

A trace has been found.

Abbreviations
$\sim X_1 = \text{aenc}(\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \sim M_2, \sim M_3), \sim M)$ $= \text{aenc}(\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{attsk}_3, \text{cert}(\text{attvid}_3, \text{pk}(\text{attsk}_3), \text{cask}_3)), \text{pk}(\text{cask}_3))$
$\sim M_7 = \text{aenc}(\text{groupkey_response}, \text{attvid}_3, \text{gsk}(\text{attvid}_3, \text{gmsk}_4), \text{gpk}(\text{gmsk}_4), \text{sign}(\text{groupkey_response}, \text{attvid}_3, \text{gsk}(\text{attvid}_3, \text{gmsk}_4), \text{gpk}(\text{gmsk}_4)), \text{cask}_3), \text{pk}(\text{attsk}_3))$
$\sim X_2 = \text{aenc}(\text{pseudocert}(\text{a_5_3-proj-4-tuple}(1\text{-proj-2-tuple}(\text{adec}(\sim M_7, \sim M_2)))), \text{revoke_request}), \text{sign}(\text{pseudocert}(\text{a_5_3-proj-4-tuple}(1\text{-proj-2-tuple}(\text{adec}(\sim M_7, \sim M_2)))), \text{revoke_request}), \sim M_5), \sim M_6, \sim M)$ $= \text{aenc}(\text{pseudocert}(\text{a_5_gsk}(\text{attvid}_3, \text{gmsk}_4), \text{revoke_request}), \text{sign}(\text{pseudocert}(\text{a_5_gsk}(\text{attvid}_3, \text{gmsk}_4), \text{revoke_request}), \text{attsk}_4, \text{cert}(\text{attvid}_4, \text{pk}(\text{attsk}_4), \text{cask}_3)), \text{pk}(\text{cask}_3))$

