PC 주변기기에 대한 보안성을 위한 Twofish 암호알고리즘 설계에 관한 연구

정우열* · 이선근**

A study on Twofish Cryptoalgorithm Design for Security in the PC Peripheral devices

Woo-yeol Jeong* · Seon-keun Lee**

요 약

초기 보안시스템 대부분은 PCI 방식으로서 미숙한 사용자들의 PC 사용에 부적합하다. 특히 사용되어지는 보안 프로그램들은 대부분 크랙에 대하여 검증되지 않았으며 해커나 바이러스 등의 공격에 대하여 노출되어지고 있다.

그러므로 본 논문은 사용자들이 쉽게 사용할 수 있고 범용 컴퓨터에서 사용될 수 있는 USB를 사용하는 Twofish 암호알고리즘을 설계하였다. 사용자들은 USB를 사용하여 보안 시스템을 쉽게 사용하게 된다. 또한 다양한 가변키 길이를 가지는 Twofish 암호알고리즘은 다양한 보안시스템에 적용이 가능하게 된다. 이러한 Twofish 암호알고리즘은 암호화와 복호화에 대한 성능을 향상시킬 수 있으며 하드웨어의 크기를 감소시키는 효과를 가지게 된다.

ABSTRACT

The previous security system was PCI way which has many difficulties for PC novices to use. Moreover the security programs in use are mostly unverified ones as they are using cracks, and are exposed to attacks such as hackers and viruses.

Therefore this thesis describes to design the security system of Twofish cryptographic algorithm using USB, which it can be used in general-purpose computers and users can handle it with ease. Users can easily use the security system by using this USB and it is applicable to various security systems that Twofish cryptographic algorithm used in the security system by having variable key length. Also the efficiency of the system can be enhanced as it can perform both encryption and decryption and it has a benefit of downsizing hardware.

키워드

Security System, PCI Way, Twofish Cryptographic algorithm, Encryption and Decryption

Ⅰ. 서 론

현재 1가구당 각 1대의 PC를 사용하고 있으며, 외부의 침입과 바이러스 및 스파이웨어 등으로 인한 피해를 막기 위해 각종 보안 프로그램 등을 사용하여 사용자의 개인 정보 등이 저장되어있는 PC를 보호하고 있다. 그러나 인터넷의 비보안적 구성과 PC 사용자의 인터넷에 의한 정보 의존도 증가, 각종 해킹 툴의 확산으

* 한려대학교 멀티미디어 정보통신공학과
접수일자 : 2007. 04. 29
** 원광대학교 전기전자 및 정보공학부
심사완료일자 : 2007. 06. 03

로 인한 해킹 사고가 증가하고 있으며 보안성이 중요한 사무실에서는 사용자의 주기적인 시스템 Format, 그리고 각종 바이러스 등으로 인한 개인 및 기업의 중요한 정보 등에 대하여 피해를 받을 경우가 많다. 따라서 사용자들이 사용하는 PC에 보안시스템을 장착해야 하지만 보안시스템 대부분은 PC 내부에 장착할 수 있게 되어 있는 PCI 인터페이스 방식으로써 PC 사용에 미숙한 사용자에게는 부적합한 방식이라 할 수 있다. 그러므로 본 논문에서는 PC의 성공적인 인터페이스 기술이라고 할 수 있는 USB 인터페이스 기술을 이용하여 외부의 침입으로부터 막을 수 있는 Twofish 암호알고리즘의 보안시스템을 설계하고자 한다[1].

II. USB에 사용되는 통신방식들

USB 통신은 크게 디바이스 열거(enumeration)에 사용되는 통신과 Application이 디바이스 본래 목적을 수행하는데 사용하는 통신으로 나눌 수 있다. 이러한 통신에 있어서 전송방식은 4가지 방식으로 제어전송과 벌크전송 그리고 인터럽트전송, 등시성전송으로 나누어진다. 첫째, 제어전송은 호스트와 디바이스가 디바이스 기능에 관한 정보를 교환 할 때와 호스트가 디바이스 정보를 읽고 설정하는 데 사용된다. 구성은 셋업 스테이지, 데이터 스테이지, 상태 스테이지로 구성되며 각 스테이지는 토큰 페이즈, 데이터 페이즈, 핸드쉐이크 페이즈로 이루어진 1개 이상의 transaction으로 구성되어있다. 셋업 스테이지에서 호스트는 리퀘스트에 관한 정보를 보내서 셋업 transaction을 시작하고, 토큰 패킷은 자신을 제어 전송으로 인식하게 하는 PID를 포함하고 있다. 그리고 데이터 패킷은 리퀘스트 번호, 데이터 스테이지의 여부와 그에 따른 데이터 흐름방향등의 리퀘스트에 관한 정보를 가지고 있다. 상태 스테이지는 1개의 IN 또는 OUT transaction으로 구성되어있으며, 상태 스테이지에서 디바이스는 앞 스테이지의 성공 또는 실패에 대한 여부를 보고한다. 상태 스테이지의 데이터 패킷 소스는 데이터 스테이지에서 데이터를 받는 쪽이며, 데이터 스테이지가 없으면 디바이스는 상태 스테이지 데이터 패킷을 보내게 되는데 이때 상태 스테이지는 디바이스가 보내는 데이터나 핸드쉐이크 패킷은 리퀘스트의 성공 또는 실패를 나타내는 코드를 가지고 있다. 따라서 제어전송에서는 셋업 스테이지와 상태 스테이지는 필수이고 데이터 스테이지는 옵션이지만 특정 리퀘스트일 때는 필요하다. 이러한 모든 제어 전송은 양방향으로 정보를 전달하기 때문에 메시지 파이프는 동일한 IN/OUT의 Endpoint 주소가 사용된다[2].

둘째, 벌크 전송은 전송 타이밍이 중요하지 않은 데이터 전송에 유용하다. 즉, 다른 전송 방식에게 버스를 양보하고 사용할 수 있을 때까지 기다리기 때문에 버스의 다른 전송을 방해하지 않고 대량의 데이터를 보낼 수 있다. 구조는 1개 이상의 IN 또는 OUT transaction으로 구성되며, 단방향전송을 갖는다. 만약 양방향전송 시에는 각 방향별로 버스를 추가하여 전송해야 한다.

셋째, 인터럽트전송은 데이터를 정해진 시간내에 전송해야 할 경우에 사용된다. 디바이스가 데이터를 보내면 바로 호스트에 하드웨어 인터럽트가 걸리며 호스트가 최소 지연으로 데이터를 요청하거나 전송하는 걸 보장해준다. 구소는 벌크와 비슷하며, 단방향성을 갖는다.

마지막으로 등시성전송은 가끔씩 발생하는 에러를 허용할 수 있으며 데이터가 일정한 속도나 지정된 시간에 도착해야만 의미가 있는 스트리밍, 실시간 전송에 적합하다. 인터럽트 전송에 비해 매 frame당 더 많은 데이터를 전송할 수 있지만 받은 데이터에 에러가 있어도 다시 전송할 수 있는 준비는 되어있지 않은 단점이 있다. 등시성전송의 구조는 1개 이상의 프레임이 일정한 간격으로 각 프레임마다 1개의 IN/OUT transaction으로 구성되어 있다. 등시성전송도 인터럽트전송과 벌크전송과 같이 단방향성이며, 양방향 데이터전송 시에는 각 방향별로 별도의 파이프가 필요하다.

호스트는 열거한 후 제어 전송을 사용해 디바이스에 관한 정보를 갖는 디스크립터를 요청하게 되며, 열거 상태인 동안 전체 디바이스, 컨피규레이션, 인터페이스, Endpoint 순으로 점점 더 작은 구성요소에 대해 디스크립터를 요청한다. 상위레벨 디스크립터는 호스트에게 추가적인 하위레벨 디스크립터에 대한 정보를 알려주며, 각 디바이스에서 디바이스 전체에 대한 정보를 가지고 있는 디스크립터는 하나만 존재함으로써 지원하는 컨피규레이션에 대한

개수를 알 수 있다. 그리고 각 디바이스는 컨피규레이션이 지원하는 인터페이스의 개수와 전원 사용에 관한 정보를 포함하는 1개 이상의 컨피규레이션 디스크립터를 가진다. 컨피규레이션의 각 인터페이스 디스크립터는 Endpoint와 통신하는데 필요한 정보를 포함하는 Endpoint 디스크립터 개수를 가지고 있으며, 각 Endpoint 디스크립터는 Endpoint가 데이터를 전송하는 방법에 대한 정보를 가지고 있다. 또한 Endpoint 디스크립터가 없는 인터페이스는 제어 Endpoint를 사용해야 한다[3].

III. USB에 적용하기 위한 Twofish 보안시스템 설계

외부로부터 침입을 막기 위해 Twofish 암호알고리즘을 적용한 암호시스템의 설계는 범용 PC와 인터페이스 할 수 있게 USB방식을 갖는다. 그리고 사용자들의 범용 PC는 상시 Network에 접속되어 있어서 외부로부터의 침입 및 공격을 받을 가능성이 있기 때문에 Twofish 암호알고리즘을 갖는 암호시스템이 범용 PC와 USB 인터페이스 방식을 이용하여 언제, 어디서나 사용자가 사용하는 PC에 꽂아 PC와 개인의 자료를 외부로부터 보호할 수 있게 시스템을 구성하였다. 그림 1은 USB를 이용한 Twofish 암호알고리즘을 갖는 보안시스템의 전체 구성도이다.

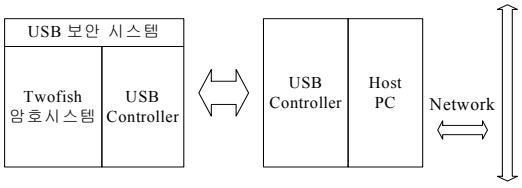

그림 1. 시스템 구성도
Fig. 1 System block diagram

Twofish 암호알고리즘은 AES의 다섯 후보 알고리즘 중 하나로 미국의 Minneapolis 연구 그룹에 의해 개발되어진 것으로 암호학적인 구조를 이용하여 암호화를 수행하는 블록 암호알고리즘이다. 이러한 Twofish 암호알고리즘의 암호화 과정은 그림 2와 같이 128비트 평문을 little-endian convention을 사용하여 4개의 32비트워드로 분류하여 각각의 워드에 32비트 부분키(subkey) 4개와 Exclusive OR 되어 입력 whitening과정을 수행한다. 그리고 각 라운드에서 좌측 2개의 워드가 F함수 내부에 있는 두 g함수의 입력으로 사용되고 이때 1개의 입력 워드는 8비트 좌측 순환을 거쳐 입력된다. 또한 g함수는 4개의 8-by-8 비트 키 값에 종속된 S-box들과 MDS 행렬 곱셈기로 구성되며 그 출력은 PHT를 이용하여 결합되고, 2개의 부분키가 32비트 modulo-2 덧셈에 의해 한 라운드 함수를 완료하게 된다[4].

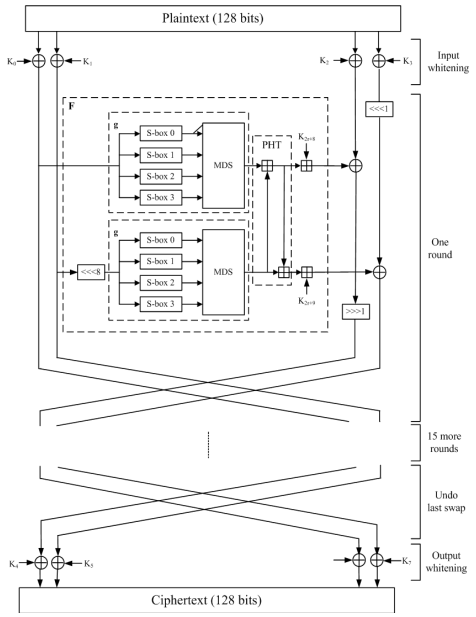

그림 2. Twofish 암호 알고리즘
Fig. 2 Twofish crypto algorithm

그리고 라운드 함수의 32 비트 두 워드 출력은 우측 2개의 워드와 비트 단위의 Exclusive-OR 및 1 비트 순환되며, 좌측 2개의 워드와 라운드 함수의 출력과 Exclusive-OR된 우측의 두 워드는 다음 라운드 입력으로 사용되기 위하여 자리바꿈함으로써 1회의 라운드를 완료하게 된다. 이와 같은 라운드를 동일하게 16회 반복하게 되며 마지막 라운드의 결과가 다시 자리바꿈되고, 4개의 32비트 부분키와 비트 단위로 Exclusive-OR되는 출력 whitening을 거쳐 128 비트 평문에 적용한 little-endian convention과 같은 방법으로 128비트의 암호문을 생성한다. 복호화 과정은 암호화 과정에서 적용한 40개의 부분키의 순서 및 F함수의

출력이 우측 2개의 워드와 Exclusive-OR 및 한 비트 되는 과정을 역으로 수행하게 되면 복호화가 이루어지게 된다.

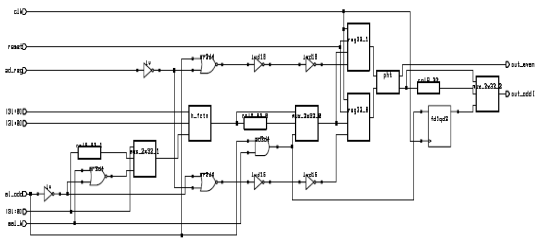

그림 3. 변형된 단일 F함수
Fig. 3 Modified single F function

그림 3은 단일 라운드에서 MDS-M2 블록을 이식하기 위하여 변형된 F함수로써 간략화 된 MDS-M2 블록으로 데이터를 보내기 위하여 h, g 함수의 q0, q1에 M0, M1, M2, M3와 S함수 값들을 재정리할 수 있는 회로이다.

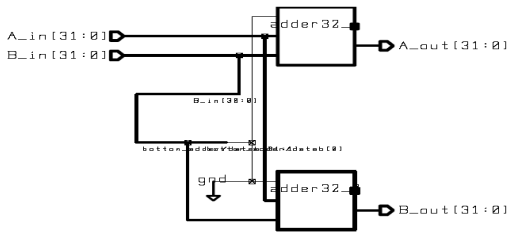

그림 4. PHT 변환 블록
Fig. 4 PHT conversion block

그림 4는 F함수에서 h 및 g함수의 데이터들을 혼합하여 하나의 데이터로 만들어주는 PHT 변환 블록이다. PHT는 h 및 g함수를 하나의 함수로 합하는 기능을 수행하기 때문에 두 개의 데이터들이 혼합되어 섞이면 원래의 데이터들을 복원할 수 없게 되므로 PHT의 의사 직교 기능을 이용하여 혼합하게 된다.

그림 5는 h 및 g함수 안에서 데이터들을 비선형 함수로 처리하는 S-box를 나타낸 그림이다. 비선형 함수는 예측하기 어렵기 때문에 보안시스템의 주요한 블록이라 할 수 있으며, 이러한 S-box는 기본연산이 순열이다.

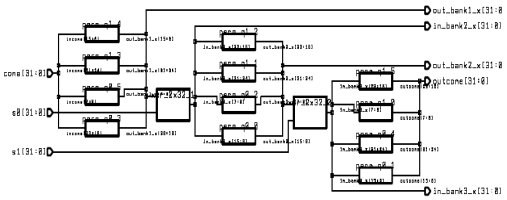

그림 5. S-box 블록
Fig. 5 S-box block

그림 6은 보안시스템에 사용되는 암호키를 생성하는 키 스케줄러 블록으로써 생성된 키들은 각각의 라운드에 별도의 데이터들을 제공한다.

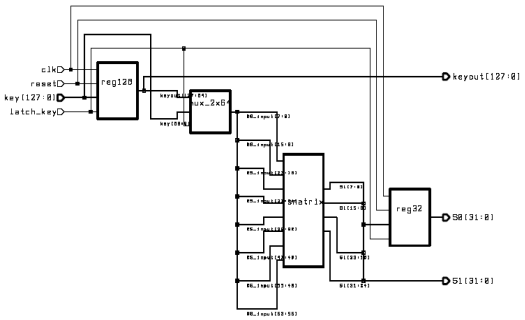

그림 6. 키 스케줄러 블록
Fig. 6 Key scheduler block

그림 7은 Twofish 암호알고리즘을 이용한 보안시스템의 MDS-M2 블록이다. 곱셈 연산으로 인한 병목현상을 줄이기 위하여 곱셈 연산에 사용되는 함수들을 줄이고 공통된 함수들은 index화하여 전체 곱셈 연산을 modulo-2연산이 가능하다.

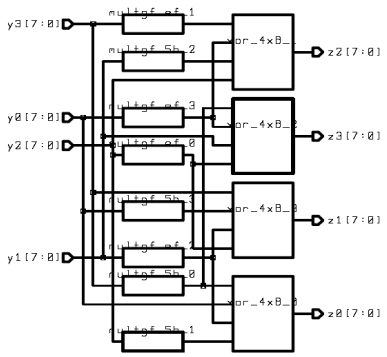

그림 7. MDS-M2 블록
Fig. 7 MDS-M2 block

그림 8은 MDS-M2를 사용한 보안시스템의 암/복호화를 조절할 수 있는 제어블록이다. Twofish 암호알고리즘은 암/복호화가 동시에 가능하기 때문에 USB의 제어전송방식을 사용하여 보안시스템을 구성하였다.

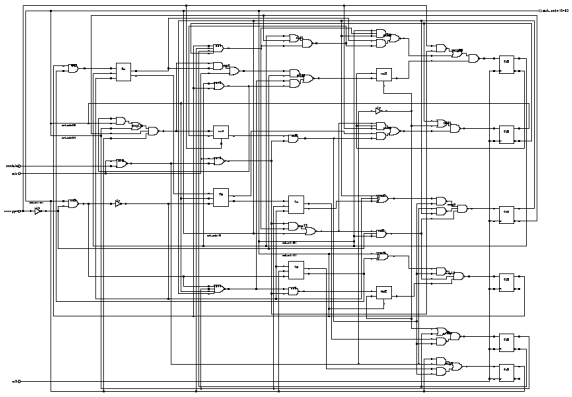

그림 8. 암/복호화 제어부

Fig. 8 Encoding/Decoding control block

그림 9는 USB 적용이 가능한 보안시스템의 전체 블록도이다. 128 비트의 입력과 키 정보를 이용하여 128비트의 출력을 산출함으로써 1:1:1의 대응관계를 갖으며, 암/복호화가 동시에 가능한 장점을 가진다.

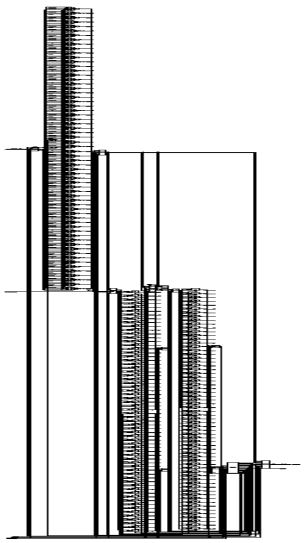

그림 9. 보안시스템의 전체 블록

Fig. 9 System block of security system

Ⅳ. 결 론

본 논문은 PC 사용에 미숙한 사용자 및 보다 안전한 정보를 유지하기 위해 USB를 이용함으로써 외부의 공격으로부터 정보를 보호할 수 있는 Twofish 암호알고리즘의 보안시스템을 설계하였다.

Twofish 암호알고리즘의 보안시스템을 설계하기 위해 VHDL코드로 작성하였으며, 사용된 CAD 툴은 synthesizing을 위하여 Synopsis Ver. 1999. 10을 사용하였고, 디바이스는 Cyclone EP1C6Q240C8을 타겟으로 하였다. 휴대하기 편하다는 장점을 가진 USB를 이용한 보안시스템은 사용자가 사용하는 PC에 꽂아 PC와 개인의 자료를 외부로부터 보호할 수 있을 것으로 사료된다.

참고 문헌

[1] 김윤구, 이기동, “USB(Universal Serial Bus)의 데이터 송수신 성능향상을 위한 적응성 통신방식”, 한국통신학회, Vol. 31, No. 10A, 2006.
[2] 강필중, “휴대용 멀티미디어 응용 서비스를 위한 변형된 Twofish 암호 시스템의 설계에 관한 연구”, 석사학위논문, 원광대학교, 2005.
[3] 김형훈 편저, “USB GUIDE”, Ohm사, 2002.
[4] Jan Axelson 저, 전준걸 역, USB완전정복, 에어콘, 2006.

저자 소개

정우열(Woo-yeol Jeong)

현재 : 한려대학교 멀티미디어 정보통신공학과교수

※ 주관심분야 : 이동통신시스템, 암호시스템, VLSI 설계

이선근(Seon-keun Lee)

현재 : 원광대학교 전기전자 및 정보공학부 전임강사

※ 주관심분야 : 이동통신시스템, 암호시스템, VLSI 설계