해쉬 체인에 기반한 분할 가능 전자화폐 시스템의 설계

용승림[0] 이은경 이상호
이화여자대학교 컴퓨터학과
{dragon[0], shlee}@ewha.ac.kr

Design of Divisible Electronic Payment System based on Hash Chain

Seung-Lim Yong[0] Eun-Kyoung Lee Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

전자화폐는 기존의 화폐가 가져야 하는 법적인 효력과 안전성 등의 기능을 그대로 가지면서 별도의 기기나 또는 컴퓨터 등에 소프트웨어 형태로 존재하는 전자지갑에 의해 관리된다. 전자화폐는 안전성을 제공해야 하고, 이중사용이 방지되어야 한다. 또한 동전의 다중사용 가능성이나 분할성을 만족시킴으로서 사용자 편리성과 효율성을 증대시킬 수 있다. 분할성은 사용자가 전자화폐를 발급받는 경우 발급받은 전자화폐를 사용자가 원하는 대로 나누어 사용할 수 있는 성질로써 거스름돈의 발생을 줄여 효율성을 증대시킬 수 있다. 본 논문에서는 이중 해쉬함수를 이용하여 동전을 생성하고 지불인증을 이용하여 생성된 동전을 마음대로 분할하여 사용할 수 있는 방법을 제안한다. 제안된 방법은 사용자의 익명성을 제공하지는 못하지만 해쉬함수를 이용하여 효율적이고 위조 불가능한 동전을 생성하며, 분할성을 만족함으로써 편리하게 이용가능하다는 장점이 있다.

1. 서 론

컴퓨터와 통신망을 이용한 전자상거래에서는 상품의 구입과 지불의 시점이 다르기 때문에 발생하는 동시성의 결여와 비대면(非對面) 거래로 인한 상대방에 신뢰성 결여로 기존의 지불 행위와 같이 안전하고 편리하게 지불을 수행하기가 어렵다. 이러한 환경에서 안전하게 사용할 수 있는 지불 방법이 전자화폐이다.

전자화폐란 액면가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보이다[1]. 전자화폐는 기존의 화폐가 가져야 하는 법적인 효력과 안전성 등의 기능을 그대로 가지면서 별도의 기기나 또는 컴퓨터 등에 소프트웨어 형태로 존재하는 전자지갑에 의해 관리된다. 전자화폐는 실물화폐가 가지고 있는 기능 뿐만 아니라 효율성과 사용자 편리성 그리고 디지털 데이터가 가지는 특징으로 발생하는 문제점 등을 해결하기 위해 위조가 불가능하도록 하는 안전성(security)을 제공해야 하고, 디지털 정보로 표시되는 화폐가 한번 이상 복사되어 사용되는 이중사용(double-spending)이 방지되어야 한다. 전자화폐를 사용하는 사용자의 익명성이 보장되어야 한다. 또한 발급받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 분할성(divisibility)을 제공하여 사용자 편리성과 효율성을 증대시킬 수 있다. 이러한 여러 전자화폐의 요구조건 중에서 분할성은 사용자가 전자화폐를 발급받는 경우 발급받은 전자화폐를 사용자가 원하는 대로 나누어 사용할 수 있는 성질이다. 즉 사용자가 보유하고 있는 전자화폐의 총액을 초과하지 않는 범위 내에서 사용자가 전자화폐를 나누어 사용할 수 있음을 말한다.

본 논문에서는 이중 해쉬함수를 이용하여 동전을 생성하고 지불인증을 이용하여 생성된 동전을 마음대로 분할하여 사용할 수 있는 방법을 제안한다. 사용자의 익명성을 제공하지는 못하나 해쉬함수를 이용하여 효율적이고 위조 불가능한 동전을 생성하며, 분할성을 만족함으로써 편리하게 이용가능하다는 장점이 있다.

2. 관련 연구

2.1 해쉬체인에 기반한 전자지불 시스템

전자화폐의 인증을 위하여 이용하는 공개키 전자서명 방식은 계산상 매우 복잡하기 때문에 동전 각각에 서명하기 위해서 Payword 시스템은 해쉬함수를 이용하여 동전을 구성하였다[2]. 사용자는 식 (1)과 같이 해쉬함수를 적용하여 역방향으로 동전 $w_1, w_2, \ldots, w_n$을 생성하고 루트 w_0에 은행의 서명을 받는다.

$$w_i = h(w_{i+1}), \quad (i = n-1, n-2, \ldots, 0) \qquad (1)$$

사용자는 상점에 서명된 w_0를 보내고 w_1부터 지불금액만큼 동전을 지불한다. 지불된 모든 동전은 식(1)에 기반하여 루트가 w_0가 되는지 확인함으로써 정당성을 검증받는다.

이중해쉬 체인은 PayWord에서 제안한 동전 구성 방법에 의해 생성한 두 개의 해쉬체인 한쌍을 하나의 동전을 구성하는데 이용한다[3]. 즉, 해쉬체인을 두 개 생성한 후 각 체인의 요소들을 서로 역순으로 번호가 같은 것끼리 쌍을 이루어 동전을 구성한다. 이 방식은 동전을 구성하는 한 체인의 종자값(seed)을 알아냈다 하더라도 다른 체인의 종자값도 알아야만 위조가 가능하다는 특징을 이용하여 동전의 위조에 대한 안전성을 향상시켰다.

2.2 분할 가능한 전자지불 시스템

분할 가능한 전자지불 시스템이란 동전의 분할성을 만족하는 전자화폐이다. 분할성은 사용자가 전자화폐를 발급 받는 경우 사용자가 보유하고 있는 전자화폐의 총액을 초과하지 않는 범위 내에서 사용자가 전자화폐를 나누어 사용할 수 있는 성질이다.

1991년 T. Okamoto 등은 이진트리 구조를 이용한 분할 가능한 효율적인 전자화폐 프로토콜을 제안하였다[4]. 이진 트리 구조에서는 트리의 각 노드는 동전의 액면가를 나타내며 트리의 자식 노드의 금액의 합이 부모 노드의 금액이 되는 방식으로 각 노드별로 금액을 준다.

대부분의 분할 사용 가능한 전자화폐 프로토콜에서는 이진 트리를 이용한 접근 방식을 이용하여 화폐의 분할 사용기능을 구현하고 있다. 그러나 이 방식은 계산량이 트리의 깊이(depth)에 따라 변하고 복잡한 수학식을 사용하고, 법(mod) 연산 방식을 사용함으로서 계산량이 많아지는 단점이 있다[5].

3. 해쉬체인에 기반한 분할가능한 전자화폐 시스템

전자화폐 시스템은 이중해쉬 체인을 여러 개로 구성하여 동전마다 다양한 액면 금액을 갖고, 동전을 분할하여 지불할 경우 지불인증을 이용하여 동전의 정당성을 입증받을 수 있다.

3.1 지불인증

각 사용자는 동전을 분할하여 지불할 경우에 지불인증을 이용한다. 사용자는 은행으로부터 동전 분할에 대한 권한을 지불인증을 통하여 부여받은 후 동전을 분할하여 지불에 이용한다. 이러한 지불인증은 동전을 인출할 당시에 그 동전보다 한 단계 낮은 액면금액에 대하여 은행으로부터 대리서명을 할 수 있는 정보를 제공받아 이루어지게 된다.

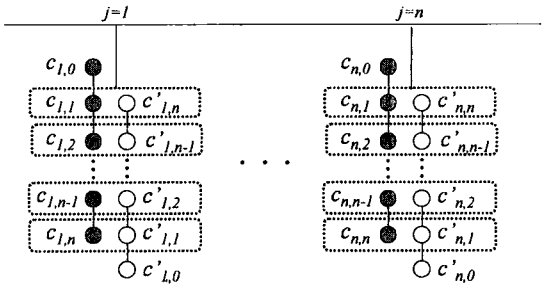
3.2 프로토콜

3.2.1 인출 프로토콜

인출 프로토콜은 크게 지불인증 서명과정과 동전의 생성과정으로 나뉜다.

■ 동전 생성 과정

다중 해쉬체인은 그림 1과 같이 이중 해쉬체인이 여러 개로 구성된 형태로서, 이중 해쉬체인 하나마다 번호를 가지고 있고 이 번호에 따라 액면금액을 다르게 설정한다. 해쉬체인의 번호가 j인 하나의 체인내의 모든 동전은 10^{j-1}원의 액면가치를 가진다. 예를 들어 해쉬체인의 번호가 j라 할 때 $j=1$이면 체인의 동전들의 액면금액은 1원, $j=2$이면 액면금액은 10원, $j=3$이면 100원의 액면가치를 갖는다.



동전의 서명과정은 다음과 같다.

1) 사용자는 해쉬체인의 번호 j에 따라 액면금액이 다른 이중 해쉬 체인의 한쪽 체인을 구성하기 위하여 임의의 수 c_{j,n_j} 을 선택하고 다음을 계산한다.

$$c_{j,i} = h(c_{j,i+1}) \quad (i=n-1, n-2, \cdots, 0)$$

2) 은행은 임의의 수 c'_{j,n_j}을 선택한 후, 해쉬함수를 적용하여 다음을 계산한다.

$$c'_{j,i} = h(c'_{j,i+1}) \quad (i=n-1, n-2, \cdots, 0)$$

3) 위에서 생성된 동전의 한쪽 체인을 사용자에게 비밀리에 보내준다.

4) 사용자는 생성된 c_{j,n_j}에 n_j번 해쉬함수를 적용하여 $c_{j,0}=h^{n_j}(c_{j,n_j})$를 생성한 후 다음을 은행에게 보낸다.

$$S(c_{j,0}, j, n_j, SK_C)$$

5) 은행은 생성된 c'_{j,n_j} 에 n_j번 해쉬함수를 적용하여 $c'_{j,0}$를 계산하고 사용자에게서 받은 $c_{j,0}$를 이용하여 $Root_j$를 계산한다.

$$c'_{j,0} = h^{n_j}(c'_{j,n_j}), \quad Root_j = h(c_{j,0} \| c'_{j,0} \| j \| n_j)$$

6) 은행은 $Root_j$에 서명한 $R_j = S(n_j Root_j, SK_B)$를 사용자에게 보내준다.

■ 지불인증 서명과정

1) 은행은 임의난수 k_B를 선택하여 $r_B = g^{k_B}$를 계산하고 $s_B = x_B h(Cert_C, r_B) + k_B$를 계산한다.

2) 은행은 사용자에게 $\langle r_B, s_B \rangle_{SK_c}$를 비밀리에 보낸다.

3) 사용자는 지불인증을 위한 대리서명키로 $P-SK_C = s_B$, $P-PK_C = g^{P-SK_C}$를 이용한다.

3.3.2 지불 및 예치 프로토콜

■ 분할하지 않고 지불할 경우

동전을 분할하지 않고 지불할 경우 지불 프로토콜은 다음과 같다.

1) 사용자는 상점에게 아래의 항목들을 보낸다.

$$S(c_{j,0}, c'_{j,0}, j, n_j, R_j, ID_C), Cert_C$$

2) 상점은 $Cert_C$과 R_j를 검증한다.

3) 상점의 확인이 끝나면, 사용자는 구매 내역과 상품의 금액의 합계에 맞도록 동전을 지불한다.

$PR,(i, c_{j,i}, c'_{j,n_j-(i+1)})\ldots(i+k, c_{j,i+k}, c'_{j,n_j-(i+k+1)})$

4) 상점은 $h^i(c_{j,i}) = c_{j,0}$, $h^{n_j-i}(c'_{j,n_j-i}) = c'_{j,0}$을 확인하여 동전의 유효성을 확인한다.

■ 분할하여 지불할 경우

적은 액면금액의 동전이 부족할 경우 액면금액이 높은 동전을 분할하여 지불한다. 이때에는 은행으로부터 미리 받아둔 지불인증을 이용하여 동전에 서명을 수행하고 이들 동전을 지불에 이용한다.

1) 사용자는 $c'_{j-1,n_{j-1}} = c'_{j,n_j} \cdot s_B$와 임의의 수 $c_{j-1,n_{j-1}}$를 선택하고 이들을 n_{j-1}번 해쉬함수를 적용하여 다음을 생성한다.

$$c_{j-1,0} = h^{n_{j-1}}(c_{j-1,n_{j-1}}),\ c'_{j-1,0} = h^{n_{j-1}}(c'_{j-1,n_{j-1}})$$

2) 사용자는 은행의 대리서명을 이용하여 새로운 동전에 서명을 수행한다.

$$m = h(c_{j-1,0}||c'_{j-1,0}||j-1||n_{j-1})$$
$$R_{j-1} = S(n_{j-1}m, P-SK_C)$$

3) 사용자는 상점에게 아래의 항목들을 보낸다.

$$\langle c_{j-1,0}, c'_{j-1,0}, j-1, n_{j-1}, R_{j-1}, r_B\rangle_{SK_C},\ Cert_C$$

4) 상점은 $Cert_C$를 확인하고 R_{j-1}를 은행의 공개키를 이용하여 서명을 확인한다.

$$V(SK_B^{h(ID_C, r_B)} r_B, m, R_{j-1}) = true$$

5) 상점의 확인이 끝나면, 사용자는 구매 내역과 상품의 금액의 합계에 맞도록 동전을 지불한다.

$$PR,(i, c_{j-1,i}, c'_{j-1,n_{j-1}-(i+1)})$$
$$\ldots(i+k, c_{j-1,i+k}, c'_{j-1,n_{j-1}-(i+k+1)})$$

6) 사용자의 동전들을 확인한다.

사용자가 분할된 동전을 다 사용하고 또 분할하고자 할 때는 종자값을 $c'_{j,n_{j-1}} \cdot h(s_B)$으로 하여 동전을 생성한다.

4. 결과 및 분석

본 논문에서 제안한 전자화폐 시스템은 액면가별로 다른 해쉬 체인을 이용하였으며, 서로 다른 액면가를 가지는 동전들 사이에 분할성을 만족하게 함으로서 오프라인(off-line)상에서 더 효율적이도록 설계하였다.

4.1 안전성

4.1.1 위조 방지

■ 동전에 대한 위조방지

제안된 시스템에서 사용된 모든 해쉬함수는 모두 일방향 함수이다. 따라서 해쉬 체인 생성시 사용되는 해쉬함수에 의해 그 역방향으로의 계산이 불가능함으로 동전을 지불한 후 지불받은 동전을 통해서 아직 사용되지 않은 동전을 알아낼 수 없다.

분할하여 사용될 동전은 은행으로부터 지불인증을 받을 때 한쪽 체인의 종자값을 $c'_{j,n_j} \cdot s_B$로 계산함으로써 사용자는 분할할 동전의 일부를 이용해야만 정당한 동전으로 분할할 수 있으며 은행이 지불인증에 대한 사용자의 정보를 가지고 있으므로 사용자가 동전을 위조하여 생성할 경우 이를 막을 수 있다.

■ 지불인증에 대한 위조방지

사용자는 은행으로부터 지불인증을 받을 때 은행의 비밀키를 알 수 없기 때문에 은행의 서명을 올바르게 생성할 수 없다.

4.1.2 이중 사용

사용자가 은행에서 인출받은 동전을 이중 사용할 경우 은행은 인출시 사용자로부터 받은 정보를 이용하여 사용자의 이중 사용여부를 알아낼 수 있다. 사용자가 분할한 동전을 이중 사용할 경우에도 분할된 동전은 그 전의 동전 정보를 가지고 있기 때문에 은행이 이중사용 여부를 알아낼 수 있다.

4.1.3 분할성

제안된 전자화폐는 오프라인형으로서 은행의 비 개입으로 인한 사용의 편리성을 만족시켰을 뿐만 아니라 지불인증을 사용하여 분할성을 만족한다.

5. 결론 및 향후 연구과제

전자화폐는 안전성, 이중 사용의 방지, 오프라인과 같은 기본적인 요구조건 외에 부가적으로 분할성, 양도성과 같은 요구조건들을 만족함으로서 효율성을 높일 수 있다. 본 논문에서는 다중 해쉬체인을 이용하여 안전하면서 액면가가 다른 동전들을 생성하고, 액면가가 서로 다른 동전들 사이에 분할이 가능하게 설계하였다. 해쉬체인을 기반으로 하여 계산이 빠르며 지불인증을 이용하여 동전을 분할하여 지불할 경우 은행의 서명을 받지 않아도 됨으로써 효율성을 증대시켰다.

참고문헌

[1] 이만영 외, *전자상거래 보안 기술*, 생능 출판사, 1999.

[2] R. L. Rivest and A. Shamir, "Payword and MicroMint: Two Simple Micropayment Schemes," CryptoBytes, (RSA Laboratories, Spring 1996), pp.7-11, 2(1), May 7, 1996.

[3] K. Q. Nguyen, Y. Mu and V. Varadharajan, "Micro-Digital Money for Electronic Commerce," In Proceedings of the 13th Annual Computer Security Applications Conference(ACSAC'97), pp.2-8, Los Alamitos, CA, USA, 1997.

[4] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme," In Proceedings of Crypto'95, Lecture Notes in Computer Science, pp.438-451, Springer-Verlag, Berlin, Germany, 1995.

[5] Y. Frankel and A. Chan, "Easy-Come-Easy-Go Divisible Cash," In Eurocrypt '98, Lecture Notes in Computer Science, pp. 561-575, Springer-Verlag, Helsinki, Finland, June 1998.