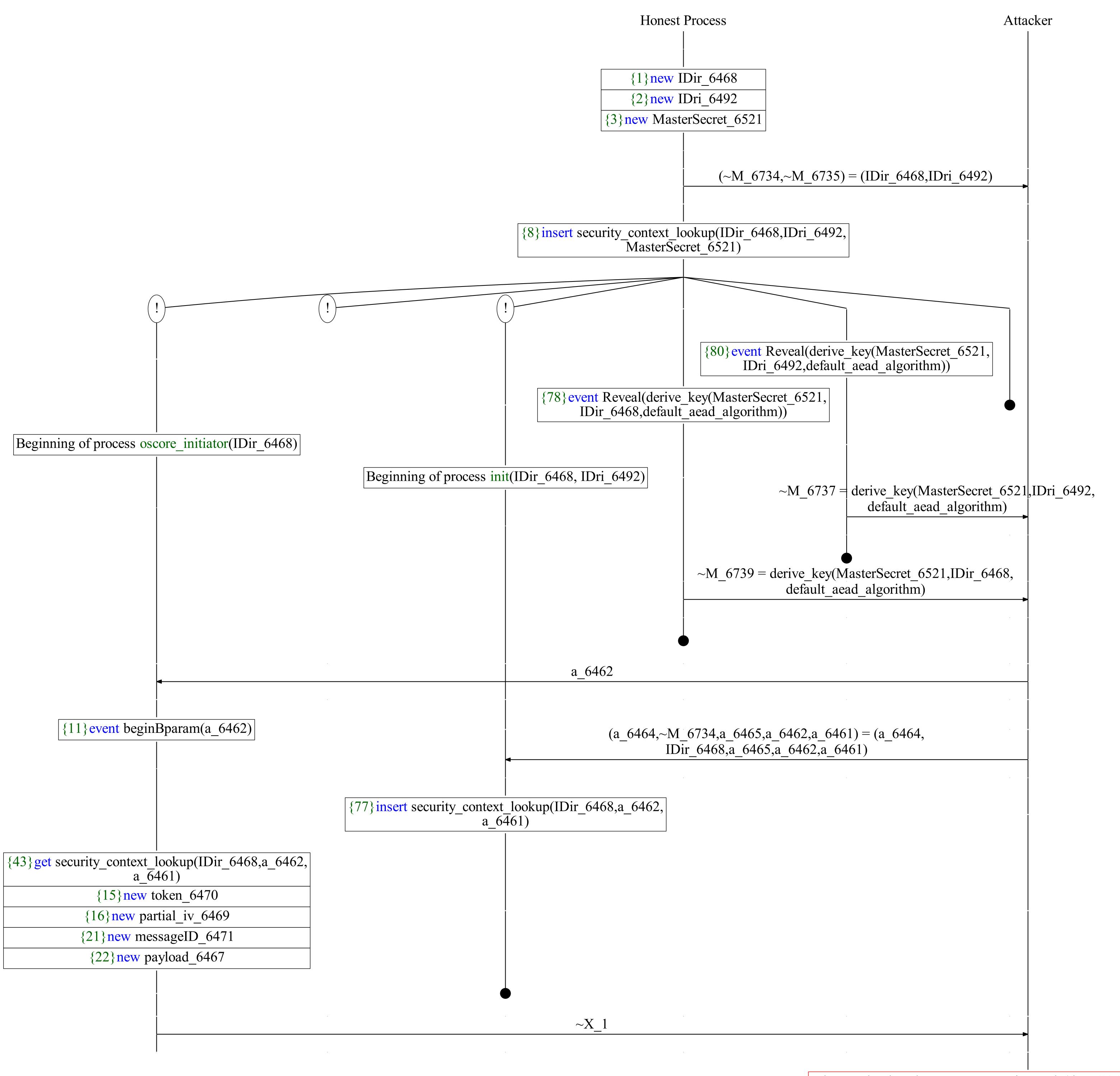
Abbreviations

~X\_1 = Request(Header(~M\_7214,~M\_7215,~M\_7216,~M\_7217, ~M\_7218),~M\_7208,CoAP\_Option\_OSCORE\_Option(~M\_7212, ~M\_7213),payload\_from\_ciphertext(~M\_7211)) = Request(

Header(CoAP\_versionOne,CoAP\_nonConfirm,CoAP\_tokenLength(token\_6470),CoAP\_GETCode,messageID\_6471),token\_6470, CoAP\_Option\_OSCORE\_Option(partial\_iv\_6469,IDir\_6468), payload\_from\_ciphertext(enc\_COSE\_ciphertext(derive\_key(a\_6461,IDir\_6468,default\_aead\_algorithm),aead\_nonce(IDir\_6468,derive\_common\_iv(a\_6461,default\_aead\_algorithm), partial\_iv\_6469),(CoAP\_POSTCode,payload\_6467), AAD(oscore\_version\_one,default\_aead\_algorithm,

IDir\_6468,partial\_iv\_6469))))

A trace has been found.



The attacker has the message 2-proj-2-tuple(dec\_COSE\_ciphertext\_no\_ad( ~M\_7211,derive\_key(a\_6461,~M\_6734,default\_aead\_algorithm), aead\_nonce(~M\_6734,derive\_common\_iv(a\_6461,default\_aead\_algorithm), ~M\_7212))) = payload\_6467