Nyberg-Rueppel 전자 서명에 기반한 새로운 분할 가능한 전자 화폐 시스템

김서진∪ 박근수
서 울 대 학 교 컴 퓨 터 공 학 부
{sjkim, kpark}@theory.snu.ac.kr

A New Divisible E-Cash System Based on Nyberg-Rueppel Signature

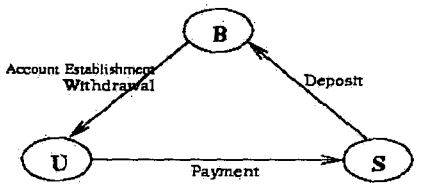
Seojin Kim∪ Kunsoo Park
School of Computer Science and Engineering, Seoul National University

요 약

분할 가능한 전자 화폐 시스템(divisible e-cash system)은 임의의 금액을 지불할 수 있는 전자 화폐 시스템이다. 현재까지 제안된 가장 효율적인 분할 가능한 전자 화폐 시스템은 Chan, Frankel, Tsiounis가 [9]에서 제시한 시스템이다. 본 논문에서는 Okamoto 시스템[2]의 구조를 그대로 따르면서 인출 프로토콜에 [11]의 방식을 응용한 새로운 분할 가능한 전자 화폐 시스템을 제시한다. 본 논문에서 제시한 시스템은 [9]에서 제시된 시스템보다 효율적인 분할 가능한 전자 화폐 시스템으로서 인출과 지불시에 [9]에서 제시된 시스템보다 더 적은 계산량을 필요로 한다.

1 서론

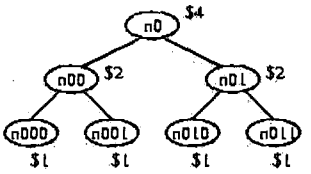
추적 불가능한 off-line 전자 화폐는 최근 암호학 분야에서 널리 연구되어 왔다.([1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11], etc). 전자 화폐 시스템은 사용자(U), 은행(B), 상점(S) 세 참여자로 구성된다([그림 1]). 사용자(U)는 계좌 개설 프로토콜을 통해 은행(B)에 계좌를 개설하고, 그 계좌로부터 인출 프로토콜을 통해서 전자 현금을 인출한다. 그리고 사용자(U)는 상점(S)에서 물건을 구입할 때 지불 프로토콜을 통해 전자 현금을 상점(S)에 지불한다. 후에 상점(S)은 사용자(U)들로부터 받은 전자 현금들을 예금 프로토콜을 통해 다시 은행(B)에 예금한다. 추적 불가능한 off-line 전자 화폐에서 "off-line"은 사용자(U)와 상점(S)이 지불 프로토콜을 수행함에 있어 은행(B)과의 통신이 이루어지지 않음을 의미하고, "추적 불가능"은 전자 화폐가 익명성을 가짐을 뜻한다.



[그림 1] 전자 화폐 시스템

전자 화폐가 실용화되려면 사용자가 전자 화폐를 이용하여 임의의 금액을 지불하는 것이 가능해야 한다. 이를 위해 분할 가능한 전자 화폐는 사용자의 익명성을 보장하면서 사용자(U)와 상점(S)간의 데이터 통신량과 계산량에 큰 부하를 주지 않는 합리적인 해결책이 된다. 분할 가능한 동전이란 일정한 가치를 지닌 동전으로 이 동전의 총 가치를 초과하지 않는 범위에서 여러 번에 걸쳐 사용될 수 있다. 동전의 총 가치 이상을 사용하는 것을 초과 지불(over-spending)이라고 한다.

[6]에서 제안된 이후로 모든 분할 가능한 전자 화폐의 동전은 이진트리로 표현되어왔다. [그림 2]는 $1까지 나누어 쓸 수 있는 $4짜리 동전의 이진트리 구조를 나타낸다. 이진트리의 루트는 동전의 총 가치를 나타내고, 각 노드는 부모노드의 가치의 절반을 나타낸다. 분할 가능한 전자 화폐 시스템에서 초과 지불을 방지하기 위해서는 동전 사용에 있어 루트 경로 법칙(root route rule)과 동일 노드 법칙(same node rule)을 지켜야 한다. 루트 경로 법칙은 루트 노드에서 단말노드에 이르는 모든 경로상에서 단 한 개의 노드만이 사용될 수 있다는 법칙이며, 동일 노드 법칙은 한 노드를 두 번 이상 사용할 수 없다는 법칙이다.



[그림 2] 분할 가능한 전자 화폐에서 의 동전을 나타내는 이진트리 구조

지금까지 분할 가능하며 추적 불가능한 여러 가지 off-line 전자 화폐 시스템들이 제안되었다[2, 4, 5, 6, 9, 10]. [2]에서는 분할 정밀도 N = (동전의 총 가치)/(분할 가능한 최소 단위)일 때 모든 프로시져가 $O(\log N)$에 수행될 수 있는 효율적인 분할 가능한 전자 화폐 시스템을 처음으로 제안하였고, 이 결과는 [12]에서 근사적으로 최적임이 증명되었다. [2]의 전자 화폐 시스템에서는 계좌 개설 과정에서 사용자(U)에게 동전을 인출할 수 있는 허가증을 주고 인출 과정에서 이 허가증을 이용하여 동전을 인출한다. [2]에서 제시한 전자 화폐 시스템의 단점은 허가증을 얻기 위한 계좌 개설 프로토콜에 약 4000번의 다중 멱승연산(multi-exponentiation)이 소요된다는 점이다. [2]의 전자 화폐 시스템이 가진 또 다른 문제점으로는 사용자가 하나의 허가증을 이용하여 여러 개의 동전을 인출하게되면 이 동전들은 서로 연관성을 갖게 된다는 점이다. 이처럼 한 사용자가 하나의 허가증을 이용하여 여러 개의 동전을 인출하여 사용할 경우 현실에서의 여러 요인들(예를 들어, 동전 사용지역의 국부성, 사용날짜, 사용빈도 등)에 의해 사용자의 신원이 밝혀질 가능성이 커진다[13]. 현재까지 제안된 가장 효율적인 분할 가능한 전자 화폐 시스템인 [9]에서는 [2]의 전자 화폐 시스템의 골격을 그대로 유지하면서 [2]의 문제점이었던 계좌 개설 프로토콜의 방대한 계산량을 현저히 감소시켰다. [9]의 기본 아이디어는 계좌 개설과 인출시에 Brands의

프로토콜[3]을 변형하여 사용한 것이다. 이를 통해 계좌 개설시의 멱승연산 회수를 수십 번으로 감소시킴으로써 계좌 개설 기능이 인출에 포함되는 것이 가능해졌다. 즉, 매 인출마다 허가증을 획득하는 것이 가능해짐으로써 [2]가 가진 또 다른 문제점이었던 동전들 사이의 연관성을 없앰과 동시에 효율성도 획득하였다.

한편, [11]에서는 Nyberg-Rueppel 전자서명 방식을 이용한 새로운 추적 불가능한 전자 화폐 시스템을 제안하고, 이 방식과 Brands의 전자 화폐 시스템[3]을 비교하였다. 비교 결과 동전 크기로 볼 때 Brands의 시스템[3]에서는 6개의 항이 사용되고 Nyberg-Rueppel 전자 서명을 이용했을 때는 5개의 항이 사용된다. 또, 멱승연산의 개수로 볼 때 인출 프로토콜에 있어서 Brands의 시스템[3]에서는 7번의 멱승연산이, Nyberg-Rueppel 전자 서명을 이용했을 때는 5번의 멱승연산이 사용된다. 따라서 Brands의 시스템[3]보다 [11]에서 제안한 Nyberg-Rueppel 전자 서명을 이용한 전자 화폐 시스템이 더 효율적이라고 할 수 있다. [11]에서 제안한 전자 화폐 시스템은 동전의 분할 가능성을 제공하지는 않는다.

본 논문에서는 지불 프로토콜과 예금 프로토콜은 [9]의 프로토콜을 그대로 적용하고, 인출 프로토콜에는 [11]에 소개된 Nyberg-Rueppel의 전자서명 방식에 기반한 프로토콜을 응용한 새로운 분할 가능한 전자 화폐 시스템을 제안한다. 본 논문에서 제안하는 분할 가능한 전자 화폐 시스템은 [9]에서 제안한 전자 화폐 시스템보다 인출과 지불시에 더 적은 수의 멱승연산을 사용하면서, [9]와 마찬가지로 한 사용자가 인출한 동전들 사이에 연관성이 존재하지 않는다.

2 프로토콜

은행 초기화 프로시저(Bank Initialization Procedure)

은행 B는 보안 계수 k와 H를 선택하고, $\delta > (2k+2)/H$ 와 $P = 2Q+1$, $|Q| = 2(1+\delta)H+6$를 만족시키는 두 소수 P, Q를 선택한다. B는 또한 그룹 G_Q의 원시근 g, 비밀키 $x \in_R Z_Q$, 임의의 두 수 w_1, w_2, 그리고 해쉬 함수들 $H, H_0, H_1, \ldots$ [14]을 선택한다.

B는 이제 G_Q에 대한 설명(즉 P와 Q), 원시근 g, 공개키 $g_1 = g^{w_1}$, $g_2 = g^{w_2}$, $h_1 = g_1^x$, $h_2 = g_2^x$ 그리고 해쉬 함수 $H, H_0, H_1, \ldots$를 공개한다.

2.1 인출 프로토콜

인출 프로토콜을 수행하기 위해 먼저 사용자(U)는 은행(B)과 인증된 채널을 설정한다.

1. U : $p \equiv 3 \bmod 8$, $q \equiv 7 \bmod 8$ 이면서 $|p| = |q| \le H = (|Q|-6)/[2(1+\delta)]$을 만족시키는 두 소수 p와 q를 선택하여 p, q의 곱 $N(=pq)$ 을 구한다.
   그리고 $I' = g_2^{\,p} \pmod P$을 B에게 전송한다.
2. U, B : 보안 계수 k와 범위 H를 이용하여 범위 한정 공약(range-bounded commitment)을 수행함으로서 U는 B에게 자신이 I'의 g_2에 대한 표현(representation), 즉 p를 알고 있으며 p가 $|p| \le (1+\delta)H$를 만족시킴을 보인다. 이때 범위 한정 공약 프로토콜은 [9]의 것을 이용하며 대화형(interactive) 방식으로 한번의 반복을 수행한다.
3. B : $I' \neq \{1, g_2\}$, $g_1 I' \neq 1$임을 확인한 후 $I = I' g_1 \pmod P = v$를 U의 신원으로서 기록한다. 그리고 $l \in_R Z_Q$를 선택한 뒤 $\eta = v^l \pmod P$와 $w = v^x \pmod P$를 U에게 전송한다.
4. U : 임의의 정수 $x_1, x_2 \in_R Z_Q$ 를 선택한다.
   $\alpha = w^q \pmod P$, $\beta = v^q \pmod P$, $\lambda = h_1^{x_1} h_2^{x_2} \pmod P$,
   $Y = g_1{}^q \pmod P$를 계산하고, 이들을 이용하여
   $m = H(N, Y, \alpha, \beta, \lambda)$을 계산한다.
   임의의 정수 $a, b \in_R Z_Q{}^*$를 선택하여
   $r = m\,\beta^a\,\eta^b \pmod P$를 구하고 이를 이용하여
   $m' = r/b \pmod Q$를 계산한 뒤 m'를 B에게 전송한다.
5. B : U의 계좌에서 해당금액을 감하고,
   $s' = m'x + k \pmod Q$를 U에게 전송한다.
6. U : $s \equiv s'b + a \pmod Q$를 구하여
   $m = \beta^{-s}\,\alpha^r\,r \pmod P$ 가 만족되는지 검사한다.
   만족된다면 $[\alpha, \beta, \lambda, r, s]$와 N, Y 는 유효한 동전을 표현한다.

2.2 지불 프로토콜

분할 가능한 전자 화폐 시스템에서 지불은 동전 인증과 액면가 공개의 두 단계로 나뉘어서 이루어진다. 동전 인증에서는 동전에 대한 은행의 서명의 유효성을 확인한다. 액면가 공개에서는 실제로 지불하려는 액수를 밝히고 초과 지불이 일어날 경우 사용자의 신원을 추적할 수 있는 정보를 상점(S)에게 제공한다.

[2]의 지불 프로토콜에서는 동전 인증 프로토콜을 통해 상점(S)은 합성수 N에 대한 은행(B)의 서명의 유효성을 판별하고, 액면가 공개 프로토콜을 통해 사용자(U)는 동전을 이진트리 구조로 정의하고 지불하려는 액수에 맞는 노드들에 대한 정보를 상점(S)에게 공개한다. 만약 사용자(U)가 초과 지불을 했을 경우 N은 인수분해 되어서 사용자(U)의 신원이 밝혀진다.

본 논문에서 제안하는 분할 가능한 전자 화폐 시스템은 [11]에서 사용한 Nyberg-Rueppel 전자서명 방식을 이용했으므로 동전 인증에 있어서 은행(B)의 서명의 유효성을 검사하는 부분이 바뀌는 것을 제외하면 [2]의 지불 프로토콜을 그대로 받아들인 [9]의 지불 프로토콜과 기본적으로 같다.

동전 인증

1. U : 동전정보를 S에게 보낸다. 즉, $N, Y, (\alpha, \beta, \lambda, r, s)$를 S에게 보내다. 이때 N과 Y는 인출 프로토콜에서 정의한대로 $N = pq$, $Y = g_1{}^q$이다.
2. S : 동전의 유효성을 검사한다.
   a. $(\alpha, \beta, \lambda, r, s)$가 $m = H(N, Y, \alpha, \beta, \lambda)$일 때 $m = \beta^{-s}\alpha^r r$을 만족하는지 검사한다.
      $Y \neq g_2$, $Y \neq g_2{}^N$, $(-1/N) = 1$, $(2/N) = -1$ 을 만족하는지 검사한다. 이때 (a/N)은 modulo N에 대한 a의 Jacobi symbol을 나타낸다.
   b. q가 올바르게 선택되었음을 증명한다. 이 과정에서 U와 S는 범위 한정 공약[9]를 수행함으로서 U가 Y의 g_1에 대한 표현(representation), 즉 q를 알고 있으며 q가 $|q| \le (1+\delta)H$를 만족시킴을 보인다. 이때 범위 한정 공약에 있어서 시험값(challenge) e는 날짜, 상점 정보, 구매내용, 지불된 노드에 대한 정보 등으로부터 얻어진 해

쉬값을 사용하며 [9]에서처럼 비대화형(non-interactive) 방식으로 2번의 반복을 거친다.

c. $g_2^N Y = \beta$ 가 만족되는지 검사한다.

d. U가 동전을 생성함에 있어 부정을 저지르지 않았는지를 검사하기 위해 N이 처음 $|N|$개의 3 mod 4와 동치류인 소수들로 나누어 떨어지는지를 검사한다. 이것은 [7]에 소개된 방식으로 U가 부정을 저질렀을 경우 U의 신원을 쉽게 추적할 수 있도록 해준다. U의 신원을 추적하기 위한 프로토콜 또한 [7]에 있는 프로토콜을 따른다.

액면가 공개

[2]의 액면가 공개 프로토콜을 그대로 사용하되 [2]에서의 동전 (C, N) 대신 (N, Y)를 사용한다. 만약 사용자(U)가 노드 법칙을 어기게 되면, 즉 초과 지불이 발생하면 액면가 공개 프로토콜을 통해 사용자(U)가 공개한 정보들에 의해서 사용자(U)의 신원이 밝혀진다.

2.3 예금 프로토콜

상점(S)는 은행(B)에 지불 내역 기록서(transcript)를 전송한다.

3. 효율성

본 논문에서 제시한 분할 가능한 전자 화폐 시스템의 효율성을 평가하기 위해 [9]에서와 같은 파라미터를 이용하겠다. $H=|p|=|q|=256$, $k=40$, $N=512$ bits, $|Q|=688$(따라서 $\delta \approx 0.33$), $|P|=689$ 이며 동전을 이루는 이진트리는 18-레벨로 \$1000를 1 cent까지 나누어 사용할 수 있는 것으로 가정한다. 또한 멱승연산보다 훨씬 빠른 무작위 해쉬 함수가 존재하며, 특별한 설명이 없는 한 전처리(pre-processing)는 하지 않는 것으로 한다.

동전 하나를 위해서 사용자(U)가 저장해야 하는 정보 $(p, q, (\lambda, r, s))$의 양은 323 Bytes로 [9]에서와 같다. 참고로 Brands의 시스템[3]에서 위에서 정한 파라미터들을 사용했을 경우 동전 하나를 위해 사용자(U)가 저장해야 하는 정보는 384 Bytes이다.

인출 프로토콜에 있어서 데이터 계산량과 전송량을 생각해 보자. [9]의 경우 인출 프로토콜을 수행함에 있어서 약 16번의 멱승연산 이 필요하다. ([9]에서는 12번의 멱승연산이 필요하다고 했으나 이것은 마지막에 은행의 서명에 대한 유효성을 판별하는 부분을 제외시킨 것이다.) 그러나 본 논문에서 제시한 분할 가능한 전자 화폐 시스템에서는 인출 프로토콜에 있어서 약 12번의 멱승연산이 소요된다.

동전 인증 프로토콜에서 사용자(U)와 상점(S)이 주고받는 정보의 양은 774 Bytes로 [9]과 같다. 계산량을 보면 [9]에서는 동전 인증 프로토콜을 위해 사용자(U)는 약 5번의 멱승연산을 수행해야 하고, 상점(R)은 약 11번의 멱승연산을 수행해야 한다. (이 경우도 역시 [9]에서는 상점(S)이 7번의 멱승연산이 필요하다고 했지만 은행의 서명에 대한 유효성을 판별하는 부분까지 고려하면 실제로 10번의 멱승연산이 필요하다.) 그러나 본 논문에서 제시한 분할 가능한 전자 화폐 시스템에서는 사용자(U)는 약 4번의 멱승연산을 필요로 하고, 상점(S)은 약 8번의 멱승연산을 필요로 한다.

마지막으로 액면가 공개 단계를 살펴보자. 동전을 나타내는 이진트리가 18개의 레벨을 가지고 있을 경우 평균적으로 한번의 지불을 위해 9개의 노드가 사용된다. 본 논문에서 제시한 분할 가능한 전자 화폐 시스템에서는 이때 각각의 노드에 대해 [9]에서와 마찬가지로 1,152 Bytes가 사용자(U)에게서 상점(S)으로 전송된다. 그리고 N이 정당한 방법으로 생성되었음을 확인하기 위해 약 320 Bytes가 추가로 전송된다. 액면가 공개 프로토콜을 수행함에 있어서의 계산량을 살펴보면 본 논문에서 제시한 시스템은 [2]나 [9]와 마찬가지로 사용자(U)의 경우 총 18(2×9)번의 root 연산이 필요하고, 상점(S)의 경우 18(2×9)번의 멱승연산이 필요하다. 참고로 근(root) $(\bmod n)$연산은 멱승연산 $(\bmod n)$ 연산과 계산량이 비슷하다[2].

참고문헌

[1] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Advances in Cryptology-Crypto '88 (Lecture Notes in Computer Science)*, pages 319-327. Springer-Verlag, 1990.

[2] T. Okamoto. An efficient divisible electronic cash scheme. In Don Coppersmith, editor, *Advances in Cryptology, Proc. of Crypto '95 (Lecture Notes in Computer Science)*, pages 438-451. Springer-Verlag, 1995. Santa Barbara, California, U.S.A., August 27-31.

[3] S. Brands. Untraceable off-line cash in wallets with observers. In *Advances in Cryptology-Crypto '93, Proceedings(Lecture Notes in Computer Science 773)*, pages 302-318. Springer-Verlag, 1993.

[4] T. Okamoto and K. Ohta. Universal electronic cash. In *Advances in Cryptology-Crypto '91 (Lecture Notes in Computer Science)*, pages 324-337. Springer-Verlag, 1992.

[5] S. D'Amiano and G. Di Crescenzo. Methodology for digital money based on general cryptographic tools. In *Advances in Cryptology, Proc. of Eurocrypt '94*, pages 157-170. Springer-Verlag, 1994. Italy, 1994.

[6] T. Eng and T. Okamoto. Single-term divisible electronic coins. In *Advances in Cryptology-Eurocrypt '94*, Proceedings, pages 306-319, New York, 1994. Springer-Verlag.

[7] A. Chan, Y. Frankel, P. MacKenzie, and Y. Tsiounis. Mis-representation of identities in e-cash schemes and how to prevent it. In *Advances in Cryptology-Proceedings of Asiacrypt '96 (Lecture Notes in Computer Science 1163)*, pages 276-285, Kyongju, South Korea, November 3-7 1996. Springer-Verlag.

[8] Y. Frankel, B. Patt-Shamir, Y. Tsiounis. Exact Analysis of Exact Change. In the 5th *Israel Symposium on the Theory of Computing Systems (ISTCS '97)*, June 17-19, Ran-Gatan Israel, pages 107-119, IEEE Computer Society Press.

[9] A. Chan, Y. Frankel, Y. Tsiounis. Easy come - easy go divisible cash. In *Advances in Cryptology-Eurocrypt '98 (Lecture Notes in Computer Science)*, pages 561-575. Springer-Verlag, 1998. Elsinki, Finland, May 31-June 4 '98.

[10] J. C. Pailles. New Protocols for Electronic Money. In Advances in Cryptology-Proceedings of Auscrypt '92 (Lecture Notes in Computer Science), pages 324-337, Springer-Verlag.

[11] K. Q. Nguyen, Y. M. Vijay, V. Varadharajan. A New Digital Cash Scheme Based on Blind Nyberg-Rueppel Digital Signature. In *Information Security - Proceedings of First International Workshop, ISW'97*, pages 313-320. Tatsunokuchi, Ishikawa, Japan September 17-19, 1997.

[12] T. Okamoto and M. Yung. Lower bounds on term-based divisible cash systems. In *International Workshop on Public Key Cryptography*, Yokohama, Japan, February 5-6 1998. Springer-Verlag.

[13] B. Pfitzmann and M. Waidner. How to break and repair a 'provably secure' untraceable payment system. In J. Feigenbaum, editor, *Advances in Cryptology, Proc. of Crypto '91 (Lecture Notes in computer Science 576)*, pages 338-350. springer-Verlag, 1992.

[14] I. B. Damgard. Collision free hash functions and ublic key signature schemes. In C. Chaum and W. L. Prive, editors, *Advances in Cryptology-Eurocrypt '87 (Lecture Notes in Computer Science 304)*. Springer-Verlag, Berlin, 1988. Amsterdam, the Netherlands, April 13-15, 1987.