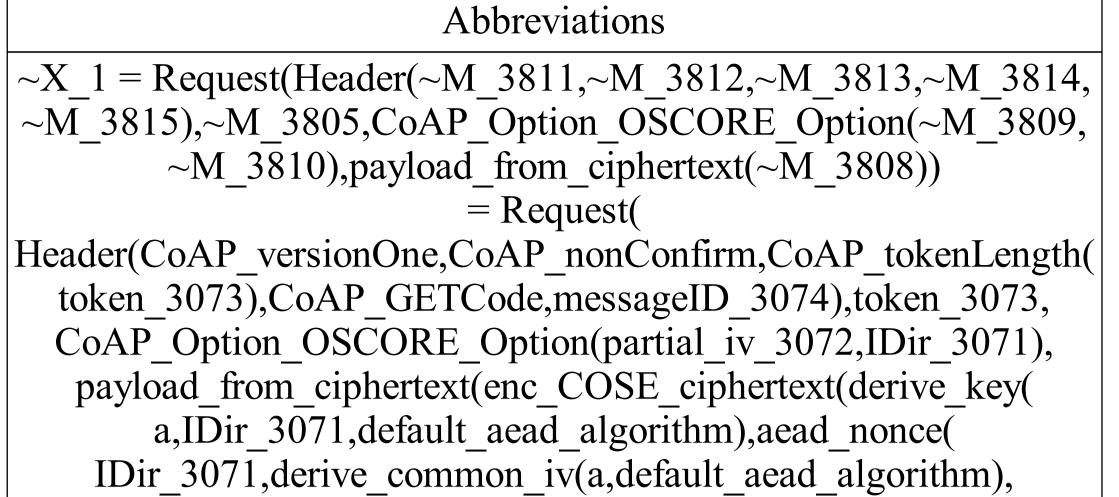
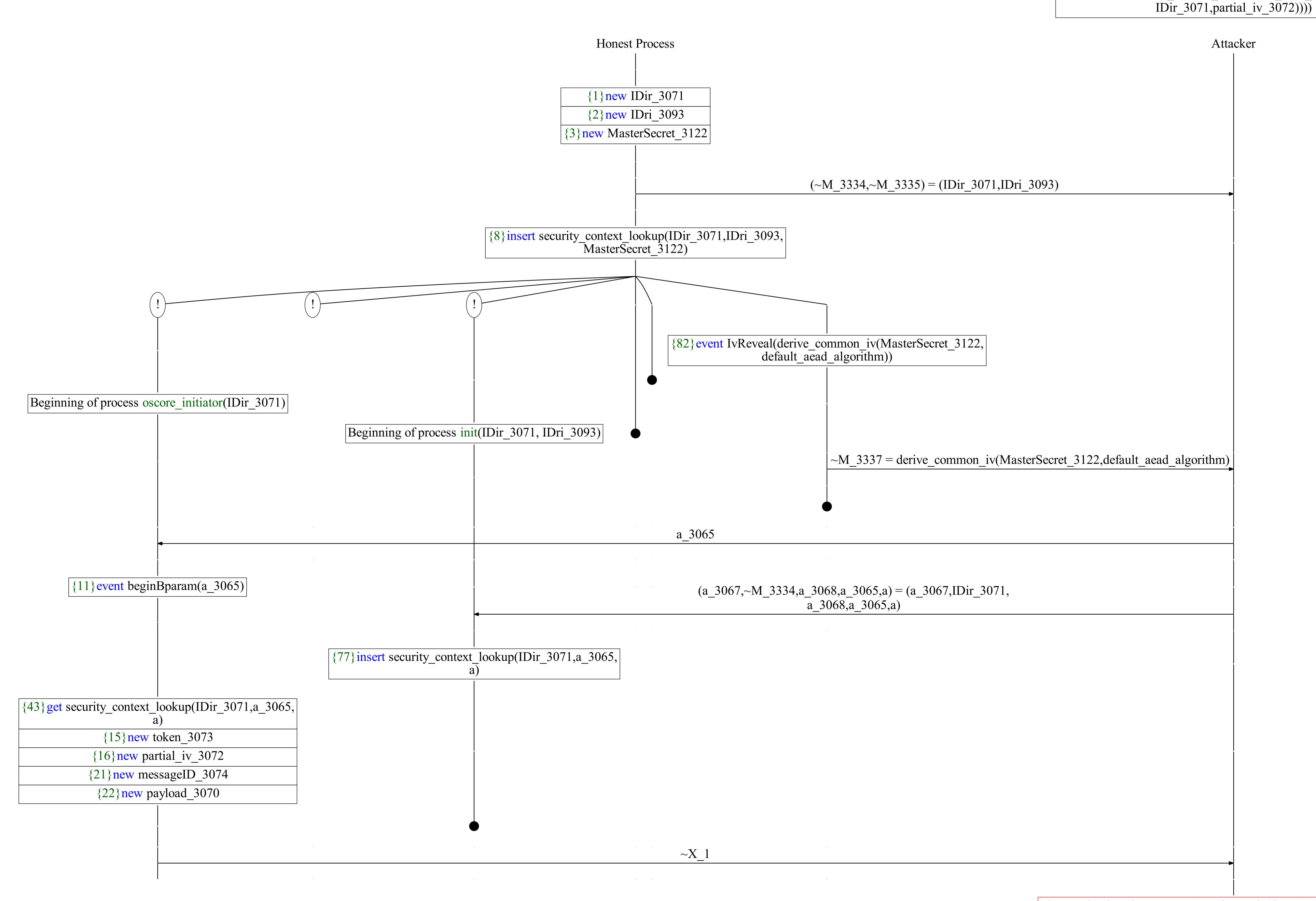
A trace has been found.



partial\_iv\_3072),(CoAP\_POSTCode,payload\_3070),

AAD(oscore\_version\_one,default\_aead\_algorithm,



The attacker has the message 2-proj-2-tuple(dec\_COSE\_ciphertext\_no\_ad( ~M\_3808,derive\_key(a,~M\_3334,default\_aead\_algorithm), aead\_nonce(~M\_3334,derive\_common\_iv(a,default\_aead\_algorithm), ~M\_3809))) = payload\_3070