Abbreviations $\sim X_1 = \text{Request(Header(}\sim M_12051, \sim M_12052, \sim M_12053, \sim M_12054,$ ~M_12055),~M_12044,CoAP_Option_OSCORE_Option_context(~M_12048,~M_12049,~M_12050),payload_from_ciphertext(~M 12047)) = Request(Header(CoAP_versionOne,CoAP_nonConfirm, CoAP_tokenLength(token_10591),CoAP_GETCode,messageID_10592), token 10591, CoAP Option OSCORE Option context(partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext(enc_COSE_ciphertext(derive_key_context(MasterSecret_10587, IDir 10590, default aead algorithm, idcontext 10588), aead nonce(IDir 10590, derive common iv context(MasterSecret_10587,idcontext_10588,default_aead_algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0_context,encrypt0(oscore_version_one, default aead algorithm, IDir 10590, partial iv 10589))))) \sim X_2 = Request(Header(a_10579,a_10580,a_10581,a_10582, a_10583),a_10584,CoAP_Option_OSCORE_Option_context(~M_12048,~M_11516,~M_11518),payload_from_ciphertext(~M 12047)) = Request(Header(a 10579,a 10580,a 10581, a_10582,a_10583),a_10584,CoAP_Option_OSCORE_Option_context(partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext(enc COSE ciphertext(derive key context(MasterSecret 10587, IDir_10590,default_aead_algorithm,idcontext 10588), aead nonce(IDir 10590, derive common iv context(MasterSecret 10587, idcontext 10588, default aead algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0_context,encrypt0(oscore_version_one, default aead algorithm, IDir_10590, partial_iv_10589))))) \sim X 3 = Request(Header(a_10579,a_10580,a_10581,a_10582, a 10583), a 10584, CoAP Option OSCORE Option context(~M 12048,~M 11516,~M 11518),payload from ciphertext(~M 12047)) = Request(Header(a 10579,a 10580,a 10581, a_10582,a_10583),a_10584,CoAP_Option_OSCORE_Option_context(partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext(enc COSE ciphertext(derive key context(MasterSecret 10587, IDir 10590, default aead algorithm, idcontext 10588), aead nonce(IDir 10590, derive common iv context(MasterSecret_10587,idcontext_10588,default_aead algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0 context,encrypt0(oscore version one, default_aead_algorithm,IDir_10590,partial_iv_10589))))) $\sim X_4 = \text{Request(Header(}\sim M_13539, \sim M_13540, \sim M_13541, \sim M_13542,$ ~M_13543),~M_13535,CoAP_Option_OSCORE_Option_empty, payload_from_ciphertext(~M 13538)) = Request(Header(CoAP versionOne,CoAP_nonConfirm,CoAP_tokenLength(a_10584),CoAP_CHANGEDCode,responseMessageId_13529), _10584,CoAP_Option_OSCORE_Option_empty,payload_from_ciphertext(enc COSE ciphertext(derive key context(MasterSecret 10587, IDri 10586, default aead algorithm, idcontext 10588), aead nonce(IDir 10590, derive common iv context(

MasterSecret 10587, idcontext 10588, default aead algorithm),

partial_iv_10589),(generateResponseCode(CoAP_POSTCode,

payload_10593),generateResponsePayload(CoAP_POSTCode,

payload_10593)),AAD(encrypt0_context,encrypt0(

oscore_version_one,default_aead_algorithm,IDri_10586,

partial_iv_10589)))))

Honest Process Attacker {1}new IDir_10590 {2}new IDri_10586 {3}new MasterSecret 10587 {4}new idcontext 10588 $(\sim M_11516, \sim M_11517, \sim M_11518) = (IDir_10590, IDri_10586,$ idcontext 10588) {6} insert security_context_lookup(IDir_10590,IDri_10586, MasterSecret 10587, idcontext 10588) Beginning of process oscore_responder(IDri_10586, IDir_10590) Beginning of process oscore_responder(IDri_10586, IDir_10590) Beginning of process oscore_initiator(IDir_10590) $(\sim M_11517, \sim M_11518) = (IDri_10586, idcontext_10588)$ {9} event beginBparam(IDri_10586) 42} get security_context_lookup(IDir_10590,IDri_10586, MasterSecret_10587,idcontext_10588) {13}new token_10591 {14} new partial_iv_10589 {19}new messageID_10592 {20} new payload_10593 ~X 1 {31} event here ~X_2 {48} event beginAparam(IDir_10590) {74} get security_context_lookup(IDir_10590,IDri_10586, MasterSecret_10587,idcontext_10588) {73} get unique_ivs(partial_12313: iv) suchthat (partial_12313 = partial_iv_10589): else branch taken {57} event partialIvAccepted(partial_iv_10589) $\sim X_3$ {48} event beginAparam(IDir_10590) [74] get security_context_lookup(IDir_10590,IDri_10586, MasterSecret_10587,idcontext_10588) {73}get unique_ivs(partial_13411: iv) suchthat (partial_13411 = partial_iv_10589): else branch taken {57} event partialIvAccepted(partial_iv_10589) {58} insert unique_ivs(partial_iv_10589) {67} new responseMessageId_13529 {71} event endBparam(IDri_10586) ~X_4 [58] insert unique_ivs(partial_iv_10589) {67}new responseMessageId_11463 {71} event endBparam(IDri_10586)

A trace has been found.