병렬 스트림암호를 위한 m-병렬 비선형 결합함수에 관한 연구

정회원 이 훈 재*, 문 상 재**

A study on the m-Parallel Nonlinear Combine Functions for the Parallel Stream Cipher

HoonJae Lee*, SangJae Moon** *Regular Members*

요 약

본 논문에서는 병렬 이동형 PS-LFSR을 활용한 여러 가지 형태의 m-병렬 비선형 결합함수에 대하여 제안하고, 이들의 효율적인 구현 방안을 검토하였다. 즉, m-병렬 비메모리-비선형 결합함수, m-병렬 메모리-비선형 결합함수, m-병렬 비선형 필터함수 및 m-병렬 클럭 조절형 결합함수 등 4가지 형태의 m-병렬 비선형 결합함수와 이들의 효율적인 병렬 구현 방안을 제안하였고, 마지막으로 클럭 조절형 LILI-128의 병렬구현 기법을 예시하여 안전성과 성능을 분석하였다.

ABSTRACT

In this paper, we propose the effective implementation of various nonlinear combiners using by PS-LFSR: m-parallel memoryless-nonlinear combiner, m-parallel memory-nonlinear combiner, m-parallel nonlinear filter function, and m-parallel clock-controlled function. Finally, we propose m-parallel LILI-128 stream cipher as an example of the parallel implementation, and we determine its cryptographic security and performance.

Ⅰ. 서 론

최근 암호학계의 큰 흐름으로 미국의 AES [1]와 유럽 주도의 NESSIE (New European Schemes for Signature, Integrity and Encryption) [2]를 들 수 있다. AES는 DES를 개선하는 미국의 대형 프로젝트로서 Rijndael [3]이 이미 표준으로 확정되었으며, NESSIE 프로젝트는 2002년 12월을 목표로 블록 암호, 스트림 암호, message authentication codes (MAC), collision-resistant and one-way hash functions, 비대칭 암호, 비대칭 디지털 서명, 비대칭 신분확인 등 10개 분야에 대하여 각각의 표준을 결정하는 유럽 차세대 암호개발 과제이다. NESSIE 과제의 동기식 스트림 암호 분야에는 현재 호주의 Simpson과 Dawson이 제안한 LILI-128 암호 [4]를 포함하여 SOBER-t16, SOBER-t32 [5]등 6개의 후보가 제안된 상태이며, 이들은 모두 고속 스트림암호에 초점을 맞추고 있다.

본 논문에서는 스트림 암호의 고속화 설계 방안인 병렬 이동형 PS-LFSR [6]의 구조를 살펴본 다음 이를 활용하여 여러 가지 m-병렬 비선형 결합

* 동서대학교 인터넷공학부(hjlee@dongseo.ac.kr), ** 경북대학교 전자전기컴퓨터학부 (sjmoon@knu.ac.kr)
논문번호 : 010191-0720, 접수일자 : 2001년 7월 20일

함수의 효율적인 구현 방안을 형태별로 제안한다. 비선형 결합함수는 구성 형태에 따라 크게 비메모리형과 메모리형, 비선형 조합형과 비선형 필터형, 그리고 동기형과 클럭 조절형 등으로 나눌 수 있다. 즉, 메모리 비트의 사용 여부에 따라 비메모리형 (memoryless-type)과 메모리형 (memory- type), 출력함수의 구성방식에 따라 여러 개의 LFSR 출력을 비선형적으로 조합하는 비선형 조합형 (nonlinear conbiner)과 하나의 LFSR로부터 비선형 필터출력을 발생시키는 비선형 필터형 (nonlinear filter function), 그리고 클럭조절 유무에 따라 클럭 동기형 (clock-synchronized type)과 클럭조절형 (clock-controlled type) 으로 대별될 수 있다. 본 논문에서는 이들 분류방법을 조합하고, m-병렬 형태로 구성하여 m-병렬 비메모리-비선형 결합함수, m-병렬 메모리-비선형 결합함수, m-병렬 비선형 필터함수, 그리고 m-병렬 클럭 조절형 결합함수 등 4가지 경우를 조합한다. 그리고 이들 각각에 대하여 효율적인 구현 방안을 분석코자 한다. 마지막으로 메모리형태인 합산 수열 발생기 [7-10]에 대한 m-병렬 합산 수열 발생기 (m-parallel SUM-BSG)와 클럭 조절 형태인 m-병렬 LILI-128 스트림 암호 구현에 관하여 설계 예시 및 분석한다.

Ⅱ. LFSR의 병렬 구성

그림 1 b)의 병렬 이동형 PS-LFSR (Parallel-Structured/Shifting LFSR) [6]은 병렬형 스트림 암호 구현을 위한 핵심 요소로서 시스템 1-클럭만에 m-비트 ($1 \le m \le n$)를 이동시키는 LFSR의 새로운 구조이다. 그림 b)에서 하단 오른쪽 n-단 LFSR은 클럭에 동기되어 병렬 형태로 m-비트씩 이동될 수 있는 병렬 구조이고, 하단 왼쪽 (m-1) 단 LBUF (left buffer)는 m-비트 병렬 귀환 탭 구성을 위한 임시 버퍼이다. 귀환 연결 (feedback connection) 1~ m 은 귀환 비트탭 들을 모아서 병렬 이동시켜주는 m-묶음의 XOR 조합 연산을 한다.

그림 2는 $n=40$ 단, $m=8$ 병렬인 (40, 8) PS-LFSR 구성 예이다. PS-LFSR은 기존 LFSR과 비교할 때 병렬 형태로 입출력이 가능하도록 구조적으로만 변경되었을 뿐 출력 수열에는 변화가 없기 때문에 암호학적 안전성이 기존 LFSR과 동일하다. 상기 구조는 소프트웨어 구현 시 8의 배수 (8-비트, 16-비트, 32-비트 등)로 처리되는 마이크로 프로세서 연산에 유리하며, 하드웨어 구현 시에는 m 배 고속화를 위한 기본 요소가 된다.

그림 2의 예제에서 사용된 40단 원시다항식 $p(x)$ 및 8개의 m-병렬 귀환 함수는 다음과 같이 정의된다.

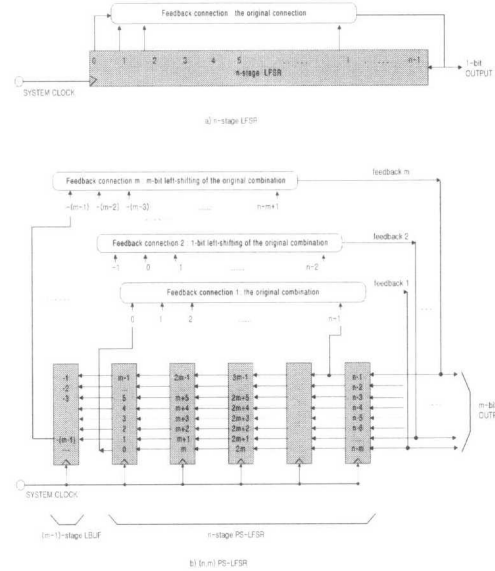

그림 1. n-단 LFSR과 병렬 이동형 (n, m) PS-LFSR

$$p(x) = x^{40} + x^{35} + x^2 + x + 1$$
: primitive polynomial

$$s(40+t) = s(35+t) \oplus s(2+t) \oplus s(1+t) \oplus s(t)$$
: feedback connection 1

$$s(39+t) = s(34+t) \oplus s(1+t) \oplus s(t) \oplus s(-1+t)$$
: feedback connection 2

$$s(38+t) = s(33+t) \oplus s(t) \oplus s(-1+t) \oplus s(-2+t)$$
: feedback connection 3

$$s(37+t) = s(32+t) \oplus s(-1+t) \oplus s(-2+t) \oplus s(-3+t)$$
: feedback connection 4

$$s(36+t) = s(31+t) \oplus s(-2+t) \oplus s(-3+t) \oplus s(-4+t)$$
: feedback connection 5

$$s(35+t) = s(30+t) \oplus s(-3+t) \oplus s(-4+t) \oplus s(-5+t)$$
: feedback connection 6

$$s(34+t) = s(29+t) \oplus s(-4+t) \oplus s(-5+t) \oplus s(-6+t)$$
: feedback connection 7

$$s(33+t) = s(28+t) \oplus s(-5+t) \oplus s(-6+t) \oplus s(-7+t)$$
: feedback connection 8

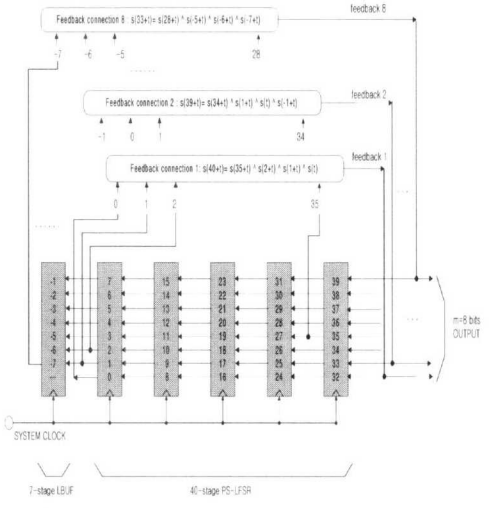

그림 2. (n=40, m=8) PS-LFSR의 구성 예

여기에서 임의의 t 순간에 정의된 40단-LFSR 레지스터 수열은 왼쪽부터 $s(t), s(1+t), s(2+t), \ldots, s(38+t)$로 표시하였고, 좌측 LBUF에 저장된 수열은 $s(-7+t), s(-6+t), \ldots, s(-1+t)$로 정의된다. 그리고 $\oplus$ 표시는 비트 단위의 XOR (bit-wide exclusive-or) 연산을 의미한다.

결국 이 발생기는 한 클럭에 m-비트 이동 후 m-비트 출력을 동시 생성하는 발생기로서 긴 주기에서의 출력 수열은 단 한번만 사용되므로 랜덤 특성, 주기 등 비도 특성이 일반 LFSR과 동일하다. 또한 비트 단위의 출력을 발생하는 LFSR과 비교할 때 PS-LFSR은 암호화 처리 속도가 m 배 빠르며, 고속화에 따른 하드웨어 복잡도는 다소 ($\leq m$) 증가될 수 있지만 이는 최근 집적회로 기술 발전으로 큰 문제가 되지 않는다.

Ⅲ. m-병렬 비선형 결합함수 유형별 제안

N개의 LFSR (linear feedback shift register)을 이용하긴 하지만 일반 스트림 암호의 키 수열 발생기와 달리 병렬형 스트림 암호 [6]는 $m(\leq N)$개의 비선형 결합 함수 $(f_1, f_2, \ldots, f_m)$를 독립적으로 설계하여 별개의 수열을 발생시키는데, 이 수열로 m-비트 블록 단위의 병렬 처리가 가능하다. 이 경우 기존의 스트림 암호보다 구현 복잡도는 증가되지만 속도가 m 배 이상 빨라질 수 있다. 또한 스트림 암호와 마찬가지로 에러 확산이 없는 특징을 살려서 무선 이동 통신 회선 등에 적용이 유리한 장점을 갖는다. 필요시 비선형 결합 함수에 메모리 비트를 활용하여 상관 면역성 [11-13]을 높일 수 있고, 이에 따라 상관성 공격(correlation attack)을 방어토록 설계할 수도 있다.

본 논문에서는 이들을 다시 조합하여 m-병렬 비메모리-비선형 결합함수, m-병렬 메모리-비선형 결합함수, m-병렬 비선형 필터함수, 그리고 m-병렬 클럭 조절 함수 등 4가지 경우로 병렬형 키수열 발생기 설계 방안을 도출하고, 각각의 효율적인 구현 방안을 분석한다. 특히, 제안된 모델들은 기존의 일반형 비선형 결합함수의 일반 모델 원형을 수용하면서 단지 하드웨어적으로 또는 소프트웨어적인 구현 측면에서 고속화 기능을 부가하였기 때문에 안전성 수준은 기존의 모델들[7,8]에 대한 안전성을 따른다.

1. m-병렬 비메모리-비선형 결합함수 제안

그림 3은 m-병렬 비메모리-비선형 결합 함수의 일반화된 모델을 나타내었다. 비메모리-비선형 결합

함수는 메모리를 사용하지 않으며, 각 LFSR은 모두 PS-LFSR 형태로 구성되어 m-병렬 수열을 출력하고 비선형 결합 함수에 공평한 입력을 제공한다. 또한 LFSR의 단수를 각각 다르게 설정하고, 일반 키 수열 발생기의 설계 조건에 부합하는 설계를 한다.

일반형 발생기에 사용될 m-병렬 비메모리-비선형 결합 함수 (키 수열 발생기)는 다음과 같이 ANF (algebraic normal form) 형태로 나타낸다.

$$y_i = f(x_{1i}, x_{2i}, \cdots, x_{N,i}) = a_{i,0} + (\sum_{j=1}^{N} a_{i,j}\, x_{ji}) + (\sum_{j,k} a_{i,jk} x_{ji} x_{ki}) + \ldots + a_{i,12..N}\, x_{1i} x_{2i} .. x_{N,i}$$

여기서 $i = 1, 2, \ldots, m$이고, x_{jk}는 LFSRj의 병렬 m비트 발생 수열 중에서 k번째 출력 수열 $(1 \le j \le N,\ 1 \le k \le m)$을 나타내며, $a_{i,0}$, $a_{i,j}$, $a_{i,jk}$, $\cdots, a_{i,12..N} \in [0,1]$ 이 된다.

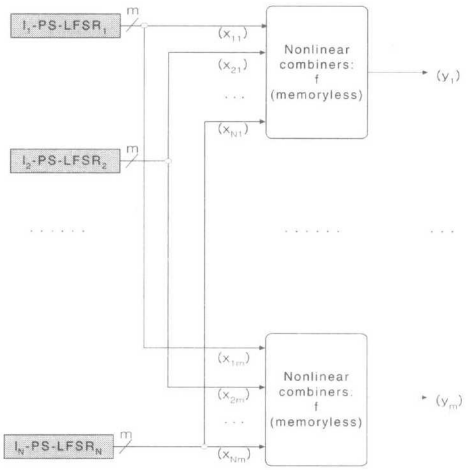

그림 3. m-병렬 비메모리-비선형 결합함수 일반형 모델 제안

2. m-병렬 메모리-비선형 결합함수 제안

그림 4는 m-병렬 메모리-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 형태로 구성되어 m-병렬로 출력하고 비선형 결합 함수에 공평한 입력을 제공한다. 또한 LFSR의 단수를 각각 다르게 설정하고, 일반 키 수열 발생기의 설계 조건에 부합하는 설계를 한다.

일반형 발생기에 사용될 m-병렬 메모리-비선형 결합 함수 (키 수열 발생기)는 다음과 같이 ANF 형태로 나타낸다.

$$f_i\ (x_{1i}, x_{2i}, \cdots, x_{N,i}, c_{i1}, c_{i2}, \cdots, c_{i,M_i}) = a_{i,0} + (\sum_{j=1}^{N} a_{i,j}\, x_{ji} + \sum_{j=N+1}^{N+m} a_{i,j}'\, c_{ij}) + (\sum_{j,k} a_{i,jk} x_{ji} x_{ki} + \sum_{j,k} a_{i,jk}'\, c_{ij} c_{ik} + \sum_{j,k} a_{i,jk}''\, x_{ji} c_{ik}) + \ldots + a_{i,12..N+M_i}\, x_{1i} x_{2i} .. x_{N,i} c_{i1} c_{i2} \cdots c_{i,M_i}$$

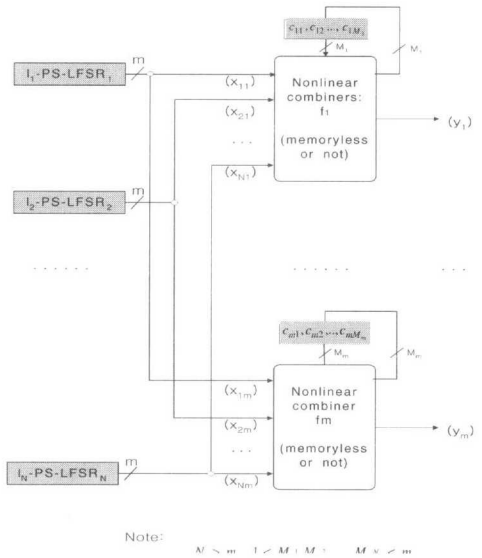

그림 4. m-병렬 메모리-비선형 결합함수 일반형 모델 제안

여기서 $i = 1, 2, \ldots m$ 이고, x_{jk}는 LFSRj의 병렬 m비트 중 k번째 출력 수열 $(1 \le j \le N,\ 1 \le k \le m)$ 을, $c_{jk}\,(1 \le j, k \le m)$는 j번째 함수의 k 메모리 수열을 나타내며, $a_{i,j}, a_{i,j}', a_{i,jk}, a_{i,jk}', a_{i,jk}'', \cdots, a_{i,12..N+M_i} \in [0,1]$, $0 \le M_1, M_2, \cdots, M_m \le m$이 된다.

또한, 병렬 메모리-비선형 결합 함수 $f_i(x_{1i}, x_{2i}, \ldots, x_{Ni}, c_{i1}, c_{i2}, \ldots, c_{iM_i})$ 는 각

각 다음과 같이 일반 비선형 결합 함수의 특성을 만족하여야 한다 [7,8].

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) 비밀키에 의하여 쉽게 제어 가능하여야 한다.

7) 출력 수열간에 고차 상관 면역도를 가져야 한다.

3. m-병렬 비선형 필터함수 제안

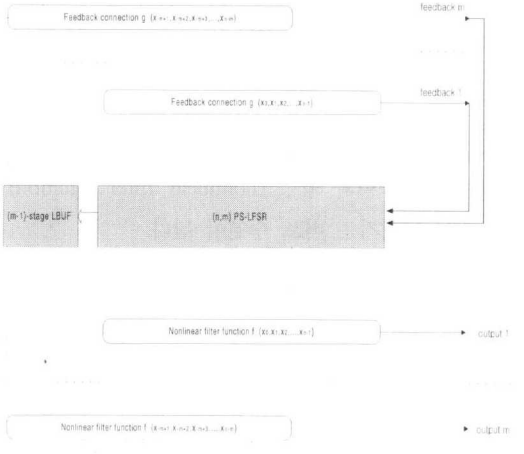

그림 5. m-병렬 비선형 필터 함수 일반형 모델 제안

m-병렬 비선형 필터함수는 기존의 비선형 필터함수의 출력 수열을 그대로 유지하면서 그 출력을 m-비트씩 발생시키기 위하여 그림 5와 같이 출력단에서 동일한 비선형 필터함수를 여러개 병렬화시켰다. 비선형 필터함수는 비메모리형의 함수를 갖고 있으며, 그 출력을 병렬화시키기 위하여 동일한 함수로서 입력 값만 서로 다르게 설정하였다.

기존의 일반형에서의 귀환 함수를 $g(x_0, x_1, \ldots, x_{n-1})$, 출력 필터함수를 $f(x_0, x_1, \ldots, x_{n-1})$라 할 때, m-병렬 귀환함수 및 m-병렬 필터함수는 기존함수를 이용하여 다음과 같이 정의된다.

$g(x_0, x_1, \ldots, x_{n-1})$: feedback connection function 1,

$g(x_{-1}, x_0, \ldots, x_{n-2})$: feedback connection function 2,

.....

$g(x_{-m+1}, x_{-m+2}, \ldots, x_{n-m})$: feedback connection function m.

그리고,

$f(x_0, x_1, \ldots, x_{n-1})$: nonlinear filter function 1,

$f(x_{-1}, x_0, \ldots, x_{n-2})$: nonlinear filter function 2,

.....

$f(x_{-m+1}, x_{-m+2}, \ldots, x_{n-m})$: nonlinear filter function m.

상기 m-병렬 귀환함수 및 m-병렬 필터함수는 기본함수를 각각 0, 1, 2, ... , $m-1$ 비트씩 이동시킨 함수로 구성되었음을 알 수 있다.

4. m-병렬 클럭 조절형 함수 예시

클럭 조절형 스트림 암호는 어떤 발생기 출력으로 제2 발생기의 클럭을 랜덤 조절하는 것으로서 그림 6의 LILI-128 암호 [4]를 예로 들 수 있다. 이러한 형태의 발생기는 여러 클럭을 구동하여 하나의 출력을 발생하기 때문에 구조적으로 속도가 저하되는 문제점을 안고 있다. 본 논문에서 예로든

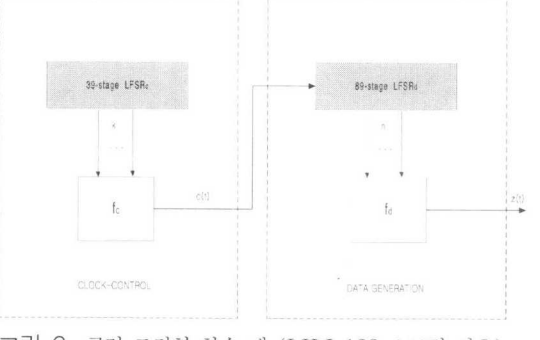

그림 6. 클럭 조절형 함수 예 (LILI-128 스트림 암호)

LILI-128 암호는 아래와 같은 방법으로 병렬화시킴으로서 속도저하 문제를 해결할 수 있다.

그림 7은 LILI-128이 갖는 구조적인 문제를 해결하기 위하여 클럭 조절회로에서 결정해주는 랜덤 비트 수 (1~4 비트)만큼 점프하면서 그 이전 비트를 각각 받아들이도록 구성시킨 "4-비트 병렬 입력 LFSRd (4-bit parallel LFSRd)" 고속 구현 방안이다 [15]. 그림 상반부에 위치한 LFSRc는 일반적인 39단 이동 레지스터 및 귀환 비트 조합으로 구현이 가능하다. 그리고 출력 f_c 회로는 LFSRd의 좌측 이동 클럭 수를 결정하는 것으로서 전가산기 (full adder)를 사용하면 쉽게 구현된다. 그러나 89단 LFSRd 각 비트들은 $d_0, d_1, \ldots, d_{88}$로 나타낸 레지스터에 저장된 다음 f_c값에 따라 1~4-비트씩 이전 값 (우측 레지스터)으로부터 4-1 멀티플렉서 (4-1 MUX) 회로를 통하여 입력된다. 예를 들면, 그림에서 d_{84} 레지스터의 경우 그 이전 4개의 레지스터들 $d_{85}, d_{86}, d_{87}, d_{88}$ 중에서 랜덤하게 어느 한 입력이 선택 ($f_c=1$일 때는 d_{85}로부터, $f_c=4$일 때는 d_{88}로부터 각각 입력)되는데 이때 선택 신호들 ($s1, s0$)은 f_c로 구현된 전가산기 출력이다. 그리고 LFSRd의 좌측에는 3-비트 크기의 LBUF를 두어서 4개의 귀환 비트 조합을 계산할 수 있도록 하였다. (LBUF에서는 d_0의 출력을 차례로 보관하고 있다.) 4개의 귀환 비트 조합 중에서 feedback 1은 원래의 귀환 비트와 동일한 탭의 XOR 조합을, feedback 2는 feedback 1에 비하여 1-비트씩 좌측 이동된 탭의 XOR 조합을, feedback 3는 2-비트씩 좌측 이동된 탭의 XOR 조합을, feedback 4는 3-비트씩 좌측 이동된 탭의 XOR 조합을 이룬다. 사용된 4개의 feedback 조합은 다음과 같이 표현된다.

$$d[89+t] = d[88+t] \oplus d[50+t] \oplus d[47+t] \oplus d[36+t] \oplus d[34+t] \oplus d[9+t] \oplus d[6+t] \oplus d[t] : feedback\ 1$$

$$d[88+t] = d[87+t] \oplus d[49+t] \oplus d[46+t] \oplus d[35+t] \oplus d[33+t] \oplus d[8+t] \oplus d[5+t] \oplus d[-1+t] : feedback\ 2$$

$$d[87+t] = d[86+t] \oplus d[48+t] \oplus d[45+t] \oplus d[34+t] \oplus d[32+t] \oplus d[7+t] \oplus d[4+t] \oplus d[-2+t] : feedback\ 3$$

$$d[86+t] = d[85+t] \oplus d[47+t] \oplus d[44+t] \oplus d[33+t] \oplus d[31+t] \oplus d[6+t] \oplus d[3+t] \oplus d[-3+t] : feedback\ 4$$

마지막으로 LILI-128의 출력 수열은 그림 하단에 설정된 비선형 여과 함수 (nonlinear filter function) f_d로부터 얻어지는 비트 수열이 된다.

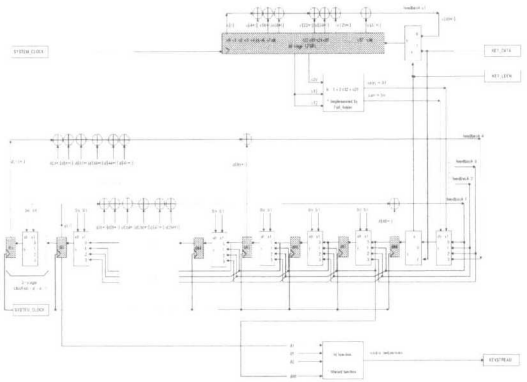

그림 7. LILI-128 고속 구현 방안 제안 (4-bit parallel LFSR$_d$)

5. 메모리 함수 설계 예시 및 분석

병렬 비선형 결합 함수이고, 상기의 특성을 잘 만족하는 또 다른 함수의 예로 Rueppel의 합산 수열 발생기(SUM-BSG: Rueppel's summation generator) [7-10]를 들 수 있다. 세부 설계 예시된 발생기는 그림8과 같이 m개의 LFSR 수열과 M 비트의 캐리 메모리 수열을 각각 입력하는 SUM-BSG를 병렬로 연결시킨 m-병렬 합산 수열 발생기 (m-parallel summation generator)이다. 제안된 발생기의 i번째 SUM-BSGi에서 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 $i=1, 2, \cdots, m$ 이고, y_i는 i번째 SUM-BSGi의 출력 수열, x_{1i}는 LFSR1의 i번째

출력 수열, x_{2i} 는 LFSR2 의 i번째 출력 수열, $x_{m,i}$ 는 LFSRm 의 i번째 출력 수열이며, c_{ij} 는 i번째 발생기에서 사용된 j번째 carry memory 수열이다.

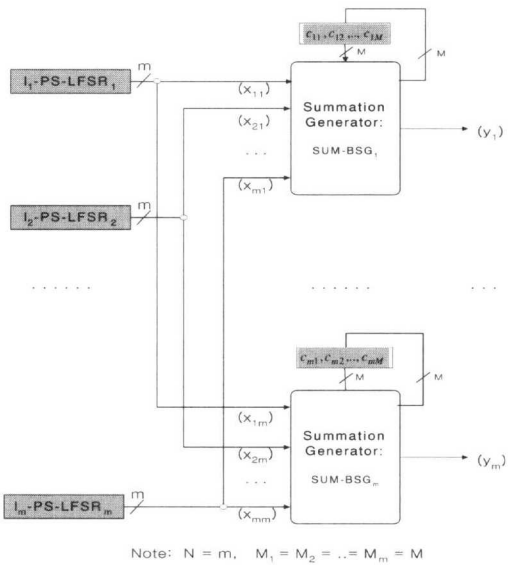

그림 8. m-병렬 합산 수열 발생기 제안

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-BSGi 발생기의 비도 특성은 다음과 같다 [7-10].

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

2) 난수 특성 : 양호

3) 선형 복잡도 : $LC_i \approx P_i$

4) 상관 면역도 : $K_i = m-1$.

SUM-BSGi는 특성 1과 같이 최대 주기, 좋은 랜덤 특성, 주기와 비슷한 크기의 선형복잡도, 그리고 최대 차수 상관 면역도를 갖는 것으로 알려져 있다.

표 1. 병렬형 키수열 발생기와 일반형의 설계 비교

Items	SUM-BSG	8-parallel SUM-BSG
Period	10^{81}	10^{81}
Randomness	random	random
Linear complexity	approximately period	approximately period
Correlation immunity	7	7
Processing rate ratio	1	m =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)

[Note] 설계에 사용된 m=8이고, 19, 23, 29, 31, 37, 41, 43, 47단 LFSR이 8개 사용됨

표 1에서는 m-병렬 합산 수열 발생기를 세부 설계하여 일반 스트림 암호의 비도 요소와 유사한 조건으로 분석하였다. 그 결과 m-비트 생성을 위한 발생기는 각각 원래의 설계 기준을 잘 만족하기 때문에 기존의 비도 수준을 유지할 수 있었으며, 병렬 배치로 인한 암호 처리 속도는 m 배 개선될 수 있음을 확인하였다. 결론적으로 제안된 여러 가지 m-병렬 비선형 발생기들은 하드웨어 복잡도가 다소 증가되지만 (게이트 집적도가 큰 문제가 되지 않는 현실을 감안할 때) 하드웨어 부담을 크게 늘리지 않고도 데이터 처리 속도를 m 배 향상시킬 수 있는 발생기로써 다가오는 정보 고속화시대에 적합하다고 할 수 있다.

V. 결 론

본 논문에서는 스트림 암호의 고속화 설계 방안인 병렬 이동형 PS-LFSR의 구조를 살펴보았으며 다음 여러 가지 형태의 비선형 결합함수에 대한 효율적인 구현 방안을 제안하였다. 즉, 비메모리-비선형 결합함수, 메모리-비선형 결합함수, 비선형 필터 함수, 클럭조절형 결합함수 등 4가지 형태의 출력함수 형태에 대한 효율적인 병렬 구현 방안을 제안하

였다.

또한 설계 검증을 위하여 m-병렬 비선형 필터 함수와 m-병렬 합산 수열 발생기의 설계 예를 제시하였고, 일반 스트림 암호의 비도 요소와 유사한 조건으로 분석하였다. 그 결과 m-비트 생성을 위한 발생기는 각각 원래의 설계 기준을 잘 만족하기 때문에 기존의 비도 수준을 유지할 수 있었으며, 병렬 배치로 인한 암호 처리 속도는 m 배 개선될 수 있음을 확인하였다. 결론적으로 제안형태의 병렬 스트림 암호 발생기는 하드웨어의 복잡도가 다소 증가되지만 (게이트 집적도가 큰 문제가 되지 않는 현실을 감안할 때) 하드웨어 부담을 크게 늘리지 않고도 데이터 처리 속도를 m 배 향상시킬 수 있는 발생기로써 다가오는 정보 고속화시대에 적합하다고 할 수 있다.

참 고 문 헌

[1] AES site in http://csrc.nist.gov/ encryption/aes/.

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

[3] J. Daemen, V. Rijmen, ''The Block Cipher Rijndael,'' Smart Card Research and Applications, LNCS 1820, J.-J. Quisquater and B. Schneier, Eds., Springer-Verlag, 2000, pp. 288-296.

[4] L. Simpson, E. Dawson, J. Dj. Golic and W. Millan, "LILI Keystream Generator," Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptology SAC'2000 to appare in Springer- Verlag LNCS, 2000.

[5] Sober-t16 in https://www.cosic.esat. kuleuven.ac.be/nessie/workshop/submission.html.

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

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

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

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

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

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

[12] 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.

[13] X. G. Zhen and J.L. Massey, "A Spectral Characterization of Cor- relation-Immune Combining Func- tions," IEEE Trans. on Infor. Theo., Vol.34, No.3, May 1988.

[14] 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.

[15] 이훈재, 문상재, "FPGA/VHDL을 이용한 LILI-128 암호의 고속화 구현에 관한 연구," 한국통신정보보호학회논문지 제11권, 제3호, pp.23-32, 2001년 6월호.

이 훈 재(HoonJae 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~2002년 2월 : 경운대학교 컴퓨터전자정보공학부 조교수

2002년 3월~현재 : 동서대학교 인터넷공학부 정보네트워크공학전공 조교수

〈주관심분야〉 정보보호, 네트워크보안, 정보통신

문 상 재(SangJae Moon) 정회원

1972년 2월 : 서울대학교 공업교육과 졸업 (전자공학 학사)
1974년 2월 : 서울대학교 대학원 전자공학과 졸업 (전자공학 석사)
1984년 6월 : 미국 UCLA 전기공학과 졸업 (통신공학박사)
2001년 2월 ~2002년 2월 : 한국정보보호학회 회장 (현 명예회장)
1974년 12월~현재 : 경북대학교 공과대학 전자전기 컴퓨터학부 교수
2000년 8월 ~ 현재 : ITRC 이동네트워크 정보보호기술 연구센터 소장
<주관심분야> 정보보호, 정보통신