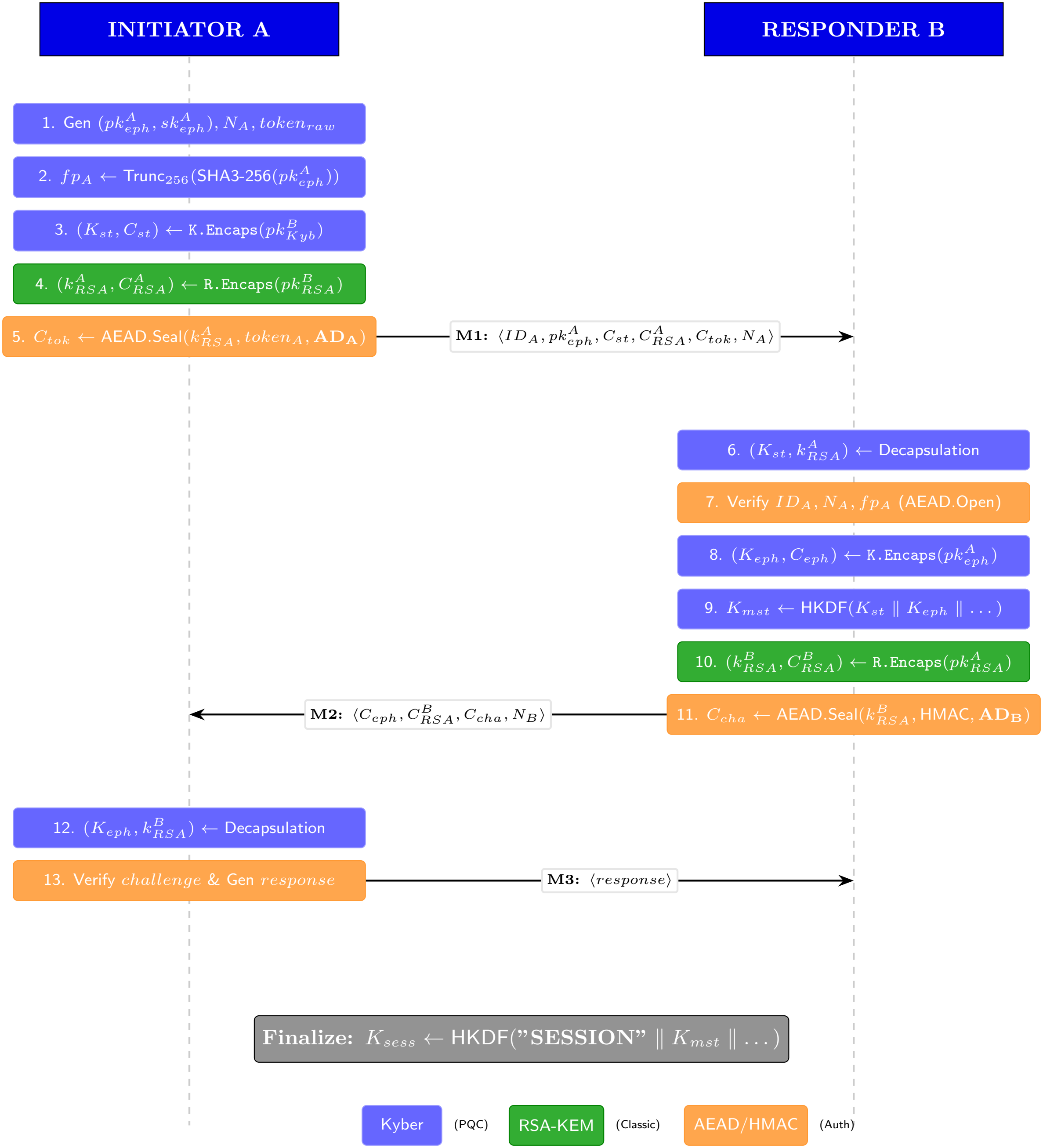
INITIATOR A
RESPONDER B
1. Gen $(pk^A_{eph}, sk^A_{eph}), N_A, token_{raw}$
2. $fp_A \leftarrow$ Trunc$_{256}$(SHA3-256(pk^A_{eph}))
3. $(K_{st}, C_{st}) \leftarrow \texttt{K.Encaps}(pk^B_{Kyb})$
4. $(k^A_{RSA}, C^A_{RSA}) \leftarrow \texttt{R.Encaps}(pk^B_{RSA})$
5. $C_{tok} \leftarrow$ AEAD.Seal($k^A_{RSA}, token_A$, $\mathbf{AD_A}$)
M1: $\langle ID_A, pk^A_{eph}, C_{st}, C^A_{RSA}, C_{tok}, N_A \rangle$
6. $(K_{st}, k^A_{RSA}) \leftarrow$ Decapsulation
7. Verify ID_A, N_A, fp_A (AEAD.Open)
8. $(K_{eph}, C_{eph}) \leftarrow \texttt{K.Encaps}(pk^A_{eph})$
9. $K_{mst} \leftarrow$ HKDF($K_{st} \parallel K_{eph} \parallel \ldots$)
10. $(k^B_{RSA}, C^B_{RSA}) \leftarrow \texttt{R.Encaps}(pk^A_{RSA})$
11. $C_{cha} \leftarrow$ AEAD.Seal(k^B_{RSA}, HMAC, $\mathbf{AD_B}$)
M2: $\langle C_{eph}, C^B_{RSA}, C_{cha}, N_B \rangle$
12. $(K_{eph}, k^B_{RSA}) \leftarrow$ Decapsulation
13. Verify $challenge$ & Gen $response$
M3: $\langle response \rangle$
Finalize: $K_{sess} \leftarrow$ HKDF(”SESSION” $\parallel K_{mst} \parallel \ldots$)
Kyber (PQC)
RSA-KEM (Classic)
AEAD/HMAC (Auth)