Cryptography in the Age of Quantum Computing

Kirsten Eisenträger

Penn State

Computational Problems in Number Theory

Over the integers:

- Compute gcd's
- Primality testing
- Factoring
- Solving Pell's equation

Main computational problems for number fields :

Compute

- discriminant, ring of integers
- Galois group of Galois closure
- class group, unit group

$$K = \mathbb{Q}(\theta)$$

$$n \Big|$$

$$\mathbb{Q}$$

Number Field Problems

Given number field:

$\mathbb{Q}(\theta)$

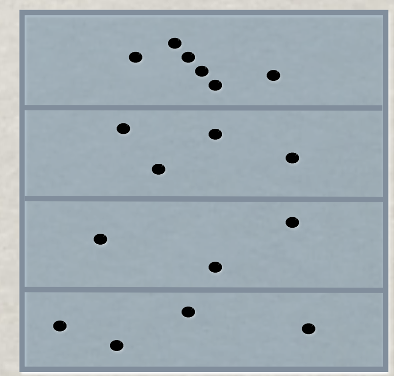
Ring of integers $\mathcal{O}$

Ideals $I_1 \; I_2 \; I_3 \; \cdots$

Compute:

1) Unit group $\mathcal{O}^*$ = Invertible elements of $\mathcal{O}$

2) Class group = Ideals mod Principal ideals



3) Principal ideal problem

$$\alpha\mathcal{O} \mapsto \alpha$$

Quantum alg for constant degree in '05

Arbitrary degree case in '14

Exponential Speedups by Quantum Algorithms

Quantum algorithms for number theoretic problems:

- Factoring, discrete log (Shor '94)
- Pell's equation (Hallgren '02)

In constant degree number fields can compute:

- Unit group, Class group (Hallgren 05, Schmidt/Vollmer 05)
- Solve Principal ideal problem (PIP)
  - Breaks Buchmann-Williams system
- Compute certain unramified field extensions of number fields (E.-Hallgren '10)

***Arbitrary* degree case:** (E-Hallgren-Kitaev-Song 14)

Function field analogues: Also have efficient algorithms (E-Hallgren '12)

Other Source of computational problems:

Number-theoretic problems related to security of public-key cryptosystems.

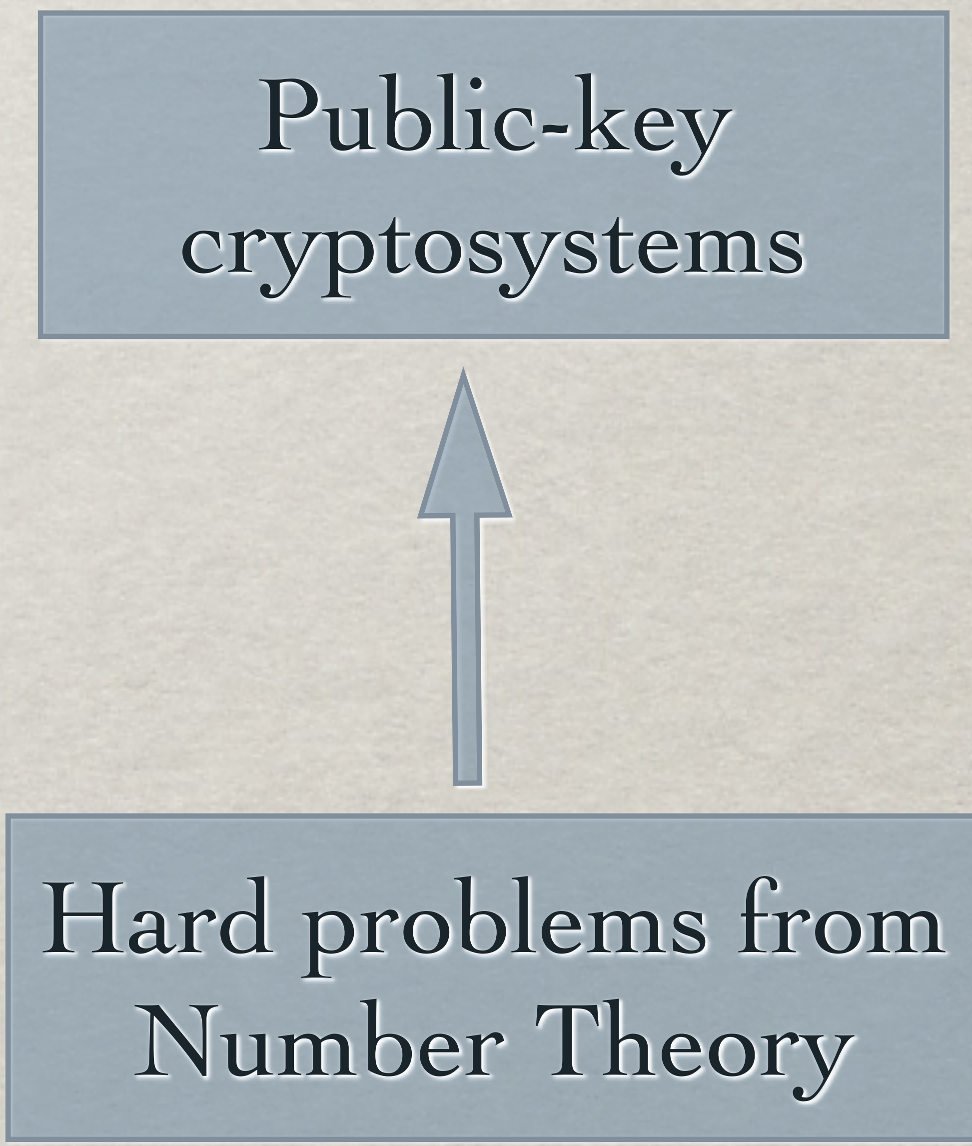
In public key cryptography: parties can communicate privately without agreeing on any secret in advance.

Example: RSA

Public-Key Cryptography

In public-key setting:

All known constructions rely on hard number theoretic problems.



Number Theoretic Problems in Cryptography

System	underlying hard? problem
RSA	Factoring
Elliptic curve cryptography	Elliptic curve discrete log
Ring-LWE	SVP in ideal lattices
Supersingular isogeny-based cryptography	Computing isogenies between curves
Soliloquy	Short generator PIP

Classical versus Quantum Algorithms

Open

- SVP
- Endomorphism rings of supersingular elliptic curves
- SVP in ideal lattices
- Isogenies between elliptic curves

Quantum poly-time

- Factoring
- Endomorphism rings of ordinary elliptic curves
- Unit group
- Discrete log
- Class group
- Principal Ideal Problem (PIP)

Classical poly-time

- Elliptic curve addition
- Isogenies between elliptic curves with torsion info
- Modular arithmetic

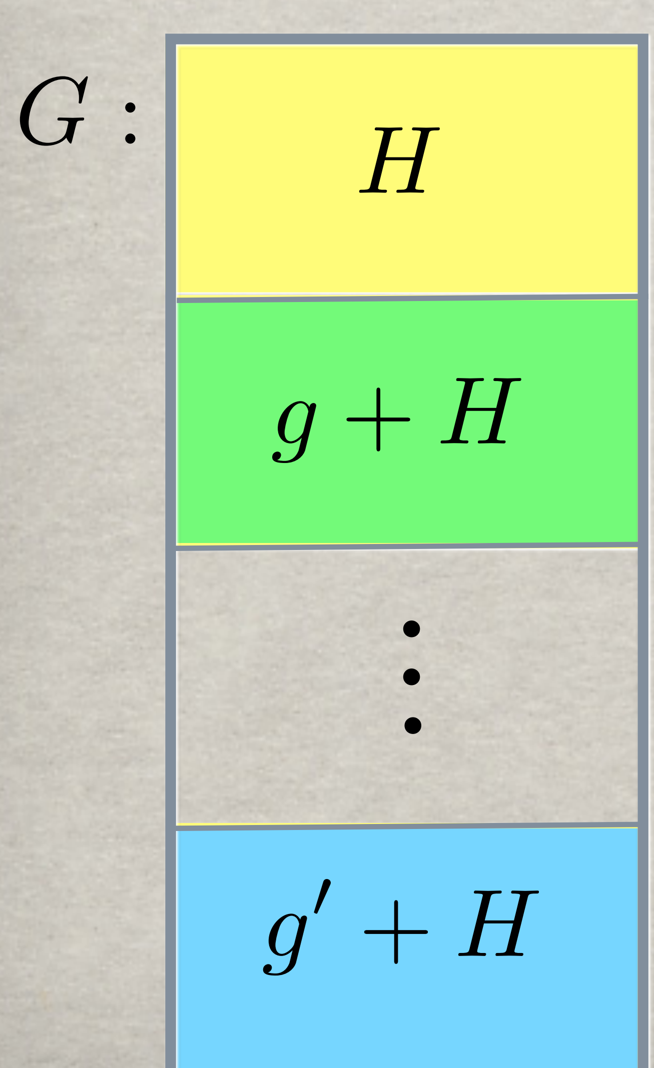
Approach for Quantum Algorithms for discrete Log, factoring

Give classical reductions from these problems to Hidden Subgroup Problems (HSPs)

Show that the HSP has an efficient quantum algorithm.

The Hidden Subgroup Problem (HSP)

Given $g : G \to S$ that is constant and distinct on cosets of a subgroup H. Find H.



The structure of G determines how hard the problem is.

Examples:

G abelian, have quantum algorithms

- Factoring N: $G = \mathbb{Z}$
- Discrete log: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$
- Pell's equation: $G = \mathbb{R}$

Post-quantum Cryptography

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

Bad choices: RSA, Elliptic Curve Cryptography, systems based on special type lattices (Soliloquy)

Good choices: ??? Have to study the problems that are open, like SVP and computing isogenies between elliptic curves. NIST competition aims to do this.

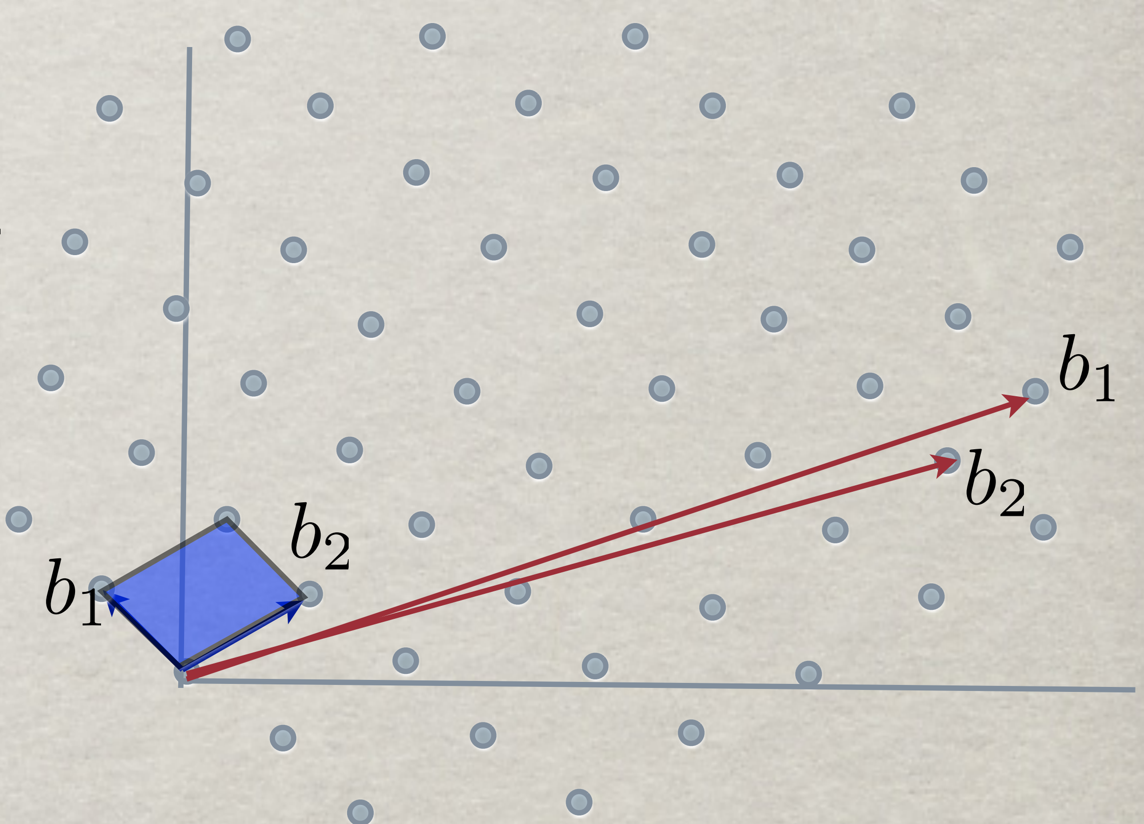
NIST Competition for Post-Quantum Cryptosystems

- Goal: Replace currently-used cryptosystems because RSA and ECC are broken by quantum computers.
- 69 submissions were accepted in round one in November 2017.
- 8 submissions broken by end of 2017, 22 submissions broken by end of 2018.
- 26 submissions advanced to round 2.
- Remaining systems are: code-based, lattice-based and supersingular isogeny-based.

Lattices and systems based on them

- Given $b_1, ..., b_n \in \mathbb{R}^n$

$$L = \left\{ \sum a_i b_i : a_i \in \mathbb{Z} \right\}$$



- Infinite number of bases for a lattice

Prototype of Lattice Problem

Problem (Shortest Vector Problem, SVP). Given vectors $b_1, \ldots, b_n \in \mathbb{R}^n$ generating a lattice $L = \left\{ \sum a_i b_i : a_i \in \mathbb{Z} \right\}$, compute the shortest nonzero vector in L.

1. L has infinitely many bases, so in general can't read off short vectors from lattice basis.

2. Can base cryptosystems on SVP, but: much slower than RSA.

3. In Soliloquy: To improve efficiency, several assumptions were made.

Assumptions for Improving Efficiency of Lattice-based Systems

1. Assume SVP is hard if L comes from an ideal I in the ring of integers in a number field. (L=ideal lattice).

2. Assume: problem still hard if, in addition, I is a principal ideal. I.e. $I = (\alpha)$.

3. Same setup as in (2.), but assume also that the generator α for I is short. Known as Short generator principal ideal problem (SGPIP).

Several constructions are based on SGPIP: Soliloquiy, multilinear maps.

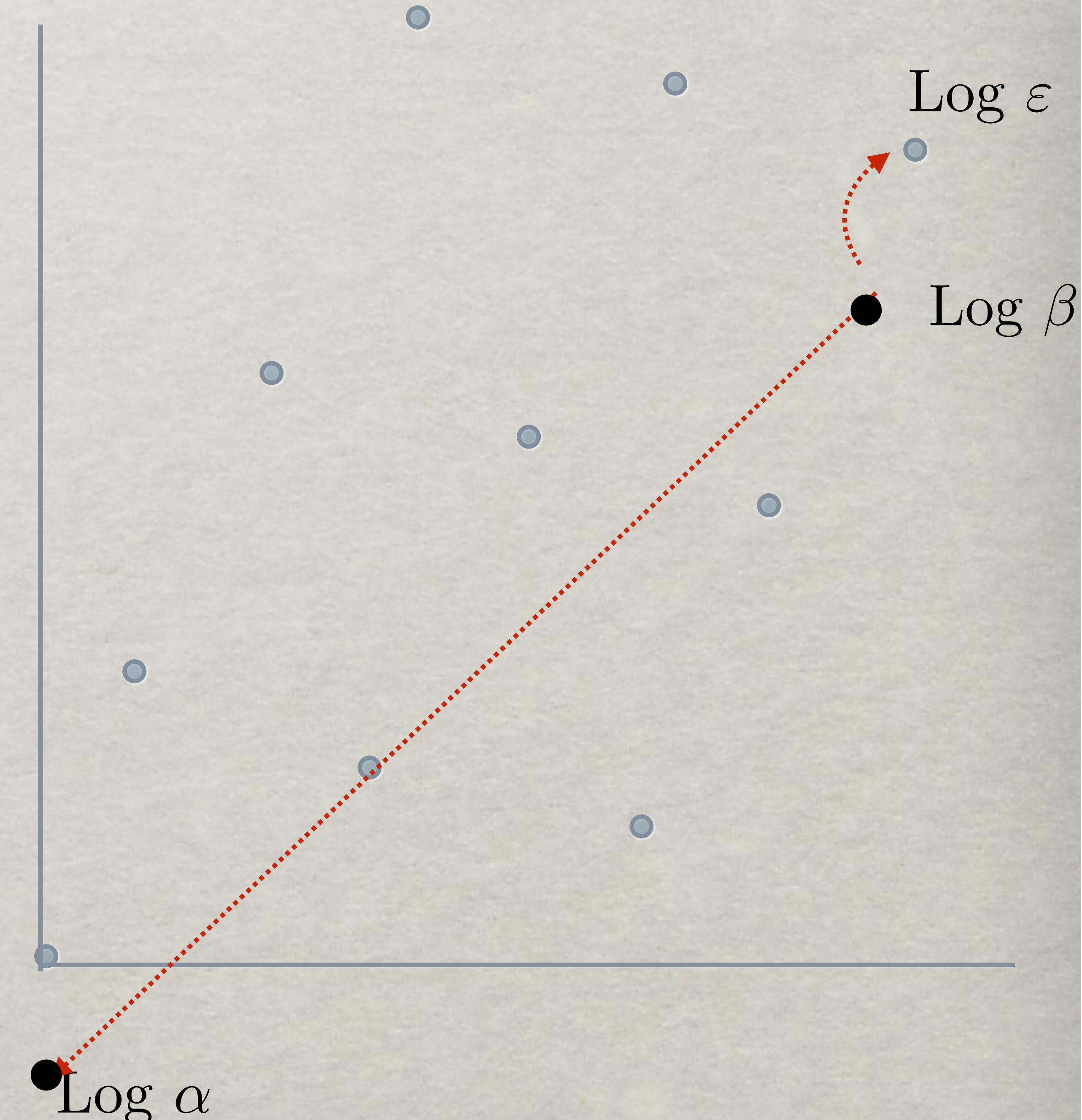
There is an efficient quantum algorithm for SGPIP.
So: these systems are broken by quantum computers.

How to compute the Short Generator

Input: ideal I in a number field
Output: $\mathrm{Log}\,\alpha$ with α short and $I = (\alpha)$.

1) Compute the unit group
2) Solve the PIP Problem to get $\mathrm{Log}\ \beta$ s.t. $I = (\beta)$
3) Solve BDD in the unit lattice to get $\mathrm{Log}\ \varepsilon$
4) Output $\mathrm{Log}\,\alpha = \mathrm{Log}\,\beta - \mathrm{Log}\,\varepsilon$

The Unit Lattice $\mathrm{Log}\,\mathcal{O}^*$



A quantum algorithm for the unit group

Step (1) is the following theorem:

Theorem (E-Hallgren-Kitaev-Song): Let K be a number field (i.e. a finite extension of $\mathbb{Q}$) of arbitrary degree, and let $\mathcal{O}$ be its ring of integers. There is a polynomial time quantum algorithm for computing the unit group $\mathcal{O}^*$.

Unit group is too big to write down generators. 'Computing the unit group' means writing down a basis for the lattice Log $\mathcal{O}^*$.

Using elliptic curves for Post-Quantum Crypto

Traditional elliptic curve cryptography:

- Fix one curve and use the group law.
- Assume discrete log is hard on this group.

Shor's quantum algorithm breaks these.

New proposal:

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

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

- Points are (x, y) satisfying above equation and extra point ∞
- Points form an abelian group
- Have several cryptosystems based on isogenies. Only submission to NIST competition was SIKE-SIDH.

Example: SIDH Key Exchange
(Supersingular Isogeny Diffie-Hellman)
Broken, Summer 2022

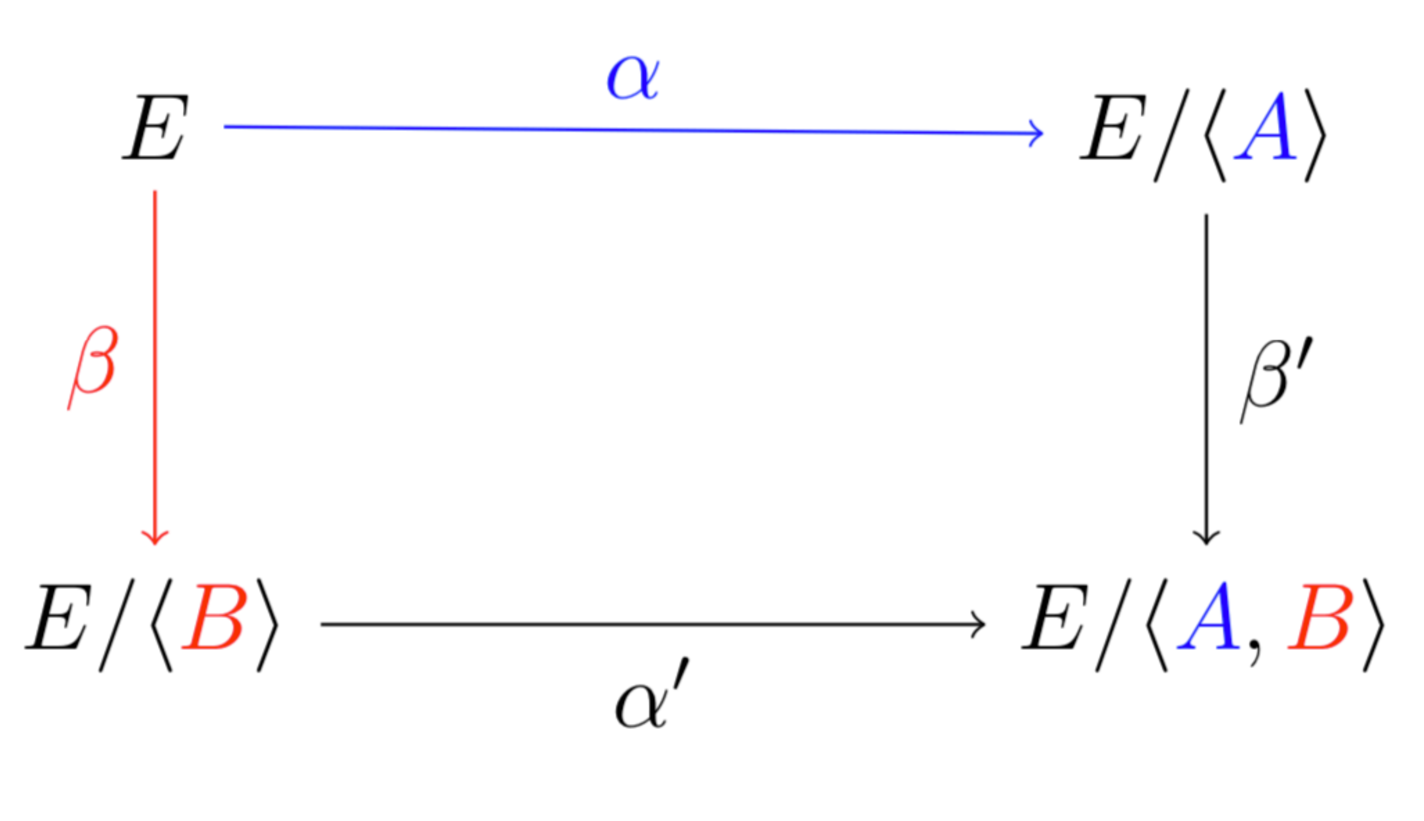
E = supersingular elliptic curve defined over $\mathbb{F}_{p^2}$.

1. **Alice:** chooses secret subgroup A of E, sends E/A to Bob.
2. **Bob:** chooses subgroup B of E and send E/B to Alice.
3. **Shared secret:** elliptic curve $E/\langle A, B\rangle$.

Alice's secret: $\ker(\alpha) = \langle A \rangle$

Bob'secret: $\ker(\beta) = \langle B \rangle$

Joint secret: $E/\langle A, B\rangle$



Breaking SIDH

Vulnerability of SIDH: have to reveal evaluation $\alpha(P), \alpha(Q)$ for certain points P, Q on E. (Same for β.)

Idea for break: Recover $\ker(\alpha)$ from $\ker(f)$, where f is an isogeny between products of curves.

$$f : C \times E' \to E \times X$$

Castryck-Decru (July 2022) Maino et al. (August 2022) Robert (August 2022)

Open question:

Are the other cryptographic constructions based on isogenies still secure ?