# ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices 

## (ILTRU: An NTRU-Like Lattice-based Cryptosystem)

Amir Hassani Karbasi<br>Dept. of Mathematics<br>University of Guilan<br>Rasht, Iran<br>karbasi@phd.guilan.ac.ir

Reza Ebrahimi Atani<br>Dept. of Computer Engineering<br>University of Guilan<br>Rasht, Iran<br>rebrahimi@guilan.ac.ir


#### Abstract

In this paper we present a new NTRU-Like public key cryptosystem with security provably based on the worst case hardness of the approximate both Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) in some structured lattices, called ideal lattices. We show how to modify the ETRU cryptosystem, an NTRU-Like public key cryptosystem based on the Eisenstein integers $\mathbb{Z}\left[\zeta_{3}\right]$ where $\zeta_{3}$ is a primitive cube root of unity, to make it provably secure, under the assumed quantum hardness of standard worst-case lattice problems, restricted to a family of lattices related to some cyclotomic fields. The security then proves for our main system from the already proven hardness of the R-LWE and R-SIS problems.


Keywords- Lattice-based cryptography; Ideal lattices; ETRU; Provable security; Dedekind domain.

## I. Introduction

The users to communicate over non-secure channels without any prior communication can use public key cryptography. The concept of public key cryptography was first proposed by Diffie and Hellman in 1976 [1]. Latticebased cryptography has attracted considerable interest in recent years as a post-quantum cryptography [6]. It enjoys very strong security proofs based on worst-case hardness, relatively efficient implementations, as well as great simplicity. Our focus here will be mainly on the theoretical aspects of lattice-based cryptography.

The NTRU cryptosystem which is a famous lattice-based crypto scheme devised by Hoffstein, Pipher and Silverman, was first presented at the Crypto'96 rump session [2]. Although its structure relies on arithmetic over the quotient polynomial ring $\mathbb{Z}_{q}[x] /<x^{N}-1>$ for $N$ prime and $q$ a small integer, it was quickly observed that breaking it could be expressed as a problem over Euclidean lattices [3]. At the ANTS' 98 conference, the NTRU authors presented an improved variant including a thorough assessment of its practical security against lattice attacks [4]. The NTRU cryptosystem standard number and version is IEEE P1363.1 [5]. The NTRU encryption (NTRUEncrypt) system is also often considered as the most practical post-quantum public key crypto scheme [6] and this scheme uses the properties of structured lattices to achieve high efficiency but its security remains heuristic and it was an important open challenge to provide a provably secure scheme with comparable efficiency.

By rising number of attacks and practical variants of NTRU, provable security in lattice-based cryptography is developed. The first provably secure lattice-based cryptosystem was presented by Ajtai and Dwork [8], and relied on a variant of GapSVP in arbitrary lattices also it is now known to rely on GapSVP [9]. Ajtai's average-case problem is
now reflected to as the Small Integer Solution problem (SIS). Another major achievement in this field was the introduction in 2005 of the Learning with Errors problem (LWE) by Regev [13]. Micciancio [10] presented an alternative based on the worst-case hardness of the restriction of Poly(n)-SVP to cyclic lattices and succeeded in restricting SIS to structured matrices while preserving a worst-case to average-case reduction, which correspond to ideals in polynomial ring $\mathbb{Z}[x] /\left\langle x^{n}-1\right\rangle$. Subsequently, Lyubashevsky and Micciancio [11] and independently Peikert and Rosen [12] showed how to modify Micciancio's function to construct an efficient and provably secure collision resistant hash function. So, they introduced the more general class of ideal lattices, which correspond to ideals in polynomial rings $\mathbb{Z}_{q}[x] /<\Phi>$ with a $\Phi$ that is irreducible cyclotomic polynomial, also is sparse (e.g., $\Phi=x^{n}+1$ for $n$ a power of 2). Their system relies on the hardness of the restriction of Poly(n)-SVP to ideal lattices (called Poly $(n)$-IdealSVP). The average-case collision-finding problem is a natural computational problem called Ideal-SIS, which has been reflected to be as hard as the worst-case instances of Ideal-SVP. In 2011, Stehlé and Steinfeld [14] proposed a structured variant of the NTRU, which they proved as hard as CPA security from the hardness of a variant of R-SIS and R-LWE (Ring Learning with Errors problem). R-LWE has great efficiency and provides more natural and flexible cryptographic constructions. The current paper was motivated by [14], in which the integers were replaced with the ring of Eisenstein integers, with the resulting cryptosystem named ILTRU.

The ETRU obtained from the NTRU by replacing $\mathbb{Z}$ with the ring of Eisenstein integers [7]. It is faster and has smaller size of keys for the same or better level of security than that of NTRU. Both division algorithm for Eisenstein integers and the choice of lattice embedding are integral, thus significantly improving their efficiency over the complex-valued versions proposed in [15]. Note that the ETRU security is based on both SVP and CVP then its security remains heuristic.

In this paper, our proposed ILTRU cryptosystem exploits the properties of the ETRU structured lattice to achieve high efficiency and it has IND-CPA security based on ideal lattices with established hardness of R-SIS and R-LWE problems. We prove that our modification of ETRU is provably secure, assuming the quantum hardness of standard worst-case problems over ideal lattices (for $\Phi=<x^{n}+x^{n-1}+\ldots+x+1>$ with $n+l$ a prime).

The rest of this paper is structured as follows: In section II, we shortly review the ETRU system and explain the security related to the computational problems. In section III, we study ideal lattices and ring learning with errors problem. In section IV, we suggest a key generation algorithm, where the generated public key follows a distribution for which Ideal-SVP reduces to R-LWE. In section V, we make the ETRU as secure as worst-case problems over ideal lattices, called ILTRU. Finally, the paper concludes in section VI.

## II. The ETRU Cryptosystem

## A. Parameters Creation

We denote by $\zeta_{3}$ a complex cube root of unity, that is $\zeta_{3}^{3}=1$ where $\zeta_{3}=1 / 2(-1+\sqrt{3} i)$ since $\zeta_{3}^{3}-1=\left(\zeta_{3}-1\right)\left(\zeta_{3}^{2}+\zeta_{3}+1\right)=0$, we have $\zeta_{3}^{2}+\zeta_{3}+1=0$ and hence $\zeta_{3}^{2}=-1-\zeta_{3}$. The ring of Eisenstein integers, denoted $\mathbb{Z}\left[\zeta_{3}\right]$, is the set of complex numbers of the form $\alpha=a+b \zeta_{3}$ with $a, b \in \mathbb{Z}$. For $\alpha=a+b \zeta_{3}$ we will define $d(\alpha)=\alpha \bar{\alpha}=a^{2}+b^{2}-a b$ which is the square of the usual analytic complex norm $|\alpha|$. Note that $d(\alpha)$ is a positive integer for $\alpha \neq 0$ since $d(\alpha)$ is the square of a norm and $a, b \in \mathbb{Z}$. For any complex numbers $\alpha, \beta$ we have that $|\alpha \beta|=|\alpha| \cdot|\beta|$ hence it follows that $d(\alpha \beta)=d(\alpha) \cdot d(\beta)$. The Eisenstein integers $\mathbb{Z}\left[\zeta_{3}\right]$ form a lattice in $\mathbb{C}$ generated by the basis $B=\left\{1, \zeta_{3}\right\}$. Note that the two basis vectors 1 and $\zeta_{3}$, represented by the vectors $(1,0)$ and $(-1 / 2, \sqrt{3} / 2)$ in $\mathbb{R}^{2}$, have 120 degrees with equal length. Let $\beta$ be an Eisenstein integer. We define the ideal $L(\beta)=\left\{a \beta+b \beta \zeta_{3} \mid a, b \in \mathbb{Z}\right\}$. Therefore $L(\beta)$ is a lattice generated by the basis $\left\{\beta, \beta \zeta_{3}\right\}$. According to [7], we deduce that the Eisenstein integers are an Euclidean domain that the units and Eisenstein primes exist. For each matrix $B$ with entries that are Eisenstein integers we will set $\langle B\rangle$ to be the $2 n$ by $2 n$ matrix. We choose an prime $n$ and set $\left.R=\mathbb{Z}\left[\zeta_{3}, x\right] /<x^{n}-1\right\rangle$, we also choose $p$ and $q$ in $\mathbb{Z}\left[\zeta_{3}\right]$ relatively prime, with $|q|$ much larger than $|p|$. Since each ETRU coefficient is a pair of integers, an element of ETRU at degree $n$ is comparable with an element of NTRU of degree $n^{\prime}=2 n$.

## B. Key Generation

Private key consists of two randomly chosen polynomials $f, g$ in $R$. We define the inverses $F_{q}=f^{-1}$ in $R_{q}$ and $F_{p}=f^{-1}$ in $R_{p}$. Hence public key is generated by $h=F_{q} * g$. The public key $h$ is a polynomial with $n$ coefficients which are reduced modulo $q$. Each coefficient consists of two integers which by theorem 3 in [7] can be stored as binary strings of length $\left\lceil\log _{2}(4|q| / 3)\right\rceil$, hence the size of the ETRU public key is $K=2 n\left\lceil\log _{2}(4|q| / 3)\right\rceil$. An NTRU public key, corresponding to polynomials with $n^{\prime}=2 n$ coefficients reduced modulo an integer $q^{\prime}$, has size $K^{\prime}=n^{\prime}\left\lceil\log _{2}\left(q^{\prime}\right)\right\rceil$. Therefore to maintain the same key size as NTRU with $n^{\prime}=2 n$ and $q^{\prime}=2^{k}$, we should choose $|q| \leq(3 / 4) q^{\prime}$ so that $\left\lceil\log _{2}(4|q| / 3)\right\rceil \leq\left\lceil\log _{2}\left(q^{\prime}\right)\right\rceil$.

## C. Encryption

Each encryption requires the user to compute $e=\phi^{*} p h+m \bmod q$ where $m$ is a plaintext and $\phi$ is a ephemeral key. In total one counts $n^{\prime 2}+n^{\prime} \sim 4 n^{2}+2 n$ operations for NTRU encryption at $n^{\prime} \sim 2 n$ in contrast to only $3 n^{2}+27 n$ operations for ETRU encryption.

## D. Decryption

Each decryption requires the user to compute both $a=f * e \bmod q$ and $m=F_{p} * a \bmod p$. For decryption, we have $2 n^{\prime 2}+2 n^{\prime} \sim 8 n^{2}+4 n$ operations for NTRU and only $6 n^{2}+29 n$ operations for ETRU.

## E. Decryption Failure and Security

In [7] is shown that in fact $|q| \sim(3 / 8) q^{\prime}$ is an optimal choice in view of security against decryption failure and lattice attacks. With this choice the public key size for ETRU will be smaller than that of the NTRU public key.

## III. Ideal Lattices and The R-LWE Problem

Our study is restricted to the sequence of rings $R=\mathbb{Z}\left[\zeta_{3}\right][x] / \Phi$ with $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ where $n+1$ is a prime that $\Phi$ is irreducible cyclotomic polynomial. The R-LWE problem is known to be hard when $\Phi$ is cyclotomic [16]. Our security analysis for the modified ETRU scheme (ILTRU) allows encrypting and decrypting $\Omega(n)$ plaintext bits for $\tilde{O}(n)$ bit operations, while achieving security against $2^{g(n)}$-time attacks, for any $g(n)$ that is $\Omega(\log n)$ and $o(n)$, assuming the worst-case hardness of poly(n)-Ideal-SVP against $2^{O(g(n))}$-time quantum algorithms for each element component-wise in complex pair-wise system because note that each polynomial in $R$ has its coefficients of the form $\left(a_{i}, b_{i} \zeta_{3}\right)$ where $a_{i}, b_{i} \in \mathbb{Z}$, so in this paper, all operations execute for $a_{i}$ 's and $b_{i}{ }^{\prime} s$ separately, that is, $\mathbb{C} \cong \mathbb{R}^{2}$. the latter assumption is believed to be valid for any $g(n)=o(n)$.

## A. Notation

Similar to [14] we denote by $\rho_{\sigma}(x)$ (respectively $v_{\sigma}$ ) the standard $n$-dimensional Gaussian function (respectively distribution) with center 0 and variance $\sigma$. We denote by $\operatorname{Exp}(\mu)$ the exponential distribution on $\mathbb{R}$ with mean $\mu$ and by $U(E)$ the uniform distribution over a finite set $E$. If $D_{1}$ and $D_{2}$ are two distributions on discrete oracle $E$, their statistical distance is $\Delta\left(D_{1} ; D_{2}\right)=1 / 2 \sum_{x \in E}\left|D_{1}(x)-D_{2}(x)\right|$. We write $z \leftarrow D$ when the random variable $z$ is chosen from the distribution $D$. The integer $n$ is called the lattice dimension. The minimum $\lambda_{1}(L)$ (respectively $\left.\lambda_{1}^{\infty}(L)\right)$ is the Euclidean (respectively infinity) norm of any shortest vector of $L \backslash 0$. The dual of lattice $L$ is the lattice $\hat{L}=\left\{c \in R^{n}: \forall i,<c, b_{i}>\in \mathbb{Z}\right\}$ where the $b_{i}$ 's are a basis of $L$. For a lattice $L, \sigma>0$ and $c \in \mathbb{R}^{\mathrm{n}}$, we define the lattice Gaussian distribution of support $L$, deviation $\sigma$ and center $c$ by $D_{L, \sigma, c}(b)=\rho_{\sigma, c}(b) / \rho_{\sigma, c}(L)$, for any $b \in L$. We extend the definition of $D_{L, \sigma, c}$ to any $M \subseteq L($ not necessarily a sub-lattice $)$, by setting $D_{M, \sigma, c}(b)=\left(\rho_{\sigma, c}(b)\right) /\left(\rho_{\sigma, c}(M)\right)$. For
$\delta>0$, we denote the smoothing parameter $\eta_{\delta}(L)$ as the smallest $\sigma>0$ such that $\rho_{1 / \sigma}(\hat{L} \backslash 0) \leq \delta$. It quantifies how large $\sigma$ needs to be for $D_{L, \sigma, c}$ to behave like a continuous Gaussian. We will typically consider $\delta=2^{-n}$.

## B. Definition

Let $n+1$ be a prime and $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ which is irreducible over $\mathrm{Q}\left[\zeta_{3}\right]$ also let $R=\mathbb{Z}\left[\zeta_{3}\right][x] / \Phi$. An (integral) ideal $I$ of $R$ is a subset of $R$ closed under addition and multiplication by arbitrary elements of $R$. By mapping polynomials to the vectors of their coefficients, we see that an ideal $I \neq 0$ corresponds to a full-rank sub-lattice of $\mathbb{Z}^{n}$. Thus we can view $I$ as both a lattice and an ideal. An ideal lattice for $\Phi$ is a sub-lattice of $\left(\mathbb{Z}^{*} \mathbb{Z}\right)^{n}$ that corresponds to a non-zero ideal $I \subseteq R$. The algebraic norm $N(I)$ is equal to det $I$, where $I$ is regarded as a lattice. In the following, an ideal lattice will implicitly refer to a $\Phi$-ideal lattice.

By restricting SVP (respectively $\gamma-$ SVP) to instances that are ideal lattices, we obtain Ideal-SVP (respectively $\gamma$ -ideal-SVP). The latter is implicitly parameterized by the polynomial $\Phi=x^{n}+x^{n-1}+\ldots+x+1$. No algorithm is known to perform non-negligibly better for $\gamma$-ideal-SVP than for $\gamma$-SVP [14].

## C. Properties of The Ring $R$

For $v \in R$ we define by $\|v\|$ its Euclidean norm. We denote the multiplicative expansion factor by $\gamma_{x}(R)=\max _{u, v \in R}(\|u \times v\|) /(\|u\| \cdot\|v\|)$. Since $\Phi$ is the $n+l$-th cyclotomic polynomial, the ring $R$ is exactly the maximal order of the cyclotomic field $K:=\frac{\mathrm{Q}\left[\zeta_{3}\right][x]}{\Phi} \cong \mathrm{Q}\left[\zeta, \zeta^{\prime}\right]$. We denote by $\left(\sigma_{i}, \sigma_{i}^{\prime}\right)_{i \leq n}$ the complex embeddings. We can choose $\left(\sigma_{i}, \sigma_{i}^{\prime}\right): K \rightarrow K\left(\zeta^{2 i+1}, \zeta^{2 i+1}\right)$ for $i \leq n$.

Lemma 1. The norm of $\alpha$ as an element in $\mathbb{Q}\left(\zeta_{3}\right)$ is $a^{2}+b^{2}-a b$. This is also $|\alpha|^{2}$, where $\alpha$ is denoted as an element of $\mathbb{C}$.

Proof. The minimal polynomial of $\zeta_{3}$ over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_{3}=x^{2}+x+1$. Thus, there exist exactly two monomorphisms (isomorphisms in this case) from $\mathbb{Q}$ to $\mathbb{C}$ fixing $\mathbb{Q}$ and permuting the roots of $\Phi_{3}$. Since $\Phi_{3}$ has two roots $\zeta_{3}$ and $\zeta_{3}^{2}$, the embeddings are $\sigma_{1}\left(a+b \zeta_{3}\right)=a+b \zeta_{3}$ and $\sigma_{2}\left(a+b \zeta_{3}\right)=a+b \zeta_{3}^{2}$, where $a, b \in \mathbb{Q}$. By definition, the algebraic norm of $\alpha=a+b \zeta_{3}$ is

$$
\begin{aligned}
N(\alpha) & =\sigma_{1}(\alpha) \sigma_{2}(\alpha) \\
& =\left(a+b \zeta_{3}\right)\left(a+b \zeta_{3}^{2}\right)
\end{aligned}
$$

Note that $\zeta_{3}^{2}=\bar{\zeta}_{3}$ and $\zeta_{3}+\bar{\zeta}_{3}=-1$. So we have

$$
\begin{aligned}
N(\alpha) & =\left(a+b \zeta_{3}\right)\left(a+b \bar{\zeta}_{3}\right) \\
& =a^{2}+b^{2}+a b\left(\zeta_{3}+\bar{\zeta}_{3}\right) \\
& =a^{2}+b^{2}-a b
\end{aligned}
$$

Now we show that $d(\alpha)=N(\alpha)=|\alpha|^{2}$.

$$
\begin{aligned}
|\alpha|^{2} & =\left|a+b \zeta_{3}\right|^{2} \\
& =\left|a+b\left(\frac{-1+\sqrt{3 i}}{2}\right)\right| \\
& =\left|a-\frac{b}{2}+\frac{b \sqrt{3 i}}{2}\right|^{2} \\
& =\left(a-\frac{b}{2}\right)^{2}+\left(\frac{b \sqrt{3}}{2}\right)^{2} \\
& =a^{2}+b^{2}-a b
\end{aligned}
$$

In rest of the paper, all of computations are done component-wise for each complex element as an integer. We define $T_{2}$-norm by $T_{2}(\alpha)^{2}=\sum_{1 \leqslant \ll 3}\left|\sigma_{i}(\alpha)\right|^{2}$. We also use the fact that for any $\alpha \in R$, we have $|N(\alpha)|=\operatorname{det}\langle\alpha\rangle$, where $\langle\alpha\rangle$ is the ideal of $R$ generated by $\alpha$. Let $q$ be a prime element such that $\Phi$ has $n$ distinct linear factors modulo $q$, that is, $\Phi=\prod_{i \leqslant n}\left(x-\zeta^{i}\right) \bmod q$ where $\zeta$ is a primitive $n+l$-th root of unity modulo $q$. Also we know that $R_{q}=R / q R$.

## D. R-LWE

In [14] is shown that R-SIS and R-LWE are dual so in this paper we discuss only about R-LWE and the results for R-SIS are trivial. For $s \in R_{q}$ and $\psi$ a distribution in $R_{q}$, we have $A_{s, \psi}$ as the distribution obtained by sampling the pair (a,as+e) with $(a, e) \leftarrow U\left(R_{q}\right) \times \psi$. The Ring Learning With Errors problem (R-LWE) was introduced by Lyubashevsky et al.[16] and shown hard for specific error distributions $\psi$. The error distributions $\psi$ that we use are an adaptation of those introduced in [16].
Definition 1. The Ring Learning With Errors Problem with parameters $q, \alpha, \Phi\left(R-L W E_{q, \alpha}^{\Phi}\right)$ is as follows. Let $\psi \leftarrow \overline{\mathrm{Y}}_{\alpha}$ and $s \leftarrow U\left(R_{q}\right)$ where $\overline{\mathrm{Y}}_{\alpha}$ is a family of distributions. Given access to an oracle $O$ that produces samples in $R_{q} \times R_{q}$, distinguish whether $O$ outputs samples from $A_{s, \psi}$ or from $U\left(R_{q} \times R_{q}\right)$. The distinguishing advantage should be $1 / \operatorname{poly}(n)\left(\right.$ resp. $\left.2^{-o(n)}\right)$ over the randomness of the input, the randomness of the samples and the internal randomness of the algorithm [14].

Theorem 1 in [14] indicates that R-LWE is hard, assuming that the worst-case $\gamma$-Ideal-SVP cannot be efficiently solved using quantum computers, for small $\gamma$. It was recently improved by Lyubashevsky et al. [18] if the number of samples that can be chosen to the oracle $O$ is bounded by a constant (which is the case in our application), then the result also holds with simpler errors than $e \leftarrow \psi \leftarrow \bar{\Upsilon}_{\alpha}$, and with an even smaller Ideal-SVP approximation factor $\gamma$. This should allow to both simplify the modified ETRU and to strengthen its security guarantee.

## E. Variants of R-LWE

For $s \in R_{q}$ and $\psi$ a distribution in $R_{q}$, we denote $A_{s, \psi}^{\times}$as the distribution obtained by sampling the pair ( $a, a s+e$ ) with $(a, e) \leftarrow U\left(R_{q}^{\times}\right) \times \psi$, where $R_{q}^{\times}$is the set of invertible elements of $R_{q}$. This variant is hard and called $R-L W E^{\times}$as [14]. Furthermore, as explained in [18], the nonce $s$ can also be sampled from the error distribution without incurring any security loss. We call this variant $R-L W E_{H N F+}^{\times}$. According to lemmata 7, 8 and 9 as well as theorem 2 in [14] the problems $R-L W E^{\times}$and $R-L W E_{H N F+}^{\times}$are dual to $\gamma$-Ideal-SVP and are defined some families of $R$-modules for $I$, an arbitrary ideal of $R_{q}$ as a lattice, also short vectors exist in ideal and statistical distance (regularity bound) is exactly appropriate and reliable.

## IV. Revised Key Generation Algorithm

We now use the results of the previous section on modular ideal lattice to derive a key generation algorithm for the ETRU for each component in vectors, where the generated public key follows a distribution for which Ideal-SVP reduces to R-LWE. Algorithm 1 is as follows.

$$
\begin{aligned}
& \text { Input: } n, q \in \mathbb{Z}, p \in R_{q}^{\times}, \sigma \in \mathbb{R} . \\
& \text { Output: A key pair }(s k, p k) \in R \times R_{q}^{\times} . \\
& \text {Sample } \quad\left(f, f^{\prime}\right)^{\prime} \quad \text { from } \quad D_{\mathbb{Z}^{n}, \sigma} ; \\
& \text { let }\left(f, f^{\prime}\right)=(p, p) \cdot\left(f, f^{\prime}\right)^{\prime}+(1,1) \text {; if }((f, f) \bmod q) \notin R_{q}^{\times}, \\
& \text {resample. Sample }\left(g, g^{\prime}\right) \text { from } D_{\mathbb{Z}^{n}, \sigma} ; \text { if }\left(\left(g, g^{\prime}\right) \bmod q\right) \\
& \notin R_{q}^{\times}, \text {resample. Return secret key } s k=\left(f, f^{\prime}\right) \text { and public } \\
& \text { key } p k=\left(h, h^{\prime}\right)=(p, p)\left(g, g^{\prime}\right) /\left(f, f^{\prime}\right) \in R_{q}^{\times} .
\end{aligned}
$$

The following Theorem ensures that for some appropriate choice of parameters, the key generation algorithm terminates in expected polynomial time.

Theorem 1[Adapted from 14]. Let $n \geq 8$ and $n+1$ be a prime such that $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ splits into $n$ linear factors modulo prime $q \geq 5$ component-wise. Let $\sigma \geq \sqrt{n \ln (2 n(1+1 / \delta)) / \pi} \cdot q^{1 / n}$, or an arbitrary $\delta \in(0,1 / 2)$. Let $\left(a, a^{\prime}\right) \in R$ and $(p, p) \in R_{q}^{\times}$Then $\operatorname{Pr}_{\left(f, f^{\prime}\right)^{\prime} \leftarrow D_{\mathbb{Z}^{n}, \sigma}}\left[\left((p, p) .\left(f, f^{\prime}\right)^{\prime}+\left(a, a^{\prime}\right) \bmod q\right) \notin R_{q}^{\times}\right] \leq n(1 / q+2 \delta)$ component-wise.

The following Lemma ensures that the generated secret key is small.
Lemma 2[Adapted from 14]. Let $n \geq 8$ and $n+1$ be a prime such that $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ splits into $n$ linear factors modulo prime $q \geq 8 n$. Let $\sigma \geq \sqrt{2 n \ln (6 n) / \pi} \cdot q^{1 / n}$. The secret key polynomials $\left(f, f^{\prime}\right),\left(g, g^{\prime}\right)$ returned by the algorithm 1 satisfy, with probability $\geq 1-2^{-n+3}:\left\|\left(f, f^{\prime}\right)\right\| \leq 2 n\|(p, p)\| \sigma$ and $\left\|\left(g, g^{\prime}\right)\right\| \leq \sqrt{n} \sigma$. If $\operatorname{deg}(p, p) \leq(1,1)$, then $\left\|\left(f, f^{\prime}\right)\right\| \leq 4 \sqrt{n}\|(p, p)\| \sigma$ with probability $\geq 1-2^{-n+3}$ component-wise.

Theorem 3 in [14] shows that the public key can be uniformly distributed in the whole ring and this satisfy cryptographic pseudo randomness for our algorithm 1, which seems necessary for exploiting the established hardness of R-LWE (and R-SIS). Now we can modify and construct the ETRU cryptosystem over ideal lattices with high efficiency and provable security (CPA-secure).

## V. ILTRU CRYPTOSYSTEM

Using our new results above, we describe a modification of the ETRU cryptosystem for which we can provide a security proof under a worst-case hardness assumption.

## ILTRU Encryption Scheme <br> Parameters Creation:

1. We use $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ with $n \geq 8$ and $n+1$ a prime, $R=\mathbb{Z}\left[\zeta_{3}\right][x] / \Phi$ and $R_{q}=R / q R$ with $q \geq 5$ prime such that $\Phi=\prod_{k=1}^{n} \phi_{k}$ in $R_{q}$ with distinct $\phi_{k}$ 's component-wise.

Key Generation:
2. We use the algorithm 1 and return $s k=\left(f, f^{\prime}\right) \in R_{q}^{\times} \quad$ with $\quad\left(f, f^{\prime}\right) \equiv(1,1) \bmod (p, p) \quad, \quad$ and $p k=\left(h, h^{\prime}\right)=(p, p)\left(g, g^{\prime}\right) /\left(f, f^{\prime}\right) \in R_{q}^{\times}$component-wise.

## Encryption:

3. Given message $\left(M, M^{\prime}\right) \in P$, set $s, e \leftarrow \bar{\Upsilon}_{\alpha}$ and return ciphertext $\left(C, C^{\prime}\right)=\left(h, h^{\prime}\right) s+(p, p) e+\left(M, M^{\prime}\right) \in R_{q}$.

## Decryption:

4. Given ciphertext $\left(C, C^{\prime}\right)$ and secret key $\left(f, f^{\prime}\right)$, compute $\left(C, C^{\prime}\right)^{\prime}=\left(f, f^{\prime}\right) .\left(C, C^{\prime}\right) \in R_{q}$ and return $\left(C, C^{\prime}\right)^{\prime} \bmod$ ( $p, p$ ).

## A. Decryption Failure

The correctness condition for each pairwise coefficient in the ILTRU cryptosystem is as follows.
Lemma 3 [Adapted from 14]. If $\omega\left(n^{1.5} \log n\right) \alpha \operatorname{deg}((p, p))\|(p, p)\|^{2} \sigma<(1,1) \quad$ (resp. $\omega\left(n^{0.5} \log n\right) \alpha\|(p, p)\|^{2} \sigma<(1,1)$ if $\left.\operatorname{deg}(p, p) \leq(1,1)\right)$ and $\alpha q \geq n^{0.5}$, then the decryption algorithm of the ILTRU recovers $\left(M, M^{\prime}\right)$ with probability $1-n^{-\omega(1)}$ over the choice of $s, e, f, f^{\prime}, g, g^{\prime}$ component-wise.
Proof. In the decryption algorithm, we have $\left(C, C^{\prime}\right)^{\prime}=(p, p) .\left(\left(g, g^{\prime}\right) s+e\left(f, f^{\prime}\right)\right)+\left(f, f^{\prime}\right)\left(M, M^{\prime}\right) \bmod (q, q)$. Let $\left(C, C^{\prime}\right) "=(p, p) .\left(\left(g, g^{\prime}\right) s+e\left(f, f^{\prime}\right)\right)+\left(f, f^{\prime}\right)\left(M, M^{\prime}\right)$ computed in $R$ (not modulo $\left.(q, q)\right)$. If $\left.\|\left(C, C^{\prime}\right)\right)^{\prime \prime} \|_{\infty}<q / 2$ then we have $\left(C, C^{\prime}\right)^{\prime}=\left(C, C^{\prime}\right)^{\prime \prime}$ in $\quad$ and hence, since $\left(f, f^{\prime}\right) \equiv(1,1) \bmod (p, p),\left(C, C^{\prime}\right)^{\prime} \bmod (p, p)=\left(C, C^{\prime}\right){ }^{\prime} \bmod (p, p)=\left(M, M^{\prime}\right) \bmod (p, p)$, i.e., the decryption algorithm succeeds. It thus suffices to give an upper bound on the probability that $\left\|\left(C, C^{\prime}\right) "^{\prime}\right\|_{\infty}>q / 2$. From Lemma 2, we know that with probability $\geq 1-2^{-n+3}$ both $\left(f, f^{\prime}\right)$ and $\left(g, g^{\prime}\right)$ have Euclidean norms $\leq 2 n\|(p, p)\| \sigma($ resp. $4 \sqrt{n}\|(p, p)\| \sigma$ if $\operatorname{deg}(p, p) \leq(1,1))$ this implies that $\left\|(p, p)\left(f, f^{\prime}\right)\right\|,\left\|(p, p)\left(g, g^{\prime}\right)\right\| \leq 2 n^{1.5}\|(p, p)\|^{2} \sigma\left(r e s p .8 \sqrt{n}\|(p, p)\|^{2} \sigma\right)$, with probability $\geq 1-2^{-n+3}$. From Lemma 6 in [14], both $(p, p)\left(f, f^{\prime}\right) e$ and $(p, p)\left(g, g^{\prime}\right) s$ have infinity norms $\leq 2 \alpha q n^{1.5} \omega(\log n)$. \|(p,p)$\|^{2} \sigma \quad$ (resp. $8 \alpha q \sqrt{n} \omega(\log n) \cdot\|(p, p)\|^{2} \sigma \quad$ with $\quad$ probability $\quad 1-n^{-\omega(1)} \quad$ Independently: $\left\|\left(f, f^{\prime}\right)\left(M, M^{\prime}\right)\right\|_{\infty} \leq\left\|\left(f, f^{\prime}\right)\left(M, M^{\prime}\right)\right\| \leq \sqrt{n}\left\|\left(f, f^{\prime}\right)\right\| \cdot\left\|\left(M, M^{\prime}\right)\right\| \leq 2 .\left(\operatorname{deg}(p, p)+1 . n^{2}\|(p, p)\|^{2} \sigma\right.$
(resp.
$\left.8 n\|(p, p)\|^{2} \sigma\right)$. Since $\alpha q \geq \sqrt{n}$, we conclude that $\left\|\left(C, C^{\prime}\right)\right\|^{\|}\left\|_{\infty} \leq(6+2 \operatorname{deg}(p, p)) \cdot \alpha q n^{1.5} \omega(\log n) \cdot\right\|(p, p) \|^{2} \sigma$ (resp. $24 \alpha q n^{0.5} \omega(\log n) \cdot\|(p, p)\|^{2} \sigma$ ), with probability $1-n^{-\omega(1)}$, component-wise.

## B. Security

The security of the ILTRU follows by an elementary reduction from the decisional $R-L W E_{H N F+}^{\times}$, exploiting the uniformity of the public key in $R_{q}^{\times}$(Theorem 3 in [14]), and the invertibility of $(p, p)$ in $R_{q}$.

Lemma 4 [Adapted from 14]. Suppose $n+1$ is a prime such that $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ splits into $n$ linear factors modulo prime $q=\omega(1)$. Let $\varepsilon, \delta>0, p \in R_{q}^{\times}$and $\sigma \geq 2 n \sqrt{\ln (8 n q)} \cdot q^{1 / 2+\varepsilon}$. If there exists an IND-CPA attack against the ILTRU that runs in time $T$ and has success probability $1 / 2+\delta$ component-wise, then there exists an algorithm solving $R-L W E_{H N F+}^{\times}$with parameters $q$ and $\alpha$ that runs in time $T^{\prime}=T+O(n)$ and has success probability $\delta^{\prime}=\delta-q^{-\Omega(n)}$ component-wise.
Proof. Let $A$ denote the given IND-CPA attack algorithm. We construct an algorithm $B$ against $R-L W E_{H N F+}^{\times}$that runs as follows, given oracle $O$ that samples from either $U\left(R_{q}^{\times} \times R_{q}\right)$ or $A_{s, \psi}^{\times}$for some previously chosen $s \leftarrow \psi$ and $\psi \leftarrow \bar{\Upsilon}_{\alpha}$.Algorithm $B$ first calls $O$ to get a sample $\left(\left(h, h^{\prime}\right)^{\prime},\left(C, C^{\prime}\right)^{\prime}\right)$ from $R_{q}^{\times} \times R_{q}$. Then, algorithm $B$ runs $A$ with public key $\left(h, h^{\prime}\right)=(p, p) .\left(h, h^{\prime}\right)^{\prime} \in R_{q}$. When $A$ outputs challenge messages $\left(M_{0}, M_{0}^{\prime}\right),\left(M_{1}, M_{1}^{\prime}\right) \in P$, algorithm $B$ picks $b \leftarrow U(\{0,1\})$, computes the challenge ciphertext $\left(C, C^{\prime}\right)=(p, p) .\left(C, C^{\prime}\right)^{\prime}+\left(M_{b}, M_{b}^{\prime}\right) \in R_{q}$, and returns $\left(C, C^{\prime}\right)$ to $A$. Eventually, when $A$ outputs its guess $b^{\prime}$ for $b$, algorithm $B$ outputs 1 if $b^{\prime}=b$ and 0 otherwise. The $\left(h, h^{\prime}\right)^{\prime}$ used by $B$ is uniformly random in $R_{q}^{\times}$and therefore so is the public key $\left(h, h^{\prime}\right)$ given to $A$, thanks to the invertibility of ( $p, p$ ) modulo $(q, q)$. Thus, by Theorem 3 in [14], the public key given to $A$ is within statistical distance $q^{-\Omega(n)}$ of the public key distribution in the genuine attack. Moreover, since $\left(C, C^{\prime}\right)^{\prime}=\left(h, h^{\prime}\right) . s+e$ with $s, e \leftarrow \psi$, the ciphertext $\left(C, C^{\prime}\right)$ given to $A$ has the right distribution as in the IND-CPA attack. Overall, if $O$ outputs samples from $A_{s, \psi}^{\times}$then $A$ succeeds and $B$ returns 1 with probability $\geq 1 / 2+\delta-q^{-\Omega(n)}$. Now, if $O$ outputs samples from $U\left(R_{q}^{\times} \times R_{q}\right)$, then, since $p \in R_{q}^{\times}$, the value of $(p, p)\left(C, C^{\prime}\right)^{\prime}$ and hence $\left(C, C^{\prime}\right)$, is uniformly random in $R_{q}$ and independent of $b$. It follows that $B$ outputs 1 with probability $1 / 2$, component-wise. The claimed advantage of $B$ follows.

By combining lemmata 3 and 4 (with theorem 1 in [14]) we obtain main result.
Theorem 2. Suppose $n+1$ is a prime such that $\Phi=x^{n}+x^{n-1}+\ldots+x+1$ splits into $n$ linear factors modulo prime $q=\operatorname{Poly}(n)$ such that $q^{1 / 2-\varepsilon}=\omega\left(n^{35} \log ^{2} n \operatorname{deg}(p, p)\|(p, p)\|^{2}\right)\left(\right.$ resp. $\left.q^{1 / 2-\varepsilon}=\omega\left(n^{4} \log ^{1.5} n \operatorname{deg}(p, p)\|(p, p)\|^{2}\right)\right)$, for arbitrary $\varepsilon \in(0,1 / 2)$ and $p \in R_{q}^{\times}$. Let $\sigma=2 n \sqrt{\ln (8 n q)} \cdot q^{1 / 2+\varepsilon}$ and $\alpha^{-1}=\omega\left(n^{1.5} \log n \operatorname{deg}(p, p)\|(p, p)\|^{2} \sigma\right)$. If there exists an IND-CPA attack against the $\operatorname{ILTRU}(n, q, p, \sigma, \alpha)$ which runs in time $T=P o l y(n)$ and has success probability $1 / 2+1 / \operatorname{Poly}(n)$ (resp. time $T=2^{\text {o(n) }}$ and success probability $1 / 2+2^{-o(n)}$ ) for each component, then there exists a Poly(n)-time (resp. $2^{o(n)}$-time) quantum algorithm for $\gamma$-Ideal-SVP with $\gamma=O\left(n^{4} \log ^{25} n \operatorname{deg}(p, p)\|(p, p)\|^{2} q^{1 / 2+e}(\right.$ resp. $\gamma=O\left(n^{5} \log ^{1.5} n \operatorname{deg}(p, p)\|(p, p)\|^{2} q^{12+\varepsilon}\right)$ Moreover, the decryption algorithm succeeds with probability $1-n^{-\omega(1)}$ over the choice of the encryption randomness for each element in pair-wise system.

## VI. Conclusion

In this paper, we provided an NTRU-Like cryptosystem (ILTRU Cryptosystem) that uses the properties of the ETRU cryptosystem and its structured lattice to achieve high efficiency by providing a provable security (CPA-secure) based on Ideal Lattices and a variant of R-LWE problem. Also we showed that each polynomial in
$R=\mathbb{Z}\left[\zeta_{3}\right][x] /<x^{n}+x^{n-1}+\ldots+x+1>$ has its coefficients of the form $\left(a_{i}, b_{i} \zeta_{3}\right)$ where $a_{i}, b_{i} \in \mathbb{Z}$, so we made both lemmata and theorems for $a_{i}{ }^{\prime} s$ and $b_{i}{ }^{\prime} s$ separately, that is we reflected $\mathbb{C} \cong \mathbb{R}^{2}$ hence we could enhance dimension of lattice without increasing $n$.

## REFERENCES

[1] W. Diffie and M.E. Hellman, "New directions in cryptography," In IEEE Trans. On Information Theory, vol. 22, pp.644-654, 1976.
[2] J. Hoffstein, J. Pipher, J.H. Silverman, "NTRU: a new high speed public key cryptosystem," Preprint; presented at the rump session of Crypto 1996.
[3] D. Coppersmith, A. Shamir, "Lattice attacks on NTRU," In Fumy, W. (ed.) EUROCRYPT, LNCS, vol. 1233, pp. 52-61. Springer, Heidelberg 1997.
[4] J. Hoffstein, J. Pipher, J.H. Silverman, "NTRU: A ring-based public key cryptosystem," In Buhler, J.P. (ed.) ANTS, LNCS, vol. 1423, pp. 267-288. Springer, Heidelberg 1998.
[5] IEEE P1363. Standard specifications for public-key cryptography, http://grouper.ieee.org/groups/1363/
[6] R.A. Perlner, D.A. Cooper, "Quantum resistant public key cryptography: a survey," In Proc. of IDtrust, ACM, New York, 2009 , pp. 85-93.
[7] K. Jarvis, and M. Nevins, "ETRU: NTRU over the Eisenstein Integers," Designs, Codes and Cryptography, DOI: 10. 1007/s10623-013-9850-3, Springer, 2013.
[8] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," In Proceedings of STOC, ACM, 1997, pp. 284-293.
[9] V. Lyubashevsky and D. Micciancio, "On bounded distance decoding, unique shortest vectors, and the minimum distance problem," In Proceedings of Crypto, vol. 5677 of LNCS, Springer, 2009, pp. 450-461.
[10] D. Micciancio, "Generalized compact knapsacks, cyclic lattices, and efficient oneway functions," Computational Complexity, vol. 16, no. 4, pp. 365-411, 2007.
[11] V. Lyubashevsky and D. Micciancio, "Generalized compact knapsacks are collision resistant," In Proceedings of ICALP, vol. 4052 of LNCS, Springer, 2006, pp. 144-155.
[12] C. Peikert and A. Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices," In Proceedings of TCC, 2006, pp. 145-166.
[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Journal of ACM, vol. 56, no. 6, 2009.
[14] D. Stehle, R. Steinfeld, "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices," In Eurocrypt, LNCS 6632, 2011, pp. 2747.
[15] M., Nevins, C. Karimianpour, A. Miri, "NTRU over rings beyond Z," Des. Codes Cryptogr., vol. 56, no. 1, pp. 65-78, 2010.
[16] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattices and learning with errors over rings," In Gilbert, H. (ed.) EUROCRYPT, LNCS, vol. 6110, Springer, Heidelberg 2010, pp. 1-23.
[17] C. Gentry, "Fully homomorphic encryption using ideal lattices," In Proc. of STOC, ACM, New York 2009, pp. 169-178.
[18] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattices and learning with errors over rings," Draft version, dated 01/02/2011.

