ANTS XIV invited talk

Isogeny-based cryptography: past, present, and future

7/2/2020

David Jao

University of Waterloo and evolution Q, Inc.

Isogenies

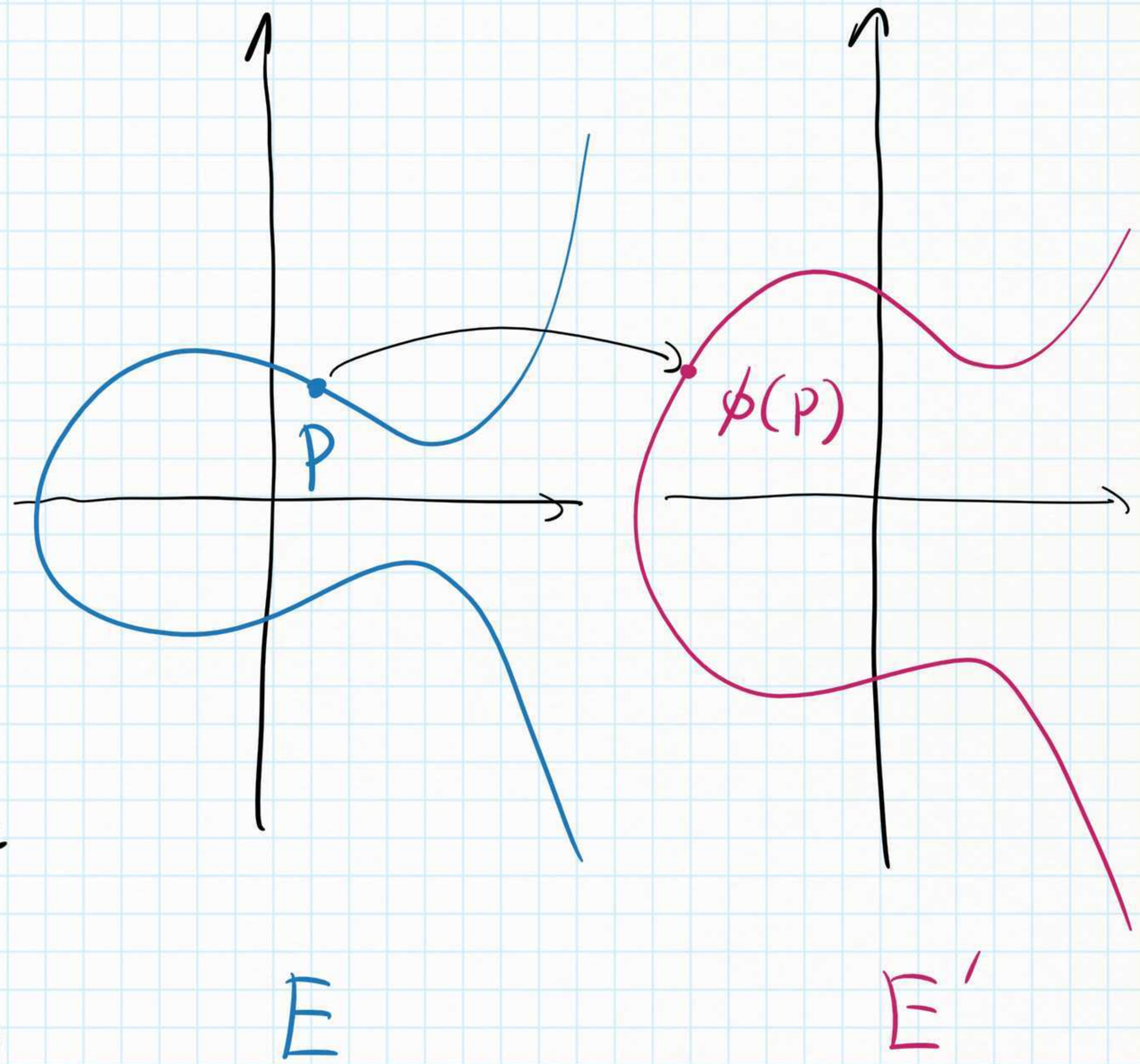
An isogeny is a rational map

$$\phi : E \to E'$$

between elliptic curves which maps the identity to the identity.

The degree of ϕ is its degree as a rational map:

$$\deg \phi = \left[K(E) : \phi^*(K(E')) \right].$$



Computational theory of isogenies

- Every purely inseparable isogeny has the form

$$\pi(x,y) = (x^q, y^q)$$

for some prime power $q = p^n$, and $\deg \phi = q$.

- Every (nonconstant) separable isogeny has a finite kernel and is determined by its kernel (up to isomorphism):

$$G = \ker \phi \quad \longleftrightarrow \quad \phi : E \to E/G,$$

and $\deg \phi = |G|$.

Vélu's formula (1971)

Given an elliptic curve E and a finite subgroup $G \subset E$, the map $\phi(P) = (\phi_1(P), \phi_2(P))$ where

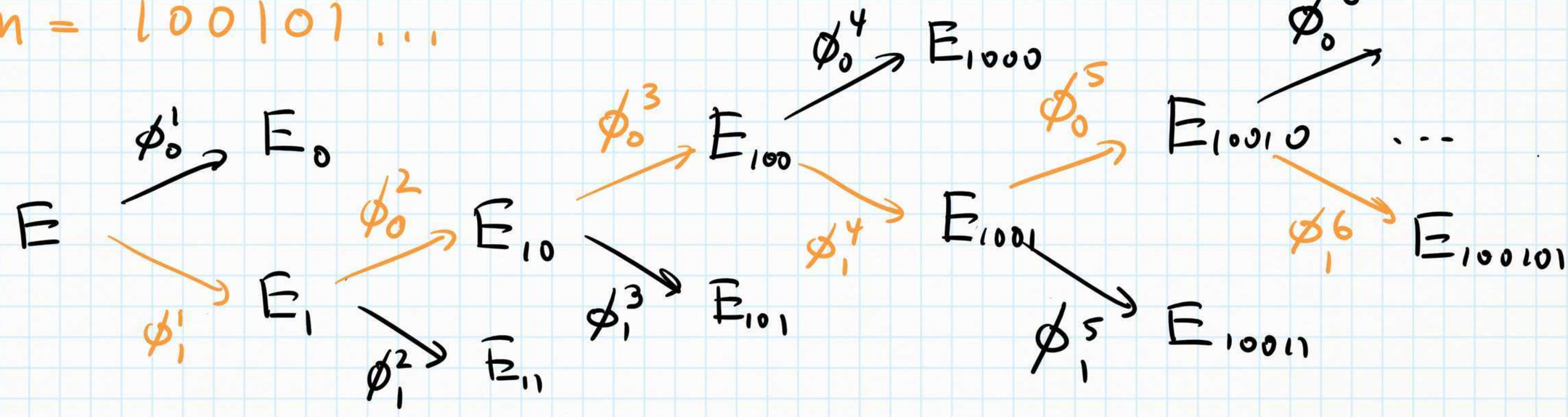
$$\phi_1(P) = x(P) + \sum_{Q \in G \setminus \{O_E\}} \left[x(P+Q) - x(Q) \right]$$

$$\phi_2(P) = y(P) + \sum_{Q \in G \setminus \{O_E\}} \left[y(P+Q) - y(Q) \right]$$

is a separable isogeny $\phi : E \to E'$ with $\ker \phi = G$.

Hash functions [Charles, Goren, Lauter J. Cryptol. 2009]

$m = 100101\ldots$



Set $H(m) = E_m$.

(This hash function has been broken by [Kohel et al. (ANTS XI)], [Eisenträger et al. (ANTS XIV)].)

Public-key cryptosystems

- CRS [Couveignes (2006), Rostovtsev & Stolbunov (2006)]

- Supersingular Isogeny Diffie-Hellman (SIDH)
  [Jao, De Feo, and Plût (2011)]

  ↳ SIKE [Jao et al. (2017)], submitted to NIST PQC

- Commutative SIDH (CSIDH)
  [Castryck et al. (Asiacrypt 2018)]

	CRS	CSIDH	SIDH	SIKE
ordinary curves	✓	✗	✗	✗
supersingular curves	✗	✓	✓	✓
public key validation	✓	✓	✗	✓✗
post-quantum security	subexponential $L_p(\frac{1}{2}, c)$		exponential $O(\sqrt[6]{p})$	

CRS

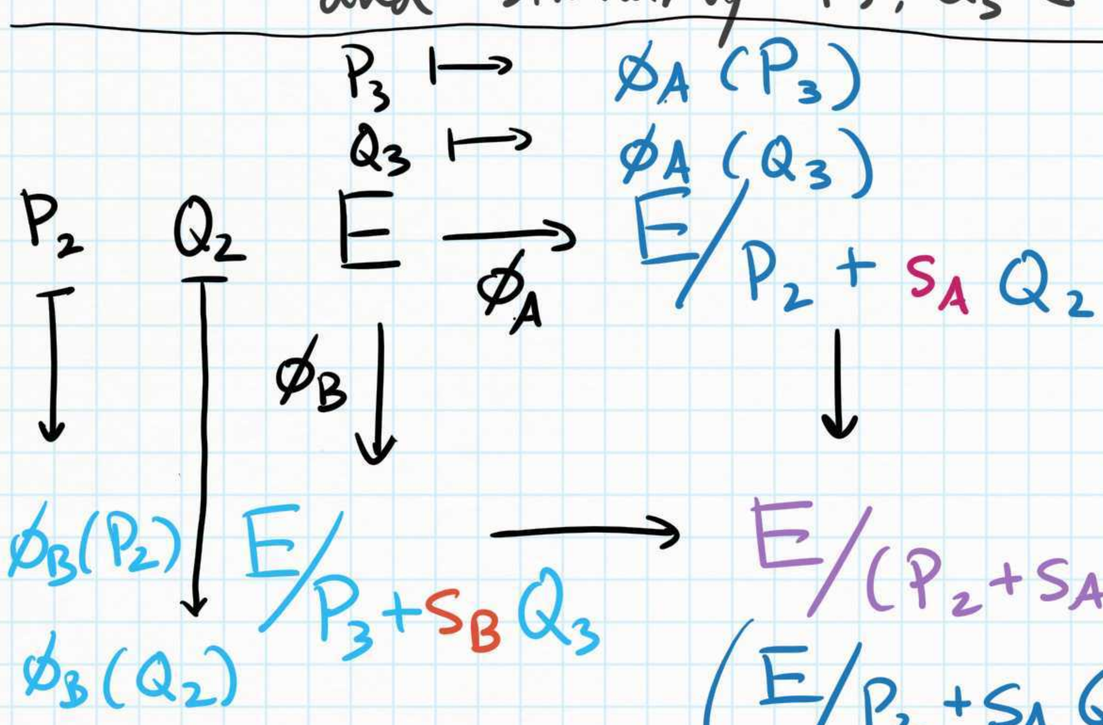
- Choose an ordinary elliptic curve $E/\mathbb{F}_p$.
- There is a complex multiplication action
  $* : Cl(End(E)) \curvearrowright \mathcal{SELL}(End(E))$ given by
  $\mathfrak{a} * E = E/E[\mathfrak{a}] = E/\bigcap \{\ker \psi : \psi \in \mathfrak{a}\}$.
- Key exchange:

Alice	Bob
Private key: $\mathfrak{a}$	Private key: $\mathfrak{b}$
Public key: $\mathfrak{a} * E$	Public key: $\mathfrak{b} * E$
Shared secret: $\mathfrak{a} * \mathfrak{b} * E = \mathfrak{b} * \mathfrak{a} * E$	

- In practice, one must use smooth $\mathfrak{a}$ and $\mathfrak{b}$ in order to be able to evaluate $*$

SIDH

- Choose a supersingular elliptic curve $E/\mathbb{F}_p$, $p = 2^e 3^f - 1$ such that $\#E(\mathbb{F}_{p^2}) = (p+1)^2 = (2^e 3^f)^2$.
- Choose $P_2, Q_2 \in E(\mathbb{F}_{p^2})$ such that $E[2^e] = \{mP_2 + nQ_2 : m,n \in \mathbb{Z}\}$ and similarly $P_3, Q_3 \in E[3^f]$.



Alice private key
Alice public key
Bob private key
Bob public key
Shared secret

SIKE : SIDH + [Hofheinz et al. (TCC 2017)] variant of the Fujisaki-Okamoto transform.

CSIDH : Choose E supersingular over $\mathbb{F}_p$,

$p = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} - 1$, $p_1, -, p_t$ small

Then (as in SIDH) isogenies of degree p_i are easier to evaluate, and (as in CRS) $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}_D$ so one has a complex multiplication action

$$\mathfrak{a} * E = E/E[\mathfrak{a}] = E/\bigcap \{\ker \psi : \psi \in \mathfrak{a}\}.$$

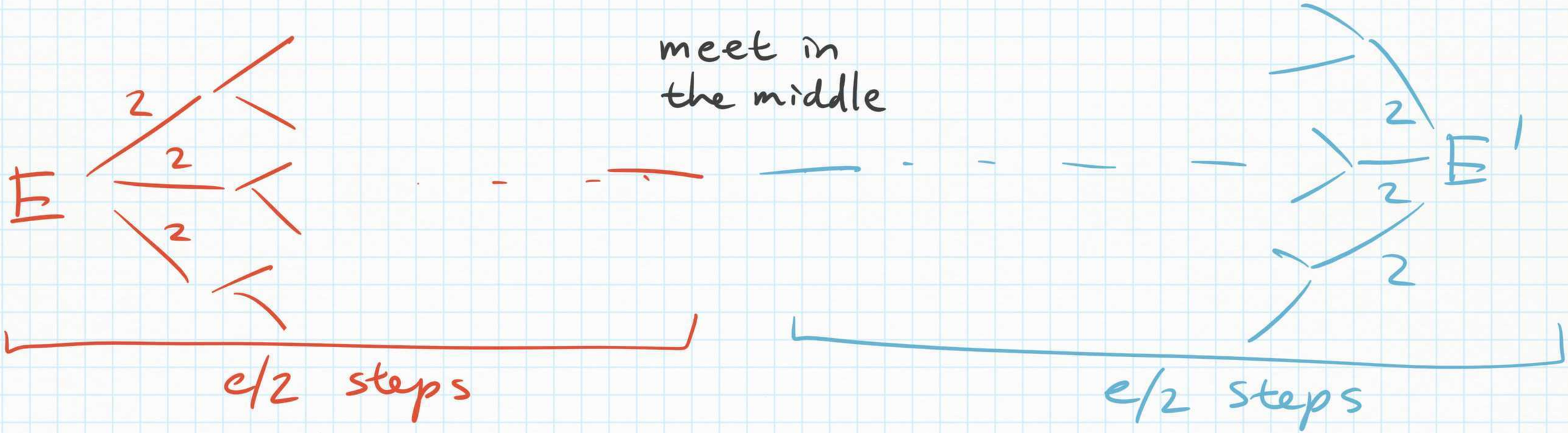
Key size / performance comparison

	CSIDH 512	SIKEp434	SIKEp434 compressed
Public key	64 bytes	330 bytes	197 bytes
Private key	37 bytes	374 bytes	350 bytes
Encryption	106 Mcycles	9.6 Mcycles	15.1 Mcycles
Decryption	106 Mcycles	10.3 Mcycles	11.1 Mcycles
Quantum security	AES-128[1]	AES-128	AES-128

[1] May be affected by [Peikert (Eurocrypt 2020)]

Quantum algorithms for isogenies

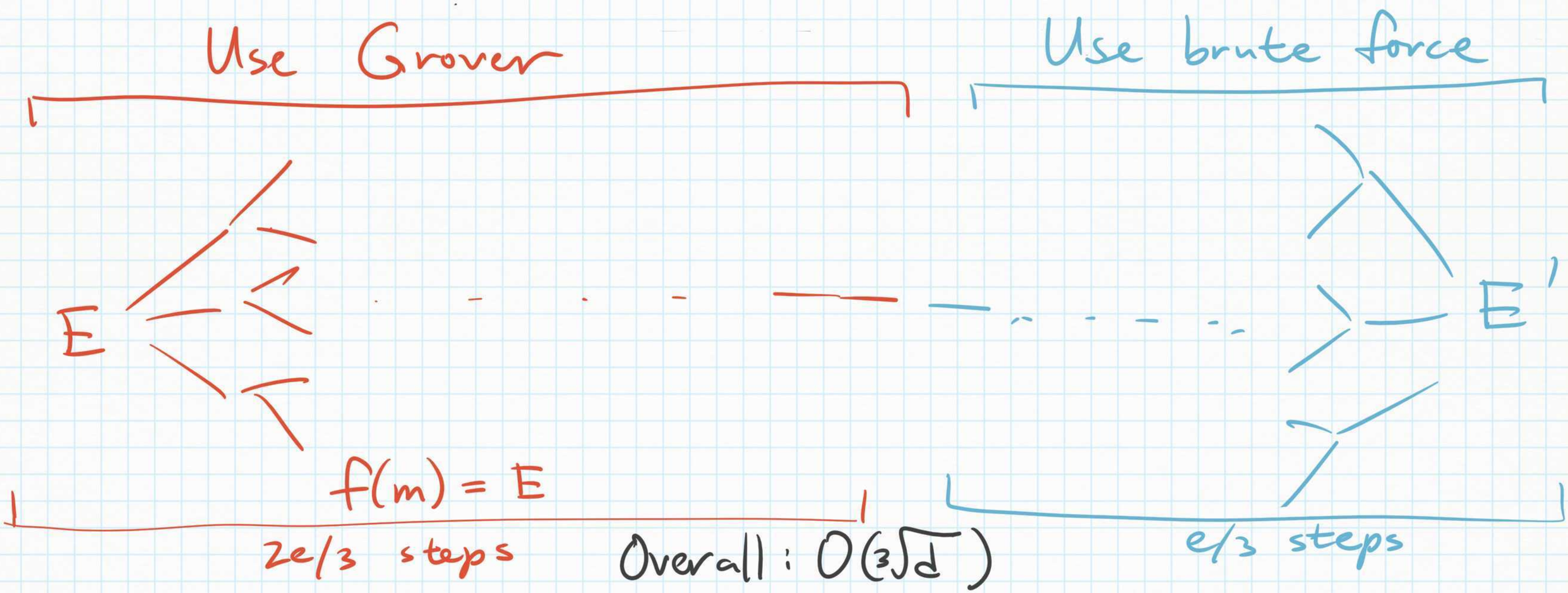
For SIDH/SIKE: Given E, E' which are 2^e-isogenous, find $\phi: E \to E'$ with $\deg \phi = 2^e$.



Classical complexity: $O(\sqrt{d})$ where $d = \deg \phi$.

Quantum meet in the middle (Tani's algorithm)

- Grover's algorithm: Invert a one-way function in $O(\sqrt{n})$ quantum time.



For CRS / CSIDH : Given E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

More generally : Given a simply transitive group action $G \times X \longrightarrow X$, and $x_0, x_1 \in X$, find $\gamma \in G$ such that $\gamma x_1 = x_0$.

There is a subexponential time quantum algorithm to solve this problem ($L_{|G|}(\frac{1}{2}, c)$ for various c) :

[Kuperberg, 2003]
[Regev, 2004]
[Kuperberg, 2011]
[Peikert, 2020]

Basics of quantum algorithms

- A quantum state is a point in complex projective space.
  - We usually normalize states to have norm 1.
- Measuring a normalized quantum state $\sum c_i \vec{v}_i$ with respect to an orthonormal basis $\{\vec{v}_1, \ldots, \vec{v}_n\}$ yields $\vec{v}_i$ with probability $|c_i|^2$.
- All operations except measurement are unitary operators (hence invertible).

Example: $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \otimes |0\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \otimes |f(i)\rangle$

This operation is invertible, since the input $|i\rangle$ is retained.

$|i\rangle$ and $|f(i)\rangle$ are entangled - measuring one constrains the other.

e.g. if we measure $|f(i)\rangle$ and get $|4\rangle$ and then measure $|i\rangle$ and get $|x\rangle$, we must have $x \in f^{-1}(4)$.

Kuperberg's algorithm: Assume for simplicity $G \cong \mathbb{Z}/n$, and $\gamma x_1 = x_0$.

1. Form the quantum state

$$\frac{1}{\sqrt{2n}} \sum_{g \in \mathbb{Z}/n} |(g, 0, g x_0)\rangle + |(g, 1, g x_1)\rangle$$

2. Measure the third coordinate. If we obtain x then our quantum state becomes

$$\frac{1}{\sqrt{2}}\left(|(g, 0, x)\rangle + |(g+\gamma, 1, x)\rangle\right)$$

where $g x_0 = x$. Discard x.

3. Apply the quantum Fourier transform to the first coordinate:

$$\xrightarrow[\text{1st coord.}]{QFT} \frac{1}{\sqrt{2n}} \sum_{k \in \mathbb{Z}/n} \left(\zeta_n^{kg} |(k, 0)\rangle + \zeta_n^{k(g+\gamma)} |(k, 1)\rangle\right) = \frac{1}{\sqrt{n}} \sum_{k \in \mathbb{Z}/n} \zeta_n^{kg} |k\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \zeta_n^{k\gamma} |1\rangle\right)$$

measure 3rd coord.

4. Measure the first coordinate. If we obtain k, then the second coordinate is

$$\psi_k = \frac{1}{\sqrt{2}}\left(|0\rangle + \zeta_n^{k\gamma} |1\rangle\right)$$

5. Given ψ_p and ψ_q, combine them:

$$\psi_p \otimes \psi_q = \frac{1}{2}\left(|0,0\rangle + \zeta_n^{p\gamma} |1,0\rangle + \zeta_n^{q\gamma} |0,1\rangle + \zeta_n^{(p+q)\gamma} |1,1\rangle\right)$$

$$\xrightarrow{CNOT} \frac{1}{2}\left(|0,0\rangle + \zeta_n^{p\gamma} |1,1\rangle + \zeta_n^{q\gamma} |0,1\rangle + \zeta^{(p+q)\gamma} |1,0\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|\psi_{p+q}, 0\rangle + \zeta_n^{q\gamma} |\psi_{p-q}, 1\rangle\right)$$

6. Measure the second coordinate. If it is $\begin{cases} |0\rangle \\ |1\rangle \end{cases}$ then first coordinate is $\begin{cases} \psi_{p+q} \\ \psi_{p-q} \end{cases}$

measure 1st coord

Algorithm:

1. Generate a bunch of (k, Ψ_k) for random k.
2. Collect them into groups of states where the least significant bits in each group match.
3. Combine states to obtain $(p \pm q, \Psi_{p \pm q})$ at random; hope for $(p - q, \Psi_{p-q})$ (cancelling low bits).
4. Continue until obtaining $\Psi_{n/2} = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\gamma}|1\rangle)$.
5. Measure $\Psi_{n/2}$ with respect to $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ to obtain $LSB(\gamma)$. Repeat for all the other bits.

Overall algorithm is subexponential. For details see references.

Other algorithms:

- [Galbraith et al. (Asiacrypt 2016)]: active attack against SIDH using falsified torsion point images.
- [Petit (Asiacrypt 2017)]: attacks against non-standard SIDH variants using torsion point images.
- [Kohel et al. (ANTS XI)]: efficient algorithms for finding isogeny paths in quaternion algebras.
- Many others: [Merz et al. (CT-RSA 2020)], [Basso et al. (ANTS XIV)], [Galbraith & Vercauteren (2017/774)]

Future developments

New cryptosystems

- OSIDH [Colò & Kohel (NutMiC 2019)]
- AKE [Xu et al. (Asiacrypt 2019)]
- SÉTA [Delpech de Saint Guilhem et al. (2019/1291)]
- SiGamal [Morita et al. (2020/613)]
- B-SIDH [Costello (2019/1145)]

Signature schemes :

- GPS [Galbraith et al. (Asiacrypt 2017)]
- Sea Sign [De Feo & Galbraith (Eurocrypt 2019)]
- CSI-FiSh [Beullens et al. (Asiacrypt 2019)]
- SQI-sign [Leroux et al, (2020)]