Rijndael 알고리즘을 이용한 물리 계층 ATM 셀 보안 기법

임 성 렬[†] · 정 기 동[††]

요 약

본 논문에서는 미국 NIST에서 차세대 암호화 알고리즘으로 채택한 Rijndeal 알고리즘을 적용한 물리 계층 ATM 셀 보안 기법에 관한 것이다. ATM 셀 보안 기법을 기술하기 위해 물리 계층에서의 데이터 암호화 시의 표준 ISO 9160을 만족하는 데이터 보안 장치를 하드웨어로 구현하여 STM-1급(155.52Mbps) 의 ATM 망에서 암호화/복호화 과정을 검증하였다. 기존의 DES 알고리즘이 블럭 및 키 길이가 64 비트이므로 대용량 데이터 처리가 어렵고 암호화 강도가 취약함에 비해, Rijndael 알고리즘은 블럭 크기가 128 비트이며 키 길이는 128, 192, 256 비트 중 선택 가능해 시스템에 적용 시 유연성을 높일 수 있고 고속 데이터 처리 시에 유리하다. 물리 계층 ATM 셀 데이터의 실시간 처리를 위해 Rijndael 알고리즘을 FPGA로 구현한 소자를 사용하여 직렬로 입력되는 UNI(User Network Interface) 셀을 순환 여유 검사 방법을 이용하여 셀의 경계를 판별하고 셀이 사용자 셀인 경우, 목적지의 주소값 등 제어 데이터를 지니고 있는 헤더 부분을 분리한 48 옥텟의 페이로드를 병렬로 변환, 16 옥텟(128 비트) 단위로 3 개의 암호화 모듈에 각각 전달하여 암호화 과정을 마친 후 버퍼에 저장해 둔 헤더를 첨가하여 셀로 재구성하여 전송하여 준다. 수신단에서 복호화 시에는 페이로드 종류를 판별하여, 사용자 셀인 경우에는 셀의 경계를 판별한 다음 페이로드를 128 비트 단위로 3 개의 암호화 모듈에 각각 전달하여 복호화하며, 유지 보수 셀인 경우에는 복호화 과정을 거치지 않는다. 본 논문에 적용한 Rijndael 암호화 소자는 변형된 암복호화 과정을 적용하여 제작된 소자로 기존에 발표된 소자에 비해 비슷한 성능을 지니면서 면적 대 성능비가 우수한 소자를 사용하였다.

키워드 : 차세대 암호표준, Rijndael, 데이터 보안, 암호화, 복호화, ATM 보안

ATM Cell Encipherment Method using Rijndael Algorithm in Physical Layer

Sung-Yeal Im[†] · Ki-Dong Chung[††]

ABSTRACT

This paper describes ATM cell encipherment method using Rijndael Algorithm adopted as an AES(Advanced Encryption Standard) by NIST in 2001. ISO 9160 describes the requirement of physical layer data processing in encryption/decryption. For the description of ATM cell encipherment method, we implemented ATM data encipherment equipment which satisfies the requirements of ISO 9160, and verified the encipherment/decipherment processing at ATM STM-1 rate(155.52Mbps). The DES algorithm can process data in the block size of 64 bits and its key length is 64 bits, but the Rijndael algorithm can process data in the block size of 128 bits and the key length of 128, 192, or 256 bits selectively. So it is more flexible in high bit rate data processing and stronger in encription strength than DES. For the real time encryption of high bit rate data stream, Rijndael algorithm was implemented in FPGA in this experiment. The boundary of serial UNI cell was detected by the CRC method, and in the case of user data cell the payload of 48 octets (384 bits) is converted in parallel and transferred to 3 Rijndael encipherment module in the block size of 128 bits individually. After completion of encryption, the header stored in buffer is attached to the enciphered payload and retransmitted in the format of cell. At the receiving end, the boundary of cell is detected by the CRC method and the payload type is decided. If the payload type is the user data cell, the payload of the cell is transferred to the 3-Rijndael decryption module in the block size of 128 bits for decryption of data. And in the case of maintenance cell, the payload is extracted without decryption processing.

Key Words : Advanced Encryption Standard(AES), Rijndael, Encryption, Decryption, ATM Security

1. 서 론

통신망을 통한 데이터의 교환이 급격히 증가하게 함에 따라 정보가 통신 도중에 제 삼자에게 유출되거나 불법적인 침입자로 인한 도청 및 변조에 대한 대책이 요구되고 있다. 데이터 보안 대책의 여러 가지 방법 중 데이터를 암호화하는 방법이 가장 안전한 데이터 보안 방법으로 사용되고 있다[1].

암호화 방식은 블럭 암호 알고리즘과 스트림 암호 알고리즘으로 구분되며 블럭 암호 알고리즘으로 현재까지 DES

† 정 회 원 : 우송대학교 철도전기, 정보통신학부 초빙교수
†† 종신회원 : 부산대학교 전자계산학과 교수
논문접수 : 2005년 9월 2일, 심사완료 : 2006년 1월 19일

(Data Encryption Standard)가 보편적으로 사용되어 왔다[2]. 그러나 최근 컴퓨터의 계산 능력 향상으로 인해 알고리즘의 안전성을 더 이상 보장받을 수 없게 되자[3] 미국 NIST(National Institute of Standards and Technology)에서 1997년 새로운 암호화 알고리즘인 AES(Advanced Encryption Standard)를 공모하여 2001년에 최종 채택하였다[4, 5]. 일반적으로 암호화 알고리즘 적용 시 소프트웨어 방식의 구현은 하드웨어로 구현한 방식에 비해 데이터 암호화 처리 속도가 느려서, 고속 데이터의 실시간 처리를 위해서는 암호 알고리즘의 하드웨어적인 구현이 필수적이다[6].

본 논문은 ATM 에서 셀 데이터 전송 시에 데이터를 물리 계층에서 실시간으로 암호화/복호화를 수행하는 ATM 셀 보안 기법에 관한 것이다. 현재 ATM 에서 암호화/복호화 구현한 방식은 블럭 길이가 64 비트 단위인 DES 알고리즘을 적용한 방식과 물리 계층의 상위 계층인 ATM 계층에서 DES를 적용하여 소프트웨어적으로 구현한 방식 등이 있다. 이러한 방식들은 암호화 전용 시스템 구축을 전제로 한 것 임에 반해, 본 논문에서 제안하는 방식은 시스템 운용 중에 필요한 가입자에게만 암호화/복호화 기능을 제공하는 방식이다.

ATM UNI셀 데이터의 실시간 암호화/복호화 처리를 위해 입력되는 셀을 순환 여유 검사 방법을 이용하여 셀의 경계를 판별한다. 셀이 사용자 셀인 경우, 헤더 부분을 분리한 48 옥텟의 페이로드를 병렬로 변환, 16 옥텟(128 비트) 단위로 3 개의 Rijndael 암호화 소자에 각각 전달하여 암호화 과정을 마친 후 버퍼에 저장해 둔 헤더를 첨가하여 셀로 재구성하여 전송하여 준다. 유지 보수 셀인 경우에는 암호화 과정을 거치지 않고 전송하여 준다.

본 논문에서는 155.52 Mbps 속도를 지니는 STM-1급 ATM 망의 UNI(User Network Interface) 규격의 셀 단위의 암호화/복호화를 위해 ISO 9160을 만족하는 물리 계층 ATM 데이터 보안 장치를 구현하여 실험을 통해 암호화/복호화 과정을 검증하였다.

본 논문의 구성으로는 제2장에 ATM 망에서의 암호화 구현 사례를 살펴보고 제3장에 Rijndeal 알고리즘을 소개하고, 제4장에서는 ATM 망 및 셀의 구조에 대해 살펴보고, 제5장에서 ATM 셀 보안 기법에 대해 설명하며 제6장에서 결론을 맺는다.

2. ATM 망에서의 암호화 구현 사례

이 장에서는 ATM 망에서의 기존의 암호화 구현 사례들에 대하여 살펴 본다. ATM 물리 계층에서 암호화/복호화 과정을 구현한 사례는 DES 알고리즘을 적용한 논문이 있으며, 시스템 설계 시에 암호화 구현을 전제한 방식이다[7]. 또 다른 방식은 물리 계층의 상위 계층인 ATM 계층에서 소프트웨어적인 암호화를 수행하는 방식으로, 이 역시 암호화 전용 시스템 구축을 전제로 한 것이다[8]. 이러한 구현 방안은 암호화 전용 시스템 설계 시에는 적합하나 시스템 구축에 소요되는 비용이 상용 시스템 구현에 비해 많이 소요되며, 시스템 구현 시 복잡도가 증가하게 되며, 시스템 유연성 측면에서도 문제점이 있다. 한편 DES 알고리즘은 최근 컴퓨터의 계산 능력의 향상으로 인해 더 이상 알고리즘의 안전을 보장받을 수 없는 문제점이 도출되어 있다[9]. 본 논문에서는 상용 시스템의 운용 중 암호화/복호화를 필요로 하는 가입자에게만 기능을 제공해 주어야 하는 경우에 별도의 부가 장치로 구성하여 유연하게 대처할 수 있는 ATM 셀 보안 기법을 제안하며, 암호화 알고리즘으로 블럭 길이를 128 비트, 키 길이를 128 비트로 한 Rijndael 알고리즘을 채택하였다.

본 논문에 적용한 Rijndael 알고리즘은 암호화 블럭 길이를 128 비트 단위로 처리하므로 동일 길이의 메시지를 암호화하는 데 DES 에 비해 적은 수의 암호화 소자로 구성할 수가 있으며, DES 와 달리 현재로는 해독이 불가능한 알고리즘이다. 또 다른 방식인 ATM 계층에서 DES 를 소프트웨어적으로 구현한 방식에 비해 본 논문의 방식은 하드웨어 구현 방식이므로 데이터 처리 속도가 현저히 빠르다..

본 논문에서는 Rijndael 알고리즘을 FPGA로 구현한 암호화 소자를 사용하여[10] 물리 계층에서 ATM 셀을 실시간으로 처리할 수 있도록 구성하였으며, 128 비트 단위로 실시간 암호화/복호화가 가능하도록 구성하였다. 또한 직렬 데이터 형태로 입력되는 ATM 셀에서 페이로드 부분만 분리하여 암호화하기 위해 셀 경계를 판별하기 위한 순환 여유 검사 회로를 기존의 방식과는 다른 보상 다항식 방식을 고안하여 판별 논리의 단순화를 기하였으며 설계 회로 게이트 수를 줄였다.

3. Rijndael 암호화 알고리즘

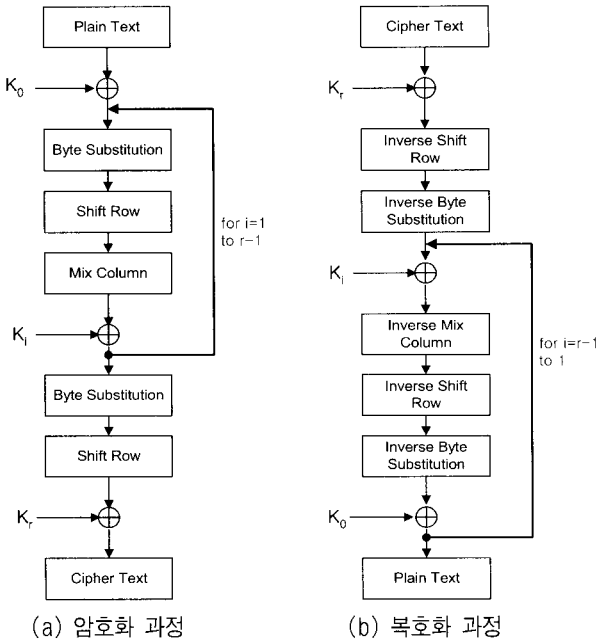
Rijndael 암호 알고리즘은 대칭키 블럭 암호 알고리즘으로서 암호화/복호화의 기본 단위인 블럭의 길이를 128 비트로 하며 키 길이를 128, 192, 256 비트 중에서 선택할 수 있는 알고리즘으로 알려진 공격에 강하고[11], 하드웨어로 구현 시에 비교적 적은 수의 RAM이나 ROM으로 구현이 가능하며, 다양한 키 길이를 지원한다. Rijndael 암호 알고리즘은 블럭의 크기에 따라 총 라운드 수를 달리하는 데 블럭 길이를 128 비트로 가정하면, 키 길이에 따라 라운드 수가 결정된다[12]. 각 라운드는 바이트 치환, 행의 쉬프트, 열의 혼합으로 구성된 3 개의 독립된 단계를 갖는다. 한 워드를 32 비트로 하고 블럭의 워드 수를 N_b, 키의 워드 수를 N_k 라 하고, 암호화 알고리즘의 라운드 수를 N_r 이라 하면, 블럭 길이 N_b, 키 길이 N_k에 따른 라운드 수 N_r 관계는 <표 1>과 같다.

본 논문에서는 블럭의 길이가 128 비트, 키의 길이가 128 비트이므로 암호화/복호화 과정은 총 10 라운드로 구성된다. (그림 1)은 Rijndael의 암호화/복호화 알고리즘의 기본 구조를 나타낸다. 각 과정의 중간 결과 값은 4 개의 행과 N_b수의 열을 가지는 2차 배열로 구성되며 각 요소의 값은 1 바

이트 길이의 2진 코드이다. 암호 키도 같은 배열을 가지며 키 확장 알고리즘으로 생성한 키 값을 워드 단위로 한 N_k 수의 열을 지닌다.

〈표 1〉 키 길이에 따른 라운드 수(N_r)

Nr	Block Length (N_b Words)	Key Length (N_k Words)	Number of Rounds(N_r)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14



(a) 암호화 과정 (b) 복호화 과정

(그림 1) Rijndael 알고리즘 구조

각 라운드 별 자세한 데이타 처리 방법은 [4]를 참고하며, 여기서는 간략히 설명한다.

SubBytes 변환은 16 x 16 행렬로 구성된 S-box 를 통한 치환 변환이며, 행렬의 각 구성 요소는 1 바이트의 2진 코드를 헥사로 표현한 값이다. 복호화 시에는 역변환 S-box가 사용된다.

ShiftRow 변환에서는 state의 행들을 왼쪽으로 순환 쉬프트하여 새로운 행을 구성하는 데, 행의 위치에 따라 쉬프트 오프셋 값을 달리하여 쉬프트 시켜준다. 첫째 행은 그대로 두고, 나머지 행들은 각각 C_1, C_2, C_3의 값만큼 순환 쉬프트 시켜준다. C_1, C_2, C_3는 N_b에 의해 다른 값을 가진다. <표 2>는 블럭의 길이 N_b값에 따른 C_1, C_2, C_3 값을 보여 준다. 본 논문의 실험에서는 N_b 값이 4이므로 C_1, C_2, C_3 값은 각각 1, 2, 3 이 된다.

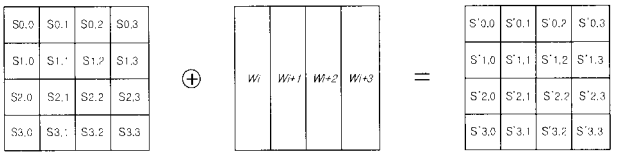
〈표 2〉 블럭의 길이에 따른 쉬프트 오프셋 값

N_b	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

MixColumms 변환은 S 행렬의 열의 4개의 구성 요소 값을 변수로 하여 새로운 행렬 S'의 요소 값으로 변환하는 데, 다음의 매트릭스 연산 과정을 거친다.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} = \begin{bmatrix} S'_{00} & S'_{01} & S'_{02} & S'_{03} \\ S'_{10} & S'_{11} & S'_{12} & S'_{13} \\ S'_{20} & S'_{21} & S'_{22} & S'_{23} \\ S'_{30} & S'_{31} & S'_{32} & S'_{33} \end{bmatrix}$$

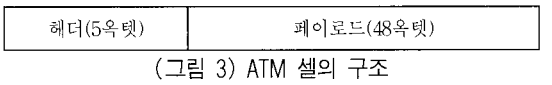
AddRoundKey 변환에서는 라운드 키와 state 들이 단순 bitwise XOR 하며 라운드 키는 키 스케줄에 의하여 암호 키로부터 유도 된다. 라운드 키 K_j 는 키 스케줄에 의하여 암호 키로부터 계산된다. 키 스케줄은 키 확장과 라운드 키 선택 두 부분으로 이루어져 있으며 라운드 키의 총 수는 N_r+1과 같다. (그림 2)에 AddRoundKey 변환을 도시하였다.



(그림 2) AddRoundKey 변환

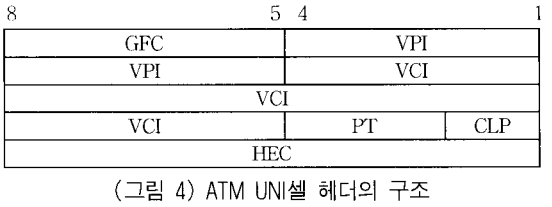
4. ATM 셀의 구조

ATM 망에서는 모든 데이터를 셀(cell)이라고 하는 고정된 크기의 패킷 단위로 전송하는 데 다음 (그림 3)과 같이 5 옥텟(octet)의 헤더와 48 옥텟의 페이로드로 구성된 셀로 전송된다[13].



(그림 3) ATM 셀의 구조

셀 헤더에는 셀과 관련된 제어 정보들이 들어가게 된다. 다음 (그림 4)는 UNI 인 경우에 헤더 필드 의미를 도시하였다[14].

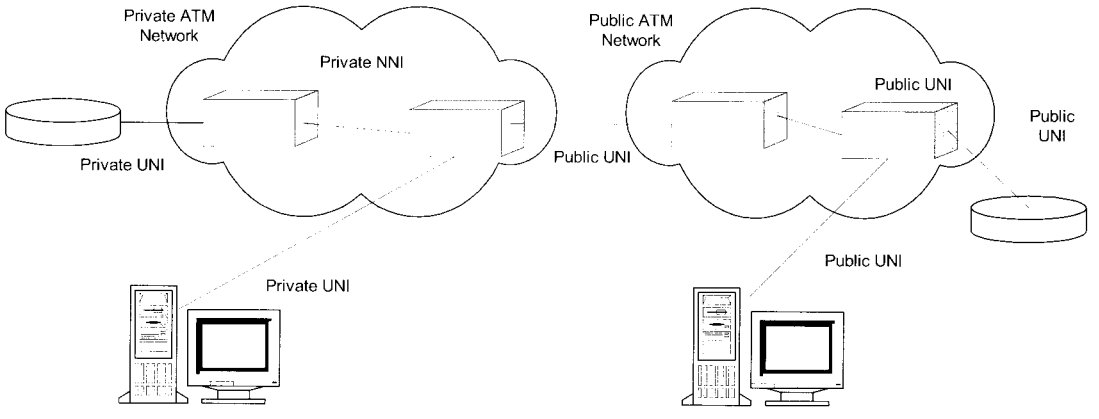


(그림 4) ATM UNI셀 헤더의 구조

필드의 의미 중 PT, CLP, HEC의 의미는 다음과 같다.

• PT(Payload Type)

페이로드의 내용이 사용자의 정보인지, 네트워크 제어를 위한 정보인 지를 구분하기 위하여 사용한다. 본 논문에서는 PT에 따라 암호화 여부를 결정하여 준다. 즉, PT 코드



(그림 5) ATM 망의 구조

가 000~011 인 사용자 데이터 셀인 경우에만 페이로드 데이터를 암호화하여 준다. <표 3>은 PT 코드에 따른 페이로드 종류를 분류한 것이다. 키 분배 시에 보류된 PT 코드 111 을 이용하여 암호화 소자에 사용되는 비밀키 값을 유지보수 셀로 전송하여 준다.

〈표 3〉 PT 코드에 따른 페이로드 종류

PT 코드	페이로드 종류
000	사용자 데이터 셀
001	사용자 데이터 셀
010	사용자 데이터 셀
011	사용자 데이터 셀
100	유지보수 셀
101	유지보수 셀
110	자원관리 셀
111	보류

• CLP(Cell Loss Priority)

CLP는 셀이 손실될 우선 순위를 표시하는 데 이용되고 이 정보는 네트워크의 서비스 품질(QoS)을 보장하기 위한 용도로 사용된다. CLP=0 은 셀이 우선 순위가 높음을 의미하고, CLP가 1 로 셋 되어 있으면 셀이 하위 순위임을 의미한다. 폭주 구간에서 CLP가 1인 셀은 원활한 트래픽을 위하여 폐기될 수도 있다.

• HEC(Header Error Control)

셀 헤더 부분의 오류 방지를 위한 목적으로 사용되며 순환 여유 검사 방법을 사용하며 생성다항식 $g(x)=x^8+x^2+x+1$ 로 하여 헤더 부분에 적용하여 그 값을 HEC 에 넣어준다 [15].

5. ATM 셀 보안 기법

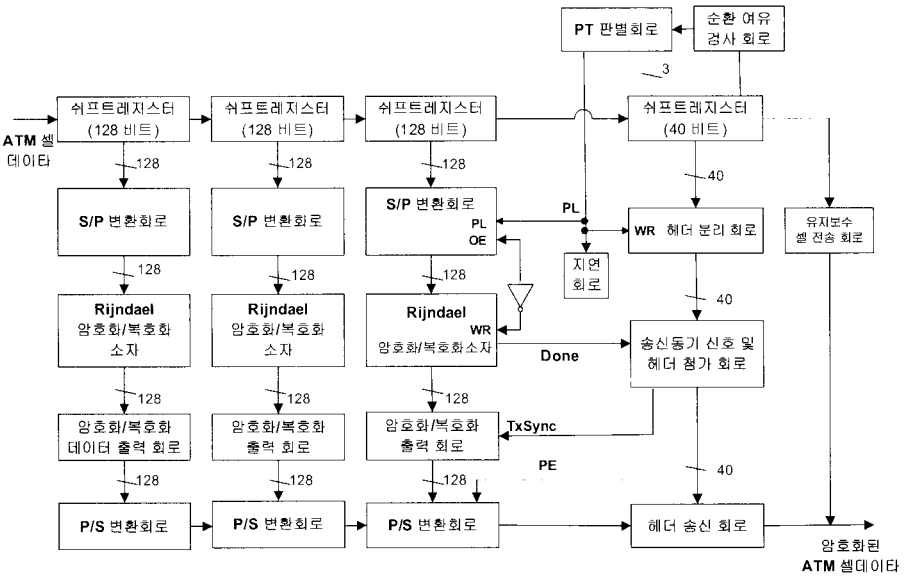
5.1 개요

ISO 9160에서는 물리 계층 데이터 처리 시의 기준을 규정하고 있는 데, ATM 데이터를 암호화하여 보낼 시에는 데이터 자체를 암호화하여 보낼 수도 있으나, 데이터 단말 장치(Data Terminal Equipment)에서는 일반 데이터 형태로 전송하고 특별히 암호화된 데이터 전송을 필요로 하는 경우에 한하여 데이터 보안 장치(Data Encipherment Equipment)를 별도의 부가 장치로 구성할 수 있음을 명시하고 있다[16]. ATM 인터페이스는 가입자 단말과 망간에 적용되는 UNI (User Network Interface) 와 망간에 적용되는 인터페이스인 NNI(Network Network Interface)로 구분할 수가 있는데 두 인터페이스가 큰 차이는 없으나 셀의 헤더의 필드 부분을 약간 달리한다[17]. 본 논문에서는 물리 계층의 ATM 셀 보안 기법을 적용한 ATM 데이터 보안 장치를 구성하여 UNI 에 적용하여 실험하였다. (그림 5)에 ATM 망의 개념도를 도시하였다. 데이터 보안 장치 구성 시에 송신측 ATM 셀의 데이터에서 헤더 부분은 목적지의 주소값 등을 포함하고 있으므로 헤더 부분은 제외한 페이로드의 데이터만을 암호화하여 출력되는 데이터에 헤더를 첨가하여 전송해 주어야 한다. 본 논문에서는 STM-1 급 속도(155.52Mbps)의 데이터를 실시간 암호화 처리가 가능하게 구성하였다. 셀 손실 시에는 일반적인 ATM 망의 제어 절차를 따른다.

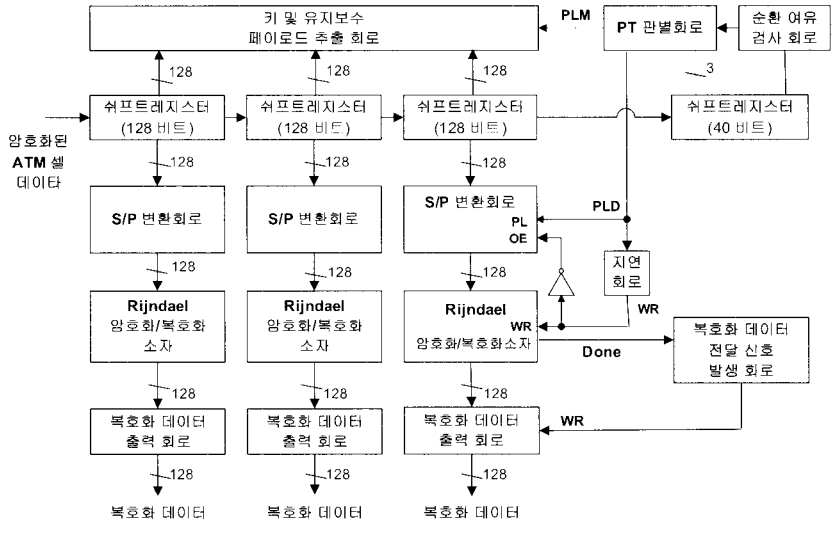
5.2 ATM 데이터 보안 장치 구성도

ATM 데이터 보안 장치의 송신측 블럭도를 (그림 6)에 도시하였다. 송신측 데이터 보안 장치에서 수행하는 기능은 다음과 같다.

- 48 옥텟의 ATM 페이로드를 동시에 처리하기 위해, 3개의 암호화 모듈로 구성
- 48 옥텟의 페이로드를 16 옥텟 단위로 각각의 암호화 모듈에 인가 기능
- 순환 여유 검사 기능(Cyclic Redundancy Check)을 이용한 셀 경계 판별 기능
- 셀 데이터의 페이로드 타입 판별 기능
- 155.520 Mbps 의 비동기 직렬 입력 데이타를 384 비트의 병렬 데이터로 변환 기능
- 384 비트의 페이로드를 128 비트 단위로 3개의 Rijndael 암호화 회로 입력단에 입력



(그림 6) ATM 데이터 보안 장치 송신측 블럭도



(그림 7) ATM 데이터 보안 장치 수신측 블럭도

- 셀 헤더 버퍼 저장 기능
- 암호화된 페이로드를 ATM 셀로 재구성하여 전송
- 유지 보수 셀 전송 기능

수신측 블럭도를 (그림 7)에 도시하였다. 수신측 데이터 보안 장치에서 수행하는 기능은 다음과 같다.

- 48 옥텟의 페이로드를 16 옥텟 단위로 각각의 복호화 모듈에 인가 기능
- 순환 여유 검사 기능(Cyclic Redundancy Check)을 이용한 셀 경계 판별 기능
- 유지 보수 페이로드 및 사용자 페이로드 판별 기능

Rijndael 알고리즘은 블럭 길이 128 비트, 키 길이를 128 비트로 구성할 시에 암호화 출력 데이터가 나오기까지 10 라운드를 거치게 된다. (그림 6)의 송신 측 블럭도에서 주요 블럭의 동작 원리를 설명하면 다음과 같다.

5.2.1 Rijndael 암호화 소자

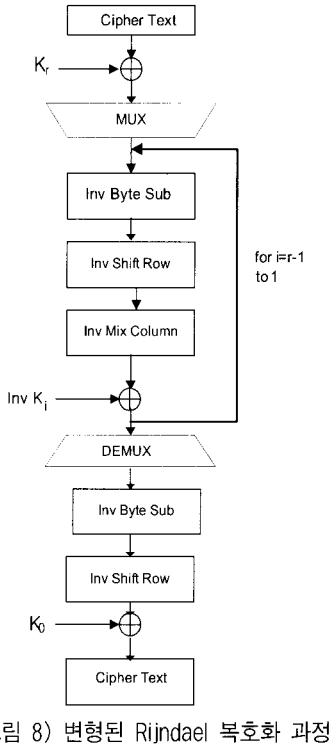
본 논문에 적용한 Rijndael 암호화 소자는 128 비트의 블럭과 128 비트의 키 길이를 지원하며 암호화/복호화 기능을 제공한다. 기존의 구현이 암호화만 제공하거나, 필요한 하드웨어 면적은 작지만 성능이 떨어지거나, 파이프 라인 구조를 사용하여 feedback 모드에서는 사용하지 못하는 단점이 있다. 본 논문에 적용된 소자는 기존의 구현 사례와 비슷한 성능을 지니면서 면적을 최소화하는 방식으로 제작되었다.

먼저 Rijndael 알고리즘에서 복호화를 수행할 경우 (그림 1) (b)와 같이 한 라운드에서 뿐만 아니라 전체적으로 암호화를 수행할 때와 반대가 된다. 그러나 대수적인 특성을 이용하면 다음과 같이 구조의 변형이 가능하다. 먼저 InvShiftRow

는 단순히 바이트 단위로 자리만 이동하므로 바이트의 값에는 아무런 변화가 없으며, InvByteSub는 바이트 단위로 독립적으로 수행되므로 두 부분의 순서를 바꾸어도 상관이 없다. 또한 AddRoundKey와 InvRoundKey의 순서를 변환할 수 있다. 이는 InvMixColumn이 선형 변환이므로 식 (3)의 특성에 따라 가능하다.

$$A(x+k)=A(x)+A(k) \quad (3)$$

대신에 AddRoundKey와 InvMixColumn의 순서를 바꾸기 위해서는 InvMixColumn이 포함되지 않은 Initial Round Key Addition과 Final Round의 AddRoundKey 에서 사용하는 첫 번째와 마지막의 라운드 키를 제외한 모든 라운드 키를 InvMixColumn으로 변형하여 사용해야 한다. 위의 두 가지 특성을 이용하여 순서가 변형된 복호화 과정은 (그림 8)과 같으며, 암호화 과정과 순서가 같아지게 된다. 본 논문에 적용한 암호화/복호화 소자는 이런 성질을 이용하여 암호화 과정만 구현하여, 외부 선택 신호에 따라 복호화 처리도 가능하게 하여 설계 게이트 수와 면적을 최소화하였으며, 암호화 소자 혹은 복호화 소자로의 선택이 가능하도록 구성하였다.



(그림 8) 변형된 Rijndael 복호화 과정

<표 4>는 본 논문에 적용한 Rijndael 암호화 모듈 사양이며, ALTERA FLEX 10KE200 디바이스를 타킷으로 합성되었다. 합성된 회로의 성능은 <표 5>와 같다. 적용된 Rijndael 암호화 소자는 34,816 비트의 메모리와 3,422 개의 로직 셀이 사용되었으며, 이는 각각 EPF10K200SRC240-1 디바이스의 메모리와 로직 셀의 35.34 % 에 해당된다. <표 6>은 128 비트의 블럭과 128 비트의 키 길이를 지원하며, 비슷한 성능을 지니며 암복호화를 모두 지원하는 [18]과 성능을 비교 분석한 표이다. <표 6>에서 알 수 있듯이 본 논문에 적용한 Rijndael 암호화 소자가 성능과 면적 측면에서 우수하다는 것을 알 수 있다.

〈표 4〉 Rijndael 암호화 모듈의 사양

소 자	EPF10K200SRC240-1
블럭 길이/키 길이	128/128
Round 수	10
성능	1.28 Gbits/sec
게이트 수	15,449.6 게이트
메모리	32K-bit ROM 1408-bit ROM
전체	44268.2 게이트

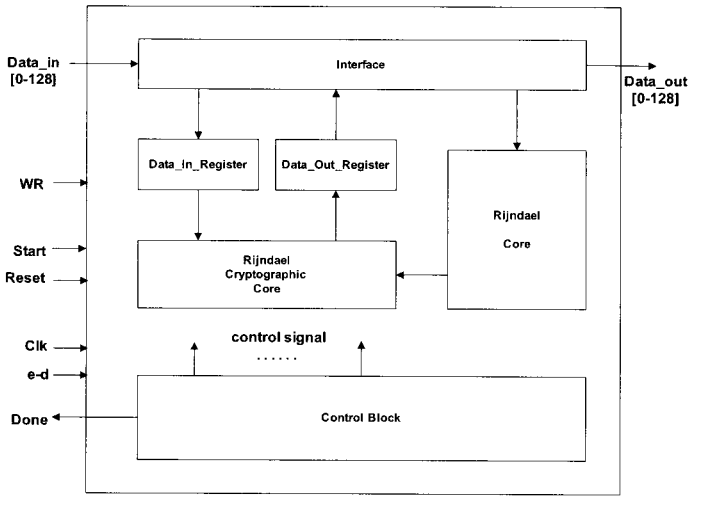
〈표 5〉 ALTERA FLEX 10KE200-1 에서 Rijndael 구현 결과

Device	EPF10K200SRC240-1
Memory bits	34816/98304(35%)
Logic Cells	3422/9984(34%)
Frequency(MHz)	29.49
Speed(Mbits/s)	343.26

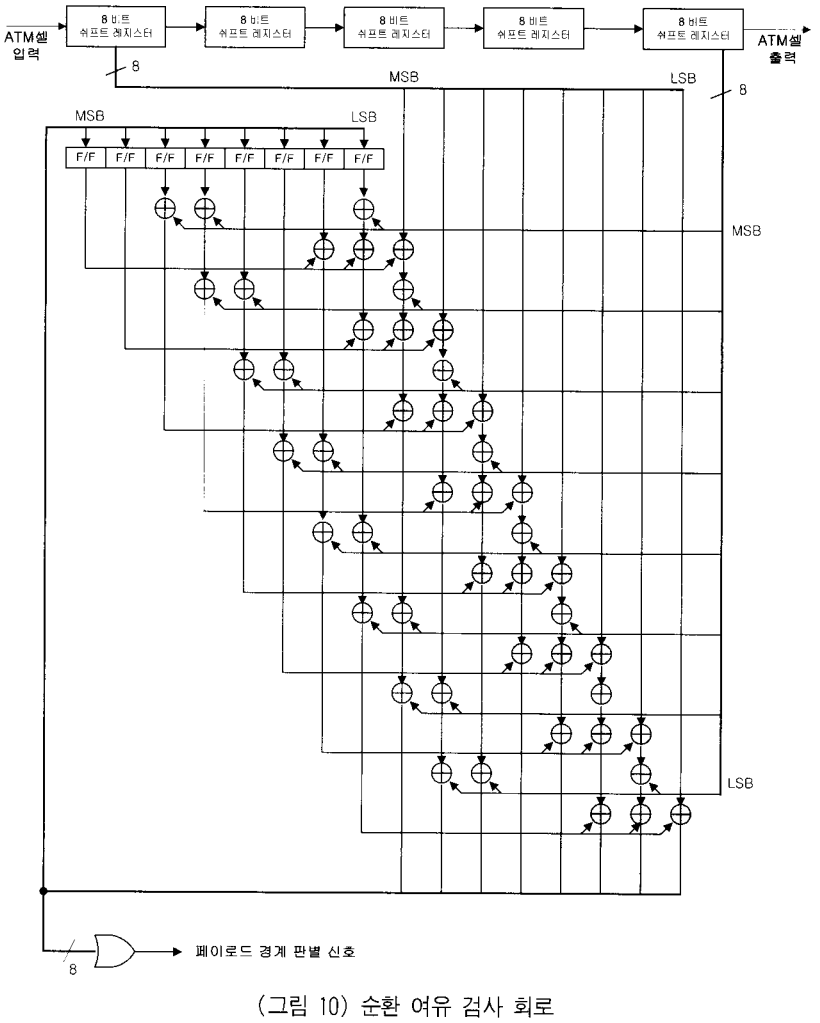
〈표 6〉 성능 비교

		Fischer[18]		본 논문에 적용한 소자
Block/Key length		128/128		128/128
No. of cycles				
Performance		1.45 Gbits/s (125MHz)	1.75 Gbits/s (150MHz)	1.28 Gbits/s (110MHz)
Area	Random Logic	13,788.8 gates	9,520.8 gates	15,449.6 gates
	Memory	64K-bits ROM 1408-bit RAM	256K-bit ROM 1408-bit RAM	32K-bit ROM 1408-bit RAM
	Total	63,629.5 gates	114,115.7 gates	44,268.2 gates
AT-product		1.26	1.89	1

Rijndael 암호화/복호화 소자의 전체 구조는 (그림 9)와 같다[10]. Rijndael 암복호화 소자는 입출력 데이터의 전송을 관리하는 인터페이스, 입출력 데이터를 저장하는 Data In/Out Register, 데이터 암복호화 연산을 수행하는 Rijndael Cryptographic Core, 외부의 키 생성부에서 생성한 라운드 키를 저장하는 RAM과 변형된 복호화 과정에 따른 InvMix Column으로 이루어진 Rijndael Core, 데이터를 암복호화하는 데 필요한 제어 신호를 발생하는 Control Block으로 이루어져 있다. 임의의 데이터를 암복호화할 경우, 먼저 데이터 버스를 통해 암호화할 데이터와 라운드 키를 입력하여 각각 Data_In_Register와 Rijndael RoundKey Core에 저장한다. 그리고 Start 신호가 발생하면 Rijndael Cryptographic core에서 암복호화 연산이 수행되며, 암복호화 연산이 수행되는 동안 Done 신호는 '1' 상태가 된다. Done 신호는 암복호화 연산이 수행 중임을 알려주는 신호로, 암복호화 연산이 끝나면 '0' 상태로 된다. e-d신호는 암호화/복호화 설정



(그림 9) Rijndael 암복호화 소자의 구조



(그림 10) 순환 여유 검사 회로

신호이며 소자를 암호화 소자로 사용할 지 복호화 소자로 사용할 지를 설정하는 단자이다.

로직 '1' 로 설정하면 소자가 암호화 과정을 로직 '0' 으로 설정하면 소자가 복호화 과정을 수행한다. 연산이 끝나면 암복호화된 데이터는 Data_out_Register에 저장된 후, 데이터 버스를 통해 출력된다. 입력된 데이터가 128 비트이므로 암호화 과정의 전체 라운드 수가 10 라운드 구성되며, 암복호화 과정의 각 라운드를 처리하는 데 1 클럭 주기가 필요하므로 암복호화 과정을 마치고 출력 시 까지는 11 클럭을 거치게 된다. 입력되는 ATM 셀이 53 옥텟이므로 STM-1급

속도에서는 ATM 셀이 2.73 μsec 주기로 입력되게 된다. 그러므로 실시간 암호화 처리를 위해서는 암호화 소자의 한 state 처리에 소요되는 시간이 2.73 μsec 보다 작으면 실시간 암호화 처리가 가능하므로 암호화 소자의 동작 클럭 속도를 최적화하여 368 KHz로 구성하였다.

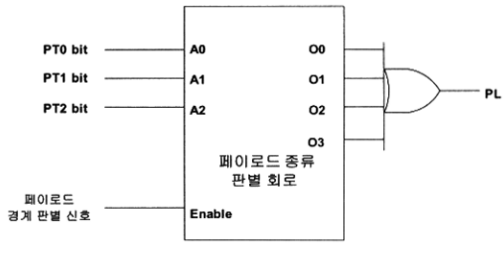
5.2.2 순환 여유 검사 회로(Cyclic Redundancy Check Circuit)

직렬로 입력되는 셀 데이터에서 셀의 경계를 파악하여, 페이로드 데이터를 분리하기 위해서는 보상 다항식 기법을 적용한 순환 여유 검사 방식을 구현하였다. 기존의 기법이 입력되는 헤더에 해당하는 5 바이트의 데이터에 대한 순환 여유 검사를 수행하여 셀 경계를 판별한 방식임에 반해, 본 기법은 최상위 바이트와 최하위 바이트의 데이터간의 보상 원리를 이용하여 경계를 판별함으로써, 설계의 단순화 및 필요 로직 게이트의 수를 줄였다. 페이로드 경계 판별 회로의 동작 원리는 다음과 같다. ATM 셀의 HEC 필드는 헤더를 생성 다항식 $g(x)=x^8+x^2+x+1$ 로 나누어 나머지가 0 이 되도록 값을 구성하여 전송하므로 순환 여유 검사 장치에서는 5 바이트의 헤더를 생성 다항식 g(x)로 나누어 주면 그 값이 0 이 되는 원리를 이용하여 페이로드 데이타의 경계를 판별한다. (그림 10)은 순환 여유 검사 회로이다. 페이로드 경계 식별은 헤더의 HEC 필드를 이용하여 순환 여유 검사(CRC)를 통하여 경계를 식별한다. 이 원리를 적용하면 HEC 필드에 해당하는 5 바이트의 데이터가 5개의 8 비트 쉬프트 레지스터에 입력되면 이 때 나머지가 0 이 된다. 이 순간 나머지의 모든 비트 값이 '0' 이므로 각 비트를 OR 연산을 취하면 로직 '0' 의 신호가 발생하고 다음 비트가 들어오는 순간에는 나머지가 '0' 이 아니므로 로직 '1' 상태로 복귀한다. 이는 클럭의 한 주기 동안만 로직 low 인 신호를 발생함을 의미한다. 이 신호를 이용하여 페이로드의 경계를 판별한다.

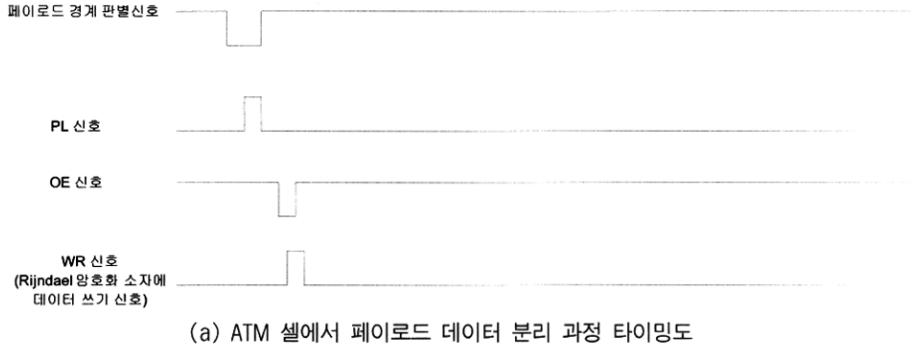
5.3 ATM 셀의 암호화 과정

5.3.1 ATM 셀의 페이로드 데이터 분리

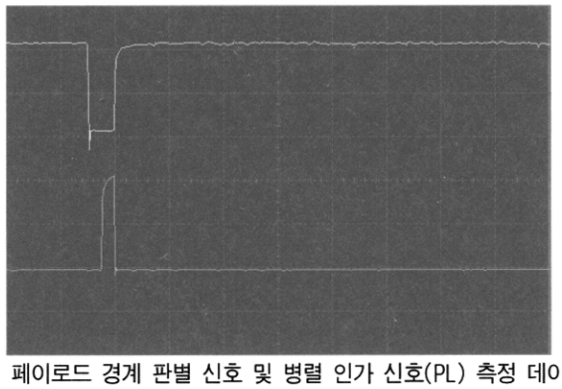
(그림 6)의 ATM 데이터 보안 장치의 송신측 블럭도에서 페이로드 데이터를 분리하여 암호화하는 과정은 다음과 같다. 직렬로 입력되는 셀에서 페이로드를 분리하여 암호화하는 과정의 타이밍도를 (그림 12) (a)에 도시하였다. ATM 셀의 헤더에 해당하는 40 비트가 (그림 6)의 블럭도의 쉬프트 레지스터(40 비트)에 입력되면 페이로드 경계 판별회로에 1 비트 구간에 해당하는 페이로드 경계 판별 신호가



(그림 11) 페이로드 종류 판별 회로



(a) ATM 셀에서 페이로드 데이터 분리 과정 타이밍도



(b) 페이로드 경계 판별 신호 및 병렬 인가 신호(PL) 측정 데이터

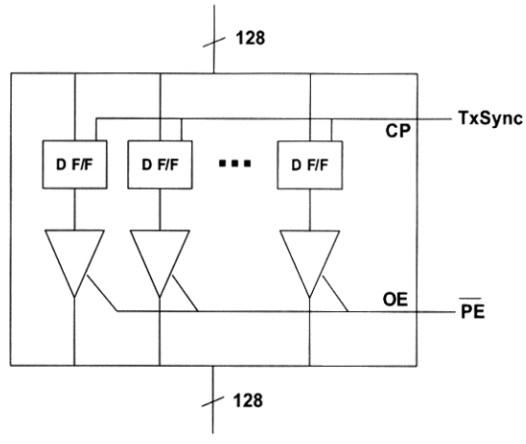
(그림 12) ATM 셀의 페이로드 데이터를 분리하여 암호화 소자에 전달 타이밍도

발생한다. 이 신호를 (그림 11)의 페이로드 종류 판별 회로의 활성(Enable) 신호로 인가해 주고 디코더의 출력 단자 중 0, 1, 2, 3 에 해당하는 단자 신호의 OR 로직을 구성하면 사용자 데이터 셀(PT 코드 값이 000~011) 일 때만 직렬/병렬 변환 회로에 데이터를 전달하기 위한 병렬 인가 신호(PL)가 발생된다. 이 신호를 직렬/병렬 변환 회로의 PL 단자에 가해 주면 쉬프트 레지스터에 입력되어 있는 페이로드 데이터가 직렬/병렬 변환 회로로 전달되게 된다. 직렬/병렬 변환 회로는 D-F/F로 구성된 128 비트의 래치 회로로 구성되어 있다. 직렬/병렬 변환 회로에 저장된 데이터는 PL 신호를 1 비트 구간 지연시킨 신호로 출력하여 암호화 소자에 전달하여 주면 암호화 과정을 거치게 된다. (그림 12) (b)에 측정한 페이로드 경계 판별 신호와 PL 신호를 보여 주고 있다. PL 신호의 상승 에지에서 3 개의 쉬프트 레지스터(128비트)에 입력된 페이로드가 직렬/병렬 변환 회로에 전달된다.

5.3.2 Rijndael 암호화 소자의 출력 데이터를 ATM 셀로 재송신

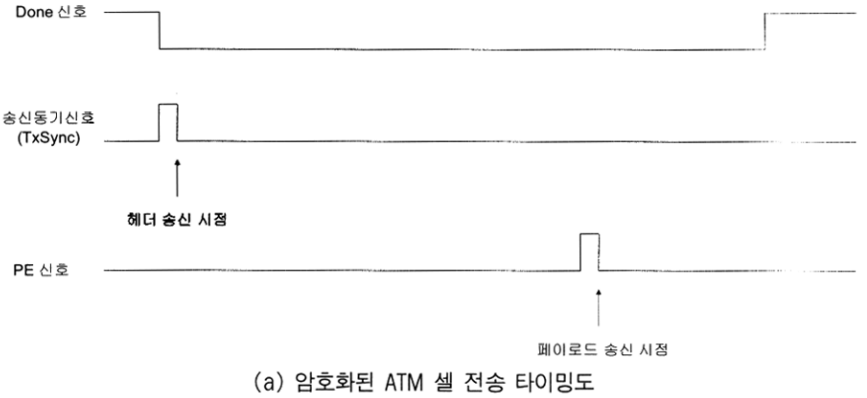
암호화 데이터 출력 회로는 Rijndael 암호화 소자의 Done 신호를 인에이블 신호로 하고 출력 인에이블(OE) 단자를 가지는 128 비트로 구성된 래치 회로이다. (그림 13)은 암호화 데이터 출력 회로의 내부이다.

암호화 과정이 완료된 페이로드 데이터를 셀로 구성하여

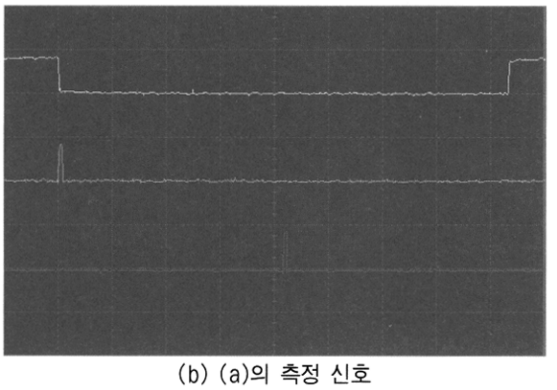


(그림 13) 암호화 데이터 출력 회로

전송하는 타이밍 동작은 (그림 14) (a)와 같다. Rijndael 암호화 소자의 Done 신호는 암호화 과정이 완료된 데이터의 출력 시에 발생되는 신호이며, 암호화 중에는 로직 '1'상태이며 암호화 데이터가 출력될 시에 로직 '0'가 된다. Done 단자가 로직 '1' 상태에서 로직 '0'로 천이하는 하강 모서리를 감지하여 155.52 MHz 클럭의 한 주기에 해당하는 송신 동기 신호(TxSync)를 발생하여 주어 이 신호에 동기를 맞추어 헤더 송신 회로에서 헤더를 전송하여 주고 헤더 전송 시작과 동시에 카운터를 동작시켜 헤더의 40 번째 비트가 전송되는 시점에 병렬/직렬 변환 회로 인가 신호(PE)를 발생



(a) 암호화된 ATM 셀 전송 타이밍도



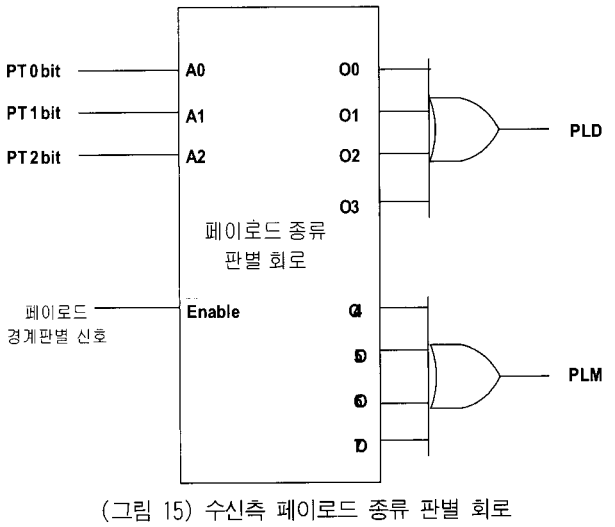
(b) (a)의 측정 신호

(그림 14) 암호화 완료된 데이터를 ATM 셀로 재전송 타이밍도

하여 주어 암호화 데이터 출력 회로의 데이터를 병렬/직렬 변환 회로에 전달하여 주면 헤더의 전송이 끝나는 시점부터 암호화된 페이로드가 전송되므로 ATM 셀의 형태로 재전송되게 된다. (그림 14) (b)에서 측정한 ATM 셀 전송 타이밍을 보여 주고 있다. 암호화 데이터 출력 회로는 암호화 소자의 출력단에서 출력되는 데이터에 헤더를 첨가하여 재전송하기 위해 동기를 맞추기 위한 버퍼 회로이다.

5.3 수신측 ATM 데이터 보안 장치의 복호화 과정

수신측의 복호화 과정도 송신측의 암호화 과정과 유사한 과정을 거친다. 먼저 입력되는 셀을 순환 여유 검사를 이용하여 페이로드의 경계를 판별한다. 페이로드의 경계가 판별되면 페이로드가 사용자 데이터이면 복호화 소자에 데이터를 전달하여 주고, 유지 보수 데이터인 경우 복호화 과정을 거치지 않도록 데이터를 분리한다. (그림 7)의 수신측 데이터 보안 장치 블럭도에서 셀 헤더 필드의 PT 코드 값이 사용자 셀 데이터에 해당하는 000, 001, 010, 011 인 경우에는 복호화 소자로 페이로드를 전달하여 주기 위한 신호(PLD)를 발생시켜 이 신호를 이용하여 복호화 소자에 데이터를 전달하여 주어 복호화 과정을 거치게 하여 주고, PT 코드 값이 유지 보수 셀 데이터에 해당하는 100, 101, 110, 111 인 경우는 유지 보수 데이터 분리 신호(PLM)를 발생시켜 복호화 과정을 거치지 않고 데이터를 분리한다. (그림 15)는 수신측의 페이로드 종류 판별 회로이다. PT 코드 값을 디코더의 주소 값으로 입력하여 주고, 페이로드 경계 신호를 활성(Enable) 신호로 인가해 주어 디코더의 출력 단자 중 0, 1, 2, 3 에 해당하는 단자 신호의 OR 로직을 구성하면 사용자 셀인 경우에는 복호화 처리를 위해 직렬/병렬 변환 회로에 데이터를 전달하기 위한 병렬 인가 신호(PLM)가 발생되고, 유지 보수 셀인 경우에는 출력 단자 4, 5, 6, 7 이 선택되므로 이들 단자를 OR 로직을 구성하여 데이터 분리 신호(PLM)를 발생시켜 이를 키 및 유지 보수 페이로드 추출 회로에 인가하여 주어 복호화 과정을 거치지 않고 데이터를 분리하여 준다.



(그림 15) 수신측 페이로드 종류 판별 회로

5.4 실험 결과

데이터 보안 장치에서는 Rijndael 알고리즘을 FPGA로 구현한 소자를 사용하여 구현하였다. FPGA 소자의 사양은 <표 4>에서 제시하였다. ATM 보드에서 송신한 UNI 규격의 데이터를 셀의 경계를 판별하여 페이로드만을 분리하여 암호화 소자에 전달해주어 암호화한 후 헤더를 첨가하여 전송한 데이터를 수신측에서 복호화를 수행하는 가를 확인하였다.

Rijndael 알고리즘 검증용 평문 벡터와 키 값를 입력하여 셀로 구성하여 전송하여 사용자 셀인 경우에만 암호화된 벡터 값이 출력으로 나오는 가를 확인하였다. 셀의 종류는 <표 3>의 PT 코드에 따라 사용자 셀과 유지 보수 셀로 구분된다. 셀의 페이로드가 사용자 데이터인 경우와 유지 보수 데이터인 경우로 각각 구분하여 입력하여 헤더 필드의 PT 코드가 사용자 셀인 경우에만 암호화되는 가를 확인하였다. CLP 비트는 high priority를 가정하여 0 으로 하였다. 다음은 암호화 블럭 길이가 128 비트, 키 길이가 128 비트일 경우에 Rijndael 알고리즘 검증용 벡터와 암호화 키 값을 입력하였을 때 출력되는 벡터이다[5].

-128 비트 Rijndael 알고리즘 검증용 입력 평문:
00112233445566778899aabbccddeeff
-키 : 000102030405060708090a0b0c0d0e0f
-출력 벡터 : 69c4e0d86a7b0430d8cdb78070b4c55a

본 실험에서는 페이로드가 세 개의 128 비트 검증용 벡터 구성된 셀을 입력하여 암호화 셀 데이터에 출력 벡터가 나오는 가를 확인하고, PT 코드가 사용자 데이터 셀인 000 인 경우와 유지 보수 데이터 셀인 100 인 경우에 수신단에서 복호화 여부를 확인하였다.

• 페이로드가 사용자 데이터 셀인 경우 (PT 코드=000)

송신측 입력 셀 데이타:

0000000000	00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff

송신측 전송 셀 데이타:

0000000000	69c4e0d86a7b0430d8cdb78070b4c55a 69c4e0d86a7b0430d8cdb78070b4c55a 69c4e0d86a7b0430d8cdb78070b4c55a

수신단 측의 복호화 셀 데이타:

0000000000	00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff

PT 코드를 000으로 하였을 때 HEC 필드의 헥사 값은 00 이 되어 헤더는 헥사 값으로 0000000000이 된다. 입력 평문 페이로드로 블럭 길이 128인 시험용 벡터를 입력하였을

때, PT 코드가 000 인 경우는 사용자 데이터 셀이므로 송신측 전송 셀 데이터에 암호화 출력 벡터가 나오는 것을 알 수 있다. 수신단 측에서는 PT 코드가 사용자 셀이므로 셀의 페이로드를 복호화하여 평문을 복원함을 알 수 있다.

- **페이로드가 유지 보수 데이터 셀인 경우 (PT 코드 =100)**

송신측 입력 셀 데이타:

0000000838	00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff

송신측 전송 셀 데이타:

0000000838	00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff

수신단 측의 출력 셀 데이타:

0000000838	00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff

PT 코드를 100 으로 하였을 때 HEC 필드의 헥사 값은 38 이 되어 헤더는 헥사 값으로 0000000838 이 된다. 입력 평문 페이로드로 블럭 길이 128 인 시험용 벡터를 입력하였을 때, PT 코드가 100 인 경우는 페이로드가 유지 보수 데이터인 셀이므로 송신단에서 페이로드를 암호화하지 않고 전송하는 것을 알 수 있으며, 수신단 측에서는 유지 보수 셀이므로 복호화 과정을 거치지 않고 데이터를 복구함을 알 수 있다.

6. 결론 및 향후 과제

본 논문에서는 ATM 망을 이용한 데이터 통신에 있어서 UNI 규격의 셀 데이터를 암호화/복호화하기 위해 Rijndael 알고리즘을 적용한 ATM 데이터 보안 장치를 구현하여 실험하였다. 본 방식은 기존에 발표된 암호화 전용 시스템을 전제로 한 방식과는 달리, 시스템 운용 중에 암호화/복호화를 필요로 하는 가입자에게만 별도의 모듈 형태의 장치로 부가하여 운용할 수 있는 장점을 지닐 뿐만 아니라, Rijndael 알고리즘을 적용하여 구현함으로써 암호화 강도 측면에서도 DES 를 적용한 방식에 비해 강점을 지닌다. ATM 데이터 보안 장치의 구현을 위해 Rijndael 알고리즘에 대해 기술하였으며, 실시간으로 입력되는 155.52 Mbps 속도의ATM 데이터를 128 비트 단위로 암호화 처리하는 3 개의 암호화 소자로 구성하여 384 비트의 페이로드 데이터의 암호화/복호화 과정을 송/수신단에서 검증하였다. ATM 셀의 헤더는 목적지의 라우팅 정보를 지니고 있으므로 헤더는 암호화하지 않고, 페이로드 부분만 분리하여 이를 암호화한 후 버퍼에 저장된 헤더를 첨부하여 재전송하여 준다. 특히 Rijndael 알고리즘의 각 라운드 단계 별로 동시에 데이터 처리가 가능하게 한 방식의 소자를 적용하여 암호화 속도를 향상시켰다. 본 논문에서는 Rijndael 알고리즘을 하드웨어로 구현한 ATM 데이터 보안 장치로 STM-1급 속도의 ATM 망에서 UNI 셀의 암호화/복호화 과정을 검증하였다. 본 논문의 장치는 암호화를 필요로 하는 셋탑 박스 설계 등에 응용될 수 있을 것이다. 향후 과제로는 ATM 셀 데이터의 스트림 암호화, 패킷 데이터의 암호화 구현에 관한 것이다.

참 고 문 헌

[1] William Stallings, Cryptography and Network Security, Prentice Hall, 1999.

[2] Davies R.W. "The Data Encryption standard in perspective," Computer Security and the Data Encryption Standard, pp.129~132.

[3] Shamir, A. "On the security of DES," Advances in Cryptology, Proc. Crypto '85, 280, Aug., 1985.

[4] NIST, "Announcing the Advanced Encryption Standard (AES)," FIPS PUB-197, Nov., 2001.

[5] Daemen, J., and Rijmen, V. "Rijndael : The Advanced Encryption Standard." Dr. Dobb's Journal, Mar., 2001.

[6] 이건배, 이병욱,"FPGA를 이용한 128 비트 암호화 알고리즘의 하드웨어 구현,"정보처리학회논문지C, 제8-C권(제3호), pp.277~286, Jun., 2001.

[7] 서정욱, 김경수,"ATM 물리계층에서의 정보보호", 정보보호학회논문지, 제7권(제1호), pp.3~14, Mar., 1997.

[8] 신효영, 유황빈, "ATM 방식의 고속 통신망에서 비밀성 보장을 위한 구조와 암호 알고리즘에 관한 연구", 한국통신학회논문지, 제23권(제1호), pp.168~177, Jan., 1998.

[9] Electronic Frontier Foundation," Cracking DES : Secrets of Encryption Research, Wiretap Politics and Chip Design", Sebastopol, CA : O'Reilly, 1998.

[10] 전신우, 정용진, 권오준, "Rijndael 암호 알고리즘을 구현한 암호 프로세서의 설계", 정보보호학회논문지, 제11권(제6호), pp.77~87, Dec., 2001.

[11] E. Biham, "New types of cryptanalytic attacks using related keys," Advances in Cryptology, Proceedings Eurocrypt'93, NCS 765, T. Helleseth, Ed., Springer-Verlag, pp.398~409, 1993.

[12] Daemen, J., and Rijmen, V. "The Design of Rijndael : The Wide Trail Strategy Explained," New York, Springer-Verlag, 2002.

[13] Newman, P., "ATM Technology for Corporate Networks",

IEEE Communications Magazine, Vol.30, No.4, pp.90~101, Apr., 1992.

[14] Handel, R."Operation and Maintenance Issues of ATM Networks," Proc. of the International Conference on Communication Technology, Beijing, 1992, Vol.1, pp.1107~1117, 1992.

[15] ITU-T : Recommendation I.432."B-ISDN User-Network Interface-Physical layer Specification," Rev.1, Genova, 1993.

[16] ISO 9160 "Information processing-Data encipherment-Physical layer interoperability requirement, "International Standards Organization, 1988.

[17] Rathgeb, E.P., Theimer, T.H., Huber, M.N."ATM Switches-Basic Architectures and their Performance," International Journal of Digital and Analog Cabled System 3, Vol.2, No.4, pp.227~236, Oct., 1989.

[18] Viktor Fisher and Milos Drutarovsky, Two Methods of Rijndael Implementation in Reconfigurable Hardware, Workshop on Cryptographic Hardware and Embedded Systems 2001(CHES 2001), May, 2001.

임 성 렬

e-mail : syim@wsu.ac.kr

1983년 서울대학교 전자공학과(공학사)

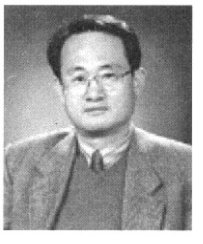
1992년 포항공대 전자전기공학과(공학석사)

2005년 부산대학교 이학박사

1983년~1998년 한국전자통신연구원 선임연구원

2003년~현재 우송대학교 철도전기 정보통신학부 초빙교수

관심분야 : 암호용 ASIC 설계, 네트워크 보안, 암호알고리즘



정 기 동

e-mail : kdchung@melon.cs.pusan.ac.kr

1973년 서울대학교 응용수학과(학사)

1975년 서울대학교 대학원 전자계산학과(이학석사)

1986년 서울대학교 대학원 전자계산학과(이학박사)

1990년~1991년 MIT대학 교환교수

1995년~1997년 부산대학교 전자계산소 소장

1999년~2001년 부산대학교 BK21단장

1978년~현재 부산대학교 전자계산학과 교수

관심분야 : 멀티미디어, 모바일 네트워크, Overlay Multicast