Abbreviations
$\sim$ M_27856 = coap_version_one
$\sim$ M_27857 = non_confirmable
~M_27858 = bounded_by(token_27653)
$\sim$ M_27859 = CoAP_POSTCode
$\sim$ M_27860 = messageid_27654
$\sim M_27861 = token_27653$
$\sim M_27864 = partial_iv_27644$
$\sim M_27865 = IDir_27640$
$\sim M_27866 = idcontext_27643$

~M\_27863 = 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))

(), |

A trace has been found.

~X\_1 = (coap\_version\_one,confirmable,a\_27634,a\_27635, a\_27636,a\_27637,(~M\_27864,~M\_27865,~M\_27866),~M\_27863)

(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)))

