비밀 분산 기법을 이용한 분할 가능한 전자화폐 시스템

장석철, 이임영

순천향대학교, 정보기술공학부

The Divisible Electronic Cash System using Secret Sharing Scheme

Seok-cheol Jang, Im-yeong Lee

Division of Information Technology Eng. Soonchunhyang University

요 약

최근 정보통신기술의 발전과 인터넷의 폭발적인 사용자 증가로 인해 전자상거래가 활성화되고 있다. 또한 전자상거래에서 가장 중요한 시스템인 전자화폐 시스템에 대한 연구와 개발이 활발하게 진행되고 있다. 특히, 전자화폐 시스템의 요구사항 중에 분할성 관련된 연구는 대부분이 계층적 구조 테이블을 이용한 방식이었다. 하지만 이 방식은 많은 메모리가 필요하고, 또한 많은 계산량을 필요로 한다는 단점이 있다. 따라서 본 논문에서는 이러한 문제점을 해결하고, 계층적 구조 테이블을 이용하지 않고 분할성을 제공할 수 있는 또 다른 방식인 비밀분산 기법을 이용하여 새로운 전자화폐 시스템을 제안한다.

I. 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.

전자화폐에 대한 연구 개발은 D.Chaum이 on-line형 전자화폐 시스템을 제안 후 전자화폐가 가져야할 조건을 만족시키는 많은 방식들이 제안되고 있다. 이 중에서 본 논문에서는 전자화폐가 가져야할 조건 중 분할성에 대해서 설명한다.

본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것 임.

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.

따라서 본 논문에서는 이러한 이점을 가지고 있는 새로운 분할 가능한 전자화폐 시스템을 제안한다. 또한, 전자화폐를 분할하여 사용하는 방법을 비밀분산 기법을 적용한다.

II. 기존방식

전자화폐 시스템의 요구사항 중 분할성 관련 연

각는 많이 진행되어왔다. 이 장에서는 분할성을 제공해 주는 기법 중 계층적 구조 테이블을 이용한 기법과 비밀분산 기법을 이용한 기법에 대해 설명한다.

1.계층적구조 테이블을 이용한 분할성

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 노드(V_0)에 있어서 해당 금액은 자식 노드들의 합($V_{00}+V_{01}$)과 같다.
- 어떤 한 노드가 사용되면, 모든 자식 노드와 부모 노드는 사용할 수 없다.
- 어떤 노드도 한 번 이상 사용될 수 없다.

기존방식들 대부분이 이 기법을 이용하여 분할성을 제공해 주는 전자화폐 시스템을 제안하였다[1]~[3]. 하지만 이 기법은 지불하기 전에 완전이진트리를 구성해야 하므로 이를 저장할 수 있는 메모리가 많이 필요하다. 또한 지불시 처리해야할 계산량이 많이 늘어난다는 단점이 있다.

2. 비밀분산기법을 이용한 분할성

Kai-Shimin-Guozhen은 이산대수 문제의 어려움을 기반으로 하는 검증 가능한 비밀 분산 기법을 제안하였다[4]. 이 기법은 비밀값을 n개로 쪼개어 이것을 n명의 사람에게 공개적으로 분배하고 만약 n-1개의 비밀 조각이 모아졌을 때만 비밀값을 복호화할 수 있는 방법이다. 또한 비밀 조각을 받은 n명의 사람들은 이 비밀 조각이 올바르게 쪼개어 졌다는 것을 검증할 수 있는 기법이다. Kai-Shimin-Guozhen은 검증 가능한 비밀 분산 기법을 활용하여 은행으로부터 서명 받은 전자화폐를 가지고 상점에 사용할 경우 전자화폐를 분할하여 사용할 수 있는 전자화폐 시스템을 제안하였다. 하지만, 인출단계에서 기존에 이미 제안된 서명방식을 사용함으로서 매우 많은 통신량을 가지고 있으며, 이중 사용시 이를 방지할 수 있는 방법이 없다는 단점이 있다.

III. 제안방식

이 장에서는 기존방식인 Kai-Shimin-Guozhen의 방식에서 지적되었던 단점을 보완하고, 국내 전자서명 표준인 KCDSA를 이용하여 전자화폐를 인출하는 방법과 이중사용시 이를 방지할 수 있는 방법을 제시한 보다 효율적인 분할 가능한 전자화폐 시스템을 제안한다.

1. 비밀분산 기법

비밀분산 기법이란 비밀 s를 n개의 분산정보 $v_1, v_2, \cdots, v_n$으로 분산부호화하여 특정분산정보의 집합에 대해서만 s의 복호를 가능토록 하는 방식이다.

Shamir는 Lagrange 보간 다항식을 근거로 한 방식을 제안했다. 분산정보는 다음의 $t-1$차의 다항식에 의해 주어진다[5][6].

$$f(x)=a_{t-1}x^{t-1}+\cdots+a_1x^1+a_0 \bmod p \quad (1)$$

단, 여기서 정수치 $a_0=s$이다. 모든 계산은 유한체 $GF(p)$에서 행하고 p는 s, k보다 큰 소수로 한다. $f(x)$가 주어지면 비밀 s는 $s=f(0)$에 의해 계산할 수 있다. k개의 분산정보를 구하기 위해 k개의 값 $x_1, \cdots, x_k$에 대해서 각각 $f(x)$의 수치를 계산한다. .

$$v_i=f(x_i) \qquad i=1,\cdots,k \qquad (2)$$

즉, 각각의 쌍 (x_i, v_i)는 곡선 $f(x)$상의 점으로 주어진다.

t개의 점이 모여 비로서 $t-1$차의 다항식을 유일하게 결정할 수 있다. 따라서 t개의 분산정보는 $f(x)$ 즉 비밀 s를 복원할 수 있다.

한편, t미만의 분산정보에서는 $f(x)$ 및 s를 복원할 수 있는 정보를 얻을 수 없다. t개의 분산정보 $v_1, v_2, \cdots, v_t$가 주어지면, $f(x)$는 Lagrange 다항식으로부터 복원된다.

2. 시스템 계수

- p, q : 소수
- $g \in Z_q$는 $g=h^{(p-1)/q} \bmod p$을 만족한 값
- $x_U \in Z_q$: 사용자의 개인키
- $y_U \equiv g^{x_u} \bmod p$: 사용자의 공개키
- $x_B \in Z_q$: 은행의 개인키
- $y_B \equiv g^{1/x_b} \bmod p$: 은행의 공개키
- ID_U : 사용자의 ID
- FID : 사용자의 가명ID
- ID_M : 상점의 ID

• $h()$: 일방향 해쉬 함수
• $f(x)$: 비밀분산 기법에서 사용할 함수

3. 신원등록단계

사용자는 은행으로부터 전자화폐를 인출받기 전에 인출단계에서 사용하게 될 사용자 가명ID를 신뢰기관에 등록해야 한다. 가명ID를 사용함으로써 은행 및 상점에 대한 사용자의 익명성은 보장된다.

• Step 1

사용자는 랜덤값을 선택하여 다음과 같이 자신의 ID_U를 생성하고, 이를 신뢰기관에 전송한다.

$$a \in {}_RZ_p,\ ID_U \equiv g^a \bmod p \qquad (3)$$

• Step 2

신뢰기관은 랜덤값을 선택하여 다음과 같이 사용자의 가명ID를 생성한다.

$$b \in {}_RZ_p,\ FID \equiv ID_U^b \bmod p \qquad (4)$$

신뢰기관은 사용자의 ID_U, FID와 랜덤값 b를 DB에 저장한 후, FID에 서명을 하여 사용자에게 전달한다.

• Step 3

사용자는 신뢰기관으로부터 받은 서명값을 확인하고, 가명ID인 FID를 얻는다.

4. 인출단계

사용자가 은행으로부터 전자화폐를 발행 받는 단계이다. 이 단계에서는 국내 전자서명 표준인 KCDSA를 변형한 은닉 KCDSA를 이용하여 서명이 이루어지며, 사용자가 발행 받은 전자화폐를 분할하여 사용할 수 있게 비밀분산 기법을 사용한다. 또한, 비밀분산 기법을 사용하기 위해 은행으로부터 발행 받은 전자화폐를 부분전자화폐로 분할하여 사용할 수 있다.

• Step 1

은행은 사용자의 요청에 따라 랜덤하게 $k' \in Z_q$를 선택하여 다음과 같이 계산하여 사용자에게 보낸다.

$$r' \equiv g^{k'} \bmod p \qquad (5)$$

• Step 2

사용자는 랜덤하게 은닉인자 $\alpha \in Z_q$와 $\beta \in Z_q$를 선택하여 r과 은닉된 값 m'을 계산하고, 가명ID FID와 같이 은행에게 전달한다.

$$r \equiv ID_U g^{\alpha} r'^{\beta} \bmod p \qquad (6)$$

$$m' \equiv r\beta^{-1} \bmod q \qquad (7)$$

• Step 3

은행은 다음과 같이 서명을 한 s'과 초과사용시 사용자를 추적할 수 있는 인자 A를 계산한다.

$$H = h(Z \| m') \qquad (8)$$

$$E \equiv m' + H \bmod q \qquad (9)$$

$$s' \equiv x_B E + k' \bmod q \qquad (10)$$

$$A \equiv FID^{x_B} \qquad (11)$$

그리고 비밀분산 기법을 사용하기 위한 함수 $f(x)$의 계수 $a_i \in {}_RZ_p (i = 1, \cdots, k)$를 선택하고, s', A와 같이 사용자에게 전달한다.

• Step 4

사용자는 은행으로부터 받은 s'을 이용하여 s를 구하고 이를 이용하여 검증을 한다.

$$s \equiv s'\beta + \alpha \bmod q \qquad (12)$$

$$ID_U \overset{?}{\equiv} g^{-s} y_B^{r+\beta H} r \bmod p \qquad (13)$$

또한, 은행으로부터 받은 $a_i \in {}_RZ_p$ $(i = 1, \cdots, k)$를 이용하여 사용자는 함수 $f(x)$를 다음과 같이 구성한다.

$$f(x) = A + a_1 x + a_2 x^2 + \cdots + a_k x^k \qquad (14)$$

전자화폐는 $coin = (r, s)$이다. 또한 다음과 같이 $coin$을 이용하여 해쉬체인을 생성한다. 이것은 부분전자화폐를 구성하는데 사용된다.

$$C_i = h(C_{i-1}), (i = 1, \cdots, k,\ C_0 = coin) \qquad (15)$$

5. 지불단계

사용자는 상품을 구입 후, 은행으로부터 받은 전자화폐를 상점에게 지불하는 단계이다. 이 단계에서는 증명 가능한 비밀분산 기법을 사용하여 상점에서 사용자가 올바르게 부분전자화폐를 올바르게 생성했는지를 검증한다. 또한, 이중사용 방지를 위해 Schnorr의 서명기법을 사용한다.

• Step 1

사용자는 상점으로부터 결제요청시 부분전자화폐 $(C_i, f(C_i))$를 구성한다. 그리고 사용자는 랜덤하게 $\sigma_1, \sigma_2 \in {}_RZ_q$를 선택하고 다음과 같이 식을 계산한다.

$$\delta_1 \equiv g^{\sigma_1} \bmod p \qquad (16)$$

$$\delta_2 \equiv g^{\sigma_2} \bmod p \quad (17)$$

$$Message = (ID_M \mid (C_i, f(C_i)) \mid \delta_1) \quad (18)$$

$$e = H(Message) \quad (19)$$

$$d_1 \equiv x_U \delta_2 + \sigma_2 C_i \bmod p \quad (20)$$

$$d_2 \equiv C_i + x_U e \bmod p \quad (21)$$

그리고 사용자는 ID_M, d_1, d_2, δ_2, $(C_i, f(C_i))$, e를 상점에게 전송한다.

• Step 2

상점은 사용자로부터 받은 값들을 이용하여 다음과 같이 부분전자화폐의 유효성을 확인한다.

$$g^{d_1} \stackrel{?}{=} \delta^{C_i} y_U^{\delta_2} \quad (22)$$

또한, 이중사용 여부를 확인하기 위해 다음과 같이 검증을 한다.

$$\gamma = g^{d_2} y_U^{\delta_2} \quad (23)$$

$$e \stackrel{?}{=} h(ID_M \| (C_i, f(C_i)) \| \gamma) \quad (24)$$

6. 예치단계

사용자가 지불한 부분전자화폐를 전송하기 위해서 상점은 거래내역서 T를 은행에 전송한다. 은행은 전송받은 T를 DB저장하고, 사용자가 전자화폐 총금액에 대한 초과사용 여부를 확인한다.

$$T = (ID_M, (C_i, f(C_i))) \quad (25)$$

IV. 제안방식 분석

제안방식은 기본적으로 사용자의 익명성을 보장하고 있으며, 상점에서는 이중사용에 대한 검출이 가능하며, 은행에서는 전자화폐 총금액을 초과사용시 비밀분산 기법에 의해 사용자를 추적할 수 있다.

1.이중사용 방지

만약 사용자가 부분전자화폐 $(C_i, f(C_i))$를 재사용할 경우, 상점에서는 C_i에 대해 (e, d_2)와 (e', d_2')을 얻는다. 따라서 d_2와 d_2'에 의해서 다음과 같이 사용자의 개인키값을 계산할 수 있으므로 사용자는 이중사용을 하지 못한다.

$$x_U \equiv \left(\frac{d_2 - d_2'}{e - e'}\right) \bmod p \quad (26)$$

2. 초과사용 방지

만약 사용자가 부분전자화폐를 k개 보다 초과사용되었을 경우, 은행은 저장된 $(C_1, f(C_1))$, $(C_2, f(C_2))$, …, $(C_{k+1}, f(C_{k+1}))$로부터 Lagrange 다항식을 이용하여 추적인자 A를 검출할 수 있다. 은행은 추적인자에 다음과 같이 계산하여 얻어진 사용자의 가명ID를 신뢰기관에 전송한다.

$$FID = (A)^{1/x_B} = (FID^{x_B})^{1/x_b} \quad (27)$$

신뢰기관은 자신의 DB에서 FID에 해당하는 사용자 ID_U를 검색하여 이를 법집행기관에 전송해 준다.

V. 결론

인터넷에서 이루어지는 전자상거래에서 가장 중요한 요소 중에 하나가 전자화폐 시스템이다. 또한 전자화폐 관련 연구도 활발하게 진행되어 왔다. 특히, 익명성과 익명성 제어에 관련된 연구는 많이 되어 왔지만 분할성 관련 연구는 많지 않다. 따라서 본 논문은 기존방식을 분석하였고, 분할기법으로 비밀분산 기법을 설명하였다. 이를 토대로 지적되었던 단점을 보완하고, 국내 전자서명 표준인 KCDSA를 이용하여 전자화폐를 인출하는 방법과 이중사용시 이를 방지할 수 있는 방법을 제시한 보다 효율적인 분할 가능한 전자화폐 시스템을 제안했다.

참고문헌

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

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

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

[4] C.Kai, W.Shimin, X.Guozhen, "A New Approach to Divisible E-cash System", SEC2000, 2000

[5] Shamir A., "How to share secret", Comm. of the ACM, 22, pp.612-613, 1979

[6] 송유진, "비밀분산방식의 새로운 구성법", 통신정보보호학회논문지 제7권 제4호, pp.3-10, 1997