Abbreviations

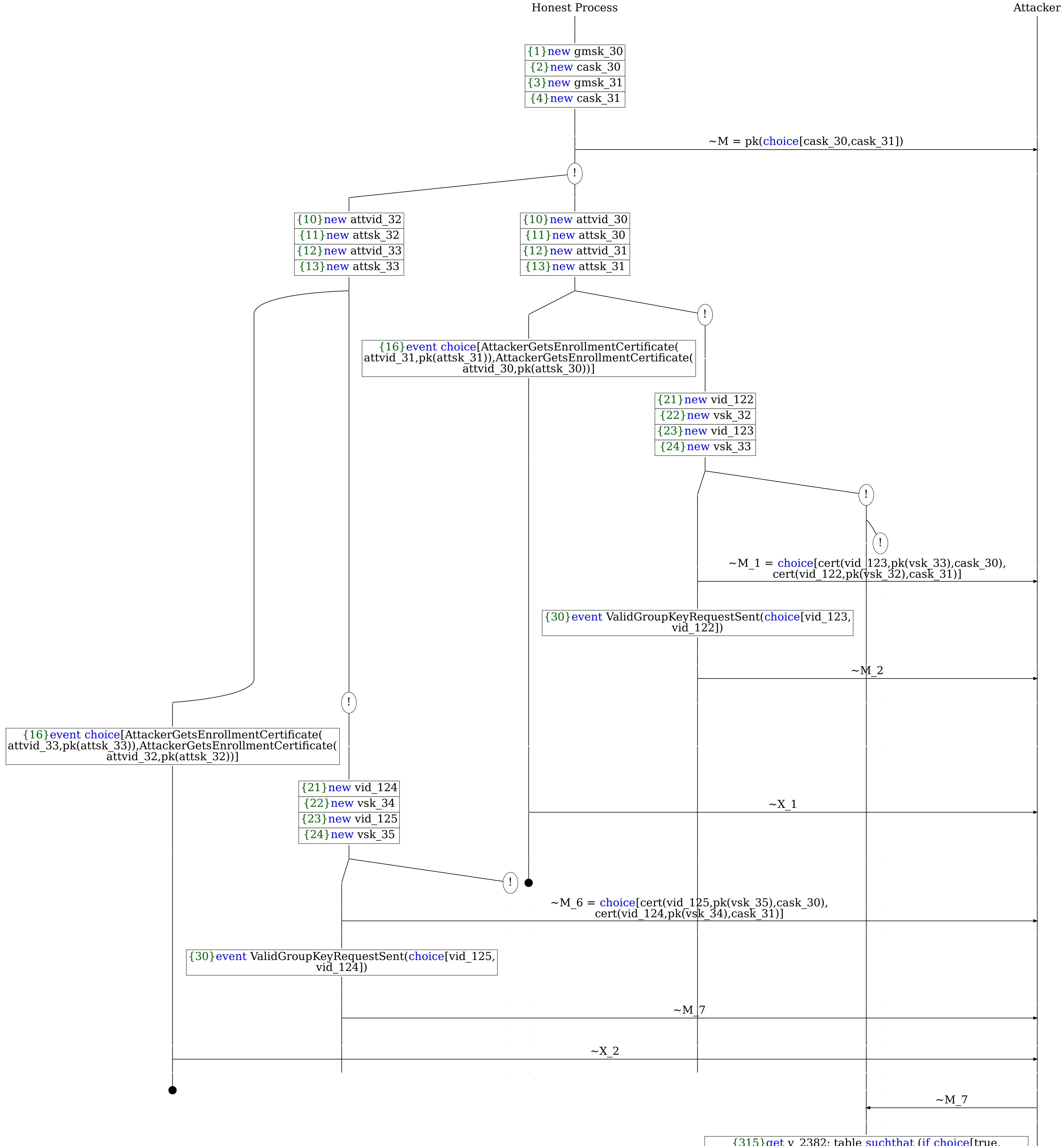
~M\_2 = choice[aenc((groupkey\_request,sign(groupkey\_request, vsk\_33),cert(vid\_123,pk(vsk\_33),cask\_30)),pk(cask\_30)), aenc((groupkey\_request,sign(groupkey\_request,vsk\_32), cert(vid\_122,pk(vsk\_32),cask\_31)),pk(cask\_31))]

~X\_1 = (~M\_3,~M\_4,~M\_5) = choice[(attvid\_31,attsk\_31, cert(attvid\_31,pk(attsk\_31),cask\_30)),(attvid\_30, attsk\_30,cert(attvid\_30,pk(attsk\_30),cask\_31))]

~M\_7 = choice[aenc((groupkey\_request, sign(groupkey\_request, vsk\_35),cert(vid\_125,pk(vsk\_35),cask\_30)),pk(cask\_30)), aenc((groupkey\_request, sign(groupkey\_request, vsk\_34), cert(vid\_124,pk(vsk\_34),cask\_31)),pk(cask\_31))]

 $\sim$ X\_2 = ( $\sim$ M\_8, $\sim$ M\_9, $\sim$ M\_10) = choice[(attvid\_33,attsk\_33, cert(attvid\_33,pk(attsk\_33),cask\_30)),(attvid\_32, attsk\_32,cert(attvid\_32,pk(attsk\_32),cask\_31))]

A trace has been found.



{315}get v\_2382: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v\_2382)) && (choice[vid\_125,caught-fail] =nf 1-proj-revokedcerts(v\_2382))) else (success?(1-proj-revokedcerts(v\_2382)) && (choice[caught-fail,vid\_124] =nf 1-proj-revokedcerts(v\_2382)))): else branch taken

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