Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_8,attsk_8,cert(attvid_8,pk(attsk_8),cask_8)),(attvid_9,attsk_9,cert(attvid_9,pk(attsk_9),cask_9))]
~M_5 = choice[aenc((groupkey_request,sign(groupkey_request,vsk_17),cert(vid_41,pk(vsk_17),cask_8)),pk(cask_8)),aenc((groupkey_request,sign(groupkey_request,vsk_19),cert(vid_43,pk(vsk_19),cask_9)),pk(cask_9))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request,vsk_16),cert(vid_40,pk(vsk_16),cask_8)),pk(cask_8)),aenc((groupkey_request,sign(groupkey_request,vsk_18),cert(vid_42,pk(vsk_18),cask_9)),pk(cask_9))]

A trace has been found.

Honest Process

Attacker

{1}new gmsk_8

{2}new cask_8

{3}new vid_40

{4}new vsk_16

{5}new vid_41

{6}new vsk_17

{7}new attvid_8

{8}new attsk_8

{9}new gmsk_9

{10}new cask_9

{11}new vid_42

{12}new vsk_18

{13}new vid_43

{14}new vsk_19

{15}new attvid_9

{16}new attsk_9

~M = pk(choice[cask_8,cask_9])

!

{325}event choice[AttackerGetsEnrollmentCertificate(attvid_8,pk(attsk_8)),AttackerGetsEnrollmentCertificate(attvid_9,pk(attsk_9))]

!

~X_1

~M_4 = choice[cert(vid_41,pk(vsk_17),cask_8),cert(vid_43,pk(vsk_19),cask_9)]

{177}event ValidGroupKeyRequestSent(choice[vid_41,vid_43])

~M_5

~M_6 = choice[cert(vid_40,pk(vsk_16),cask_8),cert(vid_42,pk(vsk_18),cask_9)]

{26}event ValidGroupKeyRequestSent(choice[vid_40,vid_42])

~M_7

~M_5

{400}get v_543: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_543)) && (choice[vid_41,caught-fail] =nf 1-proj-revokedcerts(v_543))) else (success?(1-proj-revokedcerts(v_543)) && (choice[caught-fail,vid_43] =nf 1-proj-revokedcerts(v_543)))): else branch taken

{358}if (if choice[true,false] then not((choice[true,false] && choice[false,caught-fail])) else not(choice[false,true]))
This process performs a test that may succeed on one side and not on the other.