

Abbreviations
$\sim X_1 = \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \sim M_2), \sim M_3), \sim M)$ $= \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{attsk_2}, \text{cert}(\text{attvid_2}, \text{pk}(\text{attsk_2}), \text{cask_4})), \text{pk}(\text{cask_4})))$
$\sim M_5 = \text{aenc}(((\text{groupkey_response}, \text{attvid_2}, \text{gsk}(\text{attvid_2}, \text{gmsk_4}), \text{gpk}(\text{gmsk_4})), \text{sign}((\text{groupkey_response}, \text{attvid_2}, \text{gsk}(\text{attvid_2}, \text{gmsk_4}), \text{gpk}(\text{gmsk_4})), \text{cask_4})), \text{pk}(\text{attsk_2})))$
$\sim M_6 = \text{aenc}(((\text{groupkey_response}, \text{vid_7}, \text{gsk}(\text{vid_7}, \text{gmsk_4}), \text{gpk}(\text{gmsk_4})), \text{sign}((\text{groupkey_response}, \text{vid_7}, \text{gsk}(\text{vid_7}, \text{gmsk_4}), \text{gpk}(\text{gmsk_4})), \text{cask_4})), \text{pk}(\text{vsk_4})))$
$\sim X_2 = (\text{a_4}, \text{sign}(\text{a_4}, \text{a_5}), \text{pseudocert}(\text{pk}(\text{a_5}), 3\text{-proj-4-tuple}(1\text{-proj-2-tuple}(\text{adec}(\sim M_5, \sim M_2))))))$ $= (\text{a_4}, \text{sign}(\text{a_4}, \text{a_5}), \text{pseudocert}(\text{pk}(\text{a_5}), \text{gsk}(\text{attvid_2}, \text{gmsk_4})))$

A trace has been found.

