Result • authentication? Alice -> Bob: c3 — When:
c1 → PKE_ENC(G^k_sb, CONCAT(alice, na))
alice_b → alice
b_na → na
unnamed_0 → ASSERT(alice, alice)?
c2 → PKE_ENC(G^k_sa, CONCAT(bob, na, nb))
bob_a → bob
a_na → na
a_nb → nb
unnamed_1 → ASSERT(bob, bob)?
unnamed_2 → ASSERT(na, na)?
c3 → alice ← mutated by Attacker (originally PKE_ENC(k_pb, a_nb))
b_nb → PKE_DEC(k_sb, alice)
unnamed_3 → ASSERT(PKE_DEC(k_sb, alice), nb)?
c3 (alice), sent by Attacker and not by Alice, is successfully used in PKE_DEC(k_sb, alice) within Bob's state.