PART 2

The BREAK

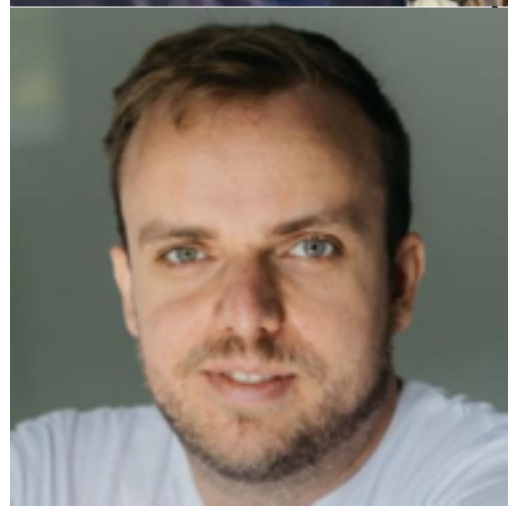
Castryck & Decru (2022)

$$\begin{tikzcd} E_0 \arrow[r, "\psi"] \arrow[d, "\varphi"'] & E_A \arrow[d, "\varphi'"] \\ E_B \arrow[r, "\psi'"] & E_{AB} \end{tikzcd}$$

in SIDH/SIKE the secrets are φ and ψ

we are given $\deg \varphi$, $\deg \psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg \varphi + \deg \psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PROBLEM!

degree of Φ is then $\deg \varphi + \deg \psi$ making Φ difficult/impossible to compute in practice...

Solution!

use knowledge of $\mathrm{End}(E_0)$ to modify the square so that Φ is of degree 2^n, then compute Φ easily

PART 2

The BREAK

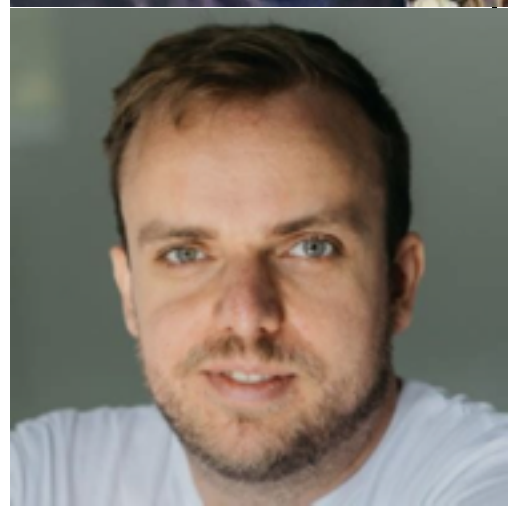
Castryck & Decru (2022)

$$\begin{tikzcd} E_0 \arrow[r, "\psi"] \arrow[d, "\varphi"'] & E_A \arrow[d, "\varphi'"] \\ E_B \arrow[r, "\psi'"] & E_{AB} \end{tikzcd}$$

in SIDH/SIKE the secrets are φ and ψ

we are given $\deg \varphi$, $\deg \psi$ and *precisely* $\varphi(P), \psi(P)$ for the points $P \in E_0$ of order $\deg \varphi + \deg \psi$

Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PROBLEM!

degree of Φ is then $\deg \varphi + \deg \psi$ making Φ difficult/impossible to compute in practice...

Solution!

use knowledge of $\mathrm{End}(E_0)$ to modify the square so that Φ is of degree 2^n, then compute Φ easily

Robert (2022)

generalize Kani's lemma:
don't just embed 1D into 2D,
embed into 4D or 8D!
Then Φ easy to compute
and we don't need $\mathrm{End}(E_0)$