Abbreviations  $\sim$ M 1 = nonce 6  $\sim$ M 2 = rpid 7  $\sim$ M 3 = senc(Auth1(username 4,rpid 7,skA 2),wk 2)  $\sim$ M 4 = dhexp(g,dh spairRP 2)  $\sim$ M 5 = sign(RP1(nonce 6,rpid 7,senc(Auth1(username 4, rpid\_7,skA\_2),wk\_2),dhexp(g,dh\_spairRP\_2)),sskey\_RP\_3)  $\sim$ M 6 = dhexp(g,dh spairRP 2)  $\sim$ M 7 = sign(RP1(nonce 6,rpid 7,senc(Auth1(username 4, rpid 7,skA 2),wk 2),dhexp(g,dh spairRP 2)),sskey RP 3)  $\sim$ X 1 = (hash(Client1(rpid 7,nonce 6)),HMAC(pinAuth 3, hash(Client1(rpid 7,nonce 6))),RP1(nonce 6,rpid 7, senc(Auth1(username 4,rpid 7,skA 2),wk 2),dhexp( g,dh spairRP 2)),sign(RP1(nonce 6,rpid 7,senc( Auth1(username\_4,rpid\_7,skA\_2),wk\_2),dhexp(g,dh\_spairRP\_2)), sskey RP 3))  $\sim$ X 2 = (Auth4(Auth2(h(rpid 7),aaguid 4,senc(Auth1(username 4, rpid 7,skA 2),wk 2),spk(skA 2)),sign(Auth3(Auth2( h(rpid 7), aaguid 4, senc(Auth1(username 4, rpid 7, skA 2),wk 2),spk(skA 2)),hash(Client1(rpid 7,nonce 6))), skA 2),senc(Auth1(username 4,rpid 7,skA 2),wk 2), RP1(nonce 6,rpid 7,senc(Auth1(username 4,rpid 7, skA 2),wk 2),dhexp(g,dh spairRP 2)),dhexp(g,dh spairA 2)), sign(Auth4(Auth2(h(rpid 7),aaguid 4,senc(Auth1( username 4,rpid 7,skA 2),wk 2),spk(skA 2)),sign( Auth3(Auth2(h(rpid 7),aaguid 4,senc(Auth1(username 4, rpid 7,skA 2),wk 2),spk(skA 2)),hash(Client1(rpid 7, nonce 6))),skA 2),senc(Auth1(username 4,rpid 7, skA 2),wk 2),RP1(nonce 6,rpid 7,senc(Auth1(username 4, rpid 7,skA 2),wk 2),dhexp(g,dh spairRP 2)),dhexp( g,dh spairA 2)),sskey RP 3))  $\sim$ M 8 = h(rpid 7)  $\sim$ M 9 = aaguid 4  $\sim$ M 10 = senc(Auth1(username 4,rpid 7,skA 2),wk 2)  $\sim$ M 11 = spk(skA 2)  $\sim$ M 12 = sign(Auth3(Auth2(h(rpid 7),aaguid 4,senc( Auth1(username 4,rpid 7,skA 2),wk 2),spk(skA 2)), hash(Client1(rpid 7,nonce 6))),skA 2)  $\sim$ M 13 = senc(Auth1(username 4,rpid 7,skA 2),wk 2)  $\sim$ M 14 = nonce 6  $\sim$ M 15 = rpid 7  $\sim$ M 16 = senc(Auth1(username\_4,rpid\_7,skA\_2),wk\_2)  $\sim$ M 17 = dhexp(g,dh spairRP 2)  $\sim$ M 18 = dhexp(g,dh spairA 2)  $\sim$ M 19 = sign(Auth4(Auth2(h(rpid\_7),aaguid\_4,senc( Auth1(username 4,rpid 7,skA 2),wk 2),spk(skA 2)), sign(Auth3(Auth2(h(rpid 7),aaguid 4,senc(Auth1( username 4,rpid 7,skA 2),wk 2),spk(skA 2)),hash( Client1(rpid\_7,nonce\_6))),skA\_2),senc(Auth1(username 4, rpid 7,skA 2),wk 2),RP1(nonce 6,rpid 7,senc(Auth1( username 4,rpid 7,skA 2),wk 2),dhexp(g,dh spairRP 2)), dhexp(g,dh spairA 2)),sskey RP 3)  $\sim$ M 20 = rpid 7  $\sim$ M 21 = nonce 6  $\sim X \ 3 = (Auth4(Auth2(h(\sim M \ 2), \sim M \ 9, \sim M \ 3, \sim M \ 11), \sim M \ 12, \sim M \ 3,$ RP1(~M 1,~M 2,~M 3,~M 6),~M 18),~M 19,Client1(  $\sim$ M 2, $\sim$ M 1)) = (Auth4(Auth2(h(rpid 7), aaguid 4,senc(Auth1(username 4,rpid 7,skA 2),wk 2),spk( skA 2)),sign(Auth3(Auth2(h(rpid 7),aaguid 4,senc( Auth1(username 4,rpid 7,skA 2),wk 2),spk(skA 2)), hash(Client1(rpid 7,nonce 6))),skA 2),senc(Auth1( username 4,rpid 7,skA 2),wk 2),RP1(nonce 6,rpid 7, senc(Auth1(username 4,rpid 7,skA 2),wk 2),dhexp( g,dh spairRP 2)),dhexp(g,dh spairA 2)),sign(Auth4( Auth2(h(rpid 7),aaguid 4,senc(Auth1(username 4, rpid 7,skA 2),wk 2),spk(skA 2)),sign(Auth3(Auth2( h(rpid 7), aaguid 4, senc(Auth1(username 4, rpid 7, skA 2),wk 2),spk(skA 2)),hash(Client1(rpid 7,nonce 6))), skA 2),senc(Auth1(username 4,rpid 7,skA 2),wk 2), RP1(nonce 6,rpid 7,senc(Auth1(username 4,rpid 7,

A trace has been found, assuming the following hypothesis: The attacker has  $\sim M_6 = dhexp(g,dh_spairRP_2[])$  The attacker has  $\sim M_7 = sign(RP1(nonce_6[],rpid_7[],senc(Auth1(username_4[],rpid_7[],skA_2[]),wk_2[]), dhexp(g,dh_spairRP_2[])),sskey_RP_3[])$ 

