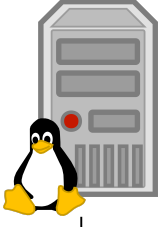

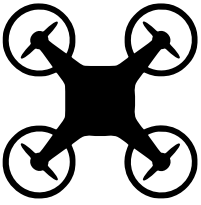

Kyber::Encaps(pk) → (ss, capsule)

capsule[0:192]

ACK

capsule[192:384]

ACK

capsule[384:576]

ACK

capsule[576:768]

Kyber::Decaps(sk, capsule) → ss

ACK

comunicazione cifrata

comunicazione cifrata