고속 병렬형 LM 이진 수열 발생기

이 훈 재†

요 약

LM 발생기는 합산 수열 발생기가 갖고 있는 최대 주기, 최대 근사 선형복잡도 및 최고 차수 상관면역도를 동시에 만족하는 발생기이며, 입출력 무상관 발생기이다. 본 논문에서는 LM 발생기를 고속화 구현하기 위하여 m-병렬 LM 수열 발생기(m-parallel LM-BSG, Lee-Moon Binary Sequence Generator)를 제안하였으며, $m=8$인 병렬 발생기(8-parallel LM-BSG)를 세부 설계한다. 기존의 스트림 암호와 비교할 때, 제안된 알고리듬은 같은 안전성을 유지하면서 속도가 $m=8$배 빨라짐을 알 수 있었다.

On a High-Speed Parallel-LM Binary Sequcence Generator

Hoon-jae Lee†

ABSTRACT

The LM generator is an improved summation generator with maximum period, near maximum linear complexity and maximum order of correlation immunity, and it has a property with the input-output correlation immunity. In this paper, we propose the high-speed m-parallel LM-BSG and 8-parallel LM-BSG for detail as a design example. When compared with a conventional stream cipher, the properties of the proposed cipher exhibited the same crypto-degree (security) with a m times faster processing.

키워드 : 이진 수열 발생기(Binary Sequcence), 스트림 암호, LM 발생기(LM Generator)

1. 서 론

통신의 발달과 함께 처리할 정보 데이터도 텍스트/음성 데이터에서 화상회의나 동영상 자료 등 점차 멀티미디어 자료 형태로 변모해가고 있으며, 이에 따라 암호 알고리듬도 고속화된 설계가 필요하다. 암호 방법은 크게 블록 암호, 스트림 암호(이상 대칭키 암호), 그리고 비대칭 키 암호로 분류될 수 있으며, 블록 암호의 적용 방법은 ECB(electronic codebook) 모드, CFB(cipher feedback) 모드, CBC(cipher block chaining) 모드 및 OFB(output feedback) 모드가 있다[1]. 이 중에서 OFB 모드는 블록 암호 자체를 랜덤 수열 발생기로 변경하여 스트림 암호처럼 적용시킨다. 한편, 1-비트 크기의 OFB 모드는 일반 ECB 모드보다도 데이터 처리 속도가 블록 크기 배 감소되기 때문에 오히려 통신망 처리 능력을 떨어뜨린다.

스트림 암호는 채널 에러 확산이 없고 안전성(비도 수준) 요소가 몇 가지 측면에서 수학적으로 보장이 되며 고속 처리가 가능한 장점이 있지만, 이 방법 역시 초고속 통신 서비스에 따른 암호 처리를 원활하게 할 수 있을지 의문이다. NESSIE 프로젝트에는 블록 암호, 스트림 암호, 메시지 인증코드(MAC), 충돌 회피(collision-free) 일방향 해쉬함수, 비대칭 암호, 비대칭 디지털 서명, 비대칭 신분확인 등 10개 분야에 대하여 각각의 표준을 결정하는 대규모 과제라고 볼 수 있다. 이 중 동기식 스트림 암호 분야에는 현재 호주의 Simpson과 Dawson이 제안한 LILI-128 암호[12]를 포함하여 LEVIATHAN[9], BGML[10], SNOW[11], SOBER-t16, SOBER-t32[14] 등 6개의 후보가 제안된 바 있으며, 이들 알고리즘들은 고속화를 위하여 워드기반(word-based) 또는 병렬 형태로 설계 개념을 채택하고 있다. 일본의 차세대 암호 과제인 CRYPTREC에는 MUGI[7] 등의 스트림 암호 알고리듬이 제안되어 있다.

본 연구에서는 암호 시스템의 초고속화와 통신 채널을 통할 때 에러 확산이 없는 통신 암호시스템의 설계라는 두 가지 목적을 설정하여 스트림 암호와 블록 암호의 장점을 혼합시킨 병렬형 스트림 암호[3]를 설계 제안한다. 즉, 스트림 암호의 비도 수준과 에러 확산 방지 기능을 유지하면서 블록 암호의 m-비트 병렬 처리 기능을 혼합시켜 고속화시킬 새로운 암호 처리 형태이다. 스트림 암호에서 LFSR은 한 클럭에 1-비트씩 이동되며 이를 개선하기 위하여 한 클럭만에 m-비트 이동이 가능한 고속 병렬형 PS-LFSR이

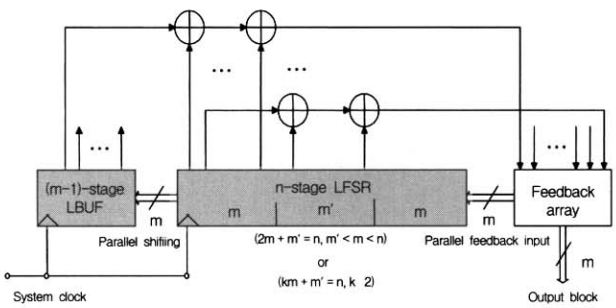
※ 이 논문은 2001년도 한국학술진흥재단(KRF-2001-003-E00198) 및 ITRC의 지원에 의하여 연구 되었음.
† 정 회 원 : 동서대학교 인터넷공학부 교수
논문접수 : 2003년 6월 14일, 심사완료 : 2003년 9월 1일

제안되었다[3]. 그리고 1-비트씩 처리되는 비선형 결합 함수의 단점을 보완하여 블록 암호처럼 동시에 여러 비트 출력이 될 수 있도록 m-비트 병렬 비선형 결합 함수의 일반형이 제안된 바 있다[3]. 본 연구에서는 m-병렬 LM 수열 발생기(m-parallel LM-BSG, Lee-Moon Binary Sequence Generator)를 제안하여 $m=8$인 병렬 발생기(8-parallel LM-BSG)를 세부 설계한다. 마지막으로 제안 발생기에 대하여 스트림 암호의 비도 요소와 처리 속도를 동일한 조건으로 적용시켜 그 특성을 분석한다.

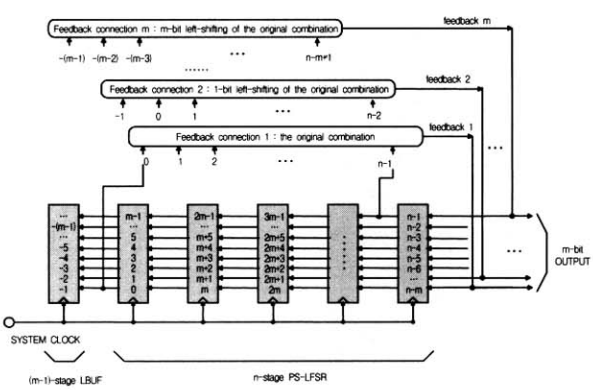
2. 병렬형 스트림 암호 설계

2.1 PS-LFSR

일반적으로 LFSR(Linear Feedback Shift Register)은 최대 주기성을 갖으며 소프트웨어나 하드웨어로 구현이 용이하기 때문에 스트림 암호의 키수열 발생기(keystream generator)나 확산 스펙트럼 통신의 의사 잡음 발생기(pseudo-noise generator) 등에 많이 사용된다. LFSR의 구현 방법은 보통 외부 시스템 클럭에 맞추어서 레지스터 값을 이동시키며, 출력 수열은 1 클럭당 1 비트 출력을 발생한다. 그러나 하드웨어 구현시에 귀환 이동할 값을 사전 계산하여 버퍼에 저장할 경우 LFSR의 출력 효율을 크게 증가시킬 수 있다.



(a) Serial 구조형



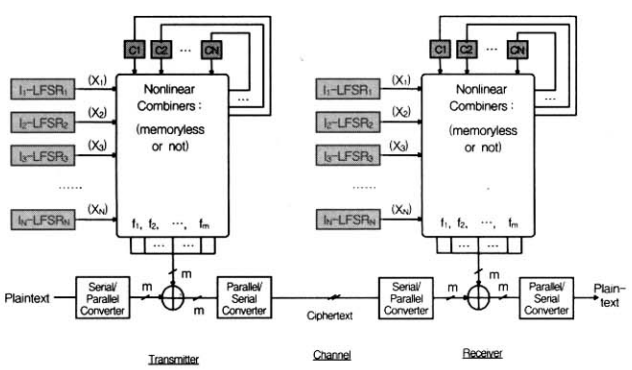
(b) Parallel 구조형

(그림 1) PS-LFSR

고속 스트림 암호 구현을 위한 기본 요소로서 (그림 1)과 같이 고속 병렬형 parallel-shifting LFSR(PS-LFSR)이 제안되었다[3]. 그림에서 PS-LFSR은 병렬형 스트림 암호 구현을 위한 핵심 요소이며, 'LFSR을 어떻게 구성하면 시스템 1-클럭 만에 m-비트를 이동시킬 것인가'하는 문제를 해결하는 기본 개념이다. (그림 1)(a)는 기존 LFSR과 유사하게 serial 형태로 PS-LFSR 구조를 나타내었고, 개념적으로 m-비트 단위로 이동한다. (그림 1)(a)에서 가운데 위치한 n-단 LFSR은 원래의 LFSR과 동일한 것이고, m-단 LBUF(left buffer)는 다음 클럭에서 입출력 값을 저장할 버퍼의 역할을, feedback array는 m-병렬 귀환 함수들의 배열을 의미한다. 모든 비트가 m-비트 단위로 병렬 이동(parallel shifting)하기 위하여 병렬 경로가 구성되어야 하며, 귀환 탭에서도 m-묶음의 XOR 조합 연산을 거쳐 feedback array에 모인 후 LFSR의 m-비트 블록 부분으로 좌측 이동되고, 계속해서 왼쪽으로 블록 크기(m) 단위 만큼 병렬 이동 된다. (그림 1)(b)는 상기 (그림 1)(a) 구조를 실제 구현에 적합한 parallel 구조로 표현한 것이다.

결국 이 발생기는 한 클럭에 m-비트 이동 후 m-비트(또는 그 이하) 출력을 동시 생성하는 발생기로서 긴 주기에서의 출력 수열은 단 한번만 사용되므로 랜덤 특성, 주기 등 비도 특성이 일반 LFSR과 동일함을 알 수 있다. 또한 비트 단위의 출력을 발생하는 일반 LFSR과 비교할 때 PS-LFSR은 암호화 처리 속도가 m배 빨라지며, 고속화에 따른 하드웨어 복잡도는 다소 증가될 수 있지만 이는 최근 집적회로 기술 발전으로 큰 문제가 되지 않을 것이다.

2.2 고속 병렬 스트림 암호 설계

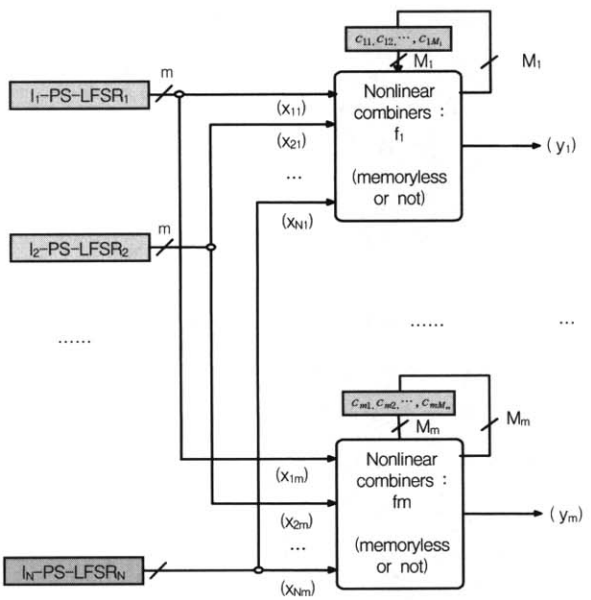


(그림 2) 고속 병렬형 스트림 암호

일반 스트림 암호의 키 수열 발생기와 달리 병렬형 스트림 암호[3]는 (그림 2)와 같이 N개의 LFSR을 이용하지만 $m(\leq N)$개의 비선형 결합 함수 $(f_1, f_2, \cdots, f_m)$를 독립적으로 설계하여 별개의 수열을 발생시키며, 이 수열로 m-비트 블록 단위의 병렬 처리가 가능하도록 한다. 이 경우 기존의 스트림 암호보다 구현 복잡도는 증가되지만 속도가

m배 이상 빨라질 수 있다. 또한 스트림 암호와 마찬가지로 에러 확산이 없기 때문에 에러 전송 부호와 같은 별도의 부가 장치 없이 전송 선로의 품질을 현행 수준으로 유지시킬 수 있게 된다. 필요시 비선형 결합 함수에 메모리 비트를 활용하여 상관 면역성[3-6]을 높이고, 상관성 공격(correlation attack)을 방어토록 할 수 있다.

(그림 3)에서는 m-비트 병렬 비선형 결합 함수 ($f_1, f_2, \cdots, f_m$)의 일반화된 모델을 나타내었다. 비선형 결합 함수의 형태는 다양하지만 비선형 요소인 M_i-비트 메모리 ($c_{i1}, c_{i2}, \cdots, c_{iM_i}$)를 사용하여 일반화시킬 수 있으며, 각 LFSR은 모두 PS-LFSR 형태로 구성하여 한 클럭만에 m-비트를 출력하고 비선형 결합 함수에 공평한 입력을 제공한다. 또한 LFSR의 단수를 각각 다르게 설정하고, 일반 키 수열 발생기의 설계 조건에 부합하는 설계를 한다.



Note : $N \geq m$, $1 \leq M_1, M_2, \cdots, M_N \leq m$

(그림 3) m-병렬 비선형 결합함수 일반형 모델

본 일반형 발생기에 사용될 m-비트 병렬 비선형 결합 함수 (키 수열 발생기)는 일반 비선형 결합 함수[2]와 유사하며, 다음과 같이 구성된다.

$$f_1(x_{11}, x_{21}, \cdots, x_{N1}, c_{11}, c_{12}, \cdots, c_{1M_1})$$
$$= a_{1,0} + \left(\sum_{i=1}^{N} a_{1,i}\, x_{i1} + \sum_{i=N+1}^{N+m} a_{1,i}'\, c_{1i}\right)$$
$$+ \left(\sum_{i,j} a_{1,ij}\, x_{i1} x_{j1} + \sum_{i,j} a_{1,ij}'\, c_{1i}\, c_{1j} + \sum_{i,j} a_{1,ij}''\, x_{i1}\, c_{1j}\right)$$
$$+ \cdots + a_{1,ij\cdots N} + m\; x_{i1} x_{j1} \cdots x_{t1}\, c_{11}\, c_{12} \cdots c_{1M_1}$$

$$f_2(x_{12}, x_{22}, \cdots, x_{N2}, c_{21}, c_{22}, \cdots, c_{2M_2})$$
$$= a_{2,0} + \left(\sum_{i=1}^{N} a_{2,i}\, x_{i2} + \sum_{i=N+1}^{N+m} a_{2,i}'\, c_{2i}\right)$$
$$+ \left(\sum_{i,j} a_{2,ij}\, x_{i2} x_{j2} + \sum_{i,j} a_{2,ij}'\, c_{2i}\, c_{2j} + \sum_{i,j} a_{2,ij}''\, x_{i2}\, c_{2j}\right)$$
$$+ \cdots + a_{2,ij\cdots N} + m\; x_{i2} x_{j2} \cdots x_{t2}\, c_{21}\, c_{22} \cdots c_{2M_2}$$

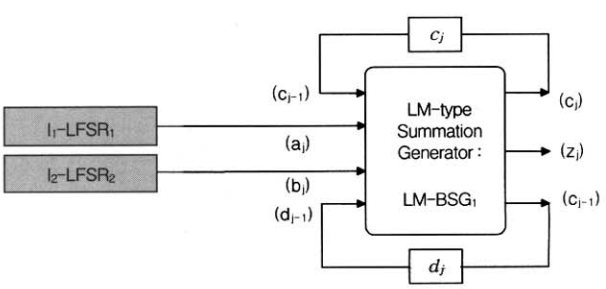
$$\cdots$$

$$f_m(x_{1m}, x_{2m}, \cdots, x_{Nm}, c_{m1}, c_{m2}, \cdots, c_{mM_m})$$
$$= a_{m,0} + \left(\sum_{i=1}^{N} a_{m,i}\, x_{im} + \sum_{i=N+1}^{N+m} a_{m,i}'\, c_{mi}\right)$$
$$+ \left(\sum_{i,j} a_{m,ij}\, x_{im} x_{jm} + \sum_{i,j} a_{m,ij}'\, c_{mi}\, c_{mj} + \sum_{i,j} a_{m,ij}''\, x_{im}\, c_{mj}\right)$$
$$+ \cdots + a_{m,ij\cdots N} + m\; x_{im} x_{jm} \cdots x_{tm}\, c_{m1} c_{m2} \cdots c_{mM_m}$$

여기서 x_{ij}는 LFSR$_i$의 병렬 m비트 중 j번째 출력 수열 ($1 \leq i \leq N, 1 \leq j \leq m$)을, c_{ij} ($1 \leq i, j \leq m$)는 i번째 함수의 j 메모리 수열을 나타내며, $a_{k,i}$, $a_{k,i}'$, $a_{k,ij}$, $a_{k,ij}'$, $a_{k,ij}''$, $\cdots$, $a_{k,ij\cdots N+m} \in [0,1]$, $0 \leq M_1, M_2, \cdots, M_m \leq m$이 된다.

또한, 병렬 비선형 결합 함수 $f_i(x_{1i}, x_{2i}, \cdots, x_{Ni}, c_{i1}, c_{i2}, \cdots, c_{iM_i})$ 함수는 각각 다음과 같이 일반 비선형 결합 함수의 특성을 만족하여야 한다[1-2].

① 입력 수열의 통계적 성질을 출력 키 수열에 그대로 전달 할 수 있어야 한다.
② 입력 수열의 주기를 조합하여 키 수열의 주기를 최대화 시켜야 한다.
③ 입력 수열의 선형 복잡도를 조합하여 키 수열의 선형 복잡도를 극대화 시켜야 한다.
④ 입력 수열과 출력 키 수열간에 고차 상관 면역도를 가져야 한다.
⑤ 구현하기 쉬워야하고 속도가 빨라야 한다.
⑥ 비밀 키에 의하여 쉽게 제어될 수 있어야 한다.



(그림 4) LM-BSG(LM Binary Sequence Generator)

(그림 4)의 LM 이진 수열 발생기[5] (LM-BSG)는 Rueppel의 합산 수열 발생기[4]를 개선한 발생기이며, 다음과 같은 출력 함수를 갖는다.

$$y_j = a_j \oplus b_j \oplus c_{j-1}$$
$$c_j = a_j b_j \oplus (a_j \oplus b_j)\, c_{j-1} \quad j = 0, 1, 2, \cdots$$
$$z_j = y_{y-1} \oplus d_{j-1}$$
$$d_j = b_j \oplus (a_j \oplus b_j)\, d_{j-1} \quad j = 0, 1, 2, \cdots$$

여기서 y_j는 j-순간의 합산 수열 발생기 출력, (a_j)는 LFSR$_1$ 의 출력 수열, (b_j)는 LFSR$_2$ 의 출력 수열, (c_j)는 carry 수열, $c_{-1}=0$(carry 초기값), (d_j)는 memory 수열, $d_{-1}=0$ (메모리 초기값), $j=0,1,2,\cdots$이다.

본 논문에서는 병렬 비선형 결합 함수이고, 상기의 비선형 결합함수 특성을 잘 만족하는 LM 이진 수열 발생기에 대한 $m=8$비트 고속 병렬화 방법을 제안한다. (그림 5)는 $m=8$개의 LFSR 수열과 $2m=16$ 비트의 캐리-메모리 수열을 각각 입력하는 LM-BSG를 병렬로 연결시킨 m-비트 병렬형 스트림 암호 발생기 제안 블록다이어그램이다. 제안된 발생기에서 고속화를 위한 각 입력 수열, 출력 수열의 관계를 나타내면 다음과 같다. 고속 구현을 위하여 캐리 비트와 메모리 비트는 각각의 출력 수열 발생기에서 미리 계산(pre-computation)한 후에 계산 결과를 적용시킨다. 그렇지 않으면 캐리 및 메모리 계산 결과가 지연되어 전체 속도를 떨어뜨린다.

첫 번째 병렬 발생기의 출력 수열 :

$$\begin{aligned} z_j &= (a_j \oplus b_j \oplus c_{j-1}) \oplus d_{j-1} \\ &= f_1(a_j; b_j; c_{j-1}; d_{j-1}) \\ c_j &= a_j b_j \oplus (a_j \oplus b_j) c_{j-1} \quad j=0,1,2,\cdots \\ &= g_1(a_j; b_j; c_{j-1}) \\ d_j &= b_j \oplus (a_j \oplus b_j) d_{j-1} \quad j=0,1,2,\cdots \\ &= h_1(a_j; b_j; d_{j-1}) \end{aligned}$$

두 번째 병렬 발생기의 출력 수열 :

$$\begin{aligned} z_{j+1} &= a_{j+1} \oplus b_{j+1} \oplus c_j \oplus d_j \\ &= a_{j+1} \oplus b_{j+1} \oplus \{a_j b_j \oplus (a_j \oplus b_j) c_{j-1}\} \\ &\quad \oplus \{b_j \oplus (a_j \oplus b_j) d_{j-1}\} \\ &= f_2(a_j, a_{j+1}; b_j, b_{j+1}; c_{j-1}; d_{j-1}) \\ c_{j+1} &= a_{j+1} b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) c_j \\ &= a_{j+1} b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \{a_j b_j \oplus (a_j \oplus b_j) c_{j-1}\} \\ &= g_2(a_j, a_{j+1}; b_j, b_{j+1}; c_{j-1}) \\ d_{j+1} &= b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) d_j \\ &= b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \{b_j \oplus (a_j \oplus b_j) d_{j-1}\} \\ &= h_2(a_j, a_{j+1}; b_j, b_{j+1}; d_{j-1}) \end{aligned}$$

세 번째 병렬 발생기의 출력 수열 :

$$\begin{aligned} z_{j+2} &= a_{j+2} \oplus b_{j+2} \oplus c_{j+1} \oplus d_{j+1} \\ &= a_{j+2} \oplus b_{j+2} \oplus [a_{j+1} b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \{a_j b_j \oplus (a_j \\ &\quad \oplus b_j) c_{j-1}\}] \oplus [b_{j+1} \oplus (a_{j+1}) \{b_j \oplus (a_j \oplus b_j) d_{j-1}\}] \\ &= f_3(a_j, a_{j+1}, a_{j+2}; b_j, b_{j+1}, b_{j+2}; c_{j-1}; d_{j-1}) \\ c_{j+2} &= a_{j+2} b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) c_{j+1} \\ &= a_{j+2} b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) [a_{j+1} b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \\ &\quad \{a_j b_j \oplus (a_j \oplus b_j) c_{j-1}\}] \\ &= g_3(a_j, a_{j+1}, a_{j+2}; b_j, b_{j+1}, b_{j+2} c_{j-1}) \\ d_{j+2} &= b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) d_{j+1} \\ &= b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) [a_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \\ &\quad \{b_j \oplus (a_j \oplus b_j) d_{j-1}\}] \\ &= h_3(a_j, a_{j+1}, a_{j+2}; b_j, b_{j+1}, b_{j+2} d_{j-1}) \end{aligned}$$

네 번째 병렬 발생기의 출력 수열 :

$$\begin{aligned} z_{j+3} &= a_{j+3} \oplus b_{j+3} \oplus c_{j+2} \oplus d_{j+2} \\ &= a_{j+3} \oplus b_{j+3} \oplus [a_{j+2} b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) [a_{j+1} b_{j+1} \\ &\quad \oplus (a_{j+1} \oplus b_{j+1}) \{a_j b_j \oplus (a_j \oplus b_j) c_{j-1}\}]] \\ &\quad \oplus [b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) [b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \\ &\quad \{b_j \oplus (a_j \oplus b_j) d_{j-1}\}]] \\ &= f_4(a_j, a_{j+1}, a_{j+2}, a_{j+3}; b_j, b_{j+1}, b_{j+2}, b_{j+3}; c_{j-1}; d_{j-1}) \\ c_{j+3} &= a_{j+3} b_{j+3} \oplus (a_{j+3} \oplus b_{j+3}) c_{j+2} \\ &= a_{j+3} b_{j+3} \oplus (a_{j+3} \oplus b_{j+3}) [a_{j+2} b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) \\ &\quad [a_{j+1} b_{j+1} \oplus b_{j+1}) \{a_j b_j \oplus (a_j \oplus b_j) c_{j-1}\}]] \\ &= g_4(a_j, a_{j+1}, a_{j+2}, a_{j+3}; b_j, b_{j+1}, b_{j+2}, b_{j+3}; c_{j-1}) \\ d_{j+3} &= b_{j+3} \oplus (a_{j+3} \oplus b_{j+3}) d_{j+2} \\ &= b_{j+3} \oplus (a_{j+3} \oplus b_{j+3}) [b_{j+2} \oplus (a_{j+2} \oplus b_{j+2}) \\ &\quad [b_{j+1} \oplus (a_{j+1} \oplus b_{j+1}) \{b_j \oplus (a_j \oplus b_j) d_{j-1}\}]] \\ &= h_4(a_j, a_{j+1}, a_{j+2}, a_{j+2}; b_j, b_{j+1}, b_{j+2}, b_{j+2}; d_{j-1}) \\ &\cdots \end{aligned}$$

m 번째 병렬 발생기의 출력 수열 :

$$\begin{aligned} z_{j+m-1} &= a_{j+m-1} \oplus b_{j+m-1} \oplus c_{j+m-1} \oplus d_{j+m-1} \\ &= f_m(a_j, a_{j+1}, \cdots, a_{j+m-1}; b_j, b_{j+1}, \cdots, b_{j+m-1}; c_{j-1}; d_{j-1}) \\ c_{j+m-1} &= a_{j+m-1} b_{j+m-1} \oplus (a_{j+m-1} \oplus b_{j+m-1}) c_{j+m-2} \\ &= g_m(a_j, a_{j+1}, \cdots, a_{j+m-1}; b_j, b_{j+1}, \cdots, b_{j+m-1}; c_{j-1}) \\ d_{j+m-1} &= b_{j+m-1} \oplus (a_{j+m-1} \oplus b_{j+m-1}) d_{j+m-2} \\ &= h_m(a_j, a_{j+1}, \cdots, a_{j+m-1}; b_j, b_{j+1}, \cdots, b_{j+m-1}; d_{j-1}) \end{aligned}$$

[특성 1] 만일 $\gcd(l_i, l_j)=1, (1 \le i, j \le m, i \ne j)$인 상호 소수(relatively prime)이고, 사용된 모든 LFSR의 초기치가 non-null일 때, m-병렬 LM-BSG 발생기의 비도 특성은 다음과 같다[4]. 단, l_i는 i번째 LFSR의 레지스터 길이이다.

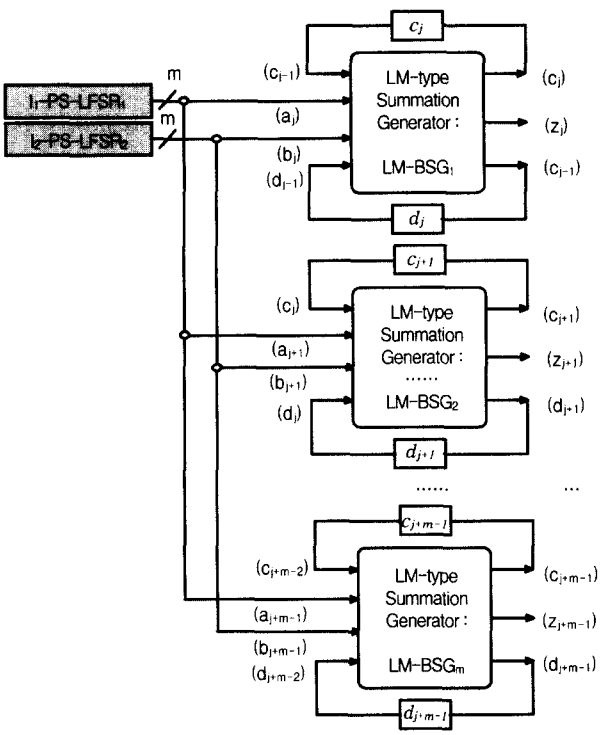
① 주기 : $P = \prod_{j=1}^{m} (2^{l_j}-1)$

② 난수 특성 : 양호

③ 선형 복잡도 : $LC \le P$

④ 상관 면역도 : $K = 2-1 = 1$.

m-병렬 LM-BSG는 기존의 LM-BSG와 동일한 출력을 발생시키며, 따라서 그 특성은 LM-BSG와 동일하다. 그러므로, m-병렬 LM-BSG는 특성 1과 같이 최대 주기, 좋은 랜덤 특성, 주기와 비슷한 크기의 선형복잡도, 그리고 최대 차수 상관 면역도를 갖는 것으로 알려져 있다.



(그림 5) m-병렬 LM-BSG(예, $m=8$)

병렬형 키 수열 발생기 세부 설계 예로 (그림 5)에서 $m=8$인 LM-BSG를 제시하였으며, 본 발생기의 LFSR 구성을 위한 원시 다항식(primitive polynomial)은 [6]에 따라 발생하였다.

$$a(x) = x^{127}+x^{31}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4} +x^{3}+x^{2}+x+1$$

$$b(x) = x^{129}+x^{110}+x^{12}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4} +x^{3}+x^{2}+x+1$$

[특성 2] 만일 $\gcd(l_1, l_2) = 1$ 이고, 사용된 모든 LFSR의 초기치가 non-null일 때 m-parallel LM-BSG ($m=8$) 수열 발생기에 대한 비도 특성 및 전체 시스템 특성은 다음과 같다.

① 주기 : $P = (2^{127}-1)(2^{129}-1) \approx 2^{256} \approx 10^{77}$

② 난수 특성 : 양호(<표 1> 참조)

③ 선형 복잡도 : $LC \approx P$

④ 상관 면역도 : $K = 2-1 = 1$

⑤ 외부 시스템 클럭을 동일하게 입력시 하드웨어로 구현된 발생기의 데이터 처리 속도는 $m=8$배이다.

⑥ 하드웨어로 구현시 전체 필요한 gate 수는 대략 1.575배 정도 증가된다(<표 2> 참조).

〈표 1〉 m-parallel LM-BSG의 랜덤 특성 검증 결과

Test items	Threshold	Test results		
		Sample 1	Sample 2	Sample 3
1) Frequency test	3.84	1.201	0.065	0.822
2) Serial test	5.99	3.290	1.782	2.551
3) Generalized				
t-serial t = 3	9.48	4.128	2.370	6.431
t = 4	15.50	4.561	3.213	7.237
t = 5	26.29	11.759	8.129	11.682
4) Poker test				
m = 3	14.067	11.326	9.435	7.426
m = 4	24.996	17.741	11.667	16.348
m = 5	44.654	27.010	19.500	33.657
5) Autocorrelation test	Max. ≤ 0.05	Max = 0.0065	Max = 0.0051	Max = 0.0049

<표 2>와 같이 m-parallel LM-BSG 병렬형 발생기는 최대 주기를 보장할 뿐 아니라 선형 복잡도가 최대 주기에 근사하며, 상관 면역도 역시 최대 값이 보장되므로 상관성 공격을 견딜 수 있는 결합 함수가 된다. 또한 3가지 샘플 데이타의 통계적인 랜덤 특성[2]이 기준치 이하로 나타남에 따라 랜덤 특성이 양호함을 알 수 있다.

결국 제안된 발생기는 하드웨어의 복잡도가 조금 증가되지만 게이트 집적도가 큰 문제가 되지 않는 현실을 감안할 때 하드웨어 부담을 크게 늘리지 않고도 데이터 처리 속도를 m배 향상시킬 수 있는 발생기로써 다가오는 고속 화시대에 적합한 데이터 암호화 방법이라고 할 수 있다.

〈표 2〉 유사 발생기의 비교 ($m=8$)

Items	LM-BSG	8-parallel LM-BSG
Period	10^{77}	10^{77}
Randomness	random	random
Linear complexity	approximately period	approximately period
Correlation immunity	1	1
Number of F/Fs	258	286
Number of XOR & AND gates	34	655
Total number of gates (if 1 F/F = 5 gates)	1324	2085 (1.575 times)
Processing rate ratio	1	8

3. 결 론

본 논문에서는 기존의 스트림 암호 방식에서 초고속 처리와 통신 채널을 활용한 통신 암호시스템의 구현에 따른

문제점 분석을 통하여 비도 수준을 현 상태로 유지하면서 구현 방법을 개선하여 고속 처리 실현이 가능한 병렬형 스트림 암호를 세부 설계 제안하였다. 병렬형 스트림 암호의 설계 예로 m = 8비트 입력을 갖는 8-병렬 LM-BSG를 세부 설계를 제시하였으며, 일반 스트림 암호의 비도 요소와 동일한 조건으로 비교 분석하였다.

분석 결과 8-병렬 LM-BSG는 각각 $l_1 = 127$, $l_2 = 129$단 LFSR로 구성되어 주기 $P \approx 2^{256}$이고, 3가지 국부 랜덤성에 의한 랜덤성이 양호하였으며, 선형 복잡도 $LC \approx 2^{256}$, 상관 면역도 차수 = 1로 분석되었다. 결과적으로 m-비트 생성을 위한 발생기는 각각 원래의 설계 기준을 만족하기 때문에 기존의 비도 수준을 유지할 수 있었다. 한편, 병렬 배치로 인한 하드웨어 복잡도는 1.575배 만큼 다소 증가되었지만, 이에 따른 처리 속도는 m = 8배 개선될 수 있었다. 결국 제안된 발생기는 하드웨어의 복잡도가 증가되지만 게이트 집적도가 큰 문제가 되지 않는 현실을 감안할 때 하드웨어 부담을 크게 늘리지 않고도 데이터 처리 속도를 m배 향상시킬 수 있는 발생기로써 다가오는 고속화시대에 적합하다고 할 수 있다.

참 고 문 헌

[1] B. Schneier, *Applied Cryptography, 2nd Ed.*, Jhon Wiley & Sons, Inc., 1996.

[2] A. Menezes, et al. *Handbook of Applied Cryptography(2nd edition)*, CRC press, 1997.

[3] Hoonjae Lee, Sangjae Moon, "Parallel Stream Cipher for Secure High-Speed Communications," Signal Processing, Vol.82, No.2, pp.259-265, Feb., 2002.

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

[5] Hoonjae Lee, Sangjae Moon, "On An Improved Summation Generator with 2-Bit Memory," *Signal Processing*, Vol.80, No.1, pp.211-217, Jan., 2000.

[6] B. Park, H. Choi, T. Chang and K. Kang, "Period of Sequences of Primitive Polynomials," *Electronics Letters*, Vol.29, No.4, pp.390-391, Feb., 1993.

[7] D. Watanabe, S. Furuya, H. Yoshida and B. Preneel, "*A new keystream generator MUGI*," Proceedings of Fast Software Encryption 2002, FSE '02, LNCS, Springer-Verlag, 2002.

[8] G. Rose, "*A stream cipher based on linear feedback over GF(2^8)*," Proceedings of ACISP '98, LNCS, Vol.1438, Springer-Verlag, 1998.

[9] D. A. McGrew and S. R. Fluhrer, "*The Stream Ciher LEVI ATHAN*," Submitted to the NESSIE process, 2001.

[10] J. Hastad and M. Naslund, "*BMGL : Synchronous Key-stream generator with provable Security*," submitted to the NESSIE process, 2000.

[11] P. Ekdahl and T. Johansson, "*SNOW - a new stream cipher*," Submited to the NESSIE process, 2000.

[12] E. Dawson, A. Clark, J. Golic, W. Millan, L. Penna, L. Simpson, "The LILI-128 Keystream Generator," 1st NESSIE Workshop, Nov., 2000.

[13] A. Clark, E. Dawson, J. Fuller, J. Golic, Hoon-Jae Lee, W. Millan, Sang-Jae Moon, L. Simpson, "The LILI-II Keystream Generator," LNCS 2384, ACISP'2002, pp.25-39, Jul., 2002.

[14] NESSIE site in https://www.cosic.esat.kuleuven.ac.be/nessie/.

이 훈 재

e-mail : hjlee@dongseo.ac.kr

1985년 경북대학교 전자공학과(학사)

1987년 경북대학교 전자공학과(석사)

1998년 경북대학교 전자공학과(박사)

1987년~1998년 국방과학연구소 선임연구원

1998년~2002년 경운대학교 컴퓨터전자정보공학부 조교수

2002년~현재 동서대학교 인터넷공학부 정보네트워크공학전공 조교수

관심분야 : 정보보안, 네트워크보안, 정보통신네트워크