Isogeny-based cryptography: A brand new day

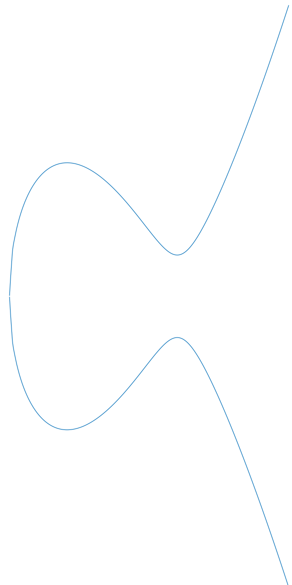
Central European Conference on Cryptology

Thomas Decru

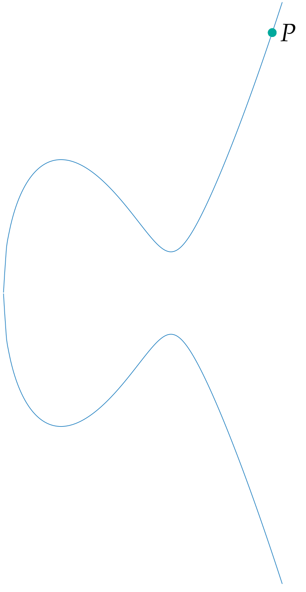
COSIC KU Leuven, Belgium

June 20th, 2025, Budapest

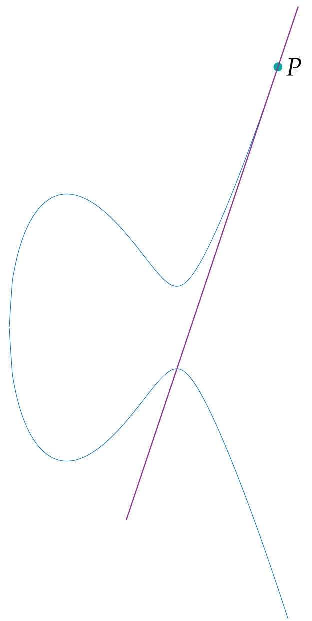
Elliptic curve group law



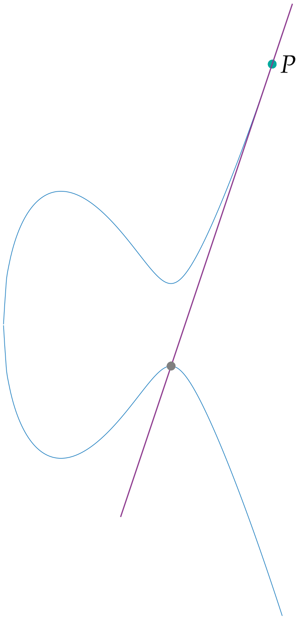
Elliptic curve group law



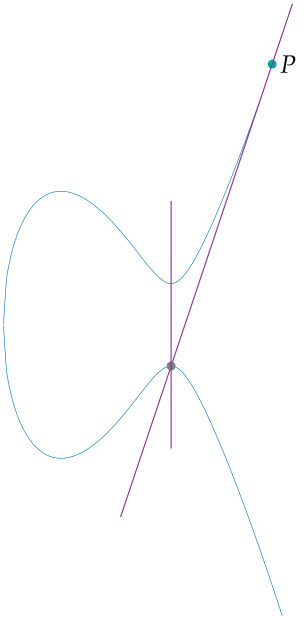
Elliptic curve group law



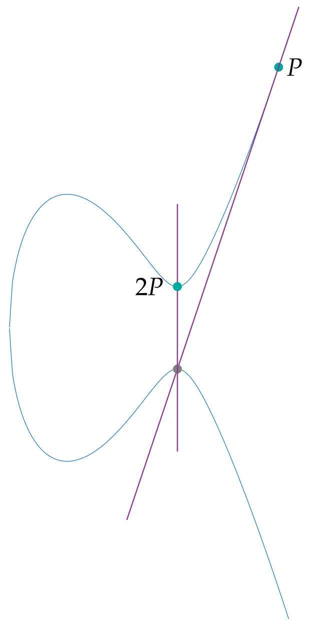
Elliptic curve group law



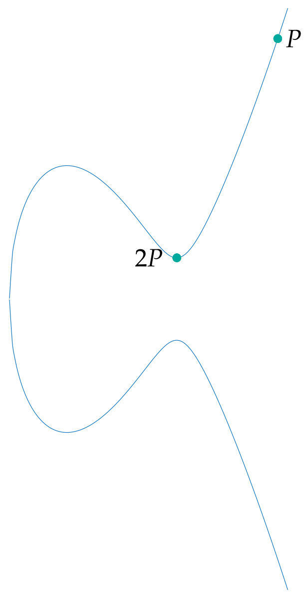
Elliptic curve group law



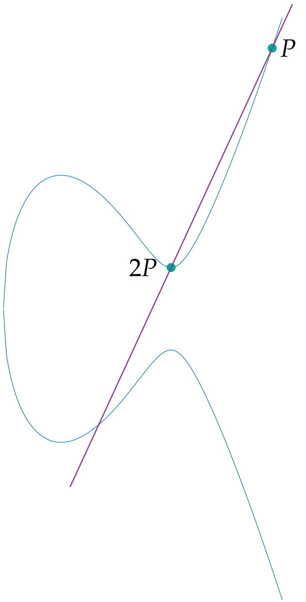
Elliptic curve group law



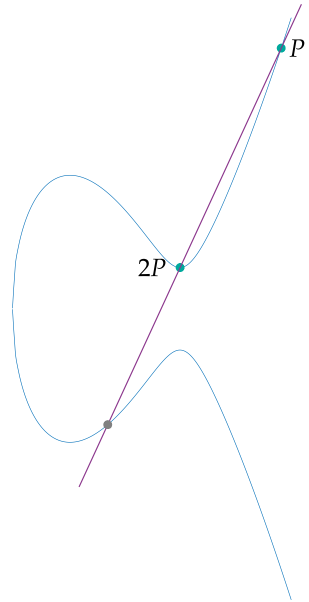
Elliptic curve group law



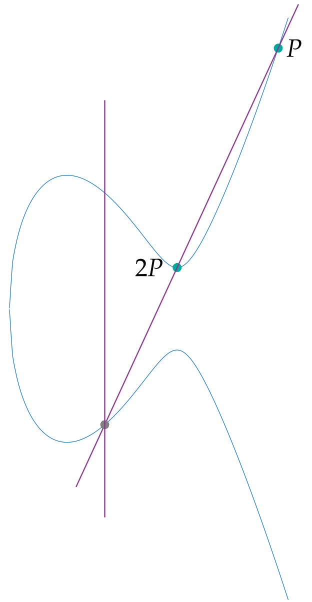
Elliptic curve group law



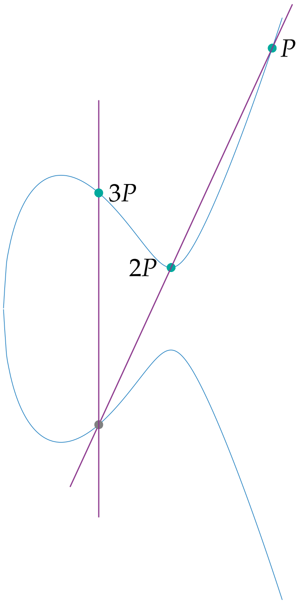
Elliptic curve group law



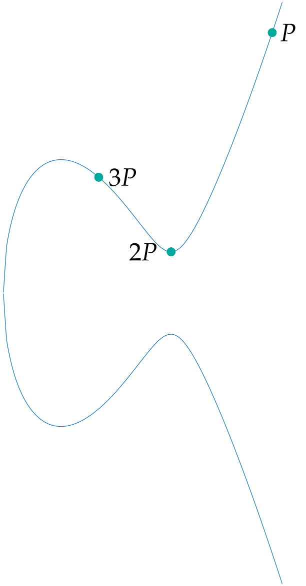
Elliptic curve group law



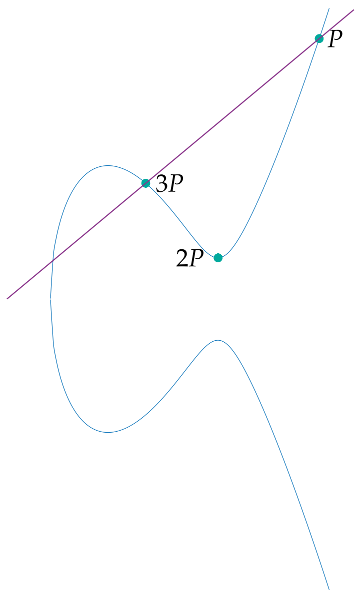
Elliptic curve group law



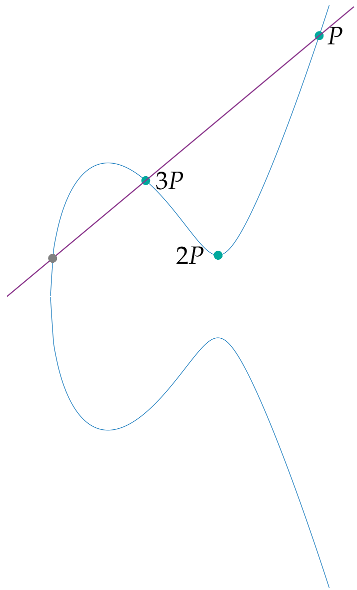
Elliptic curve group law



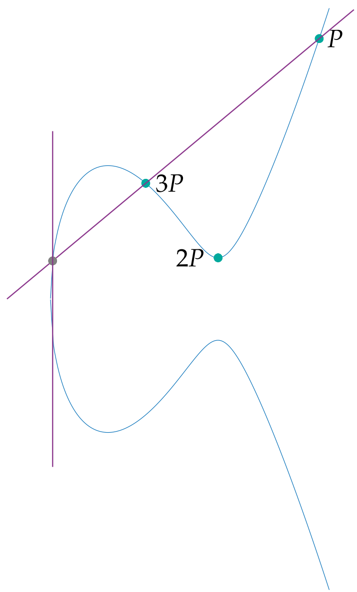
Elliptic curve group law



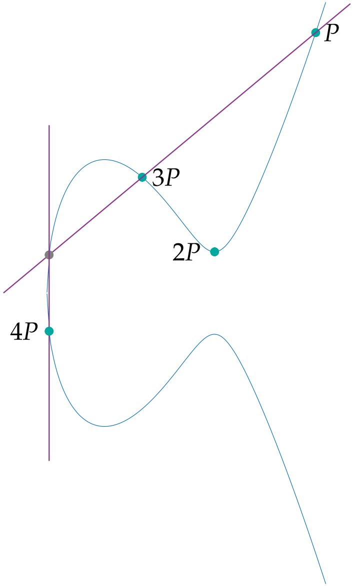
Elliptic curve group law



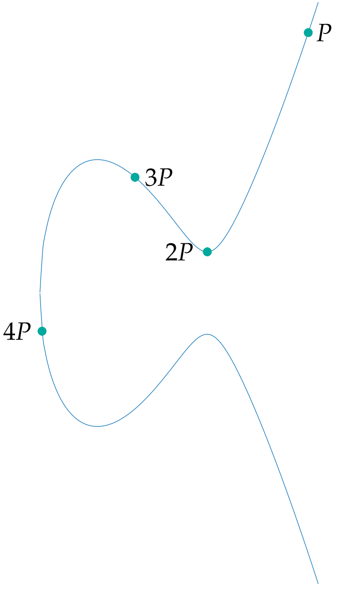
Elliptic curve group law



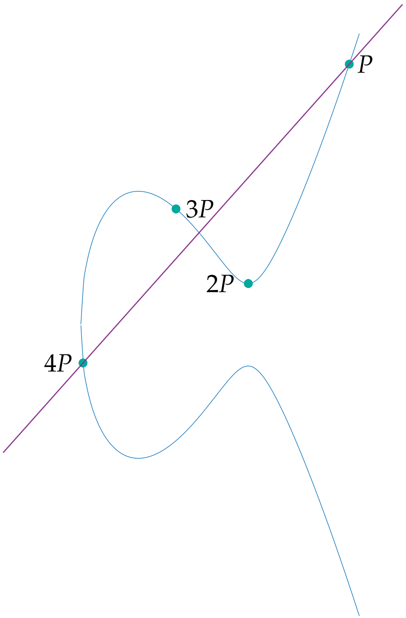
Elliptic curve group law



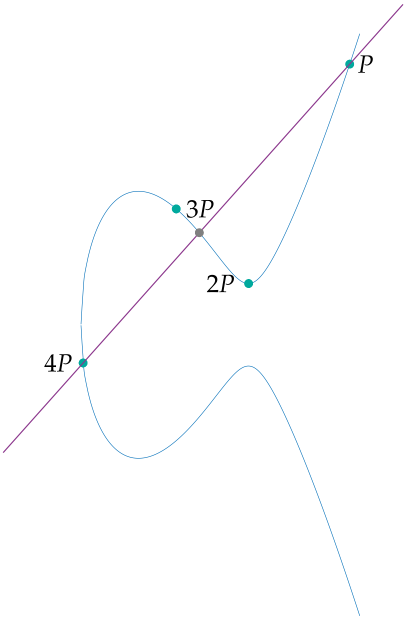
Elliptic curve group law



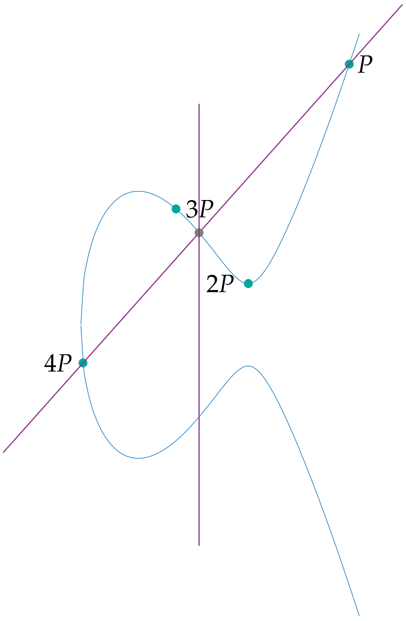
Elliptic curve group law



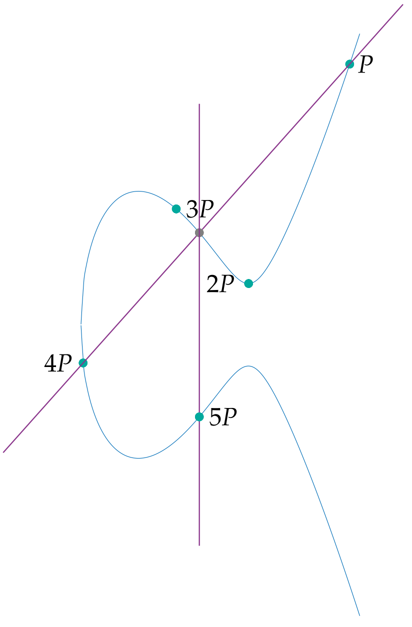
Elliptic curve group law



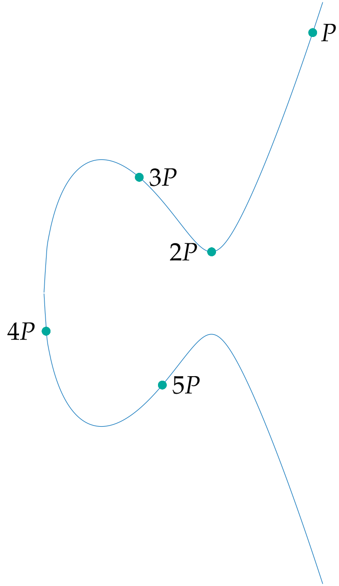
Elliptic curve group law



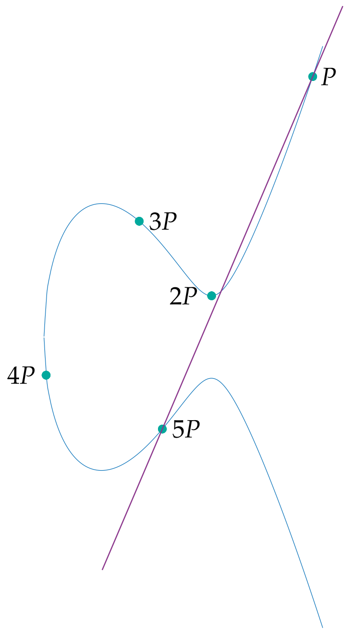
Elliptic curve group law



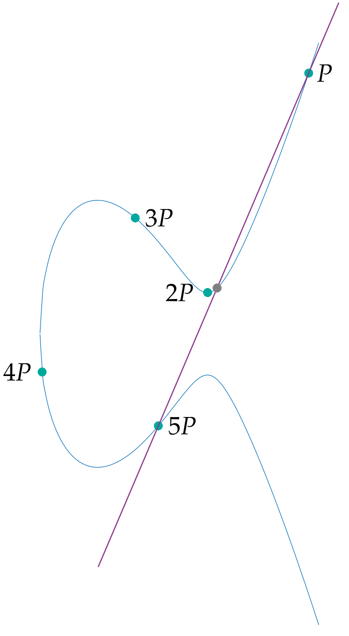
Elliptic curve group law



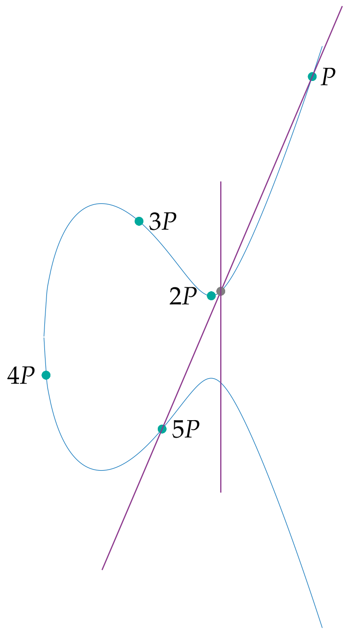
Elliptic curve group law



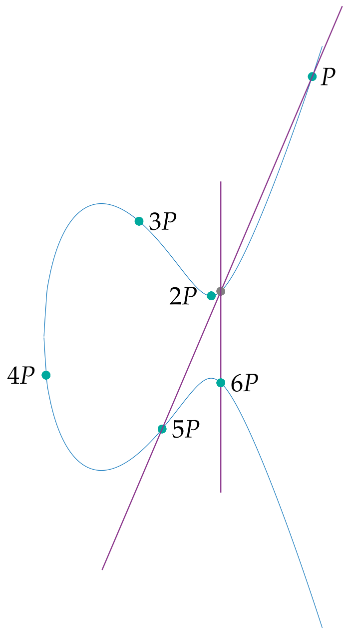
Elliptic curve group law



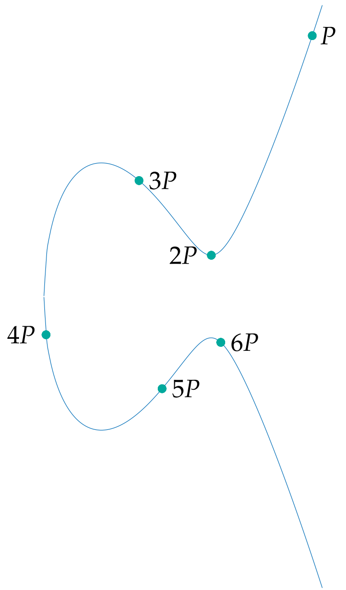
Elliptic curve group law



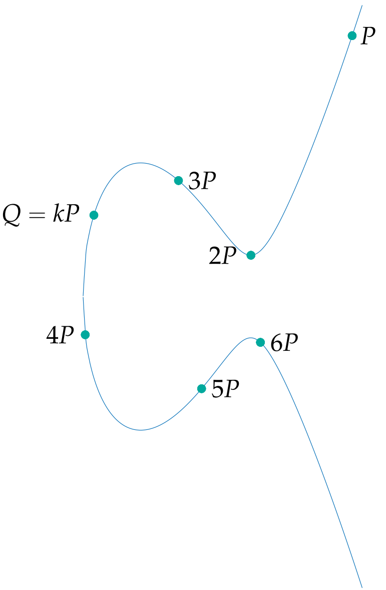
Elliptic curve group law



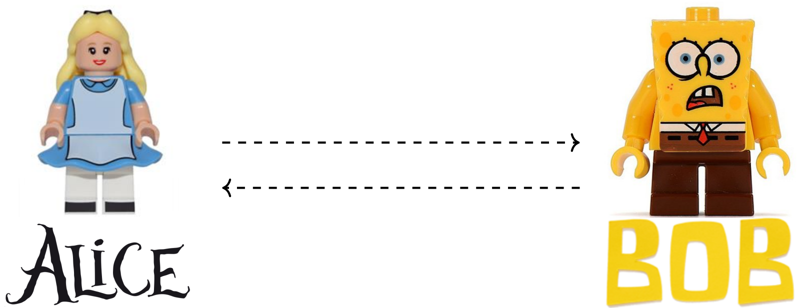
Elliptic curve group law



Elliptic curve group law

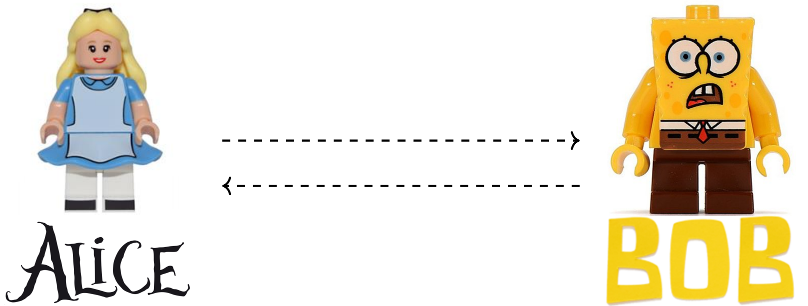


Elliptic Curve Diffie–Hellman



Elliptic Curve Diffie–Hellman

Public information: point $P \in E$



Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

Private integer b

Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

$Q_{\text{Alice}} = aP$

Private integer b

$Q_{\text{Bob}} = bP$

Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

$Q_{\text{Alice}} = aP$

Q_{Alice} ⟶

⟵ Q_{Bob}

Private integer b

$Q_{\text{Bob}} = bP$

Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

$Q_{\text{Alice}} = aP$

$Q_{\text{Alice+Bob}} = aQ_{\text{Bob}}$

Q_{Alice} →

← Q_{Bob}

Private integer b

$Q_{\text{Bob}} = bP$

$Q_{\text{Bob+Alice}} = bQ_{\text{Alice}}$

Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

$Q_{\text{Alice}} = aP$

$$Q_{\text{Alice+Bob}} = aQ_{\text{Bob}} = (ab)P$$

Q_{Alice} →

← Q_{Bob}

Private integer b

$Q_{\text{Bob}} = bP$

$$Q_{\text{Bob+Alice}} = bQ_{\text{Alice}} = (ba)P$$

Elliptic Curve Diffie–Hellman

Public information: point $P \in E$

Private integer a

$Q_{\text{Alice}} = aP$

$Q_{\text{Alice+Bob}} = aQ_{\text{Bob}}$
$= (ab)P$

ALICE

Q_{Alice} ⇢

⇠ Q_{Bob}

BOB

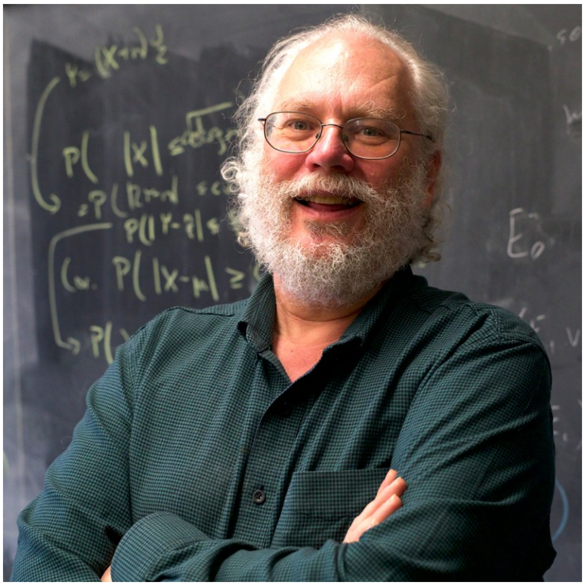
Private integer b

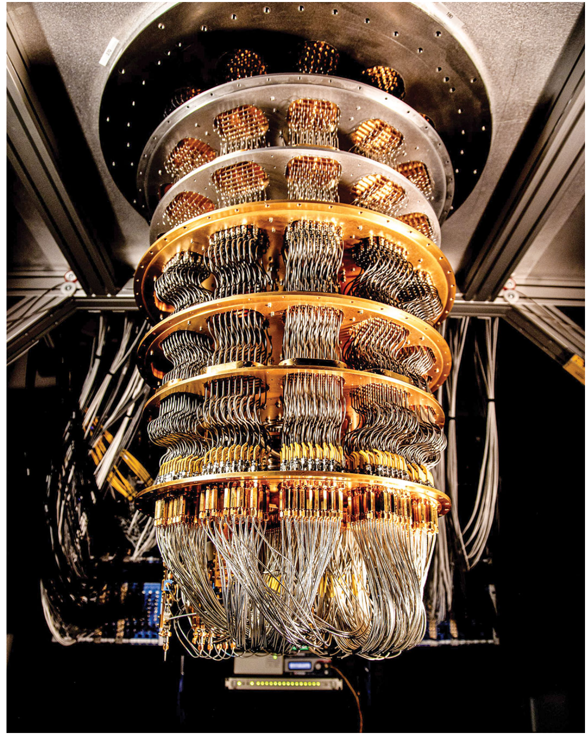
$Q_{\text{Bob}} = bP$

$Q_{\text{Bob+Alice}} = bQ_{\text{Alice}}$
$= (ba)P$

EVE

Shor's quantum algorithm





National Institute of Standards and Technology

NIST initiated a Post-Quantum Cryptography Standardization:

- December 20th, 2016: call to replace ECDH/RSA/…based on new hard problems:
  - finding short vectors in lattices
  - decoding for random linear codes
  - solving nonlinear systems of equations
  - finding isogenies between elliptic curves
  - …

National Institute of Standards and Technology

NIST initiated a Post-Quantum Cryptography Standardization:

- December 20th, 2016: call to replace ECDH/RSA/... based on new hard problems:
    - finding short vectors in lattices
    - decoding for random linear codes
    - solving nonlinear systems of equations
    - finding isogenies between elliptic curves
    - ...
- December 21st, 2017: 69 proposals accepted for round 1.
- January 30th, 2019: 26 remainders to round 2.
- July 22nd, 2020: 15 remainders to round 3.

National Institute of Standards and Technology

- July 5th, 2022:
  - 3 winners for digital signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+
  - 1 winner for public key exchange: CRYSTALS-Kyber
  - 4 alternatives for public key exchange to round 4: BIKE, Classical McEliece, HQC, SIKE

National Institute of Standards and Technology

- July 5th, 2022:
  - 3 winners for digital signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+
  - 1 winner for public key exchange: CRYSTALS-Kyber
  - 4 alternatives for public key exchange to round 4: BIKE, Classical McEliece, HQC, SIKE
- July 30th, 2022: SIKE†

National Institute of Standards and Technology

- July 5th, 2022:
  - 3 winners for digital signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+
  - 1 winner for public key exchange: CRYSTALS-Kyber
  - 4 alternatives for public key exchange to round 4: BIKE, Classical McEliece, HQC, SIKE
- July 30th, 2022: SIKE†
- March 11th, 2025: HQC was chosen for standardization

National Institute of Standards and Technology

- July 5th, 2022:
  - 3 winners for digital signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+
  - 1 winner for public key exchange: CRYSTALS-Kyber
  - 4 alternatives for public key exchange to round 4: BIKE, Classical McEliece, HQC, SIKE
- July 30th, 2022: SIKE†
- March 11th, 2025: HQC was chosen for standardization

New call for additional signature proposals in September 2022 to promote diversification!

- June 1st, 2023: 40 proposals accepted for round 1

National Institute of Standards and Technology

- July 5th, 2022:
  - 3 winners for digital signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+
  - 1 winner for public key exchange: CRYSTALS-Kyber
  - 4 alternatives for public key exchange to round 4: BIKE, Classical McEliece, HQC, SIKE
- July 30th, 2022: SIKE†
- March 11th, 2025: HQC was chosen for standardization

New call for additional signature proposals in September 2022 to promote diversification!

- June 1st, 2023: 40 proposals accepted for round 1
- October 24th, 2024: 14 remainders for round 2, including SQISign!

SQISign

SQISign still remains, the only isogeny-based submission!

- The good:
  - extremely compact (similar to current ECDSA)
  - fast verification
  - diversifies

SQISign

SQISign still remains, the only isogeny-based submission!

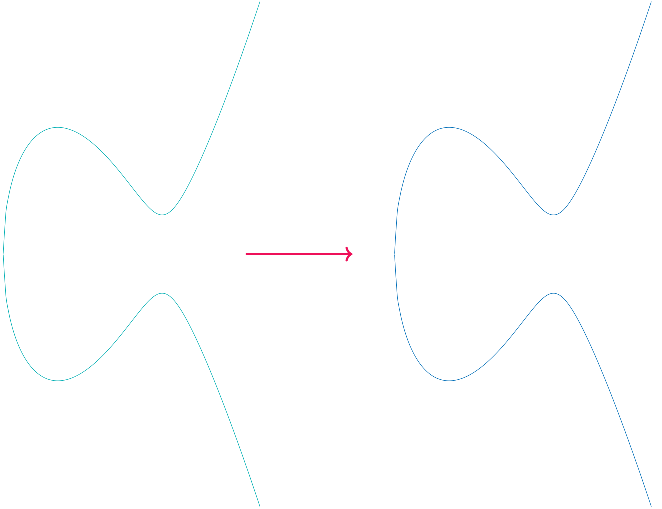
- The good:
  - extremely compact (similar to current ECDSA)
  - fast verification
  - diversifies
- The bad:
  - slow signing
  - doesn't scale well

SQISign

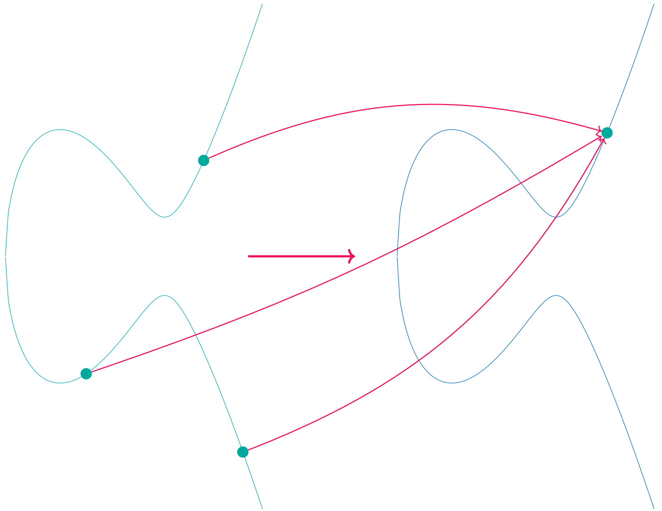
SQISign still remains, the only isogeny-based submission!

- The good:
  - extremely compact (similar to current ECDSA)
  - fast verification
  - diversifies
- The bad:
  - slow signing
  - doesn't scale well
- The ugly:
  - security assumption is complex and rather ad hoc

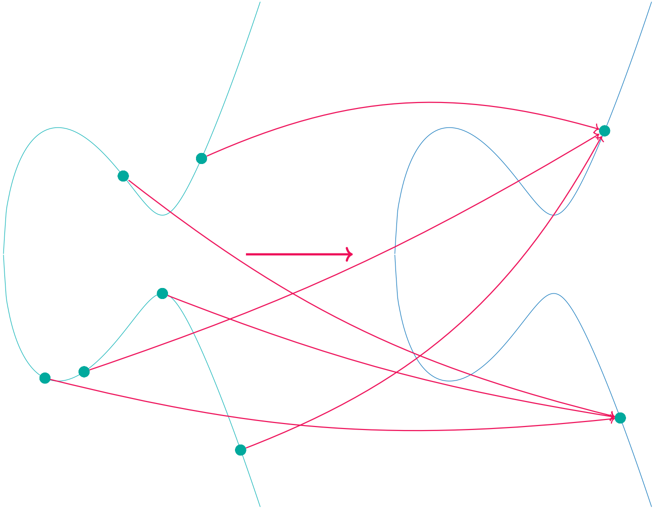
Isogenies



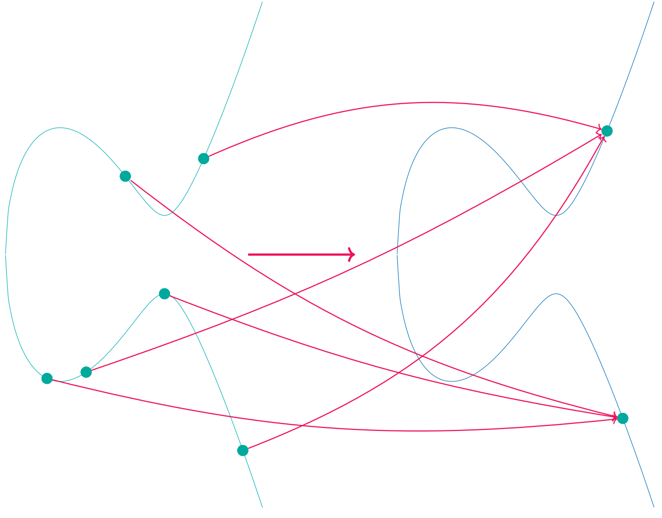
Isogenies



Isogenies

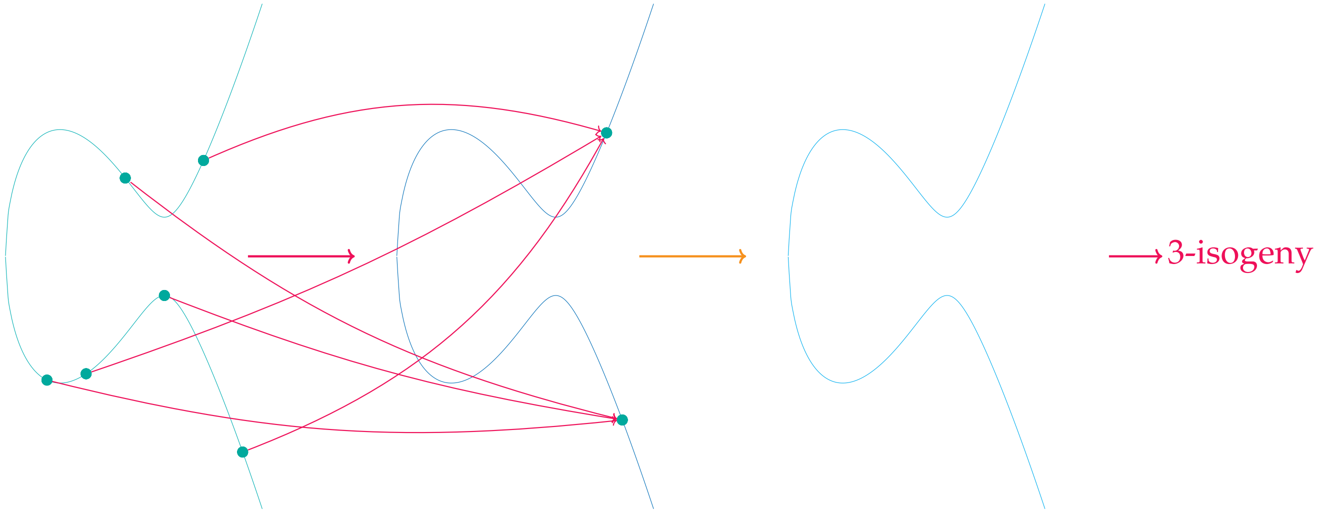


Isogenies

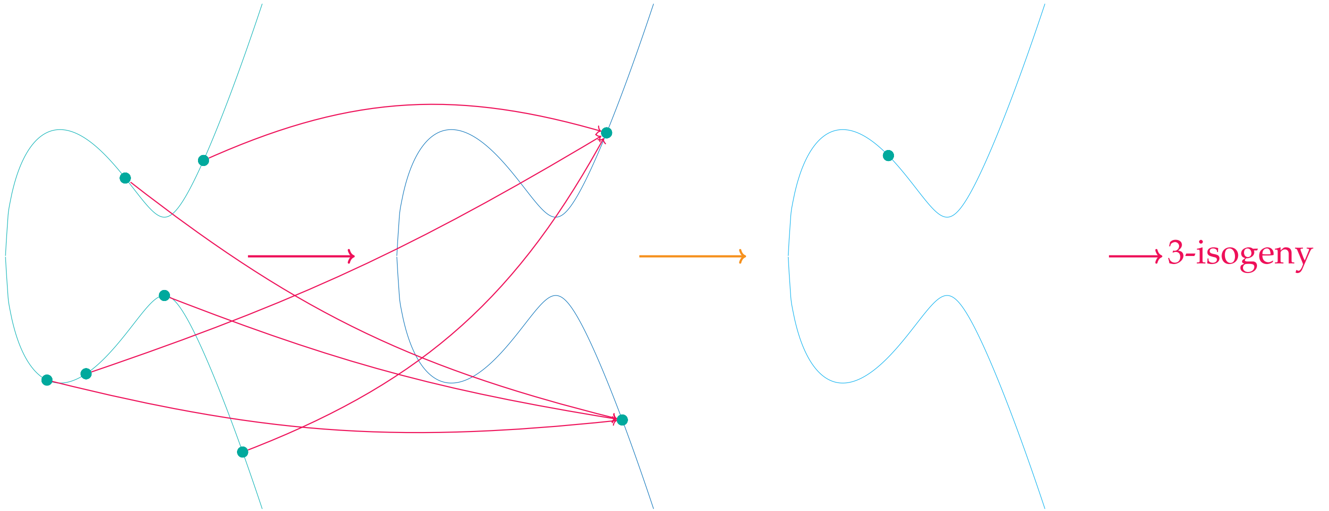


⟶ 3-isogeny

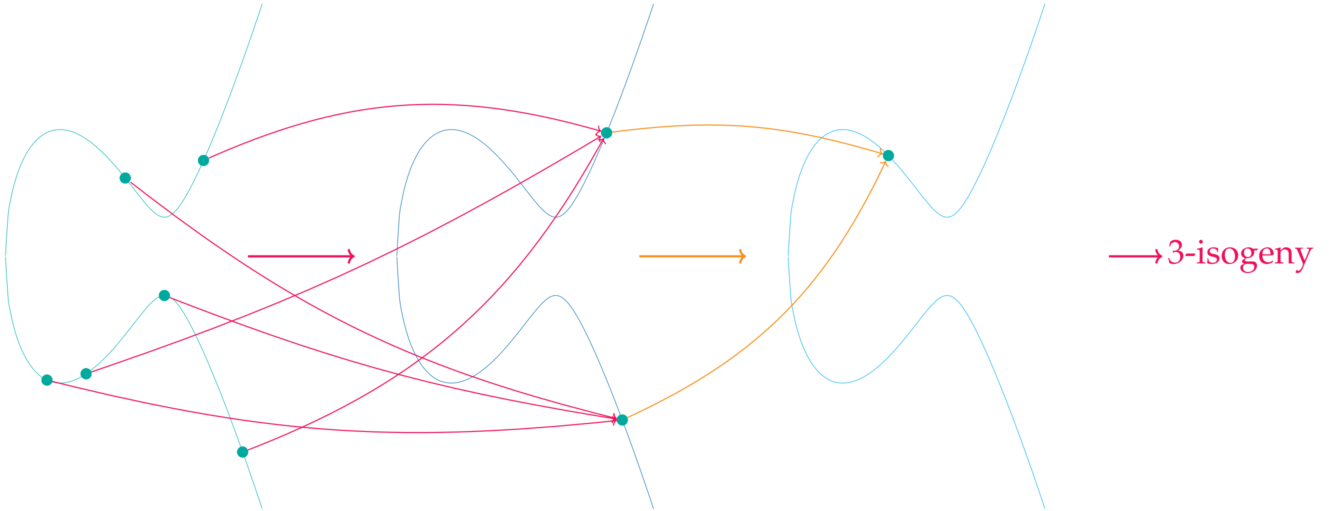
Isogenies



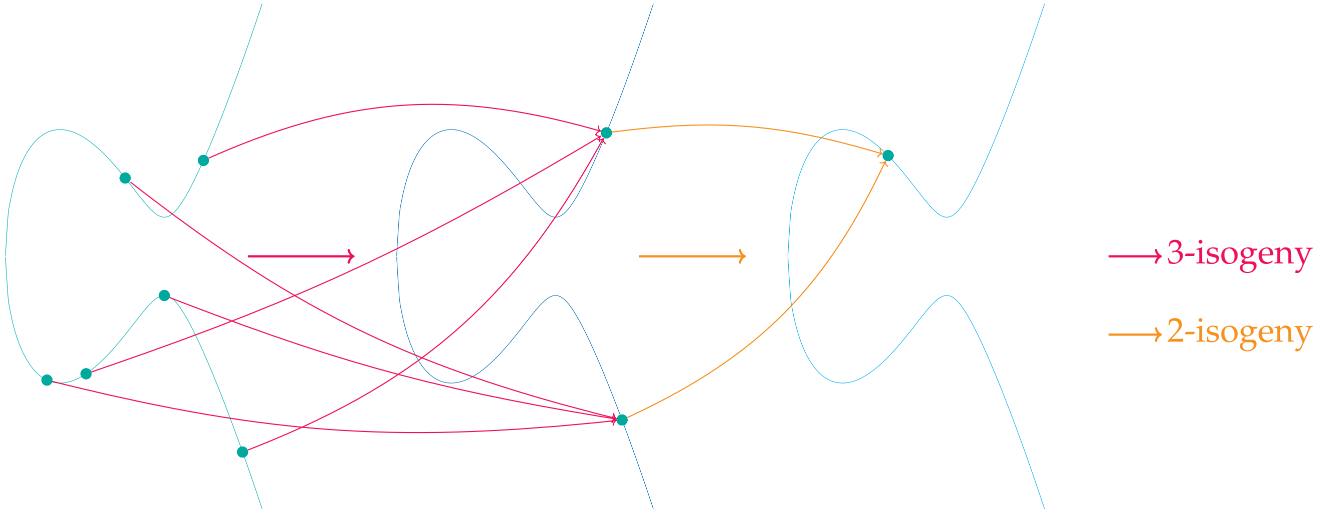
Isogenies



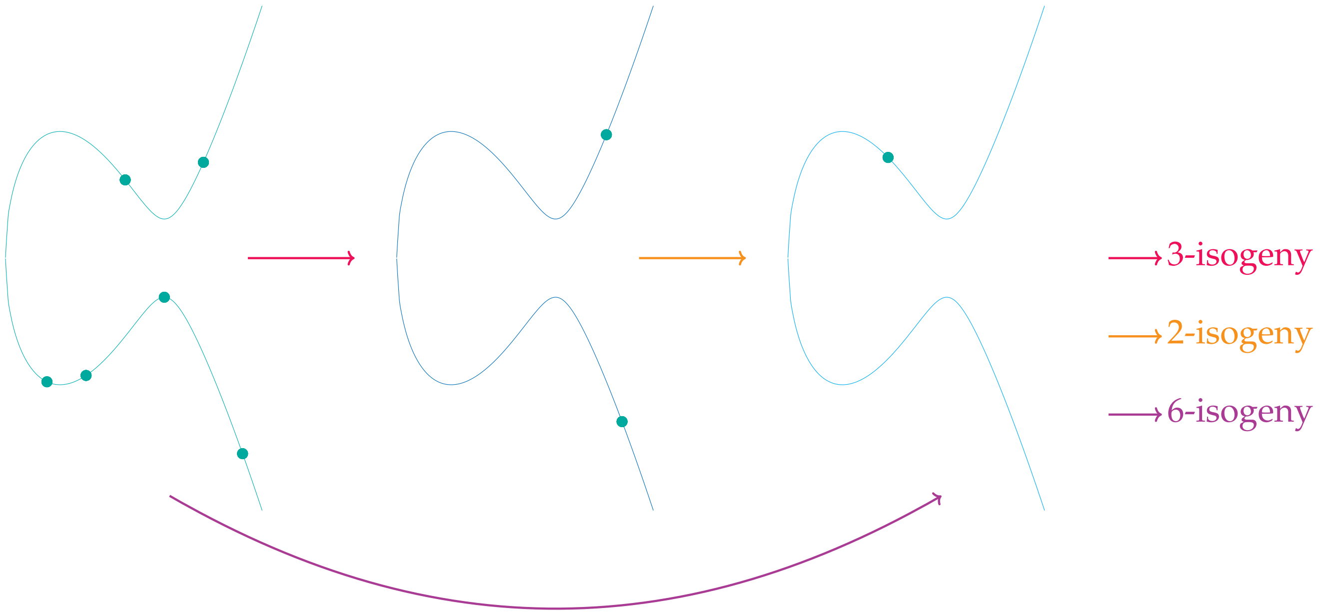
Isogenies



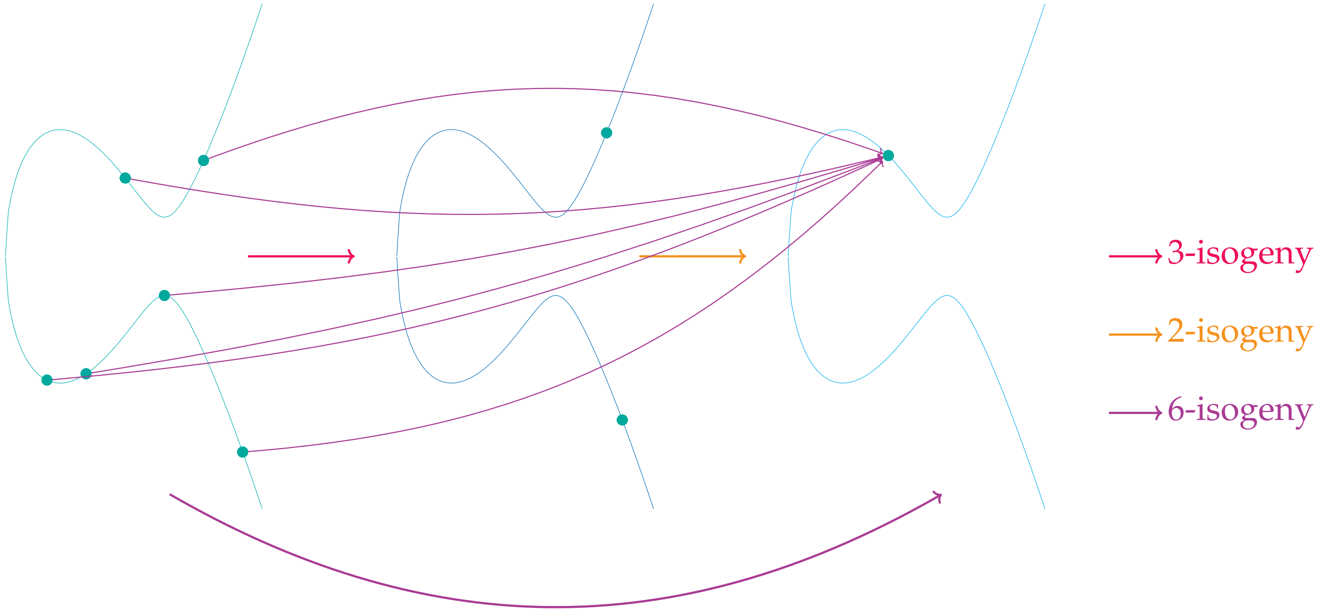
Isogenies



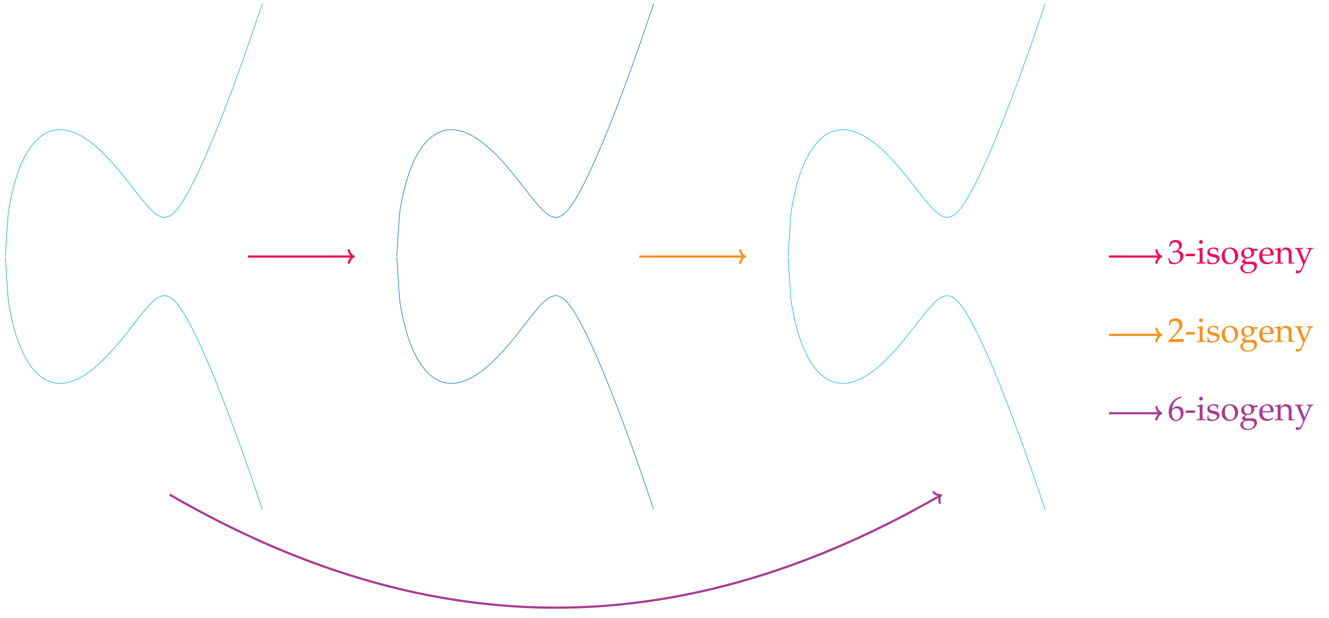
ISOGENIES



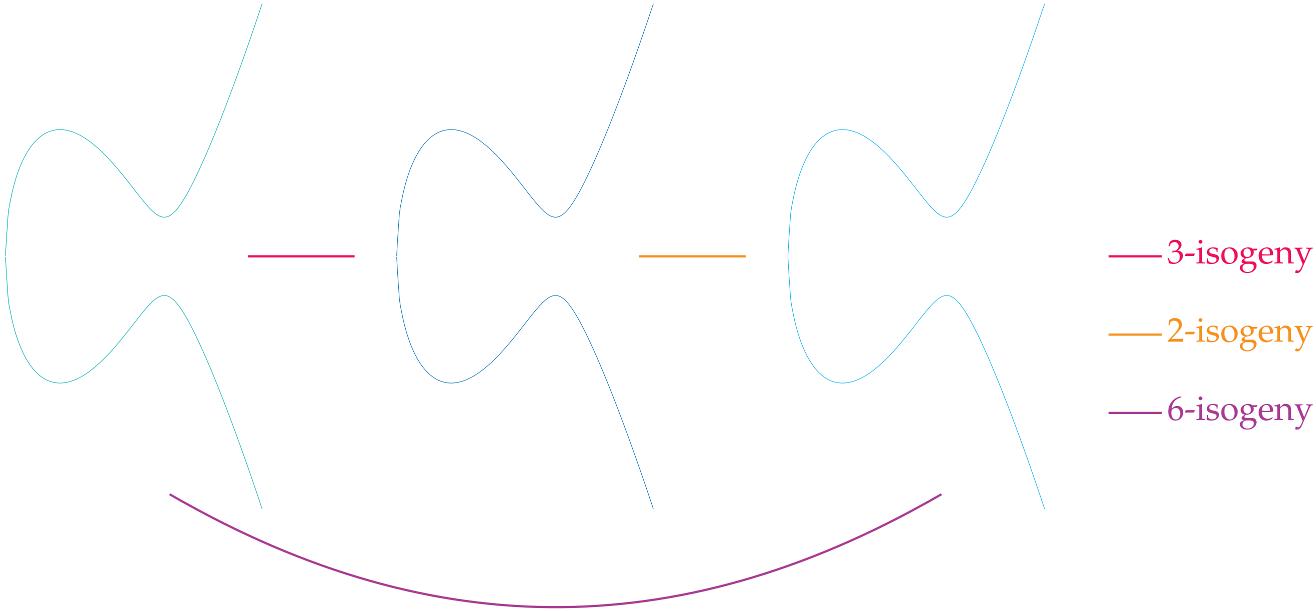
Isogenies



Isogenies



Isogenies



General:
Given E_1 and E_2, find *any* isogeny $\varphi : E_1 \to E_2$.

General:

Given E_1 and E_2, find *any* isogeny $\varphi : E_1 \to E_2$.

Attacks over $\mathbb{F}_q$:

- classical $\tilde{\mathcal{O}}(q^{1/4})$
- quantum $\tilde{\mathcal{O}}(q^{1/8})$

Hard problems

General:
Given E_1 and E_2, find *any* isogeny $\varphi : E_1 \to E_2$.

Attacks over $\mathbb{F}_q$:

- classical $\tilde{\mathcal{O}}(q^{1/4})$
- quantum $\tilde{\mathcal{O}}(q^{1/8})$

Often:
Given E_1 and E_2 supersingular, find an ℓ^n-isogeny $\varphi : E_1 \to E_2$.

General:

Given E_1 and E_2, find *any* isogeny $\varphi : E_1 \to E_2$.

Attacks over $\mathbb{F}_q$:

- classical $\tilde{\mathcal{O}}(q^{1/4})$
- quantum $\tilde{\mathcal{O}}(q^{1/8})$

Often:

Given E_1 and E_2 supersingular, find an ℓ^n-isogeny $\varphi : E_1 \to E_2$.

Isogenies need to be both represented and evaluated!

- representation typically by $\ker\varphi$ (i.e. all points mapped to neutral element ∞)
- evaluation typically by Vélu-type formulae (i.e. complexity $\mathcal{O}(\deg\varphi)$ or best case $\tilde{\mathcal{O}}(\sqrt{\deg\varphi})$)

Endomorphism-ring-finding problem:

Given E supersingular, find *all* endomorphisms $\varphi : E \to E$.

Endomorphism-ring-finding problem:

Given E supersingular, find *all* endomorphisms $\varphi : E \to E$.

One-endomorphism-finding problem:

Given E supersingular, find one (nontrivial) endomorphism $\varphi : E \to E$.

Endomorphism ring example

Assume $p \equiv 3 \bmod 4$ with

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x.$$

Endomorphism ring example

Assume $p \equiv 3 \bmod 4$ with

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x.$$

Multiplication-by-k-map:

$$\begin{aligned} [k] : E_0 &\to E_0 \\ P &\mapsto kP \end{aligned}$$

Endomorphism ring example

Assume $p \equiv 3 \bmod 4$ with

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x.$$

Multiplication-by-k-map:

$$\begin{aligned} [k] : E_0 &\to E_0 \\ P &\mapsto kP \end{aligned}$$

"Complex-multiplication-map":

$$\begin{aligned} \iota : E_0 &\to E_0 \\ (x, y) &\mapsto (-x, \sqrt{-1}y) \end{aligned}$$

Endomorphism ring example

Assume $p \equiv 3 \bmod 4$ with

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x.$$

Multiplication-by-k-map:

$$\begin{aligned}[k] : E_0 &\to E_0 \\ P &\mapsto kP\end{aligned}$$

"Complex-multiplication-map":

$$\begin{aligned}\iota : E_0 &\to E_0 \\ (x, y) &\mapsto (-x, \sqrt{-1}y)\end{aligned}$$

Frobenius map:

$$\begin{aligned}\pi : E_0 &\to E_0 \\ (x, y) &\mapsto (x^p, y^p)\end{aligned}$$

Deuring correspondence

We can concatenate endomorphisms:

$$\iota \circ \iota = [-1], \qquad \pi \circ \pi = [-p], \qquad \iota \circ \pi = [-1] \circ \pi \circ \iota$$

DEURING CORRESPONDENCE

We can concatenate endomorphisms:

$$\iota \circ \iota = [-1], \qquad \pi \circ \pi = [-p], \qquad \iota \circ \pi = [-1] \circ \pi \circ \iota$$

Under the Deuring correspondence, there is an isomorphism between the endomorphism ring of supersingular elliptic curves and maximal orders in the quaternion algebra $B_{p,\infty}$, i.e. $\mathbb{Q}(1, i, j, k)$ with

$$i^2 = -1, \qquad j^2 = -p, \qquad k = ij = -ji.$$

Deuring correspondence

We can concatenate endomorphisms:

$$\iota \circ \iota = [-1], \qquad \pi \circ \pi = [-p], \qquad \iota \circ \pi = [-1] \circ \pi \circ \iota$$

Under the Deuring correspondence, there is an isomorphism between the endomorphism ring of supersingular elliptic curves and maximal orders in the quaternion algebra $B_{p,\infty}$, i.e. $\mathbb{Q}(1, i, j, k)$ with

$$i^2 = -1, \qquad j^2 = -p, \qquad k = ij = -ji.$$

For the endomorphism ring of E_0, one possible identification is given by

$$[1] \mapsto 1, \qquad \iota \mapsto i, \qquad \pi \mapsto j$$

and then

$$\mathrm{End}(E_0) \cong \mathcal{O}_0 = \left\langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \right\rangle.$$

Deuring correspondence

Under the Deuring correspondence:

- the endomorphism ring $\mathrm{End}(E_0)$ of a supersingular elliptic curve E_0 is equivalent to a maximal order $\mathcal{O}_0$ in the quaternion algebra $B_{p,\infty}$
- an isogeny $\varphi : E_0 \to E_1$ is equivalent to a (connecting kernel) ideal I, which is a left ideal of $\mathcal{O}_0$ and a right ideal of $\mathcal{O}_1$, with

$$\mathrm{Norm}(I) = \deg \varphi$$

Deuring correspondence

Under the Deuring correspondence:

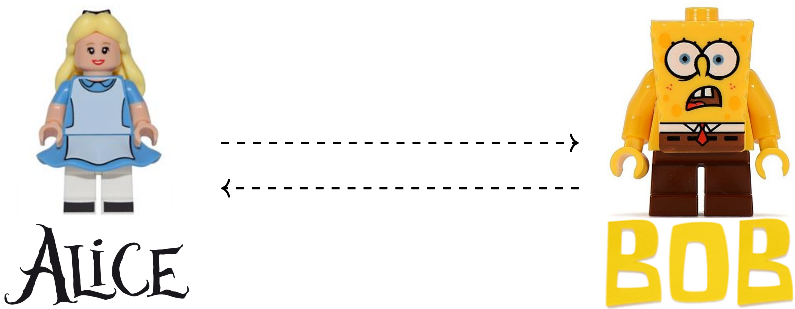
- the endomorphism ring $\mathrm{End}(E_0)$ of a supersingular elliptic curve E_0 is equivalent to a maximal order $\mathcal{O}_0$ in the quaternion algebra $B_{p,\infty}$
- an isogeny $\varphi : E_0 \to E_1$ is equivalent to a (connecting kernel) ideal I, which is a left ideal of $\mathcal{O}_0$ and a right ideal of $\mathcal{O}_1$, with

$$\mathrm{Norm}(I) = \deg \varphi$$

KLPT is an algorithmic tool which allows us to find equivalent ideals $J \sim I$ of different norm!

- The output is a lot larger than optimal, i.e. $\tilde{\mathcal{O}}(p^{3+\varepsilon})$

Isogeny-based Diffie–Hellman?



Isogeny-based Diffie–Hellman?

Public information: curve E

Isogeny-based Diffie–Hellman?

Public information: curve E

Private isogeny φ_a

Private isogeny φ_b

Isogeny-based Diffie–Hellman?

Public information: curve E

Private isogeny φ_a

$\varphi_a : E \to E_{\text{Alice}}$

Private isogeny φ_b

$\varphi_b : E \to E_{\text{Bob}}$

Isogeny-based Diffie–Hellman?

Public information: curve E

Private isogeny φ_a

$\varphi_a : E \to E_{\text{Alice}}$

E_{Alice} ⇢

⇠ E_{Bob}

Private isogeny φ_b

$\varphi_b : E \to E_{\text{Bob}}$

Isogeny-based Diffie–Hellman?

Public information: curve E

Private isogeny φ_a

$\varphi_a : E \to E_{\text{Alice}}$

$\varphi_{\text{Alice+Bob}} = \ldots ?$

E_{Alice} ⟶

⟵ E_{Bob}

Private isogeny φ_b

$\varphi_b : E \to E_{\text{Bob}}$

$\varphi_{\text{Bob+Alice}} = \ldots ?$

CSIDH

We can "make this commutative" by restricting to:

- supersingular elliptic curves defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$
- restricting to consider the endomorphism subring defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$, which is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field

CSIDH

We can "make this commutative" by restricting to:

- supersingular elliptic curves defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$
- restricting to consider the endomorphism subring defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$, which is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field

Theorem 1

The class group $cl(\mathcal{O})$ acts freely and transitively on the set of elliptic curves E with $End_{\mathbb{F}_p}(E) \cong \mathcal{O}$, where $\pi \in \mathcal{O}$ corresponds to $\mathbb{F}_p$-Frobenius.

CSIDH

We can “make this commutative” by restricting to:

- supersingular elliptic curves defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$
- restricting to consider the endomorphism subring defined over $\mathbb{F}_p$ instead of $\mathbb{F}_{p^2}$, which is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field

Theorem 1

The class group $cl(\mathcal{O})$ acts freely and transitively on the set of elliptic curves E with $End_{\mathbb{F}_p}(E) \cong \mathcal{O}$, where $\pi \in \mathcal{O}$ corresponds to $\mathbb{F}_p$-Frobenius.

This results in CSIDH:

- Alice samples $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ and act on E to get to $[\mathfrak{a}]E$
- Bob samples $[\mathfrak{b}] \in \mathrm{cl}(\mathcal{O})$ and act on E to get to $[\mathfrak{b}]E$
- they both end up on $[\mathfrak{a}\mathfrak{b}]E = [\mathfrak{b}\mathfrak{a}]E$

CSIDH SETTING

The good:

- extremely flexible due to abstraction as group action!

CSIDH SETTING

The good:

- extremely flexible due to abstraction as group action!

The bad:

- this is essentially the abelian hidden-shift problem so subexponential quantum attacks exist
  - (there's also some controversy about how high parameters should be for this)

CSIDH SETTING

The good:

- extremely flexible due to abstraction as group action!

The bad:

- this is essentially the abelian hidden-shift problem so subexponential quantum attacks exist
  - (there's also some controversy about how high parameters should be for this)
- despite speedups and the fact that everything happens over $\mathbb{F}_p$, it's quite slow:
  - you can't randomly sample from $\mathrm{cl}(\mathcal{O})$, so we resort to ideals of the form

$$(3, \pi \pm 1)^{e_1}(5, \pi \pm 1)^{e_2} \dots (587, \pi \pm 1)^{e_{74}}$$

with $e_i \in [-5; 5]$, corresponding to an isogeny of degree (at most)

$$(3 \cdot 5 \cdot \dots \cdot 587)^5$$

SIDH commutative diagram

- Alice and Bob choose (public) bases $\langle P_A, Q_A\rangle = E[2^a]$ and $\langle P_B, Q_B\rangle = E[3^b]$

SIDH commutative diagram

- Alice and Bob choose (public) bases $\langle P_A, Q_A \rangle = E[2^a]$ and $\langle P_B, Q_B \rangle = E[3^b]$
- Alice chooses φ_a such that $\ker \varphi_a = \langle P_A + s_a Q_a \rangle$
- Bob chooses φ_b such that $\ker \varphi_b = \langle P_B + s_b Q_b \rangle$

SIDH commutative diagram

- Alice and Bob choose (public) bases $\langle P_A, Q_A \rangle = E[2^a]$ and $\langle P_B, Q_B \rangle = E[3^b]$
- Alice chooses φ_a such that $\ker \varphi_a = \langle P_A + s_a Q_a \rangle$
- Bob chooses φ_b such that $\ker \varphi_b = \langle P_B + s_b Q_b \rangle$
- Alice also shares $\varphi_a(P_B), \varphi_a(Q_B)$ and Bob shares $\varphi_b(P_A), \varphi_b(Q_A)$!

SIDH COMMUTATIVE DIAGRAM

- Alice and Bob choose (public) bases $\langle P_A, Q_A \rangle = E[2^a]$ and $\langle P_B, Q_B \rangle = E[3^b]$
- Alice chooses φ_a such that $\ker \varphi_a = \langle P_A + s_a Q_a \rangle$
- Bob chooses φ_b such that $\ker \varphi_b = \langle P_B + s_b Q_b \rangle$
- Alice also shares $\varphi_a(P_B), \varphi_a(Q_B)$ and Bob shares $\varphi_b(P_A), \varphi_b(Q_A)$!

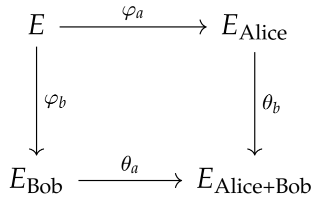
$$\begin{array}{ccc} E & \xrightarrow{\varphi_a} & E_{\text{Alice}} \\ \downarrow{\scriptstyle \varphi_b} & & \downarrow{\scriptstyle \theta_b} \\ E_{\text{Bob}} & \xrightarrow{\theta_a} & E_{\text{Alice+Bob}} \end{array}$$

with

- $\ker \theta_a = \langle \varphi_b(P_A) + s_a \varphi_b(Q_A) \rangle$
- $\ker \theta_b = \langle \varphi_a(P_B) + s_b \varphi_a(Q_B) \rangle$

SIDH commutative diagram

- Alice and Bob choose (public) bases $\langle P_A, Q_A \rangle = E[2^a]$ and $\langle P_B, Q_B \rangle = E[3^b]$
- Alice chooses φ_a such that $\ker \varphi_a = \langle P_A + s_a Q_a \rangle$
- Bob chooses φ_b such that $\ker \varphi_b = \langle P_B + s_b Q_b \rangle$
- Alice also shares $\varphi_a(P_B), \varphi_a(Q_B)$ and Bob shares $\varphi_b(P_A), \varphi_b(Q_A)$!



with

- $\ker \theta_a = \langle \varphi_b(P_A) + s_a \varphi_b(Q_A) \rangle$
- $\ker \theta_b = \langle \varphi_a(P_B) + s_b \varphi_a(Q_B) \rangle$
- $\ker(\theta_a \circ \varphi_b) = \ker(\theta_b \circ \varphi_a) = \langle P_A + s_a Q_A, P_B + s_b Q_b \rangle$

Kani's lemma

Lemma.[Ernst Kani, 1997]
Let $\mathbf{f} = (f, H_1, H_2)$ be an isogeny diamond configuration of order N from E_1 to E_2 and put $n = N/d$ and $k_i = n_i/d$, where $d = (n_1, n_2)$ and $n_i = \#H_i$. Then f factors (uniquely) over $[d]$, i.e. $f = \bar{f} \circ [d]$, and there is a unique reducible anti-isometry $\psi = \psi_{\mathbf{f}} : E_1[N] \to E_2[N]$ such that

$$\psi(k_1 x_1 + k_2 x_2) = \bar{f}(x_2 - x_1), \quad \forall x_i \in \widetilde{H}_i = [n]^{-1}(H_i),$$

and every reducible anti-isometry is of this form. Furthermore, if $\mathbf{f}' = (f', H_1', H_2')$ is another isogeny diamond configuration, then we have $\psi_{\mathbf{f}} = \psi_{\mathbf{f}'} \iff \mathbf{f} \sim \mathbf{f}'$.

Kani's lemma

Consider the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\beta} & E_3 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\gamma} \\ E_2 & \xrightarrow{\delta} & E_4 \end{array}$$

with $\deg \alpha = \deg \gamma$ and $\deg \beta = \deg \delta$

KANI'S LEMMA

Consider the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\beta} & E_3 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\gamma} \\ E_2 & \xrightarrow{\delta} & E_4 \end{array}$$

with $\deg \alpha = \deg \gamma$ and $\deg \beta = \deg \delta$, then

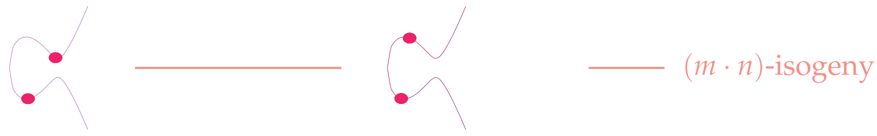
$$\Phi : E_2 \times E_3 \to E_1 \times E_4$$
$$(P, Q) \mapsto \begin{pmatrix} \hat{\alpha} & \hat{\beta} \\ -\delta & \gamma \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

is a $(\deg \alpha + \deg \beta, \deg \alpha + \deg \beta)$-isogeny between principally polarised abelian surfaces with

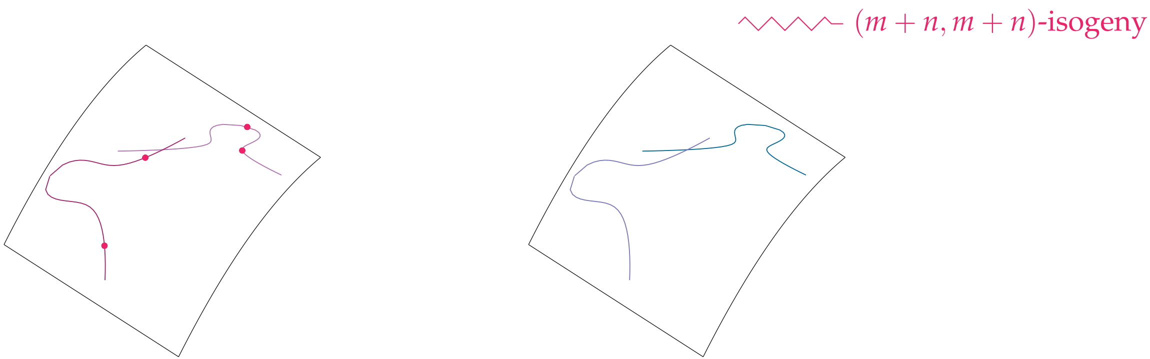
$$\ker \Phi = \{(\alpha(P), \beta(P)) \mid P \in E_1[\deg \alpha + \deg \beta]\}.$$

KANI'S LEMMA APPLIED

Given the one-dimensional isogeny



this determines the two-dimensional isogeny



Attack on SIDH/SIKE

Assume that

- Alice computes a 2^a-isogeny
- Bob computes a 3^b-isogeny $\varphi_B : E \to E_B$ and shares $\varphi_B(P_A), \varphi_B(Q_A)$ as well
- $2^a - 3^b = c^2$ is a perfect square (for simplification purposes)

Attack on SIDH/SIKE

Assume that

- Alice computes a 2^a-isogeny
- Bob computes a 3^b-isogeny $\varphi_B : E \to E_B$ and shares $\varphi_B(P_A), \varphi_B(Q_A)$ as well
- $2^a - 3^b = c^2$ is a perfect square (for simplification purposes)

Consider the diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi_B} & E_B \\ \downarrow{\scriptstyle [c]} & & \downarrow{\scriptstyle [c]} \\ E & \xrightarrow{\varphi_B} & E_B \end{array}$$

where $3^b + c^2 = 2^a$, giving rise to the $(2^a, 2^a)$-isogeny with (known!) kernel

$$\ker \Phi = \{(cP, \varphi_B(P) \mid P \in E[2^a]\}$$

Attack on SIDH/SIKE

To complete the attack:

- compute the $(2^a, 2^a)$-isogeny
  - this can be done by decomposing as a chain of $(2,2)$-isogenies of length a
- extract φ_B from this since this isogeny is given by

$$(P, Q) \mapsto \begin{pmatrix} [c] & \hat{\varphi}_b \\ -\varphi_b & [c] \end{pmatrix}$$

ATTACK ON SIDH/SIKE

To complete the attack:

- compute the $(2^a, 2^a)$-isogeny
  - this can be done by decomposing as a chain of $(2,2)$-isogenies of length a
- extract φ_B from this since this isogeny is given by

$$(P, Q) \mapsto \begin{pmatrix} [c] & \hat{\varphi}_b \\ -\varphi_b & [c] \end{pmatrix}$$

What if $3^b - 2^a$ is not a square?

- in SIKE there are tricks because E_0 was used so nontrivial endomorphisms can be used instead of $[c]$

Attack on SIDH/SIKE

To complete the attack:

- compute the $(2^a, 2^a)$-isogeny
  - this can be done by decomposing as a chain of $(2,2)$-isogenies of length a
- extract φ_B from this since this isogeny is given by

$$(P, Q) \mapsto \begin{pmatrix} [c] & \hat{\varphi}_b \\ -\varphi_b & [c] \end{pmatrix}$$

What if $3^b - 2^a$ is not a square?

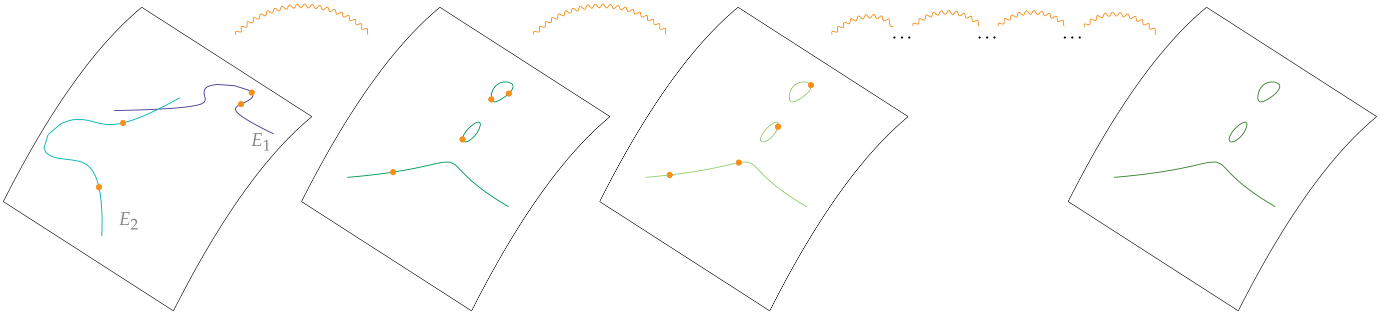
- in SIKE there are tricks because E_0 was used so nontrivial endomorphisms can be used instead of $[c]$
- more generally, you can consider an 8-dimensional isogeny

$$E^4 \times E_B^4 \to E^4 \times E_B^4$$

and take the easy isogenies $[c_1], [c_2], [c_3], [c_4]$ since those exist such that

$$3^b - 2^a = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

Different types of abelian surfaces



Isogeny representations

Several ways to represent degree-d isogeny φ:

- as a rational map $f(x)$, where

  $$\varphi : (x, y) \mapsto (f(x), y \cdot g(x))$$

  and d need be smooth to write as composition

Isogeny representations

Several ways to represent degree-d isogeny φ:

- as a rational map $f(x)$, where

  $$\varphi : (x, y) \mapsto (f(x), y \cdot g(x))$$

  and d need be smooth to write as composition
- as $\ker \varphi$, typically through generators, but computations must be feasible
  - e.g. Vélu for large prime d cannot be done

Isogeny representations

Several ways to represent degree-d isogeny φ:

- as a rational map $f(x)$, where
$$\varphi : (x, y) \mapsto (f(x), y \cdot g(x))$$
and d need be smooth to write as composition
- as $\ker \varphi$, typically through generators, but computations must be feasible
  - e.g. Vélu for large prime d cannot be done
- as kernel ideal I via Deuring correspondence but
  - must be smoothened via KLPT to be useful
  - requires knowledge of endomorphism ring

New isogeny representation

Theorem 2

Let $\varphi : E_1 \to E_2$ *be an isogeny of (known) degree* d*, with interpolation data*

$$P_1, \varphi(P_1), \ldots, P_r, \varphi(P_r)$$

such that $\langle P_1, \ldots P_r \rangle$ *has (smooth) order* $N > 4d$*. Then there exists a polynomial-time algorithm for evaluating* φ*.*

New isogeny representation

Theorem 2

Let $\varphi : E_1 \to E_2$ *be an isogeny of (known) degree* d*, with interpolation data*

$$P_1, \varphi(P_1), \ldots, P_r, \varphi(P_r)$$

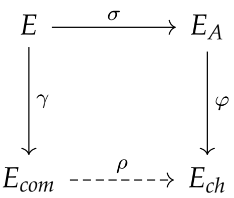
such that $\langle P_1, \ldots P_r \rangle$ *has (smooth) order* $N > 4d$*. Then there exists a polynomial-time algorithm for evaluating* φ*.*

Biggest issue is that polynomial-time is "theoretical":

- sometimes we need to use isogenies in dimension 4 and 8, with the dimension being an exponent in the complexity
- ideally we have parameters such that dimension is 2 and $N = 2^a$

SQISign

Consider the commitment scheme

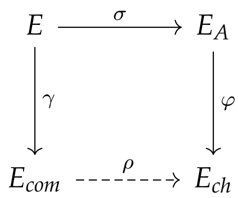


where

- σ is the secret key, γ is the commitment, φ is the challenge

SQISign

Consider the commitment scheme



where

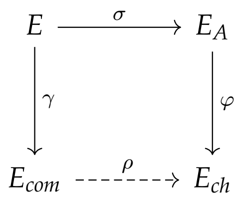
- σ is the secret key, γ is the commitment, φ is the challenge

Naively:

- respond with $\rho = \varphi \circ \sigma \circ \hat{\gamma}$ but this reveals σ!

SQISign

Consider the commitment scheme



where

- σ is the secret key, γ is the commitment, φ is the challenge

Naively:

- respond with $\rho = \varphi \circ \sigma \circ \hat{\gamma}$ but this reveals σ!

What works:

- smooth this ρ with KLPT to a different-degree isogeny
- doesn't scale well and zero-knowledge assumption is ad hoc

SQISign higher dimensions

SQISignHD:

- take $\rho : E_{com} \to E_{ch}$ represented by interpolation data for (random) small-degree isogeny

SQISign higher dimensions

SQISignHD:

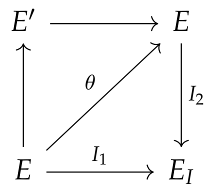
- take $\rho : E_{com} \to E_{ch}$ represented by interpolation data for (random) small-degree isogeny
- scales better and cleaner security reduction
- verification is slower since requires dimension 4

SQISIGN HIGHER DIMENSIONS

SQISignHD:

- take $\rho : E_{com} \to E_{ch}$ represented by interpolation data for (random) small-degree isogeny
- scales better and cleaner security reduction
- verification is slower since requires dimension 4

More tricks on the quaternion side, Clapoti:

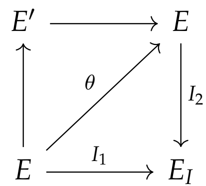


SQISign higher dimensions

SQISignHD:

- take $\rho : E_{com} \to E_{ch}$ represented by interpolation data for (random) small-degree isogeny
- scales better and cleaner security reduction
- verification is slower since requires dimension 4

More tricks on the quaternion side, Clapoti:



- given an endomorphism $\theta : E \to E$ and an ideal I, we can find two equivalent ideals such that

$$I_1 \sim I_2 \sim I, \qquad \mathrm{Norm}(I_1) + \mathrm{Norm}(I_2) = 2^a,$$

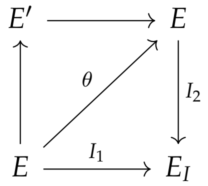
allowing us to compute the isogeny from I without smoothening!

SQISign higher dimensions

SQISignHD:

- take $\rho : E_{com} \to E_{ch}$ represented by interpolation data for (random) small-degree isogeny
- scales better and cleaner security reduction
- verification is slower since requires dimension 4

More tricks on the quaternion side, Clapoti:



- given an endomorphism $\theta : E \to E$ and an ideal I, we can find two equivalent ideals such that

$$I_1 \sim I_2 \sim I, \qquad \mathrm{Norm}(I_1) + \mathrm{Norm}(I_2) = 2^a,$$

  allowing us to compute the isogeny from I without smoothening!
- SQISign2D-East, SQISign2D-West, SQIPrime2D with verification in dimension 2!

Current state

One-dimensional isogeny-based cryptography is rather well understood, apart from perhaps

- we can't generate a supersingular E without knowing its endomorphism ring
- KLPT could be improved since the resulting isogeny degree is too large

Current state

One-dimensional isogeny-based cryptography is rather well understood, apart from perhaps

- we can't generate a supersingular E without knowing its endomorphism ring
- KLPT could be improved since the resulting isogeny degree is too large

Higher-dimensional isogenies have given us tools to make new protocols:

- FESTA, QFESTA
- SCALLOP-HD
- SQISignHD, SQISign2D-East, SQISign2D-West, SQIPrime2D
- PRISM
- ...

All of these protocols use a mixture between one-dimensional and higher-dimensional...

Future paths: computations?

Computational cost:

- efficient formulae exist for
  - isogenies of degree 2 and 3 in dimension 2
  - isogenies of degree 2 in dimension 4
- workable formulae exist for
  - isogenies of degree ℓ in dimension 2

Future paths: computations?

Computational cost:

- efficient formulae exist for
  - isogenies of degree 2 and 3 in dimension 2
  - isogenies of degree 2 in dimension 4
- workable formulae exist for
  - isogenies of degree ℓ in dimension 2

Would be nice to have:

- more efficient formulae for other degrees/dimensions
  - given how $\tilde{\mathcal{O}}(\sqrt{\deg \varphi})$ in dimension 1, can we expect $\tilde{\mathcal{O}}((\deg \varphi)^{g/2})$ in dimension g?
- constant time for protocols that need it

Future paths: protocols and algorithms in HD?

General question:

- Is it worth it to consider cryptographic protocols strictly in dimension $g > 1$?

Future paths: protocols and algorithms in HD?

General question:

- Is it worth it to consider cryptographic protocols strictly in dimension $g > 1$?

For this we will need new and efficient algorithms:

- faster isogenies in higher dimensions
- algorithmic tools similar to dimension 1:
  - KLPT^2 exists now!

Future paths: protocols and algorithms in HD?

KLPT^2 uses the Ibukiyama–Katsura–Oort correspondence:

- fix a supersingular E_0 with endomorphism ring $\mathcal{O}_0$, then the superspecial principally polarised abelian surfaces (up to polarised isomorphism) are 1–1 with the set

$$\mathrm{Mat}(E_0 \times E_0) := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_{>0}, r \in \mathcal{O}_0, st - r\bar{r} = 1 \right\} \quad \subset \mathrm{GL}_2(\mathcal{O}_0),$$

  up to the following equivalence relation:

$$g_1 \sim g_2 \in \mathrm{Mat}(E_0 \times E_0) \quad \Leftrightarrow \quad \exists u \in \mathrm{GL}_2(\mathcal{O}_0), \quad u^* g_1 u = g_2$$

Future paths: protocols and algorithms in HD?

KLPT^2 uses the Ibukiyama–Katsura–Oort correspondence:

- fix a supersingular E_0 with endomorphism ring $\mathcal{O}_0$, then the superspecial principally polarised abelian surfaces (up to polarised isomorphism) are 1–1 with the set

$$\mathrm{Mat}(E_0 \times E_0) := \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}, \quad s, t \in \mathbb{Z}_{>0}, r \in \mathcal{O}_0, st - r\bar{r} = 1 \right\} \quad \subset \mathrm{GL}_2(\mathcal{O}_0),$$

  up to the following equivalence relation:

$$g_1 \sim g_2 \in \mathrm{Mat}(E_0 \times E_0) \quad \Leftrightarrow \quad \exists u \in \mathrm{GL}_2(\mathcal{O}_0), \quad u^* g_1 u = g_2$$

Theorem 3 (KLPT^2)

There exists a polynomial-time algorithm which upon input $g_1, g_2 \in \mathrm{Mat}(E_0 \times E_0)$ and a prime number $\ell \neq p$, under plausible heuristic assumptions, returns $\gamma \in \mathrm{M}_2(\mathcal{O}_0)$ such that

$$\gamma^* g_2 \gamma = \ell^e g_1$$

where $\ell^e \in O(p^{25+\varepsilon})$.

Future paths: graph theory?

One can turn (supersingular) elliptic curves and isogenies into graphs where

- vertices are elliptic curves (up to isomorphism)
- edges are isogenies (can be made undirected due to dual isogenies)

Future paths: graph theory?

One can turn (supersingular) elliptic curves and isogenies into graphs where

- vertices are elliptic curves (up to isomorphism)
- edges are isogenies (can be made undirected due to dual isogenies)

In dimension 1 these are well understood and have nice properties:

- connectedness, $(\ell + 1)$-regular, Ramanujan (rapid mixing), etc

Future paths: graph theory?

One can turn (supersingular) elliptic curves and isogenies into graphs where

- vertices are elliptic curves (up to isomorphism)
- edges are isogenies (can be made undirected due to dual isogenies)

In dimension 1 these are well understood and have nice properties:

- connectedness, $(\ell + 1)$-regular, Ramanujan (rapid mixing), etc

When going to dimension $g > 1$ we definitely want

- supersingular $\rightarrow$ superspecial
- elliptic curves $\rightarrow$ principally polarised abelian varieties

Future paths: graph theory?

In dimension $g > 1$ there are issues if we generalize geometrically/“naively”:

- lots of small cycles making it awkward to walk around “randomly” in the graph
  - two isogenies with kernel $(\mathbb{Z}/(\ell\mathbb{Z}))^2$ can concatenate to one with kernel
    $$\mathbb{Z}/(\ell^2\mathbb{Z}) \times (\mathbb{Z}/(\ell\mathbb{Z}))^2$$
    instead of $(\mathbb{Z}/(\ell^2\mathbb{Z}))^2$

Future paths: graph theory?

In dimension $g > 1$ there are issues if we generalize geometrically/"naively":

- lots of small cycles making it awkward to walk around "randomly" in the graph
  - two isogenies with kernel $(\mathbb{Z}/(\ell\mathbb{Z}))^2$ can concatenate to one with kernel
$$\mathbb{Z}/(\ell^2\mathbb{Z}) \times (\mathbb{Z}/(\ell\mathbb{Z}))^2$$
    instead of $(\mathbb{Z}/(\ell^2\mathbb{Z}))^2$
- rapid mixing properties are okay but not as good
- several distinct types of nodes creating (connected?) subgraphs

FUTURE PATHS: GRAPH THEORY?

In dimension $g > 1$ there are issues if we generalize geometrically/"naively":

- lots of small cycles making it awkward to walk around "randomly" in the graph
  - two isogenies with kernel $(\mathbb{Z}/(\ell\mathbb{Z}))^2$ can concatenate to one with kernel
    $$\mathbb{Z}/(\ell^2\mathbb{Z}) \times (\mathbb{Z}/(\ell\mathbb{Z}))^2$$
    instead of $(\mathbb{Z}/(\ell^2\mathbb{Z}))^2$
- rapid mixing properties are okay but not as good
- several distinct types of nodes creating (connected?) subgraphs

On the bright side, we do have $\mathcal{O}(p^{2g-1})$ vertices:

- in dimension 1 we have $p/12 + \varepsilon$
- in dimension 2 we have $p^3/2880 + \mathcal{O}(p^2)$
- ...

Future paths: graph theory?

Alternative construction for graph:

- let L be a totally real field with strict class number one, e.g. $L = \mathbb{Q}(\sqrt{5})$, and ring of integers $\mathcal{O}_L$, e.g. $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
- fix a supersingular E_0 with endomorphism ring $\mathcal{O}_0$

Future paths: graph theory?

Alternative construction for graph:

- let L be a totally real field with strict class number one, e.g. $L = \mathbb{Q}(\sqrt{5})$, and ring of integers $\mathcal{O}_L$, e.g. $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
- fix a supersingular E_0 with endomorphism ring $\mathcal{O}_0$
- consider the superspecial principally polarised abelian varieties with real multiplication, i.e.

$$(E^g, \iota : \mathcal{O}_L \to \operatorname{End}(E^g)),$$

  which are the vertices of our graph, with "starting vertex"

$$E \otimes_{\mathbb{Z}} \mathcal{O}_L$$

  and g is the degree of L
- the edges of our graph are given by right ideals I_i of $\mathcal{O}_0 \otimes \mathcal{O}_L$ and we can "walk" in our graph by computing

$$I_i \otimes_{\mathcal{O}_0 \otimes \mathcal{O}_L} (E \otimes_{\mathbb{Z}} \mathcal{O}_L)$$

Future paths: graph theory?

This alternative construction has a lot of the properties we desire:

- connected
- Ramanujan (so optimal rapid mixing)
- k-regular
- you can make it undirected and avoid loops
- avoid the small cycles from the geometric construction

Future paths: graph theory?

This alternative construction has a lot of the properties we desire:

- connected
- Ramanujan (so optimal rapid mixing)
- k-regular
- you can make it undirected and avoid loops
- avoid the small cycles from the geometric construction
- vertex set is(?) uniform
- the algebraic approach may make this easier to generalize KLPT

Future paths: graph theory?

This alternative construction has a lot of the properties we desire:

- connected
- Ramanujan (so optimal rapid mixing)
- k-regular
- you can make it undirected and avoid loops
- avoid the small cycles from the geometric construction
- vertex set is(?) uniform
- the algebraic approach may make this easier to generalize KLPT

The "downside" is that we have less vertices, namely

$$\approx 2\left(\frac{p}{4\pi^2}\right)^g d_L^{3/2}.$$

instead of $\mathcal{O}(p^{2g-1})$.

Isogenies: A brand new day

Despite the fall of SIDH/SIKE, things actually improved for the better!

- existing constructions got faster
- cleaner security assumptions
- new toolboxes for protocol constructions
- somewhat uncharted terrain with lots left to discover:
  - more protocols and optimized versions of the current ones
  - computational speedups
  - algebraic and graph-theoretical results

Isogenies: A brand new day

Despite the fall of SIDH/SIKE, things actually improved for the better!

- existing constructions got faster
- cleaner security assumptions
- new toolboxes for protocol constructions
- somewhat uncharted terrain with lots left to discover:
  - more protocols and optimized versions of the current ones
  - computational speedups
  - algebraic and graph-theoretical results

Isogeny-based cryptography is alive and well with more activity than ever!