Abbreviations
~M_20 = SHA256((s_2,r_2))
~M_21 = ECIES_enc((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),pk(qe))
~M_22 = open_ch
~X_1 = (iCloudIdentifier_4,(SeedS_3,(sign((UUID,(a_4,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_5,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_23 = exp(g,s__2)
~M_24 = r__3
~M_25 = 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_26 = SeedS_3
~M_27 = sign((UUID,(a_4,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_5,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_28 = iCloudIdentifier_4
~M_29 = 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

!

{7}new iCloudIdentifier_3
{29}new SessionNonce_3
{30}new E1_3

{7}new iCloudIdentifier_4
{29}new SessionNonce_4
{30}new E1_4

{7}new iCloudIdentifier_5
{29}new SessionNonce_5
{30}new E1_5

{7}new iCloudIdentifier_6
{29}new SessionNonce_6
{30}new E1_6

{59}new s_2
{60}new r_2
{63}new SeedK1_2
{64}new exp_1
{65}new SN_2
{66}new data_2
{67}new Version_2
{70}event SessionNonceEncSource(a_4)
{71}event E1EncSource(a_5)

{73}event SendE2(ECIES_enc((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),pk(qe))),pk(qe)))

{33}new s_
{34}new r__2
{37}event H1Source(SHA256((exp(g,s_),r__2)))

{10}event RecvE2((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),ECIES_enc((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),pk(qe)))
{12}event RecvUUID(UUID)
{13}event RecvSessionNonce(a_4)
{16}new token_new
{17}new SeedS_3
{25}event SendH1(SHA256((exp(g,s_),r__2)))
{26}event SendE1(a_5)

{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)

Attacker

(~M,~M_1) = (pk(qe),pk(qa))
(~M_2,(~M_3,~M_4)) = (SessionNonce_3,(E1_3,open_ch))
(~M_5,~M_6) = (pk(qe),pk(qa))
(~M_7,(~M_8,~M_9)) = (SessionNonce_4,(E1_4,open_ch))
(~M_10,~M_11) = (pk(qe),pk(qa))
(~M_12,(~M_13,~M_14)) = (SessionNonce_5,(E1_5,open_ch))
(~M_15,~M_16) = (pk(qe),pk(qa))
(~M_17,(~M_18,~M_19)) = (SessionNonce_6,(E1_6,open_ch))
(a_4,(a_5,open_ch))
(~M_20,(~M_21,~M_22))
(a_6,(~M_21,open_ch)) = (a_6,(ECIES_enc((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),pk(qe)),open_ch))
(SHA256((a_7,a_8)),(a_9,open_ch))
(SHA256((exp(g,s_),r__2)),(ECIES_enc((a_4,(token,(UUID,(SN_2,(data_2,(Version_2,(a_5,SeedK1_2)))))),pk(qe)),pre_app1))
(SHA256((exp(g,s__2),r__3)),(a_9,pre_app1))
~X_1
(~M_23,(~M_24,(~M_25,(~M_26,(~M_27,(~M_28,~M_29))))))
(a_7,(a_8,(a_10,open_ch)))
~M_30 = AES_GCM_enc(s_SK,kdf(get_point_x(add(exp(g,a_7),exp(g,s__2))),(a_8,r__3)),zero_const)
~M_31 = AES_GCM_enc(s_d,add(a_7,s__2),zero_const)
~M_32 = AES_GCM_enc(s_P,add(exp(g,a_7),exp(g,s__2)),zero_const)

{33}new s__2
{34}new r__3
{37}event H1Source(SHA256((exp(g,s__2),r__3)))

{41}event SendS2(sign((UUID,(a_4,(SeedS_3,(SHA256((exp(g,s_),r__2)),(a_5,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))

{49}event Secret_d(add(a_7,s__2))
{50}event Secret_P(add(exp(g,a_7),exp(g,s__2)))
{51}event Secret_SK(kdf(get_point_x(add(exp(g,a_7),exp(g,s__2))),(a_8,r__3)))

The attacker has the message AES_GCM_dec(~M_30,kdf(get_point_x(add(exp(g,a_7),~M_23)),(a_8,~M_24)),zero_const) = s_SK