자바카드를 이용한 오프라인 전자화폐시스템 설계와 구현

장유탁, 유기영
경북대학교 컴퓨터공학과

Design and Implementation of Offline Electronic Cash System using JAVA Card

Yu-Tak Jang Kee-Young Yoo
Department of Computer Engineering, Kyungpook National University

요 약

전자화폐는 기존의 화폐 개념을 네트워크 상으로 옮겨 디지털화한 무형의 화폐 또는 지불수단으로, 기존 신용력에 기반을 두고 종이 화폐가 가지고 있었던 불편함을 해소하기 위해 원격지 이송에 따른 통신기능, 휴대 및 보관관리의 편리성, 위조방지 기능을 기존 화폐 개념기능에 추가 한 것이며, 온라인 방식과 오프라인 방식이 있다. 본 논문에서는 오프라인 방식 전자화폐가 만족해야 할 요구사항 즉, 익명성, 위조불가능성, 이중사용방지와 조건부 익명성 철회를 충족 시킬 수 있는 시스템의 구조와 프로토콜들을 제시하고, 이를 자바카드를 이용해서 구현하였다.

1. 서 론

최근에 인터넷 전자상거래가 증가함에 따라서 전자상거래의 결제수단으로 현재 신용카드에 의한 결제가 주류를 이루고 있지만, 앞으로는 점차 전자화폐(Electronic Money)에 의한 결제수단의 이용이 급증할 것으로 전망된다. 이미 선진국에서는 이를 개발하여 운용을 시작하는 단계에 있으나, 우리 나라에서는 아직 이에 대한 연구가 미비한 실정이다. 전자화폐란 기존의 화폐 개념을 네트워크 상으로 옮겨 디지털화한 무형의 화폐 또는 지불수단으로, 기존 신용력에 기반을 두고 종이 화폐가 가지고 있었던 불편함을 해소하기 위해 원격지 이송에 따른 통신기능, 휴대 및 보관관리의 편리성, 위조방지 기능을 기존 화폐 개념기능에 추가 한 것이다[7].

본 논문에서는 오프라인형 전자 화폐 시스템의 프로토콜을 설계하고 이를 자바카드를 이용해서 구현했다. 본 논문의 구성은 다음과 같다. 2장에서는 전자화폐의 관련연구와 요구사항에 대해서 설명하고, 3장에서는 자바카드에 대해서 설명한다. 4장에서는 오프라인 전자화폐에서의 전체적인 시스템과 프로토콜을 설명하고, 5장에서는 4장에서 제시한 프로토콜을 구현한 방법을 설명한다. 마지막으로 6장에서는 결론 및 향후 연구 방향에 대해서 기술한다.

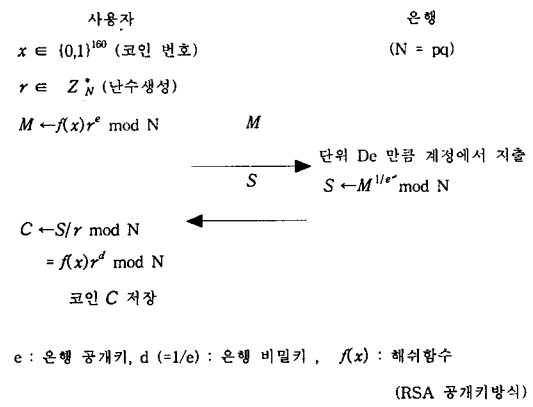
2. 전자화폐의 관련연구와 요구사항

전자화폐는 크게 온라인방식과 오프라인방식 두 분류로 발전 되어 왔다. 온라인방식은 지불 거래시 고객과 상점사이에 은행이 온라인으로 연결되어 거래하는 방식이며, 오프라인 방식은 거래시 고객과 상점 이외 은행과 같은 제삼자가 개재하지 않고 상점에서의 지불을 처리할 수 있는 방식이다. 이는 거래량증가에 따른 은행의 부하를 줄여주며, 지불의 신속화를 가져오고, 네트워크의 제한을 갖지 않는 장점을 가진다. Chaum, Flat, Naor에 의해 RSA 디지털 서명 기법을 이용한 추적 불가능한 오프라인의 전자화폐 이론이 제시된 이후 , 여러 모델들이 제시되었으며, CAFE[1,3], Mondex, VisaCash, Proton등과 같이 시범 서비스로 이어진 예도 있다. 현재는 전자화폐의 완전 익명성의 의한 돈세탁이나 갈취와 같은 범죄를 막기 위한 연구도 진행중이다[2].

전자화폐 프로토콜이 만족해야 할 요구사항에는 기본적인 요소로 위조 불가능성(Unforgeability), 익명성(Anonymity), 이중 사용방지(Double-Spending prevention), 추적 불가능성(Untraceability) 등이 있으며, 추가적으로 분할성, 양도성, 공정성, 익명성 철회, 사용자추적, 현금추적 등이 있다.

각 요구사항에 대해 본 연구에서는 은행의 디지털 서명을 통해 위조를 막고, 익명성과 추적 불가능성 보장을 위해 그림 1과 같은 블라인드 서명(Blind signature)[5]을 사용한다. 이중 사용방지를 위해 temper-resistant 장치인 스마트카드[8]를 사용하면서, 사용된 코인 DB를 이용해서 신분을 확인할 수 있는 방법을 사용한다. 또한, 완전익명성의 의한 범죄를 막기 위해서 사법기관이 요청시 특정 사용자가 사용한 내역을 추적할 수 있도록 인출시 사법기관만이 볼 수 있는 정

보를 프로토콜 내에 포함시켰다.



e : 은행 공개키, d (=1/e) : 은행 비밀키 , $f(x)$: 해쉬함수

(RSA 공개키방식)

그림 1 블라인드 서명을 이용한
단위 De를 갖는 코인 C 생성

3. 자바카드

자바카드[6]는 Java 프로그래밍 언어로 쓰여진 프로그램을 실행할 수 있는 스마트 카드이다. Java 라는 표준 프로그래밍 언어를 사용함으로써, OOP 의 장점을 얻을수 있고, 플랫폼 비의존성을 가지며, 하나의 카드 내에 여러 애플릿을 상주시킬 수 있다.

이런 장점을 가지고 개발자는 애플릿을 개발하여 손쉽게 스마트카드의 기능을 확장할 수 있다. javacard와 javacardx Class를 임포트해서 원하는 어플리케이션(.java)을 완성한후, 컴파일해서 바이트코드(.class)로 만들고, 카드 바이너리 파일(.bin)로 변환후, 카드에 로딩 및 인스턴스를 생성한다. 인스턴스가 생성되면 Select 명령어를 통해 원하는 기능을 수행할 수 있다. 본 연구에서는 Schlumberger에서 개발한 Cyberflex[4]를 이용하였으며, 그림2 와 같은 논리적 구조를 가진다. 본 연구에서는 애플릿에 터미널과의 상호인증, 암호기능, 코인의 로딩과 저장, 잔액, 히스토리에 관련된 명령어 등을 추가하였다.

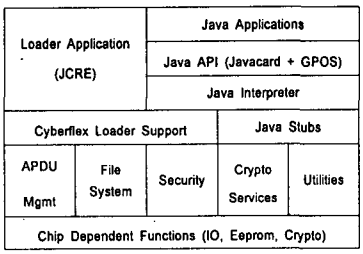


그림 2 Cyberflex 구조

4. 오프라인 전자화폐 시스템의 구조와 프로토콜

4.1 시스템 구조

전체 구성은 그림3 과 같으며, 시나리오는 다음과 같다. 은행으로부터 계좌와 스마트카드를 얻은 사용자는 은행에서 제공하는 ATM (Auto Teller Machine)이나 PC에 설치된 가상 ATM기를 통하여, 자신의 카드에 코인을 다운 받을 수 있다. 지불 거래시 카드를 상점의 지불 터미널에 넣고, 코인들을 조합하여 돈을 지불한다. 상점은 마감후나 시간이 날 때 은행에 들러, 받은 코인들을 정산하고 자신의 계좌로 금액을 이체 받는다. 은행은 사용자가 요구시 코인들을 블라인드 서명을 통해 생산하며, 결제시 사용된 코인 DB를 이용하여 이중사용을 탐지하며, 사법기관의 요청시 거래내역을 보여준다.

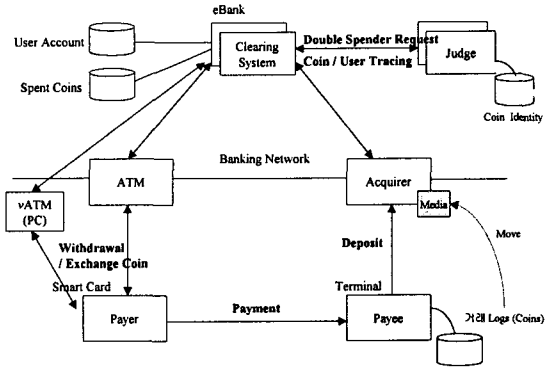


그림 3 전체 시스템 구조

4.2 프로토콜

오프라인 전자화폐 프로토콜은 기본적으로 고객, 은행, 상점사이에서 인출, 지불, 결제단계를 수행하고, 추가적으로 사법기관과 은행과의 코인/사용자 추적단계도 수행한다. 그림4, 그림5, 그림6, 그림7은 각 단계에 대한 프로토콜을 나타낸다. 기본적으로 사용자와는 PIN에 의한 인증을 하며, 카드와의 통신에는 세션키를 이용한 비밀키 암호방식을 사용하였으며, 그 밖의 통신에서는 RSA 공개키 방식을 이용하였다.

(가) 인출단계 (Withdrawal)

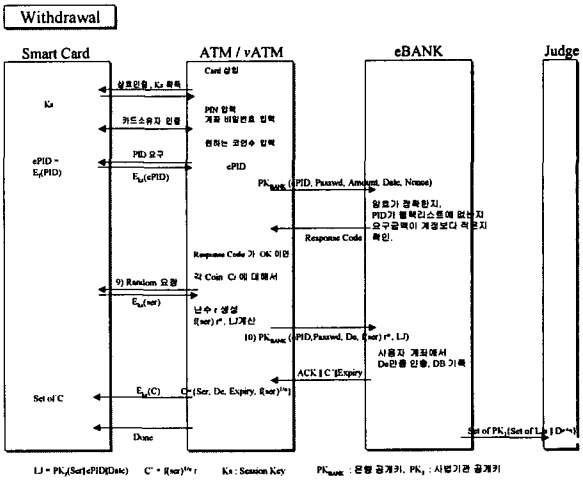


그림 4 인출 프로토콜

(나) 지불단계 (Payment)

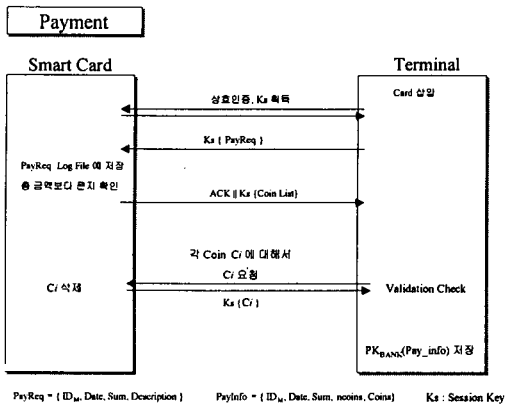


그림 5 지불 프로토콜

(다) 결제단계 (Deposit)

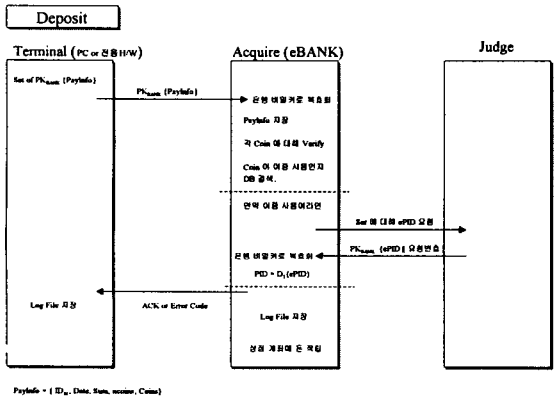


그림 6 결제 프로토콜

(라) 추적단계(Coin, User Trace)

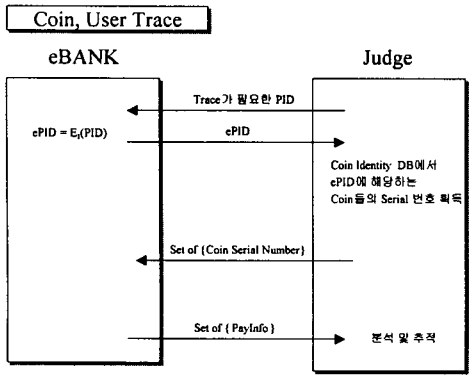


그림 7 코인,사용자 추적 프로토콜

5. 구현

본 시스템은 가상 ATM기(그림8), 지불 프로그램, 은행 DB 및 관리프로그램, 사법기관 DB 및 관리프로그램으로 구성된다. 윈도우즈(윈도우즈 95, 98)환경에서 사용 가능하도록 볼랜드사의 C++ Builder 4.0으로 개발하였고, 카드 애플릿을 만들기 위해서 Sun Microsystems 사의 JDK 1.2.1을 사용하였다. 비밀키 암호방식으로는 DES를 사용했고, 공개키 암호방식은 몽고메리 알고리즘을 이용해서 속도가 개선된 RSA 방식을 사용했으며, 해쉬 함수로는 SHA-1을 사용하였다.

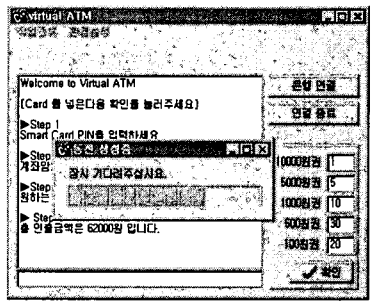


그림 8 가상 ATM 화면

6. 결론 및 향후 연구방향

본 논문에서는 오프라인 전자화폐 시스템의 프로토콜을 설계하고, 자바카드를 이용해 구현하였다. 기본적으로 익명성 보장 및 위조 방지을 위해 블라인드 서명을 사용했고, 스마트카드를 이용해서 이중사용을 방지하였으며, 기존의 전자화폐의 문제점이었던 돈 세탁과 같취와 같은 범죄를 예방하기 위해 사법기관과의 상호 프로토콜을 적용했다. 아직까지 거스름돈 문제나, 카드의 도난이나 손상에 대한 복구는 이루어지지 못했다. 향후 연구방향은 양도성이나, 분할성, 복구성을 가진 프로토콜 설계가 필요하며, 자바카드 내 암호 알고리즘을 보강하여 보안측면을 강화하여야 할 것이다.

참고문헌

[1] Boly,J.P.,et al.,"The ESPRIT Project CAFE," *Computer Security* - ESORICS'94, *Third European Symposium on Research in Computer Security Proc.*,Lecture Notes in Computer Science, Vol. 875, 1994, pp.217-230

[2] Law Laurie, et al., How to make a mint: the cryptography of a nonymous electronic cash, 1996, http://www-swiss.ai.mit.edu/6805/articles/money/nsamint/nsamint.htm

[3] Donal O'Mahony, *Electronic Payment Systems*, ARTECH HOUSE, 1997

[4] Schlumberger, *Cyberflex Access Developer's Series Programmer's Guide*, 1998

[5] Berry Schoenmakers , *Basic Security of the ecash Payment System* ,1997

[6] Sun Microsystems, *Java Card 2.0 Programming Concepts*, 1997

[7] 정완용, "전자화폐에 의한 전자결제제도의 법적문제점에 관한 고찰", 경희법학연구소 국제법무세미나 , 1998, http://www.kyungwon.ac.kr/~profsjh/wyc/ec-law.htm

[8] 김증섭, "RSA 암호 알고리즘을 이용한 스마트카드의 운영체제 구현", 석사학위 논문, 경북대학교, 1998