

Abbreviations
$\sim X_1 = \text{aenc}(((\text{groupkey_response}, \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1))), a_1, a_2), \text{sign}((\text{groupkey_response}, \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1))), a_1, a_2), \sim M_1)), \text{getpk}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1))))$ $=$ $\text{aenc}(((\text{groupkey_response}, \text{vid_8}, a_1, a_2), \text{sign}(\text{groupkey_response}, \text{vid_8}, a_1, a_2), \text{cask_4})), \text{pk}(\text{vsk_4}))$

A trace has been found.

