

A trace has been found.

Abbreviations

$$\begin{aligned} \sim X_1 &= \text{aenc}(((\text{groupkey_response}, \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1))), a_1, \text{gpk}(a_2)), \text{sign}((\text{groupkey_response}, \\ &\quad \text{getid}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1))), a_1, \text{gpk}(a_2)), \sim M_1)), \text{getpk}(3\text{-proj-3-tuple}(\text{adec}(\sim M_2, \sim M_1)))) \\ &= \\ &\quad \text{aenc}(((\text{groupkey_response}, \text{vid}_9, a_1, \text{gpk}(a_2)), \\ &\quad \text{sign}((\text{groupkey_response}, \text{vid}_9, a_1, \text{gpk}(a_2)), \text{cask}_4)), \\ &\quad \text{pk}(\text{vsk}_4)) \end{aligned}$$
