PS-WFSR 및 워드기반 스트림암호의 병렬구조 제안

성상민* · 이훈재** · 이상곤** · 임효택**

*동서대학교 유비쿼터스 IT학과, **동서대학교 컴퓨터정보공학부

On a PS-WFSR and a Parallel-Structured Word-Based Stream Cipher

SangMin Sung* · HoonJae Lee**· SangGon Lee**· HyoTaek Lim**

*Dept. of Ubiquitous IT, Dongseo University

**Div. of Computer & Information Engineering, Dongseo University

E-mail : ssm1@nate.com; hjlee@dongseo.ac.kr

요 약

본 논문에서는 일반적인 비트기반의 비선형 결합함수를 고속화하기 위하여 워드기반 스트림 암호에서 적용될 워드기반 비선형 결합함수 구조를 제안하였다. 특히, 워드기반 병렬구조를 갖는 PS-WFSR을 제안하였고, 이를 활용하여 비트 기반 비선형 결합함수를 고속화시킨 워드기반 병렬형 비선형 결합함수를 다음과 같이 제안하였다. m-병렬 워드기반 비메모리 비선형 결합함수, m-병렬 워드기반 메모리 비선형 결합함수, m-병렬 워드기반 비선형 필터함수를 신규 제안하였고, 그 성능을 분석하였다.

ABSTRACT

In this paper, we propose some parallel structures of the word-based nonlinear combine functions in word-based stream cipher, high-speed versions of general (bit-based) nonlinear combine functions. Especially, we propose the high-speed structures of popular three kinds in word-based nonlinear combiners using by PS-WFSR (Parallel-Shifting or Parallel-Structured Word-based FSR): m-parallel word-based nonlinear combiner without memory, m-parallel word-based nonlinear combiner with memories, and m-parallel word-based nonlinear filter function. Finally, we analyze its cryptographic security and performance.

키워드

Cryptosystem, PS-WFSR, m-parallel, Nonlinear Function, Word-based Stream cipher

Ⅰ. 서 론

최근 워드 기반의 스트림 암호가 NESSIE[1] 및 ECRYPT에서의 eSTRREAM[2] 등과 같은 국제공개경쟁을 통하여 제안된 바 있다. 대표적인 예로서, SOBER-t16[3] 및 SOBER-t32[3], Dragon[5] 등을 들 수 있다. 이러한 워드 기반 스트림 암호 알고리즘들은 소프트웨어적이나 하드웨어적으로 고속 구현을 목표로 설정하고 있다.

본 논문은 암호 시스템 설계에서 다음과 같은 세 가지 중점사항에 목표를 두고 있다. 즉, 높은 안전성, 고속 암·복호화 성능, 모바일 통신에서의 채널 오류 확산 방지 등이다. 이를 위하여 3가지 형태의 병렬 워드기반 비선형 결합함수를 제안한다. 일반적으로 워드기반 FSR (Feedback Shift Register)은 한 클럭에 하나의 워드(W=16, 32 또는 64-비트) 값을 출력하는 구조이다. 하지만, 본 제안 워드기반 병렬형 레지스터(PS-WFSR)는 한 클럭에 m-워드 (m x W 비트)가 출력될 수 있어, 기존 방식보다 m배 빠른 연산이 가능하다. 워드 기반 단일 비선형 함수를 이용하여 m-병렬 워드 기반 비선형 결합함수 3가지 형태를 제안하며, 이 때 m-병렬형은 단일형에 비하여 한 클럭 당 m-워드 키 수열 출력을 동시에 생성한다. 제안될 3가지 유형은 m-병렬 워드기반 비메모리 비선형 결합함수, m-병렬 워드기

반 메모리 비선형 결합함수, 그리고 m-병렬 워드기반 비선형 필터함수이며, 마지막으로 그 성능을 분석한다.

II. 워드기반 FSR의 병렬구조 제안

일반적으로 알려진 대부분의 스트림 암호는 비트단위의 암호화 연산을 실행하며, 비트기반 스트림 암호로 볼 수 있다. 최근 유럽 NESSIE와 ECRYPT의 eSTREAM의 표준화 공개경쟁을 통하여 SNOW, Sober, TURING, Dragon과 같은 워드기반 스트림 암호가 설계되고 있다 [1-5].

그림 1에서와 같이 비트기반 스트림 암호를 고속화 처리하고자 제안된 방식이 워드기반 스트림 암호이며, 처리 단위는 워드 (W-비트, $W=16,32,64$ 등)가 된다.

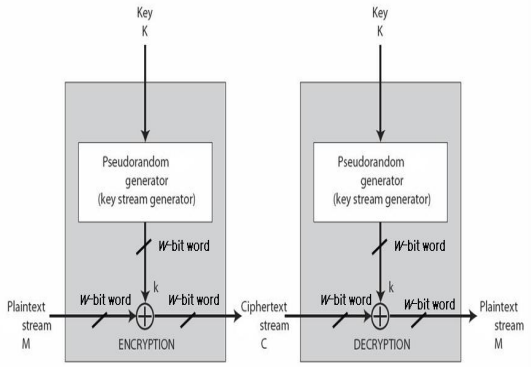

그림 1. 워드기반 스트림 암호

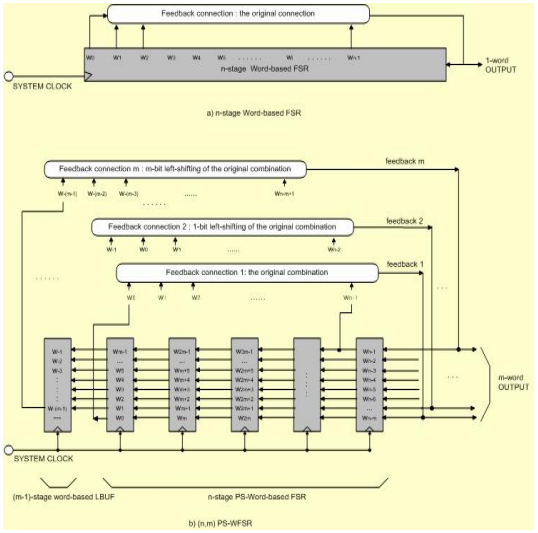

그림 2. n-단 워드 기반 WFSR 및 (n, m) PS-WFSR.

그림 2에서는 제안된 병렬 워드기반 스트림 암호의 기본 요소인 PS-WFSR $(1 \le m \le n)$을 보여주고 있다. PS-WFSR은 "한 클럭으로 어떻게 하면 워드기반 WFSR을 m-word 출력시킬 수 있을까?"에 대한 그 해답이다. (n,m) PS-WFSR은 병렬구조를 갖는데, 그림의 오른쪽 부분은 병렬화 이전에 원래의 n-워드 레지스터가 있고, 그 왼쪽에는 병렬화 구성을 위하여 $(m$-1)단 워드기반 버퍼가 추가되었다. (n,m) PS-WFSR에 대한 각 m-워드 블록이 시스템 클럭에 맞추어 이동하며, 귀환 탭 (feedback taps)의 XOR 연산 조합으로 m 병렬 경로가 각각 구성된다. 즉, n-단 PS-WFSR에서 각 m-워드 블록은 시스템 클록에 맞추어 이동하며, m 귀환 경로(feedback paths)는 귀환 탭들을 XOR 연산으로 조합한다. 이 때 조합되는 귀환 탭은 원래의 귀환 탭 구성을 각각 1-워드/2-워드/.../(m-1)-워드 단위로 시프트한 탭 구성과 같다.

첫 번째 귀환함수는 원래의 귀환함수를 사용하며, 두 번째 귀환함수는 원래의 귀환함수를 1-워드 이동시킨 함수를 사용하고, 세 번째 귀환함수는 2-워드 이동시킨 함수를 사용하고, 비슷한 방법으로 m번째 귀환함수는 원래의 귀환함수를 (m-1) 워드 이동시킨 함수를 사용하게 된다. 이렇게 되면, 병렬 PS-WFSR의 발생속도는 병렬이전의 WFSR보다 m배 빠른 속도를 내게 된다. 또한, PS-WFSR은 참고문헌[1,2]에서 언급된 안전성 요소인 주기, 선형복잡도 등에서 원래의 WFSR의 안전성 수준을 그대로 유지할 수 있다.

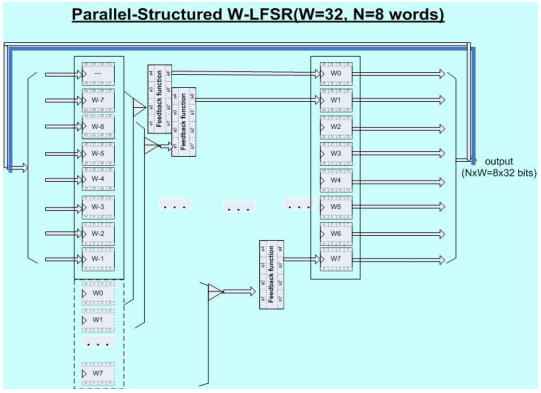

그림 3. (n=8, m=8) PS-WFSR 발생기 예제

그림 3에서는 $W=32$워드 구조를 갖는 $n=8$단 WFSR을 병렬화하고자 그 구성 예로서, $m=8$ 병렬형으로 구성한 $(n=8,m=8)$PS-WFSR의 구조를 나타내었다. 그림에서 W_0, W_1, ..., W_7로 표기된 워드 이동 레지스터 (WFSR)은 병렬화 이전의 원래의 레지스터이며, 그 왼쪽에 표기된 W_{-1}, W_{-2},..., W_{-7} 등의 $(m-1)$=7개의 워드 버퍼는 병렬화를 위하여 추가된 레지스터이다. 이 때 고속화를 위한 m의 선택은 1~n의 범위가 되는데, 본 예시에서는 최대 값이 선택된 경우를 보여주고 있다. 이때 최대 값인 $m=n$이 선택되었다는 의미는 다양한 병렬화 방법 중에서 가장 빠른 병렬구조로 설계되었다는 의미이다.

III. 다양한 m-병렬 워드기반 함수 제안

비트기반 병렬형 스트림 암호는 PS-LFSR을 독립적으로 조합하는 다양한 비선형 함수가 제안된 바 있다 [4]. 본 제안에서는 워드기반 스트림 암호에 대하여 워드기반 병렬형 PS-WFSR을 활용한 다양한 비선형 함수의 구성을 제안하고자 한다.

3.1 m-병렬 워드기반 비선형 키 수열 발생기 (비메모리 형) 제안

워드단위로 키수열을 발생시키는 PS-WFSR을 활용하여, 이를 병렬로 구성하여 속도를 높일 수 있는 방법으로 비선형 비메모리 병렬 함수는 다음과 같이 구성되어진다. 이는 비트 기반의 PS-LFSR을 이용하여 비트 기반의 비선형 비메모리 병렬 함수의 발생 원리[4]를 확장하여, 워드 기반의 PS-WFSR을 활용한 병렬 함수이다. 이 때 각 각의 함수는 워드 단위의 출력을 내며, 아래 수식의 벡터 표기는 워드 단위를 말한다.

$$F_1(\overline{x}_{11},\overline{x}_{21},...,\overline{x}_{N1}) = a_{1,0} + (\sum_{i=1}^{N} a_{1,i}\overline{x}_{i1}) + (\sum_{i,j} a_{1,ij}\overline{x}_{i1}\overline{x}_{j1}) + ... + a_{1,12..N}\overline{x}_{11}\overline{x}_{21}..\overline{x}_{N1}$$

$$F_2(\overline{x}_{12},\overline{x}_{22},...,\overline{x}_{N2}) = a_{2,0} + (\sum_{i=1}^{N} a_{2,i}\overline{x}_{i2}) + (\sum_{i,j} a_{2,ij}\overline{x}_{i2}\overline{x}_{j2}) + ... + a_{2,12..N}\overline{x}_{12}\overline{x}_{22}..\overline{x}_{N2}$$

...

$$F_m(\overline{x}_{1m},\overline{x}_{2m},...,\overline{x}_{Nm}) = a_{m,0} + (\sum_{i=1}^{N} a_{m,i}\overline{x}_{im}) + (\sum_{i,j} a_{m,ij}\overline{x}_{im}\overline{x}_{jm}) + ... + a_{m,12..N}\overline{x}_{1m}\overline{x}_{2m}..\overline{x}_{Nm}$$

여기에서 모든 계수 $a_{i,jk..m}$은 이진 값 "0"또는 "1"을 갖는다.

3.2 m-병렬 워드기반 비선형 키 수열 발생기 (메모리 형) 제안

워드단위로 키수열을 발생시키는 PS-WFSR을 활용하여, 비선형 비메모리 병렬 함수는 다음과 같이 구성되어 진다. 이는 비트 기반의 PS-LFSR을 이용하여 비트 기반의 비선형 메모리 병렬 함수의 발생 원리[4]를 확장하여, 워드 기반의 PS-WFSR을 활용한 병렬 함수이다. 이 때 각 각의 함수는 워드 단위의 출력을 내며, 아래 수식의 벡터 표기는 워드 단위를 말한다.

$$F_1(\overline{x}_{11},\overline{x}_{21},...,\overline{x}_{N1},\overline{c}_{11},\overline{c}_{12},...,\overline{c}_{1M_1}) = a_{1,0} + (\sum_{i=1}^{N} a_{1,i}\overline{x}_{i1} + \sum_{i=N+1}^{N+m} a'_{1,i}\overline{c}_{1i}) + (\sum_{i,j} a_{1,ij}\overline{x}_{i1}\overline{x}_{j1} + \sum_{i,j} a'_{1,ij}\overline{c}_{1i}\overline{c}_{1j} + \sum_{i,j} a''_{1,ij}\overline{x}_{i1}\overline{c}_{1j}) + ... + a_{1,12..N+M_1}\overline{x}_{11}\overline{x}_{21}..\overline{x}_{N1}\overline{c}_{11}\overline{c}_{12}..\overline{c}_{1M_1}$$

.....

$$F_m(\overline{x}_{1m},\overline{x}_{2m},...,\overline{x}_{Nm},\overline{c}_{m1},\overline{c}_{m2},...,\overline{c}_{mM_m}) = a_{m,0} + (\sum_{i=1}^{N} a_{m,i}\overline{x}_{im} + \sum_{i=N+1}^{N+m} a'_{m,i}\overline{c}_{mi}) + (\sum_{i,j} a_{m,ij}\overline{x}_{im}\overline{x}_{jm} + \sum_{i,j} a'_{m,ij}\overline{c}_{mi}\overline{c}_{mj} + \sum_{i,j} a''_{m,ij}\overline{x}_{im}\overline{c}_{mj}) + ... + a_{m,12..N+M_m}\overline{x}_{1m}\overline{x}_{2m}..\overline{x}_{Nm}\overline{c}_{m1}\overline{c}_{m2}..\overline{c}_{mM_m}$$

여기에서 모든 계수 $a_{i,jk..m}$은 이진 값 "0"또는 "1"을 갖는다.

3.3 m-병렬 워드기반 비선형 키 수열 발생기 (비선형 필터형) 제안

m-병렬 워드기반 비선형 필터함수는 m개의 워드기반 비선형 필터함수를 각각 0-워드, 1-워드, 2-워드,.., (m-1)-워드씩 병렬 시프트하여 배열 구성하는 구조를 가졌으며, 다음과 같이 귀환함수 병렬 구조와 출력함수 병렬 구조로 나눌 수 있다. 이때 출력함수의 수열을 병렬구조화 이전의 원래 출력수열과 동일한 값을 출력하면서 속도가 m배 향상되는 구조이다. 귀환함수 $G(\overline{x_0},\overline{x_1},...,\overline{x_{n-1}})$을 원래의 귀환함수(병렬화 이전 함수)라고 하고, 출력함수 $F(\overline{x_0},\overline{x_1},...,\overline{x_{n-1}})$을 원래의 출력함수(병렬화 이전 함수)라고 둘 때, 다음과 같이 정의할 수 있다:

$G(\overline{x_0},\overline{x_1},...,\overline{x_{n-1}})$: 1번째 워드기반 병렬귀환함수 (원래의 귀환함수),

$G(\overline{x_{-1}},\overline{x_0},...,\overline{x_{n-2}})$: 2번째 워드기반 병렬귀환함수 (1-워드 시프트된 함수),

.....

$G(\overline{x_{-m+1}},\overline{x_{-m+2}},...,\overline{x_{-m+n}})$: m번째 워드기반 병렬귀환함수 (($m-1$)-워드 시프트된 함수),

$F(\overline{x_0},\overline{x_1},...,\overline{x_{n-1}})$: 1번째 워드기반 병렬출력함수 (원래의 출력함수),

$F(\overline{x_{-1}},\overline{x_0},...,\overline{x_{n-2}})$: 2번째 워드기반 병렬출력함수 (1-워드 시프트된 함수),

.....

$F(\overline{x_{-m+1}},\overline{x_{-m+2}},...,\overline{x_{-m+n}})$: m번째 워드기반 병렬출력함수 (($m-1$)-워드 시프트된 함수).

결과적으로, m-병렬 워드기반 귀환함수와 m-병렬 워드기반 필터함수들은 각각 원래의 워드기반 함수에 각각 0, 1, 2, ..., (m-1) 워드씩 시프트된 병렬 구조를 갖게 되며, 이를 통하여 출력 키 수열 성능은 m배 암.복호화 속도가 향상이 된다.

Ⅳ. 안전성 및 성능 분석

제안된 PS-WFSR의 특성은 표 1 및 아래 4가지 특성과 같다. 이는 m배 병렬화된 논리구조를 통하여 개선하였기 때문에 당연한 결과라고 볼 수 있다.

특성 1. 만일 두 경우의 초기상태가 같을 경우, (n,m) PS-WFSR의 출력 수열은 n단 WFSR의 출력수열과 동일한 출력을 발생한다.

특성 2. (n,m) PS-WFSR의 출력수열의 주기는 2^n-1이다. 이는 n-단 WFSR의 기존 주기값과 동일한 값을 출력하기 때문에 동일한 주기를 갖게 된다.

특성 3. (n,m) PS-WFSR은 기존의 n-단 WFSR보다 속도가 m배 빨라진다. 이는 m배 병렬화 논리회로 구성을 통하여 속도가 개선되기 때문이다.

특성 4. 제안된 3가지 워드기반 병렬 함수의 성능은 일반 워드기반 함수를 사용할 때보다 암호화/복호화 속도가 $m(1 \le m \le n)$배 빨라진다.

표 1. (n,m) PS-WFSR의 안전성 및 성능

Items	Conventional n-stage WFSR	Proposed (n,m) PS-WFSR
Period	2^n-1	2^n-1
Randomness	Good	Good
Linear Complexity	n	n
Speed	1	m
Hardware complexity (Example, m=8, n=39)	1	1.83($< m$)

표 1에서와 같이, 제안된 병렬형 PS-WFSR은 기존 WFSR과 비교할 때 최대 주기를 보장하며, 동일한 선형복잡도 및 랜덤특성을 보여주었다. 결과적으로 하드웨어 구성에서 약간의 복잡도가 상승되었지만, 그 암호화/복호화 성능은 m배 상승됨을 알 수 있다. 여기에서 m은 사용자의 요구수준에 맞추어 설계가 가능하며 최소 1에서 최대 n(WFSR의 워드 단수)까지 선택이 가능함을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 블록암호와 스트림암호의 조합된 형태인 병렬 스트림암호의 구조를 고속화하기 위하여 병렬 워드기반 스트림 암호를 제안하였으며, 일반적으로 블록 암호는 블록 또는 병렬 프로세싱이 가능하고 스트림 암호는 보안성 및 에러 확산에 대한 강점이 있는 것으로 알려져 있다. 워드기반 스트림 암호에서 사용되는 모든 워드기반 WFSR은 1-클럭 입력 시에 1-워드가 이동 및 출력하는 형태이며, 본 제안에서는 이를 병렬화한 (n,m) PS-WFSR 구조를 제안하였고, 제안된 레지스터는 1-클럭 입력 시에 m-워드(m=8, 16, 23 또는 64 등)가 이동 및 출력되는 새로운 구조를 갖는다. 또한, 병렬 고속구조를 갖는 PS-WFSR을 활용하여 3가지 유형의 새로운 m-병렬 워드기반 키 수열 발생기를 제안하였다. 이는 일반적으로 잘 알려진 비트기반의 비메모리 비선형 결합함수를 고속화시킨 m-병렬 워드기반 비메모리 비선형 결합함수, 비트기반의 메모리 비선형 결합함수를 고속화시킨 m-병렬 워드기반 메모리 비선형 결합함수, 비트기반의 비선형 필터함수를 고속화시킨 m-병렬 워드기반 비선형 필터함수의 제안이며, 전체 성능을 분석한 결과 동일한 보안성 조건에서 속도가 m배 빨라질 수 있음을 보였다.

참고문헌

[1] NESSIE site at http://www.cosic.esat.kuleuven.ac.be/nessie/.

[2] ECRYPT, eSTREAM site at http://www.ecrypt.eu.org/stream/.

[3] Sober-t16, t-32 at http://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submission.html.

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

[5] K. Chen, M. Henrickson, W.Millan, J. Fuller, A. Simpson, Ed Dawson, Hoonjae Lee, Sangjae Moon, "Dragon: A Fast Word Based Stream Cipher," LNCS, Vol. 3505, Dec. 2004.