Revisiting the algorithms for the quaternion ℓ-isogeny path problems

Hyungrok Jo[1], and Junji Shikata[1,2]

[1] Institute of Advanced Sciences, Yokohama National University, Yokohama, Japan
jo-hyungrok-xz@ynu.ac.jp
[2] Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan
shikata-junji-rb@ynu.ac.jp

Abstract

The ℓ-isogeny path problems and their variations are fundamental challenges in isogeny-based cryptography, a prominent contender in post-quantum cryptography. In ANTS2014, Kohel, Lauter, Petit, and Tignol introduced the KLPT algorithm, a probabilistic polynomial algorithm addressing a mirrored version of the ℓ-isogeny path problems based on quaternion algebras under the Deuring correspondence.

In this study, we revisit the enhanced approach proposed by Petit and Smith in MathCrypt2018, which incorporated a solution to the Closest Vector Problem (CVP) for strong approximation in the primary step of the KLPT algorithm. This method minimizes the norm of target elements within an extremal order of the underlying quaternion algebra, making the Cornacchia's algorithm efficient during the strong approximation step. Although Petit and Smith's generalized KLPT algorithm should be employed in SQISign, the only isogeny-based digital signature scheme submitted to the NIST's additional call for post-quantum cryptography standardization, their work is primarily available in the form of presentation slides, providing limited algorithmic details. We meticulously reconstruct the improvements specific to the quaternion analogue of the ℓ-isogeny path problems, focusing on the strong approximation step using CVP, building upon the work of Pinto and Petit. It provides a robust theoretical foundation for our approach.

Keywords: isogeny-based cryptography, post-quantum cryptography, NIST PQC standardization, KLPT algorithm

1 Introduction

Since Couveignes [1] and Rostovtsev and Stolbunov [2] independently introduced the first cryptographic key exchange based on isogenies, isogeny-based cryptography has emerged as a promising candidate for post-quantum cryptography. In a notable contribution, Charles et al. [3] proposed cryptographic hash functions (specifically, the CGL hash function) based on explicit constructions of Ramanujan graphs, known as optimal expander graphs from a spectral perspective. The security of these cryptographic schemes hinges on the computational hardness of finding a path in the ℓ-isogeny supersingular graph between two specified vertices. Notably, Pizer's graphs used in the CGL hash function exhibit Ramanujan properties [4] and can be represented as supersingular elliptic curves and isogenies through the graph method [5]. Déchène's work [6] provides a beginner-friendly explanation of these concepts.

During the Algorithmic Number Theory Symposium in 2014 (ANTS2014), Kohel et al. introduced a polynomial time attack on CGL hash functions. These functions are based on supersingular isogeny graphs under the Deuring correspondence [7], and their vulnerability was addressed through the quaternion analogue of the ℓ-isogeny path problem, solved using what is now known as the KLPT (Kohel-Lauter-Petit-Tignol) algorithm.

In a subsequent presentation at Asiacrypt2017, Galbraith et al. [8] unveiled two public key signature schemes. These schemes derive their security from computational assumptions concerning isogeny graphs of supersingular elliptic curves. The second scheme, specifically, is an identification protocol reliant on the computational complexity of determining the endomorphism ring of a supersingular elliptic curve, effectively computing an isogeny between two specified elliptic curves. In this scheme, the public key is a supersingular elliptic curve, and the secret key is the endomorphism of the said elliptic curve. The pivotal idea behind the scheme is the utilization of the powersmooth version of the KLPT algorithm to compute a "pseudo-canonical" isogeny. This isogeny remains independent of a given isogeny and is used as the private key in the proof phase.

In Eurocrypt2018, Eisenträger et al. [9] explored the relationships among three potential computational hardness problems in the supersingular case, outlined below:

(1) Computing isogenies between supersingular elliptic curves.

(2) Computing the endomorphism ring of a supersingular elliptic curve.

(3) Computing a maximal order isomorphic to the endomorphism ring of a supersingular elliptic curve.

The researchers successfully demonstrated polynomial time reductions between these problems where possible, employing both Kohel's [10] and KLPT algorithms for heuristic security reductions. During Asiacrypt2020, De Feo et al. [11] introduced an innovative interactive identification protocol and the signature scheme "SQISign" (Short Quaternion and Isogeny Signature). This scheme was based on a generalized KLPT algorithm, custom-tailored to suit their signature scheme efficiently. The paper included the instantiation of the protocol, incorporating parameters designed to meet the NIST-1 level of post-quantum security.

In recent, the National Institute of Standards and Technology (NIST) recommended additional contributions for the digital signature category in the standardization process of Post-Quantum Cryptography. In September 2023, NIST publicly disclosed each digital signature scheme that passed Round 1 [12]. Among the candidates, SQISign is the only isogeny-based digital signature scheme. Therefore, it is anticipated that efficiently improving the SQISign algorithm will play an important role in future developments.

A generalized KLPT algorithm incorporated the utilization of the Closest Vector Problem (CVP) via LLL algorithms to solve the norm equation in the strong approximation step [13], [11, Appendix E.2]. However, the presentation slides lacked a detailed explanation of efficiently implementing algorithms in the strong approximation using CVP, despite the results presented by Petit and Pinto. This absence of a comprehensive theoretical background explanation has led to a partial integration of recent auxiliary results related to SQISign. The isogeny-based cryptographic protocol, specialized in encryption or signature methods for identity based wireless communication technologies issued by central servers, stands out for having the most compact key size and signature length compared to other PQC candidates. Therefore, this study aims to contribute to the computational efficiency of isogeny-based cryptographic protocols that have entered the competition for NIST PQC standardization. In our work, we revisit the KLPT algorithm and elucidate the process of adapting the CVP to the strong approximation within the algorithm. This adaptation yields the minimum value of the power e of the norm, resulting in $\frac{5}{2}\log p$ in comparison to the existing value $\frac{7}{2}\log p$.

2 Preliminaries

We give some notations and definitions related to the theory of quaternion algebras. We refer to [14]. Additionally, we provide an overview of the theory concerning elliptic curves, endomorphisms, and isogenies to facilitate an understanding of the Deuring correspondence.

2.1 Quaternion algebra

Let p be a prime. Let F be the field $\mathbb{Q}$ of rational numbers, or the field $\mathbb{Q}_p$ of p-adic numbers. A *quaternion algebra* B over F is a central simple algebra of dimension 4 over F. We can define

$$B := B(a,b) = F1 + Fi + Fj + Fk$$

in terms of basis $1, i, j, k$ by the following relations: 1 is the identity of B, $i^2 = a, j^2 = b$, and $ij = k = -ji$, where a, b are non-zero elements in $F^\times$. ($F^\times$ denotes invertible elements in F.) The *conjugation* on B is defined by the following: if $\alpha = w+xi+yj+zk \in B$, and $w, x, y, z \in F$, then $\bar{\alpha} = w - xi - yj - zk$. The (reduced) *norm* Nrd and (reduced) *trace* Tr of B are defined by $Nrd(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha = w^2 - ax^2 - by^2 + abz^2$ and $Tr(\alpha) = \alpha + \bar{\alpha} = \bar{\alpha} + \alpha = 2w$.

If B is a quaternion algebra over $\mathbb{Q}$, we let $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ which is a quaternion algebra over $\mathbb{Q}_p$. Over $\mathbb{Q}_p$ or $\mathbb{R}$, there are only two quaternion algebras up to isomorphism: a unique division algebra and the 2×2 matrix algebra [15]. A prime p of $\mathbb{Q}$ is said to *ramify* in B if B_p is a division algebra and is said to *split* in B if B_p is the 2×2 matrix algebra. In this paper, we only consider a quaternion algebra ramified at precisely one finite prime p and also ∞. We denote this as $B_{p,\infty}$.

2.2 Extremal orders

Let B be a quaternion algebra over $\mathbb{Q}$ (or $\mathbb{Q}_p$). A *lattice* on B is a free $\mathbb{Z}$ (or $\mathbb{Z}_p$) submodule of B of rank 4. An *order* $\mathcal{O}$ of B is a lattice on B which is also a subring containing the identity. An order $\mathcal{O}$ of B (or of B_p) is said to be *maximal* if it is not properly contained in any other order of B (or of B_p). For an order $\mathcal{O}$ of B (or of B_p), a *left $\mathcal{O}$-ideal* I is a lattice on B such that $I_p = \mathcal{O}_p a_p$ (for some $a_p \in B_p^\times$) for all $p < \infty$. Two left $\mathcal{O}$-ideals I and J are said to belong to the same *class* if $I = Ja$ for some $a \in B^\times$. One has the obvious analogous definitions for right $\mathcal{O}$-ideals similarly.

For a (left or right) $\mathcal{O}$-ideal for some order $\mathcal{O}$, the *left order* of I and the *right order* of I are defined as $\{a \in B | aI \subseteq I\}$ and $\{a \in B | Ia \subseteq I\}$, respectively. The *discriminant* of $\mathcal{O}$ is defined as $\mathrm{disc}(\mathcal{O}) = \sqrt{\det((\alpha_i, \alpha_j))}_{i,j \in \{1,2,3,4\}}$ given a basis $\langle \alpha_1, \alpha_2, \alpha_3, \alpha_3 \rangle$ of $\mathcal{O}$; $\mathrm{disc}(\mathcal{O}) \in \mathbb{Z}$ and is independent of a choice of basis. A suborder $\mathcal{O}'$ of $\mathcal{O}$ is an order of rank 4 contained in $\mathcal{O}$. If $N = [\mathcal{O} : \mathcal{O}']$ then the discriminant of $\mathcal{O}'$ satisfies $\mathrm{disc}\mathcal{O}' = N^2 \mathrm{disc}(\mathcal{O})$. We define an equivalence on orders by conjugacy and on left $\mathcal{O}$-ideals by right scalar multiplication. Two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are equivalent if there is an element $\beta \in B_{p,\infty}$ such that $\beta\mathcal{O}_1 = \mathcal{O}_2\beta$. We focus on the p-extremal maximal orders $\mathcal{O}$ containing π such that $\pi^2 = -p$. We define a *special p-extremal maximal order* $\mathcal{O}$ to be a p-extremal maximal order such that $\mathrm{disc}(\mathcal{O})$ is minimal.

2.3 Supersingular elliptic curves and isogenies

Let E, E' be two elliptic curves over a finite field $\mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field of size q, and q is a power of p. An *isogeny* $\varphi : E \to E'$ is a nonconstant morphism from E to E' that maps the neutral element to the neutral element. The degree of an isogeny φ is the degree of the finite extension, which is obtained by the usual injection of the function fields [15]. An isogeny of degree ℓ is called an ℓ-isogeny. An isogeny may be separable, inseparable, or purely inseparable depending on the corresponding property of the extension.

We consider φ is separable, so that the degree of φ is the cardinality of the kernel of φ. If there is a separable isogeny between two curves, we say that they are *isogenous*. A separable isogeny can be identified with its kernel, which means there is a one-to-one correspondence between separable isogenies (up to isomorphism) and finite subgroups of E over an algebraic closure of a given field.

The isogeny can be computed from its kernel G using Vélu's formulae [16], explicitly $\varphi : E \to E'$ with kernel G such that $E' \cong E/G$. The degree of a composition of isogenies is multiplicative. For any isogeny φ of degree $d = \Pi_{i=1}^{n} {p_i}^{e_i}$, φ can be factored as the composition of e_i isogenies of degree p_i for $i = 1$ to n. For each isogeny $\varphi : E \to E'$, there is a unique isogeny $\hat{\varphi} : E' \to E$, which is called the *dual isogeny* of φ, and which satisfies $\varphi\hat{\varphi} = \hat{\varphi}\varphi = [\deg\, \varphi]$. If we have two isogenies $\varphi : E \to E'$ and $\varphi' : E' \to E$ such that $\varphi\hat{\varphi}$ and $\hat{\varphi}\varphi$ are the identity in their respective curves, we say that φ, φ' are *isomorphisms*, and that E, E' are *isomorphic*. An isogeny $\varphi : E \to E$, mapping itself, is called an *endomorphism*. The set of endomorphisms of an elliptic curve, denoted by $\mathrm{End}(E)$, has a ring structure with the operations point-wise addition and function composition ($\varphi\psi := \varphi \circ \psi$). The endomorphism ring of an elliptic curve has an algebraic structure which can be classified. Over the algebraic closure of the field, $\mathrm{End}(E)$ is an order in a quadratic imaginary field, so that a such curve is said to *ordinary*. If $\mathrm{End}(E)$ is a maximal order in a quaternion algebra, so that a such curve is said as *supersingular*. We are interested in supersingular elliptic curves over $\mathbb{F}_q = \mathbb{F}_{p^2}$, in an isogeny class such that the full endomorphism ring is defined over $\mathbb{F}_q$.

2.4 Deuring correspondence

It is known (due to Deuring [7]) that every supersingular elliptic curve over an algebraically closed field of characteristic p has a model defined over $\mathbb{F}_{p^2}$. The set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is one-to-one correspondence with the set of ideal classes of a maximal order of the quaternion algebra $B_{p,\infty}$. If we fix a supersingular elliptic curve E over $\mathbb{F}_p$ such that $\pi_E^2 = -p$, where π_E is the relative Frobenius endomorphism of E. For example, we can consider the order $\mathcal{O} = \langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \rangle$, with $i = -1$ and $j = -p$, corresponding to the elliptic curve of j-invariant 1728 when $p = 3 \pmod 4$. The order $\mathcal{O}$ is isomorphic to the endomorphism ring of the curve $E_0 : y^2 = x^3 + x$ [8].

We have explicit endomorphisms π and ι such that

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle,$$

where π is the Frobenius morphism $(x, y) \mapsto (x^p, y^p)$ and ι is the map $(x, y) \mapsto (-x, \sqrt{-1}y)$. Pizer [17] described the explicit description of $B_{p,\infty}$ for all p along with the $\mathbb{Z}$-basis for a maximal order $\mathcal{O}$ of $B_{p,\infty}$. Let p be a prime.

p	(a, b)	$\mathcal{O}$
2	$(-1, -1)$	$\langle \frac{1+i+j+k}{2}, i, j, k \rangle$
$3 \pmod 4$	$(-1, -p)$	$\langle \frac{1+j}{2}, \frac{i+k}{2}, j, k \rangle$
$5 \pmod 8$	$(-2, -p)$	$\langle \frac{1+j+k}{2}, \frac{i+2j+k}{4}, j, k \rangle$
$1 \pmod 8$	$(-p, -q)$	$\langle \frac{1+j}{2}, \frac{i+k}{2}, \frac{1}{q(j+ak)}, k \rangle$

where a is some integer satisfying $q|(a^2p + 1)$. Here, q is a prime with $q \equiv 3 \pmod 4$ and $(\frac{p}{q}) = -1$. ($(\frac{\cdot}{\cdot})$ is a Legendre symbol.) Since there are some arguments how to choose a proper maximal order or tweak the basis of maximal order (as a *special* p*-extremal order*) in [18, Section 2.3] under the Deuring correspondence, please refer to it for details.

3 KLPT algorithms

We refer to [11], [19], [20], [9], [8], [21], [18] and [13]. The algorithm takes a maximal order and a left $\mathcal{O}$-ideal I as a input and finds an equivalent ideal $J \sim I$ of given norm. The norm is required to be a power of ℓ (ℓ^e for some $e \in \mathbb{N}$). In the procedure, it is necessary to solve the norm equation as the explicit strong approximation.

Algorithm 1: Construct an ideal of prime norm

input : $\mathcal{O}$ and left $\mathcal{O}$-ideal I
output: J, a left $\mathcal{O}$-ideal equivalent to I with ℓ^e norm

1 Reduce to the case where $\mathcal{O}$ is special ;
2 Replace I with another left $\mathcal{O}$-ideal K with prime norm N ;
3 Let $K = \mathcal{O}N + \mathcal{O}\alpha$. Compute $e \in \mathbb{Z}$, λ coprime to N and β such that
4 $\beta \equiv \lambda\alpha \pmod{N\mathcal{O}}$, ; `// Condition 1`
5 $Nrd(\beta) = N\ell^e$; `// Condition 2`
6 **return** $J = K\overline{\beta}/N$

In $B_{p,\infty} = \mathbb{Q}[i, j]$, a special extremal order is a maximal order $\mathcal{O}$ containing a suborder admitting an orthogonal decomposition $R + Rj$ where $R = \mathcal{O} \cap \mathbb{Q}[i]$ is a quadratic order of discriminant $D = \mathrm{disc}(R)$. Let w such that $R = \mathbb{Q}[w]$ where ω has smallest norm in $\mathcal{O}$. By orthogonal decomposition we mean $R \subset (Rj)^{\perp}$. In the step **2** of **Algorithm 1**, we construct a left ideal J, which is equivalent to the input ideal I but with a prime norm N.

Lemma 3.1. *Let I be a left $\mathcal{O}$-ideal of reduced norm N and α an element of I. Then $I\gamma$, where $\gamma = \overline{\alpha}/N$, is a left $\mathcal{O}$-ideal of norm $Nrd(\alpha)/Nrd(I)$.*

Using **Lemma 3.1**, we find an element α of I which gives an equivalent ideal $K = I\overline{\alpha}/Nrd(I)$ with prime norm N. Heuristically, N is expected to be of size $\widetilde{O}(\sqrt{p})$. For $s \in \mathbb{R}^+$, the number $n \in \mathbb{N}$ is said to be *s-powersmooth* if any divisor p^k of n for a prime p satisfies $p^k \leq s$. To put it simply, the idea of the algorithm is to first construct an ideal with a powersmooth norm, then use the Deuring's correspondence to compute an isogeny from E_0 which corresponds to the ideal in the **Section 5**.

3.1 Construct an ideal of powersmooth norm

We construct an element of I with a specified norm $N\ell$, where ℓ is an odd powersmooth number. If such an element is found, we can use **Lemma 3.1** to construct another ideal $J = I\overline{\beta}/N$. The norm of this ideal is indeed powersmooth, since

$$Nrd(J) = Nrd(I) \cdot \frac{Nrd(\beta)}{N} = \frac{N^2\ell}{N^2} = \ell.$$

The powersmooth norm of J will be important since we will require a factorization of $Nrd(J)$ to solve the discrete logarithm problem in the Deuring correspondence step. Unlike the previous step, we cannot simply pick a random $\beta \in I$, since this element β has to have norm $N\ell$. The process of obtaining β of a particular norm involves solving a sum of squares problem.

For the usage in the step of strong approximation, we describe the Cornacchia's algorithm.

Cornacchia's algorithm Given positive integers d and m such that $\mathrm{GCD}(d, m) = 1$, determine integers (x, y) such that

$$x^2 + dy^2 = m.$$

The algorithm proceeds as follows.

1. Put $r_0 = m$ and ${r_1}^2 = -d \pmod{m}$, where $0 \leq r_1 \leq m/2$.
2. Compute $r_{i+2} = r_i \pmod{r_{i+1}}$ recursively like in the Euclidean algorithm until an r_k where ${r_k}^2 < m$ is found.
3. If $(m - {r_k}^2)/d$ is a square integer, return $(r_k, \sqrt{(m - {r_k}^2)/d})$.

This algorithm will always return a primitive solution (solutions where $\mathrm{GCD}(x, y) = 1$) if it exists, provided one tries all possible square roots of $-d \pmod{m}$. Otherwise, one might attempt to solve the equation

$$x^2 + dy^2 = \frac{m}{g^2}$$

for some square g^2 such that m/g^2 is an integer. if a solution is found, the solution to the original equation is then (gx, gy).

3.2 Strong approximation

Basically, this phase is related to implement a deterministic polynomial time algorithm that represents a number as a sum of squares with some restricted congruence conditions (strong approximation). In our case, we apply it to solve a given norm equation.

Algorithm 2: Strong approximation in KLPT algorithm

Compute a random $\gamma \in \mathcal{O}$ of reduced norm $N\ell^{e_0}$;
Compute $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \pmod{N\mathcal{O}}$;
Compute $\lambda \in \mathbb{Z}$ and $\mu \in \mathcal{O}$ such that
$\mu \equiv \lambda[\mu]$ and $Nrd(\mu) = \ell^{e_1}$;
return $\beta := \gamma\mu$

Briefly, we explain the outline of the explicit version of strong approximation. $R + Rj$ has index D in $\mathcal{O}$ and

$$Nrd((x_1 + y_1\omega) + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2),$$

where f is a principal quadratic form of discriminant D. We have $[\mu] = (z_0 + w_0\omega)j$. We want to find $\lambda \in \mathbb{Z}$ and

$$\mu = \lambda[\mu] + N((x_1 + \omega y_1) + (z_1 + \omega w_1)j)$$

such that

$$Nrd(\mu) = N^2 f(x_1, y_1) + pf(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e.$$

We get λ from $\lambda^2 f(z_0, w_0) = \ell^e$ by modulo N. The norm equation is bilinear in z_1, w_1 by modulo N^2. Then, we take random integer solutions for (z_1, w_1) until

$$f(x_1, y_1) = \frac{\ell^e - pf(\cdot,\cdot)}{N^2}$$

can be solved. We give some details for solving each parameter.

The search for γ [19]

The first method to construct γ, which we attempt during the course of investigating this algorithm, is to construct an element $\gamma \in \mathcal{O}$, then do a brute force search for all γ with norm $N\ell^{e_0}$ such that $I\overline{\gamma} \subseteq N\mathcal{O}$.

Constructing such a γ can be done by writing $\gamma = a + bi + c\frac{i+j}{2} + d\frac{1+k}{2}$ and solving for the quadratic norm equation

$$(a + d/2)^2 + (b + d/2)^2 + p((c/2)^2 + (d/2)^2) = N\ell^{e_0}.$$

We put $a' := a + d/2$, $b' := b + d/2$, $c' := c/2$ and $d' := d/2$. First we pick a random pair of integers (c', d') as $c' \in [-m', m']$ for setting $m' := \lfloor\sqrt{\frac{4N\ell^{e_0}}{p}}\rfloor$ and $d' \in [-m'', m'']$ for setting $m'' := \sqrt{\frac{4N\ell^{e_0}}{p} - c'^2}$. Set $M = 4N\ell^{e_0} - p(c'^2 + d'^2)$. Then solving

$$a'^2 + b'^2 = N\ell^{e_0} - p(c'^2 + d'^2)$$

for (a', b') using Cornacchia's algorithm. This process is repeated until a suitable γ is found.

In the step **2-4** in **Algorithm 2**, as described in [8], we write $\gamma = \beta\mu$, each with norms $N\ell^{e_0}$ and ℓ^{e_1} respectively, where ℓ^{e_0} and ℓ^{e_1} are powersmooth numbers. To construct each γ, we first write $I = N\mathcal{O} + \mathcal{O}\alpha$, where $\alpha \in I$ such that $\mathrm{GCD}(N^2, Nrd(\alpha)) = N$. The element β is then constructed just as above in a similar way.

The search for μ [11]

We first find an element μ of the form $Cj + Dk$ which solves the following equation of ideals:

$$(\mathcal{O}\beta)\mu = (\mathcal{O}\alpha) \pmod{N\mathcal{O}}.$$

Once such a μ has been found, we find an element μ' such that $\mu' = \lambda\mu \pmod{N\mathcal{O}_0}$ and $Nrd(\mu') = \ell^{e_1}$ for some $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$. This is possible by tweaking the previous norm equation to accommodate the new information in the following way. We want this μ' to be of the form

$$\mu' = v + wi + xj + yk.$$

Since μ' also needs to satisfy $Nrd(\mu') = \ell^{e_1}$, we have to solve the following norm equation:

$$v^2 + w^2 + p(x^2 + y^2) = \ell^{e_1}. \tag{1}$$

Also, the condition that $\mu' = \lambda\mu \pmod{N\mathcal{O}}$ is equivalent to stating that (after an appropriate change of basis):

$$\begin{aligned} v &= aN \\ w &= bN \\ x &= \lambda C + cN \\ y &= \lambda D + dN, \end{aligned}$$

for some $a, b, c, d \in \mathbb{Z}$. Substituting these values for v, w, x and y in **Equation (1)** yields

$$N^2(a^2 + b^2) + p((\lambda C + cN)^2 + (\lambda D + dN)^2) = \ell^{e_1}. \tag{2}$$

To solve this equation for a, b, c, and d, we first consider Equation 2 modulo N to obtain the following:

$$p\lambda^2(C^2 + D^2) = \ell^{e_1} \pmod{N},$$

and solve for λ, provided that $\ell^{e_1}/(p(C^2 + D^2))$ is a quadratic residue modulo N. If this is not the case, the issue is easily remedied by multiplying ℓ^{e_1} by small primes. Once the λ is found, we consider Equation 2 which yields

$$p\lambda^2(C^2 + D^2) + 2p\lambda N(Cc + Dd) = \ell^{e_1} \pmod{N^2}. \tag{3}$$

From this equation, we can pick a random d, and then solve for c (or vice versa). Rearranging Equation 1 gives

$$a^2 + b^2 = \frac{\ell^{e_1} - p((\lambda C + cN)^2 + (\lambda D + dN)^2)}{N^2}$$

which we can solve for (a, b) using Cornacchia's algorithm. Note that due to our choice of λ, c, and d, the right-hand side of this equation is an integer. Solving for (λ, a, b, c, d) yields the desired (v, w, x, y) by substitution.

4 CVP to minimize the norm

Petit and Smith [13]'s technique is applied in the step of **the search for** μ. There is a similar approach in Pinto and Petit's work [22], which is used for explicit strong approximation in a Cayley hash function based on the security of the path finding problems over Lubotzky-Phillips-Sarnak Ramanujan graphs. As we argued in **Subsection 3.2** we have

$$Nrd((x_1 + y_1\omega) + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2),$$

where f is a principal quadratic form of discriminant D. We have the parameter λ satisfies

$$\mu = \lambda[\mu] + N((x_1 + \omega y_1) + (z_1 + \omega w_1)j)$$

and

$$Nrd(\mu) = N^2 f(x_1, y_1) + pf(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e.$$

The norm equation is bilinear in z_1, w_1 by modulo N^2. Instead of taking random integer solutions for (z_1, w_1) until

$$f(x_1, y_1) = \frac{\ell^e - pf(\cdot, \cdot)}{N^2},$$

we translated the solution space modulo N^2 to a lattice.

More specifically, we consider the procedure in **the search for** μ and follow the notations. From the **Equation (3)** ,

$$p\lambda^2(C^2 + D^2) + 2p\lambda N(Cc + Dd) = \ell^{e_1} \pmod{N^2}.$$

the parameters λ, C, D are already chosen. We define new parameters v and w as follows:

$$\begin{aligned} \mathrm{v} &:= \quad C/D \pmod{N}, \\ \mathrm{w} &:= \quad \left(\frac{\ell^{e_1} - p\lambda^2(C^2 + D^2)}{2p\lambda ND}\right) \pmod{N}. \end{aligned}$$

Then, we have

$$\mathrm{v}c + d = \mathrm{w} \pmod N$$

which is equivalent to the **Equation (3)**.

Lemma 4.1. *The set of solutions* $(c, d) \in \mathbb{Z}^2$ *to* ***Equation (3)*** *is the set* $\mathfrak{L} + (0, \mathrm{w}) = \{z + (0, \mathrm{w}) | z \in \mathfrak{L}\}$*, where* $\mathfrak{L}$ *is the two-dimensional lattice generated by the vectors* $(1, -\mathrm{v})$ *and* $(0, N)$*.*

So we deform this lattice by **Lemma 4.1** to one upon which we can find a CVP solution via Lenstra-Lenstra-Lovasz [23], [24]. We then rewrite the norm we want to minimize as the distance between a particular element in the Euclidean plane and a lattice element.

$$p\lambda^2(C^2 + D^2) + 2p\lambda N(Cc + Dd) = 4N^2||z - t||^2,$$

where

$$z := (c, d) - (0, \mathrm{w})$$

is a lattice point and

$$t := \left(-\frac{\ell^{e_1} - p\lambda^2(C^2 + D^2)}{2Np\lambda C}, -\frac{\ell^{e_1} - p\lambda^2(C^2 + D^2)}{2Np\lambda D} - \mathrm{w}\right).$$

Minimizing this norm is an instance of the *closest vector problem* for which standard algorithmic solutions (e.g., embedding technique) exist [23]. We adapt these solutions to incorporate the additional requirement that $n := \ell^{e_1} - 4N^2||z - t||^2$ is of a form that makes Cornacchia's algorithm efficient.

First, we compute a minimal basis for the lattice, namely, two vectors that generate the lattice and have minimal norms. This can be done using Gauss reduction, or equivalently the Euclidean algorithm. We then write t as a linear combination of the two short vectors, and we round the coefficients to obtain a lattice vector z that is close to t. Finally, we add small lattice vectors to z and compute the corresponding value of n, until it is of a suitable form. Once we find n of a suitable form, we compute the values of c and d and we apply Cornacchia's algorithm to compute a and b.

Remark. *In accordance with the findings of Petit and Smith [13], the estimated size of the lattice basis is approximated by*

$$N^{3/2}p^{1/2}D^{1/4}.$$

This estimation determines the minimum value of the power e of the norm, such that $\frac{\ell^e - pf(\cdot,\cdot)}{N^2}$ *becomes positive, yielding*

$$e \geq \log_\ell N^3 p D^{1/2} \sim \frac{5}{2}\log p.$$

This is in contrast to the previous result $e \sim \frac{7}{2}\log p$ *as mentioned in [18]. The analysis is grounded on the "Gaussian heuristic", where the two vectors in a minimal basis are expected to have a norm of approximately* $\sqrt{det(\mathfrak{L})}$*. This observation prompts us to explore further enhancements utilizing recent solutions to closest vector problems, surpassing the efficiency of the embedding technique [23] proposed by Kannan.*

5 Computing the isogeny

In order to complete the KLPT algorithm under the Deuring correspondence as an example in **Subsection 2.4**, we show how to compute the actual isogeny. Recall from the Deuring correspondence that we need to find the kernel of the isogeny, that is, the set of points P such that $\alpha(P) = O$ for all $\alpha \in J$, our output ideal. There is an isomorphism of quaternion algebras

$$\begin{aligned} \theta : B_{p,\infty} &\to \mathrm{End}(E_0) \otimes \mathbb{Q} \\ (1, i, j, k) &\mapsto ([1, \phi, \pi, \phi\pi]) \end{aligned}$$

where $\phi : (x, y) \mapsto (-x, \iota y)$ is the "square root of -1" map, and $\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius map. Given an element $\alpha \in J$, write $\alpha = a_1 + a_2 i + a_3 j + a_4 k$. Let $P(x, y)$ be a point. We then have:

$$a(P) = [a_1]P + [a_2]\pi(P) + [a_3]\phi(P) + [a_4]\phi(\pi(P)).$$

The strategy is to compute the elements of the kernel in $E_0[{\ell_i}^{e_i}]$ and compose them Chinese remainder theorem-style. To do so, since $E_0[\ell_i^{e_i}]$ is 2-dimensional, we look for two basis points P_i and Q_i. We then compute $\alpha(P_i)$ and $\alpha(Q_i)$ for every α in the basis of J. It is likely that such α contains coefficients with 2 in the denominator. It gives us

$$\alpha = \frac{(\alpha_1' + \alpha_2' i + \alpha_3' j + \alpha_4' k)}{2}$$

and performs *point division*: compute points ${P_i}'$ and ${Q_i}'$ such that $[2]{P_i}' = P_i$ and $[2]{Q_i}' = Q_i$, respectively. Although generally point division is not uniquely defined, it suffices to choose a point in this computation, since for any choice of ${P_i}'$ (and respectively Q_i),

$$2\alpha({P_i}') = \alpha([2]{P_i}') = \alpha(P_i).$$

Therefore, instead of computing as in Equation, we compute

$$\alpha(P_i) = [a_1']{P_i}' + [a_2']\pi({P_i}') + [a_3']\phi({P_i}') + [a_4']\phi(\pi({P_i}'))$$

and

$$\alpha(Q_i) = [a_1']{Q_i}' + [a_2']\pi({Q_i}') + [a_3']\phi({Q_i}') + [a_4']\phi(\pi({Q_i}')).$$

Using all of this information, we compute a point R_i on $E_0[{\ell_i}^{e_i}]$ which satisfies $\alpha(R_i) = O$ for all $\alpha \in J$ using linear algebra. We then compute an isogeny with kernel generated by $\varphi_{i-1}(R_i)$, where $\varphi_0 = [1]_{E_0}$. We proceed through all i, constructing the isogeny step-by-step by composition, and at the end we have constructed an isogeny corresponding to the output ideal J.

6 Conclusion

In the ongoing NIST standardization and evaluation of post-quantum cryptography, SQISign, a major candidate proposed, stands as the sole isogeny-based digital signature scheme. Given that the KLPT algorithm plays a pivotal role in the SQISign scheme, enhancing the efficiency of this algorithm is a meaningful task. We have distinctly outlined the improvement methodology for the strong approximation step using CVP, as proposed by Petit and Pinto, providing a solid theoretical foundation for the same. Moreover, these methodologies prove beneficial in investigating the complexity of strong approximation on the sphere [25], [22], as well as the *word problem* in group theory, which is fundamental in the security of hash functions over Cayley graphs [26], [27].

Hence, a comprehensive study on reducing the size of a norm utilizing recent results from closest vector problems or alternative approaches holds significant value. Furthermore, the distinctive features of the isogeny-based cryptographic protocol, which focuses on encryption and signature methods for identity-based wireless communication technologies issued by central servers, distinguish it by having the most compact key size and signature length among other PQC candidates. Consequently, this research not only aligns with the ongoing NIST standardization but also addresses the critical need to enhance the computational efficiency of isogeny-based cryptographic protocols.

Acknowledgement

This research was conducted under a contract of “Research and development on new generation cryptography for secure wireless communication services” among “Research and Development for Expansion of Radio Wave Resources (JPJ000254)”, which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[1] J. M. Couveignes. Hard homogeneous spaces. *IACR Cryptol. ePrint Arch.*, 2006(291), 2006.

[2] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive. https://ia.cr/2006/145, 2006.

[3] D. Charles, K. Lauter, and E. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22:93–113, 2009.

[4] A. K. Pizer. Ramanujan graphs. *AMS IP STUDIES IN ADVANCED MATHEMATICS*, 7:159–178, 1998.

[5] J. F. Mestre and A. T. Jorza. The method of graphs. examples and applications, 2011. https://www.williamstein.org/papers/rank4/mestre-en.pdf.

[6] I. Déchène. Quaternion algebras and the graph method for elliptic curves. Master's thesis, Department of Mathematics and Statistics, McGill University, Montreal, 1998.

[7] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, 14(1):197–272, 1941.

[8] S. D. Galbraith, C. Petit, and J. Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology*, 33(1):130–175, 2020.

[9] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 329–368. Springer, Cham., 2018.

[10] D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.

[11] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. Sqisign: compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security*, pages 64–93. Springer International Publishing, 2020.

[12] NIST. Post-quantum cryptography: Digital signature schemes : Round 1 additional signatures, 2023.

[13] C. Petit and S. Smith. An improvement to the quaternion analogue of the l-isogeny problem, 2018. Presentation slide in MathCrypt2018: https://crypto.iacr.org/2018/affevents/mathcrypt/medias/08-50_3.pdf.

[14] J. Voight. *Quaternion algebras*. Springer Nature, 2021.

[15] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Gradute Texts in Mathematics. Springer-Verlag, 1986.

[16] Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971.

[17] A. K. Pizer. An algorithm for computing modular forms on $\gamma_0(n)$. *Journal of Algebra*, 64(2):340–390, 1980.

[18] D. Kohel, K. Lauter, C. Petit, and J.P. Tignol. On the quaternion l-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[19] L. De Feo, A. Leroux, P. Longa, and B. Wesolowski. New algorithms for the deuring correspondence: towards practical and secure sqisign signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 659–690. Springer Nature Switzerland., 2023.

[20] R. Dimitrij. Constructing the deuring correspondence with applications to supersingular isogeny-based cryptography. Master's thesis, Technische Universiteit Eindhoven University of Technology, 2018.

[21] Y. Kambe, M. Yasuda, M. Noro, K. Yokoyama, Y. Aikawa, K. Takashima, and M. Kudo. Solving the constructive deuring correspondence via the kohel-lauter-petit-tignol algorithm. *Mathematical Cryptology*, 1(2):10–24, 2021.

[22] E. C. Pinto and C. Petit. Better path-finding algorithms in lps ramanujan graphs. *Journal of Mathematical Cryptology*, 12(4):191–202, 2018.

[23] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operations research*, 12(3):415–440, 1987.

[24] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671. Springer Science & Business Media, 2002.

[25] N. T. Sardari. Complexity of strong approximation on the sphere. *International Mathematics Research Notices*, 2019.

[26] C. Petit and J-.J. Quisquater. Rubik's for cryptographers, 2011. Cryptology ePrint Archive: https://ia.cr/2011/638.

[27] H. Jo, S. Sugiyama, and Y. Yamasaki. Ramanujan graphs for post-quantum cryptography. In *International Symposium on Mathematics, Quantum Theory, and Cryptography*, volume 33, pages 231–250. Springer, Singapore, 2020.