技術論文

정지궤도 통신위성의 CCSDS 원격명령 암호복호기 구현

김중표*, 구철희*, 최재동*

Implementation of CCSDS Telecommand Decryptor in Geostationary Communications Satellite

Joong-Pyo Kim*, Cheol-Hea Koo* and Jae-Dong Choi*

ABSTRACT

In this paper, a CCSDS(Consultative Committee for Space Data Systems) telecommand(TC) decryptor for the security of geostationary communications satellite was implemented. For the confidentiality of CCSDS TC datalink security, Option-A which implements the security services below the transfer sublayer was selected. Also CFB(Cipher Feedback) operation mode of DES(Data Encryption Standard) was used for the encryption of 56-bit data bits in 64-bit codeblock. To verify Decryptor function, the DES CFB logic implemented on A54SX32 FPGA(Field Programmable Gate Array) was integrated with interface and control logics in a PCB(Printed Circuit Board). Using a function test PC, the encrypted codeblocks were generated, transferred into the decryptor, decrypted, and the decrypted codeblocks were transmitted to the function test PC, and then compared with the source codeblocks. Through LED(Light Emitting Diode) ON operation by driving the relay related to Op-code decoded and the comparison between the codeblock output waveforms measured and those simulated, the telecommand decryptor function was verified.

초 록

본 연구에서는 정지궤도 통신위성의 보안을 위해 CCSDS 원격명령(Telecommand) 암호복호기를 구현하였다. CCSDS 원격명령 데이터링크(Datalink)의 보안 기밀성(Confidentiality)을 위해 데이터링크 계층(Layer)내의 트랜스퍼 부계층(Transfer Sublayer) 다음에서 암호화를 행하는 Option-A를 선정하고 64-비트 코드블록(Codeblock)에서 56-비트 데이터 비트의 암호화를 위해 DES CFB 모드를 사용하였다. A54SX32 FPGA에 구현된 DES CFB 로직은 원격명령 암호복호기의 기능 검증을 위한 인터페이스 및 제어 로직과 함께 PCB 보드에 구현하였다. 기능시험용 PC를 사용하여 암호화된 원격명령을 생성하고 암호복호기에 전송한 뒤 복호화한 뒤 기능시험용 PC에 피드백하고 전송한 코드블록과 비교한다. 수행코드에 해당하는 릴레이 구동에 의한 LED ON 동작 및 측정된 코드블록 파형과 시뮬레이션 파형의 비교를 통해 원격명령 암호복호기의 기능을 검증하였다.

Key Words : Encryption(암호화), Telecommand(원격명령), Decryptor(암호복호기)

† 2003년 3월 24일 접수 ~ 2003년 10월 1일 심사완료

* 정회원, 한국항공우주연구원 통신위성체계그룹
연락처, E-mail : jpkim@kari.re.kr,
대전시 유성구 어은동 45

1. 서 론

원격측정명령처리기(CTU, Command Telemetry Unit)는 정지궤도 통신위성 버스체의 원격측정명

령계(TC&R, Telemetry, Command and Ranging)의 한 부분으로 위성이 지상국과 통신할 수 있는 유일한 장치로서 높은 신뢰성과 가용성을 요구하며, 미국 및 유럽의 대형 위성 제조사들은 풍부한 설계 및 제작 기술을 이용하여 자사내에서 독자 제작하고 있으며, 설계 변경에 따른 재설계의 비용을 줄이기 위한 모듈화 개념을 적용하여 제작하고 있다. 국내에서는 처음으로 정지궤도 통신위성 전장품의 원천 설계, 제작, 시험 기술 확보 및 향후 국내 정지궤도 통신위성 버스체 국산화 전장품으로의 활용을 위해 3차년도에 걸쳐 CTU 실험모델(EM, Engineering Model)을 거쳐 CTU 인증모델(QM, Qualification Model)을 목표로 하여 개발하고 있다.

본 연구는 CTU 실험모델의 전단계로 CTU의 중요한 기능 중에 하나인 원격명령 암호복호기를 설계하고 시제품을 제작하여 기능시험을 통한 사전 성능 검증을 위함이다. 현재 국내에서 운용중인 정지궤도 통신위성인 무궁화위성의 경우 원격명령에만 암호화를 적용하여 위성을 상대 적국이나 권한이 없는 사용자들의 불순한 명령에 의한 위성의 보호를 수행하고 있다. 본 연구에서도 원격명령에 대해서만 암호화를 구현하고, 원격명령 통신링크 포맷은 PCM(Pulse Code Modulation) 기반의 독자적인 포맷을 만드는 대신에 세계 여러 우주개발기관과 위성 운영자들이 상호간에 공동 위성 운영이나 긴급한 경우에 대리로 위성을 운영할 수 있는 Cross support[1] 특성으로 인한 지상국 비용 감소의 이점을 고려하여 CCSDS 표준 권고안을 선택하였고 또한 CCSDS 표준은 저궤도위성에서 보편화되어 사용되고 있기에 저궤도위성용 원격명령 암호복호기에도 직접 활용가능한 장점을 제공한다.

정지궤도 통신위성의 보편적인 원격명령 전송 속도는 1,024bps로 국내 정지궤도 통신위성인 무궁화위성도 1,024bps를 사용하고 있다. 그래서 본 연구에서도 1,024bps 전송속도를 목표로 하고 원격명령 권고안[2,3]에 준하여 원격명령 포맷을 만들고, CCSDS 암호화 보안 권고안[5]의 데이터 링크 계층의 Option-A를 사용하여 원격명령의 기밀성을 제공하도록 하였다. 원격명령 기밀성 제공을 위한 암호화 알고리즘은 지상 및 위성에서도 충분히 검증되고 아직까지 보편적으로 사용되고 있는 대칭키 블록 알고리즘인 DES[6] 암호화 알고리즘을 선정하였고, 대칭키 블록 암호화 알고리즘의 4가지 동작 모드[7-9] 중 64-비트 이하의 가변 입력 비트 지원 및 동일한 데이터 블록에 대한 전혀 다른 결과를 주는 장점이 있는

CFB 모드를 채택하였다.

원격명령 전송 데이터 블록길이는 전송하고자 하는 데이터 56-비트에 대해 8-비트의 에러제어 코드를 붙여 만들어진 64-비트 코드블록으로 구성되며, 데이터 56-비트에 대해서만 DES CFB 모드를 적용한다. DES CFB를 구현하는 방법으로 우주용 암호화 ASIC(Application Specific Integrated Circuit)을 개발하거나 구매하여 쓸 수도 있지만 고비용이 요구된다. 따라서 지금 널리 사용되고 있고 검증된 FPGA IP(Intellectual Property)를 구매하거나 직접 개발하여 사용하면 적은 비용으로 구현할 수 있으며 향후 재사용의 장점을 제공한다. 그래서 본 연구에서도 위성의 높은 신뢰성을 고려하여 NIST(National Institute of Standards and Technology) 인증된 DES CFB 코어를 구매도 하고 DES CFB 코어를 직접 개발도 하여 구매한 것과 시뮬레이션을 통해 성능을 검증하였다. DES CFB 코어는 Innoveda사의 ViewDraw/ViewSim을 사용하여 성능 검증 뒤 Actel사의 A54SX32 FPGA에 퓨징하였다.

또한 원격명령 암호복호기의 시제품의 성능검증의 편의성을 제공하기 위해 80196 마이크로컨트롤러를 사용하여 RS-232C로 지상국을 모사하는 PC와의 원격명령 전송 및 복호화된 원격명령을 피드백하도록 하였다. 지상국을 모사하는 기능시험용 PC는 암호화된 원격명령을 만들어 시제품에 전송하고 암호복호화된 원격명령의 수행 코드를 디코딩하여 원하는 릴레이(Relay) 구동회로를 구동하도록 하였고 그것을 가시적으로 보이기 위해 시제품 전면 패널에 LED를 달아 ON이 되는 지를 확인하도록 하였다. 또한 원격명령 복호화 시뮬레이션 결과 파형 및 실제 측정된 파형을 비교하여 목표한 1,024bps 속도로 원격명령 암호복호 기능이 안정적으로 동작하고 있음을 보였다. 이 연구결과는 향후 CTU 실험모델에 직접 적용 가능함을 확인하였고, 또한 CTU 시험장비(Test Set) 개발에도 최소한의 수정으로 사용가능하다. 현재 FPGA에 DES 코어를 사용하였지만 본 연구에서 제안한 다중(Multiple) 키(Key) 사용뿐만 아니라 다중 IV(Initialization Vector)를 사용하여 지상에서 키 및 IV 변경 명령을 사용하면 훨씬 강화된 기밀성을 제공할 수 있다.

또한 대체가 용이한 FPGA IP 코어의 장점을 활용하여 하나의 키를 사용하는 DES 코어보다 기밀성이 강화된 3개의 키를 사용하는 TDEA(Triple Data Encryption Algorithm) 코어나 차세대 블록 암호 표준으로 선정된 후 활발히 연구되고 있는 AES(Advanced Encryption

Standard) 코어[10-12]로 대체하면 보다 높은 기밀성을 제공할 수 있다.

II. 본 론

2.1 암호화 알고리즘/동작모드 선정

DES 알고리즘은 지상뿐만 아니라 위성 쪽에서도 보편적으로 많이 사용되고 있는 알고리즘으로 최근에는 기상위성의 처리 데이터 정보전송 표준인 LRIT(Low Rate Information Transmission)/HRIT(High Rate Information Transmission)에도 사용하고 있다. DES는 TDEA 및 AES보다는 보안의 취약성은 있지만 동작 모드 선정 및 운용 개념을 적절히 사용하면 상당히 강화된 보안기능을 구현할 수 있으며, FPGA 구현시 비용, 처리속도 및 사용 게이트 용량이 가장 적절하여 선정하였다. 또한 FIPS PUB 81[7] 및 NIST Special PUB 800-17[8]에 정의된 동작 모드 중 가변입력 비트 사용 및 동일한 데이터 블록에 대해서 전혀 다른 결과를 생성하는 특징이 있는 CFB 모드를 선정하였다. CFB 모드의 암호화 및 복호화 동작과정은 Fig. 1과 같다.

2.2 원격명령 암호화 복호 로직 구현

정지케도 우주환경에서 높은 신뢰성을 보장하고 안정적인 동작을 위해 NIST Special PUB 800-17[8]에 나열된 시험들을 만족하는 즉 검증된 DES CFB 코어를 Netlist 버전으로 구매한 뒤 Innoveda Viewdraw/Viewsim을 통해 코어를 시뮬레이션하고 검증한 뒤, Uplink FPGA와 접속을 위한 로직들 및 다중 암호화 키 및 IV 값을 추가하여 만든 최종 Netlist를 Actel Designer Series에서 Fuse 파일을 만들고 Silicon Explorer

Fig. 2. Core Logic of DES CFB Mode

II를 통해 우주용이 아닌 상업용 Actel A54SX32 FPGA에 Fusing하였다. 향후 CTU 인증모델에 사용될 FPGA는 우주용 RT(Radiation Tolerant)급 RT54SX32S이며 TID(Total Ionization Dose)가 80-135KRad로 저궤도위성에서는 점차 사용이 증대되고 있는 상태다. 정지궤도위성의 경우는 보통 100KRad이상을 요구하고 있기에 적절한 위성체 및 박스 차폐를 통해 사용가능하다. Fig. 2에 DES CFB 모드로 최종 구현된 코어 블록 구성을 나타내었다. 여기서 64-비트의 IV(Initialization Vector)를 32 비트씩 나누어 LDIV라는 신호핀의 제어에 의해 로드하도록 하였는데 이것은 Actel사의 A54SX32 FPGA가 제공하는 가용 I/O 228개를 초과하지 않도록 하기 위함이다. A54SX32 FPGA에 합성한 결과 사용율은 I/O 94.74%, 순서 모듈(Sequential Module) 15.09%, 조합모듈(Combinational Module) 35.50%, 순서모듈 및 조합모듈을 합한 사용율은 27.85%를 나타내었다. 또한 자체 DES CFB 코어를 확보하기 직접 코어를 개발한 뒤 구매한 것과 시뮬레이션 결과를 비교하였고 그 결과 동일한 성능을 얻었으며 사용율도 거의 동일하였다.

구현된 코어는 NIST 인증된 DES 코어로 56-비트 피드백을 갖는 CFB 동작 모드로 설계되었으며, 암호화 및 복호화의 선택을 지원하며, 16 클럭 사이클로 암호화 및 복호화를 수행하며, 피드백 비트 수의 가변이 가능하며, TDEA로 변경이 가능하며, 높은 클럭 속도와 낮은 게이트 카운터로 구현되었으며, 클럭 스피드의 4 배의 비트율을 지원하도록 설계되었다. 구현된 코어의 동작 타이밍도는 Fig. 3과 같다. 암호화 혹은 복호화는 E_D 신호에 의해 선택된다(E_D High: Encryption, E_D Low: Decryption). GO 신호가 상승(Rising) 할 때에 KEY 핀의 복호화 키를 사용하여 입력 DIN에 암호 복호화 동작의 시작을 개시(Triggering) 한다.

Fig. 1. Operation Process of CFB Mode

Fig. 3. Timing Diagram of DES CFB Core

첫 번째 복호화 동작을 위해 IV 벡터를 초기화하는 것이 필요하며, 이것은 GO 신호가 High로 된 하나의 클럭 사이클 후 한 클럭 사이클 동안 INIT 입력을 High를 함으로써 이루어진다. IV 입력이 32-비트의 넓이를 갖기 때문에 LDIV 신호는 내부의 64-비트 IV 레지스터에 32-비트를 로드하기 위해 사용된다. GO 신호가 High가 될과 동시에 1 클럭 사이클 동안 High가 된다. IV의 63-32 비트 값들이 IV 입력으로부터 입력되고 31-0 비트 값들은 LDIV가 Low가 될 때, 다음 클럭 사이클에 로드된다. 16 사이클 후에 READY 출력은 입력 DIN 및 출력 DOUT이 유효하다는 것을 지시한다. 코어는 즉각적으로 매 16 사이클 마다 64 비트의 Throughput이 유지되도록 다른 동작을 위해 준비된다.

2.3 CCSDS 원격명령 암호화 권고

CCSDS 원격명령 포맷에 대한 데이터링크 계층 내에서 암호화 권고안[5]은 세그멘테이션 부계층의 다음에서 행하는 Option-B와 트랜스퍼 부계층의 다음에서 수행하는 Option-A가 있으나 Option-A가 하드웨어 구현이 더 간단하여 Option-A를 선택하였다.

원격명령 전송 데이터 형식은 전송하고자 하는 데이터 56-비트에 대해 (63,56) Modified Bose-Chaudhuri-Hocquenghem(BCH) 코드[2]를 이용하여 생성된 7개의 패리티(Parity) 비트에 '0' 비트를 부가하여 구성된 8-비트의 EC(Error Control) 코드를 붙여 만들어진 64-비트 코드블록들에 대해 16-비트의 시작(Start) 시퀀스, 64-비트의 후미(Tail) 시퀀스를 앞뒤에 붙여 만들어진 CLTU(Command Link Transmission Unit)라는 데이터 구성을 가진다. 여기서 64-비트 코드블록의 데이터 부분인 56-비트에 대해서만 DES CFB 모드로 암호화하고 나머지 EC 코드 부분 및 시작(Start)/후미(Tail) 시퀀스 부분은 암호화되지 않는다. 암호화된 CCSDS 원격명령 전송 데이터 포맷은 Fig. 4와 같다.

Fig. 4. Encrypted CCSDS Telecommand Format

2.4 다중 암호화 키 및 IV 운용

위성의 키를 하나만 갖고 운영할 경우에 거의 회박하지만 만약 위성의 공격자들에게 해킹될 경우에 위성에 치명적인 영향을 줄 수 있는 여지를 제공하게 된다. 따라서 위성에 암호 복호화를 다중 키를 저장하고 각 키에 대한 키 인덱스를 할당하여 둔다. 위성에서는 현재의 키 인덱스를 텔레메트리로 내려 보내고 지상국에서는 그것을 받아 그 인덱스에 해당하는 키 값으로 암호화하여 위성으로 올려준다. 만약 현재의 키가 노출의 가능성이 있다고 판단되면 지상국에서는 키 인덱스 변경 명령을 올려 변경하고 변경된 키 인덱스를 지상국으로 내려준다. 현재 DES CFB 모드를 사용할 경우 IV 값을 고정된 값이 아닌 카운터(Counter)나 랜더마이즈(Randomizer)를 사용하여 매번 갱신되도록 하여 지상국에 내려 보내고 지상에서 그 값을 사용하여 암호화를 하면 고정된 IV를 사용하는 것보다 훨씬 강화된 보안 기능을 제공할 수 있다. IV를 통한 보안을 강화하는 다른 하나의 방법은 다중 암호화 키에 대한 인덱스 할당 개념을 IV에도 적용하여 다중 IV에 IV 인덱스를 할당하면 암호화 키의 구현 및 운영개념을 공유할 수 있는 장점이 있다. 이렇게 다중 키 및 다중 IV를 함께 활용함을 통해서 실제로 이중키를 사용하는 것과 같은 효과가 있으며 보다 강화된 보안을 제공하게 된다. 본 시제품에서는 단순화하기 위해 단지 2개의 암호화 키 및 IV를 사용하여 구현하였다.

2.5 원격명령 암호복호기 시제품

원격명령 암호복호기를 구현한 기능 블록 구성도는 Fig. 5에 나타난 바와 같이 6개의 기능 블록으로 구성된다.

- 196 Controller Block
- Power On Reset & Voltage Regulator
- Test Set Function & Decoder
- Uplink & DES FPGA Block
- CMR Interface Block
- SCC CMD Driver Block

Fig. 5. Functional Block Diagram of Telecommand Decryptor

2.5.1 원격명령 암호복호기 시제품 기능

1) 80C196 Controller Block

이 블록은 80C196 컨트롤러 및 RAM, EPROM, 12MHz 오실레이터로 구성되며, 외부에 있는 지상국을 모사하는 기능시험용 PC와의 인터페이스는 RS-232C로서 통신을 하며, 기능시험용 PC에서 생성한 암호화된 원격명령 코드블록을 받고, 복호화된 코드블록을 기능시험용 PC로 보내어 전송한 명령코드블록과의 일치성을 비교하도록 해주는 기능을 수행한다.

2) Power On Reset & Voltage Regulator

이 블록에서는 +5V의 입력전원을 받아 A54SX32 FPGA 동작전압인 +3.3V를 만들어내는 기능을 수행하고, 전원이 인가되었을 때 Power On Reset 신호를 만들고, 아울러 외부에서 입력되는 Reset 신호를 처리하는 기능을 수행한다.

3) Test Set Function & Decoder

이 블록은 Test Set Function FPGA와 RS-422 출력단으로 구성된다. Test Set Function FPGA는 ACTEL 84PLCC FPGA를 사용하였고, 80C196 컨트롤러로부터 입력받은 병렬 업링크 명령을 직렬 데이터로 변환하고 NRZ-M 타입으로 출력한다. 또한 주소 디코딩(Address Decoding) 기능을 수행하여 80C196 컨트롤러 블록에서 필요한 제어신호를 만들어낸다. RS-422 출력단에서는 FPGA에서 출력되는 데이터와 클록을 차동(Differential) 신호로 변환하여 RF(Radio Frequency) 명령수신기(CMR, Command Receiver) 인터페이스 블록으로 출력하는 기능을 수행한다.

4) CMR Interface Block

이 블록은 CMR로부터 오는 RS-422 수신 인터페이스 기능을 제공하는 블록으로 RS-422 차동 신호로 입력되는 데이터 및 클록 신호를 입력받아 Uplink FPGA로 전송하는 기능을 수행한다.

5) Uplink & DES FPGA Block

이 블록은 Uplink FPGA 및 DES FPGA로 구성되며 각각의 FPGA는 A54SX32 FPGA를 사용한다. Fig. 6은 Uplink & DES FPGA 블록의 동작 흐름을 보여주고 있다. 먼저 Randomization ON/OFF 및 DES Disable/Enable을 설정할 수 있도록 하여 Randomization OFF이면 Derandomization 블록을 지나가며 OFF 인 경우는 Sync(동기) 신호 감지 후 Derandomization 블록을 거치도록 하였고 또한 DES Disable의 경우는 DES FPGA를 거치지 않도록 하였고 DES Enable의 경우는 DES FPGA를 통과하도록 하였다.

먼저 DES Enable의 경우의 동작 과정을 설명하면 다음과 같다. Uplink FPGA는 CMR 포트 또는 EGSE(Electrical Ground Support Equipment) 포트를 통해 입력되는 업링크 명령의 데이터 포맷 NRZ-M을 NRZ-L로 변환하고 Sync 신호를 감지한 뒤 유효하면 Derandomization[4]을 수행하고, 직렬 데이터를 64-bit 병렬 데이터로 바꾸어 DES FPGA로 보낸다. DES FPGA로부터 암호 복호화된 64-bit 병렬 명령을 다시 받아 BCH ECC(Error Correction Check)를 수행하고, 에러가 없으면 위성체 주소를 체크하고 명령 복호를 수행하고, 인터럽트를 발생시켜 80C196 컨트롤러로 통보한다. 원격명령은 SCC(Spacecraft Configuration Command) 명령과 버스(Bus) 명령의 두가지로 구분되어 수행되며 SCC 명령일 경우는 수행코드에 해당하는 릴레이 구동회로를 SCC CMD Driver Block을 통해 구동하여 LED를 ON하도록 한다. 또한 Bus 명령은 위성 OBC(Onboard Computer)로 전송되어 수행되는 명령으로 현재 OBC가 없는 관계로 명령 수행을 확인하기 위해 SCC명령처럼 수행코드에 해당되는 릴레이 구동회로를 구동하여 LED를 ON할 뿐 아니라 받은 코드블록을 기능시험용 PC로 피드백(Feedback)하여 전송한 코드블록

Fig. 6. Operation Flow of Uplink & DES FPGA Block

과 비교하도록 하였다. 그리고 DES FPGA는 DES Enable의 경우에만 Uplink FPGA로부터 64-비트 병렬 데이터를 받고 그 중 데이터 비트인 56-비트와 2.4절에 설명한 2개의 키와 IV 중 선택된 암호화 키와 IV를 사용하여 암호 복호화를 수행하고 난 후 얻은 56-비트 데이터에 사용하지 않았던 8-비트의 EC 코드를 붙여 64-비트 병렬 데이터로 만든 뒤 다시 Uplink FPGA로 전송한다.

DES Disable의 경우는 DES FPGA를 거치지 않고 직렬에서 병렬데이터로 변화하면서 BCH ECC 및 위성체 주소를 체크하고 명령을 수행하는 과정으로 진행된다.

6) SCC CMD Driver Block

이 블록에서는 Uplink FPGA에서 출력되는 SCC 명령 신호 및 버스명령의 수행코드에 해당하는 외부 릴레이를 구동하는 기능을 수행한다. 본 시제품에서는 외부에 릴레이 대신에 LED를 달아 동작을 검증하였다.

2.5.2 원격명령 암호복호기 시제품 성능 시험 결과

설계된 회로도를 이용하여 PCB를 제작하였고, 제작한 시제품의 외형을 Fig. 7에 보여주고 있다.

지상국을 모사하는 기능시험용 PC는 제작된 시제품에 RS-232C 통신을 통해 암호화된 원격명령 코드블록을 생성하여 전송하면 원격명령 암호복호기에서는 원격명령을 복호화한 뒤 수행코드에 해당하는 릴레이를 구동하여 LED 구동을 통한 검증뿐만 아니라 복호화된 코드블록을 기능시험용 PC에 RS-232C로 전송하고 보낸 명령과 비교함을 재확인하게 된다.

원격명령 암호복호기의 성능을 검증하기 위하여 기능시험용 PC에서 SCC 및 Bus 원격명령 코

드블록들을 DES Disable 및 DES Enable, DES Enable(Randomization On)의 3가지 경우로 나누어 생성하고 아래에 각각에 대한 코드블록들을 16진수로 보여주고 있다. 여기서 0x23FFFC0600은 헤더(Header)를 나타내며 0x5555555555555555는 Tail 시퀀스를 나타낸다.

a) DES Disable Case

```
-SCC1: 23FFFC0600DF1132 5555555555555555
-SCC2: 23FFFC0600DF1226 5555555555555555
-SCC3: 23FFFC0600DF171A 5555555555555555
-BUS1: 23FFFC0600DF1132 0123456789ABCD90
      EF00000000FFFF84 5555555555555555
-BUS2: 23FFFC0600DF1226 0123456789ABCD90
      EF00000000FFFF84 5555555555555555
-BUS3: 23FFFC0600DF171A 0123456789ABCD90
      EF00000000FFFF84 5555555555555555
```

b) DES Enable Case

```
-SCC1: FC964CDC230B3E32 5555555555555555
-SCC2: FC964CDC230B3D26 5555555555555555
-SCC3: FC964CDC230B3D1A 5555555555555555
-BUS1: FC964CDC230B3E32 F76695036B80E690
      717DCDBB1C7ED584 B6D235886DB90E55
-BUS2: FC964CDC230B3D26 2BDBAEDF77042190
      E8E4DAD5A76BD684 3E6A8B073C068455
-BUS3: FC964CDC230B381A A9291C161D4F1B90
      75299017FC250284 2A87591AE44FC855
```

c) DES Enable Case(Randomization On)

```
-SCC1: 03DE421CB9064E8E DB79C6F8F2E2139B
-SCC2: 03DE421CB9064D9A DB79C6F8F2E2139B
-SCC3: 03DE421CB90648A6 DB79C6F8F2E2139B
-BUS1: 03DE421CB9064E8E 79A06AECC37A05E
      2BEAB0772EDC6ABA BCC2C400F974E4E4
-BUS2: 03DE421CB9064D9A A5F73D72D0B3675E
      B273A71995C969BA 347A7A8FA8CB6EE4
-BUS3: 03DE421CB90648A6 27058FBBBAF85D5E
      2FBEEDDBCE87BDBA 2097A892708222E4
```

먼저 SCC 명령의 경우에 대한 DES Disable일 경우는 기능시험용 PC에서 암호화되지 않은 코드블록을 원격명령 암호복호기로 전송하고 만약 DES Enable일 경우에는 DES CFB로 암호화된 데이터 비트인 56-비트와 8-비트 EC 코드 비트를 붙여 원격명령 암호복호기로 전송하고 복호화된 코드블록 내의 수행코드를 디코딩하여 릴레이 구동회로를 구동하여 LED가 동작하는지를 실험하였다. DES Enable(Randomization On)의 경우는 DES CFB 암호화된 56-비트 데이터 비트와 8비트 EC 코드를 붙인 64-비트 코드블록들을 Randomizer를 통해 Randomization하여 원격명

Fig. 7. Prototype of Telecommand De cryptor

Fig. 8. Measured Waveform(SCC1, DES Disable)

Fig. 9. Simulation Waveform(SCC1, DES Disable)

령 암호복호기로 전송하여 De-randomization 및 암호 복호를 하여 수행코드에 해당하는 LED On 시험을 하였다. 시험 결과 위의 3가지 경우에 대해 명령이 들어가면 각각 SCC1, SCC2, 및 SCC3의 명령에 해당하는 LED가 ON되는 것을 확인할 수 있었다.

다음으로 Bus 명령에 대한 DES Disable, DES Enable 및 DES Enable(Randomization On) 각각의 경우에 대해 BUS1, BUS2 및 BUS3 명령을 생성하고 암호복호기에 전송한 뒤 수행코드에 해당하는 LED가 ON됨을 확인하였고 또한 첫 번째 코드블록의 헤더부분, EC 코드들, Tail 시퀀스를 제외한 데이터를 PC로 피드백하여 전송한 코드블록들과 비교를 통해 복호기능을 재확인하였다. 한가지 예로 BUS1 명령에 대한 피드백된 데이터는 0xDF110123456789ABCDEF00000000FFFF로 DES Disable의 경우의 코드블록들에서 진하게 표시된 부분들에 해당된다. BUS2 및 BUS3에 대해서도 피드백되는 부분을 진하게 표시하였다.

Fig. 8은 FPGA의 클럭 및 코드블록 데이터 출력핀에 대한 출력 파형을 직접 측정한 파형으로 SCC1, DES Disable에 대한 첫 번째 64-비트 코드블록에서 43-비트에 해당하는 파형이다. 여기서 원격명령이 1,024bps로 동작하기에 1-비트의 시간 길이는 $1/1,024=0.9765\text{ms}$ 가 되어 64-비트 코드블록에 대해서는 $0.9765\text{ms} \times 64=62.5\text{ms}$ 에 해당한다. Fig. 9는 측정파형과 비교하기 위해 SCC1, DES Disable에 대한 43-비트에 해당하는

Simulation 파형을 잘라서 보여주고 있다. 측정 파형과 시뮬레이션 파형이 잘 일치함을 확인할 수 있다. 43-비트 이후의 비트에 대해서도 서로 비교하여 보았고 잘 일치하였다.

Fig. 10은 SCC1, DES Enable의 경우에 대해 DES FPGA에서 암호복호화된 후 Uplink FPGA에 넘겨진 복호화된 64-비트 코드블록 데이터에서 50-비트에 해당하는 부분의 측정 파형을 보여주고 있으며, Fig. 11은 SCC1, DES Enable시의 시뮬레이션 파형을 보여주고 있으며 서로가 잘 일치함을 확인할 수 있다. 그리고 나머지 데이터 부분에 대해서도 비교를 통해 확인을 하였다. 또한 DES Enable(Randomization)의 경우에 대해서도 동일한 비교 실험을 통해 성능을 확인하였다.

Bus 명령에 대해서도 3가지 경우에 대한 측정 파형과 시뮬레이션 파형을 각각 비교하여 정확히 일치함을 확인할 수 있었다. 또한 암호화 키와 IV를 변경한 후 위와 동일한 과정의 시험을 수행하여 변경된 키 및 IV에 대한 암호복호화 동작을 확인하였다. 이것을 통해 DES CFB 원격명령 암호복호기가 SCC 명령 및 Bus 명령 코드블록을 정상적으로 복호화함을 확인할 수 있었다.

현재 구현된 원격명령 암호복호기로 들어오는 원격명령 데이터 전송속도가 1,024bps이므로 초당 처리되는 64-비트 코드블록의 수는 $16(=1,024/64)$ 개가 된다. 실제 DES 코어 A54SX32 FPGA

Fig. 10. Measured Waveform(SCC1, DES Enable)

Fig. 11. Simulation Waveform(SCC1, DES Enable)

는 55MHz 클럭속도까지 지원하기에 전체 Throughput은 220Mbps까지 되지만 실제 제공된 외부 클럭은 80C196에 사용된 12MHz 클럭을 사용하였다. 보다 높은 원격명령 데이터 전송속도를 지원하지만 단지 1,024bps의 전송속도를 목표로 한 것은 정지궤도 특성상 지상국과 항상 접촉이 가능하여 위성 운용에는 충분하기 때문이었다.

III. 결 론

본 연구에서는 정지궤도 통신위성의 원격명령 보안을 위해 CCSDS 원격명령 포맷에 대해 CCSDS 보안 권고안을 따라 데이터링크 계층내의 트랜스퍼 부계층 다음에서 암호화를 행하는 Option-A를 선정하고 64-비트 코드블록 중 56-비트 데이터 부분을 DES CFB 모드를 이용하여 암호화된 원격명령을 복호화하는 로직을 A54SX32 FPGA에 구현하고, 구매한 NIST 인증된 DES CFB 코어와 동작 타이밍 시뮬레이션 비교 및 A54SX32 FPGA에 합성된 후의 사용 모듈 면적을 비교하여 동일한 타이밍 시뮬레이션 결과 및 사용 모듈 면적을 얻었다. 또한 원격명령 암호복호기의 기능을 검증하기 위한 인터페이스 로직 및 제어 로직을 함께 하나의 PCB 보드에 구현하였다. 기능시험용 PC를 통하여 암호화된 원격명령 코드블록을 생성하고 원격명령 암호복호기에 전송한 뒤 복호화된 코드블록의 수행코드에 해당하는 LED ON 동작 확인, 복호화된 코드블록을 기능시험용 PC에 피드백하여 전송한 코드블록과 비교 확인 및 실제 FPGA 출력핀의 코드블록 측정 파형과 시뮬레이션 파형 비교 확인을 통해 목표한 1,024bps 전송속도로 원격명령 암호복호 기능을 정상적으로 수행함을 확인하였다.

제시한 다중 KEY 및 IV를 동시에 활용하는 운용개념 때문에 보안성이 현재로서도 충분히 보장되어 있지만 DES보다 훨씬 높은 보안성을 제공하는 TDEA나 AES 알고리즘을 FPGA로 구현하여 대체하면 현재의 설계를 크게 변경함이 없이도 훨씬 강화된 보안성을 제공할 수 있다. 본 연구 결과를 토대로 향후 진행될 CTU EM 및 QM에는 명령 재공격(Replay Attack)[5]을 막기 위한 방법으로 ACC(Authenticated Command Count)를 적용하여 강화된 보안 기능을 구현하고 검증할 예정이다.

후 기

본 연구는 과학기술부의 IMT-2000 기술 개발 지원 사업의 일환으로 수행되었으며 연구비 지원에 감사드립니다.

참고문헌

- 1) CCSDS 910.3-G-2 Consultative Committee for Space Data Systems Cross Support Concept Part 1 - Space Link Extension Services, April 2002.
- 2) CCSDS 201.0-B-1 Consultative Committee for Space Data Systems Telecommand Part 1 - Channel Service, Jan. 1987.
- 3) CCSDS 202.0-B-2 Consultative Committee for Space Data Systems Telecommand Part 1 - Data Routing Service, Nov. 1992.
- 4) CCSDS 101.0-B-3 Consultative Committee for Space Data Systems Telemetry Channel Coding, May 1992.
- 5) CCSDS 350.0-G-1 The Application of CCSDS Protocols to Secure Systems, March 1992.
- 6) FIPS PUB 46-3, Data Encryption Standard(DES), Oct. 1999.
- 7) FIPS PUB 81, DES Modes of Operation, Dec. 1980.
- 8) NIST Special PUB 800-17, Modes of Operation Validation System(MOVS): Requirements and Procedures, Feb. 1998.
- 9) NIST Special PUB 800-38A, Recommendation for Block Cipher Modes of Operation, 2001.
- 10) FIPS PUB 197, Announcing the Advanced Encryption Standard(AES), Nov. 2001.
- 11) 안하기, 신경욱, "AES Rijndael 블록 암호 알고리즘의 효율적인 하드웨어 구현", 정보보호학회논문지, 제 12권, 제 2호, 2002, pp. 53-63.
- 12) 최병윤, 박영수, 전성익, "모듈화된 라운드 키 생성회로를 갖는 AES 암호 프로세서의 설계", 정보보호학회논문지, 제 12권, 제 5호, 2002, pp. 15-25.