3 Best Papers EUROCRYPT 2023

Lyon Congress Center - Plenary - Auditorium Lumière

Session chair: Joppe Bos

YouTube

An Efficient Key Recovery Attack on SIDH

Best Paper Award

Wouter Castryck, Thomas Decru

KU Leuven

Speaker(s): Thomas Decru

Show abstract ›

(paper #409) Media:

PART 2: The BREAK.

Breaking SIDH in Polynomial Time

Honourable Mention

Damien Robert

Inria Bordeaux

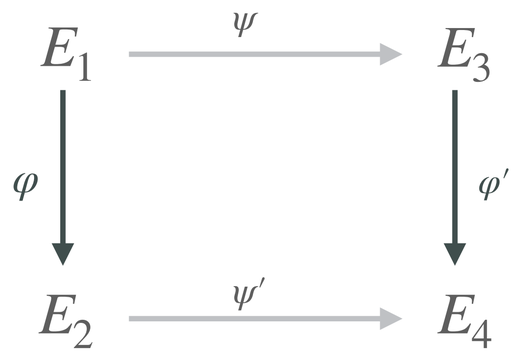
Show abstract ›

(paper #96) Media:

PART 2

The BREAK

Kani's Lemma (1997)



if $\deg \varphi = \deg \varphi'$
and $\deg \psi = \deg \psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$