Abbreviations

~X_1 = Request(Header(~M_8960,~M_8961,~M_8962,~M_8963, ~M_8964),~M_8953,CoAP_Option_OSCORE_Option_context(~M_8957,~M_8958,~M_8959),payload_from_ciphertext(~M_8956))

~X_2 = Request(Header(a_7490,a_7491,a_7492,a_7493,a_7494), a_7495,CoAP_Option_OSCORE_Option_context(~M_8957, ~M_8958,~M_8420),payload_from_ciphertext(~M_8956))

Request(Header(a_7490,a_7491,a_7492,a_7493,a_7494),
a_7495,CoAP_Option_OSCORE_Option_context(partial_iv_7501,
 IDir_7498,idcontext_7500),payload_from_ciphertext(
 enc_COSE_ciphertext(derive_key_context(MasterSecret_7499,
 IDir_7498,default_aead_algorithm,idcontext_7500),
 aead_nonce(IDir_7498,derive_common_iv_context(
 MasterSecret_7499,idcontext_7500,default_aead_algorithm),
 partial_iv_7501),(CoAP_POSTCode,payload_7506),
 AAD(encrypt0_context,encrypt0(oscore_version_one,
 default_aead_algorithm,IDir_7498,partial_iv_7501)))))

~X_3 = Request(Header(a_7490,a_7491,a_7492,a_7493,a_7494), a_7495,CoAP_Option_OSCORE_Option_context(~M_8957, ~M_8958,~M_8420),payload_from_ciphertext(~M_8956)) A trace has been found.

Request(Header(a_7490,a_7491,a_7492,a_7493,a_7494),
a_7495,CoAP_Option_OSCORE_Option_context(partial_iv_7501,
 IDir_7498,idcontext_7500),payload_from_ciphertext(
 enc_COSE_ciphertext(derive_key_context(MasterSecret_7499,
 IDir_7498,default_aead_algorithm,idcontext_7500),
 aead_nonce(IDir_7498,derive_common_iv_context(
 MasterSecret_7499,idcontext_7500,default_aead_algorithm),
 partial_iv_7501),(CoAP_POSTCode,payload_7506),
 AAD(encrypt0_context,encrypt0(oscore_version_one,
 default_aead_algorithm,IDir_7498,partial_iv_7501)))))

~X_4 = Request(Header(~M_10495,~M_10496,~M_10497,~M_10498, ~M_10499),~M_10491,CoAP_Option_OSCORE_Option_empty, payload_from_ciphertext(~M_10494)) = Request(Header(

Honest Process Attacker {1}new IDir 7498 {2}new IDri_7497 {3}new MasterSecret 7499 {4}new idcontext 7500 \sim M 8420 = idcontext 7500 {6} insert security_context_lookup(initiator,responder, IDir 7498,IDri 7497,MasterSecret 7499,idcontext 7500) {7} insert security_context_lookup(responder,initiator, IDri 7497,IDir 7498,MasterSecret 7499,idcontext 7500) Beginning of process oscore_initiator(initiator) {9}new token_7504 Beginning of process oscore_responder(responder) Beginning of process oscore_responder(responder) {10}new messageID_7505 {11}new payload_7506 {12}new partial_iv_7501 responder {14} event beginBparam(responder) {42} get security_context_lookup(initiator,responder, IDir_7498,IDri_7497,MasterSecret_7499,idcontext_7500) $\sim X_1$ $+X_2$ [73] get security_context_lookup(responder,initiator, IDri_7497,IDir_7498,MasterSecret_7499,idcontext_7500) {49} event beginAparam(initiator) {72} get unique_ivs(partial_9234: iv) suchthat (partial_9234 = partial_iv_7501): else branch taken {57} event partialIvAccepted(partial_iv_7501) $\sim X_3$ {73} get security_context_lookup(responder,initiator, IDri_7497,IDir_7498,MasterSecret_7499,idcontext_7500) {49} event beginAparam(initiator) {72} get unique_ivs(partial_10368: iv) suchthat (partial_10368 = partial_iv_7501): else branch {57} event partialIvAccepted(partial_iv_7501) {58} insert unique_ivs(partial_iv_7501) {67}new responseMessageId_10486 {70} event endBparam(responder) $\sim X_4$ {58} insert unique_ivs(partial_iv_7501) {67}new responseMessageId_8377

{70} event endBparam(responder)