	Abbreviations
	$kdf(exp(g,qe),g),kdf(exp(g,qe),g))),pre_app1)) \\ \sim M_42 = SHA256((s_2,r_2)) \\ \sim M_43 = exp(g,exp_1) \\ \sim M_44 = AES_GCM_enc((a_18,(token_2,(UUID,(SN_2,(data_2,(Version_2,(a_19,SeedK1_2))))))),kdf(exp(exp(g,qe),exp_1),exp(g,exp_1)),kdf(exp(exp(g,qe),exp_1)),$
	$ \begin{array}{c} \exp(g, \exp_1))) \\ \sim M 45 = \operatorname{open\_ch} \\ \\ \sim X 3 = (\sim M 42, ((\sim M 43, \sim M 44), \operatorname{open\_ch})) = (\operatorname{SHA256}((s 2, r 2)), ((\exp(g, \exp_1), \operatorname{AES\_GCM\_enc}((a 18, (\operatorname{token\_2}, (\operatorname{UUID}, (\operatorname{SN\_2}, (\operatorname{data\_2}, (\operatorname{Version\_2}, (a 19, \operatorname{SeedK1\_2}))))))), \\ \operatorname{kdf}(\exp(\exp(g, \operatorname{qe}), \exp_1), \exp(g, \exp_1)), \operatorname{kdf}(\exp(e_{\operatorname{sep}}(g, \operatorname{qe}), \exp_1), \exp(g, \exp_1))), \operatorname{open\_ch})) \\ \sim X 4 = (\operatorname{SHA256}((\exp(g, \operatorname{s\_3}), \operatorname{r\_4})), ((\exp(g, \exp_1), \operatorname{AES\_GCM\_enc}((a 18, (\operatorname{token\_2}, (\operatorname{UUID}, (\operatorname{SN\_2}, (\operatorname{data\_2}, (\operatorname{Version\_2}, (a 19, \operatorname{SeedK1\_2}))))))), \operatorname{kdf}(\exp(\exp(g, \operatorname{qe}), \exp_1), \operatorname{AES\_GCM\_enc}((a 18, (\operatorname{token\_2}, (\operatorname{UUID}, (\operatorname{SN\_2}, (\operatorname{data\_2}, (\operatorname{Version\_2}, (a 19, \operatorname{SeedK1\_2}))))))), \operatorname{kdf}(\exp(\exp(g, \operatorname{qe}), \exp_1), \operatorname{cong})) \\ = (a 19, \operatorname{SeedK1\_2})))))), \operatorname{kdf}(\exp(\exp(g, \operatorname{qe}), \exp_1), \operatorname{cong}) \\ = (a 19, \operatorname{SeedK1\_2})))))), \operatorname{kdf}(\exp(\exp(g, \operatorname{qe}), \exp_1), \operatorname{cong})) \\ = (a 19, \operatorname{SeedK1\_2}))))))), \operatorname{kdf}(\exp(e_{\operatorname{sp}}(g, \operatorname{qe}), \exp_1), \operatorname{cong})) \\ = (a 19, \operatorname{SeedK1\_2})))))))), \operatorname{kdf}(\exp(e_{\operatorname{sp}}(g, \operatorname{qe}), \exp_1), \operatorname{cong})))))) \\ = (a 19, \operatorname{SeedK1\_2}))))))))))) \\ = (a 19, \operatorname{SeedK1\_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)))), pre_app1))  -X_5 = (iCloudIdentifier_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),PairingSession_const)))))), ServerSharedSecret_const),PairingSession_const)))))), qa),(AES_GCM_enc(token_new_2,kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const), kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const)), kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const)), PairingSession_const)),pre_app1))))
	$ \sim M_46 = \exp(g,s) $ $ \sim M_47 = r2 $ $ \sim 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   \sim M_50 = \text{sign}((UUID,(a_18,(SeedS\_4,(SHA256)(exp(g, figure f$
A trace has been found.	$s_3,r_4)), (a_19,AES_GCM_enc(token_new_2),kdf(') \\ kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const), \\ RairingSession_const), kdf(kdf((SeedS_4,SeedK1_2),ServerSharedSecret_const),PairingSession_const)))))))), \\ qa) \\ -M_51 = iCloudIdentifier_9 \\ -M_52 = open_ch$
	~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), kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const),kdf(kdf((SeedS_3,a_17),ServerSharedSecret_const), PairingSession_const)),pre_app1))))  ~M_53 = exp(g,s_3)
	~X_7 = (~M_53,(~M_48,(~M_48,(~M_49,(~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,SeedK1_2), SeedS_4,SeedK1_2), ServerSharedSecret_const), Aging((SeedS_4,SeedK1_2), SeedS_4,SeedK1_2), ServerSharedSecret_const), PairingSession_const), kdf((SeedS_4,SeedK1_2), ServerSharedSecret_const), pairingSession_const), pairing
Honest Process	~M_67 = Status  ~M_68 = open_ch  Attacker
{1}new sec_ch {2}new UUID_paired {3}new UUID  {4}new qe {5}new qa	
[7] new iClo	oudldentifier_3  {25} new SessionNonce_3 {26} new E1_3
	$(\sim M, (\sim M_1, \sim M_2)) = (\exp(g, qe), (pk(qa), Apple\_PubKey\_and\_VerifyKey))$
{7} new iCloudIdentifier_4 {25} new SessionNonce_4 {26} new E1 4	$(\sim M_3, (\sim M_4, \sim M_5)) = (SessionNonce_3, (E1_3, open_ch))$
	$(\sim M_6, (\sim M_7, \sim M_8)) = (\exp(g,qe), (pk(qa), Apple\_PubKey\_and\_VerifyKey))$
	$(\sim M_9, (\sim M_10, \sim M_11)) = (SessionNonce_4, (E1_4, open_ch))$
[7] new iCloudIdentifier_5	

| The state of the