論 文

비선형 함수를 도입한 키스트림 생성기에 대한 등가 시스템 구성

正會員 金 志 弘*, 正會員 李 晩 榮**

A Construction of The Equivalent System to The Key Stream Generator with Nonlinear Function

Ji Hong Kim*, Man Young Rhee** *Regular Members*

要 約

비선형 결합함수와 선형귀환 치환레지스터로 구성된 키스트림 생성기의 특성에 관하여 설명하고, 원래의 키스트림 생성기의 출력계열과 동일한 계열을 생성할 수 있는 등가 시스템을 구성하는 방법을 설명한다. 또한 키스트림 생성기에서 사용된 귀환결합 방정식을 알고, 비선형 결합함수의 최대차수가 2차이내인 경우에 대하여 등가 시스템을 구성하기 위한 최소비트수와 확률에 관하여 논한다.

ABSTRACT

A Key Stream Generator consisting of a maximum-length linear feedback shift register(LFSR) and some nonlinear function is investigated. We construct the equivalent key stream generator, which can generate the same sequences, to the original key stream generator. We discuss the minimum number of key stream generator outputs and it's probability if we know the feedback connection polynomial used in the system and the maximum order of nonlinear function.

* 世明大學校 電子 工學科
Semyung University Dept. of Electronic Com
** 漢陽大學校 電子通信 工學科
Hanyang University Dept. of Electronic Com

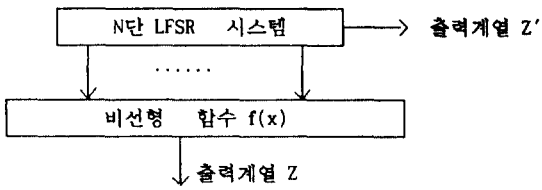
論文番號 : 94131
接受日字 : 1994年 5月 14日

1. 서 론

스트림 암호시스템의 키스트림 생성기(key stream generator)에 의해 생성되는 이진 출력계열은 선형귀환 치환레지스터(LFSR)를 사용하여 생성한다. 이러한 LFSR에 의해 구성된 키스트림 생성기에 대하여 의사난수(pseudorandom)특성과 선형복잡도(linear complexity)를 높히기 위한 수많은 연구가 수행되어 졌다. 대표적인 알고리즘으로는 J-K플립플롭, 병립형(cascaded form), 비선형 결합함수 적용 시스템등이 있으며, 그중에서 선형귀환 치환레지스터에 의해 생성되는 최대장계열에 비선형 결합함수를 도입한 방법에 대하여 논한다. 일반적으로 비선형 결합함수를 도입한 출력계열의 선형복잡도는 LFSR의 크기와 비선형 함수에 의해 결정된다. LFSR의 출력계열의 선형복잡도는 LFSR의 단수 N과 동일하지만, LFSR의 각 단의 출력에 대하여 비선형 결합함수를 도입한 후의 출력계열의 선형복잡도는 최대 2^N-1까지 높아질 수 있다. 그러나 1985년 Sigenthaler[6,7]는 비선형 결합함수를 도입한 키스트림 생성기에서 생성된 출력계열과 LFSR계열에 의해 생성되는 출력이 서로 상관관계(correlation)를 가지면, 이러한 키스트림 생성기에 대한 키(비선형결합함수, 초기조건)를 알고자하는 공격이 가능하다는 것을 보였다. 또한 상관공격을 수월하게 하기 위하여 walsh변환함수를 이용하여, 각 단의 출력에 적용된 비선형 결합함수를 Geffe시스템과 같은 각각의 LFSR에 대한 출력계열들에 대한 비선형 결합형태로 등가시스템으로 변화하는 방법을 제시하였다[8]. 또한 이러한 상관공격에 대한 연구는 Meier[9], Forre[10], Chepyzhov[11]등으로 계속되고 있다. 본 논문에서는 비선형 결합함수를 적용한 키스트림 생성기의 출력계열에 대한 특성을 분석하고, 이러한 특성을 이용하여 원래의 초기조건과 비선형결합 구조와 다른 구조를 가지면서, 원래의 키스트림 생성기의 출력과 동일한 출력계열을 생성할 수 있는 등가 키스트림 생성기를 구성하는 방법을 보인다. 또한 비선형 결합함수의 차수가 2차이내인 경우에 대하여, 등가 키스트림 생성기를 만들기 위한 출력계열의 최소 비트수와 이에 따른 등가 시스템을 찾을 수 있는 확률을 분석한다.

2. 비선형 결합함수의 특성

일반적으로 생성다항식을 귀환 결합계수로 하는 LFSR 시스템의 출력계열은 최대주기를 갖는 최대장 계열이 된다. 이러한 최대장 계열의 출력에 대하여 선형 복잡도와 비예측성을 높히기 위하여 그림1과 같이 비선형 함수을 이용한 비선형 결합기 구조를 도입한다.



〈그림1〉 비선형 결합함수를 이용한 LFSR
Fig.1 LFSR system with nonlinear function

이러한 비선형 결합함수를 도입한 키스트림 생성기(이하 키스트림 생성기라 함)의 첫번째 주기동안의 출력 계열 **Z**는 N단 LFSR의 각 단들의 출력에 대한 곱의 항들로 구성된 선형 결합 형태로 표시할 수 있다. 따라서 N단 키스트림 생성기의 출력계열에 대한 최대 주기 $p=(2^N-1)$로 표시하면, 출력계열 **Z**는 (1)식과 같이 p×p 형태의 곱행렬 **P**와 이들에 대한 계수 행렬 **A**의 곱의 형태로 표시될 수 있다 [4].

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

식(1)은 다시 식(2)와 같이 표현될수 있다.

$$\mathbf{A}^T = \mathbf{Z}^T \cdot \mathbf{P}^{-1} \qquad (2)$$

식(2)은 임의의 출력계열 행렬과 주어진 초기상태를 이용하여 생성된 곱행렬의 역행렬을 곱하면, 주어진 초기상태하에서 키스트림 생성기에서 사용된 비선형 결합함수를 찾을 수 있음을 나타낸다.

N단 LFSR에 의해 생성된 각 단의 출력계열에 대하여 비선형 함수를 적용하기 위하여 편의상 1단의 출력계열을 x1, 2단의 출력계열을 x2 , … N단의 출력계열을 XN 이라한다. N단 키스트림 생성기에 사용

된 비선형 결합함수의 형태는 일반식으로 표시할 수 있으며, 만약 최대차수 k차의 비선형 결합함수를 적용한 경우의 k차 비선형 결합함수의 형태는 식(3)과 같이 표시할 수 있다.

$$\begin{aligned} f(x) = {} & a_1x_1+a_2x_2+a_3x_3.. + a_Nx_N \\ & +a_{12}x_1x_2+a_{23}x_2x_3+a_{24}x_2x_4 +... \\ & +a_{123}x_1x_2x_3 + a_{124}x_1x_2x_4 + a_{125}x_1x_2x_5 +... \\ & +a_{1234}x_1x_2x_3x_4 + a_{1235}x_1x_2x_3x_5 +... \\ & +..... \\ & + a_{123..k}k_1x_2x_3x_4...x_k... + \\ & a_{N-k+1}.NxN-_{K+1}x_{N-k}..x_N \end{aligned} \quad (3)$$

$1 \le i_1 < i_2 < i_3 \cdots < i_k \le N$ 인 정수들의 집합을 $I_{i1\cdots ik} = (i_1, i_2, i_k)$ 라 정의한다면, 이때 출력계열의 계수 $a_{i1\cdots ik}$는 식(4)와 같이 표현될 수 있다.

$$\begin{aligned} a_{i1...ik} &= \sum_{x \in S_{ik...ki}} f(x_1, x_2, x_3..., x_N) \\ S_{i1...ik} &= \{ x | x_j = 0, \forall_j \in I_{il...ik} \} \end{aligned} \quad (4)$$

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.

N차 생성다항식에 의해 구성되는 LFSR 시스템의 출력계열의 주기p는 2^N-1 이다. 일정한 초기조건하에서 발생되는 출력계열을 살펴보면, 비선형 결합함수의 차수가 1차일때 즉 선형시스템의 경우에 대한 출력계열의 갯수는 각 단에서 생성되는 각각의 출력계열을 생성할 수 있기 때문에 전체 갯수는 $_NC_1$이다. 비선형 결합함수의 차수가 2차일때 출력계열의 갯수는 N단 LFSR 시스템의 두개의 단에서 생성되는 출력들의 곱으로 생성되며, 이러한 계열들의 갯수는 $_NC_2$이며, … 비선형 차수가 N차인 경우 출력계열의 갯수는 $_NC_N$이다. 따라서 N단 LFSR 시스템에 대한 1차, 2차 …N차의 비선형 결합함수 형태의 전체 갯수는 $_NC_1+_NC_2+ \cdots +_NC_N=2^N-1=p$개이다. 이러한 p개의 비선형 결합함수에 의해 생성되는 계열들에 대하여 선형결합을 적용하면 주기 p이내의 $2^{(2^N-1)}-1$개(영계열 제외)의 모든계열을 생성할 수 있다. 이는 역으로 설명하면 일정한 초기상태를 가진 LFSR 시스템의 각 단에서 생성되는 출력계열에 대하여 최대 k차 비선형 결합함수를 적용함으로써 생성될 수 있는 계열은 식(3)과 같이 표현될 수 있다.

(예) $g(x)=1+x+x^4$인 생성다항식을 갖는 4단 LFSR 시스템의 경우에 대하여 키스트림 생성기의 출력 Z=100011011001101… 와 같은 경우, 이러한 계열를 생성할 수 있는 초기조건과 비선형결합함수를 구하라.

식(2)에서 설명된 바와 같이 N=4인 키스트림 생성기를 이용하여 Z를 생성시킬 수 있는 각각의 초기상태와 비선형 결합함수와의 관계는 표.1 과 같다.[15]

표.1 초기상태와 비선형함수와의 관계
Table.1 Relationship between initial condition and nonlinear function

초기상태	비선형결합 함수
1000	$f(x)=x_1+x_2x_3+x_1x_3x_4$
1100	$f(x)=x_1+x2+x_1x_4+x_3x_4+x_1x_{24}$
1010	$f(x)=x_2+x_3+x_1x_2+x_1x_3+x_1x_4+x_1x_2x_3$
1001	$f(x)=x_1+x_3+x_4x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_1x_3x_4+x_2x_3x_4$
0110	$f(x)=x_1+x_2+x_4+x_1x_2+x_2x_3+x_2x_4+x_3x_4+x_1x_2x_4+x_1x_3x_4$
0011	$f(x)=x_3+x_4+x_1x_3+x_2x_4+x_3x_4+x_1x_2x_3+x_1x_3x_4+x_2x_3x_4$
1110	$f(x)=x_1+x_4+x_1x_3+x_1x_4+x_2x_4+x_1x_2x_4+x_2x_3x_4$
1010	$f(x)=x_1+x_2+x_1x_2+x_1x_4+x_2x_4+x_1x_2x_3+x_1x_3x_4$
0101	$f(x)=x_2+x_3+x_1x_2+x_1x_4+x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$
1110	$f(x)=x_1+x_3+x_4+x_1x_2+x_1x_4+x_2x_3+x_3x_4+x_1x_2x_3+x_1x_2x_4+x_1x_2x_4+x_1x_3x_4$
0111	$f(x)=x_1+x_2+x_4+x_1x_2+x_2x_3+x_3x_4+x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$
1111	$f(x)=x_2+x_3+x_2x_3+x_3x_4+x_1x_2x_3+x_1x_2x_4+x_2x_3x_4$
1011	$f(x)=x_3+x_4+x_1x_3+x_1x_4+x_3x_4+x_1x_2x_3+x_2x_3x_4$
1001	$f(x)=x_4+x_1x_2+x_2x_4+x_2x_3x_4$

3. 비선형 결합함수 분석

본 장에서는 키스트림 생성기를 구성하고 있는 LFSR의 귀환결합 구조와 함께 2차 이내의 비선형 결합함수를 사용한 경우에 대하여, 키스트림 생성기에 대한 공격 방법을 제시한다. 이러한 공격방법은 기존의 키를 알고자하는 노력(상관공격:correlation

attack)과는 달리, 2장에서 설명된 방법을 사용하여 원래의 키스트림 생성기의 출력과 동일한 출력을 얻을 수 있는 등가 키스트림 생성기를 구성하는 것이다. 즉, 키스트림 생성기의 출력계열 중 일정한 값 M개의 비트열을 이용하여, 키스트림 생성기의 출력과 동일한 출력을 생성할 수 있는 키스트림 생성기를 제작할 수 있다는 것이다. 비선형 결합함수의 최대 비선형 차수가 1차인 경우에는 출력계열중 알아야 할 비트수 M는 $_NC_1=N$이 된다. 왜냐하면 기지의 귀환결합 방정식과 초기상태를 "10000…"으로 가정한 후, N비트를 이용하여 1차 비선형 함수를 찾을 수 있다 (예제 참조). 또한 비선형 차수가 2차인 경우에는 키스트림 생성기의 출력계열중 알아야 할 최소 비트수는 $M=_NC_1+_NC_2$이 된다. 그러나 이러한 M값은 N단 LFSR의 상태벡터의 weight분포가 1차, 2차 …의 순으로 일정하게 변하지 않기 때문에, 실제로는 그보다 많은 출력계열을 알아야 한다. 이와같이 2차이내의 비선형 결합함수를 도입한 키스트림 생성기에 대한 등가회로를 알아내기 위한 최소비트수는 키스트림 생성기를 구성하는 LFSR의 귀환 결합구조와 관련된 LFSR의 상태벡터의 분포에 의한다. 또한 초기상태 값을 어떻게 선정하느냐에 따라 최소 비트수가 달라질 수 있다. 표2는 N=10인 경우에 LFSR의 각 단에 나타나는 상태벡터들을 조사하고, 2차이내의 비선형 함수에 영향을 줄 수 있는 weight=2이하의 상태

표2 N=10일때의 2이하의 weight분포.
Table.2 Weight distribution (weight ≤2) in N=10

번호	상태벡터 상태벡터	colck갯수	weight
001-003	1000000100 - 0010000001	3	2
004-013	1000000000 - 0000000001	10	1
014-020	1001000000 - 0000001001	7	2
024-027	0000001001 - 0001000001	4	2
081-089	1100000000 - 0000000011	9	2
158-165	1010000000 - 0000000101	8	2
312-317	1000100000 - 0000010001	6	2
328	1000000001	1	2
517-521	1000010000 - 0000100001	5	2
620-621	1000000010 - 0100000001	2	2

벡터들의 분포를 나타낸것이다.

다음은 이러한 상태벡터들의 weight분포에 따라 등가 키스트림 생성기를 구성하는 방법에 대하여 서술한다.

(방법1)

단지 키스트림 생성기의 출력계열만을 이용하여, 원래의 키스트림 생성기의 출력과 등가의 출력을 발생시킬 수 있느 방법은 식(2)를 이용하면 된다. 즉 2^N-1의 주기를 가진 임의의 모든 계열은 각각의 초기상태와 비선형 결합함수의 조합에 의해서 생성될 수 있다. 또한 2차이내의 비선형 결합함수에 의해 생성될 수 있는 모든 계열은 각기 다른 초기상태와 2차이내의 비선형 결합함수와의 조합에 의해 표시될 수 있다 (표1의 경우에는 3차이내의 비선형결합함수에 의해 생성된 예로서 각기 다른 초기상태와 또다른 3차이내의 비선형 결합함수와의 조합에 의해 표시됨을 보인다). 이와같이 초기상태를 일정하게 두고 비선형 함수를 찾는 방법이다. 키스트림 생성기를 구성하는 LFSR의 귀환결합 구조에 따라 상태벡터는 다르게 나타나지만, 이미 귀환결합 방정식을 알고 있는 상태하에서 초기상태값을 어떻게 선정하느냐에 따라 등가 시스템을 구현하기 위한 출력계열에 대한 최소 비트수가 달라질 수 있다. 표3은 키스트림 생성기의 비선형 함수의 차수가 2차이내인 경우에 대하여 N=6에서 N=10까지 각 초기상태와 등가 시스템을 구성하기 위

표. 3 등가 시스템을 구성하기 위한 최소 비트수
Table.3 The number of minimum bits for equivalent system

LFSR단수 N	귀환결합 방정식	초기상태	최소비트수
6	X^6+X+1	100001	36
7	X^7+X^3+1	1000100	87
8	$X^8+X^4+X^3+X^2+1$	100000110	204
9	X^9+X^4+1	101000000	510
10	$X^{10}+X^3+1$	1000000100	621

한 최소비트수와의 관계를 프로그램 처리한 결과이다. 최대 비선형 차수가 2차인 키스트림 생성기는 비선형 결합함수가 1차함수들과 2차함수들에 의해 구성됨을 의미하며, LFSR시스템의 각 단의 출력계열에 대한 1차와 2차항들의 선형결합들로 구성된다. 따라서 1차항과 2차항을 쉽게 파악할 수 있도록 초기상태를 설정한 후, 1차함수를 먼저 파악하고, LSB부터 순차적으로 제거함으로서, 2차함수를 찾으면 된다(예제 참조).

(방법2)

키스트림 생성기의 출력계열의 일부 비트만을 가지고, 등가 시스템을 구현하는 방법이다. 방법1과 마찬가지로 초기상태를 일정하게 두고 이에 따른 비선형 함수를 찾는 방법으로 이를 해석할 수 있으며, 키스트림 생성기를 구성하는 LFSR의 초기 상태값을 어떻게 선정하느냐에 따라 등가 시스템을 구현하기 위한 출력계열에 대한 최소 비트수가 달라질 수 있다. 방법2는 방법1에 대한 변형으로서, 주어진 출력계열을 이용하여 모든 1차함수와 가능한 모든 2차함수를 파악하고 난 후, 남은 2차함수에 대한 효과를 상관관계를 이용하여 찾아내는 방법이다. 이러한 방법은 키스트림 생성기의 출력계열중의 일부분을 알고 있는 경우에 적용할 수 있다. 만약 키스트림 생성기의 출력중 521비트를 알고 있다면, 521비트를 가지고 1차함수와 2차함수의 거의 대부분을 파악할 수 있다. 그러나 2개의 2차함수 (X_1X_9,X_2X_{10})에 대한 선형결합의 가능성은 4가지이므로, 주어진 521비트를 이용하여 비선형 함수를 찾을 확률은 1/4이다.

표.3 N=10일때의 최소 비트수에 대한 등가시스템을 찾을 확률
Table.4 Probablity of finding The equivalent system according to the state vector diagram.

초기상태벡터	최종상태벡터	최소비트갯수	확률
1000000100	0000000101	165	$\geq 2^{-14}$
1000000100	0000010001	317	$\geq 2^{-8}$
1000000100	1000000001	328	$\geq 2^{-7}$
1000000100	0000100001	521	$\geq 2^{-2}$
1000000100	0100000001	621	= 1

(예제)

생성다항식 $g(x)=1+X^3+X^{10}$에 의해 형성되는 GF(2^{10})에서 최대 2차의 비선형 함수들에 의해 구성된 키스트림 생성기를 고려한다.

(1). 최대 비선형 차수가 1차이며, 출력계열중 10비트를 알고 있는 경우:

키스트림 생성기의 귀환결합 방정식을 알고, 키스트림 생성기의 출력중 10비트를 알면, 초기상태를 "1000000000"로 두고, 첫번째부터 10번째까지의 비트는 각각 X_1에서부터 X_{10}까지의 비선형 함수에 해당되는 출력이다. 간단한 예로서 임의의 출력계열 Y=1001000111…인 경우, 이러한 출력을 생성하기 위해서는 초기상태를 "1000000000"로 두고, 1번째부터 10번째까지의 상태벡터값을 이용할 수 있다. 즉 $X_1=X_4=X_8=X_9=X_{10}=1$, $X_2=X_3=X_5=X_6=X_7=0$, 이므로, 임의의 출력 Y를 생성할 수 있는 비선형 결합함수는 $f(x)=X_1+X_4+X_8+X_9+X_{10}$임을 알 수 있다.

(2). 최대 비선형 차수가 2차이며, 출력계열중 621비트를 모두 알고 있을 경우:

원래의 출력계열과 동일한 출력을 생성할 수 있는 등가 시스템을 구성하기 위하여, 먼저 $g(x)=1+X^3+X^{10}$의 귀환결합을 가진 LFSR 시스템의 상태벡터들의 구성을 살펴본후, 2차 비선형함수의 출력에 영향을 줄 수 있는 상태 벡터들, 즉 weight가 2이내의 상태벡터들의 최소 그룹을 찾으면, 표.2와 같이 초기상태 "1000000100"에서 시작하여 621번째인 "0100000001" 상태까지임을 알 수 있다. 먼저 1차함수를 찾기위하여, 출력계열중 4번째 비트에서 13번째 비트까지 10개의 비트중에서 1인 값을 이용하여 1차함수를 찾고, 이러한 함수들에 의한 출력계열과 이진합을 하여 1차함수에 대한 효과를 제거한다. 그리고 LSB부터 순차적으로 2차 비선형함수를 찾으면 된다. 간단한 예로서 임의의 출력계열Y=10010001110000…인 경우, 이러한 출력을 생성하기 위해서는 초기상태를 "1000000100"로 두고, 4번째부터 13번째까지를 체크하여 1차함수를 찾으면, 4번째 비트(X_1)와 8번째 비트(X_5)와 9번째 비트(X_6)와 10번째 비트(X_7)가 1이고, 따라서 등가시스템의 1차 비선형함수는 $X_1+X_5+X_6+X_7$로 구성됨을 알 수 있다. 따라서 임의의 출력계열 Y에 대하여 이들 함수에 의해 발생되는 출력계열들과 이진합을 하여 1차함수에 대한 효과를 제거한다. 그리고 2차 비선형함수를 찾기 위하여 LSB부터 순차적으로 찾는다. 만일 1번째비트가 1이었다면, 1번째 비트는 X_1X_8 함수와 관련된것이다. 따라서 1차 함수의 효과를 제거한 출력계열에 대하여 X_1X_8함수에 의해 생성되는 계열과 이진합을 한다. 그리고 결과계열에 대하여 다음으로 영향을 주는 2차 비선형함수를 찾고, 이에 따른 2차함수들의 효과를 차례차례 제거하여, 영계열을 생성시킴으로서 원래의 키스트림 생성기의 출력계열과 동일한 출력계열을 생성할 수 있는 비선형 결합함수(초기상태:"1000000100")를 찾을 수 있다. 결국 621 비트의

영계열을 생성함으로서, 비선형 함수를 모두 찾을 수 있다.

(3) 최대 비선형 차수가 2차이며, 출력계열중 328 비트만을 알고 있을 경우:

(2)와 같은 방법으로 출력계열중 4번째 비트에서 13번째 비트까지 10개의 비트중에서 1인 값을 이용하여 1차함수를 찾는다. 또한 주어진 328비트를 이용하여 45개의 전체 2차 비선형 함수중 38개에 대한 효과를 제거하기 위하여 이진합을 한 결과 영계열이 되면 더 이상 나머지 2차함수와 상관없이 키스트림 생성기에 사용된 비선형함수는 결정된다. 그러나 영계열이 아닌 경우에는 나머지 2차함수에 의해 출력계열이 영향을 받고 있음을 의미하기 때문에, 나머지 7개의 2차함수 (X_1X_6, X_2X_7, X_3X_8, X_4X_9, X_5X_{10}, X_1X_9, X_2X_{10})들과의 상관관계를 조사함으로서 비선형 함수를 찾는다. 이들 7개의 2차곱 계열들에 대한 선형결합들과 최대 $2^7=128$번의 이진합을 수행해야 한다. 결과적으로 출력계열 중 328비트를 알고 있으면 2^{-7}의 확률로 원래의 키스트림 생성기의 출력과 동일한 출력계열을 만들 수 있는 다른 키(초기조건, 비선형결합구조)를 갖는 등가 시스템을 구성할 수 있다. 그러나 실제로 LFSR의 귀환결합방정식, 사용된 비선형함수의 차수가 2차이내란 사실을 알고 있는 경우에는 미리 ${}_{10}C_1$개에 해당되는 1차 비선형함수에 의한 생성되는 출력계열(X_1 , , X_{10})과 ${}_{10}C_2$개에 해당되는 2차 비선형함수 (X_1X_2 , , X_9X_{10})에 의한 생성되는 출력계열을 미리 ROM과 같은 메모리에 기억한 다음, 이러한 데이타를 이용하여 원래의 키스트림 생성기의 출력계열에 대하여 LSB부터 순차적으로 제거하여 감으로서, 표.4에 나타난 확률값은 급격히 줄어들 수도 있다.

4. 결 론

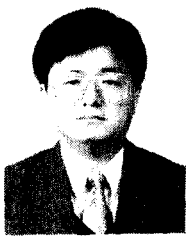
LFSR만으로 구성된 키스트림 생성기는 귀환결합의 구조를 모른다 할지라도, 2N비트의 출력계열을 이용하여 기존의 방법으로 해독이 가능하다. 따라서 이러한 단점을 보완하고 선형복잡도와 비예측성을 높히기 위하여 비선형 함수 사용방법, 병렬 배치방법, 메모리 사용방법등 여러가지 방법이 검토되었다. 이러한 방법중 비선형 결합함수를 사용하여 키스트림 생성기를 구성하는 경우에 대하여, 비합법적인 공격자가 키스트림 생성기에서 사용된 비선형 결합함수의 최대 차수와 키스트림 생성기의 귀환결합 형태를 알고 있다면, 표.3과 같이 귀환결합 함수의 형태에 따라 순환되어 나타나는 상태 벡터들의 weight분포를 이용하여, 동일한 출력계열을 생성할 수 있는 등가 시스템을 구성할 수 있음을 보였다. 또한 비선형 결합함수의 차수가 높아짐에 따라 등가시스템을 구성하기 위해서는, 키스트림 생성기의 출력계열의 비트수가 더욱 많이 필요함을 알 수 있다. 본 논문에서는 최대 비선형 차수가 2차 이내의 함수로 구성되는 경우에 대하여 원래의 키스트림 생성기의 출력과 동일한 출력계열을 생성시킬수 있는 등가 시스템을 구성하기 위한 방법을 설명하였다. 이러한 결론은 통신시스템에서 흔히 사용하는 임의의 의사난수 계열에 대한 안전성과도 밀접한 관계가 되기 때문에 시스템의 설계시 고려해야 할 것이다.

참고문헌

1. Golomb, S.W:Shift Register Sequences. Holden-Day, San Francisco, CA, 1967.
2. Key, E.L.:"An Analysis of the Structure and Complexity of Non-Linear Binary Sequence Generators", IEEE Trans. Inf. Theory,vol.IT-22, pp.732-736,1976.
3. Rhee, M.Y.:Cryptogrphy and Secure Communication, McGraw-Hill, New York, 1993
4. Rueppel, R.A.:Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, Germany,1986.
5. Rueppel, R.A:"Linear Complexity and Random Sequences", Proc. Eurocrypt '85, pp. 167-188, 1986.
6. Siegenthaler,T.:"Correlation Immunity of Nonlinear Combining Functions for Cryptographic Applications", IEEE Trans. on Inf. Theory, vol.IT-30, no.5, Sept. 1984.
7. Siegenthaler, T:"Decrypting a Class of

Stream Ciphers Using Ciphertext Only", IEEE Trans. on Computer, vol.c-34, no.1, Jan.1985.

8. Siegenthaler, T.:"Crytanalysts Representation of Nonlinearly Filtered ML-Sequences", Advances in Cryptology, Eurocrypt '85, Springer-Verlag, pp.103-110,1986.
9. Meier, W.and Staffelbach, O.:"Fast Correlation Attacks on stream Ciphers", Advances in Cryptology, Eurocrypt '88, Springer-Verlag, pp.301-304,1988.
10. Forre,R.: "A Fast Correlation Attacks on Nonlinearly Feedforward Filtered Shift-Register Seuences", Abstracts of Eurocrypt'89.
11. Chepyzhov, B.V and Smeets, B.:"On A Fast Correlation Attacks on Certain Stream Ciphers",Abstracts of Eurocrypt'91.
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. 이 만영, "선형복잡도와 난수성을 제고할 수 있는 키수열 생성방법", 데이터 보호기반기술 workshop논문집, pp43-69,1992
15. 김 지홍, 이만영, "비선형 결합함수를 이용한 난수계열의 특성분석", 대한전자 공학회 논문집-A 권, pp 1-6,8,1994



金 志 弘(Kim Ji Hong)

1959년 2월 25일생
1982년 : 한양대학교 전자공학과(공학사)
1984년 : 한양대학교 전자통신과(공학석사)
1993년 : 한양대학교 전자통신과 박사과정수료
1984년 ~ 1990년 : 금성전선 연구소
1991년 ~현재 : 세명대학교 전자공학과 근무

李 晩 榮(Rhee Man Young)

1924년 11월 30일생
서울대학교 전기공학과 공학사(BSEE)
미국 Colorado 대학교 공학석사(MSEE)및 공학박사(Ph.D.)
미국 Virginia 주립대 공과대학교수
미국 California Institute of Technology, JPL연구원
국방과학연구소 제1부소장/한국전자통신 사장/삼성반도체 사장
한양대학교 부총장/한양대학교 명예교수/한국통신보호학회 회장