pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.3.133

Authentication Scheme based on NTRU for the Protection of Payment Information in NFC Mobile Environment

Sung Wook Park† · Im Yeong Lee††

ABSTRACT

Recently, smart devices for various services have been developed using converged telecommunications, and the markets for near field communication (NFC) mobile services is expected to grow rapidly. In particular, the realization of mobile NFC payment services is expected to go commercial, and it is widely attracting attention both on a domestic and global level. However, this realization would increase privacy infringement, as personal information is extensively used in the NFC technology. One example of such privacy infringement would be the case of the Google wallet service. In this paper, we propose an mutual authentication scheme based on NTRU for secure channel in OTA and an zero-knowledge proof scheme NTRU based on for protecting user information in NFC mobile payment systems without directly using private financial information of the user.

Keywords : NFC Mobile Payment, NTRU, Zero-Knowledge Proof, User Authentication

NFC 모바일 환경에서 결제정보보호를 위한 NTRU 기반 인증 기법

박 성 욱† · 이 임 영††

요 약

최근 스마트 기기는 결제, 할인쿠폰 등 각종 기능을 제공하는 수단으로 진화되면서 통신과 금융이 융합된 모바일 NFC 서비스의 시장이 급성장할 것으로 전망되고 있다. 특히 모바일 NFC 결제 서비스 시장의 활성화가 예상됨에 따라 모바일 NFC 결제 서비스는 국내·외적으로 널리 주목받고 있다. 하지만 이에 따른 NFC 기술 활용 증가로 개인정보 이용이 늘면서 침해요소 또한 증가하고 있다. 최근 한국인터넷진흥원에서 발표한 "NFC 개인정보보호 대책 최종보고서"에 따르면 개인정보 암호화를 부분적으로 미지원하거나 불필요한 개인정보의 과도한 수집 및 저장 등이 문제점으로 제기되었으며 Google사의 Google Wallet 서비스의 개인정보 유출 사고 또한 이러한 문제점을 뒷받침하는 근거가 되고 있다. 본 논문에서는 기존에 서비스되고 있는 NFC 모바일 결제 서비스 상에서 결제정보의 이동 경로 별 결제 기술의 위협을 분석하고 OTA(Over the Air) 상에서 안전한 정보교환을 위한 NTRU 기반 상호인증 기법과 사용자와 은행 간의 결제 단계에서 결제정보를 직접적으로 사용하지 않고 결제자를 증명할 수 있는 NTRU기반 영지식 증명 기법에 대해 제안한다.

키워드 : NFC 모바일 결제, NTRU, 영지식 증명, 사용자 인증

1. 서 론

NFC(Near Field Communication)는 13.56MHz대역의 근거리 고주파 무선 통신을 이용한 전자태그(RFID)의 하나로 특히 스마트폰과의 융합을 통해 단말기 간 read/write가 가능한 양방향 데이터 통신을 제공한다. 또한 기존 비접촉식 스마트카드 기술 및 무선인식기술(RFID:Radio Frequency Identification)과의 상호 호환성을 제공하며 암호화 표준(NFC-SEC)의 적용으로 데이터 통신간의 안전성을 제공하는 등의 장점들로 인해 새로운 응용비즈니스 모델 적용이 가능할 것으로 분석되고 있다. 업계에서는 NFC의 주요 활용 분야 중 가장 먼저 활성화 될 분야로 "모바일 결제(Mobile Payment)"를 꼽고 있으며, 관련 업계의 관심도 모바일 결제시장으로 집중되고 있다.

Gartner에 따르면, 세계 모바일 결제 거래에서 NFC의 비중은 2009년 17%에서 2014년 30%까지 증가할 것으로 전망하고 있으며 NFC 거래량이 2009년 1억 3,800만 건에서

† 준 회 원 : 순천향대학교 컴퓨터소프트웨어공학과 박사과정
†† 종신회원 : 순천향대학교 컴퓨터소프트웨어공학과 교수
논문접수 : 2012년 8월 6일
수 정 일 : 1차 2012년 10월 15일
심사완료 : 2012년 11월 1일
* Corresponding Author : Im Yeong Lee(imylee@sch.ac.kr)

2014년 35억 7,200만 건으로 26배 증가할 것으로 전망하였다. 하지만 이와 같은 NFC 시장 동향과는 달리 실제적으로 NFC 모바일 결제 환경에서 적용이 가능한 NFC 결제 관련 기술 연구는 미흡한 실정이라고 할 수 있다. 최근 한국인터넷진흥원에 게재된 'NFC 개인정보보호대책 연구' 보고서에 따르면 현재 상용화된 NFC 결제 서비스 환경에서 신용카드 결제 시 신용카드 번호 출력방식에 따라 카드번호가 노출되는 위험이 존재하고 개인정보 암호화를 부분적으로 미 지원하거나, 상점 또는 VAN사가 불필요한 개인정보를 과도하게 수집 및 저장하는 점 등이 문제점으로 제기되었다. 또한 Google사의 Google Wallet 서비스의 개인정보 유출 사고 또한 이러한 문제점을 뒷받침하는 근거가 되고 있다.

이에 따라 본 논문에서는 기존에 서비스되고 있는 NFC 모바일 결제 서비스 상에서 결제정보의 이동 경로 별 결제 기술의 위협을 분석하고 OTA(Over the Air) 상에서 안전한 정보교환을 위한 NTRU 기반 상호인증 기법과 사용자와 은행 간의 결제 단계에서 결제정보를 직접적으로 사용하지 않고 결제자를 증명할 수 있는 NTRU기반 영지식 증명 기법을 제안하고자한다. 본 논문의 구성은 2장에서 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 기술의 소개와 관련 연구를 분석하고 3장에서는 NFC 환경에서의 보안위협과 결제 서비스를 위한 보안 요구사항을 분석한다. 4장에서는 기존 연구를 기반으로 OTA상에서 결제정보 발급을 위한 상호인증 기법과 결제단계에서 결제정보를 직접적으로 사용하지 않고 결제자를 증명 가능한 영지식 증명 기법을 제안하며, 5장에서는 보안 요구사항에 의한 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 NFC 기반 결제서비스의 구조를 분석하고, 본 연구에서 사용되는 암호기술인 NTRU와 영지식 증명에 대해 설명한다. 또한 기존의 사용자와 서버 간 제공되고 있는 인증기술과 증명자와 검증자간의 영지식 증명기법에 대하여 분석한다.

2.1 Google Wallet Service

Google Wallet Service[1]는 Google 사에서 제공하는 NFC 스마트폰 기반의 결제 서비스로 현재 미국 일부지역, 일부 상점에서 시범 서비스가 진행 중이다. 삼성의 '넥서스 S'를 시작으로 서비스 이용 가능 단말기는 추후 지원 기종 및 통신사가 확대 될 예정이며, 결제 흐름도는 Fig. 1과 같다. 결제에 관련하여 Citi Bank가 참여하고 사용자에 대한 다양한 개인정보를 각 금융·카드사, 이통사, 상점 등에서 수집을 수행한다. Google사 측에서 모든 신용카드 정보가 NFC 통신 결제 규격인 M/Chip 4(Mobile MasterCard(R) PayPassTM M/Chip 4)[2]에 의해 암호화 되고 이중 삼중의 보안 절차를 거치므로 물리적인 지갑보다 안전하다고 주장

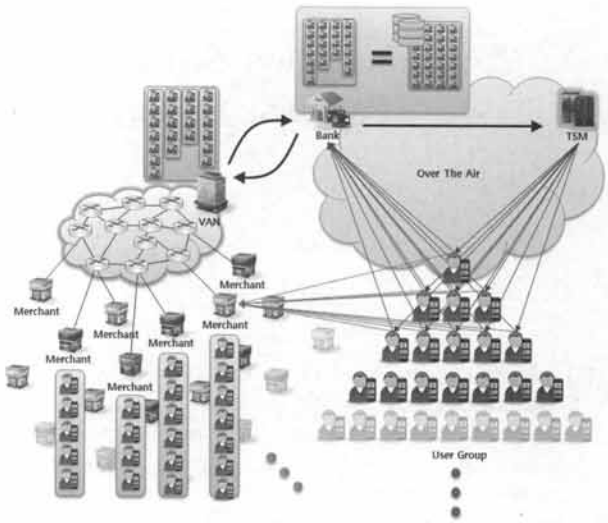


Fig. 1. Google Wallet Scenario

하고 있으나 검증된바 없으며 최근 '탈옥'하지 않은 정상적인 기기에서도 개인정보가 새나가는 문제가 수차례 발견됨에 따라 서비스의 일시적인 중단>패치>재개를 반복하고 있는 실정이다. 현재 Google Wallet Service에 적용된 PayPass의 표준 기술은 신용카드를 위한 표준 기술로서 NFC기반의 모바일 결제 흐름과 기존 신용카드 결제 흐름 자체가 유사하다. 하지만 NFC와 모바일이 융합된 NFC기반 결제환경에서는 기존의 신용카드 기반 서비스에서 제공할 수 없는 다양한 형태의 서비스 제공이 가능하므로 그 특성에 맞는 새로운 형태의 보안 기술들이 부가적으로 필요할 것으로 예상된다.

2.2 NTRU

1996년 Crypto의 럼프세션에서 Jeffrey Hoffstein 등에 의해 소개된 NTRU는 격자(Lattice) 문제를 기반으로 하는 공개키 암호 체계로 기본 연산은 다항식 환(Polynomial rings)상에서 이루어진다. 현재 IEEE에서 P1363.1로 격자 문제를 기반으로 하는 공개키 암호 표준으로 고려되고 있는 NTRU는 기존 공개키 암호 RSA, ECC(Elliptic Curve Cryptography) 등과 비교하여 동일한 안전성을 제공하면서 암·복호화 속도가 빠르다는 이점을 갖는다. 미국의 ASC X9에서는 최근 금융거래 데이터 보호를 위해 NTRU Encrypt를 사용한 X9.98이 표준으로 지정되었으며 이동 통신 사용자의 수가 점점 증가하고 전자 거래와 주식투자와 같은 높은 보안성을 요구하는 서비스가 환경에서 적합한 암호 시스템이라고 할 수 있다[3,4].

1) Truncated Polynomial Rings

NTRU는 계수가 정수이고 차수가 N-1인 다항식을 주로 사용한다.

$$a = a_0 + a_1X + a_2X^2 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

위 식에서 계수 $a_0,...,a_{N-1}$은 정수를 사용하며, 몇 개의 0을 사용할 수도 있다. 모든 다항식들의 집합은 Ring인 R에서 정의된다. R에서의 다항식은 계수를 더할 때 다음과 같이 쉽게 더할 수 있다.

$$a+b=(a_0+b_0)+(a_1+b_1)X+...+(a_{N-1}+b_{N-1})X^{N-1}$$

곱셈 또한 거의 같은 형식이지만 한 가지 다른 점이 있다. 곱셈을 할 때 X^N은 1로 대체되고, X^{N+1}은 X로 대체되며, X^{N+2}은 X^2로 대체된다. R에서의 곱셈 다항식은 다음과 같은 일반적인 식으로 정리된다.

$$a\times b=c_0+c_1X+c_2X^2+...+c_{N-2}X^{N-2}+c_{N-1}X^{N-1}$$

2) NTRU Encypt

NTRU 암호시스템은 정수 매개변수 (N, p, q)와 정수를 계수로 가지는 N-1차 다항식들의 집합들을 사용한다. q와 p는 반드시 소수일 필요는 없지만 서로소이고 q는 p보다 커야한다. NTRU Encrypt에서 사용되는 초기 키 생성 단계로는 먼저 작은 계수를 갖는 N-1차의 두 개의 다항식 $f,g\in R$을 선택한다. f는 mod p와 mod q상에서 역원이 존재해야 하며 이 역원을 f_p,f_q라고 쓴다. f는 어떤 다항식 F에 대해서 $f=1+pF$의 형태로 선택하여 $f_p=1$이 되도록 할 수 있다. f,g,f_p,f_q는 비밀로 저장된다. 공개키 h는 다음과 같이 계산된다.

$$h=f_q*g(\text{mod } q)$$

다음은 암호화를 위한 단계로 메시지 $m\in R$에 대해서, 임의의 다항식 $r\in R$을 선택한다. 메시지 m에 대한 암호문 e는 다음과 같이 계산된다.

$$e\equiv pr*h+m(\text{mod } q)$$

암호문 e에 대해서 복호화를 위해 먼저 다음을 계산하며 다항식 a는 다음과 같이 나타낼 수 있다.

$$\begin{aligned} a &\equiv f*e(\text{mod } q)\\ &\equiv f*(pr*h+m)(\text{mod } q)\\ &\equiv f*pr*h+f*m(\text{mod } q)\\ &\equiv f*pr*(f_q*g)+f*m(\text{mod } q)\\ &\equiv f*f_q*pr*g+f*m(\text{mod } q)\\ &\equiv pr*g+f*m(\text{mod } q)\end{aligned}$$

복호화 실패를 방지하기 위해서 a의 계수들은 $[-q/2,q/2]$안에 있어야 한다. 그리고, a를 이용하여 암호문 e에 해당되는 평문 m'를 다음과 같이 계산한다.

$$m'\equiv a*f_p(\text{mod } p)$$

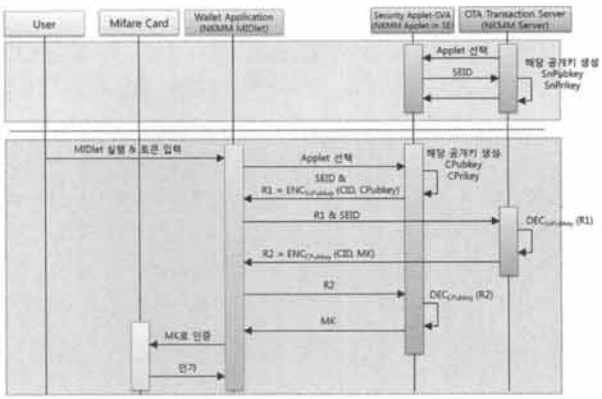


Fig. 2. NKMM Scheme

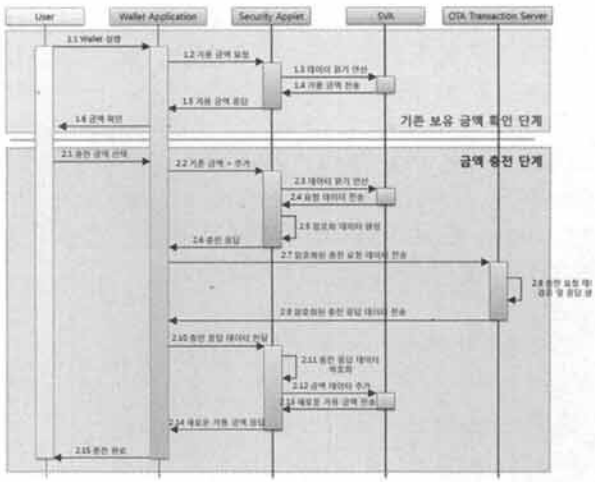


Fig. 3. NMPS Scheme

2.3 영지식 증명방식

영지식 대화형 증명 방식(ZKIPs; Zero Knowledge Interactive Proof System) 개념은 암호화 프로토콜이 '정말 안전한가?'하는 안전성 문제를 해결하기 위해 제시된 모델이다. 영지식 대화형 증명 방식은 증명자 P와 검증자 V가 대화(Interactive)를 통해 어떤 사실을 증명하는 방식으로 어떤 사실의 정당성에 관한 정보만을 전송하므로 그 외의 어떤 정보도 노출시키지 않는다는 의미를 내포한다. 즉, 증명자가 자신만이 아는 비밀정보를 검증자에게 직접 전송하지 않고 자신의 비밀정보가 아닌 다른 정보를 전송하여 검증자에게 자신만이 비밀정보를 알고 있다는 것을 증명하는 방식이다. 본 연구에서는 영지식 증명방식을 이용하여 정당한 사용자가 자신의 결제정보를 직접적으로 검증기관에 전송하지 않고 임의 정보를 통해 증명하는 기법을 제안하였다.

2.4 OTA Server와 사용자 간 인증 방식

1) NKMM

본 방식은 NFC의 3가지 운용방식 중 Read/Write 모드에 중점을 둔 방식으로 응용 프로그램 상에서 결제의 핵심 역할을 수행하는 킷값을 안전하게 관리하는 NFC 키 관리 메커

니즘이다[5]. 즉, 공유비밀키 정보를 장치에 저장하는 것이 아닌 서버에 저장하고 장치에는 필요시 서버로부터 받아오는 방법을 제시하였다. 그러나 이 방법은 NFC 내부의 중요 정보를 리더기가 접근할 수 있다는 기존의 단점을 그대로 가지며 SE영역에 대해 SEID의 법적 발행 애플릿 여부를 확인하지만 NKMM 자체를 신뢰할 수 있는 어떠한 검증 절차가 없고 전송된 데이터에 대한 검증 절차도 존재하지 않아 악의적인 목적을 가진 NKMM Server 또는 NKMM Server로 위장한 제 3자에 의한 SE영역 데이터 노출 및 수신내용 부인(거래내역 부인), 재전송 공격 등의 위협이 존재한다.

2) NMPS

본 방식은 NFC 3가지 운용방식 중 Card Emulation 모드에 중점을 둔 방식으로 SE영역에 저장되어 있는 가용 금액을 OTA 서버를 통하여 안전하게 충전하는 NFC 결제 시스템이다[6]. 본 방식은 교환되는 민감 데이터에 대해 사전에 안전한 통신을 가정하고 분배된 대칭키(AES)와 공개키(RSA)를 통해서 기밀 통신 및 데이터에 대한 무결성을 제공하지만 금전적인 거래 환경에서 필요한 상호인증 및 부인방지 기능을 제공하지 못하기 때문에 실질적인 결제 시스템 환경에 적용할 경우 다양한 위협이 존재한다.

2.5 사용자와 은행 간 사용자 증명 방식

1) Fiat-Shamir 인증 방식

Fiat-Shamir 인증 방식은 영지식 증명방식[7]과 ID정보를 이용한 암호방식[8]이 결합된 방식이다[9]. Fiat-Shamir 인증 방식의 안전성은 이차 잉여 $x^2 \equiv a \pmod{n}$상에서 n의 인수분해가 알려지지 않았을 때 제곱근을 알 수 없음에 근거한다. 본 방식은 스마트카드에서 요구되는 전체 연산수가 제일 작으나 인증 단계에서 t라운드가 수행되어야 하며 메모리를 많이 필요로 하는 문제점을 가지고 있다.

2) Guillou-Quisquater 인증 방식

GQ 인증 방식에서는 3 move 1라운드로 인증 절차를 구성하였으며, 메모리도 적게 소요된다[10]. GQ 인증 방식의 안전성은 n의 인수 분해가 알려지지 않았을 때, $A \equiv J^{l/v} \pmod{n}$을 만족하는 A를 계산할 수 없음에 근거한다. 그러나 계산량이 늘어난다는 단점을 가지고 있다.

3) Schnorr 인증 방식

Schnorr 인증 방식에서는 스마트 카드에서 수행되는 대부분의 연산을 Preprocessing단계에서 수행하여 온라인상의 연산 수를 최소화하는 방법과 지수연산을 효율적으로 수행할 수 있는 알고리즘을 제시하였다[11]. Schnorr 인증 방식의 안전성은 $v(\equiv a^{-s} \bmod p)$가 주어졌을 때 s를 구하는 것이 이산대수 문제라는 사실에 기반을 두고 있다. 본 방식은 카드에서 수행되는 온라인상의 연산수가 매우 작아 계산능력이 제한 받는 카드에서는 속도 측면에서 가장 우수하지만, 양 방향 인증이 요구될 경우 카드에서의 계산 복잡도가 증가하는 단점이 존재한다.

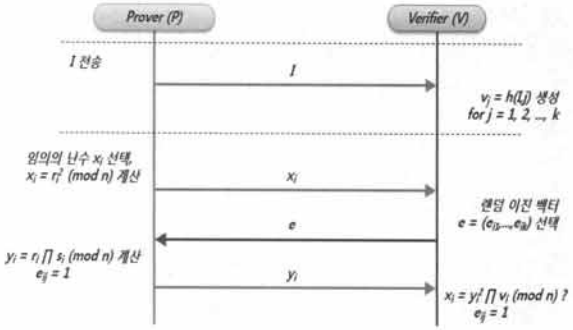


Fig. 4. Fiat-Shamir Authetication Scheme

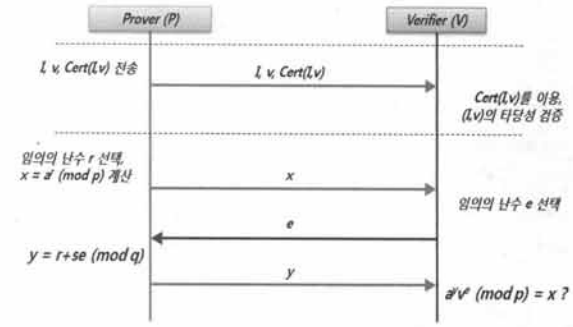


Fig. 5. Schnorr Authetication Scheme

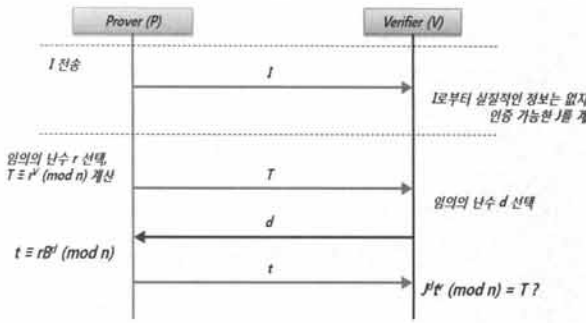


Fig. 6. Guillou-Quisquater Authetication Scheme

3. 보안요구사항

본 장에서는 NFC 모바일 결제환경에서 안전한 결제 서비스를 제공하기 위해 OTA를 이용한 MIDlet과 근거리 무선 통신 환경에서의 보안 취약성을 알아보고, 이에 따른 보안요구사항에 대해 분석한다.

3.1 NFC 모바일 기반 서비스 위협

1) 단말기 내 MIDlet 취약점에 의한 보안 위협

MIDlet은 J2ME에서 기본이 되는 어플리케이션 단위로 웹에서 구동되던 애플릿의 모바일 버전이 바로 MIDlet이다.

MIDlet은 휴대폰의 무선통신을 통해 OTA서버의 서비스와 통신을 제공받을 수 있고 JSR257와 JSR177 프로토콜을 통해 NFC 칩셋과 통신할 수 있어 NFC 모바일 환경에서 보안상 중요한 요소 중 하나라고 할 수 있다. 안전한 NFC 모바일 결제 환경 서비스를 구성하기 위해서는 다음의 공격유형들이 고려되어야 한다[12].

- 차단/방해 : 서버가 서비스를 제공하는 과정에서 발생하는 서비스 거부 공격을 수행한다.
- 도청 : 장치와 외부 서버 간의 통신이 도청되어 비밀 데이터 누출이 발생한다.
- Phishing/Spoofing/Replacing 공격 : NFC 모바일에 설치된 악성 MIDlet이 사용자가 거래하는 것을 속일 수 있으며, MIDlet과 연결된 서버 위치를 교체하여 공격한다.
- 무단 액세스 : 공격자는 사용자의 동의 없이 NFC 모바일을 무단으로 제어한다.
- 복제/재사용 공격 : NFC 모바일에 MIDlet은 disassemblers에 의해 불법으로 재사용될 수 있다.
- 데이터 손상/수정 : 저장 데이터가 삭제/손상되었을 경우 가짜 거래 정보로 수정할 수 있다.
- 데이터 변조 : NFC 모바일 칩셋 ID를 불법적으로 변조하여 인증서 데이터를 위조한다.

2) NFC 모바일과 NFC 리더기 간 보안 위협

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

- 중간자 공격 : Sun 등[13]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 개체인증(Entity Authentication)이 이루어지지 않는다.
- 도청 : Ernst Haselsteiner 등[14]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

3.2 보안요구사항

NFC 모바일 결제 환경에서 결제정보를 보호하고 사용자를 인증하기 위해선 영지식 증명 기법이 기본적으로 만족해야할 강력한 안전성이 보장되어야 한다. 또한 모바일 결제환경의 특성을 고려하여 연산량 측면에서 효율성을 제공해야 한다. 이에 따라 제안 방식에서의 보안 요구사항은 다음과 같다.

1) 영지식 증명 프로토콜 기본 요구사항

- 완전성 : 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득 시킬 수 있어야 한다.
- 건실성 : 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 한다.
- 신원확인 : 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 한다.

2) 제안방식의 보안요구사항

- 기밀성 : 통신에 사용되는 데이터들은 민감한 결제정보를 포함하고 있어, 정당한 통신객체들만이 공유되어야 하며 통신 중간에 노출되더라도 그 데이터의 값을 유추하지 못해야 한다.
- 무결성 : 통신상에서 제공되는 데이터들은 과금과 같은 금전 거래의 근거가 되므로 통신 중간에 위조 및 변조되지 않아야 한다.
- 상호인증 : 정당한 개체간의 검증을 위하여 서로간의 상호인증이 제공되어야 한다.
- 연산량 : 제한된 디바이스 환경을 위해 연산량 측면에서 효율성이 높아야 한다
- 부인방지 : 정당한 개체 간 전송된 데이터에 대한 부인을 방지하기 위해 부인할 수 없는 정보를 제공해야 한다.

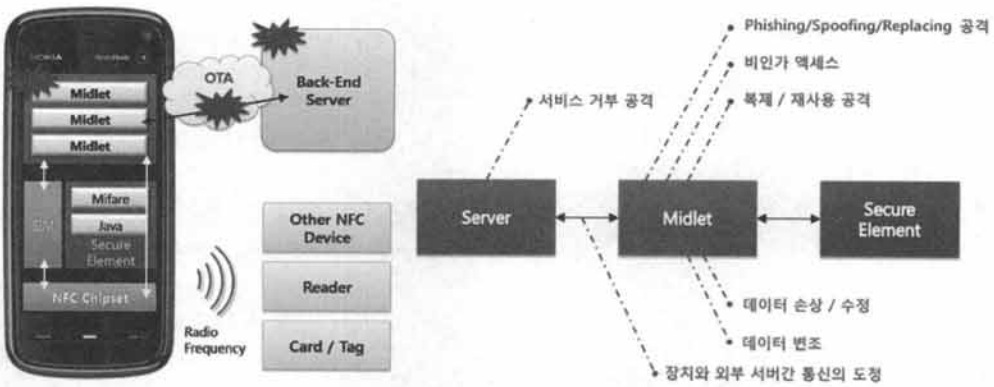


Fig. 7. Security threats that affect the vulnerability of NFC Mobiles

- 안전성 : 기본적인 영지식 증명 프로토콜의 요구사항을 만족하며 비밀정보에 대해 높은 안전성을 유지할 수 있어야 한다.

4. 제안방식

본 장에서는 보안요구사항을 만족하는 NTRU 기반 인증 기법을 제안한다. 본 제안방식은 사용자가 OTA로부터 최초로 모바일카드를 안전하게 발급 받기 위해 사용되는 사용자와 OTA간의 NTRU 기반 상호인증 기법과 결제관련 임의 정보로 결제자 자신을 은행에게 증명할 수 있는 NTRU기반 영지식 증명 기법의 순서로 설명한다.

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.

- ε : 각각의 개체 (A : *Security Applet* 또는 *User*, S : *OTA Server*, B : *Bank*)
- 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 공개 값
- $f_\varepsilon, g_\varepsilon$: ε의 비밀키 다항식, $f_\varepsilon \in L_f$, $g_\varepsilon \in L_g$
- $f_{\varepsilon p}^{-1}, f_{\varepsilon p}^{-1}$: ε의 f 역함수
- h_ε : ε의 공개키, $h_\varepsilon = pf_{\varepsilon q}^{-1} * g_\varepsilon \in Z_q[X]/(X^N-1)$
- TID : 트랜젝션 날짜와 시간을 포함한 트랜젝션 ID
- L_f, L_g: 잘려진 다항식 환 R의 부분집합
- F,G : $f_\varepsilon * G - g_\varepsilon * F = q$를 만족하는 다항식
- $*$: 순환 컨볼루션 곱(cyclic convolution product)
- ID_ε : ε의 신원확인을 위해 사용되는 ID
- $Cert_\varepsilon$: ε가 인증 기관으로부터 받은 인증서
- MK : *OTA Server*의 마스터키
- *Cash_Info* : 금액정보(가용금액, 충전금액)
- *Payment_Info* : 금융결제에 필요한 주요 사업자에 따른 결제정보
- $SEID$: Secure Element의 고유 번호

4.2 NTRU 기반 상호인증 기법

NFC환경에서의 NTRU기반 상호 인증기법을 제안한다. 본 제안방식은 키 동의단계, 결제요청 및 검증단계로 구분되며, Security Applet 및 SVA은 NFC모바일 내에 Wallet Application에 의해 관리된다. 각 단계의 수행절차는 다음과 같다. 키 동의단계에서는 사용자와 OTA Server 간 공유정보 생성을 통해 키 동의과정을 거치며 생성된 공유키를 이용하여 결제요청을 하여 검증하는 단계가 이루어진다.

1) 키 동의단계

키 동의단계에서는 *OTA Server* 인증 및 키 동의가 이루어지는 단계로 초기 파라미터값 N,p,q는 공개되어 있으며 단계는 다음과 같다.

<u>*Step1 :*</u> *Security Applet*과 *OTA Server*간의 키 생성을 위해 *Security Applet*은 잘려진 다항식 환 상에서 비밀키 값 f_A와 g_A, 그리고 f_A의 역함수 $f_{Ap}{}^{-1}$와 $f_{Aq}{}^{-1}$를 선택하고 사용자의 공개키 h_A를 계산한다. 또한 *OTA Server*도 같은 계산을 수행한다.

$$A : L_f = L(d_f, d_f), L_g = L(d_g, d_g)$$
$$A : f_A \in L_f,\ g_A \in L_g$$
$$A : f_{Ap}^{-1}, f_{Ap}^{-1}$$
$$A : h_A = pf_{Aq}^{-1} * g_A \in Z_q[X]/(X^N-1)$$
$$A : (F,G) f_A * G - g_A * F = q$$

$$S : L_f = L(d_f, d_f), L_g = L(d_g, d_g)$$
$$S : f_S \in L_f,\ g_S \in L_g$$
$$S : f_{Sp}^{-1}, f_{Sp}^{-1}$$
$$S : h_S = pf_{Sq}^{-1} * g_S \in Z_q[X]/(X^N-1)$$
$$S : (F,G) f_S * G - g_S * F = q$$

<u>*Step2 :*</u> *Security Applet*은 최초 통신을 위해 *OTA Server*에게 트랜젝션을 요청한다. 이후 *OTA Server*로부터 *OTA Server*의 인증서 $Cert_S$와 트렌젝션 ID값 TID, 서버의 식별자 ID_S, 무결성 검증을 위한 $f_S(H(TID||ID_S))$를 받고 $Cert_S$로부터 *OTA Server*의 공개키 $h_S = pf_{Aq}^{-1} * g_A \in Z_q[X]/(X^N-1)$를 얻어 TID, ID_S의 무결성을 확인한다.

$$A \rightarrow S : TID_{REQ}$$
$$S \rightarrow A : Cert_S || TID || ID_S || f_S(H(TID || ID_S))$$
$$A : H(TID || ID_S) = ?\ H(TID || ID_S)'$$

<u>*Step3 :*</u> *Security Applet*은 잘려진 다항식 환 L_r로부터 임의의 작은 다항식 r_A을 선택하고 사용자의 비밀키 f_A과 임의 다항식 r_A로부터 컨볼루션 곱을 수행하여 *OTA Server*와의 키 동의를 위한 중간 값 K_A를 생성한 후 *OTA Server*의 공개키 h_S로 K_A를 암호화한 공유키 생성정보 e_S와 $Cert_A$, TID, ID_A, $f_A(H(TID||ID_A))$를 *OTA Server*로 전송한다.

$$A : r_A \in L_r$$
$$A : K_A = f_A * r_A \bmod q$$
$$A : e_S = h_S * r_A + K_A \bmod q$$
$$A \rightarrow S : e_S || Cert_A || TID || ID_A || f_A(H(TID || ID_A))$$

<u>*Step4 :*</u> *OTA Server*는 *Security Applet*로부터 받은 *Security Applet*의 인증서 $Cert_A$로부터를 *Security Applet*의 공개키 h_A를 얻고 *Security Applet*가 보낸 TID, ID_A의 무결성을 확인한다. 이후 *Security Applet*가 생성한 공유키 생성정보 e_S를 a, b, c의 해당하는 복호화 단계를 거쳐 K_A를 얻고 h_A, g_S, r_S를 이용하여 공유키 K_{SA}를 계산한다.

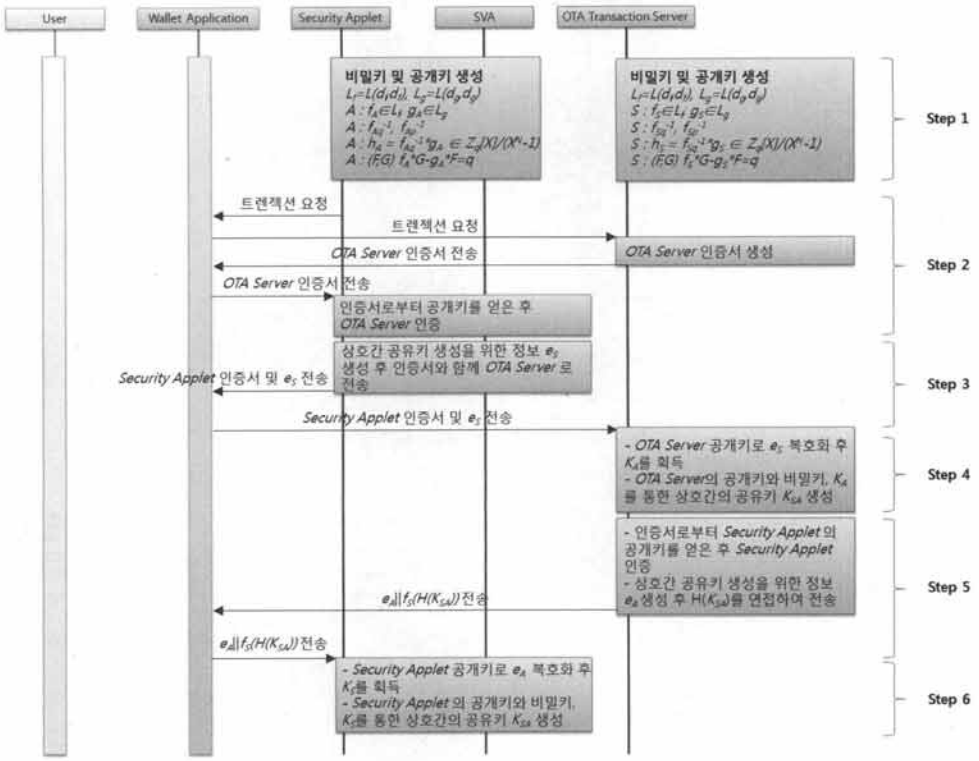


Fig. 8. Key Agreement Phase

$$
\begin{aligned}
S &: H(TID \| ID_A) = ?\, H(TID \| ID_A)' \\
S &: a = e_S * f_S \bmod q \\
&\quad = (h_S * r_A + K_A) * f_S \bmod q \\
&\quad = pr_A * g_S + K_A * f_S \bmod q \\
&\quad b = a \bmod p \\
&\quad = K_A * f_S \bmod p \\
&\quad c = f_{Sq}^{-1} * b \bmod p \\
&\quad = f_{Sq}^{-1} * f_S * K_A \bmod p \\
&\quad = K_A \\
S &: K_{SA} = H(K_A * h_A * g_S * r_S \bmod q) \\
&\quad = H(g_A * r_A * g_S * r_S \bmod q)
\end{aligned}
$$

<u>Step5 :</u> *OTA Server*는 e_A, $H(KSA)$를 연접하여 *Security Applet*로 전송한다.

$$
\begin{aligned}
S &: e_A = h_A * r_S + K_S \bmod q \\
S &\rightarrow A : e_A \| H(K_{SA})
\end{aligned}
$$

<u>Step6 :</u> *Security Applet*은 *OTA Server*로부터 받은 e_A를 통해 K_S를 획득하고 K_S를 통해 공유키 K_{SA}를 생성하여 무결성을 검증한다.

$$
\begin{aligned}
S &: K_{SA} = H(K_S * h_S * g_A * r_A \bmod q) \\
&\quad = H(g_S * r_S * g_A * r_A \bmod q) \\
A &: H(K_{SA}) = ?\, H(K_{SA})'
\end{aligned}
$$

2) 결제요청 및 검증단계

결제요청 및 검증단계에서는 사용자가 결제(충전)요청 시 데이터를 NTRUSign 프로토콜을 통해 서명하고 공유키를 이용하여 암호화한 후 *OTA Server*로 전송한다. 이후 *OTA Server*는 검증 과정을 통해 *Security Applet*의 인증 및 데이터의 무결성을 검증한다.

<u>*Step1 :*</u> *Security Applet*은 *SE*영역의 금액정보 *Cash_Info*와 *OTA Server*의 마스터키 *MK*로 암호화되어 있는 사용자의 금융결제정보 *Payment_ info* 및 *Secure Element*의 고유번호 *SEID*를 연접하여 결제정보 *D*를 생성한다.

$$A : D = CashInfo \| ENC_{MK} PaymentInfo \| SEID$$

<u>*Step2 :*</u> 사용자는 사용자의 비밀키 f_A을 사용해 서명한다. 즉, *modulo q*의 임의의 벡터 $m=(m_1, m_2)$를 생성하여 결제정보 *D*를 해쉬하고 아래와 같이 다항식 $a,b,A,B \in Z_q[X]/(X^N-1)$를 계산한다.

$$
\begin{aligned}
A &: G * m_1 - F * m_2 = A + q * B \\
&: g_A * m_1 - f_A * m_2 = A + q * B \\
&(-q/2 \le a, A\text{의 계수} \le q/2\text{의 계수})
\end{aligned}
$$

<u>*Step3 :*</u> 사용자는 사용자의 비밀키 f_A, g_A와 다항식 *B, G, F, b*를 통해 서명값 다항식 $Sig_A\{D\}$과 서명검증 중간값 T를 계산하고 *D*, $Sig_A\{D\}$를 공유키 K_{SA}로 암호화한 후 *OTA Server*로 전송한다.

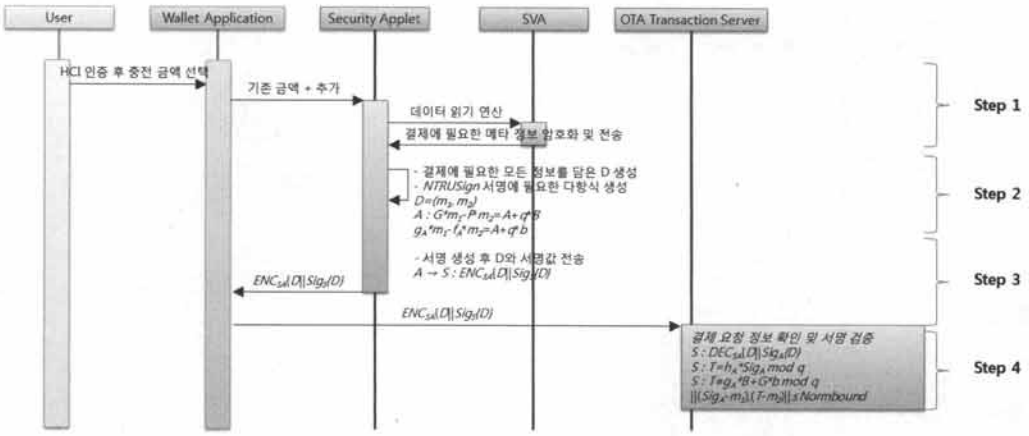


Fig. 9. Account Request and Verify Phase

$A : Sig_A\{D\} \equiv f_A * B + F * b \bmod q$
$T \equiv g_A * B + G * b \bmod q$
$A : T = h_A * Sig_A\{D\} \bmod q$
$A \rightarrow S : ENC_{SA}\{D \| Sig_A\{D\}$

<u>Step4 :</u> *OTA Server*는 데이터를 복호화 후 얻게 된 결제정보 D를 해쉬하여 $m=(m_1, m_2)$를 재생성하고 *Security Applet*의 공개키 h_A와 서명값 $Sig_A\{D\}$를 사용하여 서명검증 중간값 T를 계산한다. 이후 $Sig_A\{D\}$, T, m_1, m_2를 사용하여 다음을 확인한다.(이후 *Security Applet*도 *OTA Server*와 동일한 수행과정을 통해 서명을 검증한다.)

$S : DEC_{SA}\{D \| Sig_A\{D\}$
$S : T = h_A * Sig_A\{D\} \bmod q$
$S : T \equiv g_A * B + G * b \bmod q$
$\|(Sig_A D - m_1),(T - m_2)\| \leq Normbound$

4.3 NTRU 기반 영지식 증명 기법

NFC 모바일 결제정보보호를 위한 NTRU기반 영지식 증명 기법을 제안한다. 본 제안방식의 사용자를 은행서버에 등록하는 단계와 결제 시 금융결제정보를 상점, VAN사에 노출시키지 않고 은행에 사용자 자신을 증명하는 단계로 구성되며 수행절차는 다음과 같다.

1) 사용자 등록단계

사용자는 금융거래를 위한 사용자 등록을 다음과 같은 단계로 수행한다.

<u>Step1 :</u> 사용자(User)는 잘려진 다항식 환 상에서 비밀키 값 f_A와 g_A, 그리고 f_A의 역함수 $f_{Ap}{}^{-1}$와 $f_{Aq}{}^{-1}$를 선택하고 사용자의 공개키 v_A를 계산한다.

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

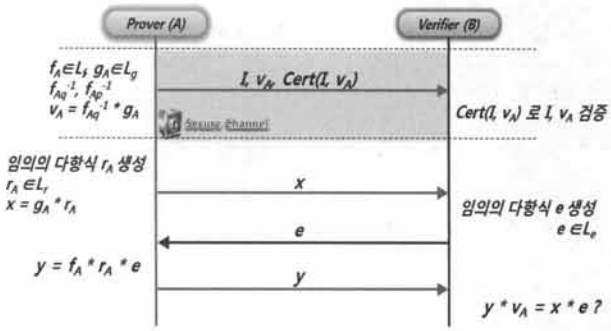


Fig. 10. Proposed Scheme

<u>Step2 :</u> 사용자는 사용자 정보와 v_A를 은행(Verifier)에 제출하고 은행은 사용자의 신원을 검사한 후 사용자 정보로 생성한 신원정보 I와 v_A를 통해 공개키 증명서 $Cert(I, v_A)$를 계산하여 사용자에게 발급한다. 이후 은행은 사용자 정보를 보관한다.

$A \rightarrow B : UserInfo, v_A$
$B : I = true$
$B : Cert(I, v_A)$

2) 사용자 신원 증명단계

사용자는 금융거래 시 자신이 정당한 금융결제정보를 보유하고 있다는 것을 증명하기 위해 다음과 같은 단계를 수행한다.

<u>Step1 :</u> 사용자는 임의의 다항식 r_A를 선택한 후 추후 사용자 증명을 위해 사용되는 $x = g_A \cdot r_A$를 계산하여 I, v_A, $Cert(I, v_A)$ 그리고 x를 은행에 전송한다.

$A : x = g_A * r_A$
$A \rightarrow B : I, v_A, Cert(I, v_A)$
$A \rightarrow B : x$

Step2 : 은행은 $Cert(I, v_A)$와 공개된 서명 시스템을 이용하여 I, v_A의 타당성을 인증하고 임의의 다항식 e를 선택하여 사용자에게 전송한다.

$B : e \in L_e$
$B \rightarrow A : e$

Step3 : 사용자는 f_A와 r_A 그리고 은행으로부터 받은 e를 통해 y를 계산하여 은행으로 전송한다.

$A : y = f_A * r_A * e$
$A \rightarrow B : y$

Step4 : 은행은 $y * v_A = x * e$인지를 검사하여 사용자를 인증한다.

$B : y * v_A = x * e$?
$B : (f_A * r_A * e) * (f_{Aq}^{-1} * g_A) = (g_A * r_A) * e$
$B : g_A * r_A * e = g_A * r_A * e$

5. 제안방식 분석

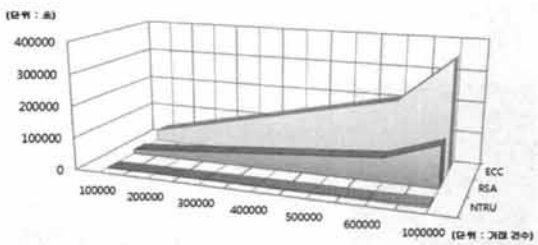
보안요구사항에 대한 제안방식 분석은 다음 Table 1과 같다.

- 기밀성 : 공격자는 상호 개체간의 공개키로 암호화된 K_A, K_S를 알 수 없고 세션키가 노출되어도 세션마다 임의로 생성되는 f_A와 r_S로 인해 통신상 기밀성을 제공한다.
- 무결성 : NTRUSign을 통해 메시지의 서명값을 생성하여 전달하였으므로 위·변조가 시도하게 되더라도 검증과정을 통해 확인이 가능하다.
- 상호인증 : $Cert_A$,S와 NTRU기반으로 생성된 공개키 쌍 중 개인키를 이용한 서명을 통해 상호인증이 제공된다.

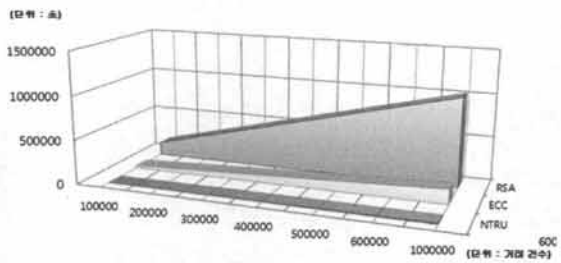
Table 1. Analysis of the Proposed Scheme

구분		NKMM[5]	NMPS[6]	제안방식
기밀성		○	○	○
		공개키 기반 통신으로 데이터 기밀성 제공	공개키 기반 통신으로 데이터 기밀성 제공	공개키 기반 통신으로 데이터 기밀성 제공
무결성		x	○	○
		서명 정보 없음	제공	제공
인증		△	x	○
		서버 위장 공격 가능성 존재	OTA 서버와 SE 간의 키교환 프로토콜 없음	제공
결제정보 직접전송 여부		x	x	○
		결제정보 전송	결제정보 전송	결제정보 기반 임의값 전송
연산량	등록	NKMM[5]	NMPS[6]	제안방식
		2M + H (일반적 방식과 동일)	2M + H (일반적 방식과 동일)	1C
	인증	FS[9]	GQ[10]	제안방식
		2M	4M	5C
통신량	등록	NKMM[5]	NMPS[6]	제안방식
		4-pass	4-pass	4-pass
	인증	FS[9]	GQ[10]	제안방식
		4-pass	4-pass	4-pass

○ : 좋음, 제공 △ : 보통, 부분제공 × : 나쁨, 제공안함
H(해쉬연산량), E(대칭키 연산량), M(모듈러 연산량), C(컨볼루션 곱셈 연산량)



	100000	200000	300000	400000	500000	600000	1000000
NTRU	700	1400	2100	2800	3500	4200	7000
RSA	12500	25000	37500	50000	62500	75000	130000
ECC	35000	70000	105000	140000	175000	210000	350000



	100000	200000	300000	400000	500000	600000	1000000
NTRU	1500	3000	4500	6000	7500	9000	10500
ECC	23800	47600	71400	95200	119000	142800	166600
RSA	145500	291000	436500	582000	727500	873000	1018500

Fig. 11. Comparison of the efficiency of the encryption algorithms

- 연산량 : 기존방식에서 사용되는 이산 대수 문제에 근간을 둔 지수승 연산과는 달리 다항식 섞음 시스템의 풀기 어려움에 안전성을 둔 단순 덧셈, 곱셈, 쉬프트 연산만을 수행하므로 연산량 측면에서 매우 효율적이다.
- 부인 봉쇄 : Security Applet의 비밀키 f_A를 통해 서명함으로써 부인 봉쇄가 가능하다.
- 안전성 : 제안 방식은 기본적인 영지식 증명 프로토콜의 요구사항을 만족하며 교환되는 정보의 검증과정을 통해 사용자가 전송한 정보의 유효성을 증명하는 것이 가능하다. 또한 공격자가 x, y를통해 g_A, f_A, r_A를 찾는 것은 큰 크기의 격자(Lattice)에서 작은 벡터를 찾는 수학 문제와 등가이므로 계산 상 불가능하다. Fig. 11은 공개키 암호의 효율성을 비교한 것이다[15]. 비교에 사용된 RSA, ECC, NTRU는 각 암호들의 파라미터를 1024비트 RSA와 동등한 안전성을 가지도록 선택하였으며 1회 결제 프로토콜 수행 시 요구 데이터 블록을 200으로 가정하여 비교 수행되었다. 위 그림과 같이 복호화 단계에서의 연산 수행속도는 NTRU가 ECC의 16배, RSA의 100배의 효율성을 보였고, 암호화 단계에서는 NTRU가 ECC의 50배, RSA의 18배에 해당하는 효율성을 나타냈다.

6. 결 론

본 논문에서는 OTA 특성을 고려하여 무선 통신 상에서 효율적인 OTA와 Client 간 상호 인증 기법과 개인의 금융정보보호를 위한 NTRU기반 영지식 증명 기법을 제안하였다. 현재 NFC 모바일 결제 시스템에서는 과금과 같은 금전 거래의 근거가 되는 민감한 데이터 교환이 무선통신 상에서 이루어지므로 안전성과 효율성이 동시에 제공되어야 한다. 본 제안방식은 기존의 다른 결제 시스템과 동일한 안전성을 제공하면서 NTRU 암호기법을 적용하여 연산량 측면에서 효율성을 제공한다. 또한 결제에 활용되는 개인의 금융정보를 결제에 직접적으로 사용하지 않고 임의의 정보를 이용해 결제자 자신을 증명함으로써 개인의 금융결제정보를 활용한 오프라인 NFC 결제 환경에서 결제정보가 중간에 노출되는 문제점을 해결하였다. 본 방식은 기존방식과 동일한 통신횟수를 가지지만 기존방식에서 사용되는 지수승 연산과는 달리 다항식 섞음 시스템의 풀기 어려움에 안전성을 둔 단순 덧셈, 곱셈, 쉬프트 연산만을 수행하므로 연산량 측면에서 매우 효율적이며 기존 방식과 동일한 안전성을 제공한다. 또한 결제 과정에서 직접적인 개인금융정보가 아닌 임의정보를 사용하므로 통신상 데이터가 노출되어도 개인정보의 노출되지 않는다. 향후 연구로는 NFC 결제 서비스 환경에서 상호 인증 가능한 영지식 증명 기법과 실제 결제 환경에서 통신 횟수를 줄이기 위한 추가적인 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] "Google Wallet: Security", Google, 2011.
[2] "MasterCard PayPass", MasterCard, 2011.
[3] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU : A Ring Based Public Key Cryptosystem", in Algorithmic Number Theory(ANTS III), 1998.
[4] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, "NtruSign : Digital Signatures using the Ntru Lattice", Topics in cryptology, 2003.
[5] HC Cheng, WW Liao, "A secure and practical key management mechanism for NFC read-write mode", IEEE, 2011. 02.
[6] G. Madlmayr, J. Langer, "Near Field Communication based Mobile Payment System", 2008.
[7] S.Goldwasser, SMicali and C.Rackoff, "The Knowled ge Complexity of Interactive Proof Systems", SIAM Journal on Computing, 18(1989), pp.186-208.
[8] A.Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp.47-53, 1985.
[9] A.Fiat and A.Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problem", Crypto'86, VFol.263, pp.186-194, 1986.
[10] L.C.Guillou and J.J.Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge", Crypto'88, pp.216-231, 1988.
[11] C.P.Schnorr, "Efficient Signature Generation by Smart Card", Journal of Cryptology, pp.161-174, 1991. 4
[12] "Mobile NFC Technical Guidelines", GSMA, 2007.
[13] S.H Lim, J.W Jeon, J.I Jin, O.Y Lee, "Study on NFC Security Analysis and UICC Alternative Effect", Korea Information and Communications Society, 2011.
[14] Ernst Haselsteiner, Klemens Breitfuß, "Security in near field communication(NFC), Workshop on RFID Security RFIDSec, 2006.
[15] "A Study on the Development of Cryptosystems for the Next Generation", National Security Research Institute, 2006.

박 성 욱
e-mail : swpark@sch.ac.kr
2011년 순천향대학교 정보기술공학부(학사)
2011년~2013년 2월 순천향대학교 컴퓨터소프트웨어공학과(석사)
현 재 순천향대학교 컴퓨터소프트웨어공학과 박사과정
관심분야 : NFC, 전자서명, NTRU

이 임 영
e-mail : imylee@sch.ac.kr
1981년 홍익대학교 전자공학과(학사)
1986년 오사카대학 통신공학전공(석사)
1989년 오사카대학 통신공학전공(박사)
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현 재 순천향대학교 컴퓨터소프트웨어공학과 교수
관심분야 : 암호이론, 정보이론, 컴퓨터보안