

Abbreviations
$\begin{aligned} \sim X_1 = & \text{aenc}(((\text{groupkey_response}, \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_1, \sim M_2))), a_1, a_2), \text{sign}((\text{groupkey_response}, \\ & \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_1, \sim M_2))), a_1, a_2), \\ & \sim M_2)), \text{getpk}(3\text{-proj-3-tuple}(\text{adec}(\sim M_1, \sim M_2)))) \\ & = \\ & \text{aenc}(((\text{groupkey_response}, \text{vid}_7, a_1, a_2), \text{sign}(\text{groupkey_response}, \text{vid}_7, a_1, a_2), \text{cask}_4)), \text{pk}(\text{vsk}_4)) \end{aligned}$

A trace has been found.

