

Abbreviations
$\sim X_1 = (\text{Auth2}(\text{h}(\sim M_1), a_1, a_2, \text{spk}(a_3)), \text{sign}(\text{Auth3}(\text{Auth2}(\text{h}(\sim M_1), a_1, a_2, \text{spk}(a_3)), \text{hash}(\text{Client1}(\sim M_1, \sim M_2))), a_3), \text{Client1}(\sim M_1, \sim M_2))$ $= (\text{Auth2}(\text{h}(\text{rp_id_4}), a_1, a_2, \text{spk}(a_3)), \text{sign}(\text{Auth3}(\text{Auth2}(\text{h}(\text{rp_id_4}), a_1, a_2, \text{spk}(a_3)), \text{hash}(\text{Client1}(\text{rp_id_4}, \text{challenge_3}))), a_3), \text{Client1}(\text{rp_id_4}, \text{challenge_3}))$

A trace has been found.

