

A trace has been found.

Abbreviations
$\sim M_5 = \text{aenc}(\text{make_presentation}(\text{didB}, \text{didU}, \text{nonceB}_3, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{skB})), \text{sign}((\text{didB}, \text{didU}, \text{nonceB}_3, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{skB})))), \text{skU})), \text{pk}(\text{skB}))$

