Fast computation of higher dimensional isogenies for cryptographic applications

Pierrick Dartois

Under the supervision of Damien Robert, Benjamin Wesolowski and Luca De Feo

2026, June 9

Introduction

Hard problems for public key cryptography

Widely used underlying problems...

- The factorisation problem (RSA):

$$N = p \times q.$$

- The discrete logarithm problem in a group $(G, +)$ generated by P (ECC):

$$Q = [n]P.$$

Hard problems for public key cryptography

Widely used underlying problems...

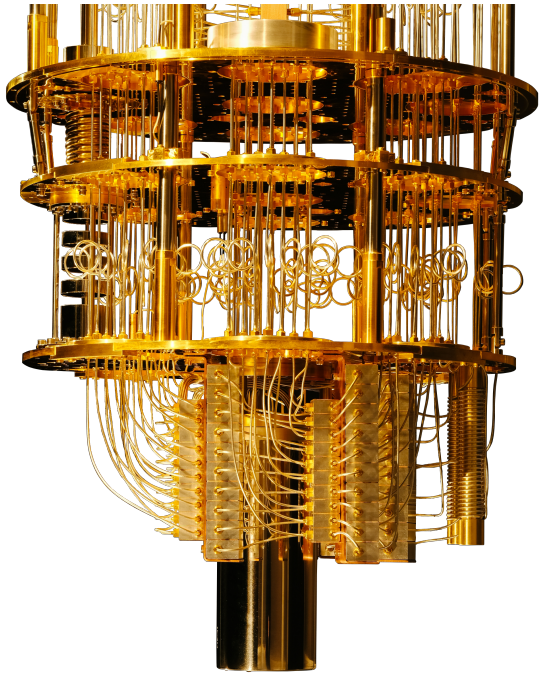
- The factorisation problem (RSA):

$$N = p \times q.$$

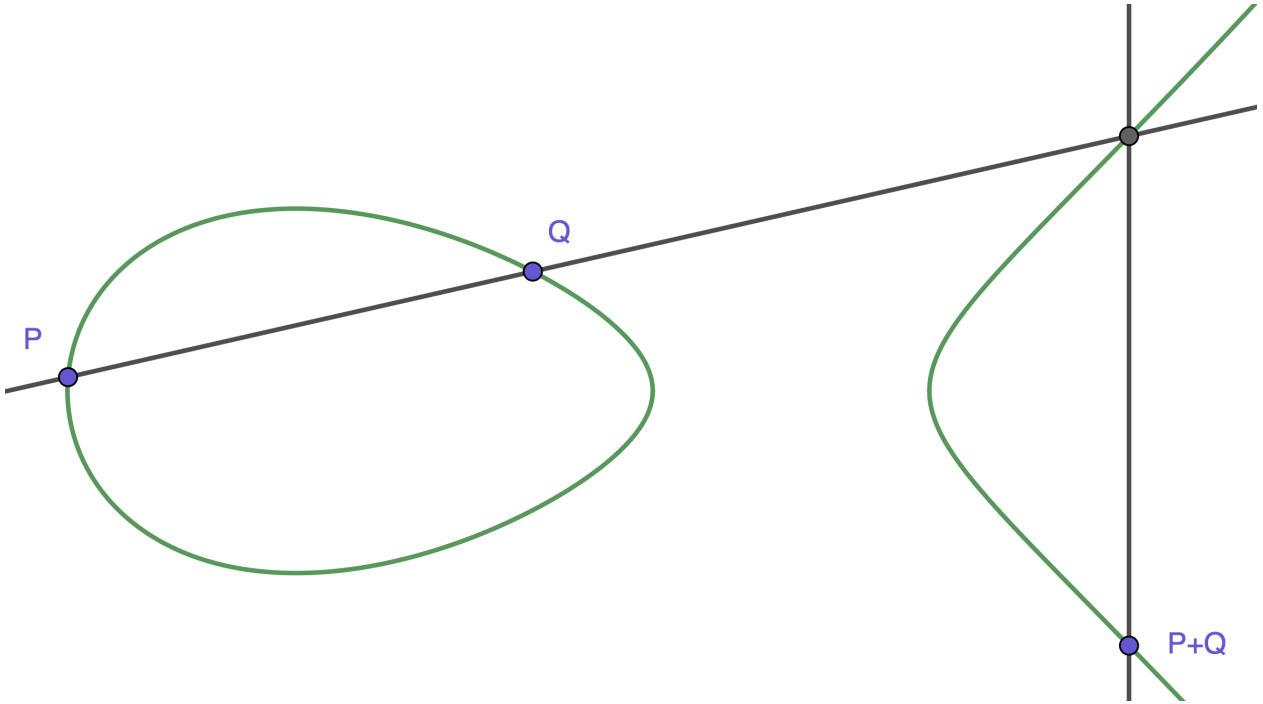
- The discrete logarithm problem in a group $(G, +)$ generated by P (ECC):

$$Q = [n]P.$$

...All broken by quantum computers



Elliptic curves

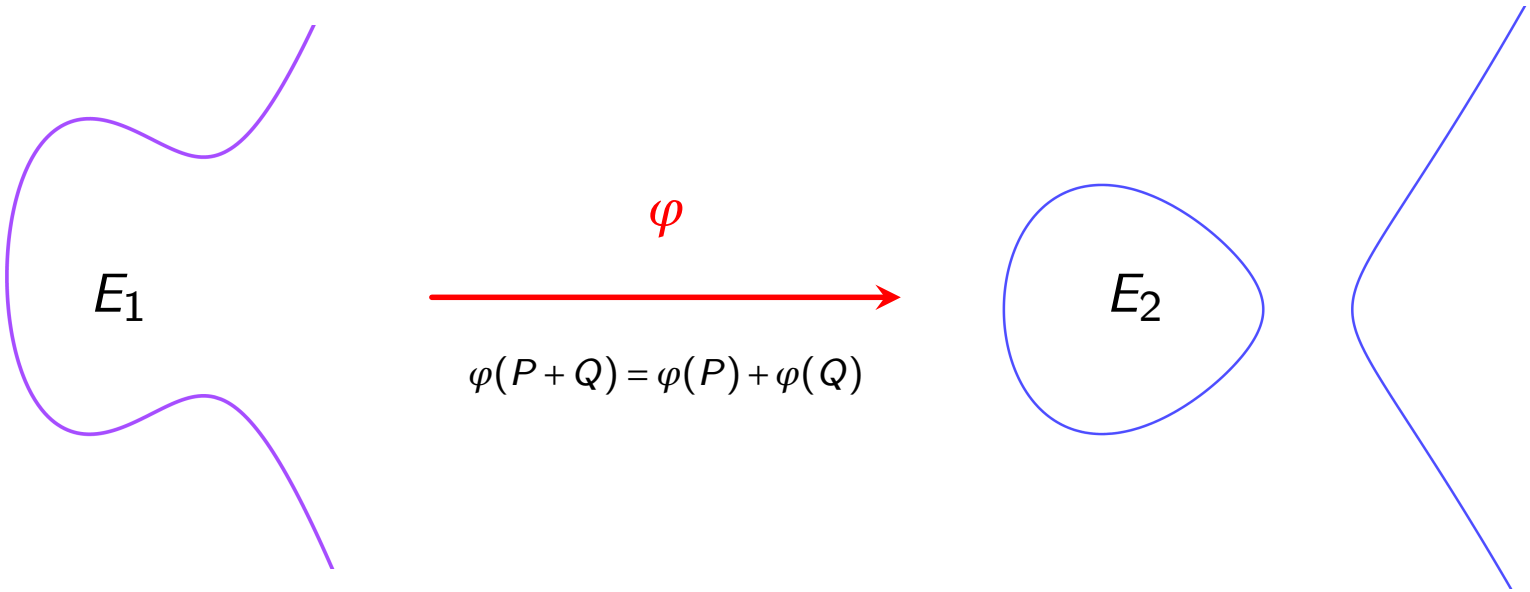


- An elliptic curve $E/\mathbb{F}_q$ is defined by:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q$$

  with an infinite element 0_E.
- E is equipped with a commutative group law.

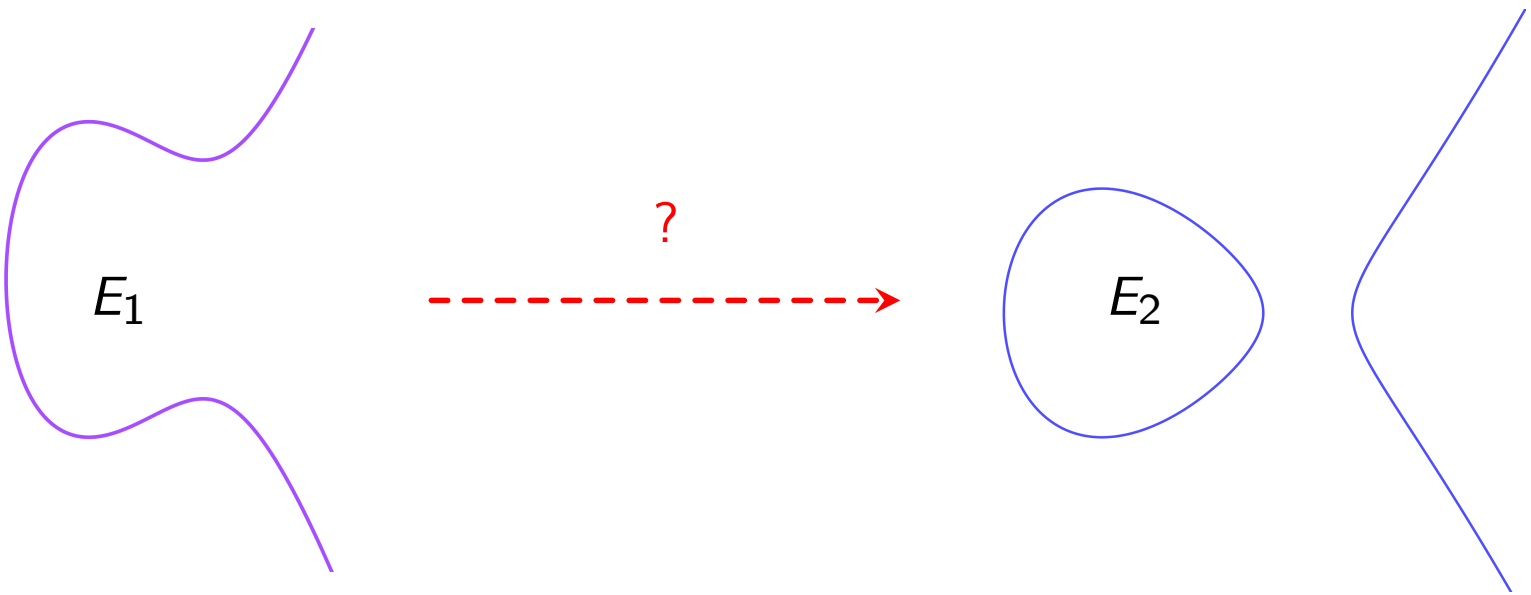
Isogenies



$$\varphi(x,y)=\left(\frac{p(x)}{q(x)},y\frac{r(x)}{s(x)}\right)$$

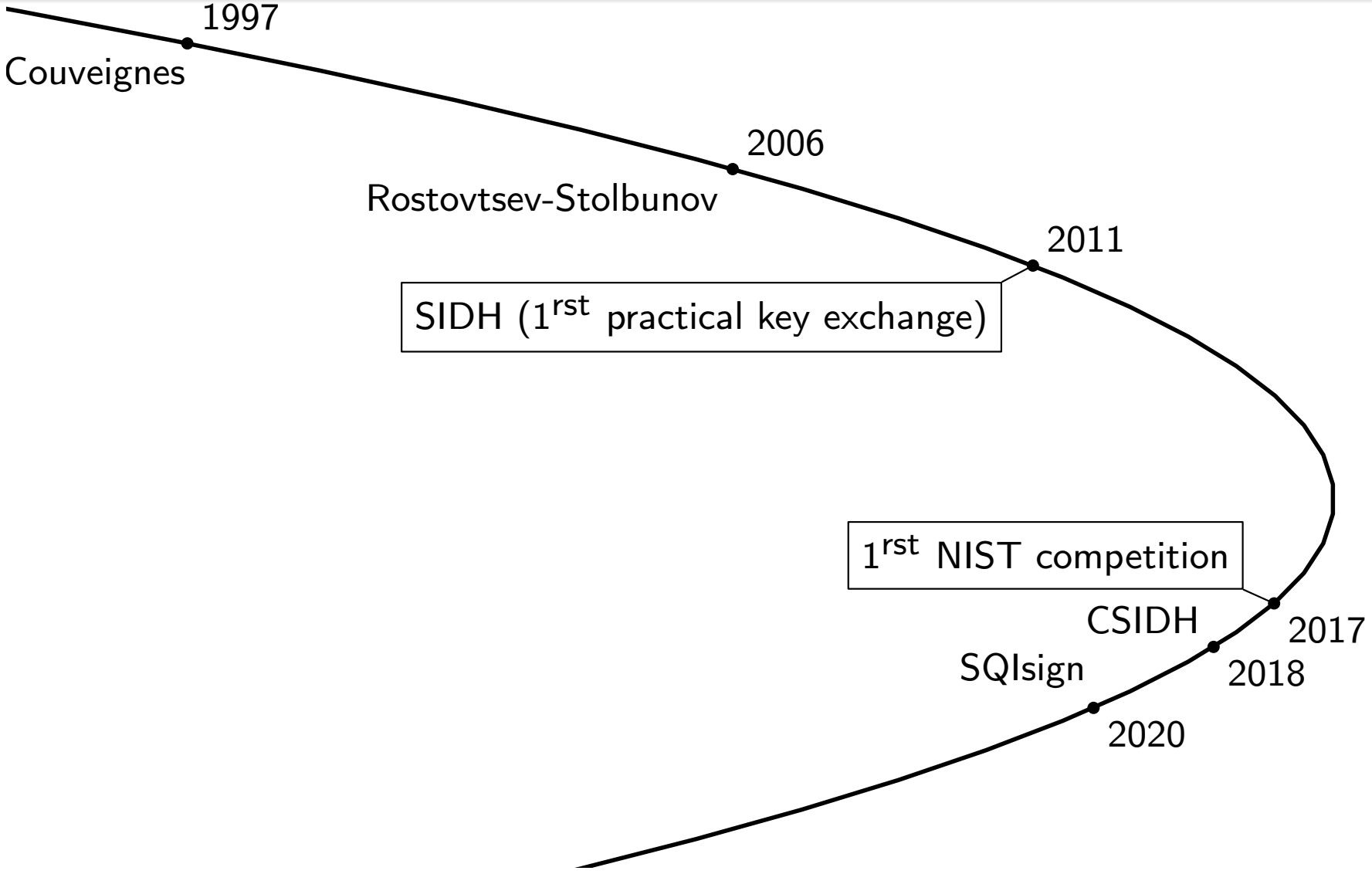
Why are isogenies interesting in cryptography?

The isogeny problem: Given two elliptic curves $E_1, E_2/\mathbb{F}_q$, find an isogeny $E_1 \longrightarrow E_2$.

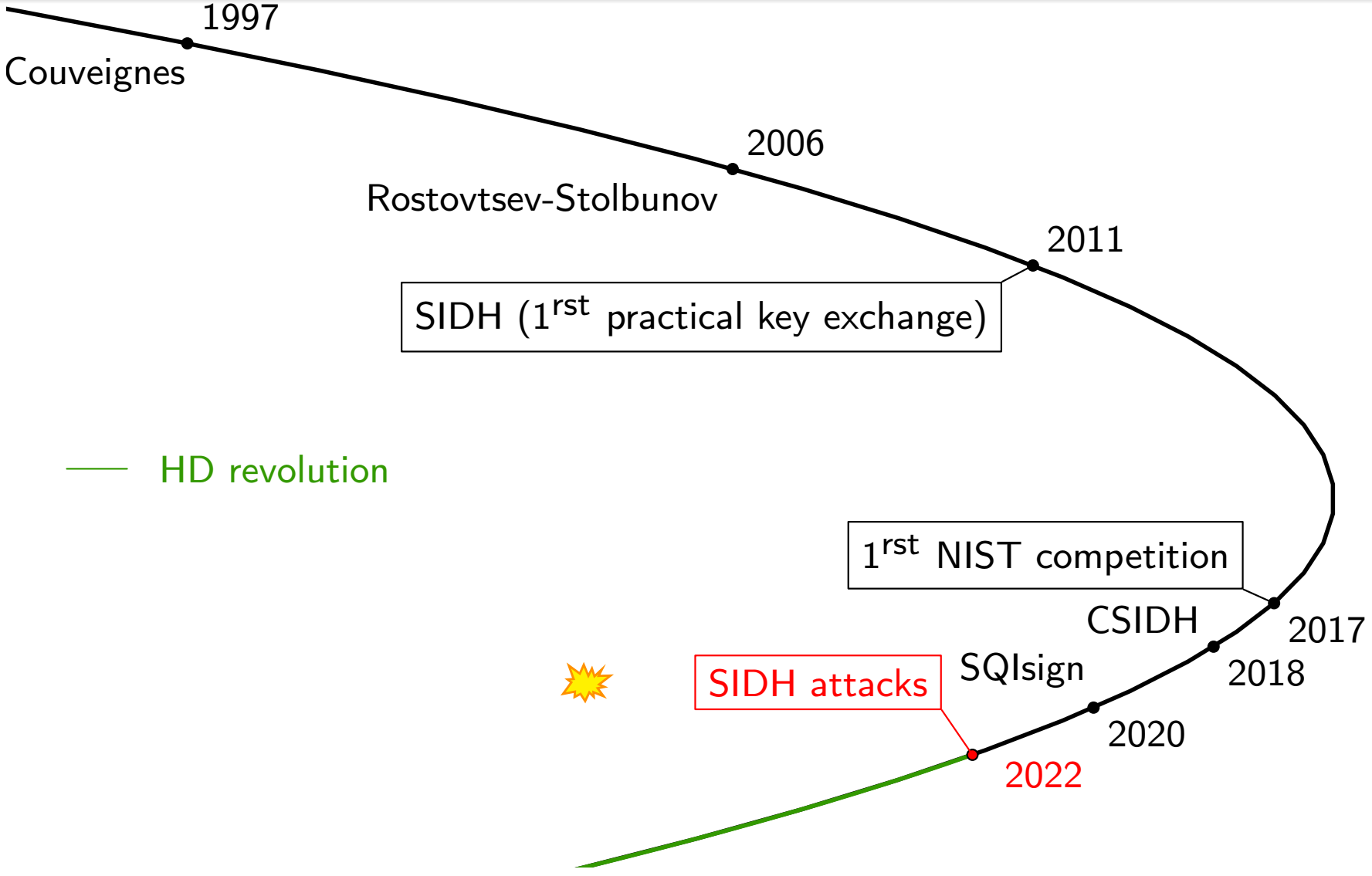


This problem is assumed to be hard for both classical and quantum computers.

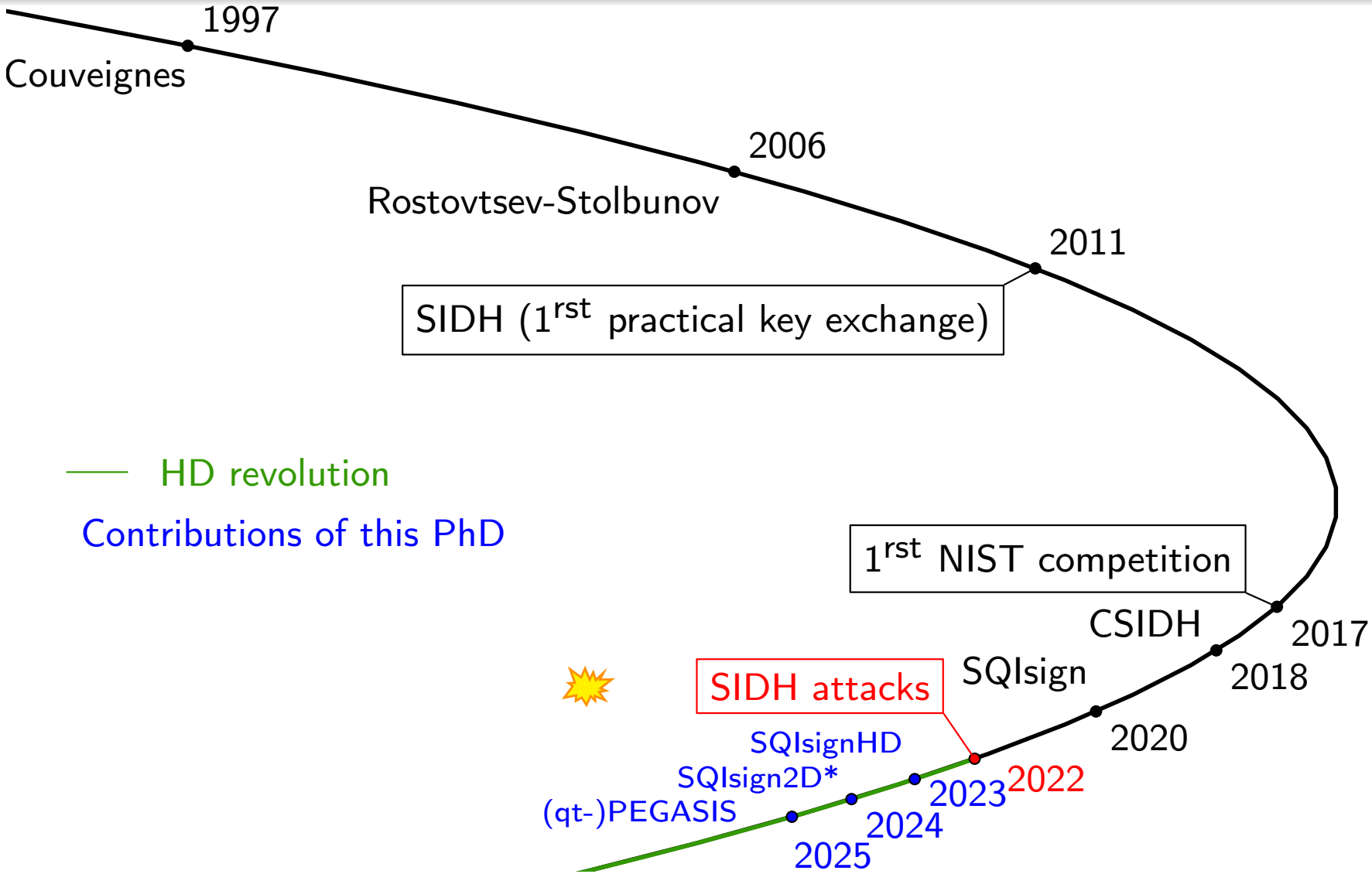
A brief (biased) history of isogeny based cryptography



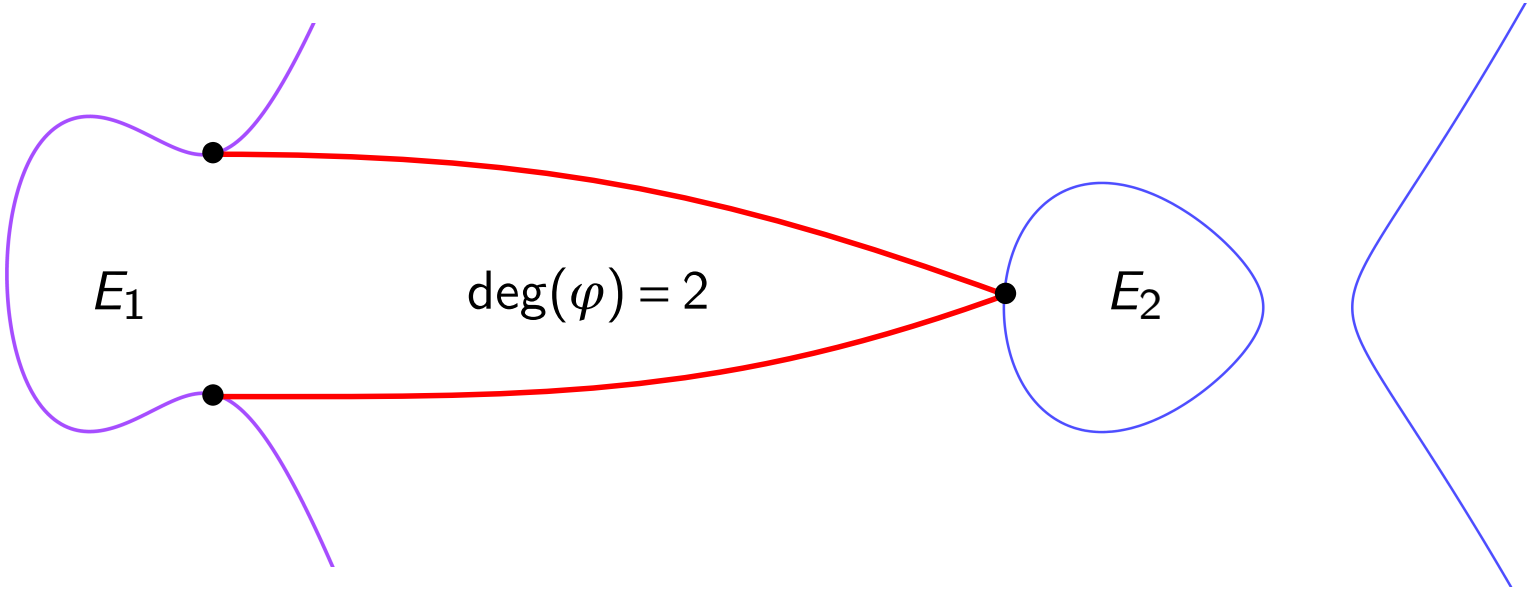
A brief (biased) history of isogeny based cryptography



A brief (biased) history of isogeny based cryptography



Isogenies - degree

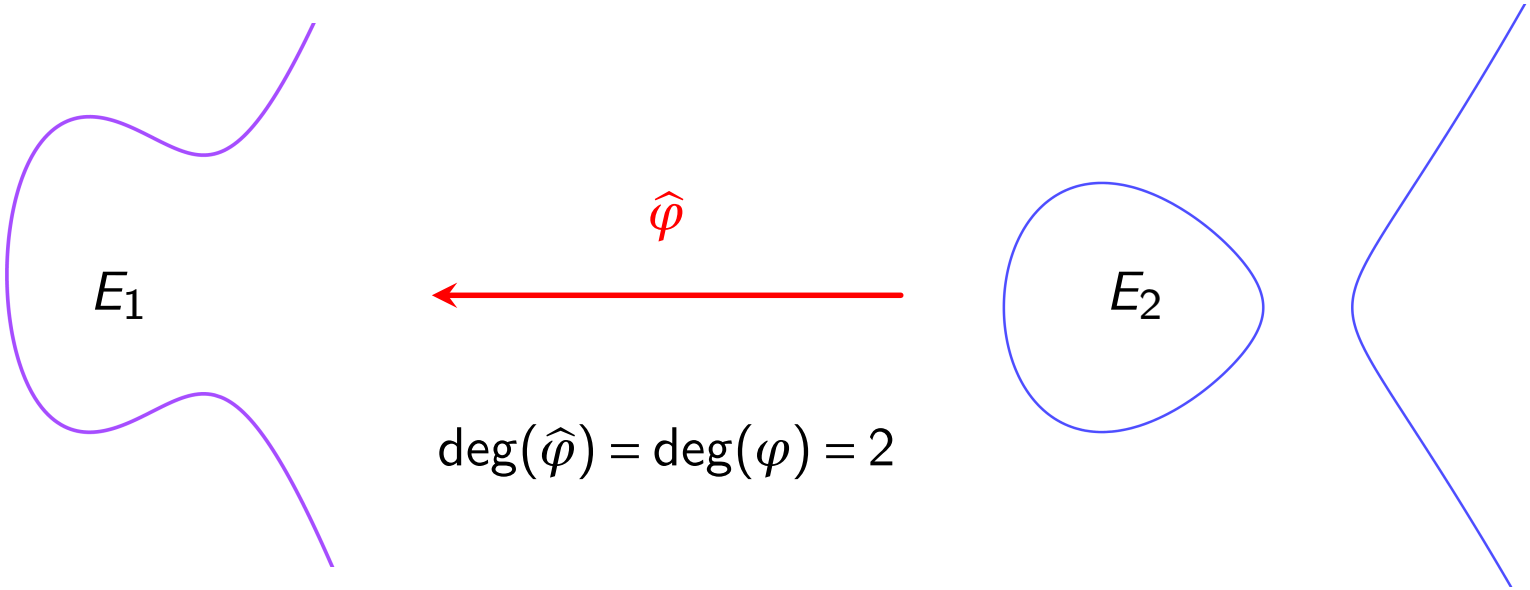


- The "size" of an isogeny: $\deg(\varphi) = \max(\deg(p), \deg(q))$ when

$$\varphi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right)$$

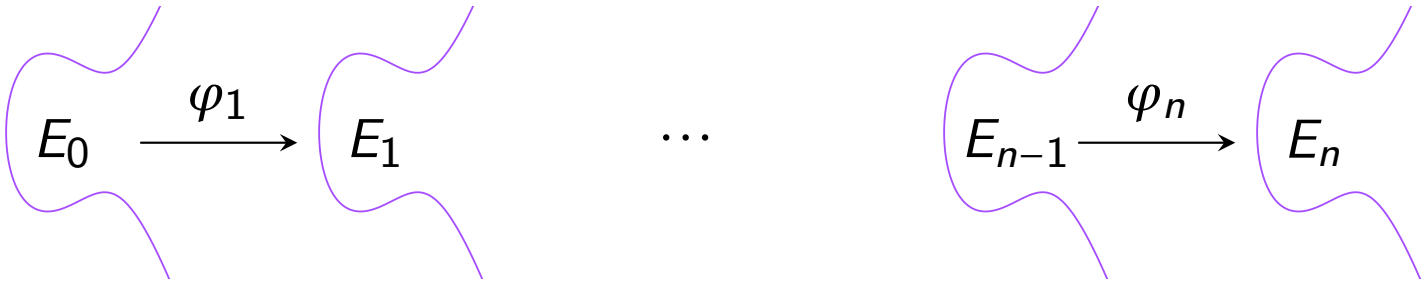
- $\deg(\varphi) = \#\ker(\varphi)$ in most cases.

Isogenies - the dual isogeny



If $\deg(\varphi) = n$, then $\widehat{\varphi} \circ \varphi = [n]$.

Isogeny chains



$$\deg(\varphi_n \circ \cdots \circ \varphi_1) = \prod_{i=1}^{n} \deg(\varphi_i)$$

How to efficiently represent an isogeny of big degree

✗ Inefficient: with rational fractions

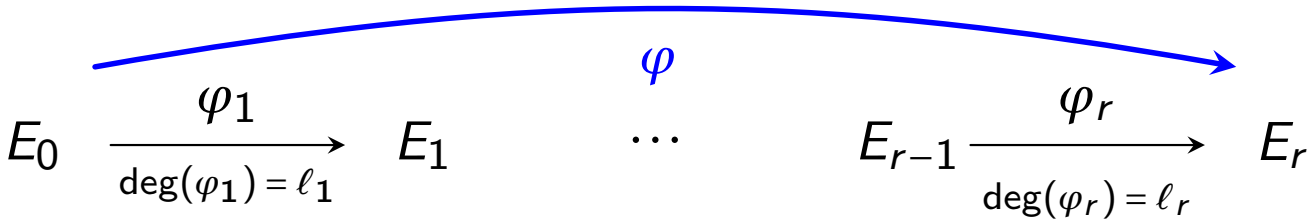
$$\varphi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right).$$

How to efficiently represent an isogeny of big degree

✗ Inefficient: with rational fractions

$$\varphi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right).$$

✓ If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$ is smooth, an isogeny chain:

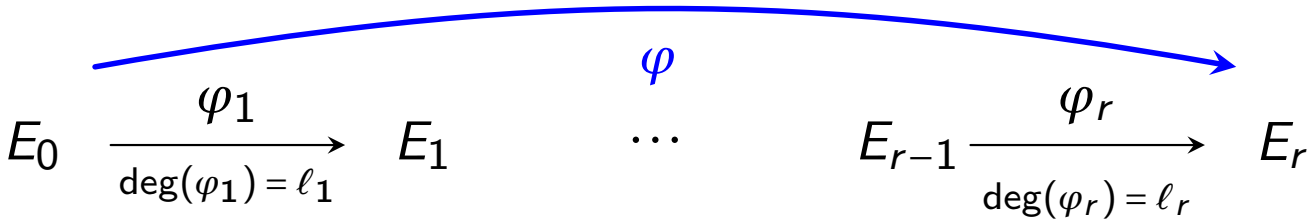


How to efficiently represent an isogeny of big degree

✗ Inefficient: with rational fractions

$$\varphi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right).$$

✓ If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$ is smooth, an isogeny chain:



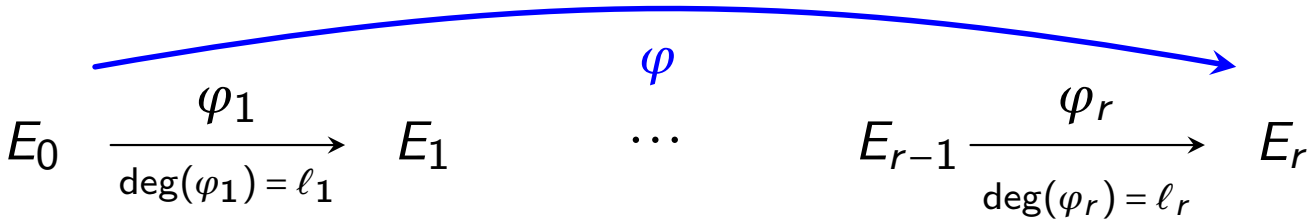
✓ If $\deg(\varphi)$ is smooth, a point P generating $\ker(\varphi)$.

How to efficiently represent an isogeny of big degree

✗ Inefficient: with rational fractions

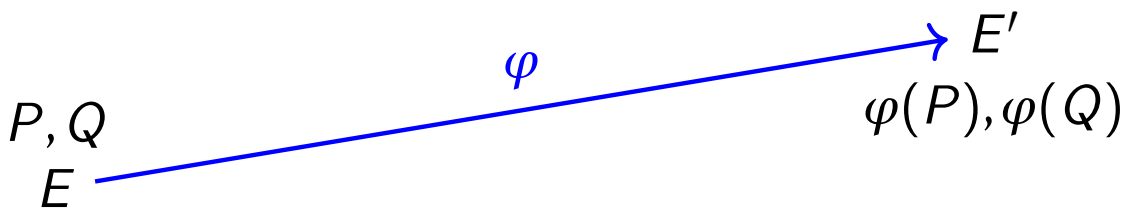
$$\varphi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right).$$

✓ If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$ is smooth, an isogeny chain:



✓ If $\deg(\varphi)$ is smooth, a point P generating $\ker(\varphi)$.

✓ **New:** If $\deg(\varphi)$ is not smooth, with higher dimensional interpolation



SQIsign and the Deuring correspondence

The Endomorphism ring

Definition (Endomorphism ring)

$$\mathrm{End}(E) = \{0\} \cup \{\text{Isogenies } \varphi : E \longrightarrow E\}$$

Defines a ring for the addition and composition of isogenies.

The Endomorphism ring

Definition (Endomorphism ring)

$$\mathrm{End}(E) = \{0\} \cup \{\text{Isogenies } \varphi : E \longrightarrow E\}$$

Defines a ring for the addition and composition of isogenies.

Theorem (Deuring)

Let $E/\mathbb{F}_q$ $(p = \mathrm{char}(\mathbb{F}_q))$. *Then* $\mathrm{End}(E)$ *is either isomorphic to:*

- *An order in a quadratic imaginary field (2D commutative object). We say that* E *is ordinary.*
- *An order in the quaternion algebra* $\mathcal{B}_{p,\infty}$ *(4D non-commutative object). We say that* E *is supersingular.*

The Endomorphism ring

Definition (Endomorphism ring)

$$\mathrm{End}(E) = \{0\} \cup \{\text{Isogenies } \varphi : E \longrightarrow E\}$$

Defines a ring for the addition and composition of isogenies.

Theorem (Deuring)

Let $E/\mathbb{F}_q$ ($p = \mathrm{char}(\mathbb{F}_q)$). Then $\mathrm{End}(E)$ is either isomorphic to:

- *An order in a quadratic imaginary field (2D commutative object). We say that E is ordinary.*
- *An order in the quaternion algebra $\mathcal{B}_{p,\infty}$ (4D non-commutative object). We say that E is supersingular.*

In isogeny-based cryptography, supersingular curves are prefered for security and efficiency reasons.

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$

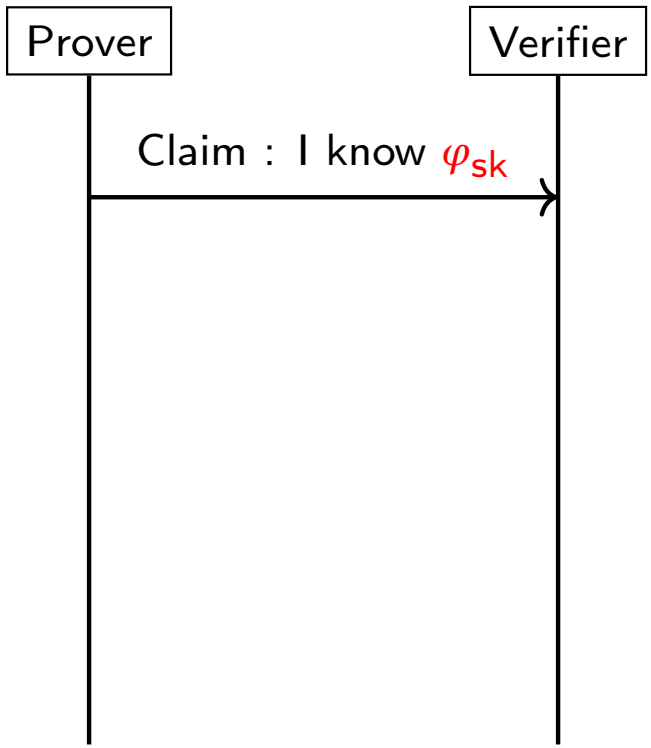
The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi)$

The SQIsign identification scheme



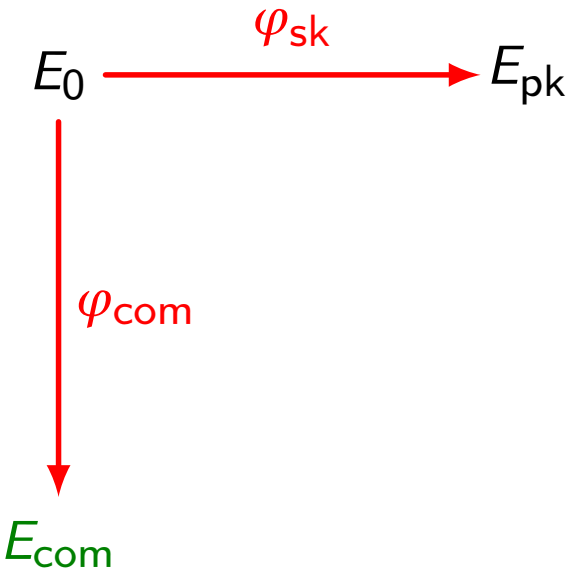
public

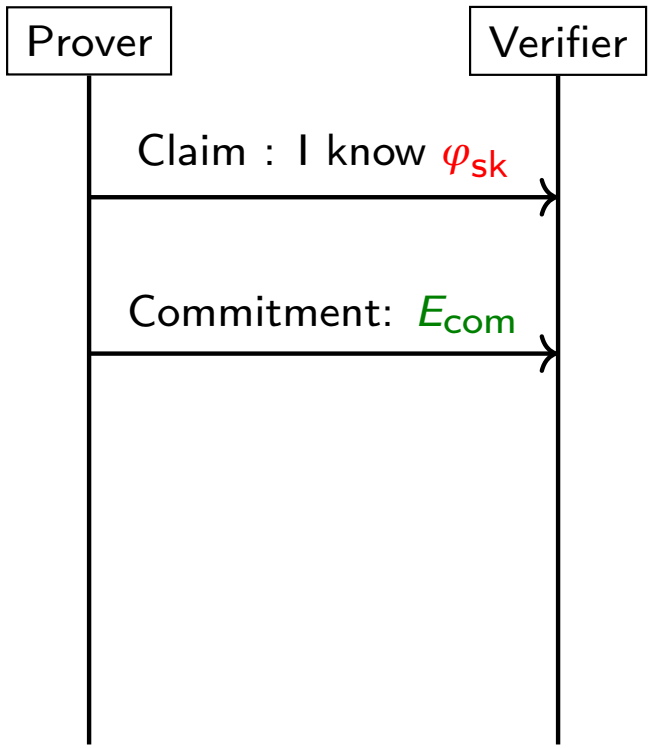
Prover's secret

published by Verifier

published by Prover

The SQIsign identification scheme





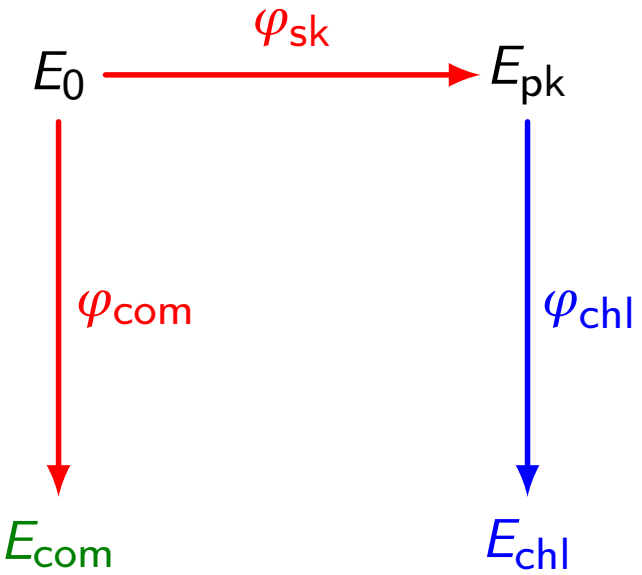
public

Prover's secret

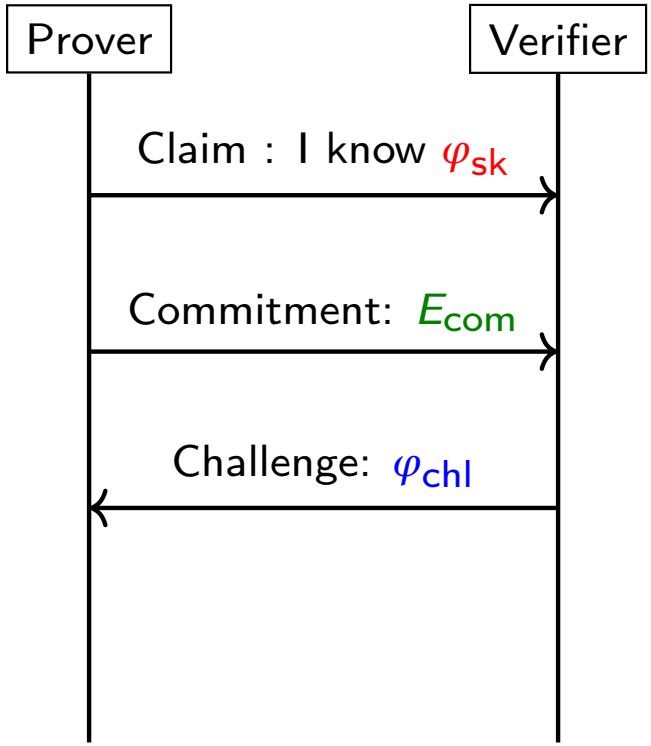
published by Verifier

published by Prover

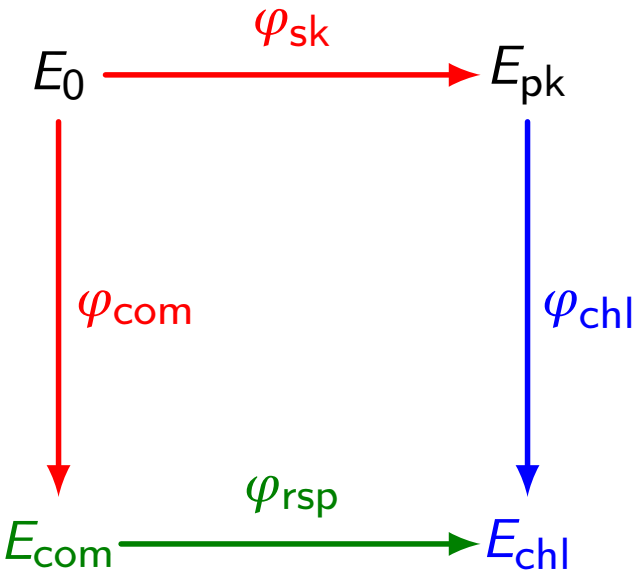
The SQIsign identification scheme



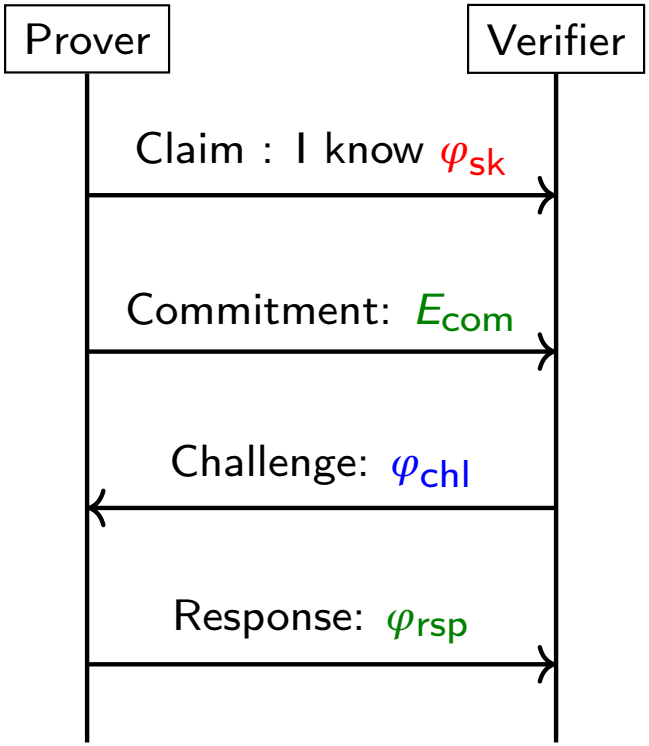
public
Prover's secret
published by Verifier
published by Prover



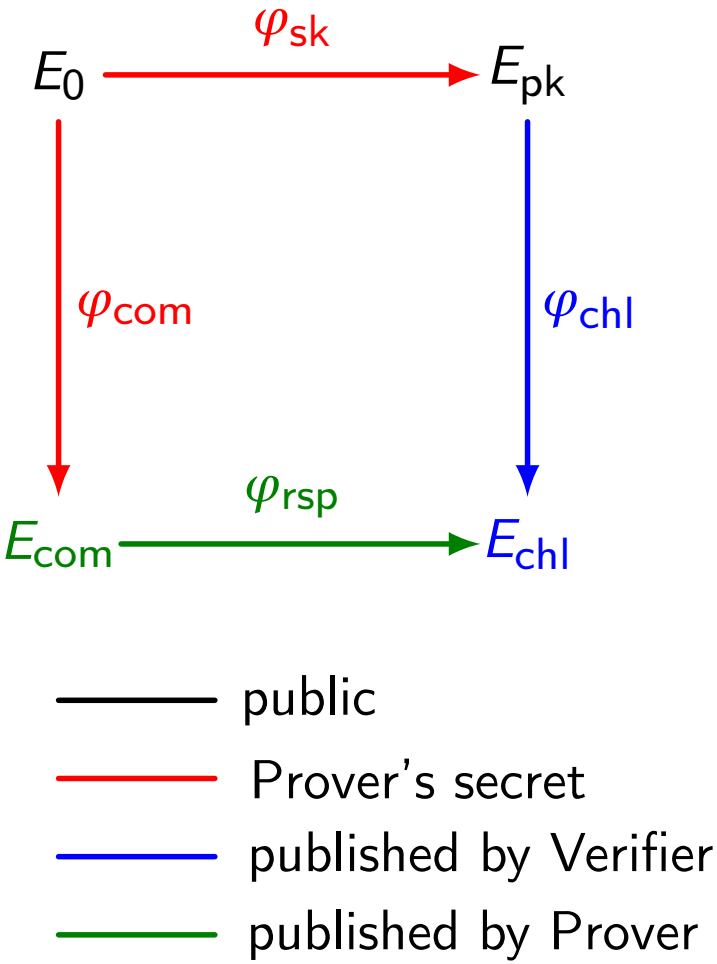
The SQIsign identification scheme

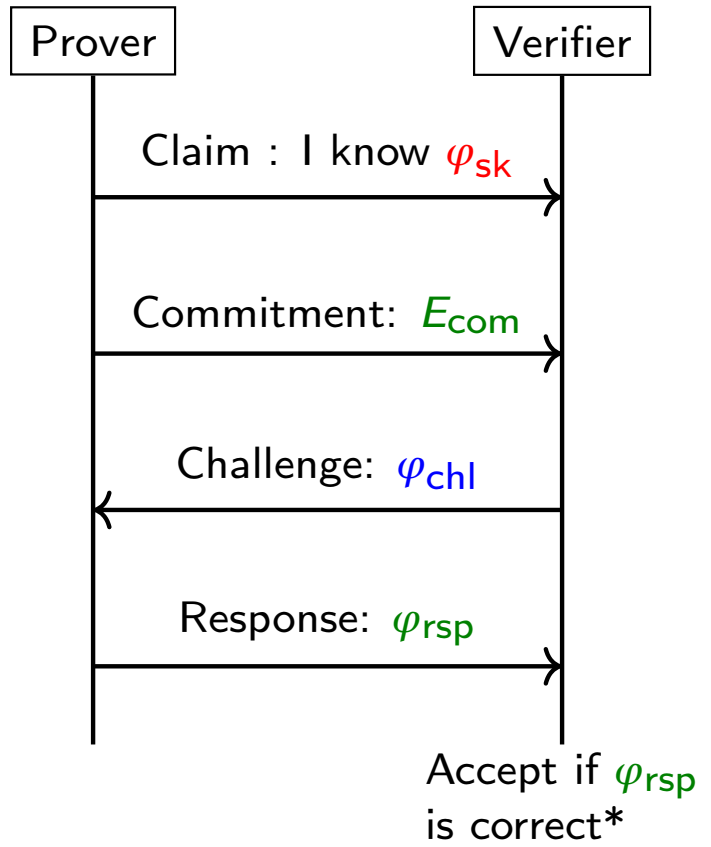


public
Prover's secret
published by Verifier
published by Prover



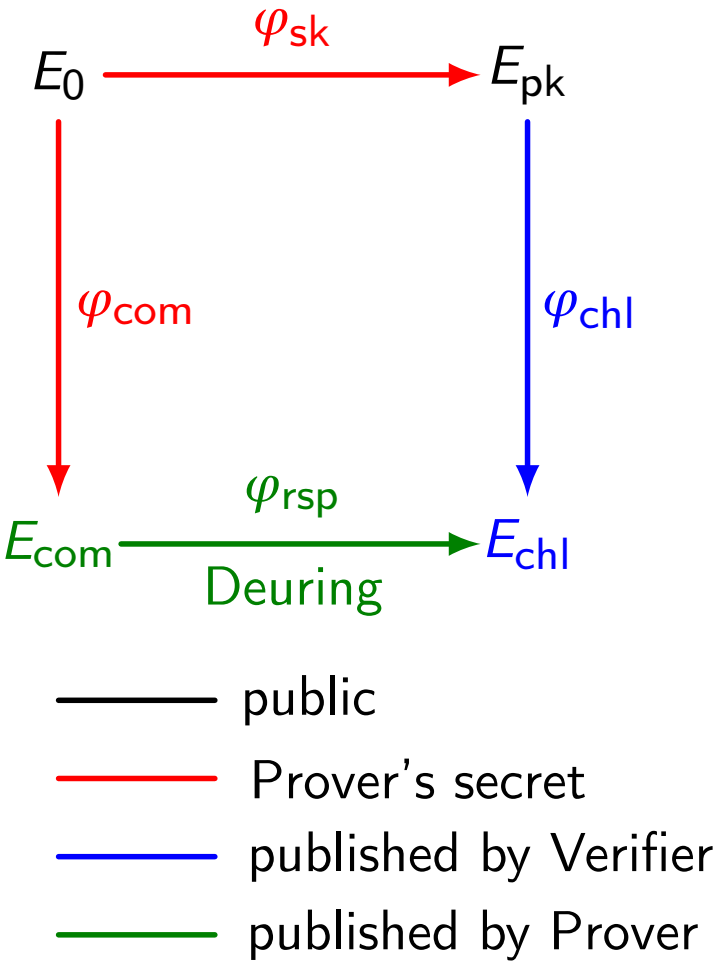
The SQIsign identification scheme

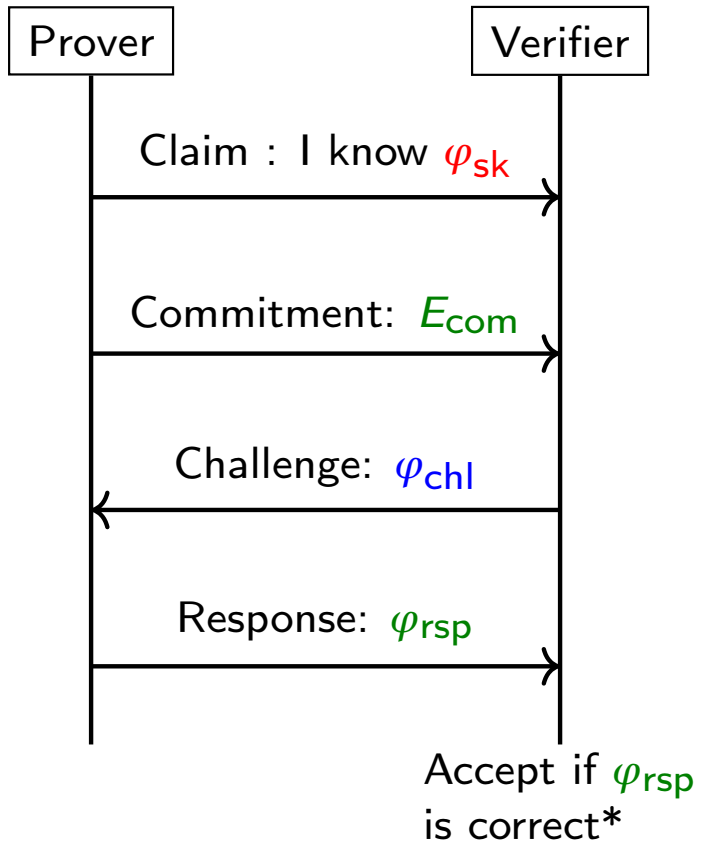




*φ_{rsp} should not factor through φ_{chl}.

The SQIsign identification scheme





*φ_{rsp} should not factor through φ_{chl}.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathsf{com}})$ and $\mathrm{End}(E_{\mathsf{chl}})$ and we want an isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \longrightarrow E_{\mathsf{chl}}$.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathrm{com}})$ and $\mathrm{End}(E_{\mathrm{chl}})$ and we want an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{com}} \longrightarrow E_{\mathrm{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- Compute a connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- Compute $J \sim I$ random with constraints on $\mathrm{nrd}(J)$.
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathrm{com}})$ and $\mathrm{End}(E_{\mathrm{chl}})$ and we want an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{com}} \longrightarrow E_{\mathrm{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- Compute a connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- Compute $J \sim I$ random with constraints on $\mathrm{nrd}(J)$.
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathrm{com}})$ and $\mathrm{End}(E_{\mathrm{chl}})$ and we want an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{com}} \longrightarrow E_{\mathrm{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- Compute a connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- Compute $J \sim I$ random with constraints on $\mathrm{nrd}(J)$.
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

✓ Becomes hard when $\mathrm{End}(E_1)$ or $\mathrm{End}(E_2)$ is unknown.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathrm{com}})$ and $\mathrm{End}(E_{\mathrm{chl}})$ and we want an isogeny $\varphi_{\mathrm{rsp}} : E_{\mathrm{com}} \longrightarrow E_{\mathrm{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

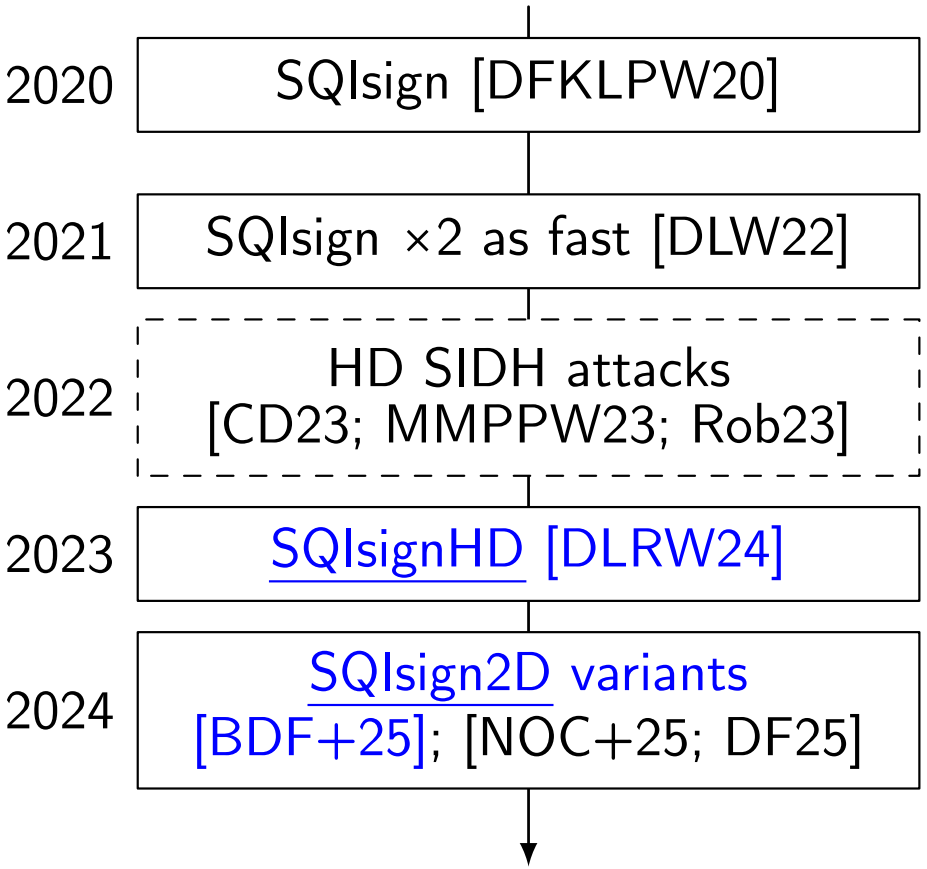
- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- Compute a connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- Compute $J \sim I$ random with constraints on $\mathrm{nrd}(J)$.
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

✓ Becomes hard when $\mathrm{End}(E_1)$ or $\mathrm{End}(E_2)$ is unknown.

⚠ Efficiency of the translation.

A brief history of SQIsign



1D Ideal to Isogeny

Enhanced 1D Ideal to Isogeny

Introduction of HD isogenies in cryptology

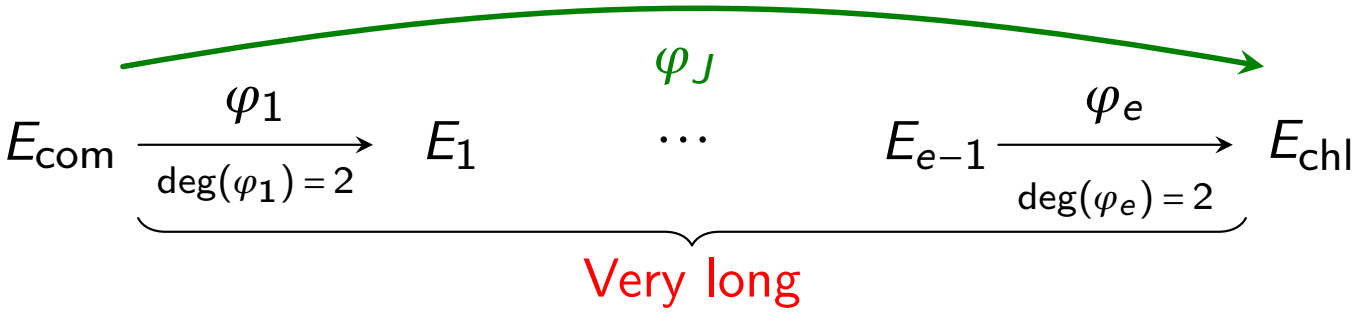
4D Ideal to Isogeny (verif)

2D Ideal to Isogeny (sign & verif)

In blue: our contributions

Ideal to isogeny translation: the HD breakthrough

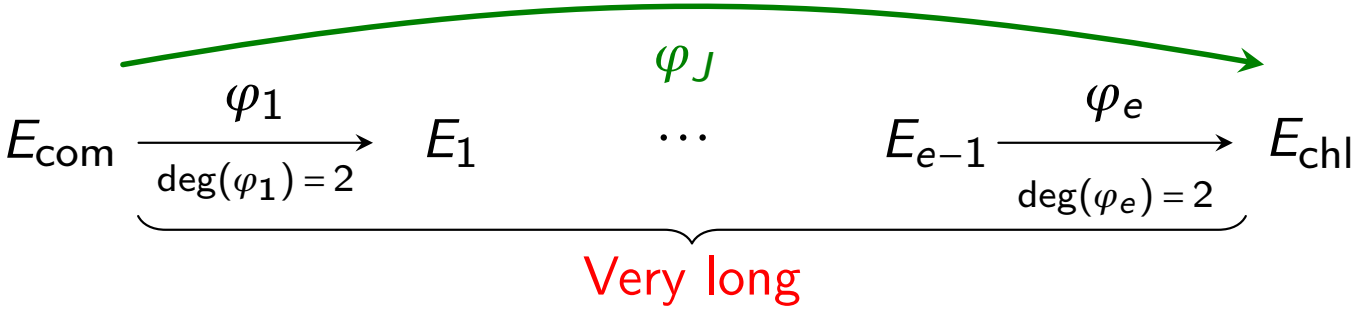
- **In SQIsign v1.0:** $\mathrm{nrd}(J) = 2^e$ very big



⚠ Very slow translation (response).

Ideal to isogeny translation: the HD breakthrough

- **In SQIsign v1.0:** $\mathrm{nrd}(J) = 2^e$ very big



⚠ Very slow translation (response).

- **In SQIsignHD/2D:** $\mathrm{nrd}(J)$ small (but not smooth)

Response

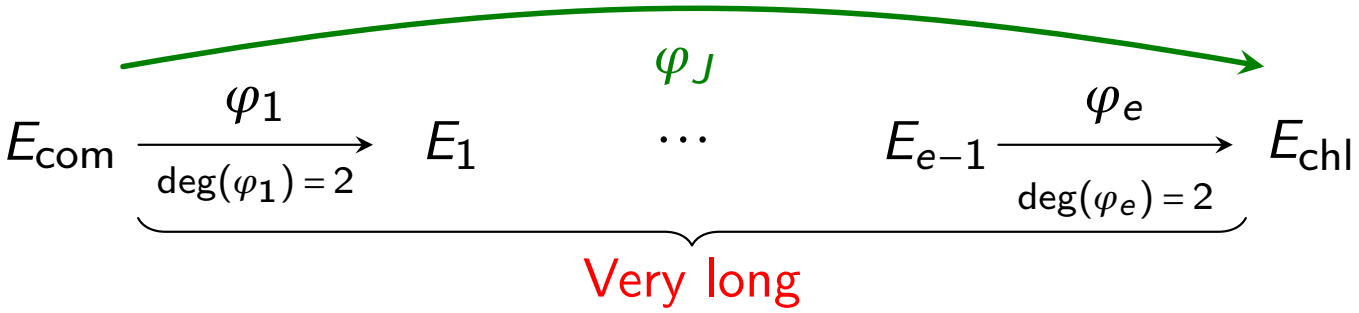
P, Q

$\varphi_J(P, Q)$

✓ Fast

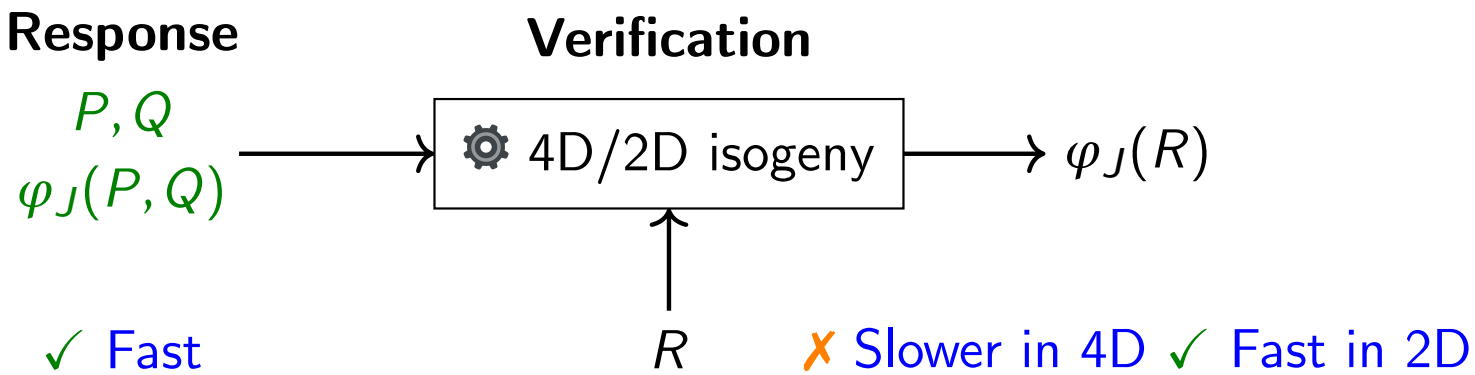
Ideal to isogeny translation: the HD breakthrough

- **In SQIsign v1.0:** $\mathrm{nrd}(J) = 2^e$ very big



⚠ Very slow translation (response).

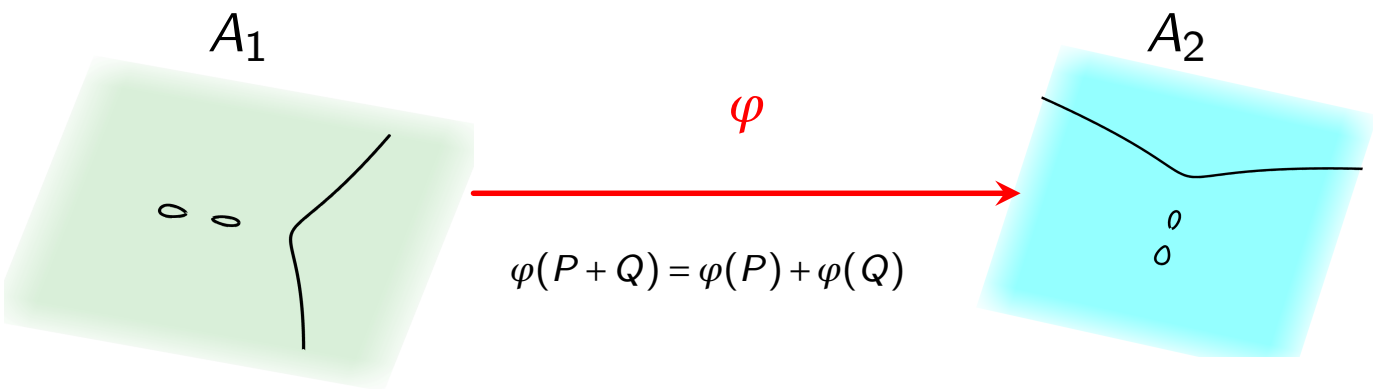
- **In SQIsignHD/2D:** $\mathrm{nrd}(J)$ small (but not smooth)



New dimensions in cryptography

Isogenies between abelian varieties

- Abelian varieties are projective abelian group varieties, generalizing elliptic curves.
  Example: $E_1 \times E_2$ is an abelian variety of dimension 2.
- Between abelian varieties, isogenies are morphisms which are surjective and of finite kernel.



An isogeny between abelian surfaces

n-isogenies in higher dimension and their degree

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.

n-isogenies in higher dimension and their degree

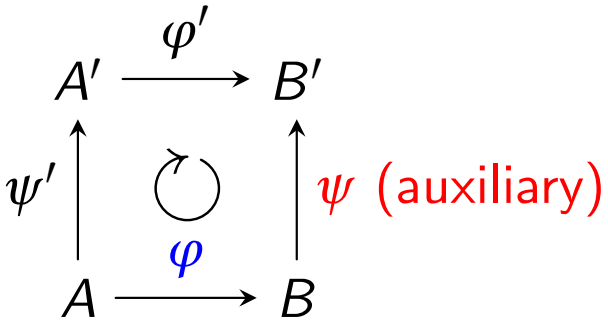
- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.
- φ is an n-isogeny if $\widetilde{\varphi} \circ \varphi = [n]$. We then denote $\deg_p(\varphi) := n$.

n-isogenies in higher dimension and their degree

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.
- φ is an n-isogeny if $\widetilde{\varphi} \circ \varphi = [n]$. We then denote $\deg_p(\varphi) := n$.
- ⚠ If φ is an n-isogeny, $\deg(\varphi) = n^{\dim(A)} = \deg_p(\varphi)^{\dim(A)}$.
- ⚠ Not all isogenies are n-isogenies ($\deg_p(\varphi)$ is not always defined) in dimension > 1.

Kani's lemma [Kan97]

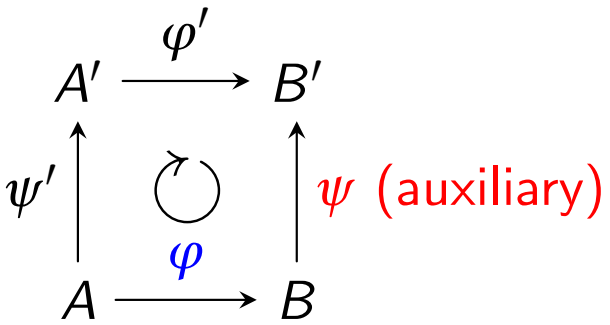
- Consider the commutative diagram:



with $\deg_p(\varphi) = \deg_p(\varphi') = q$
and $\deg_p(\psi) = \deg_p(\psi') = r$.

Kani's lemma [Kan97]

- Consider the commutative diagram:



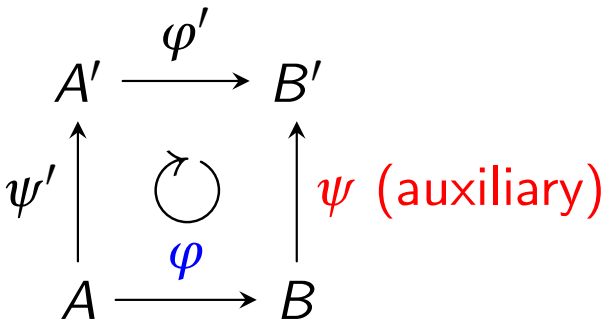
  with $\deg_p(\varphi) = \deg_p(\varphi') = q$ and $\deg_p(\psi) = \deg_p(\psi') = r$.
- Assume that $\gcd(q, r) = 1$ and $q + r = 2^e$.
- Then

$$F := \begin{pmatrix} \varphi & \widetilde{\psi} \\ -\psi' & \widetilde{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

$\deg_p(F) = q + r = 2^e$, *i.e.* $\widetilde{F} \circ F = [2^e]$.

Kani's lemma [Kan97]

- Consider the commutative diagram:



  with $\deg_p(\varphi) = \deg_p(\varphi') = q$ and $\deg_p(\psi) = \deg_p(\psi') = r$.

- Assume that $\gcd(q, r) = 1$ and $q + r = 2^e$.

- Then

$$F := \begin{pmatrix} \varphi & \widetilde{\psi} \\ -\psi' & \widetilde{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

  $\deg_p(F) = q + r = 2^e$, *i.e.* $\widetilde{F} \circ F = [2^e]$.

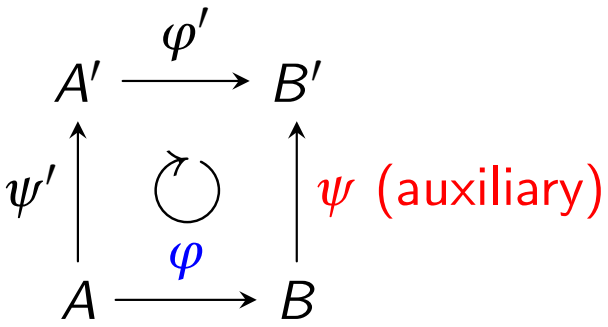
- Its kernel is:

$$\ker(F) = \{([q]P, \psi \circ \varphi(P)) \mid P \in A[2^e]\},$$

  so F can be computed from q and $\psi \circ \varphi(A[2^e])$.

Kani's lemma [Kan97]

- Consider the commutative diagram:



  with $\deg_p(\varphi) = \deg_p(\varphi') = q$ and $\deg_p(\psi) = \deg_p(\psi') = r$.
- Assume that $\gcd(q, r) = 1$ and $q + r = 2^e$.
- Then

$$F := \begin{pmatrix} \varphi & \widetilde{\psi} \\ -\psi' & \widetilde{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

  $\deg_p(F) = q + r = 2^e$, *i.e.* $\widetilde{F} \circ F = [2^e]$.
- Its kernel is:

$$\ker(F) = \{([q]P, \psi \circ \varphi(P)) \mid P \in A[2^e]\},$$

  so F can be computed from q and $\psi \circ \varphi(A[2^e])$.
- F **efficiently represents** φ:

$$F(P, 0) = (\varphi(P), -\psi'(P)).$$

SQIsignHD - verifying in dimension 4

Goal: Compute $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.

Input: Ideal I connecting $\mathcal{O}_1 \simeq \mathsf{End}(E_{\mathsf{com}})$ and $\mathcal{O}_2 \simeq \mathsf{End}(E_{\mathsf{chl}})$.

SQIsignHD - verifying in dimension 4

Goal: Compute $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.

Input: Ideal I connecting $\mathcal{O}_1 \simeq \mathsf{End}(E_{\mathsf{com}})$ and $\mathcal{O}_2 \simeq \mathsf{End}(E_{\mathsf{chl}})$.

The response/signature:

- Solve $\mathsf{nrd}(J) + a_1^2 + a_2^2 = 2^e$ for $J \sim I$ and $a_1, a_2 \in \mathbb{Z}$.
- Compute the image $(\varphi_J(P), \varphi_J(Q))$ of a basis (P, Q) of $E_{\mathsf{com}}[2^e] \simeq (\mathbb{Z}/2^e\mathbb{Z})^2$ (easy by Deuring).

SQIsignHD - verifying in dimension 4

Goal: Compute $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \to E_{\mathsf{chl}}$.

Input: Ideal I connecting $\mathcal{O}_1 \simeq \mathrm{End}(E_{\mathsf{com}})$ and $\mathcal{O}_2 \simeq \mathrm{End}(E_{\mathsf{chl}})$.

The response/signature:

- Solve $\mathrm{nrd}(J) + a_1^2 + a_2^2 = 2^e$ for $J \sim I$ and $a_1, a_2 \in \mathbb{Z}$.
- Compute the image $(\varphi_J(P), \varphi_J(Q))$ of a basis (P, Q) of $E_{\mathsf{com}}[2^e] \simeq (\mathbb{Z}/2^e\mathbb{Z})^2$ (easy by Deuring).

The verification: Apply Kani's lemma to:

- $\Phi := \mathrm{Diag}(\varphi_J, \varphi_J)$ with $\deg_p(\Phi) = \mathrm{nrd}(J)$.
- The auxiliary isogeny:

$$\Psi := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} : E_{\mathsf{chl}}^2 \to E_{\mathsf{chl}}^2,$$

with $\deg_p(\Psi) = a_1^2 + a_2^2$.

$$\begin{array}{ccc} E_{\mathsf{com}}^2 & \xrightarrow{\Phi'} & E_{\mathsf{chl}}^2 \\ {\scriptstyle\Psi'}\uparrow & \circlearrowright & \uparrow{\scriptstyle\Psi} \\ E_{\mathsf{com}}^2 & \xrightarrow{\Phi} & E_{\mathsf{chl}}^2 \end{array}$$

SQIsignHD - verifying in dimension 4

The verificarion:

- By Kani's lemma,

$$F := \begin{pmatrix} \Phi & \widetilde{\Psi} \\ -\Psi' & \widetilde{\Phi'} \end{pmatrix} := \begin{pmatrix} a_1 & -a_2 & \widehat{\varphi}_J & 0 \\ a_2 & a_1 & 0 & \widehat{\varphi}_J \\ -\varphi_J & 0 & a_1 & a_2 \\ 0 & -\varphi_J & -a_2 & a_1 \end{pmatrix} : E_{\text{com}}^2 \times E_{\text{chl}}^2 \to E_{\text{com}}^2 \times E_{\text{chl}}^2$$

satisfies $\deg_p(F) = \text{nrd}(J) + a_1^2 + a_2^2 = 2^e$.

SQIsignHD - verifying in dimension 4

The verificarion:

- By Kani's lemma,

$$F := \begin{pmatrix} \Phi & \widetilde{\Psi} \\ -\Psi' & \widetilde{\Phi'} \end{pmatrix} := \begin{pmatrix} a_1 & -a_2 & \widehat{\varphi}_J & 0 \\ a_2 & a_1 & 0 & \widehat{\varphi}_J \\ -\varphi_J & 0 & a_1 & a_2 \\ 0 & -\varphi_J & -a_2 & a_1 \end{pmatrix} : E_{\text{com}}^2 \times E_{\text{chl}}^2 \to E_{\text{com}}^2 \times E_{\text{chl}}^2$$

  satisfies $\deg_p(F) = \text{nrd}(J) + a_1^2 + a_2^2 = 2^e$.
- $\ker(F)$ can be computed with input data $a_1, a_2, P, Q, \varphi_J(P), \varphi_J(Q)$.
- Since $\deg_p(F) = 2^e$, to compute F, we decompose

$$E_{\text{com}}^2 \times E_{\text{chl}}^2 \xrightarrow{F_1} A_1 \quad \overset{F}{\cdots} \quad A_{e-1} \xrightarrow{F_e} E_{\text{com}}^2 \times E_{\text{chl}}^2$$

SQIsignHD - verifying in dimension 4

The verificarion:

- By Kani's lemma,

$$F := \begin{pmatrix} \Phi & \widetilde{\Psi} \\ -\Psi' & \widetilde{\Phi'} \end{pmatrix} := \begin{pmatrix} a_1 & -a_2 & \widehat{\varphi}_J & 0 \\ a_2 & a_1 & 0 & \widehat{\varphi}_J \\ -\varphi_J & 0 & a_1 & a_2 \\ 0 & -\varphi_J & -a_2 & a_1 \end{pmatrix} : E_{\text{com}}^2 \times E_{\text{chl}}^2 \to E_{\text{com}}^2 \times E_{\text{chl}}^2$$

  satisfies $\deg_p(F) = \text{nrd}(J) + a_1^2 + a_2^2 = 2^e$.
- $\ker(F)$ can be computed with input data $a_1, a_2, P, Q, \varphi_J(P), \varphi_J(Q)$.
- Since $\deg_p(F) = 2^e$, to compute F, we decompose

$$E_{\text{com}}^2 \times E_{\text{chl}}^2 \xrightarrow{F_1} A_1 \quad \overset{F}{\cdots} \quad A_{e-1} \xrightarrow{F_e} E_{\text{com}}^2 \times E_{\text{chl}}^2$$

- To check F represents φ_J correctly, evaluate:

$$F(R,0,0,0) = ([a_1]R, -[a_2]R, -\varphi_J(R), 0)$$

SQIsign2D - verifying in dimension 2

SQIsignHD trade-off:

✓ Very fast signing/response.

✗ Slower verification (4D).

SQIsign2D - verifying in dimension 2

SQIsignHD trade-off:

✓ Very fast signing/response.

✗ Slower verification (4D).

The solution: SQIsign2D(-West)

- **Issue:** we need an auxiliary isogeny $\psi : E_{\mathsf{chl}} \to E_{\mathsf{aux}}$ of degree $2^e - \mathrm{nrd}(J)$.

$$F := \begin{pmatrix} \varphi_J & \widetilde{\psi} \\ -\psi' & \widetilde{\varphi}' \end{pmatrix} : E_{\mathsf{com}} \times E_{\mathsf{aux}} \to E_{\mathsf{chl}} \times E'$$

- $\ker(F)$ depends on $\mathrm{nrd}(J), P, Q, \psi \circ \varphi_J(P), \psi \circ \varphi_J(Q)$, where (P, Q) is a basis of $E_{\mathsf{com}}[2^e] \simeq (\mathbb{Z}/2^e\mathbb{Z})^2$.
- **Response:** $\psi \circ \varphi_J(P), \psi \circ \varphi_J(Q)$ trickier to compute (2D computation).

The HD trade-off

SQIsign v1.0

Response of smooth and very big degree $\deg(\varphi_{\mathsf{rsp}}) = 2^e$.

VS

SQIsignHD/2D

Response of non-smooth smaller degree $\deg(\varphi_{\mathsf{rsp}})$.

component of

Smooth and small polarised degree HD isogeny.

SQIsign is very compact

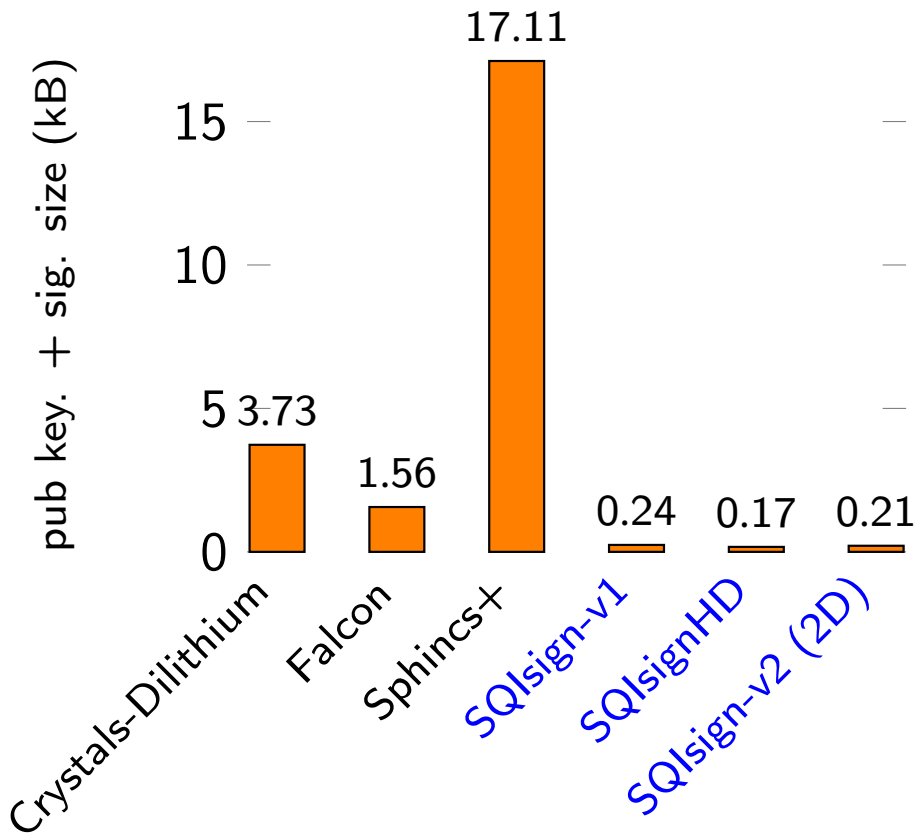


Figure: Compacity of SQIsign and other post-quantum digital signatures standardised by NIST.

In black, standardised post-quantum schemes:

- Crystals-Dilithium (lattices)
- Falcon (lattices)
- Sphincs+ (hash)

In blue, variants of SQIsign.

SQIsign is getting faster

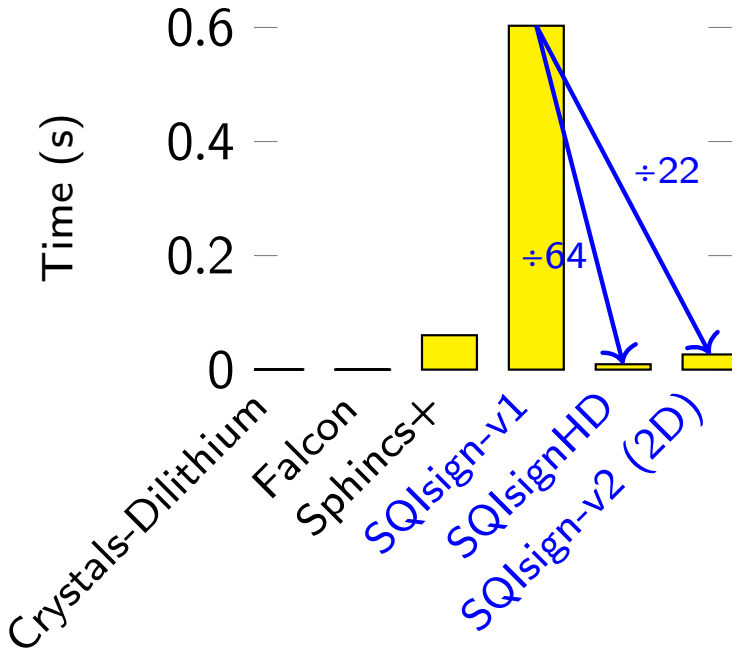


Figure: **Signing** time of SQIsign and post-quantum digital signatures standardised by NIST an a 2.3 GHz CPU.

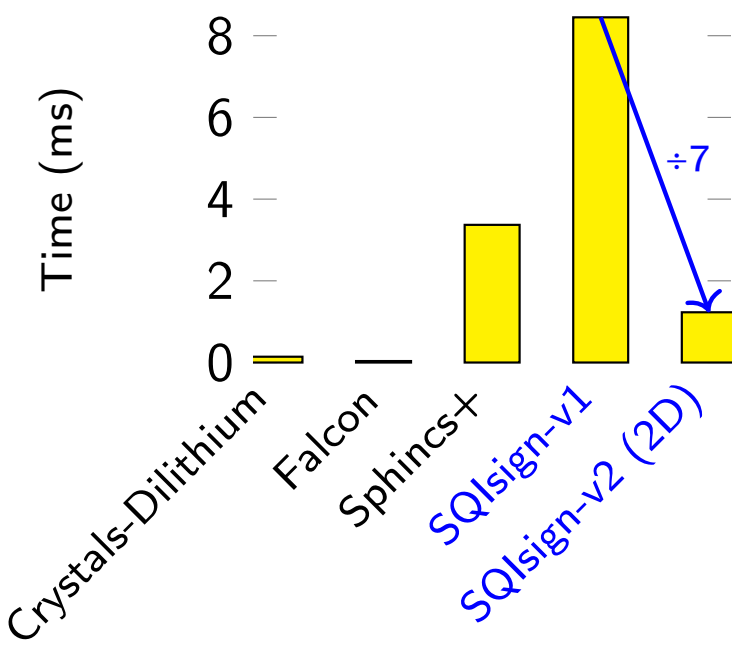


Figure: **Verification** time of SQIsign and post-quantum digital signatures standardised by NIST an a 2.3 GHz CPU.

Computing higher dimensional isogenies

Relies on Mumford's theta coordinates theory (1966).

Contributions:

- **In 2D:** Pierrick Dartois, Luciano Maino, Giacomo Pope and Damien Robert, "An Algorithmic Approach to (2,2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography", In **ASIACRYPT 2024**.
- **In 4D:** Pierrick Dartois, "Fast computation of 2-isogenies in dimension 4 and cryptographic applications", In **Journal of Algebra**, Volume 683, December 2025.
- **In 4D:** Pierrick Dartois and Max Duparc. "Chasing Rabbits Through Hypercubes: Better algorithms for higher dimensional 2-isogeny computations." Accepted at ANTS 2026.

In blue, contributions of this PhD.

From quaternionic to quadratic ideal action

Idea: Let E be a supersingular elliptic curve.

- Consider a 2-dimensional subring $\mathfrak{O} \hookrightarrow \mathrm{End}(E)$.
- A quadratic ideal $\mathfrak{a} \subseteq \mathfrak{O}$ corresponds to an isogeny $\varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$.

From quaternionic to quadratic ideal action

Idea: Let E be a supersingular elliptic curve.

- Consider a 2-dimensional subring $\mathfrak{O} \hookrightarrow \mathrm{End}(E)$.
- A quadratic ideal $\mathfrak{a} \subseteq \mathfrak{O}$ corresponds to an isogeny $\varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$.

Goal: compute the action of **any** quadratic ideal $\mathfrak{a} \subseteq \mathfrak{O}$.

From quaternionic to quadratic ideal action

Idea: Let E be a supersingular elliptic curve.

- Consider a 2-dimensional subring $\mathfrak{O} \hookrightarrow \mathrm{End}(E)$.
- A quadratic ideal $\mathfrak{a} \subseteq \mathfrak{O}$ corresponds to an isogeny $\varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$.

Goal: compute the action of **any** quadratic ideal $\mathfrak{a} \subseteq \mathfrak{O}$.

Solution: use 4-dimensional isogenies

- Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren and Benjamin Wesolowski, "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies", In **CRYPTO 2025**.
- Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi and Frederik Vercauteren. "qt-Pegasis: Simpler and Faster Effective Class Group Actions." In **EUROCRYPT 2026**.

The Module Isogeny Key Exchange (MIKE)

- Based on module action (generalising ideal action) on abelian varieties.
- Instantiation of MIKE use 4D isogenies.

The Module Isogeny Key Exchange (MIKE)

- Based on module action (generalising ideal action) on abelian varieties.
- Instantiation of MIKE use 4D isogenies.
- Some teaser can be found below:

Eurocrypt 2026 rump session, May 12, 2026.

Thank you for listening

- The curse of SIDH attacks turned into a miracle.
- These attacks led to multiple applications (*e.g.* SQIsign, Pegasis...).

Thank you for listening

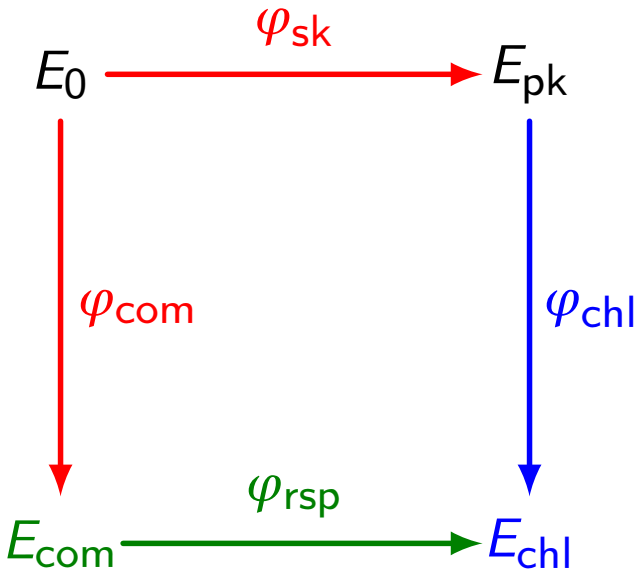
- The curse of SIDH attacks turned into a miracle.
- These attacks led to multiple applications (*e.g.* SQIsign, Pegasis...).

Future works:

- Focus on side channel proof implementation of SQIsign (NIST recommendation).
- Improve HD algorithms (*e.g.* Pegasis in 2D).

You can find my PhD manuscript here:

Response computation in SQIsignHD

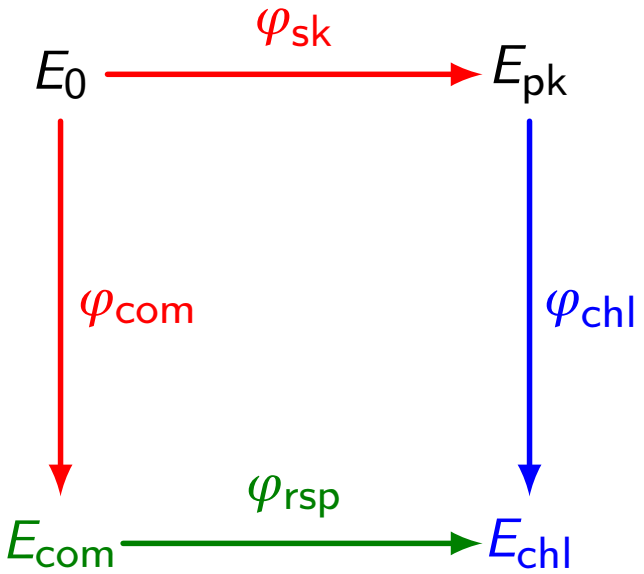


Goal: Translate J into $\varphi_{rsp} = \varphi_J$.

- Let $I := \bar{I}_{com} \cdot I_{sk} \cdot I_{chl}$.

public
Prover's secret
published by Verifier
published by Prover

Response computation in SQIsignHD

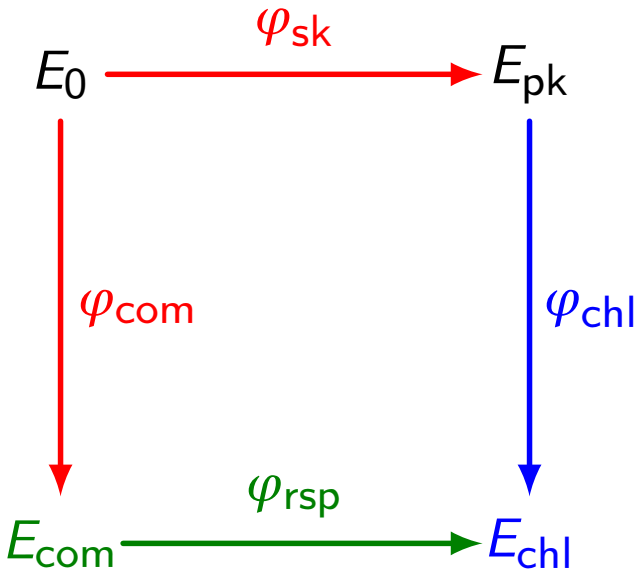


public
Prover's secret
published by Verifier
published by Prover

Goal: Translate J into $\varphi_{rsp} = \varphi_J$.

- Let $I := \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Then $J := I\overline{\alpha}/\mathrm{nrd}(I)$ for some $\alpha \in I$.
- And $\widehat{\varphi}_{com} \circ \widehat{\varphi}_{rsp} \circ \varphi_{chl} \circ \varphi_{sk} = \alpha$.

Response computation in SQIsignHD

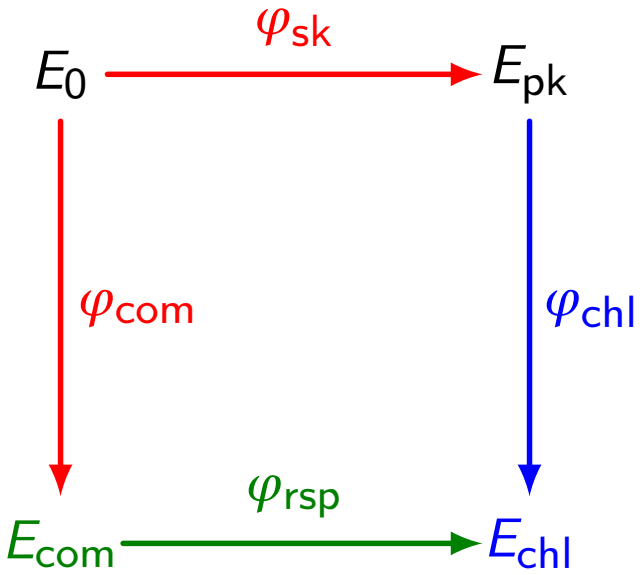


public
Prover's secret
published by Verifier
published by Prover

Goal: Translate J into $\varphi_{rsp} = \varphi_J$.

- Let $I := \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Then $J := I\overline{\alpha}/\mathrm{nrd}(I)$ for some $\alpha \in I$.
- And $\widehat{\varphi}_{com} \circ \widehat{\varphi}_{rsp} \circ \varphi_{chl} \circ \varphi_{sk} = \alpha$.
- Write $\deg(\varphi_{chl}) = 2^\lambda$.
- Let (P', Q') be a basis of $E_{com}[2^{e+\lambda}]$ and let $(P, Q) := [2^\lambda](P', Q')$.

Response computation in SQIsignHD



public
Prover's secret
published by Verifier
published by Prover

Goal: Translate J into $\varphi_{rsp} = \varphi_J$.

- Let $I := \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Then $J := I\overline{\alpha}/\mathrm{nrd}(I)$ for some $\alpha \in I$.
- And $\widehat{\varphi}_{com} \circ \widehat{\varphi}_{rsp} \circ \varphi_{chl} \circ \varphi_{sk} = \alpha$.
- Write $\deg(\varphi_{chl}) = 2^\lambda$.
- Let (P', Q') be a basis of $E_{com}[2^{e+\lambda}]$ and let $(P, Q) := [2^\lambda](P', Q')$.
- Then

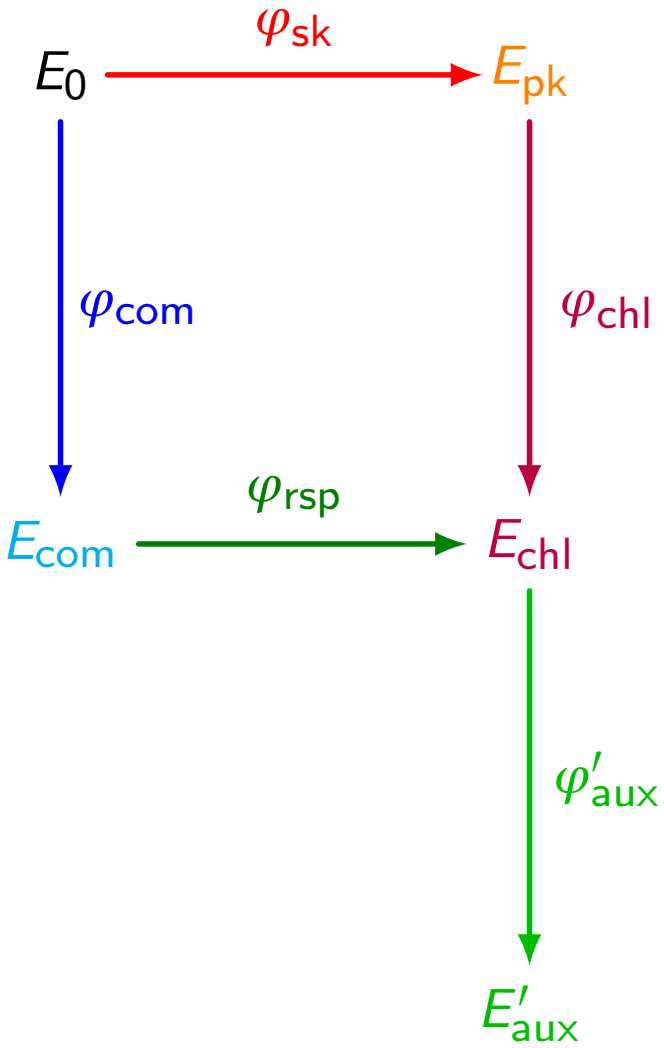
$$\varphi_{rsp}(P, Q) = [\mu]\varphi_{chl} \circ \varphi_{sk} \circ \widehat{\alpha} \circ \widehat{\varphi}_{com}(P', Q'),$$

with $\mu \equiv (\deg(\varphi_{com})\deg(\varphi_{sk}))^{-1} \bmod 2^e$.

Improvements of SQIsign security assumptions

	SQIsign	SQIsignHD	SQIsign2D
Soundness	The Endomorphism Ring Problem (strong)		
Zero knowledge	• Heuristic on the distribution of φ_{rsp}.	• An oracle returning "random" isogenies. • Heuristic on the distribution of E_{com} (uniform).	• 2 oracles returning "random" isogenies.

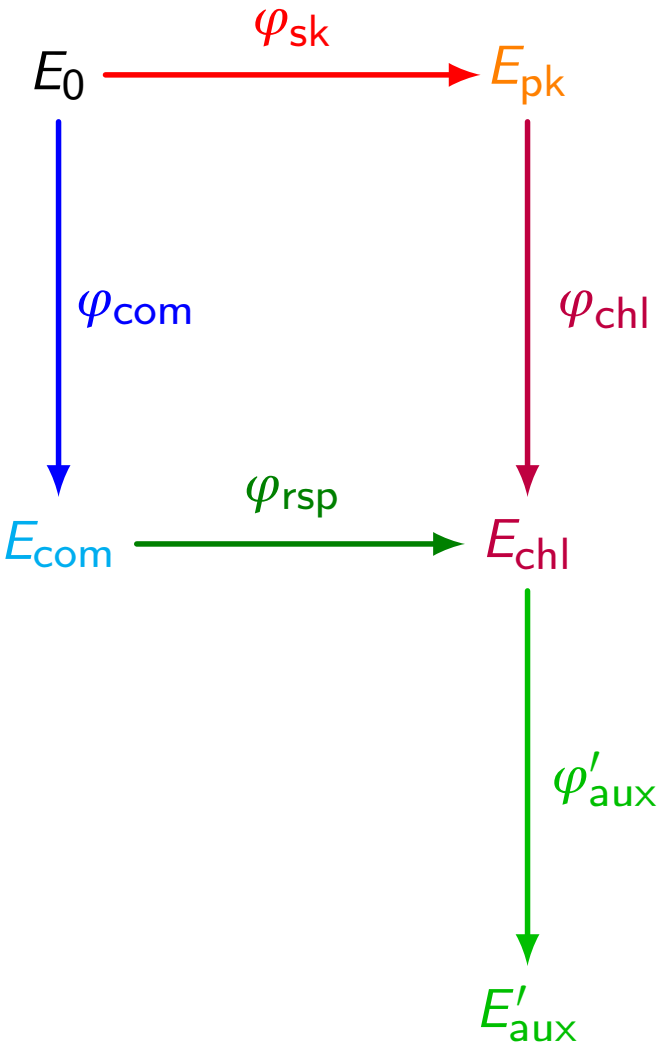
Response/signature



Response:

- Compute $I_{chl} \subset \mathrm{End}(E_{pk})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Compute $I_{rsp} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{aux} \subset \mathrm{End}(E_{chl})$ at random of norm $2^r - q$.
- Translate $I_{com} \cdot I_{rsp} \cdot I'_{aux}$ into $\varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}$.

Response/signature

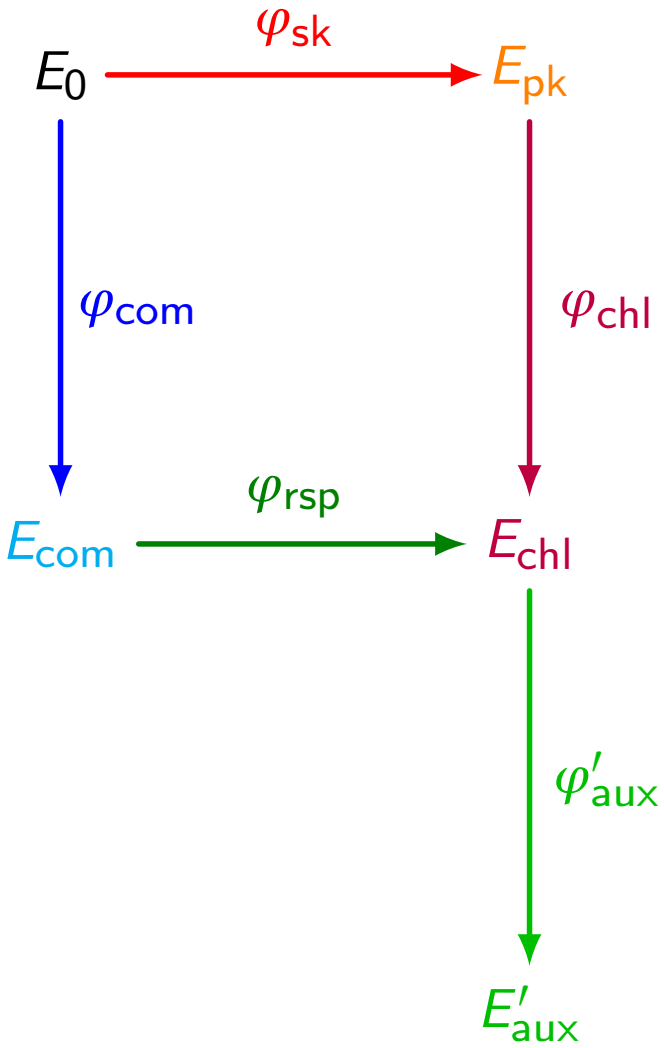


Response:

- Compute $I_{chl} \subset \mathrm{End}(E_{pk})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Compute $I_{rsp} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{aux} \subset \mathrm{End}(E_{chl})$ at random of norm $2^r - q$.
- Translate $I_{com} \cdot I_{rsp} \cdot I'_{aux}$ into $\varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}$.

✓ Starting from E_0.

Response/signature



Response:

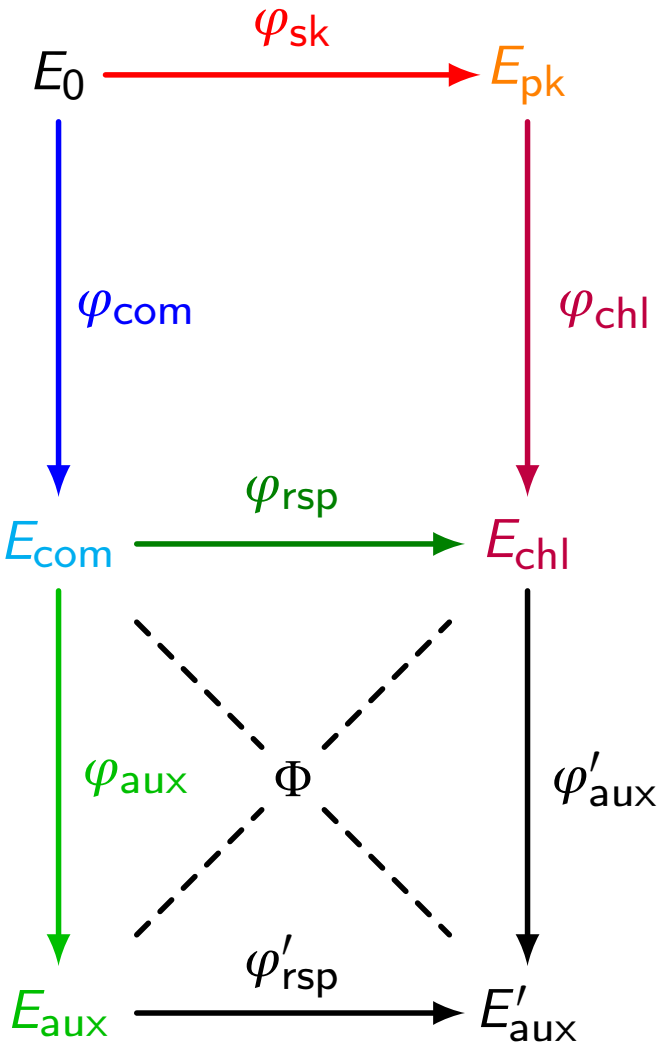
- Compute $I_{chl} \subset \mathrm{End}(E_{pk})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Compute $I_{rsp} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{aux} \subset \mathrm{End}(E_{chl})$ at random of norm $2^r - q$.
- Translate $I_{com} \cdot I_{rsp} \cdot I'_{aux}$ into $\varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}$.

✓ Starting from E_0.

Signature: Could be

$$(E_{com}, E'_{aux}, \varphi'_{aux} \circ \varphi_{rsp}(E_{com}[2^r])).$$

Response/signature - commitment recoverability



Response/signature:

- Compute the $(2^r, 2^r)$-isogeny:

$$\Phi : E_{com} \times E'_{aux} \longrightarrow E_{chl} \times E_{aux}$$

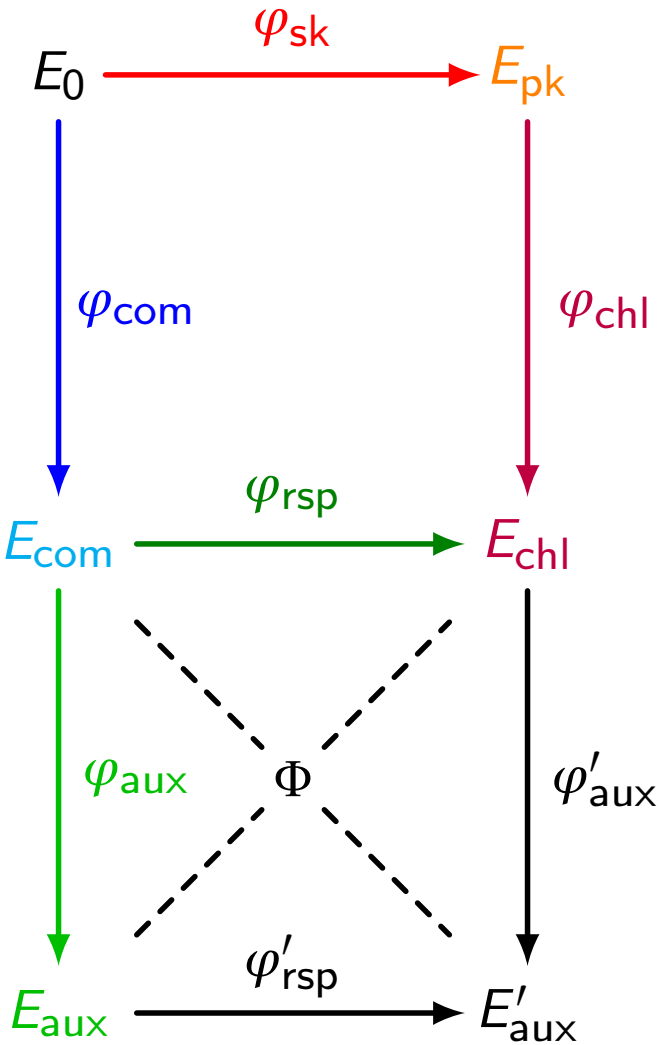
from $\varphi'_{aux} \circ \varphi_{rsp}(E_{com}[2^r])$.

- Evaluate Φ to compute $\varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])$.

Signature:

$$(E_{aux}, \varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])).$$

Verification



Verification:

- Compute the $(2^r, 2^r)$-isogeny:

  $$\widehat{\Phi} : E_{chl} \times E_{aux} \longrightarrow E_{com} \times E'_{aux}$$

  from $\varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])$.
- Check its codomain is $E_{com} \times \_$.