상호 인증이 가능한 IC카드형 전자화폐 관한 연구

하남수, 천인국, 홍인식
순천향대학교 정보기술공학부

A Study on IC Card Electronic Cash with Mutual Authentication

Nam-Su Ha, In-Gook Chun, In-Sik Hong
Division of Information Technology Engineering, Soonchunhyang University

요 약

인터넷상에서 전자상거래의 활성화로 인한 구매수단의 변화로 지불수단에 대한 많은 연구가 이루어지고 있다. 이에 지불수단의 근본적인 개념의 변화가 필요하다. 이에 대해 유력한 수단으로서 전자화폐 시스템은 크게 네트워크형과 IC카드형으로 나누어 질 수 있다. 본 논문에서는 현재 현물화폐의 대안으로 여겨지는 기존의 오프라인 IC카드형의 전자화폐 시스템에 대하여 연구하였고 이에 대하여 상호 인증 방식을 첨가한 새로운 프로토콜을 제안하였다.

1. 서론

PC의 보급과 인터넷의 보급은 전자상거래의 확산의 원인으로 작용하였고 지불수단인 전자화폐의 필요성이 대두하게 되었다. 일반적으로 전자화폐란 금속화폐나 지폐를 대신하여 지금까지 실물로 존재하던 화폐를 디지털 형태의 정보로 바꾼 것을 말한다. 이에 기존 화폐의 기본 기능인 가치척도의 기능, 지급수단의 기능에 대한 근본적인 변화가 초래된다. 이것은 또한 실물화폐가 갖고 있는 익명성, 상대성, 유통성등을 그대로 수용하고 더불어 디지털 정보화에 따라 발생하는 여러 장점들을 갖고 있다. 전자화폐 시스템은 크게 네트워크형과 IC카드형으로 나누어 질 수 있다. IC카드형 전자화폐는 네트워크형의 전자화폐보다 더욱 보안성이 강하며, 프라이버시를 제공하게된다. 또한 IC카드는 마이크로칩을 내장하여 보다 많은 정보 처리가 가능하여 스마트 카드라고도 불리운다. 이 후로는 IC카드형 전자화폐를 스마트 카드형 전자화폐라 부르겠다. 스마트 카드형 전자화폐는 현존하는 전자화폐 시스템 중에서 기본적인 요구사항 외에 편리성과 신뢰성을 가장 잘 충족시키고 있다.

본 연구는 정보통신부의 대학 S/W연구 센터 지원 사업에 의해 수행된 것임.

전자화폐의 기본 프로토콜은 그림 1과 같게되며 각 개체간 접근방식과 이에 따른 인증 방식을 첨가함으로써 프로토콜은 형성되게된다.

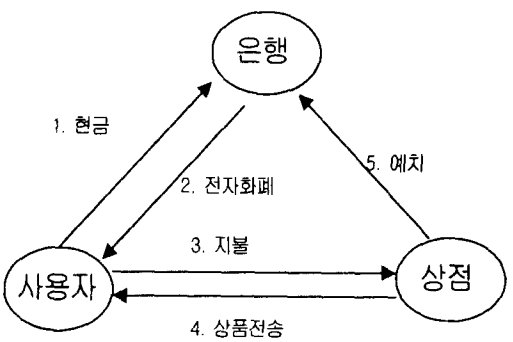

그림 1. 기본 프로토콜

스마트 카드형 전자화폐인 경우 물리적인 보안성(tamper-resistant) 외에 암호학적 가정을 통해 보안성을 가지게되며, 이러한 가정을 통해 오프라인 시스템을 구현하게된다. 본 논문에서는 기존 S.Brands의 방식[3]에서 취약한 부분이라고 할 수 있는 은행과 사용자 서로간의 상호 인증성 확보를 위해 변형된 S/key one-time password 방식[8]을 적용하였다. 먼

저, 2장에서는 전자화폐 시스템의 요구사항에 대해 소개하고, 3장에서는 기존방식에 비해 뛰어난 상호 인증성을 가진 프로토콜을 제안하였고, 4장에서는 제안논문의 유효성에 대하여 소개할 것이고, 5장의 결론에서는 향후의 연구과제를 제시한다.

2. 전자화폐 시스템의 요구사항

전자화폐 시스템의 구현을 위해서는 다양한 요구사항이 필요하다. 본 장에서는 전자화폐 시스템의 요구사항에 대해서 간략히 살펴보겠다.

2.1 기본 요구 조건

1) 안전성: 물리적 안전성, 논리적 안전성
2) 이중사용방지: 사후검출, 사전검출
3) 프라이버시: 불추적성, 불연계성
4) 오프라인성

2.2 부가 요구 조건

1) 전자수표
2) 분할성
3) n회 사용가능성

3.3 안전성 측면

1) 디지털 정보화
2) 재사용 불가성
3) 익명성
4) 오프라인성
5) 양도가능성
6) 분할 이용 가능성
7) 부정 사용자의 익명성 취소 가능성
8) 간편성, 효율성, 원거리 이전가능성

3. 제안 방식

스마트 카드형 전자화폐 구현 시 요구 사항으로는 기본적인 물리적 보안성을 위해 카드 자체의 성능 향상과 분실 시 악용방지와 분해 시 회로 난해함이 필요하다. 본 논문은 스마트 카드형 전자화폐 시스템에서 요구하는 기능뿐만 아니라 이산대수의 문제에 근거한 Schnorr 서명 방식[7]을 사용하여 보안성을 확실하게 하였고, 전자화폐 인출 단계에서 은행과 사용자 상호간의 인증을 위하여 변형된 S/key one-time password방식[8]을 사용하였다.

3.1 시스템 파라미터

다음은 각 개체에 대한 심볼을 나타낸다.

B: 은행, U_i: 사용자, S_j: 상점,
C_i: 사용자의 컴퓨터, T_i: 스마트 카드

1) 은행
- x, y ∈ Zq를 선택한다.
- g_0 ∈ Gq를 선택한다.
- $h=g_0^x$, $g_1 = g_0^y$를 생성한다.
- (n_B, e_B, d_B): 은행의 RSA 파라미터
- H(·), h(·)를 정의한다.
- accountDB: 사용자의 정보를 저장한다.
- depositDB: 지불 영수증과 관련된 정보를 저장한다.

2) 사용자
- g ∈ GF(p): 원시원
- $I = g^s \bmod p$: 사용자 식별 번호
- (n_A, e_A, d_A): 사용자의 RSA 파라미터
- $ID_A = g^{d_A} \bmod p$: 사용자의 식별자
- $S = ID_A||res||(h(ID_A||res))^{d_A} \bmod n_A$

  여기서 $res = E_{k'}(H_N(ID_A))$이다.
- BLC(Bank License Candidate)

  : 전자면허를 발급받기 위하여 사용자가 생성하여 보내는 후보이다. 다음은 BLC의 내용이고, r_1은 랜덤하게 선택하는 은닉 파라미터이다.

  $BLC = r_1^{e_B} \cdot H(I||X_N) \bmod n_B$
- BL: 전자면허

3.2 계좌 개설

1) 은행
- $x_i \in Z_q$, $I_i = x + yx_i \bmod q$

  사용자의 식별번호 I_i는 accountDB에 사용자의 다른 정보와 함께 저장되고, 타인이 사용자의 balance를 수정하거나 식별번호 빼내는 행위와 같은 문제에 대하여 은행은 적절한 보안성을 유지해야한다.
- 사용자에게 스마트 카드를 발행한다.

: g_1, x_i 와 $h_i = g_1^{x_i}$를 생성한다.
: 수행코드: 프로토콜 상에서의 코드이다.
: counter: balance에 의해 표기된다.

다음은 은행이 발행한 스마트 카드의 내용이다.

$T_i = g_1||x_i||code||balance||Info||BL()$

여기서, BL()은 전자 면허를 위한 항이다.

2) 사용자
- h_i, g_0, g_1, h, G_q와 H(·)에 대한 설명을 사용자 컴퓨터에 저장한다.
- balance의 복사본 트랙을 사용자 컴퓨터에 저장한다.

다음은 사용자 컴퓨터에 저장되는 내용이다.

$C_i = hi||g_0||g_1||h||G_q\_des||H(\cdot)\_des||BL()||$ balance_copy

3.3 인출

이 단계는 스마트 카드와 은행 사이에서 수행되고 인출 금액에 대한 기존 방식[3]에 상호간의 인증을 위해 변형된 S/key one-time password 방식과 익명성

을 위한 은닉서명 방식[1]을 사용한다. 원하는 금액 인출 시 balance가 업데이트된다. 여기서 seq는 사용자의 replay attack을 막는 효과가 있다.

1) 사용자

· H, ID_A, N(횟수)를 선택한 후 은행에 전송한다.

2) 은행

· 사용자의 비밀 정보 X_{N+1}을 생성한 후, X_{N+1}과 N+1을 저장한다.

$X_1 = H(ID_A)$, $X_2 = H(X_1)$, ... , $X_{N+1} = H(X_N)$

· 랜덤값 R, challenge값 chal를 생성 후 사용자 컴퓨터에 전송한다. 다음은 chal의 내용이다.

$chal = (N \| R \oplus X_{N+1} \| E_R(X_{N+1}))$

3) 사용자

· $H_N(ID_A)$와 $H_{N+1}(ID_A)$ 그리고 R'을 계산한 후 은행에 대한 인증 과정을 수행한다.

$R' = (H_{N+1}(ID_A) \oplus R \oplus X_{N+1})$

$D_{R'}(E_R(X_{N+1})) \stackrel{?}{=} H_{N+1}(ID_A)$

· 검증이 올바르면 I, res, S와 BLC를 계산하여 I는 공개하고, res와 BLC를 은행에 전송한다.

4) 은행

· 은행은 다음과 같이 사용자 컴퓨터의 인증 과정을 수행하고, N+1을 N으로, X_{N+1}을 $X_N = H_N(p)$로 갱신 한 후 BLC에 은행의 서명을 첨가하여 사용자 컴퓨터에 전송한다.

$D_{R'}(E_{R'}(H_N(ID_A))) \stackrel{?}{=} H_N(ID_A)$

$H(H_N(ID_A)) \stackrel{?}{=} X_{N+1}(ID_A)$

· 사용자의 인증 과정이 이루어지면 실제적인 인출 단계를 시행한다.

balance' = balance' - amount

seq = seq + 1

v = f(z, seq, amount)

여기서 z는 사전에 은행과 사용자가 공유하는 비밀키이고, amount는 사용자가 실제로 인출하려는 금액을 말하며, seq는 인출 시 무조건 1증가하게 된다.

5) 사용자

· 사용자는 은행이 서명한 BLC로부터 BL을 추출한다.

$BL = r_1 H(I \| X_N)^{d_B} \bmod n_B / r_1$

$= H(I \| X_N)^{d_B} \bmod n_B$

· $v \stackrel{?}{=} f(z, seq, amount)$인지를 검증한 후 seq = seq + 1과 balance = balance + amount를 각각 계산한다.

BL과 balance 복사 본을 저장한 후, BL과 balance를 스마트 카드에 전송한다.

3.4 확인증 발행

확인증 발행 단계는 인출 금액에 대한 은행의 서명을 포함한다.

Off-line pre-processing

이 단계는 확인증 발행을 위한 사전 단계이고, 스마트 카드와 사용자 컴퓨터 사이에서 수행된다.

1) 스마트 카드

· 랜덤값 w_i , $a_i = g_1^{w_i}$를 생성한다.

· 컴퓨터에 a_i를 전송한다.

· 지불 시 사용하기 위해 w_i를 내부에 저장한다.

2) 컴퓨터

· 랜덤값 α, β, γ, δ, ε를 생성한다.

· $h'_i = h_i \cdot g_0^{\alpha}$ 와 $a'_i = a_i \cdot g_1^{\beta} \cdot g_0^{\gamma}$ 그리고 $temp = g_0^{\delta}(h \cdot h_i)^{\varepsilon}$를 계산한다.

· 지불 시 사용하기 위해 h'_i, a'_i, α, β, γ를 저장하고 temp, δ, ε를 저장한다.

On-line actual-processing

이 단계는 확인증 발행의 실제적 단계이고, 은행과 사용자 컴퓨터 사이에서 수행된다.

1) 은행

· 랜덤값 w, $a = g_0^w$를 생성하여 a를 사용자 컴퓨터에 전송한다.

2) 사용자

· $c' = H(h'_i, a'_i, atemp)$를 계산한 후 $c = c' + \varepsilon \bmod q$를 생성한 후 c를 은행에 전송한다.

3) 은행

· $r = cI_i + w \bmod q$을 계산한 후 r을 사용자 컴퓨터에 전송

4) 사용자

· $g_0^r(hh_i)^{-c} \stackrel{?}{=} a$를 검증한 후 $r' = r + c'\alpha + \delta \bmod q$를 계산하여 r'을 저장하고, temp, δ, ε를 삭제한다.

3.5 지불

Off-line pre-processing

이 단계는 지불이 이루어지기 위한 사전 단계로 사용자의 컴퓨터와 스마트 카드 사이에서 수행된다.

1) 컴퓨터

· $(h'_i, a'_i, spec)$을 스마트 카드에 전송한다.

spec=(amount||time||date||account(S_i)||Info)

2) 스마트 카드

· w_i가 메모리에 존재하고, balance ≥ amount를 만족하는지를 확인한다.

· $d=H(h'_i, a'_i, spec)$과 $r_{i1}=dx_i + w_i \bmod q$를 각각 계산한다.

· balance = balance - amount를 계산하고, 메모리로부터 w_i를 삭제한 후 r_{i1}를 사용자 컴퓨터에 전송한다.

3) 컴퓨터

이 단계는 상점의 도움 없이 사용자 컴퓨터가 spec을 결정할 수 있다는 것을 의미한다.

· $d=H(h'_i, a'_i, spec)$를 계산하고, $g_1 r_{i1}(h'_i)^{-d} \stackrel{?}{=} a$인지를 검증한 후, $r'_{i1}=r_{i1}+\beta \bmod q$와 $r_{i2}=d\alpha+\gamma \bmod q$를 각각 계산한다.

On-line actual processing

이 단계는 사용자와 상점 사이에 실질적인 지불처리를 수행한다.

1) 컴퓨터

· h'_i, (c', r'), (a'_i, r'_{i1}, r_{i2}), BL을 상점에 전송한다.

2) 상점

· $d = H(h'_i, a'_i, spec, BL)$를 계산한다.

· $c' \stackrel{?}{=} (h'_i, a'_i, g_0^{r'}(hh'_i)^{-c}, BL)$ 와 $g_1^{r'_{i1}} g_0^{r_{i2}}(h'_i)^{-d} \stackrel{?}{=} a'_i$인지를 검증한 후 전송된 정보를 받아들인다.

3.6 예치

상점은 거래 내역 H를 은행에 전송한다. 은행이 H를 전송 받으면 전자화폐 및 전자면허의 유효성을 확인하고 은행의 DB를 이용하여 이중 사용 여부를 확인한다.

1) 상점

· 지불영수증 = h'_i, (c', r'), (a'_i, r'_{i1}, r_{i2}), BL, spec을 은행에 보낸다.

2) 은행

· $d \stackrel{?}{=} H(h'_i, a'_i, spec, BL)$인지를 검증한 후, 은행의 depositDB에 $h_{DB}(h'_i, c', r', BL)$이 저장되어 있는지 찾는다. 만약 $h_{DB}(h'_i, c', r', BL)$가 저장되어 있지 않고, 지불 영수증의 검증식이 올바르면 상점의 depositDB에 $(h_{DB}(h'_i, c', r', BL)$, spec, d, $r'_{i1})$을 저장한 후, 상점의 account에 amount를 더해준다. 그렇지 않고 $h_{DB}(h'_i, c', r', BL)$가 저장되어 있으면 상점이 이중 예치를 시도하는 것으로 간주한다.

4. 제안 방식의 유효성

기존에 S.Brands가 제안한 스마트 카드형 전자화폐 시스템은 사용자가 원하는 금액 인출 시 사용자와 은행간의 인증 문제가 발생할 소지가 있다. 이에 본 제안 방식은 변형된 S/key one-time password[8] 방식을 사용하여 상호간의 인증을 확실히 하는데 중점을 두었다.

5. 결론

서론에서 소개하였듯이 전자상거래의 활성화로 인한 전자화폐의 필요성이 대두되었다. 그 중에서도 현물화폐와 가장 유사한 스마트 카드 시스템은 유력한 대안으로 떠올랐다. 본 논문에서 소개한 시스템의 주안점은 인출 단계에서 은행과 사용자 쌍방간의 인증을 위하여 변형된 S/Key one-time password 방식을 첨가한 부분이다. 그리고 이산대수에 기반한 Schnorr의 서명 방식을 선택하여 보안성을 좀더 확보하게 하였고, 지불 시 오프라인이 가능하게 구현하였다. 보다 효율적인 상호간 인증 기술에 대해서는 후속 연구가 필요할 것이다.

[참고문헌]

[1] D.Chaum,"Blind Signautures for Untraceable Payments",Advances in Cryptography, Crypto'82, pp 199-203, 1983

[2] H.Antwerpen,"Electronic Cash", Master's thesis Univ. Eindhoven'1990

[3] S.Brands,"Off-Line Cash Transfer by Smart Cards",CWI'1994

[4] S.Brands,"Untraceable Off-Line Cash in Wallets with Observers",Crypto'1993

[5] J.Bos and D.Chaum,"Smart Cash: a practical electronic payment system",Technical Report CS-R9035, CWI'1990

[6] M.Stadler, J.M.Piveteau and J.Camenisch,"Fair Blind Signatures",In Advances in Cryptology, Proc, of Eurocrypto'1995, pp209-219, 1995

[7] C.Schnorr,"Efficient Signature Generation by Smart Cards", Journal of Cryptology, Vol. 4, No 3, (1991), pp 161-174, 1991

[8] 김기현, 은유진, 박정호, 고승철,"변형 일회용 패스워드 시스템 제안",제10회 정보보호와 암호에 관한 학술 대회(WISC'1998), pp75-92, 1998