Abbreviations
~M_3 = exp(g,Y_1)
~M_4 = encxor((a_1,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),(a_2,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),a_2))),hash_length))))))),srep,sk_3),a_2))),edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),stzero,hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),plaintext_length))
~M_5 = a_1
~X_1 = aeadenc((id(a_9,a_10),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),sfive,hash((wrap(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(~M,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),stzero,hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),plaintext_length)))))),a_2))),~M_1))),hash_length),a_10,~M_6)),six,(id(a_9,a_10),(hash((wrap(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(~M,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),stzero,hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),plaintext_length)))))),a_2))),~M_1))),(a_10,a_11)),hash_length),a_11)),a_12,edhoc_kdf(hkdfextract(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),sthree,hash((wrap(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(~M,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),stzero,hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),plaintext_length)))))),a_2))),~M_1)),key_length),edhoc_kdf(hkdfextract(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),sfour,hash((wrap(hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(~M,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,~M_6)),stzero,hash((wrap(~M_3),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),plaintext_length)))))),a_2))),~M_1))),iv_length)) = aeadenc((id(a_9,a_10),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1))),sfive,hash((wrap(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),(a_2,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),a_2))),hash_length))))))),srep,sk_3),a_2))),(pk(sk_3))),hash_length),exp(a_10,Y_1)),six,(id(a_9,a_10),(hash((wrap(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),(a_2,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),a_2))),hash_length))))))),srep,sk_3),a_2))),(pk(sk_3))),hash_length),(a_10,a_11)),hash_length),a_11)),a_12,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),sthree,hash((wrap(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(a_1,(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_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),(a_2,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(pk(sk_3),a_2))),hash_length))))))),srep,sk_3),a_2))),(pk(sk_3))),hash_length),iv_length)

A trace has been found.