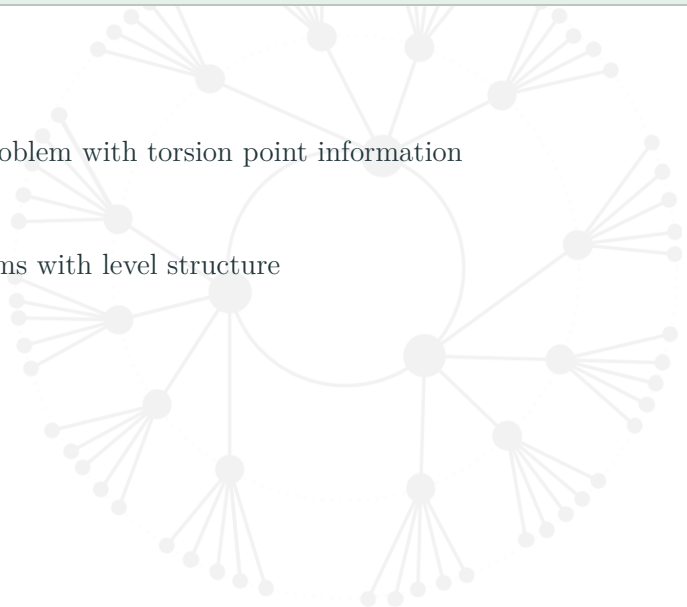
Isogeny Problems with Level Structure

[1]Luca De Feo, [2]Tako Boris Fouotsa, [3]Lorenz Panny

[1]IBM Research Europe, [2]EPFL Lausanne, [3]TU Munich

Eurocrypt, May 26-30 2024, Zürich, Switzerland

Outline



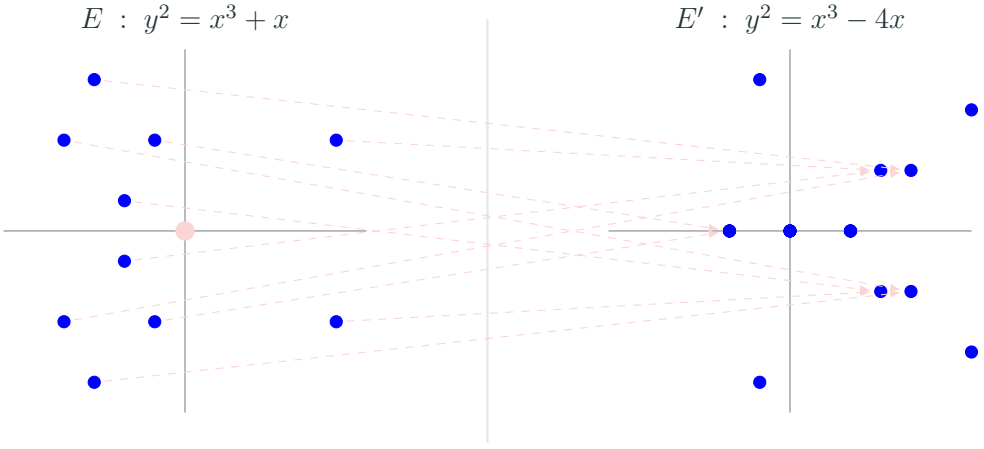
The isogeny problem with torsion point information

Isogeny problems with level structure

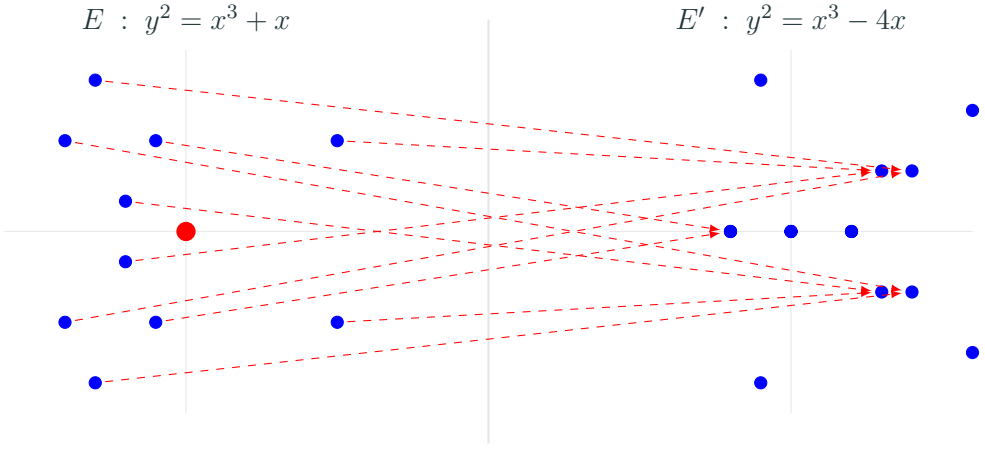
A reduction

The isogeny problem with torsion point information

Isogenies



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.

Pure isogeny problem

Pure isogeny problem: *given two (isogenous) elliptic curves E' and E', compute an isogeny $\phi : E \to E'$.*

The genesis of torsion point information

First isogeny-based key exchange (CRS[1]): class group actions on ordinary curves.

Isogeny group actions are subject to quantum sub-exponential attacks.

Jao and De Feo (SIDH 2011): use supersingular isogenies.

Caveat: supersingular isogenies do not commute in general.

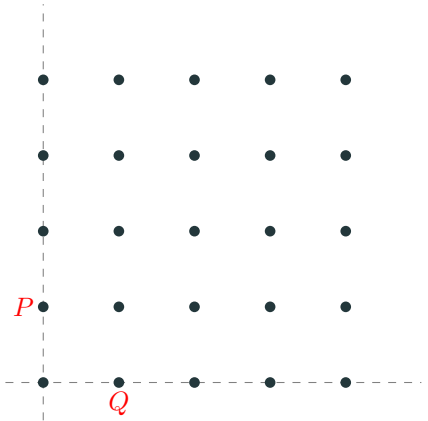
Solution: reveal the images of some torsion points.

[1] Couveignes 1997, Rostovtsev and Stolbunov 2006.

Torsion

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

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

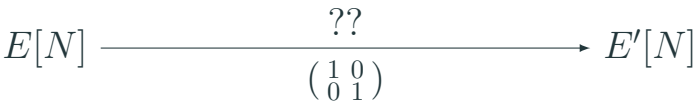


Isogeny problem with torsion point information (SIDH)

$$E, P, Q \xrightarrow{\quad ?? \quad} E', P', Q'$$

$E[N] = \langle P, Q \rangle$, $P' := \phi(P), Q' := \phi(Q)$

Isogeny problem with torsion point information (SIDH)

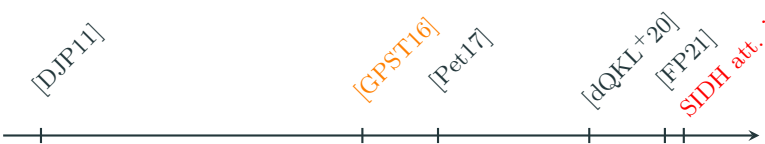


Fixing $\langle P, Q \rangle = E[N]$ and $\langle \phi(P), \phi(Q) \rangle = E'[N]$

Torsion point attacks

Non exhaustive list: BdQL+ 2019, ...

Torsion point attacks



Torsion point information!!

SIDH att. '22: [CD22, MMP+23, Rob22]

Torsion point attacks

Torsion point information!!

SIDH att. '22: [CD22, MMP+23, Rob22]

SIDH attacks (Robert's version)

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.

Isogeny problems with level structure

Γ-SIDH problems (isogeny problems with level structure)

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

$$E[N] \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)]{??} E'[N]$$

Fixing $\langle P, Q\rangle = E[N]$ and $\langle \phi(P), \phi(Q)\rangle = E'[N]$

Γ-SIDH problems (isogeny problems with level structure)

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

$$E[N] \xrightarrow[\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \cdot \Gamma]{??} E'[N]$$

Fixing $\langle P, Q\rangle = E[N]$ and $\langle \phi(P), \phi(Q)\rangle = E'[N]$

Some examples of level structures

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

$\Gamma = \{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}\}$: Image of a basis (P, Q) of $E[N]$ up to scalar; M-SIDH.

$\Gamma = \{\begin{pmatrix} * & \\ & * \end{pmatrix}\}$: Images of two cyclic subgroups $\langle P \rangle$ and $\langle Q \rangle$ of order N; isogeny group actions (CSIDH et al., SCALLOP et al., ...), binSIDH, terSIDH, ...

$\Gamma_1 = \{\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}\}$: Image of a point P of order N.

$\Gamma_0 = \{\begin{pmatrix} * & * \\ & * \end{pmatrix}\}$: Images of a cyclic group $\langle P \rangle$ of order N; SIDH signatures.

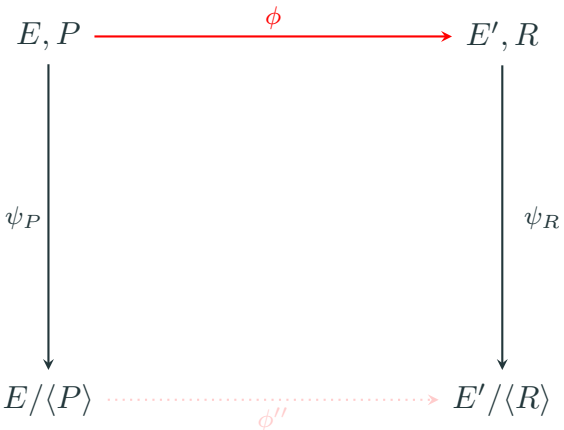
A reduction

A reduction

The Γ_1-SIDH problem (of level N)

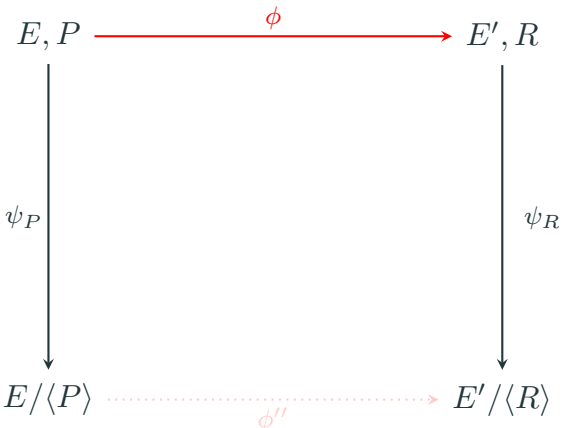
$$E, P \xrightarrow{\phi} E', R = \phi(P)$$

A reduction



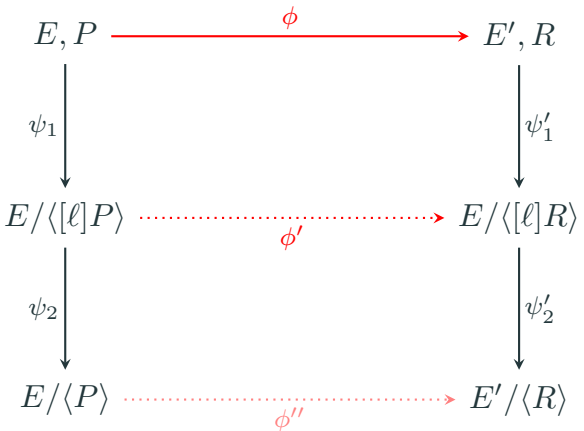
A reduction

Now, let us assume that $N = \ell^2$ is a square.



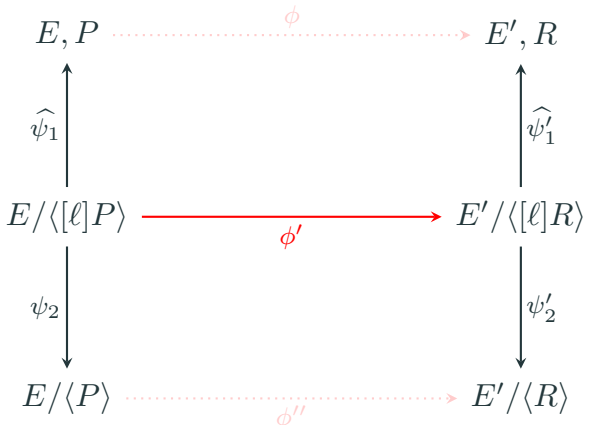
A reduction

Now, let us assume that $N = \ell^2$ is a square.



A reduction

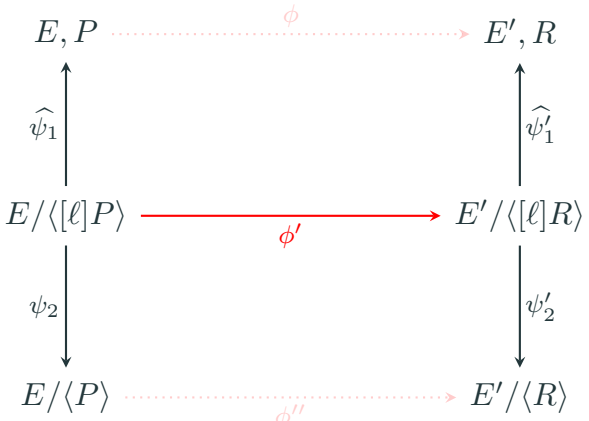
Now, let us assume that $N = \ell^2$ is a square.



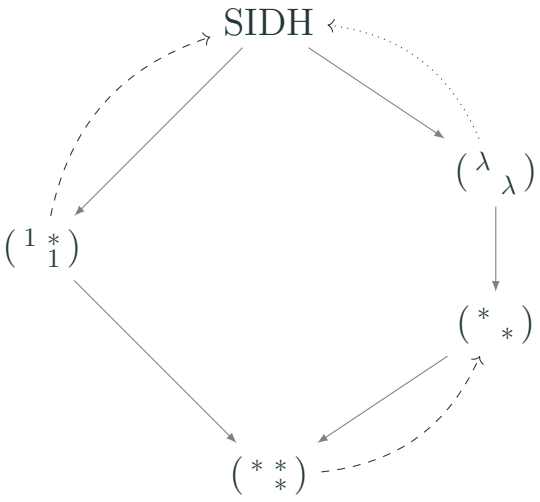
You recover the action of ϕ' on the ℓ-torsion using pairings and DLPs.

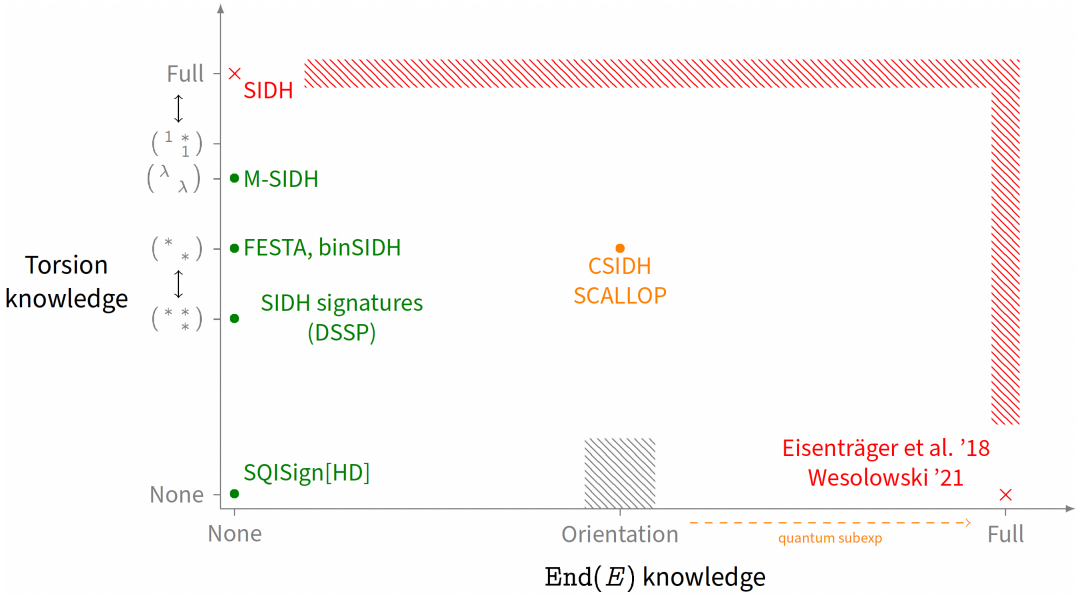
A reduction

The (plain) SIDH problem (of level $\ell = \sqrt{N}$)



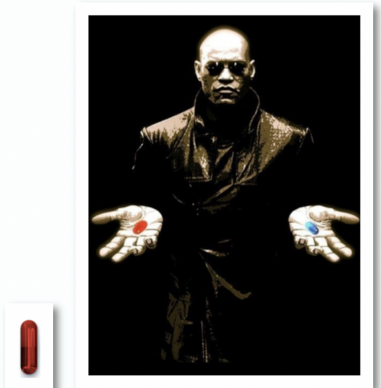
Some reductions




Full
$\begin{pmatrix} 1 & * \\ 1 & \end{pmatrix}$
$\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}$
$\begin{pmatrix} * & \\ & * \end{pmatrix}$
$\begin{pmatrix} * & * \\ & * \end{pmatrix}$
None
Torsion knowledge
SIDH
M-SIDH
FESTA, binSIDH
SIDH signatures (DSSP)
SQISign[HD]
CSIDH
SCALLOP
Eisenträger et al. ’18
Wesolowski ’21
None
Orientation
quantum subexp
Full
End(E) knowledge

Let's stop here and have lunch.

But before that, you have to choose your pill!




Wouter Castryck and Thomas Decru.
An efficient key recovery attack on SIDH.
Cryptology ePrint Archive, Paper 2022/975, 2022.
https://eprint.iacr.org/2022/975.


Luca De Feo, David Jao, and Jérôme Plût.
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
Cryptology ePrint Archive, Paper 2011/506, 2011.
https://eprint.iacr.org/2011/506.

Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange.
Improved torsion-point attacks on SIDH variants.
Cryptology ePrint Archive, Paper 2020/633, 2020.
https://eprint.iacr.org/2020/633.

Tako Boris Fouotsa and Christophe Petit.
A new adaptive attack on SIDH.
Cryptology ePrint Archive, Paper 2021/1322, 2021.
https://eprint.iacr.org/2021/1322.

Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti.
On the security of supersingular isogeny cryptosystems.
Cryptology ePrint Archive, Paper 2016/859, 2016.
https://eprint.iacr.org/2016/859.

Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski.
A direct key recovery attack on SIDH.
Cryptology ePrint Archive, Paper 2023/640, 2023.
https://eprint.iacr.org/2023/640.

Christophe Petit.
Faster algorithms for isogeny problems using torsion point images.
Cryptology ePrint Archive, Paper 2017/571, 2017.
https://eprint.iacr.org/2017/571.

Damien Robert.
Breaking SIDH in polynomial time.
Cryptology ePrint Archive, Paper 2022/1038, 2022.
https://eprint.iacr.org/2022/1038.