| Abbreviations |
| --- |
| ~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))] |
| ~X_1 = (~M_3,~M_4,~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),gpk(gmsk_35)),sign((groupkey_response, vid_138,gsk(vid_138,gmsk_35),gpk(gmsk_35)),cask_35)), pk(vsk_36))] |

A trace has been found.