

Abbreviations
$\begin{aligned} \sim X_1 &= \text{aenc}(\text{make_presentation}(a_5, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_3, a_3)), \sim M_1, \text{sign}((a_5, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_3, a_3)), \sim M_1), a_3)), \sim M_2) \\ &= \text{aenc}(\text{make_presentation}(a_5, \text{didU}, \text{nonceB}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB})), \text{sign}((a_5, \text{didU}, \text{nonceB}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), a_3)), \text{pk}(\text{skB})) \end{aligned}$

A trace has been found.

