고속 병렬형 PS-WFSR을 적용한 보안 IP SAN 설계

김봉근* · 이훈재**

Desiogn of secure IP SAN with high-speed paralllel PS-WFSR

Bong-Geun Kim* · HoonJae Lee**

본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업
지원을 받아 수행된 것임(과제번호: 2011-0004833)

요 약

최근 급격히 증가하는 정보량으로 인해 기업에서 필요한 스토리지 수요도 점차 증가하고 있다. 기존의 광선로를 이용한 SAN은 설치 및 유지비용 등의 문제로 인해 IP를 이용한 SAN환경으로 전환되고 있다. 그러나 IP 네트워크를 이용하게 됨으로써 기존의 TCP/IP 네트워크에서 발생하는 보안 취약점을 동일하게 가진다. 또한, 스토리지 트래픽의 기밀성을 위해 전송데이터를 암호화 하지만 기존에 사용하는 방식으로 10G이상 대규모 데이터트래픽을 처리할 수 없다. 이러한 네트워크 스토리지의 보안 취약점 및 암호화 속도 개선을 위해 본 논문에서는 병렬 워드기반 스트림암호(PS-WFSR)를 하드웨어로 구현하여 IP SAN 환경에 적용한 구조를 제안한다.

ABSTRACT

Rapid surge in date quantity lead to increase in storage demand from corporate. The existing SAN with fiber channel is being changed to IP-based SAN environment due to installment and maintenance cost. But the IP-based network still have some similar security problems as existing TCP/IP network. Also, for the security reasons of storage traffic, data are encrypted, but with the existing system, data larger than 10G can't be handled. To address security and speed issue, this paper proposes to a structure applied to IP SAN environment with Parallel Structure Word-based FSR (PS-WFSR) as hardware.

키워드

IP SAN보안, PS-WFSR, 스트림 암호

Key word

IP SAN보안, PS-WFSR, Stream Cipher

* 종신회원 : 동서대학교 유비쿼터스IT학과 석사
** 정회원 : 동서대학교 정보통신공학전공 책임교수
(교신저자, hjlee@dongseo.ac.kr)

접수일자 : 2011. 08. 05
심사완료일자 : 2011. 08. 31

Ⅰ. 서 론

현재의 스토리지 시장은 10G 또는 그 이상의 대역폭을 요구하는 환경으로 나아가고 있으며, 기업을 포함한 많은 기관들의 스토리지 장치들이 직접적으로 연결된다. 애플리케이션 서버에 의해 제어되는 DAS(Direct Attached Storage)에서 컴퓨팅 시스템과 소프트웨어가 LAN을 통해 파일서버 스토리지에 있는 데이터에 접근 가능 한 네트워크 스토리지로 사용되고 있다. 특히 iSCSI는 IETF에서 개발한 IP기반 스토리지 네트워킹 프로토콜로써 이더넷이 전 세계적으로 구축되어 있기 때문에, 고비용의 복잡한 파이버 채널 SAN 없이도 네트워크 스토리지의 유연한 데이터 관리 성능을 충분히 활용할 수 있다는 장점이 있다.

그러나 iSCSI와 같은 이더넷 기반의 네트워크 스토리지들은 기존의 TCP/IP 네트워크에서 발생하는 데이터 변조 및 중요 데이터 유출 등 심각한 보안 취약점을 동일하게 가지고 있어 이에 따른 보안 대책이 필요하다.

현재, IP SAN 네트워크에서 iFCP게이트웨이 스위치 및 iSCSI카드를 사용하는 장비들은 전송되는 데이터를 AES나 3DES를 사용하여 암호화 하고 암호화된 데이터의 End-to-End 전송을 보장함으로써 IP환경에서의 보안성을 유지하고 있다.

표1. 기존에 발표된 ASIC AES 성능
Table 1. Performance of Some previous published ASIC AES Designs

Implementation	Technology	Throughput (Mb/s)	Gates
Server [1]	350nm	1,690	149,000
Kim [2]	180mm	1,640	28,626
Kuo [3]	180nm	1,280	173,000
Verbauwhede [4]	180nm	1,600	173,000
Gurkaynak [5]	250nm	2,120	119,000
Li [6]	180nm	3,840	39,980
Abid [7]	180nm	6,274	13,093

위의 표1은 기존에 발표된 ASIC AES의 성능을 비교한 표이다. 2001년 Kuo가 173,000 Gates로 최대 1Gbps의 성능으로 ASIC AES의 구현에 성공한 사례를 시작으로 다양한 ASIC AES 구현이 시도되었으며, 지난 2010년 Abid은 13098 Gates로 최대 6Gbps의 성능으로 보다 경량화되고 속도가 향상된 ASIC AES의 구현에 성공하였다. 한편, 상용화된 AES ASIC의 경우 최고 10Gbps(90nm)의 속도로 암호화를 수행한다.

하지만 표1에서 보여주는 것처럼 블록암호방식은 하드웨어 구현 시 스트림암호방식과 동일성능을 내기위해 하드웨어 복잡도 증가, 고성능칩 사용이 필요하고, 현재까지 상용화된 블록암호 보안칩 제품으로도 10G 이상의 대규모 데이터를 처리하기 힘들며, 대용량 데이터의 암호화 시 전체 시스템의 가용성이 떨어질 수 있다는 점을 고려하여야 한다.

이에 본 논문에서는 블록 암호 대신 병렬 워드기반 스트림암호(PS-WFSR)를 하드웨어로 구현하여 IP SAN 환경에 적용할 것을 제안한다. 제안된 논문에서 사용하는 고속 병렬형 PS-WFSR을 적용한 Dragon128 알고리즘은 한 클럭에 m-워드(m x W비트)가 출력될 수 있어, 기존 방식보다 m배 빠른 연산이 가능하다. 그리고 스트림암호를 ASIC으로 구현 시 6524Gate로 최대 23Gbps의 속도를 예상할 수 있고 이를 병렬구성(PS-WFSR)할 경우 70.4～150Gbps의 성능이 예상된다. 또한, 주기 및 선형복잡도 등에서 원래의 WFSR의 안정성 수준을 그대로 유지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 일반적인 IP SAN 환경과 병렬 워드기반 스트림 암호 알고리즘에 대하여 설명하고, 3장에서는 고속 병렬 스트림 암호칩을 제안하고 4장에서 제안된 암호칩의 안정성과 성능 평가, 마지막 5장에서 결론을 맺도록 한다.

Ⅱ. 관련연구

2.1. IP SAN

IP SAN이란 IP를 주된 통신 프로토콜로 이용하는 스토리지 네트워크 환경이다. IP SAN을 통해 기존의 IP 설비를 그대로 스토리지 네트워크의 인프라로 이용할 수 있을 뿐 아니라 스토리지 장비와 스위치로부터 파이버 채널 트래픽을 IP 기반의 링크로 통신할 수 있다.

2.1.1 IP SAN 도입배경

SAN은 파이버 채널을 전제로 하고 있었고, 블록 데이터를 기가비트 환경에서 고속으로 전달하면서 사실상 파이버 채널은 SAN과 동의어로 사용되었다. 그러나 파이버 채널 시장은 재교육 필요성, 높은 도입가격 등으로 인해 SAN이 제대로 활용되지 못하였다. 그리고 다음과 같은 이유로 IP 기반 SAN으로 점차 변화하게 되었다.

- IP의 기술적 성숙성
- 가격의 인하
- 거리 제한의 해소
- 추가의 전송경로 확보를 통한 데이터의 고가용성 실현
- 데이터 센터 IP SAN의 확장

2.1.2 IP SAN 취약성

기존의 파이버 채널 기반의 SAN은 일반 데이터 통신과 물리적으로 분리되어 있었다는 점, 그리고 보안과 관리문제가 SAN 기술(파이버채널) 그 자체에서 안정성을 가졌기 때문에 큰 문제가 되지 않았다. 하지만 IP SAN이 사용되면서 IP 네트워크에서는 인터넷을 통해 신뢰할 수 없는 사용자 또는 네트워크 등에 노출될 가능성과 같은 기존의 TCP/IP에서 갖는 취약점을 그대로 가진다. 따라서 스토리지 데이터에 인증, 기밀성, 무결성을 제공함으로써 민감한 정보를 안전하게 관리할 수 있는 방안이 필요하다.

2.2. 워드기반 스트림암호(Dragon)

Dragon 암호는 그림 2와 같이 1024-비트 비선형 귀환 레지스터(NLFSR), F 함수, 64-비트 M 메모리로 구성되어 있다. NLFSR은 워드 단위인 32-비트로 이동하는 비선형 레지스터이며, F 함수는 그림 1에서 나타나듯이 6 워드(256비트) 입력을 받아서 256-비트의 출력을 발생시키는 암호 함수 부분이다. 64-비트 M은 메모리로부터 64-비트 값을 읽어 들이는 과정이다. 따라서 Dragon은 1-round 블록 암호의 구조와 유사하며, 64-비트 feedback 입력과 64-비트 키 수열 출력을 발생하는 워드 기반 스트림 암호이다.

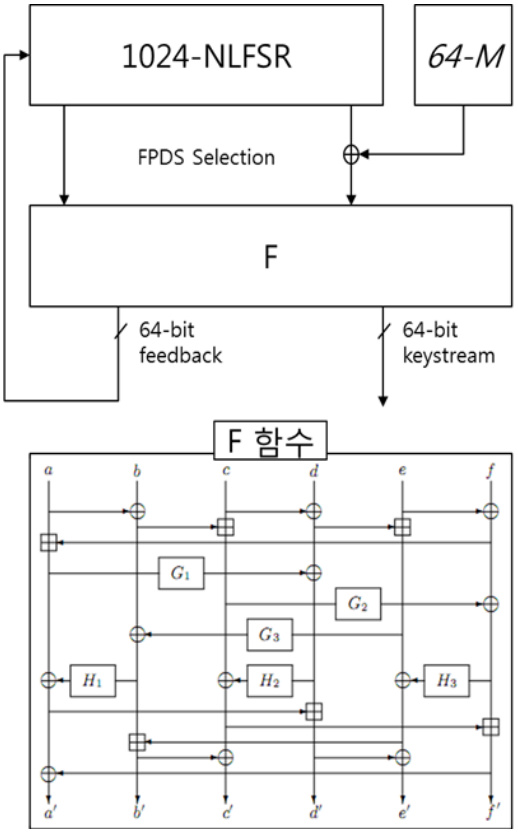

그림 1. 드래곤 스트림 암호
Fig. 1 Dragon stream cipher

2.3. PS-WFSR

PS-WFSR은 비트 기반 스트림 암호를 고속화 처리하고자 제안된 방식이며, 처리 단위는 워드 (*W*-비트, *W*=16,32,64 등)가 된다.

그림 2에서는 병렬 워드기반 스트림암호의 기본요소인 PS-WFSR ($1 \le m \le n$)을 보여주고 있다. PS-WFSR은 한 클럭에 워드기반 WFSR을 *m*-word 출력시킬 수 있는 방법이다. (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, 귀환탭 (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 귀한 탭 구성을 각각 1-워드/2-워드/.../$(m-1)$-워드 단위로 시프트한 탭 구성과 같다.

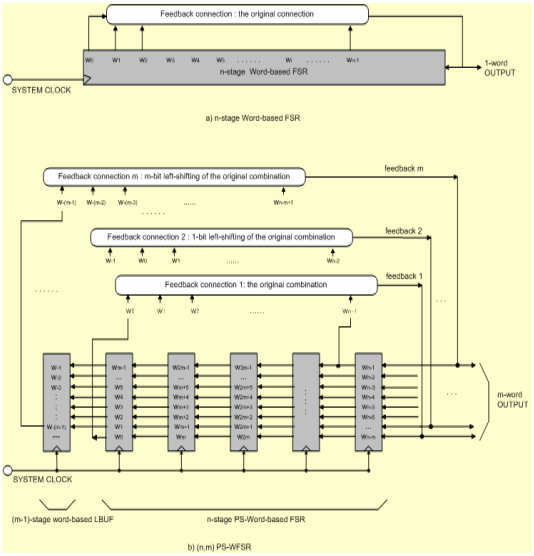

그림 2. n-단 워드 기반 WFSR 및 (n, m) PS-WFSR
Fig. 2 n-stage word-based WFSR and (n, m) PS-WFSR

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 m 배 빠른 속도를 내게 된다. 또한, PS-WFSR은 참고문헌[9,10]에서 언급된 안전성 요소인 주기, 선형복잡도 등에서 원래의 WFSR의 안전성 수준을 그대로 유지할 수 있다.

Ⅲ. 고속 병렬형 PS-WFSR을 적용한 IP SAN 보안환경

일반적으로 IP SAN 환경을 구성하기위해 사용되는 프로토콜은 IPFC, iFCP, iSCSI등이 있다. IPFC는 IP 네트워크에 떨어진 원격 파이버채널 네트워크를 연결하기 위하여 터널링을 사용하므로 Native-IP 환경이 아니므로 제외한다.

그리고 IP SAN환경에서 해당 프로토콜별로 제안한 암호칩을 적용하는 방안을 제시하였다.

3.1. 고속 병렬형 스트림 암호칩

본 논문에서 제안한 IP SAN 보안환경을 위한 암호화 칩은 다음과 같은 특징을 가지고 있다. 첫째, 블록암호에 비해 하드웨어 구현이 쉽고 높은 성능을 보여주는 워드기반 스트림 암호알고리즘을 사용한다. 둘째, 암호화/복호화 처리성능을 대폭 향상시킬 수 있는 스트림암호 병렬처리 알고리즘(PS-WFSR)을 적용한다.

3.2. 제안된 암호화 칩 적용 환경

iFCP는 기존에 구성된 파이버채널 네트워크를 IP 네트워크에 연동하기 위하여 iFCP Gateway 장비를 이용하여 파이버채널 정보를 IP 주소에 Native 모드로 IP에 대응시킴으로써 종단장치간 TCP/IP 세션이 형성시킨다.

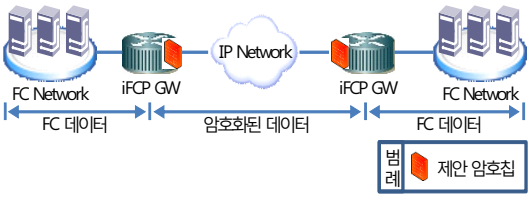

그림 3. iFCP 보안환경
Fig. 3 secure iFCP environment

하지만 iFCP는 별도로 지원하는 보안솔루션이 없어서 iFCP Gateway를 통해 IP네트워크로 나가는 데이터들은 TCP/IP가 가지는 보안위협을 그대로 안게 된다. 이에 제안된 암호칩을 통해 그림 3과 같이 iFCP Gateway를 통해 나가는 모든 데이터를 암호화 한다.

암호칩은 모듈형태 혹은 On-Board형태로 iFCP Gateway 장비에 장착한다.

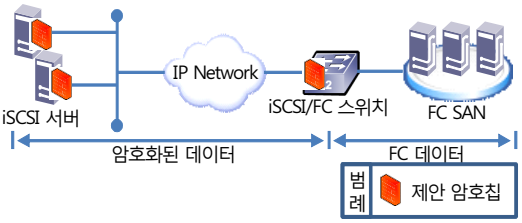

그림 4. iSCSI 보안환경
Fig. 4 secure iSCSI environment

iSCSI는 근본적으로 FC를 배제한다. 호스트 기반의 애플리케이션은 IP를 통해 네트워크로 연결된 스토리지 장치와 통신하는 것으로, 모든 전송 링크가 IP링크라는 것을 의미한다. iSCSI를 지원하는 Server는 iSCSI Adapter통해 Storage 장비들은 iSCSI/FC 스위치를 이용하여 End-to-End IP 통신을 지원한다. 제안된 암호칩은 그림 4와 같이 각 장비의 Adapter에 On-Board 형태로 부착되어 데이터 암호화를 수행한다.

Ⅳ. 관련연구

본 논문에서 제안된 암호화 칩의 고속화를 구현하기 위해 사용한 PS-WFSR의 특성은 표 2 및 아래 4가지 특성과 같다.

표 2. (*n, m*) PS-WFSR의 안전성 및 성능
Table 2. 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 (*m*=8, *n*=39)	1	1.83 (< *m*)

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

특성 2. (n, m) PS-WFSR의 출력수열의 주기는 $2^n - 1$이다. 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 m 배 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 ($1 \leq m \leq n$) 배 빨라진다.

표 2에서와 같이, 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 m 배 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.

표 3. *m*=8 및 *m*=16에서의 병렬형 Dragon 성능
Table 3. 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

Note :
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

마지막으로, m-병렬 구성을 갖는 Dragon-128[11]을 설계하였고, 그림 4 및 표 3과 같이 그 성능을 분석하였다. 일반적인 구성에서는 그 성능이 최대 23Gbps의 성능이 도출되었지만, 이를 병렬화 구성할 경우에는 70.4~152 Gbps의 성능이 가능하다.

Ⅴ. 결 론

본 논문에서는 IP SAN 환경에서 안전하고 고속의 암/복호화를 지원하기 위한 방법으로 PS-WFSR을 적용한 Dragon알고리즘으로 구현한 암호칩을 모든 어댑터 카드 및 네트워크 장비에 추가하는 것을 제안하였다.

Dragon알고리즘을 병렬형 PS-WFSR을 이용하여 구현하였을 때 표 2에서와 같이 기존 WFSR과 비교할 때 최대 주기를 보장하며 동일한 선형 복잡도 및 랜덤특성을 보여주었다. 또한, Dragon(WFSR)알고리즘을 ASIC으로 구현 시 약 6,524 게이트를 사용하여 최대 23Gbps를 예상 가능하고 이를 병렬화 구성할 경우 게이트의 복잡도는 약간 상승하지만 70.4~152Gbps 성능을 예상할 수 있다. 이를 통해 IP SAN환경에서 제안된 암호칩을 사용하였을 경우 향후 스토리지 트래픽이 10Gbps이상으로 증가되더라도 충분한 데이터 암호화 처리성능 및 스토리지 데이터 보안을 제공할 수 있을 것으로 기대된다.

향후 실제 IP SAN 환경에서 데이터 암호화를 제공하기 위한 공용 네트워크에서의 키 관리 방안과 데이터의 인증 방안에 대한 연구를 진행할 예정이다.

참고문헌

[1] R. Sever, A. Neslin, Y. Tekmen, M. Askar " A High Speed ASIC Implementation of the Rijndael Algorithm" International Symposium on circuits and systems, Volume 2, Issue 23 , pp. 541-544, 2004.

[2] Kim, N.S., Mudge, T., and Brown, R. "A 2.3 Gbit/s fully integrated and synthesizable AES Rijndael core", Proc. IEEE Custom Integrated Circuits Conference (CICC), San Jose, CA, pp. 193 – 196, 2003.

[3] H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm," Proc. Cryptographic Hardware and Embedded Systems (CHES) 2001, no. 2162 in LNCS, 2001.

[4] Verbauwhede, I., Schaumont, P., and Kuo, H.:'Design and performance testing of a 2.29-GBit/s Rijndael processor', IEEE J. Solid-State Circuits, 38, (3), pp. 569 – 572, 2003.

[5] Gurkaynak, F.K., and Burg, A. et al.: 'A 2 Gbit/s balanced AES crypto-chip implementation'. Proc. Great Lakes Symp. on VLSI 2004, pp. 39 – 44, 2004.

[6] H. Li "Efficient and flexible architecture for AES"IEE proc. on circuits, devices, and Systems, vol. 153, no. 6, 2006.

[7] A. Alma'aitah and Zine-Eddine Abid, "Area Efficient-High Throughput Sub-Pipelined Design of the AES in CMOS 180nm", proceeding of International Design and Test Workshop (IDT'10), pp. 31-36, Dec. 2010.

[8] 이훈재, 도경훈, "워드기반 스트림암호의 병렬화 고속 구현 방안", 한국해양정보통신학회, 제14권, 제4호, pp.859-867, 2010.

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

[10] ECRYPT, eSTREAM site at http://www.ecrpt.eu.org/stream/.

[11] 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

김봉근(BongGeun KIM)

2006년 동서대학교 컴퓨터정보공학과 졸업(학사)
2009년 동서대학교 유비쿼터스IT학과(석사수료)

2009년~현재 KT SD본부 프로젝트PL
※관심분야 : IDC, SAN 보안, 전송

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