

A trace has been found.

Abbreviations
$\sim M\_4 = \text{make\_presentation}(\text{didB}, \text{didU}, a\_3, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB})), \text{sign}((\text{didB}, \text{didU}, a\_3, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB}))), \text{skU}))$
$\sim X\_1 = \text{aenc}(\text{make\_presentation}(a\_6, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M\_5, a\_4)), 4\text{-proj-4-tuple}(\text{resolve\_presentation}(\sim M\_4, \sim M\_1))), \text{sign}((a\_6, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M\_5, a\_4)), 4\text{-proj-4-tuple}(\text{resolve\_presentation}(\sim M\_4, \sim M\_1))), a\_4)), \sim M\_2)$ $= \text{aenc}(\text{make\_presentation}(a\_6, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB})), \text{sign}((a\_6, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB}))), a\_4)), \text{pk}(\text{skB}))$

