Orientations and the supersingular endomorphism ring problem

Benjamin Wesolowski
Université de Bordeaux, CNRS, Inria

Eurocrypt 2022, June 2022, Trondheim, Norway

Supersingular elliptic curves

Isogenies and endomorphisms

Elliptic curves

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

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

Elliptic curves

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

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

$E(\mathbb{F}_q)$ is an additive group

Elliptic curves

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

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

$E(\mathbb{F}_q)$ is an additive group

An **isogeny** in a map

$$\varphi : E \to F$$

which preserves certain structures. In particular, it is a group homomorphism with a finite kernel

Endomorphism ring

An **endomorphism** is an isogeny $\varphi : E \to E$

Endomorphism ring

An **endomorphism** is an isogeny $\varphi : E \to E$

They form a **ring** $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

Endomorphism ring

An **endomorphism** is an isogeny $\varphi : E \to E$

They form a **ring** $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

What is the structure of $\mathrm{End}(E)$?

Endomorphism ring

An **endomorphism** is an isogeny $\varphi : E \to E$

They form a **ring** $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

What is the structure of $\mathrm{End}(E)$?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...

Endomorphism ring

An **endomorphism** is an isogeny $\varphi : E \to E$

They form a **ring** $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

What is the structure of $\mathrm{End}(E)$?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- $(\mathrm{End}(E), +)$ is a **lattice** of dimension 2 or 4

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

EndRing

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

EndRing

$\Updownarrow$

Isogeny Path Problem

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

EndRing

$\Updownarrow$

Isogeny Path Problem

Breaking isogeny-based cryptosystems

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

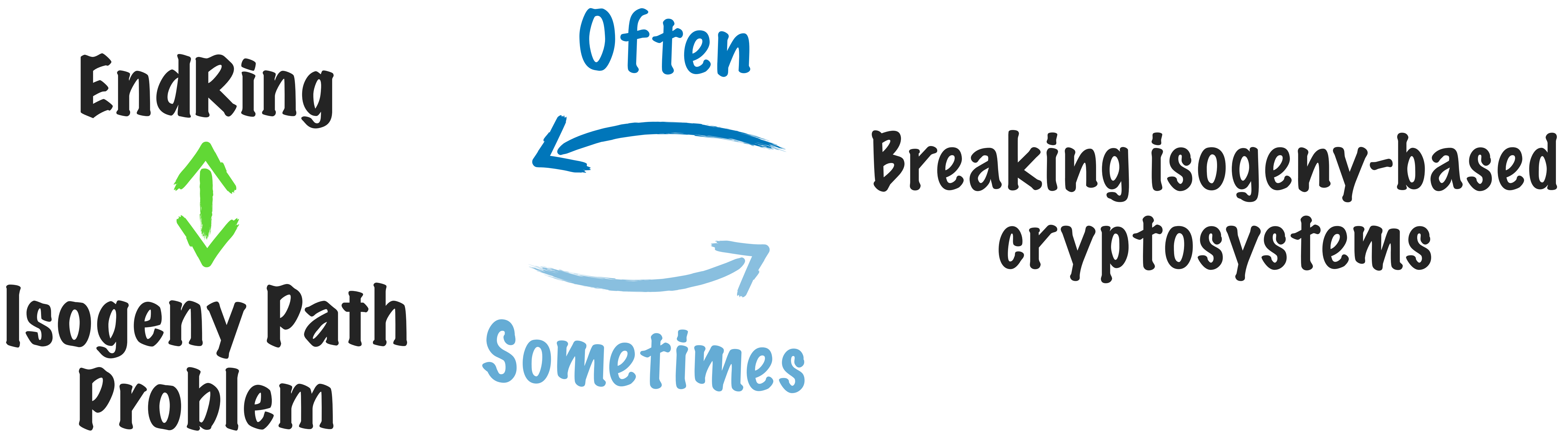
EndRing $\Updownarrow$ Isogeny Path Problem $\xleftarrow{\text{Often}}$ Breaking isogeny-based cryptosystems

The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

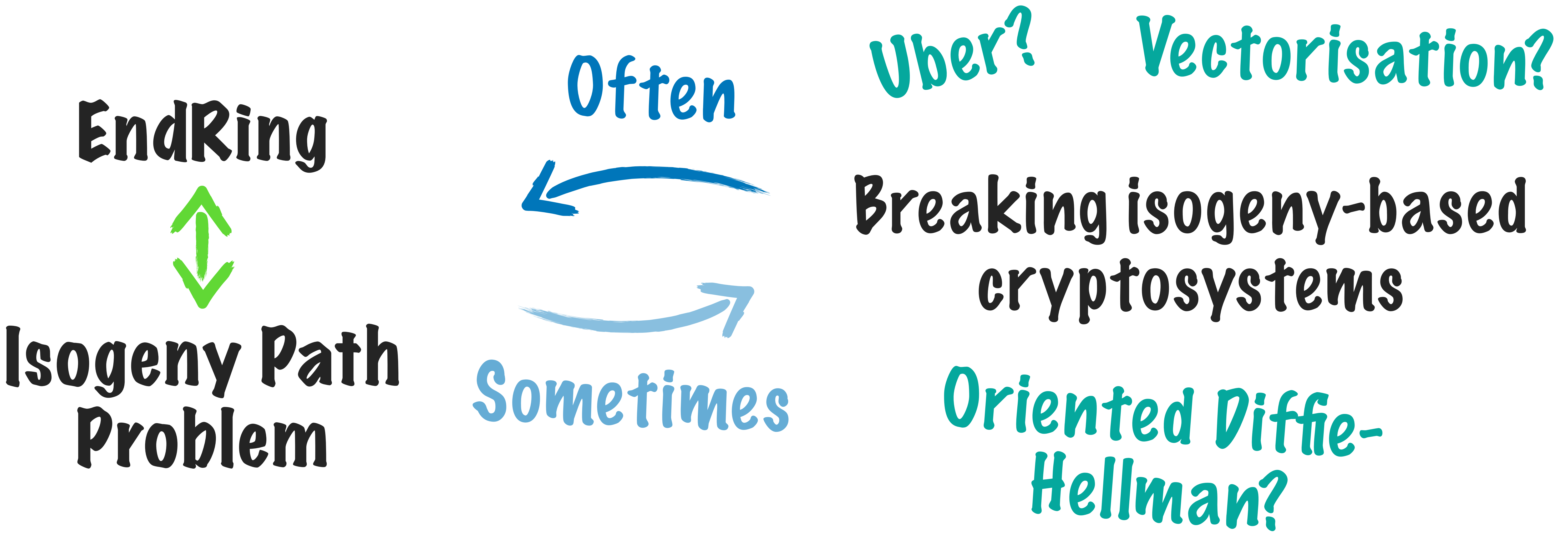


The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$



The Endomorphism Ring problem

A curve E is **supersingular** if $(\mathrm{End}(E), +)$ is a lattice of dimension 4

EndRing: Given a supersingular curve E, compute $\mathrm{End}(E)$. I.e., find 4 endomorphisms that form a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

EndRing

$\Updownarrow$

Isogeny Path Problem

Often

Sometimes

Uber?

Vectorisation?

Breaking isogeny-based cryptosystems

Oriented Diffie-Hellman?

Goal: get a sharper picture of the situation

Orientations

Of supersingular elliptic curves

Oriented elliptic curves

Let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

- $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$ is a subring of dimension 2

Oriented elliptic curves

Let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

- $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$ is a subring of dimension 2
- $\mathbb{Z}[\alpha]$ is a **quadratic ring**, i.e., a ring of the form $\mathbb{Z}[x]/(x^2 + ax + b)$

Oriented elliptic curves

Let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

- $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$ is a subring of dimension 2
- $\mathbb{Z}[\alpha]$ is a **quadratic ring**, i.e., a ring of the form $\mathbb{Z}[x]/(x^2 + ax + b)$

Fix a quadratic ring $\mathcal{O}$. An $\mathcal{O}$-orientation is an injective homomorphism

$$\iota : \mathcal{O} \to \mathrm{End}(E)$$

Oriented elliptic curves

Let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

- $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$ is a subring of dimension 2
- $\mathbb{Z}[\alpha]$ is a **quadratic ring**, i.e., a ring of the form $\mathbb{Z}[x]/(x^2 + ax + b)$

Fix a quadratic ring $\mathcal{O}$. An $\mathcal{O}$-orientation is an injective homomorphism

$$\iota : \mathcal{O} \to \mathrm{End}(E)$$

(E, ι) is an $\mathcal{O}$-oriented curve

Oriented elliptic curves

Let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

- $\mathbb{Z}[\alpha] \subset \mathrm{End}(E)$ is a subring of dimension 2
- $\mathbb{Z}[\alpha]$ is a **quadratic ring**, i.e., a ring of the form $\mathbb{Z}[x]/(x^2 + ax + b)$

Fix a quadratic ring $\mathcal{O}$. An $\mathcal{O}$-orientation is an injective homomorphism

$$\iota : \mathcal{O} \to \mathrm{End}(E)$$

(E, ι) is an $\mathcal{O}$-oriented curve

$\mathrm{Ell}_{\mathcal{O}}(p)$ is the set of (supersingular) $\mathcal{O}$-oriented curves over $\overline{\mathbb{F}}_p$

Action of the class group

Each quadratic ring $\mathcal{O}$ comes with a finite abelian group $\mathrm{Cl}(\mathcal{O})$, the **ideal class group** of $\mathcal{O}$

Action of the class group

Each quadratic ring $\mathcal{O}$ comes with a finite abelian group $\mathrm{Cl}(\mathcal{O})$, the **ideal class group** of $\mathcal{O}$

There is an action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(p)$

$$\begin{aligned} * : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) &\to \mathrm{Ell}_{\mathcal{O}}(p) \\ (\mathfrak{a}, E) &\longmapsto \mathfrak{a} * E \end{aligned}$$

Action of the class group

Each quadratic ring $\mathcal{O}$ comes with a finite abelian group $\mathrm{Cl}(\mathcal{O})$, the **ideal class group** of $\mathcal{O}$

There is an action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(p)$

$$
\begin{aligned}
* : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) &\longrightarrow \mathrm{Ell}_{\mathcal{O}}(p) \\
(\mathfrak{a}, E) &\longmapsto \mathfrak{a} * E
\end{aligned}
$$

$$\mathfrak{b} * (\mathfrak{a} * E) = (\mathfrak{b}\mathfrak{a}) * E$$

Action of the class group

Each quadratic ring $\mathcal{O}$ comes with a finite abelian group $\mathrm{Cl}(\mathcal{O})$, the **ideal class group** of $\mathcal{O}$

There is an action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(p)$

$$\begin{aligned} * : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) &\longrightarrow \mathrm{Ell}_{\mathcal{O}}(p) \\ (\mathfrak{a}, E) &\longmapsto \mathfrak{a} * E \end{aligned}$$

$$\mathfrak{b} * (\mathfrak{a} * E) = (\mathfrak{b}\mathfrak{a}) * E$$

$$\mathfrak{e} * E = E$$

Cryptography from orientations

Key exchange on the CSIDH

CSIDH key exchange

Alice

Bob

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$\xrightarrow{\mathfrak{a} * E_0}$

CSIDH key exchange

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Alice

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$\xrightarrow{\mathfrak{a} * E_0}$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$$\xrightarrow{\mathfrak{a} * E_0}$$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

CSIDH key exchange

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Alice

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$$\xrightarrow{\mathfrak{a} * E_0}$$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

$$\xleftarrow{\mathfrak{b} * E_0}$$

CSIDH key exchange

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Alice

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$\xrightarrow{\mathfrak{a} * E_0}$

$\xleftarrow{\mathfrak{b} * E_0}$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

Compute $\boldsymbol{E}_{\mathbf{AB}} = \mathfrak{a} * (\mathfrak{b} * E_0)$

CSIDH key exchange

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Alice

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$$\xrightarrow{\mathfrak{a} * E_0}$$

Bob

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

$$\xleftarrow{\mathfrak{b} * E_0}$$

Compute $E_{AB} = \mathfrak{a} * (\mathfrak{b} * E_0)$

Compute $E_{BA} = \mathfrak{b} * (\mathfrak{a} * E_0)$

CSIDH key exchange

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Alice

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$$\xrightarrow{\ \mathfrak{a} * E_0\ }$$

$$\xleftarrow{\ \mathfrak{b} * E_0\ }$$

Bob

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

Compute $E_{AB} = \mathfrak{a} * (\mathfrak{b} * E_0)$

Compute $E_{BA} = \mathfrak{b} * (\mathfrak{a} * E_0)$

$$E_{AB} = \mathfrak{a} * (\mathfrak{b} * E_0) = \mathfrak{b} * (\mathfrak{a} * E_0) = E_{BA}$$

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$\xrightarrow{\mathfrak{a} * E_0}$

$\xleftarrow{\mathfrak{b} * E_0}$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

Compute $\boldsymbol{E}_{\mathsf{AB}} = \mathfrak{a} * (\mathfrak{b} * E_0)$

Compute $\boldsymbol{E}_{\mathsf{BA}} = \mathfrak{b} * (\mathfrak{a} * E_0)$

$$\boldsymbol{E}_{\mathsf{AB}} = \mathfrak{a} * (\mathfrak{b} * E_0) = \mathfrak{b} * (\mathfrak{a} * E_0) = \boldsymbol{E}_{\mathsf{BA}}$$

$\boldsymbol{E}_{\mathsf{AB}} = \boldsymbol{E}_{\mathsf{BA}}$ is Alice and Bob's shared secret

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$\xrightarrow{\mathfrak{a} * E_0}$

$\xleftarrow{\mathfrak{b} * E_0}$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

Compute $\boldsymbol{E}_{\mathbf{AB}} = \mathfrak{a} * (\mathfrak{b} * E_0)$

Compute $\boldsymbol{E}_{\mathbf{BA}} = \mathfrak{b} * (\mathfrak{a} * E_0)$

A spy sees E_0, $\mathfrak{a} * E_0$, and $\mathfrak{b} * E_0$. Can they recover the secret $(\mathfrak{a}\mathfrak{b}) * E_0$?

CSIDH key exchange

Alice

Fix $E_0 \in \mathrm{Ell}_{\mathcal{O}}(p)$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Bob

Sample secret $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{a} * E_0$

$$\xrightarrow{\mathfrak{a} * E_0}$$

$$\xleftarrow{\mathfrak{b} * E_0}$$

Sample secret $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$

Compute $\mathfrak{b} * E_0$

Compute $\boldsymbol{E_{AB}} = \mathfrak{a} * (\mathfrak{b} * E_0)$

Compute $\boldsymbol{E_{BA}} = \mathfrak{b} * (\mathfrak{a} * E_0)$

A spy sees E_0, $\mathfrak{a} * E_0$, and $\mathfrak{b} * E_0$. Can they recover the secret $(\mathfrak{a}\mathfrak{b}) * E_0$?

The CSIDH problem

Vectorisation

And the oriented endomorphism ring problem

Vectorisation

$\mathscr{O}$-Diffie-Hellman: Given $\mathscr{O}$-oriented E, $\mathfrak{a} * E$ and $\mathfrak{b} * E$, compute $(\mathfrak{a}\mathfrak{b}) * E$.

Vectorisation

$\mathcal{O}$-Diffie-Hellman: Given $\mathcal{O}$-oriented E, $\mathfrak{a} * E$ and $\mathfrak{b} * E$, compute $(\mathfrak{a}\mathfrak{b}) * E$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Vectorisation

$\mathcal{O}$-Diffie-Hellman: Given $\mathcal{O}$-oriented E, $\mathfrak{a} * E$ and $\mathfrak{b} * E$, compute $(\mathfrak{a}\mathfrak{b}) * E$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Evidently*, $\mathcal{O}$-Diffie-Hellman reduces to $\mathcal{O}$-Vectorisation

* actually not so evident, because applying the action of $\mathfrak{a}$ on $\mathfrak{b} * E$ to get $\mathfrak{a}\mathfrak{b} * E$ may not be efficient. This issue can be fixed

Vectorisation

$\mathcal{O}$-Diffie-Hellman: Given $\mathcal{O}$-oriented E, $\mathfrak{a} * E$ and $\mathfrak{b} * E$, compute $(\mathfrak{a}\mathfrak{b}) * E$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Evidently*, $\mathcal{O}$-Diffie-Hellman reduces to $\mathcal{O}$-Vectorisation

Theorem 1: There is a quantum polynomial time reduction from $\mathcal{O}$-Vectorisation to $\mathcal{O}$-Diffie-Hellman (assuming GRH).

Vectorisation

$\mathcal{O}$-Diffie-Hellman: Given $\mathcal{O}$-oriented E, $\mathfrak{a} * E$ and $\mathfrak{b} * E$, compute $(\mathfrak{a}\mathfrak{b}) * E$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Evidently*, $\mathcal{O}$-Diffie-Hellman reduces to $\mathcal{O}$-Vectorisation

Theorem 1: There is a quantum polynomial time reduction from $\mathcal{O}$-Vectorisation to $\mathcal{O}$-Diffie-Hellman (assuming GRH).

Previous work: **subexponential**, **heuristic**, quantum reduction **[Galbraith, Panny, Smith, Vercauteren 2021]**

$\mathcal{O}$-Vectorisation

$\mathcal{O}$-Diffie-Hellman

$\mathcal{O}$-Vectorisation

$\mathcal{O}$-Diffie-Hellman

$\Updownarrow$ $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH

$\mathcal{O}$-Vectorisation

$\mathcal{O}$-Diffie-Hellman

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH

$\mathcal{O}$-Vectorisation $\rightleftarrows$ $\mathcal{O}$-Diffie-Hellman

Quantum

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH

How does this relate to EndRing ?

$\mathcal{O}$-Vectorisation $\rightleftarrows$ $\mathcal{O}$-Diffie-Hellman

Quantum

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH

Oriented EndRing

Oriented EndRing

$\mathcal{O}$-EndRing: Given $\mathcal{O}$-oriented E, compute $\mathrm{End}(E)$.

Oriented EndRing

$\mathcal{O}$-EndRing: Given $\mathcal{O}$-oriented E, compute $\mathrm{End}(E)$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Oriented EndRing

$\mathcal{O}$-EndRing: Given $\mathcal{O}$-oriented E, compute $\mathrm{End}(E)$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Theorem 2: Given the factorisation of $\mathrm{disc}(\mathcal{O})$, the problems $\mathcal{O}$-Vectorisation and $\mathcal{O}$-EndRing are equivalent (assuming GRH).

Oriented EndRing

$\mathcal{O}$-EndRing: Given $\mathcal{O}$-oriented E, compute $\mathrm{End}(E)$.

$\mathcal{O}$-Vectorisation: Given $\mathcal{O}$-oriented E and $\mathfrak{a} * E$, find $\mathfrak{a}$.

Theorem 2: Given the factorisation of $\mathrm{disc}(\mathcal{O})$, the problems $\mathcal{O}$-Vectorisation and $\mathcal{O}$-EndRing are equivalent (assuming GRH).

Previous work: **subexponential** reduction for $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ from $\mathcal{O}$-Vectorisation to $\mathcal{O}$-EndRing **[Castryck, Panny, Vercauteren 2020]**

$$
\begin{tikzcd}
\mathcal{O}\text{-Vectorisation} \arrow[r, shift right, "\text{Quantum}"'] & \mathcal{O}\text{-Diffie-Hellman} \arrow[l, shift right] \arrow[d, leftrightarrow, "\mathcal{O} = \mathbb{Z}[\sqrt{-p}]"] \\
& \text{Breaking CSIDH}
\end{tikzcd}
$$

$\mathcal{O}$-EndRing

$\mathcal{O}$-Vectorisation

$\mathcal{O}$-Diffie-Hellman

Quantum

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH

$$\begin{tikzcd} \mathcal{O}\text{-EndRing} \arrow[r, leftrightarrow] & \mathcal{O}\text{-Vectorisation} \arrow[r, bend right, "\text{Quantum}"'] & \mathcal{O}\text{-Diffie-Hellman} \arrow[l, bend right] \arrow[d, leftrightarrow, "\mathcal{O} = \mathbb{Z}[\sqrt{-p}]"] \\ & & \text{Breaking CSIDH} \end{tikzcd}$$

EndRing

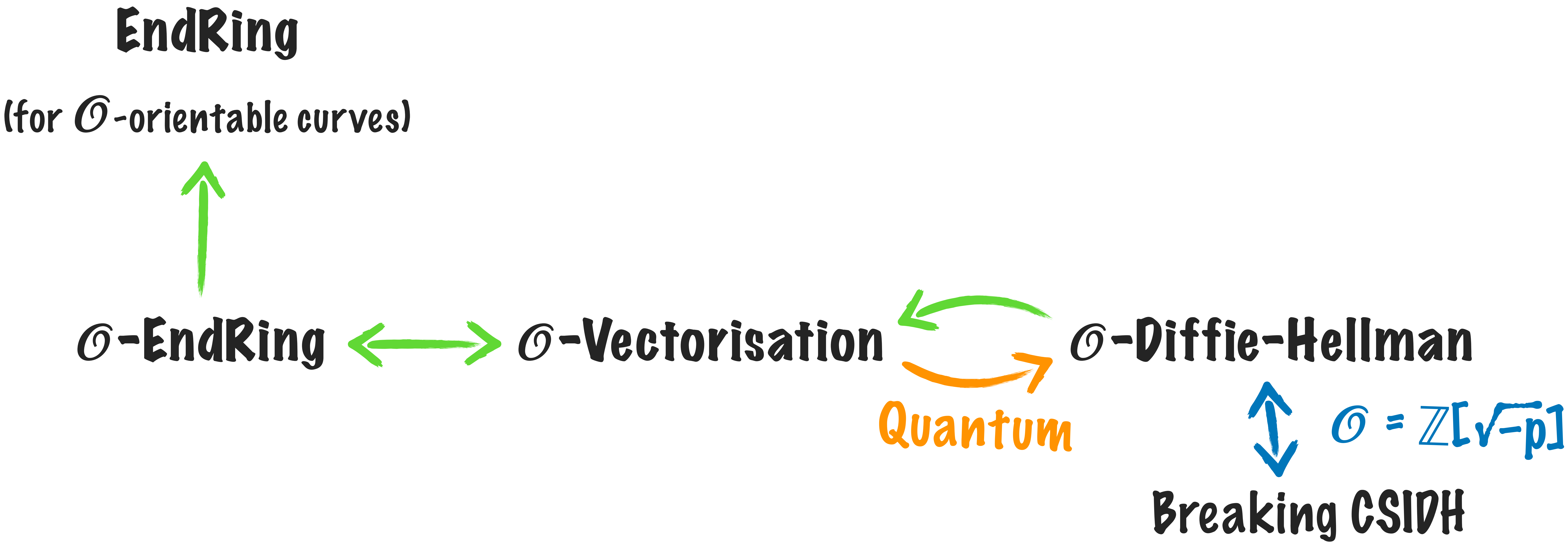
(for $\mathcal{O}$-orientable curves)

$\mathcal{O}$-EndRing $\longleftrightarrow$ $\mathcal{O}$-Vectorisation $\rightleftarrows$ $\mathcal{O}$-Diffie-Hellman

Quantum

$\updownarrow$ $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH


EndRing
(for $\mathcal{O}$-orientable curves)
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH

EndRing

(for $\mathcal{O}$-orientable curves)

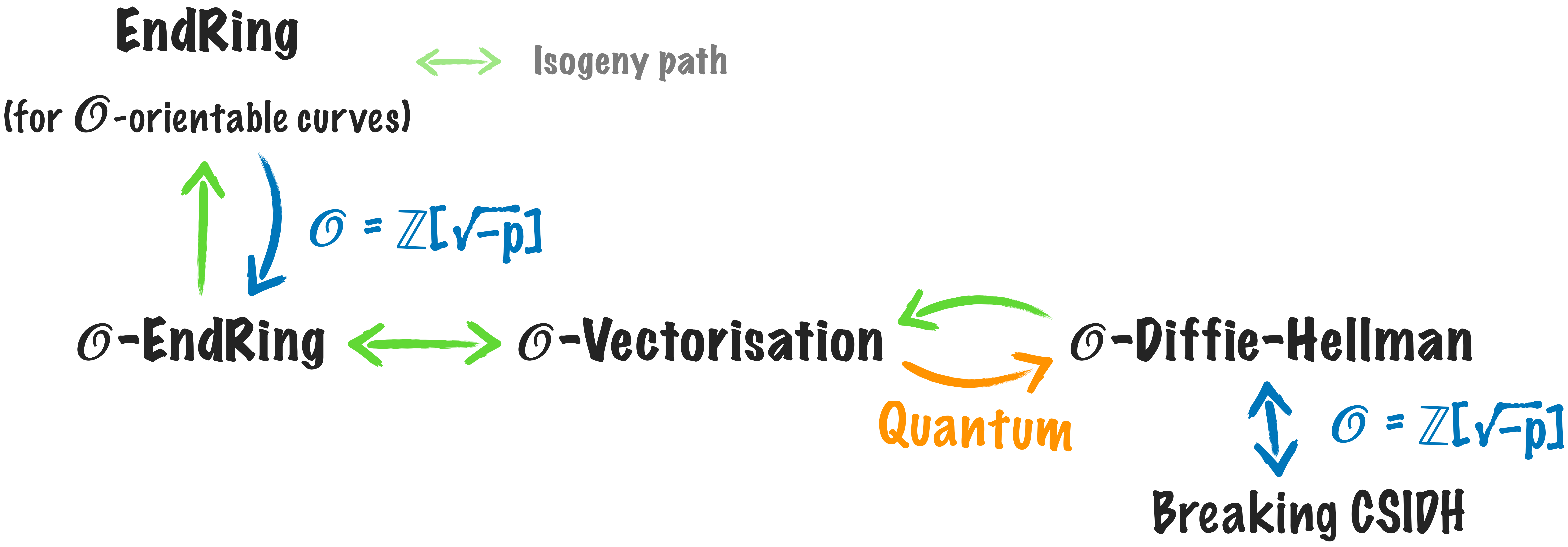
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

$\mathcal{O}$-EndRing $\longleftrightarrow$ $\mathcal{O}$-Vectorisation $\rightleftarrows$ $\mathcal{O}$-Diffie-Hellman

Quantum

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH


EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH

EndRing

(for $\mathcal{O}$-orientable curves)

Isogeny path

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking a few isogeny-based schemes

Sometimes

$\mathcal{O}$-EndRing

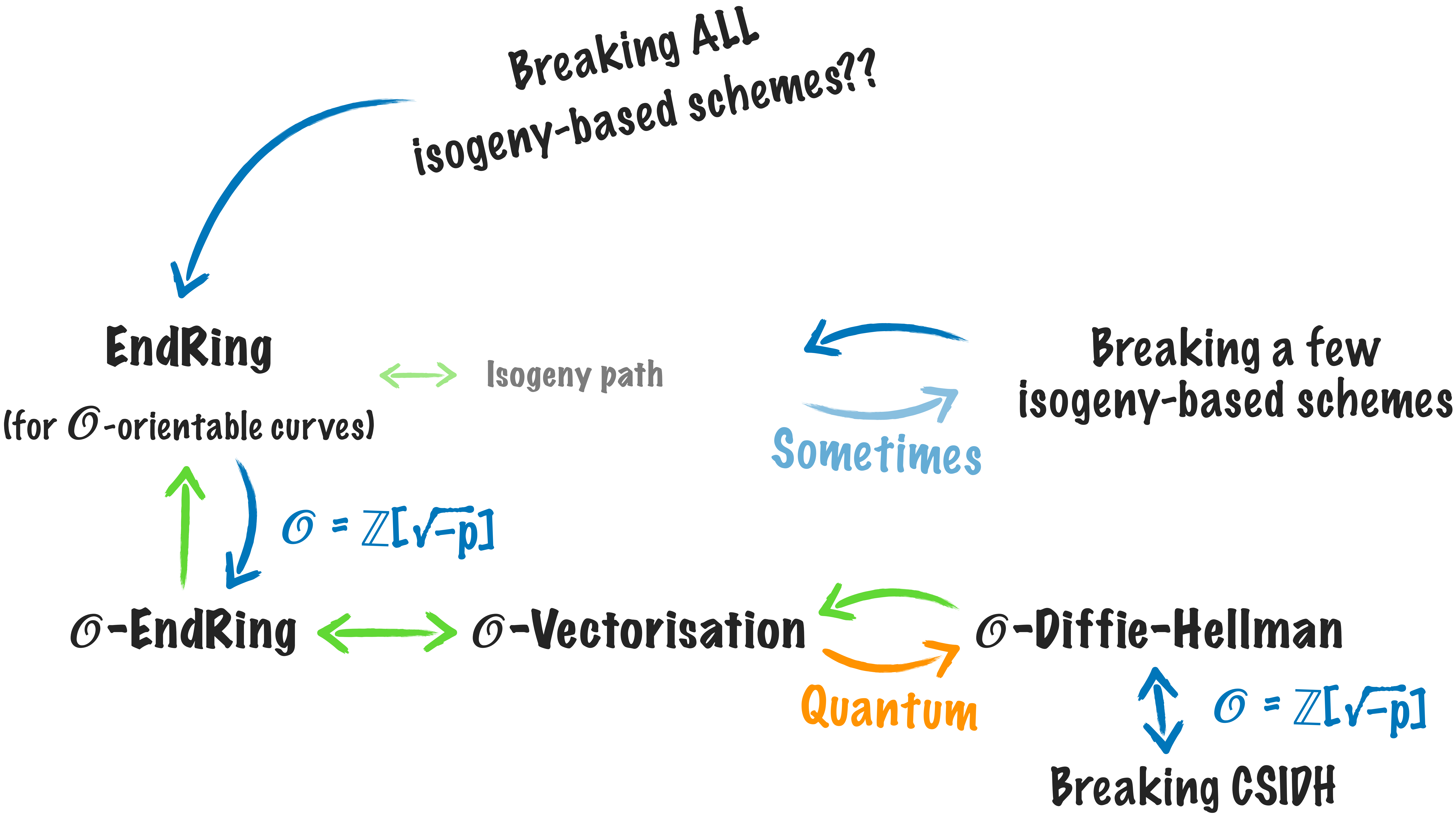
$\mathcal{O}$-Vectorisation

$\mathcal{O}$-Diffie-Hellman

Quantum

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Breaking CSIDH



Breaking ALL
isogeny-based schemes??
EndRing
(for 𝒪-orientable curves)
Isogeny path
Breaking a few
isogeny-based schemes
Sometimes
𝒪 = ℤ[√−p]
𝒪-EndRing
𝒪-Vectorisation
𝒪-Diffie-Hellman
Quantum
𝒪 = ℤ[√−p]
Breaking CSIDH

The Uber isogeny problem

And another oriented endomorphism ring problem

Uber

Many isogeny-based cryptosystems reduces to:

$\mathcal{O}$-Uber: Given $\mathcal{O}$-orient**ed** (E,ι), and an $\mathcal{O}$-orient**able** curve F, find $\mathfrak{a}$ such that $\mathfrak{a} * E = F$.

Uber

Many isogeny-based cryptosystems reduces to:

$\mathcal{O}$-Uber: Given $\mathcal{O}$-orient**ed** (E,ι), and an $\mathcal{O}$-orient**able** curve F, find $\mathfrak{a}$ such that $\mathfrak{a} * E = F$.

[De Feo, Delpech de Saint Guilhem, Fouotsa, Kutas, Leroux, Petit, Silva, W. 2021] SIDH, CSIDH, OSIDH, Séta reduce to $\mathcal{O}$-Uber

Uber

Many isogeny-based cryptosystems reduces to:

$\mathcal{O}$-Uber: Given $\mathcal{O}$-orient**ed** (E,ι), and an $\mathcal{O}$-orient**able** curve F, find $\mathfrak{a}$ such that $\mathfrak{a} * E = F$.

$\mathcal{O}$-EndRing*: Given $\mathcal{O}$-orient**able** E, compute $\mathrm{End}(E)$ and an $\mathcal{O}$-orientation ι of E.

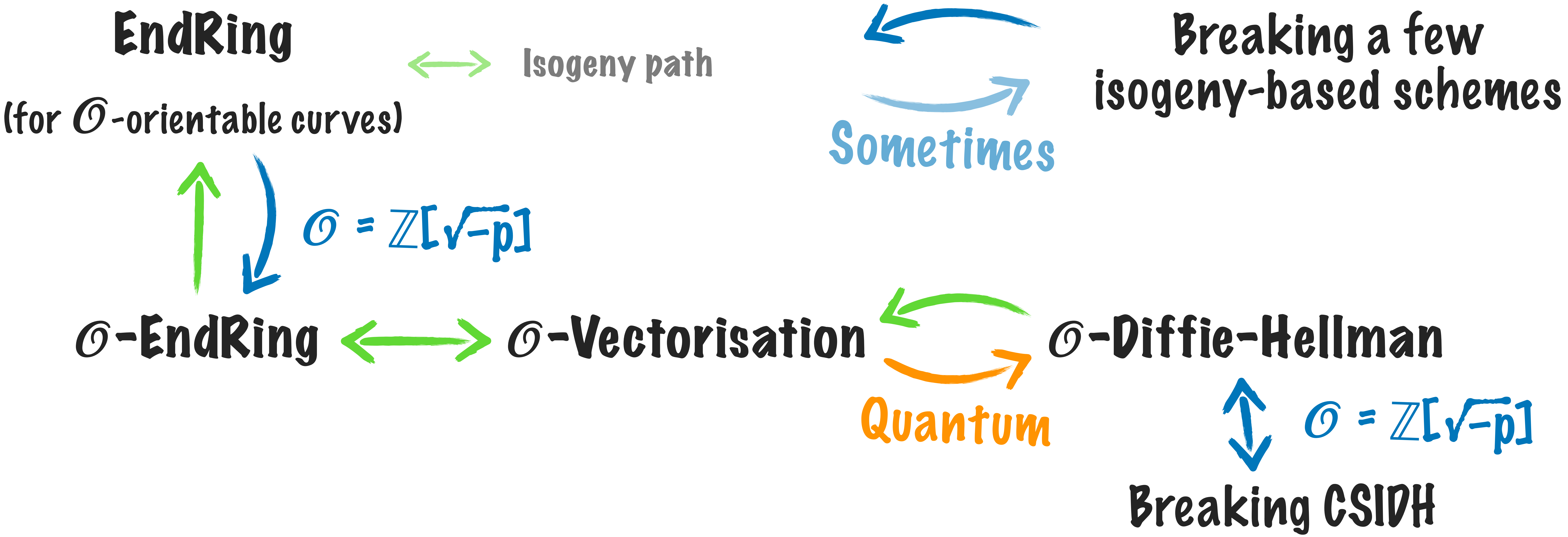
Uber

Many isogeny-based cryptosystems reduces to:

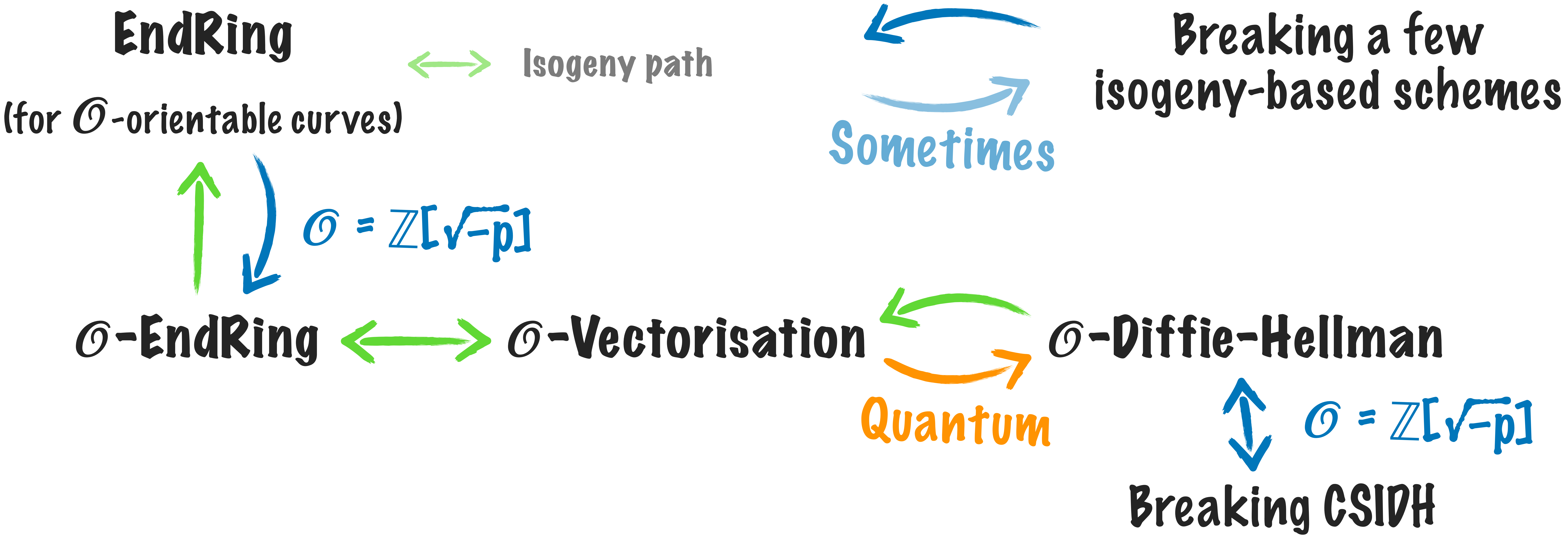
$\mathcal{O}$-Uber: Given $\mathcal{O}$-orient**ed** (E,ι), and an $\mathcal{O}$-orient**able** curve F, find $\mathfrak{a}$ such that $\mathfrak{a} * E = F$.

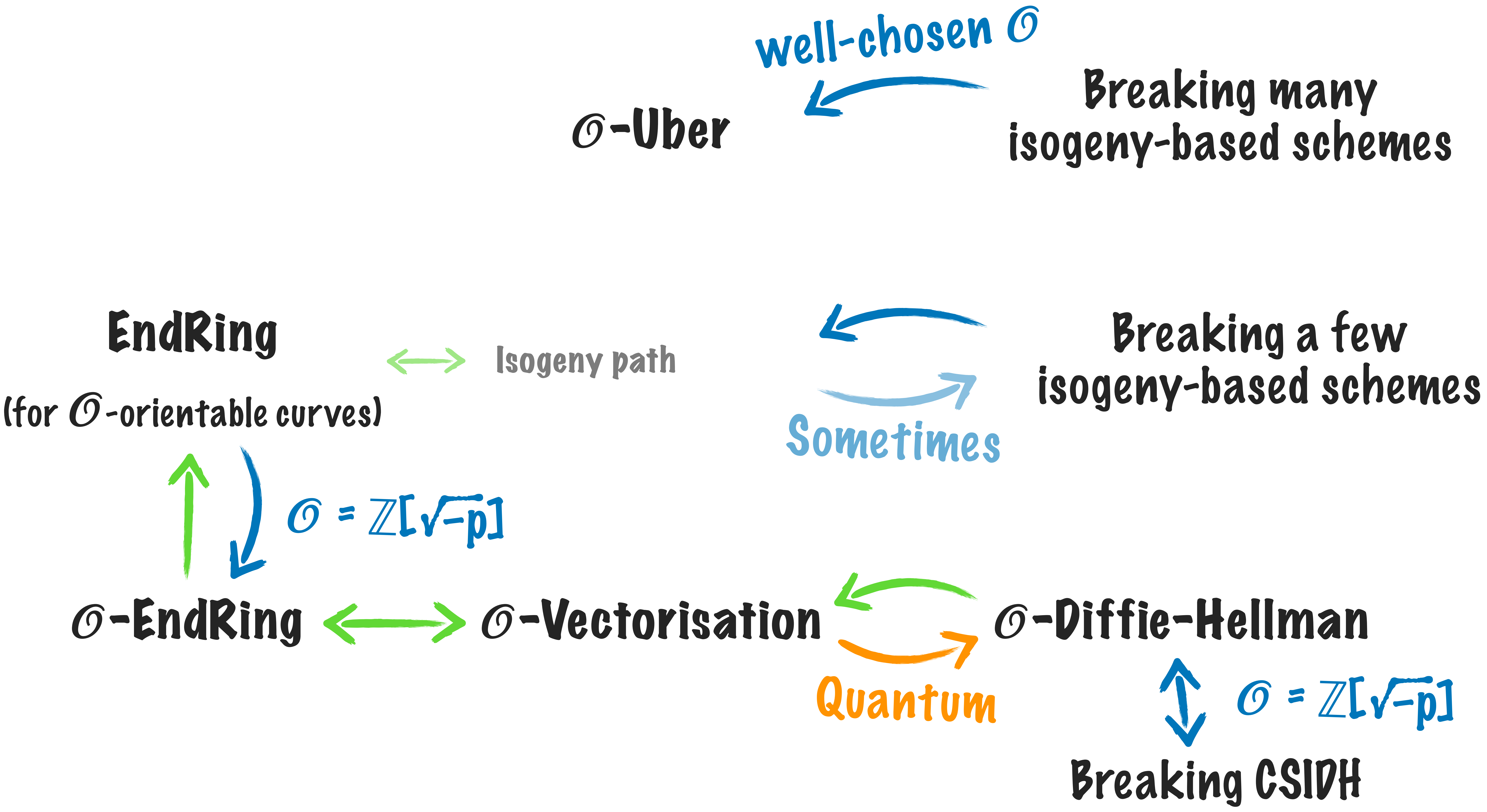
$\mathcal{O}$-EndRing*: Given $\mathcal{O}$-orient**able** E, compute $\mathrm{End}(E)$ and an $\mathcal{O}$-orientation ι of E.

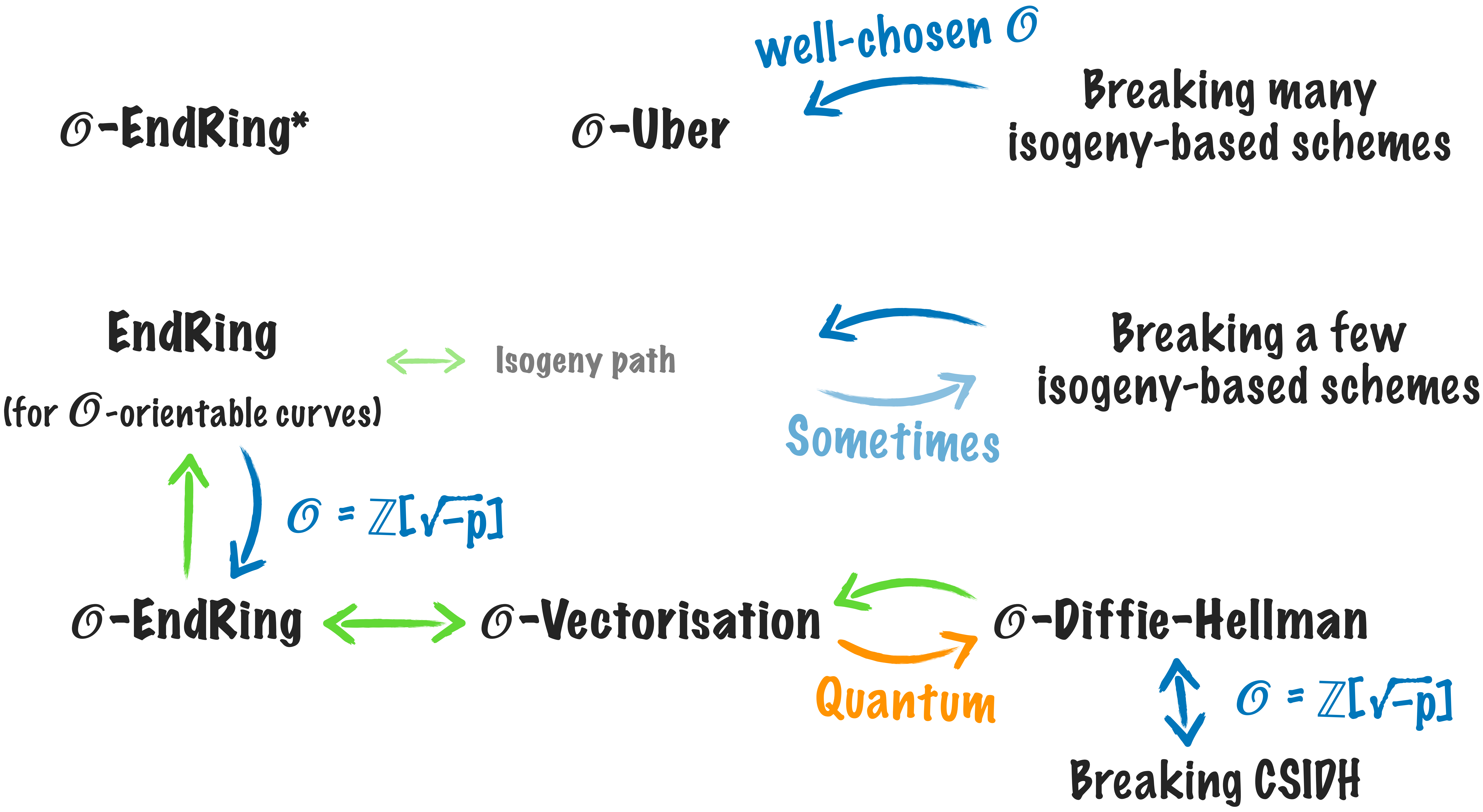
Theorem 3: Given the factorisation of $\mathrm{disc}(\mathcal{O})$, the problems $\mathcal{O}$-Uber and $\mathcal{O}$-EndRing* are equivalent (assuming GRH).


EndRing
(for 𝒪-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
𝒪 = ℤ[√−p]
𝒪-EndRing
𝒪-Vectorisation
𝒪-Diffie-Hellman
Quantum
𝒪 = ℤ[√−p]
Breaking CSIDH

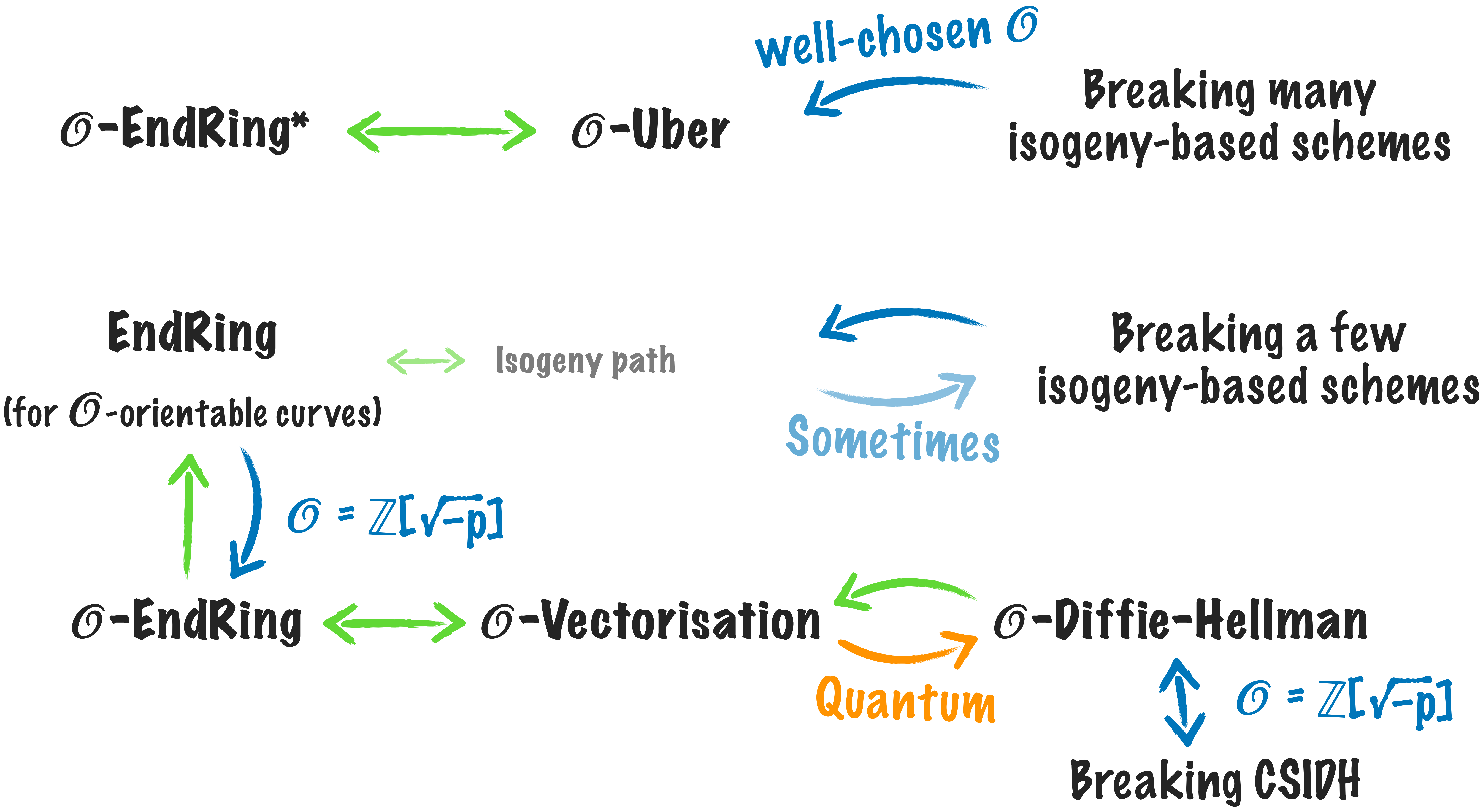
$\mathcal{O}$-Uber



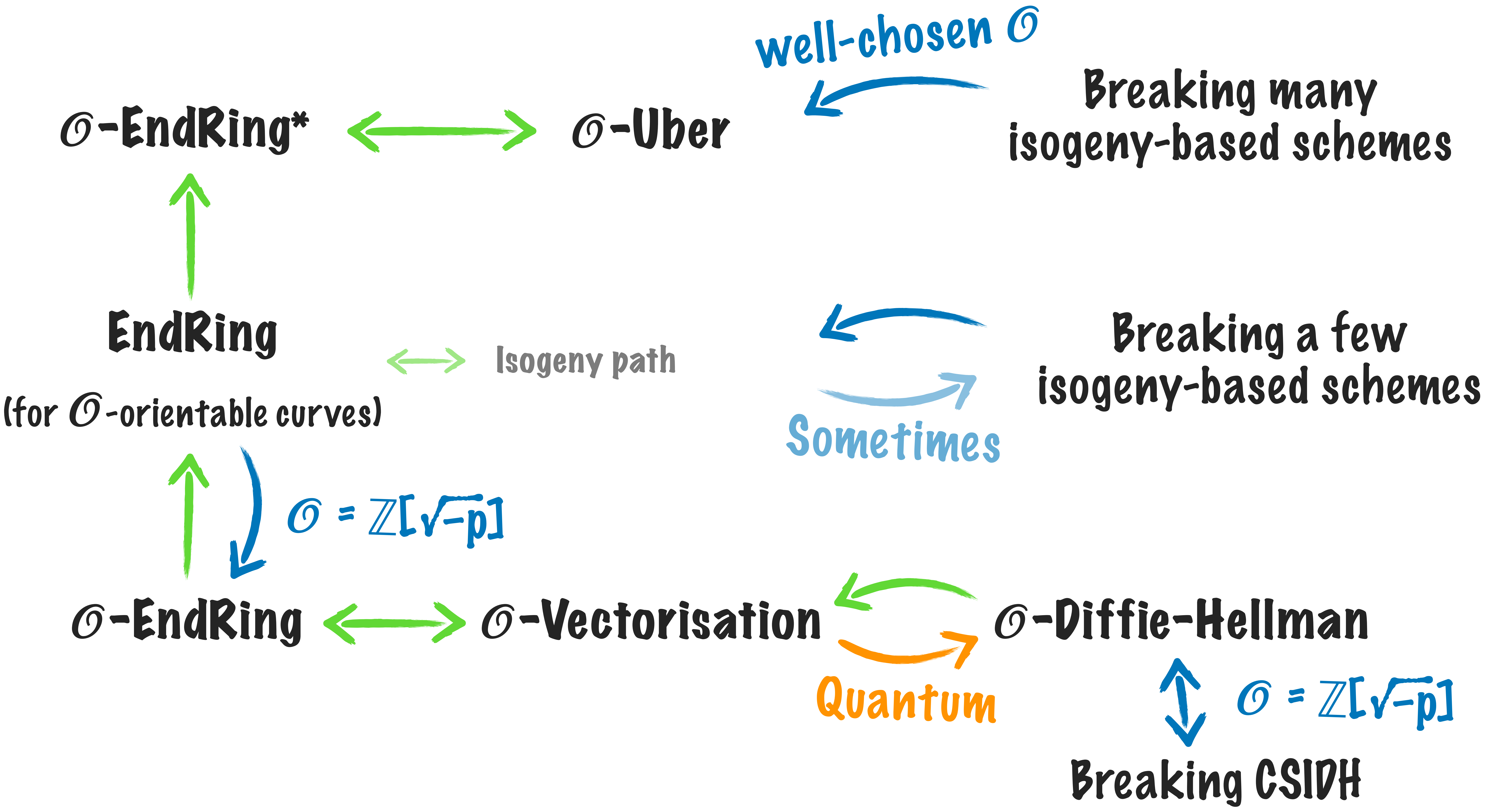

well-chosen $\mathcal{O}$
$\mathcal{O}$-Uber
Breaking many isogeny-based schemes
EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH



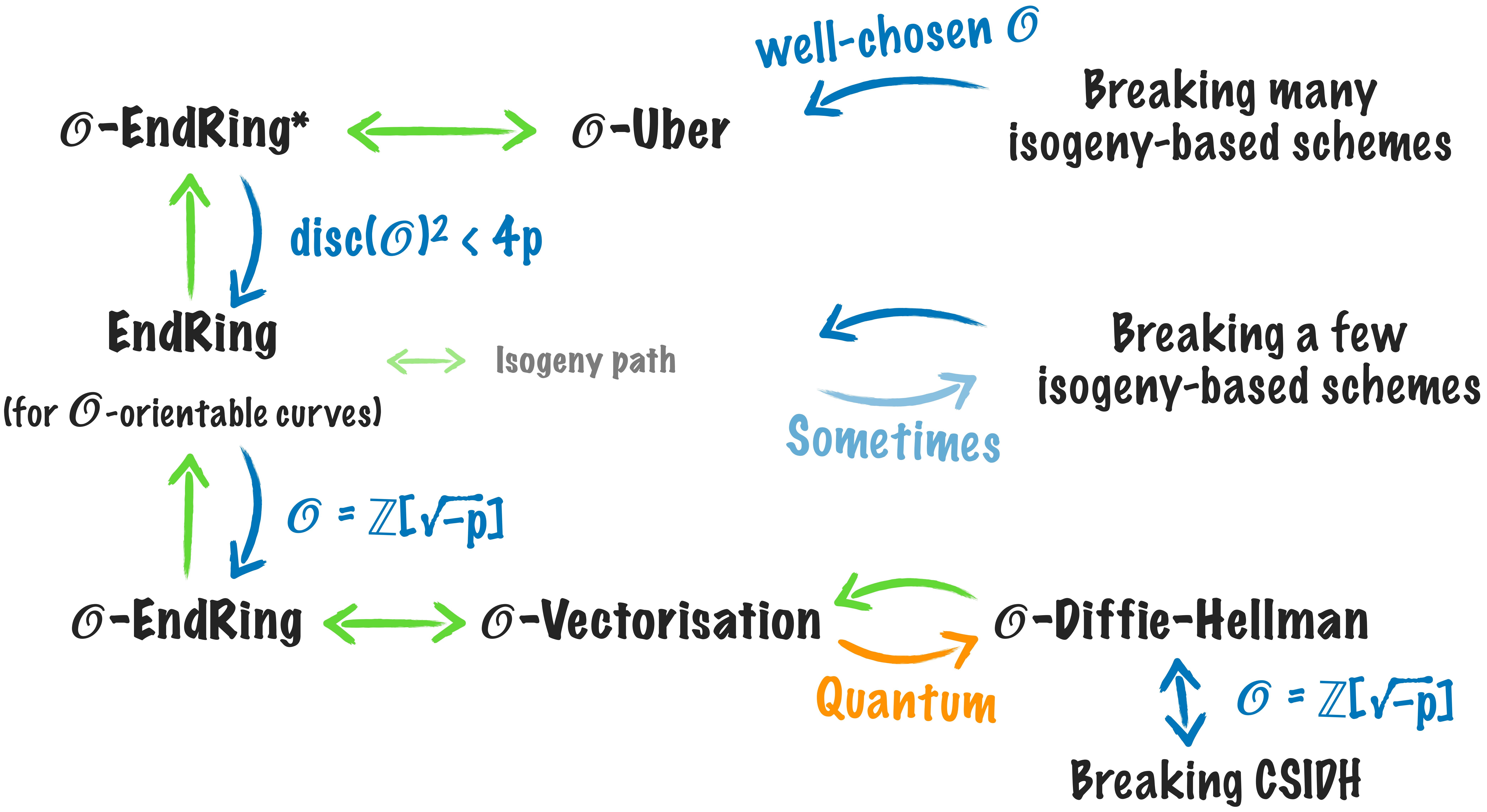
$\mathcal{O}$-EndRing*
$\mathcal{O}$-Uber
well-chosen $\mathcal{O}$
Breaking many isogeny-based schemes
EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH



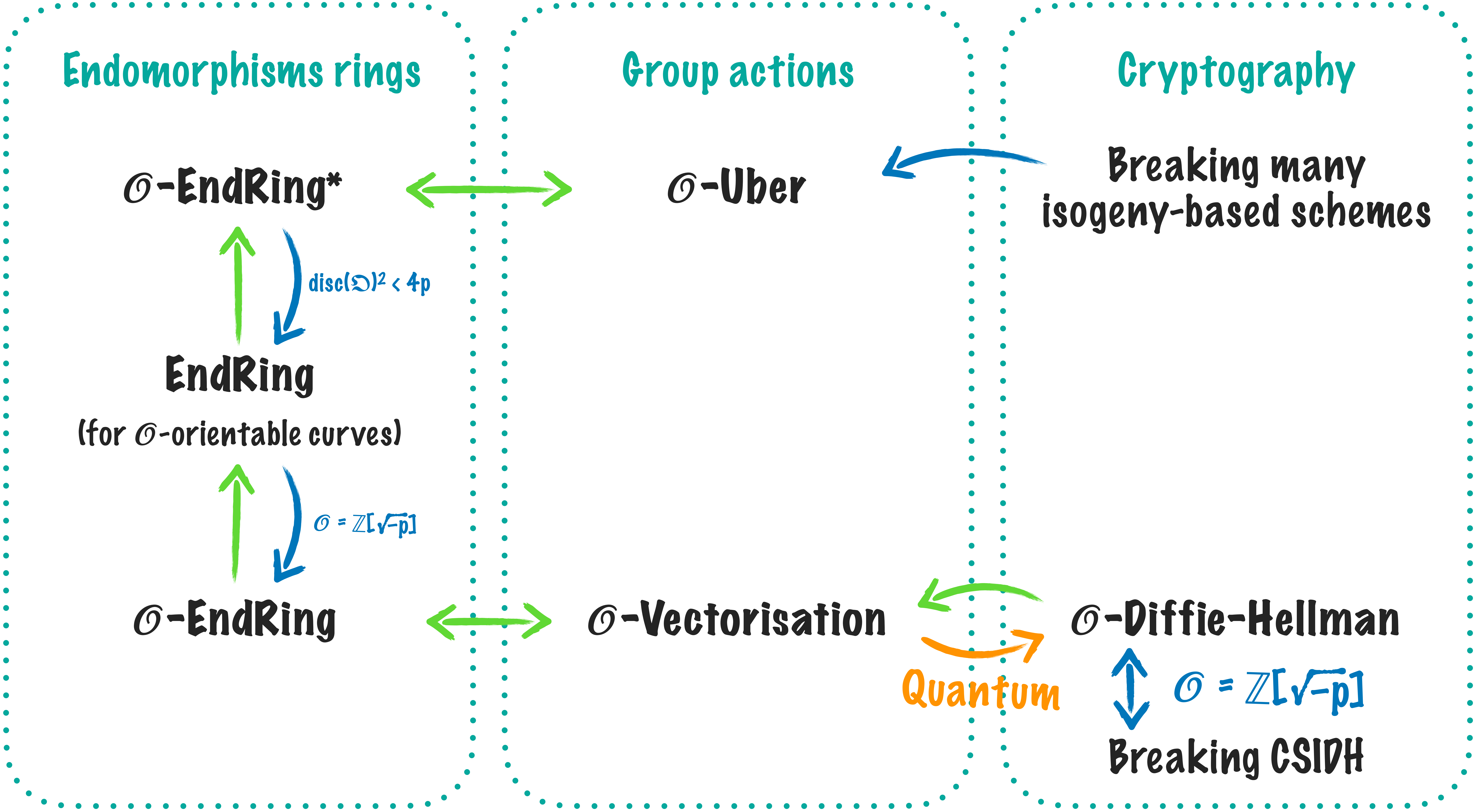
$\mathcal{O}$-EndRing*
$\mathcal{O}$-Uber
well-chosen $\mathcal{O}$
Breaking many isogeny-based schemes
EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH



$\mathcal{O}$-EndRing*
$\mathcal{O}$-Uber
well-chosen $\mathcal{O}$
Breaking many isogeny-based schemes
EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH



$\mathcal{O}$-EndRing*
$\mathcal{O}$-Uber
well-chosen $\mathcal{O}$
Breaking many isogeny-based schemes
$\mathrm{disc}(\mathcal{O})^2 < 4p$
EndRing
(for $\mathcal{O}$-orientable curves)
Isogeny path
Breaking a few isogeny-based schemes
Sometimes
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH


Endomorphisms rings
Group actions
Cryptography
$\mathcal{O}$-EndRing*
$\mathcal{O}$-Uber
Breaking many isogeny-based schemes
$\mathrm{disc}(\mathfrak{O})^2 < 4p$
EndRing
(for $\mathcal{O}$-orientable curves)
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
$\mathcal{O}$-EndRing
$\mathcal{O}$-Vectorisation
$\mathcal{O}$-Diffie-Hellman
Quantum
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
Breaking CSIDH

Orientations and the supersingular endomorphism ring problem

Benjamin Wesolowski
Université de Bordeaux, CNRS, Inria