$\begin{array}{c} Abbreviations \\ \sim X_1 = aenc((groupkey_request,sign(groupkey_request,\sim M_3),\\ \sim M_4),\sim M) \\ = aenc((groupkey_request,sign(groupkey_request,\\ attsk_3),cert(attvid_3,pk(attsk_3),cask_4)),pk(\\ cask_4)) \\ \sim M_9 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gmsk_4)),pk(\\ attsk_3)) \\ \sim X_2 = aenc(((pseudocert(a_5,3-proj-4-tuple(1-proj-2-tuple(adec(\sim M_9,\sim M_3)))),revoke_request),sign((pseudocert(a_5,3-proj-4-tuple(adec(\sim M_9,\sim M_3)))),revoke_request),\sim M_6),\sim M_7),\sim M) \\ = aenc(((pseudocert(a_5,gsk(attvid_3,gmsk_4)),revoke_request),sign((pseudocert(a_5,gsk(attvid_3,gmsk_4)),revoke_request), \\ \end{array}$

A trace has been found.

