International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 08 - Issue 09 || September 2022 || PP. 01-16

On the High Dimensional RSA Algorithm--- A Public Key Cryptosystem Based on Lattice and Algebraic Number Theory

Zhiyong Zheng[a], Fengxia Liu[b*], Man Chen[c]
[a,c]*Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Renmin University of China, Beijing, 100872, P. R. China*
Institute of Artificial Intelligence, Beihang University Beijing, 100083, P. R. China
**Corresponding author E-mail addresses: shunliliu@buaa.edu.cn*

Abstract: The most known of public key cryptosystem was introduced in 1978 by Rivest, Shamir and Adleman[19] and now called the RSA public key cryptosystem in their honor. Later, a few authors gave a simply extension of RSA over algebraic numbers field(see [20]-[22]), but they require that the ring of algebraic integers is Euclidean ring, this requirement is much more stronger than the class number one condition. In this paper, we introduce a high dimensional form of RSA by making use of the ring of algebraic integers of an algebraic number field and the lattice theory. We give an attainable algorithm (see Algorithm I below) of which is significant both from the theoretical and practical point of view. Our main purpose in this paper is to show that the high dimensional RSA is a lattice based on public key cryptosystem indeed, of which would be considered as a new number in the family of post-quantum cryptography(see [17] and [18]). On the other hand, we give a matrix expression for any algebraic number fields (see Theorem 2.7 below), which is a new result even in the sense of classical algebraic number theory.

Keywords: RSA, The Ring of Algebraic Integers, Ideal Matrix, Ideal Lattice, HNF Basis
CCS: D.4.6; H.5; F.2.1

1 Introduction

Let $Q, \mathsf{R}, \mathsf{C}$ be the rational numbers field, real numbers field, and complex numbers field respectively, Z be the integers ring. Let $E \subset \mathsf{C}$ be an algebraic numbers field of degree n, $R \subset E$ be the ring of algebraic integers of E. Suppose that $A \subset R$ is a non-zero ideal(all ideals in this paper are non-zero), then the factor ring R/A is a finite ring, we denote by $N(A)$ the number of elements of R/A, which is called the norm of A, and denote by $\varphi(A)$ the number of invertible elements of R/A, which is called the Euler totient function of A. For any $\alpha \in R,$ the principal ideal generated by α is denoted by αR, then α is an invertible element of R/A if and only if $(\alpha R, A) = 1.$ It is known (see Theorem 1.19 of [16])that

$$\varphi(A) = N(A)\prod_{P|A}(1-\frac{1}{N(P)}) \tag{1.1}$$

where the product is extended over all prime ideals P dividing A. Moreover, if $\alpha \in R$ and $(\alpha R, A) = 1,$ then

$$\alpha^{\varphi(A)} \equiv 1(\text{mod } A). \tag{1.2}$$

To generalize that RSA to arbitrary algebraic number fields E, we first show that the following assertion.

Theorem 1.1 *Let P_1 and P_2 be two distinct prime ideals of R and $A = P_1P_2$, then for any $\alpha \in R$ and integer $k \geq 0,$ we have*

$$\alpha^{k\varphi(A)+1} \equiv \alpha(mod\ A). \tag{1.3}$$

Proof. Let $\alpha \in R.$ If $(\alpha R, A) = 1,$ then (1.3) follows directly from (1.2). If $(\alpha R, A) = A,$ then $\alpha R \subset A$ and $\alpha \in A,$ (1.3) is trivial. Thus, we only consider the cases of $(\alpha R, A) = P_1$ and $(\alpha R, A) = P_2$.

If $(\alpha R, A) = P_1$, then $(\alpha R, P_2) = 1$, by (1.2) we have

$$\alpha^{\varphi(P_2)} \equiv 1 (\text{mod } P_2).$$

It follows that

$$\alpha^{k\varphi(A)} \equiv 1 (\text{mod } P_2), \ \forall k \in Z, \ k \geq 0.$$

Therefore, there exists an element $\beta \in P_2$ such that

$$\alpha^{k\varphi(A)} = 1 + \beta.$$

We thus have

$$\alpha^{k\varphi(A)+1} = \alpha + \alpha\beta, \text{ and } \alpha^{k\varphi(A)+1} \equiv \alpha (\text{mod } A),$$

since $\alpha\beta \in A$. The same reason gives (1.3) when $(\alpha R, A) = P_2$.

According to Theorem 1.1, one can easily extend the classical RSA over an algebraic number field as follows(also see [20] , but it does not give the proof of (1.3)).

	RSA in the Ring of Algebraic Integers
• **Parameters:**	$n \geq 1$ is a positive integer, E/Q is an algebraic numbers field of
	degree n, $R \subset E$ is the ring of algebraic integers of E. P_1 and P_2
	are two prime ideals of R, $A = P_1P_2$, R/A is the factor ring,
	S is a set of coset representatives of R/A, $\varphi(A)$ is the Euler
	function of A, $1 \leq e < \varphi(A)$ and $1 \leq d < \varphi(A)$ are two positive
	integers such that $ed \equiv 1 (\text{mod } \varphi(A))$.
• **Public keys:**	The ideal A and positive integer e are the public keys.
• **Private keys:**	The prime ideals P_1, P_2 and the positive integer d are the
	private keys.
• **Encryptions:**	For any input message $\alpha \in S$, the ciphertext c is $c \equiv \alpha^e (\text{mod } A)$.
• **Decryption:**	$c^d \equiv \alpha^{ed} \equiv \alpha (\text{mod } A)$, one can find plaintext α from c in S.

Table 1: RSA in the Ring of Algebraic Integers

Obviously, if $n = 1$, the above algorithm is the ordinary RSA. However, it is difficult to find the prime ideals in R and to construct a set of coset representatives of R/A yet. In [20], the author supposed the ring R is Euclidean ring, so that S can be constructed by Euclidean algorithm in R. The simplest way is to select an prime element α in R, so that the principal ideal αR is a prime ideal. In algorithm I, we would precisely construct a set of coset representatives for the factor ring R/A by the lattice theory. Here we give an approximately construction of the set of coset representatives for factor ring R/A.

If $P \subset R$ is a prime ideal, then $P \cap Z = pZ$, where $p \in Z$ is a rational prime number. Since R/P is a finite field and $Z/(pZ) \subset R/P$, thus $N(P) = p^f$, where $f(1 \leq f \leq n)$ is called the degree of P. We write $pR = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$, where $P = P_1$ and P_i are distinct prime ideals, e_i is called the ramification index of P_i. There exists a remarkable relation among ramification indexes and degrees (see Theorem 3 of page 181 of [10])

$$\sum_{i=1}^{g} e_i f_i = n. \tag{1.4}$$

Let $\{\alpha_1, \alpha_2, \cdots \alpha_n\} \subset R$ be an integral basis for $E/Q, A = P_1P_2$. Suppose that $P_1 \cap Z = pZ$ and $P_2 \cap Z = qZ$, then $A \cap Z = pqZ$, where p and q are two distinct rational prime numbers.

Lemma 1.2
Let

$$S_1 = \left\{ \sum_{i=1}^{n} a_i \alpha_i \mid 0 \le a_i < pq,\ a_i \in \mathbb{Z}, 1 \le i \le n \right\}. \tag{1.5}$$

Then S_1 covers a set of coset representatives of R/A. Moreover, if the degrees of P_1 and P_2 are n, then S_1 is precisely an set of coset representatives of R/A.

Proof. Since $A = P_1 P_2$, $P_1 \cap \mathbb{Z} = p\mathbb{Z}$ and $P_2 \cap \mathbb{Z} = q\mathbb{Z}$, we have $pqR \subset A$, thus R/pqR maps onto R/A. To prove the first assertion, it is enough to show that S_1 is a set of coset representatives of R/pqR. Since $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ is an integral basis and

$$R = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n.$$

Suppose that $\alpha = \sum_{i=1}^{n} m_i \alpha_i \in R$, write $m_i = a_i pq + r_i$, where $0 \le r_i < pq$. Clearly

$$\alpha \equiv \sum_{i=1}^{n} r_i \alpha_i (\text{mod } pqR).$$

Thus every coset of pqR contains an element of S_1. If $\sum_{i=1}^{n} r_i \alpha_i = \sum_{i=1}^{n} r_i' \alpha_i$ are in S_1 and in the same coset mod pqR, then

$$\sum_{i=1}^{n} (r_i - r_i^{'}) \alpha_i \equiv 0 (\text{mod } \ pqR).$$

Since α_i are linearly independent, it follows that

$$r_i \equiv r_i^{'} (\text{mod } \ pq) \text{ and } r_i = r_i^{'},\ 1 \le i \le n.$$

Next, suppose that the degrees of P_1 and P_2 are n, then $N(P_1) = p^n$ and $N(P_2) = q^n$, by (1.4) we thus have $P_1 = pR$, $P_2 = qR$ and $A = pqR$. The second assertion follows immediately.

If one replaces S by S_1 in Table 1, then the successful probability of decryption is

$$N(A)/p^n q^n = p^{f_1 - n} q^{f_2 - n}, \tag{1.6}$$

where f_1 and f_2 are the degrees of P_1 and P_2 respectively.

We note that $f_1 = f_2 = n$ if and only if $P_1 = pR$ and $P_2 = qR$, in this special case, we may give a numerical explanation. It is easy to see that

$$\varphi(A) = \varphi(pR)\varphi(qR) = (p^n - 1)(q^n - 1).$$

By Theorem 1.1, for any $a \in \mathbb{Z}$, we have

$$a^{k(p^n - 1)(q^n - 1) + 1} \equiv a (\text{mod } pq),\ k \in \mathbb{Z},\ k \ge 0. \tag{1.7}$$

Since S_1 is a set of coset representatives of R/A, $\alpha = \sum_{i=1}^{n} a_i \alpha_i \in S_1$, We may regard α as a vector $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}_{pq}^n$. Let $m = pq$, $1 \le e < (p^n - 1)(q^n - 1)$ and $1d < (p^n - 1)(q^n - 1)$ such that

$$ed \equiv 1 (\text{mod } \ (p^n - 1)(q^n - 1)).$$

Then for every input message $\alpha = (a_1, a_2, \cdots, a_n)$, we use the public key (m, e) and private key (p, q, d) to encryption and decryption for each a_i in order, obviously, this is the algorithms given by [20], we consider these algorithms are just a simply repeat of RSA.

The main purpose of this paper is to show that the high dimensional form of RSA algorithm is a lattice based on cryptosystem in general. To do this, we first establish a relationship between an algebraic number field

E and the Euclidean space Q^n. Let R^n be the Euclidean space of which is a linear space over R with the Euclidean norm $|x|$,

$$|x| = \left(\sum_{i=1}^{n} x_i^2\right)^{\frac{1}{2}}, \text{ where } x' = (x_1, x_2, \cdots, x_n) \in \mathsf{R}^n. \tag{1.8}$$

We use the column natation for vector in R^n, and x' is the transpose of x, which is called a row vector in R^n. $Q^n \subset \mathsf{R}^n$ is a subspace of R^n.

Without loss of generality, an algebraic number field E of degree n may express as $E = Q(\theta)$, where θ is an algebraic integer of degree n and $Q(\theta)$ is the field generated by θ over Q. Let $\phi(x)$ be the minimal polynomial of θ,

$$\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in \mathsf{Z}[x], \tag{1.9}$$

where all $\phi_i \in \mathsf{Z}$. It is known that

$$E = Q[\theta] = \left\{\sum_{i=0}^{n-1} a_i \theta^i \mid a_i \in Q\right\}. \tag{1.10}$$

We define an one to one correspondence between E and Q^n by τ:

$$\alpha = \sum_{i=0}^{n-1} a_i \theta^i \in E \xrightarrow{\tau} \overline{\alpha} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in Q^n \tag{1.11}$$

and write $\tau(\alpha) = \overline{\alpha}$ or $\alpha \xrightarrow{\tau} \overline{\alpha}$. In fact τ is a homomorphism of additive group from E to Q^n, because of $\tau(a\alpha) = a\tau(\alpha)$ for all $a \in \mathsf{Q}$.

As usual, the trace and norm mappings from E to Q are denoted by

$$tr(\alpha) = tr_{E/Q}(\alpha), \text{ and } N(\alpha) = N_{E/Q}(\alpha).$$

It is known (see corollary of page 58 of [16]) that

$$N(\alpha R) = |N(\alpha)|, \quad \forall \alpha \in R. \tag{1.12}$$

A full rank lattice L is a discrete addition subgroup of R^n, the equivalent expression for L is (See [13] and [24])

$$L = L(B) = \{Bx \mid x \in \mathsf{Z}^n\}, \tag{1.13}$$

where $B = [\overline{\beta}_1, \overline{\beta}_2, \cdots, \overline{\beta}_n]_{n\times n} \in \mathsf{R}^{n\times n}$ is an invertible matrix of $n \times n$ dimension, B is called a generated matrix of L. If $L \subset Q^n$, we call L a rational lattice, if $L \subset \mathsf{Z}^n$, we call L an integer lattice. It is not difficult to see that every ideal of R corresponds an rational lattice, we have

Lemma 1.3 *Let $A \subset R$ be an ideal and $A \neq 0$, then $\tau(A)$ is a rational lattice.*

Proof. Let $\{\beta_1, \beta_2, \cdots, \beta_n\} \subset A$ be an integral basis for E/Q, one has

$$A = \mathsf{Z}\beta_1 + \mathsf{Z}\beta_2 + \cdots + \mathsf{Z}\beta_n.$$

It follows that

$$\tau(A) = \mathsf{Z}\overline{\beta}_1 + \mathsf{Z}\overline{\beta}_2 + \cdots + \mathsf{Z}\overline{\beta}_n,$$

where $\overline{\beta}_i = \tau(\beta_i) \in Q^n$. Let $B = [\overline{\beta}_1, \overline{\beta}_2, \cdots, \overline{\beta}_n]$, since $\{\beta_1, \beta_2, \cdots, \beta_n\}$ is linearly independent over Q, thus B is an invertible matrix, and we have

$$\tau(A) = L(B) = \{Bx \mid x \in \mathsf{Z}^n\}.$$

The lemma follows at once.

Let $L \subset Q^n$ is a rational lattice, of which be corresponded by an ideal A in E for some suitable algebraic number field E, we call L an ideal lattice. Ideal lattice was first introduced by Lyubashevsky and Miccancio in [11] in the case of integer lattice, here we generalize this notation to the case of rational lattices. More detail discussion about ideal lattice, we refer to [24].

To give an attainable algorithm for high dimensional RSA, we require the following NC-property for the algebraic number field E.

$$\text{NC}-\text{property}: \qquad E = Q(\theta) \quad \text{and} \quad R = \mathsf{Z}[\theta], \tag{1.14}$$

where

$$\mathsf{Z}[\theta] = \{\sum_{i=0}^{n-1} a_i \theta^i \mid a_i \in \mathsf{Z}, 1 \le i \le n\}. \tag{1.15}$$

Some of well-known algebraic number fields satisfy the NC-property, we list a few as follows.

Algebraic Number Fields with NC – property
• Quadratic Fields(see Proposition 13.1.1 of [10]): $E = Q(\sqrt{d})$, where $d \in \mathsf{Z}$ is a square-free integer and $d = 2,3 (\mathrm{mod}\ 4)$.
• Cyclotemic Fields (see theorem 2.6 of [23]): $E = Q(\xi_n)$, where $\xi_n = e^{2\pi i/n}$ is a primitive n-th root of unity.
• Totally Real Algebraic Number Fields (see Proposition 2.16 of [23]): $E = Q(\xi_n + \xi_n^{-1})$, and $E \subset \mathsf{R}$ is the maximal real subfield of $Q(\xi_n)$.

Table 2: Algebraic Number Fields with NC-property

2 Ideal Matrices

Suppose that θ is an algebraic integer of degree n, $\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0 \in \mathsf{Z}[x]$ is the minimal polynomial of θ, thus $\phi(x)$ is irreducible. Let $\theta = \theta_0, \theta_1, \theta_2, \cdots, \theta_{n-1}$ be n different roots of $\phi(x)$, the Vandermonde matrix of $\phi(x)$ is defined by

$$V = V_\phi = \left[\theta_j^i\right]_{0 \le i, j \le n-1}, \text{ and } \Delta = \det(V_\phi) \ne 0. \tag{2.1}$$

According to $\phi(x)$, we denote the rotation matrix or adjoint matrix (see page 116 of [12]) by

$$H = H_\phi = \begin{pmatrix} 0 & \cdots & 0 & \phi_0 \\ & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{pmatrix} \in \mathsf{Z}^{n \times n}, \tag{2.2}$$

where I_{n-1} is the unit matrix of $n-1$ dimension.

Definition 2.1 *An ideal matrix* $H^*(\overline{f})$ *generated by the input vector* $\overline{f} \in \mathsf{R}^n$ *is defined by*

$$H^*(\overline{f}) = \left[\overline{f}, H\overline{f}, \cdots, H^{n-1}\overline{f}\right]_{n \times n} \in \mathsf{R}^{n \times n} \tag{2.3}$$

and all ideal matrices are denoted by

$$M_{\mathsf{R}}^{*}=\left\{H^{*}(\overline{f})\mid \overline{f}\in \mathsf{R}^{n}\right\} \text{ and } M_{Q}^{*}=\left\{H^{*}(\overline{f})\mid \overline{f}\in Q^{n}\right\}. \tag{2.4}$$

Definition 2.2 *For any two vectors* $\overline{f}$ *and* $\overline{g}$ *in* R^{n}, *the* ϕ *-conventional product is defined by*

$$\overline{f}\otimes\overline{g}=H^{*}(\overline{f})\overline{g} \tag{2.5}$$

and the m-multi product is denoted by

$$\overline{f}^{\otimes m}=\overbrace{\overline{f}\otimes\overline{f}\otimes\cdots\otimes\overline{f}}^{m},\ m\in\mathsf{Z},\ m\geq 1. \tag{2.6}$$

Remark 2.1 *If* $\phi(x)=x^{n}-1$, *then* H_{ϕ} *is the classical circulant matrix (see [5]), conventional product with circulant matrix was first proposed by Hoffstein, Pipher and Silverman in [9], which plays a key role in their cryptosystem. In [25], we generalized this definition with more general rotation matrices.*

By (2.3), $H^{*}(\overline{f})=0$ is a zero matrix if and only if $\overline{f}=0$ is a zero vector, and $H^{*}(\overline{f}+\overline{g})=H^{*}(\overline{f})+H^{*}(\overline{g})$, then $H^{*}(\overline{f})=H^{*}(\overline{g})$ if and only if $\overline{f}=\overline{g}$. Thus we may regard $H^{*}:\mathsf{R}^{n}\to \mathrm{M}_{\mathsf{R}}^{*}$ as an one to one correspondence, which is also a homomorphism of Abel group.

The main aim of this subsection is to show the Q^{n} is a field under the ϕ-conventional product and M_{Q}^{*} is also a field under the ordinary additive and product of matrices, both of them are isomorphic to the algebraic number field $E=Q(\theta)$. To do this, we require some basic properties of the ideal matrices.

Let $\overline{e}_{1},\overline{e}_{2},\cdots,\overline{e}_{n}$ be the unit vectors of R^{n}, namely

$$\overline{e}_{1}=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\overline{e}_{2}=\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix},\cdots,\quad \overline{e}_{n}=\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}. \tag{2.7}$$

Lemma 2.2 *Let* τ *be defined by (1.11), then we have*

$$\begin{cases}\tau\left(\theta^{k}\right)=\overline{e}_{k+1},\ 0\leq k\leq n-1\\ H^{*}\left(\overline{e}_{k}\right)=H^{k-1},\ 1k\ n.\end{cases} \tag{2.8}$$

Proof. $\tau\left(\theta^{k}\right)=\overline{e}_{k+1}$ follows directly from the definition of τ. We use induction to prove $H^{*}\left(\overline{e}_{k}\right)=H^{k-1}$. It is easy to see that $H^{*}\left(\overline{e}_{1}\right)=I_{n}$, the unit matrix of n dimension. Suppose that $H^{*}\left(\overline{e}_{k-1}\right)=H^{k-2}$, for $k\geq 2$, note that $\overline{e}_{k}=H\overline{e}_{k-1}$, it follows that

$$\begin{aligned}H^{*}\left(\overline{e}_{k}\right)&=\left[H\overline{e}_{k-1},H^{2}\overline{e}_{k-1},\cdots,H^{n}\overline{e}_{k-1}\right]\\&=H\left[\overline{e}_{k-1},H\overline{e}_{k-1},\cdots,H^{n-1}\overline{e}_{k-1}\right]\\&=HH^{*}(\overline{e}_{k-1})=HH^{k-2}=H^{k-1}.\end{aligned}$$

The lemma follows immediately.

Since $\phi(x)$ is the characteristic polynomial of H, by Hamilton-Cayley theorem, we have

$$\phi(H)=0,\ \text{or } H^{n}=\phi_{0}+\phi_{1}H+\cdots+\phi_{n-1}H^{n-1}. \tag{2.9}$$

Therefore, all the rotation matrices $H^k(k \geq 0)$ are the ideal matrices, especially, the unit matrix $I_n = H^*(\bar{e}_1)$ is an ideal matrix.

Let $\mathsf{R}[x]$ be the polynomials ring and $\mathsf{R}(x)/\langle\phi(x)\rangle$ be the quotient ring, where $\langle\phi(x)\rangle$ is the principal ideal generated by $\phi(x)$ in $\mathsf{R}[x]$. We establish an one to one correspondence t between R^n and $\mathsf{R}[x]/\langle\phi(x)\rangle$ by

$$\bar{f} = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathsf{R}^n \xrightarrow{t} f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \mathsf{R}[x]/\langle\phi(x)\rangle \tag{2.10}$$

and write $t(\bar{f}) = f(x)$, or $t^{-1}(f(x)) = \bar{f}$.

Lemma 2.3 *For any $\bar{f} \in \mathsf{R}^n$, the ideal matrix $H^*(\bar{f})$ is given by*

$$H^*(\bar{f}) = f(H) = f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1}. \tag{2.11}$$

Moreover, if $F(x) \in \mathsf{R}[x]$ and $F(x) \equiv f(x) (\mathrm{mod}\ \phi(x))$, then $f(H) = F(H)$.

Proof. Writing $\bar{f} = f_0\bar{e}_1 + f_1\bar{e}_2 + \cdots + f_{n-1}\bar{e}_n$, by Lemma 2.2, we have

$$\begin{aligned} H^*(\bar{f}) &= f_0 H^*(\bar{e}_1) + f_1 H^*(\bar{e}_2) + \cdots + f_{n-1}H^*(\bar{e}_n) \\ &= f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1} = f(H). \end{aligned}$$

Suppose that $F(x) \equiv f(x) (\mathrm{mod}\ \phi(x))$, by (2.9) we have $f(H) = F(H)$ immediately.

Lemma 2.4 *Let $\bar{f}$ and $\bar{g}$ be two vectors in R^n, and $f(x), g(x)$ be the corresponding polynomials respectively, then we have*

$$t(\bar{f} \otimes \bar{g}) \equiv f(x)g(x) (\mathrm{mod}\ \ \phi(x)). \tag{2.12}$$

Proof. Since t is a bijection, it is suffice to show that

$$t^{-1}(f(x)g(x)) = \bar{f} \otimes \bar{g}. \tag{2.13}$$

Let $g(x) = g_0 + g_1(x) + \cdots + g_{n-1}x^{n-1} \in \mathsf{R}[x]/\langle\phi(x)\rangle$, then

$$\begin{aligned} xg(x) &= g_0 x + \cdots + g_{n-1}x^n \\ &= g_{n-1}\phi_0 + (g_0 + \phi_1 g_{n-1})x + \cdots + (g_{n-2} + \phi_{n-1}g_{n-1})x^{n-1}. \end{aligned}$$

It follows that

$$t^{-1}(xg(x)) = Ht^{-1}(g(x)) = H\bar{g}.$$

More general, we have

$$t^{-1}\left(x^k g(x)\right) = H^k t^{-1}(g(x)) = H^k \bar{g}, \quad 0 \leq k \leq n-1. \tag{2.14}$$

Let $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$, then

$$t^{-1}(f(x)g(x)) = \sum_{k=0}^{n-1} f_k t^{-1}\left(x^k g(x)\right) = \sum_{k=0}^{n-1} f_k H^k \bar{g} = H^*(\bar{f})\bar{g} = \bar{f} \otimes \bar{g}.$$

The lemma follows immediately.

Lemma 2.5 *For any two vectors* $\overline{f} = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathsf{R}^n$, $\overline{g} = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} \in \mathsf{R}^n$, *we have the following properties for ideal matrices:*

(i) $H^*(\overline{f})H^*(\overline{g}) = H^*(\overline{g})H^*(\overline{f})$;

(ii) $H^*(\overline{f})H^*(\overline{g}) = H^*(H^*(\overline{f})\overline{g})$;

(iiii) $H^*(\overline{f}) = V_\phi^{-1} diag\{f(\theta_0), f(\theta_1), \cdots, f(\theta_{n-1})\}V_\phi$;

(iv) $det\left(H^*(\overline{f})\right) = \prod_{i=0}^{n-1} f(\theta_i)$;

(v) If $\overline{f} \in Q^n$, $\overline{f} \neq 0$, then $H^*(\overline{f})$ is an invertible matrix and

$$\left(H^*(\overline{f})\right)^{-1} = H^*(\overline{u}),$$

where $u(x) \in Q[x]$ is the unique polynomial such that $u(x)f(x) \equiv 1 (\mathrm{mod}\ \phi(x))$ in $Q[x]$.

Proof. By Lemma 2.3, we have

$$H^*(\overline{f})H^*(\overline{g}) = f(H)g(H) = g(H)f(H) = H^*(\overline{g})H^*(\overline{f}).$$

To prove (ii), we write $H^*(\overline{f})\overline{g} = \overline{f} \otimes \overline{g}$, it follows that

$$H^*\left(H^*(\overline{f})\overline{g}\right) = H^*(\overline{f} \otimes \overline{g}) = f(H)g(H) = H^*(\overline{f}) \cdot H^*(\overline{g}).$$

By theorem 3.5 of [5], we have

$$H = V_\phi^{-1} diag\{\theta_0, \theta_1, \cdots, \theta_{n-1}\}V_\phi \tag{2.15}$$

It follows that

$$H^*(\overline{f}) = f(H) = V_\phi^{-1} diag\{f(\theta_0), f(\theta_1), \cdots, f(\theta_{n-1})\}V_\phi.$$

Since $diag\{f(\theta_0), f(\theta_1), \cdots, f(\theta_{n-1})\}$ is a diagonal matrix, we have

$$det\left(H^*(\overline{f})\right) = det\left(diag\{f(\theta_0), f(\theta_1), \cdots, f(\theta_{n-1})\}\right) = \prod_{i=0}^{n-1} f(\theta_i).$$

To show that the last assertion, since $\overline{f} \in Q^n, \overline{f} \neq 0$, and $\phi(x)$ is an irreducible polynomial, thus we have $(f(x), \phi(x)) = 1$ in $Q[x]$, There are $u(x) \in Q[x]$ and $v(x) \in Q[x]$ such that

$$u(x)f(x) + v(x)\phi(x) = 1.$$

By (2.14) and noting that $t^{-1}(1) = \overline{e}_1 \in \mathsf{R}^n$, we have $\overline{u} \otimes \overline{f} = \overline{e}_1$. It follows that

$$H^*(\overline{u}) \cdot H^*(\overline{f}) = H^*(\overline{e}_1) = I_n.$$

We complete the proof of Lemma.

Next, we discuss the algebraic number field $E = Q(\theta)$, recall τ is an one to one correspondence between E and Q^n.

Lemma 2.6 *Far any two elements* α *and* β *in* E, *we have*

$$\tau(\alpha\beta) = \tau(\alpha) \otimes \tau(\beta) = \overline{\alpha} \otimes \overline{\beta}. \tag{2.16}$$

Proof. Let $\beta = \beta_0 + \beta_1\theta + \cdots + \beta_{n-1}\theta^{n-1}$, where $\beta_i \in Q$, it is easily seen that

$$\theta\beta = \phi_0\beta_{n-1} + (\beta_0 + \phi_1\beta_{n-1})\theta + \cdots + (\beta_{n-2} + \phi_{n-1}\beta_{n-1})\theta^{n-1},$$

thus we have $\tau(\theta\beta) = H\tau(\beta) = H\overline{\beta}$, and

$$\tau(\theta^k\beta) = H^k\tau(\beta) = H^k\overline{\beta}, \quad 0 \le k \le n-1. \tag{2.17}$$

Let $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1}$, by lemma 2.3, we have

$$\tau(\alpha\beta) = \sum_{k=0}^{n-1}\alpha_k\tau(\theta^k\beta) = \sum_{k=0}^{n-1}\alpha_k H^k\overline{\beta} = H^*(\overline{\alpha})\overline{\beta} = \overline{\alpha}\otimes\overline{\beta},$$

the lemma follows immediately.

Let $A = (a_{ij})_{n\times n}$ be a square matrix, the trace of A is defined by $Tr(A) = \sum_{i=1}^{n} a_{ii}$ as usual. The main result of this subsection is the following theorem.

Theorem 2.7 *Let $E = Q(\theta)$ be an algebraic number field of degree n, $\phi(x) \in Z[x]$ be the minimal polynomial of θ. Then the linear space Q^n is a field under the ϕ-conventional product, and all of ideal matrices M_Q^* generated by rational vectors is also a field with the ordinary additive and product of matrices. Both of them are isomorphic to E, namely*

$$E \cong Q^n \cong M_Q^*. \tag{2.18}$$

Moreover, let $\alpha \in E$, $tr(\alpha)$ and $N(\alpha)$ be the trace and norm of α, then we have

$$tr(\alpha) = Tr(H^*(\overline{\alpha})), \text{ and } N(\alpha) = det(H^*(\overline{\alpha})). \tag{2.19}$$

Proof. $\tau : E \to Q^n$ given by (1.11), it is clearly that

$$\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta), \text{ and } \tau(\alpha\beta) = \tau(\alpha)\otimes\tau(\beta).$$

Thus Q^n is a field under the ϕ-conventional product and $E \cong Q^n$. By lemma 2.5, we have

$$H^*(\overline{\alpha}+\overline{\beta}) = H^*(\overline{\alpha}) + H^*(\overline{\beta}) \text{ and } H^*(\overline{\alpha}\otimes\overline{\beta}) = H^*(\overline{\alpha})H^*(\overline{\beta}),$$

thus M_Q^* is also a field and $E \cong Q^n \cong M_Q^*$.

The main difficult is to prove (2.19). We observe that θ induces a linear transformation of E/Q by $\alpha \to \theta\alpha$, and the matrix of this linear transformation under basis $\{1, \theta, \theta^2, \cdots, \theta^{n-1}\}$ is just H, namely

$$\theta(1, \theta, \theta^2, \cdots, \theta^{n-1}) = (1, \theta, \theta^2, \cdots, \theta^{n-1})H.$$

By the definition of trace, we have

$$tr(\theta) = Tr(H), \text{ and } tr(\theta^k) = Tr(H^k), \quad ,1 \le k \le n-1.$$

Let $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1} \in E$, it follows that

$$tr(\alpha) = \sum_{k=0}^{n-1}\alpha_i tr(\theta^k) = \sum_{i=0}^{n-1}\alpha_i Tr(H^k) = Tr\left(\sum_{k=0}^{n-1}\alpha_i H^k\right) = Tr(H^*(\overline{\alpha})).$$

To show that conclusion on the norm, let $\alpha^{(i)}(0 \le i \le n-1)$ be the n conjugations of α in the smallest normal extension of Q containing E, where $\alpha^{(0)} = \alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1}$. It is easily seen that

$$\alpha^{(i)} = \sum_{k=0}^{n-1}\alpha_k\theta_i^k, \text{ where } \theta_0 = \theta \text{ and } 0 \le i \le n-1.$$

By property (iii) of lemma 2.5, we have

$$N(\alpha) = \prod_{i=0}^{n-1}\alpha^{(i)} = \prod_{i=0}^{n-1}\alpha(\theta_i) = det(H^*(\overline{\alpha})).$$

We complete the proof of Theorem 2.7.

The cyclic lattice in R^n was introduced by Micciancio in [14], (also see [24]), which plays an important role in Ajtai's construction of collision resistant Hash function(see [1]). As an application, we show that every ideal in an algebraic number field corresponds to a cyclic lattice:

Corollary 2.8 *Let* $A \subset R$ *be an ideal and* $A \neq 0$, *then* $\tau(A) \subset Q^n$ *is a cyclic lattice.*

Proof. Suppose that $\alpha \in A$. Since $\theta \in R$, then $\theta\alpha \in A$. By (2.16), we have

$$\tau(\theta\alpha) = H\overline{\alpha} \in \tau(A).$$

Thus $\tau(A)$ is a cyclic lattice.

3 High Dimensional RSA

In this section, we give an attainable algorithm for the high dimensional RSA by making use of lattice theory, this algorithm is significant both from the theoretical and practical point of view. Suppose that the algebraic numbers field E satisfying the NC-property, then $R = \mathsf{Z}[\theta]$ is the ring of algebraic integers of E, the restriction of correspondence τ gives a ring isomorphism from R to Z^n. Let $\mathsf{Z}(x)$ be the ring of integer coefficients polynomials and $(\phi(x))$ be the principal ideal generated by $\phi(x)$ in $\mathsf{Z}(x)$, it is easy to see that $R \cong \mathsf{Z}[x]/(\phi(x))$. Let M_{Z}^* be the set of ideal matrices generated by an integral vector, i.e.

$$M_{\mathsf{Z}}^* = \left\{H^*(\overline{f}) \mid \overline{f} \in \mathsf{Z}^n\right\}. \tag{3.1}$$

Then the following four rings are isomorphic from each other

$$\mathsf{Z}[x]/(\phi(x)) \cong R \cong \mathsf{Z}^n \cong M_{\mathsf{Z}}^*. \tag{3.2}$$

For any polynomial $\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} \in \mathsf{Z}[x]/(\phi(x))$, the corresponding algebraic integer is $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1} \in R$, we write this isomorphism by

$$\alpha(x) \to \alpha \xrightarrow{\tau} \overline{\alpha} \xrightarrow{H^*} H^*(\alpha). \tag{3.3}$$

A ϕ-ideal lattice means an integer lattice of which corresponds an ideal of $\mathsf{Z}(x)/(\phi(x))$, it was first introduced by Lyubashevsky and Micciancio in (see also [24]), which also plays a key role in Gentry's construction for the full homomorphic cryptosystem (see [7]), Fluckiger and Suarez in [6] extended this definition to total real number field. .

Lemma 3.1 *Let* E *be an algebraic numbers field with NC- property,* $R = \mathsf{Z}[\theta]$ *be the ring of algebraic integers of* E. *Then there is an one to one correspondence between ideals of* R *and the* ϕ*-ideal lattices. Moreover, if* $\alpha \in R$, *then we have*

$$\tau(\alpha R) = L\left(H^*(\overline{\alpha})\right). \tag{3.4}$$

In general, suppose that $A \subset R$ is an ideal and $A \neq 0$, then there exists two elements α and β in A such that

$$\tau(A) = L\left(H^*(\overline{\alpha})\right) + L\left(H^*(\overline{\beta})\right). \tag{3.5}$$

Proof. Since there is an one to one correspondence between the ϕ-ideal lattices and the ideals of $\mathsf{Z}[x]/(\phi(x))$ (See Corollary of [24]), by (3.2), the first assertion follows immediately. Let $\alpha \in R$, then $\alpha R = \{\alpha x \mid x \in R\}$, by lemma 2.6 we have

$$\tau(\alpha x) = H^*(\alpha)\bar{x}, \text{ where} \bar{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \in \mathsf{Z}^n.$$

It follows what

$$\tau(\alpha R) = \left\{H^*(\alpha)\bar{x} \mid \bar{x} \in \mathsf{Z}^n\right\} = L\left(H^*(\bar{\alpha})\right).$$

To prove (3.5), it is known that any an ideal of R is generated by at most two elements (see corollary 5 of page 11 of [16]), namely, $A = \alpha R + \beta R$, then we have

$$\tau(A) = \tau(\alpha R) + \tau(\beta R) = L\left(H^*(\bar{\alpha})\right) + L\left(H^*(\bar{\beta})\right).$$

To introduce an attainable algorithm for high dimensional RSA, we require some basic results from lattice theory. Let $L = L(B) \subset \mathsf{R}^n$ be a full-rank lattice, the determinant of L is defined by

$$d(L) = |\det(B)|. \tag{3.6}$$

Suppose that the generated matrix $B = [\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n], \bar{b}_i \in \mathsf{R}^n$ is the column vectors of B. Since $\{\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n\}$ is a basis for R^n, let $B^* = \{\bar{b}_1^*, \bar{b}_2^*, \cdots, \bar{b}_n^*\}$ be the corresponding orthogonal basis, where $\bar{b}_1^* = \bar{b}_1$, and $\bar{b}_i^*$ is obtained by Gram-Schmidt orthogonal process in order.

A basis B is called in Hermited Normal Form (HNF) if it is upper triangular, all elements on the diagonal are strictly positive, and any other elements b_{ij} satisfies $0 \le b_{ij} < b_{ii}$. It is easy to see that every integer lattice $L = L(B)$ has a unique basis in Hermited Normal Form, denoted by $HNF(L)$ (see Theorem 2.4.3 of [4]). Moreover, given any basis B for lattice L, $HNF(L)$ can be efficiently computed from B (see [15] and [4]).

Proposition 3.2 *Let $L = L(B)$ and $B = (b_{ij})_{n\times n}$ be the basis in HNF. Then the corresponding orthogonal basis B^* is a diagonal matrix, namely*

$$B^* = diag\{b_{11}, b_{22}, \cdots, b_{nn}\}. \tag{3.7}$$

Moreover, we have

$$d(L) = \prod_{i=1}^{n} b_{ii}. \tag{3.8}$$

Proof. See [15].

Let $L = L(B) \subset \mathsf{R}^n$ be a full-rank lattice, and $B^* = [\bar{b}_1^*, \bar{b}_2^*, \cdots, \bar{b}_n^*]$ be the corresponding orthogonal basis, the orthogonal parallelepiped $F\left(B^*\right)$ is defined by

$$F(B^*) = \left\{\sum_{i=1}^{n} x_i \bar{b}_i^* \mid 0 \le x_i < 1 \text{ and } x_i \in \mathsf{R}\right\}. \tag{3.9}$$

Proposition 3.3 *Let $L = L(B) \subset \mathsf{Z}^n$ be an integer lattice, $B = HNF(L)$ be the basis in HNF and $B^* = diag\{b_{11}, b_{22}, \cdots, b_{nn}\}$ be the corresponding orthogonal basis, $F\left(B^*\right)$ is the orthogonal*

parallelepiped given by (3.9), then S *is a set of coset representatives for the quotient group* Z^n/L *, where*

$$S = F(B^*) \cap Z^n = \{x' = (x_1, x_2, \cdots, x_n) \mid \forall x_i \in Z \text{ and } 0 \le x_1 < b_{ii}\}.$$

Proof. See section 4.1 of [15].

Now, we return to the algebraic numbers field $E = Q[\theta]$ (with NC-property). Let $\alpha, \beta \in R$ be two algebraic integers, by Lemma 3.1, the principal ideal αR corresponds to the minimal ϕ-ideal lattice $L(H^*(\overline{\alpha}))$. Thus $A = (\alpha R)(\beta R) = \alpha\beta R$ corresponds to $L(H^*(\overline{\alpha} \otimes \beta))$.

Definition 3.4

For given $\alpha, \beta \in R$, $\tau(\alpha) = \overline{\alpha}$ and $\tau(\beta) = \overline{\beta}$, we denote the lattice $L_{\alpha,\beta}$ by

$$L_{\alpha,\beta} = L(H^*(\overline{\alpha} \otimes \overline{\beta})). \qquad (3.10)$$

The HNF basis of $L_{\alpha,\beta}$ is denoted by $B_{\alpha,\beta}$ and the corresponding orthogonal basis is denoted by

$$B^*_{\alpha,\beta} = diag\{b_1, b_2, \cdots, b_n\}, \qquad (3.11)$$

where $b_i \in Z$ and $b_i \ge 1$. The parallelepiped is given by

$$S_{\alpha,\beta} = \{(x_1, x_2, \cdots, x_n) \in Z^n \mid x_i \in Z \text{ and } 0 \le x_i < b_i\}. \qquad (3.12)$$

Lemma 3.5 *Let* $\alpha \in R, \beta \in R$ *and* $A = \alpha\beta R$. *Then* $S_{\alpha,\beta}$ *given by (3.12) is corresponding to a set of coset representatives of the factor ring* R/A *in the algebraic numbers field* E *with NC-property.*

Proof. By Proposition 3.2, it is easy to see that

$$|S_{\alpha,\beta}| = \prod_{i=1}^{n} b_i = |det(H^*(\overline{\alpha} \otimes \overline{\beta}))| = |det(H^*(\overline{\alpha}))| \cdot |det(H^*(\overline{\beta}))| = d(L_{\alpha,\beta}).$$

By theorem 2.7 and (1.12), we have

$$N(A) = |N(\alpha \cdot \beta)| = |N(\alpha)| \cdot |N(\beta)| = |det(H^*(\overline{\alpha}))| \cdot |det(H^*(\overline{\beta}))| = d(L_{\alpha,\beta}).$$

It follows that $N(A) = |S_{\alpha,\beta}|$. Since E satisfies NC-property, if $\alpha \in R$, then $\overline{\alpha} = \tau(\alpha) \in Z^n$, hence $\alpha \equiv \beta (\text{mod } A)$ in R, if and only if

$$\overline{\alpha} \equiv \overline{\beta} (mod \ L_{\alpha,\beta}).$$

The lemma follows from Proposition 3.3 immediately.

The main result of this subsection is the following theorem.

Theorem 3.6 *Let* E *be an algebraic numbers field of degree* n *with NC-property,* $\alpha \in R, \beta \in R$ *be two distinct prime elements,* $A = \alpha\beta R$, *and* $L_{\alpha,\beta}$ *be the lattice given by (3.10). Then for any* $\overline{a} \in Z^n, k \in Z, k \ge 0$, *we have*

$$\overline{a}^{\otimes(k\varphi(\alpha,\beta)+1)} \equiv \overline{a} (\text{mod } L_{\alpha,\beta}), \qquad (3.13)$$

where

$$\varphi(\alpha,\beta)=\left(\left|det\left(H^*(\bar{\alpha})\right|-1\right)\left(\left|det\left(H^*(\bar{\beta})\right|-1\right). \tag{3.14}$$

Proof. Since E satisfies NC-property, $\bar{a}\in Z^n$, then $a=\tau^{-1}(\bar{a})\in R$. By Theorem 1.1 , we have

$$a^{k\varphi(A)+1}\equiv a(\text{mod } A).$$

It is easy to see that

$$\begin{aligned}\varphi(A)=\varphi(\alpha R)\varphi(\beta A) &= (N(\alpha R)-1)(N(\beta R)-1)\\ &=(|N(\alpha)|-1)(|N(\beta)|-1)\\ &=\left(\left|det\left(H^*(\bar{\alpha})\right|-1\right)\left(\left|det\left(H^*(\bar{\beta})\right|-1\right)\right.\\ &=\varphi(\alpha,\beta).\end{aligned}$$

By lemma 3.1, we have

$$\tau(A)=\tau(\alpha\beta R)=L\left(H^*(\bar{\alpha}\otimes\bar{\beta})\right)=L_{\alpha,\beta} \text{ and } \tau\left(a^{k\varphi(\alpha,\beta)+1}\right)=\bar{a}^{\otimes(k\varphi(\alpha,\beta)+1)}.$$

Therefore, (3.13) follows immediately.

According to the above theorem, we may describe an attainable algorithm for high dimensional RSA as follows.

Algorithm I: RSA in the Algebraic Numbers Field

$n\geq 1$ is a positive integer, E/Q is an algebraic numbers field with NC-property of degree n, $R\subset E$ is the ring of algebraic integers of E, $\alpha\in R$, $\beta\in R$ are two distinct prime elements of R, $A=\alpha\beta R$ is a principal ideal of R, $H^*(\bar{\alpha}\otimes\bar{\beta})$ is the ideal matrix corresponding to A, $L_{\alpha,\beta}=L\left(H^*(\bar{\alpha}\otimes\bar{\beta})\right)$ is the lattice generated by $H^*(\bar{\alpha}\otimes\bar{\beta})$, $B_{\alpha,\beta}=\text{HNF}\left(L_{\alpha,\beta}\right)$ is the basis of $L_{\alpha,\beta}$ in HNF,

$B^*_{\alpha,\beta}=diag\{b_1,b_2,\cdots,b_n\}$ is the corresponding orthogonal basis.

- **Parameters:** $\varphi(\alpha,\beta)=\left(\left|det\left(H^*(\bar{\alpha})\right|-1\right)\left(\left|det\left(H^*(\bar{\beta})\right|-1\right),$
  $S_{\alpha,\beta}=\{x'=(x_1,x_2,\cdots,x_n)\in Z^n\mid 0\leq x_i<b_i\}.\ 1\leq e<\varphi(\alpha,\beta),$
  $1\leq d<\varphi(\alpha,\beta),$ such that $ed\equiv 1(\text{mod } \varphi(\alpha,\beta))$.
- **Public keys:** The rotation matrix H, the lattice $L(B_{\alpha,\beta})=L_{\alpha,\beta}$ and the positive integer e are public keys.
- **Private keys:** Ideal matrices $H^*(\bar{\alpha}),H^*(\bar{\beta})$, the basis $H^*(\bar{\alpha}\otimes\bar{\beta})$ of $L_{\alpha,\beta}$ and positive integer d are private keys.
- **Encryption:** For any input message $\bar{a}\in S_{\alpha,\beta}$, the ciphertext $\bar{c}$ is given by $\bar{c}\equiv\bar{a}^{\otimes e}(mod\ \ L_{\alpha,\beta})$.
- **Decryption:** $\bar{c}^{\otimes d}\equiv\bar{a}^{\otimes de}\equiv\bar{a}^{\otimes(k\varphi(\alpha,\beta)+1)}\equiv\bar{a}(\text{mod } L_{\alpha,\beta})$. One can find the plaintext $\bar{a}$ from $\bar{c}$ in $S_{\alpha,\beta}$.

Table 3: Algorithm I

Remark 3.7 *If the class number* $h_E = 1$, *in other words,* R *is a UFD, then the prime elements is equivalent to irreducible elements in* R, *and one can find prime elements* α *from* $\alpha(x) \in Z[x]/(\phi(x))$ *and* $\alpha(x)$ *irreducible.*

4 Security and Example

The classical RSA public key cryptosystem is nowadays used in a wide variety of applications ranging from web browsers to smart cords. Since its initial publication in 1978, many researchers have tried to look for vulnerabilities in the system. Some clever attacks have been found (see [2] and [3]). However, none of the known attacks is devastating and the ordinary RSA system is still considered secure.

The security of high dimensional RSA depends on virtually factoring of an element of the algebraic integers ring R into product of of distinct prime elements. Factoring on R is much more complicate than factoring of a positive integer, none of efficient method is known up to day, thus we consider the high dimensional RSA almost absolutely secure.

To see the size of private keys, since $det\left(H^*(\overline{\alpha})\right) = N(\alpha)$, it may be extremely huge, for example, if $\alpha = p \in Z$, $\beta = q \in Z$ are prime numbers, then

$$det\left(H^*(\overline{\alpha})\right) = N(\alpha) = p^n, \quad det\left(H^*(\overline{\beta})\right) = q^n$$

and

$$\varphi(\alpha, \beta) = \left(p^n - 1\right)\left(q^n - 1\right),$$

which is much larger than pq, the later is the site of public key of the classical RSA cryptosystem.

The lattice based on cryptography have been intensively studied for past two decades. The GGH cryptosystem proposed by Goldreich, Goldwasser and Halevi in [8], which is perhaps the most intuitive encryption scheme based on lattices. The public key is a "bad" basis for a lattice, Micciancio proposed in [15] to use, as the public basis, the Hermite Normal Form $B = \text{HNF}(L)$. The private key of GGH is an exceptionally good basis for L. The security of GGH relies on the assumption that it is difficult to find a spacial basis for L from a known basis of L. In this sense, we regard the high dimensional RSA as secure as GGH/HNF cryptosystem at least.

Another number theoretic cryptosystem based on lattice is NTRUEncrypt. The public key cryptosystem NTRU proposed in 1996 by Hoffstein, Pipher and Silverman in [9], is the fastest known lattice based encryption scheme, although its description relies on arithmetic over polynomial quotient ring $Z[x]/\langle x^n - 1\rangle$, it was easily observed that it could be expressed as a lattice based on cryptosystem. NTRU uses a q-ary convolutional modular lattice(see [13] and [26]), its public key is also the HNF basis of L and the private key is a special basis of L containing two secrete polynomials $f(x)$ and $g(x)$. Obviously, our algorithm I is at least as hard as solving NTRUEncrypt.

Unfortunately, neither GGH nor NTRU is supported by a proof of security showing that breaking the cryptosystem is at least as hard as solving some underlying lattice problem; they are primarily practical proposals aimed at offering a concrete alternative to RSA or other number theoretic cryptosystems(see page 166 of [13]). However, the significance of this paper is to show that the real alternative of RSA is the high dimensional RSA we present here rather than GGH and NTRU.

Example 4.1 *Finally, we give an example and see how to work of the high dimensional RSA in a quadratic field. Let* $E = Q(\sqrt{d})$, $d \in Z$ *be a square-free integer and* $d \equiv 2,$ *or* $3 \bmod 4$, *thus* E *satisfies the NC-property. Let* δ_E *be the discriminant of* E, *it is known that* $\delta_E = 4d$ *(see Proposition 13.1.2 of [10]). Let* $p \in Z$ *be an odd prime satisfying the following condition*

$$p \nmid 4d, \text{ and } x^2 \equiv d \pmod{p} \text{ is not solvable in } Z. \tag{4.1}$$

By Proposition 13.1.3 of [10], we know that p is a prime element in E.

According to Algorithm I, we select two large primes p and q of which satisfying (4.1). Let $\alpha = p$ and $\beta = q$, then

$$\overline{\alpha} = \begin{pmatrix} p \\ 0 \end{pmatrix}, \overline{\beta} = \begin{pmatrix} q \\ 0 \end{pmatrix}, H^*(\overline{\alpha}) = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \text{and } H^*(\overline{\beta}) = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}.$$

It follows that

$$H^*(\overline{\alpha} \otimes \overline{\beta}) = H^*(\overline{\alpha}) H^*(\overline{\beta}) = \begin{pmatrix} pq & 0 \\ 0 & pq \end{pmatrix}, \; L_{\alpha,\beta} = L\left(H^*(\overline{\alpha} \otimes \overline{\beta})\right) \tag{4.2}$$

and

$$S_{\alpha,\beta} = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in Z^2 \mid 0 \le x_1, x_2 < pq \right\}. \tag{4.3}$$

It is easy to see that

$$\varphi(\alpha, \beta) = (p^2 - 1)(q^2 - 1). \tag{4.4}$$

In this special case, the 2-dimensional RSA maybe described as follows.

RSA in A Quadratic Field

- **Parameters:** $E = Q(\sqrt{d})$, d is a square-free integer and $d \equiv 2$ or $3 (\text{mod } 4)$, the rotation matrix $H = \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$, p, q are two large and distinct prime numbers of which satisfy (4.1). $N = pq$ and $\chi(N) = (p^2 - 1)(q^2 - 1)$. $L = L(B)$ is a lattice, $B = \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix}$. $1 \le e < \chi(N)$, $1 \le d_1 < \chi(N)$ such that $ed_1 \equiv 1 (mod \;\; \chi(N))$.
- **Public keys:** H, N and the positive integer e are public keys.
- **Private keys:** p, q and the positive integer d_1 are private keys.
- **Encryption:** For any $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in Z_{pq}^2$, the ciphertext $c = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \in Z^2$ given by $c \equiv a^{\otimes e} (mod \;\; L)$.
- **Decryption:** $c^{\otimes d_1} \equiv a^{\otimes d_1 e} \equiv a (\text{mod } L)$. One can find the plaintext a from c in Z_{pq}^2.

Table 4: RSA in A Quadratic Field

We can similarly deal with the cases of Cyclotomic Fields. Let $n = \varphi(m)$ for some positive integers m, $\xi_m = e^{2\pi i/m}$, $E = Q(\xi_m)$ and $R \subset E$ be the ring of algebraic integers of E. Suppose that $p \in Z$ is a rational prime number, then p is a prime element of R if and only if (see Theorem 2 of page 196 of [10])

$$p \nmid m \text{ and } p^{\varphi(m)} \equiv 1 (\text{mod } m). \tag{4.5}$$

Suppose that $p \in Z$ and $q \in Z$ are two distinct prime numbers satisfying (4.5), we obtain the lattice $L(H^*(\overline{p} \otimes \overline{q}))$ and an attainable algorithm in $Q(\xi_m)$.

References

[1]. M. Ajtai, C. Dwork. A Public-Key Cryptosystem with Worst-Case/Avarage -Case Equivalence. 29th ACM Symposium on Theory of Computing, 1997, 284-293.
[2]. D. Bonech. Twenty Years of Attacks on the RSA Cryptosystem. Notices of the Ams, 2002, 46(2): 203-213.
[3]. D. Coppersmith. Finding Small Solutions to Small Degree polynomials. Lecture Notes in Computer Science, 2001, 2146: 20-31.
[4]. H. Cohen. A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics. Springer-Verlag, 1993.
[5]. P. J. Davis. Circulant Matrices. 2nd Edition, Chelseea Publishing, New York, 1994.
[6]. E. B. Fluckiger, I. Suarez. Ideal Lattices Over Totally Real Number Fields and Euclidean Minima. Archiv Der Mathematik, 2006, 86(3): 217-225.
[7]. C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In STOC. 2009, 169-178.
[8]. O. Goldreich, S. Goldwasser, S. Halevi. Public-key Cryptosystems from Lattice Reduction Problems. In Advancesin cryptology, volume 1294 of Lecture Notes in Comput. Sci, 1997, 112-131.
[9]. J. Hoffstein, J. Pipher, J. H. Silverman. NTRU: A Ring-based Public Key Cryptosystem. In Proceedings of ANTS-III, volume 1423 of LNCS, 1998, 267-288.
[10]. K. Ireland, M. Rosen. A Classical Introduction to Modern Number Theory. Springer-Verlag, 1990.
[11]. V. Lyubashevsky, D. Micciancio. Generalized Compact Knapsacks are Collision Resistant. In 33rd international conference on Automata, Languages and Programming . Volume Part II. Springer-Verlag, 2006, 144-155.
[12]. Y. I. Manin, A. A. Panchishkin. Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories. Springer Berlin Heidelberg, 2005.
[13]. D. Micciancio, O. Regev. Lattice-based Cryptography. Post Quantum Cryptography. Springer Berlin Heidelberg, 2009, 147-191.
[14]. D. Micciancio. Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One Way Functions. Computational complexity, 2007, 16(4): 365-411.
[15]. D. Micciancio. Improving Lattice Based Cryptosystems Using the Hermite Normal Form. In CaLC. Springer Berlin Heidelberg, 2001, 126-145.
[16]. W. Narkiewicz. Elementary and Analytic Theory of Algebraic Numbers. Springer Berlin Heidelberg, 2004.
[17]. C. Peikert. A Decade of Lattice Cryptography. Foundations and trends in theoretical computer science, 2014, 10(4): 3-a2.
[18]. P. K. Pradhan, S. Rakshit, S. Datta. Lattice Based Cryptography. Proceedings of the Third International conference on computing methodologies and communication. ICCMC, 2019.
[19]. R. L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. Communications of the ACM 21, 1978, 120-126.
[20]. T. Takagi, S. Naito. Construction of RSA Cryptosystem over the Algebraic Field Using Ideal Theory and Investigation of Its Security. Electronics and Communications in Japan (Part III Fundamental Electronic Science), 2015, 83(8): 19-29.
[21]. Y. Uematsu et al. On the Extension of RSA Cryptosystem. Tech Rep 1985, IT 85-89.
[22]. Y. Uematsu et al. A Note on Extension of RSA Cryptosystem and Consideration of Amount of Computation. Encryption and Information Security Work shop, 1986, 27-29.
[23]. L. C. Washington. Introduction to Cyclotomic Fields (Graduate Texts in Mathematics). Springer Berlin Heidelberg, Volume 83, 1982.
[24]. Z. Y. Zheng, F. X. Liu, Y. F. Lu, K. Tian. Cyclic Lattices, Ideal Lattices and Bounds for the Smoothing Parameter. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.17626391.v1..
[25]. Z. Y. Zheng, F. X. Liu, J. Xu, W. L. Huang, K. Tian. A Generalization of NTRUEncrypt. arXiv:2112.14115[cs.IT].
[26]. Z. Y. Zheng. Modern Cryptography Volume 1---A Classical Introduction to Informational and Mathematical Principle. Springer Berlin Heidelberg. 2022.