Initiator:in (Alice)   **Antwortende:r (Bob)**

Prekey Bundle

last resort

$PQOPK_B$ OR $PQSPK_B$ ← Server

Umbenennung

$PQPK_B$

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

IK_B OPK_B^n SPK_B

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

$A : (CT_{\mathrm{KEM}}, SS_{\mathrm{KEM}}) = \mathtt{PQKEM\text{-}ENC}(PQPK_B)$
$B : SS_{\mathrm{KEM}} = \mathtt{PQKEM\text{-}DEC}(PQPK_B, CT_{\mathrm{KEM}})$

PQXDH

$DH_{\{1..4\}}$ $\mathtt{PQKEM}$

$(CT_{\mathrm{KEM}}, SS_{\mathrm{KEM}})$

Key Derivation Function (KDF)
$SK = \mathrm{KDF}(DH_1 \circ DH_2 \circ DH_3 \circ DH_4 \circ SS_{\mathrm{KEM}})$

Authenticated Encryption with Associated Data (AEAD)
$AD = \mathrm{EncodeEC}(IK_A) \circ \mathrm{EncodeEC}(IK_B) \circ \mathrm{EncodeKEM}(PQPK_B)$

$\mathtt{ENC}/\mathtt{DEC}$ von CT_{init} mittels SK & AD

Public Keys

$PQPK_B$

OPK_B^n SPK_B

IK_B

Public Keys

EK_A IK_A

falls $\mathtt{PQKEM}$ $PQPK_B$ nicht verwendet,
dann hier einarbeiten

Nachricht
$(IK_A, EK_A, CT_{\mathrm{KEM}}, CT_{\mathrm{init}}, \mathrm{Identifier})$