Abbreviations \sim M 8 = kemcipher(kemencap(Y 1,a 5)) $\sim M_9 = encxor((a,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),$ (edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y 1,a 5)),hash((method four,(a 4,(a 5,(a 6,a 7)))))), kemkey(kemencap(Y 1,a 5))),sfour,(id(pk(sk 5), ltdh 3,kempk(sk auth kem 3)),hash((kemcipher(kemencap(\bar{Y} 1,a 5)),hash((method_four,(a_4,(a_5,(a_6,a_7)))))), pk(sk 5),a 1),hash length),a 1))),edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y 1,a 5)),hash((method four, (a 4,(a 5,(a 6,a 7)))))),kemkey(kemencap(Y 1,a 5))),stwo,hash((kemcipher(kemencap(Y 1,a 5)), $hash((method_four,(a_4,(a_5,(a_6,a_7)))))))),plaintext_length))$ $\sim X 1 = aeadenc((\sim M,(edhoc kdf(hkdfextract(hash((\sim M 8,$ hash((method four,(a 4,(a 5,(a 6,a 7)))))),kemkey($kemencap(\sim M 10, a 5))), seight, (\sim M, hash((hash((\sim M 8, a 5)))))$ hash((method four,(a 4,(a 5,(a 6,a 7)))))),((a,(~M 4,(edhoc kdf(hkdfextract(hash((~M 8,hash((method four,(a 4,(a 5,(a 6,a 7)))))),kemkey($kemencap(\sim M 10, a 5))), sfour, (\sim M 4, hash((\sim M 8, hash($ $(method\ four,(a\ 4,(a\ 5,(a\ 6,a\ 7))))),\sim M\ 5,a\ 1),$ hash length), a 1))), \sim M 5))), \sim M 1, a 8), hash length), a_8)),a_9,edhoc_kdf(hkdfextract(hash($\sim M_8$),hash((method_four,(a_4,(a_5,(a_6,a_7)))))),kemkey(kemencap(~M 10,a 5))),sfive,hash((hash((~M 8,hash($(method four,(a 4,(a 5,(a 6,a 7))))),((a,(\sim M 4,$ (edhoc kdf(hkdfextract(hash((~M 8,hash((method four, (a 4,(a 5,(a 6,a 7)))))),kemkey(kemencap(~M 10,a 5))),sfour,($\sim M 4$,hash(($\sim M 8$,hash)(method four, $(a 4,(a 5,(a 6,a 7))))),\sim M 5,a 1),hash length),$ a 1))),~M 5))),key length),edhoc kdf(hkdfextract($hash((\sim M 8, hash((method four,(a 4,(a_5,(a_6,a_7))))))),$ $kemkey(kemencap(\sim M 10, a 5))), ssix, hash((hash(($ \sim M 8,hash((method four,(a_4,(a_5,(a_6,a_7)))))), ((a,(~M 4,(edhoc kdf(hkdfextract(hash((~M 8,hash((method four,(a 4,(a 5,(a 6,a 7)))))),kemkey($kemencap(\sim M 10, a 5))), sfour, (\sim M 4, hash((\sim M 8, hash($ $(method four,(a 4,(a 5,(a 6,a 7))))),\sim M 5,a 1),$ hash length), a 1))), \sim M 5))), iv length)) = aeadenc((id(pk(sk 4),ltdh,kempk(sk auth kem)),(edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y_1,a_5)), hash((method four,(a 4,(a 5,(a 6,a 7)))))),kemkey(kemencap(Y_1,a_5))),seight,(id(pk(sk_4),ltdh,kempk(sk auth kem)),hash((hash((kemcipher(kemencap(Y 1, a 5)),hash((method four,(a 4,(a 5,(a 6,a 7)))))), ((a,(id(pk(sk 5),ltdh 3,kempk(sk auth kem 3)), (edhoc kdf(hkdfextract(hash((kemcipher(kemencap($Y_1,a_5)$, hash((method_four,(a_4,(a_5,(a_6,a_7)))))), kemkey(kemencap(Y 1,a 5))),sfour,(id(pk(sk 5), ltdh 3,kempk(sk auth kem 3)),hash((kemcipher(kemencap($Y_1,a_5)$, hash((method_four,(a_4,(a_5,(a_6,a_7)))))), pk(sk 5),a 1),hash_length),a_1))),pk(sk_5)))),

pk(sk 4),a 8),hash length),a 8)),a 9,edhoc kdf(

hkdfextract(hash((kemcipher(kemencap(Y_1,a_5)),

hash((method four,(a 4,(a 5,(a 6,a 7)))))),kemkey(

kemencap(Y 1,a 5))),sfive,hash((hash((kemcipher(

kemencap(Y 1,a 5)),hash((method four,(a 4,(a 5,

(a 6,a 7)))))),((a,(id(pk(sk 5),ltdh 3,kempk(

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

kemencap(Y 1,a 5)),hash((method four,(a 4,(a 5,

(a 6,a 7))))))),kemkey(kemencap(Y_1,a_5))),sfour,

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

(kemcipher(kemencap(Y 1,a 5)),hash((method four,

(a 4,(a 5,(a 6,a_7)))))),pk(sk_5),a_1),hash_length),

a 1))),pk(sk 5)))),key length),edhoc kdf(hkdfextract(

hash((kemcipher(kemencap(Y 1,a 5)),hash((method four,

 $(a \ 4,(a \ 5,(a \ 6,a \ 7)))))),kemkey(kemencap(Y \ 1,$

a 5))),ssix,hash((hash((kemcipher(kemencap(Y 1,

a 5)),hash((method_four,(a_4,(a_5,(a_6,a_7)))))),

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

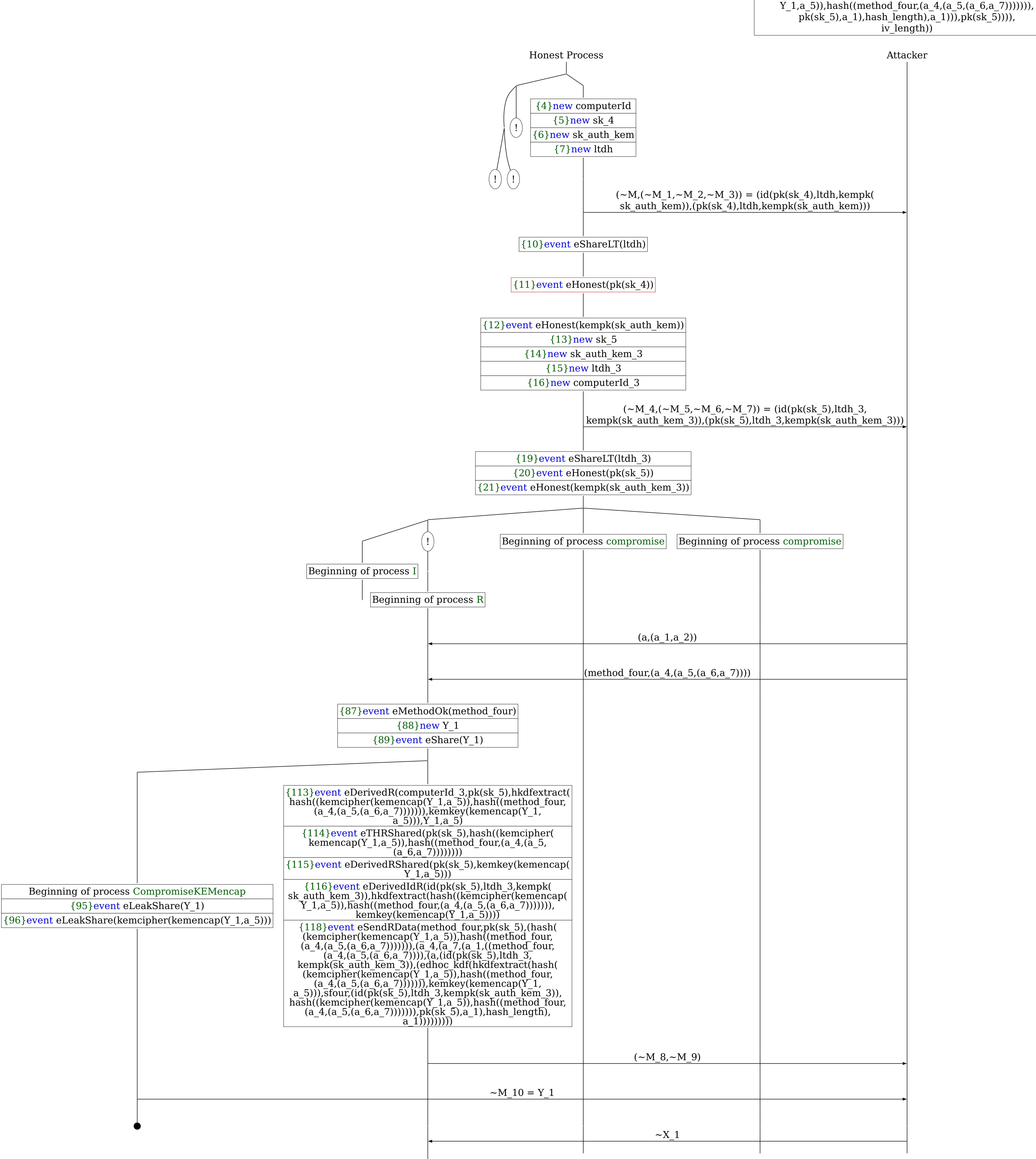
(edhoc kdf(hkdfextract(hash((kemcipher(kemencap(

 $Y_1,a_5)$, hash((method_four,(a_4,(a_5,(a_6,a_7)))))),

kemkey(kemencap(Y_1,a_5))),sfour,(id(pk(sk_5),

ltdh 3,kempk(sk auth kem 3)),hash((kemcipher(kemencap(

A trace has been found.



{131}event eCheckedMAC3(id(pk(sk 5),ltdh 3,kempk(sk auth kem 3)),edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y 1,a 5)),hash((method four,(a 4,(a 5, $(a_6,a_7)))))), kemkey(kemencap(Y_1,a_5)), seight,$ (id(pk(sk 4),ltdh,kempk(sk auth kem)),hash((hash((kemcipher(kemencap(Y_1,a_5)),hash((method four, (a_4,(a_5),(a_6,a_7))))))),((ā,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),(edhoc_kdf(hkdfextract(hash((kemcipher(kemencap(Y 1,a 5)),hash((method four, (a 4,(a 5,(a 6,a 7)))))),kemkey(kemencap(Y 1, a_5))),sfour,(id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)), hash((kemcipher(kemencap(Y_1,a_5)),hash((method_four, (a_4,(a_5,(a_6,a_7)))))),pk(sk_5),a_1),hash_length),

 $\overline{a(1)}$), $\overline{pk}(sk(5))$), $\overline{pk}(sk(4),\overline{a(8)},\overline{hash(length)})$

{95}event eLeakShare(Y 1)

{134}event eAcceptR(computerId 3,method four,pk(sk_4),pk(sk_5),hkdfextract(hash((kemcipher(kemencap(Y_1,a_5)),hash((method_four,(a_4,(a_5,(a_6,a_7))))))), kemkey(kemencap(Y_1,a_5)),hkdfextract(hash((kemcipher(kemencap(Y_1,a_5)),hash((method_four,(a_4,(a_5),)))) (a 6,a 7))))),kemkey(kemencap(Y 1,a 5))),edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y_1,a_5)), hash((method_four,(a_4,(a_5,(à_6,a_7)))))),kemkey(kemencap(Y_1,a_5))),snine,hash((hash((hash((kemcipher($kemencap(Y_1,a_5)$), $hash((method_four,(a_4,(a_5,$ $(a 6,a^{-7}))))),((a,(id(pk(sk 5),ltdh 3,kempk($ sk auth kem 3)),(edhoc kdf(hkdfextract(hash(kemcipher(kemencap(Y 1,a 5)), hash((method four,(a 4,(a 5, $(a_6,a_7)))))), kemkey(kemencap(Y_1,a_5)), sfour,$ (id(pk(sk 5),ltdh 3,kempk(sk auth kem 3)),hash((kemcipher(kemencap(Y 1, a 5)), hash((method four, $(a_4,(a_5,(a_6,a_7)))),pk(sk_5),a_1),hash_length),$ $a_1))$, $pk(sk_5))), ((id(pk(sk_4), ltdh, kempk(sk_auth_kem)), ltdh, kempk(sk_auth_kem), ltdh, kempk(sk_auth_kem)), ltdh, kempk(sk_auth_kem), ltdh, kempk($ (edhoc kdf(hkdfextract(hash((kemcipher(kemencap(Y 1,a 5)),hash((method four,(a 4,(a 5,(a 6,a 7)))))), $\overline{\text{kemkey}}(\text{kemencap}(Y_1,a_5)),\overline{\text{seight}}(id(pk(sk_4),$ ltdh,kempk(sk_auth_kem)),hash((hash)(kemcipher(kemencap($Y \ \overline{1}$, a 5), hash((method_four, (a_4, (a_5))) sk auth kem 3)),(edhoc kdf(hkdfextract(hash(kemcipher(kemencap(Y_1,a_5)), hash((method four,(a 4,(a 5, $(a_6,a_7)))))), kemkey(kemencap(Y 1,a 5)), sfour,$ (id(pk(sk_5),ltdh_3,kempk(sk_auth_kem_3)),hash((kemcipher(kemencap(Y 1, à 5)), hash((method four, (a_4,(a_5,(a_6,a_7)))))),pk(sk_5),a_1),hash_length), a_1))),pk(sk_5)))),pk(sk_4),a_8),hash_length),

(a(8)),pk(sk(4)))),hash length),Y I,a 5)