

Abbreviations
~M_27372 = non_confirmable
~M_27373 = CoAP_POSTCode
~M_27374 = messageid_26249
~M_27375 = token_26250
~M_27378 = partial_iv_26248
~M_27379 = IDir_26244
~M_27380 = idcontext_26247
~M_27377 = aeadEncrypt(HKDF(msecret_26245,msalt_26246,(IDir_26244,idcontext_26247,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_26244,partial_iv_26248,HKDF(msecret_26245,msalt_26246,(emptyId,idcontext_26247,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_26235,a_26236)),(encrypt0,oscore_version_one,AES_CCM,IDir_26244,partial_iv_26248)))
~X_1 = (a_26238,a_26239,a_26240,a_26241,(~M_27378,~M_27173,~M_27175),~M_27377) = (a_26238,a_26239,a_26240,a_26241,(partial_iv_26248,IDir_26244,idcontext_26247),aeadEncrypt(HKDF(msecret_26245,msalt_26246,(IDir_26244,idcontext_26247,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_26244,partial_iv_26248,HKDF(msecret_26245,msalt_26246,(emptyId,idcontext_26247,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_26235,a_26236)),(encrypt0,oscore_version_one,AES_CCM,IDir_26244,partial_iv_26248)))
~X_2 = (a_26238,a_26239,a_26240,a_26241,(~M_27378,~M_27173,~M_27175),~M_27377) = (a_26238,a_26239,a_26240,a_26241,(partial_iv_26248,IDir_26244,idcontext_26247),aeadEncrypt(HKDF(msecret_26245,msalt_26246,(IDir_26244,idcontext_26247,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDir_26244,partial_iv_26248,HKDF(msecret_26245,msalt_26246,(emptyId,idcontext_26247,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_26235,a_26236)),(encrypt0,oscore_version_one,AES_CCM,IDir_26244,partial_iv_26248)))

A trace has been found.

