

Abbreviations
~M_29899 = non_confirmable
~M_29900 = CoAP_POSTCode
~M_29901 = messageid_28772
~M_29902 = token_28773
~M_29905 = partial_iv_28771
~M_29906 = IDri_28767
~M_29907 = idcontext_28770
~M_29904 = aeadEncrypt(HKDF(msecret_28768,msalt_28769,(IDri_28767,idcontext_28770,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDri_28767,partial_iv_28771,HKDF(msecret_28768,msalt_28769,(emptyId,idcontext_28770,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_28758,a_28759)),(encrypt0,oscore_version_one,AES_CCM,IDri_28767,partial_iv_28771)))
~X_1 = (a_28761,a_28762,a_28763,a_28764,(~M_29905,~M_29701,~M_29702),~M_29904) = (a_28761,a_28762,a_28763,a_28764,(partial_iv_28771,IDri_28767,idcontext_28770),aeadEncrypt(HKDF(msecret_28768,msalt_28769,(IDri_28767,idcontext_28770,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDri_28767,partial_iv_28771,HKDF(msecret_28768,msalt_28769,(emptyId,idcontext_28770,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_28758,a_28759)),(encrypt0,oscore_version_one,AES_CCM,IDri_28767,partial_iv_28771)))
~X_2 = (a_28761,a_28762,a_28763,a_28764,(~M_29905,~M_29701,~M_29702),~M_29904) = (a_28761,a_28762,a_28763,a_28764,(partial_iv_28771,IDri_28767,idcontext_28770),aeadEncrypt(HKDF(msecret_28768,msalt_28769,(IDri_28767,idcontext_28770,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDri_28767,partial_iv_28771,HKDF(msecret_28768,msalt_28769,(emptyId,idcontext_28770,AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv))),(CoAP_GETCode,isLightBulbTurnedOn),msg1(a_28758,a_28759)),(encrypt0,oscore_version_one,AES_CCM,IDri_28767,partial_iv_28771)))

A trace has been found.

