https://doi.org/10.33778/kcsa.2021.21.4.015

군 통신에 적용 가능한 비밀 키 분배 기능을 갖는 디지털 음성 데이터 보안 기법

임 성 렬*

요 약

군의 음성 통신망에서 음성 통신 내용의 보안은 필수적일 것이다. 군 통신망의 음성 데이터 보안에 대해 제안된 연구는 없으나 통신 시에 음성 데이터의 보안은 필수적으로 요구될 것이다. 본 논문은 군내 통신망에서 음성 통화 시 보안을 제공하기 위한 디지털 음성 데이터의 암호화/복호화 기법에 관한 것이다. 또한 AES를 이용한 대칭키 알고리즘을 사용함으로써 비밀 키가 필요한 데 이 키를 음성 통화로 설정 전에 수신단으로 송신하는 기능을 가져 비밀 키 분배의 어려움을 해결하였다. 본 논문에서는 스트림 암호화 기법 중에서도 동기 상실 시에도 동기 복원이 비교적 용이한 동기식 스트림 암호화 방식을 적용한 디지털 음성 데이터의 보안 기법을 제안한다.

Digital voice data security techniques with secret key distribution function applicable to military communication

Im Sung Yeal*

ABSTRACT

Security of voice communication content in the military's voice communication network will be essential. There is no proposed study on voice data security of military communication networks, but security of voice data will be essential when communicating. This paper is about to an encryption/decryption technique of digital voice data to provide security in case of voice calls in a military communication network. In addition, by using a symmetric key algorithm using AES, a secret key is required, and it has the function of transmitting this key to the receiving end before setting it as a voice call, solving the difficulty of distributing the secret key. This paper proposes a security technique for digital voice data that applies a synchronous stream encryption method that is relatively easy to restore synchronization even in the event of loss of synchronization among stream encryption techniques.

Key words : synchronous stream cipher, voice data encryption, voice data decryption

접수일(2021년 09월 29일), 게재확정일(2021년 10월 28일)

*부산대학교/교양교육원

1. 서 론

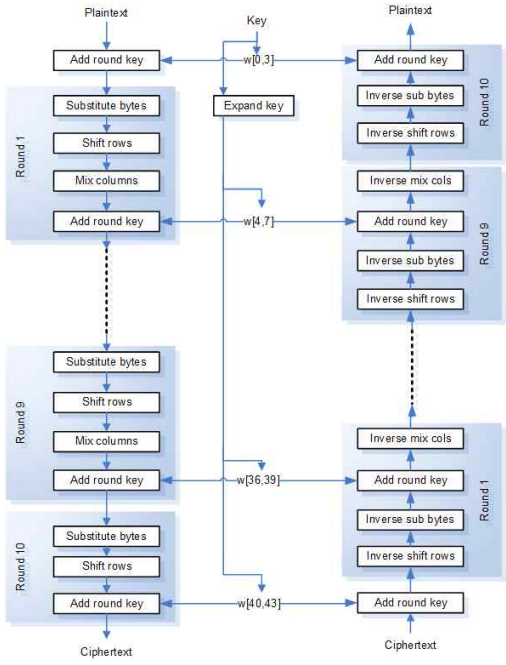
현대 사회가 고도의 정보화 사회로 발전함에 따라 통신망을 통한 정보의 전송량이 급격하게 증가하게 되었다. 이에 따라 중요하고도 가치있는 정보가 통신 도중에 제삼자에게 유출되거나 불법적인 침입자로 인한 도청 및 변조에 대한 대책이 요구되고 있다. 데이터의 보안을 위한 대책으로 데이터를 암호화하는 방법이 사용되는 데 이는 데이터의 형태를 변형함으로써 일반적인 수정을 보완할 수 있기 때문에 가장 안전한 데이터 보안 방법으로 사용되고 있다. 정보의 유출로 인한 정보의 불법적 침해 가능성을 막기 위하여 많은 방법들이 연구되고 있지만 평이한 정보를 암호화된 정보로 변환하여 저장하거나 전송하는 암호학이 오랜 연구를 통하여 구현되어 왔으며 실용화되고 있다[1].

유선망을 이용한 음성 신호 전송 시에 ITU-T의 권고 G.711에 근거한 64 Kbps PCM(Pulse Code Modulation) 기술을 이용한 음성 부호화 방식을 사용하며[2], 이는 파형 부호화 방식의 하나로, 아날로그 음성 신호를 표본화, 양자화, 부호화하여 디지털로 전송하고, 수신 측에서 복호화함으로써 아날로그 음성 신호를 재생하는 방식이다[3]. 음성 데이터는 불법 침입자가 망에 접근하여 데이터를 취득하면 정보의 해석이 용이하므로 망에 접근하여 정보를 취득하더라도 해석이 불가능하도록 하기 위해 데이터를 암호화하여 전송하는 것이 데이터 보안을 위한 하나의 방안이 될 수 있다. 본 논문에서는 부호화되어 전송되는 디지털 음성데이터를 암호화하여 수신단에서 복호화하는 기법에 관한 것이며 데칭 키 암호화를 사용함으로써 수신단에서 복호화가 가능한 비밀 키를 전송하는 기능을 갖는 방식을 제안한다.

2. AES 알고리즘과 OFB(Output Feedback) 운영 방식

2.1 AES 알고리즘

AES 알고리즘은 미국 NIST에서 차세대 암호 알고리즘으로 1997년 AES를 공모하여 2000년에 최종 알고리즘으로 채택하여[4, 5] 현재까지 블록 암호의 표준으로 사용되어 오고 있다. AES 암호 알고리즘은 대칭키 블록 암호 알고리즘으로서 대칭키 길이와 암호화/복호화의 기본 단위인 블록의 크기를 128, 192, 256 비트 중에서 선택할 수 있는 알고리즘으로 알려진 공격에 강하고[6] 블록의 크기에 따라 총 라운드 수를 달리하는 데 각 라운드는 3개의 독립된 변환으로 구성되어 있다.

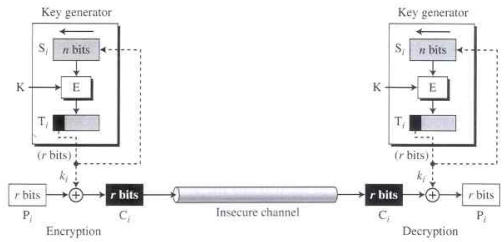


(그림 1) 암호화 라운드가 10인 AES 알고리즘

각 라운드는 바이트 치환, 행의 쉬프트, 열의 혼합 등으로 구성된 단계를 갖는 데, AES 암호 알고리즘은 128, 192 및 256 비트 단위의 가변 키 길이와 블록 길이를 가질 수 있으며 이에 따라 라운드 수가 결정된다[7]. (그림 1)에 암호화 알고리즘의 라운드가 10인 AES 알고리즘의 암호화/복호화 과정을 보여주고 있다.

2.2 AES 블록암호에 OFB(Output Feedback) 모드를 적용한 디지털 음성 데이터 암호화

AES 블록 암호에 적용 가능한 운영 모드 중 본 연구에서 디지털 음성 데이터 암호에 있어서 적용한 OFB 모드를 살펴본다. (그림 2)와 같이 OFB 모드를 구현하여 입력되는 평문과 암호화 키를 바이트 단위로 암호화한 데이터를 비트 단위로 전송이 가능함으로[8] 본 논문에서는 송신단과 수신단에서 AES 소자를 한 개씩 사용하여 바이트 단위의 암호화 키 발생용과 복호화 키 발생용으로 사용하여 스트림 암호로서의 OFB 모드를 구현한다. 본 논문에서는 평문와 키(k_i)를 바이트 단위로 암호화함으로 (그림 2)에서 r의 값은 8 이다.



(그림 2) 스트림 데이터 암호화/복호화를 위한 Output Feesback(OFB)

3. 아날로그 음성 데이터의 디지털 변환

3.1 음성 코딩 방식

음성 신호의 디지털 변환 시에는 아날로그 음성 신호의 표본화, 양자화, 부호화 과정을 거친다. 음성 신호 대역폭이 300 ~ 3400 Hz이므로 8 KHz의 속도로 표본화한 값을 8 비트의 디지털 신호로 변환한 64 Kbps 속도의 PCM 데이터로 변환하여 준다[9]. 음성 신호의 경우는 큰 신호보다 작은 신호가 확률적으로 빈번함으로 양자화 잡음을 줄이기 위해 작은 신호 구간에서는 양자화 간격 구간 크기를 작게 하고 큰 신호에서는 양자화 간격 구간 크기를 크게한 비선형 압축신장기법을 적용한다. 비선형 압축신장기법으로 국내에서는 북미 방식인 μ-law 방식을 사용한다. 식 (1)은 μ-law에 근거한 입력신호(x)와 양자화 값(y)의 관계식이다. μ-law 방식은 작은 신호 구간에서는 거의 선형 특성을 보이며 큰 신호 구간에서는 로그(logarithm) 특성을 지닌다.

$$|y| = \frac{\log(1+\mu|x|)}{\log(1+u)}, \qquad (1)$$

여기서 $x = \frac{\text{입력}}{x_{\max}} \le 1$

(정규화된 입력 값)

여기서 $(1+\mu) = \triangle\max/\triangle\min$, μ=255 이다.

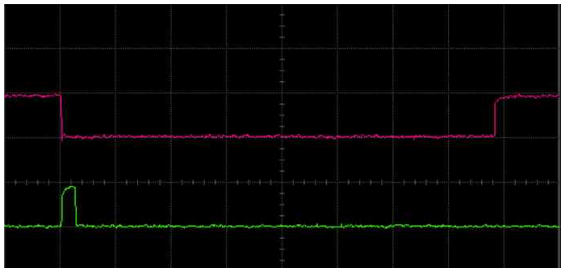
(Δ: 양자화 간격 구간 크기)

3.2 음성 데이터 PCM 전송

음성 신호를 PCM 디지털 신호로 변환·전송하는 소자로 음성 코덱 소자를 사용하는 데 음성 코덱 소자는 아날로그 음성 신호를 μ-law 변환을 거친 후 디지털 음성 데이터로 변환한 후 PCM 전송로 상으로 전송해 준다. μ-law 변환을 거친 디지털 음성 데이터 전송 시 음성 신호 표본화 속도와 동일한 8 KHz주기의 프레임 동기(FS) 신호를 사용하며 배정된 타임슬롯 구간 상에 2.048 MHz 속도의 마스터 클럭(MCLK)으로 디지털 음성 데이터를 전송한다. 다시 말하면 프레임 동기(FS) 신호 구간을 32개의 동일한 타임슬롯으로 나누어 배정된 타임슬롯에 64 Kbps속도의 8 비트 디지털 음성 데이터를 프레임 동기 신호 간격(125 μs)으로 전송한다. 음성 코덱 소자는 제어 단자를 통해 제어 데이터로 타임슬롯 0~31 사이의 타임슬롯 지정이 가능하며 고정 타임슬롯 모드도 가능하다. 고정 타임슬롯 모드를 사용할 경우에는 타임슬롯 0을 배정받는다. (그림 3)에 음성 데이터 전송 클럭과 프레임 동기 신호 및 고정 타임슬롯

모드를 사용할 시에 배정받는 타임슬롯 0 구간을 보여준다. $\overline{TS_x}$ 신호는 코덱 소자가 고정 타임슬롯 모드로 사용될 시에 타임슬롯 0을 배정받으므로 통화로 연결 시에 발생하는 음성 코덱 소자의 $\overline{TS_x}$ 단자의 신호이다. (그림 4)는 프레임 동기 신호와 타임슬롯 신호($\overline{TS_x}$ 신호)를 스크프로 측정한 것이다.

(그림 3) 프레임 동기 신호와 고정 타임슬롯 구간



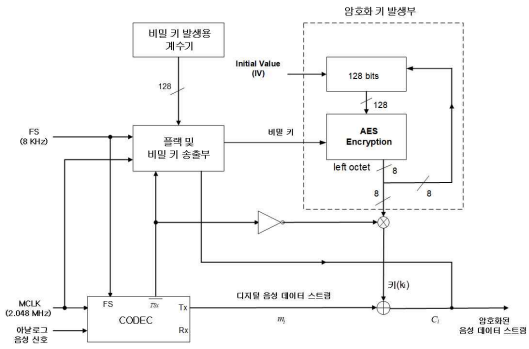
(그림 4) 프레임 동기 신호와 타임슬롯 신호($\overline{TS_x}$ 신호)

4. 디지털 음성 데이터 보안 기법

4.1 디지털 음성 데이터 보안 장치의 구성도

(그림 5)에 디지털 음성 데이터의 동기식 스트림 암호화 과정의 블록도를 도시하였다. 송신측의 음성데이터 보안장치에서 수행하는 기능은 다음과 같다.

- 대칭키 암호화/복호화를 위한 비밀 키를 무작위로 발생시키기 위한 비밀 키 발생용 계수기
- 수신단에 비밀 키를 송출하기 위한 플랙 및 비밀 키 송출부
- 아날로그 음성 신호를 PCM 디지털 데이터로 변화하여 FS로 지정된 원하는 타임슬롯으로 전송하여 주는 CODEC 회로부
- 디지털 음성 데이터 스트림과 암호화를 위한 암호화 키를 발생시키기 위한 AES 암호화부를 포함하는 OFB 방식을 적용한 암호화 키 발생부 기능으로 구성되어 있다.



(그림 5) 디지털 음성 데이터의 동기식 스트림 암호화 과정의 블록도

4.2 디지털 음성 데이터 암호화 과정

(그림 5)의 디지털 음성 데이터의 동기식 스트림 암호화 과정의 블록도에서 암호화의 원리를 설명한다. (그림 5)의 CODEC 소자로 입력되는 아날로그 음성 신호는 CODEC 회로부에서 PCM 변환된 후 고정 타임슬롯인 타임슬롯 0 를 배정받아 데이터가 전송되게 된다. 그러므로 디지털 음성데이터를 키와 암호화할 때 타임슬롯 0의 데이터만 암호화하여 주고 나머지 타임슬롯(1-31)은 암호화하지 않아야 한다. 이를 위해 TS 신호를 이용하여 타임슬롯 0 구간만 인에이블되게 하여야 한다.

4.2.1 코덱(CODEC) 회로부

음성 코덱 소자는 제어 단자의 제어를 통해 고정 타임슬롯 모드로 설정되어 운용되며 아날로그 음성신호를 8 비트의 디지털 음성 데이터로 변환한 후 (그림

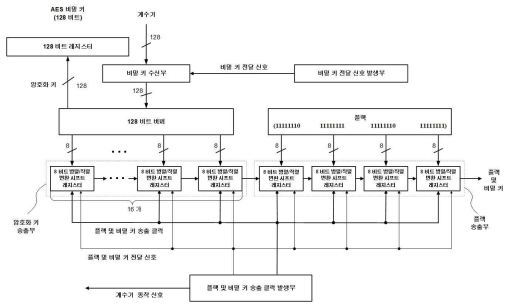
3)의 타임슬롯 0으로 전송한다. 따라서 키(k_i) 스트림과 타임슬롯 0 구간의 디지털 음성 데이터 스트림을 비트 단위로 XOR 연산을 거쳐 암호화하여 전송하며 수신단에서는 송신단의 키(k_i) 스트림과 동일한 키(k_i) 스트림으로 타임슬롯 0의 디지털 음성 데이터를 비트 단위로 XOR 연산을 하여 복호화한다. 이를 위해 송신단과 수신단 계수기의 동기를 맞추는 것이 중요하며 이를 위해 코덱 소자에서 타임슬롯 지정의 기준이 되는 프레임 동기 신호(FS)와 마스터 클럭(MCLK)을 플랙(flag) 및 비밀 키 송출부에 인가한다.

4.2.2 비밀 키 발생용 계수기

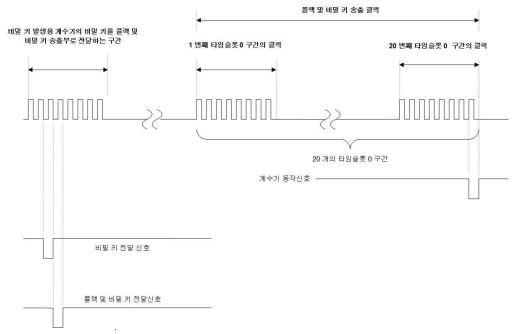
비밀 키 발생용 계수기는 비밀 키 생성을 무작위로 발생시키기 위한 계수기로 장치에 전원이 인가되는 순간부터 동작을 시작하여 통화로 연결 시 발생하는 $\overline{TS_x}$ 신호를 이용하여 $\overline{TS_x}$ 신호 발생 순간의 계수기의 출력을 암호화/복호화를 위한 비밀 키로 설정이 되게 하여 비밀 키를 무작위적으로 설정한다.

4.2.3 플랙 및 비밀 키 송출부

플랙 및 비밀 키 송출부는 통화로 설정 직후 디지털 음성 데이터가 전송되기 전에 암호화 시에 사용할 비밀 키를 수신단에 송출하는 기능을 한다. 비밀 키 송신 전에 수신단에 비밀 키 전송을 알려주기 위한 플랙 패턴을 송출한다. 플랙 패턴은 4 바이트로 구성되며 타임슬롯 0 에 바이트 단위로 4 회로 나누어 송출한다. 음성 신호는 특성상 급격한 신호의 변화가 없으므로 음성 신호의 연속적인 특성을 이용하여 양(+)의 최대 신호(11111111)와 음(-)의 최대 신호(01111111)의 패턴을 번갈아 각 2 회씩 반복한 패턴(11111111 01111111 11111111 01111111)을 플랙 패턴으로 사용한다. (그림 6)에 플랙(flag) 및 비밀 키 송출부의 블록도를 도시하였다. 코덱 소자가 통화로 설정을 위해 타임슬롯을 배정받으면 코덱 소자의 $\overline{TS_x}$ 단자는 배정받은 타임슬롯 구간은 로직 0 이고 나머지 타임슬롯 구간은 로직 1이 되는 $\overline{TS_x}$ 신호를 발생하여 송·수신을 위한 준비가 되었음을 알려주며 고정 타임슬롯 모드를 사용할 경우 타임슬롯 0 구간이 로직 0 이 된다. 통화로 설정을 위한 $\overline{TS_x}$ 신호의 타임슬롯 0 구간이 로직 0 인 상태로 전이하면 (그림 7)의 비밀 키 전달 신호 발생부에서 이를 감지하여 (그림 8)의 비밀 키 전달 신호를 발생시켜 비밀 키 발생용 계수기의 128 비트의 출력 데이터를 비밀 키 수신부로 전달하며 비밀 키 수신부로부터 전달받은 128 비트의 비밀 키는 8 비트 단위의 16 개로 나누어 8 비트 단위로 한 총 128 비트의 비밀 키가 128 비트 버퍼의 출력단에 도달하여 있게 된다.



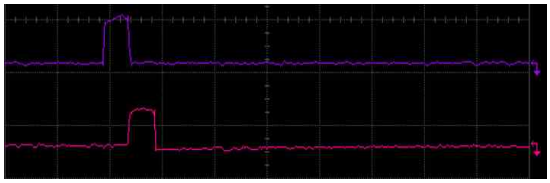
(그림 6) 플랙(flag) 및 비밀 키 송출부의 블록도



(그림 7) 플랙(flag) 및 비밀 키 송출부의 내부 신호 타이밍도

그런 다음 플랙 및 비밀 키 전달 신호를 (그림 7)에서와 같이 비밀 키 전달 신호 다음의 MCLK 클럭 한

주기 동안 로직 '0'이 되는 신호를 생성하여 이 신호로 (그림 6)의 128 비트 버퍼 출력단의 비밀 키를 비밀 키 송출부와 플랙 송출부로 각각 전달한 후 플랙 및 비밀 키 송출 클럭으로 16 개의 타임슬롯 0 구간에 걸쳐 전송한다. 비밀 키의 마지막 비트를 송출한 MCLK 클럭의 한 주기 동안 로직 '0'인 계수기 동작 신호를 발생하여 이를 계수기에 인가하여 계수기를 동작시킨다. 이 계수기의 출력은 동기식 스트림 암호화 키 생성을 위해 AES 소자에 128 비트 단위의 블록 입력으로 사용되며 AES 송출부의 소자의 128 비트 블록 출력 중 한 비트(비트 1)가 암호화 키(k_i) 스트림이 되며, 수신단에서도 복호화를 위한 키(k_i) 스트림이 송신단의 키(k_i) 스트림과 패턴이 동일해야 하므로 수신단의 계수기 동작 신호도 (그림 11)의 송신단의 계수기 동작 신호와 같게 비밀 키의 마지막 비트를 수신하는 MCLK 클럭의 상승 모서리에서 MCLK클럭의 한 주기 동안 발생한다. (그림 8)은 비밀 키 전달 신호 및 플랙(flag) 및 비밀 키 전달 신호를 스코프로 측정한 신호이다.



(그림 8) 비밀 키 전달 신호 및 플랙(flag) 및 비밀 키 전달 신호

4.2.4 암호화 키 발생부

계수기는 플랙 및 비밀 키 송출부의 계수기 동작 신호에 초기화 값을 전달받아 동작을 시작하며 128 비트의 블록 데이터를 AES 암호화 소자의 입력으로 인가한다. AES 암호화부는 플랙 및 비밀 키 송출부가 전달해 준 128 비트의 비밀 키를 사용하여 계수기부로부터 전달받는 128 비트 블록 단위의 데이터를 AES 알고리즘으로 암호화하여 128 비트 블록 단위의 데이터를 출력한다. 이 데이터를 암호화한 128 비트 단위의 출력 데이터 중 8 비트 단위로 AND 회로의 입력단자에 인가하여 $\overline{TS_x}$ 신호와 AND 연산을 하여 준다. $\overline{TS_x}$ 신호는 타임슬롯 0 구간은 로직 '0'이고 나머지 구간은 로직 '1' 인 신호임으로 8 비트 단위의 AND 출력 단자의 값은 타임슬롯 0 구간 동안은 0 이 되고 그 외 구간은 k_i 값이 된다. AND 출력 단자의 값은 디지털 음성 데이터 스트림과 암호화를 위한 키(k_i)가 되며 이는 타임슬롯 0 구간 동안은 AES 암호화부의 출력 단자 8 비트 단위의 값이 키(k_i)가 되며 그 외 구간은 키(k_i)가 '0'이 됨을 의미한다. 이는 타임슬롯 0 구간은 디지털 음성데이터 스트림이 키(k_i)로 암호화되며, 그 외 구간은 키(k_i) 값이 '0' 이므로 디지털 음성 데이터 스트림을 키(k_i)와 XOR한 연산은 암호화를 하지 않은 것과 동일하다. 수신 측에서도 송신 측과 동일한 구조로 구성하면 복호화가 가능하다. 프레임 동기 신호는 송·수신 측이 동일한 신호를 사용한다.

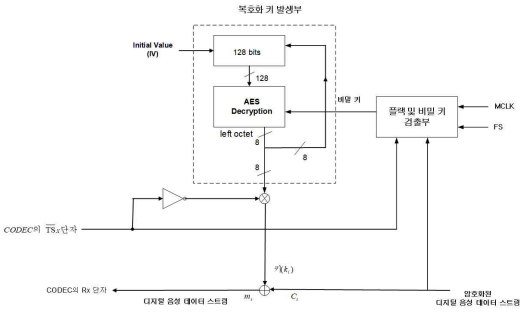
4.3 디지털 음성 데이터의 복호화 과정

수신측의 복호화 과정도 송신측의 암호화 과정과 유사한 과정을 거친다. 송신단에서 타임슬롯 0의 디지털 음성 데이터를 키(k_i)와 XOR 연산하여 암호화하여 전송함으로 수신단에서는 송신단의 키(k_i) 스트림과 동기가 일치하는 키(k_i) 스트림을 생성하여 이를 타임슬롯 0의 디지털 음성 데이터와 XOR 연산을 하여 음성 데이터를 복호화한다.

(그림 9)에 복호화 과정의 블록도를 도시하였다. 플랙 및 비밀 키 검출부에서는 암호화된 디지털 음성 데이터를 분기점을 통해 수신하여 플랙 패턴을 검출하여 비밀 키를 분리하여 비밀 키를 AES 암호화부로 전달한다. AES 암호화부에서는 계수기로부터 128 비트 블록 단위의 데이터를 입력받아 AES 알고리즘으로 암호화하여 128 비트 블록 단위로 출력하며 이 중 8 비트를 AND 회로의 입력단자 0으로 인가하여 반전 $\overline{TS_x}$ 신호와 AND 연산을 수행하면 타임슬롯 0 구간은 AES 암호화부 출력의 8 비트이고 그 외 구간은 0인 복호화 키(k_i)가 생성된다. (그림 10)

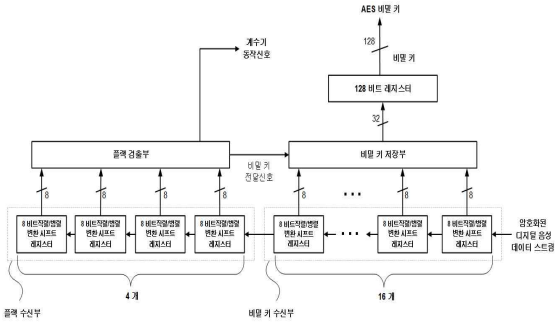
은 플랙 및 비밀 키 검출부의 내부 블록도이다.

(그림 10)에서 분기점을 통해 플랙 및 비밀 키 검출부로 직렬로 입력되는 암호화된 디지털 음성 데이터 스트림은 (그림 10)의 비밀 키 수신부를 거쳐 플랙 수신부에 입력되며 20 번째 타임슬롯 0 구간의 8 번째 클럭의 상승 모서리에서 8 비트 직렬/병렬 변환 시프트 레지스터 4 개로 구성된 플랙 검출부에 4 바이트의 플랙이 모두 입력된다. 이때 플랙이 검출되어 (그림 11)의 MCLK 클럭의 한 주기 동안 로직 0 인 플랙 검출 신호가 발생한다. 이 시점에는 비밀 키가 (그림 10)의 비밀 키 수신부의 16 개의 8 비트 직렬/병렬 변환 시프트 레지스터의 내용으로 직렬로 입력되어 도달하여 있다.



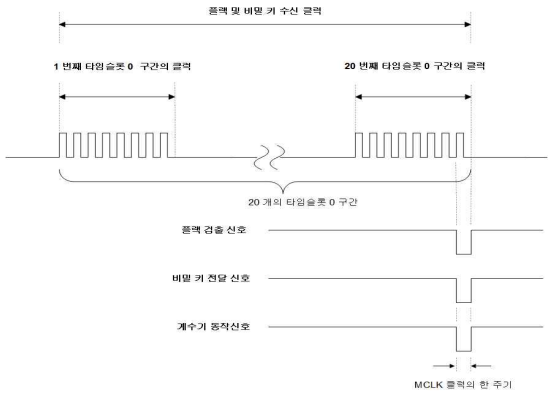
(그림 9) 수신단의 복호화 과정의 블록도

(그림 10)에서 분기점을 통해 들어온 플랙 및 비밀 키를 플랙 검출 신호를 전달 신호로 사용하여 이를 비밀 키 저장부에 인가하면 비밀 키 수신부의 내용으로 입력되어 있는 128 비트의 비밀 키가 비밀 키 저장부의 출력단으로 전달되게 된다. 한편 (그림 11)의 플랙 검출 신호를 수신단의 계수기에 인가하여 계수기를 동작시키면 송신단의 계수기의 동작 시점과 일치하여 암호화 시에 사용한 키(k_i)와 동일한 스트림의 키(k_i)가 생성된다. 계수기는 계수기 동작 신호에 초기값을 전달받아 동작을 시작하며 128 비트 단위의 블록 데이터를 AES 암호화부에 제공하여 준다. AES 복호화 키 발생부에서는 이 데이터를 복호화하여 128 비트 블록 단위로 출력하며 이 중 8 비트 단위로 AND 회로의 입력단자로 인가하여 반전 $\overline{TS_x}$ 신호와 AND 연산을 수행하면 타임슬롯 0 구간은 AES 암호화부 출력의 8 비트 단위이고 그 외 구간은 0 인 복호화 키(k_i)가 생성된다.



(그림 10) 플랙 및 비밀 키 검출부의 내부 블록도

이 키(k_i)와 디지털 음성 데이터 스트림을 XOR 연산하면 비밀 키를 수신한 다음 프레임부터 입력되는 타임슬롯 0의 암호화된 디지털 음성 데이터 스트림이 복호화된다.



(그림 11) 수신단의 계수기 동작 신호 생성 타이밍도

5. 결 론

본 논문에서는 일반적으로 암호화하지 않는 E1급(2.048Mbps) 속도의 디지털 음성 데이터를 동기식 암호화 기법을 적용하여 암호화하여 전송하고 수신단에서는 이를 수신하여 복호화가 가능함을 보였다. 계수기 모드의 동기식 암호화 기법을 사용하여 고정 타임슬롯을 배정받은 디지털

음성 데이터 스트림을 비트 단위로 암호화하여 전송하고 수신단에서는 이를 복호화하여 암호화되기 전의 디지털 음성 데이터 스트림을 복원하는 기법을 소개하였다. 또한 비밀 키 무작위 설정 및 송출 기능을 가져 비밀 키를 통화로 설정시마다 다르게 무작위로 선정하여 암호화 시에 사용하고 음성 통화로 형성 전에 플랙 패턴을 송출한 후 비밀 키를 송신하는 기법을 적용하여 수신단에서 비밀 키의 수신 오류를 방지하여 통신의 신뢰성 및 기밀성 향상을 기하였다. 본 기법은 교환 기능이 배제된 점대점 통신을 사용하는 군 통신 분야의 음성 데이터 보안에 적용이 가능할 것이다.

참고문헌

[1] William Stallings, “Cryptography and Network Security”, Pearson Education Inc., pp.15-17, 2013.

[2] Behrouz A. Forouzan,“ Data communications and Netrworking,” Focal Press, pp103-104, 2003.

[3] N.S. Jayant, and P. Noll,“Digital Coding of Waveforms,” Mcgrawhill, pp 120-129,, 2007.

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

[5] Daemon, J., and Rijmen, V., “Rijndael: The Advanced Encryption Standard,” Dr Dobb’s Journal, Mar., 2001.

[6] 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.

[7] Daemen, J., and Rijmen, V. “The Design of Rijndael: The Wide Trail Strategy Explained,“ NewYork,Springer-Verlag, 2002.

[8] William Stallings, “Cryptography and Network Security”, Pearson Education Inc., pp.185-192, 2013.

[9] David Austerberry“ Video & Audio Streaming,” Focal Press, pp.101-102, 2003.

〔저자소개〕

임 성 렬 (Sung-yeal Im)
1983년 2월 서울대학교 전자공학과 (공학사)
1992년 8월 포항공과대학교 전자전기공학과(공학석사)
2005년 8월 부산대학교 이학박사
2021년 현재 부산대학교 교양교육원 비전임교수
E-mail : syim7@pusan.ac.kr