Passing pre-defined CEK using PQC KEM

**Sender**
- Generate random CEK
- Encapsulate random SS
  - \((CT, SS) = KEM.Enc(Recipient\_Pubkey)\)
- Compute \(R = \text{XOR}(SS, CEK)\)
- Transmit \((CT, R)\)
- Use CEK

**Receiver**
- Receive \((CT, R)\)
- Decapsulate SS
  - \(SS = KEM.Dec(Recipient\_Privkey, CT)\)
- Compute \(CEK = \text{XOR}(SS, R)\)
- Use CEK