워드기반 스트림암호의 병렬화 고속 구현 방안

이훈재* · 도경훈*

On a Parallel-Structured High-Speed Implementation of the Word-Based Stream Cipher

HoonJae Lee* · KyungHoon Do*

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 4가지 형태의 워드기반 병렬형 비선형 결합함수를 다음과 같이 제안하였다. m-병렬 워드기반 비메모리 비선형 결합함수, m-병렬 워드기반 메모리 비선형 결합함수, m-병렬 워드기반 비선형 필터함수, m-병렬 워드기반 클럭조절형 함수를 제안하였고, 마지막으로 m-병렬 워드기반 DRAGON의 병렬 구조를 통하여 그 성능을 분석하였다.

ABSTRACT

In this paper, we propose some parallel structures of the word-based nonlinear combining functions in word-based stream cipher, high-speed versions of general (bit-based) nonlinear combining functions. Especially, we propose the high-speed structures of popular four 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, m-parallel word-based nonlinear filter function, and m-parallel word-based clock-controlled function. In addition, we propose an implementation example of the m-parallel word-based DRAGON stream cipher, and determine its cryptographic security and performance.

키워드

암호시스템, PS-WFSR, m-병렬, 비선형 함수, 워드기반 스트림암호

Key word

Cryptosystem, PS-WFSR, m-parallel, nonlinear function, word-based stream cipher

* 동서대학교 컴퓨터정보공학부

접수일자 : 2009. 12. 17
심사완료일자 : 2010. 02. 17

I. 서 론

최근 워드 기반의 스트림 암호가 NESSIE[1] 및 ECRYPT에서의 eSTRREAM[2] 등과 같은 국제공개경쟁을 통하여 제안되어 2008년 최종적인 평가 라운드를 거친 바 있다. 이중에서 워드기반 스트림 암호의 대표적인 예로서, SOBER-t16[5] 및 SOBER-t32[5], Dragon[12] 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[3]. 즉, 높은 안전성, 고속 암·복호화 성능, 모바일 통신에서의 채널 오류 확산 방지 등이다. 이를 위하여 4가지 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 m 배 빠른 연산이 가능하다. 워드 기반 단일 비선형 함수를 이용하여 m-병렬 워드기반 비선형 결합함수 4가지 형태를 제안하며, 이 때 m-병렬형은 단일형에 비하여 한 클럭 당 m-워드 키 수열 출력을 동시에 생성한다. 제안될 4가지 유형은 m-병렬 워드기반 비메모리 비선형 결합함수, m-병렬 워드기반 메모리 비선형 결합함수, m-병렬 워드기반 비선형 필터함수, 그리고 m-병렬 워드기반 클럭조절형 함수이며, 마지막으로 m-병렬 워드기반 DRAGON[12]이 병렬 설계 예로 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[1-2].

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.

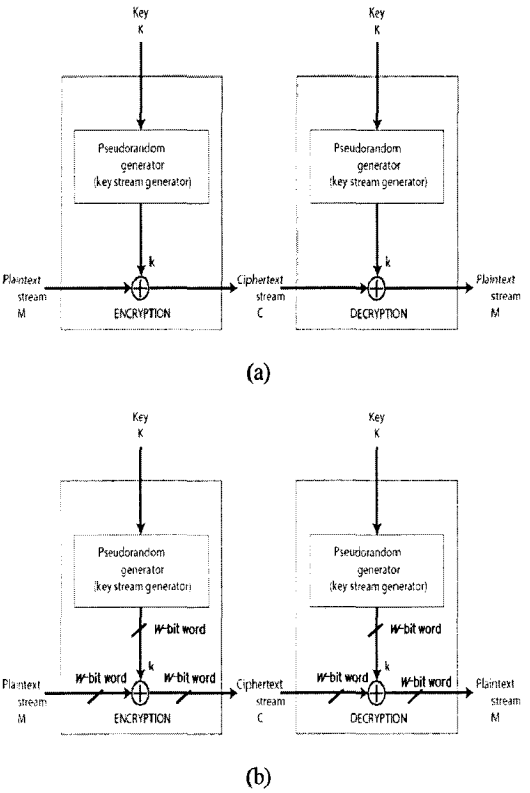


그림 1. 비트기반 스트림 암호와 워드기반 스트림 암호
(a) 비트기반 스트림 암호
(b) 워드기반 스트림 암호
Fig. 1 Bit-based stream cipher and word-based stream cipher
(a) bit-based stream cipher
(b) word-based stream cipher

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 위

드기반 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.

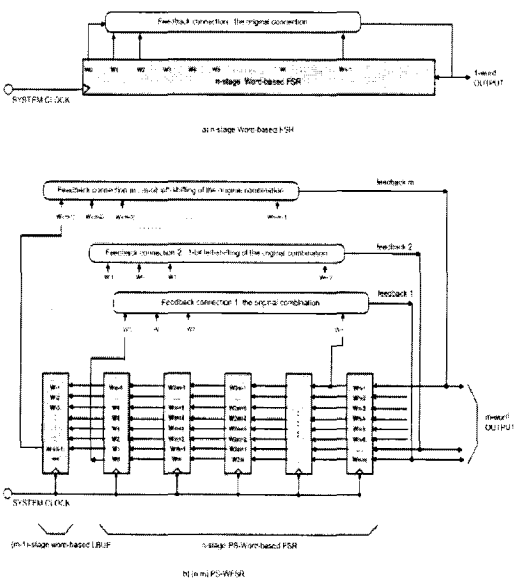
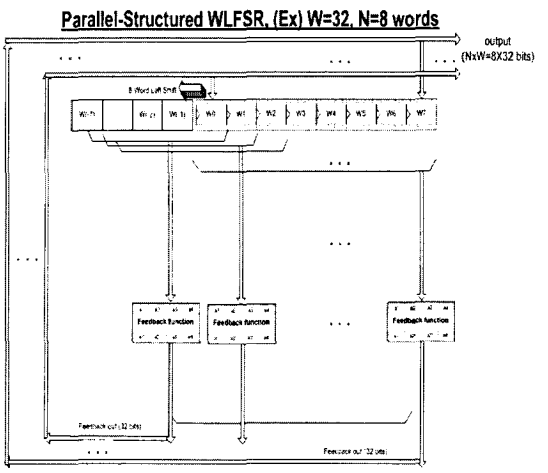
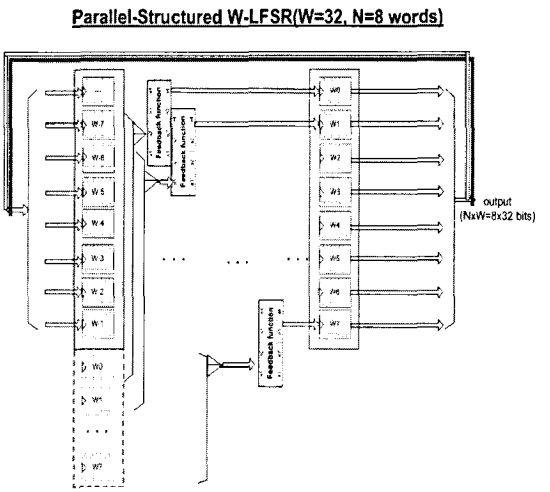


그림 2. n-단 워드 기반 WFSR 및 $(n,\ m)$ PS-WFSR.
Fig. 2 n-stage word-based WFSR and $(n,\ m)$ PS-WFSR



(a)



(b)

그림 3. (n=8, m=8) PS-WFSR 발생기 예제
(a) 일반 직렬 표기법 (b) 병렬 표기법
Fig. 3 An example for (n=8, m=8) PS-WFSR
(a) Serial-structure (b) Parallel-structure

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. 워드 이동 레지스터의 개념을 쉽게 표기하기 위하여 개념적인 일반 직렬 표기법을 그림 a)에 나타내었고, 실제 병렬형태로 작동하는 예시를 위하여 그림 b)에는 병렬 표기법을 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 $1 \sim n$의 범위가 되는데, 본 예시에서는 최대 값이 선택된 경우를 보여주고 있다. 이때 최대 값인 $m=n$이 선택되었다는 의미는 다양한 병렬화 방법 중에서 가장 빠른 병렬 구조로 설계되었다는 의미이다.

Ⅲ. m-병렬 워드기반 비선형 함수 제안

비트기반 병렬형 스트림 암호는 PS-LFSR을 독립적으로 조합하는 다양한 비선형 함수가 제안된 바 있다[6]. 본 제안에서는 워드기반 스트림 암호에 대하여 워드기반 병렬형 PS-WFSR을 활용한 다양한 비선형 함수의 구성을 제안하고자 한다.

안전한 워드기반 스트림 암호 통신을 위하여, 워드기반 비선형 함수의 키 수열 출력에 대한 예측이 불가능하여야 할 뿐 아니라, 이전에 발생된 키 수열 워드로부터 일부분의 키 수열도 찾아내기 어려운 특성이 요구된다.

아래의 내용은 키 수열에 대한 예측 불가능성의 필요조건이다[7~12]:

1) 긴 주기(long period) : 키 수열은 긴 주기를 가져야 한다.
2) 큰 선형 복잡도(large linear complexity) : 키 수열은 큰 선형 복잡도를 가져야 한다. 이는 출력 키수열을 예측할 수 있는 동등한 워드기반 LFSR을 조합할 수 없다는 의미이다.
3) 랜덤 특성(randomness) : 큰 선형 복잡도가 랜덤 특성을 의미하지는 않으며, 키 수열의 통계특성이 이상적인 랜덤 발생과 유사함을 의미한다.
4) 적절한 상관면역도(proper order of correlation immunity) : 워드 기반 비선형 함수 F의 모든 N-입력 워드 $\overline{x_1}, \overline{x_2}, ..., \overline{x_N}$에서 임의의 $k(\leq N)$조합 $\overline{x_{i_1}}, \overline{x_{i_2}}, ..., \overline{x_{i_k}} (1 \leq i_1, i_2, ..., i_k \leq N)$에서도 출력 함수 F와 무상관성 (uncorrelated)을 나타낼 때, 이때 함수 F를 k-차 상관면역도를 가졌다고 한다. 워드기반 비선형 함수의 설계 시 적절한 상관면역성을 갖도록 설계하면, 상관성 공격(correlation attack)을 방어할 수 있게 된다.

3.1 m-병렬 워드기반 비선형 키수열 발생기 (비메모리형) 제안

워드단위로 키수열을 발생시키는 PS-WFSR을 활용하여, 이를 병렬로 구성하여 속도를 높일 수 있는 방법으로 그림 4와 같은 구조를 갖는 비선형 비메모리 병렬 함수는 다음과 같이 구성되어진다. 이는 비트 기반의 PS-LFSR을 이용하여 비트 기반의 비선형 비메모리 병렬 함수의 발생 원리[6]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.

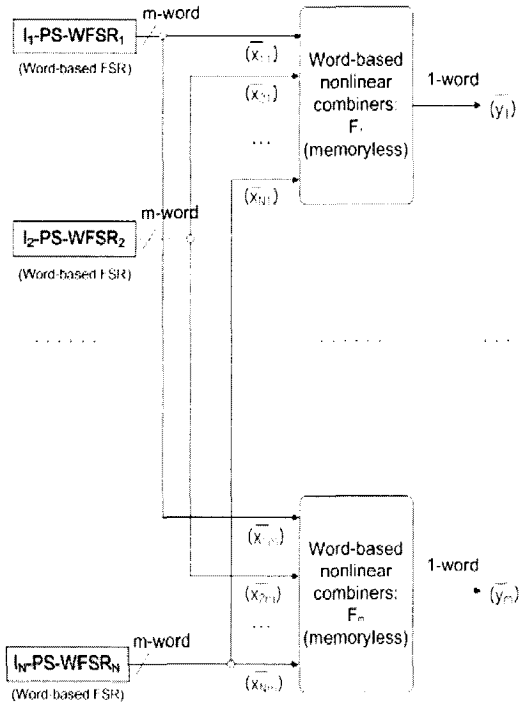


그림 4. 워드기반 비선형 병렬 키 수열 발생기 (비메모리 형)
Fig. 4 A word-based nonlinear parallel generator without memory

3.2 m-병렬 워드기반 비선형 키수열 발생기 (메모리형) 제안

워드단위로 키 수열을 발생시키는 **PS-WFSR**을 활용하여, 그림 5와 같은 구조를 갖는 비선형 비메모리 병렬 함수는 다음과 같이 구성되어 진다. 이는 비트 기반의 **PS-LFSR**을 이용하여 비트 기반의 비선형 메모리 병렬 함수의 발생 원리[6]를 확장하여, 워드 기반의 **PS-WFSR**을 활용한 병렬 함수이다. 이 때 각 각의 함수는 워드 단위의 출력을 내며, 아래 수식의 벡터 표기는 워드 단위를 말한다.

$$F_1(\bar{x}_{1t},\bar{x}_{2t},\ldots\bar{x}_{Nt},\bar{c}_{1t},\bar{c}_{2t},\ldots\bar{c}_{Mt})=a_{t0}+(\sum_{i=1}^{N}a_{ti}\bar{x}_{it}+\sum_{i=N+1}^{N+m}a_{ti}\bar{c}_{it})+(\sum_{i,j}a_{tij}\bar{x}_{it}\bar{x}_{jt}+\sum_{i,j}a_{tij}\bar{c}_{it}\bar{c}_{jt}+\sum_{i,j}a_{tij}\bar{x}_{it}\bar{c}_{jt})+\ldots+a_{t12N+M}\bar{x}_{1t}\bar{x}_{2t}\ldots\bar{x}_{Nt}\bar{c}_{1t}\bar{c}_{2t}\ldots\bar{c}_{Mt}$$

.....

$$F_m(\bar{x}_{1t},\bar{x}_{2t},\ldots\bar{x}_{Nt},\bar{c}_{1t},\bar{c}_{2t},\ldots\bar{c}_{Mt})=a_{t0}+(\sum_{i=1}^{N}a_{ti}\bar{x}_{it}+\sum_{i=N+1}^{N+m}a_{ti}\bar{c}_{it})+(\sum_{i,j}a_{tij}\bar{x}_{it}\bar{x}_{jt}+\sum_{i,j}a_{tij}\bar{c}_{it}\bar{c}_{jt}+\sum_{i,j}a_{tij}\bar{x}_{it}\bar{c}_{jt})+\ldots+a_{t12N+M}\bar{x}_{1t}\bar{x}_{2t}\ldots\bar{x}_{Nt}\bar{c}_{1t}\bar{c}_{2t}\ldots\bar{c}_{Mt}$$

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

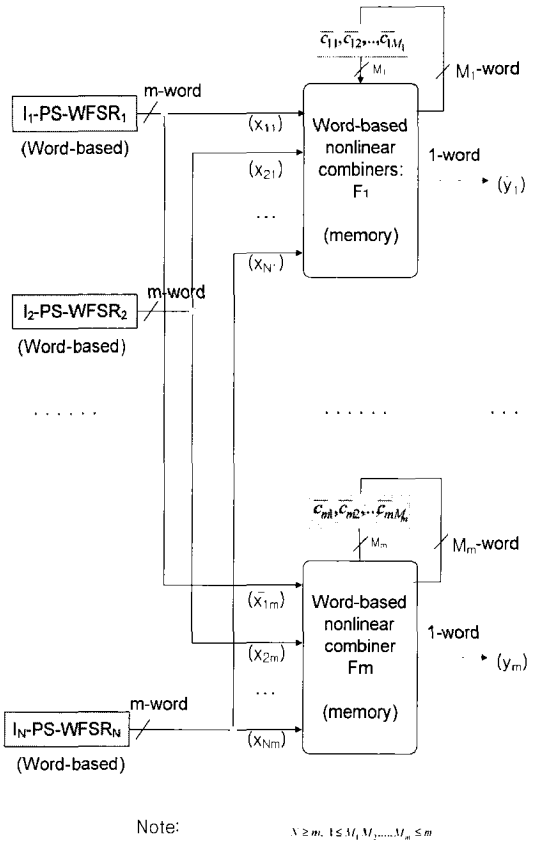


그림 5. 워드기반 비선형 병렬 키 수열 발생기 (메모리 형)
Fig. 5 A word-based nonlinear parallel generator with memories

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

m-병렬 워드기반 비선형 필터함수를 그림6과 같이 제안한다. 본 아이디어는 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 키수열 성능은 m배 암.복호화 속도가 향상이 된다.

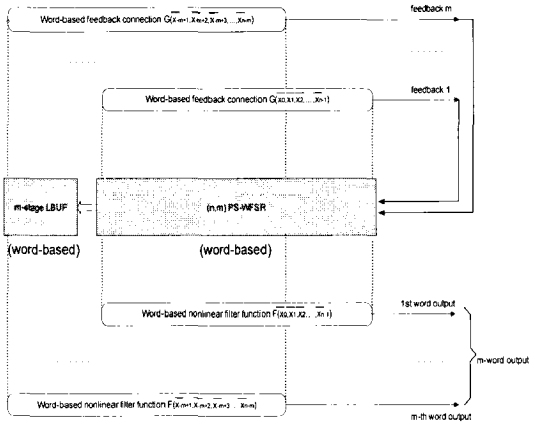


그림 6. 워드기반 비선형 병렬 키 수열 발생기 (비선형 필터형)
Fig. 6 A word-based nonlinear filter generator

3.4 m-병렬 워드기반 클럭조절형 키 수열 발생기 제안

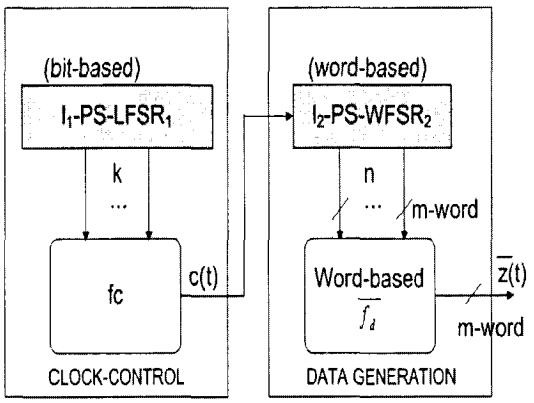


그림 7. 워드기반 비선형 병렬 키 수열 발생기 (클럭 조절형)
Fig. 7 A word-based nonlinear parallel generator with clock-control circuits

일반적으로 비트 기반 클럭 조절형 스트림 암호는 프로세싱에 있어서 구조적으로 성능이 저하된다. 왜냐하면, 클럭조절형의 경우 키 수열 출력이 1-클럭에 출력되는 정상클럭 출력에 비하여 여러 클럭을 소모하여 키 수열이 출력되기 때문이다. 이는 워드기반 클럭 조절형 발

생기에서도 안전성을 높이기 위하여 성능 저하의 손실을 제공하게 된다. 본 연구에서는 m-병렬 워드기반 클럭조절형 스트림 암호를 개선하여, 구조적인 성능저하를 보상하는 방안을 제안하고자 한다.

설계 예로서, 비트 기반 LILI-II [4] 발생기의 경우 1-비트 출력을 발생시키기 위하여 랜덤한 1~4개 중의 한가지 클럭 선택을 필요로 한다. 그림 7에서와 같이 m-병렬 워드기반 LILI-II 발생기 구조에서는 랜덤한 변화를 갖는 클럭을 병렬 구조로 랜덤하게 조합하여 1-클럭에 워드 출력이 발생될 수 있도록 개선하고 있다. 그림에서 f_c는 LILI-II 발생기의 원래의 클럭조절함수와 동일하며, $\overline{f_d}$는 LILI-II 발생기의 원래의 데이터 생성함수와 동일한 함수를 워드 단위 m개 배열하고 있어서 출력 속도를 m배 향상시킬 수 있게 된다.

Ⅳ. 안전성 및 성능 분석

제안된 PS-WFSR의 특성은 표 1 및 아래 4가지 특성과 같다. 이는 m배 병렬화된 논리구조를 통하여 개선할 경우에는 수십 Gbps의 성능이 가능하다.

표 1. (n,m) PS-WFSR의 안전성 및 성능
Table 1. Security and performances for (n,m) PS-WFSR

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($< m$)

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

표 2. m=8 및 m=16에서의 병렬형 Dragon 성능
Table 2. Parallel Dragon Performances for m=8 and m=16

Items		Worst case	Typical case	Best case
Area (gates) @comb.		8,126	8,068	8,219
Area (gates) @memory		287,600	287,600	287,544
Critical Path delay (ns)		14.36	10.26	6.72
Throughput (Gbps)		4.4	6.2	9.5
Estimated Parallel-Throughput (Gbps)	m=8	35.2	49.6	76
	m=16	70.4	99.2	152

Notes : 1) "comb." means combinational logic,
2) "Best"/"Typical"/"Worst" case means the synthesis library conditions,
3) "Throughput [bps]" = number of output in bits x speed

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

마지막으로, m-병렬 구성을 갖는 Dragon-128 [12]을 설계하였고, 그림 8 및 표 2와 같이 그 성능을 분석하였다. 일반적인 구성에서는 그 성능이 4.4~9.5Gbps의 성

능이 도출되었지만, 이를 병렬화 구성할 경우에는 70.4~152 Gbps의 성능이 가능하다.

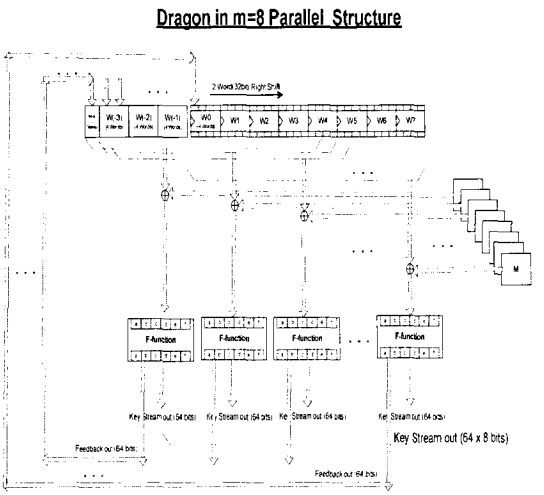


그림 8. m-병렬 워드기반 Dragon-128 구조 제안
Fig. 8 m-parallel word-based Dragon-128 Structure

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 4가지 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 필터함수 및 비트기반 클럭조절형 함수를 고속화시킨 m-병렬 워드기반 클럭조절형 함수의 제안이며, 전체 성능을 분석한 결과 동일한 보안성 조건에서 속도가 m배 빨라질 수 있음을 보였다.

마지막으로 DRAGON-128[12]을 고속화하기위한 m-병렬 워드기반 Dragon-128 병렬 구조를 통하여 그 성능을 분석하였다.

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] J. Daemen, V. Rijmen, "The Block Cipher Rijndael," Smart Card Research and Applications, LNCS 1820, Springer-Verlag, 2000, pp. 288-296.

[4] 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.

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

[6] Hoonjae Lee and 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," In 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] 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.

저자소개

이훈재(HoonJae Lee)

1985년 경북대학교 전자공학과 졸업 (학사)
1987년 경북대학교 전자공학과 졸업(석사)
1998년 경북대학교 전자공학과 졸업(박사)
1997년~1998년 국방과학연구소 선임연구원
1998년~2002년 경운대학교 조교수
2002년~현재 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격

도경훈(KyeongHoon Do)

1990년 2월 : 경북대학교 전자공학과 졸업(공학사)
1992년 2월 : 경북대학교 전자공학과 졸업 (공학석사)
1995년 8월 : 경북대학교 전자공학과 졸업(공학박사)
1996년 3월~현재 : 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : WSN, 모바일컴퓨팅, 인공지능