Abbreviations

~X_1 = (a_7,encxor((a_8,(id(pk(a_1),a_2),(sign((sSignature1,(id(pk(a_1),a_2),(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),(pk(a_1),(a_9,edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),exp(a_7,~M_8)),stwo,(id(pk(a_1),a_2),(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),(pk(a_1),a_9))),hash_length))))))),a_10,a_1),a_9))),edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),exp(a_7,~M_8)),stzero,hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),plaintext_length))) =
(a_7,encxor((a_8,(id(pk(a_1),a_2),(sign((sSignature1,(id(pk(a_1),a_2),(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),(pk(a_1),(a_9,edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),exp(a_7,X_1)),stwo,(id(pk(a_1),a_2),(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),(pk(a_1),a_9))),hash_length))))))),a_10,a_1),a_9))),edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),exp(a_7,X_1)),stzero,hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),plaintext_length)))

A trace has been found.