SQIsign

Krijn Reijnders
Crypto Working Group
June 21, 2024

Radboud University

SQIsign
SQIsign2

Krijn Reijnders
Crypto Working Group
June 21, 2024

Radboud University

SQIsign
SQIsign2
SQIsignHD

Krijn Reijnders
Crypto Working Group
June 21, 2024

Radboud University

SQIsign
SQIsign2
SQIsignHD
AprèsSQI

Krijn Reijnders
Crypto Working Group
June 21, 2024

Radboud University

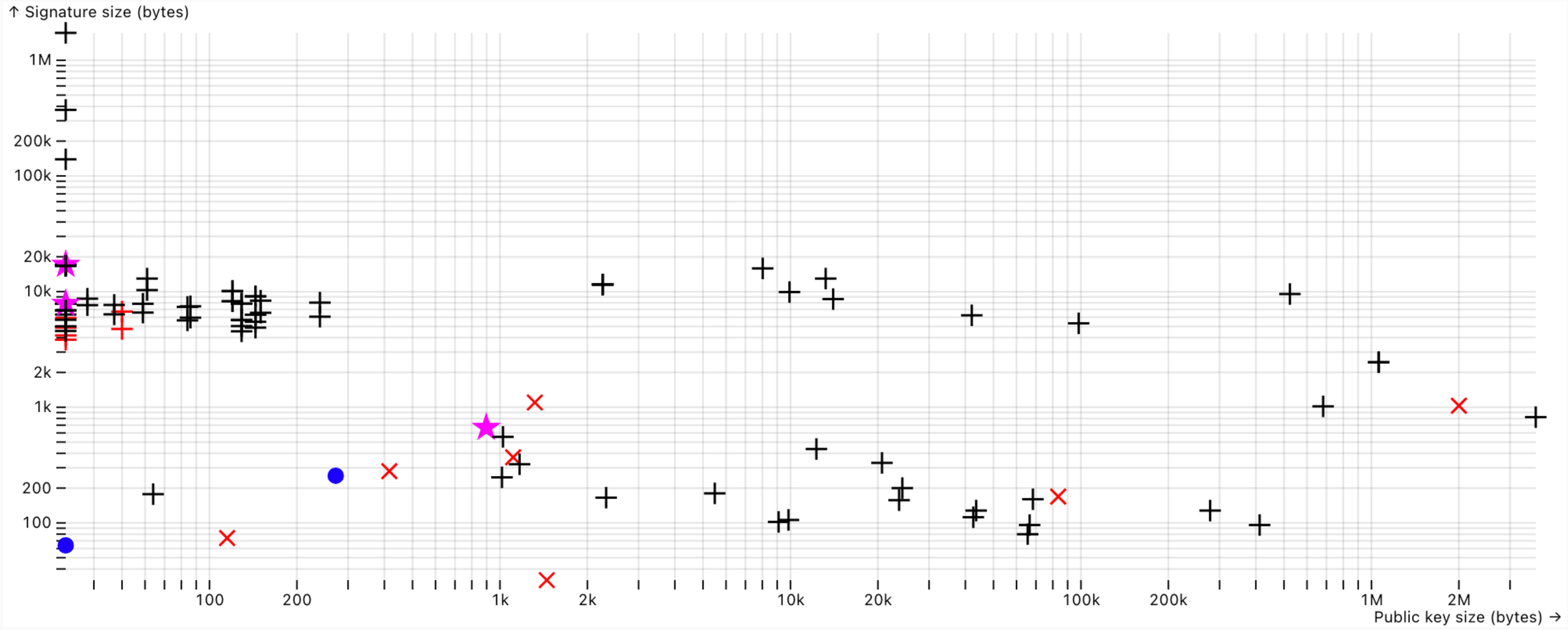
SQIsign
SQIsign2
SQIsignHD
AprèsSQI
SQIsign2D-West
SQIsign2D-East

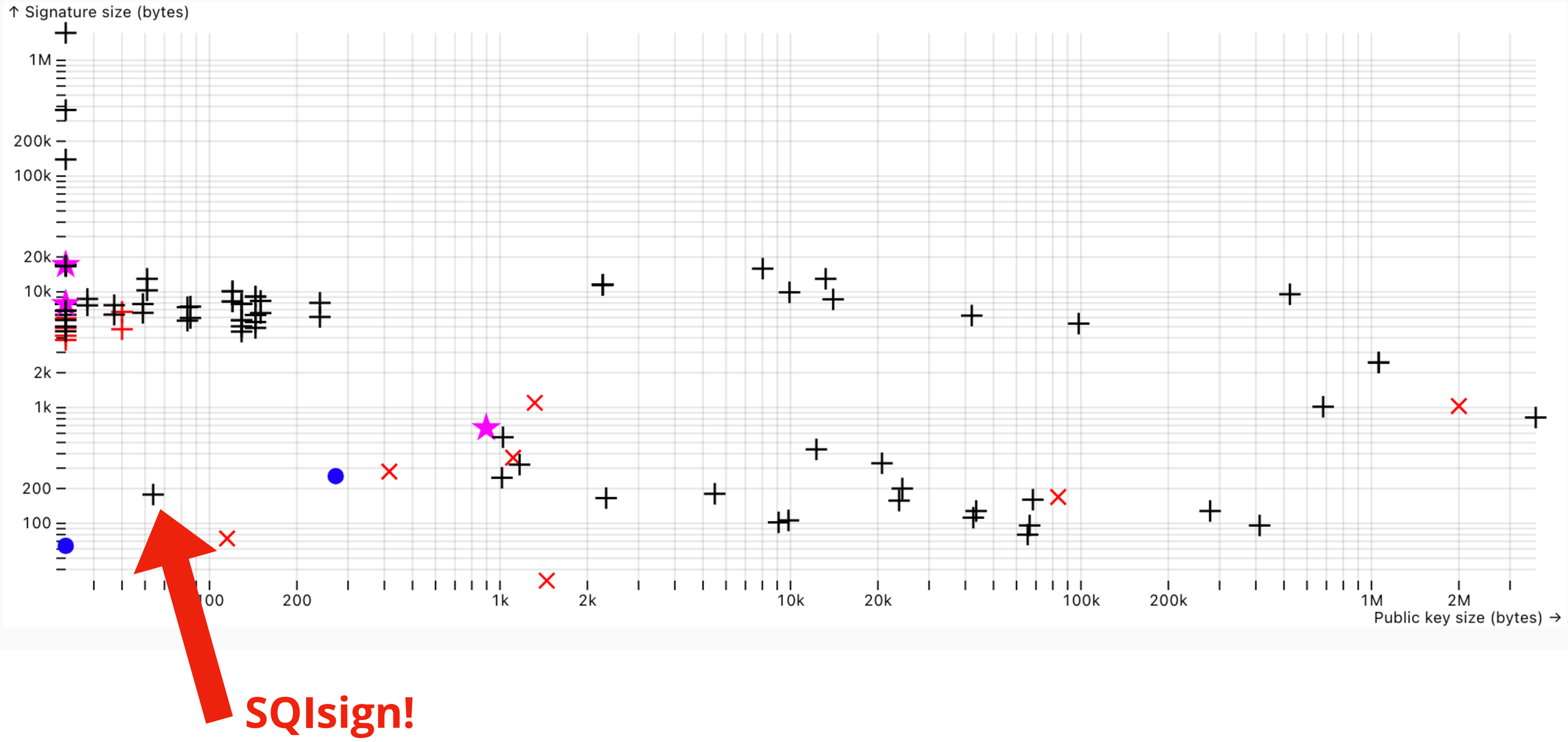
Krijn Reijnders
Crypto Working Group
June 21, 2024

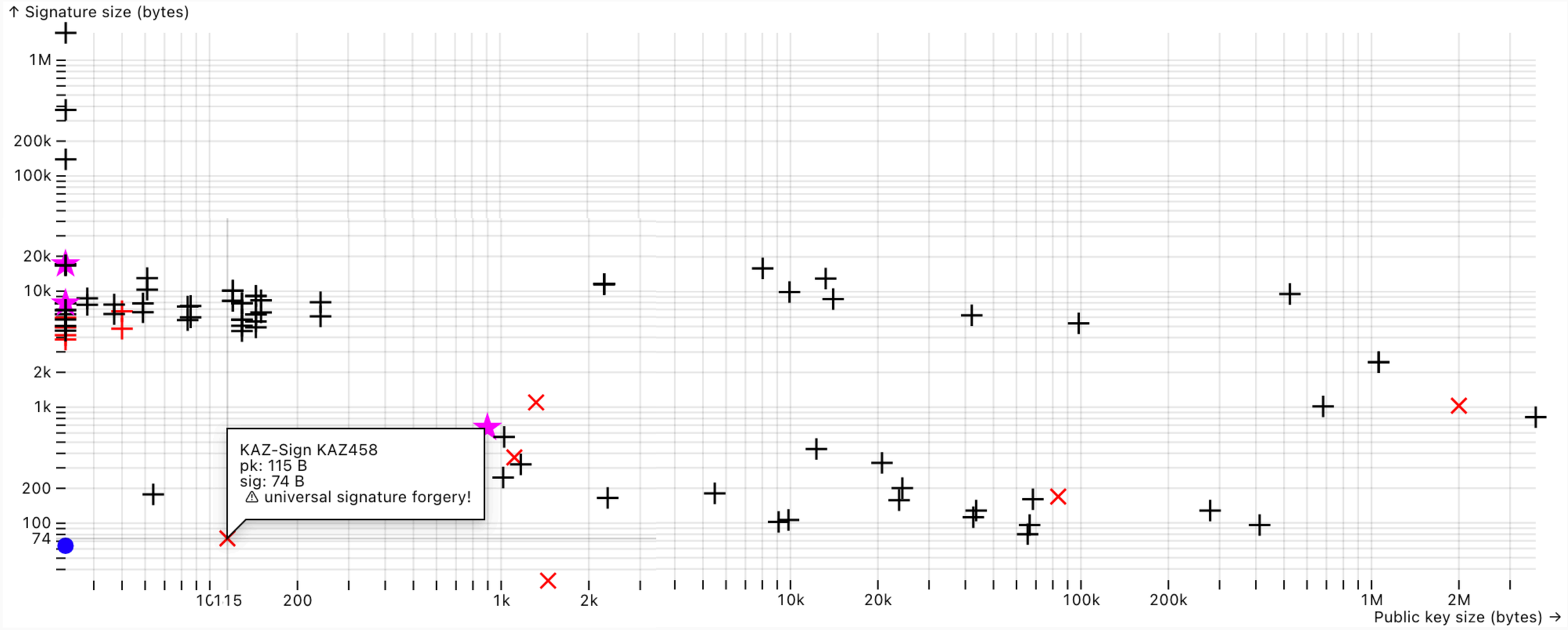
SQIsign
SQIsign2
SQIsignHD
AprèsSQI
SQIsign2D-West
SQIsign2D-East
SQIPrime

Krijn Reijnders
Crypto Working Group
June 21, 2024

(by Diego Aranha)


↑ Signature size (bytes)
1M
200k
100k
20k
10k
2k
1k
200
100
100
200
1k
2k
10k
20k
100k
200k
1M
2M
Public key size (bytes) →


↑ Signature size (bytes)
1M
200k
100k
20k
10k
2k
1k
200
100
100
200
1k
2k
10k
20k
100k
200k
1M
2M
Public key size (bytes) →
SQIsign!


↑ Signature size (bytes)
1M
200k
100k
20k
10k
2k
1k
200
100
74
KAZ-Sign KAZ458
pk: 115 B
sig: 74 B
⚠ universal signature forgery!
100
115
200
1k
2k
10k
20k
100k
200k
1M
2M
Public key size (bytes) →

100,000,000,000
1,000,000,000
10,000,000
100,000
10,000
100,000
1,000,000
10,000,000
100,000,000
1,000,000,000
Signing
Verifying
SLH-DSA (SPHINCS+)
SQIsign
FuLeeca
Ascon-Sign
SPHINCS-alpha
Wave
QR-UOV
LESS
MiRitH
SLH-DSA (SPHINCS+)
Ascon-Sign
Raccoon
MOOM
PERK
SNOVA
SDitH
RSA
CROSS
ALTEQ
AIMer
HuFu
RYDE
Squirrels
Enhanced pqsigRM
Falcon
MAYO
VOX
TUOV
UOV
HAWK
eMLE-Sig 2.0
EdDSA


SQIsign!
100,000,000,000
1,000,000,000
10,000,000
100,000
Signing
10,000
100,000
1,000,000
10,000,000
100,000,000
1,000,000,000
Verifying
SQIsign
MiRitH
SLH-DSA (SPHINCS+)
Ascon-Sign
FuLeeca
SPHINCS-alpha
Wave
QR-UOV
LESS
RSA
Raccoon
SNOVA
SDitH
PERK
MQOM
Squirrels
Enhanced pqsigRM
Falcon
MAYO
VOX
TUOV
UOV
HAWK
eMLE-Sig 2.0
EdDSA
CROSS
ALTEQ
AIMer

The Landscape of SQIsign

an overview in five acts

Krijn Reijnders
Crypto Working Group
June 21, 2024

Radboud University

PART 0: Maths

PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk “down to earth”, I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

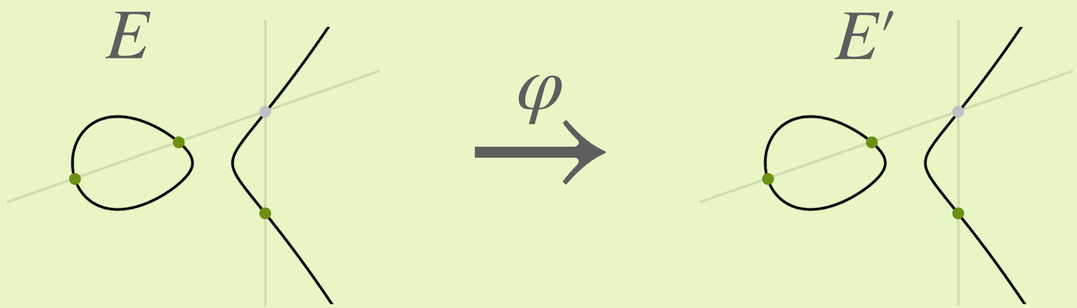
PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



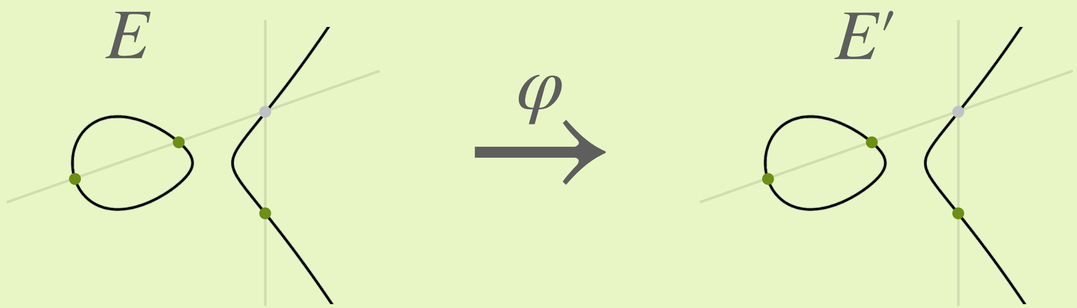
PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



Isogeny

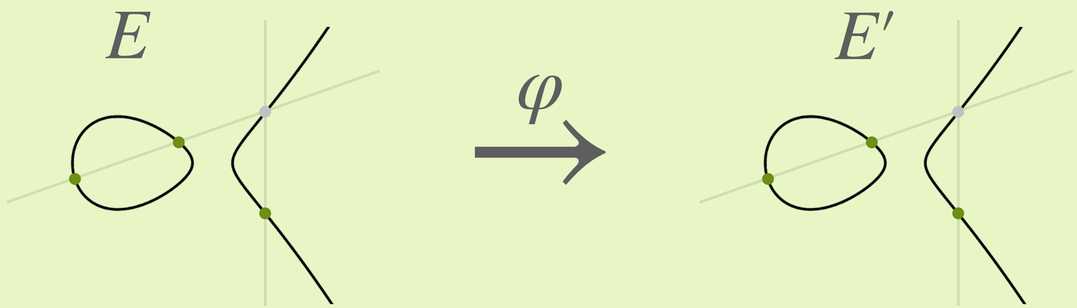
- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y))$
- size of $\ker \varphi$ is same as degree of φ!

PART 1
SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



Isogeny

- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $\left(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y) \right)$
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\varphi} E' : y^2 = x^3 + 5$$

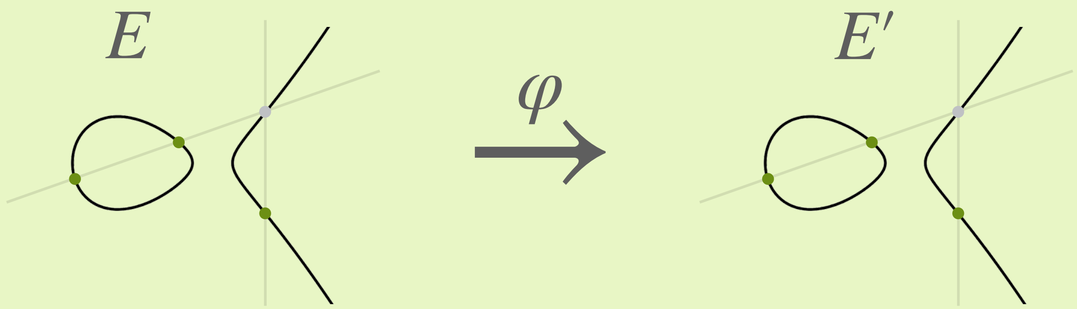
$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y(x^3 - 4x^2 + 2)}{(x-5)^3} \right) \quad \text{over } \mathbb{F}_{11}$$

PART 1
SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



Isogeny

- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y))$
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\varphi} E' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y(x^3 - 4x^2 + 2)}{(x-5)^3} \right) \quad \text{over } \mathbb{F}_{11}$$

Can check

- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}'$ and $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- kernel: $\varphi(P) = \mathcal{O}'$ when $P = \mathcal{O}$ or $x_P = 5$, so $P = (5,3)$ and $P = (5, -3)$
- so φ is of degree 3 and we can say E and E' are 3-isogenous

PART 1

SQIsign

Question

given E and E', can we find an isogeny $\varphi : E \to E'$?

PART 1

SQIsign

Question

given E and E', can we find an isogeny $\varphi : E \to E'$?

easy

easy to verify that *some isogeny* exists, e.g. that E and E' are **isogenous**

hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

PART 1

SQIsign

Question

given E and E', can we find an isogeny $\varphi : E \to E'$?

easy

easy to verify that *some isogeny* exists, e.g. that E and E' are **isogenous**

intermediate

what if we additionally know some points $P, Q \in E$ and their images $\varphi(P), \varphi(Q) \in E'$

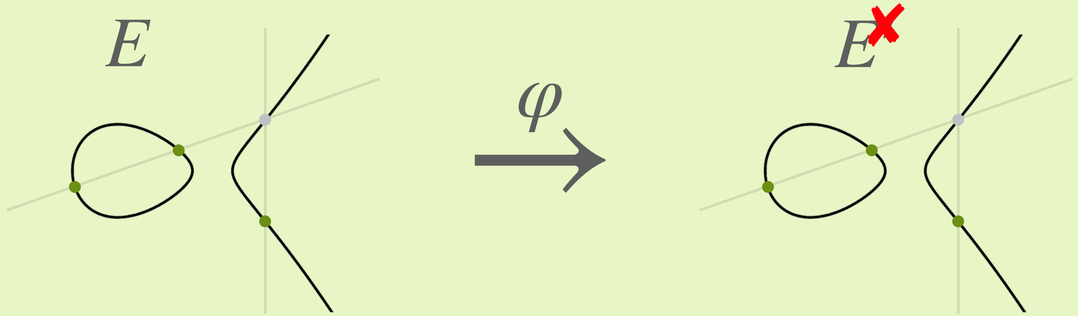
hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

PART 1

SQIsign

endomorphism



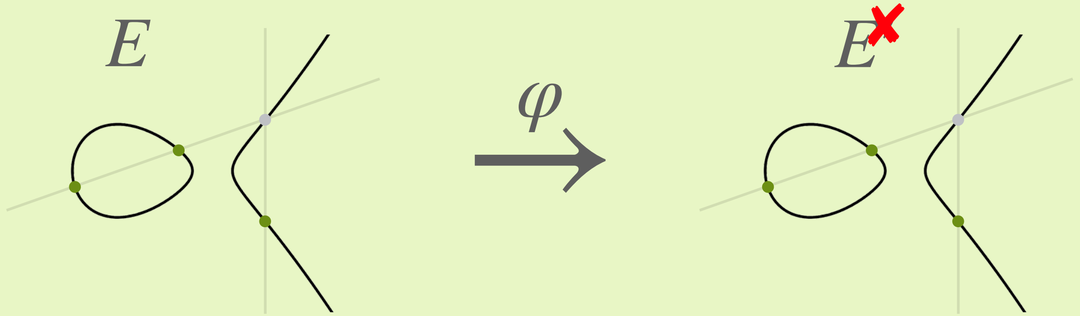
Isogeny Endomorphism

- "nice" map φ (group homomorphism) between elliptic curves $E \to E$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(f_1(x,y)/f_2(x,y) , g_1(x,y)/g_2(x,y))$
- size of $\ker \varphi$ is same as degree of φ!

PART 1

SQIsign

endomorphism



Isogeny Endomorphism

- "nice" map φ (group homomorphism) between elliptic curves $E \to E$
- given by rational functions: a point $(x, y) \in E$ is mapped to ($f_1(x,y)/f_2(x,y)$, $g_1(x,y)/g_2(x,y)$)
- size of $\ker \varphi$ is same as degree of φ!

toy example

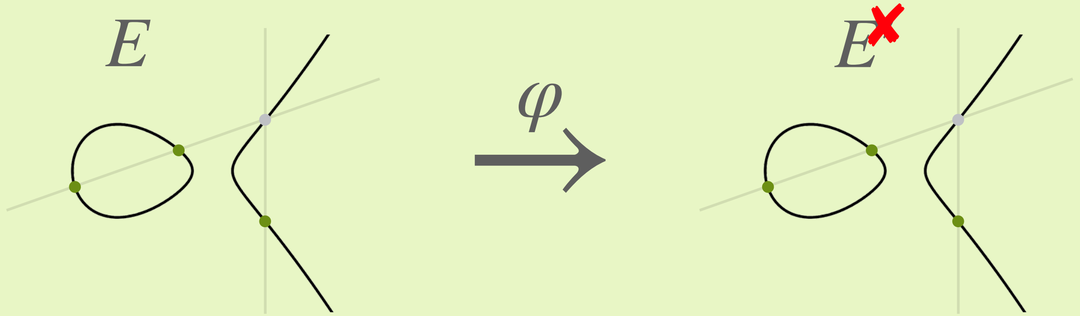
$$E : y^2 = x^3 + x \xrightarrow{\varphi} E : y^2 = x^3 + x$$

$$(x, y) \mapsto \left(\frac{x^4 - 2x^2 + 1}{4(x^3 + x)} : \frac{x^6 y + 5x^4 y - 5x^2 y - y}{8(x^6 + 2x^4 + x^2)} \right) \quad \text{over } \mathbb{F}_{11}$$

PART 1

SQIsign

endomorphism



Isogeny Endomorphism

- "nice" map φ (group homomorphism) between elliptic curves $E \to E$
- given by rational functions: a point $(x, y) \in E$ is mapped to $\left(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y) \right)$
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\ \varphi\ } E : y^2 = x^3 + x$$

$$(x, y) \mapsto \left(\frac{x^4 - 2x^2 + 1}{4(x^3 + x)} : \frac{x^6 y + 5x^4 y - 5x^2 y - y}{8(x^6 + 2x^4 + x^2)} \right) \quad \text{over } \mathbb{F}_{11}$$

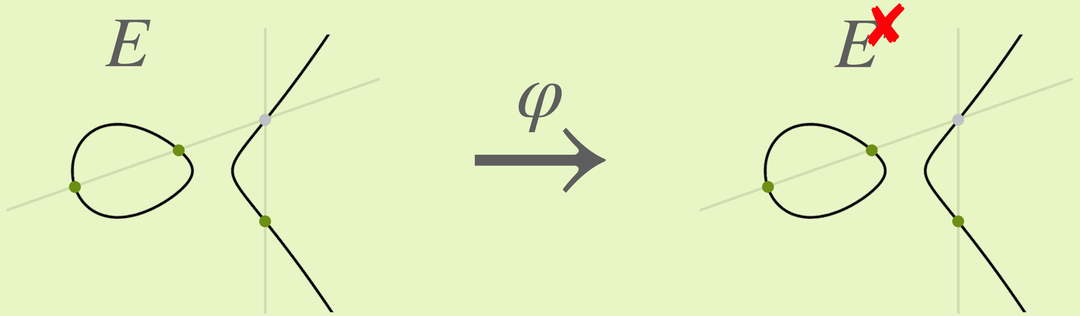
Can check

- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}$ and $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- looks difficult... but actually this just the map $[2] : P \mapsto P + P$
- so [2] has kernel $\mathcal{O}, (0,0), (8 + 7i, 0), (3 + 4i, 0)$, degree [2] is $4 = 2^2$

PART 1

SQIsign

endomorphism



Isogeny Endomorphism

- "nice" map φ (group homomorphism) between elliptic curves $E \to E$
- given by rational functions: a point $(x, y) \in E$ is mapped to ($f_1(x,y)/f_2(x,y)$, $g_1(x,y)/g_2(x,y)$)
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\varphi} E : y^2 = x^3 + x$$

$$(x, y) \mapsto \left(\frac{x^4 - 2x^2 + 1}{4(x^3 + x)} : \frac{x^6 y + 5x^4 y - 5x^2 y - y}{8(x^6 + 2x^4 + x^2)} \right) \quad \text{over } \mathbb{F}_{11}$$

Can check

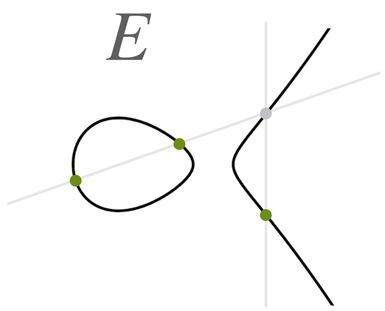
- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}$ and $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- looks difficult... but actually this just the map $[2] : P \mapsto P + P$
- so [2] has kernel $\mathcal{O}, (0,0), (8 + 7i, 0), (3 + 4i, 0)$, degree [2] is $4 = 2^2$

second toy example

Frobenius map. $\pi : (x, y) \mapsto (x^q, y^q)$ **always** an endomorphism for E over $\mathbb{F}_q$

PART 1

SQIsign

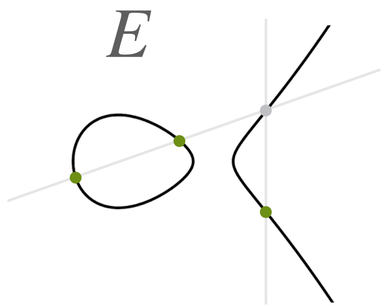


Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$

PART 1

SQIsign



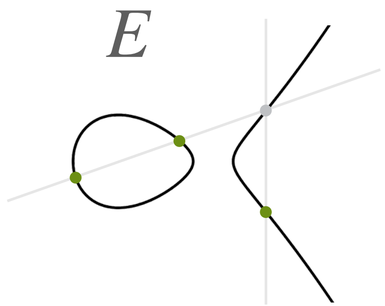
Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

PART 1

SQIsign



Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

endomorphism ring

- we can "add together" different endomorphisms

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

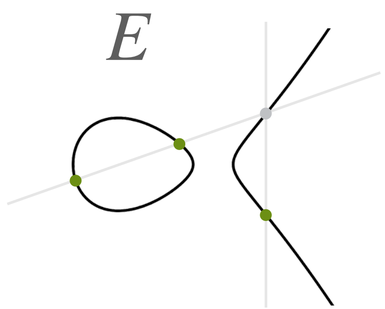
- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

PART 1

SQIsign



Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

endomorphism ring

- we can "add together" different endomorphisms

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

- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

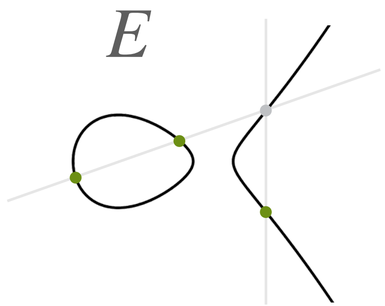
- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

if dim 2

E is **ordinary**

PART 1

SQIsign



Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

endomorphism ring

- we can "add together" different endomorphisms

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

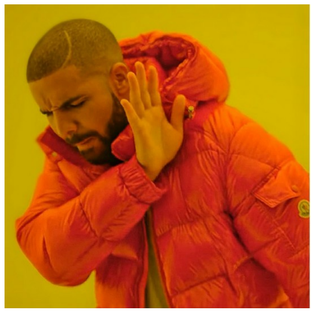
- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

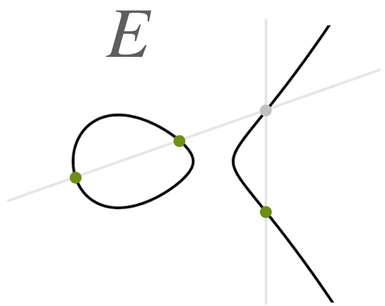
if dim 2

E is **ordinary**



PART 1

SQIsign



Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

endomorphism ring

- we can "add together" different endomorphisms

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

- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

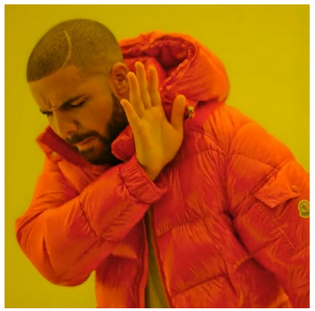
- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

if dim 2

E is **ordinary**

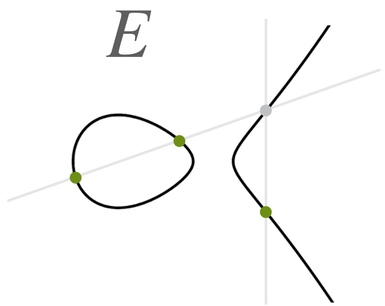
if dim 4

E is
✨✨ **supersingular** ✨✨
(weird funky maps!!)



PART 1

SQIsign



Given just any E over $\mathbb{F}_{q'}$ we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.

endomorphism ring

- we can "add together" different endomorphisms

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

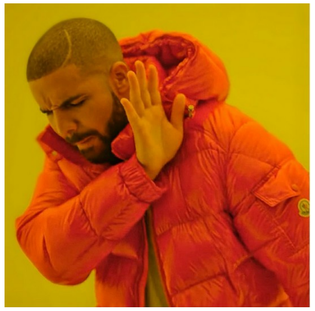
- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

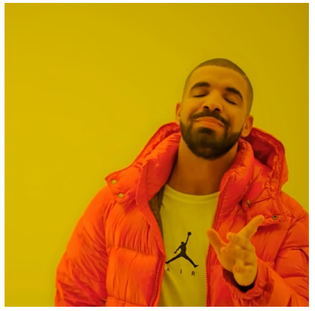
if dim 2

E is **ordinary**



if dim 4

E is
✨✨ **supersingular** ✨✨
(weird funky maps!!)



Radboud University

PART 1

SQIsign

Question

given supersingular E, can we find
weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?

PART 1

SQIsign

Question

given supersingular E, can we find
weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?

easy

easy to verify that
such endoms exists,
e.g. that E
is **supersingular**

hard

actually giving an
endom. $\omega \in \mathrm{End}(E)$
or some way to
compute this

PART 1

SQIsign

Question

given supersingular E, can we find
weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?

easy

easy to verify that
such endoms exists,
e.g. that E
is **supersingular**

surprisingly easy

we know $\mathrm{End}(E_0)$ for the
specific curve $E_0 : y^2 = x^3 + x$
and for any $E_0 \to E_A$,
we can then compute $\mathrm{End}(E_A)$
(knowledge of endom. ring is contagious)

hard

actually giving an
endom. $\omega \in \mathrm{End}(E)$
or some way to
compute this

PART 1

SQIsign

Question

given supersingular E, can we find weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?

hard

actually giving an endom. $\omega \in \mathrm{End}(E)$ or some way to compute this

Question

given E and E', can we find an isogeny $\varphi : E \to E'$?

hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

PART 1

SQIsign

Question

given supersingular E, can we find weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?

hard

actually giving an endom. $\omega \in \mathrm{End}(E)$ or some way to compute this

equivalent!!!

Question

given E and E', can we find an isogeny $\varphi : E \to E'$?

hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

Best Paper ASIACRYPT 2020

Best Paper award

YouTube Chat

Chair: Shiho Moriai & Huaxiong Wang

Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness

Show abstract ›

Akinori Hosoyamada, Tak[illegible] Yasuda

S[illegible] PRESTO, Laboratories / Nagoya Uni[illegible]ty / NTT [illegible] Research, Inc.

Media:

PART 1: SQIsign

New results on Gimli: full-permutation distinguishers and improved collisions

Show abstract ›

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras

Inria, France

Media:

SQISign: Compact Post-Quantum signatures from Quaternions and Isogenies

Show abstract ›

Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, Benjamin Wesolowski

IBM Research, Zurich; Université Aix-Marseilles; DGA, Ecole Polytechnique; University of Birmingham; Université de Bordeaux, CNRS

Media:

PART 1

SQIsign

SQIsign

A new isogeny-based signature scheme, with **high soundness**

2020 | 2021 | 2022 | 2023 | 2024

PART 1

SQIsign

Key Generation

- **System parameters:** prime p, starting curve E_0
- **Secret Key:** isogeny $\varphi_A : E_0 \to E_A$, and then also $\mathrm{End}(E_A)$
- **Public Key:** the curve $E_A : y^2 = X^3 + Ax^2 + x$, with $A \in \mathbb{F}_q$

everyone knows $\mathrm{End}(E_0)$

E_0

PART 1

SQIsign

Key Generation

- **System parameters:** prime p, starting curve E_0
- **Secret Key:** isogeny $\varphi_A : E_0 \to E_A$, and then also $\mathrm{End}(E_A)$
- **Public Key:** the curve $E_A : y^2 = X^3 + Ax^2 + x$, with $A \in \mathbb{F}_q$

everyone knows $\mathrm{End}(E_0)$

only **you** know φ_A and $\mathrm{End}(E_A)$

PART 1

SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

everyone knows $\text{End}(E_0)$

only **you** know φ_A and $\text{End}(E_A)$

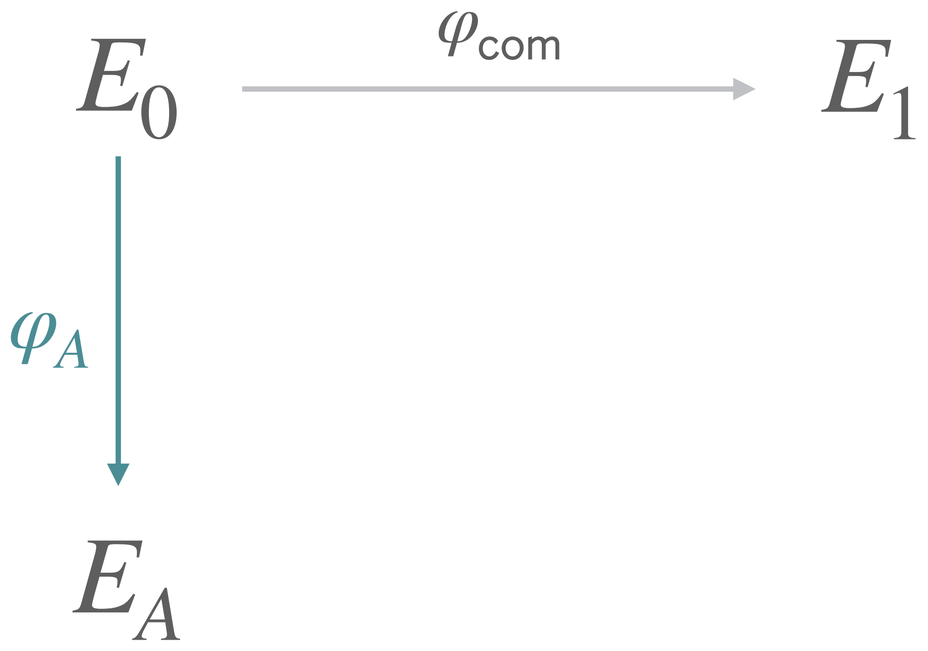
PART 1

SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

everyone knows $\text{End}(E_0)$



only **you** know φ_{com} and $\text{End}(E_1)$

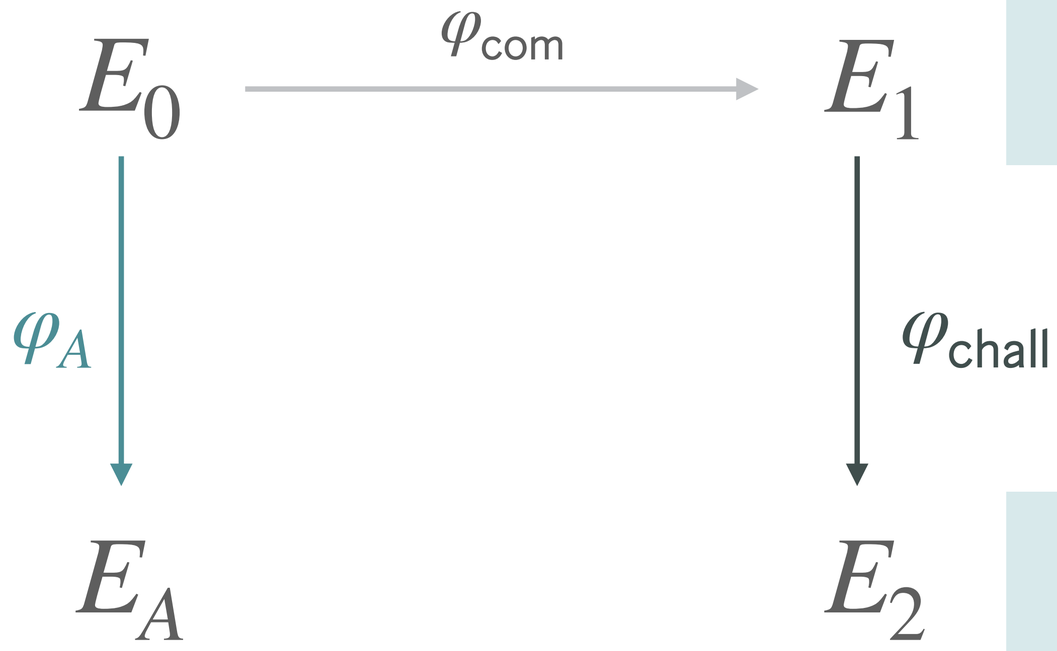
only **you** know φ_A and $\text{End}(E_A)$

PART 1
SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

everyone knows $\text{End}(E_0)$



only **you** know φ_{com} and $\text{End}(E_1)$

only **you** know φ_A and $\text{End}(E_A)$

only **you** know $\text{End}(E_2)$

PART 1

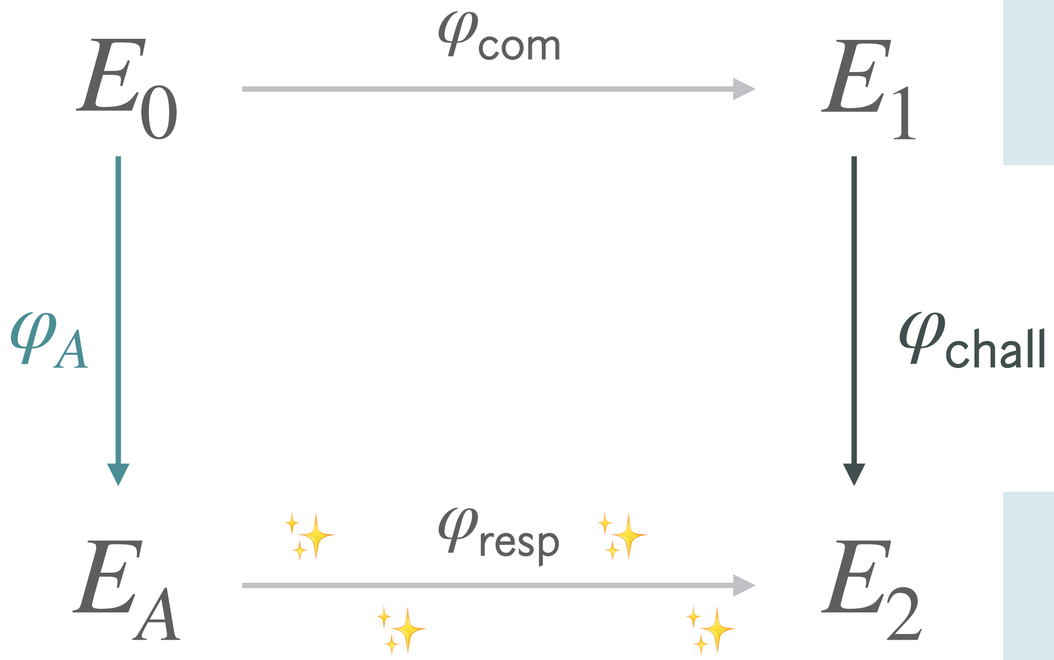
SQIsign

Identification protocol

- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

everyone knows $\text{End}(E_0)$

only **you** know φ_{com} and $\text{End}(E_1)$



only **you** know φ_A and $\text{End}(E_A)$

only **you** know $\text{End}(E_2)$

Fact: ONLY, given $\text{End}(E_a)$ and $\text{End}(E_2)$ you can compute a proper response

PART 1
SQIsign

Identification protocol

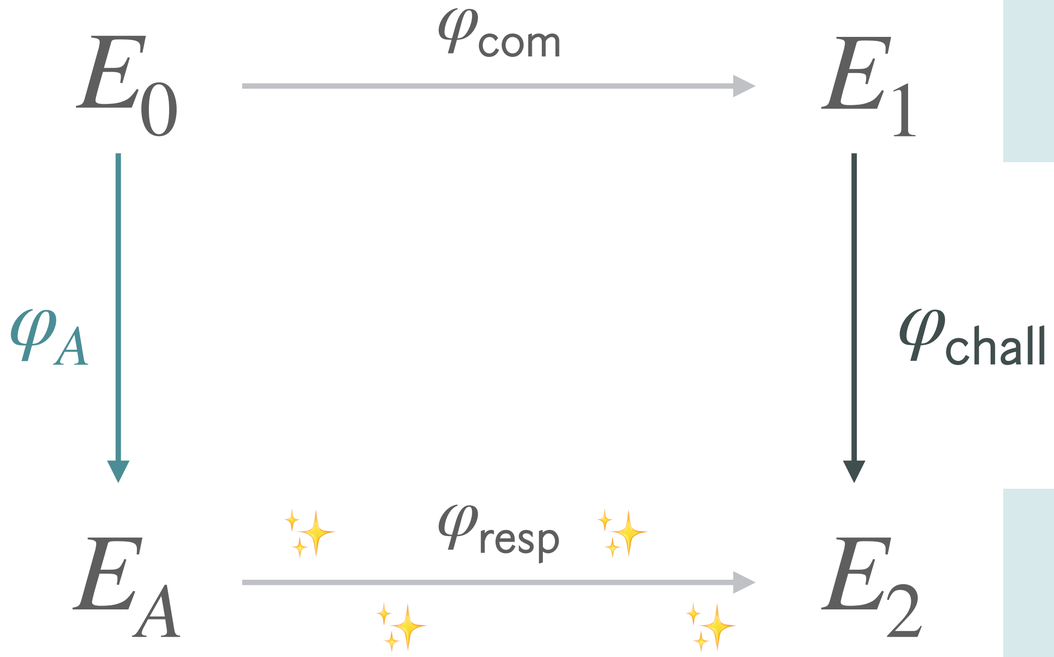
- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

signature scheme

replace semi-random φ_{chall}
by a challenge isogeny generated
from SHAKE256(msg || E_1)

everyone knows
$\text{End}(E_0)$

only **you** know
φ_{com} and $\text{End}(E_1)$



only **you** know
φ_A and $\text{End}(E_A)$

only **you** know
$\text{End}(E_2)$

Fact: ONLY, given $\text{End}(E_a)$ and $\text{End}(E_2)$
you can compute a proper response

Radboud University

PART 1

SQIsign

Identification protocol

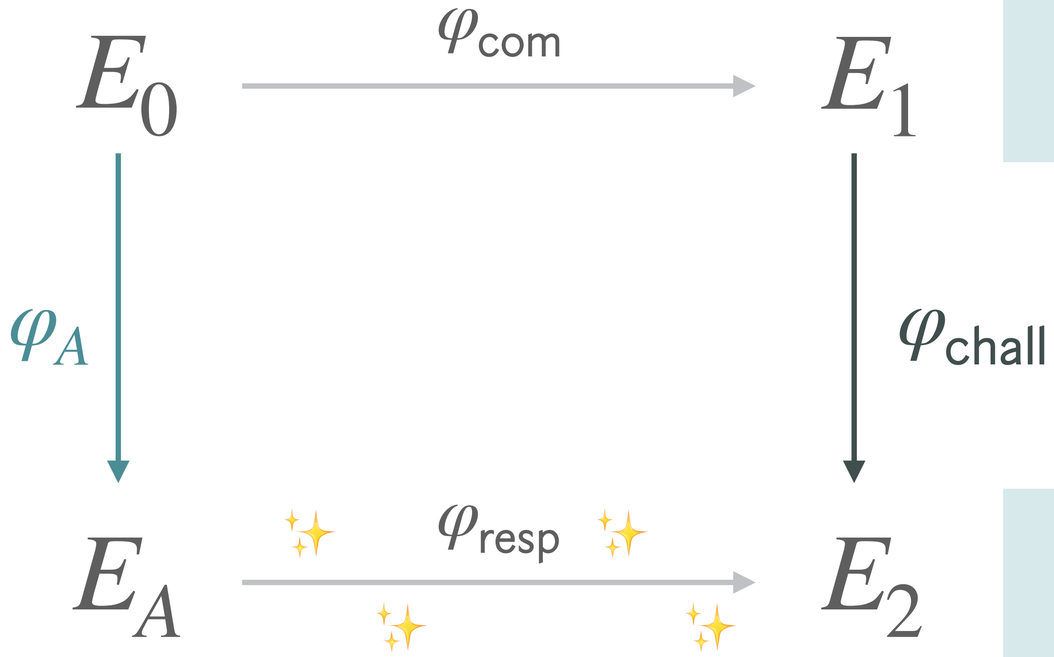
- **Commitment:** random isogeny $\varphi_{\text{com}} : E_0 \to E_1$
- **Challenge:** semi-random isogeny $\varphi_{\text{chall}} : E_1 \to E_2$
- **Response:** "matching" isogeny $\varphi_{\text{resp}} : E_A \to E_2$

signature scheme

replace semi-random φ_{chall}
by a challenge isogeny generated
from SHAKE256(msg || E_1)

everyone knows
$\text{End}(E_0)$

only **you** know
φ_{com} and $\text{End}(E_1)$



only **you** know
φ_A and $\text{End}(E_A)$

only **you** know
$\text{End}(E_2)$

WARNING!

with this approach
the response will
be **large**, degree 2^{1000}

Fact: ONLY, given $\text{End}(E_a)$ and $\text{End}(E_2)$
you can compute a proper response

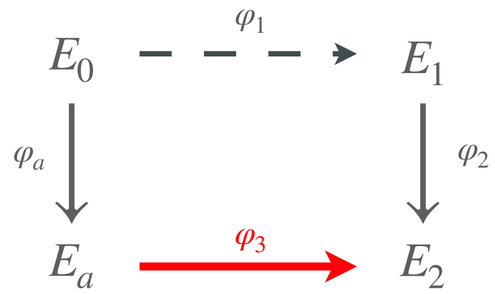
To learn more about verification in detail:
see tutorial at https://vodice.post-quantum-crypto.com
by Lorenz Panny & me

Radboud University

PART 1

SQIsign

computing the signature

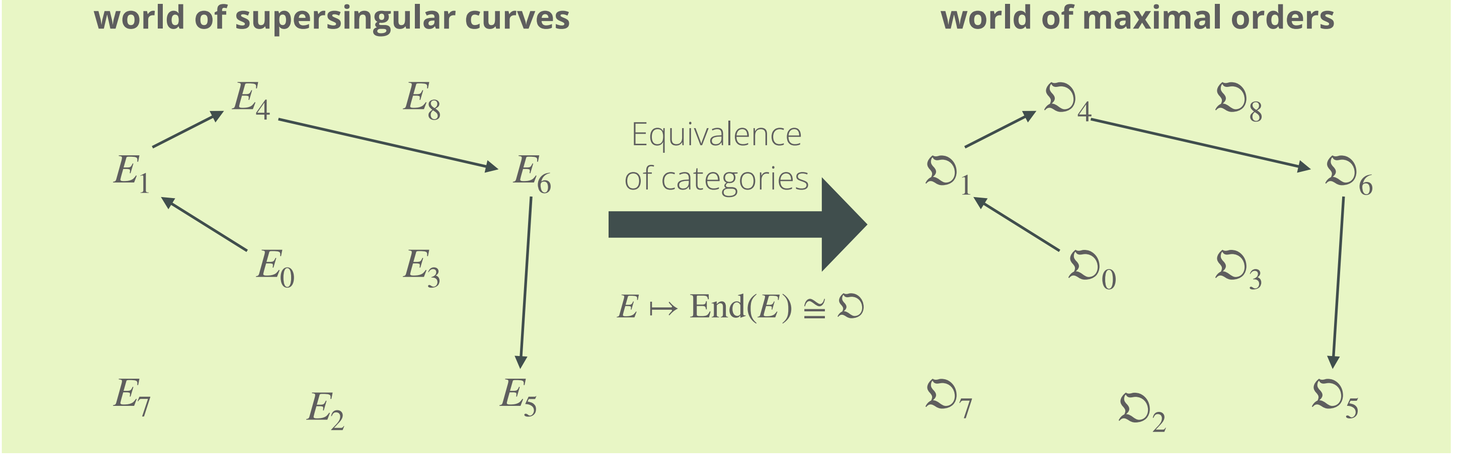


Fact: Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

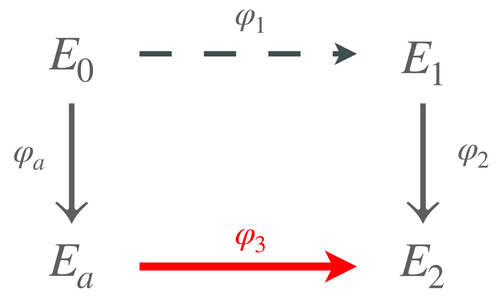
PART 1

SQIsign

Deuring correspondence



computing the signature

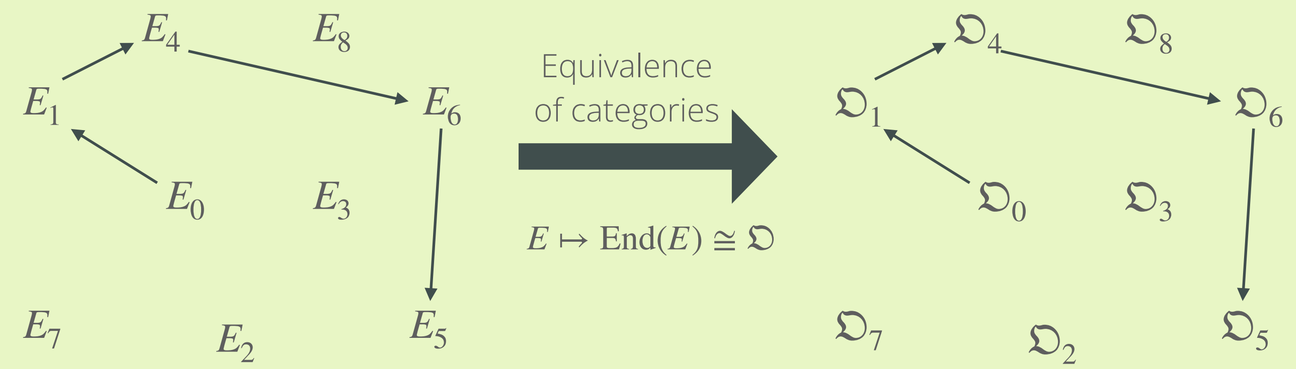


Fact: Given $\mathrm{End}(E_a)$ and $\mathrm{End}(E_2)$ you can compute $\varphi_3 : E_a \to E_2$

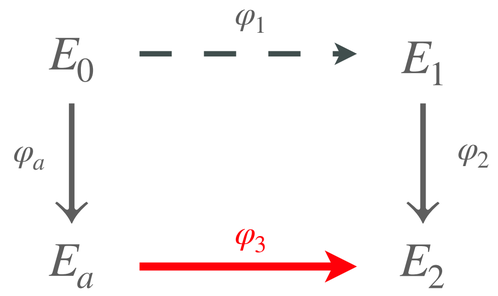
PART 1

SQIsign

Deuring correspondence



computing the signature



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

curve-order dictionary

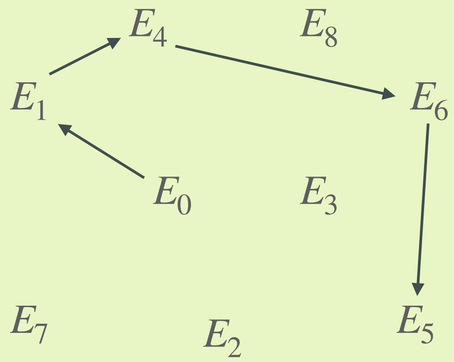
supersingular curves	quaternion orders
curve E (up to Galois conjugacy)	maximal order $\mathfrak{O}$ (up to isomorphism)

PART 1

SQIsign

Deuring correspondence

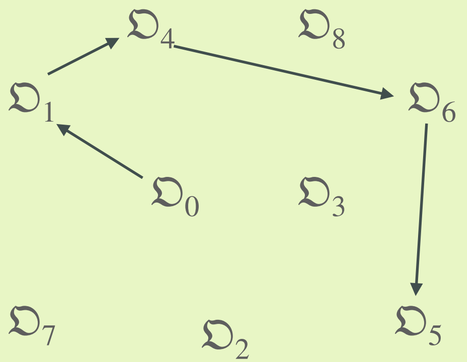
world of supersingular curves



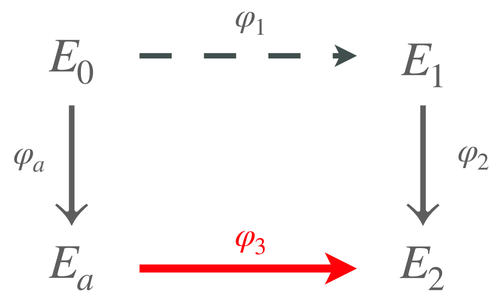
Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathfrak{O}$

world of maximal orders



computing the signature



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

curve-order dictionary

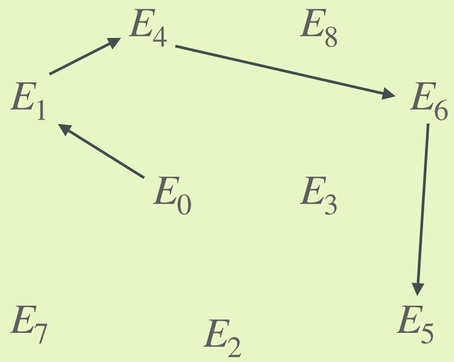
supersingular curves	quaternion orders
curve E (up to Galois conjugacy)	maximal order $\mathfrak{O}$ (up to isomorphism)
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathfrak{O}_1$-ideal and right $\mathfrak{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset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

PART 1

SQIsign

Deuring correspondence

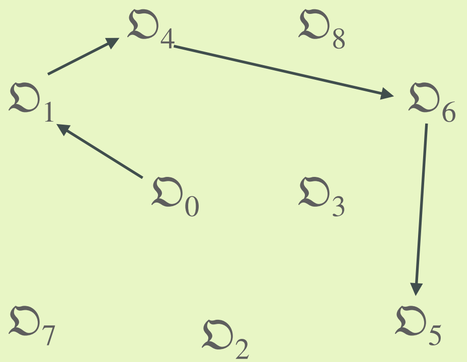
world of supersingular curves



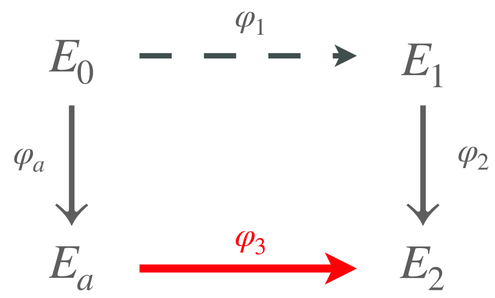
Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathfrak{O}$

world of maximal orders



computing the signature



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 $\mathfrak{O}$ (up to isomorphism)
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathfrak{O}_1$-ideal and right $\mathfrak{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset \mathfrak{O}$
and this continues for the *degree*, the *dual*, *equivalence*, *composition*...	and this continues for the *norm*, the *dual*, *equivalence*, *multiplication*...

PART 1

SQIsign

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

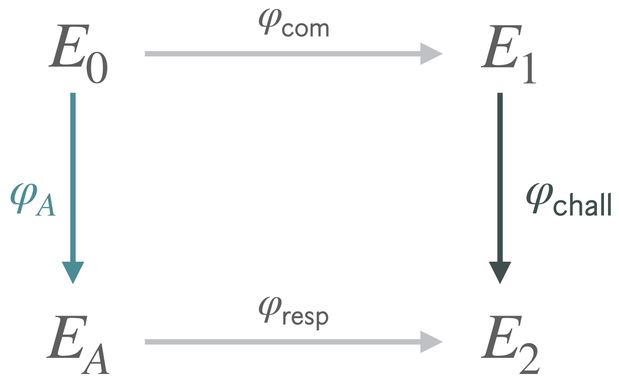
A new algorithm to translate ideals to isogenies.

2020 2021 2022 2023 2024

PART 1

SQIsign

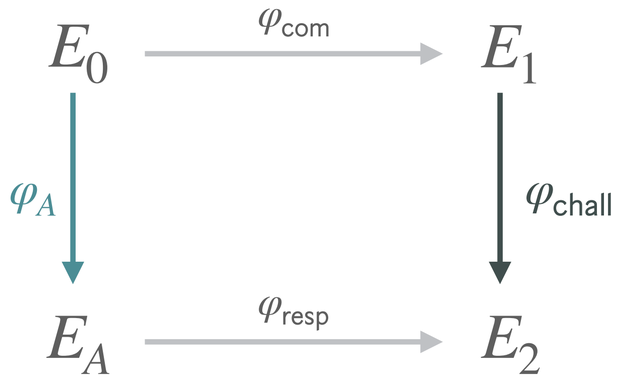
Elliptic curve world



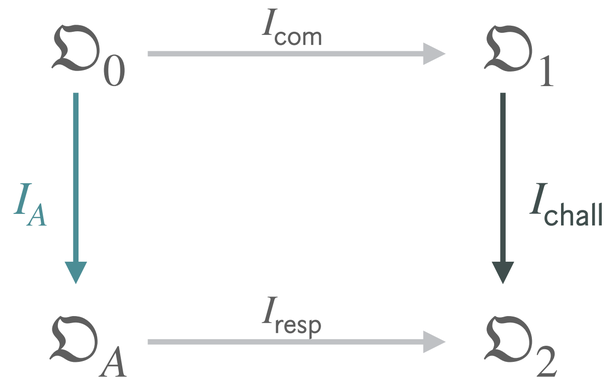
PART 1

SQIsign

Elliptic curve world

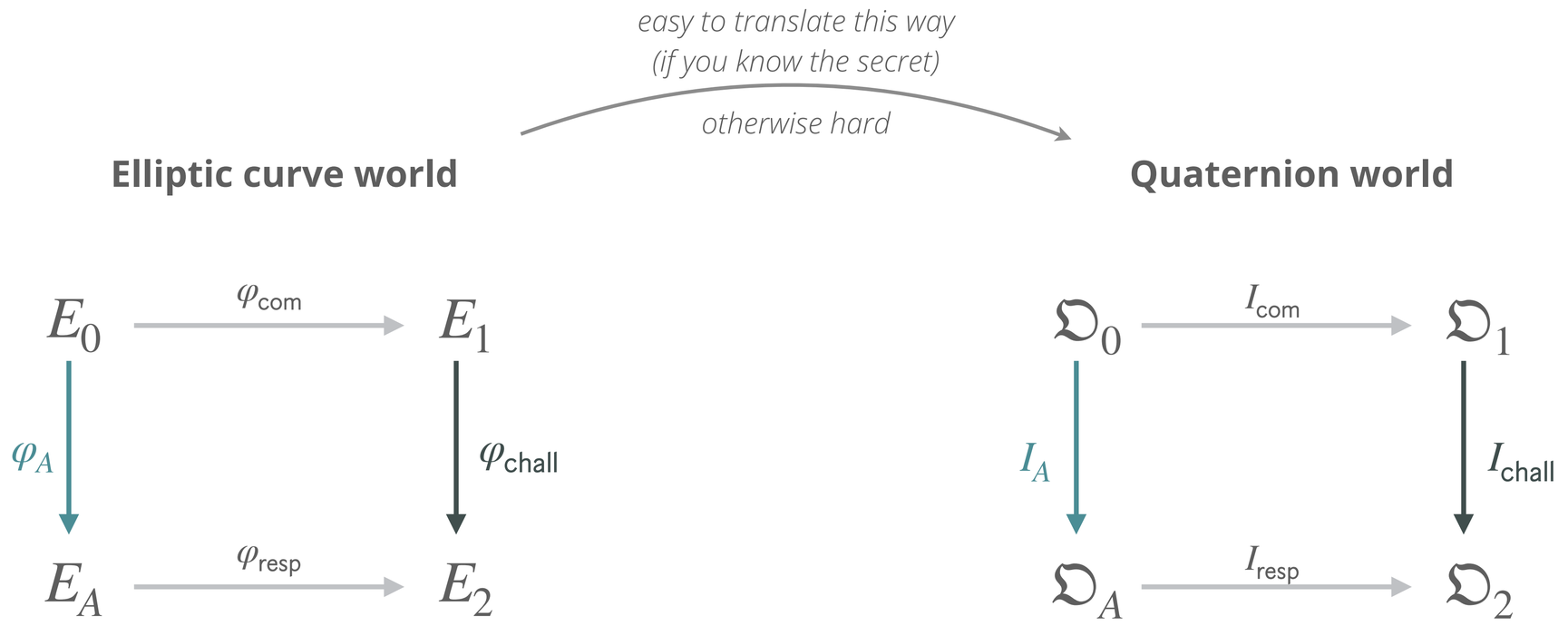


Quaternion world



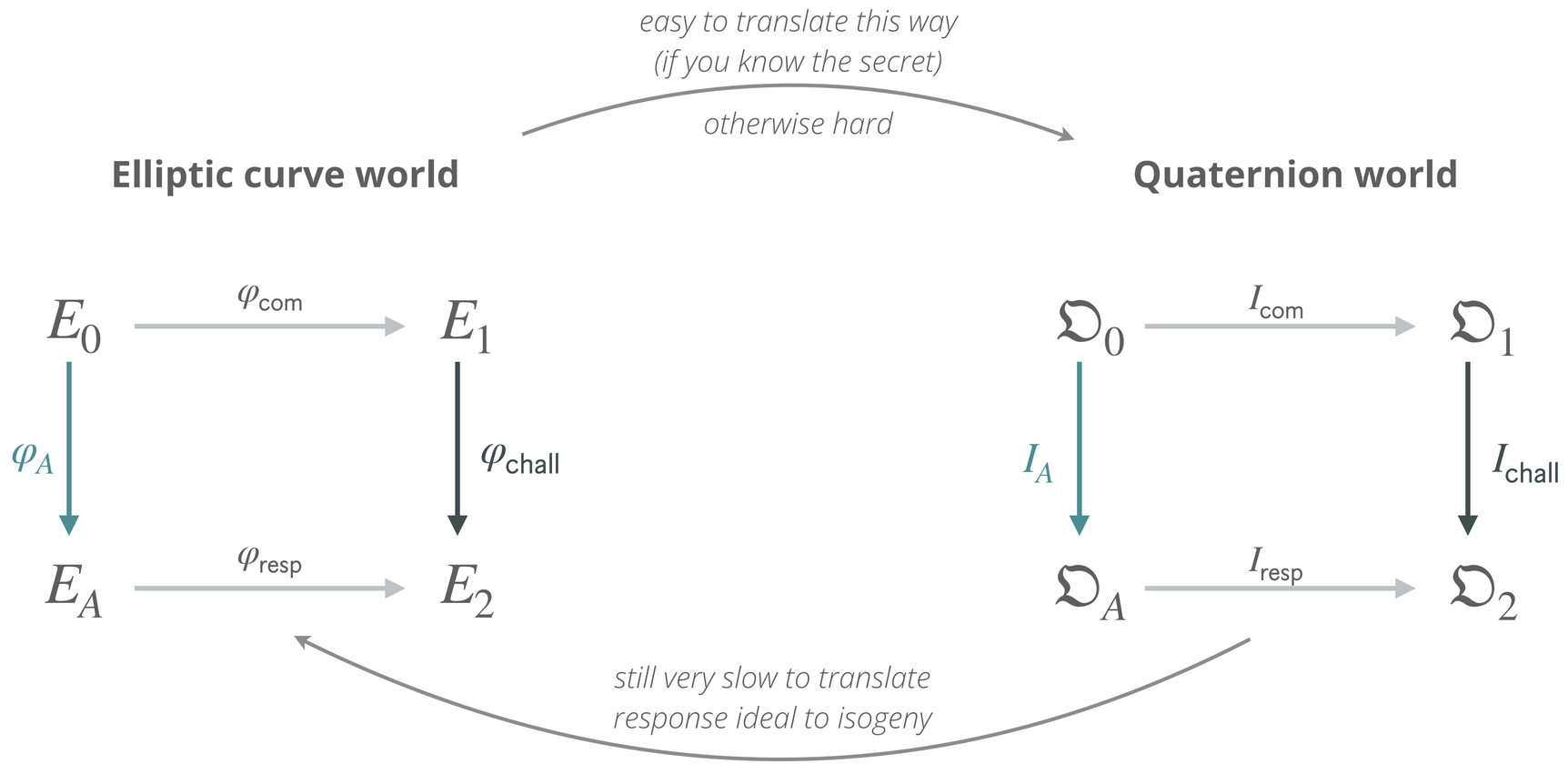
PART 1

SQIsign



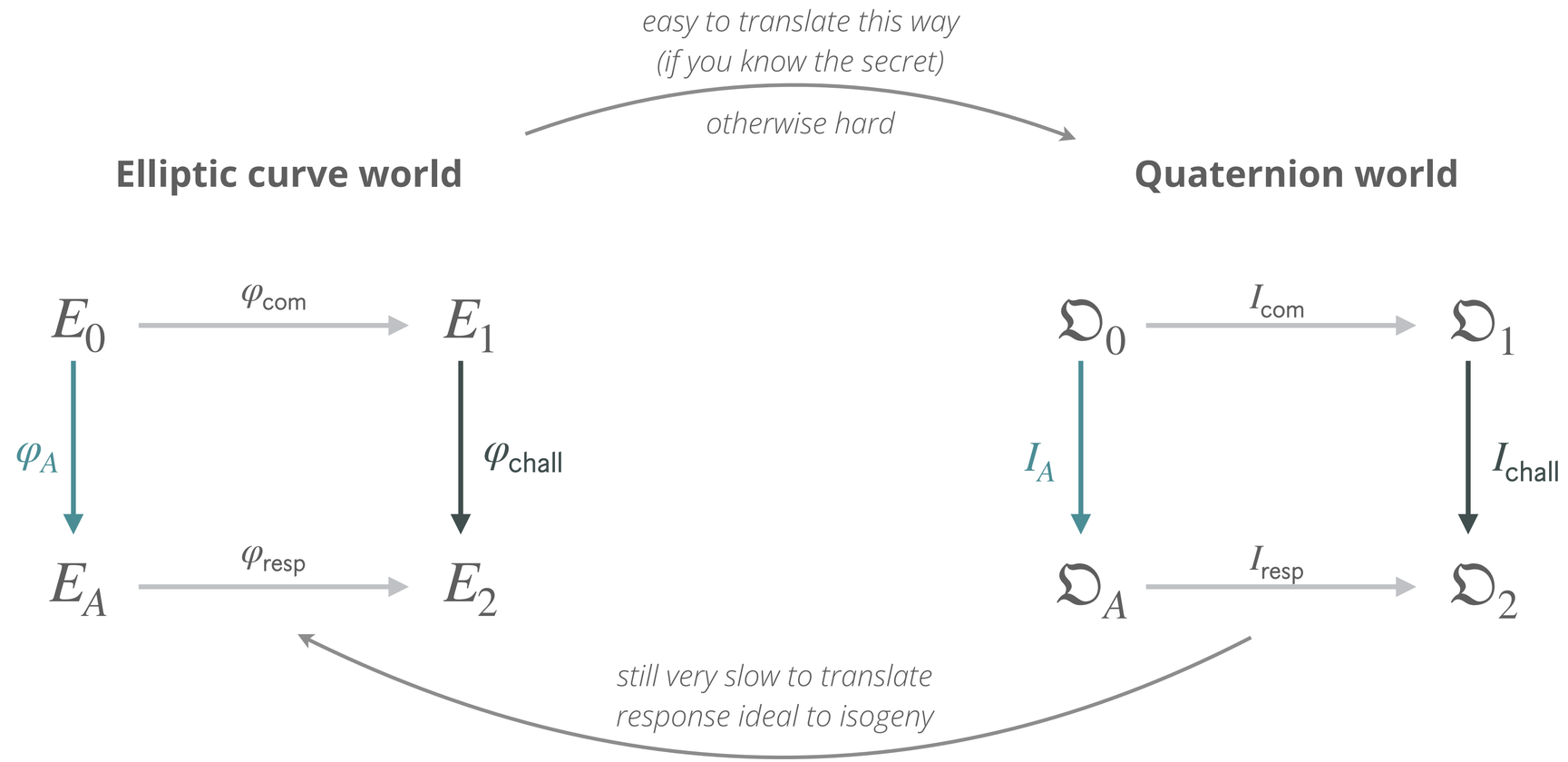
PART 1

SQIsign



PART 1

SQIsign



problem

need to break up $E_A \to E_2$ into smaller blocks

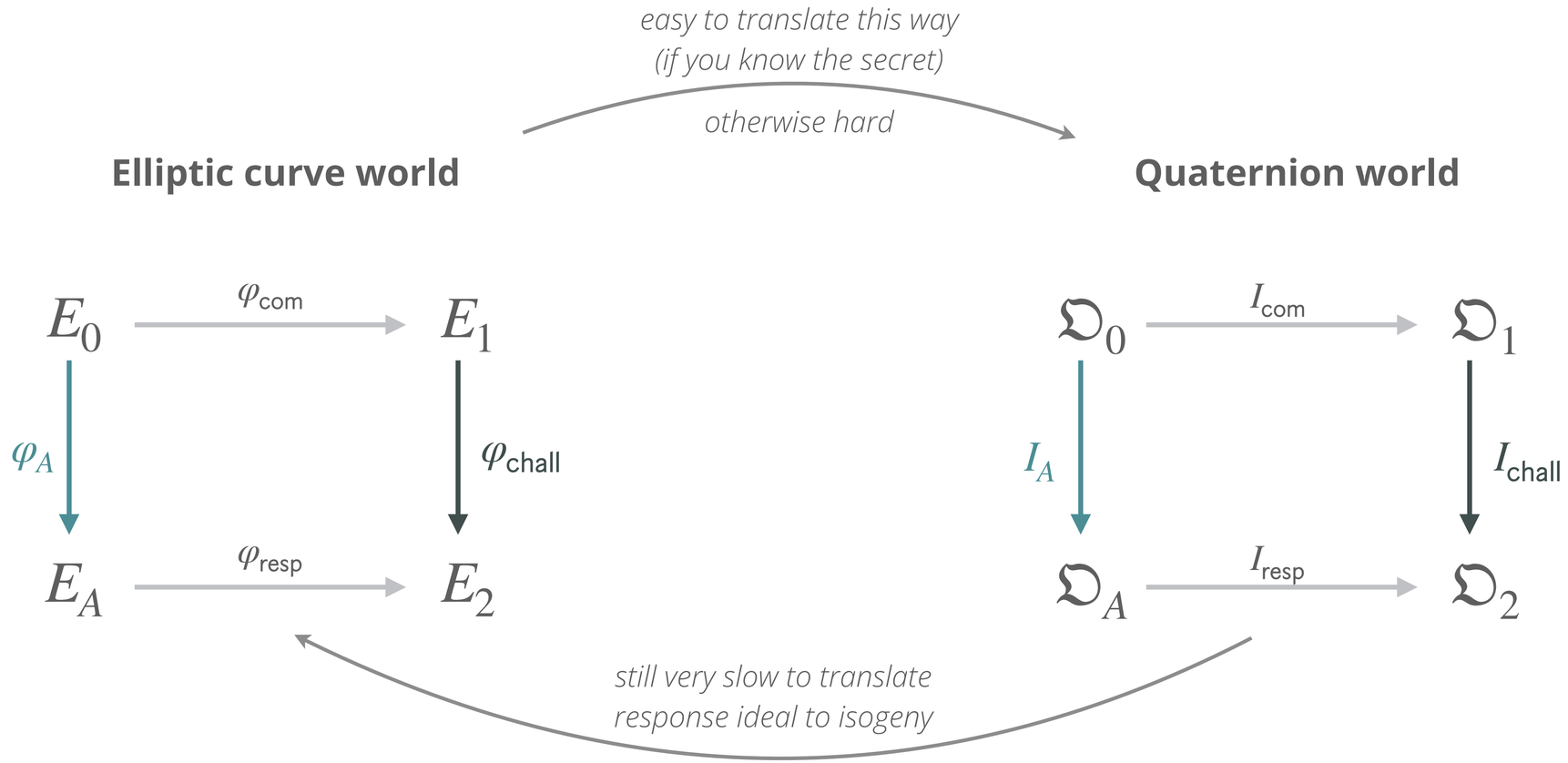
$E_A \to E^{(1)} \to E^{(2)} \to \ldots \to E^{(n-1)} \to E^{(n)} = E_2$

translating to the right blocks is very slow...

(NIST SQIsign has 13 blocks)

PART 1

SQIsign



problem

need to break up $E_A \to E_2$ into smaller blocks
$E_A \to E^{(1)} \to E^{(2)} \to \ldots \to E^{(n-1)} \to E^{(n)} = E_2$
translating to the right blocks is very slow...
(NIST SQIsign has 13 blocks)

SQIsign2

among others, a much better way
to translate I_{resp} back to φ_{resp}
improving speed **per block**

3 Best Papers EUROCRYPT 2023

Lyon Congress Center - Plenary - Auditorium Lumière

Session chair: Joppe Bos

YouTube

An Efficient Key Recovery Attack on SIDH

Best Paper Award

Wouter Castryck, Thomas Decru

KU Leuven

Speaker(s): Thomas Decru

Show abstract ›

(paper #409) Media:

PART 2: The BREAK.

Breaking SIDH in Polynomial Time

Honourable Mention

Damien Robert

Inria Bordeaux

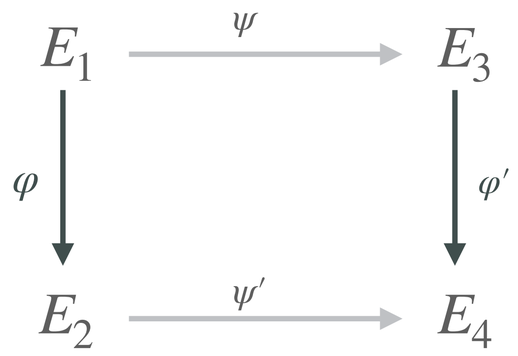
Show abstract ›

(paper #96) Media:

PART 2

The BREAK

Kani's Lemma (1997)



if $\deg \varphi = \deg \varphi'$
and $\deg \psi = \deg \psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$

PART 2

The BREAK

Kani's Lemma (1997)

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_3 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_2 & \xrightarrow{\psi'} & E_4 \end{array}$$

if $\deg\varphi = \deg\varphi'$
and $\deg\psi = \deg\psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$

1D isogeny

if we know $\ker\varphi$,
then we can compute
$\varphi : E \to E'$ and $\varphi(P)$

PART 2

The BREAK

Kani's Lemma (1997)

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_3 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_2 & \xrightarrow{\psi'} & E_4 \end{array}$$

if $\deg\varphi = \deg\varphi'$
and $\deg\psi = \deg\psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$

1D isogeny

if we know $\ker\varphi$,
then we can compute
$\varphi : E \to E'$ and $\varphi(P)$

2D kernel

the kernel of 2D-iso Φ
is given by images $\varphi(P), \psi(P)$
for $P \in E_1$ of order $\deg\varphi + \deg\psi$

PART 2

The BREAK

Kani's Lemma (1997)

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_3 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_2 & \xrightarrow{\psi'} & E_4 \end{array}$$

if $\deg\varphi = \deg\varphi'$
and $\deg\psi = \deg\psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$

1D isogeny

if we know $\ker\varphi$,
then we can compute
$\varphi : E \to E'$ and $\varphi(P)$

2D kernel

the kernel of 2D-iso Φ
is given by images $\varphi(P), \psi(P)$
for $P \in E_1$ of order $\deg\varphi + \deg\psi$

2D isogeny

if we know $\deg\varphi$ and $\deg\psi$
and we know these $\varphi(P)$, $\psi(P)$,
compute $\Phi : E_2 \times E_3 \to E_1 \times E_4$

PART 2

The BREAK

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

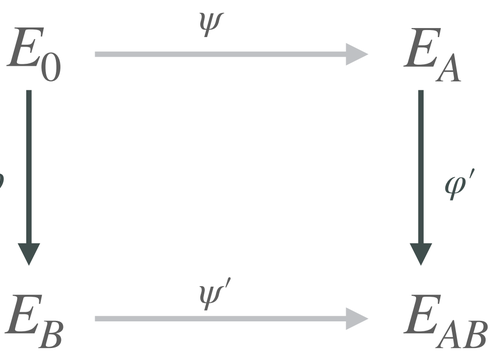
The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

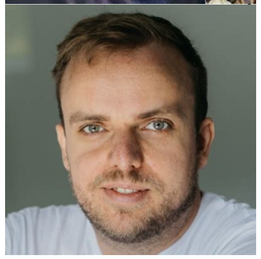
PART 2

The BREAK

Castryck & Decru (2022)



in SIDH/SIKE the secrets are φ and ψ



PART 2

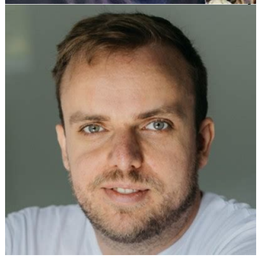
The BREAK

Castryck & Decru (2022)

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi} & E_A \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} \\ E_B & \xrightarrow{\psi'} & E_{AB} \end{array}$$

in SIDH/SIKE the secrets are φ and ψ

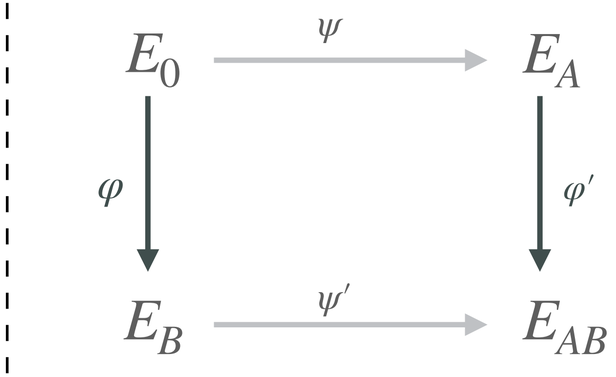
we are given $\deg \varphi$, $\deg \psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg \varphi + \deg \psi$



PART 2

The BREAK

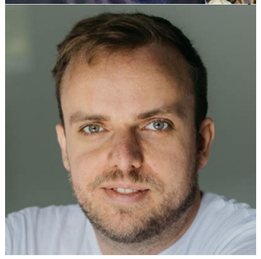
Castryck & Decru (2022)



in SIDH/SIKE the secrets are φ and ψ

we are given $\deg\varphi$, $\deg\psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg\varphi + \deg\psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PART 2

The BREAK

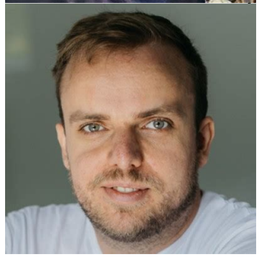
Castryck & Decru (2022)

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi} & E_A \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_B & \xrightarrow{\psi'} & E_{AB} \end{array}$$

in SIDH/SIKE the secrets are φ and ψ

we are given $\deg\varphi$, $\deg\psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg\varphi + \deg\psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PROBLEM!

degree of Φ is then
$\deg\varphi + \deg\psi$
making Φ difficult/impossible
to compute in practice...

PART 2

The BREAK

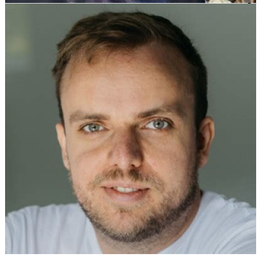
Castryck & Decru (2022)

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi} & E_A \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} \\ E_B & \xrightarrow{\psi'} & E_{AB} \end{array}$$

in SIDH/SIKE the secrets are φ and ψ

we are given $\deg\varphi$, $\deg\psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg\varphi + \deg\psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PROBLEM!

degree of Φ is then $\deg\varphi + \deg\psi$
making Φ difficult/impossible to compute in practice...

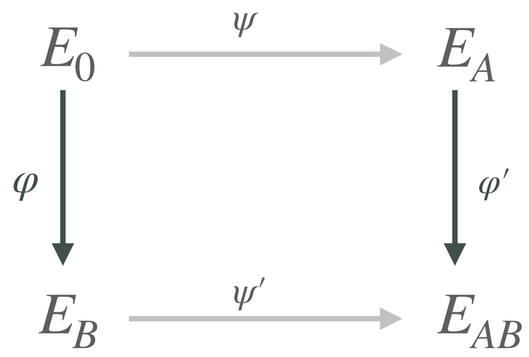
Solution!

use knowledge of $\mathrm{End}(E_0)$ to modify the square so that Φ is of degree 2^n, then compute Φ easily

PART 2

The BREAK

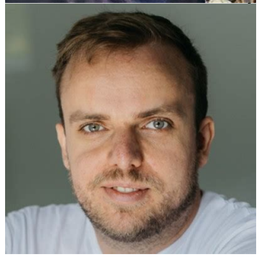
Castryck & Decru (2022)



in SIDH/SIKE the secrets are φ and ψ

we are given $\deg\varphi$, $\deg\psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg\varphi + \deg\psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PROBLEM!

degree of Φ is then $\deg\varphi + \deg\psi$ making Φ difficult/impossible to compute in practice...

Solution!

use knowledge of $\mathrm{End}(E_0)$ to modify the square so that Φ is of degree 2^n, then compute Φ easily

Robert (2022)

generalize Kani's lemma:
don't just embed 1D into 2D,
embed into 4D or 8D!
Then Φ easy to compute
and we don't need $\mathrm{End}(E_0)$

2 Best Papers EUROCRYPT 2024

Awarded Papers

Kongresssaal

Marc Joye and Gregor Leander

Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis

Itai Dinur

Ben-Gurion University

Speaker(s): Itai Dinur

(paper #326)

Show abstract ›

PART 3: New Dimensions

SQIsignHD: New Dimensions in Cryptography

Pierrick Dartois, Antonin Leroux, Damien Robert, Benjamin Wesolowski

INRIA, IMB, DGA-MI, ENS de Lyon, CNRS, UMPA

Speaker(s): Pierrick Dartois

(paper #149)

Show abstract ›

AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing

Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, Krijn Reijnders

University College London, NTNU, University of Regensburg, Radboud University Nijmegen

Speaker(s): Jonathan Komada Eriksen

(paper #86)

Show abstract ›

PART 3

New Dimensions

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

2020 | 2021 | 2022 | 2023 | 2024

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.

PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

In the words of the HD master

"If we know the value of $\varphi : E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"

- Damien Robert

PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

In the words of the HD master

"If we know the value of $\varphi : E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"
- Damien Robert

isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \to E'$ and
we assume we know $P_1, \ldots, P_n$ and images $\varphi(P_1), \ldots, \varphi(P_n)$.
Assume for the moment that $\deg \varphi = 2^n - x^2$ for some $x \in \mathbb{Z}$

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

PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

In the words of the HD master

"If we know the value of $\varphi : E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"
- Damien Robert

isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \to E'$ and
we assume we know $P_1, \ldots, P_n$ and images $\varphi(P_1), \ldots, \varphi(P_n)$.
Assume for the moment that $\deg \varphi = 2^n - x^2$ for some $x \in \mathbb{Z}$

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

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

PART 3

New Dimensions

In the words of the HD master

"If we know the value of $\varphi : E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"

- Damien Robert

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \to E'$ and
we assume we know $P_1, \ldots, P_n$ and images $\varphi(P_1), \ldots, \varphi(P_n)$.
Assume for the moment that $\deg \varphi = 2^n - x^2$ for some $x \in \mathbb{Z}$

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ {\scriptstyle [x]}\downarrow & & \downarrow{\scriptstyle [x]} \\ E & \xrightarrow{\varphi} & E' \end{array}$$

We know and can compute $[x]$ easily! So we can apply Kani's!

$$\Phi : E \times E' \to E \times E'$$

Radboud University

PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

In the words of the HD master

"If we know the value of $\varphi : E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"
- Damien Robert

isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \to E'$ and we assume we know $P_1, \ldots, P_n$ and images $\varphi(P_1), \ldots, \varphi(P_n)$.
Assume for the moment that $\deg \varphi = 2^n - x^2$ for some $x \in \mathbb{Z}$

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ {\scriptstyle [x]}\downarrow & & \downarrow{\scriptstyle [x]} \\ E & \xrightarrow{\varphi} & E' \end{array}$$

We know and can compute $[x]$ easily! So we can apply Kani's!

$$\Phi : E \times E' \to E \times E'$$

As Φ of degree 2^n, easy to compute and we can use Φ to compute $\varphi(Q)$ for any other point $Q \in E$

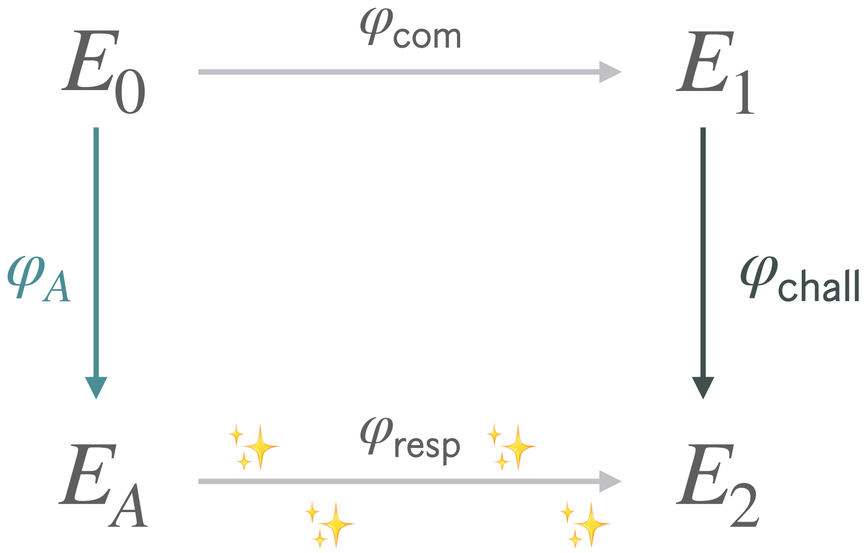
PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$



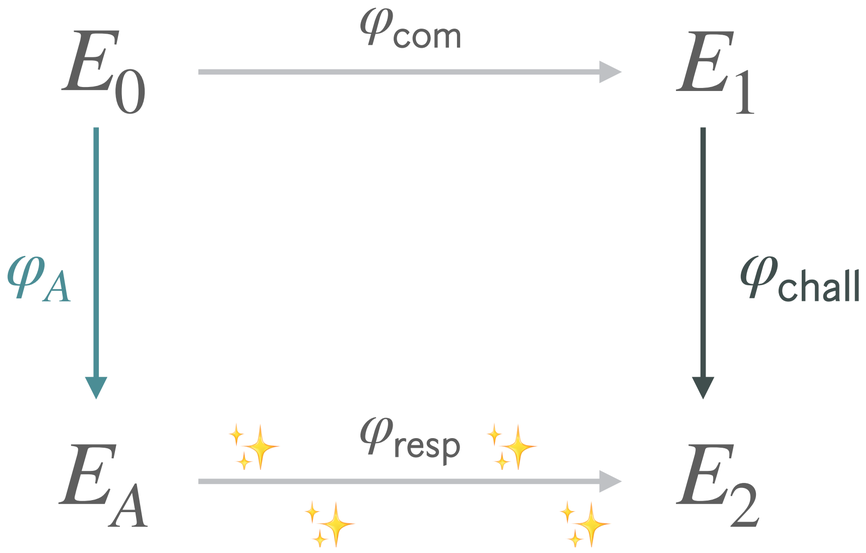
PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 HD representation: E_A is known, give points P_i and $\varphi_{\text{resp}}(P_i)$

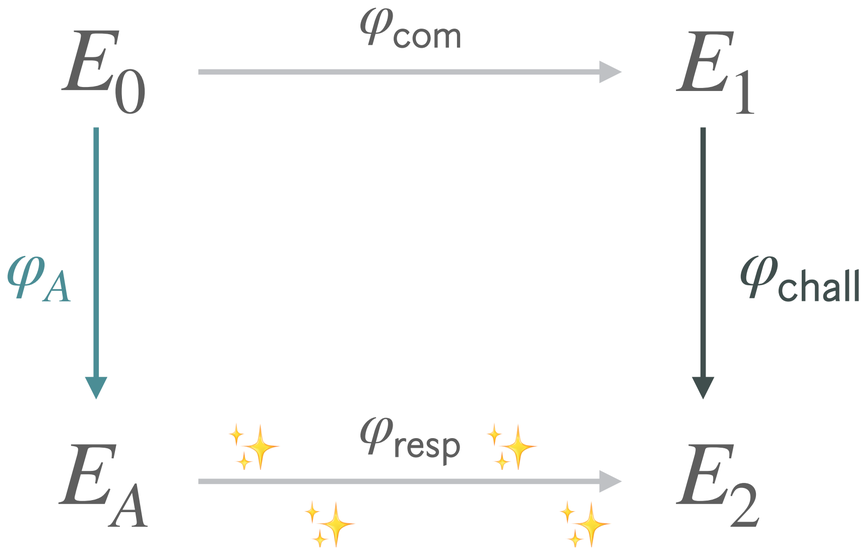
PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 HD representation: E_A is known, give points P_i and $\varphi_{\text{resp}}(P_i)$

✓ **faster primes!**

✓ **FASTER signing!**

✓ **THE BEST security!**

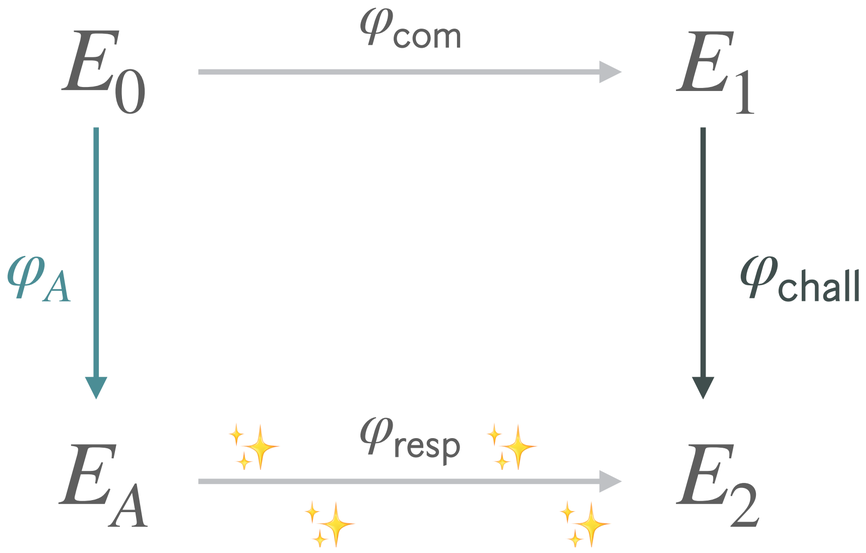
PART 3

New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 HD representation: E_A is known, give points P_i and $\varphi_{\text{resp}}(P_i)$

✓ **faster primes!**

✓ **FASTER signing!**

✓ **THE BEST security!**

✗ **verification is now a 4D- or 8D-isogeny... difficult, complex, and rather slow**

PART 3

New Dimensions

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

AprèsSQI

Signing will be slow... We push verification to the limits using extension fields.

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.

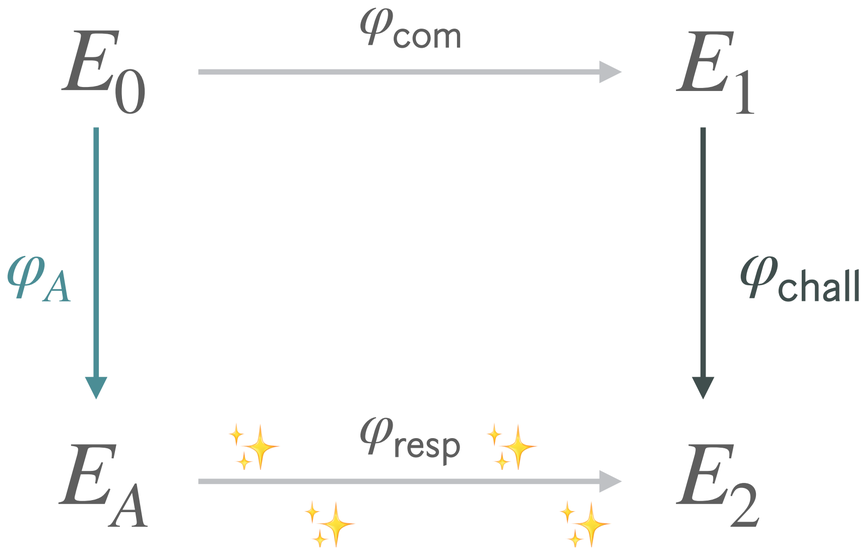
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



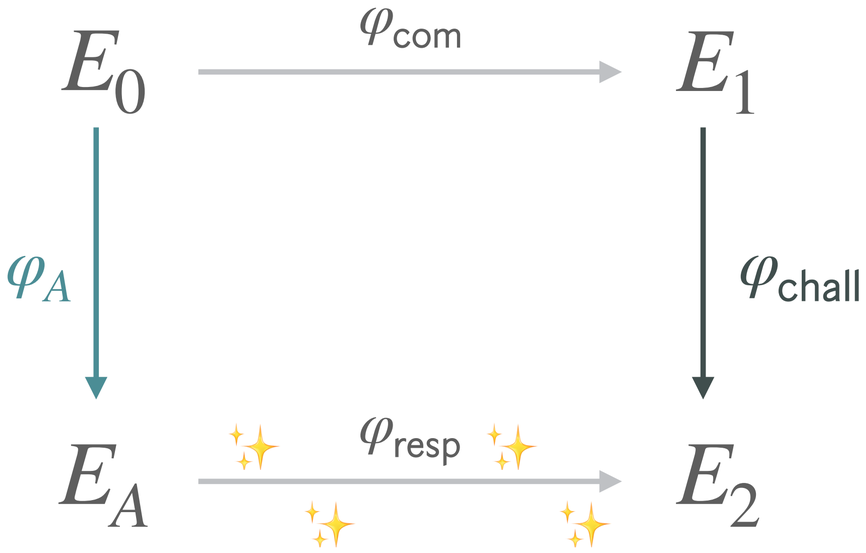
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

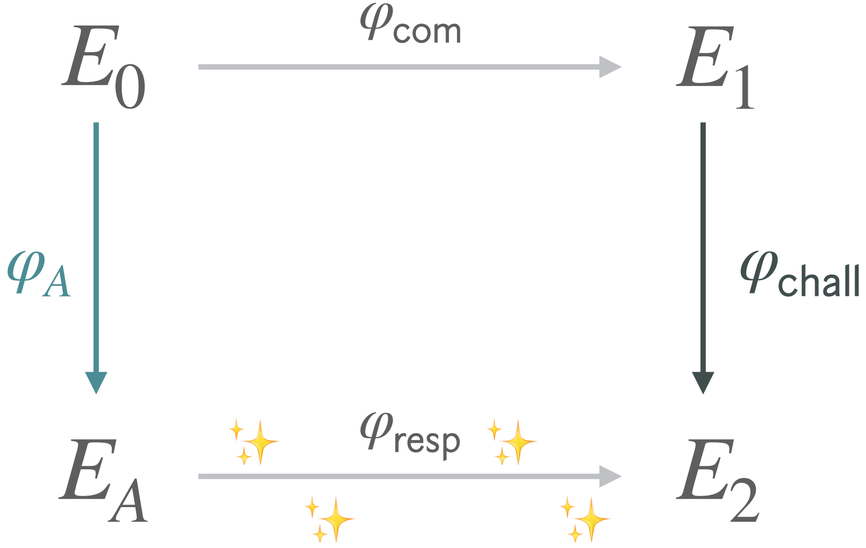
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✘ **signing is now even slower, using extension fields, takes literal seconds**

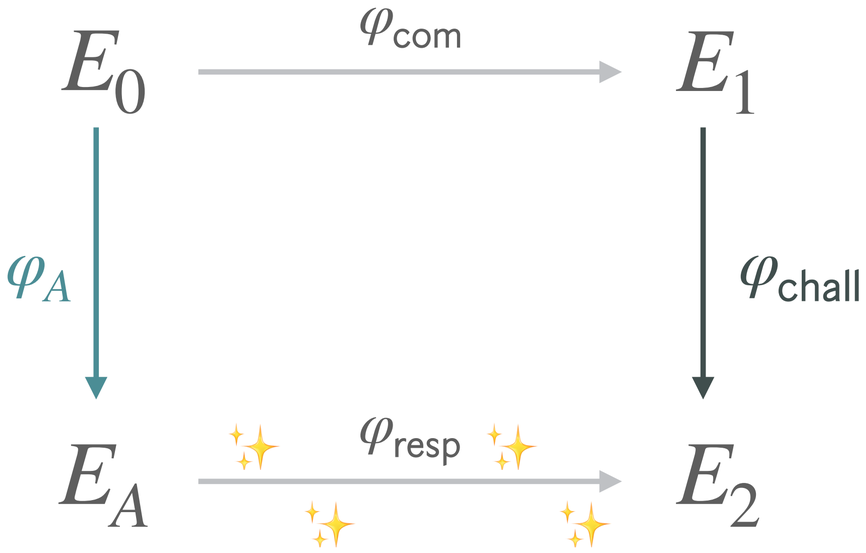
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✘ **signing is now even slower, using extension fields, takes literal seconds**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

3 Best Papers ASIACRYPT 2024?

Awarded Papers

Kongresssaal

Marc Joye and Gregor Leander

Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis

Speaker(s): Itai Dinur

(paper #326)

Show abstract ›

PART 4: 2D Future?

SQIsign2D-West: The Fast, the Small, and the Safer

Andrea Basso,Pierrick Dartois,Luca De Feo,Antonin Leroux,Luciano Maino,Giacomo Pope,Damien Robert, Benjamin Wesolowski

SQIsign2D-East

Kohei Nakagawa, Hiroshi Onuki

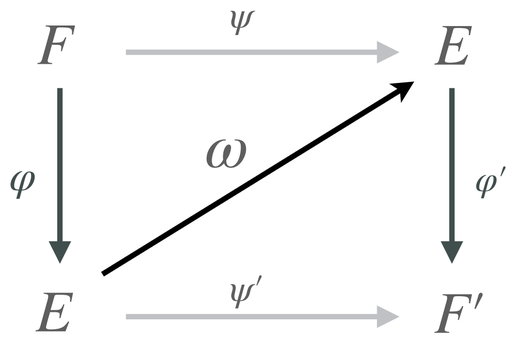
SQIPrime: a Dimension 2 Variant of SQIsignHD with Non-Smooth Challenge Isogenies

Max Duparc, Tako Boris Fouotsa

PART 4

2D Future

Nakagawa - Onuki trick (2023)



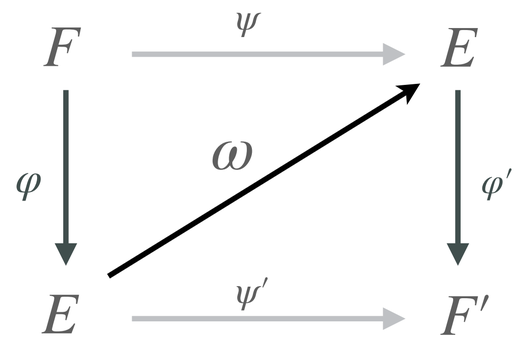
say we want to create such
a square, but we only have E
and some $\omega \in \mathrm{End}(E)$
of degree $q(2^a - q)$

we can find a suitable isogeny
$\varphi : F \to E$ using Kani!!!

PART 4

2D Future

Nakagawa - Onuki trick (2023)



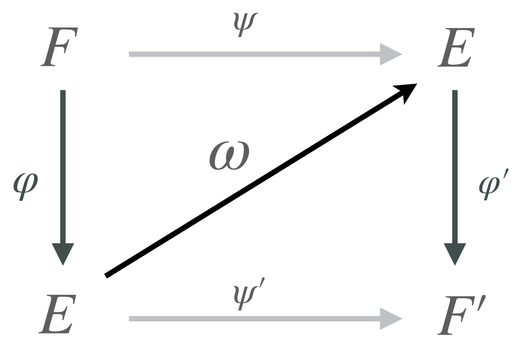
say we want to create such a square, but we only have E and some $\omega \in \mathrm{End}(E)$ of degree $q(2^a - q)$

we can find a suitable isogeny $\varphi : F \to E$ using Kani!!!

PART 4

2D Future

Nakagawa - Onuki trick (2023)



say we want to create such a square, but we only have E and some $\omega \in \mathrm{End}(E)$ of degree $q(2^a - q)$

we can find a suitable isogeny $\varphi : F \to E$ using Kani!!!

1

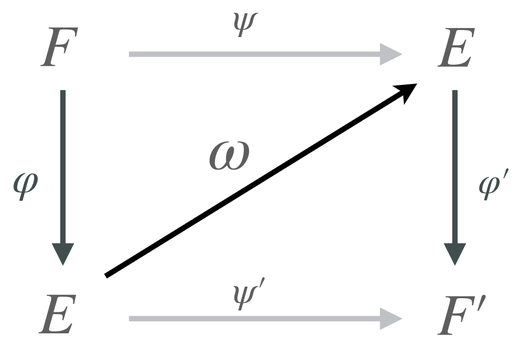
If the square above existed, then Kani's lemma should apply

should give 2D isogeny $\Phi : E \times E \to F \times F'$ of degree 2^a

PART 4

2D Future

Nakagawa - Onuki trick (2023)



say we want to create such a square, but we only have E and some $\omega \in \mathrm{End}(E)$ of degree $q(2^a - q)$

we can find a suitable isogeny $\varphi : F \to E$ using Kani!!!

1

If the square above existed, then Kani's lemma should apply

should give 2D isogeny $\Phi : E \times E \to F \times F'$ of degree 2^a

2

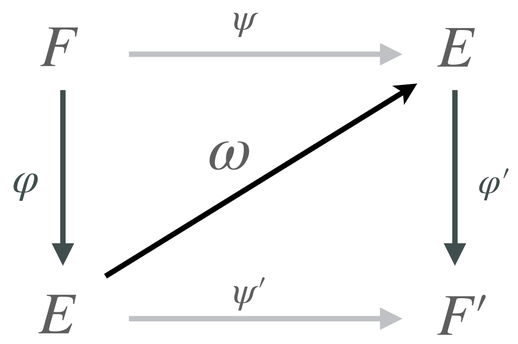
(ignoring some isogeny maths) then the kernel of Φ should be given by $[q]P, \omega(P)$ for $P \in E[2^a]$

But we know these!! We can compute 2D Φ using Kani

PART 4

2D Future

Nakagawa - Onuki trick (2023)



say we want to create such a square, but we only have E and some $\omega \in \mathrm{End}(E)$ of degree $q(2^a - q)$

we can find a suitable isogeny $\varphi : F \to E$ using Kani!!!

1

If the square above existed, then Kani's lemma should apply

should give 2D isogeny $\Phi : E \times E \to F \times F'$ of degree 2^a

2

(ignoring some isogeny maths) then the kernel of Φ should be given by $[q]P, \omega(P)$ for $P \in E[2^a]$

But we know these!! We can compute 2D Φ using Kani

3

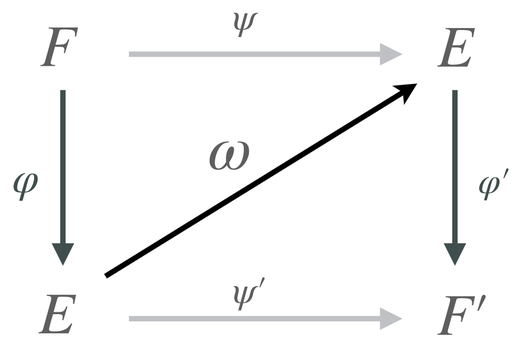
So we can also compute $\varphi : F \to E, \psi : F \to E$

that is, we can factor ω using Kani's lemma

PART 4

2D Future

Nakagawa - Onuki trick (2023)



say we want to create such a square, but we only have E and some $\omega \in \mathrm{End}(E)$ of degree $q(2^a - q)$

we can find a suitable isogeny $\varphi : F \to E$ using Kani!!!

1

If the square above existed, then Kani's lemma should apply

should give 2D isogeny $\Phi : E \times E \to F \times F'$ of degree 2^a

2

(ignoring some isogeny maths) then the kernel of Φ should be given by $[q]P, \omega(P)$ for $P \in E[2^a]$

But we know these!! We can compute 2D Φ using Kani

3

So we can also compute $\varphi : F \to E, \psi : F \to E$

that is, we can factor ω using Kani's lemma

Clapoti(s)

apply this trick to translate ideal I to suitable 2D isogenies

PART 4

2D Future

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

AprèsSQI

Signing will be slow... We push verification to the limits using extension fields.

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.

Going 2D

Simultaneously, three works adapted SQIsignHD to enable verification with **2D isogenies**

PART 4

2D Future

SQIsign2D

Don’t do “slow” translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don’t do “fast” translation of ideal into slow 4D/8D isogenies (SQIsignHD)

Do use the previous section to translate ideal into 2D isogenies

PART 4

2D Future

SQIsign2D

Don’t do “slow” translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don’t do “fast” translation of ideal into slow 4D/8D isogenies (SQIsignHD)

Do use the previous section to translate ideal into 2D isogenies

1. SQIsign2D-West

&

2. SQIsign2D-East

&

3. SQIPrime

PART 4

2D Future

- ✓ **faster primes!**
- ✓ **FASTER signing!**
- ✓ **THE BEST security!**
- ✓ **FAST verification!**

SQIsign2D

Don't do "slow" translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don't do "fast" translation of ideal into slow 4D/8D isogenies (SQIsignHD)

Do use the previous section to translate ideal into 2D isogenies

1. SQIsign2D-West
2. SQIsign2D-East
3. SQIPrime

&

&

PART 4

2D Future

- ✓ **faster primes!**
- ✓ **FASTER signing!**
- ✓ **THE BEST security!**
- ✓ **FAST verification!**

SQIsign2D

Don't do "slow" translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don't do "fast" translation of ideal into slow 4D/8D isogenies (SQIsignHD)

Do use the previous section to translate ideal into 2D isogenies

1. SQIsign2D-West **&**
2. SQIsign2D-East **&**
3. SQIPrime

concrete numbers

NIST SQIsign Level I		SQIsign2D-West Level I	
• **Public Key:**	64 bytes	• **Public Key:**	66 bytes
• **Signature :**	177 bytes	• **Signature :**	148 bytes
• **Signing:**	2,400 MCycles	• **Signing:**	160 MCycles
• **Verification:**	39 MCycles	• **Verification:**	9 MCycles

PART 4

2D Future

From here on: wishful thinking

More Best Papers??

Best Paper Session

Location: South Hall 3

Session Chairs: Diego F. Aranha, Marcel Medwed

PART 5: A 1D Miracle?

YouTube

Ideal-to-isogeny Algorithm using 2-dimensional Isogenies and its Application to SQIsign

Hiroshi Onuki, Kohei Nakagawa

Optimized Implementation of SQIsign Verification on Intel and M4

Anonymous

log(p) KLPT

Winner of next Field medal

PART 5

A 1D Miracle?

2020

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2021

2022

SQIsign2

A new algorithm to translate ideals to isogenies.

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

2023

AprèsSQI

Signing will be slow... We push verification to the limits using extension fields.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.

2024

More 1D?

Recent works seem to allow improved signing for Après-primes, *(and more...)*

Going 2D

Simultaneously, three works adapted SQIsignHD to enable verification with **2D isogenies**

PART 5

A 1D Miracle?

Remember this slide?

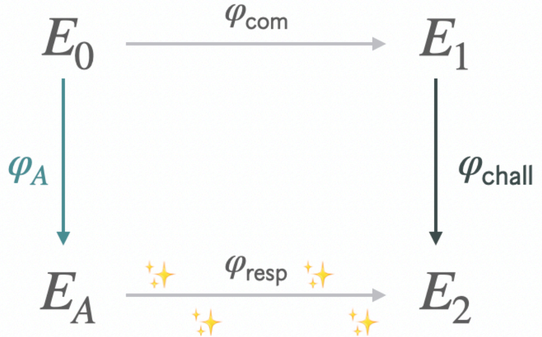
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1. instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2. slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✗ **signing is now even slower, using extension fields, takes literal seconds**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

Radboud University

[2024/778]: Hiroshi Onuki, Kohei Nakagawa *"Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign"*

PART 5
A 1D Miracle?

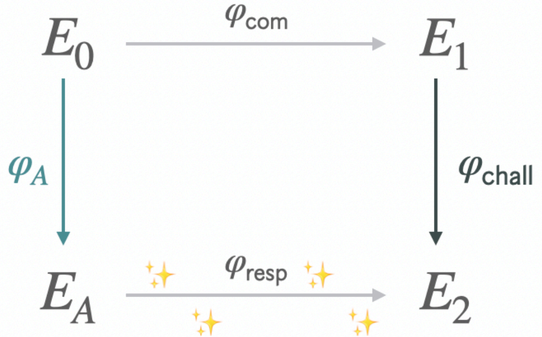
Remember this slide?

PART 3
New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✓ **signing now seems somewhat OK, better than NIST SQIsign, but not yet as fast as 2D-West,**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

Radboud University

1

2024/778 shows much more practical signing procedure for 1D using 2D-isogenies 🤯

Radboud University

[2024/778]: Hiroshi Onuki, Kohei Nakagawa *"Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign"*

PART 5
A 1D Miracle?

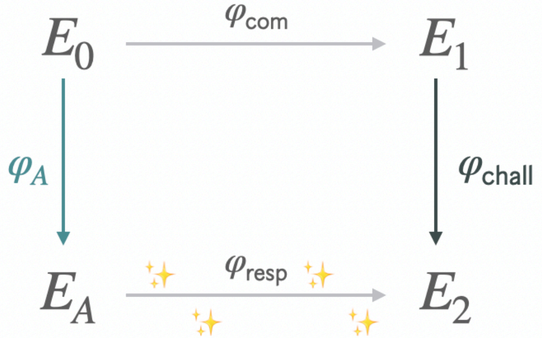
Remember this slide?

PART 3
New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✓ **signing now seems somewhat OK, better than NIST SQIsign, but not yet as fast as 2D-West,**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

Radboud University

1 2024/778 shows much more practical signing procedure for 1D using 2D-isogenies 🤯

2 Ongoing work shows highly-optimised verification for 1D verification “very likely” outperforms 2D verification

Radboud University

[2024/778]: Hiroshi Onuki, Kohei Nakagawa *“Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign”*

PART 5

A 1D Miracle?

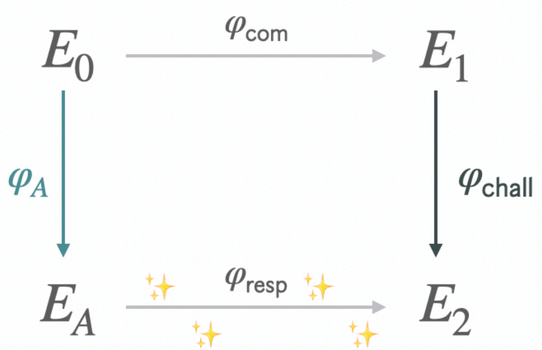
Remember this slide?

PART 3
New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✓ **signing now seems somewhat OK, better than NIST SQIsign, but not yet as fast as 2D-West,**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

Radboud University

1. 2024/778 shows much more practical signing procedure for 1D using 2D-isogenies 🤯

2. Ongoing work shows highly-optimised verification for 1D verification “very likely” outperforms 2D verification

3. However, we need a “miracle" in new techniques for 1D to get better signing times than SQIsign2D

[2024/778]: Hiroshi Onuki, Kohei Nakagawa *“Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign”*

CONCLUSION

2D SQIsign is the “way to go” for now!

1D SQIsign is not dead! However, requires a breakthrough to achieve similar results

Want best paper awards? Do SQIsign research.

BONUS PART: THE BEAST

From here on:
“this way madness lies”

PART 6

THE BEAST

Remember that I said verification is relatively easy?

PART 6

THE BEAST

Remember that I said verification is relatively easy?

1D SQIsign

Verification recomputes a 2^{1000} isogeny

$$\varphi_{\text{resp}} : E_A \to E_2$$

in a number of blocks

$$\varphi_i : E^{(i)} \to E^{(i+1)}$$

All of this is done over $\mathbb{F}_{p^2}$ and requires a few essential building blocks that we know for a long time now.

- isogeny-evaluation formulas
- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

1D SQIsign

Verification recomputes a 2^{1000} isogeny

$$\varphi_{\text{resp}} : E_A \to E_2$$

in a number of blocks

$$\varphi_i : E^{(i)} \to E^{(i+1)}$$

All of this is done over $\mathbb{F}_{p^2}$ and requires a few essential building blocks that we know for a long time now.

- isogeny-evaluation formulas
- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

2D SQIsign

Verification recomputes a 2^{128} isogeny

$$E_1 \times E_2 \to F_1 \times F_2$$

in a single block.

All of this is done over $\mathbb{F}_{p^2}$, and for such "short" 2D-isogenies, we essentially only need formulas to evaluate the isogeny.

These have recently been studied by Dartois, Maino, Pope, Robert using theta-models.

(If you ever heard of Richelot isogenies between hyperelliptic curves, they are essentially the same, but different...)

PART 6

THE BEAST

Remember that I said verification is relatively easy?

1D SQIsign

Verification recomputes a 2^{1000} isogeny

$$\varphi_{\text{resp}} : E_A \to E_2$$

in a number of blocks

$$\varphi_i : E^{(i)} \to E^{(i+1)}$$

All of this is done over $\mathbb{F}_{p^2}$ and requires a few essential building blocks that we know for a long time now.

- isogeny-evaluation formulas
- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

2D SQIsign

Verification recomputes a 2^{128} isogeny

$$E_1 \times E_2 \to F_1 \times F_2$$

in a single block.

All of this is done over $\mathbb{F}_{p^2}$, and for such "short" 2D-isogenies, we essentially only need formulas to evaluate the isogeny.

These have recently been studied by Dartois, Maino, Pope, Robert using theta-models.

(If you ever heard of Richelot isogenies between hyperelliptic curves, they are essentially the same, but different...)

however

1

Scholten has shown in 2003 that each elliptic curve over $\mathbb{F}_{p^2}$ has a "friend" in dimension 2 over $\mathbb{F}_p$, using Weil restriction.

2

Costello has shown in 2018 that the same holds for 2-isogenies between curves! They become 2D-isogenies.

PART 6

THE BEAST

Remember that I said verification is relatively easy?

1D SQIsign

Verification recomputes a 2^{1000} isogeny

$$\varphi_{\text{resp}} : E_A \to E_2$$

in a number of blocks

$$\varphi_i : E^{(i)} \to E^{(i+1)}$$

All of this is done over $\mathbb{F}_{p^2}$ and requires a few essential building blocks that we know for a long time now.

- isogeny-evaluation formulas
- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

2D SQIsign

Verification recomputes a 2^{128} isogeny

$$E_1 \times E_2 \to F_1 \times F_2$$

in a single block.

All of this is done over $\mathbb{F}_{p^2}$, and for such "short" 2D-isogenies, we essentially only need formulas to evaluate the isogeny.

These have recently been studied by Dartois, Maino, Pope, Robert using theta-models.

(If you ever heard of Richelot isogenies between hyperelliptic curves, they are essentially the same, but different…)

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D?

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? **A: No.**

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? **A: No.**

Q: Is it much more difficult?

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? **A: No.**

Q: Is it much more difficult? **A: Yes.**

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? **A: No.**

Q: Is it much more difficult? **A: Yes.**

Q: Does it develop general techniques to do 2D isogeny-based cryptography & give a good overview of the use of Kummer surfaces in cryptography?

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? **A: No.**

Q: Is it much more difficult? **A: Yes.**

Q: Does it develop general techniques to do 2D isogeny-based cryptography & give a good overview of the use of Kummer surfaces in cryptography?

A: *YES!!!*

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

THANK YOU!

ANY QUESTIONS?

Krijn Reijnders
krijn@cs.ru.nl
www.krijnreijnders.com