

Abbreviations
$\sim X_1 = (\sim M_1, \sim M_2, \sim M_3) = \text{choice}[(\text{attvid_14}, \text{attsk_14}, \text{cert}(\text{attvid_14}, \text{pk}(\text{attsk_14}), \text{cask_14})), (\text{attvid_15}, \text{attsk_15}, \text{cert}(\text{attvid_15}, \text{pk}(\text{attsk_15}), \text{cask_15}))]$
$\sim M_5 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_29}), \text{cert}(\text{vid_71}, \text{pk}(\text{vsk_29}), \text{cask_14})), \text{pk}(\text{cask_14})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_30}), \text{cert}(\text{vid_72}, \text{pk}(\text{vsk_30}), \text{cask_15})), \text{pk}(\text{cask_15}))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_28}), \text{cert}(\text{vid_70}, \text{pk}(\text{vsk_28}), \text{cask_14})), \text{pk}(\text{cask_14})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_31}), \text{cert}(\text{vid_73}, \text{pk}(\text{vsk_31}), \text{cask_15})), \text{pk}(\text{cask_15}))]$

A trace has been found.

