Algorithms and Reductions for Isogeny Problems

Kirsten Eisentraeger
Penn State
And
Simons Institute

Fields Institute
Workshop
April 20, 2022

Post-quantum Cryptography

Goal: develop public-key cryptographic algorithms that are secure against quantum computers.

Bad choices:

RSA

(Traditional) Elliptic Curve Cryptography (ECC)

Good choices: ??? - Lattice-based systems (LWE, Ring-LWE)

- McEliece

- Isogeny-based systems

This talk: Isogeny based cryptography as a candidate for post-quantum crypto

- Give different equivalent problems that these systems are based on.

- Discuss progress with quantum algorithms on these problems.

Elliptic Curves and Cryptography

Traditional Elliptic Curve Cryptography (ECC).

 - Proposed in 1985 (independently) by Neal Koblitz and Victor Miller, widely used since 2004.

 - Based on hardness of discrete log problem on elliptic curves.

 - Broken by Shor's quantum algorithm for discrete log ('94).

Object: elliptic curve defined over finite field.

Points on E are solutions (x, y) of equation

Finite field with q elements

$$E: \quad y^2 = x^3 + ax + b \qquad a, b \in \mathbb{F}_q$$

Points of E, together with "∞", form an **abelian group**.

Traditional Elliptic Curve Cryptography versus Isogenies

Traditional elliptic curve cryptography (ECC):

   - Fix one curve and use the group law.

   - Assume discrete log is hard on this group.

   - Get small key sizes.

  Shor's quantum algorithm breaks these.

New proposal(s): Isogeny-based systems

  Use an exponentially large set of elliptic curves and the **isogenies** (maps) between them.

Use terminology supersingular elliptic curves to make statements correct.

Why Supersingular isogeny crypto?

- Pool of potential post-quantum candidates is very small. Need to investigate all candidates.

- Elliptic curves: used in crypto for more than 20 years. So we have a lot of experience with them, infrastructure in place.

- Some underlying computational assumptions (e.g. the endomorphism ring problem) have been studied classically already.

Concerns

- Systems have not been sufficiently scrutinized by researchers in quantum algorithms.

- Compared to lattice-based crypto, there are fewer functionalities. Have encryption, key exchange, signatures, but no fully homomorphic encryption or ID based crypto.

Hardness Assumptions in Public-Key Cryptography

System	underlying hard? problem
RSA	Factoring
Elliptic curve cryptography (ECC)	Elliptic curve discrete log
(Ring) LWE	SVP in (ideal) lattices
Supersingular isogeny-based cryptography (SIDH,…)	Computing isogenies between curves
Commutative isogeny-based cryptography (CSIDH)	Inversion of class group action
Soliloquy	Short generator PIP

This talk

Isogeny-based systems

Hash function

    CGL: Charles-Goren-Lauter (2006)

Public-key cryptosystems

CRS: Couveignes, Rostovstev and Stolbunov
(ordinary elliptic curves) (2006)
Optimization (DKS'18)

Noncommu-
tative

Group action

Supersingular Isogeny Diffie-Hellman (SIDH)
key exchange, Jao and de Feo (2011)

CSIDH: Commutative SIDH (2018)
Castryck, Lange, Martindale, Panny, Renes
Generalizations (CD20, BKV19, CS21)

OSIDH ("O" for Oriented)
Colò-Kohel (2019), Onuki (2021)

Status of security of Isogeny-based Crypto

Much less studied than lattice-based systems. Need more research to develop confidence in security, both classically and against quantum computers!

- Need to study objects and hardness assumptions more.
- Can phrase hardness assumptions in different ways (graphs, group actions,…)
- For some objects, have no canonical "small" representatives

Some Progress:

- Can show that objects (isogenies, endomorphisms, maximal orders…) have polynomial representation size. Have to choose right description/representation. (E./Hallgren/Lauter/Morrison/Petit '18)
- Can give reductions between different hardness assumptions in different systems. (E./Hallgren/Lauter/Morrison/Petit '18, Wesolowski 21)

Computational Challenges

Analyze objects through the (supersingular) ℓ-**isogeny graph** (next slide)

- SIDH key exchange uses full s.s. ℓ-isogeny graph
- For schemes with group actions: fewer vertices, but still exponential size graph
- Key property used: full graph is expander graph

Curves are of form $E: \quad y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{p^2}$, so have small representation size.

But: - Maps between them (isogenies) are generally defined over large extension fields.
        - Can result in exponential size objects.

The isogenies used in cryptosystems have exponential size.
- Need to decompose into composition of ones with smaller size.
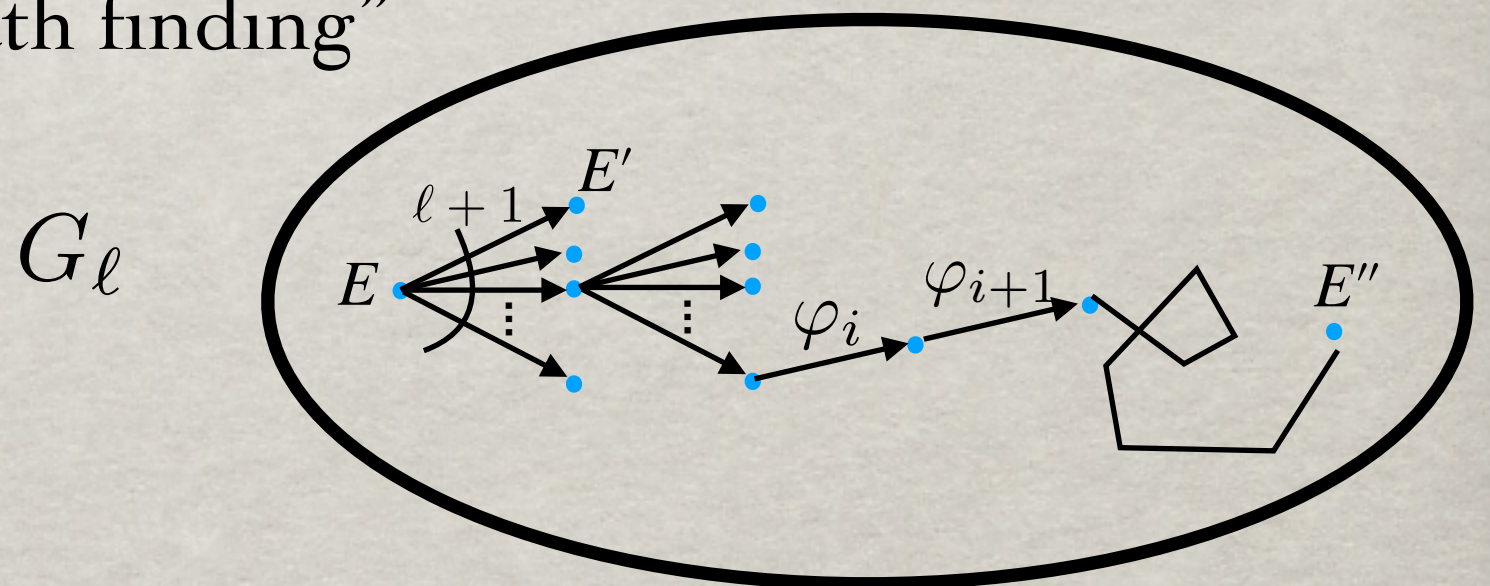
Path Finding in Supersingular Isogeny Graphs G_ℓ

Choose a small prime $\ell \neq p$ $\quad$ ($p = \mathrm{char}(\mathbb{F}_q)$ is fixed)

Graph G_ℓ is exponentially large, $p/12$ vertices.

G_ℓ is an expander.

Given a vertex, can efficiently compute neighbors.

"finding isogenies" a.k.a. "path finding"

G_ℓ

Def: $G_\ell = (V, E_\ell)$

$V := \{$ supersingular elliptic curves in char p (up to isomorphism)$\}$

$E_\ell := \{(E, E') : \exists \, \varphi : E \to E' \text{ of degree } \ell\}$ $\qquad$ ℓ = size of kernel of φ
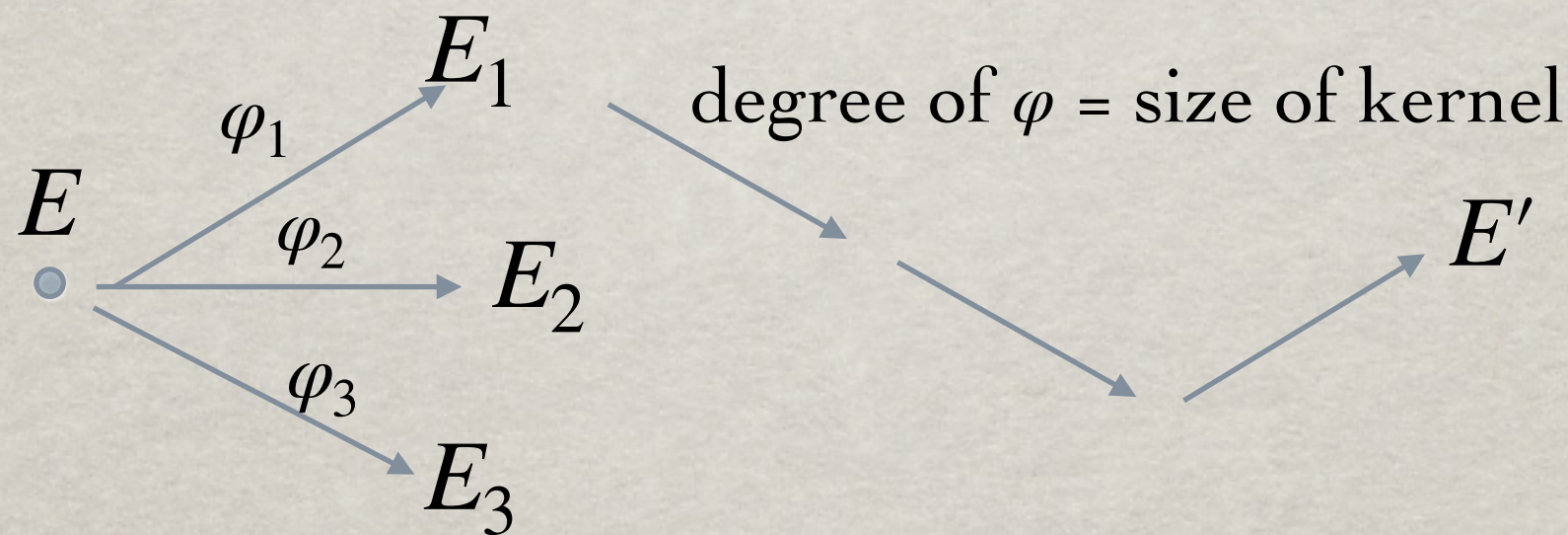
10

Computing with isogenies

Given: elliptic curve E. Points on E form abelian group.

Isogeny $\varphi : E_1 \to E_2$ is a map that respects the group structure. Isogenies are determined by their kernels.

<u>Easy</u>: compute all degree 2 isogenies to other curves. (There are three.)

degree of φ = size of kernel

<u>Hard</u>: given a second curve E', compute a degree 2^n isogeny $\varphi : E \to E'$.

Corresponds to n steps from E as above.

Hardness assumption

Hardness assumption: there is no efficient algorithm for:

ℓ-**Isogeny Pathfinding Problem:** Given prime p, super-singular curves E,E', find a path from E to E' in the ℓ-isogeny graph.

- prime p is of cryptographic size, ℓ is small prime usually 2 or 3.

- Input parameters (the curves) are of size $\log p$.

- Fastest classical algorithm for constructing isogenies between supersingular curves E,E' runs in time $\tilde{O}(p^{1/2})$ (Delfs-Galbraith)

- Fastest quantum algorithm for constructing isogenies: $\tilde{O}(p^{1/4})$ (Biasse-Jao-Sankar), uses Grover's algorithm and first finds short path from E to a curve defined over $\mathbb{F}_p$.

Both algorithms are exponential in log p.

Can show: **Pathfinding** is equivalent to computing **endomorphism rings,** and to **computing maximal orders** in quaternion algebras.

endomorphism of E = isogeny $\phi : E \to E$ from E to itself.

End(E) = set of all endomorphism of E. Has a ring structure.

E is supersingular $\leftrightarrow$ End(E) is a lattice of rank 4.

Endomorphism Ring Problem: Given prime p, supersingular elliptic curve E (with coeffs in $\mathbb{F}_{p^2}$), find four endomorphisms that generate End(E) as a lattice.

Theorem (EHLMP '18, Wesolowski' 21): Under the generalized Riemann Hypothesis, the Endomorphism Ring Problem and the ℓ-Isogeny Pathfinding Problem are equivalent under reductions that run in expected poly time.

Reductions

Pathfinding in quaternion algebra $B_{p,\infty}$

MaxOrder (Compute the maximal order in a quaternion algebra associated to endomorphism ring of E)

algebraic

SIDH key exchange
CGL hash function

$\leq$

ℓ-Isogeny Pathfinding

Graph theoretic

Pathfinding in (quotients of) Bruhat-Tits trees: **linear algebra** in $\text{Mat}_2(\mathbb{Z}_\ell)$

Endomorphism Ring Problem

arithmetic

- - - - - - - - - -   means "reduction is not efficient"

Commutative Isogeny schemes

In CSIDH, OSIDH, …: more structure, isogenies given via group actions

X= exponential size subset of supersingular elliptic curves.
E.g. all supersingular curves $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_p$.

Have group action $G \times X \to X$, $(g, x) \mapsto g * x$ (G **abelian** group)

Action should be:

1. Efficient to compute

2. Hard to invert: Given x and $g * x$, hard to compute g.
   ⬌ Security of scheme

For these schemes: have **subexponential time quantum algorithm**:
Reduce inverting the group action to solving **abelian hidden shift problem** in G.
(Childs-Jao-Soukharev '14, Wesolowski '21)

Then use Kuperberg's subexponential time algorithm for abelian hidden shift.

Reductions-commutative case

Isogeny-based systems that come with group action

$\leq$

Abelian hidden shift problem

$f_0, f_1 : G \rightarrow S, f_0(x) = f_1(xs)$

Goal: find hidden shift s

Commutative versus non-commutative isogeny crypto

DDF[+] 21: Formalize "uber" isogeny framework, allows common way for cryptanalysis of all isogeny-based crypto
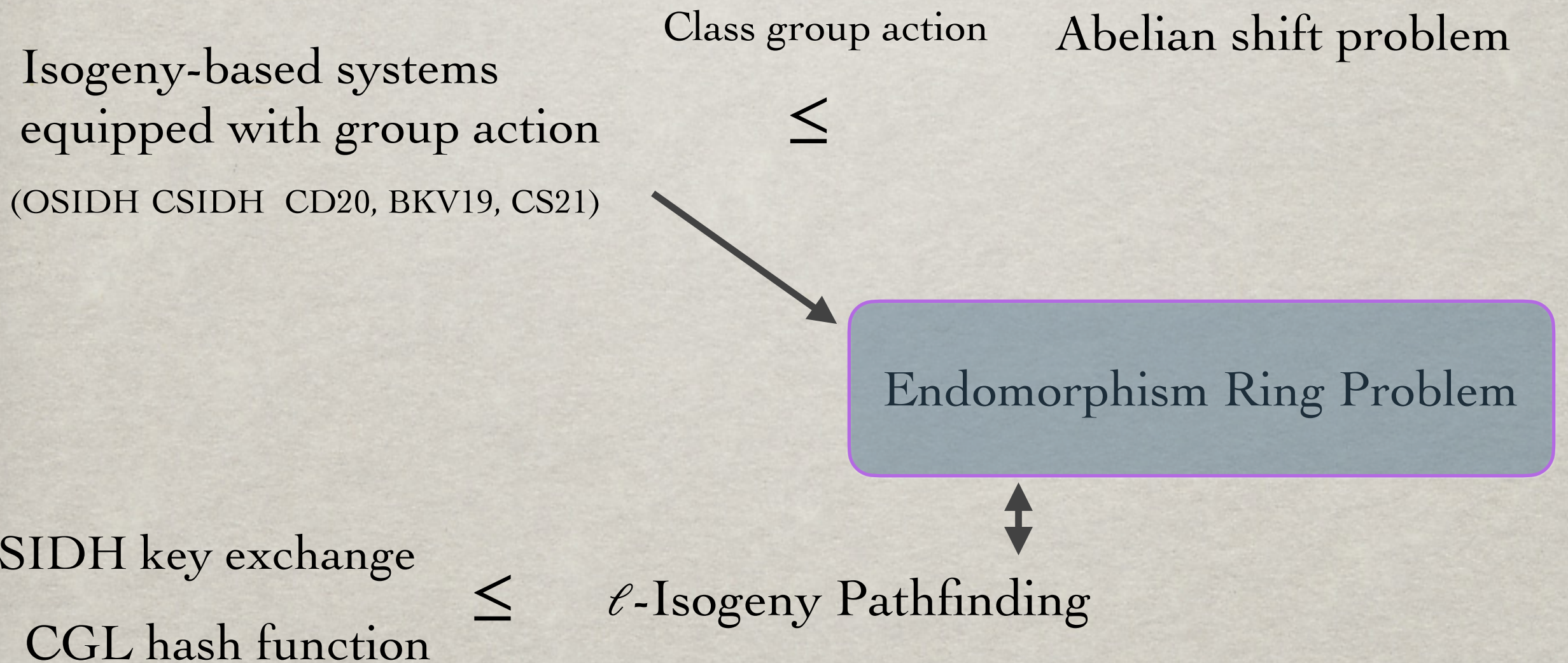
Can show: Class group actions apply to many cases that were thought to be "noncommutative".

So is there one single problem that we should try to solve and that would break all isogeny-based crypto?

Yes - the Endomorphism ring problem!

Reductions to Endomorphism ring problem

Can reduce breaking isogeny crypto based on group actions to solving Endomorphism Problem. (Wesolowski '21)

Class group action   Abelian shift problem

Isogeny-based systems
equipped with group action

$\leq$

(OSIDH CSIDH CD20, BKV19, CS21)

Endomorphism Ring Problem

SIDH key exchange

$\leq$ ℓ-Isogeny Pathfinding

CGL hash function

Conclusion

An efficient algorithm for computing endomorphism rings of supersingular curves would break all isogeny-based systems.

Fastest classical algorithm: $(\log p)^{O(1)} p^{1/2}$ (with heuristics, EHLMP '20)

Bottleneck of this algorithm: Given supersingular E, need to find cycle in isogeny graph passing through E.

Open Question: Can a quantum algorithm do better?

Summary

Supersingular Isogeny based crypto is one of the few candidates for post-quantum crypto.

For some isogeny schemes: sub exponential quantum algorithm via a reduction to the abelian hidden shift problem.

Efficient (quantum) algorithm for computing endomorphism rings of supersingular curves would break all proposed systems.

Best classical algorithm for computing endomorphism rings is exponential.
Quantum algorithms don't have an advantage so far.

Open: Is there a subexponential quantum algorithm for computing supersingular endomorphism rings?