

A trace has been found.

Abbreviations
$\sim M_5 = \text{aenc}(\text{make\_presentation}(didB, didU, nonceB_4, \text{make\_credential}(didB, didU, dataU, null_cred, sign(didB, didU, dataU, null_cred, skB)), sign(didB, didU, nonceB_4, \text{make\_credential}(didB, didU, dataU, null_cred, sign(didB, didU, dataU, null_cred, skB))), skU), pk(skB))$

