~M_2 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_37),cert(vid_139,pk(vsk_37),cask_34)),pk(cask_34)), aenc((groupkey_request,sign(groupkey_request,vsk_36), cert(vid_138,pk(vsk_36),cask_35)),pk(cask_35))] \sim X_1 = (\sim M_3, \sim M_4, \sim M_5) = choice[(attvid_35,attsk_35, cert(attvid_35,pk(attsk_35),cask_34)),(attvid_34, attsk_34,cert(attvid_34,pk(attsk_34),cask_35))] ~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_39),cert(vid_141,pk(vsk_39),cask_34)),pk(cask_34)), aenc((groupkey_request,sign(groupkey_request,vsk_38), cert(vid_140,pk(vsk_38),cask_35)),pk(cask_35))] ~X_2 = (~M_8,~M_9,~M_10) = choice[(attvid_37,attsk_37, cert(attvid_37,pk(attsk_37),cask_34)),(attvid_36, attsk_36,cert(attvid_36,pk(attsk_36),cask_35))] ~M_11 = choice[aenc(((groupkey_response,vid_139, gsk(vid_139,gmsk_34),gpk(gmsk_34)),sign((groupkey_response, vid_139,gsk(vid_139,gmsk_34),gpk(gmsk_34)),cask_34)), pk(vsk_37)),aenc(((groupkey_response,vid_138,gsk(vid_138,gmsk_35)),sign((groupkey_response, vid_138,gsk(vid_138,gmsk_35)),gpk(gmsk_35)),cask_35)), pk(vsk_36))] **Honest Process** Attacker {1}new gmsk_34 {2}new cask_34 {3}new gmsk_35 {4}new cask_35 \sim M = pk(choice[cask_34,cask_35]) {10} new attvid_36 {10} new attvid_34 {11} new attsk_36 {11} new attsk_34 {12} new attvid_37 {12} new attvid_35 {13}new attsk_37 {13} new attsk_35 {16} event choice[AttackerGetsEnrollmentCertificate(attvid_35,pk(attsk_35)),AttackerGetsEnrollmentCertificate(attvid_34,pk(attsk_34))] {21} new vid_138 {22}new vsk_36 {23} new vid_139 {24} new vsk_37 $\sim M_1 = \frac{\text{choice}[\text{cert(vid}_139,\text{pk(vsk}_37),\text{cask}_34),}{\text{cert(vid}_138,\text{pk(vsk}_36),\text{cask}_35)]}$ {30} event ValidGroupKeyRequestSent(choice[vid_139, vid_138]) {16} event choice[AttackerGetsEnrollmentCertificate(attvid_37,pk(attsk_37)),AttackerGetsEnrollmentCertificate(attvid_36,pk(attsk_36))] {21} new vid_140 {22} new vsk_38 \sim M_2 {23}new vid_141 {24} new vsk_39 +X 1 $\sim M_6 = \frac{\text{choice}[\text{cert(vid}_141,\text{pk(vsk}_39),\text{cask}_34),}{\text{cert(vid}_140,\text{pk(vsk}_38),\text{cask}_35)]}$ {30} event ValidGroupKeyRequestSent(choice[vid_141, vid_140]) \sim M 7 $\sim X_2$ ~M 2 {364}get v_2777: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_2777)) && (choice[vid_139,caught-fail] =nf 1-proj-revokedcerts(v_2777))) else (success?(1-proj-revokedcerts(v_2777)) && (choice[caught-fail,vid_138] =nf 1-proj-revokedcerts(v_2777)))): else branch taken {351}event choice[ValidGroupKeyRequestReceived(cask_34,vid_139),ValidGroupKeyRequestReceived(cask_35,vid_138)] {356} event choice[ValidGroupPrivateKeySent(vid_139, gsk(vid_139,gmsk_34),gpk(gmsk_34)),ValidGroupPrivateKeySent(vid_138,gsk(vid_138,gmsk_35),gpk(gmsk_35))] ~M 11 ~M 11 {39}new vpseudosk_116 {40} new vpseudosk_117 {41} new m_76

A trace has been found.

Abbreviations