~M\_9 = aenc(((groupkey\_response,attvid\_3,gsk(attvid\_3,gmsk\_4),gpk(gmsk\_4)),sign((groupkey\_response,attvid\_3,gsk(attvid\_3,g ~M\_10 = aenc(((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_4),gpk(gmsk\_4)),sign((groupkey\_response,vid\_7,gsk(vid\_7,gsk(vid\_7,gsk(vid\_7,gsk(vid\_7,gsk(yid\_4)),cask\_4)),pk(vsk\_3)) (groupkey\_request,sign(groupkey\_request,vsk\_3), pseudocert(pk(vsk\_3),gsk(attvid\_3,gmsk\_4))) ~M\_11 = aenc(((pseudocert(pk(vsk\_3),gsk(attvid\_3,gmsk\_4)),revoke\_request),sign((pseudocert(pk(vsk\_3), gsk(attvid\_3,gmsk\_4)),revoke\_request),vsk\_3),cert( vid\_7,pk(vsk\_3),cask\_4)),pk(cask\_4)) ~X\_3 = aenc(((pseudocert(a\_7,3-proj-4-tuple(1-proj-2-tuple(adec(~M\_9,~M\_3)))),revoke\_request),sign((pseudocert(a\_7,3-proj-4-tuple(1-proj-2-tuple(adec(~M\_9,~M\_3)))),revoke\_request),~M\_6),~M\_7),~M) = aenc(((pseudocert(a\_7,gsk(attvid\_3,gmsk\_4)),revoke\_request),sign((pseudocert(a\_7,gsk(attvid\_3,gmsk\_4)),revoke\_request),attsk\_4),cert(attvid\_4,pk(attsk\_4),cask\_4)),pk(cask\_4)) Attacker **Honest Process** {1}new gmsk\_4 {2}new cask\_4  $\sim$ M = pk(cask\_4) Beginning of process CASecretKeyReveal {5}new vid\_7 {6}new vsk\_3 {155}event CASKReveal(cask\_4)  $\sim$  M\_1 = cask\_4 {91} new attvid\_4 {91} new attvid\_3 {92} new attsk\_4 {92} new attsk\_3 Beginning of process CARegister Beginning of process CARegister Beginning of process CARegister Beginning of process CARevoke Beginning of process CARevoke {95} event AttackerGetsEnrollmentCertificate(attvid\_4, pk(attsk\_4)) {95} event AttackerGetsEnrollmentCertificate(attvid\_3, pk(attsk\_4))  $(\sim M_2, \sim M_3, \sim M_4) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_4))$  $(\sim M_5, \sim M_6, \sim M_7) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_4))$ Beginning of process VehicleRegistration {14} event ValidGroupKeyRequestSent(vid\_7) ~M\_8 = aenc((groupkey\_request,sign(groupkey\_request, vsk\_3),cert(vid\_7,pk(vsk\_3),cask\_4)),pk(cask\_4)) aenc((groupkey\_request,a\_2,~M\_4),~M) = aenc((groupkey\_request,a\_2,cert(attvid\_3,pk(attsk\_3),cask\_4)),pk(cask\_4)) {115}get revokedcerts(=attvid\_3): else branch taken {108}event ValidGroupKeyRequestReceived(cask\_4, {113}event ValidGroupPrivateKeySent(attvid\_3,gsk(attvid\_3,gmsk\_4),gpk(gmsk\_4)) ~M\_8 = aenc((groupkey\_request,sign(groupkey\_request, vsk\_3),cert(vid\_7,pk(vsk\_3),cask\_4)),pk(cask\_4)) {115}get revokedcerts(=vid\_7): else branch taken {108}event ValidGroupKeyRequestReceived(cask\_4, vid\_7) {113}event ValidGroupPrivateKeySent(vid\_7,gsk(vid\_7,gmsk\_4),gpk(gmsk\_4))  $\sim$  M\_10 {21} event ValidGroupPrivateKeyReceived(vid\_7,gsk(vid\_7,gmsk\_4),gpk(gmsk\_4)) Beginning of process VehicleReport(vid\_7, vsk\_3, cert(vid\_7,pk(vsk\_3),cask\_4), pk(cask\_4), gpk(gmsk\_4)) ~X 2 {47} event RevocationAsked(vid\_7,cert(vid\_7,pk(vsk\_3),cask\_4),pseudocert(pk(vsk\_3),gsk(attvid\_3,gmsk\_4)))  $\sim$  M\_11 {153}get revokedcerts(=attvid\_4): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a\_7,gsk(attvid\_3,gmsk\_4)),cert(attvid\_4,pk(attsk\_4),cask\_4)) {152}get revokedcerts(=attvid\_3): else branch taken {129}event RevokedVid(attvid\_3)  $\sim$  M<sub>1</sub>1 {153}get revokedcerts(=vid\_7): else branch taken {126} event ValidRevocationReportReceived(pseudocert(pk(vsk\_3),gsk(attvid\_3,gmsk\_4)),cert(vid\_7,pk(vsk\_3),cask\_4)) {152}get revokedcerts(=attvid\_3): else branch taken {129}event RevokedVid(attvid\_3) {130}insert revokedcerts(attvid\_3) {115}get revokedcerts(attvid\_3)

Abbreviations

 $\sim X_1 = aenc((groupkey\_request, sign(groupkey\_request, \sim M_3), \sim M_4), \sim M$ 

= aenc((groupkey\_request, sign(groupkey\_request, attsk\_3),cert(attvid\_3,pk(attsk\_3),cask\_4)),pk(

A trace has been found.