정 보 보 호 학 회 지
제27권 제2호, 2017. 4

LTE 통신망을 이용한 교통신호제어시스템용 HW 기반 SSL VPN 성능 분석 연구

이 재 훈*, 장 찬 국*, 위 한 샘*, 이 옥 연*

요 약

본 논문에서는 교통신호제어기 표준규격(NPA-TSC-2010 R14)과 호환성을 유지하면서, 교통신호제어시스템과 상용 LTE 이동통신망을 적용 가능한 검증필암호모듈 기반의 SSL VPN을 개발하여, 정보보안의 성능과 교통신호제어기의 통신 성능을 만족할 수 있다는 결과를 제시한다. 또한 '교통신호제어기 표준규격'의 기기 변경이 최소화될 수 있도록 SSL VPN 개발에 필요한 기술을 구현하여 실증결과를 제시함으로써, 이를 바탕으로 교통신호제어 시스템의 보안 표준규격으로 제정될 수 있도록 기술 및 절차적 결과를 제시하였다.

Ⅰ. 서 론

IoT 시장의 발전과 함께 국가 재난망, 산업제어, 주요 기반시설 등 다양한 분야에서 700MHz 기반의 무선통신망 구축과 LTE-x로 지칭되는 PS-LTE, LTE-R, LTE-M 등을 활용한 응용 서비스 개발이 빠르게 발전하면서, 정보보안에 대한 필요성이 관련 법 규정에 요구됨에 따라, 데이터 보안 및 인증을 통해 안전하고 신뢰성 있는 통신환경을 구축하기 위한 공공무선망을 위한 가상사설망(SSL VPN) 적용개발의 필요성이 제시되고 있다.

이와 함께, 2012년 국가 주요 정보통신 기반 시설로 지정된 교통신호제어망에 대한 검증필암호모듈 기반의 SSL VPN 보안 호환성 표준이 제시되고 있으며, 해당 보안 표준규격의 적용 범위는 교통 신호제어용으로 현장에 설치되어 있는 교통신호기 뿐만 아니라. 이와 관련된 교통신호 운영시스템과의 유무통신 정보보안을 위한 부분을 포함한다.

또한, 기존에는 PSTN, 광통신 등의 유선망으로 운영되고 있으나, 통신 품질의 안정성과 예산 절감 등을 위해, LTE 상용망을 이용하는 것이 필요한 만큼, 이동통신 구간의 정보보안을 위해 ARIA-128, LEA-128, SHA-256, RSAES-3072, ECDH, ECDSA(p-256) 등의 128비트급 보안강도를 갖는 암호알고리즘을 채택해야 하며, 검증필암호모듈과 공통평가기준(CC) 인증이 필수적으로 요구되고 있다.

아울러, 교통신호제어시스템은 오작동이나 통신두절 등의 경우 인명사고가 될 수 있으므로, 해당 규격에서 정의한 정보보안은 기존 교통신호제어기 내부 장치와의 호환성과 상호 운영성을 기반으로 VPN 상호인증 및 제어 데이터 암.복호화 및 LTE 무선 통신에 따른 통신 delay에 대한 증명이 필요하다.

Ⅱ. HW 기반 SSL VPN 적용 방안

2.1. 검증필암호모듈 기반 SSL VPN 개요

교통신호제어시스템용 VPN 클라이언트 하드웨어는 기존의 교통신호제어기 내부에 존재하던 모뎀부에 추가되어야 하는 보안 하드웨어 모듈과 무선 통신 모뎀으로 구성된다.[5]

도로 현장에 위치한 교통신호기의 신호주제어부(MCU, Main Control Unit) 내부의 핵심 구성요소인 CPU보드나 운영자입력장치(MMI)에 VPN을 추가할 경우, 현재 운영되고 있는 모든 교통제어시스템 모두를 수정해야 하고, 교통제어기를 교체해야 하므로, 필수적으로 교체해야 하는 기존의 유선용 모뎀보드를 새로운 교통신호제어시스템용 VPN 클라이언트 하드웨어로

* 국민대학교 금융정보보안학과

제작하는 것이 필요하다,

따라서 현재 및 미래의 교통신호 제어시스템 하드웨어와 독립적으로 동작하도록 하여 확장성을 확보하고, 모뎀에 장착 가능한 SSL VPN Client를 탑재하기 위한 교통신호용 모뎀에 장착 가능하도록 전용 HW를 개발하여 실험하였다.

2.2. 교통신호제어기 표준 적용

정보통신기반보호법에 근거하여, 2012년 정보통신기반 보호위원회에서 주요 정보통신 기반 시설로 '교통신호'가 지정됨에 따라, 검증필암호모듈 탑재와 CC 인증 제품이 필수적으로 적용되어야 한다.[3]

본 논문에서 구현한 교통신호제어시스템용 VPN은 TLS v1.2와 국내 교통신호제어시스템용 정보보안 호환 표준규격을 만족하도록 개발하였다.[2]

시험 결과는 TLS을 통해 진행되는 상호 협상의 결과로 확인하였고, 상호 인증 및 키 교환을 통해 명시한 알고리즘이 동작하는지의 여부를 확인하였다.

블록암호(ARIA, SEED, LEA)의 경우 키 길이 128비트 이상, 공개키 알고리즘의 경우 RSA-2048비트 이상을 사용하고, ECC의 경우 256비트급(p-256)의 비도를 갖추도록 하였고, 해시알고리즘의 경우 SHA-2를 사용하였다.

본 논문에서는 [표 1]의 TLS Cipher_suite for ECDH key exchange & ECDSA Certificates, TLS Cipher Suites for RSA certificates에서 명시한 알고리즘을 사용하는지 여부를 확인하기 위해 상호 협상의 결과로 확인하였다.

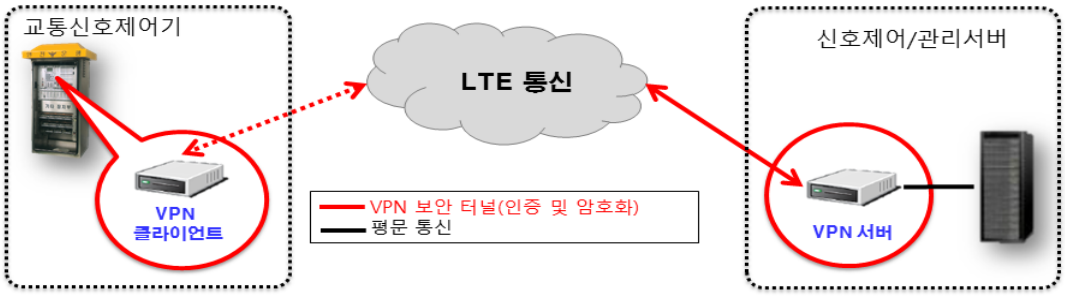
교통신호제어기용 가상사설망 H/W는 기존의 교통신호기 내부에 존재하던 모뎀부와 보안 하드웨어 모듈, 무선 이동 통신 모뎀으로 구성하였고, 교통신호제어기용 가상사설망 H/W는 교통신호제어기 내 모뎀부에 장착하여 시험하였다.

교통신호제어기 내부의 모뎀부는 19인치 표준 랙에 실장되는 카드형으로 센터 중앙장치와 교통신호기간에 데이터 통신을 가능하게 하는 장치이므로, 주제어부 CPU 보드로부터 데이터를 받아 필요한 변조 후 센터로 송출하게 하였고, 수신된 신호는 복조하여 CPU 보드로 전달하게 하는 등의 교통신호제어기 모뎀 부는 기존 교통신호제어기와의 호환성을 위해 경찰청 교통신호제어기 표준 규격을 따른 교통신호제어기와 운영센터를 연결하여 시험하였다.

또한 교통신호제어시스템 유무선범용 표준보안규격서에서 규정한 하드웨어 및 정보보안 규정을 만족하도록 개발하여 통신성능 및 보안성능을 상용 LTE망에서 시험하였다.

2.2.1. 표준 규격서 준용 사항

+ SSL VPN 클라이언트는 교통신호제어기용 모뎀형태로 제작되어야 한다.
+ SSL VPN 클라이언트는 TLS 버전 1.2를 지원해야 한다.
+ SSL VPN 클라이언트 인증이 필요하면 SSL VPN 클라이언트는 인증서를 사용해야하며, 이 인증서는 시스템 내부에 구성되어야 한다. 이 인증서는 DH, ECDH 공개키를 포함하는 인증서이어야 하고, RSA-PSS(2048bit) 또는 ECDSA(p-256)로 서명되어야 한다.
+ SSL VPN 클라이언트는 구현 시 해당 표준에 명시된 Cipher ID를 가지는 Cipher Suites를 지원하도록 구현되어야 한다.
+ SSL VPN 클라이언트는 일정 시간 이내에 복호화 또



〔그림 1〕 교통신호제어시스템용 검증필암호모듈 기반 SSL VPN과 상용 LTE 망에서의 시험 개념도

는 일정 시간 근방에서의 복호화를 지원해야 한다.
+ SSL VPN 클라이언트는 handshake에서 보여준 SSL VPN 서버 인증서에 대한 인증 경로를 만들 수 있어야 한다.
+ SSL VPN 클라이언트는 인증서 경로 유효 규칙에 따라 SSL VPN 서버 인증서를 검증해야 하고 경로 검증이 실패하면 TLS 연결을 종료해야 한다.
+ SSL VPN 클라이언트가 SSL VPN 서버 공개키 길이를 체크하는 메커니즘을 제공하면 클라이언트는 서버의 공개키 길이를 체크해야 한다.
+ SSL VPN 클라이언트는 데이터 채널 기밀성 보안기능을 위해 다음 중 한 가지를 필수적으로 지원해야 한다.
  - ARIA-128-CBC
  - SEED-128-CBC
  - LEA-128-CBC
+ SSL VPN 클라이언트는 데이터 채널 무결성 기능을 위해 다음을 필수적으로 지원해야 한다.
  - SHA256
+ SSL VPN 클라이언트는 LZO 압축 라이브러리를 사용하여 송수신 패킷에 대해 압축할 수 있는 기능을 지원해야 한다.
+ SSL VPN 클라이언트는 SSL 연결시 동작되는 키 유도함수에서 사용하는 키 ID 스트링으로 “commonvpn”을 사용해야 한다.

2.3. 교통신호제어기 표준 HW 규격 적용

모뎀의 하드웨어는 경찰청의 표준 규격에 맞춰 개발하였으며, 실제 교통신호제어기에 장착하여 교통신호 시스템과 연동 시험을 완료한 후, 보안 기능 및 성능을 시험하였다.

2.3.1. 기판(PCB) 규격

+ 크기 : 233.35mm × 160mm
+ NEMA(RR-4) Glass Epoxy
+ 모든 전기적 물질의 표면은 비 부식성임
+ 두께 : 1/16인치 이상임
+ 표시 : Unit에 사용되는 전기 소자는 기본 회로 심벌을 사용하여 표시함

2.3.2. 전면판(Front panel) 규격

+ 6U×4HP(1U : 44.45mm, 1HP : 5.08mm)
+ 모뎀 카드는 좌측 Edge로부터 0.5HP 이격하여 PCB를 접착함
+ 전원이 켜지면 POWER 램프가 켜지고, 외부망을 통해 데이터가 보내지면 두 번째 램프가 깜빡거리고, 외부망을 통해 데이터를 받으면 세 번째 램프가 깜빡거림
+ 전면판 표시 램프 : 전원램프/통신램프로 나뉨
+ 내부망을 통해 데이터가 보내지면 네 번째 램프가 깜빡이고 내부망을 통해 데이터를 받으면 다섯 번째 램프가 깜빡거림
+ 전면판 RST Switch : 모뎀 Reset Switch를 통해 Reset 할 수 있음
+ 전면판에는 외부망과 연결할 이더넷 포트와 내부망과 연결할 이더넷 포트가 있음

2.3.3. 후면 접속장치(Connector) 규격

+ J1 : DIN 41612, Type C, 96Pin, Male
+ J2 : DIN 41612, Type C, 96Pin, Male
+ 전원 12V, 5V이 해당 후면 접속장치를 통해 입, 출

〔표 1〕 교통신호제어시스템 유무선범용 보안표준규격서의 Cipher Suite 발췌

Cipher ID	Name	Key exchange	Encryption	Hash Function for HMAC	Hash Function for PRF
0xD000	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	ECDH	ARIA_128_GCM	SHA-256	SHA-256
0xD001	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_192_GCM_SHA256	ECDH	ARIA_192_GCM	SHA-256	SHA-256
0xD002	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA256	ECDH	ARIA_256_GCM	SHA-256	SHA-256
0xD003	TLS_KCMVP_ECDH_ECDSA_WITH_SEED_128_GCM_SHA256	ECDH	SEED_128_GCM	SHA-256	SHA-256
0xD004	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_128_GCM_SHA256	ECDH	LEA_128_GCM	SHA-256	SHA-256
0xD005	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_192_GCM_SHA256	ECDH	LEA_192_GCM	SHA-256	SHA-256
0xD006	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_256_GCM_SHA256	ECDH	LEA_256_GCM	SHA-256	SHA-256
etc.					

력되며, 모뎀부에서 통신 인터페이스는 전면판 이더넷 인터페이스와 후면 접속장치 등 총 2개가 존재함
+ 전면판 이더넷 인터페이스를 사용할 경우에는 모뎀부 내부의 8핀 스위치를 전부 up 시키고 아래 4핀 스위치를 전부 down 시킨 후 사용 할 수 있음
+ 반대로 후면 접속 장치를 이용할 경우에는 8핀 스위치를 전부 down 시키고 4핀 스위치를 전부 up 시키고 사용하면 됨

2.3.4. VPN HW 규격

본 실험에서 사용한 하드웨어에는 검증필암호모듈(CM-111-2021.3)을 기반으로 TLS v1.2 기반의 SSL VPN을 소프트웨어 모듈로 탑재하고, 교통신호제어기용 CPU로부터 받은 교통신호 제어 데이터를 SSL VPN과 상용 LTE망을 통해 전송하고, 교통신호운영시스템과 SSL VPN 터널링을 수행한다.

〔표 2〕 보안 하드웨어 모듈 사양

부품	사양
Processor	TI AM Processor (Max 800MHz)
RAM	Mobile DDR3 SDRAM 256MByte
Storage	EMMC 8GByte / Micro SD Card
Interface	Giga-bit Ethernet RJ45
	Terminal Socket RS-232/485
	Mini PCIe 8-pin (UART/SPI)
Voltage	DC 12V
Currency	Max 1A

〔표 3〕 무선 이동 통신 모뎀 사양

부품	사양
Main Chipset	MDM 9310
Flash Memory	256MB
RAM memery	128MB
Interface	USB 2.0, UART, GPIO
Air Interface	R99 Network
Frequency Band	LTE FDD Band 1/3/5/7

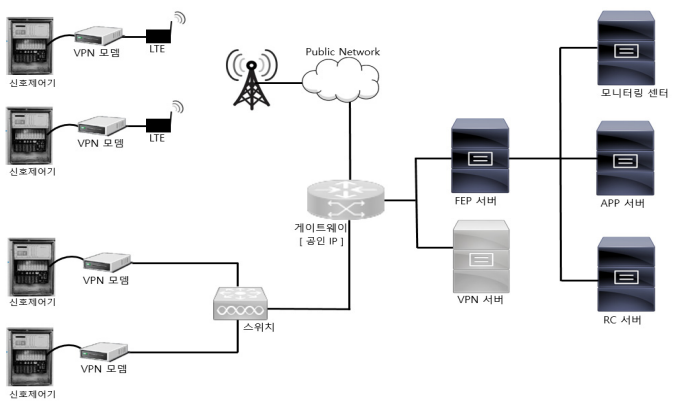
Ⅲ. 실험 방법 및 결과

본 장에서는 교통신호제어기 상용 제품과 운영센터 장비에 SSL VPN을 적용한 실제 시스템을 통해 테스트 환경을 구축하고, 네트워크 성능 측정 프로그램을 이용하여 속도를 측정하고, RSA-2048, RSA-3072, ECDH(p-256), ECDSA(p-256) 등의 공개키 암호알고리즘이 상용 LTE망을 통해 전송되기 위해 필요한 통신 delay 등을 측정하였다.

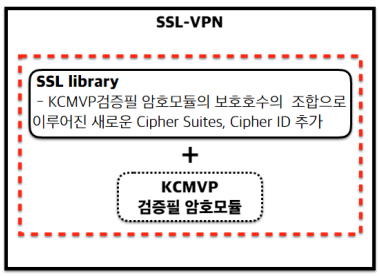
상용 LTE는 무선통신이므로, 자체적으로 갖는 통신 delay가 존재하지만, 그 delay에 비해 128비트급의 비도를 갖는 검증필암호모듈과 기반의 SSL VPN 보안 기능의 delay가 교통신호제어시스템의 운영에 필요한 요구조건을 만족한다는 것을 보인다.

3.1. 실험 방법

교통신호제어시스템용 가상사설망 연동 성능 시험은 VPN 클라이언트, 서버의 기능시험이 완료된 이후



〔그림 2〕 교통신호제어시스템 구성도



〔그림 3〕 검증필암호모듈 기반 VPN

실제 교통신호제어기에는 시험용 toolkit이 없으므로, VPN 클라이언트, VPN 서버에 각각 Laptop을 연결하여 데이터 통신시험, 통신 안전성 시험을 실시하였다.

데이터 통신 시험은 SSL VPN에서 규정한 cipher suite 기반한 보안통신 시의 전송 속도를 측정하기 위한 시험이며, VPN 클라이언트에 연결된 Laptop에서 VPN 서버에 연결된 Laptop으로 데이터 사이즈 별로 데이터를 전송하여 데이터가 전송되는 시간을 측정하였고, 통신 안정성 시험은 ping message를 1분 또는 10분 동안 전송하여 전송 시간 동안 ping에 대한 응답 지연 시간의 최댓값, 최솟값, 평균값을 측정하여 통신에 대한 안정성을 시험하였다.

+데이터 크기: 100B, 1KB, 10KB, 100K, 500K
+데이터 전송 주기: 100ms
+데이터 전송 횟수: 100회

3.2. SSL VPN 성능 실험 결과

본 교통신호제어시스템 VPN 연동 성능 시험은 검증필암호모듈에 기반한 이용한 교통신호제어시스템용 SSL VPN 표준 규격을 반영한 VPN 서버와 VPN 클라이언트 하드웨어를 상용 LTE와 연동 이후 시행한 성능시험에 대한 결과이다.

데이터 통신 시험결과는 데이터 채널 암호화 방법의 변경, 전송 데이터 사이즈 변경에 따른 데이터 통신 시험 결과치를 나타낸 것이다.

이 시험은 각 데이터 사이즈의 패킷을 100번 전송하여 그 중 측정된 최대 전송시간, 최소 전송시간, 평균 전송시간을 측정한 것이며, 통신 안정성 시험결과는 데이터 채널 암호화 방법의 변경에 따른 ping의 응답 지연 시간의 결과치를 나타낸 것이며, ping 데이터를 1분, 10분간 전송하여 결과치를 측정하였으며, 상용 이동통신 환경에 따라 이 수치는 달라질 수 있음을 보여준다.

〔표 4〕 데이터 통신 WITH LEA-128-CBC

	100 Byte	1 KByte	10 KByte	100 KByte	500 KByte
최대 전송 시간(ms)	85.118	87.349	232.280	296.250	888.181
최소 전송 시간(ms)	34.715	40.378	153.609	87.017	308.230
평균 전송 시간(ms)	49.530	62.280	196.613	148.105	504.077

〔표 5〕 데이터 통신 WITH ARIA-128-CBC

	100 Byte	1 KByte	10 KByte	100 KByte	500 KByte
최대 전송 시간(ms)	92.075	162.960	216.509	265.214	1748.71
최소 전송 시간(ms)	38.068	42.754	156.892	92.409	343.356
평균 전송 시간(ms)	60.397	60.226	192.202	152.680	497.520

〔표 6〕 데이터 통신 WITH SEED-128-CBC

	100 Byte	1 KByte	10 KByte	100 KByte	500 KByte
최대 전송 시간(ms)	82.229	106.012	218.106	263.547	1883.65
최소 전송 시간(ms)	46.992	46.283	147.574	81.292	325.240
평균 전송 시간(ms)	61.854	67.705	193.522	154.092	516.964

〔표 7〕 데이터 통신 WITH LEA-128-CBC

	1분(60회)	10분(600회)
최대 왕복 시간(ms)	101	155
최소 왕복 시간(ms)	37	38
평균 왕복 시간(ms)	51	51

〔표 8〕 데이터 통신 WITH ARIA-128-CBC

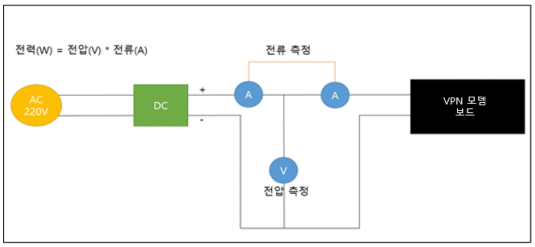
	1분(60회)	10분(600회)
최대 왕복 시간(ms)	622	263
최소 왕복 시간(ms)	44	33
평균 왕복 시간(ms)	69	58

〔표 9〕 데이터 통신 WITH SEED-128-CBC

	1분(60회)	10분(600회)
최대 왕복 시간(ms)	64	93
최소 왕복 시간(ms)	44	41
평균 왕복 시간(ms)	49	50

3.3. SSL VPN 전력 소모량 실험 결과

본 절에서는 검증필암호모듈 기반의 교통신호제어시스템용 SSL VPN이 수행되는 동안 5V와 12V 환경에서 암호알고리즘의 소모 전력량 비교 측정한 결과, 5V 시 차이가 거의 없고, 12V 전원을 사용하는 교통제어시스템 VPN 모뎀보드에 탑재되어 있는 LTE 통신 모뎀과 SSL VPN이 소비하는 전력은 VPN 작동 하지 않고 있는 평상 전력과 VPN 작동 시 전력이 약 2500mW 정도의 추가되는 결과가 도출되었다.



〔그림 4〕 소비전력을 측정하는 환경 구성도

〔표 10〕 교통신호제어시스템용 VPN 전력소모 측정

전압	평상 시 전력	VPN 작동 시 전력
5V	5V * 6.98mA = 34.9mW	5V * 6.97mA = 34.85mW
12V	12V *113.04mA = 1356.45mW	12V *319.82mA = 3837.85mW

〔그림 5〕 교통신호제어시스템 시험 환경

Ⅳ. 결 론

본 논문에서는 공인 기관 검증필암호모듈과 CC 등의 요구사항과 소프트웨어, 하드웨어 규격을 준수하도록 VPN 하드웨어를 제작하고, 교통신호운영센터와 교통신호제어기 사이에는 상용 LTE망을 이용하여, 교통신호제어기와 신호제어표출 신호등 간의 신호제어시스템의 가용성, 무결성, 기밀성의 SSL VPN의 성능 및 통신 지연시간에 대한 분석을 통하여 정보보안 표준이 현재의 무선통신망에서 동작할 수 있음을 입증하였다. 차후, 도로교통신호망이 자율주행차량 등과 보안관점에서 연동 가능함을 입증하는 연구로 발전할 수 있을 것이다.

참 고 문 헌

[1] NIST Special Publication 800-113, Guide to SSL VPNS

[2] NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS), at http://csrc.nist.gov/ publications/nistpubs/

[3] KS X ISO/IEC 19790, 24759 Korea Cryptographic Module Validation Program

[4] ISO/IEC 15408 Common Criteria

[5] 경찰청 교통신호제어기 2010 규격 릴리즈14 교통신호제어기 표준규격서

[6] Badra, M. and Hajjeh, I., ECDHE_PSK cipher_suites for Transport Layer Security (TLS), Internet Engineering Task Force, Request for Comments 5489, March 2009, http://www.ietf.org/rfc/rfc5489.txt

[7] Rescorla, E., TLS Elliptic Curve cipher_suites with SHA-256/384 and AES Galois Counter Mode (GCM), Internet Engineering Task Force, Request for Comments 5289, August 2008, http://www.ietf.org/rfc/rfc5289.txt

〈저자소개〉

이 재 훈 (Jaehoon Lee)
정회원

2013년 3월 : 국민대학교 수학과 졸업
2013년 3월~현재 : 국민대학교 금융정보보안학과 석, 박사 통합과정
관심분야 : 네트워크 보안, 정보보호

장 찬 국(Chankuk Jang)
정회원

2016년 3월 : 국민대학교 수학과 졸업
2016년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
관심분야 : 네트워크 보안, 정보보호

위 한 샘(Hansaem Wi)
정회원

2016년 3월 : 국민대학교 수학과 졸업
2016년 9월~현재 : 국민대학교 금융정보보안학과 석사과정
관심분야 : 네트워크 보안, 정보보호

이 옥 연 (Okyeon Yi)
정회원

1990년 2월 : 고려대학교 대수학 석사 졸업
1996년 8월 : University of Kentucky 대수학 박사 졸업
2001년 9월~현재 : 국민대학교 과학기술대학 금융정보보안학과 교수
관심분야 : 네트워크 보안, 정보보호