KLPT TWo: Algebraic pathfinding in dimension two (The capitalization is not a mistake)

W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit, Y.B. Ti

February 25, 2025

Setting the frame

For the whole presentation, we fix

- A prime $p = 3 \mod 4$ of cryptographic size,
- A small prime ℓ . Typically $\ell \in \{2,3\}$
- \blacksquare $E_0: y^2: x^3 + x$, the curve with j-invariant 1728 over \mathbb{F}_{p^2} ,

■ End(
$$E_0$$
) $\simeq \mathcal{O}_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \rangle$,

- $B_{p,\infty} = \mathcal{O}_0 \otimes \mathbb{Q}$, the underlying quaternion algebra,
- \blacksquare $A_0 := E_0 \times E_0$, our base abelian surface,
- λ_0 , the (principal) product polarization of A_0 .

In this presentation, every elliptic curve is supersingular

Introduction : The ℓ-isogeny path problem

The ℓ-isogeny path problem

Let E_1 , E_2 be two elliptic curves over \mathbb{F}_{p^2} . Let ℓ be a small prime.

Compute an isogeny $\varphi: E_1 \to E_2$ with degree ℓ^e .

$$E_1 \stackrel{\varphi}{\longrightarrow} E_2$$

The quaternion ℓ^e -isogeny path problem

Let $\mathcal{O}_1, \mathcal{O}_2$ be two maximal orders in the quaternion algebra $\mathcal{B}_{p,\infty}$.

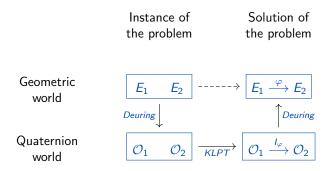
 $\overset{\textbf{Deuring}}{\longleftrightarrow}$

Compute an ideal I of norm ℓ^e such that $\mathcal{O}_L(I) \simeq \mathcal{O}_1$ and $\mathcal{O}_R(I) \simeq \mathcal{O}_2$.

$$\mathcal{O}_1 \stackrel{l}{\longrightarrow} \mathcal{O}_2$$

[Isogeny Club – S1E4]: **Antonin Leroux**, A new algorithm for the constructive Deuring correspondence: making SQISign faster

Overview of KLPT



An analogue in dimension 2

- Replace the elliptic curves by abelian surfaces
- Replace the maximal orders by matrices
- Replace the Deuring correpsondence by the Ibukiyama-Katsura-Oort correspondence.
- Replace KLPT by KLPT²

Organization of the talk

- 1. Principally polarized superspecial abelian surfaces
- 2. The Ibukiyama-Katsura-Oort correspondence
- 3. KLPT²
- 4. Constructive IKO correspondence and applications

Act I – Understanding the objects we manipulate

Act I: Principally Polarized Superspecial Abelian Surfaces?

1.1 – Abelian surfaces

Definition (Abelian varieties)

An abelian variety is an algebraic group that can be embedded in a projective space.

It is an abstract object → scary!

A simple classification of abelian varieties

$$\begin{array}{ll} \text{dim} = 1: & \textit{E} \\ \text{dim} = 2: & \left\{ \begin{array}{ll} \textit{E}_1 \times \textit{E}_2 \\ \text{Jac}(\textit{H}) \end{array} \right., \, \text{or} \\ \text{dim} = 3: & \dots \end{array}$$

with H an hyperelliptic curve of genus 2

An abelian variety of dimension 2 is called an abelian surface.

[Isogeny Club – S1E6] : Sabrina Kunzweiler, Genus 2 Isogenies

1.1 – It's time to d-d-d-dual!

To any abelian variety, we canonically associate a "mirror" variety called its dual.

$$A \xrightarrow{\varphi} B$$

$$A^{\vee} \leftarrow_{\hat{\varphi}} B^{\vee}$$

Definition (Dual variety)

The dual variety of A is the Picard group $Pic^0(A)$. Its elements are divisors.

Remark

The dual isogeny $\varphi: \mathcal{B}^{\vee} \to \mathcal{A}^{\vee}$ is **not** what we call a dual isogenies for elliptic curves !

[Isogeny Days 2022] : Benjamin Smith, Polarizations

1.1 – It's time to d-d-d-dual!

To any abelian variety, we canonically associate a "mirror" variety called its dual.

$$A \xrightarrow{\varphi} B$$

$$A^{\vee} \leftarrow_{\hat{\varphi}} B^{\vee}$$

Definition (Dual variety)

The dual variety of A is the Picard group $Pic^0(A)$. Its elements are divisors.

Remark

The dual isogeny $\varphi: \mathcal{B}^{\vee} \to \mathcal{A}^{\vee}$ is **not** what we call a dual isogenies for elliptic curves !

[Isogeny Days 2022] : Benjamin Smith, Polarizations

1.1 – It's time to d-d-d-dual!

To any abelian variety, we canonically associate a "mirror" variety called its *dual*. Any isogeny $\varphi:A\to B$ induces an isogeny $\hat{\varphi}$ between the duals.

$$A \stackrel{\varphi}{\longrightarrow} B$$

$$A^{\vee} \leftarrow_{\widehat{\varphi}} B^{\vee}$$

Definition (Dual variety)

The dual variety of A is the Picard group $Pic^0(A)$. Its elements are divisors.

Remark

The dual isogeny $\varphi: \mathcal{B}^{\vee} \to \mathcal{A}^{\vee}$ is **not** what we call a dual isogenies for elliptic curves!

[Isogeny Days 2022] : Benjamin Smith, Polarizations

1.2 - Supersingularity vs superspeciality

Let A be an abelian surface (a Jacobian or a product of elliptic curves).

Supersingularity

Superspeciality

A is supersingular if it is *isogenous* to some $E_1 \times E_2$.

A is superspecial if it is isomorphic to some $E_1 \times E_2$.

The supersingular isogeny graph

The superspecial isogeny graph

Contains a single vertex. X

Contains infinitely many vertices. X

Theorem (Deligne)

For all E_1, E_2, E_3, E_4 , we have

$$E_1 \times E_2 \simeq E_3 \times E_4$$

1.3 – Polarizations

Informal Definition (Polarization)

A polarization on A is an isogeny

$$\lambda_D$$
 : $A \rightarrow A^{\vee}$
 $P \mapsto [t_P^*(D) - (D)]$

where D is an ample divisor and t_P^* is the pullback of the translation-by-P map.

Important properties of polarizations

- Not all isogenies $A \rightarrow A^{\vee}$ are polarizations.
- If a polarization has degree 1, it is called *principal*.
- We write PPol(A) for the set of principal polarizations of A.

[CS] : James S. Milne, Arithmetic Geometry, Chapter 5 – Edited by Cornell & Silverman

1.3 – Isogenies between polarized varieties

Definition (Polarized isogeny)

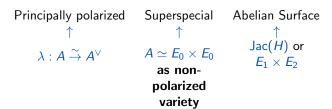
Let (A, λ_A) and (B, λ_B) be two polarized varieties.

An isogeny $\varphi: (A, \lambda_A) \to (B, \lambda_B)$ is an isogeny $\varphi: A \to B$ between the underlying varieties such that the following diagram commutes.

$$\begin{array}{ccc}
A & \xrightarrow{\varphi} & B \\
 & \downarrow^{\lambda_B} \\
A^{\vee} & \longleftarrow_{\widehat{\varpi}} & B^{\vee}
\end{array}$$

i.e. we have $\hat{\varphi}\lambda_B\varphi=N\lambda_A$, for some integer N called the reduced degree.

1 – Wrapping up



The polarized superspecial isogeny graph

The graph of principally polarized superspecial abelian surfaces over \mathbb{F}_p contains $O(p^3)$ vertices. \checkmark

Among which we have :

- $O(p^3)$ Jacobians.
- $O(p^2)$ products of elliptic curves.

A small sanity check

Example 1 : E_0

 $E_0: y^2 = x^3 + x$. It is a supersingular curve.

It is equipped with a canonical principal polarization

$$\lambda : E_0 \rightarrow E_0^{\vee}$$
 $P \mapsto (P) - (\infty)$

It is the only possible polarization on E_0 .

Example 2 : (A_0, λ_0)

 $A_0 = E_0^2$. It is superspecial.

It can be equipped with a natural polarization λ_0 called the *product polarization* inherited from E_0 .

There are a lot of non-equivalent polarizations on A_0 .

Example 3 : (A, λ)

A = Jac(H) for $H/\mathbb{F}_p : y^2 = x^6 + 1$. It is superspecial if $p = 5 \mod 6$.

The equation for H implicitely induces a polarization λ .

Act II – Stating the problem

Act II: The Ibukiyama-Katsura-Oort Correspondence

$$\left\{\begin{array}{c} \text{Abelian surfaces} \\ (A,\lambda_A) \\ \text{up to polarized} \\ \text{isomorphisms} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \text{Polarizations} \\ \lambda \text{ of } A_0 \\ \text{up to equivalence} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \text{Matrices} \\ g \in M_2(\mathcal{O}_0) \\ \text{up to congruence} \end{array}\right\}$$

2.1 – From surfaces to polarizations

Goal

Given an abelian surface (A, λ_A) , encode it as a polarization λ on A_0 .

Polarizations pullbacks

Given (A, λ_A) , A_0 and an **unpolarized** isomorphism $\varphi : A_0 \to A$, one can compute

$$\lambda = \hat{\varphi} \lambda_{\mathsf{A}} \varphi$$

This is a polarization of A_0 .

$$\begin{array}{ccc} A \xleftarrow{\varphi} & A_0 \\ \downarrow^{\lambda_A} & & \downarrow^{\lambda} \\ A^{\vee} & \xrightarrow{\hat{\varphi}} & A_0^{\vee} \end{array}$$

[GSS25]: **Gaudry-Soumier-Spaenlehauer**, *Isogeny-based Cryptography using Isomorphisms of Superspecial Abelian Surfaces*

2.2 – From polarizations to matrices: Deuring for the PPol

Goal

Given a polarization λ on A_0 , encode it as an endomorphism of A_0 . Then, write the endomorphism as a 2x2 matrix with quaternions coefficients.

Step 1:

We simply apply the map

$$\mu$$
 : $\mathsf{PPol}(A_0) \to \mathsf{End}(A_0)$
 $\lambda \mapsto \lambda_0^{-1} \lambda$

$$g\left(\bigcap_{\gamma} A_0 \xrightarrow[\lambda_0]{\lambda} A_0^{\vee} \right)$$

Step 2:

By the Deuring correspondence, $\operatorname{End}(A_0) = \operatorname{M}_2(\operatorname{End}(E_0))$ is isomorphic to $\operatorname{M}_2(\mathcal{O}_0)$.

2.2 - From polarizations to matrices: Deuring for the PPol

The image of μ (after translating into quaternions) is the set

$$\mathsf{Mat}(A_0) := \left\{ \begin{pmatrix} s & r \\ \overline{r} & t \end{pmatrix}, \quad s,t \in \mathbb{Z}_{>0}, r \in \mathcal{O}_0, st - r\overline{r} = 1 \right\} \quad \subset \mathsf{GL}_2(\mathcal{O}_0)$$

Elements of this set will be the input of KLPT².

The IKO correspondence

	Geometric world	Quaternion world
Vertices of the graph	(A,λ_A)	$g\in Mat(A_0)$
Edges of the graph	$\begin{array}{c} Isogenies \\ \varphi: (A_1, \lambda_1) \to (A_2, \lambda_2) \end{array}$	Connecting matrices $u \in M_2(\mathcal{O}_0)$
Adjoint map	Adjoint isogeny $ ilde{arphi}=\lambda_1^{-1}\hat{arphi}\lambda_2$	Conjugate-transpose $u = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$
Structure-preserving property	$\hat{arphi}\lambda_2arphi= extsf{N}\lambda_1$	$u^*g_2u=Ng_1$
Reduced norm	N	$\mathcal{N}(u)$

The quaternion isogeny path problem in dimension 2

Recall: The 2D isogeny path problem

Compute an isogeny $\varphi: (A_1, \lambda_1) \to (A_2, \lambda_2)$ with reduced norm $N = \ell^e$.

$$A_{1} \xrightarrow{\varphi} A_{2}$$

$$N\lambda_{1} \downarrow \qquad \qquad \downarrow \lambda_{2}$$

$$A_{1}^{\vee} \longleftarrow A_{2}^{\vee}$$

Theorem

The 2D isogeny path problem reduces to computing $\psi \in \operatorname{End}(A_0)$ such that the following diagram commutes

i.e. such that $\hat{\psi}\lambda_2'\psi = N\lambda_1'$ ($\longleftrightarrow \gamma^*g_2\gamma = Ng_1$). We can then output $\varphi = \varphi_2 \circ \psi \circ \varphi_1^{-1}$.

Act III - Solving the problem

Act III: The KLPT² algorithm

Main theorem

Let $g_1, g_2 \in \mathsf{Mat}^0(\mathcal{O}_0)$. There is a PPT algorithm that computes $\gamma \in \mathsf{M}_2(\mathcal{O}_0)$ such that

$$\gamma^* g_2 \gamma = N g_1$$

with $N \in O(p^{25})$ is smooth.

3.1 – Some useful lemmas

Definition (Connecting matrix)

Let h_1, h_2, u be matrices in $M_2(\mathcal{O}_0)$.

We say that $u \in M_2(\mathcal{O}_0)$ is a connecting matrix between h_1 and h_2 if it satisfies

$$u^*h_2u=\mathcal{N}(u)h_1$$

we write $u: h_1 \rightarrow h_2$.

Lemma (Inversion lemma)

If $u: h_1 \to h_2$ is invertible in $M_2(B_{p,\infty})$, then $\mathcal{N}(u)u^{-1} \in M_2(\mathcal{O}_0)$ and $\mathcal{N}(u)u^{-1} : h_2 \to h_1$.

$$h_1 \underbrace{\overset{u}{\smile}}_{\mathcal{N}(u)u^{-1}} h_2$$

3.1 – Some useful lemmas

Lemma (Composition lemma)

Let h_1, h_2, h_3, u_1, u_2 be matrices such that

$$\left\{
\begin{array}{l}
u_1:h_1\to h_2\\ u_2:h_2\to h_3
\end{array}\right.$$

Then, $u_1u_2: h_1 \to h_3$.

Proof.

This lemma comes from the fact that $u_i: h_i \to h_{i+1}$ corresponds to the identity

$$u_i^* h_{i+1} u_i = \mathcal{N}(u_i) h_i$$

and from the multiplicativity of the reduced norm $\mathcal{N}(-)$.

$$h_1 \xrightarrow{u_1} h_2 \xrightarrow{u_2} h_3$$

Outline of the strategy

Let $g_1, g_2 \in Mat(A_0)$. A solution is easily computed in the following case :

Lemma

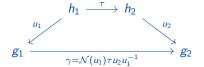
If $g_1=\left(\begin{smallmatrix} D & r_1 \\ \overline{r}_1 & t_1 \end{smallmatrix}\right)$ and $g_2=\left(\begin{smallmatrix} D & r_2 \\ \overline{r}_2 & t_2 \end{smallmatrix}\right)$, for some $D,t_1,t_2\in\mathbb{Z}$ and $r_1,r_2\in\mathcal{O}_0$, with $\det(g_1)=\det(g_2)$, then $\tau:=\left(\begin{smallmatrix} D & r_1-r_2 \\ 0 & D \end{smallmatrix}\right)$ satisfies

$$\tau^*g_2\tau=D^2g_1$$

if D is a power of ℓ , we're done.

The high-level approach

- 1. Find $u_i:h_i\to g_i$ for some h_i of the form $\begin{pmatrix}\ell^{e_2}&r_i'\\ \overline{r}'&t_i'\end{pmatrix}$, with $\mathcal{N}(u_i)=\ell^{e_1}$.
- 2. Compute $\tau: h_1 \to h_2$ with the above lemma. Its norm is ℓ^{2e_2} .
- 3. Output $\gamma = \mathcal{N}(u_1)u_2\tau u_1^{-1}$. Its norm is $\ell^{2(e_1+e_2)}$.



3.2 – Computing the $u: h \rightarrow g$

Strategy for computing u

Given $g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \in \mathsf{Mat}(A_0)$, compute $u \in \mathsf{M}_2(\mathcal{O}_0)$ such that

- 1. $h = u^*gu$ is of the form $\begin{pmatrix} \ell^{e_2} & r' \\ \bar{r}' & t' \end{pmatrix}$
- 2. $\mathcal{N}(u) = \ell^{e_1}$
- 3. e_1 and e_2 don't depend on g.

For $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, an explicit computation yields

$$u^*gu = \begin{pmatrix} s \cdot \mathbf{n}(a) + t \cdot \mathbf{n}(c) + \mathbf{tr}(\bar{c}\bar{r}a) & r' \\ \bar{r}' & s \cdot \mathbf{n}(b) + t \cdot \mathbf{n}(d) + \mathbf{tr}(\bar{b}\bar{r}d) \end{pmatrix}$$

where $\mathbf{n}(-)$ is the usual norm in the quaternion algebra.

The top-left entry only depends on a and c!

- \downarrow Fix *a* and *c* to satisfy 1.
- \downarrow Fix **b** and **d** to satisfy 2.

3.2 – Computing the $u: h \rightarrow g$

Strategy for computing u

Let
$$u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
 and $h := u^* g u = \begin{pmatrix} s' & r' \\ \overline{r}' & t' \end{pmatrix}$.

- 1. Find $a, c \in \mathcal{O}_0$ such that s' equals some ℓ^{e_2} . \downarrow Solve a diophantine equation.
- 2. Given a, c, find values $b, d \in \mathcal{O}_0$ such that $\mathcal{N}(u) = \ell^{e_1}$. \downarrow Solve a pathfinding problem in 1D \longrightarrow KLPT!

We actually start with step 2.

Finding b and d: We put KLPTs in your KLPT²

Here, we assume we have $u=\left(\begin{smallmatrix} a&b\\c&d\end{smallmatrix}\right)$ with a and c fixed and coprime. We want to find a pair $(b,d)\in\mathcal{O}_0^2$ such that

$$\mathcal{N}(u) = \mathbf{n}(a)\mathbf{n}(d) + \mathbf{n}(c)\mathbf{n}(c) - \mathbf{tr}(\bar{a}b\bar{d}c)$$

Reducing the problem to a pathfinding problem in 1D

- 1. View \mathcal{O}_0^2 as a free right \mathcal{O}_0 -module of rank 2.
- 2. Compute Bézout's coefficients ua + cv = 1.
- 3. Let $M_1 = (a, c)\mathcal{O}_0$ and $M_2 = (u \cdot \mathbf{n}(c)a, -v \cdot \mathbf{n}(a)c)B_{p,\infty} \cap \mathcal{O}_0^2$ be two submodules.
- 4. Note that $\mathcal{O}_0^2 = M_1 \oplus M_2$.

Theorem

The submodule M_2 is isomorphic to the right \mathcal{O}_0 -ideal $I = \mathbf{n}(c)\mathcal{O}_0 + a\bar{c}\mathcal{O}_0$

Finding b and d: We put KLPTs in your KLPT

The isomorphism $f: M_2 \to I$ is a $\mathbf{n}(c)$ -homothety.

Finding b and d from KLPT1

- 5. Using KLPT, we can find some $\omega \in I$ with norm $\mathbf{n}(c)\ell^{e_0} \in O(p^3)$
- 6. We translate ω into an element $(b,d)=f^{-1}(\omega)$ of M_2 with norm $\mathbf{n}(\omega)/\mathbf{n}(c)=\ell^{e_0}$.

The resulting matrix u has norm $\ell^{e_1} \in O(p^6)$ and can be written as

$$u = \begin{pmatrix} a & v \cdot \mathbf{n}(c)x + va\bar{c}y \\ c & -uc\bar{a}x - u \cdot \mathbf{n}(a)y \end{pmatrix}$$

where the quaternion ω equals $\mathbf{n}(c)x + a\bar{c}y$ and $e_1 = 2e_0$.

Remark

$$u$$
 can be rewritten as $\begin{pmatrix} a & x \\ c & -y \end{pmatrix} \begin{pmatrix} 1 & -u\bar{a}x + v\bar{c}y \\ 0 & 1 \end{pmatrix}$.

Since the second matrix has determinant 1, we can work with the left one only.

Finding a and c: Finalising the algorithm

We want to find $a, c \in \mathcal{O}_0$ such that

$$s' := s \cdot \mathbf{n}(a) + t \cdot \mathbf{n}(c) + \mathbf{tr}(\bar{c}\bar{r}a) = \ell^{e_2}$$

Similar to KLPT1

The strategy

- 1. Use the fact that \mathcal{O}_0 contains the suborder $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$
- 2. Restrict a and c to subspaces of \mathcal{O}_0 so the trace vanishes.
- 3. Fix c and use Cornacchia to compute a suitable value for a.

With some pre-processing on g, we can bound its entries and guarantee that $s' = \ell^{e_2} \in O(p^{6.5})$ and $\mathbf{n}(a)$ and $\mathbf{n}(c)$ are coprime.

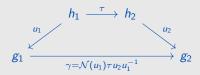
3 – Wrapping up

We showed how to compute $u_i : h_i \rightarrow g_i$ such that

- $\mathbf{u}_i \in \mathcal{O}_0$
- $\mathcal{N}(u_i) = \ell^{e_1} \in O(p^6)$
- $\bullet h_i = \begin{pmatrix} \ell^{e_2} \ r'_i \\ \overline{r}'_i \ t'_i \end{pmatrix} \text{ with } \ell^{e_2} \in O(p^{6.5}).$

The output matrix

The output $\gamma \in M_2(\mathcal{O}_0)$ of the algorithm comes from the composition



Its norm is $\mathcal{N}(\gamma) = \ell^{e_1} \cdot \ell^{e_1} \cdot \ell^{2e_2} \in O(p^{25})$.

Act IV - Constructive IKO Correspondence & Applications

Act IV - Constructive IKO Correspondence & Applications

Constructive IKO Correspondence

- Variety-to-Matrix :
 - □ Products of elliptic curves : [GSS25]
 ✓,
 - 4 Jacobians : Possibly (private communications)
- Isogeny-to-Matrix:
 - ↓ For (2,2)-isogenies: This work
 ✓
- Matrix-to-Isogeny :
 - ↓ For powersmooth degrees : [Chu21]
 ✓

Applications

- Cryptanalysis of 2D CGL without trusted setup
- Relaxed constraints for isogeny representations in 2D
- A brand new SQISign2D ???

[Chu21]: **Hao-Wei Chu**, Algorithms for abelian surfaces over finite fields and their applications to cryptographyPhd thesis

KLPT TWo: Algebraic pathfinding in dimension two (The capitalization is not a mistake)

P. Kutas, A. Laval, C. Petit, Y.B Ti, Thomas D., Wouter C.

 \sim Thank you for your attention ! \backsim