KCDSA를 이용한 분할가능 및 익명성 제어를 갖는 전자화폐 시스템

장석철[U] 이임영
순천향대학교 정보기술공학부
scjang@cse.sch.ac.kr, imylee@sch.ac.kr

An Electronic Cash System with Divisible and Anonymity Control using the KCDSA

Seok-Cheol Jang[U] Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang University

요 약

전자상거래가 활발하게 이루어짐으로서 지불수단에 대한 관심이 증가되고 있다. 또한 지불 시스템에 대한 수많은 연구가 진행되고 있다. 특히 사용자의 사생활을 보호하기 위해 익명성을 제공하는 시스템과 이로 인해 발생하는 문제점들을 해결하기 위해 익명성 제어에 관련된 전자화폐 시스템이 연구되고 있다. 따라서 본 논문에서는 국내 전자서명 표준인 KCDSA를 기반으로 하여 익명성을 유지하며 실물화폐에서 갖지 못한 효율적이고 편리한 분할성 기능과 필요시 신뢰기관의 도움으로 익명성을 제어할 수 있는 새로운 전자화폐 시스템을 제안한다.

1. 서론

이제는 제2의 화폐혁명인 전자화폐 시대가 열리고 있다. 보이지 않는 돈을 가상의 공간에서 자유롭게 사용할 수 있는 화폐가 전자화폐이다. 특히 눈부시게 발전하고 있는 디지털 기술, 인터넷의 급부상과 컴퓨터의 급속한 보급으로 인한 전자상거래의 발전은 기존 시장의 개념을 네트워크 상에서의 인터넷 쇼핑몰 개념으로 바뀌게 했다. 따라서 인터넷 쇼핑몰을 이용하여 고객은 편리하게 시간을 절약하면서 물건을 구매할 수 있다. 현재 많이 이용되고 있는 신용카드를 이용한 지불 시스템은 사용자의 사생활 침해 및 수수료가 높다는 점이 지불수단으로 적합하지 않다. 따라서 이러한 문제를 해결하기 위해 소액거래에 편리한 전자화폐의 많은 연구가 진행되고 있다.

일반적으로 전자화폐 프로토콜은 사용자, 상점 그리고 은행의 세 개체간의 거래에 의해 이루어지며 인출단계, 지불단계, 예치단계의 기본적인 프로토콜을 가지고 있다. 이러한 단계에서 사용자의 사생활(privacy)을 보호하기 위해 사용자와 사용자의 구입 내용 및 지불 내용을 연계시키지 않고 인출 단계와 지불 단계가 연결되지 않도록 기본적으로 익명성을 제공하고 있다. 또한 전자화폐는 기존의 실물 화폐가 가지고 있는 기능뿐만 아니라 분할성, 추적성 등과 같은 새로운 기능을 추가시킴으로서 그 유용성을 증대시킬 수가 있다. 그러나 그 편리함과 유용성에도 불구하고 불법적인 범죄 행위들에 이용될 수 있으며 이 때 이와 같은 범죄행위를 한 사용자와 그 돈에 대한 행방을 찾을 수가 없다.

따라서 본 논문에서는 위에서 언급한 문제점을 해결하기 위해 전자화폐의 기본적인 요구 조건을 만족하며, 또한 익명성 제공으로 인한 범죄에의 이용을 방지하기 위해 익명성을 제어하는 전자화폐 프로토콜을 제안한다.

2. 제안 방식

본 제안 방식은 전자화폐 프로토콜에 적용할 수 있도록 국내 전자서명 표준인 KCDSA를 변형한 복원형 은닉 서명 방식을 적용하여 전자화폐를 발행받고[1], 해쉬 함수에 기반한 계층적 구조 테이블을 이용한 화폐의 분할 사용[2]~[5], Schnorr의 인증 기법[6]을 이용한 이중 사용 방지와 불법 사용시 사용자 신원 노출 등의 특성을 만족시켜 주고 있다. 또한 이산 대수 문제를 이용한 동전 추적기능과 ElGamal 암호 기법을 이용한 사용자 추적기능을 제공하여 사용자의 익명성을 제어함으로써 전자화폐의 불법적 용도로서의 사용을 방지해 주고 있다[7]. 그리고 전자면허 발행시 은행과 사용자 인증을 위해 변형된 S/Key one-time password 방식[8]을 사용함으로서 전자면허를 단일항으로 구성하고 있다.

본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임.

2.1 시스템 파라메타

가. 사용자

- p : 사용자가 생성한 소수
- g_1, g_2, g_3 : GF(p)상의 원시원
- (n_A, e_A, d_A) : 사용자는 RSA 파라메타로서 p_A와 q_A를 선택하고, 공개키 $n_A(=p_A \times q_A)$, e_A와 비밀키 d_A를 생성한다. 이때, $0 < n_A \le p-1$ 이다.
- $ID_A \equiv g_1^{d_A} \bmod p$: 사용자가 생성한 식별자
- S : $ID_A \| response \| (H(ID_A \| response))^{d_A} \bmod n_A$
  여기서, $response = E_{R'}(H_N(ID_A))$
- $I \equiv g_1^{r} \bmod p$
- H : 전자면허 발행시 사용되는 일방향 해쉬 함수
- f_1, f_2 : 계층적 구조 테이블 노드 구성시 사용되는 일방향 해쉬 함수
- $BLC \equiv r_1^{e_B} \cdot H(I \| X_N) \bmod n_B$: 전자면허 후보
- $EC = \{C \| A'_1 \| A'_2 \| sign_A(C \| A'_1 \| A'_2)\}$: 전자화폐

나. 은행

- (n_B, e_B, d_B) : 은행의 전자면허용 RSA 파라메타로서, n_B, e_B는 공개키이고 d_B는 비밀키이다.
- R : 사용자와 은행 상호 인증 과정에서 사용되는 랜덤값.

다. 신뢰기관

- $X_T \in Z_p^*$: 신뢰기관의 비밀키
- $y_T \equiv g_2^{X_T} \bmod p$: 신뢰기관의 공개키

2.2 전자면허 발행 단계

과정 1 : 사용자는 H와 ID_A 그리고 해싱회수 N을 선택하고 이를 은행에 전송한다.

과정 2 : 은행은 사용자의 비밀정보(ID_A)를 $N+1$번 해싱한 $X_{N+1}(= H_{N+1}(ID_A))$을 생성하고 X_{N+1}과 $N+1$만을 저장한다. $X_1 = H(ID_A), X_2 = H(X_1), \cdots, X_{N+1} = H(X_N)$

과정 3 : 은행은 난수 R을 선택하고 다음과 같이 *challenge* 값을 생성하여 사용자에게 전송한다.

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

이때, $E_R(X_{N+1})$은 X_{N+1}을 R을 키로 사용하여 암호화한 것이다.

과정 4 : 사용자는 $H_N(ID_A)(=X_N)$와 $H_{N+1}(ID_A)(=X_{N+1})$을 계산하고 은행이 보내 온 *challenge*로부터 R을 추출하고 이로부터 R'을 계산하여 은행 인증 과정을 수행한다.

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

만약 인증과정이 유효하지 않다면 이 프로토콜을 종료하고, 은행의 인증 과정이 성립되면 *response*, S, I와 전자면허 후보 BLC값을 계산하여 I값은 공개하고 *response*와 BLC를 은행에 전송한다.

과정 5 : 은행은 사용자 인증과정을 다음과 같이 수행한다. 이때 은행은 사용자가 보내온 *response*값을 자신이 가지고 있는 R값을 이용해서 복호화하여 $H_{N+1}(ID_A)$을 구한다. 그리고 이 값이 자신의 X_{N+1}과 비교한다.

$$D_R(E_{R'}(H_N(ID_A))) \stackrel{?}{=} H_N(ID_A), \ H(H_N(ID_A)) \stackrel{?}{=} X_{N+1}$$

인증과정이 유효하다면 사용자 관련 저장 정보를 $N+1$에서 N으로, X_{N+1}을 $X_N = H_N(ID_A)$로 갱신한다. 그리고 BLC에 은행의 서명을 하여 사용자에게 전송한다.

$$(BLC)^{d_B} \equiv (r_1^{e_B} \cdot H(I \| X_N) \bmod n_B)^{d_B} \equiv r_1 \cdot H(I \| X_N)^{d_B} \bmod n_B$$

과정 6 : 사용자는 은행이 서명한 BLC로부터 전자면허 BL을 추출한다.

$$BL \equiv [r_1 \cdot H(I \| X_N)^{d_B} \bmod n_B] \ / r_1 \equiv H(I \| X_N)^{d_B} \bmod n_B$$

2.3 전자화폐 발행 단계

과정 1 : 사용자는 $v \in \{1, \cdots, p-1\}$를 랜덤하게 선택하고 A'_1과 A'_2를 생성하여 은행에 전송한다.

$$A'_1 \equiv y_T^v \bmod p, \ A'_2 \equiv I g_2 g_3^{v'} \bmod p$$

과정 2 : 은행은 A'_1, A'_2를 올바르게 생성하였는지 확인한 뒤 $k' \in Z_q$를 랜덤하게 선택하여 r'을 계산하여 사용자에게 전송한다.

$$\log_{g_3}(A'_2 / I g_2) \stackrel{?}{=} \log_{A'_1} y_T \ , \ r' = g^{k'} \bmod p$$

과정 3 : 사용자는 랜덤하게 은닉인자 $\alpha \in Z_q$와 $\beta \in Z_q$를 선택하여 r과 은닉된 값 m'을 계산하여 은행에게 전달한다.

$$m = BL \ , \ r = m g^{\alpha} r'^{\beta} \pmod p \ , \ m' = r \beta^{-1} \pmod q$$

과정 4 : 은행은 다음과 같이 서명을 한 s'을 사용자에게 보낸다.

$$H = h(Z \| m') \ , \ E = m' + H \bmod q \ , \ s' = xE + k' \pmod q$$

과정 5 : 사용자는 은행으로부터 받은 s'을 이용하여 s를 구하고 이를 이용하여 검증을 하면된다.

$$H' = h(z \| m') \ , \ s = s'\beta + \alpha \pmod q \ , \ m \stackrel{?}{=} g^{-s} y^{r' \cdot \beta H} r \pmod p$$

검증이 성립하면 실제 사용될 전자화폐를 다음과 같이 구성한다.

$$EC = \{(r,s) \| A'_1 \| A'_2 \| Sign_A((r,s) \| A'_1 \| A'_2)\}$$

2.4 전자화폐 지불 단계

과정 1 : 사용자는 지불하기 원하는 금액에 해당하는 노드 값(V_{00}, V_{010})과 (X_{00}, X_{010})를 계산한 뒤 EC, BL, A, A_1, A_2, A_3과 함께 상점에 전송한다.(이때, A_3는 선택사항이다.)

$$A = (A'_2)^v \bmod p, \ A_1 \equiv g_2^v \bmod p, \ A_2 \equiv g_1^{V_{00}} \bmod p$$

$$V_{00} \equiv V_0 \cdot f_1(V_0) \bmod p, \ V_{010} \equiv V_{01} \cdot f_1(V_{01}) \bmod p$$

$$X_{00} = g_1^{V_{00}} \bmod p \ , \ X_{010} = g_1^{V_{010}} \bmod p$$

과정 2 : 상점은 전자화폐 EC에 있는 사용자 서명을 확인한 뒤 V_{00}, V_{010}과 A, A_1, A_2를 확인한다.

$$V_{00} \stackrel{?}{\equiv} V_0 \cdot f_1(V_0) \bmod p \ ,$$

$$V_{010} \stackrel{?}{\equiv} V_{01} \cdot f_1(V_{01}) \bmod p \ , \quad A \stackrel{?}{\equiv} A_1 \cdot A_2 \cdot g_3 \bmod p$$

그리고 나서 난수 R_{00}, $R_{010} \in \{1, \cdots, p-2\}$를 생성하여 사용자에게 전송한다.

과정 3 : R_{00}, R_{010}를 이용하여 사용자는 다음의 Y_{00}, Y_{010}를 계산하여 상점에 전송한다.

$$Y_{00} \equiv V_{00} + R_{00} \cdot S \bmod p-1 \ , \ Y_{010} \equiv V_{010} + R_{010} \cdot S \bmod p-1$$

과정 4 : 상점은 Y_{00}와 Y_{010}에 대한 다음식이 성립하는지 확인하여, 만족하면 V_{00}, V_{010}를 인증하여 고객의 전자화폐 ₩75을 받아들인다.

$$g_1^{Y_{00}} \stackrel{?}{\equiv} X_{00}\cdot(I)^{R_{00}} \bmod p, \quad g_1^{Y_{010}} \stackrel{?}{\equiv} X_{010}\cdot(I)^{R_{010}} \bmod p$$

2.5 예치단계

사용자가 지불한 전자화폐 EC를 전송하기 위해서 상점은 거래내역서 T를 은행에 전송한다. 은행이 T를 전송 받으면 전자화폐 및 전자면허의 유효성을 확인하고 은행의 DB를 이용하여 이중 사용 여부를 확인한다.

$$T=(I,p,g_1,g_2,g_3,V_{00},V_{010},R_{00},R_{010},Y_{00},Y_{010},$$
$$O_A(=(A_1,A_3)),BL,EC)$$

3. 제안 방식의 분석

3.1 KCDSA 은닉 서명

기존 KCDSA는 이산대수 문제의 어려움에 기반을 둔 전자서명 알고리즘으로서, 메시지 부가형 전자서명 방식이다. 하지만 이 서명 방식을 전자화폐에 그대로 적용하기는 곤란하다. 그래서 은닉성을 추가하고, 부가형 서명 방식을 전자화폐에서 사용할 수 있는 메시지 복원형 전자서명 방식으로 변형하였다. KCDSA는 우리나라에서 개발한 전자서명 알고리즘으로서 국내 및 국제 특허에 저촉되지 않고 국내 표준이므로 응용 프로토콜에 쉽게 적용 가능하다.

3.2 안전성

가. 사용된 노드의 상·하위 노드 사용시 신원 검출

$Y_{00}\equiv V_{00}+R_{00}\cdot S \bmod p-1$, $Y_{000}\equiv V_{000}+R_{000}\cdot S \bmod p-1$ 에서

$V_{000}\equiv V_{00}\cdot f_1(V_{00}) \bmod p \equiv V_{00}\cdot f_1(C\cdot f_1(C)) \bmod p$ 이므로

이로부터,

$$Y_{00}\cdot f_1(V_{00})-Y_{000}\equiv(V_{00}\cdot f_1(V_{00})+R_{00}\cdot f_1(V_{00})\cdot S)-$$
$$(V_{00}\cdot f_1(V_{00})+R_{000}\cdot S) \bmod p\equiv(R_{00}\cdot f_1(V_{00})-R_{000})\cdot S$$

$\therefore S\equiv(Y_{000}-Y_{00}\cdot f_1(V_{00}))/(R_{000}-R_{00}\cdot f_1(X_{00})) \bmod p-1$ 와 같이 S가 구해지고 이로부터 ID_A가 구해진다.

나. 같은 동전의 이중 사용시 신원 검출

상점은 사용자가 보내온 $V_{00}, Y_{00}, Y'_{00}, X_{00}, X'_{00}$로부터

$$Y_{00}-Y'_{00}\equiv(R_{00}-R'_{00})\cdot S \bmod p-1$$

$\therefore S\equiv(Y_{00}-Y'_{00})/(R_{00}-R'_{00}) \bmod p-1$ 을 구할 수 있다.

이와 같이 S가 구해지고 이로부터 ID_A가 구해진다.

3.3 익명성 제어

익명성 제어는 익명성 조절 파라메타에 의해 제공되며 선택적으로 익명성을 취소할 수 있다.

가. 화폐 추적

과정 1 : 은행은 사용자가 제시한 인출 사본 중 A'_1을 신뢰기관에게 제공한다.

과정 2 : 신뢰기관은 A'_1으로부터 A_1을 계산해낸다.

$$(A'_1)^{X_T^{-1}} \equiv (y_T^v)^{X_T^{-1}}\equiv g_2^{X_T\cdot v\cdot X_T^{-1}} \equiv g_2^v \equiv A_1$$

과정 3 : 신뢰기관은 A_1을 은행에게 전송한다.

이때 신뢰기관이 전송해 준 A_1을 사용자가 생성하여 지불 단계에서 상점에 제공하는 A_1과 연결시킴으로서 물품 구입 단계 전에 지불과 상관없이 추적 기능을 제공한다.

나. 사용자 추적

과정 1 : 은행은 상점이 예치한 거래 내역서로부터 $O_A(=A_1,A_3)$ 를 신뢰기관에 전송한다.

과정 2 : 신뢰기관은 O_A에 있는 A_1과 A_3로부터 $A'_3\equiv ID_A^{X_T^{-1}}\cdot g_2^v \bmod p$을 구하고, 다시 ID_A를 계산한다.

$$A_3'\equiv A_3^{X_T^{-1}} \bmod p \equiv ID_A^{X_T^{-1}}\cdot g_2^v \bmod p$$
$$A_3'/A_1 \bmod p \equiv ID_A^{X_T^{-1}}\cdot g_2^v/g_2^v \bmod p \equiv ID_A^{X_T^{-1}} \bmod p$$
$$\therefore ID_A=(ID_A^{X_T^{-1}})^{X_T \bmod(p-1)} \bmod p$$

과정 3 : 신뢰기관은 O_A와 ID_A에 자신의 서명을 한 후 은행의 공개키로 암호화하여 은행에 전송한다.

$$E_{K_B^u}(O_A\|ID_A\|sign_T(O_A\|ID_A))$$

4. 결론

인터넷에서 이루어지는 전자상거래에서 가장 중요한 요소중에 하나가 전자화폐이다. 초기에 전자화폐는 익명성에 중점을 두고 연구되었지만 여러 가지 문제점으로인해 새로운 요구조건인 익명성 제어가 등장하게 되었다.

또한 기존의 화폐에서는 볼 수 없는 기능으로 일정한 가치를 가지고 있는 전자화폐는 그 금액의 크기만큼 자유롭게 분할되어 사용될 수 있어야 한다.

따라서 본 논문에서는 익명성이 가지고 오는 문제점과 익명성제어로 인해 일어날 수 있는 문제점을 해결하고, 전자화폐를 자유롭게 사용할 수 있는 분할성 기능을 추가하였다. 또한 국내 전자서명 표준 알고리즘인 KCDSA를 전자화폐 프로토콜에 적용할 수 있도록 은닉 KCDSA 서명 방식으로 변형하여 이를 적용한 전자화폐 시스템을 제안하였다. 향후 전자화폐가 현재보다 발전하기 위해서는 연구에만 전념하지 말고 연구를 통해 제안된 시스템을 실질적으로 구현하는 방향으로 연구가 진행되었으면 한다.

5. 참고 문헌

[1]http://www.tta.or.kr,"부가형 전자서명 방식표준(KCDSA) - 제2부 : 확인서 이용 전자서명 알고리즘", TTA.KO-12.0001

[2] T.Okamoto and K.Ohta, "Universal Electronic Cash", In Advances in Cryptology, Crypto'91, pp324-337, 1991

[3] T.Eng and T.Okamoto, "Single-term divisible electronic coins", In Advances in Cryptology, Eurocrypto'94, Proceedings, pp313-323, 1994.

[4] T.Okamoto,"An Effieient Divisible Electronic Cash Scheme", In Advances in Cryptology, Crypto'95, pp438-451, 1995

[5] A.Chan, Y.Frankel and Y.Tsiounis, "Easy-come easy-go divisible cash", In Advances in Cryptology, Eurocrypto'98, pp561-575, 1998

[6]C.P.Schnorr,"Efficient signature generation by smart cards", Journal of Cryptology, 4(3), 161-174, 1991

[7]G.Davida, Y.Frankel, Y.Tsiounis and M.Yung, "Anonymity control in e-cash" In Proceedings of the 1st Financial Cryptography conference, 1997

[8]김기현, 은유진, 박정호, 고승철, "변형 일회용 패스워드 시스템 제안", 제 10회 정보보호와 암호에 관한 학술 대회, pp75-92, 1998

[9]오형근,이임영, "익명성제어와 화폐 분할 기능을 가지는 효율적인 전자화폐 프로토콜", 한국정보과학회, 제25권, 1999