

Abbreviations
$\sim X_1 = (\sim M_1, \sim M_2, \sim M_3) = \text{choice}[\text{attvid_10, attsk_10, cert(attvid_10, pk(attsk_10), cask_10)}, \text{attvid_11, attsk_11, cert(attvid_11, pk(attsk_11), cask_11)}]]$
$\sim M_5 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{nonce_45}, \text{sign}(\text{groupkey_request}, \text{vsk_21}), \text{cert}(\text{vid_51}, \text{pk}(\text{vsk_21}), \text{cask_10})), \text{pk}(\text{cask_10})), \text{aenc}((\text{groupkey_request}, \text{nonce_46}, \text{sign}(\text{groupkey_request}, \text{vsk_22}), \text{cert}(\text{vid_52}, \text{pk}(\text{vsk_22}), \text{cask_11})), \text{pk}(\text{cask_11}))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey_request}, \text{nonce_44}, \text{sign}(\text{groupkey_request}, \text{vsk_20}), \text{cert}(\text{vid_50}, \text{pk}(\text{vsk_20}), \text{cask_10})), \text{pk}(\text{cask_10})), \text{aenc}((\text{groupkey_request}, \text{nonce_47}, \text{sign}(\text{groupkey_request}, \text{vsk_23}), \text{cert}(\text{vid_53}, \text{pk}(\text{vsk_23}), \text{cask_11})), \text{pk}(\text{cask_11}))]$
$\sim M_8 = \text{choice}[\text{aenc}(((\text{groupkey_response}, \text{nonce_45}, \text{vid_51}, \text{gsk}(\text{vid_51}, \text{gmsk_10}), \text{gpk}(\text{gmsk_10})), \text{sign}((\text{groupkey_response}, \text{nonce_45}, \text{vid_51}, \text{gsk}(\text{vid_51}, \text{gmsk_10}), \text{gpk}(\text{gmsk_10})), \text{cask_10})), \text{pk}(\text{vsk_21})), \text{aenc}(((\text{groupkey_response}, \text{nonce_46}, \text{vid_52}, \text{gsk}(\text{vid_52}, \text{gmsk_11}), \text{gpk}(\text{gmsk_11})), \text{sign}((\text{groupkey_response}, \text{nonce_46}, \text{vid_52}, \text{gsk}(\text{vid_52}, \text{gmsk_11}), \text{gpk}(\text{gmsk_11})), \text{cask_11})), \text{pk}(\text{vsk_22}))]$

A trace has been found.

