A trace has been found.

Honest Process

{1}new sec_ch

g))),open_ch)) = (a_9,((g,AES_GCM_enc((a_10,(a_11, (a_12,(a_13,(a_14,(a_15,(a_16,a_17))))))),kdf(exp(g,qe),g),kdf(exp(g,qe),g))),open_ch)) $\sim M_42 = SHA256((s_2,r_2))$ $\sim M_43 = \exp(g, \exp_1)$ \sim M_44 = AES_GCM_enc((a_18,(token_2,(UUID,(SN_2,(data_2, (Version_2,(a_19,SeedK1_2)))))),kdf(exp(exp(g, qe),exp_1),exp(g,exp_1)),kdf(exp(exp(g,qe),exp_1),exp(g,exp_1))) \sim M_45 = open_ch ~X_3 = (~M_42,((~M_43,~M_44),open_ch)) = (SHA256((s_2, r_2)),((exp(g,exp_1),AES_GCM_enc((a_18,(token_2, (UUID,(SN_2,(data_2,(Version_2,(a_19,SeedK1_2))))))), kdf(exp(exp(g,qe),exp_1),exp(g,exp_1)),kdf(exp(exp(g,qe),exp_1),exp(g,exp_1)))),open_ch)) ~X_5 = (iCloudldentifier_9,(SeedS_4,(sign((UUID,(a_18, (SeedS_4,(SHA256((exp(g,s_3),r_4)),(a_19,AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const), PairingSession_const),kdf(kdf((SeedS_4,SeedK1_2),
ServerSharedSecret_const),PairingSession_const)))))),
qa),(AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,
SeedK1_2),ServerSharedSecret_const),PairingSession_const),
kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const), PairingSession_const)),pre_app1)))) \sim M_46 = exp(g,s_) ~M_48 = AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4, SeedK1_2),ServerSharedSecret_const),PairingSession_const), kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const), PairingSession_const)) \sim M_49 = SeedS_4 ~M_50 = sign((UUID,(a_18,(SeedS_4,(SHA256((exp(g, s_3),r_4)),(a_19,AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const))))))), \sim M_51 = iCloudldentifier_9 \sim M_52 = open_ch ~X_6 = (iCloudldentifier_5,(SeedS_3,(sign((a_12,(a_10, (SeedS_3,(SHA256((exp(g,s_2),r_3)),(a_16,AES_GCM_enc(token_new,kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const),kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const))))))),qa),(AES_GCM_enc(token_new, kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const),kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const)),pre_app1)))) $\sim M_53 = \exp(g,s_3)$ ~M_55 = AES_GCM_enc(token_new,kdf(kdf((SeedS_3,a_17), ServerSharedSecret_const),PairingSession_const), kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const)) \sim M_56 = SeedS_3 ~M_57 = sign((a_12,(a_10,(SeedS_3,(SHA256((exp(g, s_2),r_3)),(a_16,AES_GCM_enc(token_new,kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const),PairingSession_const), kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const))))),qa) ~M_58 = iCloudldentifier_5 \sim M_59 = open_ch $\sim X_7 = (\sim M_53, (\sim M_54, (\sim M_48, (\sim M_49, (\sim M_50, (a_20, open_ch)))))$ (exp(g,s_3),(r_4,(AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const)), (SeedS_4,(sign((UUID,(a_18,(SeedS_4,(SHA256((exp(g,s_3),r_4)),(a_19,AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const))))))), qa),(a_20,open_ch)))))) $\sim M_60 = s_2$ $\sim M_61 = r_2$ \sim M_62 = UUID \sim M_63 = SN_2 $\sim M_64 = a_18$ $\sim M_65 = a_19$ \sim M_66 = token_new_2 \sim M_67 = Status \sim M_68 = open_ch Attacker

Abbreviations

 \sim X_1 = (a_9,((g,AES_GCM_enc((a_10,(a_11,(a_12,(a_13,(a_14,(a_15,(a_16,a_17)))))),kdf(\sim M,g),kdf(\sim M,

{3}new UUID {4}new qe {5}new qa {26} new E1_3 $(\sim M, (\sim M_1, \sim M_2)) = (\exp(g, qe), (pk(qa), Apple_PubKey_and_VerifyKey))$ $(\sim M_3, (\sim M_4, \sim M_5)) = (SessionNonce_3, (E1_3, open_ch))$ {25}new SessionNonce_4 $(\sim M_6, (\sim M_7, \sim M_8)) = (\exp(g, qe), (pk(qa), Apple_PubKey_and_VerifyKey))$ $(\sim M_9, (\sim M_10, \sim M_11)) = (Session Nonce_4, (E1_4, open_ch))$ [7] new iCloudldentifier_5 [25] new SessionNonce_5 [26] new E1_5 $(\sim M_12,(\sim M_13,\sim M_14)) = (\exp(g,qe),(pk(qa),Apple_PubKey_and_VerifyKey))$ $(\sim M_15,(\sim M_16,\sim M_17)) \neq (SessionNonce_5,(E1_5,$ [7] new iCloudldentifier_6 [25] new SessionNonce_6 [26] new E1_6 $(\sim M 18, (\sim M_19, \sim M_20)) = (\exp(g, qe), (pk(qa), Apple_PubKey_and_VerifyKey))$ $(\sim M_21,(\sim M_22,\sim M_23)) = (SessionNonce_6,(E1_6, open_ch))$ [7] new iCloudldentifier_7 [25] new SessionNonce_7 [26] new E1_7 $(\sim M_24,(\sim M_25,\sim M_26)) = (\exp(g,qe),(pk(qa),Apple_PubKey_and_VerifyKey))$ $(\sim M_27,(\sim M_28,\sim M_29)) = (SessionNonce_7,(E1_7, open_ch))$ {25}new SessionNonce_8 {7}new iCloudldentifier_8 {26}new E1_8 $(\sim M \ 30, (\sim M \ 31, \sim M \ 32)) = (\exp(g, qe), (pk(qa), Apple PubKey and VerifyKey))$ $(\sim M_33,(\sim M_34,\sim M_35)) = (SessionNonce_8,(E1_8, open_ch))$ $(\sim M_36,(\sim M_37,\sim M_38)) = (\exp(g,qe),(pk(qa),Apple_PubKey_and_VerifyKey))$ $(\sim M_39,(\sim M_40,\sim M_41)) = (SessionNonce_9,(E1_9, open_ch))$ (a_7,(a_8,open_ch))