SQIsign

(for humans)

Krijn Reijnders, COSIC, KU Leuven
Cloudflare, June 19, 2025

KU LEUVEN

SQIsign

~~(for humans)~~

(for people that know a bit of ECC, ECDSA, and math, but not too much to see where I shove away technically challenging material)

Krijn Reijnders, COSIC, KU Leuven
Cloudflare, June 19, 2025

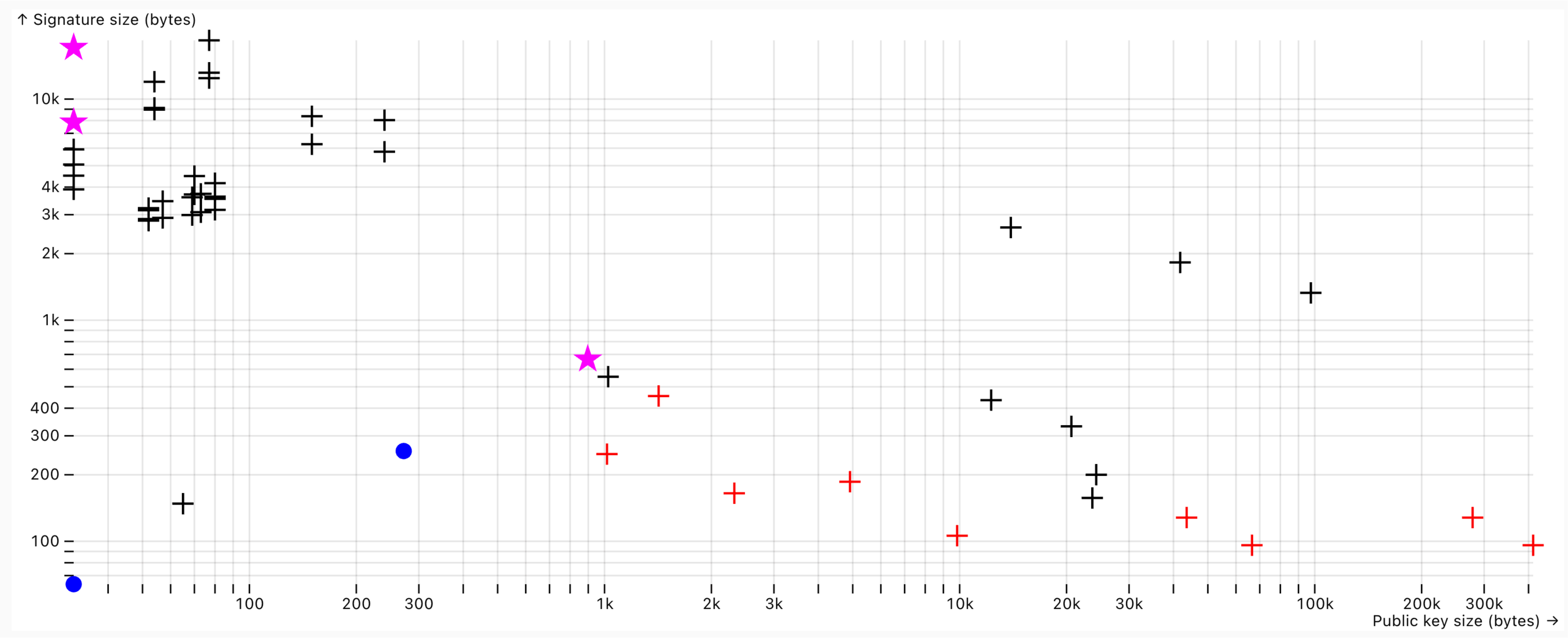
KU LEUVEN

SQIsign

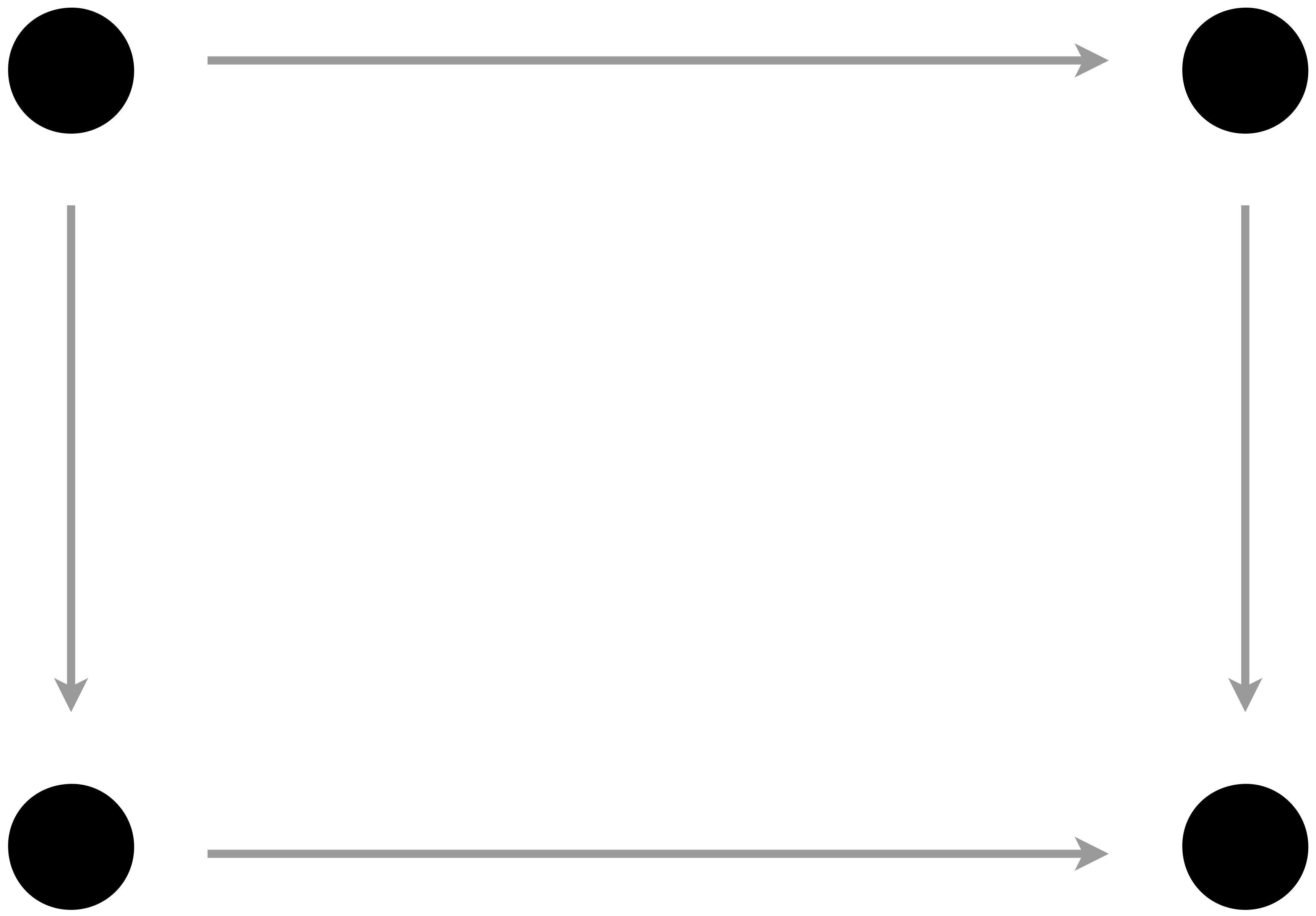
(for nerds)

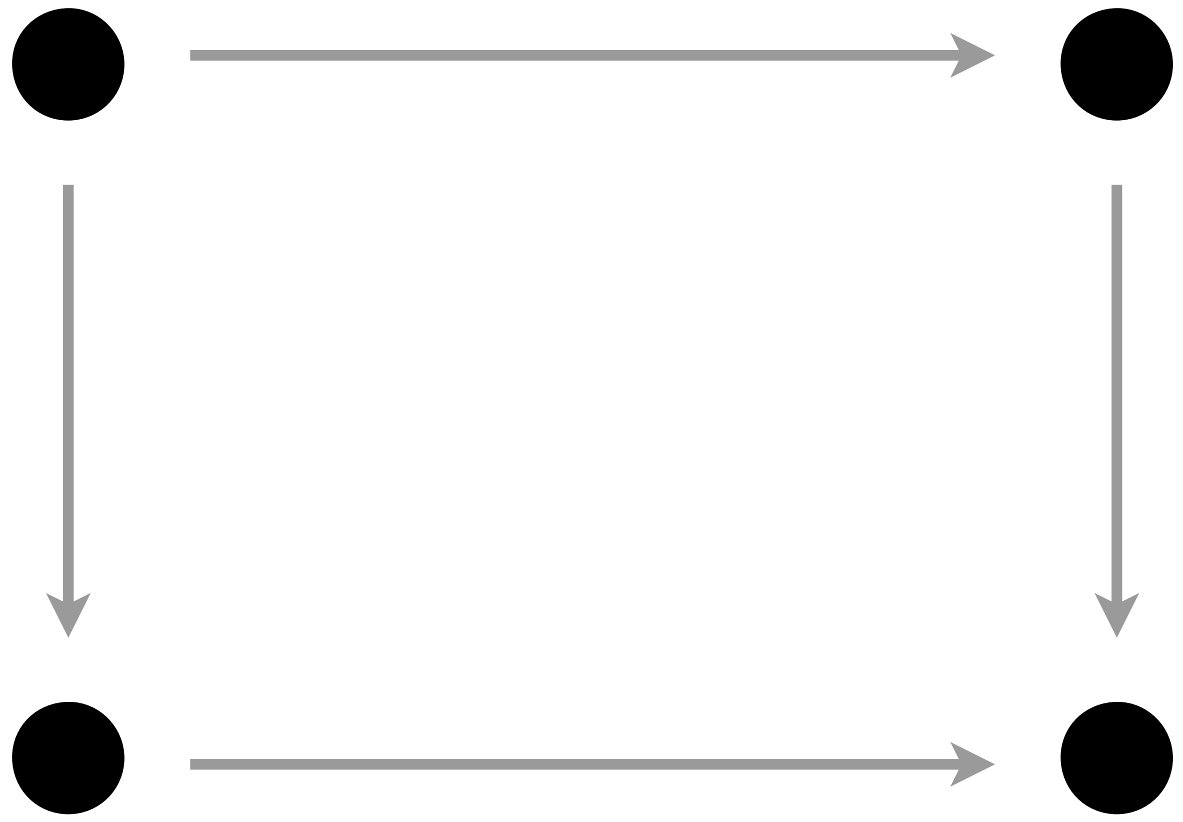
Krijn Reijnders, COSIC, KU Leuven
Cloudflare, June 19, 2025

KU LEUVEN


↑ Signature size (bytes)
10k
4k
3k
2k
1k
400
300
200
100
100
200
300
1k
2k
3k
10k
20k
30k
100k
200k
300k
Public key size (bytes) →

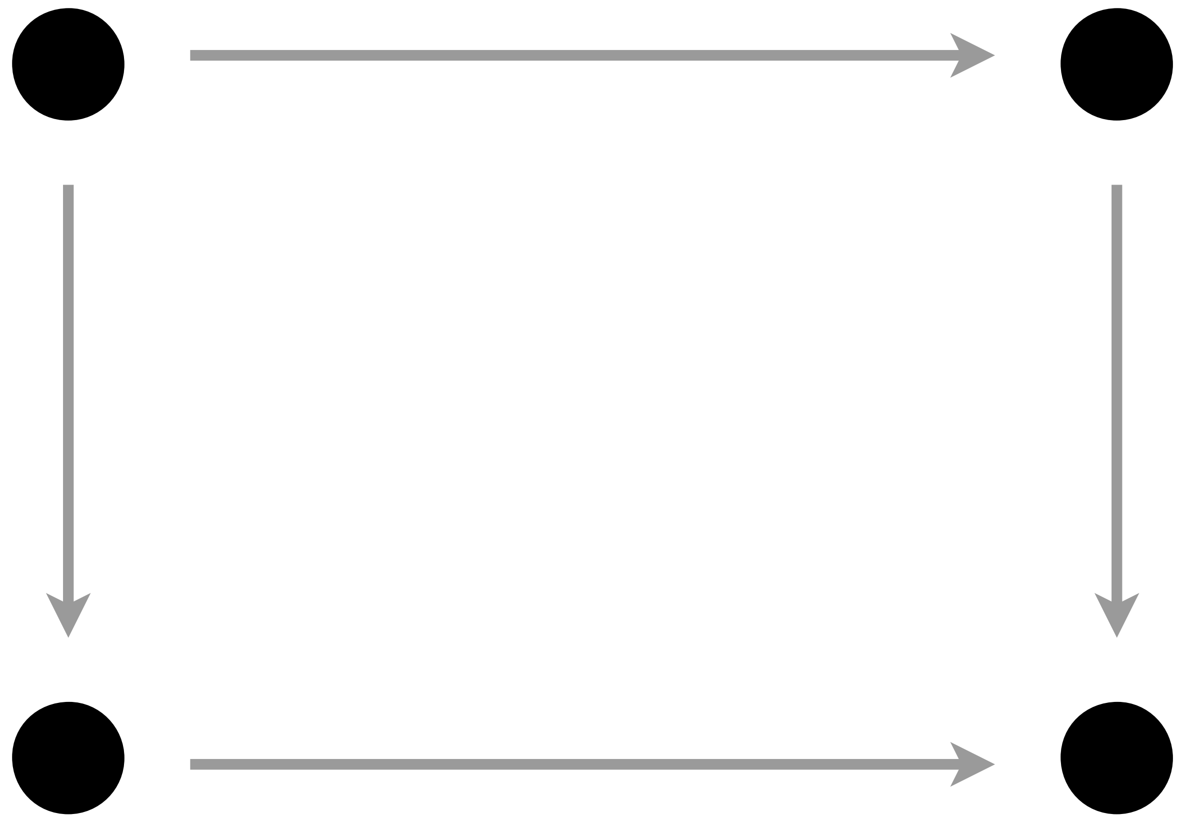

↑ Signature size (bytes)
10k
4k
3k
2k
1k
400
300
200
100
100
200
300
1k
2k
3k
10k
20k
30k
100k
200k
300k
Public key size (bytes) →
SQIsign!
OTHER PQ SCHEMES





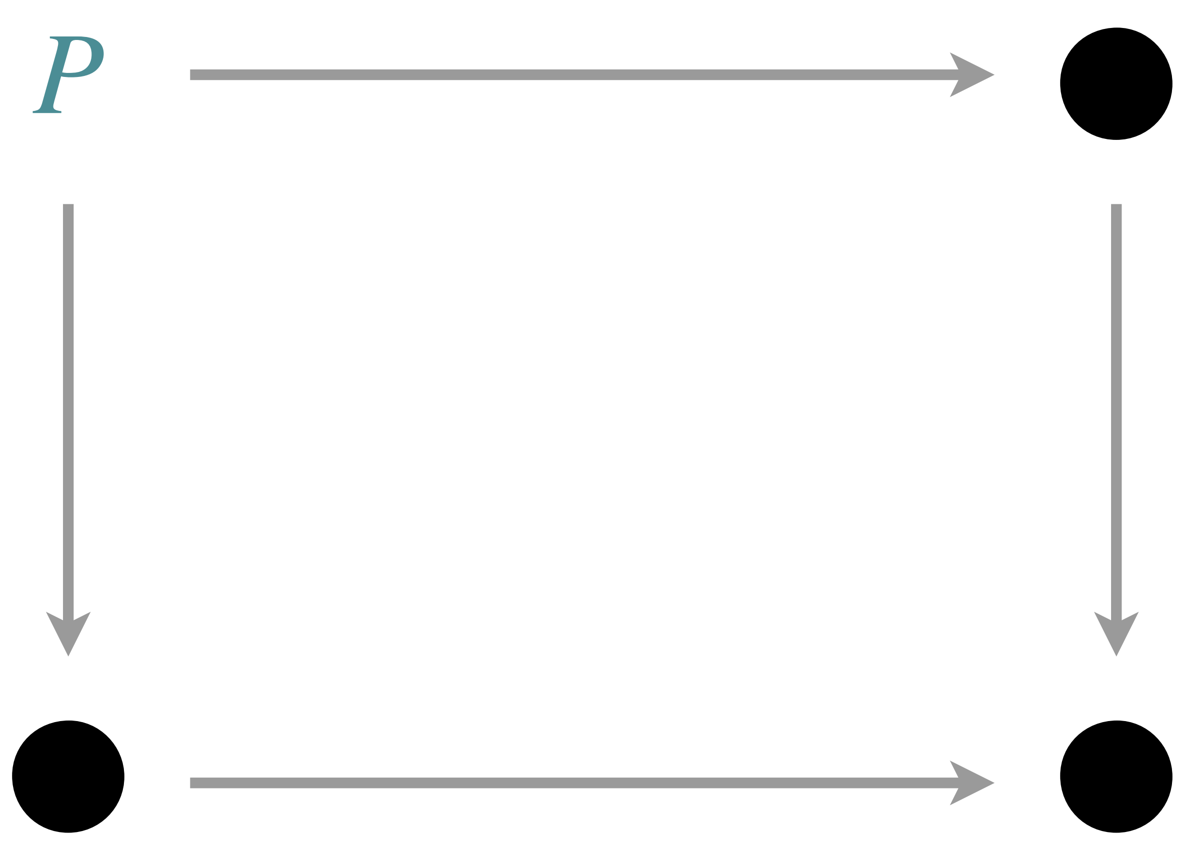
setup

1. Take your favourite elliptic curve $\mathscr{E}$



setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P



setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

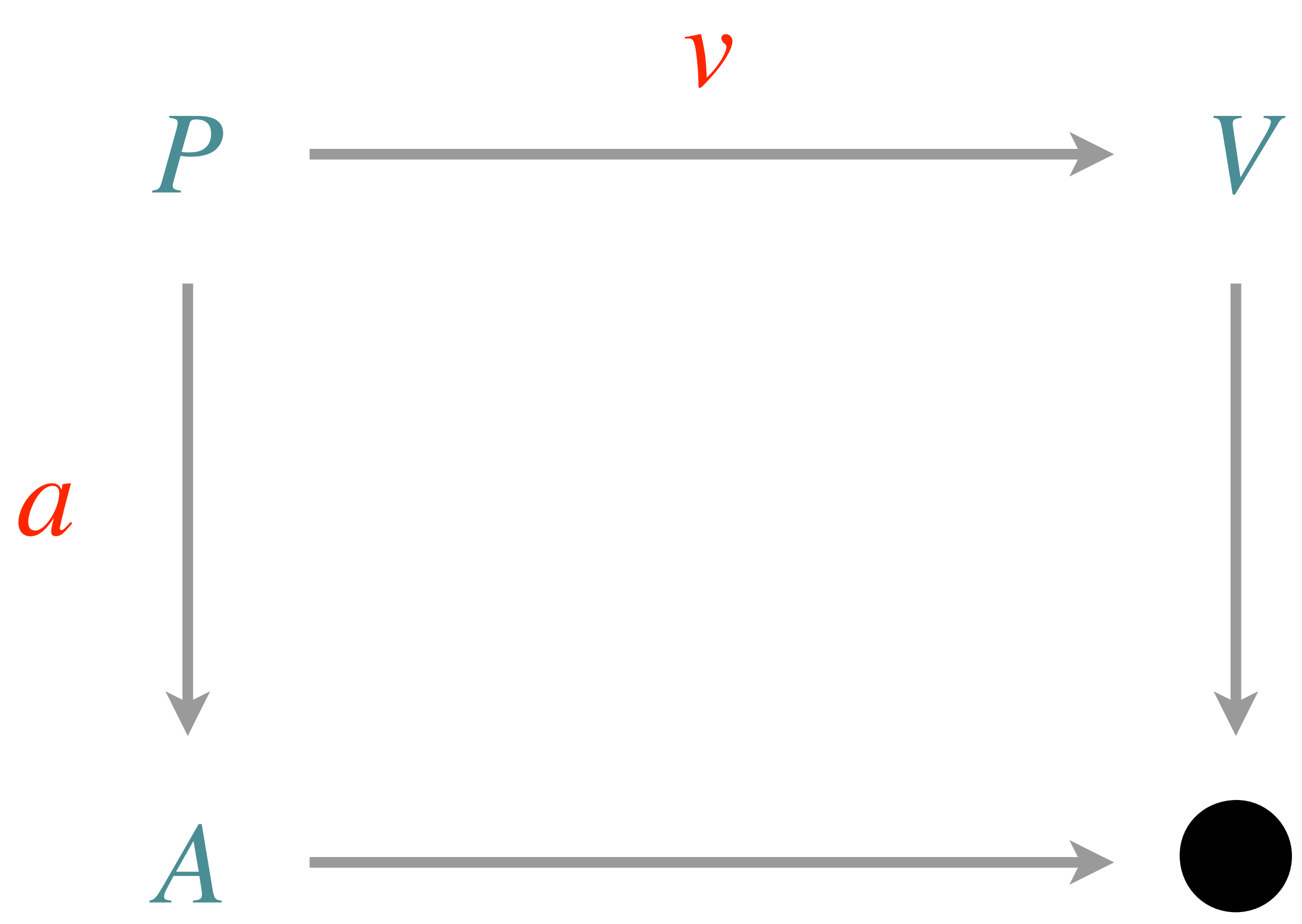
1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$

setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$



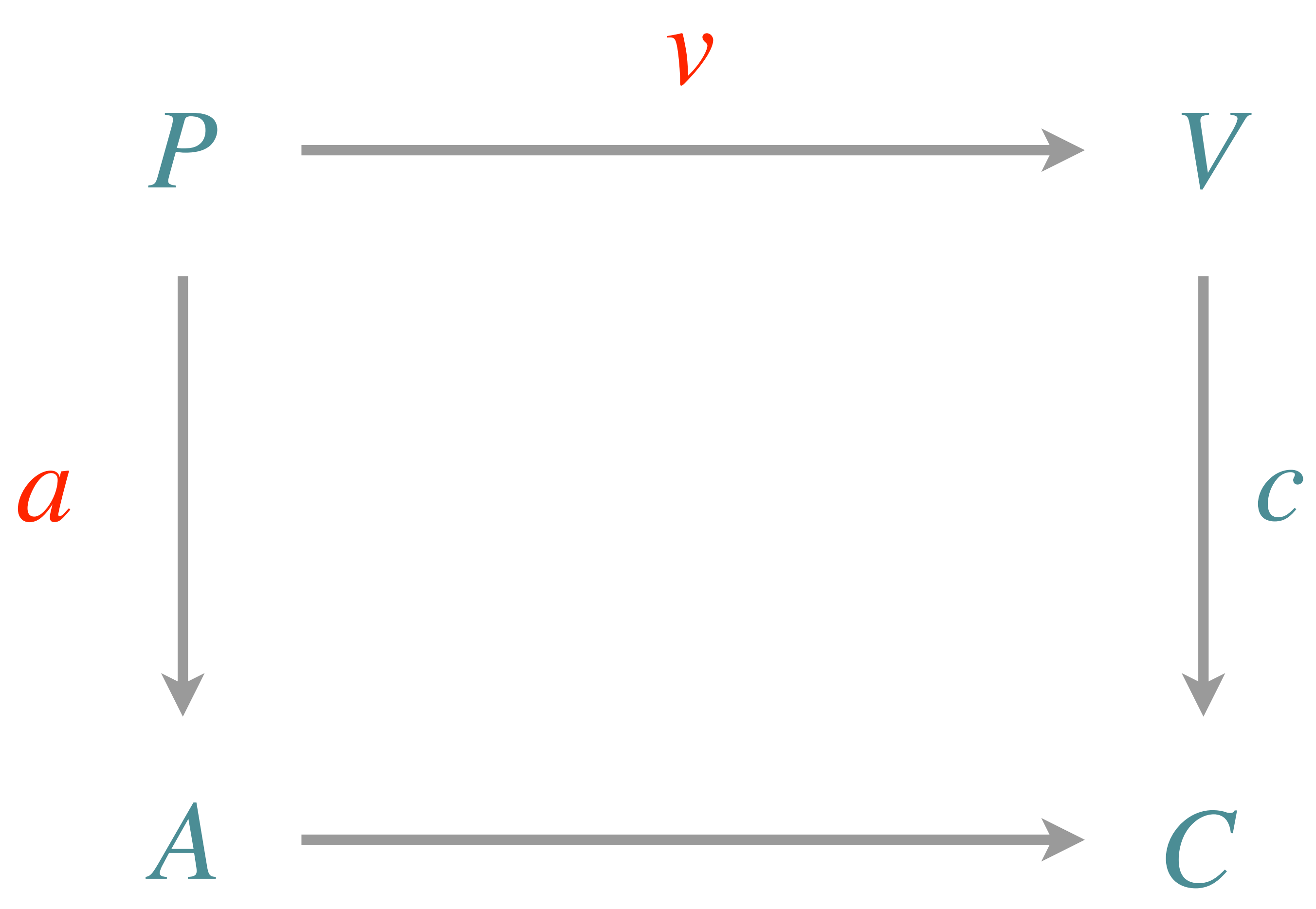
KU LEUVEN

setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$
2. Get challenged by some $c \in \mathbb{Z}_q^\times$

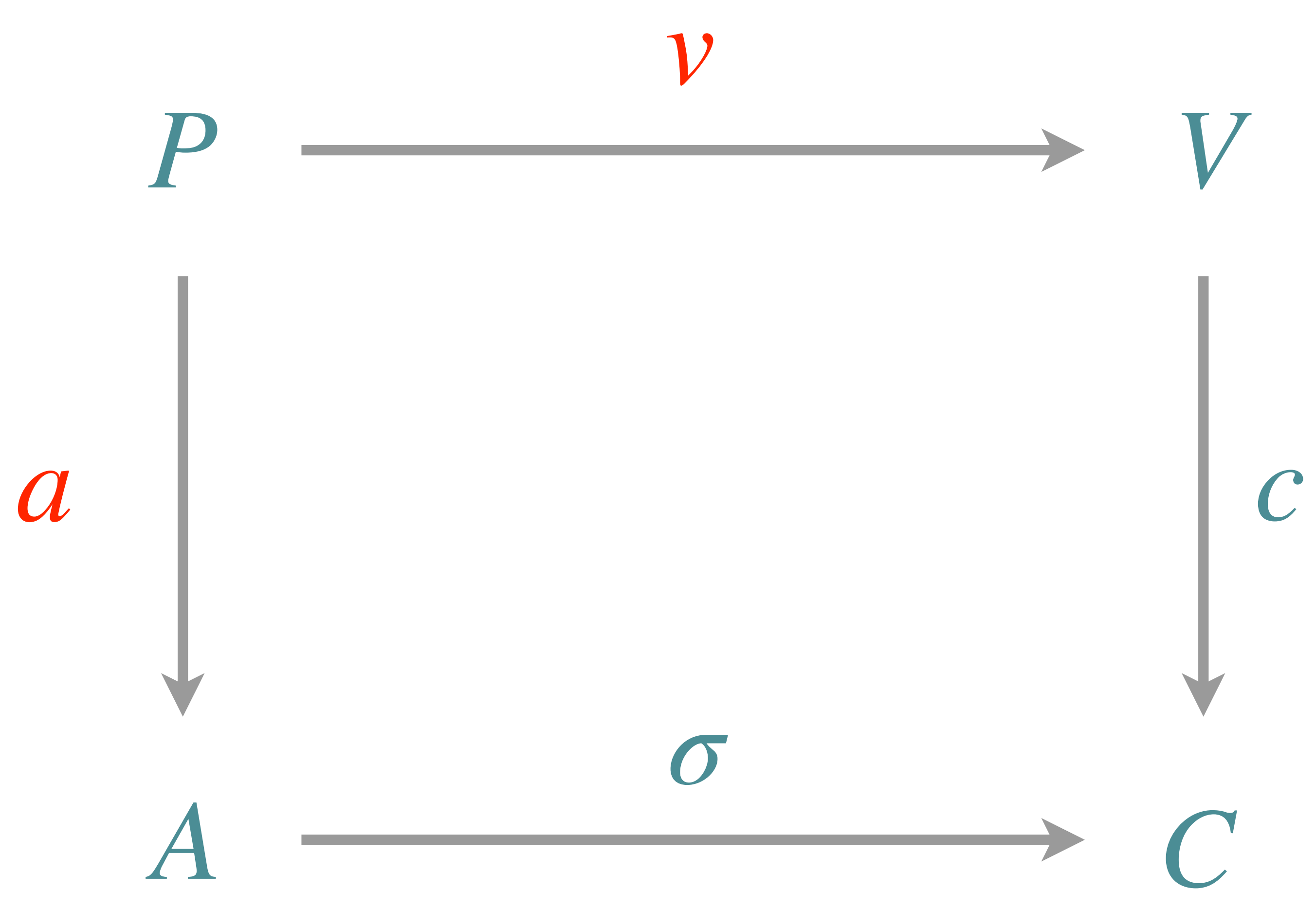


setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$
2. Get challenged by some $c \in \mathbb{Z}_q^\times$
3. Return $\sigma = \dfrac{v \cdot c}{a} \in \mathbb{Z}_q^\times$ as response

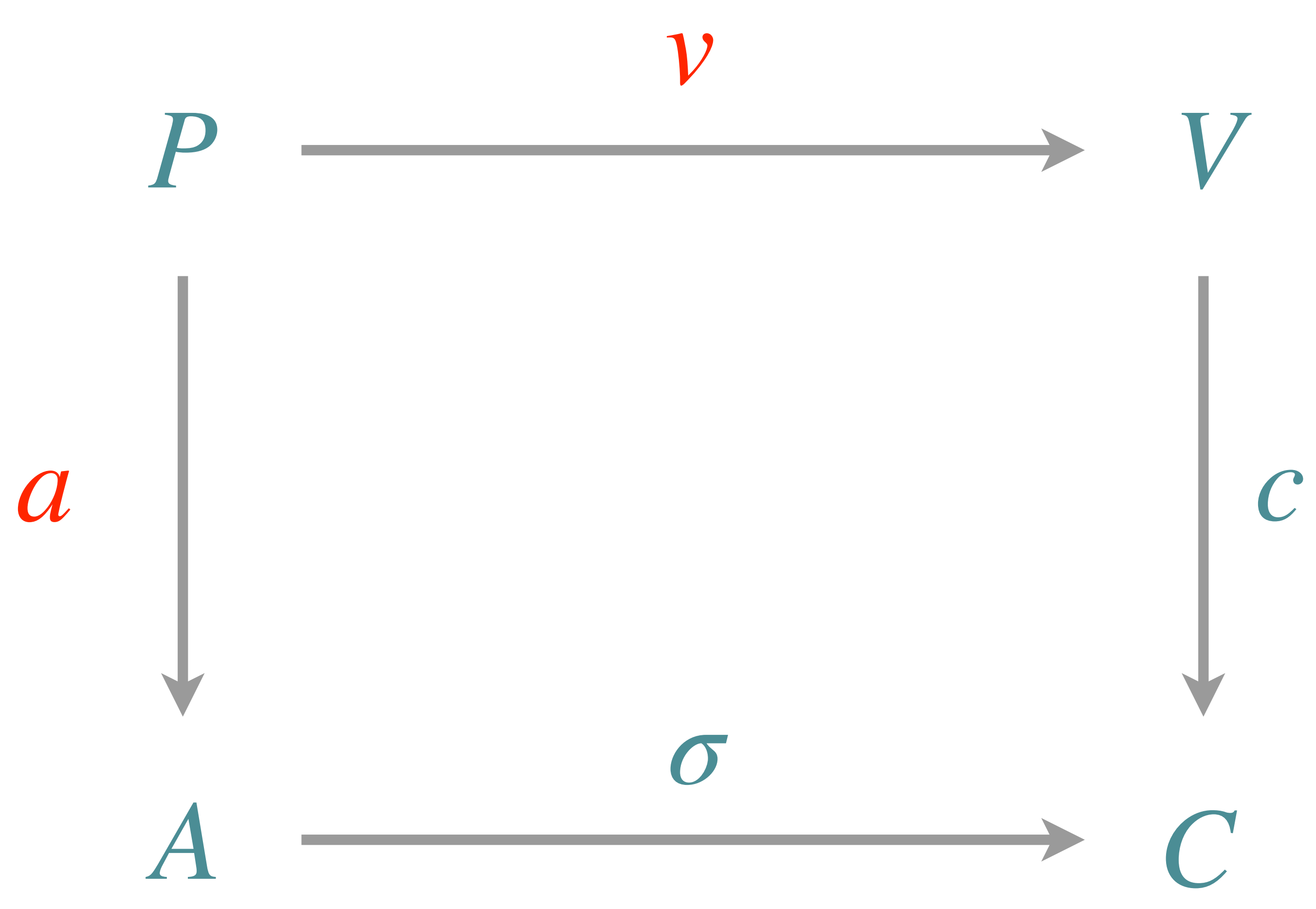


setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$
2. Get challenged by some $c \in \mathbb{Z}_q^\times$
3. Return $\sigma = \frac{v \cdot c}{a} \in \mathbb{Z}_q^\times$ as response



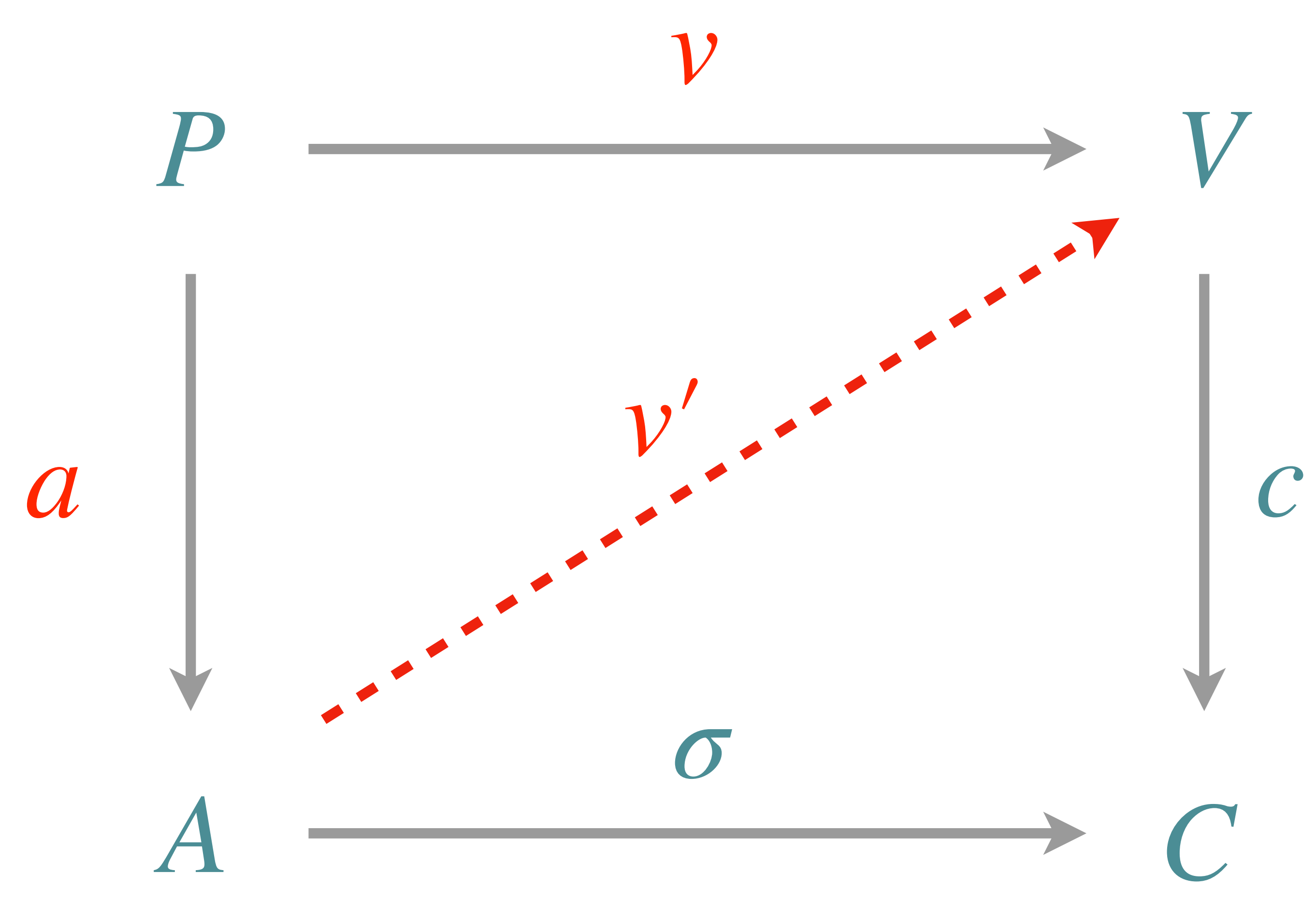
setup

1. Take your favourite elliptic curve $\mathscr{E}$
2. Take prime-order subgroup $G \subset \mathscr{E}(\mathbb{F}_p)$ with generator P
3. Take a secret key $a \in \mathbb{Z}_q^\times$ and public key $A = [a]P$

id scheme

1. Take random $v \in \mathbb{Z}_q^\times$, commit to $V = [v]P$
2. Get challenged by some $c \in \mathbb{Z}_q^\times$
3. Return $\sigma = \dfrac{v \cdot c}{a} \in \mathbb{Z}_q^\times$ as response

1. Take random v',
   commit to $V' = [v']A$
2. On challenge c,
   return $\sigma = v' \cdot c$



Our plan for today

1

Making the square work…

$$\mathscr{E} \xrightarrow{\varphi} \mathscr{E}'$$

with isogenies!

2

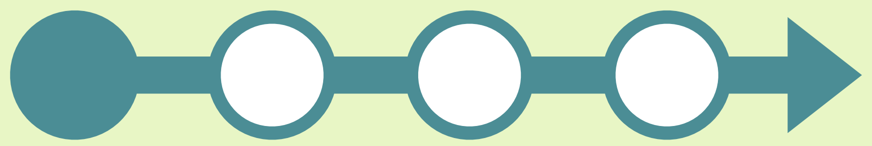
Decomposing the square

$$\mathrm{End}(\mathscr{E}) \xrightarrow{\sim} \mathscr{O}$$

with quaternions!

3

SQIsign, SQIsignHD



SQIsign2D, SQIsignXD…?

PART 1
The Square

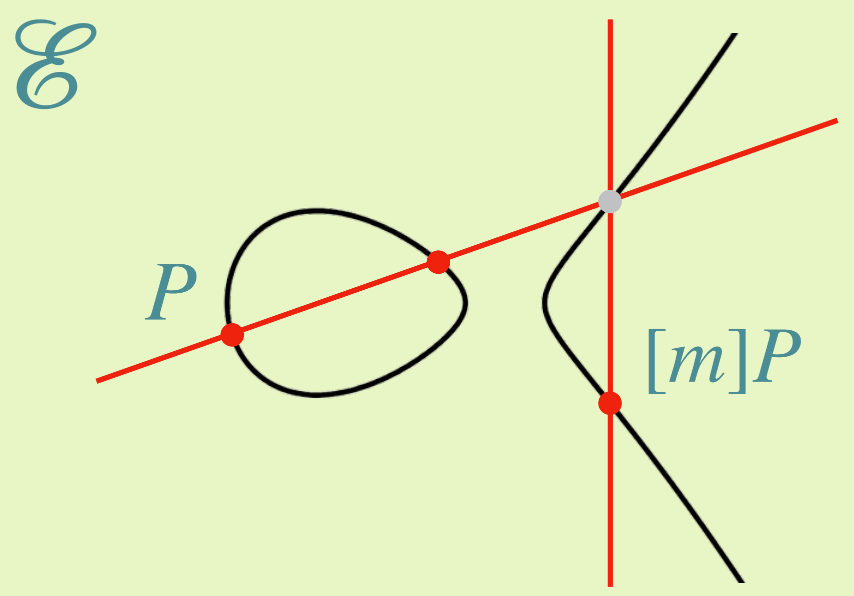
From ECC World to Isogeny World

ECC

- work on single 'nice' curve $\mathscr{E}$

$$\mathscr{E} : y^2 = x^3 + Ax^2 + x, \qquad A \in \mathbb{F}_p$$

- take a starting point P and perform scalar multiplications $[m] \in \mathbb{Z}_q^\times$



PART 1
The Square

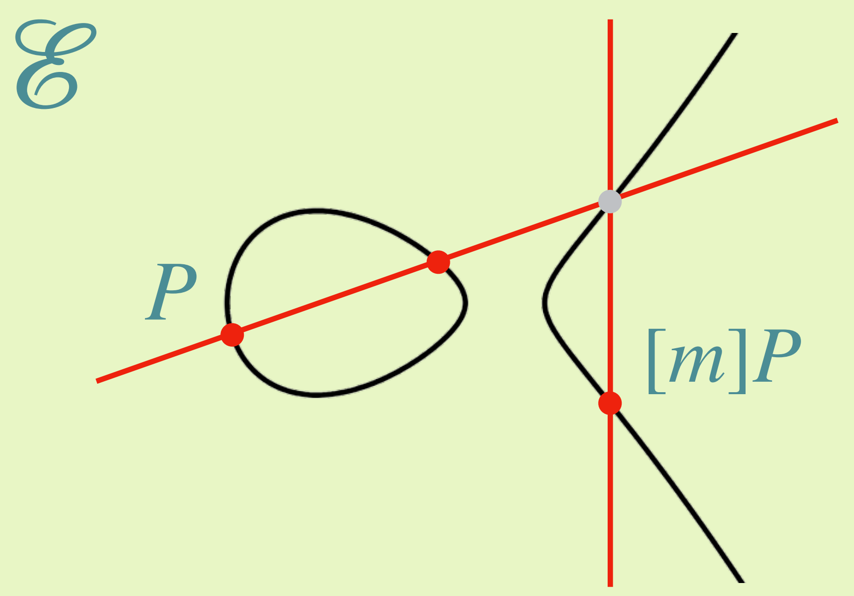
From ECC World to Isogeny World

ECC

- work on single 'nice' curve $\mathscr{E}$

$$\mathscr{E} : y^2 = x^3 + Ax^2 + x, \qquad A \in \mathbb{F}_p$$

- take a starting point P and perform scalar multiplications $[m] \in \mathbb{Z}_q^\times$

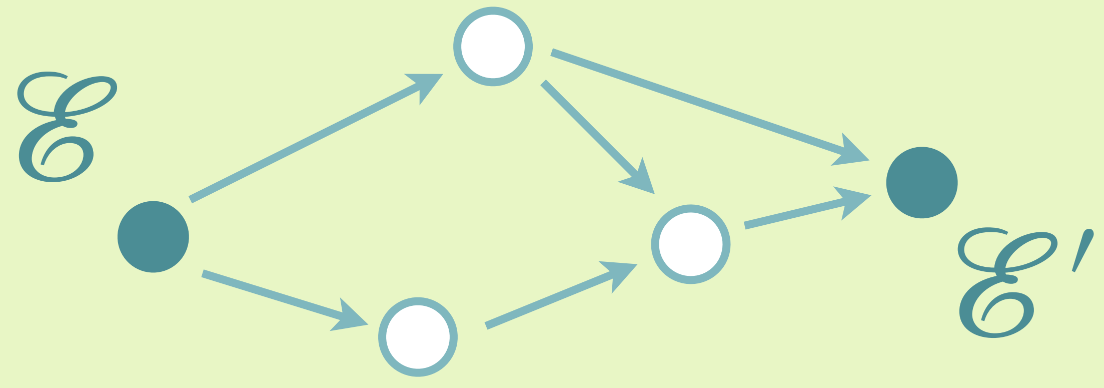


ISOGENY

- work in the whole world of curves!
- use 'nice' maps between curves, we call an **isogeny**

$$\varphi : \mathscr{E} \to \mathscr{E}'$$

- take a starting curve $\mathscr{E}_0$ and perform isogenies φ, ψ, θ



You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$

PART 1
The Square

You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$
- if $\mathscr{E}$ has more “funky” endomorphisms, we say $\mathscr{E}$ is **supersingular***
- we write $\mathrm{End}(\mathscr{E})$ for this **ring of endom**.

*this is not the formal definition

PART 1
The Square

You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$
- if $\mathscr{E}$ has more “funky” endomorphisms, we say $\mathscr{E}$ is **supersingular***
- we write $\mathrm{End}(\mathscr{E})$ for this **ring of endom**.

- **isogeny**: group hom. $\varphi : \mathscr{E} \to \mathscr{E}'$
- has a **degree**, $\deg \varphi = \#\ker \varphi$
- can compute φ when degree is **smooth**

*this is not the formal definition

You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$
- if $\mathscr{E}$ has more “funky” endomorphisms, we say $\mathscr{E}$ is **supersingular***
- we write $\mathrm{End}(\mathscr{E})$ for this **ring of endom**.

- **isogeny**: group hom. $\varphi : \mathscr{E} \to \mathscr{E}'$
- has a **degree**, $\deg \varphi = \#\ker \varphi$
- can compute φ when degree is **smooth**

a concrete example

$$\mathscr{E} : y^2 = x^3 + x \xrightarrow{\varphi} \mathscr{E}' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y \cdot (x^3 - 4x^2 + 2)}{(x-5)^3} \right)$$

over $\mathbb{F}_{11}$

*this is not the formal definition

PART 1
The Square

You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$
- if $\mathscr{E}$ has more “funky” endomorphisms, we say $\mathscr{E}$ is **supersingular***
- we write $\mathrm{End}(\mathscr{E})$ for this **ring of endom**.

- **isogeny**: group hom. $\varphi : \mathscr{E} \to \mathscr{E}'$
- has a **degree**, $\deg \varphi = \#\ker \varphi$
- can compute φ when degree is **smooth**

a concrete example

$$\mathscr{E} : y^2 = x^3 + x \xrightarrow{\varphi} \mathscr{E}' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y \cdot (x^3 - 4x^2 + 2)}{(x-5)^3} \right)$$

over $\mathbb{F}_{11}$

hard problems

1 Given $\mathscr{E}$ and $\mathscr{E}'$, find an isogeny $\varphi : \mathscr{E} \to \mathscr{E}'$

2 Given a random $\mathscr{E}$, find a ‘funky’ endom. $\vartheta : \mathscr{E} \to \mathscr{E}$

*this is not the formal definition

PART 1
The Square

You “know” isogenies already!

in general

- map from $\mathscr{E}$ to itself is **endomorphism**
- simplest examples $[m] : P \mapsto [m]P$
- also easy $\pi : (x, y) \mapsto (x^p, y^p)$
- if $\mathscr{E}$ has more “funky” endomorphisms, we say $\mathscr{E}$ is **supersingular***
- we write $\mathrm{End}(\mathscr{E})$ for this **ring of endom**.

- **isogeny**: group hom. $\varphi : \mathscr{E} \to \mathscr{E}'$
- has a **degree**, $\deg \varphi = \#\ker \varphi$
- can compute φ when degree is **smooth**

a concrete example

$$\mathscr{E} : y^2 = x^3 + x \xrightarrow{\varphi} \mathscr{E}' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y \cdot (x^3 - 4x^2 + 2)}{(x-5)^3} \right)$$

over $\mathbb{F}_{11}$

hard problems

1 Given $\mathscr{E}$ and $\mathscr{E}'$, find an isogeny $\varphi : \mathscr{E} \to \mathscr{E}'$

↔ *equivalent!*

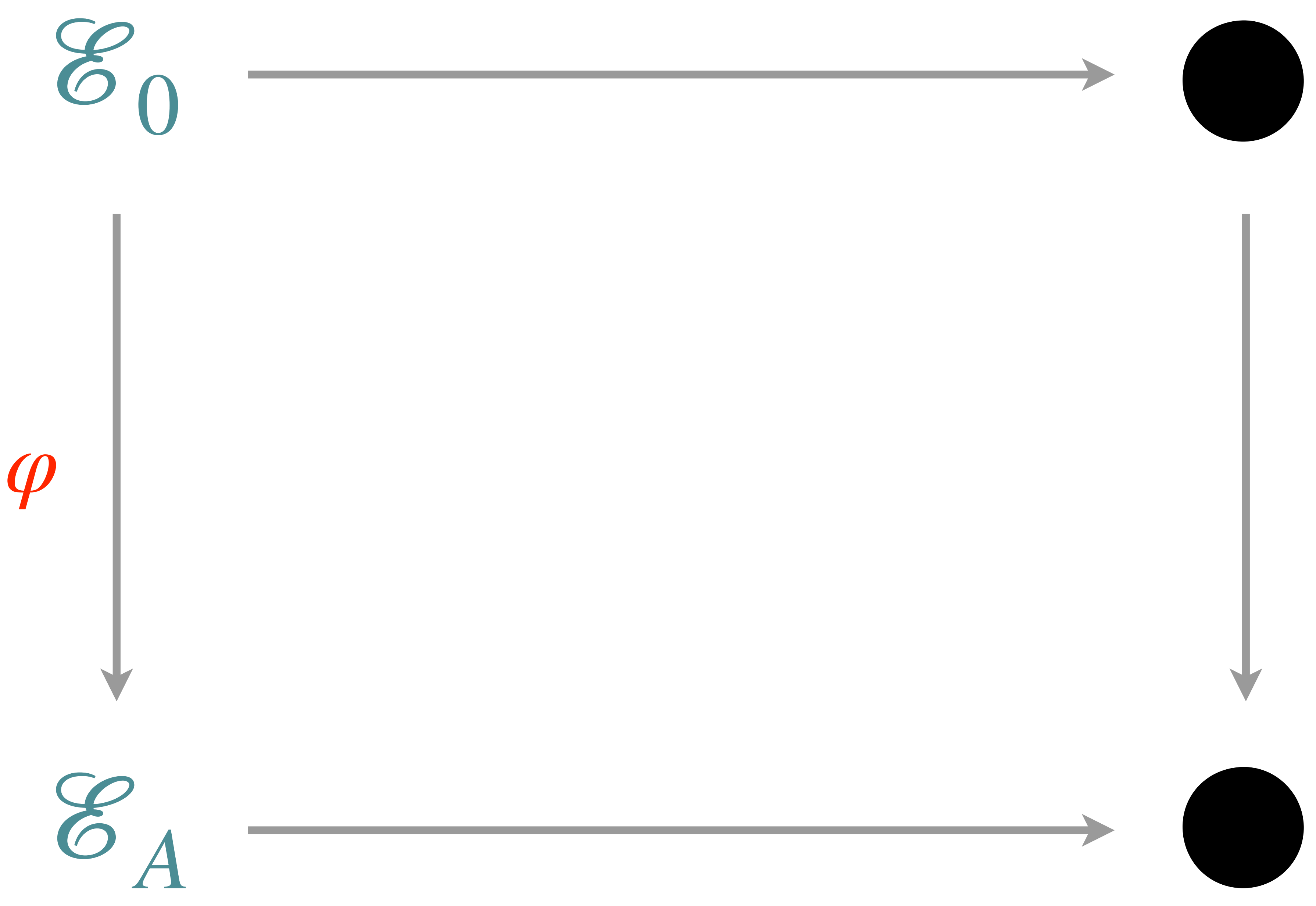
2 Given a random $\mathscr{E}$, find a ‘funky’ endom. $\vartheta : \mathscr{E} \to \mathscr{E}$

KU LEUVEN

*this is not the formal definition

PART 1
The Square

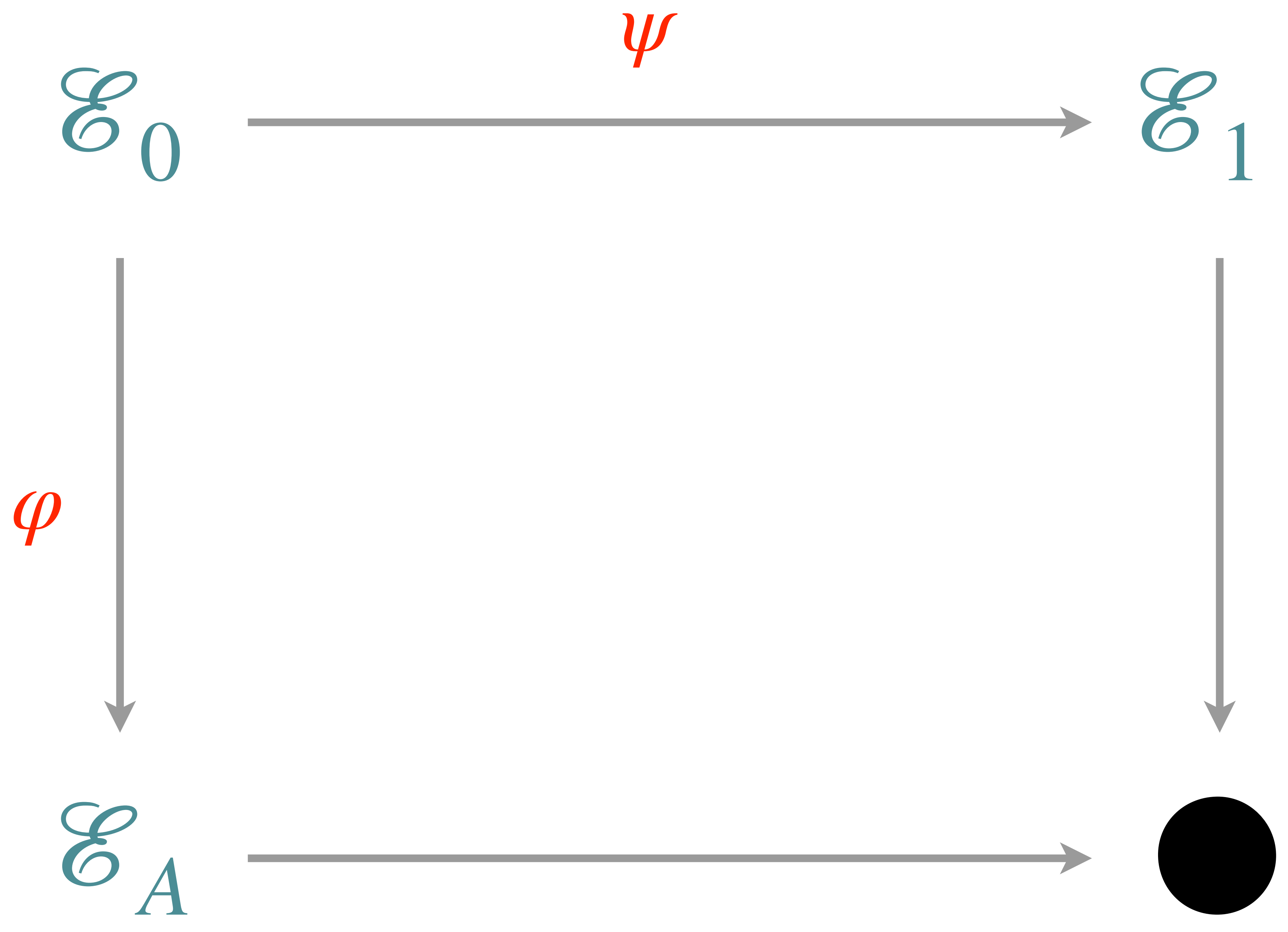
Let's fix the square with isogenies!



Same as before

1. take secret isogeny $\varphi : \mathscr{E}_0 \to \mathscr{E}_A$, send $\mathscr{E}_A$ as public key

Let's fix the square with isogenies!

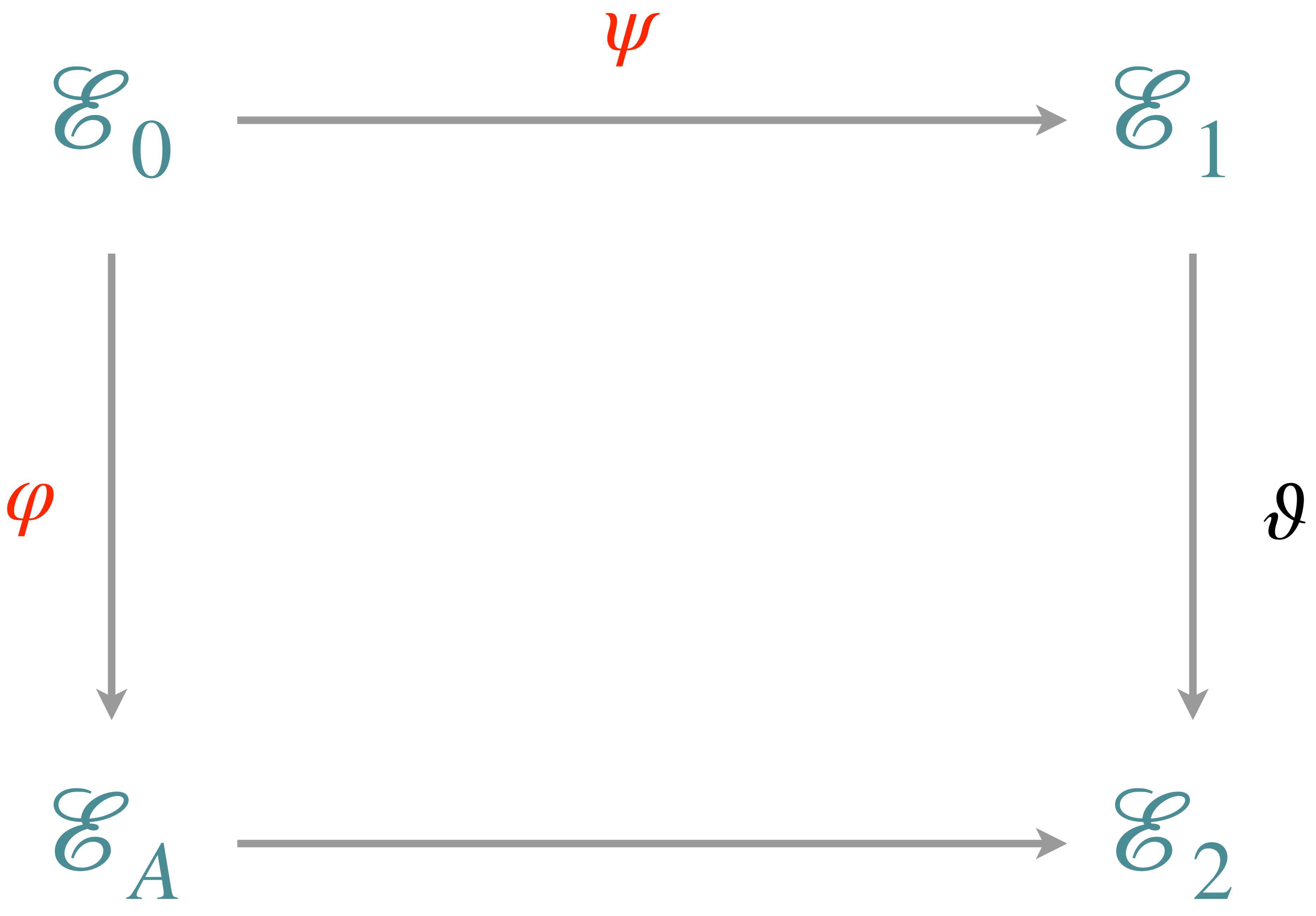


Same as before

1. take secret isogeny $\varphi : \mathscr{E}_0 \to \mathscr{E}_A$, send $\mathscr{E}_A$ as public key
2. take random commitment $\psi : \mathscr{E}_0 \to \mathscr{E}_1$

PART 1
The Square

Let's fix the square with isogenies!

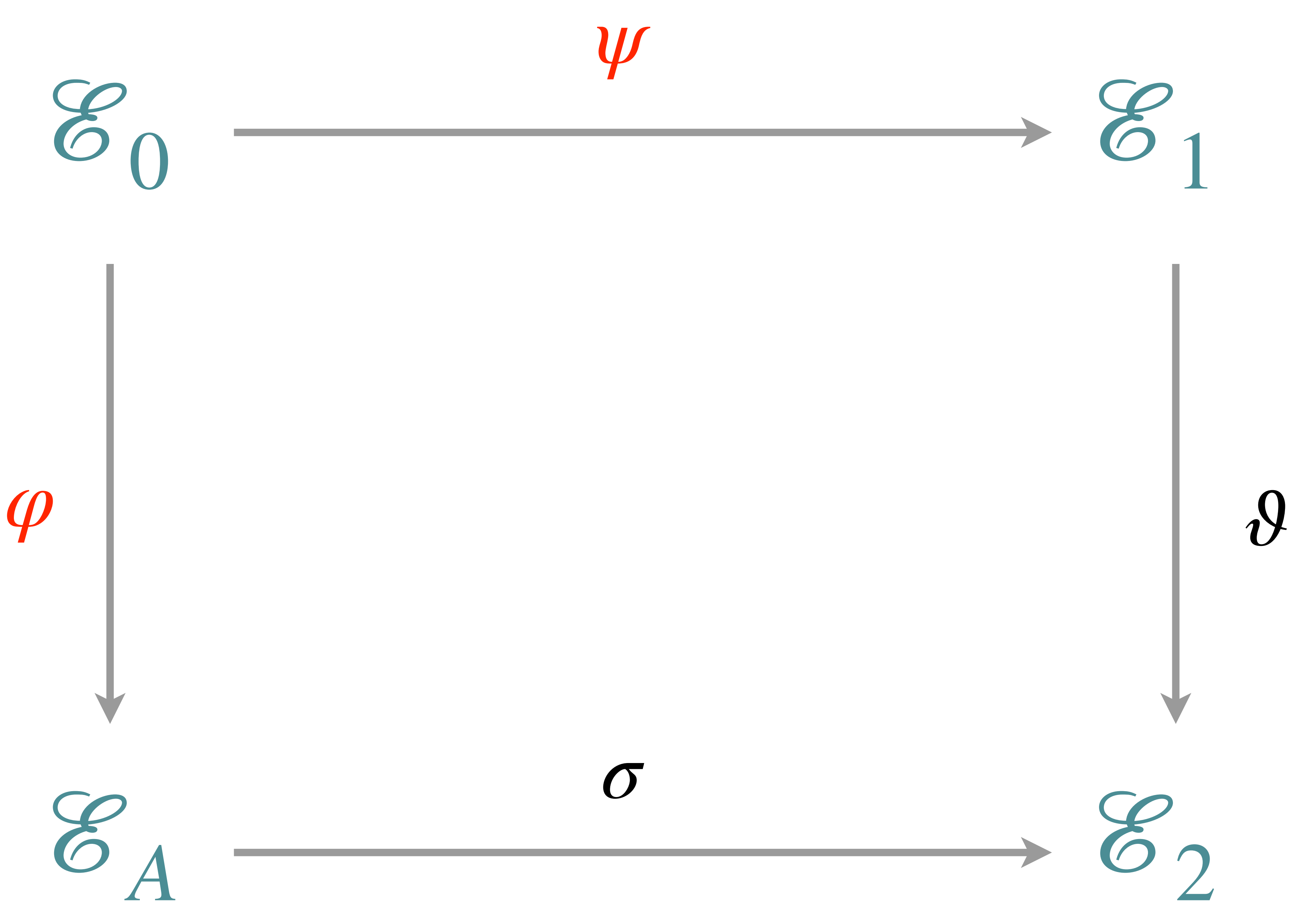


Same as before

1. take secret isogeny $\varphi : \mathscr{E}_0 \to \mathscr{E}_A$, send $\mathscr{E}_A$ as public key
2. take random commitment $\psi : \mathscr{E}_0 \to \mathscr{E}_1$
3. get a random challenge $\vartheta : \mathscr{E}_1 \to \mathscr{E}_2$

PART 1
The Square

Let's fix the square with isogenies!



Same as before

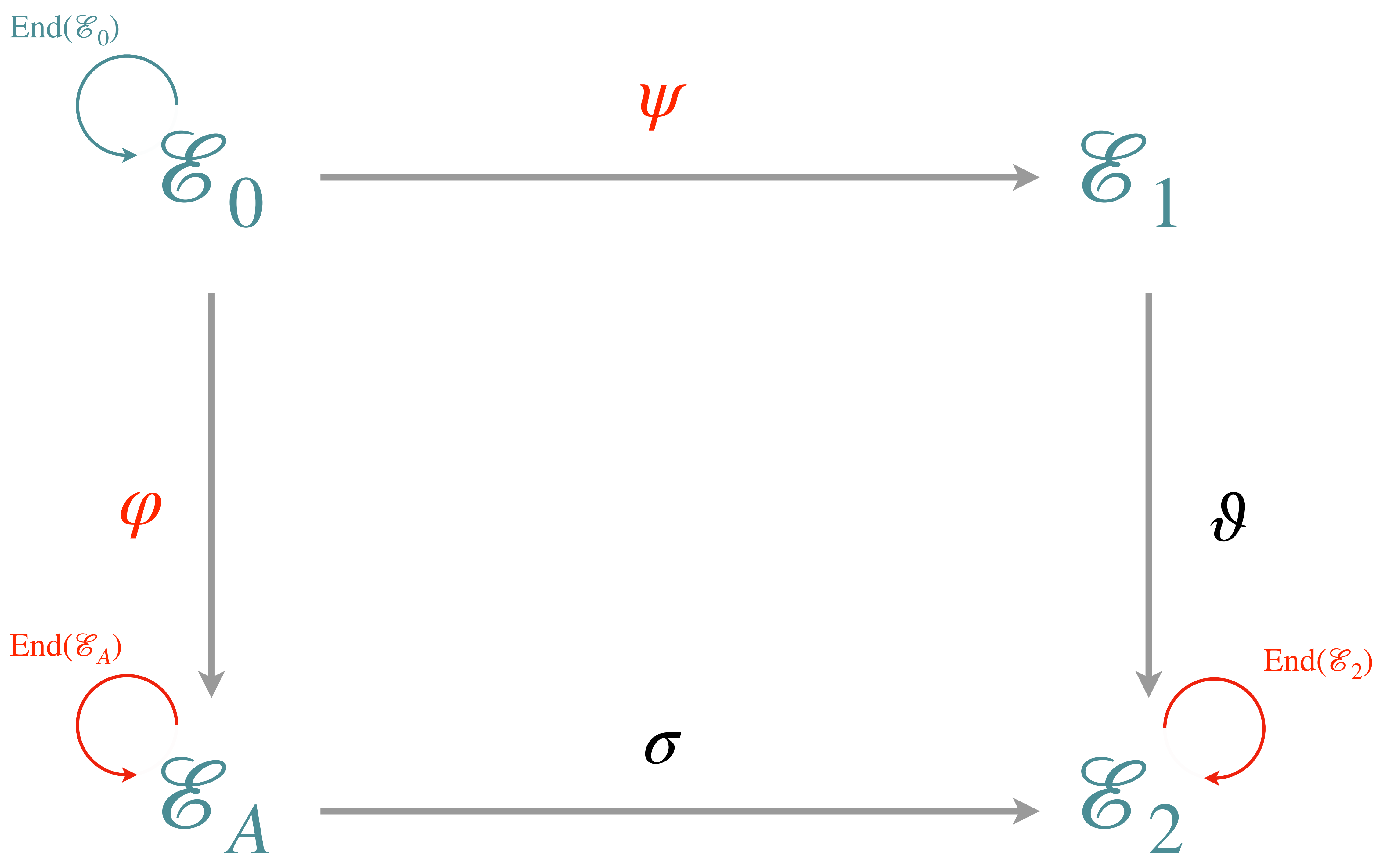
1. take secret isogeny $\varphi : \mathscr{E}_0 \to \mathscr{E}_A$, send $\mathscr{E}_A$ as public key
2. take random commitment $\psi : \mathscr{E}_0 \to \mathscr{E}_1$
3. get a random challenge $\vartheta : \mathscr{E}_1 \to \mathscr{E}_2$

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

PART 1
The Square

Let's fix the square with isogenies!

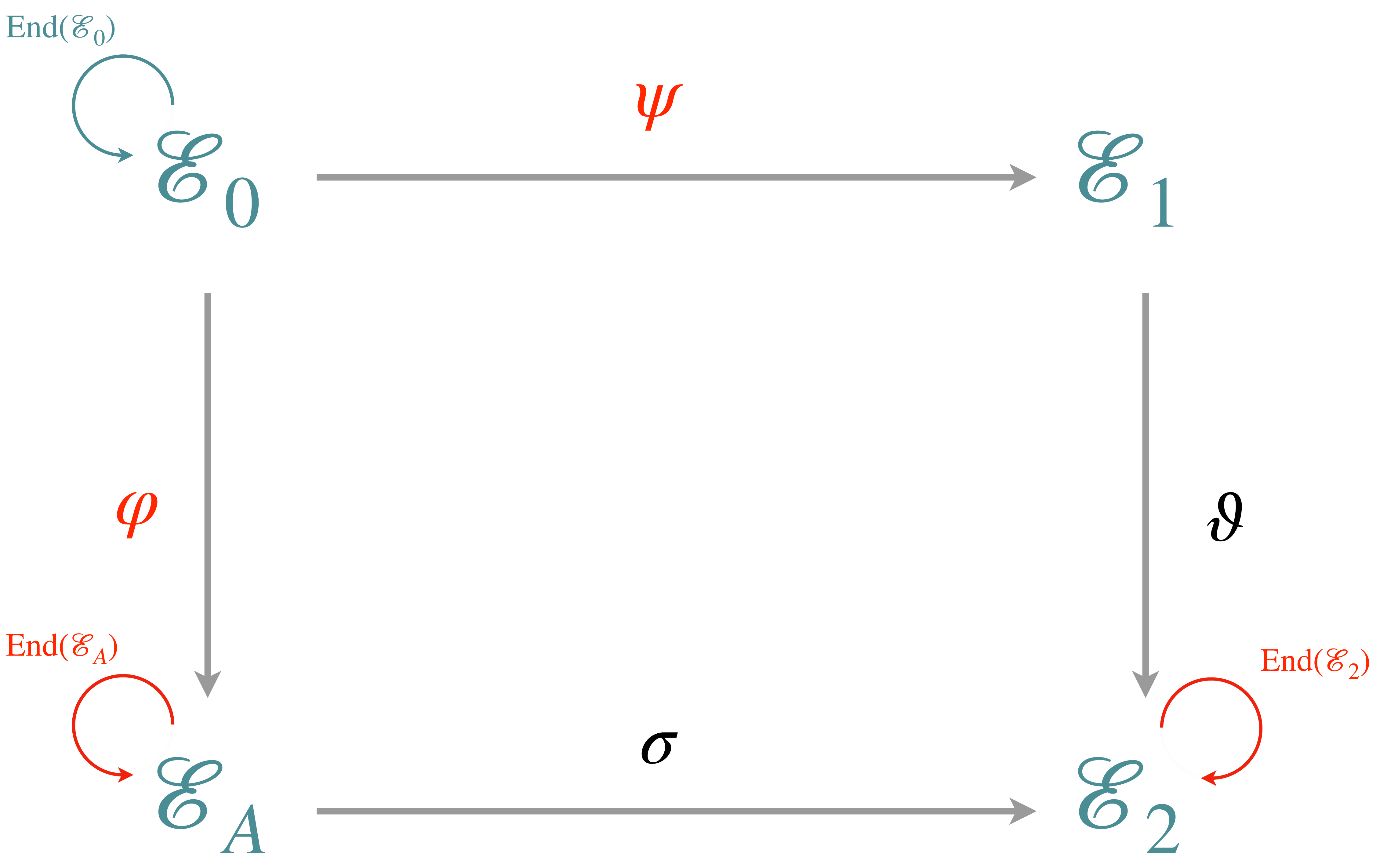


KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

PART 1
The Square

Let's fix the square with isogenies!



(magic)

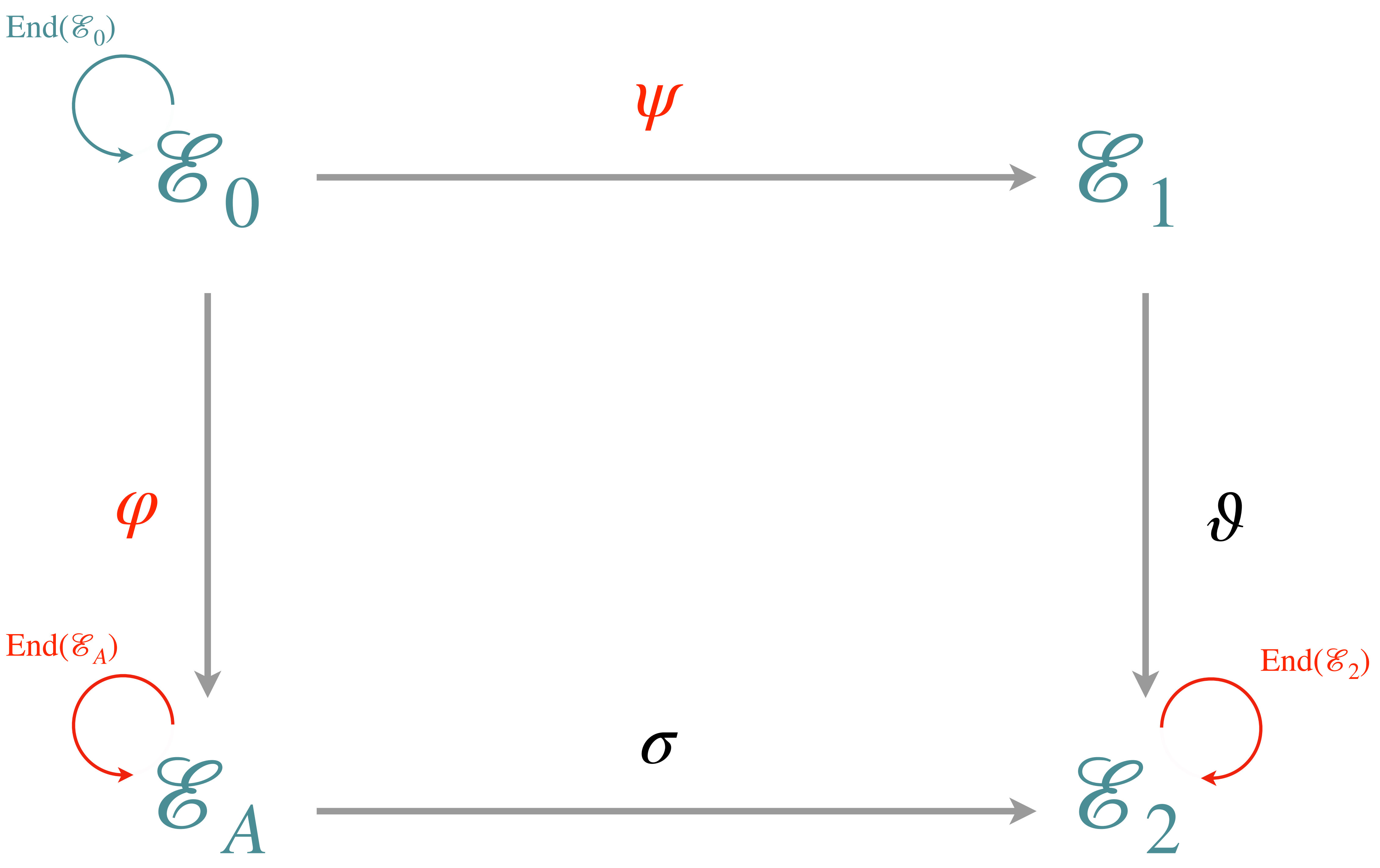
🪄: if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$, we get σ ✨

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

PART 1
The Square

Let's fix the square with isogenies!



(magic)

🪄: if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$, we get σ ✨

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

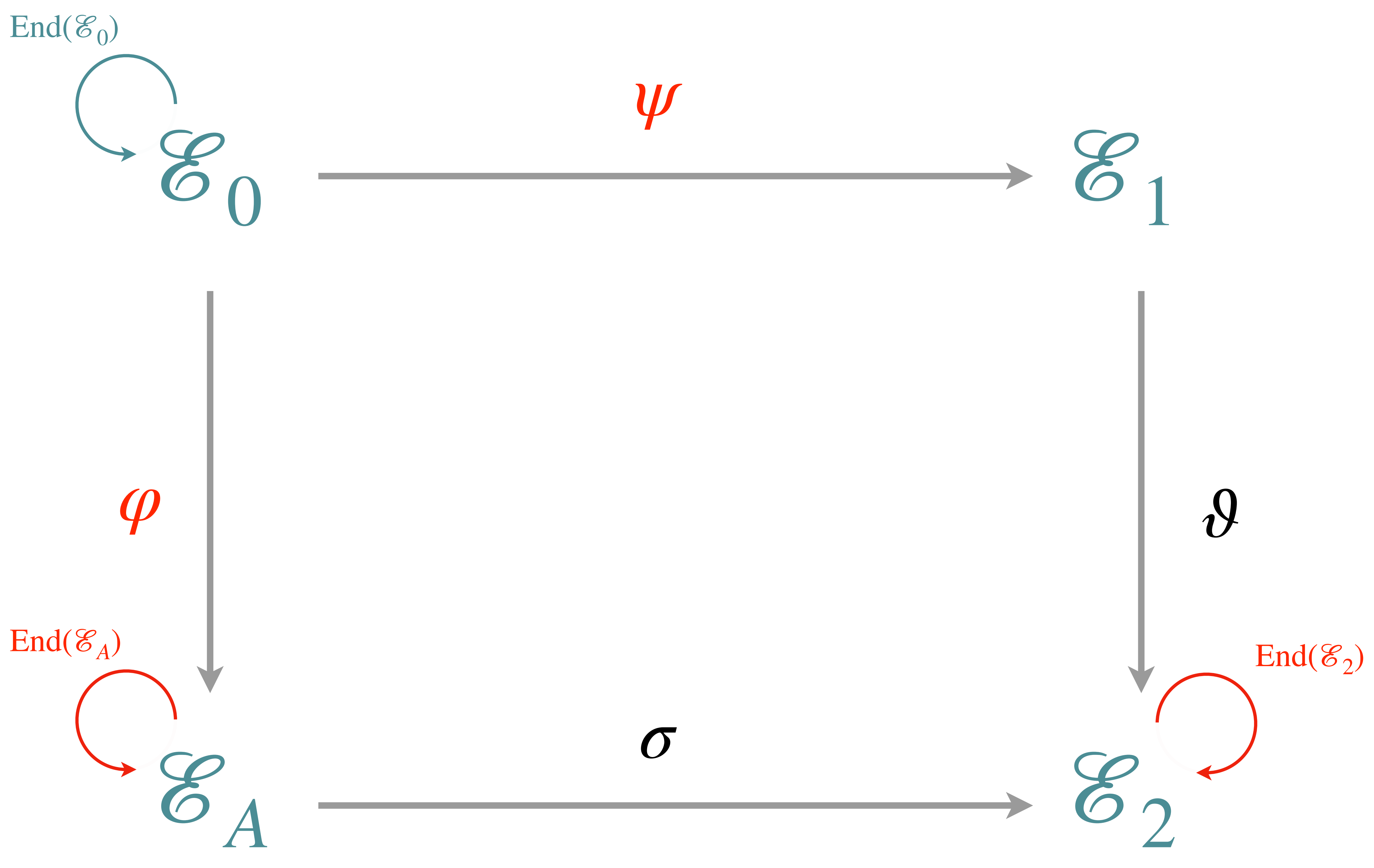
1

We can only find such σ if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$

KU LEUVEN

PART 1
The Square

Let's fix the square with isogenies!



(magic)

🪄: if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$, we get σ ✨

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

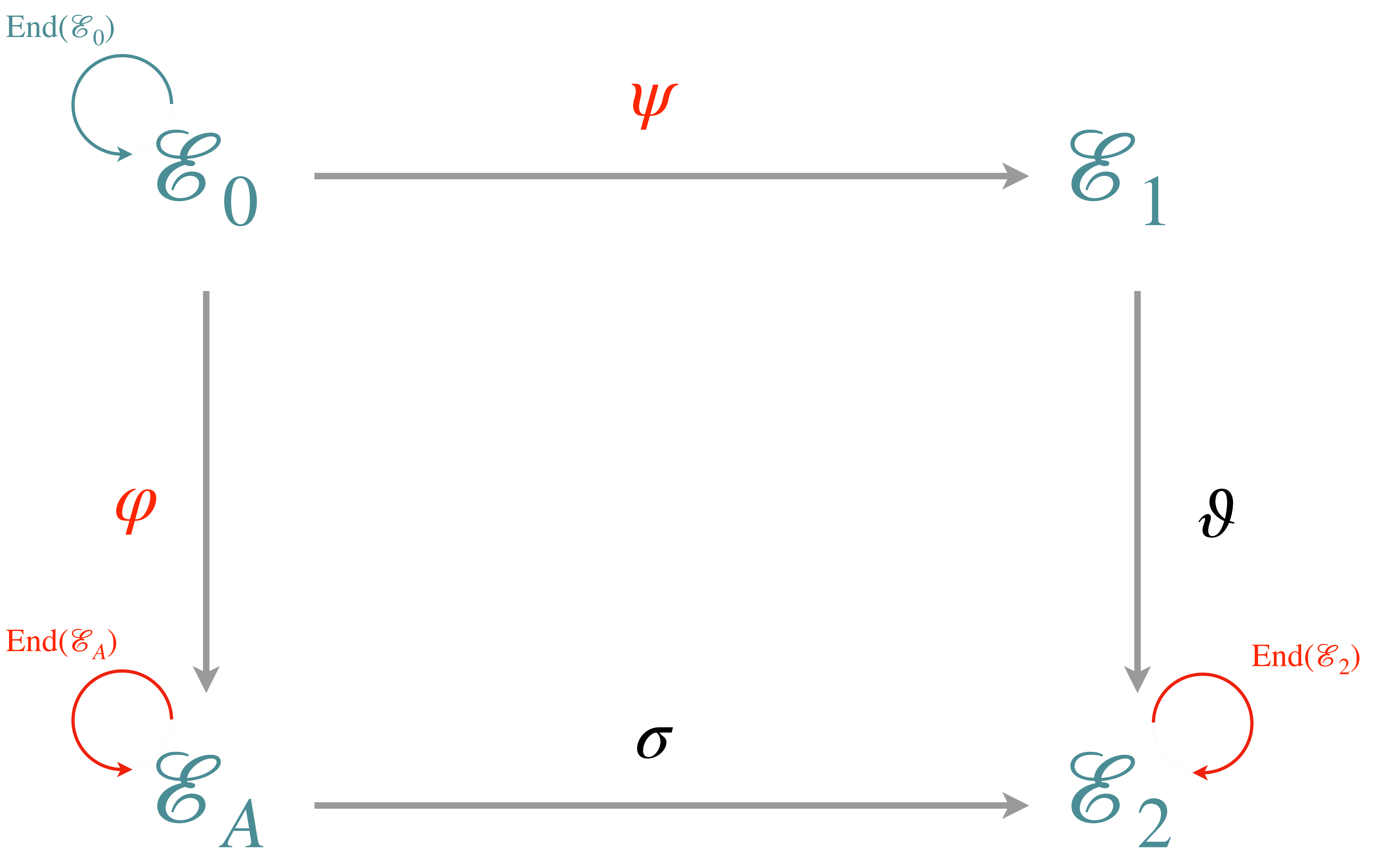
1 We can only find such σ if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$

2 Given just random $\mathscr{E}$, impossible to find $\mathrm{End}(\mathscr{E})$

KU LEUVEN

PART 1
The Square

Let's fix the square with isogenies!



(magic)

🪄: if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$, we get σ ✨

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

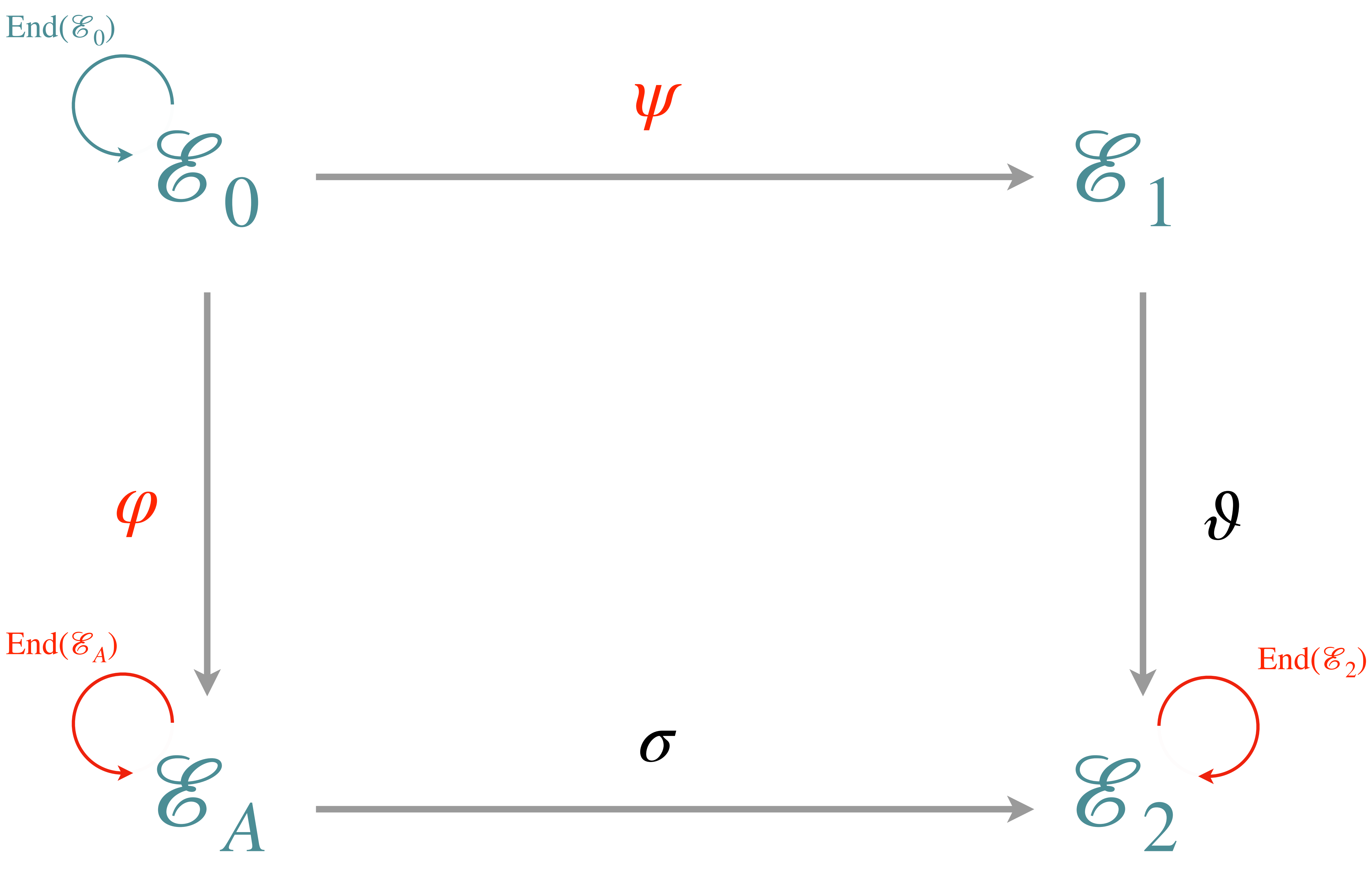
1 We can only find such σ if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$

2 Given just random $\mathscr{E}$, impossible to find $\mathrm{End}(\mathscr{E})$

3 But, we know $\mathrm{End}(\mathscr{E}_0)$, so if we know φ, ψ, ϑ, we learn $\mathrm{End}(\mathscr{E}_A)$, $\mathrm{End}(\mathscr{E}_2)$

PART 1
The Square

Let's fix the square with isogenies!



(magic)

🪄: if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$, we get σ ✨

KEY DIFFERENCE!

1. **DON'T** send $\sigma = \vartheta \circ \psi \circ \hat{\varphi}$, same issue as before
2. there are now *many* isogenies $\mathscr{E}_A \to \mathscr{E}_2$
3. set some requirement on σ, namely specific degree

1 We can only find such σ if we know $\mathrm{End}(\mathscr{E}_A)$ and $\mathrm{End}(\mathscr{E}_2)$

2 Given just random $\mathscr{E}$, impossible to find $\mathrm{End}(\mathscr{E})$

3 But, we know $\mathrm{End}(\mathscr{E}_0)$, so if we know φ, ψ, ϑ, we learn $\mathrm{End}(\mathscr{E}_A)$, $\mathrm{End}(\mathscr{E}_2)$

! Returning σ of specific degree, proves knowledge of φ

Our plan for today

1

Making the square work…

$$\mathscr{E} \xrightarrow{\varphi} \mathscr{E}'$$

with isogenies!

2

Decomposing the square

$$\mathrm{End}(\mathscr{E}) \xrightarrow{\sim} \mathscr{O}$$

with quaternions!

3

SQIsign, SQIsignHD

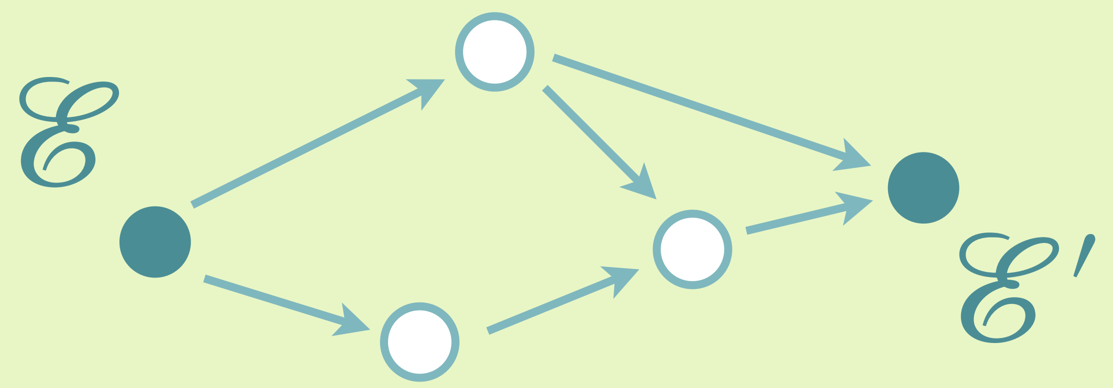
SQIsign2D, SQIsignXD…?

PART 2
Quaternions!

The Deuring correspondence transforms isogeny problems into quaternion problems

ISOGENY

- objects are **curves** $\mathscr{E}$, arrows are **isogenies** φ



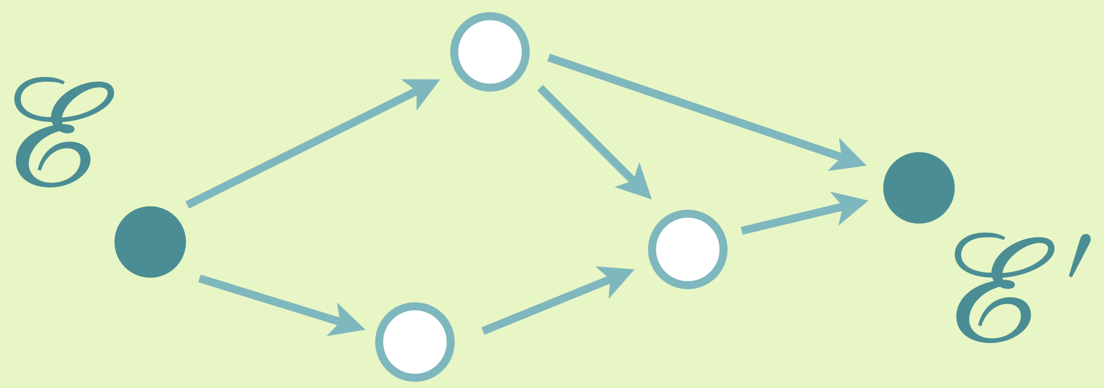
- arrows from $\mathscr{E}$ to itself are **endomorphisms**, the ring of these, $\mathrm{End}(\mathscr{E})$ is very important for SQIsign, equal to the secret key
- if we know $\mathrm{End}(\mathscr{E})$ and $\mathrm{End}(\mathscr{E}')$, we can compute an arrow $\mathscr{E} \to \mathscr{E}'$

PART 2
Quaternions!

The Deuring correspondence transforms isogeny problems into quaternion problems

ISOGENY

- objects are **curves** $\mathscr{E}$, arrows are **isogenies** φ



- arrows from $\mathscr{E}$ to itself are **endomorphisms**, the ring of these, $\mathrm{End}(\mathscr{E})$ is very important for SQIsign, equal to the secret key
- if we know $\mathrm{End}(\mathscr{E})$ and $\mathrm{End}(\mathscr{E}')$, we can compute an arrow $\mathscr{E} \to \mathscr{E}'$

QUATERNIONS

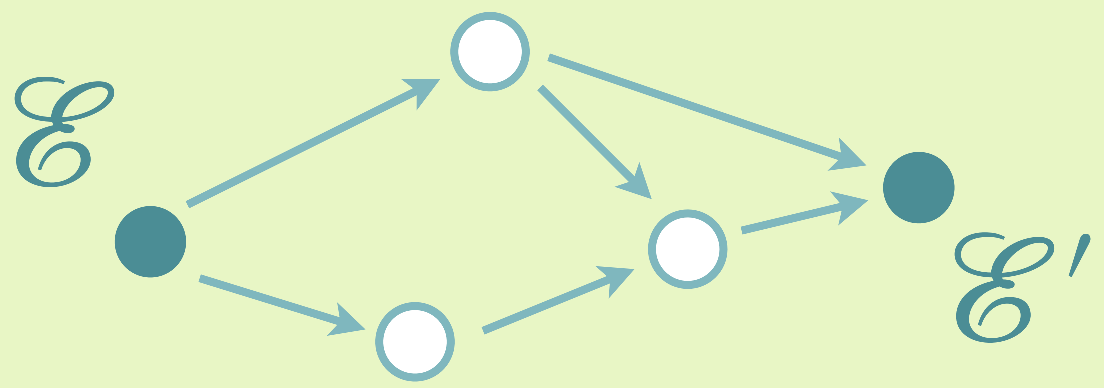
- a **quaternion** looks like $\beta = a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$ and $\mathbf{i}^2 = -1, \mathbf{j}^2 = p, \mathbf{k} = \mathbf{i} \cdot \mathbf{j}$
- form a **non-commutative** algebra, like $\mathbb{C}$ on steroids

PART 2
Quaternions!

The Deuring correspondence transforms isogeny problems into quaternion problems

ISOGENY

- objects are **curves** $\mathscr{E}$, arrows are **isogenies** φ



- arrows from $\mathscr{E}$ to itself are **endomorphisms**, the ring of these, $\mathrm{End}(\mathscr{E})$ is very important for SQIsign, equal to the secret key
- if we know $\mathrm{End}(\mathscr{E})$ and $\mathrm{End}(\mathscr{E}')$, we can compute an arrow $\mathscr{E} \to \mathscr{E}'$

QUATERNIONS

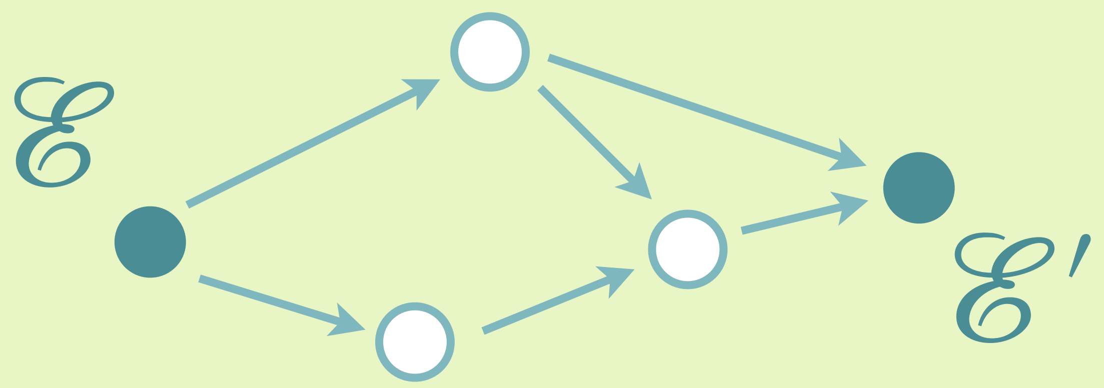
- a **quaternion** looks like $\beta = a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$ and $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = p$, $\mathbf{k} = \mathbf{i} \cdot \mathbf{j}$
- form a **non-commutative** algebra, like $\mathbb{C}$ on steroids
- precise mathematical details for this talk not necessary, just think “different mathematical world”
- objects are **maximal orders** $\mathcal{O}$, arrows are **ideals** I

PART 2
Quaternions!

The Deuring correspondence transforms isogeny problems into quaternion problems

ISOGENY

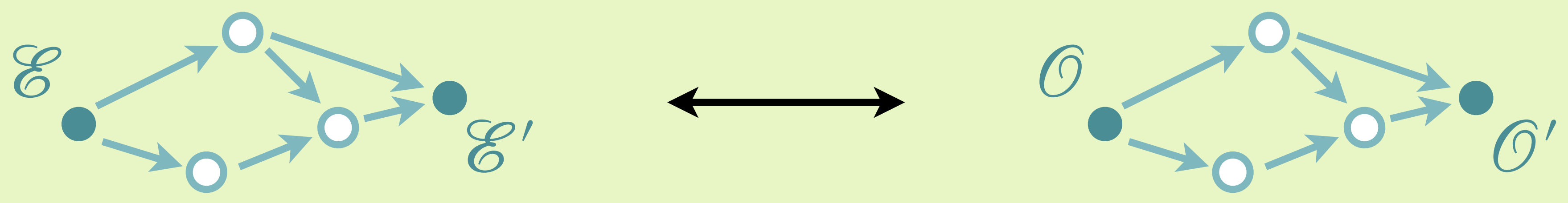
- objects are **curves** $\mathscr{E}$, arrows are **isogenies** φ



- arrows from $\mathscr{E}$ to itself are **endomorphisms**, the ring of these, $\mathrm{End}(\mathscr{E})$ is very important for SQIsign, equal to the secret key
- if we know $\mathrm{End}(\mathscr{E})$ and $\mathrm{End}(\mathscr{E}')$, we can compute an arrow $\mathscr{E} \to \mathscr{E}'$

QUATERNIONS

- a **quaternion** looks like $\beta = a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$ and $\mathbf{i}^2 = -1, \mathbf{j}^2 = p, \mathbf{k} = \mathbf{i} \cdot \mathbf{j}$
- form a **non-commutative** algebra, like $\mathbb{C}$ on steroids
- precise mathematical details for this talk not necessary, just think “different mathematical world”
- objects are **maximal orders** $\mathcal{O}$, arrows are **ideals** I
- **Thm. *(Deuring, informal)***
  Up to technical details, the world of isogenies and the world of maximal quat. orders are the same!



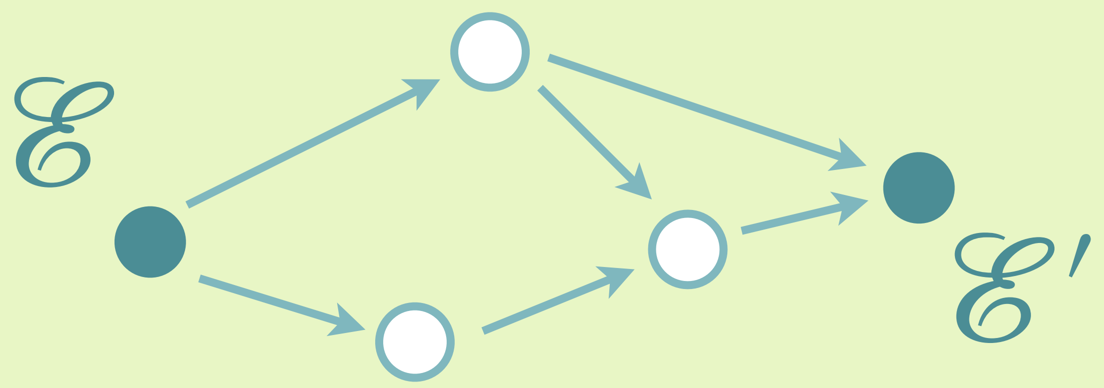
KU LEUVEN

PART 2
Quaternions!

The Deuring correspondence transforms isogeny problems into quaternion problems

ISOGENY

- objects are **curves** $\mathscr{E}$, arrows are **isogenies** φ



- arrows from $\mathscr{E}$ to itself are **endomorphisms**, the ring of these, $\mathrm{End}(\mathscr{E})$ is very important for SQIsign, equal to the secret key
- if we know $\mathrm{End}(\mathscr{E})$ and $\mathrm{End}(\mathscr{E}')$, we can compute an arrow $\mathscr{E} \to \mathscr{E}'$

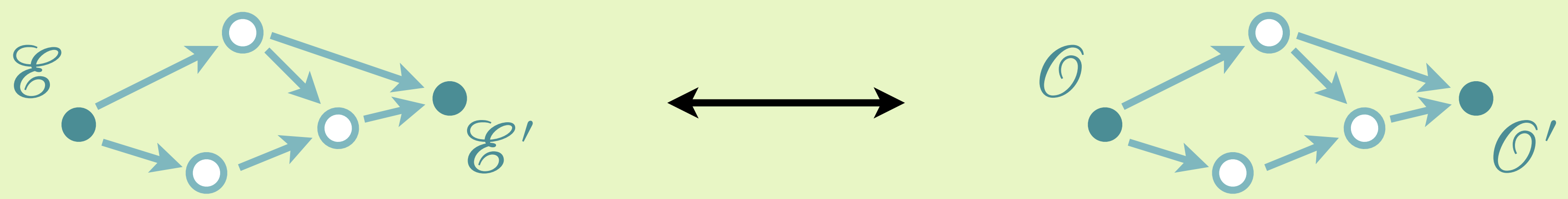
Deuring

$\mathscr{E} \mapsto \mathrm{End}(\mathscr{E})$

$\mathcal{O} \cong \mathrm{End}(\mathscr{E})$

QUATERNIONS

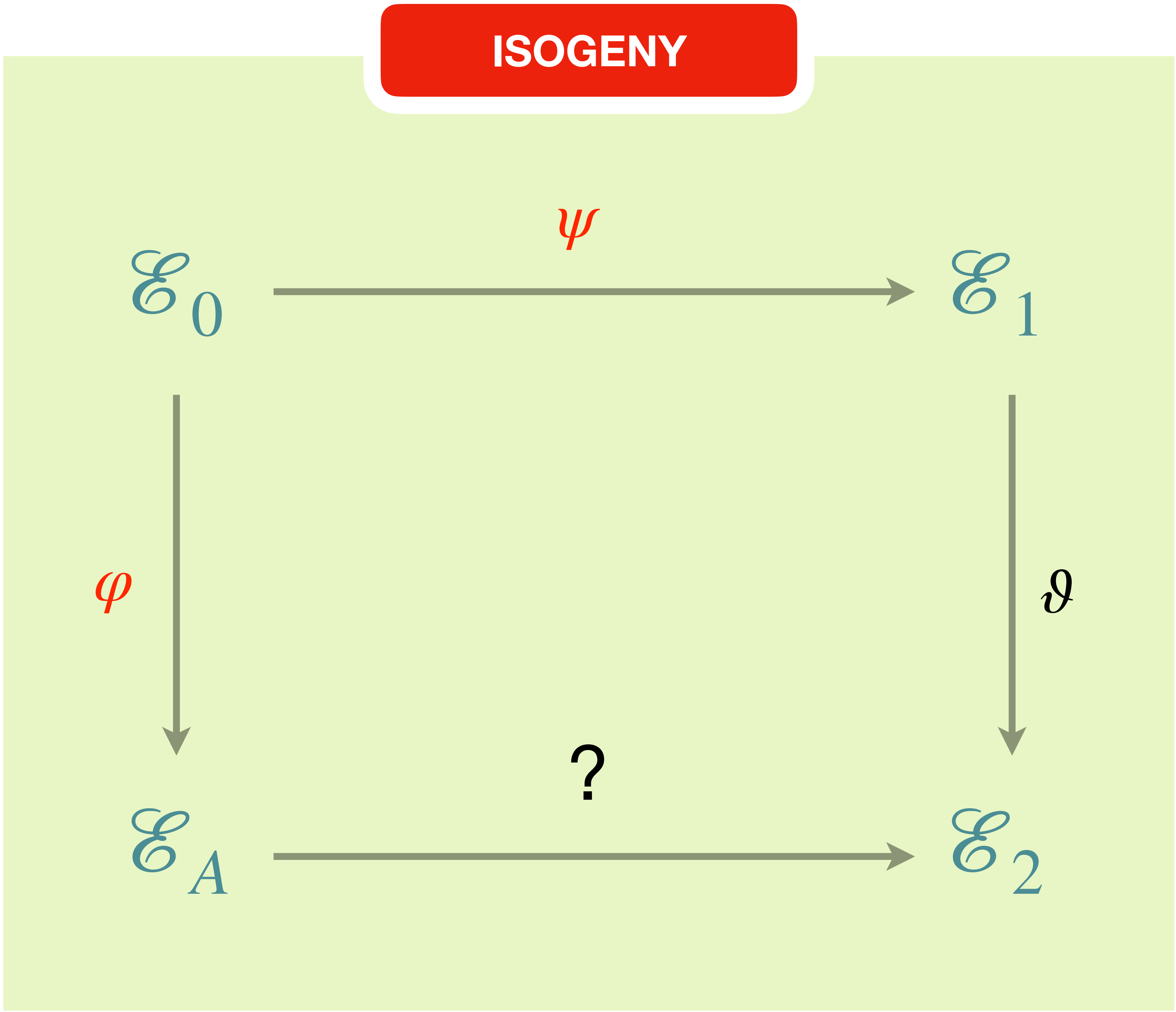
- a **quaternion** looks like $\beta = a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$ and $\mathbf{i}^2 = -1, \mathbf{j}^2 = p, \mathbf{k} = \mathbf{i} \cdot \mathbf{j}$
- form a **non-commutative** algebra, like $\mathbb{C}$ on steroids
- precise mathematical details for this talk not necessary, just think “different mathematical world”
- objects are **maximal orders** $\mathcal{O}$, arrows are **ideals** I
- **Thm. *(Deuring, informal)***
  Up to technical details, the world of isogenies and the world of maximal quat. orders are the same!



KU LEUVEN

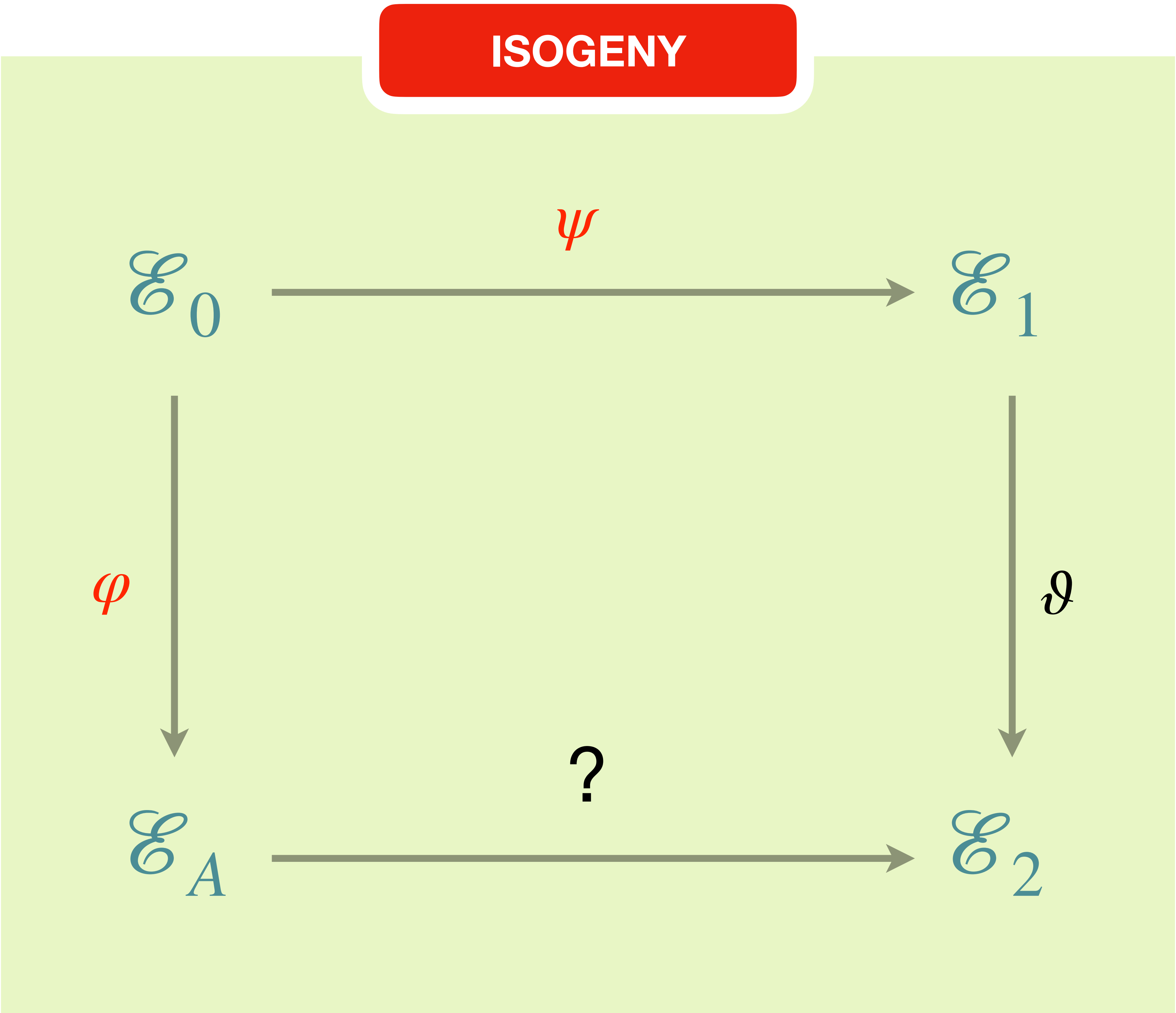
PART 2
Quaternions!

Translate the SQIsign square to the quaternion world: finding $\mathscr{E} \to \mathscr{E}'$ becomes advanced linear algebra



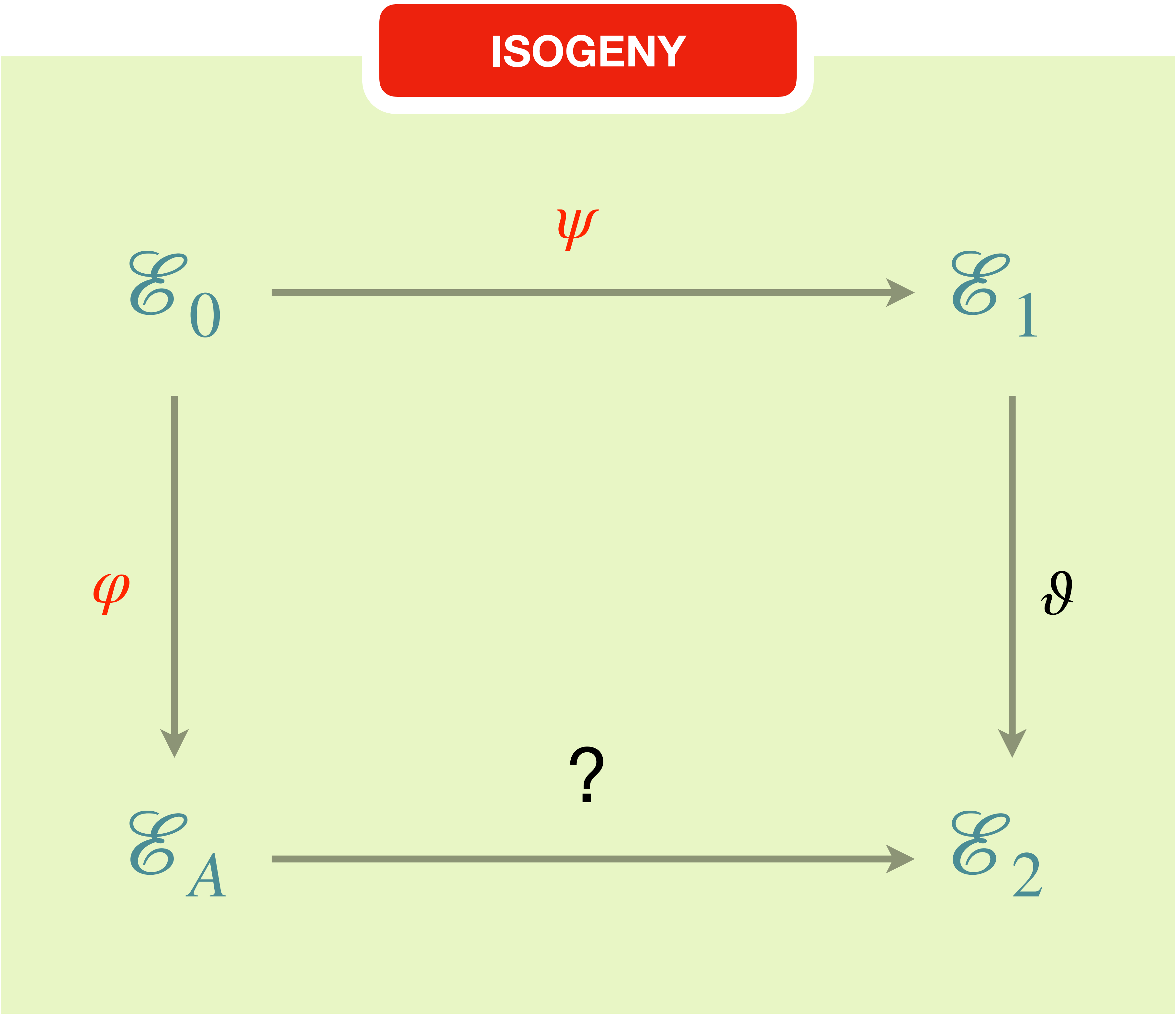
PART 2
Quaternions!

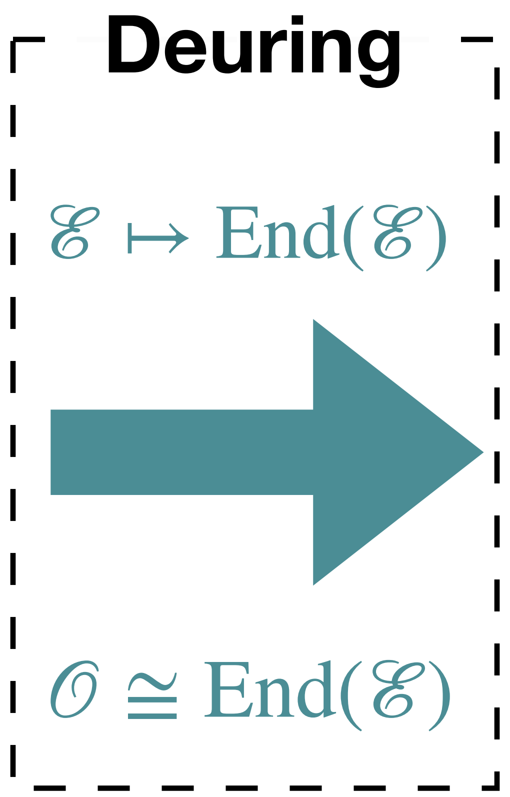
Translate the SQIsign square to the quaternion world: finding $\mathcal{E} \to \mathcal{E}'$ becomes advanced linear algebra



PART 2
Quaternions!

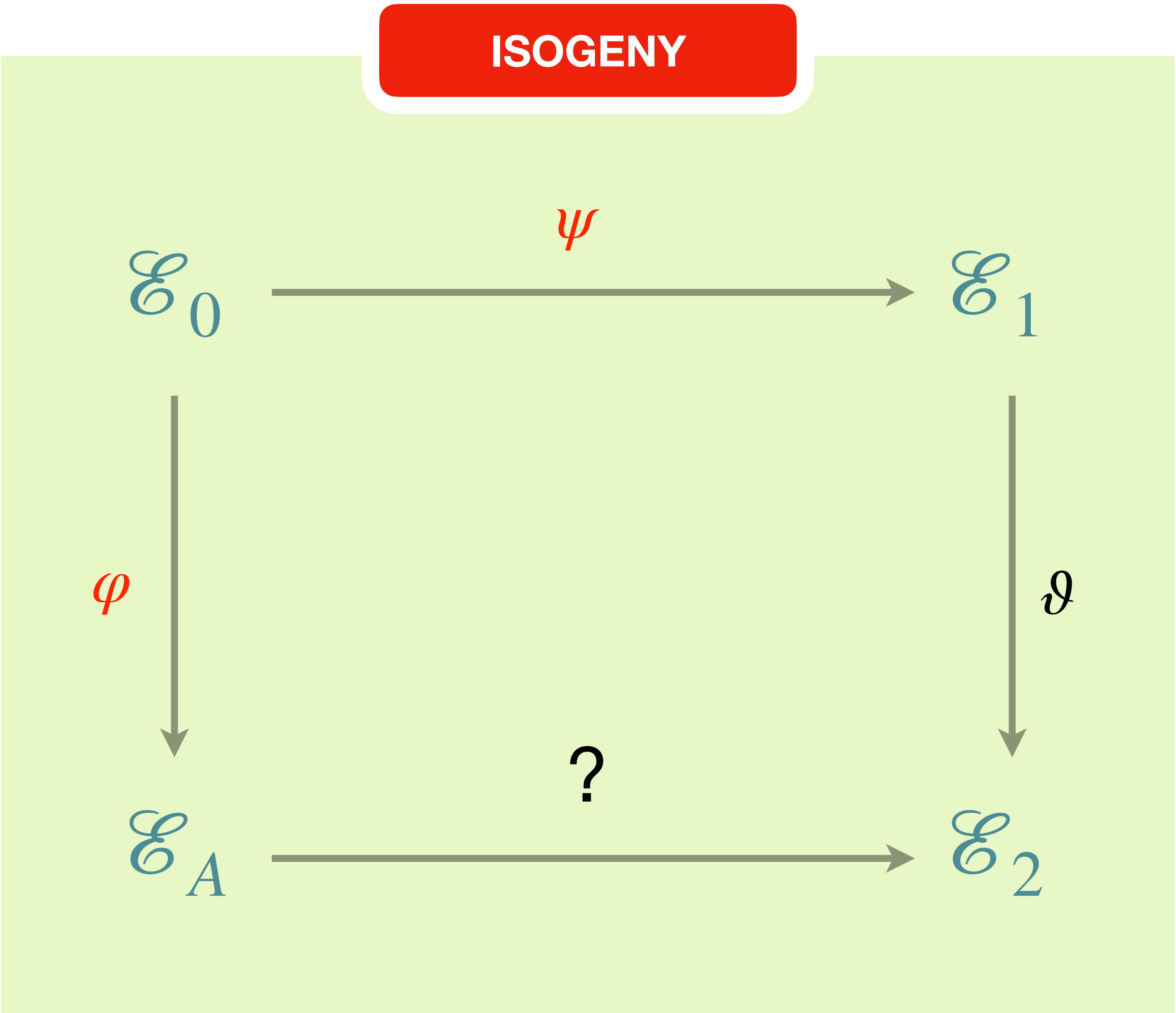
Translate the SQIsign square to the quaternion world: finding $\mathscr{E} \to \mathscr{E}'$ becomes advanced linear algebra

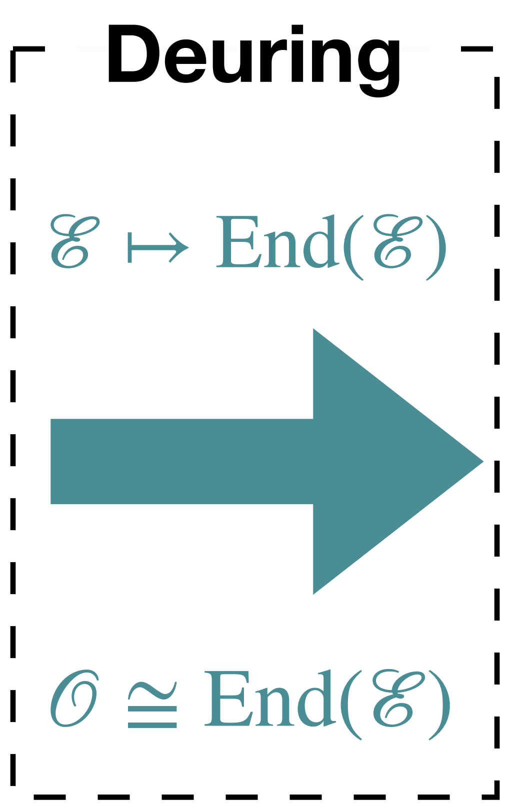


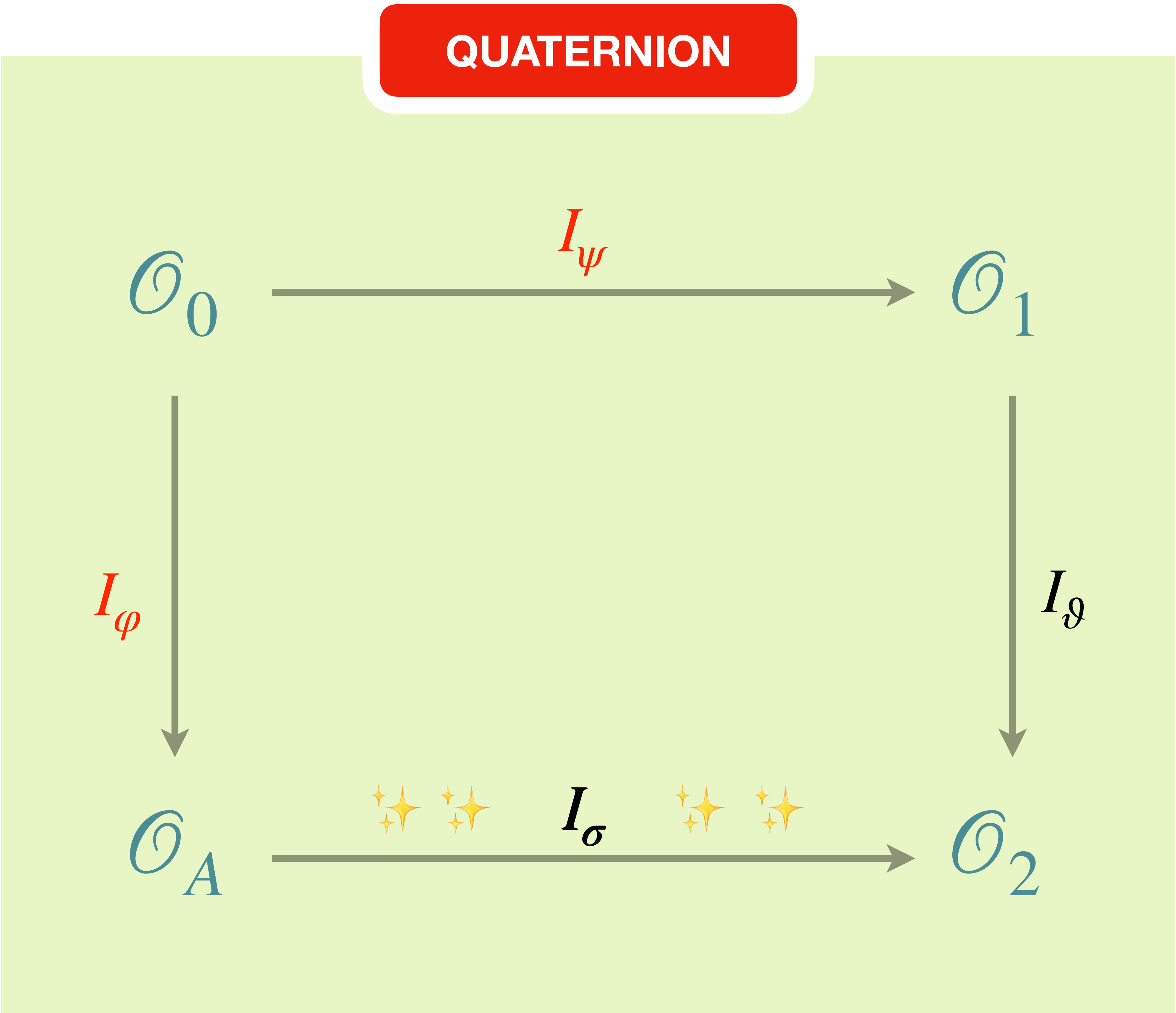


PART 2
Quaternions!

Translate the SQIsign square to the quaternion world: finding $\mathscr{E} \to \mathscr{E}'$ becomes advanced linear algebra

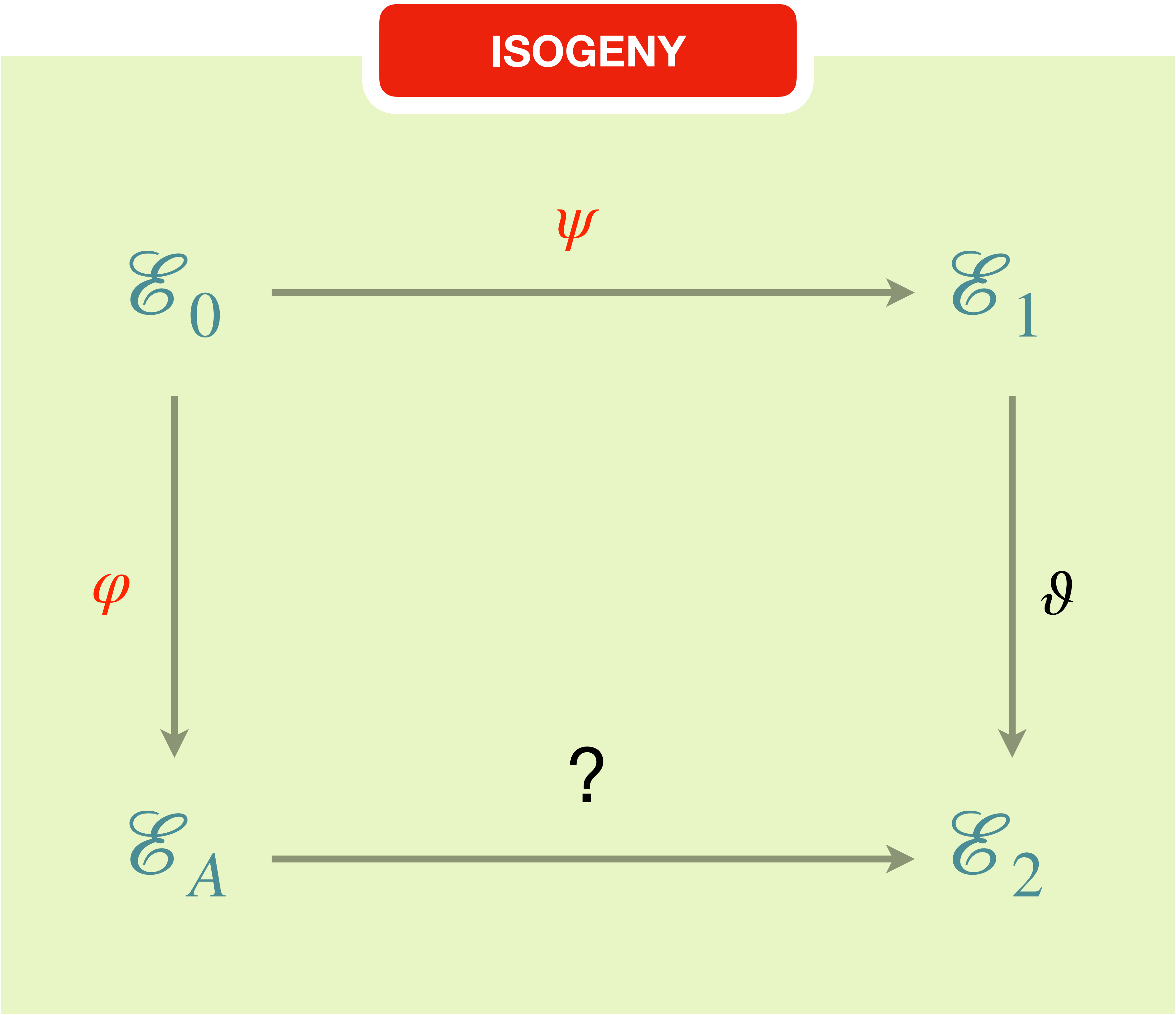


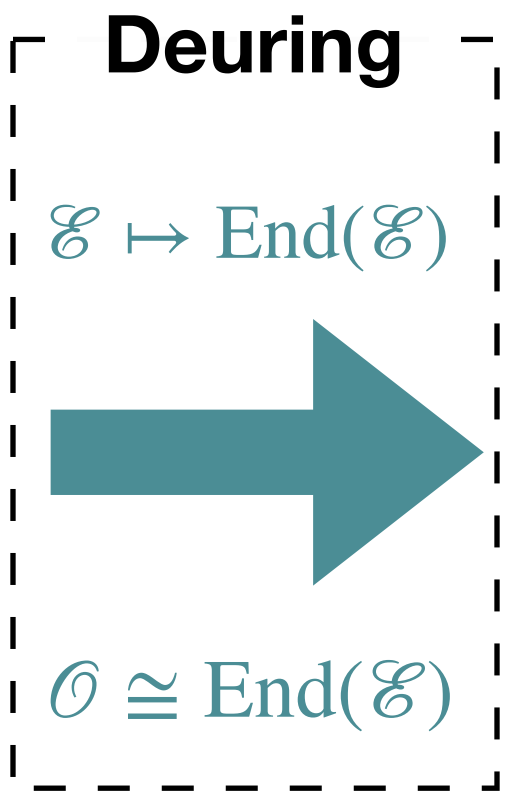




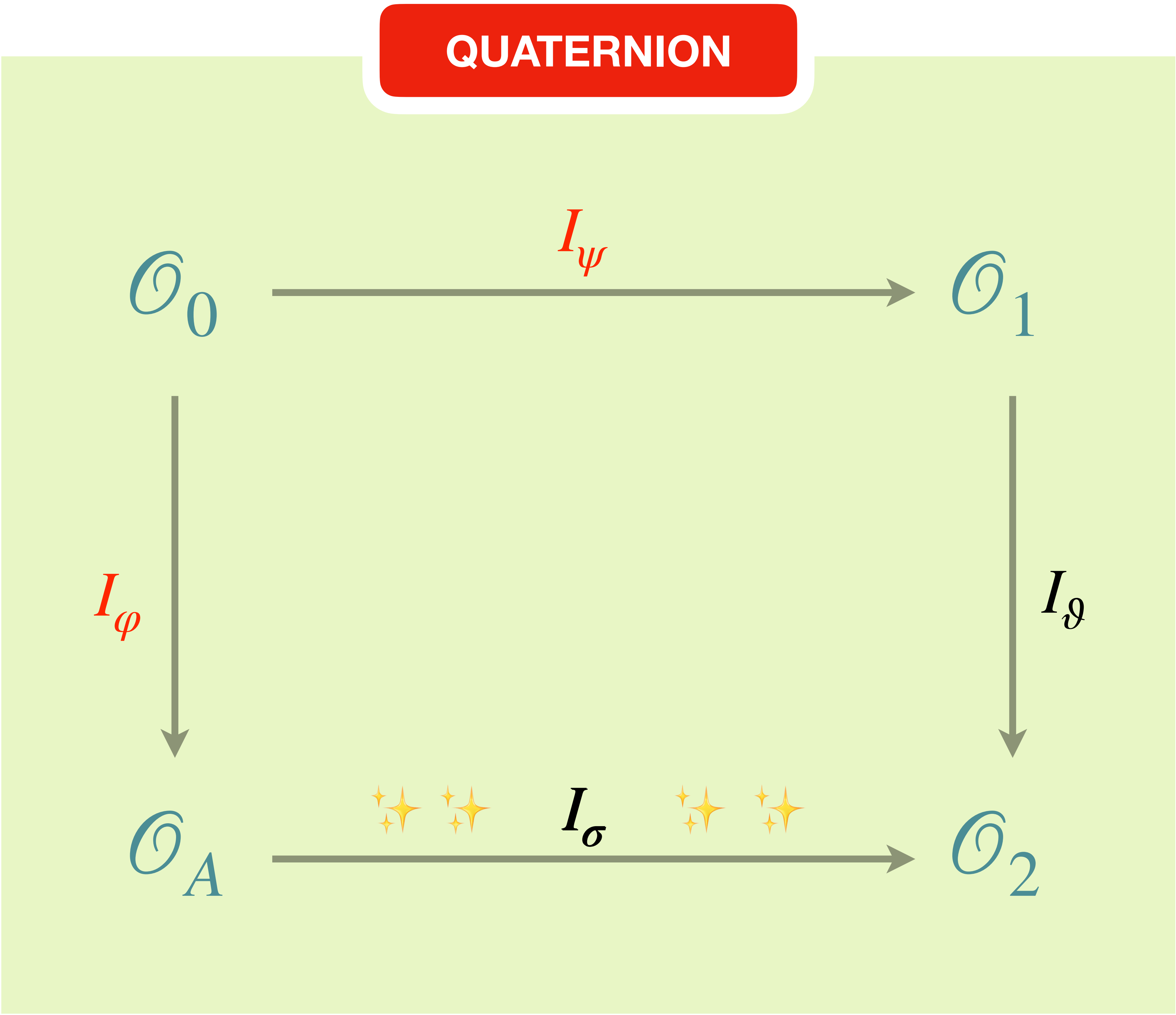
PART 2
Quaternions!

Translate the SQIsign square to the quaternion world: finding $\mathscr{E} \to \mathscr{E}'$ becomes advanced linear algebra



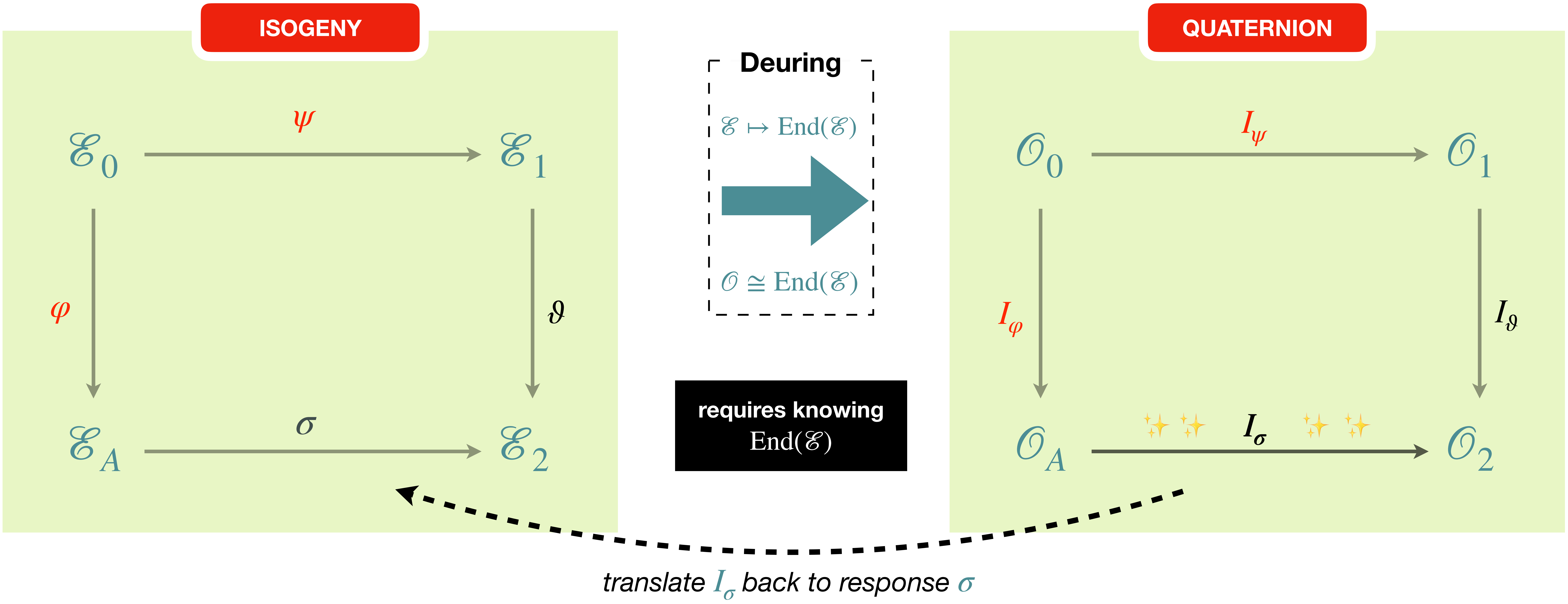


requires knowing $\mathrm{End}(\mathscr{E})$



PART 2
Quaternions!

Translate the SQIsign square to the quaternion world: finding $\mathscr{E} \to \mathscr{E}'$ becomes advanced linear algebra

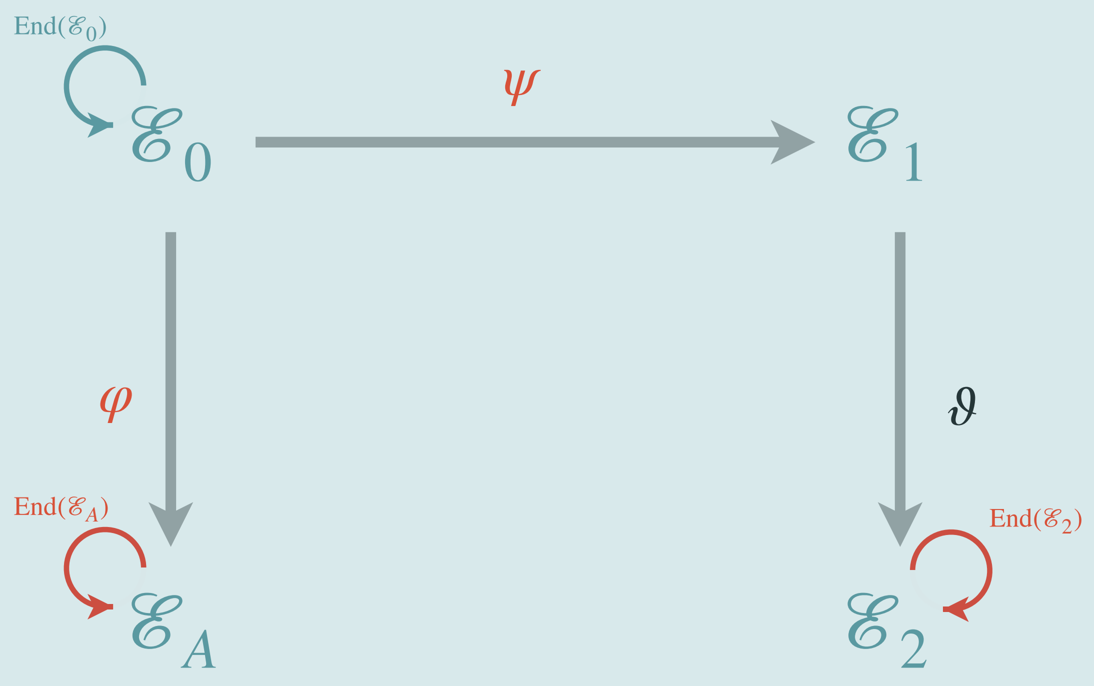


Main recipe for SQIsign: three challenges

0

SETUP

Build the square in the isogeny world, translate to the quaternion world



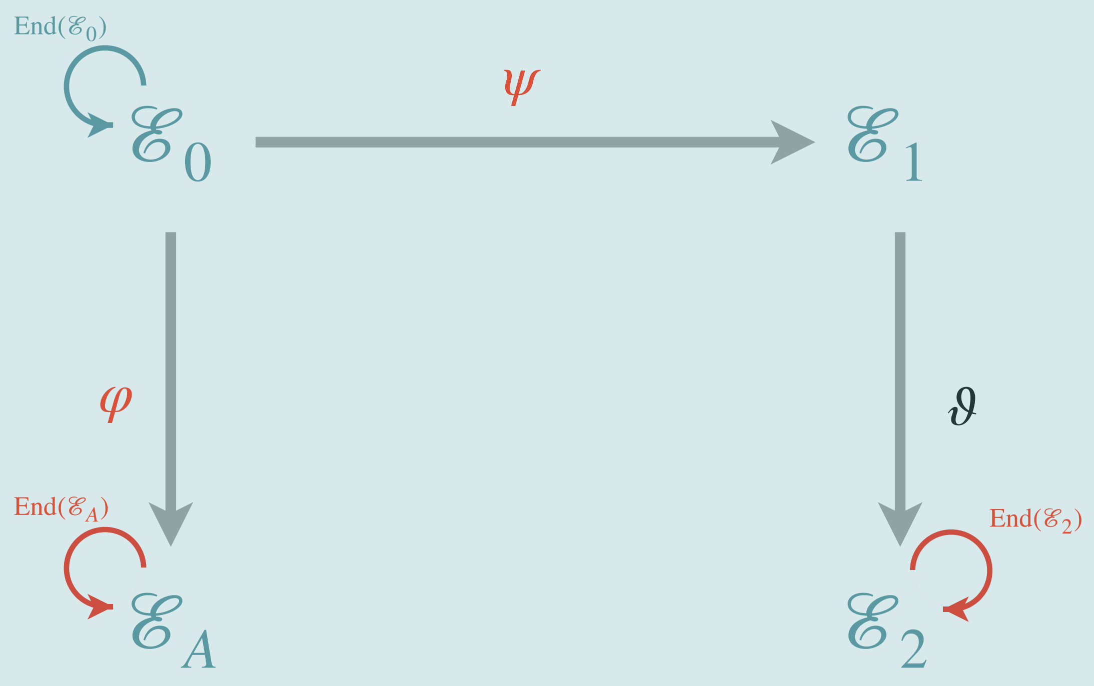
PART 2
Quaternions!

Main recipe for SQIsign: three challenges

0

SETUP

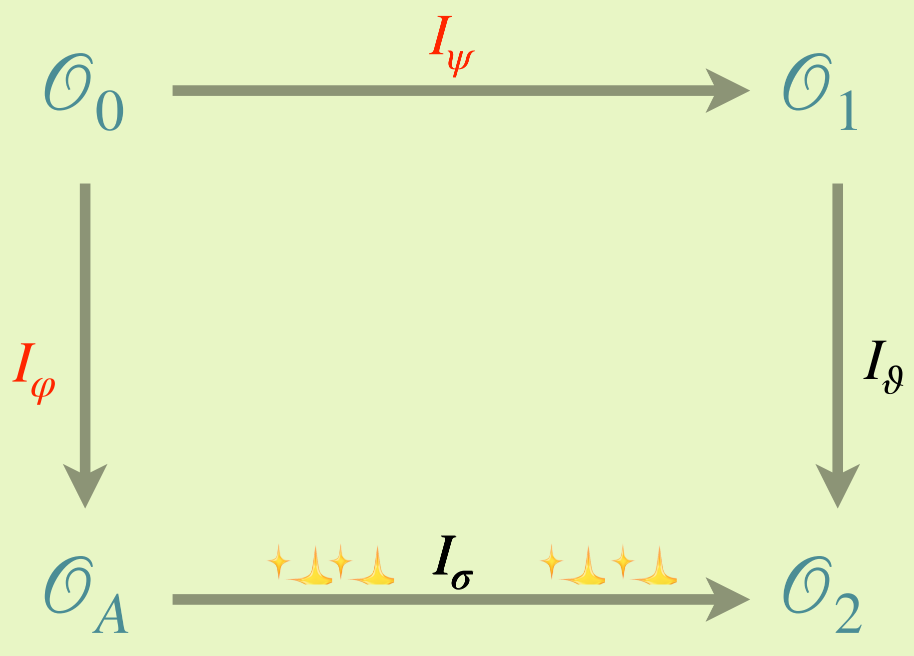
Build the square in the isogeny world, translate to the quaternion world



1

FIND IDEAL

Given the quaternion setup, find the "right" ideal I_σ up to some conditions

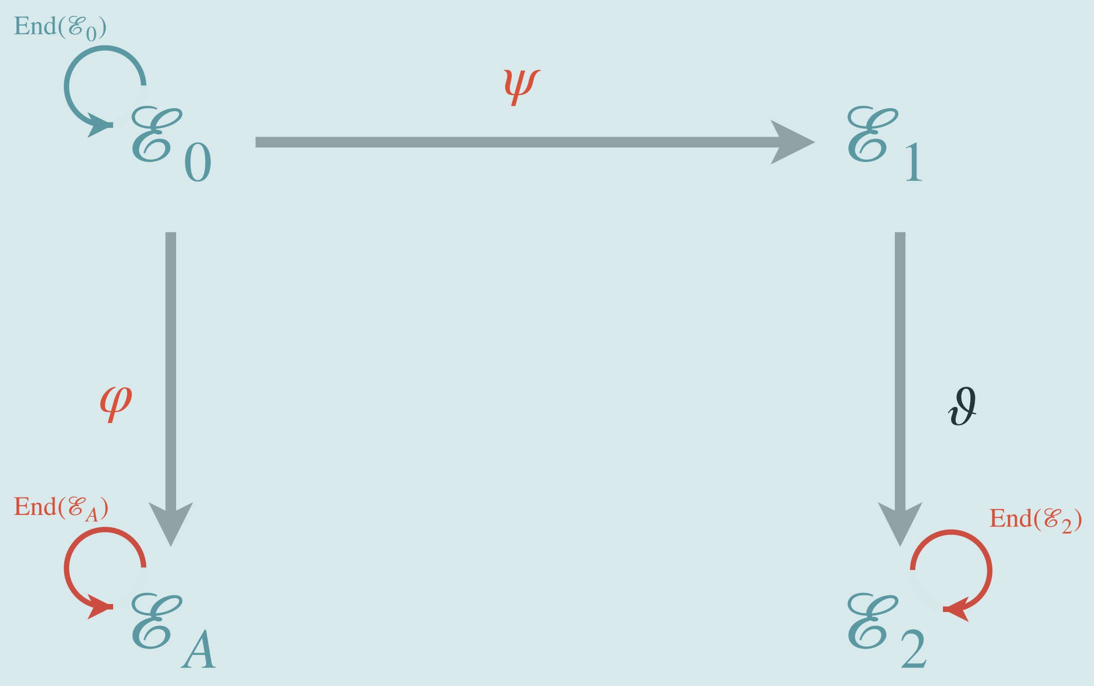


Main recipe for SQIsign: three challenges

0

SETUP

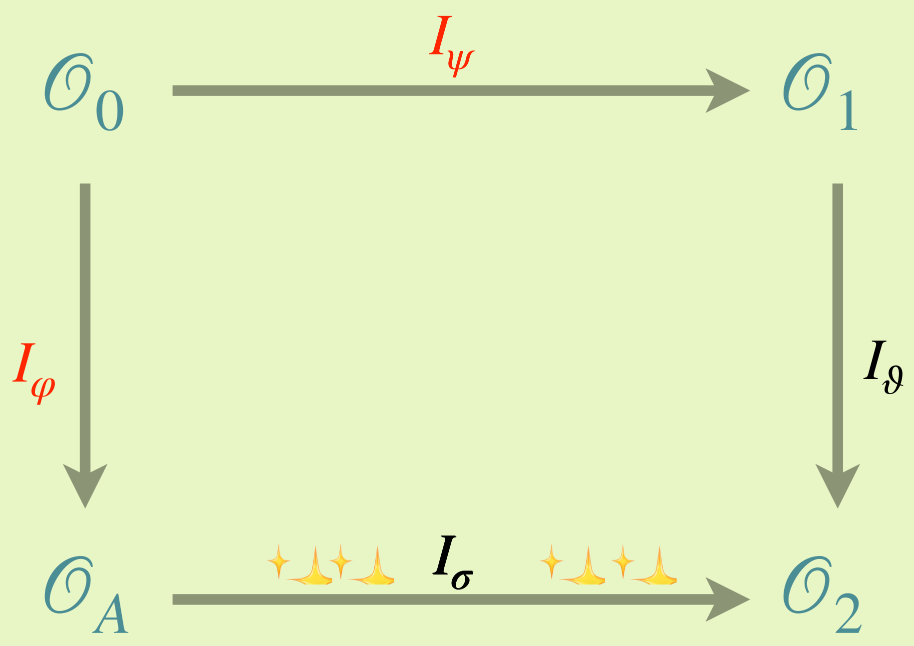
Build the square in the isogeny world, translate to the quaternion world



1

FIND IDEAL

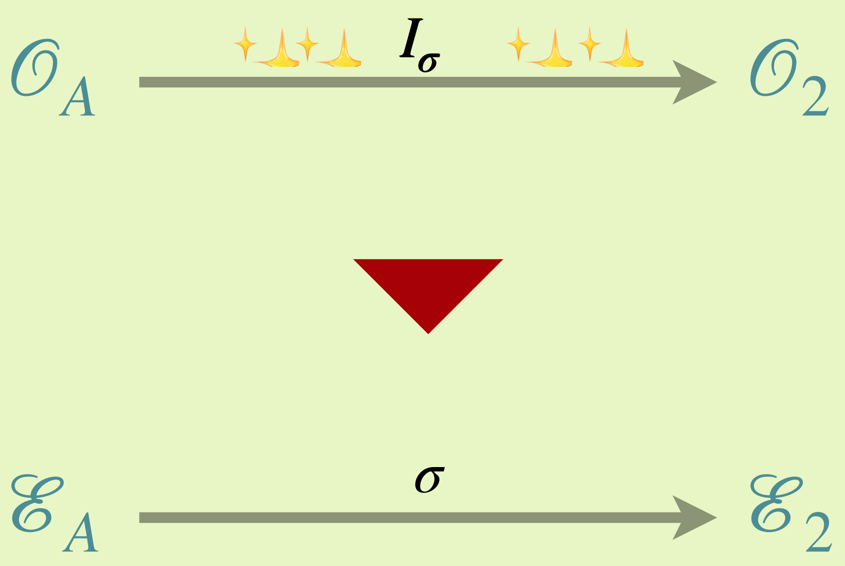
Given the quaternion setup, find the "right" ideal I_σ up to some conditions



2

IDEAL TO ISOGENY

Given this ideal I_σ, translate back to an isogeny $\sigma : E_A \to E_2$



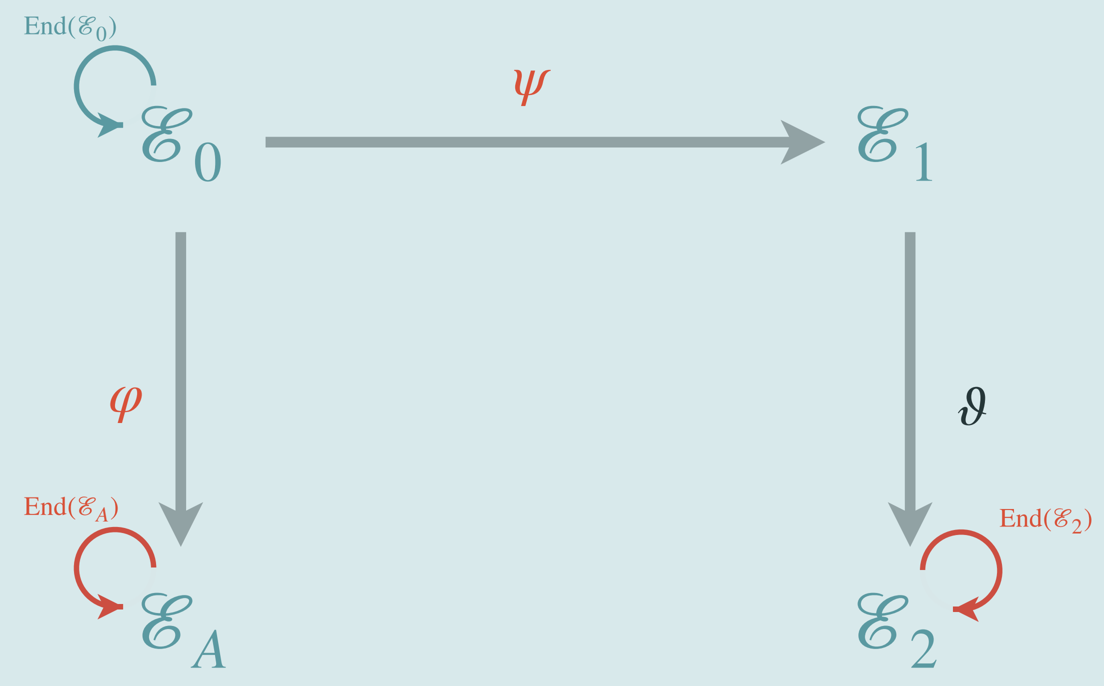
PART 2
Quaternions!

Main recipe for SQIsign: three challenges

0

SETUP

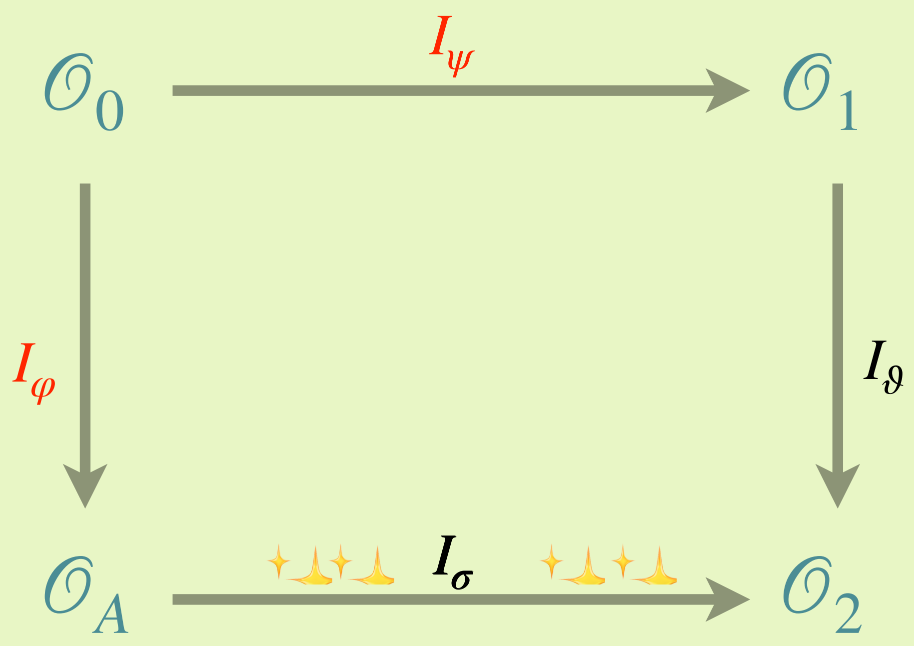
Build the square in the isogeny world, translate to the quaternion world



1

FIND IDEAL

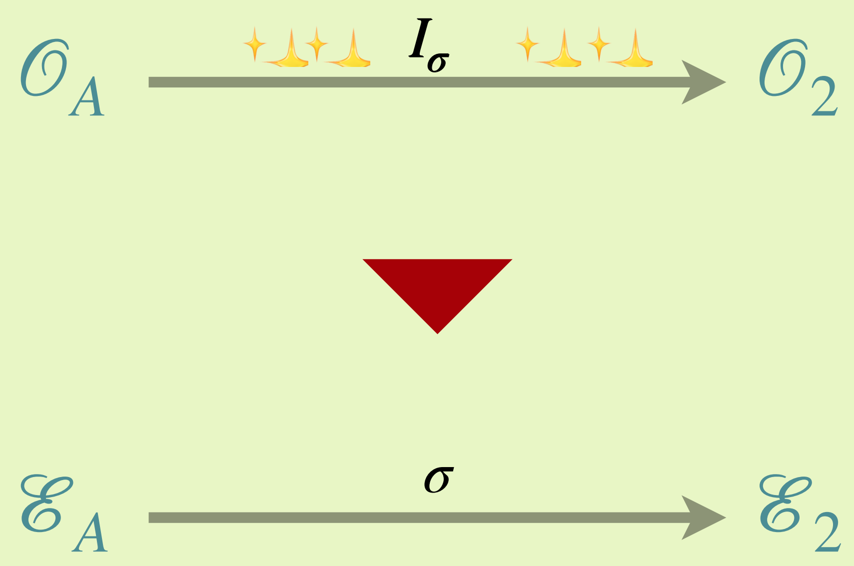
Given the quaternion setup, find the "right" ideal I_σ up to some conditions



2

IDEAL TO ISOGENY

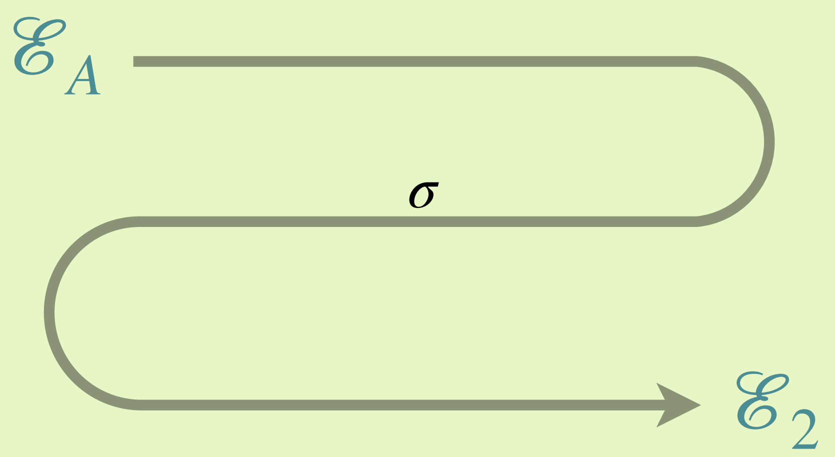
Given this ideal I_σ, translate back to an isogeny $\sigma : E_A \rightarrow E_2$



3

VERIFY

Compute the isogeny σ, which proves knowledge of the secret key φ



(determines verification speed)

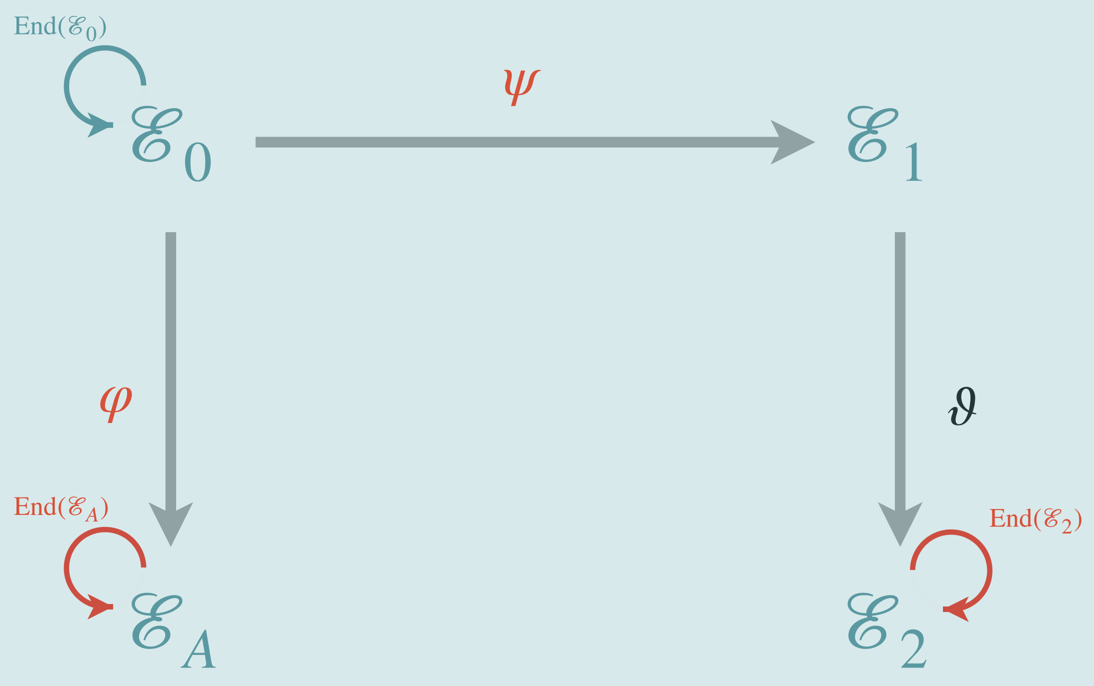
PART 2
Quaternions!

Main recipe for SQIsign: three challenges

0

SETUP

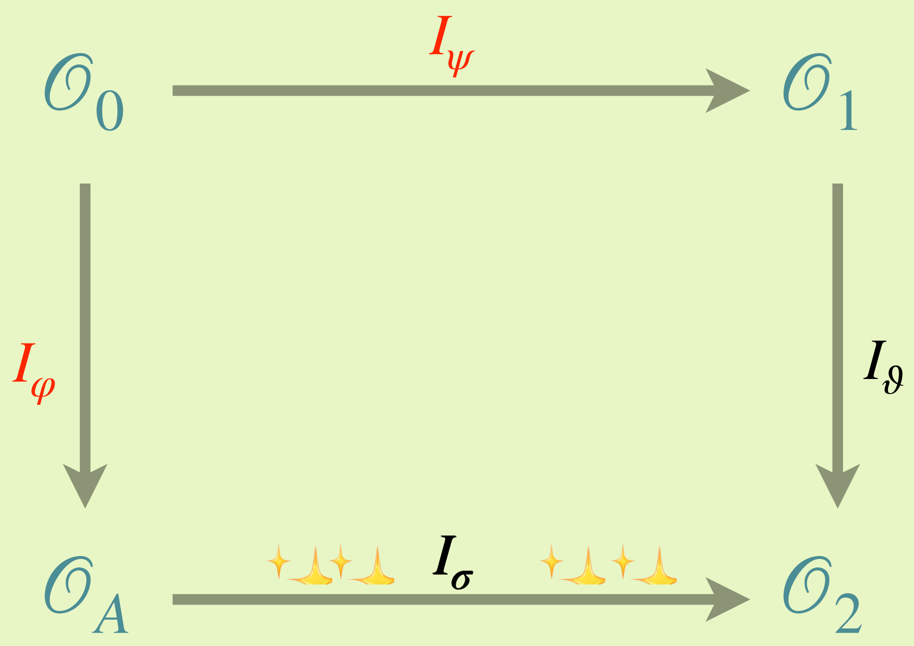
Build the square in the isogeny world, translate to the quaternion world



1

FIND IDEAL

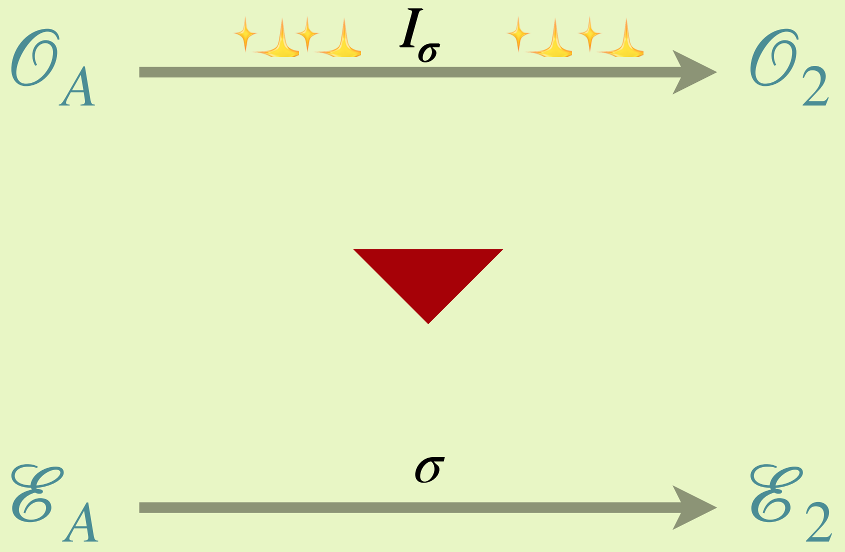
Given the q   rnion setup,
find the "r   t" ideal I_σ
up to som   conditions



2

IDEAL TO ISOGENY

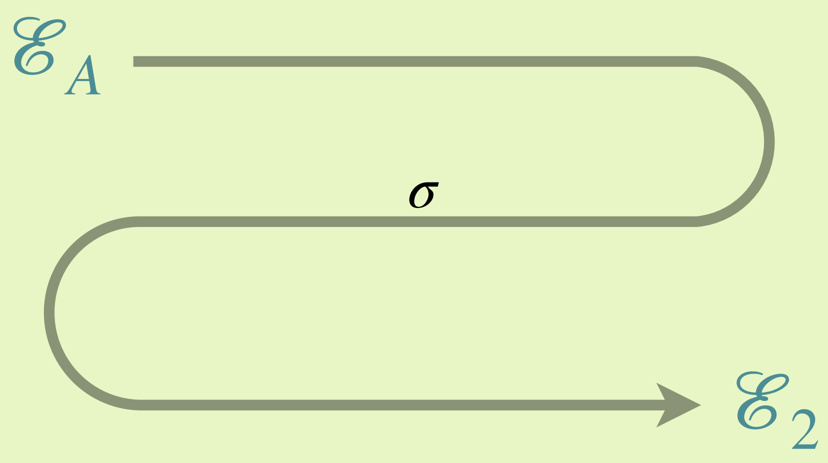
Given this ideal I_σ,
translate back to an isogeny
$\sigma : E_A \to E_2$



3

VERIFY

Compute the isogeny σ,
which proves knowledge
of the secret key φ



(determines verification speed)

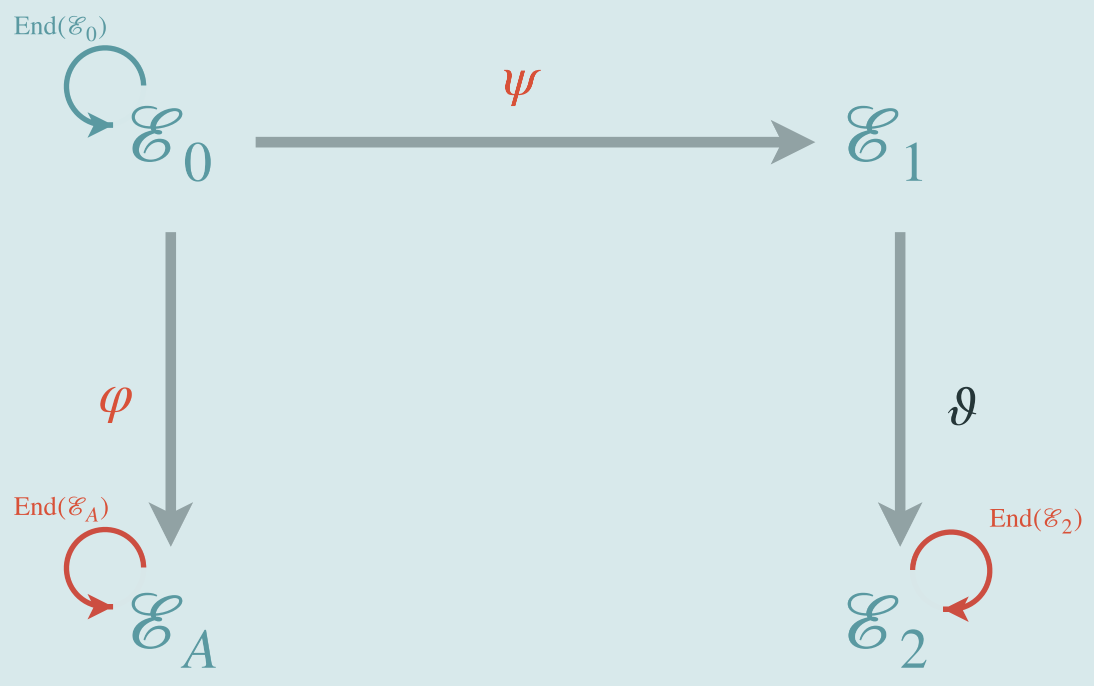
PART 2
Quaternions!

Main recipe for SQIsign: three challenges

0

SETUP

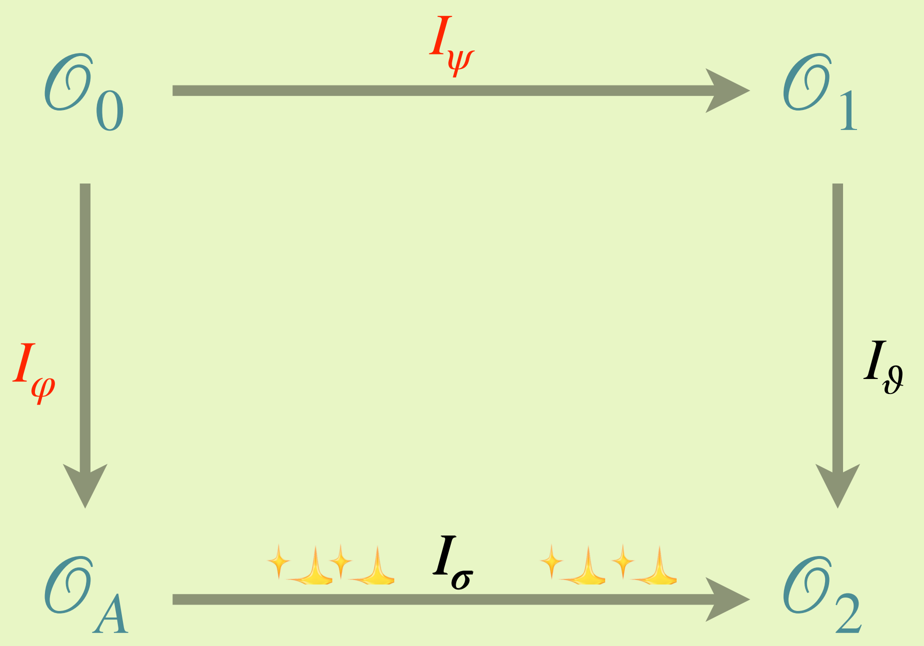
Build the square in the isogeny world, translate to the quaternion world



1

FIND IDEAL

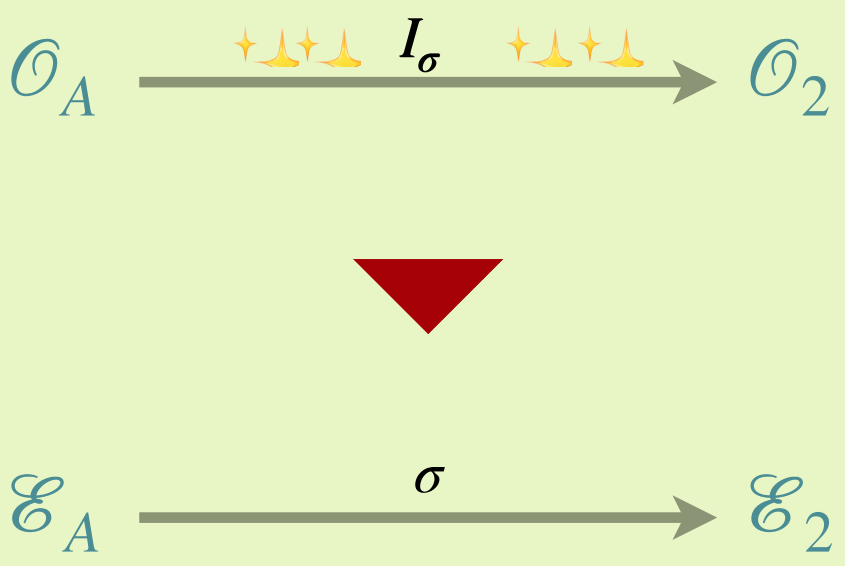
Given the q rnion setup, find the “r t” ideal I_σ up to som conditions



2

IDEAL TO ISOGENY

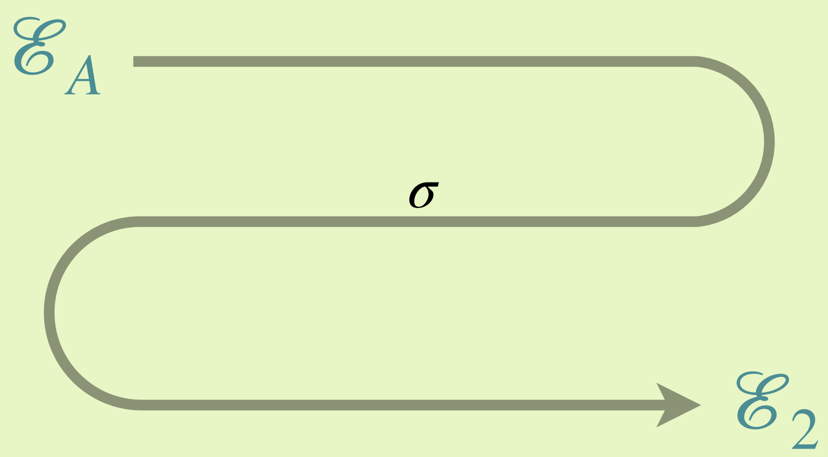
Given this idea translate back to an iso y $\sigma : E_A \to E_2$



3

VERIFY

Compute the isogeny σ, which proves knowledge of the secret key φ



(determines verification speed)

KU LEUVEN

Our plan for today

1

Making the square work…

$$\mathscr{E} \xrightarrow{\varphi} \mathscr{E}'$$

with isogenies!

2

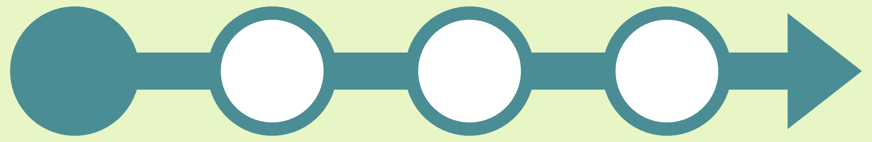
Decomposing the square

$$\mathrm{End}(\mathscr{E}) \xrightarrow{\sim} \mathcal{O}$$

with quaternions!

3

SQIsign, SQIsignHD



SQIsign2D, SQIsignXD…?

KU LEUVEN

PART 3

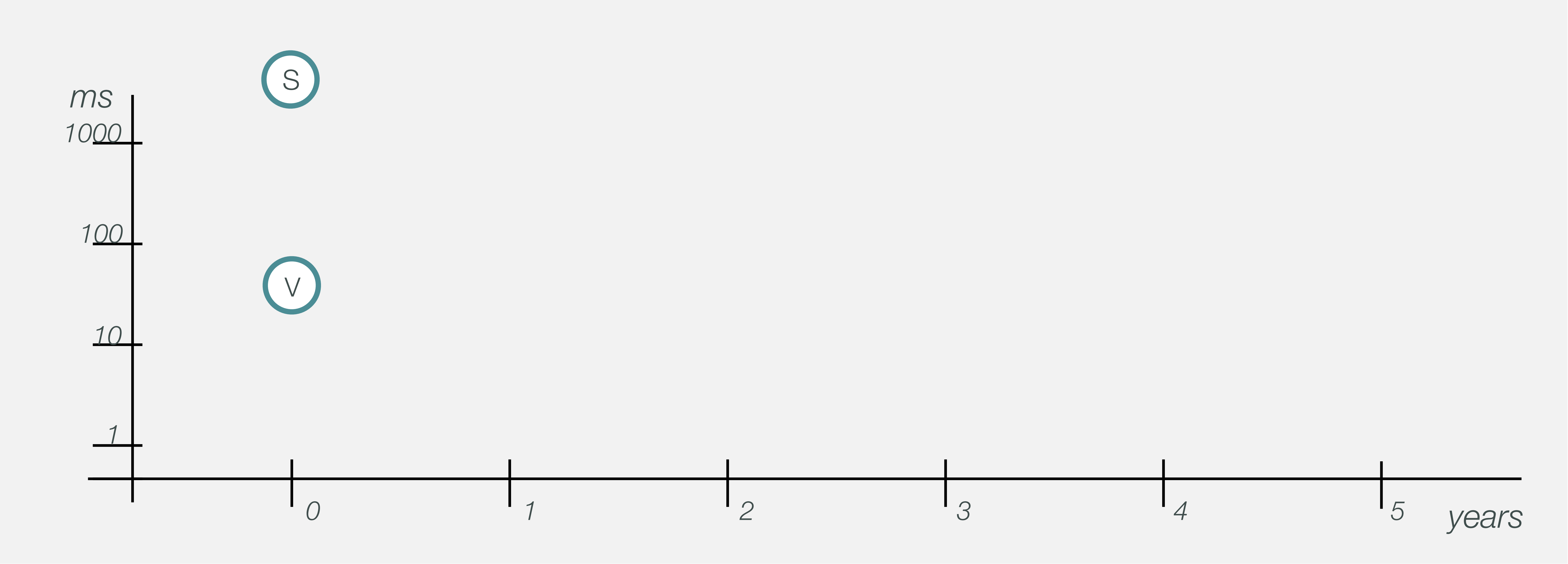
The Variants

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2020	2022	2023	2024	2025

PART 3
The Variants



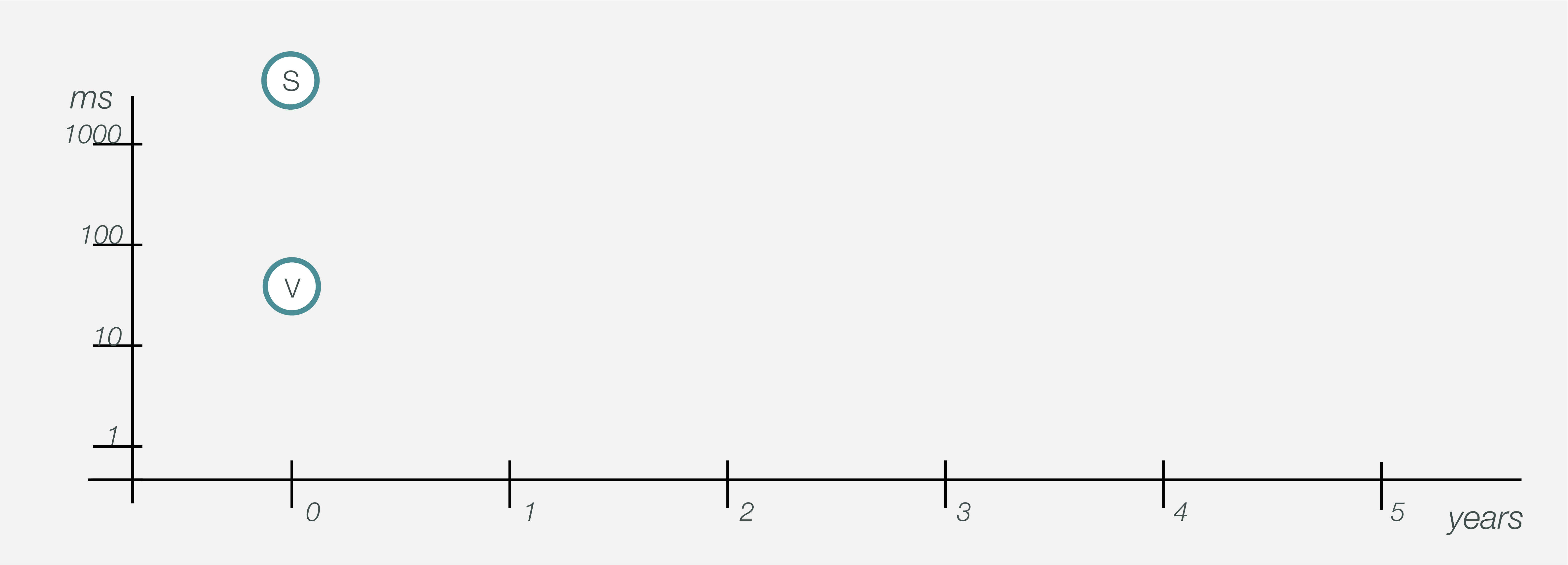
SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2020 | 2022 | 2023 | 2024 | 2025

PART 3

The Variants



SQIsign

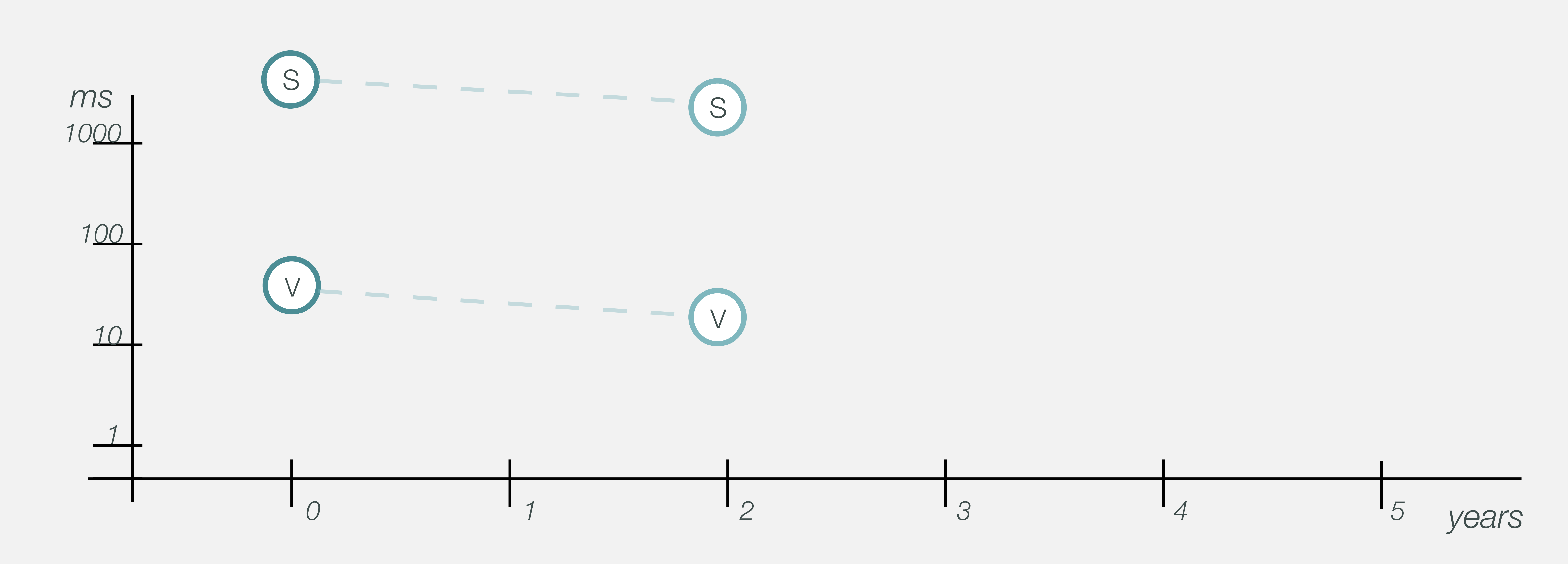
A new isogeny-based signature scheme, with **high soundness.**

2020 | 2022 | 2023 | 2024 | 2025

summary

1. **Find Ideal**: KLPT (magic)
2. **Id-2-Isog:** Slow, tedious
3. **Verify**: deg. 2^{1000} isogeny

PART 3
The Variants



SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

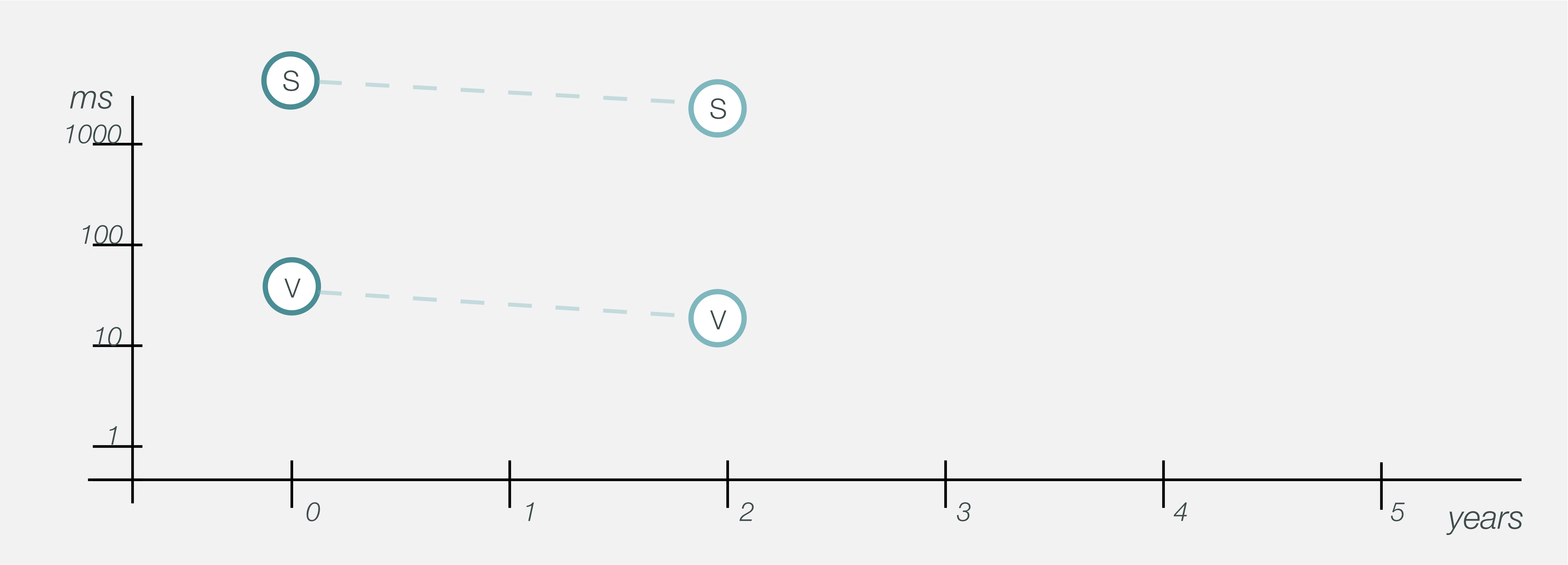
2020 | 2022 | 2023 | 2024 | 2025

summary

1. **Find Ideal**: KLPT (magic)
2. **Id-2-Isog:** Twice as fast!
3. **Verify**: deg. 2^{1000} isogeny

PART 3

The Variants



SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

2020 | 2022 | 2023 | 2024 | 2025

summary

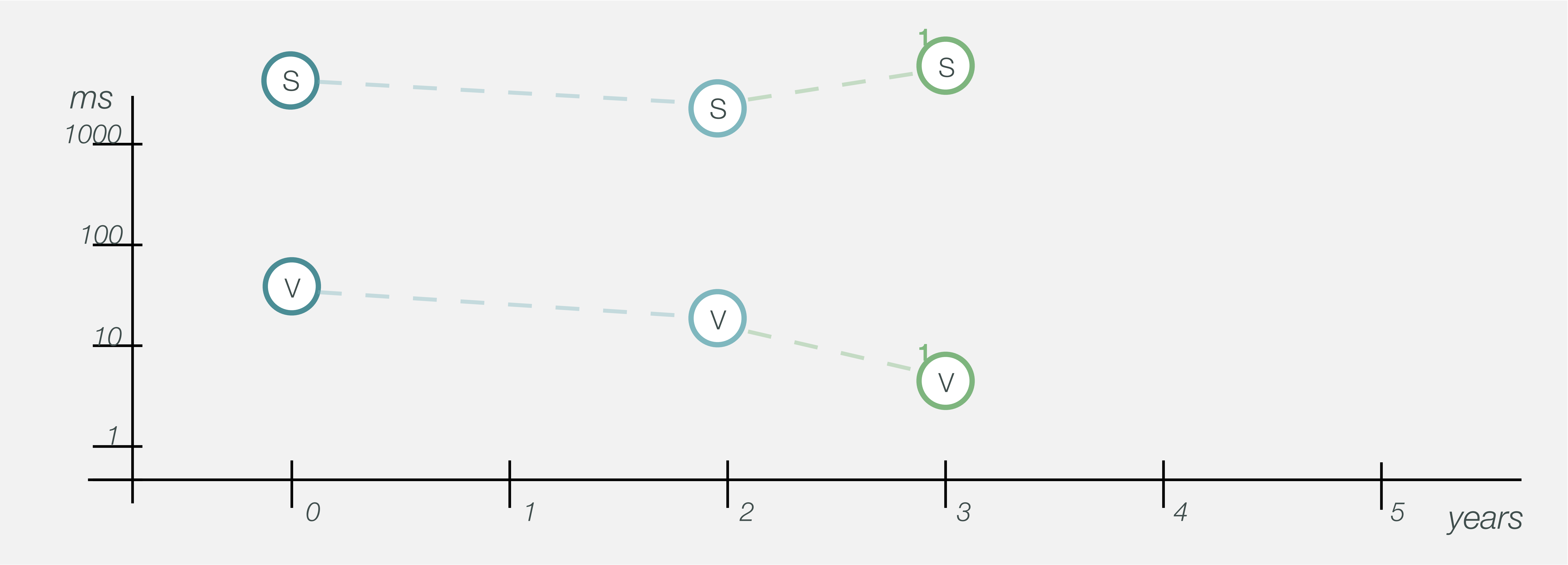
1. **Find Ideal**: KLPT (magic)
2. **Id-2-Isog:** Twice as fast!
3. **Verify**: deg. 2^{1000} isogeny

SIKE breaks

SIKE was destroyed using **HD isogenies** in the summer of 2022.

PART 3

The Variants



SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

AprèsSQI

Signing is slow anyway… Push verification to **maximal** efficiency!

2020 | 2022 | 2023 | 2024 | 2025

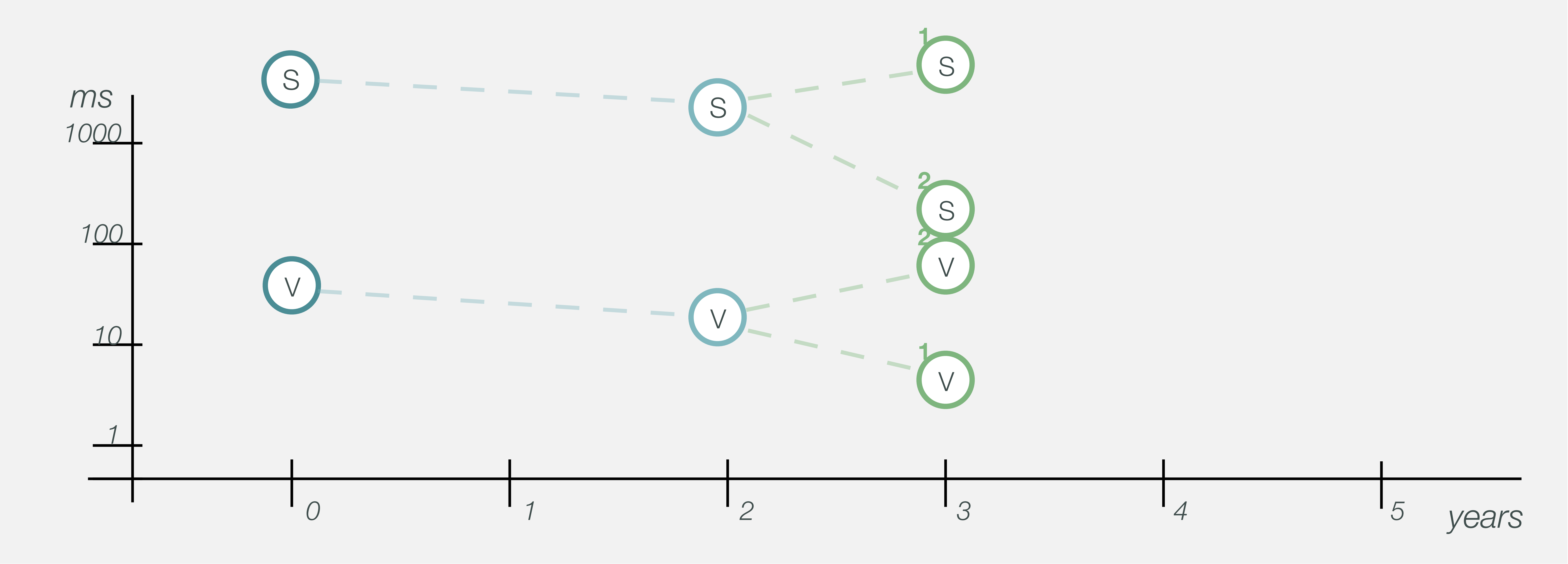
SIKE breaks

SIKE was destroyed using **HD isogenies** in the summer of 2022.

summary

1. **Find Ideal**: KLPT (magic)
2. **Id-2-Isog:** Twice as slow!
3. **Verify**: fast 2^{1000} isogeny

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

ApresSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

2020 | 2022 | 2023 | 2024 | 2025

summary

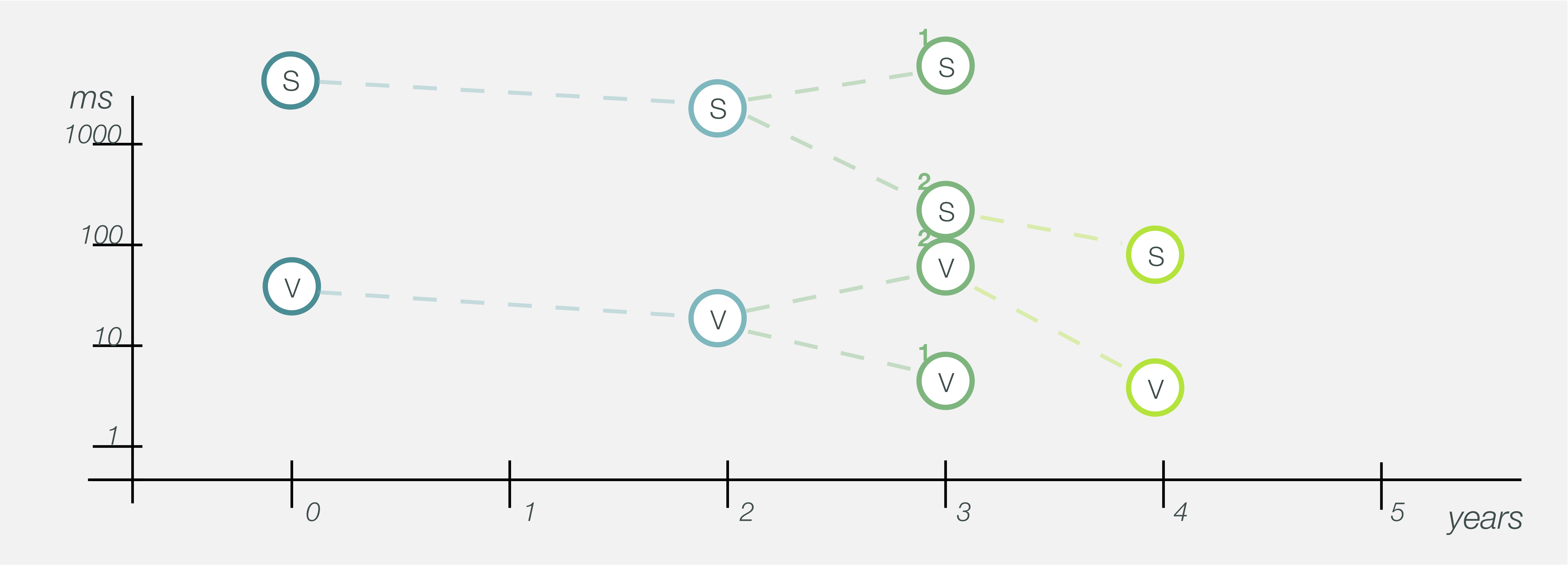
1. **Find Ideal**: HD (easy!)
2. **Id-2-Isog:** Almost trivial
3. **Verify**: SLOW 4D isogeny

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

PART 3

The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

2020 | 2022 | 2023 | 2024 | 2025

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

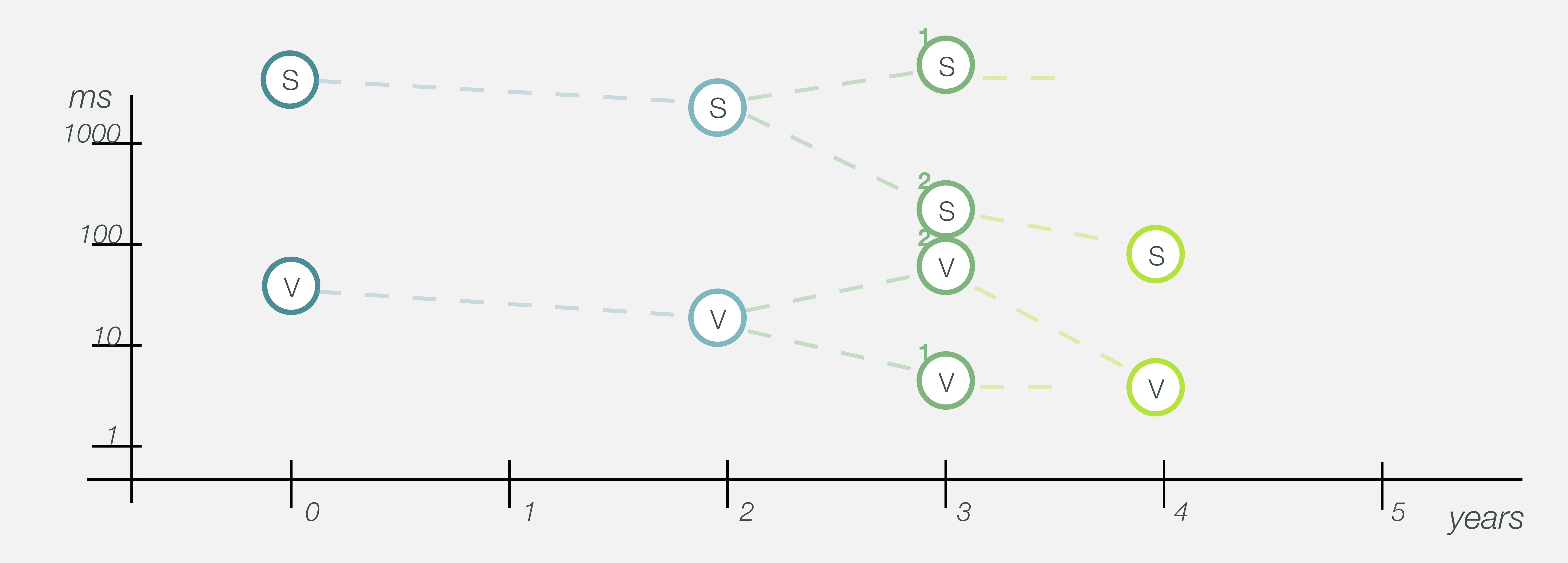
SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

summary

1. **Find Ideal**: HD (easy!)
2. **Id-2-Isog:** A few tricks
3. **Verify**: Fast 2D isogeny

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

What about 1D?
Is there still any use for one-dimensional SQIsign? Should we always do 2D?

2020 | 2022 | 2023 | 2024 | 2025

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

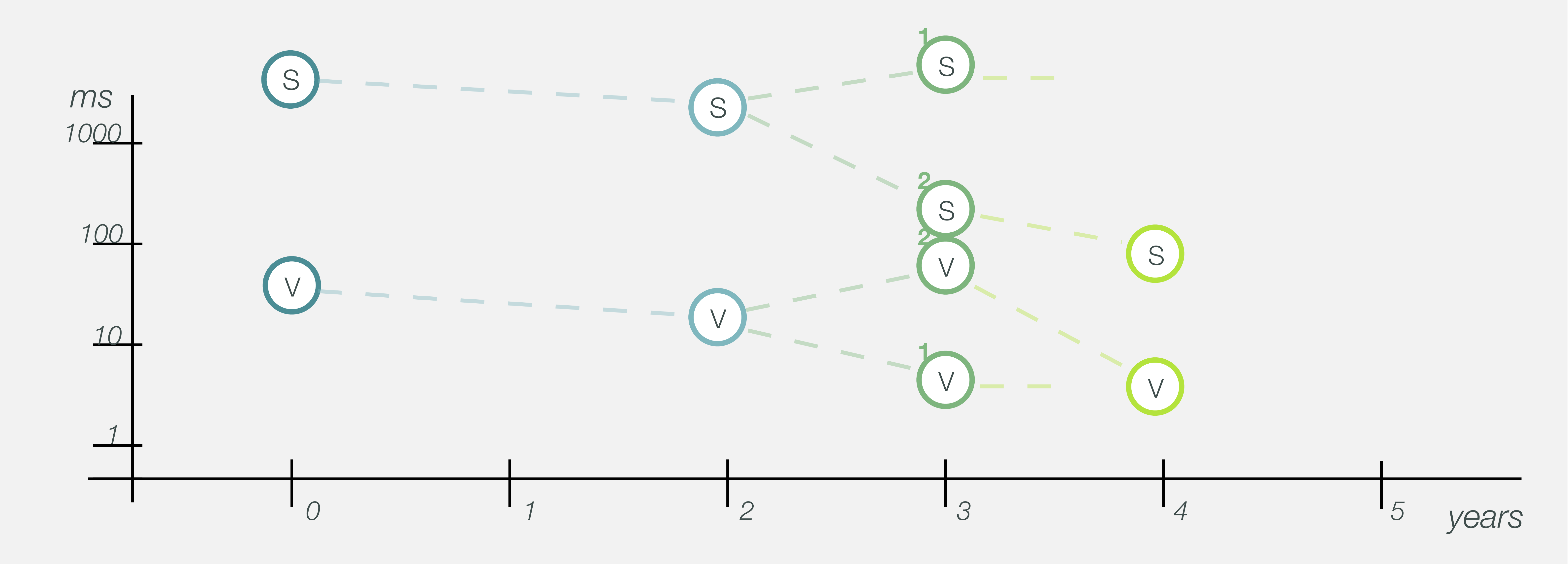
Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

summary

1. **Find Ideal**: HD (easy!)
2. **Id-2-Isog:** A few tricks
3. **Verify**: Fast 2D isogeny


SQIsign2DPush: Faster Signature Scheme Using 2-Dimensional Isogenies
Kohei Nakagawa1 and Hiroshi Onuki2[0000-0002-0202-8918]
1 NTT Social Informatics Laboratories, Japan kohei.nakagawa@ntt.com
2 The University of Tokyo, Japan hiroshi-onuki@g.ecc.u-tokyo.ac.jp
Abstract. Isogeny-based cryptography is cryptographic schemes whose security is based on the hardness of a mathematical problem called the isogeny problem, and is attracting attention as one of the candidates for post-quantum cryptography. A representative isogeny-based cryptography is the signature scheme called SQIsign, which was submitted to the NIST PQC standardization competition for additional signature. SQIsign has attracted much attention because of its very short signature and key size among candidates for the NIST PQC standardization. Recently, many new signature schemes using high-dimensional isogenies have been proposed, such as: SQIsignHD, SQIsign2D-West, SQIsign2D-East, and SQIPrime. Last year, SQIsign advanced to Round 2 of the NIST competition and was updated to version 2.0 (we call it SQIsign-v2.0), which is based on SQIsign2D-West. SQIsign-v2.0 achieves smaller signature sizes and faster verification. However, the signing costs
SQIsign2D²: New SQIsign2
Leveraging Power Smooth Isog
Dimension One
Zheng Xu1, Kaizhan Lin2, Chang-An Zhao2,3, and Yi Ouyang1,4
1 Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
xuzheng1@mail.ustc.edu.cn
yiouyang@ustc.edu.cn
2 School of Mathematics, Sun Yat-sen University, Guangzhou, China
linkzh5@mail2.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn
3 Guangdong Key Laboratory of Information Security, Guangzhou, China
4 School of Mathematical Sciences, Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei 230026, China
Abstract. In this paper, we propose SQIsign2D², a novel digital signature scheme within the SQIsign2D family. Unlike other SQIsign2D variants, SQIsign2D² employs the prime p = CD − 1 as the field characteristic, where D = 2^e2, C = 3^e3 and C ≈ D ≈ √p. By leveraging accessible C-isogenies, SQIsign2D² significantly reduces the degree requirements for two-dimensional isogeny computations, thereby lowering the overall computational overhead compared to other SQIsign2D
SQIPrime: A dim
with non-smooth
Max Duparc and Tako Boris Fouotsa
EPFL, Lausanne, Switzerland
{max.duparc,tako.fouotsa}@epfl.ch
Abstract. We introduce
the Fast, the Small, and the Safer
Andrea Basso1,2[0000-0002-3270-1069], Pierrick Dartois3,4[0009-0008-2808-9867], Luca De Feo2[0000-0002-9321-0773], Antonin Leroux5,6[0009-0002-3737-0075], Luciano Maino1[0009-0005-4495-5102], Giacomo Pope1,7, Damien 3,4[0000-0003-4378-4274], and Benjamin Wesolowski8[0000-0003-1249-6077]
University of Bristol, Bristol, United Kingdom
Zürich, Switzerland
IMB, UMR 5251, F-33400 Talence, France
F-33400, Talence, France

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

What about 1D?
Is there still any use for one-dimensional SQIsign? Should we always do 2D?

The BOOM
Everybody makes their own version of SQIsign? What is SQIsign?

2020 — 2022 — 2023 — 2024 — 2025

summary

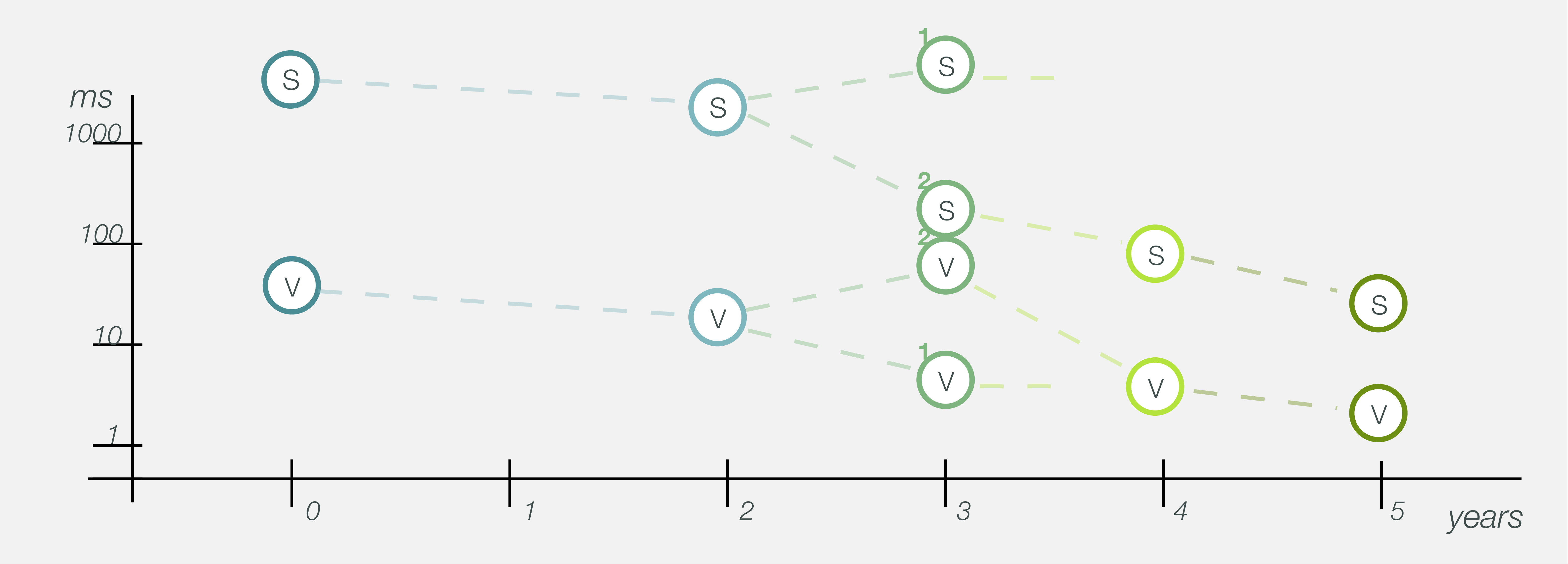
1. **Find Ideal**: HD (easy!)
2. **Id-2-Isog:** A few tricks
3. **Verify**: Fast 2D isogeny

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

What about 1D?
Is there still any use for one-dimensional SQIsign? Should we always do 2D?

The BOOM
Everybody makes their own version of SQIsign? What is SQIsign?

2020 | 2022 | 2023 | 2024 | 2025

summary

1. **Find Ideal**: Easy maths!
2. **Id-2-Isog:** Fewer tricks!!
3. **Verify**: Fast 2D isogeny

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

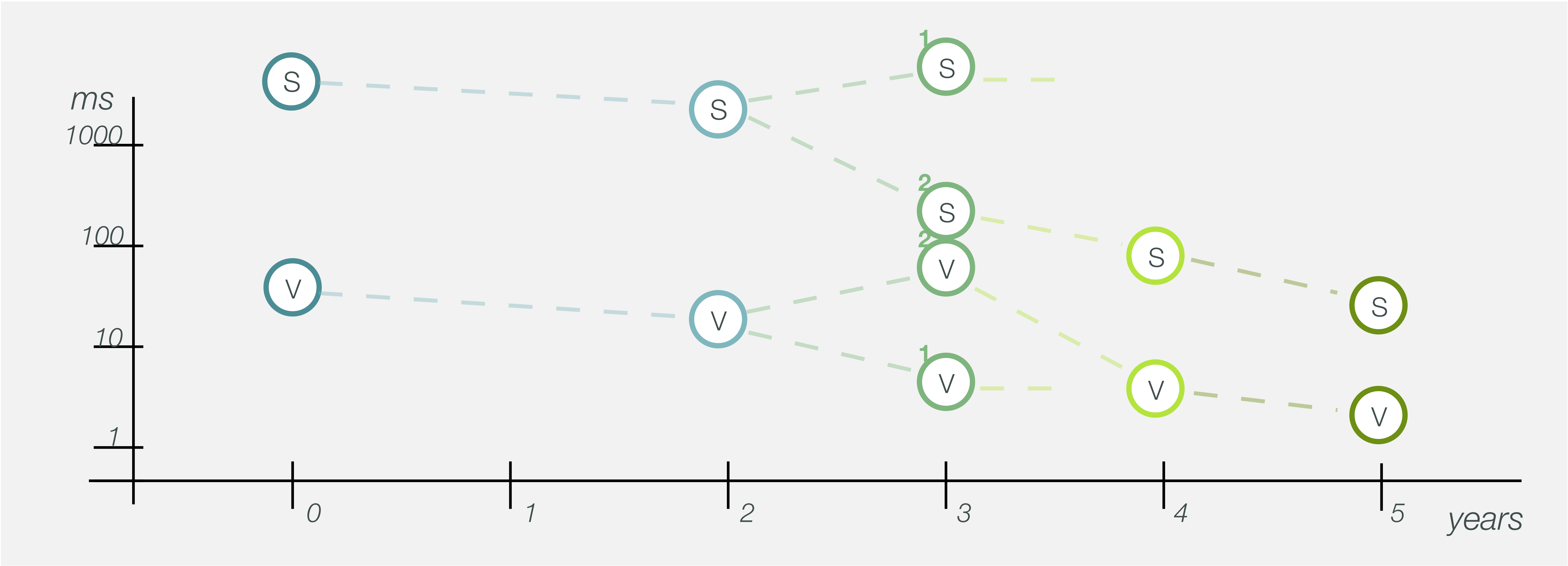
SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

Clean Solving
A cleaner solution to a key technical issue makes signing much easier!

PART 3

The Variants



2020

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2022

SQIsign2

A new algorithm to translate ideals to isogenies.

SIKE breaks

SIKE was destroyed using **HD isogenies** in the summer of 2022.

2023

AprèsSQI

Signing is slow anyway… Push verification to **maximal** efficiency!

SQIsignHD

Represent the response as **HD isogeny**. Requires 4/8-dimensions.

2024

What about 1D?

Is there still any use for one-dimensional SQIsign? Should we always do 2D?

Going 2D

Adapt SQIsignHD to enable verification with **2D isogenies**

2025

The BOOM

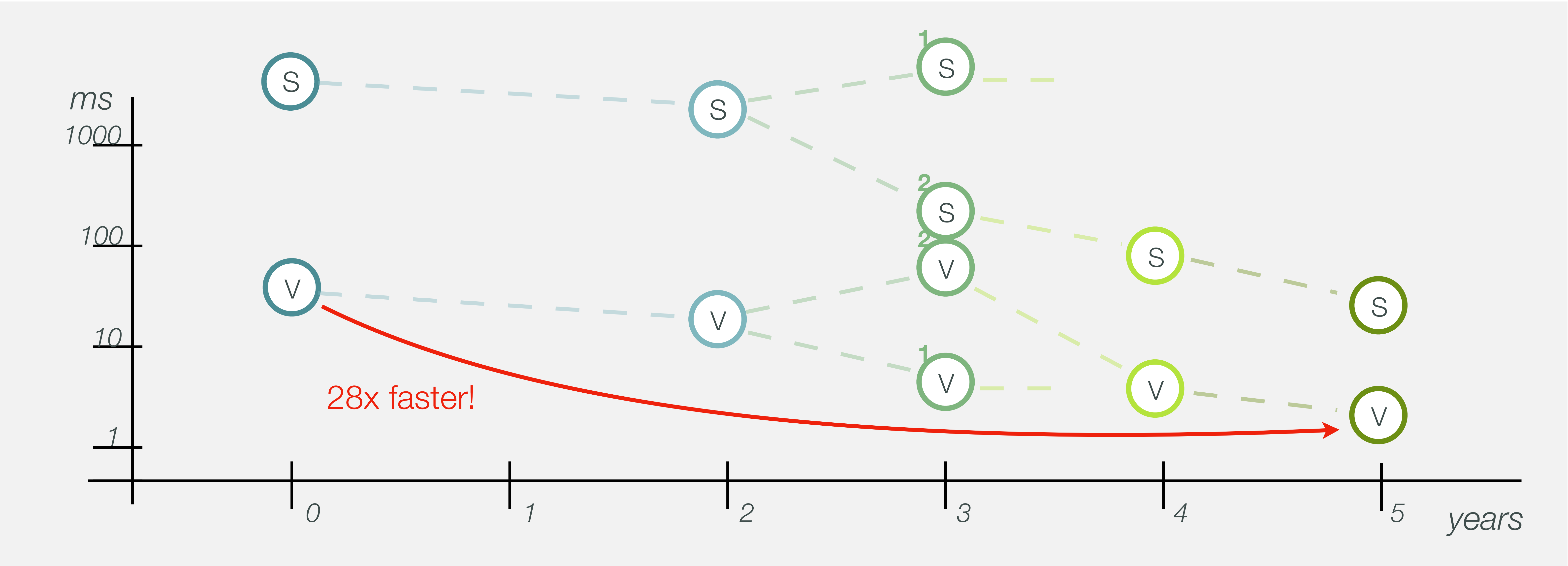
Everybody makes their own version of SQIsign? What is SQIsign?

Clean Solving

A cleaner solution to a key technical issue makes signing much easier!

KU LEUVEN

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

What about 1D?
Is there still any use for one-dimensional SQIsign? Should we always do 2D?

The BOOM
Everybody makes their own version of SQIsign? What is SQIsign?

2020 | **2022** | **2023** | **2024** | **2025**

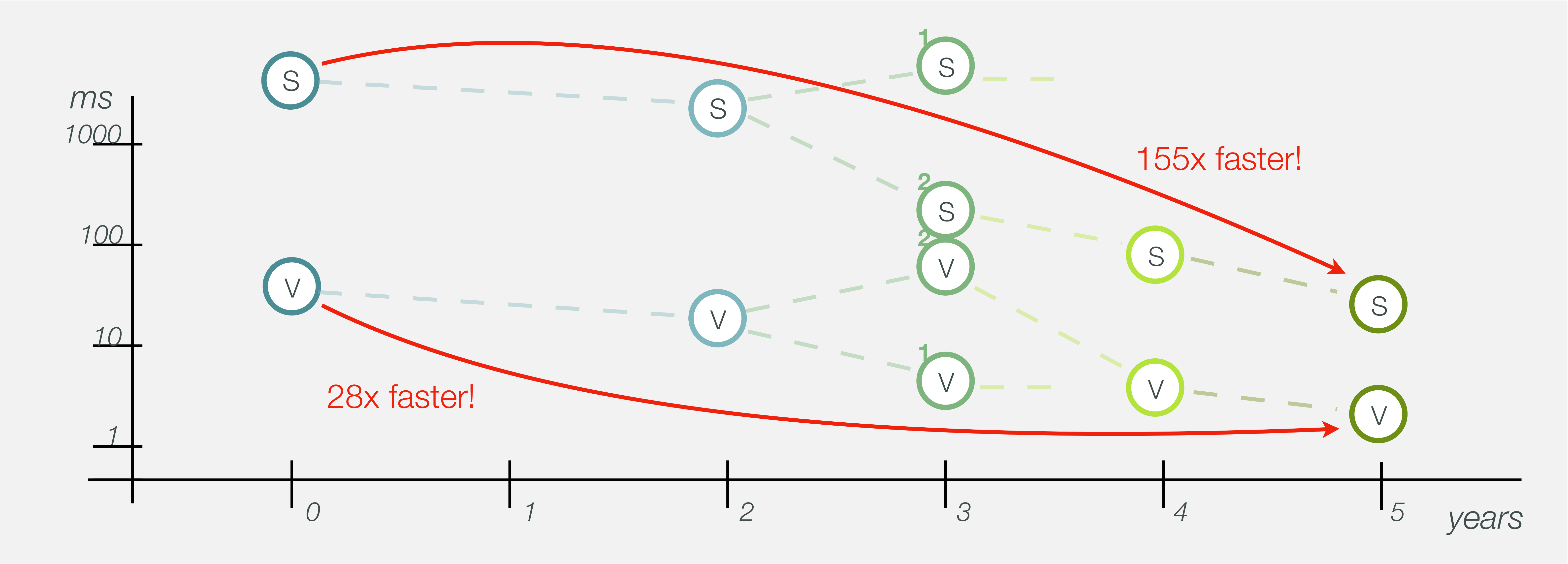
SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

Clean Solving
A cleaner solution to a key technical issue makes signing much easier!

PART 3
The Variants



SQIsign
A new isogeny-based signature scheme, with **high soundness.**

SQIsign2
A new algorithm to translate ideals to isogenies.

AprèsSQI
Signing is slow anyway… Push verification to **maximal** efficiency!

What about 1D?
Is there still any use for one-dimensional SQIsign? Should we always do 2D?

The BOOM
Everybody makes their own version of SQIsign? What is SQIsign?

2020 — **2022** — **2023** — **2024** — **2025**

SIKE breaks
SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD
Represent the response as **HD isogeny**. Requires 4/8-dimensions.

Going 2D
Adapt SQIsignHD to enable verification with **2D isogenies**

Clean Solving
A cleaner solution to a key technical issue makes signing much easier!

KU LEUVEN