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

25th of March, 2025

Setting the frame

For the whole presentation, we fix

- A prime $p = 3 \mod 4$ of cryptographic size,
- A small prime ℓ. Typically $\ell \in \{2, 3\}$
- $E_0 : y^2 : x^3 + x$, the curve with j-invariant 1728 over $\mathbb{F}_{p^2}$,
- $\mathrm{End}(E_0) \simeq \mathcal{O}_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \rangle$,
- $B_{p,\infty} = \mathcal{O}_0 \otimes \mathbb{Q}$, the underlying quaternion algebra,
- $A_0 := E_0 \times E_0$, 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.

$$E_1 \xrightarrow{\varphi} E_2$$

$$\xleftrightarrow{\textbf{Deuring}}$$

The quaternion ℓ^e-isogeny path problem

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

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

$$\mathcal{O}_1 \xrightarrow{I} \mathcal{O}_2$$

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

Overview of KLPT

	Instance of the problem	Solution of the problem
Geometric world	$E_1 \quad E_2$	$E_1 \xrightarrow{\varphi} E_2$
Quaternion world	$\mathcal{O}_1 \quad \mathcal{O}_2$	$\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2$

$$\begin{tikzcd}
\boxed{E_1 \quad E_2} \arrow[r, dashed] \arrow[d, "Deuring"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "KLPT"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "Deuring"']
\end{tikzcd}$$

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 (Section 2.2)
2. The Ibukiyama-Katsura-Oort correspondence (Section 2.3)
3. KLPT[2] (Section 3)
4. Constructive IKO correspondence and applications (Sections 4 & 5)

Act I : Principally Polarized Superspecial 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 $\rightsquigarrow$ scary !

A simple classification of abelian varieties

$$\begin{aligned} \dim = 1 : &\quad E \\ \dim = 2 : &\quad \begin{cases} E_1 \times E_2 & \text{, or} \\ \mathrm{Jac}(H) \end{cases} \\ \dim = 3 : &\quad \dots \end{aligned}$$

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*. Any isogeny $\varphi : A \to B$ induces an isogeny $\hat{\varphi}$ between the duals.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & & \\ A^\vee & \xleftarrow[\hat{\varphi}]{} & B^\vee \end{array}$$

Definition (Dual variety)

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

Remark

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

[Isogeny Days 2022] : **Benjamin Smith**, *Polarizations*

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

Supersingularity

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

The supersingular isogeny graph

Contains infinitely many vertices. ✗

Superspeciality

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

The superspecial isogeny graph

Contains a single vertex. ✗

Theorem (Deligne)

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

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

[CDS19] : **Castryck-Decru-Smith**, *Hash functions from superspecial genus-2 curves using Richelot isogenies*, eprint : 2019/296

Informal Definition (Polarization)

A polarization on A is an isogeny

$$\begin{array}{rcrcl} \lambda_D & : & A & \to & A^\vee \\ & & P & \mapsto & [t_P^*(D) - (D)] \end{array}$$

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 $A \to A^\vee$ are polarizations.
- If a polarization has degree 1, it is called *principal*.
- We write $\mathrm{PPol}(A)$ for the set of principal polarizations of A.

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

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.

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "N\lambda_A"'] & B \arrow[d, "\lambda_B"] \\ A^\vee & B^\vee \arrow[l, "\hat{\varphi}"] \end{tikzcd}$$

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

Principally polarized	Superspecial	Abelian Surface
$\uparrow$	$\uparrow$	$\uparrow$
$\lambda : A \xrightarrow{\sim} A^\vee$	$A \simeq E_0 \times E_0$ **as non-polarized variety**	$\mathrm{Jac}(H)$ or $E_1 \times E_2$

The polarized superspecial isogeny graph

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

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

$$\begin{array}{cccccc} \lambda & : & E_0 & \to & E_0^\vee \\ & & P & \mapsto & (P) - (\infty) \end{array}$$

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)

$A = \mathrm{Jac}(H)$ 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 : The Ibukiyama-Katsura-Oort Correspondence

$$\left\{ \begin{array}{c} \text{Abelian surfaces} \\ (A, \lambda_A) \\ \text{up to polarized} \\ \text{isomorphism} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Polarizations} \\ \lambda \text{ of } A_0 \\ \text{up to equivalence} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Matrices} \\ g \in \mathsf{M}_2(\mathcal{O}_0) \\ \text{up to congruence} \end{array} \right\}$$

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

$$\lambda = \hat{\varphi}\lambda_A\varphi$$

This is a polarization of A_0.

$$\begin{tikzcd}
A \arrow[d, "\lambda_A"'] & A_0 \arrow[l, "\varphi"'] \arrow[d, dashed, "\lambda"] \\
A^\vee \arrow[r, "\hat{\varphi}"'] & A_0^\vee
\end{tikzcd}$$

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

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

$$\begin{array}{cccc} \mu & : & \mathrm{PPol}(A_0) & \to & \mathrm{End}(A_0) \\ & & \lambda & \mapsto & \lambda_0^{-1}\lambda \end{array}$$

$$\begin{tikzcd} A_0 \arrow[loop left, dashed, "g"] \arrow[r, shift left, "\lambda"] & A_0^\vee \arrow[l, shift left, "\lambda_0^{-1}"] \end{tikzcd}$$

Step 2 :

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

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

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

Elements of this set will be the input of KLPT^2.

The IKO correspondence

	Geometric world	Quaternion world
Vertices of the graph	(A, λ_A)	$g \in \mathrm{Mat}(A_0)$
Edges of the graph	Isogenies $\varphi : (A_1, \lambda_1) \to (A_2, \lambda_2)$	Connecting matrices $u \in \mathrm{M}_2(\mathcal{O}_0)$
Adjoint map	Adjoint isogeny $\tilde{\varphi} = \lambda_1^{-1} \hat{\varphi} \lambda_2$	Conjugate-transpose $u = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$
Structure-preserving property	$\hat{\varphi} \lambda_2 \varphi = N \lambda_1$	$u^* g_2 u = N g_1$
Reduced norm	N	$\mathcal{N}(u)$

Recall : The 2D isogeny path problem

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

$$\begin{tikzcd} A_1 \arrow[r, "\varphi"] \arrow[d, "N\lambda_1"'] & A_2 \arrow[d, "\lambda_2"] \\ A_1^\vee & A_2^\vee \arrow[l, "\hat{\varphi}"] \end{tikzcd}$$

Theorem

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

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 $N = \ell^e$.

$$\begin{tikzcd}
A_1 \arrow[r, "\varphi"] \arrow[d, "N\lambda_1"'] & A_2 \arrow[d, "\lambda_2"] \\
A_1^\vee & A_2^\vee \arrow[l, "\hat{\varphi}"]
\end{tikzcd}$$

Theorem

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

$$\begin{tikzcd}
A_1 \arrow[d, "N\lambda_1"'] & A_0 \arrow[l, "\varphi_1"'] \arrow[r, dashed, "\psi"] \arrow[d, shift left, "N\lambda_1'"] & A_0 \arrow[r, "\varphi_2"] \arrow[d, shift right, "\lambda_2'"'] & A_2 \arrow[d, "\lambda_2"] \\
A_1^\vee \arrow[r, "\hat{\varphi}_1"'] & A_0^\vee \arrow[u, shift left, "\lambda_0^{-1}"] & A_0^\vee \arrow[l, dashed, "\hat{\psi}"] \arrow[u, shift right, "\lambda_0^{-1}"'] & A_2^\vee \arrow[l, "\hat{\varphi}_2"]
\end{tikzcd}$$

i.e. such that $\hat{\psi}\lambda_2'\psi = N\lambda_1' \quad (\longleftrightarrow \gamma^* g_2 \gamma = N g_1)$.
We can then output $\varphi = \varphi_2 \circ \psi \circ \varphi_1^{-1}$.

Act III : The KLPT^2 algorithm

Main theorem

Let $g_1, g_2 \in \mathrm{Mat}^0(\mathcal{O}_0)$. There is a PPT algorithm that computes $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ 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 $\mathrm{M}_2(\mathcal{O}_0)$.
We say that u is a connecting matrix between h_1 and h_2 if it satisfies

$$u^* h_2 u = \mathcal{N}(u) h_1$$

we write $u : h_1 \to h_2$.

Lemma (Inversion lemma)

If $u : h_1 \to h_2$ is invertible in $\mathrm{M}_2(B_{p,\infty})$,
then $\mathcal{N}(u)u^{-1} \in \mathrm{M}_2(\mathcal{O}_0)$ and $\mathcal{N}(u)u^{-1} : h_2 \to h_1$.

$$\begin{tikzcd} h_1 \arrow[r, bend left, "u"] & h_2 \arrow[l, bend left, "\mathcal{N}(u)u^{-1}"] \end{tikzcd}$$

3.1 – Some useful lemmas

Lemma (Composition lemma)

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

$$\begin{cases} u_1 : h_1 \to h_1 \\ u_2 : h_2 \to h_3 \end{cases}$$

Then, $u_1 u_2 : h_1 \to h_3$.

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

Lemma

If $g_1 = \left(\begin{smallmatrix} D & r_1 \\ \bar{r}_1 & t_1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} D & r_2 \\ \bar{r}_2 & t_2 \end{smallmatrix}\right)$, 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

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

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 $\left(\begin{smallmatrix} \ell^{e_2} & r_i' \\ \bar{r}_i' & t_i' \end{smallmatrix}\right)$, with $\mathcal{N}(u_i) = \ell^{e_1}$.
2. Compute $\tau : h_1 \to h_2$. Its norm is ℓ^{2e_2}.
3. Output $\gamma = \mathcal{N}(u_1) u_2 \tau u_1^{-1}$. Its norm is $\ell^{2(e_1+e_2)}$.

$$\begin{tikzcd}
& h_1 \arrow[r, "\tau"] \arrow[dl, "u_1"'] & h_2 \arrow[dr, "u_2"] & \\
g_1 \arrow[rrr, "\gamma=\mathcal{N}(u_1)\tau u_2 u_1^{-1}"'] & & & g_2
\end{tikzcd}$$

Strategy for computing u

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

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

For $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, an explicit computation yields

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

The top-left entry only depends on a and c !
↳ Fix a and c to satisfy 1.
↳ Fix b and d to satisfy 2.

Strategy for computing u

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

1. Find $a, c \in \mathcal{O}_0$ such that s' equals some ℓ^{e_2}.
   ↳ Solve a diophantine equation.

Strategy for computing u

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

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

We actually start with step 2.

Finding b and d : We put KLPTs in your KLPT^2

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

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

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 $f : \mathrm{M}_2 \to I$ 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 wor with the left one only.

Strategy for computing u

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

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

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 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 garantee that $s' = \ell^{e_2} \in O(p^{6.5})$ and $\mathbf{n}(a)$ and $\mathbf{n}(c)$ are coprime.

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

- $u_i \in \mathcal{O}_0$
- $\mathcal{N}(u_i) = \ell^{e_1} \in O(p^6)$
- $h_i = \begin{pmatrix} \ell^{e_2} & r_i' \\ \bar{r}_i' & t_i' \end{pmatrix}$ with $\ell^{e_2} \in O(p^{6.5})$.

The output matrix

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

$$\begin{tikzcd} & h_1 \arrow[r, "\tau"] \arrow[dl, "u_1"'] & h_2 \arrow[dr, "u_2"] & \\ g_1 \arrow[rrr, "\gamma = \mathcal{N}(u_1)\tau u_2 u_1^{-1}"'] & & & g_2 \end{tikzcd}$$

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

Constructive IKO Correspondence

- Variety-to-Matrix :
  ↳ Products of elliptic curves : [GSS25] ✓,
  ↳ Jacobians : "Aurel knows something."
- 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 cryptography* Phd thesis

Thank you for you attention !

P. **K**utas, A. **L**aval, C. **P**etit, Y.B **T**i, **T**homas D., **Wo**uter C.
KLPT TWo