고속 영상데이터 암호화에 적합한 SES Alarmed 링크 암호동기 방식

김형락¹ · 이훈재^{2*} · 권대훈³ · 박의영³

A SES Alarmed Link Encryption Synchronization Method for High-speed Video Data Encryption

HyeongRag Kim¹ · HoonJae Lee^{2*} · DaeHoon Kwon³ · UiYoung Pak³

¹Department of Computer Technology and Application, Pohang College, Pohang 791-711, Korea

²Department of Information and Communication Engineering, Dongseo University, Busan 617-716, Korea

³Agency for Defense Development, Daejeon, Korea

요 약

CCSDS 규격은 국제 우주 통신 분야에서 하나의 규격으로 폭넓게 사용되고 있다. 이 규격에서 암호화는 계층별로 고유의 암호 프로토콜을 수행해 통신 채널에서 보안 요구사항을 만족하도록 하고 있고, 동기화를 위해서는 암호화된 데이터의 시작부에 암호화 동기를 삽입하여 수행한다. 그러나 예외적인 상황(타이밍 지터링, 시스템의 비정상적인 종료 등)의 발생 시 수신 장비는 데이터를 수신하더라도 정상적인 데이터를 복원할 수 없게 되는 문제점을 가지고 있다. 본 논문에서는 송수신 도중에 문제가 발생할 경우 송신측에 SES Alarm 신호를 전송하여 정상적인 송수신이 이루어지도록 하는 SES Alarmed 링크 암호동기 방식을 제안하고, 성능 분석을 통하여 SES Alarm 신호를 위한 최적의 조건을 제시하였다.

ABSTRACT

CCSDS Standard is widely used in international space telecommunication area. In this standard, Encryption is realized using a unique hierarchical encryption protocol and satisfied security requirements of communication channels. For synchronization, encryption sync is attached in the beginning of encrypted data. But exceptional case(timing jittering, abnormal system shutdown, etc.) is occurred, receiving equipment cannot decrypt received data. In this paper, we propose a SES Alarmed link encryption synchronization method for sending warning signal to the transmitter when some problems have been occurred during the transmission and we also suggest optimum conditions for SES Alarm signal through performance analysis.

키워드 : CCSDS, 벌크 암호, 링크 암호, 암호 동기

Key word : CCSDS, Bulk encryption, Link encryption, Encryption sync

접수일자 : 2013. 07. 19 심사완료일자 : 2013. 08. 13 게재확정일자 : 2013. 08. 30

* **Corresponding Author** HoonJae Lee (E-mail:hjlee@dongseo.ac.kr, Tel:+82-51-320-1730)

Department of Information and Communication Engineering, Dongseo University, Busan 617-716, Korea

Open Access <http://dx.doi.org/10.6109/jkiice.2013.17.12.2891>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

1982년 위성과 지상 세그먼트의 상호 운용(Interoperability)을 증대시키기 위해 우주 데이터 시스템 자문 위원회(Consultative Committee for Space Data Systems, CCSDS)에서 패킷에 대한 표준 권고안을 발표한 이후 CCSDS 규격은 국제 우주 통신 분야에서 하나의 규격으로 폭넓게 사용되고 있다. 표준 권고안에는 우주 통신연결을 통해 송수신 되는 다양한 전송 기법이나 우주 통신링크 프로토콜, OSI 참조 모델에 적합한 계층화된 모델들을 제시하고 있다. 또한 CCSDS는 위성의 데이터 처리 시스템을 표준화하여 다양한 위성 임무를 수용하고 일관된 기술로 데이터 처리 시스템 개발 비용을 줄이기 위한 작업을 해나가고 있다[7-8]. 표준 권고안은 CCSDS의 자발적인 내용이며 구속력을 갖지 않는다. 따라서 타 기관에서 내용을 변경할 수 있으나 변경 시에는 서로 공유하도록 하고 있으며 압·복호화 및 무결성 알고리즘의 선택은 제약하지 않고 있고, 구현의 문제는 사용자의 몫이다.

CCSDS의 프로토콜 암호화는 계층별로 고유의 암호 프로토콜을 수행해 통신 채널에서 보안 요구사항을 만족하도록 하고 있다. 보안 요구사항의 수준은 고비도(high) 보안, 중비도(moderate) 보안, 저비도(minimal) 보안의 3가지로 구분되는데, 정부나 군에 적용되는 접근 보안은 고비도 보안이 요구된다. 즉, 지상국의 모든 데이터와 모든 원격명령 데이터는 기밀성, 무결성, 접근제어, 인증과 같은 서비스 등이 이루어져야 한다.

CCSDS 프로토콜[9-11]은 동기화를 위해 암호화된 데이터의 시작부에 암호화 동기를 삽입하여 수행한다. 그러나 예외적인 상황(타이밍 지터링, 시스템의 비정상적인 종료 등)의 발생 시 수신 장비는 데이터를 수신하더라도 정상적인 데이터를 복원할 수 없게 되는 문제점을 가지고 있다[1-2,4].

본 논문에서는 송수신 도중에 문제가 발생할 경우 송신측에 SES (Sync Error Signal) Alarm 신호를 전송하여 정상적인 송수신이 이루어지도록 하는 SES Alarmed 링크 암호동기 방식을 제안하고, 성능 분석을 통하여 SES Alarm 신호를 위한 최적의 조건을 제시한다.

II. CCSDS 프로토콜과 보안구조

CCSDS의 프로토콜의 구조는 그림 1과 같다[7-8]. 계층별로 고유의 암호화 과정을 거쳐 통신 채널에서 보안 요구사항을 만족하도록 한다. 보안 요구사항의 수준은 고비도(high), 중비도(moderate), 저비도(minimal)로 구분된다.

고비도 보안(high security)은 정부나 군에 적용된다. 위성체 제어시스템의 접근 보안은 임무 수행중이나 모든 환경 및 운용 조건하에 항상 요구된다. 지상국의 모든 데이터와 모든 원격명령 데이터는 기밀성, 무결성, 접근제어, 인증이 요구되며 모든 원격측정 데이터는 기밀성, 무결성, 인증과 같은 서비스 등이 이루어져야 한다. 중비도 보안(moderate security)는 상용통신, 기상업무, 원격감시, 위성항해 시스템 등에 적용되며 원격명령 데이터는 기밀성을 위한 요구사항, 무결성, 인증이 요구되며 일부 또는 모든 원격측정 데이터는 기밀성, 무결성 등이 이루어져야 한다. 저비도 보안(minimal security)은 기타 다른 시스템에 적용되며 원격명령 데이터는 기밀성을 위한 가능한 요구사항, 무결성, 인증이 요구되며, 일부 원격 측정 데이터와 지상국간의 일부 데이터는 기밀성이 요구된다.

그림 1. CCSDS 프로토콜과 보안구조
Fig. 1 CCSDS Protocol and Security architecture

III. CCSDS 프로토콜 링크 계층 보안

데이터링크 계층 보안을 위해 링크 암호화(link encryption)를 적용한다. 링크 암호화는 통신 시스템의 기밀성을 보장하며 무결성과 인증, 접근제어 서비스에 적용된다. 암호화는 원격명령(Telecommand), 원격

측정(Telemetry), 고급 궤도 시스템 AOS(Advanced Orbiting Systems)의 데이터 구조에 적용된다. 링크 암호화를 사용하는 장비는 데이터 동기화가 필요하고, 코딩 전에 데이터의 습득, 동기화 및 복호화가 이루어지기 때문에 에러검출 및 정정 정보를 평문에서 사용하는 것이 허락되지 않는다.

링크 암호화는 모든 통신 시스템 데이터 구조의 기밀성을 제공한다. 이는 데이터 계층에서 구현되었고, 점대-점(point-to-point) 기반에서 가능한 데이터 기밀성의 최고급 수준을 제공한다. 무결성과 분리하지 않고 인증 또는 접근제어 서비스는 암호화에 의하여 암시적으로 제공되는 기능을 갖는다. 즉, 대칭키 암호가 사용될 때 인증은 암시적으로 이루어지는 것으로 한다. 왜냐하면 수신단에서는 암호해독을 위해서 진짜 키를 알아야만 하고, 이는 확실한 키 분배 시스템에서 승인된 키임을 알 수 있다.

그림 2. 데이터 구조별 링크 암호화
Fig. 2 Link Encryption Classified by Data Structure

그림 2는 데이터 구조에 따른 링크 암호화를 보여준다[9-11]. 원격명령에 대한 링크 암호화를 수행할 경우 CLTU(Command Link Transmission Unit)에 대한 암호화 뿐만 아니라 'Acquisition' 및 'idle' 수열에 대해서도 암호화를 수행하게 된다. 원격 측정의 경우, 패킷 원격 측정 서비스 블루 책자(packet telemetry service blue book)에서 정의된 CA_DSU(Channel Access Service Data Unit)를 암호화 하게 된다. 비슷한 결과로서 링크 암호가 AOS에 적용된다면, 전체 물리채널 접속 프로토콜 데이터 유닛(PCA_PDU, Physical Channel Access

Protocol Data Unit)전체가 암호화 된다.

그림 3. (a) 소스이미지와 (b) 비정상적으로 복호화된 출력 이미지
Fig. 3 (a) Source Image and (b) Abnormal Output Image

CCSDS 프로토콜에 따르면 링크 암호화를 사용하는 암호 장비는 송수신 초기 데이터 동기화를 위해 암호화된 데이터의 시작부에 암호화 동기를 삽입하게 된다. 따라서 송수신 초기단계에서 암호화 동기가 이루어지면 수신부의 암호화 장비는 지속적으로 복호화를 수행하여 데이터를 수신하게 된다. 단, 동기화가 이루어진 이후 송수신 암호화 장비는 안정적인 상태가 계속되어야 한다. 예외적으로 타이밍 지터링 등에 의한 비트 슬림이 발생하거나 전원의 불안전성 등으로 인해 시스템이 비정상적으로 종료 되는 등의 문제가 발생하면, 수신 장비는 데이터를 수신하더라도 암호화된 데이터의 복호화가 불가능하게 되어 정상적인 데이터 복원을 할 수 없게 된다[1-2,4]. 아래 그림 3(a)는 소스이미지를 보여 주고, 그림3(b)는 복호화가 정상적으로 이루어지지 않은 결과 이미지를 보여준다.

IV. SES Alarmed 링크 암호 동기방식 제안

4.1. SES Alarmed 링크 암호 동기방식 제안 배경 및 방안

CCSDS 프로토콜에 따른 링크 암호화의 문제점은 송수신이 진행되는 도중에 문제가 발생할 경우 정상적인 데이터 송수신이 불가능하게 됨에도 송수신 암호화 장비는 이 사실을 확인할 수 있는 방법이 없다는 것이다. 이러한 문제점을 극복하기 위하여 본 논문에서는 SES Alarmed 링크 암호동기 방식을 제안한다. SES

Alarmed 링크 암호동기 방식은 초기 암호화 동기여러를 탐지하거나 링크 계층의 프레임 동기를 지속적으로 탐지하는 과정에서 연속적인 프레임 동기 에러가 검출되었을 경우 송수신 과정에서 문제가 발생한 것으로 가정하고 송신측에 암호화 동기 신호를 재전송하도록 요청한다.

4.2. 제안된 암호동기 실험을 위한 상세 구성

그림 4는 제안된 SES Alarmed 링크 암호동기 방식을 실험·분석하기 위한 상세 구성도를 보여준다.

그림 4. SES Alarmed 암호동기 실험을 위한 상세 구성도
Fig. 4 A detailed Block Diagram for SES Alarmed Encryption Synchronization Experiment

(가) 암호화 모듈의 프로토콜과 성능 분석을 위한 데이터 소스 이미지는 그림 3(a)와 같다.

(나) 암호화는 128비트 단위의 데이터를 128비트의 키로 암호화하는 AES[8] 알고리즘을 적용한다.

(다) 암호동기 삽입

링크 암호화된 데이터는 수신측에서 동기화 할 수 있도록 데이터 송신을 하기 전에 암호화 된 데이터 시작부에 암호 동기 신호를 삽입한다. 이때 동기패턴은 잡음이 존재하는 채널에서 오류가 발생하더라도 수신 동기가 잘 이루어 질수 있도록 신뢰성이 높은 동기방식이 적용되어야 한다. 일반적으로 동기패턴 검출기로는 자기 상관기(autocorrelator)를 많이 사용하는데, 본 논문에서는 잡음이 많은 무선통신 채널에서도 고속 및 고신뢰도를 보장하도록 설계된 자기 상관기에서 추출한 값으로 아래와 같이 자기 상관성이 우수한 동기 패턴을 생성하여 적용한다[3,6].

SYNPAT = 1394 DA8D 7272 C579 B3A8
B379 4BA0 087E(hexa)

(라) 암호동기 탐지

암호화된 데이터가 CAI를 거치게 되면 수신부의 암호화 장비는 먼저 암호화 동기를 검출한 후 복호화 과정을 거치게 된다. 만약 동기패턴이 검출되지 않으면 수신부는 송신측에 재동기 요청을 하게 된다.

(마) 복호화

수신부에서 암호화 동기를 검출하면 그 이후에 들어오는 데이터들에 대해서 AES 암호화의 복호화가 이루어진다. 복호화된 데이터는 이더넷 프레임 구조를 가지고 있으므로 암호화 장비는 각 프레임에서 프레임 동기를 추출한 후 페이로드(payload) 데이터를 추출하여 이미지를 출력하게 된다. 단, 수신부에서 동기화가 이루어 진후 수신이 되는 도중에 여러 가지 환경적 요인으로 인해 송수신 동기가 조금이라도 어긋나게 되면 수신부에서 암호화된 데이터의 복호화는 불가능하게 된다.

(바) 프레임 동기 탐지

복호화된 데이터는 이더넷 프레임구조를 가지게 되는데, 이때 각 프레임 데이터를 추출하기 위해서는 프레임 동기를 찾는 것이 우선된다. CAI를 거치는 과정에서 데이터 오류로 인해 프레임 동기를 찾지 못하게 되면 해당 프레임 정보는 손실된다. 채널코딩/디코딩부에서 1×10^{-6} 의 에러를 보장하더라도 확률적으로 프레임 동기 부분에서 에러가 발생하여 프레임 동기를 찾지 못하게 될 수도 있다.

실제 시스템을 운용할 경우에는 여러 가지 특성의 변화-온도, 습도 등의 환경적 요인-에 따른 시스템의 불안정성 등으로 인한 비트 슬립(bit slip) 현상이 발생하거나, 수신부 시스템의 전원차단, 셧다운 등이 발생하여 수신부의 동기화에 문제가 발생할 수 있는데, 이때 수신측은 송신측에 경고를 보내 주도록 설계한다. 이를 탐지하는 프로토콜로 본 논문에서는 링크계층의 프레임 동기 연속 오류가 일정한 횟수 이상 발생하면 송신측에 재동기 요청을 할 수 있도록 SES Alarm 신호를 전송하도록 한다. SES Alarm 신호를 수신한 송신측은 암호화된 데이터의 앞부분에 암호동기를 다시 덧붙여 전송하게 된다.

V. 실험 및 분석

5.1. CAI 에러율에 따른 실험

본 실험에서는 첫째, CAI 에러율의 변화에 따른 출력 이미지의 손실 정도로 제안된 암호통신 시스템의 성능을 평가하고, 둘째, CAI 에러율의 증가에 따라 프레임 동기 연속에러의 발생 패턴을 분석하여 송신측 재 전송 요구를 위한 최적의 연속 에러 탐지 횟수를 구하고자 한다. 단, 실험결과와 출력이미지에서 프레임 동기 에러가 발생하면 해당 프레임 정보를 찾을 수 없는 것으로 하여, 이전 프레임의 데이터를 채우는 것으로 한다.

그림 5. 에러율 $1 \times 10^{-6} \sim 1 \times 10^{-4}$ 에서의 출력 이미지
(a) 1×10^{-6} (b) 1×10^{-5} (c) 5×10^{-5} (d) 1×10^{-4}

Fig. 5 Output Images at Error rate $1 \times 10^{-6} \sim 1 \times 10^{-4}$
(a) 1×10^{-6} (b) 1×10^{-5} (c) 5×10^{-5} (d) 1×10^{-4}

(가) 에러율 $1 \times 10^{-6} \sim 1 \times 10^{-4}$ 에서 실험 결과

그림 5는 CAI 에러 확률이 (a) 1×10^{-6} , (b) 1×10^{-5} , (c) 5×10^{-5} 및 (d) 1×10^{-4} 의 값일 때 각각의 출력 이미지를 보여 준다.

그림 6. 에러율 $5 \times 10^{-4} \sim 9 \times 10^{-4}$ 에서의 출력 이미지
(a) 5×10^{-4} (b) 7×10^{-4} (c) 8×10^{-4} (d) 9×10^{-4}

Fig. 6 Output Images at Error rate $5 \times 10^{-4} \sim 9 \times 10^{-4}$
(a) 5×10^{-4} (b) 7×10^{-4} (c) 8×10^{-4} (d) 9×10^{-4}

에러 확률이 증가함에 따른 각각의 이미지는 그 값에 비례하여 산발성 이미지 손실이 증가하였지만 손실 정도가 크지 않아서 대체적으로 깨끗한 이미지를 얻을 수 있고, 1×10^{-4} 의 에러 확률에서는 낮은 발생 빈도로 프레임 동기 에러가 발생하여 해당 프레임 전체의 이미지 손실이 발생하는 것을 볼 수 있다.

(나) 에러율 $5 \times 10^{-4} \sim 9 \times 10^{-4}$ 에서 실험 결과

그림 6은 CAI 에러 확률이 (a) 5×10^{-4} , (b) 7×10^{-4} , (c) 8×10^{-4} 및 (d) 9×10^{-4} 에서 각각의 출력 이미지를 보여 준다. 각각의 결과는 에러 확률의 증가에 비례하여 랜덤한 위치에서의 산발성 이미지 손실이 크게 증가하였고, 일회성 프레임 동기 에러의 발생 빈도도 크게 증가하는 것을 확인할 수 있었다. 2회 연속 프레임 동기 에러는 CAI 에러 확률이 5×10^{-4} 의 값이었을 때 평균적으로 1~3회 정도의 빈도로 발생하였고, 에러 확률이 7×10^{-4} 에서 9×10^{-4} 으로 증가함에 따라 2회 연속 프레임 동기 에러가 발생하는 빈도가 4~10회 범위에서 발생하는 것을 확인할 수 있었다.

(다) 에러율 1×10^{-3} 에서 실험 결과

그림 7은 CAI 에러 확률이 1×10^{-3} 이었을 때 출력 이미지를 보여준다. 에러 확률의 증가로 인해 산발성 이미지 손실이 크게 증가하고 프레임 동기 탐지 에러의 발생빈도가 증가함에 따라 이미지 품질이 심각하게 저하된 것을 볼 수 있다. 에러 확률의 값이 1×10^{-3} 으로 증가할 때 나타나는 특징은 낮은 수의 빈도로 3회 연속 프레임 동기 탐지 에러가 발생한다는 것이다.

그림 7. 에러율 1×10^{-3} 의 출력 이미지
Fig. 7 Output Images at Error rate 1×10^{-3}

5.2. 결과 및 분석

앞절의 실험 결과에서 CAI 에러 확률이 1×10^{-4} 이하에서는 이미지의 품질이 양호한 것을 확인할 수 있었다. 따라서 CAI의 채널 코딩 영역에서 최소한 1×10^{-4} 의 값을 보장할 수 있도록 설계되어야 함을 보여 준다. 또한 그림 7에서 보여지는 에러 확률의 값이 1×10^{-3} 이었을 때의 출력 이미지가 수신측에서 인정하기 어려운 최저 품질의 이미지라고 한다면, 본 논문에서 제안한 SES Alarm 신호 전송을 위한 조건을 1×10^{-3} 에러 확률에서 발생하는 3회 연속 프레임 동기 탐지 에러로 설정하는 것이 타당한 것으로 보여 진다.

즉, SES Alarm 신호 전송을 위한 적절한 연속 프레임 동기 탐지 에러의 횟수 기준을 3회로 설정할 것을 제안한다. 그러나 그림 7의 출력 이미지가 수신측에 받아들일 수 있는 이미지 품질이라고 한다면, 송신측에 재동기 요청을 위한 SES Alarm 신호 전송조건을 더 많은 횟수의 연속 프레임 동기 탐지 에러로 늘리는 것이 바람직하다.

VI. 결 론

기존의 CCSDS 프로토콜에 따른 암호화 장비는 송수신 데이터 동기화를 위해 암호화된 데이터의 시작부에 암호화 동기를 삽입하여 송수신 시스템의 초기 동기화를 수행한다. 그러나 실제 시스템 운영에서는 예외적인 상황(타이밍 지터링, 시스템의 비정상적인 종료 등)의 발생시 수신 장비는 데이터를 수신하더라도 정상적인 데이터를 복원할 수 없게 된다.

본 논문에서는 송수신 도중에 문제가 발생할 경우 송신측에 경고신호를 전송하여 정상적인 송수신이 이루어지도록 하는 SES Alarmed 링크 암호동기 방식을 제안하였다. 성능을 분석하기 위하여 채널잡음으로 인한 에러 확률의 증가에 따라 출력 이미지의 열화 정도를 비교·분석하였고, 송신측에 SES Alarm 신호 전송을 위한 최적의 조건을 얻기 위하여 에러 확률의 증가에 따른 프레임 동기 연속에러 발생 빈도를 분석하였다. 그 결과 수신측에서 인정할 수 있는 최저 품질의 수신 이미지가 CAI 에러 확률이 1×10^{-3} 에서 얻은 결과로 설정하였을 경우, 3회 연속 프레임 동기 탐지 에러를 송신측 재동

기 요구를 위한 SES Alarm 전송 조건으로 설정하는 것이 적절함을 제안하였다.

필요에 따라서 에러 확률 1×10^{-3} 값에서 수신되는 이미지 보다 더 열악한 결과라도 수신할 필요성이 있다면 SES Alarm 신호의 조건을 본 논문에서 제안한 링크 계층의 프레임 동기의 연속 에러 횟수를 3회 이상으로 확장해서 사용할 수 있다.

감사의 글

본 논문은 2012년도 국방과학연구소 위탁연구 과제 및 2013년도 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:2013-071189).

REFERENCES

- [1] J.H Yoon, C.S Hwang, "A Resynchronization technique by time-synchronization for secure communication using stream cipher," Proceeding of ICICS'97 , pp.1129-1133, Singapore, 9-12 September 1997.
- [2] Ashraf D. Elbayoumy, Simon J.Shepherd, "Stream or Block Cipher for Securing VoIP?," International Journal of
- Network Security, Vol.5, No.2, Pp.128-133, Sep. 2007
- [3] HoonJae Lee, Il Seok Ko, "An Intelligent Security Agent for Reliable Cipher System using PingPong," Cybernetics and Systems , Vol. 39, No. 7, pp.705-718, Oct. 2008.
- [4] H. J. Beker and F. C. Piper, Cipher System : The Protection of Communications, Orthwood Books, London
- [5] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.
- [6] Joan Daeman, Rene Govaerts and Joos Vandewalle, "Resynchronization Weaknesses in Synchronous Stream Cipher," Pre-Proceedings Of EUROCRYPT'93. 1993.
- [7] CCSDS satellite recommended standard, <http://public.ccsds.org/publications/BlueBooks.aspx>
- [8] Procedure Manual for the Consultative Committee for Space Data Systems, CCSDS A00.0-Y-9, Yellow Book, Issue 9, Washington, D.C.:CCSDS, November 2003.
- [9] Telecommand Part 1:Channel Service, Recommendation for space Data Systems Standards, CCSDS 201.0-B-3, Blue Book, Issue 3, Washington, D.C.:CCSDS, June 2000.
- [10] TC Synchronization and Channel Coding, Recommendation for Space Data Systems Standard, CCSDS 231.0-B-1, Blue Book, Issue 1, Washington, D.C.:CCSDS, September 2003.
- [11] Space Assigned Numbers Authorith(SANA)-Role, Responsibilityes, Policies, and Procedures, CCSDS 313.0-Y-1, Yellow Book, Washington, D.C.:CCSDS, July 2011.

김형락(HyeongRag Kim)

1992년 경북대학교 전자공학과 졸업(학사)
 1994년 경북대학교 전자공학과 졸업(석사)
 2010년 경북대학교 전자공학과 졸업(박사)
 1994년~1995년 LG전자기술원 연구원
 1995년~1996년 (주)문화방송 기술연구소 연구원
 1996년~현재 포항대학교 컴퓨터응용계열 부교수
 ※관심분야: 정보보안, 암호이론, 채널코딩

이훈재(HoonJae Lee)

1985년 경북대학교 전자공학과 졸업(학사)
 1987년 경북대학교 전자공학과 졸업(석사)
 1998년 경북대학교 전자공학과 졸업(박사)
 1987년~1998년 국방과학연구소 선임연구원/팀장
 1998년~2002년 경운대학교 조교수
 2002년~현재 동서대학교 컴퓨터정보공학부 교수
 ※관심분야: 암호이론, 네트워크보안, 부채널공격, 정보통신/정보네트워크

권대훈(DaeHoon Kwon)

1999년 경북대학교 컴퓨터공학과 졸업(학사)
2002년 경북대학교 컴퓨터공학과 졸업(석사)
2002년~현재 국방과학연구소 선임연구원
※ 관심분야 : 데이터통신, 네트워크, 정보보안

박의영(UiYoung Pak)

1982년 연세대학교 전기공학과 졸업(학사)
1988년 연세대학교 전기공학과 졸업(석사)
2003년 연세대학교 전기전자공학과(박사)
1984년~현재 국방과학연구소 책임연구원/팀장
※ 관심분야 : 데이터통신, 네트워크, 정보보안