The isogeny toolbox

Luca De Feo
IBM Research Zürich

July 12, 2024
AfricaCrypt, Douala, Cameroon

Why isogenies in 2024?

- Still the smallest keys;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;
- Credible alternative in case other pq-schemes fail;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;
- Credible alternative in case other pq-schemes fail;
- …but still a long way to go!

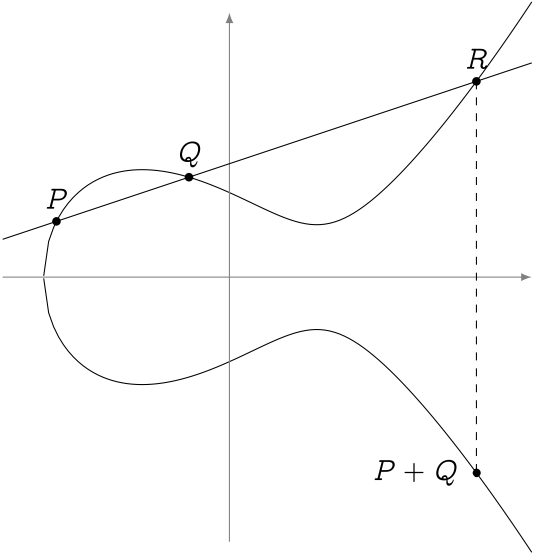
Elliptic curves

$$y^2 = x^3 + ax + b$$

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

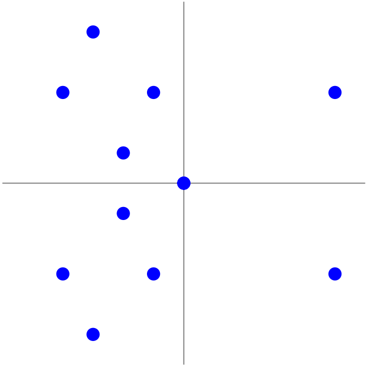


Isogenies = finite-kernel *algebraic* group morphisms: $E \to E'$

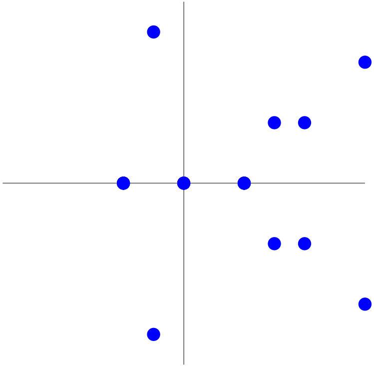
Endomorphisms = isogenies $E \to E$

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$

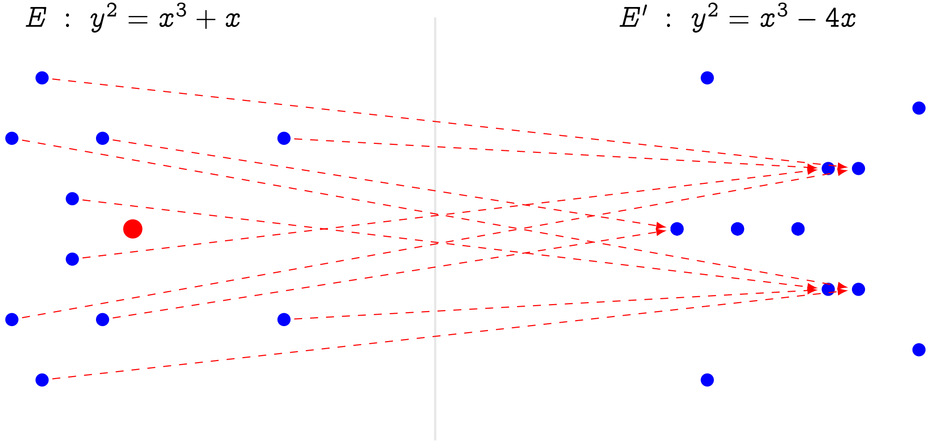


$E' : y^2 = x^3 - 4x$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y\frac{x^2 - 1}{x^2} \right)$$

Isogenies: an example over $\mathbb{F}_{11}$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Anatomy of an isogeny

$$\phi(x, y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{x^3 - x^2 - x + 1},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

Anatomy of an isogeny

degree

$$\phi(x, y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{x^3 - x^2 - x + 1},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

degree -1

Anatomy of an isogeny

degree

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{x^3 - x^2 - x + 1},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

kernel polynomial

Anatomy of an isogeny

degree

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{(x+1)(x-1)^2},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

kernel polynomial

Anatomy of an isogeny

degree

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{(x+1)(x-1)^2},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

Point of order 2

Two points of order 4

Anatomy of an isogeny

degree

$$\phi(x,y) = \left(\frac{x^4 - x^3 + 11x^2 + 9x + 12}{h(x)},\ y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1}\right)$$

$$h(x) = \prod_{P\in K\setminus\{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, \quad y\frac{x^5 - x^4 - 14x^3 - 26x^2 - 67x - 21}{x^5 - x^4 - 2x^3 + 2x^2 + x - 1} \right)$$

$$h(x) = \prod_{P \in K \setminus \{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, \qquad y\left(\frac{g(x)}{h(x)}\right)' \right)$$

$$h(x) = \prod_{P\in K\setminus\{0\}} \big(x - x(P)\big)$$

Anatomy of an isogeny

computed by Vélu–Elkies–Kohel formulas

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, \qquad y\left(\frac{g(x)}{h(x)}\right)' \right)$$

$$h(x) = \prod_{P\in K\setminus\{0\}} \big(x - x(P)\big)$$

Input: Finite kernel $K \subset E$ of order d;

Output: Rational fractions $\phi(x,y)$;

Complexity: $\tilde{O}(d)$ operations.

How many isogenies?

Finite subgroups of order d

$K \subset E$

$\longleftrightarrow$

Isogenies of degree d

$\phi : E \to E/K$

(up to composing with isomorphism)

How many isogenies?

Finite subgroups of order d ⟷ Isogenies of degree d

$$K \subset E$$

$$\phi : E \to E/K$$

(up to composing with isomorphism)

Examples:

If d is prime $\to$ at most $d+1$ possible kernels,

In general $\to$ at most $\approx d$ possible kernels.

The isogeny problem

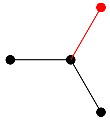
E E'

The isogeny problem

$$E \xrightarrow{\quad ?? \quad} E'$$

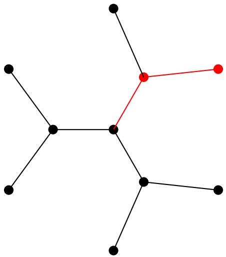
Isogeny graphs

$$\frac{x^2 + \cdots}{x + \cdots}$$



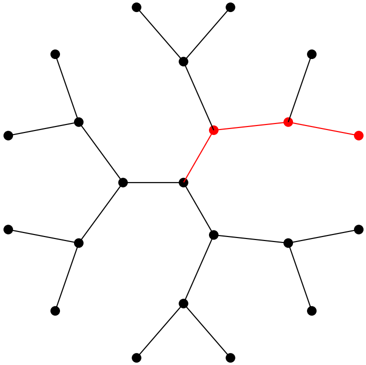
Isogeny graphs

$$\frac{x^2 + \cdots}{x + \cdots} \circ \frac{x^2 + \cdots}{x + \cdots}$$



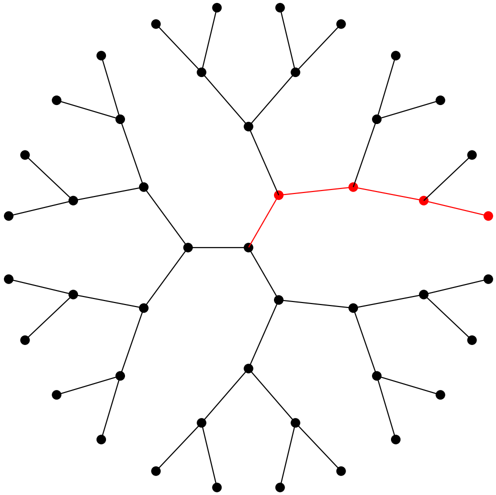
Isogeny graphs

$$\frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots}$$



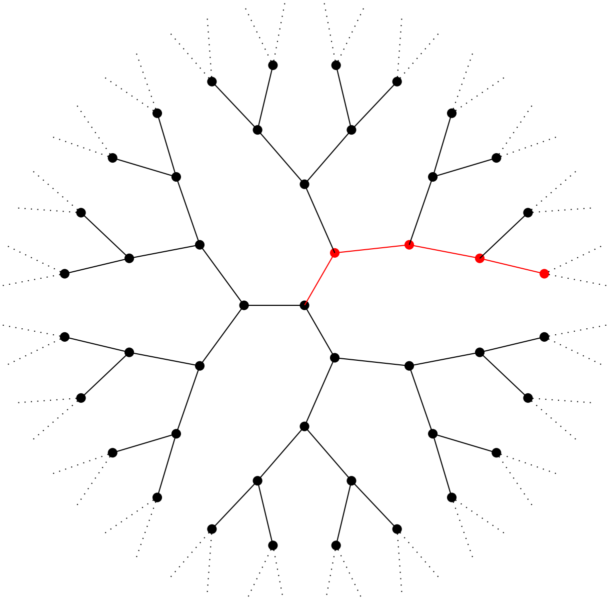
Isogeny graphs

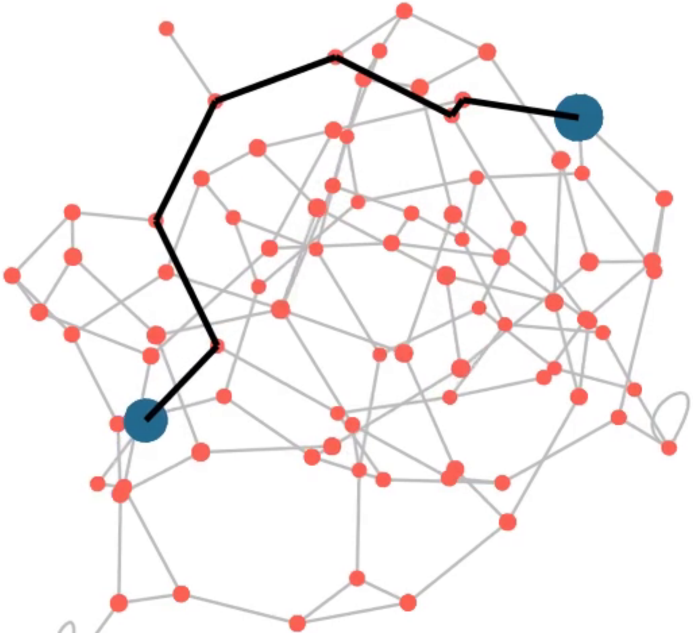
$$\frac{x^2+\cdots}{x+\cdots}\circ\frac{x^2+\cdots}{x+\cdots}\circ\frac{x^2+\cdots}{x+\cdots}\circ\frac{x^2+\cdots}{x+\cdots}$$



Isogeny graphs

$$\frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots} \circ \frac{x^2+\cdots}{x+\cdots}$$





The *smooth* criminals

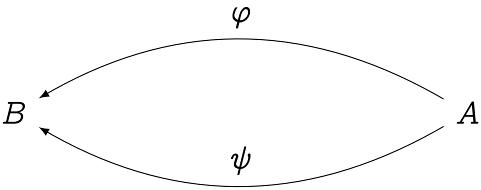
2006 Charles-Goren-Lauter hash function

2006 Couveignes-Rostovtsev-Stolbunov key exchange

2011 SIDH key exchange

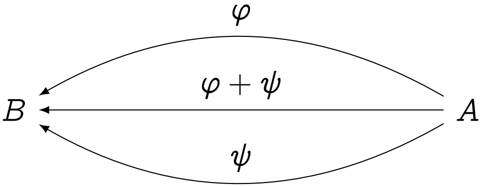
2018 CSIDH key exchange

Groups of isogenies



$$\varphi, \psi \in \mathrm{Hom}(A, B)$$

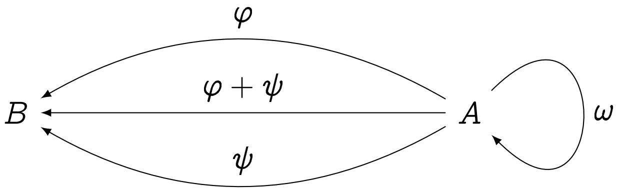
Groups of isogenies



$$\varphi, \psi \in \mathrm{Hom}(A, B)$$

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

Groups of isogenies



$$\varphi, \psi \in \mathrm{Hom}(A, B) \qquad\qquad \omega \in \mathrm{Hom}(A, A)$$

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

Endomorphism rings

- $\mathrm{Hom}(A, B)$ is a group

- Distributivity:

$$\varphi \circ (\psi + \chi) = (\varphi \circ \psi) + (\varphi \circ \chi)$$

$$(\psi + \chi) \circ \varphi = (\psi \circ \varphi) + (\chi \circ \varphi)$$

- It follows that $\mathrm{End}(A) := \mathrm{Hom}(A, A)$ is a ring.

Endomorphism rings

$\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank 1, 2 or 4. As a ring:

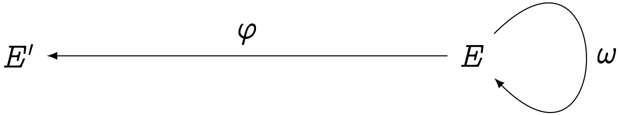
1) $\mathrm{End}(E) \simeq \mathbb{Z}$;
2) $\mathrm{End}(E) \subset$ quadratic imaginary field;
4) $\mathrm{End}(E) \subset$ quaternion algebra.

Isogenies = Ideals

$$E' \xleftarrow{\quad\varphi\quad} E$$

$$\varphi \in \mathrm{Hom}(E, E')$$

Isogenies = Ideals

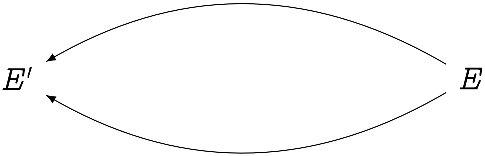


$$\varphi \circ \omega \in \mathrm{Hom}(E, E')$$

Isogenies = Ideals

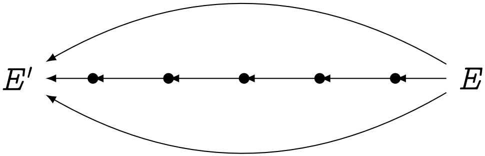
$$\omega' \circ \varphi \in \mathrm{Hom}(E, E')$$

Smoothifying ideals



$$\mathrm{Hom}(E, E') = \mathbb{Z}\varphi_1 + \mathbb{Z}\varphi_2$$

Smoothifying ideals



$$\mathrm{Hom}(E, E') = \mathbb{Z}\varphi_1 + \mathbb{Z}\varphi_2$$

$$\deg(a\varphi_1 + b\varphi_2) = \textit{smooth}$$

Smoothifying in quadratic imaginary rings

Algorithm: Index calculus

Cost: (sub)exponential complexity, fast in practice

Used in: CSI-FiSh signature scheme (2019)

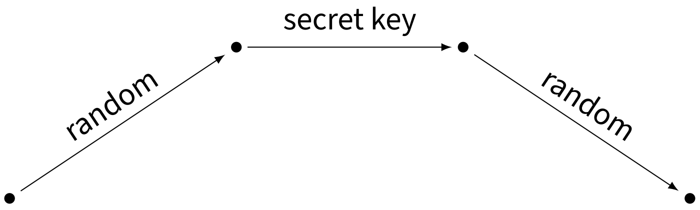
Smoothifying in quaternion rings

Algorithm: Kohel–Petit–Tignol–Lauter (KLPT)

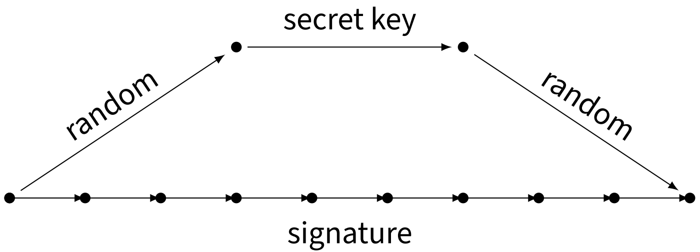
Cost: polynomial time

Used in: Galbraith–Petit–Silva (2016) and SQIsign (2020) signatures

Basically every isogeny signature



Basically every isogeny signature



SQIsign

	Bytes		Mcycles			
Secret Key	Public Key	Signature	Keygen	Sign	Verify	Security
782	64	177	3,728	5,779	108	NIST-1
1,138	96	263	23,734	43,760	654	NIST-3
1,509	128	335	91,049	158,544	2,177	NIST-5

What does it mean to “compute” an isogeny?

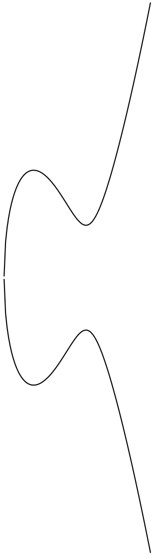
Definition (Isogeny representation)

A *representation* of an isogeny $\varphi : E \to E'$ is an algorithm / Turing machine / arithmetic circuit that:

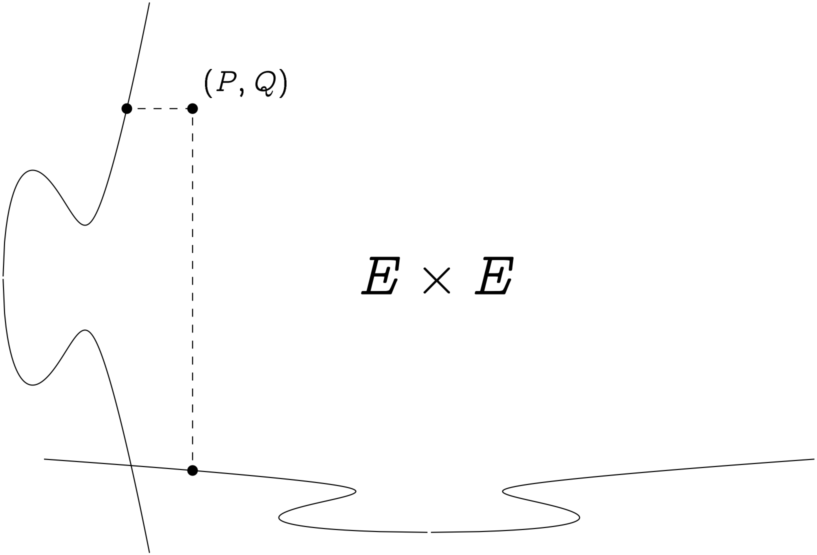
- on input $P \in E$
- outputs $\varphi(P) \in E'$

in time polynomial in $\log(\deg \varphi)$.

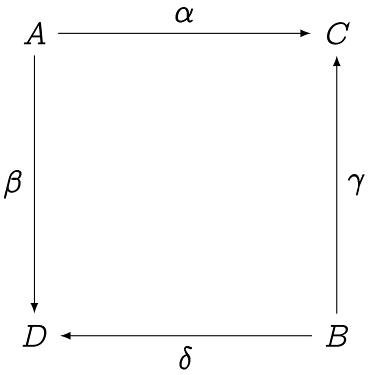
Higher dimensional abelian varieties



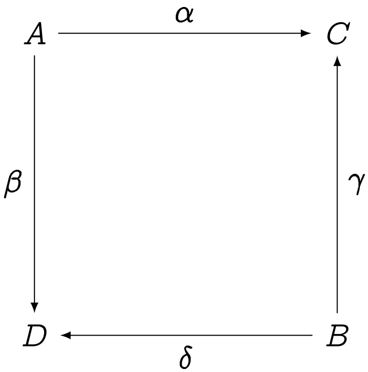
Higher dimensional abelian varieties



Higher dimensional isogenies



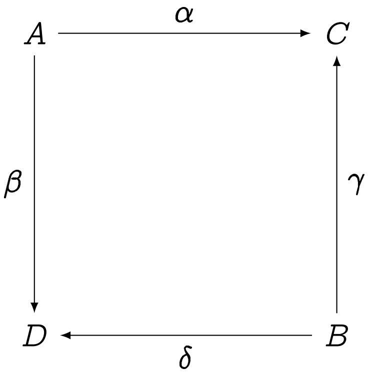
Higher dimensional isogenies



$$A \times B \longrightarrow C \times D$$

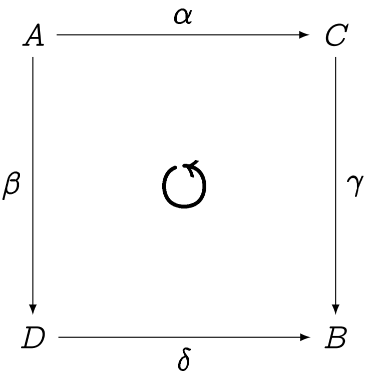
$$(P, Q) \longmapsto \big(\alpha(P) + \gamma(Q), \beta(P) + \delta(Q)\big)$$

Higher dimensional isogenies



$$A \times B \longrightarrow C \times D$$
$$(P, Q) \longmapsto \big(\alpha(P) + \gamma(Q), \beta(P) + \delta(Q)\big)$$
$$= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

Kani's lemma

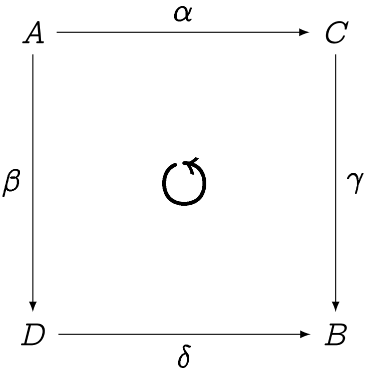


Let $\deg\alpha = \deg\delta$ and $\deg\beta = \deg\gamma$ coprime. The isogeny defined by

$$\Phi : A \times B \longrightarrow C \times D$$
$$\begin{pmatrix} P \\ Q \end{pmatrix} \longmapsto \begin{pmatrix} \alpha & \tilde{\gamma} \\ -\beta & \tilde{\delta} \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

is a $\big(\deg(\alpha) + \deg(\beta)\big)$-isogeny if and only if the diagram commutes.

Kani's lemma



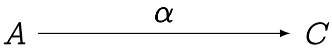
Let $\deg\alpha = \deg\delta$ and $\deg\beta = \deg\gamma$ coprime. The isogeny defined by

$$\Phi : A \times B \longrightarrow C \times D$$
$$\begin{pmatrix} P \\ Q \end{pmatrix} \longmapsto \begin{pmatrix} \alpha & \tilde{\gamma} \\ -\beta & \tilde{\delta} \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}$$

is a $\big(\deg(\alpha) + \deg(\beta)\big)$-isogeny if and only if the diagram commutes.

Note: $\Phi(P, 0) = \big(\alpha(P), -\beta(P)\big)$.

Application: breaking SIDH



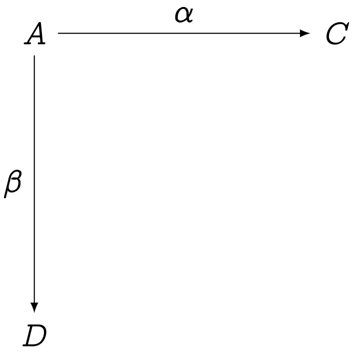
Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

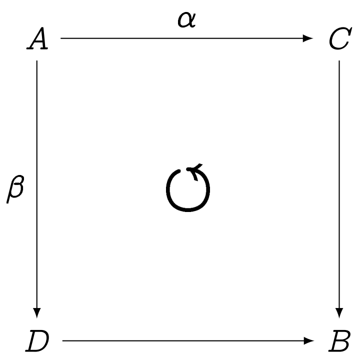
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

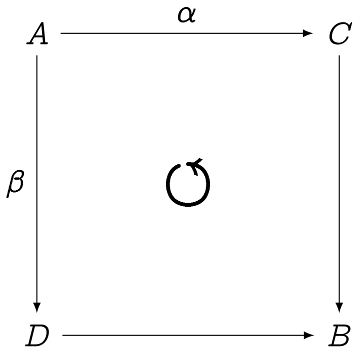
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;
2. Complete the commutative square;

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

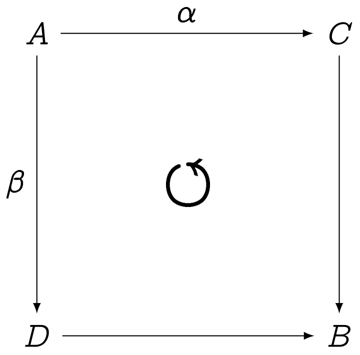
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;
2. Complete the commutative square;
3. Compute Kani's 2^n-isogeny Φ;

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

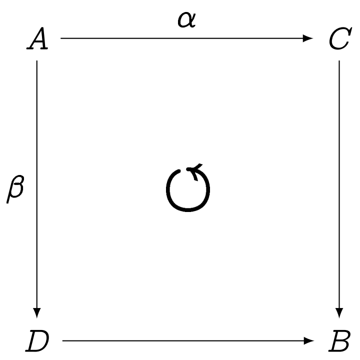
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;
2. Complete the commutative square;
3. Compute Kani's 2^n-isogeny Φ;
4. Then $\Phi(P', 0) = \big(\alpha(P'), \dots\big)$ for any $P' \in A$;

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

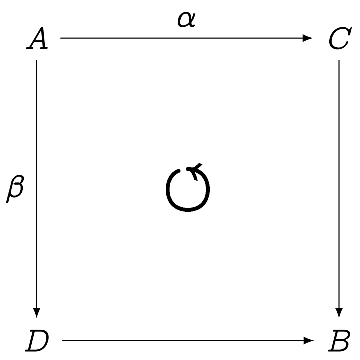
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;
2. Complete the commutative square;
3. Compute Kani's 2^n-isogeny Φ;
4. Then $\Phi(P', 0) = \big(\alpha(P'), \dots\big)$ for any $P' \in A$;
5. Deduce kernel of α;

Application: breaking SIDH



Secret: $\alpha : A \to B$ of degree $\deg(\alpha) = d$

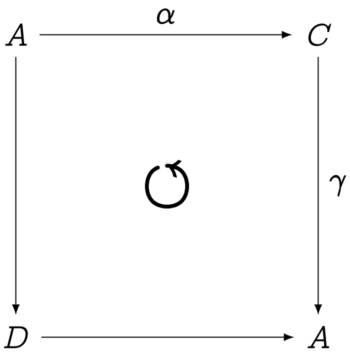
Input: $\alpha(P)$ for all P of order $2^n > d$

Goal: Compute a representation of α

Attack (sketch):

1. Compute an isogeny β of degree $e = 2^n - d$;
2. Complete the commutative square;
3. Compute Kani's 2^n-isogeny Φ;
4. Then $\Phi(P', 0) = \big(\alpha(P'), \dots\big)$ for any $P' \in A$;
5. Deduce kernel of α;
6. Claim 50 K$.

Application: from quaternions to random isogenies (QFESTA)

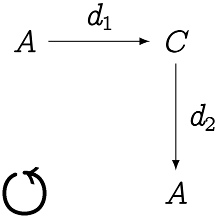


Input: $\mathrm{End}(A)$, a degree d,

Output: A random d-isogeny $A \to ?$.

1. Find endomorphism ω of degree $\deg \omega = d(2^n - d)$,
2. Factor $\omega = \alpha \circ \gamma$ with $\deg(\alpha) = d$,
3. Kani's isogeny is a representation of α.

Application: evaluate (almost) any ideal (Clapoti)

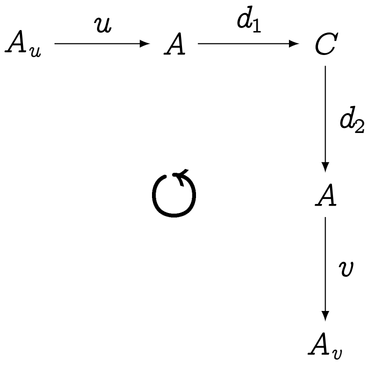


Input: $\mathrm{End}(A)$, an ideal of $\mathrm{End}(A)$,

Output: The corresponding isogeny.

1. Find random equivalent ideals of coprime degrees d_1, d_2;

Application: evaluate (almost) any ideal (Clapoti)

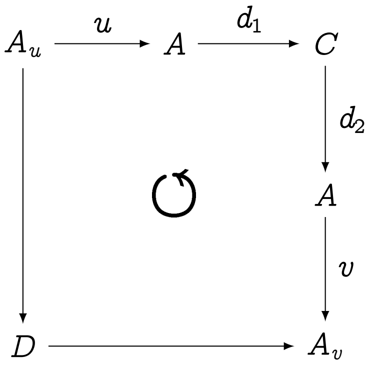


Input: $\mathrm{End}(A)$, an ideal of $\mathrm{End}(A)$,

Output: The corresponding isogeny.

1. Find random equivalent ideals of coprime degrees d_1, d_2;
2. Find integers u, v s.t. $ud_1 + vd_2 = 2^n$;
3. Find random u- and v-isogeny;

Application: evaluate (almost) any ideal (Clapoti)



Input: $\mathrm{End}(A)$, an ideal of $\mathrm{End}(A)$,

Output: The corresponding isogeny.

1. Find random equivalent ideals of coprime degrees d_1, d_2;
2. Find integers u, v s.t. $ud_1 + vd_2 = 2^n$;
3. Find random u- and v-isogeny;
4. Construct Kani square.

Putting it all together: SQIsign2D-West

Bytes		Mcycles			
Public Key	Signature	Keygen	Sign	Verify	Security
66	148	60	160	9	NIST-1
98	222	170	460	29	NIST-3
130	294	360	940	62	NIST-5

Thank you

https://defeo.lu/

@luca_defeo@ioc.exchange

@luca_defeo