論文94-31A-8-1

비선형 결합함수를 이용한 난수계열의 특성 분석

(Analysis on the Random Sequences Generated by LFSR with Nonlinear Function)

金 志 弘*, 李 晩 榮**

(Ji Hong Kim and Man Young Rhee)

要 約

본 논문에서는 선형치환 귀환레지스터에 의해 생성되는 최대장 계열에 대하여, 선형복잡도(linear complexity)와 무작위 특성(randomness)을 높이기 위하여 비선형 결합기(nonlinear combiner) 구조를 도입한다. 이러한 비선형 결합기에 의해 생성되는 출력 계열의 특성을 분석하기 위하여, 실지로 GF(2^4)상의 원시 다항식을 귀환 탭계수로 하는 선형귀환 치환레지스터(LFSR)부와 비선형 결합부로 구성되는 생성기의 원리를 제시하고, 출력 계열의 특성을 분석한다.

Abstract

In this paper, we introduce the nonlinear combiner structure which improves linear complexity and randomness properties on maximum length sequences generated by LFSR. Choosing the primitive polynomial over GF(2^4) as feedback tap polynomial, we devise nonlinear combiner structure and analyze the random output sequences generated by LFSR with nonlinear function.

Ⅰ. 서론

스트림 암호시스템의 키스트림 생성기(key stream generator)에 의해 생성되는 키스트림 이나 CDMA(code division multiple access) 방식이 도입된 이동통신 시스템에서 사용되는 Pilot sequence 혹은 long code sequence 들은 모두 선형귀환 치환레지스터(LFSR)를 사용하여 생성한다. 이러한 LFSR(linear feedback shift register)만을 이용하여 생성되는 스트림 암호시스템의 최대 단점은 출력계열이 이진(modulo 2) 연산에 의해 생성되기 때문에 2N(N: 선형치환 레지스터의 길이)비트의 출력문을 알면, 2N개의 선형방정식을 해석함으로서, 시스템을 분석할 수 있고 완벽한 랜덤 특성을 얻을 수 없다는 점이다. 따라서 이러한 단점을 해결하기 위하여 선형귀환 치환레지스터 계열들에 비선형 배치구조를 도입하여 출력계열들이 훌륭한 의사난수(pseudo-

*正會員, 世明大學校 電子工學科
(Dept. Elec. Eng., Semyung Univ.)
**正會員, 漢陽大學校 電子通信工學科
(Dept. of Elec. Comm. Eng., Hanyang Univ.)
接受日字 : 1993年 8月 14日

random)특성과 높은 선형복잡도(linear complexity)[6][8]를 얻기 위한 수많은 연구가 수행되어 졌다. 선형복잡도는 해당 계열을 생성할 수 있는 선형귀환 치환레지스터에 대한 생성다항식의 최소 차수를 의미한다.

본 논문에서는 Rueppel이 제안한 비선형 결합기[7]를 근간으로 GF(2^4)에 적용하여 생성된 출력계열에 대하여 이론적으로 분석하고, LFSR의 초기상태와 선형복잡도를 높히기 위하여 도입되는 비선형 함수간의 상관관계등의 특성을 분석한다.

Ⅱ. 비선형 결합함수에 의한 출력계열의 특성

1. 의사난수계열의 특성

의사난수계열이란, 유한계열에 의해서는 생성이 불가능하기 때문에 이와 유사한 무작위 계열을 만드는 것이다. 이러한 계열은 원시다항식을 귀환 탭계수로 하는 선형귀환 치환레지스터(LFSR)에 의해 생성될 수 있으며, 이들 중 최대주기를 가진 계열을 최대장 계열이라 한다. 이러한 의사난수계열은 다음과 같은 5개의 특성[13]을 가진다.

- 평형성(balance) 특성:

N단 LFSR에 의해 생성되는 2진 계열에 대하여 2^{N-1}개의 "1"과 $2^{N-1}-1$ 개의 "0"으로 구성됨

- 연속성(run) 특성 :

연속되는 "1" 또는"0"이 나타날 확률은 길이가 길수록 적어진다. 즉, "1" 또는 "0"의 갯수가 한개인 경우의 확률은 1/2 이며, "1" 또는 "0"의 갯수가 두개 연속될 경우의 확률은 1/4 이다.

- 상관(correlation) 특성 :

주기 p인 계열에 대하여 자기신호와 τ 만큼 지연된 신호와의 상관 관계는 일정하게 나타난다.

$$R(\tau) = 1/p \sum_{i=1}^{p} s(i)s(i+\tau) \quad 0 \le \tau < p,\ s(i) = s(i+p)$$

$$s(i)s(i+\tau) = 1, \text{ if } s(i) = s(i+\tau)$$
$$-1, \text{ if } s(i) \neq s(i+\tau)$$

$$R(\tau) = \begin{cases} 1, & \tau = 0 \\ -1/p, & \text{otherwise} \end{cases}$$

- 중첩(superposition) 특성

S = A + B 일때, 초기상태 S에 의한 출력계열은 초기상태 A에 의한 출력계열과 초기상태 B에 대한 출력계열의 합과 같다.

- 데시메이션(decimation) 특성:

PN 계열의 주기 2^{N-1} 과 서로 소인 k번째 비트를 선택하면 최대장 계열이 생성한다. k값이 2의 지수승인 경우에는 결과 계열은 원래의 계열을 천이한 형태이며, 그외의 경우에는 다른 형태의 계열을 생성한다. 만일 k가 2^{N-1}의 약수인 경우에는, 약수에 해당되는 주기의 계열을 생성한다.

2. Rueppel의 비선형 결합기 구조

전 절에서 설명된 바와 같이 최대주기를 갖게 하기 위하여 도입된 최대장 계열을 이용하고, 여기에 다시 선형 복잡도와 출력계열의 비예측성을 높히기 위하여, 비선형 결합기를 도입한다. N단 LFSR에 의해 생성된 최대장 계열에 대하여 비선형 함수를 결합한 형태에 의한 출력계열의 형태는 식(1)과 같다.

$$\begin{aligned} f(x) = {} & a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_Nx_N \\ & + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{14}x_1x_4 \ldots \\ & + a_{123}x_1x_2x_3 + a_{124}x_1x_2x_4 + a_{125}x_1x_2x_5 \ldots \\ & + a_{1234}x_1x_2x_3x_4 + a_{1235}x_1x_2x_3x_5 \ldots \\ & + \ldots \\ & + a_{1234\ldots N}x_1x_2x_3x_4 \ldots x_N \end{aligned} \tag{1}$$

$1 \le i_1 < i_2 < i_3 \ldots < i_k \le N$ 인 정수들의 집합을 $I_{i_1 \ldots i_k} = \{i_1, i_2, i_3 \ldots i_k\}$라 정의 한다면, 이때 출력계열의 계수[10] $ai_1 \ldots i_k$ 는 식(2)와 같이 표현될 수 있다.

$$ai_1 \ldots i_k = \sum_{x \in S i_1 \ldots i_k} f(x) \tag{2}$$

$$Si_1 \ldots i_k = \left\{ x \mid x_j = 0, \forall_j \notin I i_1 \ldots i_k \right\}$$

본 논문에서는 비선형 함수의 특성을 보다 쉽게 파악하기 위하여 N=4의 경우에 대하여 이론을 전개한다. 그림 1은 N=4 인 경우의 비선형 결합 함수 f(x)를 이용하여 출력계열을 얻은 예이다. 여기서 LFSR에 의한 출력 Z'는 2^4-1 =15의 주기를 갖는 계열로서, {Z' = 011110101100100 011110101100100 .. } 와 같다. 또한 주어진 비선형 결합함수 f(x)에 의해 여과된 출력계열 Z가 나타난다.

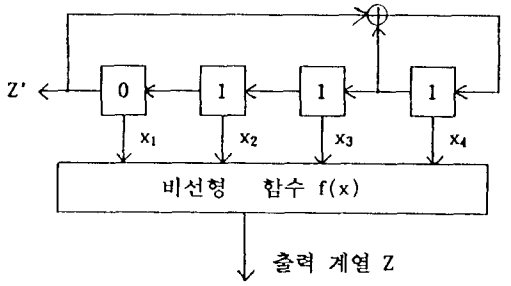

그림 1. 비선형 결합함수를 이용한 LFSR
Fig. 1. The LFSR system with nonlinear function.

식(1)에 의하여 비선형 결합기의 첫번째 주기동안의 출력 계열 Z는 자체 곱들의 항의 선형결합 형태로 표시할 수 있다. 따라서 출력계열 행렬Z 와 계수 행렬 A를 각각 (15×1) 형태의 열벡터로 구성하면, 출력계열 행렬 Z는 (15×15)의 벡터로 구성된 곱행렬과 계수행렬간의 행렬곱으로서 식(3)과 같이 표시할 수 있다.

$$\mathbf{Z} = \mathbf{P}^{T} \cdot \mathbf{A} \tag{3}$$

여기서 P는 모든 독립 곱벡터들로 행(row)을 구성하는 행렬이고, A는 계수 행렬이다. 독립 곱벡터 행렬의 각 행은 그림 2-1에서 4단 선형치환 레지스터의 각 단을 오른쪽으로 순환 치환함으로서, 선형치환 레지스터의 각 단에는 생성되는 계열 S_1, S_2, S_3, S_4 와 이러한 계열들의 서로 다른 곱의 형태로 구성된다.[7] 식(3)은 달리 표시하면 식(4)와 같이 표현될 수 있다

$$\mathbf{A}^{T} = \mathbf{Z}^{T} \cdot \mathbf{P}^{-1} \tag{4}$$

식(2-4)의 의미는 임의의 출력계열 행렬과 주어진 초기상태를 이용하여 생성된 곱행렬을 곱하면, 주어진 초기상태하에서 키스트림 생성기에서 사용된 비선형 결합함수를 찾을 수 있다는 것이다.

3. 비선형 결합함수에 의한 출력계열의 특성

n=4인 4단 LFSR에서의 초기상태 "0111" 일때의 경우를 고려하자. 생성다항식 $g(D) = 1+D+D^4$ 에 의해 생성되는 최대장계열은 전 절에서 설명한 바와 같이 Z′ = 011110101100100 이다. 만일 4단 LFSR의 비선형 결합형태가 식(5)와 같이 주어진다면 출력계열 Z = 110010111100100 이 된다.

$$f(x) = x_1 + x_2x_3 + x_1x_2x_4 \tag{5}$$

이러한 결과를 수학적으로 해석하기 위하여 각 비선형 결합의 각 계수에 해당하는 곱행렬을 구하면 표.1과 같으며, 비선형 계수행렬(A^T)과 곱행렬(P)를 이용하여 원하는 비선형 출력계열을 얻을 수 있다.따라서 이를 역으로 이용하면 비선형 결합행렬을 얻을 수 있다. 즉, 곱행렬에 대한 역행렬을 구하고, 다시 이러한 곱행렬의 역행렬을 이용하여 비선형 결합함수를 구하면 다음과 같다.

$$(1100101111100100)^{T} \begin{bmatrix} 000000000000011 \\ 000000000000001 \\ 000000000010001 \\ 000000000001001 \\ 000001000010101 \\ 000000001001011 \\ 000000000000101 \\ 000000010010011 \\ 000010000011001 \\ 000000100001101 \\ 001001010110111 \\ 010010011011011 \\ 100011100011101 \\ 000100101101111 \\ 000000000100111 \end{bmatrix} = (10000001000100)$$

표 1. 곱행렬(P) (초기조건 "0111")

Table 1. Product matrix (P)(Initial condition "0111").

x_1	:	011110101100100
x_2	:	111101011001000
x_3	:	111010110010001
x_4	:	110101100100011
x_1x_2	:	011100001000000
x_1x_3	:	011010100000000
x_1x_4	:	010100100100000
x_2x_3	:	111000010000000
x_2x_4	:	110101000000000
x_3x_4	:	110000100000001
$x_1x_2x_3$	:	011000000000000
$x_1x_2x_4$	:	010100000000000
$x_1x_3x_4$	:	010000100000000
$x_2x_3x_4$	:	110000000000000
$x_1x_2x_3x_4$	:	010000000000000

표 2. 곱행렬 (초기조건 "0011")

Table 2. Product matrix (P)(Initial condition "0111").

x_1	:	001111010110010
x_2	:	011110101100100
x_3	:	111101011001000
x_4	:	111010110010001
x_1x_2	:	001110000100000
x_1x_3	:	001101010000000
x_1x_4	:	001010010010000
x_2x_3	:	011100001000000
x_2x_4	:	011010100000000
x_3x_4	:	111000010000000
$x_1x_2x_3$	:	001100000000000
$x_1x_2x_4$	:	001010000000000
$x_1x_3x_4$	:	001000010000000
$x_2x_3x_4$	:	011000000000000
$x_1x_2x_3x_4$	:	001000000000000

계산 결과에 의한 계수행렬은 (100000010000100) 이며, 이는 $a_1 = a_{23} = a_{124} = 1$ 를 의미한다. 다음은 초기조건을 "0011" 이라고 가정하고, 생성되는 곱행렬은 표2와 같다.

전과 같은 방법으로 곱행렬에 대한 역행렬을 구하고, 다시 이러한 곱행렬의 역행렬을 이용하여 비선형 결합함수를 구하면

$$(110010111100100)^{T} \begin{bmatrix} 000000000100111 \\ 000000000000011 \\ 000000000000001 \\ 000000000010001 \\ 000000000001001 \\ 000001000010101 \\ 000000001001011 \\ 000000000000101 \\ 000000010010011 \\ 000010000011001 \\ 000000100001101 \\ 001001010110111 \\ 010010011011011 \\ 100011100011101 \\ 000100101101111 \end{bmatrix} = (0100000000110010)$$

계산 결과에 의한 계수행렬은 (0100100000110010) 이며, 이는 $a_2 = a_{34} = a_{123} = a_{234} = 1$ 를 의미한다. 따라서 초기조건 "0111" 상태의 4단 LFSR에 $f(x) = x_1 + x_2 x_3 + x_1 x_2 x_4$ 의 비선형 결합함수를 가진 여과기를 통과한 비선형 계열과 초기조건 "0011" 상태의 4단 LFSR에 $f(x) = x_2 + x_3 x_4 + x_1 x_2 x_3 + x_2 x_3 x_4$ 의 비선형 결합함수를 가진 여과기를 통과한 비선형 계열과 동일한 결과가 나타난다는 것을 알 수 있다. 또한 초기상태 "0111" 인 경우의 곱행렬과 초기상태 "0011" 인 경우의 곱행렬을 비교해보면 초기상태 "0111" 인 경우의 제 1열은 초기상태 "0011"인 경우의 제 2열과 같으므로 결국 초기상태 "0011" -〉 "0111" 이므로 곱행렬은 1열을 천이 시킨 형태로 나타나고, 곱행렬의 역행렬은 1행을 천이시킨 형태로 나타난다. 만일 초기상태를 알고 있다면, 비선형 결합구조는 간단한 행렬 연산에 의해 계산될 수 있다.

그러나 초기조건이 주어지지 않은 경우에는 그와 같은 계열을 생성할 수 있는 방법은 각 초기상태에 대하여 서로 다른 비선형 결합함수를 이용하여 구현할 수 있다. 따라서 일정한 2^N-1 비트의 비선형계열에 대하여, 이러한 비선형계열을 생성할 수 있는 2^N-1 개의 초기상태와 이에 대응하는 비선형 결합형태로 나뉘어 질 수 있다. 이러한 관계를 N=4 인 경우에 대하여 일정한 비선형계열(110010111100100) 을 가지고, 이와 관련된 각각의 초기상태와 비선형 결합관계를 도표를 이용하여 정리하면 표.3와 같다.

표 3. 초기 상태와 비선형 결합과의 관계

Table 3. The relationship between inital condition and nonlinear function.

초기상태	비선형 결합관계	비선형 함수 f(x)
0001	001100100100110	$x_3+x_4+x_1x_4+x_1x_3x_4+x_1x_2x_3x_4+x_2x_3x_4$
0010	011010011010100	$x_2+x_3+x_1x_2+x_2x_3+x_2x_4+x_1x_2x_3+x_1x_3x_4$
0011	010000000110010	$x_2+x_1x_4+x_1x_2x_3+x_2x_3x_4$
0100	110010110011010	$x_1+x_2+x_1x_2+x_1x_4+x_2x_3+x_1x_2x_3+x_1x_2x_4+x_2x_3x_4$
0101	110101111011100	$x_1+x_2+x_4+x_1x_3+x_1x_4+x_1x_3+x_2x_4$ $+x_1x_2x_3+x_1x_2x_4+x_1x_3x_4$
0110	010101100001110	$x_2+x_4+x_1x_3+x_1x_4+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$
0111	100000010001000	$x_1+x_2x_3+x_1x_2x_4$
1000	100110100101100	$x_1+x_4+x_1x_2+x_1x_4+x_3x_4+x_1x_2x_4+x_1x_3x_4$
1001	001101011001010	$x_3+x_4+x_1x_3+x_2x_3+x_2x_4+x_1x_2x_4+x_1x_3x_4$
1010	111111001011000	$x_1+x_2+x_3+x_4+x_1x_2+x_1x_3+x_2x_4+x_1x_2x_3+x_1x_2x_4$
1011	101110001111110	$x_1+x_3+x_4+x_1x_2+x_2x_4+x_3x_4$ $+x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$
1100	100001001110110	$x_1+x_1x_3+x_2x_4+x_3x_4+x_1x_2x_3+x_1x_3x_4+x_2x_3x_4$
1101	111001011110000	$x_1+x_2+x_3+x_1x_3+x_2x_3+x_2x_4+x_3x_4+x_1x_2+x_1x_2x_3$
1110	011001101000010	$x_2+x_1+x_1x_3+x_1x_4+x_2x_4+x_3x_4$
1111	001111000000100	$x_1+x_4+x_1x_2+x_1x_3+x_1x_3x_4$

4. 출력계열에 대한 행렬해석

본 절에서는 지금까지의 고찰에 대하여, 이를 요약하기로 한다. N=4 인 $GF(2^4)$인 경우에 대하여 일정한 비선형 결합함수에 의해 발생된 출력계열은 표.4 과 같이 초기 조건에 의해서 표현될 수 있다.

표 4. LFSR의 초기치와 곱행렬 및 곱행렬의 역행렬

Table 4. The representation of inverse product matrix according to initial condition.

LFSR의 초기치	생성된 최대장 계열	생성된 곱행렬 (열 이동)*	관련된 곱행렬의 역 행렬(행 이동)**
0111	011110101100100	011110101100100	000000000000011
1111	111101011001000	111101011001000	000000000000001
1110	111010110010001	111010110010001	000000000010001
1101	110101100100011	110101100100011	000000000001001
1010	101011001000111	011100001000000	000001000010101
0101	010110010001111	011010100000000	000000001001011
1011	101100100011110	010100100100000	000000000000101
0110	011001000111101	111000010000000	000000010010011
1100	110010001111010	110101000000000	000010000011001
1000	100100011110101	110000100000001	000000100001101
0010	001000111101011	011000000000000	001001010110111
0100	010001111010110	010100000000000	010010011011011
1000	100011110101100	010000100000000	100011100011101
0001	000111101011001	110000000000000	000100101101111
0011	001110101100010	010000000000000	000000000100111

예로서 LFSR의 초기치가 "0111" 이라면 생성된 최대장 계열은 최대장 계열 $Z' = 011110101100100$ 이고, 이때 생성되는 곱행렬의 형태는 표.4의 생성된 곱행렬(*)과 같으며 전 절에서 나타난 표.1와 같다. 또

한 이에 대한 역행렬은 관련된 곱행렬의 역행렬 (**) 와 같다. 이제 전 절에서 설명된 예로서 LFSR의 초기치가 "0011" 인 경우를 고려한다. 생성된 최대장 계열은 최대장 계열 Z′ = 001111010110010 이고, 이때 생성되는 곱행렬의 형태는 표.4의 생성된 곱행렬(*) 부분의 15열을 1열로 이동한 형태로 표시될 수 있으며, 이는 전 절에서 나타난 표.2와 같다. 또한 이에 대한 역행렬은 표.6의 관련된 곱행렬의 역행렬(**)부분의 15행을 1행으로 이동시킨 형태로 표시될 수 있다. 이와 같이 N=4인 비선형 결합함수를 도입한 경우에 대하여, 어느 한 초기상태에 의해서 생성되는 비선형 결합기의 곱행렬과 관련된 곱행렬의 역행렬을 구하면, 모든 초기상태에 대해서도 그와 같은 역행렬을 행 이동함으로서, 각 초기상태와 이에 대응하는 비선형 결합기로 해독할 수 있다. 이러한 결과는 N의 값이 커져도 $(2^N-1)\times(2^N-1)$의 곱행렬의 역행렬으로 모든 초기상태에 대하여, 역행렬을 행 이동함으로서 각 초기상태와 이에 대응하는 비선형 결합기로 해독할 수 있음을 알 수 있다.

Ⅲ. 결론

본 논문에서는 LFSR 출력계열에 대하여, 비예측성(unpredictablity)과 선형 복잡도(linear complexity)를 향상시키기 위하여 제안된 Rueppel의 방법을 도입하여, LFSR에 비선형 함수(non-linear function)을 적용함으로서 발생되는 임의의 출력계열에 대하여 비선형 특성을 분석하였다. N단 LFSR 시스템의 출력계열의 주기는 최대 2^N-1이다. N단 LFSR 만으로 구성된 시스템의 출력계열은 초기상태와 귀환결합에 의해 결정된다. 그러나 그림 1과 같이 각 단에 비선형 결합함수를 도입하여 생성된 계열은 초기상태, 귀환결합과 비선형 함수에 의해 결정되며, 역으로 임의의 출력계열은 이를 생성시킬 수 있는 각각의 초기상태와 비선형 함수의 결합에 의해 나타날 수 있다는 것을 알 수 있다. 이러한 초기상태와 비선형 함수에 관한 관계식은 임의의 초기상태에 대한 곱행렬과 곱행렬의 역행렬을 구한후, 이러한 곱행렬의 역행렬을 행이동 함으로써, 각각의 초기상태에 대한 비선형 결합식을 유도할 수 있다.

이와같은 결론을 좀 더 확장하면, 선형시스템으로 구성된 키스트림 생성기의 경우에는 2N 비트의 출력스트림으로 시스템의 귀환 구조를 알 수 있지만, 비선형 함수를 도입한 키스트림 생성기의 경우에는 출력 계열의 주기를 최대화시키기 위한 최대장 계열이 사용되었다는 가정하에서, 주어진 키스트림 생성기의 임의의 출력계열과 동일한 출력계열을 생성시킬 수 있는 방법은 본 논문에서 살펴본 바와 같이 각각의 귀환결합에 대해서 2^N-1이 된다. 그런데 주어진 유한체 내에서 최대장 계열을 생성시킬 수 있는 갯수는 $\Phi(2^N-1)/N$ [3] 이므로, 주어진 유한체 내에서 동일한 출력계열을 생성시킬 수 있는 총 가짓수는 $(2^N-1)\ \Phi(2^N-1)/N$ [3] 이 된다. 따라서 이러한 관계를 이용하여 원래의 키스트림 생성기의 출력과 동일한 출력계열을 생성하기 위하여 필요한 키스트림 생성기의 최소 출력비트 수를 찾고자 하는 연구는 키스트림 생성기의 안전도와 밀접한 관련이 되기 때문에 지속되어야 한다. 마지막으로 이러한 결과는 통신시스템에서 흔히 적용되는 임의의 의사난수 계열에 대하여 선형성 및 비선형 함수와의 결합관계를 규명하기 위한 기초 자료로서 사용될 수 있을 것으로 기대한다.

參考文獻

[1] Br er.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 Represen tation 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] 이 만 영, "선형복잡도와 난수성을 제고할 수 있는 키수열 생성방법", 데이터 보호기반기술 workshop 논문집, pp43 -69, 1992

著者紹介

金 志 弘(正會員)

1959年 2月 25日生. 1982年 한양대학교 전자공학과(공학사). 1984年 한양대학교 전자통신과(공학석사). 1993年 한양대학교 전자통신과 박사과정 수료. 1984年 ~ 1990年 금성전선 연구소. 1991年 ~ 현재 세명대학교 전자공학과 근무

李 晩 榮(正會員) 第 28卷 B編 第 10號 參照

현재 한양대학교 전자통신과 명예교수, 통신정보 보호학회 회장