# Hash chain 을 이용한 선불방식의 소액 전자지불 시스템의 설계

이호웅*, 김기창*
*인하대학교 전자계산공학과
e-mail : always14@super.inhc.ac.kr, kchang@super.inha.ac.kr

# Designing of Prepaid Micropayment System using The Hash chain

Ho-woong Lee*, Ki-chang Kim*
*Dept. of Computer Science & Engineering, In-Ha University

**요 약**

최근 급증하고 있는 인터넷 전자상거래의 가장 필수적인 부분이 전자지불 시스템이다. 전자적으로 처리되는 지불시스템은 사용자의 익명성 보장, 지불정보의 위조 및 재사용방지 등의 특징을 가지며, 거래 주체들간의 신뢰구축을 위한 상호 인증이 요구된다. 디지털 기술의 발달로 소액의 디지털 상품들이 많이 등장함에 따라 소액 상품만을 결제하기 위한 소액지불 시스템의 필요성이 증대되면서, Millicent, PayWord, MicroMint, MPTP 등의 소액 지불 시스템들이 연구되었으나 아직 효과적으로 사용되지 못하고 있다. 이러한 소액 지불 시스템의 경우에는 소비자가 한 상점에서 연속적인 거래를 수행하는데 따르는 비용을 먼저 생각해야 한다. 그 이유는 소액거래를 하는 대부분의 소비자들은 여러 개의 상품을 연속적으로 구입하는 경향을 가지기 때문이다. 또한 거래 주체간의 대금결제의 편의성을 도모하기위한 선불방식에 대한 연구가 필요하다. 그러나, 기존의 소액 지불 시스템들은 연속거래에 있어 제한적이거나 소비자의 신용을 기반으로 한 후불방식을 채택하고 있어 소비자의 화폐남용에 대한 자원낭비의 문제를 안고있다.

이에 본 논문에서는 Hash Chain을 이용하여 연속거래에 적합한 선불방식의 소액전자지불 시스템을 제안한다.

## 1. 서론

최근 초고속 정보통신망 구축에 따른 인터넷의 보급 확산과 함께 인터넷 전자상거래라는 새로운 문화가 활성화되고 있다. 전자상거래는 현실 생활의 상거래 환경을 인터넷 상에서 구현함으로써 거래비용의 감소와 거래의 신속성을 높이는 효과를 가져왔다. 이러한 인터넷 전자상거래가 많은 소비자들과 판매자들에게 널리 수용되고 보편화 되면서 보다 안전하고 편리한 전자지불 시스템의 필요성이 증대되고 있다.

전자지불 시스템은 효과적인 지불을 위해 여러 가지 기능을 수행해야 한다. 거래에 사용된 지불 정보들을 사용자가 복사해 두었다가 다른 거래에 복사된 지불정보를 다시 사용하는 이중사용을 방지해야 하고, 제3자에 의해 위조나 변조된 지불정보의 사용을 막을 수 있어야 한다. 그리고 거래가 인터넷을 통해 이루어지기 때문에 거래 주체간의 신뢰구축을 위한 상호 인증이 우선되어야 하며, 지불시스템 사용자의 사생활 침해를 막기위해서 사용자에 대한 익명성이 보장되어야 한다. 그러나, 지불 시스템이 이러한 기능들을 모두 수행하기 위해서는 높은 지불처리 비용을 감수해야 한다.

앞으로의 전자상거래에는 고가의 상품뿐만 아니라 문서, 각종 음악화일, 동영상이나 그림화일, 증권정보 같

은 소액의 정보 상품들이 많이 등장할 것이다[1]. 만일, 높은 지불처리 비용의 지불시스템을 소액상품의 거래에 그대로 사용한다면 실제지불금액보다 전자지불을 하기위한 처리비용이 더 높아져 전자상거래 자체의 경제성이 떨어지는 결과를 낳을 수도 있다. 그래서, 현재의 소액 전자지불 시스템들은 지불정보의 생산과 전달과정에서 암호화 과정을 줄이고, 대신에 Hash함수와 같은 빠른 연산을 사용하여 지불처리비용을 최소화 하고 있다. 그러나, 소액상품의 거래는 소비자가 상점에 들러 한 두개의 상품만 구입하는 고액거래와는 달리, 한 소비자가 한 상점에서 여러 개의 상품을 연속적으로 구입하는 거래특성을 가지고 있기 때문에 연속거래에 대한 효율적인 처리가 고려되어야 한다.

대부분의 소액 지불 시스템들이 은행계좌나 Credit카드 등의 신용을 기반으로 하는 후불방식을 채택하여 제한적인 연속거래를 보장하고 있지만, 카드 사용시 별도의 수수료비용이 추가될 수 있는 단점이 있다. 또한, 소비자가 자신의 신용한도를 초과하여 화폐사용을 남발하는 경우 지불 시스템 자체의 신용도가 떨어진다는 문제를 가지고 있다. 반면에 기존의 선불방식 지불시스템은 적절한 화폐사용을 보장하지만 거래가 발생할 때마다 브로커와 잔액을 확인하는 절차를 수행해야 하기 때문에 연속거래를 수행하는 비용이 크다는 단점이 있다.

이에 본 논문에서는 소액지불을 위한 사용이 편리하면서 연속거래 비용이 적은 선불방식의 소액 전자지불 시스템을 소개한다. 2장에서는 기존 소액 지불 시스템들의 지불방식에 대해 살펴보고, 3장에서는 본 논문에서 제안한 Hash chain을 이용한 선불방식의 소액 지불 시스템에 대해 설명하고, 4장에서 결론과 앞으로의 연구과제에 대해 설명한다.

## 2. 관련연구

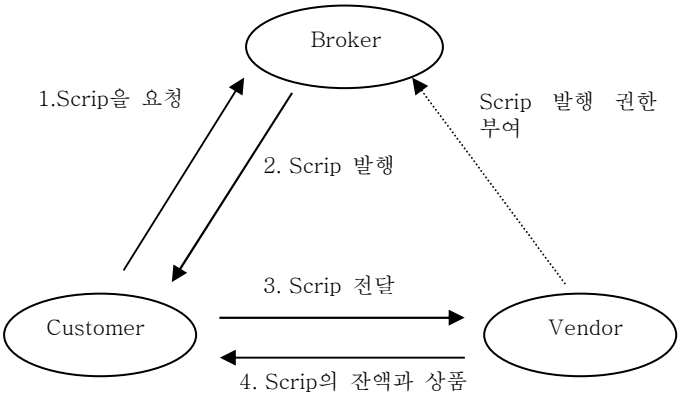
### 2.1 소액 전자지불 시스템의 종류

현재 대부분의 전자지불 시스템들은 소액지불에 사용될 경우 상품가격에 비해 상대적으로 높은 지불처리비용을 부담해야 하는 단점을 갖고 있다. 앞으로의 전자상거래는 논문이나 신문기사 같은 문서화일, MP3 같은 음악화일, MPEG나 AVI같은 동영상화일, GIF나 JPEG같은 그림화일 등 소액의 정보상품이 차지하는 비중이 높아질 것이다. 이러한 소액 정보 상품에 대한 전자지불을 효과적으로 하기 위한 전자지불 시스템으로는 Millicent[1], PayWord[2], MicroMint[2], MPTP[8] 등이 있다.

#### 2.1.1 Millicent

1995년 WWW학회에서 Steve Glassman이 처음 발표된 Millicent는 소액거래의 전자상거래를 위한 대표적인 지불 시스템으로서, Scrip이라는 전자화폐를 사용한다.

아래의 그림[1]에서와 같이 소비자는 브로커에게 Scrip을 받아 상점에게 그 Scrip을 지불함으로써 원하는 상품이나 서비스를 구매할 수 있다. 일반적으로 상점이 직접 Scrip을 발행하지만, 상점이 Scrip을 발행하지 않고 브로커에게 Scrip발행에 필요한 Parameter를 건네주어 대신 발행케 할 수 도 있다.

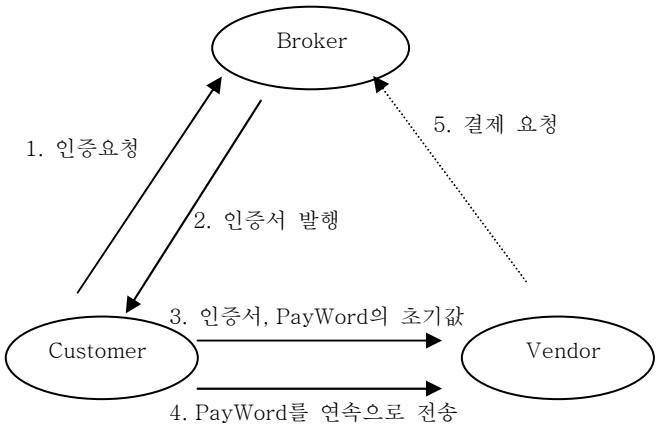



[그림 1] Millicent의 시스템 구성

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 유지 해야 하는 단점을 가지고 있으며, Scrip의 보안에 대한 내용을 Scrip의 발행인만이 알고 있기 때문에 소비자가 브로커로부터 받은 Scrip에 대한 유효성 여부를 판단할 수 없다는 문제를 가지고 있다.[3] 또한, 거래후의 잔액에 대해서는 상점이 Scrip을 잔액Scrip을 발행하기 때문에 제한적인 연속거래가 가능하지만, 마지막 거래까지 잔액이 남는 경우 잔액처리의 부담을 소비자가 안게 되는 단점이 있다.

#### 2.2.2 PayWord

PayWord 지불 시스템은 소액지불에 중점을 두고 MicroMint와 함께 제안된 소액 전자지불 시스템이다.




[그림 2] PayWord의 시스템 구성

이 시스템은 Hash Chain에 기초를 두고 있으며, 전자화폐인 Payword를 소비자가 직접 발행한다는 특징이 있다. 그림[2]에서와 같이 거래를 희망하는 소비자는 브로커에게 자신의 신용카드번호를 전송하여 인증서를 발급 받아 Payword를 생성한다. 이 지불시스템에서 소비자는 Hash chain을 생성하기 위해 임의의 $T_n$을 선택하고 Hash를 계속 수행하여 차례로 아래와 같은 $T_n$, $T_{n-1}$,…$T_0$를 얻는다.

$$T_0 = H(T_1)$$
$$T_1 = H(T_2)$$
$$\vdots$$
$$\vdots$$
$$T_{n-1} = H(T_n)$$
$$T_n = \text{상품가격}$$

소비자는 상품대금으로 $T_0$부터 $T_n$까지 차례로 상점에게 전달하고 상점은 $T_n$을 Hash 함수를 수행하여 $T_{n-1}$과 비교한 뒤 지불정보의 유효성 여부를 판단한다. 그러나, 소비자가 직접 Payword를 발행하기 때문에 다른 소비자의 Payword와 충돌을 일으킬 수 있다는 문제점을 가지고있다.[3] 또한, PayWord를 연속으로 전송하는 단계를 제외하고, 모든 과정에서 공개키 암호화 알고리즘을 수행하여 속도가 저하되는 단점이 있다. 또한 PayWord는 연속적인 거래가 가능케 하기 위해 브로커가 전자서명한 인증서를 유효기간 동안 계속 사용할 수 있도록 하는 신용기반의 후불방식을 채택하였다. 이러한 후불방식은 소비자가 화폐를 남용할 소지가 있어 시스템 자체의 신용도가 낮아질 수 있다.

2.2.3 그 외 소액 전자 지불 시스템

그 외의 소액 전자지불 시스템으로 MITLCS의 Ronald Rivest와 Weizmann Institute of Science의 Adi shamir가 제안한 MicroMint와 PayWord방식을 변형한 MPTP[8], 그리고, PayWord방식과 Ecash방식을 혼용하여 제안한 Wenbo Payment[3]가 있다.

MicroMint는 minted라고 불리는 coin을 브로커가 생산하고 소비자는 브로커로부터 coin을 사서 상점에 지불하는 방식이다. 공개키 암호화를 사용하지 않고 공유키도 사용하지 않는다. 그러나, 소비자의 요구보다 많은 coin을 생산하기 때문에 자원의 낭비가 발생하고, 위조방지를 위해 Hash 이외에 부가적인 연산을 수행해야 한다.

## 3. Hash Chain을 이용한 선불방식의 소액 전자지불 시스템

3.1 시스템의 특징

이 시스템은 선불 방식을 사용하면서 연속거래에 대한 처리비용을 최소화 하였다.

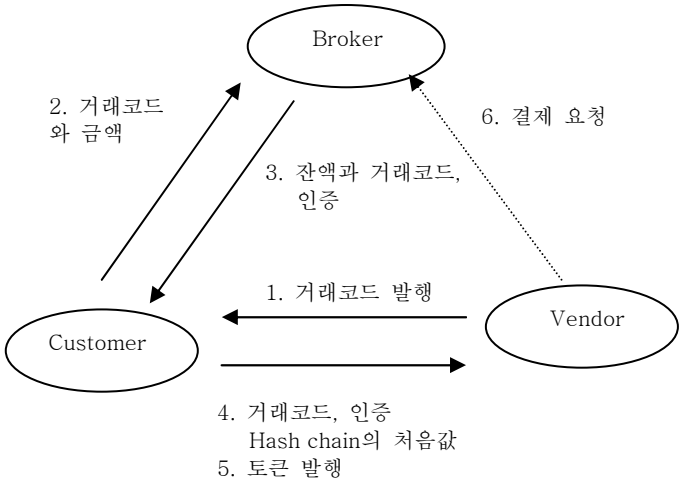
이 시스템은 PayWord에서 사용한 Hash chain방식을 이용하였으며, Hash 함수로는 MD5[5]나 SHA[6]가 사용된다. Hash chain방식이란 위에서 언급하였듯이 소비자는 먼저 임의의 $T_n$을 선택하여 Hash 함수를 n번 수행하고, 그 결과값인 $T_0$부터 $T_n$까지를 차례로 상점에 전송하여 대금 지불을 수행하는 방식을 말한다. 여기서 $T_0$ 는 Hash Chain의 무결성을 확인하기 위한 Chain의 초기값이며, $T_1$부터 $T_n$은 10원단위의 매우 적은 가치를 가지는 token을 나타낸다.

그리고, 이 시스템은 지불정보의 이중지불방지와 연속거래의 비용을 줄이기 위해 소비자가 거래코드를 상점으로부터 받아오는 방법을 이용하였다.[10] 그리고, 한 번 상점으로부터 받은 거래코드는 그 상점에서의 거래가 모두 종료할 때까지 계속 사용할 수 있도록 하여 연속거래를 보다 편리하게 수행하도록 하였다.

선불방식의 경우 소비자가 사용할 수 있는 금액이 한정되어 있기 때문에 화폐의 남용을 막을 수 있는 장점이 있지만, 거래가 발생할 때 마다 소비자의 잔액을 확인해야 하는 단점을 가지고 있었다. 그러나, 이 시스템은 소비자가 자신의 지불 한도 내에서 원하는 금액만큼의 화폐를 발행할 수 있도록 하여 잔액확인의 비용을 절감하였다. 또한, 브로커와 상점간에 약속된 PassWord를 이용한 인증방법을 사용하여 전자서명에 따른 암호화비용을 절약하였으며, 처음 브로커로부터 받은 인증을 그 상점과 거래가 종료할 때 까지 계속 사용할 수 있도록 하여 브로커와의 연결부담을 감소시켰다.

거래 후 잔액처리에 있어서도 상점이 브로커에게 소비자의 잔액 액수만큼의 충전을 요청함으로써 소비자는 잔액에 대해 신경을 쓰지 않아도 된다.

3.2 시스템의 구성 및 지불절차




[그림 3] 시스템 구성 및 지불절차

그림[3]에서와 같이 소비자, 브로커, 상점의 세가지 거래주체로 시스템이 구성되며 소비자가 상점을 방문하여 거래코드를 받아 거래를 시작하게 된다.

지불절차에 사용되는 기호는 [표 1]과 같다.

[표 1] 지불절차에 사용되는 기호

| | |
|---|---|
| C , Cid | 소비자, 소비자의 ID |
| V | 상점 |
| B | 브로커 |
| X->Y:M | X에서 Y로 M을 전달 |
| S# | 거래코드 |
| $T_0$ | 소비자가 발행할 Hash chain의 root |
| Tl | 소비자가 발행할 Hash chain의 길이 |
| H(M) | M에 대해 Hash 한 값 |
| $T_n$,n | 소비자가 Hash chain을 이용하여 생성한 token |
| Cid | 소비자의 ID |
| Pw | 브로커와 상점만이 알고있는 PassWord |

각 거래 주체간의 거래 순서와 전달되는 지불정보는 다음과 같다.

(1) 소비자가 상점을 방문하여 거래코드를 전달 받는다. 거래코드는 브로커가 상점을 식별할 수 있는 상점의 일련번호와 상점이 발행한 거래번호로 이루어져 있다. 거래코드의 노출을 막기위해 SSL을 이용한다.
**V->C: S#**

(2) 소비자는 자신의 ID와 함께 거래코드와 자신이 화폐를 발급하기 원하는 금액(Value)을 브로커에게 전달한다. ID와 거래코드의 노출을 막기 위해 SSL을 사용한다.
**C->B: Cid, S#, Value**

(3) 브로커는 소비자의 잔액을 확인하고, PassWord와 거래코드, Value를 Hash하여 소비자에게 전달한다. 그리고, 잔액을 갱신하여, 잔액(Value')을 소비자에게 알려준다. 이 시스템에서 H(S#, Value, Pw)는 인증서와 같은 효과를 가진다.
**B->C: H(S#, Value, Pw), H(S#, Cid, H(S#, Value, Pw)), Value'**

(4) 소비자는 자신이 발급할 수 있는 액수 만큼의 Hash chain을 생성하여 Hash chain의 초기값인 $T_0$, Hash chain의 길이 Tl, 거래코드, 그 외 지불에 필요한 정보들(request)을 상점에 전달한다.
**C->V: S#, Value, $T_0$, Tl, H($T_0$, Tl, H(S#,Value, Pw)), request**

(5) 소비자는 Hash chain에 의해 생성된 token을 상품 가격만큼 차례로 브로커에게 전달한다.
**C->V: ($T_n$, n)**

또한, 소비자는 연속적으로 다른 상품을 구입하고자 할 경우 새로운 $T_n$'을 선택하여 $T_0$'와 Tl을 계산하여 상점에게 전달하게 되는데 다시 브로커와 연결하여 인증을 받을 필요 없이 H(S#, Value, Pw)를 다시 사용한다.
**C->V: S#, $T_0$', Tl', H($T_0$', Tl', H(S#,Value, Pw)), request**
**C->V: ($T_n$',n')**

(6) 브로커는 만일 소비자가 Value보다 적은 금액을 사용하고 거래를 완전히 종료한 경우, 남은 잔액을 브로커에 전달하여 잔액을 충전하도록 하여, 잔액관리에 대한 소비자의 부담을 감소시켰다.
또한, 하루에 한 번 상점은 브로커에게 거래코드와 최종 $T_n$값을 전달하여 정산을 요청하고, 다음 정산 때 까지 사용할 새로운 PassWord를 다시 결정한다.

### 3.3 시스템의 기능

#### 3.3.1 이중사용방지

이 시스템은 거래코드 사용함으로써 지불정보의 이중사용 여부를 상점이 직접 확인 할 수 있도록 하였다. 다시 말해서, 상점이 직접 발행한 거래코드는 중복을 허용하지 않기 때문에 이미 사용된 거래코드가 다시 사용될 경우 상점에서 이중지불로 판단하게 된다.

#### 3.3.2 위조와 변조방지

이 시스템에서는 위조와 변조방지를 위해 브로커와 상점만이 알고있는 PassWord를 사용하여 지불정보의 무결성을 확인한다. 상점은 소비자로부터 받은 지불정보와 PassWord를 이용하여 H($T_0$, Tl, H(S#, Value, Pw))를 계산한다. 그 다음 소비자로부터 받은 H($T_0$, Tl, H(S#, Value, Pw))값과 비교하여 지불정보의 위조나 변조 여부를 판단하고, 동시에 소비자에 대한 브로커의 인증도 확인하게 된다.

#### 3.3.3 보안 및 결제

이 시스템은 거래코드나 소비자의 ID같은 중요한 정보를 전달할 경우, SSL(Secure Socket Layer)[9]을 통해 지불정보를 전송하여 보안성 보장하였다.
또한, 하루 단위로 정산을 요청하는 off-line방식의 결제를 채택하여 브로커와 상점과의 연결비용을 최소화 하였다.

#### 3.3.4 부인방지

이 시스템은 전자서명을 하는 대신에 브로커와 상점이 약속한 PassWord와 Hash를 사용하기 때문에 브로커가 인증에 대해 부인할 가능성이 있고, 상점 또한 조작된 인증을 생성할 가능성이 있다. 그러나, 브로커와 상점은 상호 신뢰를 바탕으로 연결된 거래주체이기 때문에 이러한 가능성은 배제하였다.

## 4. 결론

본 논문에서 제안한 소액지불 시스템은 기존 선불 방식이 가지고 있었던 연속거래의 문제점을 보완하여 거래 주체간의 대금 결제의 편의성을 도모하였으며, 화폐의 남용을 방지하였다. 또한, 공개키 암호화 방식을 이용한 전자서명 대신 PassWord와 Hash함수를 사용하여 전자서명에 소요되는 비용을 절약하였다. 또한, 소비자의 ID나 거래코드 같은 중요한 정보를 전송할 경우에만 SSL을 사용하기 때문에, 전달할 지불정보에 대한 암호화비용을 감소시켰다.

앞으로 이 시스템은 소액의 유료 디지털 정보서비스에 활용 될 수 있으며, 전자자금이체 방식을 이용한 양도기능의 추가가 이루어지면 실 생활의 화폐의 흐름과 매우 유사한 시스템이 될 것이다.

## 참고문헌

[1] Steve Glassman, “The Millicent Protocol for Inexpensive Electronic Commerce”,1995

[2] R.L.Rivest, “PayWord and MicroMint: Two simple micropayment schemes”, 1996

[3] Ellis Chi, “Evaluation of Micropayment Schemes”, HP Lab, technical report, 1997

[4] J.L.Abad-Peiro, “Designing a Generic Payment Service”, 1996

[5] R.L.Rivest, “The MD5 Message-digest algorithm”, RFC 1321, 1992

[6] National Institute of Standards and Technology(NIST), “Secure Hash Standard(SHS)”, 1993

[7] N.Asokan, “Electronic Payment Systems”

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

[9] D.Wagner, B.Scheiner, “Analysis of the SSL 3.0 protocol”, 1996

[10] 김창식, “Eticket:전자상거래를 위한 작고 효율적인 소액지불 시스템”, 인하대학교 석사학위논문, 2000

[11] B.Clifford Neuman and Gennady Medvinsky, “Netbill: An electronic commerce system optimized for network delivered information and services”, Proceeding of IEEE Compcon’95, March 1995