M-Commerce 향상을 위한 전자화폐 공정 은닉 서명 시스템

이현주[0] 이충세
충북대학교 전자계산학과
{leehyn2@hanmail.net[0], csrhee@cbucc.chungbuk.ac.kr}

Electronic Cash System based on Fair Blinding Signature for Mobile-Commerce Service

Hyun Ju Lee[O], Chung Sei Rhee
Dept. of Computer Science, Chungbuk National Univ

요 약

무선 전자상거래(M-Commerce)는 이동 통신 네트워크 기술과 무선 단말기를 기반으로 하여 언제 어디서나 필요한 시점에서 행할 수 있는 상거래를 의미하며 이때, 전자지불 방식의 하나인 전자화폐는 실물 화폐와 유사한 성질을 만족해야 한다. 본 논문에서는 이산대수문제에 기반한 메타-메시지 복원과 은닉 서명 기법을 이용하여 전자화폐가 이중사용, 돈 세탁 그리고 불법 무기 구매 등 부정한 수단으로 악용되었을 때 신뢰센터가 사용자의 익명성을 제어하고 지불 금액을 다시 복원할 수 있는 알고리즘을 제안한다.

1. 서 론

M-Commerce는 이동 통신 단말기와 통신 네트워크를 이용하여 각종 정보, 서비스, 재화에 대한 금전적 거래를 의미하며, 단순히 유선 인터넷 서비스를 그대로 무선 환경에 적용시킨 서비스가 아니다. 다양한 형태의 이동단말기, PDA, 노트북 등을 이용하여 B2B, B2C를 비롯하여 오락, 게임, 정보제공, 콘텐츠 등을 포함하는 모든 유료화된 서비스를 필요한 시점에서 가상공간에 접속하여 전자적 상거래를 가능하게 하는 새로운 생활 양식이라 할 수 있다.

무선 인터넷의 고유한 특성인 개인성(personalization), 위치성(location), 이동성(mobility)등을 최대한 이용한 독특한 비즈니스 모델과 서비스를 가지고 새롭게 구현될 다양하고 안전한 지불 인프라로 인하여 새로운 전기를 맞을 것으로 예상된다.

이러한 긍정적인 전망과는 달리 무선 전자상거래는 전송속도 및 데이터 용량, 보안 및 인증 등의 기술적인 측면에서 해결해야 할 제한 사항을 지니고 있다.[1]

기존의 은닉서명 방법[2]은 사용자의 지불금액과 서명된 결과와의 비연관성을 제공하기 때문에 부정한 수단으로 이중 지불되었거나 불법 무기 구매, 돈 세탁 등으로 악용되었을 때 지불 금액 추적이 불가능하다. 무선 이동통신의 급성장으로 이동 단말기에서 상거래가 활발히 이루어질 것으로 예상되는 시점에서 신뢰센터가 필요로 하는 경우에 메시지 사용자와 서명자를 연관지을 수 있어야 하고 부정한 수단으로 지불된 금액을 재생성하여야 한다.

본 논문에서는 M-Commerce 서비스 향상을 위한 전자 화폐를 구현하기 위해 필수적인 공정 은닉 서명 기법과 메시지를 복원하여 전자화폐 금액을 바로 생성할 수 있는 알고리즘을 제안한다.

2. 관련 연구

네트웍 통신망을 통한 모든 종류의 거래에 적극 활용될 수 있는 방법이 전자지불 기술인데 이 전자지불은 결제 방식에 따라 크게 전자화폐, 신용카드, 전자수표, 선불카드, 핸드폰 요금에 과금이 되는 방식으로 구분할 수 있다. 전자화폐는 다시 화폐가치 저장 매체에 따른 분류로 IC카드에 전자화폐를 저장하는 가치저장형과 인터넷상의 가상은행 계좌, 또는 인터넷과 연결된 고객의 PC에 전자화폐를 저장하는 네트웍형이 있다. 전자 상거래가 더욱 활성화 될 시점에서는 개인 단말기에서 손쉽게 지불할 수 있는 네트웍형 전자화폐 시스템이 가장 편리한 지불 수단이 될 것으로 예상되고 있다.

2.1 전자화폐 시스템 요구 사항

실생활의 화폐와 같은 안전성과 유용성을 제공하기 위한 요구 사항으로는 다음과 같다.[3]

- 비의존성(independence): 물리적인 조건에 의존하지 않고 네트웍을 통해서 전송되어야 한다.
- 안전성(security): 전자 화폐를 재사용하거나 위조되는 것이 방지되어야 한다. 온라인의 경우 이중 사용의 방지가 용이하나 off-line인 경우 전자 화폐 사용 전 거래 중지가 곤란하기에 추후 부정 사용자 방지 대책을 세

위야 한다.

• 익명성(anonymity): 거래 내역, 관계 등은 다른 사람에 의해서 추적될 수 없어야 한다. 사용된 돈의 사용자를 추적불가능(untraceable)하고 같은 계좌에서 두 번의 거래가 이루어졌음을 알 수 없도록(unlinkable) 설계되야 한다. 이러한 보호는 돈 세탁, 탈세 등의 부정적인 면이나, 전자화폐 시스템의 효율성을 떨어뜨릴 수 있기 때문에 완전한 익명성의 구현은 신중해야 한다.

• 오프라인(off-line) 거래: 사용자가 전자화폐 지불시 사용자와 상점간의 거래 과정은 오프라인 방식으로 이루어지는 것이 바람직하다. on-line 금융 체계는 안전하지만 운영 경비가 많이 들고 효율적이지 못하다.

2.2 전자화폐 시스템 기본 구조

전자화폐 시스템의 참여자는 사용자(고객), 전자화폐를 금융망과 연결시켜주는 은행, 전자화폐를 지불 수단으로 물건을 판매하는 상점으로 구성된다. 기본 프로토콜은 네 가지로 구성된다.[4]

• 인출(withdrawal protocol):사용자의 계좌로부터 전자화폐를 인출하기 위한 프로토콜이며 사용자와 은행간의 인증된 채널을 통해 이루어진다.

• 지불(payment protocol): 익명의 채널을 통해 사용자가 상점에게 전자화폐를 지불하기 위한 프로토콜

• 입금(deposit protocol): 상점이 사용자의 전자화폐 정보를 입금시키는 프로토콜

• 이중사용 검사(double-spending check protocol): 은행 단독으로 사용자 전자화폐의 이중 사용을 검사하는 프로토콜

3. 공정 은닉 서명 등록과 모델

3.1 공정 은닉 서명을 위한 사전 등록

사용자는 공개적으로 검증하기 위한 정보를 가지고 있는 신뢰센터에 사전 등록 단계를 거쳐 공정 은닉 서명에 필요한 비밀 정보를 할당받아야 하는데 등록 프로토콜 모델은 다음과 같다.

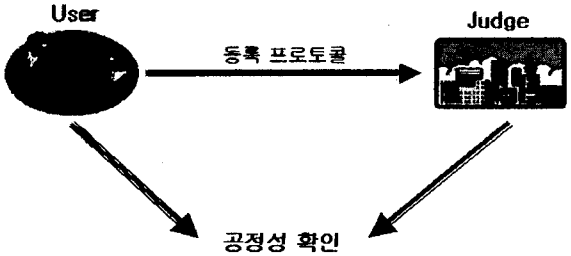

그림1. 공정 은닉 서명을 위한 등록 모델

3.2 Stadler 공정 은닉 서명 모델

은닉 서명(blind signature)[2]은 브로커가 서명하고자 하는 전자화폐에 대한 정보를 은닉하고, 서명된 결과와의 비연관성을 제시하는 서명 방식이다. Stadler가 제시한 공정 은닉 서명[5]은 사용자와 브로커간의 은닉 서명 결과에 대해서 신뢰 센터가 필요로 하는 경우 은닉 서명에 관련된 브로커와 전자화폐 사용자를 연관지을 수 있으며, 이 모델은 사용자, 브로커, 신뢰센터, 그리고 브로커와 사용자간의 서명 프로토콜(signing protocol)과 브로커와 신뢰센터의 연관성 복구 프로토콜(link-recovery protocol)인 두 개의 프로토콜로 구성되어 있다.

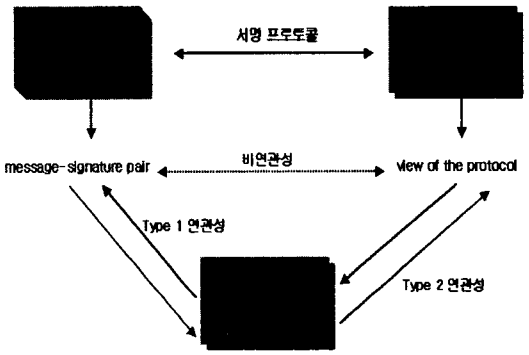

그림2. 전자화폐에 대한 공정 은닉 서명 프로토콜

신뢰센터는 연관성 복구 프로토콜을 통해 서명자로부터 받은 2가지 형태의 공정 은닉 서명 기법이 있는데 Type1은 신뢰센터가 메시지-서명 쌍을 서명자가 효과적으로 인증하기 위한 정보를 전달하고 Type2는 신뢰센터가 메시지의 전송자를 서명자가 효과적으로 검증할 수 있도록 한다. Type1을 사용하여 불공정한 인출을 검출하고, Type2를 사용하여 이중 지불 문제(double spending)를 감지할 수 있다.

4. 전자화폐 재생성 공정 은닉 서명 알고리즘

Stadler가 제시한 공정 은닉 서명 기법은 은닉 서명된 사용자의 전자화폐 금액에 대한 복원 기능을 제공하지 못한다. 본 논문에서는 Horster[6]가 제시한 이산대수문제(Discrete Logarithm Problem)에 기반한 메타-메시지 복원과 은닉 서명 기법을 이용하여 공정성을 제공하고 사용한 금액을 바로 재생할 수 있는 기법을 제안한다.

4.1 이산 대수 문제(Discrete Logarithm Problem)

$y \equiv g^x \bmod p$를 만족하는 y, g가 주어졌을 때 Z_p^*의 생성자 g, 원소 $y \in Z_p^*$에 대해 $1 \le x \le p-2$ 범위

내에서 x를 찾기 힘들다는 것에 근거를 둔 방식이다.

- $Z_p^* = \{r \in Z_p | (r, p) = 1\}$ 기약잉여계(reduced residue system)
- p : 소수 (prime number)

4.2 알고리즘 계수

다음은 본 알고리즘에서 사용되는 계수들이다.

- $c = h(\delta \cdot v_j \| \delta \cdot v_{1-j})$: 해쉬 함수값
- Z_q : modulo q에 관한 잉여계
  $v_j, v_{1-j} \in Z_q$, $j \in \{0,1\}$
- $payment$: 전자화폐 사용 금액
- $y \equiv g^x \bmod p$: 사용자의 공개키
- g : 생성자(generator)
- x: 브로커의 비밀키

4.3 지불 금액 재생성 및 공정 은닉 서명

사용자는 인출 금액에 대한 승인을 받은 후 메시지 payment에 대해 브로커의 공정 은닉 서명 단계를 수행하여 지불 금액을 다음 알고리즘에 의해 복원한다.

- 사용자는 브로커의 비밀키를 이용하여 공개키를 생성하고 신뢰센터에 사전 등록하여 공정 은닉 서명을 위해 할당받은 비밀 정보 v_j, v_{1-j}를 이용하여

$$\alpha_j \equiv g^{v_j + v_{1-j}} \bmod p$$

$$\alpha_{1-j} \equiv c \cdot (g^{v_j + v_{1-j}})^{-1} \bmod p$$

를 생성하여 브로커에게 보낸다.

- 브로커는 $c \equiv \alpha_j \cdot \alpha_{1-j} \bmod p$를 계산하여 신뢰센터가 생성한 c 값과 같은지 확인한다.
- 서명자는 자신의 비밀 랜덤 수 $z_j^*, z_{1-j}^* \in Z_q$를 생성한다.
- 브로커는 공정 은닉에 사용될 매개변수 η_0^*, η_1^* r_0, r_1을 생성하여 사용자에게 전달한다.
- 사용자는 메시지 payment에 대하여 브로커에게 받은 매개변수를 이용하여 $payment_j^*$를 생성한다.

$$r_j \equiv payment^{-1} (g)^{z_j^* \cdot v_j} y^{v_{1-j}} \bmod p$$

$$payment_j^* \equiv v_j^{-1} \cdot (r_j - v_{1-j}) - g^{z_j^*} \bmod q$$

- 사용자는 r_j와 $payment_j^*$를 브로커에게 전송한다.
- 브로커는 은닉 서명에 해당하는 s_j^* 를 생성한다.

$$s_j^* \equiv x \cdot (payment_j^* + g^{z_j^*}) - z_j^* \bmod q$$

- 브로커는 s_j^*를 다시 사용자에게 전달한다.
- 사용자는 s_j^*에 대해 $s_j \equiv v_j \cdot s_j^* \bmod q$ 를 계산하여 $payment \equiv g^{-s_j} y^{r_j} r_j^{-1} \bmod p$인 지불 금액 재생성에 대한 공정 은닉 서명 결과를 얻는다.

5. 결 론

M-Commerce 서비스 향상을 위한 전자 화폐를 이동 단말기에서 구현하기 위해 본 논문에서는 지불된 전자화폐가 악용되었을 때 신뢰센터가 필요로 하는 경우 화폐 사용자와 브로커를 연관지을 수 있고 이미 지불된 금액을 재생성 할 수 있는 알고리즘을 제안하였다.

향후 M-Commerce가 성공하기 위해서는 이동통신 사업자와 콘텐츠 개발의 전문 무선 전자상거래 기업간의 광범위한 협력이 이루어져야하고 데이터 용량 및 전송속도, 보안과 객체간의 인증 등 기술적인 측면에서의 해결 방법을 연구해야 할 것이다.

참 고 문 헌

[1] Gunther Horn and Bart Preneel, "Authentication and Payment in Future Mobile Systems," Computer Security-ESORICS'98, Lecture Notes in Computer Science, No.1485, Springer-Verlag, pp375, 1998.

[2] D. Chaum, "Blind Signature for Untraceable Payments," Advance in Cryptology-Crypto '82, Lecture Notes in Compture Science, Springer-Verlag, pp.199-203, 1983.

[3] B.Pfitzmann, "Properties of Payment Systems: General Definition Sketch and Classification," IBM Research Report, 1996.

[4] A.de Solages and J.Traore. "An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets with Observers," In Proceedings of the Second International Conference on Financial Cryptography, number 1465 in Lecture Notes in Computer Science, pp 275-295, Springer-Verlag, 1998.

[5] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind Signature," Advances in Cryptoloty-Eurocrypt'95, Lecture Notes in Computer Science, Vol . 921, Spring-Verlag, 1995.

[6] Patrick Horster, Holger Petersen, "Meta Message Recovery and Meta Blind signature schemes based on the discrete logarithm problem and their applications," Advances in Cryptology-Asiacrypt'94, Lecture Notes in Computer Science, Springer-Verlag, 1994.