SQIsign verification in higher dimensions

Maria Corte-Real Santos
www.mariascrs.com
University College London

Based on joint work with Krijn Reijnders

Séminaire de Théorie Algorithmique des Nombres
Institut de Mathématiques de Bordeaux

SQIsign

SQIsign is an isogeny-based signature scheme in Round 1 of NIST's alternate call for signature schemes.

- ✔ Small signature and public key size
- ✔ (Relatively) fast verification
- ✘ Slow and complicated signing

New variants [*SQIsign2D-West/East, SQIPrime*] have showed that SQIsign verification can be done with (2,2)-isogenies between products of elliptic curves.

We will show that original SQIsign can also be viewed in this way.

A primer on isogeny-based cryptography

Let $\varphi : E_1 \to E_2$ be a (separable) isogeny between elliptic curves E_1, E_2 over $\bar{\mathbb{F}}_p$.

The **degree** $\deg \varphi$ of the isogeny is the size of the kernel.

A primer on isogeny-based cryptography

Let $\varphi : E_1 \to E_2$ be a (separable) isogeny between elliptic curves E_1, E_2 over $\bar{\mathbb{F}}_p$.

The **degree** $\deg \varphi$ of the isogeny is the size of the kernel.

For ℓ prime, we can compute an ℓ-isogeny from its kernel using Vélu's formulae in $O(\ell)$ or in $\tilde{O}(\sqrt{\ell})$ using $\sqrt{\text{élu}}$.

To compute an isogeny of degree ℓ^k, we compute k isogenies of degree ℓ

$$\underbrace{\varphi}_{\text{degree } \ell^k} = \underbrace{\varphi_k}_{\text{degree } \ell} \circ \cdots \circ \underbrace{\varphi_1}_{\text{degree } \ell}$$

A primer on isogeny-based cryptography

Let $\varphi : E_1 \to E_2$ be a (separable) isogeny between elliptic curves E_1, E_2 over $\bar{\mathbb{F}}_p$.

The **degree** $\deg \varphi$ of the isogeny is the size of the kernel.

For ℓ prime, we can compute an ℓ-isogeny from its kernel using Vélu's formulae in $O(\ell)$ or in $\tilde{O}(\sqrt{\ell})$ using $\sqrt{\text{élu}}$.

To compute an isogeny of degree ℓ^k, we compute k isogenies of degree ℓ

$$\varphi = \varphi_k \circ \cdots \circ \varphi_1$$

degree ℓ^k degree ℓ

We work with supersingular E so it's (isomorphic to a model) defined over $\mathbb{F}_{p^2}$.

We can enforce $\ell \mid \#E(\mathbb{F}_{p^2})$ so that we have $\mathbb{F}_{p^2}$-rational ℓ-isogenies

The isogeny problem

Given supersingular E_1, E_2 defined over $\mathbb{F}_{p^2}$ compute the isogeny

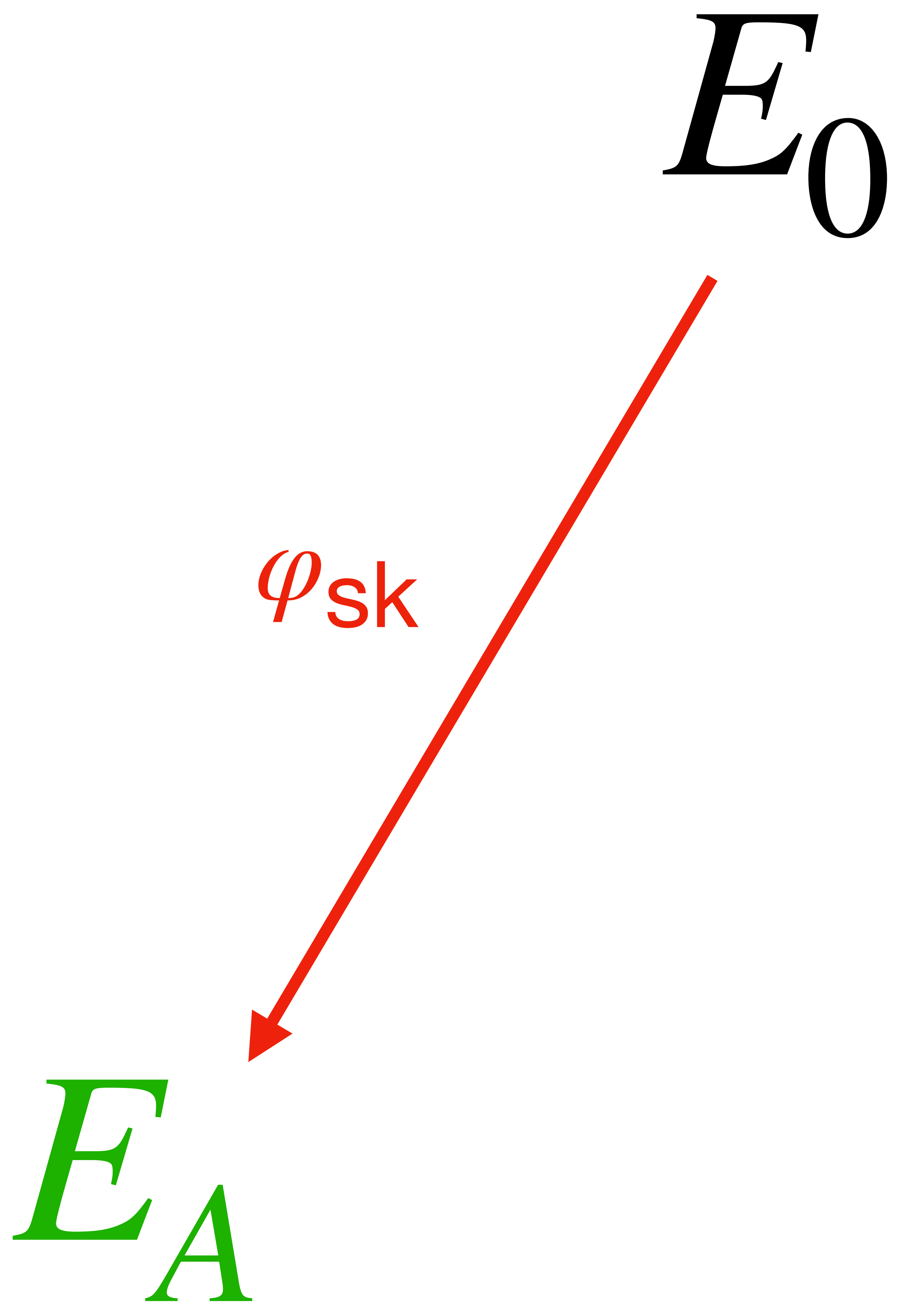
$$\varphi : E_1 \to E_2$$

The best classical attack: Delfs—Galbraith runs in $\tilde{O}(p^{1/2})$

The best quantum attack: Biasse—Jao—Sankar runs in $\tilde{O}(p^{1/4})$

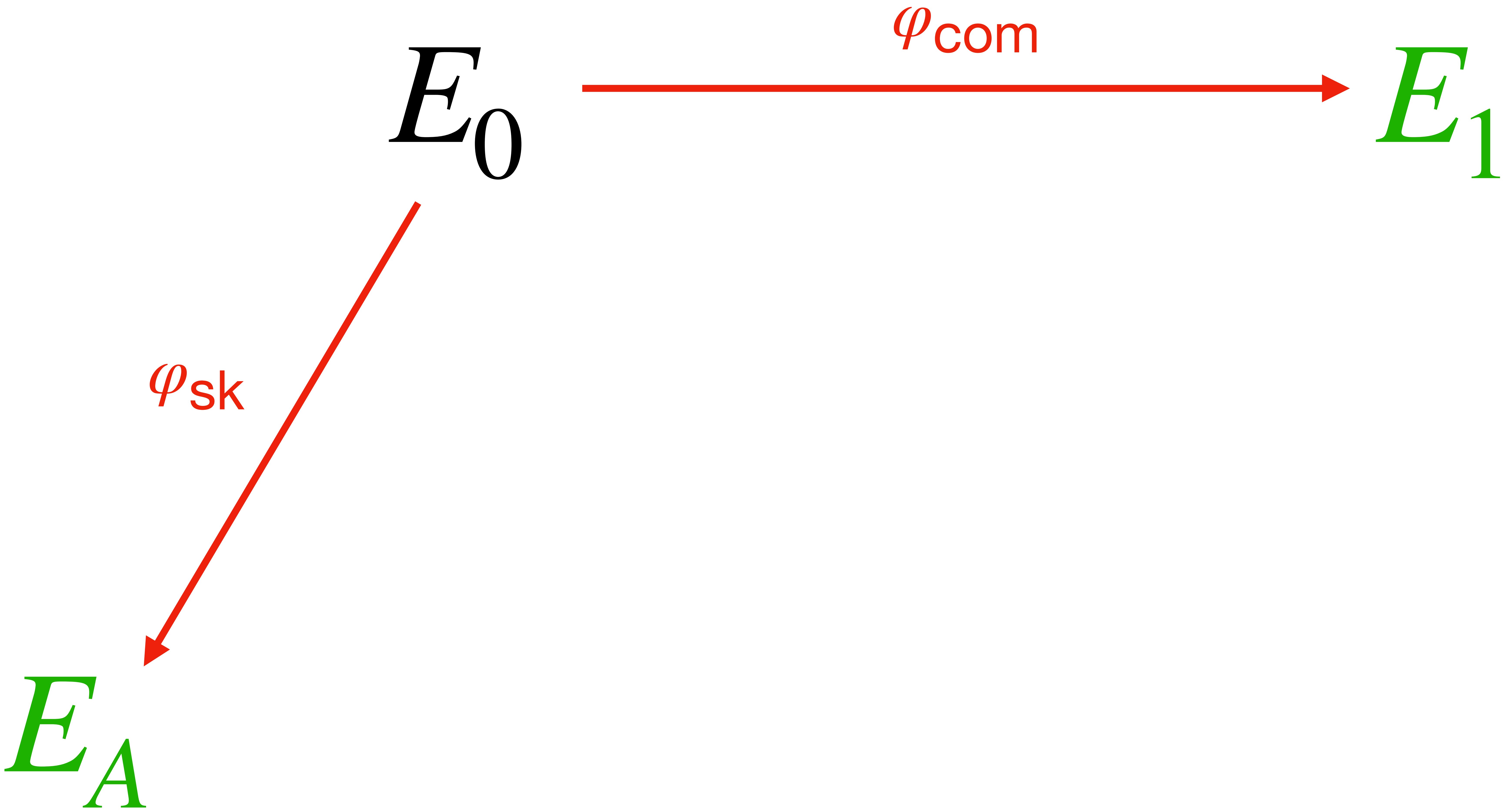
SQIsign

Key Generation



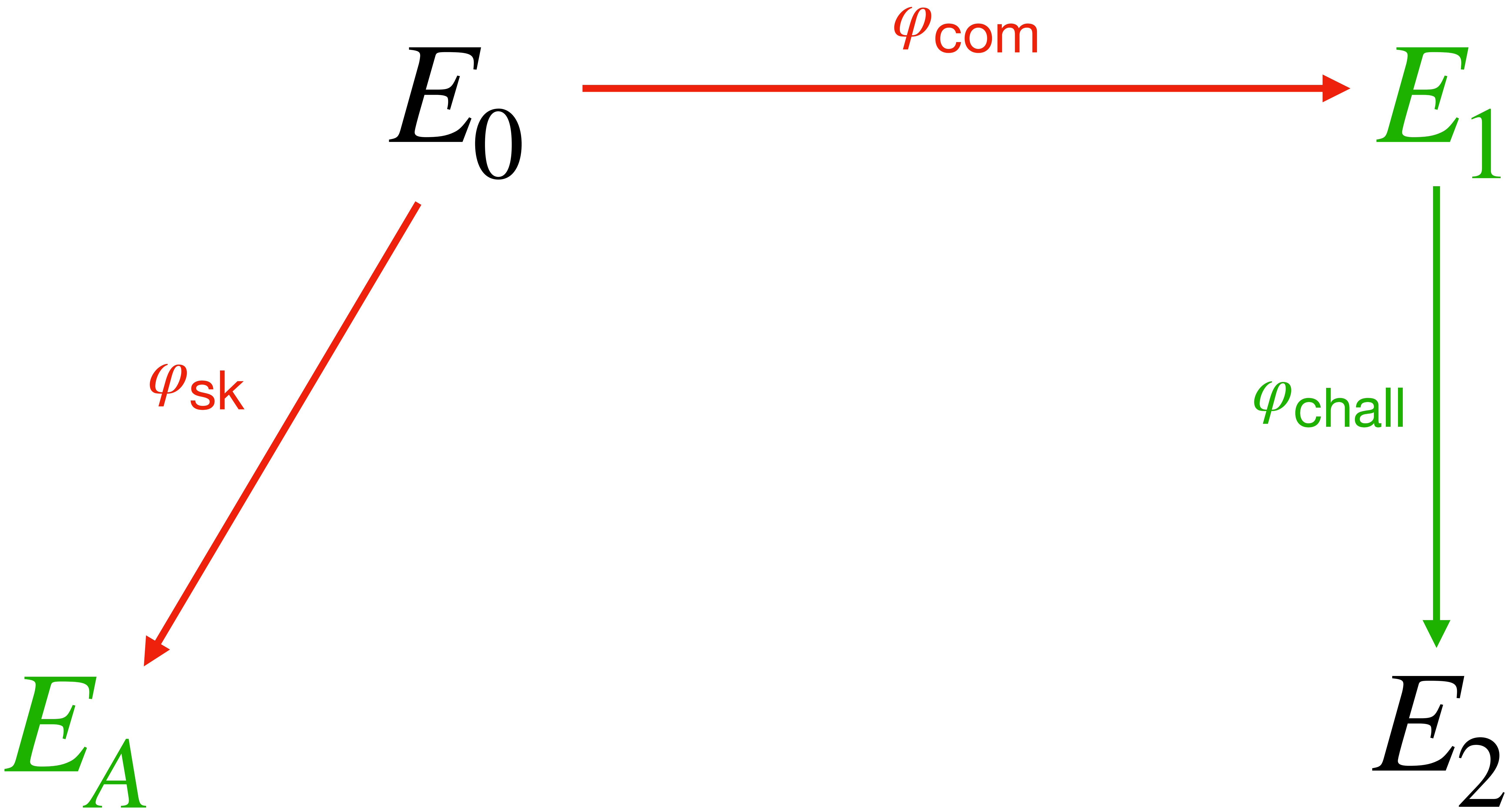
SQIsign

Commitment



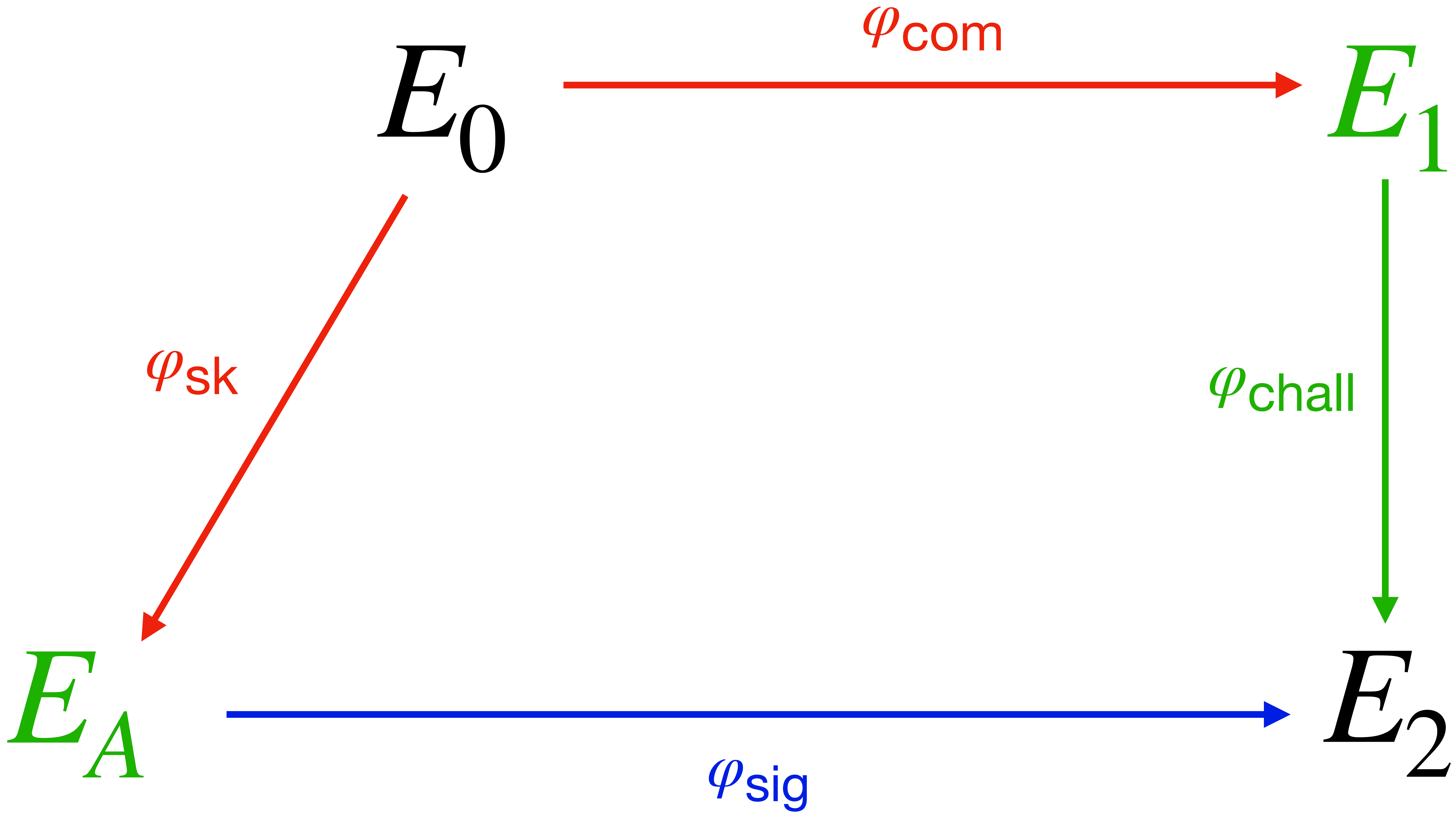
SQIsign

Challenge



SQIsign

Response



A deeper look at the response isogeny

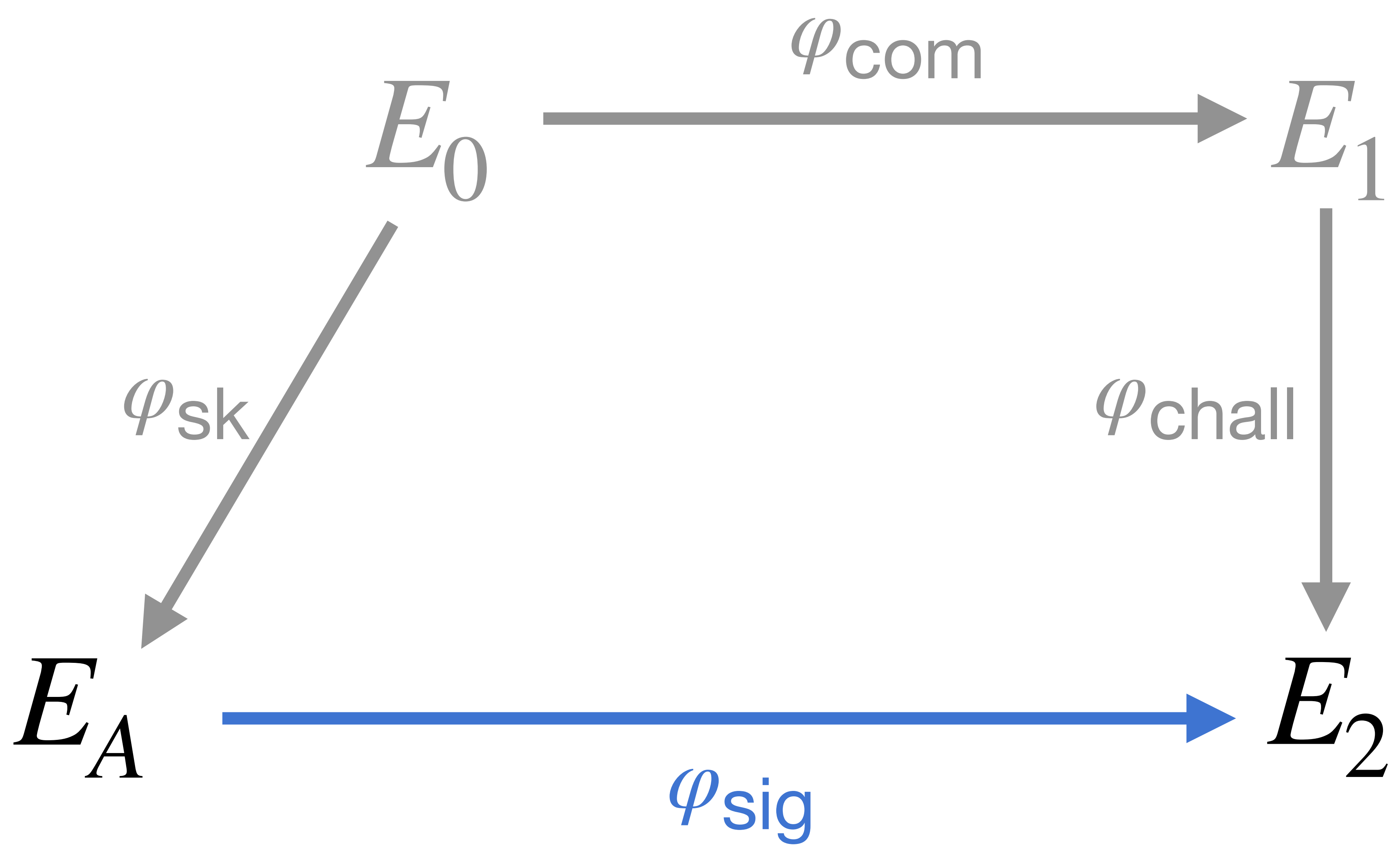
- Naive response:

  $$\varphi_{\text{chall}} \circ \varphi_{\text{com}} \circ \widehat{\varphi_{\text{sk}}}$$

  Completely leaks the secret isogeny!

- Instead we find an *equivalent isogeny* φ_{sig} using the *KLPT algorithm*.

- The isogeny output by this algorithm has degree 2^e



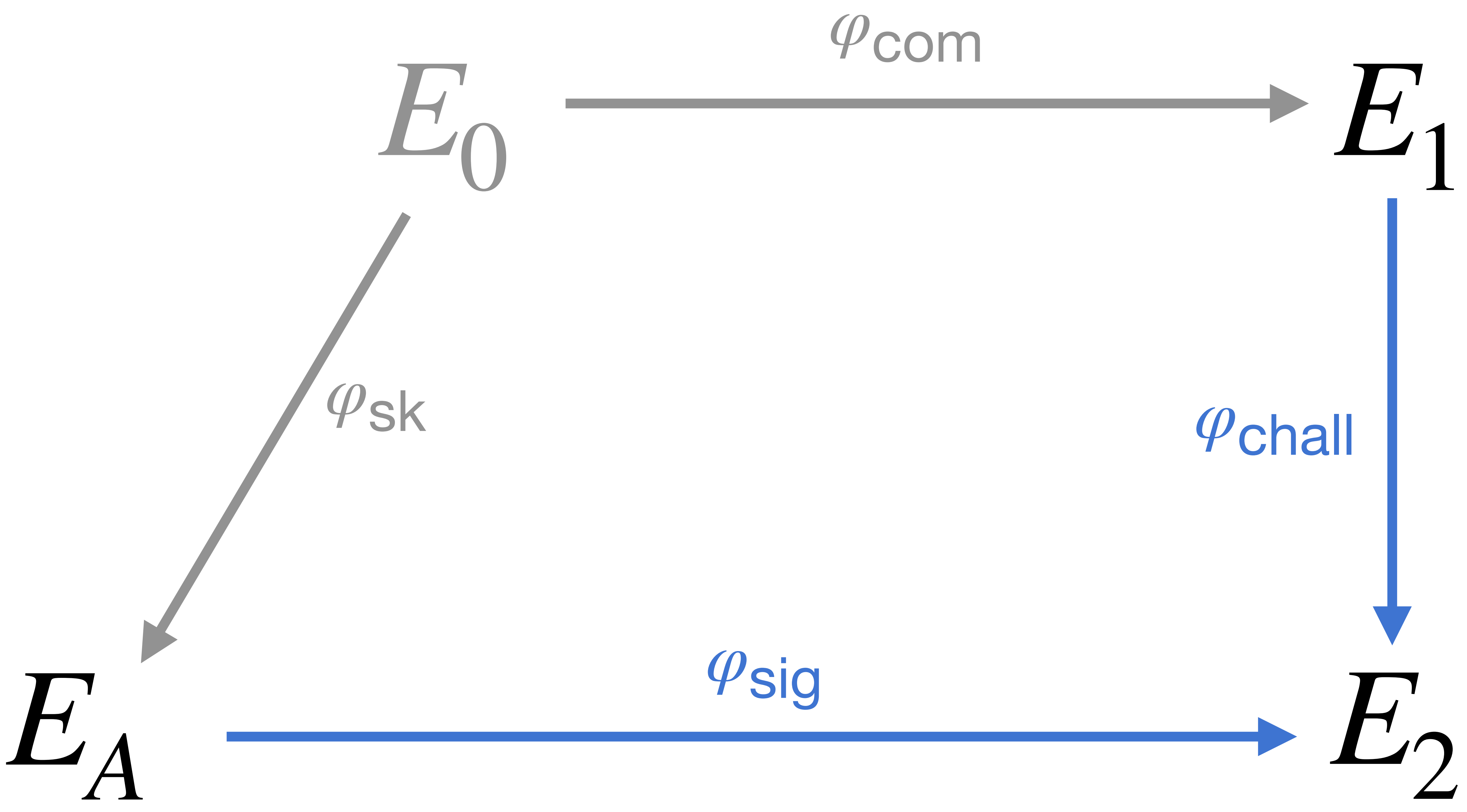
NIST-I prime has 2^{75} rational torsion and $e = 975$, and so we perform the response isogeny in 13 steps

SQIsign: verification

Uncompressed Signatures

- φ_{sig} is given as a list of kernel generators

$$K_1, K_2, \ldots, K_{13}$$



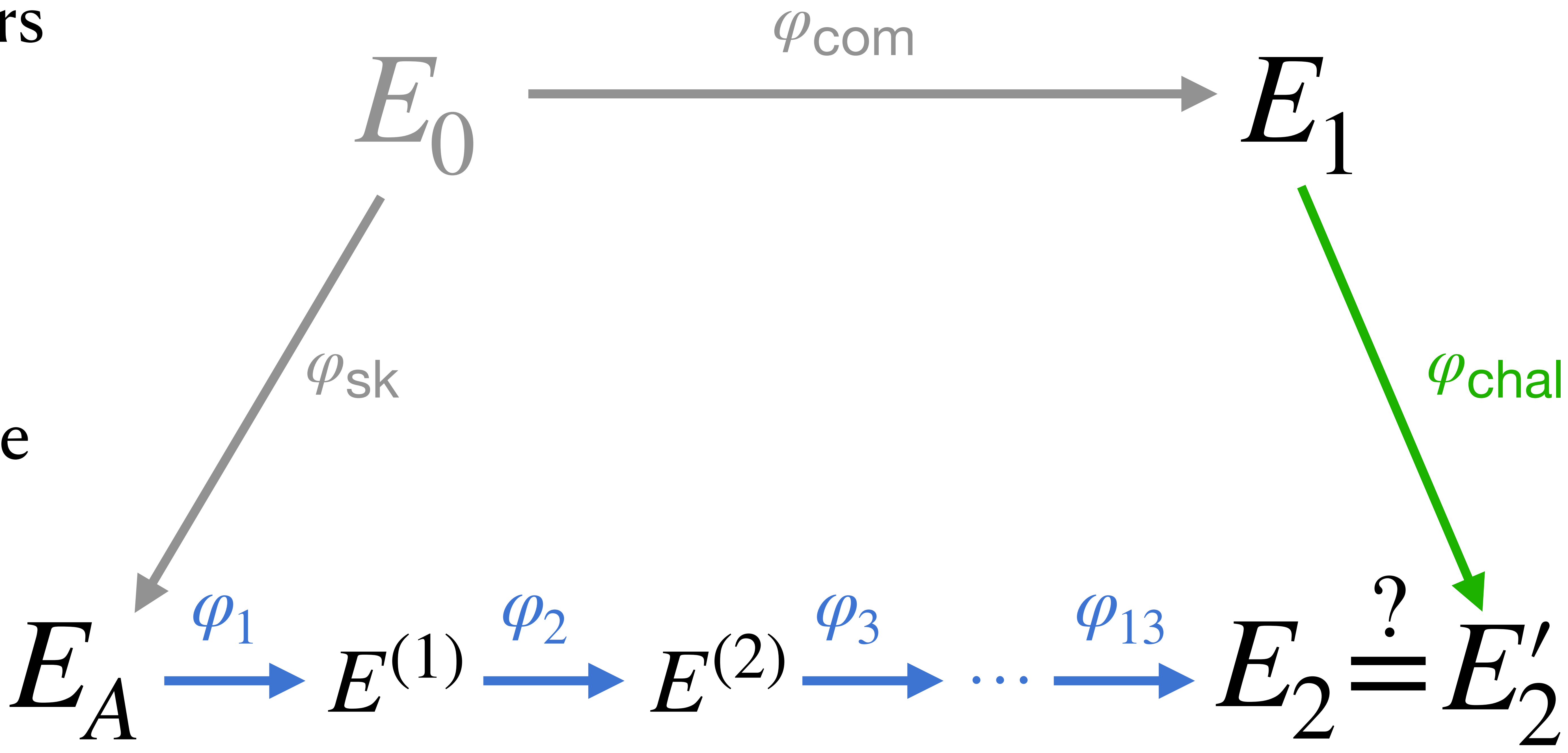
SQIsign verification in detail

Uncompressed Signatures

- φ_{sig} is given as a list of kernel generators

$$K_1, K_2, \ldots, K_{13}$$

- $K_{\text{chall}} = H(E_1 \,||\, m)$ generates challenge isogeny



SQIsign verification in detail

Compressed Signatures

- φ_{sig} is given as a list of scalars

$$s_1, s_2, \ldots, s_{13} \in \mathbb{Z}/2^{75}\mathbb{Z}$$

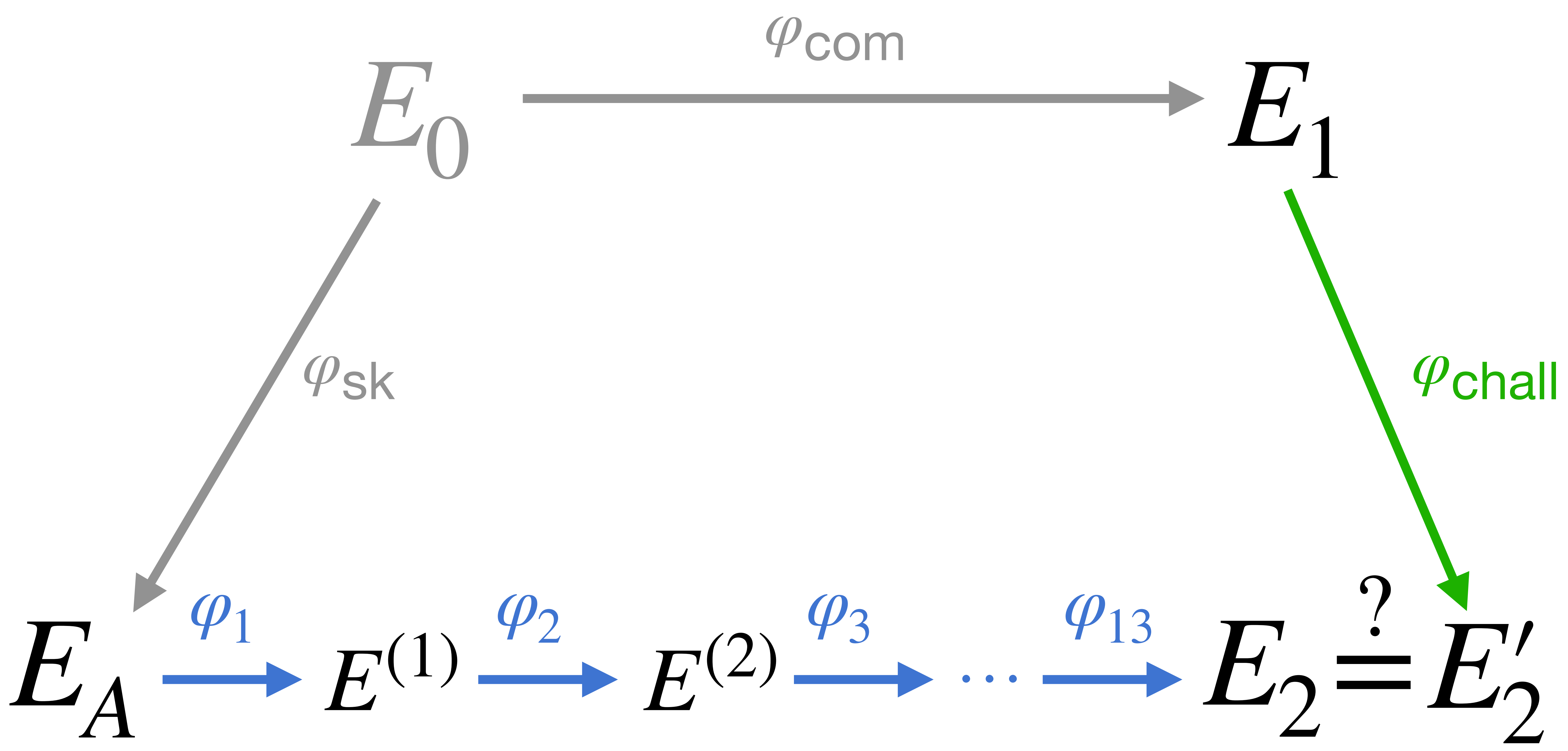
At each step i:

1) Deterministically sample a basis

$$\langle P_i, Q_i \rangle = E^{(i-1)}[2^{75}]$$

2) Obtain the kernel generator as

$$K_i = P_i + s_i Q_i$$



We can also compress E_1 needed for the challenge.

Moving to dimension 2

Abelian surfaces

There are two types of (principally polarised) abelian varieties of dimension 2:

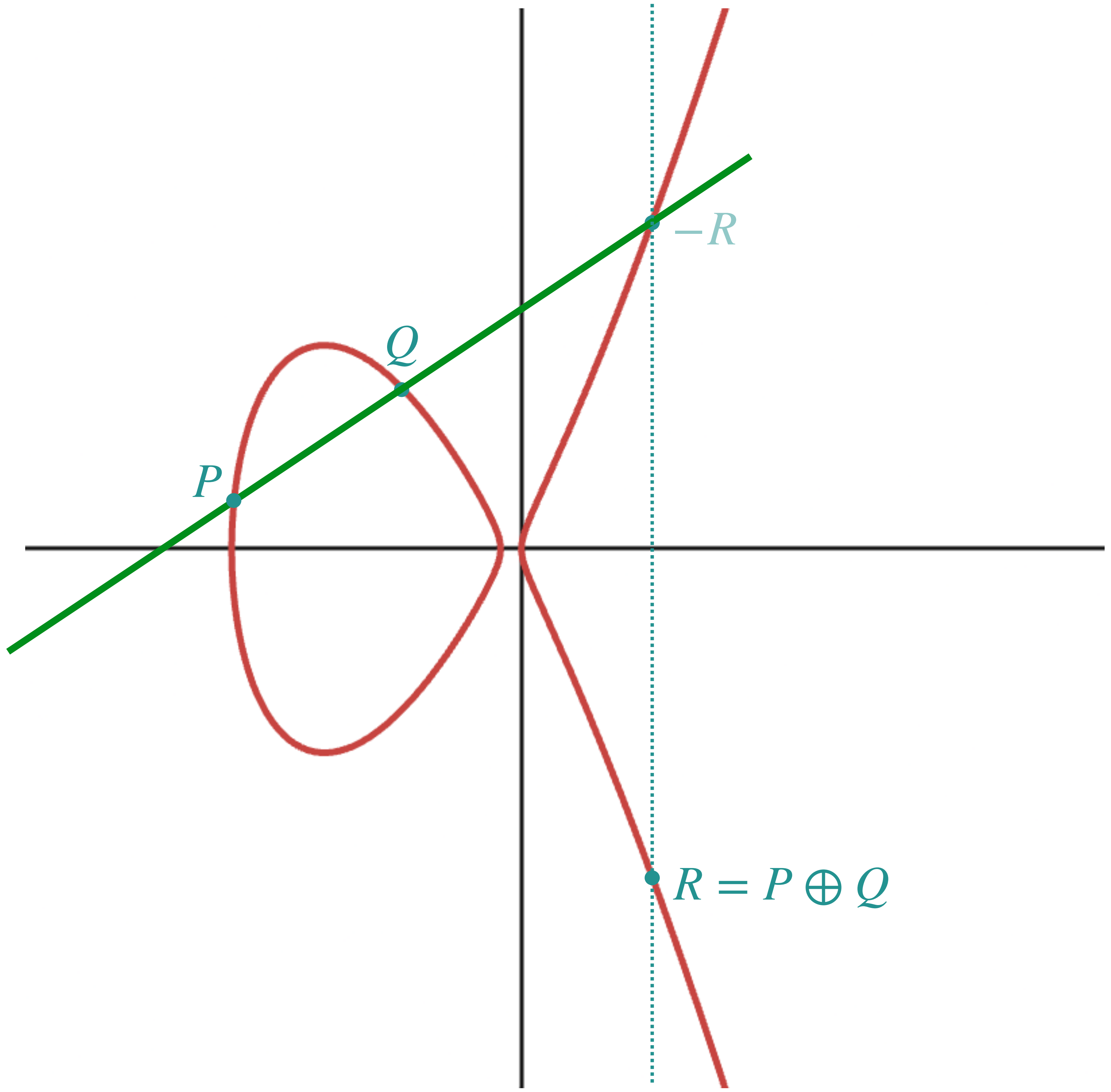
- Jacobians of hyperelliptic curves $\mathcal{J}_C$
- Products of elliptic curves $E_1 \times E_2$

Superspecial abelian surfaces are (isomorphic to a model) defined over $\mathbb{F}_{p^2}$

Hyperelliptic curves

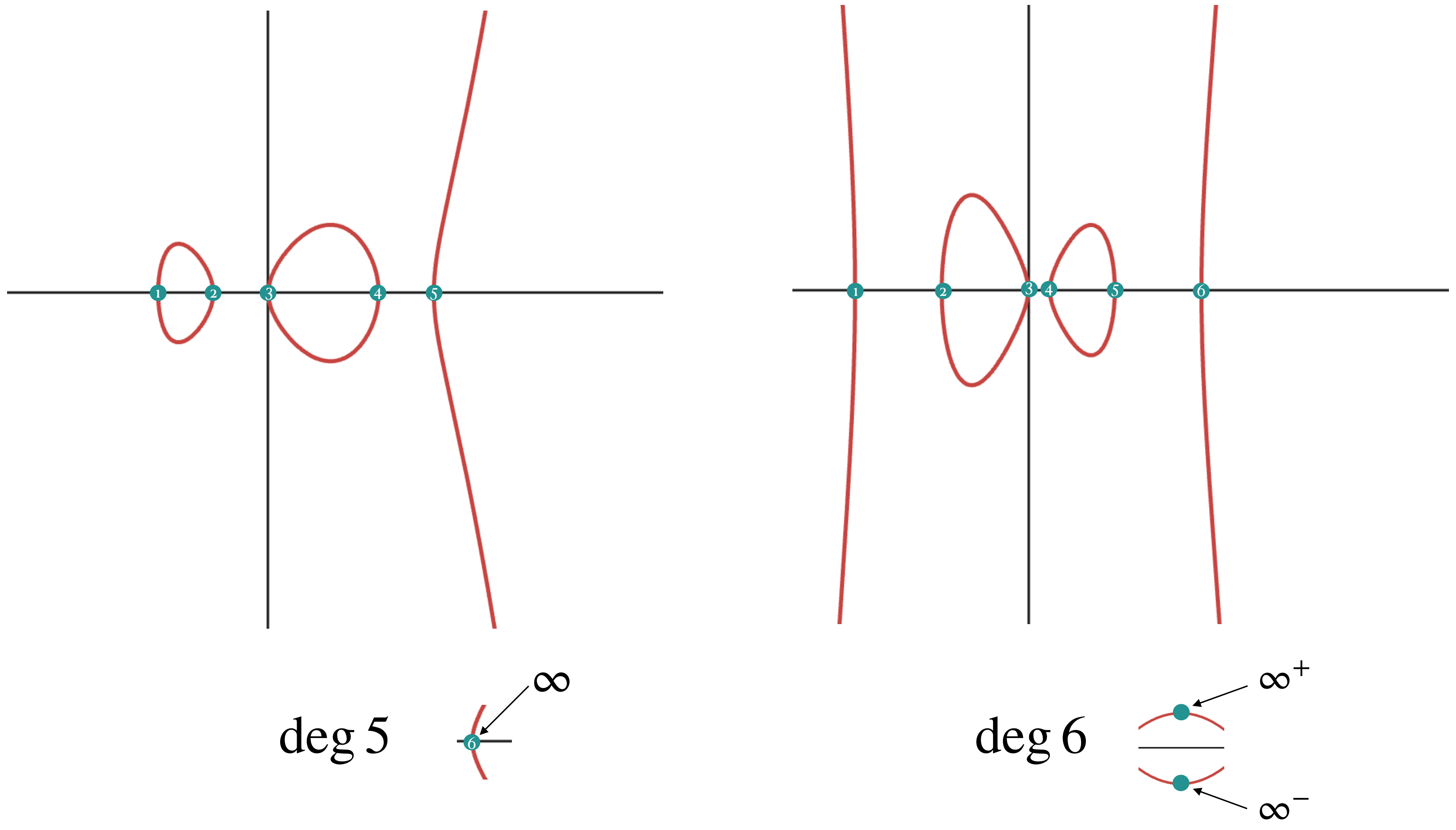
Elliptic Curves

$$E\colon y^2 = x^3 + Ax + B$$



Genus-2 Hyperelliptic Curve

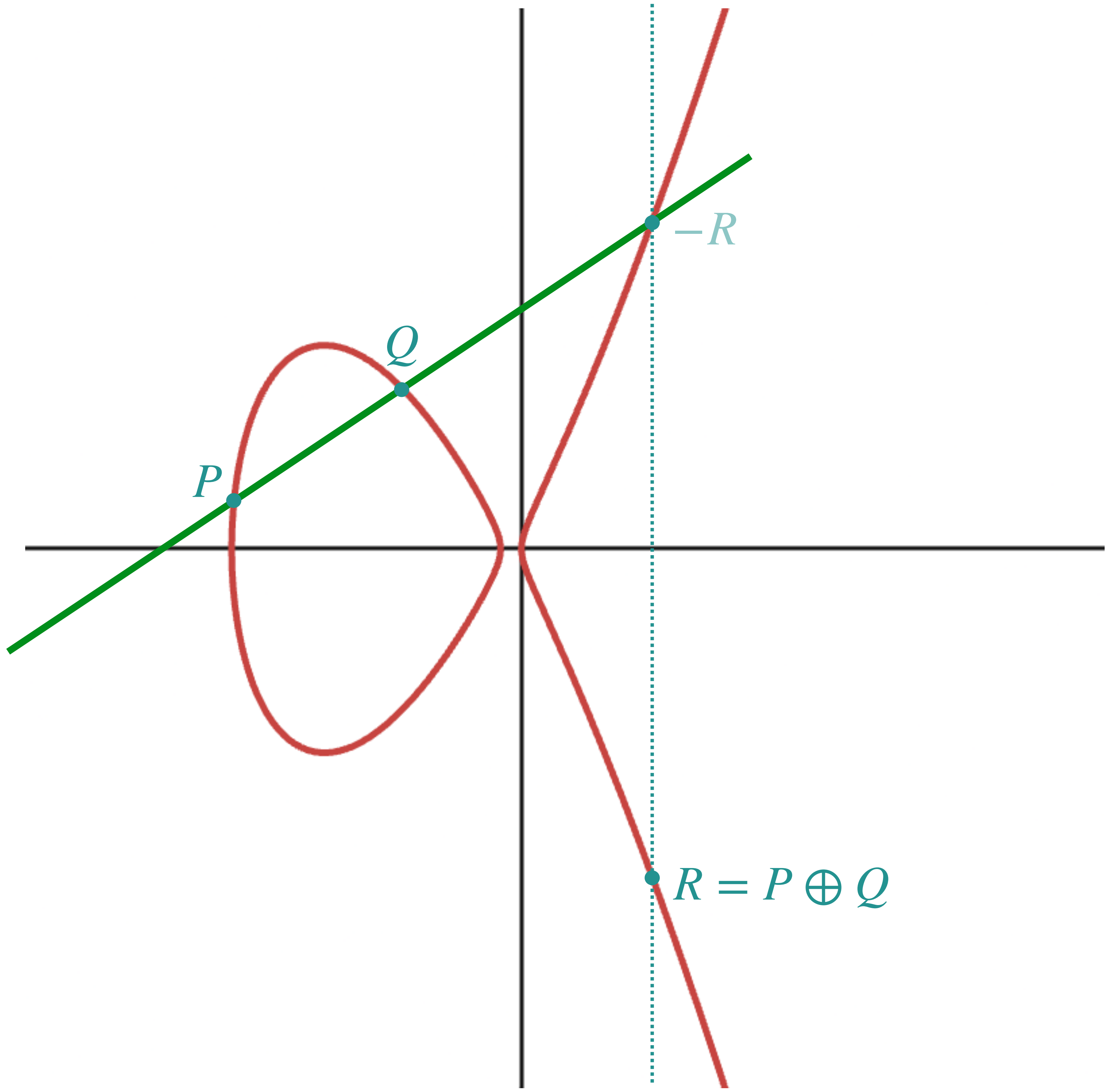
$$C\colon y^2 = f(x), \quad \deg(f) = 5 \text{ or } 6$$



Hyperelliptic curves

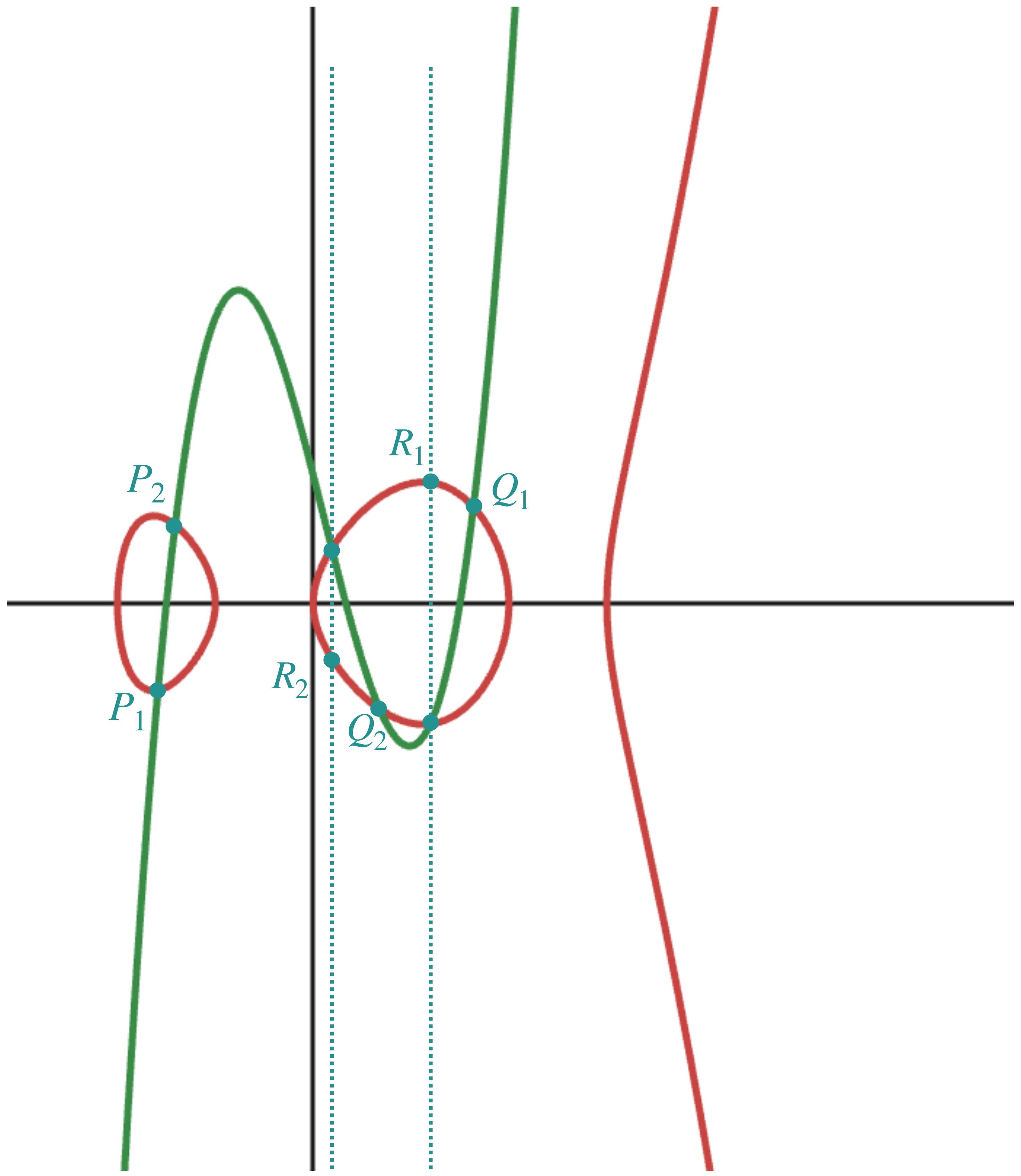
Elliptic Curves

$$E\colon y^2 = x^3 + Ax + B$$



Genus-2 Hyperelliptic Curve

$$C\colon y^2 = f(x), \quad \deg(f) = 5 \text{ or } 6$$



Jacobians and Divisors

Mumford Representation

Let $\mathscr{J}_C$ be the Jacobian of the genus 2 curve C.

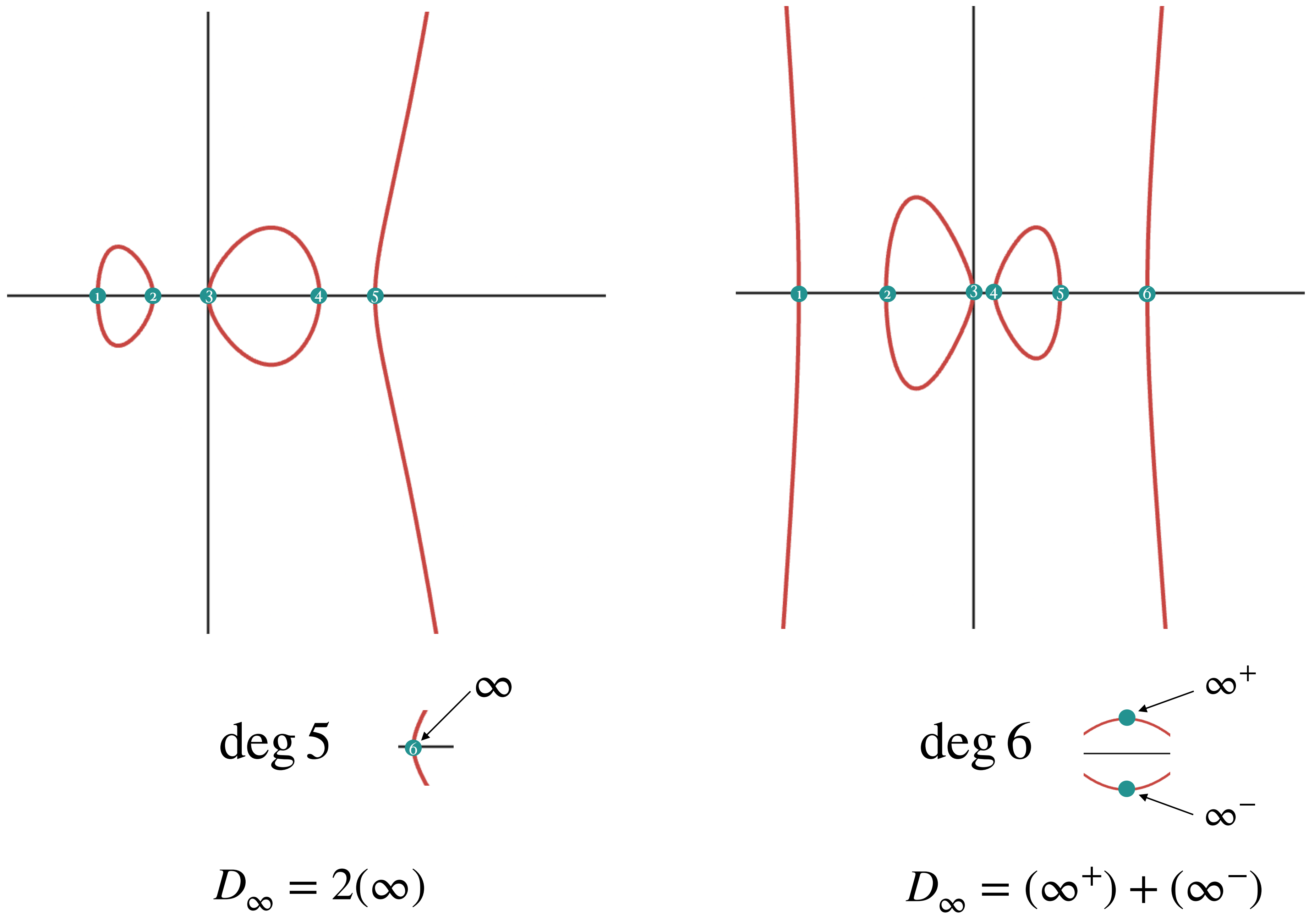
We will represent an element of the Jacobian

$$D_P = (P_1) + (P_2) - D_\infty \in J_C \qquad \begin{aligned} P_1 &= (x_1, y_1) \\ P_2 &= (x_2, y_2) \end{aligned}$$

using the *Mumford representation* $\langle a(x), b(x) \rangle$

$$a(x) = (x - x_1)(x - x_2), \quad b(x_i) = y_i$$

with $D_\infty = \langle 1{,}0 \rangle$.



Jacobians and Divisors

Mumford Representation

Let $\mathcal{J}_C$ be the Jacobian of the genus 2 curve C.

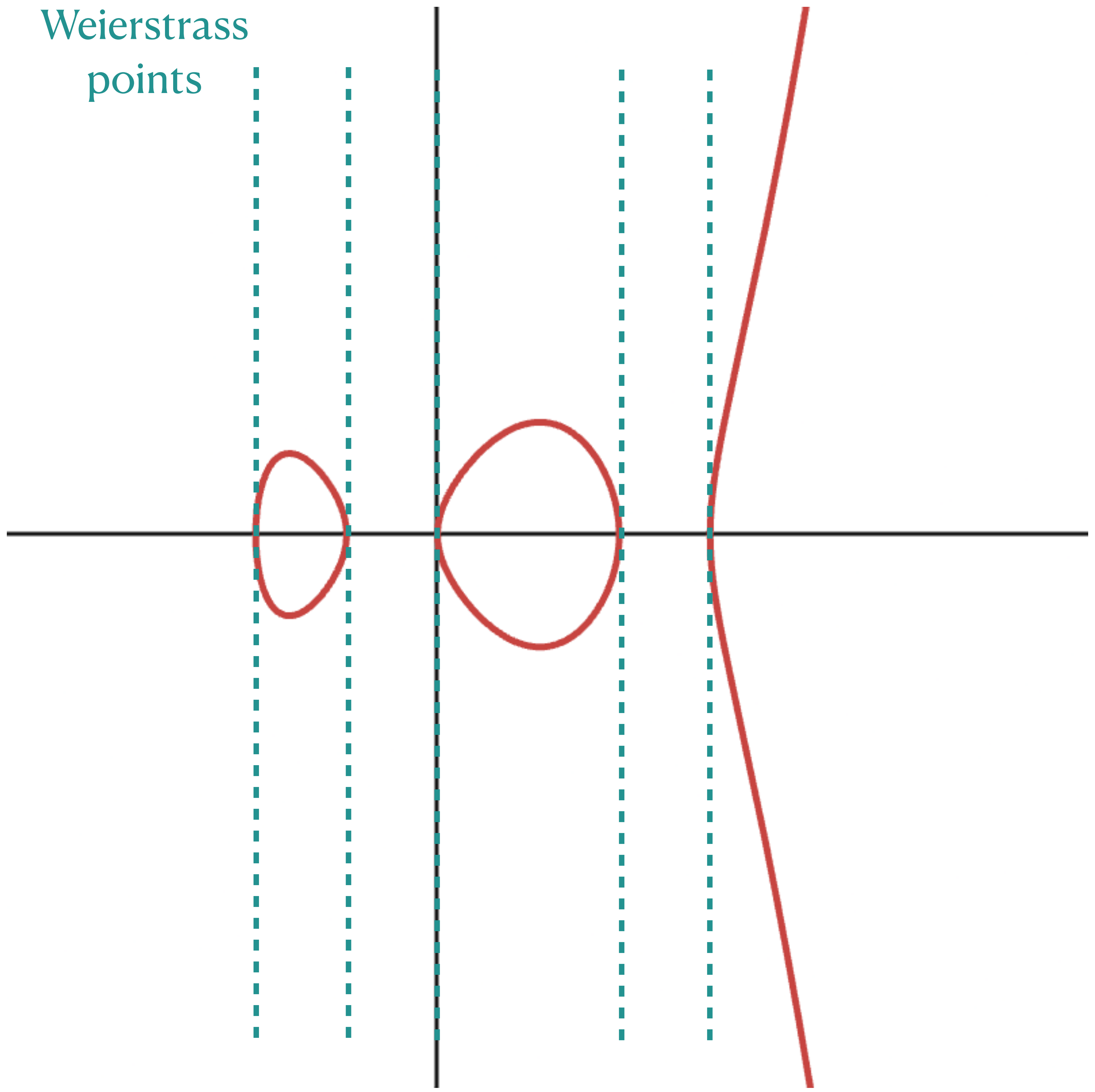
We will represent an element of the Jacobian

$$D_P = (P_1) + (P_2) - D_\infty \in J_C \qquad \begin{aligned} P_1 &= (x_1, y_1) \\ P_2 &= (x_2, y_2) \end{aligned}$$

using the *Mumford representation* $\langle a(x), b(x) \rangle$

$$a(x) = (x - x_1)(x - x_2), \quad b(x_i) = y_i$$

with $D_\infty = \langle 1,0 \rangle$.



Example: two-torsion points

Pairs of *Weierstrass* points $(w_i,0), (w_j,0)$ → $D = \langle (x - w_i)(x - w_j), 0 \rangle$

Abelian surfaces

There are two types of (principally polarised) abelian varieties of dimension 2:

- Jacobians of hyperelliptic curves $\mathcal{J}_C$
- Products of elliptic curves $E_1 \times E_2$

Superspecial abelian surfaces are (isomorphic to a model) defined over $\mathbb{F}_{p^2}$

Let $\phi : \mathscr{A}_1 \to \mathscr{A}_2$ be a homomorphism between abelian surfaces. We say that ϕ is an **isogeny** if it is surjective and has finite kernel.

Three types of isogenies:

$E_1 \times E_2 \to \mathcal{J}_C$	$\mathcal{J}_C \to \mathcal{J}_{C'}$	$\mathcal{J}_C \to E_1 \times E_2$
Glue		Split

Abelian surfaces

There are two types of (principally polarised) abelian varieties of dimension 2:

- Jacobians of hyperelliptic curves $\mathcal{J}_C$
- Products of elliptic curves $E_1 \times E_2$

Superspecial abelian surfaces are (isomorphic to a model) defined over $\mathbb{F}_{p^2}$

Let $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ be a homomorphism between abelian surfaces. We say that ϕ is an **isogeny** if it is surjective and has finite kernel.

We consider (2,2)-isogenies. The kernel G is generated by $R, S \in \mathcal{J}_1[2]$ such that $e_2(R, S) = 1$.

Rosenhain Curves

Elliptic Curves

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

If we have rational 2-torsion on E $\cong$

Montgomery Form

$$E_\alpha: y^2 = x(x - \alpha)(x - 1/\alpha)$$

Genus-2 Hyperelliptic Curve

$$C: y^2 = f(x), \quad \deg(f) = 5 \text{ or } 6$$

If we have rational Weierstrass points on C $\cong$

Rosenhain Form

$$C_{\lambda,\mu,\nu}: y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

For our cryptographic applications, we work with *superspecial* Jacobians, and so we can enforce full rational 2-torsion.

Kummer surfaces

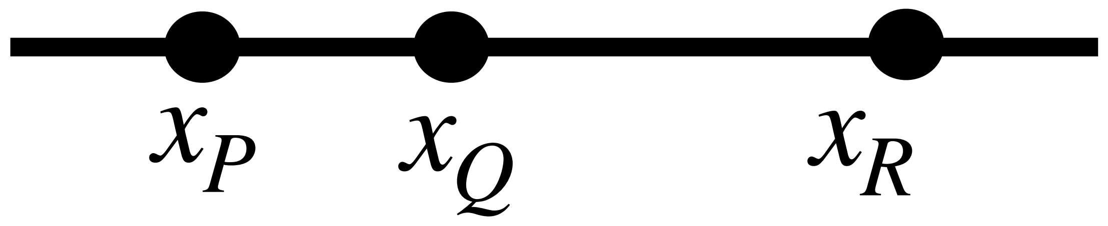
Kummer Line

"fast x-only arithmetic"

$$\mathcal{K}_E = E/\langle \pm 1 \rangle$$

$$\mathcal{K}_E \cong \mathbb{P}^1$$

1 coordinate



Kummer surfaces

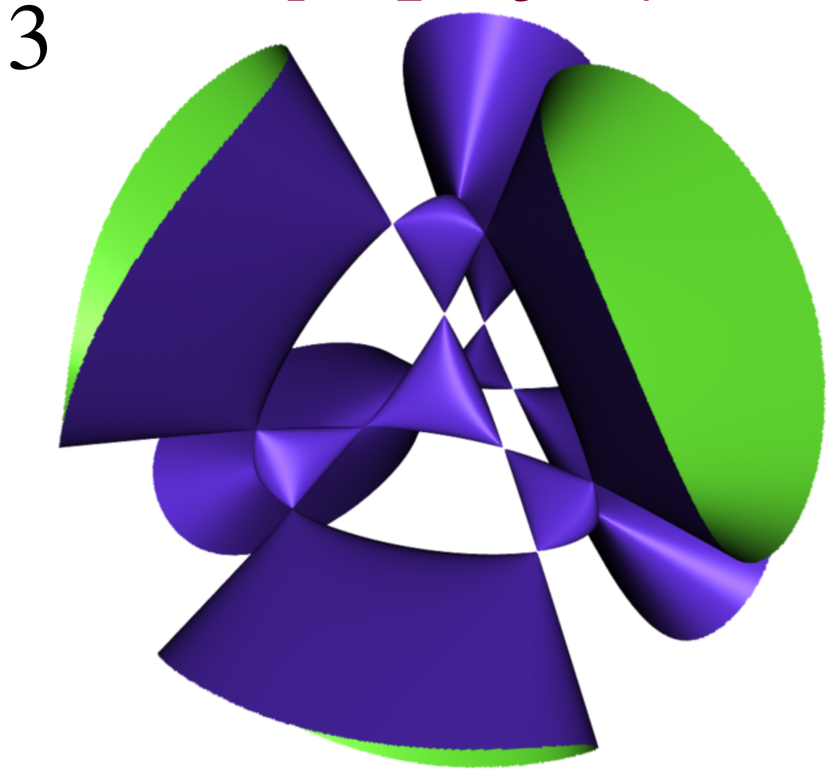
arithmetic?

$$\mathcal{K}_C = J_C/\langle \pm 1 \rangle$$

4 coordinates

X_1, X_2, X_3, X_4

$$\mathcal{K}_C \hookrightarrow \mathbb{P}^3$$



The quotient map destroys the group structure, but we still have a *pseudo-group law*.

Fast arithmetic on Kummer surfaces

Kummer surfaces from
general hyperelliptic curves

↓

General Kummer surfaces
(Cassels & Flynn)

Kummer surfaces from
Rosenhain curves

↓

Kummer surfaces arising from theta functions

Fast arithmetic!

Kummer surfaces in cryptography

Kummer surfaces in mathematics

The *general Kummer surface* has thus been the subject of interest in mathematics (see Cassels—Flynn).

Lots of theory developed for *theta functions of level 2* by Cosset, Lubicz, Robert, and others.

Allows us to develop the theory of Kummer surfaces.

Kummer surfaces in HECC

Introduced to cryptography by Gaudry (2004), who extended work by the Chudnovsky brothers (1986).

Hyperoptimised version in 2014 using the squared Kummer:

Kummer strikes back
(Bernstein, Chuengsatiansup, Lange, Schwabe)

Faster than elliptic curve Diffie-Hellman using parallelisation.

Allows us to have *fast* arithmetic.

Kummer surfaces in isogenies

General (2,2)-isogeny formulae due to Dartois, Maino, Pope, and Robert (2023).

(2,2)-isogeniesin a *special* setting developed by Costello (2018).

Allows us to have *fast* isogeny formulae.

Fast arithmetic on Kummer surfaces

Analogously to Weierstrass vs. Montgomery, the *canonical and squared Kummer surface* has the *faster* arithmetic.

The arithmetic and (2,2)-isogenies are built from these 4 simple building blocks:

$$\mathrm{H} : (X_1 : X_2 : X_3 : X_4) \mapsto (X_1 + X_2 + X_3 + X_4 : X_1 + X_2 - X_3 - X_4 : X_1 - X_2 + X_3 - X_4 : X_1 - X_2 - X_3 + X_4)$$

$$\mathrm{S} : (X_1 : X_2 : X_3 : X_4) \mapsto (X_1^2 : X_2^2 : X_3^2 : X_4^2)$$

$$\mathrm{Inv} : (X_1 : X_2 : X_3 : X_4) \mapsto (1/X_1 : 1/X_2 : 1/X_3 : 1/X_4)$$

Can be computed with 6 multiplications

$$\mathrm{C}_U : (X_1 : X_2 : X_3 : X_4) \mapsto (X_1 \cdot U_1 : X_2 \cdot U_2 : X_3 \cdot U_3 : X_4 \cdot U_4)$$

Fast arithmetic on Kummer surfaces

We work with the squared model

$$\mathcal{K}^{sqr}: E \cdot X_1X_2X_3X_4 = ((X_1^2 + X_2^2 + X_3^2 + X_4^2) - F \cdot (X_1X_4 + X_2X_3) \\ -G \cdot (X_1X_3 + X_2X_4) - H \cdot (X_1X_2 + X_3X_4))^2$$

where E, F, G, H are rational functions in the identity point $(\mu_1 : \mu_2 : \mu_3 : \mu_4)$

We also work with constants $(A^2 : B^2 : C^2 : D^2) = \mathrm{H}(\mu_1 : \mu_2 : \mu_3 : \mu_4)$, which will appear in the isogeny formulae later.

Scholten's construction

Scholten gives explicit equations to construct $J_\alpha/\mathbb{F}_p$ from $E_\alpha/\ \mathbb{F}_{p^2}$, by taking the "Weil restriction".

We can view this as a special type of *glueing*.

$$E_\alpha/\ \mathbb{F}_{p^2}$$

$$E_\alpha \times E_\alpha^{(p)}/\ \mathbb{F}_{p^2} \xrightarrow[\text{glue}]{} J_\alpha/\mathbb{F}_p$$

$$E_\alpha^{(p)}/\ \mathbb{F}_{p^2}$$

$$E_\alpha/\ \mathbb{F}_{p^2} \dashrightarrow E_\alpha \times E_\alpha^{(p)}/\ \mathbb{F}_{p^2} \dashleftarrow E_\alpha^{(p)}/\ \mathbb{F}_{p^2}$$

Elliptic Kummer surfaces

$$E_\alpha \times E_\alpha^{(p)} /\ \mathbb{F}_{p^2} \xrightarrow[\text{glue}]{} J_\alpha/\mathbb{F}_p \longrightarrow J_{\lambda,\mu,\lambda\mu}/\mathbb{F}_p \longrightarrow \mathcal{K}^{\mathrm{sqr}}/\mathbb{F}_p$$

Isogenies between Kummer surfaces

A (2,2)-**isogeny of Kummer surfaces** is a morphism φ such that the following diagram commutes.

$$
\begin{array}{ccc}
\mathscr{J}_1 & \xrightarrow[\phi]{} & \mathscr{J}_2 \\
\downarrow & & \downarrow \\
\mathscr{K}_1^{sqr} & \xrightarrow{\varphi} & \mathscr{K}_2^{sqr}
\end{array}
$$

Isogenies between Kummer surfaces

Let's consider the general case of $\bar{\mathbb{F}}_p$-rational (2,2)-isogenies between $\mathscr{K}^{sqr}/\mathbb{F}_p$ with kernel G.

$$\varphi_G = \mathrm{S} \circ \mathbf{A}_G \circ \mathrm{C}_{\mathrm{Inv}(A:B:C:D)} \circ \mathrm{H}$$

Linear map given by a 4x4 matrix whose entries are fourth roots of unity

Isogenies between Kummer surfaces

Let's consider the general case of $\bar{\mathbb{F}}_p$-rational (2,2)-isogenies between $\mathscr{K}^{sqr}/\mathbb{F}_p$ with kernel G.

$$\varphi_G = \mathrm{S} \circ \mathbf{A}_G \circ \mathrm{C}_{\mathrm{Inv}(A:B:C:D)} \circ \mathrm{H}$$

Requires square roots to compute $\mathrm{Inv}(A : B : C : D)$.

Can also use rational 4-torsion lying above in some cases

Isogenies between Kummer surfaces

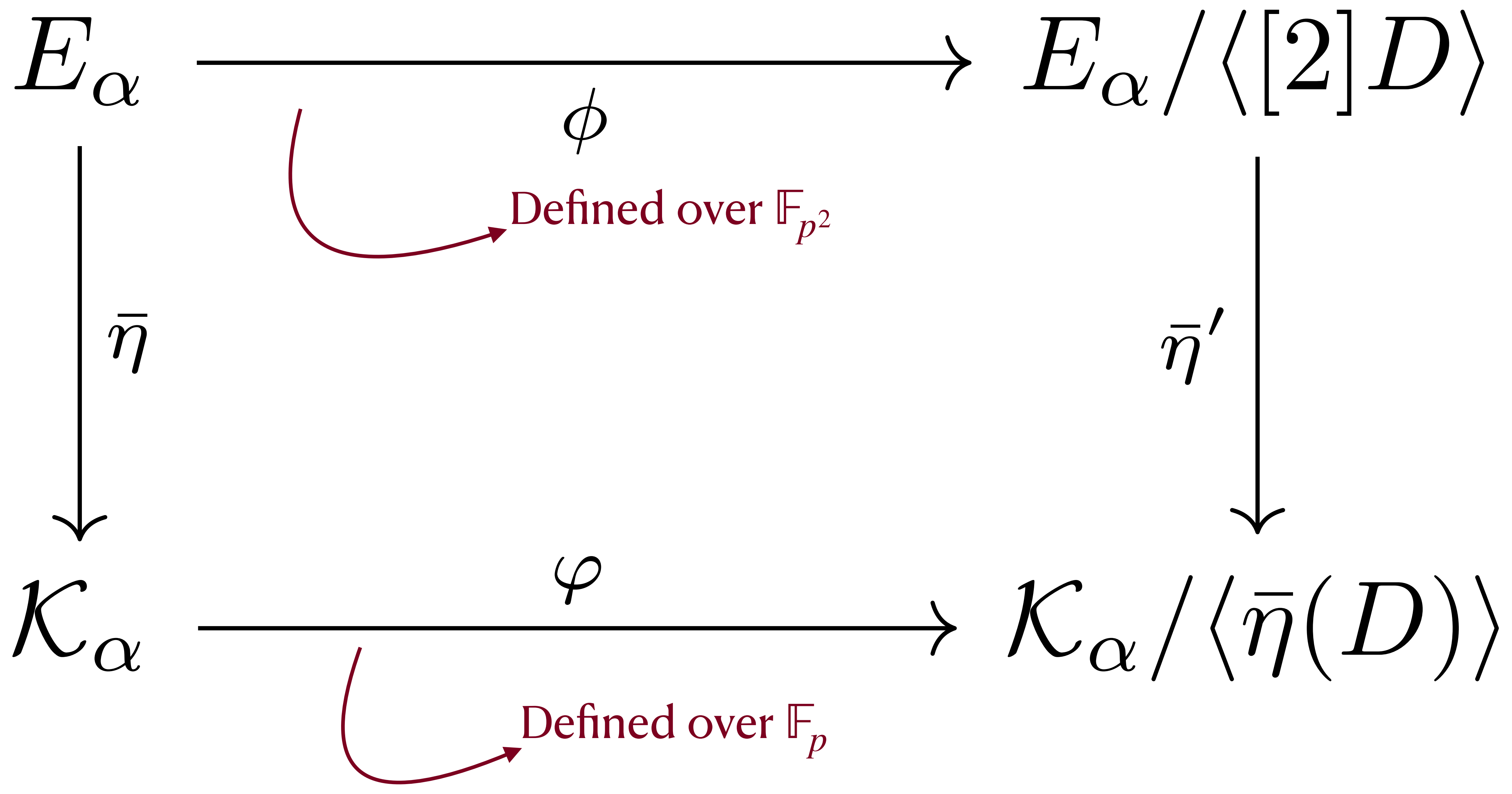
Let's consider the general case of $\bar{\mathbb{F}}_p$-rational (2,2)-isogenies between $\mathscr{K}^{sqr}/\mathbb{F}_p$ with kernel G.

$$\varphi_G = \mathrm{S} \circ \mathbf{A}_G \circ \mathrm{C}_{\mathsf{Inv}(A:B:C:D)} \circ \mathrm{H}$$

We now specialise this to the elliptic Kummer surface case.

Isogenies between elliptic Kummer surfaces

Let $D \in E_\alpha[4]$ a 4-torsion point. Then $\bar{\eta}(D) \in \mathscr{K}_\alpha[2]$ a 2-torsion point.



Isogenies between elliptic Kummer surfaces

Let $D \in E_\alpha[4]$ a 4-torsion point. Then $\bar{\eta}(D) \in \mathscr{K}_\alpha[2]$ a 2-torsion point.

$$\begin{array}{ccc} E_\alpha & \xrightarrow{\quad\phi\quad} & E_\alpha/\langle [2]D \rangle \\ \Big\downarrow \bar{\eta} & & \Big\downarrow \bar{\eta}' \\ \mathcal{K}_\alpha & \xrightarrow{\quad\varphi\quad} & \mathcal{K}_\alpha/\langle \bar{\eta}(D) \rangle \end{array}$$

An elliptic Kummer surface!

Isogenies between elliptic Kummer surfaces

Let $D \in E_\alpha[4]$ a 4-torsion point. Then $\bar{\eta}(D) \in \mathscr{K}_\alpha[2]$ a 2-torsion point.

$$\begin{array}{ccc}
E_\alpha & \xrightarrow[\phi]{} & E_\alpha/\langle [2]D \rangle \\
\Big\downarrow \bar{\eta} & & \Big\downarrow \bar{\eta}' \\
\mathcal{K}_\alpha & \xrightarrow{\varphi} & \mathcal{K}_\alpha/\langle \bar{\eta}(D) \rangle
\end{array}$$

Note: the kernel of the isogeny is now defined by *one* 2-torsion point!

Isogenies between elliptic Kummer surfaces

$$E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$$

$$\begin{array}{ccc} E_\alpha & \xrightarrow[\phi_0]{} & E_\alpha/\langle(0,0)\rangle \\ \downarrow & & \downarrow \\ \mathcal{K}_\alpha & \xrightarrow{\varphi_0} & \mathcal{K}_\alpha/\langle K_0\rangle \end{array}$$

$$\varphi_0 = \mathsf{C}_{\mathsf{Inv}(A^2:B^2:C^2:D^2)} \circ \mathsf{S} \circ \mathsf{H}$$

$K_0 = (\mu_4 : \mu_3 : \mu_2 : \mu_1)$ or $(\mu_3 : \mu_4 : \mu_1 : \mu_2)$

COST

Obtaining image: 8a

Evaluating at a point: 8M + 8a

Isogenies between elliptic Kummer surfaces

$$E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$$

$$\begin{array}{ccc} E_\alpha & \xrightarrow[\phi_\alpha]{} & E_\alpha/\langle(\alpha,0)\rangle \\ \downarrow & & \downarrow \\ \mathcal{K}_\alpha & \xrightarrow{\varphi_\alpha} & \mathcal{K}_\alpha/\langle K_\alpha\rangle \end{array}$$

$$\varphi_\alpha = \mathsf{S} \circ \mathsf{H} \circ \mathsf{C}_{\mathsf{Inv}(A:B:C:D)} \circ \mathsf{H}$$

$$K_\alpha = (1:0:0:\tau) \text{ or } (1:0:\tau:0)$$

$$\begin{array}{ccc} E_\alpha & \xrightarrow[\phi_{1/\alpha}]{} & E_\alpha/\langle(1/\alpha,0)\rangle \\ \downarrow & & \downarrow \\ \mathcal{K}_\alpha & \xrightarrow{\varphi_{1/\alpha}} & \mathcal{K}_\alpha/\langle K_{1/\alpha}\rangle \end{array}$$

$$\varphi_{1/\alpha} = \mathsf{S} \circ \mathsf{H}' \circ \mathsf{C}_{\mathsf{Inv}(A:B:C:D)} \circ \mathsf{H}$$

$$\mathsf{H}'(X:Y:Z:T) = \mathsf{H}(-X:Y:Z:T)$$

$$K_{1/\alpha} = (\tau:0:0:1) \text{ or } (\tau:0:1:0)$$

Scaling factor $\mathsf{Inv}(A:B:C:D)$ computed with **3M** + **8a** using the 4-torsion lying above the kernel generator

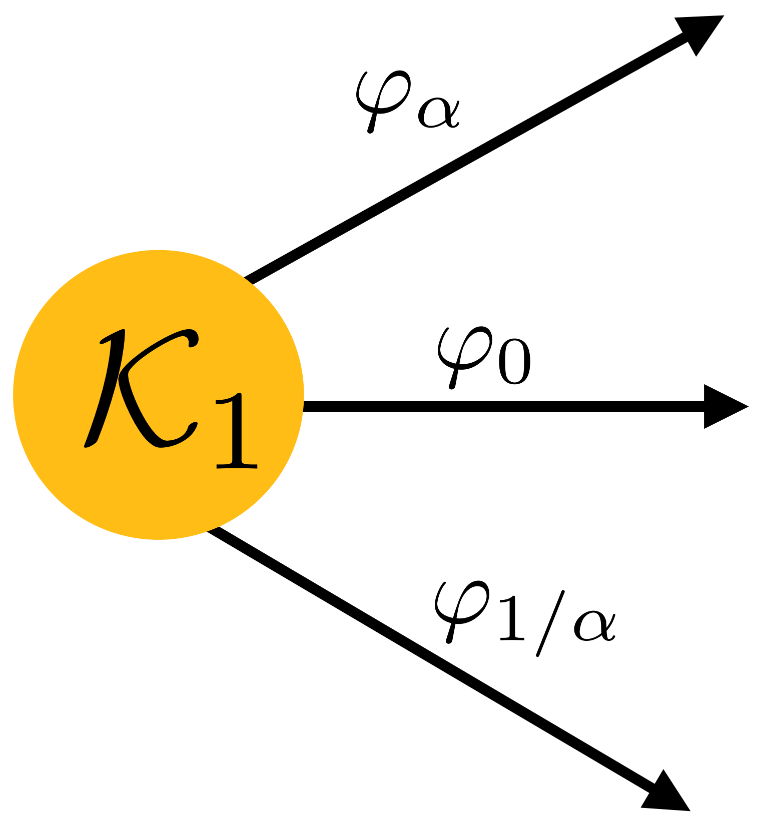
COST

Obtaining image: 11M + 32a

Evaluating at a point: 8M + 16a

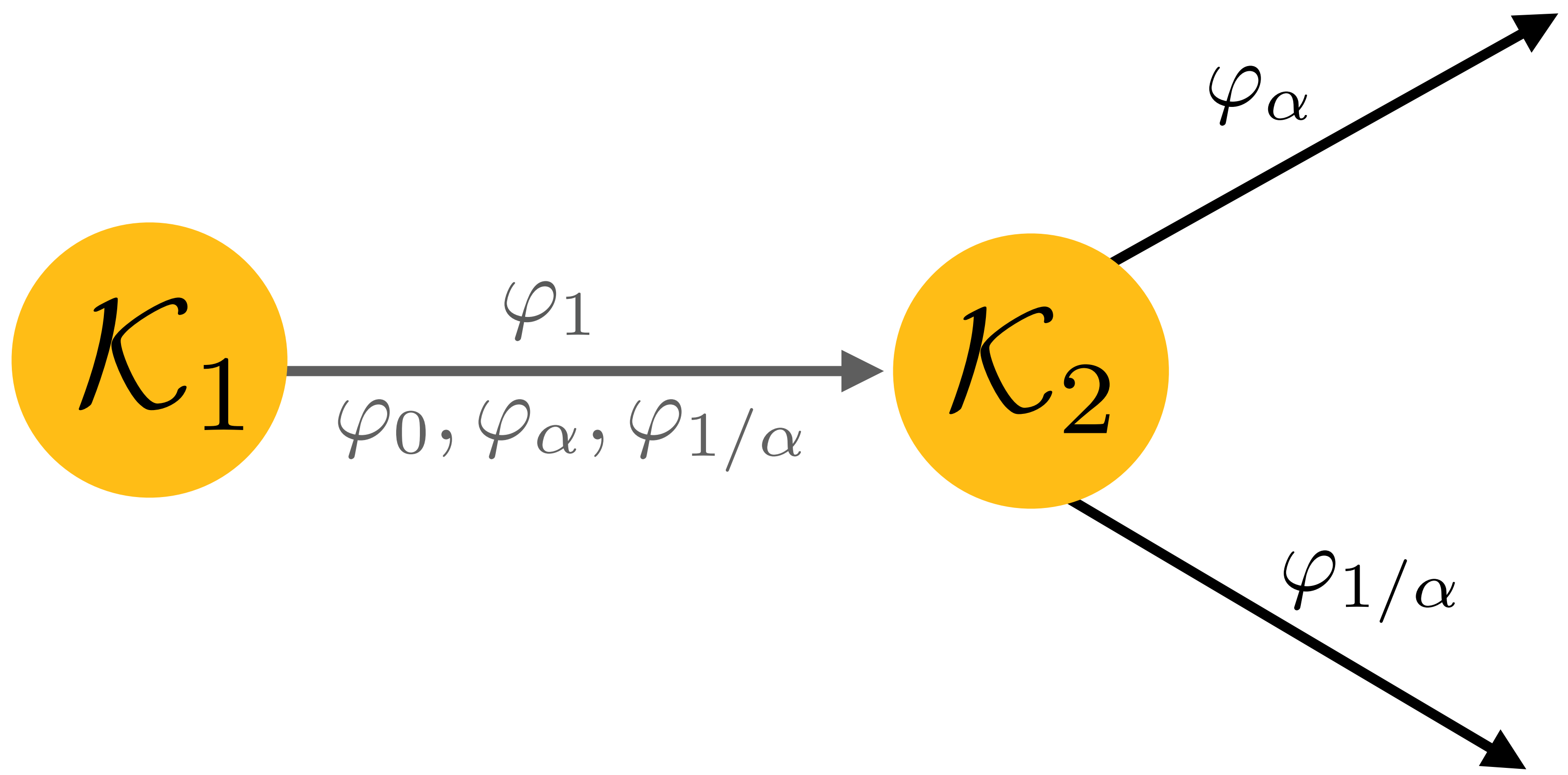
Chains of (2,2)-isogenies

We show how to construct (non-backtracking) chains of (2,2)-isogenies.



Chains of (2,2)-isogenies

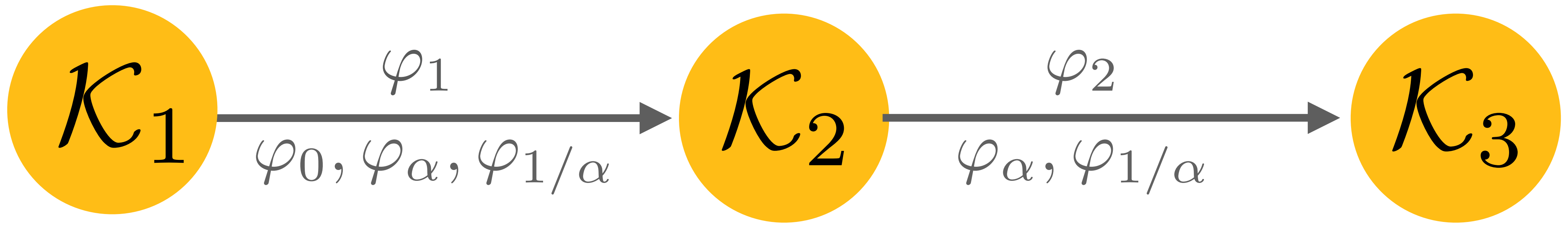
We show how to construct (non-backtracking) chains of (2,2)-isogenies.



$$\ker \widehat{\varphi}_1 \cap \ker \varphi_2 = \emptyset$$

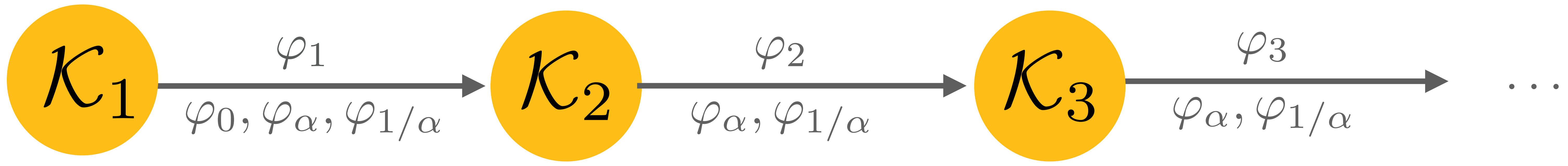
Chains of (2,2)-isogenies

We show how to construct (non-backtracking) chains of (2,2)-isogenies.



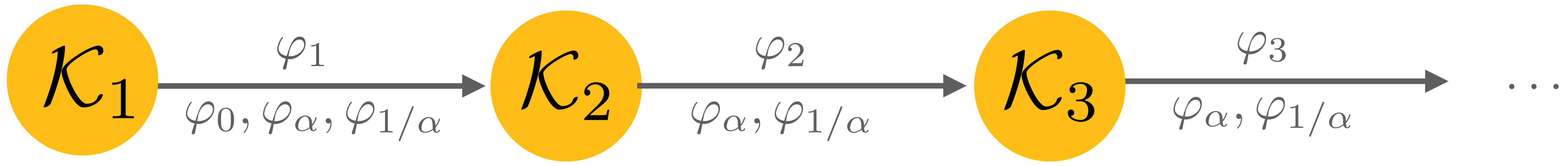
Chains of (2,2)-isogenies

We show how to construct (non-backtracking) chains of (2,2)-isogenies.



Chains of (2,2)-isogenies

We show how to construct (non-backtracking) chains of (2,2)-isogenies.



For a chain of length k, if we have $\mathbb{F}_p$-rational 2^{k+1}-torsion on $\mathcal{K}_1$, at each step we can compute the scaling using the 4-torsion.

SQIsign with Kummer surfaces

Recall: SQIsign verification is performed in 13 steps

$$E_\alpha = E^{(1)} \xrightarrow{\varphi_1} E^{(2)} \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{12}} E^{(12)} \xrightarrow{\varphi_{13}} E^{(13)} = E_{\alpha'}$$

SQIsign with Kummer surfaces

Recall: SQIsign verification is performed in 13 steps

$$E_\alpha = E^{(1)} \xrightarrow{\varphi_1} E^{(2)} \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{12}} E^{(12)} \xrightarrow{\varphi_{13}} E^{(13)} = E_{\alpha'}$$

We can instead map this down to Kummer surfaces and compute isogenies defined over $\mathbb{F}_p$

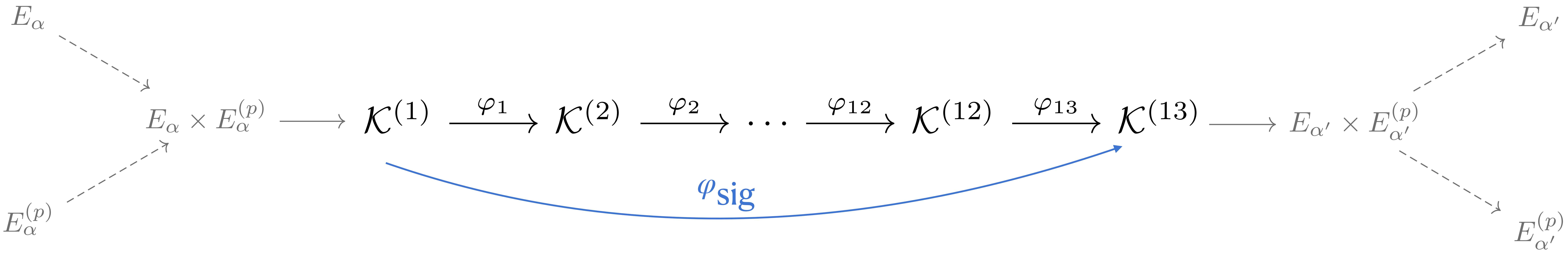
$$E_\alpha \dashrightarrow E_\alpha \times E_\alpha^{(p)} \dashleftarrow E_\alpha^{(p)}$$

$$E_\alpha \times E_\alpha^{(p)} \longrightarrow \mathcal{K}^{(1)} \xrightarrow{\varphi_1} \mathcal{K}^{(2)} \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{12}} \mathcal{K}^{(12)} \xrightarrow{\varphi_{13}} \mathcal{K}^{(13)} \longrightarrow E_{\alpha'} \times E_{\alpha'}^{(p)}$$

$$E_{\alpha'} \dashleftarrow E_{\alpha'} \times E_{\alpha'}^{(p)} \dashrightarrow E_{\alpha'}^{(p)}$$

SQIsign with Kummer surfaces

We can instead map this down to Kummer surfaces and compute isogenies defined over $\mathbb{F}_p$



Uncompressed Signatures

φ_{sig} is given as a list of kernel generators $K_1, K_2, \ldots, K_{13} \in \mathscr{K}^{sqr}[2^{76}]$

Compressed signatures?

Recall compress our elliptic signatures we needed:

- Deterministic point sampling to compute a basis $\langle P_i, Q_i \rangle = E^{(i-1)}[2^{75}]$
- Three point ladder on the Kummer line to compute the kernel generator $K_i = P_i + s_i Q_i$

Compressed signatures?

- Deterministic point sampling to compute a basis $\langle P_i, Q_i \rangle = \mathscr{K}^{(i-1)}[2^{76}]$
- Three point ladder on the Kummer surface to compute the kernel generator $K_i = P_i + s_i Q_i$

Compressed signatures?

- Deterministic point sampling to compute a basis $\langle P_i, Q_i \rangle = \mathscr{K}^{(i-1)}[2^{76}]$
- Three point ladder on the Kummer surface to compute the kernel generator $K_i = P_i + s_i Q_i$

Problem: Given P_i, Q_i and scalar s_i compute $P_i + s_i Q_i$

1) Compute $[s_i]Q_i$ using scalar multiplication
2) Compute the point difference $P_i - s_i Q_i$
3) From P_i, $[s_i]Q_i$, $P_i - s_i Q_i$, compute the kernel generator $P_i + s_i Q_i$ using a three point ladder

We develop efficient **PointDifference** and **ThreePointLadder** algorithms.

Compressed signatures?

- Deterministic point sampling to compute a basis $\langle P_i, Q_i \rangle = \mathscr{K}^{(i-1)}[2^{76}]$
- Three point ladder on the Kummer surface to compute the kernel generator $K_i = P_i + s_i Q_i$

Problem: Sample points deterministically

Solution: use pairings!

SQIsign compressed signatures

Now we know how to compute $K_i = P_i + s_i Q_i$. **How does the signer compute s_i for each step?**

Point Compression (by Signer)

1) Sample basis P_i, Q_i on Kummer surface deterministically

2) Map K_i, P_i, Q_i to their corresponding points on the Jacobian

3) Compute the discrete logarithm s_i such that $K_i = P_i + s_i Q_i$

SQIsign compressed signatures

Now we know how to compute $K_i = P_i + s_i Q_i$. **How does the signer compute s_i for each step?**

Point Compression (by Signer)

1) Sample basis P_i, Q_i on Kummer surface deterministically

2) Map K_i, P_i, Q_i to their corresponding points on the Jacobian

3) Compute the discrete logarithm s_i such that $K_i = P_i + s_i Q_i$

We develop a new efficient algorithm for this

Conclusions

- We show how SQIsign verification can be seen as a protocol between Kummer surfaces.
- We build a toolbox of new techniques to facilitate SQIsign verification of compressed signatures.
- Using our methods, new practical higher dimensional protocols may be enabled.

Any questions?

For more details: **eprint 2024/948**