + {}_NC_2 + \cdots + {}_NC_N = 2^N-1$개이다. 이와같이 2^N-1 개의 각각의 비선형 결합함수에 식(8)과 같이 선형결합함수를 적용하면 $GF(2^N)$에서의 모든 형태의 출력을 생성시킬 수 있다. 이는 역으로 설명하면 주기 2^N-1 이내의 어떠한 계열도 원시다항식을 이용한 LFSR 시스템에 일정한 초기상태와 비선형결합함수를 이용함으로서 생성할 수 있음을 의미한다[11].

2. 비선형 결합함수 분석

본 절에서는 귀환결합 방정식과 비선형함수의 최대차수 k를 알고 있다고 가정하고, 이때 구성하고자 하는 등가 시스템의 비선형 결합함수의 최대차수도 k차 이내로 구성된다. 예로서, 초기상태(A_i)와 2차이내의 비선형 결합함수를 가진 키스트림 생성기는 T개의 각기 다른 초기상태(A_i')와 2차이내의 비선형 결합함수를 가진 키스트림 생성기로서 등가시스템을 구성할 수 있음을 보인다.

일반적인 키스트림 생성기의 출력계열 s_n과 이에 대한 d번 천이된 형태의 출력계열 s_{n+d} 이며, 사용된 비선형차수가 2차일때 출력계열은 이들의 곱으로 표시된다.

$$s_n = \sum_{i=0}^{N-1} A_i(\alpha^2)^n, \quad s_{n+d} = \sum_{i=0}^{N-1} A_i(\alpha^2)^{n+d}$$

$$s_n s_{n+d} = \sum_{i=0}^{N-1} A_i(\alpha^2)^n \sum_{i=0}^{N-1} A_i(\alpha^2)^{n+d}$$

$$= \sum_{i=0}^{N-1} A_i(\alpha^2)^n \sum_{i=0}^{N-1} A_i(\alpha^2)^d(\alpha^2)^n \qquad (12)$$

식(12)에서 $r+s=2^N-1$인 r과 s를 이용하여, 다른 초기상태 $A_i' = A_i(\alpha^r)$를 가진 계열로 표시할 수 있다.

$$s_n s_{n+d} = \sum_{i=0}^{N-1} A_i'(\alpha^r)(\alpha^2)^n \sum_{i=0}^{N-1} A_i'(\alpha^s)(\alpha^2)^{n+d} \quad (13)$$

식(13)에서 알 수 있듯이 A_i'는 r의 변화에 따라 각기 다른 초기상태에서의 2차 비선형함수에 의해 출력계열을 표시할 수 있기 때문에 가능한 r의 갯수는 $T=2^N-1$이다. 이러한 결과는 원래의 2차이내의 비선형 결합함수에 의해 구성된 키스트림 생성기의 출력계열은 다른 초기상태하에서 최대 2차이내의 비선형 결합함수를 사용하여 등가 시스템을 구성할 수 있음을 의미한다.

비선형 결합함수의 최대 비선형 차수가 1인 경우에는 1차함수에 영향을 줄 수 있는 weight=1인 상태벡터들에 해당하며, ${}_NC_1 = N$개의 비트를 알면 1차함수를 찾을 수 있다. 왜냐하면 N비트와 이미 알고있는 귀환결합 방정식에 적용하면 최대주기의 출력계열을 생성할 수 있다. 최대 비선형 차수가 2인 경우에는 출력계열이 2차 함수까지를 파악할 수 있도록 초기조건을 설정하여, 1차 함수를 파악한 후, 2차함수를 찾는다. 2차함수를 찾는 방법은 1차함수를 찾는 과정과 마찬가지로 2차함수에 영향을 줄 수 있는 weight=2인 상태벡터들에 해당하며, ${}_NC_2$ 개의 비트를 알면 2차함수를 찾을 수 있다. 따라서 비선형 차수가 2인 경우의 출력계열중 알아야 할 최소 비트수는 ${}_NC_1 + {}_NC_2$ 이 된다. 마찬가지로 최대 비선형 차수가 k차인 경우에도 우선 출력계열에 대하여 k차 비선형함수까지를 파악할 수 있도록 초기조건을 설정하여, 1차 함수를 파악하고 난 후, 2차함수에 의한 효과를 제거하고, 계속하여 k차까지 차수를 증가시키면서 비선형 함수를 찾을 수 있다. 따라서 비선형 차수가 k차 인 경우의 출력계열중 알아야 할 최소 비트수는 ${}_NC_1 + {}_NC_2 + {}_NC_3 \cdots {}_NC_k$ 이 된다.

그러나 이러한 k값은 N단 LFSR의 상태벡터가 일정하게 변하지 않기 때문에, 실제로는 그보다 훨씬 많은 출력계열을 알아야 한다. 예로서, 2차이내의 비선형 결합함수를 도입한 원래의 키스트림 생성기에 대한 등가회로를 알아내기 위한 최소 출력계열 비트수는 키스트림 생성기를 구성하는 LFSR의 귀환결합 구조와 관련하여 LFSR의 상태벡터의 분포에 의한다. 또한 초기상태값을 어떻게 선정하느냐에 따라 등가시스템을 구성하기 위하여 알아야할 최소 비트수가 달라질 수 있다.

(예제)

원래의 키스트림 생성기는 원시다항식 $g(x)=1+x+x^4$의 귀환결합을 가지고, 그림(2)와 같은 구조로서, 초기

조건 "0001"이며 2차 비선형 결합함수 [$f(x)=x_1+x_4+x_3x_4$]를 사용하고 있다고 가정한다. 현재 알고 있는 사항은 귀환결합 방정식과 비선형 결합함수는 2차이내의 함수로 구성되어 있다는 사실과 연속된 출력계열(Z=110001011101100 ..)중 11비트만을 알고 있다. 이것을 이용하여 원래의 키스트림 생성기의 출력계열과 동일한 출력계열을 생성하는 등가 시스템을 구성하시오.

출력계열 Z와 동일한 출력을 생성할 수 있는 비선형 결합함수를 찾기 위하여, 원시다항식 $g(x)=1+x+x^4$ 을 귀환결합으로 사용하고 있는 LFSR 상태벡터들을 표(1)과 같이 순차적으로 열거하였다.

표 1. GF(24)에서의 상태벡터와 관련 비선형 함수

Table 1. The Nonlinear Function and LFSR Contents in GF(24).

상태벡터	출력 연관함수	weight(비선형 차수)
0011	x_3x_4	2
0001	x_4	1
1000	x_1	1
0100	x_2	1
0010	x_3	1
1001	x_1x_4	2
1100	x_1x_2	2
0110	x_2x_3	2
1011	$x_1x_3x_4$	3
0101	x_2x_4	2
1010	x_1x_3	2
1101	$x_1x_2x_4$	3
1110	$x_1x_2x_3$	3
1111	$x_1x_2x_3x_4$	4
0111	$x_2x_3x_4$	3

또한 각 상태벡터에 대하여 실제로 출력계열에 영향를 줄 수 있는 비선형 결합함수를 기술하였다. GF(2^4)에서 키스트림 생성기의 출력중, 1차및 2차 비선형 함수와 관련되는 비트 수는 ${}_4C_1 + {}_4C_2 = 4+6 = 10$ 이다. 그러나 실제 키스트림 생성기의 상태벡터의 순환은 일정하지 않다. 표 1에서 2차이내의 비선형 결합함수에 영향을 줄 수 있는 최소집합은 초기상태 "0011"에서 11번째 상태 "1010"까지 임을 알 수 있다. 그러므로 전체 주기에 해당하는 15비트중 11비트만 알면, 2차 비선형 결합함수에 대한 정보를 추출할 수 있다. 앞에서 설명하였듯이 원래의 키스트림 생성기가 2차 비선형 결합함수를 사용하였다면, 다른 초기상태와 최대 2차이내의 비선형 결합함수에 의해 동일한 출력계열을 생성할 수 있는 등가 시스템을 구성할 수 있다는 것이다. 따라서 원래의 키스트림 생성기에서 2차이내의 비선형 결합함수를 사용하였고, 출력이 전체주기중 11비트(11000101110..)를 알고 있다고 가정한다.

키스트림 생성기의 출력 Z= 110001011101100..에서 LSB부터 순차적으로 1차 비선형함수의 효과를 제거하기 위하여 출력계열과 비교하면, 3,4,5번째 비트는 "0"이며, 2번째가 "1"이므로 1차 비선형 함수는 x_4 라는 것을 알 수 있다. 따라서 키스트림 생성기의 출력 Z 와 초기상태 "0011"에서의 LFSR 시스템의 제4단 출력성분 x_4를 제거하면 다음과 같다.

$$Z' = 11000101110.. \oplus 110001001101011..$$
$$= 00000001000..$$

Z'계열은 1차성분이 제거된 형태이며, 이는 2차 비선형 출력함수들에 의해 구성된다. 따라서 이러한 2차 함수를 알기 위해서는 Z'= 00000001000..에 다시 LSB부터 순차적으로 2차성분을 제거하면 된다. 이제 1차 비선형 함수가 제거된 상태이므로 2차항을 보면 8번째 비트가 "1"이므로 x_2x_3 항이 존재한다는 것을 알 수 있다. 따라서 Z'계열에서 2차 비선형 함수 x_2x_3 를 제거하면 다음과 같다.

$$Z'' = 00000001000.. \oplus 00000001000..$$
$$= 00000000000..$$

결과적으로 "0011" 의 초기상태값과 $f(x) = x_4+x_2x_3$ 인 비선형 결합함수로 구성된 키스트림 생성기을 이용하여, 원래의 키스트림 생성기의 출력과 동일한 계열을 생성할 수 있다. 이와같이 귀환결합구조와 최대 비선형 차수 및 출력계열중 일부를 알면 원래의 키스트림 생성기와 동일한 출력계열을 생성시킬 수 있는 등가 키스트림 생성기를 구성할 수 있다. 실질적으로 LFSR의 상태벡터에 대한 weight 분포가 1차, 2차...등의 순으로 나타나지 않는다. 따라서 키스트림 생성기의 출력계열중 알아야 할 최소 비트수는 비선형 함수의 최대차수와 LFSR의 상태벡터의 변화(weight 분포)에 따라 적절히 초기벡타를 선정하여야 한다. 물론 최대 비선형 차수 k=N인 경우에는 ${}_NC_1 + {}_NC_2 + {}_NC_3 + .. + .. {}_NC_N = 2^N-1 = T$가 되기 되기 때문에, 한 주기의 키스트림 생성기의 출력을 모두 알아야 등가 키스트림 생성기를 구성할 수 있다.

그러나 k가 적은 경우에는 이러한 방법에 의하면,

동일한 출력계열을 생성할 수 있는 키스트림 생성기를 쉽게 찾을 수 있을 뿐 아니라, 실제로 2진 계열에서는 "1"의 출력만이 비선형함수의 영향을 받아 출력계열에 영향을 주기 때문에 경우에 따라서는 계산 복잡도가 대폭 감소될 수도 있다. 표(2)은 N=6,7,8에서의 비선형 등가시스템을 구성하기 위하여 필요한 최소비트수를 나타낸다.

표 2. 비선형 함수를 분석하기 위한 최소비트수.
Table 2. The minimum bit number required analyzing nonlinear function.

최대 비선형 차수	N단 등가시스템 구현을 위한 초기상태와 비트열수		
	N = 6	N = 7	N = 8
1	000001 (6)	0000100 (7)	00000010 (50)
2	000011 (36)	0100100 (86)	00011000 (201)
3	000111 (56)	0001101 (116)	00110010 (223)
4	001111 (59)	0101111 (121)	01100101 (230)
5	011111 (62)	0011111 (124)	01011110 (246)
6	무관 (63)	0111111 (126)	01111110 (251)
7		무관 (127)	01111111 (254)
8			무관 (255)

마지막으로 $GF(2^6)$에서의 비선형 함수를 분석하기 위한 최소 비트수는 표(2)과 같다. 최대 비선형 차수가 3인 경우의 예를 다룬다. 한 주기내의 비선형 관련 비트수는 ${}_6C_1 + {}_6C_2 + {}_6C_3 = 41$ 이지만, 이러한 키스트림 생성기의 출력계열과 동일한 출력계열을 생성하기 위한 등가시스템을 구현하기 위한 최소 비트수를 구하기 위해서는 N=6인 경우에 모든 상태벡터들의 weight를 분석한다. 상태벡터들 중에서 weight 3 이내의 모든 상태를 포함하는 최소집합은 초기상태 "000111"(weight 3)에서 순환하여 56번째인 "101010"(weight 3)이다. 따라서 키스트림 생성기의 출력중 56 비트를 알고 있다면, 초기상태 "000111"에서 시작하여 앞에서 서술한 방법에 의해 LSB부터 1차 비선형함수를 찾고, 다시 2차 비선형함수를 찾고, 다시 3차 비선형함수를 찾음으로서 원래의 키스트림 생성기의 출력과 동일한 출력을 얻을수 있는 시스템을 구현할 수 있다.

Ⅳ. 결 론

지금까지의 분석을 종합하면, 선형 LFSR만으로 구성된 키스트림 생성기는 2N 비트의 출력계열을 이용한 기존의 방법으로 해독이 가능하다. 따라서 이러한 단점을 보완하기 위하여 선형복잡도와 비예측성을 높히기 위하여 비선형 결합함수, 병렬배치, 메모리사용등 여러가지 방법이 검토되었다. 본 논문에서는 이러한 방법중 비선형 결합함수를 이용하여 키스트림 생성기를 구성할 경우에 대하여, 비합법적인 공격자가 키스트림 생성기의 귀환결합 형태와 비선형 결합함수의 최대 차수를 알고, 출력계열중 일부를 알고 있다면 원래의 키스트림 생성기의 출력과 동일한 출력계열을 생성시킬 수 있는 시스템을 구성할 수 있음을 보여주었다. 이러한 결론은 통신시스템에서 흔히 사용하는 임의의 의사난수계열을 생성하는 키스트림 생성기에 대한 안전성과도 밀접한 관계가 되기 때문에 시스템 설계시 고려해야 할 것이다.

참 고 문 헌

[1] Brüer, J.O.: "On Nonlinear Combinations of Linear Shift Register Sequences", Proc. IEEE Int. Symp. Inform. Theory, Les Ares, France, June 21-25, 1982.

[2] Geffe, P.R.: "How to Protect Data with Ciphers that are Really Hard to Break", Electronics, pp.99-101, Jan.4, 1973.

[3] Golomb, S.W.: Shift Register Sequences. Holden-Day, San Francisco, CA, 1967.

[4] Groth, E.J.: "Generation of Binary Sequences with Controllable Complexity", IEEE Trans. on Inform. Theory, vol.IT-17, 1971.

[5] Key, E.L.: "An Analysis of the Structure and Complexity of Non-Linear Binary Sequence Generators", IEEE Trans. Inform. Theory, vol.IT-22, pp.732-736, 1976.

[6] Rhee, M.Y.: Cryptogrphy and Secure Communication, McGraw-Hill, New York, 1993.

[7] Rueppel, R.A.: Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, Germany, 1986.

[8] Rueppel, R.A.: "Linear Complexity and Random Sequences", Proc. Eurocrypt '85, pp.167-188, 1986.

[9] Siegenthaler, T.: "Cryptanalysts Representation of Nonlinearly Filtered ML-Sequences", Advances in Cryptology, Eurocrypt '85, Springer-Verlag, pp.103-110, 1986.

[10] Siegenthaler, T.: "Correlation Immunity of Nonlinear Combining Functions for Cryptographic Applications", IEEE Trans. on Inform. Theory, vol.IT-30, no.5, Sept. 1984.

[11] Scholtz, R.A. and Welch, L.R. : "GMW Sequences", IEEE Transaction on Inform. Theory, Vol. IT-30, No.3, pp548-553 May 1984.

[12] Lidl, R. and Niedereiter, H. : "Finite Fields Encyclopedia of Mathematics and its Application, Addison-Wesley, New York, Vol. 20, 1983.

[13] Sarwate,D.V. and Pursley,M.B. : "Crosscorrelation Properties of Pseudoran dom and Related Sequences", Proceedings of the IEEE, Vol.68, No.5, May 1980.

[14] 김 지홍, 이 만영, "비선형 결합함수를 이용한 난수계열의 특성분석", 대한 전자 공학회 논문집- A권,pp1-pp6, 8, 1994

저 자 소 개

金 志 弘(正會員) 第 31卷 A編 第 8號 參照
현재 세명대학교 전자공학과 조교수

李 晩 榮(正會員) 第 31卷 A編 第 8號 參照
현재 한양대학교 전자통신학과 명예교수, 통신정보 보호학회 회장