SQISIGN
COMPACT POST-QUANTUM SIGNATURE FROM QUATERNIONS AND ISOGENIES

LFANT seminar
November 2021
IMB, Bordeaux, France

Based on a joint work with
Luca De Feo, David Kohel, Antonin Leroux and Christophe Petit

Benjamin Wesolowski

SQISIGN

A post-quantum signature scheme

THE STATE OF POST-QUANTUM CRYPTOGRAPHY

Six families in Round 3 NIST post-quantum competition (finalists + alternate candidates)

Lattices	4 encryption	2 signature		
Codes	3 encryption			
Multivariate		2 signature		
Isogenies	1 encryption		compact keys	poor efficiency
Hash-based		1 signature		
MPC		1 signature		

THE STATE OF POST-QUANTUM CRYPTOGRAPHY

Six families in Round 3 NIST post-quantum competition (finalists + alternate candidates)

Lattices	**4 encryption**	**2 signature**		
Codes	**3 encryption**			
Multivariate		**2 signature**		
Isogenies	**1 encryption**		**compact keys**	**poor efficiency**
Hash-based		**1 signature**		
MPC		**1 signature**		

Many new isogeny-base schemes since the competition

ISOGENY-BASED SIGNATURES

Generic isogeny feature: compact keys (unless tradeoff)

ISOGENY-BASED SIGNATURES

Generic isogeny feature: compact keys (unless tradeoff)

	Based on	Iterations	Sig. size	Efficiency	
[Yoo+17]	SIDH assumptions	λ	$O(\lambda^2)$	slow	
[GPS17] GPS	endomorphism computation	λ	$O(\lambda^2)$	no. implem.	weaker assumptions
[DG19] SeaSign	CSIDH assumption	λ	tradeoff	very slow	
[BKV19] CSI-FiSh	CSIDH assumption	λ	tradeoff	efficient	subexp. precomp.

λ is the security parameter

SQISIGN: SHORT QUATERNION ISOGENY SIGNATURE

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring

SQISIGN: SHORT QUATERNION ISOGENY SIGNATURE

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring

Most compact PQ signature scheme: PK + Signature combined $5\times$ smaller than Falcon (most compact NIST Round 3)

Secret key (bytes)	Public key (bytes)	Signature (bytes)	**Security**
16	**64**	**204**	**NIST-1**

SQISIGN: SHORT QUATERNION ISOGENY SIGNATURE

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring

Most compact PQ signature scheme: PK + Signature combined $5\times$ smaller than Falcon (most compact NIST Round 3)

Secret key (bytes)	Public key (bytes)	Signature (bytes)	**Security**
16	**64**	**204**	**NIST-1**

Efficient verification and reasonably efficient signature

SQISIGN: SHORT QUATERNION ISOGENY SIGNATURE

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring

Most compact PQ signature scheme: PK + Signature combined $5\times$ smaller than Falcon (most compact NIST Round 3)

Secret key (bytes)	Public key (bytes)	Signature (bytes)	**Security**
16	**64**	**204**	**NIST-1**

Efficient verification and reasonably efficient signature

	Key gen.	Signing	**Verification**
ms	**575**	**2279**	**42**

SQISIGN: SHORT QUATERNION ISOGENY SIGNATURE

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring

Most compact PQ signature scheme: PK + Signature combined $5\times$ smaller than Falcon (most compact NIST Round 3)

Secret key (bytes)	Public key (bytes)	Signature (bytes)	**Security**
16	**64**	**204**	**NIST-1**

Efficient verification and reasonably efficient signature

	Key gen.	Signing	**Verification**
ms	**575**	**2279**	**42**

New security assumption

SUPERSINGULAR ELLIPTIC CURVES

Isogenies, endomorphisms and quaternions

ELLIPTIC CURVES

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an additive group

ELLIPTIC CURVES

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an additive group

An isogeny in a map

$$\varphi : E \longrightarrow F$$

which preserves certain structures. In particular, it is a group homomorphism with a finite kernel $\ker(\varphi)$

ELLIPTIC CURVES

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an additive group

An isogeny in a map

$$\varphi : E \longrightarrow F$$

which preserves certain structures. In particular, it is a group homomorphism with a finite kernel $\ker(\varphi)$

The degree* is $\deg(\varphi) = \#\ker(\varphi)$

* for separable isogenies

ENDOMORPHISM RING

An endomorphism is an isogeny $\varphi : E \longrightarrow E$

ENDOMORPHISM RING

An endomorphism is an isogeny $\varphi : E \longrightarrow E$

They form a ring $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

ENDOMORPHISM RING

An endomorphism is an isogeny $\varphi : E \longrightarrow E$

They form a ring $\mathrm{End}(E)$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

Multiplication by $m \in \mathbb{Z}$ is an endomorphism

$$[m] : E \longrightarrow E : P \longmapsto P + ... + P$$

It forms a subring $\mathbb{Z} \subset \mathrm{End}(E)$

ENDOMORPHISM ALGEBRA

What is the structure of End(E) ?

ENDOMORPHISM ALGEBRA

What is the structure of End(E) ?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...

ENDOMORPHISM ALGEBRA

What is the structure of $\text{End}(E)$?

- It contains $\mathbb{Z} \subset \text{End}(E)$...
- $(\text{End}(E), +)$ is a lattice of dimension 2 or 4

ENDOMORPHISM ALGEBRA

What is the structure of $\mathrm{End}(E)$?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- $(\mathrm{End}(E), +)$ is a lattice of dimension 2 or 4

We say E is supersingular when $\mathrm{End}(E)$ has dimension 4

ENDOMORPHISM ALGEBRA

What is the structure of $\mathrm{End}(E)$?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- $(\mathrm{End}(E), +)$ is a lattice of dimension 2 or 4

We say E is supersingular when $\mathrm{End}(E)$ has dimension 4

Then, there is a $\mathbb{Z}$-basis $1, \alpha_2, \alpha_3, \alpha_4$: as a lattice,

$$\mathrm{End}(E) = \mathbb{Z} \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

ENDOMORPHISM ALGEBRA

What is the structure of End(E) ?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- $(\mathrm{End}(E), +)$ is a lattice of dimension 2 or 4

We say E is supersingular when End(E) has dimension 4

Then, there is a $\mathbb{Z}$-basis 1, α_2, α_3, α_4: as a lattice,

$$\mathrm{End}(E) = \mathbb{Z} \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

The **endomorphism algebra** is the vector space

$$B = \mathbb{Q} \oplus \mathbb{Q}\alpha_2 \oplus \mathbb{Q}\alpha_3 \oplus \mathbb{Q}\alpha_4$$

with a ring structure induced from that of End(E)

QUATERNION ALGEBRA

Given a supersingular elliptic curve over $\mathbb{F}_q$ (of characteristic p), it is easy to compute the endomorphism algebra: it is the quaternion algebra $B_{p,\infty}$

QUATERNION ALGEBRA

Given a supersingular elliptic curve over $\mathbb{F}_q$ (of characteristic p), it is easy to compute the endomorphism algebra: it is the quaternion algebra $B_{p,\infty}$

For instance, if $p \equiv 3 \pmod 4$,

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

QUATERNION ALGEBRA

Given a supersingular elliptic curve over $\mathbb{F}_q$ (of characteristic p), it is easy to compute the endomorphism algebra: it is the quaternion algebra $B_{p,\infty}$

For instance, if $p \equiv 3 \pmod 4$,

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

$\mathrm{End}(E)$ is a discrete subrings of $B_{p,\infty}$

QUATERNION ALGEBRA

Given a supersingular elliptic curve over $\mathbb{F}_q$ (of characteristic p), it is easy to compute the endomorphism algebra: it is the quaternion algebra $B_{p,\infty}$

For instance, if $p \equiv 3 \pmod 4$,

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

$\mathrm{End}(E)$ is a discrete subrings of $B_{p,\infty}$

- $\mathrm{End}(E)$ is a maximal order in $B_{p,\infty}$

QUATERNION ALGEBRA

Given a supersingular elliptic curve over $\mathbb{F}_q$ (of characteristic p), it is easy to compute the endomorphism algebra: it is the quaternion algebra $B_{p,\infty}$

For instance, if $p \equiv 3 \pmod 4$,

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

$\mathrm{End}(E)$ is a discrete subrings of $B_{p,\infty}$

- $\mathrm{End}(E)$ is a maximal order in $B_{p,\infty}$
- There are *many* maximal orders in $B_{p,\infty}$

DEURING CORRESPONDENCE

Supersingular curves $\boldsymbol{E}$ over $\mathbb{F}_{p^2}$	Maximal orders in $B_{p,\infty}$
(up to isomorphism)	$\mathcal{O} \simeq \mathbf{End}(\boldsymbol{E})$
	(up to equivalence)

DEURING CORRESPONDENCE

Supersingular curves E over $\mathbb{F}_{p^2}$ *(up to isomorphism)*	Maximal orders in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ *(up to equivalence)*
Isogenies $\varphi : E \longrightarrow F$	Left $\mathcal{O}$-ideals I_φ

DEURING CORRESPONDENCE

Supersingular curves E over $\mathbb{F}_{p^2}$ *(up to isomorphism)*	Maximal orders in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ *(up to equivalence)*
Isogenies $\varphi : E \longrightarrow F$	Left $\mathcal{O}$-ideals I_φ
Degree $\mathbf{deg}(\varphi)$	Norm $\mathbf{n}(I_\varphi)$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\pi^2 = [-p]$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\quad \pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\quad \pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\quad \pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

$$\mathrm{End}(E_0) \overset{?}{=} \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\pi \oplus \mathbb{Z}\iota\pi$$

$$\simeq \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij \subset B_{p,\infty}$$

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\quad \pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

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

DEURING CORRESPONDENCE

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

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

Two non-trivial endomorphisms:

- $\pi : E_0 \longrightarrow E_0 : (x, y) \longmapsto (x^p, y^p)$ $\quad \pi^2 = [-p]$
- $\iota : E_0 \longrightarrow E_0 : (x, y) \longmapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

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

$$\simeq \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i + j}{2} \oplus \mathbb{Z}\frac{1 + k}{2} \subset B_{p,\infty}$$

COMPUTATIONAL DEURING CORRESPONDENCE

For $E_0 : y^2 = x^3 + x$, it is easy to compute $\text{End}(E_0)$

COMPUTATIONAL DEURING CORRESPONDENCE

For $E_0 : y^2 = x^3 + x$, it is easy to compute $\mathrm{End}(E_0)$

- It is an exception

COMPUTATIONAL DEURING CORRESPONDENCE

For $E_0 : y^2 = x^3 + x$, it is easy to compute $\mathrm{End}(E_0)$

- It is an exception

In general:

- It is hard to compute $\mathrm{End}(E)$

COMPUTATIONAL DEURING CORRESPONDENCE

For $E_0 : y^2 = x^3 + x$, it is easy to compute $\mathrm{End}(E_0)$

- It is an exception

In general:

- It is hard to compute $\mathrm{End}(E)$
- It is hard to find any element of $\mathrm{End}(E)$ not in $\mathbb{Z}$

COMPUTATIONAL DEURING CORRESPONDENCE

For $E_0 : y^2 = x^3 + x$, it is easy to compute $\text{End}(E_0)$

- It is an exception

In general:

- It is hard to compute $\text{End}(E)$
- It is hard to find any element of $\text{End}(E)$ not in $\mathbb{Z}$

Trapdoor:

- Given $\varphi : E_0 \longrightarrow E$, easy to compute $\text{End}(E)$

The Endomorphism Ring Problem

Given a supersingular E, compute End(E)

- Hard, unless given $\varphi : E_0 \longrightarrow E$, where $\mathrm{End}(E_0)$ is known

The Endomorphism Ring Problem

Given a supersingular E, compute End(E)

⇕ heuristic

Given a supersingular E, find a non-trivial endomorphism

- Hard, unless given $\varphi : E_0 \longrightarrow E$, where $\text{End}(E_0)$ is known

AN IDENTIFICATION PROTOCOL

Proving knowledge of an endomorphism ring

PROVING KNOWLEDGE OF END(E)

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

PROVING KNOWLEDGE OF END(E)

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

- Generate a random secret $\varphi : E_0 \longrightarrow E_A$, make E_A public

PROVING KNOWLEDGE OF END(E)

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

- Generate a random secret $\varphi : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\text{End}(E_A)$

PROVING KNOWLEDGE OF END(E)

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

- Generate a random secret $\varphi : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?

PROVING KNOWLEDGE OF END(E)

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

- Generate a random secret $\varphi : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?

Idea first exploited in GPS Signatures in 2017

The isogeny path problem

Given two supersingular E and F, compute an isogeny $\varphi : E \longrightarrow F$

The isogeny path problem

Given two supersingular E and F, compute an isogeny $\varphi : E \longrightarrow F$

- Hard, unless both $\mathrm{End}(E)$ and $\mathrm{End}(F)$ are known

The isogeny path problem

Given two supersingular E and F, compute an isogeny $\varphi : E \longrightarrow F$

- Hard, unless both $\mathrm{End}(E)$ and $\mathrm{End}(F)$ are known
- Prove knowledge of $\mathrm{End}(E)$ by solving such instances?

PROVING KNOWLEDGE OF END(E)

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

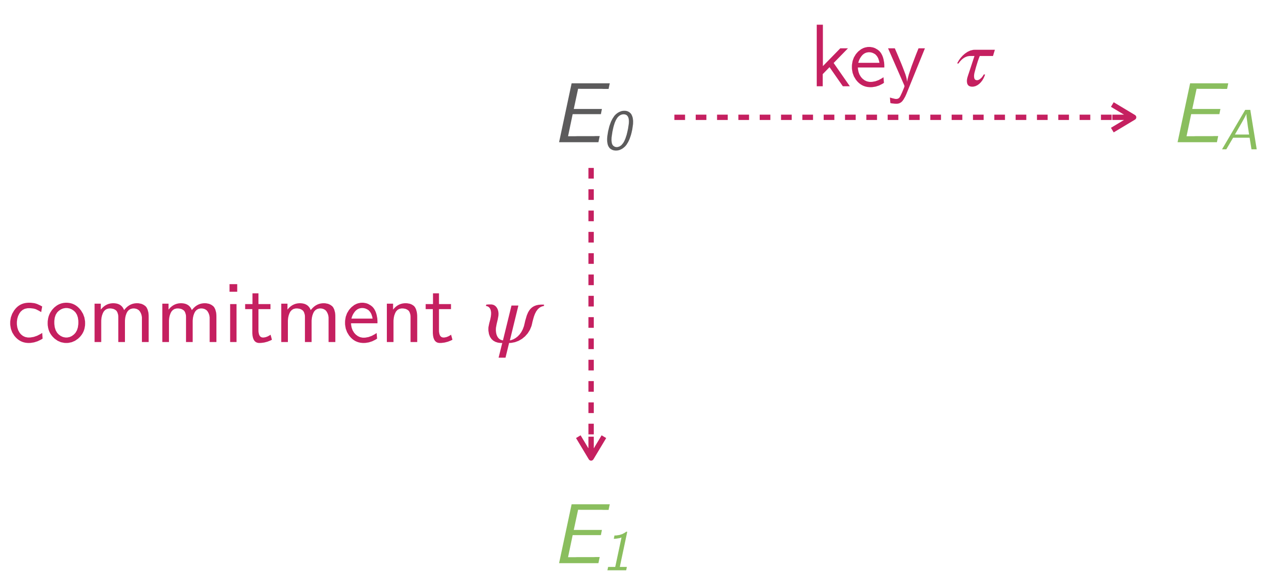
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?

$$E_0 \xrightarrow{\text{key } \tau} E_A$$

PROVING KNOWLEDGE OF END(E)

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

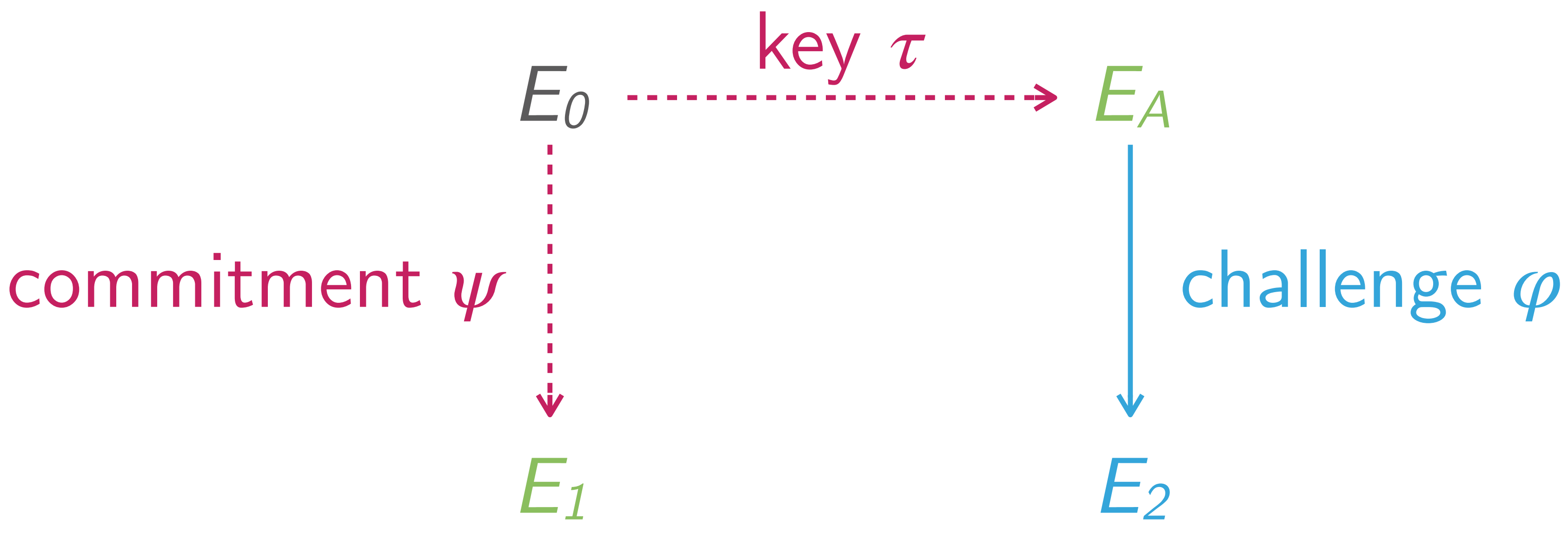
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

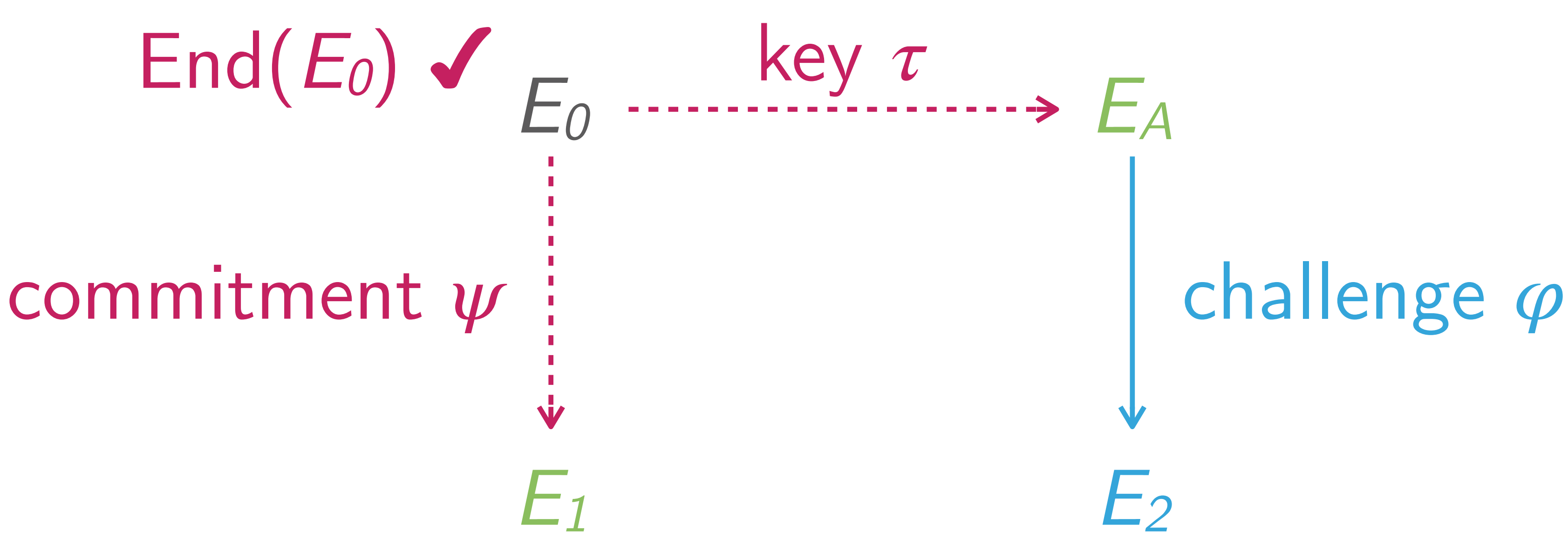
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

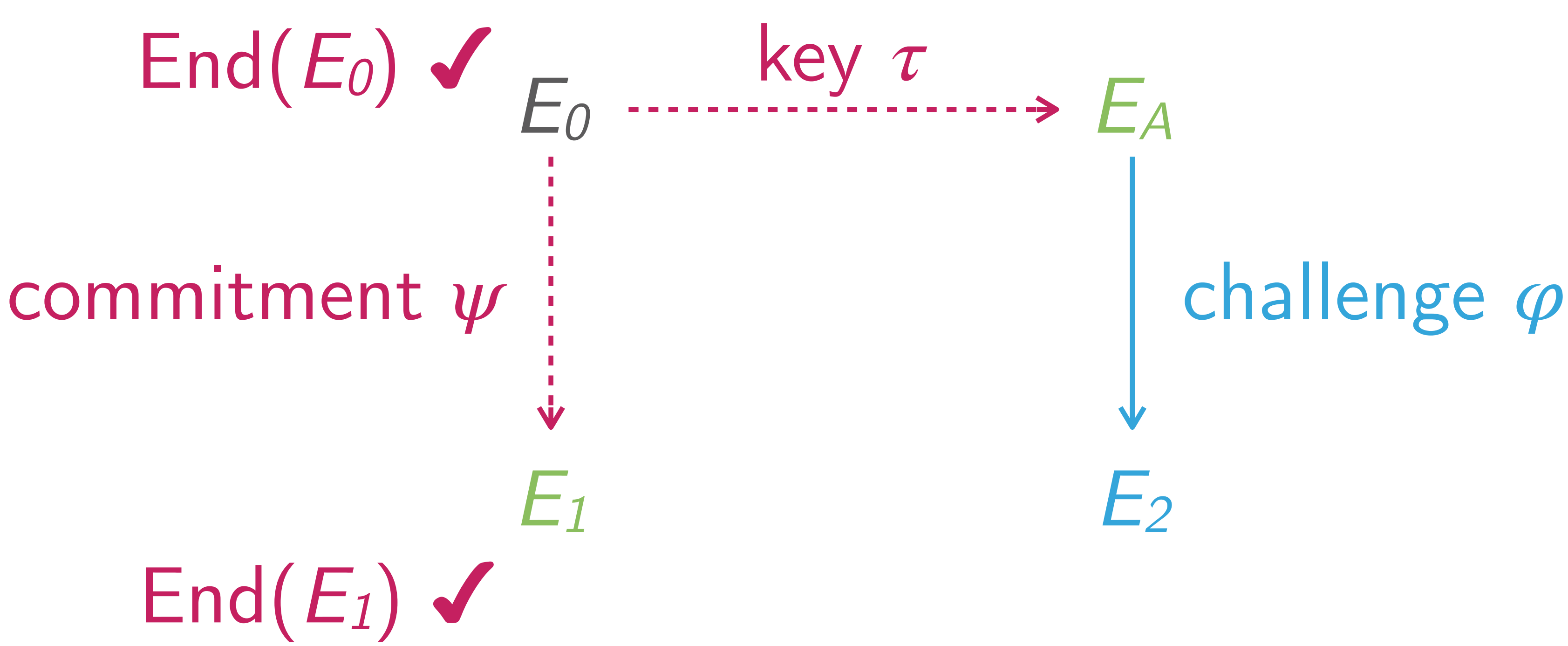
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\text{End}(E_A)$
- Can one prove knowledge of $\text{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

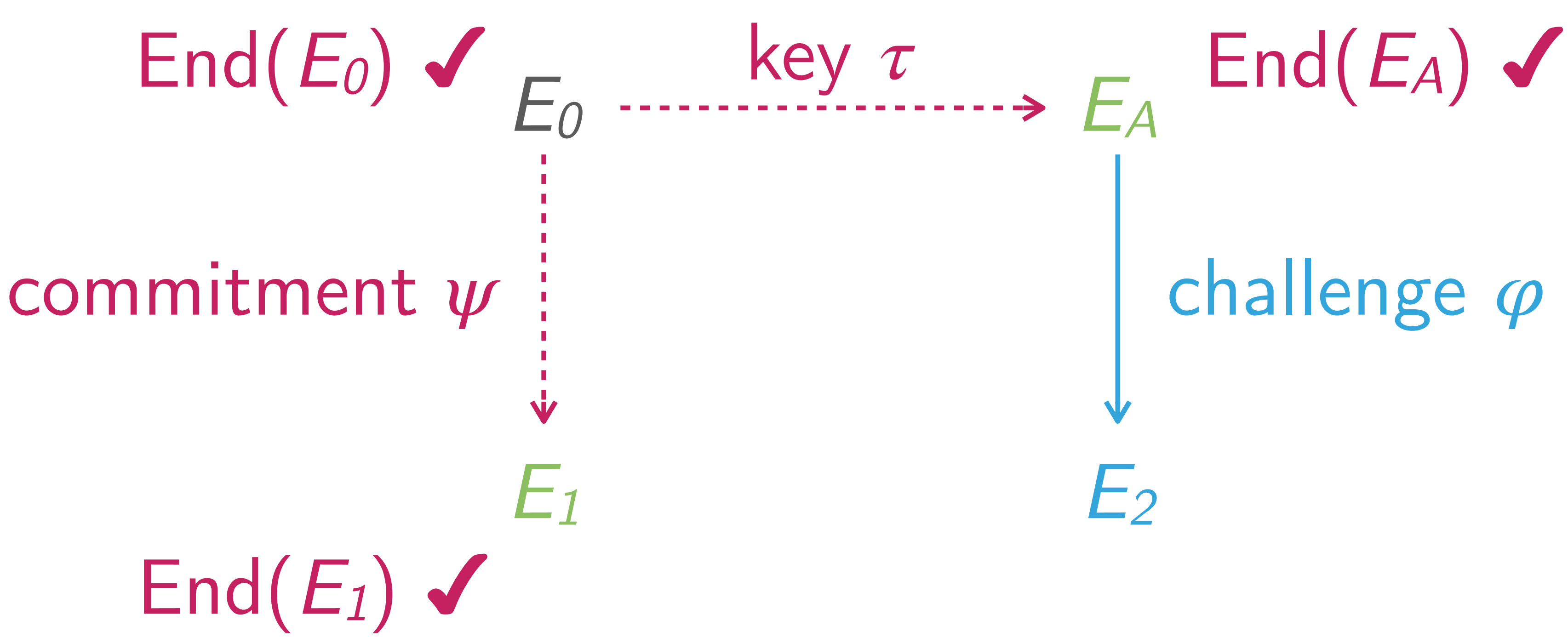
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

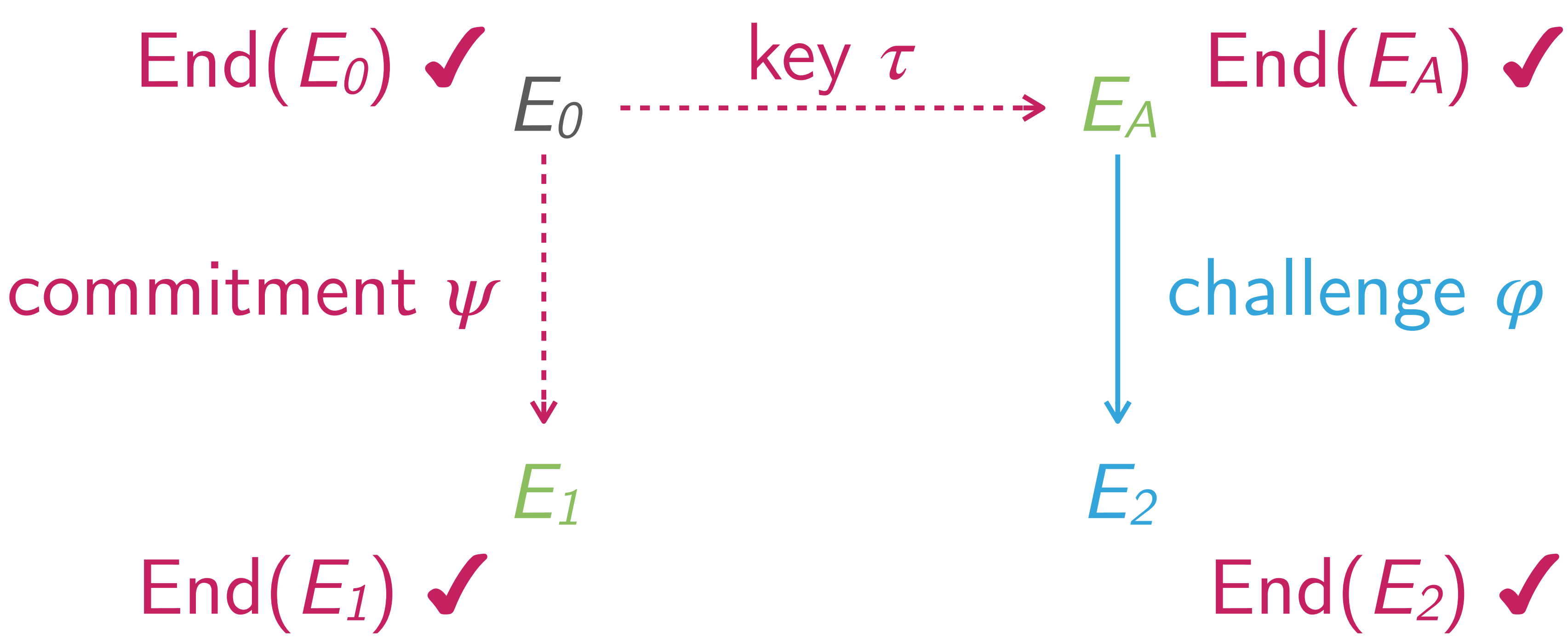
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

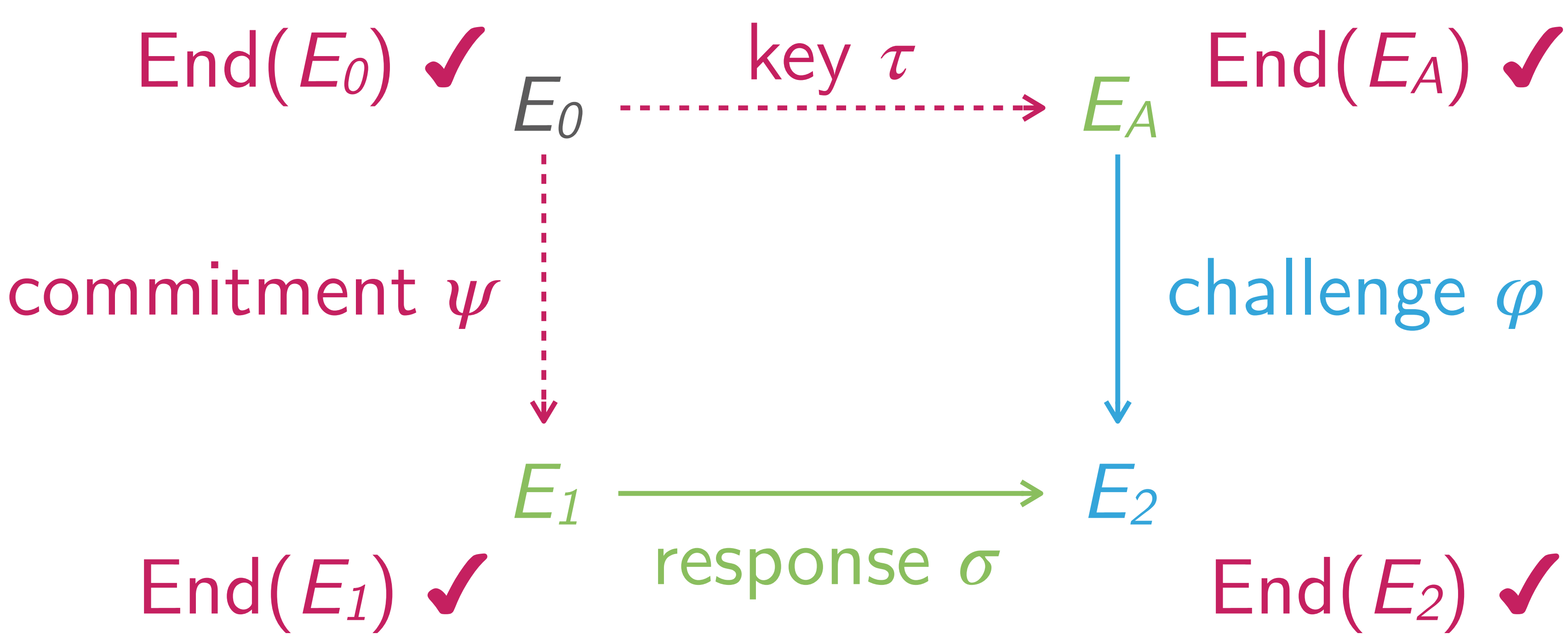
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

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

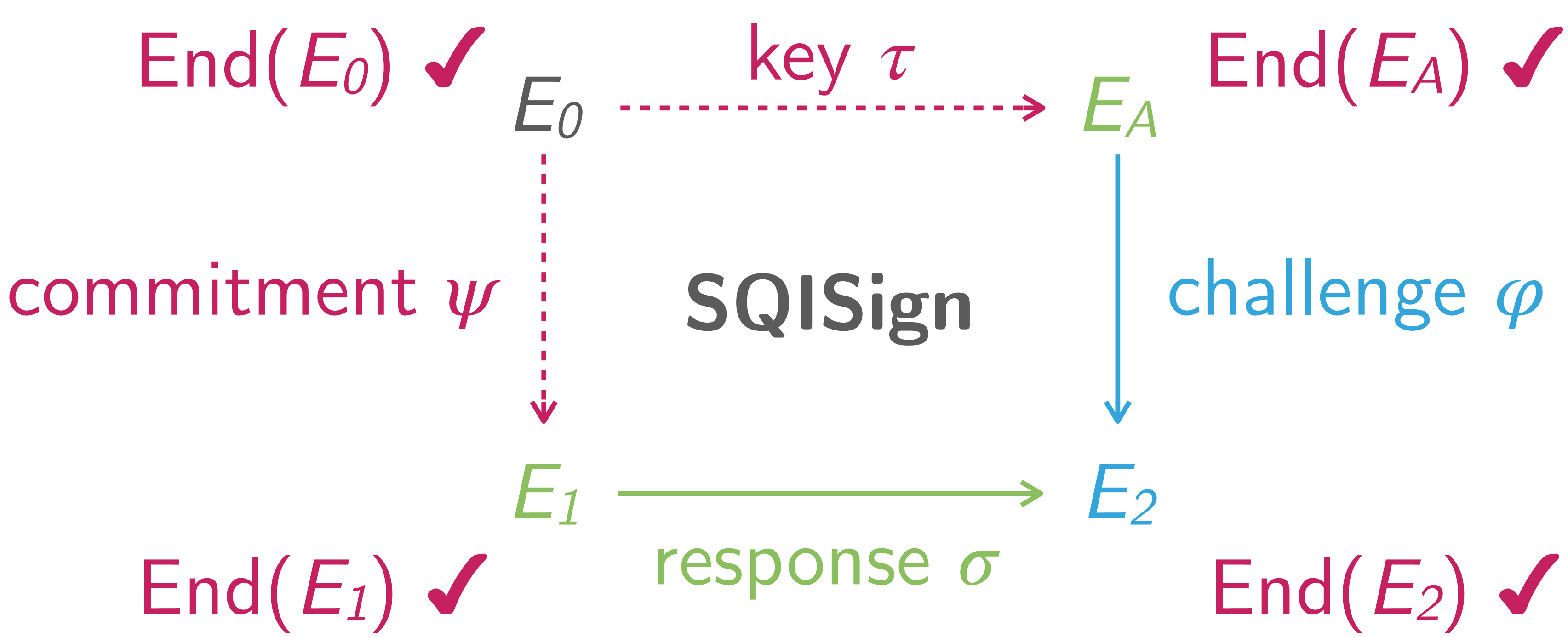
- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



PROVING KNOWLEDGE OF END(E)

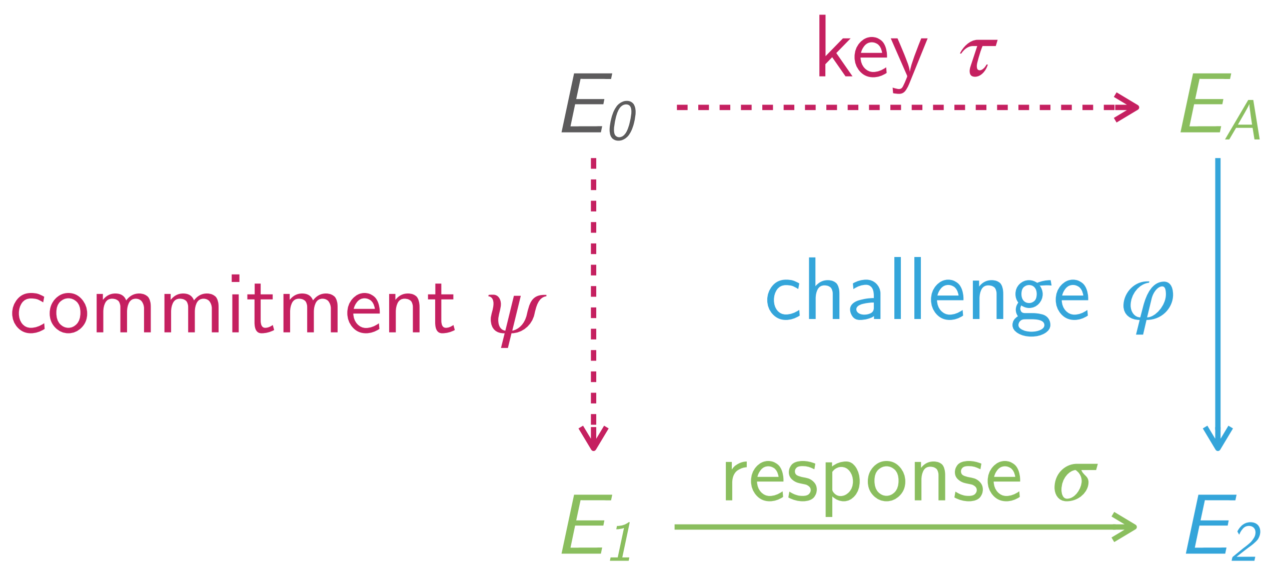
Let $E_0 : y^2 = x^3 + x$

- Generate a random secret $\tau : E_0 \longrightarrow E_A$, make E_A public
- Can compute (secretly) $\mathrm{End}(E_A)$
- Can one prove knowledge of $\mathrm{End}(E_A)$?



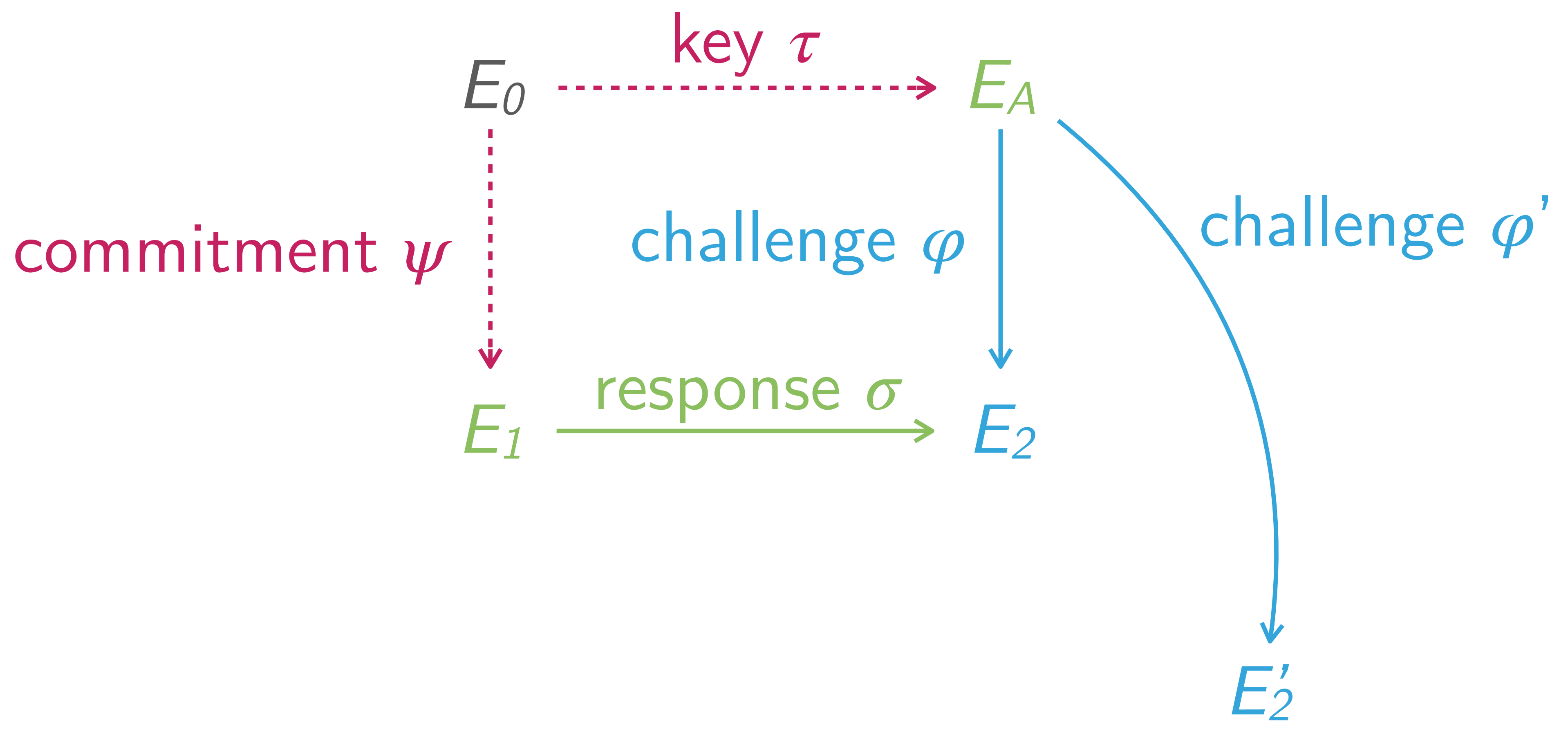
SPECIAL SOUNDNESS

Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret



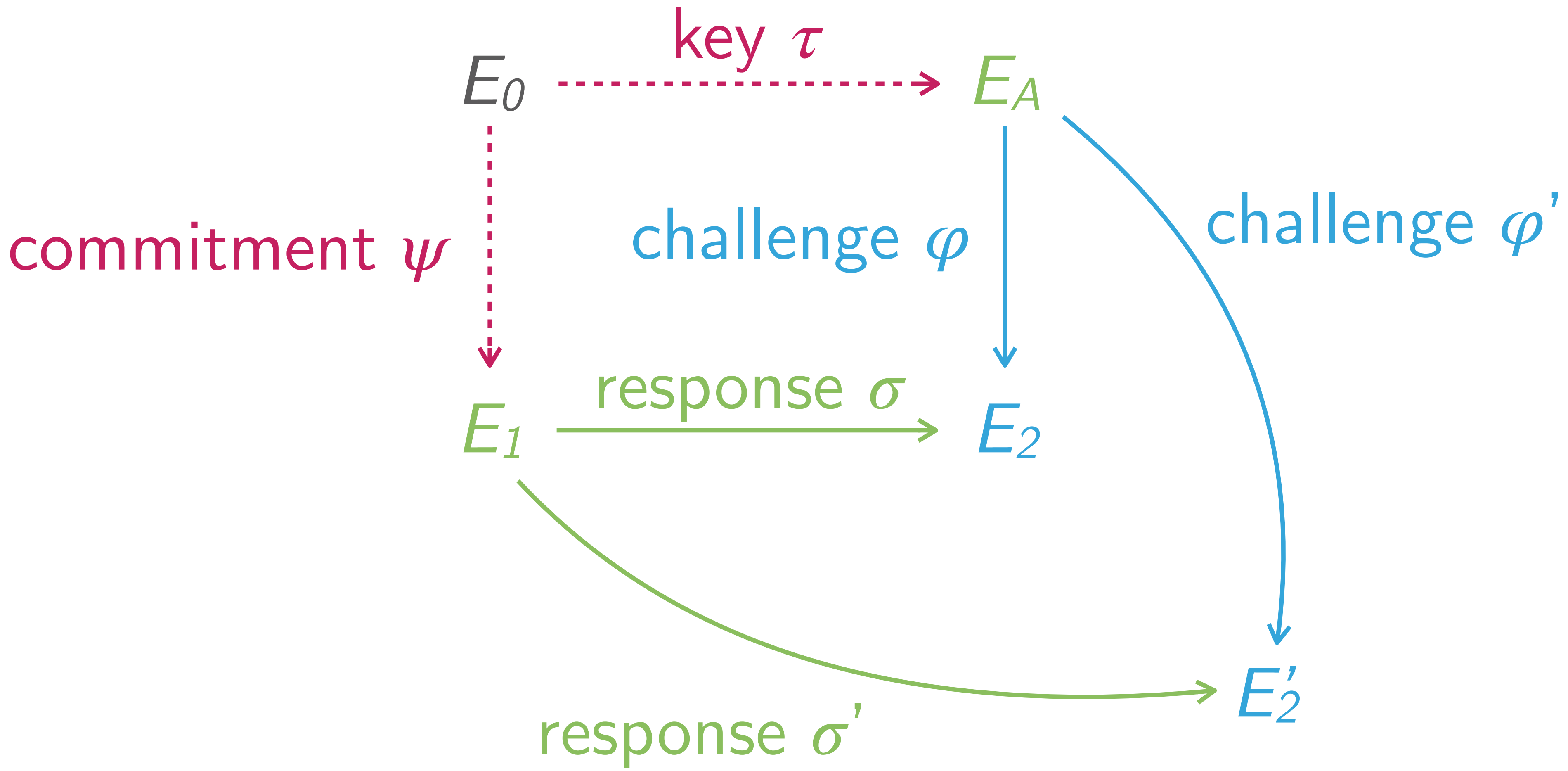
SPECIAL SOUNDNESS

Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret



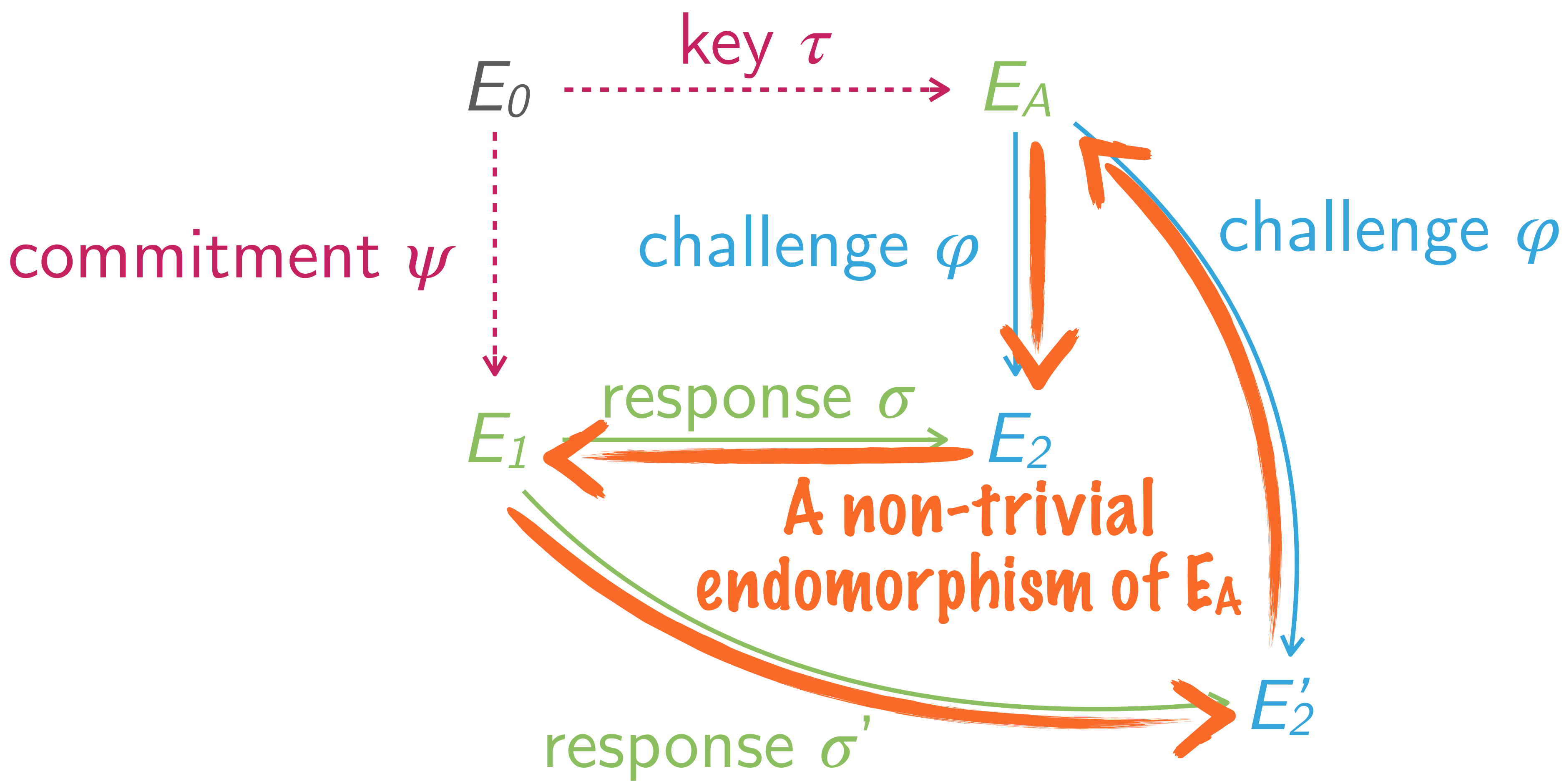
SPECIAL SOUNDNESS

Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret



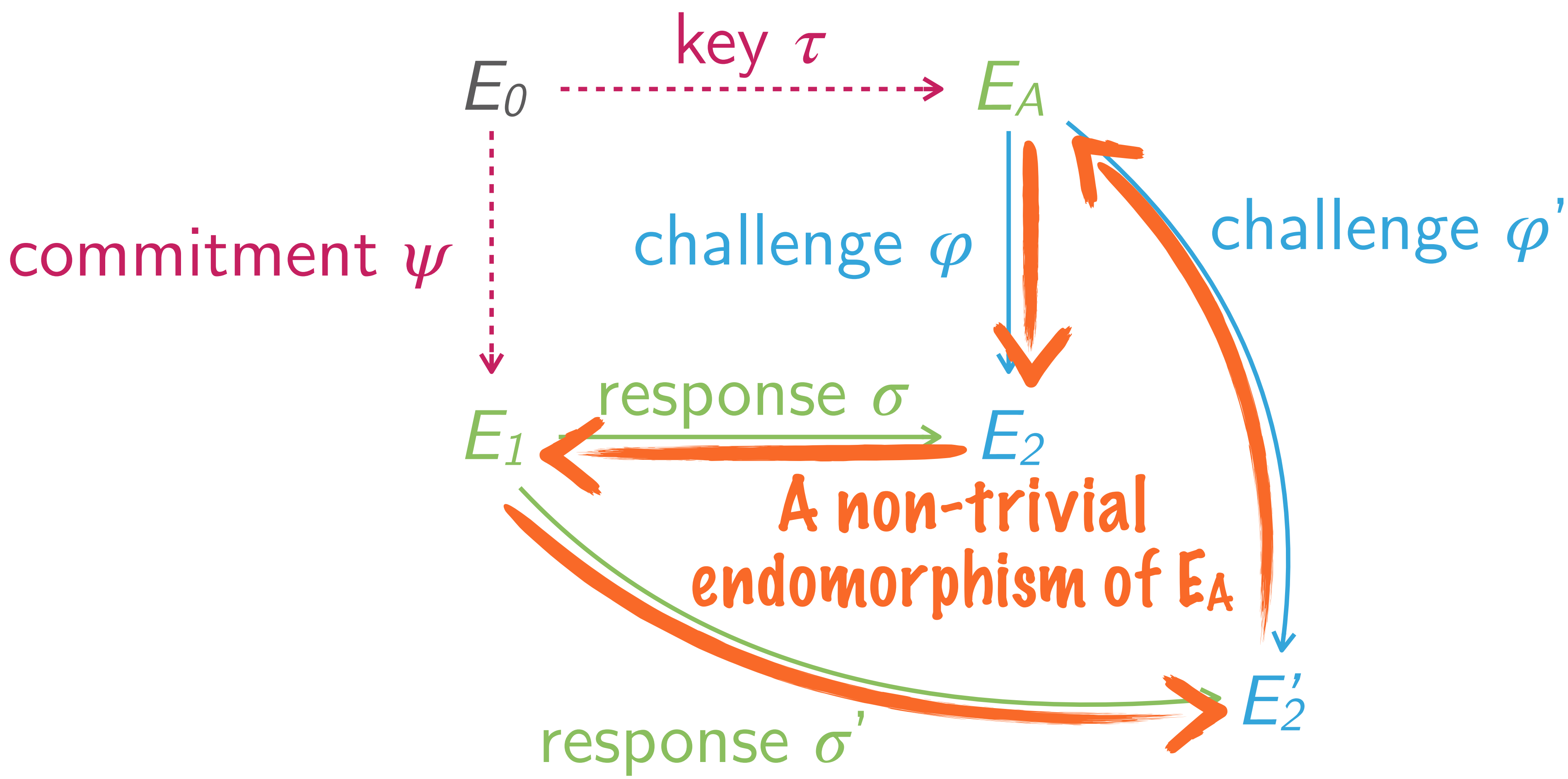
SPECIAL SOUNDNESS

Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret



SPECIAL SOUNDNESS

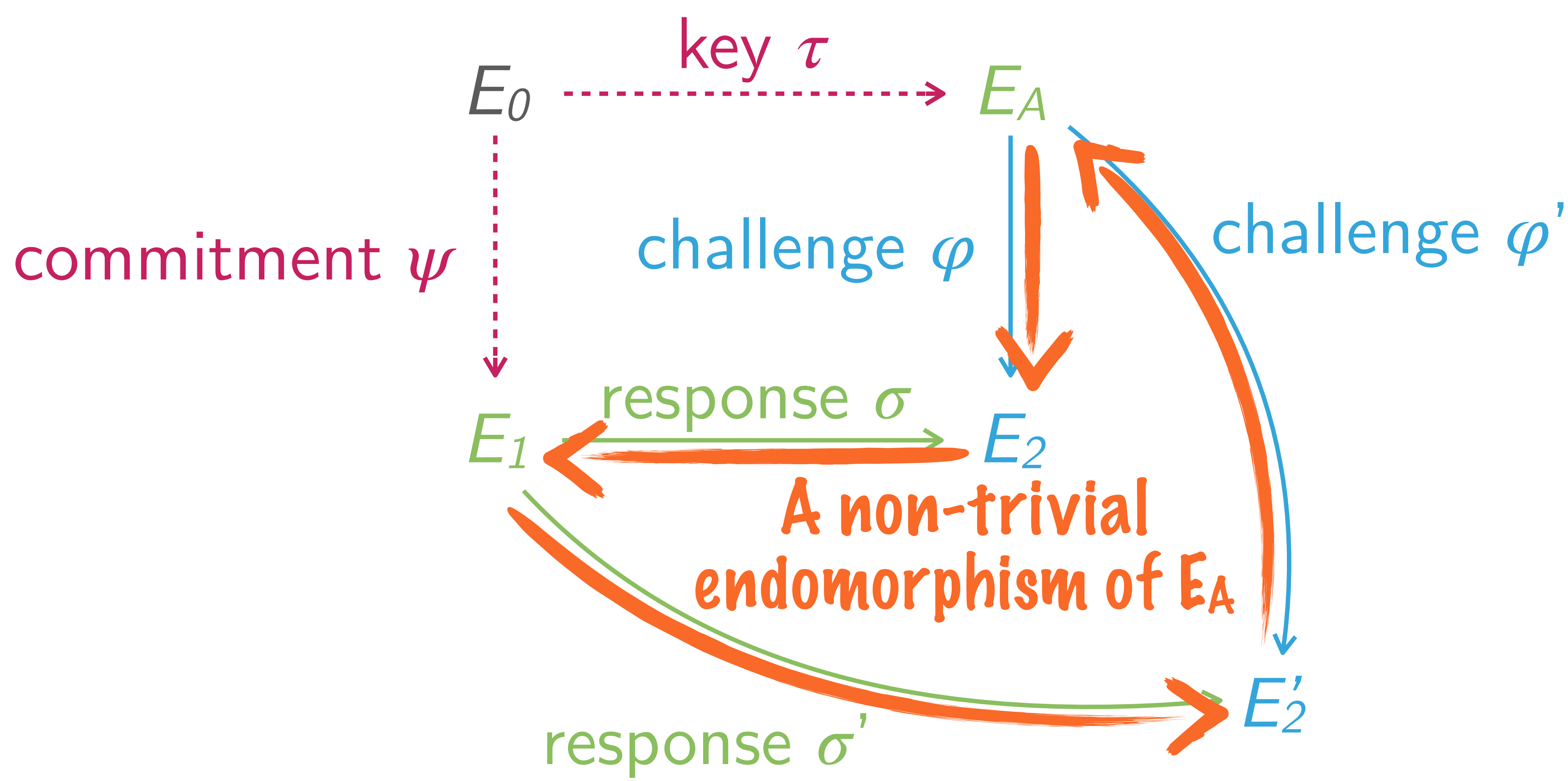
Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret



Breaking soundness $\Rightarrow$ solving "Non-trivial endomorphism"

SPECIAL SOUNDNESS

Special soundness: responding to two distinct challenges (for same commitment) allows to recover the secret

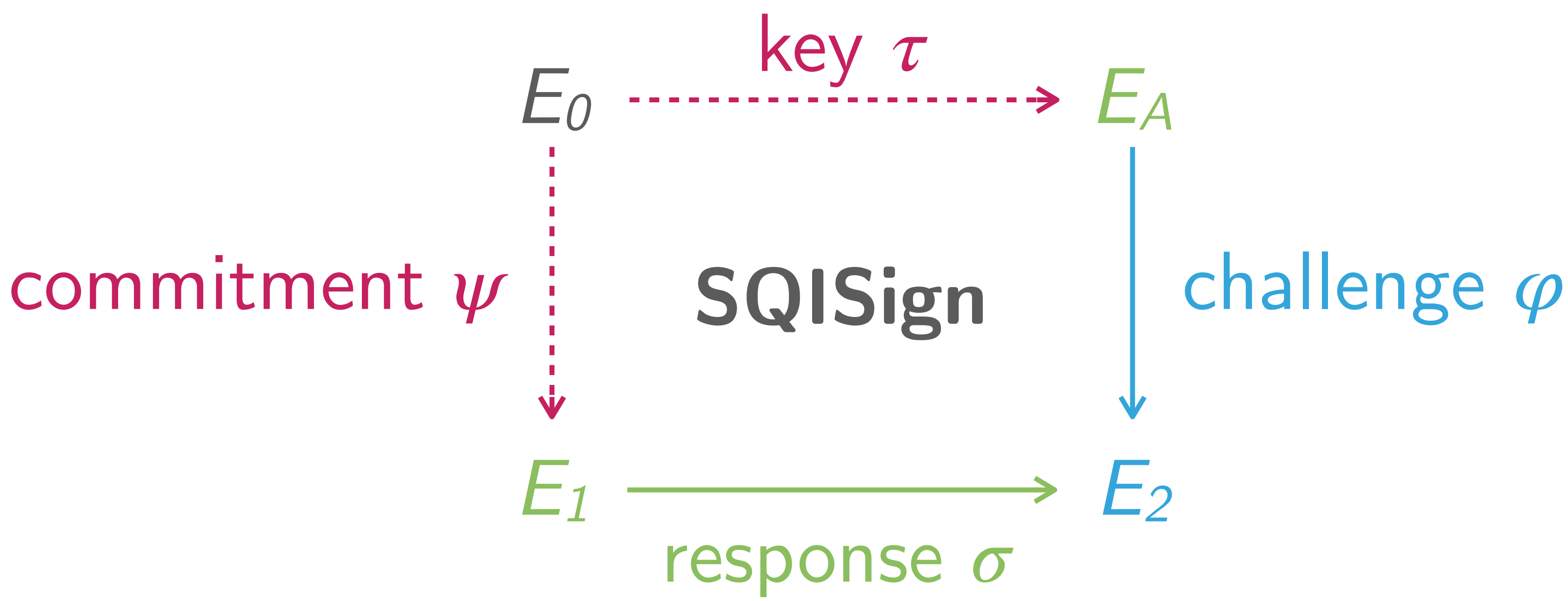


Breaking soundness $\Rightarrow$ solving "Non-trivial endomorphism" $\Rightarrow$ solving "Endo ring problem"

heuristic

ZERO-KNOWLEDGE?

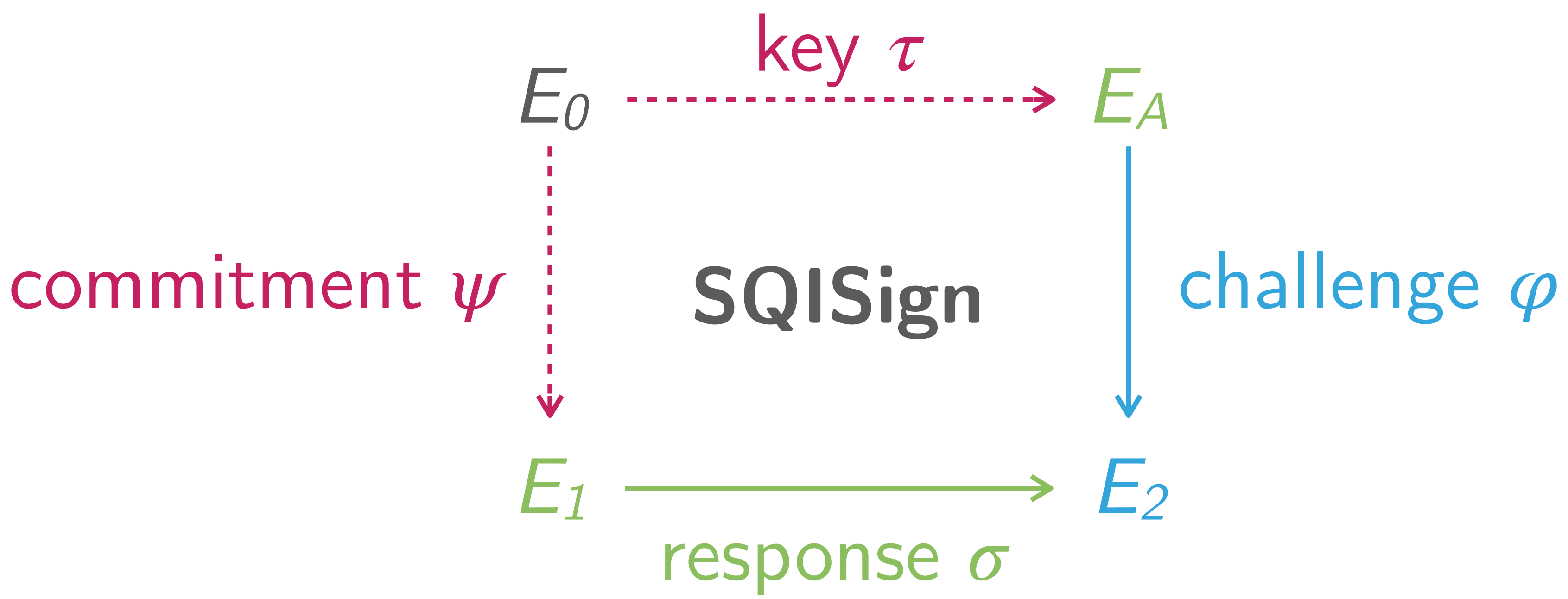
Does any information about End(E_A) leak?



ZERO-KNOWLEDGE?

Does any information about $\mathrm{End}(E_A)$ leak?

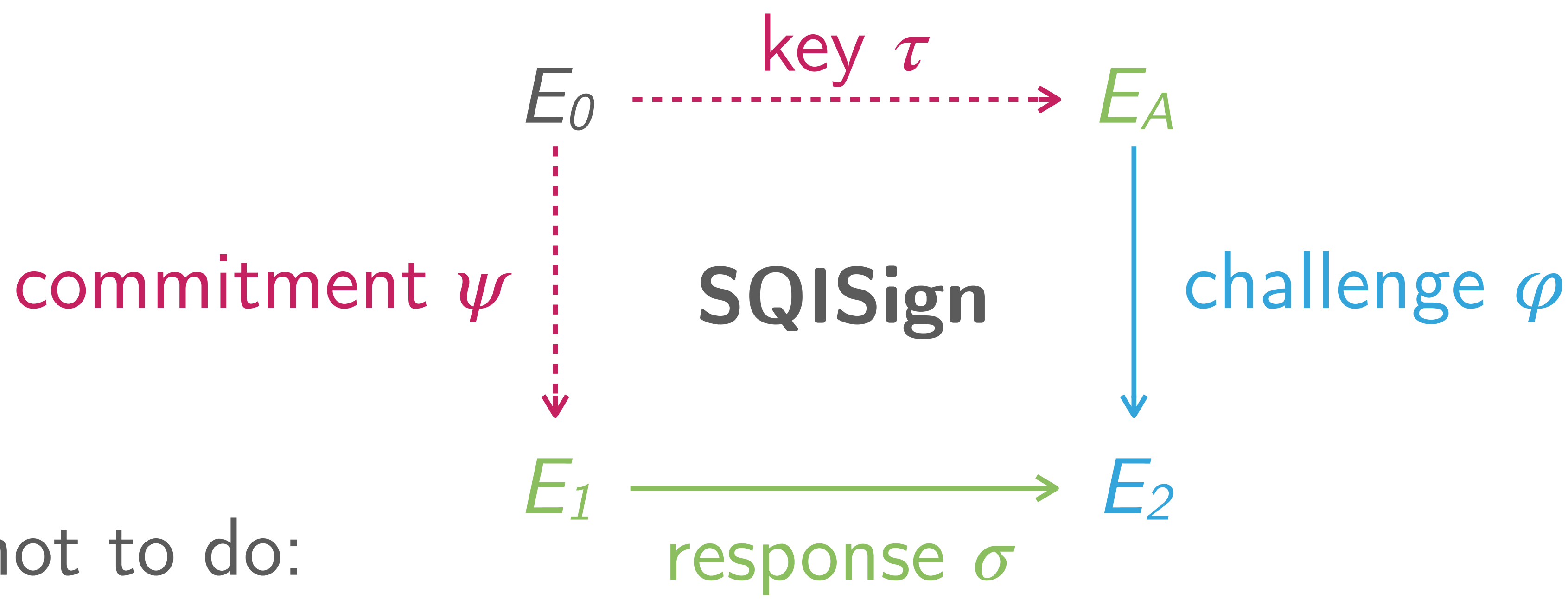
It depends on how σ is computed...



ZERO-KNOWLEDGE?

Does any information about $\mathrm{End}(E_A)$ leak?

It depends on how σ is computed...

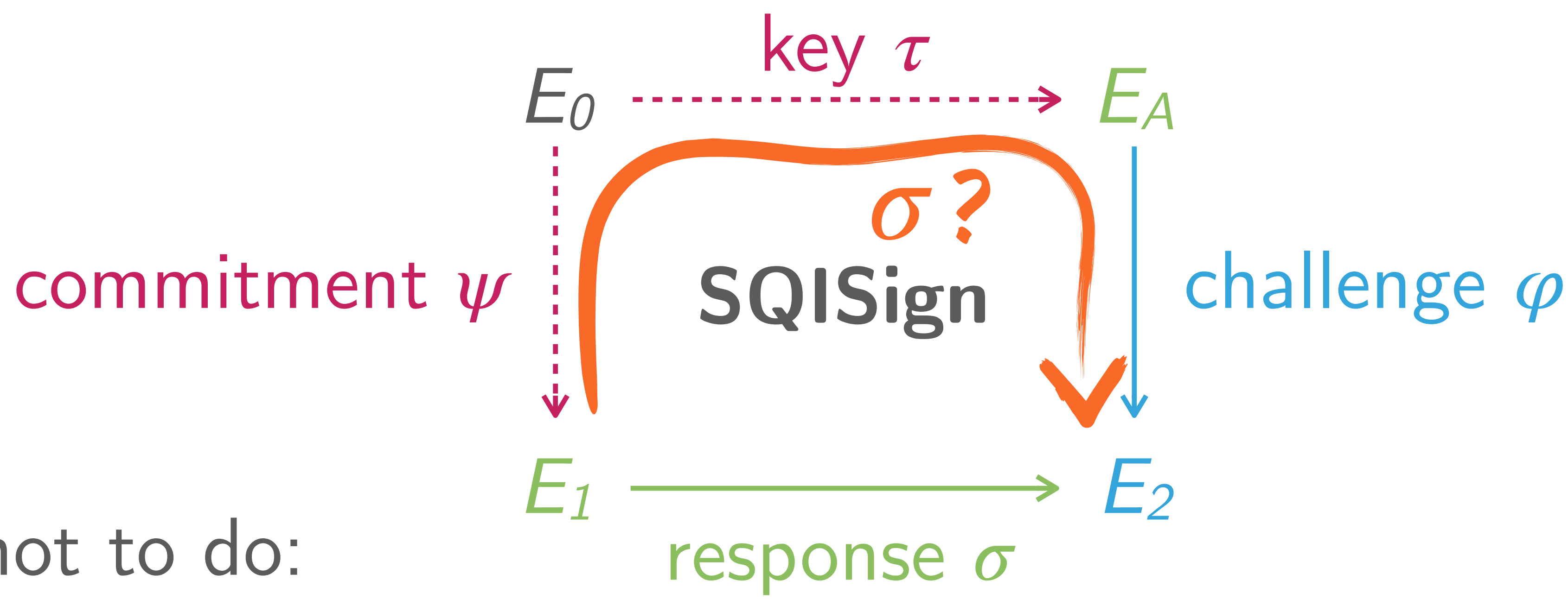


What not to do:

ZERO-KNOWLEDGE?

Does any information about $\mathrm{End}(E_A)$ leak?

It depends on how σ is computed...



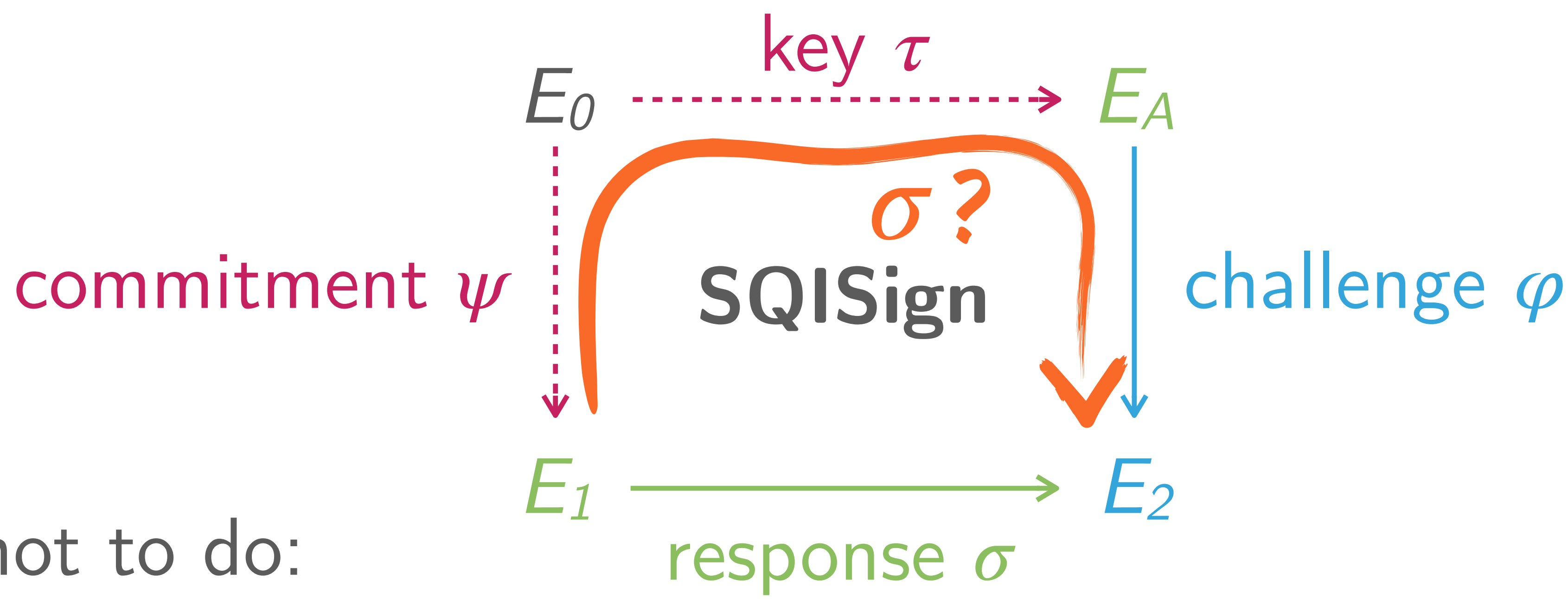
What not to do:

- Respond $\sigma = \varphi \circ \tau \circ \hat{\psi} : E_1 \longrightarrow E_2$

ZERO-KNOWLEDGE?

Does any information about End(E_A) leak?

It depends on how σ is computed...



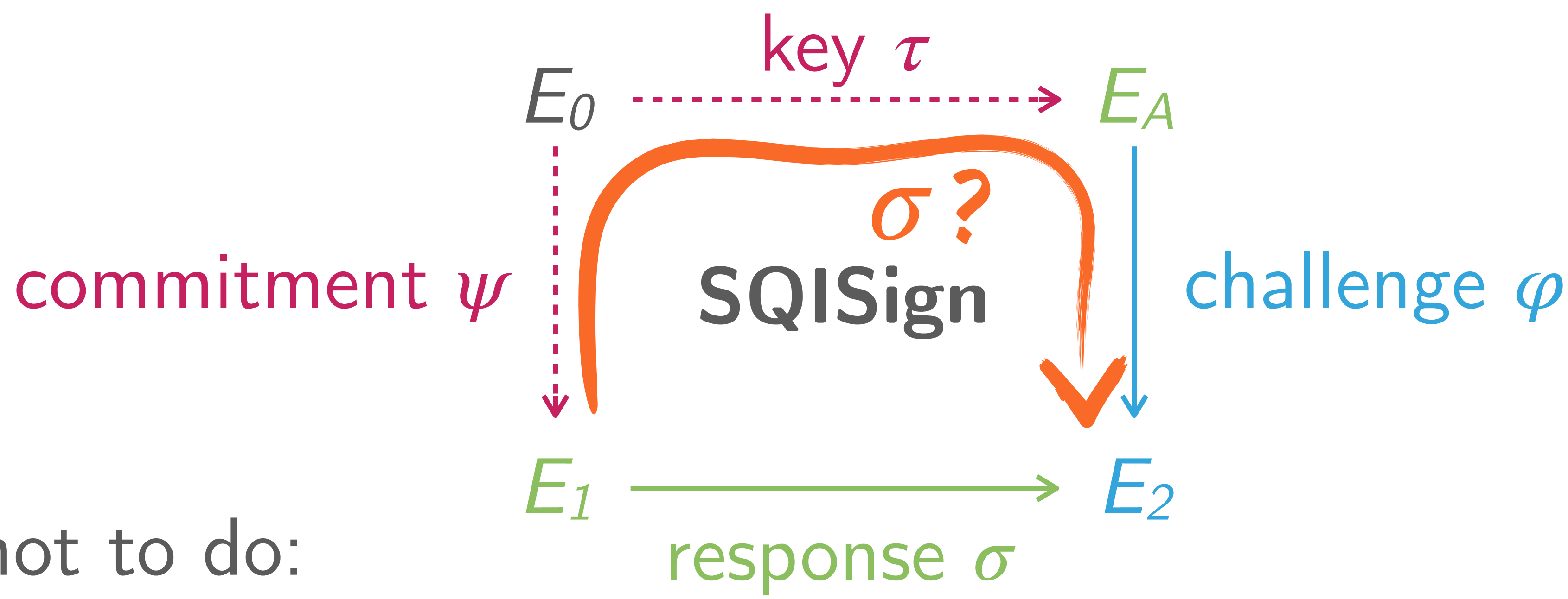
What not to do:

- Respond $\sigma = \varphi \circ \tau \circ \hat{\psi} : E_1 \longrightarrow E_2$
- It works, but leaks secret $\tau : E_0 \longrightarrow E_A$

ZERO-KNOWLEDGE?

Does any information about $\mathrm{End}(E_A)$ leak?

It depends on how σ is computed...



What not to do:

- Respond $\sigma = \varphi \circ \tau \circ \hat{\psi} : E_1 \longrightarrow E_2$
- It works, but leaks secret $\tau : E_0 \longrightarrow E_A$

Solution: new algorithm to compute response σ independent from the secret (based on new computational assumption)

ZERO-KNOWLEDGE?

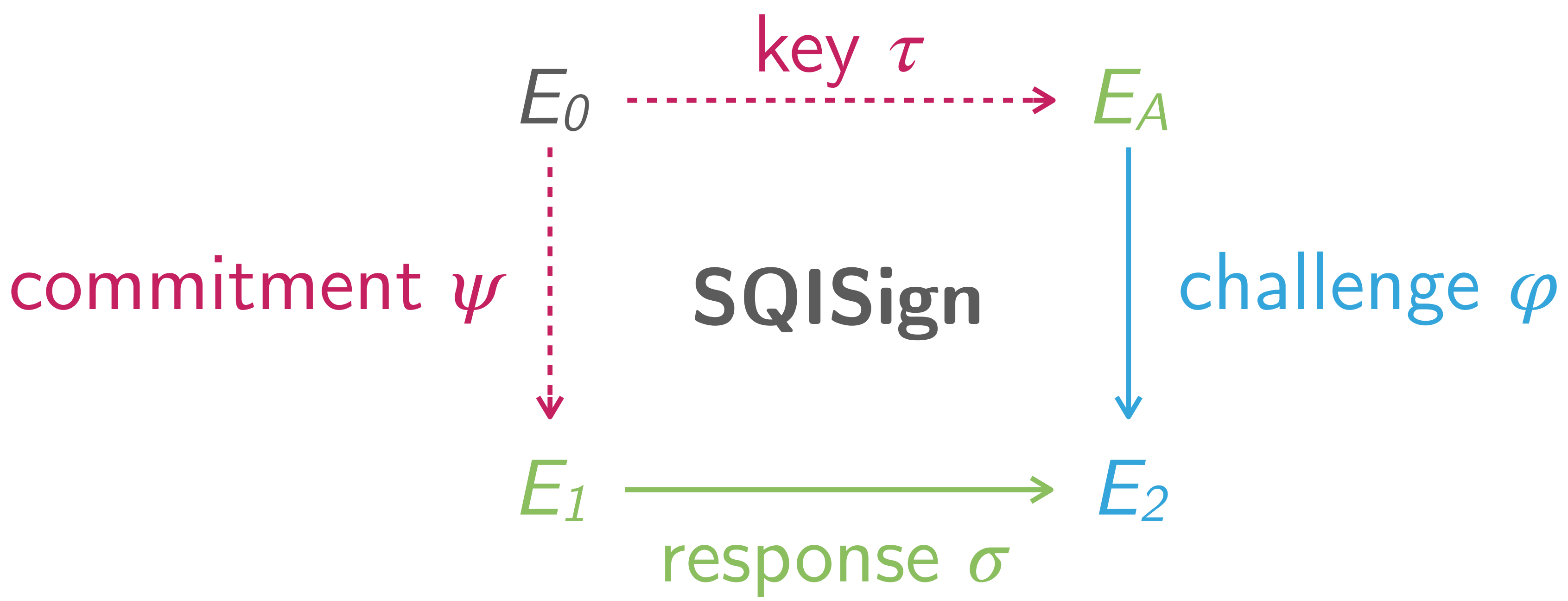
Main technical difficulty of SQISign

Solution: new algorithm to compute response σ independent from the secret (based on new computational assumption)

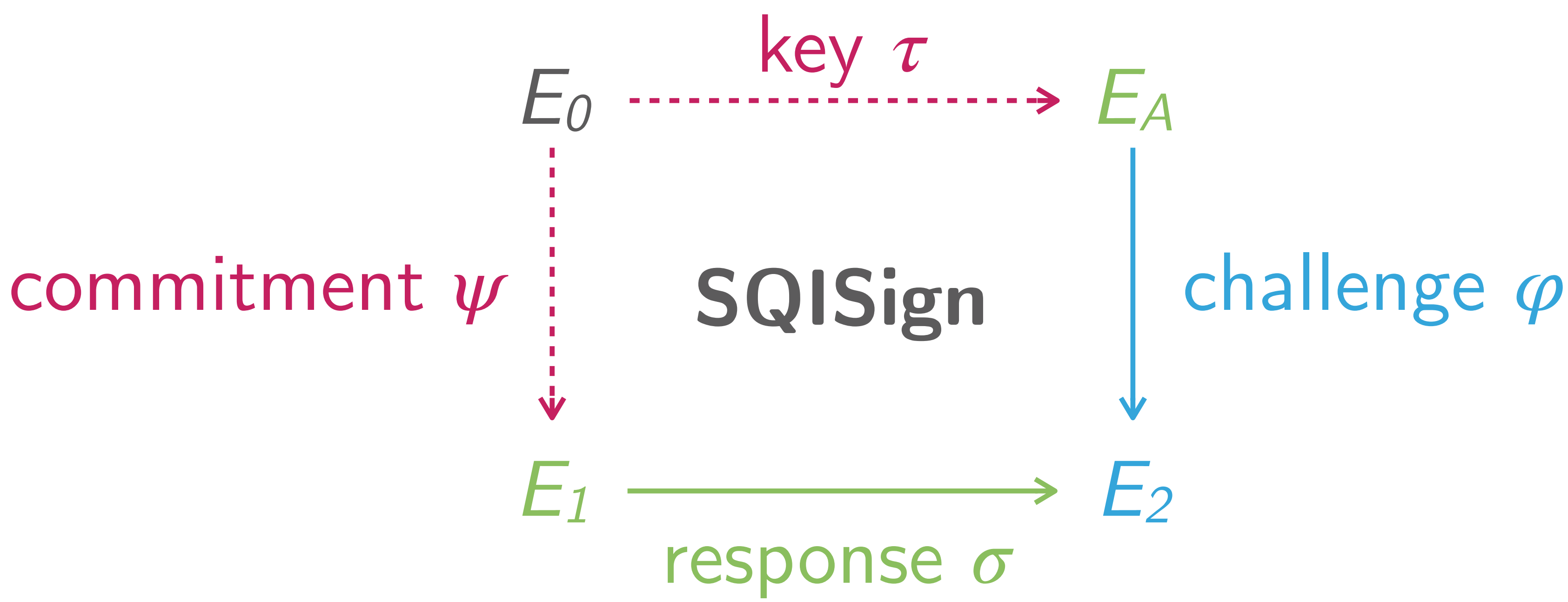
SQISIGN IN PRACTICE

How to make it fast

VERIFICATION

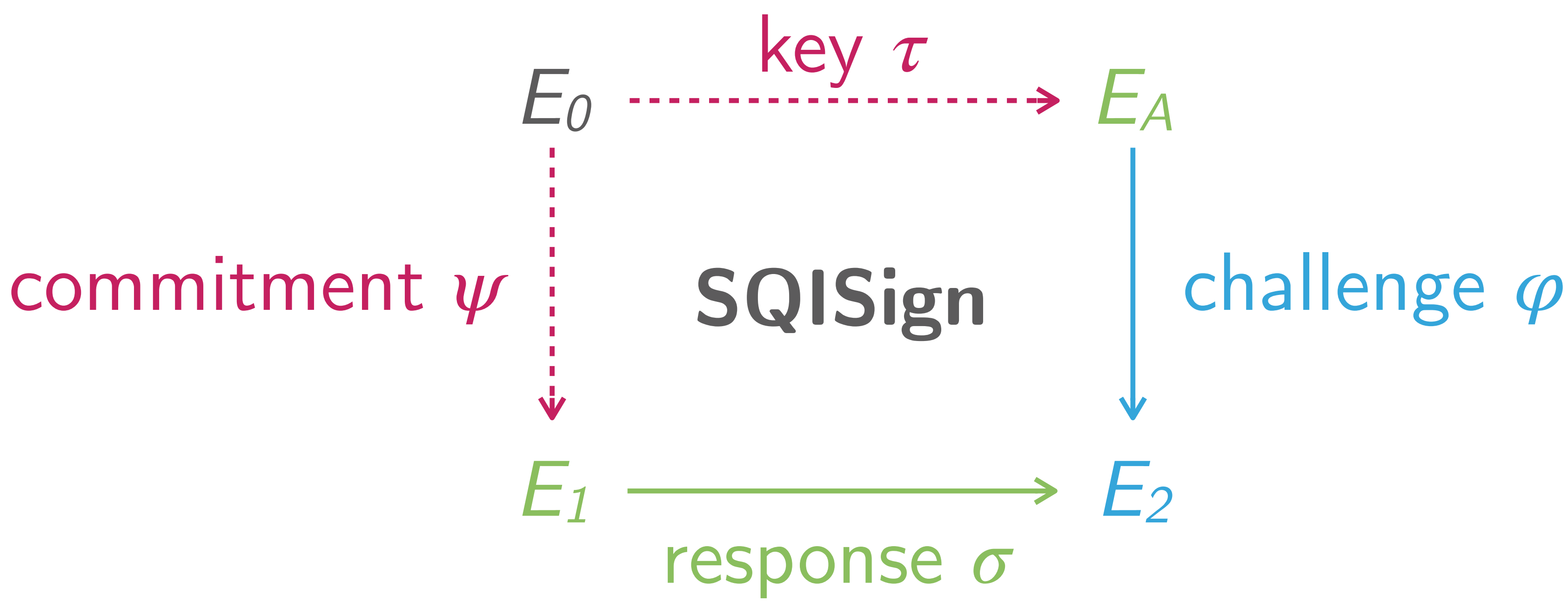


VERIFICATION



To verify, one has to

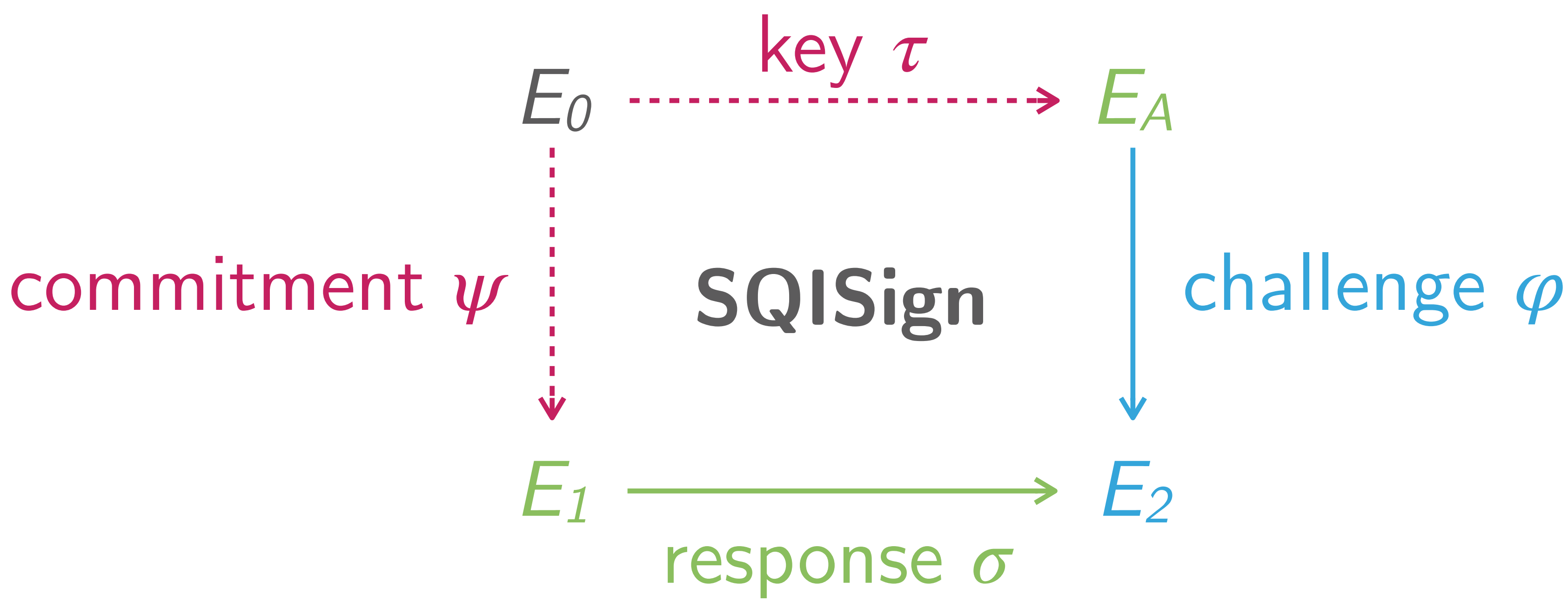
VERIFICATION



To verify, one has to

- Evaluate σ and φ

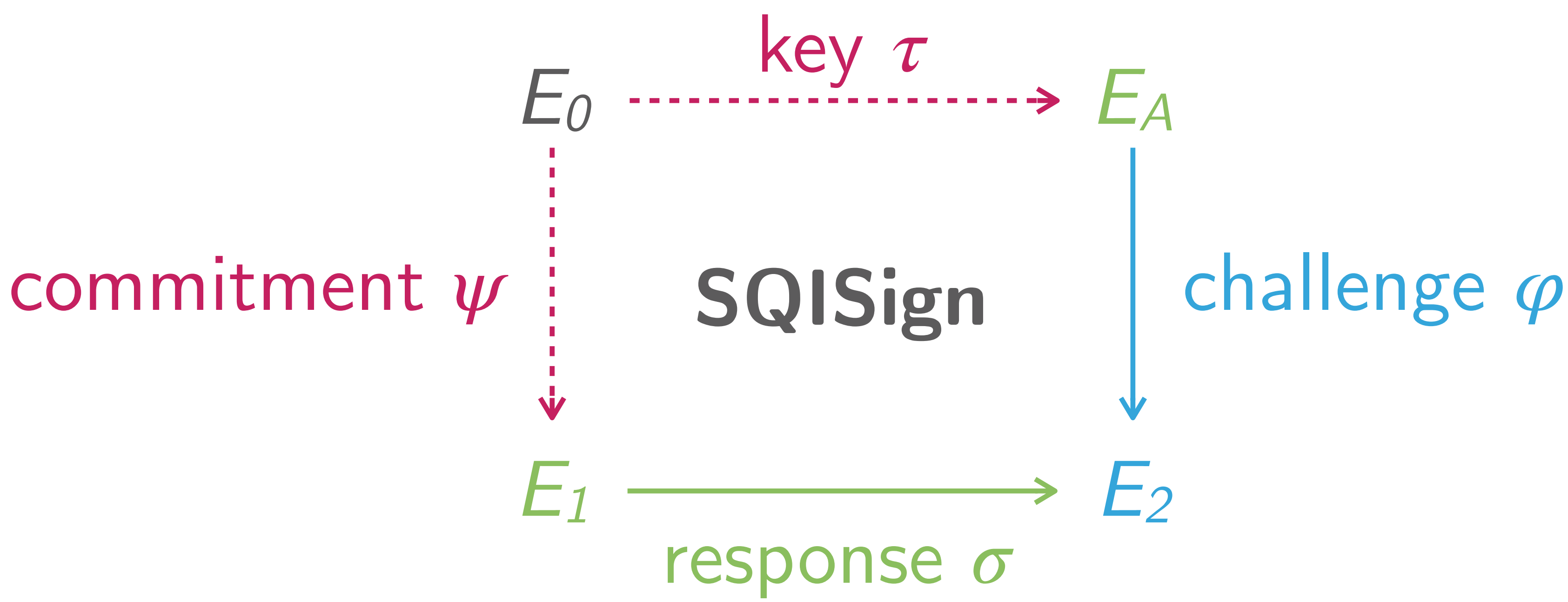
VERIFICATION



To verify, one has to

- Evaluate σ and φ
- Check that they have the correct domain and codomain

VERIFICATION



To verify, one has to

- Evaluate σ and φ
- Check that they have the correct domain and codomain

Efficient verification! (choosing $\deg(\sigma)$ and $\deg(\varphi)$ smooth)

SIGNING

To sign, one has to solve an isogeny path problem:

- Given $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$, find $\varphi : E_1 \longrightarrow E_2$

SIGNING

To sign, one has to solve an isogeny path problem:

- Given $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$, find $\varphi : E_1 \longrightarrow E_2$

Asymptotically efficient algorithm, using a variety of other algorithms translating between ideals and isogenies (Deuring correspondence)

SIGNING

To sign, one has to solve an isogeny path problem:

- Given $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$, find $\varphi : E_1 \longrightarrow E_2$

Asymptotically efficient algorithm, using a variety of other algorithms translating between ideals and isogenies (Deuring correspondence)

In practice, they can by very inefficient, using prohibitively large field extensions

SIGNING

To sign, one has to solve an isogeny path problem:

- Given $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$, find $\varphi : E_1 \longrightarrow E_2$

Asymptotically efficient algorithm, using a variety of other algorithms translating between ideals and isogenies (Deuring correspondence)

In practice, they can by very inefficient, using prohibitively large field extensions

Solution: new algorithmic tools, and a careful choice of the base prime p, so extensions are not necessary

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

- Generate a random smooth integer N

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

- Generate a random smooth integer N
- Check if $2^e N - 1$ is prime. Then let $p = 2^e N - 1$

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

- Generate a random smooth integer N
- Check if $2^e N - 1$ is prime. Then let $p = 2^e N - 1$
- $p + 1$ is smooth!

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

- Generate a random smooth integer N
- Check if $2^e N - 1$ is prime. Then let $p = 2^e N - 1$
- $p + 1$ is smooth!
- Pray that $p - 1$ has a large smooth divisor

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

How to find a good p ?

- Generate a random smooth integer N
- Check if $2^e N - 1$ is prime. Then let $p = 2^e N - 1$
- $p + 1$ is smooth!
- Pray that $p - 1$ has a large smooth divisor

Use Chinese Remainder Theorem to enlarge search space

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

For 128-bit security (NIST's level 1), $p \sim 2^{256}$

CHOICE OF THE PRIME P

Bottleneck of signing: evaluating isogenies of degree T, where

- $2^e T$ divides $p^2 - 1 = (p-1)(p+1)$
- $T \sim p^{3/2}$
- T is as smooth as possible (for efficiency!)

For 128-bit security (NIST's level 1), $p \sim 2^{256}$

We found a prime p such that $e = 33$, and

$$T = 3^{53} \cdot 43 \cdot 103^2 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \cdot 883 \cdot 1019 \cdot 1171 \cdot 1879 \cdot 2713 \cdot 4283 \cdot 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983$$

SQISIGN
COMPACT POST-QUANTUM SIGNATURE FROM QUATERNIONS AND ISOGENIES

LFANT seminar
November 2021
IMB, Bordeaux, France

Based on a joint work with
Luca De Feo, David Kohel,
Antonin Leroux and
Christophe Petit

cnrs Inria université de BORDEAUX

Benjamin Wesolowski