Quick attacker capability table (short)

- Passive eavesdropper → **stuck** unless they break *both* RSA and Kyber (or steal keys).
- Active MITM → **succeeds** unless public keys are authenticated (signatures/certs).
- Endpoint/key theft → **partially blocked** (hybrid helps if only one key stolen), **fails** if both keys stolen.
- Quantum attacker → **blocked`** if Kyber remains secure (hybrid protects against future quantum RSA-breaking).
- Implementation/side-channel attacker → **may succeed**; these are practical risks you must fix.

Practical recommendations (what to do to make the system actually secure)

1. **Authenticate keys** — sign KEM and RSA public keys (RSA signatures or PQC signatures).
2. **Use ephemeral keys** for key exchange (gives forward secrecy). For RSA use ephemeral RSA or, better, ephemeral KEMs — or derive ephemeral shared secrets each session.
3. **Use HKDF** instead of plain SHA256 on raw concatenation — include context strings (protocol IDs, role tags) when deriving final keys.
4. **AES-GCM rules:** never reuse nonce with same key; use 96-bit random nonce or counter properly.
5. **Protect private keys** (HSM/secure enclave, file permissions).
6. **Keep libs updated** and run tests against edge cases.
7. **Add replay protection** (sequence numbers, timestamps) and logging for anomaly detection.