

Abbreviations
$\sim X_1 = (\sim M_1, \sim M_2, \sim M_3) = \text{choice}[(\text{attvid_16}, \text{attsk_16}, \text{cert}(\text{attvid_16}, \text{pk}(\text{attsk_16}), \text{cask_16})), (\text{attvid_17}, \text{attsk_17}, \text{cert}(\text{attvid_17}, \text{pk}(\text{attsk_17}), \text{cask_17}))]$
$\sim M_5 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_33}), \text{cert}(\text{vid_81}, \text{pk}(\text{vsk_33}), \text{cask_16})), \text{pk}(\text{cask_16})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_34}), \text{cert}(\text{vid_82}, \text{pk}(\text{vsk_34}), \text{cask_17})), \text{pk}(\text{cask_17}))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_32}), \text{cert}(\text{vid_80}, \text{pk}(\text{vsk_32}), \text{cask_16})), \text{pk}(\text{cask_16})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_35}), \text{cert}(\text{vid_83}, \text{pk}(\text{vsk_35}), \text{cask_17})), \text{pk}(\text{cask_17}))]$

A trace has been found.

