

A trace has been found.

Abbreviations
$\sim M_3 = \text{aenc}((\text{groupkey_response}, \text{vid}_8, \text{gsk}(\text{vid}_8, \text{gmsk}_5), \text{gpk}(\text{gmsk}_5)), \text{sign}((\text{groupkey_response}, \text{vid}_8, \text{gsk}(\text{vid}_8, \text{gmsk}_5), \text{gpk}(\text{gmsk}_5), \text{cask}_3)), \text{pk}(\text{vsk}_4))$

