

Prekey Bundle

$PQOPK_B$

OR

$PQSPK_B$

Umbenennung

$PQPK_B$

$\text{Sig}(IK_B, \text{EncodeKEM}(PQPK_B))$

IK_B

OPK_B^n

SPK_B

$\text{Sig}(IK_B, \text{EncodeEC}(SPK_B))$