비선형 결합함수에 따른 병렬 스트림 암호에 관한 연구

(A Study on the Parallel Stream Cipher by Nonlinear Combiners)

이 훈 재*, 변 우 익*
(Hoon-Jae Lee* and Woo-Ick Byun*)

요 약 최근 암호학계에는 미국의 AES와 더불어 차세대 유럽 암호 표준화 프로젝트 (NESSIE)가 진행 중에 있다. 이 프로젝트의 동기식 스트림 암호 분야에서는 호주의 Simpson이 제안한 LILI-128 암호를 포함하여 6개의 후보가 제안된 상태이며, 상기 알고리즘들은 고속화를 위하여 병렬 형태로 설계 개념을 채택하려하고 있다. 본 논문에서는 스트림 암호의 고속화 설계 방안인 병렬 이동형 PS-LFSR의 구조를 살펴본 다음 여러 가지 형태의 비선형 결합함수에 대한 효율적인 구현 방안을 제안하였다. 즉, 비메모리-비선형 결합함수, 메모리-비선형 결합함수, 비선형 필터함수, 클럭조절형 결합함수 등 4가지 형태의 출력함수 형태에 대한 효율적인 병렬 구현 방안을 제안하였고, 합산 수열 발생기의 병렬구현 기법과 클럭조절형 LILI-128의 병렬구현 기법을 예시하여 안전성과 성능을 분석하였다.

Abstract In recent years, the AES in North America and the NESSIE project in Europe have been in progress. Six proposals have been submitted to the NESSIE project, including the LILI-128 by Simpson in Australia in the synchronous stream cipher category. These proposals tend towards a design with parallelism of the algorithms in order to facilitate speed-up. In this paper, we consider the PS-LFSR and propose the effective implementation of various nonlinear combiners: memoryless-nonlinear combiner, memory-nonlinear combiner, nonlinear filter function, and clock-controlled function. Finally, we propose m-parallel SUM-BSG and LILI-128's parallel implementation as examples, and we determine their securities and performances.

I. 서 론

최근 암호학계에는 미국의 AES [1]와 NESSIE (New European Schemes for Signature, Integrity and Encryption) [2]라는 차세대 유럽 암호 표준화 프로젝트가 큰 흐름을 주도하고 있다. AES는 DES를 개선시키기 위한 미국의 대형 프로젝트로서 Rijndael [3]이 이미 표준으로 확정된 바 있으며, NESSIE 프로젝트에는 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 대규모 과제라고 볼 수 있다. 이 중 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, 이러한 알고리즘들은 고속화를 위하여 병렬 형태로 설계 개념을 채택하려 하고 있다.

본 논문에서는 스트림 암호의 고속화 설계 방안인 병렬 이동형 PS-LFSR [6]의 구조를 살펴본 다음 여러 가지 비선형 결합함수의 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 비메모리형 (memoryless-type)과 메모리형 (memory-type), 출력함수의 구성방식에 따라 여러개의 LFSR 출력을 비선형적으로 조합하는 비선형 조합형 (nonlinear conbiner)과 하나의 LFSR로부터 비선형 필터출력을 발생시키는 비선형 필터형 (nonlinear filter function), 마지막으로 클럭조절 유무에 따라 클럭 동기형 (clock-synchronized type)과 클럭조절형 (clock-controlled type) 으로 대별될 수 있다. 본 논문에서는 이들을 다시 조합하여 비메모리-비선형 결합함수, 메모리-비선형 결합함수, 비선형 필터함수, 그리고 클럭조절형 결합함수 등 4가지 경우를 선택하여 병렬형 설계 방안을 도출하고, 각각의 효율적인 구현 방안을 분석코자 한다. 마지막으로 메모리형태인 합산 수열 발

* 경운대학교 컴퓨터전자정보공학부

생기 [7-10]를 고속화시킨 m-병렬 합산 수열 발생기 (m -parallel SUM-BSG)를 설계·분석하고, 클럭조절형태인 LILI-128 암호의 병렬 구현에 관하여 설계 예시 및 분석한다.

II. LFSR과 병렬 구조

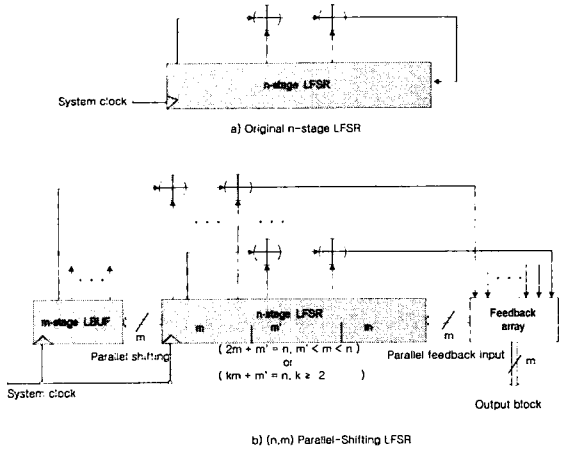


그림 1. LFSR과 병렬 이동형 PS-LFSR

병렬 이동형 PS-LFSR (Parallel-Shifting LFSR) [6]은 그림 1과 같이 병렬형 스트림 암호 구현을 위한 핵심 요소이며, 시스템 1-클럭에 m-비트를 이동시키는 LFSR의 새로운 구조이다. 그림 b)에서 가운데에 위치한 n-단 LFSR은 입출력 연결 구성만 병렬로 이루어질 뿐 기존의 LFSR과 동일한 출력을 낼 수 있으며, m-단 LBUF (left buffer)는 다음 클럭에서 입출력 값을 저장하는 임시 버퍼의 역할을 한다. 귀환 배열 (feedback array)은 귀환 비트 연결들을 모아서 병렬로 입력 처리하는 부분이다. m-비트 단위로 병렬 이동하기 위해서 병렬 경로가 구성되어야 하며, 귀환 탭에서도 m-묶음의 XOR 조합 연산을 거쳐 귀환 배열로 동시에 모인다. 다음 클럭 (시점)에서는 귀환 배열의 내용이 LFSR의 m-비트 블록 부분으로 이동되고, 계속해서 왼쪽으로 블록 크기 만큼 m-병렬 이동된다.

직렬 배열된 LFSR은 병렬 형태로 재구성이 가능하며, 일례로서 그림 2의 ($n=40, m=8$) PS-LFSR과 같은 구성을 갖는다. 이러한 PS-LFSR은 병렬 형태로 입출력이 가능하도록 재구성되었지만 레지스터의 재배열에도 불구하고 출력 수열에는 변화가 없을 뿐만 아니라 비도에도 영향을 미치지 않는 고속형 하드웨어/소프트웨어 구성 방법이다.

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

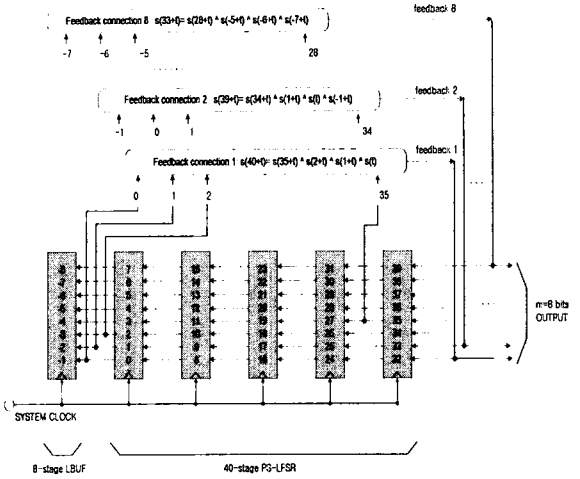


그림 2. (40, 8) PS-LFSR의 구성 예

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

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

$$s(39+t) = s(34+t) \oplus s(1+t) \oplus s(t) \oplus s(-1+t)$$

$$s(38+t) = s(33+t) \oplus s(t) \oplus s(-1+t) \oplus s(-2+t)$$

$$s(37+t) = s(32+t) \oplus s(-1+t) \oplus s(-2+t) \oplus s(-3+t)$$

$$s(36+t) = s(31+t) \oplus s(-2+t) \oplus s(-3+t) \oplus s(-4+t)$$

$$s(35+t) = s(30+t) \oplus s(-3+t) \oplus s(-4+t) \oplus s(-5+t)$$

$$s(34+t) = s(29+t) \oplus s(-4+t) \oplus s(-5+t) \oplus s(-6+t)$$

$$s(33+t) = s(28+t) \oplus s(-5+t) \oplus s(-6+t) \oplus s(-7+t)$$

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-wise exclusive-or) 연산을 의미한다.

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 동일하다. 또한 비트 단위의 출력을 발생하는 LFSR과 비교할 때 PS-LFSR은 암호화 처리 속도가 m배 빨라지며, 고속화에 따른 하드웨어 복잡도는 다소 증가될 수 있지만 최근의 집적회로 기술 발전으로 큰 문제가 되지 않는다.

III. 비선형 결합함수에 따른 병렬 스트림 암호 제안

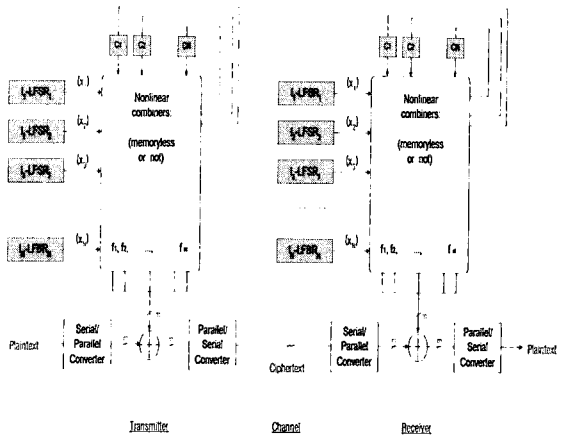


그림 3. 병렬형 스트림 암호

일반 스트림 암호의 키 수열 발생기와 달리 병렬형 스트림 암호 [6]는 그림 3과 같이 N개의 LFSR (linear feedback shift register)을 이용하지만 $m(\leq N)$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 가능하다. 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 [11-13]을 높일 수 있고, 이에 따라 상관성 공격(correlation attack)을 방어토록 할 수도 있다.

본 논문에서는 이들을 다시 조합하여 비메모리-비선형 결합함수, 메모리-비선형 결합함수, 비선형 필터형, 그리고 클럭 조절형 등 4가지 경우를 선택하여 병렬형 설계 방안을 도출하고, 각각의 효율적인 구현 방안을 분석한다.

1. 비메모리-비선형 결합함수

그림 4는 m-병렬 비메모리-비선형 결합 함수의 일반화된 모델을 나타내었다. 비메모리-비선형 결합 함수는 메모리를 사용하지 않으며, 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.

본 비메모리-일반형 발생기에 사용될 m-병렬 비선형 결합 함수 (키 수열 발생기)는 일반 비메모리-비선형 결합 함수 [7,8]와 동일하게 구성되며, 다만 입력 비트와 출력 비트만 차이가 나게 된다.

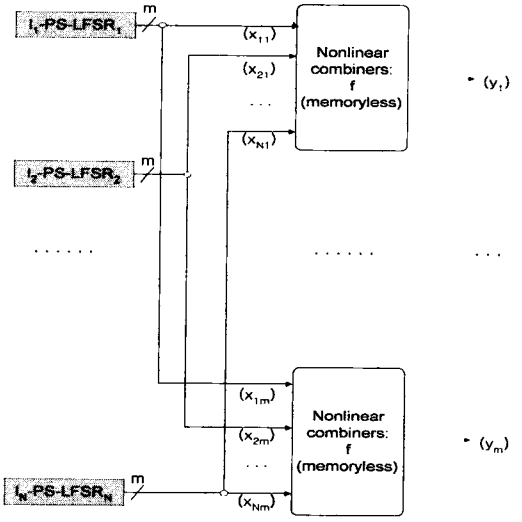


그림 4. m-병렬 비메모리-비선형 결합함수 일반형 모델

$$y_1 = f(x_{11}, x_{21}, \cdots, x_{N1}) = a_{1,0} + (\sum_{i=1}^{N} a_{1,i}\, x_{i1}) + (\sum_{i,j} a_{1,ij} x_{i1} x_{j1} +) + \ldots + a_{1,12..N}\, x_{11} x_{21} .. x_{N1}$$

$$y_2 = f(x_{12}, x_{22}, \cdots, x_{N2}) = a_{2,0} + (\sum_{i=1}^{N} a_{2,i}\, x_{i2}) + (\sum_{i,j} a_{2,ij} x_{i2} x_{j2}) + \ldots + a_{2,12..N} x_{12} x_{22} .. x_{N2}$$

$$\cdots$$

$$y_m = f(x_{1m}, x_{2m}, \cdots, x_{Nm}) = a_{m,0} + (\sum_{i=1}^{N} a_{m,i}\, x_{im}) + (\sum_{i,j} a_{m,ij} x_{im} x_{jm}) + \ldots + a_{m,12..N}\, x_{1m} x_{2m} .. x_{Nm}$$

여기서 x_{ij}는 LFSR$_i$의 병렬 m비트 중 j번째 출력 수열 $(1 \leq i \leq N,\ 1 \leq j \leq m)$을 나타내며, $a_{k,i}, a_{k,i}', a_{k,ij}, a_{k,ij}', a_{k,ij}'', \cdots, a_{k,12..N} \in [0,1]$이 된다.

2. 메모리-비선형 결합함수

그림 5는 m-병렬 메모리-비선형 결합 함수 $(f_1, f_2, \ldots, f_m)$의 일반화된 모델을 나타내었다. 비선형 결합 함

수의 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.

본 일반형 발생기에 사용될 m-병렬 비선형 결합 함수 (키 수열 발생기)는 일반 비선형 결합 함수 [7,8]와 유사하며, 다음과 같이 구성된다.

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

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

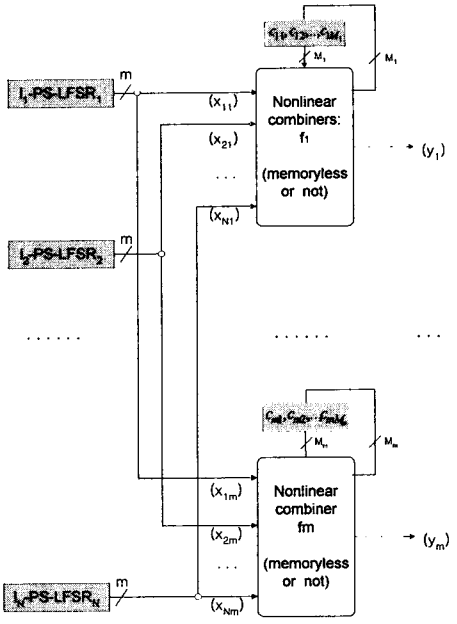
$$\cdots$$

$$f_m(x_{1m}, x_{2m}, \cdots, x_{Nm}, c_{m1}, c_{m2}, \cdots, c_{mM_m}) = a_{m,0} + \left(\sum_{i=1}^{N} a_{m,i}\, x_{im} + \sum_{i=N+1}^{N+m} a_{m,i}'\, c_{mi}\right) + \left(\sum_{i,j} a_{m,ij}\, x_{im} x_{jm} + \sum_{i,j} a_{m,ij}'\, c_{mi} c_{mj} + \sum_{i,j} a_{m,ij}''\, x_{im} c_{mj}\right) + \ldots + a_{m,12..N+M_m}\, x_{1m} x_{2m} .. x_{Nm} c_{m1} c_{m2} \cdots c_{mM_m}$$

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, $a_{k,i}, a_{k,i}', a_{k,ij}, a_{k,ij}', a_{k,ij}'', \cdots, a_{k,12..N+M_k} \in [0,1]$, $0 \le M_1, M_2, \cdots, M_m \le m$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 각각 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.



Note: $N \ge m,\ 1 \le M_1, M_2, \ldots, M_N \le m$

그림 5. m-병렬 메모리-비선형 결합함수 일반형 모델

3. 비선형 필터함수

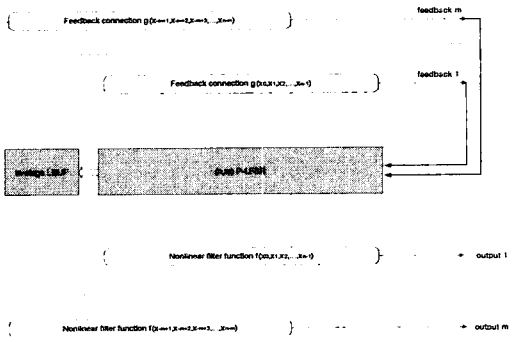


그림 6. m-병렬 비선형 필터 함수

m-병렬 비선형 필터함수는 기존의 비선형 필터함수의 출력 수열을 그대로 유지하면서 그 출력을 m-비트씩 발생시키기 위하여 그림 6과 같이 출력단에 동일한 비선형 필터함수를 여

러개 병렬화시켰다. 비선형 필터함수는 비메모리형의 함수를 갖고 있으며, 그 출력을 병렬화시키기 위하여 동일한 함수로서 입력값만 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, 병렬형의 m개 귀환함수 및 m개 필터함수는 다음과 같이 정의된다.

$$g(x_0, x_1, \ldots, x_{n-1}),$$
$$g(x_{-1}, x_0, \ldots, x_{n-2}),$$
$$\cdots\cdots$$
$$g(x_{-m+1}, x_{-m+2}, \ldots, x_{n-m}).$$

그리고,

$$f(x_0, x_1, \ldots, x_{n-1}),$$
$$f(x_{-1}, x_0, \ldots, x_{n-2}),$$
$$\cdots\cdots$$
$$f(x_{-m+1}, x_{-m+2}, \ldots, x_{n-m}).$$

4. 클럭 조절형 함수 예시

클럭 조절형 스트림 암호는 임의의 하나의 발생기로부터 다른 발생기의 클럭을 랜덤하게 조절하는 형태이며, LILI-128 암호 [4]를 예로 들 수 있다. 이러한 형태의 발생기는 여러 클럭을 구동하여 하나의 출력을 발생하기 때문에 구조적으로 속도를 저하시키는 문제점을 안고 있다. 본 절에서 예로든 LILI-128 암호는 다음과 같은 방법을 통하여 병렬화가 가능하며, 구조적인 속도저하의 문제를 해결할 수 있다.

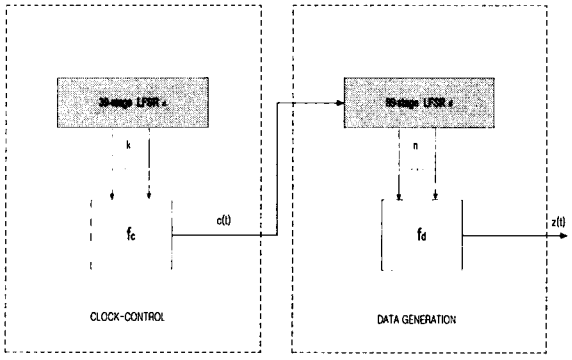


그림 7. 클럭조절형 함수 예: LILI-128 스트림 암호

LILI-128이 갖는 구조적인 문제를 해결하기 위하여 비트 이동 루트가 클럭을 초월하여 1~4 비트씩 가변적으로 이동할 수 있는 4-비트 병렬 입력 $LFSR_d$의 고속 구현 방안은 그림 8과 같이 해결될 수 있다 [15].

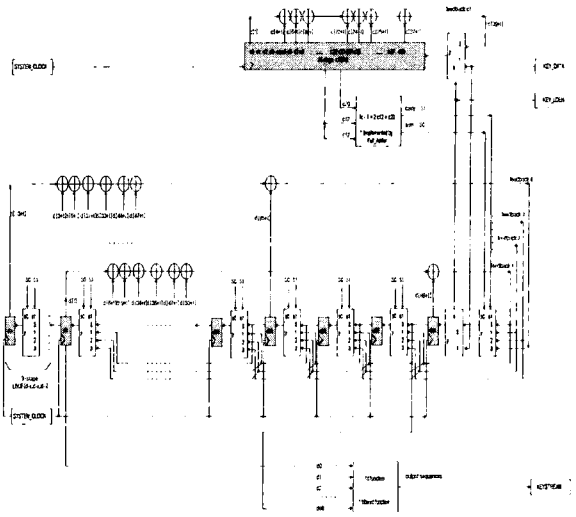


그림 8. LILI-128 고속 구현 방안 (4-bit parallel $LFSR_d$)

그림 8의 상반부에 위치한 $LFSR_c$는 일반적인 39단 이동 레지스터 및 귀환 비트 조합으로 구현이 가능하다. 그리고 출력 f_c 회로는 $LFSR_d$의 좌측 이동 클럭 수를 결정하는 것으로서 전가산기 (full adder)를 사용하면 쉽게 구현된다. 그러나 89단 $LFSR_d$ 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. 이 부분에 대한 설계 아이디어를 "4-비트 병렬 $LFSR_d$ (4-bit parallel $LFSR_d$)" 라고 부르며, 고속화 구현 회로의 핵심 부분이다. 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 전가산기의 출력으로부터 얻어진다. 그리고 $LFSR_d$의 좌측에는 3-비트 LBUF가 4개의 귀환 비트 조합을 계산하기 위하여 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.

5. 메모리함수 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 그림9와 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-BSG$_i$에서 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-BSG$_i$의 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.

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-BSG$_i$ 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 : $LC_i \le P_i$
4) 상관 면역도 : $K_i = m - 1$.

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

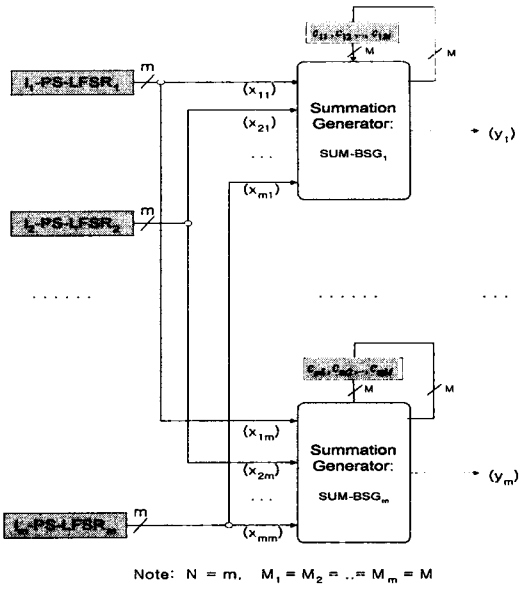


그림 9. m-병렬 합산 수열 발생기

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 m배 개선될 수 있

음을 확인하였다. 결론적으로 제안 발생기는 하드웨어의 복잡도가 다소 증가되지만 게이트 집적도가 큰 문제가 되지 않는 현실을 감안할 때 하드웨어 부담을 크게 늘리지 않고도 데이터 처리 속도를 m배 향상시킬 수 있는 발생기로써 다가오는 정보 고속화시대에 적합하다고 할 수 있다.

Ⅳ. 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 필터함수, 클럭조절형 결합함수 등 4가지 형태의 출력함수 형태에 대한 효율적인 병렬 구현 방안을 제안하였다.

또한 설계 검증을 위하여 m-병렬 비선형 필터함수와 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 m배 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 m배 향상시킬 수 있는 발생기로써 다가오는 정보 고속화시대에 적합하다고 할 수 있다.

참고문헌

[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] 이훈재, 문상재 "고속 안전 통신을 위한 병렬형 스트림 암호," 한국통신학회 논문지 2001년 5월호 게재.

[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 Correlation-Immune Combining Functions," 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 게재 예정.