

Abbreviations
$\sim X\_1 = \text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \sim M\_3), \sim M\_4), \sim M)$ $= \text{aenc}((\text{groupkey\_request}, \text{sign}(\text{groupkey\_request}, \text{attsk\_3}), \text{cert}(\text{attvid\_3}, \text{pk}(\text{attsk\_3}), \text{cask\_4})), \text{pk}(\text{cask\_4}))$
$\sim M\_8 = \text{aenc}(((\text{groupkey\_response}, \text{attvid\_3}, \text{gsk}(\text{attvid\_3}, \text{gmsk\_4}), \text{gpk}(\text{gmsk\_4})), \text{sign}((\text{groupkey\_response}, \text{attvid\_3}, \text{gsk}(\text{attvid\_3}, \text{gmsk\_4}), \text{gpk}(\text{gmsk\_4})), \text{cask\_4})), \text{pk}(\text{attsk\_3}))$
$\sim X\_2 = \text{aenc}(((\text{pseudocert}(\text{a\_5}, 3\text{-proj-4-tuple}(1\text{-proj-2-tuple}(\text{adec}(\sim M\_8, \sim M\_3))))), \text{revoke\_request}), \text{sign}((\text{pseudocert}(\text{a\_5}, 3\text{-proj-4-tuple}(1\text{-proj-2-tuple}(\text{adec}(\sim M\_8, \sim M\_3))))), \text{revoke\_request}), \sim M\_6), \sim M\_7), \sim M)$ $= \text{aenc}(((\text{pseudocert}(\text{a\_5}, \text{gsk}(\text{attvid\_3}, \text{gmsk\_4})), \text{revoke\_request}), \text{sign}((\text{pseudocert}(\text{a\_5}, \text{gsk}(\text{attvid\_3}, \text{gmsk\_4})), \text{revoke\_request}), \text{attsk\_4}), \text{cert}(\text{attvid\_4}, \text{pk}(\text{attsk\_4}), \text{cask\_4})), \text{pk}(\text{cask\_4}))$

A trace has been found.

