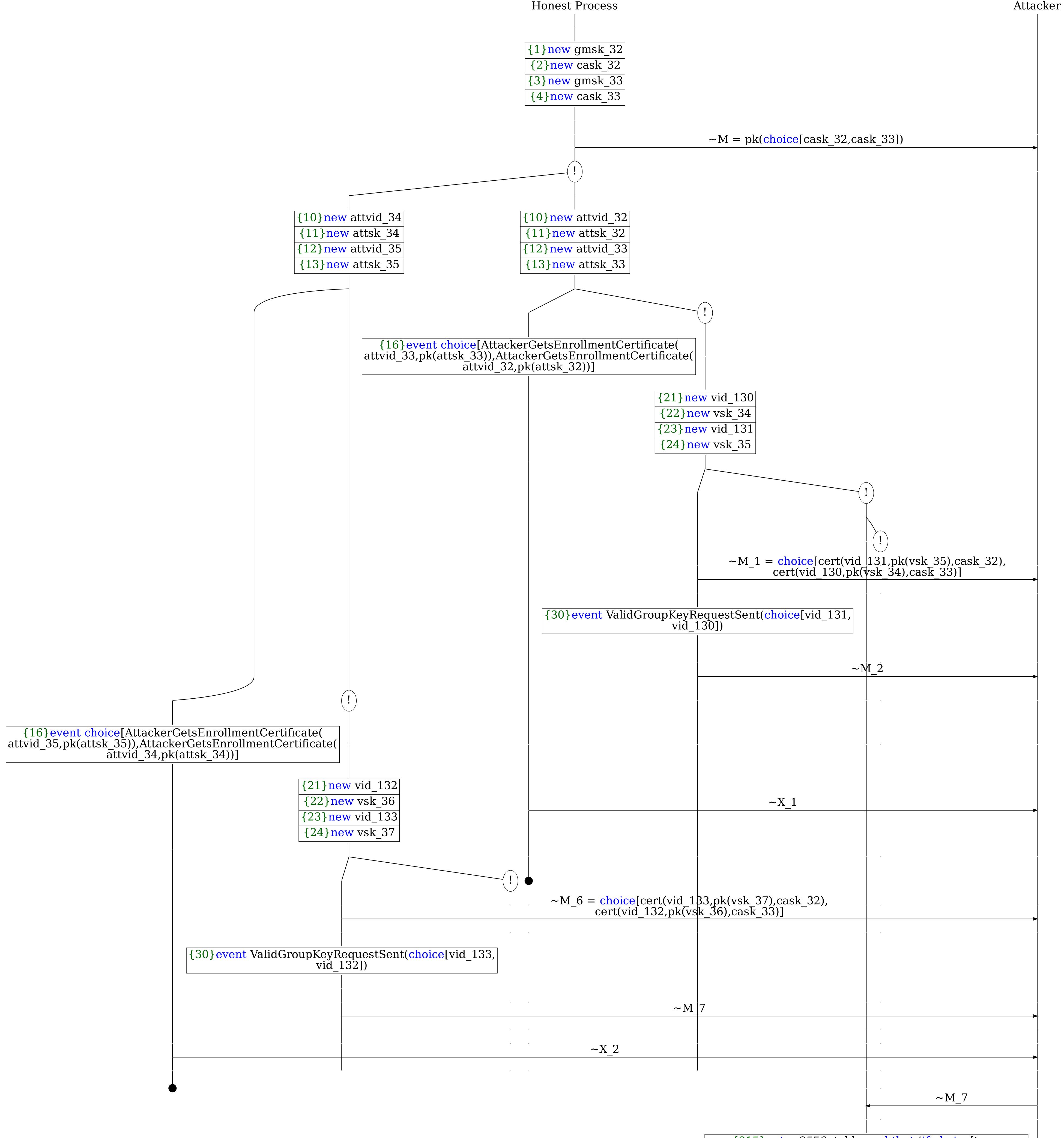
Abbreviations

- ~M_2 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_35),cert(vid_131,pk(vsk_35),cask_32)),pk(cask_32)), aenc((groupkey_request,sign(groupkey_request,vsk_34), cert(vid_130,pk(vsk_34),cask_33)),pk(cask_33))]
- ~X_1 = (~M_3,~M_4,~M_5) = choice[(attvid_33,attsk_33, cert(attvid_33,pk(attsk_33),cask_32)),(attvid_32, attsk_32,cert(attvid_32,pk(attsk_32),cask_33))]
- ~M_7 = choice[aenc((groupkey_request, sign(groupkey_request, vsk_37),cert(vid_133,pk(vsk_37),cask_32)),pk(cask_32)), aenc((groupkey_request, sign(groupkey_request, vsk_36), cert(vid_132,pk(vsk_36),cask_33)),pk(cask_33))]

A trace has been found.



{315}get v_2556: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_2556)) && (choice[vid_133,caught-fail] =nf 1-proj-revokedcerts(v_2556)) else (success?(1-proj-revokedcerts(v_2556)) && (choice[caught-fail,vid_132] =nf 1-proj-revokedcerts(v_2556)))): else branch taken

{273}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.