Modular Curves Creeping Up in Isogeny Problems

Luca De Feo

IBM Research Zürich

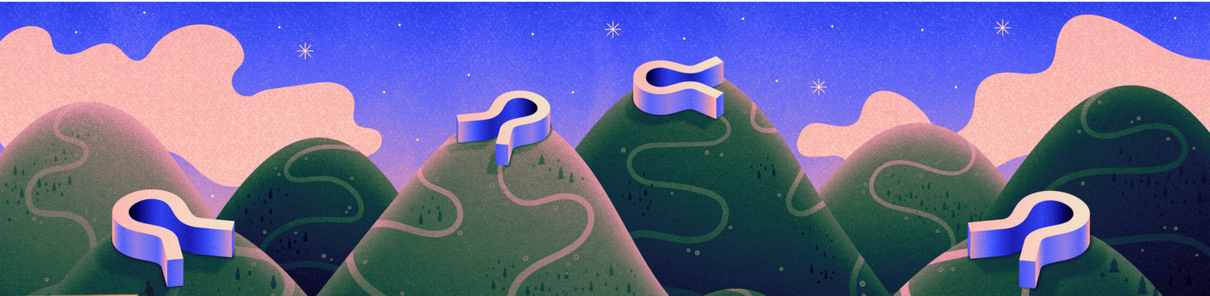
February 23, 2024

Università di Trento

CRYPTOGRAPHY

‘Post-Quantum’ Cryptography Scheme Is Cracked on a Laptop

Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.



In this paper, we introduce two such countermeasures based on partially hiding the isogeny degrees and torsion point information in the SIDH protocol. We present a preliminary analysis of the resulting schemes including non-trivial generalizations of prior attacks. Based on this analysis we suggest parameters for our M-SIDH variant with public key sizes of 4434, 7037 and 9750 bytes respectively for NIST security levels 1, 3, 5

Post-scriptum: Some months after this work was completed and made public, the SIDH assumption was broken in a series of papers by several authors. Hence, in the standard SIDH setting, some of the statements studied here now have trivial polynomial time non-interactive proofs. Nevertheless our first sigma protocol is unaffected by the attacks, and our second protocol may still be useful in present and future variants of SIDH that escape the attacks.

we stress that the attack relies crucially on the torsion point images exchanged by Alice and Bob, as well as on the knowledge of the degree of the secret isogeny. In particular, it cannot be adjusted in an obvious way to attack primitives that do not reveal this information, such as CRS/CSIDH [10], [39], [7] and SQISign [12], and the general supersingular isogeny path problem remains unaffected [44]. We forward the reader to an online project, initiated by De Feo, which attempts at organizing the most popular isogeny-based cryptographic protocols and their best classical and quantum attacks [14].

State-of-the-art. Protocols to prove knowledge of an isogeny have been mostly studied for signatures. The first such protocol is the SIDH-based proof of knowledge of [DFJP14]. Its security proof was found to be flawed and then fixed, either by changing the assumptions [GPV21] or by changing the protocol [DDGZ22]. However, these protocols are now fully broken by the recent polynomial time attacks on SIDH-like protocols [CD22, MMP+23, Rob22]. These attacks can be avoided by relying on ternary challenges [BKW20, DDGZ22].

In this paper, we introduce two such countermeasures based on partially hiding the isogeny degrees and torsion point information in the SIDH protocol. We present a preliminary analysis of the resulting schemes including non-trivial generalizations of prior attacks. Based on this analysis we suggest parameters for our M-SIDH variant with public key sizes of 4434, 7037 and 9750 bytes respectively for NIST security levels 1, 3, 5

Post-scriptum: Some months after this work was completed and made public, the SIDH assumption was broken in a series of papers by several authors. Hence, in the standard SIDH setting, some of the statements studied here now have trivial polynomial time non-interactive proofs. Nevertheless our first sigma protocol is unaffected by the attacks, and our second protocol may still be useful in present and future variants of SIDH that escape the attacks.

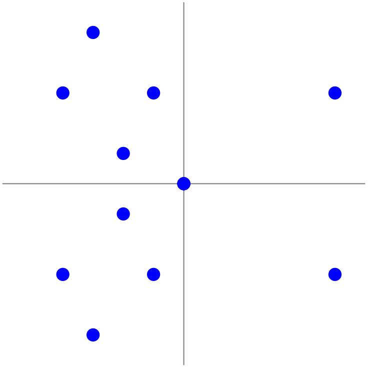
we stress that the attack relies crucially on the torsion point images exchanged by Alice and Bob, as well as on the knowledge of the degree of the secret isogeny. In particular, it cannot be adjusted in an obvious way to attack primitives that do not reveal this information, such as CRS/CSIDH [10], [39], [7] and SQISign [12], and the general supersingular isogeny path problem remains unaffected [44]. We forward the reader to an online project, initiated by De Feo, which attempts at organizing the most popular isogeny-based cryptographic protocols and their best classical and quantum attacks [14].

State-of-the-art. Protocols to prove knowledge of an isogeny have been mostly studied for signatures. The first such protocol is the SIDH-based proof of knowledge of [DFJP14]. Its security proof was found to be flawed and then fixed, either by changing the assumptions [GPV21] or by changing the protocol [DDGZ22]. However, these protocols are now fully broken by the recent polynomial time attacks on SIDH-like protocols [CD22, MMP+23, Rob22]. These attacks can be avoided by relying on ternary challenges [BKW20, DDGZ22].

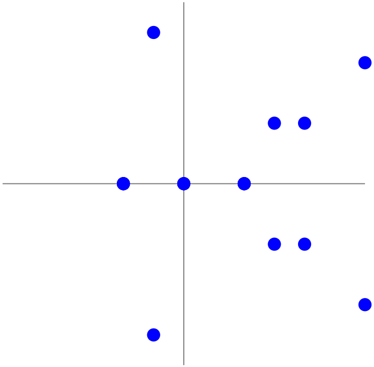
https://issikebrokenyet.github.io/

Isogenies

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

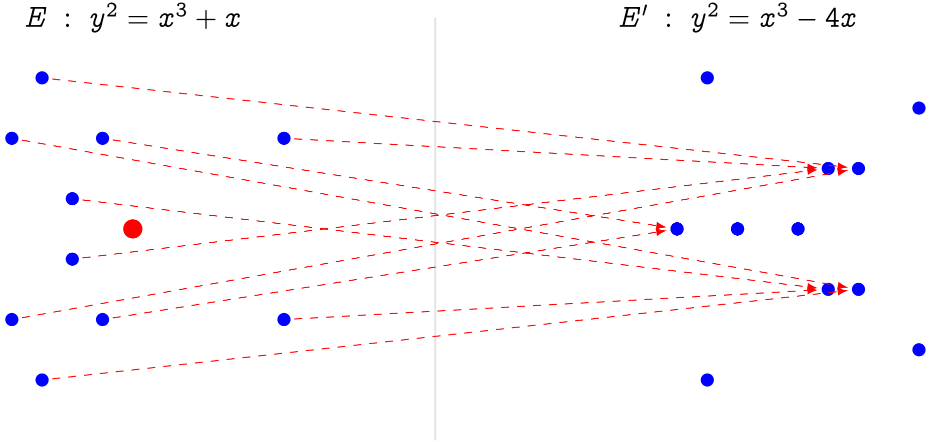


$$E' \ : \ y^2 = x^3 - 4x$$



$$\phi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2} \right)$$

Isogenies



$$\phi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

The isogeny problem

E E'

The isogeny problem

$$E \xrightarrow{\quad ?? \quad} E'$$

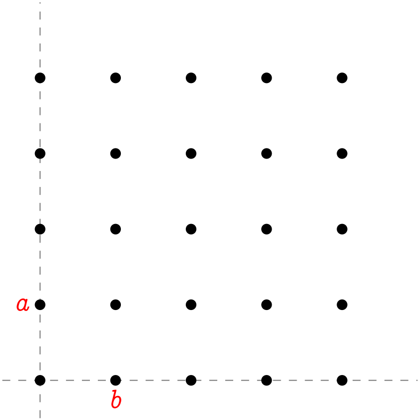
The isogeny problem

$$j(E) \xrightarrow{\quad ?? \quad} j(E')$$

Torsion

Over an algebraically closed field, for any N coprime to the characteristic:

$$E[N] \simeq \mathbb{Z}/N \times \mathbb{Z}/N$$



Isogeny problem with Torsion point information (SIDH)

$$E \xrightarrow{\quad ?? \quad} E'$$

Isogeny problem with Torsion point information (SIDH)

$$E[N] \xrightarrow{\quad ?? \quad} E'[N]$$

Isogeny problem with Torsion point information (SIDH)

$$\langle P, Q\rangle = E[N] \xrightarrow[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]{??} E'[N] = \langle P', Q'\rangle$$

Theorem (Robert)

Let E, E' be elliptic curves, let $\phi : E \to E'$ be an isogeny of degree d and let N be a smooth integer coprime to d such that $N^2 > d$.

There exists a polynomial time algorithm that, given E, E', d, N, a basis (P, Q) of $E[N]$ and its image $(\phi(P), \phi(Q))$ under ϕ, computes ϕ.

Γ-SIDH problems

Level structure = basis of $E[N]$ up to linear transformations $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}/N)$

$$\langle P, Q \rangle \xrightarrow[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]{??} \langle P', Q' \rangle$$

Γ-SIDH problems

Level structure = basis of $E[N]$ up to linear transformations $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}/N)$

$$\langle P, Q\rangle \xrightarrow[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\cdot\Gamma]{??} \langle P', Q'\rangle$$

Weil pairing

$$e_N\left(\phi(P), \phi(Q)\right)^{ad-bc} = e_N(aP + cQ, bP + dQ)^{\deg \phi}$$

Some examples of level structures

Restricting to $\Gamma \subset \mathrm{SL}_2(\mathbb{Z}/N)$:

$\Gamma = \{\left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right)\}$: A basis (P, Q) of $E[N]$, plain SIDH.

$\Gamma = \{\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)\}$: Two cyclic subgroups $\langle P\rangle$ and $\langle Q\rangle$ of order N.

$\Gamma_1 = \{\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)\}$: A point P of order N.

$\Gamma_0 = \{\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)\}$: A cyclic group $\langle P\rangle$ of order N.

$\{\begin{pmatrix} * & * \\ & * \end{pmatrix}\}$-SIDH and $\{\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}\}$-SIDH

Curve + cyclic subgroup		Curve + isogeny
$E, \langle P \rangle$	$=$	$\begin{array}{c} E \\ \downarrow \\ E/\langle P \rangle \end{array}$

$\left\{\begin{pmatrix} * & * \\ & * \end{pmatrix}\right\}$-SIDH and $\left\{\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}\right\}$-SIDH

$$\begin{tikzcd}
E \arrow[rr, dashed, "\phi"] \arrow[d] & & E' \arrow[d] \\
E/\langle P\rangle & & E'/\langle\phi(P)\rangle
\end{tikzcd}$$

Distinguishing $\left\{\begin{pmatrix} * & * \\ & * \end{pmatrix}\right\}$-problem aka Decisional SuperSingular Product (DSSP)...

$\left\{\begin{pmatrix} * & * \\ & * \end{pmatrix}\right\}$-SIDH and $\left\{\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}\right\}$-SIDH

$$\begin{tikzcd}
E \arrow[r, dashed, "\phi"] \arrow[d] & E' \arrow[d] \\
E/\langle P\rangle & E'/\langle \phi(P)\rangle
\end{tikzcd}$$

Distinguishing $\left\{\begin{pmatrix} * & * \\ & * \end{pmatrix}\right\}$-problem aka Decisional SuperSingular Product (DSSP)...

...but careful not to reveal $(E, P, E', \phi(P))$ instead!

A reduction (say $N = n^2$)

$$(E, P) \xrightarrow{\ \phi\ } (E', \alpha\phi(P)) \qquad \begin{pmatrix} \alpha & * \\ & \alpha^{-1} \end{pmatrix}$$

A reduction (say $N = n^2$)

$$
\begin{tikzcd}
E \arrow[r, dashed, "\phi"] \arrow[d] & E' \arrow[d] \\
E/\langle nP\rangle \arrow[d] & E'/\langle n\alpha\phi(P)\rangle \arrow[d] \\
E/\langle P\rangle & E'/\langle \alpha\phi(P)\rangle
\end{tikzcd}
\qquad
\begin{pmatrix} \alpha & * \\ & \alpha^{-1} \end{pmatrix}
$$

A reduction (say $N = n^2$)

$$\begin{tikzcd}
E & & E' \\
E/\langle nP\rangle \arrow[u] \arrow[d] \arrow[rr, dashed, "\phi'"] & & E'/\langle n\alpha\phi(P)\rangle \arrow[u] \arrow[d] \\
E/\langle P\rangle & & E'/\langle \alpha\phi(P)\rangle
\end{tikzcd}$$

$$\begin{pmatrix} \alpha & * \\ & \alpha^{-1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha & n* \\ n* & \alpha^{-1} \end{pmatrix}$$

A reduction (say $N = n^2$)

$$\begin{tikzcd}
E & & E' \\
E/\langle nP\rangle \arrow[u] \arrow[d] \arrow[rr, dashed, "\phi'"] & & E'/\langle n\alpha\phi(P)\rangle \arrow[u] \arrow[d] \\
E/\langle P\rangle & & E'/\langle\alpha\phi(P)\rangle
\end{tikzcd}$$

$$\begin{pmatrix} \alpha & * \\ & \alpha^{-1} \end{pmatrix}$$

$$\begin{pmatrix} \alpha & n* \\ n* & \alpha^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} \mod n$$

A reduction

$$
\begin{tikzcd}
& \text{SIDH} \arrow[dl] \arrow[dr] & \\
\begin{pmatrix}1 & *\\ & 1\end{pmatrix} \arrow[ddr] \arrow[ur, dashed, bend left] & & \begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} \arrow[d] \arrow[ul, dotted, bend right] \\
& & \begin{pmatrix}* & \\ & *\end{pmatrix} \arrow[dl] \\
& \begin{pmatrix}* & *\\ & *\end{pmatrix} \arrow[ur, dashed, bend right] &
\end{tikzcd}
$$

$\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}$-SIDH

Harder than SIDH when N has many prime factors?

See Fouotsa, Moriya, Petit – Eurocrypt 2023.

CSIDH $\to \begin{pmatrix} * & \\ & * \end{pmatrix}$-SIDH

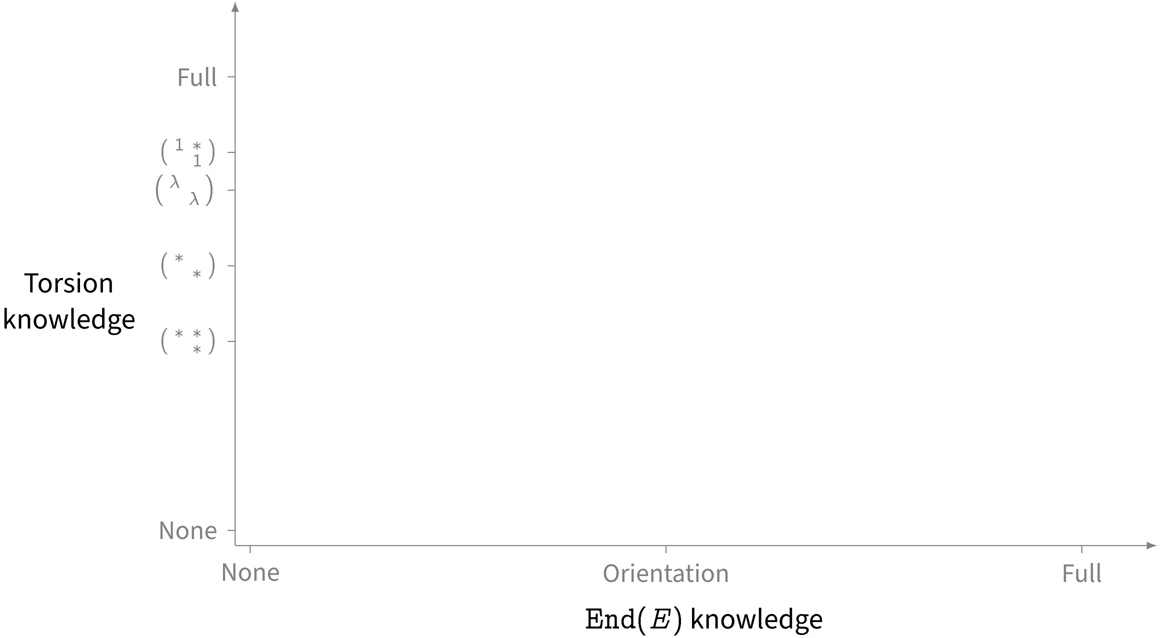
$$
\begin{tikzcd}
E \arrow[loop above, "\pi"] \arrow[r, dashed, "\phi"] & E' \arrow[loop above, "\pi'"]
\end{tikzcd}
$$

CSIDH $\to \begin{pmatrix} * & \\ & * \end{pmatrix}$-SIDH

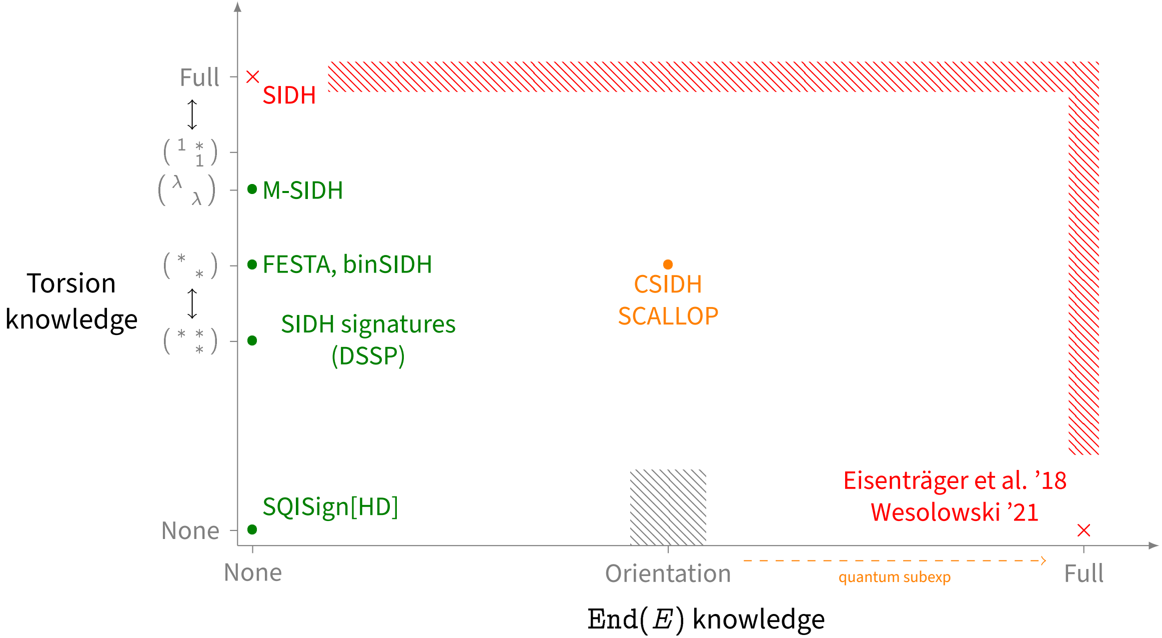
$$\begin{tikzcd} E \arrow[rrr, dashed, "\phi"] \arrow[loop above, "\pi"] & & & E' \arrow[loop above, "\pi'"] \end{tikzcd}$$

$$\pi|\langle P, Q\rangle = \begin{pmatrix} \lambda & \\ & -1/\lambda \end{pmatrix} \qquad \pi'|\langle P', Q'\rangle = \begin{pmatrix} \lambda & \\ & -1/\lambda \end{pmatrix}$$

Frobenius diagonalizes on $E[N]$ for every prime N s.t. $\left(\frac{-p}{N}\right) = 1$.



Full
$\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$
$\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}$
$\begin{pmatrix} * & \\ & * \end{pmatrix}$
Torsion knowledge
$\begin{pmatrix} * & * \\ & * \end{pmatrix}$
None
None
Orientation
Full
$\mathrm{End}(E)$ knowledge


Full
SIDH
M-SIDH
FESTA, binSIDH
SIDH signatures
(DSSP)
CSIDH
SCALLOP
Torsion
knowledge
None
SQISign[HD]
Eisenträger et al. ’18
Wesolowski ’21
None
Orientation
quantum subexp
Full
End(E) knowledge

Thank you

`https://defeo.lu/`

@luca_defeo@ioc.exchange

@luca_defeo