익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구

오형근, 이임영
순천향대학교 공과대학 컴퓨터학부

A Study on Electronic Cash Protocol with Anonymity Control

Hyung-Geun Oh, Im-Yeong Lee
Department of Computer Science, College of Engineering
Soonchunhyang University

요 약

전자상거래에 있어서 유력한 지불 시스템으로 여겨지고 있는 전자화폐 시스템에서는 상거래시 사용자의 익명성을 유지시켜 주고 있다. 그러나 이러한 익명성의 제공은 돈 세탁과 약탈 그리고 불법적인 거래 대금의 제공에 이용될 수 있으며 이러한 사회적, 경제적인 범죄로의 이용 가능성 때문에 익명성 제어에 관한 연구가 필요한 실정이다. 이에 본 고에서는 정당한 사용자의 익명성을 보장하면서 불법적인 사용자에 대해서는 그 익명성을 취소하거나 전자화폐를 추적할 수 있는 기능을 가지는 프로토콜을 제안한다.

1. 서론

정보화 시대가 도래하면서 기존의 산업 사회에서 볼 수 없었던 여러 가지 새로운 서비스들이 등장하고 있다. 그 중에서 가장 대표적인 것으로 전자상거래(Electronic Commerce)를 들 수가 있는데 이는 실물 시장의 기능을 개방된 네트워크 상의 가상 공간

에서 수행하게끔 해주고 있으며 이러한 새로운 상거래 형태는 사용자의 편리성뿐만 아니라 기업 및 국가 경쟁력 제고의 핵심으로 작용하고 있다. 전자상거래에 있어서 핵심 기술인 전자지불 시스템(Electronic Payment System)은 크게 전자화폐 시스템(Electronic Cash System)과 지불 브로커 시스템(Payment Broker System)으로 나눌 수가 있는데 이 중에서 전자화폐 시스템이 유력한 지불 수단으로 떠오르고 있다. 아직은 연구 단계 중에 머무르고 있으나 각국에서 계속해서 새로운 전자화폐 시스템들을 개발하고 있고 자국 시스템을 전자지불 시스템의 표준으로 정착시키기 위해 노력하고 있다. 전자화폐 시스템은 사이버 캐쉬(Cyber Cash) 또는 디지털 캐쉬(Digital Cash) 등으로 불리고 있으며 실물 화폐의 기능을 사이버 공간에서 수행하기 위해 구성된 디지털 데이터이다. 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 많은 문제점들을 내포하고 있으며 이러한 문제점의 완벽한 해결 없이는 결코 해결될 수가 없다. 즉, 지폐나 동전 또는 수표 등과 같은 실물 화폐 보다 대량으로 복사가 가능하며 네트워크 상으로 전송시 화폐의 위·변조가 가능하며 돈 세탁이나 기타 범죄 수단에의 이용 등과 같은 사회·경제적인 문제점들에 대한 해결책이 선행되어야 한다.

2. 연구 배경

2.1 익명성 제어의 필요성 및 연구 동향

1982년 David Chaum이 은닉 서명 기법을 이용하여 은행과 상점이 결탁하는 것으로부터 사용자의 익명성을 제공하는 전자화폐 시스템[2]을 처음으로 제안한 이후로 익명성을 제공하는 많은 제안 방식들이 등장하였다. 전자화폐 시스템은 이와 같이 사용자가 물건을 구입하고 대금을 지불하는 동안에 사용자의 익명성을 제공하고 있으나, 사용자의 익명성이 보장되는 전자화폐는 또한 돈 세탁, 돈 약탈 그리고 마약 구매나 무기 구매 자금 등의 불법적인 구매 행위 등과 같은 각종 범죄 행동을 용이하게 한다. 범죄를 예방해야 하는 상황에서 사용자의 익명성을 무조건적으로 보장하는 것은 바람직하지 않으며 익명성을 가지는 지불 시스템이 정부나 금융기관들에 의해 받아들여지기 위해서는 어떠한 특정한 조건 아래에서 사용자의 익명성을 제어하는 메카니즘을 제공해야 한다. 이에 각국 정부에서는 익명성 조절에 관심을 가지고 화폐 소유자의 프라이버시에 대한 유연성을 갖기 위해 제어 파라메타를 가지는 익명성을 도입하려하고 있다.

공정한 지불 시스템(Fair payment systems)이라고도 불리는 익명성 취소 가능한 지불 시스템에 대한 개념은 1992년 B.von Solms와 D.Naccach가 처음으로 소개[9]하였으며 1995년 E.Brickell, P.Gemmel 그리고 D.Kravitz에 의해서 그 방안이 제안[1]이 되었다. 이 방안

에서는 전자동전의 소유자를 식별하는 소유자 추적(Owner Tracing) 개념을 소개하고 있다. 또한 1995년 M.Stadler, J.M.Piveteau 그리고 J.Camenish가 제시한 방안[8]에서는 전자동전의 소유자 추적과 동전 추적(Coin Tracing)의 두 가지 익명성 취소 모델에 대해 소개하고 있다.

익명성 취소는 익명성 조절 파라메타에 의해 제공되며 선택적으로 익명성을 취소할 수 있다. 즉, 어떠한 전자화폐의 익명성은 취소가 되고 어떠한 전자화폐들은 계속해서 익명성을 유지시킬 수가 있다는 것을 의미한다. 익명성 취소는 크게 두 개의 모델로 구분해 볼 수가 있는데 하나는 전자화폐의 소유자를 식별하는 소유자 추적과 은행으로부터의 화폐 인출을 식별하기 위한 동전 추적이 있다. 소유자 추적에 있어서 익명성 제어 파라메타는 trustee가 지불이 이루어지고 난 후에 화폐의 소유자를 판별해 낼 수 있도록 해준다. 이것의 목적은 지불이 이루어지고 난 후에 많은 화폐 유통들에 대해 합법적인 단속 요구로 이중 사용이나 위·변조와 같은 불법 사용이 일어나지 않았더라도 추적하는 것을 가능하게 해준다. 그러나 소유자 추적은 화폐에 관련된 정보에 기반하기 보다는 구입 시간, 구입량, 구입 가게 등과 같은 것들에 기반하기 때문에 사기와 같은 형태에 유용하지는 못하다. 반면에 화폐의 일련번호를 추적하는 것과 유사한 동전 추적은 물건을 구입하기 전에 추적하는 기능을 제공한다. 화폐 추적에 있어서 trustee는 은행으로부터 인출된 화폐를 확인하고 물품 구입에 사용한 것과 인출된 화폐를 연결시킬 수가 있다.

2.2 익명성 제어 시스템의 요구 조건

(a) 합법적인 사용자들에 대한 익명성(Anonymity for legitimate users)

전자화폐들은 익명성을 유지하며 합법적인 사용자들은 그 동전과 자신의 식별자가 연결되지 않는다. 대신에 이중 사용자는 은행에 의해 식별된다.

(b) 정당한 이유에 의한 취소(Revocation upon warrant presentation)

익명성은 취소 될 수가 있다. 그러나 그것은 신뢰되는 기관에 의해서만 그리고 필요에 의해서만 취소가 가능해야 한다.

(c) 권력의 분산(Separation of power)

trustee는 추적하는 기능 이외에 어떠한 다른 능력도 가지고 있지 않아야 한다. 특히 trustee들은 화폐를 위조할 수가 없어야 하고 사용자를 모방해서도 안된다.

(d) 조작 불가능성(No framing)

은행은 trustee나 또는 다른 기관들과 결탁하더라도 사용자를 모방해서는 안된다.

(e) 선택성(Selectivity)

익명성의 취소는 선택적이어야 한다. 즉 그것은 판사나 기타 신뢰 기관들이 명령

하는 거래에 한하여야 하며 나머지 부분에 있어서는 완전히 익명성을 유지해야 한다.

(f) 효율성(Efficiency)

익명성 취소는 효율적으로 이루어져야 하며 특히, trustee는 단지 익명성 취소가 요구되었을 경우에만 포함되어야 하며 off-line성을 유지해야 한다.

(g) 범죄 방지(Crime prevention)

익명성 취소가 그것이 방지하려는 범죄보다 심각한 범죄를 일으키는 동기가 되어서는 안된다.

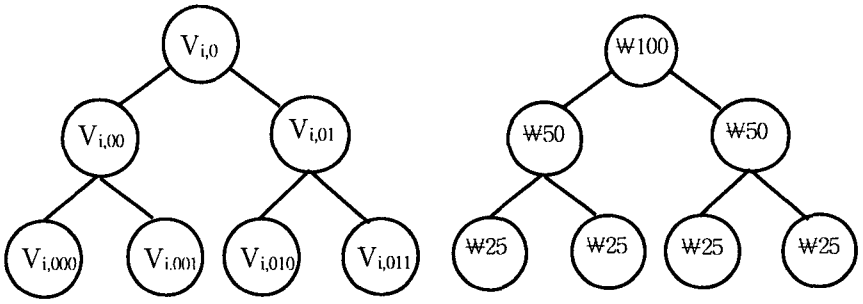
3. 제안 방식

본 논문에서 제안하고 있는 방식은 전자화폐 시스템에서 요구하는 기능뿐만 아니라 화폐의 사용자를 추적할 수 있고 익명성을 취소할 수 있는 기능을 가지고 있다. 먼저 각 개체는 RSA 알고리즘을 이용하여 키를 생성하며, 해쉬 함수에 기반한 계층적 구조 테이블(Hierachical Structure Table)을 이용한 화폐의 분할 사용, Schnorr의 인증 기법[10]을 이용한 이중 사용(Double Spending) 방지와 사용자 신원 노출 등의 특성을 만족시켜 주고 있다. 또한 이산 대수 문제를 이용한 동전 추적(Coin tracing) 기능과 ElGamal 암호 기법을 이용한 사용자 추적(Owner Tracing) 기능을 제공하여 사용자의 익명성을 조절함으로써 전자화폐의 불법적 용도로서의 사용을 방지해 주고 있다. 그리고 전자면허 발행시 은행과 사용자 인증을 위해 변형된 S/Key one-time password 방식[11]을 사용함으로서 전자면허가 단일 항으로 구성되게 하고 있다.

3.1 계층적 구조 테이블

전자화폐의 여러 가지 기능들 중에서 분할성을 만족시켜 주기 위해 계층적 구조 테이블을 사용하고 있다. 이 테이블에 의해 은행에서 발급 받은 전자화폐를 보다 작은 금액으로 분할하여 사용할 수 있으며 분할된 금액들의 합은 초기에 은행으로부터 받은 전자화폐 금액과 동일하게 된다. 계층적 구조 테이블은 트리 구조를 가지고 있고 각 노드는 화폐 금액 정보에 해당하며 다음과 같은 규칙을 가진다.

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



[그림 1] 계층적 구조 테이블

[그림 1]의 테이블은 화폐 금액과 각 노드들의 값에 대한 트리 구조를 나타내고 있으며 은행으로부터 받은 전자화폐 C는 루트 노드 V_0에 해당한다. 루트 노드는 다시 두 개의 subnode(=V_{00}, V_{01})로 나뉘어지며 이 때 자식 노드의 합은 루트노드(V_0)와 같게 된다. subnode는 두 개의 해쉬 함수 f_1과 f_2를 사용하는데 왼쪽 노드는 f_1을 사용하고 오른쪽 노드는 f_2를 사용하여 트리를 구성한다. 각 노드의 값은 다음과 같이 상위 노드를 이용하여 하위 노드를 계산해 낸다.

$$V_0 = C$$

$$V_{00} \equiv V_0 \cdot f_1(V_0) \bmod p, \quad V_{01} \equiv V_0 \cdot f_2(V_0) \bmod p$$

$$V_{000} \equiv V_{00} \cdot f_1(V_{00}) \bmod p, \quad V_{001} \equiv V_{00} \cdot f_2(V_{00}) \bmod p$$

$$V_{010} \equiv V_{01} \cdot f_1(V_{01}) \bmod p, \quad V_{011} \equiv V_{01} \cdot f_2(V_{01}) \bmod p$$

$$\vdots$$

3.2 시스템 파라메타

가. 사용자

- p : 사용자가 발생한 소수
- g_1, g_2, g_3 : GF(p)상의 원시원
- (n_A, e_A, d_A) : 사용자의 RSA 파라메타
- ID_A : 사용자가 생성한 식별자로서 은행의 계좌 번호와 연계

$$ID_A \equiv g_1^{d_A} \bmod p$$

- S : $ID_A \| response \| (h(ID_A \| response))^{d_A} \bmod n_A, \quad response = E_R(H_N(ID_A))$
- I = $g_1^s \bmod p$
- h, f_1, f_2 : 일방향 해쉬 함수(One-way hash function)로서 h는 전자면허 발행시 사용되며 f_1과 f_2는 계층적 구조 테이블에서 노드 구성시 사용된다.

· BLC(Bank License Candidate) : 전자면허를 발급 받기 위해 사용자가 생성하여 보내는 전자면허 후보

· EC(Electronic Cash) : 은행이 발행하는 전자화폐 인자 C를 사용하여 전자화폐(EC)를 구성한다.

$$EC = \{C \,||\, A_1' \,||\, A_2' \,||\, sign_A(C||A_1'||A_2')\}$$

나. 은행

· (n_B, e_B : d_B) : 은행의 전자면허용 RSA 파라메타

· (n_B', e_B' : d_B'), (n_B'', e_B'' : d_B''), . . . : 은행은 각 금액에 해당하는 RSA 파라메타를 생성한다. 예를 들어 (e_B', n_B', d_B')은 ₩100에 해당하고 (e_B'', n_B'', d_B'')은 ₩1000에 해당한다.

다. 수탁기관

· (D_T, N_T : X_T) : 수탁기관의 RSA 파라메타

· y_T : 수탁기관의 공개 정보, $y_T \equiv g_2^{X_T} \bmod t$

3.3 전자면허 발행 단계

전자화폐를 발행 받기 전에 사용자는 전자면허를 발행 받아야 한다. 이때 전자면허는 계좌 개설시에 발급 받아 전자화폐 발급시 인자로서 사용하며 사용자가 원하면 새로운 전자면허를 발행 받아 사용할 수 있다. 전자면허 발행 단계에서는 변형된 S/Key one-time password[11]를 사용하여 은행과 사용자측이 상호 인증을 하게 되며 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다. 또한 제안 방식에서의 전자면허는 단일 항으로 구성됨으로써 기존의 방식보다 효율적이다.

사용자와 은행은 상호 인증을 위한 초기화 단계를 수행한다. 먼저 사용자와 은행은 해쉬함수를 적용할 횟수 N을 결정한다. 이를 이용하여 서버측에 저장할 사용자의 비밀 정보를 생성해 낸다.

step 1 : 사용자는 hash function H와 ID_A 그리고 N을 선택하고 이를 은행에 전송한다.

step 2 : 은행은 사용자의 비밀정보 X_{N+1}을 생성하고 X_{N+1}과 N+1만을 저장한다.

$$X_1 = H_1(ID_A),\ X_2 = H_2(X_1),\ \ldots,\ X_{N+1} = H_{N+1}(X_N)$$

step 3 : 은행은 난수 R과 challenge 값을 생성하여 사용자에게 전송한다.

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

step 4 : 사용자는 $H_N(ID_A)$와 $H_{N+1}(ID_A)$ 그리고 R'을 계산하고 은행 인증 과정을 수행한다.

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

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

은행의 인증 과정이 성립되면 response, S, I와 전자면허 후보 BLC 값을 계산하여 I값은 공개하고 response와 BLC를 은행에 전송한다.

step 5 : 은행은 사용자 인증 과정을 수행하고 사용자 관련 저장 정보를 N+1에서 N으로, X_{N+1}을 $X_N = H_N(p)$로 갱신한다. 그리고 BLC에 은행의 서명을 하여 사용자에게 전송한다.

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

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

step 6 : 사용자는 은행이 서명한 BLC로부터 전자면허 BL을 추출한다.

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

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

3.3 전자화폐 발행 단계

은행이 발행한 전자면허를 이용하여 은행으로부터 전자화폐를 발행 받는 과정이다. 전자화폐를 발행 받는 동안에 화폐를 추적할 수 있는 인자 A_1'이 생성되며 이 A_1'은 화폐 추적 단계에서 trustee를 거치면서 화폐 추적을 위해 사용된다.

step 1 : 사용자는 v∈{1, . . . , p-1}를 랜덤하게 선택하고 A_1'과 A_2'를 생성하여 은행에 전송한다.

$$A_1' \equiv y_T^{v} \bmod p, \quad A_2' \equiv Ig_2 g_3^{V^{-1}} \bmod p$$

step 2 : 은행은 A_1', A_2'를 올바르게 생성하였는지 확인한 뒤 w∈{1, . . . , p-1}를 랜덤하게 선택하여 사용자에게 전송한다.

$$\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1'} y_T$$

step 3 : 사용자는 랜덤 넘버 b를 선택하여 Z를 계산한다. 또한 r값을 계산하여 Z와 함께 은행에 전송한다. 이때 r은 랜덤한 정수이며 사용자가 화폐를 전송 받기 위해 생성한 데이터를 은닉시킨다.

$$Z \equiv r^{e_B'} \cdot H(BL \| b) \bmod n_B', \quad r = Zw + v \bmod p$$

step 4 : 은행은 Z에 서명을 해 주기 전에 Z가 사용자 A에 의해 올바르게 생성되었는지 확인한 다음 Z에 서명한 값 Z'을 사용자에게 전송한다.

$$g_2^r \stackrel{?}{=} (a')^Z \cdot (A_1')^{X_T^{-1}}$$

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

$$\equiv r \cdot (f(BL \| b))^{d_B'} \bmod n_B' \qquad \text{여기서 } a' = g_2^w \bmod p \text{이다.}$$

step 5 : 사용자는 Z'으로부터 전자화폐 C를 추출해 낸다.

$$C \equiv Z'/r$$

$$\equiv (H(BL \| b))^{d_B'} \bmod n_B'$$

이때 실제 전자화폐(EC)는 $\{ C \| A_1' \| A_2' \| sign_{n_A}(C \| A_1' \| A_2') \}$으로 구성되어 있다.

3.4 대금지불 단계

은행으로부터 인출된 전자화폐와 계층적 구조 테이블을 이용하여 상점에게 원하는 금액을 지불한다. 즉 ₩100 중 ₩75를 지불하기 원한다면 노드 값 V_{00}, V_{010}을 계산하고 이와 관련된 Y_{00}, Y_{010}을 계산하여 상점에 전송함으로써 전자화폐에 대한 유효성을 검사한다.

step 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.

$$A = (A_1')^t, \quad A_1 = g_2^t, \quad A_2 = g_1^{ts}$$

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

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

step 2 : 상점은 전자화폐 EC에 있는 사용자 서명을 확인한 뒤 V_{00}, V_{010}과 A, A_1', A_2'를 확인한다.

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

$$V_{010} \stackrel{?}{\equiv} V_{01} \cdot f_1(V_{01}) \bmod p$$

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

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

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

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

$$g^{Y_{00}} \stackrel{?}{\equiv} X_{00} \cdot (I)^{R_{00}} \bmod p$$

$$g^{Y_{010}} \stackrel{?}{\equiv} X_{010} \cdot (I)^{R_{010}} \bmod p$$

3.5 예치단계

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

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

4. 제안 방식의 특징

4.1 안전성

전자화폐는 디지털 데이터가 가지는 특징으로 인해 대량으로 복사가 가능하며 이를 방지하기 위한 대책이 수립되어 있어야 한다. 본 제안 방식에서는 트리구조에서 각 노드를 구성하기 위해 필요한 조건들을 만족시키고 있다.

가. 사용된 노드의 상·하위 노드 사용시

한번 사용된 노드의 상위 노드와 하위 노드들은 사용할 수가 없어야 한다. 만약 어느 한 노드라도 사용할 수 있다면 그것은 화폐 금액의 초과 사용을 의미하게 된다. V_{00}와 V_{000}가 사용이 되었다면 Schnorr의 인증 기법을 사용하여 Y_{00}와 Y_{000}로부터 S가 구해지고 이로부터 ID_A를 검출해 낼 수 있다.

- V_{00}와 V_{000} 사용시 신원 검출 과정

$$Y_{00} \equiv V_{00} + R_{00} \cdot S \bmod p-1$$
$$Y_{000} \equiv V_{000} + R_{000} \cdot S \bmod p-1 \text{에서}$$
$$V_{000} \equiv V_{00} \cdot f_1(V_{00}) \bmod p,$$
$$\equiv V_{00} \cdot f_1(c \cdot f_1(c)) \text{ 이므로}$$

이로부터

$$Y_{00} - Y_{000} \equiv (V_{00} \cdot f_1(V_{00}) + R_{00} \cdot f_1(V_{00}) \cdot S) - (V_{00} \cdot f_1(V_{00}) + R_{000} \cdot S) \bmod p$$
$$\equiv (R_{00} \cdot f_1(V_{00} - R_{000}) \cdot S$$
$$\therefore\ S \equiv (Y_{00} - Y_{00} \cdot f_1(V_{00}))/(R_{00} - R_{00} \cdot f_1(X_{00}) \bmod p-1)$$

나. 같은 동전의 이중 사용시

같은 노드를 상점에 지불하였을 경우에 상점에서는 즉시 이중 사용 여부를 검출할 수 있어야 한다. 즉 V_{00}가 두 번 사용되었을 경우 Y_{00}와 Y_{00}'으로부터 사용자의

ID_A를 검출 할 수 있어야 한다.

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.

4.2 화폐 추적

화폐 추적은 사용자가 전자화폐를 사용하기 전에 trustee에 의해 은행에 추적 기능을 부여 할 수가 있다. 즉, 전자화폐 발행 단계에서 사용자가 은행에 전송한 인출 사본 중 A_1'으로부터 trustee는 A_1을 생성하고 이를 은행에 재 전송해 줌으로써 은행측에서는 인출 화폐를 확인하고 사용화폐와 인출화폐를 연결함으로써 화폐를 추적할 수가 있다. 화폐 발행 단계에서 다음 과정을 수행시킴으로서 화폐 추적 기능을 제공한다.

step 1 : 은행은 사용자가 제시한 인출 사본 중 A_1'을 trustee에게 제공한다.

step 2 : trustee는 A_1'로부터 A_1을 계산해낸다.

$$(A_1')^{X_T^{-1}} \equiv (y_T^v)^{x_T^{-1}}$$

$$\equiv g_2^{X_T \cdot v \cdot X_T^{-1}} \equiv g_2^v \equiv A_1$$

step 3 : trustee는 A_1을 은행에게 전송한다.

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

4.3 사용자 추적

사용자 추적 단계는 지불이 이루어지고 난 후에 사용자를 판별하는 방법으로서 합법적인 화폐 교환이 이루어지고 난 후에 추적을 가능케 한다. 이는 화폐의 부정사용에 관련된 것들에 기반하기 보다는 사용자가 구입한 물품들에 대한 혐의가 주어질 경우에 그 화폐의 사용자를 추적하게 된다. 이 단계는 예치 단계에 추가하여 구성되며 사용자가 상점에 대금 지불시 $A_3(= ID_A \cdot (y_T)^v \bmod p)$가 추가된다.

step 1 : 은행은 상점이 예치한 거래 내역서로부터 A_3를 trustee에 전송한다.

step 2 : trustee는 A_3로부터 $A_3' \equiv ID_A^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하여 은행에 전송한다.

$$A_3' \equiv A_3^{X_T^{-1}} \bmod p$$

$$\equiv ID_A^{X_T^{-1}} \cdot g_2^v \bmod p$$

step 3 : 은행은 trustee가 전송한 A_3'로부터 ID_A를 계산해 낸다.

$$A_3'/A_2 \bmod p \equiv ID_A^{X_T^{-1}} \cdot g_2^{r'}/g_2^{r'} \bmod$$

$$\equiv ID_A^{X_T^{-1}}$$

$$\therefore \quad ID_A = (ID_A^{X_T^{-1}})^{D_T}$$

5. 비교 분석

[표 1]에서는 최근에 제안된 각종 전자화폐 프로토콜들을 중심으로 사용자 익명성과 분할성, 그리고 익명성 제어 등의 특징별로 나누어 비교하고 있다. 1995년에 익명성 취소 개념의 전자화폐 시스템들이 제안된 후 여러 방안들이 제안되었으나 이전의 방안들이 고객의 계좌 개설시나 인출 단계에서 trustee의 개입을 요구하거나 cut-and-choose 방식을 이용하여 비효율적인데 반해 1996년에 제안된 Camenisch-Maurer-Stadler 방식[7]은 거래 참여자의 익명성을 제어하는 trustee가 화폐 발행시나 또는 지불시에 참여하지 않는 off-line형 trustee를 가지며 사용자와 화폐를 추적할 수 있으며 보다 효율적인 방안을 제안하였다. 또한 1997년에 G.Davida, Y.Frankel, Y.Tsiounis 그리고 M.Yung에 의해 제안된 방안[5]은 Camenisch-Maurer-Stadler 방식[3]에서 제안된 것처럼 효율적인 off-line trustee에 중점을 두었다. 그러나 위의 익명성 제어가 가능한 프로토콜들은 전자화폐의 기본적인 요구사항인 분할사용 가능성을 만족시켜 주지는 못하고 있다. 한편 1995년에 제안된 Okamoto의 방안[6]과 1998년에 제안된 Chan-Frankel-Tsiounis 방식[4]은 이중 사용시에만 사용자의 신원을 검출하여 주며 그 밖의 경우에 있어서는 사용자의 익명성을 유지시켜 주고 있다. 대신에 1991년에 제안된 Okamoto-Ohta 방식[7]을 개선하여 효율적인 분할 사용을 가능하게 해 주고 있다. 이에 반해 본 제안 방식은 전자화폐 프로토콜에서 요구하는 요구사항을 만족시켜 주고 있으며 익명성 제어도 가능한 새로운 방안이다. 또한 전자화폐를 발급 받기 위한 전자면허를 효율적인 단일 항으로 구성 시켜줌으로써 전자화폐 및 분할 사용시에도 효율적으로 구성될 수가 있다.

[표 1] 각종 전자화폐 프로토콜의 비교

비교 방식	익명성	이중사용 방지	분할성	사용자 추적	화폐 추적
Okamoto 방식 1995	Strong	O	O	X	X
Camenisch-Maurer -Stadler 방식 1996	Revocable	O	X	O	O
Davida-Frankel -Tsiounis-Yung 방식 1997	Revocable	O	X	O	O
Chan-Frankel -Tsiounis 방식 1998	Strong	O	O	X	X
제안 방식	Revocable	O	O	O	O

6. 결론

전자화폐나 기타 다른 암호학적인 전자 지불 시스템에서는 구매 및 지불 단계에서 사용자의 익명성을 제공하고 있으며 이것은 은행이 상점과 결탁하더라도 화폐 사용자를 추적할 수 없다는 것을 의미한다. 이렇게 익명성을 제공하려는 경향은 개인의 프라이버시에 대한 높은 관심과 중요성으로 볼 때 앞으로의 지불 시스템에서 계속적으로 요구될 것으로 보인다. 그러나 그에 못지 않게 익명성은 많은 사회적, 경제적인 범죄를 가져올 수 있으며 이러한 문제로 인하여 전자상거래의 발전에 큰 걸림돌로 작용할 수도 있다. 따라서 초기의 익명성 제공에만 그 연구 초점을 맞추었던 것이 현재는 익명성 제어(Anonymity Control) 또는 익명성 취소(Anonymity Revocation)에 관한 연구가 활발히 진행되고 있다. 그러나 전자화폐의 추적성은 일반적인 범죄 행위들을 감소시키는데는 기여할 수 있지만 대신에 범죄자 자신들이 신분 노출이 되지 않도록 하기 위해 보다 심각한 범죄를 저지를 수 있다. 이러한 문제점들에 대한 해결책도 익명성 제어 문제와 함께 논의가 되어야 할 것이다.

[참고 문헌]

[1] E.F.Brickell, P.Gemmell, and D.Kravitz, "Trustee-based tracing extension to anonymous cash and the making of anonymous change", In Symposium On Distributed Algorithms(SODA), Albuquerque, NM.1995, Available at http://www.cs.sandia.gov/~psgemme/

[2] D.Chaum, "Blind Signautures for untraceable payments", Advances in Cryptography, Crypto'82, pp 199-203, 1983

[3] J.Camenisch, U.Maurer, and M.Stadler, "Digital payment systems with passive anonymity-revoking trustees", In Esorics '96, Italy, 1996. To appear. Available at http://www.inf.ethz.ch/personal/camenisc/publications.html

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

[5] G.Davida, Y.Frankel, Y.Tsiounis, and M.Yung, "Anonymity control in e-cash" In Proceedings of the 1st Financial Cryptography conference(LNCS1318), Anguilla, BWI, February24-28, 1997. To appear. Available at http://www.ccs.neu.edu/home/hiannis/pubs.html.

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

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

[8] M.Stadler, J.M.Piveteau, and J.Camenisch, "Fair blind signatures", In Advances in Cryptology, Proc, of Eurocrypto '95, pp209-219, 1995

[9] B.von Solms and D.Naccache, "On blind signautures and perfect crimes", Computers and Security, pp581-583, 1992

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

[11] 김기현, 은유진, 박정호, 고승철, "변형 일회용 패스워드 시스템 제안", 제 10회 정보보호와 암호에 관한 학술 대회(WISC '98), pp75-92, 1998

[12] 오형근, 이임영, "새로운 추적 가능한 전자화폐 프로토콜에 관한 연구", '98 정보과학회 가을 학술 발표논문집(III), pp344-346, 1998