

Abbreviations

$$\begin{aligned} \sim X_1 &= \text{aenc}(((a_1, \text{revoke_request}), \text{sign}((a_1, \text{revoke_request}), \\ &\quad \sim M_2), \sim M_3), \sim M) \\ &= \text{aenc}(((a_1, \text{revoke_request}), \text{sign}(\\ &\quad (a_1, \text{revoke_request}), \text{attsk}_2), \text{cert}(\text{attvid}_2, \text{pk}(\\ &\quad \text{attsk}_2), \text{cask}_4)), \text{pk}(\text{cask}_4)) \end{aligned}$$

A trace has been found.

