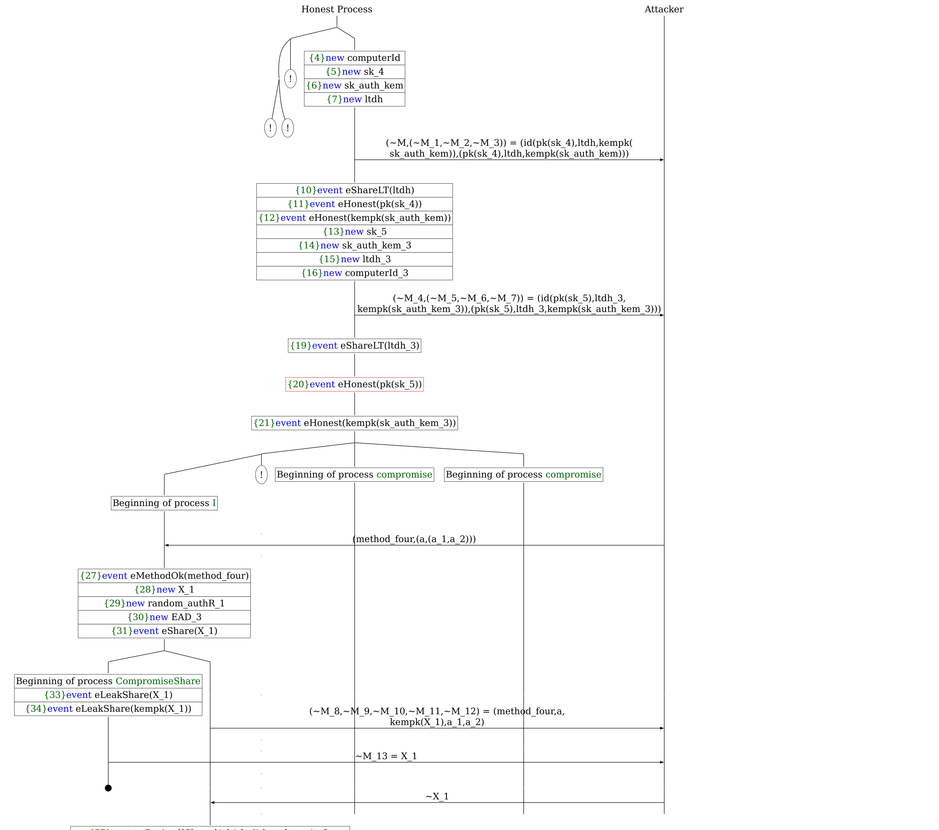
Abbreviations
~X_1 = (a_3,encxor((a_4,~M_4,edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,~M_10,a_1,a_2))),kemdecap(a_3,~M_13)),sfour,(~M_4,hash((a_3,hash((method_four,a,~M_10,a_1,a_2))),~M_5,a_5),hash_length),a_5),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,~M_10,a_1,a_2))),kemdecap(a_3,~M_13)),stwo,hash((a_3,hash((method_four,a,~M_10,a_1,a_2))),plaintext_length))) = (a_3,encxor((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),stwo,hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),plaintext_length)))

A trace has been found.



{57}event eDerivedIShared(pk(sk_4),kemdecap(a_3,X_1))

{60}event eCheckedMAC2(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length)))

{62}event eTHIShared(pk(sk_4),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),((id(pk(sk_4),ltdh,kempk(sk_auth_kem)),(edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),seight,(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),pk(sk_4),EAD_3),hash_length),a_5),pk(sk_5)))),((id(pk(sk_4),ltdh,kempk(sk_auth_kem)),(edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),seight,(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),pk(sk_4),EAD_3),hash_length),EAD_3)),pk(sk_4),EAD_3),hash_length),X_1,a_3)

{74}event eSecretsI(computerId,method_four,pk(sk_4),pk(sk_5),hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),snine,hash((hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),((id(pk(sk_4),ltdh,kempk(sk_auth_kem)),(edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),seight,(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),pk(sk_4),EAD_3),hash_length),EAD_3)),pk(sk_4),EAD_3),hash_length),X_1,a_3)

{75}event eAcceptIData(edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),snine,hash((hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),((id(pk(sk_4),ltdh,kempk(sk_auth_kem)),(edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),seight,(id(pk(sk_4),ltdh,kempk(sk_auth_kem)),hash((hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),((a_4,id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),kemdecap(a_3,X_1)),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((a_3,hash((method_four,a,kempk(X_1),a_1,a_2))),pk(sk_5),a_5),hash_length),a_5),pk(sk_5)))),pk(sk_4),EAD_3),hash_length),EAD_3)),pk(sk_4),EAD_3),hash_length),EAD_3)))))))))))