An improvement to the quaternion analogue of the ℓ-isogeny path problem

Christophe Petit & Spike Smith

May 2018

1 Introduction

In this paper, we provide an improvement to the quaternion ideal analogue of the path problem in supersingular ℓ-isogeny graphs. The improvement we offer is based on an existing algorithm for the same problem [5], which runs in probabilistic polynomial time, whose main result we briefly described.

Given a small prime ℓ and $B_{p,\infty}$ the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞, let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$ and I a left $\mathcal{O}$-ideal. The problem is to compute an equivalent left $\mathcal{O}$-ideal $J = I\beta$ such that J has norm ℓ^e for some e. The algorithm of [5] provides a PPT algorithm given certain heuristic assumptions on the distribution of primes. The algorithm of that paper is described using "p-extremal" maximal orders, but is generalized to include any maximal order.

The problem's motivation arises from the category equivalence between supersingular elliptic curves and the left ideals of quaternion orders, provided explicitly by Deuring [D41] via a bijection (up to Galois conjugacy) between supersingular curves and maximal orders in a quaternion algebra. The category equivalence derives from this bijection as follows.

Let E_0/K be an elliptic curve, with endomorphism ring $\mathcal{O} = \mathrm{End}(E_0)$ an order of the quaternion algebra $B_{p,\infty} = \mathcal{O} \otimes \mathbb{Q}$. Associated to any pair (E_1, ϕ), with $\phi : E_0 \to E_1$ an isogeny, is a left $\mathcal{O}$-ideal $I = \mathrm{Hom}(E_1, E_0)\phi$ with norm equal to $\deg(\phi)$.

The quaternion ℓ-isogeny path problem is an analogue of the ℓ-isogeny path problem: given E_0, E_1 and small prime ℓ, find an ℓ-power isogeny from E_0 to E_1. The quaternion path problem is the determination of an left $\mathcal{O}$-ideal with ℓ-power norm, where the ideal lies within the equivalence class of a given ideal I.

Kohel-Lauter-Petit-Tignol solve this problem in probabilistic polynomial time [5], posing the question of the difference between the analogous problems. In particular, the Charles-Goren-Lauter hash function [1] is resistant to attack thus far, relying on the ℓ-isogeny path problem. The result implies a clear distinction between the problem in its algebraic and geometric settings and, possibly, suggesting a reduction from the elliptic curve ℓ-isogeny problem to the algebraic analogue.

2 The Kohel-Lauter-Petit-Tignol algorithm

The [5] algorithm is based on the assumption that $\mathcal{O}$ is a "special p-extremal" maximal order for the algorithm with an explicit generalization later. We focus on the key lemma of their assumptions.

Lemma 1. *Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$ containing a subring $\mathbb{Z}\langle i, j\rangle$ with $i^2 = -q, j^2 = -p$ and $ij = -ji$, for q and p coprime. Set $R = \mathcal{O} \cap \mathbb{Q}[i]$ and let D be the discriminant of R. If R is the ring of integers of $\mathbb{Q}[i]$, then $R^\perp = Rj$ and $R + Rj$ is a suborder of index $|D|$ in $\mathcal{O}$. If ω is a generator of R then*

$$\mathrm{Nrd}(x_1 + y_1\omega + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2) \tag{1}$$

where $f(x, y)$ is a principal quadratic form of discriminant D.

Proof. See [5]. □

We can explicitly write $f(x, y)$ as:

$$f(x, y) = x^2 + \mathrm{Trd}(\omega)xy + \mathrm{Nrd}(\omega)y^2 \tag{2}$$

and D as

$$D = \mathrm{Nrd}(\omega) - \frac{\mathrm{Trd}(\omega)^2}{4} \tag{3}$$

If ω is a reduced generator of R (of trace 0 or $\pm$ 1) then for $\alpha = x_1 + y_1\omega$ and $\beta = x_2 + y_2\omega$, the norm form on $R + Rj$ is of the form:

$$\mathrm{Nrd}(\alpha + \beta j) = f(x_1, y_1) + pf(x_2, y_2) \tag{4}$$

The next step is a lemma reducing an ideal I to an isomorphic ideal of different norm.

Lemma 2. *Let I be a left $\mathcal{O}$-ideal of reduced norm N and α an element of I. Then $I\gamma$, where $\gamma = \bar{\alpha}/N$, is a left $\mathcal{O}$-ideal of norm $\mathrm{Nrd}(\alpha)/\mathrm{Nrd}(I)$.*

Proof. See [5]. □

The algorithm now assumes that N, the reduced norm of I is a large prime, coprime to p, ℓ and D. Heuristically, N is expected to be in $\tilde{O}(\sqrt{p})$. Through the use of the above lemma, the problem is then reduced to the effective strong approximation theorem [V80]. To be precise, if I is given by a pair of generators $I = \mathcal{O}(N, \alpha)$, the problem is reduced to finding λ in $\mathbb{Z}$ coprime to N and

$$\beta \equiv \lambda\alpha \mod N\mathcal{O} \tag{5}$$

with $\mathrm{Nrd}(\beta) = N\ell^e$ for some positive integer e. The problem is approached through the following steps

1. Solve for $\gamma \in \mathcal{O}$ with $\mathrm{Nrd}(\gamma) = N\ell^{e_0}$.
2. Solve for $[\mu] = \mu + N\mathcal{O}$ in $(\mathcal{O}/N\mathcal{O})^*$ such that $(\mathcal{O}\gamma/N\mathcal{O}) = I/N\mathcal{O}$.
3. Solve for the strong approximation of $[\mu]$ (mod $N\mathcal{O}$) by $\mu \in \mathcal{O}$ with $\mathrm{Nrd}(\mu) = \ell^{e_1}$.

Our improvement lies in the third step, so we briefly explain this section of the algorithm. This section assumes that ℓ is a non-quadratic residue modulo N. Let also ω be a generator of R of minimal norm, i.e. 1, 2, or $(1+q)/4$, for q a prime equivalent to 3 (mod 4).

Through the second step of the algorithm, we are given as input a lift $\mu_0 = x_0 + y_0\omega + (z_0 + w_0\omega)j$, find $\lambda \in \mathbb{Z}^+$ and $\mu_1 = x_1 + y_1\omega + (z_1 + w_1\omega)j$ such that $\mu = \lambda\mu_0 + N\mu_1$, satisfying the norm equation

$$\mathrm{Nrd}(\mu) = f(\lambda x_0 + Nx_1, \lambda y_0 + Ny_1) + pf(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e \quad (6)$$

for some $e \in \mathbb{Z}^+$, where $f(x, y) = \mathrm{Nrd}(x + y\omega)$ is the principal quadratic form of D.

The problem now is to find (x_1, y_1) and (z_1, w_1) satisfying this equation. This is simplified by taking $x_0 = y_0 = 0$, yielding

$$\mathrm{Nrd}(\mu) = N^2 f(x_1, y_1) + pf(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1) = \ell^e \quad (7)$$

Taking this equation modulo N yields λ through

$$p\lambda^2 f(z_0, y_0) \equiv \ell^e \pmod{N} \quad (8)$$

where the parity of e is chosen according to whether $pf(z_0, w_0)$ is a quadratic residue modulo N. Taking a square root modulo N yields a value of $\lambda \in (0, N)$.

Now that λ has been fixed, we may take the equation modulo N^2 to find

$$\begin{aligned} &p\lambda\Big[\big(2z_0 + \mathrm{Trd}(\omega)w_0\big)z_1 + \big(\mathrm{Trd}(\omega)z_0 + 2\,\mathrm{Nrd}(\omega)w_0\big)w_1\Big] \equiv \\ &\frac{\ell^e - p\lambda^2 f(z_0, w_0)}{N} \pmod{N} \end{aligned} \quad (9)$$

using the explicit form of $f(x, y)$ from (2).

This point is where we alter the algorithm. The original algorithm chooses random solutions (z_1, w_1) to the above equation. Then, to recover x_1 and y_1, they examine

$$f(x_1, y_1) = r := \frac{\ell^e - pf(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1)}{N^2} \quad (10)$$

where e is large enough that this is positive. If the right-hand side is a prime multiplied by a smooth square integer factor, Cornacchia's algorithm [C03] efficiently finds a solution for (x_1, y_1) if it exists, or demonstrates that a solution does not exist. If no solution exists, a new random solution to equation (9) is chosen. Assuming that the values of r behave as random values, we have $r \sim N^4 p|D|$, expecting to test $\log(N^4 p|D|)$ values before a solution is found. With $N = O(\sqrt{p})$, this approach yields $e \sim 3\log_l(p)$.

3 Optimizing the third step

3.1 Premise

The idea behind our improvement is to consider the solutions (z_1, w_1) to equation (9), the space of which is a displaced lattice. We then aim to reduce the

problem to a lattice closest-vector problem, minimizing r, while making sure it has a value suitable for Cornacchia's algorithm to run. We expect this to reduce running time and the value of e; in particular, this approach yields a reduction from $e \sim \frac{7}{2}\log_l(p)$ to $e \sim 3\log_l(p)$.

3.2 Proof of improvement

We start by examining equation (9) and defining the following constants:

$$\begin{aligned} \phi &:= p\lambda\big(2z_0 + \mathrm{Trd}(\omega)w_0\big) \\ \psi &:= p\lambda\big(\,\mathrm{Trd}(\omega)z_0 + 2\,\mathrm{Nrd}(\omega)w_0\big) \\ \chi &:= \frac{\ell^e - \lambda^2 p f(z_0, w_0)}{N} \end{aligned} \tag{11}$$

to write the linear equation in z_0, w_0 as

$$\phi z_1 + \psi w_1 \equiv \chi \pmod{N} \tag{12}$$

The general solution to this equation varies depending on ϕ and ψ. At least one of these is non-zero (otherwise, $D = 0$), so we can find one solution by inversion modulo N.
The general solution space is:

$$(z_1, w_1) \in \begin{cases} \big\langle(\psi, -\phi), (0, N)\big\rangle + (s, t) & \psi \neq 0 \\ \big\langle(\psi, -\phi), (N, 0)\big\rangle + (s, t) & \phi \neq 0 \end{cases} \tag{13}$$

where (s, t) is any solution to the equation (12). For example, if ϕ is non-zero, $(\chi\phi^{-1} \pmod{N}, 0)$ is a valid solution.

Finally, we need to find x_1 and y_1, for which we need equation (10), as in the original algorithm. We recall that [5] choose (z_1, w_1) at random until a solution is found through Cornacchia's algorithm, increasing e as necessary.

We hope to reduce this to a closest-vector problem, minimizing $f(\lambda z_0 + Nz_1, \lambda w_0 + Nw_1)$ in order to reduce the size of e and yield an improvement to the algorithm's efficiency; this must be done while seeking values in (13) suitable for Cornacchia's algorithm.

To do this, we hope to reduce the minimized function to the standard norm by creating new variables, $z = B_0(z_1 - s) + C_0(w_1 - t), w = B_1(z_1 - s) + C_1(w_1 - t)$, where the coeffecients are to be determined, (s, t) is a solution to (12) and (z', w') is the target vector of the CVP problem.

By the definitions of (z, w) and the translated lattice from (13), (z, w) must lie in a lattice L. This would yield

$$\begin{aligned} f(x_1, y_1) &= \frac{A_2 - (z - z')^2 - (w - w')^2}{N^2} = \frac{A_2 - |(z, w) - (z', w')|^2}{2} \\ &= \frac{A_2 - (A_0 + B_0 z_1 + C_0 w_1)^2 - (A_1 + B_1 z_1 + C_1 w_1)^2}{N^2} \end{aligned} \tag{14}$$

Balancing terms between (10) and (14) gives us the following equations.

$$A_2 - A_0^2 - A_1^2 = \ell^e - p\lambda^2 f(z_0, w_0) = N\chi \tag{15a}$$

$$A_0B_0 + A_1B_1 = \frac{\lambda Np(2z_0 + \mathrm{Trd}(\omega)w_0)}{2} = \frac{N\phi}{2} \tag{15b}$$

$$A_0C_0 + A_1C_1 = \frac{\lambda Np(2\,\mathrm{Nrd}(\omega)w_0 + \mathrm{Trd}(\omega)z_0)}{2} = \frac{N\psi}{2} \tag{15c}$$

$$B_0C_0 + B_1C_1 = \frac{N^2p\,\mathrm{Trd}(\omega)}{2} \tag{15d}$$

$$B_0^2 + B_1^2 = N^2p \tag{15e}$$

$$C_0^2 + C_1^2 = N^2p\,\mathrm{Nrd}(\omega) \tag{15f}$$

To find acceptable coefficients, we examine the circles defined by equations (15e) and (15f), defining a radius

$$r := N\sqrt{p} \tag{16}$$

which in turn yields, for some parametrizing angles θ and Θ,

$$\begin{aligned} B_0 &= r\cos\theta & B_1 &= r\sin\theta \\ C_0 &= r\sqrt{\mathrm{Nrd}(\omega)}\cos\Theta & C_1 &= r\sqrt{\mathrm{Nrd}(\omega)}\sin\Theta \end{aligned} \tag{17}$$

Substituting this parametrization into (15d) and using an angle addition formula, we find

$$\begin{aligned} B_0C_0 + B_1C_1 = r^2\sqrt{\mathrm{Nrd}(\omega)}\cos(\theta - \Theta) &= \frac{r^2\,\mathrm{Trd}(\omega)}{2} \\ &\iff \cos(\theta - \Theta) \neq \pm 1 \end{aligned} \tag{18}$$

where the implication follows from $D \neq 0$. The implication here is simply that this equation is satisfied if and only if our choices of z, w are linearly independent in z_1, w_1.

To find the discriminant of (z, w), we use another angle addition formula and the result of (18) to find

$$\begin{aligned} |B_0C_1 - C_0B_1| &= r^2\sqrt{|\mathrm{Nrd}(\omega)|}\,|\sin(\theta - \Theta)| \\ &= r^2\sqrt{\mathrm{Nrd}(\omega)}\sqrt{1 - \cos^2(\theta - \Theta)} \\ &= r^2\sqrt{\mathrm{Nrd}(\omega)}\sqrt{1 - \frac{\mathrm{Trd}^2(\omega)}{4\,\mathrm{Nrd}(\omega)}} \\ &= r^2\sqrt{\mathrm{Nrd}(\omega) - \frac{\mathrm{Trd}^2(\omega)}{4}} \\ &= N^2p\sqrt{D} \end{aligned} \tag{19}$$

We assume without loss of generality that $B_0C_1 - C_0B_1$ is positive by permuting z and w if necessary.

By inverting (15b) and (15c) using the discriminant from (19), we can find explicit formulae for A_0 and A_1 in terms of B_0, B_1, C_0 and C_1

$$\begin{aligned} A_0 &= \frac{C_1\phi - B_1\psi}{2Np\sqrt{D}} \\ A_1 &= \frac{B_0\psi - C_0\phi}{2Np\sqrt{D}} \end{aligned} \tag{20}$$

Finally, we determine (z', w') using (14)

$$\begin{aligned} z' &= -(A_0 + B_0 s + C_0 t) \\ w' &= -(A_1 + B_1 s + C_1 t) \end{aligned} \tag{21}$$

where (s, t) is the the solution (s, t) used in (13).

We have one degree of freedom remaining, which must used to set Θ. For example, $\Theta = 0$ gives an explicit general formula for the coefficients in (z, w):

$$\begin{aligned} B_0 &= \frac{N\sqrt{p}\,\mathrm{Trd}(\omega)}{2\sqrt{\mathrm{Nrd}(\omega)}} & B_1 &= -\frac{N\sqrt{pD}}{\sqrt{\mathrm{Nrd}(\omega)}} \\ C_0 &= N\sqrt{p\,\mathrm{Nrd}(\omega)} & C_1 &= 0 \\ A_0 &= \frac{\psi}{2\sqrt{p\,\mathrm{Nrd}(\omega)}} & A_1 &= \frac{\mathrm{Trd}(\omega)\psi - 2\,\mathrm{Nrd}(\omega)\phi}{4\sqrt{pD\,\mathrm{Nrd}(\omega)}} \end{aligned} \tag{22}$$

using (18) and (19), and where the sign of B_1 is chosen to leave $B_0C_1 - B_1C_0$ positive.

We know from (13) that (z, w) is in $\big\langle (B_0\psi - C_0\phi, B_1\psi - C_1\phi), N(C_0, C_1)\big\rangle$ or $\big\langle (B_0\psi - C_0\phi, B_1\psi - C_1\phi), N(B_0, B_1)\big\rangle$, which will form our lattice L. The discriminant of the first lattice is

$$\begin{aligned} & N|C_1(B_0\psi - C_0\phi) - C_0(C_1\phi - B_1\psi)| \\ =& N|B_0C_1 - C_0B_1||\psi| \\ =& N^3p\sqrt{D}|\psi| \end{aligned} \tag{23}$$

The discriminant of the second is clear by symmetry:

$$N^3p\sqrt{D}|\phi| \tag{24}$$

We can remove the extra $|\phi|, |\psi|$ term from the discriminant by expressing the solution space in (13) as

$$(z_1, w_1) \in \begin{cases} \big\langle (1, -\phi\psi^{-1}), (0, N)\big\rangle + (s, t) & \psi \neq 0 \\ \big\langle (\psi\phi^{-1}, -1), (N, 0)\big\rangle + (s, t) & \phi \neq 0 \end{cases} \tag{25}$$

which gives our lattice as

$$(z, w) \in \begin{cases} \big\langle (B_0 \ - C_0\phi\psi^{-1}, B_1 - C_1\phi\psi^{-1}), N(C_0, C_1)\big\rangle & \psi \neq 0 \\ \big\langle (B_0\psi\phi^{-1} - C_0, B_1\psi\phi^{-1} - C_1), N(B_0, B_1)\big\rangle & \phi \neq 0 \end{cases} \tag{26}$$

with discriminant $N^3p\sqrt{D}$. By the Gaussian heuristic, we estimate the lattice contains a basis with vectors both approximately $N^{3/2}p^{1/2}D^{1/4}$. We therefore

expect that the smallest value of e for the right-hand side of (14) to be positive to be $e \geq \log_\ell(N^3 p D^{1/2}) \sim \frac{5}{2}\log p$, by $N = \tilde{O}(p^{1/2})$. However, the value of $f(x_1, y_1)$ at this value of e is unlikely to meet the criteria to run Cornacchia's algorithm. Assuming that values returned by the norm of this CVP behave as random values, we expect to run $O(\log\log p)$ trials before a suitable (prime) value for $f(x_1, y_1)$ is found, implying $e \sim \frac{5}{2}\log(p) + O(\log\log p)$.

The algorithm of [5] is expected to run in polynomial time under heuristic assumptions, producing ideals of norm ℓ^e, where

$$e \sim \log_\ell(p/N) + \log_\ell(N^4 p|D|) \sim \frac{7}{2}\log_l(p). \tag{27}$$

assuming that $N = \tilde{O}(\sqrt{p})$. Here, the first term accounts for the contribution from the first step of the algorithm (finding γ), and the second term is $\mathrm{Nrd}(\mu)$ from the third step of the algorithm. With our improvement by $\log N$ on the second term, a new value of $e \sim 3\log_\ell p$ can be reached.

4 Conclusions

As in the original algorithm, we have produced a probabilistic polynomial time algorithm for the quaternion ℓ-isogeny problem, running in expected polynomial time given heuristic assumptions on the distribution of primes.

We expect the Deuring correspondence, providing us the category equivalence of these problems, to allow the algorithm of [5] to provide attacks on its analogue in the supersingular ℓ-isogeny problem, in particular, the Charles-Goren-Lauter hash function [1]. Also of significance will be the effect on the identification protocols of [GPS], the main signature scheme of which is built upon the algorithm we have improved: many of its heuristic assumptions and a priori bounds would be affected by this complexity analysis.

We hope to continue improving this algorithm by reevaluating the first two steps of the algorithm. Furthermore, the steps involved (such as lifting the problem $\pmod{N\mathcal{O}}$) are somewhat non-natural and a more direct approach, if possible, may be of interest.

References

[1] Denis Charles, Eyal Goren, Kristin Lauter, *Cryptographic hash functions from expander graphs* J. Cryptology, 22(1):93-113 2009

[2] Giuseppe Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} c_h x^{n-h} y^h = p$, Giornale di Matemathice di Battaglini, 46:33-90, 1903

[3] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 14:197-272, 1941

[4] Steven Galbraith, Christophe Petit, Javier Silva, *Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems* Cryptology ePrint Archive, Report 2016/1154, 2016

[5] David Kohel, Kristin Lauter, Christophe Petit, Jean-Pierre Tignol, *On the quaternion ℓ-isogeny problem*, LMS Journal of Computation and Mathematics, 17A:418-432, 2014