IKpsk2 Reponse

Initiator

Responder

(S_i^{pub}, S_i^{priv}),(E_i^{pub}, E_i^{priv})

(S_r^{pub}, S_r^{priv}),(S_i^{pub}, E_i^{pub})

(E_r^{pub}, E_r^{priv}) ←ECDH-Generate()

ee ← ECDH(E_r^{priv}, E_i^{pub})

se ← ECDH(E_r^{priv}, S_i^{pub})

E_r^{pub},AEAD.Enc(ϵ)

ee ← ECDH(E_i^{priv}, E_r^{pub})

se ← ECDH(S_i^{priv}, E_r^{pub})