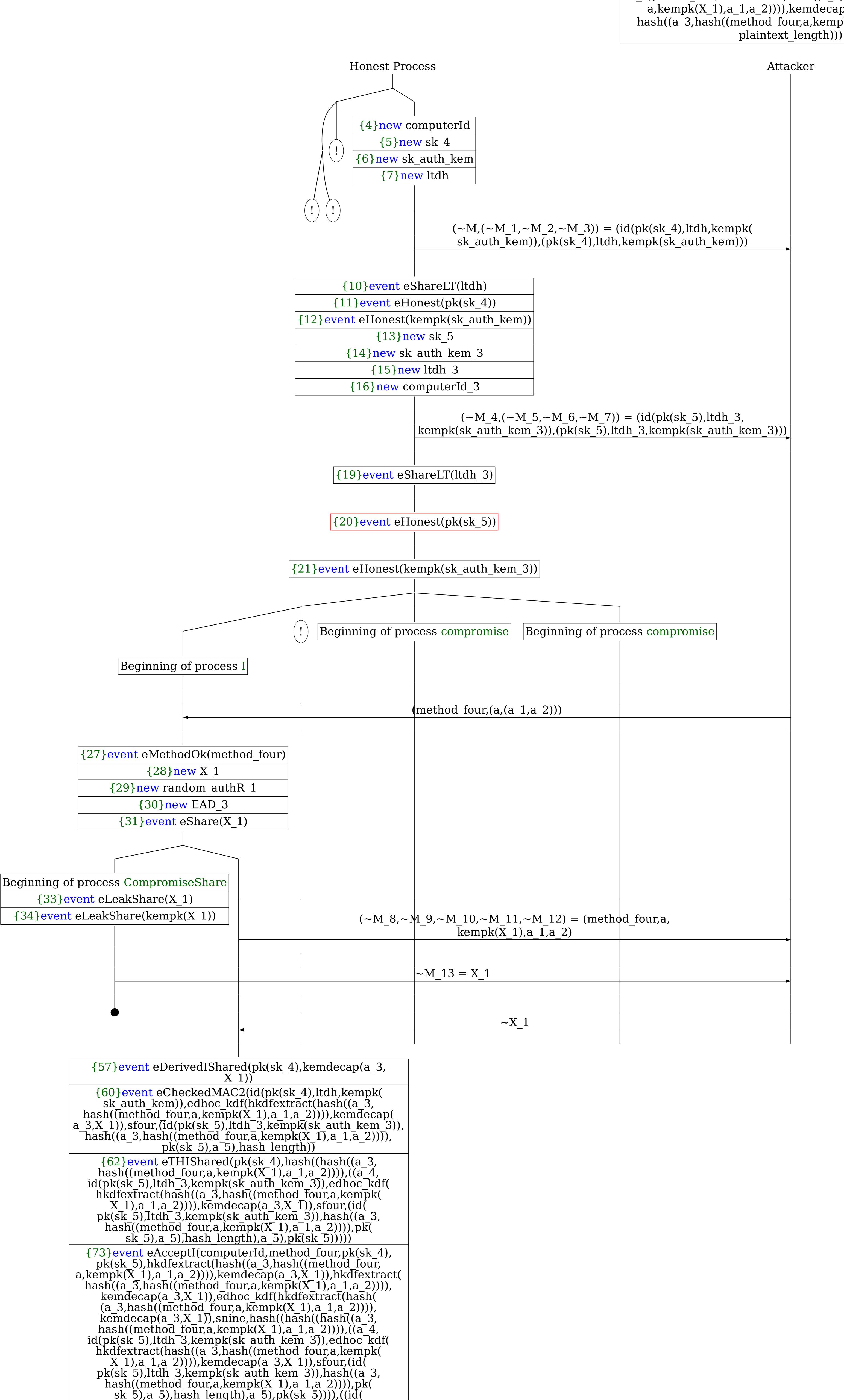
\sim X 1 = (a 3,encxor((a 4, \sim M 4,edhoc kdf(hkdfextract(hash((a 3,hash((method four,a,~M 10,a 1,a 2)))),kemdecap(a 3,~M 13)),sfour,(~M 4,hash((a 3,hash((method four, a,~M 10,a 1,a 2)))),~M 5,a 5),hash length),a 5), edhoc kdf(hkdfextract(hash((a 3,hash((method four,

Abbreviations

a,~M 10,a 1,a 2)))),kemdecap(a 3,~M 13)),stwo, $hash((a 3,hash((method four,a,\sim M 10,a 1,a 2)))),$ 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)))),



a 3,X 1)), snine, hash((hash((hash((a $\overline{3},hash((method four,$ a, kempk(X 1), a 1, a 2))), ((a 4, id(pk(sk 5), ltdh 3, ltdhkempk(sk_auth_kem_3)),edhoc_kdf(hkdfextract(hash((a 3, has h((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 $k = \overline{3}$), hash((a 3, hash($\overline{1}$) method four, a, $\text{kempk}(X^{-}1)$, a $\overline{1}$, a $\overline{2}$))), pk $\overline{(\text{sk 5})}$, a $\overline{5}$), hash $\overline{\text{length}}$), a 5),pk(sk $\overline{5}$))), $\overline{(}$ (id(\overline{p} k(sk $\overline{4}$),ltd \overline{h} ,ke \overline{m} pk(sk \overline{a} uth ke \overline{m})), (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 $\bar{3}$, has \bar{h} (method four, a, \bar{k} emp $\bar{k}(X_1)$, a 1, a 2)))), $((\bar{a} 4, id(pk(sk_5), l\bar{t}dh_3, kemp\bar{k}(sk_auth_kem_3)),$ edhoc kdf(hkdfextract(hash(a 3,hash(method four, a, kempk(X 1), a 1, a 2)))), kemdecap(a 3, X 1)), stour,(id(pk(sk 5),ltdh 3,kempk(sk auth kem 3)),hash((a $\bar{3}$, hash ((method four, a, kempk(\bar{X} 1), a 1, a 2)))), $\overline{pk}(sk 5),a 5),hash length),a 5),pk(sk 5))),pk($ \overline{sk} 4), $\overline{E}AD\overline{3}$),hash \overline{length}), $\overline{E}AD\overline{3}$)),p $\overline{k}(\overline{sk}$ 4)))), hash length), 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 $\overline{1}$, a $\overline{1}$, a 2)))), plaintex \overline{t} length), edhoc \overline{k} df(hkdfextract($\overline{hash}((a 3, hash((method four, a, kempk(X 1), a 1, a 2)))),$ $kemdecap(a 3,X 1)), \overline{s}five, hash((\overline{h}ash\overline{(a 3,hash()}ash\overline{(a 3,hash()}asha)))))))))))$ (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)))), $kendecap(a 3,X <math>\bar{1}$)),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),hash Tength),a $5\bar{)}$,pk($\bar{s}k$ 5) $\bar{)}$)), \bar{k} ey length), edhoc kdf(hkdfextract(hash(a 3,hash(method four, a, kempk(X 1), a 1, a 2))), kemdecap(a 3, X 1)), six, $hash(\bar{h}ash(\bar{h}ash(\bar{h}ash(method four,a,\bar{k}empk(X 1),$ a 1,a 2)))),((a 4,id $\overline{(}$ pk(sk 5),ltdh 3, \overline{k} empk(sk auth \overline{k} em 3)), edhoc kdf(hkdfextract(hash((a 3,hash((method four, a, kempk(X 1), a 1, a 2)))), kemdecap(a 3, X 1)), sfour, $(id(pk(sk \overline{5}), ltdh 3, kempk(sk auth kem \overline{3})), hash($ (a 3, has h(method four, a, kempk(X 1), a 1, a 2)))), $pk(sk_5),a_5),hash_length),a_5),pk(sk_5))),iv_length), X_1,a_3)$ {75}event eAcceptIData(edhoc kdf(hkdfextract(hash((a 3,hash((method four,a,ke \overline{m} pk(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,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)))),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(\bar{X} 1),a 1,a 2)))),pk(sk 5),a 5),hāsh length),a 5), $pk(s\bar{k} 5)$)),(($i\bar{d}($

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, ltdh

kempk(sk auth kem 3)),edhoc kdf(hkdfextract(hash(

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,

 $a, kempk(X 1), a 1, a 2))),((a-4, id(pk(sk_5), ltdh_3, a)))$

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,

 $\text{kempk}(X^{-}1)$, a $\overline{1}$, a $\overline{2}$))), pk(sk 5), a 5), hash $\overline{\text{length}}$),

a $\overline{5}$),p \overline{k} (sk $\overline{5}$))),p \overline{k} (sk $\overline{4}$),E \overline{A} D $\overline{3}$,hash length),

[EAD 3), pk(sk 4))), hash length), <math>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),edhoc kdf(hkdfextract(hash((a 3,hash(

(method four,a,kempk(X 1),a 1,a 2)))),kemdecap(

 $(a^{3},hash((method four,a,kempk(X 1),a 1,a 2)))),$ 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 $\overline{5}$),p \overline{k} (sk $\overline{5}$))),p \overline{k} (sk $\overline{4}$),E \overline{A} D $\overline{3}$,hash length), $EAD_3)$, $pk(sk_4)$), $hash_length$, $method_four$, $pk(sk_4)$ sk 4), \overline{p} k(sk 5), \overline{X} 1,a 3,(hash((a 3,hash((method four, \overline{a} , $\overline{kempk(X 1)}$, \overline{a} 1, \overline{a} 2)))), $\overline{(hash((a 3,hash((a 3,ha)))))))))))))))}))})$ (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)))), $k\bar{e}mdecap(a 3,X \bar{1})$,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),hash length),a 5), \overline{p} k(sk 5))),(hash((hash((hash((a 3,hash((method four,a,kempk(X 1),a 1,a 2)))),((a 4,id $(\overline{p}k(sk 5),ltdh 3,\overline{kempk}(sk auth kem 3)),$ edhoc_kdf(hkdfextract(hash(a 3,hash)(method four, a, kempk(X 1), a 1, a 2)))), kemdecap(a 3, X 1)), sfour, $(id(pk(sk \overline{5}), ltdh 3, kempk(sk auth kem \overline{3})), hash($ (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)))), $((\bar{a} 4, id(pk(sk 5), l\bar{t}dh 3, kemp\bar{k}(sk\bar{a}uth\bar{k}e\bar{m}_3)),$ edhoc kdf(hkdfextract(hash(a 3,hash(method four, $a, kempk(X 1), a 1, a 2)))), kemdecap(a_3, X_1)), sfour,$ $(id(pk(sk \overline{5}), ltdh 3, kempk(sk auth kem \overline{3})), hash($ $(a_3,hash((method_four,a,kempk(X_1),a_1,a_2)))),$ $\overline{pk}(sk 5),a 5),hash length),a 5),pk(sk 5))),pk($ sk_4), EAD_3),hash_length), EAD_3)),pk(sk_4)))), $(a, \overline{a} \ 2, (a \ \overline{5}, (EAD \ 3, (method four, a, \overline{kempk}(X \ 1), \overline{a}))$ a 1,a 2), $\overline{(}$ (a 4 $\overline{,}$ id(pk(s \overline{k} 5),ltdh 3, \overline{k} empk(sk auth \overline{k} em 3)), edhoc kdf(hkdfextract(hash(a 3,hash(method four, a, kempk(X 1), a 1, a 2)))), kemdecap(a 3, X 1)), stour, $(id(pk(sk \overline{5}), ltdh \overline{3}, kempk(sk auth kem \overline{3})), hash($ (a 3,hash((method four,a,kempk(X 1),a 1,a 2)))), $pk\bar{(}sk 5),a 5),hash\bar{(}length),a \bar{5}),(id\bar{(}pk(\bar{sk} 4),ltdh),$ kempk(sk auth kem)),(edhoc kdf(hkdfextract(hash((a $\overline{3}$, has \overline{h} (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, ltdh

kempk(sk auth kem 3)),edhoc kdf(hkdfextract(hash(

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

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 $\overline{5}$),p \overline{k} (sk $\overline{5}$))), \overline{p} k(sk $\overline{4}$),E \overline{A} D $\overline{3}$,hash length),

A trace has been found.