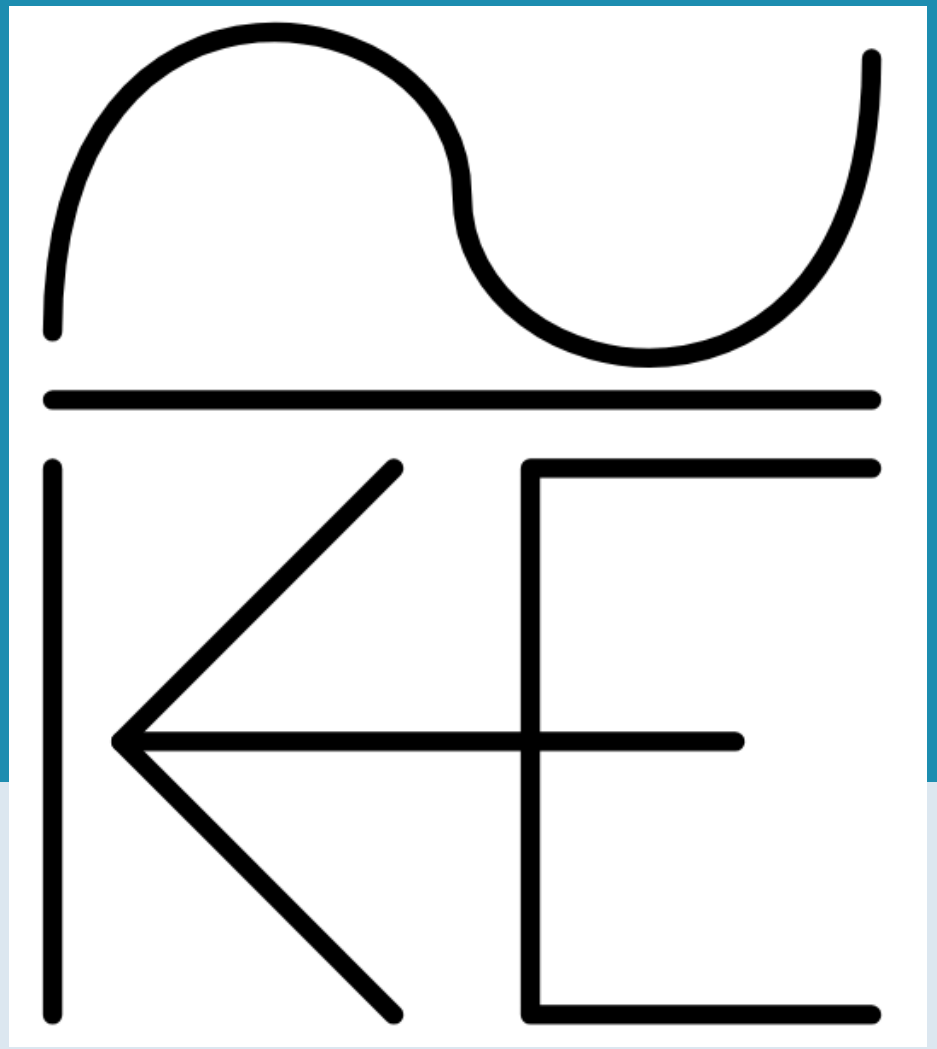
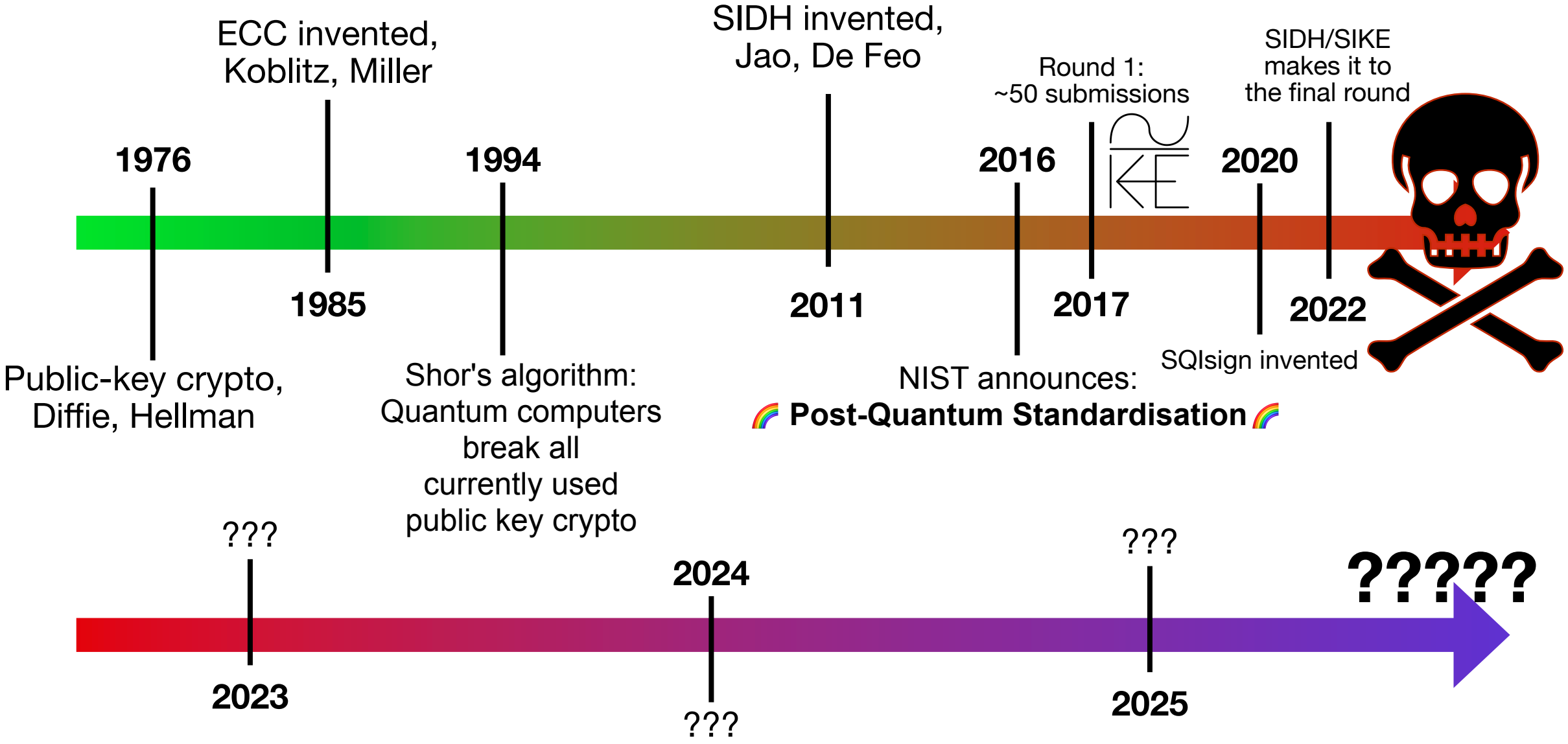
KU LEUVEN

What went ~~wrong~~ right with SIDH/SIKE?



Jonathan Komada Eriksen


ECC invented,
Koblitz, Miller
SIDH invented,
Jao, De Feo
Round 1:
~50 submissions
SIDH/SIKE
makes it to
the final round
1976
1985
1994
2011
2016
2017
2020
2022
Public-key crypto,
Diffie, Hellman
Shor's algorithm:
Quantum computers
break all
currently used
public key crypto
NIST announces:
Post-Quantum Standardisation
SQIsign invented
???
2023
2024
???
???
2025
?????

KU LEUVEN


SIDH invented,
ECC invented
SIDH broken
Jao, De Feo
Koblitz, Miller
~50 submissions
the final round
1985
1994
2016
2017
2020
2022
Shor's algorithm:
Public-key crypto
Quantum computers
Diffie, Hellman
break all
currently used
public key crypto
Post-Quantum Standards

KU LEUVEN

0

~250

Study of elliptic curves, Diophantus

1349

SIDH invented, broken

ECC invented

Jao, De Feo

Koblitz, Miller

~50 submissions

the final round

19

20

2017

2022

Shor's algorithm: Quantum computers break all currently used public key crypto

Public-key crypto: Diffie, Hellman

Post-Quantum Standards

0

~250

1349

2017

2022

Study of elliptic curves, Diophantus

Public-key crypto, Diffie, Hellman

Shor's algorithm: Quantum computers break all currently used public key crypto

SIDH invented, broken

ECC invented

Jao, De Feo

Koblitz, Miller

~50 submissions

the final round

NIST announces: **Post-Quantum Standards**

What squares are one more than a cube?*

*unsure if this specific example actually occured

0

~250

1349

2017

2022

Study of elliptic curves, Diophantus

What squares are one more than a cube?*

Rational points on the curve

$$E : y^2 = x^3 + 1$$

Public-key crypto, Diffie, Helman

Shor's algorithm: break all currently used public key crypto

*unsure if this specific example actually occured

Elliptic curves

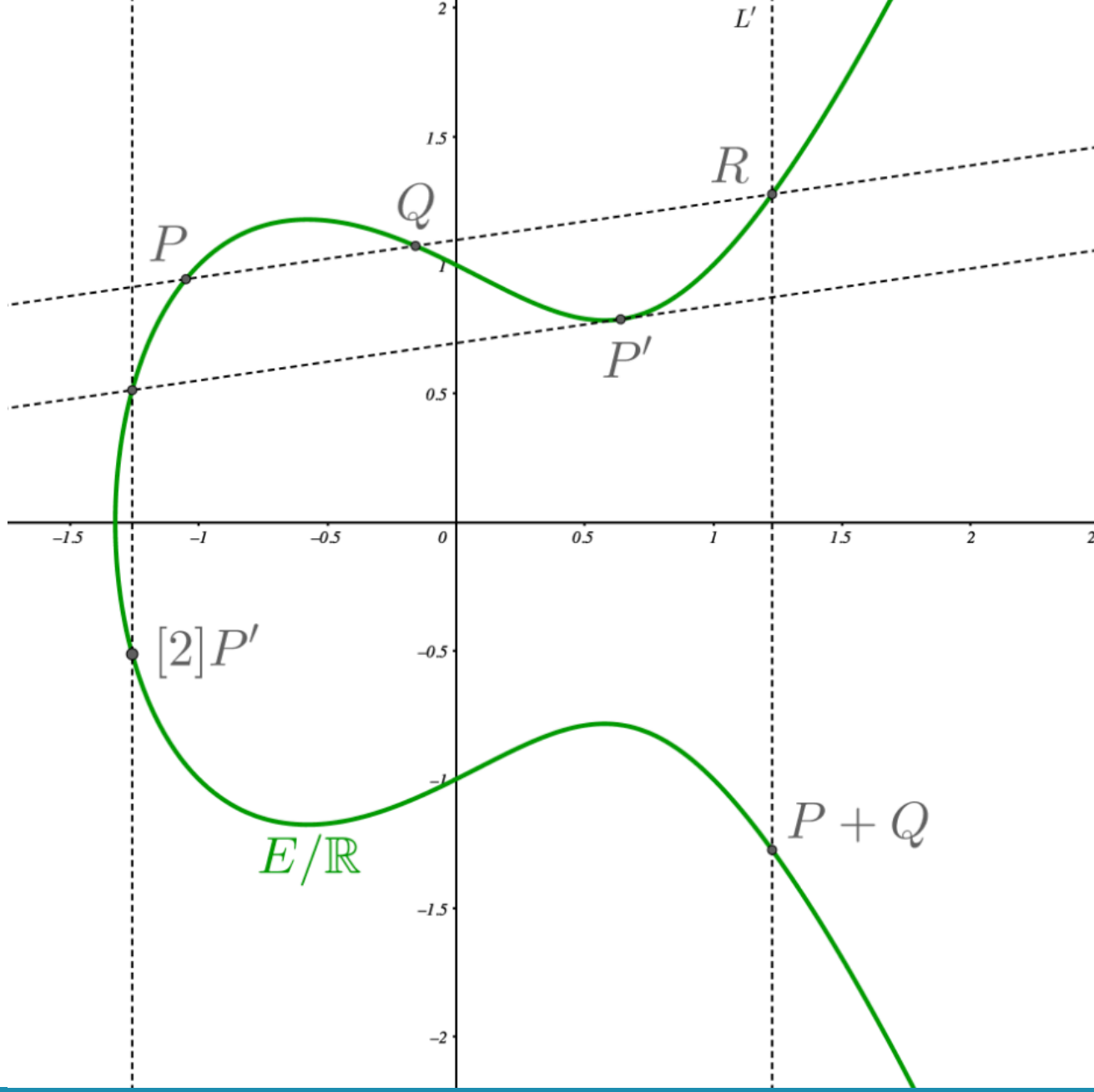
$$E : y^2 = x^3 + ax + b$$

Given $P, Q \in E$, can meaningfully define

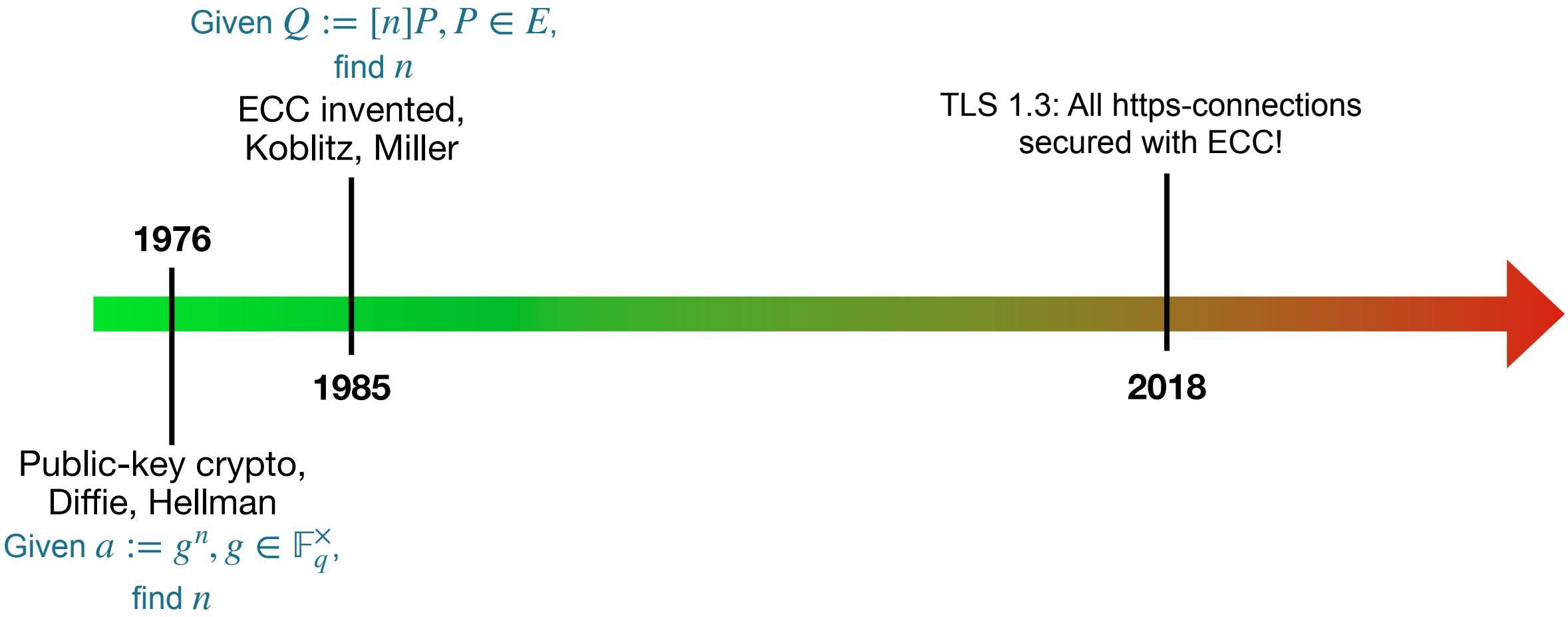
$$P + Q \in E$$

and

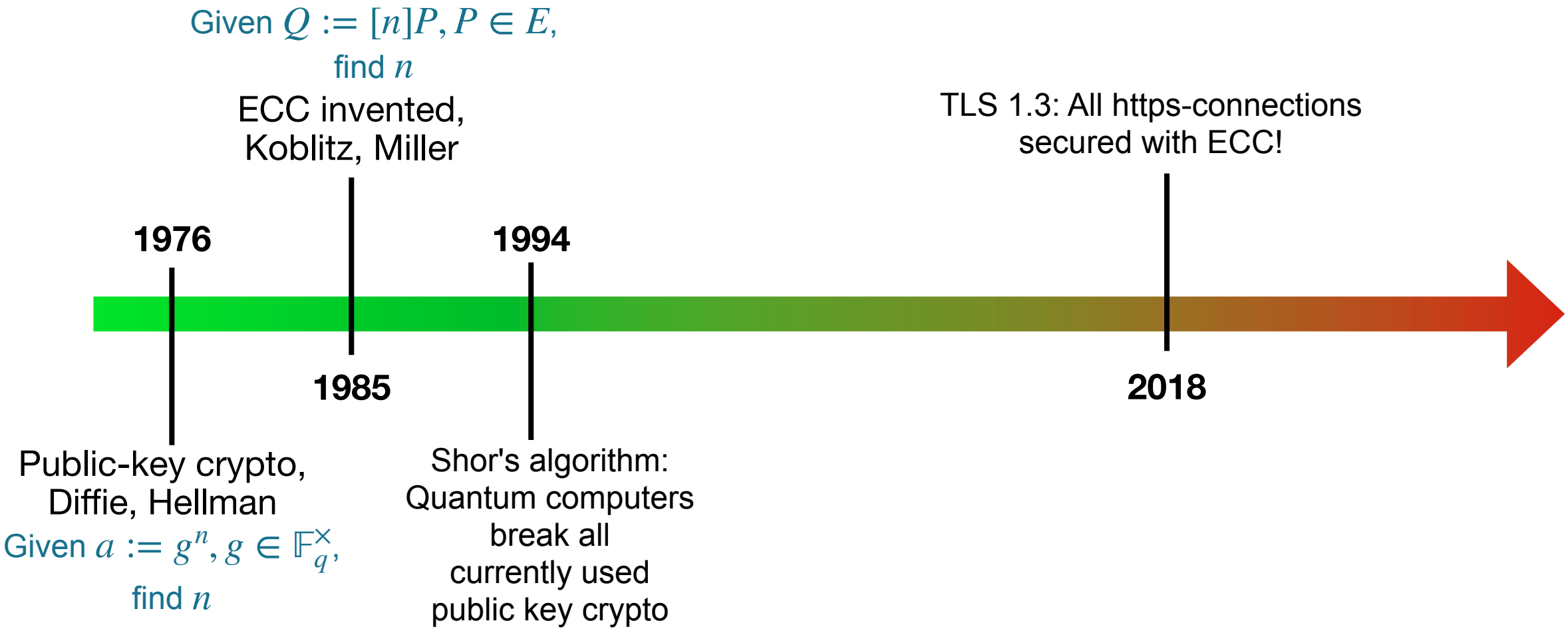
$$[n]P \in E$$



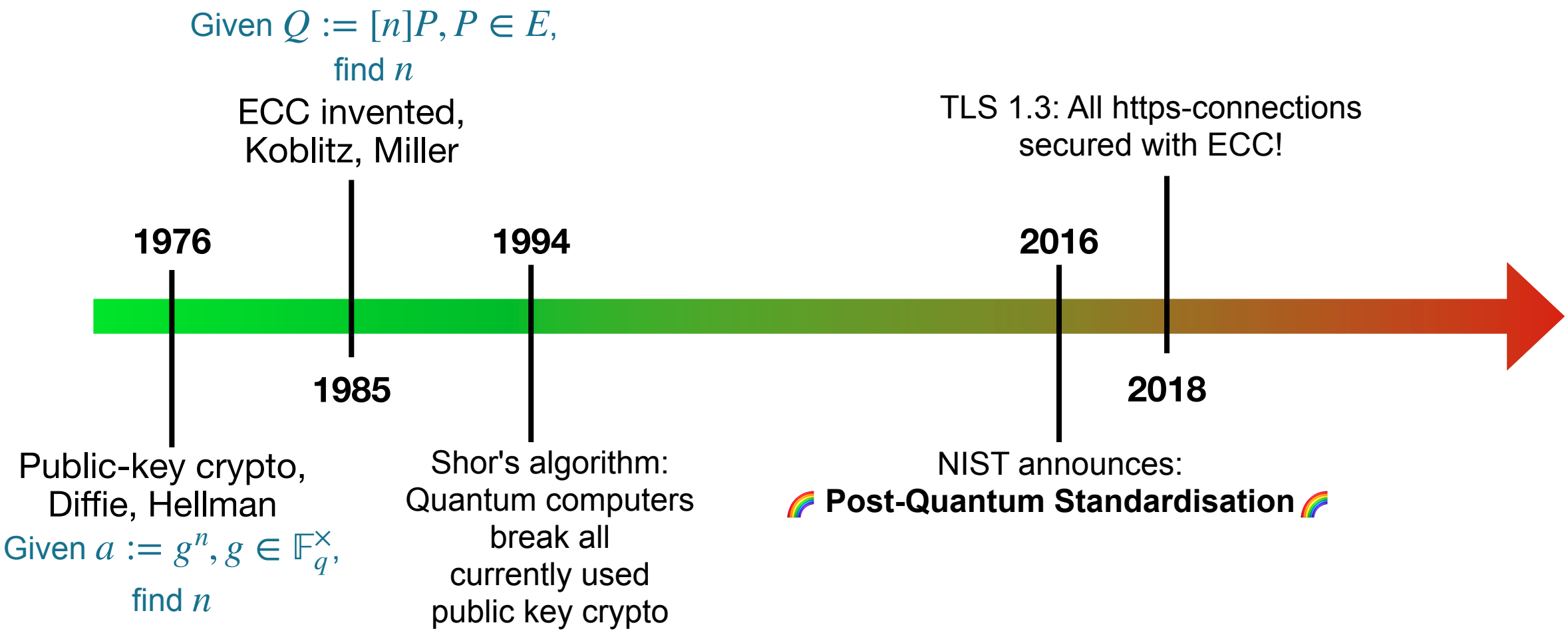
Elliptic Curve Cryptography



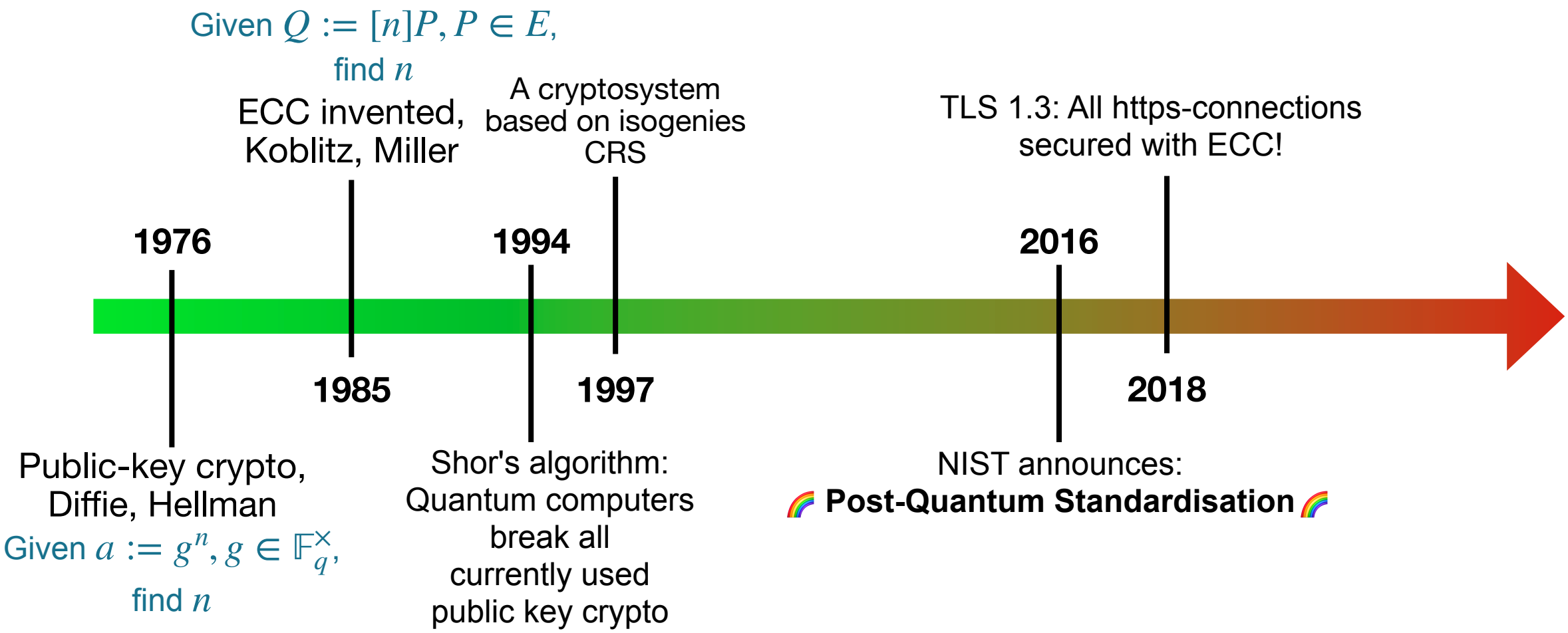
Elliptic Curve Cryptography



Elliptic Curve Cryptography



Elliptic Curve Cryptography



One step further - maps between curves

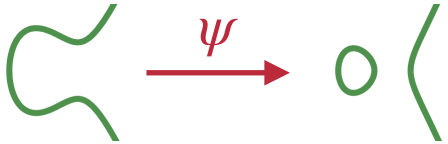
Alice

secret:

public:

Bob

secret:



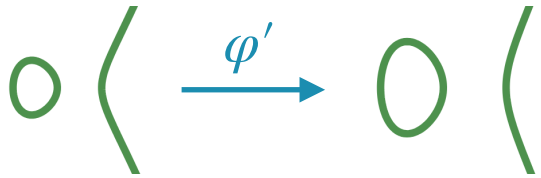
public:

One step further - maps between curves

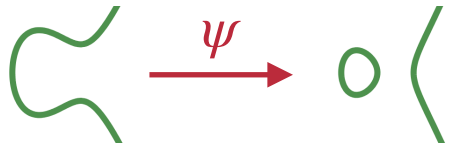
"isogenies"

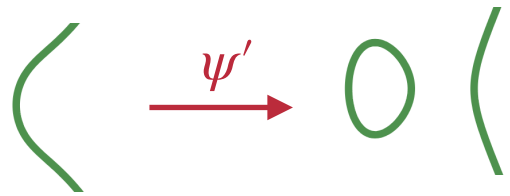
Alice

secret: 



Bob

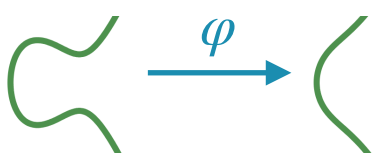
secret: 



One step further - maps between curves

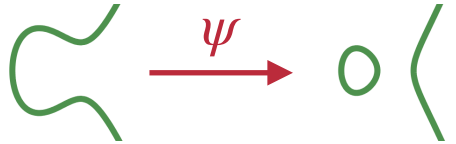
Alice

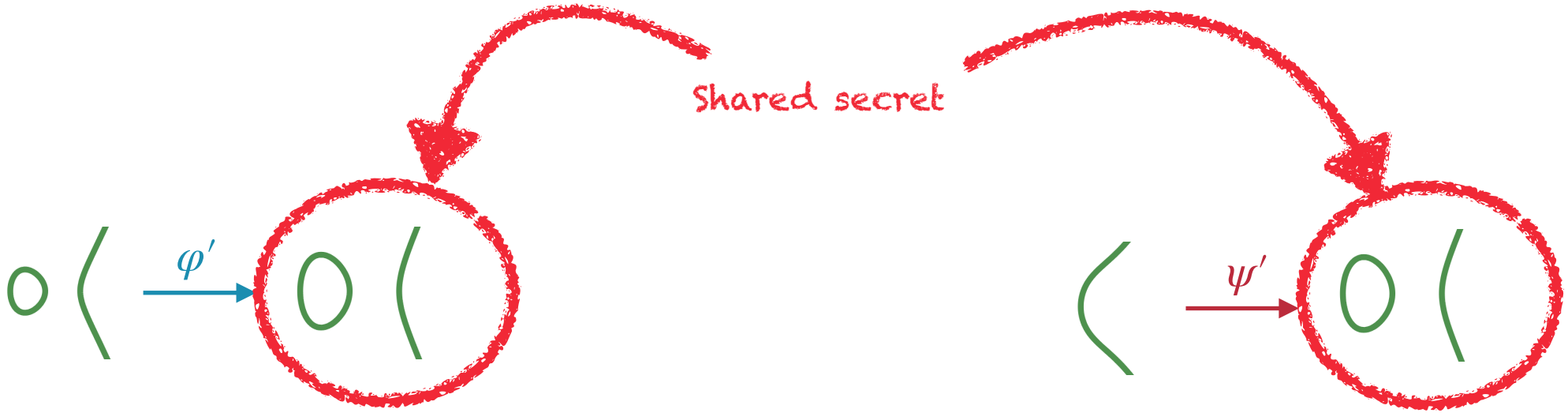
secret:



Bob

secret:





KU LEUVEN

SIDH/SIKE

Alice

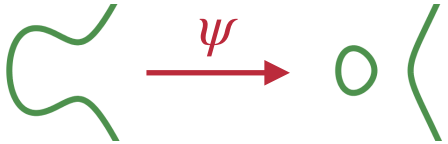
secret:

public:

$\varphi(P_1), \varphi(Q_1)$

Bob

secret:



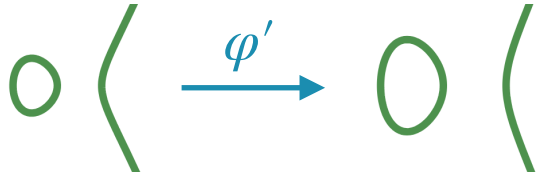
public:

$\psi(P_2), \psi(Q_2)$

SIDH/SIKE

Alice

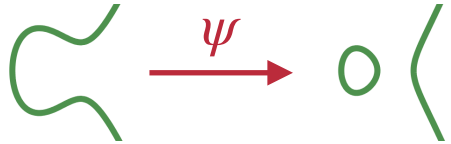
secret:

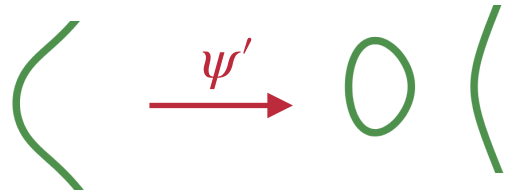


$\psi(P_2), \psi(Q_2)$

Bob

secret:

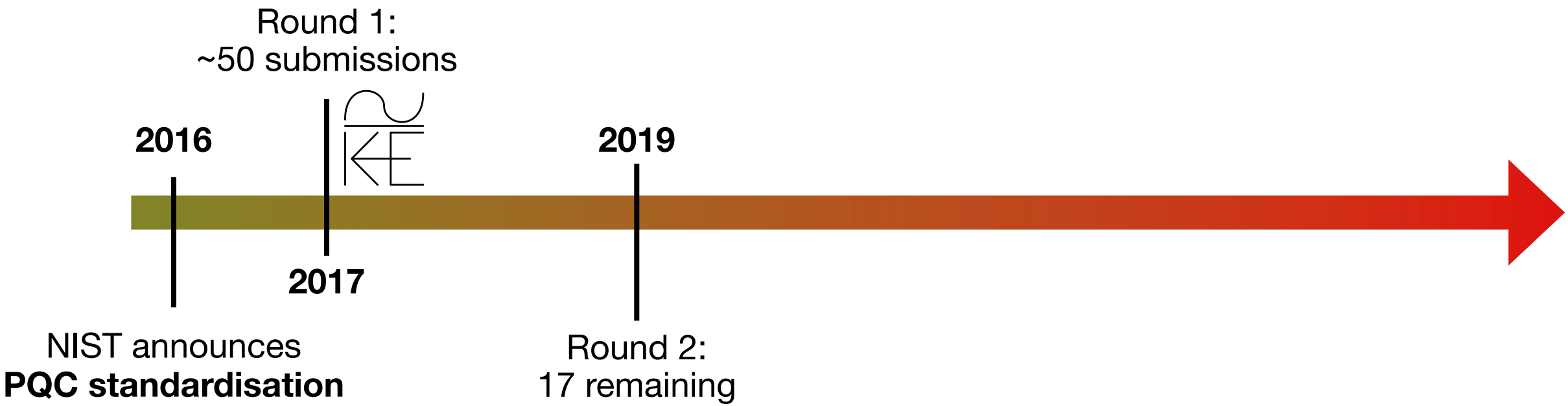




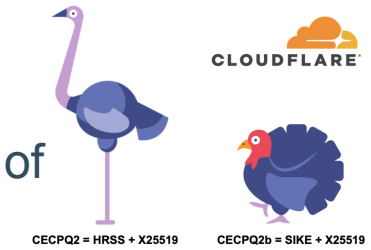
$\varphi(P_1), \varphi(Q_1)$

PQC standardisation

PQC standardisation



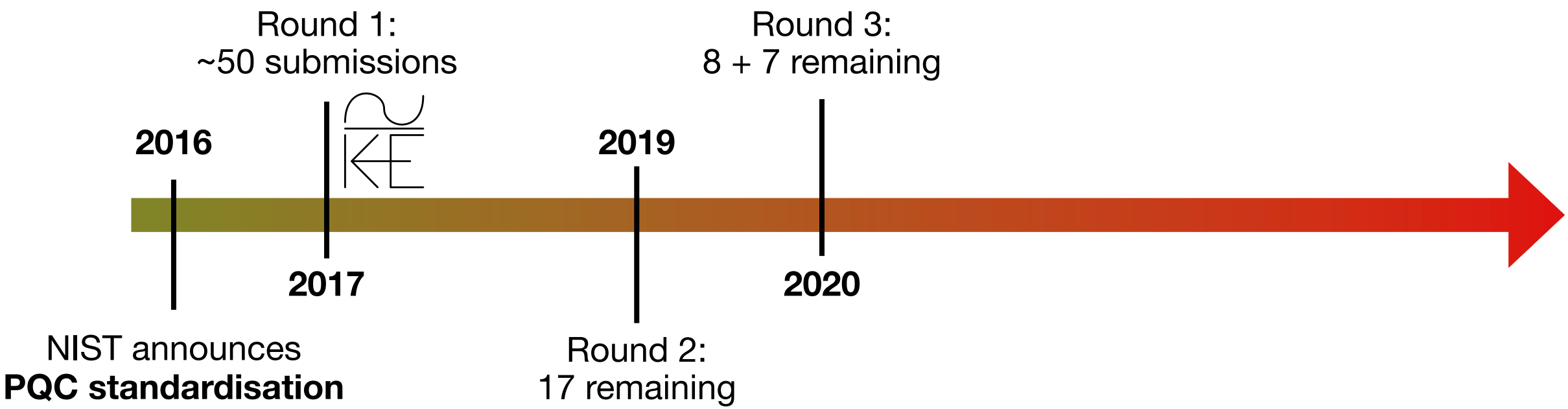
~10 million TLS connections of SIKE tested by Cloudflare*



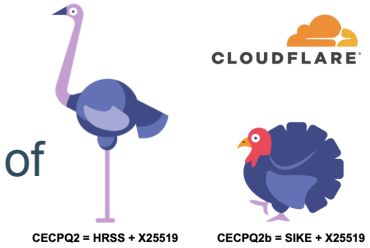
https://blog.cloudflare.com/the-tls-post-quantum-experiment/

KU LEUVEN

PQC standardisation



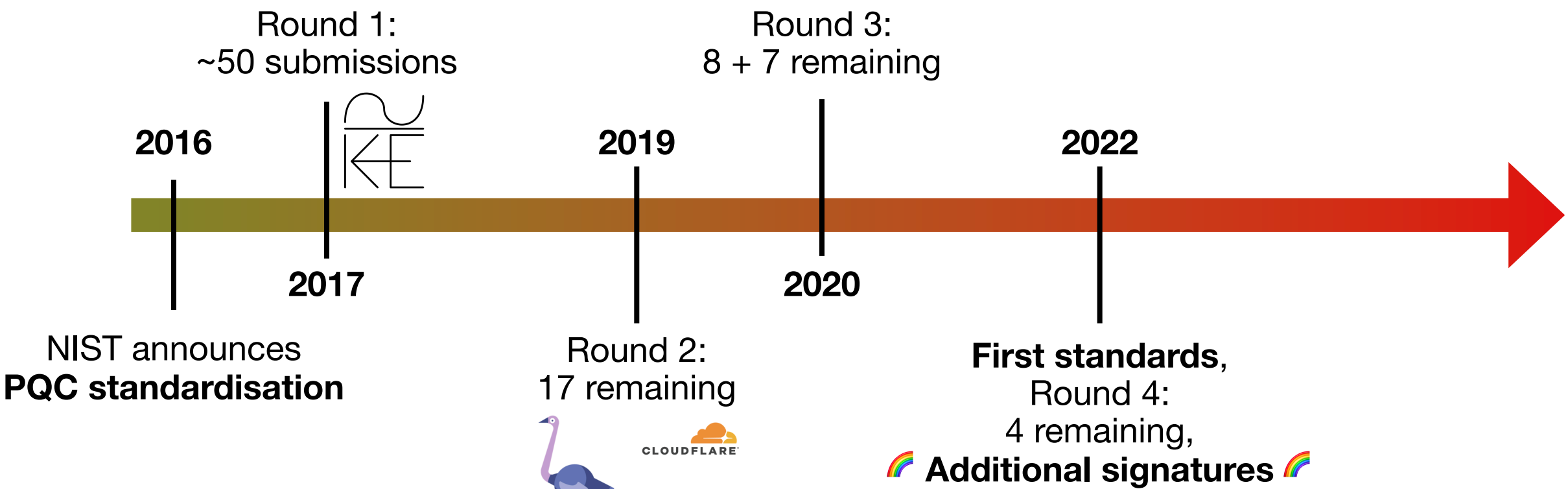
~10 million TLS connections of SIKE tested by Cloudflare*



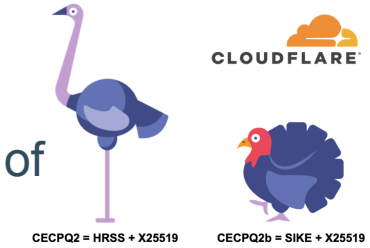
https://blog.cloudflare.com/the-tls-post-quantum-experiment/

KU LEUVEN

PQC standardisation

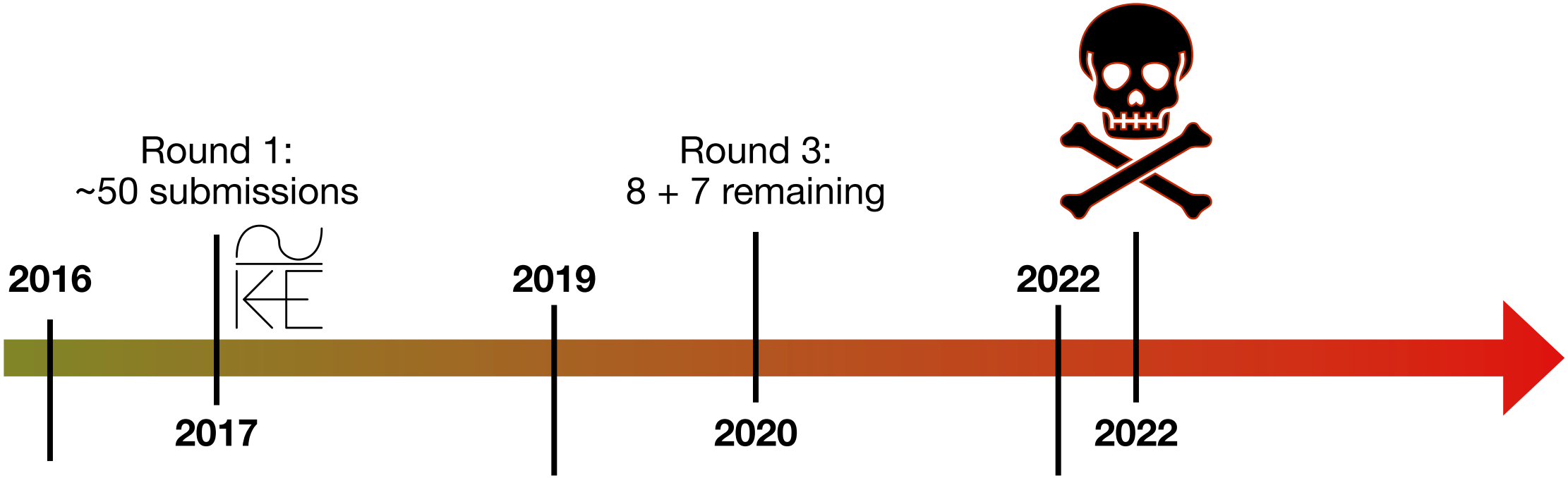


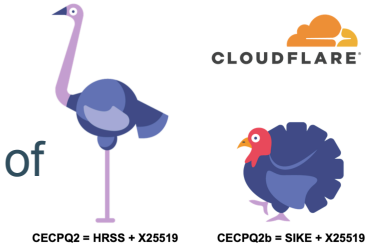
~10 million TLS connections of SIKE tested by Cloudflare*



https://blog.cloudflare.com/the-tls-post-quantum-experiment/

PQC standardisation





~10 million TLS connections of SIKE tested by Cloudflare*

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

PQC standardisation

2016

2017

Round 1:
~50 submissions

NIST announces
PQC standardisation

Round 2:
17 remaining

CLOUDFLARE

First standards,
Round 4:
4 remaining,
🌈 **Additional signatures** 🌈

~10 million TLS connections of SIKE tested by Cloudflare*

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

KU LEUVEN

PQC standardisation

Round 1:
~50 submissions

2016

2017

NIST announces
PQC standardisation

dards,
4:
ning,
gnatures 🌈

~10 million TLS connections of SIKE tested by Cloudflare*

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

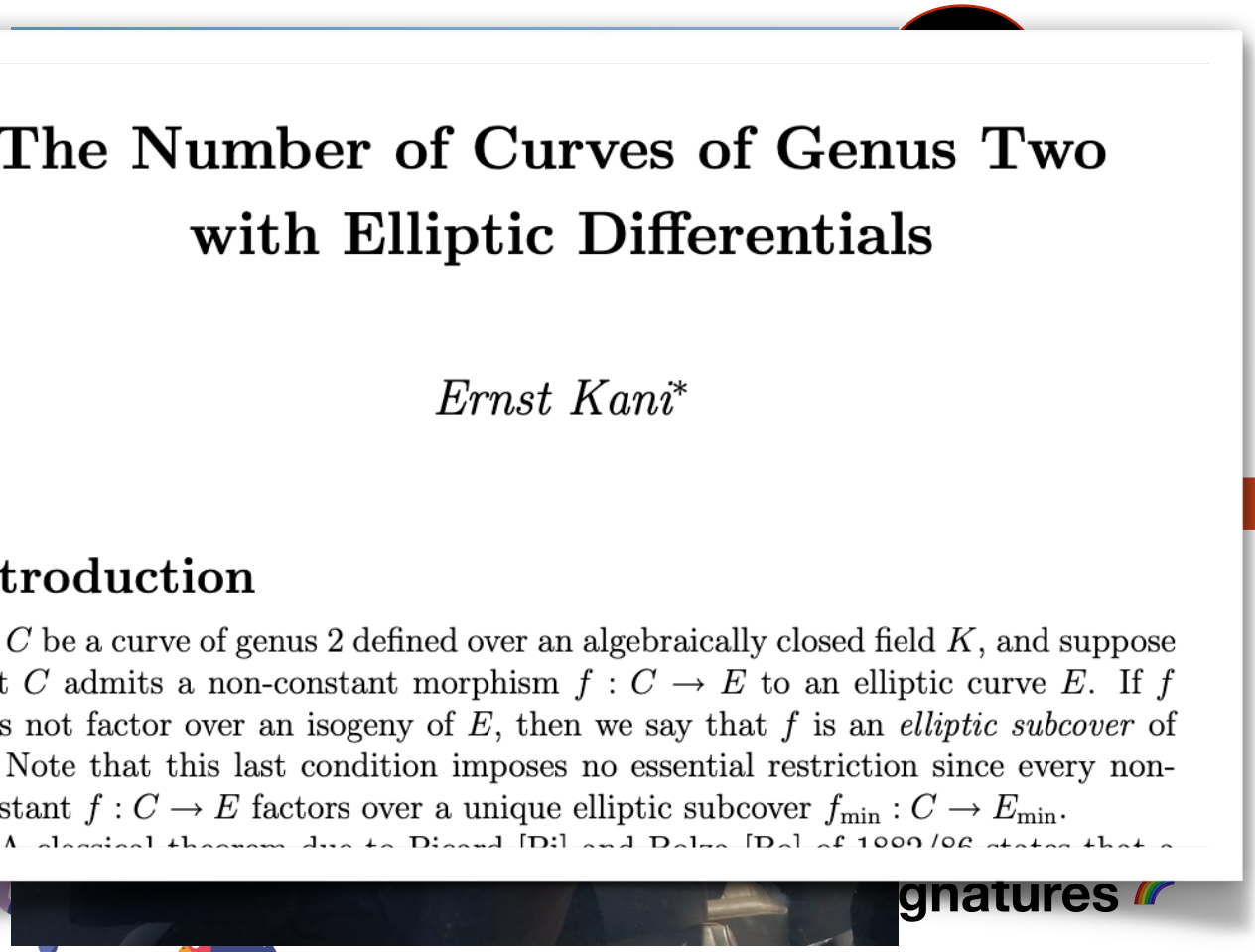
PQC standardisation

Round 1:
~50 submissions

2016

2017

NIST announces
PQC standardisation



The Number of Curves of Genus Two with Elliptic Differentials

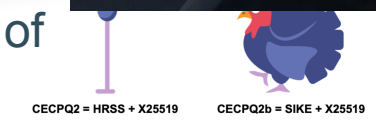
*Ernst Kani**

Introduction

Let C be a curve of genus 2 defined over an algebraically closed field K, and suppose that C admits a non-constant morphism $f : C \to E$ to an elliptic curve E. If f does not factor over an isogeny of E, then we say that f is an *elliptic subcover* of C. Note that this last condition imposes no essential restriction since every non-constant $f : C \to E$ factors over a unique elliptic subcover $f_{\min} : C \to E_{\min}$.

gnatures

~10 million TLS connections of SIKE tested by Cloudflare*



https://blog.cloudflare.com/the-tls-post-quantum-experiment/

KU LEUVEN

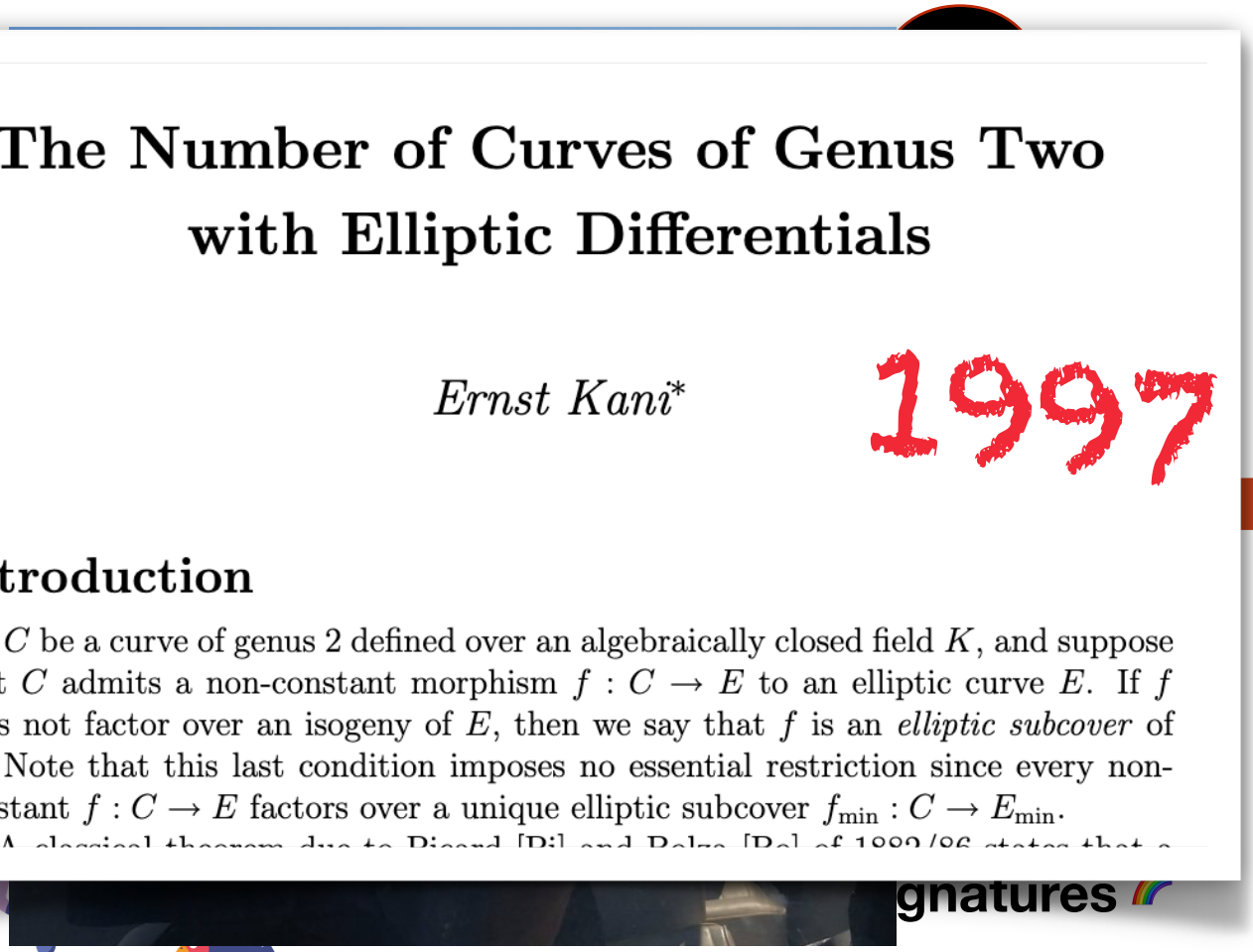
PQC standardisation

Round 1:
~50 submissions

2016

2017

NIST announces
PQC standardisation



~10 million TLS connections of
SIKE tested by Cloudflare*

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

KU LEUVEN

Abelian varieties

Given $P, Q \in E^A$, can meaningfully define

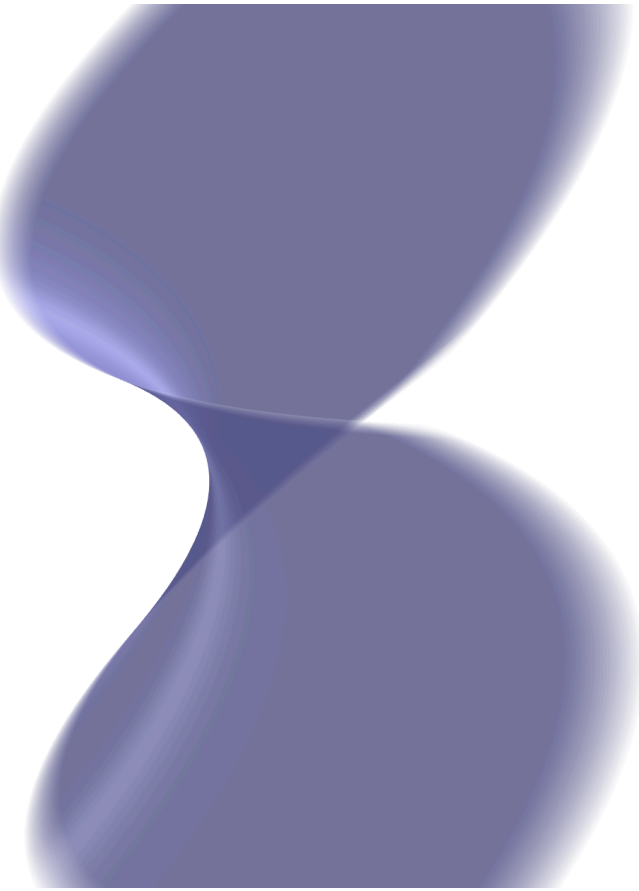
$$P + Q \in E^A$$

and

$$[n]P \in E^A$$

Def: Abelian Variety

$$\begin{aligned} A := V(\langle & -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1, \\ & -x_3x_4x_6 + x_1x_6^2 + x_1, \\ & -x_3x_5x_6 + x_2x_6^2 + x_2, \\ & -x_1x_2x_4 + x_2^2x_5 + x_3, \\ & -x_1x_2x_7 + x_2^2x_8 + x_6, \\ & -x_4^2x_6 + x_1x_6x_7 + x_1^2, \\ & -x_4x_5x_6 + x_2x_6x_7 + x_1x_2, \\ & -x_5^2x_6 + x_2x_6x_8 + x_2^2, \\ & -x_2x_4^2 + x_2x_5^2 + x_3^2, \\ & -x_2x_4x_7 + x_2x_5x_8 + x_3x_6, \\ & -x_1x_3 + x_4, \\ & -x_2x_3 + x_5, \\ & -x_2x_7^2 + x_2x_8^2 + x_6^2, \\ & -x_1x_6 + x_7, \\ & -x_2x_6 + x_8, \\ & x_1^3 - x_4^2x_7 + x_1x_7^2, \\ & x_1^2x_2 - x_4x_5x_7 + x_2x_7^2, \\ & x_1x_2^2 - x_5^2x_7 + x_2x_7x_8, \\ & -x_2x_4 + x_1x_5, \\ & -x_2x_7 + x_1x_8, \\ & x_2^3 - x_5^2x_8 + x_2x_8^2, \\ & x_3^3 - x_4^2x_5 + x_5^3, \\ & x_3^2x_6 - x_4x_5x_7 + x_5^2x_8, \\ & x_3x_6^2 - x_5x_7^2 + x_5x_8^2, \\ & -x_4x_6 + x_3x_7, \\ & -x_5x_6 + x_3x_8, \\ & -x_5x_7 + x_4x_8, \\ & x_6^3 - x_7^2x_8 + x_8^3\rangle) \end{aligned}$$



Abelian varieties

Given $P, Q \in E$, can meaningfully define

$$P + Q \in E$$

and

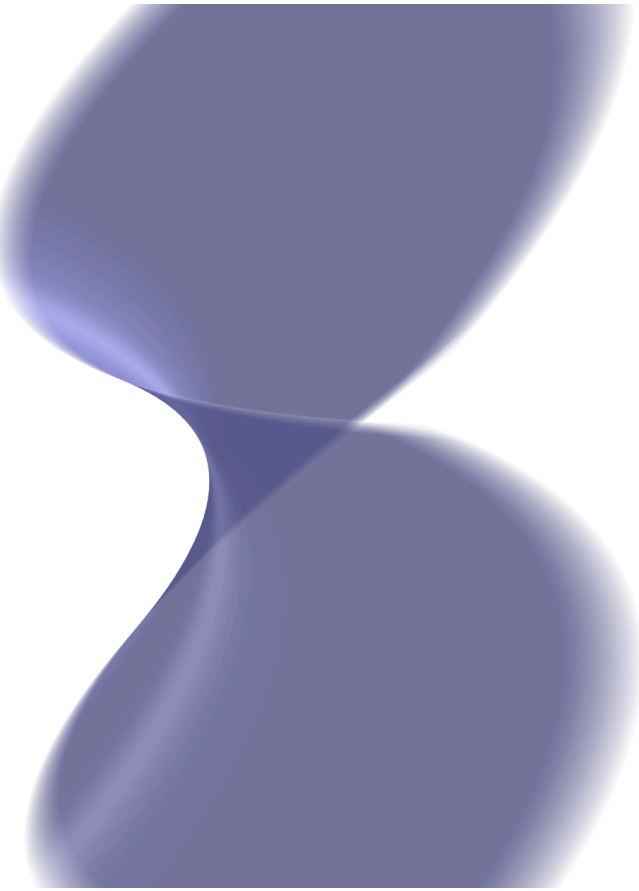
$$[n]P \in E$$

Def: Abelian Variety

Example: $P = (7,8,5,2,7,5,2,7), Q = (1,5,9,9,1,8,8,7)$,
gives $P + Q = (0,10,3,0,8,10,0,1)$

Complicated rational expression

$$\begin{aligned}
A := V(\langle & -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1, \\
& -x_3x_4x_6 + x_1x_6^2 + x_1, \\
& -x_3x_5x_6 + x_2x_6^2 + x_2, \\
& -x_1x_2x_4 + x_2^2x_5 + x_3, \\
& -x_1x_2x_7 + x_2^2x_8 + x_6, \\
& -x_4^2x_6 + x_1x_6x_7 + x_1^2, \\
& -x_4x_5x_6 + x_2x_6x_7 + x_1x_2, \\
& -x_5^2x_6 + x_2x_6x_8 + x_2^2, \\
& -x_2x_4^2 + x_2x_5^2 + x_3^2, \\
& -x_2x_4x_7 + x_2x_5x_8 + x_3x_6, \\
& -x_1x_3 + x_4, \\
& -x_2x_3 + x_5, \\
& -x_2x_7^2 + x_2x_8^2 + x_6^2, \\
& -x_1x_6 + x_7, \\
& -x_2x_6 + x_8, \\
& x_1^3 - x_4^2x_7 + x_1x_7^2, \\
& x_1^2x_2 - x_4x_5x_7 + x_2x_7^2, \\
& x_1x_2^2 - x_5^2x_7 + x_2x_7x_8, \\
& -x_2x_4 + x_1x_5, \\
& -x_2x_7 + x_1x_8, \\
& x_2^3 - x_5^2x_8 + x_2x_8^2, \\
& x_3^3 - x_4^2x_5 + x_5^3, \\
& x_3^2x_6 - x_4x_5x_7 + x_5^2x_8, \\
& x_3x_6^2 - x_5x_7^2 + x_5x_8^2, \\
& -x_4x_6 + x_3x_7, \\
& -x_5x_6 + x_3x_8, \\
& -x_5x_7 + x_4x_8, \\
& x_6^3 - x_7^2x_8 + x_8^3\rangle)
\end{aligned}$$

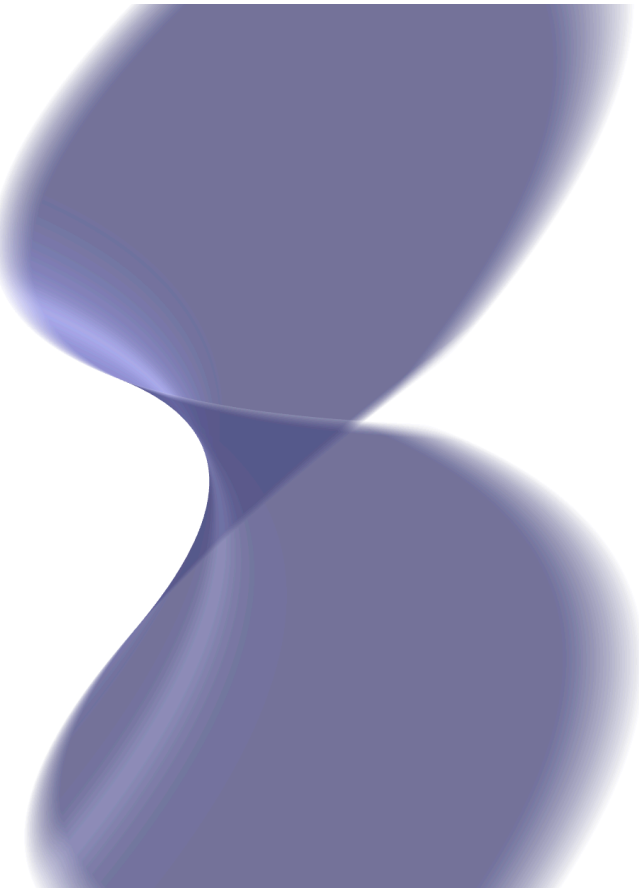


A bit of details!

$$A \simeq E_0 \times E_1, \text{ where}$$
$$E_0 : y^2 = x^3 + x, E_1 : y^2 = x^3 + 1$$

So points $X \in A$ can be thought of as pairs $X = (P_0, P_1)$, where $P_i \in E_i$

$$\begin{aligned}
A := V(\langle & -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1, \\
& -x_3x_4x_6 + x_1x_6^2 + x_1, \\
& -x_3x_5x_6 + x_2x_6^2 + x_2, \\
& -x_1x_2x_4 + x_2^2x_5 + x_3, \\
& -x_1x_2x_7 + x_2^2x_8 + x_6, \\
& -x_4^2x_6 + x_1x_6x_7 + x_1^2, \\
& -x_4x_5x_6 + x_2x_6x_7 + x_1x_2, \\
& -x_5^2x_6 + x_2x_6x_8 + x_2^2, \\
& -x_2x_4^2 + x_2x_5^2 + x_3^2, \\
& -x_2x_4x_7 + x_2x_5x_8 + x_3x_6, \\
& -x_1x_3 + x_4, \\
& -x_2x_3 + x_5, \\
& -x_2x_7^2 + x_2x_8^2 + x_6^2, \\
& -x_1x_6 + x_7, \\
& -x_2x_6 + x_8, \\
& x_1^3 - x_4^2x_7 + x_1x_7^2, \\
& x_1^2x_2 - x_4x_5x_7 + x_2x_7^2, \\
& x_1x_2^2 - x_5^2x_7 + x_2x_7x_8, \\
& -x_2x_4 + x_1x_5, \\
& -x_2x_7 + x_1x_8, \\
& x_2^3 - x_5^2x_8 + x_2x_8^2, \\
& x_3^3 - x_4^2x_5 + x_5^3, \\
& x_3^2x_6 - x_4x_5x_7 + x_5^2x_8, \\
& x_3x_6^2 - x_5x_7^2 + x_5x_8^2, \\
& -x_4x_6 + x_3x_7, \\
& -x_5x_6 + x_3x_8, \\
& -x_5x_7 + x_4x_8, \\
& x_6^3 - x_7^2x_8 + x_8^3\rangle)
\end{aligned}$$



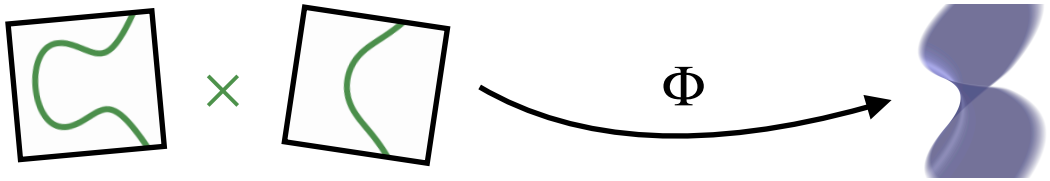
A bit of details!

$$A \simeq E_0 \times E_1, \text{ where}$$
$$E_0 : y^2 = x^3 + x,\ E_1 : y^2 = x^3 + 1$$

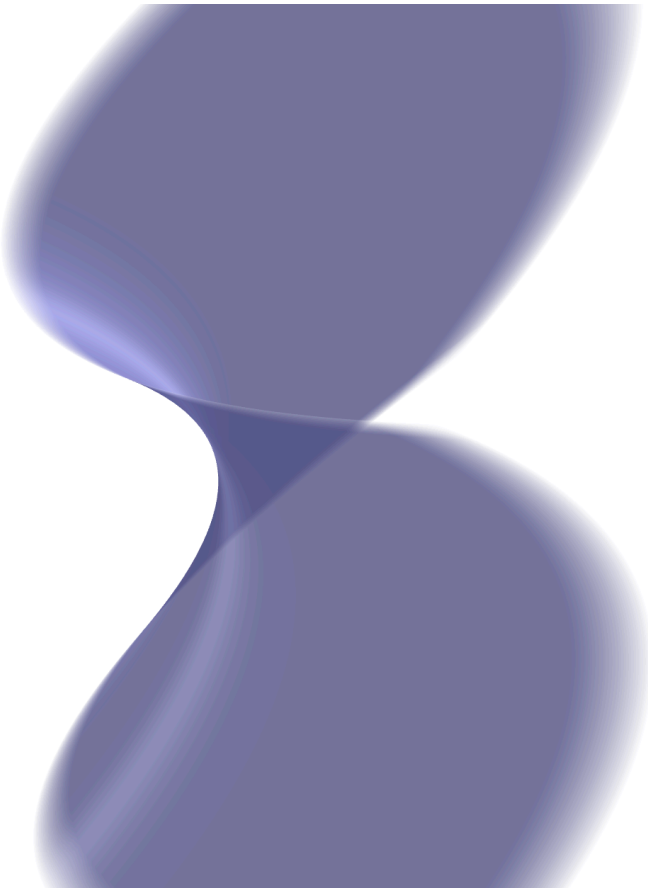
So points $X \in A$ can be thought of as pairs $X = (P_0, P_1)$, where $P_i \in E_i$

Segre embedding:

$$\Phi : \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$$
$$\Phi((x_0 : x_1 : x_2), (y_0 : y_1 : y_2)) = (x_0y_0 : x_0y_1 : \ldots : x_2y_2)$$



$$\begin{aligned}
A := V(\langle & -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1,\\
& -x_3x_4x_6 + x_1x_6^2 + x_1,\\
& -x_3x_5x_6 + x_2x_6^2 + x_2,\\
& -x_1x_2x_4 + x_2^2x_5 + x_3,\\
& -x_1x_2x_7 + x_2^2x_8 + x_6,\\
& -x_4^2x_6 + x_1x_6x_7 + x_1^2,\\
& -x_4x_5x_6 + x_2x_6x_7 + x_1x_2,\\
& -x_5^2x_6 + x_2x_6x_8 + x_2^2,\\
& -x_2x_4^2 + x_2x_5^2 + x_3^2,\\
& -x_2x_4x_7 + x_2x_5x_8 + x_3x_6,\\
& -x_1x_3 + x_4,\\
& -x_2x_3 + x_5,\\
& -x_2x_7^2 + x_2x_8^2 + x_6^2,\\
& -x_1x_6 + x_7,\\
& -x_2x_6 + x_8,\\
& x_1^3 - x_4^2x_7 + x_1x_7^2,\\
& x_1^2x_2 - x_4x_5x_7 + x_2x_7^2,\\
& x_1x_2^2 - x_5^2x_7 + x_2x_7x_8,\\
& -x_2x_4 + x_1x_5,\\
& -x_2x_7 + x_1x_8,\\
& x_2^3 - x_5^2x_8 + x_2x_8^2,\\
& x_3^3 - x_4^2x_5 + x_5^3,\\
& x_3^2x_6 - x_4x_5x_7 + x_5^2x_8,\\
& x_3x_6^2 - x_5x_7^2 + x_5x_8^2,\\
& -x_4x_6 + x_3x_7,\\
& -x_5x_6 + x_3x_8,\\
& -x_5x_7 + x_4x_8,\\
& x_6^3 - x_7^2x_8 + x_8^3\rangle)
\end{aligned}$$



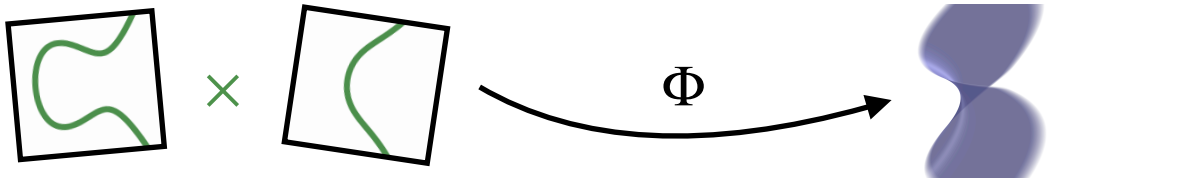
A bit of details!

$$A \simeq E_0 \times E_1, \text{ where}$$
$$E_0 : y^2 = x^3 + x,\ E_1 : y^2 = x^3 + 1$$

So points $X \in A$ can be thought of as pairs $X = (P_0, P_1)$, where $P_i \in E_i$

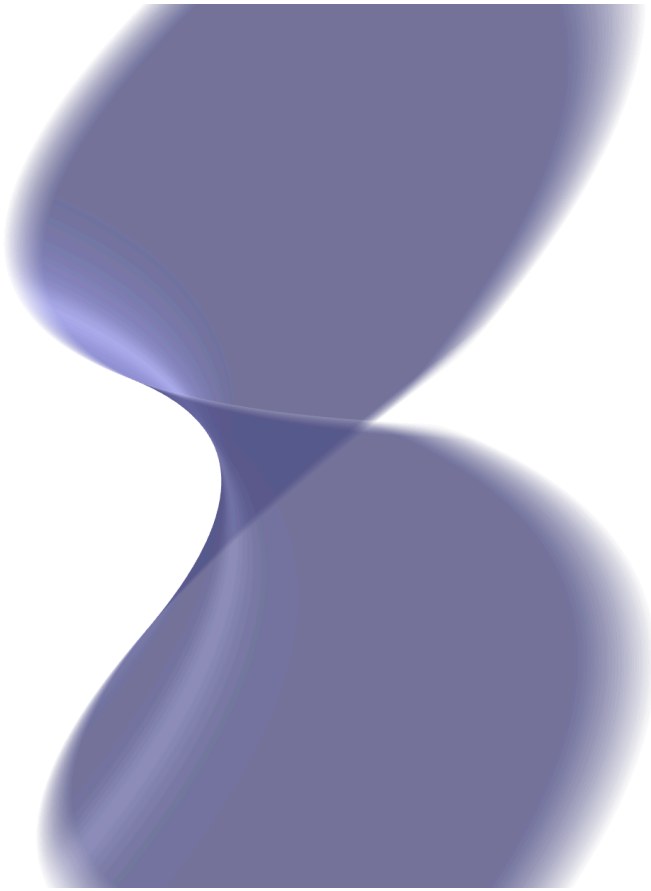
Segre embedding:

$$\Phi : \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$$
$$\Phi((x_0 : x_1 : x_2), (y_0 : y_1 : y_2)) = (x_0y_0 : x_0y_1 : \ldots : x_2y_2)$$



$$(P_1, P_2) \to (7,8,5,2,7,5,2,7)$$
$$+ \qquad +$$
$$(Q_1, Q_2) \to (1,5,9,9,1,8,8,7)$$
$$= \qquad =$$
$$(P_1 + Q_1, P_2 + Q_2) \to (0,10,3,0,8,10,0,1)$$

$$\begin{aligned}
A := V(\langle & -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1,\\
& -x_3x_4x_6 + x_1x_6^2 + x_1,\\
& -x_3x_5x_6 + x_2x_6^2 + x_2,\\
& -x_1x_2x_4 + x_2^2x_5 + x_3,\\
& -x_1x_2x_7 + x_2^2x_8 + x_6,\\
& -x_4^2x_6 + x_1x_6x_7 + x_1^2,\\
& -x_4x_5x_6 + x_2x_6x_7 + x_1x_2,\\
& -x_5^2x_6 + x_2x_6x_8 + x_2^2,\\
& -x_2x_4^2 + x_2x_5^2 + x_3^2,\\
& -x_2x_4x_7 + x_2x_5x_8 + x_3x_6,\\
& -x_1x_3 + x_4,\\
& -x_2x_3 + x_5,\\
& -x_2x_7^2 + x_2x_8^2 + x_6^2,\\
& -x_1x_6 + x_7,\\
& -x_2x_6 + x_8,\\
& x_1^3 - x_4^2x_7 + x_1x_7^2,\\
& x_1^2x_2 - x_4x_5x_7 + x_2x_7^2,\\
& x_1x_2^2 - x_5^2x_7 + x_2x_7x_8,\\
& -x_2x_4 + x_1x_5,\\
& -x_2x_7 + x_1x_8,\\
& x_2^3 - x_5^2x_8 + x_2x_8^2,\\
& x_3^3 - x_4^2x_5 + x_5^3,\\
& x_3^2x_6 - x_4x_5x_7 + x_5^2x_8,\\
& x_3x_6^2 - x_5x_7^2 + x_5x_8^2,\\
& -x_4x_6 + x_3x_7,\\
& -x_5x_6 + x_3x_8,\\
& -x_5x_7 + x_4x_8,\\
& x_6^3 - x_7^2x_8 + x_8^3\rangle)
\end{aligned}$$



A bit of details!

$$A \simeq E_0 \times E_1, \text{ where}$$
$$E_0 : y^2 = x^3 + x, E_1 : y^2 = x^3 + 1$$

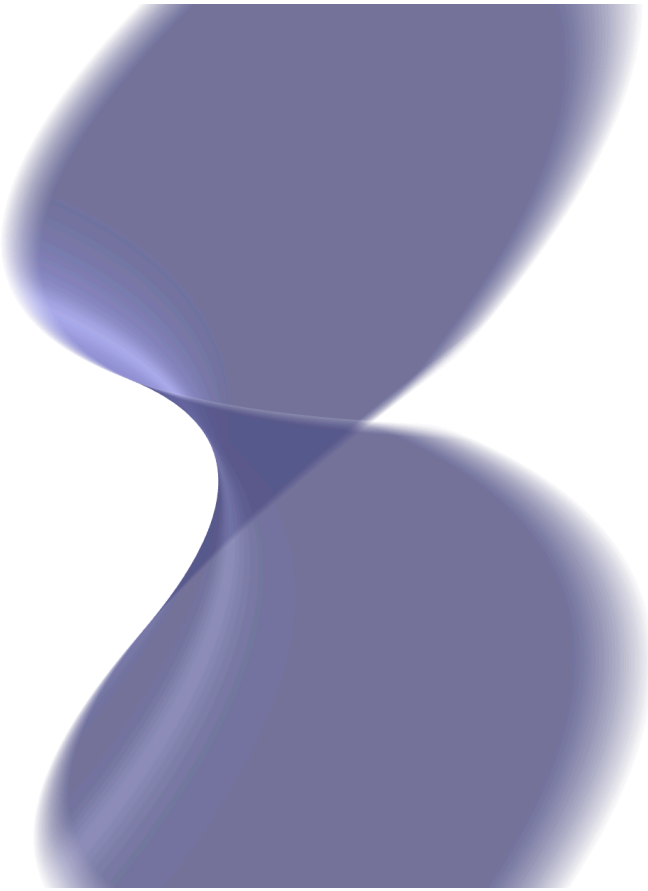
So points $X \in A$ can be thought of as pairs $X = (P_0, P_1)$, where $P_i \in E_i$

This is an exceptional case!

A abelian surface, then either:

- $A \simeq E \times E'$ for elliptic curves E, E'
- $A \simeq J(H)$ for hyperelliptic curve H

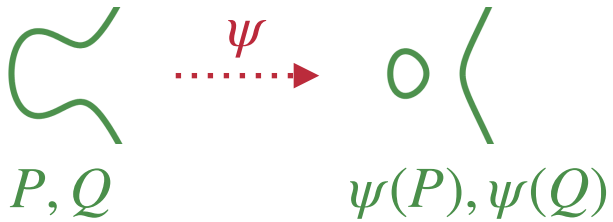
$$A := V(\langle -x_4x_5x_7 + x_2x_7^2 + x_5^2x_8 - x_2x_8^2 + 1,$$
$$-x_3x_4x_6 + x_1x_6^2 + x_1,$$
$$-x_3x_5x_6 + x_2x_6^2 + x_2,$$
$$-x_1x_2x_4 + x_2^2x_5 + x_3,$$
$$-x_1x_2x_7 + x_2^2x_8 + x_6,$$
$$-x_4^2x_6 + x_1x_6x_7 + x_1^2,$$
$$-x_4x_5x_6 + x_2x_6x_7 + x_1x_2,$$
$$-x_5^2x_6 + x_2x_6x_8 + x_2^2,$$
$$-x_2x_4^2 + x_2x_5^2 + x_3^2,$$
$$-x_2x_4x_7 + x_2x_5x_8 + x_3x_6,$$
$$-x_1x_3 + x_4,$$
$$-x_2x_3 + x_5,$$
$$-x_2x_7^2 + x_2x_8^2 + x_6^2,$$
$$-x_1x_6 + x_7,$$
$$-x_2x_6 + x_8,$$
$$x_1^3 - x_4^2x_7 + x_1x_7^2,$$
$$x_1^2x_2 - x_4x_5x_7 + x_2x_7^2,$$
$$x_1x_2^2 - x_5^2x_7 + x_2x_7x_8,$$
$$-x_2x_4 + x_1x_5,$$
$$-x_2x_7 + x_1x_8,$$
$$x_2^3 - x_5^2x_8 + x_2x_8^2,$$
$$x_3^3 - x_4^2x_5 + x_5^3,$$
$$x_3^2x_6 - x_4x_5x_7 + x_5^2x_8,$$
$$x_3x_6^2 - x_5x_7^2 + x_5x_8^2,$$
$$-x_4x_6 + x_3x_7,$$
$$-x_5x_6 + x_3x_8,$$
$$-x_5x_7 + x_4x_8,$$
$$x_6^3 - x_7^2x_8 + x_8^3\rangle)$$



$$H : y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e$$

So what went wrong?

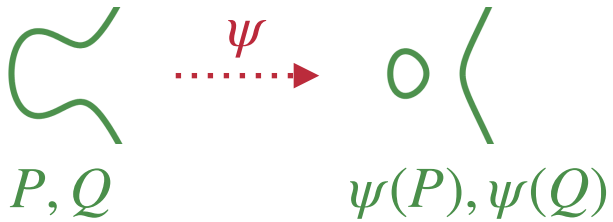
Given



recover ψ

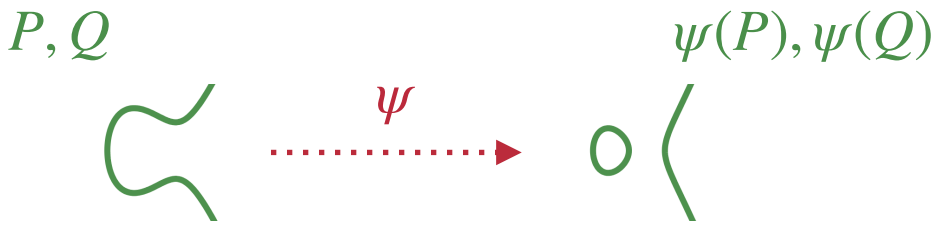
So what went wrong?

Given

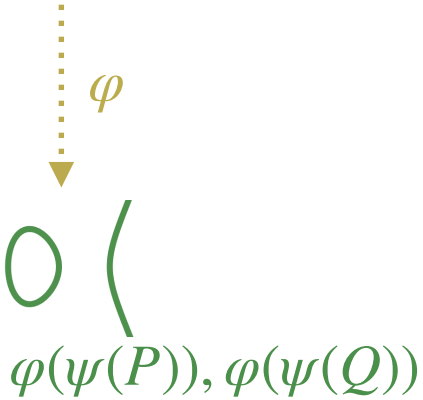


recover ψ

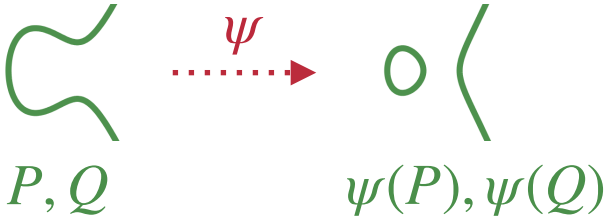
So what went wrong?



Step 1: Choose well-chosen φ

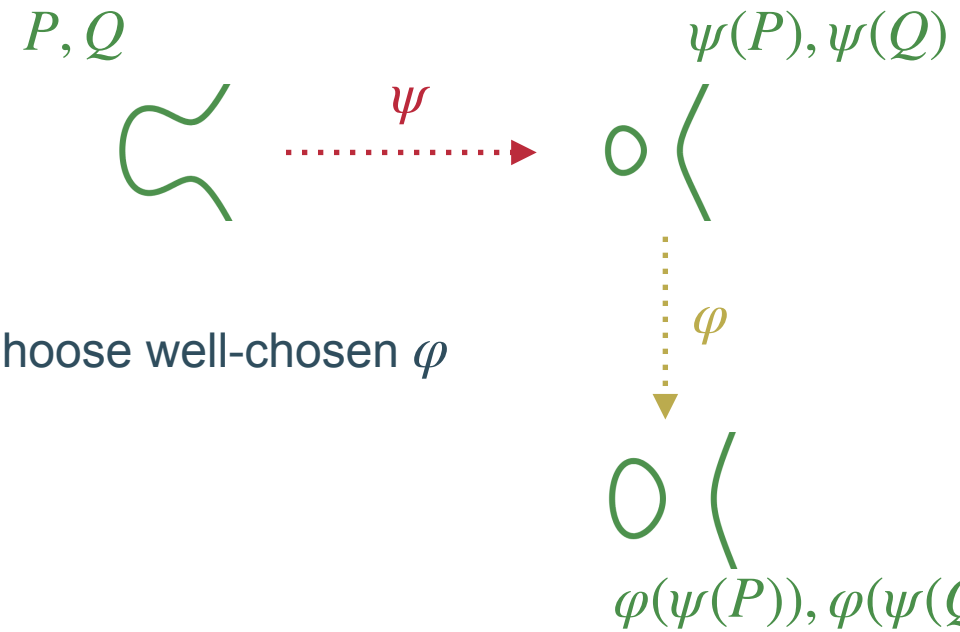


Given



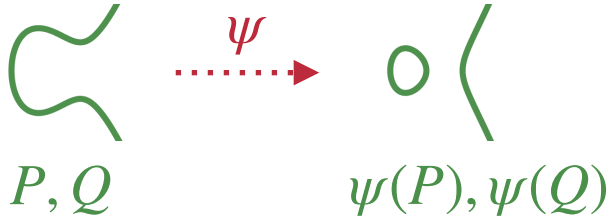
recover ψ

So what went wrong?



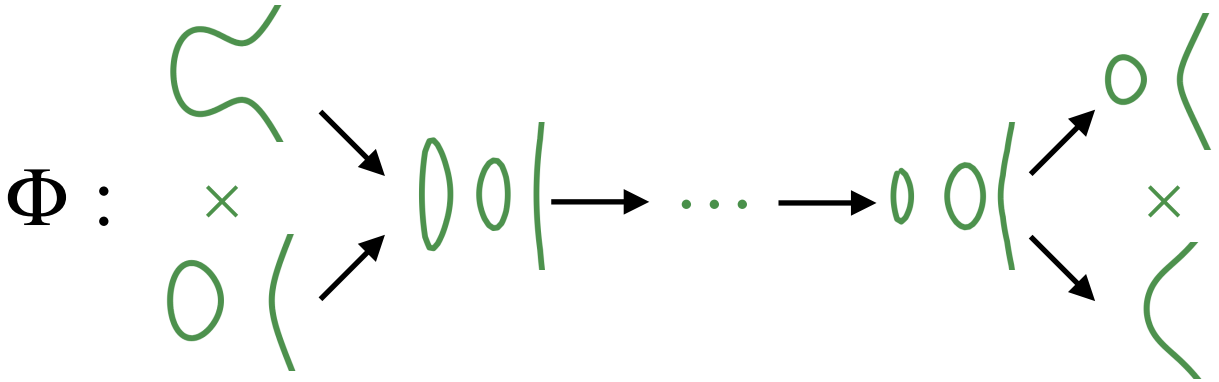
Step 1: Choose well-chosen φ

Given



recover ψ

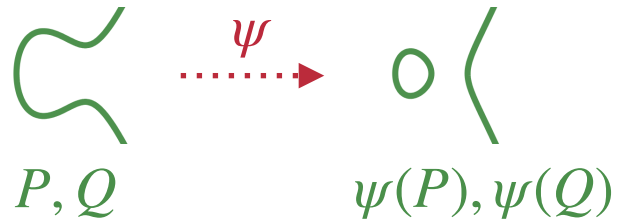
Step 2: Kani's lemma gives a way to compute Φ



$$\Phi((P,0)) = (\psi(P), \varphi'(P))$$

So what went wrong? right?

knowing ~~Given~~



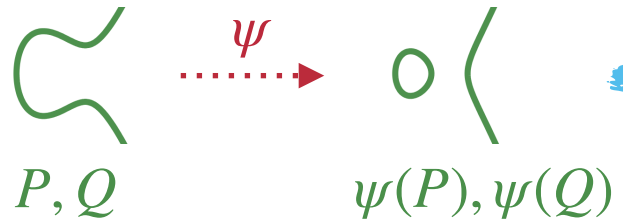
~~recover~~ ψ

is equivalent to knowing

Result of 10+ years of research!

So what went wrong? right?

knowing
~~Given~~



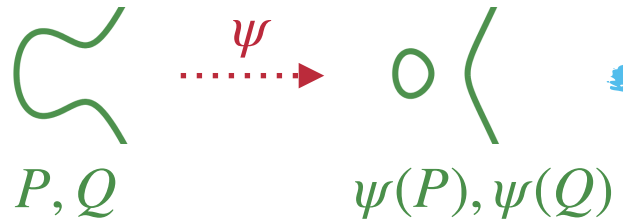
~~recover~~ ψ
is equivalent
to knowing

Result of 10+ years
of research!

Analogy:
Knowing
polynomial
$f : \mathbb{Q} \to \mathbb{Q}$
of degree d,
is equivalent to knowing $f(x_0), \ldots f(x_d)$
for $d + 1$ different values x_i
(Lagrange interpolation)

So what went wrong? right?

knowing
~~Given~~



~~recover~~ ψ
is equivalent to knowing

Result of 10+ years of research!

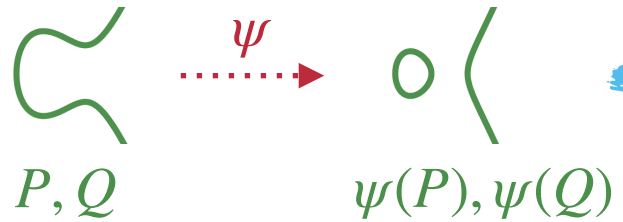
Analogy:
Knowing polynomial
$f : \mathbb{Q} \to \mathbb{Q}$
of degree d,
is equivalent to knowing $f(x_0), \ldots f(x_d)$
for $d + 1$ different values x_i
(Lagrange interpolation)

Applications?

So what went wrong? right?

knowing

~~Given~~



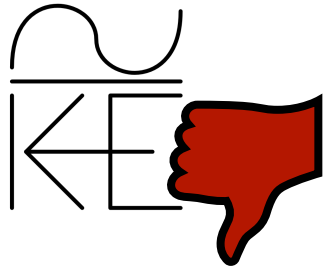
~~recover~~ ψ

is equivalent to knowing

Result of 10+ years of research!

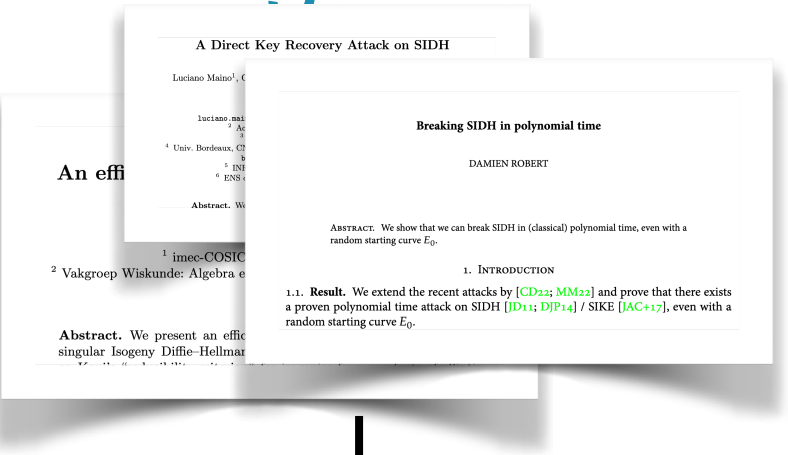
Analogy:
Knowing polynomial
$f : \mathbb{Q} \to \mathbb{Q}$
of degree d,
is equivalent to knowing $f(x_0), \ldots f(x_d)$
for $d + 1$ different values x_i
(Lagrange interpolation)

Applications?



Isogenies are dead?

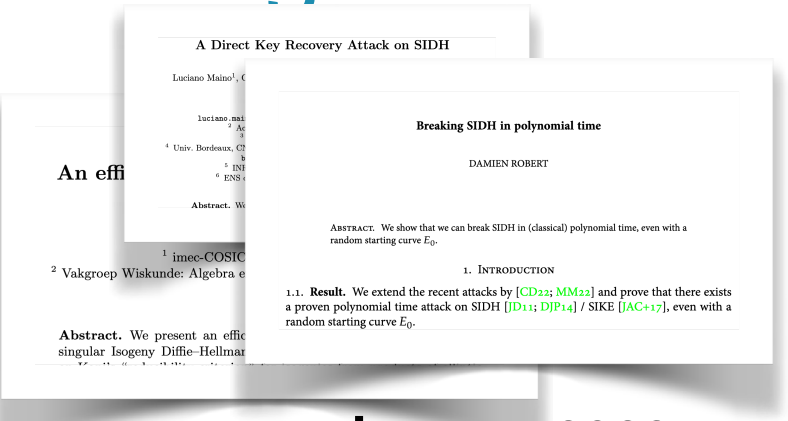
Isogenies are dead?



2022

KU LEUVEN

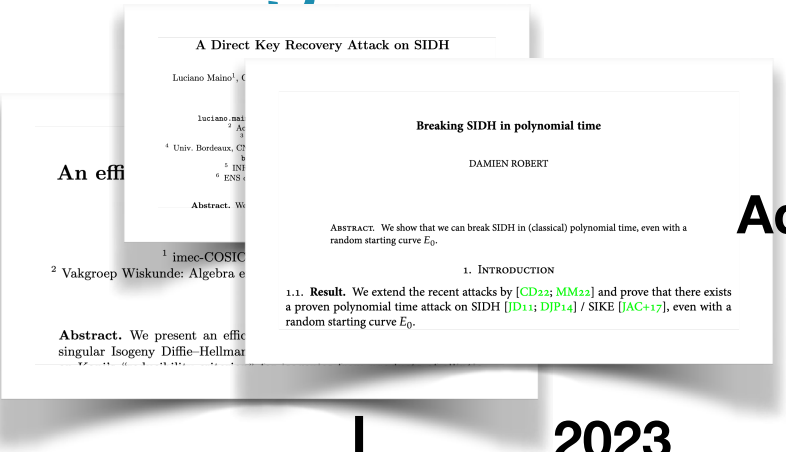
Isogenies are dead?



"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!



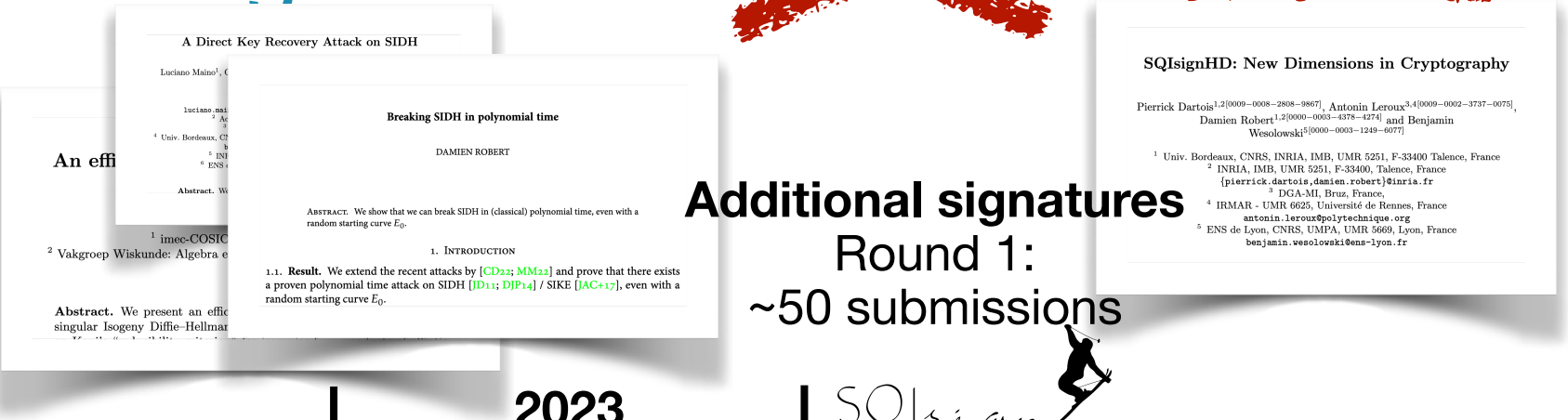
Additional signatures
Round 1:
~50 submissions

2022 — **2023** — **2023**

"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!

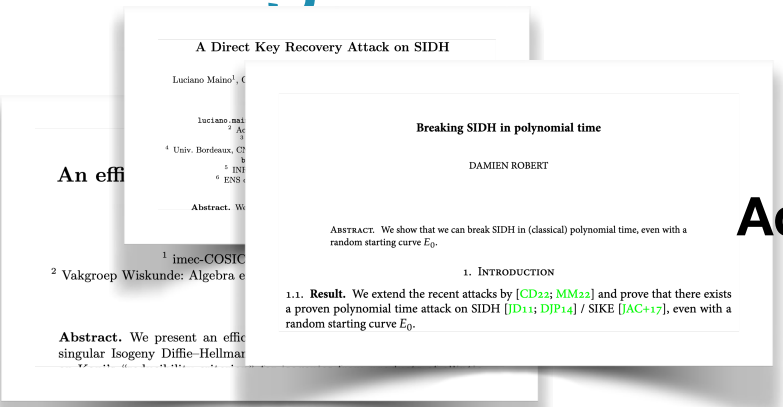


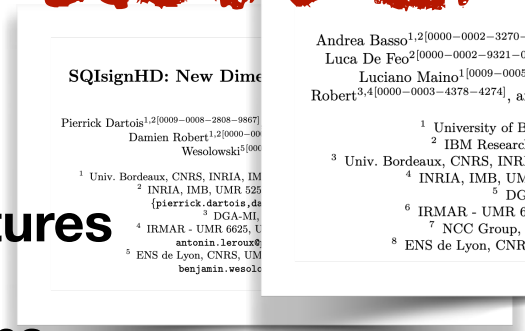
Additional signatures
Round 1:
~50 submissions

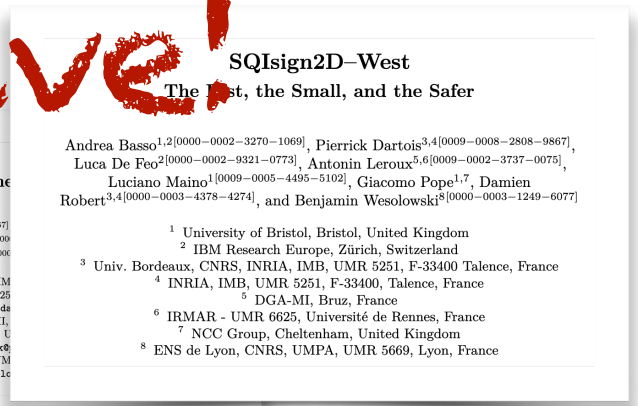
"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!







Additional signatures
Round 1:
~50 submissions

SQIsign

2022 — **2023** — **2023**

"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!

Additional signatures
Round 1:
~50 submissions

SQIsign

2022

2023

2023

"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!

Additional signatures
Round 1:
~50 submissions

SQIsign

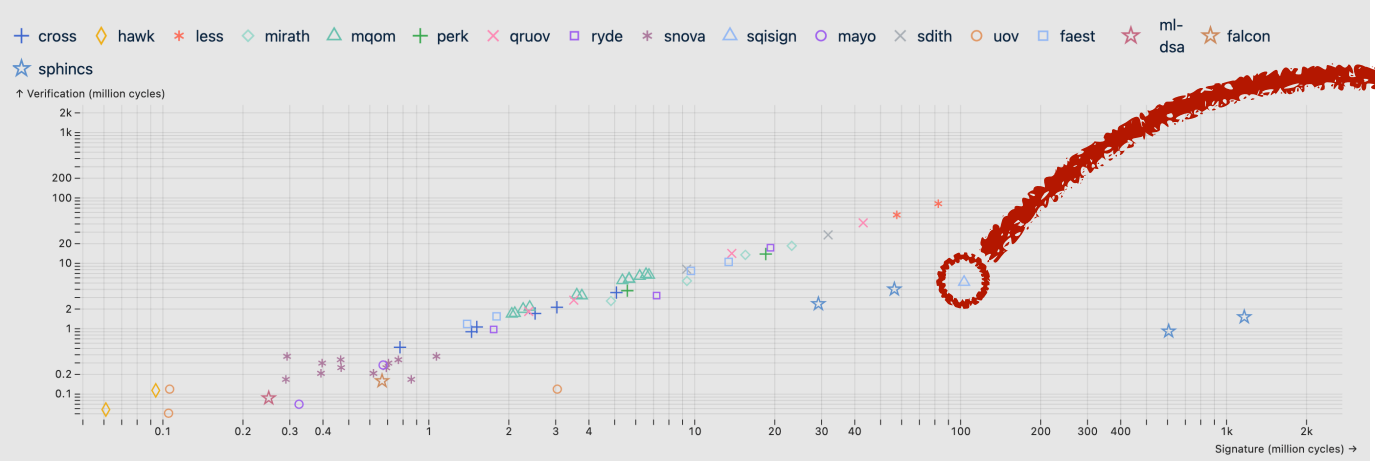
Round 2:
14 submissions

2022 — **2023** — **2023** — **2025**

"SIDH-Fixes"
Security unclear,
completely impractical

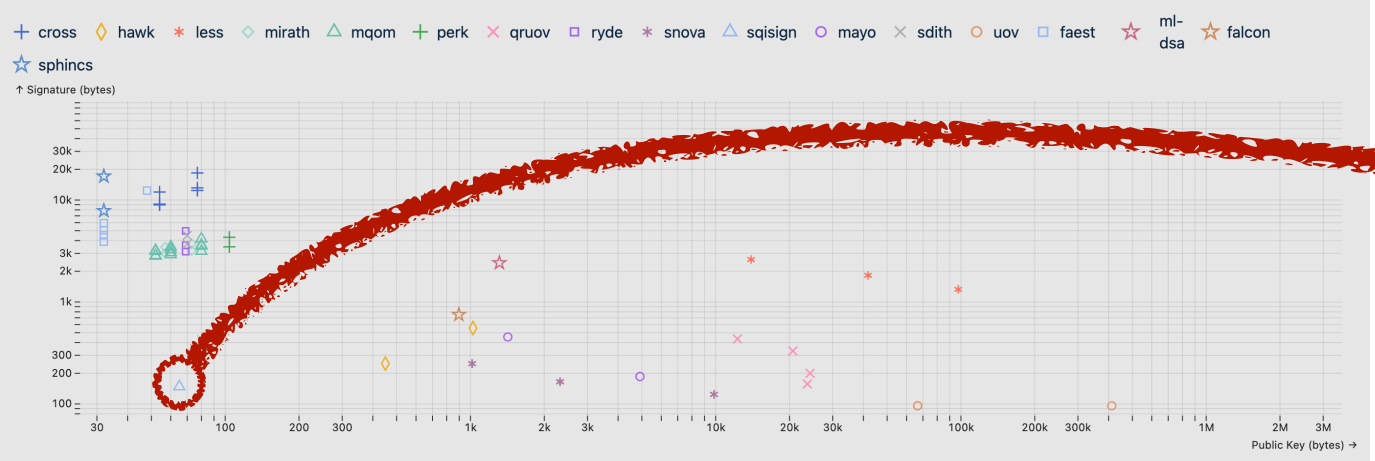
KU LEUVEN

NIST additional signatures - Round 2



Computational cost:

- Below average signing ~ 10 ms
- Average verification ~ 1 ms

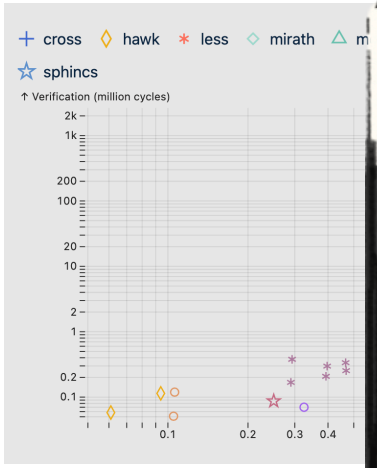


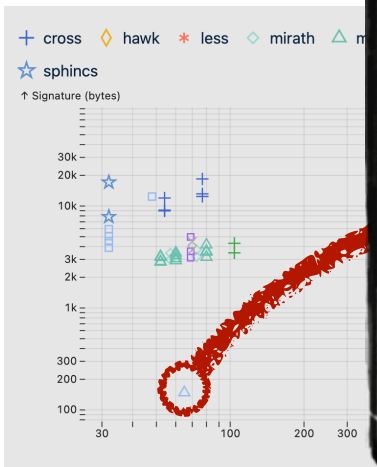
Sizes:

- Top signature size ~ 148 B
- Top public key size ~ 64 B
- Superior pb key + sig size ~ 212 B

KU LEUVEN

NIST additional signatures - Round 2



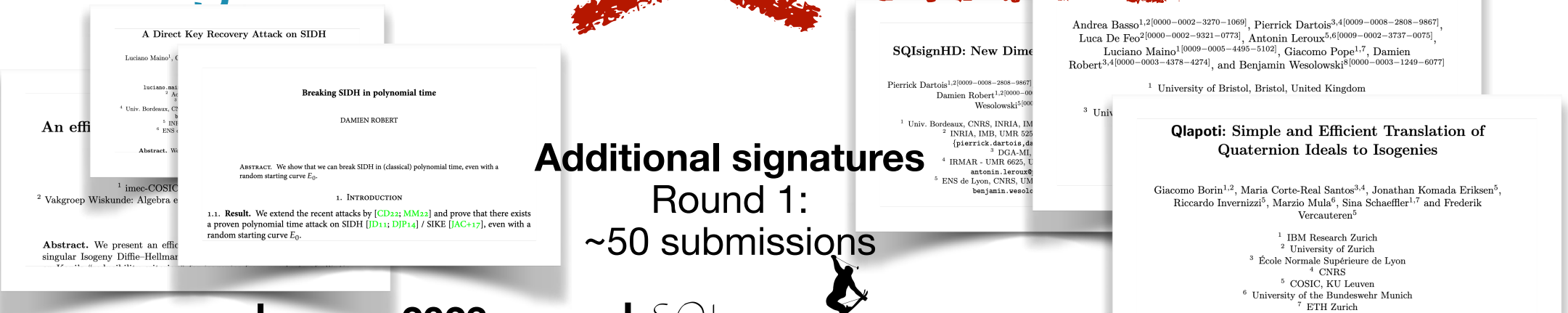


onal cost:
erage signing ~ 10 ms
verification ~ 1 ms

ture size ~ 148 B
c key size ~ 64 B
bb key + sig size ~ 212 B

KU LEUVEN

Isogenies are dead? ~~dead?~~ alive!



Additional signatures
Round 1:
~50 submissions

SQIsign

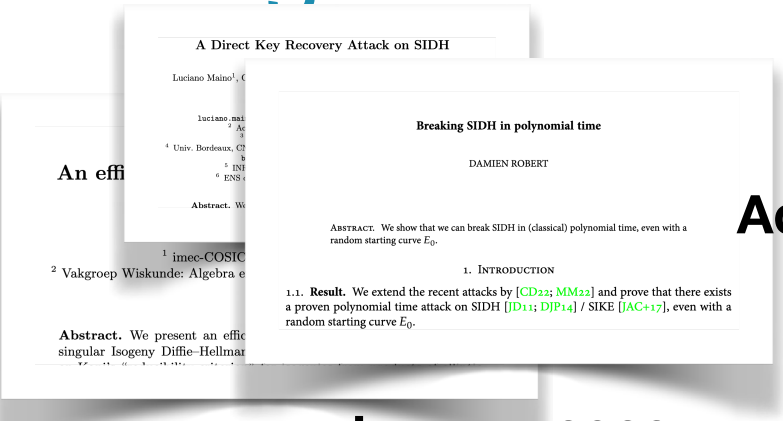
Round 2:
14 submissions

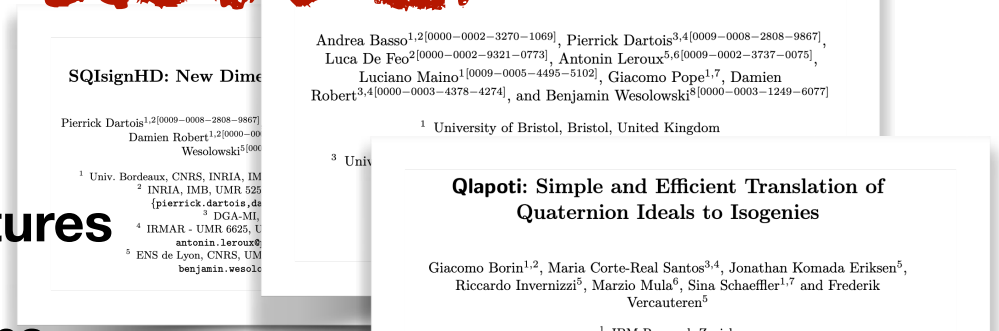
2022 — **2023** — **2023** — **2025**

"SIDH-Fixes"
Security unclear,
completely impractical

KU LEUVEN

Isogenies are dead? alive!





Additional signatures
Round 1:
~50 submissions

SQIsign

Round 2:
14 submissions

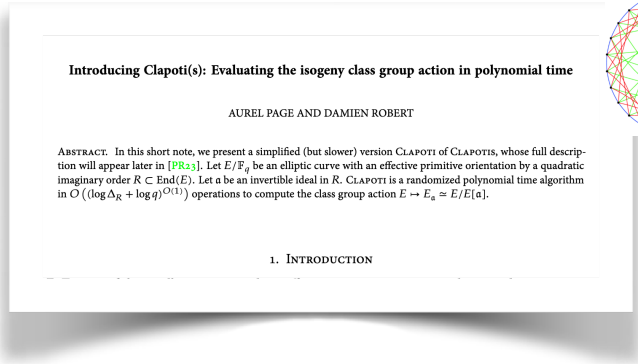
2022

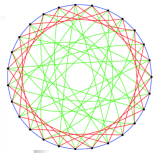
2023

2023

2025

"SIDH-Fixes"
Security unclear,
completely impractical





KU LEUVEN

Isogenies are dead? alive!

Additional signatures
Round 1:
~50 submissions

SQIsign

Round 2:
14 submissions

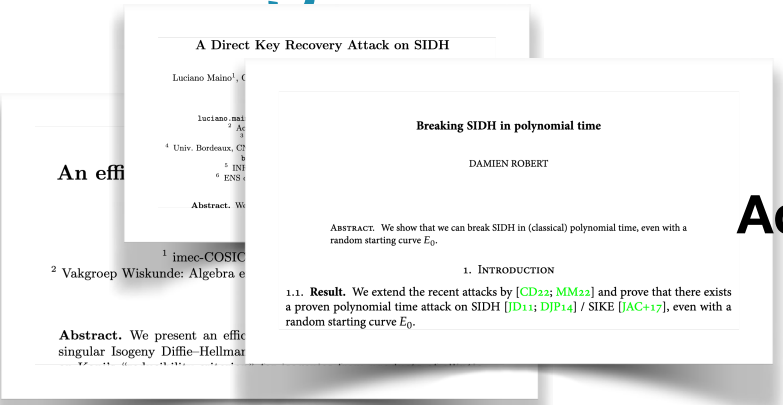
2022

2023

2023

2025

"SIDH-Fixes"
Security unclear,
completely impractical


A Direct Key Recovery Attack on SIDH

Luciano Maino[1], C…

[1] imec-COSIC …
[2] Vakgroep Wiskunde: Algebra e…

Abstract. We present an effic… singular Isogeny Diffie–Hellmar…

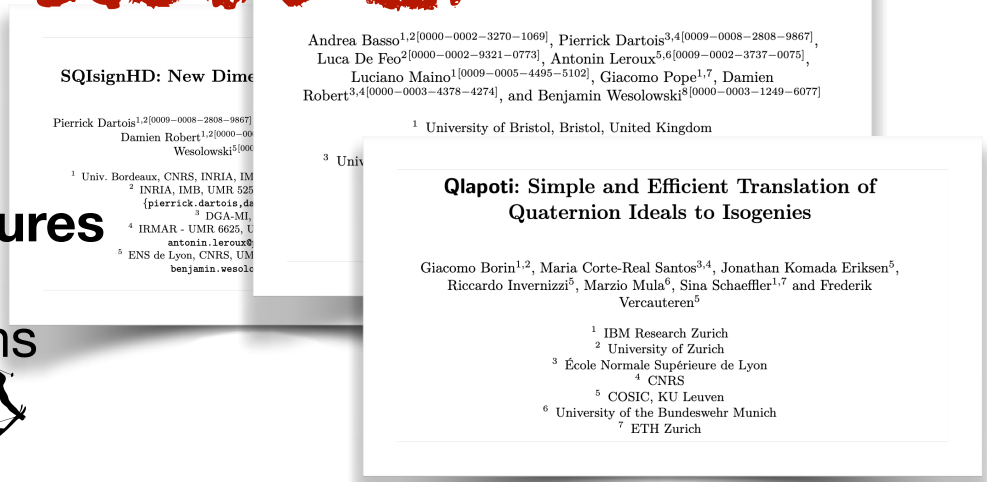
Breaking SIDH in polynomial time

DAMIEN ROBERT

Abstract. We show that we can break SIDH in (classical) polynomial time, even with a random starting curve E_0.

1. Introduction

1.1. **Result.** We extend the recent attacks by [CD22; MM22] and prove that there exists a proven polynomial time attack on SIDH [JD11; DJP14] / SIKE [JAC+17], even with a random starting curve E_0.


SQIsignHD: New Dime…

Pierrick Dartois[1,2[0009−0008−2808−9867]], Damien Robert[1,2[0000−00…], Wesolowski[5[000…]]

[1] Univ. Bordeaux, CNRS, INRIA, IM…
[2] INRIA, IMB, UMR 525…
{pierrick.dartois,da…
[3] DGA-MI, …
[4] IRMAR - UMR 6625, U…
antonin.leroux@…
[5] ENS de Lyon, CNRS, UM…
benjamin.wesolo…

SQIsign2D–West
The …st, the Small, and the Safer

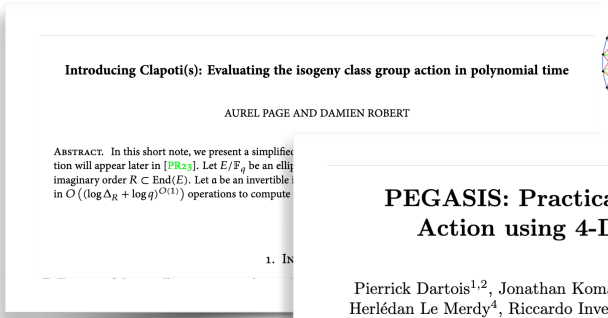
Andrea Basso[1,2[0000−0002−3270−1069]], Pierrick Dartois[3,4[0009−0008−2808−9867]], Luca De Feo[2[0000−0002−9321−0773]], Antonin Leroux[5,6[0009−0002−3737−0075]], Luciano Maino[1[0009−0005−4495−5102]], Giacomo Pope[1,7], Damien Robert[3,4[0000−0003−4378−4274]], and Benjamin Wesolowski[8[0000−0003−1249−6077]]

[1] University of Bristol, Bristol, United Kingdom
[3] Univ…

Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies

Giacomo Borin[1,2], Maria Corte-Real Santos[3,4], Jonathan Komada Eriksen[5], Riccardo Invernizzi[5], Marzio Mula[6], Sina Schaeffler[1,7] and Frederik Vercauteren[5]

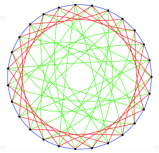
[1] IBM Research Zurich
[2] University of Zurich
[3] École Normale Supérieure de Lyon
[4] CNRS
[5] COSIC, KU Leuven
[6] University of the Bundeswehr Munich
[7] ETH Zurich


Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT

Abstract. In this short note, we present a simplifie… tion will appear later in [PR23]. Let $E/\mathbb{F}_q$ be an ellip… imaginary order $R \subset \mathrm{End}(E)$. Let $\mathfrak{a}$ be an invertible … in $O\left((\log \Delta_R + \log q)^{O(1)}\right)$ operations to compute …

1. In…




PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies

Pierrick Dartois[1,2], Jonathan Komada Eriksen[5], Tako Boris Fouotsa[3], Arthur Herlédan Le Merdy[4], Riccardo Invernizzi[5], Damien Robert[1,2], Ryan Rueger[6,7], Frederik Vercauteren[5] and Benjamin Wesolowski[4]

[1] Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
[2] INRIA, IMB, UMR 5251, F-33400, Talence, France
[3] EPFL, LASEC, Lausanne, Switzerland
[4] ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France
[5] KU Leuven, COSIC, Heverlee, Belgium
[6] IBM Research Europe, Zürich, Switzerland
[7] Technische Universität München, Germany

Isogenies are dead? alive!

Additional signatures
Round 1:
~50 submissions

Round 2:
14 submissions

2022

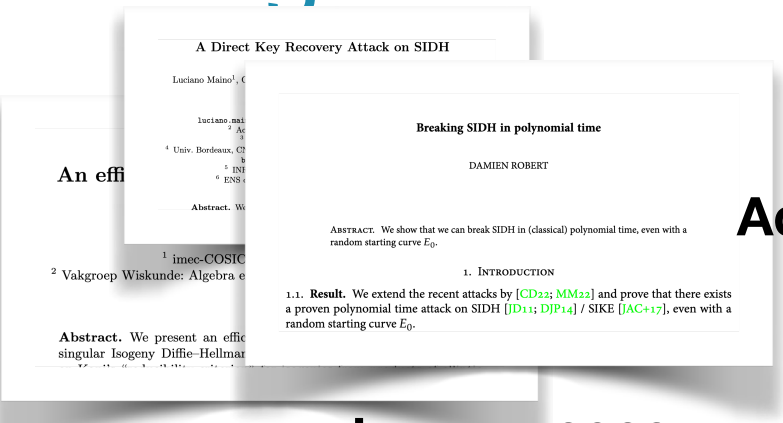
2023

2023

2025

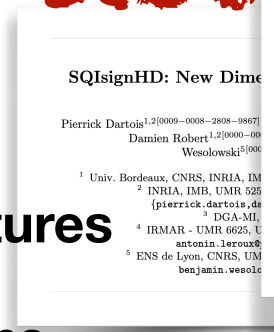
"SIDH-Fixes"
Security unclear,
completely impractical

SQIsign


A Direct Key Recovery Attack on SIDH

Breaking SIDH in polynomial time

DAMIEN ROBERT

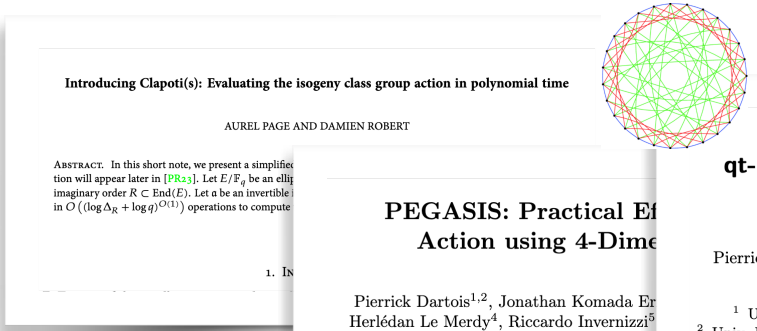

SQIsignHD: New Dime


SQIsign2D–West
The [illegible]st, the Small, and the Safer

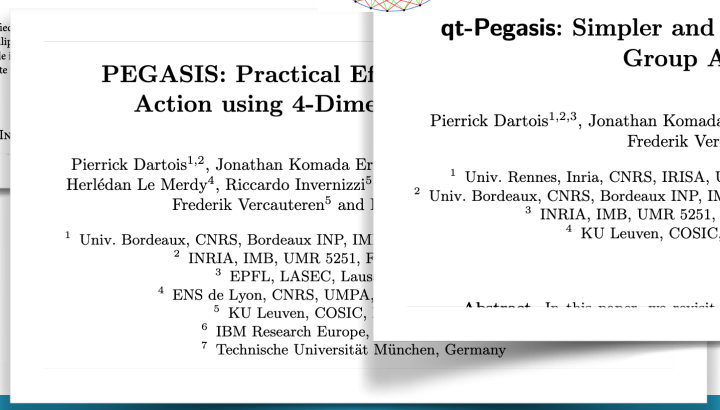
Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski

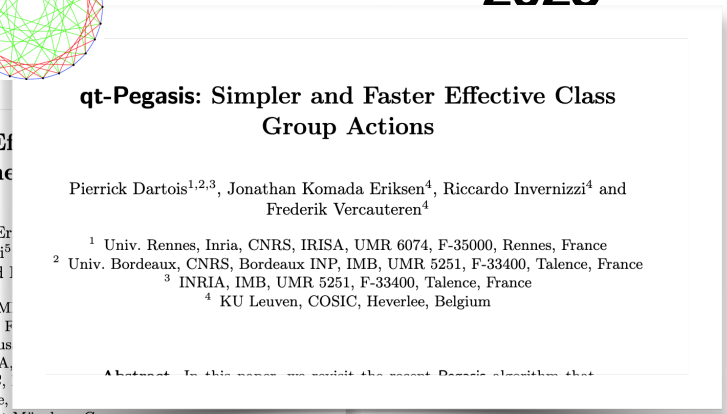

Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies

Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler and Frederik Vercauteren


Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT


PEGASIS: Practical Ef
Action using 4-Dime


qt-Pegasis: Simpler and Faster Effective Class Group Actions

Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi and Frederik Vercauteren

KU LEUVEN

Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard

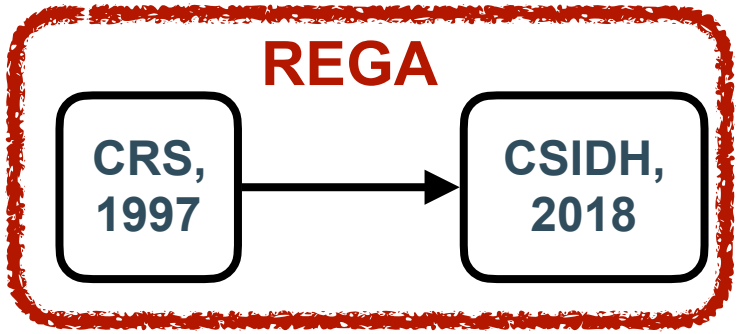
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



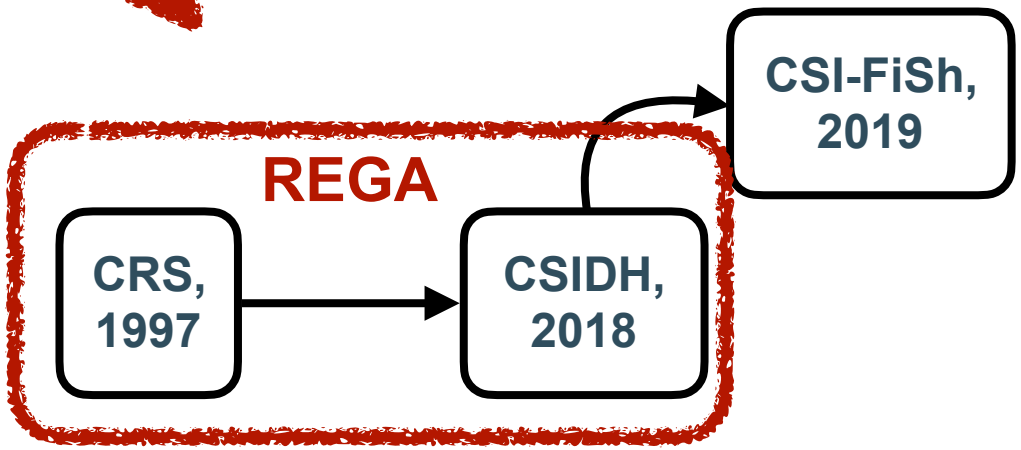
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



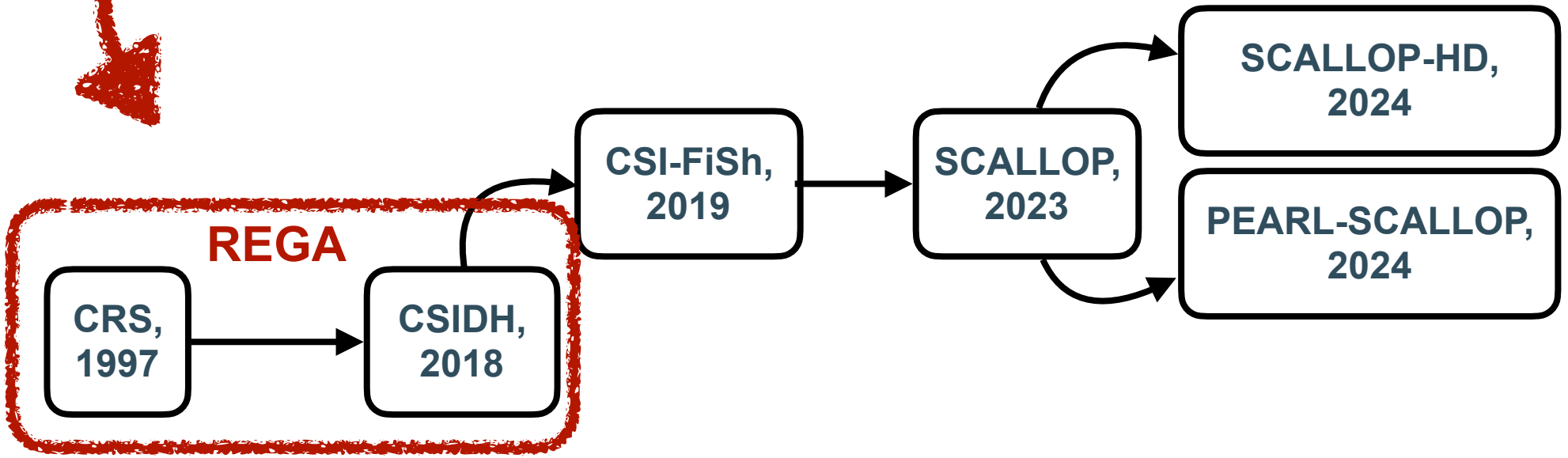
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



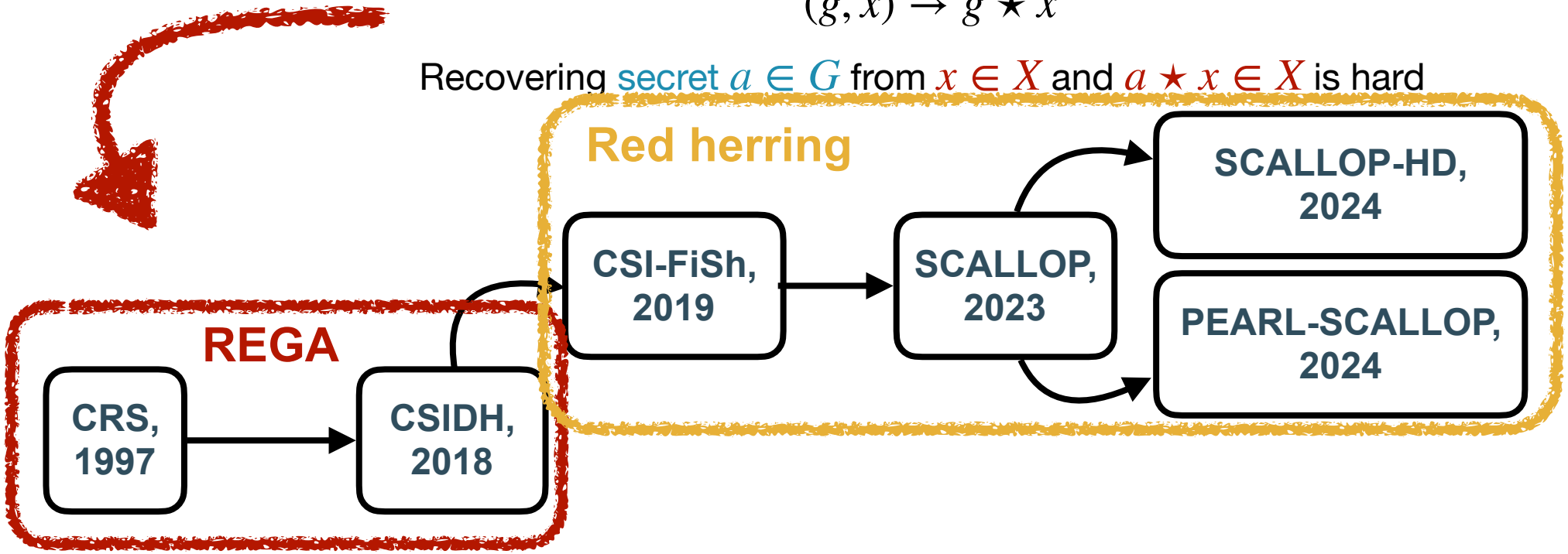
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



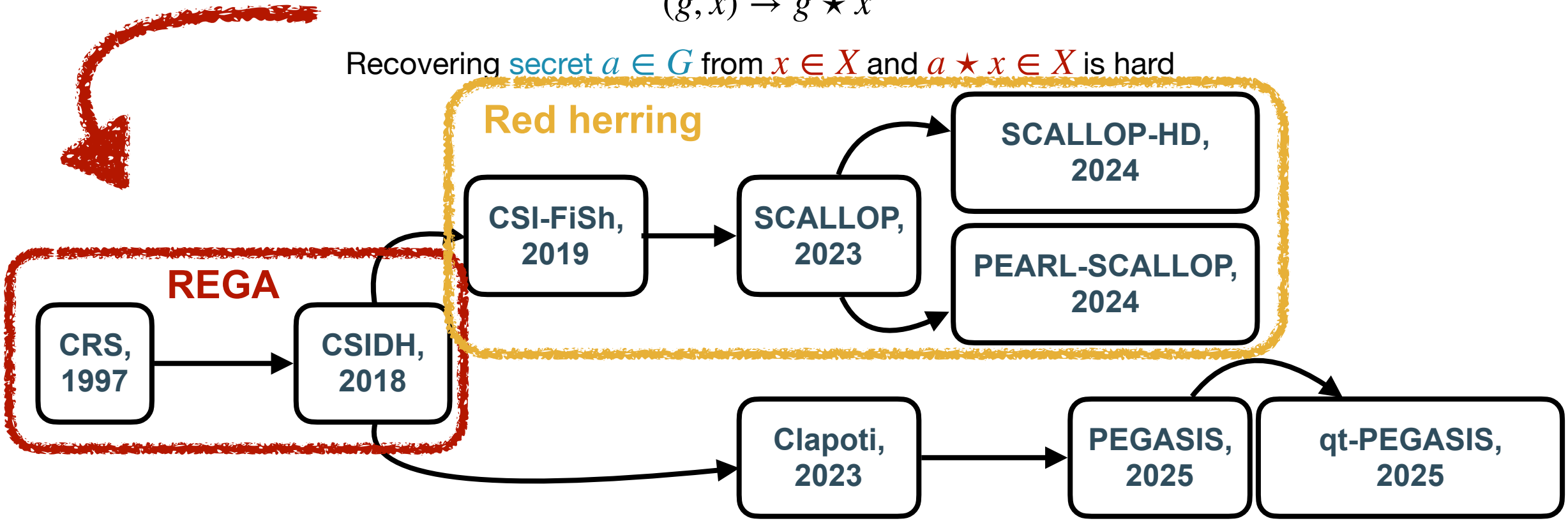
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



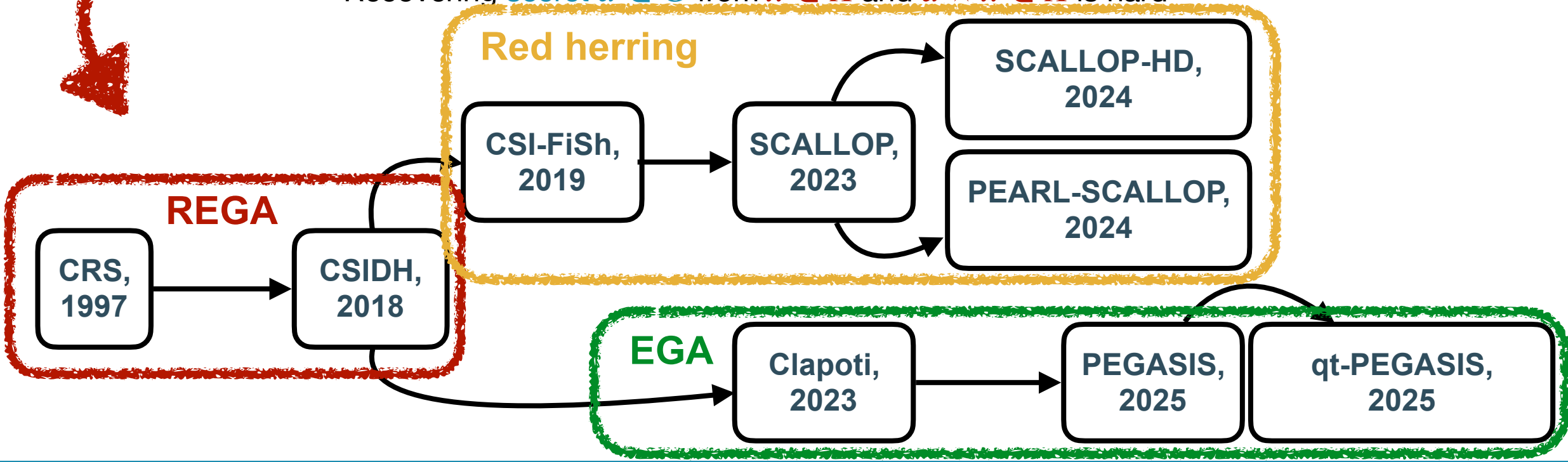
Clapoti / PEGASIS

Post-Quantum variants of many Diffie-Hellman based protocols

Commutative group G, set X:

$$G \times X \to X$$
$$(g, x) \to g \star x$$

Recovering secret $a \in G$ from $x \in X$ and $a \star x \in X$ is hard



Isogenies are dead? alive!

Additional signatures
Round 1:
~50 submissions

Round 2:
14 submissions

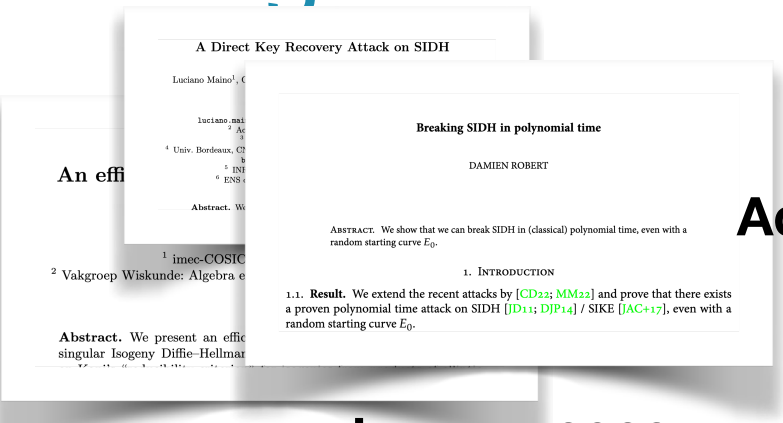
2022

2023

2023

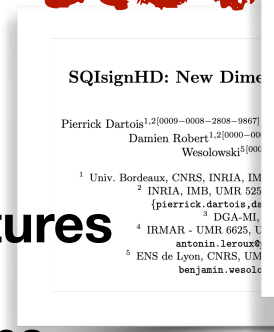
2025

"SIDH-Fixes"
Security unclear,
completely impractical


A Direct Key Recovery Attack on SIDH

Breaking SIDH in polynomial time

DAMIEN ROBERT

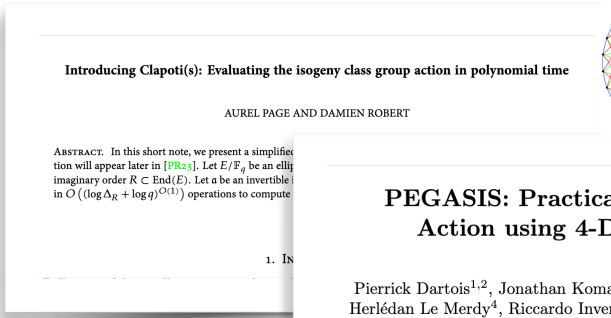

SQIsignHD: New Dime


SQIsign2D–West
The [illegible]st, the Small, and the Safer

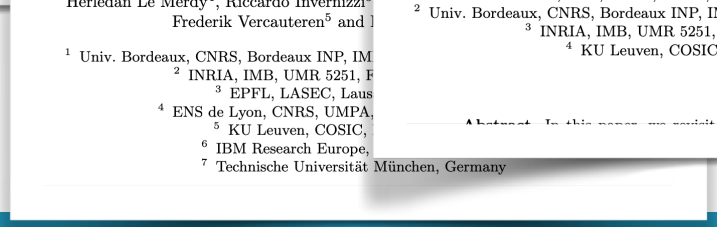
Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski

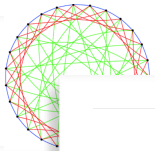

Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies

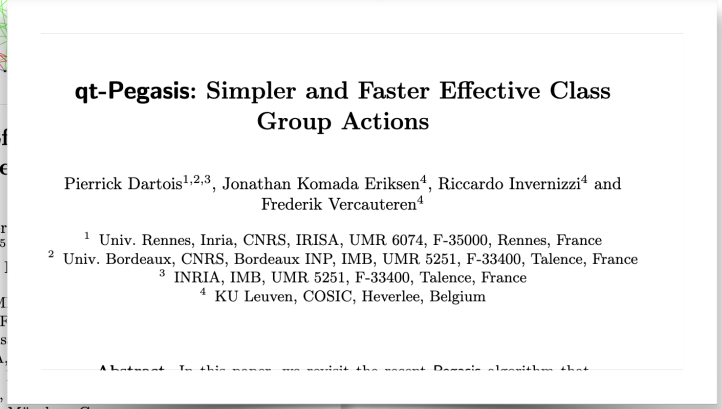
Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Schaeffler and Frederik Vercauteren


Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT


PEGASIS: Practical Ef
Action using 4-Dime




qt-Pegasis: Simpler and Faster Effective Class Group Actions

Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi and Frederik Vercauteren

KU LEUVEN

Isogenies are dead? alive!

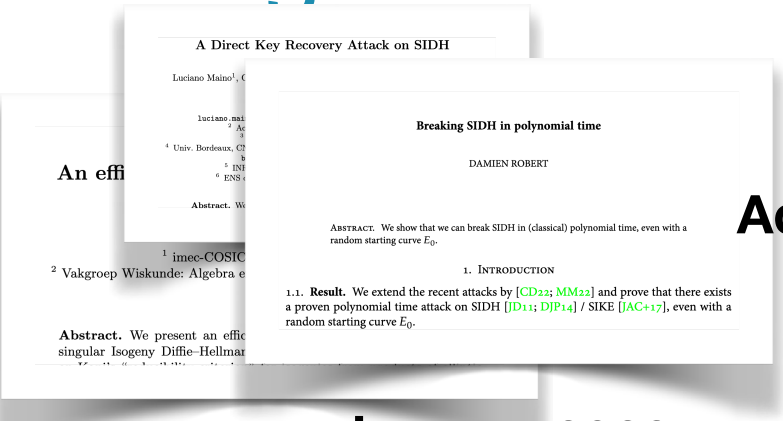
Additional signatures

Round 1:
~50 submissions

Round 2:
14 submissions

2022 — 2023 — 2023

"SIDH-Fixes"
Security unclear,
completely impractical


A Direct Key Recovery Attack on SIDH

Luciano Maino[1]

[1] imec-COSIC

[2] Vakgroep Wiskunde: Algebra e

Abstract. We present an effic
singular Isogeny Diffie–Hellmar

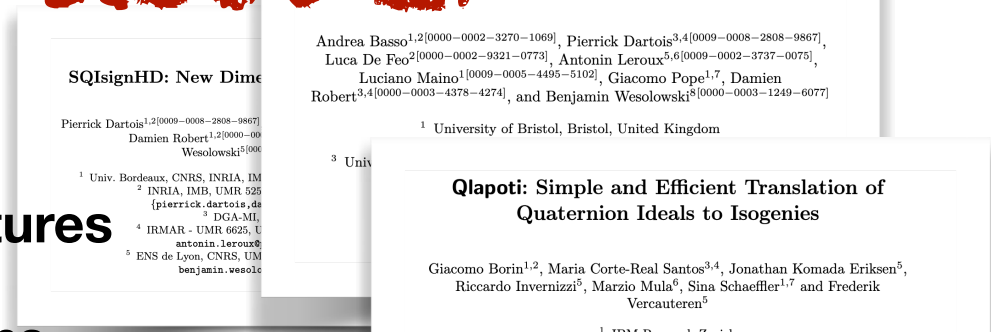
Breaking SIDH in polynomial time

DAMIEN ROBERT

Abstract. We show that we can break SIDH in (classical) polynomial time, even with a random starting curve E_0.

1. Introduction

1.1. **Result.** We extend the recent attacks by [CD22; MM22] and prove that there exists a proven polynomial time attack on SIDH [JD11; DJP14] / SIKE [JAC+17], even with a random starting curve E_0.


SQIsignHD: New Dime

Pierrick Dartois[1,2][0009−0008−2808−9867]
Damien Robert[1,2][0000−00
Wesolowski[5][000

[1] Univ. Bordeaux, CNRS, INRIA, IM
[2] INRIA, IMB, UMR 525
{pierrick.dartois,da
[3] DGA-MI,
[4] IRMAR - UMR 6625, U
antonin.leroux@
[5] ENS de Lyon, CNRS, UM
benjamin.wesolo

SQIsign2D–West
The [illegible]st, the Small, and the Safer

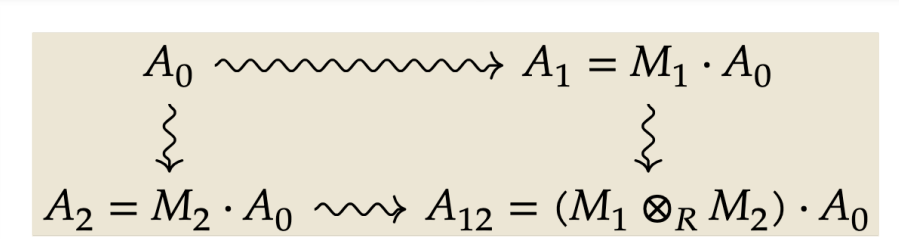
Andrea Basso[1,2[0000−0002−3270−1069]], Pierrick Dartois[3,4[0009−0008−2808−9867]], Luca De Feo[2[0000−0002−9321−0773]], Antonin Leroux[5,6[0009−0002−3737−0075]], Luciano Maino[1[0009−0005−4495−5102]], Giacomo Pope[1,7], Damien Robert[3,4[0000−0003−4378−4274]], and Benjamin Wesolowski[8[0000−0003−1249−6077]]

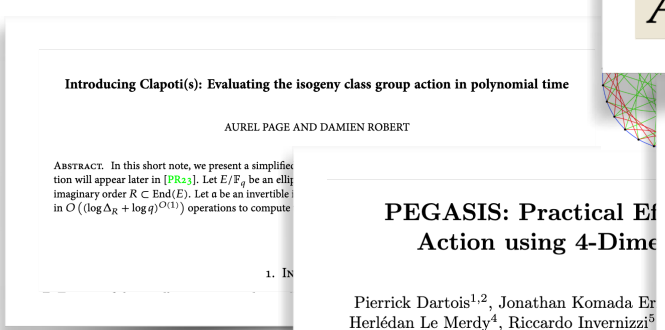
[1] University of Bristol, Bristol, United Kingdom
[3] Univ

Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies

Giacomo Borin[1,2], Maria Corte-Real Santos[3,4], Jonathan Komada Eriksen[5], Riccardo Invernizzi[5], Marzio Mula[6], Sina Schaeffler[1,7] and Frederik Vercauteren[5]

[1] IBM Research Zurich
[2] University of Zurich
[3] École Normale Supérieure de Lyon

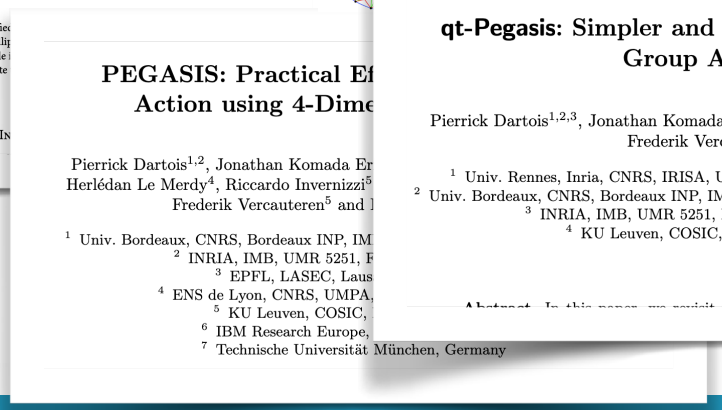

$$A_0 \rightsquigarrow A_1 = M_1 \cdot A_0$$
$$\downarrow \qquad\qquad \downarrow$$
$$A_2 = M_2 \cdot A_0 \rightsquigarrow A_{12} = (M_1 \otimes_R M_2) \cdot A_0$$


Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT

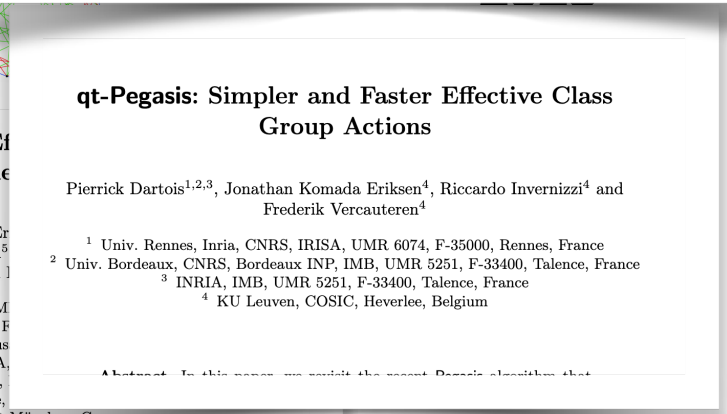
Abstract. In this short note, we present a simplifie
tion will appear later in [PR23]. Let $E/\mathbb{F}_q$ be an ellip
imaginary order $R \subset \mathrm{End}(E)$. Let $\mathfrak{a}$ be an invertible
in $O\left((\log \Delta_R + \log q)^{O(1)}\right)$ operations to compute

1. In


PEGASIS: Practical Ef
Action using 4-Dime

Pierrick Dartois[1,2], Jonathan Komada Er
Herlédan Le Merdy[4], Riccardo Invernizzi[5]
Frederik Vercauteren[5] and

[1] Univ. Bordeaux, CNRS, Bordeaux INP, IM
[2] INRIA, IMB, UMR 5251, F
[3] EPFL, LASEC, Laus
[4] ENS de Lyon, CNRS, UMPA,
[5] KU Leuven, COSIC,
[6] IBM Research Europe,
[7] Technische Universität München, Germany


qt-Pegasis: Simpler and Faster Effective Class Group Actions

Pierrick Dartois[1,2,3], Jonathan Komada Eriksen[4], Riccardo Invernizzi[4] and Frederik Vercauteren[4]

[1] Univ. Rennes, Inria, CNRS, IRISA, UMR 6074, F-35000, Rennes, France
[2] Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
[3] INRIA, IMB, UMR 5251, F-33400, Talence, France
[4] KU Leuven, COSIC, Heverlee, Belgium

KU LEUVEN

SIDH/SIKE

Alice

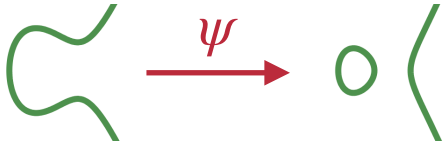
secret:

public:

$\varphi(P_1), \varphi(Q_1)$

Bob

secret:



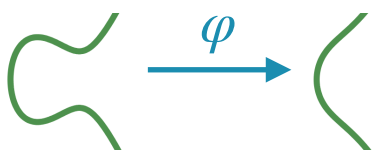
public:

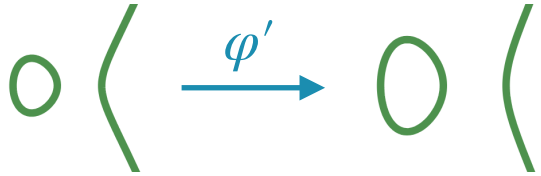
$\psi(P_2), \psi(Q_2)$

SIDH/SIKE

Alice

secret:

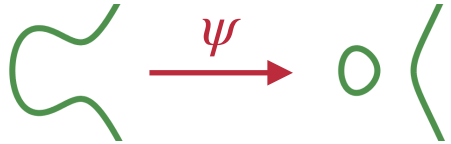


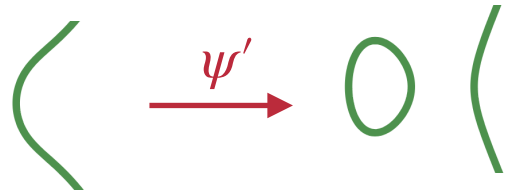


$\psi(P_2), \psi(Q_2)$

Bob

secret:





$\varphi(P_1), \varphi(Q_1)$

⊗-MIKE: SIDH without torsion points

Alice

secret: 

public: 

Bob

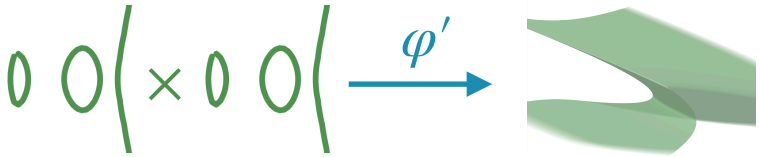
secret: 

public: 

⊗-MIKE: SIDH without torsion points

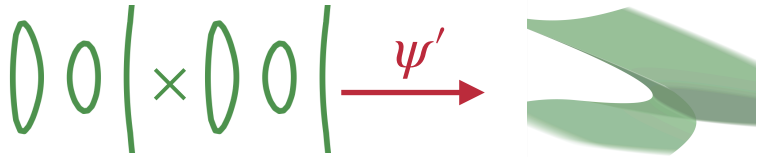
Alice

secret: 

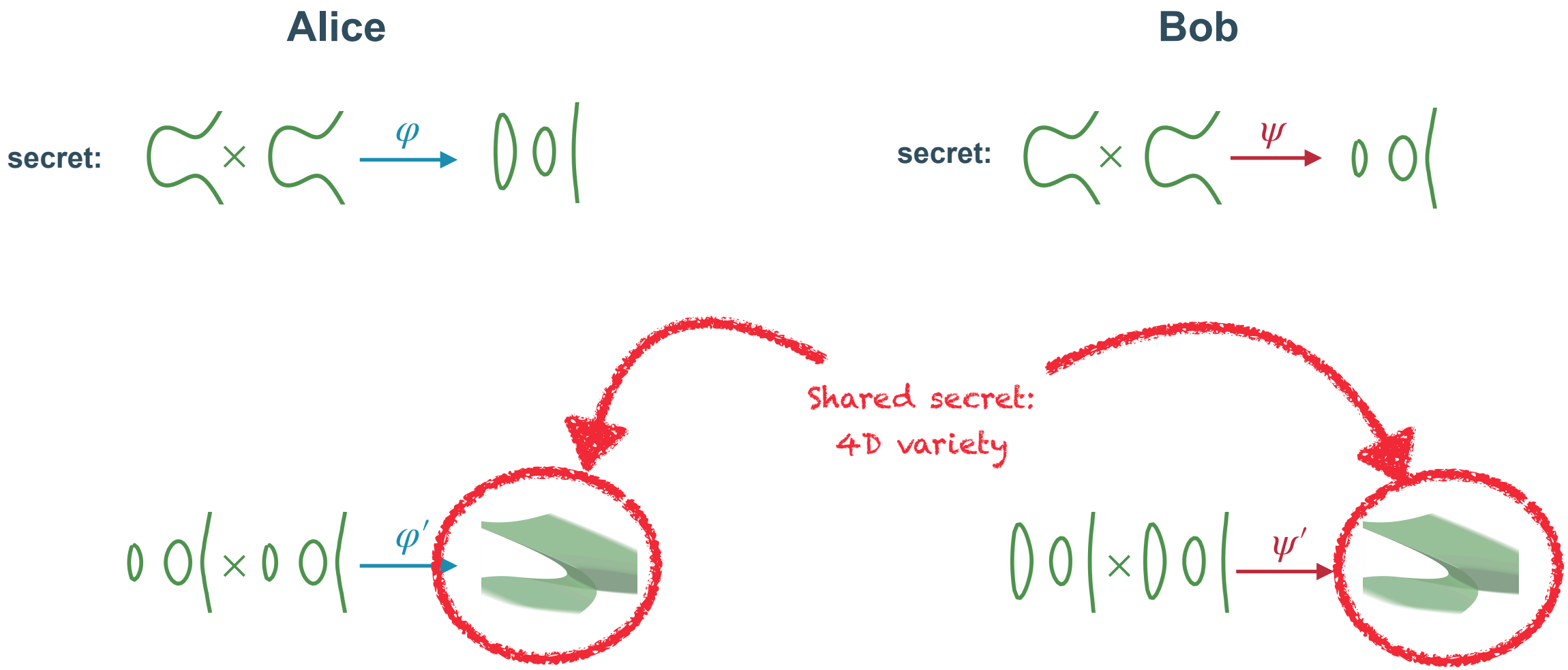


Bob

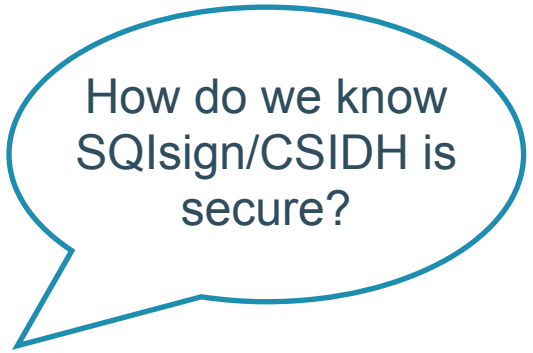
secret: 



⊗-MIKE: SIDH without torsion points



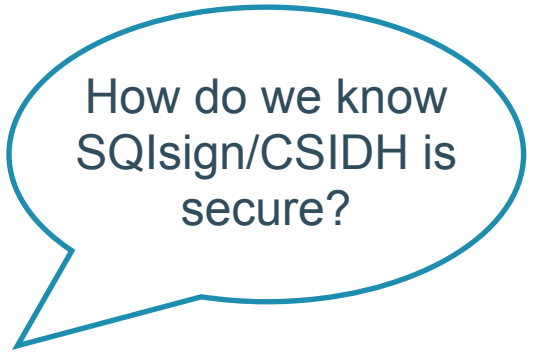
Can we trust SQIsign / CSIDH / MIKE?



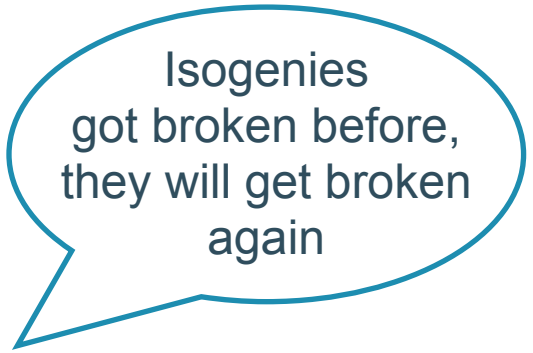
Unfortunately, we don't.
We don't even know if there is such a thing as a secure cryptosystem

Can we trust SQIsign / CSIDH / MIKE?

Example:



Unfortunately, we don't.
We don't even know if there is such a thing as a secure cryptosystem



The extra insight learned from the attacks are a good thing!

Can we trust SQIsign / CSIDH / MIKE?

How do we know SQIsign/CSIDH is secure?

Unfortunately, we don't.
We don't even know if there is such a thing as a secure cryptosystem

Isogenies got broken before, they will get broken again

The extra insight learned from the attacks are a good thing!

Example:

Can we trust SQIsign / CSIDH / MIKE?

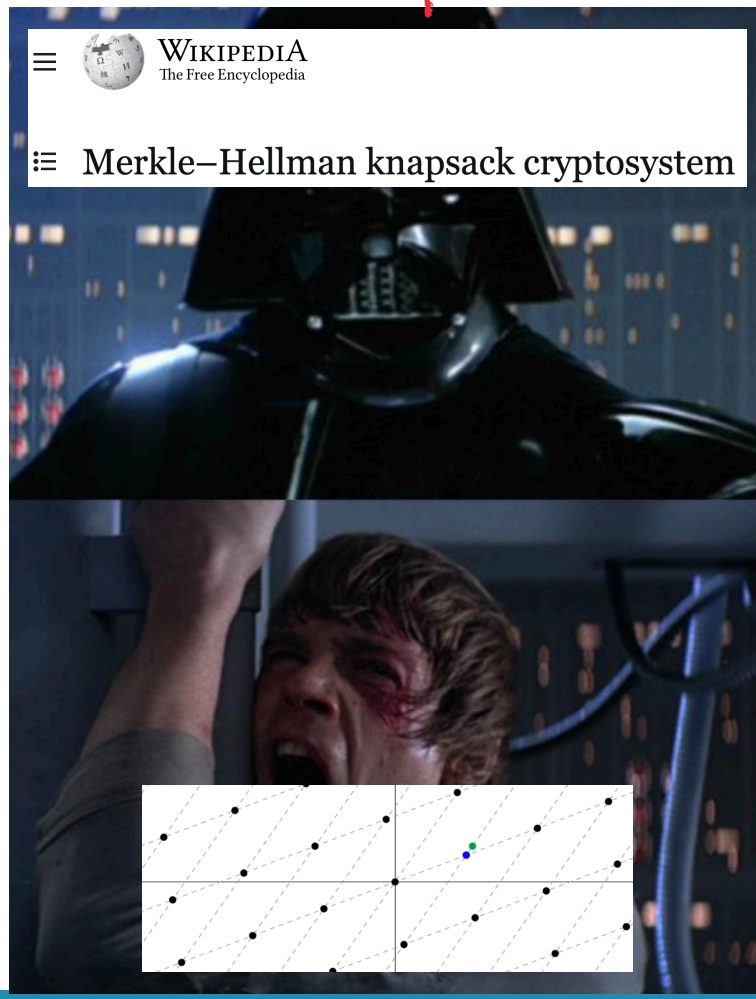
How do we know SQIsign/CSIDH is secure?

Unfortunately, we don't.
We don't even know if there is such a thing as a secure cryptosystem

Isogenies got broken before, they will get broken again

The extra insight learned from the attacks are a good thing!

Example:



KU LEUVEN

Will isogenies ever get used in the real world?

qt-PEGASIS / ⊗-MIKE

Too early to tell,
NIST threshold standardisation
interesting indicator for qt-PEGASIS

Will isogenies ever get used in the real world?

qt-PEGASIS / ⊗-MIKE

Too early to tell,
NIST threshold standardisation
interesting indicator for qt-PEGASIS

SQIsign

For some applications,
SQIsign confidently looks like
the **best option on paper**

Will isogenies ever get used in the real world?

qt-PEGASIS / ⊗-MIKE

Too early to tell,
NIST threshold standardisation
interesting indicator for qt-PEGASIS

SQIsign

For some applications,
SQIsign confidently looks like
the **best option on paper**

Will isogenies ever get used in the real world?

qt-PEGASIS / ⊗-MIKE

Too early to tell,
NIST threshold standardisation
interesting indicator for qt-PEGASIS

SQIsign

Digital certificates,
Blockchains

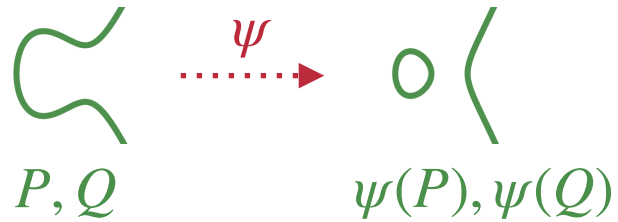
For some applications,
SQIsign confidently looks like
the **best option on paper**

When they say they like SQIsign

Because Falcon is too hard to implement

So what went wrong? right?

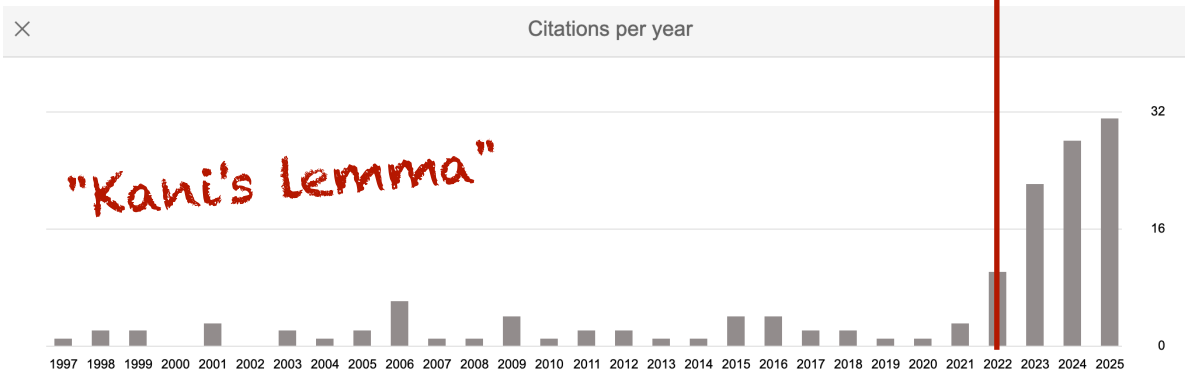
knowing ~~Given~~



~~recover~~ ψ

is equivalent to knowing

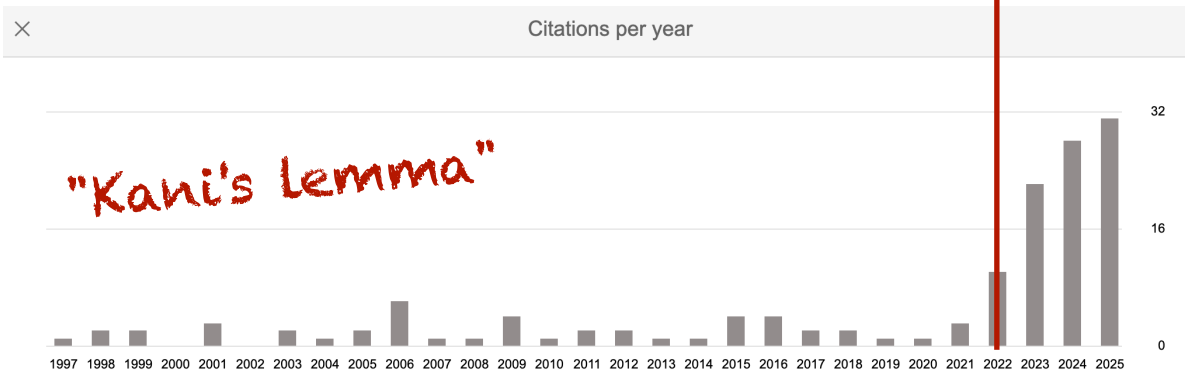
Before | After



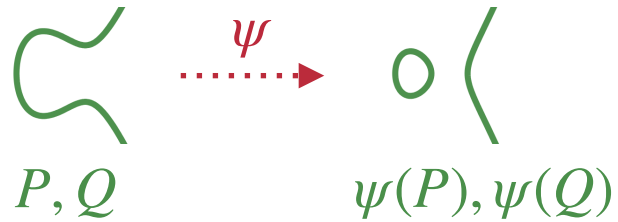
KU LEUVEN

So what went wrong? right?

Before | After

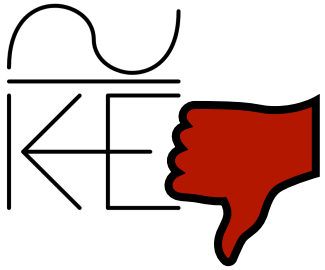


knowing ~~Given~~

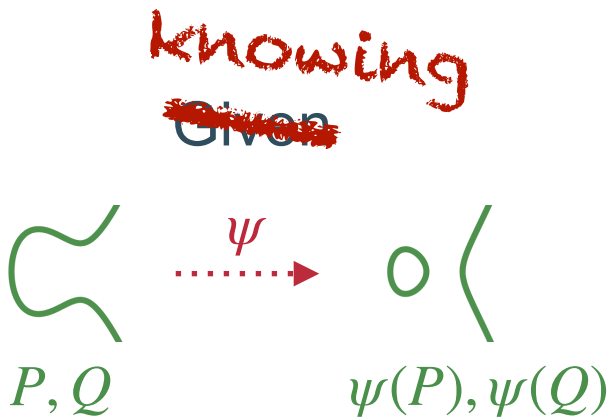


~~recover~~ ψ is equivalent to knowing

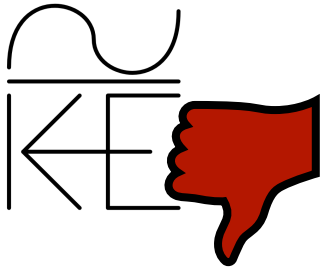
Applications



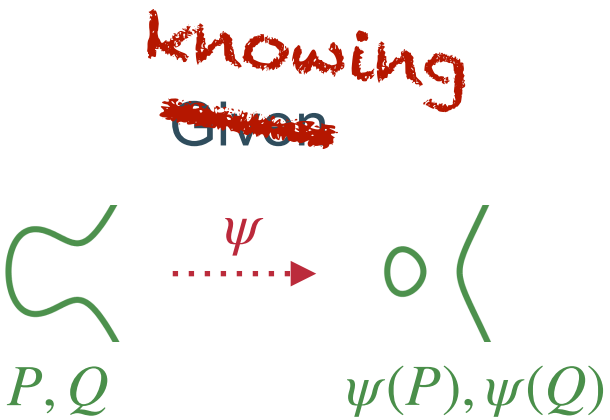
So what went wrong? right?



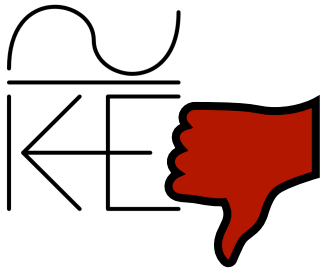
Applications

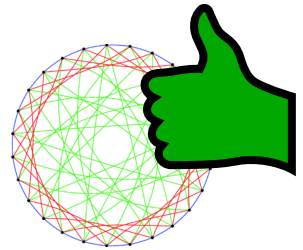


So what went wrong? right?

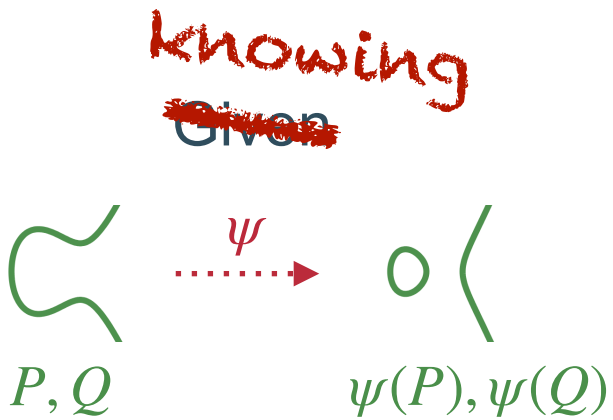


Applications

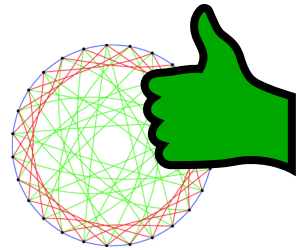




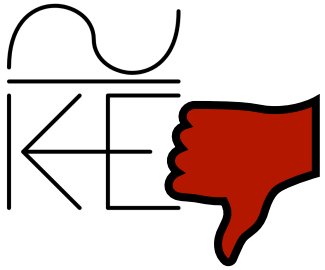
So what went wrong? right?

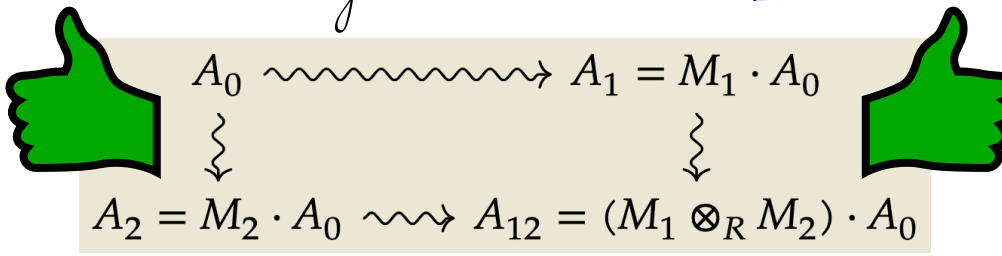


Applications



SQIsign





KU LEUVEN

Thank you

Want to see more isogenies? Visit https://isogeny.club
Questions?