The ISC Int'l Journal of Information Security

July 2015, Volume 7, Number 2 (pp. 115–126)

http://www.isecure-journal.org

EEH: A GGH-Like Public Key Cryptosystem Over The Eisenstein Integers Using Polynomial Representations

Reza Ebrahimi Atani [1,3,*], Shahabaddin Ebrahimi Atani [2], and Amir Hassani Karbasi [2,3]

[1] *Department of Computer Engineering, University of Guilan, Rasht, Iran.*
[2] *Department of Mathematics, University of Guilan, Rasht, Iran.*
[3] *School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: 18 August 2014
First Revised: 2 May 2015
Second Revised: 29 August 2015
Third Revised: 17 October 2015
Accepted: 21 October 2015
Published Online: 29 October 2015

Keywords:
Lattice-based Cryptography, Public-key Cryptosystem, GGH, Dedekind Domain, Polynomial Representation.

ABSTRACT

GGH class of public-key cryptosystems relies on computational problems based on the closest vector problem (CVP) in lattices for their security. The subject of lattice based cryptography is very active and there have recently been new ideas that revolutionised the field. We present EEH, a GGH-Like public key cryptosystem based on the Eisenstein integers $\mathbb{Z}[\zeta_3]$ where ζ_3 is a primitive cube root of unity. EEH applies representations of polynomials to the GGH encryption scheme and we discuss its key size and parameters selection. We also provide theoretical and experimental data to compare the security and efficiency of EEH to GGH with comparable parameter sets and show that EEH is an improvement over GGH in terms of security and efficiency.

1 Introduction

Lattice-based cryptographic structures are known with their very strong security proofs based on worst-case hardness and relatively efficient implementations for post-quantum cryptography which have considerable active research area, as well as suitable simplicity and great security against quantum computers. We can roughly categorize lattice-based cryptography into two groups:

- Theoretical work for providing a one way function.
- Applied work for using the properties to solve more complex cryptographic affairs.

The theoretical researches aimed at bringing lattice-based cryptography closer to applications. We can refer to [1, 2] for recent developments in this area. In addition, for readers interested in practice, we provide some references to related papers which organized by category:

- Public key encryption [3–5].
- Digital signatures [6, 7].
- Group and ring signatures [8].
- Identity based cryptography [9].
- Homomorphic encryption [10–13].
- Zero-knowledge proofs and identification protocols [14, 15].

Also, for improving the security of lattice-based cryptosystems some variants have been presented using polynomial rings with coefficients in rings other than $\mathbb{Z}$, such as $GF(2^k)[x]$ [16], the non-commutative ring of $k \times k$ matrices of polynomials in $\frac{\mathbb{Z}[x]}{<x^N-1>}$ [17], the non-commutative matrix ring $\mathbf{M} = \frac{M_k\mathbb{Z}[x]}{<X^n-I_{k\times k}>}$ with $k \times k$ matrices of polynomials in $R = \frac{\mathbb{Z}[x]}{<X^n-1>}$ [18], Dedekind domains including $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_5]$ [19–21], QTRU, based on Quaternion algebra [22] and authors' lattice-based schemes [23, 39].

* Corresponding author.
Email addresses: rebrahimi@guilan.ac.ir (R. Ebrahimi Atani), ebrahimi@guilan.ac.ir (S. Ebrahimi Atani), karbasi@phd.guilan.ac.ir (A. Hassani Karbasi)
ISSN: 2008-2045

Goldreich, Goldwasser and Halevi proposed an efficient way to build a cryptosystem in 1997 that uses lattice theory and McEliece cryptosystem based on Bounded Distance Decoding [25], called GGH cryptosystem [24]. The security of the GGH is based on the difficulty of the closest vector problem (CVP) in lattices. For the GGH, they published 5 numerical challenges for the security parameter $N = 200$, 250, 300, 350, 400, of which the public key sizes range from 330KBytes to 2MBytes. A fourth attack presented by Nguyen and broke all the GGH challenge except $N = 400$ [26], that is, the GGH cryptosystem is insecure unless over a high dimensional lattice that makes it inefficient with very large key size.

The GGH describes a clear scheme of using lattices in cryptography and uses $N \times N$ matrices as a public key and a private key, thus every lattice-based public key cryptosystem except for NTRUEncrypt [38] has an impractical key size. Some major improvements of the speed and the security of the GGH suggested in [27] by Micciancio. In this scheme, the public key is of a Hermite Normal Form (HNF), whose key sizes are much smaller than those of the GGH cryptosystem. However, implementations of this algorithm are extremely slow, again limiting practicality.

The GGH cryptosystem has some advantages and has a natural signature scheme. In this system, the computational complexity for encryption, decryption, signing, and verifying are all quadratic in the natural security parameter and it is asymptotically more efficient than the RSA and ElGamal encryption schemes. The GGH has public key of size $O(N^2)$ and computation time of $O(N^2)$, compared to public key of size $O(N)$ and computation time of $O(N^3)$ for the RSA and ElGamal systems. Also, Ajtai and Dwork [28] proposed a public key encryption scheme that is less efficient than the GGH whose security is reducible to a variant of shortest vector problem (SVP). The Ajtai-Dwork scheme has key of size $O(N^4)$ and encryption time $O(N^4)$. Currently, ETRU cryptosystem [31] is the most efficient cryptosystem among lattice-based public key schemes.

In this paper, our main technical contribution is the modification of the GGH key generation algorithm based on polynomial representations that each coefficient is an Eisenstein integer and then analysis of the efficiency and the security of the modified GGH cryptosystem. To the best of our knowledge, it is the first time that the GGH scheme is modified and analyzed based on a firm theoretical grounding and a moderate practical implementing for the security and the efficiency of the GGH-like schemes, in the ring of quotient of the NTRU-like schemes. Therefore, we present a public key cryptosystem applying ETRU polynomial representations to the GGH scheme whose key size is practical, called EEH cryptosystem. In view of security, the EEH cryptosystem has an advantage: Attackers can find out only the message by known lattice attacks, i.e. the secret key of the EEH cannot be obtained by solving the shortest vector problem (SVP) and closest vector problem (CVP).

The rest of this paper is structured as follows: In Section 2, we shortly review the GGH system and explain the security related to the choice of secret parameters. In Section 3, we study the Eisenstein integers, the ETRU and representation of polynomials by $2N \times 2N$ matrices and their direct applications to the GGH system. In Section 4, we suggest a GGH-Like public key cryptosystem (EEH) using the representation in Section 3. In Section 5, we study parameter selection, security analysis and key sizes. Also we show that key size of EEH is comparable with GGH and ETRU cryptosystems. Finally, the paper concludes in Section 6.

2 The GGH Cryptosystem

In this chapter, we describe the GGH cryptosystem and its trapdoor function [24]. The useful notion of the $orthogonality - defect$ of a lattice-based was first defined by Schnorr [29]. This is a requirement for the GGH trapdoor function.

Definition 1. Let V and V' denote two bases of the N-dimensional lattice $\mathcal{L}$. V is said to be *smaller* than V' if:

$$\prod_i ||v_i|| \leq \prod_i ||v_i'|| \tag{1}$$

where $||v_i||$ and $||v_i'||$ are the $l_2 - norm$ of the i-th column in V and V', respectively.

Definition 2. If V is a real non-singular $N \times N$ matrix, then the $orthogonality - defect$ of V is defined as:

$$orth - defect(V) := \frac{\prod_i ||v_i||}{|det(V)|} \tag{2}$$

So $orth - defect(V) = 1$ if and only if V is an orthogonal matrix.

Definition 3. Suppose V is a real non-singular $N \times N$ matrix. The $dual - orthogonality - defect$ of V is defined as:

$$orth - defect^*(V) := \frac{\prod_i ||v_i^*||}{|det(V^{-1})|} = |det(V)| \prod_i ||v_i^*|| \tag{3}$$

where v_i^* is the i-th row in V^{-1}.

The mathematical problem is used in the GGH, is called the closest vector problem (CVP). Both CVP and SVP are profound problems and by growing the dimension N of the lattice, they become computationally difficult and also are known to be NP-hard.

On the other hand, different research areas of pure and applied mathematics are emerged for approximate solutions to CVP and SVP. The GGH public key encryption scheme can be summarized as follows:

2.1 Setup

The public key $\mathbf{B}$ is a "bad basis" of a lattice $\mathcal{L}$ with a high dual-orthogonality-defect that is an $N\times N$ matrix $\mathbf{B} = \mathbf{A}\mathbf{T}^{-1}$ for some $\mathbf{T} \in GL(N,\mathbb{Z})$, where $\mathbf{T}$ is unimodular matrix and $\mathbf{A}$ is the private key or "good basis" that is an $N\times N$ matrix with a low dual-orthogonality-defect. $\mathbf{A}$ can be generated by $A' + kI$, where $A'=(A'_{ij})$ satisfies that $|A'_{ij}| \leq l$ and $k \approx \sqrt{N}\, l$ for some constant l. $\mathbf{A}$ and $\mathbf{B}$ generate the same lattice, i.e. $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$.

Definition 4. A matrix $\mathbf{T} \in \mathbb{Z}^{N\times N}$ is called *unimodular* if $det\ \mathbf{T} = \pm 1$.

2.2 Encryption

Let $m \in \mathbb{Z}^N$ be a plaintext massage vector. For an error vector $e = (\delta_1\sigma, \delta_2\sigma, \ldots, \delta_N\sigma)$, the ciphertext c by encrypting m is computed as follows:

$$c = \mathbf{B}m + e \tag{4}$$

where δ_i= -1 or 1 and σ is a small constant.

Solving the CVP for the lattice $\mathcal{L}$ is equivalent to deciphering m from equation (Equation 4). However, m can be deciphered easily, for a given "good basis" $\mathbf{A}$ for $\mathcal{L}$, so $\mathbf{A}$ is the trapdoor information.

2.3 Decryption

Using the "good basis" $\mathbf{A}$, one can solve the closest vector problem to find $\mathbf{B}m$ by computing the lattice vector closest to c in decryption process. The plaintext is obtained as follows:

$$\begin{aligned} m' &= \mathbf{T}\lceil \mathbf{A}^{-1}c \rfloor \\ &= \mathbf{T}\lceil \mathbf{A}^{-1}(\mathbf{A}\mathbf{T}^{-1}m + e) \rfloor \\ &= \mathbf{T}\lceil \mathbf{T}^{-1}m + \mathbf{A}^{-1}e) \rfloor \\ &= m + \mathbf{T}\lceil \mathbf{A}^{-1}e \rfloor \end{aligned} \tag{5}$$

note that $\lceil m \rfloor$ denotes the vector in $\mathbb{Z}^N$ which is obtained by rounding each entry in m to the nearest integer.

If $\mathbf{A}$ is a "good" basis, then decryption works. We denote the maximum of L_∞-norm of the rows in $\mathbf{A}^{-1}$ by $\frac{\gamma}{\sqrt{N}}$. If σ=$[(\gamma\sqrt{8ln\frac{2N}{\epsilon}})^{-1}]$ for some small real number ϵ >0, then the probability of decryption error is bounded by ϵ, where $[y]$=$max\{x|x\ is\ an\ integer, x \leq y\}$. The ciphertext in GGH encryption is considerably larger than the plaintext message. A precise analysis of this depends on the sizes of entries in $\mathbf{A}$.

2.4 The Gap of Lattice

In the GGH, $\mathcal{L}_{\mathbf{A}}$ and $\mathcal{L}_{\mathbf{B}}$ are the same lattices and this lattice generated by columns of $\mathbf{A}$ and $\mathbf{B}$, respectively, such that the rows of both matrices are linearly independent, hence $span(\mathbf{A}) = span(\mathbf{B})$. Suppose $\mathbf{T}$ is not unimodular and $\mathbf{B} = \mathbf{A}\mathbf{T}^{-1}$, these two matrices generate different lattices. In fact, $\mathcal{L}_{\mathbf{B}}$ is a *sublattice* of $\mathcal{L}_{\mathbf{A}}$, i.e. $\mathcal{L}_{\mathbf{B}} \subset \mathcal{L}_{\mathbf{A}}$. Even if $\mathcal{L}_{\mathbf{B}}$ is a sublattice of $\mathcal{L}_{\mathbf{A}}$, the decryption works, but in this case, its security can be weakened [30]. Therefore we should use $\mathbf{A}$ and $\mathbf{B}$ such that $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$ in view of security.

Definition 5. The gap of a lattice $\mathcal{L}$, say $G_{\mathcal{L}}$, is the ratio between the length of second successive minimum vector and the length of a shortest nonzero vector in $\mathcal{L}$.

Notice that it is easy to find the shortest vector in a lattice when the lattice gap is large [26]. As a result, in this paper, we will propose a "good" basis $\mathbf{A}$ and a "bad" basis $\mathbf{B}$ such that $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$ with the least gap based on dedekind domain $\mathbb{Z}[\zeta_3]$ where ζ_3=$\frac{1}{2}(-1+\sqrt{3}i)$.

3 The Eisenstein Integers, The ETRU Cryptosystem and Their Applications to Polynomial Representations

In this section we describe a representation of a polynomial quotient ring.

3.1 The Eisenstein Integers

We denote by ζ_3 a complex cube root of unity, that is ${\zeta_3}^3 = 1$ where $\zeta_3 = \frac{1}{2}(-1+\sqrt{3}i)$. Since ${\zeta_3}^3 - 1 = (\zeta_3 - 1)({\zeta_3}^2 + \zeta_3 + 1) = 0$, we have ${\zeta_3}^2 + \zeta_3 + 1 = 0$ and hence ${\zeta_3}^2 = -1 - \zeta_3$. The ring of *Eisenstein integers*, denoted $\mathbb{Z}[\zeta_3]$, 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 introduce $d(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 - ab$ which is the square of the usual analytic complex norm $|\alpha|$, so $d(\alpha)$ is a positive integer for $\alpha \neq 0$. For any complex numbers α, β we have that $|\alpha\beta| = |\alpha||\beta|$ hence it follows that $d(\alpha\beta) = d(\alpha)d(\beta)$.

The Eisenstein integers $\mathbb{Z}[\zeta_3]$ form a lattice in $\mathbb{C}$ generated by the basis $\mathbf{B} = \{1, \zeta_3\}$. We can show the two basis vectors 1 and ζ_3 by the vectors (1,0) and $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$ in $\mathbb{R}^2$ with 120 degrees and equal length, that is, $\mathbb{C} \cong \mathbb{R}^2$. This lattice is shown in [31] as Figure Figure 1. Also, for $q \in \mathbb{Z}[\zeta_3]$ the ideal $< q >$ is a lattice with basis $q\mathbf{B} = \{q, q\zeta_3\}$. The reduced elements

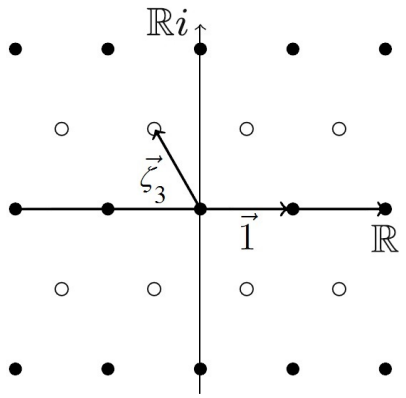


Figure 1. The *solid dots* show the rectangular sublattice L of $\mathbb{Z}[\zeta_3]$ in the complex plane, and the *open dots* show its nontrivial coset $\zeta_3 + L$ [31].

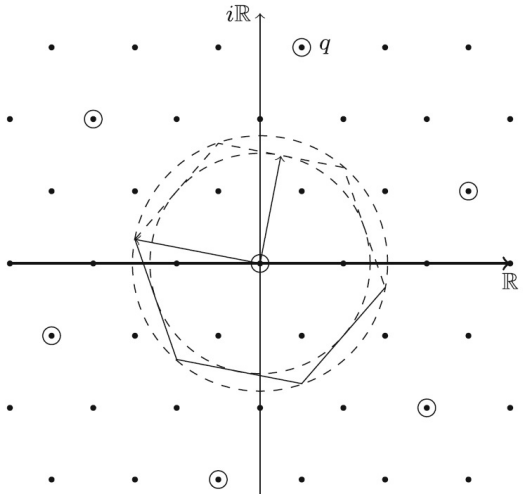


Figure 2. For $q = 2 + 3\zeta_3$, the *open dots* show the elements of the ideal $< q >$. The inscribed and circumscribed circles are of radius $|q|/2$ and $|q|/\sqrt{3}$, respectively. The hexagon shows V_q and all elements of $\mathbb{Z}[\zeta_3]$ contained in or on it, are elements of D_q [31].

modulo q is the set D_q which is defined to be those elements of $\mathbb{Z}[\zeta_3]$ contained in the Voronoi cell V_q of the origin of $< q >$. V_q is a certain regular hexagon inscribed by two circles of radius $(1/2)|q|$ and $(1/\sqrt{3})|q|$. This region is shown in [31] as Figure Figure 2.

Let β be an Eisenstein integer. We define the ideal $\mathcal{L}(\beta)$ by:

$$\begin{aligned}\mathcal{L}(\beta) &= \{\eta\beta | \eta \in \mathbb{Z}[\zeta_3]\} \\ &= \{(a + b\zeta_3)\beta | a, b \in \mathbb{Z}\} \\ &= \{a\beta + b\beta\zeta_3 | a, b \in \mathbb{Z}\}. \end{aligned} \quad (6)$$

Therefore $\mathcal{L}(\beta)$ is a lattice generated by the basis $\mathbf{B} = \{\beta, \beta\zeta_3\}$. Since multiplication by any $\beta \in \mathbb{C}$ preserves the angle between vectors, it is easy to verify that $\mathcal{L}(\beta)$ is also a hexagonal lattice. Note that we are able to develop a closest vector algorithm for the Eisenstein integers, that is, it is easy to solve the closest vector problem on a Eisenstein integers lattices. The following Theorem [31] gives a closest vector algorithm for $\mathcal{L}(\beta)$.

Theorem 1 (Division Algorithm)**.** *Let $\beta \in \mathbb{Z}[\zeta_3] \setminus \{0\}$ and $\alpha \in \mathbb{Z}[\zeta_3]$. Define $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ by:*

$$a_1 + b_1 i = \beta^{-1}\alpha \text{ and } a_2 + b_2 i = \beta^{-1}\alpha - \zeta_3.$$

For j=1,2, compute:

$$\rho'_j = (a_j - \lfloor a_j \rceil) + i(b_j - \sqrt{3}\lfloor \tfrac{b_j}{\sqrt{3}} \rceil).$$

Define $\rho_1, \rho_2, \eta_1, \eta_2 \in \mathbb{Z}[\zeta_3]$ by:

$$\rho_1 = \beta\rho'_1, \eta_1 = \lfloor a_1 \rceil + i\sqrt{3}\lfloor \tfrac{b_1}{\sqrt{3}} \rceil \text{ and}$$

$$\rho_2 = \beta\rho'_2, \eta_2 = \lfloor a_2 \rceil + i\sqrt{3}\lfloor \tfrac{b_2}{\sqrt{3}} \rceil + \zeta_3.$$

Then the following hold:

$$\alpha = \beta\eta_1 + \rho_1 = \beta\eta_2 + \rho_2,\ d(\rho_1), d(\rho_2) < d(\beta) \text{ and } Re(\eta_1) \neq Re(\eta_2),$$

where $Re(\eta)$ denotes the real part of η.

Define (ρ, η) by the following:

- *if $d(\rho_1) < d(\rho_2)$, set $(\rho, \eta) = (\rho_1, \eta_1)$;*
- *if $d(\rho_1) > d(\rho_2)$, set $(\rho, \eta) = (\rho_2, \eta_2)$;*
- *if $d(\rho_1) = d(\rho_2)$ and $Re(\eta_1) > Re(\eta_2)$ set $(\rho, \eta) = (\rho_1, \eta_1)$;*
- *if $d(\rho_1) = d(\rho_2)$ and $Re(\eta_1) < Re(\eta_2)$ set $(\rho, \eta) = (\rho_2, \eta_2)$,*

such that outputs ρ when applied to the pair (α, β) is a division algorithm.

Then the following hold:

(1) $\alpha = \beta\eta + \rho$ and $d(\rho) < d(\beta)$
(2) $\eta\beta$ is an element of $\mathcal{L}(\beta)$ closest to α
(3) ρ is a smallest representative of the congruence class modulo β
(4) the division algorithm outputs a unique representative of the congruence class, that is if $\alpha, \alpha' \in \mathbb{Z}[\zeta_3]$ satisfy $\alpha' \equiv \alpha \bmod \beta$ then the algorithm produces the same output when applied to (α, β) and (α', β).

According to [31] and Theorem 1, we deduce that the Eisenstein integers are an Euclidean domain. Hence, the following properties hold:

Proposition 1. *An Eisenstein integer $\psi \in \mathbb{Z}[\zeta_3]$ is a unit if and only if $d(\psi) = 1$.*

Proposition 2. *The units of $\mathbb{Z}[\zeta_3]$ are $\pm 1, \pm\zeta_3$ and $\pm\zeta_3^2$.*

Proposition 3. *If $\varphi \in \mathbb{Z}[\zeta_3]$ and $d(\varphi) = p$ where p is a rational prime, then φ is a prime in $\mathbb{Z}[\zeta_3]$.*

Proposition 4. *Suppose that φ is an Eisenstein integer. Then $d(\varphi)$=3 if and only if $\varphi = \psi(1 - \zeta_3)$ for some unit ψ.*

Propositions 3 and 4 and also [32] show that $1 - \zeta_3$ and its associates are Eisenstein primes. Notice in

the case for $\alpha = a + b\zeta_3$ where the $gcd(a, b)$=1 then the set of distinct congruence classes modulo α can be represented by the set $\{0, 1, \ldots, d(\alpha) - 1\}$. For example for $\alpha = 2 + 3\zeta_3$ we have $d(\alpha) = 7$ and hence the set $\{0, 1, 2, 3, 4, 5, 6\}$ is a set of distinct congruence classes modulo α.

For each Eisenstein integer $\alpha = a + b\zeta_3$ we define:

$$< \alpha >= \begin{bmatrix} a & b \\ -b & a - b \end{bmatrix} \tag{7}$$

Notice that for any Eisenstein integer β=c+dζ_3 we have:

$$\begin{bmatrix} c & d \end{bmatrix} \begin{bmatrix} a & b \\ -b & a - b \end{bmatrix} = \begin{bmatrix} ac - bd & bc + ad - bd \end{bmatrix} \tag{8}$$

which is the vector representation of the multiplication $\beta\alpha$.

For each $N \times N$matrix $\mathbf{B}$ with entries that are Eisenstein integers we will set $< \mathbf{B} >$ to be the $2N \times 2N$matrix with each entry b_{ij} replaced with the 2×2 matrix $< b_{ij} >$.

Every element of $R = \frac{\mathbb{Z}[\zeta_3][x]}{<t(x)>}$ has a unique representative of the form $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{N-1} x^{N-1}$ with the coefficients in $\mathbb{Z}[\zeta_3]$, where $t(x)$ is a polynomial of degree N, i.e. $c(x) = (a_0 + b_0\zeta_3) + (a_1 + b_1\zeta_3)x + \cdots + (a_{N-1} + b_{N-1}\zeta_3)x^{N-1}$. It is often convenient to identify a polynomial $c(x)$ with its vector of coefficients $(c_0, c_1, c_2, \ldots, c_{N-1}) = ([a_0, b_0], [a_1, b_1], \ldots, [a_{N-1}, b_{N-1}]) \in \mathbb{Z}^{2N}$.

3.2 The ETRU Cryptosystem

To define the ETRU [31], we identify $t(x) = x^N - 1$, a polynomial of degree N. So we choose an prime N and set $R = \frac{\mathbb{Z}[\zeta_3][x]}{<x^N - 1>}$, we also choose p and q in $\mathbb{Z}[\zeta_3]$ 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 $N' = 2N$.

3.2.1 Key Generation

Private key consists of two randomly chosen polynomials $f, g \in R = \frac{\mathbb{Z}[\zeta_3][x]}{<x^N - 1>}$. We define the inverses $F_q = f^{-1} \in R_q$ and $F_p = f^{-1} \in R_p$, where R_q and R_p are the reduced sets modulo q and p, respectively. Hence, public key is generated by $h = F_q \times g$. The public key h is a polynomial with N coefficients which are reduced modulo q. Each coefficient consists of two integers can be stored as binary strings of length $\lceil log_2(4.|q|/3) \rceil$, hence the size of the ETRU public key is $K = 2N\lceil log_2(4.|q|/3)$. An NTRU public key, corresponding to polynomials with $N' = 2N$ coefficients reduced modulo an integer q', has size $K' = N'\lceil log_2(q') \rceil$. Therefore to maintain the same key size as NTRU with $N' = 2N$ and $q' = 2^k$, we should choose $|q| \leqslant (3/4)q'$ so that $\lceil log_2(4.|q|/3) \rceil \leqslant \lceil log_2(q') \rceil$.

3.2.2 Encryption and Decryption

Each encryption requires the user to compute $e = \phi \times p.h + m \bmod q$, where m is a plaintext and ϕ is a ephemeral key. 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.

Each decryption requires the user to compute both $a = f \times e \bmod q$ and $m = F_p \times a \bmod p$. For decryption, we have $2N'^2 + 2N' \sim 8N^2 + 4N$ operations for NTRU and only $6N^2 + 29N$ operations for ETRU.

The speed of encrypting and decrypting 10,000 message in ETRU and NTRU for comparable parameter sets is shown in [31] as Figure 3. 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.

3.2.3 Decryption Failure and Security

In [31] is shown that in fact $|q| \sim (3/8)q'$ 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.

3.3 Polynomial Representation

We have the following representation of $R = \frac{\mathbb{Z}[\zeta_3][x]}{<t(x)>}$ into the set of $2N \times 2N$matrices with Eisenstein integer entries:

$$\rho : \frac{\mathbb{Z}[\zeta_3][x]}{< x^N - 1 >} \longrightarrow GL(2N, \mathbb{C})$$
$$g \longmapsto \rho(g), \rho(g)(h) = g(x)h(x). \tag{9}$$

Then:

$$\rho(g)(h) = (c_0 + d_0\zeta_3, \ldots, c_{N-1} + d_{N-1}\zeta_3) \in \mathbb{Z}[\zeta_3]^N \tag{10}$$

So general term can be represented as:

$$g(x)h(x) =$$
$$(c_0 + d_0\zeta_3) + \cdots + (c_{N-1} + d_{N-1}\zeta_3)x^{N-1} \in \frac{\mathbb{Z}[\zeta_3][x]}{< x^{N-1} >} \tag{11}$$

Depending on the choice of $t(x)$, we can find various representations [30]. If $t(x) = x^N - 1$, then we have a circulant $2N \times 2N$ matrix:

$$\rho(g) = \begin{bmatrix} a_0 + b_0\zeta_3 & a_{N-1} + b_{N-1}\zeta_3 & \dots & a_2 + b_2\zeta_3 & a_1 + b_1\zeta_3 \\ a_1 + b_1\zeta_3 & a_0 + b_0\zeta_3 & \dots & a_3 + b_3\zeta_3 & a_2 + b_2\zeta_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{N-1} + b_{N-1}\zeta_3 & a_{N-2} + b_{N-2}\zeta_3 & \dots & a_1 + b_1\zeta_3 & a_0 + b_0\zeta_3 \end{bmatrix} \tag{12}$$

Now, in Section 4 we can construct a "good basis" **A** and a "bad basis" **B** by this representation and apply them to the GGH scheme.

4 Proposed EEH Cryptosystem

Now we need to adapt the NTRU lattice for Eisenstein integers, that is, we introduce the ETRU lattice. Then we show that new lattice is an improvement to the GGH in terms of both lattice security and storage and comparable to the ETRU in terms of speed. In order to derive our proposed EEH cryptosystem from the vector representation of the ETRU lattice and the GGH encryption scheme, we proceed in several steps as follows:

(1) We replace the GGH lattice by $R = \frac{\mathbb{Z}[\zeta_3][x]}{<x^N-1>}$ and we exploit the fact that R is the ring of integers of a dedekind domain and its representation with Eisenstein integers.
(2) We sample the public key (bad basis) from the ETRU cyclic modular lattice (CML).
(3) We construct the private key (good basis) in two steps: At first, we use the NTRU key recovery problem based on the ETRU lattice for a "half-good basis" of short vectors, then we apply a construction used in the NTRU digital signature based on the ETRU lattice to find the other "half-good basis".
(4) We modify encryption and decryption process of the GGH based on our modified "bad" and "good" bases. This allows us to derive the ETRU security and the ETRU key sizes which are much smaller than the key sizes of the GGH scheme and its variants.

Implementation of the new trapdoor function and these modifications are similar to the ETRU cryptosystem implementation. In [31], Jarvis and Nevins proposed an implementation of the ETRU primitives, hence our presented EEH scheme provides practicality.

4.1 Parameter Selection

We would like to be able to easily calculate the inverse of $f(x) \in \frac{\mathbb{Z}[\zeta_3][x]}{<x^N-1>}$ modulo p and q thus we want to choose p and q to be prime or a prime power. For example we choose p to be $2 + 3\zeta_3$ because $d(p) = 7$ and the distinct equivalence classes modulo p based on the fundamental domain of $\mathcal{L}(p)$ are $\{0, \pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. We will choose q to be prime or a power of $1 - \zeta_3$ the smallest prime. Thus, the inverses of polynomials modulo p and q can be found using the extended Euclidean algorithm. In Table 1, all setup parameters of NTRU, ETRU, GGH, and EEH are summarized.

Let $\mathcal{L}_f$ and $\mathcal{L}_g$ be subsets of $\frac{\mathbb{Z}[\zeta_3][x]}{<x^N-1>}$. We choose $f(x) \in \mathcal{L}_f$ and $g(x) \in \mathcal{L}_g$ to be polynomials with coefficients from $\mathcal{L}(p)$ are $\{0, \pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. The polynomial $f(x)$ has d_f+1 1's and d_f of each of the other units so that $x-1$ is not a factor of $f(x)$ and the polynomial $g(x)$ has d_g of each of the units $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$ and the rest of its coefficients zero. For security reasons let N be a prime number and $d_f = d_g = d = \lfloor \frac{N}{3} \rfloor$.

4.2 Key Generation

To generate the public key one can randomly chooses $f(x) \in \mathcal{L}_f$ and $g(x) \in \mathcal{L}_g$. The polynomial $f(x)$ should be invertible modulo q. We denote this inverse by notation $F_q(x) \in \frac{\mathbb{Z}/q\mathbb{Z}[\zeta_3][x]}{< x^N - 1 >}$, that satisfying the following properties:

$$F_q(x) \times f(x) \equiv 1 \; mod \; q \tag{13}$$

Next compute:

$$h(x) \equiv F_q(x) \times g(x) \; mod \; q \tag{14}$$

Notice that modular equation (Equation 14) is the same construction used in the ETRU encryption scheme and is equivalent to the following hidden condition:

$$f(x) \times h(x) \equiv g(x) \; mod \; q \tag{15}$$

The condition (Equation 15) is a hard mathematical problem which is known as the NTRU key recovery problem. In [33] is discussed that solving the NTRU key recovery problem is (almost certainly) equivalent to solving SVP in lattices.

Hence, the following public key or the "bad" basis **B** for the lattice $\mathcal{L}_{\mathbf{B}}$ is generated by the representation ρ and $4N \times 4N$ matrix:

$$\mathbf{B} = \begin{bmatrix} \lambda < I > & < \rho(h(x)) > \\ 0 & < qI > \end{bmatrix} \tag{16}$$

where $\lambda \in \mathbb{R}$ is balancing Constant. Notice that **B** is composed of four $2N \times 2N$ blocks. Also **B** is similar to the ETRU lattice.

In order to generate the private key or the "good" basis **A** for the lattice $\mathcal{L}_{\mathbf{A}}$ such that $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$ with

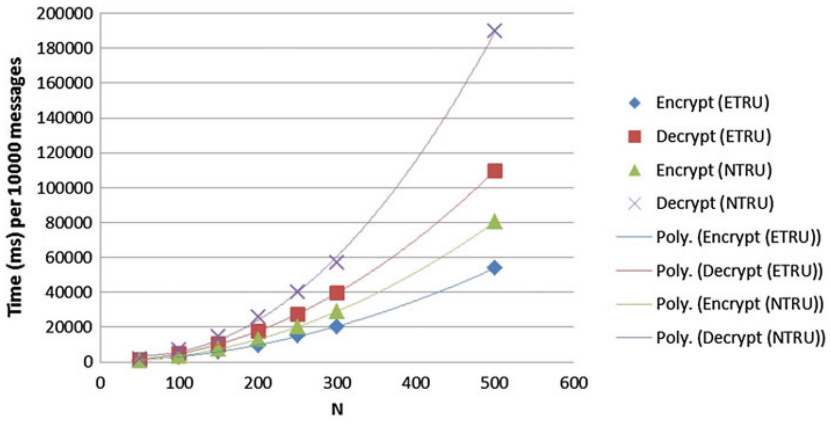


Figure 3. Comparison of encryption and decryption time between ETRU and NTRU for 10,000 random messages. The curves are the best-fitting quadratic polynomials to the data [31].

Table 1. Setup parameters.

	NTRU[38]	**ETRU**[31]	**GGH**[24]	**EEH**
Lattice Dimension N	Positive integer	Prime	Positive integer	Prime
Modulo p	Positive integer co-prime with q as $p = 3$ $(q >> p)$	Prime or prime power as $p = 2 + 3\zeta_3$ or $p = 2 + \zeta_3$ $(\|q\| >> \|p\|)$	—	Prime or prime power as $p = 2 + 3\zeta_3$ or $p = 2 + \zeta_3$
Modulo q	Positive integer co-prime with p as $q = 2048$ $(q >> p)$	Prime or prime power as $q = 81\zeta_3$ $= (1 - \zeta_3)^8$ $(\|q\| >> \|p\|)$	—	Prime or prime power as $q = 81\zeta_3$
Perturbation e	—	—	$e \in \{-1/2, 1/2\}^N$	$(e_1, e_2) \in \{-1/2, 1/2\}^{2N}$

the least gap and without decryption failure, we use the following Proposition [33]:

Proposition 5. *Assuming that* $f(x) \times h(x) \equiv g(x) \bmod q$, *let* $u(x) \in \frac{\mathbb{Z}[\zeta_3][x]}{<x^{N-1}>}$ *be the polynomial satisfying:*

$$f(x) \times h(x) = g(x) + qu(x)$$

Then

$$(f(x), -u(x))\mathbf{B} = (f(x), g(x))$$

so the vector $(f(x), g(x))$ *is in the lattice* $\mathcal{L}_\mathbf{B}$.

In other words, for every vector $(f(x), u(x)) \in \mathbb{Z}^{4N}$ with $f(x), u(x) \in \mathbb{Z}^{2N}$ we have:

$$\begin{aligned}(f(x), u(x))\mathbf{B} &= (\lambda f(x), f(x) < \rho(h(x)) > + < qI > u(x)) \\ &= (\lambda f(x), g(x)) \end{aligned} \quad (17)$$

The solution to proposition 5 is not unique, because if $(f(x), g(x))$ is one solution, then $(x^k \times f(x), x^k \times g(x))$ is also a solution for every $0 \leq k < N$. The polynomial $x^k \times f(x)$ is called a *rotation* of $f(x)$ because the coefficients have been cyclically rotated k positions. In fact, the lattice $\mathcal{L}_\mathbf{B}$ is a $4N$-dimensional lattice containing short vectors $(\lambda f(x), g(x))$ and each of the cyclical rotations $(\lambda x^k \times f(x), x^k \times g(x))$ for all $0 \leq k < N$ [33].

Therefore, we can construct a "half-good" basis of short vectors by the representation ρ for all $0 \leq k < N$ as follows:

$$\mathbf{A} = \begin{bmatrix} \lambda x^k \times f(x) & x^k \times g(x) \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \lambda < \rho(f(x)) > & < \rho(g(x)) > \\ 0 & 0 \end{bmatrix} \quad (18)$$

However, in order to use the private key for the same lattice, we need a full basis of short vectors. Indeed, the Gaussian heuristic predicts that the other $2N$ basis vectors exist and there is a reasonably efficient algorithm to find a complementary "half-good" basis $(F(x), G(x))$. More precisely, it is possible to find the other short vector polynomials $F(x)$ and $G(x)$ satisfying:

$$f(x) \times G(x) - g(x) \times F(x) = q \quad (19)$$

Notice that equation (Equation 19) is the same construction used in the NTRU digital signature scheme [34]. Thus the "good" basis $\mathbf{A}$ with short vectors in lattice is computed by the representation ρ for all $0 \leq k < N$ as follows:

$$\mathbf{A} = \begin{bmatrix} \lambda x^k \times f(x) & x^k \times g(x) \\ \lambda x^k \times F(x) & x^k \times G(x) \end{bmatrix} = \begin{bmatrix} \lambda < \rho(f(x)) > & < \rho(g(x)) > \\ \lambda < \rho(F(x)) > & < \rho(G(x)) > \end{bmatrix} \quad (20)$$

As a result, we have the following $4N \times 4N$ matrices as private key and public key for all $0 \leq k < N$ respectively, such that $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$:

$$\mathbf{A} = \text{"}Good\ Basis\text{"} = \begin{bmatrix} \lambda < \rho(f(x)) > & < \rho(g(x)) > \\ \lambda < \rho(F(x)) > & < \rho(G(x)) > \end{bmatrix} \quad (21)$$

$$\mathbf{B} = \text{"}Bad\ Basis\text{"} = \begin{bmatrix} \lambda < I > & < \rho(h(x)) > \\ 0 & < qI > \end{bmatrix} \quad (22)$$

4.3 Encryption

A message is $M = (m_1, m_2) \in (\frac{\mathbb{Z}[\zeta_3][x]}{< x^N - 1 >})$. Then the ciphertext is:

$$c = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \mathbf{B} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \in (\frac{\mathbb{C}[x]}{< x^{N-1} >}) \quad (23)$$

for an error vector $e = (e_1, e_2)$, where $e_i \in \{-\sigma, \sigma\}^N$ and σ will be set to be $\frac{1}{2}$.

4.4 Decryption

As we already mentioned because $\mathbf{A}$ is a "good" basis, decryption works and our proposed EEH decryption is the same as the GGH cryptosystem decryption.

4.5 Efficiency

We want to be able to compare the speed on the EEH to that of GGH. Recall that the encryption and decryption of GGH are both of order $O(N^2)$. For any two Eisenstein integers $\alpha = a + b\zeta_3$ and $\beta = c + d\zeta_3$ we have $\alpha\beta = (ac - bd) + (ad + bc - bd)\zeta_3$. Since bd is calculated twice, multiplication of two Eisenstein integers involves 4 integer multiplications. Hence, similar to the GGH the encryption and decryption of the EEH are also both of order $O(N^2)$. Also similar to the NTRU case, one could also apply algorithms to speed up multiplications of polynomials as described in [35]. However, in Section 5 we will show that we can take the EEH parameter N to be smaller than the GGH parameter N for similar levels of security.

5 Security Analysis and Key Sizes

We now discuss the security of the GGH cryptosystem. There are three natural ways to attack the GGH cryptosystem:

(1) Try to obtain the private key $\mathbf{A}$ from the public key $\mathbf{B}$.
(2) Try to obtain information about the message from the ciphertext, given that the error vector is small.
(3) Try to solve the CVP of c with respect to the lattice $\mathcal{L}$ defined by $\mathbf{B}$.

5.1 Embedding Attack

Nguyen attacked the GGH by the embedding attack [26]. Nguyen noted that the choice of the error vector in the original GGH cryptosystem made it extremely vulnerable to attack. Let $\sigma = (\sigma, \sigma, \ldots, \sigma) \in \mathbb{Z}^N$. The crucial observation is that if c is a GGH ciphertext then $c + \sigma \equiv \mathbf{B}M \ mod\ 2\sigma$. Precisely, the linear equation $c = \mathbf{B}M + e$ can be reduced to:

$$c' = \frac{c - \mathbf{B}M_0}{2\sigma} = \mathbf{B}M' + \frac{e}{2\sigma} \quad (24)$$

where M_0 is the solution of:

$$c + (\sigma, \sigma, \ldots, \sigma) \equiv \mathbf{B}M \ mod\ 2\sigma \quad (25)$$

So the error vector $e' = \frac{e}{2\sigma}$ is an element of $\{\pm\frac{1}{2}\}^N$. Hence the choice of a large σ is not so essential condition for the security of the GGH scheme if $\sigma \geq \frac{1}{2}$. Hence we take σ to be $\frac{1}{2}$.

5.2 Algebraic Attack

Algebraic cryptanalysis is to model a cryptographic primitive by a set of polynomial equations. The system of equations is constructed such that the solution of this system is precisely the secret information of the cryptographic primitive (for instance, the secret key of an encryption scheme). Hence, breaking the EEH system is equivalent to the problem of recovering the polynomial $f(x)$ from a given polynomial $h(x)$, knowing that $f(x) \times h(x) = g(x) + qu(x)$.

The recovering of the private key of EEH is reduced to solve a system of $2N$ quadratic equations in $2N$ variables in $\mathbb{Z}[\zeta_3][x]$. In [36] is presented a more efficient tool for solving algebraic systems, namely fast *Gröbner basis* algorithms for standard values of the parameter in NTRU, such as $N = 251$, to solve a system of N quadratic equations in N variables for $f(x) \times h(x) = g(x) + qu(x)$. But this algebraic attack using Witt vectors is not effective for NTRU and ETRU if one wants to solve the associated system using *Gröbner basis* algorithms. Thus, this attack is not effective for the EEH cryptosystem with appropriate parameters.

5.3 Lattice Attacks

Recall that the EEH lattice $\mathcal{L}_{\mathbf{A}} = \mathcal{L}_{\mathbf{B}}$ is spanned by the rows of $4N \times 4N$ matrix:

$$\mathbf{B} = \begin{bmatrix} \lambda < I > & < \rho(h(x)) > \\ 0 & < qI > \end{bmatrix} \tag{26}$$

As we mentioned earlier, the vector $(\lambda f(x), g(x))$ is a relatively short vector in the lattice, therefore we can use basis reduction techniques such as the LLL or BKZ algorithms to try and recover the vector $(\lambda f(x), g(x))$ and hence recover our EEH private key. Note that the implementations of LLL and BKZ in Shoup's NTL library [37] find short vectors relative to the Euclidean norm. We want to take $\lambda = \frac{||g(x)||}{||f(x)||}$ where $||f(x)||$ denotes the Euclidean norm of the vector representation of $f(x)$. If the length of a shortest vector is much shorter than the shortest expected vector in the lattice, the LLL and BKZ are more successful at finding a shortest vector in a lattice. The norms of $\lambda f(x) + g(x)$ and $(\lambda f(x), g(x))$ have been presented in [31] respectively as follows:

$$\tau_e = \sqrt{\lambda^2(6d_f + 1) + 6d_g} \tag{27}$$

$$\tau_c = \sqrt{\lambda^2(8d_f + 1) + 8d_g} \tag{28}$$

So the norm of the polynomial $\lambda f(x) + g(x)$ is shorter than our target vector $(\lambda f(x), g(x))$.

Now we can implement the LLL and BKZ algorithms to show the security of the EEH lattice in order to lattice attacks (lattice basis reduction). Table 2 shows the results of experiments for randomly generated EEH keys for different parameter sets. For each parameter set we keep p and q constant taking $p = 2 + \zeta_3$ and $q = 81\zeta_3 = (1 - \zeta_3)^8$. We choose $d_f = d_g$ so we have $||f(x)|| \approx ||g(x)||$ and therefore we take $\lambda = 1$.

As we can see from Table 2, the BKZ algorithm is slower however it gives better results than the LLL algorithm. The success of the LLL algorithm drops sharply on EEH lattice for $N > 21$. For $N > 29$ the LLL algorithm rarely finds a target vector on EEH lattice. Similarly, the BKZ algorithm is very successful for $N \leq 35$ the its success drops sharply and rarely finds a target vector for $N > 47$ on EEH lattice. Therefore EEH lattice is more resistant to lattice attack.

Now we compare NTRU lattice and EEH lattice on the common criteria we have developed in Table 2. In [31] is done a comparison between NTRU lattice and ETRU lattice. Note that the ETRU lattice is similar to the EEH lattice. So the lattice security for EEH with $q = 81\zeta_3$ or $q = 11 + 86\zeta_3$ and polynomials of length N appears to be similar to that of NTRU lattice with $q = 2048$ and polynomials of length of approximately $3N$. Notice that the lattice security of EEH with polynomials of length N is comparable to the lattice security of NTRU and polynomials of length approximately $3N$.

As a result, we conjecture that the lattice security of EEH with polynomials of length N is comparable to the lattice security of NTRU with polynomials of length $3N$. Note, if we take the NTRU parameter N to be twice that of the EEH parameter N then the EEH lattice and the NTRU lattice have the same dimension but the EEH lattice has higher lattice security than the NTRU lattice of the same dimension.

5.4 Key Size

It is important to know how much storage is needed to store polynomials with coefficients modulo Eisenstein integers. An integer reduced modulo q in NTRU can be converted to binary and stored in $\lceil log_2\ q \rceil$ bits. Therefore in NTRU we need approximately $N\lceil log_2\ q \rceil$ bits to store polynomials reduced modulo q [31, 38].

Recall there are $d(q)$ distinct equivalence classes modulo q. Hence to reduce a Eisenstein integer modulo q we need approximately $\lceil log_2\ d(q) \rceil$ bits [31]. Therefore in the EEH we need approximately $N\lceil log_2\ d(q) \rceil$ bits to store polynomials reduced modulo q.

Also recall the GGH has N-dimensional lattice and the attacks presented in [26] have broken $N =$

Table 2. Lattice reduction on the EEH lattice using Shoup's LLL FP and BKZ FP functions for σ=0.99 and blocksize β=10.

			LLL			BKZ		
N	d_f	d_g	$Target(\%)$	$Trials$	$AvgTime(s)$	$Target(\%)$	$Trials$	$AvgTime(s)$
17	2	2	99.9	1000	0.53	100	1000	1.05
19	2	2	100	1000	0.77	100	1000	1.62
21	3	3	94.5	1000	1.2	99.5	1000	3.27
23	3	3	47.2	1000	1.46	100	1000	3.46
25	3	3	8.4	1000	1.91	98	1000	4.82
29	3	3	0	1000	2.71	100	1000	10.11
31	3	3	0	1000	3.25	99.9	1000	16.44
33	3	3	0.1	1000	3.85	99.4	500	21.69
35	4	4	0	1000	4.43	98.8	500	39.45
41	4	4	0	1000	6.7	1.6	500	80.91
47	4	4				0	100	139.45

Table 3. Comparison of key sizes (KB) of the EEH cryptosystem with the GGH, GGH(HNF), NTRU, and ETRU for $q = 81\zeta_3$ (EEH and ETRU), and $q = 2048$ (NTRU).

N	**GGH**[30]	**GGH(HNF)**[30]	**NTRU**[38]	**ETRU**[31]	**EEH**
200	330	32	0.138	0.082	0.082
300	990	75	1.65	0.122	0.122
400	2370	140	2.2	0.163	0.163

Table 4. Operating characteristics. $f(n) = \tilde{O}(g(n))$ if $f(n) = O(g(n).log^c n)$.

	GGH[24]	**NTRU**[38]	**ETRU**[31]	**EEH**
Encryption speed	$O(N^2)$	$O(N^2)$	$O(N^2)$	$O(N^2)$
Decryption speed	$O(N^2)$	$O(N^2)$	$O(N^2)$	$O(N^2)$
Message expansion	1–1	log_p^q to 1	1–1	1–1
Public key size	$\tilde{O}(N^2)$	$\tilde{O}(N)$	$\tilde{O}(N)$	$\tilde{O}(N)$
Private key size	$\tilde{O}(N^2)$	$\tilde{O}(N)$	$\tilde{O}(N)$	$\tilde{O}(N)$

$200, 250, 300, 350$ except $N = 400$. Thus, this large key size makes the GGH inefficient and impractical. Clearly, NTRU has $2N$-dimensional lattice and lattice attacks are not effective for $N = 251$. Hence, it's key size is reduced approximately by factor of 2. In this paper, as we see, the EEH cryptosystem has $4N$-dimensional lattice therefore it's key size is reduced approximately by factor of 4. For example, let there is an 400-dimensional lattice, then we have $N = \frac{400}{4} = 100$, $q = 81\zeta_3$ and $d(q) = 6561$. For this lattice the polynomials modulo q will take about $N\lceil log_2\, d(q)\rceil = 100\lceil log_2\, 6561\rceil = 1300$ bits, so public key takes $\frac{1300}{8} = 162.5 \approx 0.163$KBytes, which is much smaller than the key sizes of both GGH and GGH using HNF expression [27]. Table 3 shows the results of the above formulas to comparison of key sizes of the EEH, GGH, GGH(HNF), and NTRU. Moreover, Table 4 summarizes operating characteristics for NTRU, ETRU, GGH, and EEH.

6 Conclusion

We proposed a lattice based public key cryptosystem using polynomial representations over the Eisenstein integers. The proposed EEH cryptosystem is an improvement of the GGH system. Our scheme has stronger lattice security than GGH and NTRU, requires less storage and is comparable in terms of speed. Furthermore, our scheme is practical in key sizes compared with the GGH.

As we see, we can make various lattices with representations of polynomials. By studying various representations and size of coefficients of polynomials, the key size might be decreased and the efficiency could be increased. Moreover, the security of the cryptosystem is closely related to the choice of representations.

The EEH is a probabilistic cryptosystem since a single plaintext leads to many different ciphertexts due to the choice of the random perturbation e. This leads to a potential danger if one sends the same message twice using different random perturbations, or sends different messages using the same random perturbation. Thus future works can include applying a hash function to the plaintext M for determining the random perturbation e and developing padding schemes for EEH cryptosystem in practice.

References

[1] V. Lyubashevsky, and D. Micciancio, *Generalized compact knapsacks are collision resistant*, In

Proceed- ings of ICALP, (2006), Vol. 4052 of LNCS, pages 144–155.

[2] C. Peikert, and A. Rosen, *Lattices that admit logarithmic worst-case to average-case connection factors*, In Proceedings of STOC, ACM, (2007), pages 478–487.

[3] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of ACM, (2009), Vol. 56, pages 6–34.

[4] C. Peikert, and B. Waters, *Lossy trapdoor functions and their applications*, In Proceedings of STOC, (2008), pages 187–196.

[5] V. Lyubashevsky, A. Palacio, and G. Segev, *Public-key cryptographic primitives provably as secure as subset sum*, In D. Micciancio, editor, Proceedings of TCC, (2010), Vol. 5978 of LNCS, pages 382–400.

[6] C. Gentry, C. Peikert, and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, In Proceedings of STOC, (2008), pages 197–206.

[7] V. Lyubashevsky, and D. Micciancio, *Asymptotically efficient lattice-based digital signatures*, In Pro- ceedings of TCC, (2008), Vol. 4948 of LNCS, pages 37–54.

[8] D. Gordon, J. Katz, and V. Vaikuntanathan, *A group signature scheme from lattice assumptions*, Advances in Cryptology-ASIACRYPT, (2010), Springer Berlin Heidelberg, pages 395–412.

[9] S. Agrawal, D. Boneh, and X. Boyen, *Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical ibe*, Advances in CryptologyCRYPTO, (2010), Springer Berlin Heidelberg, pages 98–115.

[10] C. Gentry, S. Halevi, and V. Vaikuntanathan, *A simple bgn-type cryptosystem from lwe*, In H. Gilbert, editor, Advances in Cryptology EUROCRYPT, (2010), Vol. 6110 of Lecture Notes in Computer Science, pages 506–522.

[11] C. Gentry, *Fully homomorphic encryption using ideal lattices*, In Proceedings of STOC, ACM, (2009), pages 169–178.

[12] D. Stehle, and R. Steinfeld, *Faster fully homomorphic encryption*, In M. Abe, editor, ASIACRYPT, (2010), Vol. 6477 of Lecture Notes in Computer Science, pages 377–394.

[13] N. Ogura, G. Yamamoto, T. Kobayashi, and S. Uchiyama, *An improvement of key generation algorithm for gentrys homomorphic encryption scheme*, In IWSEC, (2010), Vol. 6434 of LNCS, pages 70–83.

[14] P. Cayrel, R. Lindner, M. Ruckert, and R. Silva, *Improved zero-knowledge identification with lattices*, Tatra Mountains Mathematical Publications 53.1 (2012), pages 33–63.

[15] V. Lyubashevsky, *Lattice-based identification schemes secure under active attacks*, In Proceedings of PKC, (2008), No. 4939 in LNCS, pages 162–179.

[16] P. Gaborit, J. Ohler, and P. Sole, *CTRU, a polynomial analogue of NTRU*, Tech- nical report, INRIA, France, 2002. Available at ftp://ftp.inria.fr/INRIA/publication/ publi-pdf/RR/RR-4621.pdf.

[17] M. Coglianese, and B.M. Goi, *MaTRU: A New NTRU-Based Cryptosystem*, In Proceedings of the 6th International Conference on Cryptology in India (INDOCRYPT), (2005), pages 232–243.

[18] N. Vats, *NNRU, a Noncommutative Analogue of NTRU*, The Computing Research Repos- itory (CoRR), abs/0902.1891, (2009). Available at http://arxiv.org/abs/0902.1891.

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

[20] C. Karimianpour, *Lattice-Based Cryptosystems*, Master's thesis, University of Ottawa, Canada, (2007).

[21] M. Nevins, C. Karimianpour, and A. Miri, *NTRU over rings beyond $\mathbb{Z}$*, Designs, Codes and Cryptography, (2010), vol. 56, no. 1, pages 65–78.

[22] E. Malekian, A. Zakerolhosseini, and A. Mashatan, *QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems*, The int'l Journal of information Security (ISeCure), (2011), vol. 3, no. 1, pages 29–42.

[23] A.H. Karbasi and R.E. Atani, *ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices*, The 7th International IEEE Symposium on Telecommunications (IST2014), Tehran, Iran, (2014).

[24] O. Goldreich, Sh. Goldwasser, and Sh. Halevi, *Public-key cryptosystems from lattice reduction problems*, In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, London, UK, (1997), pages 112–131.

[25] R.J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, Deep Space Network Progress Report, (1978), No. 44, pages 114–116.

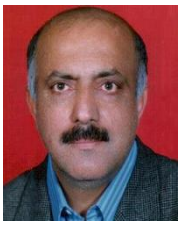
[26] P. Nguyen, *Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97*, Advances in Cryptology-Crypto '99, LNCS 1666, (1999), pages 288–304 .

[27] D. Micciancio , *Improving lattice based cryptosystems using the Hermite normal form*, In Cryptography and Lattices Conference (CaLC), (2001), pages 126–145.

[28] M. Ajtai, and C. Dwork, *A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence*, In 29th ACM Symposium on Theory of Computing, (1997), pages 284–293.

[29] C.P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theor. Comput. Sci., (1987), No. 53(2–3), pages 201–224.
[30] S. Paeng, B. Jung, and K. Ha, *A Lattice Based Public Key Cryptosystem Using Polynomial Representations*, In Y.G. Desmedt (Ed.), PKC, (2003), Vol. 2567 of LNCS, Springer, pages 292–308.
[31] K. Jarvis, and M. Nevins, *ETRU: NTRU over the Eisenstein Integers*, Designs, Codes and Cryptography 74.1, (2015), pages 219–242.
[32] K. Ireland, and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition. New York: Springer-Verlag, (1990).
[33] J. Hoffstein, J. Pipher, and J.H. Silverman, *An Introduction to Mathematical Cryptography*, Springer-Verlag, 1st edition, (2008).
[34] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, and W. Whyte, *NTRUSign: digital signatures using the NTRU lattice*, In Topics in cryptologyCT-RSA, (2003), Vol. 2612 of Lecture Notes in Comput. Sci., Springer, pages 122–140.
[35] J.H. Silverman, *High-Speed Multiplication of (Truncated) Polynomial Rings*, NTRU Cryptosystems Technical Report 11, (1999), Available from: http://www.ntru.com. Accessed: Dec 2010.
[36] G. Bourgeois, and J. Faugere, *Algebraic attack on NTRU using Witt vectors and Grobner bases*, In Journal of Math. Crypt., (2009), Vol. 3, pages 205–214.
[37] V. Shoup, *NTL: A Library for doing Number Theory*, http://www.shoup.net/ntl/. Accessed: Aug. (2010).
[38] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: a ring-based public key cryptosystem*, In Algorithmic Number Theory, Portland OR, (1998), Vol. 1423 of Lecture Notes in Comput. Sci., pages 267288.
[39] A.H. Karbasi and R.E. Atani, "PSTRU: A provably secure variant of *NTRUEncrypt* over extended ideal lattices," The 2nd National Industrial Mathematics Conference, Tabriz, Iran, (2015).

Reza Ebrahimi Atani studied Electronics Engineering at the University of Guilan, Rasht, Iran and got his B.S. degree in 2002. He followed his masters and Ph.D. studies at Iran University of Science & Technology (IUST) in Tehran, and received the the Ph.D. degree in 2010. He has an assistant professor position in Department of Computer Engineering at the University of Guilan. His research interests focuses on design and implementation of cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications.



Shahabaddin Ebrahimi Atani got his B.S. and M.S. in Mathematics. In 1996, he graduated from a Ph.D. program of Mathematical Science Department in University of Manchester, England. He is now a professor at faculty of Mathematical Sciences of the University of Guilan. His research interests include Rings and Semi-ring theory and Pullback of Rings.

Amir Hassani Karbasi studied his BSc in Applied Mathematics at the University of Tabriz in Tabriz, Iran. He received his BSc degree in 2010. He was accepted to follow his Masters study at the University of Guilan in Rasht, Iran. He received his MSc in Computer Networks in 2013. He is now a PhD candidate working on "design, analysis and implementation of lattice-based cryptography". He is a student member of IEEE and Iranian Society of Cryptology (ISC). His main research interests include lattice-based cryptography, digital signatures, network security, rings and semi-ring theory and Pullback of Rings.