Abbreviations
~M_11 = SHA256((s_2,r_2))
~M_12 = ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),pk(qe))
~M_13 = open_ch
~X_1 = (iCloudIdentifier_4,(SeedS_3,(sign((UUID,(a_8,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_9,AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const))))))),qa),(AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const)),pre_app1))))
~M_14 = exp(g,s__2)
~M_15 = r__3
~M_16 = AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const))
~M_17 = SeedS_3
~M_18 = sign((UUID,(a_8,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_9,AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const))))))),qa)
~M_19 = iCloudIdentifier_4
~M_20 = open_ch

A trace has been found.

Honest Process

{1}new sec_ch
{2}new UUID_paired
{3}new UUID
{4}event UUIDSource(UUID)
{5}new token

Attacker

{7}new iCloudIdentifier_6
{7}new iCloudIdentifier_5
{7}new iCloudIdentifier_4
{7}new iCloudIdentifier_3
{30}new SessionNonce_4
{31}new E1_4
{30}new SessionNonce_5
{31}new E1_5
{30}new SessionNonce_3
{31}new E1_3
(~M,(~M_1,~M_2)) = (SessionNonce_3,(E1_3,open_ch))
(~M_3,(~M_4,~M_5)) = (SessionNonce_4,(E1_4,open_ch))
(~M_6,~M_7) = (pk(qe),pk(qa))
(~M_8,(~M_9,~M_10)) = (SessionNonce_5,(E1_5,open_ch))
(a_8,(a_9,open_ch))
{61}new s_2
{62}new r_2
{65}new SeedK1_2
{66}new exp_1
{67}new SN_2
{68}new data_2
{69}new Version_2
{72}event SessionNonceEncSource(a_8)
{73}event E1EncSource(a_9)
(~M_11,(~M_12,~M_13))
{75}event SendE2(ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),pk(qe)))
(a_10,(~M_12,open_ch)) = (a_10,(ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),pk(qe)),open_ch))
{34}new s_
{35}new r__2
{38}event H1Source(SHA256((exp(g,s_),r__2)))
(SHA256((a_11,a_12)),(a_13,open_ch))
(SHA256((exp(g,s_),r__2)),(ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),pk(qe)),pre_app1))
{34}new s__2
{35}new r__3
{38}event H1Source(SHA256((exp(g,s__2),r__3)))
{10}event RecvE2((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2)))))),pk(qe)))
{12}event RecvUUID(UUID)
{13}event RecvSessionNonce(a_8)
{16}new token_new
{17}new SeedS_3
{25}event SendH1(SHA256((exp(g,s_),r__2)))
{26}event SendE1(a_9)
(SHA256((exp(g,s__2),r__3)),(a_13,pre_app1))
~X_1
{28}event SendE3(AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const)),SeedS_3)
(~M_14,(~M_15,(~M_16,(~M_17,(~M_18,(~M_19,~M_20))))))
{42}event SendS2(sign((UUID,(a_8,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_9,AES_GCM_enc(token_new,kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const),kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),PairingSession_const))))))),qa))
(a_11,(a_12,(a_14,open_ch)))
{50}event Secret_d(add(a_11,s__2))
{51}event Secret_P(add(exp(g,a_11),exp(g,s__2)))
{52}event Secret_SK(kdf(get_point_x(add(exp(g,a_11),exp(g,s__2))),(a_12,r__3)))
~M_21 = AES_GCM_enc(s_SK,kdf(get_point_x(add(exp(g,a_11),exp(g,s__2))),(a_12,r__3)),zero_const)
~M_22 = AES_GCM_enc(s_d,add(a_11,s__2),zero_const)
~M_23 = AES_GCM_enc(s_P,add(exp(g,a_11),exp(g,s__2)),zero_const)
The attacker has the message AES_GCM_dec(~M_23,add(exp(g,a_11),~M_14),zero_const) = s_P