通信情報保護學會論文誌
第5卷 第1號, 1995. 3

스마트카드를 이용한 새로운 전자현금 방식

염 흥 열*, 이 석 래**, 이 만 영***

Electronic Cash Schemes for EFT Using Smart Card

Heung-Youl Youm*, Seok-Lae Lee**, Man-Young Rhee***

요 약

반도체 기술의 발달은 스마트카드의 실용화를 가능케하였고 더나아가서 컴퓨터 기술과 암호 기술의 결합은 전자현금을 포함하는 전자지갑의 실현을 가능케 하였다. 지금까지 연구된 전자현금에 대한 연구는 고객의 익명성 보장, 재사용 검출, 그리고 현금의 분할 사용에 촛점을 맞추어 수행되어 왔다. 본 논문에서는 이산대수 문제와 소인수분해 문제에 바탕을 둔 새로운 전자현금 방식을 제시하며, 제시된 전자현금 방식의 특성을 분석한다. 제시된 전자현금 방식은 전자현금의 발급과정에서 은닉 디지틀 서명 기법에 바탕을 두고 있으며, 전자현금 지불 과정에서 Schnorr의 인증 기법을 이용하여 현금의 정당성을 확인하며, 일방향 해쉬함수와 이산대수문제에 기반을 둔 계층적 구조표를 이용하여 전자현금의 분할 사용을 가능케 한다. 또한, 현금의 다른 고객으로의 전이가 가능하며, 현금을 한번만 사용하는 경우 고객의 익명성을 보장하지만 동일한 현금을 두번 이상 사용하는 경우에는 고객의 신원이 검출된다. 따라서, 본 방식은 고객의 불법적인 전자현금 사용을 방지할 수 있고, 고객 측면에서 계산적 복잡도를 감소시킬 수 있는 방식이다.

Abstract

The smart card with the cryptography and VLSI technologies makes it possible to implement the electronic cash easily. A number of electronic cash schemes have been proposed by many cryptographic researchers. In this paper, we propose a practical electronic cash system, using blind digital signature scheme, Schnorr's authentication scheme based on the discrete logarithm problem, and the hierarchical cash tree based on two one-way hash functions for dividable payment. This electronic cash scheme has such properties as privacy of the payment, off-line payment, non-reuseability of cash, transferability of cash to another customer, and dividable payment of cash. This electronic cash protocol is well suited for implementing in smart card.

* 순천향대학교 공과대학 전자공학과
** LG 전자기술원 연구원
*** 종신회원, 한양대학교 전자통신공학과, 한국통신정보보호학회 회장

제1장 서 론

컴퓨터와 통신망이 결합된 전산망이 구축되고 있고, 여기에 스마트카드를 이용한 전자현금 시스템의 출현은 우리의 경제 생활에 상당한 영향을 미칠것이다. 전자현금은 기존의 종이 지폐의 기능을 전자적인 은행의 서명문을 이용하여 실현하는 시스템이다. 전자화된 정보시스템은 암호 기술을 이용하여 실현되어야 신뢰성과 안전성을 보장받을 수 있다.

암호 기술을 적용한 전자현금 시스템을 설계할 때 반드시 고려해야 할 요구사항은 고객의 사용이 편리할 것, 대규모로 시스템을 구현할 경우 시스템에 대한 관리 및 처리가 효율적일 것, 모든 위협 요소들을 정확히 파악하여 이에 총체적으로 대처할 것, 시스템의 특정부분의 안전성(security) 파괴가 전체 시스템의 안전성 파괴에 연결되지 않도록 설계될 것, 그리고 가능한 간편하고 쉬운 암호 기술을 적용할 것 등이다.

컴퓨터 통신망과 스마트카드가 결합되어 현금 및 증서의 이동을 전자적으로 실행하는 전자현금, 전자 수표, 그리고 이를 이용한 POS 시스템[3],[10],[11],[14]은 종래의 종이 지폐에 비교하면 거래가 고속으로 수행될 수 있고, 전자현금의 생성 및 관리 비용이 저렴한 특징이 있다. 그리고 통신망과 컴퓨터를 이용하므로 미래의 정보화 사회에 적합한 새로운 형태의 전자현금 시스템(일명 전자금융 시스템) 이 될 것이다.

전자 현금 시스템은 기존의 종이 지폐가 갖는 특성을 만족하도록 설계되어야 한다. 화폐, 수표, 그리고 증서 등을 총칭하여 일반적으로 환금 증서라 한다. 기존의 환금 증서가 갖는 주요 특성을 살펴보면 다음과 같다.

① 유통성 : 여러 사람이 다양한 환금 증서의 보편적 가치를 인정하여 서로 거래하며 유통한다.

② 유일성 : 지질, 인쇄의 특수성 등의 특성을 이용하여 환금 증서는 어디서나 자신의 가치를 증명할 수 있으며, 오직 하나만 존재한다.

③ 추적 불가능성 : 여러 종류의 환금 증서는 어떻게, 누구에게 유통되었는가에 대하여 추적이 불가능하다.

기존의 신용 카드를 이용하는 거래 방식은 유통성과 유일성의 특징을 갖지만, 카드소지자가 어디서 어떻게 현금을 사용했는지를 알수 있으므로 추적 불가능성을 만족시키지 못한다. 따라서 새로운 전자 현금시스템은 기존의 환금 증서가 갖는 모든 보편적 특성을 만족하도록 설계되어야 한다.

암호 기술을 이용하지 않는 전자현금시스템은 기존의 환금 증서와는 달리 여러 문제점을 안고 있다.

① 전자현금은 종이 지폐와는 달리 쉽게 복사될 수 있어서 원래의 전자현금과 복사된 전자현금을 쉽게 구별할 수 없다. 따라서 적절한 대비책을 강구하지 않으면 하나의 전자현금이 여러 번 사용될 가능성이 있다.

② 전자현금은 일반적으로 어떻게 현금이 지불되었는가 하는 것이 환금 증서보다 훨씬 쉽게 검출될 수 있다. 왜냐하면 카드 소지자가 소매점에서 물건을 사고나서 자신의 스마트카드내에 있는 전자현금을 이용하여 물건값을 지불하려 할 경우, 소매점의 점원은 자신의 단말을 이용하여 은행의 컴퓨터에 전자현금의 유효성 여부를 조회한다. 은행이 진실된 전자현금이라고 알려주면 물건 거래가 허용될 것이다. 따라서 은행은 임의의 사용자에 대한 자금 이동 경로를 쉽게 추적할 수 있다.

이들 문제점은 전자현금을 사용하려는 각 사용자의 프라이버시를 크게 위축시킬 수 있을 뿐아니라 전자 현금 시스템의 조기 정착에 큰 장애물이 될 것이다. 따라서 전자 현금 시스템은 암호 기술을 이용하여 반드시 설계되어야 한다.

전자현금 시스템에서 가장 중요한 사항은 어떤 암호 알고리듬과 프로토콜을 사용하여 안전성을 보장하면서 계산량과 저장해야 할 정보량이 적은 전자현금 발행 프로토콜, 수표 사용 프로토콜, 사용된 수표 예치 프로토콜, 그리고 잔금 예치 프로토콜을 구성하는 것이다.

한편 스마트카드는 계산력과 메모리 크기가 제한되어 있으므로 수표 인출 및 사용시에 스마트카드에 저장되어야 할 정보량이 최소화되고 통신되어야 할 정보량이 최소화되면서 불추적성을 보장받을 수 있는 개선된 오프라인 전자 수표시스템이 요구되고 있다.

전자현금이 가져야 할 주요 특성은 은행이 사용된 전자현금이 누구의 것인지에 대한 정보를 추적할 수 없는 추적 불가능한 현금(untraceable cash), 고객이 은행으로 부터 발행받은 전자현금을 한번 이상 사용할 수 없게 하는 재사용 불가능한 현금(non-reusable cash), 고객이 은행으로 부터 발행받은 전자현금을 여러 조각으로 나누어 사용케 하는 분할 사용 가능한 현금(dividable cash), 그리고 고객이 은행으로 부터 발행받은 전자현금을 타인에게 양도할 수 있는 전이 가능한 현금(transferable cash) 등이다.

지금까지 수행되어 온 연구 결과를 요약하면 다음과 같다. Chaum은 고객의 프라이버시(privacy)를 보호하기 위하여 은닉 서명을 이용한 전자현금 방식을 제안하였고[4],[5], Even, Goldreich, 그리고 Yacobi는 RSA[12] 등과 같은 공개키 암호시스템(public cryptosystem)을 이용한 전자지갑에 대한 개념을 제안하였으며[15], Chaum 등은 은행이 고객의 고유정보(identity)와 전자현금을 연결하여 저장해 두고 추후의 전자현금 사용시 고객의 신분을 추적하는 것을 막기 위한 RSA 은닉 디지틀 서명(blind digital signature), 고객이 전자현금의 불법적 이용을 위하여 전자현금의 발행과정에서 정당하지 않은 파라메타 생성을 방지하기 위한 cut-and-choose 방법, 고객이 지불과정에서 은행과 전산망을 통하여 직접 연결함이 없이 상점과의 데이타의 교환만으로 지불을 수행하는 오프라인 지불(off-line payment), 그리고 사용하고 남은 잔액을 은행으로 부터 되돌려 받기 위한 과정 및 방법 등을 제안하였다.[6],[7] Okamoto-Ohta는 위의 기본 개념을 바탕으로 전자면허(electronic license)의 발행과정을 두어 전자현금 발급과정을 간단화하고, 소인수분해(factorization) 문제와 이차근(quadratic roots) 문제에 바탕을 둔 계층적 구조표(hierachical structure table)를 이용하여 현금의 분할 사용을 가능케 하고, 고객의 프라이버시를 보장하며, 다른 고객에게 자신의 현금의 일부를 양도하는 전이 가능한 특성을 만족시키는 진보적인 전자현금 알고리듬을 제안하였다.[17], [18], [19]

본 논문에서는 이산대수문제와 소인수분해 문제에 바탕을 둔 개선된 전자현금 방식을 제시함은 물론 제안된 전자현금 방식의 특성을 분석한다. 제시된 전자현금 방식은 전자현금의 발급과정에서 RSA 은닉 디지틀 서명 기법을 이용하고, 전자현금 지불 과정에서 Schnorr의 인증법[2]을 채용하여 현금의 정당성을 확인하고, 그리고 일방향 해쉬함수(one-way hash function)와 이산대수문제에 기반을 둔 계층적 구조표를 이용하여 전자현금의 분할 사용을 가능케 한다. 또 제시된 전자현금 방식의 특징은 현금을 다른 고객으로의 전이가 가능하며, 현금을 한번만 사용하는 경우에는 고객 신원의 익명성을 보장되지만 현금을 2번 이상 사용하는 경우에는 고객의 신원이 검출되며, 현금의 분할 사용이 가능하고, 계산적 복잡도가 낮다는 등의 특징이 있다. 따라서 본 방식을 이용하면 불법 고객의 현금 사용을 막을 수 있고, 고객 측면에서 전자현금의 지불과정에서 계산적 복잡도를 감소시킬 수 있다.[1],[20],[22],[23]

제2장 이론적 배경

2.1 은닉 서명 방식과 Cut-and-Choose 방식

전자현금은 근본적으로 은행의 서명문(digital signature) 이다. 여기에 RSA 암호 알고리듬을 이용한 은닉 서명 기법(blind signature scheme)을 채용하면 고객의 신원과 전자현금을

연결시킬 수 없는 익명성(anonymity)을 유지할 수 있다. 은닉 서명을 위하여 은행은 RSA 암호 알고리듬 $(n, e : d)$을, 고객은 은닉서명을 위한 난수 r과 은행의 서명을 원하는 자신의 메시지 $f(M)$을 준비하고, 그림 2.1과 같은 프로토콜을 수행하여 메시지 $f(M)$의 서명문을 얻는다. 이 프로토콜을 수행함으로서 은행이 자신이 서명한 고객의 메세지가 무엇인지 모르고 서명하며, 고객은 자신의 메세지에 대한 은행의 서명문을 얻을 수 있다. 따라서 고객은 은행이 전자현금의 서명문과 고객을 연결시킬 수 없으므로 전자현금에 대한 불추적성의 특징을 보장받을 수 있다.

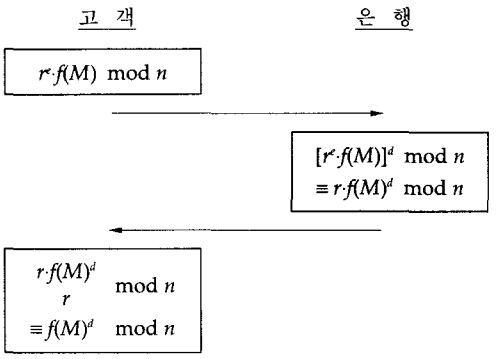


그림 2.1 RSA 은닉 서명 프로토콜

고객이 은행을 속일 경우에 대비하여 다음과 같은 cut-and-choose 방법으로 전자현금을 은행으로부터 발급받아야 한다. 고객은 그림 2.2와 같은 프로토콜을 수행하는 동안 자신이 은행으로부터 서명받기를 원하는 메세지의 반을 은행에 공개함으로서 은행으로부터 메세지 생성의 정당성을 입증받는다. 은행은 고객으로부터 수신한 나머지 반의 메세지 후보를 결합한 새 메세지에 대한 서명문을 은닉 서명방식으로 고객에 전달한다. 은행은 자신이 서명한 메세지가 어떤 메세지인지 모르면서 서명을 하는 것이고 사용자는 자신의 메세지 정당성을 입증받을수 있는 방식이다.

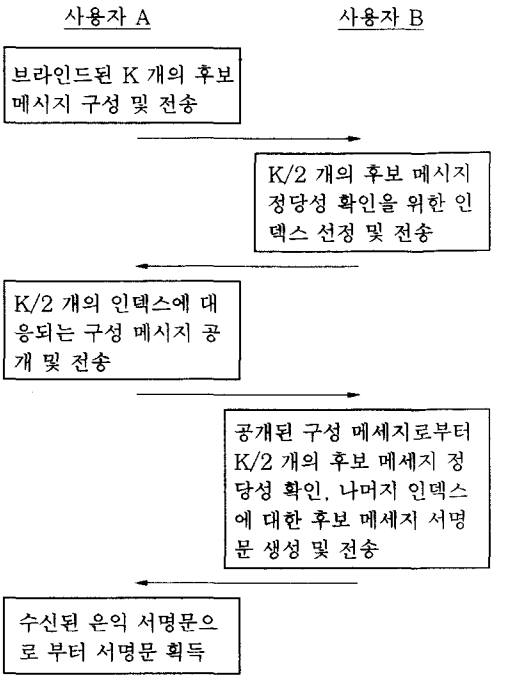


그림 2.2 cut-and-choose 서명 프로토콜

2.2 Schnorr 의 인증기법[2]

$GF(p)$상의 원시원 g가 주어졌을 때, 사용자 A는 비밀 정보 x_A를 선정하고 이에 대응되는 공개정보 $ID_A \equiv g^{x_A} \bmod p$을 공개한다. 한편, 사용자 A는 ID_A에 대응하는 비밀정보 x_A를 알고 있다는 것을 비밀정보의 밝힘이 없이 사용자 B에게 그림 2.3과 같은 프로토콜로 증명한다.

만약 동일한 x_A, v를 2번 사용하면 다음과 같이 사용자의 비밀 정보 x_A를 구할 수 있다.

$$y_1 \equiv v + c_1 \cdot x_A \bmod p\text{-}1$$
$$y_2 \equiv v + c_2 \cdot x_A \bmod p\text{-}1 \qquad (2.1)$$

식 (2.1)을 이용하여 사용자의 비밀정보 x_A는 식 (2.2)와 같이 구할 수 있다.

$$x_A \equiv \frac{y_1 - y_2}{c_1 - c_2} \bmod p\text{-}1 \qquad (2.2)$$

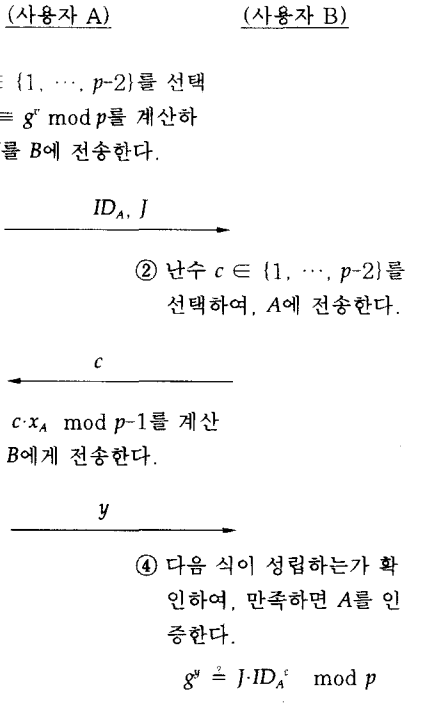


그림 2.3 Schnorr의 인증 프로토콜

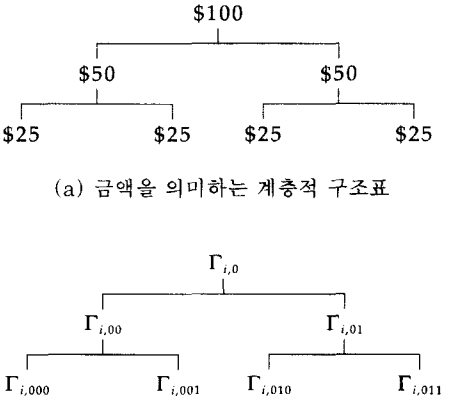
2.3 계층적 구조표(현금 트리)[9],[19]

전자현금은 사용 단위를 작게 나누어 사용할 수 있어야 한다. 현금의 분할 사용을 가능케 하는 것이 전자현금에서의 계층적 구조표이다. 따라서 계층적 구조표는 은행에 의해 발행된 전자현금을 보다 작은 현금 단위로 나누어 사용하는 데 이용된다. 계층적 구조표는 l 개의 준위을 갖는 하나의 트리(tree)로 실현된다. 트리의 각 절점(node)은 2 개의 부가지(son)를 가진다. 트리의 시초 절점(root node)은 트리의 최상단 절점(top node)이다. 따라서 l 개의 준위(level)를 갖는 계층적 구조표는 $2^l - 1$ 개의 절점이 존재한다. 계층적 구조표의 생성및 사용 법칙은 다음과 같다.

① 절점 N에 대응되는 현금 값은 N의 직계 부가지에 존재하는 절점들의 현금 값의 총합과 같다.

② 한 절점이 사용됐을 때, 이 절점과 연결된 상하 절점을 사용할 수 없다.

③ 어떤 절점도 한번 이상 사용될 수 없다.



(a) 금액을 의미하는 계층적 구조표

(b) 절점 값을 의미하는 계층적 구조표

그림 2.4 전자현금의 계층적 구조표

예를들어, $l = 3$이고 $C = \$100$인 경우의 계층적 구조표는 그림 2.4의 (a)와 같은 금액의 구조표와 그림 2.4의 (b)와 같은 각 분할 금액의 절점값을 의미하는 표로 구분될 수 있다.

사용자가 \$100중 \$75를 지불하려 하는 경우, 금액 구조표와 절점 값을 의미하는 계층적 구조표인 Γ표를 이용하여 \$75은 Γ표의 절점 $\Gamma_{i,00}$와 $\Gamma_{i,010}$를 이용하여 지불한다. 만약 \$75를 지불하기 위하여 절점 $\Gamma_{i,00}$와 $\Gamma_{i,010}$가 사용되었다면, 절점 $\Gamma_{i,0}$, $\Gamma_{i,000}$, $\Gamma_{i,001}$, 그리고 $\Gamma_{i,01}$은 추후에 다시 사용될 수 없고, 또한 한번 사용된 $\Gamma_{i,00}$와 $\Gamma_{i,010}$은 다시 사용될 수 없다.[19]

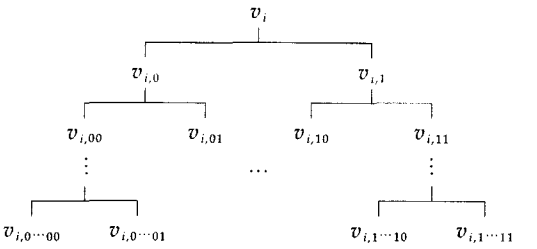


그림 2.5 이산대수문제에 기반을 둔 계층적 구조표

한편, 이산대수문제와 일방향 해쉬함수에 기반을 둔 계층적 구조표는 식 (2.3)에 바탕을 두고 그림 2.5와 같이 두개의 일방향 해쉬함수 h_1, h_2를 이용하여 상위 준위의 절점 값으로 부터 하위 준위의 절점 값을 순차적으로 구할 수 있다. 전자현금의 분할 사용과 익명성을 보장하기 위하여 계층적 구조표는 동일한 준위의 절점을 한번만 사용하거나 사용된 절점의 부가지에 존재하는 절점을 사용하지 않은 경우 사용자의 ID를 알 수 없지만, 상위 준위의 절점과 그의 부가지에 존재하는 하위 준위의 절점 값을 동시에 사용하는 경우 사용자의 구좌번호가 누출될 수 있도록 구성되어야 한다.

상기의 계층적 구조표에서 각각의 절점은 두개의 부가지의 절점을 갖고 있으며, 왼쪽 및 오른쪽의 절점값은 각각 식 (2.3)과 같이 계산될 수 있다.

$$v_{i,0} \equiv v_i \cdot h_1(g_i^{v_i}) \mod p_i - 1$$
$$v_{i,1} \equiv v_i \cdot h_2(g_i^{v_i}) \mod p_i - 1 \qquad (2.3)$$

따라서 상위의 절점 값으로 부터 하위의 절점 값은 쉽게 구할 수 있다. 그러나 하위의 절점 값으로부터 상위의 절점 값 유도는 계산적으로 불가능하다. 상기와 같은 계층적 구조표는 정리 2.1의 특성이 있다.

❖ 정리 2.1 만약 절점 N'이 절점 N의 부가지 상의 절점이라면, $v_{i,N'}/v_{i,N}$은 $g_i^{v_i}$을 이용하여 구할 수 있다.

(증 명) $v_{i,m} \equiv v_i \cdot q(g_i^{v_i}) \mod p_i - 1$을 가정하자. 이 때 식 (2.4)가 성립한다.

$$\begin{aligned} v_{i,m0} &\equiv v_{i,m} \cdot h_1(g_i^{v_{i,m}}) \mod p_i - 1 \\ &\equiv v_i \cdot q(g_i^{v_i}) \cdot h_2(g_i^{v_i \cdot q(g_i^{v_i})}) \mod p_i - 1 \\ &\equiv v_i \cdot q'(g_i^{v_i}) \mod p_i - 1 \end{aligned} \qquad (2.4)$$

따라서, 이를 확장하면 증명이 완료된다.

(증명완료)

제3장 이산대수문제에 바탕을 둔 전자현금 방식

본 장에서는 RSA 암호 알고리듬을 이용한 은닉 서명 기법, 이산 대수문제에 바탕을 둔 계층적 구조표 및 Schnorr의 인증 방식을 이용한 전자현금 프로토콜을 제시하고 관련 성능을 분석한다.[1],[19] 영지식 증명 기법을 이용한 전자현금 방식은 1992년 Pailles가 GQ의 인증방식을 이용한 전자현금 방식을 제시하였다.[8] 본 방식은 전자현금 지불과정에서 Schnorr의 인증 방식을 이용하는 전자현금 방식을 제시한다.

은행은 전자면허 발급용 RSA 파라메타 (e_B, n_B ; d_B)와 전자현금 단위용 RSA 파라메타 (e_B', n_B' ; d_B')을 공개한다. 여기서 (e_B, n_B), (e_B', n_B')는 은행의 공개 정보이고 (d_B, d_B')은 비밀 정보이다. P_u은 고객의 서명문 검증 과정이고 S_u는 고객의 서명문 생성과정이라고 가정한다. 고객은 전자면허 발급과정에서 디지틀 서명용 RSA 알고리듬 (P_u, S_u)을 공개한다. 본 방식은 불법 현금 고객을 검출할 수 있도록 구성되었다. 그러나 이 기능이 필요없을 경우 식 (3.2)에서의 전자현금의 파라메타들 d_i, f_i를 삭제한다.

3.1 전자현금 프로토콜

본 프로토콜은 전자면허 발급과정, 전자현금 발급과정, 전자현금 지불과정, 그리고 예치 과정으로 구성된다. 고객은 은행에서 구좌를 개설할 때, 전자현금을 사용하기 위한 전자면허를 다음과 같은 프로토콜을 이용하여 발급받는다.

가. 전자면허 발급과정

전자면허 발급과정전자면허 발급과정은 고객 P가 정당하게 전자현금을 사용하는 한 오직 한번 수행된다.

① 고객 P는 은닉 서명용 난수 $r_i \in Z_{n_B}^*$, idU를 은닉하기 위한 난수 $r_i \in \{1, \cdots, p_i-2\}$를 선택한다. 난수 f_i는 임의로 선택되며, d_i는 식 (3.1)을 이용하여 계산된다. 한편 d_i, f_i는 불법 고객 검출용 난수들이다.

$$d_i = h_3(S_u[(idU \parallel a_i)], f_i), \quad i = 1, \cdots, 2K \tag{3.1}$$

여기서, h_3는 d_i의 안전성 보장과 비트수를 줄이기 위해 도입된 일방향성 해쉬함수이다. 고객은 소수 p_i와 원시원 g_i을 생성한 후, 식 (3.2)와 같은 u_i, I_i, B_i을 각각 계산한 후, 고객의 구좌번호 idU와 모든 은닉 서명문 B_i를 은행에 전송한다.

$$\begin{aligned} u_i &= idU \parallel a_i \parallel S_u[(idU \parallel a_i)] \\ I_i &\equiv g_i^{u_i} \mod p_i \\ B_i &\equiv r_i^{e_B} \cdot f(I_i, p_i, d_i, f_i) \mod n_B, \\ & \quad i = 1, \cdots, 2K \end{aligned} \tag{3.2}$$

여기서, f는 일방향성 해쉬함수이다.

② 은행 B는 $1 \le i_j \le 2K$, $j = 1, \cdots, K$를 만족하는 i_j를 랜덤하게 선택하여 구한 집합 $G = \{i_j\}$를 고객에게 전송한다. 동작 설명을 단순하게 하기 위하여 은행이 선택한 집합 G를 $\{K+1, K+2, \cdots, 2K\}$라 가정하자.

③ 고객 P는 집합 G의 원소에 대응되는 r_i, a_i, p_i, g_i, d_i, f_i, $S_u[(idU \parallel a_i)]$ $(i = K+1, \cdots, 2K)$을 은행에 전송한다.

④ 은행은 r_i, a_i, p_i, g_i, d_i, f_i, $S_u[(idU \parallel a_i)]$, (for, $i \in G$)를 이용하여 I_i를 계산하고, 식 (3.1)과 식 (3.3)의 관계식이 만족하는가를 검사한다.

$$\begin{aligned} P_u[S_u[(idU \parallel a_i)]] &\stackrel{?}{=} idU \parallel a_i \\ B_i &\stackrel{?}{=} r_i^{e_B} \cdot f(I_i, p_i, d_i, f_i) \mod n_B \end{aligned} \tag{3.3}$$

⑤ 식 (3.3)의 관계식이 만족되면 은행 B는 단계 1에서 수신한 B_i 중에서 G에 속하지 않는 i에 해당하는 B_i를 이용하여 식 (3.4)와 같이 전자면허를 위한 은행의 서명문 E를 계산하여 고객 P에게 전송한다.

$$\begin{aligned} E &\equiv \prod_{i=1}^{K} [B_i]^{d_B} \mod n_B \\ &\equiv \prod_{i=1}^{K} [r_i^{e_B} \cdot f(I_i, p_i, d_i, f_i)]^{d_B} \mod n_B \\ &\equiv \prod_{i=1}^{K} r_i \cdot \prod_{i=1}^{K} f(I_i, p_i, d_i, f_i)]^{d_B} \mod n_B \end{aligned} \tag{3.4}$$

⑥ 고객 P는 식 (3.4)와 같은 은행의 서명문 E로부터 전자면허 EL을 식 (3.5)와 같이 계산하고, 그 타당성을 식 (3.6)과 같이 확인한다. 그리고 전자면허로 EL, $(I_i, p_i, g_i, a_i, d_i, f_i)$, $(i = 1, \cdots, K)$를 보관한다.

$$\begin{aligned} EL &\equiv E / \prod_{i=1}^{K} r_i \mod n_B \\ &\equiv \prod_{i=1}^{K} r_i \cdot \prod_{i=1}^{K} f(I_i, p_i, d_i, f_i)]^{d_B} / \prod_{i=1}^{K} r_i \mod n_B \\ &\equiv \prod_{i=1}^{K} f(I_i, p_i, d_i, f_i)]^{d_B} \mod n_B \end{aligned} \tag{3.5}$$

$$EL^{e_B} \stackrel{?}{=} \prod_{i=1}^{K} f(I_i, p_i, d_i, f_i)] \mod n_B \tag{3.6}$$

은행 B는 전자현금의 가치를 표시하기 위한 RSA 암호 알고리듬인 $(e_B', n_B' ; d_B')$를 준비한다. 여기서, n_B'는 두개의 큰 소수 p', q'의 곱이고 (e_B', n_B)는 공개 정보이며 d_B'는 비밀 정보이다. 이는 전자현금 발급 과정에서 이용된다.

나. 전자현금 발급 과정

고객이 은행으로부터 전자현금을 발급받는 절차는 다음과 같다.

① 고객 P는 난수 은닉 서명을 위한 $r_i \in Z_{n_B}{}^*$ 현금트리의 시초값 $v_i \in \{0, 1, \cdots, p_i-2\}$, 그리고 전자현금 면허의 노출을 방지하기 위한 $m_i \in Z_{n_B}{}^*$ $(i = 1, \cdots, K)$를 선택한다. 그리고 그림 3.1과 같은 계층적 구조표의 절점 값들 $v_{i,l}$을 식 (3.7)을 이용하여 계산한다. 그림 3.1에서의 계층적 구조표의 절점값 계산을 위한 모든 연산은 모듈러 p_i 상에서 수행된다.

$$v_{i,0} \equiv v_i \cdot h_1(g_i^{v_i}), \quad v_{i,1} \equiv v_i \cdot h_2(g_i^{v_i}) \qquad (3.7)$$

고객은 식 (3.8)과 같은 T_i와 식 (3.9)와 같이 z_i를 계산한 후, 은행 B에 idU, $\{z_1, z_2 \cdots, z_K\}$, 그리고 은닉 서명문 인증용 $S_u[f(z_1, z_2 \cdots, z_K)]$를 은행에 전송한다. 여기서 T_i는 각각의 $v_{i,l}$에 대한 서명문 계산을 예방하고 지불과정에서 이용하는 $v_{i,l}$이 정당하다는 것을 입증하는데 이용된다. 이는 전자현금 정보의 일부로 포함된다.

$$T_i \equiv (w_i, w_{i,0}, w_{i,1}, w_{i,00}, w_{i,01}, \cdots, w_{i,l}) \qquad (3.8)$$

여기서, 식 (3.8)의 변수들 $w_i = h(g_i^{v_i} \bmod p_i) = h(J_i)$, $w_{i,0} = h(g_i^{v_{i,0}} \bmod p_i) = h(J_{i,0})$, $w_{i,1} = h(g_i^{v_{i,1}} \bmod p_i) = h(J_{i,1})$, $\cdots$, $w_{i,l} = h(g_i^{v_{i,l}} \bmod p_i) = h(J_{i,l})$이다.

$$z_i \equiv r_i^{e_B} \cdot f(EL_i, T_i) \mod n_B \qquad (3.9)$$

여기서, l은 현금 트리의 준위, h, h_1, h_2는 일방향성 해쉬함수들, 그리고 $EL_i = EL \oplus m_i$이다.

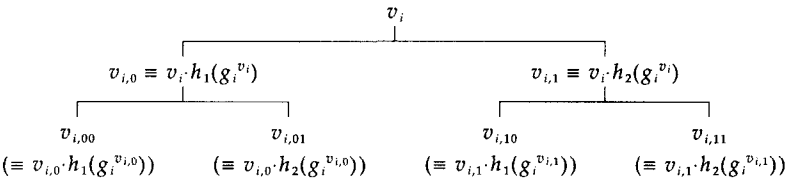


그림 3.1 계층적 구조표

② 은행은 수신된 z_i를 이용하여 계산된 $f(z_1, \cdots, z_K)$와 $P_u[S_u[f(z_1, \cdots, z_K)]]$가 동일한가를 확인함으로서 수신된 메세지가 진실된 고객으로 부터 왔음을 확인한다. 그리고 은행 B는 $1 \le i_j \le K$, $j = 1, \cdots, K/2$를 만족하는 i_j를 랜덤하게 선택한 집합 $G' = \{i_j\}$을 고객 P에게 전송한다. 개념의 단순화를 위하여 집합 G'의 원소를 $\{K/2+1, K/2+2, \cdots, K\}$라 가정한다.

③ 고객 P는 r_i, T_i, v_i, EL_i, for $i \in U'$, (즉 $i = K/2+1, \cdots, K$)를 은행 B에 전송한다.

④ 은행 B는 수신된 v_i를 이용하여 T_i'를 계산한 후, 수신된 T_i와 같은가를 확인한다. 그리고 식 (3.10)이 성립하는가를 검사한다.

$$z_i \stackrel{?}{=} r_i^{e_B} \cdot f(EL_i, T_i) \mod n_B' \qquad (3.10)$$

⑤ 은행 B는 단계 ①에서 수신한 z_i 중에서 G'에 속하지 않는 지수 i에 해당하는 z_i와 식 (3.11)을 이용하여 전자현금을 위한 은행의 서명문 BC를 계산하여 고객 P에 전송한다. 그리고, 현재 발행되고 있는 현금 액수를 고객 P의 구좌에서 인출한다.

$$BC \equiv \prod_{i=1}^{K/2} [z_i]^{d_B'} \mod n_B'$$

$$\equiv \prod_{i=1}^{K/2} [r_i^{e_B} \cdot f(EL_i, T_i)]^{d_B'} \mod n_B'$$

$$\equiv \prod_{i=1}^{K/2} r_i \cdot \prod_{i=1}^{K/2} f(EL_i, T_i)]^{d_B'} \mod n_B' \quad (3.11)$$

⑥ 고객 P는 식 (3.12)와 같이 은행의 서명문 BC로 부터 전자현금 C를 계산하고, 그 타당성을 식 (3.13)을 이용하여 확인한다. 그리고 전자현금으로 C, $\{v_i, T_i, m_i, \text{for } i = 1, \cdots, K/2\}$를 보관한다.

$$\begin{aligned} C &\equiv BC/\prod_{i=1}^{K/2} r_i \mod n_B' \\ &\equiv \prod_{i=1}^{K/2} r_i \cdot \prod_{i=1}^{K/2} f(EL_i, T_i)]^{d_B'} / \prod_{i=1}^{K/2} r_i \mod n_B' \\ &\equiv \prod_{i=1}^{K/2} f(EL_i, T_i)]^{d_B'} \mod n_B' \end{aligned} \quad (3.12)$$

$$C^{e_B'} \doteq \prod_{i=1}^{K/2} f(EL_i, T_i)] \mod n_B' \quad (3.13)$$

다. 전자현금 지불과정

고객은 상점에 $75의 전자현금을 지불하기 위하여 상점과 다음과 같은 프로토콜을 수행한다. 지불과정은 다음 프로토콜의 단계 ①에서 단계 ④의 과정을 $i = 1, \cdots, K/2$ 동안 반복함으로서 실현된다. 전자현금 지불과정에서는 고객이 $v_{i,l}$과 u_i를 알고 있다는 것을 I_i, J_i를 이용하여 상점에 입증하는 과정이다. 여기서 z_1, z_2는 초기에 "1"로 세트한다.

① 고객 P는 $v_{i,0}$를 이용하여 그림 3.1에서의 $75에 대응되는 절점 값 $J_{i,0}$, $J_{i,10}$을 식 (3.14)와 같이 계산한다. 그리고 I_i를 식 (3.15)를 이용하여 계산한다. 그후, I_i, T_i, $J_{i,0}$, $J_{i,10}$, p_i, g_i, d_i, f_i, m_i, $i = 1, \cdots, K/2$, 그리고 EL을 상점에 전송한다.

$$\begin{aligned} J_{i,0} &\equiv g_i^{v_{i,0}} \mod p_i, \\ J_{i,10} &\equiv g_i^{v_{i,10}} \mod p_i \end{aligned} \quad (3.14)$$

$$\begin{aligned} u_i &= idU \| a_i \| S_u[(idU \| a_i)] \\ I_i &= g_i^{u_i} \mod p_i \end{aligned} \quad (3.15)$$

② 상점 V는 T_i의 준위 0, 10의 부분 비트가 각각 $h(J_{i,0})$, $h(J_{i,10})$와 같은가를 확인한다. 그리고 은행으로부터 통보받은 불법 고객 리스트 $S_u[(idU \| a_i)]$를 참고로 $d_i \doteq h_3(S_u[(idU \| a_i)], f_i)$가 성립하는가를 검사한다. 그후 상점은 난수 $n_{i,0}$, $n_{i,10} \in \{1, \cdots, p_i-1\}$ $(i = 1, \cdots K/2)$를 선택하여 고객 P에게 전송한다. 그리고 식 (3.16)을 이용하여 z_1, z_2를 계산한다.

$$\begin{aligned} z_1 &:= z_1 \cdot f(I_i, p_i, d_i, f_i) \mod n_B \\ z_2 &:= z_2 \cdot f(EL_i, T_i) \mod n_B' \end{aligned} \quad (3.16)$$

여기서, $EL_i = EL \oplus m_i$이다.

③ 고객 P는 식 (3.17)과 같이 $y_{i,0}$, $y_{i,10}$를 계산하여, $(y_{i,0}, y_{i,10})$를 상점 V에 전송한다.

$$\begin{aligned} y_{i,0} &\equiv v_{i,0} + n_{i,0} \cdot u_i \mod p_i-1 \\ y_{i,10} &\equiv v_{i,10} + n_{i,10} \cdot u_i \mod p_i-1 \end{aligned} \quad (3.17)$$

④ 상점 V는 다음의 식 (3.18)가 성립하는가를 확인한다.

$$\begin{aligned} g_i^{y_{i,0}} &\doteq J_{i,0} \cdot (I_i)^{n_{i,0}} \mod p_i \\ g_i^{y_{i,10}} &\doteq J_{i,10} \cdot (I_i)^{n_{i,10}} \mod p_i \end{aligned} \quad (3.18)$$

⑤ 고객은 전자현금 C와 $\prod_{i=K/2}^{K} f(I_i, p_i, d_i, f_i)$를 상점에 전송한다.

⑥ 상점은 불법 고객 리스트 시험을 수행하여 과정 ②에서의 결과들이 모두 일치하면, 현재 거래중인 고객은 불법 고객으로 간주하고 지불을 거부한다. 상점의 불법 리스트 관련 정보를 줄이기 위하여 상점은 3-5 개의 $S_u[(idU \| a_i)]$만을 저장하고 이를 시험하여 불법 고객 여부를 판단할 수 있다. 상점은 식 (3.19)의 관계식이

만족한가를 확인한다. 그리고 모두 만족하면 식 (3.20)과 같은 고객과의 통신내용 H를 보관한다.

$$EL^{e_B} \stackrel{?}{=} z_1 \cdot \prod_{i=K/2}^{K} f(I_i, p_i, d_i, f_i) \mod n_B,$$
$$C^{e_B} \stackrel{?}{=} z_2 \mod n_B' \qquad (3.19)$$

$$H = \begin{cases} \{I_i, T_i, p_i, g_i, J_{i,0}, J_{i,10}, n_{i,0}, n_{i,10}, y_{i,0}, \\ y_{i,10}, d_i, f_i, m_i\}, \text{ for } i = 1, \cdots, K/2 \\ EL, C' \end{cases} \qquad (3.20)$$

부정한 의도를 가진 고객이 전자현금 발행시 사용하지 않았던 v_i를 전자현금 지불시 사용하면 불법 사용 사실을 숨길 수 있는 것처럼 보이나, 이는 T_i의 내용을 변경하게 되고 결국 전자현금의 변경을 의미하게 되므로 다른 v_i를 사용할 수 없다. 상점 V는 식 (3.20)과 같은 정보를 이용하여 해당 현금과 관련된 어떤 새로운 정보도 생성할 수 없다.

라. 현금 예치과정

상점 V가 고객 P로 부터 받은 전자현금에 상당하는 금액을 은행에 예치하기 위해 통신내용 H를 은행 B에 전송한다. 은행 B는 상점으로 부터 받은 H의 타당성을 확인한 후, 상점 V의 구좌에 사용된 금액을 예치한다. 또 은행은 고객의 전자현금 중복 사용을 대비하여 통신내용 H를 자신의 데이타베이스에 저장한다. 이 과정은 은행이 상점에서 수행한 과정을 거의 반복하는 현금 지불 과정의 유효성 확인 과정과 재사용 검출 과정으로 구성된다. 은행의 데이타베이스에 저장되어야 할 정보는 C와 EL을 해쉬해서 저장하는 H_1부와 나머지 정보를 저장하는 H_2부로 구성되어 있다. 재사용 검출은 동일한 C, EL이 발견되었는가 판단하고, 발견되면 동일한 위치의 l과 l'이 중복 사용되었는가, 또는 사용된 절점의 상하 절점들이 사용되었는가를 판단함으로서 이루어진다.

3.2 특성 및 안전성 분석

전자면허의 발행단계에서 고객의 고유정보 idU는 $I_i \equiv g_i^{idU \| a_i \| S_M[(idU \| a_i)]} \mod p_i$와 연관되므로 이산대수문제가 어렵다는 가정하에서 고객이 정당하게 프로토콜을 수행한다면, 비록 은행과 상점의 공모가 있을지라도, 은행과 상점은 고객의 고유정보에 관한 어떤 지식도 얻을 수 없다. 본 방식은 그림 3.1과 같이 일방향 해쉬함수 h_1, h_2를 이용한 계층적 구조표를 이용하여 전자현금의 분할 사용을 가능케 하였다. 본 방식은 계층적 구조표에서의 준위가 크면 스마트카드에서 요구되는 계산량이 증가하는 특성이 있으므로 계층적 구조표의 준위가 작은 전자현금 시스템에 매우 유용한 전자현금 시스템이다. 실제의 전자현금에서는 구조표의 준위가 작은 경우가 널리 이용될 수 있을 것이다.

고객이 불법적으로 전자현금을 한번 이상 사용하거나 계층적 구조표 상의 한 절점을 사용하고 이 절점과 연관된 상하 절점을 사용하는 경우에 은행은 고객의 구좌번호 idU를 정리 3.1를 이용하여 구할 수 있다.

❖ **정리 3.1** 사용자가 절점 $v_{i,0}$와 절점 $v_{i,00}$를 사용한 경우, 은행은 사용자의 구좌 번호를 알 수 있다.

(증 명) 은행이 상점으로부터 수신한 통신내용은 식 (3.21)과 같은 정보를 갖고 있다.

$$J_{i,0} \equiv g_i^{v_{i,0}} \mod p_i,$$
$$J_{i,00} \equiv g_i^{v_{i,00}} \mod p_i \qquad (3.21)$$

절점 $v_{i,0}$와 절점 $J_{i,00}$와의 관계는 식 (3.22)와 같다.

$$v_{i,00} \equiv v_{i,0} \cdot h_1(g_i^{v_{i,0}})$$
$$\equiv v_{i,0} \cdot h_1(J_{i,0})$$

$$\equiv v_{i,0} \cdot Q_{i,0} \qquad (3.22)$$

한편, $y_{i,0}$, $y_{i,00}$와 $n_{i,0}$, $n_{i,00}$의 관계는 식 (3.23)과 같다.

$$y_{i,0} \equiv v_{i,0} + n_{i,0} \cdot u_i \mod p_i - 1$$
$$y_{i,00} \equiv v_{i,00} + n_{i,01} \cdot u_i \mod p_i - 1 \qquad (3.23)$$

식 (3.23)의 두번째 식에 식 (3.22)를 대입하면 식 (3.24)와 같다.

$$y_{i,00} \equiv v_{i,00} \cdot Q_{i,0} + n_{i,01} \cdot u_i \mod p_i - 1 \qquad (3.24)$$

식 (3.23)의 첫번째 식에 $Q_{i,0}$를 곱하면 식 (3.25)와 같이 된다.

$$Q_{i,0} \cdot y_{i,0} \equiv v_i \cdot Q_{i,0} + n_{i,0} \cdot u_i \cdot Q_{i,0} \mod p_i - 1 \qquad (3.25)$$

식 (3.24), (3.25)를 이용하면 식 (3.26)과 같이 u_i를 구할 수 있고, 이것으로 부터 고객의 구좌번호 idU를 구할 수 있다.

$$u_i \equiv (Q_{i,0} \cdot y_{i,0} - y_{i,00}) / (n_{i,0} \cdot Q_{i,0} - n_{i,01}) \qquad (3.26)$$

(증명완료)

k = 40, $|p_i|$ = 600 bits, 계층적 구조표의 준위가 3, 그리고 일방향 해쉬함수 h의 길이가 72-bit일 경우, 2개의 절점이 사용되는 경우에 고객이 저장해야 할 정보량은 대략 5.74Kbyte이고, 고객이 지불절차에서 통신중 교환되어야 할 정보량은 약 11.5Kbyte이다. 또 고객 측면에서 평균적으로 26개의 온라인 지수연산, 20개의 오프라인 지수연산, 46개의 곱셈연산, 그리고 현금지불을 위하여 26개의 해쉬함수가 필요하다. 본 방식은 연산이 소수 및 합성수상에서 수행되며 불법현금검출을 위해 상점에서의 보조 저장장치를 요구한다.

3.3 전이 가능한 전자현금 프로토콜

본 전자현금 방식의 전이 가능한 전자현금 프로토콜은 고객 P_1, P_2가 은행에서 전자면허를 발급받는 과정, 고객 P_1이 은행에서 전자현금을 발급받는 과정, 고객 P_2가 별도의 RSA 알고리듬을 이용하여 전이용 전자현금을 생성받는 과정, 고객 P_1과 고객 P_2간의 전자현금을 전이하는 과정, 고객 P_2가 전이받은 전자현금을 상점에 지불하는 과정, 그리고 상점이 그 지불된 전자현금을 은행에 예치하는 과정으로 구성된다. 전자현금을 전이하는 일반적인 방법은 Chaum-Pedersen[7]에 의해 제시되었다. 본 전자현금의 전이 가능 프로토콜은 CP의 방식을 이용하여 고안되었다. 전자면허와 현금의 발행과정은 3.1절에서 제시된 것과 동일하다. 은행 B는 전이 현금을 위하여 3.1절에서 기술한 기본적인 RSA 알고리듬외에 현금적 가치가 전혀 없는 또다른 RSA 알고리듬 (e_t, n_t ; d_t)를 준비해야 한다. 전이 가능한 전자현금 프로토콜의 구성은 ① P_1과 P_2는 은행 B로 부터 전자면허를 얻는 과정, ② P_1이 발행받은 현금을 P_2에게 전이하는 과정, ③ P_2가 전이받은 현금을 상점 V에 지불하는 과정으로 이루어진다. 자세한 프로토콜은 참고문헌 [20]를 참조하기 바란다.

3.4 기존의 방식과의 비교

본 절에서는 전자면허의 발행 유무, 익명성 보장을 위한 수학적 배경, 추적 불가능성, 분할 사용 가능성, 재사용 불가능성, 전이 가능성 및 지불과정에서의 서명문 생성을 위한 계산적 복잡성 측면에서, 지금까지 발표된 전자현금 알고리듬의 대표적인 방식들인 Chaum 등의 방식, Okamoto-Ohta의 방식과 제안된 방식을 비교한다.

표 3.1 특성 비교

비교항목 \ 방식	Chaum 등	Okamoto-Ohta	본 방식
전자면허의 유무	무	유	유
익명성 보장을 위한 수학적 배경	소인수분해문제	소인수분해문제	이산대수문제와 소인수분해문제
분할 사용 가능성	×	○	○
익명성	○	○	○
재사용 검출	○	○	○
전이 가능성	×	○	○
계산량(지불시)	간단	이차근을 구하는 문제	모듈러 곱셈 연산

제4장 결 론

본 논문에서는 이산대수문제와 소인수분해문제에 기반을 두고 Schnorr의 영지식 인증기법을 이용한 새로운 전자현금 프로토콜을 제시하였다. 본 방식의 특징은 한번 사용하는 경우 익명성이 보장되지만 두번 사용하는 경우 고객의 구좌 번호가 밝혀지며, 현금의 분할 사용과 현금의 전이가 가능하다. 본 방식은 전자면허 발급과정, 전자현금 발급과정, 전자현금 지불과정, 그리고 전자현금 예치 과정 등으로 구성되고 있다. 전자면허 발급과정과 전자현금 발급과정에서는 은닉 RSA 서명 기법을 이용하였으며, 전자현금 사용시에는 계층적 구조표와 Schnorr의 인증기법을 이용하였다. 그리고 이산대수문제와 2개의 일방향 해쉬함수를 이용하여 새로운 계층적 구조표를 구성하여 전자현금의 분할 사용을 가능하게 하였고 동일한 현금을 한번 이상 사용하면 고객의 구좌번호가 밝혀지며, 불법 현금 리스트를 각각의 상점에 저장해 두었다가 불법 현금 사용 여부를 검사할수 있게 하였다. 그리고 전이가능한 전자현금 방식의 기본 원리 및 과정을 제시하였다. 본 제안 방식은 스마트카드를 이용한 전자현금 시스팀에 활용될 수 있다.

참 고 문 헌

[1] 이석래, 염홍열, "스마트카드에 적용가능한 전자현금 방식," 데이타보호 기반 기술 WORKSHOP 논문집, pp.3-29, 1993.8.

[2] Claus P. Schnorr, "Efficient Identification and Signatures for Smart Cards," CRYPTO '89, Lecture Notes in Computer Science, vol.435, pp.239-252, Springer-Verlag, 1990.

[3] D. Chaum, "Security Without Identification : Transation Systems to Make Big Brother Obsolete," Comm. of the ACM, vol.28, no.10, pp.1030-1044, 1985.

[4] D. Chaum, "Blind Signatures for Untraceable Payments," Proceeding of Crypto '82, pp.199-203, 1982.

[5] D. Chaum, "On-line Cash Checks," Eurocrypt '89, Lecture Notes in Computer Science, Springer-Verlag, pp.288-293, 1990.

[6] D. Chaum, A. Fiat and M. Noar, "Untraceable Electronic Cash."

CRYPTO '88, Lecture Notes in Computer Science, vol.403, pp.319-327, Springer-Verlag, 1989.

[7] D. Chaum, B.d. Boer, E.V. Heyst, S. Mjølsnes and A. Steenbeek, "Efficient Offline Electronic Checks," EUROCRYPT '89, Lecture Notes in Computer Science, vol.434, pp.294-301, Springer-Verlag, 1990.

[8] D. Chaum and T. P. Pedersen, "Transferred Cash Grows in Size," Proceeding of Eurocrypt '92, pp.357-367, 1992.

[9] J. C. Pailles, "New Protocols for Electronic Money," Proceeding of AUSCRYPT '92, pp.7.1-7.6, Gold-Coast, Australia, 1992.

[10] 木下, S. Tsujii, "プライバシー保護を 考慮した 電子資金移動方式の 提案", 신학론 D, Vol. J70-D, No. 12, pp. 2713-2721, 1987, 12.

[11] 松本, 高島, 赤池, 今井, "電子手形處理 : IC - ｸｰﾄﾞを 用いた 新しい EFT", WCIS '87 論文集, 1987, 7.

[12] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," Comm. ACM,, vol.21, no.2, pp.120-126, 1977.

[13] Rhee, M.Y,Cryptography and Secure Communications, McGraw-Hill, New York, 1993.

[14] S. B. Weinstein, "Smart Credit Cards : the answer to cashless shopping," IEEE, Sprectrum, pp.43-49, 1984, 2.

[15] S. Even, O. Goldreich, Y. Yacobi, "Electronic Wallet," Proceeding of Crypto '83, pp.383-386, 1983.

[16] T. ElGamal, "A Public-Key Cryptosystem and Signature Scheme Based on Discrete Logarithm," IEEE Trans. on Inform. Theory.IT-31, pp. 469-472, 1985.

[17] T. Okamoto and K. Ohta, "Dispoaable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash," CRYPTO '89, Lecture Notes in Computer Science, vol.435, pp.481-497, Springer-Verlag, 1990.

[18] T. Okamoto and K. Ohta, "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility," EUROCRYPT '89, Lecture Notes in Computer Science, vol.434, pp.134-149, Springer-Verlag, 1990.

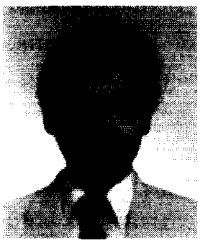
[19] T. Okamoto and K. Ohta, "Universal Electronic Cash," CRYPTO '91, Lecture Notes in Computer Science, pp.324-337, Springer-Verlag, 1992.

[20] Youm, H.Y., Lee, S.L., and Rhee, M.Y., " Practical Protocols for Electronic cash," proceeding of JW-ISC, pp. 10-22, Oct. 1993.

[21] 염홍열, "디지틀 서명 방식 고찰," 한국통신정보보호학회지, 제3권 제2호, pp. 7-18, 1993. 6.

[22] 이석래, "스마트카드에 적용가능한 전자현금 방식," 석사학위논문, 한양대학교, 1993. 12.

□ 著者紹介



염 흥 열 (정회원)

1981년 漢陽大學校 電子工學科 卒業(學士)
1983년 漢陽大學校 大學院 電子工學科 卒業(工學碩士)
1990년 漢陽大學校 大學院 電子工學科 卒業(工學博士)
1982년 12월 ~ 1990년 9월 韓國電子通信研究所 先任研究員
1990년 3월 ~ 현재 順天鄕大學校 工科大學 電子工學科 助教授

※ 관심분야 : 암호이론, 부호이론, 이동통신 분야

이 석 래

1988년 3월 ~ 1992년 2월 한양대학교 전자통신공학과 (학사)
1992년 3월 ~ 1994년 2월 한양대학교 대학원 전자통신공학과 (석사)
1994년 3월 ~ 현재 LG 전자기술원 연구원

이 만 영 (종신회원)

1924년 11월 30日生
서울大學校 電氣工學科 工學士(BSEE)
美國 Colorado 大學校 工學碩士(MSEE) 및 工學博士(Ph. D.)
美國 Virginia 州立大 工科大學 教授
美國 California Institute of Technology, JPL 責任研究員
國防科學研究所 第1副所長/韓國電子通信 社長/三星半導體通信 社長/漢陽大副總長
現 : 漢陽大 名譽教授/韓國通信情報保護學會 會長
著書 : Error Correcting Coding Theory, McGraw-Hill, New York, 1989.
Cryptography and Secure Communications, McGraw-Hill, New York, 1993.