

Abbreviations
$\sim X_1 = \text{aenc}(((a_1, \text{revoke_request}), \text{sign}((a_1, \text{revoke_request}), \sim M_3), \sim M_4), \sim M)$ $= \text{aenc}(((a_1, \text{revoke_request}), \text{sign}(a_1, \text{revoke_request}, \text{attsk_2}, \text{cert}(\text{attvid_2}, \text{pk}(\text{attsk_2}, \text{cask_3})), \text{pk}(\text{cask_3}))), \text{pk}(\text{cask_3}))$

A trace has been found.

