오프라인(off-line) 지불처리를 위한 안전한 전자화폐 프로토콜의 설계

김현라*, 주한규**
한림대학교 컴퓨터공학과
e-mail : *hyulla@center.cie.hallym.ac.kr
**hkjoo@hallym.ac.kr

Design of a Secure Electronic Cash Protocol for Off-line Payment

Hyulla Kim*, Hankyu Joo**
Dept. of Computer Engineering, Hallym University

요 약

디지털 혁명 시대에 경제활동의 변화와 더불어 등장한 전자화폐는 점차 그 영역을 넓혀가고 있다. 하지만 현재 사용되고 있는 전자화폐 시스템은 안전상의 문제점을 내포하고 있다. 각 시스템마다 그것들을 해결하려는 노력을 기울이고 있지만 대부분이 오프라인(off-line) 보다는 온라인(on-line) 지불 처리 방식을 전제로 하고 있다. 본 논문에서는 현재 운영되는 전자화폐 시스템의 문제점을 짚어보고 이를 해결할 수 있는 안전한 전자화폐 프로토콜을 오프라인(off-line) 지불 처리에 초점을 맞춰, 설계한다.

1. 서론

산업 혁명에 뒤이은 디지털 혁명 시대에 가장 큰 변화는 경제 활동의 변화를 들 수 있을 것이다. 기존에 존재하던 많은 실물 시장(Real Market)은 가상 공간(Cyber Space)상으로 이전하게 되고 이 속에서 디지털 데이터를 근간으로 각종 구입, 판매 그리고 대금 지불이 이루어지게 될 것이다. 이러한 환경에서 가장 중요하게 거론되고 있는 것은 지불 방법에 관한 문제이고 기존의 지불 방법으로는 한계가 발생하게 된다. 따라서 인터넷 환경에 적합한 새로운 지불 방법이 요구되고 있으며 그 해결책으로 전자화폐(Electronic Cash)가 등장하게 되었다. 전자화폐는 인터넷상의 전자상거래(Electronic Commerce)는 물론, 일반 상거래에서도 그 사용량이 증가되고 있으며 실물 화폐와 더불어 중요한 지불 수단으로 부상하고 있다.

이 시점에서 간단히 전자화폐를 정의하자면, 액면가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보라 할 수 있는데 이를 사용함으로써 얻을 수 있는 이점에는 다음의 여러가지가 있다.

지불, 금전의 양도, 환불이나 예금에 따른 은행 절차도 네트워크를 통해서 행할 수 있다. 전자상거래에서의 물건값 지불이 편리한 것은 물론 상점이 매상금을 네트워크 경유로 은행에 예금할 수도 있다. 야간에 거래금고에 거액을 옮기지 않고도, 업무를 마칠 수 있다. 또한, 소비자가 현금을 잃어버렸거나 도난당했을 때의 피해를 막는 데 도움이 되는데 이것은, 전자화폐를 IC 카드 등의 기억장치에 저장해서 휴대하면 패스워드 등을 이용해서 부정사용을 방지할 수 있기 때문이다. 또한 전자화폐 데이터의 전체 또는 일부의 백업으로 분실, 도난시에 소정기관에 신청하여 분실한 전자화폐를 무효로 할 수 있다.

요컨대, 이러한 전자화폐를 다른 전자지불 방식과 비교했을 때의 이점은 크게 4가지로 정리할 수 있다.

첫째, 전자화폐는 이용자의 프라이버시를 지킬 수 있다. 신용카드를 사용한 전자지불은 이용자의 프라이버시가 보장되지 않는다.

둘째, 지불에 요구되는 비용을 줄일 수 있다. 신용카드의 경우는 일정금액 이상 물건을 사지 않으면 이용할 수 없는 상점이 적지 않다. 신용카드로 지불할

때의 수수료가 싸지 않기 때문이다. 이에 반해 전자화폐는 이용자의 신용조사 등의 절차가 필요없기 때문에 신용카드에 비교해서 운용비용을 싸게 할 수 있다.

셋째, 개방성을 갖추고 있다. 전자화폐의 발행체가 중앙은행인 경우나 발행체가 현행 지폐와의 태환성을 보증하고 있는 경우 전자화폐는 원칙으로 국내 어디에서도 이용할 수 있다. 그런데 신용카드로 지불할 이용자나 지불받을 상점은 미리 특정한 신용카드회사와 사전에 가맹계약을 해놓을 필요가 있다. 이 때문에 신용카드 회사에 의한 상점의 의존 등이 발생할 우려가 있다. 당연히 전자화폐인 경우도 상점에 전자화폐를 취급하는 장치를 설치할 필요가 있으나 전자화폐 자체가 가치를 갖는다는 성질상 발행체에 의한 의존도는 적을 것이다.

넷째, 현행의 신용카드나 선불카드는 카드 보유자로부터 다른 카드보유자에게 가치를 양도할 수 없다. 이에 비해 전자화폐는 현금의 양도에 상당하는 처리 즉, 유통성을 실현할 수 있다[1].

하지만 현재 온라인(on-line) 혹은 오프라인(off-line) 상에서 전자화폐를 지불수단으로 하는 전자화폐 시스템이 장점만을 갖추고 있는 것은 아니다. 아직도 그 이면에는 극복해야할 여러가지 문제점들도 많이 내재되어 있다. 그 중 민감한 부분이라 할 수 있는 상품의 구입이나 특정 서비스에 대한 대금지불에 있어서의 문제점은 영수증 부재이다. 모든 거래에 있어 그 거래의 증거 자료로 이용할 수 있는 것이 영수증이다. 영수증은 언제 누가 누구에게서 얼마의 가격에 어떤 상품을 구입했는지 혹은 특정 서비스에 대한 대금지불 결과를 증명해 줌으로써 구매자와 상점간의 논란을 해결해줄 수 있는 문서이다[2]. 또한 사용자 입장에서는 자신의 거래 내역을 확인하고 정산할 수 있도록 도와주기도 한다. 하지만 현재 사용되고 있는 대다수의 전자화폐 시스템은 이러한 영수증 발급에 무관심하며 이로써 많은 문제점들을 발생시키기도 한다.

본 논문에서는 이러한 영수증 부재의 문제를 해결하는 오프라인(off-line) 상에서의 안전한 전자지불 프로토콜을 설계하였다. 본 논문의 2 장에서는 전자화폐의 흐름과 전자화폐 시스템의 유형별 특성 그리고 전자화폐의 기본 프로토콜을 살펴본다. 3 장에서는 본 논문에서 제안한 영수증 및 거래명세서를 위한 프로토콜의 동작원리와 메시지의 구성 형태를 설명한다. 마지막으로 4 장에서 결론과 앞으로 연구되어야할 사항들을 알아본다.

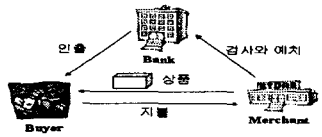
2. 전자화폐(Electronic Cash) 시스템

전자화폐 시스템은 독립적인 신용구조를 가지고 있어서 물품 구입시 은행이나 카드 발행사로부터의 거래 승인이 없다. 사용자간의 가치 이전도 가능한 현금과 유사한 개념으로 전자지불 시스템이 지향하는 궁극적인 목표 시스템이다. 전자화폐 시스템은 화폐가치를 디지털 정보의 형태로 발행하여 네트워크를 통한 온라인 대금결제를 가능하도록 한 네트워크형 전자화폐 시스템과 플라스틱 카드 위에 부착된 IC 칩을 이용해 오프라인 대금결제에 활용하는 IC 카드형 전자화폐 시스템으로 나눌 수 있다[1].

다음에서 전자화폐의 흐름 및 전자화폐 시스템의 유형별 특성 그리고 전자화폐의 기본 프로토콜을 살펴 본다.

2.1 전자화폐의 흐름

(그림 1)은 전자화폐를 이용하여 상점에서 물건을 구입하고 물품 대금을 지불하는 기본적인 흐름에 대하여 나타내고 있다. (그림 1)에서 전자화폐의 기본 모델은 은행, 이용자, 상점의 3 가지 실체의 집합과 전자화폐의 인출, 지불, 검사와 예치 단계로 나누어진다.



(그림 1) 전자화폐의 흐름

여기서 기본 모델에 대하여 살펴본다. 우선, 이용자와 상점은 은행에 자신의 계좌를 개설하도록 한다[3].

① 은행은 이용자에게 전자화폐를 발행하는 대신 발행액에 대응하는 금액을 이용자의 계좌로부터 인출한다. 여기서 이용자와 은행간에 인출 프로토콜이 실행된다.

② 이용자는 상점에서 물건을 사고 은행에서 받은 전자화폐를 지불한다. 여기서 이용자와 상점간에 지불 프로토콜이 실행된다.

③ 상점은 은행에게 전자화폐의 이중사용 검사를 의뢰한다. 그리고 정당한 경우(이중 사용 되지 않은 경우)에만 자신의 계좌로 자금이체가 이루어지게 된다. 정당하지 않은 경우에는 상점의 전자화폐 예치는 거부된다. 여기서 상점과 은행간에 예치 프로토콜이 실행된다.

2.2 네트워크형 전자화폐 시스템

최근에 스마트 카드와 같은 추가적인 하드웨어가 요구되지 않는 다음과 같은 대표적인 세 가지의 전자화폐 시스템들이 WWW 상에서 지불을 할 수 있도록 개발되었다. 첫번째가 완전한 익명성을 가지는 전자화폐 시스템인 Ecash[4]가 그것이다. 두번째로는 완전한 익명성을 제공하는 것은 아니지만 좀 더 규모가 크며 신원확인이 가능한 전자화폐인 NetCash[5]가 있다[1].

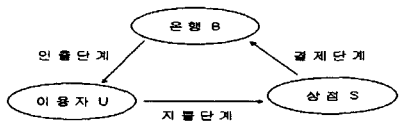
2.3 IC 카드형 전자화폐 시스템

IC 카드는 프로그램화된 정보를 저장할 수 있기 때문에 스마트 카드라고도 한다. 즉, IC 카드는 정보처리 능력을 보유하여 빈번하게 변화하는 자료를 저장하는데 적합하고 암호화 알고리즘의 저장 시 이용되어 디지털 서명 및 신분확인에도 활용될 수 있다 또한 IC

카드는 이동이 가능하고 IC 카드 판독기와 자료 표시기를 갖춘 전화선을 이용하여 출금할 수 있어 전자상거래 뿐만 아니라 일반 소매점에서도 사용이 가능하다[6]. 이러한 IC 카드 중심의 전자화폐 시스템의 대표적인 예로는 Mondex[7]와 VisaCash[8]가 있다.

2.4 전자화폐의 기본 프로토콜

전자화폐의 기본 프로토콜은 (그림 2)와 같이 기본적으로 은행 B, 이용자 U, 상점 S 로 구성되어 있으며 이용자와 은행간에 이루어지는 인출단계(withdrawal phase), 이용자가 발행단계에서 받은 전자화폐를 상점에 지불하고 물건을 사는 지불단계(payment phase), 상점이 이용자로부터 받은 전자화폐를 은행에 제출하여 상점의 계좌로 일정 금액을 입금 받는 예치단계(deposit phase)로 구성된다[3].



(그림 2) 전자화폐의 기본 프로토콜 구성

2.3.1 인출 프로토콜

인출 프로토콜은 이용자가 은행으로부터 전자화폐를 인출하는 단계의 프로토콜이다.

- 이용자는 임의로 작성한 난수를 블라인드 서명 처리하여 계좌의 소유자인 것을 증명하는 ID 카드, 인출할 금액과 함께 은행에 전달한다.
- 은행은 ID 카드에 의해 이용자를 인증하고 이용자의 계좌로부터 지정된 금액을 인출한 뒤, 그에 대응한 전자서명을 계산하여 이용자에게 전달한다.
- 이용자는 블라인드 서명을 제거하여 선택한 난수에 대한 은행의 전자서명을 복원하며 그것이 전자화폐가 된다.

이러한 개념적인 인출 과정을 수식으로 나타내기 위해 프로토콜에 사용된 암호 기호들의 의미를 간단히 정리하면 다음과 같다.

f, 일방향 함수
r, 블라인드 변수
x, 이용자가 작성한 난수
dB, 전자화폐 액면에 대응한 은행의 비밀키
eB, 전자화폐 액면에 대응한 은행의 공개키
mod n, n 은 은행의 RSA 모듈러 값

다음은 블라인드 서명에 근거한 전자화폐 인출 프로토콜을 수식으로 나타낸 것이다.

- 이용자는 x 와 r 을 랜덤하게 선택하고 인출하고자 하는 금액에 대응하는 은행의 공개키 eB 를 사용하여 $B = r^{eB} f(x)$를 계산한다.
- 이용자는 ID 카드를 제시하고 인출하고자 하는 금액(예를 들어, 100 만원)과 함께 B 를 은행에 송신한다.
- 은행은 B 에 100 만원에 대응한 서명 $B^{dB} \pmod n$을 계산하고 이용자에게 보낸다. 동시에 이용자의 계좌로부터 100 만원을 인출한다.
- 이용자는 B^{dB} 를 r 로 나누어 $C = f(x)^{dB}$ 을 얻는다. 또한 $C^{eB} = f(x)$에 의해 은행의 서명을 확인한다.
- 최종적으로 이용자는 은행이 서명한 정당한 전자화폐(x, $f(x)^{dB}$)를 얻을 수 있다.

이 프로토콜에서 은행은 B 밖에 수신할 수 없으므로 x 나 C 의 값에 대해 전혀 모른다. 그러나 이용자의 ID 카드가 제시되어 계좌로부터 지정금액을 인출할 수 있고 실제 전자화폐로써 이용되는 C 의 내용을 모른 채 B 에 서명해도 은행에 돌아갈 불이익은 없다[3][9][10].

2.3.2 지불 프로토콜

인출된 전자화폐를 사용하는 지불 프로토콜을 오프라인(off-line) 관점에서 서술하면 다음과 같다.

- 이용자와 상점간에 상품과 금액의 교섭이 성립되면, 이용자는 상품을 지정해서 전자화폐를 상점에 지불한다.
- 상점은 이용자로부터 받은 전자화폐를 확인한 뒤, 상품을 이용자에게 배달한다[3].

2.3.3 예치 프로토콜

상점이 이용자로부터 받은 전자화폐를 은행에 제공하고 이중사용 검출 과정을 무사히 통과하면 상점의 계좌로 자금이체가 이루어지는 단계의 프로토콜이다.

- 상점은 전자화폐의 이중사용 유무를 은행에 검사 의뢰한다.
- 은행은 전자화폐에 부가되어 있는 은행의 서명을 확인하고 다음에 동일한 색인의 전자화폐가 과거에 예치(deposit)되 적이 있는가를 은행 데이터베이스를 사용하여 조사한다. 만약 예치되어 있지 않으면 새로 예치하고 데이터베이스에 이 전자화폐의 색인을 등록한다.

이러한 개념적인 예치 과정을 앞에서 언급한 수식을 사용하여 나타내면 다음과 같다.

- 상점은 (x, C)을 수취하면 은행과 연결하여 동일한 (x, C)가 이미 예치되었는지를 조회한다.
- 은행은 전자화폐의 서명을 $C^{eB} = f(x)$에 의해 확인하고 만약, 예치되어있지 않으면 (x, C)을 예치한다.

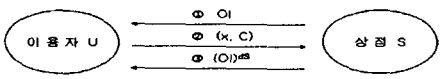
전자화폐는 디지털 정보이므로 완전한 복사본을 얻는 것이 용이하다. 따라서 이러한 점을 이용한 부정 행위 발생 가능성이 매우 높다. 이에 은행은 과거에 축적된 전자화폐의 색인을 모두 데이터베이스에 기록해 두고 새롭게 예치되는 전자화폐와의 색인의 중복을 검사한다. 은행은 만약 동일 색인의 전자화폐가 예치된 경우, 이중사용으로 간주하고 상점의 전자화폐 예치를 거부한다[3][9][10].

3. 영수증 및 거래명세서를 위한 프로토콜

앞에서 살펴본 전자화폐의 기본 프로토콜 중, 오프라인 관점에서 서술된 지불 처리 부분을 확장하여 이용자가 영수증 및 거래명세서를 발급 받을 수 있도록 한다.

3.1 확장된 지불 프로토콜

(그림 3)은 상점과 이용자간에 은행의 개입 없이 지불 처리가 이루어지는 단계를 간단히 나타낸 것이다.



(그림 3) 확장된 지불 프로토콜

① OI 는 상품의 구매 정보를 나타낸다. 즉, 이용자가 이번 거래에서 구입하려고 하는 상품에 관한 정보를 나타낸다. OI 에는 상품명, 구매 개수, 상품별 단가, 총 금액, 배달지 및 구매 당시의 날짜, 시간이 포함된다. 상점은 OI 를 이용자에게 전송한다.

② 이용자는 날짜, 시간(동기화 필요)을 비롯한 OI 내용을 확인하고 (OI, (x, C))을 기록한 후, (x, C)을 상점에 전송한다.

③ 상점은 (OI)을 상점의 비밀키인 dS 로써 서명한 후, 사용자에게 전송, 사용자는 OI 와 $(OI)^{dS}$ 를 확인한다.

최종적으로 $(OI)^{dS}$ 는 영수증 역할을 한다.

3.2 토의

확장된 지불 프로토콜은 상점이 이용자에게 보낸 구매정보를 상호간의 지불 확인절차를 거친 후, 상점의 서명을 더해 영수증으로 사용할 수 있도록 한다. 이 때, 이용자가 전자화폐(x, C)를 전송하고 영수증을 받지 못하여 논란의 여지가 있는 경우, (OI, (x, C))을 제시함으로써 상점이 (x, C)을 가지고 있으면 사용자가 대금을 지불하였음이 증명된다. 만약, 그렇지 않고 이용자가 지불하지 않았을 경우, 이용자가 보여줄 수 있는 (OI, (x, C))가 없으므로 이후의 논쟁을 방지할 수 있다.

하지만 본 논문에서 제안한 프로토콜은 기존의 프로토콜에 안전성을 보완함과 동시에 다음의 문제점들을 추가로 가지게 되었다. 우선, 상점은 지불처리가 발생할 때마다 매번 서명해야 하기 때문에 기존의 시스템보다 처리 시간이 오래 걸린다. 다음으로, 시간 동기화, 적어도 편차를 기록하는 작업이 이루어져야 한다. 마지막으로 카드가 저장하게 될 정보의 양이 많아지므로 축약 정보의 저장이 필요하게 된다.

4. 결론 및 향후 연구

현재 전자화폐라는 새로운 지불 수단에 대한 다양한 연구가 진행되고 있지만 일반가정에서도 이용할 수 있는 사회적 기반구조로써 보급되고 있지는 않다. 그러나 이러한 상황이 점차 변해가면서 각 가정의 재산목록에 컴퓨터 한 대가 기본적인 항목으로 올라가듯, 전자화폐를 사용하려는 일반인의 수도 급격히 늘어날 전망이다.

이와 같이 실용적인 전자화폐 시스템을 경제적으로 구축할 수 있는 전망이 보이면서 금융업뿐만 아니라 유통, 교통, 통신 등 다양한 업종에서 활용 의지를 보이고 있다. 이러한 상황에서 안전성이 결여된 전자화폐 시스템의 사용은 사회적으로 큰 부작용을 발생시킬 수 있다.

본 논문에서 제안한 전자화폐 프로토콜은 상품을 주문 처리하는 상황에서 이용자와 상점간의 대금지불 처리과정에 초점을 맞춰, 영수증 부재로 인해 발생할 수 있는 문제를 해결하였다. 이로써 이용자와 상점간의 영수증 부재로 인한 논쟁을 미연에 방지함으로써 기존 전자화폐 프로토콜에 안전성을 보강하였다

그러나 상점에서 처리되어야 할 작업의 양이 증가됨으로써 처리시간이 지연되고 카드가 저장해야 하는 정보의 양이 많아지는 결과를 가져온다. 따라서 좀 더 안전하면서 빠른 서명 및 확인 방법(예를 들어, 타원곡선 암호[11])을 도입한 새로운 전자화폐 시스템의 개발에 대한 추가 연구가 필요하다.

참고문헌

[1] 김지홍, 송유진, 이만영, 이임영, "전자상거래 보안 기술", 생능출판사, 2000

[2] 박현동, 이은성, 송상헌, 강신각, 박정수, 류재철, "안전한 인터넷 전자지불 프로토콜의 설계 및 구현", 한국정보처리학회 논문지 제 6 권 제 8 호, 1999

[3] 송유진, 주재훈, "전자화폐(전자상거래 보안 응용)", 동국대학교 출판부, 2001

[4] "Ecash", DigiCash, Inc. http://www.digicash.com

[5] "NetCash", http://www.isi.edu/gost/info/NetCash/

[6] 장활식, 이정영, 유호진 정지숙, "전자지불 시스템의 현황과 발전과제"

[7] "Mondex", http://www.mondex.com

[8] "VisaCash" http://www.visacash.co.kr"

[9] David Chaum, Amos Flat, Moni Naor, "Untraceable Electronic Cash", Proceedings of Crypto '88, Sprigner-Verlag, pages 319-327.

[10] Stefan Brands, "Untraceable off-line Cash in Wallets with Observers", Proceedings of Crypto '93, Springer-Verlag, pages, 302-318.

[11] Aleksander Jurisic, Alfred J.Menezes, "Elliptic Curves and Cryptography", http://www.rsa.com