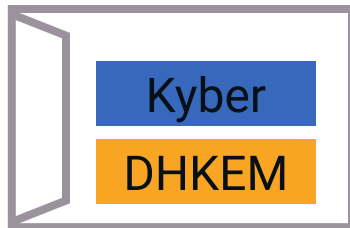


HPKE Diffie-Hellman
based AKEM (Authenticated
Key Encapsulation Method)
x25519HkdfSha256



KEM
(Key Encapsulation Method)
Kyber768



signature scheme
Dilithium3



confidentiality

classic

post-
quantum



authenticity

classic

post-
quantum

