Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1237

AES 블록 암호에 OFB 모드를 적용한 ATM 셀 보안 기법

임 성 렬†‡
부산대학교 (강사)

ATM Cell Security Techniques Using OFB Mode on AES Block Cipher

Sung-Yeal Im†‡
Pusan Nat'l University (Instructor)

요 약

본 논문은 AES 블록 암호에 OFB(Output Feedback) 모드를 적용한 ATM(Asynchronous Transfer Mode) 셀 보안에 관한 것이다. ATM 셀은 사용자 데이터 셀과 유지 보수 셀로 구분되며 각 셀의 크기는 53 옥텟이며 5 옥텟의 헤더와 48 옥텟의 페이로드로 구성되어 있다. ATM 셀의 암호화/복호화를 위해서는 셀의 경계를 감지해야 하는 데 이는 헤더 내의 HEC(Header Error Control)필드를 이용하여 가능하다. 셀의 경계를 감지한 후에는 사용자 셀만 암호화하기 위하여 PT(Payload Type)코드를 이용하여 페이로드의 종류를 감지한다. 본 논문에서는 ISO 9160의 요구사항을 만족하는 ATM 셀의 보안 방법을 제시하였다.

ABSTRACT

This paper is about Asynchronous Transfer Mode (ATM) cell security in which an Output Feedback (OFB) mode is applied to an AES block ciphers. ATM cells are divided into user data cells and maintenance cells, and each cell is 53 octets in size and consists of a header of 5 octets and a payload of 48 octets. In order to encrypt/decrypt ATM cells, the boundaries of cells must be detected, which is possible using the Header Error Control (HEC) field in the header. After detecting the boundary of the cell, the type of payload is detected using a payload type (PT) code to encrypt only the user cell. In this paper, a security method for ATM cells that satisfies the requirements of ISO 9160 is presented.

Keywords: ATM cell, stream encipherment, OFB

I. 서 론

데이터 통신에 있어서 데이터 보안은 데이터 유출이나 변조로부터 데이터를 보호하는 가장 중요한 사안이다. 데이터 보안을 유지하는 여러 방법들 중에 데이터를 암호화하는 방법이 제3자에게 데이터 유출에 대한 대책이 되며, 망에 접근한 제3자로 부터 데이터 변조를 예방하는 가장 좋은 해결책이다.

암호화 알고리즘 적용 시 고속 데이터 실시간 처리를 위해서는 하드웨어적으로 구현할 필요가 있을 것이다[1,2]. 본 논문은 ATM 통신망에서 셀 데이터 전송 시에[3] 셀 데이터를 실시간으로 암호화/복호화를 수행하는 보안 기법이다. 암호화 방식에는 블록 암호와 암호화 변환 속도가 빠른 스트림 암호화 방식으로 분류할 수 있다[4].

AES 알고리즘[5,6]을 ATM 망에 적용 시 ATM 셀의 페이로드가 48 옥텟(384 비트)로 길이가 고정되어 있어 AES 의 암호화 블록 길이 중

Received(08. 03. 2021), Modified(09. 24. 2021), Accepted(10. 15. 2021)
† 주저자, syim7@pusan.ac.kr
† 교신저자, syim7@pusan.ac.kr(Corresponding author)

384의 약수가 되는 128 비트를 블록 단위로 적용하면 AES 소자 3개를 병렬로 사용하여 블록 암호 구현이 가능하나 하드웨어 회로가 복잡해진다.

ATM 셀은 사용자 데이터 셀과 네트워크 관리를 위한 유지 보수 셀로 구분된다. 본 논문에서는 페이로드 종류를 구분하는 헤더의 PT 필드의 값 따라 셀의 종류를 판별하고, 사용자 데이터 셀의 경우 암호화/복호화를 수행한다. ATM 셀은 5 옥텟 헤더와 48 옥텟 페이로드로 구성되어 있는 데, 직렬로 입력되는 ATM 셀의 HEC (Header Error Control) 필드를 이용하여 페이로드의 경계를 판별하고 목적지 주소와 같은 제어 데이터가 포함된 헤더는 암호화하지 않고 페이로드만 암호화한다. 본 논문에서는 블록 암호인 AES 알고리즘 기반에 OFB 모드를 적용하여 직렬로 전송되는 ATM 셀과 암호화 키를 1 바이트 단위로 암호화를 수행하는 스트림 암호화 기법을 제안한다[7].

본 논문에서는 AES에 기반한 OFB 모드를 적용한 스트림 암호화 회로를 하드웨어로 구현하여 STM-1 속도(155.52 Mbps)의 직렬 입력 ATM 셀의 암호화/복호화 처리가 되는 것을 검증하였다. 본 논문은 6개의 장으로 구성되는 데, 2장에서는 기존 연구를 3장에서 AES 와 암호화 모드을 소개하고 4장에서는 ATM 셀의 구조를 언급하고 5장에서 AES 블록 암호에 OFB 모드를 적용한 ATM 셀 보안 기법을 설명하고 6장에서 결론을 내린다.

II. 기존 연구

이 장에서는 관련된 연구로 ATM 망에서의 암호화 구현에 대하여 살펴본다. ATM 물리 계층에서 DES 알고리즘을 구현한 논문이 있으며, 시스템 구현 시에 암호화/복호화를 전제한 방식이다[8]. 이는 본 논문에서 제안하는 보안을 필요로 하는 구성원에게만 보안 기능을 제공하는 방식과 유연성 측면에서 차이가 많다. 한편 DES 암호화 알고리즘은 더 이상 안전하지가 않다[9]. 또 다른 논문은 ATM 계층에서 암호화를 소프트웨어적인 하는 논문이 있다[10]. 이는 소프트웨어적으로 암호화를 수행하는 방식으로 암호화 알고리즘 검증용으로는 적합하나 시스템에 적용 시 하드웨어로 구현한 방식에 비하여 암호화 수행 속도가 하드웨어 구현한 방식이 비하여 현저히 느리며 실시간적인 암호화 처리가 어렵다. 또 다른 연구는 AES 알고리즘의 블록 암호화 기법을 ATM 셀에 적용하여 암호화 블록 길이를 128 비트, 키 길이를 128 비트로 하여 하드웨어로 암호화를 구현한 방식이 있는데[11] 이는 AES 알고리즘의 블록 암호화 기법을 적용하여 이전의 DES 알고리즘을 적용한 ATM 셀 보안 방식에 비하여 암호화 강도도 더 강하고 실시간 암호화 처리가 가능하나 블록 길이를 128 비트로 하는 블록 암호화 기법을 적용하여 길이가 48 옥텟(384비트)인 페이로드를 블록 단위로 암호화하기 위해 3개의 AES 소자를 필요로 하며 ATM 셀의 헤더를 분리하여 페이로드를 암호화한 후 ATM 셀의 헤더를 패딩하여 주어야 함으로 이를 구현하기 위한 하드웨어 회로가 복잡하다. 반면에 본 논문에서는 AES 알고리즘 기반에 OFB 모드를 적용함으로써 AES의 블록 암호화 기법을 적용한 방식에 비하여 회로 설계 시에 소자의 수를 현저히 줄이고 AES 알고리즘을 적용하여 128 비트 단위로 블록 암호화 과정만 수행하는 기존의 방식[11]에 비하여 본 논문에서는 암호화된 데이터를 입력으로 궤한하여 주는 OFB 모드를 적용하여 AES 알고리즘의 블록 암호만 적용한 방식에 비해 암호화 강도를 더욱 강화하였으며 기존의 방식보다 AES 소자의 수도 줄이고 하드웨어 회로의 구현도 상대적으로 용이해져 60% 정도의 하드웨어 구현 비용 절감이 예상되는 등의 경제적 잇점을 지닌다.

본 논문에서는 AES 알고리즘에 OFB 방식을 적용한 스트림 암호화로 구현한 ATM 보안 장치를 제안하며, 본 논문에서 제안하는 방식이 기존 연구들에 비해 암호화 강도도 더 강하며, 하드웨어 회로를 더 간결하게 하여 경제성 측면에서도 잇점이 있다고 할 것이다. 또한 기존의 방식이 제공하는 상용 시스템의 운용 중 보안을 필요로 하는 구성원에게만 기능 제공이 필요할 시 별도의 부가 장치로 구성하여 제공할 수도 있다.

III. AES와 암호화 모드

3.1 AES 알고리즘

AES는 미국 NIST에서 2000년에 차세대 알고리즘으로 채택하여[5,6] 지금까지 표준으로 사용되어 오고 있다. AES 암호 알고리즘은 대칭키 알고리즘으로[6] 암호화 단위인 블록의 크기를 선택할 수 있다. 각 라운드는 바이트 치환, 행의 쉬프트, 열의 혼

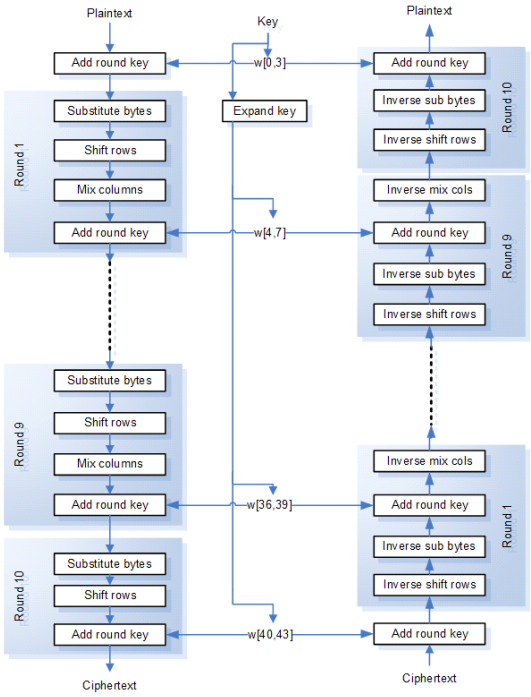

Fig. 1. AES Algorithm with round 10

합 등으로 구성된 단계를 갖는 데, 암호 블록 길이에 따라 라운드 수가 결정된다. 본 논문에서는 키 길이를 128 비트, 블록의 길이를 128 비트 단위로 하여 이 경우 라운드 수는 10 이 된다. Fig. 1은 라운드가 10 인 AES 알고리즘 과정이다.

3.2 AES 블록 암호에 적용 가능한 운영 방식

블럭 암호인 AES에 적용할 수 있는 암호화 모드는 몇 가지가 있으나 여기서는 CFB(Cipher Feedback), CTR(Counter)과 OFB(Output Feedback) 모드에 대해 알아보고 본 논문에서 ATM 셀의 암호화 모드로 OFB 모드를 채택한 배경을 살펴본다.

3.2.1 CFB(Cipher Feedback) 모드

이 방식은 평문과 암호문을 블록 암호를 이용하여 암호화하거나 복호화하지 않고 n 비트의 이동 레지스터의 값 S를 블록 암호를 이용하여 암호화하거나 복호화한다. 암호화 과정은 r 비트 평문 블럭과 이동 레지스터의 r 비트를 XOR함으로서 이루어지고 복

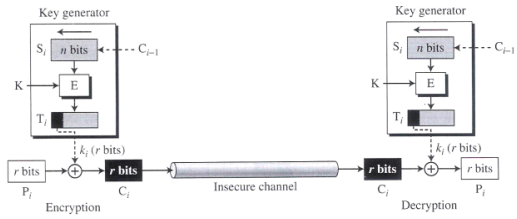

Fig. 2. CFB mode as a stream cipher

호화 과정은 r 비트 암호문 평문 블록과 이동 레지시터 r 비트를 XOR함으로써 이루어진다. CFB 모드가 DES나 AES와 같은 블록 암호를 이용한 암호화 모드이지만 그 결과는 스트림 암호와 같으며 키 스트림이 암호문에 의존하는 비동기식 스트림 암호이다. CFB 모드는 전송 도중 암호문 한 비트의 오류가 해당 블록의 한 비트에만 오류가 발생하는 OFB 모드와 달리 전송 도중 암호문 한 비트의 오류가 다른 여러 블록의 비트 오류로 파급된다[12]. Fig. 2는 AES 알고리즘을 적용한 스트림 암호로서의 CFB 모드이다.

3.2.2 OFB(Output Feedback) 모드

OFB 모드는 CFB 모드와 매우 유사하나, OFB 모드의 모든 암호문 블록의 각 비트는 이전 암호문 블록의 비트와 독립이다. 이는 오류 파급의 영향을 피할 수 있음을 의미한다. 만약 암호문 블록 전송 도중 1 비트 오류가 발생한다면, 그 오류는 다음 블록의 비트 오류에 영향을 미치지 않는다. Fig. 3에 OFB 모드의 암호화 과정을 보여주고 있다. Fig. 3에서 각 단계의 E 박스는 AES 알고리즘을 사용하며 식(1)로 암호화되며

$$C_j = P_j \oplus E(k_j, [C_{j-1} \oplus P_{j-1}]) \quad (1)$$

복호화는 식(2)의 과정을 거친다.

$$P_j = C_j \oplus E(k_j, [C_{j-1} \oplus P_{j-1}]) \quad (2)$$

OFB 모드의 유리한 점은 전송 중에 발생한 비트 에러가 전파되지 않는다는 것이다. Fig 3의 암호문에서 C_1 바이트에서 1 비트의 에러가 발생하면 복호화된 평문의 P_1바이트에만 영향을 미친다.[7]

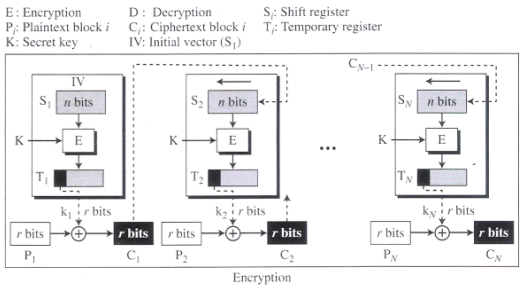

Fig. 3. Encryption in OFB mode

3.2.3 CTR(Counter) 모드

CTR 모드는 암호화 시 피드백이 존재하지 않지만 키 스트림의 의사 난수성은 카운터를 사용함으로써 구현이 가능하다. n 비트의 카운터는 초기값(IV)으로 초기화 되고 사전에 정의된 규칙($\bmod 2^n$)에 따라 증가한다.[13] 평문 블록과 암호문 블록 사이의 관계는 다음과 같이 정의된다.

암호화: $C_i = P_i \oplus E_{ki}(counter)$

복호화: $P_i = C_i \oplus E_{ki}(counter)$

CTR 모드는 암호화 및 복호화 과정에서 평문 블록과 암호문 블록에 상관없이 블록 암호 E_k를 사용하여 키 스트림을 생성한다. CTR 모드는 OFB 모드와 동일하게 이전 암호문 블록과 독립인 키 스트림을 생성하지만 피드백을 사용하지 않는다. CTR 모드의 안전성 문제는 OFB 모드의 안전성과 동일 시되며[14] 전송 중의 암호문의 1 비트의 오류는 대응되는 평문의 1 비트에만 영향을 주므로 이는 OFB 모드와 동일하다. 하지만 카운터 값 증가식 $\bmod 2^n$은 하드웨어로 구현하기가 어렵다.

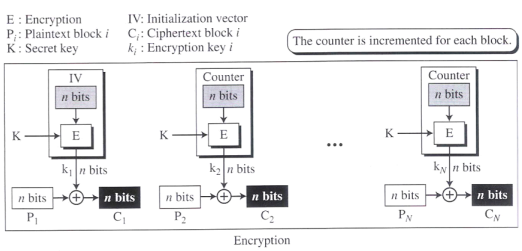

Fig. 4. Encryption in CTR mode

3.2.4 AES에 기반한 OFB 모드를 적용한 ATM 셀 암호화

앞서 살펴본 AES 블록 암호의 운영 모드 중 ATM 셀 암호에 있어서 OFB 모드가 가장 적합한 모드임을 살펴본다. Fig. 5와 같이 OFB 모드를 사용하여 평문과 키를 바이트 단위로 암호화하여 비트 단위로 전송함으로[16] 송신측과 수신측에서 AES 소자를 한 개로 암호화 키와 복호화 키 발생용으로 사용하여 OFB 모드를 구현한다.

CFB 모드에서는 1 바이트 단위로 암호화하여 전송되는 데이터의 전송 중에 발생하는 1 비트의 에러가 복호화되는 평문의 여러 바이트의 비트 에러를 유발하게 되는 데, 이는 같은 상황에서 OFB 모드는 암호문의 1 바이트의 1 비트의 에러가 복호화된 해당 바이트에 국한한 1 비트의 에러만 발생하게 된다. 이는 전송 중에 에러 비트의 발생이나 침입자의 변조에 대비하면 CFB 모드에 비하여 상당히 유리한 점이 될 것이다. 한편 CTR 모드에서는 n 비트의 카운터가 정의된 규칙($\bmod 2^n$)에 의해 증가하는 하드웨어 회로를 구현하기가 어렵고 암호화 강도면에서는 CTR 모드와 OFB 모드가 같다고 볼 수 있으므로[14] 본 논문의 ATM 셀 보안 기법으로는 OFB 모드가 적용하는 것이 최적의 방책이라고 할 것이다.

또한 4.3 절에서 언급되지만 ATM 셀에서 헤더와 같은 중요한 정보를 지니는 필드에서의 전송 중의 1 비트의 에러 발생은 헤더 내에 있는 HEC(Head Error Control)필드를 이용하여 오류 비트 정정이 가능하며 여러 개의 비트 에러 발생의 경우는 다수개 비트의 에러가 발생했다는 사실의 감지가 가능하여 해당 셀을 폐기하여 대처하니[15] 헤더 필드에서는 인증(Authentication)기능도 지니고 있다고 할 것이다. 페이로드 부분의 에러 발생 인증 여부도 페이로드의 중요성에 따라 상위 계층인 AAL(ATM

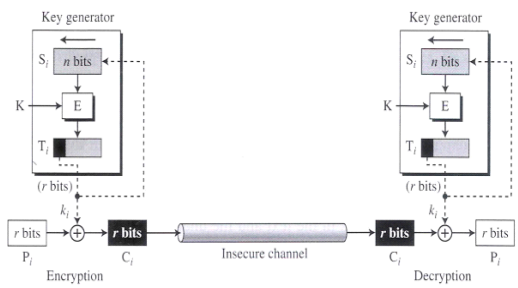

Fig. 5. Output Feedback (OFB) with stream data encryption/decryption

Adaption Layer)에서 적용 여부를 결정하면 될 것이다. 본 논문에서는 평문와 키(k_i)를 암호화 단위가 바이트임으로 Fig 5에서 r 값은 8 이다.

IV. ATM 셀의 구조

ATM 망에서는 데이터를 셀(cell) 단위로 전송하는 데 셀은 Fig. 6과 같이 5 옥텟의 헤더와 48 옥텟의 페이로드로 구성된다[17]. 셀의 비트는 연속 스트림에서 오른쪽에서 왼쪽으로 전송 경로를 통해 전송된다.

셀 헤더에는 셀의 제어 정보가 포함되어 있는데, Fig. 7은 UNI의 경우에 헤더 필드의 의미를 도시하였다[18, 19].

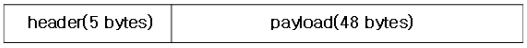

Fig. 6. The format of ATM cell

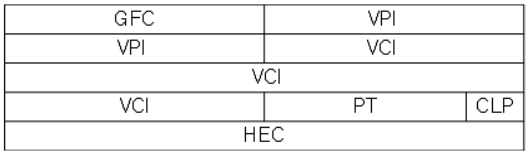

Fig. 7. Header Structure of ATM UNI Cells

4.1 PT(Payload Type)

페이로드(payload)가 사용자의 데이터인지, 네트워크 제어 데이터인 지를 구분한다. 본 논문에서는 페이로드의 암호화 여부를 페이로드 종류에 따라 결정한다. 즉, PT 값이 000~011인 경우에만 페이로드 데이터를 암호화한다. Table 1은 페이로드 종류에 따른 PT 코드 값이다.

Table 1. Payload type according to PT code

PT Code	Payload type
000	user data cell
001	user data cell
010	user data cell
011	user data cell
100	maintenance cell
101	maintenance cell
110	resource management cell
111	reserved

4.2 CLP(Cell Loss Priority)

CLP는 트래픽 정체 시 셀의 손실 순위를 나타낸 것이다. CLP=0 는 셀이 우선 순위가 높음을 의미하고, CLP=1 이면 셀이 하위 순위이다. 폭주 구간에서 CLP=1인 셀은 트래픽을 원활하게 하기 위해 폐기될 수도 있음을 의미한다.

4.3 HEC(Head Error Control)

이 필드는 셀 헤더의 오류를 정정하는 데 사용된다. 여기에는 물리 계층에서 처리되는 헤더 오류 제어 (HEC) 시퀀스가 포함되어 있다. 헤더를 생성 다항식 $g(x)=x^8+x^2+x+1$로 나누어 떨어지도록 HEC 필드를 구성한다.[19]

V. AES 블록 암호에 OFB 모드를 적용한 ATM 셀 보안

5.1 개요

ISO 9160에서는 물리 계층에서 데이터 처리의 기준을 명시하고 있는 데, ATM 데이터를 암호화할 경우 데이터 보안 장치를 별도의 장치로 할 수도 있다[20].

ATM 인터페이스는 UNI와 NNI로 나눌 수가 있는 데 셀의 헤더의 필드 부분이 약간 다르다[21]. 본 논문에서는 ATM 데이터 보안 장치를 구성하여 물리 계층인 UNI 에 적용하였다. Fig. 8에 ATM 망의 개념도를 도시하였다. ATM 셀의 암호화 시 헤더는 라우팅 값 등을 지니고 있음으로 헤더를 제외한 페이로드만을 스트림 암호화 모드로 보안하여 전송해 주어야 한다.

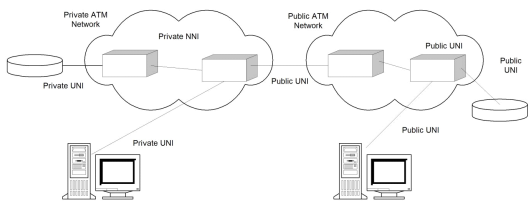

Fig. 8. Structure of ATM network

5.2 AES 암호화 소자

본 논문에서는 암호화/복호화 기능을 제공을 위해 블록 길이 128 비트, 키 길이 128 비트인 암호화 소자를 사용한다.

Table 2는 본 논문에 적용한 AES 암호화 모듈 사양이며 합성된 회로의 성능은 Table 3과 같다.

Table 2. Specification of AES module

Device	EPF10K200SRC240-1
B;ock length/Key length	128/128
Number of round	10
Performance	1.28 Gbits/sec
Number of gates	15,449 gates
Memory	32K-bit ROM 1408-bit ROM
Total	44268.2 gates

Table 3. AES implementation result on ALTERA RLEX 10KE200-1

Device	EPF10K200SRC240-1
Memory bits	34816/98304(35%)
Logic cells	3442/9984(34%)
Frequency(MHz)	29.49
Speed(Mbits/sec)	343.26

5.3 ATM 데이터 보안 장치의 암호화 과정

ATM 데이터 보안장치의 송신측 블록도를 Fig. 9에 도시하였다. 블록도의 각 기능을 설명하면 다음과 같다.

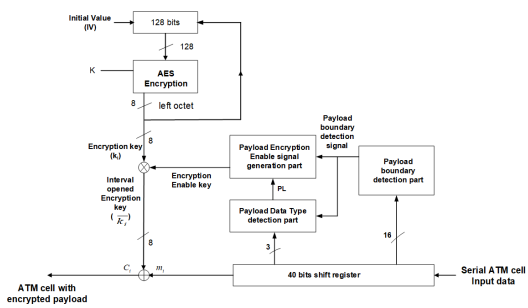

Fig. 9. ATM Cell Encryption on Transmitter

5.3.1 페이로드 경계 판별 회로

입력되는 셀 데이터에서 페이로드 데이터를 분리하기 위해 페이로드 경계 판별 회로는 순환 여유 검사 방식으로 구현한다. ATM 셀의 헤더가 $g(x)=x^8+x^2+x+1$로 나누어지게 HEC 필드 값이 설정되어 있으므로 순환 여유 검사 장치에서는 입력되는 셀의 헤더를 $g(x)$로 나누어 그 값이 0 이 되는 지점을 찾아 페이로드 데이터의 경계 판별을 한다[22]. Fig. 10은 페이로드 경계 판별 회로이다.

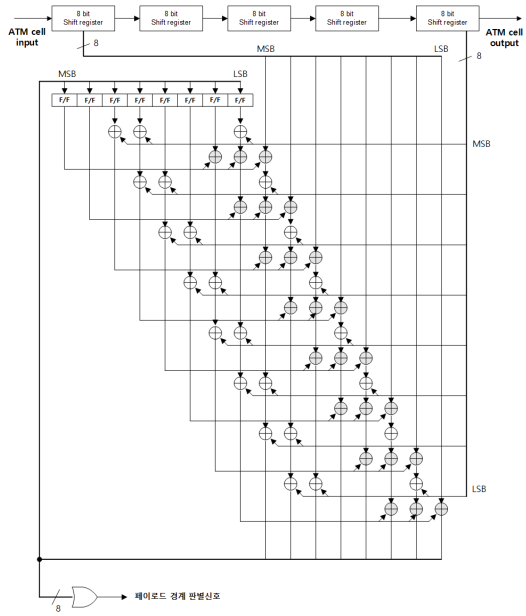

Fig. 10. Payload boundary detection circuit

5.3.2 ATM 셀의 페이로드 데이터 종류 판별회로

페이로드의 경계를 판별한 후 페이로드가 사용자 데이터이면 페이로드의 데이터를 암호화하여 준다. 이 신호는 셀 헤더 필드의 PT code 값이 000, 001, 010, 011 인 경우에만 발생시켜 준다. Fig. 11은 페이로드 타입 판별 회로이다. PT code 값을 디코더의 입력단자로 인가하여 주고, 페이로드 경계 신호를 인에이블 신호로 하여 0, 1, 2, 3 출력 단자의 신호를 OR 로직으로 구성하여 셀이 사용자 데이터인 경우에만 페이로드 데이터를 암호화한다.

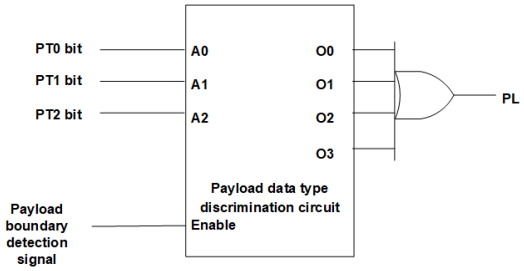

Fig. 11. Payload data type discrimination circuit

5.3.3 페이로드 암호화 동작 신호 발생부

암호화 동작 신호 발생부에서는 페이로드의 경계 판별 신호가 인가되면 내부 계수기의 초기값으로 페이로드의 길이인 48을 값으로 설정한 후 페이로드 데이터를 카운트 하여 페이로드 구간 동안만 신호 값이 1 이고 나머지 구간은 0 이 되는 암호화 동작 신호를 생성한다.

이는 암호화 동작 신호는 ATM 셀의 페이로드에 해당하는 구간만 로직 1이고 그 외 그간은 로직 0 인 신호가 된다. Fig. 12에 페이로드 경계 판별 신호와 암호화 동작 신호 및 ATM 셀의 타이밍 도를 도시하였으며, Fig. 13은 데이터 프레임 경계 판별 신호와 암호화 동작 신호를 오실로스코프로 측정한 것이다.

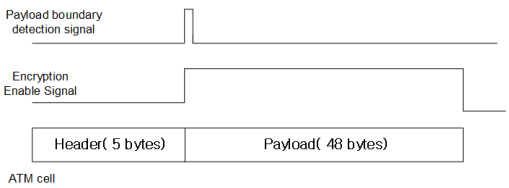

Fig. 12. ATM Cells and Encryption Enable Signal

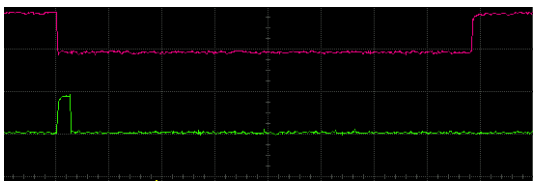

Fig. 13. Inverted encryption enable signal and payload boundary determination signal

5.3.4 AES 키 발생부

AES 키 발생부는 OFB 모드로 구현하여 키 스트림을 발생시키며 페이로드 경계 판별 신호에 준해 AES 키 발생부의 동작을 시작한다. 발생 된 암호화 키(k_i)가 암호화 동작 신호와 AND 연산을 하여 암호화 키($\overline{k_i}$) 가 생성된다. Fig. 9에서 보듯이 암호화 동작 신호는 ATM 셀의 페이로드 구간 동안만 로직 1 임으로 암호화 키(k_i)와 AND 연산한 암호화 키($\overline{k_i}$) 는 ATM 셀의 페이로드 구간에서는 $\overline{k_i}=k_i$ 이고 나머지 구간에서는 $\overline{k_i}=$(로직 0) 이다. 암호화 키($\overline{k_i}$)는 ATM 셀(m_i)과 비트 단위로 XOR 연산 회로를 거친다. 암호화 키($\overline{k_i}$) 는 페이로드 영역 구간에서는 $\overline{k_i}=k_i$ 이므로 ATM 셀의 페이로드 영역 구간에서는 $C_i=m_i\otimes\overline{k_i}$ 연산에 의해 암호화되고 ATM 셀의 나머지 구간에서는 $\overline{k_i}=$(로직 0) 이므로 $C_i=m_i\oplus 0$ 연산을 하면 $C_i=m_i$ 이다. ATM 셀(m_i)과 암호화 키($\overline{k_i}$)는 페이로드 경계 판별 신호와 동기가 맞은 상태이므로 ATM 셀(m_i)과 암호화 키($\overline{k_i}$)를 XOR 연산하면 ATM 셀에서 페이로드 영역만 암호화되어 전송된다.

5.4 수신 측 ATM 셀 보안 장치의 복호화

Fig. 14에 수신단의 ATM 셀 복호화부의 블록도를 도시하였다. 먼저 직렬로 입력되는 ATM 셀을 페이로드 경계 판별회로에서 페이로드의 경계를 판별한 후, 사용자 셀인 페이로드만 복호화 과정을 거치도록 페이로드 복호화 동작 신호를 발생한다. 수신측 페이로드 종류 판별 회로도 Fig. 11의 송신측 페이로드 종류 판별회로와 동일하다. PT 코드 값이 000, 001, 010, 011 인 경우에 사용자 셀로 간주하여 페이로드를 복호화 하여 주기 위한 로직 신호가

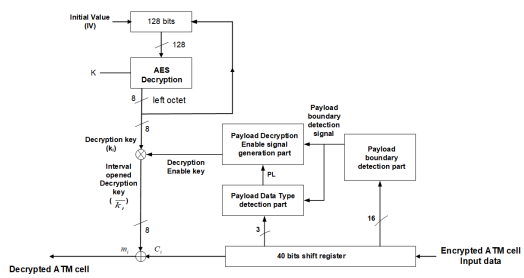

Fig. 14. ATM Cell Decryption on Receiver

발생하여 이 신호를 이용하여 페이로드 복호화 동작 신호 발생부에서 복호화 동작 신호를 발생하게 하여 페이로드가 복호화 과정을 거치게 한다.

5.5 실험 결과

AES 알고리즘의 검증을 위하여 시험 시에 AES 표준에서 제시하는 검증용 벡터와 키 값를 사용하여 사용자 셀인 경우에만 벡터 값이 암호화되는 것을 확인하였다. HEC 필드는 생성 다항식 g(x)를 헤더에 적용한 값이다. 다음은 암호화할 ATM 셀의 페이로드가 48 옥텟, 키 길이를 128 비트로 하여 AES 검증용 벡터와 키 값을 사용한 경우이다.

● 입력 셀의 평문 페이로드용 입력 벡터(48 옥텟)

000102030405060708090a0b0c0d0e0f
1011121314151617
000102030405060708090a0b0c0d0e0f
1011121314151617

● 암호화키 (128 비트)

00112233445566778899aabbccddeeff

● 암호화된 출력 셀 페이로드의 출력 벡터

80121e0776fd1d8a8d8c31bc965d1fee
80121e0776fd1d8a
80121e0776fd1d8a8d8c31bc965d1fee
80121e0776fd1d8a

본 실험에서는 페이로드가 48 옥텟 검증용 벡터로 구성된 셀을 입력하여 수신단에서 전송된 암호화된 셀 데이터가 복호화가 됨을 검증하였다.

● 페이로드가 사용자 데이터 셀인 경우
(PT code = 000)

입력 셀 헤더 : 0000000107

입력 셀 데이터:

0000000000	000102030405060708090a0b 0c0d0e0f1011121314151617 000102030405060708090a0b 0c0d0e0f1011121314151617

암호화 셀 데이타:

0000000000	80121e0776fd1d8a8d8c31bc 965d1fee80121e0776fd1d8a 80121e0776fd1d8a8d8c31bc 965d1fee80121e0776fd1d8a

복호화 셀 데이터

0000000000	000102030405060708090a0b 0c0d0e0f1011121314151617 000102030405060708090a0b 0c0d0e0f1011121314151617

● 페이로드가 유지 보수 데이터 셀인 경우
(PT code = 100)

입력 셀 헤더 : 0000000838

입력 셀 데이타:

0000000838	000102030405060708090a0b 0c0d0e0f1011121314151617 000102030405060708090a0b 0c0d0e0f1011121314151617

출력 셀 데이타:

0000000838	000102030405060708090a0b 0c0d0e0f1011121314151617 000102030405060708090a0b 0c0d0e0f1011121314151617

PT code를 100으로 하였을 때 HEC 필드의 헥사 값은 817이 되어 헤더는 헥사 값으로 0000000817이 된다.

VI. 결 론

본 논문에서는 ATM 셀 데이터 보안을 위해 AES 블록 암호에 OFB 모드를 적용하여 송/수신하는 ATM 데이터 보안 장치를 구현하여 실험하였다. 일반적으로 암호화 알고리즘은 소프트웨어 구현보다 하드웨어로 구현하는 것이 처리 속도가 빠른데, 본 연구에서는 하드웨어로 구현하여 소프트웨어로 구현한 모드에 비해 데이터 처리 속도가 현저히 빠르게 구성하였다. ATM 데이터 보안 장치의 구현을 위해 데이터 암호화 기법 중 블럭 암호에 적용하여 스트림 암호로 이용하는 운영 모드를 고찰하고 하드웨어 회로 구현에 있어 블럭 암호화에 비해 구현이

다소 덜 복잡한 스트림 암호화 방법을 이용하여 회로 구성의 경제성에 잇점을 둔 ATM UNI 셀 보안 방안을 검증하였다. 기존의 블록 암호 적용 방식보다 AES 소자의 수를 줄여서 비용 절감의 효과도 거두고, OFB 모드를 적용하여 AES 소자의 출력단의 암호화된 데이터를 AES 소자의 입력으로 피드백함으로써 암호화 강도를 더 강하게 하는 효과를 주었다. ATM 셀은 헤더와 데이터에 해당하는 페이로드로 구성되어 있는 데 헤더는 제어 관련 데이터이므로 페이로드 부분만 암호화하여 전송하여 준다. 이를 위해 ATM 셀의 HEC 영역을 이용하여 입력 셀의 경계를 판별한 다음 사용자 데이터 셀만 암호화하기 위한 셀의 종류를 판별하기 위해 셀 내의 PT 필드의 PT 코드를 PT 타입 검출 회로로 전송하였다. 유지보수 셀의 경우 암호화없이 전송된다. 실제로 이러한 암호화 기법을 적용하여 ATM UNI (Network Node Interface)에서 ATM STM-1 속도(155.52 Mbps)로 인가되는 직렬 입력 셀이 암호화/복호화 처리가 됨을 확인하였다.

References

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

[2] 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

[3] 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, October 1989

[4] Denning, D. E., "Cryptography and Data Security," Addison-Wesley Publishing Co., pp. 138-139, 1983

[5] Daemen, J., and Rijmen, V. "AES Proposal: Rijndael, Version 2," Submission to NIST, March 1999

[6] NIST, "Announcing the Advanced Encryption Standard (AES)," FIPS PUB 197, 2001

[7] William Stallings, "Cryptography and Network Security:Principles and Practice," Pearson Education Inc., pp.187-189, 2014

[8] Suh Jeong-Wook, Kim Kyeong-Soo, "Information protection at ATM physical layer," JKIISC, Vol 7, No 1, Mar. 1997

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

[10] Sin Hyeo-Bin, Yoo Hwang=Bin, "A Study on the Structure and Cryptographic Algorithm for Secrets in ATM-type High-Speed Communication Networks," JKICS, Vol 23, No. 1, May 1998

[11] Im Sung-Yeal, Chung Ki-Dong,"ATM cell Encryption Method using Rijndael Algorithm in Physical Layer," KIPS, Vol 13-c, No.1, Feb., 2006

[12] Forouzan, B., "Security for Computer Networking," John Willy & sons, pp. 231-234, 2008

[13] Forouzan, B., "Security for Computer Networking," John Willy & sons, pp. 236-238, 2008

[14] Forouzan, B., "Security for Computer Networking," John Willy & sons, pp. 236-237, 2008

[15] Rainer Handel, Manfred N.Huber and Stefan Schroder, "ATM Networks: Concepts, Protocols, Applications," Addison-Wesley Publishing Co., pp. 88-95, 1994

[16] Forouzan, B., "Security for Computer Networking," John Willy & sons, pp. 236-237, 2008

[17] Newman, P.,"ATM Technology for Corporate Networks," IEEE Commu-

nications Magine, Vol.30, No.4, pp.90~101, Apr.,1992
〔18〕 Handel,R."Operation and Maintenance Issues of ATM Networks," Proc. of the International Conference on Communication Technology, Beijing, 1992, Vol.1, pp1107~1117, 1992
〔19〕 Rainer Handel, Manfred N.Huber and Stefan Schroder, "ATM Networks: Concepts, Protocols, Applications," Addison-Wesley Publishing Co., pp. 88-95, 1994
〔20〕 ISO 9160 "Information processing - Data encipherment - Physical layer interoperability requirement," International Standards Organization, 1988
〔21〕 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
〔22〕 ITU-T:recommendation I.432. 'B-ISDN User-Network Interface-Physical Layer Specification,' Rev. 1, Geneva, 1993

〈저 자 소 개〉

임 성 렬 (Sung-Yeal Im) 정회원
1983년 2월: 서울대학교 전자공학과 학사
1992년 8월: 포항공과대학교 전자전기공학과 석사
2005년 8월: 부산대학교 이학박사
2012년 9월~현재: 부산대학교 교양교육원 비전임교수
〈관심분야〉 정보보호, 네트워크 보안, 암호용 ASIC 설계