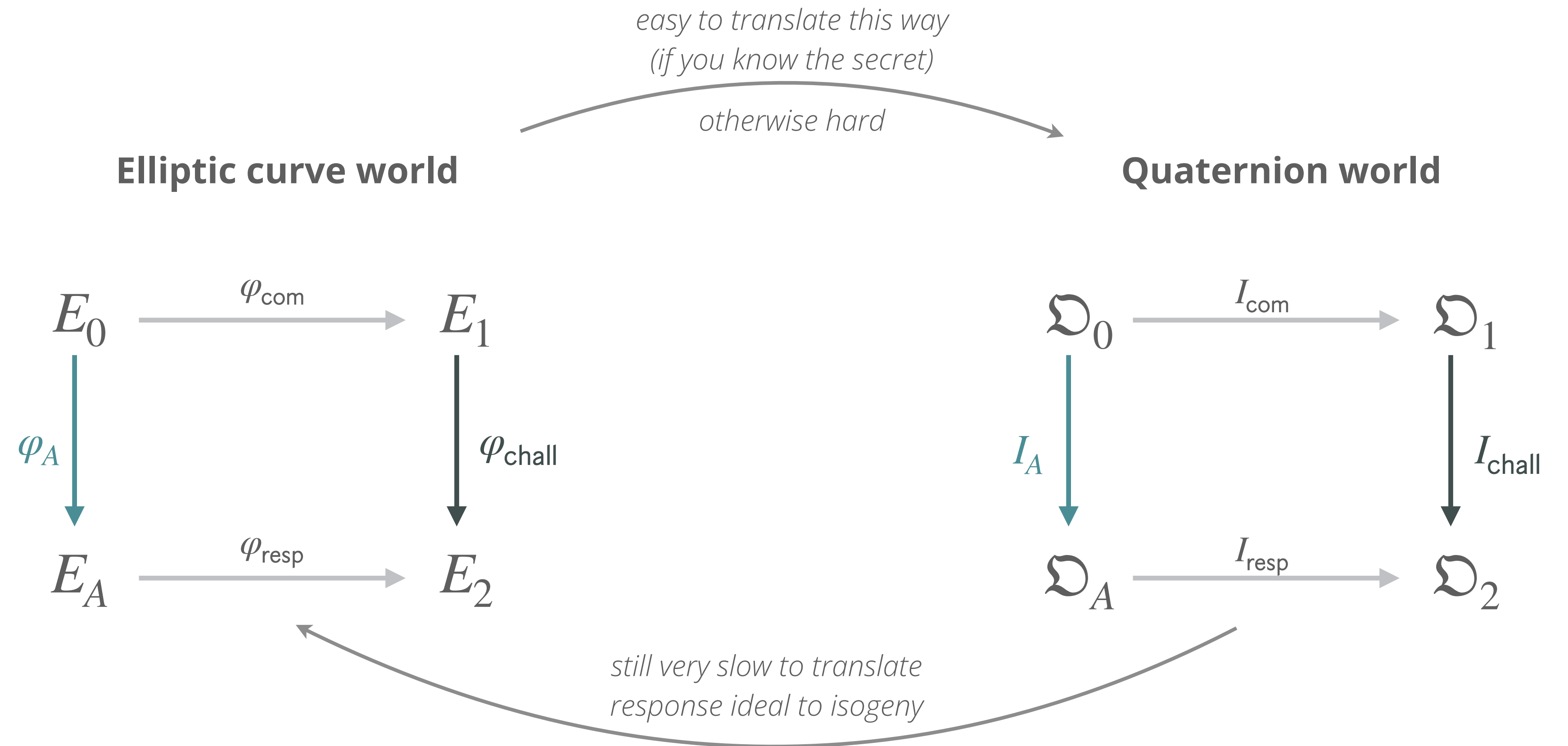
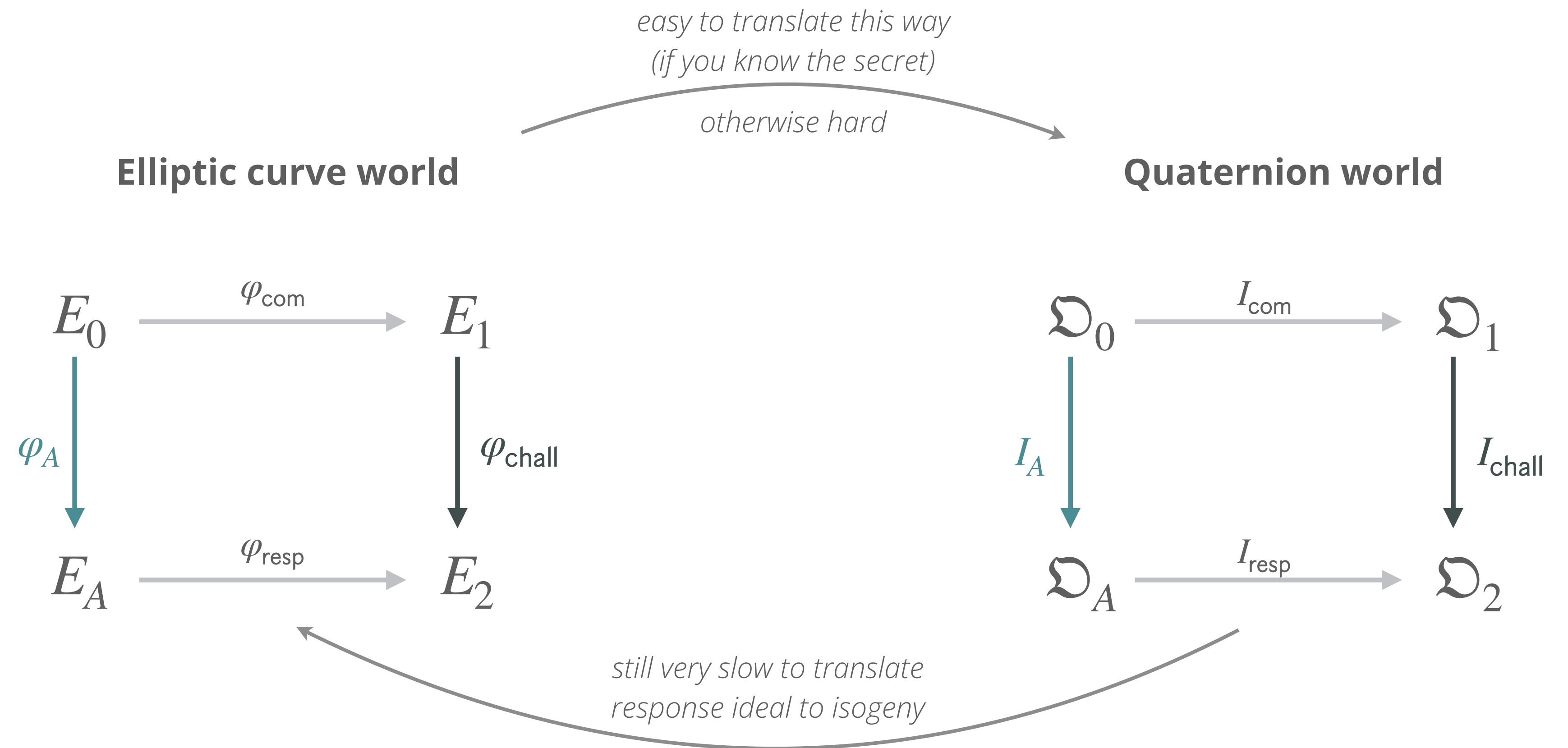


PART 1
SQLsign



PART 1

SQIsign



problem

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