Abbreviations $\sim X_1 = \text{Request(Header(}\sim M_14732, \sim M_14733, \sim M_14734, \sim M_14735,$ ~M_14736),~M_14725,CoAP_Option_OSCORE(~M_14729, ~M 14730,~M 14731),payload from ciphertext(~M 14728)) Request(Header(CoAP versionOne,CoAP nonConfirm, CoAP_tokenLength(token_12949),CoAP_GETCode,messageID_12950), token_12949,CoAP_Option_OSCORE(partial_iv_12946, IDir_12942,idcontext_12945),payload_from_ciphertext(enc_COSE_ciphertext(toKey(HKDF(msecret_12943,msalt_12944, info(IDir 12942,idcontext 12945,default_aead_algorithm, label_key),alg_key_length(default_aead_algorithm, label_key))),aead_nonce(IDir_12942,toIV(HKDF(msecret_12943, msalt_12944,info(emptyId,idcontext_12945,default_aead_algorithm, label_iv),alg_key_length(default_aead_algorithm, label_iv))),partial_iv_12946),(CoAP_POSTCode,payload_12951), AAD(encrypt0_context,encrypt0(oscore_version_one, default aead algorithm, IDir_12942, partial_iv_12946))))) \sim X_2 = Request(Header(a_12934,a_12935,a_12936,a_12937, a_12938),a_12939,CoAP_Option_OSCORE(~M_14729,~M 14730, ~M_14067),payload_from_ciphertext(~M_14728)) Request(Header(a_12934,a_12935,a_12936,a_12937, a_12938),a_12939,CoAP_Option_OSCORE(partial_iv_12946, IDir_12942,idcontext_12945),payload_from_ciphertext(enc_COSE_ciphertext(toKey(HKDF(msecret_12943,msalt_12944, info(IDir 12942,idcontext 12945,default aead algorithm, label key), alg key length (default aead algorithm, label key))),aead nonce(IDir 12942,toIV(HKDF(msecret 12943, msalt_12944,info(emptyId,idcontext_12945,default_aead_algorithm, label iv), alg key length(default aead algorithm, label_iv))),partial_iv_12946),(CoAP_POSTCode,payload_12951), AAD(encrypt0_context,encrypt0(oscore version one, default_aead_algorithm,IDir_12942,partial_iv_12946))))) \sim X 3 = Request(Header(a 12934,a 12935,a 12936,a 12937, a_12938),a_12939,CoAP_Option_OSCORE(~M_14729,~M_14730, ~M 14067),payload from ciphertext(~M 14728)) Request(Header(a 12934,a 12935,a 12936,a 12937, a_12938),a_12939,CoAP_Option_OSCORE(partial_iv_12946, IDir 12942,idcontext 12945),payload from ciphertext(enc COSE ciphertext(toKey(HKDF(msecret 12943,msalt 12944, info(IDir 12942,idcontext 12945,default aead algorithm, label_key),alg_key_length(default_aead algorithm, label key))),aead nonce(IDir 12942,toIV(HKDF(msecret 12943, msalt 12944,info(emptyId,idcontext 12945,default aead algorithm, label iv), alg key length(default aead algorithm, label iv))),partial iv 12946),(CoAP POSTCode,payload 12951), AAD(encrypt0_context,encrypt0(oscore_version one, default aead algorithm, IDir 12942, partial iv 12946))))) $\sim X_4 = \text{Request(Header(}\sim M_16667, \sim M_16668, \sim M_16669, \sim M_16670,$ ~M 16671),~M 16660,CoAP Option OSCORE(~M 16664, ~M_16665,~M_16666),payload_from_ciphertext(~M_16663)) Request(Header(CoAP versionOne,CoAP nonConfirm, CoAP tokenLength(a 12939), CoAP CHANGEDCode, responseMessageId 16655), a_12939,CoAP_Option_OSCORE(emptyIv,emptyId,emptyIdC), payload_from_ciphertext(enc_COSE_ciphertext(toKey(HKDF(msecret 12943,msalt 12944,info(IDri 12941, idcontext 12945, default aead_algorithm, label_key), alg key length(default aead algorithm, label key))), aead nonce(IDir 12942,toIV(HKDF(msecret 12943, msalt_12944,info(emptyId,idcontext_12945,default_aead_algorithm, label_iv),alg_key_length(default_aead_algorithm, label iv))),partial iv 12946),(generateResponseCode(CoAP_POSTCode,payload_12951),generateResponsePayload(CoAP_POSTCode,payload_12951)),AAD(encrypt0 context, encrypt0(oscore_version_one,default_aead_algorithm, IDri 12941,partial iv 12946))))) **Honest Process** Attacker {1}new IDir_12942 {2}new IDri 12941 {3}new msecret 12943 {4}new msalt 12944 \sim M 14067 = idcontext 12945

A trace has been found.

{5}new idcontext 12945 [7] insert security_context_lookup(initiator,responder, IDir_12942,IDri_12941,msecret_12943,msalt_12944, idcontext_12945) {8} insert security_context_lookup(responder,initiator, IDri_12941,IDir_12942,msecret_12943,msalt_12944, idcontext_12945) Beginning of process oscore_initiator(initiator) {10}new token_12949 Beginning of process oscore_responder(responder) Beginning of process oscore_responder(responder) {11}new messageID_12950 {12}new payload_12951 {13}new partial_iv_12946 responder {15} event beginBparam(responder) [46] get security_context_lookup(initiator,responder, IDir_12942,IDri_12941,msecret_12943,msalt_12944, idcontext_12945) ~X 1 [80] get security_context_lookup(responder,initiator, IDri_12941,IDir_12942,msecret_12943,msalt_12944, idcontext 12945) {53} event beginAparam(initiator) {79} get unique ivs(partial 15087: iv) suchthat (partial_15087 = partial_iv_12946): else branch taken {64} event partialIvAccepted(partial_iv_12946) ~X_3 {80} get security_context_lookup(responder,initiator, IDri_12941,IDir_12942,msecret_12943,msalt_12944, idcontext_12945) {53} event beginAparam(initiator) {79} get unique_ivs(partial_16534: iv) suchthat (partial_16534 = partial_iv_12946): else branch {64} event partialIvAccepted(partial_iv_12946) {65} insert unique_ivs(partial_iv_12946) {74}new responseMessageId 16655 {77} event endBparam(responder) $\sim X_4$ [65] insert unique_ivs(partial_iv_12946) {74}new responseMessageId_14024 {77} event endBparam(responder)