~M_2 = choice[aenc((groupkey_request, sign(groupkey_request, vsk_31),cert(vid_115,pk(vsk_31),cask_28)),pk(cask_28)), aenc((groupkey_request, sign(groupkey_request, vsk_30), cert(vid_114,pk(vsk_30),cask_29)),pk(cask_29))] ~X_1 = (~M_3,~M_4,~M_5) = choice[(attvid_29,attsk_29, cert(attvid_29,pk(attsk_29),cask_28)),(attvid_28, attsk_28,cert(attvid_28,pk(attsk_28),cask_29))] ~M_7 = choice[aenc((groupkey_request, sign(groupkey_request, vsk_33),cert(vid_117,pk(vsk_33),cask_28)),pk(cask_28)), aenc((groupkey_request, sign(groupkey_request, vsk_32), cert(vid_116,pk(vsk_32),cask_29)),pk(cask_29))] ~X_2 = (~M_8,~M_9,~M_10) = choice[(attvid_31,attsk_31, cert(attvid_31,pk(attsk_31),cask_28)),(attvid_30, attsk_30,cert(attvid_30,pk(attsk_30),cask_29))] ~M_11 = choice[aenc(((groupkey_response,vid_115, gsk(vid_115,gmsk_28),gpk(gmsk_28)),sign((groupkey_response, vid_115,gsk(vid_115,gmsk_28),gpk(gmsk_28)),cask_28)), pk(vsk_31)),aenc(((groupkey_response,vid_114,gsk(vid_114,gmsk_29)),sign((groupkey_response, vid_114,gsk(vid_114,gmsk_29),gpk(gmsk_29)),cask_29)), pk(vsk_30))] Attacker Honest Process {1}new gmsk_28 {2}new cask_28 {3}new gmsk_29 {4}new cask_29 \sim M = pk(choice[cask_28,cask_29]) {10} new attvid_30 {10} new attvid_28 {11}new attsk_30 {11}new attsk_28 {12} new attvid_29 {12} new attvid_31 {13} new attsk_31 {13}new attsk_29 {16} event choice[AttackerGetsEnrollmentCertificate(attvid_29,pk(attsk_29)),AttackerGetsEnrollmentCertificate(attvid_28,pk(attsk_28))] {21} new vid_114 {22} new vsk_30 {23} new vid_115 {24} new vsk_31 ~M_1 = choice[cert(vid_115,pk(vsk_31),cask_28), cert(vid_114,pk(vsk_30),cask_29)] {30} event ValidGroupKeyRequestSent(choice[vid_115, vid_114]) {16} event choice[AttackerGetsEnrollmentCertificate(attvid_31,pk(attsk_31)),AttackerGetsEnrollmentCertificate(attvid_30,pk(attsk_30))] ~M 2 {21}new vid_116 {22} new vsk_32 {23}new vid_117 {24} new vsk_33
$$\label{eq:mean_self_model} \begin{split} \sim & M_6 = \frac{\text{choice}[\text{cert(vid}_117,\text{pk(vsk}_33),\text{cask}_28),} \\ & \text{cert(vid}_116,\text{pk(vsk}_32),\text{cask}_29)] \end{split}$$
{30} event ValidGroupKeyRequestSent(choice[vid_117, vid_116]) ~M 7 ~M 2 {284}get v_2209: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_2209)) && (choice[vid_115,caught-fail] =nf 1-proj-revokedcerts(v_2209))) else (success?(1-proj-revokedcerts(v_2209)) && (choice[caught-fail,vid_114] =nf 1-proj-revokedcerts(v_2209)))): else branch taken {271}event choice[ValidGroupKeyRequestReceived(cask_28,vid_115),ValidGroupKeyRequestReceived(cask_29,vid_114)] {276} event choice[ValidGroupPrivateKeySent(vid_115, gsk(vid_115,gmsk_28),gpk(gmsk_28)),ValidGroupPrivateKeySent(vid_114,gsk(vid_114,gmsk_29),gpk(gmsk_29))] ~M 11 ~M 11 {39}new vpseudosk_95 {40}new vpseudosk_96 {41} new m_64

A trace has been found.

Abbreviations

[59] if choice[true,false]
This process performs a test that may succeed on one side and not on the other.