

# The generalized KLPT algorithm

---

Antonin Leroux

DGA, Inria Saclay

Current cryptography :

- The Integer Factorization Problem
- The Discrete Logarithm Problem

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) → 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

1. Isogeny-based cryptography
2. The Deuring Correspondence
3. The Quaternion  $\ell$ -isogeny Path Problem
4. Contribution

# Isogeny-based cryptography

---

Separable isogeny:

$$\phi : E \rightarrow E'$$

# Isogeny notations

**Separable isogeny:**

$$\phi : E \rightarrow E'$$

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



# Isogeny notations

**Separable isogeny:**

$$\phi : E \rightarrow E'$$

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

The **dual** isogeny  $\hat{\phi} : E' \rightarrow E$

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

# Endomorphism ring

An isogeny  $\phi : E \rightarrow E$  is an **endomorphism**.  $\text{End}(E)$  is a ring with addition and composition.

# Endomorphism ring

An isogeny  $\phi : E \rightarrow E$  is an **endomorphism**.  $\text{End}(E)$  is a ring with addition and composition.

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

# Endomorphism ring

An isogeny  $\phi : E \rightarrow E$  is an **endomorphism**.  $\text{End}(E)$  is a ring with addition and composition.

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

On elliptic curves over finite fields:

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

# Supersingular Isogeny Graph

Supersingular  $\ell$ -isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are  $\ell$ -isogenies.

This graph is

- Finite

# Supersingular Isogeny Graph

Supersingular  $\ell$ -isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are  $\ell$ -isogenies.

This graph is

- Finite
- Fully connected

# Supersingular Isogeny Graph

Supersingular  $\ell$ -isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are  $\ell$ -isogenies.

This graph is

- Finite
- Fully connected
- Regular

# Supersingular Isogeny Graph

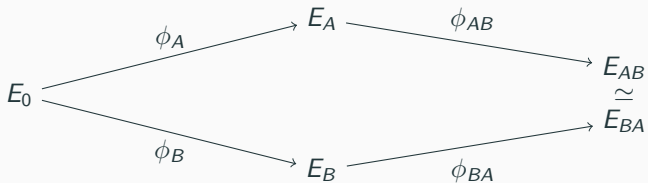
Supersingular  $\ell$ -isogeny graph: **Vertices** are supersingular elliptic curves, **Edges** are  $\ell$ -isogenies.

This graph is

- Finite
- Fully connected
- Regular
- Ramanujan (optimal expander graph)



# Supersingular Isogeny Diffie Hellman



# Supersingular Isogeny Problem

The underlying security problem:

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

# 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:**

$$\alpha = a_1 + a_2i + a_3j + a_4k \mapsto \bar{\alpha} = a_1 - a_2i - a_3j - a_4k$$

# 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:**

$$\alpha = a_1 + a_2i + a_3j + a_4k \mapsto \bar{\alpha} = a_1 - a_2i - a_3j - a_4k$$

The **reduced norm**

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

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

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



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

The (maximal) **left order**  $O_L(I)$  of an ideal is

$$O_L(I) = \{\alpha \in H(a, b), \alpha I \subset I\}$$

An ideal is **integral** when  $I \subset O_L(I)$ .

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

The (maximal) **left order**  $O_L(I)$  of an ideal is

$$O_L(I) = \{\alpha \in H(a, b), \alpha I \subset I\}$$

An ideal is **integral** when  $I \subset O_L(I)$ .

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

# The Deuring Correspondence

Supersingular elliptic curves over  $\mathbb{F}_{p^2}$   $\longleftrightarrow$  Maximal orders in  $\mathcal{A}_p$

# The Deuring Correspondence

Supersingular elliptic curves over  $\mathbb{F}_{p^2} \longleftrightarrow$  Maximal orders in  $\mathcal{A}_p$

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

$$E_0 : y^2 = x^3 + x \text{ and } \text{End}(E_0) \simeq \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle$$

with  $\pi$  is the Frobenius and  $\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$

# The Deuring Correspondence, Summary

|   |   |
|---|---|
| Supersingular elliptic curve over $\mathbb{F}_{p^2}$<br>$E_0$ | Maximal Orders in $\mathcal{A}_p$<br>$O_0 \simeq \text{End}(E_0)$ |
| $(E_1, \phi)$ with $\phi : E_0 \rightarrow E_1$               | $I_\phi$ integral left $O_0$ -ideal                               |
| $\text{deg}(\phi)$  | $n(I_\phi)$   |
| $\hat{\phi}$  | $\overline{I_\phi}$   |
| $\phi : E_0 \rightarrow E_1, \psi : E_0 \rightarrow E_1$      | Equivalent Ideals $I_\phi \sim I_\psi$                            |

# The Quaternion $\ell$ -isogeny Path Problem

---

# The problem

The Quaternion  $\ell$ -Isogeny Path Problem is the problem corresponding to the Supersingular  $\ell$ -Isogeny Problem through the Deuring Correspondence.

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

This problem allows to reduce the Supersingular  $\ell$ -isogeny problem to the **computation of the endomorphism ring**.

## Lemma

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

Solving the Quaternion  $\ell$ -Isogeny Path Problem reduces to solving a norm equation over  $I$ .



# The solution of KLPT

In 2014, Kohel et al. polynomial time solution when  $O$  is a *special extremal* order.

Algorithm KLPT:

**Input:**  $I$ ,  $n(I) = N$

**Output:**  $J \sim I$

# The solution of KLPT

In 2014, Kohel et al. polynomial time solution when  $O$  is a *special extremal* order.

Algorithm KLPT:

**Input:**  $I$ ,  $n(I) = N$

**Output:**  $J \sim I$

1. Find  $\gamma \in O$  of norm  $N\ell^{\epsilon_0}$ .

# The solution of KLPT

In 2014, Kohel et al. polynomial time solution when  $O$  is a *special extremal* order.

Algorithm KLPT:

**Input:**  $I$ ,  $n(I) = N$

**Output:**  $J \sim I$

1. Find  $\gamma \in O$  of norm  $N\ell^{\epsilon_0}$ .
2. Find  $\nu_0$  such that  $\gamma\nu_0 \in I$ .

# The solution of KLPT

In 2014, Kohel et al. polynomial time solution when  $O$  is a *special extremal* order.

Algorithm KLPT:

**Input:**  $I$ ,  $n(I) = N$

**Output:**  $J \sim I$

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

# The solution of KLPT

In 2014, Kohel et al. polynomial time solution when  $O$  is a *special extremal* order.

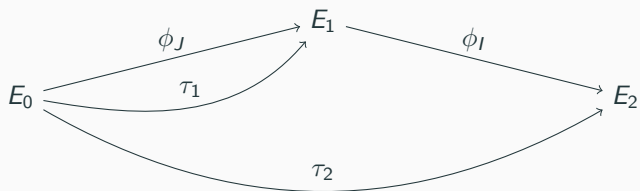
Algorithm KLPT:

**Input:**  $I$ ,  $n(I) = N$

**Output:**  $J \sim I$

1. Find  $\gamma \in O$  of norm  $N\ell^{e_0}$ .
2. Find  $\nu_0$  such that  $\gamma\nu_0 \in I$ .
3. Find  $\nu$  the *strong approximation* of  $\nu_0$  of norm  $\ell^{e_1}$ .
4. Output  $J = I \frac{\bar{\beta}}{N}$  with  $\beta = \gamma\nu$ .

# The generic Solution



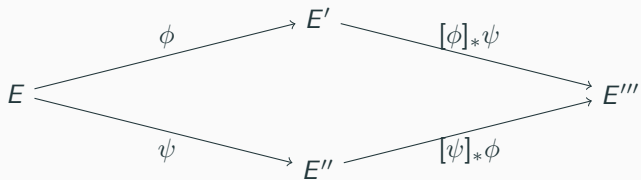
**Input:**  $\phi_I, \phi_J$

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

# Contribution

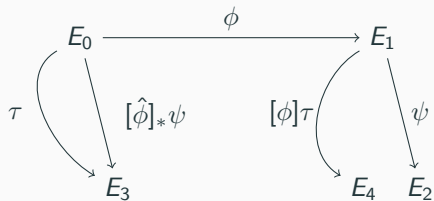
---

# Pushforward isogenies

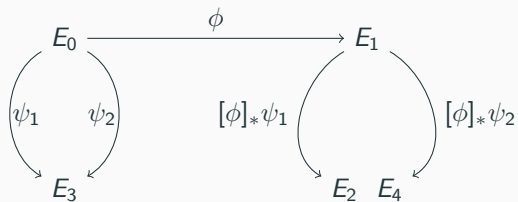




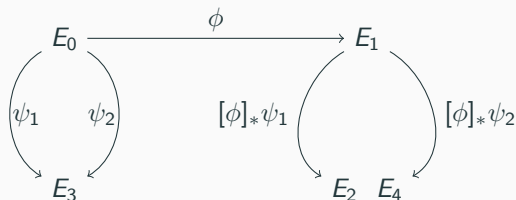
# The idea of the algorithm



When does  $E_2 \simeq E_4$  ?



# When does $E_2 \simeq E_4$ ?



## Lemma

Given:

- Two isogenies  $\psi_1, \psi_2$  from  $E_0$  to  $E_3$  of degree  $N_1, N_2$ ,  $\beta = \hat{\psi}_2 \circ \psi_1$
- $\phi : E_0 \rightarrow E_1$  of kernel  $\langle R \rangle$  and degree  $N$  coprime with  $N_1$  and  $N_2$

$$E_2 \simeq E_4 \Leftrightarrow I_{\psi_2} = I_{\psi_1} \frac{\bar{\beta}}{N_1} \text{ and } \exists \lambda \in \mathbb{Z}/N\mathbb{Z}^* \text{ such that } \beta - \lambda \in I_\phi$$

# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

1. Compute  $I' = \left[ I_{\hat{\phi}} \right]_* I$

# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

1. Compute  $I' = \left[ I_{\hat{\phi}} \right]_* I$
2. Find  $\beta_1 \in I'$  of norm  $N\ell^{e_0}$  with KLPT.

# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

1. Compute  $I' = \left[ I_{\hat{\phi}} \right]_* I$
2. Find  $\beta_1 \in I'$  of norm  $N\ell^{e_0}$  with KLPT.
3. Find  $\nu_0 \in O_0$  such that  $\exists \lambda \in \mathbb{Z}^*$ , such that  $\beta_1 \nu - \lambda \in I_\phi$ .

# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

1. Compute  $I' = \left[ I_{\hat{\phi}} \right]_* I$
2. Find  $\beta_1 \in I'$  of norm  $N\ell^{e_0}$  with KLPT.
3. Find  $\nu_0 \in O_0$  such that  $\exists \lambda \in \mathbb{Z}^*$ , such that  $\beta_1 \nu - \lambda \in I_\phi$ .
4. Find  $\nu$ , the *strong approximation* of  $\nu_0$  of norm  $\ell^{e_1}$ .



# The new generic algorithm

Algorithm GeneralizedKLPT:

**Input:**  $I$  a left  $O_1$  ideal,  $I_\phi$ .

**Output:**  $J \sim I$  of norm  $\ell^e$ .

1. Compute  $I' = [I_{\hat{\phi}}]_* I$
2. Find  $\beta_1 \in I'$  of norm  $N\ell^{e_0}$  with KLPT.
3. Find  $\nu_0 \in O_0$  such that  $\exists \lambda \in \mathbb{Z}^*$ , such that  $\beta_1\nu - \lambda \in I_\phi$ .
4. Find  $\nu$ , the *strong approximation* of  $\nu_0$  of norm  $\ell^{e_1}$ .
5. Set  $\beta = \beta_1\nu$ ,  $J' = I' \frac{\bar{\beta}}{N}$  and output  $J = [I_\phi]_* J'$ .

# Analysis of the solution

The KLPT algorithm for the *special extremal* case produces a solution of norm  $\ell^e$  where  $e \sim \frac{7}{2} \log_\ell(p) = \frac{1}{2} \log_\ell(p) + 3 \log_\ell(p)$ <sup>1</sup>.

---

<sup>1</sup>The size of the smallest solution is around  $\log_\ell(p)$ .

# Analysis of the solution

The KLPT algorithm for the *special extremal* case produces a solution of norm  $\ell^e$  where  $e \sim \frac{7}{2} \log_\ell(p) = \frac{1}{2} \log_\ell(p) + 3 \log_\ell(p)$ <sup>1</sup>.

The solution of our algorithm has norm  $\ell^e$  with  $e \sim \frac{7}{2} \log_\ell(p) + 3 \log_\ell(p) = \frac{13}{2} \log_\ell(p)$ .

---

<sup>1</sup>The size of the smallest solution is around  $\log_\ell(p)$ .

# Analysis of the solution

The KLPT algorithm for the *special extremal* case produces a solution of norm  $\ell^e$  where  $e \sim \frac{7}{2} \log_\ell(p) = \frac{1}{2} \log_\ell(p) + 3 \log_\ell(p)$ <sup>1</sup>.

The solution of our algorithm has norm  $\ell^e$  with  $e \sim \frac{7}{2} \log_\ell(p) + 3 \log_\ell(p) = \frac{13}{2} \log_\ell(p)$ .

An optimization allows to reduce this term by  $\log_\ell(p)$ , yielding a solution of size  $\frac{11}{2} \log_\ell(p)$ .

---

<sup>1</sup>The size of the smallest solution is around  $\log_\ell(p)$ .

# Analysis of the solution

The KLPT algorithm for the *special extremal* case produces a solution of norm  $\ell^e$  where  $e \sim \frac{7}{2} \log_\ell(p) = \frac{1}{2} \log_\ell(p) + 3 \log_\ell(p)$ <sup>1</sup>.

The solution of our algorithm has norm  $\ell^e$  with  $e \sim \frac{7}{2} \log_\ell(p) + 3 \log_\ell(p) = \frac{13}{2} \log_\ell(p)$ .

An optimization allows to reduce this term by  $\log_\ell(p)$ , yielding a solution of size  $\frac{11}{2} \log_\ell(p)$ .

The output isogeny  $\phi_I$ , does it reveal any information on  $\phi$ ?

---

<sup>1</sup>The size of the smallest solution is around  $\log_\ell(p)$ .

A new solution to generic Quaternion  $\ell$ -isogeny path problem:

- Attacks and Security Reductions.

A new solution to generic Quaternion  $\ell$ -isogeny path problem:

- Attacks and Security Reductions.
- A generalization of the signature protocol from Galbraith et al. in 2017.

A new solution to generic Quaternion  $\ell$ -isogeny path problem:

- Attacks and Security Reductions.
- A generalization of the signature protocol from Galbraith et al. in 2017.
- Other applications?



**Thank you for your time.**