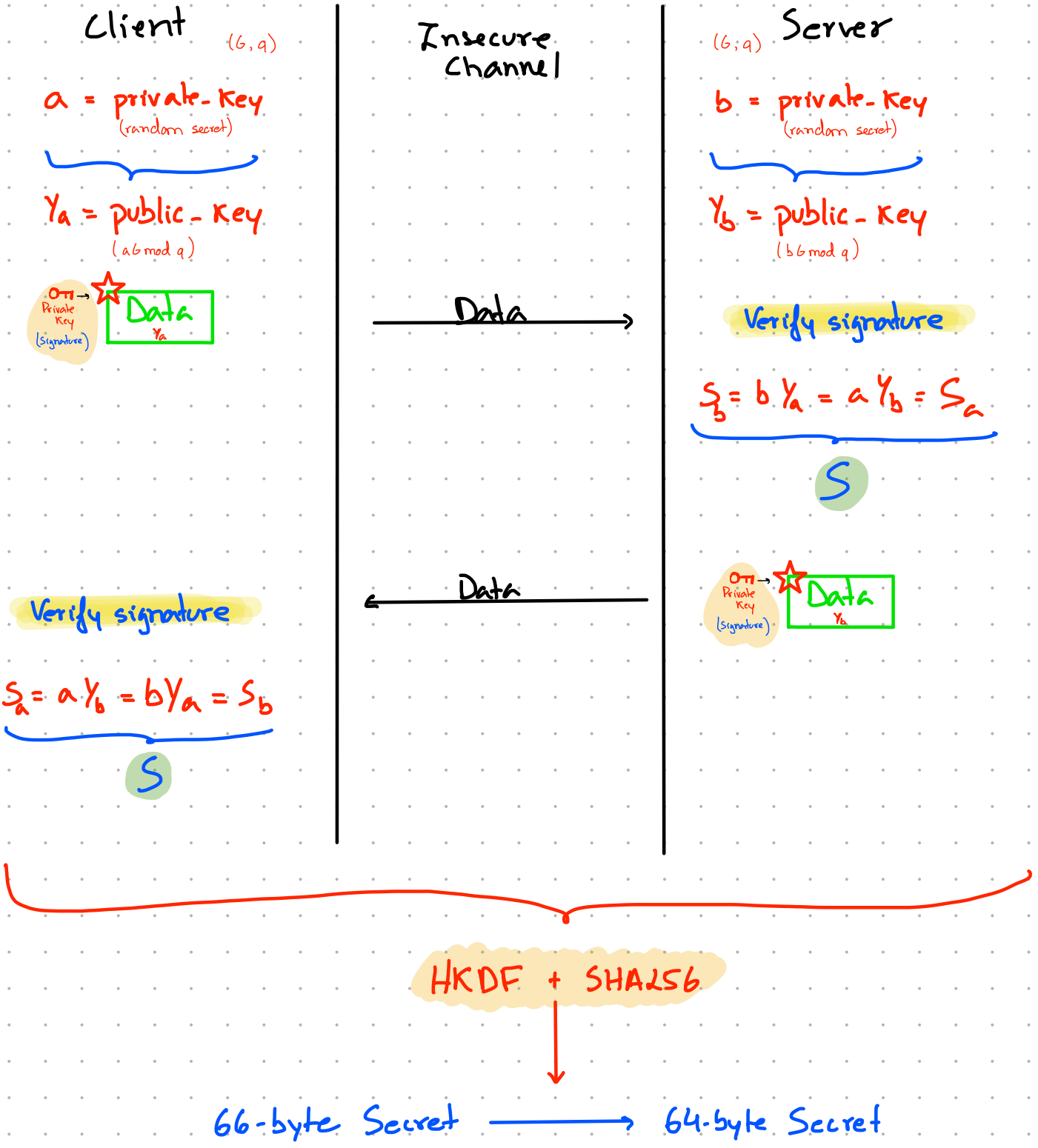
Session: Authentication



Session: Encryption

(session key)
S = K_s = secret
(K_s symmetric)

64 bytes
32 bytes | 32 bytes
K_{s1} (Encryption key) + K_{s2} (Integrity key)

① Use ECDH for secret agreement

② Divide in 2 32-byte symmetric keys

③ Encrypt the message using the symmetric encryption key.

Message + K_{s1} + IV_1 → D (Message, IV_1)

SHA2(D) → Digest

④ & ⑤ Create a Message Authentication Code (MAC) with the output of ③, using SHA2 digest function and the symmetric integrity key.

Digest + K_{s2} + IV_2 → MAC (IV_2)

⑥ Concatenate all the data to send.

Data to send ①: Message (IV_1) + MAC (IV_2)

⑦ Send it through an insecure channel