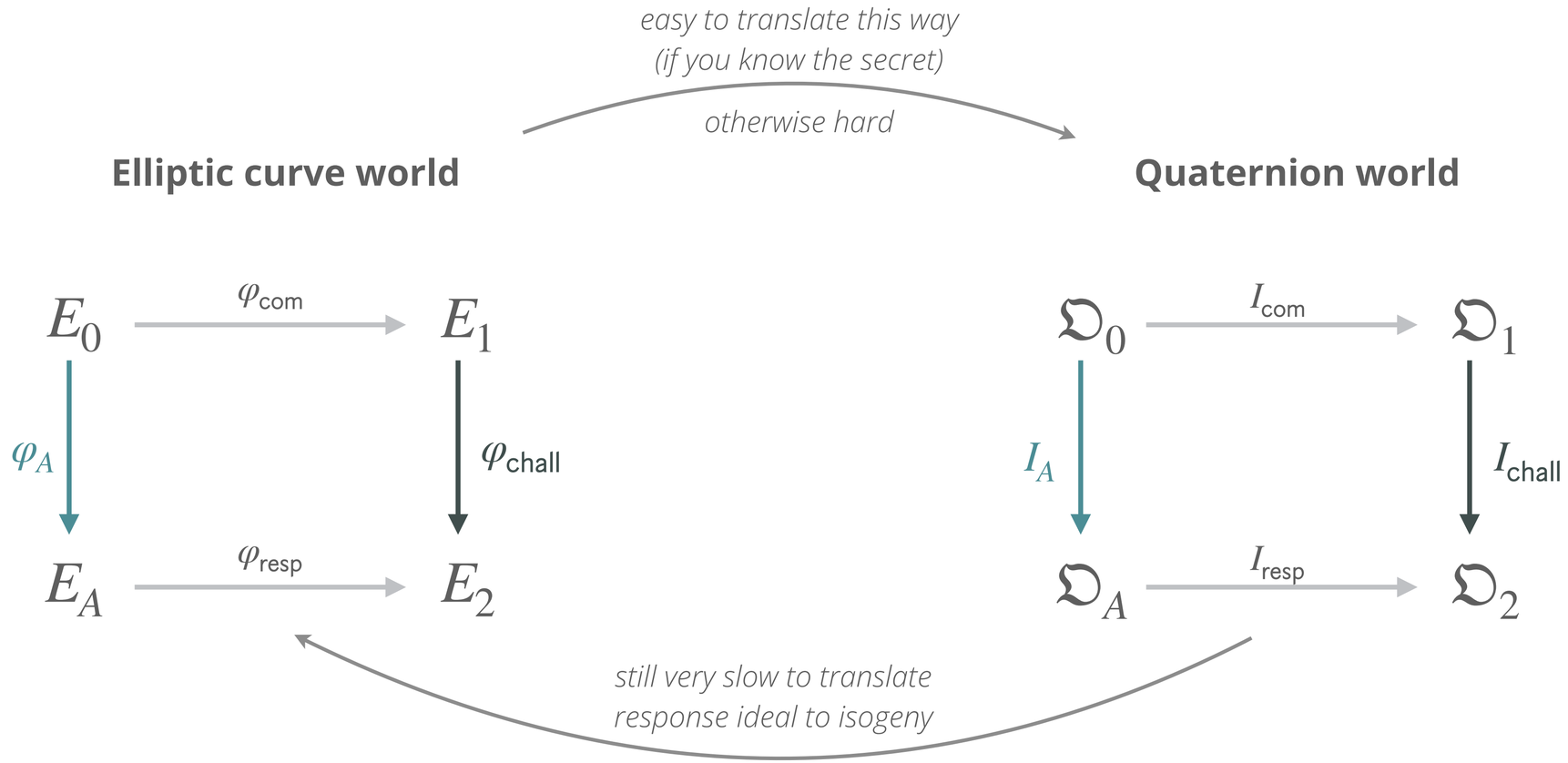
PART 1

SQIsign



problem

need to break up $E_A \to E_2$ into smaller blocks
$E_A \to E^{(1)} \to E^{(2)} \to \ldots \to E^{(n-1)} \to E^{(n)} = E_2$
translating to the right blocks is very slow...
(NIST SQIsign has 13 blocks)

SQIsign2

among others, a much better way
to translate I_{resp} back to φ_{resp}
improving speed **per block**

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: