Abbreviations \sim M_28267 = coap_version_one \sim M 28268 = non confirmable ~M 28269 = bounded_by(token_27653) \sim M 28270 = CoAP POSTCode \sim M 28271 = messageid 27654 \sim M 28272 = token 27653 \sim M_28275 = partial_iv_27644 \sim M 28276 = IDir 27640 \sim M 28277 = idcontext 27643 \sim M_28274 = aeadEncrypt(HKDF(msecret_27641,msalt_27642, (IDir 27640,idcontext 27643,AES CCM,label key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_27640, partial iv 27644,HKDF(msecret 27641,msalt 27642, (emptyId,idcontext_27643,AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))),((CoAP_GETCode,isLightBulbTurnedOn), msg_1id_27655),(encrypt0,oscore_version_one,AES_CCM, IDir 27640,partial iv 27644)) \sim X 1 = (coap version one, confirmable, a 27634, a 27635, a_27636,a_27637,(~M_28275,~M_28276,~M_28277),~M_28274) (coap version one, confirmable, a 27634, a 27635, a_27636,a_27637,(partial_iv_27644,IDir_27640,idcontext_27643), aeadEncrypt(HKDF(msecret 27641,msalt 27642,(IDir 27640, idcontext 27643,AES CCM,label key),alg key length(AES_CCM,label_key)),aeadNonce(IDir_27640,partial iv 27644, HKDF(msecret 27641,msalt 27642,(emptyId,idcontext 27643, AES_CCM,label_iv),alg_key_length(AES_CCM,label_iv))), ((CoAP GETCode, is LightBulbTurnedOn), msg 1id 27655), (encrypt0,oscore version one,AES CCM,IDir 27640, partial iv 27644))) \sim X 2 = (coap version one, confirmable, a 27634, a 27635, a 27636,a 27637,(~M 28275,~M 28276,~M 28277),~M 28274) (coap version one, confirmable, a 27634, a 27635, a 27636,a 27637,(partial iv 27644,IDir 27640,idcontext 27643), aeadEncrypt(HKDF(msecret 27641,msalt 27642,(IDir 27640, idcontext 27643,AES CCM,label key),alg key length(AES CCM, label key), aeadNonce(IDir 27640, partial iv 27644, HKDF(msecret 27641,msalt 27642,(emptyId,idcontext_27643, AES CCM, label iv), alg key length(AES CCM, label iv))), ((CoAP_GETCode,isLightBulbTurnedOn),msg 1id 27655), (encrypt0,oscore version one,AES CCM,IDir 27640, partial_iv_27644))) \sim M 29113 = coap version one \sim M 29114 = non confirmable \sim M 29115 = bounded by(a 27637) ~M 29116 = CoAP CHANGEDCode \sim M 29117 = responseId 29100 \sim M 29118 = a 27637 \sim M 29119 = empty ~M 29120 = aeadEncrypt(HKDF(msecret 27641,msalt 27642, (IDri 27639,idcontext 27643,AES CCM,label key), alg_key_length(AES_CCM,label_key)),aeadNonce(IDir_27640, partial_iv_27644,HKDF(msecret_27641,msalt_27642, (emptyId,idcontext 27643,AES CCM,label iv),alg key length(

A trace has been found.

