KLPT2 & isogeny-based cryptography without isogenies

based on a paper by
Wouter Castryck, Thomas Decru, Péter Kutas, **Abel Laval**, Christophe Petit, Yan Bo Ti

April 4, 2025

Definition (Elliptic curve)

An elliptic curve E over a field $\mathbb{F}_q$ is the set of solution of a cubic equation, with a special *point at infinity*.

$$E = \left\{ y^2 = x^3 + ax + b, \quad x, y \in \overline{\mathbb{F}}_q \right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.

Definition (Elliptic curve)

An elliptic curve E over a field $\mathbb{F}_q$ is the set of solution of a cubic equation, with a special *point at infinity*.

$$E = \left\{y^2 = x^3 + ax + b, \quad x, y \in \overline{\mathbb{F}}_q\right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.
E is the elliptic curve; $E(\mathbb{F}_q)$ is the set of rational points over K.
$E(\mathbb{F}_q)$ is an abelian group. Its neutral element is ∞.

Definition (Elliptic curve)

An elliptic curve E over a field $\mathbb{F}_q$ is the set of solution of a cubic equation, with a special *point at infinity*.

$$E = \left\{ y^2 = x^3 + ax + b, \quad x, y \in \overline{\mathbb{F}}_q \right\} \cup \{\infty\}$$

with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.
E is the elliptic curve; $E(\mathbb{F}_q)$ is the set of rational points over K.
$E(\mathbb{F}_q)$ is an abelian group. Its neutral element is ∞.

Example

Let's take $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$. It has 6 rational points :

$$E(\mathbb{F}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0), \infty\}$$

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : & y^2 = x^3 + 1 \\ E_2 & : & y^2 = x^3 + 2 \end{cases}$$

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, \frac{x^2 + 2x - 2}{x^2 + 2x + 1} y \right)$$

Definition (Isogeny)

Let E_1, E_2 be two elliptic curves over $\mathbb{F}_q$.
An isogeny $\varphi : E_1 \to E_2$ is a group homomorphism with finite kernel.
It can be represented with rational maps.
The *degree* of a (separable) isogeny is the size of it kernel.

Example

Over $\mathbb{F}_5$, we take :

$$\begin{cases} E_1 & : \quad y^2 = x^3 + 1 \\ E_2 & : \quad y^2 = x^3 + 2 \end{cases}$$

We can consider the isogeny $\varphi : E_1 \to E_2$ given by the map

$$\varphi : (x, y) \mapsto \left(\frac{x^2 + x - 2}{x + 1}, \frac{x^2 + 2x - 2}{x^2 + 2x + 1} y \right)$$

The kernel of φ is $\{(4, 0), \infty\} \leadsto \deg(\varphi) = 2$.

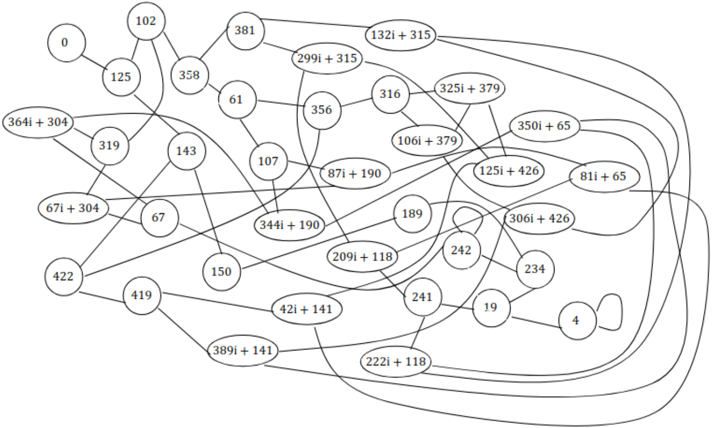

Figure: The ℓ-isogeny graph over $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[i]$, for $p = 431$ and $\ell = 2$.

[Cos] : **Costello**, *SIKE for beginners*

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (Order of an algebra)

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define “rings of integers” for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Quaternion algebras and orders

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Example

$\mathcal{O} = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ is an order.

Definition (The quaternion algebra ramified at p and ∞)

We will make use of the quaternion algebra $B_{p,\infty}$ defined as :

$$B_{p,\infty} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = -1$, $j^2 = -p$, $k := ij = -ji$.

We can define "rings of integers" for this algebra :

Definition (Order of an algebra)

An order $\mathcal{O}$ of $B_{p,\infty}$ is a full-rank lattice in B that is also a ring.
An order is called *maximal* if not contained in any other order.

Example

$\mathcal{O} = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ is an order.
$\mathcal{O}_0 = \mathbb{Z} + i\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + \frac{1+k}{2}\mathbb{Z}$ is a maximal order.

The Deuring Correspondence in one slide

Theorem (Deuring)

Supersingular elliptic curves can be

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{(supersingular) elliptic curves} \\ \text{over } \mathbb{F}_{p^2} \text{ and their isogenies} \end{array} \right\} \xleftrightarrow{\text{2-to-1}} \left\{ \begin{array}{c} \text{Maximal orders of } B_{p,\infty} \\ \text{and their connecting ideals} \end{array} \right\}$$

Theorem (Deuring)

Supersingular elliptic curves can be

$$\left\{\begin{array}{c}\text{Isomorphism classes of}\\ \text{(supersingular) elliptic curves}\\ \text{over } \mathbb{F}_{p^2} \text{ and their isogenies}\end{array}\right\} \overset{\text{2-to-1}}{\longleftrightarrow} \left\{\begin{array}{c}\text{Maximal orders of } B_{p,\infty}\\ \text{and their connecting ideals}\end{array}\right\}$$

The canonical example

Take $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$, with $p = 3 \mod 4$.
Then, we have

$$\begin{array}{ccc}\mathrm{End}(E_0) & = & \mathbb{Z} + \iota\mathbb{Z} + \frac{\iota+\pi}{2}\mathbb{Z} + \frac{1+\pi\iota}{2}\mathbb{Z}\\ \wr\| & & \\ \mathcal{O}_0 & = & \mathbb{Z} + i\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + \frac{1+k}{2}\mathbb{Z}\end{array}$$

Translating 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.

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

The quaternion ℓ-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 connect $\mathcal{O}_1$ to $\mathcal{O}_2$.

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

Translating 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.

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

$$\overset{\text{Deuring}}{\longleftrightarrow}$$

The quaternion ℓ-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 connect $\mathcal{O}_1$ to $\mathcal{O}_2$.

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

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

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{E_1 \qquad E_2}$	$\boxed{E_1 \xrightarrow{\varphi} E_2}$

Kohel-Lauter-Petit-Tignol (2014)

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{E_1 \qquad E_2}$	$\boxed{E_1 \xrightarrow{\varphi} E_2}$
Quaternion world		

Kohel-Lauter-Petit-Tignol (2014)

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{E_1 \qquad E_2}$	$\boxed{E_1 \xrightarrow{\varphi} E_2}$
	$\big\downarrow$ *Deuring*	
Quaternion world	$\boxed{\mathcal{O}_1 \qquad \mathcal{O}_2}$	

Kohel-Lauter-Petit-Tignol (2014)

$$\begin{tikzcd} & \text{Instance of the problem} & \text{Solution of the problem} \\ \text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[d, "\mathit{Deuring}"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\ \text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "\mathit{KLPT}"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \end{tikzcd}$$

Kohel-Lauter-Petit-Tignol (2014)

$$
\begin{tikzcd}
 & \text{Instance of the problem} & & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[d, "\mathit{Deuring}"'] & & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[rr, "\mathit{KLPT}"'] & & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "\mathit{Deuring}"']
\end{tikzcd}
$$

Kohel-Lauter-Petit-Tignol (2014)

$$\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[r, dashed] \arrow[d, "Deuring"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "KLPT"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "Deuring"']
\end{tikzcd}$$

Kohel-Lauter-Petit-Tignol (2014)

$$
\begin{tikzcd}
 & \text{Instance of the problem} & & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[d, "Deuring"'] \arrow[rr, dashed] & & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[rr, "KLPT"'] & & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "Deuring"']
\end{tikzcd}
$$

What about an analogue in dimension 2 ??

Kohel-Lauter-Petit-Tignol (2014)

	Instance of the problem		Solution of the problem
Geometric world	$\boxed{E_1 \quad E_2}$	$\dashrightarrow$	$\boxed{E_1 \xrightarrow{\varphi} E_2}$
	$\downarrow$ *Deuring*		$\uparrow$ *Deuring*
Quaternion world	$\boxed{\mathcal{O}_1 \quad \mathcal{O}_2}$	$\xrightarrow[KLPT]{}$	$\boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2}$

What about an analogue in dimension 2 ??

- Replace the elliptic curves by *polarized abelian surfaces*.

Kohel-Lauter-Petit-Tignol (2014)

$$
\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[r, dashed] \arrow[d, "\mathit{Deuring}"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "\mathit{KLPT}"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "\mathit{Deuring}"']
\end{tikzcd}
$$

What about an analogue in dimension 2 ??

- Replace the elliptic curves by *polarized abelian surfaces*.
- Replace the maximal orders by matrices in $\mathrm{M}_2(\mathcal{O}_0)$.

Kohel-Lauter-Petit-Tignol (2014)

$$\begin{tikzcd}
 & \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[r, dashed] \arrow[d, "Deuring"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "KLPT"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "Deuring"']
\end{tikzcd}$$

What about an analogue in dimension 2 ??

- Replace the elliptic curves by *polarized abelian surfaces*.
- Replace the maximal orders by matrices in $\mathrm{M}_2(\mathcal{O}_0)$.
- Replace the Deuring correpsondence by the Ibukiyama-Katsura-Oort correspondence.

Kohel-Lauter-Petit-Tignol (2014)

	Instance of the problem		Solution of the problem

$$\begin{tikzcd}[column sep=large]
\text{Geometric world} & \boxed{E_1 \quad E_2} \arrow[r, dashed] \arrow[d, "Deuring"'] & \boxed{E_1 \xrightarrow{\varphi} E_2} \\
\text{Quaternion world} & \boxed{\mathcal{O}_1 \quad \mathcal{O}_2} \arrow[r, "KLPT"'] & \boxed{\mathcal{O}_1 \xrightarrow{I_\varphi} \mathcal{O}_2} \arrow[u, "Deuring"']
\end{tikzcd}$$

What about an analogue in dimension 2 ??

- Replace the elliptic curves by *polarized abelian surfaces*.
- Replace the maximal orders by matrices in $\mathrm{M}_2(\mathcal{O}_0)$.
- Replace the Deuring correpsondence by the Ibukiyama-Katsura-Oort correspondence.
- **Replace KLPT by KLPT2 !**

Overview of KLPT^2

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{(A_1, \lambda_1) \quad (A_2, \lambda_2)}$	$\boxed{(A_1, \lambda_1) \xrightarrow{\varphi} (A_2, \lambda_2)}$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

Overview of KLPT^2

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)}$	$\boxed{(A_1, \lambda_1) \xrightarrow{\varphi} (A_2, \lambda_2)}$
Quaternion world		

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{(A_1, \lambda_1) \qquad (A_2, \lambda_2)}$	$\boxed{(A_1, \lambda_1) \xrightarrow{\varphi} (A_2, \lambda_2)}$
	*IKO*86 $\downarrow$	
Quaternion world	$\boxed{g_1 \qquad g_2}$	

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

- g_1, g_2 are matrices encoding the abelian surfaces.

[IKO86] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

Instance of the problem

Solution of the problem

Geometric world

Quaternion world

$$\begin{tikzcd} \boxed{(A_1,\lambda_1) \qquad (A_2,\lambda_2)} \arrow[d, "IKO86"'] & \boxed{(A_1,\lambda_1) \xrightarrow{\varphi} (A_2,\lambda_2)} \\ \boxed{g_1 \qquad g_2} \arrow[r, "\mathrm{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2} \end{tikzcd}$$

- (A_1,λ_1) and (A_2,λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO86] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

	Instance of the problem	Solution of the problem
Geometric world	$\boxed{(A_1, \lambda_1) \quad (A_2, \lambda_2)}$	$\boxed{(A_1, \lambda_1) \xrightarrow{\varphi} (A_2, \lambda_2)}$
Quaternion world	$\boxed{g_1 \quad g_2}$	$\boxed{g_1 \xrightarrow{\gamma} g_2}$

$$\begin{tikzcd}
\boxed{(A_1, \lambda_1) \quad (A_2, \lambda_2)} \arrow[d, "IKO86"'] & \boxed{(A_1, \lambda_1) \xrightarrow{\varphi} (A_2, \lambda_2)} \\
\boxed{g_1 \quad g_2} \arrow[r, "\mathrm{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2} \arrow[u, "IKO86"']
\end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO86] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

$$\begin{tikzcd}
& \text{Instance of the problem} & \text{Solution of the problem} \\
\text{Geometric world} & \boxed{(A_1,\lambda_1) \qquad (A_2,\lambda_2)} \arrow[r, dashed] \arrow[d, "IKO86"'] & \boxed{(A_1,\lambda_1) \xrightarrow{\varphi} (A_2,\lambda_2)} \\
\text{Quaternion world} & \boxed{g_1 \qquad g_2} \arrow[r, "\mathrm{KLPT}^2"'] & \boxed{g_1 \xrightarrow{\gamma} g_2} \arrow[u, "IKO86"']
\end{tikzcd}$$

- (A_1, λ_1) and (A_2, λ_2) are *principally polarized superspecial abelian surfaces*.

$\rightsquigarrow$ analogue of supersingular elliptic curves in dimension 2.

- g_1, g_2 are matrices encoding the abelian surfaces.
- γ is a matrix encoding an isogeny.

[IKO86] : **Ibukiyama-Katsura-Oort**, *Supersingular curves of genus two and class numbers*

For everything that follows, 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 $\mathbb{F}_{p^2}$,
- $\mathrm{End}(E_0) \simeq \mathcal{O}_0 = \mathbb{Z} + i\mathbb{Z} + \frac{i+j}{2}\mathbb{Z} + \frac{1+k}{2}\mathbb{Z}$,
- $B_{p,\infty} = \mathcal{O}_0 \otimes \mathbb{Q}$, the underlying quaternion algebra,
- $\mathbf{n}(x) = x\bar{x}$ is the norm; $\mathbf{tr}(x) = x + \bar{x}$ is the trace.

KLPT in dimension 2

Quaternion path problem in dimension 2

Given $g_1, g_2 \in \mathsf{Mat}(\mathcal{O}_0)$, find $\gamma \in \mathsf{M}_2(\mathcal{O}_0)$ such that :

$$\gamma^* g_2 \gamma = \ell^n g_1$$

for some small prime ℓ and with :

- $\mathsf{Mat}(\mathcal{O}_0) = \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_>, st - \mathbf{n}(r) = 1 \right\}$.
- $-^* : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$ is the conjugate-transpose.

KLPT in dimension 2

Quaternion path problem in dimension 2

Given $g_1, g_2 \in \mathrm{Mat}(\mathcal{O}_0)$, find $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that :

$$\gamma^* g_2 \gamma = \ell^n g_1$$

for some small prime ℓ and with :

- $\mathrm{Mat}(\mathcal{O}_0) = \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_>, st - \mathbf{n}(r) = 1 \right\}$.
- $-^* : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$ is the conjugate-transpose.

Theorem (KLPT2)

This problem can be solved in polynomial time with output norm $\ell^n = O(p^{25})$.

Definition (Connecting matrix)

Let $h_1, h_2 \in \mathrm{Mat}(A_0)$ and $u \in \mathrm{M}_2(\mathcal{O}_0)$.
We say that u is a connecting matrix between h_1 and h_2 if it satisfies

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

for some integer $\mathcal{N}(u)$ called its norm.
We write $u : h_1 \to h_2$.

Some useful lemmas

Definition (Connecting matrix)

Let $h_1, h_2 \in \mathrm{Mat}(A_0)$ and $u \in \mathrm{M}_2(\mathcal{O}_0)$.
We say that u is a connecting matrix between h_1 and h_2 if it satisfies

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

for some integer $\mathcal{N}(u)$ called its norm.
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 $\mathcal{N}(u)u^{-1} : h_2 \to h_1$.

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

Lemma (Composition lemma)

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

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

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

$$\begin{tikzcd} h_1 \arrow[r, "u_1"] \arrow[rr, bend right, "u_1 u_2"'] & h_2 \arrow[r, "u_2"] & h_3 \end{tikzcd}$$

How we solve KLPT2

The inputs of the algorithm

Two matrices $g_1 = \begin{pmatrix} s_1 & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} s_2 & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$.

The strategy

g_1 g_2

How we solve KLPT2

The inputs of the algorithm

Two matrices $g_1 = \begin{pmatrix} s_1 & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} s_2 & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$.

The strategy

- We note that if the inputs have a certain shape, there exists a connecting matrix τ between them.

$$g_1 \qquad \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix} \xrightarrow{\tau} \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix} \qquad g_2$$

How we solve KLPT2

The inputs of the algorithm

Two matrices $g_1 = \begin{pmatrix} s_1 & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} s_2 & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$.

The strategy

- We note that if the inputs have a certain shape, there exists a connecting matrix τ between them.
- We transform our inputs so they have the aforementioned shape.

$$g_1 \xrightarrow{u_1} \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix} \xrightarrow{\tau} \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix} \xleftarrow{u_2} g_2$$

How we solve KLPT2

The inputs of the algorithm

Two matrices $g_1 = \begin{pmatrix} s_1 & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} s_2 & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$.

The strategy

- We note that if the inputs have a certain shape, there exists a connecting matrix τ between them.
- We transform our inputs so they have the aforementioned shape.
- We output the product of the three connecting matrices.

$$g_1 \xrightarrow{u_1} \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix} \xrightarrow{\tau} \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix} \xleftarrow{u_2} g_2$$

The output of the algorithm

The composition $\gamma := u_1 \cdot \tau \cdot \mathcal{N}(u_2) u_2^{-1}$.

The norm of γ is $\mathcal{N}(u_1)\mathcal{N}(u_2)\mathcal{N}(\tau)$.

Connecting matrices between special inputs

Lemma (Step 1 : Connecting special matrices)

Let $h_1 = \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix}$ and $h_2 = \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix}$ be two "input" matrices such that $\det(h_1) = \det(h_2)$.

Connecting matrices between special inputs

Lemma (Step 1 : Connecting special matrices)

Let $h_1 = \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix}$ and $h_2 = \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix}$ be two "input" matrices such that $\det(h_1) = \det(h_2)$.

Then, there exists $\tau \in \mathrm{M}_2(\mathcal{O}_0)$ connecting h_1 to h_2.

Connecting matrices between special inputs

Lemma (Step 1 : Connecting special matrices)

Let $h_1 = \begin{pmatrix} \ell^f & r_1' \\ \bar{r}_1' & t_1' \end{pmatrix}$ and $h_2 = \begin{pmatrix} \ell^f & r_2' \\ \bar{r}_2' & t_2' \end{pmatrix}$ be two "input" matrices such that $\det(h_1) = \det(h_2)$.
Then, there exists $\tau \in \mathrm{M}_2(\mathcal{O}_0)$ connecting h_1 to h_2.

Proof.

Take $\tau = \begin{pmatrix} \ell^f & r_1 - r_2 \\ 0 & \ell^f \end{pmatrix}$. □

Lemma (Step 2 : Transforming the input matrices)

For any $g \in \mathrm{Mat}(\mathcal{O}_0)$, one can compute $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties :

Lemma (Step 2 : Transforming the input matrices)

For any $g \in \mathrm{Mat}(\mathcal{O}_0)$, one can compute $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties :

1. u is a connecting matrix from g to some matrix $h = \begin{pmatrix} \ell^f & r' \\ \bar{r}' & t' \end{pmatrix}$.

Lemma (Step 2 : Transforming the input matrices)

For any $g \in \mathrm{Mat}(\mathcal{O}_0)$, one can compute $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties :

1. u is a connecting matrix from g to some matrix $h = \begin{pmatrix} \ell^f & r' \\ \bar{r}' & t' \end{pmatrix}$.
2. u has norm ℓ^e.

Modifying the shape of the inputs

Lemma (Step 2 : Transforming the input matrices)

For any $g \in \mathrm{Mat}(\mathcal{O}_0)$, one can compute $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties :

1. u is a connecting matrix from g to some matrix $h = \begin{pmatrix} \ell^f & r' \\ \bar{r}' & t' \end{pmatrix}$.
2. u has norm ℓ^e.
3. The integers e and f does not depends on the input matrix g.

Lemma (Step 2 : Transforming the input matrices)

For any $g \in \mathrm{Mat}(\mathcal{O}_0)$, one can compute $u \in \mathrm{M}_2(\mathcal{O}_0)$ with the following properties :

1. u is a connecting matrix from g to some matrix $h = \begin{pmatrix} \ell^f & r' \\ \bar{r}' & t' \end{pmatrix}$.
2. u has norm ℓ^e.
3. The integers e and f does not depends on the input matrix g.

Proof.

Read the paper :)
Or check my talk at The Isogeny Club – S6E1 □

Why do we do this ?

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Future work :

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Future work :

1. Optimize the algorithm. Lower the bound $\ell^e = O(p^{25})$.

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Future work :

1. Optimize the algorithm. Lower the bound $\ell^e = O(p^{25})$.
2. Complete the work on the constructive IKO correspondence.

[GSS25] : **Gaudry-Soumier-Spaenlehauer**, *Isogeny-based Cryptography using Isomorphisms of Superspecial Abelian Surfaces*, eprint : 2025/136

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Future work :

1. Optimize the algorithm. Lower the bound $\ell^e = O(p^{25})$.
2. Complete the work on the constructive IKO correspondence.
3. Some constructive applications ? Another SQIsign ??

[GSS25] : **Gaudry-Soumier-Spaenlehauer**, *Isogeny-based Cryptography using Isomorphisms of Superspecial Abelian Surfaces*, eprint : 2025/136

Motivations and future work

Why do we do this ?

1. Because it's an obvious question.
2. It's a piece of the constructive IKO correspondence.
3. It's a cryptanalytic tool for niche theoretical hash functions based on isogenies (2D CGL).

Future work :

1. Optimize the algorithm. Lower the bound $\ell^e = O(p^{25})$.
2. Complete the work on the constructive IKO correspondence.
3. Some constructive applications ? Another SQIsign ??

Thank you for your attention !

[GSS25] : **Gaudry-Soumier-Spaenlehauer**, *Isogeny-based Cryptography using Isomorphisms of Superspecial Abelian Surfaces*, eprint : 2025/136