# 이동통신 시스템에서 추적 가능한 전자지불 프로토콜의 제안

강혁*, 김태윤
고려대학교 컴퓨터학과
paranblue@netlab.korea.ac.kr

# A Proposal of traceable Electronic Payment Protocol in Mobile System

Hyeok kang*, Tai-Yun Kim
Dept of Computer Science, Korea University

**요 약**

최근 IT 산업의 발달로 인터넷 이용자가 폭발적인 성장에 따라 인터넷을 통한 전자 상거래가 새로운 경제 활동으로 등장과 동시에 무선 인터넷 시장이 급속한 성장을 하고 있다. 이에 따라 기존에 사용되어지고 있는 on-line상에서의 전자 지불 방식보다 실용적인 무선 인터넷상의 전자 지불 방식이 요구되고 있다. 이에 따라 본 논문에서는 무선 인터넷 상에서 전자상거래를 통한 결제대금 지급을 할 때 부정 사용자에 대한 사용자 추적, 즉 익명성 제어가 가능한 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜의 특징은 기존의 on-line 상에서의 제공되어지고 있는 전자지불 프로토콜의 추적기능을 무선 인터넷 환경에서 보다 효율적이며 안전하게 사용할 수 있는 프로토콜을 제시한다.

## 1. 서 론

현대 사회가 IT 산업이 급성장하는 사회로 변화됨에 따라 신물 중심의 거래에서 인터넷 이용을 통한 새로운 경제 활동으로 급속히 변화되고 있다. 거기에 무선 인터넷의 보급으로 시.공간적 한계를 넘어 보다 용이하게 소비자와 기업이 상품과 서비스를 가지고 거래하는 전자상거래 시장이 형성되었다. 이 전자상거래에서 가장 부각되는 문제는 크게 지불의 문제와 보안의 문제로 생각할 수 있다. 이러한 급속히 확대, 발전해 가는 전자 상거래는 앞에서의 문제에 적합한 새로운 형태의 전자 지불 시스템들이 선보이고 있다. 이에 따라 전자 지불 시스템 중에서 현재 관심의 초점으로 부상하는 것이 전자 화폐이며, 이는 기존의 카드와는 달리 실물 화폐에 모든 성질을 갖도록 디지털화 된 것으로서 가장 현실성이 있는 대안으로 평가되고 있다. 이와 같은 전자화폐에 대한 연구 개발은 1982년 David Chaum의 On-Line형 전자 화폐 시스템[1]이 처음으로 등장하였다.

또한 기존의 on-line상의 전자 화폐의 불법적인 사용, 즉 돈 세탁, 자금의 해외 불법 유출 등의 문제점을 해결하기 위해서는 추적 가능성이 전자 화폐의 기능에 포함되어야 하며, 한편 사용자 개인의 익명성을 보호하기 위해서는 조건부 추적 가능성이 요구되고 있다. 이와 같은 문제가 무선 인터넷 상의 전자지불에서도 나타날 수 있으므로 해결방법으로 우선 on-line상에서 문제들을 해결하며 그것을 무선 인터넷 상에서 적용시켜본다. 그래서 on-line상에서의 문제를 해결하기 위해 [3]에서 D. Chaum이 제안한 blind signature 방식을 이용한 조건부 추적 가능한 프로토콜을 제안한 바 있다. 그러나 이 방식은 각 구성원간의 통신 데이터 양이 많고, 멱승 연산이 많아서 일반 pc에서의 계산량이 많아서 무선 인터넷에서 구현하기 어려움이 있다. 따라서 이렇게 많은 계산량을 줄이면서 보다 낮은 안전성을 갖도록 하는 무선 인터넷 지불 프로토콜을 제안한다. 2장에서는 전자 지불 시스템의 기본 개념에 대하여 알아보고, 3장에서는 제안한 프로토콜에 대해 알아본다. 그리고 4장에서는 제안 프로토콜의 안전성에 대하여 알아보고, 마지막으로 5장에서 결론을 맺는다.

## 2. 기본 프로토콜

전자 지불 시스템의 기본 프로토콜은 은행(B), 사용자, 그리고 판매자(M)사이에 이루어지는 통신을 말한다. 본 시스템에서는 무선 인터넷 상에서의 인증기관(CA)을 첨가 시켜서 사용자와 은행에서 발행하는 화폐에 대한 등록을 할 수 있게 하였다. 그러나 판매자는 전자 지불 시스템을 구성하는 시스템의 프로토콜에 아무런 영향을 미치지 않고 단지 사용자에게서 전송되는 데이터를 받아서 은행에 전송하는 역할만을 담당하도록 하였다. 사용자의 신원을 알기 위해서는 은행과 신뢰기관이 서로 협조하지 않으며 사용자의 신원을 알 수 없도록 하였다.[3]

### 2.1 Blind Signature 기본 프로토콜

Blind Signature Scheme의 기본 개념은 Chaum에 의해서 1982년에 소개되었다. Blind Signature Scheme은 기본적으로 송신자와 수신자, 두 개의 Entity를 갖는다. 송신자가 수신자에게 메시지를 전송하면서 수신자는 자신의 서명을 덧붙여 송신자에게 다시 전송한다. 그러면 송신자는 그 서명된 정보로부터 임의의 정보를 제거하여 익명성을 갖는다. 이러한 프로토콜 사용의 예로서 전자 선거 프로토콜이나 전자 지불 프로토콜이 있다.[3.6.7]

전자 지불 시스템의 기본 모델은 다음과 같고 이들 사이의 통신을 기본 프로토콜이라고 한다.

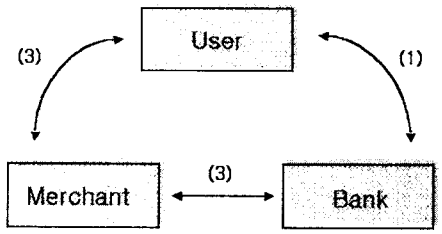



그림 1. 전자 지불 시스템의 기본 모델

이 프로토콜은 크게 다음과 같이 세가지로 나눌 수 있다.

① 인출 프로토콜(Withdrawal Protocol)
사용자가 은행에 전자 화폐 발생을 요구하면 은행측에서 사용자 확인과 함께 전자 화폐를 발행한다.
② 지불 프로토콜(Payment Protocol)
사용자가 인터넷을 통하여 원하는 물품을 구입하는 단계로 발행 받은 전자 화폐를 물품 구매 대금으로 지불하고 판매자는 물품을 배달한다.
③ 예치 프로토콜(Deposit Protocol)
판매자와 은행간에 이루어지는 관계로서 판매자가 은행에 물품 대금으로 받은 전자 화폐를 예치하는 프로토콜이다.

현재 사용자 익명성을 얻는 방법으로 가장 많이 사용하는 Blind Signature 프로토콜을 간단히 살펴보면 다음과 같은 세 단계로 구성된다.[3,10]

① Blinding 단계
수신자는 랜덤한 정수인 blinding factor r을 선택하고 $m' = mr^e \bmod n$ ( m은 message)를 계산한 후, 서명자에게 이 $m'$을 보낸다.
② Signing 단계
서명자는 자신의 비밀키 d를 사용하여 $s' = m'^d \bmod n$ 를 계산하고 수신자에게 $s'$ 를 돌려보낸다.
③ Unblinding 단계
수신자는 서명 $s = s/r \bmod n$ 을 얻는다.

본 논문에서 제안하고자 하는 방식은 Blind Signature 방식이 아닌 실제적으로 구현 가능하도록 RSA 알고리즘[8]을 이용한 각 Entity의 키 생성과 이산 대수 문제 및 hash 함수[9]에 기반을 둔 서명 기법을 사용하는 프로토콜을 제안한다.

## 3. 제안 프로토콜

### 3.1 시스템 요소

1) 인증기관(Certification Authentication)

| | 비밀키 | 공개키 |
|---|---|---|
| 데이터 암호용 키 | $d_{CA}$ | $e_{CA}$ |
| 인증용 키 | $D_{CA}$ | $E_{CA}$ |

데이터를 암호화하기 위해 RSA key를 생성하고 사용자를 인증하기 위한 인증용 키를 생성한다. 하나의 키를 가지고 사용할 수 있지만 데이터의 안전성을 높이기 위해서 두 개의 키를 분리하였다. 데이터의 무결성을 보장하기 위한 방안으로는 hash 함수를 사용한다. hash 함수는 일방향 함수이면서 메시지 압축을 한다. 주로 메시지 압축에 사용되는 예로 MD4와 MD5등이 있는데 본 논문에서는 MD5를 사용한다.

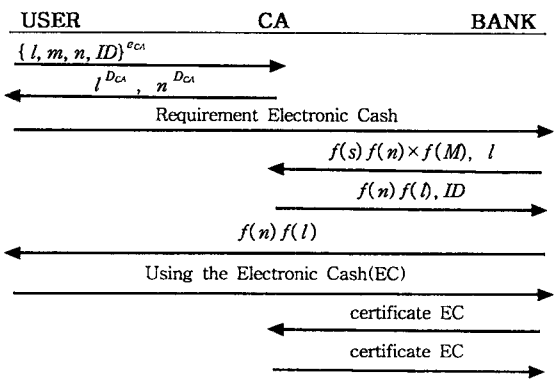
2) 은행
은행은 은행만의 암호화를 위하여 공개키와 비밀키를 생성하여 공개키는 각 사용자에게 전송하고 비밀키는 보관한다

| | 비밀키 | 공개키 |
|---|---|---|
| 은행 키 | $d_B$ | $e_B$ |

3) 사용자(User)
임의의 랜덤 한 값을 4개(l, m, n, s)를 생성한다 이중 3개(l, m, n)는 인증하기 위해 사용하고 나머지 (s)는 화폐의 일련 번호를 사용한다.

| | 사 용 |
|---|---|
| $l$ | 전자화폐 지불시 인증용으로 사용 |
| m | 전자화폐 발행시 인증용으로 사용 |
| n | 은행으로부터의 은닉용으로 사용 |
| s | 전자화폐의 일련 번호로 사용 |

### 3.2 전자 지불 시스템의 흐름




① 사용자는 자신의 $l$, m, n을 인증기관의 공개키로 암호화하여 인증기관에게 전송한다.

② 인증기관은 사용자를 확인하고 인증 비밀키를 이용하여 l,m을 서명한 후 사용자 측에 전송한다.
③ 사용자는 자신의 데이터와 인증 받은 데이터를 이용하여 전자 화폐 발행 요구한다.
④ 올바른 인증인 경우 hash해서 곱한 값에 사용자가 요구한 인출 금액을 hash해서 다시 곱한다. 그리고 그 값과 사용자의 랜덤 값 m을 인증기관에 전송한다.
⑤ 인증기관은 은행으로부터 전송된 m 값을 사용하는 사용자를 검색하여 그 사용자의 $l$ 값을 hash한다. 그리고 그 값을 은행으로부터 전송된 값에 곱한다. 이렇게 생성된 값을 다시 hash하여 그 사용자의 데이터 베이스에 저장한다. 그리고 그 ID를 화폐의 서명으로 하여 hash 값과 함께 은행에 전송한다.
⑥ 은행에서는 먼저 인증기관으로부터 전송된 ID가 자신이 보낸 ID인가를 검사하여 같으면 바르게 인증되었다고 보고 신뢰기관으로부터 전송된 f(n)f($l$)를 사용자에게 전송한다.
⑦ 사용자는 은행으로부터 전송된 데이터와 자신의 데이터 n과 $l$ 을 각각 hash하여 곱한 값과 비교한다. 같으면 바르게 서명되었음을 알고 화폐를 사용하게 된다.
⑧ 판매자를 통하여 들어온 화폐를 검증한다.
⑨ 은행으로부터 화폐에 대한 확인을 요청 받은 인증기관은 먼저 $l$ 에 해당하는 사용자를 찾는다. 그리고 그 사용자의 n 을 hash하고 또한 $l$ 을 hash한다. 각 각을 곱하고 은행에서 전송된 값에 다시 곱한다. 그리고 그 값을 다시 hash한다. 그리고 $l$ 사용자의 데이터 베이스에 저장된 발행 화폐와 비교하여 정당한 화폐인지를 검사 후 결과를 은행에 전송한다.

### 3.3 사용자 추적과정

은행은 ⑧의 과정 중 상점을 통하여 들어온 전자 화폐의 일련 번호를 검색한다. 만약 이전에 한 번이라도 사용한 적이 있는 화폐인 경우 그 화폐의 일련번호는 ⑧의 과정에서 이미 은행의 DB에 저장되어진다. 그 화폐의 일련번호를 다시 사용하게 되면 ⑧의 과정에서 자신의 데이터 베이스에서 같은 일련 번호가 있는 지를 검사하게 된다. 따라서 화폐의 이중 사용을 검출할 수 있다. 이때 판매자로부터 전송된 데이터 중 $l$ 의 값을 인증기관에 전송하면 인증기관은 그 $l$ 값을 사용하는 사용자를 검사하게 된다. 따라서 화폐 사용자의 신원을 검출 할 수 있다.

## 4. 익명성 및 안정성

은행은 화폐가 들어오더라도 그 화폐에서는 사용자에 대한 아무런 데이터도 얻을 수 없다. 판매자로부터 전송된 데이터에 사용자 인증에 관한 데이터가 있지만 이 데이터만으로는 누구의 데이터인지 구별할 수 없다.

인증기관의 입장에서 사용자가 상점을 통하여 은행에 지불한 전자화폐를 가로채기를 하더라도 이미 은행의 공개키로 암호화되었기 때문에 인증기관은 이 암호화된 정보로는 아무 것도 이룰 수 없다. 이 정보의 해독은 RSA의 해독과 직결 된 것으로 이산 대수의 문제에 속하게 되어 문제를 해결하기 무척 어렵게 된다.

## 5. 결 론

최근 On-Line 상에서의 전자 상거래가 많이 이루어지고 있다. 이에 따라 Off-Line에 해당되는 무선 인터넷을 통한 전자 상거래도 점차 증가하는 추세이다. 상거래 시 익명성 제어 또는 익명성 취소에 관한 연구가 활발히 진행되고 있다. 본 논문에서는 이러한 연구의 일환으로 무선 인터넷 환경에서 보다 효율적으로 적용될 수 있는 RSA와 hash 함수만을 응용하여 익명성 제어 방법의 하나인 조건부 추적성을 전자 화폐에 부여한 프로토콜을 제안하였다. 또한 제안된 프로토콜은 RSA와 hash 함수만을 사용함으로 해서 계산 능력이 열악한 PC 환경에서도 효율적인 실제 구현을 가능케 하고 있으며 시스템 구성 요소간의 정보의 주고받음을 경감시킬 수 있도록 하였다. 제안된 프로토콜을 이용할 경우 어느 기관이든 단독으로 사용자 추적을 할 수 없고 반드시 은행과 신뢰기관이 서로 협조해야만 사용자의 신원을 확인할 수 있다. 향후 보다 정확한 추적성과 보안성을 유지하면서 전자 화폐를 분할 할 수 있는 방안에 대한 연구가 필요하다.

## 6. 참고 문헌

[1] D . Chaum, " Blind Signature for Untraceable Payments", Proceeding of Crypto'82 pp.199-223 (1982)
[2] T. Okamoto and K. Ohta, " Universal Electronic Cash ", Advance in Crytology-crypto'91 Lecture Notes in CS, Springer- Verlag, pp32-27, (1992)
[3] 김해만, 이임영, "분할성과 부분적인 추적이 가능한 효율적인 전자 시스템에 관한 연구" (1999) http://www.multimedia.or.kr/multimedia/nonmoon/
[4] S. Band ; " Untraceable Off-line Cash in Wallets with Observe", Proceedings of Crypto'93 LNCS 773, Springer Verleg, pp.302-318
[5] J.Camenish, J.M Pirveteau, M. Stadler: " Efficient Payment System Protesting Privacy of ESORICS '94, Lecture Note in Computer Science 875, Springer Verlag, pp.27-215
[6] R.L.Rivest, A.shamor and L.Adleman," A method of Obtaining Digital Signatures and Public-key Cryptosystem" ACM, V0121 no2, pp.120-126(1997)
[7] R.L.Rrivest," The MD5 message-digest algorithm", Request for Comments(RFC) 1320, Internet Activities Board, Internet Privacy Task Force, April (1992 )