Noname manuscript No.
(will be inserted by the editor)

ETRU: NTRU over the Eisenstein Integers

Katherine Jarvis · Monica Nevins

June 7, 2013

Abstract NTRU is a public-key cryptosystem based on polynomial rings over $\mathbb{Z}$. Replacing $\mathbb{Z}$ with the ring of Eisenstein integers yields ETRU. We prove through both theory and implementation that ETRU is faster and has smaller keys for the same or better level of security than does NTRU.

Keywords Public-key cryptography · lattice-based cryptography · NTRU · Eisenstein integers

Mathematics Subject Classification (2000) 11T71 · 13G

1 Introduction

The NTRU public key cryptosystem was proposed by J. Hoffstein, J. Pipher and J. H. Silverman in 1996. It has since been standardized [1], [15] and has been implemented both for commercial applications [28] and open-source models [2]. In comparison with RSA and ECC, NTRU is faster and has significantly smaller keys. Moreover, because its security is conjectured to rely on the hardness of certain lattice problems, which are not known to be susceptible to quantum attack, 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's security has been and continues to be scrutinized by the cryptographic community, as a consequence of which the original design underwent several improvements over its first decade.

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 [18], integer matrices [4] or quaternion algebras [22]. The current paper was motivated by [25], in which the integers were replaced with the ring of Eisenstein integers, with

The second author's research is supported by a Discovery Grant from NSERC Canada.

K. Jarvis E-mail: kjarvis@rogers.com · M. Nevins E-mail: mnevins@uottawa.ca
Department of Mathematics and Statistics
University of Ottawa, Canada

the resulting cryptosystem named ETRU. The theoretical functionality of ETRU, and of other variants over suitable Dedekind domains, was proven in [25], but its implementation, and the study of its actual efficiency, was left as an open problem.

In this paper we show that in the basic model ETRU: is faster and has smaller key sizes than NTRU; allows simple encoding of binary messages; and affords a level of security equal to or greater than NTRU. We present a theoretical analysis supported by experimental data, using C++ and Java implementations of ETRU. We use these to experimentally demonstrate the validity of the decryption failure model. We also compare ETRU and NTRU in terms of both their efficiency and their security in light of meet-in-the-middle and lattice attacks. We claim that this presentation of a thorough slate of analytical and experimental evidence to support our claims of greater efficiency and security of an NTRU-variant is an important new contribution to the literature.

Both our division algorithm for Eisenstein integers (Algorithm 1) and the choice of lattice embedding (see Section 8) are integral, thus significantly improving their efficiency over the complex-valued versions proposed in [25]. As [25] was devoted to proving the functionality of NTRU over Dedekind rings, as well as the correctness of the division scheme and the use of a lattice embedding, we do not repeat any of those proofs here.

This paper also builds on the preliminary results obtained in [17] (unpublished), where the first author gave a first implementation of ETRU, based on [25], as well as deriving the decryption failure model presented here in Section 6.3, adapting the meet-in-the-middle attack to ETRU (as in Section 7.2) and implementing the BKZ lattice reduction algorithms used here in Section 8. The current article includes further improvements and deeper analysis, including: Algorithm 1 and further improvements to the efficiency of operations in ETRU; further analysis of decryption failure in Section 6.4; a stronger meet-in-the-middle attack in Section 7 and explicit comparisons of lattice security (Section 8) and keysizes (Theorem 3) for ETRU vs NTRU at comparable parameter sets.

Both ETRU and NTRU were implemented in Java and C++, using Shoup's number theory library for C++ [29]. All timed experiments were performed on a desktop PC with a 2.33 GHz Intel Core2 Quad Q8200 processor running the Windows Vista (64-bit) operating system.

The paper is organized as follows. In Section 2 we introduce the basic form of the NTRU cryptosystem. In Section 3 we present the Eisenstein integers, proving some necessary algebraic results including Theorem 2, towards giving the details necessary for the implementation of the ETRU cryptosystem. At the end of this section we establish how to compare parameter sets of ETRU and NTRU. We then analyze the speed of the ETRU cryptosystem in comparison with NTRU at comparable parameter sets in Section 4, using both theory and data gleaned from our implementation. In Theorem 3 we determine the maximum size of the integer coefficients of our reduced polynomials and consequently compare key sizes with NTRU in Section 5. In Section 6 we address several questions relating to decryption failure in NTRU and ETRU, and in particular establish that the size of the modulus q in ETRU may be chosen to be significantly smaller than the NTRU modulus at comparable parameter sets and yet offer a lower probability of decryption failure.

We then turn to the two major themes in the security of NTRU. In Section 7 we compare the size of the key spaces of NTRU and ETRU, and then describe the modification of a meet-in-the-middle attack to ETRU and the resulting combinatorial security. We find that although ETRU has lower combinatorial security than does

NTRU at comparable parameter sets, this security remains in excess of the key security claimed by NTRU, as published in standardized NTRU parameter sets, and thus remains secure. In Section 8 we analyze lattice attacks against NTRU and ETRU. These are the most significant attacks to date and we establish that at comparable parameter sets ETRU shows greater resistance to lattice attacks.

We summarize and present our conclusions (including that ETRU is faster, smaller, and yet as secure as NTRU) in Section 9, where we also discuss avenues for future work.

Acknowledgments. The authors would like to thank the anonymous referees for several helpful comments, including pointers to recent literature on the use of the FFT in NTRU-like rings. The second author would also like to acknowledge the warm hospitality of the *Institut de Mathématiques et de Modélisation de Montpellier, Université Montpellier II, France*, where this work was completed.

2 The NTRU Cryptosystem

The NTRU public key cryptosystem as described in [8] depends on three integer parameters N, p and q, such that $N > 1$, p and q are relatively prime and q is much larger than p. Commonly p is chosen to be 3, N is chosen to be prime (to reduce the number of factors of $X^N - 1$) and q is power of 2. Let

$$\mathcal{R} = \mathbb{Z}[X]/\langle X^N - 1\rangle$$

be the ring of convolution polynomials of degree $N - 1$. We denote multiplication in the ring $\mathcal{R}$ by $*$. When convenient, we freely identify the polynomial $f = f_0 + f_1X + \cdots + f_{N-1}X^{N-1}$ with the vector $f = (f_0, f_1, \ldots, f_{N-1}) \in \mathbb{Z}^N$.

Given a positive integer n, a polynomial $f \in \mathcal{R}$ is **reduced modulo** n if the coefficients of f all lie in the interval $(-\frac{n}{2}, \frac{n}{2}]$. Let $\mathcal{R}_n \subset \mathcal{R}$ denote the set of polynomials which are reduced modulo n. Given $r \in R$, recall that the notation

$$s \equiv r \mod n$$

means that s is congruent to r modulo n. On the other hand, when we write

$$s = r \mod n$$

we mean to assign to s the unique element of $\mathcal{R}_n$ which is congruent to r modulo n.

Next, one chooses $\mathcal{L}_f$, $\mathcal{L}_g$ and $\mathcal{L}_\phi$ to be certain subsets of $\mathcal{R}$. In general these sets are defined so that elements of $\mathcal{L}_g$ and $\mathcal{L}_\phi$ have a specified number of nonzero coefficients of small norm, equally distributed among all choices (ensuring that these polynomials are divisible by $X - 1$), while $\mathcal{L}_f$ has one additional nonzero coefficient (usually a 1). Although in practice, one chooses different numbers of nonzero coefficients for these sets to take advantage of potential efficiencies in implementation, for simplicity we henceforth assume that there exists $0 < r < 1$ such that the number of nonzero coefficients in elements of $\mathcal{L}_g$ and $\mathcal{L}_\phi$ are both rN, and the number of nonzero entries of elements of $\mathcal{L}_f$ is $rN + 1$. The ratio we take for published parameter sets is the largest of the three, corresponding to elements of $\mathcal{L}_f$.

The quadruple (N, q, p, r) defines the basic public NTRU parameters. Given these parameters, an NTRU private key is an element $f \in \mathcal{L}_f$ which is invertible modulo p and modulo q. Denote by $F_p, F_q \in \mathcal{R}$ representatives of these respective inverses.

Choose $g \in \mathcal{L}_g$. The corresponding NTRU public key is $h = F_q * g \mod q$, which satisfies $f * h \equiv g \mod q$.

To encrypt a binary message M, first map it to a polynomial $m \in \mathcal{R}_p$. Then choose a random polynomial $\phi \in \mathcal{L}_\phi$. Our encrypted message is then

$$e = p\phi * h + m \mod q.$$

To decrypt an encrypted message $e \in \mathcal{R}$ we set

$$a = f * e \mod q,$$

which is equivalent modulo q to $a' = p\phi * g + f * m$. Therefore whenever the coefficients of a' are small enough that a' is already reduced modulo q, we have $a' = a$. Since modulo p we have $F_p * (p\phi * g + f * m) \equiv F_p * f * m \equiv m$, we then recover the original message as

$$m = F_p * a \mod p.$$

If the polynomial a' is not reduced modulo q, however, then we have *decryption failure*; we discuss this further in Section 6. The parameters of NTRU are chosen to minimize or eliminate the probability of decryption failure by ensuring that the coefficients of a' are sufficiently small.

If (f', g') is a pair satisfying $f' * h \equiv g' \mod q$ and for which the expression $p\phi * g' + f' * m$ is reduced modulo q (in particular, for which the coefficients of f' and g' are sufficiently small relative to q and N) then f' is an *alternate decryption key*. For example, any cyclic shift of f is an alternate key.

There are many variations and optimizations on the basic version of NTRU we have summarized here, aimed at improving efficiency and security. These include: replacing the prime $p = 3$ with the polynomial $p = X + 2$, which allows one to work with binary rather than trinary data; choosing the private key of the form $1 + pf$, for $f \in \mathcal{L}_f$, to eliminate one convolution in the decryption process; introducing redundancy and self-referential padding to the message m, to thwart common attacks and reveal decryption failure; and choosing the polynomial ϕ to depend on m through the use of a hash function [13]. In this paper we focus on the basic parameters, referring to the optimized parameters in context or in Section 9.

From this point onwards, we use primed symbols to denote the NTRU parameter set in order to distinguish it from the quadruple of an ETRU parameter set, that is, an NTRU parameter set is a quadruple (N', q', p', r'). We give examples of current NTRU parameter sets in Table 1.

3 The Eisenstein Integers and ETRU

Let ω be a complex cube root of unity, that is $\omega^3 = 1$, where $\omega = \frac{1}{2}\left(-1 + i\sqrt{3}\right)$. The ring of **Eisenstein integers**, denoted $\mathbb{Z}[\omega]$, is the set of complex numbers of the form $a + b\omega$ with $a, b \in \mathbb{Z}$. For $q = a + b\omega$ we have $|q|^2 = a^2 + b^2 - ab$. Write μ_n for the cyclic subgroup of nth roots of unity in $\mathbb{C}$; then note that $\mu_3 = \{1, \omega, \omega^2 = -1 - \omega\}$ and $\mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}$ are both contained in $\mathbb{Z}[\omega]$.

We have two choices of embeddings of $\mathbb{Z}[\omega]$ into $\mathbb{R}^2$. The first is via the isomorphism of additive groups $\mathbb{Z}[\omega] \to \mathbb{Z}^2$ mapping $a + b\omega$ to (a, b); under this embedding, right multiplication by $\alpha = a + b\omega$ is realized by the matrix

$$\langle \alpha \rangle = \begin{bmatrix} a & b \\ -b & a - b \end{bmatrix}. \tag{3.1}$$

Security level	Standard	N'	q'	d_f	r'
"moderate"	NTRU167	167	128	61	0.72
"highest"	NTRU503	503	256	216	0.86
128	APR2011_439	439	2048	146	0.67
256	APR2011_743	743	2048	248	0.67
256	EES1087EP2	1087	2048	120	0.22

Table 1 Some NTRU parameters sets with their specified security levels. In each case $p' = 3$. NTRU167 and NTRU503 are original parameter sets from [8] and [28]; the rest are current parameter sets publicly distributed through [16]. We give $r' = (2d_f - 1)/N'$, the proportion of nonzero coefficients in f.

This is distinct from, and computationally more efficient to use than, the isometric ring monomorphism of $\mathbb{Z}[\omega]$ into $\mathbb{C}$ (identified with $\mathbb{R}^2$) given by $a + b\omega \mapsto (a - b/2) + i(\sqrt{3}b/2)$. What we exploit in the sequel, and which (among rings of algebraic integers) is unique to those of non-real quadratic extensions of $\mathbb{Q}$, is that the image of this isometric embedding is also a lattice in $\mathbb{R}^2$ — in fact the 2-dimensional sphere-packing lattice. This feature allows implies a greater density of elements of $\mathbb{Z}[\omega]$ and also allows us to control the growth of remainders upon division by q in Section 6.

3.1 Eisenstein primes

To extend NTRU to $\mathbb{Z}[\omega]$, a first step is to choose elements $p, q \in \mathbb{Z}[\omega]$ which are relatively prime. In practice, for reasons of efficiency of the inversion algorithms modulo p and q, one prefers to choose them to be prime, or else prime powers. The following is well-known; for a proof see for example [17].

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

Thus the smallest Eisenstein primes (up to multiplication by a unit) are: $p = 1 - \omega$, which has $|p|^2 = 3$; $p = 2$, with $|p|^2 = 4$; and $p = 2 + 3\omega$, with $|p|^2 = 7$.

3.2 The number of residue classes and reduction mod $q \in \mathbb{Z}[\omega]$

Over $\mathbb{Z}$, the number R of residue classes mod q is simply q. Over $\mathbb{Z}[\omega]$, letting $\langle q \rangle = \{rq \mid r \in \mathbb{Z}[\omega]\}$ denote the ideal in $\mathbb{Z}[\omega]$ generated by q, the number of residue classes R is the cardinality of the quotient ring $\mathbb{Z}[\omega]/\langle q \rangle$.

Theorem 2 *Let $q \in \mathbb{Z}[\omega]$ be nonzero. Then the cardinality R of $\mathbb{Z}[\omega]/\langle q \rangle$ is $|q|^2$.*

Proof Write $q = a + b\omega$. If $g = \gcd(a, b)$ then $x = q\overline{q}/g \in \mathbb{Z} \cap \langle q \rangle$; in fact x is the least positive integer in $\langle q \rangle$. We show that the elements of the parallelogram

$$P_q = \{c + d\omega \mid c, d \in \mathbb{Z}, 0 \leq c < x, 0 \leq d < g\} \tag{3.2}$$

are in bijection with $\mathbb{Z}[\omega]/\langle q\rangle$, by showing that for any $\alpha = m+n\omega \in \mathbb{Z}[\omega]$, there exists a unique $\rho \in \langle q\rangle$ such that $\alpha - \rho \in P_q$.

Choose $s, t \in \mathbb{Z}$ so that $sb + ta = g$. With $\alpha = m + n\omega$ as above, let $k \in \mathbb{Z}$ be such that $d = n - kg \in [0, g)$. Then one verifies that $\alpha - q(ks - kt\omega^2) = m' + d\omega$ for some integer m'. Next, find $\ell \in \mathbb{Z}$ such that $c = m' - \ell x \in [0, x)$; as noted above $\ell x \in \langle q\rangle$. Thus with $\rho = q(ks - kt\omega^2) + \ell x \in \langle q\rangle$, we have $\alpha - \rho \in P_q$. Uniqueness follows from properties of the gcd.

Remark 1 It follows that if q is prime then $\mathbb{Z}[\omega]/\langle q\rangle$ is a finite field with $|q|^2$ elements. In light of Theorem 1, these fields are of the form $\mathbb{Z}/p\mathbb{Z}$ with p a rational prime which is not congruent to 2 modulo 3, and a quadratic extension field of $\mathbb{Z}/p\mathbb{Z}$ otherwise.

For example, $\mathbb{Z}[\omega]/\langle 2\rangle$ is a field with four elements, represented by the set $P_2 = \{0, 1, \omega, 1+\omega\}$.

Although P_q as defined in (3.2) is a complete set of residues modulo q, for use with NTRU one prefers a set of residues which is clustered around 0, to decrease the probability of decryption failure. Furthermore, like for P_q, there must exist an efficient algorithm to compute the residue of any element. A logical choice satisfying both requirements arises from isometrically embedding $\mathbb{Z}[\omega]$ and $\langle q\rangle$ as lattices in $\mathbb{C}$, as follows.

First note that $\mathbb{Z}[\omega]$ is a regular hexagonal lattice in $\mathbb{C} \cong \mathbb{R}^2$ with basis $B = \{1, \omega\}$ over $\mathbb{Z}$. It contains a rectangular sublattice L, spanned by $\{1, \sqrt{3}i\}$ over $\mathbb{Z}$, of index 2, with unique nontrivial coset $\omega + L$. See Figure 1.

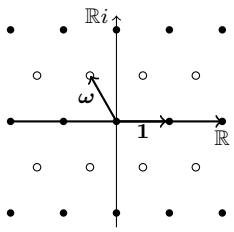

Fig. 1 The dots represent elements of $\mathbb{Z}[\omega]$ in the complex plane. The rectangular sublattice L of $\mathbb{Z}[\omega]$ is represented by solid dots, and its nontrivial coset, $\omega + L$, is represented by open dots.

Given $q \in \mathbb{Z}[\omega]$, the ideal $\langle q\rangle$ is again a lattice, with basis $qB = \{q, q\omega\}$. In analogy with the definition of reduced elements in the lattice $\mathbb{Z}$, we define the set D_q of *reduced elements modulo* q to be those elements of $\mathbb{Z}[\omega]$ contained in the Voronoi cell V_q of the origin of $\langle q\rangle$ (with some exclusion on boundary elements, specified below). Thus the closure of V_q is the region bounded by a certain regular hexagon inscribed between circles of radius $\frac{1}{2}|q|$ and $\frac{1}{\sqrt{3}}|q|$; see Figure 2.

As shown in [25], determining the reduced element $\beta \in D_q$ corresponding to $\alpha \in \mathbb{Z}[\omega]$ is equivalent to finding β and r in $\mathbb{Z}[\omega]$ such that β is reduced modulo q and

$$\alpha = rq + \beta. \tag{3.3}$$

This is equivalent to finding the closest vector $rq \in \langle q\rangle$ to α, or rather, finding the closest $r \in \mathbb{Z}[\omega]$ to $q^{-1}\alpha \in \mathbb{C}$ (and deducing β from (3.3)). This last restatement is the closest vector problem (CVP) in the lattice $\mathbb{Z}[\omega]$, which is solved as follows.

First find the closest vectors to the complex number $q^{-1}\alpha$ on each of the rectangular lattice L spanned by $\{1, i\sqrt{3}\}$, and on its coset $\omega + L$, by rounding each of the coordinates of $q^{-1}\alpha$ (respectively, of $q^{-1}\alpha - \omega$) to the nearest integer multiples of 1 and $i\sqrt{3}$. More precisely, for $\alpha = m + n\omega$ and $q = a + b\omega$, we compute

$$\frac{\alpha}{q} = \frac{\alpha\overline{q}}{|q|^2} = \frac{s + t\sqrt{3}i}{2|q|^2}$$

where $s, t \in \mathbb{Z}$ are given by $s = m(2a-b) + n(2b-a)$ and $t = na - mb$. Writing $\lceil y \rfloor$ for the nearest integer to y (rounding down on half-integers), we deduce that the nearest element on the lattice L to $q^{-1}\alpha$ is

$$r_1 = \left\lceil \frac{s}{2|q|^2} \right\rfloor + \left\lceil \frac{t}{2|q|^2} \right\rfloor \sqrt{3}i =: x_0 + x_1\sqrt{3}i.$$

In Eisenstein coordinates, this is $r_1 = (x_0 + x_1) + 2x_1\omega$. The calculation for $q^{-1}\alpha - \omega$ is similar, yielding $r_2 \in \mathbb{Z}[\omega]$.

Secondly, choose r to be the closer of the two lattice points thus obtained. When $q^{-1}\alpha$ is equidistant from two or more lattice points, a choice is made. In contrast with the algorithm presented in [25], where the choice was arbitrary, we here choose the one geometrically further to the left, which is consistent with our function $\lceil \rfloor$ and thus guarantees correct decoding in the boundary case as well.

See Algorithm 1 for the full details. The set V_q thus obtained is illustrated for $q = 2 + 3\omega$ in Figure 2. Note that the set of reduced elements we obtain mod $p = 2$ is the set $D_2 = \{0, 1, \omega, \omega^2\} = \{0\} \cup \mu_3$, which is more symmetric about 0 than is P_2.

Algorithm 1 Solution to CVP for $\mathbb{Z}[\omega]$

Input: $\alpha = m + n\omega$ and $q = a + b\omega$
Output: (r, β) such that $\alpha = rq + \beta$ and β is reduced modulo q.
Use functions: $|c + d\omega|^2 = c^2 + d^2 - cd$ and $\lceil \frac{c}{d} \rfloor = (c - \overline{c})/d$ where $\overline{c} = c \mod d \in (-d/2, d/2]$.
$\varepsilon_\mathbf{1} := 2a - b$, $\varepsilon_\mathbf{2} := 2b - a$
$\mathbf{Q} := |q|^2$, $\mathbf{d} := 2Q$
Compute the closest vector on the sublattice L:
$\mathbf{s} := m\varepsilon_1 + n\varepsilon_2$, $\mathbf{t} := na - mb$
$\mathbf{x_0} := \lceil s/d \rfloor$, $\mathbf{x_1} := \lceil t/d \rfloor$
$\mathbf{r_1} := (x_0 + x_1) + 2x_1\omega$
$\beta_\mathbf{1} := \alpha - q * r_1 \in \mathbb{Z}[\omega]$
Compute the closest vector on the coset $\omega + L$:
$\mathbf{s'} := s + Q$, $\mathbf{t'} := t - Q$
$\mathbf{y_0} := \lceil s'/d \rfloor$, $\mathbf{y_1} := \lceil t'/d \rfloor$
$\mathbf{r_2} := (y_0 + y_1) + (2y_1 + 1)\omega$
$\beta_\mathbf{2} := \alpha - q * r_2 \in \mathbb{Z}[\omega]$
Choose the closest:
if $|\beta_1|^2 < |\beta_2|^2$ return (r_1, β_1)
elsif $|\beta_1|^2 > |\beta_2|^2$ return (r_2, β_2)
elsif $x_0 < y_0$ return (r_1, β_1)
else return (r_2, β_2)

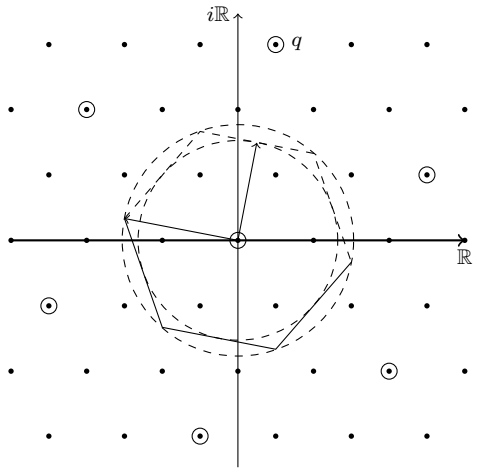

Fig. 2 The open circles represent the elements of the ideal $\langle q \rangle$ with $q = 2 + 3\omega$. The hexagon defines V_q and all elements of $\mathbb{Z}[\omega]$ contained in it (or on the solid line boundary, in general) are elements of D_q. The inscribed and circumscribed circles have radii $|q|/2$ and $|q|/\sqrt{3}$, respectively.

3.3 Complexity of reduction modulo q in $\mathbb{Z}[\omega]$

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

We begin with the built-in integer modulus operation. We generated 100 million pairs of random 4-byte signed integers and compared the cost of multiplying them (0.228 seconds) to taking the first mod the second (0.231 seconds); we conclude that for our purposes we may treat these operations as equally costly. The nearest integer function is based on two calls to the mod operation, so incurs cost $2M$.

The norm function incurs a cost of $3M+2A$. The product of two Eisenstein integers $a + b\omega$ and $c + d\omega$ is given by

$$(a + b\omega)(c + d\omega) = ac - bd + (ad + bc - bd)\omega = ac - bd + (ac + (a - b)(d - c))\omega$$

so has cost $3M + 4A$. The sum of two Eisenstein integers has cost $2A$.

We now turn to Algorithm 1. The first phase has cost $3M + 7A$; the second $11M + 10A$; the third $7M + 11A$ and the final comparison $6M + 4A$. The total cost, of $27M + 32A$, is significantly higher than that of a simple integer modulus, but by a constant factor.

3.4 Defining ETRU

To define ETRU, we choose an integer N (preferably prime) and set $\mathcal{R}^{\mathcal{E}} = \mathbb{Z}[\omega][X]/\langle X^N - 1\rangle$; we also choose p and q in $\mathbb{Z}[\omega]$ relatively prime, with $|q|$ much larger than $|p|$. For any $\alpha \in \mathbb{Z}[\omega]$, let $\mathcal{R}^{\mathcal{E}}_{\alpha}$ denote the set of reduced elements of $\mathcal{R}^{\mathcal{E}}$ modulo α. Note that an element $f \in \mathcal{R}^{\mathcal{E}}$ is a polynomial $f_0 + f_1 X + \cdots + f_{N-1} X^{N-1}$ where each coefficient

is an Eisenstein integer $f_i = a_i + b_i\omega$. Then $f \in \mathcal{R}_\alpha^{\mathcal{E}}$ if and only if each $f_i \in D_\alpha$. We identify f with the vector

$$(a_0, b_0, a_1, b_1, \cdots, a_{N-1}, b_{N-1}) \in \mathbb{Z}^{2N}. \tag{3.4}$$

We choose $p = 2$ throughout, which has several advantages. Reduction modulo 2 is straightforward, and does not require Algorithm 1: given $a + b\omega$, reduce each of a and b to elements of $\{0, 1\}$ modulo 2, replacing $1 + \omega$ with $-1 - \omega$ if it occurs. The encoding of binary messages as elements of $\mathcal{R}_p^{\mathcal{E}}$ is also simple: identify the ith pair of bits ab with the coefficient $a + b\omega$ of X^{i-1}, with the exception that 11 is encoded as $-1 - \omega$. (In contrast, the choice $p = 2 + 3\omega$ was treated in [17]; there remainders are computed via a CVP algorithm and, as $D_p = \{0\} \cup \mu_6$, encoding messages requires some additional data treatment.)

Let $0 < r < 1$ be fixed and let $\mathcal{L}_f$, $\mathcal{L}_g$ and $\mathcal{L}_\phi$ be subsets of $\mathcal{R}^{\mathcal{E}}$ with approximately rN nonzero coefficients which are chosen from μ_6. We choose the sets as follows.

The polynomials in $\mathcal{L}_g$ and $\mathcal{L}_\phi$ should be divisible by $X-1$ modulo q (see Sections 6 and 8, respectively); therefore let s be the nearest multiple of 3 to rN and randomly choose $s/3$ triples of coefficients, each one to be either $\{1, \omega, \omega^2\}$ or $\{-1, -\omega, -\omega^2\}$ in some order. Each such polynomial ψ satisfies $\psi(1) = 0$.

Let t be the nearest integer to rN; we let $\mathcal{L}_f$ consist of all polynomials with t nonzero entries, such that each nonzero entry lies in μ_6. The private key f will be an invertible element of $\mathcal{L}_f$; we note that as with NTRU, a randomly chosen element of $\mathcal{L}_f$ will be invertible with very high probability [30].

The encryption and decryption algorithms are the same as in Section 2.

3.5 On comparing ETRU with NTRU

Since each ETRU coefficient is a pair of integers, an instance of ETRU at degree N is comparable with an instance of NTRU of degree $N' = 2N$. This correspondence is apt: each Eisenstein integer coefficient of the polynomials f, g and ϕ in ETRU is stored as a pair (a, b) of integers representing $a+b\omega$, and for coefficients in μ_6, a and b 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 $\{0\} \cup \mu_6 \subset \mathbb{Z}[\omega]$, whereas all 9 pairs occur in pairs of integers mod 3.

Throughout we therefore compare ETRU with NTRU assuming that $N' \sim 2N$. In practice N' is odd, but where this is irrelevant we may simply set $N' = 2N$ to simplify the discussion.

We also assume $r' = r$, that is, the polynomials have the approximately the same ratio of nonzero coefficients. Note that to take advantage of the efficiency of multiplying by sparse polynomials, it is desirable for r to be small; but to increase combinatorial security in the face of brute force and meet-in-the-middle attacks (see Section 7), one prefers r to be large. For most tests, we assume $r = 2/3$, which is consistent with several parameter choices from Table 1.

In the following sections, we compare ETRU, for parameters $(N, q, p = 2, r)$ with NTRU, for parameters $(N' \sim 2N, q', p' = 3, r' = r)$. We derive the optimal ratio of q to q' in Section 6.

4 Encryption and Decryption Speed

Each encryption requires the user to compute $e = \phi * \tilde{h} + m \mod q$ (where $\tilde{h} = ph \mod q$ can be precomputed and stored as the public key) and each decryption requires the user to compute both $a = f * e \mod q$ and $m = F_p * a \mod p$. Let us discount the costs of integer addition and compare the complexity of encryption and decryption in ETRU and NTRU just as a function integer multiplications.

Computing a sum of polynomials has equal cost for ETRU and NTRU when $N' = 2N$. The convolution of two polynomials of degree $n-1$ requires nominally n^2 ring products. Therefore this cost is $3N^2$ in $\mathcal{R}^{\mathcal{E}}$ whereas for NTRU one needs $N'^2 \sim 4N^2$ integer multiplications. It follows that the convolution of Eisenstein polynomials is faster than for integer polynomials of twice the degree.

From Section 3.3 we know the cost of reducing a coefficient mod q is 27 times more costly for $\mathbb{Z}[\omega]$ than for $\mathbb{Z}$. Therefore in $\mathcal{R}^{\mathcal{E}}$ the total cost of reducing a polynomial mod q is $27N$ whereas for NTRU it is $N' \sim 2N$. Since reducing an Eisenstein polynomial mod $p = 2$ in the decryption step is achieved at the cost of reducing each coefficient modulo 2, it costs only $2N$.

Therefore in total one counts $N'^2 + N' \sim 4N^2 + 2N$ operations for NTRU encryption at $N' \sim 2N$ in contrast to only $3N^2 + 27N$ operations for ETRU encryption. For decryption, we have $2N'^2 + 2N' \sim 8N^2 + 4N$ operations for NTRU and only $6N^2 + 29N$ operations for ETRU. This complexity is essentially independent of the size of q.

To verify the greater speed of ETRU, we first compare the costs of polynomial convolution modulo q of $10,000$ pairs of polynomials from comparable parameter sets in Table 2, for each of NTRU and ETRU. We see that ETRU is significantly faster than NTRU for large N. In fact we see that in implementation the actual cost of the

	NTRU (ms)	ETRU (ms)	ratio
$N = N'/2$	$f * g \mod q'$	$f * g \mod q$	NTRU/ETRU
50	867	708	1.22
100	3312	2419	1.37
150	7174	5075	1.41
200	12773	9056	1.41
250	20040	13721	1.46
Model	$4N^2 + 2N$	$3N^2 + 27N$	~ 1.33

Table 2 Comparison of time, in ms, to compute the convolution product of 10,000 pairs of polynomials modulo q, in each of ETRU ($N, q = 239, p = 2, r = 2/3$) and NTRU ($N' = 2N, q' = 239, p' = 3, r = 2/3$). The rightmost column is the ratio of their speeds and the last row is the estimated number of integer multiplications per convolution.

Eisenstein integer convolution modulo q is smaller than estimated by the model, since the ratio of the two columns exceeds the expected value of $4/3$ for larger values of N.

We next compare the speed of encrypting and decrypting 10,000 messages in ETRU and NTRU for comparable parameter sets, in Figure 3. This data includes the overhead costs of generating messages and the variable ϕ for encryption. We see that the data

in each case fits a quadratic curve, and that for each of encryption and decryption, for $N' = 2N$, ETRU is distinctly faster.

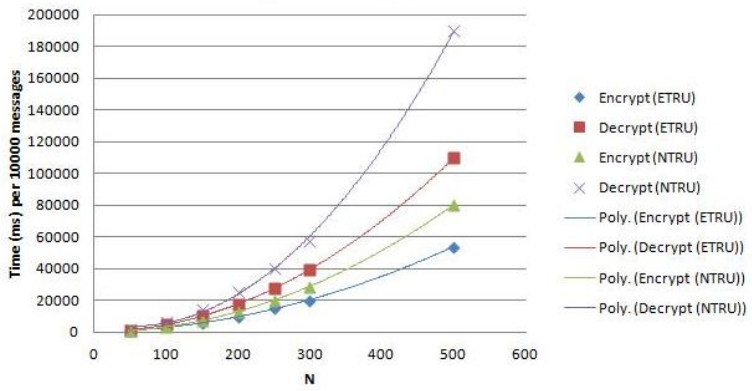

Fig. 3 Encryption/Decryption speed of ETRU vs NTRU. Comparison of time, in ms, to encrypt and decrypt 10,000 random messages in each of ETRU ($N, q = 239, p = 2, r = 2/3$) and NTRU ($N' = 2N, q' = 239, p' = 3, r = 2/3$). The curves are the best-fitting quadratic polynomials to the data.

4.1 Further optimizations

We note that since q is chosen to be prime, one has the possibility of using a number-theoretic transform (that is, FFT) to compute the convolution product. This approach has been adopted in several recent lattice-based cryptographic protocols, including [20].

Namely, if N and q are chosen so that N divides $|q|^2 - 1$, then the field $\mathbb{Z}[\omega]/\langle q \rangle$ contains the group of N^{th} roots of unity; let α be a generator. Then the transform $\mathcal{F}$ given on $f = \sum_{i=0}^{N-1} f_i X^i \in \mathcal{R}_q^{\mathcal{E}}$ by $\mathcal{F}(f)_j = \sum_{i=0}^{N-1} f_i \alpha^{ij}$ has the property that $f * e = \mathcal{F}^{-1}(\mathcal{F}(f) \cdot \mathcal{F}(e))$, where $\cdot$ indicates the simple pointwise product. For example, with $N = 83$ one could choose the prime $q = 51 + 19\omega$, since $|q|^2 = 1993$ and 83 divies 1992. One primitive 83^{rd} root of unity in $\mathbb{Z}[\omega]/\langle q \rangle$ is $\alpha = -11 - 16\omega$.

In general, using a number-theoretic FFT algorithm to compute $\mathcal{F}$ reduces the complexity of the convolution product from $O(N^2)$ to $O(N \log^2(N))$. For sufficiently large N, one would expect this to be more efficient despite the added overhead costs (such as storing the powers of α).

Choosing q so that N divides $|q|^2 - 1$ limits our freedom to choose ETRU parameters which are directly comparable with NTRU, however, and we do not exploit this optimization here.

5 Key Size

As per Theorem 2, there are $|q|^2$ choices for each coefficient of $h \in \mathcal{R}_q^{\mathcal{E}}$. In practice, each coefficient is stored as a pair of integers (a, b) representing $a + b\omega \in \mathbb{Z}[\omega]$. Our

goal in this section is to determine the range of these variables as $a+b\omega$ runs over D_q, which determines the size of the ETRU public key.

Theorem 3 *Let $q \in \mathbb{Z}[\omega]$ and let D_q be the set of reduced elements modulo q. Write $B_s = [-s,s] \times [-s,s] \subset \mathbb{R}^2$. Then the Eisenstein coordinates of the elements in D_q all lie in the bounding box $B_{2|q|/3}$, that is,*

$$\{(c,d) \mid c+d\omega \in D_q\} \subset B_s$$

with $s = 2|q|/3$. There exist choices of q for which this s is optimal; and there exist choices of q for which the inclusion is instead satisfied with $s = |q|/\sqrt{3}$, which is the minimum possible.

Proof It suffices to verify the assertion for the vertices of the Voronoi cell $V_q \supset D_q$. We begin by determining (through geometry or direct calculation) that for $q = 1$ the vertices of V_1 are $\pm\frac{1}{3}(1+2\omega)$, $\pm\frac{1}{3}(1-\omega)$ and $\pm\frac{1}{3}(2+\omega)$. Let $q = a+b\omega$; multiplying the vertices of V_1 by q yields the vertices of V_q. Writing each vertex in the form $c+d\omega$ yields $c, d \in S$ where

$$S = \{\pm\frac{1}{3}(2a-b), \pm\frac{1}{3}(a+b), \pm\frac{1}{3}(2b-a)\}.$$

We see directly, using $|q|^2 = a^2+b^2-ab$, that each of these terms is at most $2|q|/3$ in absolute value, and equality of an element of S to this bound is achieved when either $a = 0$, or $b = 0$ or $a = b$, proving the first two assertions.

Next, we note that if the square of each element in S were at most $|q|^2/3$, then we'd have simultaneously $(a+b)(2a-b) \geq 0$, $(a+b)(a-2b) \leq 0$ and $(a-2b)(2a-b) \geq 0$. This can hold only if one factor (and hence one element of S) is zero, whereupon the other two elements of S are equal in absolute value to $|q|/\sqrt{3}$, proving the remaining assertions.

Remark 2 Geometrically, the theorem is a statement of the fit of D_q within a parallelogram with sides parallel to 1 and ω. The vectors q allowing the best fit (that is, the minimum value of s) are the vectors in the same direction as a vertex of the hexagon V_1, but these are not prime except when $|q| = \sqrt{3}$.

The public key h is a polynomial with N coefficients which are reduced modulo q. Each coefficient consists of two integers which by the theorem can be stored as binary strings of length $\lceil \log_2(4|q|/3) \rceil$, whence the size of the ETRU public key is

$$K^{\mathcal{E}} = 2N\lceil \log_2(4|q|/3) \rceil.$$

An NTRU public key, corresponding to polynomials with $N' = 2N$ coefficients reduced modulo an integer q', has size $K^{\mathcal{N}} = N'\lceil \log_2(q') \rceil$. Therefore to maintain the same key size as NTRU with $N' = 2N$ and $q' = 2^k$, we should choose $|q| \leq \frac{3}{4}q'$ so that $\lceil \log_2(4|q|/3) \rceil \leq \lceil \log_2(q') \rceil$. In Sections 6 and 8 we show that in fact $|q| \sim \frac{3}{8}q'$ is an optimal choice in view of security against decryption failure and lattice attacks. With this choice we have

$$K^{\mathcal{E}} = 2N\lceil \log_2(4|q|/3) \rceil \sim N'\lceil \log_2(q'/2) \rceil \sim K^{\mathcal{N}} - N'.$$

Therefore, the public key for ETRU will be smaller than that of the NTRU public key. These values are computed for comparable parameters in Section 9.

We note that in contrast the coefficients of the private key f and its inverse F_p modulo p are confined to a limited range ($\{0\}\cup\mu_6$ and $\{0\}\cup\mu_3$, for ETRU, and binary or trinary for NTRU, depending on the choice of p) and so may be stored in less space if required, between $4N$ and $8N$ bits.

6 Probability of ETRU Decryption Failure

Recall that a decryption failure occurs if in the encryption of a message m, the polynomial $a' = p\phi * g + f * m$ is not in $\mathcal{R}_q^{\mathcal{E}}$.

6.1 Detectability of decryption failure

Since encryption is probabilistic, the recipient cannot verify that their received message m' is equal to the sent message m by re-encrypting m'. Instead, note that since $X-1$ divides g (and X^N-1), it divides h. Thus the gcd of ph with X^n-1 is divisible by $X-1$, and will be equal to $X-1$ with high probability. In this case, there exist polynomials H and s such that

$$H * ph + s * \frac{X^N-1}{X-1} = 1.$$

Such an H is a called a *pseudo-inverse* [6] of ph, and one can see that for any polynomial ϕ divisible by $X-1$, we have $H*(ph)*\phi \equiv \phi \mod q$. Consequently, since $e-m \equiv p\phi*h \mod q$, we accept the decryption m' of e if $H*(e-m') \in \mathcal{L}_\phi$.

6.2 Weakness induced by decryption failure

In [6], Gama and Nguyen propose the following chosen ciphertext attack. If an attacker can generate pairs (m, m') of messages and failed decryptions, and if the private key f is reduced modulo p, then the attacker can recover f. This succeeds when exactly one coefficient of a' is false, so that $a = a' + \varepsilon$ where ε is a monomial; then $m' - m \equiv F_p * \varepsilon \mod p$, whence the attacker recovers F_p (up to a cyclic shift). Whenever the private key f is reduced mod p, f is uniquely identified as the inverse modulo p of F_p.

We note that ETRU is resistant to this, and similar, chosen ciphertext attacks, since the coefficients of f are chosen from among all six units in $\mathbb{Z}[\omega]$, not just those three which are reduced modulo 2. In this case, the recovery of f modulo 2 by a successful attack must be followed by a search through the 2^{rN} possible values of f with this reduction. We see from Table 6 that this is sufficiently large.

Optimized NTRU is resistant to this kind of attack. For example, choosing f to be of the form $1+p'F$ or $f_1 + f_2 * f_3$, for small polynomials F or f_1, f_2 and f_3, eliminates or reduces the leakage of information from $F_{p'}$, although at the expense of increasing the size of the coefficients and thus increasing the risk of decryption failure. Another tendency is to choose q' sufficiently large so as to eliminate the possibility of decryption failure (see Section 6.5); the tradeoff is a decreased resistance to lattice attack [6].

6.3 Characterizing the probability of decryption failure

Let us model the probability of decryption failure in ETRU with a view towards decreasing or eliminating its occurrence. For NTRU this has been done variously in [5, 18], among others.

We make some simplifying assumptions to model the distribution of the coefficients of the polynomial a'. Assume that rN is evenly divisible by 6 and that the nonzero coefficients of f, g and ϕ are evenly distributed over μ_6 whereas the coefficients of m are evenly distributed over $\mu_3 \cup \{0\}$. Write h_i for the coefficient of X^i in a polynomial $h \in \mathcal{R}^{\mathcal{E}}$.

The coefficients of a' are given by

$$a'_i = p \sum_{j+k \equiv i} \phi_j g_k + \sum_{j+k \equiv i} f_j m_k$$

for each $0 \leq i < N$, where the congruences in the summations are modulo N. If N is large, we may by the central limit theorem model the real and imaginary parts of this sum as a bivariate normal distribution (Y, Z).

Given a pair (j, k), the term $\phi_j g_k$ takes on each value in μ_6 with equal probability $r^2/6$, while $f_j m_k$ takes on each value in μ_6 with equal probability $r/8$. It follows that the mean of the real and imaginary parts of the sum are each zero, and that these parts have correlation coefficient zero. To compute their variance, we note first that

$$Var(Re(\phi_j g_k)) = E((Re(\phi_j g_k))^2) - E(Re(\phi_j g_k))^2 = \frac{1}{4}(4)\frac{r^2}{6} + (1)(2)\frac{r^2}{6} = \frac{1}{2}r^2$$

which is the same value as $Var(Im(\phi_j g_k))$. Similarly,

$$Var(Re(f_j m_k)) = Var(Im(f_j m_k)) = \frac{3}{8}r.$$

This yields total variance of the real and imaginary parts of

$$\sigma_Y^2 = \sigma_Z^2 = p^2 N \frac{1}{2} r^2 + N \frac{3}{8} r = rN(2r + \frac{3}{8}). \tag{6.1}$$

Then the probability distribution function for (Y, Z) for each coefficient $y + zi$ is given by

$$\varphi(y, z) = \frac{1}{2\pi\sigma_Y\sigma_Z} \exp\left(\frac{-(y^2 + z^2)}{2\sigma_Y\sigma_Z}\right).$$

We deduce that the probability that all N coefficients of a' are reduced modulo q (that is, of decryption success) is modelled by

$$P^{\mathcal{E}}(N, q, r) = \left(\int\int_{V_q} \varphi(y, z) dy dz\right)^N.$$

Given the symmetry of the function φ about the origin, we may replace V_q with the rotated region $V_{|q|}$, on which the integral is simpler to compute. Using numerical integration, we plot this probability function, for fixed $N = 53$ and $r = 2/3$, and varying values of $|q|$, in Figure 4.

To confirm the validity of the model and the irrelevance of our simplifying assumptions, we chose a range of Eisenstein primes q and generated private and public keys for

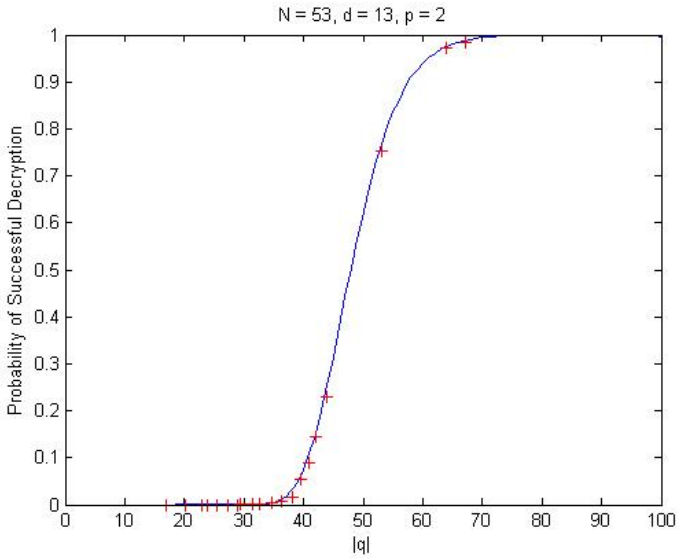

Fig. 4 The probability of decryption success in ETRU as a function of $|q|$, for $N = 53$ and $r = 2/3$. The solid curve represents the function $P^{\mathcal{E}}(N, q, r)$. The crosses represent experimental data. For each q we encrypted 10,000 messages. Plotted is the ratio of these messages which were correctly decrypted.

$N = 53$, $r = 2/3$ and $p = 2$. We chose g and ϕ to satisfy $g(1) = \phi(1) = 0$ by assigning their 36 nonzero entries equally from the six choices in μ_6, but chose the 35 nonzero coefficients of f randomly from μ_6. Then we generated 10,000 random messages and encrypted them with ETRU. The percentage of successful decryptions at each $|q|$ are plotted as crosses on Figure 4. We conclude that the data confirms the validity of our model.

6.4 Comparing decryption failure in ETRU and NTRU

Our next step is to compare the probability of successful decryption of NTRU and ETRU as functions of $|q|$. In [18], Kouzmenko applied this analysis to NTRU with trinary coefficients, where the coefficients of a' are modelled as real Gaussian random variables with mean zero and variance $\sigma'^2 = rN'(9r + \frac{2}{3})$. (His analysis included the possibility of different ratios of nonzero coefficients for each of the sets $\mathcal{L}_f, \mathcal{L}_g$ and $\mathcal{L}_\phi$, in substantially the same way as presented here.) Thus the probability of successful decryption in NTRU is determined by way of the Gaussian cumulative distribution function Φ as

$$P^{\mathcal{N}}(N', q', r) = \left(2\Phi\left(\frac{q'}{2\sigma'}\right) - 1\right)^{N'}.$$

To determine the value of $|q|$ for which the probability of decryption failure of ETRU is less than or equal to that of NTRU, for $N' = 2N$ and same r, let us underestimate the probability of successful decryption of each Eisenstein integer coefficient as the integral

r	N	q'	$\log_2(1-P)$	$\lvert q\rvert$	$q'/\lvert q\rvert$
0.25	25	64	−22	26	2.5
0.25	50	64	−11	26	2.4
0.5	25	64	−7	25	2.5
0.5	50	64	−3	26	2.5
0.25	100	128	−22	52	2.5
0.25	200	128	−11	53	2.4
0.5	100	128	−7	50	2.5
0.5	200	128	−3	51	2.4
0.5	100	256	−25	97	2.6
0.5	200	256	−13	99	2.6
0.75	100	256	−12	97	2.6
0.75	200	256	−6	99	2.6
0.75	200	512	−23	190	2.7
0.75	300	512	−16	192	2.7

Table 3 Values of $|q|$ (rounded to nearest integer) vs q' at which the probability of decryption failure is equal, for various combinations of parameters N, $N' = 2N$, and r. Given is the approximate value of $\log_2(1-P)$, the probability of decryption failure for a single Eisenstein coefficient in ETRU or of at most two integer coefficients in NTRU.

of $\varphi(y,z)$ over the disk C of radius $|q|/2$ inscribed inside V_q. This integral admits a closed-form solution

$$\widetilde{P}^{\mathcal{E}}(N,q,r) = \left(\int\int_C \varphi(y,z)dydz\right)^N = \left(1 - exp\left(-|q|^2/(8\sigma^2)\right)\right)^N.$$

Lacking a similar expression for $P^{\mathcal{N}}$, we simply solve for $|q|$ in the equality $\widetilde{P}^{\mathcal{E}}(N,q,r) = P^{\mathcal{N}}(2N,q',r)$ for various choices of N, r and q' (limited by the precision of our calculator) to obtain the values in Table 3. We see that the ratio of q' to $|q|$ at which the decryption probability is equal increases slightly as N, r and q' increase, and is about 2.6 or 2.7 for larger N and q.

6.5 Elimination of decryption failure

We claim that for the most recent parameter sets (Table 1), q' is chosen sufficiently large as to eliminate the possibility of decryption failure. Namely, since our coefficients are all units, the maximum absolute value of any coefficient of the convolution is equal to the number of nonzero entries of one polynomial. It follows that, independent of the distribution of the nonzero coefficients in f, g, and ϕ, and independent of m, no coefficient of $a' = p'\phi * g + f * m$ can exceed $rN'(p'+1) = 4rN'$ in absolute value. Therefore decryption is guaranteed to be successful if $q'/2 > 4rN'$. This is the case for EES1087EP2 as written. In the APR class, in reality g is chosen to have far fewer nonzero entries and the coefficients of the resulting a' are also less than $q'/2$.

On the other hand, decryption success in ETRU is guaranteed if the largest possible (absolute) value of any coefficient, $rN(p+1) = 3rN$, lies in the disk C of radius

$|q|/2$. This yields the bound $|q| > 6rN$, lower than the comparable NTRU bound $q' > 8rN' \sim 16rN$.

Hence for NTRU parameter sets which allow no decryption failure, we may choose $|q| \sim \frac{3}{8}q'$ for ETRU. This gives a ratio $q'/|q| \sim 2.67$ which is consistent with our results in Table 3. We conclude that for $N' \sim 2N$ and low or zero level of decryption failure, choosing q so that

$$|q| \sim 3q'/8 \tag{6.2}$$

will provide ETRU with an equivalent level of protection against decryption failure as NTRU.

7 Combinatorial Security of ETRU

7.1 Brute force search and key space size

Given a ciphertext e, equal to $p\phi * h + m$, an attacker can recover m if he determines any of the polynomials f, g, ϕ or (obviously) m. One option is brute force search: finding $f' \in \mathcal{L}_f$ such that modulo q we have $h * f' \in \mathcal{L}_g$, or finding $\phi' \in \mathcal{L}_\phi$ such that $e - p\phi' * h$ mod q is reduced modulo p; or else, using the pseudo-inverse H of h as described in Section 6, finding m', reduced mod p, such that modulo q, $H * (e - m') \in p\mathcal{L}_\phi$, or finding $g' \in \mathcal{L}_g$ such that modulo q, $H * g' \in \mathcal{L}_f$.

The sizes of the sets to be searched are as follows. There are (minus conditions on valid messages introduced by padding schemes or other security measures) approximately 4^N valid choices for m'. By construction, $\mathcal{L}_g$ and $\mathcal{L}_\phi$ have size

$$|\mathcal{L}_g| = |\mathcal{L}_\phi| = \binom{N}{rN} \sum_{k=0}^{\frac{rN}{3}} (rN; k, k, k, \frac{rN}{3} - k, \frac{rN}{3} - k, \frac{rN}{3} - k)$$

where $(\sum n_i; n_1, \cdots, n_k)$ is a multinomial coefficient. The set $\mathcal{L}_f$ consists of invertible (mod q) polynomials with rN nonzero entries chosen from μ_6. In practice one generates an f with rN nonzero entries chosen from μ_6 then verifies its invertibility (which occurs with overwhelming probability). Hence for the purposes of a brute-force search we estimate

$$|\mathcal{L}_f| = \binom{N}{rN} 6^{rN},$$

as compared with $(N'; rN'/2, rN'/2 - 1)$ for NTRU. Some sample values are computed in Table 4.

7.2 Meet in the middle attack and combinatorial security

Instead of a brute force search, the attacker may employ a meet-in-the-middle attack, as proposed by Odlyzko and presented in [12] for $p = 2$, which aims to halve the effective size of the key space. Since recovering f is the most desirable option for the attacker, and since Gama and Nguyen proved in [6] that the existence of a decryption oracle for NTRU (in the presence of decryption failures) implied the recovery of f, we restrict our discussion to this case.

The method of the meet-in-the-middle attack is to search for polynomials f_1 and f_2, each with half the nonzero entries of f such that $f = f_1 + f_2$. Given a list of candidates f_1 and f_2, a successful choice will satisfy that $h*(f_1+f_2) = h*f_1 + h*f_2$, modulo q, lies in $\mathcal{L}_g$, and so is in part characterized by the property that the coefficients of $h*f_1$ and $-h*f_2$ differ, modulo q, by a coefficient of g (which is small).

Let $\mathcal{F}$ be the set of polynomials of degree $\lfloor N/2 \rfloor - 1$ with $\lfloor rN/2 \rfloor$ nonzero coefficients chosen from μ_2 for NTRU and from μ_6 for ETRU; this set is a valid choice as it includes the first half of at least one cyclic shift of f. Define $\mathcal{F}^2$ in a similar manner to include the second half of f (thus consisting of polynomials of degree $N-1$, divisible by $x^{\lfloor N/2 \rfloor}$, and with the complementary number of nonzero entries from appropriate sets). The proposed approach is to sort the $f_1 \in \mathcal{F}$ into bins, whose label is the sequence of the most significant (sign) bits of each of the first k coefficients of $h*f_1$ (modulo q). (For ETRU, where each coefficient is a pair of integers, one chooses simply the first k integer components.)

For each $f_2 \in \mathcal{F}^2$, if $-h*f_2$ gives a sequence whose bin is occupied by some f_1, then the first k integer coefficients of $h*f_1 + h*f_2$ are relatively small. Set $f' = f_1 + f_2$ and compute $h*f' \mod q$. If all its coefficients have norm at most 1, then f' is potentially a key.

Otherwise, and before rejecting f_2, one must additionally verify some adjacent bins, to account for all bins corresponding to $-h*f_2 + g$ for varying choices of g.

For NTRU with $p = 3$, one must account for cases in which the most significant bit of $-h*f_2$ changes upon adding ± 1; this happens with probability $\mathcal{P} = 4/q'$.

For ETRU one must account for cases in which the most significant bit of one of the integer coefficients of $-h*f_2$ changes upon adding an element of μ_6. This occurs for approximately $2/3$ of the elements lying near the boundary of the domain D_q, as well as for those elements with that coefficient equal to 0 or -1. We estimate the number of these elements as the ratio of the area of the corresponding regions in V_q to the determinant $d = \sqrt{3}/2$ of the lattice $\mathbb{Z}[\omega]$. The area of a hexagon with inner radius r is $2\sqrt{3}r^2$; hence the area of the boundary strip of width 1 in V_q (where $r = |q|/2$) is $2\sqrt{3}(|q|-1)$. The area of a diagonal strip of width 2 in V_q is at least $2|q|$. Thus the number of elements is $\frac{2}{\sqrt{3}}\left(\frac{2}{3}\cdot 2\sqrt{3}(|q|-1) + 2|q|\right) \sim 5|q|$. Since there are $|q|^2$ elements in total, the probability that a single integer coefficient is affected is approximately $\mathcal{P} = 5/|q|$. If $|q| \sim \frac{3}{8}q'$ then this probability is $10/3$ times that for NTRU.

The probable number of bins to be checked for each f_2 is $2^{k\mathcal{P}}$. We see that the number of additional bins that may need to be checked is significantly higher for ETRU than for NTRU, slightly increasing the complexity of the attack on ETRU versus on NTRU.

As per [12], to carry out the attack effectively one should choose k so that $2^k >> |\mathcal{F}|$; thus most bins are empty, decreasing the number of unsuccessful checks of $(f_1 + f_2)*h$. Then $2^{k\mathcal{P}}$ is effectively a small constant and the complexity of this attack is simply proportional to $|\mathcal{F}| \sim |\mathcal{F}^2|$, corresponding to generating the candidates for f_1 and f_2 and computing the necessary convolutions.

For NTRU we have (omitting the floor function for brevity) $|\mathcal{F}| = 2^{rN'/2}\binom{N'/2}{rN'/2}$ whereas for ETRU we have $|\mathcal{F}| = 6^{rN/2}\binom{N/2}{rN/2}$. Comparing these with $|\mathcal{L}_f|$ in each case, we see that as expected, the meet-in-the-middle attack effectively halves the log-size of the keyspace.

Parameter set	NTRU167	APR2011_439	EES1087EP2
NTRU N'	167	439	1171
ETRU N	83	223	541
Security level (bits)	-	**128**	**256**
$\|\mathcal{L}_f\|$ NTRU	255	686	> 1000
$\|\mathcal{F}\|$ NTRU	127	343	529
$\|\mathcal{L}_f\|$ ETRU	222	568	719
$\|\mathcal{L}_g\|$ ETRU	210	562	705
$\|\mathcal{F}\|$ ETRU	109	286	357

Table 4 Approximate $\log_2$ of key space size and level of combinatorial security in light of meet-in-the-middle attacks (the log size of $|\mathcal{F}|$) of NTRU vs ETRU at $N' \sim 2N$ in specified parameter sets, compared with specified security level.

We compare the sizes of the key spaces, and the combinatorial security of NTRU and ETRU in light of the meet-in-the-middle attack, with the prescribed security level of some parameter sets in Table 4. Where necessary, we used Stirling's approximation and the bounds

$$\frac{1}{4rN}\left(\frac{(1-r)^{r-1}}{r^r}\right)^N \leq \binom{N}{rN} \leq \left(\frac{(1-r)^{r-1}}{r^r}\right)^N, \tag{7.1}$$

valid for $\frac{1}{2} \leq r < 1$, from [32], to estimate the values of binomial coefficients. We note that in each case where a security level is specified, the combinatorial security of NTRU far exceeds its target security parameter. In particular, we note that although ETRU has smaller key spaces and lower combinatorial security than NTRU for comparable parameter sets (due largely to the smaller value of N), ETRU maintains a combinatorial security well in excess of the prescribed value. Thus we conclude that ETRU is secure against brute force and meet-in-the-middle attacks at these levels.

8 Lattice Security of ETRU

The most critical measure of the security of NTRU is its resistance to lattice attacks, as pioneered in [5], and further analyzed in [10]. The lattices to be attacked in NTRU (8.2) and ETRU (8.5) are generalizations of so-called *ideal lattices*, whose use in cryptography is growing in prominence. In the case of ETRU, the set

$$\{(f, g) \in \mathcal{R}^{\mathcal{E}} \times \mathcal{R}^{\mathcal{E}} \mid f * h \equiv g \mod q\} \tag{8.1}$$

is an $\mathcal{R}^{\mathcal{E}}$-module (*i.e.* a generalization of an ideal) and a $4N$-dimensional integral lattice. The vector corresponding to the private key pair (f, g) is a short vector in this lattice, and one could therefore discover the private key (or perhaps an alternate) if one could find a sufficiently short vector in the lattice. The shortest vector problem on random lattices, under suitable assumptions, is NP-hard [23] but it is an open problem if this is true of the subclass of ideal lattices. It is also unknown if the SVP, in general or on this subclass, admits a quantum polynomial-time solution.

Lattice attacks use lattice basis reduction techniques, such as LLL [19], BKZ [27] or BKZ 2.0 [3], to identify a short vector. For a fixed parameter $\delta \in (0.25, 1)$, LLL runs in polynomial time, but may fail to produce a basis containing sufficiently small vectors. It may however be run with increasingly large δ until a vector of a given target norm is found, at the cost of exponential running time in n [24]. BKZ has an additional parameter, corresponding to block size, and is more efficient in practice. Several further improvements have been made to BKZ, leading to BKZ 2.0, implemented in [3]. In our experiments, we applied classical BKZ with a blocksize of 10 and $\delta = 0.99$, as implemented in the G_BKZ_FP algorithm from Shoup's NTL library [29].

Throughout this section, we freely identify f with the row vector corresponding to the polynomial f as in (3.4). Given a polynomial h of degree $n-1$, let H be its $n \times n$ circulant matrix, that is, the matrix satisfying $fH = f * h$ where $f * h$ is the usual convolution.

8.1 The NTRU lattice

Given the public key h' of an instance of NTRU with parameters $(N', q', p' = 3, r)$, let H' be its circulant matrix and let $L^{\mathcal{N}}$ be the lattice generated by (right multiplication by) the $2N' \times 2N'$ matrix

$$\begin{bmatrix} I_{N'} & H' \\ 0 & q' I_{N'} \end{bmatrix}. \tag{8.2}$$

Since $L^{\mathcal{N}}$ consists of all vectors (f, g) in $\mathbb{Z}^{2N'}$ satisfying $f * h' \equiv g \mod q'$, our private key (f, g) is a short element of this lattice, having norm approximately $\sqrt{2rN'}$. By the Gaussian heuristic, the expected shortest vector of a lattice L of dimension n and volume v has length [26]

$$s = \sqrt{\frac{n}{2\pi e}} v^{1/n}. \tag{8.3}$$

For a given dimension of lattice, it has been observed that the likelihood of success of LLL in finding a target vector of (short) length t increases as the ratio s/t increases [11]. For $L^{\mathcal{N}}$ we have $n = 2N'$ and $v = {q'}^{N'}$, so $s^{\mathcal{N}} = \sqrt{N'q'/(\pi e)}$ whereas the norm of the key (f, g) is $t^{\mathcal{N}} = \sqrt{2rN'}$. Thus the relevant ratio is

$$c^{\mathcal{N}} = \sqrt{q'/(2\pi e r)}, \tag{8.4}$$

which in practice has proven to be small enough to allow NTRU at current parameter sizes to withstand lattice reduction attacks.

Alternately, for an n-dimensional lattice L [7] and [3] propose the (nth root of the) Hermite factor $\gamma_n = t/v^{1/n}$ as a measure of the effort required of a lattice reduction algorithm to succeed; this has been shown to be an effective measure on random lattices. The Hermite factor for most NTRU parameter sets is less than 1, reflecting the non-random nature of the NTRU lattice. Instead, [7] and [3] compute the Hermite factor of an algorithm achieving a target vector in an NTRU lattice of norm less than q'; this yields $\gamma_{2N'} = \sqrt{q'}$.

8.2 The ETRU lattice

We fix an isomorphism of $\mathbb{Z}[\omega]$ with $\mathbb{Z}^2$ and define $\langle\alpha\rangle$, as in (3.1).[1] Note that $\det(\langle\alpha\rangle) = |\alpha|^2$. Given an $n \times n$ matrix A with entries in $\mathbb{Z}[\omega]$, write $\langle A\rangle$ for the $2n \times 2n$ matrix over $\mathbb{Z}$ in which each entry a_{ij} is replaced with the 2×2 block $\langle a_{ij}\rangle$. Then the lattice $L^{\mathcal{E}}$ corresponding to (8.1) in $\mathbb{Z}^{4N}$ is given by (right multiplication by) the matrix

$$\begin{bmatrix} I_{2N} & \langle H\rangle \\ 0 & \langle qI_N\rangle \end{bmatrix}. \tag{8.5}$$

Again, the private keys of ETRU correspond to short vectors of $L^{\mathcal{E}}$.

The length of the expected shortest vector of $L^{\mathcal{E}}$, as computed from (8.3), is $s^{\mathcal{E}} = \sqrt{2N|q|/(\pi e)}$. Our keys f and g each have rN nonzero entries, each of which has norm 1 as an element of $\mathbb{C}$. However, viewed as vectors in this lattice, we have

$$\pm 1 = (\pm 1, 0), \quad \pm\omega = (0, \pm 1), \quad \pm\omega^2 = (\mp 1, \mp 1),$$

so that the norm of the target vector (f, g) lies between $\sqrt{2rN}$ and $\sqrt{4rN}$. For the sake of discussion, we will assume the coefficients are equally distributed, so that $t^{\mathcal{E}} = \sqrt{8rN/3}$. We calculate that the ratio

$$c^{\mathcal{E}} = s^{\mathcal{E}}/t^{\mathcal{E}} = \frac{1}{2}\sqrt{3|q|/(\pi er)}. \tag{8.6}$$

Similarly, one may compute the Hermite factor required for a lattice reduction algorithm to produce a target vector of length at most $|q|$; as for NTRU, this gives a Hermite factor for ETRU of $\sqrt{|q|}$.

8.3 Comparing $L^{\mathcal{N}}$ and $L^{\mathcal{E}}$

Note that for $N' = 2N$, the NTRU and ETRU lattices have the same dimension. However, the smaller size of $|q|$ reduces the ratio of the length of the expected shortest vector to the length of the target vector for $L^{\mathcal{E}}$. Comparing (8.4) with (8.6) with $q' \sim \frac{8}{3}|q|$ yields

$$c^{\mathcal{N}} \sim \frac{4}{3}c^{\mathcal{E}}.$$

Consequently one expects that ETRU will have the stronger lattice for the same dimension. Alternately, comparing Hermite factors supports the same hypothesis: that $L^{\mathcal{E}}$ is more resistant to lattice attack than is $L^{\mathcal{N}}$.

To test their lattice strength, we generated repeated lattice attacks on each of the ETRU and NTRU lattices at comparable parameter sets.

For each parameter set, and each of several gradually increasing values of N, we generated 1000 pairs of keys (f, g). We then applied BKZ reduction with a fixed block size of 10 to the resulting lattice. The attack was considered successful only if the resulting lattice basis contained a suitably short vector. We recorded the rate of success of these attacks, that is, the percentage of the 1000 cases for which the attack yielded a potential key.

[1] The isometric embedding of $\mathbb{Z}[\omega]$ into $\mathbb{C}$ was chosen in [25] instead, but it was shown in [17] that as the resulting lattice is not integral, the corresponding LLL and BKZ attacks are significantly slower and less effective for the attacker.

We present the comparison of two pairs of matched parameters in Figure 5: NTRU at $q' = 1024$ versus ETRU at $q = 383$, as well as NTRU at $q' = 2048$ vs ETRU at $q = 761$. In each case, the ETRU lattice shows equal or greater resistance to lattice

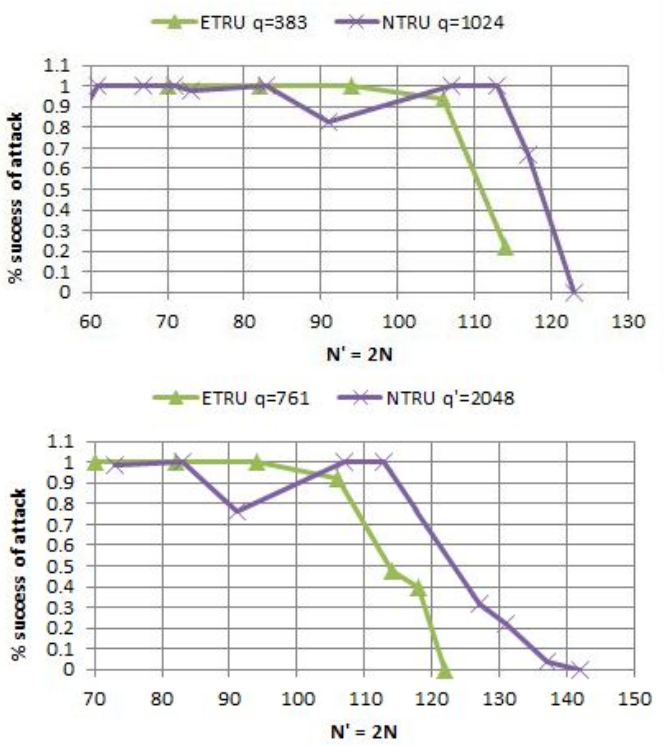

Fig. 5 ETRU vs NTRU lattice strength tests. Comparison of success rate of BKZ attack as a function of (half the) lattice dimension for ETRU $(N, q, p = 2, r = 2/3)$ and NTRU $(N' \sim 2N, q', p' = 3, r = 2/3)$, for two pairs of comparable moduli, $|q| \sim \frac{3}{8}q'$.

attack as the dimension of the lattice increases. We observe that the success profile of the BKZ attack on the ETRU lattice is very uniform, in contrast to the NTRU lattice, where BKZ fails on some inputs for some isolated small values of N'. Nevertheless, the overall tendency observed for both lattices (and typical of NTRU lattice attacks [8]) is the existence of a point of sharp decline in BKZ attack success, after which the attack consistently fails. We see that the dimension of lattice at which this point occurs for ETRU is slightly lower than its NTRU counterpart, and that for similar-sized lattices, ETRU exhibits the greater resistance to lattice attack overall.

We summarize the results of our repeated lattice attacks in Table 5 by giving the interval in which the point of sharp decline (measured as the point at which BKZ succeeds half the time) occurred, for each of our tests. We see that $L^{\mathcal{E}}$ thwarts the lattice attack at a smaller dimension than does $L^{\mathcal{N}}$.

These tests suggest that, as anticipated, an ETRU lattice shows some greater resistance to lattice attacks than does a corresponding NTRU lattice. Lattice attacks

ETRU	N	$N' = 2N$	NTRU	N'
$q = 47$	$[31, 35]$	$[62, 70]$	$q' = 128$	$[73, 83]$
$q = 99 + 7\omega$	$[35, 41]$	$[70, 82]$	$q' = 256$	$[83, 91]$
$q = 191$	$[41, 47]$	$[82, 94]$	$q' = 512$	$[97, 103]$
$q = 383$	$[53, 57]$	$[106, 114]$	$q' = 1024$	$[117, 123]$
$q = 761$	$[53, 57]$	$[106, 114]$	$q' = 2048$	$[113, 127]$

Table 5 Summary of results of BKZ tests on several pairs of comparable q, q' (6.2) for ETRU and NTRU, with $r = 2/3$. Given in each case is the interval of values of N and N' prior to which BKZ always succeeded in at least 50% of the trials and after which BKZ always failed in at least 50% of trials. The dimension of the lattice in each case is $4N$ and $2N'$, respectively. We compute $2N$, which is to be compared with N'. Note that $|99 + 7\omega| \sim 96$.

are the strongest known attack on NTRU [9]; consequently, we assert that ETRU has equal or greater security at $N' \sim 2N$ and $q' \sim \frac{8}{3}|q|$ than does NTRU.

9 Conclusions and Future Work

We conclude with a summary of sample NTRU parameter sets and comparable ETRU parameter sets in Table 6.

Security	NTRU		ETRU				
level	Name	keysize	N	q	rN	r	keysize
-	NTRU167	1169	83	47	60	0.72	996
-	NTRU503	4024	251	$99 + 7\omega$	216	0.86	3514
128	APR2011_439	4829	223	761	144	0.65	4460
256	APR2011_743	8173	373	761	246	0.66	7460
256	EES1087EP2	11957	541	761	120	0.22	10820

Table 6 ETRU parameter sets (with $p = 2$) with comparable security to established NTRU parameter sets (with $p' = 3$). In each case, N is chosen to be prime near $N'/2$ and q is chosen to be an Eisenstein prime whose norm is close to $\frac{3}{8}q'$ (using Theorem 1). The ETRU keysize was computed in Section 5.

The theory and evidence support that ETRU is a cost-effective, fast alternative to NTRU, offering comparable or better security for smaller key sizes and higher speed. The essential ingredient which offers ETRU such an advantage over prior alternative NTRU variants is that the ring $\mathbb{Z}[\omega]$ has greater density of elements than rings such as $\mathbb{Z}[i]$ or $M_2(\mathbb{Z})$, and its multiplication, although algebraically more complex, is computationally simpler per pair of integers. The relatively large number of units in $\mathbb{Z}[\omega]$ not only provides resistance against chosen ciphertext attacks, but also reduces the expected size of the coefficients in any convolution product, thus reducing the probability of decryption failure. The use of $\mathbb{Z}[\omega]$ also provides a nontrivial improvement to NTRU's resistance to lattice-based attacks due to the lower value for $|q|$.

There are many further directions to pursue. It would be interesting to adapt the meet-in-the-middle attack presented in Section 7 to search for $g = g_1 + g_2$, which lies in a smaller sized key space already; the attack described is unable to exploit the restricted nature of the coefficients of g to achieve a lower complexity. It would be interesting to adapt the hybrid attack proposed by Howgrave in [14] to ETRU, particularly in light of the slightly smaller key space size of ETRU.

Recent progress has been made on the effective extrapolation of the security of a given random lattice in the face of BKZ and BKZ 2.0 reduction [7,3]. In particular, the work of Y. Chen and P.Q. Nguyen includes a simulation algorithm which predicts the number of iterations and blocksize of BKZ 2.0 required to find a suitably short vector, as well as means to compute the cost of running this algorithm. This is a vast improvement over the extrapolations from small blocksize used in, for example, [10]. However, as the authors take care to point out, their algorithm is designed for a random lattice and may not apply to $L^{\mathcal{N}}$. Determining its analogue for ideal lattices in general or NTRU-like lattices in particular would solidify our understanding of the true practical security of NTRU and its analogues.

It would be interesting to further explore the use of the FFT, as discussed in Section 4.1, to speed up convolution in ETRU. This implies choosing parameters so that N divides $|q|^2 - 1$. Since $|q| \sim 6rN$ implies $|q|^2 \in O(N^2)$, we can expect to find pairs (N, q) with the necessary divisibility properties which also meet the conditions specified in this paper, close to any target size of N.

In this paper we restricted our comparison to the basic model. Optimized NTRU also chooses g and ϕ to be more sparse than f, for greater efficiency, and f of the form $1 + pF$ to remove one convolution in the decryption process; these may be equally applied to ETRU. One should also analyse, in the ETRU setting, the padding schemes employed in optimized NTRU, as well as adapting to this case the hash functions evaluated on the message m in the choice of the randomizing element ϕ.

Stehlé and Steinfeld [31] recently proposed modifications to NTRU under which the resulting system can be proven to be CPA-secure (with certain constraints on the parameters, and assuming the hardness of the worst-case SVP on certain ideal lattices). In particular, the most significant of these modifications — replacing the modulus polynomial $X^N - 1$ with the irreducible polynomial $X^N + 1$, N prime — makes the resulting NTRU ring into the ring of integers of a cyclotomic field, where all the results of [21] are shown to hold. To generalize this proof of security to an ETRU variant, one must determine if those results extend also to cyclotomic extensions of other number fields (in particular the number field $\mathbb{Q}[\omega]$). (We note that in fact many of the results in [21] are shown to hold in the much broader setting of rings of algebraic integers.) Proving the security of such an ETRU-variant would support the thesis that the introduction of the Eisenstein integers does not itself introduce any new weakness to the NTRU cryptosystem.

More generally, extending NTRU's base ring to other rings of algebraic integers (in particular those corresponding to cyclotomic fields) holds much promise. The challenge lies in choosing a division algorithm whose remainders are small enough to avoid decryption failure. As mentioned in Section 3, the CVP method on $\mathbb{Z}[\omega]$ used here gives the optimal solution for 2 dimensions, but does not directly generalize to higher dimensions.

References

1. Accredited Standards Committee, *Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry*, ANSI X9.98-2010, American National Standards Institute, 2010.
2. T. Buktu, The NTRU Project, `http://ntru.sf.net/`
3. Y. Chen and P.Q. Nguyen, *BKZ 2.0: better lattice security estimates* in Advances in cryptology — ASIACRYPT 2011, pages 1-20, Lecture Notes in Comput. Sci., 7073, Springer, Heidelberg, 2011.
4. M. Coglianese and B.-M. Goi, *MaTRU: A New NTRU-Based Cryptosystem*, INDOCRYPT 2005, Lecture Notes in Computer Science 3797, pages 232-243, Springer-Verlag, 2005.
5. D. Coppersmith and A. Shamir, *Lattice Attacks on NTRU*, Advances in Cryptology, EUROCRYPT '97, Lecture Notes in Computer Science 1233, pages 52-61, Springer-Verlag, 1997.
6. N. Gama and P.Q. Nguygen, *New Chosen-Ciphertext Attacks on NTRU*, Public key cryptography PKC 2007, Lecture Notes in Computer Science 4450, pages 89–106, Springer-Verlag, 2007.
7. N. Gama and P.Q. Nguygen, *Predicting Lattice Reduction*, Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science 4965, pages 31-51, 2008.
8. J. Hoffstein, J. Pipher and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, Algorithmic Number Theory, Lecture Notes in Computer Science 1423, pages 267-288, Springer-Verlag, 1998.
9. J. Hoffstein, J. Pipher and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Undergraduate Texts in Mathematics, Springer, 2008.
10. J. Hoffstein, J. H. Silverman and W. Whyte, *Estimated Breaking Times for NTRU Lattices*, NTRU Cryptosystems Technical Report 12, Version 2, updated 2006. Available from: http://www.ntru.com. Accessed: Dec. 2010.
11. J. Hoffstein, N. Howgrave-Graham, J. Pipher and W. Whyte, *Practical lattice-based cryptography: NTRUEncrypt and NTRUSign*, The LLL Algorithm: Survey and Applications, pages 349-390, Information Security and Cryptography, Springer-Verlag, 2010.
12. N. Howgrave-Graham, J. H. Silverman and W. Whyte, *A Meet-in-the-Middle Attack on an NTRU Private Key*, NTRU Cryptosystems Technical Report 4, Version 2, updated 2006. Available from: http://www.ntru.com. Accessed: Dec. 2010.
13. N. Howgrave-Graham, J. H. Silverman, A. Singer, and W. Whyte, *NAEP: Provable Security in the Presence of Decryption Failures*, Available from: http://www.securityinnovation.com. Accessed: September 2012.
14. N. Howgrave-Graham, *A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU*, CRYPTO 2007, Lecture Notes in Computer Science 4622, pages 150-169, 2007.
15. IEEE Computer Society, *IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices*, IEEE Std 1363.1-2008, The Institute of Electrical and Electronics Engineers, 2009.
16. `net.sf.ntru.encrypt` package, J@rvana (jarvana.com), 2011.
17. K. Jarvis, *NTRU over the Eisenstein Integers*, Masters Thesis, University of Ottawa, 2011.
18. R. Kouzmenko, *Generalizations of the NTRU Cryptosystem*, Diploma Project, École Polytechnique Federale de Lausanne, 2005-2006.
19. A. K. Lenstra, H. W. Lenstra, and L. Lovasz, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261, pages 515-534, 1982.
20. V. Lyubashevsky, D. Micciancio, C. Peikert and A. Rosen, *SWIFFT: A Modest Proposal for FFT Hashing*, Fast Softward Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 2008, pages 54-72; Lecture Notes in Computer Science, Vol 5086, 2008.
21. V. Lyubashevsky, C. Peikert and O. Regev, *On ideal lattices and learning with errors over rings*. Advances in cryptology — EUROCRYPT 2010, 1-23, Lecture Notes in Comput. Sci., 6110, Springer, Berlin, 2010.
22. 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.
23. D. Micciancio, *The Shortest Vector Problem is NP-hard to approximate to within some constant*, SIAM Journal on Computing, Vol 30, No 6, pages 2008-2035, 2001.
24. D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671 of The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Boston, Massachusetts, 2002.

25. M. Nevins, C. Karimianpour and A. Miri, *NTRU over rings beyond* $\mathbb{Z}$, Designs, Codes and Cryptography, Volume 56, Number 1, pages 65-78, 2010.
26. P. Q. Nguyen, *Hermite's Constant and Lattice Algorithms*, The LLL Algorithm: Survey's and Applications, pages 16-69, Information Security and Cryptography, Springer-Verlag, 2010.
27. C. P. Schnorr, *A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms*, Theoretical Computer Science 53, pages 201-224, 1987.
28. Security Innovation, The Application Security Company, SSL Encryption Library, http://www.securityinnovation.com, 2012.
29. V. Shoup. *NTL: A Library for doing Number Theory*. http://www.shoup. net/ntl/. Accessed: Aug. 2010.
30. J. H. Silverman, *Invertibility in Truncated Polynomial Rings*, NTRU Cryptosystems Technical Report 9, Version 1, 1998. Available from: `http://www.securityinnovation.com`. Accessed September 2012.
31. D. Stehlé and R. Steinfeld, *Making NTRU as secure as worst-case problems over ideal lattices*, Advances in cryptology — EUROCRYPT 2011, 27-47, Lecture Notes in Comput. Sci., 6632, Springer, Heidelberg, 2011.
32. E. W. Weisstein, "Binomial Coefficient." From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/BinomialCoefficient.html`