情報保護學會論文誌
第12券 第3號, 2002. 6

NTRU기반의 이동 통신에서의 인증 및 키 합의 프로토콜

박 현 미*, 강 상 승**, 최 영 근***, 김 순 자***

Authentication and Key Agreement Protocol based on NTRU in the Mobile Communication

Hyun-Mi Park*, Sang-Seung Kang**, Yeong-Geun Choe***, Soon-Ja Kim***

요 약

이동 통신에서의 보안은 전자 거래가 급증함에 따라 더욱 중요하게 되었다. 무엇보다도 이동 통신 환경에 적합한 인증 및 키 합의는 보안의 필수 조건이다. 이를 위하여 Diffie-Hellman, ElGamal 등의 공개키 암호 시스템을 기반으로 하는 프로토콜이 제안되었으며, 이들은 대수학의 기반 아래 이산 대수 문제 어려움을 바탕으로 이뤄지는데, 연산 속도가 느리고 키 길이가 길어 이동 통신 환경에 적용하기에는 많은 제약점이 있다. 본 논문에서는 이동 통신 환경의 제약점인 제한된 자원들, 제한된 계산력, 제한된 대역폭을 극복할 수 있는 NTRU 기반의 인증 및 키 합의 프로토콜을 제안한다. 이는 잘려진 다항식 환(truncated polynomial ring)에서 작은 수의 덧셈과 쉬프트 연산만 행하기 때문에 속도가 빠르며 키 생성이 용이하고 쉽다. 또한 NTRU 래티스 상에서의 짧은 벡터 찾는 어려운 문제(SVP/CVP)로 인해 보안성이 강하여 안전하다.

ABSTRACT

As the electronic commerce increases rapidly in the mobile communication, security issues become more important. A suitable authentication and key agreement for the mobile communication environment is a essential condition. Some protocols based on the public key cryptosystem such as Diffie-Hellman, ElGamal etc. were adapted in the mobile communication. But these protocols that are based on the difficult mathematical problem in the algebra, are so slow and have long key-length. Therefore, these have many limitation to apply to the mobile communication. In this paper, we propose an authentication and key agreement protocol based on NTRU to overcome the restriction of the mobile communication environment such as limited sources, low computational power, and narrow bandwidth. The proposed protocol is faster than other protocols based on ECC, because of addition and shift operation with small numbers in the truncated polynomial ring. And it is as secure as other existent mathematical problem because it is based on finding the Shortest or Closest Vector Problem(SVP/CVP).

Keyword : *NTRU, Authentication, Key Agreement, Mobile Communication*

* 경북대학교 정보통신학과(purehyun@palgong.knu.ac.kr)
** 한국전자통신연구원(sskang@econos.etri.re.kr)
*** 경북대학교 전자 전기 공학부(ind@palgong.knu.ac.kr, snjkim@ee.knu.ac.kr)

Ⅰ. 서 론

이동 통신 기술의 발달로 이동 통신 서비스뿐만 아니라 이동 컴퓨팅, 이동 멀티미디어 서비스 등 이동 통신 시스템을 이용한 응용 서비스 개발과 서비스 제공이 급증하면서 이용자 신분 및 위치 정보의 노출, 송수신 데이터의 도청 및 변조, 불법적인 서비스 이용 등 이동 통신 환경에서의 보안 문제 해결이 급선무로 떠올랐다. 이동 통신 환경에서의 인증 및 키 합의 프로토콜 설계 시에 이동 통신 환경이 갖는 제약점, 즉 제한된 메모리, 자원, 계산력, 대역폭을 고려해야 한다. 따라서 빠른 키 생성, 빠른 계산 속도, 적은 양의 메모리를 사용하면서도 보안성이 보장되어야 한다.

지금까지 암호 기술을 이용한 인증 및 키 설정 프로토콜이 많이 제안되었다. 이들은 적용된 암호 알고리즘에 따라 대칭키 암호 알고리즘 방식[1,2,5]과 공개키 암호 알고리즘 방식,[3,4,19] 그리고 대칭키 암호 알고리즘 방식과 공개키 암호 알고리즘을 결합한 혼합형 방식[6]등으로 분류된다. 대칭키 암호 알고리즘은 계산 속도가 빨라 이동 통신의 제약점을 잘 극복할 수 있지만, 보안성과 키 관리에 큰 어려움이 있다. 그래서 최근에는 강한 보안성을 제공하는 공개키 암호 알고리즘을 이용한 인증 및 키 합의 프로토콜이 제안한다. 공개키 기반의 인증 및 키 합의 프로토콜은 대칭키 암호 알고리즘에 비해 계산량이 많고 키 길이가 길어 효율성이 떨어지지만, 강한 보안성과 키 관리가 용이하다. 따라서 연구가 계속 진행중인 부분은 이동 통신 제약을 극복하고 강한 보안성을 갖는 공개키 기반의 인증 프로토콜이다.

기존의 공개키 기반의 인증 및 키 설정 프로토콜은 대부분 Rabin, Diffie-Hellman, ElGamal 등을 이용한다.[3,4,5,19] 이들은 대수학을 기초를 한 것으로 유한 군(finite group), 유한 체를(finite field) 바탕으로 한 어려운 수학 문제기반의 알고리즘이다. 예로 큰 두 소수의 곱으로 이뤄진 큰 수의 인수분해 문제, 이산 대수 문제 등이다. 이들은 큰 소수를 찾아야 하는 어려움으로 키 생성이 어렵고 오랜 시간이 걸린다. 그리고 생성자에 임의의 큰 수 승을 해야하므로 계산이 복잡하고 암·복호 시간이 길다. 이를 해결하기 위해 연구된 분야가 타원곡선 암호시스템(ECC)을 이용한 인증 프로토콜이다. 이로써 짧은 키를 사용하여 기존의 계산량 문제를 조금이나마 해결하였다.[3,9,8]

본 논문에서는 이보다도 더 빠른 공개키 암호 시스템을 적용하여 이동 통신 환경에서 문제시되는 제약점들을 해결하고자 한다. NTRU 암호 시스템은 CRYPTO'96년에 처음 소개된 것으로 기존에 대수학에서의 이산 대수 문제에 반해 NTRU는 다항식환(polynomial ring)에 기반을 둔 것으로 큰 크기의 래티스(lattice)에서 작은 벡터를 찾는 수학 문제이다.[9] $R=\frac{Z[X]}{(X^n-1)}$는 0과 1, -1을 계수로 갖는 $n-1$차의 다항식이다. 암호화 과정에서 모듈라 p와 모듈라 q로 독립적으로 연산되어져, 무엇보다 강한 보안성을 갖는 암호 시스템으로 기존의 암호 시스템과 비교해 빠르며 특히 최근에 연구된 ECC와 비교해 볼 때, 최저 20배에서 최고 100배까지 빠르다.[10,18] 그리고 무엇보다 주목할 만한 것은 키 생성과정이 간단하며 쉽다. 따라서 언제든지 비밀키와 공개키를 재생성 할 수 있는 특징을 갖고 있다. 그리고 저장 공간을 많이 차지하지 않아서 8비트 프로세서에도 적합하다. 한편, 다항식 환을 바탕으로 하는 큰 래티스에서 작은 벡터를 찾는 수학문제를 기반으로 한 PASS, PASS(II)와 같은 인증 프로토콜이 연구되고 있다.[11,12]

본 논문에서는 NTRU와 NTRU 서명을 이용한 인증 및 키 합의 프로토콜을 제안한다. 제안한 프로토콜은 NTRU의 특징인 다항식 환에서 다항식들의 빠른 곱과 합으로 인해 전체 프로토콜의 수행 속도가 빠르다. 또한 키 생성이 쉽고 간단하여 언제든지 키 갱신이 가능하므로 불안정한 시스템과 공격으로부터 프로토콜의 수행을 더 안전하게 할 수 있다.

먼저, 2장에서는 이동 통신이 갖는 제약점과 보안 특성을 소개하고, 3장에서는 NTRU와 NTRU 서명인 NtruSign에 대해 살펴본다. 그리고 4장에서 NTRU와 NTRU 서명을 이용하여 안전하고 효율적인 인증 및 키 합의 프로토콜을 제안하며 5장에서는 제안한 프로토콜이 만족하는 보안 요구 조건을 분석하고 성능을 평가한다.

Ⅱ. 이동 통신 환경에서의 제약점과 보안 특성

이동 통신 사용자는 언제 어디서나 보다 편리하고 안전하게 서비스 제공자가 제공하는 서비스와 자원을 이용하고자 한다.

이를 위해 이동 통신 환경에서 요구되는 보안 특성은 아래와 같다.[3,8,13,19]

1) 함축적 키 인증성

프로토콜에 참여하는 개체 A와 개체 B가 있을 때, A와 B는 공유키를 생성하는데, A는 B이외에 다른 어느 누구도 공유키를 생성할 수 없음을 확신할 수 있다. 이 경우를 A는 B에 대한 함축적 키 인증성(implicit key authentication)을 갖는다고 한다. 그리고 반대로, B는 A 이외에 다른 어느 누구도 공유키를 생성할 수 없음을 확신할 수 있다. 이 경우를 B는 A에 대한 함축적 키 인증성을 갖는다고 한다. 이 두 조건을 만족하는 경우에 인증된 키 합의프로토콜(authenticated key agreement)이라 한다.

2) 명시적 키 인증성

프로토콜에 참여하는 개체 A와 개체 B가 있다. 이들 A와 B는 공유키를 생성한다. 이때, A는 B가 실제로 공유키를 계산해 가지고 있음을 확인 할 수 있을 때, B에 대한 명시적 키 인증성(explicit key authentication)을 갖는다. 그리고 반대로 B는 A가 실제로 공유키를 계산해 가지고 있음을 확인할 수 있을 경우에 A에 대한 명시적 키 인증성을 갖는다. 명시적 키 인증성은 함축적 키 인증성에 실제로 상대방이 공유키를 계산할 수 있음을 추가하는 것이다.

3) 알려진 키에 대한 안전성

개체 A와 개체 B가 인증 및 키 합의 프로토콜에 참여할 때, 세션마다 유일한 개인키를 생성하게 되는데, 이를 세션키(session key)라 한다. 만일 이전에 다른 세션에서 공격자로부터 세션키를 공격당해 세션키가 노출되더라도 현 프로토콜이 안전함이 보장되는 것을 알려진 키에 대한 안전성(known-key security)이라 한다.

4) 상호 개체 인증

프로토콜에 참여하는 개체 A와 개체 B가 있다. 상호 개체 인증(mutual entity authentication)은 A는 B의 신분을, B는 A의 신분을 확인하는 과정이다. 이는 서로 다른 개체에 대한 가장을 방지하기 위해 필요한 것이다.

5) 갱신키 확인

이전에 사용한 메시지를 재사용할 때, 이전의 키를 재 설정하는 것을 재실행 공격(replay attack)이라고 한다. 이 공격을 방지하기 위해 키를 새롭게 설정해야한다. 이를 갱신키 확인(confirmation freshness of key)이라 한다.

여기에 이동 통신 사용자의 익명성과 전송된 정보의 부인 봉쇄가 보안 요구 조건에 추가된다.

- 이동 통신 사용자의 익명성

사용자의 위치가 고정된 유선 환경에서는 위치 정보가 그다지 중요하지 않지만, 휴대성과 편리함을 특징으로 갖는 이동 통신 환경에서는 사용자의 위치 정보 및 사용자의 활동에 대한 보안이 중요하다. 만일 정보가 노출되게 되면, 사용자의 프라이버시를 침해받게 된다. 그러므로 이동 통신 환경에서 사용자의 익명성(anonymity of mobile user)이 제공되어야 한다. 이는 통신에 참여한 개체 중에서 정보를 전송하는 상대의 공개키 또는 세션키를 이용하여 사용자 인증 정보를 암호화함으로써 이동 통신 사용자의 익명성을 제공할 수 있다.

- 전송된 정보의 부인 봉쇄

ASPeCT프로토콜과 같이 전자상거래에 적합한 프로토콜이 설계되었다. 그래서 사용자는 서비스 제공자로부터 서비스를 제공받기 위해 확인 가능한 위탁 정보를 제공할 수 있다. 그리고 사용자에게 청구된 금액이 부정확할 경우를 방지하기 위해 부인할 수 없는 정보를 제공할 필요가 있다. 이것은 디지털 서명을 사용해 만족시킬 수 있다.

이동 통신에서는 위와 같은 여러 가지 보안 특성을 만족해야 한다. 그러면서 이동 통신이 갖는 제약점인 저용량의 메모리와 같은 제한된 자원, 제한된 계산력, 제한된 대역폭에 적합한 프로토콜이 설계되어야 한다. 다음은 이동 통신 환경에 적합한 프로토콜을 설계 시에 만족시켜야하는 요구사항이다.

1) 이동 통신 측의 최소한의 연산량

이동 통신 장치는 보다 휴대하기 쉽게 더 작고 더 가벼워지고 있다. 그래서 비교적 제한된 자원, 제한된 계산 전력을 갖게 된다. 따라서 이동 통신 환경에서 통신을 위한 프로토콜을 설계할 때 이동 통신 측의 계산량을 최소화시켜야 한다.

2) 최소한의 정보 전송

이동 통신 네트워크의 제한된 대역폭과 높은 에러

율을 감안하여 메시지 전송량과 프로토콜의 패스 수를 최소화해야 한다.

Ⅲ. NTRU와 NtruSign

NTRU기반의 암호 알고리즘으로 NtruEncypt가 있으며, 서명 알고리즘으로 NtruSign, 그리고 인증에는 PASS가 있다. 이 장에서는 NTRU에 관한 전반적인 내용과 NtruSign에 관해 기술한다.[14~17]

3.1 NTRU 암호 시스템

이동 통신 사용자의 수가 점점 증가하면서 이동 통신 장치를 통해 음성통화 이상의 멀티미디어 통신이 이루어지게 되었다. 그리고 전자 거래와 주식투자와 같은 높은 보안성을 요구하는 서비스가 제공되면서 보다 안전하고도 빠른 인증 및 키 합의 프로토콜이 필요하게 되었다. 이에 맞는 암호 시스템이 NTRU 이다. 이것은 큰 크기의 래티스(lattice)에서 매우 짧은 벡터를 찾는 수학 문제(shortest or closest vector problem(SVP/CVP))를 기반으로 이루어진다. 이 시스템은 잘려진 다항식 환(truncated polynomial ring)을 기반으로 하는 수학 문제로서 작은 정수의 덧셈과 곱셈, 그리고 쉬프트(shift) 연산이 이뤄지기 때문에 수행 속도가 빠르다.[9,16,17] 그리고 키 생성이 쉽고 빨라 스마트 카드와 같은 작은 디바이스에서도 키를 쉽게 갱신할 수 있으므로 보안성이 강하다. 따라서 이것은 빠른 연산 속도와 간단하고 빠른 키 생성으로 인하여 비교적 저렴한 프로세서에서도 안전한 프로토콜을 설계할 수 있다. 여기에서는 제안한 프로토콜에 적용한 NtruEncrypt 중에서 키 생성에 관한 알고리즘을 살펴본다.[16,17] 이는 NTRU 래티스 상에서 짧은 벡터를 찾는 어려움 기반으로 이뤄졌으며 모든 연산은 $R=\frac{Z[X]}{x^n-1}$ 인 다항식 환에서 이루어진다.

1) 매개 변수

① F_f : R의 부분집합으로써, 계수가 0,1,-1로 이루어지는 다항식의 집합이다. 이 집합은 1,-1의 갯수가 d_f로 사전에 정의되어 있으며, 나머지의 계수는 0이다.

② F_g : R의 부분집합으로써, 계수가 0,1,-1로 이루어지는 다항식의 집합이다. 이 집합은 1,-1의 갯수가 d_g로 사전에 정의되어 있으며, 나머지의 계수는 0이다.

③ p, q:소수일 필요는 없으며, $\gcd(p, q)=1$를 만족하는 값이다. 그리고 q는 p보다 크다.

④ $\otimes$: 순환 컴볼루션 곱(cyclic convolution product)이다.

2) 키 생성

① 두 다항식 $f \in F_f$와 $g \in F_g$를 선택한다.

② f의 역함수 f_p^{-1}와 f_q^{-1}를 계산한다.
즉, $[f_p^{-1} \otimes f \equiv 1]_p$와 $[f_q^{-1} \otimes f \equiv 1]_q$인 f_p^{-1}와 f_q^{-1}를 계산한다.

③ $h \equiv [f_q^{-1} \otimes g]_q$를 계산한다.
공개키는 다항식 h가 되고, 비밀키는 다항식 f가 된다.

〔표 1〕은 NtruCrypt에서 사용되는 매개변수 (N, p, q)의 보안성에 따른 크기를 나타낸다.

〔표 1〕 NtruCrypt의 매개 변수(N,p,q)

매개 변수 / security	N	q	p
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

3.2 NTRU 서명

NTRU 서명은 NTRU 암호 시스템과 같이 NTRU 래티스에서 작은 벡터를 찾는 문제인 SVP(shortest vector problem), 또는 NTRU 래티스에서 가장 근접한 벡터를 찾는 문제인 CVP(closet vector problem)를 기반으로 이루어진다. 2000년도에 NSS라 불리는 NTRU 서명 알고리즘이 Crypto'2000의 럼프(rump) 세션에서 소개되었으며, 이를 개선한 NSS가 Eurocrypt' 2001에서 발표되었다.[14,15] 이것은 서명자의 비밀키를 모르더라도 서명 값을 위조할 수 있음을 Asiacrypt' 2001에서 밝혔다.[20] 이는 NSS 알고리즘과 기반 문제인 CVP사이의 완전한 연결이 이뤄지지 않아 발생된 결점이다. 이런 결점을 해결한 NtruSign은 CVP기반의 NTRU 서명 알고리즘으로 NtruSign과 CVP 사이에 직접적이고 완전한 연결이 이뤄진다.[21] 다음은 NtruSign 알고리즘의 키 생성, 서명 과정, 확인 과정을 기술한다.[21]

1) 매개 변수

① N : $R=\frac{Z[X]}{X^N-1}$의 차수를 정하는 차원(dimension) 매개변수이다

② q : 모듈라 값으로써 $q=O(N)$이다. 그리고 $\frac{1}{3}N\le q\le\frac{2}{3}N$의 값을 택한다.

③ d_f, d_g : 키 크기를 정하는 변수이다.

④ *NormBound* : 서명 확인 바운드(bound) 변수이다.

⑤ $\otimes$: 순환 컨볼루션 곱(cyclic convolution product)이다.

⑥ $\|\cdot\|$: centered norm이다.

2) 키 생성

① 각각 d_f, d_g개의 계수 1을 갖는 f, g를 선택한다. 그리고 f, g는 R의 부분 집합이다.

② 모듈라 q에 대해서 f의 역함수를 구한다. 즉, $[f_q^{-1}\otimes f\equiv 1]_q$인 f_q^{-1}을 구한다.

② $h=[f^{-1}\otimes g]_q$를 계산한다.

③ $f\otimes G-g\otimes F=q$를 만족하는 작은 다항식 (F, G)를 계산한다.

임의의 상수 c에 대해 $\|f\|\approx c\sqrt{N}$와 $\|g\|\approx c\sqrt{N}$를 만족하는 f, g를 선택하면 (F, G)는 $\|F\|\approx\|G\|\approx c\frac{N}{\sqrt{12}}$가 된다.

즉, 비밀키는 f가 되고, 공개키는 h가 된다.

3) 서명 과정

디지털 문서 D를 서명하는 과정이다.

① 모듈라 q의 임의 벡터 $m=(m_1, m_2)$를 생성하기 위해 디지털 문서 D를 해쉬한다.

② 다음과 같이 다항식 $a, b, A, B\in\frac{Z[X]}{(x^N-1)}$를 계산한다.

$$\begin{cases} G\otimes m_1-F\otimes m_2=A+q\otimes B \\ -g\otimes m_1+f\otimes m_2=a+q\otimes b \end{cases}$$

$-\frac{q}{2}\le a, A$의계수$\le\frac{q}{2}$의 계수

③ D의 서명 값은 $s\equiv[f\otimes B+F\otimes b]_q$이다.

4) 확인 과정

서명 값 s의 유효성을 확인한다.

① 디지털 문서 D를 해쉬해 $m=(m_1, m_2)$를 재생성한다.

② 공개키 h와 서명 값 s를 이용하여 $t\equiv[h\otimes s]_q$를 계산한다.

③ $\|(s-m_1), (t-m_2)\|\le$ *NormBound*를 확인한다. 이것은 (s, t)와 (m_1, m_2)사이의 거리를 측정한 것으로 *NormBound*는 다음과 같다.

$$\|(m_1-s, m_2-t)\|^2\approx c^2\frac{N^3}{72}\left(1+\frac{12}{N}\right)$$

예를 들어서 *RSA* 1024비트와 NtruSign 251비트는 동일한 보안 강도를 갖는다. 이때, $(N, q, c)=(251, 128, 0, 45)$는 NtruSign의 매개변수이고, *NormBound*는 250이다.

Ⅳ. 제안한 프로토콜

이동 통신 환경에서의 인증 및 키 합의 프로토콜은 무엇보다 높은 효율성과 보안성이 중요하다. 이는 단말기와 이동 통신 환경이 갖는 제약점을 극복해야하기 때문이다. 이 장에서는 이런 제약적인 환경에 적합한 프로토콜을 제안하며 무엇보다 NTRU와 NtruSign의 수학 문제 기반인 CVP 어려움을 이용한 세션키를 생성한다. 이는 잘려진 환에서 다항식들의 컨볼루션 곱으로 이루어져 보다 빠르고 안전한 인증 및 키 합의 프로토콜을 제안한다.

4.1 제안한 프로토콜 스킴

제안한 NTRU 기반의 인증 및 키 합의 프로토콜은 잘려진 다항식 환, $R=\frac{Z[X]}{x^n-1}$에서 이루어지는데, R은 $n-1$차의 모든 다항식 집합이다.

다음은 프로토콜에 사용된 기호들을 기술한다.

- p, q : 소수일 필요는 없으며, $\gcd(p, q)=1$를 만족시키는 값이다. 그리고 q는 p보다 크다.
- F_r : R의 부분집합으로써, 계수가 0,1,-1로 이루어지는 다항식의 집합이다. 이 집합은 1,-1의 개수가 d_r로 사전에 정의되어 있으며, 나머지의 계수는 0이다.
- *CertM, CertV* : 이동 통신 사용자와 서비스 제공자가 인증 기관으로부터 받은 인증서이다.
- ID_M, ID_V : 이동 통신 사용자와 서비스 제공자의 신원확인을 위해 사용되는 아이디(ID)이다.
- *COUNT* : 메시지 재사용을 방지하기 위해 사용하는 값이다.

4.1.1 초기화 단계

이동 통신 단말기가 제조되면서 단말기에서 사용될 서비스에 필요한 기능이 탑재된다. 또한, 공개키와 비밀키가 생성되어 탑재된다. 물론 키 생성이 쉽고 빠르기 때문에, 키 생성 알고리즘이나 칩을 사용해 서비스를 이용할 때마다 공개키와 비밀키를 생성하여 보다 안전한 프로토콜을 수행할 수 있다. 초기화 단계에서는 이동 통신 사용자가 단말기를 사용하지 않는 시간에 공개키와 비밀키를 생성한다. 마찬가지로 서비스 제공자도 프로토콜 수행 전이나 다른 이동 통신 사용자와 프로토콜을 수행하는 동안에 공개키와 비밀키를 생성한다.

1) 이동 통신 사용자

- $f_M \in F_f$, $g_M \in F_g$를 임의로 선택한다.
- f_M은 모듈라 q에 대해 역함수를 계산한다. $[f_{Mq}^{-1} \otimes f_M \equiv 1]_q$
- $h_M \equiv [f_{Mq}^{-1} \otimes g_M]_q$를 계산한다.
- $f_M \otimes G - g_M \otimes F = q$를 만족하는 작은 다항식 (F, G)를 계산한다.

이동 통신 사용자의 공개키는 h_M이고, 비밀키는 f_M, g_M이다.

2) 서비스 제공자

- $f_M \in F_f$, $g_M \in F_g$를 임의로 선택한다.
- f_V는 모듈라 p와 모듈라 q에 대해서 역함수를 계산한다. 즉, $[f_{Vp}^{-1} \otimes f_V \equiv 1]_p$, $[f_{Vq}^{-1} \otimes f_V \equiv 1]_q$
- $h_V \equiv [f_{Vq}^{-1} \otimes g_V]_q$를 계산한다.

서비스 제공자(VASP)의 공개키는 h_V이고, 비밀키는 f_V, g_V이다.

4.1.2 실행 단계

초기화가 된 상태에서 이동 통신 사용자는 서비스 제공자로부터 이동 통신을 통한 서비스를 제공받고자 할 때, 먼저 이동 통신 사용자는 서비스 제공자에게 서비스 요구(service request)를 한다. 그러면 서비스 제공자는 이동 사용자의 인증을 요구한다. 다음은 이동 통신 사용자와 서비스 제공자간의 인증과 키 합의가 이뤄지는 단계이며 [그림 1]에서 수행되는 프로토콜을 나타내고 있다.

[1 단계]

첫 번째 단계에서 이동 통신 사용자는 다음과 같이 생성된 $K_M \otimes h_M, COUNT$를 서비스 제공자에게 전송한다.

- $r_M \in F_r$을 임의로 선택한다.
- 이동 통신 사용자의 비밀키 f_M와 세션 비밀키 r_M을 이용하여 $K_M = [f_M \otimes r_M]_q$을 계산한다.
- $K_M \otimes h_M, COUNT$을 연결하여 서비스 제공자에게 전송한다.

[2 단계]

서비스 제공자는 이동 통신 사용자로부터 받은 값을 통해 다음을 수행한다.

- $r_V \in F_r$을 임의로 선택한다.
- 서비스 제공자의 비밀키 g_V와 세션 비밀키 r_V를 이용하여 세션키를 계산한다.

$$K_{MV} = h([h_M \otimes K_M \otimes g_V \otimes r_V]_q)$$
$$= h([f_M^{-1} \otimes g_M]_q \otimes [f_M \otimes r_M]_q \otimes g_V \otimes r_V]_q)$$
$$= h([g_M \otimes r_M \otimes g_V \otimes r_V]_q)$$

Mobile User		VASP
• $r_M \in F_r$ • $K_M = [f_M \otimes r_M]_q$	$K_M \otimes h_M, COUNT$ →	• $r_V \in F_r$ • K_{MV} $= h([h_M \otimes K_M \otimes g_V \otimes r_V]_q)$ $= h([g_M \otimes r_M \otimes g_V \otimes r_V]_q)$
• K_{MV} $= h([h_V \otimes K_V \otimes g_M \otimes r_M]_q)$ $= h([g_V \otimes r_V \otimes g_M \otimes r_M]_q)$	← $CertV, K_V, COUNT$ $h(ID_V, K_{MV})$	• $K_V = [f_v \otimes r_V]_q$
• $CertM, h(COUNT, K_V, ID_M, K_{MV})$을 D이라 둔다.	$Enc_{K_{MV}}\{D, Sig_M\{D\}\}$ →	

[그림 1] NTRU를 이용한 인증 및 키 합의 프로토콜

- 서비스 제공자의 비밀키 f_V와 세션 비밀키 r_V를 이용하여 $K_V = f_V \otimes r_V$를 계산한다.
- ID_V, K_{MV}를 연결하여 해쉬한다.
- $CertV, K_V, COUNT, h(ID_V, K_{MV})$을 연결하여 이동 통신 사용자에게 전송한다.

〔3 단계〕

이동 통신 사용자는 서비스 제공자에게 받은 메시지에 다음과 같은 과정으로 서명하고, 이를 세션키 K_{MV}를 이용하여 암호화한 후에 서비스 제공자에게 다시 보낸다.

- 사용자는 받은 K_V와 비밀키 g_M, 세션 비밀키 r_M을 사용해 세션키를 계산한다.

$$\begin{aligned} K_{MV} &= h([h_V \otimes K_V \otimes g_M \otimes r_M]_q) \\ &= h([f_V^{-1} \otimes g_V]_q \otimes [f_V \otimes r_V]_q \otimes g_M \otimes r_M]_q) \\ &= h([g_V \otimes r_V \otimes g_M \otimes r_M]_q) \end{aligned}$$

- $h(COUNT, K_V, ID_M, K_{MV})$를 계산한다.
- $CertM$와 $h(COUNT, K_V, ID_M, K_{MV})$를 연결하면 다음과 같다..

$$D = \{CertM, h(COUNT, K_V, ID_M, K_{MV})\}$$

- 비밀키 f_M을 사용해 서명한다.

즉, 모듈라 q의 임의의 벡터 $m = (m_1, m_2)$를 생성하여 D를 해쉬한다.

$$\begin{cases} G \otimes m_1 - F \otimes m_2 = A + q \otimes B \\ -g \otimes m_1 + f_M \otimes m_2 = a + q \otimes b \end{cases}$$

$$-\frac{q}{2} \le a, A\text{의 계수} \le \frac{q}{2}$$

$$Sig_M\{CertM, h(COUNT, K_V, ID_M, K_{MV})\} = [f_M \otimes B + F \otimes b]_q$$

- $D, Sig_M\{D\}$를 세션키를 이용하여 암호화한다.
- 암호화한 $Enc_{K_{MV}}\{D, Sig_M\{D\}\}$를 서비스 제공자에게 전송한다.

4.1.3 확인 단계

서비스 제공자는 이동 통신 사용자로부터 받은 메시지($Enc_{K_{MV}}\{D, Sig_M\{D\}\}$)를 전 단계에서 계산한 세션키 K_{MV}를 이용해 복호한다. 이로 인해 얻게되는 $D, Sig_M\{D\}$를 사용하여 이동 통신 사용자의 신원을 확인한다. 또한 D을 이용하여 $Sig_M\{D\}$의 유효성을 확인한다.

- 문서 D를 해쉬해서 $m = (m_1, m_2)$를 재성생한다.
- 서비스 제공자는 이동 통신 사용자의 공개키 h_M와 서명값 $Sig_M\{D\}$를 사용하여 t를 계산한다.

$$t \equiv [h_M \otimes Sig_M\{D\}]_q$$

- $Sig_M\{D\}, t, m_1, m_2$를 사용하여 다음을 확인한다.

$$\|(Sig_M - m_1), (t - m_2)\| \le NormBound$$

위 조건이 만족되면, 서비스 제공자는 이동 통신 사용자가 서명한 서명 값이 유효한 것으로 인정하고 이동 통신 사용자는 서비스 제공자에게 서비스를 제공한다.

V. 제안한 프로토콜의 보안 특성 및 성능 평가

4.1 보안 특성

- 함축적 키 인증성

서비스 제공자는 사용자로부터 받은 K_M와 사용자의 공개키 h_M을 이용하여 세션키를 생성하는데, 이때, 서비스 제공자의 비밀키와 세션 비밀키도 이용하여 세션키를 생성한다. 다시 말해, 서비스 제공자의 비밀키를 알고 있는 사람만이 세션키를 생성할 수 있으므로 사용자는 서비스 제공자에 대한 함축적 키 인증성을 갖는다. 반대로 서비스 제공자도 마찬가지로 이동 통신 사용자에 대한 함축적 키 인증성을 갖는다.

- 명시적 키 인증성

계산된 공유키 $K_{MV} = h([g_M \otimes r_M \otimes g_V \otimes r_V]_q)$를 이용해 메시지 D와 $Sig_M\{D\}$를 암호화해서 서비스 제공자에게 전송한다. 이때 서비스 제공자는 전 단계에서 계산한 K_{MV}를 이용해 복호화함으로써 이동 통신 사용자가 생성한 공유키를 확인할 수 있다. 즉, 서비스 제공자는 이동 통신 사용자에 대한 명시적 키 인증성을 갖게 되는 반면 이동 통신 사용자는 서비스 제공자에 대한 명시적 키 인증성을 갖지 않는다.

- 알려진 키에 대한 안전성

생성된 키는 $K_{MV} = h([g_M \otimes r_M \otimes g_V \otimes r_V]_q)$이다.

사용자로부터 서비스 제공자에게로 K_M을 전송할 때, 이 값이 노출되더라도 서비스 제공자의 세션 비밀키를 모르면 세션키를 생성할 수 없다. 또한 사용자측에서도 서비스 제공자로부터 전송된 K_V가 노출되어도 사용자의 세션 비밀키를 모르는 한 세션키를 생성할 수 없다. 즉, 제안한 프로토콜의 세션키는 전송되는 K_V, K_M이 노출되어도 세션 비밀키를 각자

만 알고 있기에 어느 누구도 생성할 수 없다. 그리고 이전 세션에서 세션키가 노출되어도 r_M, r_V가 세션마다 임의로 생성되며, CVP문제로 그 값을 알 수 없다. 즉, 이것은 알려진 키에 대한 안정성을 보장한다.

• 상호 개체 인증

두 번째 메시지에서 서비스 제공자는 이동 통신 사용자에게 $CertV$와 해쉬한 ID_V를 전송한다. 이것을 받은 이동 통신 사용자는 $CertV$에서 ID_V를 추출해 해쉬한다. 그리고 받은 해쉬값과 비교해봄으로써 서비스 제공자의 신원을 확인할 수 있다. 그리고 세 번째 메시지에서 이동 통신 사용자는 서비스 제공자에게 $CertM$과 해쉬한 ID_M을 전송한다. 전송된 정보를 받은 서비스 제공자는 $CertM$으로부터 ID_M을 추출해 해쉬한다. 그리고 받은 해쉬값과 비교해봄으로써 이동 통신 사용자의 신원을 확인할 수 있다. 이로 이동 통신 사용자와 서비스 제공자간에 신원 확인이 가능함으로 이 프로토콜은 상호 개체 인증성을 갖는다.

• 갱신키 확인

프로토콜에 참여하는 이동 통신 사용자와 서비스 제공자는 공유키 K_{MV}를 갖는다. 이 값은 이동 통신 사용자가 임의로 선택한 r_M과 서비스 제공자가 임의로 선택한 r_V를 이용하여 얻어지는 값이다. 세션마다 r_M과 r_V가 임의로 선택되기 때문에 공유키가 다름을 알 수 있다.

• 이동 통신 사용자의 익명성

프로토콜에서는 $CertM$와 ID_M의 정보를 서비스 제공자에게 세션키로 암호화해서 보냄으로써 이동 통신 사용자의 익명성이 보장된다.

• 전송된 정보의 부인 봉쇄

제안된 프로토콜에서는 이동 통신 사용자의 비밀키인 f_M을 이용하여 메시지에 서명함으로써 부인 봉쇄가 이루어진다.

4.2 성능 평가 및 비교 분석

4.2.1 기존 프로토콜과의 보안 특성 비교

지금까지 이동 통신 환경에서의 인증 및 키 합의 프로토콜이 많이 제안되었다. DLP기반의 ASPeCT[3]와 개선된 BCY,[7] ECC-DLP기반의 AYK,[22] NTRU의 SVP/CVP기반의 제안한 프로토콜 간의 보안 특성을 비교하면 〔표 2〕와 같다.

4.2.2 성능 평가

성능 평가는 DLP, EC-DLP, SVP/CVP기반의 세션키 생성을 통해 이뤄지는 프로토콜들의 연산량을 비교한다.[3,7,22] 다음은 이동 통신 사용자와 서비스 제공자에서의 연산량를 계산한다. 단, ASPeCT와 개선된 BCY 프로토콜은 DLP기반으로 1024bit, AYK는 ECDLP기반으로 160bit, 그리고 제안한 프로토콜은 SVP/CVP기반으로 512bit 보안 강도를 갖는다.[10,18,22]

아래의 약어를 사용하여 비교하면, ASPeCT와 개선된 BCY는 PKE계산으로 exponentiation을 행하며, AYK는 eP와 ECD계산으로 점의 곱셈을 행한다. 반면에 제안한 프로토콜은 NSIGN과 NOPER계산으로 쉬프트-덧셈을 행한다. exponentiation은 multiplication보다 더 많은 연산량를 갖고 있

〔표 2〕 기존 프로토콜과의 보안 특성 비교

보안 특성	제안 프로토콜		ASPeCT		개선된 BCY		AYK	
	M->V	V->M	M->V	V->M	M->V	V->M	M->V	V->M
함축적 키 인증성	○	○	○	○	○	○	○	○
명시적 키 인증성	○	×	○	×	×	×	×	×
키 합의	○	○	○	○	○	○	○	○
개체 인증	○	○	○	○	×	×	○	○
갱신키 확인	○	○	○	○	×	×	○	○
익명성	○	×	○	×	○	×	○	×
부인 봉쇄	○	×	○	×	×	×	○	×

※ M : 이동 통신 사용자, V : 서비스 제공자

으며, multiplication은 쉬프트-덧셈만 행하는 것보다 더 많은 연산량를 갖는다.[22,23]

1) 이동 통신 사용자 측에서의 연산량

- 개선된 BCY : 1 PKE(1024bit)+2 SKE(2048bit) + 사전 계산
- AYK : 1eP(160bit)+1ECD(160bit)+2SKE (672bit)+1 SHA(288bit)
- 제안한 프로토콜 : 1 NSIGN(251bit)+1 SKE (502 bit)+ 2 NOPER(251bit)+사전 계산

2) 서비스 제공자 측에서의 연산량

- 개선된 BCY : 1 PKE(1024bit)+1SKE(1024bit) +사전 계산
- AYK : 1eP(160bit)+1ECD(160bit)+2SKE (672bit)+1 SHA(288bit)
- 제안한 프로토콜 : 1 NSIGNV(251bit)+1SKE (502bit)+1 NOPER(251bit)+사전계산

약어는 다음을 뜻한다.

- PKE : Public Key Encryption
- SKE : Secret Key Encryption or Decryption
- eP : Point Multiplication
- ECD : Elliptic Curve DSA Verification
- NSIGN : NtruSign Algorithm
- NOPER : NTRU Operation(shift-add)
- NSIGNV : NtruSign Verification

Ⅵ. 결 론

본 논문에서는 NTRU 기반의 이동 통신에서의 인증 및 키 합의 프로토콜을 제안했다. 기존의 프로토콜은 랜덤 값의 해쉬 값, DLP기반의 exponentiation값, 또는 이 exponentiation의 해쉬 값 등을 세션키로 갖는다. 이에 반해 제안한 프로토콜은 NTRU 래티스의 SVP/CVP기반의 둘 이상 다항식의 컨볼루션 곱을 세션키로 갖는다. 제안한 프로토콜은 두 다항식의 덧셈과 shift-addition 연산으로 인해 DLP기반의 exponentiation값, 또는 이 exponentiation의 해쉬 값을 세션키로 갖는 것에 비해 생성 속도가 빠르다. 또한, 이동 통신 환경에 적합한 대표적인 프로토콜인 DLP기반의 ASPeCT와 개선된 BCY, ECDLP기반의 AYK와 제안한 프로토콜간의 보안 특성 및 통신 오버헤드를 비교 분석하였다. 제안한 프로토콜은 ASPeCT와 같은 수준의 보안 특성을 만족하고, exponentiation과 multiplication이 shift-addition보다 많은 연산량을 요구하기 때문에 ASPeCT와 AYK에 비해 연산량이 적다. 따라서 제안한 프로토콜은 DLP기반, ECDLP기반의 기존 프로토콜에 비해 성능이 우수하며 SVP/CVP기반으로 인해 안전하다.

본 논문은 향후 전송시간과 전송 데이터 량을 비교 분석하여 보다 정확한 성능 평가가 이루어져야하며 제안한 프로토콜에 대한 공격들을 분석해야한다.

참 고 문 헌

[1] A. Mehrotra and L. S. Golding, "Mobility and Security Management in the GSM System and some Proposed Future Improvements," *Proceedings of the IEEE, Volume 86, Issue 7*, pp. 1480~1497, July 1998.

[2] C. H. Lee, M. S. Hwang, W. P. Yang, "Enhanced Privacy and Authentication for the Global System for Mobile Communications," *Wireless Networks 5*, pp. 231~243, 1999.

[3] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," *Computer Security - ESORICS'98*, Lecture Notes in Computer Science, 1485, pp. 277~293, 1998.

[4] D. G. Park, C. Boyd and S. J. Moon, "Forward Secrecy and Its Application to Future Mobile Communications Security," *PKC 2000, Springer-Verlag*, pp. 433~445, 2000.

[5] K. H. Lee and S. J. Moon, "AKA Protocols for Mobile Communications," *ACISP' 2000*, LNCS 1841, pp. 400~41, 2000.

[6] H. Y. Lin and L. Harn, "Authentication Protocols for Personal Communication Systems," *Proceedings of ACM SIGCOMM'95*, pp. 256~261, August 1995.

[7] V. Varadharajan, Y. Mu, "On the Design of Security Protocols for Mobile Communications," Australasian Conference, ACISP '96, pp. 134~145, Springer-Verlag, 1996.

[8] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, "An Efficient Protocol for Authenticated Key Agreement Protocol," *Technical report CORR 98-05*, University of Waterloo, Canada, March, 1998.

[9] J. H. stein, J. Pipher, J. H. Silverman, "NTRU: A new high speed public key cryptosystem," *preprint; presented at the rump session of Crypto'96*, 1996.

[10] P. Karu, J. Loikkanen, "Practical comparison of Fast Public-key Cryptosystems," *Telecommunications Software and Multimedia Lab. at Helsinki Univ. of Technology*, http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers.html, 2001.

[11] J. Hoffstein, D. Lieman, J. H. Silverman, "Polynomial Rings and Efficient Public Key Authentication," *in Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce(CrypTEC '99)*, 1999.

[12] J. Hoffstein, J. H. Silverman, "Polynomial Rings and Efficient Public Key Authentication II," *Proceedings of a Conference on Cryptography and Number Theory(CCNT '99)*, 1999.

[13] C. J. Mitchell, "Security in Future Mobile Networks," *in Proceedings of the Second International Workshop on Mobile Multi-Media Communications(MoMuC-2)*, Bristol, April 1995.

[14] J. Hoffstein, J. Pipher, J. H. Silverman, "The NTRU Signature Scheme: Theory and Practice," Preprint, 2001.

[15] J. Hoffstein, J. Pipher, J. H. Silverman, "NSS : An NTRU Lattice-Based Signature Scheme," *Eurocrypt'01*, pp. 211~228, 2001.

[16] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU : A Ring Based Public Key Cryptosystem," *in Algorithmic Number Theory(ANTS III)*, Portland, J.P. Buhler (ed.), *Lecture Notes in Computer Science 1423, Springer-Verlag*, Berlin, pp. 267~288, 1998.

[17] J. Hoffstein, D. Lieman, J. Pipher, J. H. Silverman, "NTRU : A Public Key Cryptosystem," *IEEE P1363 : Protocols from other families of public-key algorithms, Technical Report*, October 1999.

[18] M. J. Wiener, "Performance Comparison of Public-Key Cryptosystems," *RSA CryptoBytes*, pp. 1~5, 4(1):1~5, 1998.

[19] 최영근, 김순자, "이동시스템에서의 효율적인 인증 및 키교환 프로토콜," *한국정보보호학회 논문지*, Vol. 11, No. 2, pp. 73~82, Apr. 2001.

[20] C. Gentry, J. Jonsson, J. Stern, M. Szydlo, "Cryptoanalysis of the NTRU Signature Scheme(NSS) from Eurocrypt 2001," *Advances in Cryptology-Asiacrypt '01, Lecture Notes in Computer Science*, Springer-Verlag, 2001.

[21] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, "NtruSign : Digital Signatures using the Ntru Lattice," *Preliminary version distributed at AsiaCrypt 2001*, 2001.

[22] M. Aydos, T. Yamk, and C. K. Koc, "High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor," *IEE Proceedings : Communications*, 148(5) : 273 - 279, October 2001.

[23] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography," *CRC Press*.

[24] C. Boyd, D. G. Park, "Public key protocols for wireless communications," *ICISC 1998*, 47-57, 1998.

〈著者紹介〉

박 현 미 (Hyun-mi Park) 학생회원
2000년 8월 : 영남대학교 수학과 졸업(컴퓨터 공학과 복수 전공)
2000년 8월~2002년 8월 : 경북대학교 정보통신학과 석사 과정
〈관심분야〉 정보 보호, 무선 인터넷 기술

강 상 승 (Sang-seung Kang) 정회원
1997년 2월 : 경북대학교 전자공학과 졸업
1999년 2월 : 경북대학교 전자공학과 석사
1999년 6월~현재 : 한국전자통신연구원 전자거래연구부 연구원
〈관심분야〉 전자상거래, 정보보호, 무선인터넷 기술

최 영 근 (Yeong-Geun Choe) 학생회원
1994년 2월 : 경북대학교 전자공학과 졸업
1995년 3월~2001년 2월 : 경북대학교 전자공학과 석사 졸업
2001년 3월~현재 : 경북대학교 전자공학과 박사
〈관심분야〉 정보 보호 및 보안 기술, 정보 보호 응용 기술

김 순 자 (Soon-Ja Kim) 종신회원
1975년 2월 : 경북대학교 수학과 졸업
1977년 2월 : 경북대학교 수학과 석사 졸업
1988년 2월 : 계명대학교 수학과 박사 졸업
1993년~현재 : 경북대학교 공과대학 전자공학과 교수
〈관심분야〉 정보 보호 및 보안 기술, 정보 보호 응용 기술