정보학연구 제3권 제1호 2000년 3월(pp.89-97)
The Studies of Information Technology, Vol.3, No.1

전자면허의 기능을 갖는 분할 가능한 전자화폐시스템에 관한 연구

이애리*/이지영**

요 약

통신상의 전자상거래를 위해서는 전자화폐 시스템이라 불리는 새로운 개념의 지불 시스템이 필요하다. 전자화폐는 기존의 화폐를 디지털화한 정보이다. 그러나 전자화폐의 안전성은 기존의 화폐와는 달리 어떤 물리적 조건에 의존하지 않기 때문에 위조와 변조가 쉽게 이루어질 수 있으며, 쉽게 추적 당할 수 있다. 전자화폐가 안심하고 새로운 지불 수단으로 사용되기 위해서는 안전성과 사용자의 프라이버시가 보장되어야 한다.
본 논문에서는 기존에 제안되어진 전자동전 시스템, 분할 가능한 전자화폐, 전자면허등의 전자화폐시스템을 분석하고 통신량과 계산량에서 효율적이며, 전자면허의 문제점을 해결할 수 있는 시스템을 제안한다.

Ⅰ. 서론

전자상거래는 거래 구성원들간의 직접적인 대면 접촉방식의 거래가 아닌 전자적 통신방법을 통한 간접적인 비대면 방식의 거래가 되는 것이다. 이러한 전자상거래는 기존의 상거래 관습에서 가장 문제되고 있는 시간적, 공간적 제약을 극복할 수 있는 장점을 지니고 있다. 이것이 바로 전자상거래가 기존의 상거래 문화를 변화시킬 수 있는 원동력이 될 수 있다.

전자상거래에서 중요하게 고려되어야 할 것이 지불 방법에 관한 것이다. 현금형태는 전자상거래에 이용하기에 적절치 못하다. 이에 새로운 화폐가 요구되는데 이것이 전자화폐이다. 전자화폐가 안심하고 새로운 지불수단으로 사용될 수 있기 위해서는 안전성과 사용자의 프라이버시를 보장하는 암호기법들의 사용이 필수적이며 이에 대한 연구가 이루어져야 한다.

본 논문은 일반적인 전자화폐시스템의 기본원리와 요구조건 등에 대해 기술하고, 그것을 이용한 새로운 전자화폐시스템에 대해서 제안한다.

Ⅱ. 전자화폐시스템

2.1 전자화폐시스템의 기본원리

2.1.1 전자화폐 시스템의 구성원

전자화폐 시스템은 시스템 구성에 참여하는 구성원들과 그 구성원들 사이에서 일어나는 프로토콜로 이루어진다. [1]

① 사용자(user): 전자화폐를 발행기관으로부터 발급 받아 그것을 각 상점에서 사용하는 주체

* 세명대학교 컴퓨터과학과
** 세명대학교 컴퓨터과학과

1) 백은경. "전자대금 결재를 위한 보안 기술 현황", 정보통신 연구 제11권 제2호, 1997. 6

② 상점(shop): 사용자로부터 전자화폐를 구매대금으로 받는 공급자

③ 은행(bank): 사용자에게는 전자화폐를 발급해 주는 발행기관이며, 상점에게는 전자화폐를 결재해 주는 결재기관

위에서 설명된 구성원은 전자화폐시스템에서의 최소 구성원이며, 확장된 요구사항과 가정에 따라 그것의 구성원이 증가할 수도 있다.

2.1.2 전자화폐 시스템의 기본적인 프로토콜

전자화폐 시스템은 시스템 구성원들 사이에서 수행되는 프로토콜에 그 기반을 둔다. 전자화폐 시스템의 프로토콜은 시스템을 구성하는 구성원의 수와 시스템이 요구하는 기능에 따라 그 구성은 달라질 수 있다.

① 인출 프로토콜(withdrawal protocol)

사용자와 은행 사이에서 수행되는 프로토콜로서 은행이 사용자에게 전자화폐를 발급해 주는 절차를 명세한 것으로서 전자화폐 시스템 설계시 가장 중요한 부분이 된다.

② 지불 프로토콜(payment protocol)

사용자와 상점 사이에서 수행되는 프로토콜로서 사용자가 구매대금으로 자신의 전자화폐를 상점에 지불하는 과정을 명세한 프로토콜이다.

③ 예치프로토콜(deposit protocol)

상점과 은행 사이에서 수행되는 프로토콜로서 상점이 사용자로부터 받은 전자화폐를 은행이 결재해주는 프로토콜이다.

2.2 전자화폐시스템의 요구조건

2.2.1 기본적인 요구조건

전자화폐가 기존의 화폐 시스템을 대체하기 위해서는 물리적 화폐가 가지고 있는 다음과 같은 조건을 만족해야 한다.

① 안전성(security)

안전성이란 물리적 안전성과 논리적 안전성으로 구분 지을 수 있는데, 물리적 안전성은 전자화폐 자체에 대한 위조의 어려움을 의미하는 것이며, 논리적 안전성은 전자화폐 자체에 대한 위조 여부를 의미하는 것이 아니라, 전자화폐 시스템의 각 구성원은 나머지 다른 구성원들의 공모 공격(collusion attack)에 대해 안전해야 함을 의미하는 것이다. 물리적 안전성이라고 하는 것은 전자화폐의 안전성이라고 하기보다는 스마트 카드 자체의 안전성을 의미하기 때문에 일반적으로 전자화폐 시스템의 안전성이라고 하는 것은 논리적 안전성을 의미하는 것으로 해석할 수 있을 것이다.[2)]

② 이중사용(double-spending)의 방지

전자화폐에 대한 이중 사용 방지는 사용된 전자화폐로부터 컴퓨터가 동일한 전자화폐를 조사하여 이중 사용자의 계좌번호와 사용자의 신분을 알아내는 방식을 주로 취하고 있다. 이중사용의 의미는 악의 있는 사용자가 전자화폐를 불법 복제하여 무단으로 반복적으로 사용하는 것을 의미하는 것이며, 이것은 전자화폐 시스템 설계시 가장 중요하게 고려해야 될 부분인 것이다.

2) 김지연, 이동렬, 원동호, "전자면허를 이용한 전자현금 시스템의 문제점 분석" 한국통신정보보호학회 종합학술발표회 논문집, Vol.6 No.1

③ 프라이버시(privacy)

사용자 프라이버시의 보장은 전자화폐 시스템의 가장 큰 장점이 되며, 프라이버시 보장 강도에 따라 다음과 같이 두 가지로 나뉜다.

가. 불추적성(untraceability): 은행과 상점이 어떠한 공모를 행하더라도 전자화폐를 지불한 사용자의 지불정보와 인출정보는 서로 연결될 수 없는 것을 의미한다. 즉, 은행은 상점과 공모하더라도 사용자의 지불 내역을 추적할 수 없게 된다[3]

나. 불연계성(unlinkability): 은행과 상점이 공모하는 경우 은행은 비록 사용자의 거래 내역을 추적할 수는 없지만, 두 가지의 지불이 같은 사용자에 의한 것임을 알 수 있는 경우가 있는데, 이 경우 연계성(linkability)이 있다고 일컬어진다. 이러한 연계성이 전자화폐 시스템이 존재할 경우 궁극적으로는 사용자의 불추적성이 보장되지 않을 수도 있게 된다. 그러므로, 전자화폐 시스템이 완벽하게 사용자의 프라이버시를 보장하기 위해서는 불연계성이 보장되어야만 한다.[4]

④ 오프라인(off-line)

오프라인 전자화폐 시스템은 지불단계와 결재단계가 동시에 이루어지지 않는 형태로 사용자와 상점의 거래시 은행의 개입이 필요치 않은 것이다. 일정시간이 경과된 전자화폐를 일괄 처리해 은행에 결재 요구를 하는 것으로 모든 단계가 종료된 후에 이중사용이 이루어지고 난 후 은행에서 이중사용자에 대한 신분검출이 가능한 문제점이 생기게 된다. 이중사용한 후 도피할 수 있는 문제점이 생기기는 하지만 통신량의 집중화 방지와 거래에 따른 통신 비용은 적게 든다.

2.2.2 전자화폐 시스템의 부가적인 요구사항

전자화폐를 실제 화폐와 같이 사용하기 위해서는 기본적인 요구사항 이외에도 다음과 같은 몇 가지 부가적인 요구사항이 있어야 한다.

① 분할성(divisibility): 분할성은 사용자가 전자화폐를 발급 받는 경우 발급 받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 성질이다. 즉, 인출 받을 당시의 금액을 기준으로 사용한 총액이 지정된 금액을 넘지 않을 때까지 사용자가 나누어 사용할 수 있음을 말하는 것이다. 이것은 한 번 발급 받은 전자화폐를 여러 번 나누어 사용할 수 있으며, 상환 프로토콜(refund protocol)이 필요 없다는 장점을 갖는다.[5]

② n회 사용가능성(n-spendability): 이것은 분할성의 개념과 비슷하지만 본질적으로는 큰 차이가 있다. 분할성은 사용자가 발행받은 전자화폐 금액내에서 사용자가 지불하기 원하는 금액만큼 사용금액에 맞추어 지불할 수 있는 기능이다. 반면에 n회 사용가능성은 금액을 나누어 사용한다는 개념보다는 지하철 정기권과 같이 동일한 금액을 횟수 기준으로 n번까지 사용한다는 개념이다. 즉, n회 사용가능성은 어느 일정한 금액을 일정 횟수만큼만 사용 가능케 하는 것이다.

③ 양도성(transferability): 실제 화폐의 성질

3) D. Chaum, A. Fiat, M. Naor,"Untraceable Electronic Cash," Advances in Cryptology, Proceedings of Crypto 88,1988

4) T. Okamoto, K. Ohta, "Universal Electronic cash", Advances in Cryptology, Proceeding of Crypto 91, 1991

5) A. Chan, Y. Frankel and Y.Tsiounis, "Easy-come easy-go divisible cash", In advances in Cryptology-Eurocrypto '98, proceeding pp.561-575, 1998

들 중 가장 특기할 만한 것은 쉽게 양도 가능하다는 것이다. 즉, 발행기관으로부터 만들어진 화폐는 그것의 수명이 다할 때까지 계속해서 사회에 유통된다. 그러나, 기본적인 요구 사항만을 만족하는 전자화폐는 그러한 양도 기능이 없으며, 이것은 전자화폐가 실제 화폐를 대치하지 못하고 있는 이유중의 하나가 된다. 이러한 문제점을 해결하고자, T. Okamoto는 양도성 기능을 갖는 전자화폐 시스템을 제안하였다.[6] 그러나, 양도성 성질은 사용자의 프라이버시가 보장되기 어렵고 전자화폐는 양도횟수가 증가할 수록 그것의 크기가 증가한다는 문제점이 있다.[7]

Ⅲ. 기존의 전자화폐 시스템

3.1 Brands의 전자화폐 시스템

1993년 Brands는 CFN시스템의 가장 큰 문제점인 cut-and-choose 방식의 인출 프로토콜을 challenge-and-response 방식의 인출 프로토콜로 설계함으로써 CFN시스템이 가지고 있는 통신량의 지나친 증가라는 문제를 해결하게 된다. 이 방식은 이중사용시 반드시 이중 사용여부를 확인하므로써 이중 사용을 사전에 방지할 수 있고, 기존의 방식들이 인수분해문제(factoring problem)에 근거를 둔데 반하여 이산대수 문제의 확장인 표현문제(representation problem)를 이용하여 안전성을 근거하고 있다. 표현문제란 군(群) G의 k개의 고정된 원소 g_1, g_2, …, $g_k \in G$가 주어지고 $h \in G$가 임의로 주어질 때 $h = g_1^{a_1} g_2^{a_3} \cdots g_k^{a_k}$를 만족시키는 $(a_1, a_2, \cdots a_k)$를 구하는 문제이다[8][9]. Brands의 프로토콜은 제한적인 은닉서명 기법(restrictive blind signatures)과 Schnorr 인증기법을 사용하여 화폐 발행 프로토콜과 지불 프로토콜을 간소화하였다.[10]

3.2 Okamoto의 전자화폐 시스템

Okamoto는 분할성의 정확도 개념에 의존하는 대수적인 프로토콜에 의한 전자화폐방식을 처음 제안했다.[11]

Okamoto의 방식은 계좌개설(전자면허 발급) 단계, 인출단계, 지불단계 그리고 예치단계의 프로토콜로 구성된다. 이전의 방식보다 효율적으로 구성하여 실질적으로 사용 가능하도록 하기 위해 cut-and-choose방법을 대신하여 전자면허 발행시 이산대수 문제에 기반한 Bit Commitment 방법의 형식을 취하고 있다. 여기서 사용자는 은행과의 통신 중에 위탁한 값을 영지식 방법으로 은행에게 증명할 수 있고, 위탁된 값들을 증명할 수 있는 프로토콜은 지불과 인출 예치과정에서 단지 O(log N) 계산만으로 분할 가능한 익명성을 가지는 오프라인 전자화폐를

6) T. Okamoto, "An efficient divisible electronic cash sheme", Advances in Cryptology, Proc. of Crypto95 pp.438-451, 1995

7) T. Okamoto and K. Ohta, " Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic cash", Proceeding of Crypto '89, pp.481-496 1989

8) S. Brands, "Untraceable off-line Cash in wallets with observers", Advances in Cryptology, Proceedings of Crypto 93,1993

9) 박승안, 신현용, " 전자화폐 연구동향', 통신정보보호학회지, 제4권 제4호, pp.29~33,1994. 12

10) C. Shnorr, "Efficient signature generation by smart cards", Jounal of Cryptology 4, pp.161-174, 1991

11) T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", IEEE Trans. Inform. Theory, Vol.31, No.4, pp.469-472,1985

만들었다. 그러나 Bit commitment를 이용한 영지식 프로토콜은 그것이 전자면허 발행시에만 사용된다 하더라도 굉장히 많은 트렌젝션을 발생시키기 때문에 매우 비효율적이다. 12)

Ⅳ. 제안하는 전자화폐 시스템

전자면허란 은행에서 발급하는 현금을 사용할 수 있는 일종의 면허증과 같은 개념으로 계좌 개설시 한번만 수행된다.13) 우선 사용자는 계좌 개설시 전자면허 발급 프로토콜을 통해 전자면허를 발행 받고 전자면허를 이용하여 전자화폐를 발행 받는다. 그리고 지불 프로토콜을 통해 현금을 상점에 지불하고, 상점은 사용자로부터 받은 현금을 예치프로토콜을 통해 자신의 계좌로 예치하거나 교환 프로토콜을 이용하여 나중에 다른 곳에 사용할 형태의 현금으로 변환한다. 전자면허를 이용하는 모든 시스템에서는 사용자의 현금 사이에 연결성이 생기는 문제점이 발생한다. 즉, 두 거래가 발생했을 때 누구에 의한 것인지는 알 수 없으나 그 두 거래가 같은 사람에 의한 것임을 알 수 있게 된다.

분할성이란 실제화폐에는 없는 개념으로 사용자가 화폐를 발급 받은 경우 발급 받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 성질이다.

본 논문에서는 전자면허를 발행하지 않고, Brands의 인출프로토콜을 수정하고 전자 면허의 기능성만을 추가하여 이 문제를 해결하고 효율성을 개선한다. 인출단계에서 동전 서명을 위해 은행에 의해 서명되는 방식은 제한 은닉 서명기법을 사용하고 분할성을 위해서 Okamoto 시스템과 같이 계층적 구조표를 이용한다.

본 전자화폐 시스템은 사용자, 은행, 상점사이에서, 초기화단계, 인출단계, 지불단계, 예치단계의 4개의 프로토콜로 구성된다.

4.1 초기화단계

Brands의 방식에 기반하며, 은행과 사용자의 초기화 단계 두 부분으로 구성된다.

4.1.1 은행의 초기화 단계

가. 은행은 보안 파라메타 n과 S 그리고 H=|p|=|q|=|N|/2를 고른다.

:2H는 RSA 계수의 크기이며, 익명성은 이 계수의 인수분해의 어려움에 의존하기 때문에 이 보안 파라메타는 사용자를 위한 보안을 통제한다.

나. 은행은 δ를 계산하고, 소수 Q, P를 선택한다.

: $\delta > (2n+2)/H$, $P = 2Q + 1$, $|Q| = 2(1+\delta)H+6$, 모든 연산은 G_Q에서 수행된다.

다. 은행은 G_Q의 생성원(generator)) (g, g_1, g_2, g_3), H, H_0, H_1, ..., 액면 금액마다 다른 키가 사용되는 A 개인키 $x \in_R Z_Q$ (각 다)선택한다.

라. 은행은 G_Q 설명서를 공개한다: P, Q, 생성원 집합($g, g_1, g_2, g3$), H, H_0, H_1, ...의 설명서와 그 공개키 $h = g^x$, $h_i = g_i^x$ (i=(1,2,3))

12) N. Ferguson, "Single-term off-line coins", Advances in Cryptology, Proceedings of Eurocrypto '93, 1993

13) S. Brands, "An efficient off-line electronic cash system based on the representation problem", Tecnical report CS-R9323, CWI 1993

4.1.2 사용자의 초기화 단계

가. 사용자는 물리적 혹은 다른 방법에 의해 그의 신원을 은행에 보여주고 $I = g_3^u$로 자기 자신을 은행에 가입시킨다.

나. 사용자는 Schnorr 인증 방식에 의해 u의 지식을 입증한다.

다. 은행은 $I \neq \{1, g_3\}$를 확인한다.

라. 첫 번째 단계에서 사용자는 은행에게 자신의 공개키를 보낸다. 그래서 인출 시에 인증된 채널이 만들어질 수 있다.

4.2 인출 프로토콜

동전에 서명하기 위해 사용되는 은행의 서명은 Brands의 방식과 같이 제한 은닉 서명 기법을 사용한다. 인출 프로토콜 초기에 사용자는 은행과 인증된 채널을 만든다. 이것은 오직 소유자만이 계좌 인출을 하고 있다는 것과 사용자가 실제 은행과 통신하고 있다는 것을 보장하기 위해 모든 전자화폐 프로토콜에 필요하다. 즉, 이것으로 전자면허의 기능을 대신할 수 있게 되는 것이다. 인출프로토콜은 I의 제한은닉서명을 만든다. 사용자는 s가 임의의 수인 Schnorr서명 $(Ig_2)^s$를 가지고 끝날 것이다. 사용자는 은행에 그가 $I w.r.t$의 representation을 알고 있고 sign(A,B)의 정확성 검사에 의해 은행의 신원이 납득되어질 수 있다는 것을 입증한다.

4.3 지불 프로토콜

지불 프로토콜은 Okamoto의 방식과 같이 동전 인증과 액면금액 노출의 두 단계로 구성된다. 동전 인증 단계는 동전에 대한 은행의 서명을 확인하는 단계이며, 액면금액 노출 단계에서는 고객이 그가 사용하기를 원하는 금액에 해당하는 노드들의 집합에 대한 정보를 드러낸다. 동전 인증 단계는 Brands의 방식을 수정하여 사용하고, 액면금액 노출 단계는 Okamoto의 방식에서와 같이 계층적 트리 구조를 이용하여 화폐의 분할 사용을 가능하게 한다.

4.3.1 동전 인증

가. 사용자는 $x_3 \in {}_RZ_Q$를 선택하고 $Y_3 = g_3^{uq}, y_3 = g_3^{x_3}, d = H(A, B, Y_3, y_3, date/time, ID_S)$ $Y = g_2^q$, 를 계산한다.

어느 경우나 $(A, B, Y_3, y_3, date/time, ID_S)$는 반드시 해쉬안에 포함되어야만 한다. 상호작용이 없는 경우는 사용자로부터 은행으로의 한번의 이동에서 지불 프로토콜이 수행되어지는 것을 고려해야한다

나. 사용자는 상점에게 동전을 보낸다: A,B=[N,Y], $sign(A, B), Y_3, y_3$를 전송하고. $r_3 = duq + x_3$를 가지고 challenge d에게 응답한다.

다. 상점은 동전이 정당하다는 것을 입증한다.

a. 서명 sign(A,B)를 입증한다.

$Y \neq g_2, Y \neq g_2^N, A \neq 1, Y_3 \neq g_3, (-1/N) = 1, (2/N) = -1$

b. Schnorr 인증기법을 사용하여 사용자가 g_3에 관하여 Y_3의 representation을 안다는 것을 입증한다.: $g_3^{r_3} \stackrel{?}{=} y_3 Y_3^d$

c. q를 정확하게 선택했다는 것을 입증한다. $|q| \leq (1 + \delta)H$:를 입증하기 위해서 $Y = g_2^q$를 가지고 g_2에 바탕을 둔 range-bounded commitment를 이용한다. 대화식 경우를 위해

challenge e는 hash 함수에 기반하여 계산된다. 이 경우 사용자와 상점의 공모는 증거 위조를 할 수 없다.

d. A가 정확하게 작성되었다는 것을 입증한다.: $g_1^N YY_3 \doteq A$

e. 사용자가 부정한 짓을 할 수 있는 방법을 제한한다. N이 3 mod 4에 일치하는 첫 번째 |N|소수에 의해 나누어지는지 점검한다. 이는 이중사용자의 신분증명을 도와준다.

4.3.2 액면금액 노출

가. 사용자 는 $\Gamma_{j_1,\ldots,j_t}$를 계산하고 상점에게 보낸다.

나. 상점은 $i \in \{1,\ldots,t-1\}$동안 $J_{i+1}=1$이면 $\Omega_{j_1,\ldots,j_{t-1}}$을 계산한다. 그리고 다음의 검사에 의해 $\Gamma_{j_1,\ldots,j_t}$의 정당함을 증명한다.

다. 사용자는 $e \in \{0,1\}^k$인 $e = H_0(C, date/time, ID_S, N)$을 계산한다.

타이밍과 상점 정보 (ID_S)는 부인방지를 위해 필요하다. 그 밖의 e는 각 경우와 확인되어진 사용자에서는 다르다. challenge는 S에 의해 공급되어진 무작위 값인 $e' \in \{0,1\}^k$에서 $e = H_0(C, date/time, ID_S, e', N)$에 의해 세팅된 대화식 방법에서 계산되어질 수 있어야 한다.

사용자는 $\Lambda_{j_1,\ldots,j_t}$를 계산한다.

라. 상점은 다음 검사에 의해 $\Lambda_{j_1,\ldots,j_t}$의 정당함을 증명한다.

$$(\Lambda_{j_1,\ldots,j_t})^{2^{k+1}} \equiv d^2 2^{2e} H_\Lambda(A, B, j_1 \ldots\ldots j_t) \mod N),$$

만약 증명이 성공한다면 고객의 지불로서 메시지를 받아들인다.

4.4 예치 프로토콜

상점은 은행에게 지불 사본을 보낸다.

V. 결론

전자화폐는 정보통신의 비약적인 발달로 새롭게 부각되는 전자상거래의 중요한 지불수단이다. 이는 물리적 화폐를 대신하여 네트워크 상에서 물리적 화폐와 유사한 기능으로 사용되고 있다.

본 논문은 전자화폐의 인출 프로토콜에 전자면허의 기능성만을 두어 실제 전자면허를 이용했을 때 수반되는 문제점을 제거하려고 했다. 인출 프로토콜은 기본적인 개념에서는 Brands의 방식을 따른다. 또한 Okamoto의 프로토콜을 변형하여 분할성을 추가하였다. 화폐의 분할개념은 물리적 화폐에는 없는 개념으로 네트워크상에서 전자화폐의 구현시 사용자의 편리성 및 시스템 구축을 위한 효율성 증대 효과도 가져올 수 있다.

참고문헌

1) 백은경. "전자대금 결재를 위한 보안 기술 현황", 정보통신 연구 제11권 제2호, 1997. 6

2) 김지연, 이동렬, 원동호, "전자면허를 이용한 전자현금 시스템의 문제점 분석" 한국통신정보보호학회 종합학술발표회 논문집,

Vol.6 No.1

3) D. Chaum, A. Fiat, M. Naor, "Untraceable Electronic Cash," Advances in Cryptology, Proceedings of Crypto 88, 1988

4) T. Okamoto. K. Ohta, "Universal Electronic cash",Advances in Cryptology, Proceeding of Crypto 91, 1991

5) A. Chan, Y. Frankel and Y. Tsiounis, "Easy-come easy-go divisible cash", In advances in Cryptology-Eurocrypto '98, proceeding pp561-575, 1998

6) T. Okamoto. "An efficient divisible electronic cash sheme". Advances in Cryptology, Proc. of Crypto95 pp.438-451, 1995

7) T. Okamoto and K. Ohta, "Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic cash", Proceeding of Crypto '89, pp.481-496 1989

8) S. Brands, "Untraceable off-line Cash in wallets with observers", Advances in Cryptology, Proceedings of Crypto 93, 1993

9) 박승안, 신현용, " 전자화폐 연구동향', 통신정보보호학회지, 제4권 제4호, pp29~33, 1994. 12

10) C. Shnorr. "Efficient signature generation by smart cards", Jounal of Cryptology 4, pp.161-174, 1991

11) T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", IEEE Trans. Inform. Theory, Vol.31, No.4, pp.469-472, 1985

12) N. Ferguson, "Single-term off-line coins", Advances in Cryptology, Proceedings of Eurocrypto '93, 1993

13) S. Brands. "An efficient off-line electronic cash system based on the representation problem", Tecnical report CS-R9323, CWI 1993

A Study on the Divisible Electronic Cash System Functioning Electronic License

Ae-Ri, Lee*/Jim-young, Lee**

Abstract

Electronic commerce on the network requires a new payment system, electronic cash that carries digitalized information of cash. The new system, however, demands the security and privacy because electronic cash is different from real cash in that it can be easily duplicated, forged, or traced.

Therefore, electronic cash system should be guaranteed security and privacy to be used as a new payment mechanism with assurance.

First, this paper analyzes the existing electronic cash system involving electronic coins, divisible electronic bills, and electronic license.

Then the paper proposes a new electronic cash system which claims to be more efficient in the amount of communication and computation. Finally, this study attempts to solve the problem of electronic license.

* *Dept of Computer science Semyung University*
** *Dept of Computer science Semyung University*