기술논단

Pay-TV 서비스를 위한 스마트 카드

조 현 숙/ETRI 위성통신기술연구단 선임연구원
임 춘 식/ETRI 지상시스템연구 부장

차례

Ⅰ. 개 요

스마트 카드는 서비스 사용에 대한 요금지불, 데이타 저장 등을 위한 편리한 도구로서 최근 10여년 사이에 이에 대한 기술이 급속도로 발전하여 여러 응용 분야에 광범위하게 사용하는 추세이다.

스마트 카드 기술이 발달되지 않았던 시대의 Pay-TV 시스템에서 디스크램블링을 위한 키가 디코더 박스에 내재되어 만약 키가 누출되었을때 시스템의 안전성은 가입자의 디코더를 교체했을때 만이 가능하였다. 그러나, 스마트 카드에 기반을 둔 Pay-TV 시스템에서의 안전성은 신용카드 크기의 플라스틱 카드에 안전한 마이크로 프로세서 칩을 내장시켜 유지시킬 수 있다. 즉, 디코더 자체로서는 더 이상의 안전성을 보장할 수 없었으며, 각 가입자들에게 주기적으로 혹은 카드의 안전성에 문제가 발견되었을때 값싸고 편리한 방법으로 키와 알고리즘을 교체할 수 있는 스마트 카드로의 대체가 불가피 하였다.

본 고에서는 Pay-TV에서 필수적인 기능처리 즉, 스크램블링 처리에서의 스마트 카드 기능에 대해서 논하고자 한다.

Ⅱ. Pay-TV 시스템

1. Pay-TV 서비스?

유료 방송에서 제공할 수 있는 서비스 형태는 크게 Subscription과 PPV(Pay-Per-View)로 나누어 고려할 수 있다.

- **Subscription**

가입자가 가입시 신청한 프로그램(즉, 스포츠, 영화, 음악등 채널별)에 대해서 일정기간 만큼

시청할 수 있는 서비스를 말하며, 서비스 운영은 가입자에 주어진 가입자격 및 관리메시지(Entitlement Control/Management Message)에 의해 이루어진다.

• Pay-Per-View(PPV)

1) Advance Booking PPV

가입자가 프로그램 가이드에 제시된 프로그램에 대한 자격을 운영센타에 요구하게 되면, 운영센타는 프로그램이 방영되기전에 가입자격을 해당 가입자에게 보낸다.

2) Impulse PPV

신뢰성이 주어지는 각 가입자는 언제든지 프로그램을 시청할 수 있는 권한이 주어지며, 이에는 프로그램 단위 즉, 선택한 프로그램을 모두 시청하든지 일부분만 시청하든지 해당 프로그램에 대한 요금을 지불하는 형식이다.

• Pay-Per-Time

시청한 시간만큼 요금이 부과되는 방식

2. Pay-TV 시스템의 구조

Pay-TV 시스템은 이미 cable, 지상 전송 매체 혹은 위성을 통하여 NTSC, PAL, SECAM 혹은 MAC 방식으로 서비스를 해왔다. 그 Pay-TV 시스템들의 대부분은 다음과 같이 크게 두 분야로 나누어 고려해 볼 수 있다.

• 스크램블링/디스크램블링 시스템

이 시스템이 갖는 특징은 수신 권한이 부여되지 않은 수신자는 시청할 수 없도록 프로그램 신호(오디오/비디오)를 변환하는 것이다. 보통 이 신호의 물리적인 변환은 시스템에서 어떤 논리적인 순서에 의해서 real-time으로 처리된다. 스크램블링의 예는 비디오 신호 자체 혹은 동기화시 수정을 가하거나, 디지탈 신호 처리를 통한 sound waveform를 변경하는 방법등이 있다.

• 암/복호화 시스템

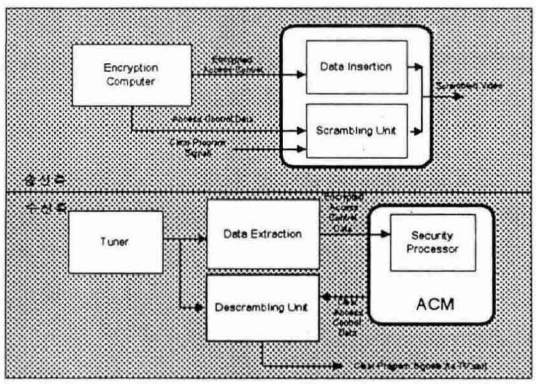
이 시스템은 수신단에서 디스크램블링을 처리하기 위해 사용되는 논리적 순서를 비밀로 처리한다는 것이다. 암호화는 보통 물리적으로 스크램블링 순서를 감추는 데이타 순서에 적용되는 복잡한 수학적인 변환을 말하며, 이 시스템은 안전한 다항식, 비밀키 혹은 공개키 알고리즘을 포함한다. 암/복호화 시스템 수신단은 보통 다음과 같이 두 단계로 나누어 처리된다.

1) Access Control Module

프로그램에서 Access Control은 요금지불과 같은 어떤 조건을 만족하는 시청자들에게만 복호화를 수행하는 것이다. 따라서, 이 Access Control Module은 복호화 처리를 하기 전에 프로그램의 parameter와 가입자의 자격을 조사하게 된다.

2) Security Processor

대부분의 경우에, Access Control Module은 데이타를 보호할 수 있도록 안전한 형태로 관련 비밀 사항과 가입자의 자격을 저장하는 소위 security processor를 가지고 있다.



〈Pay-TV 시스템의 구조〉

Ⅲ. Pay-TV 시스템의 안전성

1. 안전성 문제 제기

Pay-TV 시스템에서의 안전성은 스크램블링 부분과 암호화 부분에서 좌우된다고 할 수 있는데, 보통 안전성 시스템에 문제가 되는 것은 스크램블링 시스템, 암호화 시스템, 혹은 두 시스템 모두에 피해를 당하는 경우이다.

• 안전한 스크램블링

Pay-TV 시스템의 스크램블링 부분에 문제가 되는 것은 스크램블링 처리시 작용했던 access-control data를 모르고서도 스크램블링의 패턴을 알아내기 위해 real-time으로 신호의 특성을 분석하는 것이다. 안전한 스크램블링을 처리하기 위한 여러 방법 중에서 궁극적으로는 깨지지 않는 것이 없으나 문제는 안전성과 가격면을 적절히 조화시킨 것들이 있을 수 있다.

RF-level의 스크램블링은 주파수를 교란시키는 특성을 아는 누군가가 원래의 신호를 복구시키기 위해 관련 filter를 제거하거나 더할 수 있기 때문에 안전하다고 할 수 없다.

동기화 단계의 스크램블링은 복잡한 동기화 분리 회로를 가진 최근의 TV 수신기들은 방해를 받지 않은 영상을 잘 나타낼 수 있기 때문에 역시 안전하다고 할 수 없다.

비디오 신호 자체에 수정을 가하는 스크램블링은 앞의 두가지 형태들 보다는 더 높은 안전성을 제공할 수 있으며, 그러한 신호들을 공격하기 위해서 auto-correlation이나 real-time spectrum 분석을 요한다.

스크램블링 안전성의 가장 높은 단계는 스크램블링/디스크램블링시 신호가 디지탈로 처리되는 시스템에서 발견할 수 있다. 예를들어, 아주 강한 스크램블링 시스템은 음성 신호를 디지탈화하여 time domain에서 sound sample들을 뒤섞으므로서 구축될 수도 있다.

결국, Pay-TV 시스템을 공격한다는 것이 복잡하고 비싼 신호 분석 장비를 필요로 하고 모든 경우에 신뢰성이 보장되는 결과를 초래하지 않으므로 스크램블링 그 자체가 Pay-TV시스템에서의 취약점이라고는 할 수 없다.

• 안전한 암호화

안전성을 요하는 시스템에서 암/복호화는 보통 "firmware"로 구현된다. 소프트웨어 부분은 암호 변환을 위해서 필요로 하는 수학적 함수들을 나타내는 프로그램일 뿐이다. 보통 암호화는 firmware로 구현되고, 이러한 기술들이 컴퓨터 해커들에게 잘 알려져 있기 때문에 그것이 차주 Pay-TV 시스템의 취약점이 될 수 있다.

복호화 시스템과 디스크램블링 시스템 둘다 동시에 공격을 가하는 것은 심지어 더 위험하다고 할 수 있다. 대표적으로 디스크램블링 부분의 간단한 신호의 분석은 복호화 열의 부분을 누설하기 위한 충분한 정보를 만들어 낼 수도 있다. 예를 들어, 외견상 많은 계수들을 가지는 다항식 열과 같은 강한 암호식도 디스크램블링 과정에서 적절한 신호 패턴들을 분석함으로서, 발견할 수 있는 많은 간단한 열들을 모아 놓은 것을 알 수 있다. 대부분의 경우에 복호화장비는 디스크램블링 회로 다음에 놓이게 되며, 같은 "decoder box"에서 동작하게 된다. 또한 암호화 코드가 누설되었을 때, 시스템의 안전성은 가입자의 디코더를 교체함으로써 만이 회복될 수 있었다.

이 방법은 엄청나게 비싼 해결책이라 할 수 있다. 명백한 결론은 decoder box에서 복호화 부분을 떼어 내어 그것을 분리 가능한 모듈로 운영하는 것이 최선책이라 할 수 있다.

2. 안전성을 고려한 모듈 구성

Decoder box로부터 복호화 알고리즘을 취급하는 부분을 떼어내어, security processor로 그들을 분리함으로써, 시스템은 새로운 알고리즘과 향상된 암호화 기술을 받아 들일 수 있는 융통성을 얻을 수 있다고 할 수 있다. TV 안전성에 대한 기술이 계속해서 발전할 것이고 또한, 고정된 알고리

즘은 장기간을 고려해 볼때 안전하지 않기 때문에 이러한 사항은 필수적이라 할 수 있다.

• 분리 가능한 Security Processor

분리형 Security Processor는 시스템의 안전성에 문제가 있다고 판단되었을때는 언제든지 변경될 수 있으며, 또한 보다 강력한 알고리즘이 개발되었을때 수용할 수 있는 융통성을 가지고 있다.

• 분리 가능한 Access Control Module

security processor는 ACM 자체에 포함된다. 복호 알고리즘을 수행하는 것외에 ACM은 프로그램 매개 변수들(date, cost, moral levels..)을 해석하는 것을 하며, 가입자의 자격을 저장한다. 그러므로, 그것의 수행은 pay-TV 운영 구조 즉, 가입 서비스 운영과 고객 관리 방법등을 잘 반영한다. 복호화를 처리하는 security processor 뿐만 아니라 ACM까지도 디코더에서 분리하는 것은 완전한 security를 보장함과 아울러 시스템의 융통성을 더욱 증가 시킬 수 있다.

Ⅳ. 스마트 카드

1. 스마트 카드의 구조 및 기능

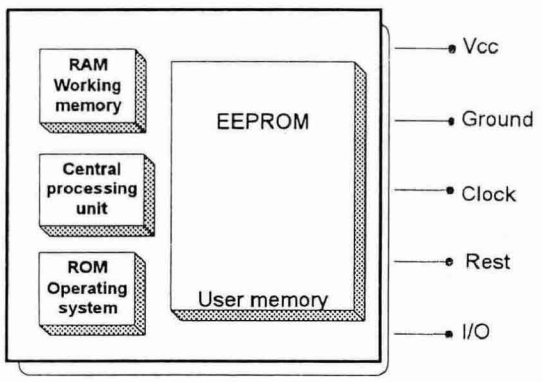
스마트 카드는 신용 카드와 같은 크기의 플라스틱으로 둘러 쌓인 메모리를 가진 micro-computer chip이라 하며, 메모리의 모든 access는 microchip 내에 있는 CPU에 의해서만 제어된다. 스마트 카드를 순수 기억 장치를 가진 메모리 카드와 혼돈하지 말아야 하며, 외견상 신용카드 보다는 약간 두꺼우며, 복수의 메모리 칩들을 가지고 있다. 스마트 카드내에 내장된 마이크로 칩은 OTS(off-the-shelf) 회로가 아니며, HW/SW 보호와 안전성 특성을 가진 customer-designed devide라 할 수 있다. 외부 장치와의 인터페이스는 serial asynchronous eletrical bus를 통해서 수행된다. 스마트 카드의 dimensions, 기계적 특성 및 전기적 인터페이스는 ISO 7816에서 규정하고 있다. 지엽적인 처리 능력, 저장 능력 및 안전성 특성을 고려할 때, 스마트 카드는 분리형 Access Control Module을 완전히 구현할 수 있을 것이다.

• 스마트 카드에 기반을 둔 디코더

Smart Card에 기반을 둔 디코더는 자동 출납 기계의 slot과 같은 인터페이스를 가진 디스크램블러라 할 수 있다. 모든 비밀이 스마트 카드 내에 저장되고, 스마트 카드는 real-time으로 복호화 알고리즘을 처리하는 active device이다. 카드를 decoder box로부터 꺼내게 되면, decoder는 디스크램블링하기 위해서 필요로한 데이타를 더이상 제공하지 않으며, 따라서 더이상 원래의 신호를 생성할 수 없다.

• 스마트 카드 구조

스마트 카드의 microchip은 기본적으로 다른 micro-controller chip과 같은 구조이다. CPU는 ROM, RAM PROM 혹은 EEPROM에 access를 한다. 이 메모리는 외부와 직접 access 할 수 없고, 모든 access는 serial I/O link를 통해 CPU에 의해서 control된다. CPU는 보통 low-voltage detection low-frequency detection, light-detection 혹은 다른 proprietary security 특성들과 같은 special protec-



〈Single Chip의 구조〉

tion circurity를 가진 8-bit 혹은 16-bit 프로세서이다.

• 스마트 카드에 Pay-TV 응용을 어떻게 적용시킬 것인가?

Pay-TV 서비스를 위한 전용 스마트 카드를 개발하는 것은

- 가입자의 자격(entitlement)을 안전하게 저장하고,
- date, level, cost등과 같은 프로그램이 가지고 있는 변수들과 가입자의 자격을 비교하고,
- 프로그램이 가지고 있는 변수들이 가입자의 매개변수들과 같을때 복호화 알고리즘을 수행하는 등의 특별한 프로그램을 스마트 카드에 쓰는 것을 말한다.

대부분의 스마트 카드들은 maked ROM에 OS를 가지고 있어서 memory management, I/O functions, security function등을 운영하며, apllication memory는 특별한 수행을 할 수 있는 프로그램을 가진 OS를 통해서 load된다.

• Marketing Tool로서 스마트 카드

매우 높은 안전성외에 스마트 카드는 TV 방송 운영자가 새로운 서비스와 특성들을 제공하기 위한 장점을 가지는 매우 강력한 marketing tool로서 이용된다.

1) 융통성

인코더/디코더 시스템이 망을 운영하기 위한 데이타들을 처리한다는 것이 명백하기 때문에, 전체 시스템의 동작은 가입자 관리 센타에서 운영되는 소프트웨어와 가입자 측의 스마트 카드에 있는 소프트웨어에 의해 결정된다고 할 수 있다. 이것은 TV 운영자가 스마트 카드에 새로운 프로그램을 교체하거나 스마트 카드를 갱신함으로써, 실제로 가입 방법, 프로그램 가격, 방영 수준 결정, PPV 관리와 같은 정책을 변경할 수 있다.

2) 독립성

여러 TV 운영자들이 같은 디코더 박스들을 공유한다 해도, 그들은 운영 방법과 그들의 비밀성을 공유하는 것을 필요로 하지 않는다. 그들 각각이 자신의 logo를 가진 스마트 카드를 가지고 자신의 방법대로 그들의 운영을 구현할 수 있다.

3) 광고 효과

카드는 종이와 같이 프린트되기 때문에 상업성의 효과도 발휘할 수 있다.

4) TV 서비스의 확장

TV 채널에 가입하는 새로운 방법을 제공하는 것 외에도, 스마트 카드는 새로운 형태의 서비스를 창출할 수 있다. 예를 들면, Pre-paid Teleshopping, Interactive Games, Electronic Coupons 등을 들 수 있다.

2. 스마트 카드 안전성과 알고리즘

• 하드웨어 안전성

기존의 마이크로컴퓨터 칩들과는 달리, 스마트 카드는 안전성 목적을 위해서 특별히 설계되고, 구조 역시 안전성을 위해서 최적화 되었으며, single chips를 사용한다. 외부장치와는 단지 하나의 serial signal connection만을 가지고 있으며, silicon level에서 다음의 protection mechanisms를 가지고 있다.

- 칩내에 addressing line들의 memory pattern들은 어떤 주어진 데이타의 물리적 위치 검색을 어렵게 하기 위해서 "스크램블"될 수 있다.
- 고온, 낮은 전류, 낮은 클럭 주파수 등과 같은 비정상적인 조건들을 찾기 위해서 많은 실리콘 센서들이 내장되어 있다.
- 어떤 위험스런 access lines를 절단하기 위해서 fuse logic이 사용될 수 있다.

• 비밀 코드를 통한 수동적인 카드 안전성

스마트 카드내의 메모리 영역은 자신의 비밀 코드를 가진 작은 가상의 안전성으로 생각할 수 있다. 카드의 마이크로 프로세서는 관련 비밀 코드가 올바르게 생성되지 않으면 메모리의 특별한 영역을 엑세스할 수 없다. 단지 제한된 횟수(보통 3~4회)의 범위내에서만 카드의 엑세스가 가능하고 일정횟수 이상 잘못 엑세스 되었을때는 카드가 lock된다. 비밀 코드는 보통 64비트 이상될 수 있으며, 아주 민감한 영역을 보호하기 위해 여러가지 방법으로 혼합될 수 있다. 비밀 코드는 카드의 생명 주기중 운영 단계에서 사용될 수 있으며, 그 특이한 예로 PIN이 사용된다.

• 암호를 통한 능동적인 카드 안전성

스마트 카드가 디코더로 투입될때, 중앙 관리 센타로부터 전송되어온 유일한 ID 번호로 어드레스된다. 그러한 메시지들은 스마트 카드에 도달하기 전에는 수정될 수 없으며, 어떤 경우에는 프라이버시가 보장될 때, 그들의 내용을 감추기 위해서 필요하다. 카드로 보내진 메시지의 무결성에 대한 보호는 "signatures"로 수행되고, 카드만이 알고 있는 비밀성에 기반을 둔 암호 기능은 보호될 메시지의 내용에 적용되어 그 결과가 그 메시지의 끝에 첨가되어 함께 전달된다. 카드는 적절한 알고리즘을 가지고 그 signature를 계산하며, 그것이 전송된 signature와 부합되는지를 검증한다. 메시지 그자체의 내용을 감추는 것은 암호를 통해서 수행될 수 있으며, 카드가 알고 있는 비밀키 S에 기반을 둔 암호 함수 Fs가 메시지에 적용된다. 그 함수의 결과는 암호화된 메시지가 된다. 스마트 카드는 처리전에 메시지를 복구하기 위해 역함수 Fs를 적용한다. 스마트 카드의 주기능이 디스크램블링을 하기 위한 real-time access-control data를 복호화하는 것이기 때문에 Pay-TV Smart Card는 항상 복호화 기능을 포함한다.

• 능동적인 카드 인증

위에 제시된 보호 기능 외에도 진짜 카드를 흉내냄으로써 스마트 카드를 완전히 모방 하려고 하는 해커들이 있다. 여러가지 ID number를 가지고 스마트 카드를 파생시키거나 카드의 모방을 감소시키기 위해 인증 스킴이 필요하다.

Pay-TV 시스템에서 카드 리더처럼 동작하는 디코더가 카드에 저장된 비밀 키를 알 수 없기 때문에 그러한 인증 기능은 전통적인 비밀키 알고리즘에 기반을 둘 수 없으며, 소위 "zero-knowledge proof" 스킴 즉, 카드가 비밀을 포함하는지를 디코더가 결정할 수 있는 시스템을 사용한다. 각 카드의 ID number가 비밀코드를 포함하는 함수를 가지고 sign 할 수 있다.

zero-knowledge proof algorithm은 비밀코드를 알 필요도 없이 카드의 ID signature의 인증을 체크하기 위해 사용된다.

디코더는 증거를 검증하기 위해 필요로 하는 zero-knowledge proof algorithm을 포함해야 하는 한편 스마트 카드는 그 증거를 계산하기 위해서 사용된 알고리즘을 포함해야 한다.

• 복호 알고리즘

Pay-TV 시스템의 주된 임무는 디스크램블링 메카니즘을 작동시키는 암호화된 데이타를 real-time으로 복호화시키는 것이다. 위에서 언급했던 것처럼, 스마트카드에 기반을 둔 Pay-TV의 원리는 고정된 암호 기술은 역 공학에 공격 받기 쉽다는 암시하고 있다. 따라서, 스마트 카드에 의해 수행된 알고리즘은 변경될 수 있음을 알 수 있다. 더우기, TV 운영자는 정기적으로 스마트 카드를 변경시킬 수 있다.

• 카드 분실로부터의 보호

카드 교체시 카드의 도난이 우려되는 이러한 것을 막기 위해 'chaing' 메카니즘이 이용될 수 있다.

이상과 같이 카드의 안전성 면을 고려하면 다음 표와 같다.

ATTACK	ANSWER
Attack the contents	HW Protection
of the card's memory	Presentation of Secret Codes
Attack the interface to the smart card	Message Signatures Message Encryption
Emulating or cloning Smart Cards	Active Authentication and fingerprinting
Theft of Smart Cards	Chaining Mechanism

V. Smart Card와 TV 시스템의 결합

Pay-TV 시스템에 스마트 카드를 적용시키는 것은 아주 간단하다. 스마트 카드를 나머지 시스템들로부터 분리시키는 인터페이스를 명확히 규정되어야 하고 관련 소프트웨어는 카드와 송신측의 중앙 시스템 둘다에 쓰여져야 한다.

• 디코더와 스마트 카드의 인터페이스

스마트 카드는 카드 컨넥터와 적절한 전기적 인터페이스 회로와 부합되어야 한다. low-level 통신 프로토콜과 마찬가지로 물리적 인터페이스는 ISO7816-3에 정의되어 있으며, 이 인터페이스는 9600 bauds에서 동작되는 serial asynchronous protoeol에 기반을 두고 있다.

• 스마트 카드내의 소프트웨어

스마트 카드 마이크로 프로세서칩이 특별한 하드웨어 안전성을 위한 특성들을 가지고 있다 할지라도, 그들의 core는 6805나 8048과 같은 표준화된 마이크로 프로세서 구조를 따르고 있다. 그러므로, 스마트 카드에 의해서 수행될 code를 개발한다는 것은 상품화를 위한 product를 위한 code를 쓰는 것과 같으나 주된 차이는 디버깅 과정이라 할 수 있다. 이를 위해 스마트 카드 칩을 제조하는 모든 제조자들은 개발자들에게 특별한 에뮬레이터를 제공한다. Pay-TV 코드는 칩 제조 단계에서 ROM으로 적재된다.

• 카드의 분배

카드는 플라스틱 카드에 고객의 이름과 주소등을 프린트함으로써 personalize된다. 카드가 서비스 제공자를 통해서 제공된다면 카드의 로고도 프린트될 수 있다.

카드의 분배과정 중에 시스템의 안전성에 위협을 받지 않도록 특별한 주의를 해야 한다.

VI. 결 론

Pay-TV 시스템에 스마트 카드를 소개하는 것은 unmatched level에서 안전성을 제공하고, 새로운 가입자 관리 기술과 marketing 방법들에서 새로운 아이디어를 제공하는 강력한 도구라 할 수 있다. 스마트 카드가 많은 나라들에서 아직까지는 잘 알려져 있지 않더라도 기술은 서유럽에서 선도적인 역할을 하면서 아주 발달되어 왔다. ISO 표준이 카드의 low-level 기능들을 기술하고 있다.

스마트 카드는 보통 반도체 기술에 기반을 두고 있으므로, 이 분야에서 거대한 향상을 꾀할 수 있을 것이다. 따라서, Pay-TV 시스템에서 스마트 카드를 사용하는 것은 미래 지향적인 선택이라 할 수 있다. Pay-TV에서 스마트 카드의 소개가 최근에 나타나고 있는 실정이며, 영국, 프랑스, 호주, 뉴질랜드, 독일, 스페인 등에서 각자의 기술을 발표하고 있는 현실이다. 스마트 카드는 차세대를 위한 Pay-TV에서의 필수 불가결한 기술임에 분명하다.

筆者紹介

▲趙 賢 淑
- 1980년 2월 : 전남대학교 수학과 졸업(학사)
- 1990년 8월 : 충북대학교 대학원 전산학과(석사)
- 1982년 3월 ~ 1992년 12월 : ETRI 교환기술연구단
- 1993년 1월 ~ 현재 : ETRI 위성통신기술연구단

※주관심분야 : Cryptography, Communication Security

▲任 春 植
- 1975년 2월 : 한국항공대학교 통신공학과(공학사)
- 1986년 2월 : 한국항공대학 대학원 석사(통신전공)
- 1992년 3월 : 일본 요코하마국립대학 전자정보공학과박사(전자정보)
- 1973년 3월 : 군복무(공군ROTC)
- 1980년 6월 : 국방과학연구소
- 1995년 현재 : 한국전자통신연구소 지상시스템연구부장

※주관심분야 : 정보이론(체널코딩), 디지틀이동통신, 대역확산통신, 위성통신망 및 신호처리기술