ISSN 0974 - 9373

Vol. 20 No. 3 (2016) **Journal of International Academy of Physical Sciences** pp. 177-183

KTRU: NTRU over the Kleinian Integers

Khushboo Thakur and B. P. Tripathi

Department of Mathematics
Govt. N. P. G. College of Science, Raipur (C. G.), India

Email: khushboo.thakur784@gmail.com, bhanu.tripathi@gmail.com

M. R. Yadav

S.O.S.in Mathematics, Pt.Ravishankar Shukla University
Raipur(C.G.), India

Email: yadavmryadav@gmail.com

(Received July 24, 2016)

Abstract: NTRU is a public-key cryptosystem based on polynomial rings over Z. Replacing Z with the ring of Kleinian integers yields KTRU. Kleinian integers have higher significant than simple integer such as NTRU.

Keywords: Encryption, Decryption, kleinian integer, public key, privatekey.

1. Introduction

The NTRU public key cryptosystem was proposed by J. Hoffstein, J. Pipher and J. H. Silverman[1] in 1996. Its name NTRU (pronounced ‘ain't true") indicates the use of number theory and rings. Its security is based on the hardness of the short vector problem for some special lattice. Its strong points are short key size,speed of encryption and speed of decryption, two assets of crucial importance in embarked application like hand held devices and wireless systems.NTRU is viewed as a quantum-resistant cryptosystem. One weakness of NTRU is the possibility of decryption failure; however, parameters may be chosen to minimize or eliminate this error.

NTRU keys are truncated polynomials with integer coefficients. An important direction for research about NTRU is the development and analysis of variants in which the integers are replaced by elements of another ring, such as the Gaussian integers[2], integer matrices[3] or quaternion algebras[4]. The current paper is motivated by the work of J. Hoffsteinet. al.[5],

in which the integers are replaced with the ring of Kleinian integers, with the resulting cryptosystem named KTRU. In this paper we show that in the basic model ETRU is faster and has smaller key sizes than NTRU.

2. NTRU Cryptosystem

A simple description of the NTRU cryptosystem is summarized in this section[6-10]. The NTRU system is principally based on the ring of the convolution polynomials of degree $N-1$ denoted by $R=Z[x]/(x^n-1)$. It depends on three integer parameters N, p and q such that $(p, q)=1$. Before going through NTRU phases, there are four sets used for choosing NTRU polynomials with small positive integers denoted by L_m, L_f, L_g and $L_r \subseteq R$. It is like any other public key cryptosystem constructed through three phases: key generation, encryption and decryption.

2.1. Key Generation Phase

To generate the keys, two polynomials f and g are chosen randomly from L_f and L_g respectively. The function f must be invertible. The inverses are denoted by $F_p, F_q \in R$, such that

$$F_p * f \equiv 1(\text{mod } p) \text{ and } F_q * f \equiv 1(\text{mod } q).$$

The above parameters are private. The public key h is calculated by

$$h \equiv p F_q * g (\text{mod } q). \tag{1}$$

Therefore, the public key is $\{h, p, q\}$ and the private key is $\{f, F_p\}$.

2.2. Encryption Phase

The encryption is done by converting the input message to a polynomial $m \in L_m$ and the coefficient of m is reduced modulo p. A random polynomial r is initially selected by the system, and the cipher text is calculated as follows,

$$e \equiv r * h + m(\text{mod } q). \tag{2}$$

2.3. Decryption Phase

The decryption phase is performed as follows: the private key f is multiplied by the cipher text e such that

$$a \equiv f * e \pmod{q}$$
$$a \equiv f * (r * h + m) \pmod{q}$$
$$a \equiv f * h * r + f * m \pmod{q}$$
$$a \equiv pf * F_q * g * r + f * m \pmod{q}$$
$$a \equiv pg * r + f * m \pmod{q}.$$

The last polynomial has coefficientsmost probably within the interval $[-q/2, q/2]$, which eliminates the need for reduction $\bmod q$. This equation is reduced also by $\bmod p$ to give a term $f * m \bmod p$, after diminishing of the first term $pg * r$. Finally, the message m is extracted after multiplying by F_p^{-1}, as well as adjusting the resulting coefficients via the interval $[-p/2, p/2]$.

3. Proposed Cryptosystem

3.1 The Kleinian integers and KTRU

Let τ be a complex number, where $\tau = \left(1 + i\sqrt{7}\right)/2$. The ring of Kleinian integers, denoted by $Z[\tau]$, is the set of complex numbers of the form $m+n\tau$ with m and n rational integers or $m, n \in Q$. For $q = m+n\tau$ we have $|q^2| = m^2 + 2n^2 + mn$. Write μ_n for the cyclic subgroup of nth roots of unity in C, then note that $\mu_6 = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5\}$ and $\mu_{12} = \{\pm 1, \pm\tau, \pm\tau^2, \pm\tau^3, \pm\tau^4, \pm\tau^5\}$ are both contained in $Z[\tau]$.

We have two choices of embeddings of $Z[\tau]$ into R^2. The first is using the isomorphism of additive groups $Z[\tau] \to Z^2$ mapping $m+n\tau$ to (m, n) under this embedding, right multiplication by $\gamma = m+n\tau$ is realized by the matrix

$$\langle\gamma\rangle=\begin{bmatrix} m & 2n \\ -n & m+n \end{bmatrix}$$

This is distinct from, and computationally more efficient to use than the isometric ring monomorphism of $Z[\tau]$ into C (identified with R^2) given by

$$m+n\tau \mapsto m+\frac{n}{2}+i\left(\frac{\sqrt{7}n}{2}\right).$$

Theorem 3.1: *The set* μ_6 *consists of exactly all units (invertible elements) of* $Z[\tau]$. *The primes of* $Z[\tau]$ *are (up to multiplication by a unit):* $1-\tau$; *rational primes* $p \in \tau$ *satisfying* $p \equiv 2 \bmod 3$; *and those* $q \in Z[\tau]$ *for which* $|q^2| = p$ *is a rational prime satisfying* $p \equiv 1 \bmod 3$.

Thus the smallest kleinianprimes are: $p=1-\tau$, which has $|p|^2=1$, $p=2+3\tau$, with $|p|^2=19$ and $p=3+4\tau$, with $|p|^2=37$.

3.2 Example

Find the closest vector problem (CVP) in the lattice $Z[\tau]$, **which is solved as follows:**

First find the closest vectors to the complex number $q^{-1}\gamma$ on each of the rectangular lattice L spanned by $\{1, i\sqrt{7}\}$ and on its coset $\tau+L$, by rounding each of the coordinates of $q^{-1}\gamma$ to the nearest integer multiples of 1 and $i\sqrt{7}$. More precisely, for $\gamma=s+t\tau$ and $q=m+n\tau$, we compute

$$\frac{\gamma}{q}=\frac{\gamma\bar{q}}{|q^2|}=\frac{x+iy\sqrt{7}}{|2q^2|},$$

where $x, y \in Z$ are given by $x=s(2m+n)+t(m+4n)$ and $y=tm-sn$. So

$$v_1=\frac{x}{2|q^2|}+\left[\frac{y}{2|q^2|}\right]i\sqrt{7}.$$

In Kleinian integers for coordinates, $v_1=(u_0+u_1)+2u_1\tau$. The calculation for $q^{-1}\gamma-\tau$ is similar, yielding $v_2\in Z[\tau]$. See Algorithm 1 for the full details.

Algorithm 1: Solution to CVP for $Z[\tau]$

First Phase:

Input: $\gamma=s+t\tau$ and $q=m+n\tau$

Output: (v,α) such that $\gamma=vq+\alpha$ and α is reduced modulo q.

Use functions: $|c+d\tau|^2=c^2+2d^2+cd$ and $\frac{c}{d}=\frac{c-\bar{c}}{d}$,

where $\bar{c}=c \bmod d\in[-d/2, d/2]$

$\phi_1=2m+n, \qquad \phi_2=m+4n$

$Q=|q|^2, \qquad d=2Q.$

Second Phase:

Compute the closest vector on the sublattice L:

$$x=s\phi_1+t\phi_2,\ y=tm-sn$$

$$u_0=\left[\frac{x}{d}\right], \qquad u_1=\left[\frac{y}{d}\right]$$

$$v_1=(u_0+u_1)+2u_1\tau,$$

$$\alpha_1=\gamma-q^*v_1\in Z[\tau].$$

Third Phase:

Compute the closest vector on the coset $\tau+L$:

$$X'=x+Q,\ Y'=y-Q$$

$$w_0=\left[\frac{x'}{d}\right],\ w_1=\left[\frac{y'}{d}\right]$$

$$v_2=(w_0+w_1)+(2w_1+1)\tau$$

$$\alpha_2=\gamma-q^*v_2\in Z[\tau].$$

Fourth Phase:

Choose the closest:

If $|\alpha_1|^2 < |\alpha_2|^2$ return (v_1, α_1),

elseif $|\alpha_1|^2 > |\alpha_2|^2$ return (v_2, α_2),

elseif $u_0 < w_0$ return v_1, α_1,

else return (v_2, α_2)

3.4 Complexity of reduction modulo q in $Z[\tau]$

We analyze the complexity of Algorithm 1 by estimating its cost in terms of integer multiplications, doubling and additions is denoted by (M), and squarings, subtractions is denoted by (A)

The product of two Eisenstein integers $a+b\tau$ and $c+d\tau$ is given by $(a+b\tau)(c+d\tau) = ac - 2bd + ((a+b)+(c+d)-ac)\tau$ has cost 9M+2A and The norm function $|q|^2 = a^2 + 2b^2 + ab$ has cost $5M + 2A$. The sum of two kleinian integers $(a+b\tau)+(c+d\tau)$ has cost $3M$ We now turn to Algorithm 1. The first phase has cost $18M + 3A$, the second $9M + 2A$, the third $6M + 2A$ and the final comparison $4A$. The total cost of $33M + 11A$ is significantly higher than that of a simple integer modulus, but by a constant factor.

3.5 On Comparing KTRU with NTRU

Since each ETRU coefficient is a pair of integers, an instance of KTRU at degree N is comparable with an instance of NTRU of degree $N' = 2N$. Each Kleinian integer coefficient of the polynomials f, g and ϕ in KTRU is stored as a pair (m, n) of integers representing $m + n\tau$ and for coefficients in μ_{12}, m and n takes values in $\{-1, 0, 1\}$, just as do all N' coefficients of the polynomials for trinary NTRU. Only 7 pairs of trinary integers are used in the representation of $\{0\} \cup \mu_{12} \subset Z[\tau]$, whereas all 15 pairs occur in pairs of integers mod 3.Throughout we therefore compare KTRU with NTRU assuming that $N' \approx 2N$. In practice N' is odd, but where this is irrelevant we may simply set $N' = 2N$ to simplify the discussion.

References

1. J. Hoffstein, J. Pipher and J. H. Silverman, ‘’NTRU",*A Ring Based Public Key Cryptosystem*, In Proc. Of ANTS III, LNCS. Springer-Verlag, Available at http://www.ntru.com, **1423**1998 267-288.
2. R. Kouzmenko, *Generalizations of the NTRU Cryptosystem*, Diploma Project, EcolePoly-technique Federale de Lausanne, 2005-2006.
3. D. Coppersmith and A. Shamir, Lattice attacks on NTRU, *EUROCRYPT*, (1997) 52-61.
4. E. Malekian, A. Zakerolhosseini and A. Mashatan, QTRU,*A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra*, preprint, Available from the Cryptology ePrint Archive: http://eprint.iacr.org/2009/386.pdf.
5. J. Hoffstein, J. Pipher and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*, In Lecture Notes in Computer Science Springer-Verlag, **1423** (1998)267-288.
6. J. Hoffstein, J. Pipher and J. H. Silverman, *An Introduction to Mathematical Cryptography, Science Bussiness Media*, Springer, 2008.
7. J. Pipher,*Lectures on the NTRU encryption algorithm and digital signature scheme*, Brown University, 2002.
8. R. Kouzmenko, Generalizations of the NTRU cryptosystem. Master’s thesis, Polytechnique, Montreal, Canada, 2006.
9. M. Nevins, C. Karimianpour and A. Miri, Ntru over rings beyond Z, *Codes and Cryptography*, **56(1)** (2010) 65-78.
10. J. Koplinger, Signature of gravity in conic sedenions. *Applied Mathematics and Computation*, **188** (2007) 942-947.