The generalized KLPT algorithm

Antonin Leroux

DGA, Inria Saclay

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

Isogeny notations

Separable isogeny:

$$\phi : E \to E'$$

Isogeny notations

Separable isogeny:

$$\phi : E \to E'$$

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

Isogeny notations

Separable isogeny:

$$\phi : E \to E'$$

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

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

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

Endomorphism ring

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

Endomorphism ring

An isogeny $\phi : E \to E$ 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 $\phi : E \to E$ 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 $\pi : (x, y) \to (x^p, y^p)$

On 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

Supersingular Isogeny Graph

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

This graph is

- Finite
- Fully connected

Supersingular Isogeny Graph

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

This graph is

- Finite
- Fully connected
- Regular

Supersingular Isogeny Graph

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

This graph is

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

Supersingular Isogeny Diffie Hellman

$$
\begin{tikzcd}
& E_A \arrow[rr, "\phi_{AB}"] & & E_{AB} \\
E_0 \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & & \simeq \\
& E_B \arrow[rr, "\phi_{BA}"'] & & E_{BA}
\end{tikzcd}
$$

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 $\phi : E_1 \to E_2$ 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** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

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

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** 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 $I \subset O_L(I)$.

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** 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 $q \in H(a,b)^\star$

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

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

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

The Deuring Correspondence, Summary

Supersingular elliptic curve over $\mathbb{F}_{p^2}$ E_0	Maximal Orders in $\mathcal{A}_p$ $O_0 \simeq \mathrm{End}(E_0)$
(E_1, ϕ) with $\phi : E_0 \to E_1$	I_ϕ integreal left O_0-ideal
$\deg(\phi)$	$n(I_\phi)$
$\hat{\phi}$	$\overline{I_\phi}$
$\phi : E_0 \to E_1, \psi : E_0 \to E_1$	Equivalent Ideals $I_\phi \sim I_\psi$

The Quaternion ℓ-isogeny Path Problem

The problem

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

Quaternion ℓ-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 ℓ^e for $e \in \mathbb{N}^\star$.

This problem allows to reduce the Supersingular ℓ-isogeny problem to the **computation of the endomorphism ring.**

A key lemma

Lemma

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

Solving the Quaternion ℓ-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 $N\ell^{e_0}$.

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 $N\ell^{e_0}$.
2. Find ν_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 ν_0 such that $\gamma\nu_0 \in I$.
3. Find ν the *strong approximation* of ν_0 of norm ℓ^{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 ν_0 such that $\gamma\nu_0 \in I$.
3. Find ν the *strong approximation* of ν_0 of norm ℓ^{e_1}.
4. Output $J = I\frac{\overline{\beta}}{N}$ with $\beta = \gamma\nu$.

The generic Solution

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

Input: ϕ_I, ϕ_J

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

Contribution

Pushforward isogenies

$$\begin{tikzcd}
 & E' \arrow[dr, "{[\phi]_*\psi}"] & \\
E \arrow[ur, "\phi"] \arrow[dr, "\psi"'] & & E''' \\
 & E'' \arrow[ur, "{[\psi]_*\phi}"'] &
\end{tikzcd}$$

The idea of the algorithm

$$
\begin{tikzcd}
E_0 \arrow[rrr, "\phi"] \arrow[dr, bend right, "\tau"'] \arrow[dr, "{[\hat{\phi}]_*\psi}"] & & & E_1 \arrow[d, bend right, "{[\phi]\tau}"'] \arrow[dr, "\psi"] & \\
& E_3 & & E_4 & E_2
\end{tikzcd}
$$

When does $E_2 \simeq E_4$?

$$
\begin{tikzcd}
E_0 \arrow[rrr, "\phi"] \arrow[d, bend right, "\psi_1"'] \arrow[d, bend left, "\psi_2"] & & & E_1 \arrow[dl, bend right, "{[\phi]_*\psi_1}"'] \arrow[dr, bend left, "{[\phi]_*\psi_2}"] & \\
E_3 & & E_2 & & E_4
\end{tikzcd}
$$

When does $E_2 \simeq E_4$?

$$\begin{tikzcd}
E_0 \arrow[rr, "\phi"] \arrow[d, bend right, "\psi_1"'] \arrow[d, bend left, "\psi_2"] & & E_1 \arrow[d, bend right, "{[\phi]_*\psi_1}"'] \arrow[dr, bend left, "{[\phi]_*\psi_2}"] & \\
E_3 & & E_2 & E_4
\end{tikzcd}$$

Lemma
Given:

- *Two isogenies ψ_1, ψ_2 from E_0 to E_3 of degree N_1, N_2,* $\beta = \hat{\psi}_2 \circ \psi_1$
- $\phi : E_0 \to E_1$ *of kernel $\langle R \rangle$ and degree N coprime with N_1 and N_2*

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

The new generic algorithm

Algorithm `GeneralizedKLPT`:
Input: I a left O_1 ideal, I_ϕ.
Output: $J \sim I$ of norm ℓ^e.

The new generic algorithm

Algorithm `GeneralizedKLPT`:

Input: I a left O_1 ideal, I_ϕ.

Output: $J \sim I$ of norm ℓ^e.

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

The new generic algorithm

Algorithm `GeneralizedKLPT`:

Input: I a left O_1 ideal, I_ϕ.

Output: $J \sim I$ of norm ℓ^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_ϕ.

Output: $J \sim I$ of norm ℓ^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. $\boxed{\text{Find } \nu_0 \in O_0 \text{ such that } \exists \lambda \in \mathbb{Z}^\star, \text{ such that } \beta_1 \nu - \lambda \in I_\phi.}$

The new generic algorithm

Algorithm `GeneralizedKLPT`:

Input: I a left O_1 ideal, I_ϕ.

Output: $J \sim I$ of norm ℓ^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. $\boxed{\text{Find } \nu_0 \in O_0 \text{ such that } \exists \lambda \in \mathbb{Z}^\star, \text{ such that } \beta_1\nu - \lambda \in I_\phi.}$
4. Find ν, the *strong approximation* of ν_0 of norm ℓ^{e_1}.

The new generic algorithm

Algorithm `GeneralizedKLPT`:

Input: I a left O_1 ideal, I_ϕ.

Output: $J \sim I$ of norm ℓ^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. $\boxed{\text{Find } \nu_0 \in O_0 \text{ such that } \exists \lambda \in \mathbb{Z}^\star\text{, such that } \beta_1\nu - \lambda \in I_\phi.}$
4. Find ν, the *strong approximation* of ν_0 of norm ℓ^{e_1}.
5. Set $\beta = \beta_1\nu$, $J' = I'\frac{\overline{\beta}}{N}$ and output $J = [I_\phi]_* J'$.

Analysis of the solution

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

[1] 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 ℓ^e where $e \sim \frac{7}{2}\log_\ell(p) = \frac{1}{2}\log_\ell(p) + 3\log_\ell(p)$[1].

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

[1] 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 ℓ^e where $e \sim \frac{7}{2}\log_\ell(p) = \frac{1}{2}\log_\ell(p) + 3\log_\ell(p)$[1].

The solution of our algorithm has norm ℓ^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 $\frac{11}{2}\log_\ell(p)$.

[1] 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 ℓ^e where $e \sim \frac{7}{2}\log_\ell(p) = \frac{1}{2}\log_\ell(p) + 3\log_\ell(p)$[1].

The solution of our algorithm has norm ℓ^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 ϕ_I, does it reveal any information on ϕ?

[1] The size of the smallest solution is around $\log_\ell(p)$.

Conclusion

A new solution to generic Quaternion ℓ-isogeny path problem:

- Attacks and Security Reductions.

Conclusion

A new solution to generic Quaternion ℓ-isogeny path problem:

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

Conclusion

A new solution to generic Quaternion ℓ-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.