On the quaternion ℓ-isogeny problem

Christophe Petit, University College London

Partially based on joint work with
David Kohel, Kristin Lauter and Jean-Pierre Tignol

Charles-Goren-Lauter hash function

Hash of the Future?

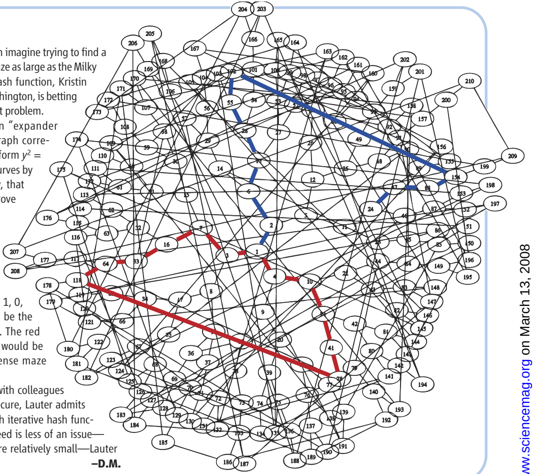
Have you ever struggled to solve a maze? Then imagine trying to find a path through a tangled, three-dimensional maze as large as the Milky Way. By incorporating such a maze into a hash function, Kristin Lauter of Microsoft Research in Redmond, Washington, is betting that neither you nor anyone else will solve that problem.

Technically, Lauter's maze is called an "expander graph" (see figure, right). Nodes in the graph correspond to elliptic curves, or equations of the form $y^2 = x^3 + ax + b$. Each curve leads to three other curves by a mathematical relation, now called isogeny, that Pierre de Fermat discovered while trying to prove his famous Last Theorem.

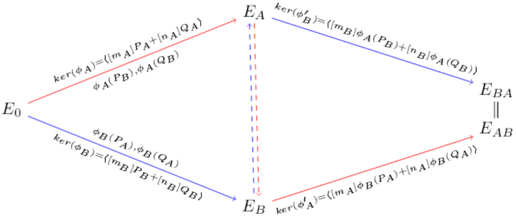
To hash a digital file using an expander graph, you would convert the bits of data into directions: 0 would mean "turn right," 1 would mean "turn left." In the maze illustrated here, after the initial step 1-2, the blue path encodes the directions 1, 0, 1, 1, 0, 0, 0, 0, 1, ending at point 24, which would be the digital signature of the string 101100001. The red loop shows a collision of two paths, which would be practically impossible to find in the immense maze envisioned by Lauter.

Although her hash function (developed with colleagues Denis Charles and Eyal Goren) is provably secure, Lauter admits that it is not yet fast enough to compete with iterative hash functions. However, for applications in which speed is less of an issue—for example, where the files to be hashed are relatively small—Lauter believes it might be a winner.

–D.M.



Key exchange of the future?



- De Feo - Jao - Plût key exchange:
  Alice and Bob use isogeny paths with two different primes ℓ_1, ℓ_2; these paths commute
- Also public key encryption, zero-knowledge protocol

Deuring's correspondence

- Bijection from **supersingular elliptic curves** over $\bar{\mathbb{F}}_p$ (up to Galois conjugacy) to **maximal orders** in the quaternion algebra $B_{p,\infty}$ ramified at p and infinity (up to equivalence)

$$E \to \mathcal{O} = \mathrm{End}(E)$$

- An **isogeny** $\varphi : E_0 \to E_1$ is sent to the **left $\mathcal{O}$-ideal** $I = \mathrm{Hom}(E_1, E_0)\varphi$
- A path between two curves in the supersingular ℓ-isogeny graph is sent to an ideal of ℓ-power norm

Strategy to break CGL hash

- Translate collision and preimage resistance properties in the quaternion world
- Break collision and preimage resistance properties in the quaternion world
- Translate the attacks (as much as possible) back to the elliptic curve world

Outline

Outline

Definitions and notations

Quaternion algorithm overview

Subalgorithms

Partial translation to elliptic curves

Conclusion and future work

Endomorphism ring of elliptic curves

- Endomorphism of E: group homomorphism defined by a rational map $E \to E$

$$(x, y) \to \left(\frac{p_X(x, y)}{q_X(x, y)}, \frac{p_Y(x, y)}{q_Y(x, y)} \right)$$

- Form a ring for point addition and map composition
  - Include scalar multiplications $[k] : (x, y) \to [k](x, y)$
  - Over $\mathbb{F}_q$, include Frobenius $\pi : (x, y) \to (x^q, y^q)$
  - Include linear combinations of both $[a + b\pi]$

Supersingular elliptic curves

- A curve / j-invariant over $\bar{\mathbb{F}}_p$ is **supersingular** if its *trace* is 0 mod p
- Roughly $p/12$ supersingular j-invariants in $\bar{\mathbb{F}}_p$, all of them defined over $\mathbb{F}_{p^2}$
- Endomomorphism ring of a supersingular curve
  - Contains some extra element ϕ such that $\phi\pi \neq \pi\phi$
  - Contains linear combinations $[a + b\pi + c\phi + d\pi\phi]$
  - Is a *maximal order* in the *quaternion algebra* $B_{p,\infty}$

The quaternion algebra $B_{p,\infty}$

- Quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
- $B_{p,\infty} = \mathbb{Q}\langle i, j\rangle$ with $i^2 = -q$, $j^2 = -p$, $k = ij = -ji$ for some q coprime to p
- Canonical involution, reduced trace, reduced norm and associated bilinear form are
$$\alpha = a + bi + cj + dk \to \bar{\alpha} = a - bi - cj - dk$$
$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2a$$
$$\mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = a^2 + qb^2 + pc^2 + pqd^2$$
$$\langle x, y\rangle = \mathrm{Nrd}(x + y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)$$
- Under GRH we can choose $q = O(\log^2 p)$

Ideals and Orders

- An **ideal** $I \subset B_{p,\infty}$ is a lattice of dimension 4
- An **order** $\mathcal{O} \subset B_{p,\infty}$ is an ideal which is also a ring

Ideals and Orders

- An **ideal** $I \subset B_{p,\infty}$ is a lattice of dimension 4
- An **order** $\mathcal{O} \subset B_{p,\infty}$ is an ideal which is also a ring
- $\alpha \in B_{p,\infty}$ is **integer** if $\mathrm{Trd}(\alpha)$ and $\mathrm{Nrd}(\alpha)$ are integers
- Order elements are integers

Ideals and Orders

- An **ideal** $I \subset B_{p,\infty}$ is a lattice of dimension 4
- An **order** $\mathcal{O} \subset B_{p,\infty}$ is an ideal which is also a ring
- $\alpha \in B_{p,\infty}$ is **integer** if $\mathrm{Trd}(\alpha)$ and $\mathrm{Nrd}(\alpha)$ are integers
- Order elements are integers
- The **left order** of an ideal I is defined as

  $$\mathcal{O}_\ell(I) = \{h \in B_{p,\infty} | hI \subset I\}$$

  We say I is a **left $\mathcal{O}$-ideal**
- Right orders and right ideals are defined similarly

Ideals and Orders

- We can multiply ideals together, conjugate them
- If I is a left $\mathcal{O}$-ideal then $I\bar{I} = N\mathcal{O}$

Ideals and Orders

- We can multiply ideals together, conjugate them
- If I is a left $\mathcal{O}$-ideal then $I\bar{I} = N\mathcal{O}$
- A left $\mathcal{O}$-ideal I of norm N can be written as $I = \mathcal{O}N + \mathcal{O}\alpha$ where $N|\mathrm{Nrd}(\alpha)$

Ideals and Orders

- We can multiply ideals together, conjugate them
- If I is a left $\mathcal{O}$-ideal then $I\bar{I} = N\mathcal{O}$
- A left $\mathcal{O}$-ideal I of norm N can be written as $I = \mathcal{O}N + \mathcal{O}\alpha$ where $N|\mathrm{Nrd}(\alpha)$
- We say two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are in the same class if $q\mathcal{O}_1 q^{-1} = \mathcal{O}_2$ for some $q \in B_{p,\infty}^*$
- We say two left $\mathcal{O}$-ideals I_1 and I_2 are in the same class and write $I_1 \approx I_2$ if $I_1 = I_2 q$ for some $q \in B_{p,\infty}^*$

Norm and norm forms

- **Norm** of ideal I is the minimal N such that $\forall \alpha \in I$, $\mathrm{Nrd}(\alpha)/N \in \mathbb{Z}$
- Norms are multiplicative

Norm and norm forms

- **Norm** of ideal I is the minimal N such that $\forall\alpha \in I$, $\mathrm{Nrd}(\alpha)/N \in \mathbb{Z}$
- Norms are multiplicative
- **Norm form** associated to ideal I is

$$\mathsf{N}(a, b, c, d) = \mathrm{Nrd}(a\omega_1 + b\omega_2 + c\omega_3 + d\omega_4)$$

where $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ is a $\mathbb{Z}$-basis of I

Norm and norm forms

- **Norm** of ideal I is the minimal N such that $\forall \alpha \in I$, $\mathrm{Nrd}(\alpha)/N \in \mathbb{Z}$
- Norms are multiplicative
- **Norm form** associated to ideal I is

  $$\mathrm{N}(a, b, c, d) = \mathrm{Nrd}(a\omega_1 + b\omega_2 + c\omega_3 + d\omega_4)$$

  where $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ is a $\mathbb{Z}$-basis of I
- Norm forms are quadratic equations with large coefficients in general

Maximal and extremal orders

- An order $\mathcal{O}$ is **maximal** if there is no other order in $B_{p,\infty}$ that contains $\mathcal{O}$
- We say a maximal order $\mathcal{O}$ of $B_{p,\infty}$ is p-**extremal** if it contains π ($= j$ as above) such that $\pi^2 = -p$
- Extremal orders correspond to elliptic curves defined over $\mathbb{F}_p$, with Frobenius endomorphism π

Special orders

- Let $\mathcal{O}$ extremal, and $j \in \mathcal{O}$ with $j^2 = -p$
- Let $R = \mathcal{O} \cap \mathbb{Q}[i]$
- Let ω such that $R = \mathbb{Q}[\omega]$ and let $D = \mathrm{disc}(R)$

Special orders

- Let $\mathcal{O}$ extremal, and $j \in \mathcal{O}$ with $j^2 = -p$
- Let $R = \mathcal{O} \cap \mathbb{Q}[i]$
- Let ω such that $R = \mathbb{Q}[\omega]$ and let $D = \mathrm{disc}(R)$
- Then $R + Rj$ has index D in $\mathcal{O}$ and

  $$\mathrm{Nrd}((x_1 + y_1\omega) + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2)$$

  where f principal quadratic form of discriminant D
- We say $\mathcal{O}$ is **special** if it is p-extremal with minimal D among all p-extremal orders

Special orders

- Let $\mathcal{O}$ extremal, and $j \in \mathcal{O}$ with $j^2 = -p$
- Let $R = \mathcal{O} \cap \mathbb{Q}[i]$
- Let ω such that $R = \mathbb{Q}[\omega]$ and let $D = \mathrm{disc}(R)$
- Then $R + Rj$ has index D in $\mathcal{O}$ and

  $$\mathrm{Nrd}((x_1 + y_1\omega) + (x_2 + y_2\omega)j) = f(x_1, y_1) + pf(x_2, y_2)$$

  where f principal quadratic form of discriminant D
- We say $\mathcal{O}$ is **special** if it is p-extremal with minimal D among all p-extremal orders
- Special norm form will be crucial in our algorithms

Isogenies

- An isogeny is a group homomorphism $\varphi : E_1 \to E_2$ defined by a rational map

Isogenies

- An isogeny is a group homomorphism $\varphi : E_1 \rightarrow E_2$ defined by a rational map
- $\deg \varphi := \# \ker \varphi$
- Dual isogeny $\bar{\varphi}$ is the unique isogeny such that $\varphi\bar{\varphi} = [\deg \varphi]$

Isogeny graphs

- Let p, ℓ be prime numbers, $\ell \neq p$
- Define a supersingular isogeny graph by
  - Vertices $=$ supersingular elliptic curves over $\bar{\mathbb{F}}_p$ (up to Galois conjugacy)
  - Edges $=$ ℓ-degree isogenies between them

Isogeny graphs

- Let p, ℓ be prime numbers, $\ell \neq p$
- Define a supersingular isogeny graph by
  - Vertices = supersingular elliptic curves over $\bar{\mathbb{F}}_p$ (up to Galois conjugacy)
  - Edges = ℓ-degree isogenies between them
- $(\ell + 1)$-regular undirected graph
- No multiple edges if $p = 1 \bmod 12$

Hash function

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

- **Collision resistance:**
  hard to find m, m' such that $H(m) = H(m')$
- **Preimage resistance:**
  given h, hard to find m such that $H(m) = h$
- **Second preimage resistance:**
  given m, hard to find m' such that $H(m') = h$

CGL hash function

$H : \{1, \ldots, \ell\}^* \to \{$supersingular j-invariants over $\mathbb{F}_{p^2}\}$

- Let p, ℓ be prime numbers, $\ell \neq p$, $p = 1 \bmod 12$
- For every j, define its neighbour set N_j
- For two neighbours j_{i-1}, j_i and for $m_{i+1} \in \{1, \ldots, \ell\}$, define a rule $\sigma(j_{i-1}, j_i, m_{i+1}) = j_{i+1} \in N_{j_i} \setminus \{j_{i-1}\}$
- Let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular j-invariant, and let j_{-1} be one of its neighbours
- To hash a message, start from j_{-1}, j_0, compute j_{i+1} with σ recursively, return last j-invariant

The ℓ-isogeny path problem

- **Preimage problem for CGL hash function:**
  Let E_0 and E_1 be two supersingular elliptic curves over $\mathbb{F}_{p^2}$ with $|E_0(\mathbb{F}_{p^2})| = |E_1(\mathbb{F}_{p^2})| = (p+1)^2$.
  Find $e \in \mathbb{N}$ and an isogeny of degree ℓ^e from E_0 to E_1.

The ℓ-isogeny path problem

- **Preimage problem for CGL hash function:**
  Let E_0 and E_1 be two supersingular elliptic curves over $\mathbb{F}_{p^2}$ with $|E_0(\mathbb{F}_{p^2})| = |E_1(\mathbb{F}_{p^2})| = (p+1)^2$.
  Find $e \in \mathbb{N}$ and an isogeny of degree ℓ^e from E_0 to E_1.
- **Quaternion version:**
  Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be two maximal orders in $B_{p,\infty}$.
  Find $e \in \mathbb{N}$ and a left $\mathcal{O}_0$-ideal I with norm ℓ^e, with right order isomorphic to $\mathcal{O}_1$.

Outline

A simpler problem

- Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be two maximal orders in $B_{p,\infty}$. Compute a left $\mathcal{O}_0$-ideal I (of arbitrary norm) with right order isomorphic to $\mathcal{O}_1$

A simpler problem

- Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be two maximal orders in $B_{p,\infty}$. Compute a left $\mathcal{O}_0$-ideal I (of arbitrary norm) with right order isomorphic to $\mathcal{O}_1$
- Solution:
  - Compute $\mathcal{O}_{01} := \mathcal{O}_0 \cap \mathcal{O}_1$
  - Compute $M =$ the index of $\mathcal{O}_{01}$ in $\mathcal{O}_0$
  - Compute $I = \{\alpha \in B_{p,\infty} | \alpha \mathcal{O}_1 \bar{\alpha} \subseteq M\mathcal{O}_0\}$

A simpler problem

- Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be two maximal orders in $B_{p,\infty}$. Compute a left $\mathcal{O}_0$-ideal I (of arbitrary norm) with right order isomorphic to $\mathcal{O}_1$
- Solution:
  - Compute $\mathcal{O}_{01} := \mathcal{O}_0 \cap \mathcal{O}_1$
  - Compute $M =$ the index of $\mathcal{O}_{01}$ in $\mathcal{O}_0$
  - Compute $I = \{\alpha \in B_{p,\infty} | \alpha \mathcal{O}_1 \bar{\alpha} \subseteq M\mathcal{O}_0\}$
- Finding an ideal I connecting $\mathcal{O}_0$ and $\mathcal{O}_1$ is easy; the norm condition makes the problem harder

A reformulation

- **Lemma:**
  Let I be a left $\mathcal{O}$-ideal with $\mathrm{Nrd}(I) = N$. Let $\beta \in I$.
  Then $I\bar{\beta}/N$ is a left $\mathcal{O}$-ideal of norm $\mathrm{Nrd}(\beta)/N$.

A reformulation

- **Lemma:**
  Let I be a left $\mathcal{O}$-ideal with $\mathrm{Nrd}(I) = N$. Let $\beta \in I$.
  Then $I\bar{\beta}/N$ is a left $\mathcal{O}$-ideal of norm $\mathrm{Nrd}(\beta)/N$.
- **The quaternion ℓ-isogeny problem reduces to**:
  Finding $\beta \in I$ with $\mathrm{Nrd}(\beta) = N\ell^e$ for some $e \in \mathbb{N}$

Main algorithm's overview

- Input: $\mathcal{O}_0$ and $\mathcal{O}_1$
- Output: ideal connecting them with power of ℓ norm

Main algorithm's overview

- Input: $\mathcal{O}_0$ and $\mathcal{O}_1$
- Output: ideal connecting them with power of ℓ norm

- Reduce to the case where $\mathcal{O}_0$ is special
- Compute an ideal connecting $\mathcal{O}_0$ and $\mathcal{O}_1$
- Replace it by an ideal I with prime norm N

Main algorithm's overview

- Input: $\mathcal{O}_0$ and $\mathcal{O}_1$
- Output: ideal connecting them with power of ℓ norm

- Reduce to the case where $\mathcal{O}_0$ is special
- Compute an ideal connecting $\mathcal{O}_0$ and $\mathcal{O}_1$
- Replace it by an ideal I with prime norm N
- Let $I = \mathcal{O}_0 N + \mathcal{O}_0 \alpha$. Compute $e \in \mathbb{Z}$, λ coprime to N and β such that

$$\begin{cases} \beta \equiv \lambda\alpha \bmod N\mathcal{O}_0 \\ \mathrm{Nrd}(\beta) = N\ell^e \end{cases}$$

- Return $J = I\bar{\beta}/N$

Main algorithm's overview (2)

- Satisfying $\beta \equiv \lambda\alpha \bmod N\mathcal{O}_0$ and $\mathrm{Nrd}(\beta) = N\ell^e$ seems easier when $\alpha \in Rj$

Main algorithm's overview (2)

- Satisfying $\beta \equiv \lambda\alpha \bmod N\mathcal{O}_0$ and $\mathrm{Nrd}(\beta) = N\ell^e$ seems easier when $\alpha \in Rj$ so we
  1. Compute a random $\gamma \in \mathcal{O}_0$ of reduced norm $N\ell^{e_0}$
  2. Compute $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$
  3. Compute $\lambda \in \mathbb{Z}$ and $\mu \in \mathcal{O}_0$ such that $\mu \equiv \lambda[\mu]$ and $\mathrm{Nrd}(\mu) = \ell^{e_1}$
  4. Let $\beta := \gamma\mu$

Main algorithm's overview (2)

- Satisfying $\beta \equiv \lambda\alpha \bmod N\mathcal{O}_0$ and $\mathrm{Nrd}(\beta) = N\ell^e$ seems easier when $\alpha \in Rj$ so we
  1. Compute a random $\gamma \in \mathcal{O}_0$ of reduced norm $N\ell^{e_0}$
  2. Compute $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$
  3. Compute $\lambda \in \mathbb{Z}$ and $\mu \in \mathcal{O}_0$ such that $\mu \equiv \lambda[\mu]$ and $\mathrm{Nrd}(\mu) = \ell^{e_1}$
  4. Let $\beta := \gamma\mu$
- (This part can be seen as an explicit version of the strong approximation theorem for $B_{p,\infty}$)

Outline

Focus on prime ideals

- Let $\mathcal{O}$ be an arbitrary maximal order and let I be a left $\mathcal{O}$-ideal of norm N
- We want J in the same class as I but with prime norm

Focus on prime ideals

- Let $\mathcal{O}$ be an arbitrary maximal order and let I be a left $\mathcal{O}$-ideal of norm N
- We want J in the same class as I but with prime norm
- Algorithm:
  - Compute a Minkowski basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for I
  - Generate random elements $\alpha = \sum_i x_i \alpha_i$ with $x_i \in [-m, m]$ until $\mathrm{Nrd}(\alpha)/N$ prime
  - Return $I\bar{\alpha}/N$

Focus on special orders

- Suppose we have an algorithm when $\mathcal{O}_0$ is special
- Let $\mathcal{O}_1$ another maximal order and I_{12} a $\mathcal{O}_1$-left ideal

$$\mathcal{O}_0 \qquad\qquad \mathcal{O}_1 \xrightarrow{I_{12}}$$

- Algorithm for $\mathcal{O}_1$:

Focus on special orders

- Suppose we have an algorithm when $\mathcal{O}_0$ is special
- Let $\mathcal{O}_1$ another maximal order and I_{12} a $\mathcal{O}_1$-left ideal

$$\begin{tikzcd}
\mathcal{O}_0 \arrow[r, "I_{01}"] \arrow[rr, bend left, "I_{02} = I_{01} I_{12}"] & \mathcal{O}_1 \arrow[r, "I_{12}"] & {}
\end{tikzcd}$$

- Algorithm for $\mathcal{O}_1$:
  1. Let I_{01} connecting $\mathcal{O}_0$ to $\mathcal{O}_1$ and let $I_{02} = I_{01} I_{12}$

Focus on special orders

- Suppose we have an algorithm when $\mathcal{O}_0$ is special
- Let $\mathcal{O}_1$ another maximal order and I_{12} a $\mathcal{O}_1$-left ideal

$$
\begin{tikzcd}
\mathcal{O}_0 \arrow[r, bend left=15, "I_{01}"] \arrow[r, bend right=15, "J_{01}"'] \arrow[rr, bend left=30, "I_{02} = I_{01} I_{12}"] \arrow[rr, bend right=30, "J_{02}"'] & \mathcal{O}_1 \arrow[r, "I_{12}"] & {}
\end{tikzcd}
$$

- Algorithm for $\mathcal{O}_1$:
  1. Let I_{01} connecting $\mathcal{O}_0$ to $\mathcal{O}_1$ and let $I_{02} = I_{01} I_{12}$
  2. Compute $J_{01} = I_{01}\bar{\beta}_{01}/\mathrm{Nrd}(I_{01})$ with $\mathrm{Nrd}(I_{01}) = \ell^{e_{01}}$
     Compute $J_{02} = I_{02}\bar{\beta}_{02}/\mathrm{Nrd}(I_{02})$ with $\mathrm{Nrd}(I_{02}) = \ell^{e_{02}}$

Focus on special orders

- Suppose we have an algorithm when $\mathcal{O}_0$ is special
- Let $\mathcal{O}_1$ another maximal order and I_{12} a $\mathcal{O}_1$-left ideal

$$
\begin{tikzcd}
\mathcal{O}_0 \arrow[r, bend left, "I_{01}"] \arrow[r, bend right, "J_{01}"'] \arrow[rr, bend left=40, "I_{02} = I_{01} I_{12}"] \arrow[rr, bend right=40, "J_{02}"'] & \mathcal{O}_1 \arrow[r, bend left, "I_{12}"] \arrow[r, bend right, "J_{12}"'] & {}
\end{tikzcd}
$$

- Algorithm for $\mathcal{O}_1$:
  1. Let I_{01} connecting $\mathcal{O}_0$ to $\mathcal{O}_1$ and let $I_{02} = I_{01} I_{12}$
  2. Compute $J_{01} = I_{01}\bar{\beta}_{01}/\mathrm{Nrd}(I_{01})$ with $\mathrm{Nrd}(I_{01}) = \ell^{e_{01}}$
     Compute $J_{02} = I_{02}\bar{\beta}_{02}/\mathrm{Nrd}(I_{02})$ with $\mathrm{Nrd}(I_{02}) = \ell^{e_{02}}$
  3. Let $J_{12} := I_{12}\bar{\beta}_{02}\beta_{01}/\mathrm{Nrd}(I_{02})$

Integer representation by special orders

- Let $\mathcal{O}_0$ be special and let M a large enough integer
- We want $\gamma \in R + Rj \subset \mathcal{O}_0$ with reduced norm M

$$\mathrm{Nrd}(\gamma) = f(x_1, y_1) + pf(x_2, y_2) = M$$

Integer representation by special orders

- Let $\mathcal{O}_0$ be special and let M a large enough integer
- We want $\gamma \in R + Rj \subset \mathcal{O}_0$ with reduced norm M

$$\mathrm{Nrd}(\gamma) = f(x_1, y_1) + pf(x_2, y_2) = M$$

- Choose x_2, y_2 randomly until $f(x_1, y_1) = M - pf(x_2, y_2)$ can be solved with Cornaccia's algorithm
- Note: crucial that $D = \mathrm{disc}(R)$ small for efficiency

Computing $[\mu]$

- Let $\mathcal{O}_0$ be special and let $I = \mathcal{O}_0 N + \mathcal{O}_0 \alpha$
- Let $\gamma \in \mathcal{O}_0$ with norm $N\ell^{e_0}$
- We want $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$

Computing $[\mu]$

- Let $\mathcal{O}_0$ be special and let $I = \mathcal{O}_0 N + \mathcal{O}_0\alpha$
- Let $\gamma \in \mathcal{O}_0$ with norm $N\ell^{e_0}$
- We want $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$
- The kernel of $m_\gamma : \mu \to \gamma\mu$ has dimension 2 in $B_{p,\infty}$
- Rj also has dimension 2
- Solution space of $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$ very likely to intersect Rj modulo $N\mathcal{O}_0$ for random γ

Computing $[\mu]$

- Let $\mathcal{O}_0$ be special and let $I = \mathcal{O}_0 N + \mathcal{O}_0\alpha$
- Let $\gamma \in \mathcal{O}_0$ with norm $N\ell^{e_0}$
- We want $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$
- The kernel of $m_\gamma : \mu \rightarrow \gamma\mu$ has dimension 2 in $B_{p,\infty}$
- Rj also has dimension 2
- Solution space of $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$ very likely to intersect Rj modulo $N\mathcal{O}_0$ for random γ
- Linear system of equations over $\mathbb{Z}/N\mathbb{Z}$

Lifting $[\mu]$ to an ℓ power norm element

- We have $[\mu] = (z_0 + w_0\omega)j$ and want to find $\lambda \in \mathbb{Z}$ and
$$\mu = \lambda[\mu] + N\left((x_1 + \omega y_1) + (z_1 + \omega w_1)j\right)$$
such that
$$\mathrm{Nrd}(\mu) = N^2 f(x_1, y_1) + p\, f(\lambda z_0 + N z_1, \lambda w_0 + N w_1) = \ell^e$$

Lifting $[\mu]$ to an ℓ power norm element

- We have $[\mu] = (z_0 + w_0\omega)j$ and want to find $\lambda \in \mathbb{Z}$ and
$$\mu = \lambda[\mu] + N\left((x_1 + \omega y_1) + (z_1 + \omega w_1)j\right)$$
such that
$$\mathrm{Nrd}(\mu) = N^2 f(x_1, y_1) + p\, f(\lambda z_0 + N z_1, \lambda w_0 + N w_1) = \ell^e$$

- Algorithm:
  - Get λ from $\lambda^2 f(z_0, w_0) = \ell^e \bmod N$
  - Modulo N^2, the norm equation is bilinear in z_1, w_1
  - Take random small solutions for (w_1, z_1) until $f(x_1, y_1) = \frac{\ell^e - pf(\cdot,\cdot)}{N^2}$ can be solved

Lifting $[\mu]$ to an ℓ power norm element

- We have $[\mu] = (z_0 + w_0\omega)j$ and want to find $\lambda \in \mathbb{Z}$ and
$$\mu = \lambda[\mu] + N\left((x_1 + \omega y_1) + (z_1 + \omega w_1)j\right)$$
such that
$$\mathrm{Nrd}(\mu) = N^2 f(x_1, y_1) + p\, f(\lambda z_0 + N z_1, \lambda w_0 + N w_1) = \ell^e$$
- Algorithm:
  - Get λ from $\lambda^2 f(z_0, w_0) = \ell^e \bmod N$
  - Modulo N^2, the norm equation is bilinear in z_1, w_1
  - Take random small solutions for (w_1, z_1) until $f(x_1, y_1) = \frac{\ell^e - pf(\cdot,\cdot)}{N^2}$ can be solved
- Note: crucial that $D = \mathrm{disc}(R)$ small for efficiency

Algorithm summary

- Reduce to the case where $\mathcal{O}_0$ is special
- Compute an ideal connecting $\mathcal{O}_0$ and $\mathcal{O}_1$
- Replace it by an ideal I with prime norm N
- Let $I = \mathcal{O}_0(N, \alpha)$. Compute $e \in \mathbb{Z}$, λ coprime to N, and β such that $\beta \equiv \lambda\alpha \bmod N\mathcal{O}_0$ and $\mathrm{Nrd}(\beta) = N\ell^e$
  1. Compute a random $\gamma \in \mathcal{O}_0$ of reduced norm $N\ell^{e_0}$
  2. Find $[\mu] \in Rj$ such that $\alpha \equiv \gamma[\mu] \bmod N\mathcal{O}_0$
  3. Find $\lambda \in \mathbb{Z}$ and $\mu \in \mathcal{O}_0$ such that $\mu \equiv \lambda[\mu]$ and $\mathrm{Nrd}(\mu) = \ell^{e_1}$
  4. Let $\beta := \gamma\mu$ and $e = e_0 + e_1$
- Return $J = I\bar{\beta}/N$

Heuristic analysis

- We rely on heuristic assumptions on randomness of representation of integers by quadratic forms and distribution of primes
- For special orders, we then expect polynomial time algorithm returning ideals of norm ℓ^e with

$$e \sim \frac{7}{2}\log_\ell(p)$$

  (Note that diameter $\sim 2\log_\ell p$)
- These features were verified in practice with a Magma implementation, with p up to 200 bits

Heuristic analysis

- We rely on heuristic assumptions on randomness of representation of integers by quadratic forms and distribution of primes
- For special orders, we then expect polynomial time algorithm returning ideals of norm ℓ^e with

$$e \sim \frac{7}{2}\log_\ell(p)$$

(Note that diameter $\sim 2\log_\ell p$)
- These features were verified in practice with a Magma implementation, with p up to 200 bits
- Totally breaks quaternion variant of CGL

Powersmooth ideals

- Input: $\mathcal{O}_0$ and $\mathcal{O}_1$
- Output: ideal connecting them with *powersmooth* norm

$$N = \prod_i p_i^{e_i} \qquad \text{with } p_i^{e_i} < B$$

Powersmooth ideals

- Input: $\mathcal{O}_0$ and $\mathcal{O}_1$
- Output: ideal connecting them with *powersmooth* norm

$$N = \prod_i p_i^{e_i} \qquad \text{with } p_i^{e_i} < B$$

- Can adapt previous algorithm and analysis; similar complexity

Outline

Deuring's correspondence

- Bijection from **supersingular elliptic curves** over $\bar{\mathbb{F}}_p$ (up to Galois conjugacy)
  to **maximal orders** in the quaternion algebra $B_{p,\infty}$ ramified at p and infinity (up to equivalence)

$$E \to \mathcal{O} = \mathrm{End}(E)$$

- An isogeny $\varphi : E_0 \to E_1$ is sent to the left $\mathcal{O}$-ideal $I = \mathrm{Hom}(E_1, E_0)\varphi$
- A path between two curves in the supersingular ℓ-isogeny graph is sent to an ideal of ℓ-power norm

Special supersingular invariants

- When $p = 3 \bmod 4$, the curve $E_0 : y^2 = x^3 - x$ is supersingular with invariant $j = 1728$
- Let ι such that $\iota^2 = -1$. The map $\phi : (x, y) \rightarrow (-x, \iota y)$ is an endomorphism of E_0

Special supersingular invariants

- When $p = 3 \bmod 4$, the curve $E_0 : y^2 = x^3 - x$ is supersingular with invariant $j = 1728$
- Let ι such that $\iota^2 = -1$. The map $\phi : (x, y) \to (-x, \iota y)$ is an endomorphism of E_0
- The application $\theta : B_{p,\infty} \to \mathrm{End}(E_0) \otimes \mathbb{Q}$:

$$a + bi + cj + dk \quad \to \quad 1 + b\pi + c\varphi + d\varphi\pi$$

  is an isomorphism of quaternion algebras
- We have $\mathrm{End}(E_0) \approx \mathcal{O}_0 := \langle 1, j, \frac{j+k}{2}, \frac{1+i}{2} \rangle$

Local travel in the supersingular graph

- Given a curve E and a positive integer d, we can compute the d torsion $E_0(\bar{\mathbb{F}}_p)[d]$
- Given cyclic $G \subset E_0(\bar{\mathbb{F}}_p)[d]$, we can use **Vélu's formulae** to compute an isogeny of degree d with kernel G, as well as its image E_1
- Allows to travel locally in supersingular isogeny graph (used to evaluate CGL hash function)

Special supersingular invariants (2)

- Compute a supersingular invariant over $\mathbb{F}_p$
- Under GRH we can choose $q = O(\log^2 p)$

Special supersingular invariants (2)

- Compute a supersingular invariant over $\mathbb{F}_p$
- Under GRH we can choose $q = O(\log^2 p)$
- Compute the q-torsion and its $q+1$ cyclic subgroups
- Compute all degree q isogenies using Vélu's formulae
- One is sending j_0 to itself: gives endomorphism φ

Special supersingular invariants (2)

- Compute a supersingular invariant over $\mathbb{F}_p$
- Under GRH we can choose $q = O(\log^2 p)$
- Compute the q-torsion and its $q+1$ cyclic subgroups
- Compute all degree q isogenies using Vélu's formulae
- One is sending j_0 to itself: gives endomorphism φ
- We have $\mathrm{End}(E_0) \subseteq \langle 1, \varphi, \pi, \varphi\pi \rangle$
- Deduce an isomorphism $\theta : \mathcal{O}_0 \to \mathrm{End}(E_0)$
- Identify the exact subring

Explicit Deuring's correspondence

- Input: maximal order $\mathcal{O} \subset B_{p,\infty}$
- Output: supersingular curve E with $\mathrm{End}(E) \approx \mathcal{O}$

Explicit Deuring's correspondence

- Input: maximal order $\mathcal{O} \subset B_{p,\infty}$
- Output: supersingular curve E with $\mathrm{End}(E) \approx \mathcal{O}$

- Compute a special E_0, the corresponding $\mathcal{O}_0$ and a map $\theta : \mathcal{O}_0 \to \mathrm{End}(E_0)$
- Compute an ideal I connecting $\mathcal{O}_0$ and $\mathcal{O}$
- Let $N = \mathrm{Nrd}(I)$ and let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ a $\mathbb{Z}$-basis
- Compute the corresponding isogeny φ
  - Kernel of φ is the only cyclic subgroup of $E_0[N]$ such that $(\theta(\omega_k))(G) = 0$
  - Use Vélu's formulae as above

Explicit Deuring's correspondence

- Input: maximal order $\mathcal{O} \subset B_{p,\infty}$
- Output: supersingular curve E with $\mathrm{End}(E) \approx \mathcal{O}$

- Compute a special E_0, the corresponding $\mathcal{O}_0$ and a map $\theta : \mathcal{O}_0 \to \mathrm{End}(E_0)$
- Compute an ideal I connecting $\mathcal{O}_0$ and $\mathcal{O}$
- Let $N = \mathrm{Nrd}(I)$ and let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ a $\mathbb{Z}$-basis
- Compute the corresponding isogeny φ
  - Kernel of φ is the only cyclic subgroup of $E_0[N]$ such that $(\theta(\omega_k))(G) = 0$
  - Use Vélu's formulae as above

- Problem: $G \subseteq E_0[N]$ is large

Composite isogenies

- When $N = \prod p_i^{e_i}$, we have $E_0[N] = \prod E_0[p_i^{e_i}]$ and $\ker \varphi = \prod G_i$, where G_i cyclic subgroup of $E_0[p_i^{e_i}]$

Composite isogenies

- When $N = \prod p_i^{e_i}$, we have $E_0[N] = \prod E_0[p_i^{e_i}]$ and $\ker\varphi = \prod G_i$, where G_i cyclic subgroup of $E_0[p_i^{e_i}]$
- Compute a basis $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ of I
- Initialize φ to the trivial map on E_0
- For each i:
  - Find $G_i \subset E_0[p_i^{e_i}]$ satisfying

$$(\theta(\omega_k))(G_i) = 0$$

  - Compute an isogeny φ_i with kernel $\varphi(G_i)$
  - Set $\varphi \leftarrow \varphi_i\varphi$

Composite isogenies

- When $N = \prod p_i^{e_i}$, we have $E_0[N] = \prod E_0[p_i^{e_i}]$ and $\ker \varphi = \prod G_i$, where G_i cyclic subgroup of $E_0[p_i^{e_i}]$
- Compute a basis $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ of I
- Initialize φ to the trivial map on E_0
- For each i:
  - Find $G_i \subset E_0[p_i^{e_i}]$ satisfying
$$(\theta(\omega_k))(G_i) = 0$$
  - Compute an isogeny φ_i with kernel $\varphi(G_i)$
  - Set $\varphi \leftarrow \varphi_i \varphi$
- Complexity now polynomial in $\max p_i^{e_i}$

Explicit Deuring's correspondence (2)

- Input: maximal order $\mathcal{O} \subset B_{p,\infty}$
- Output: supersingular invariant j with $End(j) \approx \mathcal{O}$

Explicit Deuring's correspondence (2)

- Input: maximal order $\mathcal{O} \subset B_{p,\infty}$
- Output: supersingular invariant j with $End(j) \approx \mathcal{O}$
- Compute a special j_0, the corresponding $\mathcal{O}_0$ and a map $\theta : \mathcal{O}_0 \to \mathrm{End}(j_0)$
- Compute an ideal I connecting $\mathcal{O}_0$ and $\mathcal{O}$
- Compute $J \approx I$ with *powersmooth* norm
- Compute the corresponding isogeny φ as above

Endomorphism ring computation

- Given a supersingular j-invariant, compute $\mathrm{End}(j)$ and a map $\theta : \mathrm{End}(j) \otimes \mathbb{Q} \to B_{p,\infty}$

Endomorphism ring computation

- Given a supersingular j-invariant, compute $\mathrm{End}(j)$ and a map $\theta : \mathrm{End}(j) \otimes \mathbb{Q} \to B_{p,\infty}$
- Explicit Deuring correspondence, in the other direction
- Kohel: $\tilde{O}(p)$ algorithm by expanding an isogeny tree
- Galbraith: $\tilde{O}(p^{1/2})$ algorithm with birthday paradox
- Still a plausible "hard problem" today

CGL attack on special initial points

- What: compute an endomorphism of E_0 of degree ℓ^e (collision attack for special parameters)

CGL attack on special initial points

- What: compute an endomorphism of E_0 of degree ℓ^e (collision attack for special parameters)
- Compute $\alpha \in \mathcal{O}_0$ of norm ℓ^e
- Deduce $I_i = \mathcal{O}_0\alpha + \mathcal{O}_0\ell^i$, $i = 1, \ldots, e$
- For each i
  - Compute $J_i \approx I_i$ with powersmooth norm
  - Compute corresponding isogeny φ_i and j-invariant j_i
- Deduce a collision path $(j_0, j_1, \ldots, j_e = j_0)$

A trapdoor collision attack

- What: compute genuine-looking parameters together with a collision trapdoor

A trapdoor collision attack

- What: compute genuine-looking parameters together with a collision trapdoor
- Choose a random path from j_0, ending at j_1
- Reveal j_1 as initial point in the graph
- Keep the path as a trapdoor
- Use collision attack on j_0
- Combine paths to produce collision on j_1

A trapdoor collision attack

- What: compute genuine-looking parameters together with a collision trapdoor

- Choose a random path from j_0, ending at j_1
- Reveal j_1 as initial point in the graph
- Keep the path as a trapdoor
- Use collision attack on j_0
- Combine paths to produce collision on j_1

- "Trapdoor one-way function" based on hardness of computing the endomorphism ring of a random supersingular elliptic curve
(except that using the trapdoor will reveal it)

Impact of attacks

- CGL explicitely prevented small cycles to occur, but existence of large cycles cannot be avoided
- To the best of our knowledge, the only way to generate a random j is to start from j_0 and do a random walk as above

Outline

Conclusion

- Total break of "quaternion CGL"
  Can travel in the graph in polynomial time
- Partial break of original CGL hash function
  - Collision attack on special parameters
  - Trapdoor collision attack
- Explicit Deuring correspondence in one direction:
  Given $\mathcal{O}$, can compute corresponding j in polytime

Future work and open problems

- Remove heuristic approximations in analysis
- Extend approach to other norm equations (quaternions and beyond)

Future work and open problems

- Remove heuristic approximations in analysis
- Extend approach to other norm equations (quaternions and beyond)
- Explicit Deuring correspondence in the other direction: Given E, compute its endomorphism ring
- Security of De Feo-Jao-Plût schemes

Thanks!

Looking forward to your questions / comments!