Isogeny-based cryptography
After the Snap

Benjamin Wesolowski, CNRS and ENS de Lyon

16 August 2023, PQCrypto 2023, College Park, MD, USA

Isogeny crypto

Elliptic curves, isogenies, computational problems

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

Isogeny: a map

$$\varphi : E_1 \longrightarrow E_2$$

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

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

Isogeny: a map

$$\varphi : E_1 \longrightarrow E_2$$

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

The **degree*** is $\deg(\varphi) = \#\ker(\varphi)$

* for separable isogenies

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

Isogeny: a map

$$\varphi : E_1 \longrightarrow E_2$$

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

The **degree*** is $\deg(\varphi) = \#\ker(\varphi)$

* for separable isogenies

- $\deg(\varphi \circ \psi) = \deg(\varphi) \cdot \deg(\psi)$

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- Cryptosystems "based on" the isogeny problem?

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- Cryptosystems "based on" the isogeny problem?

Expectations: cryptosystems as secure as isogeny problem is hard

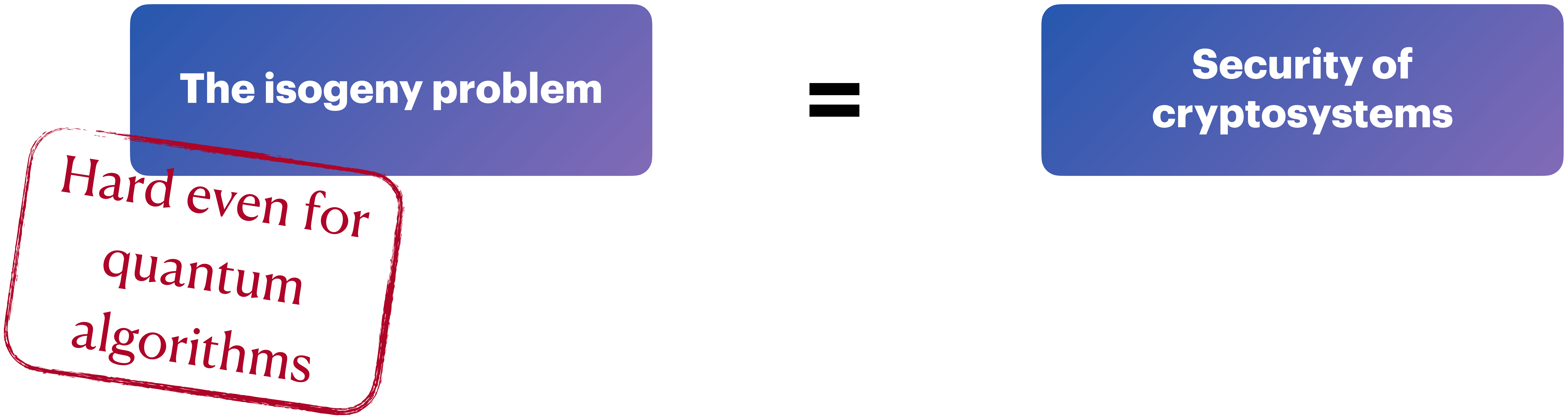
The isogeny problem = **Security of cryptosystems**

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- Cryptosystems "based on" the isogeny problem?

Expectations: cryptosystems as secure as isogeny problem is hard



The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- Cryptosystems "based on" the isogeny problem?

Expectations: cryptosystems as secure as isogeny problem is hard

The isogeny problem = **Security of cryptosystems**

Hard even for quantum algorithms

Post-quantum cryptography

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny…

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny…
- How to represent an isogeny?
- *Hint*: $\ker(\varphi)$ determines φ…

Efficient isogenies

- Given ker(φ) (list of points), can evaluate φ in poly time — Vélu's formulae
  - ✓ Isogenies of *small* degree ℓ = 2, or 3... "ℓ-isogenies"

Efficient isogenies

- Given ker(φ) (list of points), can evaluate φ in poly time — Vélu's formulae

  ✓ Isogenies of *small* degree $\ell = 2$, or 3… "ℓ-isogenies"

- Given random E_1 and E_2, smallest $\varphi : E_1 \to E_2$ has degree poly(p)

  ✗ Typically, $p > 2^{256}$

Efficient isogenies

- Given $\ker(\varphi)$ (list of points), can evaluate φ in poly time — Vélu's formulae

  ✓ Isogenies of *small* degree $\ell = 2$, or 3… "ℓ-isogenies"

- Given random E_1 and E_2, smallest $\varphi : E_1 \to E_2$ has degree poly(p)

  ✗ Typically, $p > 2^{256}$

- Compose small isogenies to build bigger ones!

  ✓ Isogenies with **smooth degree** (small prime factors):

  $\varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1$ represented by ('compose', $\varphi_1, \varphi_2, \ldots, \varphi_n$), with $\deg(\varphi_i)$ small

Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies

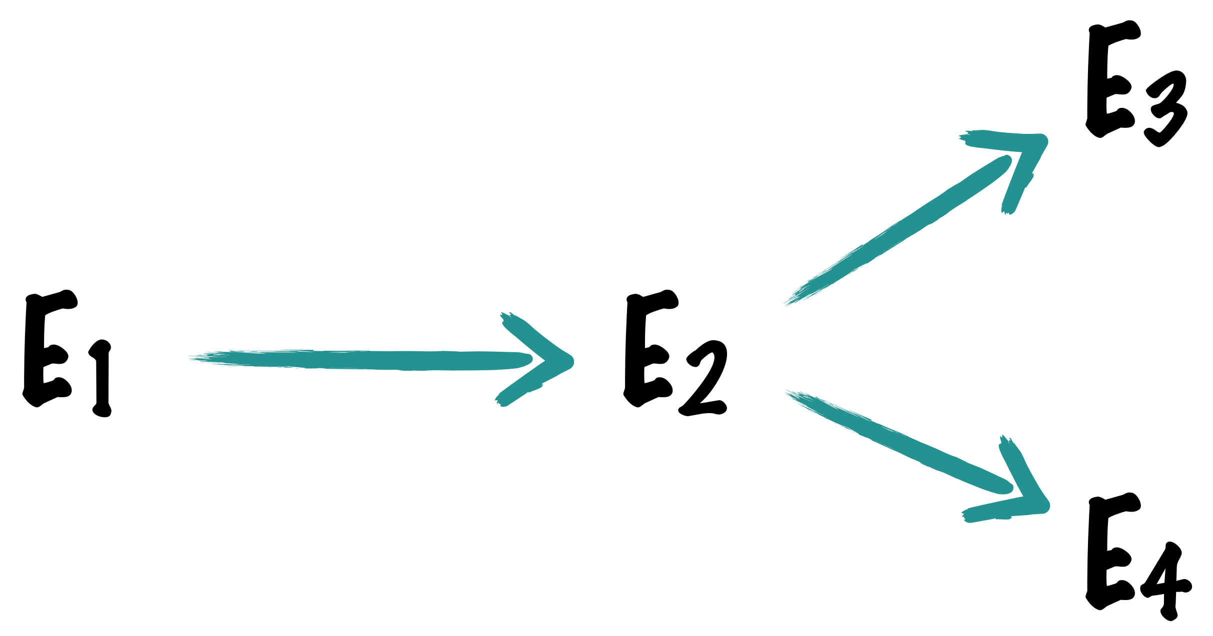
Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies

an isogeny of degree ℓ = an edge in a graph

Isogeny graph

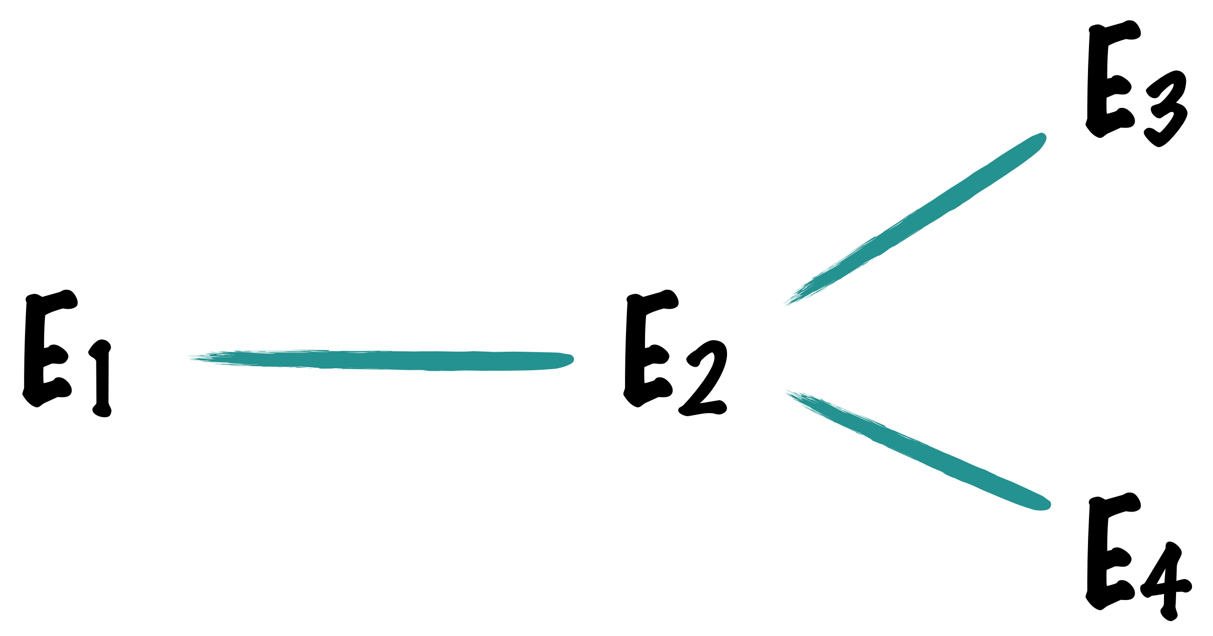
- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies



an isogeny of degree ℓ = an edge in a graph

Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies

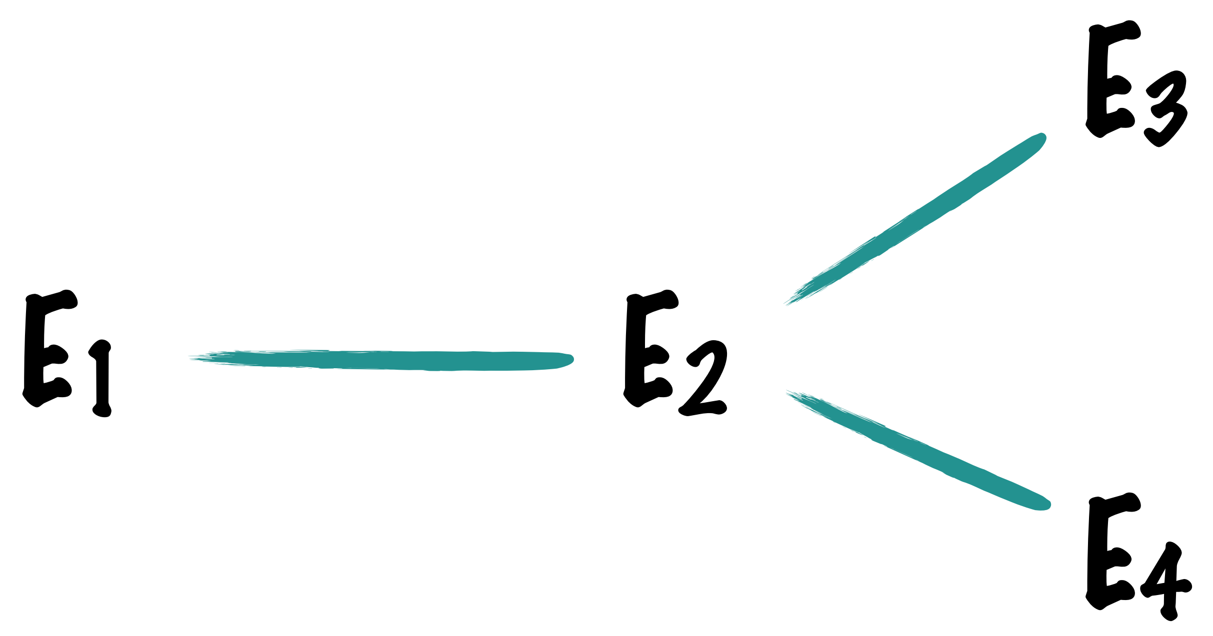


an isogeny of degree ℓ = an edge in a graph

$\exists\ \ell$-isogeny $E_1 \to E_2 \Rightarrow \exists\ \ell$-isogeny $E_2 \to E_1$

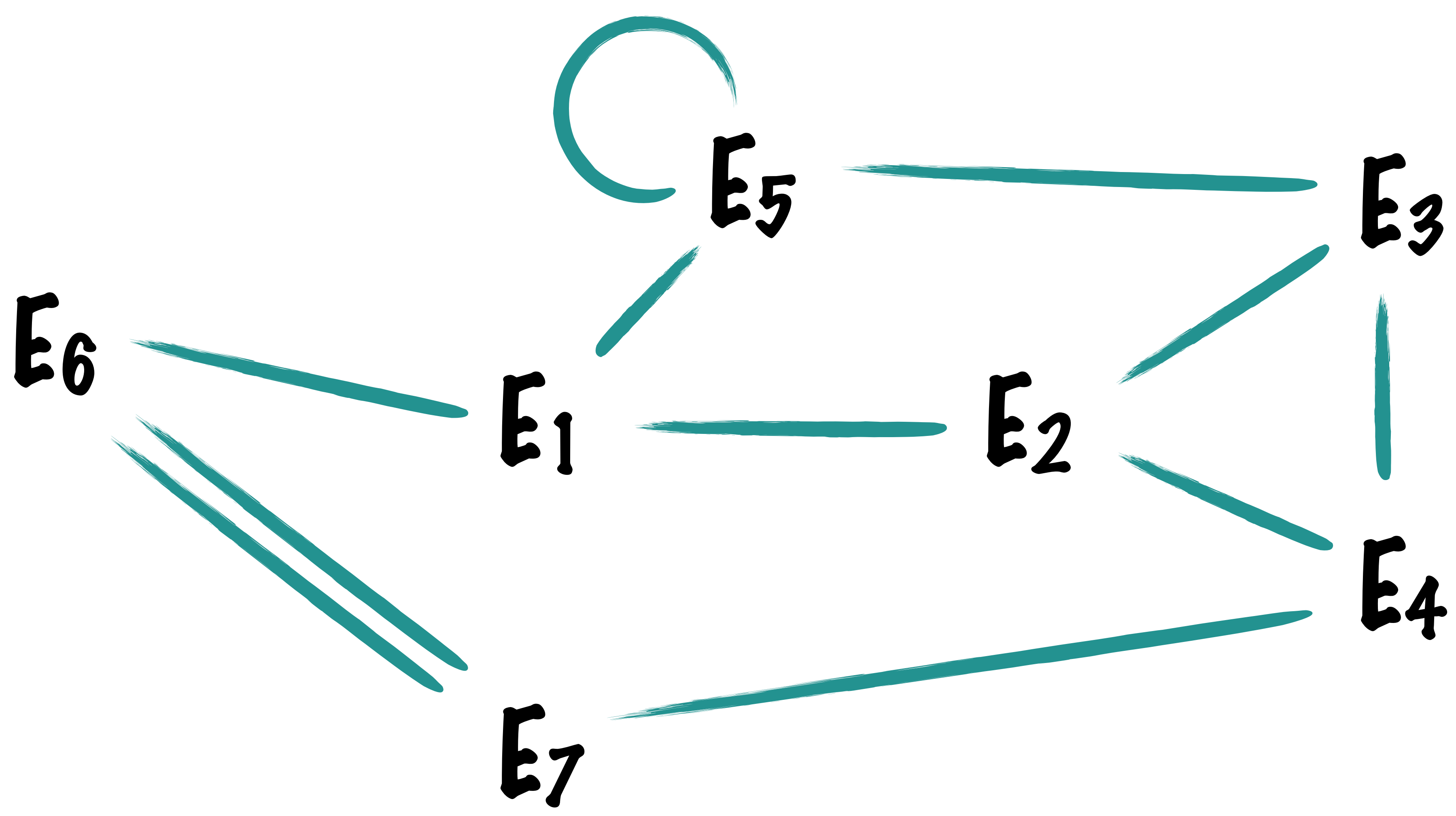
Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies
- **The ℓ-isogeny graph** (supersingular…)



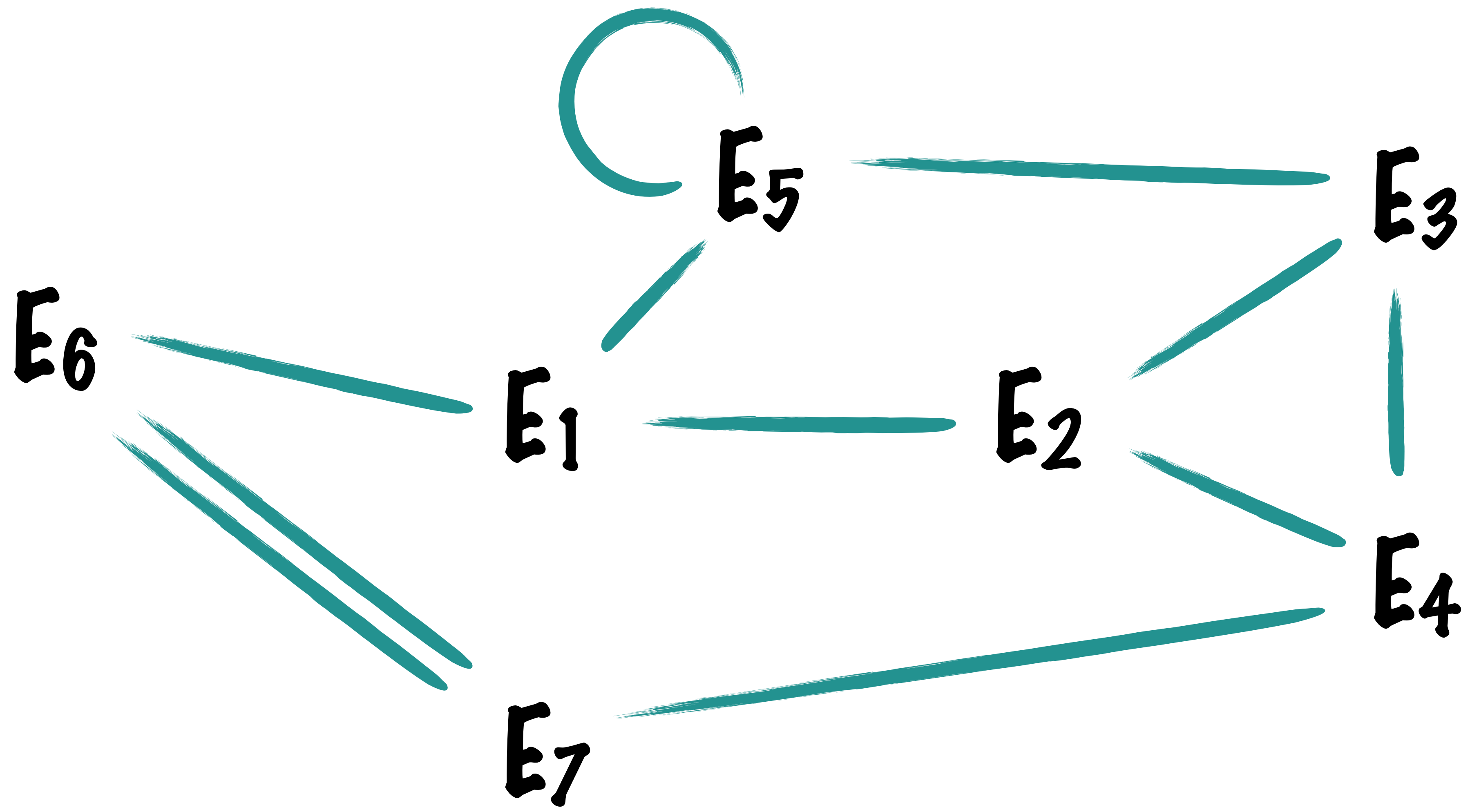
Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies
- **The ℓ-isogeny graph** (supersingular...)



Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies
- **The ℓ-isogeny graph** (supersingular...)



- $(\ell + 1)$-regular, **connected** (for supersingular curves)

The ℓ-isogeny path problem

ℓ-isogeny path problem: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

The ℓ-isogeny path problem

ℓ-isogeny path problem: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

- Path finding in a graph
- Hard! Best known algorithms = generic graph algorithms
- Typical meaning of ***"the isogeny problem"***

Isogeny-based cryptography

Expectations: cryptosystems as secure as isogeny problem is hard

The isogeny problem = **Security of cryptosystems**

Hard even for quantum algorithms

Post-quantum cryptography

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems $\leq$ **Security of cryptosystems** $\leq$ **The isogeny problem**

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems	$\leq$	Security of cryptosystems	$\leq$	The isogeny problem

The isogeny problem = CGL hash function (preimage)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems	≤	Security of cryptosystems	≤	The isogeny problem

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems $\leq$ **Security of cryptosystems** $\leq$ **The isogeny problem**

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems	$\leq$	Security of cryptosystems	$\leq$	The isogeny problem

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
SSI-T	=	SIDH (key recovery)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems	≤	**Security of cryptosystems**	≤	**The isogeny problem**

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
SSI-T	=	SIDH (key recovery)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems ≤ Security of cryptosystems ≤ The isogeny problem

[Jao, De Feo] PQCrypto 2011
Isogeny-based key exchange
NIST PQC alt-finalist

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
SSI-T	=	SIDH (key recovery)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems	≤	Security of cryptosystems	≤	The isogeny problem

The isogeny problem with "torsion point information"...

[Jao, De Feo] PQCrypto 2011
Isogeny-based key exchange
NIST PQC alt-finalist

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
SSI-T	=	SIDH (key recovery)

SIDH

Jao–De Feo 2011

Quotients

- Let E be an elliptic curve
- Let G a finite subgroup of E

Quotients

- Let E be an elliptic curve
- Let G a finite subgroup of E
- **Quotienting by G:** there is a unique (separable) isogeny

$$\varphi : E \longrightarrow E/G$$

  with $\ker(\varphi) = G$

Quotients

- Let E be an elliptic curve
- Let G a finite subgroup of E
- **Quotienting by G:** there is a unique (separable) isogeny

  $$\varphi : E \to E/G$$

  with $\ker(\varphi) = G$
- $\deg(\varphi) = \#G$

Quotients

- Let E be an elliptic curve
- Let G a finite subgroup of E
- **Quotienting by G:** there is a unique (separable) isogeny

$$\varphi : E \to E/G$$

  with $\ker(\varphi) = G$

- $\deg(\varphi) = \#G$
- Given generators of G, if $\#G$ has **only small prime factors**, then φ can be **computed efficiently**

SIDH

Fix reference elliptic curve E_0

Alice

Bob

SIDH

Fix reference elliptic curve E_0

Alice

Bob

Random subgroup G of E_0

SIDH

Fix reference elliptic curve E_0

Alice **Bob**

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

SIDH

Fix reference elliptic curve E_0

Alice

Bob

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

SIDH

Fix reference elliptic curve E_0

Alice | **Bob**

Random subgroup G of E_0

Compute $\varphi_A : E_0 \longrightarrow E_0/G$

Let $E_A = E_0/G$

E_A →

SIDH

Fix reference elliptic curve E_0

Alice

Bob

Random subgroup G of E_0

Compute $\varphi_A : E_0 \longrightarrow E_0/G$

Let $E_A = E_0/G$

$\xrightarrow{E_A}$

$$E_0 \xrightarrow{\varphi_A} E_A = E_0/G$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

$\xrightarrow{E_A}$

Bob

Random subgroup H of E_0

$$\begin{array}{c} E_0 \\ \varphi_A \big\downarrow \\ E_A = E_0/G \end{array}$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

E_A →

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

$$E_0 \xrightarrow{\varphi_A} E_A = E_0/G$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

$\xrightarrow{E_A}$

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

$$\begin{array}{c} E_0 \\ \varphi_A \big\downarrow \\ E_A = E_0/G \end{array}$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

E_A →

← E_B

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

$$E_0 \xrightarrow{\varphi_A} E_A = E_0/G$$

SIDH

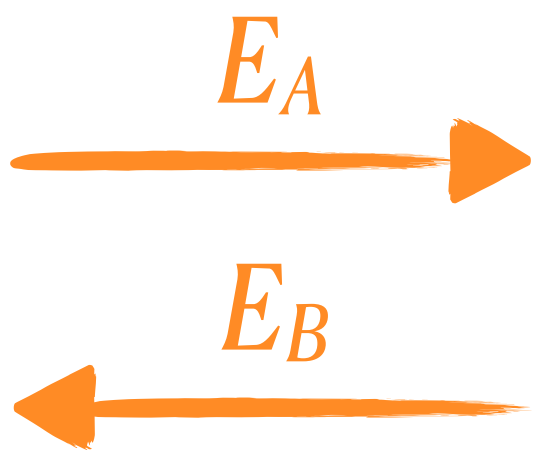
Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

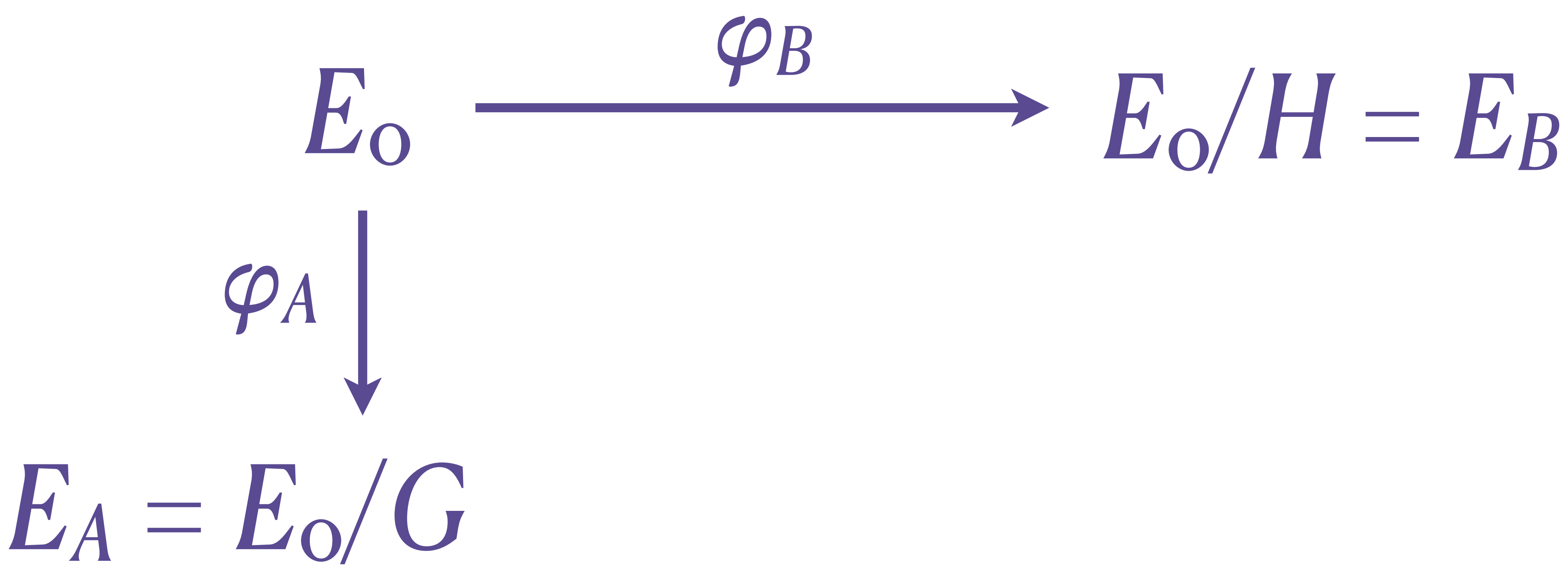


Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$



SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

E_A →

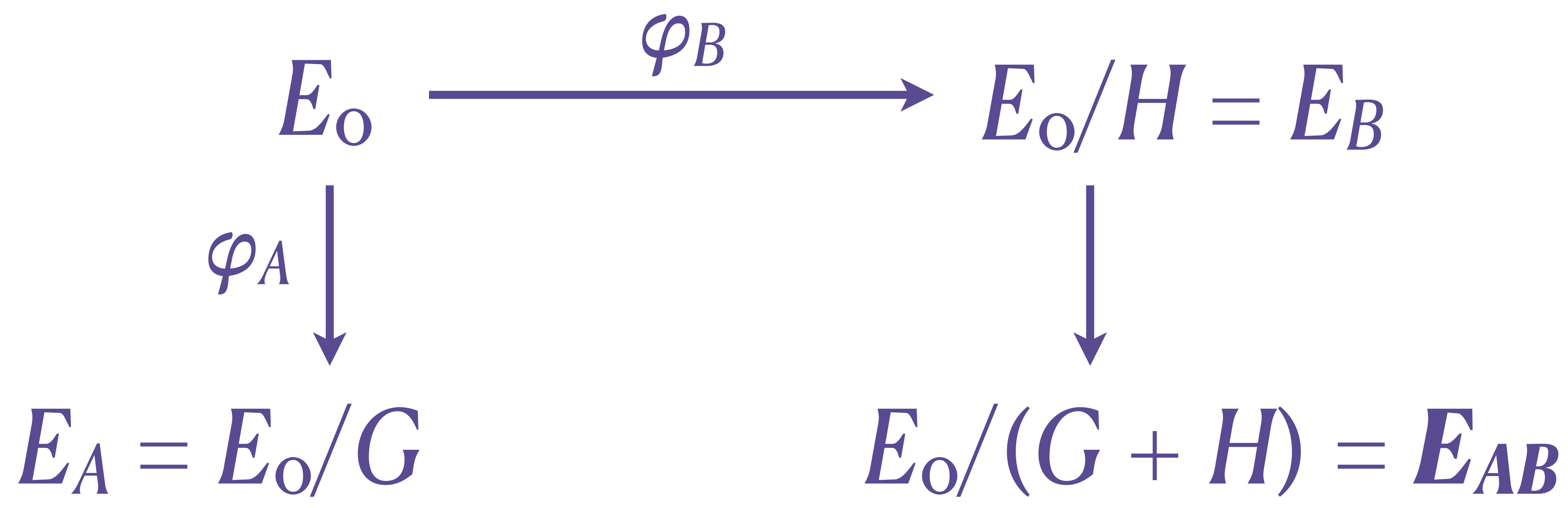
← E_B

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$



SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

Compute $\boldsymbol{E_{AB}} = E_B/G$

E_A →

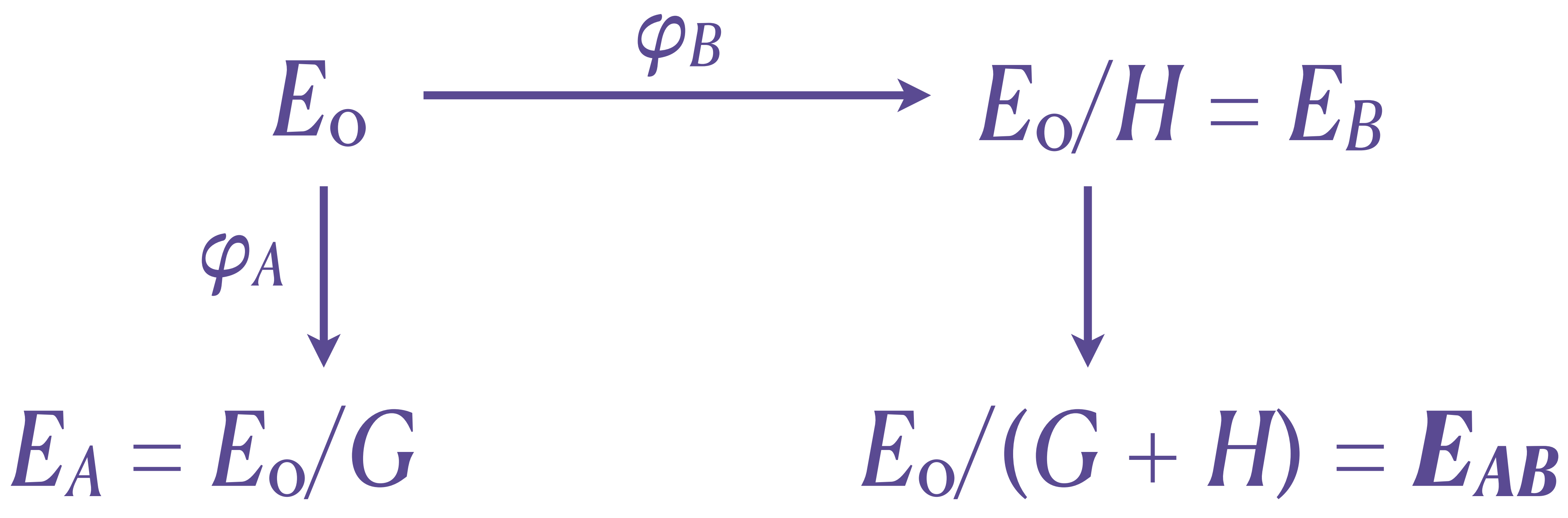
← E_B

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$



SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

Compute $\boldsymbol{E_{AB}} = E_B/G$

E_A →

← E_B

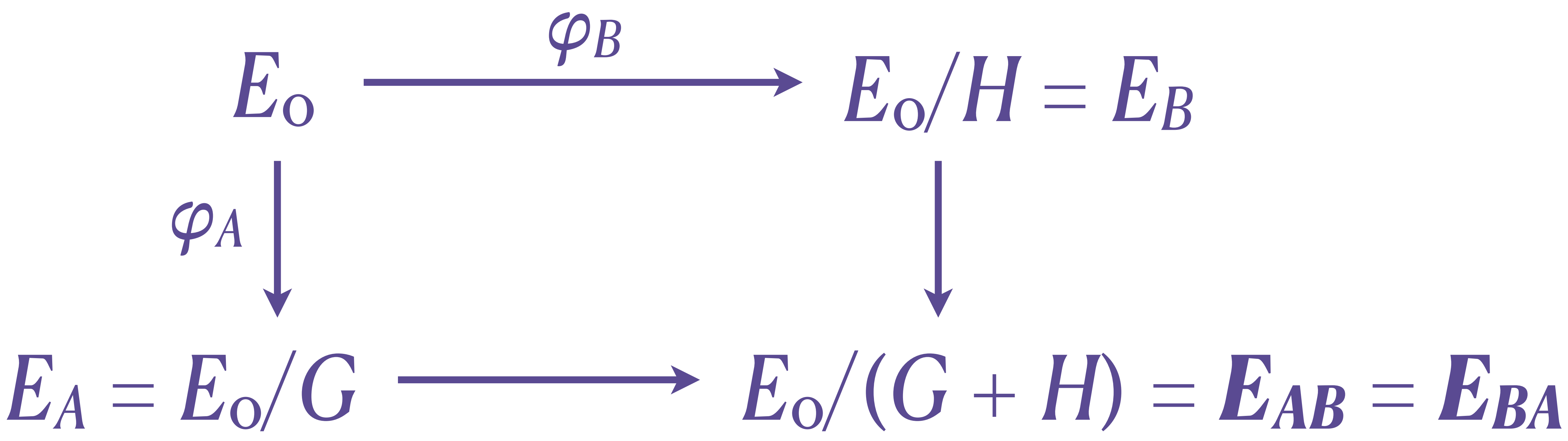
Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/H$



SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

Compute $\boldsymbol{E_{AB}} = E_B/G$

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/H$

Alice → Bob: E_A

Bob → Alice: E_B

G is not a subgroup of E_B

$\varphi_B(G)$ is!

SIDH

Fix reference elliptic curve E_0

Alice		**Bob**
Random subgroup G of E_0		Random subgroup H of E_0
Compute $\varphi_A : E_0 \to E_0/G$	E_A →	Compute $\varphi_B : E_0 \to E_0/H$
Let $E_A = E_0/G$	← E_B	Let $E_B = E_0/H$
Compute $\boldsymbol{E_{AB}} = E_B/G$		Compute $\boldsymbol{E_{BA}} = E_A/H$

G is not a subgroup of E_B
$\varphi_B(G)$ is!

How to compute $\varphi_B(G)$?
Alice does not know φ_B...

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Idea:

- Alice picks a subgroup G of $E_0[2^n]$
- Bob gives φ_B on $E_0[2^n]$
- Alice can compute $\varphi_B(G)$

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Idea:

- Alice picks a subgroup G of $E_0[2^n]$ ⟵ Many choices, good entropy
- Bob gives φ_B on $E_0[2^n]$
- Alice can compute $\varphi_B(G)$

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Idea:

- Alice picks a subgroup G of $E_0[2^n]$ ← Many choices, good entropy
- Bob gives φ_B on $E_0[2^n]$ ← φ_B remains secret everywhere else…
- Alice can compute $\varphi_B(G)$

Torsion

- The N-torsion of E is the subgroup

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Idea:

- Alice picks a subgroup G of $E_0[2^n]$ ← Many choices, good entropy
- Bob gives φ_B on $E_0[2^n]$ ← φ_B remains secret everywhere else...
- Alice can compute $\varphi_B(G)$ ← Can compute shared secret $\boldsymbol{E_{AB}} = E_B/\varphi_B(G)$

SIDH

Fix: an elliptic curve E_0

Generators P_2, Q_2 of $E_0[2^n] \cong (\mathbb{Z}/2^n\mathbb{Z})^2$

Generators P_3, Q_3 of $E_0[3^m] \cong (\mathbb{Z}/3^m\mathbb{Z})^2$

Alice

Random subgroup G of $E_0[2^n]$

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

$E_A, \varphi_A(P_3), \varphi_A(Q_3)$ →

← $E_B, \varphi_B(P_2), \varphi_B(Q_2)$

Compute $\boldsymbol{E_{AB}} = E_B/\varphi_B(G)$

Bob

Random subgroup H of $E_0[3^m]$

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/\varphi_A(H)$

The SSI-T problem

Context:

- two elliptic curves E_0 and E_1
- an isogeny $\varphi : E_0 \to E_1$ (say, of degree 3^m like Bob's isogeny)
- an integer N coprime to $\deg(\varphi)$ (say, $N = 2^n$...)
- generators P and Q of $E_0[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

SSI-T: Given E_0, E_1, P, Q, $\varphi(P)$ and $\varphi(Q)$, find the isogeny $\varphi : E_0 \to E_1$

The SSI-T problem

Context:

- two elliptic curves E_0 and E_1
- an isogeny $\varphi : E_0 \to E_1$ (say, of degree 3^m like Bob's isogeny)
- an integer N coprime to $\deg(\varphi)$ (say, $N = 2^n$...)
- generators P and Q of $E_0[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

"torsion point information"

SSI-T: Given E_0, E_1, P, Q, $\varphi(P)$ and $\varphi(Q)$, find the isogeny $\varphi : E_0 \to E_1$

The SSI-T problem

Context:

- two elliptic curves E_0 and E_1
- an isogeny $\varphi : E_0 \to E_1$ (say, of degree 3^m like Bob's isogeny)
- an integer N coprime to deg(φ) (say, $N = 2^n$...)
- generators P and Q of $E_0[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

"torsion point information"

SSI-T: Given E_0, E_1, P, Q, $\varphi(P)$ and $\varphi(Q)$, find the isogeny $\varphi : E_0 \to E_1$

SIDH key recovery ⇔ SSI-T

Torsion point information: a weakness?

Torsion point information: a weakness?

Torsion point information: a weakness?

2011

Birth of SIDH

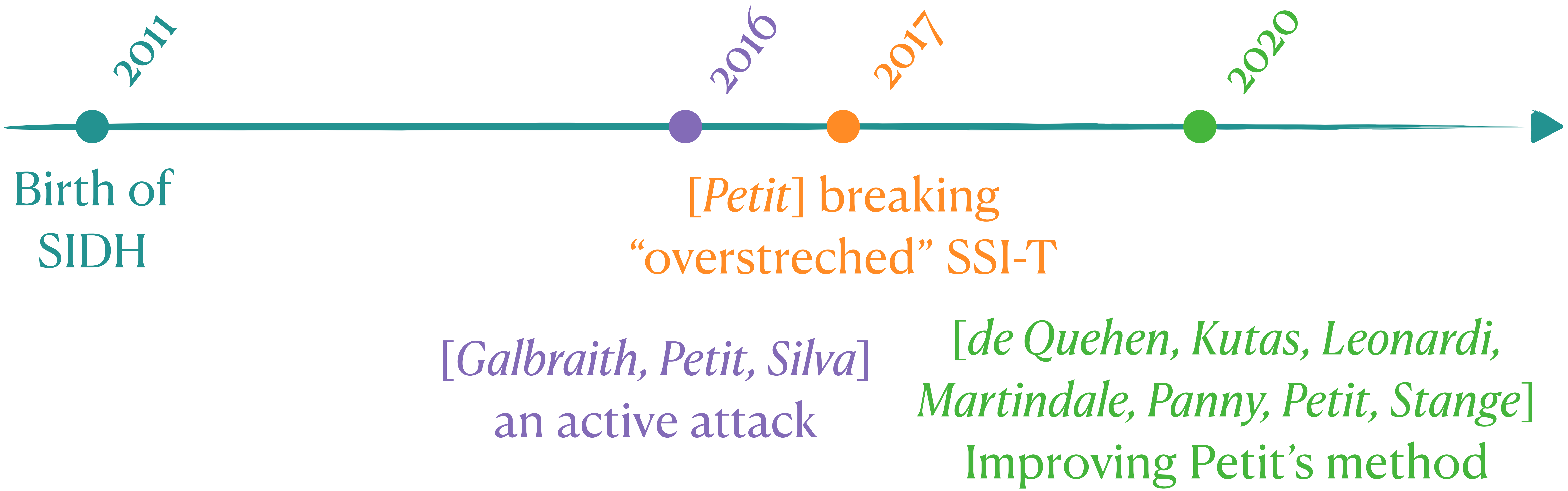
2016

[*Galbraith, Petit, Silva*] an active attack

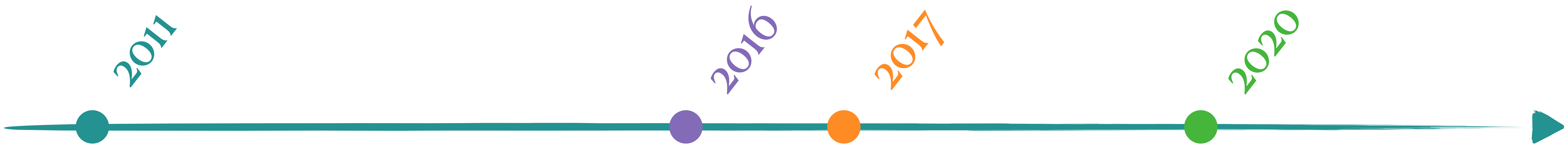
2017

[*Petit*] breaking "overstreched" SSI-T

Torsion point information: a weakness?



Torsion point information: a weakness?



Birth of SIDH

[*Petit*] breaking "overstreched" SSI-T

[*Galbraith, Petit, Silva*] an active attack

[*de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange*] Improving Petit's method

Standard SIDH parameters totally unaffected

The Snap

July 30 2022


July 29 2022
Enjoying the French Alps

July 30 2022

eprint 2022/975

July 30 2022

eprint 2022/975

An efficient key recovery attack on SIDH

July 30 2022

eprint 2022/975

An efficient key recovery attack on SIDH

Wouter Castryck, Thomas Decru

July 30 2022

eprint 2022/975

An efficient key recovery attack on SIDH

Wouter Castryck, Thomas Decru

"Breaks SIKEp434 challenge in ten minutes"

Eurocrypt 2023 – “Isogeny 1” session

Efficient Key Recovery Attack on SIDH (Best Paper Award)

[Castryck, Decru]

A Direct Key Recovery Attack on SIDH (Honourable Mention)

[Maino, Martindale, Panny, Pope, W.]

Breaking SIDH in Polynomial Time (Honourable Mention)

[Robert]

Main result of the attacks

Interpolating isogenies [CD, MMPPW, R]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Main result of the attacks

Interpolating isogenies [CD, MMPPW, R]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points ⇒ Knowing φ everywhere**

Main result of the attacks

Interpolating isogenies [CD, MMPPW, R]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

Corollary: The few points leaked by SIDH leak the full secret.

Isogeny-based cryptography

Body count

Weird scheme-dependent variants of isogeny problems	$\leq$	**Security of cryptosystems**	$\leq$	**The isogeny problem**

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
SSI-T	=	SIDH (key recovery)

Isogeny-based cryptography

Body count

Weird scheme-dependent variants of isogeny problems $\leq$ **Security of cryptosystems** $\leq$ **The isogeny problem**

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
~~SSI-T~~	~~=~~	~~SIDH (key recovery)~~

Isogeny-based cryptography

Body count

Weird scheme-dependent variants of isogeny problems ≤ **Security of cryptosystems** ≤ **The isogeny problem**

The isogeny problem	=	CGL hash function (preimage)
One endomorphism	=	SQISign (soundness)
Vectorisation	=	CSIDH (key recovery)
~~SSI-T~~	~~=~~	~~SIDH (key recovery)~~

~~B-SIDH~~

~~k-SIDH~~

~~Séta~~

~~SHealS~~

Rundown of survivors

Rundown of survivors

- **The isogeny path problem is unaffected**

Rundown of survivors

- **The isogeny path problem is unaffected**
- SQIsign [De Feo, Kohel, Leroux, Petit, W.] unaffected
  - ➡ Signature scheme, most compact `pk` + `sig` of all PQ schemes
  - ➡ Submitted to the NIST PQ signature call 2023

Rundown of survivors

- **The isogeny path problem is unaffected**
- SQIsign [De Feo, Kohel, Leroux, Petit, W.] unaffected
  - ➡ Signature scheme, most compact `pk` + `sig` of all PQ schemes
  - ➡ Submitted to the NIST PQ signature call 2023
- CSIDH [Castryck, Lange, Martindale, Panny, Renes] unaffected
  - ➡ Key exchange very similar to Diffie–Hellman

Rundown of survivors

- **The isogeny path problem is unaffected**
- SQIsign [De Feo, Kohel, Leroux, Petit, W.] unaffected
  - ➡ Signature scheme, most compact pk + sig of all PQ schemes
  - ➡ Submitted to the NIST PQ signature call 2023
- CSIDH [Castryck, Lange, Martindale, Panny, Renes] unaffected
  - ➡ Key exchange very similar to Diffie–Hellman
- Wide variety of *CSIDH-inspired* constructions
  - ➡ "group action" cryptography
  - ➡ Signatures, PRFs, threshold stuff, oblivious stuff…

Fixing SIDH?

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Fixing SIDH?

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Use random secret degree:
MD-SIDH (Masked Degree)

Fixing SIDH?

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Use random secret degree:
MD-SIDH (Masked Degree)

Instead of $\varphi(P), \varphi(Q)$, send $a \cdot \varphi(P)$, $a \cdot \varphi(Q)$ for random integer a: **M-SIDH**

Fixing SIDH?

Interpolating isogenies [CD23, MMPPW23, Rob23]:

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Use random secret degree: **MD-SIDH** (Masked Degree)

Instead of $\varphi(P), \varphi(Q)$, send $a \cdot \varphi(P)$, $a \cdot \varphi(Q)$ for random integer a: **M-SIDH**

- Fouotsa, Moriya, Petit. Eurocrypt 2023

Fixing SIDH?

Interpolating isogenies [CD23, MMPPW23, Rob23]:

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

Use random secret degree: **MD-SIDH** (Masked Degree)

Instead of $\varphi(P), \varphi(Q)$, send $a \cdot \varphi(P)$, $a \cdot \varphi(Q)$ for random integer a: **M-SIDH**

- Fouotsa, Moriya, Petit. Eurocrypt 2023
- Huge cost: 4434 bytes public keys (vs. 197 bytes in SIKE)

Representing isogenies

Back to the foundations

The isogeny problem

"Idealised" isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

ℓ-isogeny path problem: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

The isogeny problem

"Idealised" isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

ℓ-isogeny path problem: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

- The **ℓ-isogeny path problem** is the standard version of "**the isogeny problem**" because… no other way to represent solution $\varphi : E_1 \to E_2$ than as a path?

  ➡ Strong restriction on φ because of technical obstacle

The isogeny problem

"Idealised" isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

ℓ-isogeny path problem: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

- The **ℓ-isogeny path problem** is the standard version of "**the isogeny problem**" because... no other way to represent solution $\varphi : E_1 \to E_2$ than as a path?

    ➡ Strong restriction on φ because of technical obstacle

- **How to represent an isogeny?**

Efficient representation of isogenies

How to represent an isogeny?

- an **efficient representation** of φ: can evaluate $\varphi(P)$ in poly. time for any P

Efficient representation of isogenies

How to represent an isogeny?

- an **efficient representation** of φ: can evaluate $\varphi(P)$ in poly. time for any P

Examples:

- Small degree isogenies
- Compositions of small degree isogenies
- Linear combinations of compositions of small degree isogenies…

Main result of the attacks

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

Main result of the attacks

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points ⇒ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ.

Main result of the attacks

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points ⇒ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ.

- **“Interpolation representation”** of φ, or “HD representation”

Main result of the attacks

Interpolating isogenies [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let $n > (\log_2(d) + 1)/2$, and (P, Q) is a basis of $E_1[2^n]$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time
- Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ.

- **"Interpolation representation"** of φ, or "HD representation"
- Universal! Given any efficient repr. of φ, can compute its interpolation repr.

The universal isogeny problem

The universal isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$ represented by interpolation.

The universal isogeny problem

The universal isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$ represented by interpolation.

- No restriction on φ like in ℓ-isogeny path: any φ can be a valid response

The universal isogeny problem

The universal isogeny problem: Given E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$ represented by interpolation.

- No restriction on φ like in ℓ-isogeny path: any φ can be a valid response

Universal isogeny $\Leftrightarrow$ ℓ-isogeny path

[Page, W.] to appear

From attacks to constructions

Interpolation representation: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient repr. of φ

- **Powerful new tool**

From attacks to constructions

Interpolation representation: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient repr. of φ

- **Powerful new tool**

New constructions are emerging

From attacks to constructions

Interpolation representation: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient repr. of φ

- **Powerful new tool**

New constructions are emerging

- **SQIsign HD** [Dartois, Leroux, Robert, W.]: signature scheme inspired by SQIsign
  - ➡ Faster, simpler signing
  - ➡ Improved security proof

From attacks to constructions

Interpolation representation: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient repr. of φ

- **Powerful new tool**

New constructions are emerging

- **SQIsign HD** [Dartois, Leroux, Robert, W.]: signature scheme inspired by SQIsign
  - ➡ Faster, simpler signing
  - ➡ Improved security proof
- **FESTA** [Basso, Maino, Pope]: Fast Encryption from Supersingular Torsion Attacks

From attacks to constructions

Interpolation representation: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient repr. of φ

- **Powerful new tool**

How efficient is it?

New constructions are emerging

- **SQIsign HD** [Dartois, Leroux, Robert, W.]: signature scheme inspired by SQIsign
  - ➡ Faster, simpler signing
  - ➡ Improved security proof
- **FESTA** [Basso, Maino, Pope]: Fast Encryption from Supersingular Torsion Attacks

The attack

Isogenies in higher dimension

Dual

Let E an elliptic curve over $\mathbb{F}_q$ and N an integer

- Multiplication by N is an isogeny

$$[N] : E \to E : P \longmapsto [N]P = P + P + \ldots + P$$

Dual

Let E an elliptic curve over $\mathbb{F}_q$ and N an integer

- Multiplication by N is an isogeny

$$[N] : E \to E : P \longmapsto [N]P = P + P + \ldots + P$$

- Let $\varphi : E_1 \to E_2$ be an isogeny

Dual

Let E an elliptic curve over $\mathbb{F}_q$ and N an integer

- Multiplication by N is an isogeny

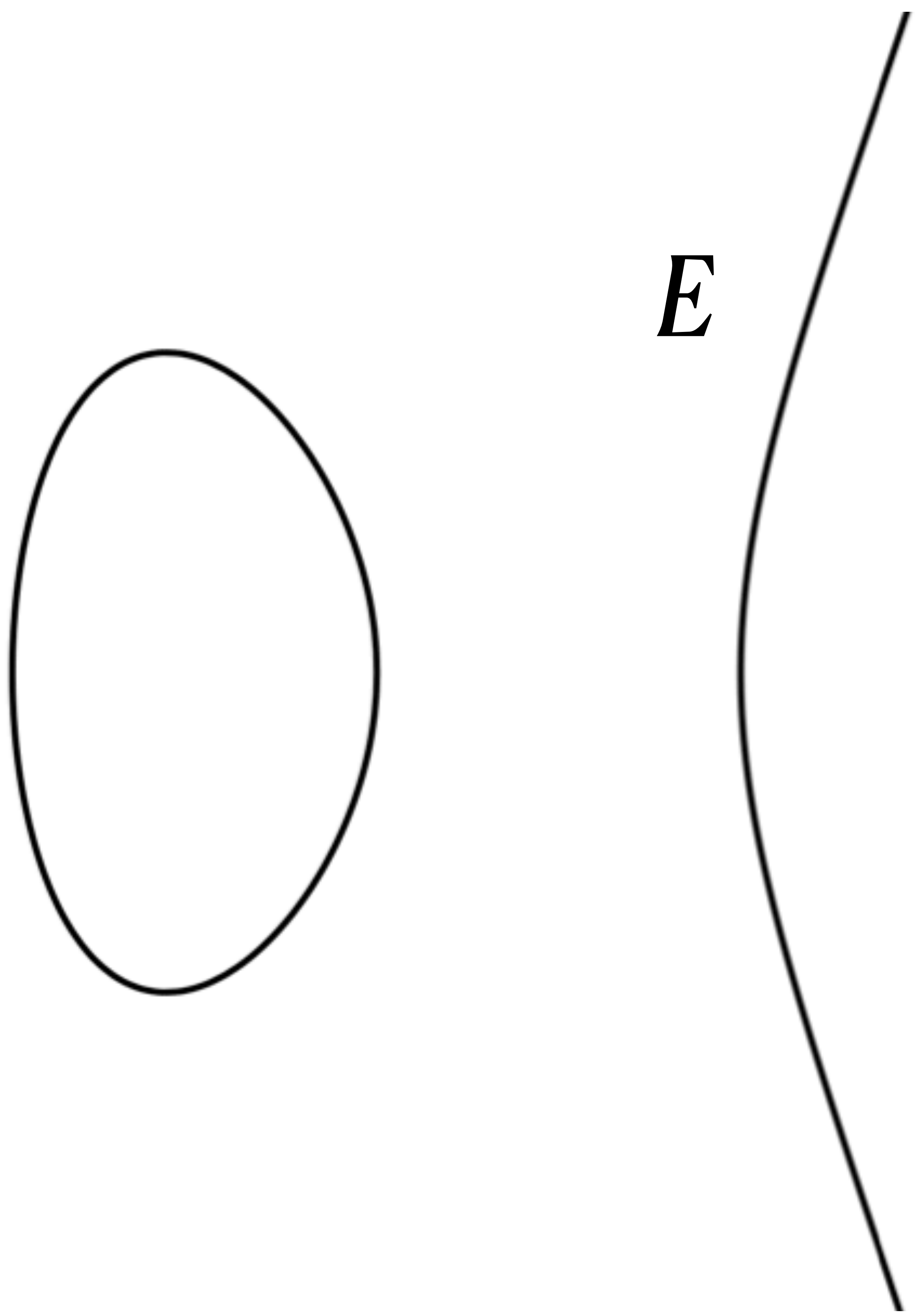
$$[N] : E \to E : P \longmapsto [N]P = P + P + ... + P$$

- Let $\varphi : E_1 \to E_2$ be an isogeny
- **Dual of φ:** unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that

$$\hat{\varphi} \circ \varphi = [\deg(\varphi)]$$

Abelian varieties

Elliptic curve: a curve that is also a group

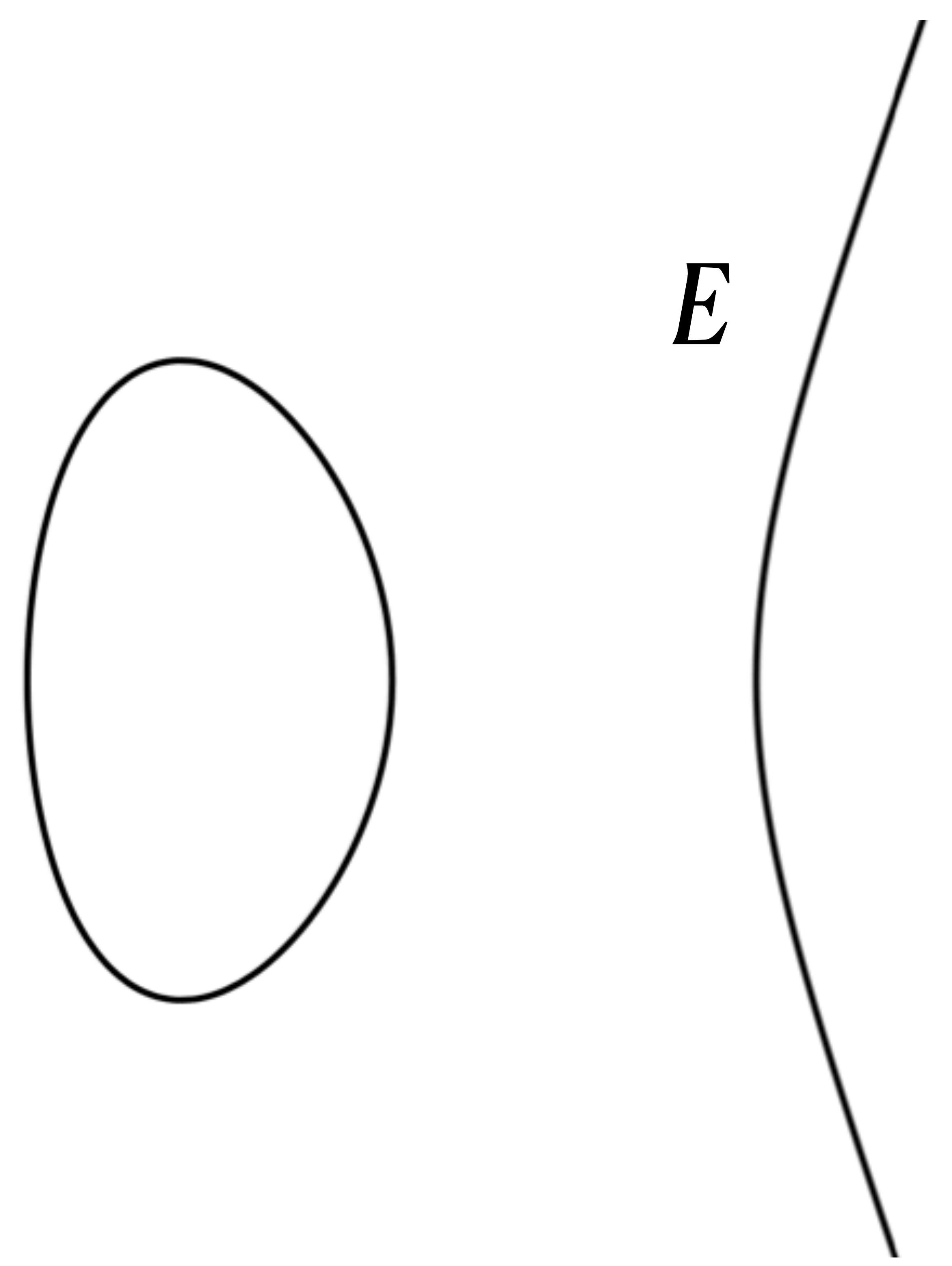


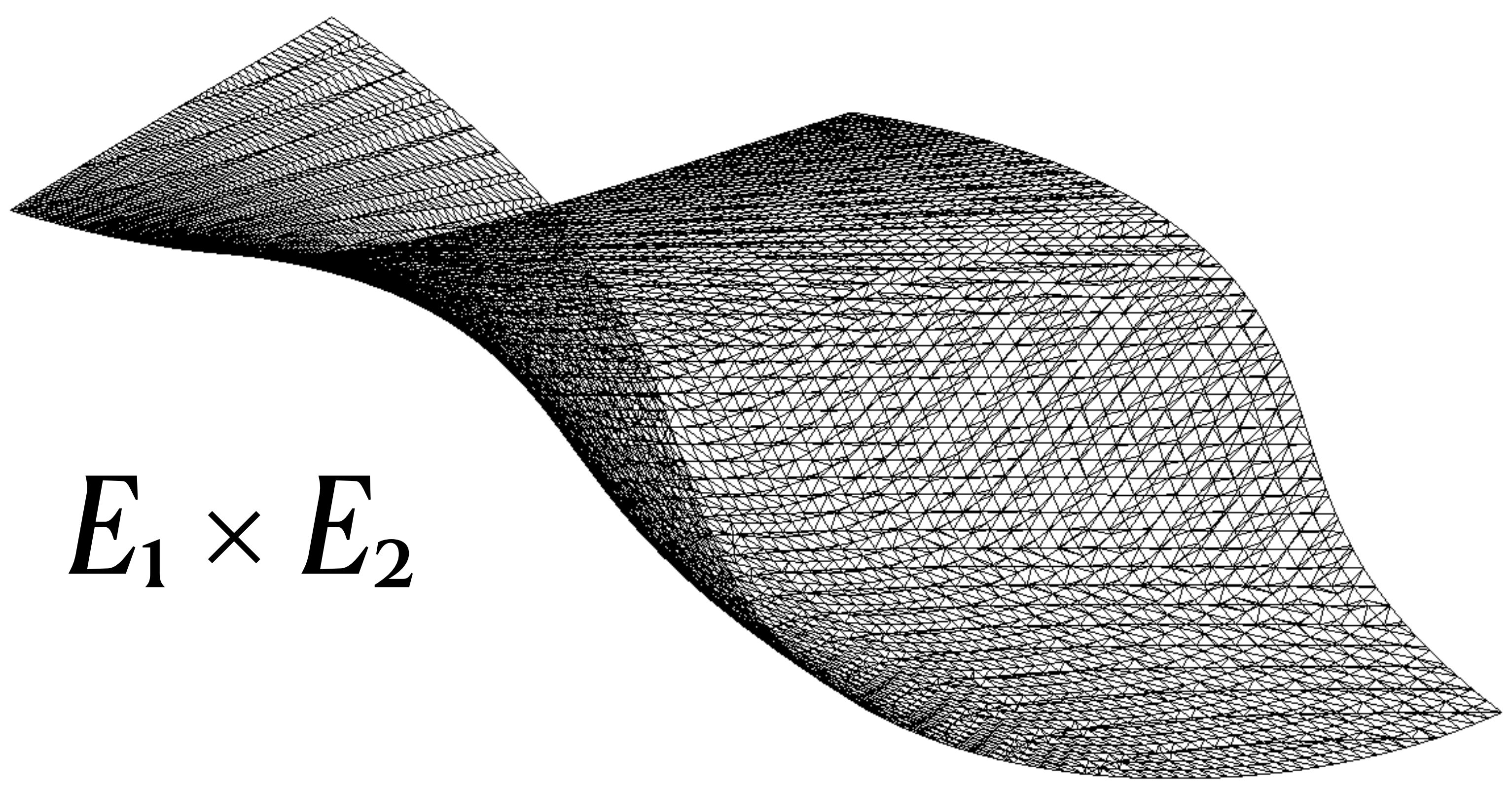
Abelian varieties

Elliptic curve: a curve that is also a group

Abelian surface: surface that is also a group

- Example: product $E_1 \times E_2$





Abelian varieties

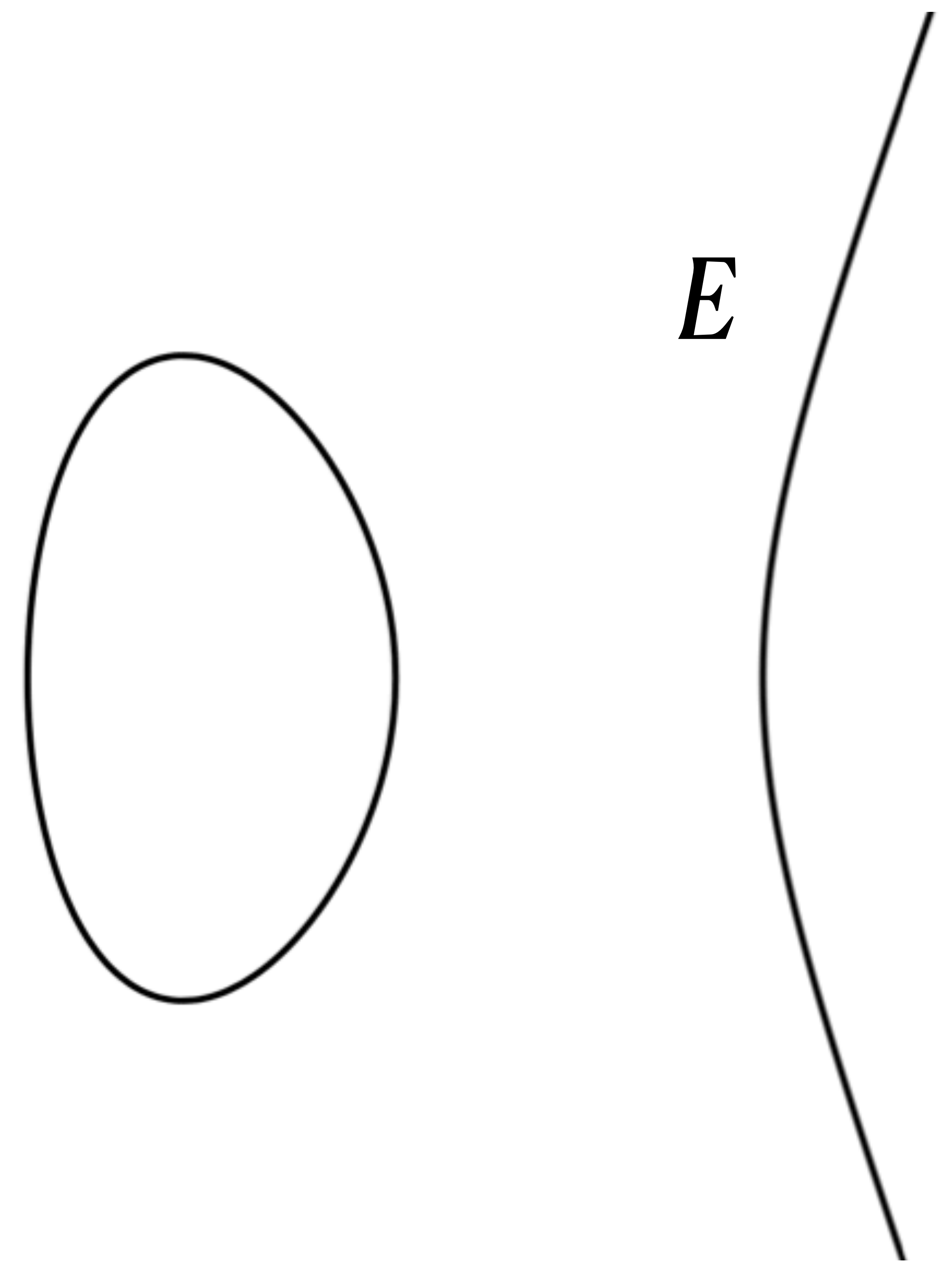
Elliptic curve: a curve that is also a group

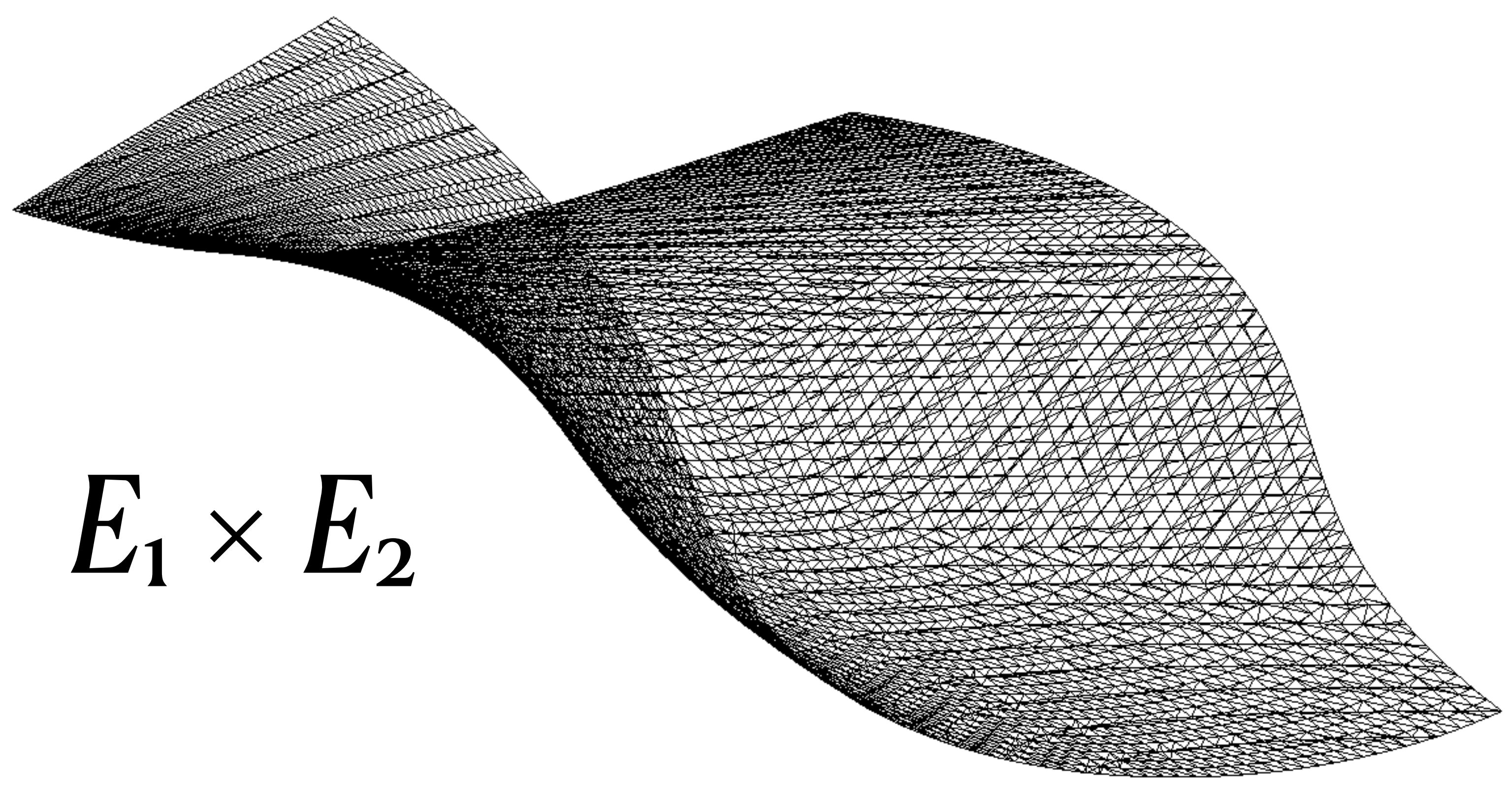
Abelian surface: surface that is also a group

- Example: product $E_1 \times E_2$

Abelian variety: same but any dimension

- Example: product $E_1 \times E_2 \times \ldots \times E_n$





Isogenies between products

$$\Psi : \; E_1 \times E_2 \longrightarrow F_1 \times F_2$$

Isogenies between products

$$\Psi : E_1 \times E_2 \longrightarrow F_1 \times F_2$$

$$(P_1, P_2) \longmapsto$$

Isogenies between products

φ_{11}

$$\Psi: \quad E_1 \times E_2 \longrightarrow F_1 \times F_2$$

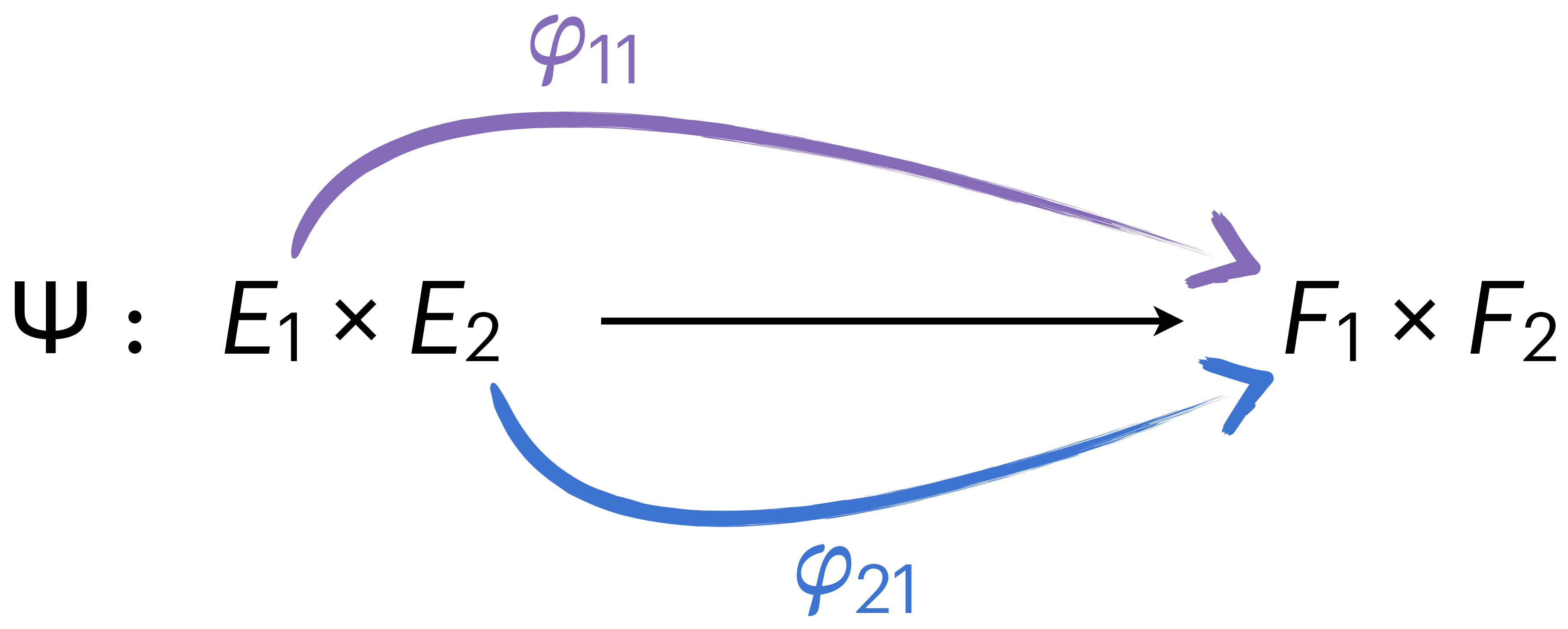
$$(P_1, P_2) \longmapsto$$

Isogenies between products

$$\Psi: E_1 \times E_2 \xrightarrow{\varphi_{11}} F_1 \times F_2$$

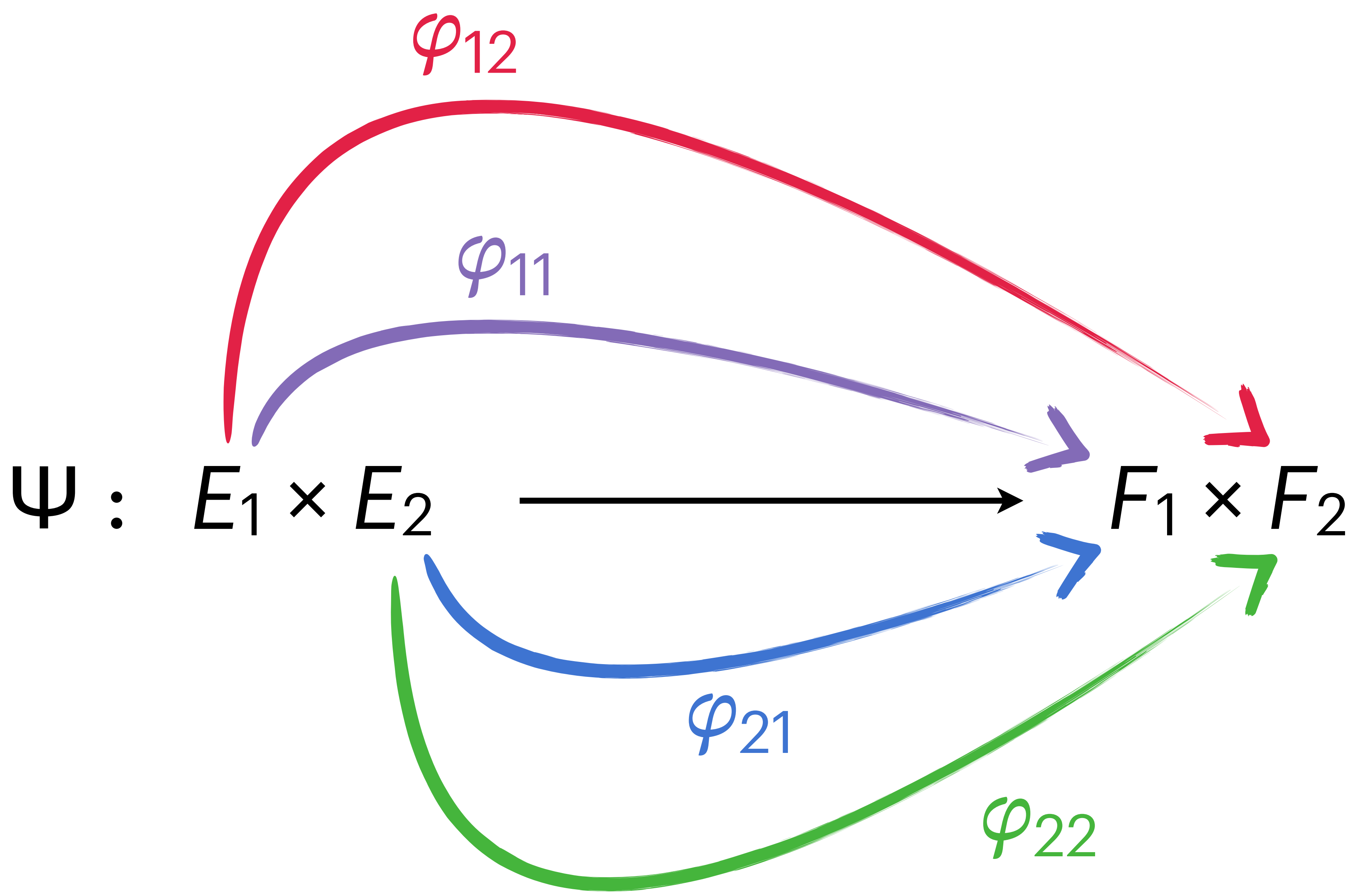
$$(P_1, P_2) \longmapsto (\varphi_{11}(P_1), ?)$$

Isogenies between products



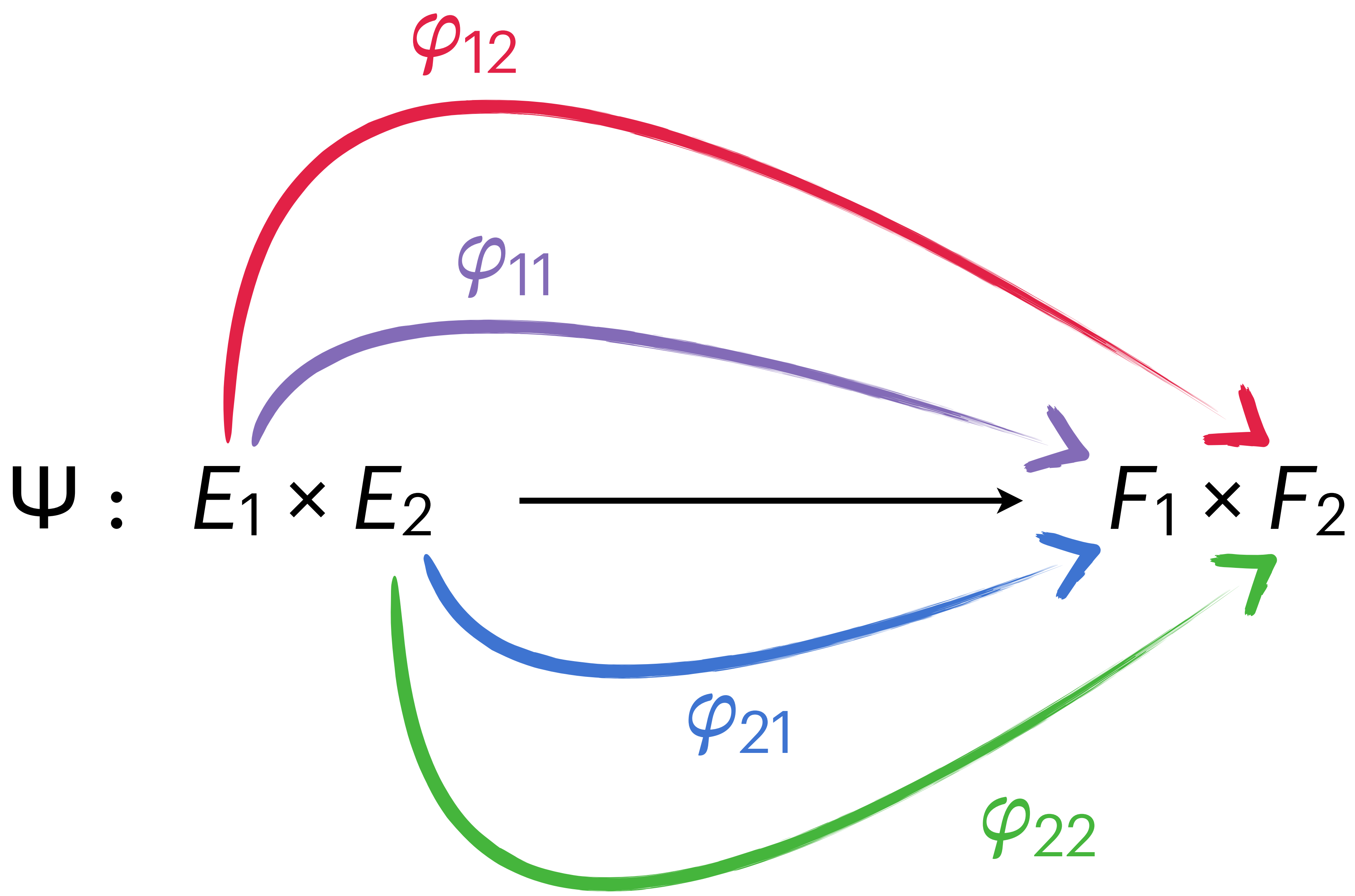
$$(P_1, P_2) \longmapsto (\varphi_{11}(P_1) + \varphi_{21}(P_2), ?)$$

Isogenies between products



$$(P_1, P_2) \longmapsto (\varphi_{11}(P_1) + \varphi_{21}(P_2), \varphi_{12}(P_1) + \varphi_{22}(P_2))$$

Isogenies between products



$$\Psi : E_1 \times E_2 \longrightarrow F_1 \times F_2$$

$$(P_1, P_2) \longmapsto (\varphi_{11}(P_1) + \varphi_{21}(P_2), \varphi_{12}(P_1) + \varphi_{22}(P_2))$$

$$= \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

Isogenies between products

Every isogeny $\Psi : E_1 \times E_2 \to F_1 \times F_2$ is of the form

$$\begin{aligned} \Psi : \quad E_1 \times E_2 & \longrightarrow F_1 \times F_2 \\ (P_1, P_2) & \longmapsto \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \end{aligned}$$

where $\varphi_{ij} : E_i \to F_j$

Isogenies between products

Every isogeny $\Psi : E_1 \times E_2 \to F_1 \times F_2$ is of the form

$$\begin{aligned} \Psi : \quad E_1 \times E_2 &\longrightarrow F_1 \times F_2 \\ (P_1, P_2) &\longmapsto \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \end{aligned}$$

where $\varphi_{ij} : E_i \to F_j$

- It is an ***N*-isogeny** if

$$\begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} \hat{\varphi}_{11} & \hat{\varphi}_{12} \\ \hat{\varphi}_{21} & \hat{\varphi}_{22} \end{pmatrix} = \begin{pmatrix} [N] & 0 \\ 0 & [N] \end{pmatrix}$$

Isogenies between products

Every isogeny $\Psi : E_1 \times E_2 \to F_1 \times F_2$ is of the form

$$\Psi : \quad E_1 \times E_2 \longrightarrow F_1 \times F_2$$
$$(P_1, P_2) \longmapsto \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

where $\varphi_{ij} : E_i \to F_j$

- It is an ***N*-isogeny** if

$$\begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} \cdot \begin{pmatrix} \hat{\varphi}_{11} & \hat{\varphi}_{12} \\ \hat{\varphi}_{21} & \hat{\varphi}_{22} \end{pmatrix} = \begin{pmatrix} [N] & 0 \\ 0 & [N] \end{pmatrix}$$

- Given the kernel of a 2^n-isogeny, can evaluate it in polynomial time

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \longrightarrow E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \longrightarrow E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

$$E_1 \xrightarrow{\text{inclusion}} E_1 \times E_2 \xrightarrow{\Psi} E_1 \times E_2 \xrightarrow{\text{projection}} E_2$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

$$\begin{array}{ccccccc} E_1 & \xrightarrow{\text{inclusion}} & E_1 \times E_2 & \xrightarrow{\Psi} & E_1 \times E_2 & \xrightarrow{\text{projection}} & E_2 \\ P_1 & & & & & & \end{array}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

$$\begin{array}{ccccccc} E_1 & \xrightarrow{\text{inclusion}} & E_1 \times E_2 & \xrightarrow{\Psi} & E_1 \times E_2 & \xrightarrow{\text{projection}} & E_2 \\ P_1 & & (P_1, 0) & & & & \end{array}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

$$\begin{array}{ccccccc} E_1 & \xrightarrow{\text{inclusion}} & E_1 \times E_2 & \xrightarrow{\Psi} & E_1 \times E_2 & \xrightarrow{\text{projection}} & E_2 \\ P_1 & & (P_1, 0) & & (aP_1, \varphi(P_1)) & & \end{array}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- If we can evaluate Ψ, we can evaluate φ:

$$\begin{array}{ccccccc} E_1 & \xrightarrow{\text{inclusion}} & E_1 \times E_2 & \xrightarrow{\Psi} & E_1 \times E_2 & \xrightarrow{\text{projection}} & E_2 \\ P_1 & & (P_1, O) & & (aP_1, \varphi(P_1)) & & \varphi(P_1) \end{array}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \longrightarrow E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \longrightarrow E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret)
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

$$\begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix} \cdot \begin{pmatrix} [a] & \hat{\varphi} \\ -\varphi & [a] \end{pmatrix}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \longrightarrow E_2$ of degree 3^m (Bob's secret) $\hat{\varphi} \circ \varphi = [3m]$
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \longrightarrow E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

$$\begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix} \cdot \begin{pmatrix} [a] & \hat{\varphi} \\ -\varphi & [a] \end{pmatrix} = \begin{pmatrix} [a^2] + [3^m] & 0 \\ 0 & [a^2] + [3^m] \end{pmatrix}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret) $\hat{\varphi} \circ \varphi = [3m]$
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

$$\begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix} \cdot \begin{pmatrix} [a] & \hat{\varphi} \\ -\varphi & [a] \end{pmatrix} = \begin{pmatrix} [a^2] + [3^m] & 0 \\ 0 & [a^2] + [3^m] \end{pmatrix} = \begin{pmatrix} [2^n] & 0 \\ 0 & [2^n] \end{pmatrix}$$

HD embedding of an isogeny

- Let $\varphi : E_1 \to E_2$ of degree 3^m (Bob's secret) $\quad \hat{\varphi} \circ \varphi = [3^m]$
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \to E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

$$\begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix} \cdot \begin{pmatrix} [a] & \hat{\varphi} \\ -\varphi & [a] \end{pmatrix} = \begin{pmatrix} [a^2] + [3^m] & 0 \\ 0 & [a^2] + [3^m] \end{pmatrix} = \begin{pmatrix} [2^n] & 0 \\ 0 & [2^n] \end{pmatrix}$$

- $\ker(\Psi) = \{ ([3^m]P, [a]\varphi(P)) \mid P \in E_1[2^n] \}$

HD embedding of an isogeny

- Let $\varphi : E_1 \longrightarrow E_2$ of degree 3^m (Bob's secret) $\hat{\varphi} \circ \varphi = [3m]$
- Suppose $2^n - 3^m = a^2$ is a square
- Define $\Psi : E_1 \times E_2 \longrightarrow E_1 \times E_2$ as

$$\Psi = \begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix}$$

- Is it a 2^n-isogeny?

$$\begin{pmatrix} [a] & -\hat{\varphi} \\ \varphi & [a] \end{pmatrix} \cdot \begin{pmatrix} [a] & \hat{\varphi} \\ -\varphi & [a] \end{pmatrix} = \begin{pmatrix} [a^2] + [3^m] & 0 \\ 0 & [a^2] + [3^m] \end{pmatrix} = \begin{pmatrix} [2^n] & 0 \\ 0 & [2^n] \end{pmatrix}$$

- $\ker(\Psi) = \{ ([3^m]P, [a]\varphi(P)) \mid P \in E_1[2^n] \}$
- Given φ on $E_1[2^n]$ (torsion information) $\Rightarrow$ can compute $\ker(\Psi)$ $\Rightarrow$ can compute φ

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution
- Suppose $2^n - 3^m = a^2 + b^2$ is a **sum of 2 squares**...

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution
- Suppose $2^n - 3^m = a^2 + b^2$ is a **sum of 2 squares**...
- Define $\Psi : E_1 \times E_1 \times E_2 \times E_2 \to E_1 \times E_1 \times E_2 \times E_2$ as

$$\begin{pmatrix} a & b & -\hat{\varphi} & 0 \\ -b & a & 0 & -\hat{\varphi} \\ \varphi & 0 & a & b \\ 0 & \varphi & -b & a \end{pmatrix}$$

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution
- Suppose $2^n - 3^m = a^2 + b^2$ is a **sum of 2 squares**…
- Define $\Psi : E_1 \times E_1 \times E_2 \times E_2 \to E_1 \times E_1 \times E_2 \times E_2$ as

$$\begin{pmatrix} a & b & -\hat{\varphi} & 0 \\ -b & a & 0 & -\hat{\varphi} \\ \varphi & 0 & a & b \\ 0 & \varphi & -b & a \end{pmatrix}$$

- It is a 2^n-isogeny

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution
- Suppose $2^n - 3^m = a^2 + b^2$ is a **sum of 2 squares**...
- Define $\Psi : E_1 \times E_1 \times E_2 \times E_2 \to E_1 \times E_1 \times E_2 \times E_2$ as

$$\begin{pmatrix} a & b & -\hat{\varphi} & 0 \\ -b & a & 0 & -\hat{\varphi} \\ \varphi & 0 & a & b \\ 0 & \varphi & -b & a \end{pmatrix}$$

- It is a 2^n-isogeny
- Isogeny in dimension 4

4D embedding of an isogeny

- **$2^n - 3^m$ not a square**? [Robert] has a solution
- Suppose $2^n - 3^m = a^2 + b^2$ is a **sum of 2 squares**…
- Define $\Psi : E_1 \times E_1 \times E_2 \times E_2 \to E_1 \times E_1 \times E_2 \times E_2$ as

$$\begin{pmatrix} a & b & -\hat{\varphi} & 0 \\ -b & a & 0 & -\hat{\varphi} \\ \varphi & 0 & a & b \\ 0 & \varphi & -b & a \end{pmatrix}$$

- It is a 2^n-isogeny
- Isogeny in dimension 4
- Many integers are sum of 2 squares… but not all

8D embedding of an isogeny

- $2^n - 3^m$ not a sum of two square? [Robert] has another solution: Zarhin's trick

8D embedding of an isogeny

- $2^n - 3^m$ not a sum of two square? [Robert] has another solution: Zarhin's trick
- Every integer is a **sum of 4 squares**: $2^n - 3^m = a^2 + b^2 + c^2 + d^2$

8D embedding of an isogeny

- $2^n - 3^m$ not a sum of two square? [Robert] has another solution: Zarhin's trick
- Every integer is a **sum of 4 squares**: $2^n - 3^m = a^2 + b^2 + c^2 + d^2$

$$\begin{pmatrix}
a & -b & -c & -d & -\hat{\varphi} & & & \\
b & a & d & -c & & -\hat{\varphi} & 0 & \\
c & -d & a & b & & & -\hat{\varphi} & \\
d & c & -b & a & 0 & & & -\hat{\varphi} \\
\varphi & & & & a & -b & -c & -d \\
 & \varphi & 0 & & b & a & d & -c \\
 & & \varphi & & c & -d & a & b \\
 & 0 & & \varphi & d & c & -b & a
\end{pmatrix}$$

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks

  ➡ **2D isogenies** for decryption

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**
  - ➡ Good implementations available

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**
  - ➡ Good implementations available
- **SQIsign HD:** signature scheme inspired by SQIsign

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**
  - ➡ Good implementations available
- **SQIsign HD:** signature scheme inspired by SQIsign
  - ➡ **4D isogenies** for verification

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**
  - ➡ Good implementations available
- **SQIsign HD**: signature scheme inspired by SQIsign
  - ➡ **4D isogenies** for verification
  - ➡ Not well studied

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, “Richelot isogenies”, **efficient**
  - ➡ Good implementations available
- **SQIsign HD**: signature scheme inspired by SQIsign
  - ➡ **4D isogenies** for verification
  - ➡ Not well studied
  - ➡ Previous literature says it can be done in polynomial time…

Applications

- **FESTA:** Fast Encryption from Supersingular Torsion Attacks
  - ➡ **2D isogenies** for decryption
  - ➡ Well-studied, "Richelot isogenies", **efficient**
  - ➡ Good implementations available
- **SQIsign HD:** signature scheme inspired by SQIsign
  - ➡ **4D isogenies** for verification
  - ➡ Not well studied
  - ➡ Previous literature says it can be done in polynomial time…
  - ➡ Back-of-the-envelope suggests it will be **practical**™