The generalized Quaternion ℓ-isogeny path problem

Antonin Leroux

DGA, Ecole Polytechnique, Institut Polytechnique de Paris, Inria Saclay

Classical Cryptography

Current cryptography :

- The Integer Factorization Problem
- The Discrete Logarithm Problem

Classical Cryptography

Current cryptography :

- The Integer Factorization Problem
- The Discrete Logarithm Problem

Hard for *classical* computers, solved in **polynomial time** on a *quantum* computer using Shor's Algorithm.

Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) $\rightarrow$ usable on classical computer but **resistant** to quantum computers.

In 2016, the NIST launched a competition for PQC. Looked for **Signature** and **Key exchange** protocols. Different Candidates :

- Lattice-based crypto
- Code-based crypto
- Multivariate-based crypto (Signatures only)
- Hash-based crypto (Signatures only)
- Isogeny-based crypto (Key exchange only)

For isogenies : SIKE a variant of the SIDH protocol (2011 by D. Jao and L. De Feo).

Table of contents

Isogeny-based cryptography

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

The set of (x, y) defined over $\mathbb{F}_q$ is a group with addition $\oplus$. The scalar multiplication by $n \in \mathbb{Z}$ is n consecutive addition and is denoted $[n]_E$.

Separable isogeny:

$$\varphi : E \to E'$$

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

The set of (x, y) defined over $\mathbb{F}_q$ is a group with addition $\oplus$. The scalar multiplication by $n \in \mathbb{Z}$ is n consecutive addition and is denoted $[n]_E$.

Separable isogeny:

$$\varphi : E \to E'$$

The **degree** is $\deg(\varphi) = |\ker(\varphi)|$.

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

The set of (x, y) defined over $\mathbb{F}_q$ is a group with addition $\oplus$. The scalar multiplication by $n \in \mathbb{Z}$ is n consecutive addition and is denoted $[n]_E$.

Separable isogeny:

$$\varphi : E \to E'$$

The **degree** is $\deg(\varphi) = |\ker(\varphi)|$.

The **dual** isogeny $\hat{\varphi} : E' \to E$

$$\hat{\varphi} \circ \varphi = [\deg(\varphi)]_E$$

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with addition and composition.

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with addition and composition.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with addition and composition.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

Elliptic curves over finite fields:

- **Ordinary** when $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with addition and composition.

Examples: $[n]_E$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

Elliptic curves over finite fields:

- **Ordinary** when $\mathrm{End}(E)$ is an order of a quadratic imaginary field.
- **Supersingular** when $\mathrm{End}(E)$ is a maximal order of a quaternion algebra.

Supersingular Isogeny Graph

Supersingular ℓ-isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are ℓ-isogenies.

This graph is

- Finite and defined over $\mathbb{F}_{p^2}$

Supersingular Isogeny Graph

Supersingular ℓ-isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are ℓ-isogenies.

This graph is

- Finite and defined over $\mathbb{F}_{p^2}$
- Fully connected

Supersingular Isogeny Graph

Supersingular ℓ-isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are ℓ-isogenies.

This graph is

- Finite and defined over $\mathbb{F}_{p^2}$
- Fully connected
- $(\ell + 1)$-Regular

Supersingular Isogeny Graph

Supersingular ℓ-isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are ℓ-isogenies.

This graph is

- Finite and defined over $\mathbb{F}_{p^2}$
- Fully connected
- $(\ell + 1)$-Regular
- Ramanujan (optimal expander graph)

$$
\begin{tikzcd}
 & E_A \arrow[r, "\varphi_{AB}"] & E_{AB} \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & \simeq \\
 & E_B \arrow[r, "\varphi_{BA}"'] & E_{BA}
\end{tikzcd}
$$

Supersingular Isogeny Problem

The underlying security problem:

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

The Deuring Correspondence

Quaternion Algebra

The **quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

Quaternion Algebra

The **quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

Conjugates:

$$\alpha = a_1 + a_2 i + a_3 j + a_4 k \longmapsto \overline{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$$

Quaternion Algebra

The **quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

Conjugates:

$$\alpha = a_1 + a_2 i + a_3 j + a_4 k \longmapsto \overline{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$$

The **reduced norm**

$$n(\alpha) = \alpha\overline{\alpha}$$

Order and ideals

Fractional ideals are $\mathbb{Z}$-lattices of rank 4

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\mathrm{gcd}(n(\alpha)), \alpha \in I\}$

[1]similary for the **right order** $\mathcal{O}_R(I)$

Order and ideals

Fractional ideals are $\mathbb{Z}$-lattices of rank 4

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\mathrm{gcd}(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an ideal which is also a ring, it is **maximal** when not contained in another order.

[1] similary for the **right order** $\mathcal{O}_R(I)$

Order and ideals

Fractional ideals are $\mathbb{Z}$-lattices of rank 4

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an ideal which is also a ring, it is **maximal** when not contained in another order.

The (maximal) **left order**[1] $\mathcal{O}_L(I)$ of an ideal is

$$\mathcal{O}_L(I) = \{\alpha \in H(a,b), \alpha I \subset I\}$$

An ideal is **integral** when $I \subset \mathcal{O}_L(I)$.

[1] similary for the **right order** $\mathcal{O}_R(I)$

Order and ideals

Fractional ideals are $\mathbb{Z}$-lattices of rank 4

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\text{gcd}(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an ideal which is also a ring, it is **maximal** when not contained in another order.

The (maximal) **left order**[1] $\mathcal{O}_L(I)$ of an ideal is

$$\mathcal{O}_L(I) = \{\alpha \in H(a,b), \alpha I \subset I\}$$

An ideal is **integral** when $I \subset \mathcal{O}_L(I)$.

The **equivalence relation** $\sim$ is $I \sim J$ when $I = Jq$ for $q \in H(a,b)^\star$

[1] similary for the **right order** $\mathcal{O}_R(I)$

The Deuring Correspondence

$$\begin{array}{ccc} \text{Supersingular curves over } \mathbb{F}_{p^2} & \longleftrightarrow & \text{Maximal orders in } \mathcal{A}_p \\ E & \longmapsto & \mathcal{O} \cong \mathrm{End}(E) \end{array}$$

The Deuring Correspondence

$$\begin{array}{ccc} \text{Supersingular curves over } \mathbb{F}_{p^2} & \longleftrightarrow & \text{Maximal orders in } \mathcal{A}_p \\ E & \longmapsto & \mathcal{O} \cong \mathrm{End}(E) \end{array}$$

Example : $p \equiv 3 \mod 4$, $\mathcal{A}_p = H(-1, -p)$.

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

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius and $\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ is the twisting automorphism.

The Deuring Correspondence, Summary

Supersingular elliptic curve over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
(E_1, φ) with $\varphi : E \to E_1$	I_φ integral left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal
$\deg(\varphi)$	$n(I_\varphi)$
$\hat{\varphi}$	$\overline{I_\varphi}$
$\varphi : E \to E_1, \psi : E \to E_1$	Equivalent Ideals $I_\varphi \sim I_\psi$

The problem

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

The problem

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

$$\updownarrow$$

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{A}_p$, find J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

The problem

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

$$\updownarrow$$

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{A}_p$, find J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

Easier Problem ? Can we use it to solve supersingular isogeny problem ?

The problem

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

$$\updownarrow$$

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{A}_p$, find J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

Easier Problem ? Can we use it to solve supersingular isogeny problem ?

KLPT14: *heuristic* **polynomial time** algorithm `KLPT` for quaternion path problem.

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using `KLPT`.

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using `KLPT`.

$E \to \mathcal{O}$	✗	$\mathcal{O} \to E$	✓
$\varphi \to I_\varphi$	✗	$I_\varphi \to \varphi$	✓
$E_1, E_2 \to \varphi$	✗	$\mathcal{O}_1, \mathcal{O}_2 \to I$	✓

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using `KLPT`.

$E \rightarrow \mathcal{O}$	✗	$\mathcal{O} \rightarrow E$	✓
$\varphi \rightarrow I_\varphi$	✗	$I_\varphi \rightarrow \varphi$	✓
$E_1, E_2 \rightarrow \varphi$	✗	$\mathcal{O}_1, \mathcal{O}_2 \rightarrow I$	✓

EHLMP18: use `KLPT` to prove *heuristic* **polynomial time** reduction from supersingular ℓ-isogeny problem to :

Endomorphism ring Problem: Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

The Quaternion ℓ-isogeny Path Problem

A key lemma

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, a maximal order $\mathcal{O}$ of $\mathcal{A}_p$ and I a left integral $\mathcal{O}$-ideal, find $J \sim I$ of norm ℓ^e for $e \in \mathbb{N}^\star$.

A key lemma

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, a maximal order $\mathcal{O}$ of $\mathcal{A}_p$ and I a left integral $\mathcal{O}$-ideal, find $J \sim I$ of norm ℓ^e for $e \in \mathbb{N}^\star$.

Following lemma indicates a method of resolution :

Lemma: Let I be a left integral $\mathcal{O}$-ideal and $\alpha \in I$. Then, $I \frac{\overline{\alpha}}{n(I)}$ is an integral left $\mathcal{O}$-ideal of norm $\frac{n(\alpha)}{n(I)}$.

A key lemma

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, a maximal order $\mathcal{O}$ of $\mathcal{A}_p$ and I a left integral $\mathcal{O}$-ideal, find $J \sim I$ of norm ℓ^e for $e \in \mathbb{N}^\star$.

Following lemma indicates a method of resolution :

Lemma: Let I be a left integral $\mathcal{O}$-ideal and $\alpha \in I$. Then, $I\frac{\overline{\alpha}}{n(I)}$ is an integral left $\mathcal{O}$-ideal of norm $\frac{n(\alpha)}{n(I)}$.

Solving the Quaternion ℓ-Isogeny Path Problem reduces to solving the **norm equation** $n(\alpha) = n(I)\ell^e$ over I.

KLPT14 $\rightarrow$ possible when **norm equations** can be solved over $\mathcal{O}$.

Norm equation over Special Extremal Orders

We have a *poly. time* solution when $\mathcal{O}$ is **special extremal** :

[2] when it exists

Norm equation over Special Extremal Orders

We have a *poly. time* solution when $\mathcal{O}$ is **special extremal** : contains suborder $\mathbb{Z}\langle \omega_1, \omega_2 \rangle$ with small $q = n(\omega_1)$ and $n(\omega_2) = p$.

[2] when it exists

Norm equation over Special Extremal Orders

We have a *poly. time* solution when $\mathcal{O}$ is **special extremal** :
contains suborder $\mathbb{Z}\langle\omega_1, \omega_2\rangle$ with small $q = n(\omega_1)$ and $n(\omega_2) = p$.

$$\alpha = (x, y, z, t) \in \mathbb{Z}\langle\omega_1, \omega_2\rangle, \;\; n(\alpha) = (x^2 + qy^2) + p(z^2 + qt^2)$$

[2] when it exists

Norm equation over Special Extremal Orders

We have a *poly. time* solution when $\mathcal{O}$ is **special extremal** :
contains suborder $\mathbb{Z}\langle\omega_1, \omega_2\rangle$ with small $q = n(\omega_1)$ and $n(\omega_2) = p$.

$$\alpha = (x, y, z, t) \in \mathbb{Z}\langle\omega_1, \omega_2\rangle, \;\; n(\alpha) = (x^2 + qy^2) + p(z^2 + qt^2)$$

Algorithm to solve $n(\alpha) = M$:
Try random z, t until $x^2 + qy^2 = M - p(z^2 + qt^2)$ has a solution.

[2] when it exists

Norm equation over Special Extremal Orders

We have a *poly. time* solution when $\mathcal{O}$ is **special extremal** :
contains suborder $\mathbb{Z}\langle\omega_1, \omega_2\rangle$ with small $q = n(\omega_1)$ and $n(\omega_2) = p$.

$$\alpha = (x, y, z, t) \in \mathbb{Z}\langle\omega_1, \omega_2\rangle, \;\; n(\alpha) = (x^2 + qy^2) + p(z^2 + qt^2)$$

Algorithm to solve $n(\alpha) = M$:
Try random z, t until $x^2 + qy^2 = M - p(z^2 + qt^2)$ has a solution.

Cornacchia's algorithm : solutions[2] to $x^2 + qy^2 = M'$ when M' is prime.

[2] when it exists

The solution of KLPT

Algorithm KLPT:
Input: $\mathcal{O}$,I, $n(I) = N$
Output: $\beta \in I$ of norm $N\ell^e$.

The solution of KLPT

Algorithm KLPT:
Input: $\mathcal{O}$,I, $n(I) = N$
Output: $\beta \in I$ of norm $N\ell^e$.

1. Find $\gamma \in \mathcal{O}$ of norm $N\ell^{e_0}$.

The solution of KLPT

Algorithm KLPT:
Input: $\mathcal{O}$,I, $n(I) = N$
Output: $\beta \in I$ of norm $N\ell^e$.

1. Find $\gamma \in \mathcal{O}$ of norm $N\ell^{e_0}$.
2. Find $\nu_0 \in \mathcal{O}$ such that $\gamma\nu_0 \in I$.

The solution of KLPT

Algorithm KLPT:
Input: $\mathcal{O}$,I, $n(I) = N$
Output: $\beta \in I$ of norm $N\ell^e$.

1. Find $\gamma \in \mathcal{O}$ of norm $N\ell^{e_0}$.
2. Find $\nu_0 \in \mathcal{O}$ such that $\gamma\nu_0 \in I$.
3. Find $\nu \in \mathcal{O}$: the *strong approximation* of ν_0 of norm ℓ^{e_1}.

The solution of KLPT

Algorithm KLPT:
Input: $\mathcal{O}$,I, $n(I) = N$
Output: $\beta \in I$ of norm $N\ell^e$.

1. Find $\gamma \in \mathcal{O}$ of norm $N\ell^{e_0}$.
2. Find $\nu_0 \in \mathcal{O}$ such that $\gamma\nu_0 \in I$.
3. Find $\nu \in \mathcal{O}$: the *strong approximation* of ν_0 of norm ℓ^{e_1}.
4. Output $\beta = \gamma\nu$ of norm $N\ell^{e_0+e_1}$

The generalized Solution

We consider the case where neither $\mathcal{O}_1$ nor $\mathcal{O}_2$ are special extremal order. Take $\mathcal{O}_0$ such an order.

The solution given in KLPT14 : perform `KLPT` twice between $\mathcal{O}_0, \mathcal{O}_1$ and $\mathcal{O}_0, \mathcal{O}_2$, then concatenate the paths.

$$\begin{tikzcd}
 & E_1 \arrow[dr, "\varphi_I"] & \\
E_0 \arrow[ur, "\tau_1"] \arrow[rr, "\tau_2"'] & & E_2
\end{tikzcd}$$

Output: $\tau_2 \circ \hat{\tau}_1$

Contribution

Another Generalized KLPT algorithm, why bother ?

After all, KLPT14's results are sufficient for our security reductions.

Another Generalized KLPT algorithm, why bother ?

After all, KLPT14's results are sufficient for our security reductions.

Why we need a new, more refined, algorithm :

- Very specific solution, not satisfying from the theoretical point of view.

Another Generalized KLPT algorithm, why bother ?

After all, KLPT14's results are sufficient for our security reductions.

Why we need a new, more refined, algorithm :

- Very specific solution, not satisfying from the theoretical point of view.
- Twice the size of the solution in the special case $\rightarrow$ we should be able to do better.

Another Generalized KLPT algorithm, why bother ?

After all, KLPT14's results are sufficient for our security reductions.

Why we need a new, more refined, algorithm :

- Very specific solution, not satisfying from the theoretical point of view.
- Twice the size of the solution in the special case $\rightarrow$ we should be able to do better.
- Constructive application (GPS17) relying on KLPT.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Eichler Order: $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_0$

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Eichler Order: $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_0$ decomposes as $\mathbb{Z} + J$ where J is a left-$\mathcal{O}_0$ ideal $\rightarrow$ solving in $\mathfrak{O}$ is similar to `KLPT`.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Eichler Order: $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_0$ decomposes as $\mathbb{Z} + J$ where J is a left-$\mathcal{O}_0$ ideal $\to$ solving in $\mathfrak{O}$ is similar to `KLPT`.

`KLPT`: Solve a norm equation in $I \subset \mathcal{O}_0$.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Eichler Order: $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_0$ decomposes as $\mathbb{Z} + J$ where J is a left-$\mathcal{O}_0$ ideal $\rightarrow$ solving in $\mathfrak{O}$ is similar to `KLPT`.

`KLPT`: Solve a norm equation in $I \subset \mathcal{O}_0$.
New Generalized `KLPT`: Solve a norm equation in $I \cap \mathbb{Z} + J \subset \mathcal{O}_0$.

Solving norm equations over non-extremal special orders

For a **random** maximal $\mathcal{O}$ the smallest q we can choose is $p^{2/3}$.

When q is big, $x^2 + qy^2 = M$ has *very small probabilty* to have a solution.

Solution: look for another type of suborder inside $\mathcal{O}$. We know how to solve things in $\mathcal{O}_0$.

Eichler Order: $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_0$ decomposes as $\mathbb{Z} + J$ where J is a left-$\mathcal{O}_0$ ideal $\rightarrow$ solving in $\mathfrak{O}$ is similar to `KLPT`.

`KLPT`: Solve a norm equation in $I \subset \mathcal{O}_0$.
New Generalized `KLPT`: Solve a norm equation in $I \cap \mathbb{Z} + J \subset \mathcal{O}_0$.

Norm equation in $I \cap \mathbb{Z} + J$: `KLPT` but with two strong approximation steps.

Analysis of the solution

Output: ideal of norm ℓ^e, size of e ? The smallest solution is $e \approx \log_\ell(p)$.

KLPT[3]:

$$e = e_0 + e_1 \approx \underbrace{1/2 \log_\ell(p)}_{\text{first norm equation}} + \underbrace{3 \log_\ell(p)}_{\text{strong approximation}} = 7/2 \log_\ell(p)$$

[3] The size of the generalized solution of KLPT14 is twice that size

Analysis of the solution

Output: ideal of norm ℓ^e, size of e ? The smallest solution is $e \approx \log_\ell(p)$.

KLPT[3]:

$$e = e_0 + e_1 \approx \underbrace{1/2 \log_\ell(p)}_{\text{first norm equation}} + \underbrace{3 \log_\ell(p)}_{\text{strong approximation}} = 7/2 \log_\ell(p)$$

New generalized KLPT:

$$e = e_0 + e_1 \approx \underbrace{1/2 \log_\ell(p)}_{\text{first norm equation}} + \underbrace{5 \log_\ell(p)}_{\text{2 combined strong approx.}} = 11/2 \log_\ell(p)$$

[3] The size of the generalized solution of KLPT14 is twice that size

Analysis of the solution

Output: ideal of norm ℓ^e, size of e ? The smallest solution is $e \approx \log_\ell(p)$.

$\mathtt{KLPT}$[3]:

$$e = e_0 + e_1 \approx \underbrace{1/2 \log_\ell(p)}_{\text{first norm equation}} + \underbrace{3 \log_\ell(p)}_{\text{strong approximation}} = 7/2 \log_\ell(p)$$

New generalized $\mathtt{KLPT}$:

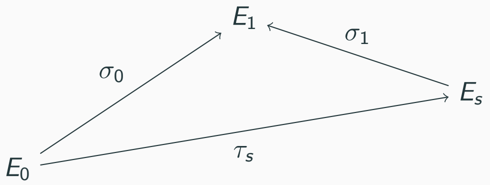
$$e = e_0 + e_1 \approx \underbrace{1/2 \log_\ell(p)}_{\text{first norm equation}} + \underbrace{5 \log_\ell(p)}_{\text{2 combined strong approx.}} = 11/2 \log_\ell(p)$$

New solution is less specific : *no obvious property*. More analysis ?

[3] The size of the generalized solution of KLPT14 is twice that size

A constructive application: Signature

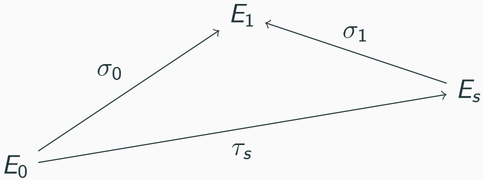
GPS17 : A 2-special sound identification protocol.



Secret key is τ_s, public key is E_s, Alice wants to identify to Bob.

A constructive application: Signature

GPS17 : A 2-special sound identification protocol.

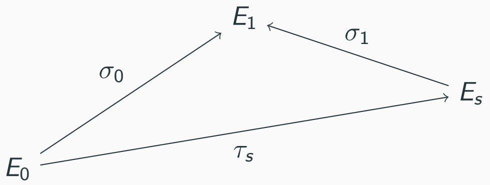


Secret key is τ_s, public key is E_s, Alice wants to identify to Bob.

1. **Commitment**: Alice selects random path σ_1, sends E_1.

A constructive application: Signature

GPS17 : A 2-special sound identification protocol.

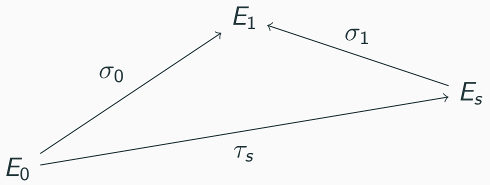


Secret key is τ_s, public key is E_s, Alice wants to identify to Bob.

1. **Commitment**: Alice selects random path σ_1, sends E_1.
2. **Challenge**: Bob sends a bit b.

A constructive application: Signature

GPS17 : A 2-special sound identification protocol.



Secret key is τ_s, public key is E_s, Alice wants to identify to Bob.

1. **Commitment**: Alice selects random path σ_1, sends E_1.
2. **Challenge**: Bob sends a bit b.
3. **Challenge's answer**: Alice sends σ_b.

A constructive application: Signature

GPS17 : A 2-special sound identification protocol.

$$\begin{tikzcd} & E_1 & & \\ & & & E_s \arrow[ull, "\sigma_1"'] \\ E_0 \arrow[uur, "\sigma_0"] \arrow[urrr, "\tau_s"'] & & & \end{tikzcd}$$

Secret key is τ_s, public key is E_s, Alice wants to identify to Bob.

1. **Commitment**: Alice selects random path σ_1, sends E_1.
2. **Challenge**: Bob sends a bit b.
3. **Challenge's answer**: Alice sends σ_b.
4. **Verification**: Bob checks if the arrival curve of σ_b is E_1.

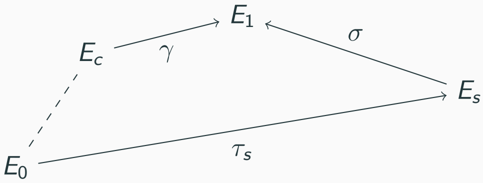
A constructive application: Signature

Previous identification protocol can be extended to 2^λ soundness by repeating it λ times. Can we do better and batch it[4] ?

[4] This is an on-going work with L. de Feo, D. Kohel, C. Petit, B. Wesolowski

A constructive application: Signature

Previous identification protocol can be extended to 2^λ soundness by repeating it λ times. Can we do better and batch it[4] ?

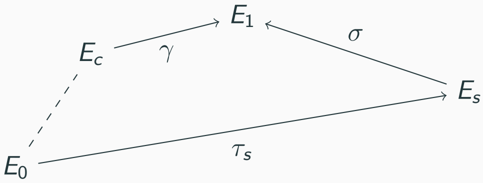


Take an isogeny γ as the challenge ? Answering requires to compute σ $\Rightarrow$ we need generalized `KLPT`.

[4]This is an on-going work with L. de Feo, D. Kohel, C. Petit, B. Wesolowski

A constructive application: Signature

Previous identification protocol can be extended to 2^λ soundness by repeating it λ times. Can we do better and batch it[4] ?



Take an isogeny γ as the challenge ? Answering requires to compute σ $\Rightarrow$ we need generalized `KLPT`.

Previous solution reveals a path to E_0, not ours.

[4]This is an on-going work with L. de Feo, D. Kohel, C. Petit, B. Wesolowski

Conclusion

A new generalized solution to the Quaternion ℓ-isogeny path problem:

- Smaller and more generic solution to the problem.

Conclusion

A new generalized solution to the Quaternion ℓ-isogeny path problem:

- Smaller and more generic solution to the problem.
- A generalization of the signature protocol from GPS17.

Conclusion

A new generalized solution to the Quaternion ℓ-isogeny path problem:

- Smaller and more generic solution to the problem.
- A generalization of the signature protocol from GPS17.
- Other applications?

Questions ?