initiator: a | server | recipient: b

Identity Key: $\mathsf{I}_a = (d_{\mathsf{I}_a}, Q_{\mathsf{I}_a}) \leftarrow \mathsf{Curve25519}()$
Signed Pre Key: $\mathsf{S}_a = (d_{\mathsf{S}_a}, Q_{\mathsf{S}_a}) \leftarrow \mathsf{Curve25519}()$
One-Time Pre Key: $\mathsf{O}_a = (d_{\mathsf{O}_a}, Q_{\mathsf{O}_a}) \leftarrow \mathsf{Curve25519}()$

$Q_{\mathsf{I}_a}, Q_{\mathsf{S}_a}, Q_{\mathsf{O}_a}, \mathsf{Sign}_{d_{\mathsf{I}_a}}(Q_{\mathsf{S}_a})$ →

← $Q_{\mathsf{I}_b}, Q_{\mathsf{S}_b}, Q_{\mathsf{O}_b}, \mathsf{Sign}_{d_{\mathsf{I}_b}}(Q_{\mathsf{S}_b})$

Identity Key: $\mathsf{I}_b = (d_{\mathsf{I}_b}, Q_{\mathsf{I}_b}) \leftarrow \mathsf{Curve25519}()$
Signed Pre Key: $\mathsf{S}_b = (d_{\mathsf{S}_b}, Q_{\mathsf{S}_b}) \leftarrow \mathsf{Curve25519}()$
One-Time Pre Key: $\mathsf{O}_b = (d_{\mathsf{O}_b}, Q_{\mathsf{O}_b}) \leftarrow \mathsf{Curve25519}()$

get recipient public keys →

← $Q_{\mathsf{I}_b}, Q_{\mathsf{S}_b}, Q_{\mathsf{O}_b}$

Ephemeral Key: $\mathsf{E}_a = (d_{\mathsf{E}_a}, Q_{\mathsf{E}_a}) \leftarrow \mathsf{Curve25519}()$

$Q_{\mathsf{I}_a}, Q_{\mathsf{E}_a}$ →

Exchange K_1 ← ECDH($\mathsf{I}_a, \mathsf{S}_b$) → Exchange K_1

Exchange K_2 ← ECDH($\mathsf{E}_a, \mathsf{I}_b$) → Exchange K_2

Exchange K_3 ← ECDH($\mathsf{E}_a, \mathsf{S}_b$) → Exchange K_3

Exchange K_4 ← ECDH($\mathsf{E}_a, \mathsf{O}_b$) → Exchange K_4

$K_{\mathsf{master}} \leftarrow K_1 \| K_2 \| K_3 \| K_4$
$K_{\mathsf{root}}, K_{\mathsf{chain}} = \mathsf{HKDF}(K_{\mathsf{master}})$

Ephemeral Key: $\mathsf{E}_a = (d_{\mathsf{E}_a}, Q_{\mathsf{E}_a}) \leftarrow \mathsf{Curve25519}()$
$K_{\mathsf{message}} = \mathsf{HMAC}_{K_{\mathsf{chain}}}(1)$
$K_{\mathsf{chain}} = \mathsf{HMAC}_{K_{\mathsf{chain}}}(2)$
$\mathsf{cipher} = \mathsf{Encrypt}_{K_{\mathsf{message}}}(\mathsf{message})$
$\mathsf{signature} = \mathsf{HMAC}_{K_{\mathsf{message}}}(\mathsf{cipher})$

cipher, signature, Q_{E_a} →

$K_{\mathsf{master}} \leftarrow K_1 \| K_2 \| K_3 \| K_4$
$K_{\mathsf{root}}, K_{\mathsf{chain}} = \mathsf{HKDF}(K_{\mathsf{master}})$
$K_{\mathsf{message}} = \mathsf{HMAC}_{K_{\mathsf{chain}}}(1)$
$K_{\mathsf{chain}} = \mathsf{HMAC}_{K_{\mathsf{chain}}}(2)$
$\mathsf{message} = \mathsf{Decrypt}_{K_{\mathsf{message}}}(\mathsf{cipher})$

Keep sending new messages until recipient responds.

← Q_{E_b}

Ephemeral Key: $\mathsf{E}_b = (d_{\mathsf{E}_b}, Q_{\mathsf{E}_b}) \leftarrow \mathsf{Curve25519}()$

Exchange $K_{\mathsf{ephemeral}}$
$K_{\mathsf{chain}}, K_{\mathsf{root}} = \mathsf{HKDF}(K_{\mathsf{root}}, K_{\mathsf{ephemeral}})$

ECDH($\mathsf{E}_a, \mathsf{E}_b$)

Exchange $K_{\mathsf{ephemeral}}$
$K_{\mathsf{chain}}, K_{\mathsf{root}} = \mathsf{HKDF}(K_{\mathsf{root}}, K_{\mathsf{ephemeral}})$

As K_{chain} and K_{root} are rolled,
the rest of the protocol follows from above.

Notation: $(d, Q) \leftarrow \mathsf{Curve25519}()$ is the key generation function that generates d as private key and Q as public key.