

A trace has been found.

Abbreviations
$\sim M_5 = \text{aenc}(\text{make_presentation}(didB, didU, nonceB_4, make_credential(didB, didU, dataU, null_cred, sign((didB, didU, dataU, null_cred), skB)), sign((didB, didU, nonceB_4, make_credential(didB, didU, dataU, null_cred, sign((didB, didU, dataU, null_cred), skB))), sign((didB, didU, dataU, null_cred, skB))), pk(skB))$

