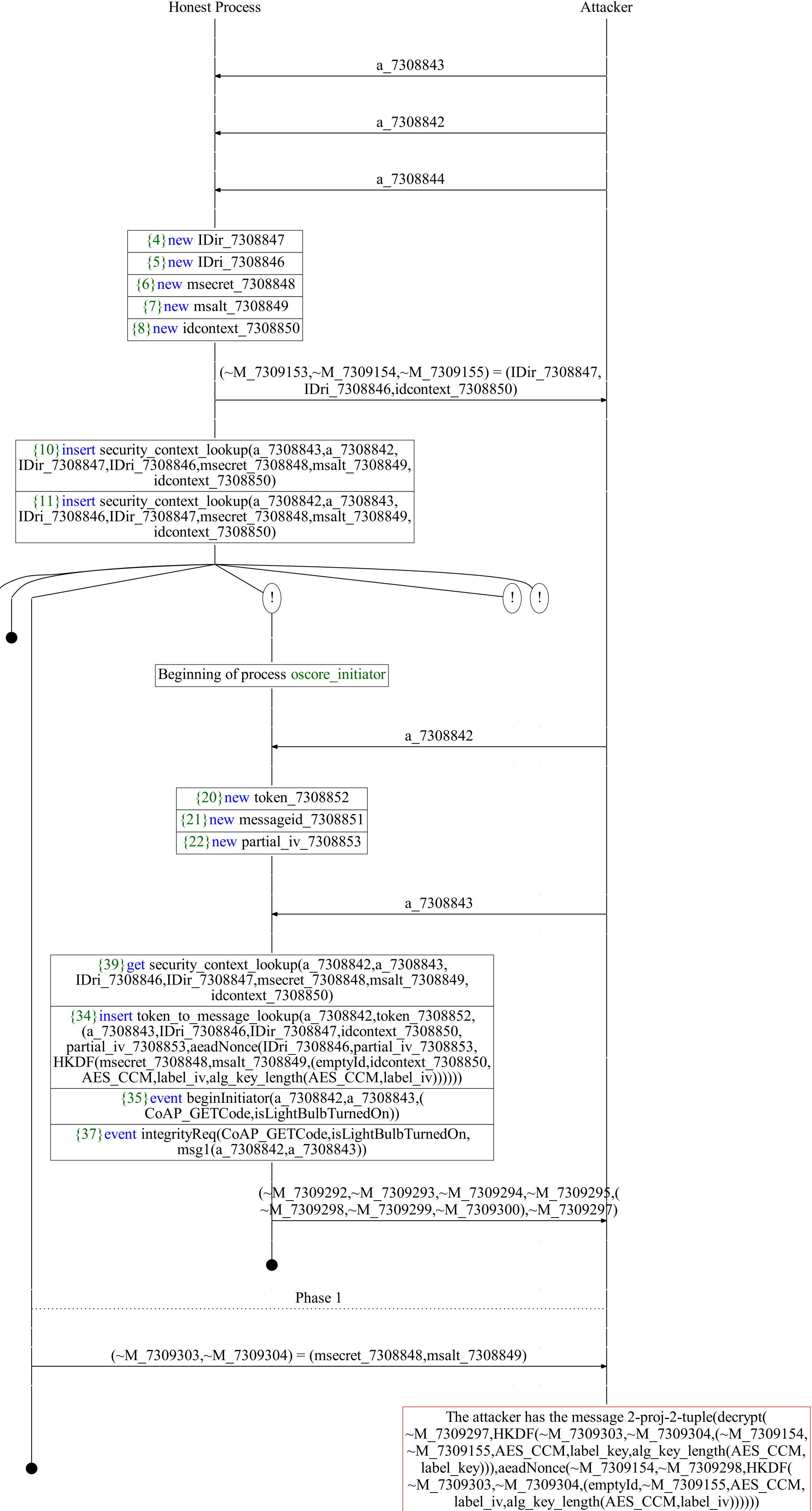
Abbreviations
$\sim$ M_7309292 = non_confirmable
~M_7309293 = CoAP_POSTCode
~M_7309294 = messageid_7308851
~M_7309295 = token_7308852
~M_7309298 = partial_iv_7308853
~M_7309299 = IDri_7308846
~M_7309300 = idcontext_7308850

A trace has been found.

 $\sim M_{7309297} = aeadEncrypt(HKDF(msecret_7308848,msalt_7308849,$ (IDri\_7308846,idcontext\_7308850,AES\_CCM,label\_key, alg key length(AES CCM,label key)),aeadNonce( IDri\_7308846,partial\_iv\_7308853,HKDF(msecret\_7308848, msalt\_7308849,(emptyId,idcontext\_7308850,AES\_CCM, label\_iv,alg\_key\_length(AES\_CCM,label\_iv))),( (CoAP\_GETCode,isLightBulbTurnedOn),msg1(a\_7308842, a\_7308843)),(encrypt0,oscore\_version\_one,AES\_CCM, IDri 7308846,partial iv 7308853))



= msg1(a 7308842, a 7308843) in phase 1