Passing pre-defined CEK using PQC KEM

Sender

- Generate random CEK
- Encapsulate random SS
  - (CT, SS) = KEM.Enc(Recipient_Pubkey)
- Compute R = XOR (SS, CEK)
- Transmit (CT, R)
- Use CEK

Receiver

- Receive (CT, R)
- Decapsulate SS
  - SS = KEM.Dec(Recipient_Privkey, CT)
- Compute CEK = XOR(SS, R)
- Use CEK