모바일 전자상품권 프로토콜의 설계

용승림*
*인하공업전문대학 컴퓨터시스템과
e-mail:slyong@inhatc.ac.kr

Design of protocol of mobile e_gift certificate

Seunglim Yong*
*Dept of Computer Science, Inha technical colledge

요 약

모바일 기기의 성능 향상과 모바일 인터넷 서비스의 활성화, 스마트폰 시장의 급속한 성장으로 모바일 쿠폰 시장 빠르게 활성화 되고 있으나 이로 인한 다양한 문제점이 발생되고 있다.
본 논문에서는 이러한 문제점들을 방지하고 일회성의 쿠폰 이외에 다회 이용 가능한 모바일 전자상품권 프로토콜을 제안한다. 동형암호를 적용하여 모바일 기기에서 암호화와 복호화 연산을 최소화하도록 설계하였으며, 쿠폰의 정보는 암호화되고 사용시마다 새로 생성되도록 하여 이중사용과 복제가 불가능하도록 설계하였다.

1. 서론

전자 쿠폰(e-쿠폰)은 사용자가 인터넷과 같은 수단을 이용하여 쿠폰을 받고 이를 프린터로 프린트하여 이용하거나, 프린트하지 않고 전자적으로 데이터를 전송하는 방법을 이용하여 쿠폰을 이용하는 방법이 있다[4].
최근에는 모바일 기기의 발전으로 인하여 전자쿠폰의 형태를 모바일로 옮겨온 형태의 m-쿠폰의 연구가 많이 진행되고 있다. 모바일 기기의 성능 향상과 모바일 인터넷 서비스의 활성화, 스마트폰 시장의 급속한 성장으로 모바일 마케팅의 다양한 시도가 이루어지면서 모바일 쿠폰 시장은 빠르게 활성화 되고 있으나 이로 인한 다양한 문제점이 발생되고 있다. 소비자들의 쿠폰위조나 이중사용과 같은 부정행위로 인한 기업 손실이 발생될 수 있으며 최근에는 소비자의 쿠폰 유효기간 내 미사용으로 인한 손실도 커지고 있다.

본 논문에서는 안전한 모바일 상품권 프로토콜을 제안한다. 모바일 상품권은 일회성이 아닌 하나의 상품권을 가지고 결제 금액만큼 또는 설정된 횟수만큼 다회 사용 가능하도록 설계하였다. 동형암호를 적용하여 모바일 기기에서 암호화와 복호화 연산을 최소화하도록 하며, 쿠폰의 정보는 암호화되고 사용시마다 새로 생성되도록 하여 이중사용과 복제가 불가능하다.

2. 관련 연구

2.1 모바일 쿠폰

Anand et al.은 인터넷에서 e-쿠폰을 발급하는 시스템을 제안하였다. 이 시스템은 사용자들이 인터넷 상에서 온라인 스토어에 방문할 때 적절한 시기에 e-쿠폰을 사용자에게 제공한다[1].
Garg et al은 할인 금액이나 상품 설명 등을 알 수 없는 제 3의 기관의'쿠폰 민트'를 제안하여 온라인 쿠폰 인증을 위한 인프라만을 제공하는 안전한 e- 쿠폰 시스템을 제안하였다[3].
Chang et al은 모바일 사용자들을 위하여 모바일 단말기에서의 지수승 연산과 같은 복잡한 계산 과정을 제거하고, 발급된 쿠폰에 시리얼 넘버를 부여하여 이중 사용을 막고, 발급자로 하여금 쿠폰에 서명을 하게 함으로써 상점이 쿠폰을 인증하고 위조를 막을 수 있는 시스템을 제안하였다[2].

2.2 보안 요구사항

모바일 쿠폰 시스템의 일반적인 보안 요구사항은 다음과 같다.

1) 인증(authentication) 및 권한(authorization)
사용자는 자신이 단말기의 소유주이며 그 서비스와 쿠폰을 사용할 정당한 권한을 가졌음을 입증하여야 한다.
2) 위조방지(unforgeability)
발급자만이 유효한 쿠폰을 제공할 수 있으며, 다른 어떤

참가자나 공격자가 그것을 위조할 수 없다.
3) 부인방지(non-repudiation)
각 참여자는 자신이 관여한 트랜잭션을 부인할 수 없다.
4) 이중사용 방지(preventing from double-spending)
사용자가 같은 쿠폰을 한번 이상 사용하는 것으로부터 제조업자를 보호하여야 한다.

3. 모바일 전자상품권 프로토콜

3.1 동형 암호

본 논문에서 적용할 동형 암호란 암호시스템 E가 어떤 정의된 연산 $\oplus$에 대하여, 알려지지 않은 평문 x와 y에 대한 암호문 $E(x)$와 $E(y)$가 주어졌을 때, 누구든지 암호 해제 과정을 생략하고 암호화된 상태 그대로 $E(x \oplus y)$를 계산할 수 있는 암호시스템이다. 연산을 보존하는 암호화 기법은 RSA 공개키 암호 기법이 발표된 직후 privacy homomorphism이라는 이름으로 처음 제안되었다[5].

3. 2 모바일 전자상품권 프로토콜

제안하는 프로토콜은 일회 사용 횟수가 정해지는 것이 아니라 결제 금액만큼 또는 정해진 횟수만큼 다회 사용할 수 있다.

3.2.1 등록 및 결제

1) 사용자는 모바일폰에 상품권 어플리케이션을 다운로드 한다.
2) 사용자의 전자지갑은 임의의 난수 k를 선택하여 $k' = g^k$를 계산하고 사용자의 폰번호 x를 이용하여 $y = g^x$를 계산하여 y, k'와 함께 발급자에게 등록을 요청한다.
3) 발급자는 폰번호를 이용하여 y값을 확인하고 검증이 성공하면 사용자를 등록한다.

3.2.2 발급

1) 사용자는 상품권 어플리케이션을 이용하여 발급자에게 쿠폰을 요청한다.
2) 발급자는 임의의 난수 a를 사용자의 어플리케이션에 전송한다.
3) 사용자의 어플리케이션은 $b' = k - xa$를 계산하여 b'을 발급자에게 보낸다.
4) 발급자는 $k'' ? = g^{b'} y^a$ 를 계산하여 값을 확인한다.
5) 발급자는 동형암호를 이용하여 쿠폰번호(N_{coupon})를 암호화한 $E_s(N_{coupon})$과 서명값을 사용자에게 전송한다. 암호화 알고리즘 $E()$는 연산 $\oplus$에 동형 성질을 가지고 있으며 암호화키는 s를 의미한다. 즉, $E(x) \oplus E(y) = E(x \oplus y)$ 이 된다.
6) 발급자는 폰번호와 쿠폰번호, 암호화 키를 데이터베이스에 저장한다.
7) 사용자는 서명값을 확인하고 발급받은 암호화된 쿠폰 $E_s(N_{coupon})$을 어플리케이션에 저장한다.

3.3 상품 교환

1) 사용자는 어플리케이션에 사용 요청을 한다.
2) 상품권 어플리케이션은 사용자의 인증정보를 발급자에게 보낸다.
3) 발급자는 사용자의 인증정보와 결제 금액 또는 횟수 초과 사용 여부를 확인하고 검증이 되면 랜덤 값($rand$)을 생성하고 암호화한다.
3) 발급자는 $E_s(rand)$를 어플리케이션에 전송한다.
4) 어플리케이션은 저장되어 있는 암호화된 쿠폰값과 랜덤값을 같이 계산한다.

$$E_s(N_{coupon}) \oplus E_s(rand) = E_s(N_{coupon} \oplus rand)$$

5) 어플리케이션은 생성된 새로운 쿠폰값 $E_s(N_{coupon} \oplus rand)$ 으로 바코드를 생성한다.
6) 상점은 바코드를 스캔하여 스캔한 값을 발급자에 보낸다.
7) 발급자는 상점으로부터 받은 $E_s(N_{coupon} \oplus rand)$ 값을 복호화하여 N_{coupon}과 $rand$값을 확인하여 유효성을 검증한다.
8) 사용자는 상품을 받는다.

4. 안전성 검증

제안한 모바일 전자상품권 프로토콜의 안전성은 다음과 같다.

1) 인증 및 권한
사용자는 발급자에게 등록시에 자신의 핸드폰 번호를 드러낼 뿐 사용 중에는 사용자 인증을 위하여 임의의 값을 이용하여 안전하게 사용자를 인증하게 된다.
2) 위조 방지
제안 프로토콜은 발급자가 쿠폰과 매회 새로운 $rand$값을 생성하여 암호화하게 된다. 이때 암호화키는 발급자만 알 수 있으므로 제 3자는 정당한 쿠폰을 생성해낼 수 없다.
3) 부인방지
발급자는 서명을 통하여 쿠폰을 발급했음을 증명하며 사용자는 자신만이 계산할 수 있는 값을 계산함으로써 부인을 방지할 수 있다.
4) 이중사용 방지
바코드 형태의 쿠폰은 이미지를 복사하거나 사용한 쿠폰을 다시 사용할 수 있으나, 제안한 프로토콜에서는 사용시마다 발급자로부터 새로운 $rand$값을 받고 이를 쿠폰에 적

용한 후 사용해야 유효성을 입증 받을 수 있으므로 이중 사용을 방지할 수 있다.

또한 제안 프로토콜은 복잡한 암호화의 계산이나 복호화의 계산은 모두 발급자 쪽에서 계산을 수행하며, 모바일 기기에서는 등록시 2번의 지수 연산을 제외하고는 프로토콜의 수행 내내 다른 암호화,복호화 연산과 지수 연산 등을 수행하지 않는다. 동형 암호의 종류에 따라 곱셈 또는 덧셈 연산만으로 안전한 모바일 전자상품권 프로토콜이 수행될 수 있다.

5. 결론

본 논문에서는 안전하게 이용할 수 있는 모바일 전자상품권 프로토콜에 관하여 제안하였다. 모바일 전자상품권 프로토콜은 다회 사용 가능하며, 이중사용과 부인, 위조 등으로부터 발급자의 권리를 보호한다. 모바일 기기에서는 시간이 오래걸리는 암호화와 복호화 계산을 배제하기 위하여 동형암호를 적용함으로써 효율성을 향상시켰다.

참고문헌

[1] R. Anand, M, Kumar and A, Jhingran, “Distributing E-coupon on the Internet”, Proceedings of the 9th Annual Conference of the Internet Society, 1999.

[2] C.C.Chang, C.C. Wu, and I. C. Lin, “A secure e-coupon system for mobile users”, International journal of computer science and network security, Vol6, No1. 2006.

[3] R. Garg, P. Mittal, and V. Agarwal, “An Architecture for Secure Generation and Verification of Electronic Coupons”, Proceedings of the General Track: 2002 USENIX Annual Technical Conference, PP. 51-63, 2002.

[4] M. Kumar, A. Rangachari, A. Jhingran and R.Mohan, “Sales Promotions on the Internet,” Third USENIX workshop on Electronic Commerce, pp. 167-176, 1998.

[5] L. Rivest, Len Adleman, and L. Dertouzos, “On data bank and privacy homomorphisms”, proceedings of the 19th Annual Symposium on Foundations of Secure computation- FSC 1978, pp 169-180, 1978.