Ratio Mathematica **ISSN**: 1592-7415
Vol. 34, 2018, pp. 49-65 **eISSN**: 2282-8214

A New Provably Secure Cryptosystem Using Dedekind Domain Direct Product Approach

Amir Hassani Karbasi[1]

Received: 27-02-2018. **Accepted**: 01-06-2018. **Published**: 30-06-2018

doi: 10.23755/rm.v34i0.404

Abstract

We would like to prevent, detect, and protect communication and information systems' attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service by providing cryptographic techniques. If we prove that an encryption algorithm is based on mathematical NP-hard problems, we can prove its security. In this paper, we present a new NTRU-Like public-key cryptosystem with security provably based on the worst-case hardness of the approximate lattice problems (NP-hard problems) in some structured lattices (ideal lattices) in order to attain the applicable objectives of preserving the confidentiality of communication and information system resources (includes hardware, software, firmware, information/data, and telecommunications). Our proposed scheme is an improvement of ETRU cryptosystem. ETRU is an NTRU-Like public-key cryptosystem based on the Eisenstein integers

[1] Department of Mathematics, University of Guilan, Rasht, Iran. karbasi@phd.guilan.ac.ir

where is a primitive cube root of unity. ETRU has heuristic security and it has no proof of security. We show that our cryptosystem has security stronger than that of ETRU, over Cartesian product of Dedekind domains and extended cyclotomic polynomials. We prove the security for our main algorithm from the R-SIS and R-LWE problems as NP-hard problems.
Keywords: Lattice-based cryptography; Ideal lattices; ETRU; Provable security; Dedekind domain.
2010 subject classification: 94A60; 11T71; 14G50; 68P25.

1. Introduction

Public-key cryptography has many exciting applications for web browsers, e-mail programs, cell phones, bank cards, RFID tags, smart cards, government communications, banking systems, and so on. The users to communicate over non-secure channels without any prior communication can use public-key cryptography. The idea of public-key cryptography was first proposed by Diffie and Hellman in 1976 [1]. Lattice-based cryptography as a field of public-key cryptography has attracted considerable interest and it has been categorized into post-quantum cryptography [6]. Lattice-based cryptography enjoys efficient implementations, very strong security proofs based on worst-case hardness, 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 $\mathbf{Z}_q[x]/<x^N-1>$ for N prime and q a small integer, it was quickly shown that breaking it could be reflected 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. For example, an 8-dimensional lattice in 2D view is shown in Figure 1.

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 and its variant of GapSVP in arbitrary lattices were presented by Ajtai and Dwork [8, 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 $\mathbf{Z}[x]/<x^n-1>$. 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 $\mathbf{Z}_q[x]/<\Phi>$ with a Φ 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)-Ideal-SVP). 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 Cartesian product of Eisenstein integers.

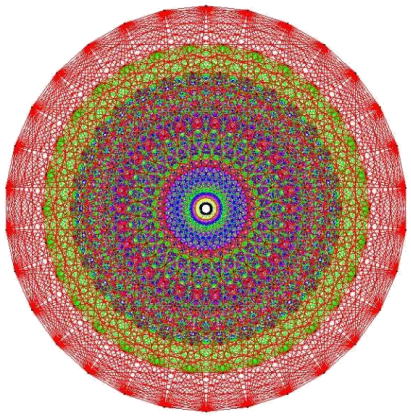

Figure 1. An 8-dimensional lattice in 2D view.

The ETRU is obtained from the NTRU by replacing $\mathbf{Z}$ 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 then CVP so its security remains heuristic. The other author's lattice-based schemes are [20 – 28] which are suitable for application to WSNs and IoT [29-31].

In this paper, our proposed cryptosystem based on extended ideal lattices over $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ (for $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ with $n+1$ a prime) 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 extended ideal lattices.

The rest of this paper is structured as follows: In section 2, we shortly review the ETRU system and explain the security related to the computational problems. In section 3, we study ideal lattices, R-SIS and R-LWE problems. In section 4, we suggest a key generation algorithm, where the generated public key follows a distribution for which Ideal-SVP reduces to R-LWE. In section 5, we make our modified ETRU cryptosystem as secure as worst-case problems over ideal lattices. Finally, the paper concludes in section 6.

2. ETRU Cryptosystem

2.1. Parameters Creation

We denote by ζ_3 a complex cube root of unity, that is $\zeta_3^3 = 1$ where $\zeta_3 = 1/2(-1+\sqrt{3}i)$ since $\zeta_3^3 - 1 = (\zeta_3 - 1)(\zeta_3^2 + \zeta_3 + 1) = 0$, we have $\zeta_3^2 + \zeta_3 + 1 = 0$ and hence $\zeta_3^2 = -1 - \zeta_3$. The ring of Eisenstein integers, denoted $\mathbf{Z}[\zeta_3]$, is the set of complex numbers of the form $\alpha = a + b\zeta_3$ with $a, b \in \mathbf{Z}$. For $\alpha = a + b\zeta_3$ we will define $d(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 - ab$ 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 $a, b \in \mathbf{Z}$. 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 $\mathbf{Z}[\zeta_3]$ form a lattice in X generated by the basis $B = \{1, \zeta_3\}$. Note that the two basis vectors 1 and ζ_3, represented by the vectors (1, 0) and $(-1/2, \sqrt{3}/2)$ in P^2, have 120 degrees with equal length. Let β be an Eisenstein integer. We define the ideal $L(\beta) = \{a\beta + b\beta\zeta_3 \mid a, b \in \mathbf{Z}\}$. Therefore $L(\beta)$ is a lattice generated by the basis $\{\beta, \beta\zeta_3\}$. 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 < *B* > to be the *2n* by *2n* matrix. We choose an prime *n* and set $R = \mathbf{Z}[\zeta_3, x]/ < x^n - 1 >$, we also choose *p*

and q in $\mathbf{z}[\zeta_3]$ 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 $n' = 2n$.

2.2. Key Generation

Private key consists of two randomly chosen polynomials f, g in R. We define the inverses $Fq = f^{-1}$ in Rq and $Fp = f^{-1}$ in Rp. Hence public key is generated by $h = Fq * g$. 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 $\lceil \log_2(4|q|/3) \rceil$, hence the size of the ETRU public key is $K = 2n\lceil \log_2(4|q|/3) \rceil$. An NTRU public key, corresponding to polynomials with $n' = 2n$ coefficients reduced modulo an integer q', has size $K' = n'\lceil \log_2(q') \rceil$. Therefore to maintain the same key size as NTRU with $n' = 2n$ and $q' = 2k$, we should choose $|q| \leq (3/4)q'$ so that $\lceil \log_2(4|q|/3) \rceil \leq \lceil \log_2(q') \rceil$.

2.3. Encryption

Each encryption requires the user to compute $e = \phi * ph + m \bmod q$ 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.

2.4. 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 $2n'^2 + 2n' \sim 8n^2 + 4n$ operations for NTRU and only $6n^2 + 29n$ operations for ETRU.

2.5. Decryption Failure and Security

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

3. Ideal Lattices and Their Hard Problems

Our results are restricted to the sequence of rings $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ with $\Phi = < (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + \ldots + (1,1,1,1)x + (1,1,1,1) >$ where n+1 is a prime

that Φ is irreducible cyclotomic polynomial. We can refer to [19] for irreducibility of cyclotomic polynomials F_n in $\mathbf{Z}[z_3][x]$ where n is prime in $\mathbf{Z}[z_3]$ The R-LWE problem is known to be hard when Φ is cyclotomic [16]. The security analysis for our proposed scheme 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 $((a_i, b_i z_3), (c_i, d_i z_3))(a_i, b_i \zeta_3)$ where $a_i, b_i, c_i, d_i \in \mathbf{Z}$, so in this paper, all operations execute for a_i's, b_i's, c_i's and d_i's separately, that is, $X \cong P^2$ component-wise. The latter assumption is believed to be valid for any $g(n)=o(n)$. Also we can define £ and ³ as poset orders.

3.1. Notation

Similar to [14] we denote by $\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}(x_1, x_2, x_3, x_4)$ (respectively $\upsilon_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$) the standard n-dimensional Gaussian function (respectively distribution) with center (0,0,0,0) and variance $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. We denote by $Exp(\mu)$ the exponential distribution on P^{4n} with mean μ 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 $\Delta(D_1; D_2) = 1/2\sum_{x\in E} | D_1(x_1, x_2, x_3, x_4) - D_2(x_1, x_2, x_3, x_4) |$. We write $z \leftarrow D$ when the random variable z is chosen from the distribution D. The integer n is called the *lattice dimension*. Note that in our proposed scheme with pairwise components and coefficients in vectors, the dimension increases four times without increasing n. The *minimum* $\lambda_1(L)$ (respectively $\lambda_1^{\infty}(L)$) is the Euclidean (respectively infinity) norm of any shortest vector of $L \setminus (0,0,0,0)$.

The *dual* of lattice L is the lattice $\hat{L} = \{(c_1, c_2, c_3, c_4) \in R^{4n} : \forall i, <(c_1, c_2, c_3, c_4), (b_{i1}, b_{i2}, b_{i3}, b_{i4})> \in \mathbf{Z}^4\}$ where the b_{ij}'s are a *basis* of L. For a lattice L, $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) > (0, 0, 0, 0)$ and $(c_1,c_2,c_3,c_4) \in P^{4n}$, we define the *lattice Gaussian distribution* of support L, deviation $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and center (c_1,c_2,c_3,c_4) by

$D_{L,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1, b_2, b_3, b_4) = \rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1, b_2, b_3, b_4) / \rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(L)$, for any $(b_1, b_2, b_3, b_4) \in L$.

We extend the definition of $D_{L,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}$ to any $M \subseteq L$ (not necessarily a sub-lattice), by setting

$D_{M,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1,b_2,b_3,b_4) = (\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1,b_2,b_3,b_4)) / (\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(M))$ and for

$(\delta_1,\delta_2,\delta_3,\delta_4) > (0,0,0,0)$, we denote the *smoothing parameter* $\eta_{(\delta_1,\delta_2,\delta_3,\delta_4)}(L)$ as the smallest $(\sigma_1,\sigma_2,\sigma_3,\sigma_4) > (0,0,0,0)$ such that

$\rho_{(1,1,1,1)/(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}(\hat{L} \setminus (0,0,0,0)) \le (\delta_1,\delta_2,\delta_3,\delta_4)$.

It quantifies how large $(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ needs to be for $D_{L,(\sigma_1,\sigma_2,\sigma 3,\sigma_4),(c_1,c_2,c_3,c_4)}$ to behave like a continuous Gaussian. We will typically consider $\delta_i = 2^{-n}$.

3.2. Definition

Let *n*+1 be a prime and $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ which is irreducible over $\mathrm{Q}[z_3]' \ \mathrm{Q}[z_3]$ also let $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$. 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 $I \neq (0,0,0,0)$ corresponds to a full-rank sub-lattice of Z^{4n}. Thus we can view *I* as both a lattice and an ideal. An *ideal lattice* for Φ is a sub-lattice of $(Z*Z)^{2n}$ 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 Φ -ideal lattice.

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

3.3. Properties of The Ring of Cartesian Product

For $(v_1,v_2,v_3,v_4) \in R$ we define by ||(v_1, v_2, v_3, v_4)|| its Euclidean norm. We denote the multiplicative *expansion factor* by

$\gamma_{\times}(R) = \max_{u_i,v_i \in R}(\| (u_1,u_2,u_3,u_4) \times (v_1,v_2,v_3,v_4) \|) / (\| (u_1,u_2,u_3,u_4) \| . \| (v_1,v_2,v_3,v_4) \|)$.

Since Φ is the *n+1*-th cyclotomic polynomial, the ring *R* is exactly the maximal order of the cyclotomic field $K := \frac{(\mathrm{Q}[z_3]' \ \mathrm{Q}[z_3])[x]}{\mathrm{F}} @ \mathrm{Q}[z,z']$. We denote by $(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4})_{i \le n}$ the complex embeddings. We can choose $(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4}) : K \to K(\zeta_1^{2i+1},\zeta_2^{2i+1},\zeta_3^{2i+1},\zeta_4^{2i+1})$ for $i \le n$.

Lemma 3.1. *The norm of* α *as an element in* $\Theta(\zeta_3)$ *is* $a^2 + b^2$ *- ab. This is also* $|\alpha|^2$, *where* α *is denoted as an element of* **X**.

Proof. The minimal polynomial of ζ_3 over Θ is the cyclotomic polynomial $\Phi_3 = x^2 + x + 1$. Thus, there exist exactly two monomorphisms (isomorphisms in this case) from Θ to X fixing Θ and permuting the roots of Φ_3. Since Φ_3 has two roots ζ_3 and ζ_3^2, the embeddings are $\sigma_1(a+b\zeta_3) = a+b\zeta_3$ and $\sigma_2(a+b\zeta_3) = a+b\zeta_3^2$, where $a, b \in \Theta$. By definition, the algebraic norm of $\alpha = a+b\zeta_3$ is

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)$$
$$= (a+b\zeta_3)(a+b\zeta_3^2)$$

Note that $\zeta_3^2 = \overline{\zeta}_3$ and $\zeta_3 + \overline{\zeta}_3 = -1$. So we have

$$N(\alpha) = (a+b\zeta_3)(a+b\overline{\zeta}_3)$$
$$= a^2 + b^2 + ab(\zeta_3 + \overline{\zeta}_3)$$
$$= a^2 + b^2 - ab$$

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

$$|\alpha|^2 = |a+b\zeta_3|^2$$
$$= |a+b(\frac{-1+\sqrt{3}i}{2})|$$
$$= |a-\frac{b}{2}+\frac{b\sqrt{3}i}{2}|^2$$
$$= \left(a-\frac{b}{2}\right)^2 + \left(\frac{b\sqrt{3}}{2}\right)^2$$
$$= a^2 + b^2 - ab$$

□

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 $T_2(\alpha_1,\alpha_2,\alpha_3,\alpha_4)^2 = (\sum_{i\le n}|\sigma_{i1}(\alpha_1)|^2, \sum_{i\le n}|\sigma_{i2}(\alpha_2)|^2, \sum_{i\le n}|\sigma_{i3}(\alpha_3)|^2, \sum_{i\le n}|\sigma_{i4}(\alpha_4)|^2)$. We also use the fact that for any $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \in R$, we have $|N(\alpha_1,\alpha_2,\alpha_3,\alpha_4)|$ = det $< (\alpha_1,\alpha_2,\alpha_3,\alpha_4) >$, where $<(\alpha_1,\alpha_2,\alpha_3,\alpha_4)>$ is the ideal of R generated by $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$. Let (q_1, q_2, q_3, q_4) be a prime element such that Φ has n distinct linear factors modulo (q_1, q_2, q_3, q_4), that is,
$\Phi = (\prod_{i\le n}((x_1,x_2,x_3,x_4) - (\zeta_1^i, \zeta_2^i, \zeta_3^i, \zeta_4^i)) \bmod (q_1,q_2,q_3,q_4)$ where ζ_i's are primitive $n+1$-th root of unity modulo (q_1, q_2, q_3, q_4) component-wise. Also we know that $R_{(q_1,q_2,q_3,q_4)} = R/(q_1R)' R/(q_2R)' R/(q_3R)' R/(q_4R)$.

3.4. Adaptation of Ideal Lattice Problems

Definition 3.1. *The ring small integer solution problem with parameters* $(q_1, q_2, q_3, q_4), m, (b_1, b_2, b_3, b_4), \mathrm{F}$ *is: Given m polynomials* $(a_{11}, a_{21}, a_{31}, a_{41}), ..., (a_{m1}, a_{m1}, a_{m1}, a_{m1})$ *chosen uniformly and independently in* $R_{(q_1,q_2,q_3,q_4)}$, *find* (t_1, t_2, t_3, t_4) *in assumed R-module such that* $\| (t_1, t_2, t_3, t_4) \| £ (b_1, b_2, b_3, b_4)$.

In [14] is shown that R-SIS and R-LWE are dual. For $(s_1, s_2, s_3, s_4) \in R_{(q_1,q_2,q_3,q_4)}$ and $(\psi_1, \psi_2, \psi_3, \psi_4)$ some distributions in $R_{(q_1,q_2,q_3,q_4)}$, we have $A_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ as the distribution obtained by sampling the pair $((a_1, a_2, a_3, a_4), (a_1, a_2, a_3, a_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4))$ with $((a_1, a_2, a_3, a_4), (e_1, e_2, e_3, e_4)) \leftarrow U(R_{(q_1,q_2,q_3,q_4)}) \times (\psi_1, \psi_2, \psi_3, \psi_4)$. The Ring Learning With Errors problem (R-LWE) was introduced by Lyubashevsky *et al.*[16] and shown hard for specific error distributions ψ. The error distributions $(\psi_1, \psi_2, \psi_3, \psi_4)$ that we use are an adaptation of those introduced in [16].

Definition 3.2. $(R - LWE^{\Phi}_{(q_1,q_2,q_3,q_4),(\alpha_1,\alpha_2,\alpha_3,\alpha_4)})$*: Let* $(\psi_1, \psi_2, \psi_3, \psi_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ *and* $(s_1, s_2, s_3, s_4) \leftarrow U(R_{(q_1,q_2,q_3,q_4)})$ *where* $\overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ *is a family of distributions. Given access to an oracle O that produces samples in* $R_{(q_1,q_2,q_3,q_4)} \times R_{(q_1,q_2,q_3,q_4)}$ *, distinguish whether O outputs samples from* $A_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ *or from* $U(R_{(q_1,q_2,q_3,q_4)} \times R_{(q_1,q_2,q_3,q_4)})$. *The distinguishing advantage should be* $1/poly(n)$ $(resp.\ 2^{-o(n)})$ *over the randomness of the input, the randomness of the samples and the internal randomness of the algorithm, component-wise [14].*

Theorem 1 in [14] indicates that R-LWE is hard, assuming that the worst-case γ-Ideal-SVP cannot be efficiently solved using quantum computers, for small γ. 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 $(e_1, e_2, e_3, e_4) \leftarrow (\psi_1, \psi_2, \psi_3, \psi_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$, and with an even smaller Ideal-SVP approximation factor γ. This should allow to both simplify the proposed scheme and to strengthen its security guarantee.

3.5. Our Proposed Variants of R-LWE

For $(s_1, s_2, s_3, s_4) \in R_{(q_1,q_2,q_3,q_4)}$ and $(\psi_1, \psi_2, \psi_3, \psi_4)$ some distributions in $R_{(q_1,q_2,q_3,q_4)}$, we denote $A^{\times}_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ as the distribution obtained by sampling

the pair $((a_1,a_2,a_3,a_4),(a_1,a_2,a_3,a_4)(s_1,s_2,s_3,s_4)+(e_1,e_2,e_3,e_4))$ with $((a_1,a_2,a_3,a_4),(e_1,e_2,e_3,e_4)) \leftarrow U(R^{\times}_{(q_1,q_2,q_3,q_4)})\times(\psi_1,\psi_2,\psi_3,\psi_4)$, where $R^{\times}_{(q_1,q_2,q_3,q_4)}$ is the set of invertible elements of $R_{(q_1,q_2,q_3,q_4)}$. This variant is hard and called $R-LWE^{\times}_{++}$ as [14]. Furthermore, as explained in [18], the nonce (s_1,s_2,s_3,s_4) can also be sampled from the error distribution without incurring any security loss. We call this variant $R-LWE^{\times}_{HNF++}$. According to adaptation of lemmas 7, 8 and 9 as well as Theorem 2 in [14] the problems $R-LWE^{\times}_{++}$ and $R-LWE^{\times}_{HNF++}$ are dual to γ-Ideal-SVP and are defined some families of *R*-modules for *I*, an arbitrary ideal of $R_{(q_1,q_2,q_3,q_4)}$ as a lattice, also short vectors exist in ideal and statistical distance (regularity bound) is exactly appropriate and reliable.

4. The Proposed 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.

Input: $n, q_1, q_2, q_3, q_4 \in \mathbf{Z}, p_1, p_2, p_3, p_4 \in R^{\times}_{(q_1,q_2,q_3,q_4)}, (\sigma_1,\sigma_2,\sigma_3,\sigma_4) \in \mathbf{R}$.

Output: A key pair $(sk, pk) \in R \times R^{\times}_{(q_1,q_2,q_3,q_4)}$.

Sample $(f_1, f_2, f_3, f_4)'$ from $D_{\mathbf{Z}^{4n},(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$; let $(f_1, f_2, f_3, f_4) = (p_1, p_2, p_3, p_4).(f_1, f_2, f_3, f_4)'+(1,1,1,1)$; if $((f_1, f_2, f_3, f_4) \mod (q_1, q_2, q_3, q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}$, resample. Sample (g_1, g_2, g_3, g_4) from $D_{\mathbf{Z}^{4n},(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$; if $((g_1, g_2, g_3, g_4) \mod (q_1, q_2, q_3, q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}$, resample. Return secret key $sk = (f_1, f_2, f_3, f_4)$ and public key $pk = (h_1, h_2, h_3, h_4) = (p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4) / (f_1, f_2, f_3, f_4) \hat{I}\ R^{'}_{(q_1,q_2,q_3,q_4)}$.

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

Theorem 4.1[Adapted from 14]**.** *Let* $n \geq 8$ *and n+1 be a prime such that* $\Phi = <(1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1)>$ *splits into n linear factors modulo prime* $(q_1,q_2,q_3,q_4) \geq (5,5,5,5)$ *component-wise. Let*

$\sigma_i \geq \sqrt{n \ln(2n(1+1/\delta_i))/\pi}.q_i^{1/n}$, *or an arbitrary* $\delta_i \in (0,1/2)$. *Let* $(a_1, a_2, a_3, a_4) \in R$ *and* $(p_1, p_2, p_3, p_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$

Then

$\Pr_{(f_1,f_2,f_3,f_4)' \leftarrow D_{\mathbb{Z}^4,(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}}[((p_1,p_2,p_3,p_4).(f_1,f_2,f_3,f_4)'+(a_1,a_2,a_3,a_4) \bmod (q_1,q_2,q_3,q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}] \leq n((1,1,1,1)/(q_1,q_2,q_3,q_4)+$
$+2(\delta_1,\delta_2,\delta_3,\delta_4))$

component-wise.

The following Lemma ensures that the generated secret key is small.

Lemma 4.1[Adapted from 14]**.** *Let* $n \geq 8$ *and n+1 be a prime such that* $\Phi = <(1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1)>$ *splits into n linear factors modulo prime* $(q_1, q_2, q_3, q_4) \geq (8,8,8,8)n$. *Let* $\sigma_i \geq \sqrt{2n \ln(6n)/\pi}.q_i^{1/n}$. *The secret key polynomials* $(f_1, f_2, f_3, f_4), (g_1, g_2, g_3, g_4)$ *returned by the algorithm* 1 *satisfy, with probability* $\geq 1 - 2^{-n+3}$:
$\| (f_1, f_2, f_3, f_4) \| \leq (2,2,2,2)n \| (p_1, p_2, p_3, p_4) \| (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *and* $\| (g_1, g_2, g_3, g_4) \| \leq \sqrt{n}(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.
If $\deg(p_1, p_2, p_3, p_4) \leq (1,1,1,1)$, then

$\| (f_1, f_2, f_3, f_4) \| \leq (4,4,4,4)\sqrt{n} \| (p_1, p_2, p_3, p_4) \| (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *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 construct the proposed cryptosystem over ideal lattices with high efficiency and provable security (CPA-secure).

5. The Proposed New Cryptosystem

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

5.1. Decryption Failure

The correctness condition for each pairwise coefficient in the proposed cryptosystem is as follows.

Lemma 5.1 [Adapted from 14]**.** *If* $\omega(n^{1.5} \log n)\alpha_i \deg((p_i)) \| (p_i) \|^2 \sigma_i < (1,1,1,1)$ *(resp.* $\omega(n^{0.5} \log n)\alpha_i \| (p_i) \|^2 \sigma_i < (1,1,1,1)$ *if* $\deg(p_i) \leq (1,1,1,1)$*)* *and* $\alpha_i q_i \geq n^{0.5}$, *then the decryption algorithm of the proposed cryptosystem recovers* (M_1, M_2, M_3, M_4) *with probability* $1 - n^{-\omega(1)}$ *over the choice of* s_i, e_i, f_i *and* g_i *component-wise.*

Proof. In the decryption algorithm, we have

$$(C_1, C_2, C_3, C_4)' = (p_1, p_2, p_3, p_4).((g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4)(f_1, f_2, f_3, f_4)) +$$
$$+ (f_1, f_2, f_3, f_4)(M_1, M_2, M_3, M_4) \bmod (q_1, q_2, q_3, q_4)$$

and let

$$(C_1, C_2, C_3, C_4)'' = (p_1, p_2, p_3, p_4).((g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4)(f_1, f_2, f_3, f_4)) +$$
$$+ (f_1, f_2, f_3, f_4)(M_1, M_2, M_3, M_4)$$

computed in R (not modulo (q_1, q_2, q_3, q_4)). If $\| (C_1, C_2, C_3, C_4)'' \|_\infty < (q_1, q_2, q_3, q_4)/2$ then we have $(C_1, C_2, C_3, C_4)' = (C_1, C_2, C_3, C_4)''$ in R and hence, since $(f_i) \equiv (1,1,1,1) \bmod (p_i), (C_i)' \bmod (p_i) = (C_i)'' \bmod (p_i) = (M_i) \bmod (p_i)$, i.e., the decryption algorithm succeeds. It thus suffices to give an upper bound on the probability that $\| (C_1, C_2, C_3, C_4)'' \|_\infty > (q_1, q_2, q_3, q_4)/2$. From Lemma 2, we know that with probability $\geq 1 - 2^{-n+3}$ both (f_1, f_2, f_3, f_4) and (g_1, g_2, g_3, g_4) have Euclidean norms $\leq 2n \| (p_i) \| \sigma_i$ $(resp.\ (4,4,4,4)\sqrt{n} \| (p_i) \| \sigma_i$ *if* $\deg(p_i) \leq (1,1,1,1))$ this implies that, $\| (p_i)(f_i) \|, \| (p_i)(g_i) \| \leq (2,2,2,2) n^{1.5} \| (p_i) \|^2 \sigma_i$ $(resp.\ (8,8,8,8)\sqrt{n} \| (p_i) \|^2 \sigma_i)$ with probability $\geq 1 - 2^{-n+3}$. From Lemma 6 in [14], both $(p_1, p_2, p_3, p_4)(f_1, f_2, f_3, f_4)(e_1, e_2, e_3, e_4)$ and $(p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4)$ have infinity norm

$(resp. \leq (2,2,2,2)\alpha_i q_i n^{1.5} \omega(\log n). \| (p_i) \|^2 \sigma_i$ $(8,8,8,8)\alpha_i q_i \sqrt{n} \omega(\log n). \| (p_i) \|^2 \sigma_i$), with probability $1 - n^{-\omega(1)}$. Independently:

Proposed Encryption Scheme

Parameters Creation:

1. We use $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ with $n \geq 8$ and $n+1$ a prime, $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ and $R_{(q_1,q_2,q_3,q_4)} = R/(q_1R) \times R/(q_2R) \times R/(q_3R) \times R/(q_4R)$ with $(q_1,q_2,q_3,q_4) \geq (5,5,5,5)$ prime such that $\Phi = \prod_{k=1}^{n} \phi_k$ in $R_{(q_1,q_2,q_3,q_4)}$ with distinct ϕ_k's component-wise.

Key Generation:

2. We use the algorithm 1 and return $sk = (f_1, f_2, f_3, f_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$ with $(f_1, f_2, f_3, f_4) \equiv (1,1,1,1) \bmod (p_1, p_2, p_3, p_4)$, and $pk = (h_1,h_2,h_3,h_4) = (p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4) / (f_1, f_2, f_3, f_4) \hat{\mathrm{I}} \ R'_{(q_1,q_2,q_3,q_4)}$, component-wise.

Encryption:

3. Given message $(M_1,M_2,M_3,M_4) \in P$, set $(s_1, s_2, s_3, s_4), (e_1, e_2, e_3, e_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ and return ciphertext $(C_1,C_2,C_3,C_4) = (h_1,h_2,h_3,h_4)(s_1,s_2,s_3,s_4) + (p_1,p_2,p_3,p_4)(e_1,e_2,e_3,e_4) + (M_1,M_2,M_3,M_4) \in R_{(q_1,q_2,q_3,q_4)}$

Decryption:

4. Given ciphertext (C_1,C_2,C_3,C_4) and secret key (f_1, f_2, f_3, f_4), compute $(C_1,C_2,C_3,C_4)' = (f_1, f_2, f_3, f_4).(C_1,C_2,C_3,C_4) \in R_{(q_1,q_2,q_3,q_4)}$ and return $(C_1,C_2,C_3,C_4)' \bmod (p_1, p_2, p_3, p_4)$.

$$\| (f_i)(M_i) \|_\infty \leq \| (f_i)(M_i) \| \leq \sqrt{n} \| (f_i) \| . \| (M_i) \| \leq (2,2,2,2).(\deg(p_i) + (1,1,1,1).n^2 \| (p_i) \|^2 \ \sigma_i$$

(resp. $(8,8,8,8)n \| (p_i) \|^2 \ \sigma_i$). Since $\alpha_i q_i \geq \sqrt{n}$, we conclude that $\| (C_i)'' \|_\infty \leq ((6,6,6,6) + (2,2,2,2)\deg(p_i)).\alpha_i q_i n^{1.5} \omega(\log n). \| (p_i) \|^2 \ \sigma_i$ (resp. $(24,24,24,24)\alpha_i q_i n^{0.5} \omega(\log n). \| (p_i) \|^2 \ \sigma_i$), with probability $1 - n^{-\omega(1)}$, component-wise.

□

5.2. Security

The security of the proposed cryptosystem follows by an elementary reduction from the decisional $R-LWE^{\times}_{HNF++}$, exploiting the uniformity of the public key in $R^{\times}_{(q_1,q_2,q_3,q_4)}$ (adaptation of Theorem 3 in [14]), and the invertibility of (p_1, p_2, p_3, p_4) in $R_{(q_1,q_2,q_3,q_4)}$.

Lemma 5.2 [adapted from 7]**.** *Suppose n+1 is a prime such that* $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ *splits into n linear factors modulo prime* $q_i = \omega(1)$. *Let* $\sigma_i \geq (2,2,2,2)n\sqrt{\ln(8nq_i)}.q_i^{(1/2,1/2,1/2,1/2)+\varepsilon_i}$ *and* $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4),(\delta_1,\delta_2,\delta_3,\delta_4) > (0,0,0,0), (p_1, p_2, p_3, p_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$. *If there exists an IND-CPA attack against the proposed cryptosystem that runs in time T and has success probability* $(1/2,1/2,1/2,1/2)+\delta_i$ *with parameters* αi *and* q_i*, then there exists an algorithm solving* $R-LWE^{\times}_{HNF++}$ *that runs in time T' = T + O(n) and has success probability* $\delta_i' = \delta_i - q_i^{-\Omega(n)}$.

Proof. Let *A* denote the given IND-CPA attack algorithm. We construct an algorithm *B* against $R-LWE^{\times}_{HNF++}$ that runs as follows, given oracle *O* that samples from either $U(R^{\times}_{q_i} \times R_{q_i})$ or $A^{\times}_{s_i,\psi_i}$ for some previously chosen $s_i \leftarrow \psi_i$ and $\psi_i \leftarrow \bar{\Upsilon}_{\alpha_i}$. Algorithm *B* first calls *O* to get a sample $((h_i)', (C_i)')$ from $R^{\times}_{q_i} \times R_{q_i}$. Then, algorithm *B* runs *A* with public key $(h_i) = (p_i).(h_i)' \in R_{q_i}$. When *A* outputs challenge messages $(M_{0i}), (M_{1i}) \in P$, algorithm *B* picks $b \leftarrow U(\{0,1\})$, computes the challenge ciphertext $(C_i) = (p_i).(C_i)' + (M_{bi}) \in R_{q_i}$, and returns (C_i) to *A*. Eventually, when *A* outputs its guess *b'* for *b*, algorithm *B* outputs 1 if *b' = b* and 0 otherwise. The $(h_i)'$ used by *B* is uniformly random in $R^{\times}_{q_i}$ and therefore so is the public key (h_i) given to *A*, thanks to the invertibility of (p_i) modulo (q_i). 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, component-wise. Moreover, since $(C_i)' = (h_i).s_i + e_i$ with $s_i, e_i \leftarrow \psi_i$, the ciphertext (C_i) given to *A* has the right distribution as in the IND-CPA attack. Overall, if *O* outputs samples from $A^{\times}_{s_i,\psi_i}$ then *A* succeeds and *B* returns 1 with probability $\geq (1/2,1/2,1/2,1/2) + \delta_i - q_i^{-\Omega(n)}$. Now, if *O* outputs samples from $U(R^{\times}_{q_i} \times R_{q_i})$, then, since $p_i \in R^{\times}_{q_i}$, the value of $(p_i)(C_i)'$ and hence (C_i), is uniformly random in R_{qi} 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 adaptation of Theorem 1 in [14]) we obtain main result.

6. Conclusions

In this paper, we provided a new 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 $R = (\mathbf{Z}[\zeta_3] \times \mathbf{Z}[\zeta_3])[x] / < (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ has its coefficients of the form $((a_i, b_i z_3), (c_i, d_i z_3))$ where $a_i, b_i, c_i, d_i \in \mathbf{Z}$, so we made both lemmata and theorems here for a_i's, b_i's, c_i's and d_i's separately, that is, we reflected $(C, C) @ (R^2, R^2)$. Hence, we could enhance the dimension of lattice 4-times without increasing *n*.

References

[1] W. Diffie and M.E. Hellman, "*New directions in cryptography*," In IEEE Trans. On Information Theory, (1976), 22, 644-654.

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

[3] D. Coppersmith and A. Shamir, "*Lattice attacks on NTRU*," In Fumy, W. (ed.) EUROCRYPT, LNCS, (1997), 1233, 52–61.

[4] J. Hoffstein, J. Pipher, and J.H. Silverman, "*NTRU: A ring-based public-key cryptosystem*," In Buhler, J.P. (ed.) ANTS, LNCS, (1998), 1423, 267–288.

[5] IEEE P1363. Standard specifications for public-key cryptography, http://grouper.ieee.org/groups/1363/

[6] R.A. Perlner and D.A. Cooper, "*Quantum resistant public-key cryptography: a survey*," In Proc. of IDtrust, ACM, New York, (2009), 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, (2013).

[8] M. Ajtai and C. Dwork, "*A public-key cryptosystem with worst-case/average-case equivalence*," In Proceedings of STOC, ACM, (1997), 284-293.

[9] V. Lyubashevsky and D. Micciancio, "*On bounded distance decoding, unique shortest vectors, and the minimum distance problem*," In Proceedings of Crypto, (2009), 5677, 450-461.

[10] D. Micciancio, "*Generalized compact knapsacks, cyclic lattices, and efficient oneway functions*," Computational Complexity, (2007), 16, 4, 365-411.

[11] V. Lyubashevsky and D. Micciancio, "*Generalized compact knapsacks are collision resistant*," In Proceedings of ICALP, (2006), 4052, 144-155.

[12] C. Peikert and A. Rosen, "*Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices*," In Proceedings of TCC, (2006), 145-166.

[13] O. Regev, "*On lattices, learning with errors, random linear codes, and cryptography*," Journal of ACM, (2009), 56, 6.

[14] D. Stehle and R. Steinfeld, "*Making NTRU as Secure as Worst-Case Problems over Ideal Lattices*," In Eurocrypt, (2011), 6632, 27-47.

[15] M. Nevins, C. Karimianpour, and A. Miri, "*NTRU over rings beyond Z*," Des. Codes Cryptogr., (2010), 56, 1, 65–78.

[16] V. Lyubashevsky, C. Peikert, and O. Regev, "*On ideal lattices and learning with errors over rings*," In Gilbert, H. (ed.) EUROCRYPT, (2010), 6110, 1–23.

[17] C. Gentry, "*Fully homomorphic encryption using ideal lattices*," In Proc. of STOC, (2009), 169–178.

[18] V. Lyubashevsky, C. Peikert, and O. Regev, "*On ideal lattices and learning with errors over rings*," Draft version, dated 01/02/2011.

[19] P. Garrett, "*Abstract Algebra*," University of Minnesota, (2007), 211-217.

[20] R.E. Atani, S.E. Atani, and A.H. Karbasi, "*EEH: A GGH-Like Public Key Cryptosystem Over The Eisenstein Integers Using Polynomial Representation*," The ISC International Journal of Information Security (IseCure), (2015), 7, 2, 115-126.

[21] A.H. Karbasi and R.E. Atani, "*ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices*," IACR Cryptology ePrint Archive, (2015), 549.

[22] 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).

[23] A.H. Karbasi and R.E. Atani, "*A Survey on Lattice-based Cryptography*," (in Persian), Biannual Journal for Cyberspace Security (Monadi AFTA), (2015), 3, 1, 3-14.

[24] A.H. Karbasi, M.A. Nia, and R.E. Atani, "*Designing of An Anonymous Communication System Using Lattice-based Cryptography*," (in Persian), Journal of Electronic and Cyber Defence, (2014), 2, 3, 13-22.

[25] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*A Provably Secure Variant of ETRU Based on Extended Ideal Lattices over Direct Product of Dedekind domains*," Submitted.

[26] A.H. Karbasi, R.E. Atani, and S.E. Atani, "*A New Ring-Based SPHF and PAKE Protocol On Ideal Lattices*," Submitted.

[27] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*PairTRU: Pairwise Non-commutative Extension of The NTRU Public key Cryptosystem*," International Journal of Information Security Science, (2018), 7, 1, 11-19.

[28] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*NETRU: A Non-Commutative and Secure Variant of CTRU Cryptosystem*," The ISC international journal of information security (IseCure), (2018), 10, 1, 1-9.

[29] A.H. Karbasi and R.E. Atani, "*Application of dominating sets in wireless sensor networks*," Int. J. Security and its Application, (2013), 7, 4.

[30] A.H. Karbasi and R.E. Atani. "*Projective plane-based key pre-distribution by key copying and exchanging based on connected dominating set in distributed wireless sensor networks*," International Journal of Information and Communication Technology, (2016), 9, 4, 438-462.

[31] S. Tahouri, R.E. Atani, A.H. Karbasi, and Y. Deldjou, "*Application of connected dominating sets in wildfire detection based on wireless sensor networks*," International Journal of Information Technology, Communications and Convergence, (2015), 3, 2, 139-160.