ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-01-28
200

j.inst.Korean.electr.electron.eng.Vol.23,No.1,200~206,March 2019
http://dx.doi.org/10.7471/ikeee.2019.23.1.200

스크립트 공격을 막기 위한 NTRUSign 보안 연구

A Study on NTRUSign security to prevent script attacks

배 성 현*, 정 종 혁*★

Sung-Hyun Bae*, Jong-hyeog Jeong*★

Abstract

Recently, there is a growing preference for a fast and secure cryptographic protocol that is applicable to Internet of things environments. Among the lattice-based cryptographic algorithms, the NTRU cryptosystem is secure by virtue of the shortest vector problem (SVP) and the closest problem(CVP), which is a problem of finding very short vectors and closest vector. NTRUSign, an electronic signature based on this cryptographic algorithm, has been proposed and proved unsafe for script attacks. In this paper, we propose a security protocol using a symmetric key algorithm by securing a shared key using key exchange. Therefore, the attacker can not compute the key value and intends to propose a more secure digital signature.

요 약

최근 사물인터넷 환경에서 적용가능하며 빠르고 보안성이 뛰어난 암호프로토콜에 대한 선호도가 높아지고 있다.

래티스 기반의 암호알고리즘 중 NTRU 암호시스템은 매우 짧은 벡터를 찾는 문제인 SVP와 가장 가까운 벡터를 찾는 문제인 CVP에 의해 안전하다. 이 암호알고리즘의 안전성에 근거한 전자서명인 NTRUSign이 제안되었으며 스크립트 공격에 대해 안전하지 않음이 밝혀졌다. 본 논문에서는 키 교환을 사용하여 공유 키를 확보하고 대칭 키 알고리즘을 사용한 보안 프로토콜을 제안한다. 따라서 공격자는 키 값을 계산할 수 없으며 보다 안전한 디지털 서명을 제안하고자 한다.

Key words : NTRUSign, SVP, CVP, script attacks, finite field

Ⅰ. 서론

1996년 Crypto에서 소개된 NTRU는 키 생성이 쉽고 빠르며 보안성이 높다. 따라서 빠른 연산 속도로 인해 저사양의 프로세서를 기반으로 하는 프로토콜 설계에 적합하다. 현재 NTRU그룹에서는 이 시스템을 이용한 사물인터넷 환경이나 무선 환경 등의 분야에 적용하고 있다[1-2]. 기존의 공개키 기반의 서명기법은 대수학을 기초로 한 것으로 유한군(finite group), 유한 체(finite field)를 바탕으로 한 어려운 수학문제기반의 알고리즘이다. 그 외 소인수분해 문제의 RSA 서명기법, 이산대수문제의 ElGamal 서명기법 등이 있다. 이들은 큰 소수 p, q를 찾는 시간이 많이 걸리며 키생성이 어렵다. 또한, 생성자에 임의의 큰 수 멱승을 해야하므로 계산이 복잡하고 암・복호화 시간이 길다. 이에 반해 NTRU 암호시스템 기반의 서명기법은 많은 장점을 가진다. 그러나, NTRU 암호시스템에 많은 공격

* Dept. of Aviations Information & Communication, KyungWoon University.
★ Corresponding author
E-mail : jhjeong@ikw.ac.kr, Tel : +82-54-479-1314
※ Acknowledgment
Manuscript received Mar. 10, 2019; revised Mar. 20, 2019; accepted Mar. 21, 2019

이 제안되었으며, NTRU 기반의 서명인 NSS 역시 결함이 있었다[3, 7]. 그 뒤NTRUSign이 제안되었으나[5], 서명복사본 공격이 있음이 밝혀졌다[4, 9].

본 논문에서는 기존에 제안된 NTRU 암호시스템의 공격인 래티스 공격과 합성수 공격에 안전하고 NTRU 기반 서명에 치명적인 복사본 공격을 막는 방법을 제안한다. 제안된 프로토콜은 키 교환을 통해 생성된 공유키 K와 대칭키 암호를 결합하여 메시지 인증과 기밀성을 제공하고 공유키 K와 $Keyed\ hash$로부터 생성된 메시지 M_A를 이용하여 생성된 서명값 $S_A\{KH(M_A)\}$를 추측할 수 없게 하였다. 따라서, 기존에 제안된 각종 공격을 막을 수 있었다. 또한, 본 프로토콜은 서버와 클라이언트간 메시지 전달 등에 사용하여 메시지 인증, 기밀성, 디지털 서명을 제공할 수 있다.

II. 본론

1. NTRUSign

NSS가 소개된 이후 개선된 NSS가 Eurocrypt 2001에서 발표되었다[3]. 그러나, AsiaCrypt 2001에서 서명자의 비밀키를 모르더라도 서명복사본들로부터 비밀키가 드러남이 밝혀졌다[7, 9]. 그로 인해, NSS를 대신할 NTRUSign를 개발하게 되었다[5].

가. 키생성

NTRUSign의 매개변수는 N,p,q,d_f,d_g가 있다.

서명자 A는 두 다항식 f,g를 선택하여 공개키 h를 계산하고 작은 다항식 F,G를 계산한다.

1) A는 두 다항식 $f\in L_f$와 $g\in L_g$를 비밀키로 선택한다.
2) f_q^{-1},f_p^{-1}를 계산한다.
   각각 $\frac{Z_q[x]}{(x^N-1)}$, $\frac{Z_p[x]}{(x^N-1)}$에서 f의 역함수이다.
3) 공개키를 계산한다.
   $h=f_q^{-1}*g \bmod q \in Z_q[x]/(x^N-1)$
4) $f*G-g*F=q$를 만족하는 작은 다항식 (F,G))를 계산한다.
   여기서, $\|f\| \approx c\sqrt{N}$, $\|g\| \approx c\sqrt{N}$,
   $\|F\| \approx \|G\| \approx c\frac{N}{\sqrt{12}}$, c는 상수이다.
   즉, 비밀키는 f가 되고, 공개키는 h가 된다.

나. 서명 과정

1) 디지털 문서 D를 해쉬하여 모듈라 q의 임의 벡터 $m=(m_1,m_2)$를 생성한다.
2) 다음 조건을 만족하는 다항식 a,b,A,B를 계산한다. $\begin{cases}G*m_1-F*m_2=A+q*B\\-g*m_1+f*m_2=a+q*b\end{cases}$
   단, $-\frac{q}{2}\le a, A$의 계수$\le \frac{q}{2}$의 계수이다.
3) D의 서명 값은 $s\equiv[f*B+F*b] \bmod q$이다.

다. 확인 과정

1) 디지털 문서 D를 해쉬해 $m=(m_1,m_2)$을 재생성한다.
2) 공개키 h와 서명값 s를 이용하여 $t\equiv[h*s] \bmod q$를 계산한다.

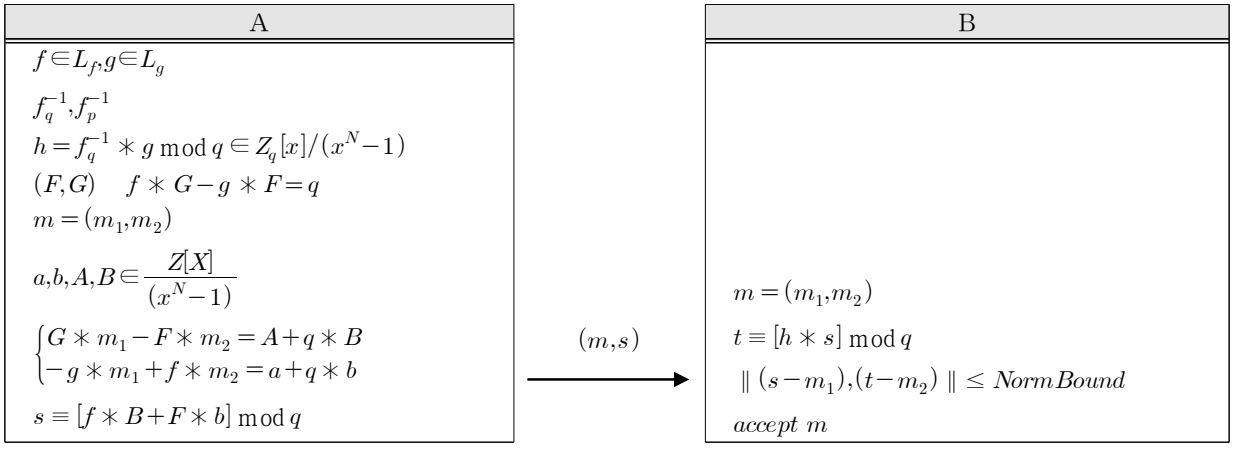


Fig. 1. NTRUSign signing.
그림 1. NTRUSign 서명과정

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

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

서명자 A로부터 받은 서명값 s의 유효성을 확인한다. 그림 1은 NTRUSign에서 서명자 A와 확인자 B에 의해 이루어지는 서명과정을 나타낸 것이다.

2. NTRU상에서의 공격

가. 래티스 공격

래티스 공격은 Eurocrypt 97에서 소개되었다[12]. 그들은 래티스를 $L_{cs} = \begin{bmatrix} I & H \\ 0 & qI \end{bmatrix}$로 정의하였으며, 공개키 h와 공개된 정보만 이용해서 비밀키 f를 찾으려고 했다. 그러나, 실제로 $f*h=g \pmod q$ 정보만으로 비밀키 f를 찾아내기 어렵다. 따라서, $f'*h=g' \pmod q$를 만족하는 $f', g' \in Z^N$의 쌍의 집합이 있다면 q^N개의 다른 (f',g')쌍을 구할 수 있고 2개의 쌍으로부터 (f,g)를 찾을 수 있음을 밝혔다. 그 알고리즘 중 가장 효율적인 것은 LLL알고리즘 등이 있다[10]. May는 래티스 공격에서 목표 벡터보다 더 작은 벡터를 찾을 수 없음을 밝혔다[13]. N의 값이 167 이상의 수로 사용할 경우 래티스 기저 줄임방식의 공격이 비효율적이었다[11].

나. 합성수 공격

Gentry는 FFT(Fast Fourier Transform)를 사용하기 위해 2의 지수승 값을 갖는 N을 선택함으로서 발생하는 문제점을 제기했다[9]. N이 합성수였을 때 비밀키를 발견할 수 있음을 보였다. 그러나, N이 소수일 때 folding은 동작하지 않음을 보였다.

다. NSS 공격

이 공격법은 Hoffstein과 Kaliski에 의해 먼저 제안되었다[8]. 비밀키에 관한 정보를 얻기 위해 서명의 복사본에 평균을 취하는 방법을 연구하였다.

만약 서명복사본들 $\{(m_1,s_1),(m_2,s_2),...,(m_r,s_r)\}$이 주어진다면 공격자는 서명자의 공개키와 이 복사본들을 이용하여 직접 다음을 구할 수 있다.

$\{f*w_1 \bmod q, \cdots, f*w_r \bmod q\}$

$\{g*w_1 \bmod q, \cdots, g*w_r \bmod q\}$

여기서, w_i는 서명과정을 통해 계산되어질 수 있다. 이것을 모듈라 q하지 않은 형태로 바꾸게 되면 다음과 같다.

$\{f*w_1, \cdots, f*w_r\}$, $\{g*w_1, \cdots, g*w_r\}$

여기서, w_1과 w_2가 서로소이며 $a*w_1+b*w_2=1$을 만족할 때, $GCD(f*w_1, f*w_2)=(f)$가 된다. 이것을 GCD래티스 공격을 하게 되면 개인키 f를 얻을 수 있다.

라. NTRUSign 공격

Asiacrypt 2001에 발표된 NTRUSign은 이전에 나온 NTRU기반의 서명기법들보다 더 간단하다. 서명자가 짧은 기저 벡터를 가지는 비밀지식을 가진다[5, 10].

이 서명에서의 문제점은 메시지 m에서 서명 s으로 보내는 과정에서 완전 치환방식이 아니고 개인식별 프로토콜(identification protocol)이 영지식(zero knowledge)이 아니므로 복사본 공격이 일어날 수 있다[8].

즉, 서명값 $s \equiv m_1-(A*f+a*F)/q \pmod q$로부터 다수의 서명 복사본 다항식$(A*f+a*F)$을 얻게 된다면 다음 식을 계산할 수 있어 복사본 공격에 노출되게 된다.

$$Avg_{ff}(r) = (1/r)\sum_{i=1}^{r}(a_i*F+A_i*f)*\overline{(a_i*F+A_i*f)}$$
$$= (1/r)\sum_{i=1}^{r}(a_i*\overline{a_i})*(F*\overline{F})+(A_i*\overline{A_i})*(f*\overline{f})+other\ terms$$

여기서, $other\ terms$을 0으로 수렴할 것이다. A와 a는 랜덤한 모듈라 q에 고르게 분포되어있다. 따라서, $f*\overline{(f)}+F*\overline{(F)}$을 근사화하여 평균을 얻을 수 있을 것이다. 실제 암호분석(Cryptanalysis)으로부터 복사본 공격을 막기 위해 긴 복사본이 필요하였다.

3. 제안하는 프로토콜

키교환을 통해 생성된 공유키 K와 대칭키 암호를 결합하여 메시지 인증과 기밀성을 제공하고 공유키 K와 $Keyed\ hash$로부터 생성된 메시지 M_A를 이용하여 생성된 서명값 $S_A\{KH(M_A)\}$를 추측할 수 없게 하여 복사본 공격을 막을 수 있는 보완 프로토콜을 제안한다. 이 보완 프로토콜을 이용하여 메시지 인증과 안전한 NTRU 기반의 디지털 서명을 제공할 수 있다.

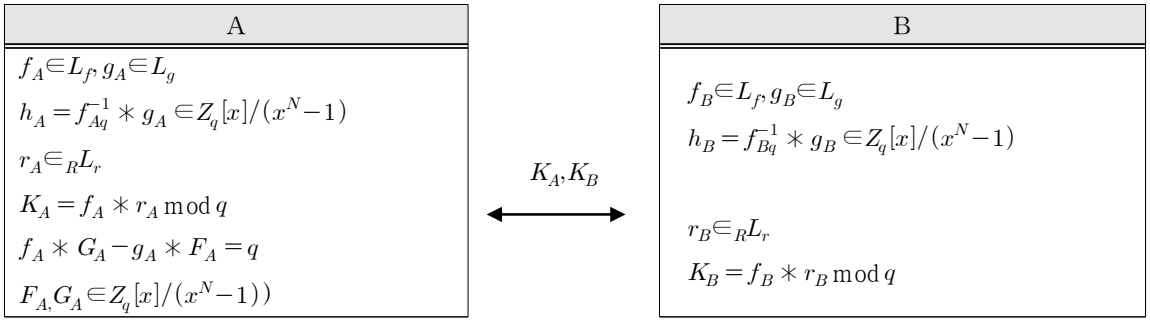


Fig. 2. key generation.
그림 2. 키생성 과정

가. 추가된 요소와 매개변수 선택

잘려진 다항식 환 $R = \frac{Z[x]}{(x^N-1)}$에서 연산이 이루어지며, 래티스 공격과 합성수 공격을 막기 위해 제안하는 매개변수 값은 N=251, q=128, d_f=73, d_g=71, d_r=71, $Normbound = 310$이다.

다음은 표 1은 프로토콜에 사용된 추가된 요소와 매개변수에 관한 기호를 설명하고 있다.

나. 키 생성 과정

서명을 주고받는 개체들은 키 생성 알고리즘을 이용하여 공개키와 비밀키를 생성하여 안전한 프로토콜을 수행한다. 각 개체는 대칭키 암호에 필요한 공유키를 만들기 위해 랜덤하게 생성된 r값으로부터 K_A와 K_B를 이용하여 공유키 K를 생성하게 된다. 그림 2는 서명자 A와 확인자 B의 키생성 과정을 나타내고 있다. 기존에 제안된 NTRUSign에 B의 키생성 과정이 추가되었으며 공유키를 만들기 위해 K_A와 K_B의 계산과정이 추가되었다. 이 K_A와 K_B를 NTRU 암호시스템을 이용하여 안전하게 전달됨을 가정한다.

(1) A의 키생성 과정

A는 서명자로서 비밀키 f_A, g_A를 선택하고 공개키 h_A를 계산한 다음 공유키에 사용될 랜덤한 r_A 값을 생성한다. 그 다음 공유키를 만들기 위한 K_A를 생성하여 B에게 안전하게 전달하고 F_A, G_A를 생성한다.

1) f_A, g_A - A의 비밀키 $f_A \in L_f, g_A \in L_g$를 선택한다.
2) h_A - A의 공개키를 계산한다.

$$h_A = f_{Aq}^{-1} * g_A \in Z_q[x]/(x^N-1)$$

여기서, f_{Aq}^{-1}는 $\frac{Z[x]}{(x^N-1)}$에서 f_A의 역함수이다.

3) $r_A \in_R L_r$를 랜덤하게 생성한다.
4) 공유키를 만들기 위해 $K_A = f_A * r_A \bmod q$를 생성한다.
5) $f_A * G_A - g_A * F_A = q$ 를 만족하는 F_A, G_A를 생성한다. ($F_A, G_A \in Z_q[x]/(x^N-1)$)

Table 1. notation description.
표 1. 사용된 표기법

Notation	Description
R	A truncated polynomial expression of n-1 th order with integer coefficients
N	The value of the dimension that determines the degree of r
p, q	$\gcd(p, q) = 1,\ p > q$
d_f, d_g	Variable that determines the key size
L_f, L_g	A set of secret keys
$hash$	One-way hash function
$Keyed\ hash$	Hash function with shared key
(ENC, DEC)	Encryption and decryption of symmetric key cryptosystem
*	cyclic convolution product

(2) B의 키생성 과정

B는 확인자로서 비밀키 f_B, g_B를 선택하고 공개키 h_B를 계산한 다음 공유키에 사용될 랜덤한 r_B 값을 생성한다. 그 다음 공유키를 만들기 위한 K_B를 생성하여 A에게 안전하게 전달한다.

1) f_B, g_B - B의 비밀키 $f_B \in L_f, g_B \in L_g$를 선택

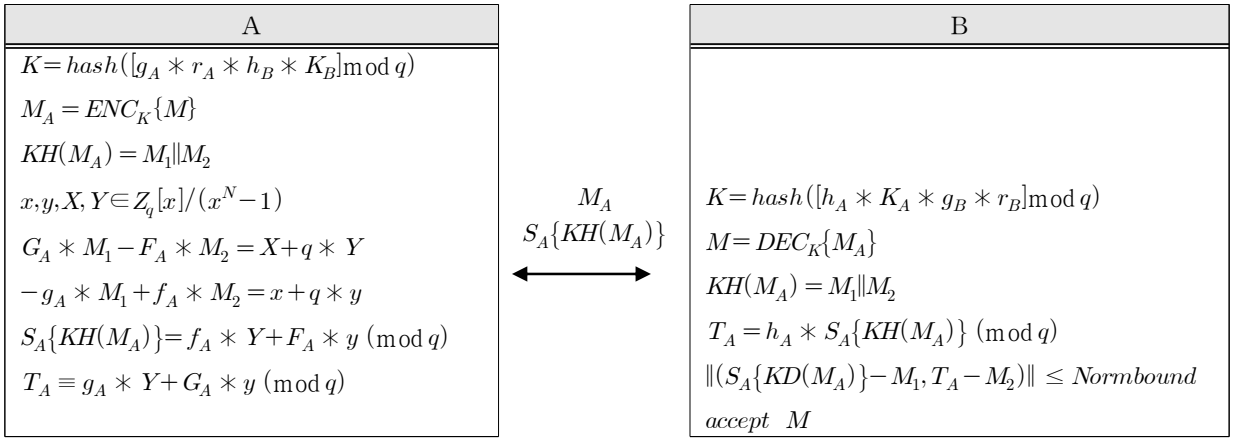


Fig. 3. signing and Verification.
그림 3. 서명 및 확인 과정

한다.

2) h_B – B의 공개키를 계산한다.

$h_B=f_{Bq}^{-1}*g_B\in Z_q[x]/(x^N-1)$

여기서, f_{Bq}^{-1} 는 $\frac{Z[x]}{(x^N-1)}$에서 f_B의 역함수이다.

3) $r_B\in_R L_r$를 랜덤하게 생성한다.

4) 공유키를 만들기 위해 $K_B=f_B*r_B \bmod q$를 생성한다.

다. 서명 과정

키 생성과정이 끝난 후 서명을 주고받을 사용자의 공개키 h_B와 K_B를 이용하여 프로토콜을 진행한다. 공유키 K를 가지고 메시지 M를 암호화함으로써 M_A를 구하게 된다. 여기서, 랜덤하게 변하는 r_A와 r_B에 의해 생성된 공유키K로 암호화하기 때문에 같은 메시지 M으로 부터 나온 암호화된 메시지 M_A는 다르게 된다.

1) A는 공유키 $K=hash([g_A*r_A*h_B*K_B]\bmod q)$를 생성한다.

$K=hash([g_A*r_A*h_B*K_B]\bmod q)$
$=hash([g_A*r_A*f_B^{-1}*g_B*f_B*r_B]\bmod q)$
$=hash([g_A*r_A*g_B*r_B]\bmod q)$

2) 공유키 K로 M을 암호화한다.

$M_A=ENC_K\{M\}$

3) 벡터 $(M_1\|M_2)\bmod q$를 생성하기 위해 암호화된 메시지 M_A를 $Keyed\ hash$ 하여 $KH(M_A)=M_1\|M_2$를 계산한다.

4) 아래 조건을 만족하는 다항식 x, y, X, Y $\in Z_q[x]/(x^N-1)$을 계산한다.

$G_A*M_1-F_A*M_2=X+q*Y$
$-g_A*M_1+f_A*M_2=x+q*y$

여기서, x,X는 $-q/2$와 $q/2$사이의 계수이다.

5) 서명값인 다항식 $S_A\{KH(M_A)\}$와 T_A를 계산한다.

$S_A\{KH(M_A)\}=f_A*Y+F_A*y\ (\bmod q)$
$T_A\equiv g_A*Y+G_A*y\ (\bmod q)$

메시지(M)상의 서명은 다항식 $S_A\{KH(M_A)\}$이다.

6) M_A와 $S_A\{KH(M_A)\}$을 B에게 전달한다.

라. 확인과정

A로부터 받은 암호화된 메시지M_A를 이용하여 메시지 M을 구할 수 있고 서명값 $S_A\{KH(M_A)\}$을 통해 서명을 확인한다. 먼저 A와 같이 사용했던 공유키 K 값을 계산하여 원본 메시지를 복호화하고 서명을 확인하게 된다.

1) $K=hash([h_A*K_A*g_B*r_B]\bmod q)$를 생성한다.

2) 공유키 K로 M_A를 복호화한다.

$M=DEC_K\{M_A\}$

3) $KH(M_A)=M_1\|M_2$를 분리해낸다.

4) $T_A=h_A*S_A\{KH(M_A)\}\ (\bmod q)$를 계산한다.

5) $\|(S_A\{KD(M_A)\}-M_1,T_A-M_2)\|\le Normbound$임 을 계산하여 서명을 확인한다.

6) 메시지 M을 받아들인다.

그림 3은 서명과정과 확인과정을 나타낸 것이다.

4. 제안한 프로토콜의 안전성 분석

가. 래티스 공격과 합성수 공격에 대한 안전성

공개 매개변수인 N값이 합성수였을 때 개인키 f를 구할 수 있었다. 그러나, 소수일 경우 "folding"은 동작하지 않음을 알 수 있었으며 제안된 N값은 251로서 167 이상이므로 래티스 공격에 안전하며, 합성수 공격에 대해 안전하다.

나. 공유키의 안전성

제안한 프로토콜에서 공유키K를 이용하여 암호화된 메시지 M_A를 복호화하게 되면 메시지 M을 구할 수 있고 M_1과M_2를 구할 수 있게 된다. 따라서, 공격자가 키생성 과정에서 교환되는 K_A와 K_B를 가로채어 A와 B사이에 생성되어지는 공유키 K를 계산할 가능성이 있다. 그러나, NTRU 암호시스템의 안전성을 기반으로 전달된 K_AA와 K_B의 값을 가로채더라도 SVP, CVP에 의해 K_A와K_B의 값을 계산할 수 없다. 또한, K_A와 K_B의 값을 알고 있더라도 매번 랜덤하게 선택된 다항식 r_A와 r_B을 모르고서 공유키 K를 구할 수 없다. 따라서, 공유키는 안전하며 함축적 키 인증성을 갖는다. 또한, 이미 알려진 키에 대해서도 세션 비밀키를 각자만 알고 있으므로 안전하다.

다. 서명복사본 공격에 대한 안전성

제안된 프로토콜에서 랜덤한 r_A와 r_B에 따라 공유키 K값이 변하고 치환방식을 지원하기 위해 대칭키 암호를 사용하여 K_A값을 계산한다. 그 다음 Keyed hash하여 K_1과 M_2으로 나누어 서명을 생성한다. 서명자 A가 확인자 B에게 보내는 서명값들은 아래와 같을 것이다.

$$G_A * M_1 - F_A * M_2 = X + q * Y \quad (1)$$

$$-g_A * M_1 + f_A * M_2 = x + q * y \quad (2)$$

식 (1)과 식 (2)에 각각 f_A와 F_A를 곱한 다음 q로 양변을 나누어준다.

$$\frac{G_A * M_1 * f_A}{q} - \frac{F_A * M_2 * f_A}{q} = \frac{X * f_A}{q} + Y * f_A \quad (3)$$

$$\frac{-g_A * M_1 * F_A}{q} + \frac{f_A * M_2 * F_A}{q} = \frac{x * F_A}{q} + y * F_A \quad (4)$$

식 (3)과 식 (4)에서 $Y * f_A$와 $F_A * y$을 더하면, $Y * f_A + y * F_A = M_1 - (X * f_A + x * F_A) \bmod q$가 된다. 따라서, 서명값은 $M_1 - (X * f_A + x * F_A) \bmod q$이 된다. 이때 공격자는 매번 서명자가 전송하는 서명값들을 수집한다고 가정한다면 공격자는 같은 값으로 추정되는 M_1의 값을 찾아서 M_1을 제거하여 다수의 $(X * f + x * F)$를 계산하여 복사본 공격을 하려 할 것이다. 그러나, 본 논문에서 제안한 M_1의 값은 공유키 K값에 대칭키 암호를 사용하여 메시지M에 따른 M_1값을 추측할 수 없게 된다. 따라서, $(X * f + x * F)$ 값을 구할 수 없다. 그러므로, 서명복사본 공격에 대해 안전하다.

III. 결론

본 논문에서는 기존에 제안된 NTRU 암호시스템의 공격인 래티스 공격과 합성수 공격에 안전하고 복사본 공격을 해결할 수 NTRUSign 보완 방법을 제안하였다. 키 교환을 통해 생성된 공유키 K와 대칭키를 결합하여 메시지 인증과 기밀성을 제공하고 공유키 K와 $Keyed\ hash$로부터 생성된 메시지 M_A를 이용하여 생성된 서명값을 추측할 수 없게 하여 복사본 공격을 막을 수 있었다. 따라서, 본 논문에서 제안된 프로토콜은 서버와 클라이언트간 메세지 전달 등에 사용하여 메시지 인증과 기밀성, 그리고, 안전한 NTRU기반의 디지털 서명을 제공할 수 있었다. 그러나, 본 프로토콜은 기존의 NTRUSign에 사용된 서명에 비해 1회의 암호화와 랜덤키 생성, keyed hash 과정이 추가되어 연산량이 증가하게 되었다. 따라서, 속도증가와 연산량 감소를 위한 방안에 대해 연구가 필요하다.

References

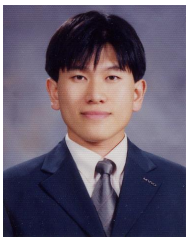
[1] J. H. stein, J. Pipher, J. H. Silverman, "NTRU: A new high speed public key cryptosyst em," preprint; *presented at the rump session of CRYOTO '96*, 1996.

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

DOI: 10.1007/BFb0054868
[3] J. Hoffstein, J. Pipher, J. H. Silverman, "NSS: An NTRU Lattice-Based Signature Scheme," *EUROCRYPT 2001 Proceeding, L ecture Notes in Computer Science, Springer - Verlag,* pp. 211-228, 2001. DOI: 10.1007/3-540-44987-6_14
[4] A. May "Cryptanalysis of NTRU," at http : //www.informatik.uni-frankfurt.de/~alex/crypto.html, 1999.
[5] Hoffstein, J., Graham, N. A. H., Pipher, J., Silverman, J. H., and Whyte, W., "NTRUSign: Digital signatures using the NTRU lattice," *In Proceeding of CT-RSA, vol 2612 of Lecture Notes in Computing Sci.* pages 122-140. Springer-Verlag, 2003. DOI: 10.1007/3-540-36563-X_9
[6] Hyunmi Park, Sang-Seung Kang, Young-Keun Choi, Soonja Kim, "Authentication in NT RU-based Mobile Communication And Key Agreement Protocol," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 12, no. 3, pp. 49-59, 2002.
[7] C. Gentry, J. Jonsson, J. Stern, M. Szydlo "Cryptoanalysis of the NTRU Signature Schem e (NSS) from EUROCRYPT 2001," *Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science 2048, Springer - Verlag*, pp. 1-20, 2001.
[8] C. Gentry, "Key Recovery and Message Attacks on NTRU-Composite," Advances in Cryptology-*EUROCRYPT 2001 Proceeding, Lecture Notes in Computer Science 2045, Springer-Verlag*, pp. 182-194, 2001. DOI: 10.1007/3-540-44987-6_12
[9] C. Gentry, M. Szydlo "Analysis of the Revised NTRU signature scheme R-NSS," at *"http://www.szydlo.net," Full version*, 2002.
[10] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *"Handbook of Applied Cryptography," CRC Press,* 1996.
[11] J. H. Silverman, "Estimated breaking tim es for NTRU lattices," NTRU Cryptosystems T echnical Report # 012 at http://www.ntru.com/cryptolab/tech_notes.htm
[12] D. Coppersmith, Adi. Shamir "Lattice Attacks on NTRU," A dvances in Cryptology - *EUROCRYPT '97, Lecture Notes in Computer Science 1233, Springer-Verlag*, pp. 52-61, 1997. DOI: 10.1007/3-540-69053-0_5
[13] Sung-hyun Bae, Sungmin Hwang, Young-Keun Choi, Soonja Kim, "Improved NTRUSign protocol," *proceeding of the Korea Institute of Information Security and Cryptology*, 2002.
[14] Sung-hyun Bae, "The improvement of the NTRUSign using the key exchange," Master thesis, Kyungpook National University. 2003.

BIOGRAPHY

Sung-hyun Bae (Member)



2000 : BS degree in Electronics and electrical Engineering, Kyungpook National University.
2003 : MS degree in Electronics Engineering, Kyungpook National University.
2005 : Ph. D course completion in Electronics Engineering, Kyungpook National University.
2017~Present : Assistant Professor, Dept. of Aviation Information & Communication Engineering, Kyungwoon University.

Jong-hyeog Jeong (Member)

1992 : BS degree in Electronics Engineering, Pukyong National University.
1994 : MS degree in Electronic Engineering, Donga University.
1999 : Ph. D: degree in Electronic & Communications Engineering, Korea Maritime and Ocean University.
2000~Present : Professor, Dept. of Aviation Information & Communication Engineering, Kyungwoon University.