KCDSA를 이용한 분할성 기능을 가진 익명성 제어 전자화폐 시스템

장 석 철[†] · 이 임 영[††]

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 발행하는 문제점들을 해결하기 위한 익명성 제어에 관련된 전자화폐 시스템이 연구되고 있다. 그리고 전자화폐의 효율성을 위해서 분할성을 가지는 전자화폐에 대한 연구도 같이 진행되고 있다. 본 논문에서는 분할성과 관련된 기존 방식을 분석하고 익명성 제어에 대한 개념을 살펴본다. 그리고 국내 전자서명 표준인 KCDSA에 온닉서명을 추가한 새로운 온닉서명 방식을 제안한다. 이를 기반으로 하여 익명성을 유지하며 필요시 신뢰기관의 도움으로 익명성을 제어할 수 있고 전자화폐의 효율적 사용을 위해 분할성 기능을 함께 제공하는 새로운 전자화폐 시스템을 제안한다.

An Anonymity Control Electronic Cash System with Divisible using KCDSA

Seok-cheol Jang[†] · Im-yeong Lee[††]

ABSTRACT

The increase of electronic commerce leads to the increasing attention to the way customers pay and a large number of researches on payment system. Recently many researches on a system which provides anonymity in order to protect user's privacy have been carried out. And some potential problems from that system are being reviewed by anonymity control system. This thesis will include the following. First, I want to analyze the old scheme related to divisible and examine general ideas of anonymity control. Second, I propose a new blind signature in addition to KCDSA, the standard digital signature in Korea. The last one I want to propose is a new electronic cash system with the divisible for more efficient use of electronic cash which can control anonymity with the help of trustee.

키워드 : 전자화폐시스템(Electronic Cash System), 전자서명(Digital Signature), 분할성(Divisible), 익명성 제어(Anonymity Control)

1. 서 론

최근에는 정보통신 및 컴퓨터 기술의 발달로 신용카드, 전자 자금이체, 인터넷 뱅킹 등 현금대체 결제수단이 보편화되고 있다. 하지만 이러한 현금 대체 결제 수단을 인터넷에서 사용할 경우 개인 사생활이 노출될 수 있고 범죄에 이용될 수도 있다. 따라서 인터넷과 같은 네트워크 상에서 지불수단으로써 전자화폐의 필요성이 증가되고 있다. 그리고, 시간절약과 편리성 때문에 인터넷 쇼핑몰의 사용이 급증함에 따라 전자화폐에 대한 필요성이 증가되고 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 구입내용 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 돈 세탁, 약탈과 불법 거래와 같은 불법적인 범죄 행위들에 이용될 수 있으며, 이때 이와 같은 범죄행위를 한 사용자와 그 돈에 대한 행방을 찾을 수가 없다.

따라서 본 논문에서는 위에서 언급한 문제점을 해결하기 위해 Okamoto-Ohta가 제안한 전자화폐의 기본적인 요구 조건을 만족하며, 또한 익명성 제공으로 인한 범죄에의 이용을 방지하기 위해 익명성을 제어하는 전자화폐 프로토콜을 제

※ 본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임.
† 준 회 원 : 순천향대학교 대학원 전산학과
†† 종신회원 : 순천향대학교 정보기술공학부 교수
논문접수 : 2001년 5월 11일, 심사완료 : 2001년 9월 14일

안한다. 그리고 전자화폐 발급시 사용자와 은행간에 효율적인 인증 과정을 수행하며 전자화폐가 단일항(single-term)으로 구성되도록 하기 위해 변형된 S/Key one-time password 방식을 이용한다. 마지막으로 전자화폐 발급시 은행과 사용자간에 국내 전자서명 표준인 KCDSA를 기반으로 하여 익명성을 유지하며 필요시 신뢰기관의 도움으로 익명성을 제어할 수 있는 새로운 공정 은닉 서명 기법을 사용한다.

2. 전자화폐에 대한 분할성 및 익명성 제어

이번 장에서는 전자화폐의 전체 요구사항 중 분할성과 익명성 제어에 대한 기본 개념에 대해 설명한다.

2.1 분할성

분할성은 합계 금액이 액면 금액이 될 때까지 분할해서 사용할 수 있는 기능이다. 이러한 기능은 기존의 화폐에서는 볼 수 없는 기능으로 일정한 가치를 가지고 있는 전자화폐는 그 금액의 크기만큼 자유롭게 분할되어 사용될 수 있어야 한다. 이때 분할된 전자화폐의 안전성은 분할되기 전의 전자화폐와 같은 안전성을 유지해야하며 또한 상점에서는 같은 동전의 이중 사용 여부를 검사할 수 있어야 한다. 분할 사용 기능을 통해 사용자는 작은 금액을 지불하기 위해 은행으로부터 작은 금액의 전자화폐를 발행 받지 않아도 되는 등 화폐 관리 면에서 효율적이다. 또한 상점 측에서도 거스름 발생에 대비하여 작은 금액의 전자화폐를 보관하던가 또는 새로운 거스름 전자화폐를 발행하지 않아도 된다[2].

2.2 익명성 제어

D. Chaum이 은닉 서명 기법을 이용하여 사용자의 익명성을 제공하는 전자화폐 시스템을 처음으로 제안한 이후로 대부분 사용자의 제안 방식들에서는 익명성을 제공하고 있다. 전자화폐에 있어서 익명성은 개인의 사생활 보호라는 긍정적인 측면 이외에 불법적으로 사용된 돈의 정보를 알지 못하게 함으로서 완전한 돈 세탁(money laundering)과 약탈(black mailing)을 가능하게 한다. 이처럼 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 메커니즘을 제공해야 한다[8].

3. 기존 방식

전자화폐에 대한 연구 개발은 D.Chaum이 on-line형 전자화폐 시스템을 제안한 후 전자화폐가 가져야할 조건을 만족시키는 많은 방식들이 제안되고 있다[1]. 이번 장에서는 전자화폐 관련 많은 방식들 중에서 전자화폐가 가져야할 분할성에 대한 기존방식을 분석한다.

3.1 Okamoto-Ohta 방식

2장에서 설명한 분할성은 Okamoto-Ohta가 처음으로 제안하였다[2]. 이 방식 이전에 Okamoto-Ohta는 화폐의 분할성 개념을 도입한 electronic coupon ticket system을 제안하였다. 그러나 이 방식에서 하나의 전자화폐 조각은 가치가 동등한 많은 화폐 조각들로 나뉘어지는 형식을 취하고 있으며, 이것은 단지 동일한 가치를 여러 개의 화폐로 나누는 것으로 진정한 의미의 분할성 개념을 가지고 있다고 할 수는 없을 것이다. 이 방식은 전자면허 발행시 cut-and-choose 방식을 사용하였다. 이 방식의 문제점은 상점과 은행사이에서 발생하는 통신량과 은행에 의해서 유지되어야 하는 데이터베이스의 메모리 크기가 크다는 것이고, cut-and-choose 방법을 사용하고 있기 때문에 화폐는 많은 term들로 구성되어야 한다.

3.2 Eng-Okamoto 방식

Eng-Okamoto는 Okamoto-Ohta방식보다 효율적인 분할성을 가지는 오프라인 전자화폐 방식을 제안하였다[3]. Eng-Okamoto는 Okamoto-Ohta방식에서 나타난 문제점들인 큰 통신량과 메모리 크기 그리고 비효율적인 화폐 term들의 구성을 해결하였다. 이 방식은 Brands의 방법을 기초로 하였으며, 최초로 단일항을 가지는 화폐 시스템으로서 요구되는 통신량과 메모리는 Okamoto-Ohta의 방법에 비해 1/10밖에 들지 않는다. 그러나 이러한 방식에서도 지불시 요구되는 계산량은 Okamoto-Ohta 방식만큼 크다.

3.3 Okamoto 방식

Eng-Okamoto의 단점인 큰 계산량을 해결하고자 Okamoto는 모든 단계가 효율적으로 수행될 수 있는 분할 가능한 방식을 제안하였다[4]. 이 방식에서는 cut-and-choose 방법을 대신하여 전자면허 발행시 이산대수 문제에 기반한 새로운 bit commitment 방법으로 은행에게 위탁된 값들을 증명할 수 있는 프로토콜을 제안하였다. Okamoto가 사용한 bit commitment를 이용한 zero-knowledge는 매우 많은 트랜젝션을 발생시키기 때문에 비효율적이다.

3.4 Chan-Frankel-Tsiounis 방식

Okamoto는 인출, 지불과 예치 과정에서 각각에 대해서 오직 $O(\log N)$의 계산량을 요구하는 처음으로 효율적인 분할성과 익명성을 가진 오프라인 전자화폐를 발표했다. 그러나, Okamoto에 의해서 은닉된 비연결 동전의 제안을 사용한 영지식 증명 프로토콜은 아주 비효율적이다. 그래서 Chan-Frankel-Tsiounis는 이러한 비효율적인 시스템을 효율적 시스템

으로 만들기 위해서 전자면허 발행 단계가 필요하여 이 부분을 추가한 방식을 제안하였다[5].

4. 제안 방식

본 제안 방식은 전자화폐 프로토콜에 적용할 수 있도록 국내 전자서명 표준인 KCDSA를 변형한 공정한 은닉 서명 방식을 적용하여 전자화폐를 발행 받고[6], 해쉬함수에 기반한 계층적 구조 테이블(hierarchical structure table)을 이용한 화폐의 분할 사용, Schnorr의 인증 기법을 이용한 이중사용(double spending)방지와 불법 사용시 사용자 신원 노출 등의 특성을 만족시켜 주고 있다[7]. 또한 이산 대수 문제를 이용한 화폐 추적(coin tracing) 기능과 ElGamal 암호 기법을 이용한 사용자 추적(owner tracing) 기능을 제공하여 사용자의 익명성을 조절함으로써 전자화폐의 불법적 용도로서의 사용을 방지해 주고 있다[8]. 그리고 전자면허 발행시 은행과 사용자 인증을 위해 변형된 S/Key one-time password 방식을 사용함으로서 전자면허를 단일 항으로 구성하고 있다[9].

4.1 은닉 KCDSA

4.1.1 시스템 매개변수

본 시스템에서 사용되는 시스템 매개변수는 다음과 같다.

- p : $2^{|p|-1} < p < 2^{|p|}$, $|p| = 512 + 256i\ (0 \le i \le 6)$를 만족하는 소수
- q : $q | p-1$, $2^{|q|-1} < q < 2^{|q|}$, $|q| = 128 + 32j\ (0 \le j \le 4)$를 만족하는 소수
- $g \in Z_q$는 $g \equiv h^{(p-1)/q} \bmod p\ (g > 1,\ 1 < h < p-1)$을 만족한다.
- H : 일방향 해쉬 함수
- $x \in Z_q$: 서명자의 비밀키
- $y \equiv g^x \bmod p$: 서명자의 공개키

4.1.2 서명 단계

- 과정 1 : 서명자는 랜덤하게 $k' \in Z_q$를 선택하여 다음과 같이 계산하여 검증자에게 보낸다.

$$r' \equiv g^{k'} \bmod p$$

- 과정 2 : 검증자는 랜덤하게 은닉인자 $\alpha \in Z_q$와 $\beta \in Z_q$를 선택하여 r과 은닉된 값 m'을 계산하여 서명자에게 전달한다.

$$r \equiv mg^{\alpha} r'^{\beta} \bmod p,\quad m' \equiv r\beta^{-1} \bmod q$$

- 과정 3 : 서명자는 다음과 같이 서명을 한 s'을 검증자에게 보낸다.

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

- 과정 4 : 검증자는 서명자로부터 받은 s'을 이용하여 s를 구하고 이를 이용하여 검증한다.

$$s \equiv s'\beta + \alpha \bmod q,\quad m \stackrel{?}{\equiv} g^{-s} y^{r} + \beta H r \bmod p$$

4.2 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.

- 어떤 한 노드에 있어서 해당 금액은 자식 노드들의 합과 같다.
- 어떤 한 노드가 사용되면, 모든 자식 노드와 부모 노드는 사용할 수 없다.
- 어떤 노드도 한 번 이상 사용될 수 없다.

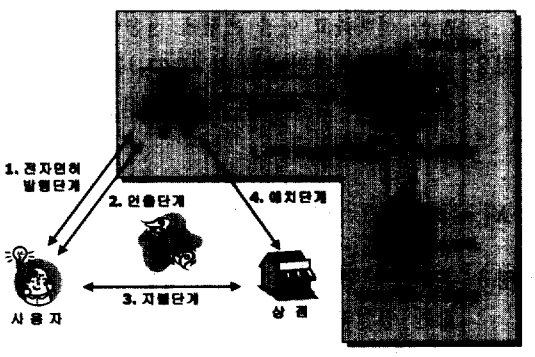
4.3 시스템 매개변수

본 시스템에서 사용되는 시스템 매개변수는 다음과 같다.

4.3.1 사용자

- p : 사용자가 발생한 소수
- g_1, g_2, g_3 : $GF(p)$상의 원시원
- (n_A, e_A, d_A) : 사용자는 RSA 매개변수로서 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 식별자로서 은행의 계좌 번호와 연계된 값이다.
- S : $ID_A \| response \| (H(ID_A \| response))^{d_A} \bmod n_A$

이때, *response*는 은행이 보내온 *challenge* 값에서 추출해 낸 값 R'을 키로 하여서 사용자의 ID_A를 N번 해쉬한 결과($X_N = H_N(ID_A)$)를 암호화 한 값이다. 즉, $response = E_{R'}(H_N(ID_A))$이다.



(그림 1) 제안방식 전체 흐름도

- $I \equiv g_1^s \bmod p$
- H, f_1, f_2 : 일방향 해쉬함수(one-way hash function)로서 H는 전자면허 발행시 사용되며 f_1과 f_2는 계층적 구조테이블에서 노드 구성시 사용된다.
- *BLC*(*Bank License Candidate*) : 전자면허를 발급받기 위해 사용자가 생성하여 보내는 전자면허 후보, $BLC \equiv r_1^{e_B} \cdot H(I \| X_N) \bmod n_B$, 여기서 r_1은 랜덤하게 선택한 값이다.
- *EC*(*Electronic Cash*) : 은행이 발행하는 전자화폐 인자 C를 사용하여 전자화폐(EC)를 구성한다. 실제 전자화폐는 $EC = \{C \| A_1' \| A_2' \| sign_A(C \| A_1' \| A_2')\}$로 구성된다.

4.3.2 은행

- (n_B, e_B, d_B) : 은행의 전자면허용 RSA 매개변수로서, n_B, e_B는 공개키이고 d_B는 비밀키이다.
- R : 은행이 랜덤하게 선택한 값으로 사용자와 은행 상호 인증 과정에서 사용된다.

4.3.3 신뢰기관

- 신뢰기관은 랜덤하게 그의 비밀키 $X_T \in Z_p^*$를 선택한다. 그리고 그의 공개키 $y_T \equiv g_2^{X_T} \bmod p$를 계산한다.

4.4 전자면허 발행 단계

전자화폐를 발행 받기 전에 사용자는 전자면허를 발행 받아야 한다. 이때 전자면허는 계좌 개설시에 발급받아 전자화폐 발급시 인자로서 사용하며 사용자가 원하면 새로운 전자면허를 발행받아 사용할 수 있다. 전자면허 발행 단계에서는 변형된 S/Key one-time password를 사용하여 은행과 사용자측이 상호 인증을 하게 되며 은닉 서명 방식을 사용하여 사용자의 익명성을 유지한다.

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.

- 과정 1 : 사용자는 해쉬함수 H와 ID_A 그리고 해쉬 횟수 N을 선택하고 이를 은행에 전송한다.
- 과정 2 : 은행은 사용자의 비밀정보(ID_A)를 $N+1$번 해쉬한 $X_{N+1}(= H_{N+1}(ID_A))$을 생성하고 X_{N+1}과 $N+1$만을 저장한다.

$$X_1 = H(ID_A),\ X_2 = H(ID_1),\ \cdots,\ X_{N+1} = H(X_N)$$

- 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 BLC 값을 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.

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

4.5 전자화폐 발행 단계

은행이 발행한 전자면허를 이용하여 은행으로부터 전자화폐를 발행받는 과정이다. 이 단계에서는 국내 전자서명 표준인 KCDSA를 변형한 공정한 은닉 서명 방식을 적용하여 전자화폐를 발행받는다. 그리고 전자화폐를 발행받는 동안에 화폐를 추적할 수 있는 인자 A_1'이 생성되며 이 A_1'은 화폐 추적 단계에서 신뢰기관을 거치면서 화폐 추적을 위해 사용된다.

- 과정 1 : 사용자는 $v \in \{1, \cdots, p-1\}$를 랜덤하게 선택하고 A_1'과 A_2'를 생성하여 은행에 전송한다.

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

● 과정 2 : 은행은 A_1', A_2'를 올바르게 생성하였는지 확인한 뒤 $k' \in Z_q$를 랜덤하게 선택하여 r'을 계산하여 사용자에게 전송한다.

$$\log_{g_3}(A_2' / Ig_2) \stackrel{?}{=} \log_{A_1} y_T,\ r' \equiv g^{k'} \bmod p$$

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

$$m = BL,\ r \equiv mg^{\alpha} r'^{\beta} \bmod p,\ m' \equiv r\beta^{-1} \bmod q$$

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

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

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

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

검증이 성립하면 실제 사용될 전자화폐를 다음과 같이 구성한다.

$$EC = \{(r, s) \| A_1' \| A_2' \| Sign_A((r, s) \| A_1' \| A_2')\}$$

4.6 전자화폐 지불 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.

● 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.)

$$A \equiv (A_2')^{v} \bmod p,\ A_1 \equiv g_2^{v} \bmod p,\ A_2 \equiv g_1^{ss} \bmod p$$

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

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

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

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

$$A \stackrel{?}{\equiv} A_1 \cdot A_2 \cdot g_3 \bmod p$$

그리고 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 다음 식이 성립하는지 확인하여, 만족하면 V_{00}, V_{010}를 인증하여 고객의 전자화폐 ₩75을 받아들인다.

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

4.7 예치단계

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

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

이때, O_A는 사용자 및 화폐 추적인자 A_1, A_3로 구성된 데이터로서 선택적으로 사용할 수 있다.

5. 제안 방식의 분석

제안방식은 S/Key one-time password를 사용함으로써 은행과 사용자측이 상호 인증이 가능하며 해쉬함수만으로 연산이 이루어지는 타방식에 비해 전자면허 발행 단계에서 계산적 효율성이 높다. 또한 분할성을 제공하기 위해 계층적 구조 테이블을 사용하였고, 이중사용방지를 위해 Schnorr의 인증 기법을 사용하였다. 그리고 전자화폐 발행시 국내 전자서명 표준인 KCDSA를 이용하였다.

제안방식의 보다 자세한 분석은 다음과 같다.

5.1 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 서명방식을 전자화폐에서 사용할 수 있는 메시지 복원형 전자서명 방식으로 변형하였다. KCDSA는 국내에서 개발한 전자서명 알고리즘으로서 국내 및 국제 특허에 저촉되지 않고 국내 표준이므로 응용 프로토콜에 쉽게 적용 가능하다. 또한 기존의 KCDSA가 가지는 특징과 장점인 공개키 확인서 이용한 전자서명 방식, 유한체 $GF(p)$상에서 정의, 안전성은 유한체에서 이산대수 문제를 풀기 어렵다는 사실 등을 그대로 적용 가능하다.

5.2 안전성

전자화폐는 디지털 데이터가 가지는 특징으로 인해 대량으로 복사가 가능하며 이를 방지하기 위한 대책이 수립되어 있어야 한다. 이를 위해 본 제안 방식에서는 계층적 구조 테이블을 구성하기 위해 필요한 규칙들을 만족시키고 있다.

5.2.1 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. 만약, V_{00} 와 V_{000} 가 사용이 되었다면 Schnorr의 인증 기법을 사용하여 Y_{00} 와 Y_{000} 로부터 S 가 구해지고 이로부터 ID_A 를 검출해 낼 수 있다.

- V_{00} 와 V_{000} 사용시 신원 검출 과정

$Y_{00} \equiv V_{00} + R_{00} \cdot S \mod p-1$ 그리고

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

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

이므로 이로부터,

$$\begin{aligned} Y_{00} \cdot f_1(V_{00}) - Y_{000} &\equiv (V_{00} \cdot f_1(V_{00}) + R_{00} \cdot f_1(V_{00}) \cdot S) \\ &\quad - (V_{00} \cdot f_1(V_{00}) + R_{000} \cdot S) \mod p \\ &\equiv (R_{00} \cdot f_1(V_{00}) - R_{000}) \cdot S \end{aligned}$$

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

와 같이 S 가 구해지고 이로부터 ID_A 가 구해진다.

5.2.2 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_A 를 검출 할 수 있어야 한다.

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

$$Y_{00} - Y_{00}' \equiv (R_{00} - R_{00}') \cdot S \mod p-1$$

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

이와 같이 S 가 구해지고 이로부터 ID_A 가 구해진다.

5.3 익명성 제어

익명성 제어는 익명성 조절 매개변수에 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 추적(owner tracing)과 은행으로부터의 화폐 인출을 식별하기 위한 화폐 추적(coin tracing)이 있다. 소유자 추적에 있어서 익명성 제어 매개변수는 신뢰기관이 지불이 이루어지고 난 후, 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 신뢰기관은 은행으로부터 인출된 화폐를 확인하고 물품 구입에 사용한 것과 인출된 화폐를 연결시킬 수가 있다.

5.3.1 화폐 추적

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

- 과정 1 : 은행은 사용자가 제시한 인출 사본 중 A_1' 을 신뢰기관에게 제공한다.
- 과정 2 : 신뢰기관은 A_1' 로부터 A_1을 계산해낸다.

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

- 과정 3 : 신뢰기관은 A_1을 은행에게 전송한다.
  이때 신뢰기관이 전송해 준 A_1 을 사용자가 생성하여 지불 단계에서 상점에 제공하는 A_1 과 연결시킴으로서 물품 구입 단계 전에 지불과 상관없이 추적 기능을 제공한다.

5.3.2 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 $A_3(\equiv ID_A \cdot (y_T)^v \mod p)$가 추가된다.

- 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 $A_3' \equiv$

〈표 1〉 기존방식들과 제안방식 비교 분석표

	Okamoto-Ohta 방식	Eng-Okamoto 방식	Okamoto방식	Chan-Frankel -Tsiounis 방식	
Off-line	○	○	○	○	
분 할 성	○	○	○	○	
익 명 성	○	○	○	○	
익명성 제어	×	×	×	×	
초과사용 방지	○	○	○	○	
계층적 구조 테이블	○	○	○	○	
서 명 방 식	RSA 은닉 서명 방식	Schnorr 은닉 서명 방식 Brand's 방식	RSA 은닉 서명 방식	Schnorr 은닉 서명 방식 Rang-bounded commitment	
Electronic license	○	×	○	×	
전자면허 발행시 사용하는 방식	Cut-and-choose 방식	•	Bit Commitment 방식	•	
동 전 구 성	$C = (g(B \| b))^{d_A'} \bmod n_A'$	m', sign(m')	$C = (H(N \| b))^{1/e_w} \bmod n_w$	(z, a, b, r)	
예치시 거래 내역서 작성	○	○	○	○	

$ID_A^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하고, 다시 ID_A를 계산한다.

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

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

$$\therefore ID_A \equiv (ID_A^{X_T^{-1}})^{X_T \bmod (p-1)} \bmod p$$

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

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

6. 결 론

인터넷에서 이루어지는 전자상거래에서 가장 중요한 요소 중에 하나가 전자화폐이다. 초기에 전자화폐에 대한 연구는 개인의 사생활을 보호하기 위해 완전한 익명성에 중점을 두고 연구되었다. 하지만 완전한 익명성을 제공함으로써 약탈, 돈세탁 및 불법적인 사용과 같은 범죄 행위에 사용될 가능성이 높아졌다. 따라서 개인의 사생활은 보호하면서 불법적인 사용에 대해 추적할 수 있는 새로운 요구 조건인 익명성 제어가 등장하게 되었다. 하지만 익명성 제어 기능의 남용으로 은행, 신뢰기관 그리고 사용자 사이의 공평성 문제가 발생하게 되었다. 이에 공정성이라는 개념이 도입되었다. 그리고 공정성에 대한 연구가 활발하게 진행되었다.

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 변형한 은닉 KCDSA 서명 방식을 제안하였고, 이를 적용한 전자화폐 시스템을 제안하였다. 향후 전자화폐가 현재보다 발전하기 위해서는 연구에만 전념하지 말고 연구를 통해 제안된 시스템을 실질적으로 구현하는 방향으로 연구가 진행되었으면 한다.

참 고 문 헌

[1] D. Chaum, "Blind Signautures for untraceable payments," *In Advances in Cryptology*, Crypto'82, pp.199-203, 1983.

[2] T. Okamoto and K. Ohta, "Universal Electronic Cash," *In Advances in Cryptology*, Crypto'91, pp.324-337, 1991.

[3] T. Eng and T. Okamoto, "Single-term divisible electronic coins," *In Advances in Cryptology Eurocrypto'94 Proceedings*, pp.313-323, 1994.

[4] T. Okamoto, "An Effieient Divisible Electronic Cash Scheme," *In Advances in Cryptology Crypto'95*, pp.438-451, 1995.

[5] A. Chan, Y. Frankel and Y. Tsiounis, "Easy-come easy-go divisible cash," *In Advances in Cryptology Eurocrypto'98*, pp.561-575, 1998.

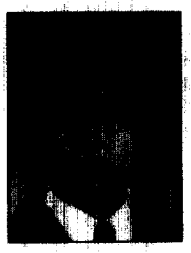
[6] http : // www.tta.or.kr, "Digital Signature Mechanism with Appendix - Part 2 : Certificate-based Digital Signature Algorithm," TTA.KO-12.0001

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

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

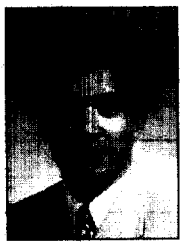
[9] K. H. Kim, Y. J. Eun, C. H. Park, S. C. Goh, "Modified One-Time Password System Proposed," *WISC'98*, pp.75-92, 1998.

[10] Hyung-geun Oh, Im-yeong Lee, "An Efficient Electronic Cash Protocol with Anonymity Control and Divisible Scheme," *Proceedings of KISS*, Vol.25, 1999.



장 석 철

e-mail : scjjang@yahoo.co.kr
1999년 선문대학교 수학과 졸업(학사)
2000년~현재 순천향대학교 대학원 전산학과 석사과정 재학 중
관심분야 : 암호이론, 컴퓨터보안



이 임 영

e-mail : imylee@sch.ac.kr
1981년 홍익대학교 전자공학과 졸업(학사)
1986년 오사카대학 통신공학전공 석사(공학석사)
1989년 오사카대학 통신공학전공 박사(공학박사)
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안