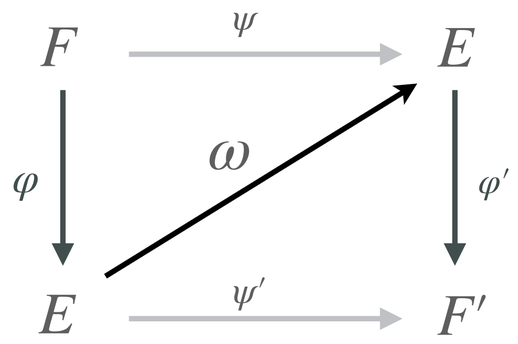
PART 4

2D Future

Nakagawa - Onuki trick (2023)



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

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

1

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

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

2

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

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

3

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

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

Clapoti(s)

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

PART 4

2D Future

SQIsign

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

SQIsign2

A new algorithm to translate ideals to isogenies.

AprèsSQI

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

The SIKE breaks

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

SQIsignHD

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

Going 2D

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