새로운 추적 가능한 전자화폐 프로토콜에 관한 연구

오형근°, 이임영
순천향대학교 컴퓨터학부

A Study on New Traceable Electronic Cash Protocol

Hyung-Geun Oh°, Im-Yeong Lee

Department of Computer Science, College of Engineering
Soonchunhyang University

요 약

전자상거래가 새로운 상거래 시스템으로 부각되면서 전자상거래에 있어서 핵심 기술인 전자 지불 시스템에 대한 연구가 활발히 진행되고 있다. 이 중 전자화폐 시스템은 인터넷과 같이 개방된 네트워크 환경하에서 사용하기 위한 목표 시스템으로 기존의 화폐를 대신하여 사용될 것이다. 이에 본 고에서는 전자화폐의 요구 조건 및 특성에 대해 알아보고 사용자를 추적할 수 있는 새로운 프로토콜을 제안한다. 특히 제안된 방식은 전자화폐 사용자가 정당하게 화폐를 사용하였다 하더라도 법원의 허락에 의해 수탁기관과 은행의 연합으로 사용자의 신원을 검출할 수 있는 추적 가능한 전자화폐 프로토콜이다.

1. 서론

정보화가 진행되면서 상거래 패턴은 기존의 실물 시장에서 거래가 되던 것이 점차 가상 몰(Cyber Mall)상에서의 전자상거래(Electronic Commerce) 형태로 이전되어 가고 있다. 이러한 전자상거래에 있어서 가장 중요한 것은 전자 지불 시스템(Electronic Payment Systems)이며 여러 가지 전자 지불 시스템 중에서 주된 관심사가 되고 있는 것은 전자화폐 시스템(Electronic Cash Systems)이다. 사이버 캐쉬(Cyber Cash) 또는 디지털 캐쉬(Digital Cash) 등으로 불리는 전자화폐는 기존의 실물 화폐가 사이버 공간상의 상거래에서 사용되기에 부적합하기 때문에 이를 대신하여 사용되게 될 것이다 전자화폐에 대한 연구 개발은 1982년 David Chaum의 on-line형 전자화폐 시스템[1]이 처음 등장한 이래 전자화폐가 요구하는 여러 가지 조건들을 만족시키는 많은 방식들이 제안되고 있다. 이러한 전자화폐는 디지털 데이터가 가지는 특징으로 인해 편리함과 유용함에도 불구하고 많은 문제점을 내포하고 있으며 이러한 문제점을 반드시 해결하여야 한다. 최근의 전자화폐 연구 동향은 안전성 및 편리성 등의 기능을 갖춘 IC 카드형 전자화폐가 주류를 이루고 있다 또한 초기에는 개인의 프라이버시를 보호하는 데 연구의 초점을 맞추어 왔으나 현재는 여러 가지 사회·경제적인 문제점들의 제기로 말미암아 이의 해결을 위한 연구가 진행 중이다. 전자화폐는 그것이 가지고 있는 자체 특성과 사용 환경으로 인해 여러 가지 공격이 가능하며 불법적인 사용이나 범죄에의 이용 등으로 경제 활동에 큰 장애를 초래할 가능성이 많다 따라서 전자화폐 개발시에는 다음과 같은 요구조건을 반영하여야 한다.

- Independence(완전 정보화, 독립성)
- Security(보안성, 이중사용방지)
- Off-line payment(오프라인상에서의 지불)
- Transferability(가치이전성, 양도성)
- Dividability(분할성)
- Untraceability(추적불가능성, 익명성)

2. 제안 방식

본 논문에서 제안하고 있는 방식은 RSA 알고리즘[2]을 이용한 각 개체의 키 생성, 이산 대수 문제와 해쉬함수에 기반한 계층적 구조 테이블(Hierarchical Structure Table)을 이용한 전자화폐의 분할 사용, Schnorr의 인증 기법[3]을 이용한 이중 사용(Double Spending) 방지와 사용자의 신원 노출 등의 특성을 만족시키고 있다. 특히 사용자는 신원 검출 인자 P_1과 P_2를 생성하고 나중에 법원의 허가를 얻은 수탁기관은 이 P_1과 P_2 인자로부터 사용자의 신원(ID_A)을 검출하게 된다.

2.1 계층적 구조 테이블(Hierarchical Structure Table)

이 테이블에 의해 은행으로부터 받은 전자화폐는 보다 작은 금액으로 분할이 되어 사용될 수 있으며 분할된 전체 화폐 금액(EM_1, EM_2, . . . , EM_n)의 합은 초기에 은행으로부터 받은 EM과 동일하다.

계층적 구조 테이블의 tree 구조와 관련하여 전자화폐를 사용하기 위해서는 다음과 같은 규칙을 따른다.

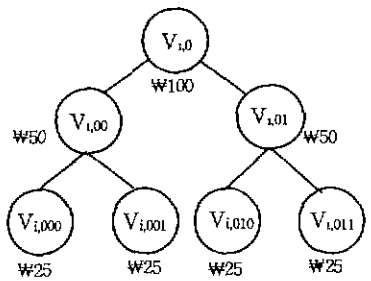
a. 노드 N에 있어서 해당 금액은 자식 노드들의 합과 같다.
b. 어떤 한 노드가 사용되면, 모든 자식 노드와 부모 노드는 사용할 수 없다
c. 어떤 노드도 한번 이상 사용될 수 없다.

각각의 노드는 다음과 같이 구해진다.

$V_{1,0} \equiv g_1^c \mod p_1$

$V_{1,00} \equiv V_{1,0} \cdot h_1(g_1^{V_{1,0}} \mod p_1)$

$V_{1,01} \equiv V_{1,0} \cdot h_2(g_1^{V_{1,0}} \mod p_1)$, . . . (for i=1, . ., K/2)



[그림 1] Hierarchical Structure Table

2.2 시스템 파라메타

가. 사용자(Alice)

사용자는 다음과 같은 시스템 파라메타를 생성한다.

- p_i : 소수, g_i : GF(p)상의 원시원
- X_A : 사용자의 비밀키
- ID_A : 은행의 계좌 번호와 연계, $ID_A = g^{X_A} \bmod p$
- BLC_i(Bank License Candidates) : 전자면허 후보들
- P_1, P_2 : 사용지 추적을 위한 factor
- f, h_1, h_2 : 일방향 해쉬 함수(one-way hash function)

나. 은행(Bank)

- (e_B, n_B, d_B) : 전자면허용 RSA 파라메타
- (e_B', n_B', d_B'), (e_B'', n_B'', d_B''), . . .
  : 전자화폐용 RSA 파라메타.

예를 들어 (e_B', n_B')은 ₩100에 해당하고 (e_B'', n_B'')은 ₩1000에 해당한다 등.

- BL(Bank License) : 전자면허

다. 수탁기관(Trustee)

- (e_T, n_T, d_T) : 신원 검출용 RSA 파라메타

2.3 전자면허 발행 단계

사용자 A는 은행으로부터 전자면허 BL을 발행 받는다. 이 전자면허는 계좌 개설시에 한번만 발행 받으며 화폐 발행을 위한 factor로써 사용이 된다. cut-and-choose 방식과 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다.

Step 1 : 사용자 A는 소수 p_i와 원시원 g_i, 그리고 랜덤한 값 r_i, a_i를 생성하고 자신의 비밀키로 ID_A를 생성한다 이를 이용하여 K개의 블라인드된 BLC_i를 은행에게 보낸다.

$$BLC_i \equiv r_i^{e_B} \cdot f(I_i \| P_i) \bmod n_B, \text{ for } 1 \le i \le K$$

여기서, $S_i \equiv ID_A \| a_i \| (g(ID_A \| a_i))^{d_A} \bmod n_A$,

$$I_i \equiv g_i^{S_i} \bmod p_i, \qquad ID_A \equiv g^{X_A} \bmod p$$

$(p \in \{p_1, p_2, \ldots, p_i\}, g \in \{g_1, g_2, \ldots, g_i\})$

Step 2 . 은행은 $U=\{i_j\}$, $1 \le i_j \le K$, for $1 \le j \le K/2$를 선택하고 사용자에게 전송한다.

Step 3 : 사용자 A는 U에 대해 a_i, p_i, g_i, $(g(ID_A \| a_i))^{d_A} \bmod n_A$, r_i, ID_A, 를 공개한다.

Step 4 : 은행 B는 Step 3에서 공개한 factor들에 대한 유효성 검사를 한다. 유효하다면 은행에 U에 속하지 않는 나머지 BLC_i에 대해 BS를 계산하여 사용자 A에게 전송한다.

$$BS \equiv \left(\prod_{i=1}^{K/2} BLC_i\right)^{d_B} \bmod n_B \equiv \prod_{i=1}^{K/2} r_i \cdot \left(\prod_{i=1}^{K/2} f(I_i \| p_i)\right)^{d_B} \bmod n_B$$

Step 5 : 사용자는 BS로부터 전자면허 BL을 계산한다.

$$BL \equiv BS / \prod_{i=1}^{K/2} r_i \equiv \prod_{i=1}^{K/2} (f(I_i \| p_i))^{d_B} \bmod n_B$$

2.4 전자 화폐 발행 단계

은행은 사용자에게 전자 화폐를 발행하기 전에 그가 가지고 있는 전자면허에 대한 유효성 검사를 한다. 그 뒤 은행은 전자화폐 factor C를 은닉 서명 방식을 사용하여 사용자에게 발급하게 되는데 이때 사용자는 수탁기관에 전송하게 될 신원 검출인자 P_1과 P_2를 생성한다. 그리고 이를 통해 EM이 만들어진다.

Step 1 : 사용자 A는 난수 $S \in \{1, \ldots, p_r-2\}$를 선택한다. 그리고 $W = g^{BL} \bmod p$와 $S = g^s \bmod p$를 계산하여 p, q와 함께 은행에게 전송한다.

Step 2 : 은행은 난수 $k \in \{1, \ldots, p_r-2\}$를 선택하여 사용자 A에게 전송한다.

Step 3 : 사용자 A는 $y \equiv S + k \cdot BL \bmod p-1$을 계산하여 은행에게 전송한다. y를 전송 받은 은행은 사용자 A가 가진 전자면허의 유효성을 확인한다.

$$g^y \equiv ? \; s \cdot w^k \bmod p$$

Step 4 : 사용자 A는 랜덤한 정수 b와 b', r을 선택하여 다음과 같은 Z를 은행에게 전송한다. 그리고 P_1과 P_2를 생성한다.

$$Z \equiv r^{e_B'} \cdot f(BL \| b) \bmod n_B'$$

$$P_1 \equiv e_r \cdot e_B + b \cdot ID_A \bmod p\text{-}1$$

$$P_2 \equiv e_r \cdot e_B + b' \cdot ID_A \bmod p\text{-}1$$을 생성

여기서, (e_B', n_B')은 ₩100에 해당하는 은행의 공개키

Step 5 : 사용자로부터 Z를 받아 은행은 $Z(= Z^{d_B'})$을 생성하여 사용자에게 전송한다.

$$Z^{d_B'} \equiv (r^{e_B'} \cdot f(BL \| b) \bmod n_B')^{d_B'}$$

$$\equiv r \cdot (f(BL \| b))^{d_B'} \bmod n_B'$$

Step 6 . 사용자는 $Z^{d_B'}$로부터 전자화폐 factor C를 계산한다

$$C \equiv Z'/r \equiv (f(BL \| b))^{d_B'} \bmod n_B'$$

여기서, EM은 $\{C, P_1^{e_B}, sign_A(C, P_1^{e_B})\}$로 구성

2.5 대금 지불 단계

은행으로부터 인출된 전자화폐를 사용하는 경우 Schnorr의 인증 기법을 사용하여 상점에 전자 화폐를 지불한다. 예를 들어 은행으로부터 받은 ₩100 중에서 ₩75을 지불한다고 하면 해당 노드 값 $(V_{1,00}, V_{1,010})$을 계산하고 이와 관련된 $Y_{1,00}$와 $Y_{1,010}$를 계산하여 은행에 전송, 화폐에 대한 유효성 검사를 한다.

Step 1 . 먼저 사용자 A는 지불하려고 하는 금액에 해당하는 노드값을 계산한다.

$$V_{1,0} \equiv g_1^c \bmod p_1, \qquad V_{1,00} \equiv V_{1,0} \cdot h_1(g_1^{V_{1,0}} \bmod p_1)$$

$$V_{1,01} \equiv V_{1,0} \cdot h_2(g_1^{V_{1,0}} \bmod p_1)$$

$$V_{1,010} \equiv V_{1,01} \cdot h_2(g_1^{V_{1,01}} \bmod p_1) \qquad (\text{for } i=1, \ldots, K/2)$$

그 뒤 $X_{i,00} \equiv g_i^{V_{i,00}} \bmod p_i$. $X_{i,010} \equiv g_i^{V_{i,010}} \bmod p_i$를 계산하여 I_i, p_i, g_i, BL, EM과 함께 상점 V에 전송한다.

Step 2 . 상점 V는 우선 EM에 있는 사용자 A의 서명을 확인한 뒤 $V_{1,00}$와 $V_{1,010}$를 확인한다.

$$V_{1,00} \equiv ? \; V_{1,0} \cdot h_1(g_1^{V_{1,0}} \bmod p_1)$$

$$V_{1,010} \equiv ? \; V_{1,01} \cdot h_1(g_1^{V_{1,01}} \bmod p_1)$$

그리고나서 난수 R_{00}, $R_{1,010} \in \{1, \ldots, p_r-2\}$를 생성하여 사용자 A에게 전송한다.

Step 3 : $R_{i,00}$와 $R_{i,010}$를 이용하여 사용자 A는 다음의 $Y_{i,00}$와 $Y_{i,010}$를 계산하여 상점 V에게 전송한다.

$Y_{i,00} \equiv V_{i,00} + R_{i,00} \cdot S_i \bmod p_i - 1$

$Y_{i,010} \equiv V_{i,010} + R_{i,010} \cdot S_i \bmod p_i - 1$, for i = 1,2, ... ,K/2

Step 4 : $Y_{i,00}$와 $Y_{i,010}$에 대한 다음 식이 성립하는지 확인하여, 만족하면 고객의 전자화폐 ₩75을 받아들인다.

$$g_i^{Y_{i,00}} \equiv {}^{?}X_{i,00} \cdot (I_i)R_{i,00} \bmod p_i$$

$$g_i^{Y_{i,000}} \equiv {}^{?}X_{i,010} \cdot (I_i)R_{i,010} \bmod p_i$$

2.6 전자화폐 예치 과정

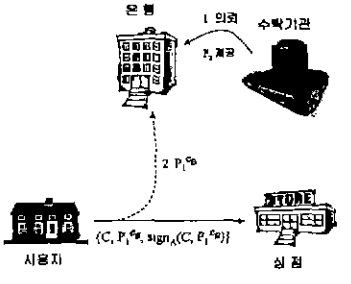
상점 V가 은행에 전자화폐 EM을 전송하기 위해서 거래 내역서(H)를 은행에게 전송한다. 은행이 H를 전송 받으면 먼저 H의 유효성을 확인하고 사용자가 이미 지불을 한 적이 없는지 은행의 DB를 이용하여 확인한다.

H = I_V, p_V, g_V, $V_{i,00}$, $V_{i,010}$, EL, EM,
$R_{i,00}$, $R_{i,010}$, $Y_{i,00}$, $Y_{i,010}$ for i=1,2, ... ,K/2

3. 제안 방식의 특성 및 안전성

3.1 사용자 추적 과정

수탁기관이 정당한 화폐 사용자의 신원을 검출하기 위해서는 먼저 법원 등의 허락을 얻은 뒤에 자신이 가지고 있는 P_2를 [그림 2]과 같이 은행에게 제시한다. P_2를 받은 전자화폐 발행 은행은 EM을 이용하여 사용자의 신원을 검출한다. 이때 은행이나 수탁기관 단독으로 EM을 가로채어 사용자의 신분 확인을 하지 못하게 된다.



[그림 2] 수탁기관의 사용자 추적 의뢰

· 은행

$(P_1^{e_B})^{d_B} = P_1$과 수탁기관이 제시한 P_2로부터,

$P_1 = e_T + e_B + b \cdot ID_A \bmod p - 1$

$P_2 = e_T + e_B + b' \cdot ID_A \bmod p - 1$

$ID_A = P_1 - P_2 / b - b'$

3.2 안전성

전자화폐는 디지털 데이터가 가지는 특성으로 인해 복사가 용이하며 이에 대한 문제점을 해결하지 않으면 화폐 유통에 큰 장애가 발생하게 된다. 이에 본 제안 방식에서는 Schnorr의 인증 기법을 이용하여 전자화폐를 이중 사용시 상점에서 사용자의 신원을 검출할 수 있도록 되어 있다.

- 전자화폐 이중 사용시 사용자 신원 검출 과정

상점은 사용자가 보내온 $V_{i,00}$, $Y_{i,00}$, $Y_{i,00}'$, $X_{i,00}$, $X_{i,00}'$로부터

$$Y_{i,00} \equiv V_{i,00} + R_{i,00} \cdot S_i \bmod p_i - 1$$

$$- \quad Y_{i,00}' \equiv V_{i,00} + R_{i,00}' \cdot S_i \bmod p_i - 1$$

$$Y_{i,00} - Y_{i,00}' \equiv (R_{i,00} - R_{i,00}') \cdot S_i \bmod p_i - 1$$

$$\therefore S_i \equiv (Y_{i,00} - Y_{i,00}') \,/\, (R_{i,00} - R_{i,00}') \bmod p_i - 1$$

여기서 $S_i \equiv (ID_A \| a_i \| (g(ID_A \| a_i))^{d_A} \bmod n_A)$이므로 이로부터 ID_A를 구할수 있다.

또한 분할성을 위해 구성된 계층적 구조 테이블에서 어느 한 노드 사용시 그 노드의 상위 노드 및 하위 노드 사용은 금지되어야 한다. 이러한 조건을 만족시키기 위해 불법 사용시 마찬가지로 사용자의 신원이 노출되어야 한다.

- $V_{i,00}$와 $V_{i,000}$ 사용시 신원 검출 과정

$Y_{i,00} \equiv V_{i,00} + R_{i,00} \cdot S_i \bmod p_i - 1$

$Y_{i,000} \equiv V_{i,000} + R_{i,000} \cdot S_i \bmod p_i - 1$에서

$V_{i,000}$은 $X_{i,000} = g_i^{V_{i,000}} \bmod p_i$로부터

$V_{i,000} \equiv V_{i,00} \cdot h_1(g_i^{V_{i,00}} \bmod p_i) \equiv V_{i,00} \cdot h_1(X_{i,00})$

이로부터

$Y_{i,00} \cdot h_1(X_{i,00}) \equiv V_{i,00} \cdot h_1(X_{i,00}) + R_{i,00} \cdot h_1(X_{i,00}) \cdot S_i \bmod p_i - 1$

$Y_{i,000} \equiv V_{i,00} \cdot h_1(X_{i,00}) + R_{i,000} \cdot S_i \bmod p_i - 1$

$\therefore \quad S_i \equiv (Y_{i,00} - Y_{i,00} \cdot h_{1(X_{i,00})} / (R_{i,00} - R_{i,00} \cdot h_1(X_{i,00}) \bmod p_i - 1)$

4. 결론

본 논문은 사용자의 익명성 유지와 고객이 가진 전자화폐의 분할 사용을 위해 Okamoto, Ohta가 제시한 방식[6]에 근거하고 있다. 그러나 Okamoto, Ohta가 제시한 방식에서와 같이 이중 사용시를 제외한 나머지 부분에서 완전한 익명성을 유지하는 것은 돈 세탁 및 범죄자들에 대한 추적도 아울러 방지가 되기 때문에 화폐를 유지 및 관리해야 하는 측면에서는 범죄 단체 및 불법적인 사용자의 돈 세탁, 자금 해외 유출 등 여러 가지 사회·경제적인 문제 발생에 대해 고려가 있어야 한다. 따라서 법원이나 기타 법 집행 기관의 결정이 있으면 사용자가 설령 정당하게 사용하였다하더라도 화폐 사용자가 누구였는지 추적할 수 있는 기능이 전자화폐 시스템 내에 포함되어 있어야 할 것이다. 이에 본 논문에서는 사용자의 익명성 유지뿐만 아니라 필요시 전자화폐 사용자를 추적할 수 있는 기능을 추가하였다. 그리고 추적시 어느 한 기관이 단독으로 사용자를 추적할 수 있는 것이 아니라 두 기관이 협력해야만 추적할 수 있도록 함으로써 추적성의 남용으로 인한 사용자 프라이버시의 침해를 방지하고자 하였다.

참 고 문 헌

[1] D.Chaum, "Blind Signatures for Untraceable Payments", Proceeding of Crypto'82, pp.199-203, 1982

[2] R.L.Rivest, A.Shamir and L.Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", ACM, vol.21, no.2, pp.120-126, 1977

[3] Claus.P.Schnorr, "Efficient Identification and Signatures for Smart Cards", Crypto'89, LNCS, vol.435, pp.235-252, 1990

[4] D.Chaum, A.Fiat and M.Noar, "Untraceable Electronic Cash", Crypto'88, LNCS, vol.403, pp.319-327, 1989

[5] T.Okamoto and K.Ohta, "Disposable zero-knowledge Authentications and Their Applications to Untraceable Electronic Cash", Crypto'89, LNCS, vol.435, pp.481-497

[6] T.Okamoto and K.Ohta, "Universal Electronic Cash", Crypto'91, LNCS, pp.324-337, 1992

[7] T.Eng and T.Okamoto, "Single-term divisible electronic coins", Eurocrypto'94, pp.311-325, 1994