분할성과 부분적인 추적이 가능한 효율적인 전자 지불 시스템에 관한 연구

김해만°, 이임영
순천향대학교 공과대학 컴퓨터학부

A Study on efficient electronic payment system with divisibility and limited traceability

Hae-Man Kim°, Im-Yeong Lee
Department of Computer Science, College of Engineering,
Soonchungyang University

요 약

초기의 전자 지불 시스템은 안전성과 사용자의 익명성이 주요 관심사였다. 하지만 최근에는 그러한 안전성과 익명성 뿐만 아니라 전자화폐의 분할성과 불법적인 사용자에 대한 부분적인 추적성이 커다란 관심사가 되고 있다. 본 논문에서는 전자화폐의 분할성을 기존의 이진 트리 구조를 이용한 방식과 다른 방식으로 해결함으로써 보다 간단하고 효율적인 방법을 제시하고 부분적인 추적성을 가질 수 있는 방식을 제안하도록 한다.

1. 서론

컴퓨터 보급 확산과 네트워크를 이용한 컴퓨터 통신의 발달로 인터넷 사용자가 전세계적으로 급증함에 따라 이를 상업적으로 이용하기 위한 시도가 증가하고 있다. 그 중에서 많은 주목을 받고 있는 분야가 바로 전자상거래(Electronic Commerce)이다.[6]

전자상거래는 지불 방식에 따라 크게 지불브로커 시스템과 전자화폐 시스템으로 나눌 수 있다. 지불브로커 시스템은 독립적인 신용구조를 가지지 않고 신용카드나 은행이 계좌를 이용해 네트워크상에서 지불을 하는 방식이다. 따라서 물품 구입시 브로커의 거래 승인을 거친 후 거래가 이루어지게 된다. 전자화폐 시스템은 독립적인 신용구조를 가지고 있어서 물품 구입시 은행이나 카드 발행사로부터의 거래 승인이 필요없다. 전자화폐 시스템은 플라스틱 카드 위에 부착된 IC칩을 이용해 오프라인 대금결재에 활용하는 IC카드형 전자화폐와 화폐가치를 디지털 정보의 형태로 발행하여 네트워크를 통한 온라인 대금결재를 가능하도록 한 Network형 전자화폐로 나눌 수 있다.

현재 이루어지는 전자상거래를 살펴보면 신용카드를 이용한 브로커 시스템이 많이 사용되어지고 있다. 이미 신용카드는 널리 사용되어지고 있고 이를 이용한 전자상거래의 구축이 용이하기 때문이다. 대표적인 것으로 널리 알려진 SET이 있다.

하지만 현금을 대신할 수 있는 진정한 전자상거래는 전자화폐 시스템이라고 할 수 있다. 이는 전자상거래의 궁극적인 목표 시스템이다.

아직까지 폭넓게 사용되고 있지 않지만 이에 대한 연구와 개발이 활발하게 이루어지고 있다.

초기에는 사용자의 부정한 전자화폐 사용 방지, 제3자의 부정한 개입 방지 등 안전성에 대한 문제와 사용자의 프라이버시를 위한 익명성 문제가 주요 관심사가 되었다.

최근에는 안전성과 익명성 뿐만 아니라 전자화폐에 대한 분할성[1][2]과 부분적인 추적성[3]에 대한 연

구가 활발히 이루어지고 있다.

전자화폐의 분할성은 사용자가 편리하게 사용할 수 있도록 한다. 만약 분할성이 제공되지 않는다면 사용자는 전자화폐를 사용할 때마다 해당 금액에 맞는 전자화폐를 발행 받거나, 해당 금액에 맞게 지불할 수 있도록 다양한 금액의 전자화폐를 미리 인출하고 저장하여야 할 것이다. 또는 상점측에서 거스름돈에 해당하는 전자화폐를 주는 방법도 생각해 볼 수 있을 것이다. 하지만 이는 모두 비효율적이고 불편함을 초래한다. 따라서 전자화폐의 분할성 제공은 매우 중요하다.

초기에 중요한 관심사였던 개인의 프라이버시를 위한 익명성은 새로운 문제를 발생시켰다. 왜냐 하면 돈세탁 등과 같은 불법적인 사용자에 대한 추적이 불가능하기 때문이다. 이와 같은 문제점을 해결하기 위해 제안된 것이 부분적인 추적이 가능한 방식이다. 따라서 정당한 사용자에 대한 익명성은 보장해주고 불법적인 사용자에 대해서는 법원 등의 허가를 통하여 사용자의 신원을 추적할 수 있게 된다.

전자화폐의 분할성에 대한 논문이 많이 나와 있는데 대부분 이진 트리 구조를 이용한 방식이다. 이 방식은 수학적으로 상당히 복잡한 과정을 거치게 된다.

본 제안 방식에서는 기존의 이진 트리 구조를 이용한 방식이 아닌 소액 지불을 위해 제안되었던 MPTP[4]를 응용하여 분할성 문제를 해결하였다. 이 방식은 매우 간단히 분할성 문제를 해결해준다. 또한 신뢰기관인 CA를 통하여 익명성과 부분적인 추적성을 제공함으로써 보다 안전하고 효율적인 전자지불 시스템을 제안하였다.

본 논문의 구성을 살펴보면 우선 2장에서는 본 논문에서 응용한 방식인 MPTP에 대하여 간단히 살펴보고, 3장에서는 이를 응용한 제안 방식을 기술하고, 4장에서는 제안 방식에 대한 안전성을 분석하였다.

2. MPTP
(Micro Payment Transfer Protocol)

MPTP는 1995년에 소액거래를 위해 제안된 W3C working draft이다. 소액거래를 위해서는 최소한의 안전성을 유지하고 처리 비용을 최대한 낮추는 것이 중요하다.

2.1 지불 메커니즘

가. 구성요소

참여하는 주체는 broker, vendor, customer로 구성되어 있다. Broker는 사용자 인증과 계정을 관리하고, vendor는 정보나 서비스를 제공하고, customer는 적당한 token을 생성해서 상품 구입을 한다.

나. 지불 명령

지불 명령은 크게 지불 authority와 지불 token으로 나누어지는데 지불 authority는 지불에 필요한 paychain_root 값, 식별자 등 지불에 필요한 정보를 디지털 서명한다. 지불 token은 연쇄 해쉬 함수를 이용하여 금액을 결정한다.

여기에서 연쇄 해쉬 함수란 token을 인증하기 위해 사용되는데, 우선 customer는 랜덤한 w_n 값을 선택한다. 그리고나서 w_i = h(w_i+1)를 계산함으로써 일련의 지불 토큰(paychain) w_0, w_1, · · ·, w_n을 계산한다. 이 때, 금액은 해쉬 횟수에 의해서 결정된다.

여기서 paychain을 생성하는 최초의 root값(w_0)을 paychain_root라고 한다. h는 암호학적으로 안전한 MD5와 같은 one way 해쉬 함수를 나타낸다.

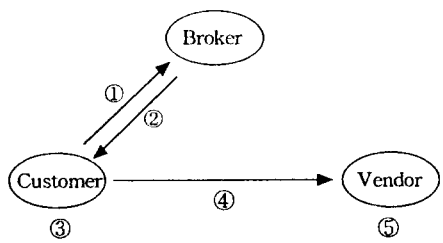
2.2 Payment Flow

지불 처리는 크게 Session Establishment(세션 설정) 단계와 Payment Transfer(지불 전송) 단계로 나눌 수 있다.

가. Session Establishment

세션 설정 단계는 지불 처리를 하기 위해 미리 지불 처리에 필요한 정보(authority, 계정 확인서)를 broker, customer, vendor가 서로 주고받는 단계이다.

이 단계는 거래를 하기 전에 한번만 수행을 하고 그 후에는 이 정보를 기반으로 계속적인 지불을 수행할 수 있다.



[그림1] MPTP 세션 설정 과정

- ①, ② 단계
  - Customer는 broker에게 계정 확인서를 요구하고 계정 확인서를 받는 단계
  - 만약 broker가 공개키를 서명을 사용하여 계정 확인서를 생성하면, vendor는 broker의 서명을 확인함으로써 계정 확인서를 인증
  - 만약 broker가 대칭키 서명을 사용할 경우 vendor는 broker에게 계정 조회를 의뢰
- ③ 단계
  - Customer가 authority를 생성하는 단계
  - Authority는 authority를 인증할 수 있는 정보와 paychain을 생성할 수 있는 정보를 포함.
- ④ 단계
  - Customer는 authority에 서명을 해서 계정 확인서와 함께 안전하게 vendor에게 전송한다.
- ⑤ 단계
  - Vendor는 전송받은 authority와 계정 확인서를 점검하는 단계이다.
  - 점검 단계는 다음과 같다.

i) authority 유효기간 점검
ii) 이중사용여부 점검 (authority_id 점검)
iii) authority_id 추가
iv) 계정 확인서의 서명 확인
v) authority의 서명 확인
vi) authority를 online 파일에 추가

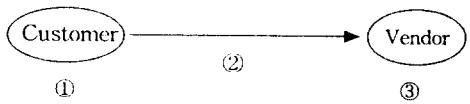
나. Payment Transfer

지불 전송하는 단계로써 세션 설정이 이루어진 후에는 계속해서 지불 처리를 할 수 있다.

Customer는 vendor에 접속해서 원하는 상품을 선택한 후에 그 상품 금액에 해당하는 token을 생성하여 charge 메시지를 만든 후에 이것을 vendor에게 전송하고 상품을 전송 받는다.

Vendor는 이 메시지를 broker에게 전송하고 자신의 계정에 입금을 요구하면 broker는 유효성을 확인한 후 customer의 계정에서 vendor의 계정으로 입금을 한다.

이 과정을 단계별로 살펴보면 다음과 같다.



[그림2] 지불 전송 과정

- ① 단계
  - Customer는 charge 메시지를 준비하는 단계
  - 금액을 결정할 수 있는 authority_id와 payword 등의 정보를 포함
  - Vendor_id와 일치하는 authority 정보를 검색해서 해당 vendor에 맞는 paychain_root값을 적절한 횟수만큼 연쇄 해쉬함으로써 요구된 금액과 일치하는 payword를 결정
- ② 단계
  - Charge 메시지를 전송
- ③ 단계
  - Charge 메시지를 점검하는 단계
  - Authority_id를 이용해서 해당 paychain_root를 선택한 후, 이것을 사용하여 연쇄 해쉬 함수를 수행함으로써 payword를 확인한 후 세션 레코드에 payword정보와 증가량을 갱신

2.3 기존 방식 분석

동전을 생성할 수 있는 정보(paychain_root)는 안전한 서명 방식으로 설정되어지기 때문에, 그 정보를 모르는 제 3자는 부정한 동전을 생성할 수 없고 유일한 authority 식별자의 점검으로 이중사용 방지할 수 있다. 또한 customer가 거래 금액에 맞는 동전을 생성하므로 broker의 부하가 감소하고, vendor의 거스름돈이 필요 없다는 장점이 있다.

반면에 MPTP는 다음과 같은 문제점이 있다.

- 익명성이 보장되지 않는다.
- Customer의 신용이 필요하다. (후불 방식)
- Vendor의 부정한 동전 생성 가능하다.

3. 새로운 전자 지불 시스템

기존의 MPTP 방식은 소액거래를 위한 방식으로 높은 안전성을 제공하지 못한다. 본 제안 방식에서는 처리비용이 다소 높아지더라도 익명성과 vendor의 부정한 token 생성을 방지함으로써 안전성을 높여 고액 지불에 적합하도록 하였다.

또한 후불방식이 아닌 선불방식으로 바꿈으로써 customer의 신용이 문제가 되지 않도록 하였다.

3.1 지불 메커니즘

가. 구성요소

참여하는 주체는 앞에서 설명한 broker, vendor, customer와 익명성과 부분적인 추적성을 제공하기

위한 인증 기관인 CA로 구성되어진다.

나. Paychain의 생성 방법

기본적으로 paychain을 구성하는 방식은 MPTP의 방식과 동일하게 paychain_root을 해당 금액만큼 연쇄 해쉬를 함으로써 얻어진다.

다. Paychain_root 값 생성 방법

기존의 방식에서는 customer가 해당 vendor에 대한 paychain_root 값을 생성하고 이를 Session Establishment 단계를 통하여 설정을 하게 되는데 이는 다수의 customer가 다수의 vendor와 거래를 할 때 비효율적이다. 따라서 이를 효율적으로 처리하기 위해 본 제안 방식에서는 Diffie-Hellman의 키 교환 방식을 이용하여 paychain_root 값을 결정한다. 이 방식의 절차는 다음과 같다.

(1) customer와 vendor들은 각각의 비밀값 c_i 와 v_i를 생성한다. 이 때 g^{c_i}와 g^{v_i}는 공개값이 된다.

(2) 각각의 customer와 vendor 사이에 교환된 비밀키가 paychain_root 값이 된다.

$$paychain\_root = g^{c_i v_i}$$

라. 금액 결정 방법

본 제안 방식에서는 선불 방식으로 처리하기 위해 customer는 먼저 broker에게 지불을 하고 해당 금액에 맞는 금액 생성 범위 인증서를 받는다.

여기서 금액 생성 범위 인증서는 지불된 금액에 해당하는 각 금액 단위별의 생성 범위를 인증하게 되며, 형식은 다음과 같다.

$$S_B(M_L\_K \parallel PID \parallel SN)$$

PID는 customer의 Pseudo_ID이고 SN은 Serial Number로써 이 인증서의 부정한 사용을 막기 위해 사용되어진다.

간단한 사용 예를 살펴보면 다음과 같다.

ex) $S_B(M_1\_5000 \parallel M_{10}\_1000 \parallel M_{100}\_800 \parallel M_{1000}\_50 \parallel M_{10000}\_10 \parallel PID \parallel SN)$

- 1단위는 5000회(5,000원)까지 사용 가능
- 10단위는 1000회(10,000원)까지 사용 가능
- 100단위는 800회(80,000원)까지 사용 가능
- 1000단위는 50회(50,000원)까지 사용 가능
- 10000단위는 10회(100,000원)까지 사용 가능

다. Token의 구조

PID	payword · · ·	금액단위 · · ·	props	⇒token_body
h(token_body ‖ secret_key_C)				⇒certificate

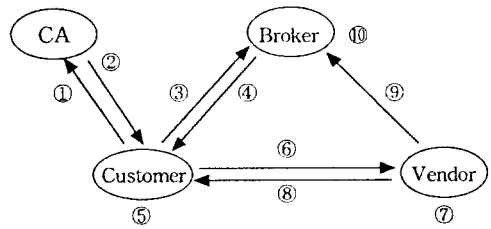
· token_body
- PID : customer의 Pseudo_ID
- payword : paychain_root를 해당 금액만큼 해쉬한 값
- 금액 단위 : payword가 의미하는 금액 단위 결정
- props : 기타 데이터

· certificate
: token_body와 secret_key_C를 해쉬하여 생성

ex) 20,430원을 생성할 경우

PID	payword	금액 단위	props
hae	M_2	10,000	
	M_4	100	
	M_3	10	
h(token_body ‖ secret_key_C)			

3.2 지불 프로토콜



[그림3] 제안 방식 프로토콜

- ① 단계 (PID와 공개값 인증서 요구)
· customer는 자신의 비밀값 c를 생성
· CA에게 자신의 신원정보와 공개값 g^c를 전송

customer —— customer_ID, g^c ——▶ CA

- ② 단계 (PID와 공개값 인증서 전송)
  · CA는 customer_ID에 대응하는 PID(Pseudo_ID)를 생성 후 DB에 저장
  · customer에게 PID와 공개값 인증서 $S_{CA}(PID \| g^c)$를 전송

$$CA \xrightarrow{PID,\ S_{CA}(PID \| g^c)} customer$$

- ③ 단계 (금액생성범위 인증서 요구)
  · customer는 온라인 입금 등의 방법으로 금액을 지불(선불 방식)
  · customer는 지불된 금액에 맞게 전자화폐를 사용하기 위한 각각 금액 단위별의 지불생성범위 결정한 후 PID와 자신이 생성한 비밀값 c와 함께 금액생성범위 인증서를 요구하는 request문 전송

$$customer \xrightarrow{E_B(PID \| secret\_key\_c),\ request} broker$$

- ④ 단계 (금액생성범위 인증서 전송)
  · ③ 단계에서의 입금과 request를 확인
  · customer로부터 받은 PID와 secret_key_c를 DB에 저장
  · broker는 금액생성범위 인증서를 전송

$$broker \xrightarrow{S_B(M_i\_K \| PID \| SN)} customer$$

- ⑤ 단계 (token 생성)
  · broker로부터 받은 금액생성범위 인증서를 확인
  · customer는 vendor의 접속하여 원하는 상품을 선택한 후 해당 금액에 맞는 token 생성 (paychain_root값은 해당 vendor의 공개값 g^v와 자신의 비밀값 c 로 생성된 g^{cv})

- ⑥ 단계 (구매 요구)
  · customer는 원하는 상품정보(상품명, 상품 가격 등)와 token, 공개값 인증서, 금액생성범위 인증서 등을 vendor에게 전송하므로써 구매를 요구

$$customer \xrightarrow{Ev[상품정보 \| S_{CA}(PID \| g^c) \| token \| S_B(M_i\_K \| PID \| SN)]} vendor$$

- ⑦ 단계 (verify)
  · vendor가 ⑥ 단계에서 받은 정보를 확인
    1) vendor는 공개값 인증서 $S_{CA}(PID \| g^c)$를 확인한 후 g^c와 자신의 비밀값 v를 이용하여 paychain_root 값 결정
    $$paychain\_root = g^{cv}$$
    2) 계산된 paychain_root 값으로부터 token을 검사함으로써 생성금액이 맞는지를 검사

- ⑧ 단계 (상품 전송)
  · ⑦ 단계에서 인증이 올바르다면 vendor는 cutomer에게 해당 상품을 전송한다.

$$broker \xrightarrow{상품\ 전송} customer$$

- ⑨ 단계 (token 반환)
  · vendor는 자신이 받은 token을 자신의 계좌에 예치하기 위해 token값과 자신의 ID를 전송

$$vendor \xrightarrow{E_B(token \| vendor\_ID)} broker$$

- ⑩ 단계 (token 확인 후 인출)
  · 해당 PID의 secret_key_C로 token_body와 해쉬함으로써 token의 certificate 확인
  · vendor의 공개값 g^v와 secret_key_c로 계산되어지는 paychain_root 값으로 금액 검사
  · hash_count가 인증된 금액생성범위를 만족하는지 검사 후 DB의 hash_count 갱신
  · 모든 인증이 올바르다면 해당 금액을 vendor의 계정에 예치

4. 제안 방식 분석

4.1 안전성 분석

가. customer의 부정한 사용 방지

본 방식에서 customer가 부정하게 사용하는 경우는 구입할 상품 금액과 다른 값을 사용하는 경우와 자신에게 주어진 금액생성범위를 초과해서 사용하는 경우를 생각할 수 있다.

첫번째 경우는 vendor에서 동일한 paycain_root 값으로 해당 금액만큼 해쉬하여 금액이 맞는지 확인함으로써 발견이 가능하다.

두번째 경우는 broker에서 customer가 얼마만큼

사용했는지를 나타내는 각 금액 단위의 hash_count를 저장하여 관리하고 금액생성범위 인증서와 비교함으로써 customer의 부당한 사용을 발견하게 된다.

나. vendor의 부정한 사용 방지

vendor는 paychain_root값은 알지만 customer와 broker가 공유하고 있는 secret_key_C값을 모르므로 token의 certificate부분을 올바르게 생성할 수 없다. 따라서 부정한 token의 생성이 불가능하다.

다. 제3자의 부정한 사용 방지

제3자는 customer의 비밀값 c나 vendor의 비밀값 v는 통신상에서 전혀 나타나지 않으므로 그 값을 알 수 없다. 따라서 paychain_root 값을 알아낼 수 없으므로 제3자가 부정한 token을 만드는 것은 불가능하다.

라. 익명성 및 부분적인 추적성 부여

본 제안 방식에서는 CA를 통하여 자신의 신원정보와 연결될 수 있는 PID(Pseudo_ID)를 받아서 사용함으로써 익명성이 부여된다. CA는 단지 customer의 신원정보와 PID를 연결할 수 있는 정보를 가지고 있고, broker는 PID와 그에 대한 token의 정보를 가지고 있다. 따라서 그들 각각은 token의 실제 사용자가 누구인지는 알지 못한다.

하지만 만약 customer가 불법적인 사용을 했을 경우 CA와 broker는 서로의 데이터로 불법적인 token의 사용자 신원을 추적할 수 있다.

4.2 효율성 분석

분할성에 대한 기존의 대부분의 논문에서 언급되어진 이진 트리 구조를 이용한 방식은 token 생성 방법이나 검증하는 과정이 수학적으로 상당히 복잡하게 구성되어져 있다. 하지만 제안 방식에서는 단지 customer가 해당 금액만큼 해쉬를 하면 되기 때문에 매우 간명하게 처리되어진다. 또한 해쉬 함수는 처리 속도가 빠르기 때문에 기존의 방식보다 훨씬 빠른 처리가 가능하다.

4. 결 론

현재 전자상거래는 많은 곳에서 주목받고 있다. 아직까지는 신용카드에 기반한 지불 브로커 시스템에 비하여 전자화폐 시스템이 활성화되지 않고 있지만, 전자상거래를 위한 궁극적인 목표 시스템은 전자화폐 시스템이다.

전자화폐 시스템은 계속해서 연구, 개발되고 있는 단계인데 최근에 관심의 대상이 되고 있는 분할성과 부분적인 추적성에 대하여 기존의 접근 방식과 다른 새로운 방식을 제안하여 효율성을 높이고자 했다.

제안한 프로토콜은 복잡한 수식이 없는 간명한 방식으로 실제로 구현이 용이할 뿐만 아니라 빠른 처리 속도를 기대할 수 있다.

머지않아 다가올 본격적인 전자상거래 시대는 국경 없는 경쟁을 가져올 것이다.

이러한 경쟁에서 뒤처지지 않기 위해서는 이에 대한 지속적인 관심과 연구가 필요할 것이다.

[본 연구는 한국과학재단 특정기초연구과제 (과제번호 : 97-01-00-06-01-3) 연구비 지원에 의해 수행되었음]

<참고 문헌>

[1] Tatsuaki Okamoto, "An Efficient Divisible Electronic Cash Scheme", Advances in Cryptology-CRYPTO '95, pp437-451, 1995

[2] T.Eng and T.Okamoto, "Single-term divisible electronic coins", In Advances in Cryptology-Eurocrypto '94, pp313-323, 1994.

[3] David M'Raihi, "Cost-Effective Payment Schemes with Privacy Regulation", Advances in Cryptology - ASIACRYPTO '96, pp266-275, 1996

[4] "MPTP", http://www.w3.mag.keio.ac.jp/TR/WD-mptp -951122

[5] 김해만외 2명, "새로운 소액지불에 관한 연구", 춘계학술발표논문집, pp181-186, 1998

[6] 이임영외 8명, "전자 상거래 환경을 위한 기술조사 연구", 한국 전산원 연구 보고서, 1996. 10