[5A-21]

자바 카드를 위한 암호화 기반 클래스 구현

*채철주, **김상국, **이명선, *이성현, *이재광
*한남대학교 컴퓨터공학과, **한국과학기술정보연구원
cjchae@netwk.hannam.ac.kr

Implementation of Cryptographic Base Class For Java Card

*Cheol-Joo Chae, **Sang-Kuk Kim, **Myung-Sun Lee, *Seoung-Hyun Lee, *Jae-Kwang Lee
*Dept. of Computer Engineering, Hannam University,
**Korea Institute of Science and Technology Information

요 약

자바카드 API는 스마트 카드와 같은 작은 메모리를 가진 임베디드 장치에서 실행환경을 최적화하기 위해 구성되었다. 자바카드 API의 목적은 스마트 카드와 같이 작은 메모리를 가진 임베디드 장치에서 사용되도록 개발되었다. 따라서 한정된 메모리를 가진 스마트 카드 기반의 프로그램을 개발할 때 많은 이점을 제공한다. 그러나 스마트 카드의 주된 목적이 보안이라는 것을 생각할 때 최근 널리 쓰이는 공개키 암호화 과정에서 필요한 모듈러 연산, 최대공약수 계산, 그리고 소수 판정과 생성 등의 연산을 지원하지 않는다는 것은 큰 단점이 될 수 있다. 본 논문에서는 이러한 단점을 해결하고 쉽게 공개키 암호화 알고리즘을 구현하고자 암호화 연산에서 기반 클래스라 할 수 있는 BigInteger 클래스를 설계하고 구현하였다.

I. 서론[1)]

IC(Integrated Circuit) 카드는 인터넷 사용의 급증과 정보통신 환경의 급속한 변화에서 강력하고 효과적인 정보보호 서비스를 제공한다. 근래에 IC 카드의 사용이 급증하고 있으며 이와 관련한 기술 개발이 활발히 이루어지고 있다[2]. 개인용 컴퓨터나 무역망, 금융망, 행정망 및 의료망 등에서 정보보호에 IC 카드를 사용하는 기술이 이미 일부 국가에서는 실용화 단계에 있으나 국내에서는 미진한 상태이다. 현재 주로 실용화되고 있는 IC 카드 기술은 스마트 카드 관련 기술과 자바 카드 관련 기술이 주류를 이루고 있다.

자바 카드 API에는 자바 API의 일부분만을 정의해 놓았다. 때문에 공개키 암호 알고리즘의 구현에 필요한 BigIntger 클래스를 지원하지 않는다. 본 논문에서는 자바 카드에서 동작할 수 있는 BigInteger 클래스를 구현한다. 2장에서는 자바카드와 구현에 적용한 알고리즘을 살펴보고, 3장에서는 구현한 클래스의 내용에서 응용연산 부분을 설명하였다. 4장에서는 이를 기반으로 BigInteger 클래스를 구현하고, 5장에서 결론을 맺는다.

* 본 연구는 과학기술부
지역협력연구센터(R12 2003-02004 0) 지원으로
수행되었음

II. 연구 배경

1. 자바 카드(Java Card)

자바 카드란 COS(Card Operating System)위에 JCVM(Java Card Virtual Macine)이 랩핑(Wrapping)되어 있는 구조의 스마트 카드를 말한다[1]. 자바 카드 API는 자바 카드 상에서 Java를 이용한 소프트웨어 개발에 필요한 API들을 정의한 것이다.

이것은 스마트 카드의 보안성을 연구하던 Schlumberger사의 연구팀에 의해 1996년에 소개되었다. 이 후 발표된 자바 카드 API 1.0은 단지 명세서의 역할만을 했다. 그러나 1997년 Sun Microsystem사에서 자바API의 일부 제한된 기능을 수행하는 자바 카드 API 2.0을 발표하였다. 그 후 계속 발전하여 현재 2.1.1버전까지 개발되어 있는 상태이다[6].

자바 카드 API는 전자상거래, 네트워크 접근, 인증을 위한 차세대 네트워크 기술을 제시하였다. Bull, Gemplus, Schulmberger 등 전 세계 스마트카드 제조 회사의 90%이상이 자바 카드의 개발을 위해 라이센스를 이미 받은 상태이다[8].

자바 카드 API는 스마트 카드와 같은 작은 메모리를 가진 임베디드 장치를 위한 프로그래밍에 필요한 패키지와 클래스만을 정의하고 있다. 또한 국제 표준인 ISO7816과 산업 명세 표준인 EMV(Europay/ MasterCard/Visa)와 서로 호환된다. 아래 표 1은 Java와 자바 카드의 자료형을