Abbreviations ~M_2 = choice[aenc(((vid_13,n_13),sign((vid_13,n_13),vsk_11),cert(vid_13,pk(vsk_11),cask_8)), pk(cask_8)),aenc(((vid_12,n_12),sign((vid_12,n_12),vsk_10),cert(vid_12,pk(vsk_10),cask_9)),pk(cask_9))] \sim X_1 = (\sim M_3, \sim M_4, \sim M_5) = choice[(attvid_9,attsk_9,cert(attvid_9,pk(attsk_9),cask_8)),(attvid_8,attsk_8,cert(attvid_8,pk(attsk_8),cask_9))] ~M_7 = choice[aenc(((vid_15,n_15),sign((vid_15,n_15),vsk_13),cert(vid_15,pk(vsk_13),cask_8)), pk(cask_8)),aenc(((vid_14,n_14),sign((vid_14,n_14),vsk_12),cert(vid_14,pk(vsk_12),cask_9)),pk(cask_9))] $\begin{array}{l} -X_2 = (\sim M_8, \sim M_9, \sim M_10) = \frac{-1}{2} & \text{choice}[(\text{attvid}_11, \text{attsk}_11, \text{cert}(\text{attvid}_11, \text{pk}(\text{attsk}_11), \text{cask}_8)), (\text{attvid}_10, \text{attsk}_10, \text{cert}(\text{attvid}_10, \text{pk}(\text{attsk}_10), \text{cask}_9))] \end{array}$ ~M_11 = choice[aenc(((groupkey_response,vid_13, n_13,gsk(vid_13,gmsk_8),gpk(gmsk_8)),sign((groupkey_response, vid_13,n_13,gsk(vid_13,gmsk_8),gpk(gmsk_8)),cask_8)), pk(vsk_11)),aenc(((groupkey_response,vid_12,n_12, gsk(vid_12,gmsk_9),gpk(gmsk_9)),sign((groupkey_response, vid_12,n_12,gsk(vid_12,gmsk_9),gpk(gmsk_9)),cask_9)), pk(vsk_10))] **Honest Process** Attacker {1}new gmsk_8 {2}new cask_8 {3}new gmsk_9 {4}new cask_9 \sim M = pk(choice[cask_8,cask_9]) {10} new attvid_8 {11}new attsk_8 {12} new attvid_9 {13}new attsk_9 {16} event choice[AttackerGetsEnrollmentCertificate(attvid_9,pk(attsk_9)),AttackerGetsEnrollmentCertificate(attvid_8,pk(attsk_8))] {21} new vid_12 {22} new vsk_10 {23} new n_12 {24} new vid_13 {25} new vsk_11 {26} new n_13 $\sim M_1 = \frac{\text{choice}[\text{cert}(\text{vid}_13,\text{pk}(\text{vsk}_11),\text{cask}_8),\text{cert}(\text{vid}_12,\text{pk}(\text{vsk}_10),\text{cask}_9)]}{\text{vid}_12,\text{pk}(\text{vsk}_10),\text{cask}_9)]}$ {32} event ValidGroupKeyRequestSent(choice[vid_13, vid_12]) ~M 2 $+X_1$ \sim M_6 = choice[cert(vid_15,pk(vsk_13),cask_8),cert(vid_14,pk(vsk_12),cask_9)] ~M 2 ~M 11 ~M 11 [{41}new vpseudosk_22] {42}new vpseudosk_23 {43}new m_24 [63] if choice[true,false]
This process performs a test that may succeed on one side and not on the other.

{10} new attvid_10

{11} new attsk_10

{12} new attvid_11

{13}new attsk_11

{21} new vid_14

{22} new vsk_12

{23} new n_14

{24} new vid_15

{25} new vsk_13

{26} new n_15

{287}get v 383: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v 383)) && (1-proj-2-tuple(1-proj-3-tuple(choice[((vid 13,n 13),sign((vid 13,n 13),vsk 11),cert(vid 13,pk(vsk 11),cask 8)),caught-fail])) =nf
1-proj-revokedcerts(v 383))) else (success?(1-proj-revokedcerts(v 383)) && (1-proj-2-tuple(1-proj-3-tuple(choice[caught-fail,((vid 12,n 12),sign((vid 12, n 12),vsk 10),cert(vid 12,pk(vsk 10),cask 9))])) =nf 1-proj-revokedcerts(v 383)))): else branch taken

{270}event choice[ValidGroupKeyRequestReceived(cask_8,vid_13),ValidGroupKeyRequestReceived(cask_9, vid_12)]

{275}event choice[ValidGroupPrivateKeySent(vid_13, gsk(vid_13,gmsk_8),gpk(gmsk_8)),ValidGroupPrivateKeySent(vid_12,gsk(vid_12,gmsk_9),gpk(gmsk_9))]

 \sim M⁷

~X 2

{32} event ValidGroupKeyRequestSent(choice[vid_15, vid_14])

{16} event choice[AttackerGetsEnrollmentCertificate(attvid_11,pk(attsk_11)),AttackerGetsEnrollmentCertificate(attvid_10,pk(attsk_10))]

A trace has been found.