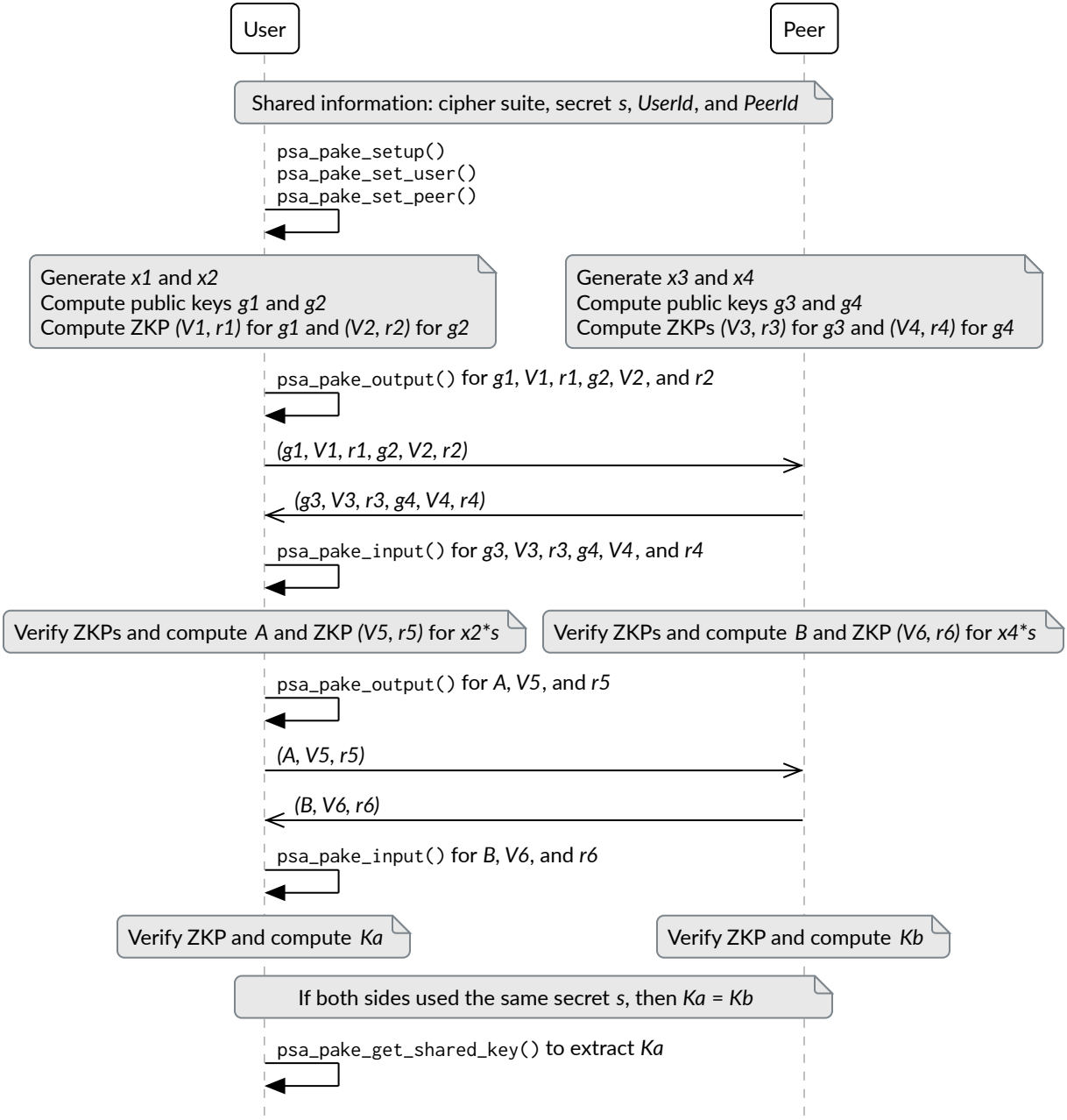
User
Peer
Shared information: cipher suite, secret s, UserId, and PeerId
psa_pake_setup()
psa_pake_set_user()
psa_pake_set_peer()
Generate x1 and x2
Compute public keys g1 and g2
Compute ZKP (V1, r1) for g1 and (V2, r2) for g2
Generate x3 and x4
Compute public keys g3 and g4
Compute ZKPs (V3, r3) for g3 and (V4, r4) for g4
psa_pake_output() for g1, V1, r1, g2, V2, and r2
(g1, V1, r1, g2, V2, r2)
(g3, V3, r3, g4, V4, r4)
psa_pake_input() for g3, V3, r3, g4, V4, and r4
Verify ZKPs and compute A and ZKP (V5, r5) for x2*s
Verify ZKPs and compute B and ZKP (V6, r6) for x4*s
psa_pake_output() for A, V5, and r5
(A, V5, r5)
(B, V6, r6)
psa_pake_input() for B, V6, and r6
Verify ZKP and compute Ka
Verify ZKP and compute Kb
If both sides used the same secret s, then Ka = Kb
psa_pake_get_shared_key() to extract Ka