PART 2

The BREAK

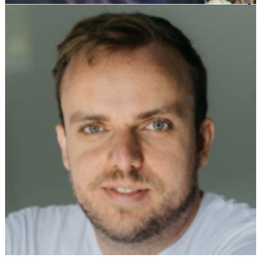
Castryck & Decru (2022)

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

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

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 $\mathrm{End}(E_0)$

2 Best Papers EUROCRYPT 2024

Kongresssaal

Marc Joye and Gregor Leander

Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis

Itai Dinur

(paper #326)

Show abstract ›

PART 3: New Dimensions

SQIsignHD: New Dimensions in Cryptography

Pierrick Dartois, Antonin Leroux, Damien Robert, Benjamin Wesolowski

INRIA, IMB, DGA-MI, ENS de Lyon, CNRS, UMPA

Speaker(s): Pierrick Dartois

(paper #149)

Show abstract ›

AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing

Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, Krijn Reijnders

University College London, NTNU, University of Regensburg, Radboud University Nijmegen

Speaker(s): Jonathan Komada Eriksen

(paper #86)

Show abstract ›