Constructing the Deuring Correspondence with Applications to Supersingular Isogeny-Based Cryptography

Dimitrij Ray

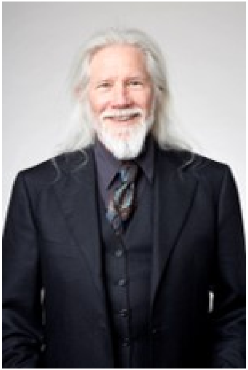
Technische Universiteit Eindhoven
University of Technology

August 3, 2018

Contents

The first public-key cryptosystem

Diffie-Hellman key exchange (1976)



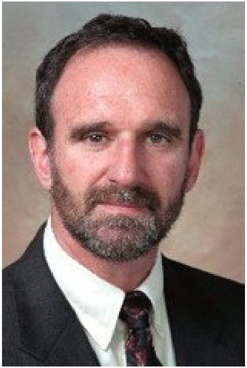


Image source: Wikimedia Commons

Enter quantum computers

Image source: D-Wave Systems

- "Algorithms for quantum computation: Discrete logarithms and factoring" (Peter Shor, 1994)

SIDH to the rescue

- **S**upersingular **I**sogeny **D**iffie-**H**ellman (SIDH) by Jao and De Feo (2011)
- Uses isogenies between supersingular elliptic curves

Curves!

- SIDH uses "initial" curve E_0 over $\mathbb{F}_{p^2}$ as its parameter, where E_0 has a certain number of points.
- Proposal by Costello, Longa, Naehrig (2016): use $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$ where $p = 2^{372}3^{239} - 1$.
- Constructing random curves might be difficult
- The Kohel-Lauter-Petit-Tignol algorithm, used in an attack and a signature scheme.

Elliptic curves

Definition

An elliptic curve over a field K is a nonsingular projective curve of genus one with a specified base point O.

When the field K is not of characteristic 2 or 3, an elliptic curve can be written as

$$y^2 = x^3 + Ax + B$$

where $A, B \in K$.

Elliptic curves

$y^2 = x^3 + 3x + 1$ over $\mathbb{R}$

Elliptic curves

$$y^2 = x^3 + Ax + B, \quad A, B \in K$$

$$j = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

- Elliptic curves E_1 and E_2 isomorphic over $\overline{K}$ if and only if $j(E_1) = j(E_2)$ (important for SIDH!).
- Set of points form an abelian group.

Isogenies

Definition

Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2$$

such that $\phi(O_{E_1}) = O_{E_2}$. Two elliptic curves E_1 and E_2 are *isogenous* if there exists an isogeny from E_1 to E_2 where $\phi(E_1) \neq \{O_{E_2}\}$.

- Isogenies are birational maps.
- We can compute isogenies from its kernel (and vice versa).

One ring to rule some of them

- An isogeny from a curve E to itself is called an *endomorphism*. The set of all endomorphisms of E forms a ring, called the *endomorphism ring*.
- Some endomorphisms:
  - The multiply-by-m map $[m]$
  - If $E/\mathbb{F}_q$ The Frobenius map $\pi : (x, y) \mapsto (x^q, y^q)$
  - If a curve is *supersingular*, there are less obvious ones $\rightarrow$ "unusual".

Endomorphism ring

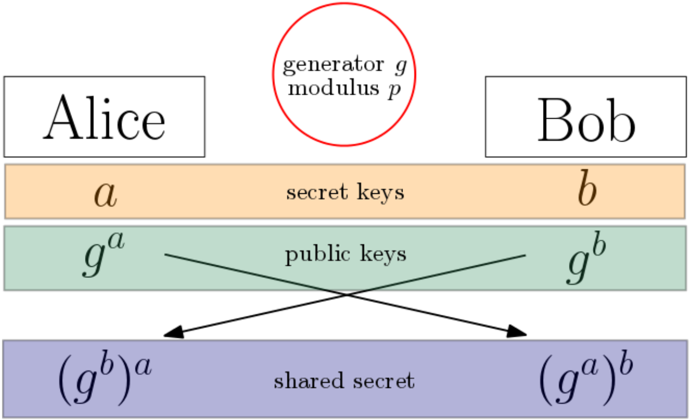
Theorem

Let E be an elliptic curve defined over a field K. The endomorphism ring of E is either:

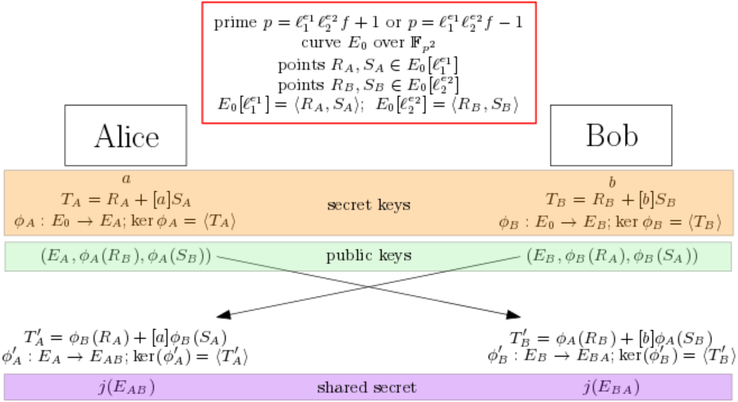
1. *the ring $\mathbb{Z}$,*
2. *an order in an imaginary quadratic field, or*
3. *a maximal order in a quaternion algebra.*

If $\operatorname{char}(K) = 0$, only the first two are possible.

The Diffie-Hellman key exchange



The Jao-De Feo algorithm (SIDH)



Quaternion algebra

Definition

A *quaternion algebra* B over a field K not of characteristic 2 is an algebra with basis 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ for B as a K-vector space, such that

$$\mathbf{i}^2 = a,\ \mathbf{j}^2 = b,\ \text{ and } \mathbf{k} = \mathbf{ij} = -\mathbf{ji}$$

for some fixed a, $b \in K^*$.
This quaternion algebra is denoted $\left(\frac{a,b}{K}\right)$.

Quaternion algebras are **NOT** commutative.

Reduced norm

Definition

Let $\alpha = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ where $t, x, y, z \in K$ be an element of a quaternion algebra. The reduced norm of α are

$$\mathrm{nrd}(\alpha) = \alpha\bar{\alpha},$$

where

$$\bar{\alpha} = t - x\mathbf{i} - y\mathbf{j} - z\mathbf{k}.$$

There, and back again: Deuring correspondence

Definition

Let B be a finite-dimensional $\mathbb{Q}$-algebra. An *order* $\mathcal{O} \subset B$ is a lattice that is also a subring of B. An order is *maximal* if it is not properly contained in another order.

- **Deuring's correspondence:**
  - The endomorphism ring is isomorphic to a **maximal order** in the quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$.
  - For every maximal order in B, there exists a supersingular elliptic curve whose endomorphism ring is isomorphic to it.
- The elements a and b depend on the prime p.

Constructing the Deuring correspondence

Given: a curve E_0 with a known endomorphism ring $\mathcal{O}_0$; a maximal order $\mathcal{O}$

1. Construct a left ideal I of $\mathcal{O}_0$ such that there exists an elliptic curve E' with endomorphism ring $\mathcal{O}$ and an isogeny $\phi_I : E_0 \mapsto E'$ with kernel I. (uses KLPT)
2. Compute the isogeny $\phi_I : E_0 \mapsto E'$.
3. Using the isogeny, compute E'.

KLPT in a nutshell

- Curve defined over $\mathbb{F}_{p^2}$ where $p \equiv 3 \pmod 4$.
- $B = \left(\frac{-1,-p}{\mathbb{Q}}\right)$
- Uses the maximal order

$$\mathcal{O}_0 = \left\langle 1, \mathbf{i}, \frac{1+\mathbf{k}}{2}, \frac{\mathbf{i}+\mathbf{j}}{2} \right\rangle \subseteq B.$$

isomorphic to the endomorphism ring of

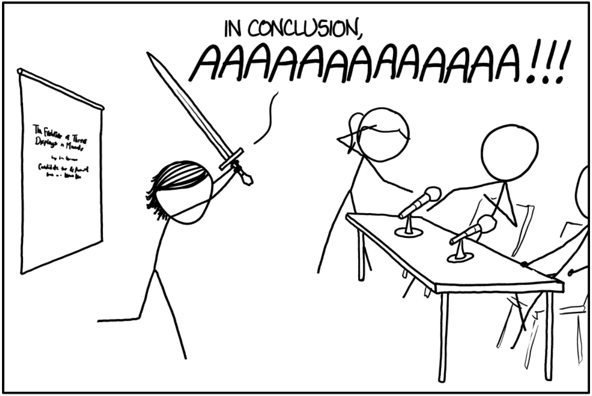
$$E_0 : y^2 = x^3 + x.$$

- Constructing the left ideal I to have powersmooth norm $\rightarrow$ allows the isogeny construction to be efficient.

Implementation

The Sage program is available at:
`https://github.com/dimitrijray/masters-thesis`

Thank you!



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

Image: xkcd

The KLPT algorithm

- Let $\mathcal{O}_0$ be the maximal order that is generated as a $\mathbb{Z}$-module as

$$\mathcal{O}_0 = \left\langle 1, \mathbf{i}, \frac{1+\mathbf{k}}{2}, \frac{\mathbf{i}+\mathbf{j}}{2} \right\rangle \subseteq B.$$

- The order $\mathcal{O}_0$ is isomorphic to the endomorphism ring of the curve

$$E_0 : y^2 = x^3 + x.$$

The KLPT algorithm

Let I be a left $\mathcal{O}$-ideal, then:

1. Compute the ideal:
   1. Compute an element $\delta \in I$ and an ideal $I' = I\bar{\delta}/\operatorname{nrd}(I)$ of some prime norm N.
   2. Fix a powersmoothness bound $s = (7/2)\log p$ and an odd s-powersmooth number S. Find $\beta \in I'$ with norm NS.
   3. Output $J = I'\bar{\beta}/N$.

The KLPT algorithm

Let I be a left $\mathcal{O}$-ideal, then:

2. Compute the isogeny:
   1. Write the norm of J as its prime factorization $\mathrm{nrd}(J) = \prod_{i=1}^{r} \ell_i^{e_i}$ and write $J = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$.
   2. Let $\varphi_0 = [1]_{E_0}$. For every $1 \leq i \leq r$:
      1. Compute a basis (P_i, Q_i) of $E_0[\ell_i^{e_i}]$.
      2. For every generator α_k of J, compute $\alpha_k(P_i)$ and $\alpha_k(Q_i)$.
      3. Find a point R_i of order ℓ_i such that $\alpha_k(R_i) = O$ for all k. This point generates $\ker \phi_I \cap E_0[\ell_i^{e_i}]$.
      4. Compute an isogeny ϕ_i with kernel generated by $\varphi_{i-1}(R_i)$, then compute the composition $\varphi_i = \phi_i \varphi_{i-1}$.

Constructing an ideal of prime norm

- Target: an ideal I' that is equivalent to the input ideal I but with prime norm.
- i.e. $I' = Iq$, $q \in B$, $\operatorname{nrd}(I')$ prime.

Lemma

Let I be a left $\mathcal{O}$-ideal of reduced norm $\operatorname{nrd}(I)$ and δ an element of I, then $I\gamma$, where $\gamma = \bar{\delta}/\operatorname{nrd}(I)$ is a left $\mathcal{O}$-ideal of norm $\operatorname{nrd}(\delta)/\operatorname{nrd}(I)$.

Constructing an ideal of powersmooth norm

- Target: find an element β of I' with norm NS where N is prime and S is powersmooth.
- If such an element found: construct $J = I'\bar{\beta}/N$. We have $\mathrm{nrd}(J) = S$, thus powersmooth.
- Powersmoothness needed for the isogeny computation step, since we will be solving DLP.
- Finding β requires solving *sum-of-squares problem*: given positive integers d and m such that $\gcd(d, m) = 1$, determine integers (x, y) such that

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

- Can be solved with Cornacchia's algorithm.

Searching for β

- Alternative 1: do a brute force search for all β with norm NS such that $I'\bar{\beta} \subseteq N\mathcal{O}_0$
- Write $\beta = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, and then solve the norm equation
$$a^2 + b^2 + p(c^2 + d^2) = NS$$
using Cornacchia
- Will later see that this is not efficient.

Searching for β

- Alternative 2: write $\beta = \beta_1\beta_2'$, whose norms are NS_1 and S_2 respectively, where S_1 and S_2 are powersmooth numbers.
- To construct each β: write $I' = N\mathcal{O}_0 + \mathcal{O}_0\alpha$, where $\alpha \in I'$ such that $\gcd(N^2, \mathrm{nrd}(\alpha)) = N$
- The element β_1 is then constructed like before: solve

$$a^2 + b^2 = NS_1 - p(c^2 + d^2).$$

Solving for β_2'

- Find an element β_2 of the form $C\mathbf{j} + D\mathbf{k}$ which solves

$$(\mathcal{O}_0\beta_1)\beta_2 = \mathcal{O}_0\alpha \mod N\mathcal{O}_0.$$

- How likely to find a solution?

Solving for β_2'

Proposition

Let $\alpha \in I'$, $\beta_1 \in \mathcal{O}_0$, and $\beta_2 \in \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{k}$. Consider the equation of ideals

$$(\mathcal{O}_0\beta_1)\beta_2 = (\mathcal{O}_0\alpha) \mod N\mathcal{O}_0.$$

1. *If N is inert, the equation is always solvable.*
2. *If N is split, it is solvable with probability $\frac{N^2-2N+3}{(N+1)^2}$.*

Solving for β_2'

Lemma

The quotient ring $\mathcal{O}_0/N\mathcal{O}_0$ is a quaternion algebra over $\mathbb{Z}/N\mathbb{Z}$.

Lemma

The quotient ring $\mathcal{O}_0/N\mathcal{O}_0$ is isomorphic to the matrix ring $M_2(\mathbb{Z}/N\mathbb{Z})$.

Corollary

The quotient ring $\mathcal{O}_0/N\mathcal{O}_0$ has $N+1$ nontrivial left ideals.

Solving for β_2'

Lemma

Let R be the ring $\mathbb{Z} + \mathbb{Z}\mathbf{i}$ and let $\mathcal{L}$ be the set of all nontrivial left $\mathcal{O}_0$-ideals. The map

$$\rho: \quad \mathcal{L} \times (R/NR)^* \to \mathcal{L}$$
$$(I, \beta) \mapsto I\beta$$

is a group action whose kernel is $(\mathbb{Z}/N\mathbb{Z})^*$.

1. *If N is split in R, the group action has an orbit of size $N-1$ and two fixed points.*
2. *If N is inert in R, the group action has only one orbit.*

Solving for β_2': after β_2

- Find an element β_2' such that $\beta_2' = \lambda\beta_2 \mod N\mathcal{O}_0$ and $\mathrm{nrd}(\beta_2') = S_2$ for some $\lambda \in (\mathbb{Z}/N\mathbb{Z})^*$.
- Want this β_2' to be of the form

$$\beta_2' = v + w\mathbf{i} + x\mathbf{j} + y\mathbf{k}.$$

- Solve:

$$v^2 + w^2 + p(x^2 + y^2) = S_2.$$

Technische Universiteit Eindhoven University of Technology

Solving for β_2': after β_2

- Condition that $\beta_2' = \lambda\beta_2 \pmod{N\mathcal{O}_0}$ is equivalent to

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

  for some $a, b, c, d \in \mathbb{Z}$. Substitute for v, w, x, y.
- Yields

$$N^2(a^2 + b^2) + p\left((\lambda C + cN)^2 + (\lambda D + dN)^2\right) = S_2.$$

- Consider modulo N and N^2, then use Cornacchia.

Computing isogenies

- Need to find the kernel of the isogeny: the set of points P such that $\alpha(P) = O$ for all $\alpha \in J$, the output ideal.
- What is $\alpha(P)$?
- Let $\phi : (x, y) \mapsto (-x, \iota y)$ be the "square root of -1" map, and $\pi : (x, y) \mapsto (x^p, y^p)$ be the Frobenius map. There is an isomorphism of quaternion algebras:

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

Computing isogenies

- Write $\alpha = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$
- Compute

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

Computing isogenies

- Strategy: compute the kernels (and therefore the isogenies) in $E_0[\ell_i^{e_i}]$ for each prime factor $\ell_i^{e_i}$ of $\mathrm{nrd}(J)$, then compose them Chinese remainder theorem-style.
- Compute a basis of each $E_0[\ell_i^{e_i}]$. Let $\{P_i, Q_i\}$ be a basis.
- Compute $\alpha(P_i)$ and $\alpha(Q_i)$ for every α in the basis of J
- 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.
- Compute an isogeny with kernel generated by $\varphi_{i-1}(R_i)$, where $\varphi_0 = [1]_{E_0}$. Proceed through all i step-by-step, constructing the full isogeny by composition.

A potential improvement

- Recall: a step in the algorithm involved constructing an element β of norm NS
- Since I' has norm N, we can write

$$I' = N\mathcal{O}_0 + \mathcal{O}_0\alpha$$

where $\alpha \in I'$ such that $\gcd(\mathrm{nrd}(\alpha), N^2) = N$.

- Condition $I'\bar{\beta} \subseteq N\mathcal{O}_0$ is equivalent to

$$(\mathcal{O}_0\alpha)\bar{\beta} = \mathbf{0} \pmod{N\mathcal{O}_0}$$

where $\mathbf{0}$ is the zero ideal.

A potential improvement

- The equation of ideals is then equivalent to

$$\alpha\bar{\beta} = 0 \pmod{N\mathcal{O}_0}$$

- $\beta = \alpha \pmod{N\mathcal{O}_0}$ is a solution.
- Rewrite this solution as

$$\beta = \alpha + Nu + Nv\mathbf{i} + Nw\mathbf{j} + Nx\mathbf{k}$$

  for some $u, v, w, x \in \frac{1}{2}\mathbb{Z}$.
- Solving the norm equation gives a family of solutions $(v, w, x) = \lambda(b, c, d)$ for some λ.
- May help the KLPT algorithm by plugging back the family of solutions and solving a generalized sum-of-squares problem.

Enumerating powersmooth numbers S_1 and S_2

- Galbraith, Petit, Silva (2017) gave bounds: $S_1 > p \log p$ and $S_2 > p^3 \log p$
- Let s be the powersmooth bound and let ℓ_i be the i-th odd prime.

Initializing S_1

For S_1:

1. Set $S_1 = \ell_1^{e_1}$, where $e_1 = \lfloor(\lfloor\log_{\ell_1} s\rfloor)/2\rfloor)$ and set $i = 2$.
2. While $S_1 \leq p \log p$ and $e_i > 0$, replace S_1 by $S_1 \cdot \ell_i^{e_i}$ where

$$e_i = \left\lfloor \frac{\lfloor \log_{\ell_i} s \rfloor}{2} \right\rfloor.$$

Increment i.

Initializing S_2

For S_2:

1. Set $S_2 = \ell_1^{e_1}$, where $e_1 = \lceil (\lfloor \log_{\ell_1} s \rfloor)/2 \rceil$ and set $i = 2$.
2. While $S_2 \leq p^3 \log p$ and $e_i > 0$, replace S_2 by $S_2 \cdot \ell_i^{e_i}$ where

$$e_i = \left\lceil \frac{\lfloor \log_{\ell_i} s \rfloor}{2} \right\rceil .$$

   Increment i.

Enumerating powersmooth numbers S_1 and S_2

- When lower bound is not satisfied: multiply by small primes.
- Otherwise, raise the powersmoothness bound.

Constructing a random input ideal

- Construct a random upper-triangular integer matrix $\mathbf{U}$ of nonzero square determinant.
- Put generators of $\mathcal{O}_0$ in a vector $\mathbf{b}$
- Compute $\mathbf{x} = \mathbf{U}\mathbf{b}$
- Check whether $\mathbf{x}$ generates an ideal.

Constructing a random input ideal

Proposition

Let $\mathbf{U}$ *be a matrix and* $\mathbf{b}$ *a vector of generators of* $\mathcal{O}_0$*. If* $\mathbf{U}\mathbf{b}$ *generates an ideal, then* $\det(\mathbf{U})$ *is a square.*

Corollary

If $\mathbf{U}\mathbf{b}$ *generates an ideal* I*, then*

$$\operatorname{nrd}(I) = \sqrt{\det(\mathbf{U})}.$$

Constructing a random input ideal

- $O(n^6)$ possible lattices constructed this way.
- There are $n + 1$ possible ideals when n is prime.
- Expected running time is $O(n^5)$.

Constructing an ideal of prime norm

- Let $m = \lceil \log p \rceil$ and let $\{b_1, b_2, b_3, b_4\}$ be the generators of I
- Perform an exhaustive search for a 4-tuple $(x_1, x_2, x_3, x_4) \in [-m, m]^4$ of integers until we find an element δ, where

$$\delta = x_1 b_1 + x_2 b_2 + x_3 b_3 + x_4 b_4$$

- δ should satisfy that $N := \operatorname{nrd}(\delta)/\operatorname{nrd}(I)$ is a prime.
- Construct the ideal $I' = I\bar{\delta}/\operatorname{nrd}(I)$.

Constructing an ideal of powersmooth norm - Alternative 1

- Randomly choose β until β satisfies

$$I'\bar{\beta} = \mathbf{0} \pmod{N\mathcal{O}_0}$$

- There are $\frac{1}{N+3}$ $\mathcal{O}_0/N\mathcal{O}_0$-ideals, hence runs in $O(N)$.
- From Galbraith, Petit, Silva (2017), N is $O(\sqrt{p})$. Asymptotically exponential.

Constructing an ideal of powersmooth norm - Alternative 2

- Need to solve:

$$(\mathcal{O}_0\beta_1)\beta_2 = \mathcal{O}_0\alpha \pmod{N\mathcal{O}_0}$$

  for $\beta_2 = C\mathbf{j} + D\mathbf{k}$.
- KLPT suggests using explicit isomorphism to $M_2(\mathbb{Z}/N\mathbb{Z})$.
- We used more elementary approach.
- Solve

$$\beta_1\beta_2 = u\alpha \pmod{N\mathcal{O}_0}$$

  for (β_2, u) where u is a unit.

Constructing an ideal of powersmooth norm - Alternative 2

- Write $u = u_1 + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$, $\beta_1 = b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}$, and $\alpha = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$.
- We have the following homogeneous system of equations modulo N:

$$\begin{bmatrix} -pb_3 & -pb_4 & -a_1 & a_2 & pa_3 & pa_4 \\ -pb_4 & pb_3 & -a_2 & -a_1 & -pa_4 & pa_3 \\ b_1 & -b_2 & -a_3 & a_4 & -a_1 & -a_2 \\ b_2 & b_1 & -a_4 & -a_3 & a_2 & -a_1 \end{bmatrix} \begin{bmatrix} C \\ D \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Constructing an ideal of powersmooth norm - Alternative 2

- Requirement that β_2 and u are units not reflected in matrix, hence needs some criteria.

Constructing an ideal of powersmooth norm - Alternative 2

Proposition

Let β_1 and α be the generators of the ideals $(\mathcal{O}_0\beta_1)$ and $(\mathcal{O}_0\alpha)$, respectively. Solving the equation of ideals

$$(\mathcal{O}_0\beta_1)\beta_2 = (\mathcal{O}_0\alpha) \pmod{N\mathcal{O}_0}$$

for $\beta_2 = \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{k}$ is equivalent to solving the linear system of equations

$$\beta_1\beta_2 = u\alpha \pmod{N\mathcal{O}_0}.$$

for units β_2 and u. If the solution space of the system is a 4-dimensional $\mathbb{Z}/N\mathbb{Z}$-vector space, there is always a valid solution. If the solution space of the system is 3-dimensional, a family of valid solutions exist if and only if the nonzero solutions for β_2 are generated by a unit.

Computing the isogeny

- Factor $\mathrm{nrd}(J) \to$ since powersmooth, is not expensive; if constructed like proposed a few slides ago, factorization known.
- Compute the basis for the torsion groups: pick random points P_i and Q_i in $E_0[\ell_i^{e_i}]$ with the correct order.
- Check for independence. Enough to check $[\ell^{e-1}]P$ and $[\ell^{e-1}]Q$ using DLP.

Proposition

Let P and Q be points on E_0 of order ℓ^e. If P and Q do not span $E_0[\ell^e]$, then $[\ell^{e-1}]P$ and $[\ell^{e-1}]Q$ are dependent.

Computing the isogeny

- Compute the point R_i such that $\alpha(R_i) = O$ for every generator α of J:
- Write $\alpha(P_i) = [A]P_i + [B]Q_i$ and $\alpha(Q_i) = [C]P_i + [D]Q_i$.
- The integers A, B, C, D are determined by solving a generalized discrete logarithm problem.
- Construct the matrix

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

whose nullspace is the set of points $R_i' \in E_0[\ell_i^{e_i}]$ where $\alpha(R_i') = 0$.

Computing the isogeny

- Once we have the nullspaces for each matrix corresponding to each generator α of J, we intersect the nullspaces and choose a point R_i of order $\ell_i^{e_i}$ in the intersection.
- Such a point R_i will be the generator of a generating set of the kernel of the output isogeny in $E_0[\ell_i^{e_i}]$ with which we perform the composition of isogenies.

Performance

p	S_1	S_2	Largest extension	Running time of ideals step (sec.)	Running time of isogenies step (sec.)
431	4515	8948537162565	$GF(431^{84})$	0.47	443.11
431	4515	8948537162565	$GF(431^{84})$	0.45	407.32
431	4515	8948537162565	$GF(431^{84})$	0.43	460.69
1619	17017	621058354640325	$GF(1619^{84})$	0.48	718.34

Issues

- Choosing S_2 as described earlier gives abysmal success rate despite satisfying the lower bound $p^3 \log p$.
- The n-torsion points involved in the computation of the isogeny might be in large extensions of the initial field.

Possible solutions

- Simply increase S_2 or increase p.
- Optimizing choices made in the computation involving S_2
- Replacing powersmooth condition with (e.g.) smooth
- Pick powersmooth numbers S_1, S_2 such that resulting extension is small.

Conclusion

- We have given our implementation details for the KLPT algorithm and suggested an improvement.
- There are some issues which impact the implementation.

Future work

- Optimizing sum-of-squares
- Smoothness vs. powersmoothness
- Looking into the suggested improvement.