Abbreviations
~M_3 = exp(g,Y_1)
~M_4 = encxor(a_3,(id(pk(sk_3),exp(g,ltdh_1)),(sign((sSignature1,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (pk(sk_3),(a_4,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8, Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),a_4))),hash_length)))))),srep,sk_3),a_4))), edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8,Y_1)),stzero,hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), plaintext_length))
~M_5 = a_3
~X_1 = (~M,(hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (~M_1,(a_4,(edhoc_kdf(hkdfextract(hash((wrap(~M_3), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),exp(a_8,~M_6)),stwo,(~M, (hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (~M_1,a_4)),hash_length),mangle(1-proj-2-tuple(2-proj-2-tuple(2-proj-2-tuple(decxor(~M_4,edhoc_kdf(hkdfextract(hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), exp(a_8,~M_6)),stzero,hash(wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),plaintext_length))))),a_11)))))) = (id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7), (wrap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),(a_4,(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),exp(a_8,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),(pk(sk_3),a_4))),hash_length)))), sign((sSignature1,(id(pk(sk_3),exp(g,ltdh_1)), (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (pk(sk_3),(a_4,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8, Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),a_4))),hash_length))))))),a_11,sk_3)))))))
~X_2 = (~M,(hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (~M_1,(a_4,(edhoc_kdf(hkdfextract(hash((wrap(~M_3), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),exp(a_8,~M_6)),stwo,(~M, (hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (~M_1,a_4)),hash_length),mangle(1-proj-2-tuple(2-proj-2-tuple(2-proj-2-tuple(decxor(~M_4,edhoc_kdf(hkdfextract(hash((wrap(~M_3),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), exp(a_8,~M_6)),stzero,hash(wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),plaintext_length))))),a_12)))) = (id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7), (wrap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),(a_4,(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),exp(a_8,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8), (wrap(a_9),a_10))))))),(pk(sk_3),a_4))),hash_length)))), sign((sSignature1,(id(pk(sk_3),exp(g,ltdh_1)), (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (pk(sk_3),(a_4,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8, Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),a_4))),hash_length)))))),a_12,sk_3))))))

A trace has been found.