cask 4) \sim M_10 = aenc(((groupkey_response,attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)),sign((groupkey_response, attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)),cask_4)), pk(attsk_5)) $\sim X_2 = aenc((pseudocert(a_6, 3-proj-4-tuple(1-proj-2-tuple($ adec(~M_10,~M_5)))),revoke_request),sign((pseudocert(a_6,3-proj-4-tuple(1-proj-2-tuple(adec($\sim M_10$, $\sim M_5)))),$ revoke_request), $\sim M_8$), $\sim M_9$), $\sim M$ A trace has been found. = aenc(((pseudocert(a_6,gsk(attvid_5,gmsk_4)),revoke_request),sign((pseudocert(a_6,gsk(attvid_5,gmsk_4)),revoke_request), attsk_6),cert(attvid_6,pk(attsk_6),cask_4)),pk(\sim X_3 = aenc(((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(\sim M_10, \sim M_5)))),revoke_request),sign((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(\sim M_10, \sim M_5)))), revoke_request), $\sim M_2$), $\sim M_3$), $\sim M$ = aenc(((pseudocert(Attacker **Honest Process** {1}new gmsk_4 {2}new cask_4 \sim M = pk(cask_4) {92} new attvid_5 {92} new attvid_4 {92} new attvid_6 {93}new attsk_6 {93} new attsk_5 {93}new attsk_4 Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke Beginning of process CA {96} event AttackerGetsEnrollmentCertificate(attvid_5, pk(attsk_5)) {96} event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4)) {96} event AttackerGetsEnrollmentCertificate(attvid_6, pk(attsk_6)) $(\sim M_1, \sim M_2, \sim M_3) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_4))$ $(\sim M_4, \sim M_5, \sim M_6) = (attvid_5, attsk_5, cert(attvid_5, pk(attsk_5), cask_4))$ $(\sim M_7, \sim M_8, \sim M_9) = (attvid_6, attsk_6, cert(attvid_6, pk(attsk_6), cask_4))$ $aenc((groupkey_request,a_3,\sim M_6),\sim M) = aenc((groupkey_request,a_3,cert(attvid_5,pk(attsk_5),cask_4)),pk(cask_4))$ ~X 1 {116}get revokedcerts(=attvid_5): else branch taken {109}event ValidGroupKeyRequestReceived(cask_4, attvid 5) {114}event ValidGroupPrivateKeySent(attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)) \sim M₁₀ {154}get revokedcerts(=attvid_6): else branch taken {127} event ValidRevocationReportReceived(pseudocert(a_6,gsk(attvid_5,gmsk_4)),cert(attvid_6,pk(attsk_6),cask_4)) {153}get revokedcerts(=attvid_5): else branch taken {130}event RevokedVid(attvid_5) ~X 3 {154}get revokedcerts(=attvid_4): else branch taken {127} event ValidRevocationReportReceived(pseudocert(a_8,gsk(attvid_5,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_4)) {153}get revokedcerts(=attvid_5): else branch taken {130}event RevokedVid(attvid_5) {131}insert revokedcerts(attvid_5) {116}get revokedcerts(attvid_5) {107} event RevokedCannotGetGroupKey(attvid_5)

Abbreviations

 $\sim X_1 = aenc((groupkey_request, sign(groupkey_request, \sim M_5), \sim M_6), \sim M$

= aenc((groupkey_request, sign(groupkey_request,

attsk_5),cert(attvid_5,pk(attsk_5),cask_4)),pk(