通信情報保護學會論文誌
第7卷 第3號, 1997. 9

다수열 출력 이진 수열 발생기

이 훈 재*, 문 상 재**

Binary Sequence Generator with a Large Number of Output Sequences

Hoon Jae Lee, Sang Jae Moon

요 약

출력 수열의 수가 스트림암호의 새로운 평가요소로서 제안된 바 있으나 일반적으로 발표된 대부분의 이진 수열 발생기는 출력 수열이 1개 뿐인 것으로 알려졌다. 본 논문에서는 출력 수열의 수가 여러개인 다수열 출력 이진 수열 발생기를 2가지 유형으로 제안하였다. 첫 번째는 여러개의 feedback tap 중 하나를 초기키에 따라 선택하는 Switched-Tap LFSR(STLFSR)과 이를 이용한 일반형 모델 및 Geffe 발생기의 적용 예를 제안하였다. 나머지는 다수열 출력 수열로 이미 알려진 golic의 메모리 수열 발생기(MEM-BSG)를 개선하여 대용량 메모리 사용이 가능하도록 일반화시킨 대용량 메모리형 다수열 출력 발생기(GMEM-BSG)를 제안하고, 이 발생기의 주기, 선형복잡도 및 출력 수열의 수를 분석하였다.

Abstract

The number of output sequence was proposed as a characteristic of binary sequence generators for cryptographic application, but in general most of binary sequence generators have single number of output sequence. In this paper, we propose two types of binary sequence generators with a large number of output sequences. The first one is a Switched-Tap LFSR (STLFSR) and it applies to the generalized nonlinear function and the Geffe's generator as example. The other is a generalized memory sequence generator(GMEM-BSG) which is an improved version of the Golic's memory sequence generator (MEM-BSG) with a large number of output sequences, and its period, linear complexity, and the number of output sequence are derived.

---

* 국방과학연구소
* * 경북대학교 전기전자공학부

1. 서 론

Beker와 Piper[1]는 스트림 암호의 출력 수열에 대한 요구조건으로 다음과 같이 3가지 요건을 제안하였다. 그 후에 Sigenthaler[3]는 상관면역도를, Golic[4]은 출력 수열의 수를 필요성으로 제기함에 따라 두가지 항목을 더 추가하여 5가지 요구조건을 정리하였으며, 특히 본 논문에서는 출력 수열의 수에 대하여 알아보려 한다.

(스트림 암호의 요구조건)
1) 출력 수열은 주기에 대한 최소값이 보장될 것
2) 출력 수열은 좋은 난수성을 갖을 것
3) 출력 수열은 큰 선형복잡도를 갖을 것
*4) 출력 수열은 충분한 정도의 상관면역도 차수를 갖을 것
*5) 출력 수열의 수가 충분히 많을 것

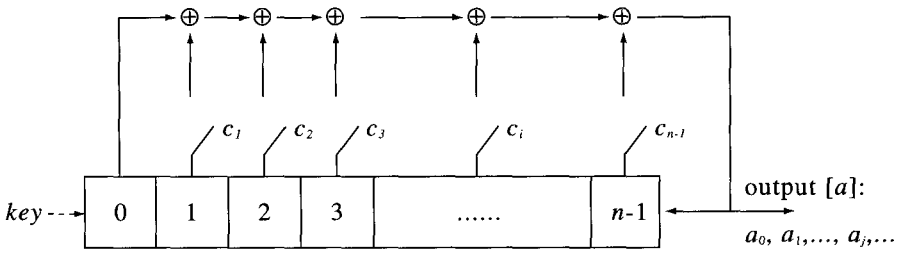
Golic은 스트림암호의 비도(crypto-degree)를 높이는 방안으로 출력 수열의 수를 새로운 평가요소로 제안하였다. 일반적으로 알려진 대부분의 이진 수열 발생기에서는 출력 수열이 1개 뿐이며, 이 경우 수열 발생기는 출발점만 다를 뿐 항상 동일한 수열 cycle을 따라 키수열이 발생된다. 하지만, 출력 수열이 2개 이상인 경우 초기화 값(키)이 변경됨에 따라 다른 수열 cycle의 출력 수열이 발생될 수 있기 때문에 암호분석이 그만큼 어려워진다.

본 논문에서는 스트림암호를 이용한 암호시스템에서 출력 수열의 수가 갖는 실질적인 의미를 살펴본 후 기존하는 어떤/임의 발생기에도 적용이 가능한 다수열 출력 이진 수열 발생기를 2가지 유형으로 제안하고자 한다. 즉, 스트림암호 시스템에서 난수동기에 따라 출력 수열 cycle이 변경되지 않을 경우 Dawson 공격[5]에 해독될 수 있음을 먼저 보여 준다. 그리고 출력 수열의 수를 늘릴 수 있는 구체적인 방안으로 여러개의 feedback tap 중 하나를 초기키에 따라 선택하는 Switched-Tap LFSR(STLFSR)과 이를 이용한 일반형 모델 및 Geffe 발생기의 적용 예를 제안한다. 또한 다수열 출력 수열로 이미 알려진 golic의 메모리 수열 발생기(MEM-BSG)를 개선하여 대용량 메모리 사용이 가능하도록 일반화시킨 대용량 메모리형 다수열 출력 발생기(GMEM-BSG)를 제안하고, 이 발생기의 주기, 선형복잡도 및 출력 수열의 수를 분석한다.

2. 출력 수열의 수

2.1 일반형 이진 수열 발생기

[정리 2.1] n-단 LFSR(그림 2-2 a))의 주기는



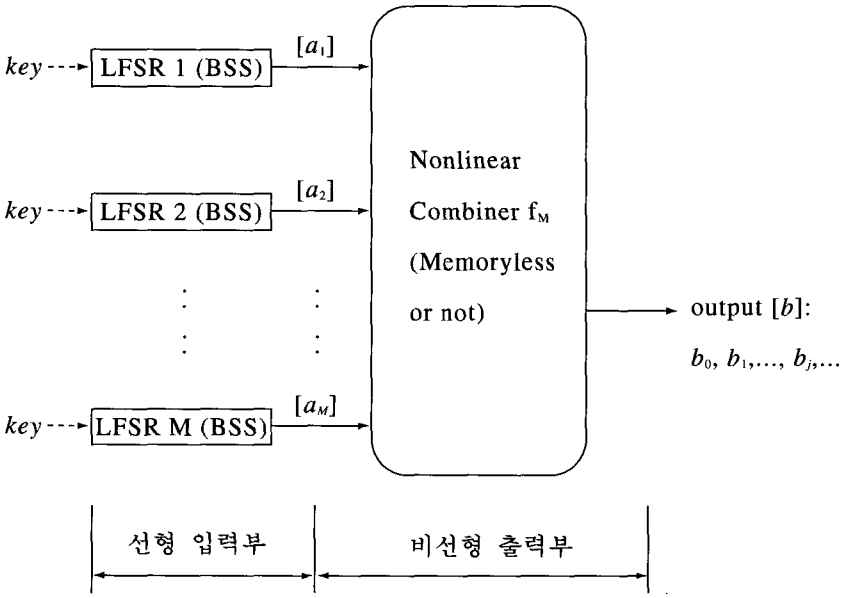
$f(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots+c_1x+1$

그림 2-1. Linear Feedback Shift Register(LFSR)

초기치가 nonnull 일때 최대주기를 갖으며, 그 주기는 (2^n-1)이 된다.[1-2] 이 때 n-단 LFSR은 원시다항식(primitive polynomial)으로부터 얻어진다.

[정리 2.2] n차 원시다항식의 총 갯수는 $\lambda(n) = \frac{\phi(2^n-1)}{n}$ 이며, 이는 최대주기를 만족하는 n단 LFSR의 feedback 함수의 총 갯수를 의미한다. 여기서 $\phi(n)$은 오일러 함수이다.

n-단 LFSR은 선형 출력을 발생하기 때문에 $2n$ 비트만 알면 feedback tap을 유추할 수 있으며[1-2], 일반적으로 이를 방지하기 위해 그림 2-2와 같이 여러개의 LFSR(선형 입력부)을 비선형적으로 조합(비선형 출력부)함으로서 출력 수열의 선형복잡도(linear complexity)를 증가시킨다.



* BSS : Binary Symmetric Source

그림 2-2. 일반형 수열 발생기

2.2 출력 수열의 수와 Dawson 공격

스트림 암호에서는 송/수신 키수열 발생기에서 발생되는 출력 수열의 동기가 일치되지 않으면 암호문을 평문으로 복호할 수 없기 때문에 송/수신 키수열 발생기의 동기를 일치시키는 문제가 필수적이다. 난수동기방식이란 송/수신 키수열 발생기에서 동일한 키수열을 발생시키고 그 키수열에서의 시작점을 일치시키는 방식을 말하며, 실제로 난수동기를 일치시키기 위해서는 추가적으로 동기신호를 교환해야 하는데 세션키도 동기신호에 포함될 수 있다. 난수동기방식은 난수동기를 일치시키는 횟수에 따라 초기동기방식(Initial Synchronization only) 또는 절대동기방식(Absolute

Synchronization)과 연속동기방식(Continuous Synchronization)으로 분류된다.[2] 초기동기방식은 그림 2-3 a)와 같이 암호통신 시작시에만 동기시켜 통신을 유지하는 방식이고, 연속동기방식은 b)와 같이 통신도중 주기적으로 재동기시키는 방식이다. 여기서 난수동기를 재동기시킨다는 뜻은 키수열의 시작점(starting point)을 바꾸고 통신동기를 재확립한다는 의미이다. 초기동기방식에서는 1-대-다수 통신시 나중 가입자(late entry)에게는 난수동기 불일치로 암호통신이 불가능한 문제가 생기지만, 연속동기방식에서는 통신 도중에 동기신호가 포함되어 있으므로 나중 가입자에게도 가입시점 이후 정보에 대해서는 통신가능하다. 결과적으로 연속동기방식은 통신중에도 동기신호가 포함되어 있으므로 통신효율은 떨어지지만 채널오류가 많은 무선통신망 또는 일방쌍신(Half Duplex)통신에서는 더 효과적일 수 있다.

한편, Dawson[5]은 동일한 키로 암호화시키는 스트림 암호시스템에 대하여 과거의 암호문을 갖고 있다면 현 암호문과 XOR시킴으로써 키수열은 서로 상쇄되고, 결과적으로 과거 평문과 현 평문이 XOR된 형태로 남기 때문에 평문의 redundant를 이용하여 암호해독이 가능함을 보였다. 즉, 과거 평문 $P' = p_0', p_1', p_2', \ldots$, 과거 키수열 $K' = k_0', k_1', k_2', \ldots$, 과거 암호문 $C' = c_0', c_1', c_2', \ldots$, 현 평문 $P = p_0, p_1, p_2, \ldots$, 현 키수열 $K = k_0, k_1, k_2, \ldots$, 현 암호문 $C = c_0, c_1, c_2, \ldots$, 이라 두면, 가정에서 $K = K'$ 이므로

$$C' = p_0' \oplus k_0,\ p_1' \oplus k_1,\ p_2' \oplus k_2,\ p_3' \oplus k_3,\ p_4' \oplus k_4,\ p_5' \oplus k_5, \ldots \quad (2\text{-}1)$$

$$C = p_0 \oplus k_0,\ p_1 \oplus k_1,\ p_2 \oplus k_2,\ p_3 \oplus k_3,\ p_4 \oplus k_4,\ p_5 \oplus k_5, \ldots \quad (2\text{-}2)$$

$$C \oplus C' = p_0' \oplus p_0,\ p_1' \oplus p_1,\ p_2' \oplus p_2,\ p_3' \oplus p_3,\ p_4' \oplus p_4,\ p_5' \oplus p_5, \ldots \quad (2\text{-}3)$$

가 되어 결국 암호문 2개를 XOR하면 평문 2개의 XOR 형태로 남기 때문에 Dawson의 방법대로 평문의 redundent를 이용하여 암호문이 해독될 수 있다. 그러므로, 이 문제를 해결

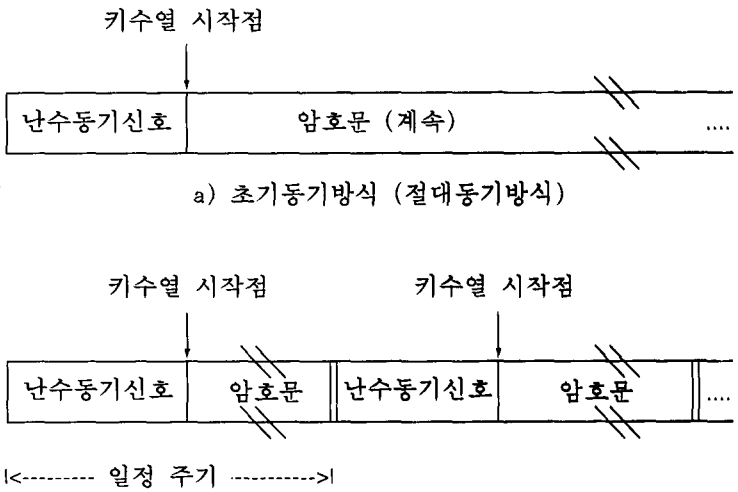


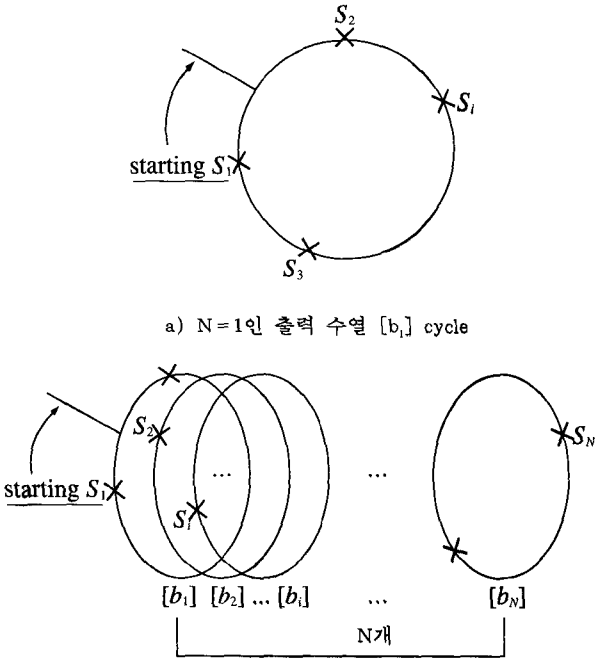
그림 2-3. 난수동기신호의 삽입위치

하기 위해서는 동기를 확립할 때마다 새로운 세션키(session key)로 초기화시켜야 하는데, 이러한 난수동기방식을 어떻게 설계하느냐에 따라 암호통신의 안전성과 통신성능 및 통신 신뢰성이 결정된다.

[정의 2.3] 어떤 수열 발생기에 대하여 초기값을 변경함으로서 주기가 같고 출력 수열 cycle이 변경될 수 있는 총 갯수를 **출력 수열의 수(number of output sequence) 또는 키수열 수**라 한다.

그림 2-4는 스트림암호를 이용한 암호통신에서 출력 수열이 1개 뿐인 경우와 여러개(N≥2)인 경우 암호분석적인 안전성은 어떤 차이가 나는지 살펴보기 위한 그림이다. 그림 a)에서 출력 수열이 1개뿐인 경우 초기키가 지정되면 출발점(starting point) S_1으로부터 정해진 수열 cycle을 따라 발생된 키수열이 암호화에 사용되고, 후속 통신시에도 동일한 수열 cycle 속에서 출발점만 S_2로 바뀌어서 키수열이 암호화에 사용되어지기 때문에 과거 키수열과 현재 키수열이 겹치는 부분에 대응되는 암호문은 Dawson 공격을 피할 수 없다. 그러나 $N \geq 2$이고 S_i가 속하는 수열 cycle과 $S_j(i \neq j)$가 속하는 수열 cycle이 서로 다를 경우(최상의 경우, 세션키 설정수 만큼의 출력 수열이 존재할 때) 세션키가 다른 통신에서는 키수열 cycle이 겹칠 수 없기 때문에 Dawson 공격에 안전하다고 할 수 있다. 게다가 일부분의 키수열로부터 나머지 키수열의 유추가 어렵고 세션키 설정 수(키 공간)가 충분히 크다고 가정하면 one-time pad와 유사한 수준의 perfect secrecy를 갖는 수열을 발생할 수도 있다.

그림 2-4에서 주기 P인 두 출력 수열 cycle $[b_i]$, $[b_j](i \neq j)$를 다음과 같이 나타내기로 한다.



a) N=1인 출력 수열 $[b_i]$ cycle

b) N≥2인 출력 수열 $[b_i]$ cycle

× : starting point

그림 2-4. 출력 수열 cycle의 구조

$[b_i]=b_{i0}, b_{i1}, b_{i2}, b_{i3}, \ldots, b_{ik}, \ldots, b_{i,P-1}, b_{i0}, b_{i1}, \ldots,$
$i=1,2,\ldots,N$ (2-4)

$[b_j]=b_{j0}, b_{j1}, b_{j2}, b_{j3}, \ldots, b_{jk}, \ldots, b_{j,P-1}, b_{j0}, b_{j1}, \ldots,$
$j=1,2,\ldots,N$ (2-5)

이 때 임의의 정수 $k(0\leq k\leq P)$와 j에 대하여 $[b_j]$ 수열을 k만큼 순회(cyclic rotate)시킨 수열 $\mathrm{Rot}([b_j], k)$와 $[b_i]$가 같지 않다면 출력 수열 cycle의 수는 N이 된다. 즉,

$$\mathrm{Rot}([b_j], k)\neq[b_i] \quad (2\text{-}6)$$

이 된다. 그리고 본 논문에서는 일반형 수열 발생기(그림 2-2)에서 출력 수열의 수를 늘릴 수 있는 방법으로 선형 입력부를 가변하는 방법과 비선형 출력부를 가변하는 방법을 각각 한가지씩 제안 하고자 한다.

3. Switched-Tap 다수열 출력 발생기

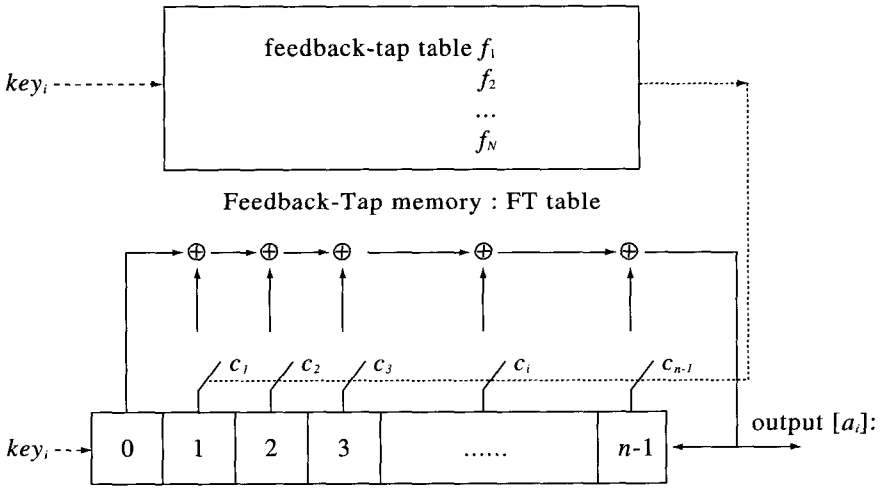
본 절에서는 일반형 수열 발생기(그림 2-2)에서 선형 입력부를 보완하여 switched-tap 다수열 출력 이진 수열 발생기를 제안한다.

3.1 Switched-Tab LFSR(STLFSR) 제안

[정리 3.1] n-단 LFSR의 출력 수열의 수는 단 1개 뿐이다.

(증명) n-단 LFSR은 그림 2-4 a)와 같이 항상 동일한 수열 cycle 내에서 초기값이 변경되면 출발점만 바뀌게 되므로 출력 수열의 수는 1개 뿐이다.

Feedback-tap이 고정된 일반 LFSR은 출력 수열이 단 1개만 존재한다. 하지만 n단 LFSR로 구성될 수 있는 feedback-tap의 총 갯수는 $\lambda(n)=\frac{\phi(2^n-1)}{n}$ 개이므로 본 논문에서는 feedback 함수를 변경하여 출력 수열의 수를 확대시킬 수 있는 Switched-Tap LFSR(STLFSR)을 제안한다. STLFSR은 그림 3-1과 같이 $N(1\leq N$



$f_i(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots+c_1x+1,\ i=1,2,\ldots,N$

그림 3-1. Switched-Tap LFSR(STLFSR)

$\leq\lambda(n)$)개의 feedback 함수 $f_i(i=1,2,..N)$를 memory에 저장하여 두었다가 세션키 key_i가 바뀔 때마다 feedback-tap 함수 f_i가 변경되도록 함으로서 결국 출력 수열 $[a_i]$는 N개의 출력 수열 cycle을 갖게 된다.

[정리 3.2] 메모리에 저장된 feedback-tap 함수의 수를 $N(1\leq N\leq\lambda(n))$이라 할 때 n-단 STLFSR의 출력 수열$[a_i]$의 수는 N개이다.
(증명) n단 LFSR의 *feedback* 함수 f_i의 갯수는 N이고, 세션키 key_i가 바뀔 때마다 feedback-tap 함수 f_i가 변경되기 때문에 출력 수열 $[a_i]$는 서로 다른 N개의 출력 수열 cycle을 갖는다.

3.2 Switched-Tap 다수열 출력 발생기

그림 2-2의 일반형 수열 발생기에서 출력 수열의 수를 증대시킬 수 있는 간단한 방법은 그림 3-2와 같이 M개의 LFSR 중에서 한 개(또는 여러개)를 선택하여 STLFSR로 대체함으로써 가능해진다. 이 경우 개선된 일반형 수열 발생기의 출력 수열의 수는 feedback-tap table의 갯수(N)만큼 커지기 때문에 적당히 N을 선택하면 설계에 필요한 최소 출력 수열의 수를 얻을 수 있다. 즉, 출력 수열 $[b_i]$ ($i=1,2,..N$)의 $t(t=0,1,2,...)$ 순간 출력은 $b_i(t)=f(a_1(t), a_2(t),...,a_{Mi}(t))$이고, $a_{Mi}(t)$값이 N개의 출력 수열을 갖기 때문에 $[b_i]$ 수열도 N개의 출력 수열을 갖는 것을 알 수 있다. Geffe 발생기[6]의 예를 들어 보면, 출력 수열의 수를 증대하기 위해서 그림 3-3과 같이 LFSR3 대신 STLFSR로 교체함으로서 N개의 출력 수열을 갖는 Geffe 발생기를 얻을 수 있다.

4. 대용량 메모리형 다수열 출력 발생기

본 절에서는 일반형 수열 발생기(그림 2-2)에서 비선형 출력부를 보완하여 대용량 메모리 형태의 다수열 출력 이진 수열 발생기를 제안코자 한다. 메모리를 이용하여 random 값을 생성하면서/읽게 되면 메모리의 내용에 따라서 LFSR의 초기값이 같을 경우에도 출력 키수열이 달라질 수 있기 때문에 출력 수열의 수를 크게 증가시킬 수 있다. 본 논문에서는

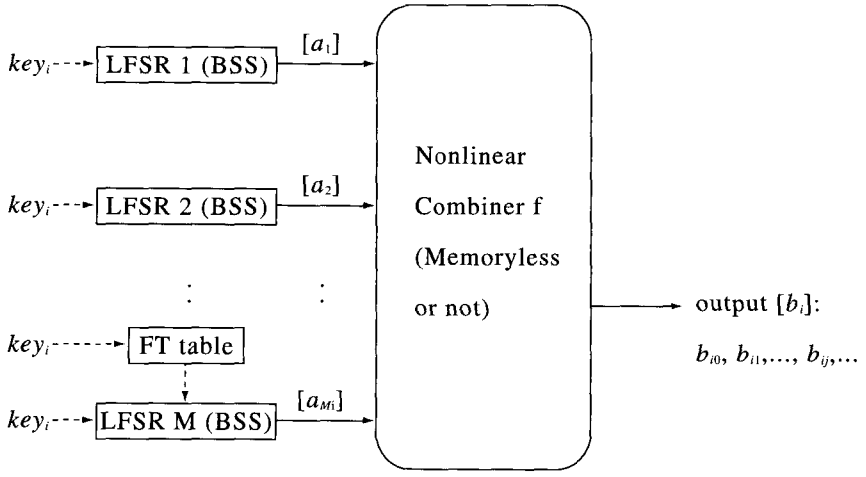


그림 3-2. Switched-Tap 다수열 출력 발생기(일반형)

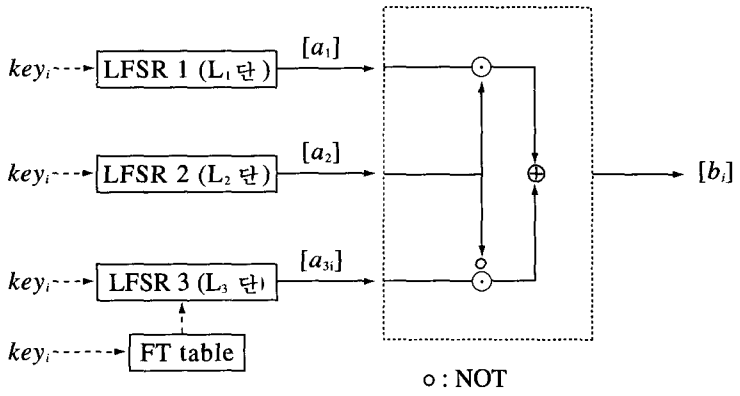


그림 3-3 Geffe 발생기 개선 예

기존의 메모리 형태 발생기와 출력 수열의 수의 관계로부터 새로운 메모리 수열 발생기를 도출하고자 한다.

4.1 MEM-BSG 발생기

메모리를 이용한 수열 발생기는 여러 가지 제안된 바 있다. MacLaren-Marsaglia 발생기[7]는 pointer(번지) 발생기로부터 메모리 번지를 임의 지정하여 메모리 내용을 읽은(read) 후 바로 그 자리에 value 발생기의 출력값을 쓰는(write) 메모리 발생기이다. 그러나 이 경우 메모리는 단순히 버퍼로서 random permutation시키는 효과만을 갖게 될 것이며, 아래와 같은 가정하에 Retter[8]에 의하여 기지평문공격(kwown-plaintext attack)으로 해독되었다.

(가정)

1) 어떤 순간에도 value 발생기는 0~R-1의 큰 수를 생성한다(range=R).
2) 어떤 수도 value 발생기의 한 주기내에서 반복되지 않는다.
3) table은 비교적 작다(range=T).
4) pointer 발생기는 랜덤하게 억세스한다.

이는 주어진 상당량의 출력 키수열로부터 value 발생기와 pointer 발생기의 초기값(키)를 찾아낼 수 있음을 의미한다. 즉, 상기 가정하에서 메모리의 어떤 번지도 평균적으로 T 시간 마다 한 번씩 임의 value가 메모리에 저장되는 것으로 예측되며, 만일 키수열 출력과 value 출력을 안다면 각 value 값이 메모리에 얼마나 오래동안 머물렀는지 계산할 수 있다. 이 때 value 발생기에 대하여 가짜 키가 선택되었을 경우에는 계산 지연 평균값=R이고, 진짜 키가 선택될 경우에만 계산 지연 평균값 $= \frac{RT}{R+T-1}$ 이 되므로 계산지연 평균값만 알면 진짜키를 찾아낼 수 있다.[8] 이에 대한 보완책으로 Retter는 value 발생기와 pointer 발생기를 서로 의존되게(dependent) 설계할 것, value 출력을 1-비트 크기로 최소화 할 것, 그리고 메모리를 대용량화할 것을 권장하였다.

Golic의 MEM-BSG 발생기[9-10]는 MacLaren-Marsaglia 발생기와 달리 write 번지와 read 번지가 별도로 구성되어 있어 메모리 write 시

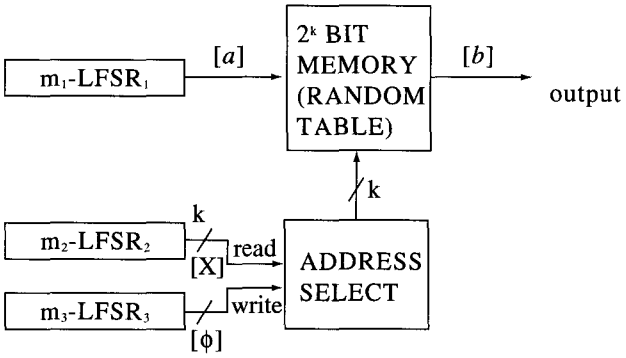


그림 4-1. Golic의 MEM-BSG 발생기

에는 write 발생기가 데이타 번지를 지정해주고, read 시에는 read 발생기가 데이터 번지를 지정해주기 때문에 이원화 분리에 따른 비선형성이 높다고 할 수 있다.

(MEM-BSG 발생기 설계 조건)[9-10]

C1: $1 \le k < \min(m_2, m_3)$

C2: $2^{m_3}-1 < m_1$

C3: m_1, m_2, m_3는 각각 쌍으로 서로소이다 (pairwise coprime).

C4: $3 \le k < m_2-2$라면, LFSR2의 k개 비트들은 등간격으로 출력되어야 한다.

[정리 4.1] (MEM-BSG의 주기, 선형복잡도)[9,10]
만일 MEM-BSG가 설계조건 C1-C4를 모두 만족하고, 모든 $\mathrm{LFSR}_i(i=1,2,3)$의 초기치가 nonnull일 때 출력수열 [b]에 대한 주기 P[b]와 선형복잡도 LC[b]는 다음과 같다.

$$P_1P_2 \mid P[b] \mid P_1P_2P_3 \tag{4-1}$$

$$m_1 \sum_{i=0}^{k} \binom{m_2}{i} \le LC[b] \le (2^{m_3}-1)m_1 \sum_{i=0}^{k} \binom{m_2}{i} \tag{4-2}$$

여기서 P_i는 LFSR_i의 주기를 말한다.

[정리 4.2] (MEM-BSG의 출력 수열의 수)[4]
만일 MEM-BSG 발생기가 Golic의 설계조건 C1, C2를 만족하고, 또한

$$\gcd(m_1, m_2) \neq m_1 \tag{4-3}$$

$$\gcd\left(P_2, \frac{P_1}{\gcd(P_1, P_2)}\right) = 1 \tag{4-4}$$

$$\gcd(P_3, P_1P_2) = 1 \tag{4-5}$$

를 만족할 때 출력 수열의 수는 $P_1P_2P_3$가 된다. 단, $\mathrm{LFSR}_i(i=1,2,3)$는 nonnull 초기상태이어야 한다. 이 때 $i=0,1,2,\ldots,P_1-1$, $j=0,1,2,\ldots,P_2-1$, $n=0,1,2,\ldots,P_3-1$에 대하여 출력 수열 $b_{ijn}(t)$는

$$b_{ijn}(t) = \sum_{s=0}^{P_3-1} C_s(t)\, a_0(t+i-\phi^0_{s+n}(X^0_{t+j})),$$
$$t=0,1,2,\ldots \tag{4-6}$$

이다. 여기서 $C_s(t)=1$, $t-s=0 \bmod P_3$ (4-7)
$=0$, $t-s \neq 0 \bmod P_3$, $s=0,1,\ldots,P_3-1$이고, $[a_0(t)]$, $[X^0_i]$, $[\phi^0_i(j)]$, $j \in \underline{K}=\{0,1\}$는 각각의 $\mathrm{LFSR}_i(i=1,2,3)$에 대한 임의 설정 초기값이다.

한편, MEM-BSG는 선형 LFSR 출력을 그대로 memory에 저장하도록 설계되었기 때문에 선형 LFSR에 의하여 발생된 수열은 $2n$ 비트만 조합하면 해독이 가능하다는 점에서 안전성이 문제될 수 있다.

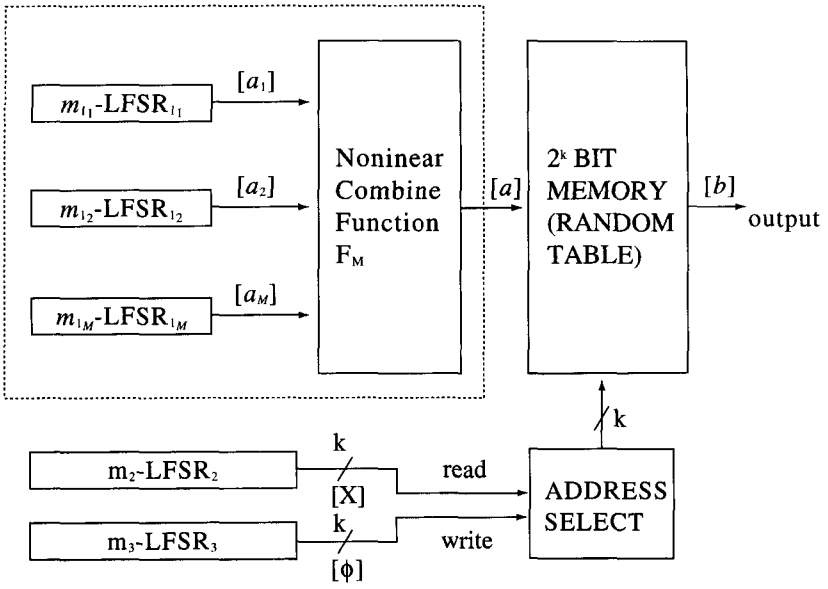


그림 4-2. 대용량 메모리형 다수열 출력 발생기(GMEM-BSG)

4.2 대용량 메모리형 다수열 출력 발생기 제안

Golic의 발생기에서 메모리를 대용량화할 경우에 대하여 살펴본다. 설계조건 C1에서 m_2, m_3는 k보다 커야하므로 메모리 크기(k)를 증가시킬 경우 m_2, m_3는 더욱 커져야 하며, 아울러 C2 조건을 만족하려면 m_3가 커질수록 기하급수적으로 m_1이 커져야 한다. 하지만 golic 발생기에서 m_1은 선형 LFSR의 단수이므로 이 값을 무한정 크게 늘릴 수 없다. 예를 들어 64-Mbit RAM(k=26)의 경우 m_2, m_3>26이고, m_1>2^{26}-1이어야 하지만, 현실적으로 2^{26}-1 보다 큰 단수의 LFSR을 구성한다는 것은 불가능하다. 그러므로 상기 문제를 현실화할 수 있는 개선된 일반화 모델이 요구된다.

대용량 추세에 맞추어 Golic 발생기의 메모리를 대용량화시켜 적용할 수 있도록 제안한 것이 그림 4-2의 일반화 모델(GMEM-BSG)이다. 그림에서 LFSR$_1$ 대신 점선처리된 블록과 같이 여러개의 LFSR을 비선형 결합함수로 조합함으로서 수열[a]의 선형복잡도를 크게 설계할 수 있으며, 이 때 메모리 크기 k의 증가에 따른 LC$_1$(본 제안에서는 m_1 대신 LC$_1$임)의 선택에 제약성이 사라질 수 있다. 그리고 GMEM-BSG 발생기는 대용량 메모리로부터 랜덤한 데이터값을 1-비트 읽은(read) 후 M개의 LFSR$_{1_i}$로부터 조합된 비선형 함수 $F_M(a_1,a_2,..,a_M)$의 출력 수열 [a]를 랜덤한 위치에 1-비트 쓰면서(write) 출력 수열 [b]를 반복적으로 발생한다.

(GMEM-BSG 발생기 설계 조건)

G1: $1 \le k < \min(m_2, m_3)$

G2: $2^{m_3}-1 < LC_1$

G3: m_{1_1}, m_{1_2},..., m_{1_N}, m_2, m_3는 각각 쌍으로 서로소이다(pairwise coprime).

G4: $3 \le k \le m_2-2$라면, LFSR$_2$의 k개 비트들은 등간격으로 출력되어야 한다.

[정리 4.3] (GMEM-BSG의 주기, 선형복잡도) 만일 GMEM-BSG가 설계조건 G1-G4를 모두 만족하고, 모든 LFSR의 초기치가 nonnull일 때 출력수열 $[b]$에 대한 주기 $P[b]$와 선형복잡도 $LC[b]$는 다음과 같다.

$$P_1P_2 \mid P[b] \mid P_1P_2P_3 \tag{4-8}$$

$$LC_1 \sum_{i=0}^{k} \binom{m_2}{i} \le LC[b] \le (2^{m_3}-1)LC_1 \sum_{i=0}^{k} \binom{m_2}{i} \tag{4-9}$$

여기서 P_1은 [a] 수열의 주기, P_2와 P_3는 $LFSR_2$와 $LFSR_3$의 주기를 말하며, LC_1은 [a] 수열의 선형복잡도(Linear Complexity)를 말한다.

(증명) $LFSR_{1_1}$ ~ $LFSR_{1_M}$의 비선형 조합인 F_M 함수의 출력 [a]를 등가적인 단일 $LFSR$로 나타낼 수 있고, 그 크기를 LC_1이라고 가정하였으므로 결국, 정리4.1에서 m_1 대신 LC_1으로 대체시킴으로서 GMEM-BSG에 대한 주기와 선형복잡도를 계산할 수 있다.

[정리 4.4] (GMEM-BSG의 출력 수열의 수) 만일 일반화 모델인 GMEM-BSG가 설계 조건 G1 ~ G3를 만족하고 또한

$$\gcd(LC_1, m_2) \neq LC_1 \tag{4-10}$$

$$\gcd\left(P_2, \frac{P_1}{\gcd(P_1, P_2)}\right) = 1 \tag{4-11}$$

$$\gcd(P_3, P_1P_2) = 1 \tag{4-12}$$

를 만족할 때 출력 수열의 수는 $P_1P_2P_3$가 된다. 단, $LFSR_i(i=1_1, 1_2, .. 1_M, 2, 3)$는 nonnull 초기상태이다.

(증명) 정리 4.2에서 m_1 대신 LC_1을 대체하면 GMEM-BSG 발생기의 출력 수열의 수를 얻을 수 있다.

제안 발생기는 선형 $LFSR_1$ 대신 $LFSR_{1_1}$ ~ $LFSR_{1_M}$의 비선형함수 도입으로 정리 4.2~4.3에서와 같이 기존 MEM-BSG 발생기에 비해서 주기, 선형복잡도 및 출력 수열의 수가 크게 개선되었음을 알 수 있다.

5. 결 론

본 논문에서는 Golic이 모델링한 출력 수열의 수를 스트림 암호의 비도요소로서 채택하여 많은 출력 수열을 갖는 경우 Dawson의 해독에 안전할 수 있음을 보였고, 또한 출력 수열의 수가 세션키 설정 수와 같도록 최대값으로 선택되고 세션키 설정수가 아주 큰 값이라면 이러한 수열 발생기는 개념적으로 one-time pad와 유사하게 작동할 수 있음을 보였다. 그리고 동일한 주기를 갖으면서 출력 수열의 수를 간편하게 늘릴 수 있는 기본 모델로 Switched-Tap LFSR(STLFSR)를 제안하였고, 이를 이용한 구체적인 방안으로 일반형 모델 및 Geffe발생기의 적용 예를 제안하였다. 또한 다수열 출력으로 이미 알려진 golic의 메모리 수열 발생기(MEM-BSG)를 개선하여 대용량 메모리 사용이 가능한 대용량 메모리형 다수열 출력 발생기(GMEM-BSG)를 제안하였고, 이 발생기에 대한 주기, 선형복잡도 및 출력 수열의 수를 분석하였다. 본 제안 발생기는 기존 MEM-BSG 발생기에 비해서 주기, 선형복잡도 및 출력 수열의 수가 크게 개선되었다.

참 고 문 헌

[1] Henry J. Beker and Fred C. Piper, Cipher systems: The Protection of Communications, Northwood Books, London, 1982.

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

[3] 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.

[4] J. Dj. Golic, "The Number of Output Sequences of a Binary Sequence Generator," LNCS 547, Advances in Cryptology-EUROCRYPT'91, pp.160-167, 1991.

[5] E. Dawson, L. Nielsen, "Automated Cryptanalysis of XOR Plaintext Strings," Cryptologia, Vol.XX, No.2, pp.165-181, Apr. 1996.

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

[7] M. D. Maclaren, G. Marsagilia, "Uniform Random Number Generators," JACM, Vol.17, No.1, pp.83-89, Jan. 1965.

[8] Charles T. Retter, "A Key-Search Attack on Maclaren-Marsaglia Systems," Cryptologia, Vol.9, No.2, pp.114-130, Apr. 1985.

[9] J. Dj. Golic, "On the Linear Complexity of Functions of Periodic GF(q) Sequences," IEEE Trans. on Infor. Theo., Vol. 35, No. 1, pp.69-75, Jan. 1989.

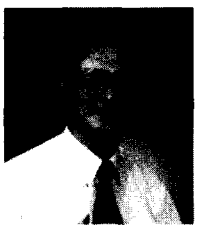
[10] J. Dj. Golic, "On a Binary Sequence Generator," EUROCRYPT'89 rump session, 1989.

□ 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