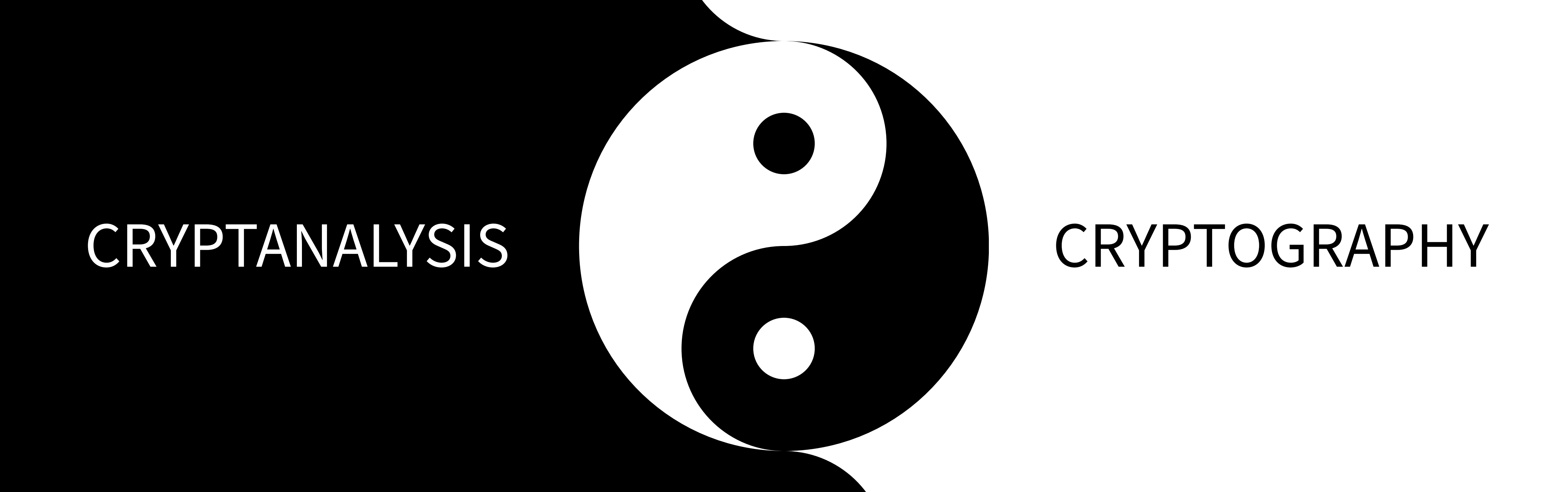
SQIsign
past, present and future

Luca De Feo
IBM Research Zürich

December 20, 2024
Indocrypt, Chennai, India


CRYPTANALYSIS
CRYPTOGRAPHY

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

2011 – Subexponential quantum attacks on group actions

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

2011 – Supersingular Isogeny Diffie-Hellman (SIDH)

2011 – Subexponential quantum attacks on group actions

2014 – Kohel-Lauter-Petit-Tignol algorithm (KLPT)

2017 – Torsion point attacks on SIDH

2018-2021 – Equivalence of EndRing and IsogenyPath

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

2011 – Supersingular Isogeny Diffie-Hellman (SIDH)

2011 – Subexponential quantum attacks on group actions

2014 – Kohel-Lauter-Petit-Tignol algorithm (KLPT)

2017 – Torsion point attacks on SIDH

2018-2021 – Equivalence of EndRing and IsogenyPath

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

2011 – Supersingular Isogeny Diffie-Hellman (SIDH)

2019 – CSIDH: group action on supersingular curves

2020 – SQIsign (NIST signature candidate)

2011 – Subexponential quantum attacks on group actions

2014 – Kohel-Lauter-Petit-Tignol algorithm (KLPT)

2017 – Torsion point attacks on SIDH

2018-2021 – Equivalence of EndRing and IsogenyPath

2022 – SIDH attacks

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

2011 – Supersingular Isogeny Diffie-Hellman (SIDH) †

2019 – CSIDH: group action on supersingular curves

2020 – SQIsign (NIST signature candidate)

2011 – Subexponential quantum attacks on group actions

2014 – Kohel-Lauter-Petit-Tignol algorithm (KLPT)

2017 – Torsion point attacks on SIDH

2018-2021 – Equivalence of EndRing and IsogenyPath

2022 – SIDH attacks

2006 – CRS key exchange based on the CM group action

2006 – CGL hash function from supersingular curves

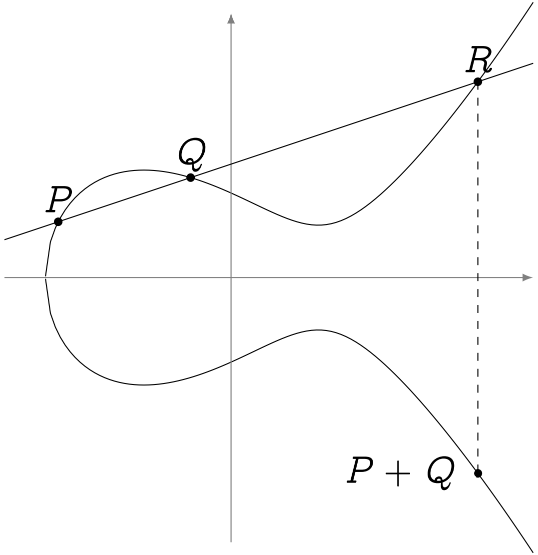
2011 – Supersingular Isogeny Diffie-Hellman (SIDH) †

2019 – CSIDH: group action on supersingular curves

2020 – SQIsign (NIST signature candidate)

2023 – SQIsignHD

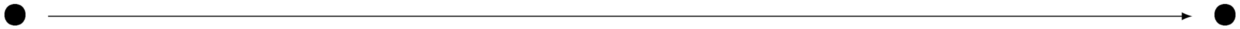
2024 – SQIsign2D

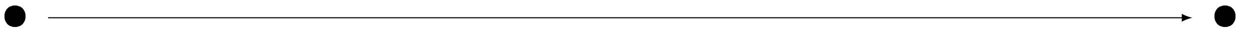


Isogenies = finite-kernel *algebraic* group morphisms of elliptic curves

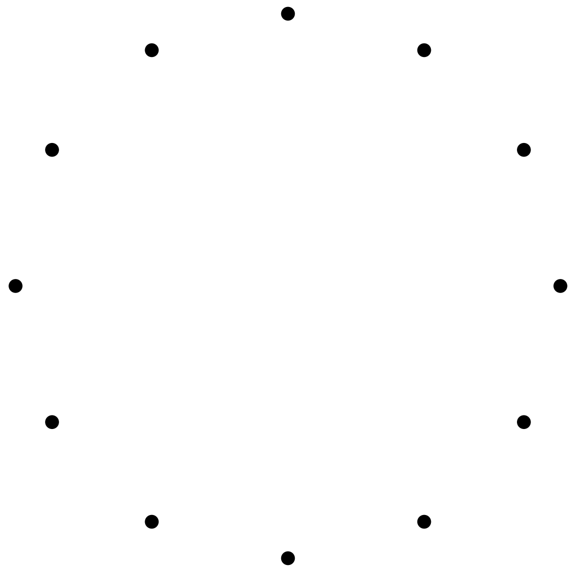
Endomorphisms = isogenies $E \to E$

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

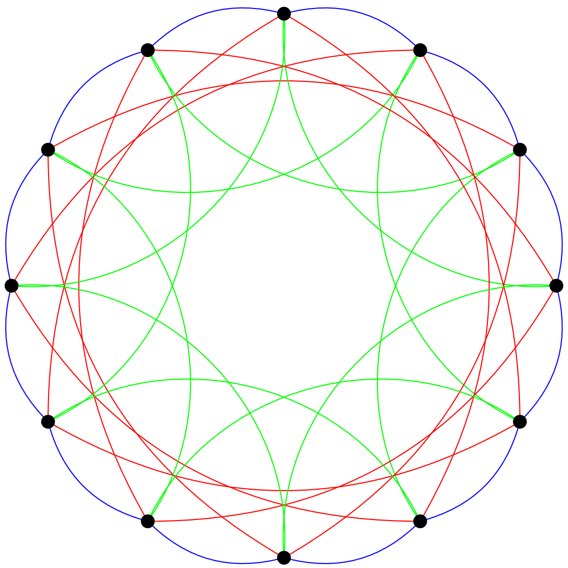




Isogenous



Isogeny class



Isogeny class

Isogeny graph

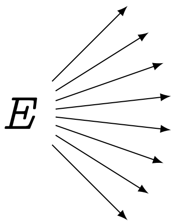
The isogeny problem

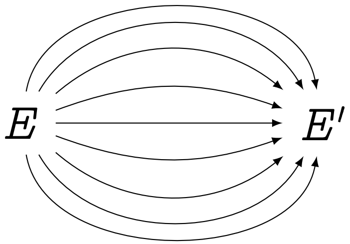
E $\qquad\qquad\qquad\qquad$ E'

The isogeny problem

$$E \xrightarrow{\quad ?? \quad} E'$$

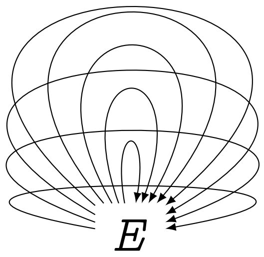
Isogeny Yantras





$\mathrm{Hom}(E, E')$

Ideal class



$\mathrm{End}(E)$

Order

Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

$$\begin{tikzcd} \bullet \arrow[r, bend left, "\varphi"] & \bullet \arrow[rr, bend left, "\psi"] & & \bullet \end{tikzcd}$$

- A measure of “size”;

Degree

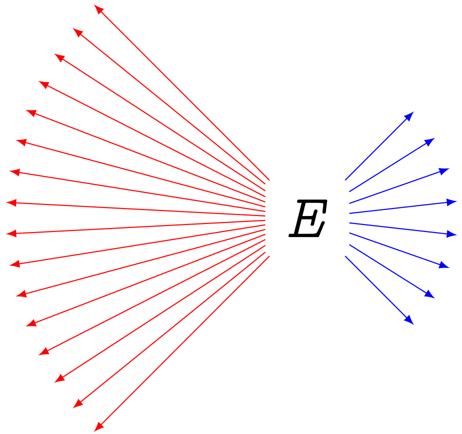
$$\deg(\varphi) \in \mathbb{N}^+$$

- A measure of "size";
- Multiplicative;

$$\bullet \xrightarrow{\varphi} \bullet \xrightarrow{\psi} \bullet$$

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

The larger the degree, the more isogenies



Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

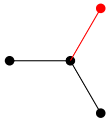
- A measure of “size”;
- Multiplicative;
- A measure of “complexity”:
  only isogenies of small degree fit into a computer!

$$\bullet \xrightarrow{\varphi} \bullet \xrightarrow{\psi} \bullet$$

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

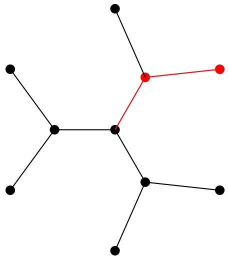
Isogenies of smooth degree

degree 2



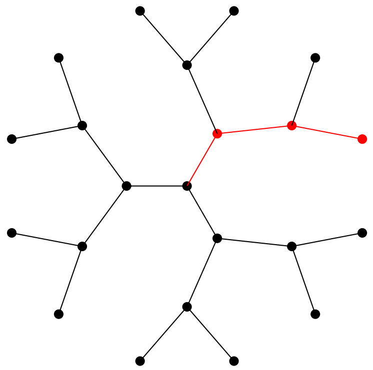
Isogenies of smooth degree

degree 4



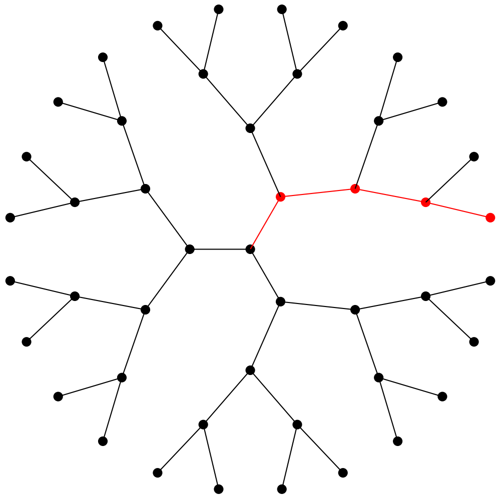
Isogenies of smooth degree

degree 8



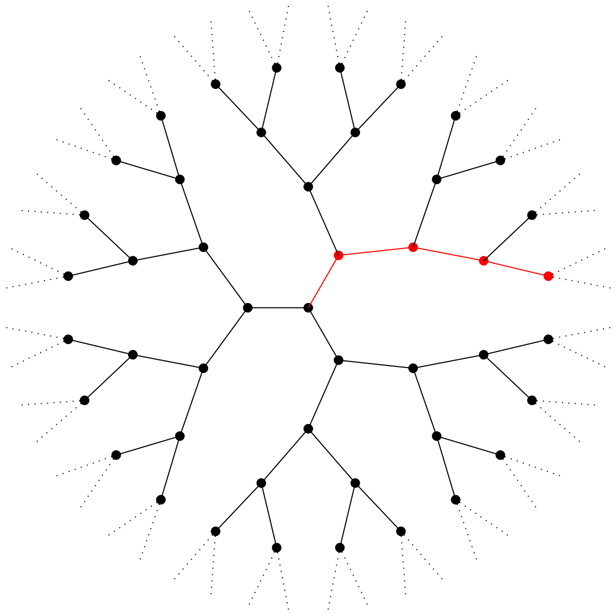
Isogenies of smooth degree

degree 16

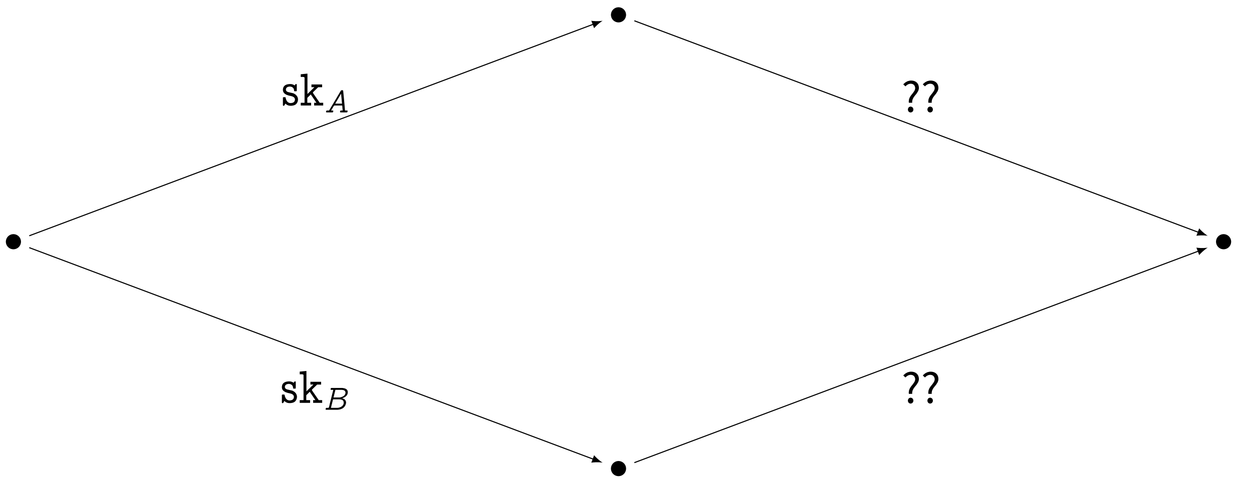


Isogenies of smooth degree

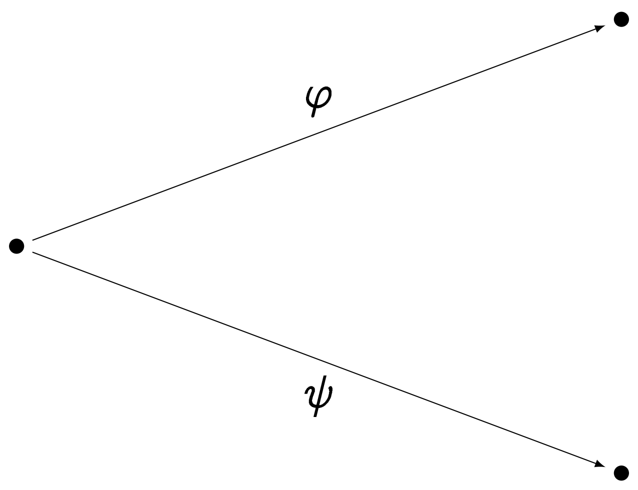
degree 2^x



Key exchange?

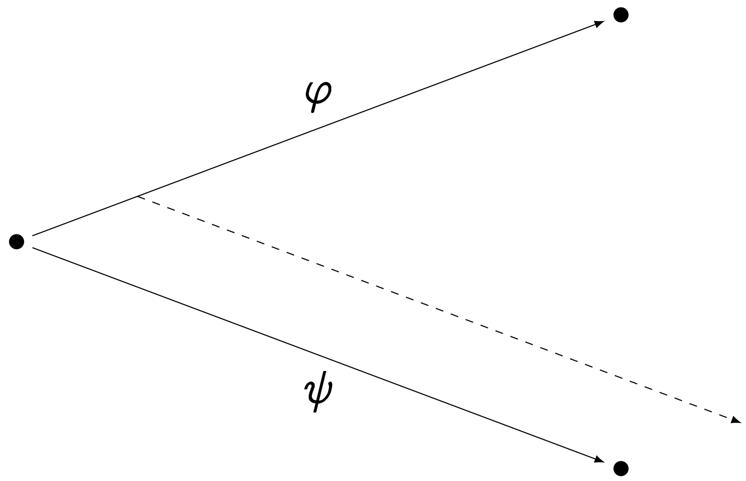


Push-forward



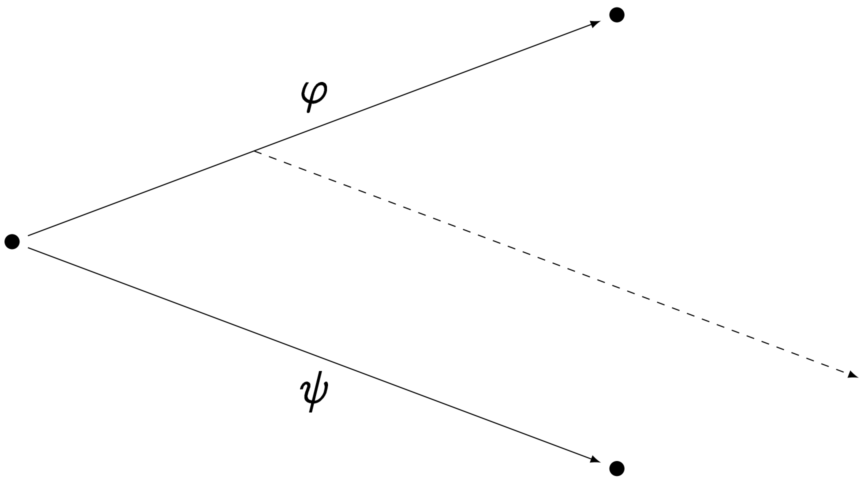
$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

Push-forward



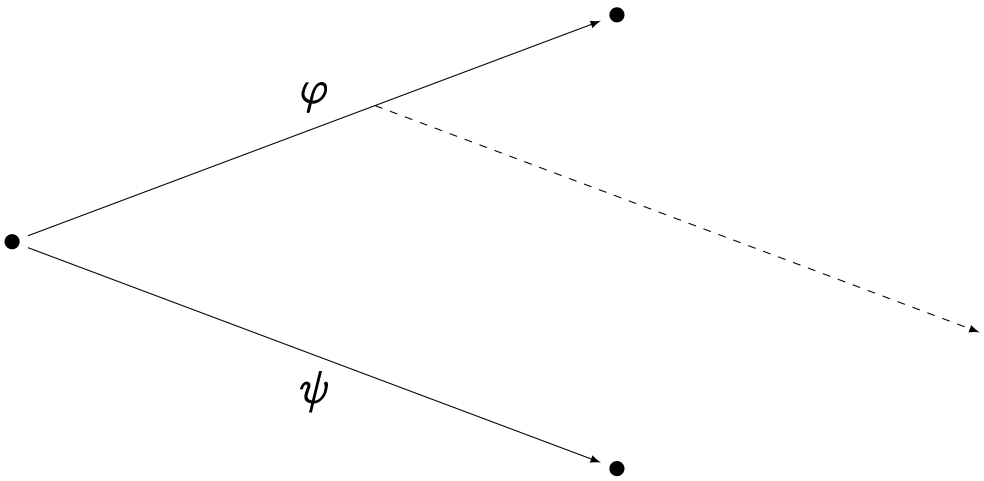
$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

Push-forward



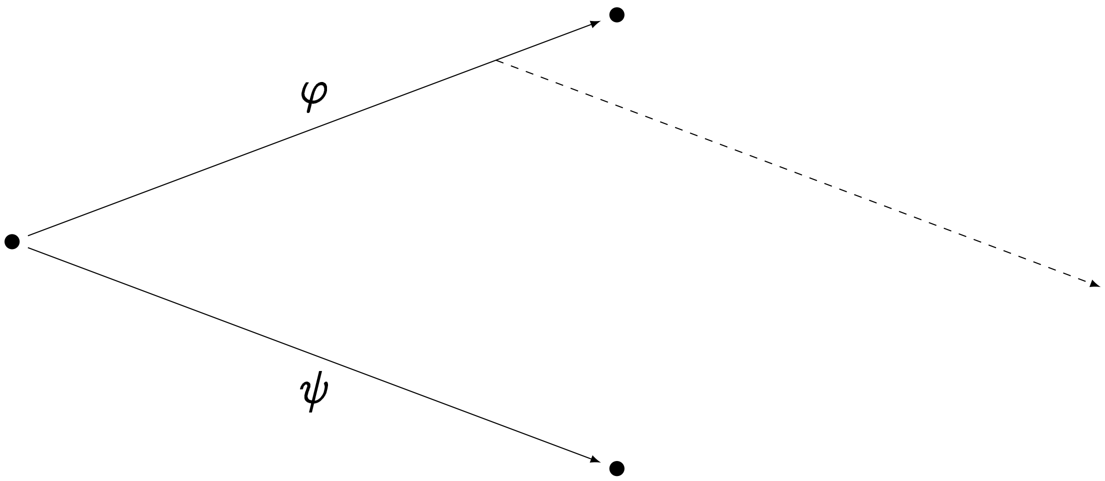
$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

Push-forward



$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

Push-forward



$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

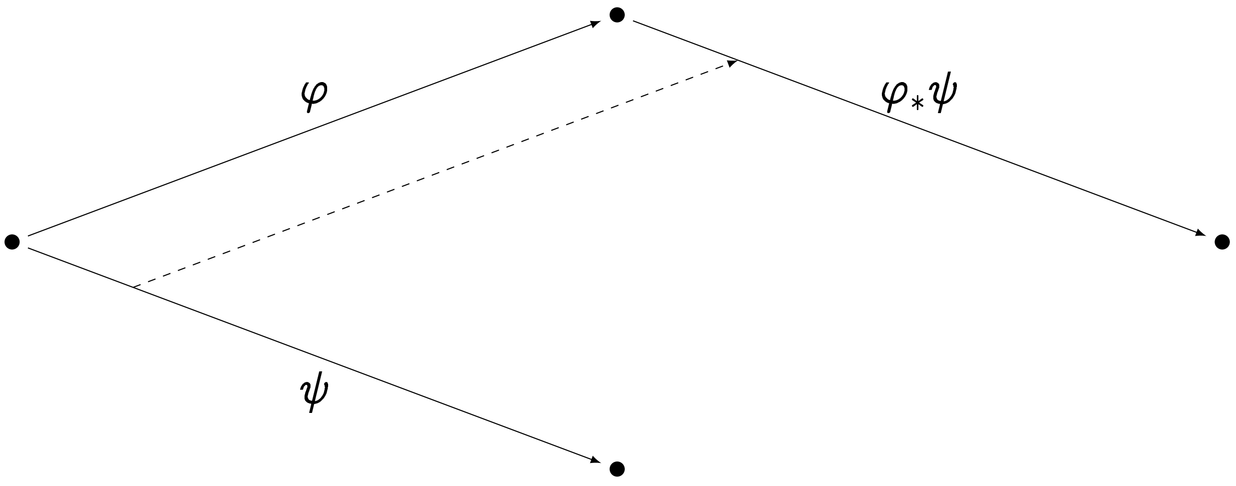
Push-forward

$$\begin{tikzcd}
& \bullet \arrow[dr, "\varphi_*\psi"] & \\
\bullet \arrow[ur, "\varphi"] \arrow[dr, "\psi"'] & & \bullet \\
& \bullet &
\end{tikzcd}$$

$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

$$\deg(\varphi_*\psi) = \deg(\psi)$$

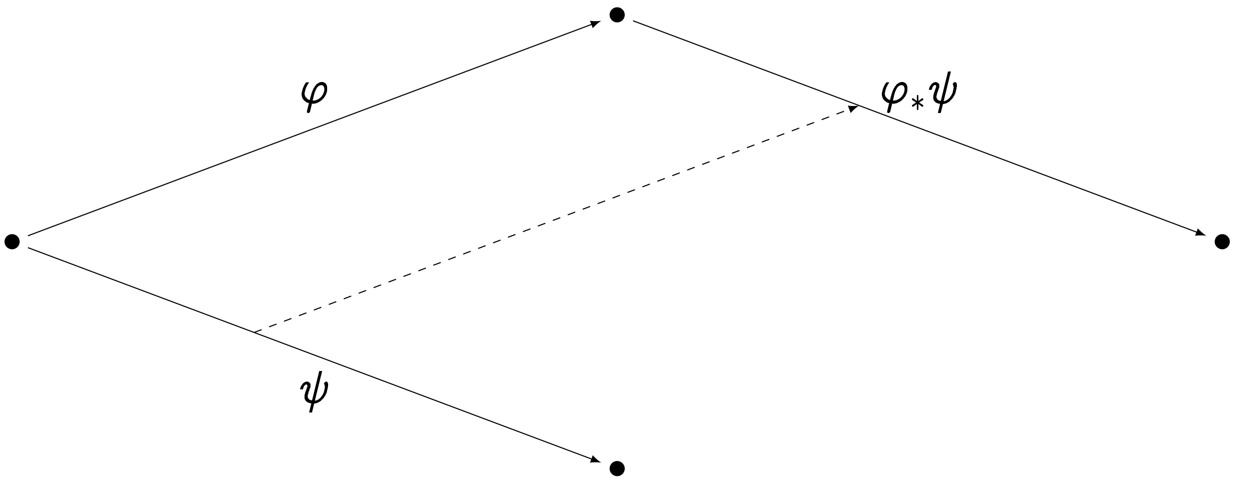
Push-forward



$$\Big(\deg(\varphi), \deg(\psi)\Big) = 1$$

$$\deg(\varphi_*\psi) = \deg(\psi)$$

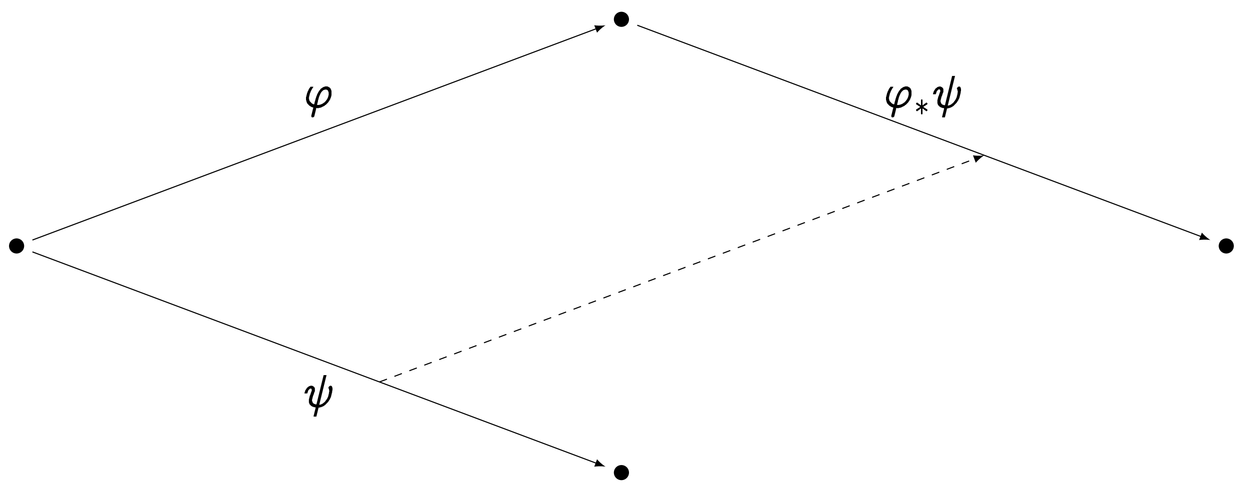
Push-forward



$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

$$\deg(\varphi_*\psi) = \deg(\psi)$$

Push-forward



$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

$$\deg(\varphi_*\psi) = \deg(\psi)$$

Push-forward

$$\begin{tikzcd}
 & \bullet \arrow[dr, "\varphi_*\psi"] & \\
\bullet \arrow[ur, "\varphi"] \arrow[dr, "\psi"'] & & \bullet \\
 & \bullet \arrow[ur, dashed] &
\end{tikzcd}$$

$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

$$\deg(\varphi_*\psi) = \deg(\psi)$$

Push-forward

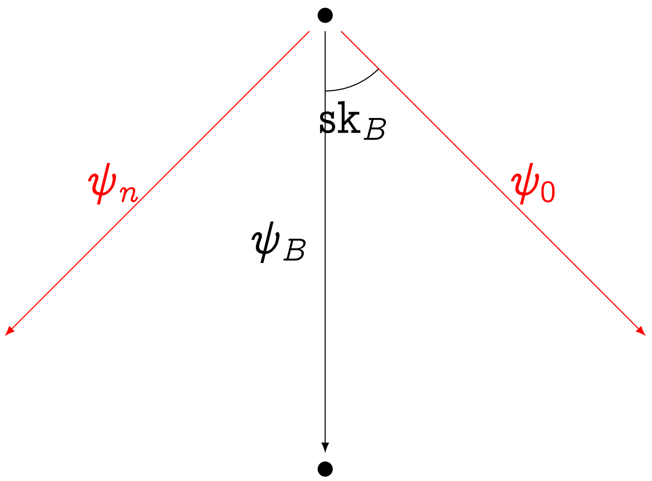
$$
\begin{tikzcd}
& \bullet \arrow[dr, "\varphi_*\psi"] & \\
\bullet \arrow[ur, "\varphi"] \arrow[dr, "\psi"'] & & \bullet \\
& \bullet \arrow[ur, "\psi_*\varphi"'] &
\end{tikzcd}
$$

$$\big(\deg(\varphi), \deg(\psi)\big) = 1$$

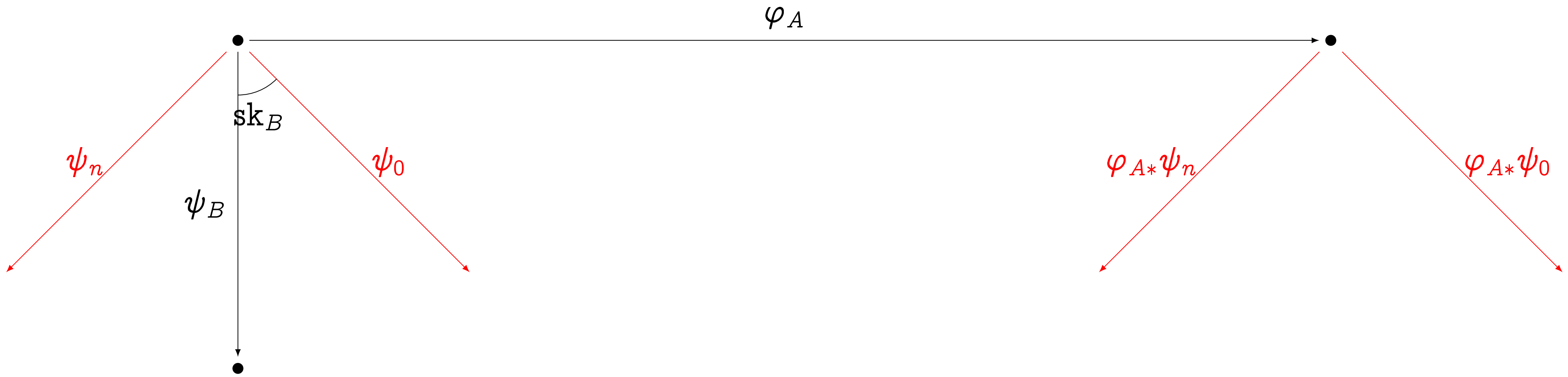
$$\deg(\varphi_*\psi) = \deg(\psi)$$

$$\deg(\psi_*\varphi) = \deg(\varphi)$$

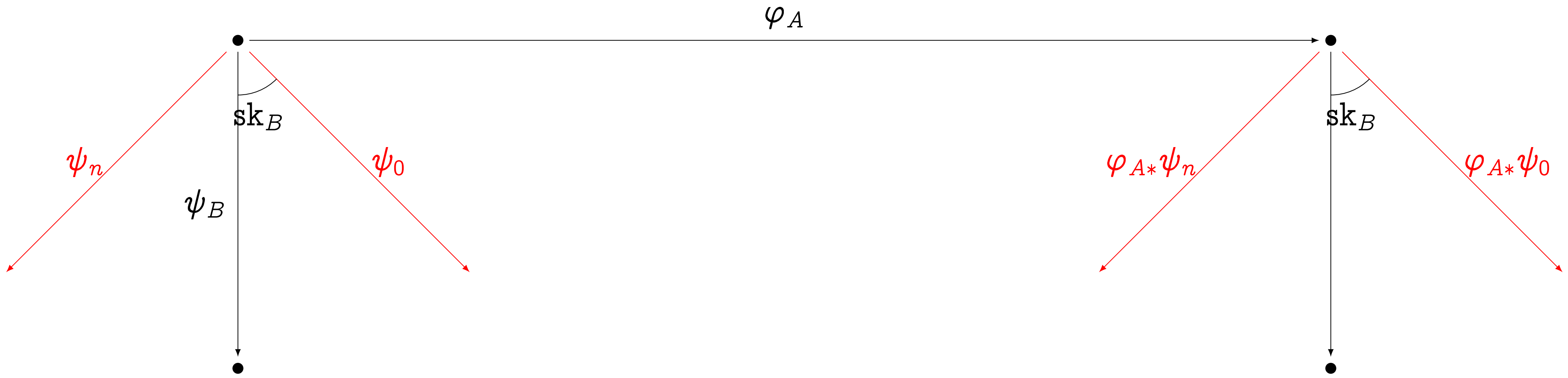
Supersingular Isogeny Diffie-Hellman (SIDH)



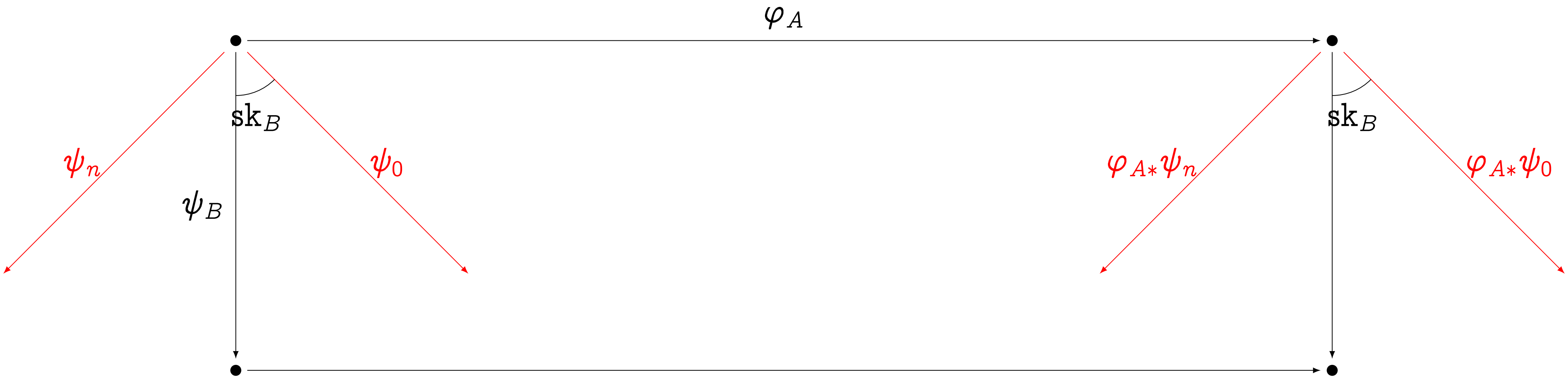
Supersingular Isogeny Diffie-Hellman (SIDH)



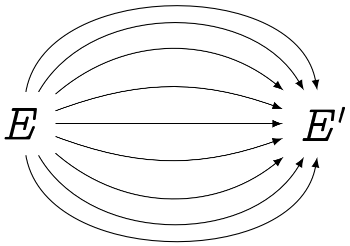
Supersingular Isogeny Diffie-Hellman (SIDH)



Supersingular Isogeny Diffie-Hellman (SIDH)



The Deuring Correspondence



$$\mathrm{Hom}(E, E')$$

ॐ

Homs are groups

$$\begin{tikzcd} E' & E \arrow[l, bend right, "\varphi"'] \arrow[l, bend left, "\psi"] \end{tikzcd}$$

$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

Homs are groups

$$\begin{tikzcd}[column sep=huge] E' & E \arrow[l, bend right, "\varphi"'] \arrow[l, dashed, "\varphi+\psi"'] \arrow[l, bend left, "\psi"] \end{tikzcd}$$

$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

Ends are rings

Distributivity

$$\varphi \circ (\psi + \chi) = (\varphi \circ \psi) + (\varphi \circ \chi)$$

$$(\psi + \chi) \circ \varphi = (\psi \circ \varphi) + (\chi \circ \varphi)$$

Supersingular endomorphism rings

$$\mathrm{End}(E) \qquad \simeq \qquad \mathcal{O} \qquad \subset \qquad \mathcal{B}_{p,\infty}$$

Supersingular endomorphism rings

$$\mathrm{End}(E) \quad \simeq \quad \mathcal{O} \quad \subset \quad \mathcal{B}_{p,\infty}$$

quaternion algebra

Supersingular endomorphism rings

$$\mathrm{End}(E) \quad \simeq \quad \mathcal{O} \quad \subset \quad \mathcal{B}_{p,\infty}$$

maximal order

quaternion algebra

Supersingular endomorphism rings

$$\mathrm{End}(E) \quad \simeq \quad \mathcal{O} \quad \subset \quad \mathcal{B}_{p,\infty}$$

maximal order

rank 4 submodule

quaternion algebra

4-dimensional $\mathbb{Q}$-vector space

Supersingular endomorphism rings

$$\mathrm{End}(E) \simeq \mathcal{O} \subset \mathcal{B}_{p,\infty}$$

maximal order

rank 4 submodule

quaternion algebra

4-dimensional $\mathbb{Q}$-vector space

EndRing problem: given E supersingular, compute an order $\mathcal{O} \simeq \mathrm{End}(E)$.

Homs $\longleftrightarrow$ Modules $\longleftrightarrow$ Ideals

$$E' \xleftarrow{\varphi} E$$

$$\varphi \in \mathrm{Hom}(E, E')$$

Homs $\longleftrightarrow$ Modules $\longleftrightarrow$ Ideals

$$\begin{tikzcd} E' & & E \arrow[ll, "\varphi"'] \arrow[loop right, "\omega"] \end{tikzcd}$$

$$\varphi \circ \omega \in \mathrm{Hom}(E, E')$$

Homs $\longleftrightarrow$ Modules $\longleftrightarrow$ Ideals

$$\begin{tikzcd} E' \arrow[loop left, "\omega'"] & & E \arrow[ll, "\varphi"'] \end{tikzcd}$$

$$\omega' \circ \varphi \in \mathrm{Hom}(E, E')$$

Homs $\longleftrightarrow$ Modules $\longleftrightarrow$ Ideals

$$E' \xleftarrow{\varphi} E \qquad\qquad \mathcal{O} \xrightarrow{I_\varphi} \mathcal{O}'$$

$$\varphi \in \mathrm{Hom}(E, E')$$

$$\mathrm{Hom}(E, E') \simeq I_\varphi$$

$$\mathcal{O} \supset I_\varphi \subset \mathcal{O}'$$

Endomorphism ring

Isogeny

$\mathrm{Hom}(E, E')$

Degree

Maximal order

Ideal

Ideal class

Norm

Kohel-Lauter-Petit-Tignol (KLPT)

$$E \xrightarrow{??} E'$$

Kohel-Lauter-Petit-Tignol (KLPT)

$$\mathrm{End}(E) \xrightarrow{\quad ?? \quad} \mathrm{End}(E')$$

Kohel-Lauter-Petit-Tignol (KLPT)

$$\mathrm{End}(E) \xrightarrow{\quad\quad\quad\quad I \quad\quad\quad\quad} \mathrm{End}(E')$$

$$N(I) = 2^x$$

Kohel-Lauter-Petit-Tignol (KLPT)

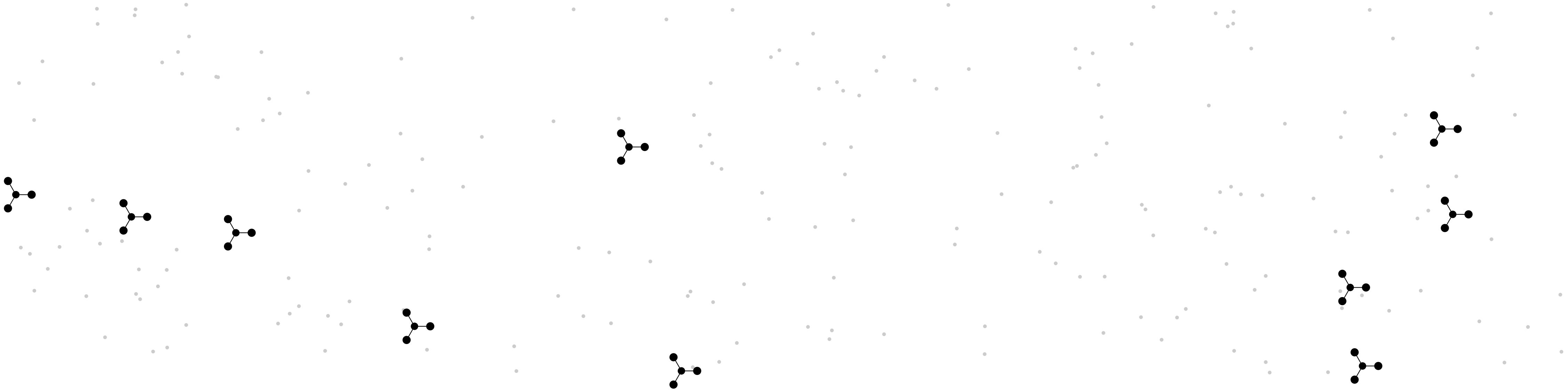
$$\mathrm{End}(E) \xrightarrow{\quad\quad\quad I \quad\quad\quad} \mathrm{End}(E')$$

$$N(I) = 2^x$$

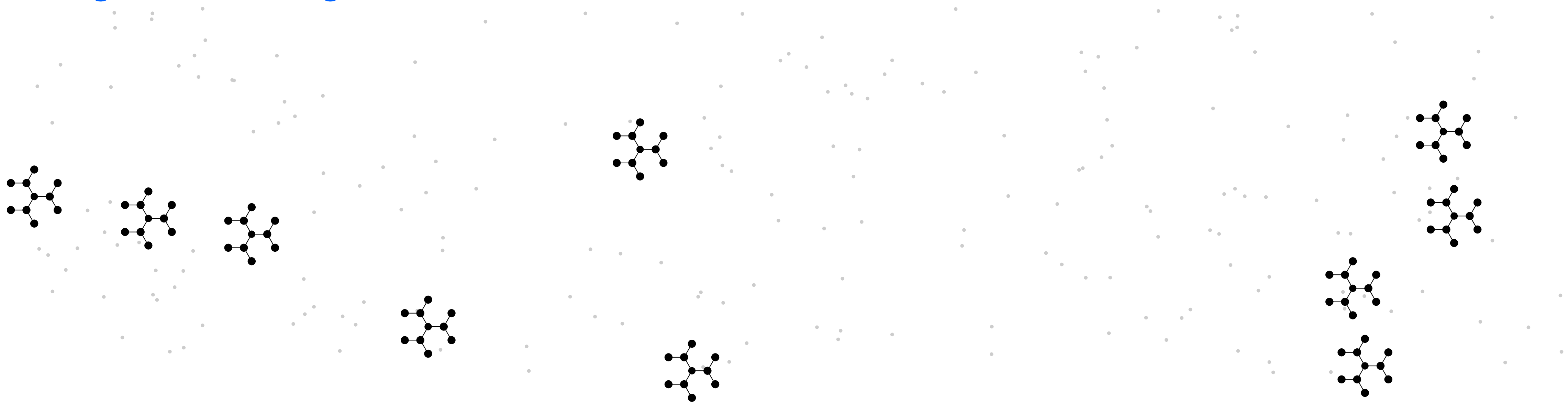
Corollary: Isogeny problem $\simeq$ EndRing problem

Contagious knowledge

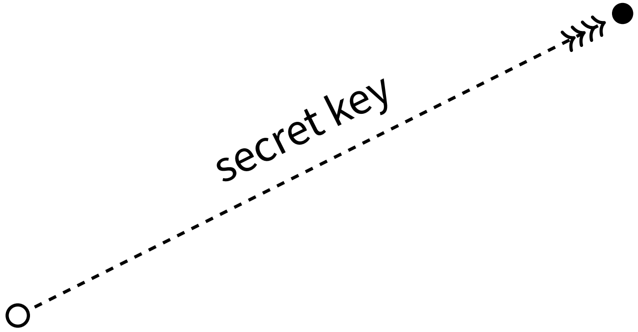
Contagious knowledge



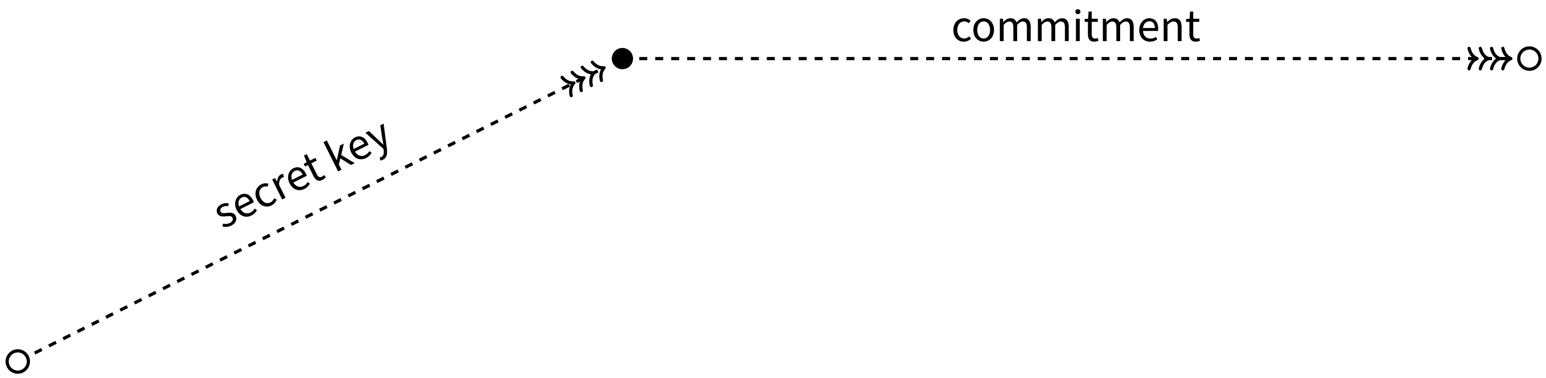
Contagious knowledge



SQIsign (identification scheme)



SQIsign (identification scheme)

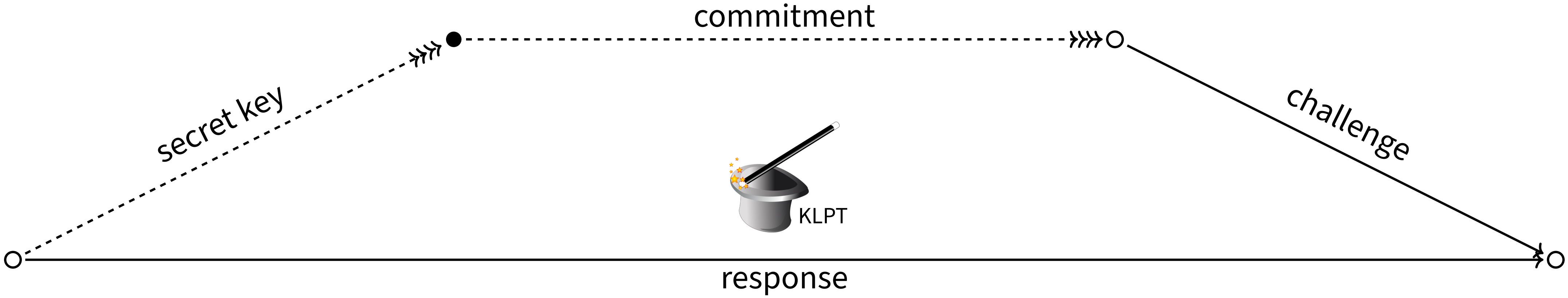


SQIsign (identification scheme)

SQIsign (identification scheme)

SQIsign (identification scheme)

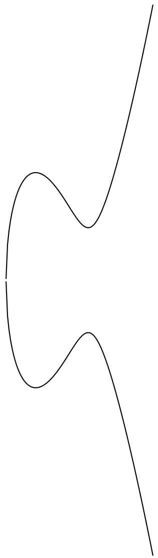
SQIsign (identification scheme)



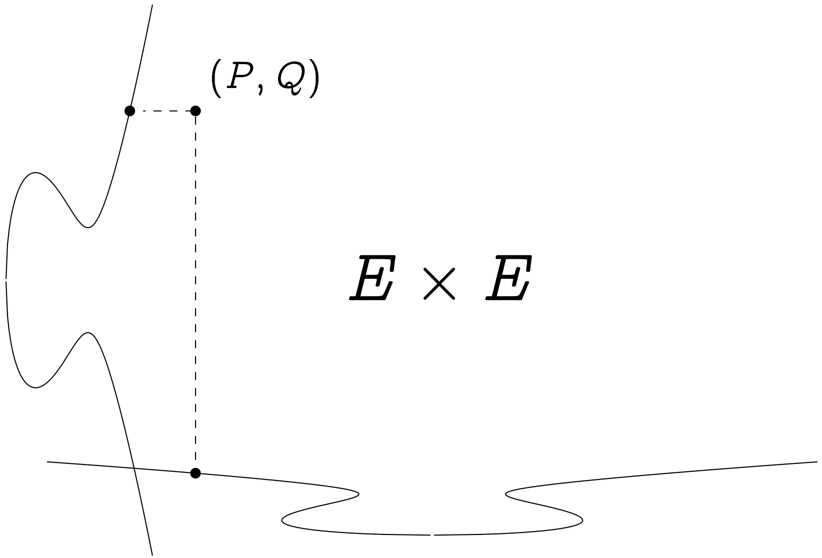
SQIsign

Bytes		Mcycles			
Public Key	Signature	Keygen	Sign	Verify	Security
64	177	3,728	5,779	108	NIST-1
96	263	23,734	43,760	654	NIST-3
128	335	91,049	158,544	2,177	NIST-5

Higher dimensional abelian varieties



Higher dimensional abelian varieties



Higher dimensional isogenies

$$A \times B \longrightarrow C \times D$$

Higher dimensional isogenies

$$
\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\beta"'] & C \\
D & B \arrow[l, "\delta"] \arrow[u, "\gamma"']
\end{tikzcd}
$$

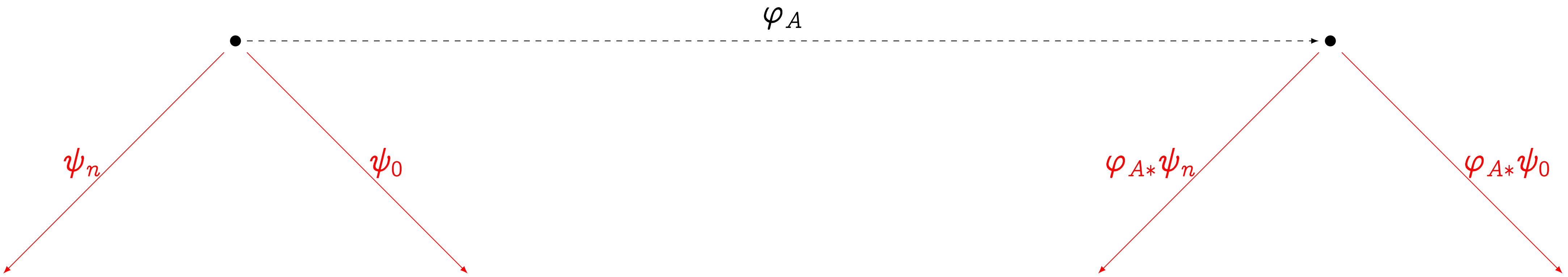
$$
\begin{aligned}
A \times B &\longrightarrow C \times D \\
(P, Q) &\longmapsto \big(\alpha(P) + \gamma(Q), \beta(P) + \delta(Q)\big)
\end{aligned}
$$

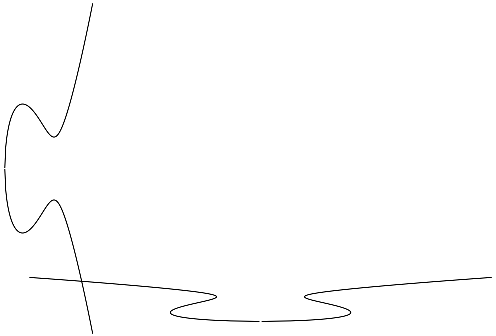
Higher dimensional isogenies

$$
\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\beta"'] & C \\
D & B \arrow[l, "\delta"] \arrow[u, "\gamma"']
\end{tikzcd}
$$

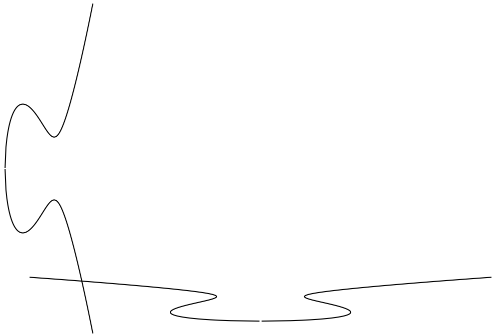
$$
\begin{aligned}
A \times B &\longrightarrow C \times D \\
(P, Q) &\longmapsto \big(\alpha(P) + \gamma(Q), \beta(P) + \delta(Q)\big) \\
&= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}
\end{aligned}
$$

Isogeny problem + Torsion point information (SIDH)





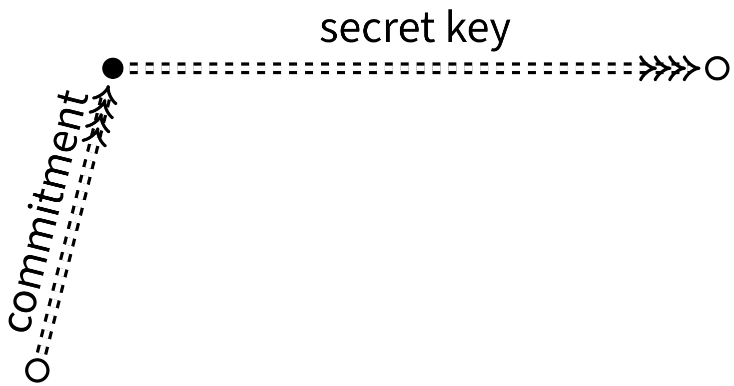
$$\xrightarrow{\Phi_A}$$



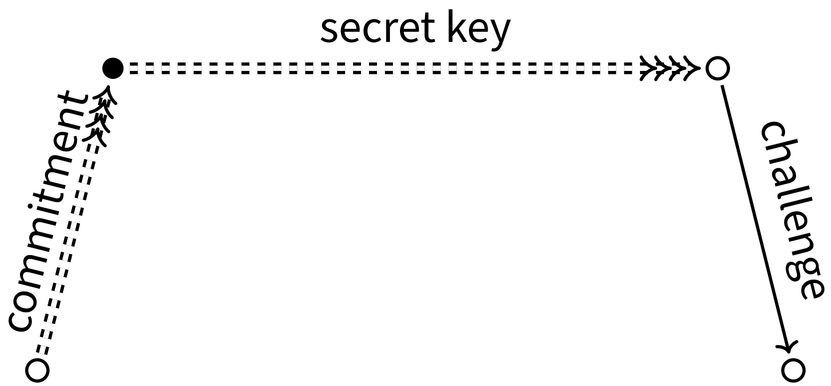
$$\deg(\varphi_A) \approx \deg(\Phi_A) = 2^x$$

SQIsign2D

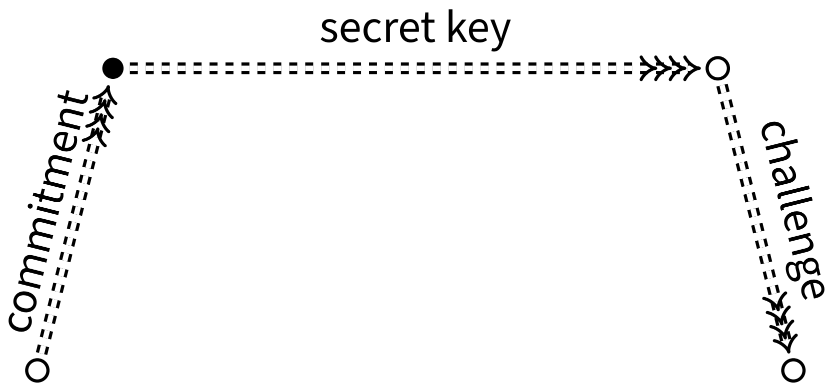
SQIsign2D



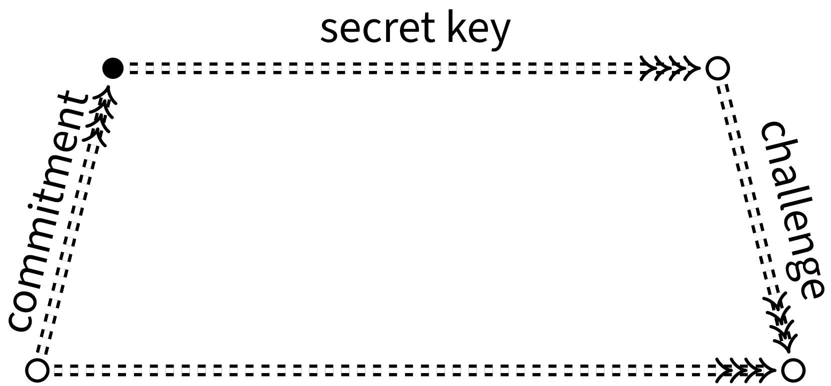
SQIsign2D



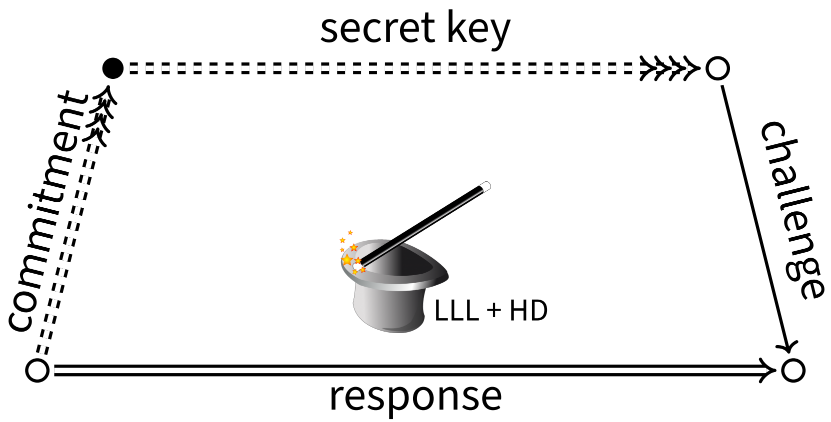
SQIsign2D



SQIsign2D

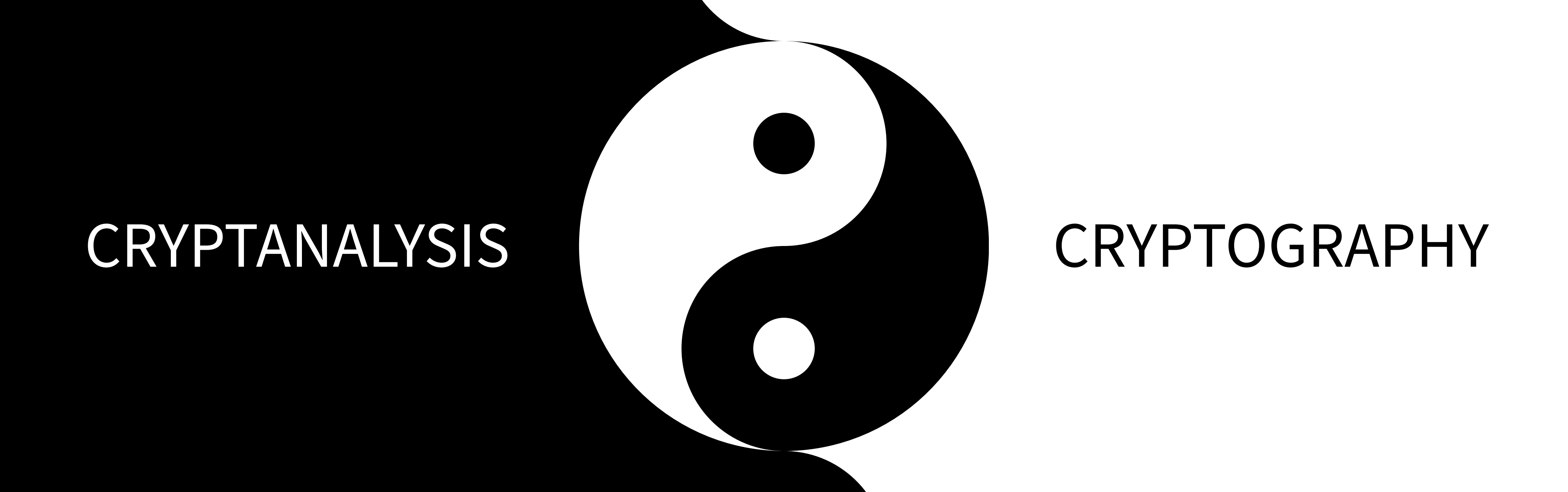


SQIsign2D



SQIsign2D

Bytes		Mcycles			
Public Key	Signature	Keygen	Sign	Verify	Security
66	148	60	160	9	NIST-1
98	222	170	460	29	NIST-3
130	294	360	940	62	NIST-5


CRYPTANALYSIS
CRYPTOGRAPHY