# Post-quantum signatures

A mathematical quest for the holy grail

Krijn Reijnders
June 14th, 2023

## Three things I want to discuss today

# Three things I want to discuss today

1

$$\bullet \xrightarrow{g} \bullet$$

from groups
to group actions

## Three things I want to discuss today

**1**

$$\bullet \xrightarrow{g} \bullet$$

**from groups to group actions**

**2**

$$\begin{tikzcd} \bullet \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r, dashed] & \bullet \end{tikzcd}$$

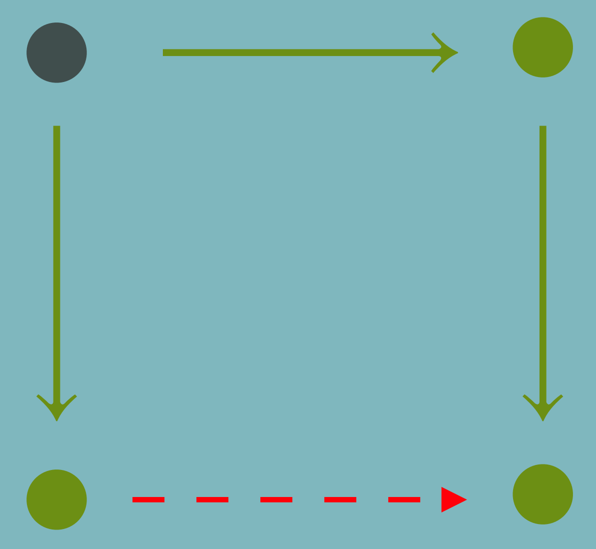
**the difficulty of signatures**

## Three things I want to discuss today

**1**

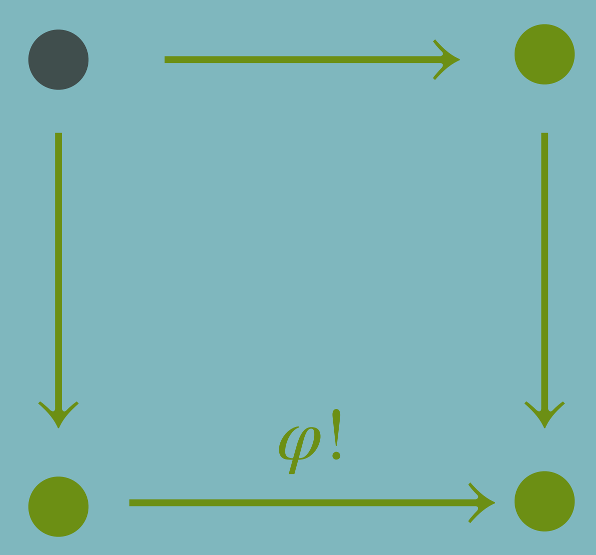

**from groups to group actions**

**2**



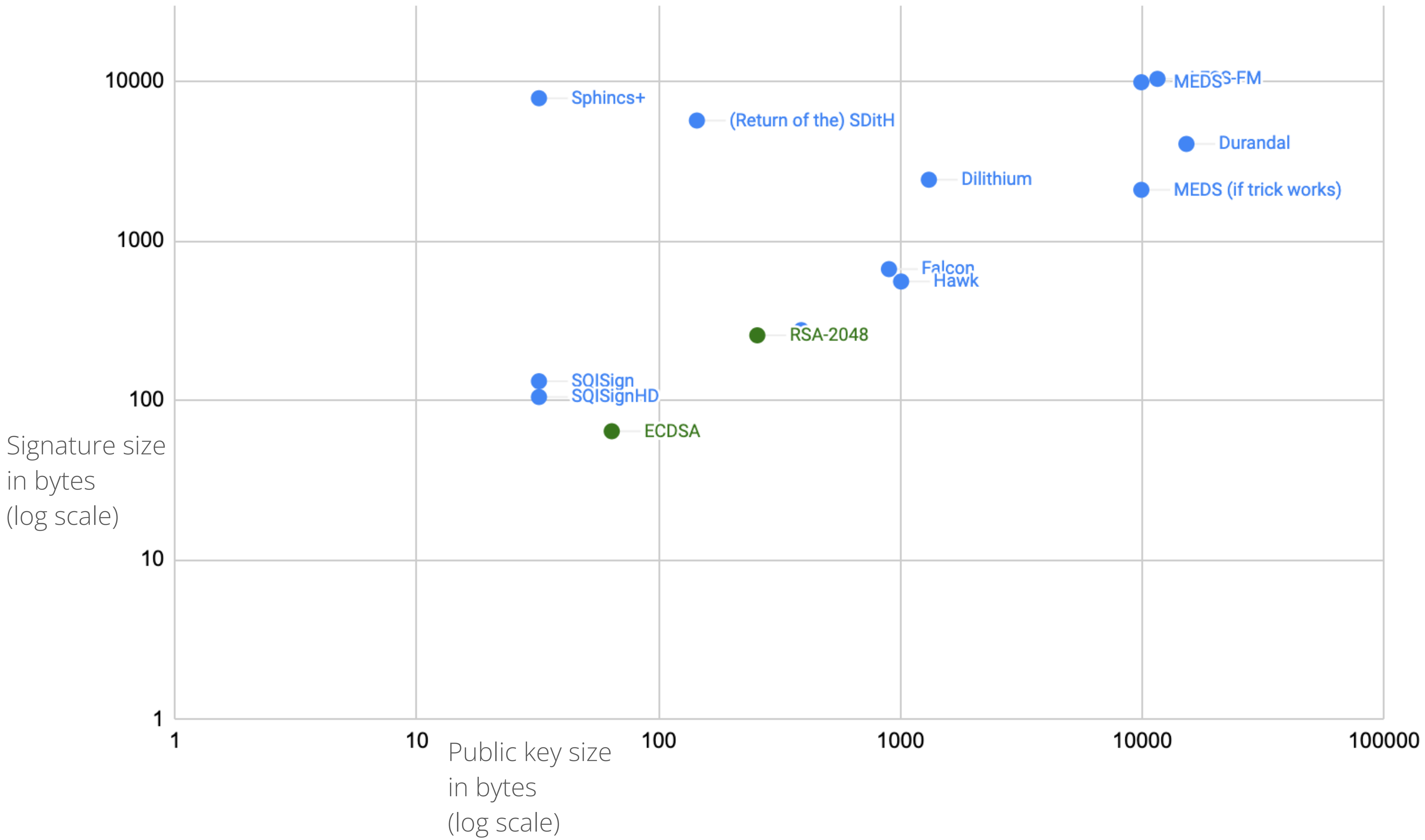
**the difficulty of signatures**

**3**




**the miracle of SQISign**

# A quick look at the current *state-of-the-art*



# Pre-quantum everything is tremendous

1. take any group $G$ where $\log_G$ is hard
2. draw the right diagrams
3. *fast* and *small* cryptography

# Pre-quantum everything is tremendous

**1** take any group $G$ where $\log_G$ is hard

**2** draw the right diagrams

**3** *fast* and *small* cryptography

---

**key exchange**

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$

public key

$$\begin{tikzcd} g \arrow[r, "a"] \arrow[d, "b"'] & g^{a} \arrow[d, "b"] \\ g^{b} \arrow[r, "a"] & g^{ab} \end{tikzcd}$$

public key

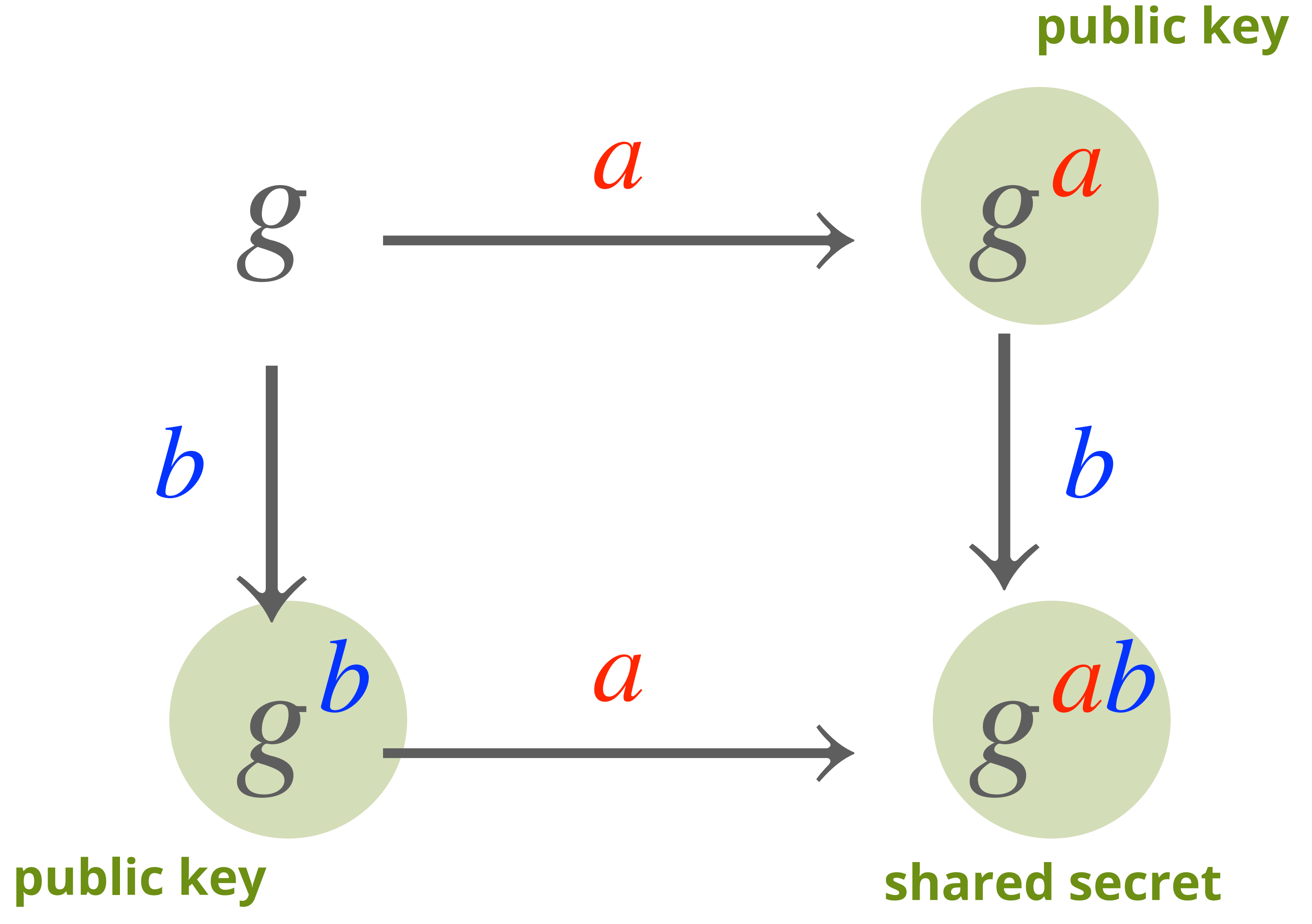
shared secret

# Pre-quantum everything is tremendous

1. take any group $G$ where $\log_G$ is hard
2. draw the right diagrams
3. *fast* and *small* cryptography

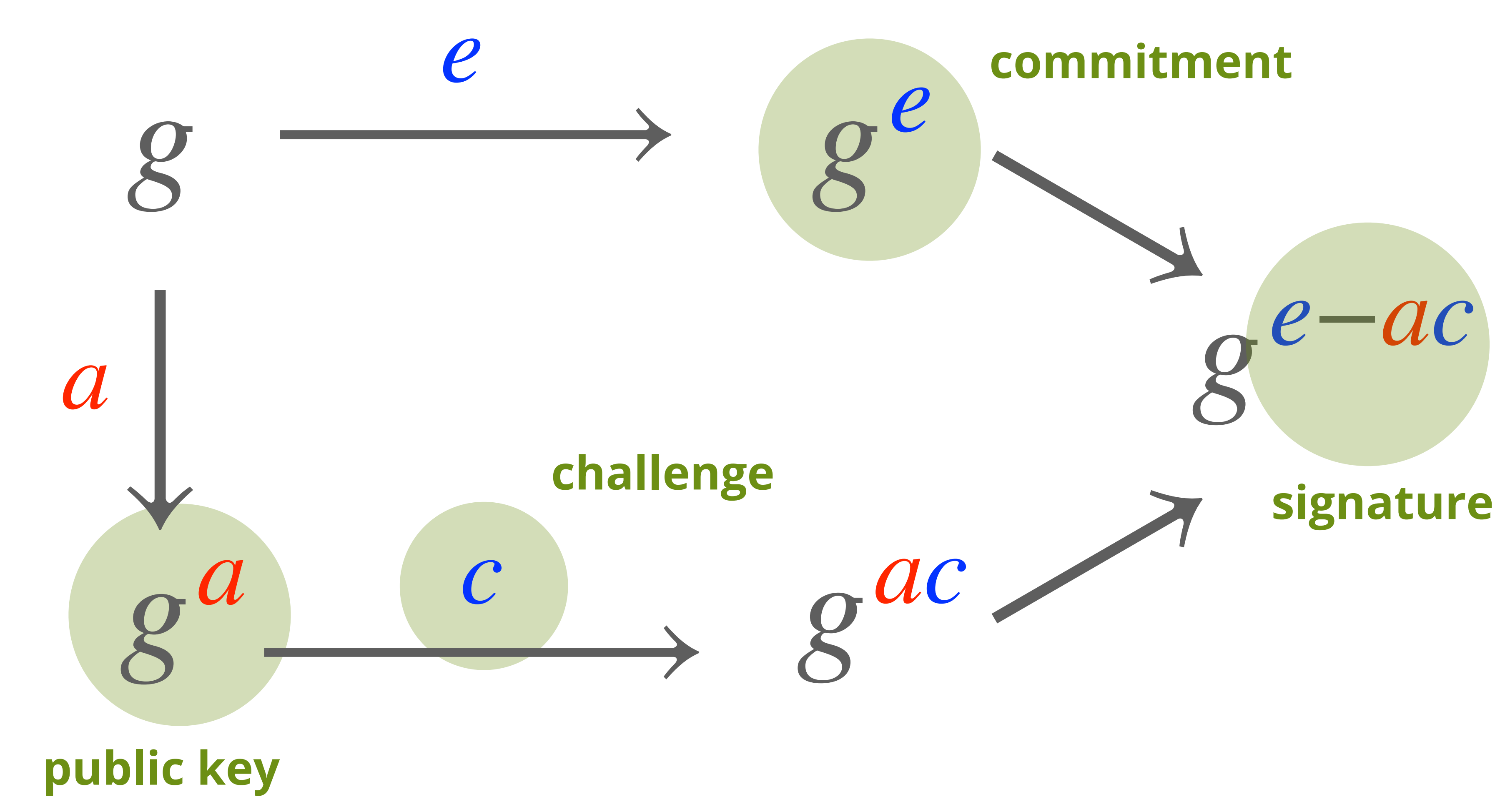
## key exchange

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$




## signatures

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$



# The quantum threat of Shor's algorithm

**1** take any group $G$ where $\log_G$ is hard

**2** Shor's quantum algorithm solves $\log_G$

# The quantum threat of Shor's algorithm

**1** take any group $G$ where $\log_G$ is hard

**2** Shor's quantum algorithm solves $\log_G$

## Shor's algorithm

Peter Shor

- Requires a large quantum computer
- Originally designed to solve integer factorisation in polylogarithmic time (thus breaks RSA)
- Also solves discrete logarithms in abelian groups in polynomial time (thus breaks DH and ECDH)

# from groups to group actions

## group actions, a saviour for key exchange

*(in theory)*

**pre-quantum**

$$G \xrightarrow{\mathbb{Z}} G$$

**hardness**

Given $g$ and $g^a$, find $a$

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$

$$\begin{tikzcd} g \arrow[r, "a"] \arrow[d, "b"'] & g^{a} \arrow[d, "b"] \\ g^{b} \arrow[r, "a"] & g^{ab} \end{tikzcd}$$

# group actions, a saviour for key exchange

*(in theory)*

**pre-quantum**

$$G \xrightarrow{\mathbb{Z}} G$$

**hardness**

Given $g$ and $g^a$, find $a$

**post-quantum**

$$X \xrightarrow{G} X$$

**hardness**

Given $x$ and $g \star x$, find $g$

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$

$$\begin{tikzcd}
g \arrow[r, "a"] \arrow[d, "b"'] & g^{a} \arrow[d, "b"] \\
g^{b} \arrow[r, "a"] & g^{ab}
\end{tikzcd}$$

**group actions, a saviour for key exchange**

***(in theory)***

**pre-quantum**

$$G \xrightarrow{\mathbb{Z}} G$$

**hardness**

Given $g$ and $g^a$, find $a$

**post-quantum**

$$X \xrightarrow{G} X$$

**hardness**

Given $x$ and $g \star x$, find $g$

Group $G = \mathbb{F}_q$ or $G = E(\mathbb{F}_q)$
with generator $g \in G$

$$\begin{array}{ccc} g & \xrightarrow{a} & g^a \\ \downarrow b & & \downarrow b \\ g^b & \xrightarrow{a} & g^{ab} \end{array}$$

Usual examples come from
isogenies and isometries

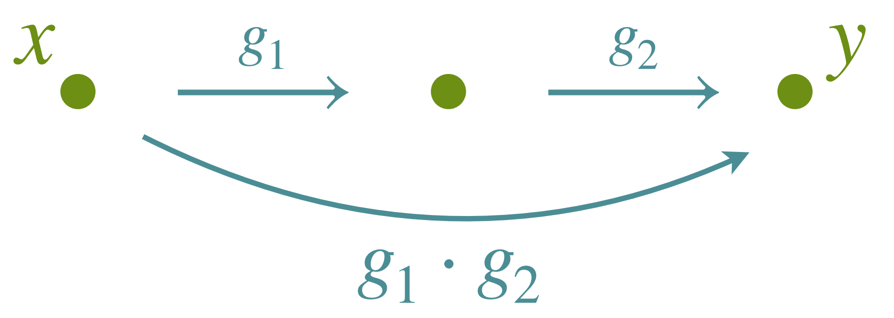
$$\begin{array}{ccc} x & \xrightarrow{g_1} & g_1 \star x \\ \downarrow g_2 & & \downarrow g_2 \\ g_2 \star x & \xrightarrow{g_1} & (g_1 \cdot g_2) \star x \end{array}$$

# What is a *cryptographic* group action?

**group action**

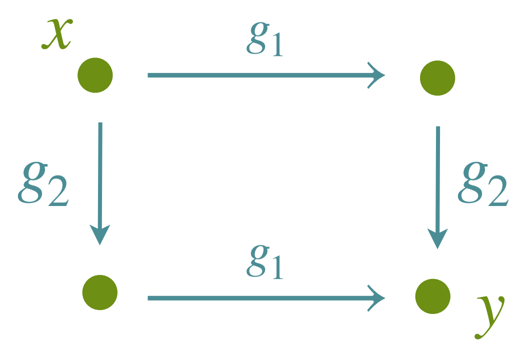
$$X \xrightarrow{g \in G} X$$

**must**

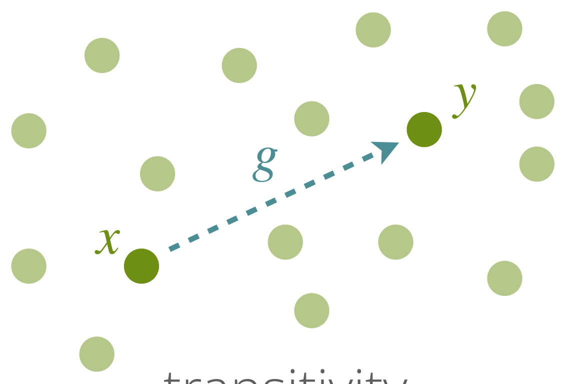



compatible

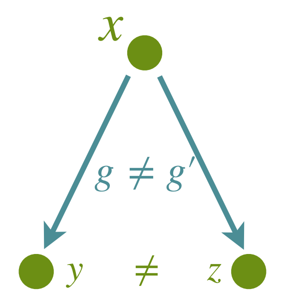
**nice**




commutative




transitivity



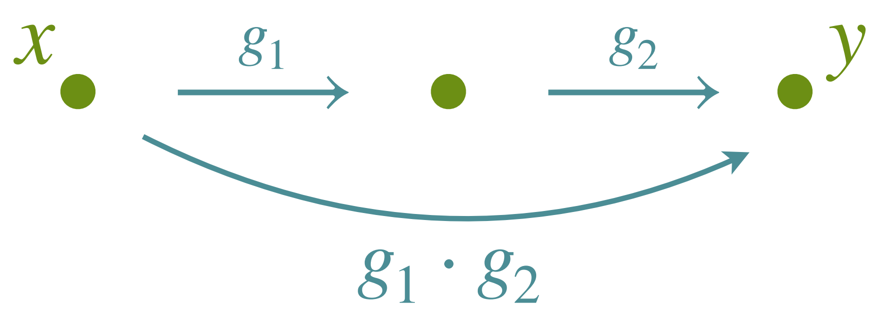

free

# What is a *cryptographic* group action?

**group action**

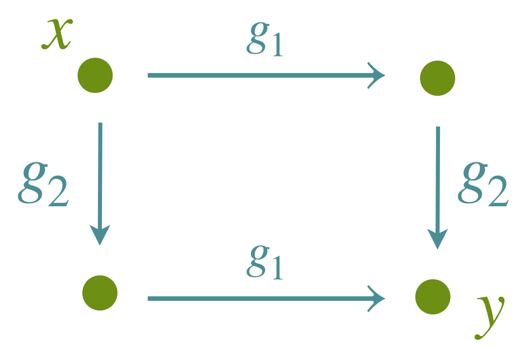
$$X \xrightarrow{g \in G} X$$

**must**

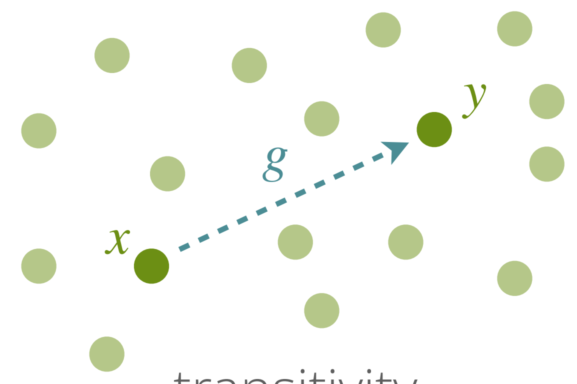



compatible

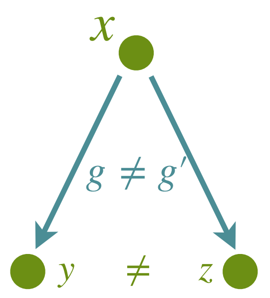
**nice**




commutative




transitivity

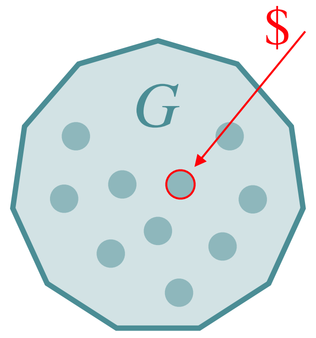



free

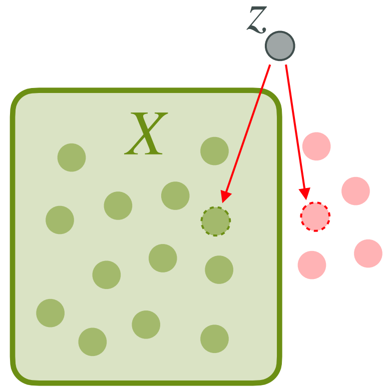
***cryptographic* group action**

## efficiency


evaluation




sampling




membership

## hardness

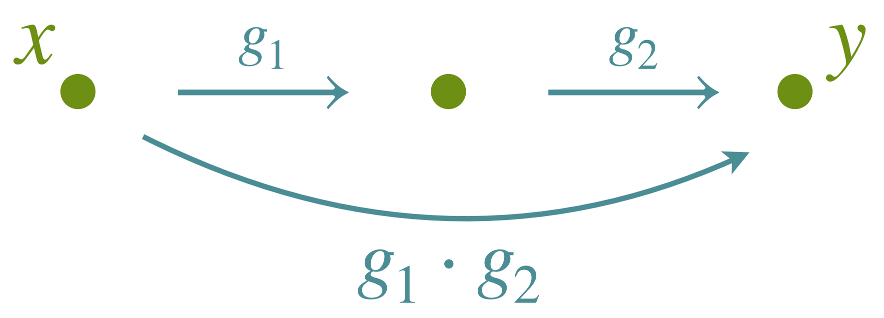
## examples

# What is a *cryptographic* group action?

**group action**

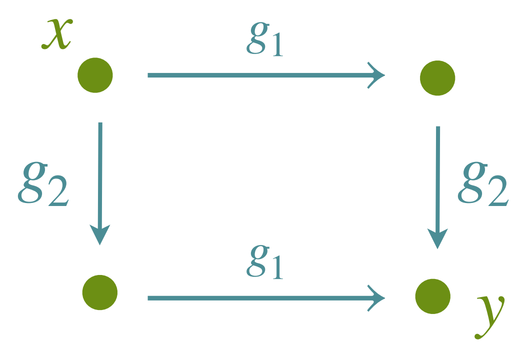
$$X \xrightarrow{g \in G} X$$

**must**

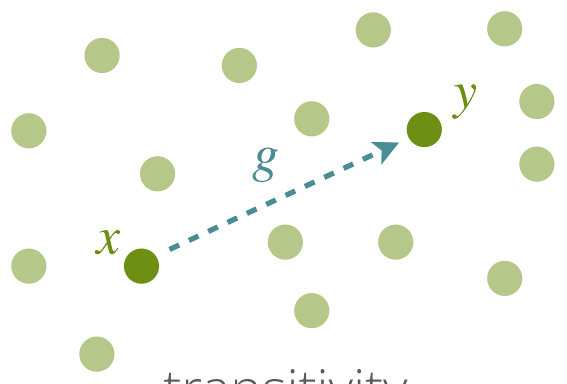



compatible

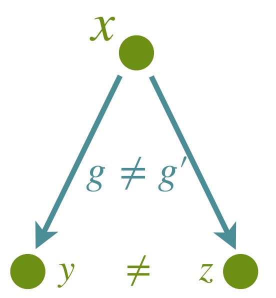
**nice**




commutative




transitivity

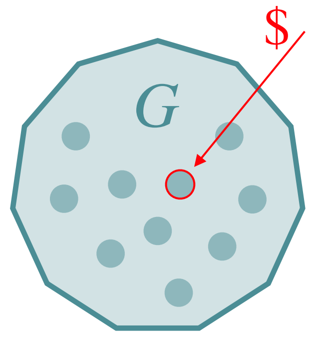



free

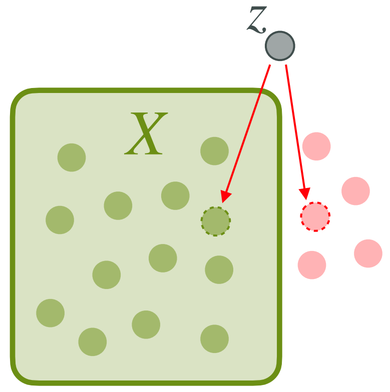
***cryptographic* group action**

## efficiency


evaluation



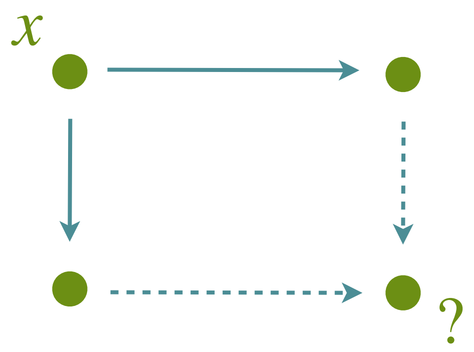

sampling




membership

## hardness


vectorisation




parallelisation

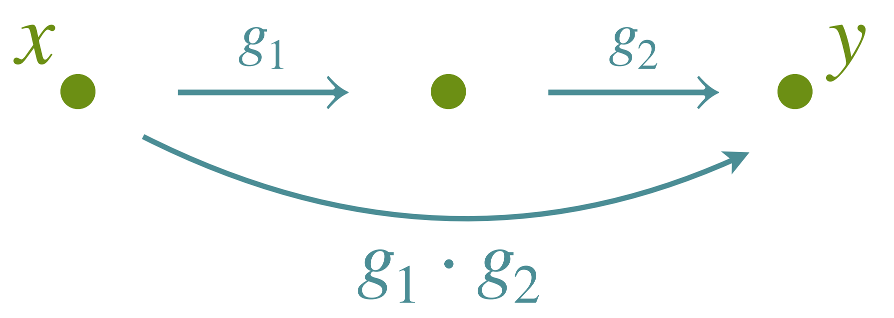
## examples

# What is a *cryptographic* group action?

**group action**

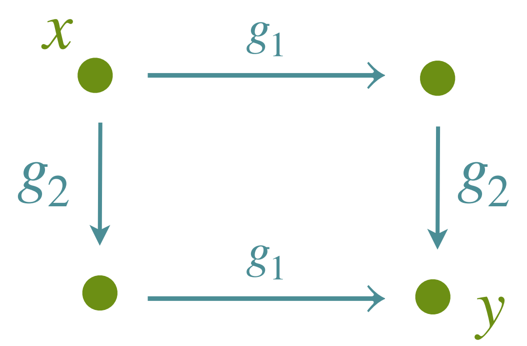
$$X \xrightarrow{g \in G} X$$

**must**

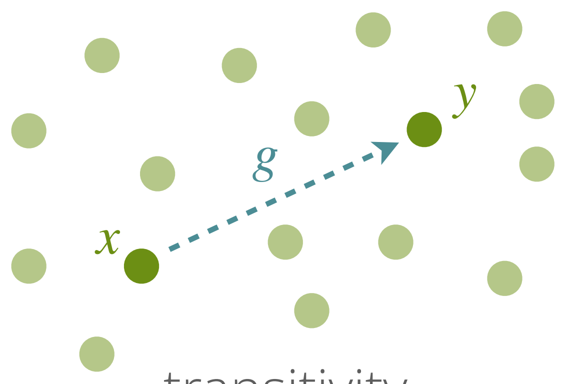



compatible

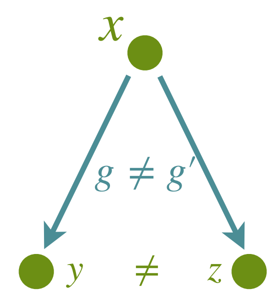
**nice**




commutative




transitivity

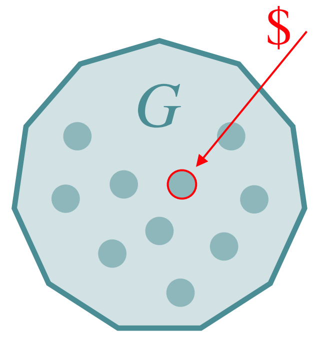



free

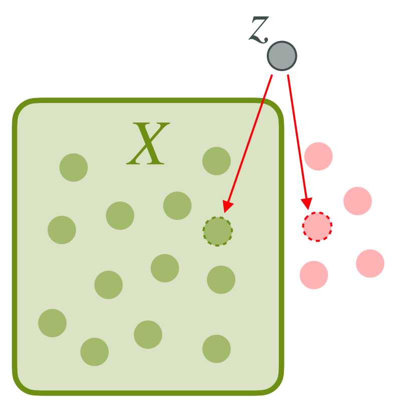
***cryptographic* group action**

## efficiency


evaluation



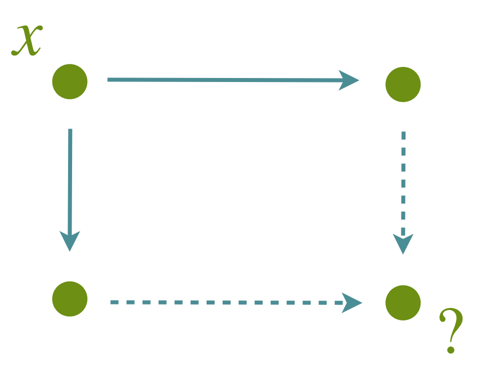

sampling




membership

## hardness


vectorisation

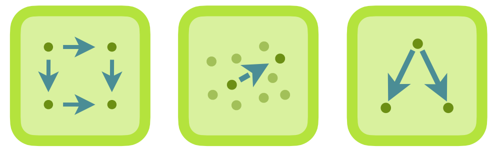



parallelisation

## examples

$X = \mathcal{E}\ell\ell_p(\mathcal{O}) \,/ \sim$

$G = \mathcal{C}\ell(\mathcal{O})$



isogenies

$X = k$-dim codes / $\mathbb{F}_q$

$G = \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$

isometries

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$$\xrightarrow{\varphi}$$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$P, Q \in E$

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

**Isogeny**

$$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

## Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$P, Q \in E$

$\xrightarrow{\varphi}$

**Isogeny**

$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

**Endomorphism**

$\varphi : E \to E$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$P, Q \in E$

$\varphi$

**Isogeny**

$(x,y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

---

**Endomorphism**

$\varphi : E \to E$

**1** $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

**2** $\pi : E \to E, \quad (x,y) \mapsto (x^q, y^q)$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$\varphi$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

**Isogeny**

$$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

$P, Q \in E$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

---

**Endomorphism**

$\varphi : E \to E$

1 $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

2 $\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

1
2

**Ordinary elliptic curve**

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

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

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

**Isogeny**

$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$

$P, Q \in E$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

**Endomorphism**

$\varphi : E \to E$

**1** $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

**2** $\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

**?** “weird” endomorphisms?
$\varphi : E \to E$

**1 2** **Ordinary elliptic curve**

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$\varphi$

**Another curve**

$E' : y^2 = x^3 - 3x + 3$

$P, Q \in E$

**Isogeny**

$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

---

**Endomorphism**

$\varphi : E \to E$

1 $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

2 $\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

? "weird" endomorphisms?

$\varphi : E \to E$

1 2 **Ordinary elliptic curve**

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

1 2 3 4 **Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

# Elliptic curves, isogenies, and supersingularity: the basis for isogeny-based cryptography

**Elliptic curve**

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

$P, Q \in E$

$\varphi$

**Isogeny**

$(x, y) \mapsto \left( \frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$

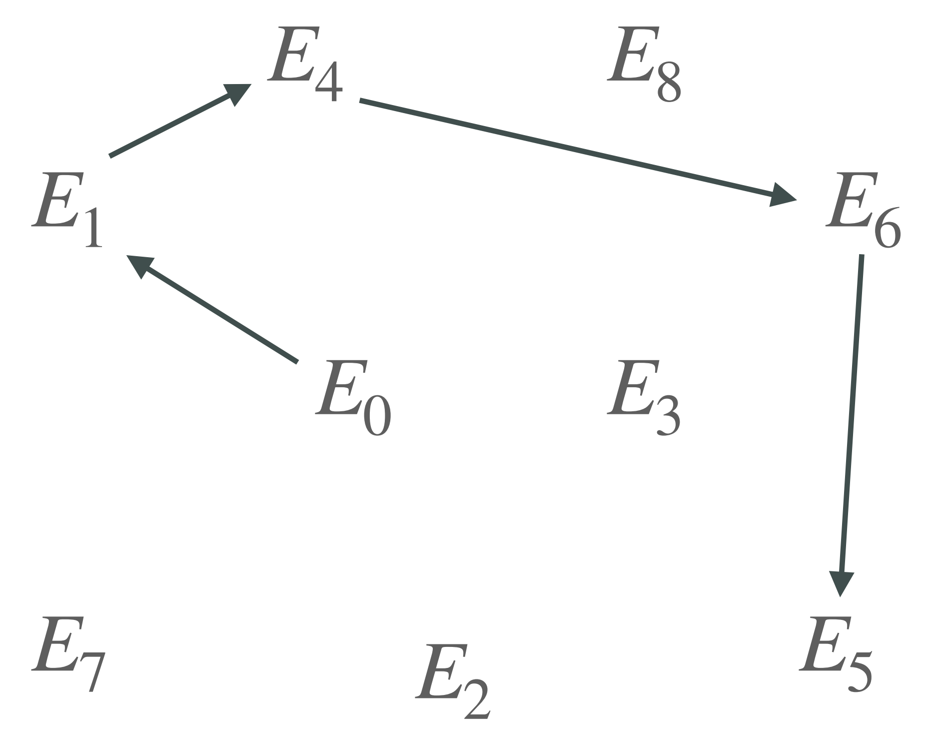
**Another curve**

$E' : y^2 = x^3 - 3x + 3$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

---

**isogeny-based crypto**




**Endomorphism**

$\varphi : E \to E$

**1** $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

**2** $\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

**?** "weird" endomorphisms?

$\varphi : E \to E$

**1 2** **Ordinary elliptic curve**

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

**1 2 3 4** **Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

## We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

## We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order
$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathscr{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathscr{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathscr{C}\ell(\mathcal{O})$ acts on $\mathscr{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathcal{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathcal{C}\ell(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

*In theory:*

**1** take an ideal $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$

**2** for all generators $\varphi \in \mathfrak{a}$, compute $I := \ker \mathfrak{a} = \cap_\varphi \ker \varphi$

**3** then $\mathfrak{a} \star E$ is given by $\varphi_I := E \to E/I$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathscr{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathscr{C}\ell(\mathcal{O})$ acts on $\mathscr{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

*In theory:*

PROBLEM

**1** take an ideal $[\mathfrak{a}] \in \mathscr{C}\ell(\mathcal{O})$

**2** for all generators $\varphi \in \mathfrak{a}$, compute $I := \ker \mathfrak{a} = \cap_\varphi \ker \varphi$

**3** then $\mathfrak{a} \star E$ is given by $\varphi_I := E \to E/I$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathscr{C}\ell(\mathbb{Z}[\pi])$ now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathscr{C}\ell(\mathcal{O})$ acts on $\mathscr{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

*In theory:*

PROBLEM

1 take an ideal $[\mathfrak{a}] \in \mathscr{C}\ell(\mathcal{O})$

PROBLEM

2 ...ll generators $\varphi \in \mathfrak{a}$, compute $I := \ker \mathfrak{a} = \cap_\varphi \ker \varphi$

3 then $\mathfrak{a} \star E$ is given by $\varphi_I := E \to E/I$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathcal{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathcal{C}\ell(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

*In theory:*

PROBLEM 1

take an ideal
$[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$

PROBLEM 2

...ll generators
$\varphi \in \mathfrak{a}$, compute
$I := \ker \mathfrak{a} = \cap_\varphi \ker \varphi$

PROBLEM 3

...en $\mathfrak{a} \star E$ is given
by $\varphi_I := E \to E/I$

# We know *one* commutative cryptographic group action: CSIDH

**Supersingular elliptic curve**

non-commutative maximal order
$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

If $E/\mathbb{F}_p$ then $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$

**cool fact**

the class group $\mathcal{C}\ell(\mathbb{Z}[\pi])$
now acts on such curves $E/\mathbb{F}_p$

---

**Group action (slightly more general)**

1. Take a quadratic order $\mathcal{O}$, such as $\mathcal{O} = \mathbb{Z}[\pi]$
2. Take all elliptic curves $E$ with $\mathcal{O} \subset \mathrm{End}(E)$
3. Then $\mathcal{C}\ell(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_p(\mathcal{O}) := \{\ E \mid \mathcal{O} \subset \mathrm{End}(E)\}$

*In theory:*

PROBLEM 1: take an ideal $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$

PROBLEM ...ll generators $\varphi \in \mathfrak{a}$, compute $I := \ker \mathfrak{a} = \cap_\varphi \ker \varphi$

PROBLEM ...en $\mathfrak{a} \star E$ is given by $\varphi_I := E \to E/I$

*In practice:*

**0** if $p = 4 \cdot \prod \ell_i - 1$, then $(\ell_i) = \underbrace{(\ell_i, \pi + 1)}_{\mathfrak{l}_i} \cdot \underbrace{(\ell_i, \pi - 1)}_{\mathfrak{l}_i^{-1}}$

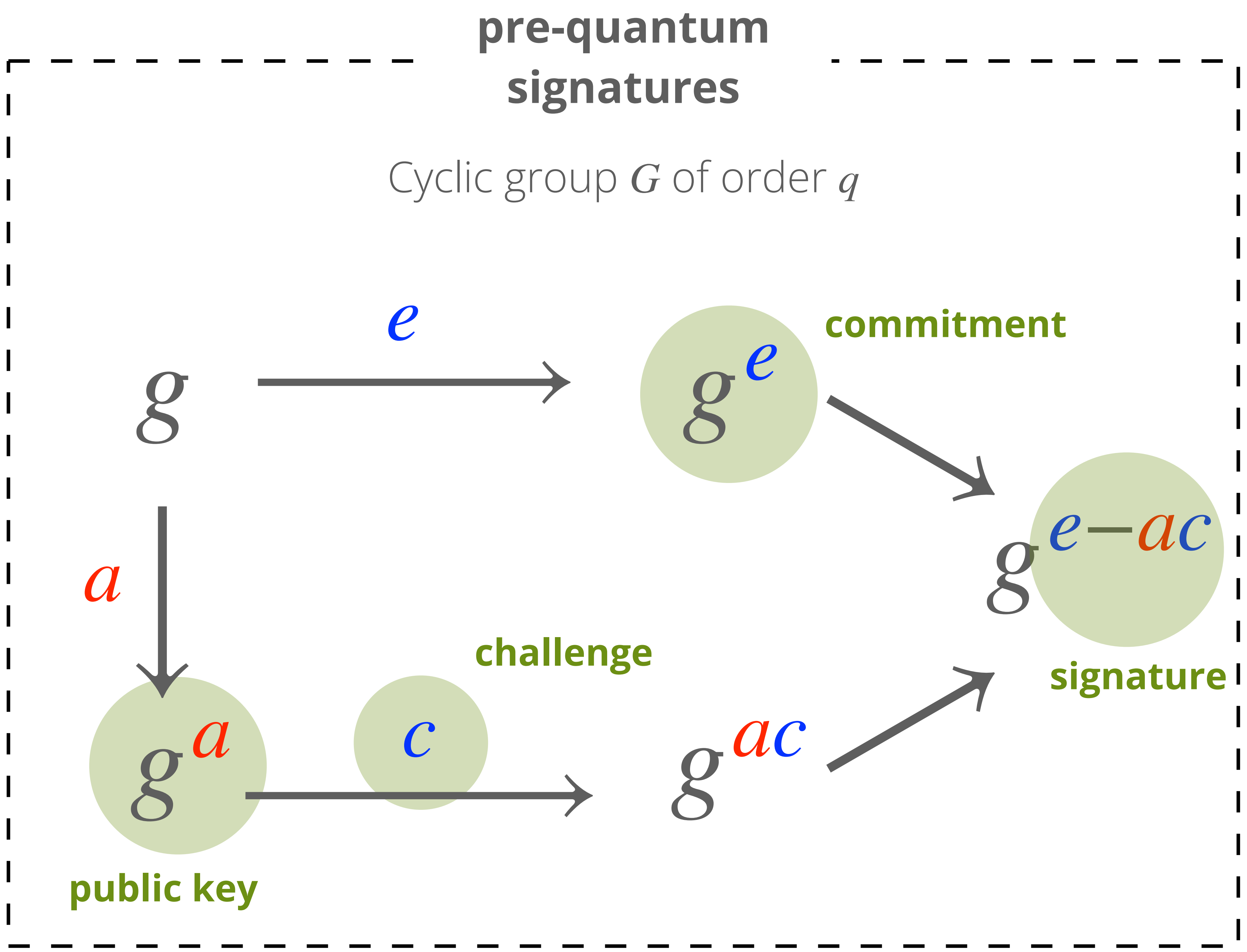
**1** take an ideal $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$ by $\mathfrak{a} = \prod \mathfrak{l}_i^{e_i}$

**2** for $\mathfrak{l}_i^{\pm 1}$, the kernel is generated by $P \in \ker[\ell_i] \cap \ker \pi \pm 1$

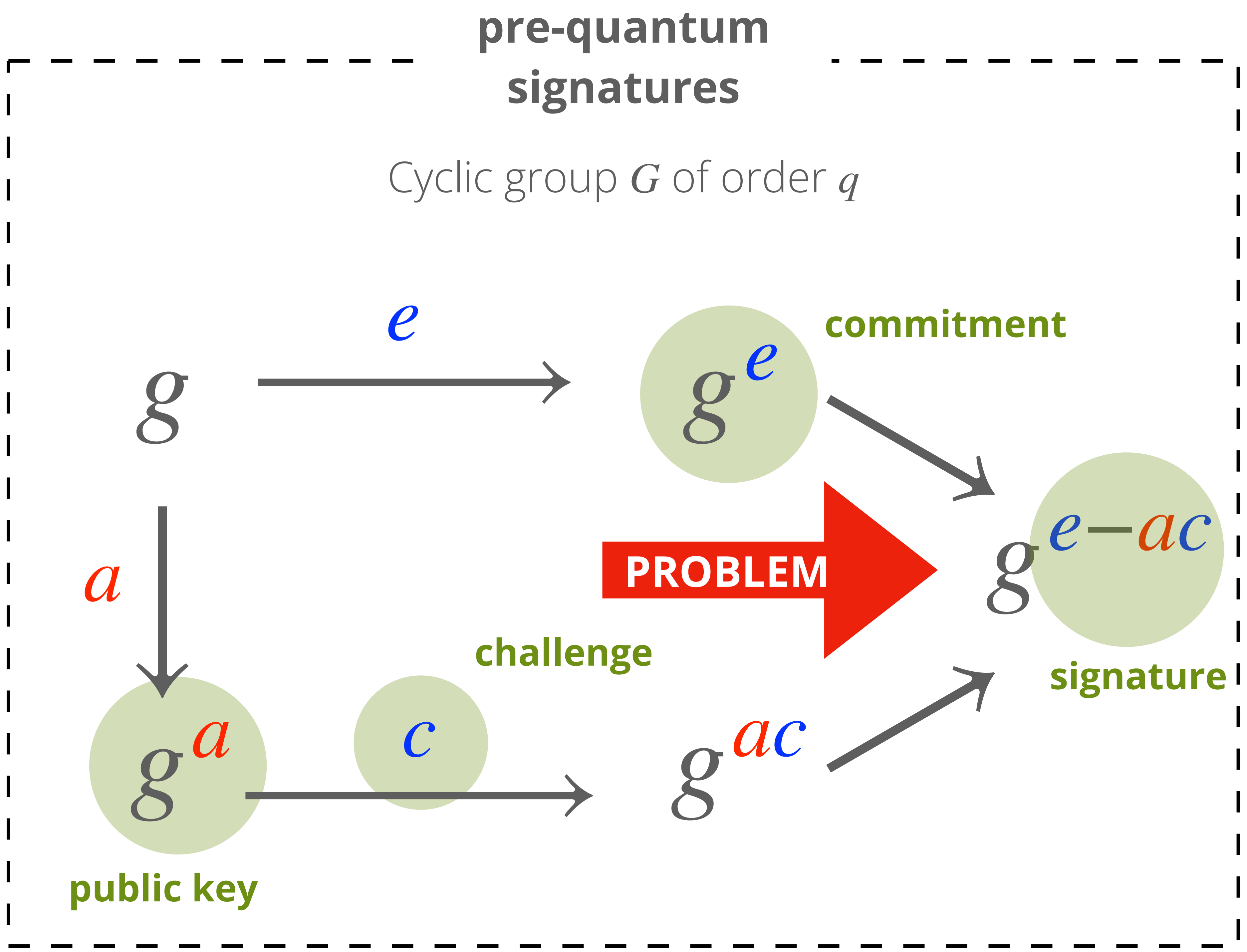
**3** then $\mathfrak{a} \star E$ is given by decomposition into $\mathfrak{l}_i^{\pm 1} \star E$

the difficulty of signatures

Without the group structure, there is the problem of *soundness*



**Without the group structure, there is the problem of *soundness***



**Without the group structure, there is the problem of *soundness***

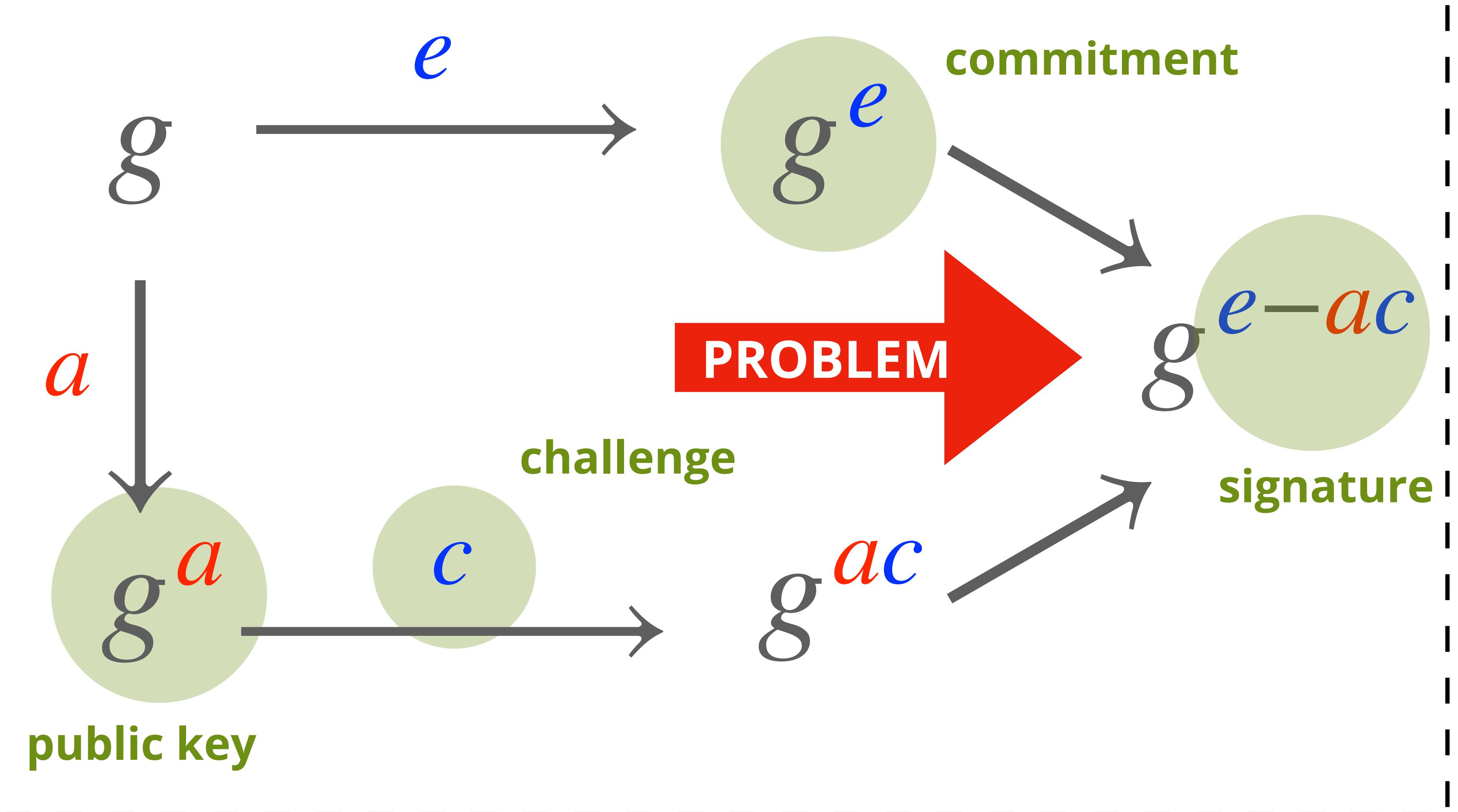
## group actions from equivalence

*In theory*

1. Take mathematical objects $X \in \mathrm{Obj}(C)$ with some structure
2. Take the natural maps $\mu \in \mathrm{Hom}(C)$ that preserve this structure
3. Fingers crossed that it is cryptographically hard to find the map $\mu$ given the objects $X, Y$, where $\mu : X \to Y$

**pre-quantum signatures**

Cyclic group $G$ of order $q$



**Without the group structure, there is the problem of *soundness***

## group actions from equivalence

*In theory*

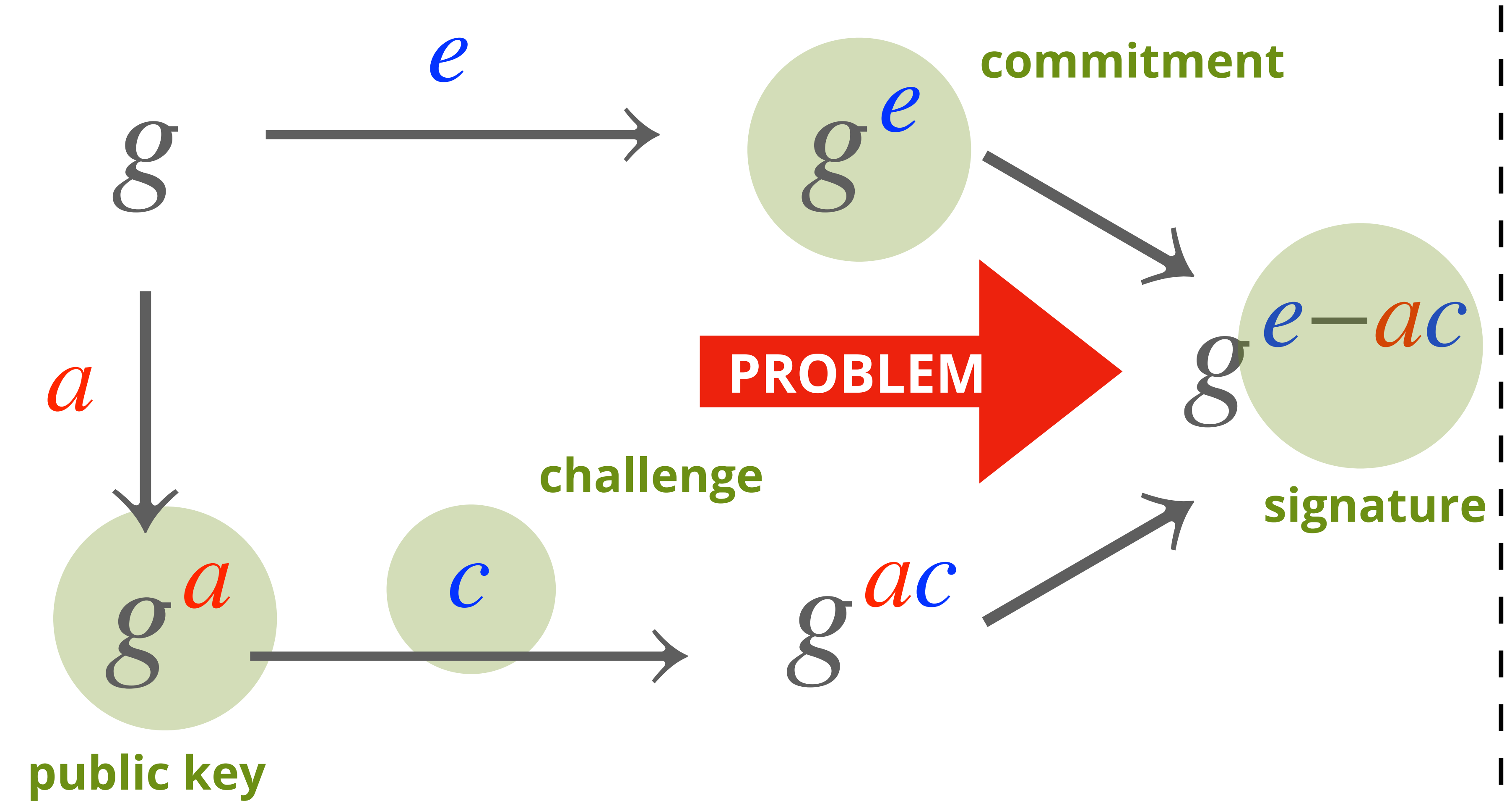
1. Take mathematical objects $X \in \mathrm{Obj}(C)$ with some structure
2. Take the natural maps $\mu \in \mathrm{Hom}(C)$ that preserve this structure
3. Fingers crossed that it is cryptographically hard to find the map $\mu$ given the objects $X, Y$, where $\mu : X \to Y$

*In practice (MEDS)*

1. Objects: $k$-dimensional matrix codes, e.g. *Grasmannian* $\mathrm{Gr}_k(\mathbb{F}_q^{n \times m})$
2. Maps: $\mu$ preserves the rank, isometry! Group that acts is $\mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$
3. Finding $\mu : \mathscr{C} \to \mathscr{D}$ given $\mathscr{C}, \mathscr{D}$ is hard (matrix code equivalence)

**pre-quantum signatures**

Cyclic group $G$ of order $q$



**Without the group structure, there is the problem of *soundness***

## group actions from equivalence

*In theory*

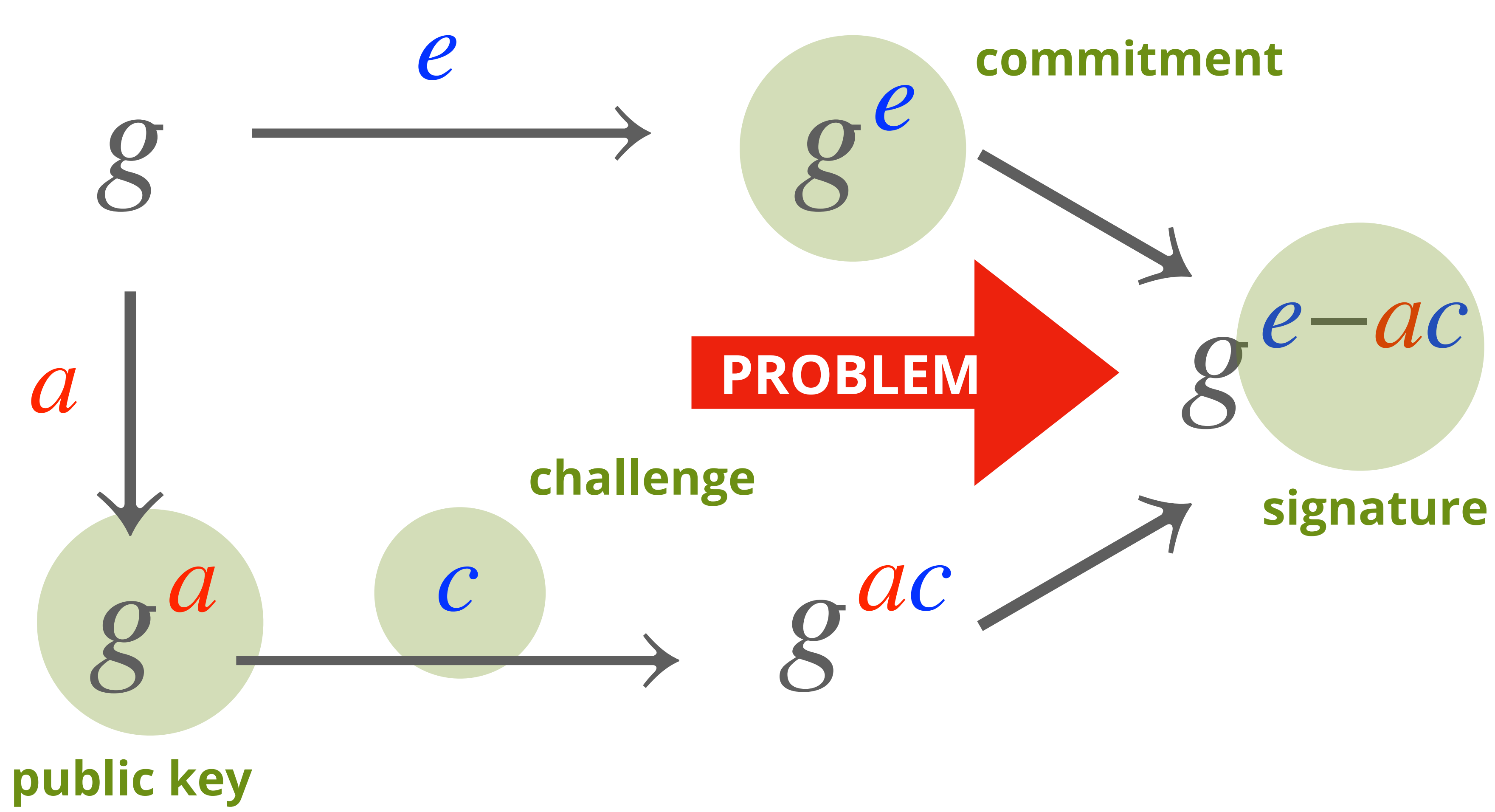
1. Take mathematical objects $X \in \mathrm{Obj}(C)$ with some structure
2. Take the natural maps $\mu \in \mathrm{Hom}(C)$ that preserve this structure
3. Fingers crossed that it is cryptographically hard to find the map $\mu$ given the objects $X, Y$, where $\mu : X \to Y$

*In practice (MEDS)*

1. Objects: $k$-dimensional matrix codes, e.g. *Grasmannian* $\mathrm{Gr}_k(\mathbb{F}_q^{n\times m})$
2. Maps: $\mu$ preserves the rank, isometry! Group that acts is $\mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$
3. Finding $\mu : \mathscr{C} \to \mathscr{D}$ given $\mathscr{C}, \mathscr{D}$ is hard (matrix code equivalence)

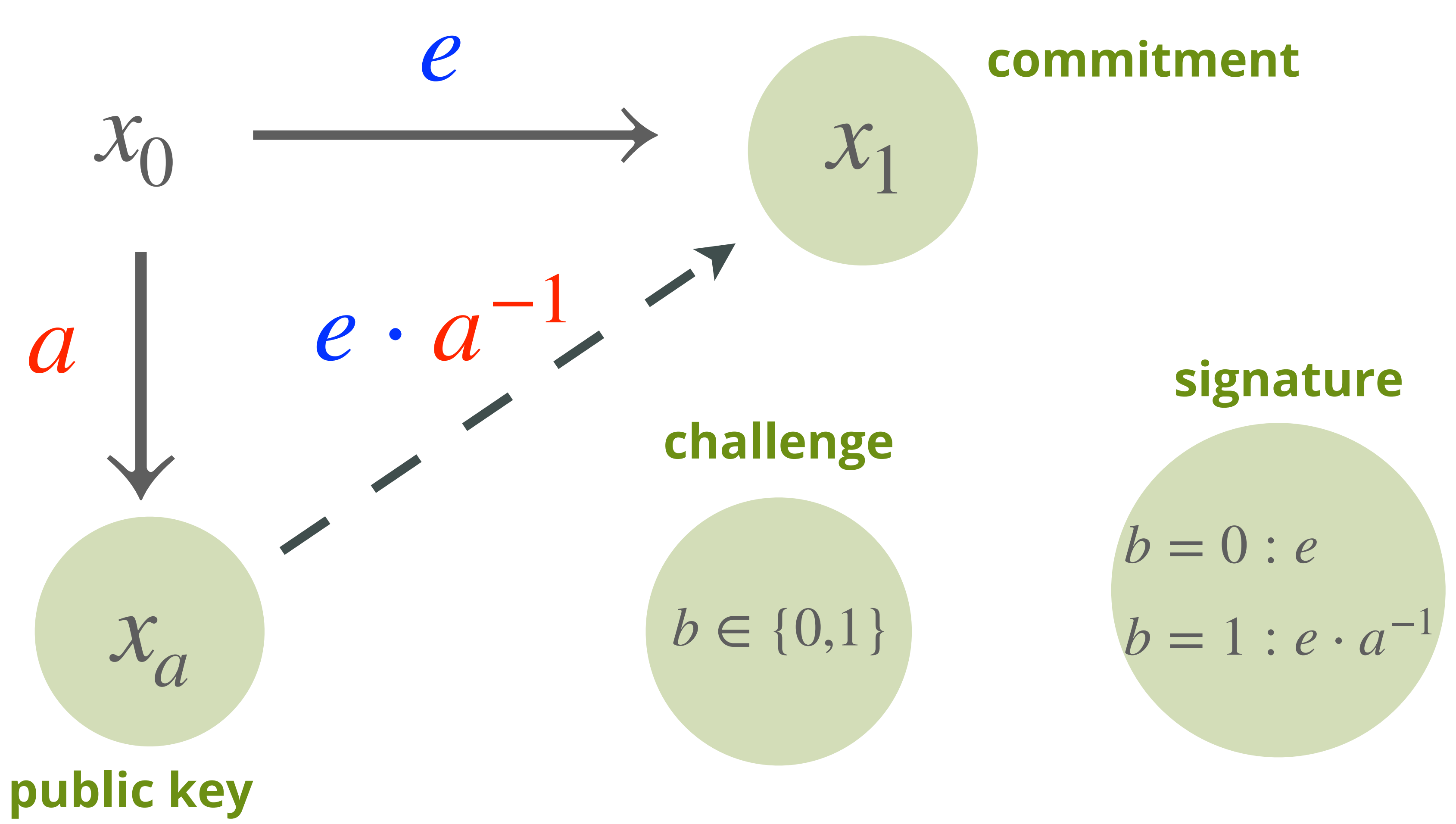
**pre-quantum signatures**

Cyclic group $G$ of order $q$




**group action signatures**

Group action $G$ on $X$



**Without the group structure, there is the problem of *soundness***

## group actions from equivalence

*In theory*

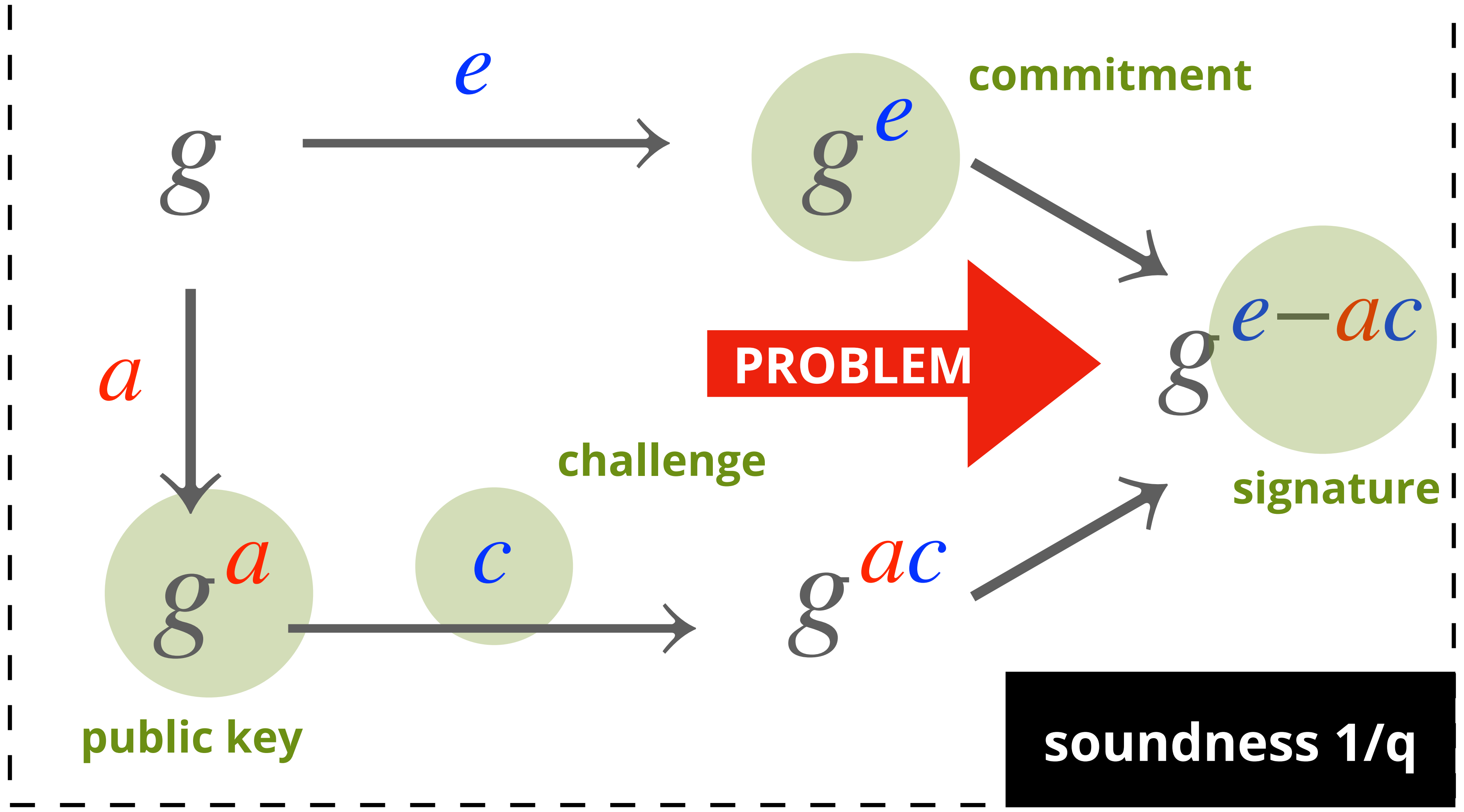
1. Take mathematical objects $X \in \mathrm{Obj}(C)$ with some structure
2. Take the natural maps $\mu \in \mathrm{Hom}(C)$ that preserve this structure
3. Fingers crossed that it is cryptographically hard to find the map $\mu$ given the objects $X, Y$, where $\mu : X \to Y$

*In practice (MEDS)*

1. Objects: $k$-dimensional matrix codes, e.g. *Grasmannian* $\mathrm{Gr}_k(\mathbb{F}_q^{n \times m})$
2. Maps: $\mu$ preserves the rank, isometry! Group that acts is $\mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$
3. Finding $\mu : \mathscr{C} \to \mathscr{D}$ given $\mathscr{C}, \mathscr{D}$ is hard (matrix code equivalence)

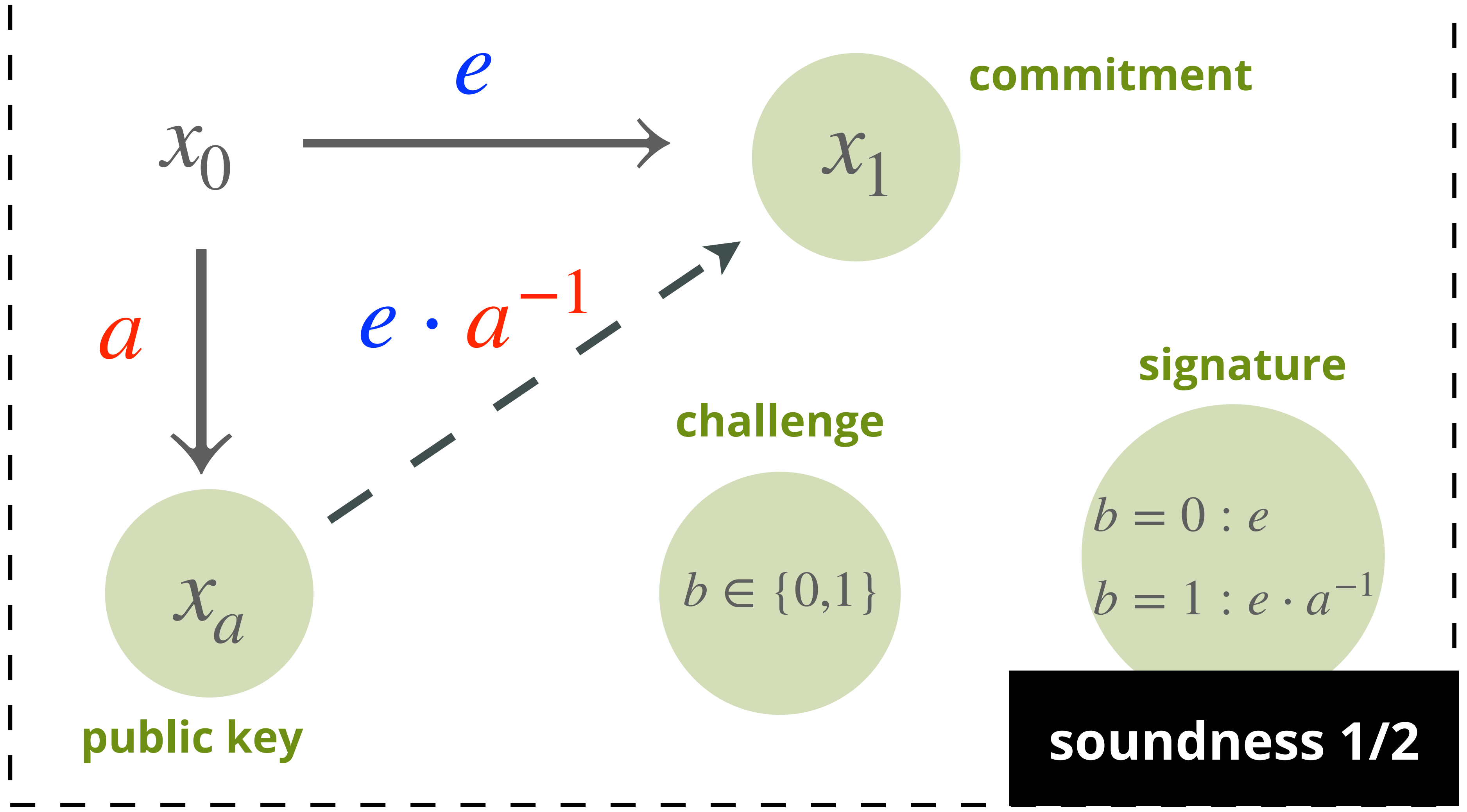
**pre-quantum signatures**

Cyclic group $G$ of order $q$

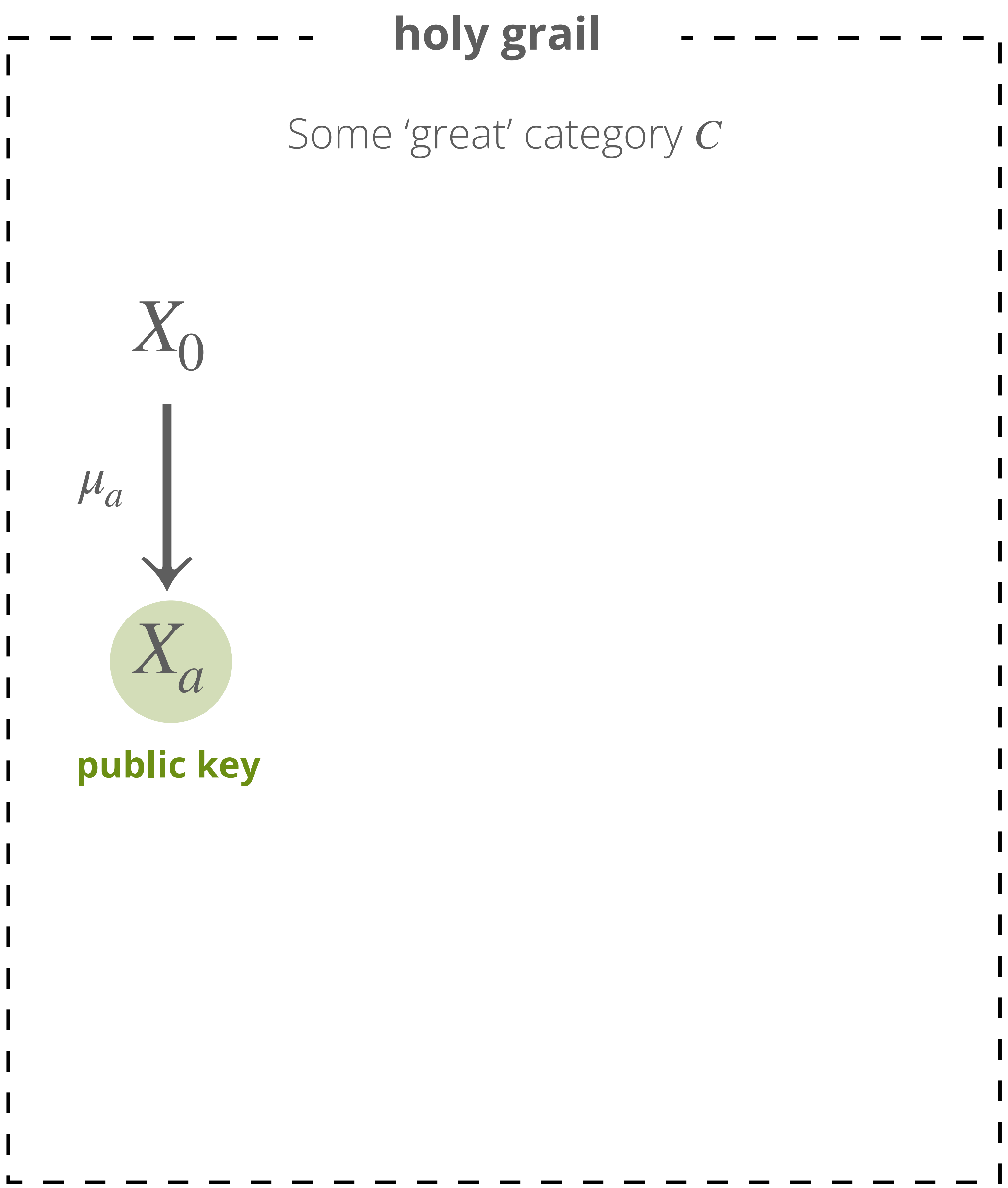



**group action signatures**

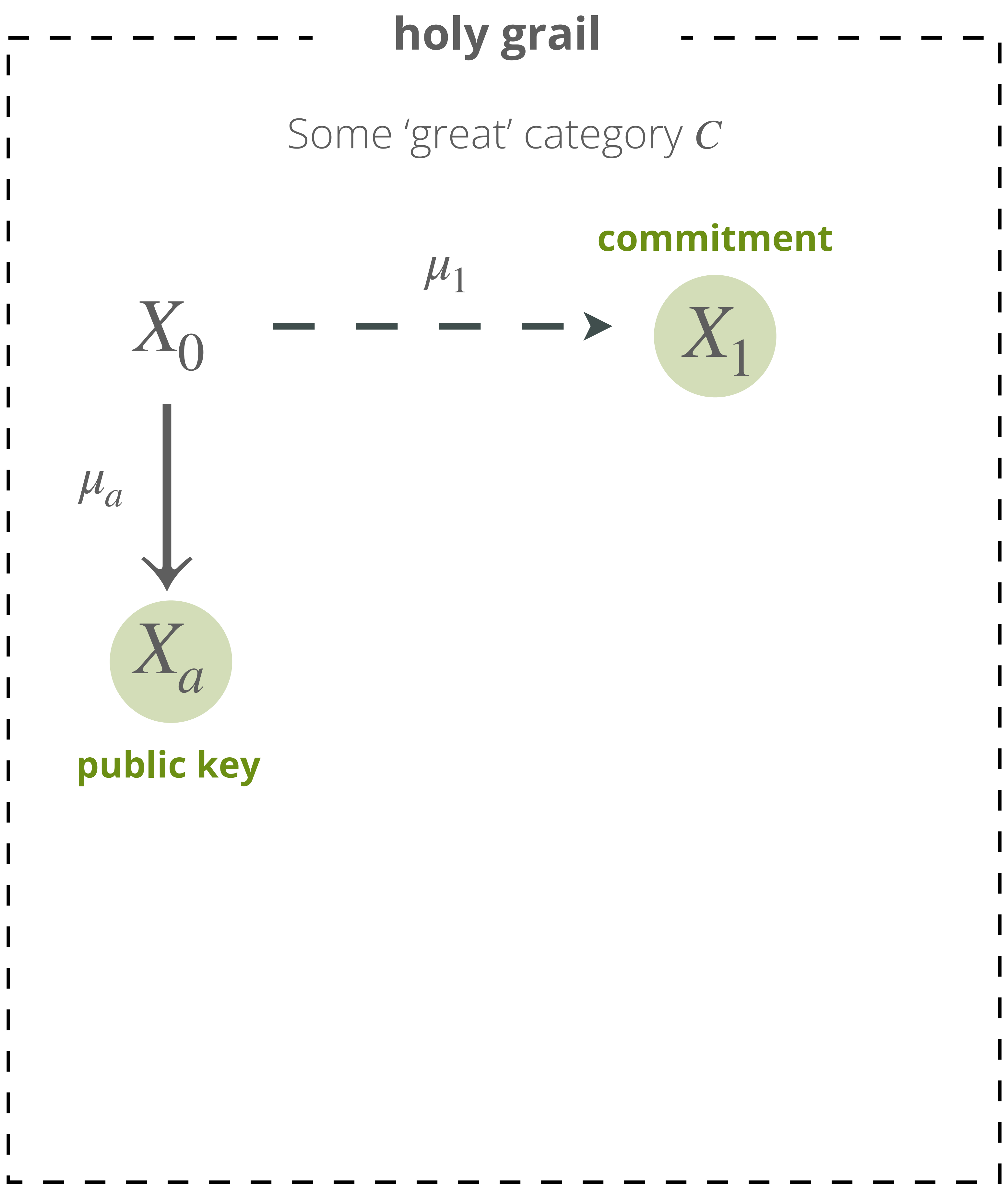
Group action $G$ on $X$



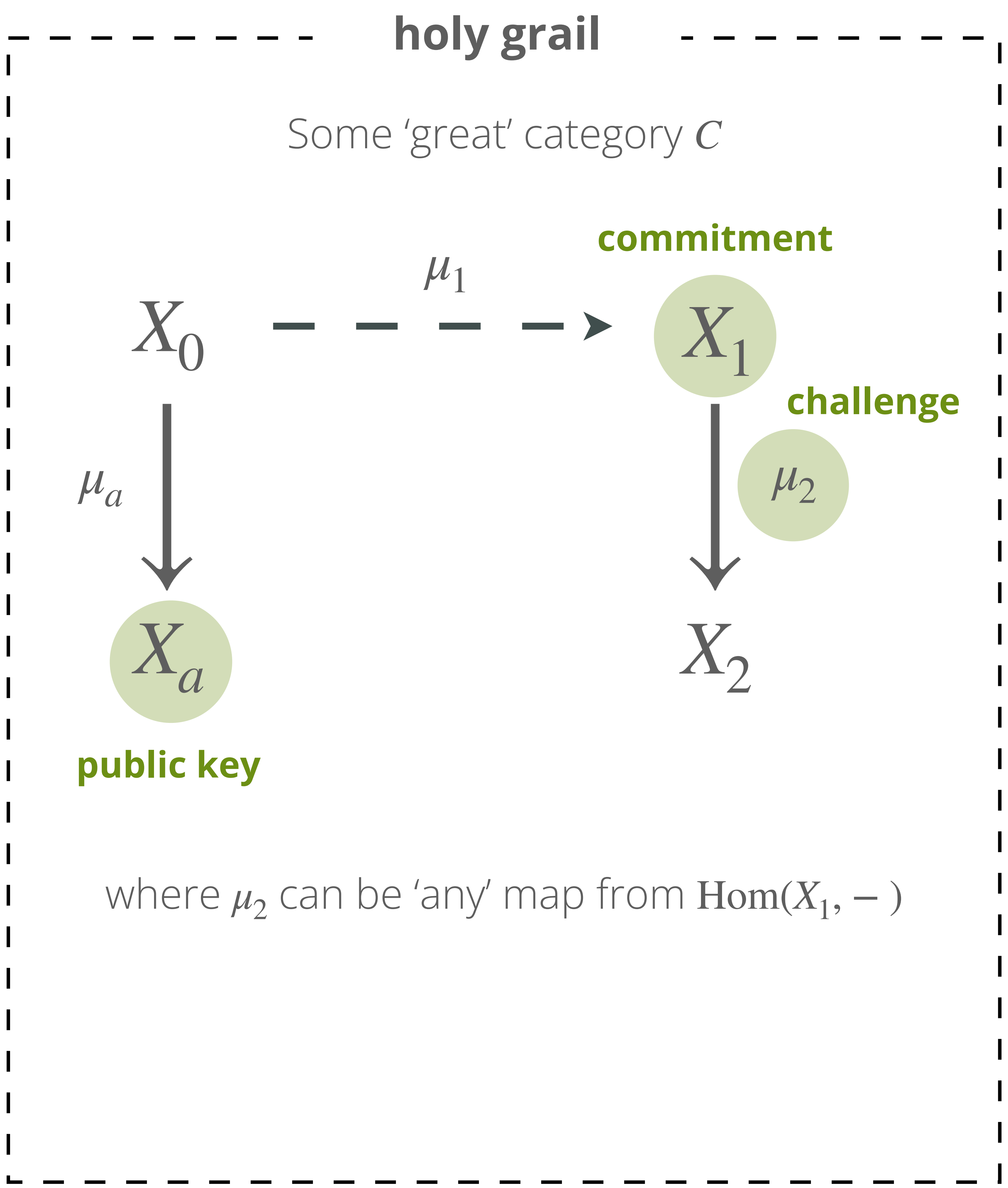
**The holy grail is *post-quantum* high soundness**



## The holy grail is *post-quantum* high soundness



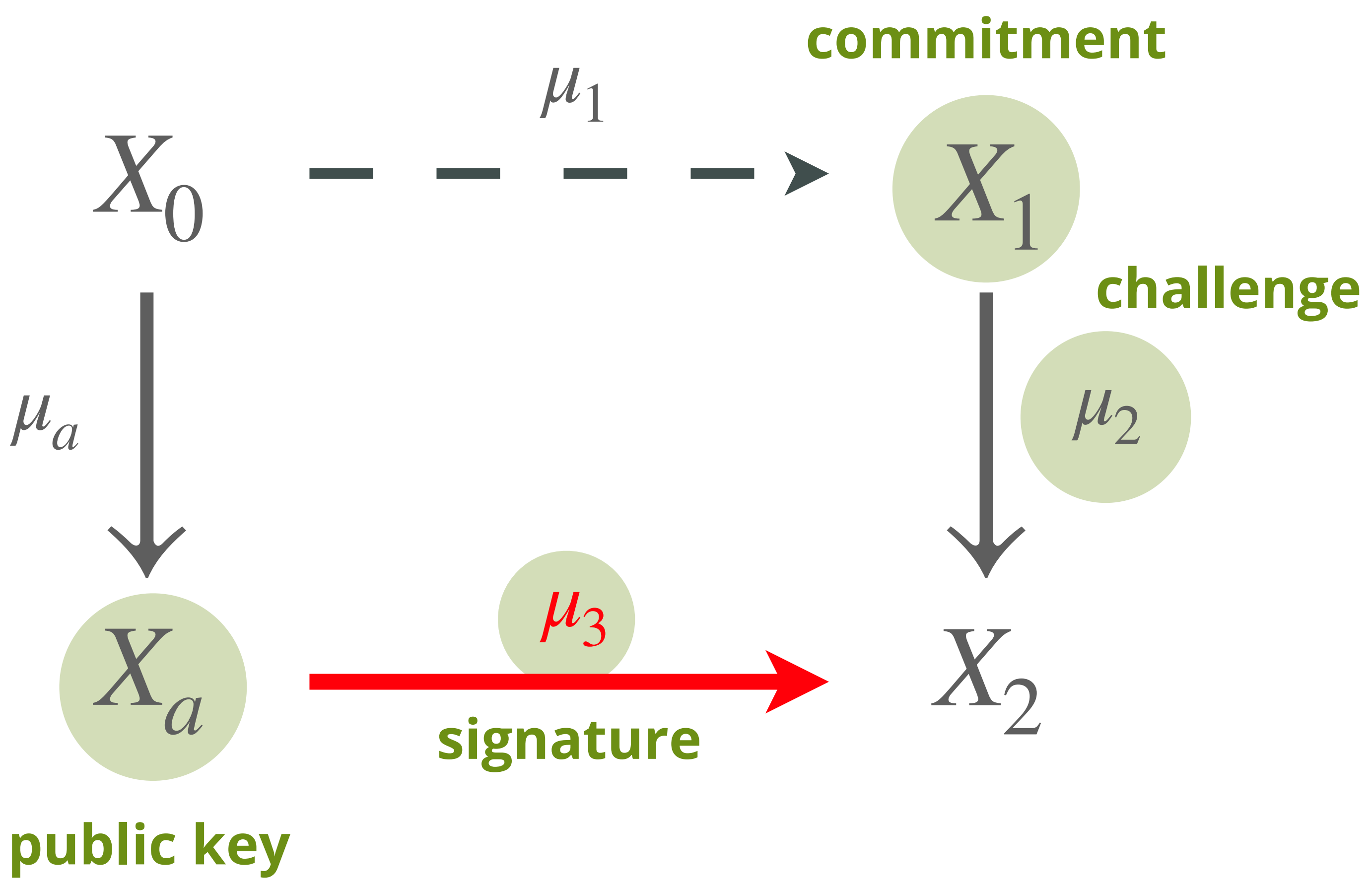
## The holy grail is *post-quantum* high soundness



## The holy grail is *post-quantum* high soundness

**holy grail**

Some ‘great’ category $C$




where $\mu_2$ can be ‘any’ map from $\mathrm{Hom}(X_1, -)$
and we can find $\mu_3$ in such a way
that it leaks nothing on $\mu_a$

**The holy grail is *post-quantum* high soundness**

**holy grail**

Some 'great' category $C$

commitment

challenge

$$\begin{tikzcd}
X_0 \arrow[r, dashed, "\mu_1"] \arrow[d, "\mu_a"'] & X_1 \arrow[d, "\mu_2"] \\
X_a \arrow[r, "\mu_3", "\text{signature}"'] & X_2
\end{tikzcd}$$

public key

where $\mu_2$ can be 'any' map from $\mathrm{Hom}(X_1, -)$
and we can find $\mu_3$ in such a way
that it leaks nothing on $\mu_a$

**MEDS**

$k$-dimensional matrix codes $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

commitment

challenge

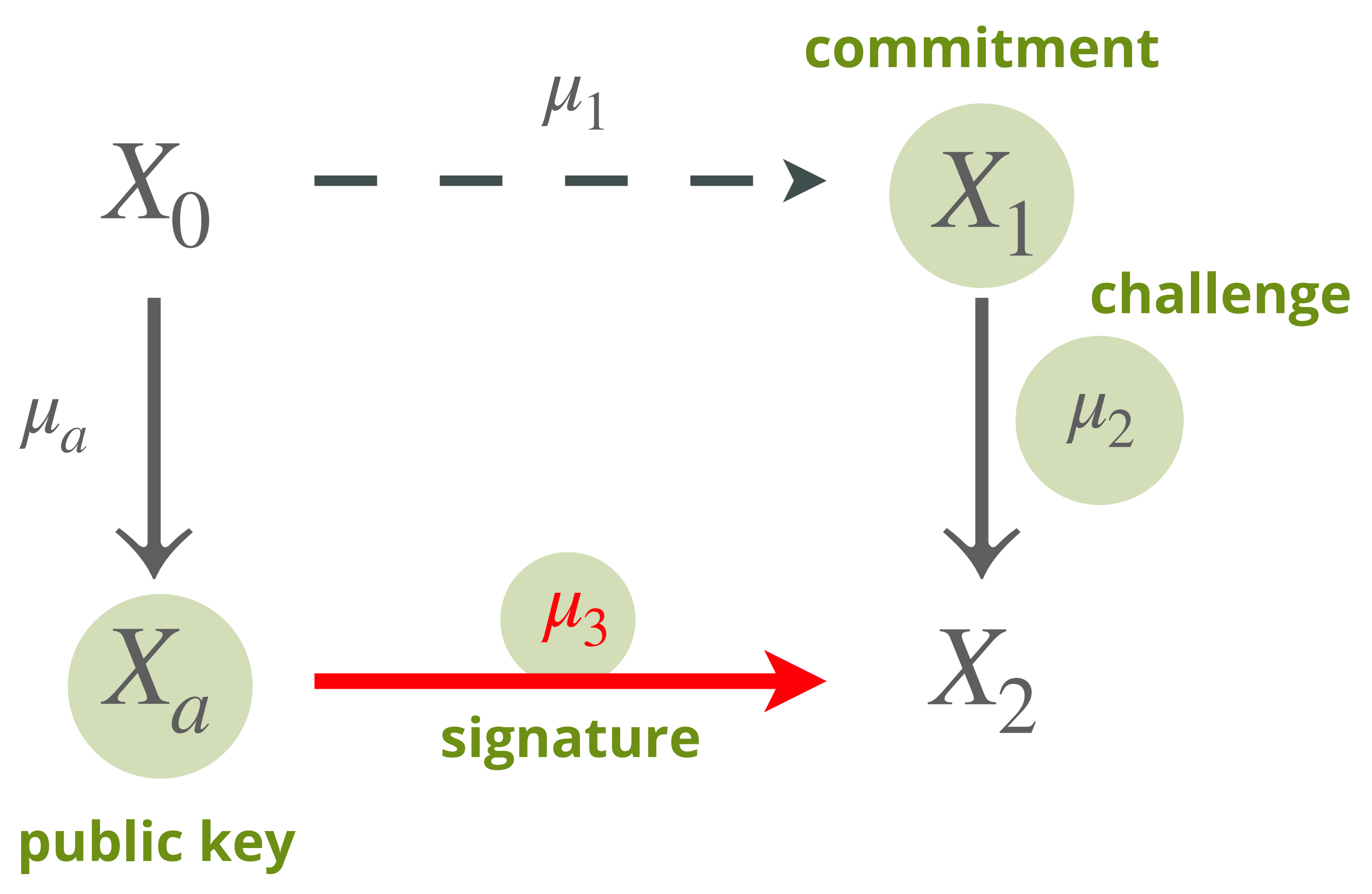
$$\begin{tikzcd}
\mathscr{C}_0 \arrow[r, dashed, "\mu_1"] \arrow[d, "\mu_a"'] & \mathscr{C}_1 \arrow[d, "\mu_2"] \\
\mathscr{C}_a \arrow[r, "\mu_3 = \mu_2 \cdot \mu_1 \cdot \mu_a^{-1}"] & \mathscr{C}_2
\end{tikzcd}$$

public key

# The holy grail is *post-quantum* high soundness

**holy grail**

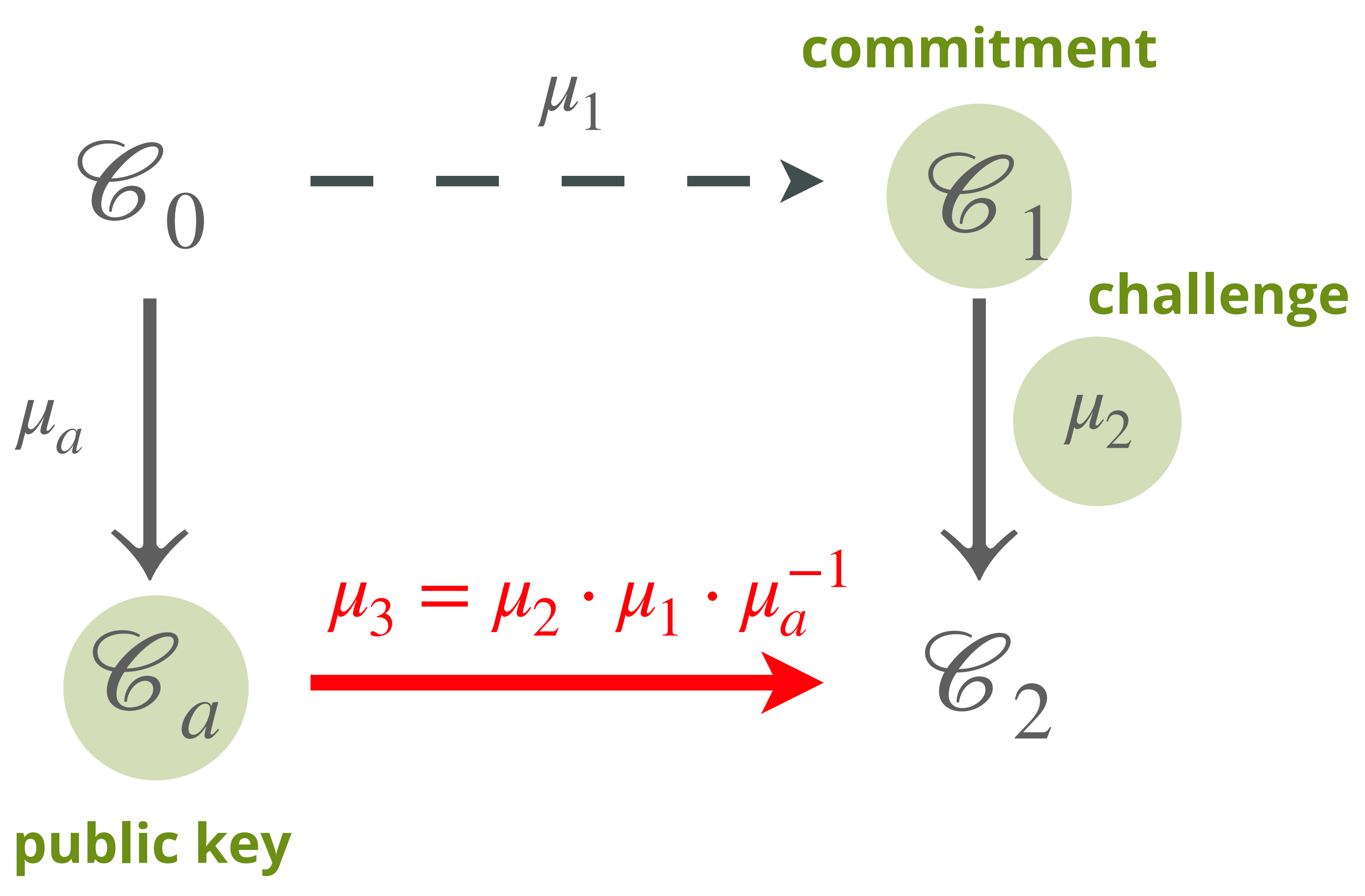
Some 'great' category $C$




where $\mu_2$ can be 'any' map from $\mathrm{Hom}(X_1, -)$
and we can find $\mu_3$ in such a way
that it leaks nothing on $\mu_a$

**MEDS**

$k$-dimensional matrix codes $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$

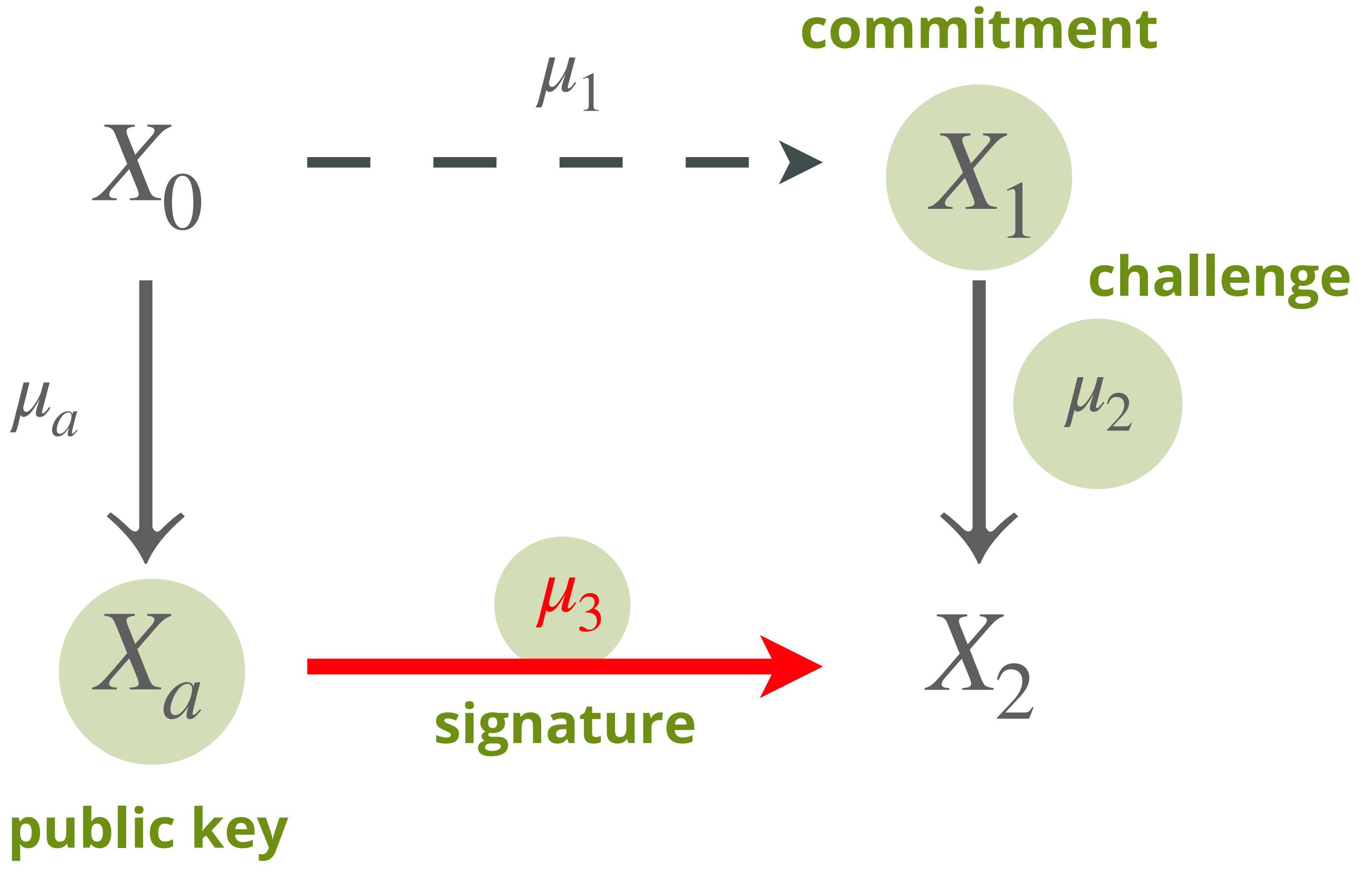



Now $\mu_3$ doesn't show I know $\mu_a$!
It shows I know $\mu_1 \cdot \mu_a^{-1}$, but that is
trivial for anyone given $\mathscr{C}_a$

## The holy grail is *post-quantum* high soundness

### holy grail

Some ‘great’ category $C$

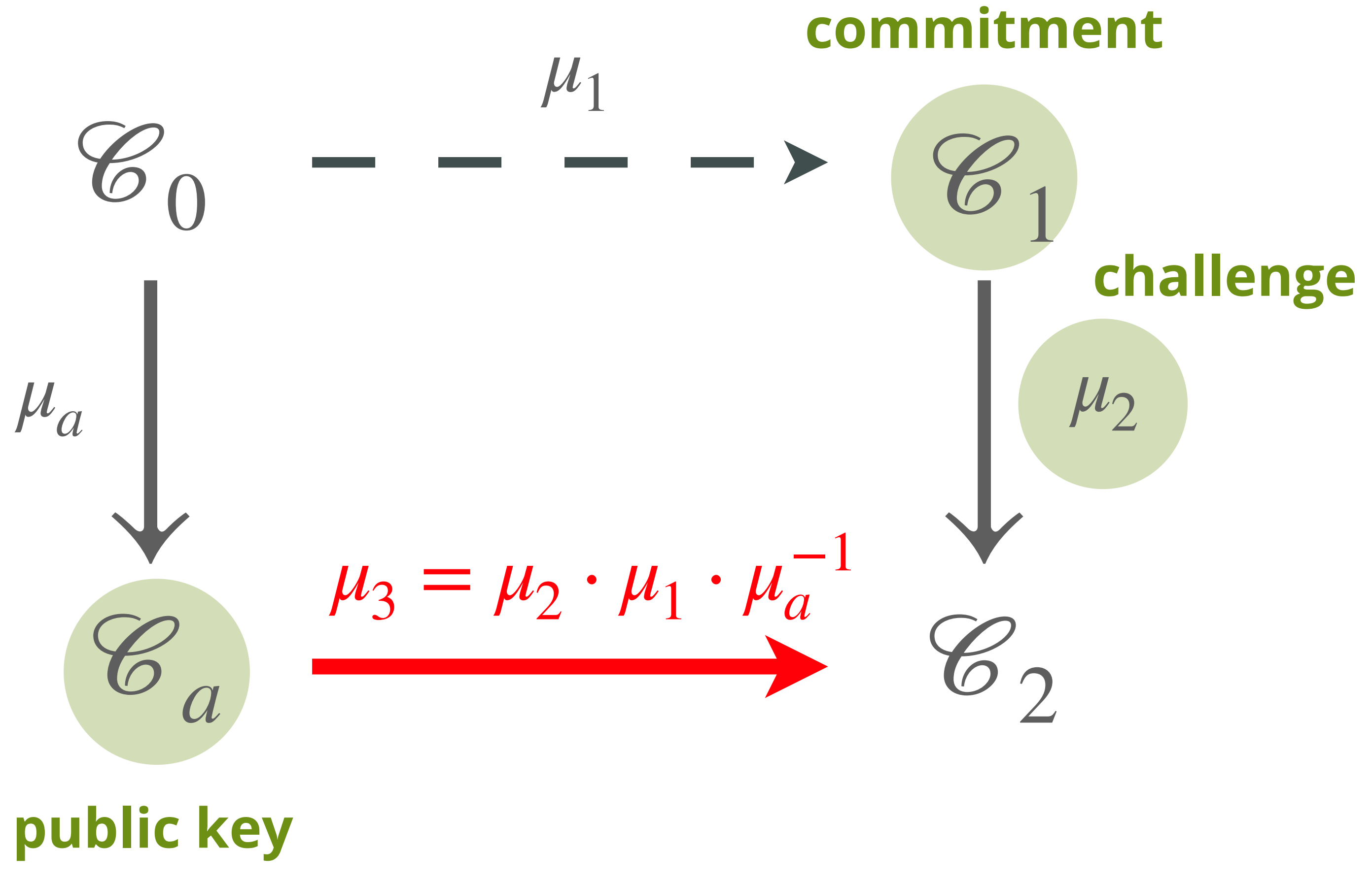



where $\mu_2$ can be ‘any’ map from $\mathrm{Hom}(X_1, -)$
and we can find $\mu_3$ in such a way
that it leaks nothing on $\mu_a$

**soundness: size of hom!**

### MEDS

$k$-dimensional matrix codes $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$




Now $\mu_3$ doesn’t show I know $\mu_a$!
It shows I know $\mu_1 \cdot \mu_a^{-1}$, but that is
trivial for anyone given $\mathscr{C}_a$

# Hints from the *categorical perspective*

**Q**

What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$?

# Hints from the *categorical perspective*

**Q**

What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$?

**A**

$\mathrm{End}(X) = \mathrm{Hom}(X, X)$,
i.e., maps $\mu : X \to X$

# Hints from the *categorical perspective*

abstraction

**Category**

Q

What is a natural object relating $X \in \mathrm{Obj}(C)$ and Hom?

A

$\mathrm{End}(X) = \mathrm{Hom}(X, X)$,
i.e., maps $\mu : X \to X$

**Group actions**

Q

What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

# Hints from the *categorical perspective*

*abstraction*

**Category**

Q

What is a natural object relating $X \in \mathrm{Obj}(C)$ and Hom?

A

$\mathrm{End}(X) = \mathrm{Hom}(X, X)$,
i.e., maps $\mu : X \to X$

**Group actions**

Q

What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

A

$g \in G$ such that $g \star X = X$
e.g. *stabilisers* of $X$

# Hints from the *categorical perspective*

abstraction

**Category**

Q

What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$?

A

$\mathrm{End}(X) = \mathrm{Hom}(X, X)$, i.e., maps $\mu : X \to X$

**Group actions**

Q

What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

A

$g \in G$ such that $g \star X = X$
e.g. *stabilisers* of $X$

**Matrix codes**

Q

What stabilises a matrix code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

# Hints from the *categorical perspective*

*abstraction*

**Category**

**Q** What is a natural object relating $X \in \mathrm{Obj}(C)$ and Hom?

**A** $\mathrm{End}(X) = \mathrm{Hom}(X, X)$, i.e., maps $\mu : X \to X$

**Group actions**

**Q** What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

**A** $g \in G$ such that $g \star X = X$ e.g. *stabilisers* of $X$

**Matrix codes**

**Q** What stabilises a matrix code $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$

**A** $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$

# Hints from the *categorical perspective*

*abstraction*

**Category**

**Q** What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$?

**A** $\mathrm{End}(X) = \mathrm{Hom}(X, X)$, i.e., maps $\mu : X \to X$

**Group actions**

**Q** What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

**A** $g \in G$ such that $g \star X = X$ e.g. *stabilisers* of $X$

**Matrix codes**

**Q** What stabilises a matrix code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

**A** $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$

$$\begin{tikzcd} \mathrm{End}(X_0) \circlearrowright X_0 \arrow[d, "\mu_a"'] \\ \mathrm{End}(X_a) \circlearrowright X_a \end{tikzcd}$$

# Hints from the *categorical perspective*

*abstraction*

| | Q | | A |
|---|---|---|---|
| **Category** | What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$? | ▶ | $\mathrm{End}(X) = \mathrm{Hom}(X, X)$, i.e., maps $\mu : X \to X$ |
| **Group actions** | What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action? | ▶ | $g \in G$ such that $g \star X = X$ e.g. *stabilisers* of $X$ |
| **Matrix codes** | What stabilises a matrix code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$ | ▶ | $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$ |

$$
\begin{tikzcd}
X_0 \arrow[loop left, "\mathrm{End}(X_0)"] \arrow[r, dashed, "\mu_1"] \arrow[d, "\mu_a"'] & X_1 \arrow[d, "\mu_2"] \\
X_a \arrow[loop left, "\mathrm{End}(X_a)"'] \arrow[r, red, "\mu_3"] & X_2
\end{tikzcd}
$$

# Hints from the *categorical perspective*

*abstraction*

**Category**

**Q** What is a natural object relating $X \in \mathrm{Obj}(C)$ and $\mathrm{Hom}$?

**A** $\mathrm{End}(X) = \mathrm{Hom}(X, X)$, i.e., maps $\mu : X \to X$

**Group actions**

**Q** What is $\mathrm{End}(X)$ for $X \in \mathrm{Obj}(C)$ where we had group action?

**A** $g \in G$ such that $g \star X = X$ e.g. *stabilisers* of $X$

**Matrix codes**

**Q** What stabilises a matrix code $\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

**A** $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$

$$\begin{tikzcd} X_0 \arrow[loop left, "\mathrm{End}(X_0)"] \arrow[r, dashed, "\mu_1"] \arrow[d, "\mu_a"'] & X_1 \arrow[d, "\mu_2"] \\ X_a \arrow[loop left, "\mathrm{End}(X_a)"'] \arrow[r, "\mu_3"] & X_2 \end{tikzcd}$$

## wishlist

- for random $X$, hard to compute $\mathrm{End}(X)$
- for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- knowledge of $\mathrm{End}$ is "contagious"
- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

# Quick check: matrix code equivalence

**Objects**

$k$-dimensional matrix codes
$\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$

**Morphisms**

isometries (preserve rank)
$\mu \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$

**End($X$)**

$A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$
such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$
(automorphisms)

**wishlist**

- for random $X$, hard to compute $\mathrm{End}(X)$
- for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- knowledge of End is "contagious"
- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

# Quick check: matrix code equivalence

**Objects**

$k$-dimensional matrix codes
$\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

**Morphisms**

isometries (preserve rank)
$\mu \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$

**End($X$)**

$A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$
such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$
(automorphisms)

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of $\mathrm{End}$ is "contagious"

- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

# Quick check: matrix code equivalence

**Objects**

$k$-dimensional matrix codes
$\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

**Morphisms**

isometries (preserve rank)
$\mu \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$

**End(*X*)**

$A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$
such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$
(automorphisms)

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of $\mathrm{End}$ is "contagious"

- X can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

# Quick check: matrix code equivalence would need new ideas

**Objects**

$k$-dimensional matrix codes

$\mathscr{C} \subseteq \mathbb{F}_q^{n \times m}$

**Morphisms**

isometries (preserve rank)

$\mu \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$

**End($X$)**

$A \in \mathrm{GL}_n(\mathbb{F}_q)$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$
such that $ACB \in \mathscr{C}$ for all $C \in \mathscr{C}$
(automorphisms)

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of $\mathrm{End}$ is “contagious”
- X can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- ? but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- ? hence, $\mu_3$ proves knowledge of $\mu_a$

# the miracle of SQISign

## The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End(*X*)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

**wishlist**

- for random $X$, hard to compute $\mathrm{End}(X)$
- for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- knowledge of $\mathrm{End}$ is "contagious"
- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

## The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End(*X*)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

### Endomorphism problem

Given: a supersingular elliptic curve $E$ over a finite field $\mathbb{F}_{p^2}$

Goal: compute $\mathrm{End}(E)$

assumed to be **hard** (equivalent to finding isogeny $\varphi : E \to E'$ given only $E, E'$)

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- knowledge of End is "contagious"
- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

## The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End(*X*)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

### starting curve

$$E_0 : y^2 = x^3 + x$$

$$\mathrm{End}(E_0) = \mathbb{Z} + \imath\mathbb{Z} + \frac{\imath + \pi}{2}\mathbb{Z} + \frac{1 + \imath \cdot \pi}{2}\mathbb{Z}$$

$$\imath : E \to E, \quad (x, y) \mapsto (-x, i \cdot y)$$

$$\pi : E \to E, \quad (x, y) \mapsto (x^p, y^p)$$

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- knowledge of End is "contagious"
- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

## The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End($X$)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

### contagious knowledge

Given two supersingular curves $E, E'$ and an isogeny $\varphi : E \to E'$

Assume you know $\mathrm{End}(E)$, then you can compute $\mathrm{End}(E')$

$$\psi \circlearrowright E \underset{\hat{\varphi}}{\overset{\varphi}{\rightleftarrows}} E'$$

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of $\mathrm{End}$ is "contagious"

- can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

# The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End(*X*)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

## computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of End is "contagious"
- ✓ can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- hence, $\mu_3$ proves knowledge of $\mu_a$

## The category that has *everything!*

**Objects**

supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to isomorphism)

**Morphisms**

isometries (preserve group) $\varphi : E \to E/G$

**End(*X*)**

isogenies $\varphi : E \to E$ are called endomorphisms, $\mathrm{End}(E)$ is *ring*

### computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

🪄 **Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**wishlist**

- ✓ for random $X$, hard to compute $\mathrm{End}(X)$
- ✓ for some $X_0$ we know/compute $\mathrm{End}(X_0)$
- ✓ knowledge of End is "contagious"
- ✓ can **only** compute $\mu_3$ if I know $\mathrm{End}(X_a)$
- 👋 but $\mu_3$ leaks **nothing** on $\mu_a$ or $\mathrm{End}(X_a)$
- 👋 hence, $\mu_3$ proves knowledge of $\mu_a$

## The magic is given by a fascinating fact: the Deuring correspondence

**computing the signature**

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

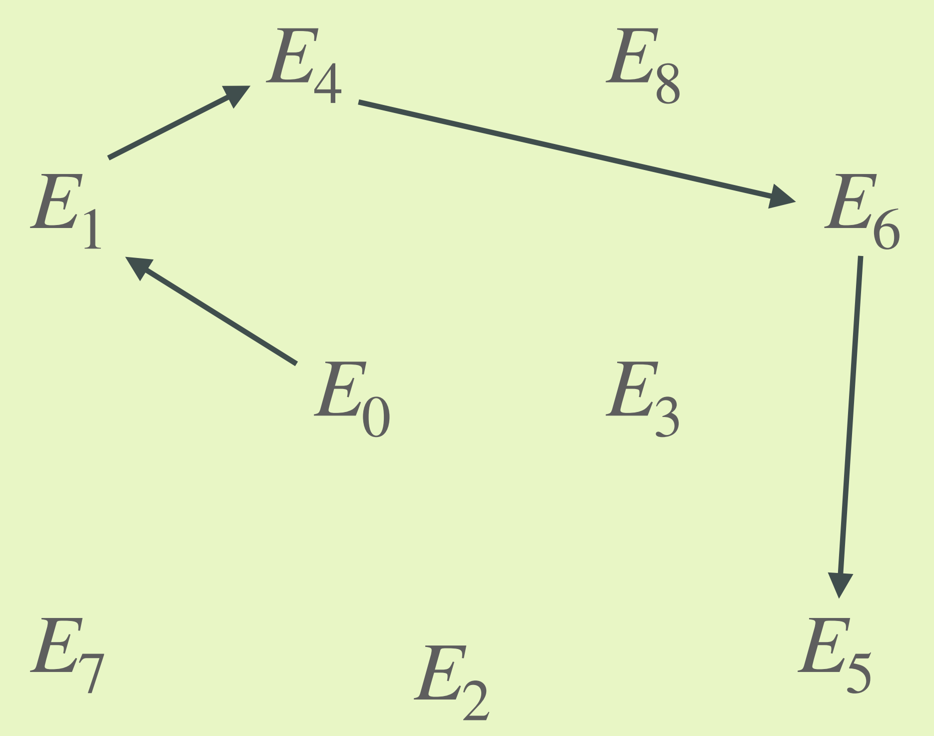
Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

✨ **Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

## The magic is given by a fascinating fact: the Deuring correspondence

**Deuring correspondence**

world of supersingular curves




### computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence

world of supersingular curves | world of maximal orders


### computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, red, "\varphi_3"] & E_2 \end{tikzcd}$$

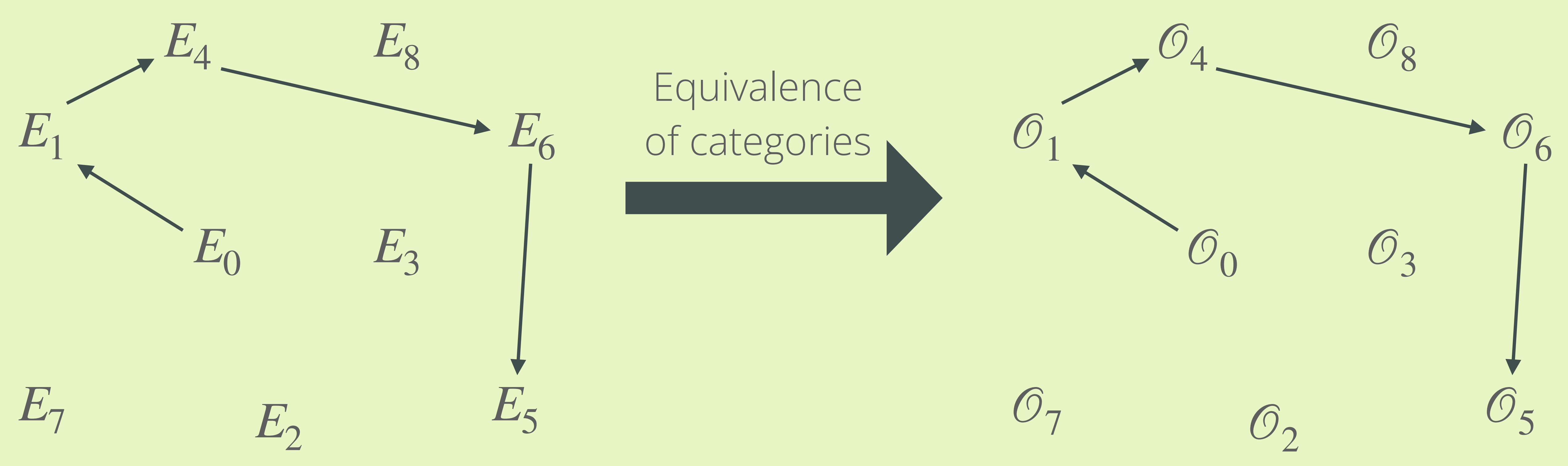
Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




### computing the signature

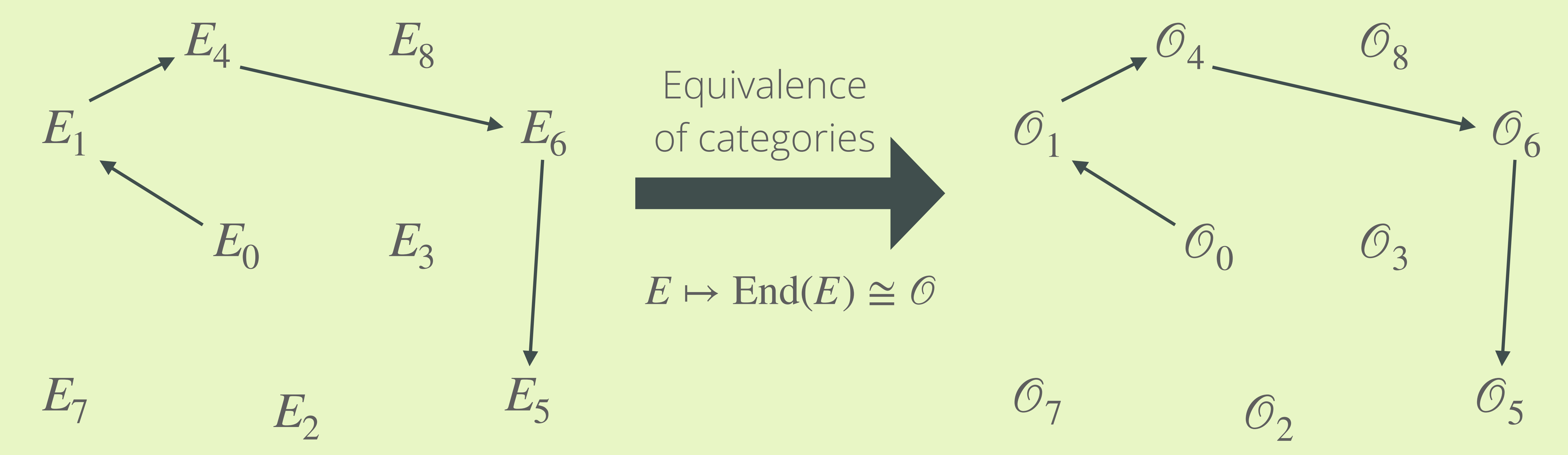
$$
\begin{tikzcd}
E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\
E_a \arrow[r, "\varphi_3"] & E_2
\end{tikzcd}
$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence




## computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

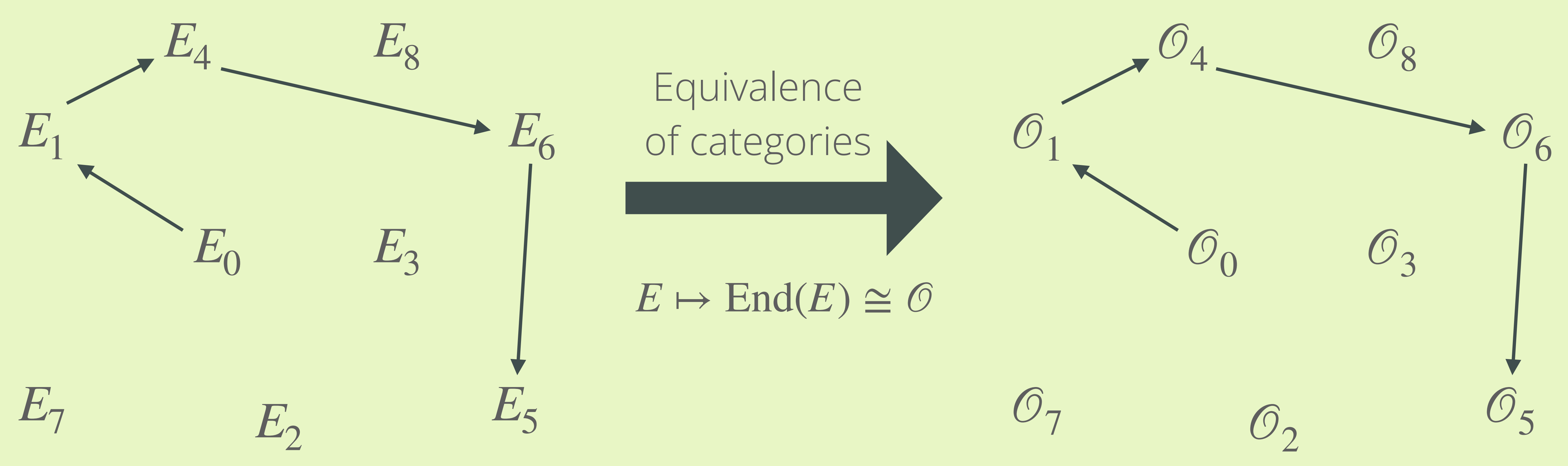
Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




## computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

🪄 **Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

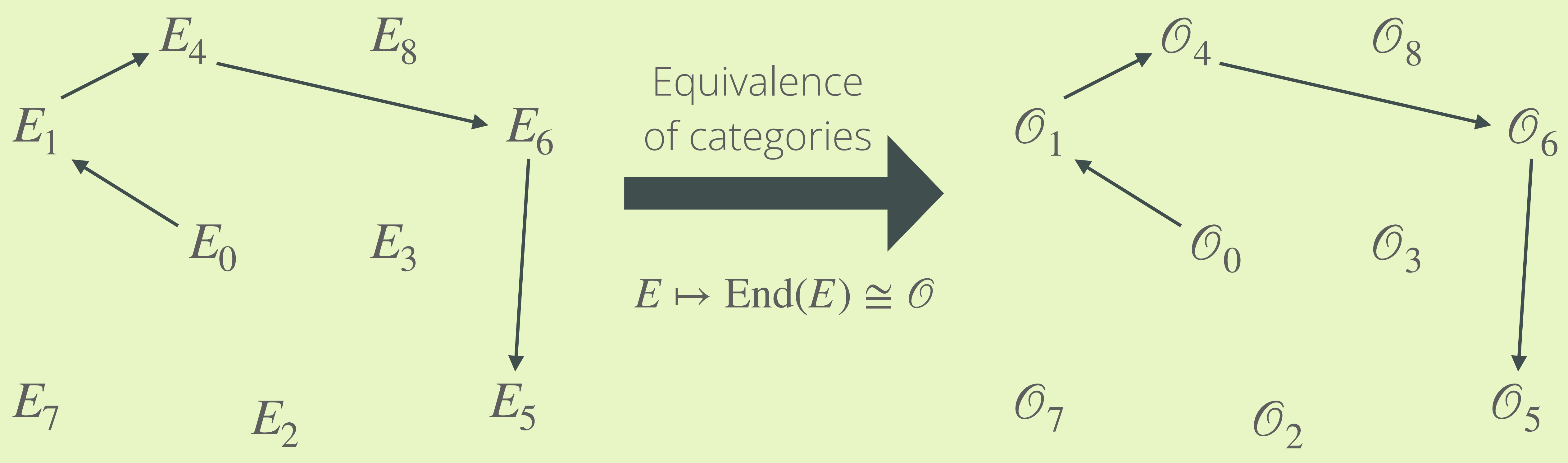
## curve-order dictionary

| supersingular curves | quaternion orders |
|---|---|

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




## computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, red, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

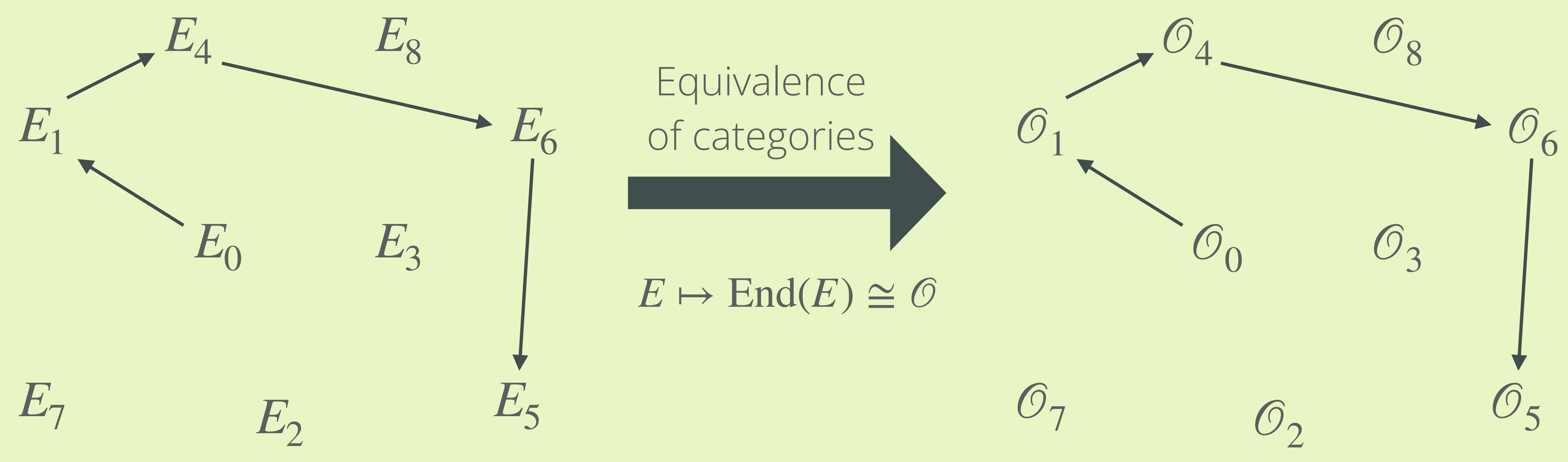
## curve-order dictionary

| supersingular curves | quaternion orders |
|---|---|
| curve $E$ (up to Galois conjugacy) | maximal order $\mathcal{O}$ (up to isomorphism) |

**The magic is given by a fascinating fact: the Deuring correspondence**

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




## computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

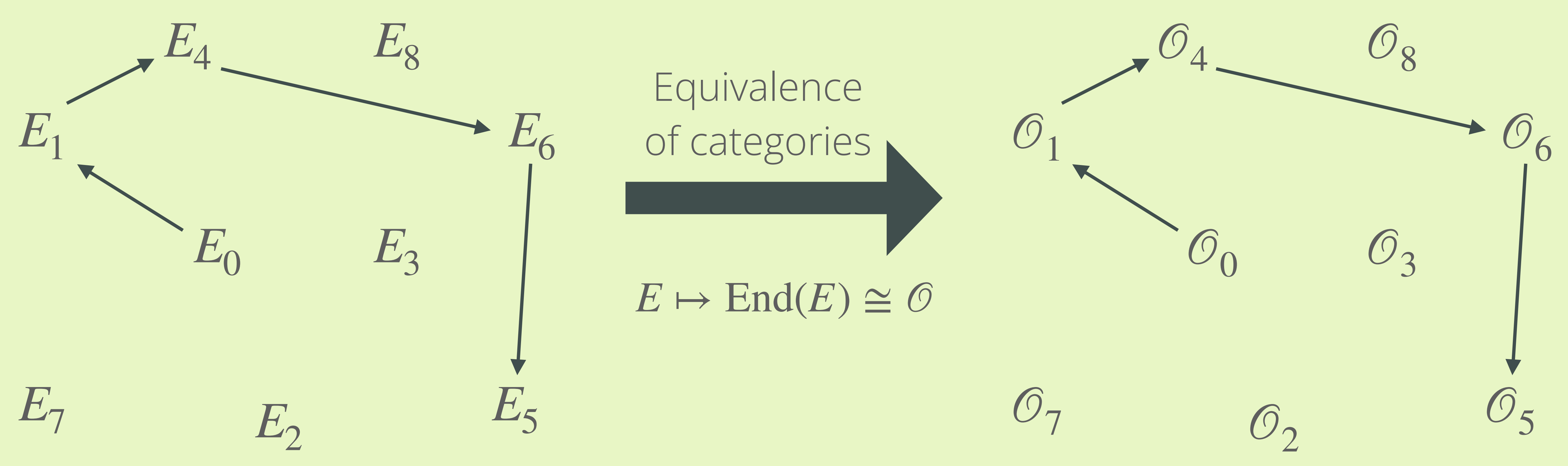
## curve-order dictionary

| supersingular curves | quaternion orders |
|---|---|
| curve $E$ (up to Galois conjugacy) | maximal order $\mathcal{O}$ (up to isomorphism) |
| isogeny $\varphi : E_1 \to E_2$ | integral ideal $I_\varphi$ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal |
| endomorphism $\psi : E \to E$ | principal ideal $(\beta) \subset \mathcal{O}$ |

## The magic is given by a fascinating fact: the Deuring correspondence

## Deuring correspondence

**world of supersingular curves** | **world of maximal orders**




### computing the signature

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_1"] \arrow[d, "\varphi_a"'] & E_1 \arrow[d, "\varphi_2"] \\ E_a \arrow[r, "\varphi_3"] & E_2 \end{tikzcd}$$

Only if you know $\varphi_a$, you can know $\mathrm{End}(E_a)$

**Fact:** Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

## curve-order dictionary

| **supersingular curves** | **quaternion orders** |
|---|---|
| curve $E$ (up to Galois conjugacy) | maximal order $\mathcal{O}$ (up to isomorphism) |
| isogeny $\varphi : E_1 \to E_2$ | integral ideal $I_\varphi$ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal |
| endomorphism $\psi : E \to E$ | principal ideal $(\beta) \subset \mathcal{O}$ |
| and this continues for the *degree*, the *dual*, *equivalence*, *composition*… | and this continues for the *norm*, the *dual*, *equivalence*, *multiplication*… |

# Wrapping up: (where) can we find the holy grail?

# Wrapping up: (where) can we find the holy grail?

**isogenies**

- Is the security of SQISign somehow related to the slowness of the functor?
- Are CSIDH and SQISign the only ‘miracles’ for post-quantum key exchange/signatures?
- Is it a coincidence that both structures come from isogenies?
- Is there something deeply mathematical about elliptic curves over finite fields that makes them perfect for cryptographic design and protocols?

# Wrapping up: (where) can we find the holy grail?

**isogenies**

- Is the security of SQISign somehow related to the slowness of the functor?
- Are CSIDH and SQISign the only 'miracles' for post-quantum key exchange/signatures?
- Is it a coincidence that both structures come from isogenies?
- Is there something deeply mathematical about elliptic curves over finite fields that makes them perfect for cryptographic design and protocols?

**holy grail**

- Are there other mathematical objects or categories that imply a cryptographic group action, hence key exchange?
- Are there other 'perfect' categories that allow an easily designed digital signature with high soundness (hence small signatures)
- Can we deduce from `the wishlist' how such categories should behave? Can they be faster?
- Are they always functorially equivalent to orders in quaternion algebras perhaps?
- Can **the holy grail** even exist?