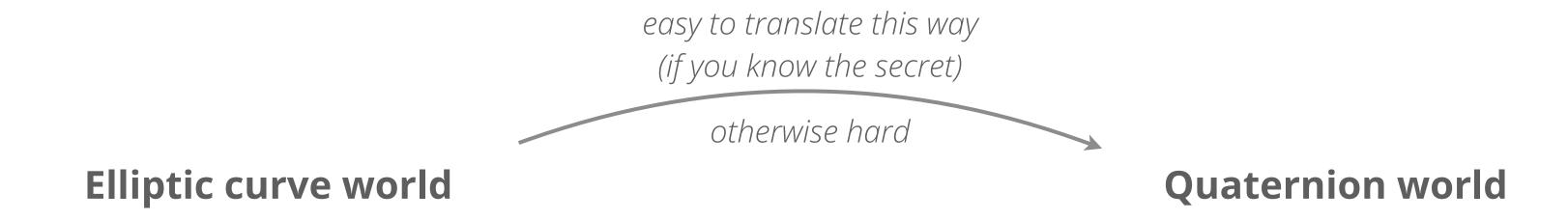
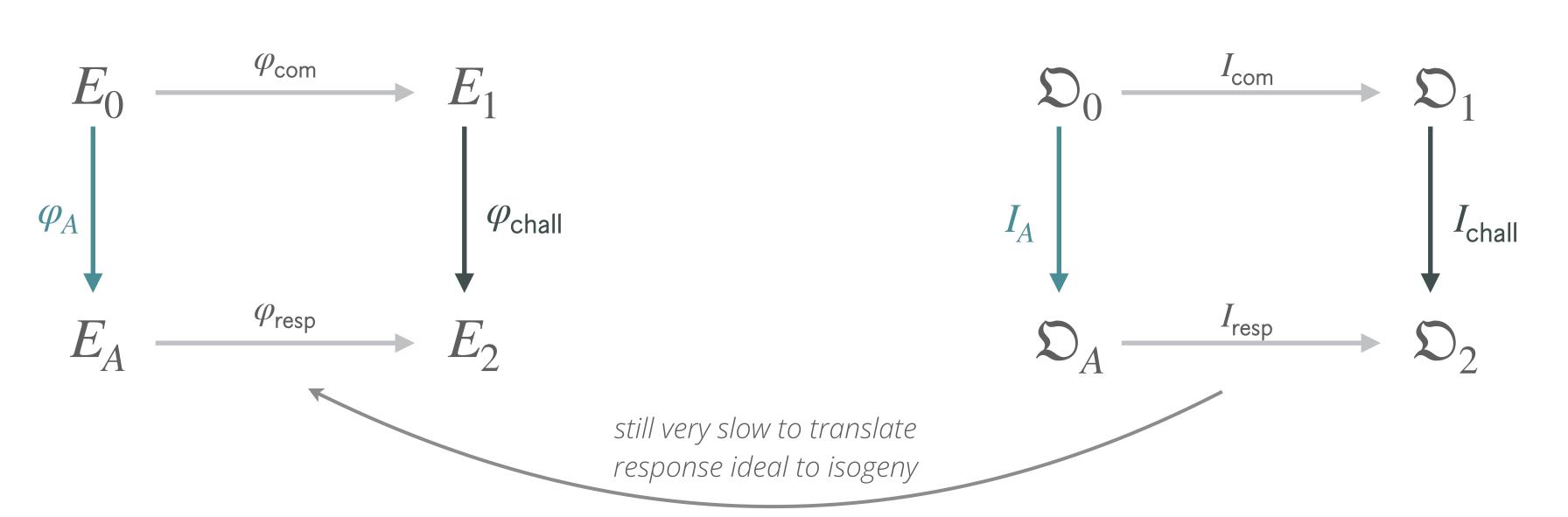
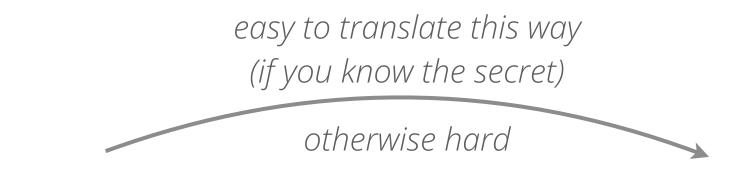
# PART 1 SQIsign



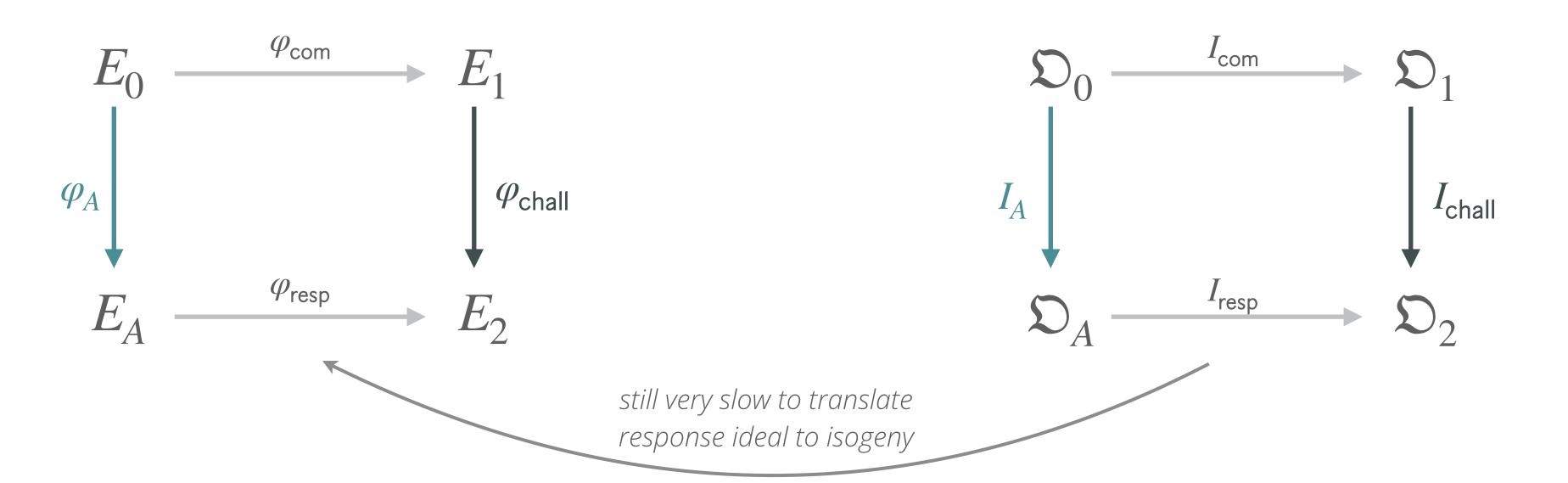


## PART 1 SQIsign



### Elliptic curve world

### **Quaternion world**



#### problem

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

