



Kyber::Gen()  $\rightarrow$  (pk, sk)

Kyber::Encaps(pk)  $\rightarrow$  (capsule, ss)

Kyber::Decaps(sk, capsule)  $\rightarrow$  ss

pk

capsule

Process  
Complete

Comunicazione  
Cifrata

Comunicazione  
Cifrata