

**Initiator**

**Responder**

*sigB covers: MessageA + selectedSuite*

MessageA: suites[], keyShares[], nonce\_I, sigA

MessageB: selectedSuite, keyShare, nonce\_R, sigB

Finished\_R2I: HMAC(transcriptHash)

Finished\_I2R: HMAC(transcriptHash)

