通信情報保護學會論文誌
第 11 券 第 1 號, 2001. 2

거스름의 재사용이 가능한 온라인 전자수표시스템

김 상 진*, 최 이 화*, 오 희 국*

Refunds Reusable Online Electronic Check System

Sangjin Kim*, Ihwa Choi*, Heekuck Oh*

요 약

전자수표는 계산량이나 정보교환량 측면에서 전자동전보다 효율적인 지불수단이다. 그럼에도 불구하고 수표의 액면가가 제한되어 있고, 대금지불 과정에서 발생하는 거스름의 재사용이 용이하지 않기 때문에 활성화되지 못하고 있다. 이 논문은 기존의 전자수표시스템이 가지고 있는 이러한 문제점을 해결한 새로운 전자수표시스템을 제안한다. 이 시스템은 부분은닉서명 기법을 이용하여 수표의 액면가를 임의로 표현할 수 있으며 거스름의 형태가 수표와 같아서 이를 다시 사용할 수 있다. 물론 수표의 익명성이 보장되며, 수표를 사용하고 받은 거스름은 어떤 수표의 거스름인지를 알 수 없다. 그밖에 일회성 비밀키를 수표의 일련번호로 활용함으로써 지불의 효율성을 높였으며, 온라인 지불의 문제점을 극복하고자 같은 상점과는 오프라인으로 다중 지불세션을 가질 수 있도록 하였다. 이 과정에서 부인방지 기능을 제공하기 위해 일방향 축적기를 사용하였다. 새로운 시스템의 안전성, 효율성, 원자성에 대해 분석하였고, 기존의 전자수표시스템과 비교하였다.

ABSTRACT

Electronic check schemes are more efficient than electronic coin schemes with respect to computational costs and the amount of information exchanged. In spite of these, difficulties in making a refund reusable and in representing the face value of a check have discouraged its development. In this paper, a new online electronic check system is presented, which solves the above problems. This system uses the partially blind signature to provide user anonymity and to represent the face value of a check. The partially blind signature enables us to make the format of refunds and initially withdrawn checks identical. Thus, it allows refunds to be reused to buy goods without any limitations. Both initially withdrawn checks and refunds in our system guarantee untraceability as well as unlinkability. We also use a one-time secret key as the serial number of a check to increase the efficiency of payments. The presented check system also provides multiple offline shopping sessions to minimize the number of online messages handled by a bank. During the multiple offline shopping session, we use a one-way accumulator to provide non-repudiation service. We also analyze our new system's security, efficiency, and atomicity.

keyword : *electronic payment system, electronic check system, partially blind signature, reusable refund, one-way accumulator*

Ⅰ. 서 론

전자화폐(electronic cash)는 David Chaum[1]이 1982년에 처음 소개한 이후 많은 발전을 거듭하여 오늘날까지 다양한 모델과 시스템이 개발되었다.[2~6] 전자화폐는 전자상거래에서 지불수단으로 사용하기 위해 개발된 화폐로서, 모든 것이 전자적으로 처리되며, 디지털 정보 형태로 표현되므로 통신망으로 전달이 가능하다. 이상적인 전자화폐란 기존의 실물화폐가 가지고 있는 장점과 명령에 의한 지불방식

* 한양대학교 컴퓨터공학과 분산컴퓨팅연구실 ({sangjin,ihwa,hkoh}@cse.hanyang.ac.kr)

(payments by instruction)이라고 불리는 신용카드와 같은 지불수단의 장점만을 가지는 전자화폐를 말한다. 즉, 이상적인 전자화폐는 실물화폐가 가지고 있는 익명성(anonymity), 분할성(divisibility), 양도성(transferability), 오프라인(offline)과 같은 특성을 지니는 동시에 명령에 의한 지불방식처럼 하나의 정보로 취급될 수 있어야 한다. 그러나 이상적인 전자화폐를 만드는 것은 쉽지 않으며, 많은 연구가 있었지만 아직까지 효율성과 경제성까지 고루 갖춘 이상적인 전자화폐는 등장하지 않고 있다. 이 때문에 현재 인터넷 등에서는 신용카드 기반의 지불방식이 널리 사용되고 있다. 그러나 신용카드 기반의 지불방식은 처리비용과 수수료 때문에 소액지불에 적합하지 않을 뿐만 아니라 익명성, 오프라인과 같은 특성을 제공하지 못한다. 따라서 발전되고 있는 전자상거래 시장이 보다 활성화되기 위해서는 전자화폐에 대한 지속적인 연구가 필요하다.

전자화폐는 쓰임새에 따라 분류하는 방법이 다양하다. 전자화폐가 하드웨어 기반인지 아니면 소프트웨어만으로 구성되어 있는지에 따라 분류하기도 하고, 거래규모에 따라 고액, 소액화폐로 분류하기도 한다. 이런 분류 가운데 전자화폐를 전자동전(electronic coin)방식[2]과 전자수표(electronic check)방식[3]으로 분류하는 것이 있다. 전자동전방식에서는 각 동전이 고정된 액면가를 가지고 있으며, 고객은 지불대금에 맞도록 필요한 개수의 동전을 이용하여 지불한다. 이와는 달리 전자수표방식에서는 시스템이 정해놓은 고정된 금액의 수표 또는 고객이 원하는 금액의 수표를 인출 받아 지불한다. 전자수표는 수표 하나만으로도 지불이 가능하기 때문에 여러 개의 동전을 사용해야하는 전자동전방식보다는 계산량이나 정보교환량 측면에서 효율적이다.[3,7]

전자수표방식이 전자동전방식보다 효율적인 지불수단임에도 불구하고 활성화되지 못한 것에는 몇 가지 이유가 있다. 첫째, 거스름에 대한 처리가 복잡하고 제한적이다. 전자수표방식의 경우 수표의 액면가와 지불대금이 언제나 일치할 수는 없다. 이런 경우가 발생하면 고객은 지불한 수표에 대한 거스름을 돌려 받아야 한다. 거스름은 지불대금과 사용된 수표의 액면가에 따라 다양한 금액이 될 수 있다. 또한 거스름의 형태는 재사용이 가능한 수표가 바람직하며 처음에 인출한 수표와 마찬가지로 익명성이 보장되어야 한다. 이 때 거스름으로 발행된 수표는 대금지불에 사용된 고객의 수표와 어떤 연관관계도 없어야 한다. 그러나 이와 같은 거스름 메커니즘을 제공하기란 쉽지 않다. 현재까지 제안된 전자수표방식은 시스템이 정해놓은 고정된 금액의 수표만을 인출할 수 있으며, 액면가 표현방법의 한계 때문에 지불과정에서 발생한 거스름을 일부 제한된 금액에 대해서만 다시 사용할 수 있는 단점을 가지고 있다.[3,7,8] Chaum의 전자수표시스템은 이러한 거스름의 문제점을 그대로 가지고 있다.[3] Chaum이 제안한 쿠키통(cookie-jar) 방식은 거스름을 재사용하기 보다는 이를 축적해 놓고 나중에 은행에 입금할 수 있다. Chaum 시스템 이후에 발표된 전자수표시스템에도 이러한 문제는 여전히 해결되지 않고 있다.[7,8] 만일 효율적인 액면가 표현방법과 재사용이 가능한 거스름 메커니즘이 제공되면 전자수표방식은 전자동전방식보다 궁극적으로 효율적인 지불수단이 된다.

둘째, 오프라인 방식의 전자수표시스템을 만드는 것이 어렵다. 전자수표시스템도 전자동전시스템처럼 지불방식에 따라 온라인 방식과 오프라인 방식으로 분류할 수 있다. 통신비용, 통신지연 등 여러 문제점 때문에 전자화폐는 궁극적으로는 오프라인 방식이어야 한다. 그러나 오프라인 전자수표시스템은 수표 발행기관인 은행의 참여 없이 고객과 판매자간에 이루어지는 지불과정에서 거스름을 생성해야 하는 근본적인 문제점을 지니고 있다. 이것은 Chaum 등이 제안한 시스템처럼 효율성이 매우 떨어지는 cut-and-choose 방법을 사용하지 않으면 해결하기가 쉽지 않다.[8] 이 시스템은 오프라인으로 거스름을 생성할 수는 있으나 거스름을 지불에 다시 사용할 수는 없다. Deng 등은 온라인 전자수표시스템을 제안하면서 온라인 시스템의 문제점을 극복하기 위해 같은 상점과 오프라인으로 다중 지불세션을 가질 수 있는 기능을 제공한다.[7]

이 논문은 앞에서 서술한 기존의 전자수표시스템이 갖고 있는 문제점에 대한 해를 제공한다. 이 논문에서 제안하고 있는 전자수표시스템의 특성을 간단히 요약하면 다음과 같다.

- 임의의 액면가를 가지는 수표를 인출할 수 있다.
- 거스름의 형태가 재사용이 가능한 새로운 수표가 되며, 처음에 인출한 수표와 마찬가지로 익명성이 보장된다.
- 거스름으로 발행된 수표로부터 대금지불에 사용된 고객의 수표를 알 수 없다.
- 온라인 시스템의 문제점을 극복하기 위하여 같은

상점하고 연속적으로 거래할 경우에는 오프라인으로 이루어질 수 있도록 다중 지불세션 기능을 지원한다.
- 지불과정의 계산효율을 높이기 위해 공개키 대신에 일회성 비밀키를 사용한다.
- 오프라인으로 이루어지는 다중 지불세션에서 부인방지(non-repudiation) 기능을 제공하기 위해 일방향 축적기(one-way accumulator)를 사용한다.

이 논문에서 제안하는 전자수표시스템은 부분은닉서명(partially blind signature)[9]을 사용하여 수표의 익명성을 보장하였고 거스름의 재사용을 가능하게 하였다. 부분은닉서명을 사용하면 차액에 대해 익명으로 새로운 수표를 발행할 수 있기 때문에 이를 거스름으로 사용한다. 또한 온라인 시스템의 문제점을 극복하기 위해 Deng 등이 제안한 시스템과 마찬가지로 같은 상점과 오프라인으로 다중 지불세션을 가질 수 있다. 그밖에 이 시스템은 지불의 효율성을 높이기 위해 두 개의 일회성 비밀키를 수표에 포함한다. 일회성 비밀키는 수표의 일련번호 역할을 하며 비밀이 요구되는 정보를 교환하기 위해 사용된다. 특히, 전자상거래에서 디지털 상품을 암호화하기 위해 활용된다. 대부분의 전자화폐는 일련번호로 난수를 사용하며,[1-6] 일회성 공개키를 사용하는 경우도 있다.[7] 일회성 비밀키를 사용하면 지불과정에 필요한 계산량을 줄여주지만 두 참여자가 키를 공유하기 때문에 부인방지 기능을 제공하는 것이 어렵다. 특히 오프라인으로 이루어지는 다중 지불세션에서는 나중에 발생할 수 있는 분쟁을 해결하기 위해서는 부인방지 기능을 반드시 제공하여야 한다. 이를 위해 이 시스템은 일회성 비밀키와 일방향 축적기[10]라는 암호연산을 활용하여 부인방지 문제를 해결한다.

이 논문의 구성은 다음과 같다. 2장에서 기존의 전자수표시스템의 특성과 문제점을 분석하고, 3장에서는 이 논문에서 제안하는 전자수표시스템을 서술한다. 4장에서는 제안한 전자수표시스템과 기존 전자수표시스템과 비교하여 장단점을 논의한다. 끝으로 5장에서 결론과 향후 연구 방향에 대해 서술한다.

Ⅱ. 기존 전자수표시스템

전자수표시스템은 David Chaum에 의해 1989년에 처음 소개되었다.[3] 이 시스템은 온라인 방식이

1. 고객 → 판매자 → 은행 : n, $h(n)^{37}$, $h(j)s^{511}$
2. 은행 → 판매자 → 고객 : $h(j)^{511}s$

〔그림 1〕 Chaum의 온라인 수표방식에서 지불과정

며 RSA 은닉서명을 이용한다. 고객은 일반 해쉬함수 h를 이용하여 $h(n)$을 만들고, 여기에 은행으로부터 은닉서명을 받아 수표를 인출한다. 여기서 n은 고객이 선택한 난수로 수표의 일련번호가 되며, 고객은 시스템에서 정해놓은 고정된 액면가를 가진 수표를 인출 받게된다. 이 시스템에서는 수표의 액면가를 나타내는 4비트 이진 표현의 각 비트를 RSA 공개지수(public exponent) 3, 5, 7, 11에 대응하는 비밀지수(private exponent)와 연관시켜 표현한다. 즉, 공개지수 3, 5, 7, 11에 대응되는 비밀지수가 수표에 모두 적용되어 있으면 이 수표의 액면가의 이진 표현은 1111이 된다. 따라서 수표의 액면가를 나타내는 이진 표현 0001이 100원이면 $h(n)^{37}$은 0101에 해당하므로 500원이며, $h(n)^{3571}$은 이진표현 1111에 해당하므로 1500원을 나타낸다.

수표의 지불은 지불대금에 따라 해당 공개지수로 수표를 거듭제곱하여 만든 값과 수표의 일련번호를 〔그림 1〕과 같이 판매자에게 전달하여 이루어진다. 또한 거스름을 축적하기 위해 은닉된 쿠키통 $h(j)s^{511}$을 함께 전달한다. 〔그림 1〕은 500원을 지불하고 거스름으로 1000원을 쿠키통에 축적하는 과정이다. 쿠키통은 다음 지불에도 계속해서 사용할 수 있으며, 나중에 은행에 입금하여 해당 금액을 돌려 받을 수 있다. 지불은 온라인 형태로 이루어지며 판매자는 고객으로부터 받은 메시지를 단순히 은행에 전달하고, 은행으로부터 확인메시지와 메시지 2를 받아 고객에게 전달한다. 여기서 j는 쿠키통의 일련번호이며, s는 은닉요소이다. 이 밖에 Chaum은 동일 논문에서 쿠키통을 지불에 다시 사용할 수 있는 방식도 제시하고 있다. 그러나 거스름의 액면가 한도 내에서 자유롭게 사용할 수 없고 일부 금액의 경우에만 지불할 수 있다. 예를 들어 축적한 거스름의 액면가가 600원이면 600원, 400원, 200원을 지불하기 위해서만 사용할 수 있고, 500원, 300원, 100원을 지불하기 위해서는 사용할 수는 없다.

Chaum은 또한 오프라인 방식의 전자수표시스템도 발표하였다.[8] 이 시스템에서 고객은 기존 온라인 시스템과 마찬가지로 시스템에서 정해놓은 고정

된 금액의 수표를 인출한다. 인출과정에서 고객은 다음과 같은 방법으로 40개의 α_i값을 만들어 은행에 전달한다. 여기서 a_i, b_i, c_i, d_i는 임의로 선택한 난수이고 U는 고객 식별자이며 r_i는 은닉요소이다. 그리고 g, f, h는 모두 일방향 해쉬함수지만 특성이 조금씩 다르다.

$$
\begin{aligned}
x_i &= g(a_i \| b_i, c_i) \\
y_i &= g(a_i \oplus U, d_i) \\
M_i &= f(x_i \| y_i) \\
m_i &= h(g(b_i \| e_i)) \\
\alpha_i &= M_i^{3^{10}} \cdot m_i^{17} \cdot r_i^{17\,3^{10}}
\end{aligned}
$$

은행은 cut-and-choose 기법을 통해 값의 구성을 확인하고, 40개의 α_i값 중에 개봉하지 않은 20개의 값에 서명을 하여 고객에게 전달한다. 고객은 은행으로부터 받은 값을 2개 부분으로 나누어 지불에 사용하게 된다. 나누어진 두 부분 중 하나는 지불대금을 나타내기 위해 사용되며, 다른 한 부분은 거스름을 받기 위해 사용된다. 지불과정에서 판매자는 challenge-and-response 기법을 이용하여 수표를 확인한다. 이 과정에서 판매자가 전달하는 이진 도전 벡터의 일부가 지불대금을 나타낸다. 이처럼 이 시스템은 오프라인 방식이라는 장점이 있지만 인출과정에서 cut-and-choose 기법을 사용하고, 수표의 구성이 복잡하므로 효율성이 떨어진다.

1997년에 Robert Deng 등은 기존 Chaum의 온라인 전자수표시스템을 확장한 시스템을 발표하였다.[7] Chaum의 시스템은 일련번호로 임의의 난수를 사용하는 반면에 이 시스템은 일회성 공개키를 생성하여 그것을 일련번호로 사용한다. 이것의 장점은 일련번호에 대응되는 개인키를 알고 있는 고객만이 수표를 이용하여 지불할 수 있다는 것과 같은 판매자와 여러 차례 거래를 할 경우 오프라인으로 지불이 가능하다는 것이다. 그러나 공개키 쌍을 생성하는데 소요되는 비용은 암호학적으로 안전한 난수를 생성하는 비용보다 비싸므로 이런 측면에서는 효율성이 떨어진다고 볼 수 있다. 물론 논문에서는 사전에 공개키 쌍들을 생성해 놓으면 이런 문제점을 극복할 수 있다고 하였으나 완전한 해결책이라고 볼 수는 없다.

이 시스템은 Chaum의 시스템과 달리 고정된 하나의 공개지수를 이용하여 수표의 액면가를 표현한다.

1.	고객	→ 판매자 →	은행	: $e_1, h(e_1)^{d_b}$
2.	은행	→ 판매자 →	고객	: ok
3.	고객	→ 판매자		: $\{400원, e_1, I_1\}^{d_1}$
4.	판매자	→ 고객		: item 1
5.	고객	→ 판매자		: $\{1000원, e_1, I_2\}^{d_1}$
6.	판매자	→ 고객		: item 2
7.	고객	→ 판매자 →	은행	: $h(e_1)s_1^{3^{13}}$
8.	은행	→ 판매자 →	고객	: $h(e_1)^{\frac{1}{3^{13}}}s_1$

[그림 2] Robert Deng 등의 수표시스템의 지불과정

이것이 가능한 이유는 수표의 액면가를 지불과정에서 전자동전처럼 바꾸지 않기 때문이다. 따라서 Chaum의 시스템보다는 적은 연산을 이용하여 수표금액이나 지불대금을 확인할 수 있다. 그러나 거스름과 수표 자체가 전혀 다른 형태가 되므로 거스름을 재사용하기 힘들다는 단점을 가지고 있다. 거스름 메커니즘은[3]에서 사용한 쿠키통 방식을 그대로 사용하고 있다. 다만 쿠키통에 경우도 난수 대신에 일회성 공개키를 일련번호로 사용하고 있다. 따라서 보다 안전하게 입금할 수 있다. [그림 2]는 Deng 등의 시스템에서 다중 지불세션으로 지불하는 과정을 기술한 것이다. 여기서 d_b는 은행이 수표를 발행할 때 사용하는 은행의 개인키이다. e_1은 고객이 생성하여 수표의 일련번호로 사용하고 있는 일회성 공개키이고, d_1은 e_1에 대응되는 개인키이다. 각 세션마다 고객은 주문서를 수표에 포함된 일회성 공개키의 대응되는 개인키로 서명한다. 여기서 I_i는 판매자 식별자, 거래시간 등의 필요한 추가 정보이다.

Ⅲ. 거스름의 재사용이 가능한 수표시스템

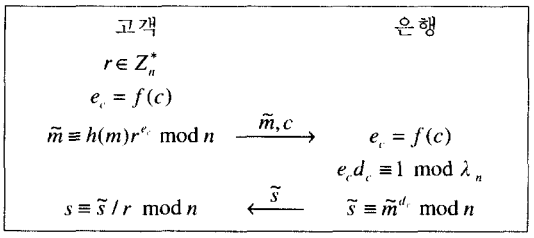
이 장에서는 기존의 전자수표시스템이 가지고 있는 거스름에 대한 문제점을 해결한 온라인 전자수표시스템을 제안한다. 새롭게 제안한 전자수표시스템은 부분은닉서명[9]을 사용하여 고객의 익명성을 보장하고 전자수표의 액면가를 표현한다. 부분은닉서명을 활용하면 대금지불 과정에서 발생하는 차액에 대해 익명으로 새로운 수표를 발행할 수 있다. 제안하는 시스템은 이렇게 발행한 수표를 거스름으로 사용한다. 이렇게 함으로써 거스름의 형태는 곧 수표와 같게 되어 액면가 한도 내에서는 어떤 제약 없이

다시 사용할 수 있다. 결과적으로 거스름의 재사용 문제를 가장 바람직한 방향으로 해결하였다. 그밖에 수표의 일련번호로 난수를 사용하지 않고 일회성 비밀키를 사용하여 지불의 효율성을 높였다. 뿐만 아니라 온라인 시스템의 문제점을 극복하기 위해 같은 상점과 거래를 계속할 경우에는 오프라인으로 처리가 가능하도록 다중 지불세션 기능을 제공한다. 여기서 일반 전자서명 대신 일방향 축적기[10]라는 암호연산을 사용한다. 시스템 설명에 앞서 먼저 부분은닉서명과 일방향 축적기에 대해 간략히 소개한다.

3.1 부분은닉서명

부분은닉서명은 Masayuki Abe가 개발한 서명기법으로 은닉되는 m과 공개되는 c에 서명자의 서명을 받게되지만 서명자는 서명 $Sig(m,c)$와 m을 연관시키는 것이 계산적으로 용이하지 않다.[9] 일반 은닉서명에서 서명자는 서명 내용을 전혀 알 수 없지만 부분은닉서명에서 서명자는 c정보가 서명에 포함된다는 것을 확신할 수 있다. 즉, 서명자와 사용자가 동의한 어떤 정보를 은닉서명에 포함시킬 수 있다. 이 기법을 응용하여 전자화폐를 구성할 때 m은 일련번호로 사용하고, 공개되는 c정보를 화폐의 금액이나 유효기간을 나타내는 정보로 활용할 수 있다. 이 논문에서는 부분은닉서명을 수표의 액면가 표현 방법으로 활용한다.

RSA를 기반으로 하는 부분은닉서명은 [그림 3]에 기술되어 있다. r은 은닉요소이고, 함수 f는 공개지수 생성함수이다. e_c는 공개되는 c정보를 이용하여 생성한 공개지수이며, d_c는 대응되는 비밀지수이다. 일반적으로 RSA는 Euler ϕ함수를 사용하지만 최근에는 $\phi(n)$과 동일한 역할을 하는 n의 보편지수(universal exponent) λ_n을 사용한다. λ_n은 $n=pq$일 때 $\mathrm{lcm}(p-1, q-1)$로 정의되며, ϕ대신 λ를 사용하면 비밀지수 값이 작아지므로 복호화 성능이 좋아



[그림 3] RSA 기반 부분은닉서명

진다. RSA 기반 부분은닉서명에서 서명자의 공개키는 (n, f)이며, n의 인수분해는 오직 서명자만 알고 있다. 서명의 확인은 다음을 이용한다.

$$s^{f(c)} ? \equiv h(m) \bmod n$$

RSA 기반 부분은닉서명이 안전하기 위해서는 함수 f가 다음을 만족하여야 한다.

- 서로 다른 c값에 대해 다른 출력을 주어야 한다.
- 출력은 λ_n과 서로소이어야 한다.
- 출력은 최소한 하나의 독특한 소수 인수를 가지고 있어야 한다.

Abe는 f함수로 가장 적합한 것은 서로 다른 입력 c 값에 대해 다른 출력을 주는 소수 생성함수라고 하였다. 그러나 소수 생성함수는 성능 측면에서 전자지불에 활용하기 어렵다. 따라서 Abe는 소수 생성함수 대신에 일반 해쉬함수 h를 활용하여 f함수를 다음과 같이 정의하였다.

$$f(c) = 2h(c)+1$$

이 함수의 안전성은[10]에 증명되어 있다.

3.2 일방향 축적기

함수 $f: X \times X \rightarrow X$가 모든 $x_0, x_1, x_2 \in X$에 대해 다음을 만족하면 함수는 준교환성(quasi-commutative)을 가지고 있다고 한다.

$$f(f(x_0, x_1), x_2) = f(f(x_0, x_2), x_1)$$

일방향 축적기란 준교환성을 만족하는 일방향 함수를 말한다. 일방향 축적기는 전자서명 대신에 사용할 수 있는 암호기법으로서 기존 전자서명과 달리 중앙 인증서버가 필요 없는 기법이다. 일방향 축적기는 Josh Benaloh와 Michael Mare가 처음 소개하였다.[10] 이들은 일방향 축적기로 다음을 제안하였다.

$$e_n(x, y) = x^y \bmod n$$

이 함수는 RSA 가정에 의해 일방향성이 보장되며,

준교환성이 쉽게 만족함을 알 수 있다. 이들은 일방향 축적기의 응용으로 타임스템핑 프로토콜과 멤버쉽 검사를 제안하였다. 타임스템핑 프로토콜이란 문서에 시간을 부여하여 문서의 생성 순서를 보장하는 프로토콜이며, 멤버쉽 검사란 자신이 어떤 그룹에 속해있음을 제3자나 다른 멤버에게 증명할 때 사용하는 프로토콜을 말한다. 하지만 e_n함수의 사용은 계산비용 측면에서 RSA 전자서명과 같다. Kaisa Nyberg는 Benaloh 등의 방법보다 효율적인 축적기를 제안하였다.[11] 이 시스템은 일반 해쉬함수와 암호학적으로 안전한 의사난수 비트 생성기만을 사용함으로 성능을 많이 개선하였다. 이 논문에서는 Nyberg가 제안한 축적기를 사용한다고 가정한다. 만약 기존에 발표되어 있는 일방향 축적기보다 더 효율적인 기법이 개발되면 이 논문에서 제안하는 지불 프로토콜의 효율은 더 개선될 것이다.

3.3 시스템 설정

은행은 부분은닉서명을 위한 매우 큰 RSA modulus $n=pq$와 공개지수 생성함수 f를 선택한다. 그리고 일반 전자서명을 위한 매우 큰 RSA modulus $n_b=p_bq_b$를 선택하고 RSA 공개키 쌍 (e_b, d_b)를 생성한다. 은행은 부분은닉서명 공개키 (n, f)와 일반 전자서명 공개키 (e_b, n_b)를 공개한다. 또한 은행에는 판매자와 고객의 계좌가 개설되어 있고, 판매자 계좌는 S로 고객 계좌는 U로 식별된다. 각 판매자도 일반 전자서명을 위한 매우 큰 RSA modulus $n_s=p_sq_s$를 선택하여 RSA 공개키 쌍 (e_s, d_s)를 생성하고, 공개키 (e_s, n_s)를 공개한다.

3.4 인출 프로토콜

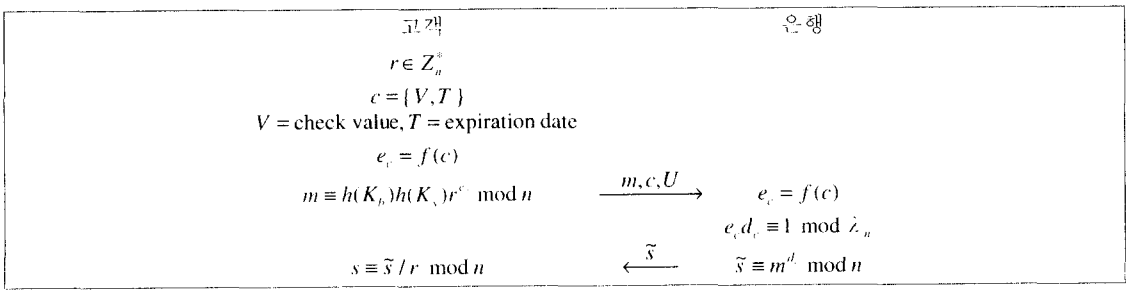
고객은 은행으로부터 [그림 4]에 있는 프로토콜을 이용하여 수표를 인출한다. 고객은 은닉요소 r과 두 개의 일회성 비밀키 K_b와 K_s를 생성하여 부분은닉서명 과정을 수행한다. 각 키의 역할은 다음과 같다.

- K_b : 수표의 일련번호 역할을 하고 고객과 은행간에 정보를 암호화하여 교환하기 위한 일회성 비밀키
- K_s : 고객과 판매자간에 정보를 암호화하여 교환하기 위한 일회성 비밀키

부분은닉서명에서 공개되는 $c=\{V, T\}$정보는 인출하고자 하는 수표의 액면가와 유효기간을 나타낸다. 앞으로 $c.V$는 c에 포함된 액면가를 나타내며, $c.T$는 수표의 만기날짜를 나타낸다. 유효기간을 통해 수표를 식별할 수 없도록 만기날짜만을 명시하며, 만기날짜는 매 달 특정 일로 고정시켜 여러 값을 가질 수 없도록 한다. 인출 프로토콜을 통해 고객이 최종적으로 얻게 되는 수표의 형태는 다음과 같다.

$$s \equiv (h(K_b)h(K_s))^d \mod n$$

이 시스템은 두 개의 일회성 비밀키를 수표에 사용한다. 이것은 기존 Deng 등의 시스템보다 지불과정의 효율성을 높이기 위함이다. Deng 등의 시스템은 일회성 공개키를 사용하였는데 일회성 공개키 대신에 일회성 비밀키를 사용하게 되면 계산에 드는 비용을 줄일 수 있다. 반면에 비밀키를 사용하게 되면 공개키를 사용하는 전자서명과는 달리 값의 확인이나 부인방지 기능을 쉽게 제공할 수 없다. 본 시스템은 일회성 비밀키를 사용하여도 안전한 지불이 가능하다. 본 시스템에서 두 개의 일회성 비밀키를 사용하는 이유는 다음과 같다. K_b는 수표의 일련번호 역할을 하며, 고객과 은행간에 정보를 암호화하여 교환하기 위해 반드시 필요한 키이다. 그러나 K_s는 고객과 판매자간에 정보를 암호화하여 교환하기



[그림 4] 인출 프로토콜

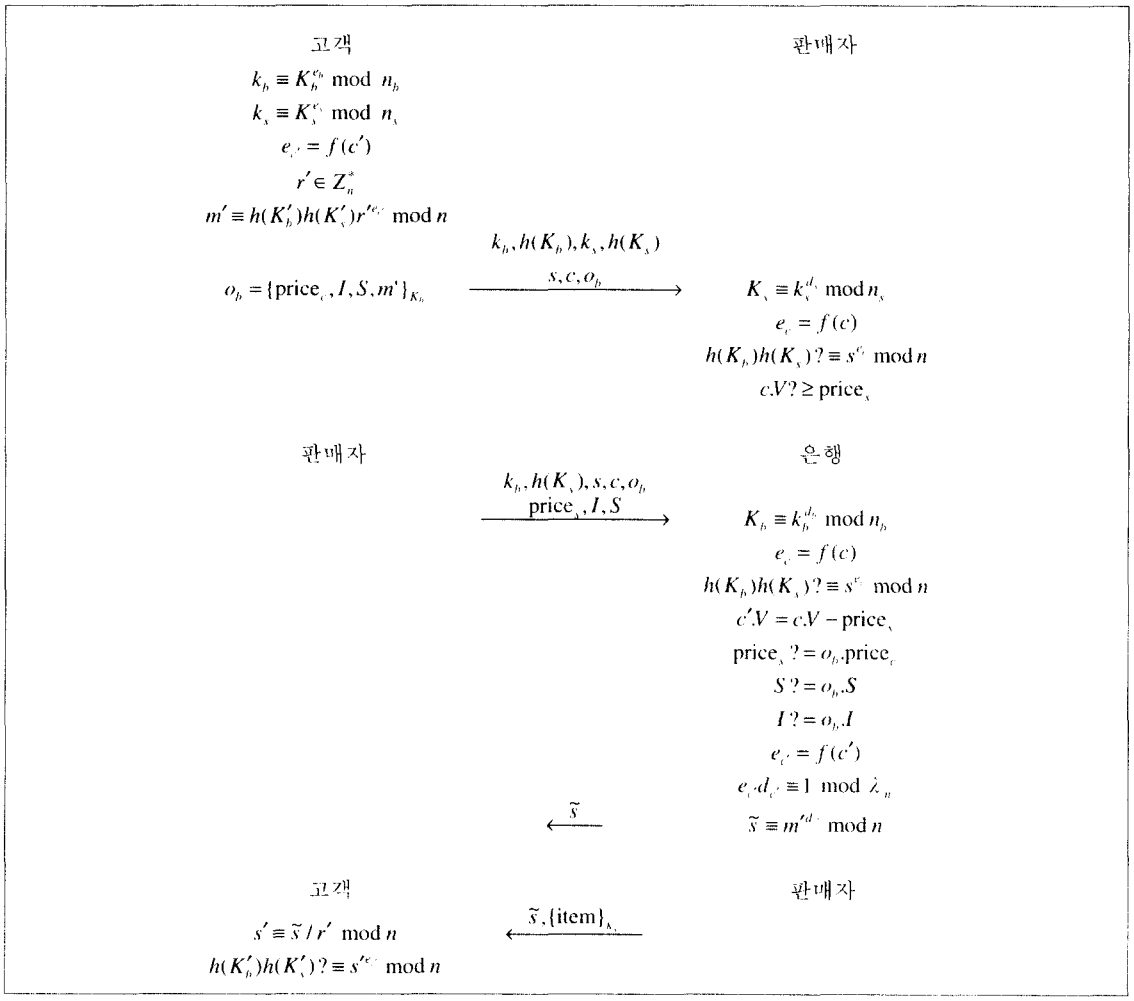
위해 사용되므로 수표에 포함시키지 않고 별도로 교환할 수 있다고 생각할 수 있다. 만약 별도로 교환할 경우 판매자는 수표를 이용하여 지불하는 고객이 정당한 사용자인지를 인증할 수 없다. 물론 온라인 방식이므로 판매자가 수표를 확인할 필요는 없지만 판매자가 원할 경우에는 K_s를 이용하여 고객을 인증할 수 있다. 또한 K_s는 거래과정에서 디지털 상품을 암호화해서 보내기 위해 사용할 수 있다. 만약 수표와는 별도로 정보를 암호화하여 교환하기 위해 세션키가 필요하다면 단순히 세션키를 판매자의 공개키로 암호화하여 교환할 수는 없고 복잡한 키 교환 프로토콜이 필요하다. 따라서 판매자와 고객간에 사용할 수 있는 비밀키를 수표에 포함하면 여러 측면에서 유용하다.

3.5 지불프로토콜

본 시스템에는 두 가지 지불 형태가 있다. 하나는 한 가지 상품이나 서비스를 구입하는 경우에 사용하는 프로토콜이고, 다른 하나는 한 상점에서 여러 개의 상품이나 서비스를 구입하는 경우에 사용하는 프로토콜이다. 전자의 프로토콜을 단일 지불세션 프로토콜이라 하고 후자를 다중 지불세션 프로토콜이라 한다.

3.5.1 단일 지불세션 프로토콜

단일 지불세션 프로토콜은 [그림 5]에 기술되어 있다. 고객은 수표 s를 판매자를 통해 은행에 전달하며, 거스름 s'을 받기 위해 판매자를 통해 인출과정과 동일한 과정을 수행한다. 고객은 지불에 사용



[그림 5] 단일 지불세션 프로토콜

할 수표에 포함되어 있는 두 개의 비밀키 K_b와 K_s를 각각 은행과 판매자의 공개키로 암호화한다. 암호화한 키를 각각 k_b, k_s라 한다. 그리고 거스름으로 받을 수표를 위해 은닉요소 r'과 두 개의 비밀키 K''_b와 K''_s를 생성하여 m'을 만든다. m'은 은행에 전달되어 거스름으로 되돌려 받을 수표로 전환된다. 만든 m'과 지불대금 $price_c$, 상품/서비스 식별자 I, 그리고 판매자의 식별자 S를 K_b로 암호화하여 거스름 요청서 o_b를 만든다. 고객은 k_b, $h(K_b)$, k_s, $h(K_s)$, s, c, o_b를 판매자에게 전달하여 지불을 시작한다. 은행은 o_b에 포함된 지불대금과 상품정보를 알게되지만 수표 자체가 익명성을 보장하기 때문에 고객의 프라이버시는 침해되지 않는다. o_b는 K_b로 암호화하여 만들어지므로 오직 은행만 확인할 수 있다. 거스름을 받기 위한 값 m'을 o_b에 포함하여 비밀을 보장하는 것은 제 3자나 판매자가 비합법적으로 거스름을 얻을 수 없도록 하기 위함이다. 앞으로 o_b를 복호화하여 얻은 값 x를 나타내기 위해 $o_b.x$로 표기한다.

판매자는 k_s를 복호화하여 K_s를 얻고 K_s와 $h(K_b)$를 이용하여 수표 s를 확인한다. 만약 K_s를 활용하지 않으면 이 과정은 생략될 수 있다. 판매자는 고객으로부터 받은 값 중에 k_b, $h(K_s)$, s, c, o_b와 정산금액 $price_s$, 상품 식별자, 판매자 식별자를 은행에 전달한다. 은행은 k_b를 복호화하여 K_b를 얻어 수표 s를 확인하고, 판매자가 전달한 정보를 이용하여 o_b의 구성을 확인한다. 수표와 거스름 요청서의 값이 올바르면 거스름 금액을 계산하고 거스름 요청서에 포함된 m'에 서명하여 판매자에게 돌려준다. 판매자는 서명된 m'과 상품/서비스를 K_s로 암호화하여 고객에게 전달한다. 상품 또는 서비스의 암호화는 환경에 따라 다르게 적용할 수 있는 부분이다. 고객은 은닉요소를 제거하고 거스름 s'을 확인한다.

3.5.2 다중 지불세션 프로토콜

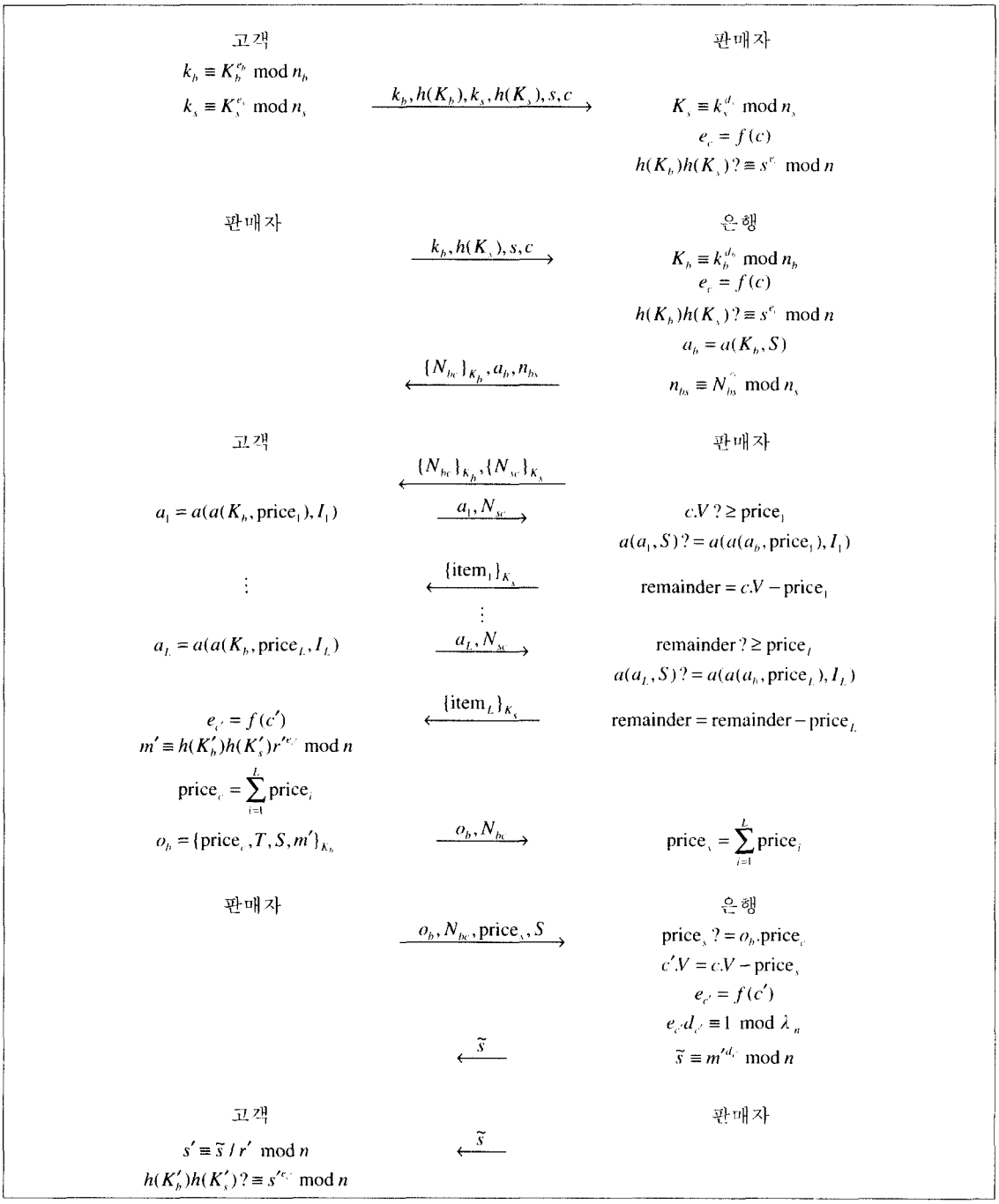
다중 지불세션 프로토콜은 [그림 6]에 기술되어 있다. 이 프로토콜은 다음과 같은 3개의 난스(nonce)를 사용하고 있다.

- N_{bc} : 은행이 생성한 난스로 고객에게 비밀로 전달된다. 고객은 거스름을 요청할 때 이 난스를 사용한다. 은행은 데이터베이스에서 현재 정산이 진행중인 수표를 검색할 때 키로 사용한다.
- N_{bs} : 은행이 생성한 난스로 판매자에게 비밀로 전달된다. 판매자는 고객의 도움없이 독자적으로 지불을 정산할 때 이 난스를 사용한다.
- N_{sc}: 판매자가 생성한 난스로 고객에게 비밀로 전달된다. 다중 지불세션에서 고객은 매 지불마다 이 난스를 판매자에게 제시한다. 판매자는 이 난스를 통해 다중 지불세션을 식별한다.

다중 지불세션 프로토콜에서 각 지불은 오프라인으로 이루어진다. 따라서 판매자는 스스로 지불을 확인할 수 있어야 하며, 나중에 분쟁이 발생하였을 때 분쟁을 해결하기 위해 각 지불마다 고객이 지불을 하였다는 것을 증명할 수 있어야 한다. 그러나 수표에 포함된 비밀키를 이용한 단순 암호화를 통해서는 이와 같은 기능을 제공할 수 없다. 따라서 본 시스템은 일방향 축적기를 사용하여 이 기능을 제공한다. 다중 지불세션 프로토콜의 상세 과정은 다음과 같다.

고객은 단일 지불세션과 달리 먼저 수표 s만 판매자에게 전달한다. 판매자는 고객으로부터 받은 수표 s를 은행에 전달하여 유효성을 확인한다. K_s를 활용할 경우에는 판매자도 스스로 수표를 반드시 확인하여야 한다. 은행은 수신한 수표의 서명만을 확인하고 이상이 없으면 난스 N_{bc}, N_{bs}를 생성하여 N_{bc}는 K_b로 암호화하고, N_{bs}는 판매자의 공개키로 암호화한다. 난스의 무결성을 보장하기 위해 c와 같은 명백한 여분정보(redundancy)를 암호문에 포함할 수도 있다. N_{bc}는 은행이 사용된 수표와 나중에 받게 되는 거스름 요청을 연관시키기 위한 수단이다. N_{bs}는 N_{bc}와 동일한 역할을 하는 것으로서 나중에 판매자가 고객의 도움 없이 지불을 정산할 때 사용한다. N_{bs}을 이용한 지불 정산은 다음 절에 설명한다. 은행은 일방향 축적기 a를 이용하여 $a_b = a(K_b, S)$를 계산하고, 암호화된 두 개 난스와 함께 판매자에게 전달한다. 판매자도 난스 N_{sc}를 생성하여 K_s로 암호화하여 은행으로부터 받은 암호화된 난스 $\{N_{bc}\}_{K_b}$와 함께 고객에게 전달한다. 판매자는 고객의 각 대금 지불마다 N_{sc}를 이용하여 사용 중인 수표 s를 식별한다.

고객은 수표 s의 유효기간 동안 s의 액면가를 초과하지 않는 범위 내에서 계속 오프라인으로 지불할 수 있다. 고객은 각 지불마다 일방향 축적기를 이용하여 계산한 $a_i = a(a(K_b, price_i), I_i)$를 판매자에게 전달한다. 판매자는 고객으로부터 a_i값을 받아 다음 식을 이용하여 확인한다. 이 때 은행이 수표를 확인한 다음에 만들어서 보낸 a_b값을 이용한다.

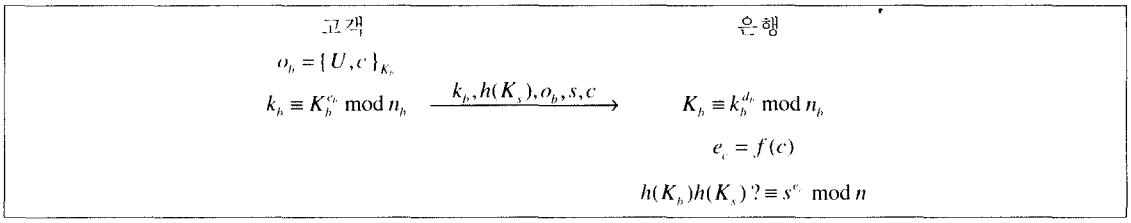


〔그림 6〕 다중 지불세션 프로토콜

$$a(a_i, S) \; ? = a(a(a_b, \text{price}_i), I_i)$$

이 논문에서는 은행은 부정을 하지 않는다고 가정한다. 따라서 a_i값은 K_b를 알고 있는 고객만 만들 수 있다. 그러므로 서명을 한 것과 동일한 효과가 있다.

고객은 더 이상 구입할 상품이 없으면 거스름 요청서 o_b와 N_{bc}를 판매자에게 전달하여 세션을 종료할 수 있다. 거스름 요청서 o_b에는 지금까지 이루어



〔그림 7〕 입금 프로토콜

진 모든 지불대금의 총액 $price_C$, 판매자 식별자, 현재 시간 T, 거스름 수표를 위한 m'이 포함된다. 이와 같은 거스름 요청서를 사용하면 은행은 지불에 사용한 모든 a_i값들을 확인하지 않고 정산을 할 수 있다. 따라서 은행은 분쟁이 발생할 경우에만 a_i값을 확인한다. 판매자는 고객으로부터 받은 거스름 요청서, N_{bc}, 정산금액 $price_S$, 그리고 자신의 식별자를 은행에게 전달한다. 은행은 o_b를 복호화하여 내용을 확인하고 거스름 금액을 계산하여 m'에 서명한다. 서명된 이 정보는 판매자에게 전달되며, 판매자는 이 정보를 고객에게 중계하여 준다. 고객은 단일 지불세션과 마찬가지로 은닉요소를 제거하고 거스름을 확인한다.

3.5.3 정산 프로토콜

다중 지불세션 프로토콜에서 고객이 여러 물건을 구입한 후에 지불 정산을 포기하거나 장기간 동안 정산을 하지 않으면 판매자는 손해를 볼 수가 있다. 판매자는 고객이 장시간 지불 정산을 하지 않을 경우에 고객의 도움 없이 아래와 같은 정보를 은행에 전달하여 정산과정을 수행할 수 있다.

$$N_{bs}, (a_1, I_1, \text{price}_1), \ldots, (a_K, I_K, \text{price}_K)$$

즉, 정산과정을 수행하기 위해 판매자는 은행으로부터 받은 N_{bs}와 고객이 전달한 모든 a_i와 각 a_i를 확인하기 위해 필요한 정보를 은행에게 전달한다. 은행은 a_i를 확인하고 정산이 되었다는 사실을 데이터베이스에 기록한다. 정산과정이 수행된 후에 고객으로부터 거스름 요청을 받으면 판매자는 지불 정산이 되었다는 사실을 고객에게 알려준다. 이와 같은 경우에 고객은 다중 지불세션 프로토콜에서 사용한 방법을 이용하여 은행에 직접 거스름을 요구할 수 있다.

3.6 입금 프로토콜

보통 전자지불시스템에서 입금 프로토콜은 판매자와 은행간에 이루어지는 과정이지만 이 시스템의 입금 프로토콜은 고객이 거스름으로 받은 수표를 은행에 입금할 때 사용하는 프로토콜을 말한다. 이 프로토콜은 〔그림 7〕에 기술되어 있다. 이 프로토콜을 이용하여 거스름으로 받은 수표 또는 처음에 발행된 수표를 은행에게 전달하여 해당금액을 자신의 계좌로 돌려 받을 수 있다. 여기서 o_b는 입금서가 된다. 이 입금서는 K_b로 암호화되어 있으므로 오직 이것을 알고 있는 정당한 고객만 입금요청을 할 수 있다.

Ⅳ. 시스템 성능 분석

4.1 안전성

RSA 서명이 안전하다고 가정하면 RSA를 기반으로 하는 부분은닉서명도 안전하다. Abe가 제시한 것처럼 적절한 공개지수 생성함수를 선택하면 인출된 수표나 거스름으로 받은 수표의 위조는 불가능하다. 뿐만 아니라 수표에 있는 공개된 값 c를 바꾸어 인출한 수표의 액면가를 바꿀 수 없다. 수표를 구성하는 두 개의 비밀키는 공개키로 암호화하거나 해쉬된 형태로 전달하므로 제 3자가 통신상에 전달되는 정보를 가로채어 수표를 위조하거나 수표에 포함된 비밀키를 알 수 없다. 판매자도 비밀키 가운데 판매자용 비밀키 밖에 모르기 때문에 고객으로부터 받은 수표를 가로채서 사용할 수 없다. 은행은 지불에 사용된 각 수표에 대해 필요한 정보를 보관하므로 수표의 이중사용을 발견할 수 있다.

부분은닉서명은 완전익명성를 제공한다. 고객은 자신의 신분노출이나 추적을 걱정하지 않고 지불할 수 있으며, 수표를 사용하고 거스름으로 받은 새로운 수표로부터 사용된 수표를 알 수 없으므로 연결불가능성(untraceability)을 제공한다. 전자수표시스템에서는 판매자나 제 3자가 고객을 대신하여 거스름을 받아 지불에 사용할 수 없어야 한다. 본 시스템에서는 거스름을 지급하는 과정이 지불프로토콜

과 상관없이 항상 온라인으로 이루어지므로 부정행위가 있을 경우에는 쉽게 발견된다. 더욱이 거스름을 만들기 위한 정보 m'은 정당한 고객과 은행만 알고 있는 비밀키로 암호화되어 전달되므로 제 3자가 자신에게 유리한 값으로 바꿀 수 없다. 판매자는 비밀키 K_b를 모르기 때문에 거스름 요청서 o_b를 만들 수 없으며, N_{bc}값을 모르기 때문에 고객의 도움 없이 은행에 거스름을 요청할 수 없다.

4.2 효율성

전자수표시스템이므로 기존 동전방식의 시스템보다는 효율적으로 지불할 수 있다. 다만 온라인 방식이므로 지불과정에 항상 은행이 참여하여야 한다는 문제점이 있다. 그러나 고액환경에서는 오프라인 방식을 사용할 수 없을 뿐만 아니라 본 시스템에서는 다중 지불세션 기능을 지원하므로 온라인 방식의 문제점을 부분적으로 극복할 수 있다. 또한 기존 전자수표시스템에 비해 다음과 같은 측면에서 효율적이다.

- 인출할 수 있는 수표의 액면가에 대한 제한이 없다.
- 거스름을 아무런 제한 없이 지불에 다시 사용할 수 있다.
- 일회성 비밀키를 사용하여 지불과 입금 과정의 계산효율을 높였다.
- 수표에 포함된 비밀키를 이용하여 디지털 상품을 효율적이고 안전하게 교환할 수 있다.
- 전자서명 대신에 일방향 축적기를 사용한다.
- 은행이 지불을 승인하기 위해 확인하여야 하는 정보가 상대적으로 적다.

4.3 원자성

지불시스템에서 원자성(atomicity)이란 판매자는 상품을 전달하였는데 지불을 받지 못하는 경우가 없어야 하고, 고객은 지불하고도 상품을 받지 못하는 경우가 없어야 한다는 것을 말한다. 이 시스템에서 단일 지불세션의 경우에는 온라인으로 이루어지므로 중간에 문제가 발생하면 은행이 지불 전체를 취소함으로써 분쟁의 소지가 없다. 그러나 다중 지불세션의 경우에는 오프라인 지불이므로 원자성 문제가 발생할 수 있다.

원자성의 보장 여부는 고객이 다중 지불세션 도중에 지불한 사실이 없음을 부인하는 경우와 판매자가 고객으로부터 받은 지불을 부인할 경우로 나누어 생각할 수 있다. 전자의 경우는 실제로 고객이 지불한 사실이 없는 경우와 고객이 지불한 사실이 있지만 부인하는 경우로 다시 나눌 수 있다. 고객이 지불한 사실이 없는 경우에 판매자는 올바른 a_i를 만들 수 없으므로 문제가 되지 않는다. 또한 지불한 사실이 있지만 부인하는 경우 판매자는 고객으로부터 받은 확인된 a_i값을 가지고 있으므로 분쟁을 해결할 수 있다. 후자의 경우도 실제로 판매자가 지불을 받은 사실이 없는 경우와 고객으로부터 지불을 받았지만 판매자가 부인하는 경우로 나눌 수 있다. 실제로 판매자가 지불을 받은 사실이 없는 경우에는 상품이나 올바른 a_i가 교환되지 않았을 뿐만 아니라 판매자가 정산을 하지 못하므로 어느 누구도 손해를 보거나 이득을 얻을 수 없다. 반대로 고객으로부터 지불을 받았지만 판매자가 부인하는 경우에 문제가 되는 상황은 판매자가 a_i값을 받았지만 상품을 전달하지 않은 경우이다. 이 경우에는 고객은 상품의 재전송을 요구하여 분쟁을 해결할 수 있다. 이와 같은 경우 외에 거스름 요청서와 판매자가 청구한 금액이 다른 경우가 있을 수 있다. 그러나 판매자가 a_i들을 모두 은행에 전달함으로써 누가 부정을 했는지 확인할 수 있다. 따라서 본 시스템에서는 수표를 발행하는 은행이 부정을 하지 않는다면 원자성을 보장한다.

4.4 다른 전자수표시스템과의 비교

Deng 등의 전자수표시스템과 본 시스템은 둘 다 온라인 방식이다. 그러나 Deng 등의 전자수표시스템은 수표의 액면가를 표현하는 방법과 거스름으로 받은 쿠키통의 액면가를 표현하는 방법이 다르며 항상 시스템에서 정해놓은 고정된 금액의 수표밖에 인출할 수 없다. 쿠키통 방식은 하나의 쿠키통에 여러 개의 지불에서 받은 거스름을 축적할 수 있다는 장점을 가지고 있다. 그러나 지불에 사용할 수 없으며 반드시 은행에 입금해야하는 문제점을 지니고 있다. Deng 등의 전자수표시스템은 온라인 방식의 단점을 극복하고자 오프라인으로 다중 지불세션 기능을 지원하며, 오프라인에서 각 지불을 연결시키기 위해 일회성 공개키를 사용하였다.

본 시스템은 수표의 액면가 표현방법과 거스름으로 받는 수표의 액면가 표현방법이 동일하며, 거스름으로 받는 수표도 인출한 수표와 동일하게 지불에 사용할 수 있다. 고객은 액수에 제한 없이 원하는 금액을 수표로 인출하여 사용할 수 있다. 또한 Deng 등의 시스템과 마찬가지로 온라인 방식의 단점을 극

〔표 1〕 시스템 비교

			Chaum의 온라인 전자수표시스템	Deng등의 온라인 전자수표시스템	이 논문에서 제안하고 있는 시스템
인출	공개지수		3·5·7·11	3	e_c
	고정금액		○	○	×
	일련번호		난수	공개키	비밀키 2개
지불	주문서/거스름 요청서	단일 지불세션	주문서 개념이 프로토콜에서 생략되어 있음	개인키로 서명	비밀키로 암호화
		다중 지불세션		- 각 지불마다 서명 - 모든 주문서를 은행에 전달	- 각 지불마다 일방향 축적값 - 단일 요청서를 은행에 전달
	다중 지불세션 지원		×	○	○
	거스름의 재사용		△	×	○
	거스름 생성비용		은닉서명, 쿠키통 방식	은닉서명, 쿠키통 방식	부분은닉서명
	기타 소요 연산				공개키로 비밀키를 암호화
입금	특징		쿠키통 암호화하여 전달	개인키로 입금서 서명	비밀키로 입금서 암호화

복하고자 같은 상점과 여러 번의 거래를 할 경우에는 오프라인으로 거래가 가능하도록 하였다. 그러나 본 시스템은 Deng 등의 시스템과는 달리 일회성 비밀키를 사용하여 거스름 요청서를 만들며, 다중 지불세션에서는 일방향 축적기를 사용한다. 일회성 비밀키는 디지털 상품을 암호화하는데 사용할 수도 있고 비밀이 요구되는 다른 정보를 암호화하여 교환하는데 사용할 수 있다. 〔표 1〕은 Chaum의 온라인 전자수표시스템, Deng 등의 온라인 전자수표시스템과 본 시스템을 비교한 표이다.

V. 결 론

이 논문에서 제안한 온라인 전자수표시스템은 부분은닉서명을 이용하여 고객의 익명성을 보장한다. 또한 부분은닉서명에서 공개 정보를 이용하여 수표의 액면가를 표현함으로써 거스름의 형태가 바로 수표가 되도록 하였다. 이렇게 함으로써 기존 전자수표시스템에서 문제가 되었던 거스름의 재사용을 가능하게 하였다. 기존 전자수표시스템의 경우 시스템에서 정해놓은 고정된 금액의 수표를 인출하여야 하는 제한이 있었지만 제안한 시스템에서는 임의의 액면가를 가진 수표를 인출할 수 있다. 뿐만 아니라 초기 수표와 거스름으로 받은 수표는 액면가의 한도 내에서 금액에 대한 제한 없이 사용할 수 있다.

이 논문에서 제안한 시스템의 또 다른 특징은 일련번호로 기존 Deng 등이 제시한 일회성 공개키를 사용하는 대신 일회성 비밀키를 사용한다는 것이다. 이렇게 함으로써 Deng 등이 제시한 시스템의 장점을 그대로 수용함과 동시에 보다 저렴한 연산을 이용하여 효율적으로 지불할 수 있고 입금할 수 있다. 예를 들어 단일 지불세션에서는 서명 방식 대신에 비밀키를 이용하여 거스름 요청서를 만든다. 본 시스템도 온라인 지불의 문제점을 극복하기 위해 Deng 등이 제시한 다중 지불세션 기능을 제공한다. 차이점은 Deng 등의 시스템이 각 지불마다 개인키로 주문서를 서명하여 지불하는 것에 반해 본 시스템에서는 일방향 축적기를 사용한다. 또한 정산과정에서 은행이 확인하여야 하는 정보가 Deng 등의 시스템보다 상대적으로 적다.

일방향 축적기를 지불 프로토콜에 응용한 것은 지금까지 시도된 바가 없는 새로운 접근 방식이다. 효율적인 일방향 축적기에 대한 연구와 새로운 모델의 등장[11]은 이러한 접근방식에 고무적이라 할 수 있다. 그러나 이 논문에서 제안한 시스템은 여전히 온라인 방식이기 때문에 소액환경에서 사용하기에는 다소 문제점이 있다. 물론 다중 지불세션을 통해 어느 정도 극복을 할 수 있지만 궁극적인 해결책이라고 볼 수는 없다. 앞으로 이 논문에서 제안한 시스템 수준의 효율성을 가진 오프라인 전자수표시스템에 대한 연구가 향후 필요하다.

참 고 문 헌

〔1〕 David Chaum, "Blind Signature for Untraceable Payments," *Crypto'82*, pp. 199~203, 1982.

〔2〕 David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash," *Crypto'88*, Springer Verlag, LNCS 403, pp. 319~327, 1988.

〔3〕 David Chaum, "Online Cash Checks,"

Eurocrypt'89, Springer Verlag, LNCS 434, pp. 288~293, 1989.

[4] Stefan Brands, "Untraceable Off-Line Cash in Wallet with Observers," *Crypt'93*, Springer Verlag, LNCS 773, pp. 302~318, 1993.

[5] Ronald L. Rivest and Adi Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," *Proc. of 1996 Int. Workshop on Security Protocols*, Springer Verlag, LNCS 1189, pp. 69~87, 1996.

[6] Yair Frankel, Yiannis Tsiounis, and Moti Yung, "Fair Off-line E-cash Made Easy," *Asiacrypt'98*, Springer Verlag, LNCS 1514, pp. 257~270, 1998.

[7] Robert H. Deng, Yongfei Han, Albert B. Jeng, and Teow-Hin Ngair, "A New On-Line Cash Check Scheme," *Proc. of the 4th ACM Conf. on Computer and Communication Security*, pp. 111~116, 1997.

[8] David Chaum, Bert Boer, Eugene Heyst, Stig Mjoelsnes, and Adri Steenbeek, "Efficient Offline Electronic Checks," *Eurocrypt'89*, Springer Verlag, LNCS 434, pp. 294~301, 1989.

[9] Masayuki Abe and Jan Camenisch, "Partially Blind Signature Schemes," *Proc. of the 1997 Symp. on Cryptography and Information Security Workshop*, 1997.

[10] Josh Benaloh and Michael de Mare, "One-way Accumulators: A Decentralized Alternative to Digital Signatures," *Eurocrypt'93*, Springer Verlag, LNCS 765, pp. 274~285, 1994.

[11] Kaisa Nyberg, "Fast Accumulated Hashing," *Proc. of the 3rd Fast Software Encryption Workshop*, Springer Verlag, LNCS 1039, pp. 83~87, 1996.

〈著者紹介〉

김 상 진 (Sangjin Kim) 정회원
1995년 2월 : 한양대학교 전자계산학과(학사)
1997년 2월 : 한양대학교 전자계산학과(석사)
1997년 3월~현재 : 한양대학교 컴퓨터공학과(박사과정)
〈관심분야〉 암호기술 응용, 전자지불시스템
URL: http://distcomp.hanyang.ac.kr/~sangjin/

최 이 화 (Ihwa Choi) 학생회원
2000년 2월 : 한양대학교 전자계산학과(학사)
2000년 3월~현재 : 한양대학교 컴퓨터공학과(석사과정)
〈관심분야〉 암호기술 응용, 전자지불시스템
URL: http://distcomp.hanyang.ac.kr/~ihchoi/

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과
1989년: 아이오아주립대학 전자계산학과(석사)
1992년: 아이오아주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년~현재: 한양대학교 전자컴퓨터공학부 조교수
〈관심분야〉 암호이론, 전자상거래, 이동컴퓨팅
URL: http://cse.hanyang.ac.kr/~hkoh/