Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.275

NFC mCoupon 서비스를 위한 경량화 서명 기법에 관한 연구*

박 성 욱,† 이 임 영‡
순천향대학교 컴퓨터소프트웨어공학과

A Study on Light-weight Signature Scheme for NFC mCoupon Service*

Sung-Wook Park,† Im-Yeong Lee‡
Department of Computer Software Engineering Soonchunhyang University

요 약

최근, 모바일과 NFC의 결합은 NFC 서비스 시장의 활성화를 위한 큰 추진력을 불러 일으켰다. 특히 NFC를 사용한 mCoupon 서비스는 다양한 소비자 마케팅에 활용되고 있다. 일반적으로 mCoupon과 같은 전자 형태의 쿠폰은 일반적인 종이 형태의 쿠폰과 크게 다르다고 할 수 있다. 종이 쿠폰과 달리 보호되지 않은 데이터 형태의 전자 쿠폰은 누구나 쉽게 큰 비용을 소모하지 않고 복사를 하거나 불법적인 수정이 가능하기 때문이다. 그러나, NFC 서비스 트렌드를 쫓기 바쁜 국내 업체들은 보안상 검증되지 않은 NFC 서비스 시장 활성화에만 열을 올리고 있으며, NFC 태그의 제한된 자원과 기존 기술로는 NFC 서비스에서 발생하는 보안위협에 모두 대처하기 어렵다. 따라서 본 논문에서는 제한된 자원을 사용하는 NFC 모바일 결제 환경에서 부정한 사용으로부터 보호되는 경량화 서명 기법에 대하여 제안한다.

ABSTRACT

Recently, the combination of mobile and NFC aroused great momentum for Activation of NFC services market. Especially, mCoupon service using NFC has been utilized in a variety consumer marketing. However, mCoupons differ significantly from paper-based coupons because unprotected data can be easily copied or modified without significant cost by anyone. A high number of uncontrolled copies of coupons can result in a significant loss. In this paper, we proposed a light-weight signature scheme that is protected against illegal use in nfc mobile payment environment to using limited resources.

Keywords: NFC, mCoupon, Light-weight, Authentication, Digital Signature

I. 서 론

NFC(Near Field Communication)는 13.56MHz대역의 Short range high frequency를 이용한 전자태그(RFID)의 하나로 특히 스마트 폰과의 융합을 통해 단말 간 read/write가 가능한 양방향 데이터통신을 제공한다. 또한, 기존 비접촉식 스마트카드 기술 및 RFID:Radio Frequency Identification과의 상호 호환성을 제공하며 암호화 표준(NFC-SEC)의 적용으로 데이터 통신간의 안전성을 제공하는 등의 장점들로 인해 새로운 응용비즈니스 모델 적용이 가능할 것으로 분석되고 있다[1].

NFC의 이와 같은 속성은 모바일 쿠폰으로 사용하기에 매우 적합하다고 할 수 있다. 이러한 이유로 최근 업계에서는 NFC 특성을 활용하여 다양한 모바일

접수일(2013년 11월 13일), 수정일(2014년 3월 26일), 게재확정일(2014년 3월 27일)
* 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2013R1A1A2012940)
† 주저자, swpark@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr(Corresponding author)

Table 1. Comparative Analysis of eCoupon and mCoupon

보너스 위치		eCoupon		mCounpon	
		실제 매장	인터넷	실제 매장	커뮤니티
취득 방법		download→print	download	download	download
		E-mail→print	E-mail	SMS	SMS
발행자 관점	발행가격	낮음	낮음	낮음	낮음
	유통가격	낮음	낮음	높음	높음
	유통량	큼	큼	고정적	고정적
	게시(발행) 형태	개인/인가	개인	개인/인가	인가
	자체시스템	x	o	x	x
사용자 관점	획득 난이도	쉬움	쉬움	쉬움	쉬움
	휴대성	어려움	어려움	쉬움	쉬움
	보너스신청	불편함	일반적	불편함	편리함
	즉시신청여부	x	o	x	o

쿠폰 서비스를 활성화 하고 있다. NFC 태그를 부착한 신문이나 스마트 포스터가 그 예이다. NFC 서비스 활용의 대표 주자인 Google사는 소셜 커머스와 NFC를 결합한 'Google Offers'라는 서비스를 시작하였고 이는 온/오프라인에서 폭발적인 강세를 띨 것으로 예상하고 있다.

이에 따라, NFC 서비스 트렌드를 쫓기 바쁜 국내 업체들은 보안상 검증되지 않은 NFC 서비스 시장 활성화에만 열을 올리고 있으며, 이는 NFC 기반 쿠폰 서비스 사용의 증가에 따른 다양한 보안상 침해요소에 대해 대처하기 힘들 것으로 예상된다. 여기서 발생하는 피해 대상은 일반적인 금융사고와는 달리 일반 사용자가 아닌 기업이다. 악의적인 목적을 가진 공격자에 의한 쿠폰 위조나 이중사용, 부정행위 등으로 인해 기업 측에 금전적인 피해가 발생할 수 있다[6]. 이처럼 NFC 기반 비즈니스 모델은 다양한 위협이 존재하지만, NFC 시장 동향과는 달리 관련 기술 연구는 미흡한 실정이다. 특히 mCoupon 연구에서 제안된 기존 방식들은 다양한 보안상 취약점 및 결함이 존재한다. 공개키 방식이 적용되지 않은 Hsiang 등[5]의 방식의 경우, 사용자가 악의적인 목적으로 타 사용자들의 ID를 수집하는 경우 수집된 타인의 ID를 이용하여 쿠폰을 무한히 생성하는 것이 가능하다.

따라서 본 논문은 2장에서 기본적인 쿠폰 생성방식에 대해 알아보고 기존에 연구된 NFC기반의 mCoupon 기법들에 대해 분석한다. 3장에서는 기존에 연구된 mCoupon의 보안요구사항에 대해 알아보며 4장에서 보안요구사항을 만족하는 제안방식을 기술한다. 5장에서는 보안요구사항에 의한 제안방식을 분석하고 마지막으로 6장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 모바일 쿠폰에 대해 설명하고 기존에 연구된 NFC기반 mCoupon 인증 방식에 대해 분석한다.

2.1 기존 mCoupon 연구

일반적인 전자형태의 eCoupon은 인터넷을 통해 발행되며 사용자가 이를 다운로드하고 인쇄하여 사용한다[15]. 종이 쿠폰에 비해 eCoupon은 게시 및 배포 비용이 낮고, 전달 속도가 매우 빠르며, 타겟 고객에게 바로 전달될 수 있으며, 소비자가 원격으로 전자쿠폰을 다운로드할 수 있다는 장점을 가진다. 하지만 eCoupon을 발급받는 방법에 있어 사용이 번거로우며, 쿠폰 사용 시 모든 매장에서 사용자가 쿠폰을 인쇄해 올 것을 요구한다. 그 외에 보안상의 다양한 위협들이 존재한다[2]. 이러한 현시점에서, 최근 m-Commerce 시대가 도래함에 따라 모바일 플랫폼이 많은 전자 상거래의 움직임을 주도하기 시작했다. 이에 따라 효율적인 마케팅을 위해 e쿠폰은 모바일을 활용한 mCoupon 형태로 발전하였다[3,4,5].

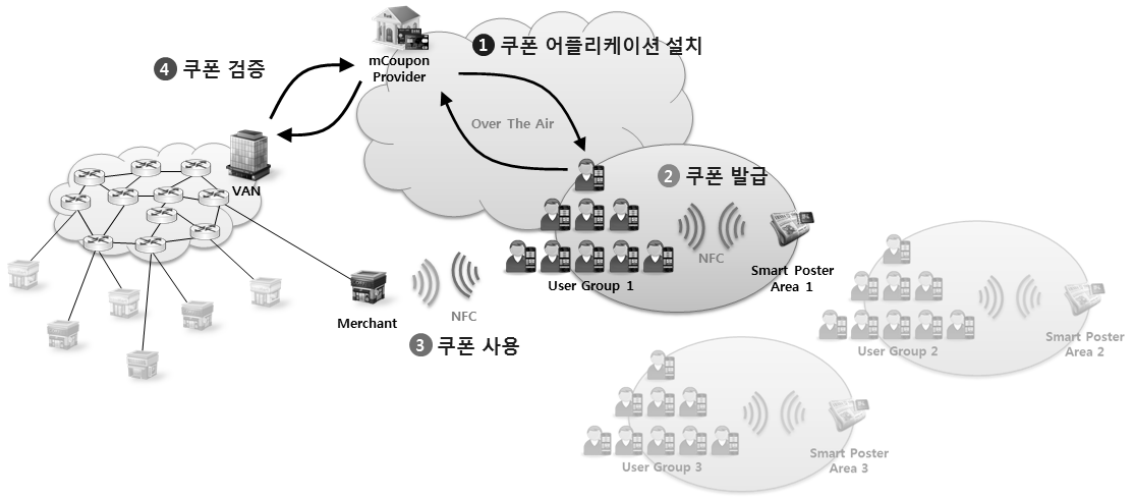


Fig.1. mCoupon Scenario

2.2 쿠폰의 분류

쿠폰은 아래와 같이 네 가지 범주로 분류할 수 있으며 eCoupon과 mCoupon을 〔Table 1〕과 같이 비교 및 분석한다〔6〕. 본 논문에서는 "NFC 기반 포스터 형태의 발행" 방식을 중점으로 분석한다.

- SMS 형태로 이통사에 의해 게시되는 방식
- mCoupon을 판매하는 웹사이트
- LBS 기반의 mCoupon 전송 방식
- NFC 기반의 포스터에 의한 발행

2.3 쿠폰 프로세스

쿠폰 프로세스는 Delivery(발급), Redemption (상품교환), Clearing(청산)의 3가지 과정으로 이루어진다〔4,5,6〕. 발급 단계는 사용자가 쿠폰을 발급받는 과정으로 Pull(요청)과 Push(전송)의 과정으로 구성된다. Pull은 사용자가 모바일 쿠폰을 발급 받기 위해 관련 어플리케이션을 다운로드하고 요청 메시지를 보내며 Push는 사용자의 요청에 대해 쿠폰을 사용자에게 전송한다. 다음은 상품교환 단계로 사용자가 쿠폰을 통해 상점에서 물품을 받는 과정이다. 사용자가 쿠폰을 상점에 제시하면 상점은 비치된 스캐너로 쿠폰의 바코드를 스캔하고 그것을 인증하기 위해 중앙 데이터베이스에 접속한다. 이러한 인증 절차를 거쳐 유효한 쿠폰임이 입증되면 사용자는 상품을 수령하게 된다. 마지막으로 청산 단계는 구매 완료 후, 상점은 완벽한 구매증거(proof of purchase)를 은행이나 특정 금융기관 같은 청산소(clearing house)에 보낸다. 청산소(clearing house)는 쿠폰에 대한 구매 증거를 확인하고 상점에게 해당 금액을 지불한다.

2.4 기존 인증기술 연구

일반적인 mCoupon 발행 흐름도는 〔Fig. 1〕과 같다. 사용자는 Provider를 통해 쿠폰 어플리케이션을 다운받고 Smart Poster를 통해 쿠폰을 받급 받는다. 이후 사용자는 상점을 통해 쿠폰을 사용하며, 상점은 사용자로부터 받은 쿠폰을 Provider에게 전송하여 검증을 요청한다. 기존에 제안된 mCoupon은 보호되지 않은 데이터로 인해 쉽게 복사되거나 추가 비용 없이 변경하는 것이 가능하다. 2007년 Dominikus 등은 mCoupon에 대한 보안 공격 가능성을 설명하고 이를 해결하기 위한 기법을 제안하였다〔3,4〕. 그러나 해당 기법들은 NFC 태그를 전혀 고려하지 않았다. 즉, 연산량과 통신량이 매우 높아 실제 NFC 태그 상에서 구현이 불가능하다. 이후 2009년 Hsiang 등은 Dominikus 방식의 문제점을 해결하기 위한 해시 기반의 새로운 기법을 제안하였다〔5〕. 이 기법은 대부분의 계산을 해시연산만을 사용하므로 효율적이다. 그러나 악의적인 목적으로 정당한 사용자의 ID를 수집한 공격자는 수집된 ID정보들을 이용하여 불법 쿠폰을 생성할 수 있는 취약점을 가지고 있다. 본 연구에서는 공개키 방식의 안전성을 갖추며,

연산 효율성을 극대화 시키기 위해 기존에 제안된 Schnorr 서명기법과 Lattice기반 상호인증 스킴을 이용하여 새로운 방식의 서명 기법을 제안한다[7,8].

2.4.1 Aigner 등의 방식

본 방식은 NFC 태그와 NFC 모바일 단말기 간의 쿠폰교환단계에서 대칭키 방식으로 NFC 모바일 단말 정보 및 쿠폰 정보 교환을 수행하며 NFC 모바일 단말기와 Cashier간의 상품교환 단계에서 공개키 방식으로 쿠폰정보를 전송하여 인증을 수행하는 방식이다[3]. 하지만 본 방식은 쿠폰교환단계에서 동일한 키를 가진 제 3자에 의해 쿠폰정보(인증정보) 및 사용자의 신원식별정보가 노출되며 올바른 사용자임을 증명하기 어렵다. 또한, 통신 프로토콜 측면에서 정보량에 비해 통신횟수 및 연산량이 많아 비효율적이다.

2.4.2 Dominikus 등의 방식

본 방식은 공유된 비밀키로 데이터를 보호하고 전자서명을 통해 개체 인증을 제공하는 쿠폰 서비스를 제공하는 방법으로 서비스 이용자는 대칭키에 대한 정보를 가지지 않으며 공개키 정보만을 인증 기관에 등록한다[4]. 본 방식에서는 ISO.IEC 9798 표준 일방향 인증 스킴을 응용하여 PKI기반 서명기법을 통해 인증을 제공한다. 본 방식은 Aigner 등의 방식의 문제점을 해결하였지만, 기존 방식에 비해 통신횟수 및 연산량이 더욱 증가하여 비효율적이다.

2.4.3 Hsiang 등의 방식

본 방식은 앞서 Dominikus et al.의 제안방식을 개선한 것으로 해쉬 기반의 연산만을 사용하여 효율성을 높인 방식이다[5]. 본 방식은 기존 방식과는 달리 해쉬 연산만을 사용하므로 연산량 측면에서 매우 효율적이지만, 쿠폰의 재사용성을 방지하기 위해 보호되어야 하는 NFC 태그의 ID가 NFC 태그에 접근하는 사용자 누구나가 쉽게 얻을 수 있어 악의적인 목적으로 타 사용자들의 ID를 수집한 공격자가 수집된 타인의 ID를 이용하여 쿠폰을 무한히 생성하는 것이 가능하다.

III. 보안요구사항

본 장에서는 NFC mCoupon 환경에서의 보안위협에 대해 알아보고, 안전하고 효율적인 mCoupon 서비스를 위한 보안요구사항에 대해 분석한다.

3.1 NFC mCoupon 환경에서의 보안위협

안전한 NFC 모바일 결제 환경 서비스를 구성하기 위해서 근거리 무선 통신 환경에서 다음의 공격유형들이 고려되어야 한다.

- 중간자 공격 : Lim 등[9]은 NFC가 물리적인 특성인 사용자 중심의 Proximity 통신을 지원하기 때문에 DoS 공격 및 중간자 공격이 물리적 차원에서 어렵다고 했지만 NFC 디바이스가 통신하기 전에 비밀 값이 공유되지 않기 때문에 개체 인증(Entity Authentication)이 이루어지지 않는다.
- 도청 : Ernst Haselsteiner 등[10]은 NFC 통신이 근접한 거리에서 이루어지지만, 공격자가 이러한 RF 신호를 검색하는데 얼마나 가까워야 하는지에 대한 답은 없다고 서술하였으며 아래와 같은 위협이 존재한다.
  - RF 필드 장치 특성에 따른 위협
  - 안테나 특성에 따른 위협
  - 리시버 퀄리티에 따른 위협
  - RF Signal Decoder 퀄리티에 따른 위협
  - 공격이 수행되는 위치에 따른 위협
- 권한 없는 생성 : 공격자의 새로운 유효 mCoupon 생성에 의한 위협
- 무단 복제 : 공격자의 올바른 mCoupon 복사본에 의한 금전적 위협
- 조작 : 공격자는 mCoupon을 조작할 수 있으며, 조작된 쿠폰이 여전히 유효할 수 있음
- 다중 현금 기능 : 동일한 mCoupon을 여러 번 사용할 수 있게 함

3.2 mCoupon환경에서의 보안요구사항

본 연구에서 제안하는 안전한 mCoupon 서비스를 위해서는 아래와 같은 기본적인 쿠폰 서비스의 요구사항을 만족해야한다. 먼저 사용자에 의해 발급된 쿠폰이 저장 및 보관되어 재사용 되어서는 안 되며, 발급된 쿠폰 정보가 복호화되어 사용자에게 노출되어서는

안 된다. 또한 쿠폰 발행자(Tag 또는 스마트포스터)에게서 발행되는 쿠폰은 누구나 발급이 가능해야하며, 따라서 사실상 중간자 공격이 의미가 없고 공개키를 안전하게 전송할 필요가 없다. 다만, 사용자가 검증자(Cashier 또는 상점)의 공개키 또는 쿠폰 발행자의 공개키를 통해 쿠폰의 암호화가 이루어질 경우, 또, 사전에 분배된 공개키 일 경우 등, 인증을 위한 수단이 제공되어야 한다. 마지막으로 NFC 태그의 연산능력을 고려하여 현실적인 연산수행이 가능해야 한다. 따라서 NFC 모바일 쿠폰 서비스에서의 보안요구사항은 다음과 같다.

- 인증 및 권한 : 사용자는 자신의 단말기의 소유주이며 해당 서비스와 쿠폰을 사용할 정당한 권한을 가졌음을 입증해야 한다.
- 위조 방지 : 발급자만이 유효한 쿠폰을 제공할 수 있으며, 다른 어떠한 참여자나 공격자가 그것을 위조할 수 없다.
- 무결성 : 쿠폰의 유효기간, 수량, 제공하는 서비스와 같은 쿠폰의 컨텐츠를 사용자나 다른 공격자에 의해 변경되지 않고 전송 에러 없이 안전하게 원래와 같은 상태로 전송되어야 한다.
- 효율성 : 제한된 모바일 환경을 고려하여 연산량 측면에서 효율성을 제공하여야 한다.

IV. 제안방식

본 장에서는 NFC 모바일 환경에서의 3장의 보안요구사항을 만족하는 NFC mCoupon 서비스를 위한 Schnorr 기반 서명 기법과 Lattice 기반의 서명 기법을 제안한다. 본 제안방식에서 실제 mCoupon 결제 프로세스상의 단계는 연구 범위 밖으로 간주하며, 본 논문상에서 배제한다. 각 단계의 수행절차는 서명생성 단계와 서명검증 단계로 구성되며 내용은 다음과 같다.

4.1 Lattice기반의 서명 기법(제안 방식 1)

4.1.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

- $*$: 각각의 개체 (A : *Issuer*, B : *Cashier*)
- *Issuer* : 스마트 포스터 또는 신문 광고에 부착되는 수동형 NFC (m-Coupon 발행 역할 수행)
- *Cashier* : 상점에서 상품 또는 서비스를 제공하며 mCoupon의 유효성을 검증하는 역할 수행
- m : 암호화된 쿠폰정보
- N : 잘려진 다항식 환 $R = Z[X]/(X^N-1)$의 차수를 정하는 차원 파라미터 값(N= 소수)
- p, q : $\gcd(p,q)=1$을 만족하는 큰 소수
- f_*, g_* : $*$의 비밀키 다항식, $f_* \in L_f, g_* \in L_g$
- ${f_*}_p^{-1}, {f_*}_q^{-1}$: $*$의 f 역함수
- v_* : $*$의 공개키, $v_* = pf_{*q}^{-1} \bullet g_* \in Z_q[X]/(X^N-1)$
- L_f, L_g : 잘려진 다항식 환 R의 부분집합
- r_* : 임의의 다항식 값
- $H()$: 암호학적 해시함수

4.1.2 서명 생성 단계

서명 생성 단계는 *Issuer*가 쿠폰을 발급 하는 단계에서 수행되는 단계로 NFC Tag가 발행될 당시에 발행기관으로부터 잘려진 다항식 환 상에서 비밀키 값 f_A와 g_A, 그리고 f_A의 역함수 ${f_A}_p^{-1}$와 ${f_A}_q^{-1}$가 선택되고 *Issuer*의 공개키 v_A가 계산되어 저장되었음을 가정한다.

$A: f_A \in L_f,\ g_A \in L_g$
$A: f_{Ap}^{-1}, f_{Aq}^{-1}$
$A: v_A = pf_{Aq}^{-1} \bullet g_A \in Z_q[X]/(X^N-1)$

Step 1: *Issuer*는 임의의 다항식 r_A를 선택한다. r_A은 매회 서명 생성 시 새롭게 갱신되며 임의 생성이 어려운 환경일 경우 Seed값으로 변경하여 활용할 수도 있다.

$A: r_A \in L_r$

Step 2: *Issuer*는 쿠폰정보 m에 대한 서명과 검증정보를 생성하여 *Cashier*에게 전송한다.

$A: C = H(m \| v \bullet r \bmod p)$
$A: S = r + c \bullet f$
$A \rightarrow B: m, C, S$

4.1.3 서명 검증 단계

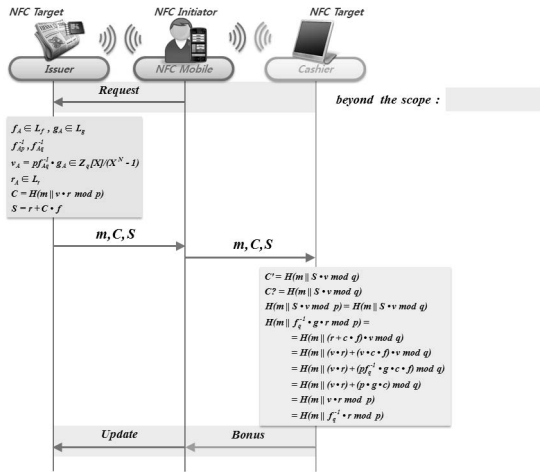


Fig.2. Proposed Scheme 1

서명검증 단계는 *Cashier*가 *Issuer*로부터 받은 mCoupon에 대한 서명을 검증하는 단계로 전달받은 m, C, S를 통해 쿠폰의 대한 무결성을 검증한다.

Step 1: *Cashier*는 *Issuer*로부터 전달받은 C와 m과 S를 이용하여 생성한 C'를 비교하여 검증을 수행하며 서명 검증 단계는 아래와 같다.

$$B: C' = H(m \| S \cdot v \bmod q)$$
$$B: C\,? = H(m \| S \cdot v \bmod q)$$
$$B: H(m \| v \cdot r \bmod p) = H(m \| S \cdot v \bmod q)$$
$$B: H(m \| f_q^{-1} \cdot g \cdot r \bmod p)$$
$$= H(m \| (r + c \cdot f) \cdot v \bmod q)$$
$$B: \quad = H(m \| v \cdot r + v \cdot c \cdot f \bmod q)$$
$$B: \quad = H(m \| v \cdot r + f_q^{-1} \cdot g \cdot c \cdot f \bmod q)$$
$$B: \quad = H(m \| v \cdot r + p \cdot g \cdot c \bmod p)$$
$$B: \quad = H(m \| v \cdot r \bmod p)$$
$$B: \quad = H(m \| f_q^{-1} \cdot g \cdot r \bmod p)$$

4.2 Schnorr 기반의 서명 기법(제안 방식 2)

4.2.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

- $*$: 각각의 개체 (A : *Issuer*, B : *Cashier*)
- *Issuer* : 스마트 포스터 또는 신문 광고에 부착되는 수동형 NFC (m-Coupon 발행 역할 수행)
- *Cashier* : 상점에서 상품 또는 서비스를 제공하며 mCoupon의 유효성을 검증하는 역할 수행
- m : 암호화된 쿠폰정보
- G_q : G_q의 위수가 소수 q인 부분군
- p : 소수(1024bit)
- g : 군의 생성자(원시군)
- x: 개인키
- y : 공개키, $y = g^x \bmod p$

4.2.2 서명 생성 단계

서명 생성 단계는 *Issuer*가 쿠폰을 발급 하는 단계에서 수행되는 단계로 NFC Tag가 발행될 당시에 발행기관으로부터 비밀키 값 x와 임의 값 w를 생성한 후 g^w를 계산하여 모두 저장되었음을 가정한다. 또한 g, y, p, q는 공개정보이다.

Step 1: *Issuer*는 쿠폰정보 m에 대한 서명과 검증정보를 생성하여 *Cashier*에게 전송한다.

$$A: C = H(m \| g^w \bmod p)$$
$$A: S = w - Cx \bmod q$$
$$A \rightarrow B: m, C, S$$

Step 2: *Cashier*에게 m, C, S를 전송 후, *Issuer*는 w값의 카운팅 증가 및 기존 g^w 값에 g를 한번 곱한 g^{w+1}값을 저장한다. 이후 $w+1$과 g^{w+1}을 다음 서명 생성 시에 사용한다.

key update

$$A: w_i = w_{i-1} + 1$$
$$A: g^{w_i} = g^{w_{i-1}+1} = g^w \cdot w$$

4.2.3 서명 검증 단계

서명검증 단계는 *Cashier*가 *Issuer*로부터 받은 쿠폰에 대한 서명을 검증하는 단계로 전달받은 m, C, S를 통해 쿠폰의 대한 무결성을 검증한다. 이 단계는 기존의 Schnorr 방식과 동일하다.

Step 1: *Cashier*는 *Issuer*로부터 전달받은 C와 m과 S를 이용하여 생성한 C'를 비교하여 검증을 수행하며 서명 검증 단계는 아래와 같다.

$$B: C = H(m \| g^w \bmod p)$$
$$B: C\,? = H(m \| g^S y^C \bmod p)$$
$$B: \quad g^w \equiv g^S y^C$$
$$B: \quad g^w \equiv g^{w-Cx} y^C$$
$$B: \quad g^w \equiv g^{w-Cx} g^{Cx}$$
$$B: \quad g^w \equiv g^w$$

Table 2. Analysis of Proposed Schemes

		Aigner[3]	Dominikus[4]	Hsiang[5]	Schnorr	제안방식 1	제안방식 2
인증		△	△	△	△	△	△
		ID 기반	ID 기반	ID 기반	ID 기반	ID 기반	ID 기반
다중 사용 방지		○	○	X	○	○	○
		DB 기반	DB 기반	쿠폰 복제 가능	DB 기반	DB 기반	DB 기반
무결성 (전자서명)		○	○	X	○	○	○
		PKI 기반	PKI 기반	해당 없음	PKI 기반	PKI 기반	PKI 기반
효율성		X	X	△	X	○	○
		지수승 기반	지수승 기반	해시 기반	지수승 기반	다항식 기반	지수승 기반
연산량	등록	1U+1E	2U+1E	2H+3Å	1U+1H+1M	2C+1H	2M+1H
	검증	1U+1E	2U+1E	2H+3Å	2U+1H	1C+1H	2U+1H
통신량	등록	4rounds	4rounds	2rounds	2rounds	2rounds	2rounds
	검증	5rounds	4rounds	2rounds	2rounds	2rounds	2rounds
○ : 좋음, 제공 △ : 보통, 부분제공 X : 나쁨, 제공안함 H(해시 연산량), E(대칭키 연산량), U(공개키 연산량) M(곱셈 연산량), C(컨볼루션 곱셈 연산량)							

V. 제안방식 분석

본 제안방식은 3장에서 도출된 보안요구사항을 아래와 같이 만족한다. 특히, 본 제안방식 효율성 측면에서 효율성을 제공할 수 있다. 첫 번째 제안방식의 경우 다항식 기반의 연산 수행으로 기존 공개키 기반에서 사용되던 지수승 연산과 비교하여 효율성이 매우 높으며, 두 번째 제안방식의 경우 g^w가 $\bmod p$에 의해 항상 잉여류 상에 존재하므로 숫자가 무한히 커지지 않아 저장 공간의 낭비가 없고 연산 효율이 떨어지지 않는다.

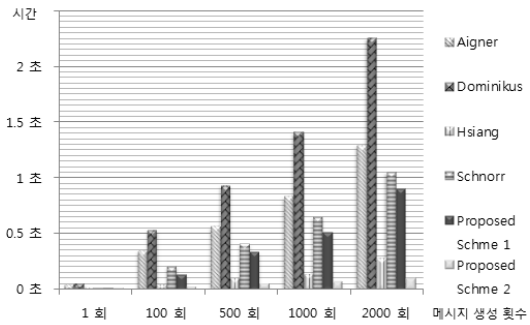
- 인증 및 권한 : 사용자는 초기 어플리케이션 설치를 통해 ID값을 할당받고 생성된 ID의 대한 서명을 통해 자신이 정당한 사용자임을 증명한다.
- 위조 방지 : 공개키 기반 서명 방식을 통해 다른 어떠한 참여자나 공격자가 그것을 위조할 수 없다.
- 이중사용 방지 : *Cashier*가 보유한 데이터베이스를 통해 한번 사용된 쿠폰이나 이미 이용한 사용자의 재사용 방지가 가능하다. 또한 서명을 통해 쿠폰과 사용자정보의 연결성을 제공하여 기존방식의 문제점이 해결되었다.
- 무결성 : *Issuer*와 *Cashier*간의 공유된 비밀키를 통해 *Offer*의 노출없이 안전한 통신이 가능하다.
- 효율성 : 단순 해시 연산 및 컨볼루션 곱셈 연산을 사용하며 NFC 태그의 연산이 매우 한정적이므로 연산량 측면에서 효율적이다.

Dominikus 등의 방식은 PKI기반의 전자서명을 사용하므로 데이터에 대한 무결성을 제공한다. 그러나 많은 양의 통신 횟수와 높은 연산량으로 인해 매우 비효율적이다. 반면 Hsiang 등의 방식은 해시 기반의 연산 및 각 단계별로 2round의 통신 횟수만을 사용하므로 효율성 측면에서 매우 우수하다 볼 수 있다. 그러나 전자 서명 기능을 제공하지 않아 데이터의 대한 무결성이 제공되지 않으며 통신상에서 사용자의 식별정보가 평문으로 전송되므로 매우 위험하다. 제안방식은 서명 생성단계에서 매 통신마다 갱신되는 임의 다항식 r에 의해 서명 값이 매 회 임의 변경되므로 공격자에 의해 중간에 노출되어도 서명이 재사용 될 수 없고, 매 회의 메시지 전송 시 변경되는 임의서명정보를 통해 공격자에 의해 메시지가 노출되어도 금전적인 피해의 발생을 막을 수 있으며, 계산량 측면에서 기존 공개키 시스템에 비해 효율성이 높아 기존에 컴퓨팅 능력이 낮은 NFC 태그에서 구동이 가능하다.

이미 기존 연구를 통해, NTRU가 RSA에 비해 암호화 과정에서 5.9배, 복호화 과정에서 14.4배, 키생성 단계에서 5배 이상 빠른 것으로 증명되었다[11,12,13,14]. 그러나 본 연구에서는 공개키 방식과 대칭키 방식, 해쉬 방식의 실제적인 연산량 비교분석을 위해 각각의 암호 알고리즘들을 구현하여 알고리즘별 연산량 및 mCoupon환경에 적용 시 연산량을 비교 측정하였다. 비교 측정에 사용되는 RSA, NTRU, SHA-1, AES의 각 암호들의 파라미터는 1024비트 RSA와 동등한 안전성을 가지도록 선택하

	Aigner	Dominikus	Hsiang	Schnorr	Proposed Scheme 1	Proposed Scheme 2
1 회	0.037 초	0.051 초	0.002 초	0.015 초	0.007 초	0.001 초
100 회	0.35 초	0.536 초	0.044 초	0.208 초	0.134 초	0.022 초
500 회	0.57 초	0.936 초	0.094 초	0.413 초	0.333 초	0.047 초
1000 회	0.835 초	1.418 초	0.136 초	0.651 초	0.51 초	0.068 초
2000 회	1.296 초	2.26 초	0.276 초	1.056 초	0.908 초	0.092 초

	Aigner	Dominikus	Hsiang	Schnorr	Proposed Scheme 1	Proposed Scheme 2
1 회	0.059 초	0.101 초	0.002 초	0.101 초	0.01 초	0.085 초
100 회	0.904 초	1.687 초	0.044 초	1.687 초	0.124 초	1.588 초
500 회	3.552 초	6.857 초	0.094 초	6.857 초	0.596 초	6.657 초
1000 회	7.224 초	13.95 초	0.136 초	13.95 초	1.286 초	13.51 초
2000 회	14.055 초	27.33 초	0.184 초	27.33 초	2.404 초	26.63 초



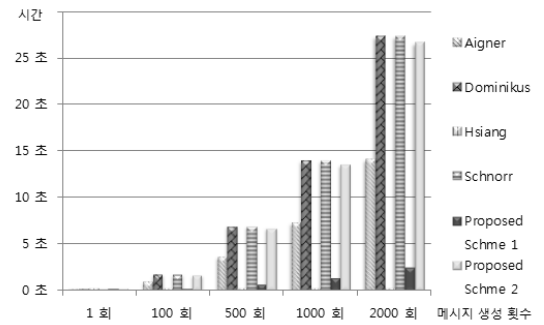


Fig.3. Comparative Analysis of Computational on the Registration phase/Verification phase

였으며 1회 암복호화 수행 시 메시지 길이를 동일하게 선택하여 적용하였다. 기존 연구에서 발표한 NTRU와 RSA의 연산량 차이에는 미치지 못하지만 (Fig.3)을 통해 〔Table 2〕에서 언급한 연산량 분석표와 유사한 결과를 얻었다는 것을 확인할 수 있다.

등록 단계에서 제안방식 1의 경우, 계산상 증명에 따르면 기존방식에 비해 연산 효율성이 높게 측정되었어야 했지만, 실제 구현결과가 계산 상 증명에 미치지 못했다. 그러나 NTRU와 RSA의 계산복잡도에 따라, 메시지 암·복호화 수행이 늘어날수록 연산량의 차이는 더욱 명확해질 것임을 확인할 수 있었고, 제안방식 2의 경우, 서명 발급 단계에서 단순 덧셈 및 해쉬 연산만이 수행되므로 연산 효율성이 가장 높다고 할 수 있다.

검증 단계에서 제안방식 2의 경우, 기존 방식과의 변화가 거의 없으므로 기존방식과의 연산량 차이가 미미하지만, 제안방식 1의 경우 기존방식들과 대비해 굉장히 높은 효율을 보여준다. 앞서 언급한 결과를 종합해 볼 때, 본 제안 방식은 경량화 인증이 필요한 서비스 환경에서 클라이언트 측면과 서버 측면에 모두 효율성을 제공할 수 있을 것으로 판단된다.

VI. 결 론

본 연구에서는 NFC 기반의 쿠폰 서비스 환경에서 서명의 재사용 방지를 위한 인증 기법을 제안하였다. 본 연구에서는 서명 생성단계에서 매 통신마다 갱신되는 임의 다항식 r에 의해 서명 값이 매 회 임의 변경되므로 공격자에 의해 중간에 노출되어도 서명이 재사용될 수 없고, 매 회의 메시지 전송 시 변경되는 임의서명정보를 통해 공격자에 의해 메시지가 노출되어도 금전적인 피해의 발생을 막을 수 있다. 또한, 다항식 섞음 시스템의 풀기 어려움에 안전성을 두고 있으므로 계산량 측면에서 기존 공개키 시스템에 비해 효율성이 높아 기존에 컴퓨팅 능력이 낮은 NFC 태그에서 구동이 가능하기 때문에 기존의 mCoupon 서비스에서의 보안요구사항을 만족하며 위조된 NFC태그로부터 사용자를 보호한다. 따라서, 제한된 디바이스의 연산량을 고려한 본 제안 방식은 NFC 모바일 환경에서 효율적인 mCoupon 서비스를 제공할 수 있을 것으로 예상된다.

References

〔1〕 Mobile NFC Technical Guidelines, GSMA, 2007

〔2〕 Garg, R., Mittal, P., Agarwal, V., and Modani, N, "An architecture for secure generation and verification of electronic coupons," In Proceedings of the Usenix Annual Technical Conference, USA, 2001

〔3〕 M. Aigner, S. Dominikus, M. Feldhofer,

"A System of Secure Virtual Coupons Using NFC Technology," PerComW'07, 2007,

〔4〕 S. Dominikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)," Proc. of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), pp.421-428, 2007.

〔5〕 HC. Hsiang, HC. Kuo, WK. Shih, "A Secure Mcoupon Scheme Using Near Field Communication," in International Journal of Innovative Computing, Information and Control, vol. 5, pp. 3901 - 3909, Nov 2009.

〔6〕 SC Hsueh, JM Chen, "Sharing secure m-coupons for peer,-generated targeting via eWOM communications," lectronic Commerce Research and Applications, Elsevier, 2010

〔7〕 CP Schnorr, "Efficient signature generation by smart cards," Journal of cryptology, Springer, 1991

〔8〕 El Moustaine, E, "A lattice based authentication for low-cost RFID," RFID-TA, Nov. 2012

〔9〕 S.H Lim, J.W Jeon, J.I Jin and O.Y Lee, "Study on NFC Security Analysis and UICC Alternative Effect," Korea Information and Communications Society, 2011

〔10〕 Ernst Haselsteiner, Klemens Breitfuß, "Security in near field communication(NFC)", Workshop on RFID Security RFIDSec, 2006

〔11〕 "A Study on the Development of Cryptosystems for the Next Generation," National Security Research Institute, 2006

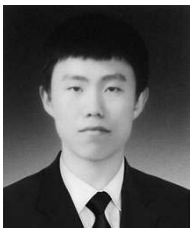
〔12〕 Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "NTRU: A ring-based public key cryptosystem," Algorithmic Number Theory, 1998

〔13〕 J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU : A Ring Based Public Key Cryptosystem," in Algorithmic Number Theory(ANTS III), 1998.

〔14〕 J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, "NtruSign : Digital Signatures using the Ntru Lattice," Topics in cryptology, 2003

〔15〕 Fortin, D. R. "Clipping coupons in cyber-space: a proposed model of behavior for dealprone consumers," Journal of Psychology & Marketing, 2000

〈저 자 소 개〉



박 성 욱 (Sung Wook Park) 학생회원
2011년 2월: 순천향대학교 정보기술공학부 졸업
2013년 2월: 순천향대학교 컴퓨터학과 석사
2013년 3월 ~ 현재: 순천향대학교 컴퓨터학과 박사과정
〈관심분야〉 NFC, 전자서명, NTRU

이 임 영 (Im Yeong Lee) 종신회원
1981년 2월: 홍익대학교 전자공학과 졸업
1986년 2월: 오사카대학 통신공학전공 석사
1989년 2월: 오사카대학 통신공학전공 박사
1989년 ~ 1994년: 한국전자통신연구원 선임연구원
1994년 ~ 현재: 순천향대학교 컴퓨터소프트웨어공학과 교수
관심분야 : 암호이론, 정보이론, 컴퓨터보안