

A trace has been found.

Abbreviations
$\sim M\_5 = \text{aenc}(\text{make\_presentation}(\text{didB}, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB})), \text{sign}((\text{didB}, \text{didU}, \text{nonceB\_4}, \text{make\_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null\_cred}), \text{skB}))), \text{skU})), \text{pk}(\text{skB}))$

