Abbreviations a,~M 10,a 1,a 2)))),kemdecap(a 3,~M 13)),stwo, = (a 3,encxor((a 4,id(pk(sk 5), plaintext length))) Attacker $(\sim M, (\sim M_1, \sim M_2, \sim M_3)) = (id(pk(sk_4), ltdh, kempk($ sk_auth_kem)),(pk(sk_4),ltdh,kempk(sk_auth_kem))) $(\sim M_4, (\sim M_5, \sim M_6, \sim M_7)) = (id(pk(sk_5), ltdh_3,$ kempk(sk auth kem 3)),(pk(sk 5),ltdh 3,kempk(sk auth kem 3))) Beginning of process compromise (method four,(a,(a 1,a 2))) $(\sim M_8, \sim M_9, \sim M_{10}, \sim M_{11}, \sim M_{12}) = (\text{method}_{10}, \sim M_{11}, \sim M_{12})$ kempk(X 1),a 1,a 2)

Honest Process

{4}new computerId

{5}new sk 4

{6}new sk auth kem

{7}new ltdh

{10}event eShareLT(ltdh)

{11}event eHonest(pk(sk 4))

{12}event eHonest(kempk(sk auth kem))

{13}new sk 5

{14}new sk_auth_kem_3

{15}new ltdh 3

{16}new computerId 3

{19}event eShareLT(ltdh_3)

{20}event eHonest(pk(sk 5))

{21}event eHonest(kempk(sk auth kem 3))

Beginning of process compromise

 \sim M 13 = X 1

~X 1

Beginning of process I

{27} event eMethodOk(method_four)

 $\{28\}$ new X 1

{29}new random_authR_1

{30}new EAD 1

{31}event eShare(X 1)

 $\{57\}$ 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(\(\bar{method}\) four,a,kem\(\bar{pk}(X 1),a 1,a 2)))),kem\(\bar{decap}(

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,

 $hash((method four,a,kempk(X_1),a_1,a_2)))),((a_4,a_5))$

id(pk(sk 5),ltdh 3,kempk(sk auth kem 3),edhoc kdf(

hkdfextract(hash((a 3,hash((method_four,a,kempk(

 $X_1),a_1,a_2))),kemdecap(a 3,X <math>\overline{1})),sfour,(id($

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 $\overline{5}$),pk $\overline{(sk 5)}$))))

{73}event eAcceptI(computerId,method_four,pk(sk 4),

pk(sk_5),hkdfextract(hash((a_3,hash((method_four,

 $a, kempk(\bar{X} 1), a 1, a 2)))), kemdecap(a 3, X 1)), hkdfextract($

hash((a $\overline{3}$,hash((method four,a,kempk(\overline{X} 1),a 1,a 2)))),

kemdecap(a 3,X 1)),edhoc kdf(hkdfextract(hash(

(a_3,hash((method_four,a,kempk(X 1),a 1,a 2)))),

 $ke\overline{m}decap(a_3,X_1)$, snine, has $h((hash((hash((a_3,x_1)),x_1)),x_1))$

 $hash((me\bar{t}ho\bar{d} four,a,kempk(X 1),a 1,a 2)))),((a\bar{d} 4,a))$

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)))), $kendecap(a_3,X_1)$),sfour,(id(

pk(sk_5), Itdh_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),hāsh length),a 5), $pk(s\bar{k} 5)$)),((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_1 , hash_length),

 \overline{EAD} 1)), pk(sk 4))), hash \overline{length} , $X \overline{1}$, a 3)

Beginning of process CompromiseShare

{33}event eLeakShare(X 1)

{34}event eLeakShare(kempk(X 1))

 \sim X 1 = (a 3,encxor((a 4, \sim M 4,edhoc kdf(hkdfextract(hash((a 3,hash((method four,a,~M 10,a 1,a 2)))),kemdecap(a $\overline{3}$,~M 13)),sfour,(~M 4,has \overline{h} ((a $\overline{3}$,has \overline{h})(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,

 $hash((a 3,hash((method four,a,\sim M 10,a 1,a 2)))),$ plaintext length)))

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)))),

A trace has been found.