Journal of The Korea Society of Computer and Information
Vol. 18, No. 10, October 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.10.081

다회 사용가능한 안전한 모바일 쿠폰 프로토콜

용 승 림*

A Reusable Secure Mobile e-Coupon Protocol

Seunglim Yong*

요 약

모바일 기기의 성능 향상과 모바일 인터넷 서비스의 성장으로 모바일 쿠폰 시장은 사용자들에게 중요한 시장으로 자리잡고 있다. 모바일 쿠폰은 사용자에게 이동성을 제공해주고 발급자에게 발급의 편리성도 제공해줄 수 있다.

본 논문에서는 해쉬 함수와 XOR 연산과 같이 간단한 암호학적인 기법을 적용하여 모바일에서 효율적으로 수행할 수 있는 모바일 쿠폰 시스템에 대하여 제안한다. 제안하는 시스템은 사용자가 모바일 쿠폰의 횟수를 선택하고 발급자는 이중 사용을 방지할 수 있다. 사용자는 모바일기기에서 프로토콜 수행시 지수연산과 암호화 또는 복호화연산과 같은 복잡한 연산을 수행하지 않아도 된다. 제안한 스킴은 payword의 해쉬 체인을 이용하여 사용자의 이중 사용을 방지하였다.

▸ Keywords : 모바일 쿠폰, 해쉬 함수, 다회 사용

Abstract

Since nowadays mobile phone messages are flourishing, the application of electronic coupon (e-coupon) will become a trend for mobile users. E-coupon for mobile commerce can provide mobility for users and distribution flexibility for issuers.

In this paper, we propose a mobile e-coupon system that just applies some simple cryptographic techniques, such as one-way hash function and XOR operation. In our system, the customer can control the number of issued e-coupons and the issuer can prevent them from double-redeeming. The customer does not need to perform any exponential computation in redeeming and transferring the coupons. Our scheme uses one-way hash chains for preventing from double-spending.

▸ Keywords : Mobile coupon, Hash function, Reusable

•제1저자 : 용승림
•투고일 : 2013. 10. 3, 심사일 : 2013. 10. 10, 게재확정일 : 2013. 10. 17.
* 인하공업전문대학 컴퓨터시스템과(Dept. of Computer Systems and engineering. Inha technical college)

I. 서 론

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[1].

현재 쿠폰은 시장에서 가장 보편적인 가격할인 수단으로서 온라인, 오프라인 등을 통해서 다양하게 쿠폰을 발급 받을 수 있다. 이렇듯 쿠폰의 유형과 매체들이 다양해지면서 사용자들은 쿠폰을 접할 수 있는 기회가 늘어나고 있다. 쿠폰 시스템은 정보 통신 기술의 발전으로 인해 종이 쿠폰, 인터넷 쿠폰, 모바일 쿠폰 순으로 점차 발달해 갔다.

초창기 인터넷이 발달하기 전에는 신문이나 잡지, 광고지 등으로 배포되는 종이 형태의 쿠폰들이 많이 배포되었다[2]. 종이 쿠폰을 사용하기 위해서는 사용자가 직접 쿠폰을 오리고 다양한 종류의 쿠폰을 지갑, 주머니 등에 보관하는 등의 사용상의 불편성이 많았다. 인터넷이 발달하면서 종이쿠폰 대신 사용자가 원하는 쿠폰을 컴퓨터를 통해서 발급 받을 수 있는 인터넷 쿠폰이 등장하였다. 이 쿠폰은 인터넷을 통해서 안전하게 제공하고 있기 때문에 쿠폰의 신뢰성을 제공하고 있다. 그리고 다양한 서비스를 제공하는 쿠폰들을 확인할 수 있으며 원하는 쿠폰을 선택하여 발급 받을 수 있다[3]. 그러나 발급 과정은 인터넷을 이용함으로써 편리해졌지만 쿠폰 사용과정에서는 사용자가 직접 쿠폰을 프린트하고 오려서 사용하기 때문에 준비 과정이나 보관문제에 있어서 문제점이 발생한다.

최근에는 모바일기기의 발달과 보급으로 쿠폰의 발급과정부터 사용과정까지 종이를 이용하지 않고 모바일 기기를 이용하는 모바일 쿠폰이 생겨났다. 모바일 쿠폰은 무선 네트워크를 통해 원하는 쿠폰을 검색 및 선택해서 발급 받을 수 있는 형태를 지닌다. 모바일을 이용하여 이동하면서 손쉽게 쿠폰을 받을 수 있기 때문에 이동성과 편리성을 제공한다.

본 논문에서는 안전하게 다회 사용할 수 있는 모바일 쿠폰 프로토콜을 제안한다. 모바일 쿠폰은 일회만 사용하는 것이 아니라 한 번의 등록으로 설정된 횟수만큼 여러 번 쿠폰을 사용할 수 있도록 설계하였다. 다회 사용시 쿠폰 정보를 새로 생성되도록 하여 이중사용과 복제가 불가능하도록 한다. 모바일 기기에서는 해쉬연산과 XOR, 덧셈 또는 곱셈 연산 이외의 암호화와 복호화 연산과 같은 복잡한 연산을 배제하여 수행하지 않도록 하여 효율성을 높였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 쿠폰에 관한 시스템에 대해 알아보고 장단점을 분석한다. 3장에서는 본 논문에서 제안하는 시스템에 대한 상세 내용을 제시하고 제안 시스템의 성능분석을 제시한다. 마지막으로 4장에서 결론을 도출한다.

II. 관련 연구

1. 쿠폰 시스템

기존의 쿠폰은 종이 형태의 쿠폰에서 인터넷의 발달과 모바일의 발달로 다양한 형태로 제공되고 있다.

종이 쿠폰 방식의 경우에는 신문이나 잡지 등을 통하여 배포하거나, 무작위 배포 등의 다양한 방법을 이용하여 종이형태의 쿠폰을 배포하고 이용하는 방식이다. 이러한 방식은 지정된 장소 내에서 다양한 사용자들에게 쿠폰을 다량으로 배포할 수 있는 장점이 있다. 그러나 종이로 생산하고, 배포하는 비용 문제가 발생될 수 있으며, 사용자들은 쿠폰을 보관해야 하는 불편이 있다.

인터넷 쿠폰 방식은 사용자가 직접 인터넷을 통하여 원하는 쿠폰을 획득하고 종이로 출력하여 사용하는 방식이 일반적이다. 이 방식은 사용자가 필요시 인터넷을 통하여 발급받고 사용할 수 있으며, 쿠폰의 안전한 배포와 사용에 대한 많은 연구가 진행되어 왔다. Anand et al.은 인터넷 상에서 사용자에게 e-쿠폰을 사용자에게 제공하는 방법을 제안하였다[4]. e-쿠폰은 수명주기에 대하여 제안하고, 온라인스토어에서 사용자들에게 e-쿠폰을 배부하는 방법에 대하여 제안하였다. Garg et al은 이중사용을 막기 위하여 제 3의 기관인 '쿠폰 민트(coupon mint)'를 제안하였다. 쿠폰민트는 온라인 쿠폰 인증을 위한 인프라만을 제공하고 검증하는 역할만 하도록 하였으며 다양한 쿠폰 생성이 가능한 안전한 e-쿠폰 시스템을 제안하였다[5].

모바일 쿠폰 방식의 경우에는 모바일 기기를 사용하여 무선 네트워크를 통해 사용자가 원하는 쿠폰을 다운로드해서 사용하는 방식이다. 이 방식은 다운로드된 쿠폰을 출력하지 않고 모바일 기기에 저장 후 바로 이용할 수 있다. Chang et al은 모바일 사용자들을 위하여 모바일 단말기에서의 지수승 연산과 같은 복잡한 계산 과정을 제거하는 기법에 대하여 제안하였다. 발급된 쿠폰에 시리얼 번호를 부여하여 이중 사용을 막고, 발급자로 하여금 쿠폰에 서명을 하게 함으로써 상점이 쿠폰을 인증하고 위조를 막을 수 있는 시스템을 제안하였다[6]. Bao는 디지털 티켓 형태의 쿠폰시스템을 제안하였다. 쿠폰을 디지털 티켓 형태로 구성하여 디지털 티켓의 포맷과

사용가능한 시나리오 구성을 제안하였다[7]. Park et al은 발급, 상품교환, 청산 단계의 모바일 쿠폰 프로토콜을 설계하였다. 특히 위조나 이중사용 뿐 아니라 도/소매업자 및 청산소에 의한 청산과정 조작을 효율적으로 방지할 수 있는 기법에 대하여 제안하였다. 프로토콜상에서 사용자와 발급자 모두의 공개키 연산을 최소화하고 대칭암호 연산을 이용하여 효율성을 고려하였다[8].

2. 암호학적인 기술들

2.1 payword

payword 방식은 1996년 Rivest와 Shamir가 제안한 소액 지불시스템이다. payword 시스템은 사용자, 상점, 브로커로 구성된다[9].

사용자는 지불을 하고자 할 때 소액의 화폐 가치를 지닌 n개의 payword를 생성해야 한다. 즉, n번째 payword w_n을 임의로 생성하고 $i=n-1,n-2,...,1,0$에 대하여 다음과 같이 해쉬 체인을 생성한다.

$$w_i = h(w_{i+1})$$

사용자의 i번째 지불은 (w_i,i)로 구성되며, 상인은 w_{i-1}을 사용한 해쉬 연산으로 유효성을 확인할 수 있다. 하루의 마지막에 상인은 각 사용자에게 받은 마지막 지불인 $P_l=(w_l,l)$과 이에 대응하는 위임 메시지를 함께 브로커에게 보낸다. 브로커는 l번의 해쉬 함수를 반복 수행하여 w_l을 확인한 후, 사용자의 계좌에서 l만큼의 금액을 청구하여 상인의 계좌로 지급한다.

payword는 각 상인에 대한 고유한 payword를 사용하기 때문에 상인이 독립적으로 payword 의 이중사용, 위조, 변조를 검사할 수 있다는 장점이 있다.

본 논문에서는 payword 의 해쉬 체인을 쿠폰의 횟수제한 확인에 적용하고자 한다.

2.2 준동형 암호

수학에서의 준동형성이란 연산이 정의된 두 집합 사이의 맵핑으로 두 집합에서 정의된 연산을 보존하는 맵핑을 의미한다[10].

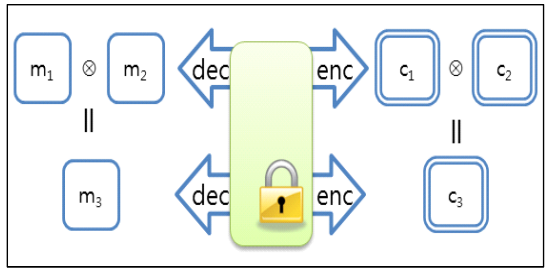


그림 1. 준동형 암호
Fig. 1. homomorphic encryption

준동형 암호(homomorphic encryption)란 [그림 1]과 같이 암호화 함수 중에서 평문 공간과 암호문 공간에 정의된 연산을 보존하는 암호화 함수이다. 어떤 암호시스템 E가 동형 암호시스템이라는 것은 대표적인 산술연산인 덧셈 연산과 곱셈 연산을 암호문에 적용하여 평문에 대한 연산을 다음과 같이 수행할 수 있다는 것이다.

$$E_k(m_1)+E_k(m_2)=E_k(m_1+m_2),$$
$$E_k(m_1)\times E_k(m_2)=E_k(m_1\times m_2)$$

연산을 보존하는 암호화기법은 RSA 공개키 암호 기법이 발표된 직후 privacy homomorphism이라는 이름으로 처음 제안되었다[11]. Rivest 등은 RSA 시스템을 변형한 기법을 포함하여 다섯 가지 기법을 발표하였으나 현실에서의 적용에는 안정성에 문제가 있었다.

준동형 암호는 암호화된 데이터에 대해 복호화하지 않고 마음대로 연산을 수행할 수 있다. 현재의 클라우드 컴퓨팅 환경에서는 사용자의 데이터가 서버에 저장되고 관리되면서 개인의 정보보호와 관련된 문제들이 대두되고 있다. 이에 일반적인 암호화를 통한 데이터 보호가 아닌 암호 해제 과정을 생략하고 암호화된 상태 그대로 연산을 수행할 수 있는 동형 암호에 대한 연구는 현재에도 지속적으로 이루어지고 있다.

III. 다회 사용가능한 모바일 쿠폰

1. 용어 정의와 보안 요구사항

상세 프로토콜을 제안하기 앞서 모바일 쿠폰 시스템의 일반적인 보안 요구사항에 대하여 기술하고, 본 논문에서 사용되는 용어에 대한 정의를 수행한다.

1.1 보안 요구사항

모바일 쿠폰 시스템의 일반적인 보안 요구사항은 다음과 같다[7].

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 참여자나 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 이중 사용할 수 없어야 한다.

1.2 용어 정의

본 논문에서 제안한 프로토콜에서 사용될 용어들은 [표 1]과 같이 정의한다.

표 1. 용어 정의
Table 1. Notation

기호	설명
ID_i	사용자 U_i의 아이디
PW_i	사용자 U_i의 패스워드
CID_i	사용자의 가명ID
w_i	i번째 해쉬 체인의 값
$h()$	일방향 해쉬 함수
$\oplus$	XOR 비트 연산자
$\otimes$	준동형 암호의 연산
$\|\|$	연결(concatenation) 연산
x	서버의 비밀값
sig	서명
N_C	초기 coupon 정보
$Coup$	암호화된 쿠폰정보
$S(\ )$	서명을 생성하는 함수
$E_{H_k}(m)$	키 k로 메시지 m을 암호화하는 준동형 암호 알고리즘

2. 프로토콜

본 절에서 모바일 쿠폰의 상세 프로토콜에 대하여 기술한다. 구매자는 어플리케이션을 다운로드 받아 스마트폰에 설치하고 쿠폰 다운로드를 위한 등록을 수행한다. 등록이 완료되면 쿠폰의 발급 프로토콜을 진행하게 되며, 발급 받은 쿠폰은 상점 교환 프로토콜을 통하여 사용할 수 있다. 모바일 쿠폰 프로토콜의 단계는 [그림 2]와 같다.

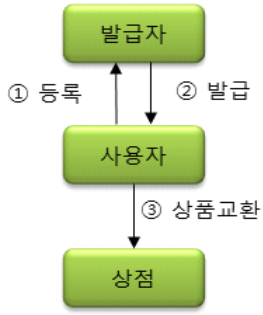


그림 2. 모바일 쿠폰 프로토콜
Fig. 2. mobile coupon protocol

2.1 등록 프로토콜

1) 사용자는 먼저 자신의 모바일폰에 쿠폰 어플리케이션을 다운로드한다.
2) 쿠폰 어플리케이션을 통하여 쿠폰 발급자의 서버에 회원 등록을 한다. 사용자는 자신의 ID와 PW의 해쉬값 $h(PW)$을 안전한 채널을 통하여 서버에게 전달한다.
3) 서버는 사용자의 ID값과 $h(PW)$값을 저장한다. 발급자는 비밀값 x를 이용하여 A, A_c, B 값을 식 1)~3)과 같이 계산하고, 서버의 임의의 값 y과 함께 서명값(식 4))을 사용자의 어플리케이션에 전송한다.

$$A \leftarrow h(ID_i \oplus x) \text{-------} \quad 1)$$
$$A_c \leftarrow h(ID_i \oplus x) \oplus h(ID_i) \oplus h(PW_i) \text{-------} \quad 2)$$
$$B \leftarrow h(x) \oplus h(PW_i) \oplus h(h(ID_i) \oplus x) \text{ -------} \quad 3)$$
$$sig_r = S(h(I \| I_c \| R_i \| y)) \text{-------} \quad 4)$$

4) 사용자의 어플리케이션은 서버로부터 받은 값을 이용하여 서버의 서명이 맞는지 검증한다. 검증이 확인되면 A, A_c 값과 자신의 ID_i, PW_i값을 이용하여 서버로부터 받은 값을 확인한다. B, y의 값은 모바일 폰에 저장하여 두고 발급 프로토콜에 사용토록 한다.

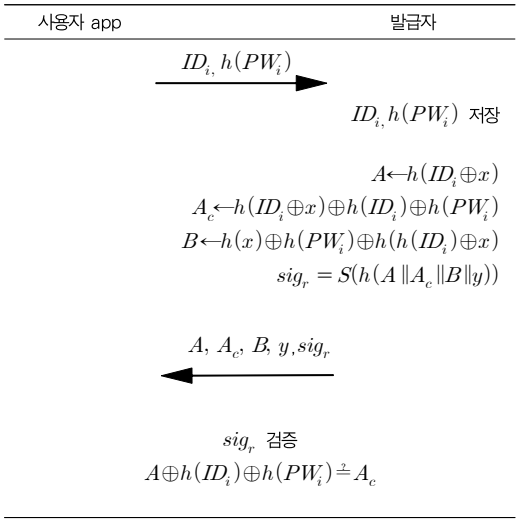


그림 3. 등록 프로토콜
Fig. Registration protocol

2.2 발급 프로토콜

1) 사용자는 쿠폰 어플리케이션을 이용하여 발급자에게 쿠폰 요청을 위하여 먼저 C_{ID_i}, V, X 값을 계산한다. X는 사용자의 어플리케이션에서 임의의 값으로 선택하고, 등록 단계에서 서버로부터 받아 저장해둔 B, y의 값을 이용하여 V, C_{ID_i}값을 다음의 식 5)~6)과 같이 계산한다.

$$V \leftarrow h(X \oplus y) \oplus h(ID_i) \text{-------} \quad 5)$$

$$C_{ID_i} \leftarrow h(B \oplus h(PW_i) \oplus h(y \oplus X)) \text{-------} \quad 6)$$

계산이 완료되면 쿠폰의 횟수를 인증받기 위한 해쉬체인 생성을 위하여 임의의 w_n값을 생성하고 $i = n-1, n-2, ..., 1, 0$에 대하여 식 7)과 같이 계산한다.

$$w_i = h(w_{i+1}) \text{-------} \quad 7)$$

2) 사용자는 발급자에게 C_{ID_i}, V, X, w_0 값을 전송한다.

3) 발급자는 사용자로부터 받은 값 C_{ID_i}, V, X와 자신의 임의의 값 y를 이용하여 사용자의 가명 ID인 C_{ID_i}값을 확인한다.

$$Y \leftarrow V \oplus h(X \oplus y) \text{-------} \quad 8)$$

$$Y_1 \leftarrow h(x) \oplus h(Y \oplus x) \text{-------} \quad 9)$$

$$C_{ID_i} \stackrel{?}{=} h(Y_1 \oplus h(y \oplus X)) \text{-------} \quad 10)$$

사용자의 가명 ID 인증에 성공하면 w_0값과 함께 발급자의 데이터베이스에 가명 ID를 저장하고 인증이 완료되었음을 사용자에게 알린다.

4) 발급자로부터 확인 메시지를 받은 사용자는 쿠폰 값에 대한 결제를 수행하고 결제내역을 발급자에게 전송한다.

5) 발급자는 쿠폰(N_C)을 생성하고 이를 동형암호를 이용하여 암호화한 $Coup = E_{H_k}(N_C)$과 서명값 sig를 생성하여 이를 사용자에게 전송한다.

6) 사용자는 서명값 sig을 확인하고 발급받은 암호화된 쿠폰 $Coup = E_{H_k}(N_C)$을 어플리케이션에 저장한다.

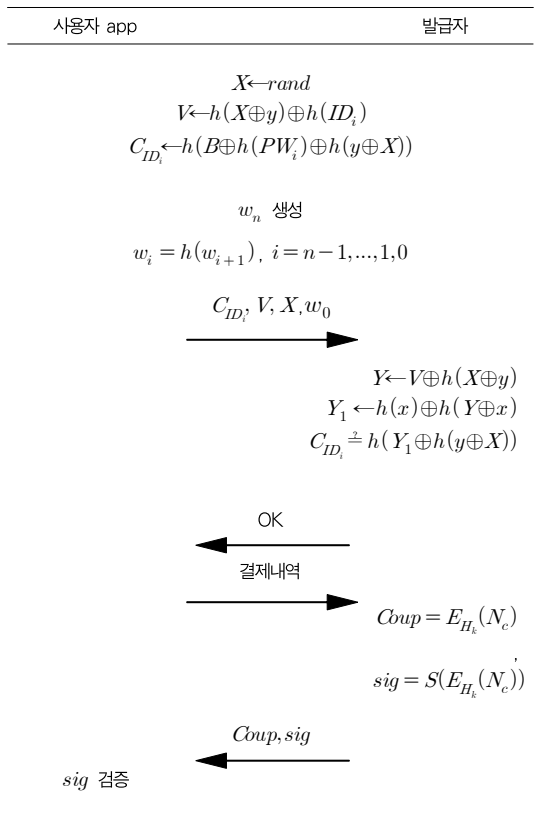


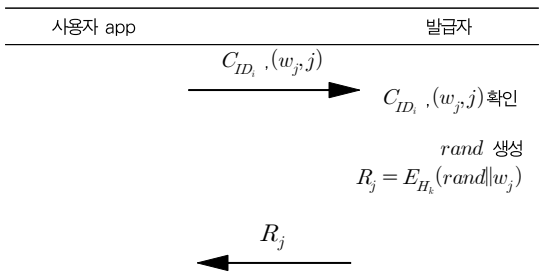
그림 4. 발급 프로토콜
Fig. 4. delivery protocol

2.3 상품 교환 프로토콜

1) 사용자는 어플리케이션에 쿠폰 사용 요청을 한다.
2) 쿠폰 어플리케이션은 사용자의 인증정보 C_{ID_i} 와 (w_j, j) 값을 발급자에게 보낸다. j의 값은 사용자의 쿠폰 사용 횟수에 관한 정보이다.
3) 발급자는 사용자의 가명 ID인 C_{ID_i}값을 확인하고 j값을 이용하여 횟수 초과 사용 여부를 확인한다. 횟수가 초과되지 않았을 경우, 즉 j의 값이 데이터베이스에 저장되어 있는 값보다 클 경우, 발급자의 서버는 해쉬 함수를 j번 돌리는 $w_j = h^j(w_0)$을 수행하여 w_j를 계산하고 사용자 C_{ID_i}가 보낸 값이 맞는지 확인한다. 인증 정보에 대한 검증이 되면 랜덤 값$(rand)$을 생성하고 이번 쿠폰의 해쉬 체인값인 w_j을 이용하여 $R_j = E_{H_k}(rand \| w_j)$를 생성하여 사용자 어플리케이션에게 전송한다.
4) 어플리케이션은 저장되어 있는 암호화된 쿠폰값과 랜덤 값을 같이 계산하고 새로운 쿠폰 정보를 생성한다.

$$Coup \otimes R_j = E_{H_k}(N_c) \otimes E_{H_k}(rand \| w_j) \text{------} \quad 11)$$

5) 어플리케이션은 생성된 새로운 쿠폰값의 해쉬값 $Coup_j = h(E_{H_k}(N_c \otimes (rand \| w_j))$ 으로 바코드를 생성한다.
6) 상점은 바코드를 스캔하여 스캔한 값을 발급자에 보낸다.
7) 발급자는 상점으로부터 받은 $Coup_j$ 값에서 N_c과 $rand$, w_j값을 확인하여 유효성을 검증한다.
8) 검증이 성공하면 사용자는 상품을 받는다.



$$Coup_j = Coup \otimes R_j = E_{H_k}(N_c) \otimes E_{H_k}(rand \| w_j) = E_{H_k}(N_c \otimes (rand \| w_j))$$

$$bcode - Coup_j = C_{ID_i} \| h(Coup_j) = C_{ID_i} \| h(E_{H_k}(N_c \otimes (rand \| w_j))$$

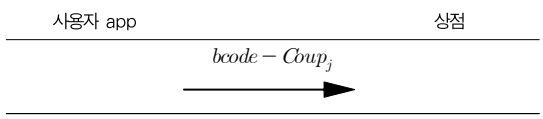


그림 5. 상품교환 프로토콜
Fig. 5. redemption protocol

3. 시스템의 분석

3.1 시스템의 안전성 분석

제안한 모바일 쿠폰 프로토콜의 안전성은 다음과 같다.

1) 인증 및 권한

사용자는 발급자에게 등록시에 회원가입을 위하여 ID와 PW정보를 발급자에게 등록한다. 이후 사용자는 프로토콜에서 이용된 가명의 ID를 발급하여 이용함으로써 사용자의 최소한의 정보가 프로토콜 상에서 교환되도록 설계하였다. 사용자는 등록 당시의 발급자가 제공한 정보를 토대로 가명 ID를 생성하고 이에 대한 인증이 발급자의 서버에서 성공적으로 이루어질 수 있으므로 사용자를 인증할 수 있으며, 사용자는 발급자의 제공 정보를 발급자의 서명을 통하여 인증할 수 있다.

2) 위조 방지

제안 프로토콜은 사용자가 쿠폰 사용을 하기 위해서는 발급자가 생성한 쿠폰을 그대로 이용하는 것이 아니라 매회 발급자가 발급해준 새로운 값$(rand)$을 이용하여 쿠폰에 재생성해야 한다. 쿠폰을 다회 이용하기 위해서 사용 시점마다 사용자는 발급자의 도움으로 쿠폰을 재생성하게 되며, 쿠폰 재생성시 필요한 정보는 발급자만이 알 수 있는 암호화키를 이용하여 암호화되어 전송되고 계산되므로 제 3자는 정당한 쿠폰을 생성해낼 수 없다. 또한 사용자는 쿠폰 사용횟수를 확인할 수 있는 해쉬 체인을 생성하고 이를 프로토콜에서 이용하는데 전송되는 해쉬 함수의 특성으로 인하여 해쉬 체인의 일부 정보를 이용하여 해쉬 체인의 정당한 다른 값을 생성할 수 없기

때문에 제 3자는 사용자를 위장하여 쿠폰을 이용할 수 없다.

3) 부인방지

발급자는 서명을 통하여 쿠폰을 발급했음을 증명하며 사용자의 해쉬 체인 값이 새로운 쿠폰 생성시에 삽입되게 되므로 사용자도 쿠폰 발급과 사용에 대한 부인을 방지할 수 있다.

4) 이중사용 방지

바코드 형태의 쿠폰은 이미지를 복사하거나 사용한 쿠폰을 다시 사용할 수 있다. 제안한 프로토콜에서는 사용시마다 발급자로부터 쿠폰 재생성에 필요한 임의의 값($rand$)을 받아 쿠폰을 재생성해서 사용해야 하며, 사용자는 사용횟수에 따른 해쉬체인의 w_j값을 이용하여 매번 새로운 쿠폰 정보를 제공해야 한다. 쿠폰 사용시마다 매번 새로운 정보가 재생성되는 쿠폰에 추가되기 때문에 사용자는 기 생성된 쿠폰을 이중 사용할 경우 그 유효성을 입증 받을 수 없으므로 이중사용을 방지할 수 있다.

3.2 시스템의 효율성 분석

제안 프로토콜은 복잡한 암호화의 계산이나 복호화의 계산은 모두 발급자의 서버에서 계산을 수행한다. 모바일 기기에서는 해쉬 연산과 동형암호화 수행을 위한 연산, 그리고 가명 ID생성을 위한 XOR 연산을 수행하게 된다.

프로토콜의 수행 중에 모바일폰에서는 발급자가 생성한 정보에 대한 발급자의 서명을 확인하는 연산을 제외하고는 암호화, 복호화 연산과 지수 연산 등을 수행하지 않고, 동형 암호의 종류에 따라 곱셈 또는 덧셈 연산을 수행하도록 설계하였다. 또한 사용자 편의를 위하여 상품교환 프로토콜에서는 사용자의 어플리케이션에서 바코드 생성이 가능하도록 설계하여 사용자가 쿠폰 어플리케이션에서 바로 바코드를 사용하고 이를 상품 구매시 결제에 이용할 수 있도록 설계하였다.

IV. 결 론

본 논문에서는 안전하게 이용할 수 있는 모바일 전자쿠폰 프로토콜에 관하여 제안하였다. 모바일 전자쿠폰 프로토콜은 다회 사용 가능하며, 해쉬체인을 이용하여 이중 사용과 부인, 위조 등으로부터 발급자의 권리를 보호할 수 있다. 또한 모바일 전자쿠폰의 위조 방지와 이중 사용 방지를 위하여 발급자가 제공하는 정보를 이용하여 매회 사용 시 쿠폰정보를 재생성하도록 설계하였다. 그러나 쿠폰 정보 재생성을 위한 암호화 연산은 동형암호를 이용함으로써 모바일 기기에서는 시간이 오래 걸리는 암호화와 복호화 계산을 배제하고 서버에서 새로운 정보를 생성하여 제공할 수 있게 하였으며 모바일 기기에서는 비트연산과 해쉬 연산만으로 안전한 쿠폰 프로토콜이 설계되도록 하였다.

참고문헌

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

[2] S. M. Jeong, "Factors Affecting Consumers' Response To Mobile Coupon", Graduate School, Ch onnam National University, 2011.

[3] C. Blundo, S. Cimato and A. D. Bonis., "A Lightweight Protocol for the Generation and Distribution of Secure E-coupons", Proceedings of the 11th international conference on World Wide Web, pp.542-552, 2002.

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

[5] 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.

[6] 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, VOL.6 No.1, 2006.

[7] Feng Bao, "A Scheme of Digital Ticket for Personal Trusted Device," Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004), Vol. 4, pp. 3065-3069, 2004.

[8] H. Park, J. Park, "Secure mobile couponing process Scheme", Review of KIISC v.20, n.6 , 2010.

[9] Rivest and A. Shamir. "PayWord and MicroMint: Two simple Micropayment schemes." Security Protocol, LNCS 1189, pp69-87, 1996.

[10] N. S, Jho, K, Y, Jang, "Trend and Issue on homomorphic encryption", weekly IT Brief, Vol.1522, pp.15-25, 2011.

[11] 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.

저 자 소 개

용 승 림

1998: 이화여자대학교 전자계산학과 공학사.

2000: 이화여자대학교 컴퓨터공학과 공학석사.

2006: 이화여자대학교 컴퓨터공학과 공학박사

현 재: 인하공업전문대학 컴퓨터시스템과 교수

관심분야: 컴퓨터공학, 알고리즘, 정보보안

Email : slyong@inhatc.ac.kr