							skA_2), wk_2), $spk(skA_2)$), $hash(Client1(rpid_5,challer_5))$ skA_2), $Client1(rpid_5,challenge_4)$) $\sim M_4 = h(rpid_5)$
							$\sim M_5 = aaguid_4$ $\sim M_6 = senc(Auth1(username_5,rpid_5,skA_2),w$ $\sim M_7 = spk(skA_2)$
							$\sim M_8 = sign(Auth3(Auth2(h(rpid_5),aaguid_4,senc(username_5,rpid_5,skA_2),wk_2),spk(skA_2)),ha$ $Client1(rpid_5,challenge_4))),skA_2)$ $\sim M_9 = rpid_5$
							$ \sim M_9 = rpid_5 $ $ \sim M_10 = challenge_4 $ $ \sim X_4 = (Auth2(h(rpid_5), aaguid_4, senc(Auth1(usern rpid_5, skA_2), wk_2), spk(skA_2)), sign(Auth3(Authpid_5), aaguid_4, senc(Auth1(username_5, rpid_skA_2), wk_2), spk(skA_2)), hash(Client1(rpid_5, challen_skA_2), Client1(rpid_5, challenge_4)) $
			Honest Process				Attacker
			{1}new rpid_5 {2}new clientid_1 {3}new pinAuth_3 {4}new wk_2				
		{9}insert rp_red username_s {10}insert auth_	{5}new aaguid_4 {6}new username_5 {7}new skA_2 ord(username_5,aaguid_4,senc(Auth1(5,rpid_5,skA_2),wk_2),spk(skA_2)) record(senc(Auth1(username_5,rpid_5,skA_2)) wk_2)				
			SKA_Z),WK_Z))	!			
Beginning of process RP_Auth Beginning of process	ess Client_Auth Beginning of prod	cess Client_Auth Beginning of process Client_Auth Beginning of process Client_Auth Beginning of process Client_Auth	rocess Client_Auth Beginning of process Client_Auth Beginning	of process Client_Auth Beginning of process Auth_Auth Beginning of pro	cess LoadBalancer Beginning of process LoadBalancer Beginning of process	ss LoadBalancer Beginning of process LoadBalancer Beginning of process LoadI	Balancer Beginning of process LoadBalancer
		user	name_5				
						~M = sanity1	
		username_5					
{23}get rp_record(username_5,aaguid_4,senc(Auth1(username_5,rpid_5,skA_2),wk_2),spk(skA_2)) {14}new challenge_4	username 5						
		username_5					
		username_5					
		username_5					
			username_5				
	•	(rpid_5,challenge_4,senc(Auth1(username skA_2),wk_2))	_5,rpid_5,		→		
			· · · · · · · · · · · · · · · · · · ·	roid 5 challenge 4 senc(Auth1(username 5 roid 5		$(\sim M_1, \sim M_2, \sim M_3) = (rpid_5, challenge_4, senc(Auth1) $ $username_5, rpid_5, skA_2, wk_2))$	
				skA_2),wk_2))			
			[32] event Client_Init_Auth(username_5,rpid_5)	~ X 1			
				{48}get auth_record(senc(Auth1(username_5,rpid_5, skA_2),wk_2)) {46}event Authnr_Finish_Auth(username_5,aaguid_4, senc(Auth1(username_5,rpid_5,skA_2),wk_2),spk(
				~X_2			
				◆		(Auth2(~M_4,~M_5,~M_6,~M_7),~M_8,Client1(~M_9, ~M_10))	
✓		~X_4					

rpid_5,skA_2),wk_2),spk(skA_2)),sign(Auth3(Auth2(h(rpid_5),aaguid_4,senc(Auth1(username_5,rpid_5,skA_2),wk_2),spk(skA_2)),hash(Client1(rpid_5,challenge_5)

kA_2),wk_2)
4,senc(Auth1(A_2)),hash(

A trace has been found.