PART 2

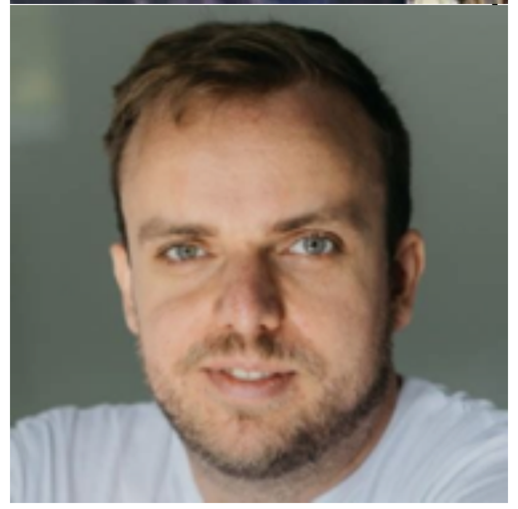
The BREAK

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 $\deg \varphi + \deg \psi$



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.