

Abbreviations
$\sim M_2 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_33}), \text{cert}(\text{vid_123}, \text{pk}(\text{vsk_33}), \text{cask_30})), \text{pk}(\text{cask_30})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_32}), \text{cert}(\text{vid_122}, \text{pk}(\text{vsk_32}), \text{cask_31})), \text{pk}(\text{cask_31}))]$
$\sim X_1 = (\sim M_3, \sim M_4, \sim M_5) = \text{choice}[(\text{attvid_31}, \text{attsk_31}, \text{cert}(\text{attvid_31}, \text{pk}(\text{attsk_31}), \text{cask_30})), (\text{attvid_30}, \text{attsk_30}, \text{cert}(\text{attvid_30}, \text{pk}(\text{attsk_30}), \text{cask_31}))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_35}), \text{cert}(\text{vid_125}, \text{pk}(\text{vsk_35}), \text{cask_30})), \text{pk}(\text{cask_30})), \text{aenc}((\text{groupkey_request}, \text{sign}(\text{groupkey_request}, \text{vsk_34}), \text{cert}(\text{vid_124}, \text{pk}(\text{vsk_34}), \text{cask_31})), \text{pk}(\text{cask_31}))]$
$\sim X_2 = (\sim M_8, \sim M_9, \sim M_{10}) = \text{choice}[(\text{attvid_33}, \text{attsk_33}, \text{cert}(\text{attvid_33}, \text{pk}(\text{attsk_33}), \text{cask_30})), (\text{attvid_32}, \text{attsk_32}, \text{cert}(\text{attvid_32}, \text{pk}(\text{attsk_32}), \text{cask_31}))]$

A trace has been found.

