SQISign: Light post-quantum signatures from quaternions and isogenies

L. De Feo, D. Kohel, **A. Leroux**, C. Petit, B. Wesolowski

ANTS 2020, Rump Session

A fishy name trend

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

pronounced "sea fish".

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

pronounced "sea fish".

SeaSign (De Feo, Galbraith '19):

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

pronounced "sea fish".

SeaSign (De Feo, Galbraith '19):

no subtlety here.

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

pronounced "sea fish".

SeaSign (De Feo, Galbraith '19):

no subtlety here.

Threshold Sch. from Isog. Assump. (De Feo, Meyer '20):

A fishy name trend

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18):

pronounced "sea side".

CSI-FiSh (Beullens, Kleinjung, Vercauteren '19):

pronounced "sea fish".

SeaSign (De Feo, Galbraith '19):

no subtlety here.

Threshold Sch. from Isog. Assump. (De Feo, Meyer '20):

SQISign: reaching new heights

Short

SQISign: reaching new heights

Short **Q**uaternion

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

Signature from **one round**, **high soundness** interactive identification protocol

SQISign: reaching new heights

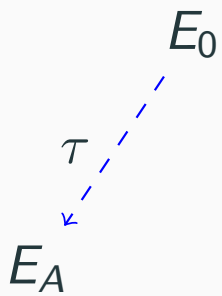
Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

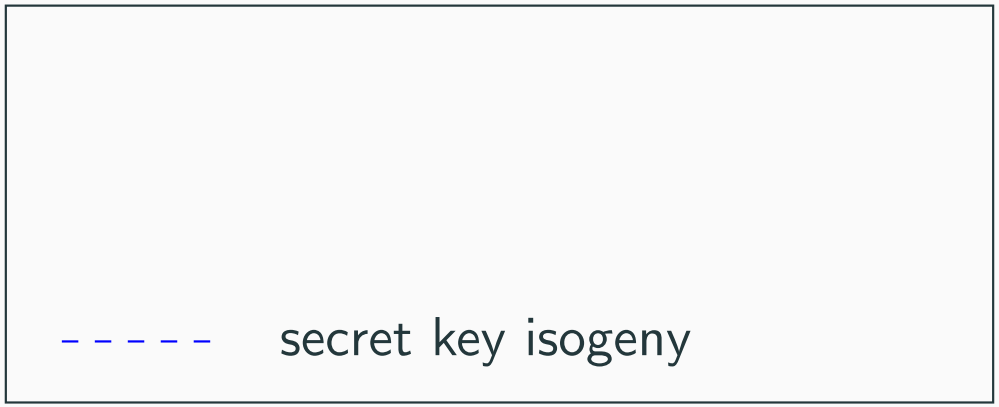
Signature from **one round**, **high soundness** interactive identification protocol based on **endomorphism ring** proof of knowledge.

SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

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

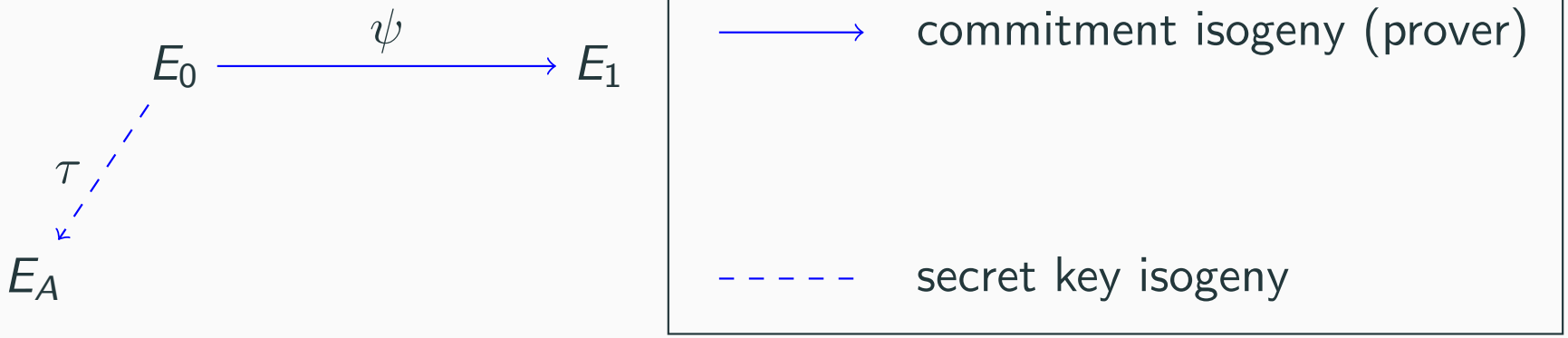




SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

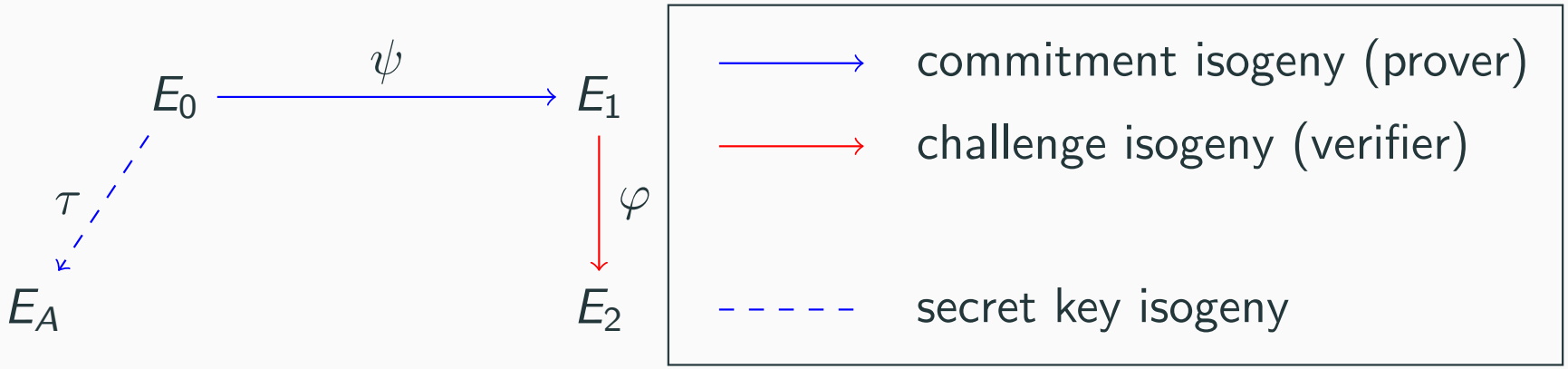
Signature from **one round**, **high soundness** interactive identification protocol based on **endomorphism ring** proof of knowledge.



SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

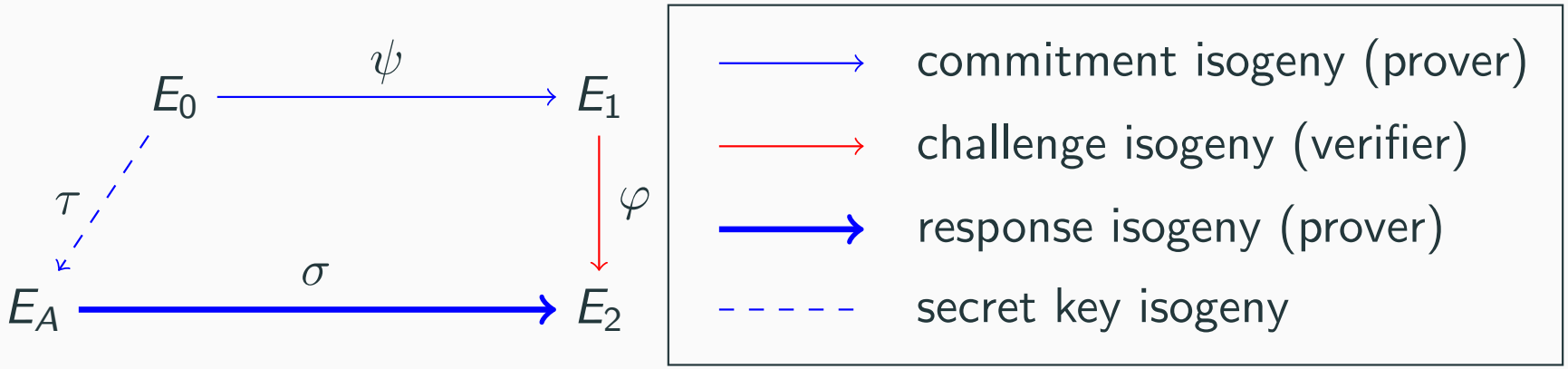
Signature from **one round**, **high soundness** interactive identification protocol based on **endomorphism ring** proof of knowledge.



SQISign: reaching new heights

Short **Q**uaternion **I**sogeny **Sign**ature (pronounced "ski sign")

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



Performances

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)
16	64	204

Table 1: Size of SQISign keys and signature for 128-bit of security and NIST level 1.

Performances

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)
16	64	204

Table 1: Size of SQISign keys and signature for 128-bit of security and NIST level 1.

PK + Sign. combined **5**$\times$ smaller than Falcon (most compact NIST Round 2 candidate).

Performances

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)
16	64	204

Table 1: Size of SQISign keys and signature for 128-bit of security and NIST level 1.

PK + Sign. combined **5**× smaller than Falcon (most compact NIST Round 2 candidate).

	Keygen	Sign	Verify
Mcycles	1,959	7,767	142
ms	575	2,279	42

Table 2: Performance of SQISign in millions of cycles and in milliseconds, on an Intel core i7 Skylake @ 3.40 GHz CPU

Thanks!