

A trace has been found.

Abbreviations
$\sim M_6 = \text{make_presentation}(\text{didU}, \text{didTPP}, \text{dataTPP}, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB})), \text{sign}((\text{didU}, \text{didTPP}, \text{dataTPP}, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), \text{skU})), \text{sign}((\text{didU}, \text{didTPP}, \text{a}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB})), \text{sign}((\text{didU}, \text{didTPP}, \text{dataTPP}, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), \text{skU}))), \text{sign}((\text{didU}, \text{didTPP}, \text{a}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), \text{skU})))$
$\sim X_1 = \text{make_presentation}(\text{didU}, \text{a}_5, \text{3-proj-3-tuple}(\text{adec}(\sim M_7, \text{a}_6)), \text{make_credential}(\text{didU}, \text{a}_5, \text{a}_8, \text{4-proj-4-tuple}(\text{resolve_credential}(\text{4-proj-4-tuple}(\text{resolve_presentation}(\sim M_6, \sim M_1), \sim M_2)), \text{sign}((\text{didU}, \text{a}_5, \text{a}_8, \text{4-proj-4-tuple}(\text{resolve_credential}(\text{4-proj-4-tuple}(\text{resolve_presentation}(\sim M_6, \sim M_1), \sim M_2)), \text{sign}((\text{didU}, \text{a}_5, \text{3-proj-3-tuple}(\text{adec}(\sim M_7, \text{a}_6)), \text{make_credential}(\text{didU}, \text{a}_5, \text{a}_8, \text{4-proj-4-tuple}(\text{resolve_credential}(\text{4-proj-4-tuple}(\text{resolve_presentation}(\sim M_6, \sim M_1), \sim M_2)), \text{sign}((\text{didU}, \text{a}_5, \text{a}_8, \text{4-proj-4-tuple}(\text{resolve_credential}(\text{4-proj-4-tuple}(\text{resolve_presentation}(\sim M_6, \sim M_1), \sim M_2)), \text{a}_9)), \text{sign}((\text{didU}, \text{a}_5, \text{a}_8, \text{4-proj-4-tuple}(\text{resolve_credential}(\text{4-proj-4-tuple}(\text{resolve_presentation}(\sim M_6, \sim M_1), \sim M_2)), \text{a}_9)), \text{a}_6)) = \text{make_presentation}(\text{didU}, \text{a}_5, \text{nonceB}_4, \text{make_credential}(\text{didU}, \text{a}_5, \text{a}_8, \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{didU}, \text{a}_5, \text{a}_8, \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{a}_9)), \text{sign}((\text{didU}, \text{a}_5, \text{a}_8, \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{didU}, \text{a}_5, \text{a}_8, \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{a}_9))), \text{a}_6))$

