Eisenträger-Hallgren-Lauter-Morrison-Petit

Shahed Sharif

April 6, 2019

1 The Deuring correspondence

Fix an odd prime p and let k be a finite field of characteristic p. Let $\operatorname{End} E$ be the ring of endomorphisms of E over $\overline{k}$. Recall that an elliptic curve E/k is *supersingular* if and only if the endomorphism ring $\operatorname{End} E$ is isomorphic to an order in a quaternion algebra. Let B be the quaternion algebra in question. Then the *Deuring correspondence* states that there is a bijection

$$\{E/\overline{k} \text{ supersingular}\}/\cong, \text{conj} \longrightarrow \{\mathscr{O} \subset B \text{ maximal order}\}/\cong,$$

where the first set is isomorphism classes of supersingular elliptic curves up to conjugacy over $\mathbb{F}_p$. Since all supersingular elliptic curves have j-invariant in $\mathbb{F}_{p^2}$, the left side contains either 1 or 2 isomorphism classes per conjugacy class.

Fix a prime $\ell \neq p$. Let $G = G(\ell)$ be the graph whose vertices are isomorphism classes of supersingular elliptic curves, and whose edges are ℓ-isogenies. A number of cryptographic primitives are based on G. The main point of this paper is the following:

Question 1. *Can algorithms on G be efficiently reduced to algorithms on B?*

The answer is, essentially, yes. This means that working directly with B either is hard, or will lead to a break of the associated cryptosystems.

2 Quaternion algebras

For $a, b \in \mathbb{Q}$ nonzero, let $H := H(a, b)$ be the quaternion algebra with $\mathbb{Q}$-basis $1, i, j, ij$ for which $i^2 = a$, $j^2 = b$, and $ij = -ji$. Every quaternion algebra over $\mathbb{Q}$ can be written this way for some a, b.

Fix a supersingular elliptic curve E. Then the quaternion algebra B is completely determined by p:

Theorem 2.1. *With notation as above, $B \cong H(-p, -q)$ where*

- *if $p \equiv 3 \pmod 4$, then $q = 1$;*
- *if $p \equiv 5 \pmod 8$, then $q = 2$;*

- *if $p \equiv 1 \pmod 8$, then q is a prime satisfying certain arithmetic conditions.*

From now on, let B be as above.

For $\alpha \in B$, if

$$\alpha = a_0 + a_1 i + a_2 j + a_3 ij$$

then let

$$\overline{\alpha} = a_0 - a_1 i - a_2 j + a_3 ij.$$

Define $\mathrm{Nrd}(\alpha)$ to be $\alpha \cdot \overline{\alpha}$. One checks that $\mathrm{Nrd}(\alpha) \in \mathbb{Q}$.

Given a maximal order $\mathscr{O} \subset B$, let $I \subset \mathscr{O}$ be an ideal—left, right, or two-sided. Then

$$\{\mathrm{Nrd}(\alpha) \mid \alpha \in I\}$$

is a fractional $\mathbb{Q}$-ideal. Define $\mathrm{Nrd}\, I$ to be the positive generator of this ideal.

If $I \subset B$ is a rank 4 $\mathbb{Z}$-module (for example, an ideal of $\mathscr{O}$), then define

$$\mathscr{O}_R(I),$$

the *right order* of I, to be $\{\beta \in B \mid I\beta \subset I\}$. The *left order* $\mathscr{O}_L(I)$ is defined similarly.

Suppose $I \subset \mathrm{End}\, E$ is a left ideal. Define $E[I]$ to be $\cap \ker \alpha$ for $\alpha \in I$. Define E_I to be $E/E[I]$ and φ_I the natural isogeny. Then

$$\deg \varphi_I = \mathrm{Nrd}\, I.$$

Furthermore, we can relate $\mathrm{End}\, E$ and $\mathrm{End}\, E_I$ to each other.

Proposition 2.2. *The map*

$$\varphi_I^* : \mathrm{Hom}(E_I, E) \to I$$

given by $\varphi_I^*(\psi) = \psi\varphi_I$ is an isomorphism of left $\mathrm{End}\, E$*-modules.*

Fix an isomorphism $\mathrm{End}\, E \to \mathscr{O} \subset B$, where $\mathscr{O}$ is a maximal order.

Proposition 2.3. *The map*

$$\iota : \mathrm{End}\, E_I \to B$$

given by

$$\iota(\beta) = \frac{1}{\deg \varphi_I} \varphi_I^\vee \beta \varphi_I$$

induces an isomorphism of $\mathrm{End}\, E_I$ *with* $\mathscr{O}_R(I)$.

Computationally, we would like to represent maximal orders in B. The typical way to do this is to give a $\mathbb{Z}$-basis. Fortunately, such representations can be made to be small.

Theorem 2.4. *Given a maximal order $\mathscr{O} \subset B$, there exists a maximal order $\mathscr{O}'$ isomorphic to $\mathscr{O}$ with a basis of size $O(\log p)$.*

Here, the size means the size of the numerator and denominator of coefficients in $1, i, j, ij$.

3 Computational problems and reductions

EHLMP explores five related computational problems:

Problem 1 (Constructive Deuring)**.** *Given a maximal order $\mathcal{O} \subset B$, find a j-invariant of a curve E with* $\operatorname{End} E \cong \mathcal{O}$.

Problem 2 (Max Order)**.** *Given a supersingular curve E, output a compact representation for a maximal order $\mathcal{O} \subset B$ with $\mathcal{O} \cong \operatorname{End} E$.*

Problem 3 (End Ring)**.** *Given a supersingular j-invariant j_0, compute 4 rational maps giving a $\mathbb{Z}$-basis for* $\operatorname{End} E$*, E satisfying $j(E) = j_0$.*

Problem 4 (Action on ℓ-torsion)**.** *If $\nu : \mathcal{O} \to \operatorname{End} E$ is an isomorphism, denote ν_ℓ the composition*

$$\mathcal{O} \to \operatorname{End} E \to \operatorname{End} E[\ell].$$

Let $E[\ell] = \langle P_1, P_2 \rangle$. Given a $\mathbb{Z}$-basis $\beta_1, \beta_2, \beta_3, \beta_4$ for $\mathcal{O}$, compute $\nu_\ell(\beta_i)(P_j)$ for some choice of ν.

Problem 5 (Pathfinding)**.** *Given E, E' representing vertices in G, find a path between them; that is, find a cyclic ℓ-power isogeny between them.*

The main results of EHLMP are as follows. All theorems depend on heuristic assumptions on certain quadratic forms and on the structure of the isogeny graphs; in particular, "polynomial time" below should really be "heuristic polynomial time."

Theorem 3.1. *Constructive Deuring can be solved in polynomial time.*

Theorem 3.2. *Max Order, End Ring, and Pathfinding are computationally equivalent.*

That is, there are polynomial-time reductions between them.

Theorem 3.3. *Given an oracle for Max Order and Action on ℓ-torsion, one can solve End Ring and Pathfinding in polynomial time.*

This appears to be weaker than the previous theorem! Morrison has informed me that the difference is that the algorithm in the latter theorem makes use of fewer heuristic assumptions, as well as fewer oracular queries.

4 Sketch of proofs

4.1 Auxiliary algorithms

We will be using the following auxiliary algorithms. Some of these are from other papers, and are thus treated as black boxes.

Special Constructive Deuring. For each B given above, Pizer found a special maximal order $\mathscr{O}_0$ that can be easily written down. For example, when $p \equiv 3 \pmod 4$, $\mathscr{O}_0$ is generated by $1, j, \frac{j+k}{2}, \frac{1+i}{2}$.

Let $p \equiv 3 \pmod 4$, and let E_0 be the curve $y^2 = x^3 + x$. Let π be Frobenius and φ a nontrivial automorphism of E_0. Then there is an explicit isomorphism $\theta : B \to \operatorname{End} E_0 \otimes \mathbb{Q}$ given by

$$(1, i, j, k) \mapsto (1, \varphi, \pi, \pi\varphi)$$

But $\theta(\mathscr{O}_0) \subset \operatorname{End} E_0$, and hence the two are isomorphic. To check that this is true, one cannot directly check if, say, $\theta(\frac{1+i}{2})$ lies in $\operatorname{End} E_0$. Instead, one shows that $E_0[2] \subset \ker \theta(\frac{1+i}{2})$.

Even when $p \not\equiv 3 \pmod 4$, EHLMP shows we can find E_0 and an isomorphism $\mathscr{O}_0 \to \operatorname{End} E_0$ in polynomial time. The idea is that $j(E_0) \in \mathbb{F}_p$ and $\mathbb{Q}(\sqrt{-q}) \hookrightarrow \operatorname{End} E_0 \otimes \mathbb{Q}$. The algorithm constructs a list of j-invariants for curves with these two properties; there are $O(\log p)$ of them. For each curve E from the list, we compute θ and check whether $\theta(\mathscr{O}_0) \subset \operatorname{End} E$.

Connecting ideal. Given two maximal orders $\mathscr{O}, \mathscr{O}' \subset B$, compute I for which $\mathscr{O} = \mathscr{O}_L(I)$ and $\mathscr{O}' = \mathscr{O}_R(I)$. (Kirschmer-Voight 10)

Factored ideal. Given a left ideal $I \subset \mathscr{O}$, find an ideal J, written as a product of ideals of norm ℓ, such that $\alpha I = J$ for some J. In our situation, they will induce the same isogeny. (Galbraith-Petit-Silva 17) There is an older version due to (Kohel-Lauter-Petit-Tignol 14) which instead outputs J as a product of ideals with norm prime of size $O(\log p)$.

Ideal-isogeny. Given J as above an ideal in $\mathscr{O}_0$, compute $\varphi : E_0 \to E$ corresponding to J. (Galbraith-Petit-Silva 17)

Constructive Deuring

Given a maximal order $\mathscr{O}$, we would like to find E with $\operatorname{End} E \cong \mathscr{O}$.

1. Compute a connecting ideal I between $\mathscr{O}_0$ and $\mathscr{O}$.
2. Use Factored Ideal to replace I with J given as a product of ideals with small prime norm.
3. Compute the corresponding isogeny $\varphi : E_0 \to E$. Then $\operatorname{End} E \cong \mathscr{O}$.

Max Order → Pathfinding

Given E and E' representing vertices in the isogeny graph G, we want to find a path between them.

1. Use our oracle to compute $\mathscr{O} \subset B$ such that $\mathscr{O} \cong \operatorname{End} E$.

2. Compute a connecting ideal I between $\mathscr{O}_0$ and $\mathscr{O}$.

3. Use Factored Ideal to replace I with J given as a product of norm ℓ ideal.

4. Compute the corresponding isogeny $\varphi : E_0 \to E$. This gives a path from E_0 to E.

5. Repeat with E' and concatenate paths.

Pathfinding → End Ring

We start with E. Initialize $R = \mathbb{Z}$.

1. Do a random walk to find a path to random E' in G.

2. Use the pathfinding algorithm to find a path from E to E'; under our heuristic assumptions, this will be a different path.

3. The concatenation will be an endomorphism α of E. Replace R with $R[\alpha]$.

4. Repeat until R is a maximal order.

We can verify the last condition by computing the discriminant of the associated norm form, which should be $4p^2$.

End Ring → Max Order

Given E, we would like to compute a $\mathbb{Z}$-basis for $\mathscr{O} \subset B$ such that $\mathscr{O} \cong \operatorname{End} E$. We first define inner products on B and $\operatorname{End} E \otimes \mathbb{Q}$, which agree for any choice of isomorphism between them. On B, our inner product is just

$$\langle \alpha, \beta \rangle = \alpha\overline{\beta} + \overline{\alpha}\beta.$$

Furthermore, under the inner product $(1, i, j, ij)$ is an orthogonal basis for B. Fix an embedding $\operatorname{End} E \hookrightarrow B$. If α comes from an endomorphism φ, one checks that $\varphi^\vee$ maps to $\overline{\alpha}$. Thus we can compute the inner product on $\operatorname{End} E$, and it is independent of the embedding. Write V for $\operatorname{End} E \otimes \mathbb{Q}$, viewed as an inner product space. Observe that for $x \in V$, we can define $\operatorname{Nrd}(x)$ as $\frac{1}{2}\langle x, x \rangle$.

1. Use Gram-Schmidt to compute an orthogonal basis $1, \alpha', \beta', \alpha'\beta'$ for V.

2. Use this basis to find $\iota \in V$ for which $\operatorname{Nrd} \iota = q$.

3. Find a new orthogonal basis $(1, \iota, \delta, \iota\delta)$.

4. Find λ in the span of $\delta, \iota\delta$ such that $\operatorname{Nrd} \lambda = p$.

5. Identify V with B via $(1, \iota, \lambda, \iota\lambda) = (1, i, j, ij)$. Write $\alpha, \beta, \alpha\beta$ in terms of $1, i, j, ij$.

5 Morrison on Heuristic 3

Given a vertex E in G, a loop starting and ending at E corresponds to an ℓ-power endomorphism of E. One of the heuristic assumptions in EHLMP, Heuristic 3, is that these endomorphisms generate $\mathrm{End}\, E$—in particular, the Pathfinding $\to$ End Ring algorithm makes use of this assumption. I asked Morrison if there is any data about the heuristic, and his (lightly edited) response follows:

> My thoughts on heuristic 3 are hard to formalize, but I think there is some reason to be skeptical that cycles in G starting at j are distributed "randomly". For example, if $\ell = 2$, then any two cycles with no repeated vertices which start at j will share an edge; if the terminal vertex of that edge is not equal to j^p, then the order generated by the two cycles can not be maximal.
>
> Another problem: suppose we try to randomize our cycles in G by first taking a walk P from j to another vertex j', and then computing a cycle C at j'. Let C' be the cycle $C' = P + C + \mathrm{dual}(P)$. The corresponding order S generated by (an endomorphism arising from C') will embed into $\mathrm{End}(E(j))$ and $\mathrm{End}(E(j'))$. Or, put another way, the order S is not maximal at ℓ and so in particular $S \otimes \mathbb{Q}$ intersected with $\mathrm{End}(E(j))$ is not equal to S, but is larger than S.