

Abbreviations
$\sim X_1 = (\sim M_1, \sim M_2, \sim M_3) = \text{choice}[(\text{attvid_6}, \text{attsk_6}, \text{cert}(\text{attvid_6}, \text{pk}(\text{attsk_6}), \text{cask_6})), (\text{attvid_7}, \text{attsk_7}, \text{cert}(\text{attvid_7}, \text{pk}(\text{attsk_7}), \text{cask_7}))]$
$\sim M_5 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_13}), \text{cert}(\text{vid_19}, \text{pk}(\text{vsk_13}), \text{cask_6})), \text{pk}(\text{cask_6})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_14}), \text{cert}(\text{vid_20}, \text{pk}(\text{vsk_14}), \text{cask_7})), \text{pk}(\text{cask_7}))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_12}), \text{cert}(\text{vid_18}, \text{pk}(\text{vsk_12}), \text{cask_6})), \text{pk}(\text{cask_6})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_15}), \text{cert}(\text{vid_21}, \text{pk}(\text{vsk_15}), \text{cask_7})), \text{pk}(\text{cask_7}))]$
$\sim M_8 = \text{choice}[\text{aenc}(((\text{groupkey_response}, \text{vid_19}, \text{gsk}(\text{vid_19}, \text{gmsk_6}), \text{gpk}(\text{gmsk_6})), \text{sign}((\text{groupkey_response}, \text{vid_19}, \text{gsk}(\text{vid_19}, \text{gmsk_6}), \text{gpk}(\text{gmsk_6})), \text{cask_6})), \text{pk}(\text{vsk_13})), \text{aenc}(((\text{groupkey_response}, \text{vid_20}, \text{gsk}(\text{vid_20}, \text{gmsk_7}), \text{gpk}(\text{gmsk_7})), \text{sign}((\text{groupkey_response}, \text{vid_20}, \text{gsk}(\text{vid_20}, \text{gmsk_7}), \text{gpk}(\text{gmsk_7})), \text{cask_7})), \text{pk}(\text{vsk_14}))]$

A trace has been found.

