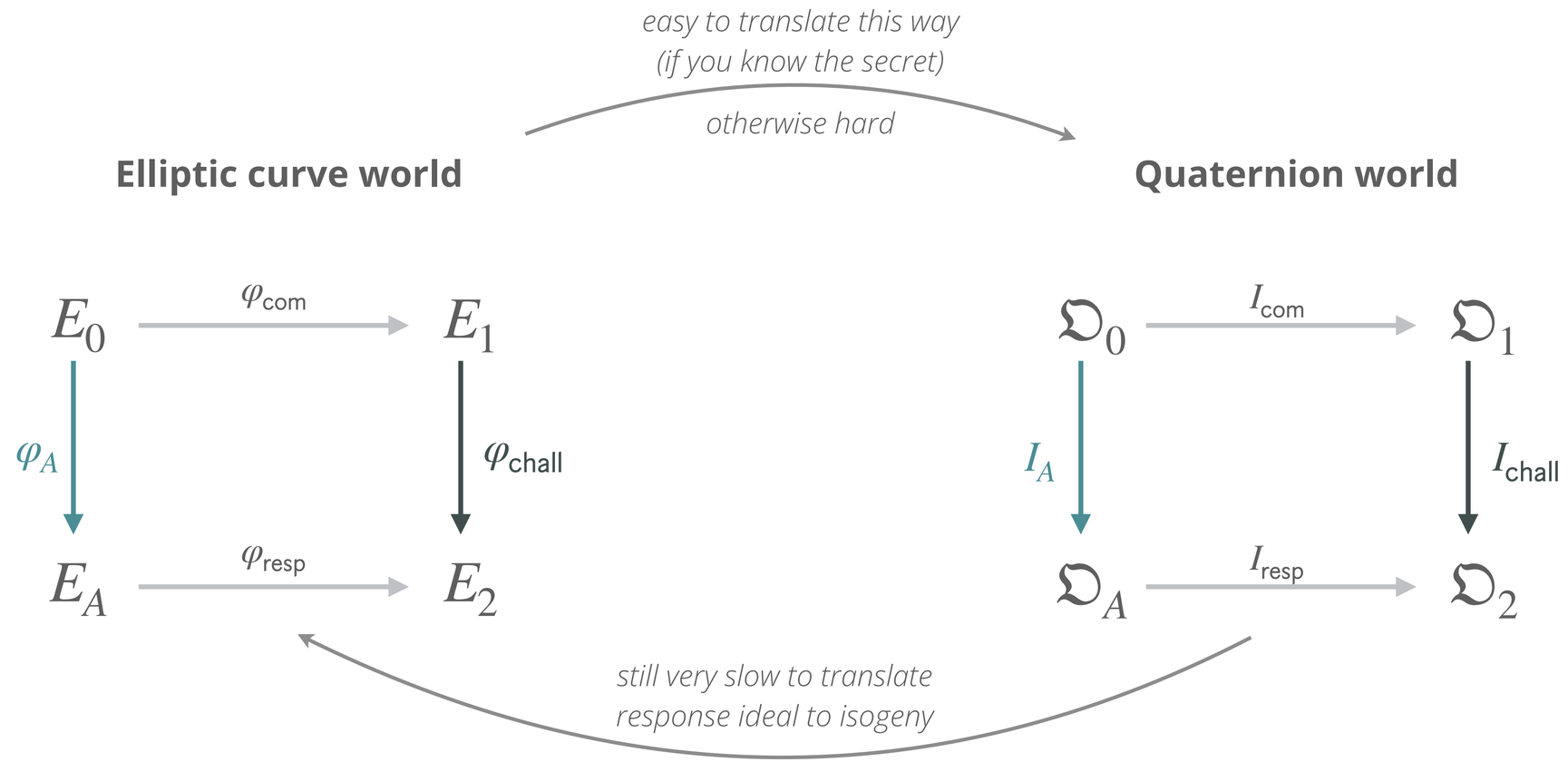
PART 1

SQIsign



problem

need to break up $E_A \to E_2$ into smaller blocks

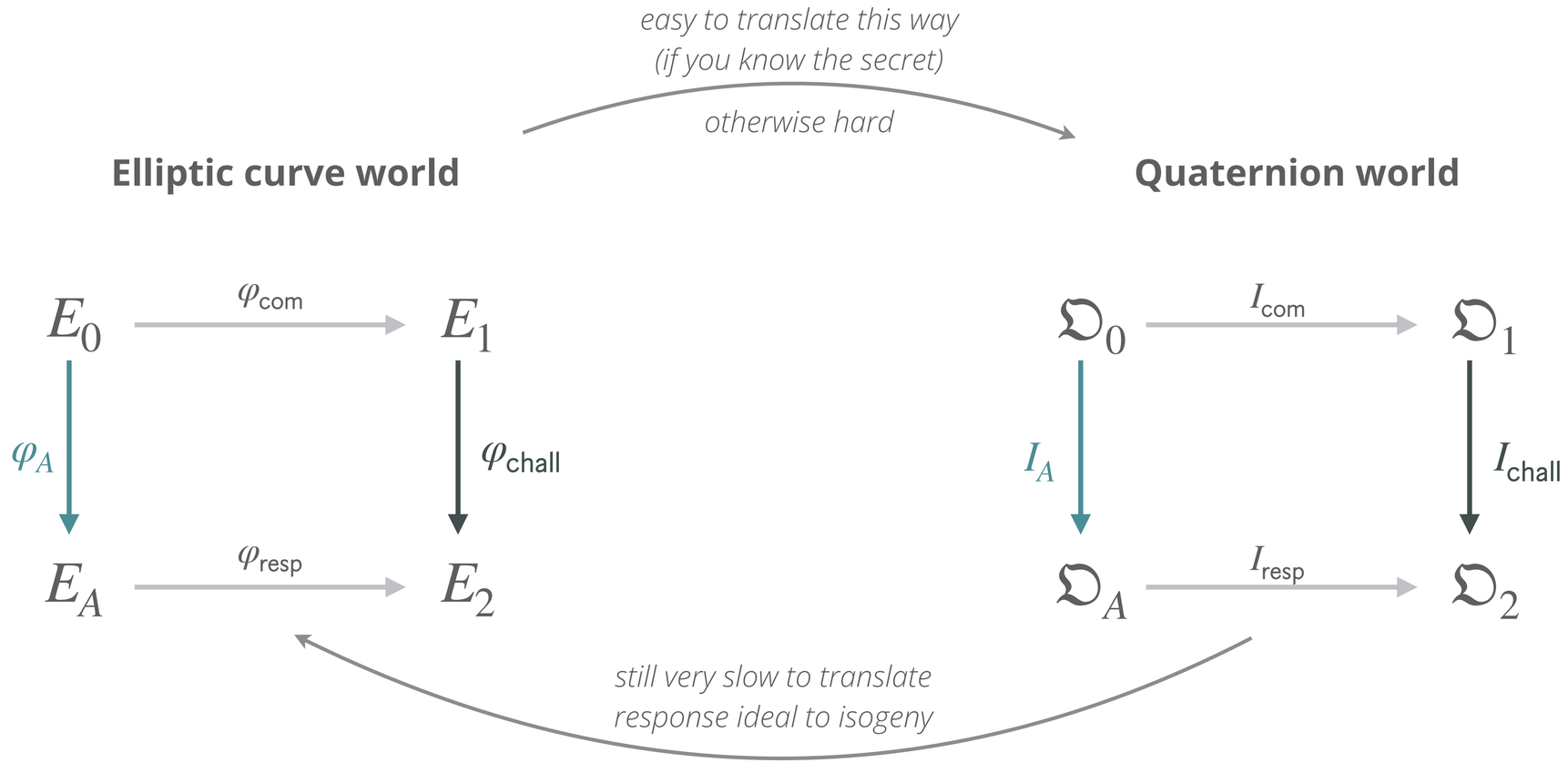
$E_A \to E^{(1)} \to E^{(2)} \to \ldots \to E^{(n-1)} \to E^{(n)} = E_2$

translating to the right blocks is very slow...

(NIST SQIsign has 13 blocks)

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**