A trace has been found.

Abbreviations

-M\_55284 = non\_confirmable

-M\_55285 = CoAP\_POSTCode

-M\_55286 = messageid\_54814

-M\_55287 = token\_54807

-M\_55290 = partial\_iv\_54811

-M\_55291 = IDir\_54808

-M\_55292 = idcontext\_54810

-M\_55289 = aeadEncrypt(HKDF(msecret\_54812,msalt\_54813,

~M\_55289 = aeadEncrypt(HKDF(msecret\_54812,msalt\_54813, (IDir\_54808,idcontext\_54810,AES\_CCM,label\_key, alg\_key\_length(AES\_CCM,label\_key))),aeadNonce(IDir\_54808,partial\_iv\_54811,HKDF(msecret\_54812, msalt\_54813,(emptyId,idcontext\_54810,AES\_CCM,label\_iv, alg\_key\_length(AES\_CCM,label\_iv)))),((CoAP\_GETCode, isLightBulbTurnedOn),msg1(a\_54796,a\_54796)),(encrypt0, oscore\_version\_one,AES\_CCM,IDir\_54808,partial\_iv\_54811))

a\_54802,(partial\_iv\_54811,IDir\_54808,idcontext\_54810),
aeadEncrypt(HKDF(msecret\_54812,msalt\_54813,(IDir\_54808,
idcontext\_54810,AES\_CCM,label\_key,alg\_key\_length(
AES\_CCM,label\_key))),aeadNonce(IDir\_54808,partial\_iv\_54811,
HKDF(msecret\_54812,msalt\_54813,(emptyId,idcontext\_54810,
AES\_CCM,label\_iv,alg\_key\_length(AES\_CCM,label\_iv)))),
((CoAP\_GETCode,isLightBulbTurnedOn),msg1(a\_54796,
a\_54796)),(encrypt0,oscore\_version\_one,AES\_CCM,
IDir\_54808,partial\_iv\_54811)))

~M 55527 = non confirmable

 $\sim$ M\_55528 = CoAP\_CHANGEDCode  $\sim$ M\_55529 = responseId\_54855

~M\_55529 = responseId\_54855

 $\sim$ M\_55530 = a\_54802  $\sim$ M 55531 = empty

~M\_55532 = aeadEncrypt(HKDF(msecret\_54812,msalt\_54813, (IDri\_54809,idcontext\_54810,AES\_CCM,label\_key, alg\_key\_length(AES\_CCM,label\_key))),aeadNonce( IDir\_54808,partial\_iv\_54811,HKDF(msecret\_54812, msalt\_54813,(emptyId,idcontext\_54810,AES\_CCM,label\_iv, alg\_key\_length(AES\_CCM,label\_iv)))),((CoAP\_CONTENTCode, bounded\_by((CoAP\_GETCode,isLightBulbTurnedOn))), msg2(a\_54796,a\_54796)),(encrypt0,oscore\_version\_one, AES\_CCM,IDir\_54808,partial\_iv\_54811))

 $\sim$ X\_2 = ( $\sim$ M\_55287,a\_54799,a\_54800,a\_54801,empty, $\sim$ M\_55532)

(token\_54807,a\_54799,a\_54800,a\_54801,empty,aeadEncrypt(
HKDF(msecret\_54812,msalt\_54813,(IDri\_54809,idcontext\_54810,
AES\_CCM,label\_key,alg\_key\_length(AES\_CCM,label\_key))),
aeadNonce(IDir\_54808,partial\_iv\_54811,HKDF(msecret\_54812,
msalt\_54813,(emptyId,idcontext\_54810,AES\_CCM,label\_iv,
alg\_key\_length(AES\_CCM,label\_iv)))),((CoAP\_CONTENTCode,
bounded\_by((CoAP\_GETCode,isLightBulbTurnedOn))),
msg2(a\_54796,a\_54796)),(encrypt0,oscore\_version\_one,
AES\_CCM,IDir\_54808,partial\_iv\_54811)))

