

A trace has been found.

Abbreviations
$\sim X\_1 = \text{aenc}(((a\_1, \text{revoke\_request}), \text{sign}((a\_1, \text{revoke\_request}), \sim M\_2), \sim M\_3), \sim M)$ $= \text{aenc}(((a\_1, \text{revoke\_request}), \text{sign}(a\_1, \text{revoke\_request}, \text{attsk\_2}), \text{cert}(\text{attvid\_2}, \text{pk}(\text{attsk\_2}, \text{cask\_3})), \text{pk}(\text{cask\_3})))$

