논문 01-26-5B-4 한국통신학회논문지 '01-5 Vol.26 No.5B

고속 안전 통신을 위한 병렬형 스트림 암호

정회원 이 훈 재*, 문 상 재**

On a Parallel Stream Cipher for Secure High-Speed Communications

Hoon-jae Lee*, Sang-jae Moon** *Regular Members*

요 약

통신망의 급격한 발전과 통신 속도의 향상에 따라 암호 알고리듬의 고속화 필요성이 절실하다. 본 논문에서는 LFSR을 고속화하기 위하여 한 클럭에 m번의 이동이 이루어지는 고속 병렬형 PS-LFSR을 제안하였고, 이를 기본으로 다수의 키 수열 발생기를 병렬 연결하여 속도를 개선시킨 병렬형 스트림 암호를 제안하였다. 그리고 병렬형 스트림 암호 예로서 m-병렬 합산 수열 발생기(m-parallel SUM-BSG)를 제안하여 m=8인 병렬 발생기를 세부 설계 예시하였으며, 제안된 발생기는 기존의 비도 수준을 유지하면서 처리 속도를 m배 높일 수 있음을 확인하였다.

ABSTRACT

Due to ongoing improvements in high-speed communication, it is necessary to increase the speed of data encryption. In this paper, we have proposed the PS-LFSR with $m(\geq 2)$ times faster shifting for a clock and the parallel stream cipher, which have speeded up by paralleling many similar keystream generators using PS-LFSR. Finally, we have proposed m-parallel SUM-BSG and 8-parallel in detail as an example of the parallel stream cipher, and we have determined its properties by having the same crypto-degree and m times high-speed processing as compared with the original stream cipher.

I. 서 론

최근 통신망의 급격한 발전과 더불어 처리할 데이터도 텍스트/음성 데이터에서 화상회의나 동영상 자료 등 점차 멀티미디어 자료 형태로 변모해가고 있으며, 이에 따라 암호 알고리듬도 고비도, 고속화 및 고 신뢰도 설계가 요구된다.

암호 방법은 스트림 암호, 블록 암호 그리고 공개키 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]. ECB 모드는 블록 크기의 입력에 대하여 비밀키와 DES 함수로부터 블록 출력을 생성하는 일반적인 적용 방법이고, CFB 모드는 출력 암호문을 입력에 귀환시킴으로써 통신 동기를 자체 확립하는 적용 방법이다. CBC 모드는 송수신 데이터 인증을 위하여 현재 암호문 블록과 다음 번 평문 블록을 XOR (exclusive-or)시킨 후 블록 암호에 입력시켜 새로운 출력을 생성하고, 이 출력을 다시 그 다음 번 입력과 XOR시키는 반복 과정으로 최종 인증 값을 얻는 방법이다. 데이터 위조 시 최종 인증 값이 바뀌게 되므로 진위 구별이 가능하다. OFB 모드는 블록 암호 자체를 랜덤 수열 발생기로 변경하여 스트림 암호 처럼 적용시킨다. 그러나 상기 4가지 모두 암호통신을 하는 실용화 측면에서 채널 에러(암호문에서)에 대부분 취약하거나 또 다른 문제점을 안고 있기 때문에 어떤 대책이 필요하다. 우선 ECB 모드는 채널 에러 시 그 여파가 블록 크기만큼 확산(error propagation) 되므로 암호 통신으로 인한 통신 선로의 품질 저하를 유발시킨다. 예를 들면, 128-비트 블록 암호를 10^{-6} 비트 에러율 (BER, bit

* 경운대학교 컴퓨터전자정보공학부 (hjlee@kyungwoon.ac.kr), ** 경북대학교 전자전기공학부 (sjmoon@knu.ac.kr)
논문번호 : 00124-0414, 접수일자 : 2000년 4월 14일

error rate)을 갖는 채널에 적용하여 암호통신을 할 경우 채널 에러 특성이 128배 떨어지고 10^{-4} ($\approx 128 \times 10^{-6}$) 채널로 기능이 저하된다. CFB 모드에서는 한 비트의 채널 에러가 블록 크기의 두 배로 확산되며, CBC 모드에서는 에러 발생 이후 모든 블록이 에러이다. 블록 암호의 에러 확산을 줄이기 위하여 도입된 OFB 모드는 입력 귀환 비트 수 (블록 크기 보다 작음) 만큼 확산을 줄일 수 있으며, 최상의 경우 1-비트를 귀환시켜 근본적으로 확산을 방지할 수 있다. 하지만 1-비트 크기의 OFB 모드는 일반 ECB 모드보다도 데이터 처리 속도가 블록 크기 배 감소되기 때문에 오히려 통신망 처리 능력을 떨어뜨린다.

한편, 공개 키 암호는 처리 속도가 느리기 때문에 고속 데이터 처리에 부적합할 뿐 아니라 ECB 모드처럼 에러가 블록 전체로 확산되는 단점이 있다. 그리고 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 있을 지 의문이다.

본 논문에서는 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 암호를 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-LFSR을 제안한다. 그리고 1-비트씩 처리되는 비선형 결합함수의 단점을 보완하여 블록 암호처럼 동시에 여러 비트 출력이 될 수 있도록 m-비트 병렬 비선형 결합함수의 일반형을 제안한다. 이러한 설계 예로서 m-병렬 합산 수열 발생기 (m-parallel SUM-BSG)를 제안하여 $m=8$인 병렬 발생기 (8-parallel SUM_{11}-BSG)를 세부 설계 예시한다. 마지막으로 제안 발생기에 대하여 스트림 암호의 비도 요소와 처리 속도를 동일한 조건으로 적용시켜 그 특성을 분석한다.

Ⅱ. 병렬형 스트림 암호

1. Parallel-Shifting LFSR 제안

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

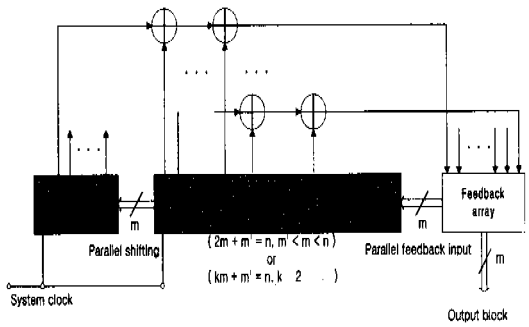


그림 1. LFSR과 PS-LFSR

고속 스트림 암호 구현을 위한 기본 요소로서 그림 1과 같이 고속 병렬형 parallel-shifting LFSR (PS-LFSR)을 제안한다. 고속 병렬형 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 b)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. 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 비

교할 때 PS-LFSR은 암호화 처리 속도가 m배 빨라지며, 고속화에 따른 하드웨어 복잡도는 다소 증가될 수 있지만 최근의 집적회로 기술 발전으로 큰 문제가 되지 않을 것이다.

2. 병렬형 스트림 암호

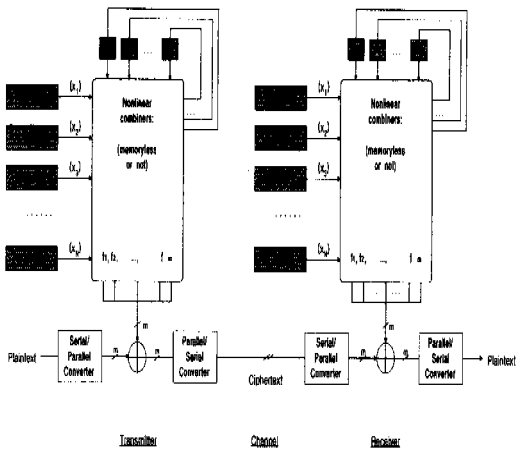


그림 2. 병렬형 스트림 암호

일반 스트림 암호의 키 수열 발생기와 달리 병렬형 스트림 암호는 그림 2와 같이 N개의 LFSR (linear feedback shift register)을 이용하지만 $m(\le N)$개의 비선형 결합 함수 $(f_1, f_2, \ldots, f_m)$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 높여 상관성 공격(correlation attack)을 방어토록 할 수도 있다.

그림 3에서는 m-비트 병렬 비선형 결합 함수 $(f_1, f_2, \ldots, f_m)$의 일반화된 모델을 나타내었다. 비선형 결합 함수의 형태는 다양하지만 비선형 요소인 M_i-비트 메모리 $(c_{i1}, c_{i2}, \ldots, c_{iM_i})$를 사용하여 일반화시킬 수 있으며, 각 LFSR은 모두 PS-LFSR 형태 (그림 1)로 구성하여 한 클럭만에 m-비트를 출력하고 비선형 결합 함수에 공평한 입력을 제공한다. 또한 LFSR의 단수를 각 각 다르게 설정하고, 일반 키 수열 발생기의 설계 조건에 부합하는 설계를 한다.

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

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

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

$$\cdots$$

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

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

또한, 병렬 비선형 결합 함수 $f_i(x_{1i}, x_{2i}, \ldots, x_{Ni}, c_{i1}, c_{i2}, \ldots, c_{iM_i})$ 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 키이에 의하여 쉽게 제어될 수 있어야 한다.

병렬 비선형 결합 함수이고, 상기의 특성을 잘 만족하는 함수의 예로 Rueppel의 합산 수열 발생기 (SUM-BSG: Rueppel's summation binary sequence generator)[2],[7]를 들 수 있다. 그림 4는 m개의 LFSR 수열과 M 비트의 캐리 메모리 수열을 각각 입력하는 SUM-BSG를 병렬로 연결시킨 m-비트 병렬형 스트림 암호 발생기를 제안한 것이다. 제안된 발생기에서 i번째 SUM-BSG의 k번째 입력 수열 (x_{ik}), j번째 캐리 수열 (c_{ij}) 및 출력 수열 (y_i)의 관계는 다음과 같다.

$$(y_i) = \{(x_{1i}) \oplus \cdots \oplus (x_{mi})\} \oplus \{(c_{i1}) \oplus \cdots \oplus (c_{iM})\}$$

여기서 $i = 1, 2, \cdots, m$, y_i 는 i번째 SUM_{12}-BSG의 출력 수열, x_{1i}는 $LFSR_1$ 의 i번째 출력 수열, x_{2i}는 $LFSR_2$ 의 i번째 출력 수열, $x_{m,i}$는 $LFSR_m$ 의 i번째 출력 수열이며, c_{ij}는 i번째 발생기에서 사용된 j번째 carry (memory) 수열이다.

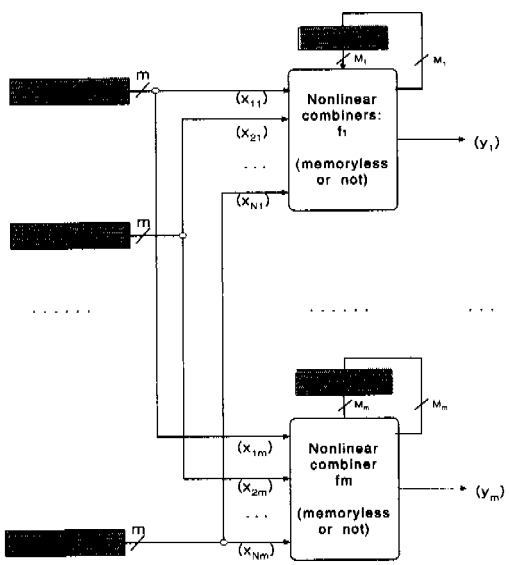


그림 3. m-병렬 비선형 결합함수 일반형 모델

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, 개별 SUM_{11}-BSG_i 발생기의 비도 특성은 다음과 같다 [2]-[3].

1) 주기 : $P_i = \prod_{j=1}^{m}(2^{l_j}-1)$
2) 난수 특성 : 양호
3) 선형 복잡도 : $LC_i \le P_i$
4) 상관 면역도 : $K_i = m-1$.

SUM_{11}-BSG는 특성 1과 같이 최대 주기, 좋은 랜덤 특성, 주기와 비슷한 크기의 선형복잡도, 그리고 최대 차수 상관 면역도를 갖는 것으로 알려져 있다.

병렬형 키 수열 발생기 세부 설계 예로 그림 4에서 $m = 8$, $M = 3$인 11-입력 Rueppel의 합산 수열 발생기 (SUM_{11}-BSG)를 제시하였으며, 표 1과 같이 입력 11-비트들 (x_{1i} x_{2i} x_{3i} x_{4i} x_{5i} x_{6i} x_{7i} x_{8i} c_{i3} c_{i2} c_{i1})을 실수 합산한 후 이진수로 변환하여 출력시키는 원리이다. 출력 4-비트 (c_{i3} c_{i2} c_{i1} y_i) 중에서 최하위 비트를 키 수열 출력으로 사용하며, 그 중에서 캐리 출력 3-비트 (c_{i3} c_{i2} c_{i1}) 는 결합 함수의 비선형성을 증가시키고, "0"-"1" 균일 분포를 유지하기 위하여 입력에 귀환시킨다.

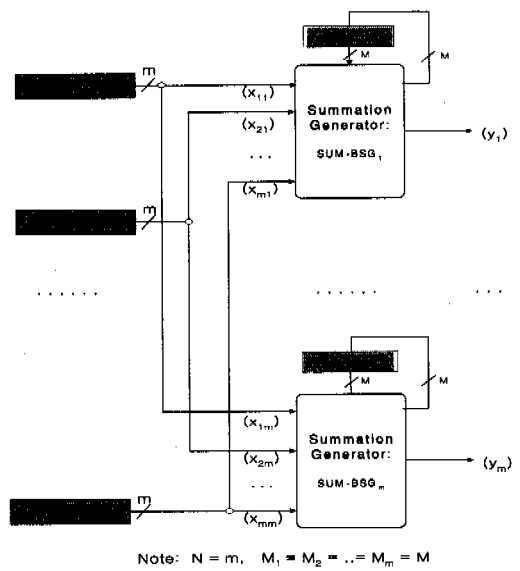


그림 4. m-병렬 SUM_{11}-BSG

본 발생기의 LFSR 구성을 위한 원시 다항식은 참고 문헌[8]에 따라 다음과 같이 발생하였다.

$$g_1(x) = x^{19} + x^9 + x^6 + x^3 + x^2 + x + 1$$
$$g_2(x) = x^{23} + x^{12} + x^6 + x^3 + x^2 + x + 1$$
$$g_3(x) = x^{29} + x^{11} + x^7 + x^3 + x^2 + x + 1$$

$$g_4(x)=x^{31}+x^3+1$$
$$g_5(x)=x^{37}+x^{18}+x^2+x+1$$
$$g_6(x)=x^{41}+x^7+x^4+x^3+x^2+x+1$$
$$g_7(x)=x^{43}+x^{16}+x^4+x^3+x^2+x+1$$
$$g_8(x)=x^{47}+x^{14}+x^4+x^3+x^2+x+1$$

특성 2. 만일 $\gcd(l_i, l_j)=1, (1\le i, j\le m,\ i\ne j)$ 인 상호 소수이고, 사용된 모든 LFSR의 초기치가 non-null일 때 m-parallel SUM_{11}- BSG ($m=8$) 수열 발생기에 대한 i번째 개별 발생기의 비도 특성 및 전체 시스템 특성은 다음과 같다.

1) 주기 :

$$P_i = (2^{19}-1)(2^{23}-1)(2^{29}-1)(2^{31}-1)(2^{37}-1)(2^{41}-1)(2^{43}-1)(2^{47}-1)$$
$$\approx 2^{270}\approx 10^{81},$$
$$(i=1,2,\cdots,m)$$

2) 난수 특성 : 양호 (표 2 참조)

3) 선형 복잡도 :

$LC_i \le P_i,\ (i=1,2,\ldots,m)$

4) 상관 면역도 :

$K_i = m-1 = 7,\ (i=1,2,\ldots,m).$

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

6) 하드웨어로 구현시 전체 필요한 gate 수는 대략 1.67배 정도 증가된다.(표 3 참조)

표 1. i번째 SUM11-BSG의 입·출력 상태

Inputs x_{11} x_{2i} x_{3i} x_{4i} x_{5i} x_{6i} x_{7i} x_{8i} c_{13} c_{12} c_{11}	Sum (Decimal)	Outputs c_{13} c_{12} c_{11} y_j
0 0 0 0 0 0 0 0 0 0 0	0	0 0 0 0
0 0 0 0 0 0 0 0 0 0 1	1	0 0 0 1
0 0 0 0 0 0 0 0 0 1 0	1	0 0 0 1
0 0 0 0 0 0 0 0 0 1 1	2	0 0 1 0
0 0 0 0 0 0 0 0 1 0 0	1	0 0 0 1
0 0 0 0 0 0 0 0 1 0 1	2	0 0 1 0
0 0 0 0 0 0 0 0 1 1 0	2	0 0 1 0
0 0 0 0 0 0 0 0 1 1 1	3	0 0 1 1
0 0 0 0 0 0 0 1 0 0 0	1	0 0 0 1
...	...	...
1 0 1 0 1 1 0 1 0 1 1	7	0 1 1 1
...	...	...
1 1 1 1 1 1 1 1 0 0 1	9	1 0 0 1
1 1 1 1 1 1 1 1 0 1 0	9	1 0 0 1
1 1 1 1 1 1 1 1 0 1 1	10	1 0 1 0
1 1 1 1 1 1 1 1 1 0 0	9	1 0 0 1
1 1 1 1 1 1 1 1 1 0 1	10	1 0 1 0
1 1 1 1 1 1 1 1 1 1 0	10	1 0 1 0
1 1 1 1 1 1 1 1 1 1 1	11	1 0 1 1

표 2. m-parallel SUM11-BSG의 랜덤 특성 검증 결과

Test items	Thres-hold	Test results Sample 1	Sample 2	Sample 3
1) Frequency test	3.84	0.048	0.231	0.032
2) Serial test	5.99	0.332	2.267	0.456
3) Generalized t-serial t=3	9.48	2.757	1.550	3.335
t=4	15.50	3.413	7.212	6.328
t=5	26.29	12.216	15.421	10.219
4) Poker test m = 3	14.067	16.223	6.328	4.238
m = 4	24.996	14.991	14.118	17.284
m = 5	44.654	22.860	22.853	32.451
5) Autocorrelation test	Max. ≤0.05	Max= 0.0056	Max= 0.0048	Max= 0.0084

표 3. 유사 발생기의 비교

Items	SUM_{11}-BSG	8-parallel SUM_{11}-BSG
Period	10^{81}	10^{81}
Randomness	random	random
Linear complexity	approximately period	approximately period
Correlation immunity	7	7
Processing rate ratio	1	8
Number of F/Fs	270	398
Number of XOR gates	42	336
Total number of gates (if 1 F/F = 5 gates)	1392	2326 (1.67 times)

기존 형태의 SUM_{11}-BSG 수열 발생기를 m개 병렬로 연결할 경우 비선형 결합 함수 상호간의 상관 면역이 보장 ($K=7$) 되기 때문에 개개의 SUM_{11}-BSG_i 특성은 기존의 SUM_{11}-BSG 비도 특성을 갖는다고 볼 수 있다. 표 3과 같이 병렬형 발생기는 최대 주기를 보장할 뿐 아니라 선형 복잡도가 최대 주기에 근사하며, 상관 면역도 역시 최대값이 보장되므로 상관성 공격을 견딜 수 있는 결합 함수가 된다. 또한 3가지 샘플 데이타의 통계적인 랜덤 특성[9]-[10]이 기준치 이하로 나타남에 따라 랜덤 특성이 양호함을 알 수 있다.

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

Ⅲ. 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 제안하였다. 우선 고속처리를 위하여 LFSR을 고속화시킨 PS-LFSR을 제안하였으며, 이 발생기에서는 m-비트 동시 출력에도 불구하고 각각의 출력이 이중으로 사용되지 않는 특징을 갖는다. 또한 PS-LFSR을 사용하여 구성되는 병렬형 스트림 암호 (m-병렬 키 수열 발생기 일반형)는 기존의 스트림 암호에서 1-비트씩 처리되는 단점을 보완하여 동시에 여러 비트가 처리될 수 있도록 블록 암호 개념을 혼합시켰다.

마지막으로 병렬형 스트림 암호의 설계 예로 11 비트 입력을 갖는 m-parallel SUM_{11}-BSG와 m=8인 세부설계를 제시하였으며, 일반 스트림 암호의 비도 요소와 동일한 조건으로 비교 분석하였다. 분석 결과 m-비트 생성을 위한 발생기는 각각 원래의 설계 기준을 만족하기 때문에 기존의 비도 수준을 유지할 수 있었으며, 병렬 배치로 인한 하드웨어 복잡도는 다소 증가되지만 처리 속도는 m배 개선되었다. 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] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

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

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

[5] 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.

[6] 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.

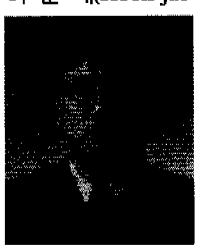
[7] Hoonjae Lee, Sangjae Moon, "On An Improved Summation Generator with 2-Bit Memory," *Signal Processing*, Vol. 80, No.1. pp. 211-217, Jan. 2000.

[8] 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.

[9] H. J. Beker and F. C. Piper, *Cipher systems: The Protection of Communications*, Northwood Books, London, 1982.

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

이 훈 재(Hoon-jae Lee) 정회원

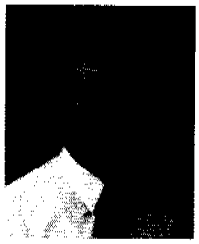


1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)

1987년 2월~1998년 1월 : 국방과학연구소 선임연구원
1998년 2월~현재 : 경운대학교 컴퓨터전자정보공학부 조교수

<주관심 분야> 암호이론, 네트워크보안, 디지털 통신

문 상 재(Sang-jae Moon) 정회원



1972년 2월 : 서울대학교 공업교육과 졸업 (전자공학 학사)
1974년 2월 : 서울대학교 대학원 전자공학과 졸업 (전자공학 석사)
1984년 6월 : 미국 UCLA 통신공학과 졸업(통신공학 박사)
1984년 7월~1985년 6월 : UCLA Postdoctor 근무
1974년 12월~현재 : 경북대학교 공과대학 전자전기공학부 교수
2001년 2월~현재 : 한국정보보호학회 회장
<주관심 분야> 정보보호, 이동 네트워크