BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem

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

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

ABSTRACT

NTRU is a public key cryptosystem based on polynomial ring over Z. Replacing Z with the ring of polynomial in one variable α over a rational field. In this paper the complexity of BTRU cryptosystem is faster than NTRU cryptosystem.

Keywords

NTRU, Rational Field, Encryption, Decryption

1. INTRODUCTION

The NTRU public-key cryptosystem has attracted much attention by the cryptographic community since its introduction in 1996 by Hoffstein, Pipher and Silverman [3, 4]. Unlike more classical public-key cryptosystems based on the hardness of integer factorisation or the discrete logarithm over finite fields and elliptic curves, NTRU is based on the hardness of finding small solutions to systems of linear equations over polynomial rings, and as a consequence is closely related to geometric problems on certain classes of high-dimensional Euclidean lattices. From a practical point of view, the distinguishing feature of NTRU compared with classical systems, has mainly been its very high speed of encryption and decryption operations for practical security levels under best known attacks, being faster than classical systems by 2 or more orders of magnitude. This highly attractive feature has include of NTRU in the IEEE P1363 industry standard for cryptography [6]. It is also often considered as the most viable post-quantum public-key encryption due to its conjectured resistance to attack by quantum computers (see, e.g., [10]), whereas classical systems have been shown [12] to be insecure in the presence of quantum computing.

In this paper a new NTRU based cryptosystem which is known as BTRU cryptosystem. The role played by Z in NTRU replaced by the ring Q[α] of polynomial in one variable α over the Rational Field.

The rest of this paper is organized in the following way: a brief summarization of the NTRU cryptosystem is presented in Section 2. The proposed cryptosystem is described in Section 3. In section 4, the security analysis is discussed. The performance analysis is discussed in Section 5, and the conclusions are presented in Section 6.

2. NTRU CRYPTOSYSTEM

A simple description of the NTRU cryptosystem is summarized in this section. For more details, the reader is referred to [1, 4, 5, 8, 9, 13] . 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 gcd (p, q) = 1. Before going through NTRU phases, there are four sets used for choosing NTRU polynomials with small positive integers denoted by L_f ,L_m , 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 Lf and Lg respectively. The function f must be invertible. The inverses are denoted by Fp , Fq $\in$ R, such that:

$$F_p * f = 1(\mathrm{mod}\, p) \quad \text{and} \quad F_q * f = 1(\mathrm{mod}\, q)$$

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

$$h = pF_q * g(\mathrm{mod}\, q) \text{……………………….(1)}$$

Therefore, the public key is {h,p,q} and the private key is {f,Fp}.

2.2 Encryption Phase

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

e = r *h + m (mod q)…………..(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,

$$a = f * e(\mathrm{mod}\, q)$$

$$a = f * (r * h + m)(\mathrm{mod}\, q)$$

$$a = (f * r * h + f * m)(\mathrm{mod}\, q)$$

$$a = (f * r * (pF_q * g) + f * m)(\mathrm{mod}\, q)$$

$$a = (p * r * g + f * m)(\mathrm{mod}\, q) \mathrm{since}[f * F_q = 1(\mathrm{mod}\, q)$$

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

3. PROPOSED CRYPTOSYSTEM

3.1 Parameters and Notations

The main parameter of proposed cryptosystem are integer N and two irreducible polynomials S,T of B:=Q[α]. We shall assume that S and T are polynomial of respective degrees u and v with u,m ∈ R and last but not least GCD(u;m) = 1. We work in the ring R := B[X]/(X^N -1),of “truncated polynomial with rational polynomial coefficients". The following notation are:

NTRU	ProposedAlgorithm
Z	B
p	S
q	T
$\log_2(p)$	u
$\log_2(q)$	m
$Z[X]/(X^N-1)$	$B[X]/(X^N-1)$
$\|\|$	deg()

The quotients rings B_s and B_t of B by the ideals (S) and (T) respectively are the rational field Q_u and Q_m. We denote by RS, RT the quotient rings of R by the ideals (S) and (T) respectively. The degree of F [deg(F)] as a polynomial in α Like for NTRU we need to define some auxiliary sets of polynomials.

Let

$$L(d) := \{F \in R \mid \deg(f) \prec d\}$$

be defined for any integers d ≤ m. Let d_f, d_f, d_ϕ be integes ≤ m. With these notations we define

$$L_f := L(d_f+1),\ L_g := L(d_g+1),\ L_\phi := L(d_\phi+1),$$

3.2 Key Generation Phase

Dan randomly chooses two polynomials f;,g ∈ L_g . Also, the polynomial f should have inverse mod S and T. In other words, one should be able to calculate f_S^{-1} and f_T^{-1} such that

$$f * f_S^{-1} = 1(\mathrm{mod}\, S)$$

and

$$f * f_T^{-1} = 1(\mathrm{mod}\, T)$$

Private key is composed of the polynomial f and f_S^{-1} After choosing the polynomials appropriately, public key can be computed as

$$h = S * \frac{g}{f}(\mathrm{mod}\, T)$$

3.3 Encryption phase:

Suppose that Cathy (the encrypter) wants to send a message to Dan (the decrypter). She begins by selecting a message m from the set of plaintexts L_m. Next she randomly chooses a polynomial $\phi \in L_\phi$ and uses Dan's public key h to compute

$$e = \phi \circ h + M \circ g \ (\mathrm{mod}\ T)$$

$$e = \phi \circ S \circ \frac{g}{f} + M \circ g \ (\mathrm{mod}\ T)$$

$$ef = S\,\phi \circ g + M \circ g \circ f \ (\mathrm{mod}\ T)$$

3.4 Decryption phase:

To decrypt, Bob computes

$$a = ef \circ g^{-1} \ (\mathrm{mod}\ T)$$

$$a = S\,\phi \circ g \circ g^{-1} + M \circ g \circ f \circ g^{-1} \ (\mathrm{mod}\ T)$$

$$a = S\,\phi + M \circ f \ (\mathrm{mod}\ T)$$

Through suitable selection of system parameters, the coefficients of the polynomial S ·ϕ +f ∘ M will most probably lie in the interval (-T/2,+T/2] and there will be no need for reduction mod T. With this assumption, when we reduce the result of S ·ϕ + f ∘ M by mod S, the term S ·ϕ vanishes and f ∘ M remains. In order to extract the message m, it is enough to multiply f ∘ M (mod S) by f_S^{-1}.

4. SECURITY ANALYSIS

4.1 Brute Force Attack

An attacker can recover the private key by trying all possible $f \in L_f$ and testing if f *h(mod T) has small entries, or by trying all $g \in L_g$ and testing if g* h^{-1} (mod T) has small entries. Similary, an attacker can recover a message by trying all possible $\phi \in L_\phi$ and testing if ef - $\phi \circ$ g (mod T) has small entries. In practice, Lg will be smaller than Lf , so key security is determined by Lg, and individual message security is determined by L_ϕ. However, as described in the next section, there is a meet in the middle attack which cuts the search time by the usual square root.

4.2 Meet in the middle Attacks

A meet in the middle attack was proposed by Odlyzko for NTRU and developed by silverman in [11]. This attack can also be used against this cryptosystem using the same argument on the degree of the rational coefficient of polynomials. This attack needs a lot of storage capacity and cut the search time by the usual square root. Hence it means that the set of possible g and ϕ has to contain at least 2^{160} elements in order to obtain a security of 2^{80}.

5. PERFORMANCE ANALYSIS

The Comparison of proposed cryptosystem and NTRU cryptosystem as follows:

1. The complexity of BTRU in terms of rational operation is the complexity of NTRU in terms of integer operation.
2. The complexity of encryption and decryption for both cryptosystem is O (N^2).
3. The complexity of multiplication in Q and The complexity of addition in Z is O(m).
4. Assuming m ≤ 12, The complexity of multiplication in Z is at best, for these value of m using Toom Cook multiplication algorithm or Toom- 3 [2, 7] of order

O(m^c) with c= $\frac{\log 5}{\log 2} \approx$ 1.465, where c = log $\frac{(2k-1)}{2k}$ for k=3.

Z_q	Q_q	$operation$
$\cong m$	$\cong m$	$+$
$\cong m^{1.46}$	$\cong$	$\times$

So, for moderate m and the same value of N CTRU is certainly faster than NTRU. For large value of m the performance will depend on the implementation.

6. CONCLUSION

In this paper the new Ntru public key cryptosystem is based on the rational field. The proposed scheme is more secure and more time complexity than NTRU cryptosystem.

7. ACKNOWLEDGMENTS

We thank Gaborit Philippe, Ohler Julien and Sole Patrick for attracting our interest in this problem and many fruitful discussions.

8. REFERENCES

[1] D. Coppersmith, A. Shamir, "Lattice attacks on NTRU", in EUROCRYPT, (1997), 52-61.

[2] R. Crandall and C. Pomerance, Prime Numbers- A Computational Perspective, Second Edition, Springer, (2005), Section 9.5.1, Karatsuba and ToomCook methods, pg.473.

[3] J. Hoffstein, J. Pipher and J. H. Silverman NTRU: a new high speed public key cryptosystem, Preprint; presented at the rump session of Crypto96, (1996).

[4] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, In Lecture Notes in Computer Science Springer-Verlag, (1998), 267-288.

[5] J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, Science Business Media, Springer, (2014).

[6] IEEE P1363, Standard Specifications For Public-Key Cryptography, http://grouper. ieee.org/groups/1363/.

[7] D. Knuth, The Art of Computer Programming, Volume 2. Third Edition, Addison-Wesley, (1997), pg.294.

[8] R. Kouzmenko, Generalizations of the NTRU cryptosystem, Master's thesis, Polytechnique, Montreal, Canada, (2006).

[9] J. Pipher, Lectures on the NTRU encryption algorithm and digital signature scheme, Brown University, (2002).

[10] R. A. Perlner and D. A. Cooper, Quantum resistant public key cryptography, a survey, in: Proc. of ACM, (2009), 85-93.

[11] J. H. Silverman, A Meet-In-The-Middle on an NTRU Private Key, preprint available from www.ntru.com.

[12] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Review 41 (1999), 303-332.

[13] M. Nevins, C. Karimianpour, A. Miri, Ntru over rings beyond Z, Codes and Cryptography, 56(1) (2010), 65-78.