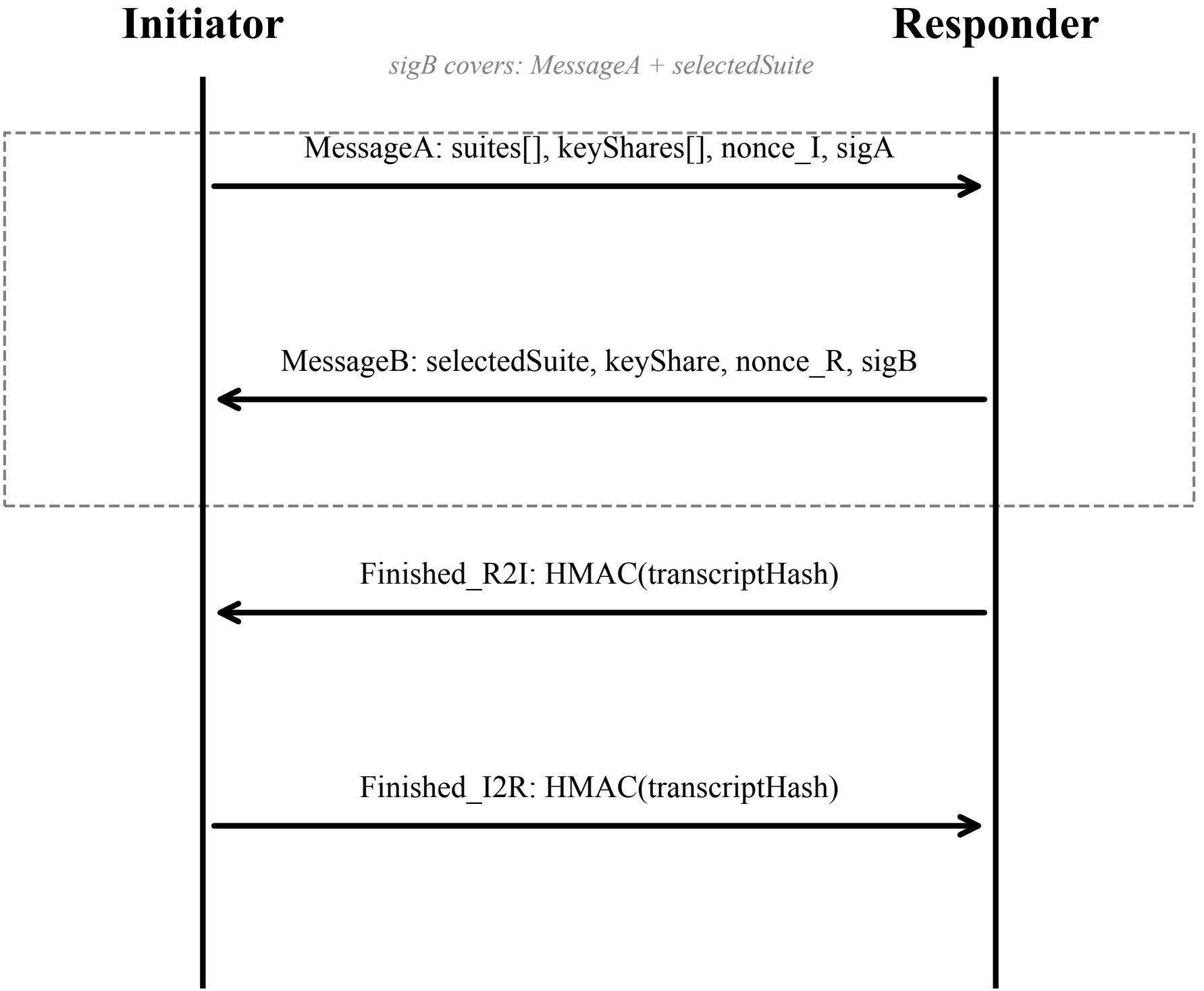
Initiator
Responder
sigB covers: MessageA + selectedSuite
MessageA: suites[], keyShares[], nonce_I, sigA
MessageB: selectedSuite, keyShare, nonce_R, sigB
Finished_R2I: HMAC(transcriptHash)
Finished_I2R: HMAC(transcriptHash)