# SET 기반 초소액 지불 시스템

신준범°*, 송병렬***, 조현규***, 한상근*, 이광형**
* 한국과학기술원 수학과
** 한국과학기술원 전산학과
*** 시스템공학연구소 전자거래연구실

# Micro-Payment System based on SET

Jun Bum Shin°*, Byoung Youl Song***, Hyun Kyu Cho***, Sang Geun Hahn*, Hyung Lee Kwang**
* Department of Mathematics, KAIST
** Department of Computer Science, KAIST
*** Electronic Commerce Laboratory, SERI

## 요 약

정보화의 발전은 전자 상거래로 대표되는 사이버스페이스 상의 새로운 형태의 시장을 형성하였고, 따라서 전자 상거래를 위한 안전하면서도 효율적인 전자 지불 방식이 요구되었다. 전자 지불 방식으로는 전자 현금, SET(Secure Electronic Transaction)등과 같은 중간 이상의 금액에 사용 가능한 시스템과 PayWord 같은 작은 금액의 지불에 사용되는 초소액 지불 시스템으로 나뉜다. 본 논문에서는 여러 상점과의 거래를 효율적으로 수행할 수 있는 초소액 지불 모형을 제시하고, 이를 이용하여 SET을 기반으로 하는 초소액 지불 시스템을 제안하였다. 초소액 지불 모형에서는 사용자의 의도적인 부정 사용에 대한 효율적인 해결책을 제시함과 동시에 일회용 서명을 사용하여 공개키 서명을 사용하는 시스템에 비해 효율성을 높였다.

## 1. 서론

정보화의 진행으로 컴퓨터 네트워크가 발달하면서 디지털 데이터화된 정보의 전송을 가능하게 하여 공간상의 제약을 무너뜨리고 많은 정보를 쉽게 접할 수 있게 되었다. 이러한 편이성으로 이용하는 사람들의 증가를 가져왔고 이에 따라 전자 상거래로 대표되는 새로운 시장이 형성되게 되었다. 전자 상거래는 정보 통신망을 통하여 전자 정보를 주고 받음으로써 경제 활동을 수행하는 것을 가리킨다. 특히 월드와이드웹(World Wide Web, WWW)의 등장은 인터넷 상에서의 전자 상거래(Electronic Commerce)를 구체화 하는데 큰 기여를 했다. 사용자들에게 시각적, 청각적 데이터에 쉽게 접근할 수 있도록 해 줌으로써 상업적으로 이를 이용하려는 조직들에게 인터넷 상에 기업 홍보, 상품 홍보, 판매 등의 창구를 마련해 준 것이다.

최근 전자 상거래의 중요한 요소로 떠오르고 있는 것이 전자 지불 시스템(Electronic Payment System)이다. 상거래의 본질은 어떠한 상품이나 서비스와 그에 상응하는 경제적 가치간의 교환이다. 따라서 인터넷 상에서 교환 가능한 경제적 가치를 마련하는 것이 전자 상거래 활성화의 필수 요소이다. 하지만 전자 상거래는 실제 거래와는 거래상에서 상대방을 볼 수 없으므로 전자 지불 시스템도 이에 맞추어 개발되어야 한다.

전자 지불 시스템은 거래에 참여하는 기관들과 그들이 지불 과정에서 참여하는 방식에 따라 전자 현금, 전자 수표, 신용카드, 전자 자금 이체(EFT, electronic fund transfer)등을 기반으로 하는 기존의 전자 지불 시스템이 있으며, 또한 이들을 확장한 형태로 초소액 지불 시스템이 있다. 모든 시스템은 암호화 된 문서의 교환을 통하여 도청을 방지하며 전자 서명을 사용하여 사용자가 거래를 승인 하였다는 사실을 보일 수 있다.

현실적인 면에서 어떤 시스템의 보안이 아무리 잘 되어 있다고 하더라도 그에 소요되는 비용이 너무 크게 되면 사용할 수가 없다. 전자 지불의 경우도 마찬가지로 안일 전자 지불 시스템에서 각 거래 당 소요되는 비용이 실제적으로 구매되는 상품 가격의 특정 비율을 초과하게 되면 사용할 수 없게 된다. 기존의 전자 지불 시스템은 안전성을 위하여 비용이 많이 드는 암호 함수들(공개키 암호 알고리즘, 공개키 전자 서명 등)을 사용하였으므로 적은 금액(가령 1000 원 이하)의 지불에는 부적절 하다.

초소액 지불 시스템은 신문, 저널 등의 기사, 주식 정보와 같은 특정 서비스에 대한 요금 지불이나, 자바 애플릿등 작은 소프트웨어의 구매와 같은 아주 적은 금액의 지불을 위하여 개발된 방식이다. 일반적으로는 특정 금액(기존의 전자 지불 시스템에서 지원할 수 있는 금액)을 지불하고 적은 금액을 사용할 수 있는 쿠폰을 얻는 방식을 택한다. 현재까지 개발된 초소액 지불 시스템으로는 PayWord[10], Millicent[7], micro-iKP[6]등이 있다.

micro-iKP 의 경우는 여러 상점과 거래를 할 경우 비효율 적이며, Millicent 는 상점과의 거래를 시작할 경우 별도의 기관을 거쳐야 하며 또한 보안성이 다른 방식에 비해 떨어진다는 단점을 갖는다. PayWord 는 사용자가 신용 한도를 초과하여 사용할 경우에 대한 대책이 없다.

본 논문에서는 새로운 방식의 효율적인 초소액 지불 모형을 제시하고, 기존의 전자 지불 시스템을 초소액 지불 시스템으로 확장할 수 있는 일반적인 방법을 제시하며, VISA 가와 MasterCard 사에서 제안하였고 현재 가장 활발히 연구가 진행되고 있는 SET(Secure Electronic Transaction)[11]을 기반으로 한 초소액 지불 시스템을 제안하고자 한다. 다음 장에서는 전자 지불 시스템에서 사용되는 기본적인 암호화 함수를 정리하고, 초소액 지불 시스템의 일반적인 모형을 제시하였다. 그리고 SET 의 내용을 정리하였다. 3 장에서는 새로운 초소액 지불 모형을 제시하고, 4 장에서는 SET 을 기반으로 한 초소액 지불 시스템을 제안 및 일회용 전자 서명 방식을 제안한다. 5 장에서는 제안된 시스템의 안전성과 효율성을 다루며 마지막으로 6 장에서는 결론을 내리기로 한다.

## 2. 기존 연구

### 2.1 기본적인 암호학적 연산

- *암호 알고리즘* 암호 시스템은 크게 공개키 암호 시스템과 비밀키 암호 시스템으로 나뉜다. 비밀키 암호 시스템은 암호화 하는 키와 복호화 하는 키가 같은 암호 시스템을 말하며 공개키 암호 시스템에 비해 속도가 빠르다. DES[1]가 대표적이다. 공개키 암호 시스템은 암호화 하는 키와 복호화 하는 키가 서로 다르고 복호화 하는 키로부터 암호화 하는 키를 유추해 낼 수 없도록

만들어 진 암호 시스템이다. 때문에 복호화 하는 키를 공개할 수 있으므로 공개키 암호 시스템이라 한다. 대표적인 알고리즘으로는 RSA[9], ElGamal[4]이 있다. 문서를 암호화 하여 전달하는 경우 비밀키 알고리즘을 써서 문서를 암호화 한 다음 그 키를 공개키 암호를 사용하여 암호화 하여 전달하는 것이 일반적이다.

- *전자 서명* 서명하고자 하는 문서의 암호화 해쉬 함수를 적용하여 얻어진 값을 공개키 암호 알고리즘을 사용하여 암호화 한 것을 말한다. 인터넷 상에서는 사용자의 공개키에 CA (Certification Authority)가 서명을 하여 사용자의 공개키로부터 신원이 인증되는 방식을 택한다. RSA 서명의 경우는 공개키 암호 알고리즘과 동일한 구조를 갖으나 실질적으로는 이러한 인증 과정에서 꼭 복호화가 요구되는 것은 아니므로 사용자가 비밀키를 알고 있는지를 확인하는 방식이 사용되기도 한다. 이러한 방식으로는 DSS[2], KCDSA 등이 있다. 하지만 공개키 알고리즘을 이용한 전자 서명은 시간이 오래 걸리므로 단 한번의 서명만 요구되는 경우는 reply attack 이 적용되지 않으므로 비밀 정보를 알고 있는지를 검사하는 방식만으로 서명을 하기도 한다.
- *암호화 해쉬 함수* 충돌을 찾기 힘든(collision free)해쉬 함수를 말한다. 즉 해쉬함수 h 의 정의역에서 h(a)=h(b)를 만족하는 a,b 를 찾기가 매우 어려운 함수 h 를 가리킨다. 암호화 해쉬 함수는 전자 서명의 가장 핵심적인 요소중의 하나로써 데이터의 기밀성(integrity)을 보장한다. 암호화 해쉬 함수로는 SHS-1[3], MD5[8]등이 있다.
- *해쉬 사슬* 특정한 값을 아는지를 검사하는 방식중의 하나이며 암호화 해쉬 함수의 충돌 회피성을 바탕으로 한다. 해쉬 사슬은 임의의 값(w)으로부터 암호화 해쉬 함수를 반복적으로 적용하여 일련의 해쉬값들을 얻어냄으로써 생성된다. 길이가 N인 해쉬 사슬은 다음과 같이 구성된다.

$$w\_N = w, \qquad w\_(i-1) = h(w\_i)$$

앞으로는 이와 같이 길이가 N 이고 시작 값이 w 인 해쉬 사슬을 [w , w_0 , t, N]으로 표시하기로 한다( t = h(w_0)).

암호화 해쉬 함수를 사용했을 경우 해쉬 함수의 역함수를 구하는 것은 매우 어려운 문제이므로 사용자가 해쉬값의 역을 알고 있다는 것으로부터 사용자가 해쉬 사슬의 정보를 알고 있다고 믿는다. 암호화 해쉬 함수는 공개키 암호 알고리즘에 비해 속도가 대단히 빠르므로 우리는 이 성질을 이용하여 사용자가 비밀값을 알고 있다는 사실을 효율적으로 확인할 수 있다.

### 2.2 초소액 지불 시스템의 모형

기존의 전자 지불 방식은 큰 금액의 거래를 지원하기 때문에 매우 강력한 보안성을 요구한다. 하지만 시스템의 보안성을 높이기 위해서는 그에 소요되는 경비가 커지게 된다. 때문에 만일 기존의 전자 지불 방식을 초소액 지불 시스템과 같이 아주 작은 비용의 지불에 사용하게 된다면 지불 자체를 위한 비용이 실제 지불 비용의 특정 비율을 초과하게 되어서 효율성이 떨어지게 된다. 때문에 초소액 지불 시스템은 쿠폰을 사용하기 위한 인증서를 발급 받는 과정과 같은 큰 금액이 오가는 과정에서는 안전한 기존의 전자 지불 시스템을 사용하고 각 쿠폰의 사용과 같은 작은 금액의 거래에 있어서는 상대적으로 약한 보안성을 갖고 있지만 효율적인 구조를 사용한다. micro-iKP 에서 지원하는 하나의 상점에 대하여 초소액 지불을 하는 과정을 보면 다음과 같다.

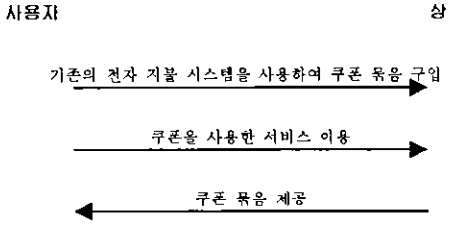


그림 1. 하나의 상점에 대한 초소액 지불 시스템

초소액 지불 시스템은 현재 우리가 사용하는 전화 카드의 경우와 비슷하다. 위의 그림과 비교해 보면 쿠폰 묶음은 전화 카드를 말하며, 전화 카드를 구입할 경우에는 현금을 지급하므로 기존의 전자 지불 시스템을 사용한다. 그리고 쿠폰을 사용하여 서비스를 용하는 것은 전화를 걸때마다 전화 카드의 남은 금액이 줄어드는 것과 같다. 보안성에 관한 측면을 보면 현금의 경우는 조폐공사만 신뢰하면 되지만 전화 카드의 경우는 전화 카드의 보안성과, 전화 서비스를 제공하는 기관을 추가적으로 신뢰해야 하며 초소액 지불 시스템 역시 마찬가지이다.

초소액 지불 시스템은 안전성과 효율성을 만족시키기 위하여 다음과 같은 성질을 만족해야 한다.

- 쿠폰의 등록 절차는 관련된 금액이 크므로 비용이 많이 들어도 보안성을 위주로 설계된 방식을 사용한다.
- 쿠폰의 사용은 관련된 금액이 작으므로 효율성을 위주로 설계된 방식을 사용한다.

그림 1 에서 나온 모형은 하나의 상점하고만 거래하는 모형이다. 하지만 대부분의 경우 사용자는 여러 개의 상점과 거래를 한다. 이 경우 각 상점마다 위의 과정을 계속 수행하는 것은 비효율 적이므로 중개인(broker)을 사용한다. 즉 중개인으로부터는 대금 지불을 통하여 쿠폰 묶음을 사용할 수 있다는 인증서를 받으며, 각 상점에게는 중개인의 인증서를 제공함으로써 쿠폰 묶음이 사용할 수 있는 것인지를 확인받는 것이다. 이 과정 까지가 그림 1 에서 나온 쿠폰 묶음을 사용하는 과정과 같으며, 실제 쿠폰을 사용하는 절차는 하나의 상점에 대해 거래하는 경우와 같다.

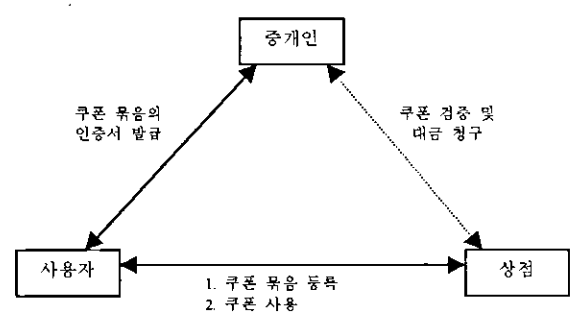


그림 2. 여러 상점에 대한 초소액 지불 시스템

중개인은 누구든지 믿을 수 있는 기관이고, 사용자는 쿠폰을 중개인을 통하여 구입함으로써 중개인에 등록된 여러 상점들에 쿠폰을 사용할 수 있게 하는 것이다.

지금까지 제안된 초소액 지불 시스템으로는 Millicent, PayWord, micro-iKP 등이 있으며 대부분의 경우 중개인이 들어간 방식을 사용하나 micro-iKP 의 경우는 중개인이 있는 방식과 없는 방식 모두를 지원한다.

### 2.3 SET

SET 은 VISA 사와 MasterCard 사에서 제안한 신용 카드 기반 전자 지불 시스템이다. SET 은 현재의 카드 회사의 기반 구조를 사용하면서도 전자 상거래를 위한 안전한 지불 방식을 제안하기 위해 개발되었다. 이 장에서는 SET 의 지불 데이터 흐름을 간략하게 기술하기로 한다.

SET 의 지불 과정은 사용자(Cardholder)와 상점(Merchant), 거래를 승인해 주는 기관(PG)으로 구성되며 각 구성원의 신원 인증을 위하여 사용하는 키에 대하여 CA(Certification Authority)의 인증서를 갖고 있다. SET 의 지불 과정을 대략적으로 기술하면 다음과 같다.

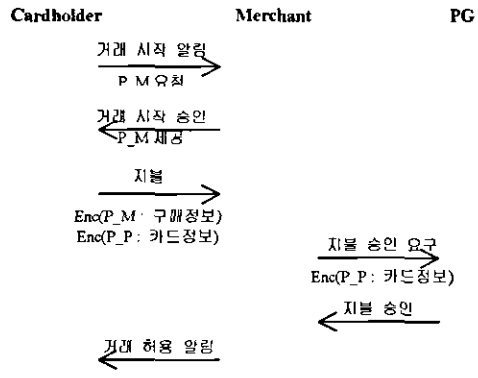


그림 3. SET 지불 데이터 흐름도

P_M, P_P는 각각 상점과 PG의 공개키이고 암호화 된 문서의 전송을 위하여 필요하다. 그리고 Enc(P_A : 문서)는 문서를 A의 공개키로 암호화 한 것을 말한다.
SET 에서는 구매 정보나 카드 정보와 같이 비밀이 요구되는 데이터는 암호화 되어서 전송되므로 거래에 참여하는 이들의 암호화 할 수 있는 키가 요구된다. SET 에서는 PG의 공개키는 알려져 있고 상점측의 공개키는 알려져 있지 않다고 가정한다. 따라서 암호화 된 문서의 전송을 위하여 사용자가 상점의 공개키 P_M을 요구함으로써 거래를 시작한다. 위의 그림을 보면 구매 정보는 상점의 공개키로 암호화 되어 상점만이 알 수 있고 카드 정보는 PG의 공개키로 암호화 되어 PG만이 알 수 있다는 것을 알 수 있다. 그리고 위의 그림에는 빠져 있지만 SET 에서는 지불 과정에서 이중 서명(dual signature)를 사용하여 구매 정보와 카드 정보가 연관성을 갖고 있다는 것을 확인할 수 있게 하였다. SET 에 관한 자세한 내용은 [11]를 참조 바란다.

### 3. 초소액 지불 시스템 제안 모형

초소액 지불 시스템은 지불 하는데 드는 비용이 적으면서 안전해야 한다. 본 논문에서는 이 조건들을 모두 충족시키면서 보다 효율적으로 여러 상점과의 거래를 가능하게 하기 위한 초소액 지불 시스템을 제안하고자 한다.
2.2 에서 보았듯이 중개자가 들어간 초소액 지불 시스템을 4 단계의 구조를 갖는다.

- 사용자는 중개자에게 대금 지불을 통하여 쿠폰 묶음에 대한 인증서 발급 받음.
- 사용자는 상점에게 쿠폰을 등록하기 위하여 쿠폰 묶음의 인증서를 제공함.
- 사용자는 상점에게 쿠폰을 사용하여 서비스 제공 받음.
- 상점은 중개자에게 대금 지불 요구.

제안하는 시스템 역시 기본 구조는 위와 같고 인증서(Cert)의 구조 및, 등록 절차를 바꿈으로써 여러 상점과의 거래를 용이하게 하고자 한다. Cert를 받는 과정은 기존의 전자 지불 방식을 사용하는 것이 가능하기 때문에 이 장에서는 Cert를 받았다는 가정하에서 쿠폰을 사용하는 방식을 다룬다. 본 논문에서 사용하는 SET을 기반으로 Cert를 받는 과정은 다음 장을 참조 바란다.

우선 Cert 데이터 구조를 보기로 한다.
*만일 k 개의 상점을 이용한다면 k 개의 해쉬 사슬이 필요하다.*
**w1** = [w1, w1_0, t1, N], **w2** = [w2, w2_0, t2, N],..., **wk** = [wk, wk_0, tk, N]

그렇다면 중개자의 비밀키가 S_B라고 할 때 Cert는 다음과 같다.

coupon_info = [ UID, MAX, expi, t1, t2,..., tk, AUX ]
Cert = Sign( S_B : coupon_info )

위에서 UID는 사용자의 신원이고, MAX는 Cert를 이용하여 지불 가능한 총 금액이며, expi는 Cert를 사용할 수 있는 기간이다. 그리고 AUX는 지불과 관련된 보조적인 정보를 가르킨다. 따라서 Cert는 지불과 관련된 정보인 coupon_info를 중개자가 자신의 비밀키를 이용하여 서명한 값이다.
중개자로부터 Cert를 받아 왔다는 가정 하에서 상점에 대하여 쿠폰을 등록하는 과정은 다음과 같다. 해쉬 사슬 **w2** = [w2, w2_0, t2, N]를 사용한다고 하자.

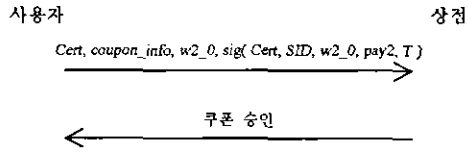


그림 4. 쿠폰 묶음 등록 과정

SID는 중개자에 대한 상점 고유 번호이며 pay2는 해쉬 사슬 **w2** = [w2, w2_0, t2, N]를 사용하여 상점에게 지불할 금액이다. 그리고 sig( Cert, SID, w2_0, pay2, time )는 상점에게 지불하게 될 금액에 대한 사용자의 서명인데 공개키 암호를 사용하여 생성하여도 되나 본 논문에서는 효율성을 위하여 암호화 해쉬 함수를 사용한 일회용 서명을 이용한다. 이에 대한 자세한 내용은 다음 장을 참조 바란다.

상점은 사용자의 쿠폰 묶음을 검증하기 위하여 다음의 순서를 거친다. 우선 Cert로부터 중개자의 서명이 올바른 것인지를 검사하며, 유효 기간이 합당한지를 검사한다. 또한 실제 사용자가 사용하는지를 알기 위해서 t2 = h (w2_0)가 맞는지를 검사한다. 만일 맞다면 암호화 해쉬 함수의 역값을 아는 것은 매우 어려우므로 상점은 올바른 사용자가 사용한다고 생각한다. 그리고 거래 가능 금액의 설정을 위하여 pay2가 MAX를 넘지 않는지 여부를 검사한다. 상점은 중개자의 서명을 통하여 MAX 까지의 거래 가능성을 보증받게 된다. 나중에 중개자는 발행된 Cert에 대하여 pay들의 합이 MAX를 넘는지 여부를 검사하게 된다.
실제 쿠폰 사용에 있어서는 해쉬 사슬의 역 값을 차례대로 공개하는 방식을 사용한다. 지금까지 쿠폰을 r개 사용하였고 1개의 쿠폰에 해당하는 금액을 지불하려 한다면 w2_(r+1)을 상점에게 제공하면 된다. 해쉬 사슬 **w2**에 대한 정보는 상점에서 관리하므로 역시 도청에 대하여 안전하다.
각 해쉬 사슬을 사용하는 규칙은 다음과 같다.

- 하나의 해쉬 사슬은 한 상점에 대해서만 사용할 수 있다. (추가적인 거래의 성립을 위하여 두개의 해쉬 사슬을 한 상점에서 사용하는 것은 가능하다.)
- 해쉬 사슬 **w1, w2,..., wk** 을 이용하여 지불한 금액인 pay1, pay2,...,payk 의 합은 MAX를 넘지 않아야 한다.

사용자가 만일 이 규칙을 어긴다면 상점이 중재자에게 지불을 요구하는 과정에서 사용자의 부정 사용이 밝혀지게 된다.
상점은 사용자의 쿠폰 묶음 등록이 끝나면 중개자에게 대금 지불을 요구할 수 있다. 상점이 중개자에게 건네어 주는 데이터는 다음과 같다.

Cert, UID, t2_0, pay2, time, sig( Cert, SID, t2_0, pay2, time )

중개인은 이 데이터를 받아 사용자의 서명이 올바른지를 확인하고, 지금까지 지불 요구된 pay들의 합이 MAX를 넘지 않는지를 검사한다. 만일 넘는다면 중개인은 부정 사용으로 인정하고 사용자를 부정 사용으로 고발한다.
위와 같은 지불방식은 상점이 중개인에게 대금 지불을 요구하는 과정이 반드시 실시간으로 일어날 필요가 없으므로 중개인의 병목 현상을 방지할 수 있다. 또한 쿠폰을 다 사용하지 않은 상태(상점은 하루 이내에 대금 지불을 요구하게 됨)에서 상점이 중개자에게 대금 지불을 요구하기 때문에 사용자의 의도적인 부정 사용에 대한 효과적인 적발이 가능하다.

#### 4. SET 기반 초소액 지불 시스템

3 장에서 기술한 쿠폰을 지불 방식은 대부분의 기존의 전자 지불 시스템에 적용이 가능하다. 이장에서는 SET을 기반으로 쿠폰에 대한 인증서를 획득하는 방식 및 암호화 해쉬 함수를 사용하여 사용자가 자신의 서명을 생성할 수 있는 방식을 다루기로 한다.

SET을 통한 쿠폰의 인증서를 획득을 위해서는 SET을 통하여 중개자에게 금액의 지불을 하고, 추가의 데이터(coupon_info)에 중개자의 서명을 얻는다. 이때 coupon_info 은 구매 정보와 같이 연결되어 전달되어지고 SET 에서 구매 정보는 중개자의 공개키로 암호화 되어 전달되므로 coupon_info 은 안전하게 중개자에게 전달될 수 있다. coupon_info 의 데이터 구성은 다음과 같다(앞장에서 기술한 바와 같이 사용 가능한 금액은 MAX 이고, k 개의 해쉬 사슬을 얻는 과정이다). coupon_info 에 대한 중개자의 서명인 Cert 는 거래 허용 알림과 같이 사용자에게 전달된다. 이 데이터 역시 SET 에서는 암호화 하여 보내므로 사용자에게 안전하게 전달될 수 있다. 그리고 중개자는 Cert 와 coupon_info 를 저장한다.

실질적으로 SET 에서 보조적인 데이터의 전송을 허용하므로 중재자에게 Cert 를 얻는 과정에서 중개자가 Cert 를 계산하는 것을 제외하고는 SET 을 그대로 사용하게 된다. 또한 전송되는 모든 데이터가 SET 의 데이터와 같은 방식으로 전송되므로 안전하다.

제안하는 시스템은 지불하는데 필요한 비용을 줄이기 위하여 공개키 서명이 아닌 해쉬 함수를 사용한 일회용 전자 서명 방식을 사용한다. 그리고 서명은 상점이 검사하는 방식이 아닌 중개자가 검사하는 방식을 택한다. w2 에 대한 사용자의 서명은 다음과 같으며 상점에게 지불할 금액인 pay2 에 대한 서명이다(T 는 time-stamp 이다).

$$sig(Cert, SID, w2\_0, pay2, T) = h(Cert, SID, w2\_0, pay2, s2, T)$$
$$s2 = h(s, w2\_0, T)$$

위에서 s 는 사용자의 비밀정보로서 사용자와 중재자만이 아는 값이다. 중개자가 서명을 확인하기 위해서는 우선 소비자가 상점에게 쿠폰을 등록한 시점인 T 가 Cert 를 받을 때의 expi 를 넘지 않는지를 검사한다. 만일 올바른 거래라면 상점의 신원으로부터 SID 값을 얻고, 소비자의 신원(UID)으로부터 s 값을 얻어 s2 를 계산한다. 그 다음에 상점이 보내준 정보로부터 나머지 값을 얻은 다음에 해쉬 함수값을 계산한다. 만일 이 값이 sig( Cert, SID, w2_0, pay2, T )와 같다면 서명이 성립하는 것이고 중개자는 Cert 에 대하여 pay2 의 금액이 추가로 쓰여 졌음을 기록한다. 만일 값이 틀린다면 사용자 또는 상점이 서명의 내용을 조작한 것이 된다. 이 경우 중개자는 상점과 소비자를 조사하여 누가 조작을 했는지를 검사한다.

각 쿠폰을 사용하는 방식은 앞장에서 기술한 방식과 같다.

#### 5. 안전성 및 효율성

본 논문에서는 SET 의 확장형으로써의 초소액 지불 시스템을 소개하였다. 즉 쿠폰 묶음을 구입하는 절차에서 SET 를 사용하였고 쿠폰을 개별적으로 사용하는 방식은 여러 상점과의 거래를 지원하기 위해 별도의 기관인 중개자를 사용하는 방식의 새로이 개발된 방식을 적용하였다.

보안성 측면에서 보면 쿠폰 묶음을 구입하는 것과 같은 많은 금액의 거래가 따르는 것은 SET 을 통해 전달되게 하여 SET 데이터와 동일한 레벨의 보안성을 갖고, 적은 금액의 거래인 쿠폰을 사용하는 과정은 해쉬 사슬을 사용함으로써 보안성을 얻었다. 시스템 전반적인 면에서 중개자라는 추가적인 신뢰해야만 하는 기관을 넣었기 때문에 보안성은 SET 자체에 비해 상대적으로 떨어지나 만일 중개자가 올바르게만 작동 한다면 상대적으로 높은 레벨의 보안성을 얻을 수 있다.

그리고, 본 논문에서는 사용자의 서명에 있어 암호화 해쉬 함수를 사용한 일회용 전자 서명 방식을 사용하기 때문에 보다 효율적인 서명 방식을 제공하였다.

또한 기존의 초소액 지불 시스템과는 다르게 선불 카드 방식으로 대금의 지불이 이루어 지므로 사용자가 같은 해쉬 사슬을 여러 번 사용하거나 사용 금액을 넘어 사용하는 것처럼 의도적인 불법 행위를 할 경우도 적발이 용이하고 또한 블랙 리스트를 만들어 상점에 배포함으로써 추가적인 불법 행위를 막을 수 있다.

지금까지 제안되었던 초소액 지불 시스템과의 비교는 다음과 같다. (k 개의 상점과 거래를 한다.)

| | 제안 프로토콜 | Millicent | PayWord | micro-iKP broker | micro-iKP no broker |
|---|---|---|---|---|---|
| 기존지불시스템 사용 횟수 | 1 | 1 | 1 | 1 | k |
| 사용자의 공개키서명 생성 횟수 | 0 | 0 | k | 1 | k |
| 상점의공개키 서명확인 횟수 | k | 0 | 2k | 0 | 2k |
| 중개자 접속 횟수 | 0 | k | 0 | 쿠폰사용 횟수 | 0 |
| 상점의 위조 가능성 | 없음 | 있음 | 없음 | 없음 | 없음 |
| 사용자의 부정사용 검사 | 블랙리스트 생성 관리 | 부정사용 없음 | 신용한도 초과 위험성 | 부정사용 없음 | 부정사용 없음 |
| 중개자의 병목현상 | 없음 | 있음 | 없음 | 매우심함 | 없음 |
| 보안성 | 보통 | 낮음 | 보통 | 보통 | 높음 |

표 1. 기존의 초소액 지불 시스템과의 비교

#### 6. 결론

본 논문에서는 대부분의 기존의 전자 지불 시스템에 적용이 가능한 초소액 지불 모형을 제시하였고, 그것의 구체적인 형태로서 SET 의 확장형으로서의 초소액 지불 시스템을 제시하였다. 초소액 지불 모형은 특히 일회용 전자 서명의 사용으로 인하여 기존의 공개키 서명 방식에 비하여 효율성을 높였고, 선불 카드 형태를 사용함으로써 사용자의 의도적인 불법 사용에 대하여 효율적인 해결 방안을 제시하였다.

## Reference


[1] National Institute for Standard and Techonology (NIST), Data Encryption Standard (DES), *FIPS 46-2*, Dec 1993

[2] National Institute for Standard and Techonology(NIST), Digital Signature Standard (DSS), *FIPS 186*, Nov 1994,

[3] National Institute for Standard and Techonology (NIST), Secure Hash Standard (SHS), *FIPS 180-1*, Apr 1995

[4] T. ElGamal, "A Public-Key Cryptosystem and a Signature Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, v. IT-31, n. 4, 1985, pp. 469-472

[5] N. M. Haller. "The S/KEY one-time password system," *In ISOC*, 1994

[6] R. Hauser, M. Steiner and M. Waidner "Micro-payment based on iKP" Aug. 1996. http://www.zurich.ibm.com:80/Techonology/Security/publications/1996/HSW96.ps.gz

[7] S. G. Mark and S. Manasse, " The millicent protocols for inexpensive electronic commerce," *in 4-th International World Wide Web Conference*, Dec. 1995.

[8] R. L. Rivest, "The MD5 message-digest algorithm." Internet Request for Comments, Apr. 1992. RFC 1321

[9] R. L. Rivest, A. Shamir and L. M. Adleman, " A Method for Obtaining Digital Signature and Public Key Cryptosystems," *Communications of the ACM*, v. 21, n. 2, Feb. 1978, pp. 120-126

[10] R. L. Rivest and Adi Shamir. "PayWord and MicroMint : Two simple micropayment schemes," May. 1996

[11] Secure Electronic Transaction(SET) Specification. book. 1 : Business Description May. 1997 http://www.visa.com/sf/set/set_bk1.pdf