Isogeny graphs, computational problems, and applications to cryptography

Steven Galbraith

University of Auckland, New Zealand

Plan

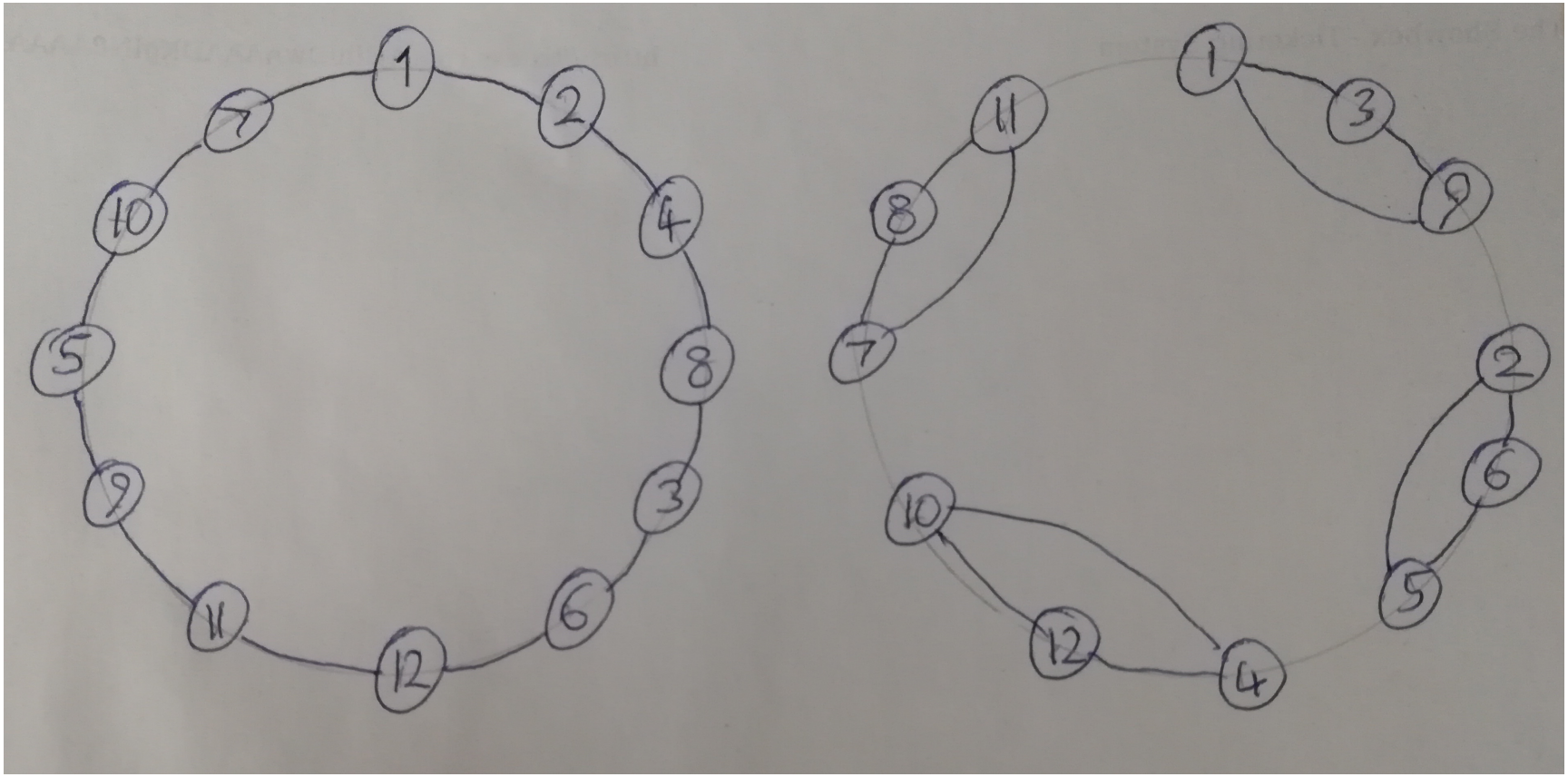
- Cayley graphs, expanders and walks
- Isogenies and isogeny graphs
- Class group action and volcanoes
- Classical and quantum algorithms for isogeny problems
- Isogeny key exchange and computational problems
- Structures in the supersingular isogeny graph
- CSIDH
- (if time) SeaSign signatures

Please interrupt to ask questions any time.

Cayley graphs

- Let G be a finite group and $S \subseteq G$.
- The *Cayley graph* $\Gamma(G, S)$ has vertex set G and edge set $\{(g, gs) : g \in G, s \in S\}$.
- Typically S is closed under inversion, so the graph is undirected.
- Example: Let $G = \mathbb{Z}_p^*$ with $p > 7$ and $S = \{2, 2^{-1} \pmod p\}$. The edges include $(1, 2), (2, 1), (2, 4), (4, 2), (3, 6), (6, 3), \ldots$

$p = 13$, $S = \{2, 2^{-1}\}$; $S = \{3, 3^{-1}\}$



Schreier graphs

- Let G be a finite group acting on a finite set X via a map $G \times X \to X$ written as $(g, x) \mapsto g(x)$, such that for $g, h \in G$ we have $g(h(x)) = (gh)(x)$.
- In this talk all groups will be Abelian.
- Let $S \subseteq G$.
- The *Schreier graph* $\Gamma(G, S)$ has vertex set X and edge set $\{(x, s(x)) : x \in X, s \in S\}$.
- A Cayley graph is the Schreier graph of G acting on itself.

Expander graphs and walks

- Kristin's talk will have discussed expander graph families.
- We are interested in graphs that can be represented in space logarithmic in the number of vertices.
- Let G be an expander graph. End points of random walks of length polynomial in $\#G$ are (close to) uniformly distributed.
- Cayley graphs $\Gamma(G, S)$ of Abelian groups with fixed degree $\#S$ are not expander families.
- But if $\#S$ grows with $\log(\#G)$ then one can still plausibly get close to uniform distribution from random walks of polynomial length.

Computational Problem

- In a large expander graph, given an initial vertex v_0 and a long enough "random walk" that ends with a random vertex v it may be hard to determine a path from v_0 to v.
- Let p be a large prime and $\ell_1, \ldots, \ell_k$ the first k primes.
- Let $B \in \mathbb{N}$ be such that $(2B+1)^k \approx p$ and $(k \log(k))^{kB/2} \gg p$.
- Given $u \equiv \prod_{i=1}^{k} \ell_i^{e_i} \pmod{p}$ where $e_i \in \mathbb{Z}$ with $|e_i| \leq B$ for all i, it is hard in general to determine $(e_1, \ldots, e_k)$.
- Special case $k = 1$ and $B = (p-1)/2$: Discrete logarithm problem.
  This is not very interesting since the walk has exponential length.
- If discrete logs are easy and k is large enough then this problem may still be hard, as we explain on the next slide.

Lattices

- Let p be a large prime and $\ell_1, \ldots, \ell_k$ the first k primes.
- Define the lattice

$$L = \{(x_1, \ldots, x_k) \in \mathbb{Z}^k : \prod_{i=1}^{k} \ell_i^{x_i} \equiv 1 \pmod{p}\}.$$

- Let $u = \prod_{i=1}^{k} \ell_i^{e_i} \pmod{p}$ where $e_i \in \mathbb{Z}$ with $|e_i| \leq B$ for all i.
- Choose random $y_2, \ldots, y_k \in \mathbb{Z} \cap [-B, B]$ and solve discrete logarithm problem (repeat if there is no solution)

$$\ell_1^{y_1} \equiv u \prod_{i=2}^{k} \ell_i^{-y_i} \pmod{p}$$

- Then $\mathbf{x} = (y_1 - e_1, \ldots, y_k - e_k) \in L$, and if $\mathbf{e} = (e_1, \ldots, e_k)$ is short then $\mathbf{x} \approx \mathbf{y} = (y_1, \ldots, y_k)$.
- Hence if we can compute a lattice point $\mathbf{x}$ that is close to $\mathbf{y}$ then $\mathbf{y} - \mathbf{x}$ is a candidate solution $\mathbf{e}$.

Lattices

- Note that the close vector problem is believed to be hard in general.
- For more applications of lattices of this type see:
  Léo Ducas and Cécile Pierrot, "Polynomial time bounded distance decoding near Minkowski's bound in discrete logarithm lattices", Designs, Codes Cryptography, 2019.

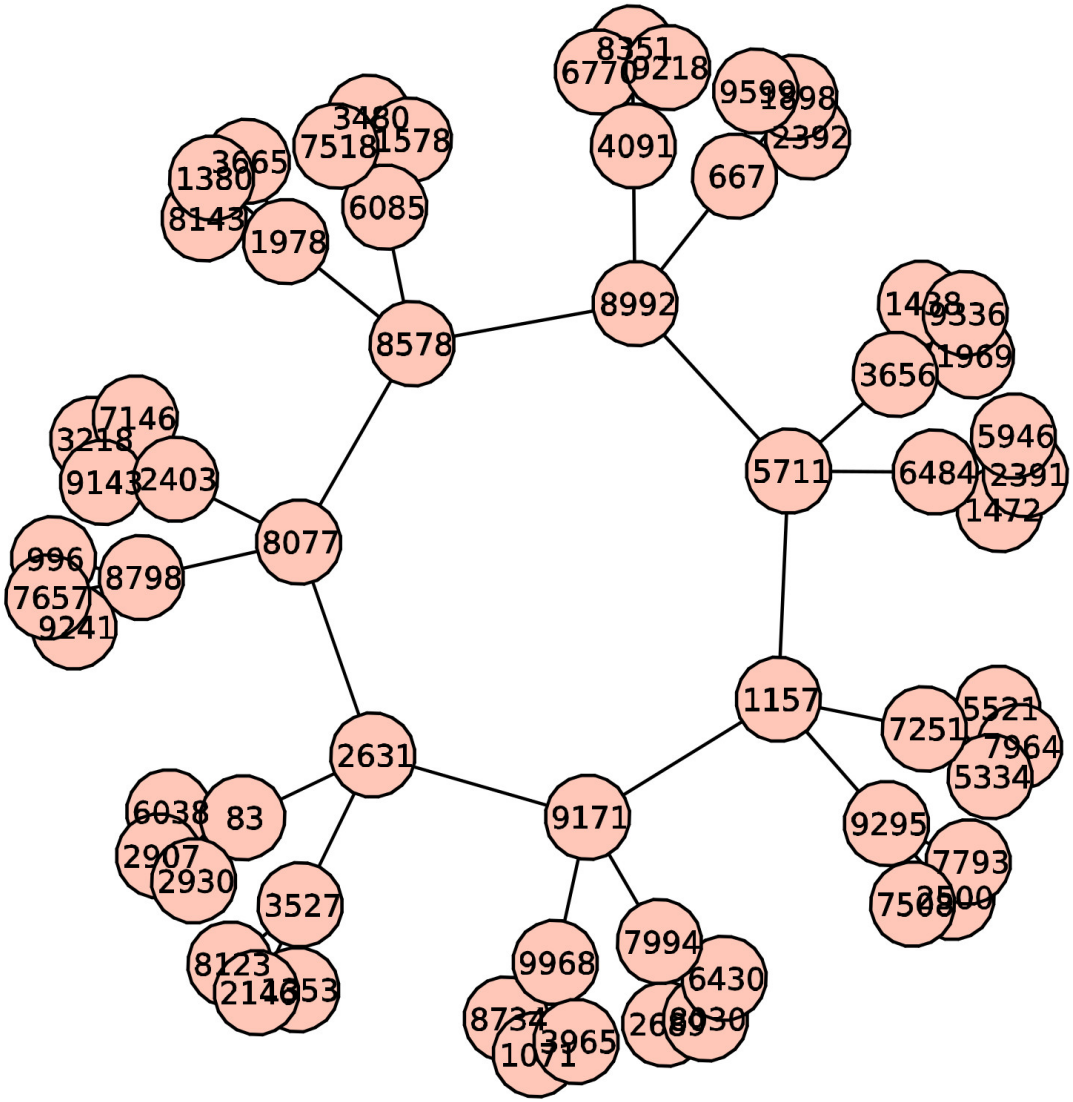
Isogenies

- An **isogeny** $\phi : E_1 \to E_2$ of elliptic curves is a (non-constant) morphism and a group homomorphism.
- An isogeny has finite kernel.
- Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}}_q)$ there is a (unique separable) isogeny $\phi_G : E_1 \to E_2$ with kernel G.
  Can compute ϕ_G using Vélu's formulae.
- We will sometimes write $E_2 = E_1/G$.
- We focus on separable isogenies, in which case $\deg(\phi) = \#\ker(\phi)$.
- For every $\phi : E_1 \to E_2$ there is a *dual isogeny* $\hat{\phi} : E_2 \to E_1$.
- $\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \overline{\mathbb{F}}_q\} \cup \{0\}$.

Isogeny Graph

- Fix q a prime power, E_0 over $\mathbb{F}_q$, and a set of primes $S = \{\ell_i\}$.
- Let $V = \{j(E) : \text{elliptic curves } E/\mathbb{F}_q \text{ such that there is an isogeny } E_0 \to E \text{ over } \mathbb{F}_q\}$.
- This vertex set is the set of $\bar{\mathbb{F}}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ isogenous to E_0.
- Let $E = \{(j(E), j(E')) : \text{there is an isogeny } \phi : E \to E' \text{ with } \deg(\phi) \in S\}$.
- (V, E) is a directed graph.
  I sometimes denote it $X(E_0, \mathbb{F}_q, S)$. Or $X(\mathbb{F}_q, S)$ if E_0 is clear.
- Because of the dual isogeny we can essentially assume the graph is undirected.

Isogeny Graphs



Credit: Dustin Moody

Ordinary

- $\#E(\mathbb{F}_q) = q + 1 - t$, $\gcd(q, t) = 1$
- $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\sqrt{t^2 - 4q})$
- Isogeny graph is essentially Cayley/Schreier graph of ideal class group, so "regular"

Supersingular

- $\#E(\mathbb{F}_q) = q + 1 - t$, $\gcd(q, t) \neq 1$
- $j(E) \in \mathbb{F}_{p^2}$
- $\mathrm{End}(E)$ is a maximal order in a quaternion algebra over $\mathbb{Q}$
- Isogeny graph an expander, so not a principal homog space for any abelian group action

Class Group Action on Elliptic Curves

- Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}$ an order in an imaginary quadratic field.
- Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal.
- Define the subgroup

$$E[\mathfrak{a}] = \{P \in E(\overline{\mathbb{F}}_q) : \phi(P) = 0 \ \forall \phi \in \mathfrak{a}\}.$$

  (Waterhouse 1969)
- There is an isogeny $E \to E'$ with kernel $E[\mathfrak{a}]$. Define $\mathfrak{a} * E$ to be $E' = E/E[\mathfrak{a}]$.
- $\mathfrak{a} * E$ depends only on the ideal class of $\mathfrak{a}$.
- This gives an action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set of E with $\mathrm{End}(E) \cong \mathcal{O}$.

Class Group Action on Elliptic Curves

- Fix an order $\mathcal{O}$ in an imaginary quadratic field.
- Let X be the set of isomorphism classes of ordinary elliptic curves over $\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}$.
- Let G be the group of classes of invertible $\mathcal{O}$-ideals.
- We have an action of G on X, as

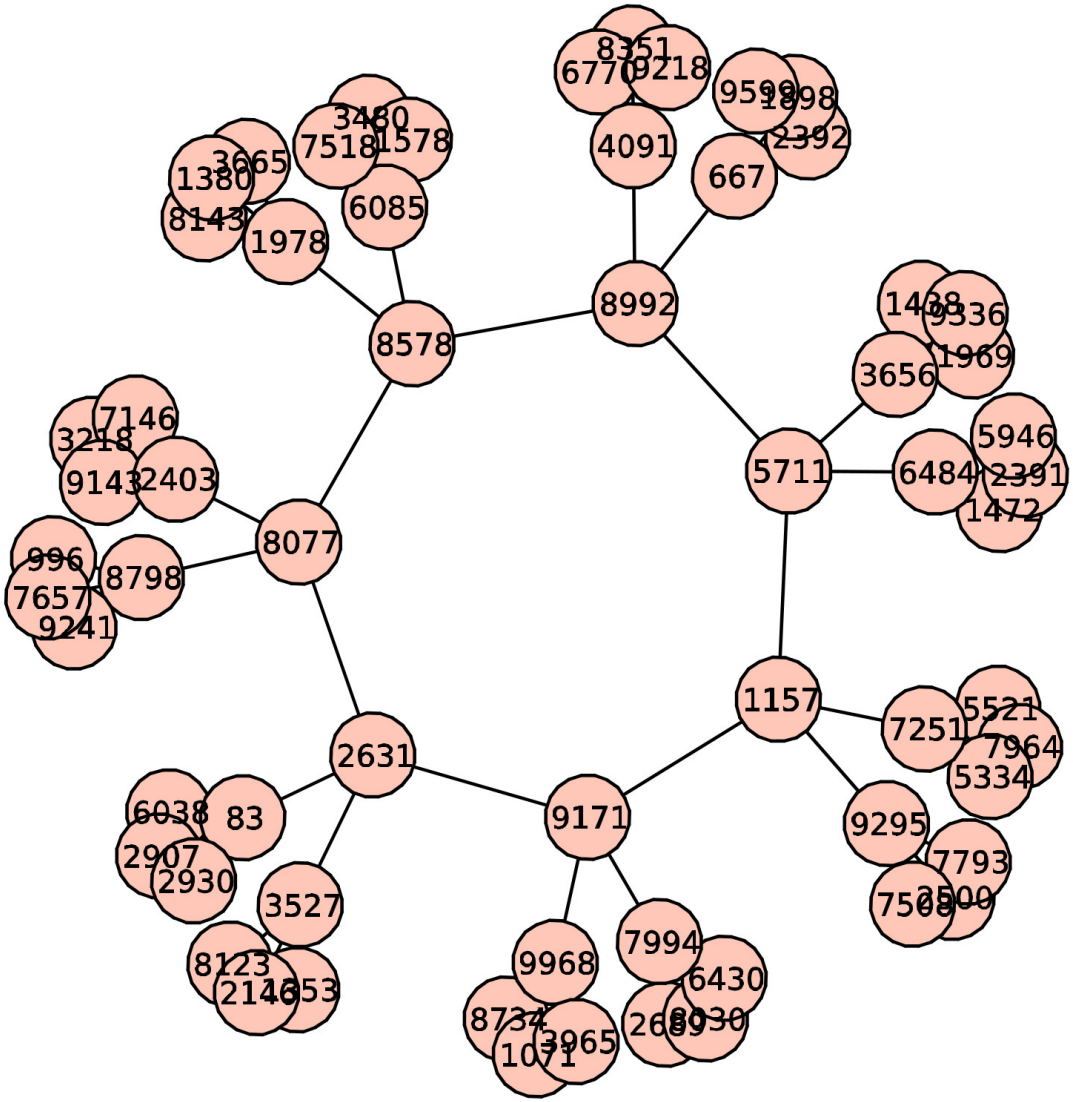
$$([\mathfrak{a}], E) \mapsto \mathfrak{a} * E.$$

- Let S be a set of invertible $\mathcal{O}$-ideals.
- Then we have a corresponding Schreier graph $\Gamma(G, S)$.

Class group action: Volcanoes (Kohel, Fouquet-Morain)

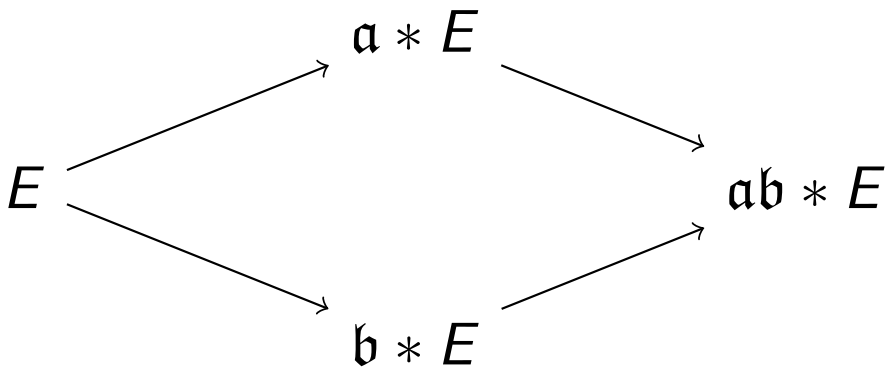
- Let E be an ordinary elliptic curve over $\mathbb{F}_q$.
- The Frobenius map is $\pi(x, y) = (x^q, y^q)$.
- We have $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ and $\#E(\mathbb{F}_q) = q + 1 - t$.
- Each subring $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ arises as $\mathrm{End}(E)$ for some elliptic curve(s).
- If $\mathrm{End}(E_1) = \mathcal{O}_1$ and $\mathrm{End}(E_2) = \mathcal{O}_2$ with $\mathcal{O}_1 \subseteq \mathcal{O}_2$ then any isogeny $\phi : E_1 \to E_2$ has degree divisible by $[\mathcal{O}_2 : \mathcal{O}_1]$.
- Isogenies that change the endomorphism ring do not correspond to invertible ideals.

Ordinary Isogeny Graph ($\ell = 3$)



Credit: Dustin Moody

Generalised Diffie-Hellman using Group Action (Brassard-Yung, Couveignes, Rostovtsev-Stolbunov)



Computational problems and algorithms

- Given E and $E' = \mathfrak{a} * E$ to determine the ideal (class) $\mathfrak{a}$.
- Equivalently: Find any efficiently computable isogeny $\phi : E \to E'$.
- Classical algorithms due to Galbraith and Galbraith-Hess-Smart in time $\tilde{O}(\sqrt{\#G})$ (bug fixed by Stolbunov).
- **Hidden shift problem:** G an abelian group and $f, g : G \to S$ such that, for some $s \in G$, $g(x) = f(xs)$ for all $x \in G$. Problem: find s.
- Idea (Childs-Jao-Soukharev): Given $(E, E' = \mathfrak{a} * E)$ define $f(\mathfrak{b}) = \mathfrak{b} * E$ and $g(\mathfrak{b}) = \mathfrak{b} * E' = f(\mathfrak{b}\mathfrak{a})$.

Quantum algorithms for hidden shift

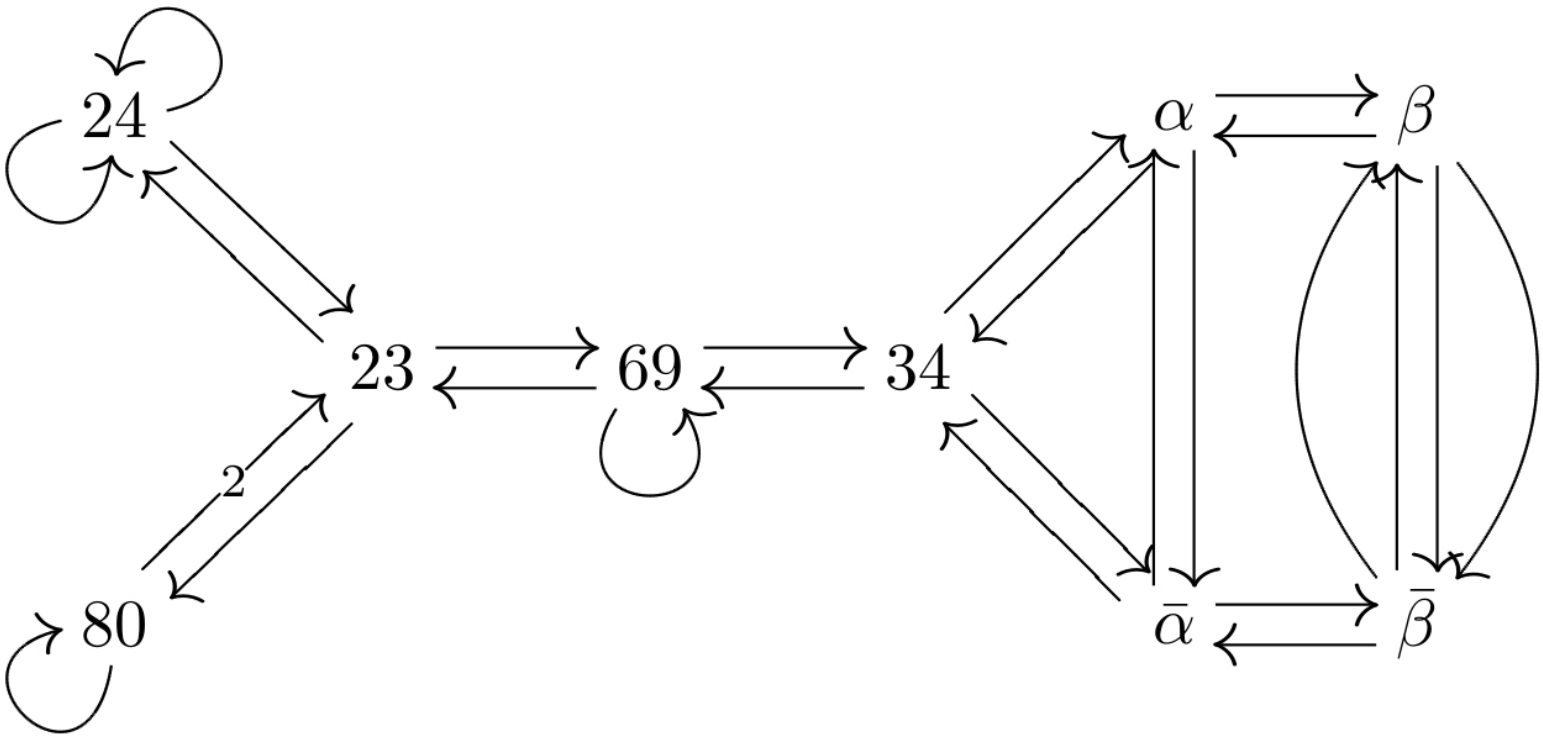
- Kuperberg (2004, 2011) gave subexponential-time quantum algorithms for hidden shift.
  Assume cost $O(1)$ for the functions f and g.
  (i.e., the unit of time is cost to compute $\mathfrak{a} * E$)
  Complexity is $2^{O(\sqrt{\log(\#G)})}$
- For certain groups Kuperberg states the time complexity is $\tilde{O}(2^{1.8\sqrt{\log(\#G)}})$.
- Requires massive quantum storage, which may be unrealistic.
- Regev (2004) gave low quantum storage variant.
- In the isogeny setting, further refinements due to Peikert, Bonnetain-Schrottenloher, etc.
  Plus work on the quantum circuit for $\mathfrak{a} * E$ by Bernstein-Lange-Martindale-Panny etc.

Challenges

- Class group action on ordinary curves does not seem to give an efficient and practical key exchange system.
- Supersingular isogeny graphs have practical applications.
- Natural to try to use supersingular curves for the class group action.

Supersingular Isogeny Graph

FIGURE 9. Supersingular Isogeny Graph $X(\bar{\mathbb{F}}_{103}, 2)$



From: C. Delfs and S. D. Galbraith, "Computing isogenies between supersingular elliptic curves over F_p", Des., Codes and Crypto., 2016.

Supersingular Curves over $\mathbb{F}_p$

- There are $p/12 + \epsilon$ supersingular elliptic curves in characteristic p.
- There are $N = O(\sqrt{p}\log(p))$ supersingular elliptic curves E with $j(E) \in \mathbb{F}_p$.
- Let $E/\mathbb{F}_p$ be supersingular. Then $\#E(\mathbb{F}_p) = p + 1$ and the Frobenius map $\pi(x, y) = (x^p, y^p)$ satisfies $\pi^2 = [-p]$.
- Hence $\mathrm{End}(E)$ is an order in a quaternion algebra, and $\sqrt{-p} \in \mathrm{End}(E)$.
- Let $K = \mathbb{Q}(\sqrt{-p})$.
- One can show that $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E) = \mathrm{End}(E) \cap K$ is an order in K such that $\sqrt{-p} \in \mathcal{O}$.
- So $\mathcal{O}$ is either $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[(1 + \sqrt{-p})/2]$.
- For each case, the number of such elliptic curves is given by the ideal class number of the order.

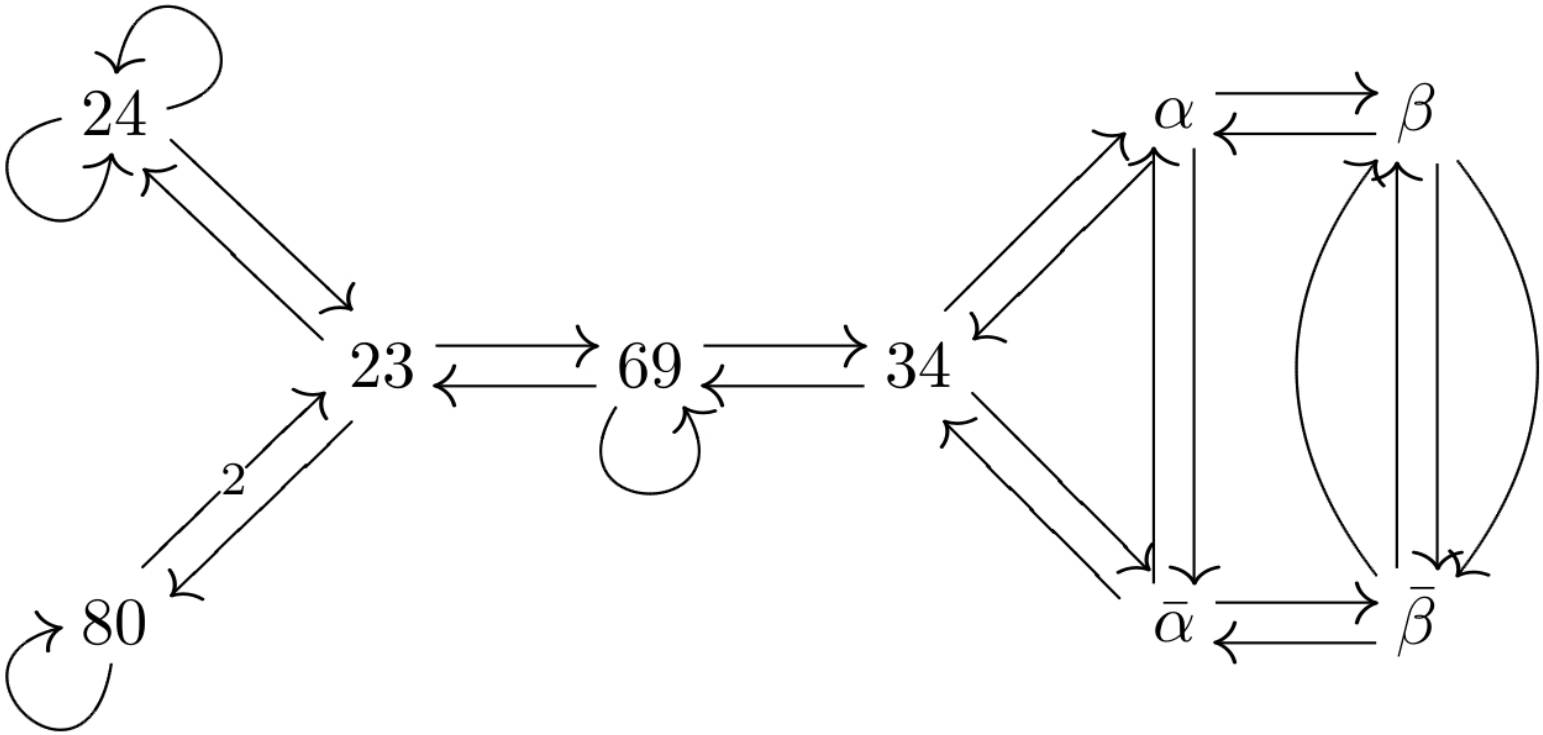
Structures in the supersingular isogeny graph

C. Delfs and S. Galbraith, "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$", Des., Codes and Crypto., 2016.

- Consider the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves with $j(E) \in \mathbb{F}_p$, and the graph $X(\mathbb{F}_p, S)$ for a suitable set of primes S.
- The size of the graph is $N = O(\sqrt{p}\log(p))$.
- The ideal class group of $\mathbb{Q}(\sqrt{-p})$ acts on this graph.
- The basic idea is that, since $\mathrm{End}_{\mathbb{F}_p}(E)$ is an order in $\mathbb{Q}(\sqrt{-p})$, we rediscover the ordinary case within the supersingular graph.

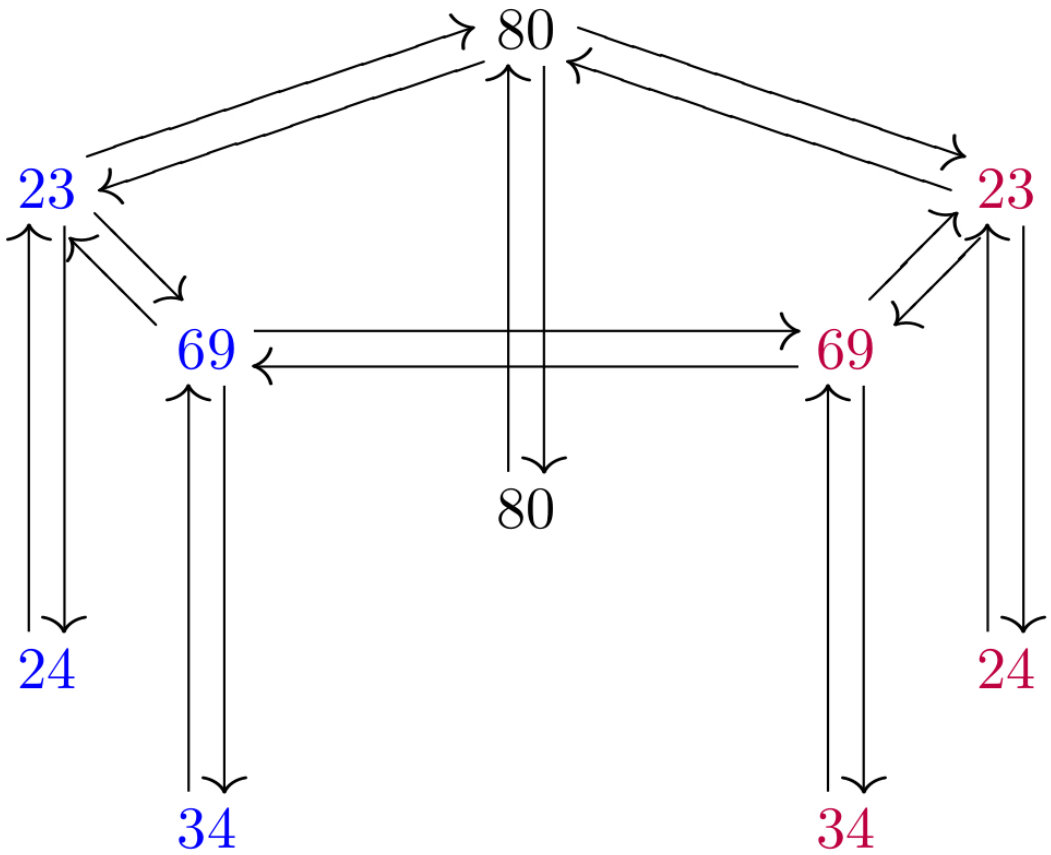
Supersingular Isogeny Graphs

FIGURE 9. Supersingular Isogeny Graph $X(\bar{\mathbb{F}}_{103}, 2)$



Supersingular Isogeny Graphs

FIGURE 10. Rational Supersingular Isogeny Graph $X(\mathbb{F}_{103}, 2)$



Supersingular Isogeny Graphs

FIGURE 9. Supersingular Isogeny Graph $X(\bar{\mathbb{F}}_{103}, 2)$

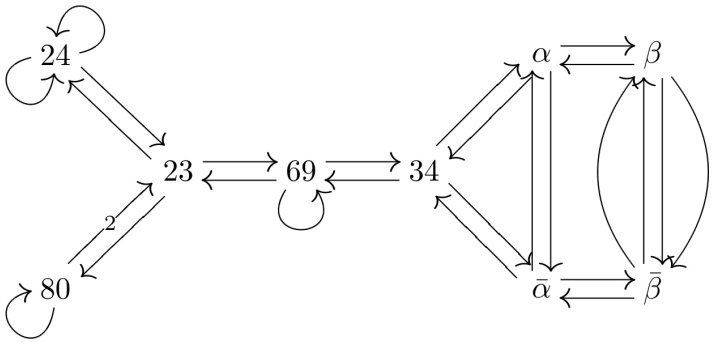
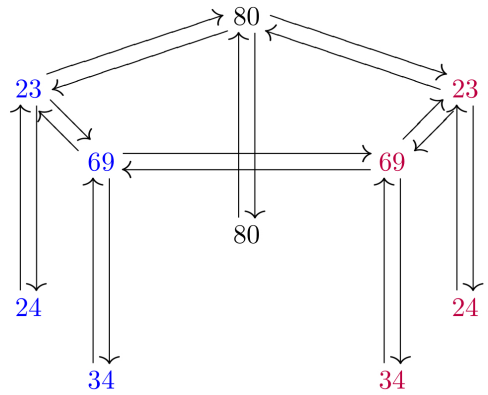


FIGURE 10. Rational Supersingular Isogeny Graph $X(\mathbb{F}_{103}, 2)$



Several special situations in ℓ-isogeny graph

- $p \equiv 1 \pmod 4$ so $\mathbb{Z}[\sqrt{-p}]$ is maximal.
  - (ℓ) splits in $\mathbb{Q}(\sqrt{-p})$ as $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$:
    Isogeny graph is a collection of cycles (of size the order of $\mathfrak{l}_1$ in the ideal class group).
  - (ℓ) is inert: isolated vertices.
    This case does not arise when $\ell = 2$.
  - Note: $\ell \neq p$ so (ℓ) is never ramified in $\mathbb{Q}(\sqrt{-p})$.
- $p \equiv 3 \pmod 4$ so $\mathbb{Z}[(1+\sqrt{-p})/2]$ is maximal.
  - $(\ell) = (2)$ splits in $\mathbb{Q}(\sqrt{-p})$ as $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$:
    Coffee table(s) with legs.
  - $(\ell) = (2)$ is inert in $\mathbb{Q}(\sqrt{-p})$: "stars".

CSIDH (Castryck, Lange, Martindale, Panny, Renes 2018)

- Let $p = 4\ell_1 \cdots \ell_k - 1$.
- Let X be the set of isomorphism classes of supersingular elliptic curves E with j-invariant in $\mathbb{F}_p$.
- All $E \in X$ have $\mathrm{End}_{\mathbb{F}_p}(E)$ an order in $\mathbb{Q}(\sqrt{-p})$.
  Here $\mathrm{End}_{\mathbb{F}_p}(E) = \{\phi : E \to E \text{ defined over } \mathbb{F}_p\}$.
- CSIDH is an instantiation of group action crypto using supersingular curves, which gives massive performance improvements over ordinary case.
- Features:
  - No public key validation needed, so unlike SIDH can do non-interactive key exchange.
  - Better bandwidth than SIDH.
  - Only sub-exponentially quantum secure.
  - Not broken by recent attacks on SIDH.

Other cool stuff

- Wouter Castryck, Jana Sotáková and Frederik Vercauteren, "Breaking the Decisional Diffie-Hellman Problem for Class Group Actions Using Genus Theory", CRYPTO 2020.
- Wouter Castryck, Marc Houben, Frederik Vercauteren and Benjamin Wesolowski, "On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves", 2022.
- Steven Galbraith, Lorenz Panny, Benjamin Smith and Frederik Vercauteren, "Quantum Equivalence of the DLP and CDHP for Group Actions", Mathematical Cryptology (2021). Given a perfect algorithm $A(\mathfrak{a} * E, \mathfrak{b} * E) = (\mathfrak{a}\mathfrak{b}) * E$ and a CSIDH instance $(E, \mathfrak{a} * E)$ we show how to use Shor's algorithm to compute $[\mathfrak{a}]$.
- Hart Montgomery and Mark Zhandry, "Full Quantum Equivalence of Group Action DLog and CDH, and More", Asiacrypt 2022.

Open problems

- How close to uniform is the distribution

$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$

  over uniform $e_i \in [-B, B]$, for fixed small prime ideals $\mathfrak{l}_i$? (Let's assume $\{\mathfrak{l}_i\}$ generates the class group.)
- Can small prime factors of $\#\mathrm{Cl}(\mathcal{O})$ be determined? Can subgroups of ideal class group be exploited?
- (Boneh): Find other homogeneous spaces/torsors for group actions that are efficient and secure for crypto.

Public Key Signatures

- L. De Feo and S. Galbraith "SeaSign: Compact isogeny signatures from class group actions", EUROCRYPT 2019.
- Public key: E and $E_A = \mathfrak{a} * E$ where

$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$

  and $\mathfrak{l}_i$ ideals of small prime norm, $|e_i| \leq B$.
- Signer generates random ideals $\mathfrak{b}_k = \prod_{i=1}^n \mathfrak{l}_i^{f_{k,i}}$ for $1 \leq k \leq t$ and computes $\mathcal{E}_k = \mathfrak{b}_k * E$.
- Compute $H(j(\mathcal{E}_1), \ldots, j(\mathcal{E}_t), \text{message})$ where H is a cryptographic hash function with t-bit output $b_1, \ldots, b_t$.
- If $b_k = 0$ signature includes $\mathsf{f}_k = (f_{k,1}, \ldots, f_{k,n})$ and if $b_k = 1$ it includes

$$\mathsf{f}_k - \mathsf{e} = (f_{k,1} - e_1, \ldots, f_{k,n} - e_n).$$

- Use relation lattice or "Fiat-Shamir with aborts".

Thank You