Abbreviations  $\sim X_1 = aenc((groupkey\_request, sign(groupkey\_request, \sim M_2), \sim M_3), \sim M$ = aenc((groupkey\_request, sign(groupkey\_request, attsk\_3),cert(attvid\_3,pk(attsk\_3),cask\_3)),pk( ~M\_8 = aenc(((groupkey\_response,attvid\_3,gsk(attvid\_3,gmsk\_5),gpk(gmsk\_5)),sign((groupkey\_response,attvid\_3,gsk(attvid\_3,g ~M\_9 = aenc(((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_5),gpk(gmsk\_5)),sign((groupkey\_response,vid\_7,gsk(vid\_7,gsk(vid\_7,gsk(vid\_7,gmsk\_5)),cask\_3)),pk(vsk\_4))  $\sim$ X\_2 = (a\_5,sign(a\_5,a\_6),pseudocert(pk(a\_6),3-proj-4-tuple( 1-proj-2-tuple(adec( $\sim$ M\_8, $\sim$ M\_2)))))
= (a\_5,sign(  $a_5,a_6)$ , pseudocert(pk( $a_6$ ), gsk(attvid\_3, gmsk\_5)))  $\sim$ M\_10 = aenc(((pseudocert(pk(a\_6),gsk(attvid\_3, gmsk\_5)),revoke\_request),sign((pseudocert(pk(a\_6), gsk(attvid\_3,gmsk\_5)),revoke\_request),vsk\_4),cert( vid\_7,pk(vsk\_4),cask\_3)),pk(cask\_3))  $\sim X_3 = aenc((pseudocert(a_8, 3-proj-4-tuple(1-proj-2-tuple($ adec(~M\_8,~M\_2)))),revoke\_request),sign((pseudocert( Attacker  $\sim$ M = pk(cask\_3) Beginning of process CARevoke ~M\_7 = aenc((groupkey\_request,sign(groupkey\_request, vsk\_4),cert(vid\_7,pk(vsk\_4),cask\_3)),pk(cask\_3)) **∼**M 9 ~X 3 ~M\_10 {158}get revokedcerts(=vid\_7): else branch taken

A trace has been found.

**Honest Process** {1}new gmsk\_5 {2}new cask\_3 {92} new attvid\_4 {92}new attvid\_3 {6}new vid\_7 {93}new attsk\_4 {93}new attsk\_3 Beginning of process CA Beginning of process CA Beginning of process CARevoke {96} event AttackerGetsEnrollmentCertificate(attvid\_4, {96} event AttackerGetsEnrollmentCertificate(attvid\_3, pk(attsk\_4)) pk(attsk\_3))  $(\sim M_1, \sim M_2, \stackrel{\downarrow}{\sim} M_3) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_3))$  $(\sim M_4, \sim M_5, \sim M_6) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_3))$ Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid\_7)  $\sim$  M\_7 = aenc((groupkey\_request, sign(groupkey\_request, vsk\_4),cert(vid\_7,pk(vsk\_4),cask\_3)),pk(cask\_3)) {116}get revokedcerts(=attvid\_3): else branch taken {109}event ValidGroupKeyRequestReceived(cask\_3, attvid\_3) {114}event ValidGroupPrivateKeySent(attvid\_3,gsk(attvid\_3,gmsk\_5),gpk(gmsk\_5)) {116}get revokedcerts(=vid\_7): else branch taken {109}event ValidGroupKeyRequestReceived(cask\_3, vid 7) {114}event ValidGroupPrivateKeySent(vid\_7,gsk(vid\_7,gmsk\_5),gpk(gmsk\_5))  $\sim$ M\_9 {22} event ValidGroupPrivateKeyReceived(vid\_7,gsk(vid\_7,gmsk\_5),gpk(gmsk\_5)) Beginning of process VehicleReport(vid\_7, vsk\_4, cert(vid\_7,pk(vsk\_4),cask\_3), pk(cask\_3), gpk(gmsk\_5)) {48} event RevocationAsked(vid\_7,cert(vid\_7,pk(vsk\_4),cask\_3),pseudocert(pk(a\_6),gsk(attvid\_3,gmsk\_5)))  $\sim$  M<sub>10</sub> {158}get revokedcerts(=attvid\_4): else branch taken {127} event ValidRevocationReportReceived(pseudocert(a\_8,gsk(attvid\_3,gmsk\_5)),cert(attvid\_4,pk(attsk\_4),cask\_3)) {157}get revokedcerts(=attvid\_3): else branch taken {130}event RevokedVid(attvid\_3) {131}insert revokedcerts(attvid\_3) {127} event ValidRevocationReportReceived(pseudocert(pk(a\_6),gsk(attvid\_3,gmsk\_5)),cert(vid\_7,pk(vsk\_4),cask\_3)) {157}get revokedcerts(attvid\_3)