CrossMark

A non-commutative cryptosystem based on quaternion algebras

Khadijeh Bagheri[1] · **Mohammad-Reza Sadeghi**[1] ·
Daniel Panario[2]

Abstract We propose BQTRU, a non-commutative NTRU-like cryptosystem over quaternion algebras. This cryptosystem uses bivariate polynomials as the underling ring. The multiplication operation in our cryptosystem can be performed with high speed using quaternions algebras over finite rings. As a consequence, the key generation and encryption process of our cryptosystem is faster than NTRU in comparable parameters. Typically using Strassen's method, the key generation and encryption process is approximately 16/7 times faster than NTRU for an equivalent parameter set. Moreover, the BQTRU lattice has a hybrid structure that makes inefficient standard lattice attacks on the private key. This entails a higher computational complexity for attackers providing the opportunity of having smaller key sizes. Consequently, in this sense, BQTRU is more resistant than NTRU against known attacks at an equivalent parameter set. Moreover, message protection is feasible through larger polynomials and this allows us to obtain the same security level as other NTRU-like cryptosystems but using lower dimensions.

Keywords Quaternion algebras · Public key cryptosystem · Lattice based cryptosystem · NTRU

Mathematics Subject Classification 11T71 · 94A60

Communicated by L. Perret.

✉ Mohammad-Reza Sadeghi
msadeghi@aut.ac.ir

Khadijeh Bagheri
kbagheri@aut.ac.ir

Daniel Panario
daniel@math.carleton.ca

[1] Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran

[2] School of Mathematics and Statistics, Carleton University, Ottawa, Canada

🦎 Springer

1 Introduction

The NTRU public key cryptosystem was proposed by Hoffstein et al. in 1996 [20]. The first version of this public key cryptosystem was standardized and published within IEEE P1363.1 [22]. Its security is based on the hardness of finding the shortest vector problem (SVP) and the closest vector problem (CVP) in a particular type of lattices, the convolutional modular lattices [30]. Furthermore, these two lattice problems are known to be NP-hard problems [31,32]. Thus, NTRU is a candidate for quantum-resistant public key cryptosystems.

The NTRU cryptosystem has been shown to be faster than RSA and elliptic curve cryptosystems [18]. Indeed, the linearity of lattice operations offers speed advantages over cryptosystems based on other known hard problems. Considering computational efficiency and low cost of implementation, NTRU is one of the fastest public key cryptosystems [18].

NTRU is based on the polynomial ring $R = \mathbb{Z}[x]/\langle x^n - 1 \rangle$. Coppersmith and Shamir [11] present a lattice attack against NTRU that finds the private key from its public key by solving the SVP on the NTRU lattice. They suggest that a non-commutative algebra can be considered for the underlying algebra to avoid these attacks. Several non-commutative proposals have been introduced and, consequently, have been broken. Gaborit et al. [14] introduce CTRU as an analogue to NTRU where the coefficients of polynomials are from $\mathbb{F}_2$ instead of $\mathbb{Z}$. Kouzmenko [25] shows that CTRU can be broken using a polynomial time attack. Generalizations of NTRU over the Dedekind domains including $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\zeta_5]$, where ζ_3 and ζ_5 are 3rd and 5th roots of unity, are presented in [23] and [33]. A non-commutative version of NTRU over the non-commutative ring of $k \times k$ matrices of polynomials in the ring R is also available in the literature [9]. Another non-commutative version of NTRU, called QTRU, is addressed by Malekian et al. over quaternion algebras [28,29]. The computational processes of QTRU have high complexity and at equivalent parameters set, QTRU is slower that NTRU. In a different direction, Caboara et al. [7] increase the number of variables in the polynomial ring R, instead of operating in a different coefficient ring. Moreover, they introduce an ideal of R in their scheme so to complicate the attacking scenarios of NTRU-like cryptosystem. However, this scheme is inefficient due to the high complexity of the key generation, the encryption and the decryption algorithms. An improvement of this work is presented for bilinear polynomial rings in [4], which is secure against the lattice based attack and has an efficient encryption algorithm but its key generation and decryption algorithm are still not efficient enough to be practical. The proposed method in this paper, inspired by [4] and [28], leads to an efficient NTRU-like cryptosystem that is secure against lattice based attacks in smaller dimensions.

There are other advantages and practical potentialities when using non-commutative structures like quaternions as the underlying ring of NTRU. On the one hand, many applications in image processing are concerned with signals and images that have three or four dimensional samples. Quaternions are useful tools for modeling and analyzing such signals that arise very naturally in the physical world from the three dimensions of physical space to trichromatic nature of human color vision. More generally, the four dimensions of quaternions can be used to represent a most general set of geometric operations in three dimensions using homogenous coordinates. The reader is pointed to the recent book [13] that shows quaternions usages in signal and image processing. Given this number of applications of quaternions, looking at scenarios that require secure data transmission of a source that generates vector-valued samples, leads us to design a fast cryptosystem based on quaternions. On the other hand, under special conditions, quaternion algebras over a field $\mathbb{F}$ are isomorphic to $M_2(\mathbb{F})$, the ring of 2×2 matrices over $\mathbb{F}$. In this case, the multiplication of two elements of these quater-

nion algebras is equivalent to a multiplication of their corresponding 2×2 matrices over $\mathbb{F}$. Strassen shows that two 2×2 matrices can be multiplied using only seven multiplications and some additions [38]. Thus, any quaternion multiplication can be done with seven multiplications over $\mathbb{F}$ instead of 16. Therefore, if we use the special case of quaternion algebra in a cryptosystem, it leads to low complexity encryption and decryption algorithms due to the high speed operations in this algebra. This also motivated us to present an extensions of NTRU cryptosystem over quaternions.

In this paper, we introduce an NTRU-like cryptosystem called BQTRU. We change the underlying algebraic structure of NTRU to a quaternion algebra over the bivariate polynomial ring $R' = \mathbb{Z}[x, y]/\langle x^n - 1, y^n - 1 \rangle$. In BQTRU, four messages from four different sources are encrypted at the same time; this is useful in multiuser applications. Moreover, the processing in the BQTRU cryptosystem is fast thanks to several quaternion properties.

Similar to [4] and [7], we use an ideal of R' when designing the BQTRU cryptosystem to enhance the security of our proposed NTRU-like cryptosystem against lattice attacks. Therefore, the BQTRU lattice also has a hybrid structure that makes inefficient standard lattice attacks on the private key. Hence, the lattice based attacks on our private key have higher complexity than other NTRU-like cryptosystems. As a consequence of some special properties, BQTRU is more resistant than other NTRU-like cryptosystems against lattice based attacks in smaller dimensions. Typically, we can obtain the same security level of other NTRU-like cryptosystems but here in lower dimensions. This high complexity of lattice based attacks opens the possibility of smaller key sizes and more message protection with respect to NTRU.

The rest of the paper is organized as follows. In Sect. 2, the original presentation of the NTRU cryptosystem and required mathematical background about quaternion algebras are revisited. The design of the proposed cryptosystem is presented in Sect. 3. In Sect. 4, we present the choice of parameters for BQTRU which makes the probability of decryption failure to be close to negligible. In Sect. 5, the security analysis of the proposed cryptosystem against known attacks on both the public key and the message are discussed. Using the parameters presented in the previous section, the size of the key space and message space of BQTRU is compared with NTRU and QTRU. We also design a lattice based attack on BQTRU and we show that BQTRU is resistant against this attack. Conclusions are given in Sect. 6.

2 Preliminaries

2.1 The NTRU cryptosystem

In this section, we briefly describe the original NTRU public key cryptosystem; for more information, see [19,20]. We follow the presentation in [20]. We start by fixing an integer $n > 1$ and two coprime moduli p and q with $q \gg p$. Commonly n is chosen to be prime and p is chosen to be 3. Let $R = \mathbb{Z}[x]/\langle x^n - 1 \rangle$ be the ring of truncated polynomials with convolutional multiplication denoted by the symbol $*$. In this ring, the addition of two polynomials is defined by the pairwise addition of the coefficients. We consider the rings $R_q = \mathbb{Z}_q[x]/\langle x^n - 1 \rangle$ and $R_p = \mathbb{Z}_p[x]/\langle x^n - 1 \rangle$ and the subsets L_f, L_g, L_r and L_m of R. The set L_f (respectively, L_g and L_r) contains ternary polynomials, that is polynomials with coefficients $+1$ and -1, in R with $2d_f$ (respectively, $2d_g$ and $2d_r$) monomials with coefficients ± 1, and the set L_m contains polynomials in R whose coefficients are between $-(p-1)/2$ and

$(p - 1)/2$. In NTRU the usual choice is $d_f = d_g = d_r = d$ approximately of size $n/3$. For correctness of the decryption algorithm in NTRU, we concentrate on polynomials of small norm, compared to the modulus q. We use the term "small" polynomial to indicate polynomials in R having small norm compared to the modulus q. Specially in the original NTRU, small polynomials are those ternary polynomials such that many coefficients are zero and the rest ($2d \approx 2n/3$) are in the set $\{1, -1\}$. The usage of these type of polynomials is key for NTRU security.

Using public parameters n, p and q, NTRU key generation selects two small random polynomials $f \in L_f$ and $g \in L_g$ such that f is invertible in R_q and R_p. The inverses of f in R_q and R_p are denoted by f_q^{-1} and f_p^{-1}, respectively.

The public key is $h = f_q^{-1} * g \pmod q$.

The private key is (f, g).

To encrypt a message m from the set of messages L_m, we pick a random polynomial $r \in L_r$ and compute

$$c = ph * r + m \pmod q.$$

To decrypt a ciphertext c, we use the private key f and compute

$$e = f * c = f * (ph * r + m) = pf * (f_q^{-1} * g) * r + f * m = pg * r + f * m \pmod q.$$

We can ensure that all of the coefficients of $pg * r + f * m$ fall in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$ by a careful choice of parameters. Thus, $e \in R_q$ is equal to $pg * r + f * m \in R$ and the message m is obtained from e by reducing the coefficients of $f_p^{-1} * e$ modulo p. The public parameters (n, p, q) of NTRU are chosen such that the probability of decryption failure is minimized. If $q > (6d + 1)p$, then the decryption process never fails [20].

There are several known attacks on NTRU which are classified in two types of attacks: combinatorial and lattice based attacks. The combinatorial attacks are easily avoided by a careful choice of parameters [21]; the lattice based attacks are the most significant attacks to date and lead to the more recent developments of NTRU [11]. Coppersmith and Shamir introduced the NTRU lattice as a submodule $\mathscr{L}$ of $R \times R$ generated by $(q, 0)$ and $(1, h)$. When we represent the elements of R by their coefficient vectors in $\mathbb{Z}^n$, the submodule $\mathscr{L}$ can also be viewed as a $2n$-dimensional lattice L_{NTRU} with row basis matrix

$$\begin{bmatrix} qI & 0 \\ \mathscr{H} & I \end{bmatrix},$$

where $\mathscr{H}$ is a circulant $n \times n$ matrix defined by the coefficient vector of h as first row, and each additional row is obtained from the one above it by cyclic shifting one position to the right. An attempt at finding the private key (f, g) leads to solving SVP in L_{NTRU} [11], while an attempt at obtaining the message m leads to finding CVP in L_{NTRU} [20]. Lattice basis reduction algorithms like LLL [26] and BKZ [35] (or BKZ 2.0 [8]) can find SVP in an n dimensional lattice $\Lambda \subseteq \mathbb{R}^n$ with length up to a factor of at most $2^{O(n)}$ the size of a shortest vector in Λ. Therefore, when n gets sufficiently large the algorithms fail to determine a suitable result for SVP. Thus the dimension of the lattice must be large enough in order to have a reasonable level of security in the cryptosystem.

2.2 Quaternion algebra

In this section, we briefly review quaternion algebras which contain the underlying algebra of our proposed cryptosystem as a special case. Hamilton discovered the real quaternion

algebra $\mathbb{H}$ in 1843. It is known that the only real normed division algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and the Octonions $\mathbb{O}$ [10], where the normed division algebras are not necessarily commutative or associative. Among the above algebras, $\mathbb{H}$ is the only one that is associative and non-commutative. The real quaternions can be considered as a vector space of dimension 4 over $\mathbb{R}$ with an ordered basis $\{1, i, j, k\}$ as follows

$$\mathbb{H} = \{s_0 + s_1 i + s_2 j + s_3 k \mid s_0, s_1, s_2, s_3 \in \mathbb{R}\}.$$

The addition of two quaternions and the scalar multiplication are defined by component-wise vector addition and scalar multiplication. The multiplication of two quaternions denoted by ◦ is defined by the following rules:

$$i^2 = j^2 = k^2 = -1, \quad i \circ j = -j \circ i = k, \quad j \circ k = -k \circ j = i, \quad k \circ i = -i \circ k = j.$$

We define quaternion algebras over general fields whose characteristic are not 2. Some of the basic properties of these algebras are derived using straightforward computational arguments.

Definition 1 Let a and b be non-zero elements of a field $\mathbb{F}$. The quaternion algebra $\mathbb{A}$ over $\mathbb{F}$ is a four dimensional $\mathbb{F}$-space with basis 1, i, j and k, where the bilinear multiplication is defined by the conditions that 1 is a unity element, and

$$i^2 = a, \quad j^2 = b, \quad i \circ j = -j \circ i = k.$$

Therefore

$$k^2 = -ab, \quad j \circ k = -k \circ j = -ib, \quad k \circ i = -i \circ k = -ja$$

and $\mathbb{A}$ is an associative algebra over $\mathbb{F}$.

For each quaternion $s = s_0 + s_1 i + s_2 j + s_3 k$ in $\mathbb{A}$, its conjugate is given by $\bar{s} = s_0 - s_1 i - s_2 j - s_3 k$, and its norm is defined by $N(s) = s \circ \bar{s} = \bar{s} \circ s = s_0^2 - a s_1^2 - b s_2^2 + a b s_3^2$. A quaternion is a *unit quaternion* if its norm is 1. The inverse of the quaternion s is given by $s^{-1} = \bar{s}/N(s) = \bar{s} \circ (N(s))^{-1}$ provided that its norm is nonzero.

The constructed algebra is denoted by $\left(\frac{a,b}{\mathbb{F}}\right)$ as a (generalized) quaternion algebra over $\mathbb{F}$. Hamilton's quaternions occur as the special case $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. It is well known that $\left(\frac{a,b}{\mathbb{F}}\right)$ is a four-dimensional associative algebra with central field $\mathbb{F}$.

A quaternion algebra over $\mathbb{F}$ is either a division algebra or else is isomorphic to $M_2(\mathbb{F})$. In [27], it is shown that for any field $\mathbb{F}$,

$$M_2(\mathbb{F}) \cong \left(\frac{1,1}{\mathbb{F}}\right),$$

where the isomorphism is induced by

$$i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The *Lipschitz* quaternions or *integral quaternions* $\mathbb{L} = \left(\frac{a,b}{\mathbb{Z}}\right)$ form a subring of the real quaternions $\mathbb{H}$. The algebra $\mathbb{L}_q = \left(\frac{a,b}{\mathbb{F}_q}\right)$ is defined over the finite field $\mathbb{F}_q$, where q is a prime number.

In general, the quaternion algebra $\mathbb{A}$ can be defined over any commutative ring R with identity. In this paper, we define the quaternion algebra over the polynomial ring $R' = \mathbb{Z}[x, y]/\langle x^n - 1, y^n - 1\rangle$, where we can perform arithmetic operations efficiently, low complexity and low memory requirements.

When we work with fields like the complex numbers, we have efficient algorithms for solving the equations with coefficients belonging to this field. In the quaternions, some problems like root finding algorithms, even solving a quadratic equation with coefficients belonging to $\mathbb{H}$, become nontrivial. Kalantari in [24] suggests a new and simple approach for computing the solutions of a quadratic polynomial in $\mathbb{H}[x]$. We remark that even quadratic equations where the variable and the coefficients may not commute are fairly complicated to solve.

Factoring a polynomial in $R[x]$ where R is noncommutative does not preserve evaluation, that is, given $P, E, H \in R[x]$, the evaluation of the polynomials at $r \in R$ is not a ring homomorphism. That is,

$$P(x) = E(x)H(x) \text{ does not imply } P(r) = E(r)H(r).$$

Example 1 Consider $P(x) = (x - i)(x - j) \in \mathbb{H}[x]$. We might expect i and j to be roots of P. However, $P(x) = x^2 - (i + j)x + k$. and hence

$$P(i) = i^2 - (i + j) \circ i + k = -1 - i^2 - i \circ j + k = 2k \neq 0,$$
$$P(j) = j^2 - (i + j) \circ j + k = -1 - i \circ j - j^2 + k = 0.$$

Therefore, j is a (right) root of P, but i is not.

Definition 2 ([24]) Two quaternions s and s' are congruent or equivalent, denoted by $s \sim s'$, if for some quaternion $w \neq 0$ we have, $s' = w \circ s \circ w^{-1}$. The congruence class of $s = s_0 + s_1 i + s_2 j + s_3 k$, denoted by $[s]$, is the set

$$[s] = \left\{ s' \in \mathbb{H} \mid s' \sim s \right\}.$$

It is proved in [24] that $[s] = \left\{ s_0 + x_1 i + x_2 j + x_3 k \mid x_1^2 + x_2^2 + x_3^2 = s_1^2 + s_2^2 + s_3^2 \right\}$.

Definition 3 ([24]) Let R be a noncommutative ring. An element $r \in R$ is a right root of a nonzero polynomial $P \in R[x]$ if and only if $P(x) = E(x)(x - r)$ for some polynomial $E \in R[x]$.

Theorem 1 ([24]) *Let D be a division ring, and let $P(x) = E(x)H(x)$ with $P, E, H \in D[x]$. An element $d \in D$ is a root of P if and only if either d is a root of H, or a conjugate of d is a root of E.*

The fact that the evaluation map over the quaternions does not define a ring homomorphism from $\mathbb{H}[x]$ to $\mathbb{H}$, is a source of difficulty in polynomial root-finding over the quaternions. On the other hand, in contrast with real or complex polynomials, a quaternion polynomial can have infinitely many roots or it could have fewer roots than its degree without multiplicity. This arises from the following theorem.

Theorem 2 [16] *Let D be a division ring. A polynomial in $D[x]$ of degree m can have infinitely many roots, however these roots come from at most m distinct conjugacy classes of D.*

A method has been presented for approximating the zeros of a real quaternion polynomial in [24]. Moreover, a simple method for constructing a quaternion polynomial with prescribed zeros and a decomposition theorem for a quaternion polynomial in $\mathbb{H}[x]$ is also described in [24].

The proposed cryptosystem in this paper requires the study of quaternion algebras over commutative ring $R' = \mathbb{Z}[x, y]/\langle x^n - 1, y^n - 1\rangle$. Factorization, decomposition and classification of zeros of a quaternion polynomial in this ring have not been addressed in the literature as far we know.

One of the important structures in our cryptosystem is the ideal J of $\mathbb{A}$, quaternion algebra over R', which we introduce in the next section. The key generation process involves finding the inverse of a polynomial $F = f_0 + f_1 i + f_2 j + f_3 k \in \mathbb{A}$ modulo the ideal J which requires an efficient division algorithm in general. Due to the lack of such algorithm in the literature, we consider a special form for ideal J that makes the existence of a quaternion division algorithm inessential for us. We consider $J = Q + Qi + Qj + Qk$, where the ideal Q is a central ideal of $\mathbb{A}$, that is $Q \subseteq Z(\mathbb{A})$, where $Z(\mathbb{A})$ is the center of $\mathbb{A}$, that is, the set of all elements in $\mathbb{A}$ that commute with every element. The construction method of Q and J is also presented in the next section. It is related to the choice of a set containing n-th roots of unity, roots of the polynomial $x^n - 1$ in $\mathbb{A}$. Our construction method for ideal J considers only central roots of $x^n - 1$. If this restriction could be removed and non-central roots in the construction of J could be used, then Theorem 2 would provide enhanced security to our system by improving the resistance to a brute force attack on the private ideal J.

3 BQTRU: a cryptosystem based on bivariate polynomials and quaternions

In this section, we introduce our cryptosystem by using the quaternion algebras as its underlying algebraic structure. Operations in this cryptosystem are performed in the ring of bivariate polynomials $R' = \mathbb{Z}[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1\rangle$. It is possible to take two different exponents n_1 and n_2, however for simplicity we consider $n_1 = n_2 = n$ in the rest of the paper. We consider an order on monomials, like lexicographical order, embedding every polynomial $f \in R'$ in $\mathbb{Z}^{n^2}$. This embedding maps a polynomial $f \in R'$ into a vector $\overrightarrow{f} = (f_0, f_1, \ldots, f_{n^2-1}) \in \mathbb{Z}^{n^2}$.

We choose the public parameters (n, p, q) similar to the original NTRU: n is a prime number, p and q are two different prime numbers such that $\gcd(p, q) = \gcd(n, q) = 1$ where $q \gg p$ and L_f, L_g, L_ϕ and L_m are subsets of R' that are defined similar to their corresponding subsets in NTRU. In the proposed cryptosystem, the integers d_f, d_g, d_ϕ and d_m associated to these subsets are considered such that $d_f = d_g = d_\phi = d_m = d \approx n^2/7$. An additional condition is the choice of n and q such that $n|(q - 1)$.

We choose an ideal Q_q of $R'_q = \mathbb{Z}_q[x, y]/\langle x^n - 1, y^n - 1\rangle$ and use this ideal for key generation and decryption in our cryptosystem. In the next section, we show that the use of this ideal leads to applying a different lattice for decryption. Since $\langle x^n - 1, y^n - 1\rangle \subset Q_q$, therefore Q_q corresponds to the intersection of ideals of the form $\langle x - a, y - b\rangle$ where (a, b) belongs to the set $E = \{(a, b) \in \mathbb{Z}_q \times \mathbb{Z}_q \mid a^n = 1, b^n = 1\}$. Let $T \subset E$ be the set of points for which there is at least one polynomial in Q_q with no roots from T. Then, it is clear that the ideal Q_q is equal to the set of polynomials that vanish on $E \backslash T$.

The condition $n|(q - 1)$ yields the factorization of $x^n - 1$ into linear factors in $\mathbb{Z}_q$. Then, E is a set of elements of $\mathbb{Z}_q \times \mathbb{Z}_q$ with cardinality n^2.

Obviously, R'_q is a vector space of dimension n^2 over $\mathbb{Z}_q$ where we can consider the Lagrange basis with Lagrange interpolants defined for each point (a, b) of E by

$$\lambda_{a,b}(x, y) = \frac{ab(x^n - 1)(y^n - 1)}{n^2(x - a)(y - b)}. \tag{1}$$

Any polynomial $f(x, y)$ of R'_q can be identified by its values over E as [3]

$$f(x, y) = \sum_{(a,b) \in E} f(a, b) * \lambda_{a,b}(x, y). \tag{2}$$

For each $(a, b) \in E$, the Lagrange interpolant $\lambda_{a,b}(x, y)$ is a polynomial that vanishes on E except at (a, b) where its value is equal to 1. Moreover, every $\lambda_{a,b}(x, y)$ have the property that for each $\alpha \in R'_q$

$$\alpha(x, y) * \lambda_{a,b}(x, y) = \alpha(a, b) * \lambda_{a,b}(x, y). \tag{3}$$

In this way, when we see R'_q as a vector space over $\mathbb{Z}_q$, then Q_q can be consider as a vector subspace of R'_q. Since any polynomial $\rho \in Q_q$ vanishes outside of T, by considering (2), we have $\rho(x, y) = \sum_{(a,b) \in T} \rho(a, b) * \lambda_{a,b}(x, y)$. Without loss of generality, we assume that the first $|T|$ elements of the set E are exactly the points of T. Hence, each $\rho \in Q_q$ is written as a linear combination of $\{\lambda_{a_i,b_i}(x, y)\}_{i=1}^{|T|}$ and this set can be a basis of Q_q as a vector subspace of R'_q.

On the other hand, Q_q, as an ideal, can be generated by

$$\sigma(x, y) = \sum_{i=1}^{|T|} q_i \lambda_{a_i,b_i}(x, y), \tag{4}$$

where for $i = 1, \ldots, |T|$, q_i is a nonzero element of $\mathbb{Z}_q$ chosen at random, or given by any other polynomial which does not vanish on T. We observe that $\sigma(x, y) * \lambda_{a_i,b_i}(x, y)(q_i)^{-1} = \lambda_{a_i,b_i}(x, y)$ for $i = 0, \ldots, |T|$, therefore the ideal generated by $\sigma(x, y)$ contains our basis for the vector space Q_q. Consequently, we can consider $Q_q = \langle \sigma(x, y) \rangle$. In this way, the ideal $Q = \langle q, \sigma(x, y) \rangle$ of R' has $\{q\} \cup \{\lambda_{a_i,b_i}(x, y)\}_{i=1}^{|T|}$ as its generators, where $T \subseteq E$.

In our cryptosystem, we consider the quaternion algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$ over the rings $R' = \mathbb{Z}[x, y]/\langle x^n - 1, y^n - 1 \rangle$, $R'_p = \mathbb{Z}_p[x, y]/\langle x^n - 1, y^n - 1 \rangle$ and $R'_q = \mathbb{Z}_q[x, y]/\langle x^n - 1, y^n - 1 \rangle$, respectively:

$$\mathbb{A} = \left(\frac{1, 1}{R'} \right) = \left\{ f_0 + f_1 i + f_2 j + f_3 k \,\middle|\, f_0, f_1, f_2, f_3 \in R'; \ i^2 = j^2 = 1, \ i \circ j = -j \circ i = k \right\},$$

$$\mathbb{A}_p = \left(\frac{1, 1}{R'_p} \right) = \left\{ f_0 + f_1 i + f_2 j + f_3 k \,\middle|\, f_0, f_1, f_2, f_3 \in R'_p; \ i^2 = j^2 = 1, \ i \circ j = -j \circ i = k \right\},$$

$$\mathbb{A}_q = \left(\frac{1, 1}{R'_q} \right) = \left\{ f_0 + f_1 i + f_2 j + f_3 k \,\middle|\, f_0, f_1, f_2, f_3 \in R'_q; \ i^2 = j^2 = 1, \ i \circ j = -j \circ i = k \right\},$$

which are isomorphic to $M_2(R')$, $M_2(R'_p)$ and $M_2(R'_q)$, respectively. These quaternion algebras possess the properties seen in Sect. 2, except that some nonzero elements might have zero norm and then such elements do not have a multiplicative inverse [10].

The multiplication of two quaternions F and G of these quaternion algebras is equivalent to a multiplication of two 2×2-matrices over their underlying ring. For example, a quaternion $F = f_0 + f_1 i + f_2 j + f_3 k \in \mathbb{A}$ is isomorphic to a 2×2-matrix in $M_2(R')$ with generators

$$i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Therefore, since $ij = k$, we obtain

$$F = f_0 + f_1 i + f_2 j + f_3 k \cong f_0 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + f_1 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + f_2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + f_3 \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$\cong \begin{bmatrix} f_0 + f_1 & f_2 + f_3 \\ f_2 - f_3 & f_0 - f_1 \end{bmatrix}.$$

Strassen [38] shows that two 2×2 matrices can be multiplied using only seven multiplications. An improvement on Strassen's algorithm for 2×2 matrices is given by Winograd [40]. More information about Strassen's algorithm and its variants is available in [6] (page 11–13). Hence, the multiplication of two quaternions F and G of $\mathbb{A}$ is equivalent to a multiplication of their equivalent 2×2-matrices over the the ring R'. Thus, this multiplication is possible with seven convolutional multiplications in R' and some additional sums.

In the following we present some lemmas and a theorem that are needed for the key generation of our cryptosystem. The proof of some lemmas is trivial and they are left to the reader. Without loss of generality, we assume that the points are ordered such that the first $|T|$ points are exactly the points of the subset T.

Lemma 1 *Let $\rho : \mathbb{A}_q \rightarrow (\mathbb{L}_q)^{n^2}$ be a map defined by*

$$\rho(F) = \left(F(a_1, b_1), F(a_2, b_2), \ldots, F(a_{n^2}, b_{n^2}) \right),$$

where $(a_i, b_i) \in E$ and $\mathbb{L}_q = \left(\frac{1,1}{\mathbb{Z}_q} \right)$ is the algebra of quaternions over $\mathbb{Z}_q$. Then the following properties hold

$$\rho(F + G) = \rho(F) + \rho(G),$$
$$\rho(F \circ G) = \rho(F) \bullet \rho(G),$$

where

$$\rho(F) \bullet \rho(G) = (F(a_1, b_1) \circ G(a_1, b_1), F(a_2, b_2) \circ G(a_2, b_2), \ldots, F(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2})).$$

Proof Considering Eqs. (2) and (3), the following relationship holds:

$$F(x, y) = \sum_{i=1}^{n^2} F(a_i, b_i) \circ \lambda_{a_i, b_i}(x, y),$$

$$F \circ G = \left(\sum_{i=1}^{n^2} F(a_i, b_i) \circ \lambda_{a_i, b_i}(x, y) \right) \circ G = \sum_{i=1}^{n^2} F(a_i, b_i) \circ G \circ \lambda_{a_i, b_i}(x, y)$$

$$= \sum_{i=1}^{n^2} \left(F(a_i, b_i) \circ G(a_i, b_i) \right) \circ \lambda_{a_i, b_i}(x, y).$$

We observed that since $\lambda_{a_i, b_i}(x, y) \in \mathbb{Z}_q[x, y]$ commutes with G, the second equation holds. Therefore,

$$\rho(F \circ G) = \left(F(a_1, b_1) \circ G(a_1, b_1), F(a_2, b_2) \circ G(a_2, b_2), \ldots, F(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2}) \right)$$
$$= \rho(F) \bullet \rho(G).$$

$\square$

Lemma 2 *Let $\mathbb{A}_q = R'_q + R'_q i + R'_q j + R'_q k$ and let $\mathbb{B}_q = \mathbb{Z}_q[x, y] + \mathbb{Z}_q[x, y]i + \mathbb{Z}_q[x, y]j + \mathbb{Z}_q[x, y]k$. Then*

$$\mathbb{A}_q \cong \frac{\mathbb{B}_q}{\langle x^n - 1, y^n - 1 \rangle} = \frac{\mathbb{Z}_q[x, y] + \mathbb{Z}_q[x, y]i + \mathbb{Z}_q[x, y]j + \mathbb{Z}_q[x, y]k}{\langle x^n - 1, y^n - 1 \rangle}.$$

Lemma 3 *Let $J_q = Q_q + Q_q i + Q_q j + Q_q k$, where Q_q is the ideal of R'_q generated by $\sigma = \sum_{i=1}^{|T|} q_i \lambda_{a_i,b_i}(x, y)$. Then J_q is an ideal of $\mathbb{A}_q$ and is generated by σ. Furthermore, J_q contains the ideal $\langle x^n - 1, y^n - 1 \rangle$ of $\mathbb{B}_q$.*

In a similar way, we obtain the following lemma.

Lemma 4 *Let $J = Q + Qi + Qj + Qk$, where $Q = \langle \sigma, q \rangle$ is an ideal of R'. Then, J is an ideal of $\mathbb{A} = R' + R'i + R'j + R'k$ and is generated by q and σ, that is $J = \langle q, \sigma \rangle_\mathbb{A}$.*

Lemma 5 *Let $J = Q + Qi + Qj + Qk$ and $\mathbb{A} = R' + R'i + R'j + R'k$. Then*

$$\frac{\mathbb{A}}{J} \cong \frac{R'}{Q} + \frac{R'}{Q}i + \frac{R'}{Q}j + \frac{R'}{Q}k.$$

Corollary 1 *The computation of $F = f_0 + f_1 i + f_2 j + f_3 k \in \mathbb{A}$ modulo J is equivalent to the computation of f_i modulo Q, for $i = 0, \ldots, 3$.*

In the following, we recall the combinatorial nullstellensatz theorem.

Theorem 3 *(Combinatorial Nullstellensatz) Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $U_1, \ldots, U_n$ are subsets of F with $|U_i| > t_i$, there are $a_1 \in U_1, a_2 \in U_2, \ldots, a_n \in U_n$ so that $f(a_1, \ldots, a_n) \neq 0$.*

Remark 1 In accordance with the Combinatorial Nullstellensatz theorem [2], for any set of $T \subseteq E$, there is a unique polynomial $\sigma(x, y)$ that generates Q.

Proof Let T' and T be two subsets of E that generate the same polynomial $\sigma(x, y)$. Without loss of generality assume that the points are ordered such that the first $|T|$ (or $|T'|$) points are exactly the points of the subset T (or T'). Equation (4) implies that $\sigma(x, y) = \sum_{i=1}^{|T|} q_i \lambda_{a_i,b_i}(x, y) = \sum_{i=1}^{|T'|} q_i \lambda_{a_i,b_i}(x, y)$ and $k(x, y) = \sum_{i=1}^{|T|} q_i \lambda_{a_i,b_i}(x, y) - \sum_{i=1}^{|T'|} q_i \lambda_{a_i,b_i}(x, y) = 0$. According to the Combinatorial Nullstellensatz theorem, since the degree of k is $2(n-1)$ and $U_1 = U_2 = \{b \in \mathbb{Z}_q \mid b^n = 1\}$, where the condition $n | (q - 1)$ yields $|U_1| = |U_2| = n$, there are $a \in U_1, b \in U_2$ so that $k(a, b) \neq 0$. However $k(x, y) = 0$, and this contradiction completes the proof. □

In this cryptosystem, we choose a set $T \subseteq E$ such that the cardinality of this set is small. Then, we construct the ideal $Q = \langle q, \sigma(x, y) \rangle$ of R'. We consider $J = Q + Qi + Qj + Qk$ as the *private ideal* of $\mathbb{A}$ and use it for key generation and decryption. In the next subsection, we explain how to choose the subset T.

By considering a monomial basis for R', we get that R' is isomorphic to $\mathbb{Z}^{n^2}$ as an additive modulo over $\mathbb{Z}$. Since Q is an ideal of R', then $Q \subset R' \cong \mathbb{Z}^{n^2}$ is an additive subgroup of $\mathbb{Z}^{n^2}$ and so Q can be viewed as an n^2 dimensional lattice, denoted by Λ_Q, in $\mathbb{Z}^{n^2}$. Similarly, when we specify a basis for $\mathbb{A}$, we get that $\mathbb{A}$ is isomorphic to $\mathbb{Z}^{n^2} + \mathbb{Z}^{n^2} i + \mathbb{Z}^{n^2} j + \mathbb{Z}^{n^2} k$ that is also isomorphic to $\mathbb{Z}^{4n^2}$ as an additive group. The *private ideal* J is an ideal of $\mathbb{A} = R' + R'i + R'j + R'k$ and $J \subset \mathbb{A} \cong \mathbb{Z}^{4n^2}$ can be viewed also as a lattice in $\mathbb{Z}^{4n^2}$. We use this private lattice, denoted by $\Lambda_{private}$, in our cryptosystem.

To construct a generator matrix for the private lattice Λ_{private}, we first give a generator matrix for the lattice Λ_Q and develop it for Λ_{private}. In the following, we give the generator matrix of the lattice Λ_Q.

Let D' be the generator matrix of Λ_Q. Then, D' is an $n^2 \times n^2$ matrix whose rows are coefficient vectors of the Lagrange interpolants $\{\lambda_{a_i,b_i}\}_{i=1}^{|T|}$ and some qe_{j_i}'s to be explained next, where $j_i \in S \subseteq \{1, \dots, n^2\}$, for $i = 1, \dots, n$ and e_k is the vector with one in k-th position and zero in other positions. Consider the matrix L whose rows are the coefficient vectors of the Lagrange interpolants $\{\lambda_{a_1,b_1}, \dots, \lambda_{a_{|T|},b_{|T|}}\}$. Using that the row rank of an integer matrix is equal to its column rank [5] (see Chapter 4), the row rank and column rank of L is $|T|$. We can assume that the columns $i_1, \dots, i_{|T|}$ are independent columns in this matrix L. Let

$$S := \{j_1, \dots, j_{n^2-|T|}\} = \{1, \dots, n^2\} \setminus \{i_1, \dots, i_{|T|}\},$$

where $j_1 < j_2 < \cdots < j_{n^2-|T|}$. Then, $qe_{j_1} \dots, qe_{j_{n^2-|T|}}$ and the coefficient vectors of interpolants $\{\lambda_{a_i,b_i}\}_{i=1}^{|T|}$ form a basis for Λ_Q with high probability. Now, since $J \cong Q^4$ as additive groups, the private lattice Λ_{private} is generated by the rows of the following matrix

$$M_{\text{private}} = \begin{bmatrix} D' & 0 & 0 & 0 \\ 0 & D' & 0 & 0 \\ 0 & 0 & D' & 0 \\ 0 & 0 & 0 & D' \end{bmatrix}. \tag{5}$$

3.1 Key generation

For creating public and private keys, we randomly choose two quaternion polynomials F and G in $\mathbb{A}$ as

$$F = f_0 + f_1 i + f_2 j + f_3 k, \quad f_0, f_1, f_3, f_4 \in L_f,$$
$$G = g_0 + g_1 i + g_2 j + g_3 k, \quad g_0, g_1, g_3, g_4 \in L_g.$$

The polynomials $f_i \in L_f$ and $g_i \in L_g$, for $i = 0, \dots, 3$, are small ternary polynomials in R', that is, they are random polynomials that most coefficients are zero and the rest are in the set $\{1, -1\}$. Therefore, the two quaternion polynomials F and G are small ternary quaternion polynomials. If we consider the coefficient vector of each element $F = f_0 + f_1 i + f_2 j + f_3 k \in \mathbb{A}$ as

$$\overrightarrow{F} = \left(\overrightarrow{f_0}, \overrightarrow{f_1}, \overrightarrow{f_2}, \overrightarrow{f_3} \right)$$

then, the coefficient vectors of $\overrightarrow{F}$ and $\overrightarrow{G}$ have many zeros and few 1 and -1. Therefore, the Euclidean norm of $\overrightarrow{F}$ and $\overrightarrow{G}$ is small.

Both F and G should be invertible in $\mathbb{A}/J$, that is, there exist F^{-1} and G^{-1} in $\mathbb{A}$ such that

$$F \circ F^{-1} = F^{-1} \circ F = 1 \pmod{J},$$
$$G \circ G^{-1} = G^{-1} \circ G = 1 \pmod{J}.$$

The quaternion F must satisfy the additional requirement that it is invertible in $\mathbb{A}_p$ for decryption purpose. In order for the quaternion F to be invertible over $\mathbb{A}_p$, the polynomial $N(F) = f_0^2 - f_1^2 - f_2^2 - f_3^2$ must be nonzero and invertible over its underlying ring R'_p. By Lemma 5, $\mathbb{A}/J$ is a quaternion algebra over the ring R'/Q. Hence, the necessary and sufficient condition for invertibility of F and G in $\mathbb{A}/J$ is the existence of $(N(F))^{-1}$ and $(N(G))^{-1}$ in the ring R'/Q.

In the sequel, we present a method for choosing F and G to fulfill the above conditions. Our method uses the fact that the polynomial $N(F)$ is invertible modulo Q if and only if the roots of $N(F)$ which belong to E are also contained in T. Thus our method selects T after choosing F and G to make sure that $N(F)$ and $N(G)$ are invertible modulo Q: choose G at random and define the set $T = \bigcap_{i=0}^{3}\{(a, b) \in E \mid g_i(a, b) = 0\}$. If $T = \emptyset$, then pick another G. Select F randomly such that $\{(a, b) \in E \mid N(F)(a, b) = 0\} \subset T$.

The inverses of the quaternion F in $\mathbb{A}/J$ and $\mathbb{A}_p$ are denoted by F^{-1} and F_p^{-1}, respectively; they are computed as follows

$$F^{-1} = \left(f_0^2 + f_1^2 + f_2^2 + f_3^2 \right)^{-1} \circ \bar{F} = l_0 + l_1 i + l_2 j + l_3 k; \quad l_0, l_1, l_2, l_3 \in R'/Q$$

$$F_p^{-1} = \left(f_0^2 + f_1^2 + f_2^2 + f_3^2 \right)^{-1} \circ \bar{F} = s_0 + s_1 i + s_2 j + s_3 k; \quad s_0, s_1, s_2, s_3 \in R'_p.$$

A necessary issue in public key generation is to choose a quaternion $W = w_0 + w_1 \cdot i + w_2 \cdot j + w_3 \cdot k$ in $\mathbb{L}_q = \left(\frac{1,1}{\mathbb{Z}_q} \right)$, such that W be invertible over $\mathbb{L}_q$ and $w_0, w_1, w_2, w_3 \neq 0$. This quaternion prevents the leakage of public key information. Then we compute $\tilde{H} = F^{-1} \circ G + \vartheta \pmod{q}$ where $F \circ F^{-1} = F^{-1} \circ F = 1 \pmod{J}$ and $\vartheta = W \circ \sigma \in J_q$ is unknown to the attacker. The quaternion

$$\tilde{H} = F^{-1} \circ G + \vartheta \pmod{q}, \tag{6}$$

is the public key in our cryptosystem. The modulo q operation is componentwise, it means that the corresponding quaternion of $F^{-1} \circ G + \vartheta$ in $\mathbb{A}_q$ that is $(h_0(\text{mod } q)) + (h_1(\text{mod } q))i + (h_2(\text{mod } q))j + (h_3(\text{mod } q))k$ is considered as the public key $\tilde{H}$. The coefficient vectors $\overrightarrow{h_i(\text{mod } q)}$'s, for $i = 0, \ldots, 3$, denote the public key $\tilde{H}$. Therefore, the memory needed to store the public key $\tilde{H}$ is equal to $4n^2 \lceil \log_2 q \rceil$ bits.

We have that $F \circ F^{-1} = F^{-1} \circ F = 1 + \alpha \circ \sigma \pmod{q}$, where $\alpha \in \mathbb{A}$ is unknown to the attacker. Therefore, multiplying Eq. (6) by F implies that

$$\begin{aligned} F \circ \tilde{H} &= F \circ F^{-1} \circ G + F \circ \vartheta \pmod{q} \\ &= (1 + \alpha \circ \sigma) \circ G + F \circ \vartheta \pmod{q} \\ &= G + \sigma \circ \alpha \circ G + F \circ \vartheta \pmod{q} \\ &= G + \gamma \pmod{q}. \end{aligned}$$

Thus,

$$F \circ \tilde{H} = G + \gamma \pmod{q}, \tag{7}$$

$$\gamma = \sigma \circ \alpha \circ G + F \circ \vartheta, \tag{8}$$

where $\gamma \in J_q$. Subsequently, the private key consists of $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$, where $\overrightarrow{\rho(\gamma)} = \left(\rho(\gamma_0), \ldots, \rho(\gamma_3) \right)$.

Using Lemma 1, we have

$$\rho(\sigma) = \left(q_1, \ldots, q_{|T|}, 0, \ldots, 0 \right), \tag{9}$$

$$\rho(G) = \left(0, \ldots, 0, G(a_{|T|+1}, b_{|T|+1}), \ldots, G(a_{n^2}, b_{n^2}) \right), \tag{10}$$

$$\rho(\vartheta) = \left(q_1 W, \ldots, q_{|T|} W, 0, \ldots, 0 \right). \tag{11}$$

Therefore,

$$\begin{aligned}
\rho(\gamma) &= \rho(\sigma \circ \alpha \circ G) + \rho(F \circ \vartheta) \\
&= (0, \ldots, 0) + \rho(F \circ \vartheta) \\
&= \rho(F \circ \vartheta).
\end{aligned} \tag{12}$$

3.2 Encryption

To encrypt the incoming data m, we convert it into a quaternion having four small polynomials. We map m to a quaternion $M = m_0 + m_1 i + m_2 j + m_3 k \in \mathbb{A}$, where $m_i \in L_m$, for $i = 0, \ldots, 3$. The incoming data can be generated from the same or four different sources. Then, the data is transformed into the quaternion M. After that, we pick a random quaternion $\Phi = \phi_0 + \phi_1 i + \phi_2 j + \phi_3 k$ such that $\phi_i \in L_\phi$, for $i = 0, \ldots, 3$. The encrypted message is

$$C = p\tilde{H} \circ \Phi + M \pmod{q}.$$

In this cryptosystem we can set up to four messages at once and encrypt them simultaneously as one quaternion and transmit it as the ciphertext. Encryption and key generation need one quaternion multiplication including 16 convolution multiplications but we show that the multiplication of two quaternions of $\mathbb{A}_q$ is equivalent to a multiplication of their equivalent 2×2-matrices over the the ring R'_q. Moreover, by Strassen method [38] the multiplication of two quaternions is possible with only seven convolutional multiplications.

Since each quaternion in our cryptosystem is a 4-tuple vector of integers and since we use bivariate polynomials, an instance of BQTRU with the parameters (n, p, q) is comparable with an instance of NTRU with the public parameters $(4n^2, p, q)$. We believe this is a fair comparison between NTRU and our system.

We note that the number of multiplication operations in a convolutional product of two polynomials using standard arithmetic with degree $n - 1$ is equal to n^2. Therefore, if we consider NTRU with the public parameters $(4n^2, p, q)$, the number of multiplication operations in encryption and key generation is $(4n^2)^2 = 16n^4$. While, the multiplication of two quaternions in our encryption and key generation process needs only 7 convolutional multiplications in R'_q. Therefore, the number of multiplication operations in key generation and encryption of our cryptosystem with dimension n is $7n^4$. Hence, if we apply Strassen method in our cryptosystem, the key generation and encryption process is $16/7$ times faster than NTRU with dimension comparable parameters.

3.3 Decryption

Let $C \in \mathbb{A}_q$ be the received ciphertext. In order to decrypt it, a receiver first computes

$$F \circ C \pmod{q}.$$

Then she finds the closest vector B to $F \circ C$ in the private lattice Λ_{private}. If we choose the public parameters carefully, then $V = F \circ C - B$ is a quaternion with integer coefficients, and the receiver recovers the message by computing

$$F_p^{-1} \circ V \pmod{q}.$$

The decryption works since

$$
\begin{aligned}
F \circ C &= F \circ (p\tilde{H} \circ \Phi + M) \pmod{q} \\
&= pF \circ \tilde{H} \circ \Phi + F \circ M \pmod{q} \\
&= p(G + \gamma) \circ \Phi + F \circ M \pmod{q} \\
&= pG \circ \Phi + p\gamma \circ \Phi + F \circ M \pmod{q} \\
&= pG \circ \Phi + F \circ M + (p\gamma \circ \Phi + \varepsilon q) \\
&= pG \circ \Phi + F \circ M + B,
\end{aligned}
$$

where $\varepsilon \in \mathbb{A}$ and $B = (p\alpha \circ G \circ \Phi + pF \circ W \circ \Phi) \circ \sigma + \varepsilon q \in J$ is unknown to the receiver. The quaternion $pG \circ \Phi + F \circ M \in \mathbb{A}_q$ should be found in order to make the process feasible. To this end, we find $B \in J$ and after that we subtract it from $F \circ C = pG \circ \Phi + F \circ M + B$. Then, the process continues in the same fashion as in the NTRU decryption method.

Considering the vector representation, we have $\overrightarrow{F \circ C} = \overrightarrow{pG \circ \Phi + F \circ M} + \overrightarrow{B}$. We show that $\overrightarrow{B} \in \Lambda_{\text{private}}$, is the closest vector of Λ_{private} to $\overrightarrow{F \circ C}$: the vector $\overrightarrow{B}$ is a integer linear combination of the rows of the generator matrix M_{private} which consist of some of $\overrightarrow{\lambda_{a,b}}$'s. We observe that, the polynomials $\lambda_{a,b}$ have many monomials with large coefficients. So, the Euclidean norm of the vectors $\overrightarrow{\lambda_{a,b}}$ and $\overrightarrow{B}$ (as integer linear combination of $\overrightarrow{\lambda_{a,b}}$'s) is very large. Moreover, since F, G, Φ and M are small ternary quaternion polynomials, that is, they have few coefficients that are equal to 1 and -1, the Euclidean norm of $\overrightarrow{F}, \overrightarrow{G}, \overrightarrow{\Phi}$ and $\overrightarrow{M}$ is small. Therefore, the Euclidean norm $\overrightarrow{pG \circ \Phi + F \circ M}$ is very small relative to the Euclidean norm of $\overrightarrow{B}$. Thus, treating $\overrightarrow{pG \circ \Phi + F \circ M}$ as a noise, $\overrightarrow{F \circ C}$ can be viewed as a perturbed lattice point $\overrightarrow{B}$ with small noise vector and $\overrightarrow{B}$ is, with high probability, the closest vector of Λ_{private} to $\overrightarrow{F \circ C}$.

Due to the structure of the private lattice Λ_{private} and the probabilistic property of the noise vector, it is easy to find the CVP in Λ_{private}. More information about this can be found in Sect. 4.

If we choose suitable public parameters for our cryptosystem, the coefficients of the four polynomials in $pG \circ \Phi + F \circ M$ lie in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$ and decryption does not fail. Then, we can reduce $pG \circ \Phi + F \circ M$ modulo p and the term $pG \circ \Phi$ vanishes. Hence, the message M is recovered by multiplying $F \circ M \pmod{p}$ by F_p^{-1} from the left side.

The decryption phase of our cryptosystem, with dimension n, needs to calculate 14 convolution products instead of 32 in NTRU cryptosystem with dimension $4n^2$. The legitimate receiver should solve a CVP in the private lattice Λ_{private} and this makes the decryption process of our cryptosystem to be slower than NTRU. However, the presence of the private ideal makes our cryptosystem to be secure against lattice based attacks; this is explained in Sect. 5.

4 Successful decryption

It is important that the public parameters in the cryptosystem be chosen in such a way that the probability of decryption failure is very small (e.g., 2^{-80}) [19]. The decryption process is successful if the closest vector to $F \circ C = pG \circ \Phi + F \circ M + B$ is found correctly and all quaternion coefficients of $V = pG \circ \Phi + F \circ M$ lie in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$.

Kouzmenko [25] demonstrates the validity of a simple probabilistic model for the coefficients of the corresponding polynomial in the NTRU cryptosystem. Using this model, we estimate the probability distribution of the coefficients of the polynomials in the quaternion

$V = v_0 + v_1 i + v_2 j + v_3 k$, under certain reasonable hypotheses. Therefore, by using similar computations as in [28], we have

$$E(v_{i,j}) = 0, \tag{13}$$

$$\text{Var}(v_{i,j}) = \frac{16p^2 d_\phi d_g}{n^2} + \frac{4d_f(p^2 - 1)}{6}, \tag{14}$$

for $i = 0, \ldots, 3$ and $j = 0, \ldots, n^2 - 1$. This together with the assumption that the $v_{i,j}$s have Gaussian distribution with zero mean and standard deviation $\theta = \sqrt{\frac{16p^2 d_\phi d_g}{n^2} + \frac{4d_f(p^2-1)}{6}}$, gives

$$Pr\left(|v_{i,j}| \leq \frac{q-1}{2}\right) = 2\Phi\left(\frac{q-1}{2\theta}\right) - 1,$$

for $i = 0, \ldots, 3$ and $j = 0, \ldots, n^2 - 1$, where Φ is the normal cumulative distribution function. Thus, the probability for all coefficients of V lying in the interval $[-\frac{q-1}{2}, \frac{q-1}{2}]$, is determined as

$$\left(2\Phi\left(\frac{q-1}{2\theta}\right) - 1\right)^{4n^2}.$$

Another reason for unsuccessful decryption is failing to estimate the vector B from $V' := F \circ C = V + B$. Finding B involves solving a CVP in the private lattice Λ_{private}. In general, CVP is an NP-hard problem and the computational complexity of the algorithms for finding the closest vector of a lattice to an arbitrary vector is intractable, however it is tractable in our special case which is described in the sequel.

We note that the closest vector problem is equivalent to the integer least-squares (ILS) problem which is the problem of finding the least-squares solution to a system of linear equations where the unknown vector is comprised of integers, but the matrix coefficient and given vector are comprised of real numbers. Lifting $V' = v_0' + v_1' i + v_2' j + v_3' k$ from $\mathbb{A}/J$ into $\mathbb{A}$ involves solving the CVP problem or the ILS problem in Λ_{private} with the generator matrix M_{private} presented in Eq. (5):

$$\underset{z \in \mathbb{Z}^{4n^2}}{\text{Argmin}} \left\| \overrightarrow{V'} - z M_{\text{private}} \right\|^2 = \sum_{i=0}^{3} \underset{z_i \in \mathbb{Z}^{n^2}}{\text{Argmin}} \left\| \overrightarrow{v_i'} - z_i D' \right\|^2. \tag{15}$$

As argued in the previous section, the ideal Q can be viewed as an n^2 dimensional lattice Λ_Q generated by the matrix D'. Therefore, this step of our decryption involves solving four CVP's in dimension n^2. Indeed, our problem is equivalent to finding the closest lattice point in Λ_Q to the given point $\overrightarrow{v_i'}$ in Eq. (15), for $i = 0, \ldots, 3$, that has been perturbed by an additive noise vector $\overrightarrow{v_i}$, where $(\overrightarrow{v_0}, \overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}) = \overrightarrow{V} = \overrightarrow{pG \circ \Phi + F \circ M}$.

Our highest level of security occurs in $n \geq 11$ ($n^2 \geq 121$). There exist less complex methods for computing CVP in such small dimensions. One of the prominent methods is sphere decoding that searches for the closest lattice point within a given hyper sphere [17,39]. The sphere decoding is feasible in small dimensions, typically in dimensions less than 130 [37]. By applying some techniques (like LLL lattice reduction algorithm), the complexity of this algorithm can be decreased [1].

We observe that $\overrightarrow{V}$ has Gaussian distribution with zero mean and variance given in Eq. (14). We show in a numerical example that the variance of this additive noise is small for an optimal decoder like sphere decoder. In the rest of this subsection, it is discussed that

in our case, the expected complexity of the sphere decoding algorithm is polynomial in the dimension of the lattice Λ_Q. Furthermore, since the dimension of Λ_Q in the highest security level is 121, which is less that 130, solving the CVP problems in our decryption process are feasible.

We use the Poltyrev limit [34] to know the amount of the maximum variance of the additive Gaussian noise under which a maximum-likelihood decoder like sphere decoder results in a correct estimation of a desired lattice vector. Indeed, Poltyrev proved that there exists a lattice Λ, with basis matrix L and large enough dimension N, such that decoding is possible with arbitrarily small error probability if and only if the variance of the additive noise vector is smaller than

$$\sigma_{\max}^2 := \frac{\left(\text{vol}(\Lambda)\right)^{\frac{2}{N}}}{2\pi e},$$

where $\text{vol}(\Lambda) = |\det L|$.

If a lattice point is perturbed by a Gaussian noise with zero mean and variance σ^2, which is smaller than $\sigma_{\max}^2$, the CVP problem can be solved in polynomial (or even cubic) time using sphere decoding algorithm [17]. Indeed, the error probability of the sphere decoding algorithm and its complexity are related to the variance of the additive noise. When the variance of the additive noise is much smaller than $\sigma_{\max}^2$, the error probability of the sphere decoding algorithm approaches zero and the algorithm returns the correct estimation for a desired lattice vector. In this case, the complexity of the sphere decoding algorithm is polynomial in the dimension of the lattice, which is reasonable and affordable in small dimensions (typically less than 130).

According to the basis of Λ_Q, $\text{vol}(\Lambda_Q) = |\det D'| > q^{n^2 - |T|}$ and a lower bound for $\sigma_{\max}^2$ is estimated as

$$\sigma_{\max}^2 > \frac{q^{\frac{2(n^2 - |T|)}{n^2}}}{2\pi e} = \frac{q^{2\left(1 - \frac{|T|}{n^2}\right)}}{2\pi e}.$$

We have assumed that $|T| \leq n$, therefore $\sigma_{\max}^2 > \frac{q^{2\left(1 - \frac{1}{n}\right)}}{2\pi e}$. For the dimension $n = 11$, the highest level of security in our cryptosystem, $\sigma_{\max}^2 > 885$, while the variance of the additive noise, $\text{Var}(v_i) \approx 263$, for $i = 0, \ldots, 3$.

Since $|T|$ is chosen very small compared to n^2, the variance of the vectors v_i's is much smaller than $\sigma_{\max}^2$. Also, the dimension of the lattice Λ_Q in our highest level of security is $n^2 = 121 < 130$. Hence, if a legitimate receiver which has generator matrix D', uses the sphere decoding algorithm, then solves the CVP in the decryption process with negligible error probability and affordable complexity and continues the decryption.

4.1 Parameter selection and comparisons

In BQTRU cryptosystem, we consider $p \neq 2$ since the probability of invertibility F modulo $p = 2$ is too low. The initial condition $n|(q - 1)$ is required. Since a primitive k-th root of unity does not always exist modulo q, it is necessary to work in an extension ring. The condition $n|(q - 1)$ yields the factorization of $x^n - 1$ into linear factors in $\mathbb{Z}_q$. Then, E is a set of elements of $\mathbb{Z}_q \times \mathbb{Z}_q$ which has maximum cardinality n^2. The subsets $T \subseteq E$ are chosen such that $|T|$ is small compared to n^2 (e.g. $|T| < n$). Therefore, the number of small subsets $T \subseteq E$ that can be selected is approximately equal to $\sum_{i=1}^{n} \binom{n^2}{i}$. Then, the number of ideals Q_q generated by $\sigma(x, y) = \sum_{i=1}^{|T|} q_i \lambda_{a_i, b_i}(x, y)$ that can be used for decryption is

$$\sum_{i=1}^{n}(q-1)^i\binom{n^2}{i}.$$

For this reason, an exhaustive search for the ideal Q_q containing $\langle x^n - 1, y^n - 1 \rangle$ in $\mathbb{Z}_q[x, y]$ is infeasible when n is large enough. The large number of these ideals enhances the security of the cryptosystem against brute force attack.

The security of the NTRU cryptosystem depends on the size of all polynomials f, g, r, m and h. Since finding the private key (f, g) leads to solving SVP in the NTRU lattice [11], when the sizes of f and g increase (d_f and d_g increase), the security of the private key enhances. On the other hand, obtaining the message m leads to finding CVP in the NTRU lattice [15] and then if the sizes of m and r increase (d_m and d_r increase), the security of the message enhances. Therefore, increasing the size of f, g, r and m is reasonable for enhancing the security of NTRU but by increasing the size of f, g, r and m, the expected size of $p.g * r + f * m$ is increased and then the probability of decryption failure is relatively increased. Hence, there is a tradeoff between the message security and the key security; we can not increase the size of the private key f, g (for the key security) and the polynomials m and r (for the message security), simultaneously.

In the proposed scheme, the presence of Q allows us to reduce the size of F and G (that is, the size of f_i's and g_i's, for $i = 0, \ldots, 3$) without detracting from the private key's security. This enables us to increase the sizes of Φ and M (increase d_ϕ and d_m) without increasing the probability of decryption failure. In this sense, the proposed scheme is more robust against message attacks than NTRU.

The decryption of NTRU is impractical when the sizes of the private keys are large while in BQTRU, the decryption with small sizes of F and G is impossible when $|T|$ is large.

The parameter sets in Table 1, are chosen sufficiently large to eliminate the possibility of decryption failure. Namely, if we pick $d_f = d_g = d_\phi = d_m = d$, since all polynomials in $V = pG \circ \Phi + F \circ M$ are ternary, their coefficients have maximum value equal to $2(6d+1)p$. It follows that no coefficient of V can exceed $2(6d+1)p$ in absolute value and the decryption is guaranteed to be successful if $2(6d+1)p < q/2$ or $q > 4(6d+1)p$. Therefore, decryption is successful if $q > 24dp$ approximately and since $d \approx n^2/7$, then $q > 24pn^2/7$ is sufficient condition for the successful decryption in our cryptosystem. However, an examination of the computation of the maximum coefficient of V shows that decryption is likely to succeed even for considerably smaller values of q. Therefore, similar to the NTRU cryptosystem, for additional efficiency and to reduce the size of the public key, it may be advantageous to choose a smaller value of q.

In the NTRU cryptosystem with parameters (n, q', p), which was introduced in Sect. 2.1, we state that if $q' > (6d+1)p$ or $q' > 2np$ (when we select $d \approx n/3$), then decryption never fails. Hence for the NTRU cryptosystem with parameter sets $(4n^2, q', p)$, if $q' > 8n^2p$, it has no decryption failure. It implies that $q/q' \approx 3/7$. Therefore, choosing the prime number q such that $n|(q-1)$ and $q \approx \frac{3}{7}q'$, provides (n, q, p)-BQTRU with an equivalent level of protection against decryption failure as $(4n^2, q', p)$-NTRU. We summarize our results about the parameter's selection in Table 1 given at the end of Sect. 5.

5 Security analysis

In this section, we discuss the key security and the message security of our cryptosystem. We prove that the security of the proposed cryptosystem relies on the hardness of SVP in a

certain type of lattice. We show that our cryptosystem is secure against lattice based attacks due to the specific structure of its lattice.

We recall that the convolution multiplication of two polynomials f and h in $R = \mathbb{Z}[x]/\langle x^n - 1 \rangle$ is equivalent to the matrix multiplication of the coefficient vector $\overrightarrow{f}$ and the circulant matrix $\mathscr{H}$ of the coefficient vector $\overrightarrow{h}$. This matrix is not circulant when f and h belong to $R' = \mathbb{Z}[x, y]/\langle x^n - 1, y^n - 1 \rangle$. It can be shown that each row of $\mathscr{H}$ is a permutation of the coefficient vector $\overrightarrow{h}$ and these permutations are related to the monomial order that we have used for R'. Consequently, the convolution product of two polynomials f and h in the proposed cryptosystem is also equivalent to the matrix multiplication $\overrightarrow{f} \mathscr{H}$, where $\mathscr{H}$ is a matrix such that its rows are a permutation of the coefficient vector $\overrightarrow{h}$.

In the sequel, we explain how the key recovery of our cryptosystem is formulated as a shortest vector problem in a certain special form of a lattice.

The parameters n, p, q, d_f, d_g, d_ϕ and the public key $\tilde{H} = F^{-1} \circ G + \vartheta$, where $F \circ F^{-1} = F^{-1} \circ F = 1 \pmod{J}$, are known to the attacker. For key recovery, the attacker should find a vector $(G, F, -\rho(\gamma))$ which satisfies the equation $F \circ \tilde{H} = G + \gamma \pmod{q}$. Let $F = f_0 + f_1 i + f_2 j + f_3 k$ and $\tilde{H} = h_0 + h_1 i + h_2 j + h_3 k$, where f_i and h_i are polynomials in the ring R', for $i = 0, \ldots, 3$. Then

$$
\begin{aligned}
F \circ \tilde{H} &= (f_0 + f_1 i + f_2 j + f_3 k) \circ (h_0 + h_1 i + h_2 j + h_3 k)) \\
&= (f_0 * h_0 + f_1 * h_1 + f_2 * h_2 - f_3 * h_3) \\
&\quad + (f_0 * h_1 + f_1 * h_0 + f_2 * h_3 - f_3 * h_2) i \\
&\quad + (f_0 * h_2 - f_1 * h_3 + f_2 * h_0 + f_3 * h_1) j \\
&\quad + (f_0 * h_3 + f_1 * h_2 - f_2 * h_1 + f_3 * h_0) k.
\end{aligned}
$$

If we expand the quaternion equation $F \circ \tilde{H} = G + \gamma \pmod{q}$ for a given quaternion $\tilde{H}$, then we have a system of linear equations

$$
\begin{cases}
f_0 * h_0 + f_1 * h_1 + f_2 * h_2 - f_3 * h_3 - \gamma_0 = g_0 + q u_0, \\
f_0 * h_1 + f_1 * h_0 + f_2 * h_3 - f_3 * h_2 - \gamma_1 = g_1 + q u_1, \\
f_0 * h_2 - f_1 * h_3 + f_2 * h_0 + f_3 * h_1 - \gamma_2 = g_2 + q u_2, \\
f_0 * h_3 + f_1 * h_2 - f_2 * h_1 + f_3 * h_0 - \gamma_3 = g_3 + q u_3,
\end{cases}
\tag{16}
$$

where $u_0, u_1, u_2, u_3 \in R'$. We consider

$$
\tilde{\mathscr{H}} = \begin{bmatrix}
\mathscr{H}_0 & \mathscr{H}_1 & \mathscr{H}_2 & \mathscr{H}_3 \\
\mathscr{H}_1 & \mathscr{H}_0 & -\mathscr{H}_3 & \mathscr{H}_2 \\
\mathscr{H}_2 & \mathscr{H}_3 & \mathscr{H}_0 & -\mathscr{H}_1 \\
-\mathscr{H}_3 & -\mathscr{H}_2 & \mathscr{H}_1 & \mathscr{H}_0
\end{bmatrix},
$$

where $\mathscr{H}_i$ is the corresponding matrix of $\overrightarrow{h_i} = [h_{i0}, h_{i1}, \cdots, h_{in^2-1}]$, for $i = 0, \ldots, 3$. According to the above mentioned issues

$$
\overrightarrow{F \circ \tilde{H}} = \overrightarrow{F} \tilde{\mathscr{H}} = \begin{bmatrix} \overrightarrow{f_0} & \overrightarrow{f_1} & \overrightarrow{f_2} & \overrightarrow{f_3} \end{bmatrix}
\begin{bmatrix}
\mathscr{H}_0 & \mathscr{H}_1 & \mathscr{H}_2 & \mathscr{H}_3 \\
\mathscr{H}_1 & \mathscr{H}_0 & -\mathscr{H}_3 & \mathscr{H}_2 \\
\mathscr{H}_2 & \mathscr{H}_3 & \mathscr{H}_0 & -\mathscr{H}_1 \\
-\mathscr{H}_3 & -\mathscr{H}_2 & \mathscr{H}_1 & \mathscr{H}_0
\end{bmatrix}.
$$

Therefore, when we represent the elements of $\mathbb{A}$ by their coefficient vectors in $\mathbb{Z}^{4n^2}$, the set Λ_{BQTRU} formed by the vectors $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$ that are also equivalent to the set of

all solutions (G, F, γ) to Eq. (16), forms an integer lattice. From the above equations one obtains that the BQTRU lattice, denoted by Λ_{BQTRU}, is generated by the following matrix

$$M_{\text{BQTRU}} = \begin{bmatrix} q I_{4n^2} & 0 & 0 \\ \mathscr{H} & I_{4n^2} & 0 \\ \mathfrak{D} & 0 & I_{4n^2} \end{bmatrix}, \tag{17}$$

where

$$\mathfrak{D} = \begin{bmatrix} D & 0 & 0 & 0 \\ 0 & D & 0 & 0 \\ 0 & 0 & D & 0 \\ 0 & 0 & 0 & D \end{bmatrix}.$$

and D is an $n^2 \times n^2$ matrix which consists of $\overrightarrow{\lambda_{a,b}}$, coefficient vectors of all Lagrange interpolators $\lambda_{a,b}(x, y)$, such that $(a, b) \in E$.

We now consider that the public key $\tilde{H}$ is created using the private quaternions F, G and γ and compute what happens when we multiply the M_{BQTRU} by a carefully chosen vector.

Proposition 1 *Assume that $F \circ \tilde{H} = G + \gamma \pmod{q}$, let $U \in \mathbb{A}$ be the quaternion that satisfies*

$$F \circ \tilde{H} = G + \gamma + qU. \tag{18}$$

Then

$$\left(\overrightarrow{-U}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right) M_{BQTRU} = \left(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right),$$

and therefore the vector $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$ belongs to the BQTRU lattice.

Proof When we multiply the vector $(\overrightarrow{-U}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$ by the columns of M_{BQTRU}, we have

$$\left(\overrightarrow{-U}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right) M_{BQTRU} = \left(\overrightarrow{-U}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right) \begin{bmatrix} q I_{4n^2} & 0 & 0 \\ \mathscr{H} & I_{4n^2} & 0 \\ \mathfrak{D} & 0 & I_{4n^2} \end{bmatrix}$$

$$= (-q\overrightarrow{U} + \overrightarrow{F} \mathscr{H} - \overrightarrow{\rho(\gamma)}\mathfrak{D}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)}).$$

Based on Eq. (17), we have $\overrightarrow{F} \mathscr{H} = \overrightarrow{F \circ \tilde{H}}$ and also

$$\overrightarrow{\rho(\gamma)}\mathfrak{D} = \left(\rho(\gamma_0)D, \ldots, \rho(\gamma_3)D \right)$$

$$= \left(\sum_{i=1}^{n^2} \gamma_0(a_i, b_i)\overrightarrow{\lambda_{a_i,b_i}}, \ldots, \sum_{i=1}^{n^2} \gamma_3(a_i, b_i)\overrightarrow{\lambda_{a_i,b_i}} \right)$$

$$= \left(\overrightarrow{\gamma_0}, \ldots, \overrightarrow{\gamma_3} \right) = \overrightarrow{\gamma}.$$

We obtain Eq. (18) resulting in $-qU + F \circ \tilde{H} - \gamma = G$. Thus,

$$\left(\overrightarrow{-U}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right) M_{BQTRU} = \left(\overrightarrow{-qU + F \circ \tilde{H} - \gamma}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right)$$

$$= \left(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)} \right),$$

and the private key is an integer linear combination of the rows of M_{BQTRU}. Hence,

$$\left(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)}\right) \in \Lambda_{BQTRU}.$$

$\square$

The quaternion $\gamma \in J_q$ is a linear combination of $\lambda_{a,b}$'s and therefore it may have many monomials with large coefficients. As a consequence, the Euclidean norm of $\overrightarrow{\rho(\gamma)}$ may be very large and the private key $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)}) \in \mathbb{Z}^{4n^2} \times \mathbb{Z}^{4n^2} \times \mathbb{Z}_q^{4n^2}$ may not be a short nonzero vector in the BQTRU lattice using the Euclidean norm. Thus, we consider a hybrid metric on $\mathbb{Z}^{4n^2} \times \mathbb{Z}^{4n^2} \times \mathbb{Z}_q^{4n^2}$: Euclidean on the first two components and Hamming on the third one.

Definition 4 For every $(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)}) \in \mathbb{Z}^{4n^2} \times \mathbb{Z}^{4n^2} \times \mathbb{Z}_q^{4n^2}$, the hybrid norm is defined as

$$\|(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)})\|_{hyb} := \|(\overrightarrow{G}, \overrightarrow{F})\|_2 + \|\overrightarrow{\rho(\gamma)}\|_H,$$

where $\| \cdot \|_2$ and $\| \cdot \|_H$ are the Euclidean and Hamming norms, respectively.

It can be easily shown that $\| \cdot \|_{hyb}$ has the properties of a norm. In this case, since $\rho(\gamma)$ is determined by the element of the subset T, where $|T|$ is small, the Hamming norm of $\overrightarrow{\rho(\gamma)}$ is small. Moreover, the Euclidean norm of $\overrightarrow{F}$ and $\overrightarrow{G}$ is small. Therefore, the private key is a short vector in the lattice measured by the hybrid metric. In the sequel, we present several results and show that recovering the private key can be reduced to solving an SVP in the BQTRU lattice with hybrid norm.

Lemma 6 ([12]) *Let F be an arbitrary field. Given a set $U \subset F$ of size n, then any polynomial $f(x, y) \in F[x, y]$ of degree less than n in each variable, is determined by its evaluation in $U \times U$.*

Let $U = \{b \in \mathbb{Z}_q \mid b^n = 1\}$, where the condition $n|(q-1)$ yields $|U| = n$. Then, Lemma 6 implies that any polynomial f in R' is determined by its evaluation on $U \times U = E$ or equivalently by knowing the vector $\rho(f)$.

Corollary 2 *Let f and g be two polynomials in R' such that $\rho(f) = \rho(g)$. Then, $f = g$.*

Obviously, this result is satisfied in the case that F and G are two quaternions in $\mathbb{A}$ where $\rho(F) = \rho(G)$.

We use the next lemma to show that for two fixed quaternions F and G satisfying the public key Eq. (6), the vector $\overrightarrow{\rho(\gamma)}$ has the smallest Hamming norm among all quaternions that can be chosen as the third component in the private key $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$.

Lemma 7 *Let F and G be two fixed quaternions satisfying* Eq. (6). *Then for any element $\tau' \neq \vartheta$ belonging to the set*

$$\chi = \left\{\tau' \in \mathbb{A} \mid F \circ F' = F' \circ F = 1 + \alpha' \circ \tau' \pmod q, \quad \tilde{H} = F' * G + \tau' \pmod q\right\},$$

we have $\|\overrightarrow{\rho(\tau')}\|_H > 4|T|$.

Proof We know $\tilde{H} = F^{-1} \circ G + \vartheta \pmod{q}$, where $F \circ F^{-1} = F^{-1} \circ F = 1 + \alpha \circ \sigma$ (mod q). Therefore, $F \circ F^{-1} = F^{-1} \circ F = 1 + \alpha'' \circ W \circ \sigma \pmod{q}$ too, where $\alpha'' \in \mathbb{A}$. Then, $\vartheta = W \circ \sigma \in \chi$. Using Eqs. (10) and (11), we have

$$\rho(\tilde{H}) = \rho(F^{-1}) \bullet \rho(G) + \rho(\vartheta)$$
$$= \Big(0, \ldots, 0, F^{-1}(a_{|T|+1}, b_{|T|+1}) \circ G(a_{|T|+1}, b_{|T|+1}), \ldots$$
$$\ldots, F^{-1}(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2})\Big) + \Big(q_1 W, \ldots, q_{|T|} W, 0, \ldots, 0\Big),$$

that is,

$$\rho(\tilde{H}) = \Big(q_1 W, \ldots, q_{|T|} W, F^{-1}(a_{|T|+1}, b_{|T|+1}) \circ G(a_{|T|+1}, b_{|T|+1}), \ldots$$
$$\ldots, F^{-1}(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2})\Big). \tag{19}$$

If we consider an arbitrary $\tau' \in \chi$, where $\tau' \neq \vartheta$, then

$$F \circ F' = F' \circ F = 1 + \alpha' \circ \tau' \pmod{q}, \quad \tilde{H} = F' \circ G + \tau' \pmod{q}.$$

Similarly,

$$\rho(\tilde{H}) = \rho(F') \bullet \rho(G) + \rho(\tau')$$
$$= \Big(0, \ldots, 0, F'(a_{|T|+1}, b_{|T|+1}) \circ G(a_{|T|+1}, b_{|T|+1}), \ldots$$
$$\ldots, F'(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2})\Big) + \rho(\tau').$$

As a result $\tau'(a_i, b_i) = q_i W \neq 0$, for $i = 1, \ldots, |T|$. On the other hand, $\tau' \neq \vartheta$ and $F'(a_i, b_i) \circ G(a_i, b_i) \neq F^{-1}(a_i, b_i) \circ G(a_i, b_i)$ for some $i = |T| + 1, \ldots, n^2$. Therefore, $\rho(\tau')$ should be nonzero on at least one of the $n^2 - |T|$ last positions. Hence $\|\overrightarrow{\rho(\tau')}\|_H > 4|T|$. $\qquad\square$

Proposition 2 *Let F and G be two fixed quaternions satisfying Eq. (6). Then, $\vartheta = W \circ \sigma$ has the smallest Hamming norm in χ. Also, for any $\tau' \in \chi$ such that $\tau' \neq \vartheta$*

$$\|\overrightarrow{\rho(F \circ \tau')}\|_H \geq \|\overrightarrow{\rho(F \circ \vartheta)}\|_H,$$

where, in accordance with Eq. (12), we have $\overrightarrow{\rho(\gamma)} = \overrightarrow{\rho(F \circ \vartheta)}$.

Proof Since $\vartheta \in \chi$ and $\|\overrightarrow{\rho(\vartheta)}\|_H = 4|T|$ (according to Eq. (11)), then ϑ has the smallest Hamming norm in χ. Let $\tau' \in \chi$, where $\tau' \neq \vartheta$. Then, we have

$$F \circ F' = F' \circ F = 1 + \alpha' \circ \tau' \pmod{q}, \quad \tilde{H} = F' \circ G + \tau' \pmod{q}.$$

Therefore,

$$F \circ \tilde{H} = G + (\alpha' \circ \tau' \circ G + F \circ \tau') \pmod{q}.$$

Moreover, $\tilde{H} = F^{-1} \circ G + \vartheta \pmod{q}$ and by considering Eqs. (7) and (8), we have

$$F \circ \tilde{H} = G + \gamma \pmod{q},$$

where $\gamma = (\sigma \circ \alpha \circ G + F \circ \vartheta)$. Thus,

$$\alpha' \circ \tau' \circ G + F \circ \tau' = \sigma \circ \alpha \circ G + F \circ \vartheta,$$
$$\rho(\alpha' \circ \tau' \circ G + F \circ \tau') = \rho(\sigma \circ \alpha \circ G + F \circ \vartheta),$$
$$\rho(\alpha' \circ \tau' \circ G) + \rho(F \circ \tau') = \rho(F \circ \vartheta),$$
$$\rho(F \circ \tau') = \rho(F \circ \vartheta) - \rho(\alpha' \circ \tau' \circ G).$$

Hence, we can conclude that

$$\|\overrightarrow{\rho(F \circ \tau')}\|_H \geq \|\overrightarrow{\rho(F \circ \vartheta)}\|_H.$$

$\square$

An important consequence of this proposition is that for fixed quaternions F and G that satisfy Eq. (6), $\vartheta \in \chi$ is the best choice in the public key Eq. (6) and $\overrightarrow{\rho(\gamma)} = \overrightarrow{\rho(F \circ \vartheta)}$ has the smallest Hamming norm among all quaternions that can be chosen as the third component in the solution of the public key equation. Consequently, $\| \overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(F \circ \vartheta)}\|_{hyb} < \| \overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(F \circ \tau')}\|_{hyb}$, for any $\tau' \in \chi$.

In the following theorem which is the most important result of this section, we prove that any reduction in the Hamming norm of the third component of a solution of the public key Eq. (6) like $(\overrightarrow{G''}, \overrightarrow{F''}, \overrightarrow{\rho(F'' \circ \tau'')})$, where $\tilde{H} = F''^{-1} \circ G'' + \tau''$ (mod q) and $F'' \circ F''^{-1} = F''^{-1} \circ F'' = 1 + \alpha'' \circ \tau''$ (mod q), results in a considerable increase in the hybrid norm of the solution $(\overrightarrow{G''}, \overrightarrow{F''}, \overrightarrow{\rho(F'' \circ \tau'')})$.

Theorem 4 *Assume that there exist $F'', G'' \in \mathbb{A}$ and $\tau'' \in J_q$ such that $\tilde{H} = F''^{-1} \circ G'' + \tau''$ (mod q), $F'' \circ F''^{-1} = F''^{-1} \circ F'' = 1 + \alpha'' \circ \tau''$ (mod q), for some $\alpha'' \in \mathbb{A}$ (that is, they are a solution of the public key equation) and $\|\overrightarrow{\rho(\tau'')}\|_H < \|\overrightarrow{\rho(\vartheta)}\|_H$. Then*

$$\left\| \overrightarrow{G''}, \overrightarrow{F''}, \overrightarrow{\rho(F'' \circ \tau'')} \right\|_{hyb} > \left\| \overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(F \circ \vartheta)} \right\|_{hyb}.$$

Proof Let $supp(F) = \{(a, b) \in E \mid F(a, b) \neq 0\}$, for any $F \in \mathbb{A}$. Using Eq. (11), we have $|supp(\vartheta)| = |T|$. Without loss of generality we consider that $|supp(\tau'')| = |T|-1$ and $\rho(\tau'')$ is nonzero over the first $|T|-1$ positions. Similar to the initial considerations that we presented for private key and public key in our proposed scheme, if $F'' = f_0'' + f_1''i + f_2''j + f_3''k$ and $G'' = g_0'' + g_1''i + g_2''j + g_3''k$ in $\mathbb{A}$ and $\tau'' \in J_q$ are a solution of the public key Eq. (6) for given public key $\tilde{H}$, then

$$\tilde{H} = F''^{-1} \circ G'' + \tau'' \text{ (mod } q),$$
$$F'' \circ F''^{-1} = F''^{-1} \circ F'' = 1 + \alpha'' \circ \tau'' \text{ (mod } q), \qquad (20)$$

where,

$$supp(\tau'') = \bigcap_{i=0}^{3} \{(a, b) \in E \mid g_i''(a, b) = 0\},$$
$$\{(a, b) \in E \mid N(F'')(a, b) = 0\} \subset supp(\tau'').$$

Therefore,

$$\begin{aligned}
\rho(\tilde{H}) &= \rho(F''^{-1}) \bullet \rho(G'') + \rho(\tau'') \\
&= \Big(0, \ldots, 0, F''^{-1}(a_{|T|}, b_{|T|}) \circ G''(a_{|T|}, b_{|T|}), \ldots, F''^{-1}(a_{n^2}, b_{n^2}) \circ G''(a_{n^2}, b_{n^2})\Big) \\
&\quad + \Big(\tau''(a_1, b_1), \ldots, \tau''(a_{|T|-1}, b_{|T|-1}), 0, \ldots, 0\Big) \\
&= \Big(\tau''(a_1, b_1), \ldots, \tau''(a_{|T|-1}, b_{|T|-1}), F''^{-1}(a_{|T|}, b_{|T|}) \circ G''(a_{|T|}, b_{|T|}), \ldots \\
&\quad \ldots, F''^{-1}(a_{n^2}, b_{n^2}) \circ G''(a_{n^2}, b_{n^2})\Big).
\end{aligned}$$

On the other hand, Eq. (19) gives

$$\begin{aligned}
\rho(\tilde{H}) &= \Big(q_1 W, \ldots, q_{|T|} W, F^{-1}(a_{|T|+1}, b_{|T|+1}) \circ G(a_{|T|+1}, b_{|T|+1}), \ldots \\
&\quad \ldots, F^{-1}(a_{n^2}, b_{n^2}) \circ G(a_{n^2}, b_{n^2})\Big).
\end{aligned}$$

Thus, we obtain

$$\tau''(a_i, b_i) = q_i W = \vartheta(a_i, b_i), \quad i = 1, \ldots, |T| - 1; \tag{21}$$
$$F''^{-1}(a_{|T|}, b_{|T|}) \circ G''(a_{|T|}, b_{|T|}) = q_{|T|} W, \quad i = |T|; \tag{22}$$
$$F''^{-1}(a_i, b_i) \circ G''(a_i, b_i) = F^{-1}(a_i, b_i) \circ G(a_i, b_i), \quad i = |T| + 1, \ldots, n^2. \tag{23}$$

Therefore, $\vartheta = \tau'' + (q_{|T|} W) \circ \lambda_{a_{|T|}, b_{|T|}}$ and $\tilde{H} = F^{-1} \circ G + \tau'' + (q_{|T|} W) \circ \lambda_{a_{|T|}, b_{|T|}}$ (mod q). As a result

$$F''^{-1} \circ G'' = F^{-1} \circ G + (q_{|T|} W) \circ \lambda_{a_{|T|}, b_{|T|}}. \tag{24}$$

We can consider

$$F''^{-1} = F^{-1} + \sum_{i=1}^{n^2} \Big(F''^{-1}(a_i, b_i) - F^{-1}(a_i, b_i)\Big) \circ \lambda_{a_i, b_i},$$
$$G'' = G + \sum_{i=1}^{n^2} \Big(G''(a_i, b_i) - G(a_i, b_i)\Big) \circ \lambda_{a_i, b_i},$$

since by Lemma 6 they are equal over the set E. Next,

$$\begin{aligned}
F''^{-1} \circ G'' &= F^{-1} \circ G + \sum_{i=1}^{n^2} \Big(F''^{-1}(a_i, b_i) \circ G''(a_i, b_i) - F^{-1}(a_i, b_i) \circ G(a_i, b_i)\Big) \circ \lambda_{a_i, b_i} \\
&= F^{-1} \circ G + \sum_{i=|T|+1}^{n^2} \Big(F''^{-1}(a_i, b_i) \circ G''(a_i, b_i) - F^{-1}(a_i, b_i) \circ G(a_i, b_i)\Big) \circ \lambda_{a_i, b_i} \\
&\quad + \Big(F''^{-1}(a_{|T|}, b_{|T|}) \circ G''(a_{|T|}, b_{|T|})\Big) \circ \lambda_{a_{|T|}, b_{|T|}} \\
&= F^{-1} \circ G + \sum_{i=|T|+1}^{n^2} \Big(F''^{-1}(a_i, b_i) \circ G''(a_i, b_i) - F^{-1}(a_i, b_i) \circ G(a_i, b_i)\Big) \circ \lambda_{a_i, b_i} \\
&\quad + \Big(q_{|T|} W\Big) \circ \lambda_{a_{|T|}, b_{|T|}}.
\end{aligned}$$

From the last equation and Eq. (24) we have

$$\sum_{i=|T|+1}^{n^2} \Big(F''^{-1}(a_i, b_i) \circ G''(a_i, b_i) - F^{-1}(a_i, b_i) \circ G(a_i, b_i)\Big) \circ \lambda_{a_i, b_i} = 0,$$

that is, $F''^{-1}(a_i, b_i)$ and $G''(a_i, b_i)$ satisfy Eq. (23). Without loss of generality, we take $F''^{-1}(a_i, b_i) = F^{-1}(a_i, b_i)$ and $G''(a_i, b_i) = G(a_i, b_i)$, for $i = |T| + 1, \ldots, n^2$, then

$$F''^{-1} = F^{-1} + \sum_{i=1}^{|T|} \left(F''^{-1}(a_i, b_i) - F^{-1}(a_i, b_i) \right) \circ \lambda_{a_i, b_i}, \tag{25}$$

$$G'' = G + \sum_{i=1}^{|T|} \left(G''(a_i, b_i) - G(a_i, b_i) \right) \circ \lambda_{a_i, b_i}. \tag{26}$$

Next, we prove that

$$F'' = F + \sum_{i=1}^{|T|} \left(F''(a_i, b_i) - F(a_i, b_i) \right) \circ \lambda_{a_i, b_i}. \tag{27}$$

Indeed, we show that F'' as above satisfies the equation $F'' \circ F''^{-1} = F''^{-1} \circ F'' = 1 + \theta \circ \tau''$ (mod q), where $\theta \in \mathbb{A}$. We know $F \circ F^{-1} = F^{-1} \circ F = 1 + \beta \circ \vartheta$ (mod q), for some $\beta \in \mathbb{A}$. Therefore, in accordance to Eqs. (20) and (21), we have

$$F'' \circ F''^{-1}$$
$$= F \circ F^{-1} + \sum_{i=1}^{|T|} \left(F''(a_i, b_i) \circ F''^{-1}(a_i, b_i) - F(a_i, b_i) \circ F^{-1}(a_i, b_i) \right) \circ \lambda_{a_i, b_i}$$
$$= 1 + \beta \circ \vartheta + \left(F''(a_{|T|}, b_{|T|}) \circ F''^{-1}(a_{|T|}, b_{|T|}) \right.$$
$$\left. - F(a_{|T|}, b_{|T|}) \circ F^{-1}(a_{|T|}, b_{|T|}) \right) \circ \lambda_{a_{|T|}, b_{|T|}}$$
$$+ \sum_{i=1}^{|T|-1} \left(F''(a_i, b_i) \circ F''^{-1}(a_i, b_i) - F(a_i, b_i) \circ F^{-1}(a_i, b_i) \right) \circ \lambda_{a_i, b_i}$$
$$= 1 + \beta \circ \vartheta + \left(1 - \left(1 + \beta(a_{|T|}, b_{|T|}) \circ \vartheta(a_{|T|}, b_{|T|}) \right) \circ \lambda_{a_{|T|}, b_{|T|}} \right)$$
$$+ \sum_{i=1}^{|T|-1} \left(\left(1 + \alpha''(a_i, b_i) \circ \tau''(a_i, b_i) \right) - \left(1 + \beta(a_i, b_i) \circ \vartheta(a_i, b_i) \right) \right) \circ \lambda_{a_i, b_i}$$
$$= 1 + \beta \circ \vartheta - \beta(a_{|T|}, b_{|T|}) \circ \vartheta(a_{|T|}, b_{|T|}) \circ \lambda_{a_{|T|}, b_{|T|}}$$
$$+ \sum_{i=1}^{|T|-1} \xi(a_i, b_i) \circ \tau''(a_i, b_i) \circ \lambda_{a_i, b_i}$$
$$= 1 + \sum_{i=1}^{|T|} \beta(a_i, b_i) \circ \vartheta(a_i, b_i) \circ \lambda_{a_i, b_i} - \beta(a_{|T|}, b_{|T|}) \circ \vartheta(a_{|T|}, b_{|T|}) \circ \lambda_{a_{|T|}, b_{|T|}}$$
$$+ \sum_{i=1}^{|T|-1} \xi(a_i, b_i) \circ \tau''(a_i, b_i) \circ \lambda_{a_i, b_i}$$
$$= 1 + \sum_{i=1}^{|T|-1} \beta(a_i, b_i) \circ \vartheta(a_i, b_i) \circ \lambda_{a_i, b_i} + \sum_{i=1}^{|T|-1} \xi(a_i, b_i) \circ \tau''(a_i, b_i) \circ \lambda_{a_i, b_i}$$
$$= 1 + \sum_{i=1}^{|T|-1} \beta(a_i, b_i) \circ \tau''(a_i, b_i) \circ \lambda_{a_i, b_i} + \sum_{i=1}^{|T|-1} \xi(a_i, b_i) \circ \tau''(a_i, b_i) \circ \lambda_{a_i, b_i}$$
$$= 1 + \tau'' \circ \left(\sum_{i=1}^{|T|-1} \beta(a_i, b_i) \circ \lambda_{a_i, b_i} \right) + \tau'' \circ \left(\sum_{i=1}^{|T|-1} \xi(a_i, b_i) \circ \lambda_{a_i, b_i} \right)$$
$$= 1 + \beta \circ \tau'' + \xi \circ \tau'' = 1 + \theta \circ \tau''.$$

Thus, $F'' = F + \sum_{i=1}^{|T|} \left(F''(a_i, b_i) - F(a_i, b_i) \right) \circ \lambda_{a_i, b_i}$ and

$$\|\overrightarrow{F''}\|_2^2 = \|\overrightarrow{F}\|_2^2 + \left\| \sum_{i=1}^{|T|} \overrightarrow{\left(F''(a_i, b_i) - F(a_i, b_i) \right) \circ \lambda_{a_i, b_i}} \right\|_2^2$$
$$+ 2 \left(\overrightarrow{F} \cdot \left(\sum_{i=1}^{|T|} \overrightarrow{\left(F''(a_i, b_i) - F(a_i, b_i) \right) \circ \lambda_{a_i, b_i}(x, y)} \right) \right),$$

where "$\cdot$" is the inner product. Since F is a small ternary quaternion polynomial, $\overrightarrow{F}$ is a vector with most elements equal to zero and the rest are 1 or -1. As a consequence, many products in $\left(\overrightarrow{F} \cdot \left(\sum_{i=1}^{|T|} \overrightarrow{\left(F''(a_i, b_i) - F(a_i, b_i) \right) \circ \lambda_{a_i, b_i}} \right) \right)$ vanish. On the other hand, the

polynomials λ_{a_i,b_i}, for $i = 0, \ldots, |T|$, have many monomials with large coefficients and then the vectors $\overrightarrow{\lambda_{a_i,b_i}}$'s have many nonzero coefficients with large values belonging to $\mathbb{Z}_q$. Therefore, the Euclidian norm of $\sum_{i=1}^{|T|} \overrightarrow{(F''(a_i, b_i) - F(a_i, b_i)) \circ \lambda_{a_i,b_i}}$ is very larger with respect to $\left(\overrightarrow{F} \cdot \left(\sum_{i=1}^{|T|} \overrightarrow{(F''(a_i, b_i) - F(a_i, b_i)) \circ \lambda_{a_i,b_i}} \right) \right)$. Hence,

$$\left\| \sum_{i=1}^{|T|} \overrightarrow{(F''(a_i, b_i) - F(a_i, b_i)) \circ \lambda_{a_i,b_i}} \right\|_2^2$$
$$> 2 \left(\overrightarrow{F} \cdot \left(\sum_{i=1}^{|T|} \overrightarrow{(F''(a_i, b_i) - F(a_i, b_i)) \circ \lambda_{a_i,b_i}} \right) \right),$$

and the immediate result is

$$\| \overrightarrow{F''} \|_2 > \| \overrightarrow{F} \|_2.$$

Under the same computations and according to Eq. (26), we have $\| \overrightarrow{G''} \|_2 > \| \overrightarrow{G} \|_2$.

Putting all pieces together, a small reduction in the Hamming norm of $\overrightarrow{\rho(\tau'')}$, leads to a small reduction in the Hamming norm of $\overrightarrow{\rho(F'' \circ \tau'')}$, entailing a high Euclidean norm for $\overrightarrow{F''}$ and $\overrightarrow{G''}$. This gives a considerable enlargement for the hybrid norm of $(\overrightarrow{G''}, \overrightarrow{F''}, \overrightarrow{\rho(F'' \circ \tau'')})$. One concludes that the private key $(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)}) = (\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(F \circ \vartheta)})$ is mostly likely one of the nonzero shortest vectors in Λ_{BQTRU}. $\qquad\square$

We remark that a consequence of the previous theorem is that recovering the private key in our cryptosystem can be reduced to solving an SVP in a lattice with hybrid norm.

5.1 Lattice based attack

The lattice based attacks, presented by Coppersmith and Shamir [11], are the most important attacks on the NTRU cryptosystem. The purposes of this type of attacks can be classified in two subclasses: an attempt at finding the private key and an attempt at obtaining the message. In this section, we present a lattice based attack that attempts at obtaining the private key. We show that our cryptosystem is secure against lattice based attacks.

In Theorem 4 it is shown that the private key $(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)})$ is with high probability one of the nonzero shortest vectors, measured by the hybrid metric, in Λ_{BQTRU}. Solving SVP or CVP with the hybrid metric is a challenging problem and as far as we know no algorithm has been developed to handle them. In the following we expand our BQTRU lattice to a lattice for which the SVP and CVP are measured using the Euclidean norm.

We select a small subset $\{c_0, c_1, \ldots, c_l\}$ of elements of $\mathbb{Z}_q$ such that each element $z \in \mathbb{Z}_q$ can be represented as $\sum_{i=0}^{l} z_i \cdot c_i$, where $(z_0, z_1, \ldots, z_l)$ is a vector with small Euclidean norm. In this work, we consider $\{c_0, c_1, \ldots, c_l\} = \{1, 2, \ldots, 2^l\}$, where $2^l \leq q < 2^{l+1}$. Then, we expand the BQTRU lattice to the lattice which is generated by the rows of the following matrix

$$M_{\text{expanded}} = \begin{bmatrix} q I_{4n^2} & 0 & 0 \\ \mathscr{H} & I_{4n^2} & 0 \\ \mathcal{D} & 0 & I_{4(l+1)n^2} \end{bmatrix},$$

where

$$\mathcal{D} = \begin{bmatrix} \mathbf{c} \otimes D & 0 & 0 & 0 \\ 0 & \mathbf{c} \otimes D & 0 & 0 \\ 0 & 0 & \mathbf{c} \otimes D & 0 \\ 0 & 0 & 0 & \mathbf{c} \otimes D \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} c_0, c_1, \dots, c_l \end{bmatrix}^{Tr}.$$

Then, we solve SVP in this lattice, $\Lambda_{\text{expanded}}$, that is measured under the Euclidean metric. Finally, the points of the expanded lattice are mapped to the points of the original lattice as follows

$$\psi : \mathbb{Z}^{4n^2} \times \mathbb{Z}^{4n^2} \times \overbrace{\mathbb{Z}_2^{n^2} \times \cdots \times \mathbb{Z}_2^{n^2}}^{4(l+1) \text{ times}} \to \mathbb{Z}^{4n^2} \times \mathbb{Z}^{4n^2} \times \overbrace{\mathbb{Z}_q^{n^2} \times \cdots \times \mathbb{Z}_q^{n^2}}^{4 \text{ times}}$$

$$(r, s, B_{0,0}, \dots, B_{0,l}, B_{1,0}, \dots, B_{1,l}, \dots, B_{3,0}, \dots, B_{3,l})$$

$$\mapsto \left(r, s, \sum_{i=0}^{l} B_{0,i} c_i, \sum_{i=0}^{l} B_{1,i} c_i, \dots, \sum_{i=0}^{l} B_{3,i} c_i \right).$$

The binary representation of any $z \in \mathbb{Z}_q$ is unique and all z_i in the linear combination $z = \sum_{i=0}^{l} z_i \cdot c_i$ are one or zero. Therefore, the Euclidean norm of $(z_0, z_1, \dots, z_l)$ is small. Hence, if we consider $\{c_0, c_1, \dots, c_l\} = \{1, 2, \dots, 2^l\}$, where $l = \lfloor \log_2 q \rfloor$, then any $z \in \mathbb{Z}_q$ can be written as a linear combination of them. Since the binary representation of any $z \in \mathbb{Z}_q$ is unique, then the mapping ψ is one to one and this mapping returns a unique solution.

We show that the equivalent vector for the private key $(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)})$ in the expanded lattice is its shortest vector under the Euclidean norm. If we consider the binary representation of any point in $\rho(\gamma_i)$, for $i = 0, \dots, 3$, we have

$$\rho(\gamma_i) = \left(\gamma_i(a_1, b_1), \gamma_i(a_2, b_2), \dots, \gamma_i(a_{n^2}, b_{n^2}) \right)$$

$$= \left(\sum_{j=0}^{l} z_{i,1j} c_j, \sum_{j=0}^{l} z_{i,2j} c_j, \dots, \sum_{j=0}^{l} z_{i,n^2 j} c_j \right).$$

Also

$$\rho(\gamma_i)D = \left(\sum_{j=0}^{l} z_{i,1j} c_j, \sum_{j=0}^{l} z_{i,2j} c_j, \dots, \sum_{j=0}^{l} z_{i,n^2 j} c_j \right) D$$

$$= \left(\sum_{j=0}^{l} (z_{i,1j}, z_{i,2j}, \dots, z_{i,n^2 j}) \right) c_j D$$

$$= \left((z_{i,10}, z_{i,20}, \dots, z_{i,n^2 0}), (z_{i,11}, z_{i,21}, \dots, z_{i,n^2 1}), \dots, (z_{i,1l}, z_{i,2l}, \dots, z_{i,n^2 l}) \right) \begin{pmatrix} c_0 D \\ c_1 D \\ \vdots \\ c_l D \end{pmatrix}$$

$$= (A_{i,0}, A_{i,1}, \dots, A_{i,l}) \begin{pmatrix} c_0 D \\ c_1 D \\ \vdots \\ c_l D \end{pmatrix}$$

$$= \sum_{j=0}^{l} A_{i,j} c_j D.$$

Therefore, $(\overrightarrow{G}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l})$ is the equivalent vector of the private key and

$$
\left(\overrightarrow{-U}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right) M_{expand}
$$

$$
= \left(-q\overrightarrow{U} + \overrightarrow{F}\,\tilde{\mathscr{H}} + \left(\sum_{i=0}^{l} A_{0,i}\,c_i\,D, \ldots, \sum_{i=0}^{l} A_{3,i}\,c_i\,D\right),\right.
$$
$$
\left.\overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right)
$$

$$
= \left(-q\overrightarrow{U} + \overrightarrow{F}\,\tilde{\mathscr{H}} + \left(\rho(\gamma_0)D, \ldots, \rho(\gamma_3)D\right),\right.
$$
$$
\left.\overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right)
$$

$$
= \left(-q\overrightarrow{U} + \overrightarrow{F}\,\tilde{\mathscr{H}} + \overrightarrow{\rho(\gamma)}\mathfrak{D}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right)
$$

$$
= \left(\overrightarrow{-qU + F \circ \tilde{H} + \gamma}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right)
$$

$$
= \left(\overrightarrow{G}, \overrightarrow{F}, A_0^0, \ldots, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\right).
$$

We conclude that, $(\overrightarrow{G}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}) \in \Lambda_{expanded}$. Next we show that it is one of the shortest vector in the expanded lattice.

In the following proposition, we consider the recommended parameters in Sect. 4.1 in such a way that the possibility of decryption failure be negligible. Choosing the prime number q such that $n|(q-1)$ and $q > 24dp$ in the BQTRU cryptosystem ensures that the decryption never fails. Following the method of selecting parameters in NTRU (see Proposition 6.61 of [19]), for simplicity, we can remove p in the last equation and assume that $q \approx 24d$. Moreover, $q = \alpha n + 1$, for some $\alpha \in \mathbb{N}$. Hence, since $d \approx n^2/7$ in BQTRU, we consider a prime number q, where $q \approx 24n^2/7 + 1$ in the following proposition.

Proposition 3 *Let (n, p, q, d) be BQTRU parameters such that*

$$
d \approx n^2/7, \quad q \approx 24n^2/7 + 1, \quad |T| \le n.
$$

Then the Gaussian heuristic predicts that the equivalent vector of the private key in $\Lambda_{expanded}$, that is $(\overrightarrow{G}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l})$, is the shortest nonzero vector in the Λ_{expand} with maximum likelihood.

Proof The average length of the shortest nonzero vector in a lattice Λ with dimension n is predicted by the Gaussian heuristic [19] (see page 377) as

$$
\lambda_1(\Lambda) = \sqrt{\frac{n}{2\pi e}}(\det(\Lambda))^{\frac{1}{n}}.
$$

This prediction in the extended lattice with dimension $(4l + 12)n^2$ and $\det(\Lambda_{expand}) = q^{4n^2}$ is

$$
\lambda_1(\Lambda_{expand}) = \sqrt{\frac{(4l + 12)n^2}{2\pi e}} q^{\frac{4}{(4l+12)}}.
$$

Since $2^l \leq q < 2^{l+1}$, we have

$$\lambda_1(\Lambda_{\text{expand}}) \geq \sqrt{\frac{(2l+6)n^2}{\pi e}}\, 2^{\frac{l}{(l+3)}},$$

where $l = \lfloor \log_2 q \rfloor$ and we assume $q \approx 24n^2/7 + 1 \approx 3.4n^2 + 1$. Therefore, we can paste $l \approx \log_2(3.4n^2 + 1)$ and have

$$\lambda_1(\Lambda_{\text{expand}}) \geq \sqrt{\frac{\left((2\log_2(3.4n^2 + 1) + 6)n^2\right)\left((3.4n^2 + 1)^2\right)^{1/(\log_2(27.4n^2 + 8))}}{\pi e}}.$$

On the other hand, if $\|\overrightarrow{\rho(\gamma)}\|_H = t'$, then

$$\|g, f, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\|_2 \leq \sqrt{16d + t'(l+1)}.$$

Since $d \approx n^2/7$ and $t' < 4|T|$, then

$$\|g, f, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\|_2 \leq \sqrt{\frac{16n^2}{7} + 4|T|(\log_2(3.4n^2 + 1) + 1)}.$$

In general, we consider $|T| \leq n$ and hence for $n \geq 7$,

$$\sqrt{\frac{16n^2}{7} + 4n(\log_2(3.4n^2 + 1) + 1)}$$

$$\leq \sqrt{\frac{\left((2\log_2(3.4n^2 + 1) + 6)n^2\right)\left((3.4n^2 + 1)^2\right)^{1/(\log_2(27.4n^2 + 8))}}{\pi e}}.$$

This proves that

$$\|g, f, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l}\|_2 \leq \lambda_1(\Lambda_{\text{expand}}),$$

and if n is large, with high probability, $(\overrightarrow{G}, \overrightarrow{F}, A_{0,0}, \ldots, A_{0,l}, \ldots, A_{3,0}, \ldots, A_{3,l})$ is the shortest nonzero vector in the expanded lattice using Euclidean norm. □

The image of the vector in the proof of the previous proposition is the private key $(\overrightarrow{G}, \overrightarrow{F}, \overrightarrow{\rho(\gamma)})$ under the mapping ψ. Indeed, finding the approximate solution of SVP in the hybrid metric leads to expanding this lattice to a lattice with a higher dimension and finding SVP in the expanded lattice. Therefore, finding the private key in our cryptosystem with parameters (n, p, q) is equivalent to finding a shortest vector in the expanded lattice with dimension $(4l + 12)n^2 = (4\log_2(3.4n^2 + 1) + 12)n^2$.

In this case, since $\dim(\Lambda_{\text{NTRU}}) = 8n^2$ and $\dim(\Lambda_{\text{expand}}) = 12n^2 + 4n^2 \log_2(3.4n^2 + 1)$, the dimension of Λ_{expand} is at least $(2 + \log_2 n)$ times larger than the dimension of NTRU lattice with parameters $(4n^2, q', p)$:

$$\frac{\dim(\Lambda_{\text{expand}})}{\dim(\Lambda_{\text{NTRU}})} = \frac{12n^2 + 4n^2 \log_2(3.4n^2 + 1)}{8n^2} = \frac{3}{2} + \frac{\log_2(3.4n^2 + 1)}{2}$$

$$\geq \frac{3}{2} + \frac{\log_2 3.4}{2} + \frac{\log_2 n^2}{2} \geq \frac{3}{2} + \frac{1.7}{2} + \log_2 n \geq 2 + \log_2 n.$$

For example when $n = 7$, the dimension of the expanded lattice is approximately 2036 while the dimension of the $(4n^2, q', p)$-NTRU lattice is 392. This increase in the dimension of the lattice forces high cost to the attacker of the cryptosystem. We note that only the attacker,

for key recovery, faces with this higher dimensions caused by the expansion. Since the computational complexity increases as a result of this expansion, this cryptosystem achieves a good security against lattice attacks.

We observe that we can reduce the size of the private keys F and G without violating the system security. This allows the use of larger messages. As a consequence, the security of the message is also increased.

5.2 Brute force attack

In our cryptosystem, the public parameters are $n, p, q, d_f, d_g, d_\phi$ and the public key is equal to $\tilde{H} = F^{-1} \circ G \pmod{J}$, where $J = \langle \sigma, q \rangle_\mathbb{A}$. For a brute-force search, Eve searches exhaustively every possible key and tests whether it is the correct one or not. In order to break our cryptosystem, she searches all quaternions F, G and polynomials σ which satisfy the equation $F \circ \tilde{H} = G \pmod{\langle \sigma, q \rangle_\mathbb{A}}$. Therefore, she may first enumerate all candidates for the ideal $Q = \langle \sigma, q \rangle$ that can be used for decryption. Then she tries each quaternion $F = f_0 + f_1 i + f_2 j + f_3 k \in \mathbb{A}$ where $f_i \in L_f$, for $i = 0, \ldots, 3$, until she finds a decryption key. That is, she finds the private key F by verifying that $F \circ \tilde{H} \pmod{J}$ is a small ternary quaternion polynomial. Eve could also find the private key by trying all possible quaternions $G = g_0 + g_1 i + g_2 j + g_3 k \in \mathbb{A}$ where $g_i \in L_g$, for $i = 0, \ldots, 3$, and $G \circ H^{-1} \pmod{J}$ is a small ternary quaternion.

The number of possible ideals Q generated by $\sigma(x, y) = \sum_{i=1}^{|T|} q_i \lambda_{a_i, b_i}(x, y)$ is equal to

$$\sum_{i=1}^{n} (q-1)^i \binom{n^2}{i}$$

and the number of possible small ternary quaternions F and G is

$$\#L_F = \binom{n^2}{d_f}^4 \binom{n^2 - d_f}{d_f}^4,$$

$$\#L_G = \binom{n^2}{d_g}^4 \binom{n^2 - d_g}{d_g}^4.$$

On the other hand, $\rho(\gamma) = \rho(F \circ \vartheta)$ where $\vartheta = W \circ \sigma$ and $W \in \mathbb{A}_q^\star$. Therefore, she needs to check $|\mathbb{A}_q^\star|$ quaternion W to find $\rho(\gamma)$. Since d_g is generally smaller than d_f, L_G is smaller than L_F. Hence, using a Meet-In-The-Middle attack approach [21], the search space for recovering the private key $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$ is approximately

$$\binom{\text{Key}}{\text{Security}} = |\mathbb{A}_q^\star| \binom{n^2}{d_g}^2 \binom{n^2 - d_g}{d_g}^2 \sum_{i=1}^{n} (q-1)^i \binom{n^2}{i},$$

where $\mathbb{A}_q^\star$ is the set of invertible elements in $\mathbb{A}_q$.

Using another point of view, Eve can just try to recover the original message M from the corresponding ciphertext C, instead of making a total break by finding the private key $(\overrightarrow{G}, \overrightarrow{F}, -\overrightarrow{\rho(\gamma)})$. She simply tries all random quaternion $\Phi = \phi_0 + \phi_1 i + \phi_2 j + \phi_3 k \in \mathbb{A}$ such that $\phi_i \in L_\phi$ for $i = 0, 1, 2, 3$ and test whether $C - p\tilde{H} \circ \Phi \pmod{q}$ is a small ternary quaternion or not. If the obtained quaternion has small coefficients it might be the original message M. Hence the search space for recovering the message (using a Meet-In-The-Middle attack approach) is

Table 1 Public key size, parameter sets and their specified security levels with comparisons to NTRU [20] and QTRU [28] cryptosystems (in each case $p = 3$)

Sec. level	Cryptosystem	n	q	d_f	d_g	d_ϕ	Key Sec.	Msg. Sec.	Successful dec.	Public key size (bit)
Moderate	NTRU	167	128	60	20	18	2^{82}	2^{77}	0.9999292925	1169
Highest	NTRU	503	256	215	72	55	2^{285}	2^{170}	0.9999532447	4024
Moderate	QTRU	47	59	7	6	5	2^{90}	2^{80}	0.9986364660	1128
Highest	QTRU	149	191	22	15	12	2^{263}	2^{225}	0.9999998808	4768
Moderate	BQTRU	7	113	7	6	6	$> 2^{166}$	2^{92}	0.9985784846	1372
Highest	BQTRU	11	199	17	17	13	$> 2^{396}$	2^{212}	0.9999995349	3872

$$\binom{\text{Message}}{\text{Security}} = \binom{n^2}{d_\phi}^2 \binom{n^2 - d_\phi}{d_\phi}^2 = \frac{(n^2!)^2}{(d_\phi!)^4 \, (n^2 - 2d_\phi)!^2}.$$

The key and message security estimates for the presented parameter sets in NTRU, QTRU and BQTRU cryptosystems are given in Table 1. The provided lower bounds on the key security for BQTRU are given by assuming $|\mathbb{A}_q^\star| = 1$. According to this table, the brute-force attack on BQTRU with values greater than $n = 11$ appears to be practically impossible. That is a necessary condition but not really a strong argument for security.

Moreover, the public key size of these cryptosystems is presented in Table 1. The public key in NTRU cryptosystem is a polynomial in $R_q = \mathbb{Z}_q[x]/\langle x^n - 1\rangle$, therefore its key size is equal to $n\lceil \log_2 q\rceil$ bits. In QTRU cryptosystem, the public key includes four polynomials in R_q and then the public key size is equal to $4n\lceil \log_2 q\rceil$ bits. Furthermore, the public key size of the proposed scheme is $4n^2\lceil \log_2 q\rceil$ bits due to the four public polynomials $h_i \in R_q' = \mathbb{Z}_q[x, y]/\langle x^n - 1, y^n - 1\rangle$, for $i = 0, \ldots, 3$. According to the result of Table 1, the public key size of BQTRU is smaller than NTRU and QTRU with higher security level.

See Sect. 4.1 for more details about the parameter's selection. These parameter sets, which are obtained from our experiments, are chosen in such a way that the parameter q be a prime number, $n | (q - 1)$ and $q \approx \frac{3}{7} q'$, where q' is equivalent parameter in $(4n^2, q', p)$-NTRU. Then, (n, q, p)-BQTRU has an equivalent level of security as $(4n^2, q', p)$-NTRU. We compare the combinatorial security of NTRU, QTRU and BQTRU in light of the meet-in-the-middle attack, with the prescribed parameter sets for two different security levels.

5.3 The Gentry attack

The parameter n of the ring $R = \mathbb{Z}[x]/ < x^n - 1 >$ in the original version of NTRU cryptosystem, is chosen to be a prime number, because having n prime maximizes the probability that the private key has an inverse with respect to a specified modulus. In 1999, Silverman has proposed taking n to be a power of 2 to allow the use of Fast Fourier Transforms when computing the convolution product of elements in the ring [36]. In the Gentry's attack [15], it is shown that choosing a composite number $n = cd$, especially one with a small factor, significantly reduces the security of the NTRU cryptosystem. Indeed, when $n = cd$ is a composite number, a ring homomorphism is used to construct much smaller (and more easily reduceable) lattices whose shortest vectors contain at least some useful cryptanalytic information about the secret key.

In general, when n is composite and d is a nontrivial divisor, there exist a ring homomorphism

$$\mathbb{Z}[x]/(x^n - 1) \longrightarrow \mathbb{Z}[x]/(x^d - 1)$$
$$f \mapsto f(d).$$

Then a $2d$-dimensional lattice $\Lambda(d)$ analog to the NTRU lattice can be constructed. This lattice contains the vector $(f(d), g(d))$. Therefore, at least when $d > \sqrt{n}$, $(f(d), g(d))$ is almost certainly the shortest vector in $\Lambda(d)$ for the same reasons that (f, g) is almost certainly the shortest vector for the NTRU lattice. Thus, significant partial information about the private key is recovered by reducing to a $2d$-dimensional lattice. Alternatively, we can use $(f(d), g(d))$ to recover (f, g). We thereby obtain the private key without ever having to reduce a $2n$-dimensional lattice in NTRU. Indeed, we can decrease the dimension of the NTRU lattice by about $2d$ in a similar fashion. This $2d$ reduction in lattice dimension should reduce LLL's running time by a factor exponential in $2d$. To avoid the presented attack, n should be chosen to be prime, or to have only large nontrivial factors [15].

We now consider this attack on BQTRU in the same context. Indeed, for the bivariate case, the ring dimension is n^2 which is composite ($n^2 = n \cdot n$) and there are many suitable homomorphisms from the bivariate NTRU ring $\mathbb{Z}[x, y]/(x^n - 1, y^n - 1)$ to a univariate NTRU ring $\mathbb{Z}[t]/(t^n - 1)$; suitable maps are all the maps $\phi_{r,s} : x \to t^r, y \to t^s$ [4]. Therefore, the Gentry attack can be applied against BQTRU. For considering this attack, we should map the BQTRU lattice, from bivariate to univariate. However, the problem is more difficult than in the NTRU case since the Euclidean part of the BQTRU lattice can pass to the quotient but this is not the case for the Lagrange part $\mathfrak{D}$. When we use a homomorphism to map $\lambda_{a,b}(x, y)$ to the univariate ring, then its image is not an univariate interpolator. In fact it is a product of two univariate interpolators [4]. Hence, while the the Euclidean part can be reduced from dimension n^2 to dimension n, the Lagrange part $\mathfrak{D}$ is reduced from n^2 to approximately $n^2/2$ dimension. As a consequence, solving the reduced lattice remains too hard and we conjecture that BQTRU is practically secure against this attack. This problem is left for future study.

6 Conclusions

In this paper, we present a NTRU-like public key cryptosystem based on the quaternion algebras and bivariate polynomials. We show that the multiplication operation in our cryptosystem can be done by means of matrix multiplication. Using Strassen's efficient method for (2×2) matrix multiplication, we obtain $16/7$ times faster operations in the key generation and encryption process of our cryptosystem compared to NTRU within comparable parameters.

For designing a cryptosystem which is resistant against known lattice based attacks for low dimensions, we use bivariate polynomials ring and an ideal of this ring. This ideal is a lattice and the decryption process entails solving a CVP in this private lattice. Moreover, we show that the variance of the additive noise in this closest vector problem is small for an optimal decoder, like sphere decoder. Therefore, in the decryption process of our cryptosystem with the presented parameter sets, a legitimate receiver using the private generator matrix, solves CVP with affordable complexity and negligible error probability.

Due to the hybrid structure of the BQTRU lattice, recovering the private key in our cryptosystem leads to solving SVP in the expanded lattice which is at least $(2 + \log_2 n)$ times larger than the dimension of the NTRU lattice with equivalent parameters. This increasing

in the dimension of the lattice force a high cost to the attacker using a lattice attack in this cryptosystem. As a result of this expansion, this cryptosystem achieves high security against lattice attacks. Also we can reduce the size of the private keys without violating the system security and use larger message. Hence, message protection is feasible through larger polynomials increasing message security.

References

1. Agrell E., Eriksson T., Vardy A., Zeger K.: Closest point search in lattices. IEEE Trans. Inf. Theory **48**(8), 2201–2214 (2002).
2. Alon N.: Combinatorial nullstellensatz. Comb. Probab. Comput. **8**, 7–29 (1999).
3. Blahut R.E.: Algebraic Codes on Lines, Planes and Curves. Cambridge University Press, Cambridge (2008).
4. Boschini C., Orsini E., Traverso C.: Between codes and lattices: hybrid lattices and the NTWO cryptosystem. Effective Methods in Algebraic Geometry, MEGA'15, Italy, June 15–19. (2015). https://www.cs.bris.ac.uk/home/cseao/papr/MEGA2015.pdf
5. Brown W.: Matrices over Commutative Rings, Chapman & Hall Pure and Applied Mathematics. Taylor & Francis, Abingdon (1992).
6. Bürgisser P., Lickteig T., Clausen M., Shokrollahi A.: Algebraic Complexity Theory. Springer, Berlin (1996).
7. Caboara M., Caruso F., Traverso C.: Gröbner bases for public key cryptography. In: Proceedings of ISSAC 2008, pp. 315–323. ACM, New York (2008).
8. Chen, Y., Nguyen, P.Q.: BKZ 2.0: better lattice security estimates. In: Advances in Cryptology ASIACRYPT 2011, Lecture Notes in Computer Science, vol. 7073, pp. 1–20. Springer, Heidelberg (2011).
9. Coglianese, M., Goi, B.M.: MaTRU: A New NTRU-Based Cryptosystem. In: Progress in Cryptology INDOCRYPT 2005, Lecture Notes in Computer Science, vol. 3797, pp. 232–243. Springer, Berlin (2005).
10. Conway J.H., Smith D.A.: On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry. A. K. Peters, Ltd., Natick (2003).
11. Coppersmith, D., Shamir, A.: Lattice Attacks on NTRU. In: Advances in Cryptology, EUROCRYPT 1997. Lecture Notes in Computer Science, vol. 1233, pp. 52–61. Springer, Berlin (1997).
12. Cox D.A., Little J., O'Shea D.: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Publishing Company, Incorporated, Berlin (2015).
13. Ell T.A., Bihan N.L., Sangwine S.J.: Quaternion Fourier Transforms for Signal and Image Processing. Wiley, Hoboken (2014).
14. Gaborit P., Ohler J., Solé P.: CTRU, A polynomial analogue of NTRU. NTRU Technical Report Inria RR–4621 (2006).
15. Gentry, C.: Key recovery and message attacks on NTRU-Composite. In: Advances in Cryptology, EUROCRYPT 2001, Lecture Notes in Computer Science, vol. 2045, pp. 182–194. Springer, Berlin (2001).
16. Gordon B., Motzkin T.S.: On the zeros of polynomials over division rings. Trans. Am. Math. Soc. **116**, 218–226 (1965).
17. Hassibi B., Vikalo H.: On the sphere-decoding algorithm I. Expected complexity. IEEE Trans. Signal Process. **53**(8), 2806–2818 (2005).
18. Hermans, J., Vercauteren, F., Preneel, B.: Speed records for NTRU. Topics in Cryptology—CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, Lecture Notes in Computer Science, vol. 5985, pp. 73–88. Springer (2010).
19. Hoffstein J., Pipher J., Silverman J.H.: An Introduction to Mathematical Cryptography, 1st edn. Springer, Berlin (2008).
20. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU, a ring-based public-key cryptosystem. In: Algorithmic number theory, Lecture Notes in Computer Science, vol. 1423, pp. 267–288. Springer, Berlin (1998).
21. Howgrave-Graham, N., Silverman, J.H., Whyte, W.: A Meet-in-the-Middle Attack on an NTRU Private Key. NTRU Cryptosystems Technical Report 4, Version 2, updated (2006). http://www.ntru.com
22. IEEE.: P1363.1 Public-Key Cryptographic Techniques Based on Hard Problems over Lattices, June 2003. IEEE. (2003) http://grouper.ieee.org/groups/1363/lattPK/index.html

23. Jarvis K., Nevins M.: ETRU: NTRU over the Eisenstein integers. Des. Codes Cryptogr. **74**(1), 219–242 (2015).
24. Kalantari B.: Algorithms for quaternion polynomial root-finding. J. Complex. **29**, 302–322 (2013).
25. Kouzmenko, R.: Generalizations of the NTRU cryptosystem. Diploma Project, École Polytechnique Fédérale de Lausanne (2005–2006).
26. Lenstra A.K., Lenstra H.W., Lovász L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 513–534 (1982).
27. Maclachlan C., Reid A.W.: The Arithmetic of Hyperbolic 3-Manifolds. Springer, Berlin (2003).
28. Malekian E., Zakerolhosseini A., Mashatan A.: QTRU: quaternionic version of the NTRU public-key cryptosystems. ISC Int'l J. Inf. Sec. (ISeCure) **3**(1), 29–42 (2011).
29. Malekian, E., Zakerolhosseini, A.: NTRU-like public key cryptosystems beyond Dedekind domain up to alternative algebra. Trans. Comput. Sci. **10**, 25–41 (2010).
30. May, A., Silverman, J.H.: Dimension Reduction Methods for Convolution Modular Lattices. In: CaLC 2001, Lecture Notes in Computer Science, vol. 2146, pp. 110–125. Springer, Berlin (2001).
31. Micciancio, D.: The hardness of the closest vector problem with preprocessing. IEEE Trans. Inf. Theory **47**(3), 1212–1215 (2001).
32. Micciancio D.: The shortest vector problem is NP-hard to approximate to within some constant. SIAM J. Comput. **30**, 2008–2035 (2001).
33. Nevins M., Karimianpour C., Miri A.: NTRU over rings beyond $\mathbb{Z}$. Des. Codes Cryptogr. **56**(1), 65–78 (2010).
34. Poltyrev, G.: On coding without restrictions for the AWGN channel. IEEE Trans. Inf. Theory **40**, 409–417 (1994)
35. Schnorr C.P., Euchner M.: Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Programm. **66**, 181–199 (1994).
36. Silverman, J.H.: Wraps, gaps, and lattice constants. NTRU cryptosystems technical report No. 11 (1999). http://www.ntru.com
37. Solé P., Charnes C., Martin B.: A lattice-based McEliece scheme for encryption and signature. Electron. Notes Discret. Math. **6**, 402–411 (2001).
38. Strassen V.: Gaussian elimination is not optimal. Numer. Math. **13**, 354–356 (1969).
39. Viterbo E., Boutros J.: A universal lattice code decoder for fading channels. IEEE Trans. Inf. Theory **45**(5), 1639–1642 (1999).
40. Winograd S.: On multiplication of 2×2 matrices. Linear Algebra Its Appl. **4**, 381–388 (1971).