정보보호를 위한 스마트 카드의 성능 분석

백창현°, 이대기
한국전자통신연구소

On the Performance of Smart Card For Security

Chang-Hyun Paek, Dae-Ki Lee
Electronics and Telecommunications Research Institute

요 약

통신기술과 정보 통신 서비스의 발달로 인하여 여러 가지 목적에 활용될 수 있는 카드가 요구되고 있다. 이러한 요구에 맞추어 발달된 반도체 기술에 의해 스마트 카드가 출현 하였고, 대용량의 기억장치와 연산장치를 갖춘 스마트 카드는 그 응용 분야가 날로 확대되어 가고 있다. 여기서는 보안 기능을 위한 스마트 카드의 암호 알고리즘을 실현하기 위한 성능을 살펴 본다.

I. 서 론

현대 사회에서는 정보와 통신 서비스의 발달로 분야별 개인에 대한 각종 정보와 신용을 중요시 하고 이에 근거하는 다양한 서비스를 제공하게 되는데, 이 모든 것들에 대한 관리가 개별적으로 이루어지고 있다. 기존의 마그네틱 카드는 사용상의 한계를 갖기 때문에 정보를 저장하거나, 거래 내역의 계산, 보안성 유지가 어렵다. 이러한 문제를 해결하기 위한 방안으로서 스마트 카드의 이용이 증가하고 있는 추세이다. 특히 암호 시스템에서 키의 중요성을 감안할 때, 키가 카드 외부로 유출 되지 않아야 하고, 고도의 안전성 확보가 필요하다. 또한 마이크로 프로세서와 메모리를 보유함으로써 개인의 정보 기록은 물론 연산 기능을 이용하여 복잡한 암호 알고리즘을 계산할 수 있으며, 복제가 어렵고, 이동성이 뛰어 나다. 뿐만 아니라 기존의 카드가 할 수 없는 양방향 통신, 분산처리, 개인에 대한 과금 서비스 등의 기능을 제공한다. 앞으로도 스마트 카드의 발전은 반도체 및 관련 기술의 빠른 발달로 인해 더욱 성능이 강력한 스마트 카드가 출현할 것으로 기대되며, 이에 따라 더 복잡하고, 많은 정보의 저장, 서비스의 양적 질적 증가가 있을 것이다. 특히 정보보호 기술에의 응용이 증가할 것으로 본다.

또한 스마트 카드는 보안성을 제공하는 데 있어서 필수적인 도구가 되어가고 있으며, 액세스 제어 시스템과 같은 물리적인 보안 분야 뿐만 아니라, 암호 알고리즘을 이용한 안전한 데이터 전송에 대해서도 활용이 증가될 것이다.

이러한 보안성 있는 스마트 카드의 필요성은 최신 스마트 카드 IC 의 암호화 기능들로 인하여 전자 해방꾼들이 거의 위조할 수 없는 온라인 거래를 가능하게 한다. 위조나 부정한 사용을 방지하고, 통신을 해야 하는 응용에서 필요한 보안 레벨을 달성하기 위해서는 암호 알고리즘을 사용하여 메세지를 암호화하여야 한다. 따라서 안전한 스마트 카드의 응용을 위해서 그 문제점이 무엇이고, 어떠한 보안 조치들이 있는 지 살펴보고, 기 생산된 카드의 암호화 성능 등에 대해서 비교 분석하고자 한다.

II. 스마트 카드의 취약성

스마트 카드의 기술은 공공과 개인 분야의 정보 보호를 위한 다양한 정보보호 시스템 구현에 적용되고 있다. 그러나 이 기술은 우리의 데이터와 시스템의 안전을 위해 어떠한 취약성을 갖고 있는 지, 카드에 주어진 보호기능이 사용자의 환경과 잘 어울려 질 것인지를 판단하기 위해 먼저 스마트 카드의

여기서 말하는 취약성이란 스마트 카드가 하나 또는 그 이상의 응용을 목적으로 사용되면서 나타날 수 있는 문제점 및 위험성을 의미하며, <표 1>과 같다.

<표 1> 스마트 카드의 나타날 수 있는 취약성들.

발생 요인	발생 원인	발생 결과
카드의 손실	-카드 홀더의 PIN(personal Identification Number)의 취약.	-비합법적인 사람이 카드에 접근하여 카드에 기록된 자산, 개인 정보, 서비스등이 손실된다.
여러 응용 서비스간의 방해	- 각 응용 서비스가 공통으로 사용하는 고유 메모리 영역을 access 한다.	-응용 서비스간 정보의 양보 -여러 서비스중의 일부 양보
카드를 직접 접근할 수 있는 제조자, 사용자, 카드 홀더등의 문제	-제조자의 PIN 이 노출된다면, 복제 또는 재 제작이 가능. -깨지기 쉬운, 약한 PIN 사용시.	-카드가 제공하는 보호기능 상실 -카드에 의해 접근될 수 있는 것들에 대한 노출 및 불법적 접근 가능.
모방의 문제	-스마트 카드와 그 정합장치간의 통신을 가로채기 또는 모니터.	-카드가 제공하는 보호기능 상실 -개인정보, 서비스등의 손실 및 카드와 그 응용 서비스에 대한 신뢰성 상실.
복제 및 재 생산	- 기술상의 난이도와 고가의 금액에 의존. - 카드와 주문제작 처리과정에 개입하여 카드 복제를 가능하게 함.	- 카드가 제공하는 보호기능 상실 - 개인정보, 서비스등의 손실 및 카드와 그 응용 서비스에 대한 신뢰성 상실
수정	- 카드 Operating System 과 응용 서비스를 위한 설계, 제조, 주문 제작 처리가 약함.	- Operating System, Application : 카드에 비 합법적인 은밀한 접근 가능 - Information : 카드의 주문제작 및 카드홀더에 연결시 응용 서비스를 속이기 위해 카드의 데이터를 삭제, 수정이 가능케 함.

이와 같은 문제는 더 추정하여 많은 취약성들을 찾아 냄으로써 정확하고, 안전성이 뛰어난 스마트 카드 제작 및 운용이 될 수 있어야 할 것이다.

III. 물리적 보호

스마트 카드와 카드 인식 장치의 하드웨어를 포함한 암호 칩의 보호는 엑스포 수지로 처리되어 있으므로 엑스포 수지를 벗겨 낼 때 칩이 손상 될 수 있다. 그리고 ROM 에는 카드 운영 프로그램 및 암호 알고리즘이 저장되어 있고, EEPROM 에는 암호 알고리즘, 가입자 고유 번호, 키 등이 저장되어 있다. 일반적으로 칩의 설계 시에는 VHDL(VHSIC Hardware Description Language) Core Library 를 이용하여 이들 메모리와 마이크로 프로세서가 단일 칩상에 설계되므로, 내부 기억 내용을 알기 위하여는 칩 분석을 해야 하며, 물리적인 개봉 및 전기적으로 카드의 내용을 읽으려는 시도가 있으면 EEPROM 의 내용이 빛 또는 특수한 논리회로에 의하여 자동 삭제되는 자폭 기능(kill bit logic)이 있다. 그러므로, 스마트

카드에 대한 역 엔지니어링(reverse engineering)은 매우 어렵다 할 수 있다. 이러한 물법적인 액세스를 방지하기 위한 방법으로서 아래와 같은 기술을 사용하고 있다.

- Power Down Reset 기능 : 전압이 일정 수준 이하나 이상으로 변화할 때마다 전압 센서가 동작 전압을 자동적으로 끊어준다. 이것은 먼저 리셋해 주어야만 다시 켤 수 있다.

- Bus Scrambling : 주소 및 데이터 채널을 손쉽게 찾아내지 못하도록 막아 준다.

- 주파수 센서 기능 : 동작이 특정 범위 내로 국한되도록 보장해 준다. 클럭 주파수가 특정 범위 내에 있지 않으면 파워 다운 모드로 들어가게 되므로 제어기의 단계적 테스팅 및 분석을 막아 준다.

- 감시 장치 타이머 : 프로그램 runaway를 감시하고 정확한 프로그램 플로우가 재개되도록 한다.

- 코드에 의한 통제 : PIN이나 개인 신상의 특정한 정보를 기록하여 둔다.

- 테스트 패드의 물리적 제거 : 칩 다이스가 웨이퍼로부터 나오는 scribing 단계에서, 물리적으로 패드를 지워버린다.

이러한 기능을 수용하면서 다음과 같은 메커니즘을 이용하여 보다 개선된 방법으로 발전될 것이다.

- 바이오메트릭 데이터기록 : 바이오메트릭 데이터는 스마트 카드 소지자의 특징들로서 지문, 서명의 역학, 음성 패턴, 또는 안면 패턴등이다.

- 광학적 판독 방지 : 메모리에 대한 외부로부터의 액세스와 ROM을 광학적으로 판독하는 것도 방지된다.

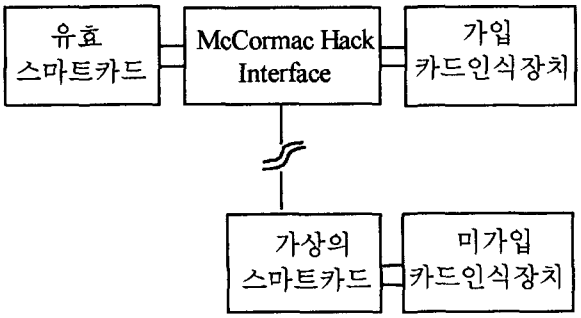
이와 같이 일단의 물리적 보안을 갖추고 있는 스마트 카드는 보안과 관련된 서비스에 만족한 조건을 갖는다고 본다. 스마트 카드의 칩 집적도가 커지고, 메모리의 용량이 증가하게 되면, 더욱더 강력한 보안기능이 수용될 수 있다.

IV. 인증 및 암호 알고리즘의 적용

인증은 사용자 인증, 카드 인증과 카드인식장치 인증으로 분류한다. 불법 사용자가 스마트 카드의 EEPROM의 내용을 읽어 다른 스마트 카드에 복사하는 시도가 발생 할지라도, ROM과 EEPROM 내의 데이터의 관계 및 패스워드와 생물학적 특징을 이용한 사용자 인증 방법을 이용하여 불법 복제한 카드 및 사용자를 무효화 할 수 있다. 카드 인증은 카드와 카드 인식 장치간의 인증이다. 대표적인 해킹 방법으로 유료 TV에서 McCormac Hack으로 알려진 이 가상적인 해킹은 (그림 1)과 같이 스마트 카드와 카드인식장치 사이의 데이터를 모뎀이나 무선 전송에 의하여 한 개 이상의 미 가입 카드인식장치와 가상의 스마트 카드에 전달하여 미 가입자도 정상적인 신호를 수신하도록 한다.

McCormac Hack이 실현되려면 스마트 카드와 카드 인식 장치 사이의 인증 작업이 가상의 스마트 카드와 카드인식장치 사이에서도 정상적으로 이루어져야 한다. 그러나, RSA 공개키 알고리즘 및 영지식

알고리즘을 이용한 Fiat-Shamir 인증 방법 등 대부분의 인증 방법들이 난수를 발생하여 인증을 하므로 가상의 스마트 카드와 연결된 가입 카드인식장치와 미가입 카드인식장치가 동기화 되어야 한다.



(그림 1) McCormac Hack

이 McCormac Hack의 방지를 위하여는 스마트 카드와 카드인식장치 사이의 중요 데이터를 암호화 해야 한다. 카드 인식 장치 인증은 암호 프로토콜을 이용한 카드 인식 장치와 호스트 컴퓨터 사이의 인증이다.

또한 설계에 고려할 수 있는 암호화 방식에는 기본적으로 대칭 및 비대칭 방식의 두 가지 형태가 있다. 대칭형 암호화 방식에서는 가장 잘 알려진 알고리즘으로 DES가 있으며, 암호화와 복호화에 동일한 키를 사용한다. 그러나, 이 암호화 처리 방식의 최대 약점은 키를 비밀로 유지하기 위하여 키를 별도의 안전한 채널을 통해 송신자로부터 수신자에게 보내야 하는 것이다. 현재로서는 키의 관리 문제가 발생할 수 있으므로 심각하게 받아들여 진다. 또 하나의 문제는 디지털 서명에 적용하기 어렵다는 점이다.

비대칭 암호화 방식에는 이러한 문제점들이 존재하지 않는다. 이 방법을 사용하면 모든 사용자들이 두 개의 키, 즉 공개 키와 비밀 키의 조합을 갖게 된다. 이러한 시스템을 사용하면 전송용 데이터를 암부호화하기 위해서는 원하는 수신측의 공개 키만 알고 있으면 된다. 전송되는 데이터가 특정인이나 특정 근원으로부터 오는 증거가 필요하다면, 송신자는 자신의 비밀 키로 암호화하여 전송하고, 수신자는 송신측의 공개 키를 사용하여 그 메시지가 실제로 본인에게로 전달되는 것인지를 점검할 수 있다. 이러한 절차를 디지털 서명이라 한다.

이러한 암호화 방식에 따른 암호의 선정은 스마트 카드의 서비스 목적에 따라 결정 될 수 있다. 일반적인 상용 서비스, 또는 특정한 목적을 위한 서비스인가에 따라 그 방식은 결정될 수 있다.

V. 성능 비교

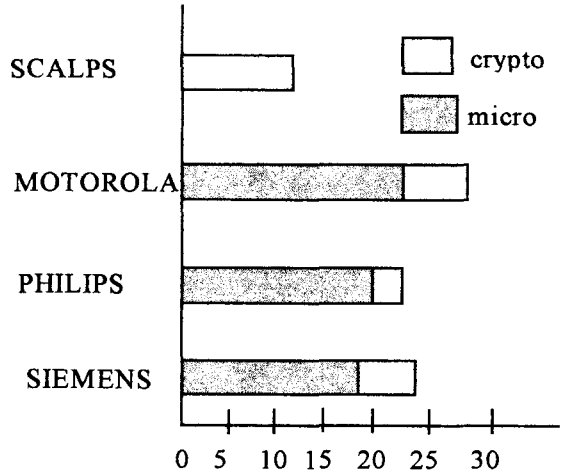
스마트 카드 칩을 제조하고 있는 회사들을 보면 SGS-Thomson, Texas Instruments, Motorola, Philips, Catalyst, Hitachi, NEC, Oki, Siemens, Toshiba 등이 있다. 또한 정보보호 분야에 적용하기 위한 목적으로 복잡한 연산이 요구되는 암호 알고리즘을 카드 내에 내장한 형태의 스마트 카드가 개발되고 있는데, DES, RSA, FEAL 등을 내장하나 주종은 RSA를 적용한다.

일반적으로 스마트 카드용 Arithmetic Co-processor는 모듈러 연산을 위한 연산 모듈을 내장하고 있다. 이 모듈러 연산을 기반으로 한 상용 Co-processor의 성능 및 응용 분야는 <표 2>와 같다.

<표 2> 상용 Co-processor의 특성 비교

칩명	제조회사	core uP	제조기술	연산알고리즘	주파수 (MHz)	최대 N (비트)	응용분야
ST16CF54	SGS	68HC05	1.2uCMOS	Montgomery	5	768	비공개
ST16KL74	SGS	68HC05	1.2uCMOS	Montgomery	5	1024	not communicated
SLE44C200	Simens	80C51	1uCMOS	Sedlak	5	540	CAFE, DSM-fax, CP8
P83C852	Philips	80C51	1.2uCMOS	Quisquater	10	648	DX, Mimosa, Starcos
P83C855	Philips	80C51	1.2uCMOS	Quisquater	10	1328	not communicated
MC68C05S29	Motorola	68HC05	1.2uHCMOS	Montgomery	5	1024	French health card
RSA512	AMTEC	co-uP	0.5uCMOS	Bucci/Barrett	100	513	banking, X.25 security
SCALPS	UCL	custom	1.5uCMOS2ML	Montgomery	6	512	university prototype
CY512i	Cylink	80C31	1.5uCMOS	Massey-Omura	15	512	not communicated
CRIPT	CNET	custom	1.2uCMOS	bit-by-bit	25	1024	PCMCIA cards
PCC200	Pijnenb.	co-uP	1uCMOS2ML	비공개	20	1023	GSM and banking

N 은 a, b, n (d = a * b mod n)의 비트 수이다. 제조 회사별 마이크로 프로세서에서 Crypto-processor가 차지하는 영역은 (그림 2)와 같다. SCALPS 에서는 Crypto 전용 프로세서를 설계하였다.



(그림 2) Microprocessor 면적 (mm^2)

Siemens의 SLE44C200은 540비트의 arithmetic crypto-coprocessor가 내장 되었는데, 5MHz 클럭으로 동작시 220ms이내에 512비트 암호 단어를 복호할 수 있다.

또한, Philips의 P83C852라는 crypto 카드는 특수 연산 unit에 의해 빠른 곱셈과 덧셈을 수행하며 450msec만에 공개 키 암호화를 끝낸다. Motorola는 아직 crypto-coprocessor가 내장된 스마트 카드를 내놓지 않고 있으나, 512비트 키를 이용하여 500msec이내에 해독할 수 있는 M68HCO5SC29가 생산될 예정이다.주요 Crypto-processor에 대한 성능을 RSA, DSA(Digital Signature Algorithm), SHA(Secure Hash Algorithm)에 대하여 동일 clock을 기준으로 수행 시간을 비교하면 <표 3>과 같다.

<표 3> Crypto-processor의 특성

알고리즘 \ Crypto-processor	44C200	ST16CF54	83C852
512 bit RSA	60 ms	54 ms	600 ms
768 bit RSA	271 ms	290 ms	3,600 ms
1024 bit RSA	456 ms	390 ms	-
512 DSA 서명	92 ms	80 ms	1020 ms
512 DSA 검증	171 ms	120 ms	2,160 ms
SHA-1	17 ms	11 ms	17 ms

ST16CF54 가 44C200에 비교하여 512 비트 및 1024 비트 연산에서는 성능이 우수하지만, Montgomery 연산으로 인한 많은 곱셈을 수행하게 되므로, 중국인의 나머지정리 및 DSA 역 모듈러 연산 등에 주로 쓰이는 256 비트 연산에서는, 오히려 44C200이 14% 정도 우수하다. 또한, 83C852는 성능면에서는 뒤지나 실리콘 면적, 단순한 회로 면에서는 우수하다. 그러므로, 우수한 스마트 카드를 선정하기 위해서는 실리콘의 면적 및 공정기술, 비트 수, 동작속도, 알고리즘, 신뢰성 있는 회로, 메모리 용량, 전력소비율, 범용성 등 다양한 면을 검토하여야 한다.

또한, 스마트 카드를 이용하여 응용 분야에 효율적으로 적용하기 위해서 COS(Card/Chip Operating System)에서의 자료 구조 관리 기능, 데이터가 저장이 되는 형태, 디렉토리의 제공 여부, 화일 형태의 종류(순차, 랜덤, 환형 화일), 로그인 및 감사 추적 기능, 액세스 제어, 암호 함수 라이브러리 등의 기능을 검토하여야 한다.

ISO/IEC 7816의 제 4 부에서는 TLV(Tag Length Value)를 이용한 효율적인 자료 방법을 정의하고 있다. 그러나, 아직도 많은 운영 체계에서는 논리적 참조 방법인 TLV 개념을 도입하고 있지 않다.

VII. 결 론

사용 및 응용 분야가 확산되고 있는 스마트 카드의 보안성 및 그 성능을 살펴보았다. 보안적인 관점에서 보조연산용 프로세서의 성능은 스마트 카드의 성능에 큰 영향을 미치므로, 병렬처리 기법을 이용한 연산의 병렬화 구조로의 발전이 요망된다. 최근에는 VLIW(Very Long Instruction Word)등의 구조가 개발되고 있다. 체계적인 보안을 위해서는 카드의 물리적 보안 및 키 관리, 카드 인증, 사용자 및 메시지 인증, 암호 프로토콜, 통신 및 데이터 암호화 등 다양한 분야에 걸쳐 연구의 대상이 되고 있다.

참 고 문 헌

[1] 김영수, 이대기, "스마트 카드 기술 동향 및 분석", 전자통신동향분석, 제 11 권제 2 호, pp.61-69, 7.1996.

[2] John Gallant, "Smart-Card ICs... Trained for security", EDN ASIA, pp.21-28, April, 1996.

[3] Bernd Schendel, "Smartcard crypto-controllers improve data security", Electronics Engineer, pp.114-116. July, 1996.

[4] D.H.Edmondson, "Smart cards : A Generic Threat Assessment", Bulletin 37, Infomation Technology Security, Canada, December, 1994.