韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-2-2

비밀키를 이용한 사용자 중심의 소액지불시스템

백 승 호*, 정 윤 수**, 원 종 권***, 이 상 호****

A User-based MicroPayment System Using Secret Key

Seung-Ho Baek*, Yun-Soo Jeong**, Jong-Kwon Won***, Sang-Ho Lee****

요 약

최근 인터넷을 통한 거래의 활성화로 인하여 소액지불시스템의 필요성이 더욱 커지고 있으며, 그에 따라 지불금액에 대한 보호뿐만 아니라 사용자의 정보보호에 대한 요구도 증대되고 있다. 그러나 기존의 소액지불시스템들은 익명성을 제공하지 못하거나 익명성으로 인한 지불처리 비용 증가라는 문제점을 가진다. 이 논문에서는 사용자의 익명성을 보장하고 동시에 지불금액을 보호하는 사용자 중심의 소액지불시스템을 제안한다. 제안 시스템은 익명서명 방법으로 사용자 정보를 암호화한 후 난수와의 조합으로 은닉 서명된 익명 아이디를 사용한다. 또한 인증서를 통한 상품과 지불금액 재확인 과정을 통해 사용자의 지불 금액을 보호하고, 공개키 대신 비밀키와 세션키를 사용하므로 효율성을 향상시킨다.

Abstract

Now it is increasing the necessity for micropayment system according to activation for trade on internet. Because of the reason, it is requesting safety for personal information as well as for payment cost. But current micropayment systems cannot support anonymity or have heavy overheads in payment process. This paper suggests a micropayment system to keep anonymity of users and also to keep payment cost safe. The proposed system is to use blind signature anonymous ID which is combined nonce with an encryption of personal information. It also keeps payment cost of users by reconfirmation payment cost and product from certification and increases the computational efficiency by using secret key and session key instead of public key.

▸ Keyword : 비밀키(Secret Key), 소액지불시스템(MicroPayment), 인증서(Certificate), 익명성(Anonimity)

• 제1저자 : 백승호
• 접수일 : 2005.05.10, 심사완료일 : 2005.06.20
* 충북대학교 전자계산학과 석사과정, ** 충북대학교 전자계산학과 박사과정
*** 배화여자대학 컴퓨터정보과 부교수, **** 충북대학교 전기전자컴퓨터공학부&컴퓨터정보통신연구소 교수

Ⅰ. 서 론

전자상거래란 실세계에서 이루어지는 상거래를 통신 매체를 이용하여 가상의 공간에서 이루어지게 하는 상행위이다. 컴퓨터와 통신망을 이용한 전자상거래에서는 상품의 구입과 지불의 시점이 다르기 때문에 발생하는 동시성의 결여와 비대면(非對面) 거래로 인한 상대방의 신뢰성 결여로 기존의 지불 행위와 같이 안전하고 편리하게 지불을 수행하기가 어렵다. 이러한 환경에서 안전하게 사용할 수 있는 지불 방법이 전자화폐이다.

현재까지 개발된 전자지불시스템들은 각기 다른 특성을 갖는다. 전자지불시스템 중, 지불 처리비용을 최소화하여 상대적으로 적은 금액의 지불에 사용할 수 있는 것을 소액지불시스템(MicroPayment System)이라 한다. 소액지불시스템을 사용하여 구매할 수 있는 대표적인 상품은 네트워크를 통하여 전송 가능한 신문, 저널 등의 기사 및 주식 정보, 음악 및 그림 파일, 그리고 자바 애플릿 등과 같은 작은 소프트웨어가 있다[1-8].

대부분의 소액지불시스템은 지불 과정에서 화폐의 유효성을 확인하는 비용을 줄이기 위해 해쉬체인을 사용하여 화폐를 구성한다[1-4, 8]. 또한 트랜잭션의 처리 비용이 커지는 것을 피하기 위해 설계 단계부터 익명을 고려하지 않거나[1, 5-7], 실명으로 하는 신용기반의 후불 시스템으로 구성하기도 한다[1, 8]. 익명 거래가 가능한 [2, 3]은 해쉬체인을 이용한 범용화폐로 익명성은 제공되지만 연산비용이 작지 않아 소액지불시스템에는 부담스럽다는 단점을 가지고 있으나, 거래의 규모가 아무리 작더라도 사용자는 자신의 거래가 알려지기를 꺼려한다. 사이버 거래가 일반화될수록 거래에 사용되고 있는 사용자의 지불비용과 사용자의 개인정보에 대한 보호 요구가 점점 높아지고 있다.

이 논문에서는 기존 소액지불시스템에서 사용되고 있는 오프라인 전자화폐 시스템을 개선한 새로운 사용자 중심의 소액지불시스템을 제안한다. 제안 시스템은 상인이 상품을 사용자에게 전달하지 않고 지불 요청을 하거나, 지불금액을 임의로 변경하여 사용자에게 부당한 금액 처리가 되지 않도록 하기 위해 은행은 사용자의 상품 수령 여부와 상품 금액에 대한 확인 과정을 거쳐 사용자의 이중 지불 방지를 막는다. 특히, 제안시스템은 은닉서명[9]을 통해 사용자의 익명성을 보장하고, 시스템에 사용되는 공개키 대신 비밀키와 세션키 만을 사용하므로 효율성을 향상시킨다. 또한 다른 사용자가 은행에 지불 승인을 임의로 할 수 없도록 하기 위해 인증서를 사용하여 사용자의 금액을 안전하게 보호한다.

이 논문의 구성은 다음과 같다. 2장에서는 기존 소액지불시스템들의 지불방식에 대해 기술하고, 3장에서는 비밀키를 이용한 사용자 중심의 소액지불시스템을 제안하고, 4장에서는 제안시스템을 안전성 측면과 효율성 측면에서 비교평가한다. 마지막으로 5장에서는 결론에 대해 기술한다.

Ⅱ. 관련연구

현재 우리가 일상생활에서 이용하고 있는 현금, 수표 그리고 신용카드 중에서 소액 거래에는 현금이 가장 적합한 지불 수단이라고 할 수 있으나, 현금 그 자체도 1센트나 1원 미만의 액수가 수반되는 거래에는 사용될 수가 없다. 현재 유료 서비스를 제공하는 사이트들에서의 가장 보편적인 지불방식은 사전에 가입신청을 하고 월말에 사용금액을 지불하는 후불방식이다. 정보 서비스 사업이 활성화되기 위해서는 거래 건 당 소액의 요금을 지불 할 수 있는 효율적인 소액지불시스템이 필요하다. 이러한 요구를 충족시키기 위하여 Millicent[10], PayWord[11], MicroMint[11], MPTP[12] 등의 전자지불시스템이 존재한다.

2.1 Millicent

1995년 WWW 학회에서 Steve Glassman이 처음 발표한 Millicent는 소액거래의 전자상거래를 위한 대표적인 지불 시스템으로서, Scrip이라는 전자화폐를 사용한다.

Millicent 지불 시스템은 암호화 알고리즘을 사용하지 않고, 메시지 다이제스트를 이용하여 Scrip을 함으로써 지불비용을 최소화 하였다. 반면, 이 시스템은 거래 주체들 끼리 공유키를 사용하여 Scrip의 유효성 여부를 판단하기 때문에 공유키만을 위한 별도의 데이터베이스를 유지해야 하는 단점을 가지고 있으며, Scrip의 보안에 대한 내용을 Scrip의 발행인만이 알고 있기 때문에 사용자가 은행으로부터 받은 Scrip에 대한 유효성 여부를 판단할 수 없다는 문

제를 가지고 있다[13]. 또한, 거래 후의 잔액에 대해서는 상인이 잔액 Scrip을 발행하기 때문에 제한적인 연속거래가 가능하지만, 마지막 거래까지 잔액이 남는 경우 잔액처리의 부담을 소비자가 안게 되는 단점이 있다.

2.2 Payword

PayWord 지불 시스템은 소액지불에 중점을 두고 MicroMint와 함께 제한된 소액지불시스템이다. 이 시스템은 해쉬체인(Hash Chain)에 기초를 두고 있으며, 전자화폐인 PayWord를 소비자가 직접 발행한다는 특징이 있다. 거래를 희망하는 사용자는 은행에게 자신의 신용카드 번호를 전송하여 인증서를 발급 받아 PayWord를 생성한다. 이 지불시스템에서 소비자는 해쉬체인을 생성하기 위해 임의의 T_n을 선택하고 해쉬 함수를 계속 수행하여 $T_n, T_{n-1}, ..., T_0$를 얻는다.

사용자는 상품대금으로 T_0부터 T_n(상품 가격)까지 차례로 상인에게 전달하고 상인은 T_n을 해쉬 함수를 수행하여 T_{n-1}과 비교한 뒤 지불정보의 유효성 여부를 판단한다. 그러나 사용자가 직접 PayWord를 발행하기 때문에 다른 사용자의 PayWord와 충돌을 일으킬 수 있다는 문제점을 가지고 있다[13]. 또한, PayWord를 연속으로 전송하는 단계를 제외하고, 모든 과정에서 공개키 암호화 알고리즘을 수행하여 속도가 저하되는 단점이 있고, 연속적인 거래가 가능케 하기 위해 은행이 전자 서명한 인증서를 유효기간 동안 계속 사용할 수 있도록 하는 신용기반의 후불방식을 채택하였다. 이러한 후불방식은 사용자가 화폐를 남용할 소지가 있어 시스템 자체의 신용도가 낮아질 수 있다.

2.3 기타 소액지불시스템

iKP 기반 소액지불시스템은 PayWord와 마찬가지로 후불방식의 판매자 전용 화폐이다[14]. 그러나 후불방식에서 신용한도를 제한하기 위해 체인을 상인에게 처음으로 지불할 때 체인의 액면가만큼 사용자가 지불할 수 있는지 상인이 은행으로부터 확인하는 방식을 사용하고 있는 온라인과 오프라인의 중간형태의 지불방식을 사용하고 있다.

Mao는 익명인증서(anonymous certificate)에 포함된 공개키를 화폐에 포함하는 전자화폐를 제안하였다[2]. 사용자는 공개키에 대응되는 개인키로 서명을 함으로써 지불을 하게 되며, 이중사용하면 개인키가 노출되도록 하여 이중사용을 방지하고 있다. 그러나 익명인증서를 이용하므로 같은 해쉬체인을 이용한 지불뿐만 아니라 서로 다른 체인을 이용한 지불도 같은 사용자의 것이라는 것을 알 수 있다. 뿐만 아니라 입금 과정에서 은행이 화폐를 확인하지 않기 때문에 가짜 화폐를 입금할 수 있는 치명적인 허점이 있다. 이 시스템에서는 해쉬체인을 사용하고 남은 부분을 다시 사용할 수 있도록 은행이 아닌 상인이 서명을 하여 만들어 준다. 이렇게 하면 범용성은 서명을 하여 만들어 준다. 이렇게 하면 범용성은 충족되지만 화폐가 사용 될수록 그 크기가 커지는 문제점이 있다.

Nguyen 등은 이중 잠금 해쉬체인이라는 두 개의 해쉬체인을 이용한 구조를 사용하여 PayWord를 범용화폐로 바꾸고자 하였다[3]. 이중 잠금 해쉬체인은 먼저 두개의 해쉬체인$(C_0, ..., C_1)$, $(C'_0, ..., C'_1)$을 만들고, 체인의 루트를 $(C_0, C'_0, l+1)$로 사용한다. 이때 각 동전은 (C_i, C'_{l-i})쌍이 되며, $(C_0, C'_1), (C_1, C'_{l-1}), ...$ 순으로 사용한다. 이렇게 하면 단일 체인을 사용할 때와는 달리 (C_i, C'_{l-i})를 가지고 있어도 그것의 이전 값(C_{i-1}, C'_{l-i+1})이나 이후 값(C_{i+1}, C'_{l-i-1})을 만들 수 없다. 그러나 만약 j>i인 (C_i, C'_{l-i})와 (C_j, C'_{l-j})를 가지고 있으면 두 값 사이에 있는 모든 값을 만들 수 있다는 문제점이 있다.

Nguyen 등은 또한 같은 학술대회에서 오프라인 동전방식의 익명화폐에서 여러 개의 동전을 이용하여 지불하여야 할 경우에 지불의 효율성이 떨어지는 문제점을 해쉬 체인을 이용하여 극복하고자 하였다[4]. 이를 위해 오프라인 동전들을 해쉬체인을 이용하여 연결하여 사용하고 있다. 해쉬체인에 있는 동전 각각에 대해 은행으로부터 은닉서명을 이용하여 연결하여 사용하고 있다. 그러나 해쉬체인에 있는 동전 각각에 대해 은행으로부터 은닉서명을 받아 사용하여야 하므로 인출과정이 복잡하다. 반면에 각 지불에서 첫 동전에 대한 확인과정은 기존의 오프라인 동전과 비슷한 연산량이 요구되지만 그것을 제외한 나머지 동전은 해쉬체인의 특성을 이용하여 확인하므로 저렴하게 확인할 수 있다. 이 시스템은 선불방식의 화폐이지만 환불에 대한 언급은 없다.

Nguyen 시스템에서 사용한 제한적 은닉서명이란 용어는 Chaum과 Pedersen이 제안한 서명기법[15]을 brands[16]가 응용하면서 처음으로 사용되었다. 제한적 은닉서명은 기존의 cut-end-choose 기법을 사용하지 않고 서명 받는 사람이 부정을 못하게 하는 은닉서명이다.

III. 비밀키를 이용한 소액지불시스템 설계

사용자의 익명성을 보장하기 위하여 은닉서명을 사용하며, 사용자의 지불 정보 보호를 위해 상인이 지불 요청 시 은행이 사용자에게 상품 수령과 금액에 대한 확인을 사용자의 인증서를 통해 확인하도록 함으로써 사용자의 지불 금액을 안전하게 처리할 수 있는 소액지불시스템을 제안한다. 제안 시스템은 사용자, 은행 그리고 상인 등 세 개의 구성원으로 이루어지며, 사용자와 상인이 은행에게 계정을 개설하고 비밀키를 발급하는 등록 프로토콜, 사용자와 상인사이에 사용할 세션키를 생성하고 사용자의 인증서를 발급하는 키 생성 프로토콜과 사용자와 상인간의 실제 거래와 지불이 이루어지는 지불 프로토콜로 동작한다.

3.1 가정

제안시스템의 동작을 위한 주요 가정은 아래와 같다[17, 18].

① 사용자와 상인은 거래를 하기 전 은행으로부터 계정을 받는다. 이때 계좌의 생성은 온라인이 아닌 오프라인으로 이루어진다.

② 은행은 사용자와 상인의 중계역할 업무, 계정 관리, 키 생성과 전자화폐 거래의 타당성 검증 등의 역할을 한다.

③ 사용자 개인 신상정보는 사용자와 은행사이의 거래에서만 공유된다. 이것은 RFC 2905의 개인정보 요구에 정의되어 있으며[19] 상인의 업무 처리에 사용자의 신상정보가 필요 없기 때문이다.

④ 구매 정보는 사용자와 상인 사이에서 공유하며, 은행이 구매정보의 내용을 알 필요가 없기 때문이다.

3.2 용어 정의

이 절에서는 앞으로 사용하게 될 주요 기호들을 정의한다.

- C_M : 상품 코드
- ID_C : 거래에서 사용되는 사용자의 아이디
- ID_C' : 은닉서명이 되어 있는 사용자의 익명아이디
- ID_M / ID_B : 상인/은행의 아이디
- N_C : 사용자가 생성한 난수
- ED(Expired Date) : 인증서의 만기일자
- C_U : 은행이 생성한 사용자의 인증서
- L_C / L_M : 사용자/상인의 위치정보
- N : 상인이 사용자에게 전달하는 금액 정보
- N' : 상인이 은행에게 지불 요청 시 사용하는 금액 정보
- K_{CB} : 사용자와 은행간에 공유된 비밀키
- K_{MB} : 상인과 은행간에 공유된 비밀키
- K_{CM} : 은행에서 생성한 사용자와 상인간의 공유된 one-time 세션키
- $h()$: MD5와 SHA-1과 같은 암호 해쉬 함수

3.3 제안시스템의 개요

제안 시스템의 구성원은 은행, 사용자, 상인으로 구성되며, 구성원간의 관계도는 (그림 1)과 같다.

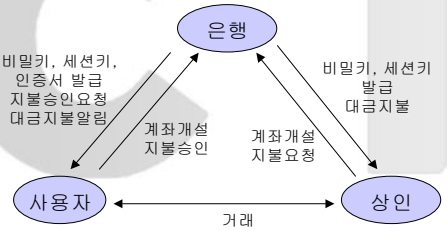

그림 1 구성원간의 관계도
Fig 1. The entity relation scheme

제안 시스템에서 은행, 사용자와 상인 사이에 이루어지는 등록과 지불 등의 주요 동작 흐름은 (그림 2)와 같다.

제안 소액지불시스템에서의 각 단계별 동작 내용은 다음과 같다.

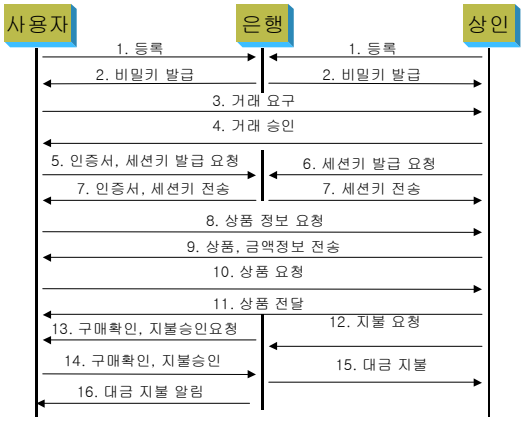

그림 2 제안 시스템의 동작 흐름도
Fig 2. Operation flow of proposed system

사용자와 상인은 은행에게 계좌를 등록한다. 이때 은행은 사용자와 상인의 인증 절차를 거쳐 계좌를 생성하고 사용자와 은행 사이에 사용할 수 있는 비밀키를 생성하여 사용자에게 전달하고, 상인과 은행 사이에 사용할 수 있는 비밀키를 생성하여 상인에게 전달한다(단계 1,2).

사용자는 상인에게 거래 요구를 하고, 상인도 사용자와의 거래를 승인한다(단계 3,4). 사용자는 은행에게 인증서와 상인과 거래 시 사용할 세션키 발급을 요청하며, 상인도 사용자와 거래 시 사용할 세션키를 은행에게 요청한다(단계 5,6). 은행은 사용자의 정보를 이용하여 사용자의 인증서를 생성하며, 사용자와 상인의 정보를 조합하여 세션키를 생성하여 사용자와 상인에게 각각 전달한다(단계 7).

사용자가 상인에게 구매하고자 하는 상품에 대한 정보를 요청하면 상인은 사용자에게 상품에 대한 정보와 금액 정보를 전송한다(단계 8,9). 사용자는 상인에게 받은 상품정보와 금액정보를 검토하여 상인에게 구매의사를 알리고 상품을 요청하면, 상인은 사용자에게 해당 상품을 전달한다(단계 10,11).

상품을 전달한 상인은 은행에게 해당 금액의 지불을 요청한다(단계 12). 지불 요청을 받은 은행은 사용자에게 상품구매 확인과 지불 승인을 요청하며, 사용자는 상품 수령 여부와 상인에게 받은 금액 정보와 은행으로부터 받은 지불 승인 금액이 일치하는지 확인하고, 인증서를 통해 은행에게 지불을 승인한다(단계 13,14). 은행은 해당 금액을 상인에게 전달하고, 사용자에게 지불 내역을 통보한다(단계 15,16).

3.4 소액지불시스템의 프로토콜 설계

제안 시스템의 동작을 위한 주요 프로토콜은 다음과 같다.

- **등록 프로토콜** : 사용자와 상인이 은행에 계좌를 개설하고 사용자와 은행사이에 사용할 비밀키와 은행과 상인 사이에 사용할 비밀키의 발급
- **키 생성 프로토콜** : 사용자의 인증서와 사용자와 상인 사이에 사용될 세션키의 생성
- **지불 프로토콜** : 실제 구매와 지불 절차를 처리

3.4.1 등록 프로토콜

등록 프로토콜은 (그림 3)에서와 같이 사용자와 상인이 은행에 계좌를 생성하고, 비밀키를 발급한다.

사용자는 자신의 개인 정보와는 무관한 ID_C를 생성한 후, 이를 검증받기 위해 ID_C를 은행에게 전달한다(단계 1). ID_C를 전달받은 은행은 사용자의 신원정보를 통해 ID_C를 검증한다(단계 2). 검증이 끝나면 은행은 사용자의 계정을 만들고, 사용자의 사용자 식별자 정보를 데이터베이스에 기록해 놓는다. 이 과정이 종료되면 사용자와 은행은 비밀키 K_{CB}를 공유한다(단계 3).

상인도 사용자와 유사한 방법으로 은행에 계정을 개설하고 은행과 비밀키 K_{MB}를 공유한다(단계 4,5,6).

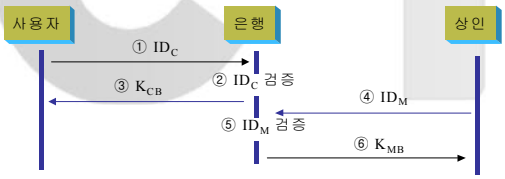

그림 3 등록 프로토콜
Fig 3. Registration protocol

3.4.2 키 생성 프로토콜

키 생성 프로토콜은 (그림 4)와 같이 사용자의 인증서 생성과 사용자와 상인 사이에 사용될 세션키를 생성하여 사용자와 상인에게 전달하는 기능을 수행 한다.

사용자는 은닉 서명을 위해 ID_C를 K_{CM}으로 암호화 하고 N_C를 생성하여 ID_C를 만든다.

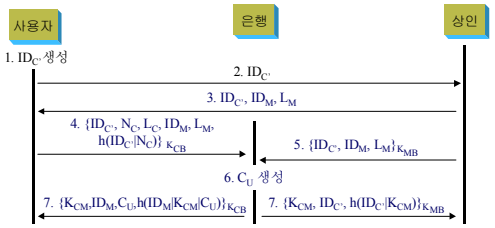

그림 4 키 생성 프로토콜
Fig 4. Key generation protocol

이 결과 상인이나 다른 사람이 사용자의 신분 정보를 알 수 없도록 한다(단계 1).

$$ID_{C'} = \{ID_C\}_{K_{CM}} | N_C \quad \cdots\cdots (3.1)$$

사용자는 상인에게 구매의사를 밝히기 위해 $ID_{C'}$를 전달한다(단계 2).

상인 또한 사용자와 거래를 위해 ID_M과 L_M, 사용자에게서 받은 $ID_{C'}$를 사용자에게 전달한다. 이때 L_M은 사용자의 익명성 및 사생활 정보를 노출시키지 않으면서 서로 다른 상인과 거래를 할 수 있도록 하기 위하여 상인의 위치정보로 사용된다(단계 3).

사용자는 상인과 거래 시 사용 할 세션키를 생성하기 위하여 $ID_{C'}$, N_C, L_C, ID_M, L_M을 K_{CB}로 암호화 하여 전송한다. 이때 부인방지를 위하여 $ID_{C'}$와 N_C는 해쉬 연산을 통하여 보낸다(단계 4).

$$\{ID_{C'}, N_C, L_C, ID_M, L_M, h(ID_{C'}|N_C)\}_{K_{CB}} \quad \cdots\cdots (3.2)$$

상인도 사용자와 거래 시 사용할 세션키 생성을 위해 $ID_{C'}$, ID_M, L_M을 K_{MB}로 암호화 하여 전송한다(단계 5).

$$\{ID_{C'}, ID_M, L_M\}_{K_{MB}} \quad \cdots\cdots (3.3)$$

은행은 사용자와 상인에게서 받은 정보와 N_B를 이용하여 K_{CM}을 생성한다(단계 6).

$$K_{CM} = (ID_{C'}|ID_M|N_B) \quad \cdots\cdots (3.4)$$

또한 $ID_{C'}$, ID_B, L_C, ED를 K_{CB}로 암호화 하여 인증서를 생성한다(단계 6).

$$C_U = \{ID_{C'}, ID_B, L_C, ED\}_{K_{CB}} \quad \cdots\cdots (3.5)$$

은행은 상인에게 K_{CM}과 세션키를 공유할 상대방의 $ID_{C'}$를 전송한다. 이때 부인방지를 위한 두 정보를 해쉬 연산한 $h(ID_{C'}|K_{CM})$값을 첨부하여 K_{MB}로 암호화 하여 전달한다(단계 7).

$$\{K_{CM}, ID_{C'}, h(ID_{C'}|K_{CM})\}_{K_{MB}} \quad \cdots\cdots (3.6)$$

또한 사용자에게 K_{CM}, 공유할 상대방의 ID_M, C_U를 전송한다. 이때 부인방지를 위해 해쉬 연산한 $h(ID_M|K_{CM}|C_U)$ 값을 첨부하여 K_{CB}로 암호화 하여 전달한다(단계 7).

$$\{K_{CM}, ID_M, C_U, h(ID_M|K_{CM}|C_U)\}_{K_{CB}} \quad \cdots\cdots (3.7)$$

은행은 사용자와 상인에게 K_{CM}을 전달하고 난 후 생성한 세션키는 삭제한다. 따라서 추후 사용자와 상인사이에 이루어지는 거래 내용에 대해서 은행은 알 수 없다.

3.4.3 지불 프로토콜

지불 프로토콜은 실제 상품의 구매와 지불과정이 이루어지는 단계로 (그림 5)와 같은 흐름을 가진다.

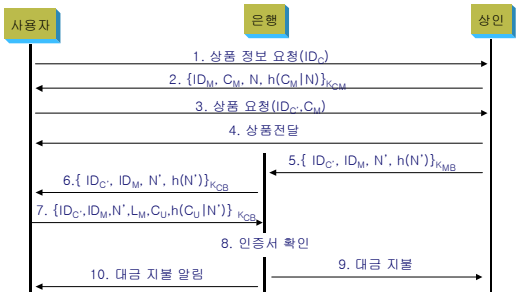

그림 5 지불 프로토콜
Fig 5. Payment protocol

사용자는 구매를 위해 상인에게 ID_C를 전달하여 상품정보를 요청한다(단계 1). 상인은 ID_M과 C_M, N을 K_{CM}으로 암호화 하여 전달한다. 이때 부인방지를 위해 상품정보와 상품금액을 해쉬 연산을 한 $h(C_M|N)$값을 첨부하여 전달한다(단계 2).

$$\{ID_M, C_M, N, h(C_M|N)\}_{K_{CM}} \quad \cdots\cdots (3.8)$$

사용자는 전달 받은 정보를 검토하여 구매의사가 있을 경우 상인에게 ID_C와 C_M을 전달하여 상품을 요청한다(단계 3). 상인은 사용자가 요청한 상품을 전달한다(단계 4). 사용자에게 서비스를 제공한 후 상인은 은행에게 금액에 대한 지불을 요청하기 위해 ID_C, ID_M, N'를 K_{MB}로 암호화 하여 전송한다. 이때 부인방지를 위해 금액을 해쉬 연산한 $h(N')$값을 첨부하여 보낸다(단계 5).

$$\{ID_C, ID_M, N', h(N')\}_{K_{MB}} \quad \cdots\cdots (3.9)$$

은행은 상인에게서 받은 ID_C, ID_M, N'를 K_{CB}로 암호화 하여 고객에게 전달한다. 이때 금액에 대한 부인방지를 위하여 금액정보를 해쉬 연산한 $h(N')$값을 첨부하여 보낸다. 이 과정을 통하여 은행은 사용자가 상품을 수령 했는지 여부와 상품의 금액과 상인이 요구하는 금액이 일치하는지 여부를 확인하여 지불 승인 여부를 결정하게 된다. 이러한 확인 과정을 통하여 사용자의 지불을 보호할 수 있게 된다(단계 6).

$$\{ID_C, ID_M, N', h(N')\}_{K_{CB}} \quad \cdots\cdots (3.10)$$

사용자는 은행으로부터 받은 N'와 이전에 상인에게서 받은 N을 비교하여 상인이 지불을 요청하는 금액이 정확한지를 확인한다. 금액이 일치할 경우 ID_C, ID_M, N', L_M, C_U를 K_{CB}로 암호화 하여 전달한다. 이때 부인방지를 위하여 N'와 C_U를 해쉬 연산 한 $h(N'|C_U)$값을 첨부하여 전달한다. 인증서 사용하기 때문에 인증서를 가지고 있지 않은 다른 사용자가 임의로 지불 승인을 할 수 없도록 한다(단계 7).

$$\{ID_C, ID_M, N', L_M, C_U, h(C_U|N')\}_{K_{CB}} \quad \cdots\cdots (3.11)$$

은행은 사용자에게서 받은 인증서를 확인하여 이상이 없을 경우, 해당 금액을 상인에게 지불하고 사용자에게 대금 지불을 알린다(단계 8, 9, 10).

Ⅳ. 평가

이 장에서는 제안 소액지불시스템을 안전성 측면과 효율성 측면으로 평가한다. 안전성 측면의 평가는 부인방지, 상호인증, 위조방지, 익명성, 이중사용방지 등의 항목을 통하여 기존의 소액지불시스템들과 비교 평가한다. 효율성 측면에서는 기존 해쉬체인 기반 지불시스템인 PayWord, iKP 기반 소액지불시스템, Mao의 시스템, Nyugen의 이중 잠금 해쉬체인, Nyugen의 시스템, 일반 오프라인 동전방식과 비교 평가한다.

4.1 안전성 측면

안전성은 보안성, 익명성, 위조방지, 부인방지, 상호인증의 다섯 가지 항목으로 평가한다.

4.1.1 보안성(Security)

제안 시스템은 일방향 해쉬 함수와 사용자와 은행사이에 비밀키를 사용한다. 상인과 은행, 사용자와 은행 사이의 거래 정보는 항상 비밀키로 암호화 되며 사용자와 상인 사이는 세션키를 사용하여 암호화되기 때문에 안전하다.

이때 사용자와 상인 사이에 사용되는 세션키는 은행이 생성하지만 생성된 키는 사용자와 상인에게 전달한 후 삭제하기 때문에 사용자와 상인 사이에 주고받는 정보에 대해서 은행은 알지 못한다.

상인이 은행에 요청하는 지불은 항상 사용자의 승인이 있어야지 지불되기 때문에 사용자의 지불을 보호할 수 있다. 공격자가 임의로 지불을 요청할 수 없으며, 사용자의 승인 시 인증서가 사용되기 때문에 공격자가 임의로 승인을 하여 사용자의 금액이 지불되는 것이 방지된다.

4.1.2 익명성(Anonymity)

사용자의 익명성 보장은 소액지불시스템의 가지야 할 중요한 기능이다. 제안시스템은 은닉 서명을 통하여 사용자의 익명성을 보장하고 있다. 즉, 거래에 사용되는 ID_C는 사용

자의 실제 정보와 관련이 없다. 상인은 사용자가 거래하는 것을 결정하지 못하지만 은행은 상인의 위치정보가 포함된 사용자의 구매정보를 이용한다. de Solages 와 Traore의 제한적 은닉서명 정리 2에 의해 은행은 서명과정에서 얻은 정보로부터 서명한 메시지나 결과 서명에 대한 어떤 정보도 얻을 수 없다[19].

4.1.3 위조방지

제안시스템은 은행이 직접 지불하는 후불 방식이기 때문에 동전에 대한 위조문제는 발생하지 않는다. 거래에 사용되는 금액 정보는 해쉬 연산과 비밀키, 세션키를 통한 암호화를 통해 보호되며, 상인이 사용자에게 전달한 N과 상인이 은행에게 지불 요청을 하는 N'를 사용자가 확인하여 승인하기 때문에 금액 정보를 임의로 조작 할 수 없다.

4.1.4 부인방지

부인방지는 비밀 서명키를 이용한 전자 서명을 통해 제공될 수 있다. 시스템의 각 구성원들은 자신의 공개키와 개인키의 쌍을 생성하여 부인 방지가 필요한 메시지에 대하여 서명 알고리즘을 적용해야 한다. 제안 프로토콜에서는 사용자가 지불 단계에서 C_U를 포함하는 승인 메시지를 은행에게 전송하며 이 승인 메시지는 사용자와 은행 사이의 비밀키로 암호화된다. 따라서 사용자는 이후부터 지불 정보에 대하여 부인할 수 없으며 판매자도 사용자에게 제공하는 서비스에 대하여 부인할 수 없다.

4.1.5 상호인증

상호인증은 사용자와 상인사이의 인증을 말한다. 은행으로부터 K_{CM}이 생성되기 때문에 키 인증과 개체 인증에 대한 요구사항을 만족시킨다. 또한 사용자와 상인 사이에 사용되는 세션키를 통해 서로를 신뢰하고 상대방을 인증 할 수 있다.

4.1.6 평가

기존 해쉬 체인 기반의 소액지불시스템과 제안 시스템의 안전성 측면의 평가 결과는 <표 1>과 같다.

표 1 기존 해쉬체인 기반 지불시스템과의 안전성 비교
Table 1. Security analysis of pre-proposed hash-chain based micropayment

	부인 방지	상호 인증	위조 방지	익명성	이중사용 방지
PayWord	○	○	○	×	○
ikP기반 소액지불시스템	○	○	△	×	○
Mao의 시스템	○	○	×	△(가명사용)	○
Nguyen의 이중잠금 해쉬체인	○	○	△	×	○
Nguyen의 시스템	×	△	○	○(각 동전에 은닉서명)	○
일반오프라인 동전방식	△	△	○	○	×
제안시스템	○	○	○	○(사용자 아이디에 은닉서명)	×

○:지원, △:일부지원, ×:지원안함

<표 1>에서 보는 바와 같이 해쉬체인을 기반으로 화폐를 구성하는 기존 기법들은 체인의 루트를 통해 n번 은닉서명을 사용하여 익명성을 제공하지만 제안기법에서는 사용자 아이디에 한번만 은닉서명을 사용하고 있기 때문에 기존 기법들보다 익명성을 효과적으로 지원한다. 또한, 대부분의 분할 가능한 화폐는 이진트리 구조를 이용하고 있다. 이 이진트리 구조는 인출하기 전에 미리 만든 구조가 아니며 지불할 때 필요한 노드만 만들어 사용한다. 반면 제안 시스템에서는 어떤 임의의 대금을 지불하기 위해 그만큼의 노드를 전달할 필요가 없다. 그러나 제안시스템의 이런 특징은 선불방식이 아닌 후불방식으로 은행이 직접 금액을 지불하는 기법으로 기존 소액지불시스템들이 제공하는 이중사용방지를 제공하지 않는 단점을 가진다.

4.2 효율성 측면

기존 해쉬 체인 기반의 소액지불시스템과 제안 시스템의 효율성 측면의 평가 결과는 <표 2>와 같다.

표 2 기존 해쉬체인 기반 지불시스템과의 효율성 비교
Table 2. Efficiency analysis of pre-proposed hash-chain based micropayment

	선불:○ 후불:◇	범용:○ 판매자 전용:◇	인증서 유형	인출 비용	지불비용
PayWord	◇	◇	공개키, 인증서사용	×	- 체인루트에 대한 서약(서명) 확인 - 나머지 : 해쉬연산
iKP 기반 소액지불시스템	◇	◇	공개키, 인증서사용	×	- 체인루트에 대한 서약(서명) 확인 - 신용한도 확인, 나머지 : 해쉬연산
Mao의 시스템	○	○ 상인이 거스름	공개키, 인증서사용	한번 은닉서명	- 여러 상인에게 지불할수록 그 다음 상인이 확인하여야 하는 정보가 많음
Nyugen의 이중잠금 해쉬체인	○	○ 이중잠금 해쉬체인	공개키, 인증서사용	한번 일반서명	- 체인루트에 대한 서약(서명) 확인 - 나머지 : 해쉬연산 - 영수증 발급
Nyugen의 시스템	○	○ 각 동전에 서명	공개키, 인증서사용	n번 은닉서명	- 첫 동전: 서명과 시도와 응답 - 나머지 : 서명
제안 시스템	◇	◇	비밀키 인증서사용	×	- 은행의 지불 재확인 요청을 통해 서약(서명) 확인
일반 오프라인 동전방식	○	○ 각 동전에 서명	공개키, 인증서사용	n번 은닉서명	- 각 동전마다 서명과 시도와 응답

<표 2>에서와 같이 제안 시스템은 후불 방식의 판매자 전용 화폐로 인증서와 비밀키를 사용하며, 은행의 지불 재확인 요청을 통한 서명 확인 시 지불비용이 발생한다. 또한 후불구조로 공개키의 사용 없이 비밀키와 세션키만으로 모든 거래가 이루어진다. 이때 사용되는 세션키 K_{CB}는 은행에서 생성하나, 사용자와 상인에게 전달한 후 삭제하기 때문에 사용자와 상인의 거래 시 이루어지는 내용에 대해서는 은행은 알 수 없다.

초기 PayWord 기법에서 사용자는 은행에 의해 생성된 인증서와 루트 값 W_0의 디지털 시그너처, 기타 다른 정보 및 지불을 수신받기 위한 상인의 아이디 등을 생성한다. 이것은 디지털 시그너처가 후에 사용자가 지불하기 위한 약속으로써 사용되었다. 그러나 공개키 기반의 디지털 시그너처 요구는 계산 시간의 측면에서 커다란 단점을 가진다. 이 문제를 해결하기 위해 제안시스템에서는 세션키를 사용하여 연산비용을 줄인다.

V. 결론

대부분의 전자상거래에서 네트워크를 통해 직접 전송이 가능한 비교적 소액의 상품들의 거래가 많이 이루어지고 있으며, 앞으로 더욱더 그 활용도가 더욱 증가할 전망이다. 이러한 소액 상품의 지불을 위해 해쉬 함수와 같은 비용이 적게 드는 암호화 기법을 사용하는 Millicent, PayWord, MicroMint와 같은 지불 시스템들이 있다. 하지만 이러한 기존의 지불 시스템들은 사용자의 익명성을 보장하지 못한다.

이 논문에서는 사용자의 익명성을 보장하며, 사용자의 지불 금액을 보호하는 새로운 소액지불시스템을 제안하였다. 즉, 한 번의 은닉서명을 통해 사용자의 익명성을 보장하며, 기존 시스템들이 사용하는 공개키 대신 비밀키와 세션키만을 사용하여 지불을 처리함으로써 효율성을 향상시켰다. 또한 상인이 사용자에게 부당한 지불요청을 은행이 사용자에게 상품 수령확인과 사용자가 구매한 상품의 가격과 상인이 지불 요청한 금액의 확인을 통하여 해결하였다.

제안 시스템은 인증서를 사용하여 은행이 지불 전에 사용자에게 상품 전달과 금액의 재확인 과정을 거쳐 사용자의 지불 금액에 대한 보호를 높였으며, 은닉서명을 통하여 사용자 정보의 노출을 방지하였다. 또한 공개키 기반이 아닌 비밀키와 세션키를 이용함으로써 지불처리에 소요되는 연산비용을 줄였다.

참고문헌

[1] Rivest, R.L, and Shamir, A., "PayWord and MicroMint-Two Simple Micropayment Schemes," Proc. of the 1996 Int, Workshop on Security Protocols, LNCS 1189, pp. 69-87, Springer, 1997

[2] Mao, W., "Lightweight Micro-Cash for the Internet," Proc. of the 1996 European Symp. on Research in Computer Security, ESORICS 1996, LNCS 1146, pp. 15-32, Springer, 1996

[3] Nguyen, K.Q., Mu Y., and Varadharajan, V., "Micro-Digital Money for Electronic Com-merce," Proc. of the 13th IEEE Annual Computer Security Applications Conf., pp. 2-8, IEEE Computer Society Press, 1997

[4] Nguyen, K.Q., Mu Y., and Varadharajan, V., "Secure and Efficient Digital Coins," Proc. of the 13th IEEE Annual Computer Security Applications Conf., pp. 9-15, IEEE Computer Society Press, 1997

[5] M. S. Manasse, "The Milicent Protocols for Electronic Commerce," Proc. of the 1st USENIX Workshop on Electronic Commerce, pp. 117-128, Jul. 1995

[6] A. Herzberg and H. Yochai, "Mini-pay: Charging per Click on the Web," Proc. of the 6th Int. World Wide Web Conf., Apr. 1997

[7] C. Jutla and M. Yung, "PayTree: Amortized -Signature for Flexible MicroPayments," Proc. of the 2nd USENIX Workshop on Electronic Commerce, pp. 213-221, Nov. 1996

[8] Y. Mu, V. Varadharajan, and L. Y. X. Lin, "New Micropayment Schemes Based on PayWords," In Proceedings of 2nd Australasian Conference on Information Security and Privacy(ACISP '97), Lecture Notes in Computer Science 1270, pp. 283-293, Springer-verlag, 1997

[9] 이재영, 이지영, "디지털서명과 은닉서명에 관한 연구," 한국컴퓨터정보학회, 5권, 3호, 2005년

[10] Steve Glassman, "The Millicent Protocol for Inexpensive Electronic Commerce," 1995

[11] R.L.Rivest, "PayWord and MicroMint:Two simple micropayment schemes," 1996

[12] Phillip M.Hallam-Baker, "Micro Payment Transfer Protocol(MPTP) Version 0.1," W3C Working Draft, 1995

[13] Ellis Chi, "Evaluation of Micropayment Schemes," HP Lab, technical report, 1997

[14] Hauser, R., Steiner, M., and Waidner, M., "Micro-payments based on iKP," Proc. of the 14th Worldwide Congress on Computer and Communications Security and Protection, SECURICOM 1996, pp. 67-82, 1996

[15] Chaum, D. and Pedersen, T.P., "Wallet Databases with Observers," Advances in Cryptology, Crypto 1992, LNCS 740, pp. 89-105, Springer, 1993

[16] Brands, S., "Untraceable Off-Line Cash in Wallets with Observers," Advances in Cryptology, Crypto 1993, LNCS 773, pp. 302-318, Springer, 1994

[17] Jing-Jang Hwang, Tzu-Chang Yeh, Jung-Bin Lie, "Securing on-line credit card payments without disclosing privacy information," computer Standards&Interfaces 25, pp 119-129, 2003

[18] Pointcheval, D. and Stern, J., "Security Arguments for Digital Signatures and Blind Signatures," J. of Cryptology, Vol. 13, No. 3, pp. 361-396, 2000

[19] Network Working Group, "AAA Authorization Application Examples," RFC 2905, http://www.faqs.org/rfcs/rfc2905.html

[20] de Solages, A. and Traore, J., "An Efficient Fair Off-line Electronic Cash System with Extensions to Checks and Wallets with Observers," Proc. of the 2nd Int. Conf. on Financial Cryptography, FC 1998, LNCS 1465, pp. 275-295. Springer, 1998

저 자 소 개

백 승 호

2003년 2월 : 한밭대학교 컴퓨터공학과 공학사

2003~현재 : 충북대학교 전자계산학과 석사과정

<관심분야> 침입탐지, 정보보호, Network Security, 전자상거래보안

정 윤 수

1998년 2월 : 청주대학교 이학사

2000년 2월 : 충북대학교 전자계산학과 이학석사

2003년~현재 : 충북대학교 전자계산학과 박사과정

<관심분야> 정보보호, Network Security, 이동통신보안, 전자상거래보안, MIPv6 보안

원 종 권

1982년 2월 : 충북대학교 공과대학 공학사

1988년 8월 : 충북대학교 전자계산학과 이학석사

1992년2월 : 충북대학교 전자계산학과 이학박사

1992년~현재 : 배화여자대학 컴퓨터정보과 부교수

<관심분야> CDMA 이동통신, 트래픽제어, 네트워크 보안

이 상 호

1981년 : 숭실대학교 대학원 전자계산학과 이학석사

1989년 : 숭실대학교 대학원 전자계산학과 이학박사

1990년~1991년 : 캐나다 UBC 객원교수

1981년~현재 : 충북대학교 전기전자컴퓨터공학부 교수

<관심분야> Protocol Engineering, Network Security, Network Management, Network Architecture