PART 2

The BREAK

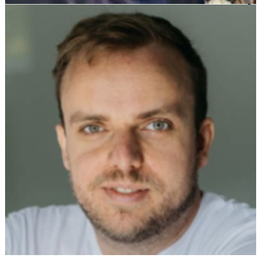
Castryck & Decru (2022)

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi} & E_A \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_B & \xrightarrow{\psi'} & E_{AB} \end{array}$$

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...

PART 2

The BREAK

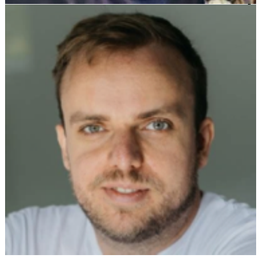
Castryck & Decru (2022)

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi} & E_A \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_B & \xrightarrow{\psi'} & E_{AB} \end{array}$$

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