情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

# SIM/USIM의 표준화 동향에 관한 연구

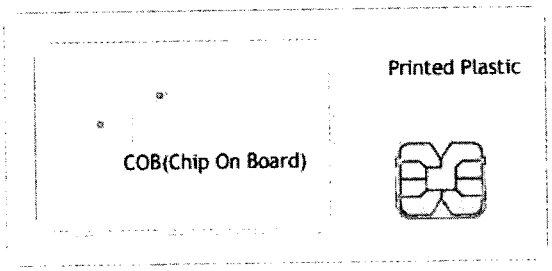
원 동 규*, 조 은 성*, 양 형 규**, 김 승 주***, 원 동 호****

요 약

정보통신 기술의 발전으로 산업 각 분야에서 이러한 기술을 활용한 여러 서비스들이 제공되고 있다. 하지만 이러한 정보통신기술이 삶에 편리함을 주는 반면, 정보화 사회의 역기능으로 인한 문제들이 대두되면서 보안의 중요성은 날로 증가되고 있다. 전 세계적으로 널리 보급된 이동통신 기술에서도 통신의 도청과 정당한 사용자로의 위장 등 많은 사회적 문제들이 제기됨으로서 이동통신에서의 보안은 그 초기부터 고려된 사항이었다. 이러한 문제점을 해결하기 위해 많은 기술들이 적용되기 시작하였고, 그 중에서도 암호 기술은 보안에서 빼놓을 수 없는 주요 기술이 되었다. 이동통신 기술의 빠른 발전과 더불어 보안의 중요성이 크게 대두되기 시작하였으며, 현재 그 중심에는 SIM과 USIM 카드가 자리잡고 있다. 통신단말기에 삽입되어 이용되는 스마트카드는 통신 트래픽(traffic)의 암호화 기능을 제외한 사용자 관련정보의 보안기능 수행에 있어 빠질 수 없는 중요한 요소가 되었다. 그러므로 본 고에서는 SIM과 USIM의 발전동향과 그 기반이 되는 스마트카드 기술에 대해 알아보고, SIM의 보안특성과, 현재 3G서비스(USIM)에 제공되는 보안기술에 대하여 설명한다.

## Ⅰ. 서 론

스마트카드인 SIM(Subscriber Identity Module)과 USIM(Universal Subscriber Identity Module)은 마이크로프로세서와 메모리를 내장하고 있어 카드 내부에서 정보의 저장과 연산, 처리가 가능한 카드를 말한다. SIM 카드는 기존 스마트카드의 일반규격을 활용하는 동시에 새로운 규격이나 특성을 개발하여 이동전화단말기 환경에 적합한 형태로 진보하였다. 스마트카드가 지닌 보안특성과 이동통신 상에서의 무선 전자상거래를 위한 사용자 인증 기능을 가진 SIM은 현재 이동통신 사업에서 없어서는 안 될 중요한 요소로 자리잡고 있다. SIM 기술의 빠른 발전으로 이제 IMT-2000기술을 모두 수용하는 USIM의 도입 등 보다 광범위한 혁신 및 변화가 이뤄지고 있으며, USIM은 이동통신 사업자들이 전 세계 고객들에게 무선 전자상거래, 무선 동영상 및 다양한 부가가치 서비스를 제공할 수 있는 기회를 확대시켜 주고 있다. 다음




〔그림 1〕 스마트카드

그림 1은 스마트카드의 기본 구성을 나타내고 있다.

CDMA 2000과 WCDMA 같은 제 3세대 이동통신 서비스(3G service)와 함께 등장한 USIM 카드의 역사는 1982년 유럽 통신 관할 기관들의 협의체였던 CERT(Conference Europeennedes Postes et Tele-communication)가 유럽지역 내 제 2세대 이동통신의 단일표준을 만들기로 결성하면서부터 시작되었다. CERT는 여러 유럽국가간의 이동통신서비스가 호환성을 제공하지 못한다는 불편함을 해결하기 위

* 성균관대학교 정보통신공학부 정보통신보호연구실({dkwon, escho}@dosan.skku.ac.kr)
** 강남대학교 컴퓨터미디어 공학부 부교수(hkyang@kangnam.ac.kr)
*** 성균관대학교 정보통신공학부 조교수(skim@ece.skku.ac.kr)
**** 성균관대학교 정보통신공학부 정교수(dhwon@dosan.skku.ac.kr)

해 GSM(Groupe Mobile Special)이라는 하위기관을 만들었으며, GSM은 유럽 국가들에게 통일된 서비스와, 무선망 규격을 제공하기 위해 새로운 표준을 제정하였다.

이러한 규격을 제정하던 GSM은 국가간의 로밍 사용에 따른 가입자 인증 필요성의 강화와 불편한 가입 절차의 해결을 위해 SIM카드를 도입하기로 결정하였다. 초기의 SIM은 사용자 인증을 위한 데이터와 기본적인 네트워크 정보 및 사용자 정보만을 가진 형태로 도입되었으며, 부가 서비스를 제공하기 위한 토큰으로서 그 역할을 점차 확대시키게 되었다.

이 후 3G(3세대 이동통신) 서비스를 위해 3GPP와 EP SCP(ETSI Project Smart Card Platform)를 중심으로 새로운 스마트카드 기술을 정의하고자 하였다. CDMA와 TDMA 등의 표준화 기구가 ETSI와 3GPP의 입장에 동의하면서 EP SCP에서는 통신방식에 관계없는 스마트카드 규격으로 UICC (Universal IC Card)와 USIM(Universal SIM) 규격을 작성하고 있다.

## II. 스마트카드

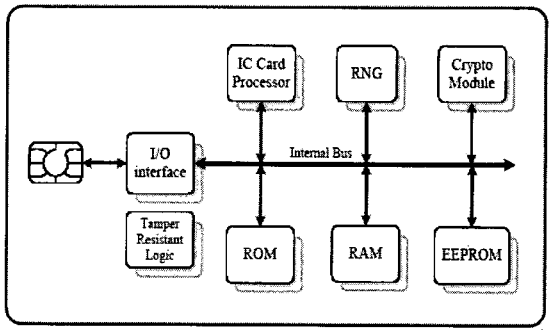
### 2.1 스마트카드의 구조

본 장에서는 스마트카드의 정의와 표준규격, 보안요소 등에 관한 내용을 간단히 설명한다.

스마트카드(Smart Card)는 일반적인 신용카드와 동일한 재질과 크기의 플라스틱 표면에 자체 연산기능이 있는 마이크로프로세서와 운영체제(COS), 메모리, 암호알고리즘이 내장되어 있는 직접회로(IC) 칩이 부착된 전자식 카드이다.

- ㅇ 스마트카드의 구성요소 : 마이크로프로세서, 운영체제, 저장메모리(ROM, RAM, EEPROM), 암호모듈, 랜덤 수 발생기 (RNG), I/O 인터페이스
- ㅇ 스마트카드의 특징
  - 별도의 전원공급장치가 내장되어 있지 않음 (외부로부터 전력공급)
  - 마그네틱카드보다 10-100배 많은 정보를 저장
  - 스마트카드와 터미널 사이에 상호인증 작업 수행

초기의 스마트카드는 I/O 인터페이스와 프로세서, ROM, EEPROM, RAM 등으로 구성되었다. 하지만 보안성 강화를 위해 현재 암호모듈과 랜덤 수 발생기 등이 추가되어 사용된다.



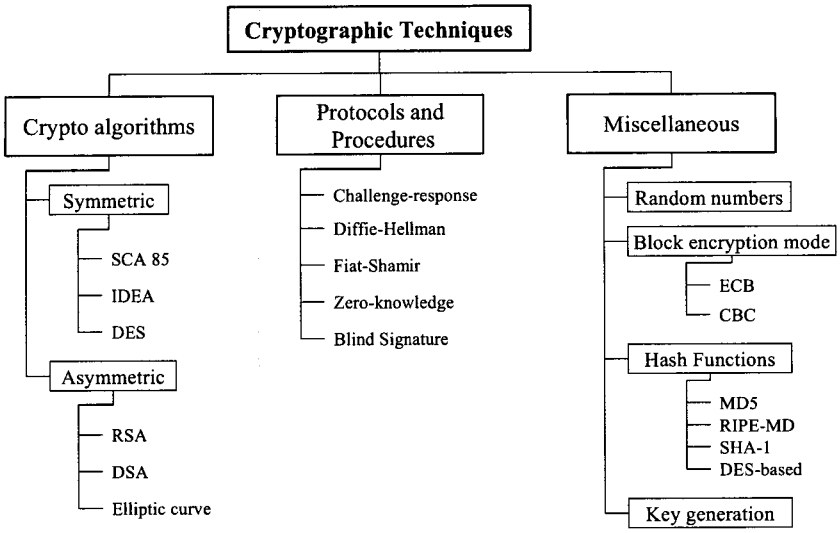

〔그림 2〕 스마트카드의 구조

랜덤 수 생성을 위해 여러 기법이 사용되는데, 주로 사용되는 방법으로는 FIPS 140-2(Security Requirements for Cryptographic Module)에서 정의한 네 가지 방법과 물리적 현상을 이용한 방법이 있다. 그림 3은 스마트카드에서 사용되는 암호기법을 나타낸 것이다.

- ㅇ FIPS 140-2에서 정의한 랜덤 수 생성기
  - NIST, Digital Signature Standard(DSS), FIPS 186-2, Appendix 3.1
  - NIST, Digital Signature Standard(DSS), FIPS 186-2, Appendix 3.2
  - ANSI X9.31, Appendix A.2.4
  - ANSI X9.62, Appendix A.4

물리적 현상을 이용한 랜덤 수 발생기는 자연현상을 이용하여 랜덤 수를 발생시킨다. 대표적인 예로는 Intel 랜덤 수 발생기가 있다. Intel 랜덤 수 발생기는 열잡음을 사용하는데, Intel CPU에 내장된 칩셋을 이용하여, 레지스터에 있는 열소음에서 표본을 취한 값을 시드(Seed) 값으로 이용한다. 회로는 오직 CMOS에 의해 구성되며, 외부입력을 받지 않는다. 이러한 물리적 현상을 이용한 랜덤 수 발생기는 높은 수준의 랜덤 수를 생성할 수 있으며, 다음의 랜덤 수 생성을 위한 요구사항을 만족한다.

- ㅇ 랜덤 수의 요구사항
  - 패턴을 숨길 수 있도록 충분히 긴 주기를 가져야 한다.
  - 생성된 랜덤 값의 평균은 1 또는 0이어야 한다. (0 비트와 1비트의 숫자가 비슷해야 한다.)
  - 출력값을 예측할 수 없어야 한다.




〔그림 3〕 스마트카드에 적용되는 암호 기법

- 빠른 수행능력을 가지며, 간단한 알고리즘이어야 한다.

렌덤 수는 FIP 140-2에서 정의한 방식을 이용한 테스트 회로를 가지고 있으며, 이 방식은 다음과 같다.

- o n(>15)비트 블록을 생성하는 각각의 요청에 대해 랜덤 수는 처음 n비트 블록은 저장하고 다음에 생성되는 블록들과 비교한다. 만약 나중에 생성된 블록과 처음에 생성한 블록이 같다면 테스트는 실패.
- o n(<16)비트 생성하는 각각의 요청에 대해 랜덤 수는 처음 n비트는 저장하고 다음에 생성되는 비트들과 비교한다. 만약 나중에 생성된 비트와 처음에 생성한 비트의 시퀀스(sequence)가 같다면 테스트는 실패.

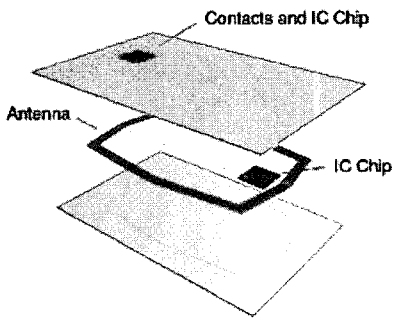
## 2.2 스마트카드의 분류

스마트카드는 계산 능력, 인터페이스, 운영체제에 의해 구분된다. 연산 능력에 따른 분류는 프로세스의 탑재 여부에 따라 메모리카드와 마이크로프로세서 카드로 분류된다.

- o 메모리(Memory) 카드
  - 카드내의 비휘발성 메모리를 포함
  - 데이터의 쓰기/읽기 가능
  - 공중전화 지불 시스템
- o 마이크로프로세서(Microprocessor) 카드
  - 마이크로프로세서(Intel 8051, Microchip PIC) 내재
  - 적은용량의 프로그램 수행 및 정보 저장

인터페이스에 따른 분류는 스마트카드 I/O 포트의 접촉유무에 따라 접촉식(Contact) 카드와 비접촉식(Contactless) 카드로 구분되며, 하나의 마이크로프로세서에 접촉패드와 안테나가 연결되어 있는 것을 콤비(Combi)카드, 하나의 스마트카드 안에 접촉식 마이크로프로세서와 비접촉식 마이크로 프로세서가 동시에 들어있는 형태를 하이브리드 (Hybrid) 카드라고 한다. 그림 4는 하이브리드 카드의 구조를 나타낸 것이다.

현재 스마트카드의 운영체제로 오픈 플랫폼 (Open-platform) 카드와 멀티플 어플리케이션 (Multiple-Apllication) 카드가 있다. 오픈 플랫폼 카드는 카드




〔그림 4〕 하이브리트 카드 구조

가 발행된 후 주어진 카드에 새로운 어플리케이션 기능을 추가할 수 있도록 허용한 카드로, 표준언어와 개방형 API(Application Programming Interface)를 사용하는 새로운 어플리케이션 개발이 가능해지는 계기가 되었다. 이러한 운영체제를 가지는 대표적인 카드로는 자바카드와 마이크로 소프트 카드, MULTOS 등이 있다. 멀티플 어플리케이션 (Multple-Application) 카드란 다른 형태의 어플리케이션을 지원할 수 있도록 만들어진 카드이다.

스마트카드의 물리적 규격은 ISO/IEC 표준기구에서 정의하였고, 이는 추후 SIM카드의 물리적 규격에도 적용되는데, 이를 살펴보면 다음과 같다.

- ISO/IEC 7810 : ID카드의 물리적 특성 규정
- ISO/IEC 7811-1 : ID카드의 기록방법 중 엠보싱 방법을 규정
- ISO/IEC 7811-3 : ID카드의 기록방법 중 ID-1 카드에 양각된 문자의 위치를 규정
- ISO/IEC 7816-1 : 접점을 가지는 집적회로 카드에 대하여 물리적 특성을 규정
- ISO/IEC 7816-2 : 접점을 가지는 집적 회로 카드에 대하여 접점의 치수 및 위치를 규정
- ISO/IEC 7816-3 : 접점을 가지는 집적회로 카드에 대하여 전자신호 및 전송프로토콜을 규정
- ISO/IEC 7816-4 : 접점을 가지는 집적회로 카드에 대하여 상호교환을 위한 산업간 명령체계를 규정

## Ⅲ. SIM과 USIM

### 3.1 SIM, USIM의 표준동향

SIM은 앞에서 정의한 스마트카드 표준규격을 활용하는 동시에 이동통신 단말기 환경에서 활용하기 위해 새로운 규격과 특성을 개발하였다. GSM에서 널리 사용되고 있는 플러그인 형태의 작은 스마트카드나 고온에서 견딜 수 있는 재질의 플라스틱 도입, 3V-5V 전압으로 동작하는 스마트 카드의 규격작업 및 개발 등이 그러한 예들이다.

SIM은 식별자(Identity)를 가진 개체로서, 모바일 상에서 이용되는 IMSI(International Mobile Sub- scriber Identity)정보를 포함하고 있다. 이 IMSI 정보를 이용하여 사용자 인증을 수행하게 되며, SIM카드가 ME(Mobile Equipment)에 삽입되었을 때 비로소 GSM 네트워크에 등록된 MS(Mobile Station)로 동작할 수 있게 된다. 하지만 SIM에 대한 서비스의 요구는 실제로 크게 적용되지 못했다. 유럽 표준과 북미 표준 간의 상호 로밍을 위한 SIM은 3G 서비스를 겨냥해 3G 서비스 이전에 글로벌 로밍을 구현하겠다는 목표로 수행되었지만 실제 상용화에는 실패하였다. 이에 GSM은 3G 서비스를 위하여 USIM 카드의 표준화작업을 진행 하였다.

이동통신 방식별로 사용되는 가입자 모듈과 표준화 기구를 간단히 정리하면 다음 표 1, 2, 3과 같다.

〔표 1〕 표준화 기구 현황

| 이동통신방식 | 가입자 모듈 | 표준화 기구 |
|---|---|---|
| GSM | SIM | ETSI SMG 9 |
| WCDMA+α | USIM | EP SCP / 3GPP TSG-T |
| CDMA | UIM | 3GPP2 |

〔표 2〕 SIM 규격

| 규격번호 | 규격내용 |
|---|---|
| GSM 02.17 | SIM카드의 일반적인 개요 |
| GSM 02.19 | SIM카드용 API에 대한 요구사항 |
| GSM 03.40 | SMS 서비스 정의 |
| GSM 11.11 | SIM카드의 물리적, 논리적 규격 정의 |
| GSM 11.12 | 저전압(3V) SIM카드 규격 정의 |
| GSM 11.14 | SIM Application Tool Kit(STK) 규격 정의 |
| GSM 02.48 | STK를 이용한 SIM – 네트워크 간 인터페이스에 대하여 표준 보안 방법 |
| GSM 03.48 | 일반적인 형태와 SMS를 사용하는 경우의 패킷 보안방법 |
| GSM 11.15 | STK를 이용한 SIM-네트워크 간 인터페이스에 대하여 표준 보안방법의 타당성 조사 |
| GSM 11.17 | SIM 테스트 규격 |
| GSM 11.21 | GSM 무선망 기지국 규격 |

〔표 3〕 USIM(및 UICC) 규격

| 규격번호 | 규격내용 |
|---|---|
| TS 102 221 | 멀티 애플리케이션 플랫폼으로서의 물리적, 논리적, 전기적 규격을 정의 |
| TS 102 223 | 기술방식에 독립적인 범용의 CAT |
| TS 102 222 | 개인화 과정을 위한 규격 |
| TS 31.102 | TS 102 221의 물리/논리적 규격을 USIM에 적용 |
| TS 51.011 | GSM 단말기의 USIM 지원방법 |
| TS 122 038 | USIM 애플리케이션 툴킷 서비스 기술 |
| TS 131 101 | 3G IC카드(UICC)의 물리적, 논리적 특성 정의 |
| TS 121 111 | USIM과 UICC의 요구사항 정의 |

### 3.2 약어

ETSI에서 사용되는 약어 중 본 고에서 사용되는 용어는 다음과 같다.

- o AK Anonymity Key
- o AKA Authentication and Key Agreement
- o AMF Authentication management field
- o AN Access Network
- o AuC Authentication Center
- o AUTN Authentication Token
- o CK Cipher Key
- o CCK Common Cipher Key
- o DCK Derived Cipher Key
- o GCK Group Cipher Key
- o HE Home Environment
- o HLR Home location Register
- o IMSI International Mobile Subscriber Identity
- o IMEI Internation Mobile Station Equipment Identity
- o IMEISV Internation Mobile Station Equipment Identity and Software Version
- o KSI Key Set Identifier
- o LI Lawful Interception
- o MGCK Modified Group Cipher Key
- o MS Mobile Station
- o SCK Static Cipher Key
- o SGCK Sealed Group Cipher Key
- o SGSN Serving GPRS Support Node
- o SN Serving Network
- o SQN Sequence Number
- o SwMI Switching and Management Infrastructure
- o VLR Visitor Location Register

## Ⅳ. SIM의 보안특성

본 절에서는 ETSI EN 300 812에서 정의한 SIM/USIM의 보안 특성에 대하여 설명한다. SIM/USIM이 지원하는 보안 특성을 살펴보면 다음과 같다.

- o 가입자 ID 인증
- o 데이터의 기밀성
- o 파일접근 제어
- o 키의 기밀성

ETSI EN 300 392-7표준은 MS의 보안레벨을 정의하였다. 아래의 표 4와 표 5는 보안 레벨과 레벨에 따른 SIM의 보안능력을 정의하였다.

SIM과 GSM의 기반시스템간의 인증은 그림 5와 같은 방식으로 이뤄진다. 인증과정을 위해 A3과 A8과 같은 암호 알고리즘을 사용하는데, GSM 시스템에서의 암호 알고리즘은 기밀사항으로 다뤄지고 있다. 이는 키르히호프의 법칙(Kerckhoff's principle) 중 '암호 알고리즘이 공개되었을 때, 키의 길이는 짧아서는 안 된다.'는 원칙에 기반 한다. 실제로 GSM은 128비트 길이의 키를 사용하는데, 이는 암호 알고리즘을 공개하기에는 너무 짧은 길이를 가지기 때문이다. SIM에서 사용되는 알고리즘을 정리하면 다음 표 6과 같다.

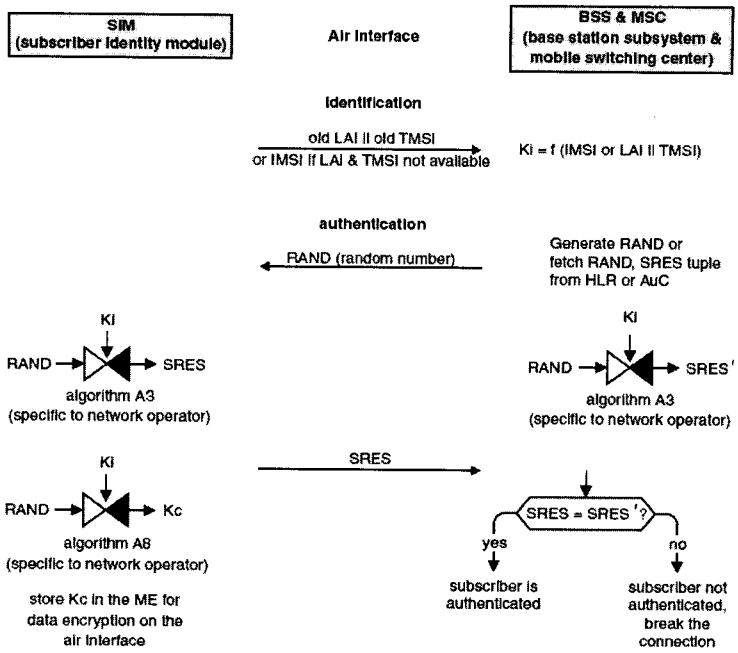
〔표 4〕 보안레벨

| | |
|---|---|
| Class 1: | 암호화를 사용하지 않음 |
| | 인증기능 사용 |
| Class 2: SCK Mode | SCK 암호화 사용 |
| | SCK를 이용한 ESI 사용 |
| | 인증기능 사용 |
| Class 3: DCK Mode | 인증기능 사용 |
| | DCK, CCK, GCK, MGCK의 사용 |
| | CCK를 이용한 ESI 사용 |

〔표 5〕 보안레벨에 따른 SIM의 보안 서비스와 키의 저장

| Class | Authentication | Key store | OTAR SCK | OTAR GCK | OTAR CCK |
|---|---|---|---|---|---|
| 1 | O | n/a | n/a | n/a | n/a |
| 2 | O | SCK | O | n/a | n/a |
| 3 | M | DCK, CCK, GCK, MGCK | O | O | M |

Note 1: 인증기능이 제공될 경우, SIM은 인증 키 K를 저장해야 한다.
Note 2: M=Mandatory, O=Optional, n/a=not applicable




〔그림 5〕 SIM과 GSM 기반 시스템간의 인증과정

〔표 6〕 SIM에서 사용되는 알고리즘

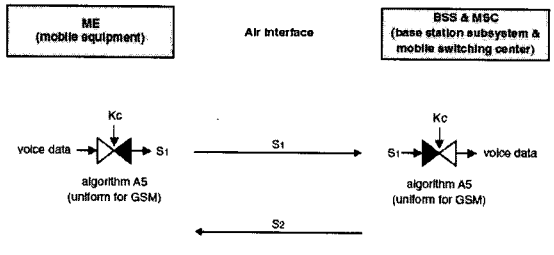
| 알고리즘 | 기능 |
|---|---|
| TA 11/TA 12 | SwMI에서 SIM 인증 |
| TA 21/TA 22 | SIM서 SwMI 인증 |
| TB 4 | DCK 생성 알고리즘 |
| TA 32 | 봉합된 CCK로 부터 CCK 획득 |
| TA 41/TA82 | 봉합된 SGCK로 부터 GCK 획득 |
| TA41/TA52 | 봉합된 SCK로 부터 SCK 획득 |
| TA71/TE | GCK로 부터 MGCK 획득 |
| TB7/TA52 | OTAR에 의해 분배되는 SSCK로 부터 SCK 획득 |
| TB7/TA82 | SGCK로 부터 GCK 획득 |

사용자가 통화를 하는데 있어 통화내용의 실시간 암호화는 연산능력과 전송능력을 고려했을 때 스마트 카드인 SIM에서 수행하는 것은 많은 무리가 있다. 따라서 이러한 실시간 암호화는 단말 장비인 ME에서 수행되며, 대신 SIM에서는 통신연결마다 생성되는 $K_c$의 키 생성 기능을 수행한다.

## V. 3G 보안(USIM)

### 5.1 USIM

UMTS(Universal Mobile Telecommunication System)로도 알려진 3G(3세대 이동통신 기술) 관련




〔그림 6〕 암호화를 통한 데이터 전송

작업이 활발히 진행되고 있다. UMTS에 관련된 표준화 작업은 1998년도 까지 ETSI에 의해 수행되어 졌으며, 후에 3GPP(Third Generation Partnership Project)로 이관되었다. UMTS의 표준화 작업 내에는 USIM 관련 기술이 포함되어 있다. USIM은 GSM의 SIM과 동일하게 사용자 프로파일, UMTS 상에서의 인증을 위한 키, 사용자 데이터등을 저장하고 있으며, SIM과 같이 ME에 삽입과 제거가 가능한 장치이다. USIM의 기술 개발은 인증 프로세스의 유연성과 보다 강력한 보안에 초점을 맞추어 진행되었다. USIM 표준화는 보다 강력한 보안기능을 제공하기 위해 공개키 기반구조(PKI)의 사용을 목표로 진행되었으나, 짧은 연구기간과 공개키 기반 구조를 적용하는데 있어서의 복잡성으로 인해 아직 공개키 기반 구조를 적용하지 못하고, 대칭키 시스템을 그대로 사

용하고 있다. 3GPP는 추후 USIM이 가지는 어플리케이션의 유연성을 기반으로 대칭키 시스템에서 공개키 시스템으로의 변환을 진행 중에 있다.

USIM은 대칭키 시스템을 기반으로 한 인증기능을 제공하지만, GSM에서 사용된 프로토콜과 알고리즘에 많은 변화를 주었다. 그 첫 번째가 $MAC_s$과 같은 새로운 암호 알고리즘의 적용이고, 두 번째로 카운터(counter) 기능을 제공하였다. 카운터는 USIM이 메시지의 freshness를 확인할 수 있는 기능을 제공한다.

앞에서 기술한 어플리케이션의 유연성을 제공하기 위해 USIM에서는 PDL(Protocol Description Language)를 적용하였다. 이 언어는 UMTS의 인증을 위한 프로토콜의 설계를 위한 플랫폼으로 사용될 것이며, 다음과 같은 특징을 제공한다.

- o USIM에 새로운 알고리즘을 저장하지 않고, 프로토콜의 변환이 가능하다.
- o 암호알고리즘의 기술에 있어 간단한 방정식과 기호로 표시할 수 있다.
- o PDL은 대칭키 시스템뿐만 아니라 공개키 시스템에도 적합하며, 이는 하나의 시스템에서 다른 시스템으로의 매끄러운 이동이 가능하게 한다.
- o PDL은 Java와 같은 소프트웨어 플랫폼과 호환이 가능하다.

### 5.2 3G 보안 원칙

3G 보안은 다음 세 가지 원칙에 따라 발전하였으며, TS 33.120에서 정의하고 있다.

- o 3G 보안은 2G보안에 기반하여 개발된다.
- o 3G 보안은 2G보안보다 향상되어야 한다.
- o 3G 보안은 새로운 보안 특성을 제공할 것이며, 3G에서 제공되는 새로운 서비스를 안전하게 할 것이다.

3G에서 이용되는 2G 보안서비스는 다음과 같다.

- o 서비스 접근을 위한 사용자 인증 : 2G에서 사용되었던 부적합한 알고리즘을 검토하고, 인증 옵션 조건을 명확하게 한다.
- o 암호기능 : 2G에서 보다 암호 강도를 강화한다.(키의 길이, 알고리즘 설계)
- o 사용자 ID의 기밀성 : 보다 안전한 메커니즘 설계
- o SIM과 홈 네트워크 서버 사이의 안전한 어플리케이션 계층을 제공하는 SIM 어플리케이션 툴킷 보안 특성
- o 보안특성은 사용자에게 독립적으로 동작한다.(사용자는 시스템 동작과정에서 어떠한 것도 수행하지 않는다.) 하지만 보안특성 동작의 가시성을 사용자에게 제공해야 한다.
- o 보안기능에 대하여 SN에서 HE의 신용을 최소화 한다.

2G 보안의 취약점은 다음과 같다.

- o "false BTS"를 이용한 active attacks이 가능하다.
- o 네트워크 사이와 네트워크 안에서 암호 키와 인증 데이터가 그대로 전송된다.
- o 암호화는 코어 네트워크(core network)의 전 부분에 걸쳐 사용되지 않았다.
- o RAND를 사용하는 사용자 인증에서 이전에 생성된 암호화 키를 사용한다. 또한 임의의 네트워크에서는 암호화를 사용하지 않으며, 채널 탈취에 대한 보안규정은 맹목적인 사용자 인증을 제공한다.
- o 데이터의 무결성이 제공되지 않았다.
- o IMEI는 안전하지 않은 ID이다.
- o 2G 시스템은 유동적인 보안업그레이드를 제공하지 않는다.
- o LI는 2G 시스템의 설계 단에서 고려되지 않았으나 후에 주요 설계 사항으로 재고되었다.

새로운 3G 보안은 기존의 2G 보안의 승계와 더불어 2G의 보안 취약점을 보완함으로서 보다 안전한 서비스를 제공할 수 있게 되었다.

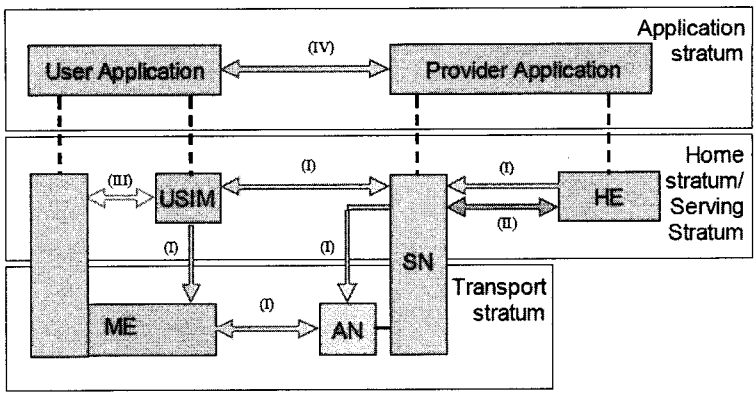
### 5.3 3G 보안 아키텍쳐

본 절은 ETSI TS 133 102 표준에 정의된 기술을 정리한 것이다.

#### 5.3.1 SIM과 USIM의 보안 특성

본 표준에서는 5개의 보안특성 그룹을 정의하고 있다.

- o Network access security(I): 3G 서비스의 안전한 접근을 사용자에게 제공, 특히 access




〔그림 7〕 보안 아키텍쳐

link 상에서의 공격에 대한 보안을 취급.

- Network domain security(II): 신호 데이터 (signalling data)의 안전한 교환을 위해 서비스 제공자 도메인 노드에 대한 보안을 정의하며, 무선네트워크 상에서의 공격에 대한 보안을 연구
- User domain security(III): MS으로의 안전한 접근을 위한 보안 특성을 연구.
- Application domain security(IV): 사용자 어플리케이션과 서비스 제공자 어플리케이션 간의 안전한 메시지 전송을 위한 보안 특성을 연구
- Visibility and configurability of security(V): 각 보안 특성의 동작여부와 서비스의 제공과 사용이 보안 특성에 관련되어 사용되는지의 여부를 사용자에게 알려주는 보안의 가시성과 구성에 대해 연구

보안특성 (I), (III), (IV), (V)는 다음과 같은 세부적인 특성을 포함하고 있다.

### o Network access security(I)

◆ 사용자 신원의 기밀성(User identity confidentiality)

: 이 특성은 다음과 같은 세 가지 보안특성으로 이뤄져 있다.

- 사용자 신원의 기밀성: 서비스가 수행될 때, 영구적인 사용자 신원(IMSI)는 통신상에서 추적 불가능해야 한다.
- 사용자 위치 기밀성: 사용자가 있는 지역 및 위치는 통신상 도청에 의해 발견되지 않아야 한다.
- 사용자 추적 불가: 공격자는 도청을 수행함으로서, 사용자의 다른 서비스의 실행여부를 아는 것이 불가능해야 한다.

이러한 특성은 일시적 신원확인(temporary identity)을 통해 사용자 인증을 수행함으로서 이뤄진다. 또한 사용자의 신원을 노출시킬 수 있는 사용자 데이터와 시그널링을 암호화함으로서 지켜질 수 있다.

◆ 객체 인증(Entity authentication)

- 사용자 인증: 이는 serving network가 사용자의 신원를 확인함으로서 이뤄진다.
- 네트워크 인증: 사용자에게 서비스를 제공하는 HE에 의해 권한을 부여받은 serving network를 사용자가 확인함으로서 이뤄진다.

이러한 인증은 사용자와 네트워크 사이의 연결설정 단계에서 이뤄진다. 이 두 가지 인증은 사용자의 HE에 의해 유도되는 인정벡터를 사용하는 인증메커니즘과 인증 전에 수행되는 사용자와 서브 네트워크 사이에 생성된 무결성 키를 사용한 로컬 인증(local authentication) 메커니즘이 있다.

◆ 기밀성(Confidentiality)

- 암호 알고리즘 동의: MS와 SN은 이후 통신에 사용될 알고리즘을 안전하게 협상한다.
- 암호키 동의: MS와 SN은 이후 사용할 암호키를 협상한다.
- 사용자 데이터의 기밀성: 사용자의 데이터는 통신 인터페이스 상에서 누설되지 않아야 한다.
- 시그널링 데이터의 기밀성: 시그널링 데이터는 통신 인터페이스 상에서 누설되지 않아야 한다.

◆ 데이터 무결성(Data integrity)

· 무결성 알고리즘 동의: MS와 SN은 이후 사용될 무결성 알고리즘을 협상한다.

· 무결성 키 동의: MS와 SN은 이후 사용될 무결성 키를 협상한다.

· 데이터 무결성과 시그널링 데이터의 인증: MS 또는 SN은 SN과 MS에서 보내진 데이터가 권한없는 방식으로 수정되지 않았음을 확인할 수 있는 성질을 가지고 있어야 한다.

이러한 기밀성과 데이터 무결성은 키 동의와 인증 메커니즘을 통해 이뤄진다.

◆ ME 신원확인

· SN은 MS에게 터미널의 IMEI 또는 IMEISV의 전송을 요구한다. IMEI는 터미널에 안전한 방식으로 저장된 정보이다. 하지만 IMEI와 IMEISV는 네트워크 상에서의 신원확인 과정 중 보호되지 않는 정보이다.

o User domain security(III)

◆ 사용자와 USIM 사이의 인증

· USIM을 정당한 사용자만이 사용할 수 있도록 규정한 것으로, 사용자 개인 또는 사용자들에게 권한을 부여할 수 있다. 이는 사용자와 USIM 사이에 비밀정보(PIN)를 공유하도록 한 방식이다. 사용자는 비밀정보의 검증을 통해 USIM에 접근 할 수 있다.

◆ USIM과 터미널간의 연결

· 터미널이 USIM의 권한을 확인하는 과정으로, USIM과 터미널은 상호간에 비밀정보를 공유하고 있어야 한다.

o Application Security(IV)

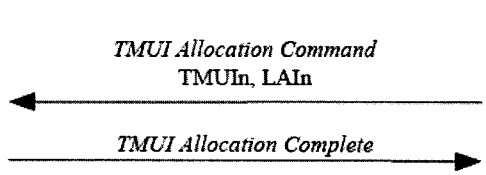
◆ USIM과 네트워크 사이의 안전한 메시지 전송

· USIM 어플리케이션의 안전한 네트워크 통신을 위해 요구되는 보안요소이다. 이러한 보안요소의 레벨은 네트워크 운영자 또는 어플리케이션 제공자에 의해 선택되어진다.

o Security Visibility and configurability(V)

◆ 가시성(Visibility)

· 일반적으로 보안특성은 사용자에게 투명하게 제




〔그림 8〕 TMSI의 분배과정

시되어야 하며, 다음과 같은 보안 이벤트 정보가 사용자에게 전달되어진다. 사용자 정보가 암호화 여부, 사용자가 방문한 네트워크의 보안레벨, 낮은 보안 레벨을 가지는 네트워크와의 로밍 서비스 여부 등이 그 예이다.

◆ 구성(Configurability)

· 사용자가 시스템 동작과 관련한 보안서비스의 레벨 설정 및 사용여부를 결정할 수 있도록 한 것으로, 다음과 같은 구성 특징을 제공한다. 사용자와 USIM간의 인증 수행 여부, 통신설정 중 암호화 기능의 설정 여부, 암호 알고리즘의 사용 여부 등이 있다.

5.3.2 네트워크 접근 보안 매커니즘

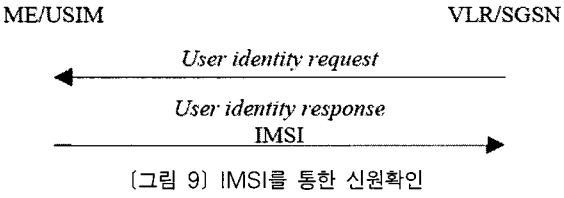
• 일시적 신원확인

이 메커니즘은 TMSI(Temporary Mobile Subscriber Identity)를 사용하여 사용자 인증을 수행하는 것으로, 라우팅 지역(routing area)와 같은 한정된 지점에서 사용된다. 이 후의 지역에선 LAI(Location Area Identification)와 RAI(Routing Area Identification)등을 인증에 사용한다. 이러한 TMSI의 분배는 그림 8과 같은 방식을 통해 이뤄지며, 전송되는 메시지들은 암호화 되어 전송된다.

VLR은 새로운 TMSI($TMSI_n$)을 생성하고 $TMSI_n$과 IMSI의 상관관계를 저장하여 둔다. 새롭게 생성된 TMSI는 예측할 수 없는 값이어야 하며, VLR은 TMSI와 새로운 위치 지역 ID($LAI_n$)을 사용자에게 전송하여 준다. 사용자의 MS는 새로운 TMSI를 저장하고, 이전에 분배된 TMSI를 제거한다. 후에 확인 메시지를 VLR에게 전송해 준다. VLR은 확인메시지를 수신하면, 이전의 IMSI와 $TMSI_o$를 삭제한다.

• 영구적 ID의 신원확인

영구적 ID(IMSI)는 일시적 ID(TMSI)를 사용하여 인증할 수 없을 때나, 서브네트워크에 처음 등록할



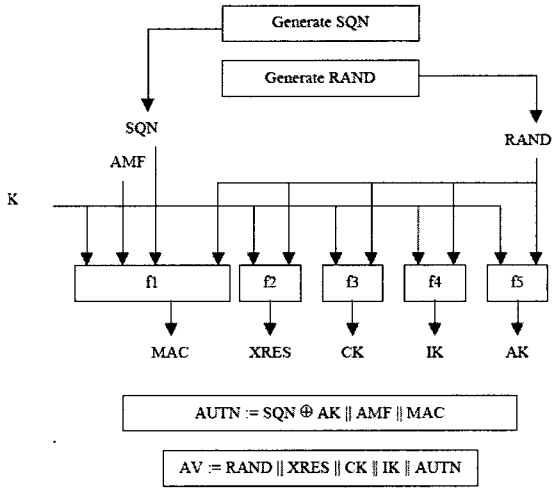

〔그림 9〕 IMSI를 통한 신원확인

때 또는 서브네트워크가 TMSI로부터 IMSI를 복구할 수 없을 때 사용된다. 신원확인 절차는 다음 그림 9와 같다.

• AKA 프로토콜

그림 10은 AKA 프로토콜의 동작과정을 나타내며, 이 과정은 VLR/SGSN으로부터 처음 시작된다. HE는 n개의 배열로 이루어진 인증 백터를 VLR로 전송해주게 되고, VLR은 이전에 사용된 인증 벡터 다음의 인증벡터 중 RAND와 AUTN를 MS에 전송해 준다. 인증벡터는 랜덤 수 RAND와 기댓값 XRES, 암호화 키 CK, 무결성 키 IK, 인증토큰 AUTN로 구성되어져 있다. 이러한 각 인증 벡터는 한번의 인증과 키 동의에 사용되어 진다.

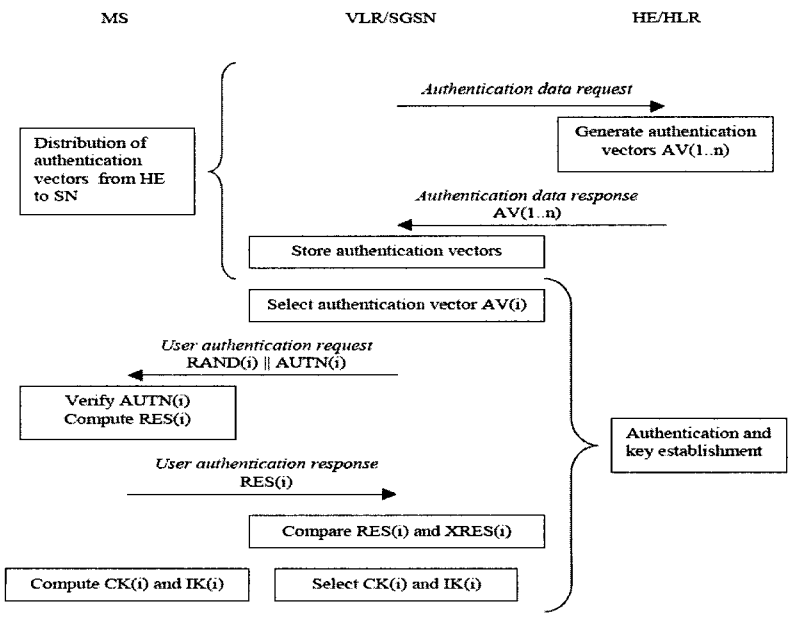
RAND와 AUTN을 수신한 MS는 RES를 계산하여 VLR로 전송해 주고, CK와 IK를 계산한다. VLR은 수신한 RES와 기댓값 XRES를 비교하여 값이 동일할 경우 가지고 있던 CK와 IK를 이용



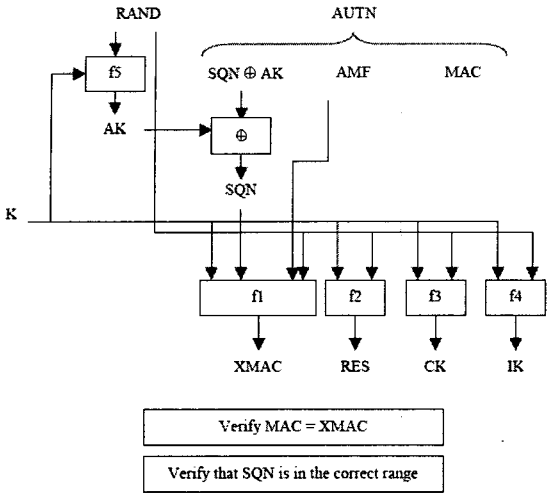

〔그림 11〕 HE에서의 인증벡터 생성

MS와 안전한 통신을 수행하게 된다.

그림 11은 HE에서 생성하는 인증벡터 생성과정을 나타낸다. HE는 각 가입자에 대해 저장하고 있는 Sequence Number SQN과 새로 생성한 랜덤 수 RAND, 인증 관련 필드 AMF를 이용하여 인증벡터를 생성하게 된다. 이렇게 생성된 키 중 AK는 SQN을 보호하기 위해 사용되며, IK는 ME와 네트워크 단에서의 시그널 메시지의 무결성을 제공하기 위해 사용된다. $f_1$ - $f_5$는 암호 함수로 $f_1$, $f_2$은 MAC




〔그림 10〕 AKA 프로토콜(인증과 키 동의과정)




〔그림 12〕 USIM에서의 사용자 인증 함수

함수이며, $f_3$, $f_4$, $f_5$는 키 생성 함수이다. 이 함수의 자세한 사항은 3GPP TS 25.321과 ETSI EN 300 392-7에서 정의하고 있다. 하지만 앞에서도 언급했듯이 함수 알고리즘에 대해서는 공개하지 않는다. SQN의 자세한 사항은 ETSI TS 133 102을 살펴보라. 그림 12는 인증토큰 ATUN과 RAND를 사용하여 USIM에서의 키 생성과 RES 생성과정을 보여준다.

이러한 인증 및 키 동의(AKA) 프로토콜은 다음과 같은 특성을 가지고 있다.

- o 객체 인증
- o SN과 사용자간의 키 동의
- o 양방향 묵시적 키인증
- o 양방향 Key freshness
- o Key Seed 확인
- o 사용자 정보에 대한 기밀성 제공

인증 파라미터들의 길이
- *K*: 128비트
- *RAND*: 128비트
- *SQN*: 48비트
- *AK*: 48 비트
- *AMF*: 16비트
- *CK*: 128비트
- *IK*: 128비트
- *RES*: 4-16 octets

## Ⅵ. 결 론

본고에서는 SIM과 USIM의 기반이 되는 스마트 카드의 동향과 보안 기능에 대해 설명하였다. 또한 이동통신 사업의 보안에 있어 중요한 요소로 부각되고 있는 SIM과 USIM의 표준화 동향과 보안특성에 대해 기술하였다. SIM과 USIM의 관련표준 중 보안에 관련한 표준인 ETSI EN 300 392-7, TS 133 102, EN 300 812를 중심으로 설명하였으며, 이러한 표준은 인증, 무결성, 기밀성, 데이터 접근조건, 네트워크 보안요소, 보안 아키텍처 등 다양한 보안특성을 기술하고 있다. 본고에서는 이러한 보안특성 중 인증기술, 암호 알고리즘, 2G에서 3G로 넘어가는 과정에서의 보안요구사항 3G(USIM)의 추가적인 보안 기술 위주로 기술하였다.

본 연구는 향후 SIM과 USIM의 보안연구를 진행함에 있어서의 기반자료로 널리 활용할 수 있을 것으로 기대된다.

## 참 고 문 헌

〔1〕 Wolfgang Rankl and Wolfgang Effing, John, "Smart Card Handbook - third edition", Wiley & Sons, Ltd.

〔2〕 ETSI, "ETSI TS 133 102, Universal Mobile Telecommunications System(UMTS): 3G security: Security architecture", Technical Specification, 2004.

〔3〕 Günther Horn, Peter Howard, "Review of third generation mobile system security architecture", ISSE 2000, Barcelona, Spain.2000

〔4〕 "3G TS 33.120, 3rd Generation Partnership Project: Technical Specification Goup Services and System Aspects: 3G Security: Security Principles and Objectives", Technical Specification, 3GPP, 1999.

〔5〕 인선준, "SIM, UIM과 USIM", TTA 저널, 제 83호.

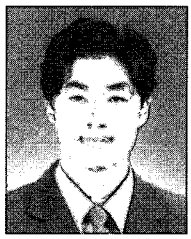
〔6〕 "ETSI EN 300 392-7, Terrestrial Trunked Radio(TETRA): Voice plus Data(V+D): Part 7: Security", European Standard, ETSI, 2004.

[7] "ETSI EN 300 812-3, Terrestrial Trunked Radio(TETRA); Subscriber Identity Module to Mobile Equipment(SIM-ME) interface; Part 3; Integrated Circuit (IC); Physical, logical and TSIM application characteristics." European Standard, ETSI, December, 2001
[8] "ETSI TS 121 111 Universal Mobile Telecommunications System(UMTS); USIM and IC card requirements(3GPP TS 21.111 version 5.0.0 Release 5", Technical Specification, ETSI, 2002
[9] "TESI TR 101 494 Terrestrial Trunked Radio(TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment(SIM-ME) interface", European Standard, ETSI, December, 2001
[10] "SIM - The basic for Mobile value Added Services", White Paper, SmartTrust
[11] "USIM-the smart card for UMTS", Ulrich Heckmanns, ACTS Mobile summit 1999, Sorento, Italy, June 1999.
[12] Günther Horn, Bart Vinck, Klaus Müller, "A vialble security architecture for UMTS", ACTS Mobile Summit 1999, Sorento, Italy, June 1999.
[13] Peter Howard, "3G Security Overview", IIR Fraud and Security Conference, March 2000.
[14] FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", NIST, May 25, 2001

## 〈著 者 紹 介〉

**원 동 규 (Dongkyu Won)**
**학생회원**

2003년 2월 : 인천시립대학교 전자공학과(공학사)
2005년 2월 : 성균관대학교 정보통신공학부 석사
2005년 4월~현재 : 한국전산원 전임 연구원



**조 은 성 (Eunsung Cho)**
**학생회원**

2000년 8월 : 성균관대학교 산업공학과(공학사)
2002년 8월 : 성균관대학교 산업공학과 석사
2003년 3월~현재 : 성균관대학교 정보통신공학부 컴퓨터공학과 박사과정
2005년 6월~현재 : 삼성전자 선임 연구원

**양 형 규 (Hyungkyu Yang)**
**정회원**

1983년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1985년 2월 : 성균관대학교 대학원 전자공학과(공학석사)
1984년 12월~1991년 2월 : 삼성전자 선임 연구원
1995년 2월 : 성균관대학교 대학원 정보공학과(공학박사)
1995년 3월~현재 : 강남대학교 컴퓨터미디어공학부 부교수

**김 승 주 (Seungjoo Kim)**
**종신회원**

1994년 2월 : 성균관대학교 정보공학과(공학사)
1996년 2월 : 성균관대학교 대학원 정보공학과 (공학석사)
1999년 2월 : 성균관대학교 대학원 정보공학과(공학박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2001년 1월~현재 : 한국정보보호학회 논문지편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년 3월~현재 : 성균관대학교 정보통신공학부 조교수

**원 동 호 (Dongho Won)**
**종신회원**

1976년~1988년 : 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1988년~1999년 : 성균관대학교 교학처장, 전기·전자 및 컴퓨터공학부장, 정보통신대학원장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
2002년~2004년 : 성균관대학교 연구지원처장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정통부지정 정보보호인증기술연구센터 센터장