JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 24(2): 134-141, Apr. 2020

ARIA 암호 알고리즘을 이용한 원격측정 시스템 암호화 기법

Telemetry System Encryption Technique using ARIA Encryption Algorithm

최 석 훈* · **이 남 식** · **김 복 기**
단암시스템즈(주) 기술연구소

Seok-Hun Choi* · **Nam-Sik Lee** · **Bok-Ki Kim**
R&D Center, DANAM Systems, Gyeonggi-do, 13930, Korea

[요 약]

원격측정 시스템은 무인기, 위성 발사체 등의 비행체 개발과정에서 비행 데이터 수집과 모니터링을 위해 비행체 내 다양한 신호를 계측하여 지상으로 전송하는 통신시스템이다. 최근 무선통신 기술의 발전으로 비행 데이터의 전송 과정에서 일어날 수 있는 보안 위협에 대응하기 위해 원격측정 시스템의 암호화 기술 적용은 중요해지고 있다. 따라서 본 논문에서는 원격측정 시스템의 암호화 적용을 위해 국가 표준 암호 알고리즘인 ARIA-256의 적용 방법을 제안하고 구현하였다. 블록 오류 확산과 원격측정 프레임의 특성을 고려하여 CTR (counter) 모드를 응용하고, 위성통신 표준화 기구(CCSDS)에서 권장하는 리드솔로몬 코드를 적용할 수 있도록 프레임을 구성하여 암호화하였다. ARIA-256 알고리즘과 암호 프레임은 FPGA(filed programmable gate array)로 구현하였고 시뮬레이션과 하드웨어 검증 시스템을 통해 연속성 있는 프레임의 암호화를 확인하였다.

[Abstract]

Telemetry system is a communication system that measures and transmits various signals in the aircraft to the ground for collecting and monitoring flight data during the development of unmanned air vehicle and satellite launch vehicles. With the recent development of wireless communication technology, it is becoming important to apply encryption of telemetry system to prepare with security threats that may occur during flight data transmission. In this paper, we suggested and implemented the application method of ARIA-256, Korean standard encryption algorithm, to apply encryption to telemetry system. In consideration of the block error propagation and the telemetry frame characteristics, frame is encrypted using the CTR mode and can apply the Reed-solomon codes recommended by CCSDS. ARIA algorithm and cipher frame are implemented in FPGA, and simulation and hardware verification system confirmed continuous frames encryption.

Key words : Telemetry system, ARIA-256, Frame encryption, CTR mode.

https://doi.org/10.12673/jant.2020.24.2.134

Received 24 March 2020; **Revised** 25 March 2020
Accepted (Publication) 21 April 2020 (30 April 2020)

***Corresponding Author; Seok-Hun Choi**

Tel: +82-31-538-6056
E-mail: choi6946@danam.co.kr

Ⅰ. 서 론

원격측정 시스템은 비행체의 센서 신호와 상태 신호를 계측하고 영상 데이터를 처리하여 전송하는 탑재 원격측정장치와 지상에서 데이터를 수신하여 처리하는 지상 점검장비로 이루어진 통신 시스템이다[1]. 실시간 비행 데이터 전송과 비행체 상태 모니터링을 목적으로 위성 발사체, 항공 무인기 등의 개발 과정에 사용되고 있으며, 항공우주산업과 방위산업의 비행체 개발에 중요한 역할을 하고 있다. 원격측정 데이터를 지상으로 송신하는 과정에서 허가되지 않은 제3자가 데이터를 무단으로 획득하면 비행 정보가 누출될 수 있으며 데이터의 기밀성 보장을 위해 원격측정 시스템의 암호화 보안 기술 적용은 점차 중요해 지고 있다. 국내에서는 비행체 명령신호의 기밀성을 위해 비행종단시스템과 명령 처리기의 암호화에 대한 연구는 진행되었지만[2], 원격측정 시스템의 데이터 암호화에 대한 구체적인 연구는 진행이 필요하다. 따라서 본 논문은 원격측정 시스템의 암호화 적용 방법을 제안하고 구현하였다.

보안 기술 적용을 위한 암호 방식은 대칭키 암호, 비 대칭키 암호, 단방향 해시(hash) 함수 등 다양한 암호 기술들이 사용되고 있다. 대칭키 암호는 암호화와 복호화에 동일한 키를 사용하여 기밀성을 제공하는 기본적인 암호 방식이고, 비 대칭키 암호는 정보 송/수신자가 공개된 키와 자신의 비밀 키를 사용하여 암호화와 복호화를 진행하는 방식으로 전자서명과 같은 인증에 주로 사용이 된다[3]. 원격측정 시스템은 정해진 시간에 데이터를 처리하는 실시간 처리가 요구되기 때문에 암호화 과정에서 병목현상이 없어야 하며 이를 위해 처리 속도가 빠른 하드웨어 환경에서 구현이 가능해야 한다. 이에 적절한 방식은 대칭키 암호 방식이며, 미국 표준 블록 알고리즘인 AES (advanced encryption standard), 국가 표준(KS; Korean industrial standards) 블록 알고리즘인 ARIA (academy, research institute, agency), 경량 블록 알고리즘인 LEA(lightweight encryption algorithm)가 대표적이다. ARIA 알고리즘은 AES 알고리즘과 비교하여 하드웨어 환경에서 동등한 수행 속도를 보이며, 16×16 이진 행렬을 이용하여 기존 블록 암호 알고리즘과 차별성이 있으며 국가 표준으로 제정되어 여러 분야에 사용되고 있다[4]. ARIA 암호 알고리즘은 암호화와 복호화가 일정한 크기의 블록으로 진행되기 때문에 연속성 있는 프레임으로 구성된 원격측정 데이터를 암호화하려면 적절한 블록 암호 운용 모드를 선정해야 하고 복호화 과정에서 오류 확산을 고려해야 한다. 따라서 기밀성이 높고 인접 블록으로 오류 확산이 없는 CTR 모드를 응용하여 프레임을 암호화하였고, 전송 과정에서의 오류를 정정하기 위해 위성통신 표준화 기구 (CCSDS; Consultative Committee for Space Data Systems)에서 권장하는 리드솔로몬 코드가 적용 가능하도록 프레임을 구성하였다.

본 논문의 구성은 제 Ⅱ 장에서 ARIA 알고리즘에 대한 설명과 ARIA-256 설계 그리고 본 논문에서 제시하는 원격측정 시스템의 암호화 방법에 대해 기술한다. 제 Ⅲ 장에서는 제안된 원격측정 시스템의 암호화 방법을 FPGA에 로직으로 구현하여 하드웨어 동작을 검증하고, 제 Ⅳ장에서는 결론을 맺는다.

Ⅱ. ARIA-256 설계 및 원격측정 시스템 적용 방안

본 논문은 원격측정 시스템의 암호화 적용을 위해 ARIA 알고리즘의 구조와 ARIA-256의 설계, 암호화를 위한 프레임 구조의 설계에 대해 기술한다.

2-1 ARIA 알고리즘의 구조[5]

ARIA 알고리즘은 involution SPN (substitution permutation network) 구조의 대칭키 방식의 블록 알고리즘으로 128 비트의 블록을 가지며 128 비트, 192 비트, 256 비트의 키 선택이 가능하다. involution 구조는 암호화와 복호화 과정이 동일한 구조이며, SPN 구조는 비선형 치환 테이블인 S-box를 이용한 치환과 확산이 반복되는 구조로 하드웨어 구현에 적합하다. ARIA 알고리즘의 암호화와 복호화 전체 과정은 그림 1과 같으며 키의 크기에 따라 12, 14, 16 라운드로 진행이 된다. 각 라운드는 라운드 함수와 라운드 키로 진행이 되는데 암호화는 라운드 키 ek가 사용이 되고 복호화는 dk가 사용이 된다. 라운드 함수는 라운드 키 XOR(exclusive OR)연산, 치환 계층(substitution layer), 확산 계층(diffusion layer)으로 구성이 되며 마지막 라운드 F_f는 확산 계층 대신 라운드 키 XOR 연산을 진행한다.

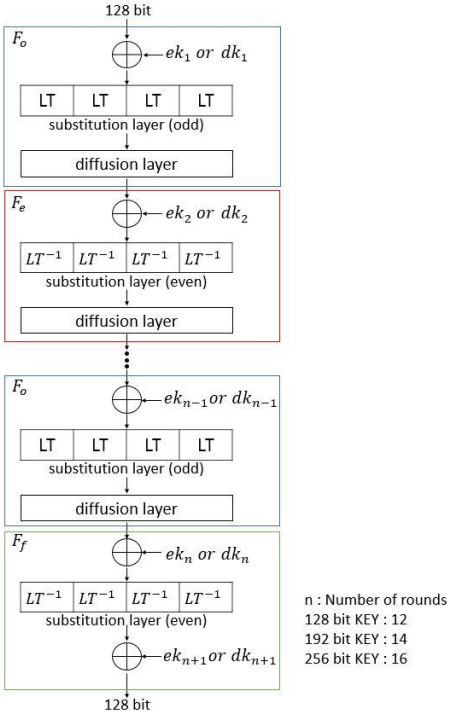

그림 1. ARIA의 암호화 복호화 처리과정
Fig. 1. Encryption and decryption of ARIA process.

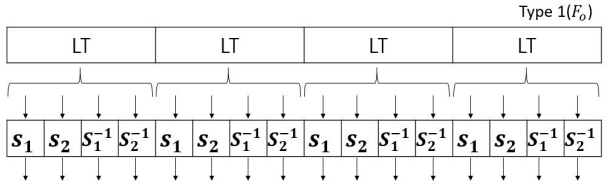

그림 2. 유형 1 홀수 라운드 치환 계층
Fig. 2. Type 1 odd-round substitution layer.

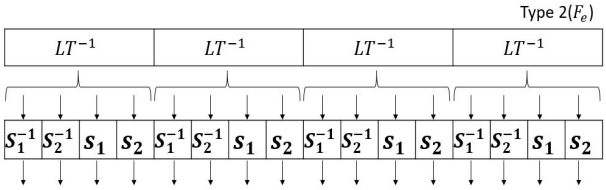

그림 3. 유형 2 짝수 라운드 치환계층
Fig. 3. Type 2 even-round substitution layer.

치환 계층은 두 가지 유형이 있으며, 그림 2의 유형 1은 홀수 라운드 함수 F_o(odd)에 사용이 되고, 그림 3의 유형 2는 짝수 라운드 함수 F_e(even)에 사용이 된다. 두 유형의 치환 계층은 LT, LT^{-1}치환 함수로 구성이 되며, 각 함수는 8 비트 입/출력을 가진 S-box S_1, S_2, S_1^{-1}, S_2^{-1}로 세부 구성이 된다. 치환 함수 LT와 LT^{-1}은 서로 역 치환 관계로 암호화의 involution 구조가 가능하도록 한다. 확산 계층은 그림 4와 같이 16×16 involution 이진 행렬 A를 사용하여 바이트 단위의 행렬 곱셈을 수행하는 계층으로 16 바이트 입력에 대하여 16 바이트 출력을 한다.

암호화와 복호화의 각 라운드에 사용되는 라운드 키 ek와 dk는 키 확장을 통해 생성이 된다. 키 확장은 키 초기화와 라운드 키 생성 두 단계로 진행이 되며, 키 초기화는 그림 5와 같이 3개 라운드를 가진 feistel 구조를 연산하여 진행한다. 그 결과 128 비트의 W0, W1, W2, W3이 생성되고 이를 식 (1)과 같이 연산하여 라운드 키 ek가 생성된다.

$$
\begin{aligned}
ek_1 &= (W_0) \oplus (W_1^{\gg 19}), \quad ek_2 = (W_1) \oplus (W_2^{\gg 19}) \\
ek_3 &= (W_2) \oplus (W_3^{\gg 19}), \quad ek_4 = (W_0^{\gg 19}) \oplus (W_3) \\
ek_5 &= (W_0) \oplus (W_1^{\gg 31}), \quad ek_6 = (W_1) \oplus (W_2^{\gg 31}) \\
ek_7 &= (W_2) \oplus (W_3^{\gg 31}), \quad ek_8 = (W_0^{\gg 31}) \oplus (W_3) \\
ek_9 &= (W_0) \oplus (W_1^{\ll 61}), \quad ek_{10} = (W_1) \oplus (W_2^{\ll 61}) \\
ek_{11} &= (W_2) \oplus (W_3^{\ll 61}), \quad ek_{12} = (W_0^{\ll 61}) \oplus (W_3) \\
ek_{13} &= (W_0) \oplus (W_1^{\ll 31}), \quad ek_{14} = (W_1) \oplus (W_2^{\ll 31}) \\
ek_{15} &= (W_2) \oplus (W_3^{\ll 31}), \quad ek_{16} = (W_0^{\ll 31}) \oplus (W_3) \\
ek_{17} &= (W_0) \oplus (W_1^{\ll 19})
\end{aligned} \tag{1}
$$

복호화에 사용되는 dk는 ek로부터 식 (2) 연산을 통해 유도가 되는데 키의 순서가 바뀌고 확산 계층의 이진 행렬 A로 연산하여 생성이 된다.

$$
\begin{aligned}
&dk_1 = ek_{n+1},\ dk_2 = A(ek_n),\ dk_3 = A(ek_{n-1}) \cdots, \\
&dk_n = A(ek_2),\ dk_{n+1} = ek_1
\end{aligned} \tag{2}
$$

$$
\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} =
\begin{pmatrix}
0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0 \\
0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1 \\
0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\
1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\
1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\
0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\
1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\
0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\
1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\
1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\
0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1 \\
0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\
0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\
1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\
1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\
0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1
\end{pmatrix} \cdot
\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}
$$

그림 4. 확산계층의 이진행렬 A
Fig. 4. Binary matrix A of diffusion layer.

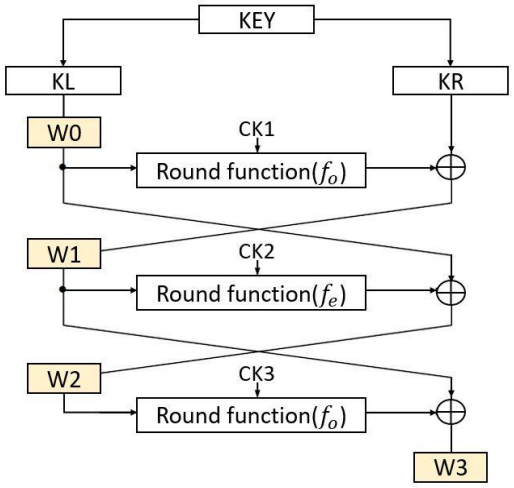

그림 5. 키 초기화 과정
Fig. 5. Process of KEY initialization.

2-2 ARIA-256 알고리즘 로직 설계

본 논문은 원격측정 시스템을 암호화하기 위해 보안성이 가장 높은 256 비트 암호 키를 사용하여 16 라운드로 암호화를 진행하는 ARIA-256을 설계하였다. 설계된 ARIA-256 암호 로직의 구조는 그림 6과 같으며, 암호화와 복호화의 구조가 같은 involution 구조의 장점을 활용하여 하나의 로직이 라운드 키 생성 모드에 따라 암호화와 복호화가 모두 가능하도록 설계 하였다. 256 비트 암호 키는 바이트 단위로 입력을 받고 명령 신호에 따라 연산하여 암호화 라운드 키 ek와 복호화 라운드 키 dk로 확장이 된다. 확장된 17개의 라운드 키는 FPGA 내부 램에 임시 보관되어 매 라운드에 사용이 되며, 3개의 계층으로 설계된 라운드 함수는 블록 단위로 순환하여 암호화와 복호화를 진행 한다. 이때 마지막 라운드는 확산 연산 대신 XOR 연산을 진행하여 최종 암호문을 만든다. 평문의 입력은 바이트 단위 연산과 병렬처리를 위해 하나의 블록을 32 비트 4개의 열로 분리하였고, 출력도 동일하게 4개의 열을 하나의 블록으로 구성하였다. 설계 검증은 규격서의 테스트 벡터를 통해 진행하였고 결과는 제 Ⅲ장에서 확인할 수 있다.

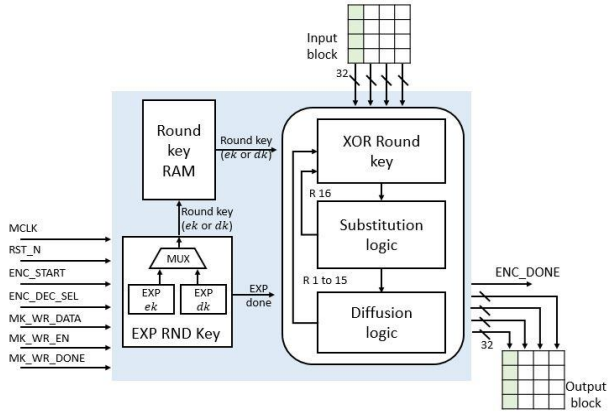

그림 6. ARIA-256 암호 로직 구조
Fig. 6. Structure of ARIA-256 encryption logic.

2-3 ARIA-256 적용을 위한 프레임 구조 설계

원격측정 시스템은 데이터를 PCM(pulse code modulation) / FM(frequency modulation) 변조 방식으로 전송을 하는데, 데이터 전송 과정에서 여러 환경 조건의 영향으로 수신 SNR(signal to noise ratio)의 변화가 생길 수 있다. 이는 데이터 전송 오류를 발생시키고 암호화된 데이터의 복호화 과정에서 블록 전체 혹은 인접 블록으로 오류를 확산 시킨다. 따라서 원격측정 프레임의 ARIA-256 적용을 위해서는 오류 확산이 최소화 되는 운용 모드를 선정해야 하고, 동일한 SNR에서 낮은 BER(bit error ratio) 성능을 위해 오류 정정이 가능한 프레임 구조가 필요하다. 이를 위해 본 논문은 CTR 암호 모드를 응용하고, CCSDS에서 권장하는 오류 정정 방식 중 하나인 리드솔로몬 코드가 적용 가능한 프레임 구조를 제안하고 설계하였다. CTR 모드는 그림 7과 같이 1씩 증가하는 난수를 암호화하여 키 스트림을 만들고 평문과 XOR 비트 연산하여 암호화와 복호화를 진행한다. 따라서 블록 내부와 인접 블록으로 오류 확산이 없고, 원격측정 프레임의 특성에 맞추어 싱크 채널과 리드솔로몬 체크 비트 등 블록 내 암호화가 불필요한 워드를 구분하여 암호화할 수 있기 때문에 원격측정 시스템에 적합한 방식이다. 리드솔로몬 오류 정정 코드는 연집 오류와 랜덤 오류의 우수한 정정 능력을 가지고 있으며, CCSDS에서는 오류 정정 능력에 따라 표 1과 같이 두 개의 옵션을 권장하고 있다[6].

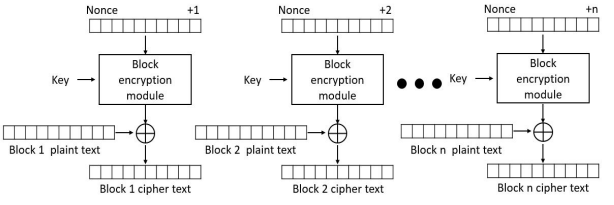

그림 7. CTR 모드 암호화 과정
Fig. 7. Process of CTR mode encryption.

표 1. CCSDS에서 권장하는 리드솔로몬 옵션
Table 1. Recommended Reed-solomon option by CCSDS.

Option	Bits per symbol	Symbols per code word	Parity (symbols)	Error correct (symbols)
Maximum performance	8	255	32	16
Lower overhead	8	255	16	8

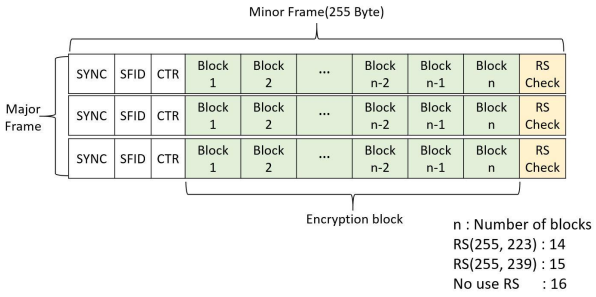

그림 8. 원격측정시스템 프레임 구조
Fig. 8. Structure of telemetry system frame.

원격측정 시스템의 IRIG-106 표준 프레임은 여러 채널 워드가 들어있는 마이너 프레임들이 모여 하나의 메이저 프레임을 만든다[7]. 따라서 그림 8과 같이 두 옵션의 리드솔로몬 코드가 적용 가능하도록 255 바이트를 하나의 마이너 프레임으로 구성하고, CTR 모드를 응용하여 암호화가 필요한 채널 워드를 블록 단위로 나누어 암호화하도록 설계하였다.

프레임 암호를 위한 암호 로직의 구조는 그림 9와 같으며, 암호화 과정은 그림 10과 같다. 원격측정 마이너 프레임을 32 비트 단위로 입력받아 프레임 버퍼에 임시 저장하고, ARIA-256 암호 로직은 키 인터페이스를 통해 수신된 암호 키를 라운드 키로 확장하여 암호화를 준비한다. 16 비트로 구성된 프레임 카운트는 외부에서 입력된 112 비트 비공개 난수와 비트 접합하여 128 비트 프레임 난수를 만들고 ARIA-256 로직으로 암호화 하여 키 스트림을 만든다. 암호 키 스트림은 블록 내부의 암호화가 필요한 채널 워드와 XOR 연산하여 암호화하고, 암호화가 완료되면 다음 블록의 암호화를 위해 프레임 난수를 증가시킨다.

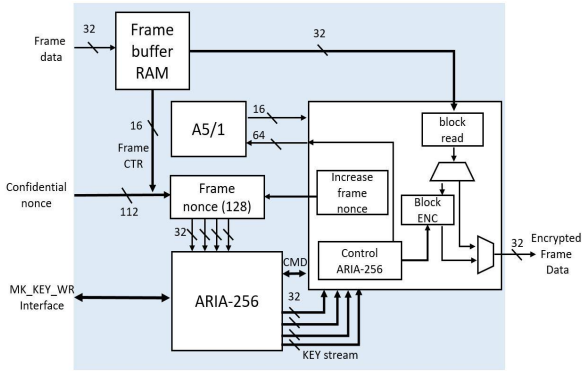

그림 9. 프레임 암호 로직 구조
Fig. 9. Structure of frame encryption logic.

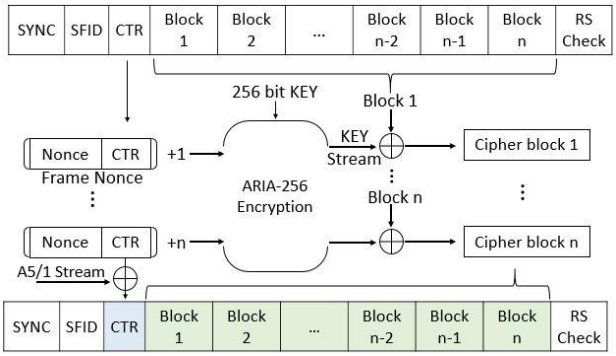

그림 10. 원격측정 프레임 암호 과정
Fig. 10. Process of telemetry frame encryption.

표 2. 리드솔로몬 옵션에 따른 프레임 구조 정보
Table 2. Frame structure according to RS option.

Option	Encryption blocks(128 bit)	Channel words(16 bit)	RS symbols(8 bit)
NO RS	16 block	124 word	0
RS(255, 239)	15 block	116 word	16
RS(255, 223)	14 block	108 word	32

증가된 프레임 난수는 ARIA-256 암호 로직으로 다시 키 스트림을 만들어 다음 블록을 암호화하며, 이 과정은 하나의 프레임이 모두 암호화될 때까지 반복된다. 하나의 프레임이 암호화가 완료되면 다음 프레임에 있는 카운트 값으로 새로운 프레임 난수를 만들고 동일한 과정으로 프레임을 암호화한다. 따라서 프레임의 각 블록들은 모두 다른 키 스트림으로 암호화가 되며 같은 데이터를 암호화하더라도 프레임과 블록마다 다른 결과값이 나오게 된다. 프레임 카운트는 해당 프레임의 암호화 완료 후 기밀성 보장을 위해 A5/1 스트림 암호 알고리즘으로 암호화되어 최종 암호 프레임에 구성이 된다. A5/1 암호화는 64 비트 암호 키로 스트림을 만들고 XOR 연산하여 암호화를 하는데, 암호 키는 ARIA-256 초기화 과정에서 생성되는 W3의 상위 64 비트를 사용하였다. 암호화가 불필요한 마이너 프레임의 싱크워드, 리드솔로몬 체크 워드는 암호화를 진행하지 않으며, 프레임의 세부 구성은 리드솔로몬 사용 여부와 옵션에 따라 표 2와 같이 정리할 수 있다. 프레임 복호 로직은 프레임 카운트의 A5/1 스트림 암호 적용 시점을 제외하고 암호 로직과 동일한 구조와 방법으로 복호화 하도록 설계하였다. 프레임 암호 로직은 프레임 난수를 만들고 프레임의 구성 과정에서 프레임 카운트를 암호화 하는데, 복호 로직은 먼저 수신 된 프레임 카운트를 원래 프레임 카운트 값으로 복호화하고 프레임 난수를 만들어 암호 프레임을 복호화 한다.

Ⅲ. 구현 및 검증

원격측정 시스템의 ARIA-256 적용을 위해 본 논문에서 설계한 ARIA-256 알고리즘과 원격측정 프레임의 암호화 방법을 VHDL 로직으로 구현하고, 시뮬레이션과 하드웨어 시스템을 구축하여 검증을 진행하였다.

3-1 시뮬레이션 검증

FPGA에 구현된 ARIA-256 알고리즘의 검증은 Intel FPGA 개발 소프트웨어인 Quartus Ⅱ의 시그널 탭 로직 분석 툴을 활용하여 키 초기화, 암호화, 복호화 순서로 진행하였고, 검증 방법은 표준서의 테스트 벡터와 결과를 비교하여 검증하였다. 키 초기화 결과는 그림 11과 같으며 256 비트 암호 키는 KL, KR로 분리되고, 3 라운드의 feistel 연산을 통해 테스트 벡터와 동일한 W0, W1, W2, W3의 생성결과를 확인하였다. 초기화 된 W0 ~ W3은 로테이션과 XOR 연산을 통해 17개의 라운드 키로 확장이 되며, 각 라운드 함수 진행을 위해 램에 임시 저장이 된다. 키 초기화 이후 암호화 라운드 함수의 검증을 위해 테스트 벡터 평문 “00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF”를 4개의 열로 입력하고 암호화를 진행하였다. 16 라운드 암호화 진행 결과 130 clock이 소요되었고, 그림 12와 같이 테스트 벡터와 동일한 암호문을 확인하였다. 암호화된 블록의 무 결성 검증을 위해 “ENC_DEC_SEL” 신호를 복호화 모드로 세팅하여 그림 13과 같이 원래 평문을 확인하였다.

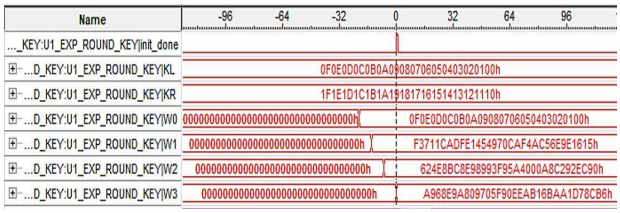

그림 11. 키 초기화의 시그널 탭 결과
Fig. 11. Signal tap result of key initialization.

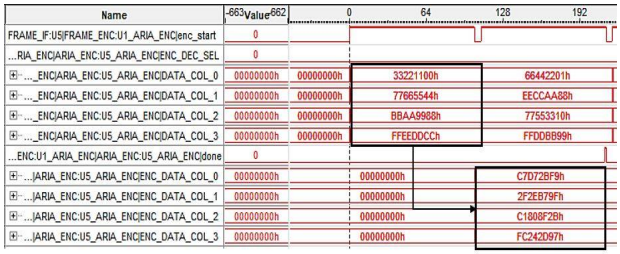

그림 12. ARIA-256 암호화의 시그널 탭 결과
Fig. 12. Signal tap result of ARIA-256 encryption.

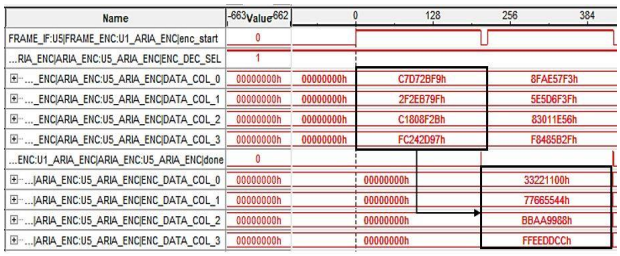

그림 13. ARIA-256 복호화의 시그널 탭 결과
Fig. 13. Signal tap result of ARIA-256 decryption.

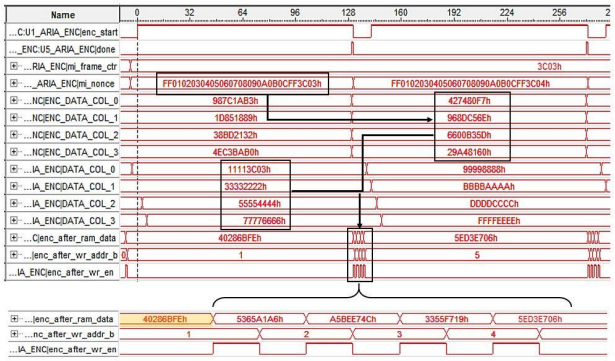

그림 14. 프레임 블록 암호화 시그널 탭 결과
Fig. 14. Signal tap result of frame block encryption.

구현이 검증된 ARIA-256은 원격측정 프레임의 암호화 과정에서 각 블록의 키 스트림을 생성하는데 사용이 되며, 프레임 블록의 암호화 과정은 그림 14와 같다. 프레임의 시작을 알리는 싱크워드 "0x40286BFE"는 암호화를 진행하지 않으며, 다음 워드부터 블록 단위로 암호화하여 프레임이 구성된다. 비공개 난수"0xFF01020304050607080090A0B0CFF"와 해당 프레임의 암호 카운트 "0x3C03"은 128 비트 프레임 난수 "mi_nonce"를 만들고, ARIA-256으로 암호화하여 32비트 4개의 열로 구성된 키 스트림"0x427480F7", "0x968DC56E", "0x6600B35D", "0x29A48160"이 생성된다. 생성된 키 스트림은 프레임의 블록 데이터 "0x11113C03", "0x33332222", "0x55554444", "0x77776666"을 암호화하는데 첫 번째 블록의 경우 암호 카운트"0x3C03"이 포함되어 있어 이는 A5/1방식으로 암호화하고, 나머지 블록은 생성된 키 스트림으로 암호화를 진행하여 "0x5365A1A6", "0xA5BEE74C", "0x3355F719", "0x5ED3E706"의 생성을 확인하였다. 하나의 블록이 암호화되면 프레임 난수 "mi_nonce"를 증가시켜 블록마다 매번 다른 키 스트림을 생성하고, 프레임의 마지막 블록까지 암호화를 진행한다. 암호화 된 프레임 블록은 다음 블록의 암호화를 위해 32 비트 단위로 버퍼 램에 저장이 되며, 모든 프레임이 암호화 되면 다음 프레임의 암호화를 위해 프레임 난수를 다시 구성하여 진행한다. 암호화된 프레임의 복호화 검증을 위해 매 프레임마다 같은 데이터 값을 넣어 암호 프레임을 만들고, 복호 로직으로 복호화 하여 원래 데이터를 확인해 복호화를 검증 하였다. 복호화 로직은 프레임 난수 "mi_nonce" 생성을 위해 먼저 암호화된 프레임의 암호 카운트를 A5/1 암호 스트림으로 복호화 하여 "0x19F0"을 생성하고, ARIA-256으로 키 스트림을 만들어 암호화 방법과 동일하게 복호화를 하였다. 프레임 복호화 결과는 그림 15와 같으며, 원래 프레임의 블록 데이터를 확인할 수 있었다.

프레임 암호 로직과 복호 로직의 Quartus II FPGA 합성 결과는 표 3과 같으며, 80 MHz 동작 주파수에서 한 프레임을 암호화 하는데 27 us의 소요시간을 확인하였다. 따라서 원격측정 시스템 class I 규격의 최대 전송속도 10 Mbps에서 하나의 프레임을 구성하는데 요구되는 시간과 비교해보았을 때 약 86%의 여유로 암호 프레임을 구성할 수 있다.

표 3. FPGA 합성 결과
Table 3. Results of FPGA synthesis.

Item	Frame encryption	Frame decryption
Total logic elements	12,394	12,345
Total registers	10,499	10,473
Total memory bits	78,080	78,080

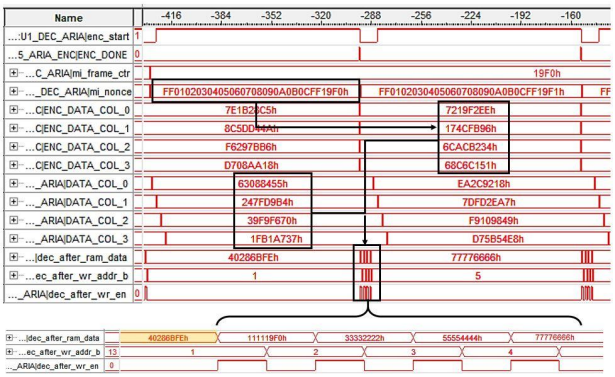

그림 15. 프레임 블록 복호화 시그널 탭 결과
Fig. 15. Signal tap result of frame block decryption.

3-2 하드웨어 구현 검증

구현된 ARIA-256 프레임 암호 로직을 원격측정 시스템에 적용하려면 연속성 있는 프레임에 대하여 실시간 암호 처리 검증이 필요하다. 따라서 그림 16과 같이 하드웨어 시스템을 구성하여 동작을 검증하였다. 검증 시스템은 FPGA 보드, 지상 점검 장비, PC와 통신을 위한 JTAG-UART (joint test action group universal asynchronous receiver / transmitter) 인터페이스, PC, 모니터링을 위한 command shell 터미널 툴로 구성이 된다.

FPGA 보드 DE2-115는 Intel FPGA CycloneⅣ로 구성되어 있으며, 연속성 있는 프레임을 생성하고 암호화한다. 프레임은 16 비트로 구성된 각 채널 워드에 0~65535 범위로 1씩 증가하는 데이터를 구성하여 각 채널 워드와 프레임 사이에 연속성 있는 값을 가지도록 하였다. 구성된 프레임은 암호화가 되고 PCM 코드 중 하나인 NRZ-L(non return to zero-level) 디지털 신호로 출력이 된다.

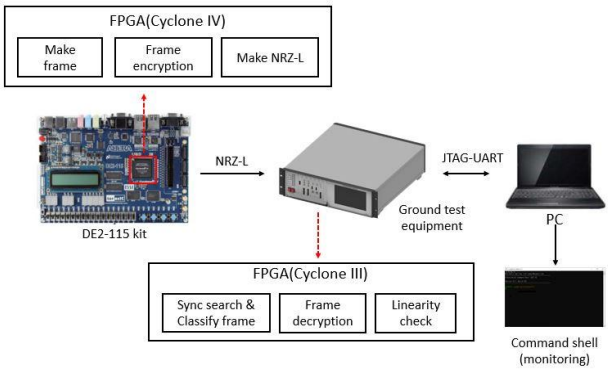

그림 16. 프레임 암호화 시험 구성도
Fig. 16. Test configuration of frame encryption.

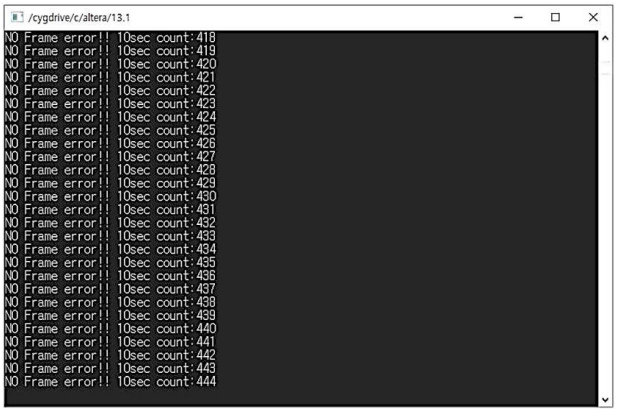

그림 17. 원격측정 프레임의 실시간 암호화/복호화 모니터링 결과
Fig. 17. Result of telemetry frame real-time encryption/decryption monitoring.

지상 점검장비는 Intel FPGA CycloneⅢ로 구성되어 있으며, NRZ-L 데이터를 받아 싱크 패턴을 찾고 연속되는 프레임을 정렬한다. 정렬된 프레임은 프레임 복호 로직으로 복호화를 진행하고, 복호화 된 프레임의 각 채널과 프레임 사이의 연속성을 검사하여 무 결성을 확인하였다. 프레임의 연속성 확인은 지상 점검장비의 FPGA 내부 CPU인 NIOS-Ⅱ core를 활용하였는데, 각 채널 데이터는 1씩 증가하는 값으로 구성되었기 때문에 복호화 된 프레임을 가져와 1차로 각 채널 데이터 값의 차이를 비교하고, 2차로 이전 프레임의 마지막 채널 값과 현재 프레임의 처음 채널 값을 비교하여 연속성을 검증하였다. 연속성 비교 결과는 NIOS-Ⅱ command shell 터미널을 통해 이상 유무를 메시지로 확인 할 수 있으며, 메시지는 복호화 된 프레임의 연속성을 매 프레임마다 검사하여 10초 주기로 출력이 된다. 실시간 모니터링 결과는 그림 17과 같으며, 이를 통해 연속성 있는 원격측정 프레임의 실시간 암호화와 복호화에 대한 무 결성을 확인하였다.

Ⅳ. 결 론

원격측정 시스템의 운용 과정에서 발생할 수 있는 보안 위협에 대응하기 위해 본 논문은 국가 표준 암호 알고리즘인 ARIA-256의 적용 방법을 연구하여 FPGA에 로직으로 구현하였다. 프레임 암호 로직의 합성 결과 12,394개의 LE(logic elements)와 78,080 메모리 비트로 구현이 되었고, 복호 로직은 동일한 메모리 비트를 사용하여 12,345개의 LE로 구현 되었다. 구현된 원격 측정 프레임 암호 로직은 시뮬레이션을 통해 1차 검증을 하고, 하드웨어 시스템을 통해 연속성 있는 원격측정 프레임의 실시간 암호화와 복호화를 최종 검증하였다. 암호 프레임은 사용자의 대역폭 여유에 따라 CCSDS에서 권장하는 2가지 리드솔로몬 코드를 적용할 수 있으며, 원격측정 시스템 class Ⅰ 최대 규격인 10 Mbps에서 86%의 동작 여유를 가진다. 원격측정 시스템의 암호화 설계와 구현을 통해 기밀성 있는 보안 기술이 확보되었고, 암호화 선택의 폭을 넓히기 위해 다양한 암호 알고리즘의 적용 방안과 암호 키 관리 및 운용 방법에 대한 연구를 계속 진행할 예정이다.

References

[1] G. H. Kim, M. H. Jin and B. K. Kim, “Design of a simple PCM encoder architecture based on programmable ROM,” *Journal of Advanced Navigation Technology*, Vol. 23, No. 2, pp. 186-193, Apr. 2019.

[2] J. P. Kim and C. h. Koo, “Telecommand decryption verification for engineering qualification model of command telemetry unit in communications satellite,” *Journal of The Korean Society Aeronautical and Space Sciences,* Vol. 33, No. 7, pp. 98-105, Jul. 2005 .

[3] K. B. Kim and K. W. Shin, “A unified ARIA-AES cryptographic processor supporting four modes of operation and 128/256-bit key lengths,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 21, No. 4, pp. 795-803, Apr. 2017.

[4] D. S. Kwon, J. S. Kim, S. W. Park, S. H. Sung, Y. K. Sohn, J. H. Song, Y. J. Yeom, E. J. Yoon, S. J. Lee, J. W. Lee, S. T. Chee, D. W. Han and J. Hong, “New block cipher: ARIA,” I*nternational Conference on Information Security and Cryptology(ICISC)*, Seoul: Korea, pp. 432-445, Nov. 2003.

[5] Chairman of Korea Industrial Standards Commission, 128bit block encryption algorithm ARIA - part1: general, Ministry of Science and ICT(MSIT), Korea, KS X 1213-1, Dec. 2014.

[6] CCSDS, TM synchronization and channel coding, Consultative Committee for Space Data Systems (CCSDS), Washington DC: USA, Technical Report CCSDS 131.0-B-3, Sep. 2017.

[7] Telemetry Group, Range Commanders Council (RCC). IRIG Standard document 106-19 chapter 4. pulse code modulation standards [Internet]. Available: https://www.irig106.org/wiki/irig_106-19.

최 석 훈 (Seok-Hun Choi)
2013년 2월 : 건양대학교 전자정보공학과 (공학사)
2013년 2월 ~ 현재 : 단암시스템즈(주) 통신기술연구소
※ 관심분야 : 원격측정 시스템, 암호화, 채널코딩

이 남 식 (Nam-Sik Lee)
2001년 2월 : 경희대학교 전파공학과 (공학사)
2001년 2월 ~ 현재 : 단암시스템즈(주) 통신기술연구소
※ 관심분야 : 무선통신 시스템, 암호화, 원격측정장치

김 복 기 (Bok-Ki Kim)
1995년 2월 : 서울대학교 수학과 (이학사)
1997년 2월 : 서울대학교 수학과(정수론) (이학석사)
1997년 1월 ~ 2002년 4월 : 단암전자통신(주) 연구소
2002년 5월 ~ 현재 : 단암시스템즈(주) 통신기술연구소
※ 관심분야 : 무선통신, 채널코딩, 디지털 신호처리 구조