Elliptic Curve Isogeny Based Cryptosystems

Frederik Vercauteren

Open Security Research (China)

KU Leuven ESAT/COSIC (Belgium)

frederik.vercauteren@gmail.com

23 August 2016

Post-quantum cryptography

- Shor's algorithm: breaks RSA, DLP, ECDLP in polytime on quantum computer
- Post-quantum cryptographic systems:
  - Code-based crypto: McEliece, ...
  - Lattice based crypto: NTRU, LWE, ...
  - Hash-based crypto: Merkle hash tree signatures, ...
  - Multivariate crypto: Hidden Field Equations, ...
- What about isogeny based crypto ?

Isogeny based crypto: history

- Diffie-Hellman key agreement:
  - 1997: Couveignes: Talk at ENS about ”Hard Homogeneous Spaces”
  - 2006: Rostovtsev, Stolbunov: ordinary isogeny Diffie-Hellman
  - 2010: Weiwei, Debiao: key agreement protocols
  - 2011: de Feo, Jao, Plût: supersingular isogeny Diffie-Hellman
  - 2016: Costello, Longa, Naehrig: efficient implementation of SIDH

Isogeny based crypto: history

- Diffie-Hellman key agreement:
  - 1997: Couveignes: Talk at ENS about ”Hard Homogeneous Spaces”
  - 2006: Rostovtsev, Stolbunov: ordinary isogeny Diffie-Hellman
  - 2010: Weiwei, Debiao: key agreement protocols
  - 2011: de Feo, Jao, Plût: supersingular isogeny Diffie-Hellman
  - 2016: Costello, Longa, Naehrig: efficient implementation of SIDH
- Other cryptographic constructions:
  - 2003: Teske: elliptic curve trapdoor system
  - 2004: Rostovtsev, Makhovenko, Shemyakina: ordered digital signature scheme
  - 2009: Charles, Lauter, Goren: hash function based on isogeny graph
  - 2010-2011: Debiao, Jianhua and Jin: random number generator and key agreement
  - 2014: Sun, Tian, Wang: strong designated verifier signature
  - 2014: Jao, Soukharev: undeniable signatures

Idea 1: Diffie-Hellman from abelian group action

- Let G be a finite abelian group and X a set with a group action $\star$

$$G \times X \to X : (g, x) \mapsto g \star x$$

- Recall $(gh) \star x = g \star (h \star x)$ and $e \star x = x$
- Key agreement:

$$\begin{array}{ccc}
\textbf{Alice} & & \textbf{Bob} \\
a \in_R G & & b \in_R G \\
\alpha = a \star x & & \beta = b \star x \\
& \xrightarrow{\alpha} & \\
& \xleftarrow{\beta} & \\
k = a \star \beta = (ab) \star x & & k = b \star \alpha = (ba) \star x
\end{array}$$

Idea 1: instantiation

- Couveignes (1997), Rostovtsev, Stolbunov (2006)
- Set X consists of j-invariants of elliptic curves $E/\mathbb{F}_q$ with $End(E) \simeq \mathcal{O}_K$, ring of integers of quadratic imaginary field
- Group G is class group $cl(\mathcal{O}_K)$
- Ideal $\mathfrak{a}$ in $\mathcal{O}_K$ defines a subgroup $E[\mathfrak{a}]$ and isogeny

$$\varphi_{\mathfrak{a}} : E \to E' = E/E[\mathfrak{a}]$$

- Action: $[\mathfrak{a}] \star j(E) = j(E')$

Elliptic curves

- Elliptic curve E over field k with $char(k) > 3$ can be defined by

$$y^2 = x^3 + ax + b \quad a, b \in k, \qquad 4a^3 + 27b^2 \neq 0$$

- For any field extension k'/k, $E(k')$ set of k'-rational points forms an abelian group with $\mathbb{O}$ as identity element

Elliptic curves

- Elliptic curve E over field k with $char(k) > 3$ can be defined by

$$y^2 = x^3 + ax + b \quad a, b \in k, \qquad 4a^3 + 27b^2 \neq 0$$

- For any field extension k'/k, $E(k')$ set of k'-rational points forms an abelian group with $\mathbb{O}$ as identity element
- The j-invariant $j(E) = j(a, b) = 1728\frac{4a^3}{4a^3+27b^2}$ determines isomorphism class over $\overline{k}$
- Given $j_0 \in k$, easy to write down curve with j-invariant equal to j_0
  - $j(0, b) = 0$ and $j(a, 0) = 1728$
  - General case: $a = -3c$ and $b = 2c$ with $c = j_0/(j_0 - 1728)$

Torsion subgroups

- Multiplication by n map: $[n] : E \to E : P \mapsto nP$
- n-torsion subgroup is kernel of $[n]$

$$E[n] = \{P \in E(\bar{k}) : nP = \mathbb{O}\}$$

- If $char(k) \nmid n$, then structure of $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
- If $char(k) = p$, then either:
  - Supersingular: $E[p^e] = \{\mathbb{O}\}$ or
  - Ordinary: $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$

Isogenies

- An **isogeny** $\varphi : E_1 \to E_2$ is a morphism (rational map) that preserves identity
- The degree of an isogeny is its degree as rational map
- If isogeny is separable, then $\deg(\varphi) = \# \ker(\varphi)$
- For isogeny $\varphi : E_1 \to E_2$ of degree n we have **dual isogeny** $\hat{\varphi} : E_2 \to E_1$ with

$$\hat{\varphi} \circ \varphi = [n]_{E_1} \text{ and } \varphi \circ \hat{\varphi} = [n]_{E_2}$$

Isogenies

- An **isogeny** $\varphi : E_1 \to E_2$ is a morphism (rational map) that preserves identity
- The degree of an isogeny is its degree as rational map
- If isogeny is separable, then $\deg(\varphi) = \# \ker(\varphi)$
- For isogeny $\varphi : E_1 \to E_2$ of degree n we have **dual isogeny** $\hat{\varphi} : E_2 \to E_1$ with

$$\hat{\varphi} \circ \varphi = [n]_{E_1} \text{ and } \varphi \circ \hat{\varphi} = [n]_{E_2}$$

Theorem

- For every finite subgroup $H \subset E_1(\overline{k})$, there exists elliptic curve E_2 and separable isogeny $\varphi : E_1 \to E_2$ with $\ker \varphi = H$

- **Vélu's formulae**: compute curve E_2 and isogeny φ given H

ℓ-Isogenies and modular polynomial

- Let $\ell \neq char(k)$ be prime, then isogeny of degree ℓ has cyclic kernel of order ℓ
- Recall: $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, so there are $\ell + 1$ cyclic subgroups
- Each subgroup is kernel of isogeny
- Isogeny is defined over k iff its kernel is Galois invariant under $Gal(k(E[\ell])/k)$
- So there are: 0, 1, 2 or $\ell + 1$, k-rational isogenies

ℓ-Isogenies and modular polynomial

- Let $\ell \neq char(k)$ be prime, then isogeny of degree ℓ has cyclic kernel of order ℓ
- Recall: $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, so there are $\ell + 1$ cyclic subgroups
- Each subgroup is kernel of isogeny
- Isogeny is defined over k iff its kernel is Galois invariant under $Gal(k(E[\ell])/k)$
- So there are: 0, 1, 2 or $\ell + 1$, k-rational isogenies
- **Modular polynomial**: $\Phi_\ell(X, Y)$
  - Symmetric in X, Y and of degree $\ell + 1$
  - Two elliptic curves E_1, E_2 are ℓ-isogenous iff $\Phi_\ell(j(E_1), j(E_2)) = 0$

ℓ-Isogenies and modular polynomial

- Let $\ell \neq char(k)$ be prime, then isogeny of degree ℓ has cyclic kernel of order ℓ
- Recall: $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, so there are $\ell + 1$ cyclic subgroups
- Each subgroup is kernel of isogeny
- Isogeny is defined over k iff its kernel is Galois invariant under $Gal(k(E[\ell])/k)$
- So there are: 0, 1, 2 or $\ell + 1$, k-rational isogenies
- **Modular polynomial**: $\Phi_\ell(X, Y)$
  - Symmetric in X, Y and of degree $\ell + 1$
  - Two elliptic curves E_1, E_2 are ℓ-isogenous iff $\Phi_\ell(j(E_1), j(E_2)) = 0$
- **Elkies algorithm**: isogeny and its kernel given $j(E_1)$ and $j(E_2)$

Endomorphism ring

- Endomorphism is an isogeny from E to itself
- The set of endomorphisms $End(E)$ forms a ring

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \qquad (\varphi\psi)(P) = \varphi(\psi(P))$$

Endomorphism ring

- Endomorphism is an isogeny from E to itself
- The set of endomorphisms $End(E)$ forms a ring

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \qquad (\varphi\psi)(P) = \varphi(\psi(P))$$

Theorem

$End(E)$ of a curve E/k can be:

1. $End(E) \simeq \mathbb{Z}$
2. $End(E) \simeq$ an order $\mathcal{O}$ in imaginary quadratic extension of $\mathbb{Q}$
3. $End(E) \simeq$ an order $\mathcal{O}$ in quaternion algebra over $\mathbb{Q}$

- If $End(E)$ is strictly larger than $\mathbb{Z}$, then E is said to have **complex multiplication**
- Case 3 occurs if and only if E is supersingular (see later)

Endomorphism rings of isogenous curves

- The endomorphism algebra $End^0(E) = End(E) \otimes \mathbb{Q}$
- $End^0(E)$ is isogeny invariant:
  - so if E_1 is supersingular then also E_2
- In general $End(E_1) \neq End(E_2)$, but for ℓ-isogenies we have
  - $End(E_1) = End(E_2)$ (horizontal)
  - $End(E_1)$ has index ℓ in $End(E_2)$ (ascending)
  - $End(E_2)$ has index ℓ in $End(E_1)$ (descending)

Frobenius endomorphism

- Let E be elliptic curve over finite field $k = \mathbb{F}_q$
- The Frobenius endomorphism

$$\pi_E : E \to E : (x, y) \mapsto (x^q, y^q)$$

Theorem

The characteristic equation of π_E is given by

$$X^2 - tX + q = 0\,, \quad |\, t \,| \leq 2\sqrt{q}$$

and $\#E(\mathbb{F}_q) = q + 1 - t$

- $\Delta = t^2 - 4q \leq 0$, so $\mathbb{Q}(\pi_E)$ is imag quad field K for $|t| \neq 2\sqrt{q}$

Ordinary curves over finite fields

- Curve $E/\mathbb{F}_q$ is ordinary iff $E[p] \neq \{\mathbb{O}\}$ with $p = char(\mathbb{F}_q)$
- $End(E)$ is order in imaginary quadratic field $K = \mathbb{Q}(\pi_E)$

$$\mathbb{Z}[\pi_E] \subset End(E) \subset \mathcal{O}_K$$

- Write $\Delta = t^2 - 4q = f^2 D_K$ with D_K fundamental discriminant of K

$$f = [\mathcal{O}_K : \mathbb{Z}[\pi_E]]$$

- Vertical isogenies can only occur for $\ell \mid f$
- So if Δ is squarefree then $End(E) = \mathbb{Z}[\pi_E] = \mathcal{O}_K$, and only horizontal isogenies exist

Horizontal isogenies and class group

- **For simplicity assume:** $End(E) = \mathbb{Z}[\pi_E] = \mathcal{O}_K$
- For an ideal $\mathfrak{a} \in \mathcal{O}_K$ define the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] = \{P \in E(\overline{k}) : \alpha(P) = \mathbb{O} \text{ for all } \alpha \in \mathfrak{a}\}$$

Horizontal isogenies and class group

- **For simplicity assume:** $End(E) = \mathbb{Z}[\pi_E] = \mathcal{O}_K$
- For an ideal $\mathfrak{a} \in \mathcal{O}_K$ define the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] = \{P \in E(\overline{k}) : \alpha(P) = \mathbb{O} \text{ for all } \alpha \in \mathfrak{a}\}$$

Properties

- $E[\mathfrak{a}]$ is kernel of separable horizontal isogeny $\phi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} = E/E[\mathfrak{a}]$
- If $char(k) \nmid N(\mathfrak{a})$, then $\deg(\phi_{\mathfrak{a}}) = N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$
- For two ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$ we have: $\phi_{\mathfrak{a}\mathfrak{b}} = \phi_{\mathfrak{a}}\phi_{\mathfrak{b}}$
- For principal ideal $\mathfrak{a}$ we have $E \simeq E_{\mathfrak{a}}$

Horizontal isogenies and class group

- Define $Ell_{\mathcal{O}_K}(k) = \{j(E) : E/k \text{ with } End(E) \simeq \mathcal{O}_K\}$
- Then class group $cl(\mathcal{O}_K)$ acts on $Ell_{\mathcal{O}_K}$ where $[\mathfrak{a}] \star j(E) = j(E_{\mathfrak{a}})$
- The action of $cl(\mathcal{O}_K)$ on $Ell_{\mathcal{O}_K}$ is simply transitive
- Conclusion: $\#Ell_{\mathcal{O}_K}(k) = \#h(\mathcal{O}_K)$ (or $Ell_{\mathcal{O}_K}(k)$ is empty)

Horizontal isogenies and class group

- Define $Ell_{\mathcal{O}_K}(k) = \{j(E) : E/k \text{ with } End(E) \simeq \mathcal{O}_K\}$
- Then class group $cl(\mathcal{O}_K)$ acts on $Ell_{\mathcal{O}_K}$ where $[\mathfrak{a}] \star j(E) = j(E_\mathfrak{a})$
- The action of $cl(\mathcal{O}_K)$ on $Ell_{\mathcal{O}_K}$ is simply transitive
- Conclusion: $\#Ell_{\mathcal{O}_K}(k) = \#h(\mathcal{O}_K)$ (or $Ell_{\mathcal{O}_K}(k)$ is empty)

- For prime $\ell \neq char(k)$, require ideal of norm ℓ in $\mathcal{O}_K = \mathbb{Z}[\pi_E]$
  - If ℓ splits, then $\ell\mathcal{O}_K = \mathfrak{l}\mathfrak{m}$, two horizontal isogenies $\mathfrak{l}$ and $\mathfrak{m}$
  - If ℓ ramifies, then $\ell\mathcal{O}_K = \mathfrak{l}^2$ so one horizontal isogeny $\mathfrak{l}$
  - If ℓ is inert, no horizontal isogenies
  - Ideals are of the form $\mathfrak{l} = \langle \ell, \pi_E - \lambda \rangle$, so kernel is λ-eigenspace of Frobenius in $E[\ell]$

Example

- Let $p = 241$ and consider $E/\mathbb{F}_p : y^2 = x^3 + x + 3$, $j(E) = 188$
- Then $\#E(\mathbb{F}_p) = 231$ and $t = 11$
- $\Delta = t^2 - 4p = -843$ which is squarefree
- Define $K = \mathbb{Q}(\pi_E) = \mathbb{Q}[x]/(x^2 - tx + p)$, then $\mathcal{O}_K = \mathbb{Z}[\pi_E]$

Example

- Let $p = 241$ and consider $E/\mathbb{F}_p : y^2 = x^3 + x + 3$, $j(E) = 188$
- Then $\#E(\mathbb{F}_p) = 231$ and $t = 11$
- $\Delta = t^2 - 4p = -843$ which is squarefree
- Define $K = \mathbb{Q}(\pi_E) = \mathbb{Q}[x]/(x^2 - tx + p)$, then $\mathcal{O}_K = \mathbb{Z}[\pi_E]$
- Class group $cl(\mathcal{O}_K)$ is cyclic of order 6
- Generator can be taken: $[g] = [\langle 11, \pi_E - 1\rangle]$
- Small representatives:

$$
\begin{array}{ll}
[g] : \langle 11, \pi_E - 1\rangle & [g^4] : \langle 7, \pi_E - 1\rangle \\
[g^2] : \langle 7, \pi_E - 3\rangle & [g^5] : \langle 11, \pi_E - 10\rangle \\
[g^3] : \langle 3, \pi_E - 1\rangle & [g^6] : \langle 1\rangle
\end{array}
$$

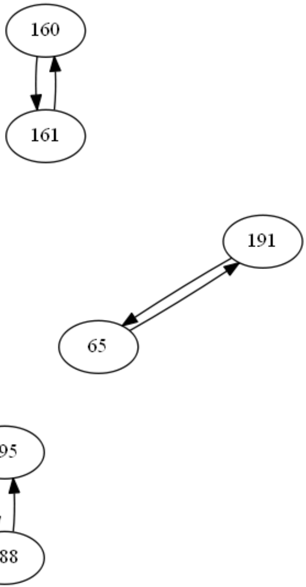
Example

- j-invariants having same endomorphism ring

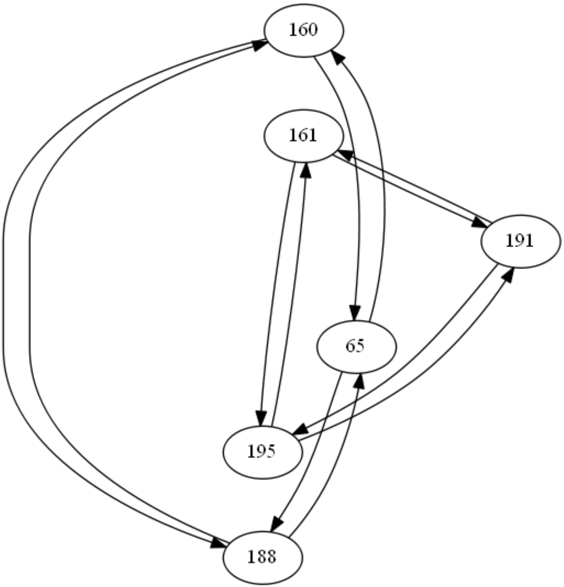
$$\{160, 161, 188, 195, 65, 191\}$$

- For primes $\ell \in \{2, 3, 5, 7, 11\}$:
  - No horizontal isogenies of degree 2 and 5
  - For $\ell = 3$, precisely one horizontal isogeny per j-invariant
  - For $\ell = 7, 11$, precisely two horizontal isogenies per j-invariant

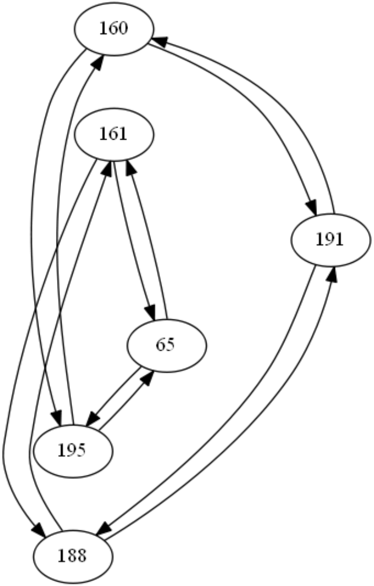
Isogeny graph on $Ell_{\mathcal{O}_K}(k)$ $\ell = 3$



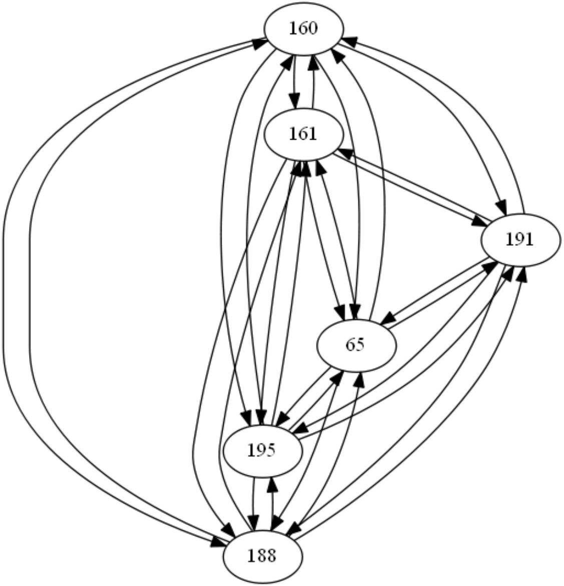
Isogeny graph on $Ell_{\mathcal{O}_K}(k)$ $\ell = 7$



Isogeny graph on $Ell_{\mathcal{O}_K}(k)$ $\ell = 11$



Isogeny graph on $Ell_{\mathcal{O}_K}(k)$ $\ell = 3, 5, 11$



Computing class action

- System setup: curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ points
- $\Delta = t^2 - 4q$ squarefree so $End(E) = \mathbb{Z}[\pi_E]$ with $\pi_E^2 - t\pi_E + q = 0$
- If $f(x) = x^2 - tx + q$ has two roots λ, μ modulo ℓ, then $\ell\mathcal{O}_K = \mathfrak{m}\mathfrak{l}$ with $\mathfrak{m} = \langle \ell, \pi_E - \lambda \rangle$ and $\mathfrak{l} = \langle \ell, \pi_E - \mu \rangle$

Computing class action

- System setup: curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ points
- $\Delta = t^2 - 4q$ squarefree so $End(E) = \mathbb{Z}[\pi_E]$ with $\pi_E^2 - t\pi_E + q = 0$
- If $f(x) = x^2 - tx + q$ has two roots λ, μ modulo ℓ, then $\ell\mathcal{O}_K = \mathfrak{m}\mathfrak{l}$ with $\mathfrak{m} = \langle \ell, \pi_E - \lambda \rangle$ and $\mathfrak{l} = \langle \ell, \pi_E - \mu \rangle$
- Given j-invariant $j(E)$ and ideal $\mathfrak{l} = \langle \ell, \pi_E - \lambda \rangle$ in $\mathcal{O}_K$ of norm ℓ
  - Compute possible j-invariants j_1, j_2 as roots of $\Phi_\ell(x, j(E)) = 0$
  - For j_1 use Elkies' algorithm to compute curve E' with $j(E') = j_1$ and kernel H of isogeny
  - If H eigenspace corresponding to λ, then correct
  - Otherwise select j_2

Sampling elements in $cl(\mathcal{O}_K)$

- Do not want to compute $h(\mathcal{O}_K)$ nor the structure of $cl(\mathcal{O}_K)$
- Under GRH there exists constant c_0 such that degree one ideals of norm smaller than $\ell_{\max} = c_o \log^2 \mid \Delta \mid$ generate $cl(\mathcal{O}_K)$

$$L = \{\mathfrak{l}_i \text{ degree one } \quad N(\mathfrak{l}_i) = \ell_i \text{ and } \quad \ell_i \leq \ell_{\max}\}$$

- To select a "random" element, select exponents e_i for $i = 1, \ldots, \#L$ and set

$$\mathfrak{a} = \prod_{i=1}^{\#L} \mathfrak{l}_i^{e_i}$$

- Box containing exponents should have volume $\gg h(\mathcal{O}_K)$
- Very slow: Stolbunov for 428-bit prime p requires 230s

Ordinary isogeny computation: hardness

- Given two ordinary elliptic curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ with $End(E_1) = End(E_2)$
- **Classical computers**: algorithm of Galbraith, Hess, Smart (optimized by Stolbunov) computes isogeny in time $\tilde{O}(q^{1/4+o(1)})$
- **Quantum computers**: Childs, Jao, Soukharev algorithm runs in time

$$L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$$

Ordinary isogeny computation: hardness

- Given two ordinary elliptic curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ with $End(E_1) = End(E_2)$
- **Classical computers**: algorithm of Galbraith, Hess, Smart (optimized by Stolbunov) computes isogeny in time $\tilde{O}(q^{1/4+o(1)})$
- **Quantum computers**: Childs, Jao, Soukharev algorithm runs in time

$$L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$$

Abelian hidden shift problem

- Let A be a finite abelian group and $f_0 : A \to R$ an injective function
- Let $f_1 : A \to R$ be defined by $f_1(x) = f_0(xs)$ for some unknown s
- Problem: find s
- Isogeny setting: $f_0([\mathfrak{a}]) = [\mathfrak{a}] \star E_1$ and $f_1([\mathfrak{a}]) = [\mathfrak{a}] \star E_2$
- We know that for some secret $[\mathfrak{s}]$ we have $E_2 = [\mathfrak{s}] \star E_1$

Supersingular curves

- E over $\mathbb{F}_q$ with $q = p^n$ is **supersingular** iff $E[p] = \{\mathbb{O}\}$
- $End(E)$ isomorphic to an order in a quaternion algebra
- All supersingular curves can be defined over $\mathbb{F}_{p^2}$
- Let S_{p^2} be the set of all supersingular j-invariants in $\mathbb{F}_{p^2}$

Theorem

$$\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \bmod 12 \\ 1 & \text{if } p \equiv 5, 7 \bmod 12 \\ 2 & \text{if } p \equiv 11 \bmod 12 \end{cases}$$

Supersingular isogeny graph

- $E[\ell] \simeq (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell)$, so subgroup H_i of order ℓ gives isogeny

$$\psi_i : E \to E_i \simeq E/H_i$$

- Isogenous curve E_i is supersingular so has j-invariant in S_{p^2}
- Immediately leads to $\ell + 1$ directed regular graph $X(S_{p^2}, \ell)$

Theorem

The graph $X(S_{p^2}, \ell)$ is connected.

Supersingular isogeny graph

- $E[\ell] \simeq (\mathbb{Z}/\ell) \times (\mathbb{Z}/\ell)$, so subgroup H_i of order ℓ gives isogeny

$$\psi_i : E \to E_i \simeq E/H_i$$

- Isogenous curve E_i is supersingular so has j-invariant in S_{p^2}
- Immediately leads to $\ell + 1$ directed regular graph $X(S_{p^2}, \ell)$

Theorem

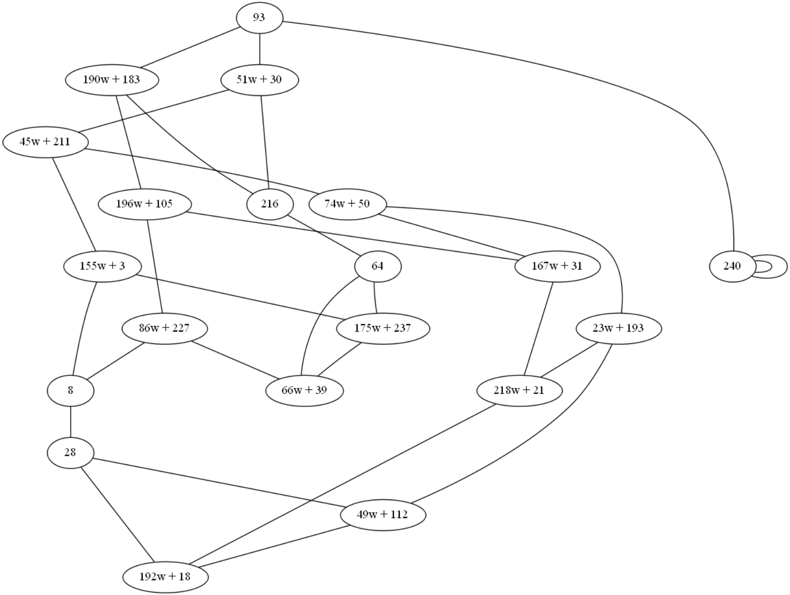
The graph $X(S_{p^2}, \ell)$ is connected.

- Edges (j_1, j_2) not incident to 0 or 1728 have same multiplicity as (j_2, j_1)
- Obtain undirected graph $X(S'_{p^2}, \ell)$ with $S'_{p^2} = S_{p^2} \setminus \{0, 1728\}$
- For $p \equiv 1 \bmod 12$, we have $S'_{p^2} = S_{p^2}$

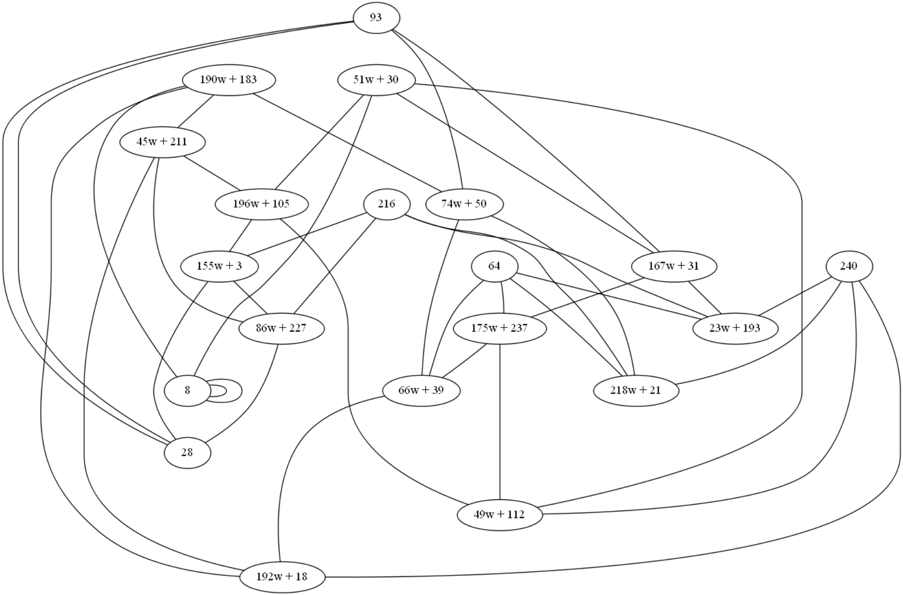
Supersingular isogeny graph: example

- Let $p = 241$, then $\#S_{p^2} = 20$
- $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 + 238x + 7)$
- $S_{p^2} = \{93, 51w + 30, 190w + 183, 240, 216, 45w + 211, 196w + 105, 64, 155w + 3, 74w + 50, 86w + 227, 167w + 31, 175w + 237, 66w + 39, 8, 23w + 193, 218w + 21, 28, 49w + 112, 192w + 18\}$

Supersingular isogeny graph $\ell = 2$



Supersingular isogeny graph $\ell = 3$



Expander graphs

- An undirected graph $G = (V, E)$ is an **expander graph** with expansion constant $c > 0$, if for any subset $U \subset V$ and $|U| \leq |V|/2$, its boundary $\Gamma(U)$ has size $|\Gamma(U)| \geq c|U|$.
- An expander graph is connected.
- Diameter of G is maximal distance between any two vertices in a graph.
- For expander graph:

$$Diam(G) \leq \frac{2\log(|V|)}{\log(1 + c)}$$

Theorem

For $p \equiv 1 \bmod 12$, the graph $X(S_{p^2}, \ell)$ is a Ramanujan graph, i.e. an expander graph with "optimal" expansion factor.

Idea 2: a commutative diagram

- de Feo, Jao, Plût derive Diffie-Hellman type key agreement on S_{p^2}
- Basic idea: commutative diagram

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\psi"'] & E/\langle P \rangle \arrow[d] \\ E/\langle Q \rangle \arrow[r] & E/\langle P, Q \rangle \end{tikzcd}$$

Idea 2: a commutative diagram

- de Feo, Jao, Plût derive Diffie-Hellman type key agreement on S_{p^2}
- Basic idea: commutative diagram

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\psi"'] & E/\langle P\rangle \arrow[d] \\ E/\langle Q\rangle \arrow[r] & E/\langle P, Q\rangle \end{tikzcd}$$

- Common key will be j-invariant of curve $E/\langle P, Q\rangle$
- P and Q should be kept secret
  - Should also be impossible to derive from E and $E/\langle P\rangle$ and $E/\langle Q\rangle$
- Need to know $\phi(Q)$ to be able to compute $E/\langle P\rangle$
  - But at the same time $\phi(Q)$ should be secret ...

SIDH: de Feo, Jao, Plût

- Take prime $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ and supersingular curve E over $\mathbb{F}_p$ with
$$\#E(\mathbb{F}_{p^2}) = (p \mp 1)^2 = (\ell_A^{e_A} \ell_B^{e_B} \cdot f)^2$$
- With $E[\ell_A^{e_A}]$ rational over $\mathbb{F}_{p^2}$ (similarly for ℓ_B)
- Contains $\ell_A^{e_A} + \ell_A^{e_A - 1}$ cyclic subgroups of order $\ell_A^{e_A}$
- Any point P of order $\ell_A^{e_A}$ defines path of length e_A in $X(S_{p^2}, \ell_A)$ starting from $j(E)$

SIDH: de Feo, Jao, Plût

- Let $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ be public bases of $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$

Alice		**Bob**
$m_A, n_A \in_R \mathbb{Z}/\ell_A^{e_A}$		$m_B, n_B \in_R \mathbb{Z}/\ell_B^{e_B}$
$P = m_A P_A + n_A Q_A$		$Q = m_B P_B + n_B Q_B$
$\phi_A : E \to E_A = E/\langle P \rangle$		$\phi_B : E \to E_B = E/\langle Q \rangle$
	$E_A, \phi_A(P_B), \phi_A(Q_B)$ $\longrightarrow$	
	$E_B, \phi_B(P_A), \phi_B(Q_A)$ $\longleftarrow$	
$\phi_B(P) =$		$\phi_A(Q) =$
$m_A\phi_B(P_A) + n_A\phi_B(Q_A)$		$m_B\phi_A(P_B) + n_B\phi_A(Q_B)$
$E_{AB} = E_B/\langle \phi_B(P) \rangle$		$E_{BA} = E_A/\langle \phi_A(Q) \rangle$

Computing power ℓ isogenies

- Let P be a point of order ℓ^e, and isogeny $\phi : E \to E/\langle P \rangle$
- Decompose ϕ as $\phi_{e-1} \circ \phi_{e-2} \circ \cdots \circ \phi_0$ with $E_0 = E$ and $P_0 = P$

$$\phi_i : E_i \to E_{i+1} \quad E_{i+1} = E_i / \langle \ell^{e-i-1} P_i \rangle \quad P_{i+1} = \phi_i(P_i)$$

- **Multipilication based strategy**:
  - compute $\ell^{e-i-1} P_i$, then ϕ_i and then P_{i+1}
- **Isogeny based strategy**:
  - compute all powers once $Q_i = \ell^i P$, compute ϕ_0 and apply ϕ_0 to all Q_i for $0 \leq i \leq (e-2)$ and repeat for $\phi_1, \ldots, \phi_{e-1}$
- de Feo, Jao, Plût: optimal strategy that uses a mix of both

SIDH implementation

- Costello, Longa, Naehrig: curve $y^2 = x^3 + x$ over field $\mathbb{F}_p$ with $p = 2^{372}3^{239} - 1$
- Security: classical 192 bits, post-quantum 128 bits
- Large number of optimizations in curve model, base points, isogeny computation
- Full key agreement in 10^8 cycles (roughly 30 per second on PC)

Supersingular isogeny computation: hardness

Classical computers

- Given two supersingular elliptic curves E_1 and E_2 over $\mathbb{F}_{p^2}$, can compute isogeny in time $\tilde{O}(p^{1/4})$
- But: problem is much less general, since degree is known $\ell_A^{e_A}$ and $< \sqrt{p}$, so both curves are not that far apart in isogeny graph
- Claw problem: given two functions $f : A \to C$ and $g : B \to C$ find pair (a, b) with $f(a) = g(b)$
- Let A (resp. B) be subgroups of order $\ell_A^{e_A/2}$ on E_1 (resp. on E_2) and f and g maps induced by isogeny
- Again $O(p^{1/4})$ attack

Supersingular isogeny computation: hardness

Quantum computers

- Claw problem can be solved in time $O(p^{1/6})$
- Abelian hidden shift problem?
  - de Feo, Jao, Plût argue this does not apply since $End(E)$ is not abelian
  - Do we need full $End(E)$?
  - Is there a natural group action in this case?

Supersingular isogeny computation: hardness

Quantum computers

- Claw problem can be solved in time $O(p^{1/6})$
- Abelian hidden shift problem?
  - de Feo, Jao, Plût argue this does not apply since $End(E)$ is not abelian
  - Do we need full $End(E)$?
  - Is there a natural group action in this case?

$$\boxed{\text{Can people in this room do better?}}$$