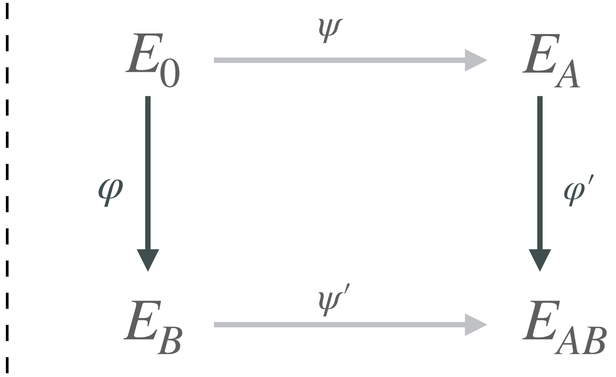
PART 2

The BREAK

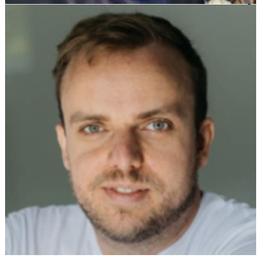
Castryck & Decru (2022)



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 $\deg\varphi + \deg\psi$

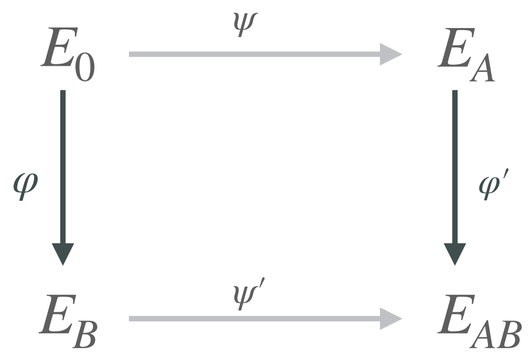
Kani's lemma directly applies!
Knowing Φ gives us φ, ψ.



PART 2

The BREAK

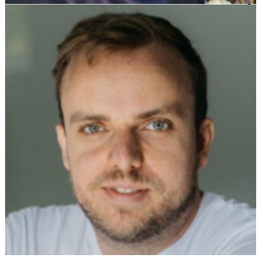
Castryck & Decru (2022)



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...