(Version_2,(a_9,SeedK1_2)))))),pk(qe)) \sim M 13 = open_ch $\sim X_1 = (iCloudldentifier_4,(SeedS_3,(sign((UUID,(a_8,$ (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)))) A trace has been $\sim M_14 = \exp(g,s_2)$ found. $\sim M_15 = r_3$ \sim 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)) \sim M_17 = SeedS_3 \sim 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, r SeedK1_2), ServerSharedSecret_const), PairingSession_const), kdf(kdf((SeedS_3,SeedK1_2),ServerSharedSecret_const),
PairingSession_const)))))),qa) \sim M_19 = iCloudldentifier_4 \sim M_20 = open_ch Attacker **Honest Process** {1}new sec_ch {2}new UUID_paired {3}new UUID {4}event UUIDSource(UUID) {5}new token [7] new iCloudldentifier_3 {30}new SessionNonce_3 {31}new E1_3 {7}new iCloudldentifier_5 {30} new SessionNonce_4 $(\sim M, (\sim M_1, \sim M_2)) = (SessionNonce_3, (E1_\beta, open_ch))$ {7}new iCloudldentifier_4 {31} new E1_4 [7] new iCloudldentifier_6 $(\sim M_3, (\sim M_4, \sim M_5)) = (SessionNonce_4, (E1 4, open_ch))$ {30}new SessionNonce_5 {31}new E1_5 $(\sim M_6, \sim M_7) = (pk(qe), pk(qa))$ $(\sim M_8, (\sim M_9, \sim M_10)) = (SessionNonce_5, (E1_5, open_ch))$ (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) $(\sim M_11, (\sim M_12, \sim M \downarrow 13))$ {75} event SendE2(ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2))))))),pk(qe))) $(a_10,(\sim M_12,open_ch)) = (a_10,(ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,(Version_2,(a_9,SeedK1_2))))))), pk(qe)),open_ch))$ {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) $(\sim M_14,(\sim M_15,(\sim M_16,(\sim M_17,(\sim M_18,(\sim M_19,\sim M_20))))))$ {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), Respectively. $(a_11,(a_12,(a_14,open_ch)))$ {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))) \sim 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) \sim M_22 = AES_GCM_enc(s_d,add(a_11,s_2),zero_const) \sim M_23 = AES_GCM_enc(s_P,add(exp(g,a_1|1),exp(g, s $\overline{2}$)), zero const) The attacker has the message AES_GCM_dec(\sim M_21, kdf(get_point_x(add(exp(g,a_11), \sim M_14)),(a_12, \sim M_15)),zero_const) = s_SK

Abbreviations

 \sim M_11 = SHA256((s_2,r_2))

 \sim M_12 = ECIES_enc((a_8,(token,(UUID,(SN_2,(data_2,