~X_1 = aenc((groupkey_request, sign(groupkey_request, ~M_2), ~M_3), ~M)
= aenc((groupkey_request, sign(groupkey_request, attsk_3), cert(attvid_3, pk(attsk_3), cask_3)), pk(~M_7 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3)),cask_3)),pk(A trace has been found. \sim X_2 = aenc(((pseudocert(a_5,3-proj-4-tuple(1-proj-2-tuple(adec(~M_7,~M_2)))),revoke_request),sign((pseudocert(a_5,3-proj-4-tuple(1-proj-2-tuple(adec($\sim M_7$, $\sim M_2$)))), revoke_request), $\sim M_5$), $\sim M_6$), $\sim M$) = aenc(((pseudocert(**Honest Process** Attacker {1}new gmsk_4 {2}new cask_3 \sim M = pk(cask_3) {92} new attvid_4 {92} new attvid_3 {93}new attsk_4 {93} new attsk_3 Beginning of process RSU_Register Beginning of process RSU_Revoke Beginning of process RSU_Register {96} event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4)) {96} event AttackerGetsEnrollmentCertificate(attvid_3, pk(attsk_3)) $(\sim M_1, \sim M_2, \sim M_3) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_3))$ $(\sim M_4, \sim M_5, \sim M_6) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_3))$ ~X 1 {116}get revokedcerts(=attvid_3): else branch taken {109}event ValidGroupKeyRequestReceived(cask_3, {114}event ValidGroupPrivateKeySent(attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)) ~M 7 $aenc((groupkey_request,a_3,\sim M_3),\sim M) = aenc((groupkey_request,a_3,cert(attvid_3,pk(attsk_3),cask_3)),pk(cask_3))$ ~X_2 {154}get revokedcerts(=attvid_4): else branch taken {127}event ValidRevocationReportReceived(pseudocert(a_5,gsk(attvid_3,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_3)) {153}get revokedcerts(=attvid_3): else branch taken {130}event RevokedVid(attvid_3) {131}insert revokedcerts(attvid_3) {116}get revokedcerts(attvid_3)

{107} event RevokedCannotGetGroupKey(attvid_3)

Abbreviations