스마트카드상에서의 ID 기반 인증서비스 구현

○이윤호, 장청룡
한국통신 연구개발원

An Implementation of ID-based Authentication Service on Smart Card

○Yun-Ho Lee, Chung-Ryong Jang
Korea Telecom Research Laboratories

Abstracts

기존의 인증과정에서 이용되는 토큰으로는 자기카드가 많이 쓰이고 있으나 앞으로는 스마트카드가 이를 대체할 전망이다. 그러나 우리나라의 실정은 차세대카드로 불리는 스마트카드의 활용이 극히 부진한 실정이다. 스마트카드는 초기의 단순 메모리형 카드에서 점차 복잡한 형태의 카드로 발전하고 있으며 DES나 RSA 암호계를 내장하였을 뿐만 아니라 근래에는 현대암호학의 고속계산 모듈을 담고 있는 카드까지 등장하고 있다. DES를 이용한 인증은 빠른 속도와 구현의 용이성으로 인한 장점이 있는 반면, 카드 인증에 필요한 키를 단말기가 모두 관리해야 하는 문제가 있었다. 본 논문에서는 DES 내장형 스마트카드에 ID 개념을 적용하여 키관리가 필요없는 사용자인증 및 카드와 단말기간의 양방향 인증을 구현하였다. 사용된 스마트카드는 8-bit CPU를 내장하고 2kbytes의 EEPROM을 이용하며 프로그램의 다운로드수행은 고려하지 않았다.

1. 서 론

현대사회가 정보화사회에서 '정보고속도로'로 대변되는 고도 통신사회로 진입함에 따라 이를 '암호화사회'라고 부를 만큼 개인정보나 국가기밀, 기업비밀 등의 누출로 인한 역기능이 심각하게 드러나고 있다. 과거 암호라고 하면 국가간의 스파이전이나 일반인과는 전혀 거리가 먼 이야기처럼 생각된 때가 있었으나 근래에는 매스컴을 통해 정보의 불법 누출이 얼마나 심각한 피해를 가져올 수 있는가를 자주 접하면서 이러한 피해를 예방할 수 있는 정보보호기술에 대한 관심이 높아지고 있다.

중요한 정보자원으로의 접근을 막는 보편적인 방법은 접근이 허용된 사람만을 선별하여 허가하는 인증(또는 개인 식별)을 주로 이용하는데 개인을 인증하기 위해 사용되는 방법은 주로 다음의 방법을 이용하고 있다.[1][2]

1. 알고있는 것(패스워드, ...)
2. 소유하고 있는 것(신용카드, 신분증, ...)
3. 신체적인 특징(지문, 안구, ...)

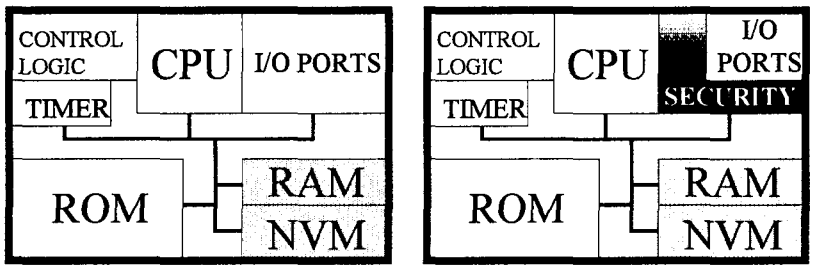
이 가운데 널리 사용되는 방법은 '알고있는 것'에 의한 방법과 '소유하고 있는 것'에 의한 방법이다. 자기카드의 일종인 신용카드는 이 둘을 모두 이용하는 예로 어느 한 방법만을 사용하는 경우보다 비교적 높은 안전성을 보이지만 자기카드의 특성상 위조나 변조에 약하다는 단점으로 인해 다른 대체 수단을 강구하기에 이르렀다. 그 결과 카드내에 프로세서를 내장하여 단일칩 컴퓨터를 구현한 IC 카드 또는 스마트카드가 유력한 대체 수단으로 각광받고 있다. 본 논문에서는 스마트카드의 개요와 이를 이용하여 ID 기반 양방향 인증 시스

팀의 구현결과를 소개하고자 한다.

2. 스마트카드

2.1. 스마트카드의 H/W 구조

스마트카드에 내장된 chip은 single-chip 마이크로컴퓨터이다. 그림 2.1은 범용 마이크로컴퓨터와 secure single-chip 마이크로컴퓨터를 비교한 것이다. 가장 큰 차이점은 secure single-chip 마이크로컴퓨터의 경우 접근제어 기능이 추가되어 chip 내의 CPU, RAM, ROM 등으로의 임의접근이 어렵다는 점이다.



A. 범용 마이크로컴퓨터 B. Secure single-chip 마이크로컴퓨터

그림 2.1 범용 마이크로컴퓨터와 secure single-chip 마이크로컴퓨터의 비교

□ CPU

대부분의 스마트카드는 8-bit CPU를 이용한다. CPU의 기능은 OS 및 사용자 프로그램의 실행, R/W 제어, 외부와의 I/O 처리 등 일반적인 CPU와 동일하다.

□ RAM, ROM, NVM

기억장치를 이용함에 있어 범용 컴퓨터와 다른 점은 프로그램이나 화일 혹은 키의 기억장소로 RAM을 이용하지 않고 NVM(non volatile memory)을 이용한다는 것이다. 이는 스마트카드가 갖는 면적과 관련된다. 즉, ROM의 경우 가장 작은 면적을 차지하며 RAM은 상대적으로 가장 큰 면적을 차지한다. 이러한 이유로 RAM은 계산의 중간결과 등을 저장하는데 이용되며 ROM은 OS 등을 저장하고 NVM은 사용자의 프로그램이나 중요한 데이터 등을 저장하는데 이용하며 NVM으로는 보통 EPROM이나 EEPROM이 사용된다.

이들 기억장치의 용량을 보면, RAM은 대개 수십 ~ 수백 바이트 정도이며 ROM은 6 ~ 16KB, NVM은 64 바이트에서 64KB까지 다양하다.

□ I/O 포트

스마트카드와 외부장치(보통 카드리더기)가 데이터를 교환하는 경로를 제공하며 대부분의 스마트카드는 6~8개의 접점(contact point)을 갖고 있다. 이들 접점의 위치, 전기적인 특성 및 인터페이스 프로토콜은 모두 ISO/IEC 7816으로 표준화되어 있는 상태이다.

2.2. 암호학적 알고리즘의 적용

스마트카드의 작동과정을 보면 크게 3 단계로 구분할 수 있다. 1 단계는 카드의 소유자가 정당한 소유자인지를 검사하는 사용자 인증과정이며 2 단계는 카드와 단말기간의 상호인증 과정이고 3 단계는 인증을 마친 사용자가 원하는 응용(application)을 수행하는 과정이다. 보통 1 단계에서는 사용자를 확인할 때는 패스워드 방식의 일종인 PIN(personal identification number) 확인과정을 거치는데 이 때 자신만 알고 있는 패스워드를 입력하여 확인한다. 2 단계로는 카드와 단말기가 서로를 확인하는 과정, 즉 상호인증(mutual authentication)이 수행되는데, 카드만을 확인하지 않고 상호인증을 하는 이유는 단말기 자체도 신뢰할 수 없다는 것을 가정하기 때문이다. 실제로 자기카드의 경우이기는 하지만 정당하지 못한 단말기를 이용하여 카드내의 정보를 빼낸 사례도 있다.[3] 3 단계는 인증 이후의 과정이 필요할 경우 수행된다. 예로서 전자결재를 위한 전자서명(digital signature)의 생성 등을 들 수 있다. 그림 2.2는 이러한 과정을 나타낸다.

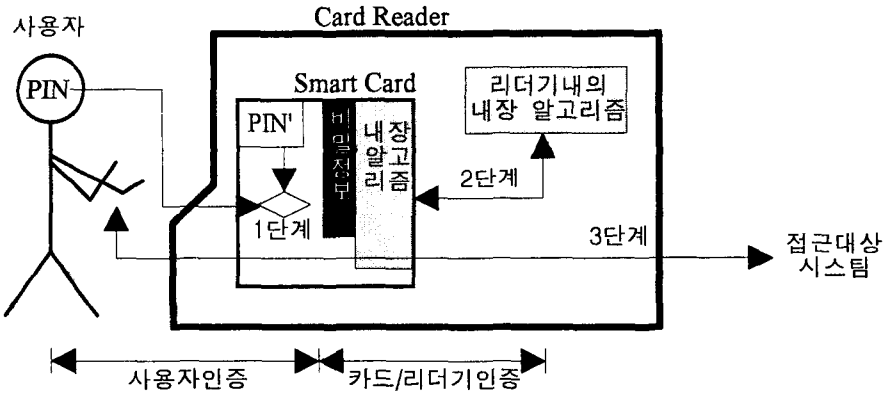


그림 2.2 알고리즘의 수행단계

암호학적인 안전도 관점에서 생각해볼 때 1 단계만 수행하는 경우는 가장 안전성이 결여된 방법으로 주로 단순한 메모리카드에 적용되는 방법이다. 자기카드의 경우와 방법은 같지만 자기카드보다 변조나 위조의 가능성은 적다. 위의 세 단계중 가장 중요한 것은 2 단계로 스마트카드를 이용한 응용의 핵심을 이루게 된다. 스마트카드를 이용한 인증 알고리즘의 대부분은 바로 2 단계에 적용하기 위해 연구되고 있으며 현재 상당히 많은 알고리즘이 개발되었다.

□ 인증 알고리즘의 적용

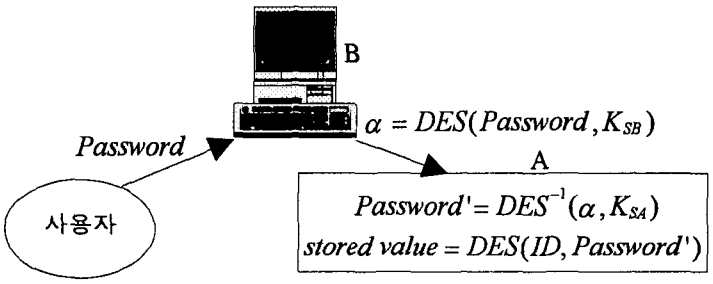
인증 알고리즘은 크게 다음과 같은 3 종류가 있다.

- 관용암호계를 이용한 알고리즘
- 공개키암호계를 이용한 알고리즘
- 영지식상호증명(*zero-knowledge interactive proof*)을 이용한 알고리즘

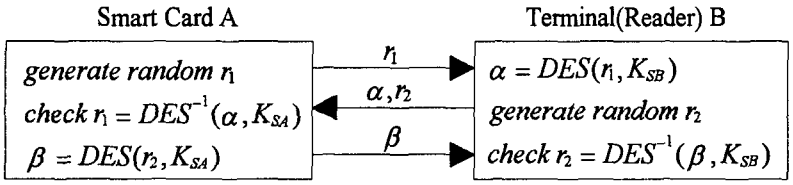
이중 가장 안전하다고 알려진 방법은 영지식증명을 이용한 것이다. 영지식은 1985년 Goldwasser, Micali, Rackoff가 제안한 개념으로 인증과정으로부터 제 3 자는 물론이고 검증자조차 증명자의 비밀정보를 알 수 없도록 한 가히 획기적인 방법이다.[4] 보통 1984년 Shamir가 제안한 ID 개념과 결합하여 사용되는데, 대표적인 방법으로는 Fiat-Shamir 방식[5], Micali-Shamir 방식, Guillou-Quisquater 방식 및 Schnorr 방식 등이 있다. 대

부분 대화적인 방법을 사용하기 때문에 ZKIP(zero-knowledge interactive proof)이라고도 한다. 현재는 관용암호계의 일종인 DES(data encryption standard) 알고리즘을 내장한 카드가 많이 나와 있으며, 공개키암호계의 대표적인 방식으로 RSA(Rivest-Shamir-Adlman) 알고리즘을 내장한 카드도 있다.

DES를 이용한 스마트카드 인증 시스템의 예로는 미국 NIST의 ASACS(The NIST Advanced Smartcard Access Control System) 프로젝트를 들 수 있다. 이 프로젝트는 사용자의 프로그램을 수행할 수 있는 스마트카드를 이용하여 사용자인증 및 카드와 단말기간의 양방향인증을 구현하였다.[6](그림 2.3 참조)



가) 사용자인증 절차



나) 카드/리더기간의 인증 절차

그림 2.3 NIST의 ASACS 인증 시스템

그러나 이 인증시스템은 사용자의 접근제어기능에만 중점을 두었기 때문에 인증 이후의 통신을 위한 세션키생성 등은 고려하지 않았다. 또한, 카드와 단말기간의 인증시 카드에 담겨있는 각 사용자의 비밀키를 단말기가 모두 가지고 관리해야하는 문제가 있다.

본 논문에서는 프로그램의 수행능력이 없는 DES 내장형 스마트카드를 이용하여 NIST의 인증시스템과 마찬가지로 사용자인증 및 카드와 단말기간의 인증을 수행하면서 ID 개념을 도입하여 각 단말기가 관리해야하는 키의 수를 1개로 줄였고, 인증 이후의 응용을 위한 키전달까지를 고려하여 스마트카드 인증 시스템을 구현하였다.

3. ID를 이용한 양방향 인증

스마트카드를 이용하는 가장 큰 이유는 안전한 사용자인증이 가능하다는 점이다. 즉, 인증의 기본 방법중 알고 있는 것(패스워드)과 소유하고 있는 것(스마트카드)을 통하여 인증하는 것 이외에 소유하고 있는 것의 위조나 변조가 현실적으로 불가능하다는 장점으로 인해 앞으로 그 사용이 크게 확대될 전망이다. 본 절에서는 스마트카드만을 인증하는 단방향 인증보다 발전된 형태인 양방향 인증의 구현에 대해 살펴보기로 한다.

3.1. 구현환경

양방향 인증의 구현에 사용된 환경은 표 3.1과 같다. 스마트카드 및 카드리더는 프랑스 GemPlus 사의 제품이며 프로그램의 라이브러리 역시 GemPlus 에서 제공한 것을 이용하여 MS-C 8.0으로 컴파일 및 링크하였다. 제공되는 라이브러리는 스마트카드로의 Power ON, ISO 명령전달 등 기본적인 루틴만을 포함한 형태이며 Large model과 Small model의 두가지만 제공되었고 본 구현에서는 Large model을 이용하였다.[7]

표 3.1 양방향 인증 구현 환경

구 분	항 목		내 용	비 고
S/W	구 현 언 어		MS-C 8.0	Large Model
H/W	호 스 트	프로세서	80386-DX 33MHz	
	R/W	인터페이스	RS-232C	
	CARD	프로세서	8-bit	프로그램 수행 능력 없음
		EEPROM	2 kbytes	DES 암호화 알고리즘 내장
		RAM	160 bytes	난수발생 알고리즘 내장

본 구현에 사용한 GemPlus 스마트카드는 I/O 형식을 ISO 7816-3[8]의 권고에 맞추고 있다. ISO 7816-3에서 권고한 명령의 형식은 아래와 같다.

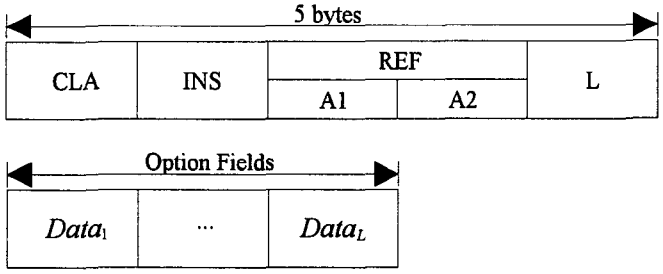


그림 3.1 ISO 7816-3의 스마트카드 명령 형식

CLA는 명령의 class로 실험에 사용한 GemPlus 카드의 명령은 모두 class 0이다. INS는 명령 code로서 이는 각 카드 제조회사에서 결정하며, A1, A2는 INS에 대한 reference이고 L은 선택적으로 필요한 데이터 필드의 길이를 나타낸다. 만약 $L \neq 0$이면 추가적인 L 바이트의 데이터 필드가 필요하게 된다. 이러한 명령의 결과로 스마트카드는 2바이트의 결과값 SW1, SW2를 돌려보내게 되는데 2바이트의 값중 일부는 ISO 7816-3에서 미리 정의하였으며 그 값은 표 3.2와 같다.

표 3.2 미리 정의된 결과값

CODE			명령의 의미
SW1		SW2	
6X	6E	Don't Care	카드가 해당 명령 class를 지원하지 않음
	6D		해당 명령 코드의 오류
	6B		refrence(A1, A2) 오류
	67		길이(L) 오류
	6F		원인을 알 수 없는 오류
90		00	해당 명령의 정상 종료

3.2. ID를 이용한 양방향 인증

스마트카드를 이용한 사용자 인증에서 구현해야 할 사항은 크게 사용자 인증, 카드 인증 및 단말기 인증이 있다. 먼저 사용자 A에게 스마트카드를 발급하는 과정은 다음과 같다. 모든 가입자를 관리하는 센터는 가입자 A가 가입을 요청하였을 때 가입자 A의 패스워드, 실제 응용에 사용될 비밀키 KK와 함께 ID_A(이름, 주민등록번호 등의 고유한 정보)를 결정하고 ID_A로부터 가입자 A의 비밀인증키 S_{KA}를 계산하여 스마트카드에 ID_A, $Password$, KK와 함께 저장하여 발급한다. 이상의 과정을 그림으로 표현하면 그림 3.2와 같다.

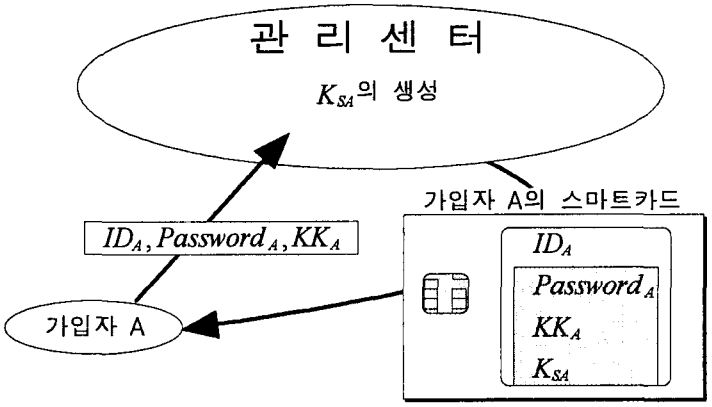


그림 3.2 카드 발급과정

주의할 것은 각 가입자는 임의의 ID_i로부터 해당 비밀인증키 K_{Si}를 구하지 못한다는 것이다. 정당한 카드를 발급받은 가입자 A는 발급받은 카드를 이용하여 자신의 신분을 인증하고 원하는 응용을 수행할 수 있게 된다. 가입자 인증과정을 보면 그림 3.3과 같다.

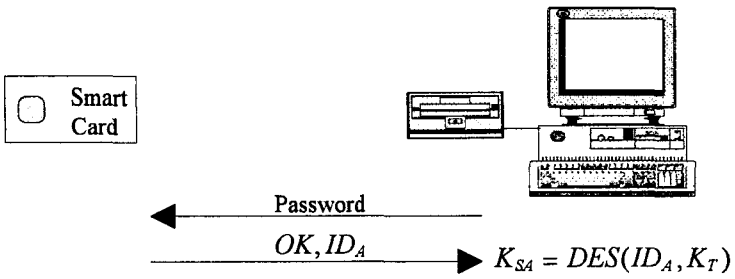


그림 3.3 사용자 인증 과정

먼저 카드를 리더기에 삽입하면 단말기는 카드로부터 소유자의 ID인 ID_A를 읽어 화면에 표시한다. 이때 가입자 A는 단말기의 키보드를 이용하여 자신의 패스워드를 입력한다. 단말기는 이를 카드에 전달하고 카드는 이를 확인하여 맞을 경우 소유자 A의 비밀인증키 K_{SA} 이용하여 카드인증과 단말기인증 과정의 수행을 준비한다. 단말기는 카드로부터 읽은 ID_A로부터 사용자 A의 비밀인증키인 K_{SA}를 생성하여 카드와 단

말기간의 상호인증을 시작한다.

카드와 단말기간의 인증은 양자가 동일한 비밀인증키를 갖고 있는가를 확인하는 것이다. 따라서 이를 확인하는 방법으로는 임의의 난수 R을 선택하여 전달했을 때 상대방이 R을 비밀인증키로 암호화시킬 수 있는가 하는 것이다. 단말기는 R_1을 생성하고 카드는 R_2를 생성한 후 위의 방법을 이용하여 단말기는 카드를 인증한다. 인증이 성공되면 양자는 $R_1 \oplus R_2$를 이용하여 동일한 세션키를 만들 수 있게 되고 카드는 이 세션키를 이용하여 단말기가 생성한 A의 비밀인증키 K_{SA}를 확인한다. 여기서 생성된 세션키는 양자만 공유할 수 있는 키로서 키분배의 효과도 얻을 수 있다.

3.3. 각 인증시스템 비교

Fiat-Shamir 인증시스템, NIST의 ASACS 시스템과 제안한 인증시스템을 관리 키의 수와 수행시간 측면에서 비교한 결과는 표 3.3과 같다. 표에서 알 수 있듯이 ASACS 시스템과 제안 시스템 모두 관용암호계인 DES를 이용하지만 ASACS 시스템은 각 사용자의 카드에 내장된 키를 모두 소유하고 있어야 한다는 문제가 있지만 제안한 시스템은 사용자의 ID로부터 키를 구하기 위한 센터의 비밀키 하나만 알고 있으면 된다. Fiat-Shamir 시스템인 경우 ID 기반의 영지식 증명방식으로 관리해야 할 키는 없지만 스마트카드에서 구현하기에는 속도가 느리다는 단점이 있다. 제안한 시스템에서 관리해야 할 키의 수가 1개인 이유는 관용암호계인 DES를 이용하기 때문이다.

표 3.3 세가지 인증시스템의 비교

항 목	제안 시스템	ASACS 시스템	Fiat-Shamir 시스템
터미널의 관리 키 수	1개(터미널키)*	사용자수	없음
상대적인 인증 수행시간	고속	고속	저속

* 1 개의 키관리가 필요한 이유는 관용암호계인 DES를 이용하기 때문이다.

4. 결 론

본 논문에서는 실제로 스마트카드를 이용하여 프로그램의 수행능력을 고려하지 않고 카드내에 내장된 명령만을 이용하여 카드와 단말기간의 양방향 인증 시스템을 구현하였다. 실제로 DES 내장형 스마트카드를 이용하여 인증을 구현한 예는 미국 NIST의 ASACS 프로젝트 등이 있으나 이는 키관리에 문제가 있고 인증 이후를 위한 세션키생성 등을 고려하지 않았다. 그러나 본 구현에서는 카드에 내장된 DES와 기본 명령만을 이용하여 양방향 인증을 구현하였고 Shamir의 ID 개념을 도입하여 단말기가 각 가입자의 비밀인증키를 모두 갖고 있어야 하는 단점을 해결하였다.

정보보호기술은 다른 기술과는 달리 어떠한 원천기술도 타국으로의 유출을 방지하는 외국의 선례에 비추어 볼 때 하루빨리 기술개발과 함께 육성이 필요한 분야이다. 정보보호기술이 외국에 종속된다면 우리나라의 안방을 훤하게 내어주는 격이 될 것이기 때문이다. 향후의 연구는 스마트카드의 고성능화 및 저가격화에 맞춰 보다 개선된 알고리즘을 개발해야 할 것이고 이와 함께 카드자체의 개발능력도 갖추어야 한다. 유럽의 경우 이미 공중전화는 물론이고 이동전화에 IC 카드를 활용하는 단계이긴 하지만 스마트카드의 활용이 신기술에

속하기 때문에 지금이라도 기술개발은 늦지 않은 상태이다. 또한 고도의 보안능력을 갖는 스마트카드 이외에 광카드나 스마트카드에서 입출력장치의 불편함을 없앤 RF 카드(무선카드) 등에 대한 연구도 진행중이다. 따라서 스마트카드에 대한 연구도 진행하면서 스마트카드의 응용분야를 매워줄 다른 카드의 개발도 함께 진행되어야 할 것이다.

참 고 문 헌

1. Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Authentication Framework, Draft Recommendation X.811, International Telecommunication Union.
2. Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 2: Authentication Framework, DIS 10181-2, International Organization for Standadization.
3. Stephan Seidman, Editorial, Smart Card Monthly, pp. 3, July 1993.
4. S.Goldwasser, S.Micali, and C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems," The 17th ACM STOC, pp. 291~304, 1985.
5. A.Shamir, "Identity-Based Cryptosystems and Signature Schemes," Crypto'84, pp.47~53, 1985.
6. James F. Dray, "The NIST Advanced Secure Access Control System", NIST.
7. MCOS 16K EEPROM DES Reference Manual Version 2.2 - Reference CCH01U22, GemPlus Card International, 1990.
8. Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocol, IS 7816-3, International Organization for Standadization.