

Abbreviations
$\sim X_1 = (\sim M_1, \sim M_2, \sim M_3) = \text{choice}[(\text{attvid}_9, \text{attsk}_9, \text{cert}(\text{attvid}_9, \text{pk}(\text{attsk}_9), \text{cask}_8)), (\text{attvid}_8, \text{attsk}_8, \text{cert}(\text{attvid}_8, \text{pk}(\text{attsk}_8), \text{cask}_9))]$
$\sim M_5 = \text{choice}[\text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \text{vsk}_{11}), \text{cert}(\text{vid}_{35}, \text{pk}(\text{vsk}_{11}), \text{cask}_8)), \text{pk}(\text{cask}_8)), \text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \text{vsk}_{10}), \text{cert}(\text{vid}_{34}, \text{pk}(\text{vsk}_{10}), \text{cask}_9)), \text{pk}(\text{cask}_9))]$
$\sim M_7 = \text{choice}[\text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \text{vsk}_{13}), \text{cert}(\text{vid}_{37}, \text{pk}(\text{vsk}_{13}), \text{cask}_8)), \text{pk}(\text{cask}_8)), \text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \text{vsk}_{12}), \text{cert}(\text{vid}_{36}, \text{pk}(\text{vsk}_{12}), \text{cask}_9)), \text{pk}(\text{cask}_9))]$

A trace has been found.

