通信情報保護學會論文誌
第7卷 第2號, 1997. 6

2 비트 메모리를 갖는 개선된 합산 수열 발생기

이 훈 재*, 문 상 재**

On an Improved Summation Generator with 2-Bit Memory

Hoon Jae Lee, Sang Jae Moon

요 약

합산 수열 발생기는 비메모리형 발생기에서는 생각할 수 없었던 최대 주기, 최대 근사 선형복잡도 및 최고 차수 상관면역도를 동시에 만족하는 발생기이다. 그러나 이 발생기는 연속해서 동일한 "1" 또는 "0"가 출력될 경우 입·출력상관성이 존재하여 carry 비트를 유추할 수 있기 때문에 상관성 공격에 약하다. 이를 피하는 방법으로 입출력 상관 관계를 유추할 수 없도록 LFSR 선형 출력을 발생기 출력에 XOR 시킨 무상관 합산키 발생기가 제안된 바 있지만, 그 발생기는 임의의 선형출력을 k 만큼 시차를 두고 재사용될 뿐아니라 특별한 경우에는 최대주기가 보장되지 않는 단점이 있다. 본 논문에서는 합산 수열 발생기와 무상관 합산키 발생기의 취약점을 보완할 수 있는 새로운 개념의 2비트 메모리를 갖는 개선된 합산 수열 발생기를 제안하고, 비도요소를 분석, 검증하였다.

Abstract

Summation generator is a real adder generator with maximum period, near maximum linear complexity and maximum order of correlation immunity. But this generator has been analyzed by a correlation attack(a kind of known-plaintext attack), which confers carry bits from output sequences of consecutive 0's or 1's. As methods of immunizing carry-output correlation, an immunized summation generator which exclusively-ORed summation generator output with output of a stage of LFSR was proposed. But the immunized generator reuses the output of LFSR by k-bit later and does not garantees maximum period in special case. In this paper we proposed an improved summation generator with 2-bit memory and analyzed it.

* 경북대학교 정보통신

* * 경북대학교 공과대학 전기전자공학부

1. 서 론

정보화 사회로의 본 궤도 진입을 앞둔 현 시점에서 정보의 중요성 특히, 정보의 누설 및 수정 방지 그리고 정보보호에 대한 필요성이 크게 요구된다. 정부차원에서는 초고속정보통신망, 무궁화호 위성 및 5대 기간전산망이 구축되어 통신의 안전성(Security)이 다각도로 요구되며, 기업이나 민간에서도 중요 정보의 보호에 심혈을 기울이고 있다. 이러한 정보보호를 위한 실질적이고 확실한 방법은 암호체계(Cryptosystem)를 적용하는 것이다. 암호체계는 사용되는 암·복호키의 대칭성 여부에 따라 대칭키 암호시스템(symmetric key cryptosystem)과 비대칭키 암호시스템(asymmetric key cryptosystem)으로 대별되며, 대칭키 암호는 스트림 암호(stream cipher)와 블록암호(block cipher)로 다시 나누어진다.[1-2] 블록암호는 블록단위로 평문을 암호화/복호화시키기 때문에 암호문에 1-비트 에러 발생시 수신단에서 블록크기만큼 에러가 확산되어 채널 효율(channel efficiency)을 떨어뜨릴 뿐 아니라 비도수준에 대한 정량화가 불가능하다. 반면 스트림 암호는 송신단에서 동일한 난수열 발생기로 예측 불가한 키수열(keystream)을 발생시킨 후 평문과 XOR시키고, 수신단에서도 동일한 키수열을 발생한 후 암호문에 XOR하여 평문을 복호해내기 때문에 에러 확산이 없을 뿐아니라 비도수준(주기, 선형복잡도, 상관면역도등)에 대한 정량화가 가능하고, 하드웨어 구현이 용이하며, 통신지연이 없고, 고속통신에 적합하다는 등 여러가지 잇점이 있으므로 전송로 구간 통신보안에서 많이 사용된다.

난수열 발생기는 비선형 결합함수(nonlinear combine function)의 메모리비트 사용 유·무에 따라서 비메모리(memoryless)형 발생기와 메모리형 발생기(combiner with memory)로 구분된다. 비메모리형 발생기의 예로 Geffe 발생기[3]를 들 수 있는데, 이 발생기는 최대주기가 보장되는 반면 선형복잡도가 작고 상관면역도(order of correlation immunity)가 0이므로 상관성 공격에 취약하다.[4] 한편 메모리형 발생기의 대표적인 예는 Rueppel[5-6]이 제안한 합산 수열 발생기 (summation generator)를 들 수 있으며, 이 발생기는 비메모리형에 비해 주기 뿐만 아니라 선형복잡도와 상관면역도를 동시에 거의 최대로 만족하는 발생기이다. 그러나 이 발생기에 대하여 Meier등[7]과 Dawson[8]은 연속해서 동일한 "1" 또는 "0"을 출력할 경우 carry-출력간 입출력 상관성이 존재하여 carry 비트를 유추할 수 있기 때문에 상관성 공격(correlation attack)에 약함을 지적하였고, 이상진등[9]은 이를 피하는 한 방법인 무상관 합산키 발생기를 제시하였다. 그러나 이 발생기는 연속 "0" 또는 "1" 출력시에도 입출력 상관 관계를 유추할 수 없도록 LFSR2의 임의 단수를 출력에 XOR 시켰지만 임의의 선형출력을 k 만큼 시차를 두고 재사용될 뿐아니라 특별한 경우에는 최대주기가 보장되지 않는 단점이 있다.

본 논문에서는 합산 수열 발생기와 무상관 합산키 발생기의 취약점을 보완할 수 있는 새로운 개념의 2비트 메모리를 갖는 개선된 합산 수열 발생기를 제안하고, 이 발생기의 입·출력 상관특성 및 2비트 메모리-출력간의 상관특성을 분석한다. 또한 비도요소로서 주기, 선형복잡도 및 상관면역도를 분석하고, 여러 가지 측면에서 난수성(randomness)을 검증한다.

2. 스트림 암호

스트림 암호는 그림 2-1과 같이 키로 초기화된 난수열 발생기로부터 출력 난수열을 발생시킨 다음 평문과 XOR하여 암호문을 생성하며, 수신단에서는 동일한 난수 비트열로 암호문을 복호하는 대칭키 암호의 일종이다.

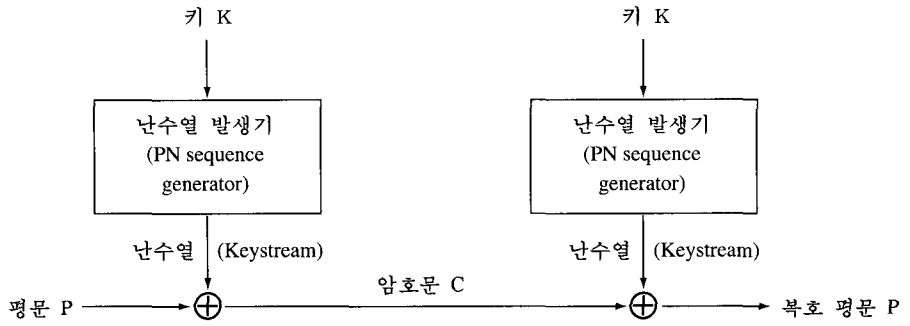


그림 2-1. 스트림 암호

스트림 암호의 안전성(비도)은 여러종류의 암호공격에 대해서 얼마나 강한 난수열 발생기를 설계하느냐에 달려 있으며, Beker등[2]은 스트림 암호의 비도요구사항으로 다음 1)~3) 항을 제시했는데, 그 후 상관면역도에 대한 논란이 많으므로 본 논문에서는 4)항을 추가하여 검토한다.

(스트림 암호의 비도요구사항)

1) 출력난수열은 주기에 대한 최소값이 보장될 것
2) 출력난수열은 좋은 난수성을 갖을 것
3) 출력난수열은 큰 선형복잡도를 갖을 것
*4) 출력난수열은 높은 상관면역도를 갖을 것

2.1 주기(Period)

임의의 $i(\geq 0)$에 대하여 어떤 수열 x_i의 주기는 $x_i = x_{i+P}$를 만족하는 가장 작은 양의 정수 P로 정의되며, 단일 LFSR 및 XOR된 수열의 주기는 다음과 같다.

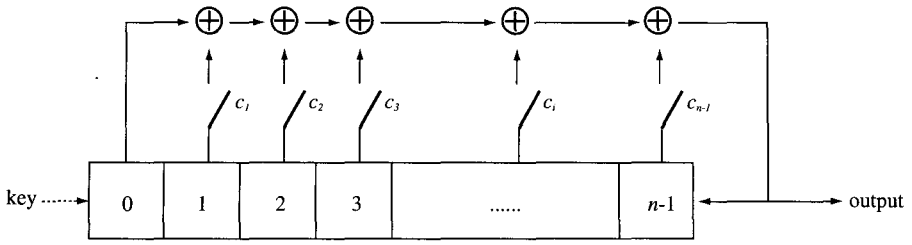
[정리 2.1]

1) n-단 LFSR(그림 2-2 a))의 주기는 모든 레지스터 초기치가 0 아닌 가정하에서 최대주기를 갖으며, 그 주기는 (2^n-1)이 된다.[1-2] 이 때 n-단 LFSR은 원시다항식(primitive polynomial)으로부터 얻어진다.
2) $\gcd(L_a, L_b)=1$ 인 경우 XOR 수열발생기(그림 2-2 b))의 주기는 $P=lcm(P_a, P_b)$이 된다.[1-2]

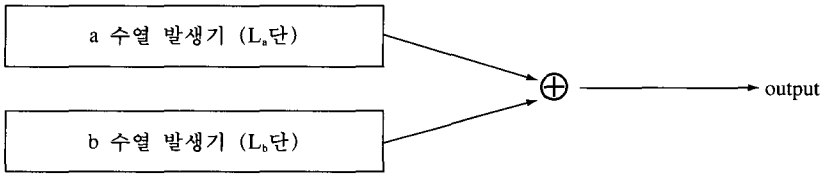
여기서 $P_a = 2^{L_a}-1$, $P_b = 2^{L_b}-1$이다.

2.2 선형 복잡도(Linear Complexity:LC)

임의의 난수열은 동일한 난수열을 발생시킬 수 있는 가장 짧은 LFSR로 표시될 수 있으며, 이러한 LFSR의 단수를 이 난수열의 선형 복잡도라 정의한다. 임의의 난수열에 대한 선형복잡도는 Massey[11]의 LFSR 합성방법에 의하여 구할 수 있는데, 일반적으로 선형 복잡도를 증가시키기 위하여 그림 2-3과 같은 비선형 결합함수를 사용한다. Rueppel등[12]은 비메모리



a) LFSR : $f(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots+c_1x+1$ (primitive)



b) XOR된 수열

그림 2-2. LFSR 및 XOR된 수열

(memoryless)형 비선형 결합함수 f_N과 이 함수의 선형복잡도를 계산하기 위한 star-등식 f_N^*를 다음과 같이 정의하였다.

$$f_N(x_1, x_2, \ldots, x_N) = a_0 + \sum a_i x_i + \sum a_{ij} x_i x_j + \ldots + a_{12..N} x_1 x_2 \ldots x_N \quad (2\text{-}1)$$

$$f_N^*(x_1, x_2, \ldots, x_N) = a_0^* + \sum a_i^* x_i + \sum a_{ij}^* x_i x_j + \ldots + a_{12..N}^* x_1 x_2 \ldots x_N \quad (2\text{-}2)$$

여기서, a_0, a_i, a_{ij}, ... ,$a_{12\cdots N} \in \{0, 1\}$이고, $a_0^*=0(a_0=0$일때) 또는 $1(a_0\neq0$일때), $a_i^*=0(a_i=0$일때) 또는 $1(a_i\neq0$일때), ... , $a_{12\cdots N}^*=0(a_{12\cdots N}=0$일 때) 또는 $1(a_{12\cdots N}\neq0$일때)이며, f_N의 계산영역은 GF(2)영역, f_N^*의 계산영역은 실수영역이다.

[정리 2.2] (Rueppel과 Stafflebach) 비메모리형 난수열 발생기(그림 2-3)의 출력 키수열 z에 대한 선형복잡도는 다음과 같이 star-등식으로 주어진다.

$$LC(z) = f_N^*(L_1, L_2, \ldots, L_N) \quad (2\text{-}3)$$

여기서, $L_i = LC(x_i) = \deg[g_i(x)]$, $i=0,1, \ldots, N$이고, $g_i(x)$는 원시다항식이다.

2.3 상관면역도(Order of Correlation-Immunity)

스트림 암호에 대한 암호분석방법 중 상관성 공격(correlation attack)[13-14]은 입력과 출력 간의 상관성을 조사하여 입-출력 조합을 함수적으로 분리시킨 후 각개 공격(divide and conquer attack)함으로써 키이를 알아내는 방법이며, 이 공격에 취약할 경우 LFSR 탭과 단수를 알고있다는 가정하에서 LFSR 초기키를 찾기 위한 계산복잡도는 $\prod_{i=0}^{N}(2^{L_i}-1)$에서 $\sum_{i=1}^{N}(2^{L_i}-1)$로 크게 떨어진다.

Siegenthaler[15]는 일반형 난수열 발생기에서 입력 변수가 독립적이고 균일분포를 갖고 있다(independent & uniformly distributed)는 가정하에서, 출력변수와 임의의 m개의 입력변수 부분 집합(subset)간에 상호정보(mutual

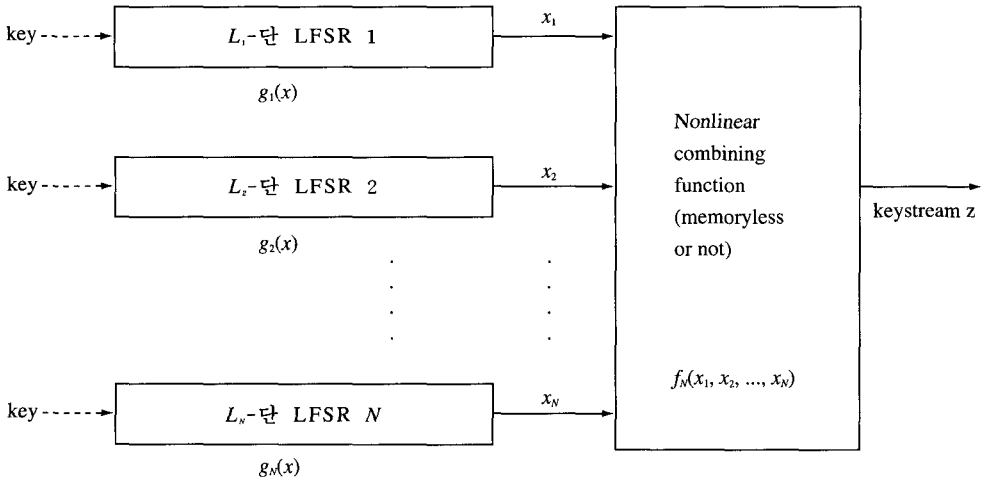


그림 2-3. 난수열 발생기(일반형)

information)가 0일 때 난수열 발생기는 m차 상관면역도(mth order of correlation immunity)를 갖는다고 정의하였으며, 수식으로 표기하면 다음과 같다.

$$I(Z^j; X_{i1}^j, X_{i2}^j, \ldots, X_{im}^j) = 0, \; j \geq 0 \qquad (2\text{-}4)$$

여기서, $X_i^j = (x_{i0}, x_{i1}, \ldots, x_{ij})$, $Z^j = (z_0, z_1, \ldots, z_j)$이며, x_{ij}는 i번째 입력수열 (x_i)의 j 순간값, z_j는 출력수열 (z)의 j 순간값을 나타낸다.

[정리 2.3] (Siegenthaler) 메모리없는 일반형 함수 $f_N(x_1, x_2, \ldots, x_N)$의 비선형 차수(k)와 상관면역도(m) 사이에는 다음과 같은 tradeoff 특성이 있다.

$$k+m \leq N-1, \; 1 \leq m \leq N-2 \qquad (2\text{-}5)$$

한편 Zhen등[16]은 walsh 변환을 이용하여 주파수 측면에서 상관면역도를 해석하였다. 두 벡터를 $X = (x_0, x_1, \ldots, x_{N-1})$, $W = (w_0, w_1, \ldots, w_{N-1})$이라 할 때 내적은 $X \cdot W = x_0w_0 + x_1w_1 + \ldots + x_{N-1}w_{N-1}$이 되며, 그림 2-3의 일반형에 대한 walsh 변환 F(w) 및 역변환 f(x)는 다음과 같다.

$$F(w) = \sum_{x=0}^{2^N-1} f(x)(-1)^{x \cdot w} \qquad (2\text{-}6)$$

$$f(x) = 2^{-N} \sum_{w=0}^{2^N-1} F(w)(-1)^{x \cdot w} \qquad (2\text{-}7)$$

[정리 2.4] (Zhen과 Massey) N개 2진 변수들에 대하여 부울함수 f(x)가 m차 상관면역도($0 \leq m \leq N-1$)를 가질 필요충분조건은 다음과 같다.

$$F(w) = 0, \; 1 \leq H(w) \leq m \qquad (2\text{-}8)$$

여기서, H(w)는 w의 Hamming weight 즉, w를 이진 표현했을 때 "1"인 비트 수를 뜻한다.

3. 이진 수열 발생기 분석 및 제안

3.1 합산 수열 발생기 분석

Rueppel[5-6]이 제안한 합산 수열 발생기(summation generator)는 그림 3-1과 같이 2개의 LFSR 출력 sequence와 과거 carry를 이용하여 비선형 함수의 출력을 다음과 같이 얻는

다.

합산 수열 발생기 :

$$z_j = a_j \oplus b_j \oplus c_{j-1}$$
$$c_j = a_j b_j \oplus (a_j \oplus b_j) c_{j-1} \quad j = 0, 1, 2, \ldots$$

여기서 (a_j)는 LFSR 1 수열, (b_j)는 LFSR 2 수열, (c_j)는 carry 수열, $c_{-1}=0$(carry 초기값)이다.

[정리 3.1] (Rueppel) 합산 수열 발생기에 대한 비도요소 특성은 다음과 같다.

1) 주기 $P_{SG}=(2^{L_1}-1)(2^{L_2}-1)$: 최대 주기

2) 난수특성 : 양호함

3) 선형복잡도 $LC_{SG} \le P_{SG}$ (최대 근사 선형복잡도)

4) 상관면역도 $m_{SG}=1$: 최고 차수 상관면역도

정리 3.1에서 알 수 있듯이 합산 수열 발생기는 기존의 Geffe 발생기[3]등과는 비교할 때 매우 큰 선형복잡도와 최대 차수 상관면역도를 동시에 갖고 있지만, carry와 출력간의 상관관계 특성으로 인하여 Meier등[7]과 Dawson[8]에 의해서 분석되었다.

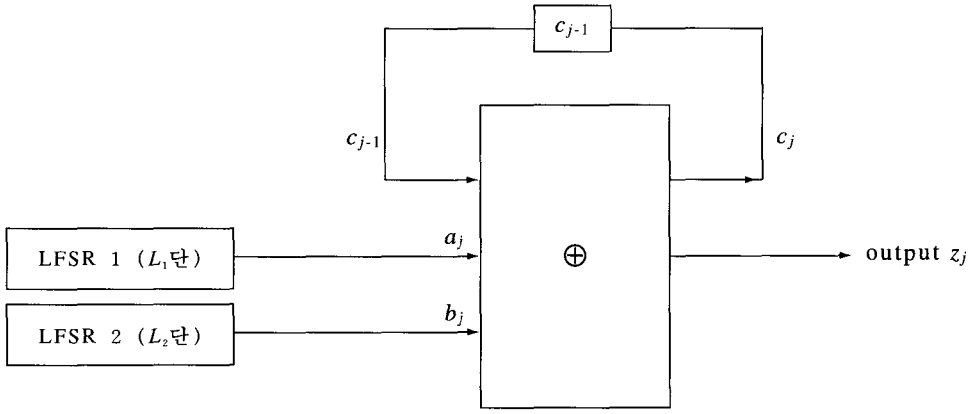


그림 3-1. 합산 수열 발생기

[정리 3.2] (Meier와 Staffelbach)

(1) 합산 수열 발생기 출력이 $z_{j+1}=z_{j+2}=\ldots=z_{j+s}=0$ 및 $z_{j+s+1}=1$을 만족하면, $1 \le t \le s$인 임의의 t에 대하여 아래 s-t+2개의 방정식이 최소한 $1-2^{-t}$확률로 동시 만족한다.

$$\begin{aligned} z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} + 1 = 0, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} + 1 = 0, \\ &\cdots\cdots \\ z_{j+s+1} &= a_{j+s+1} + b_{j+s+1} + 1 = 1, \\ z_{j+s+2} &= a_{j+s+2} + b_{j+s+2} + a_{j+s+1} \end{aligned} \qquad (3\text{-}1)$$

(2) 합산 수열 발생기 출력이 $z_{j+1}=z_{j+2}=\ldots=z_{j+s}=1$ 및 $z_{j+s+1}=0$을 만족하면, $1 \le t \le s$인 임의의 t에 대하여 아래 s-t+2개의 방정식이 최소한 $1-2^{-t}$ 확률로 동시 만족한다.

$$\begin{aligned} z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} = 1, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} = 1, \\ &\cdots\cdots , \\ z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} = 0, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} + a_{j+t+1} \end{aligned} \qquad (3\text{-}2)$$

3.2 무상관 합산키 발생기 분석

이상진 등[9]은 합산 수열 발생기의 출력에 적당한 난수열을 XOR하여 출력으로부터 carry를 유추할 수 없도록 하는 무상관 합산키 발생기(그림 3-2)를 다음과 같이 제안하였다.

무상관 합산키 발생기:

$z_j = a_j \oplus b_j \oplus c_{j-1} \oplus b_{j+k}$

$c_j = a_j b_j \oplus (a_j \oplus b_j) c_{j-1} \quad j = 0, 1, 2, \ldots$

여기서 (a_j)는 LFSR 1 수열, (b_j)는 LFSR 2 수열, (c_j)는 carry 수열, $c_{-1}=0$(carry 초기값)이다.

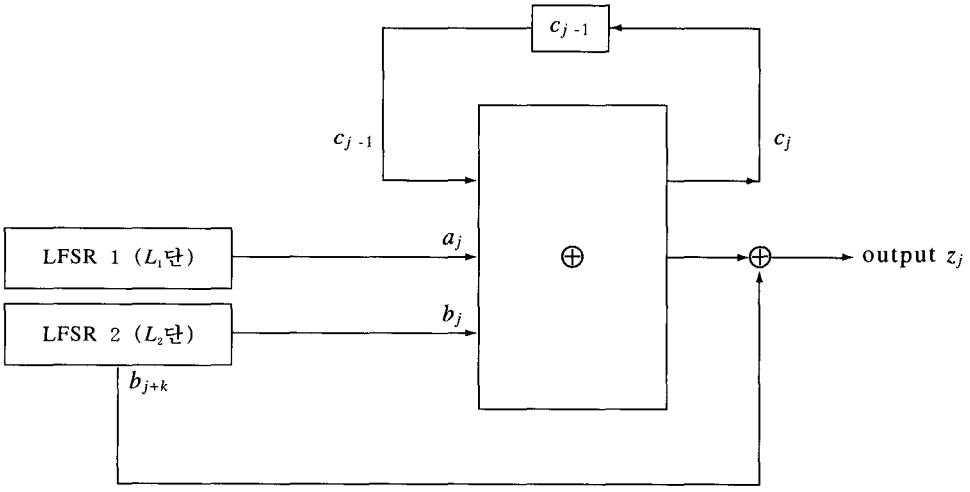


그림 3-2. 무상관 합산 키 발생기

[정리 3.3] (이상진 등) 무상관 합산키 발생기의 주기, 선형복잡도 및 상관면역도는 다음과 같다.

1) 주기 $P_{LEE} = (2^{L_1}-1)(2^{L_2}-1)$ 단, 위상이 일치 않는 한가지 경우 제외[9]

2) 선형복잡도 $LC_{LEE} \fallingdotseq LC_{SG}$(같거나 특별한 한가지 경우 q만큼 작음)

3) 상관면역도 $m_{LEE}=1$(최고차수 상관면역도)

그러나 상기 발생기는 LFSR 2 출력 b_j에 대하여 k비트 시차를 두고 b_{j+k}로 출력 z_j에 선형적으로 XOR시킴으로써 LFSR 2를 해석할 경우 비선형 함수를 분석할 우회방법을 제공할 수도 있다. 즉, b_j와 b_{j+k}의 상관성 $r_j = b_j \oplus b_{j+k}$ (0 또는 1)이 알려질 경우 전체 시스템의 안전성은 LFSR 2를 제외한 나머지 함수를 분석하는 문제로 축소될 수도 있다.

3.3 2비트 메모리를 갖는 개선된 합산 수열 발생기 제안

2비트 메모리를 갖는 개선된 합산 수열 발생기는 그림 3-3과 같이 2개의 LFSR로 부터 얻은 sequence(a_j, b_j)와 과거 carry(c_{j-1}) 및 새로 추가된 과거 메모리(d_{j-1})를 XOR하여 비선형 함수 출력을 다음과 같이 얻는다.

제안된 발생기:

$z_j = y_j \oplus d_{j-1}$

$d_j = f(a_j, b_j, d_{j-1}) = b_j \oplus (a_j \oplus b_j) d_{j-1}$

여기서 y_j는 j 순간의 합산 수열 발생기 출

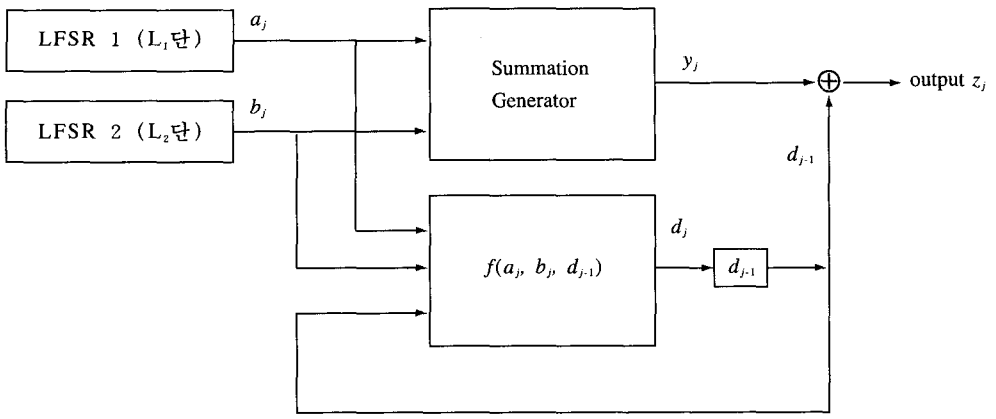


그림 3-3. 2 1비트 메모리를 갖는 기선된 합산 수열 발생기

력, (a_j)는 LFSR 1의 출력 수열, (b_j)는 LFSR 2의 출력 수열, (d_j)는 memory 수열, $d_{-1}=0$ (메모리 초기값), j=0, 1, 2 ...이다.

합산 수열 발생기는 carry-출력간 상관확률이 1/4로 매우 큰 상관성을 갖기 때문에 출력에 연속된 "0" 또는 "1"이 나타날 때 상관성 공격[7-8]에 의하여 해독될 수 있지만, 본 발생기에서는 상관성 확률이 1/2인 비선형 함수(메모리 비트)를 합산 수열 발생기의 출력에 추가로 XOR함으로서 출력으로부터 carry 뿐만 아니라 메모리를 유추할 수 없도록 보완하였다. 또한, 무상관 합산키 발생기에서는 선형 LFSR의 출력을 k 비트 시차를 두고 2번 사용하면서 합산 수열 발생기 출력단에 XOR 하였지만, 본 발생기에서는 비선형 함수(메모리 비트) 출력을 XOR시킴으로써 무상관 합산키 발생기의 약점도 보완하였다.

4. 비도요소 비교 분석

4.1 상관 관계 특성 비교 분석

합산 수열 발생기의 입-출력 상관성 및 carry-출력 상관성은 표 4-1에 나타낸 바와 같이 조사되었다. 표에서 알 수 있듯이 입-출력 상관성은 각각 1/2로 양호한 것으로 조사되었지만, carry-출력간 상관 확률은 1/4로 편중됨을 알 수 있다. 그러나 제안된 발생기의 경우 입력(a_j, b_j, c_{j-1} 또는 d_{j-1})과 출력 z_j 간의 상관 확률은 표 4-2와 같이 각각 1/2이 되어 상관성이 없으며, 각 메모리(c_j 또는 d_j)와 출력 z_j 간에도 상관확률이 1/2로 나타났다. 그러므로 제안된 발생기에서는 상관관계 특성이 크게 개선되었음을 알 수 있다.

4.2 비도요소 분석

제안된 발생기의 주기, 선형복잡도 및 상관면역도등 비도요소 특성을 분석하면 다음과 같다.

[정리 4.1] 길이가 L_1, L_2인 두 LFSR로 구성된 2 비트 메모리를 갖는 개선된 합산 수열 발생기에서 $\gcd(L_1, L_2)=1$일 경우 전

〈표 4-1〉 합산 수열 발생기의 입·출력 상관관계 특성

a_j	b_j	c_{j-1}	c_j	z_j	상관성 확률
0	0	0	0	0	*입출력 상관확률
0	0	1	0	1	$P[a_j = z_j] = 1/2$
0	1	0	0	1	$P[b_j = z_j] = 1/2$
0	1	1	1	0	$P[c_{j-1} = z_j] = 1/2$
1	0	0	0	1	
1	0	1	1	0	*carry-출력 상관확률
1	1	0	1	0	$P[c_j = z_j] = 1/4$
1	1	1	1	1	

〈표 4-2〉 제안된 발생기의 상관관계 특성

a_j	b_j	c_{j-1}	d_{j-1}	c_j	y_j	d_j	z_j	상관성 확률
0	0	0	0	0	0	0	0	
0	0	0	1	0	0	0	1	
0	0	1	0	0	1	0	1	
0	0	1	1	0	1	0	0	*입출력 상관확률
0	1	0	0	0	1	1	1	$P[a_j = z_j] = 1/2$
0	1	0	1	0	1	0	0	$P[b_j = z_j] = 1/2$
0	1	1	0	1	0	1	0	$P[c_{j-1} = z_j] = 1/2$
0	1	1	1	1	0	0	1	$P[d_{j-1} = z_j] = 1/2$
1	0	0	0	0	1	0	1	
1	0	0	1	0	1	1	0	*carry-출력 상관확률
1	0	1	0	1	0	0	0	$P[c_j = z_j] = 1/2$
1	0	1	1	1	0	1	1	$P[d_j = z_j] = 1/2$
1	1	0	0	1	0	1	0	
1	1	0	1	1	0	1	1	
1	1	1	0	1	1	1	1	
1	1	1	1	1	1	1	0	

체주기 $P_{SG2} = (2^{L_1}-1)(2^{L_2}-1)$이 된다. 단, 두 LFSR의 초기값이 모두 0일 경우는 각각 제외되어야 하며, 또한 두 LFSR이 모두 초기 상태가 될 때 d=0로 설정한다.

(증명) $j \geq 0$, 수열 a_j의 주기 P_a, 수열 b_j의 주기 P_b, 추정되는 주기 $P = \mathrm{lcm}(P_a, P_b)$라 두면,

$$d_j = b_j \oplus (a_j \oplus b_j) d_{j-1} = b_j \oplus (a_j \oplus b_j)[b_{j-1} \oplus b_{j-2}(a_{j-1} \oplus b_{j-1}) \oplus b_{j-3}(a_{j-2}a_{j-1} \oplus a_{j-2}b_{j-1} \oplus \dots \oplus b_{j-2}b_{j-1}) \oplus \dots \oplus b_0(a_1 \dots a_{j-1} \oplus b_1 \dots b_{j-1})]$$

$$d_{j+p} = b_{j+p} \oplus (a_{j+p} \oplus b_{j+p})[b_{j-1+p} \oplus b_{j-2+p}(a_{j-1+p} \oplus b_{j-1+p}) \oplus b_{j-3+p}(a_{j-2+p}a_{j-1+p} \oplus a_{j-2+p}b_{j-1+p} \oplus \cdots \oplus b_{j-2+p}b_{j-1+p}) \oplus \cdots \oplus b_p(a_{1+p} \cdots a_{j-1+p} \oplus \cdots \oplus b_{1+p} \cdots b_{j-1+p}) \oplus d_p]$$

이고, $d_P = 0$(두 LFSR이 모두 초기상태일 때 0임), $b_{j+P} = b_j$, $a_{j+P} = a_j$이므로 $d_{j+P} = d_j$가 되어 d_{j-1}의 주기는 $P_d = P = \mathrm{lcm}(P_a, P_b)$이 된다.

한편, y_j의 주기는 Rueppel[5-6]에 의하여 증명된 바와 같이 $P_y = \mathrm{lcm}(P_a, P_b)$이며, 두 수열 y_j와 d_{j-1}의 XOR된 수열인 본 발생기의 전체주기는 $\gcd(L_1, L_2) = 1$일 경우 정리 2.1의 b)에 따라 $P_{SG2} = \mathrm{lcm}(P_y, P_d) = \mathrm{lcm}(P_a, P_b) = (2^{L_1}-1)(2^{L_2}-1)$가 된다.

[정리 4.2] 2 비트 메모리를 갖는 개선된 합산 수열 발생기에서 선형복잡도 LC_{SG2}는 거의 주기에 근접하며 최대값은 주기와 같다.

합산 수열 발생기와 제안된 발생기의 짧은 단수 LFSR에 대한 주기 및 선형 복잡도 시뮬레이션 결과는 표 4-3과 같다. 특히, 선형복잡도는 Berlekamp-Massey 알고리즘[11]으로 컴퓨터 시뮬레이션 확인 결과 거의 주기에 근사하는 값이 되며, 특별한 경우에는 주기와 동일한 값이 얻어짐을 알 수 있다.

〈표 4-3〉 주기 및 선형복잡도 시뮬레이션 예(작은 값 L_1, L_2)

두개의 LFSR 단수		합산 수열 발생기		제안된 발생기	
L_1	L_2	P_{SG}	LC_{SG}	P_{SG2}	LC_{SG2}
3	4	105	100	105	103
3	5	217	208	217	217
4	5	465	455	465	463

[정리 4.3] 2 비트 메모리를 갖는 개선된 합산 수열 발생기의 상관면역도 m_{SG2}는 최고값인 1차가 된다.

(증명) 정리 2.4에 따라 walsh transform 값을 구하면 아래표와 같으며, 표에서 알 수 있듯이 $w = 0000_B$와 $w = 1111_B$를 제외한 나머지 모든 w에 대하여 $F(w) = 0$가 되므로 메모리 입력 2비트를 포함한 상관면역도는 3차가 된다. 한편, 정리2.3에 의하여 최고 차수 상관면역도는 $m_{max} = N-1 = 2-1 = 1$이므로 본 발생기는 메모리 입력 2 비트를 제외하면 최고 차수인 1차 상관면역도를 갖는다.

〈표 4-4〉 walsh 변환 결과

w	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(w)$	8	0	0	0	0	0	0	0	0	0	0	0	0	0	-8

4.3 난수성 검증

제안된 발생기의 난수열 전 주기에 대한 난수성 검증은 불가능하므로 적당한 길이로 표본추출(sampling)한 난수열의 local randomnes[2]를 검증하였으며, 그 결과를 다음 표4-5에 나타내었다. 검증방법으로는 몇가지 항목에 대한 이상적인 경우의 난수열에 대한 적합도를 검증하였으며, 여기에는 널리 알려진 Chi-square test를 사용하였다. 그리고 판정치를 결정하는

유의수준(significance level)은 일반적 값인 = 0.05를 택하였다. Chi-square 분포는 참고문헌[2]에서 취하였고, 검증항목은 Frequency test,[2] Serial test,[2] Generalized serial test,[10] Poker test[2] 및 Autocorrelation test[2]를 적용하였다.

난수성 검증 분석을 위하여 제안된 발생기에 임의의 초기키를 설정한 후 아래의 3가지 발생기에 대하여 약 16만 비트씩 3개군의 표본 난수열를 무작위로 추출하였다. 난수성 검증을 위하여 선택된 발생기는 (31단, 33단), (63단, 65단) 및 (127단, 131단)으로 구성된 LFSR 쌍을 갖는 3가지 경우이다.

- 예제 발생기 1 : $P(X) = X^{31} + X^3 + 1$
  (초기값 = 10101010...101)
  $Q(X) = X^{33} + X^{13} + 1$
  (초기값 = 11111111...111)
- 예제 발생기 2 : $P(X) = X^{63} + X^1 + 1$
  (초기값 = random)
  $Q(X) = X^{65} + X^{18} + 1$
  (초기값 = random)
- 예제 발생기 3 : $P(X) = X^{127} + X^1 + 1$
  (초기값 = random)
  $Q(X) = X^{131} + X^{13} + X^2 + X^1 + 1$
  (초기값 = random)

3개의 발생기에서 구한 표본 난수열에 대한 검증결과를 요약하면 아래 표4-5와 같다. 표에서 보는 바와 같이 3개의 표본데이터는 Frequency test, Serial test, Generalized serial test(t = 3, 4, 5), Poker test(m = 3,4,5), 및 Autocorrelation test를 각각 5% 유의수준으로 통과하는 좋은 난수특성을 갖는다.

4.4 종합 비교

합산 수열 발생기는 carry-출력간 상관확률이 1/4로 매우 큰 상관성을 갖기 때문에 출력에 연속된 "0" 또는 "1"이 나타날 때 상관성 공격[7-8]에 의하여 해독될 수 있지만, 본 발생기는 메모리-출력 상관확률이 1/2인 비선형 메모리값을 합산 수열 발생기의 출력에 XOR하므

〈표 4-5〉 난수특성 검증 결과

검증 항목	판정치	검증 결과		
		표본 1	표본 2	표본 3
1) Frequency test	3.84	0.027	0.005	2.042
2) Serial test	5.99	1.390	0.023	2.233
3) Generalized t-serial test				
t = 3	9.48	6.919	1.836	3.696
t = 4	15.50	12.459	3.412	5.462
t = 5	26.29	23.057	12.727	7.762
4) Poker test				
m = 3	14.067	6.185	7.035	6.850
m = 4	24.996	17.287	7.617	17.510
m = 5	44.654	37.304	24.487	20.592
5) Autocorrelation test	max. ≤ 0.05	max. = 0.0060	max. = 0.0063	max. = 0.072

〈표 4-6〉 유사 발생기 비교

비교 항목	합산 수열 발생기	무상관 합산키 발생기	제안된 발생기
주 기	$P_{SG}=(2^{L_1}-1)(2^{L_2}-1)$	$P_{LEE}=(2^{L_1}-1)(2^{L_2}-1)$ 단, 한가지 예외 있음	$P_{SG2}=(2^{L_1}-1)(2^{L_2}-1)$
난 수 성	양호함	양호함	양호함
선형복잡도	$LC_{SG}\fallingdotseq P_{SG}$	$LC_{LEE}\fallingdotseq P_{LEE}$	$LC_{SG2}\fallingdotseq P_{SG2}$
상관면역도 차수(CI)	$m_{SG}=1$차	(unknown)	$m_{SG2}=1$차
상관성 공격 취약성	취약함(연속 동일한 출력 발생시)	LFSR 선형출력을 k 비트후 재사용하므로 불안전함.	안전함.

로 안전하다. 즉, 비선형 함수(메모리 비트)를 출력에 추가 XOR함으로서 출력으로부터 carry 뿐만 아니라 메모리를 유추할 수 없게 함으로써 합산 수열 발생기의 단점을 보완하였다. 또한, 무상관 합산키 발생기에서는 선형 LFSR의 출력을 k 비트 시차를 두고 2번 사용하면서 합산 수열 발생기 출력단에 XOR 하였지만, 본 발생기에서는 비선형 함수(메모리 비트) 출력을 XOR시킴으로써 무상관 합산키 발생기의 약점도 보완하였다. 결론적으로, 제안된 발생기는 2 비트 메모리의 사용으로 인하여 입-출력간 상관성 및 carry-출력간에 상관성이 없는 무상관 발생기일 뿐 아니라 주기, 선형복잡도, 상관면역도 및 구현복잡도 측면에서는 합산 수열 발생기의 수준을 유지하면서 carry-출력간 분석을 통한 상관성 공격에 안전한 발생기임을 알 수 있다.

5. 결 론

스트림 암호에서 강력한 분석 방법인 상관성 공격에 대하여 비메모리 함수인 Geffe's Generator등은 취약한 방식으로 판명되었으나 메모리 형태인 합산 수열 발생기는 입·출력 무상관 특성으로 인하여 안전한 방식으로 인식되었었다. 그러나 합산발생기는 출력값이 연속 "0" 또는 "1"을 갖을 경우 carry 값을 쉽게 유추할 수 있기 때문에 Dawson, 이상진등은 이에 대한 보완책으로 각각 변형방식을 제안하였다. 하지만 Dawson 발생기는 비도요소에 대한 분석이 없으며, 무상관 합산키 발생기는 선형 LFSR 출력을 k 클럭 시차를 두고 2번 사용될 뿐만 아니라 최대주기가 보장되지 않는다는 단점이 있다. 그리고 합산 수열 발생기 및 무상관 합산키 발생기는 1 비트 메모리를 갖는 비선형 결합함수이며, 본 논문에서는 새로운 개념으로서 2 비트 메모리를 갖는 발생기를 제안하였다.

제안된 발생기는 메모리-출력 상관확률이 1/2인 비선형 메모리값을 출력에 XOR하므로서 합산 수열 발생기와는 달리 출력값이 연속해서 "0" 또는 "1"이 나타날 때에도 상관성 공격에 안전하다. 또한, 무상관 합산키 발생기에서는 선형 LFSR의 출력을 k 비트 시차를 두고 2번 사용하면서 합산 수열 발생기 출력단에 XOR 하였지만, 본 발생기에서는 비선형 함수(메모리 비트) 출력을 XOR시킴으로써 무상관 합산키 발생기의 약점을 보완하였다. 그러므로 제안된 발생기는 입-출력간 상관성 및 carry-출력간에 상관성이 없는 무상관 발생기일 뿐 아니라 주기, 선형복잡도, 상관면역도 및 구현복잡도 측면에서는 합산 수열 발생기

의 수준을 유지하면서 carry-출력간 상관성 공격에 안전한 발생기임을 알 수 있다.

참 고 문 헌

[1] van Tilborg, H. C. A., An Introduction to Cryptology, KLUWER ACADEMIC PUBLISHERS, Boston, etc., 1988.

[2] H. J. Beker and F. C. Piper, Cipher systems : The Protection of Communica -tions, Northwood Books, London, 1982.

[3] P. R. Geffe, "How to Protect Data with Ciphers that are really hard to Break," Electronics, pp.99-101, Jan. 1973.

[4] T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only," IEEE Trans. on Computer, Vol. C-34, N0.1, pp.81-85, Jan. 1985.

[5] R. A. Rueppel, "Correlation Immunity and the Summation Generator," Advances in Cryptology, Proceedings of CRYPTO'85, pp. 260-272, 1985.

[6] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

[7] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers," Journal of Cryptology, Vol.5, pp.67-86, 1992.

[8] E. Dawson, "Cryptanalysis of Summation Generator," Advances in Cryptology - AUSCRYPT'92, Lecture Notes in Computer Science, Springer-Verlag, pp.209-215, 1993.

[9] 이상진, 지성택, 김용대, 고승철, "상관관계 공격에 안전한 합산 키 수열 발생기," 통신정보보호학회 논문지, 제5권, 제2호, pp.15-22, 1995년 6월.

[10] M. Kimberley, "Comparision of Two Statistical Tests for Keystream Sequences," Electronics Letters, Vol.23, No.8, pp.365-366, Apr. 1987.

[11] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Trans. on Infor. Theo., Vol. IT-15, No. 1, pp.122-127, Jan. 1969.

[12] R. A. Rueppel and O. J. Stafflebach, "Products of Linear Recurring Sequences with Maximum Complexity," IEEE Trans. on Infor. Theo., Vol. IT-33, No. 1, pp. 124-131, Jan. 1987.

[13] T. Siegenthaler, "Design of Combiners to Prevent Divide and Conquer Attacks," Advances in Cryptology, Proceedings of CRYPTO'85, pp. 273-279, 1985.

[14] W. Meier and O. Staffelbach, "Fast Correlation Attacks on Stream Ciphers," Journal of Cryptology, Vol.1, pp.159-176, 1989.

[15] T. Siegenthaler, "Correlation-Immunity of Nonlonear Combining Functions for Cryptographic Applications," IEEE Trans. on Infor. Theo., Vol.IT-30, No. 5, pp. 776-780, Sep. 1984.

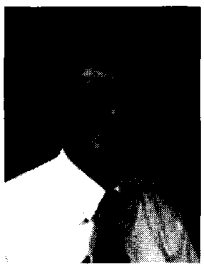
[16] X. G. Zhen and J.L. Massey, "A Spectral Characterization of Correlation - Immune Combining Functions," IEEE Trans. on Infor. Theo., Vol.34, No. 3, May 1988.

□ 著者紹介

이 훈 재

1985년 2월 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1987년 2월 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1987년 2월 ~ 현재 국방과학연구소 선임연구원
1993년 3월 ~ 현재 경북대학교 정보통신 박사과정

※ 주관심분야 : 정보보호기술, 디지털 통신, 정보통신망



문 상 재

1972년 2월 서울대학교 공과대학 공업교육과(전자공학, 공학사)
1974년 2월 서울대학교 대학원 전자공학과(통신공학, 공학석사)
1984년 6월 미국 UCLA(통신대학, 공학박사)
1984년 6월 ~ 85년 6월 UCLA Postdoctor 근무
1984년 6월 ~ 85년 6월 미국 OMNET 컨설턴트
1974년 ~ 현재 경북대학교 공과대학 전기전자공학부 교수

※ 주관심분야 : 정보보호, 디지털 통신, 정보통신망