

A trace has been found.

Abbreviations
$\sim X\_1 = \text{aenc}(\text{make\_presentation}(a\_5, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M\_3, a\_3)), \sim M\_1, \text{sign}((a\_5, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M\_3, a\_3)), \sim M\_1), a\_3)), \sim M\_2)$ $= \text{aenc}(\text{make\_presentation}(a\_5, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB})), \text{sign}((a\_5, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB})), a\_3)), \text{pk}(\text{skB}))$

