SQIsign

Marius A. Aardal
Andrea Basso
Maria Corte-Real Santos
Max Duparc
Décio Luiz Gazzoni Filho
Antonin Leroux
Michael Meyer
Lorenz Panny
Giacomo Pope
Francisco Rodríguez-Henríquez
Gora Adj
Isaac Andrés Canales Martínez
Pierrick Dartois
Jonathan Komada Eriksen
Basil Hess
Patrick Longa
Kohei Nakagawa
Sikhar Patranabis
Krijn Reijnders
Sina Schaeffler
Diego F. Aranha
Jorge Chávez-Saab
Luca De Feo
Tako Boris Fouotsa
David Kohel
Luciano Maino
Hiroshi Onuki
Christophe Petit
Damien Robert
Benjamin Wesolowski

https://sqisign.org/

September 24-26, 2025
6th PQC Standardization Conference
NIST, Gaithersburg, USA


AARHUS
UNIVERSITY

amU
Aix Marseille Université

UNIVERSITY OF
BIRMINGHAM

EPFL

DGA

Radboud Universiteit

UEL

ULB

Université
de Rennes

UTokyo

University of
BRISTOL

cnrs

ENS DE LYON

ETH zürich

IBM

Inria

KU LEUVEN

Microsoft

TII
Technology
Innovation
Institute

TUM

TR

Short

Public Key	Signature	Security
66	148	NIST-1
98	222	NIST-3
130	294	NIST-5

Quaternion and **I**sogeny

Only candidate based on isogenies of supersingular elliptic curves

signature

Fiat-Shamir paradigm

Weren't isogenies broken?

Yes, SIKE was broken:

- Security based on isogeny problem with torsion point information;
- Very efficient classical algorithm to solve the SIKE problem found in 2022 (Castryck–Decru, Maino–Martindale, Robert);
- SQIsign v2 incorporates techniques developed in these attacks.

But isogenies live:

- The supersingular isogeny problem still is exponentially difficult for quantum computers;
- SQIsign's EUF-CMA reduces almost exactly to the supersingular isogeny problem;
- Breaks are part of life in cryptography.

Isogenies = algebraic group morphisms of elliptic curves

$$y^2 = x^3 + x \longrightarrow y^2 = x^3 + 1$$

Isogenies = algebraic group morphisms of elliptic curves

$$y^2 = x^3 + x \xrightarrow{\quad ?? \quad} y^2 = x^3 + 1$$

The isogeny problem

Given two isogenous curves, compute an isogeny between them.

For random supersingular curves defined over a finite field $\mathbb{F}_{p^2}$:

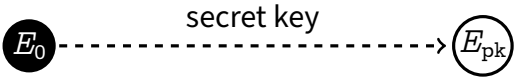
- Best classical attack in $p^{1/2+\epsilon}$ — Delfs–Galbraith, DCC 2016
- Best quantum attack in $p^{1/4+\epsilon}$ — Biasse–Jao–Sankar, Indocrypt 2014

Endomorphisms = Isogenies from a curve to itself

The supersingular endomorphism ring problem

Given a supersingular curve, compute a basis for its endomorphism ring

- Equivalent to the supersingular isogeny problem under (mostly tight) polynomial-time reductions
- Best algorithms = same as for the isogeny problem

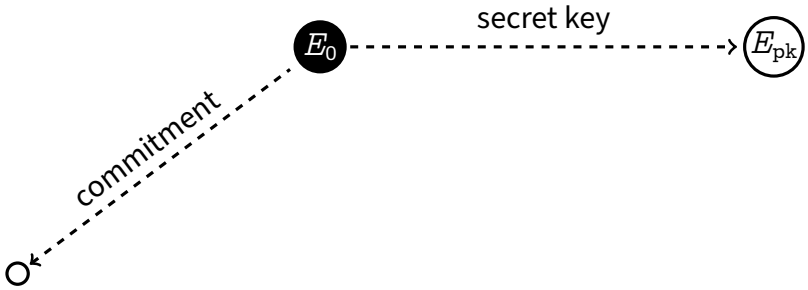


● Fixed curve: $y^2 = x^3 + x$

Legend:

⟶ public isogeny ⇢ secret isogeny

SQIsign's sigma-protocol

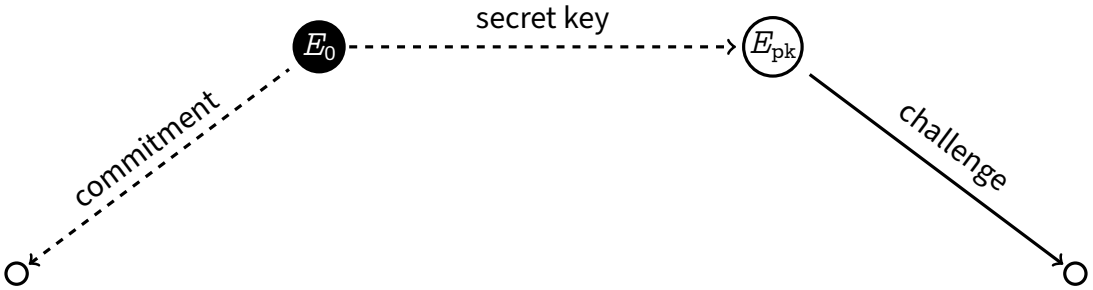


● Fixed curve: $y^2 = x^3 + x$

Legend:

⟶ public isogeny - - - -→ secret isogeny

SQIsign's sigma-protocol

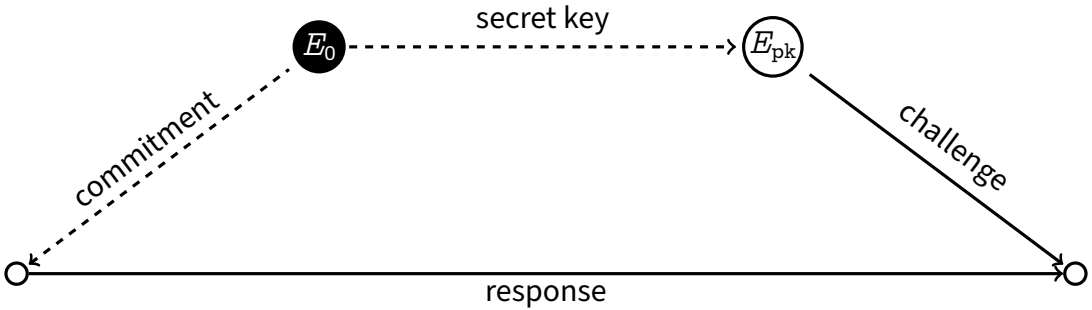


● Fixed curve: $y^2 = x^3 + x$

Legend:

⟶ public isogeny - - - → secret isogeny

SQIsign's sigma-protocol



● Fixed curve: $y^2 = x^3 + x$

Legend:

⟶ public isogeny ⇢ secret isogeny

Single choice: characteristic of the finite field

Constraint: $p + 1$ divisible by a large power of 2, for performance reasons

p	Security
$5 \cdot 2^{248} - 1$	NIST-1
$65 \cdot 2^{376} - 1$	NIST-3
$27 \cdot 2^{500} - 1$	NIST-5

All other pre-computed constants are easily explainable and provably do not affect security

Parameter set	KeyGen	Sign	Verify
Reference implementation (with default GMP installation)			
NIST-I	71.8	163.1	11.3
NIST-III	188.2	427.0	30.4
NIST-V	325.4	751.8	61.9
Reference implementation (with GMP `--disable-assembly`)			
NIST-I	84.4	203.1	11.3
NIST-III	227.9	548.9	30.5
NIST-V	402.6	1021.0	62.2
Assembly-optimized implementation for Intel Broadwell or later			
NIST-I	43.3	101.6	5.1
NIST-III	134.0	309.2	18.6
NIST-V	212.0	507.5	35.7

Performance in 10^6 CPU cycles on an Intel Core i7-13700K CPU.

Changes from Round 1

Before

“1D” paradigm
(De Feo–Kohel–Leroux–Petit–Wesolowski 2020)

Slow keygen and signing

Reduction to non-standard problem

More complex algorithms

After

“HD” paradigm
(Dartois–Leroux–Robert–Wesolowski 2023)

Fast

Reduction to “well-studied” problem

More complex mathematics

Endomorphism ring with hints (Aardal–Basso–De Feo–Patranabis–Wesolowski 2025)

Given:

- a random supersingular curve E,
- a polynomially-sized list of random isogenies of E of degree $< \sqrt{p}$,

compute the endomorphism ring of E.

Endomorphism ring problem

Given a random supersingular curve E, compute its endomorphism ring.

Endomorphism ring with hints (Aardal–Basso–De Feo–Patranabis–Wesolowski 2025)

Given:

- a random supersingular curve E,
- a polynomially-sized list of random isogenies of E of smooth degree $< \sqrt{p}$,

compute the endomorphism ring of E.

Endomorphism ring problem

Given a random supersingular curve E, compute its endomorphism ring.

“Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies”
Borin–Corte-Real Santos–Komada Eriksen–Invernizzi–Mula–Schaeffler–Vercauteren

- Simplifies key subroutine of SQIsign;
- Total speed-up between 10% and 80%;
- Reduced memory footprint;
- Removes some heuristics from security proof.

Summary

SQIsign advantages:

- Very small public keys and signatures (< RSA)
- Good performance
- Conservative assumption
- Still some potential for speed-ups
- Adds diversity to pq-signature portfolio

SQIsign disadvantages:

- 1-2 orders of magnitude slower than lattices ($\approx$ SPHINCS+)
- New assumption
- Constant-time implementation still a research topic