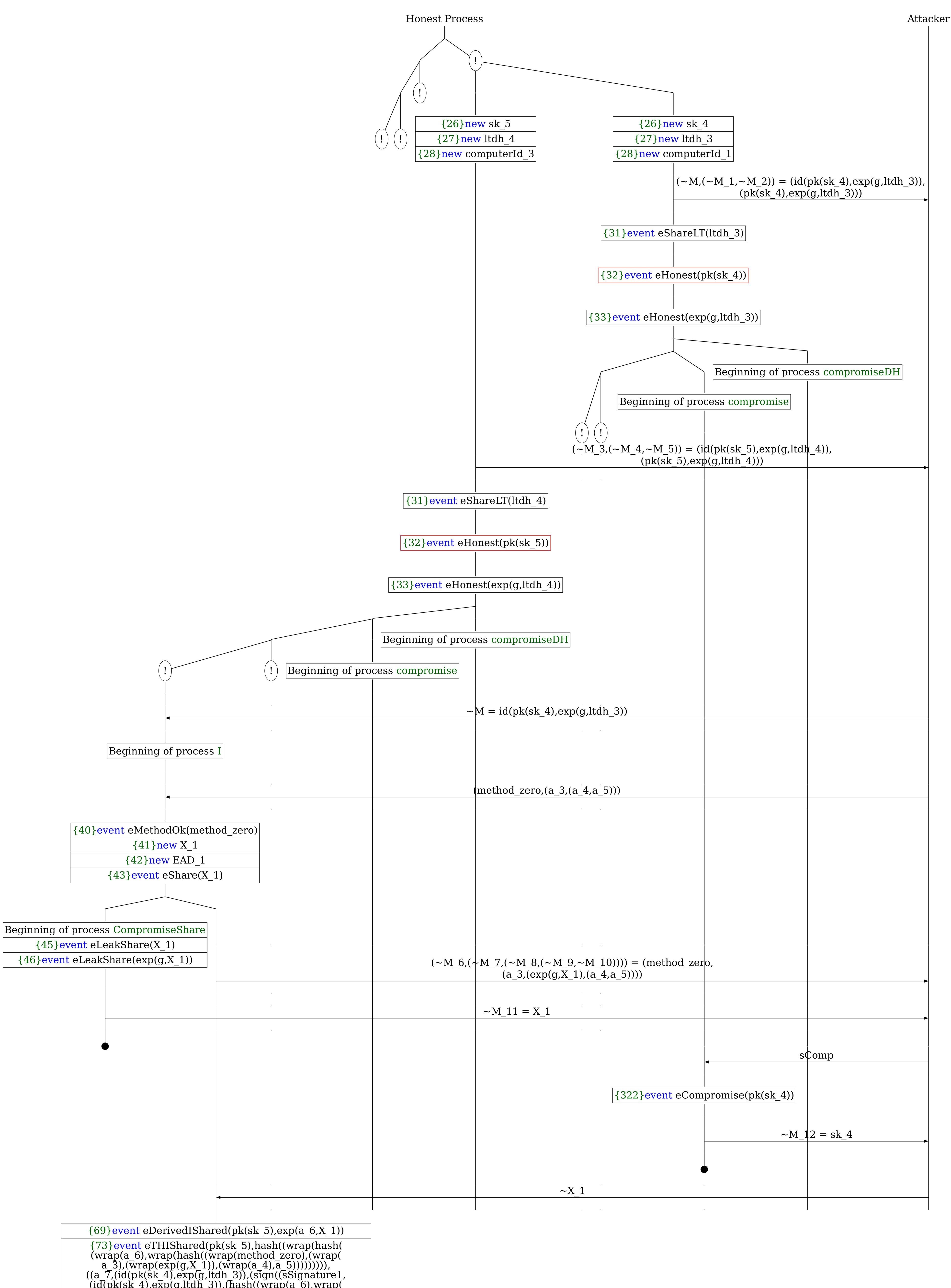
Abbreviations

~X_1 = (a_6,encxor((a_7,(~M,(sign((sSignature1,(~M,(hash(wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(~M_8),(wrap(a_4),a_5))))))),(~M_1, (a_8,edhoc_kdf(hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(~M_8), (wrap(a_4),a_5))))))),exp(a_6,~M_11)),stwo,(~M, (hash((wrap(a_6),wrap(hash((wrap(method_zero), (wrap(a_3),(wrap(~M_8),(wrap(a_4),a_5))))))), (~M_1,a_8))),hash_length)))))),a_9,~M_12),a_8))), edhoc_kdf(hkdfextract(hash((wrap(a_6),wrap(hash(wrap(method_zero),(wrap(a_3),(wrap(~M_8),(wrap(a_4),a_5)))))))),exp(a_6,~M_11)),stzero,hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(~M_8),(wrap(a_4),a_5)))))))),plaintext_length)))

A trace has been found.

(a 6,encxor((a 7,(id(pk(sk 4),exp(g,ltdh 3)), (sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)), (hash((wrap(a 6), wrap(hash((wrap(method zero), $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ (pk(sk 4),(a 8,edhoc kdf(hkdfextract(hash((wrap(a 6), wrap(hash((wrap(method zero), (wrap(a 3), ($wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),exp(a_6,$ $X_1)$, stwo, $(id(pk(sk_4), exp(g, ltdh_3))$, (hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3), $(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))))))(pk(sk_4),$ a 8))),hash length)))))),a 9,sk 4),a 8))),edhoc kdf(hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero), $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ exp(a 6,X 1)),stzero,hash((wrap(a 6),wrap(hash($(wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),$



{83}event eAcceptI(computerId_3,method_zero,pk(sk_5),pk(sk_4),hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),exp(a_6,X_1)),hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))), exp(a_6,X_1)),edhoc_kdf(hkdfextract(hash((wrap(a 6),wrap(hash((wrap(method_zero),(wrap(a_3),(\overline{w} rap(exp(g,X_1)),(wrap(a_4),a_5)))))))),exp(a_6,X_1)),sseven,hash((wrap(hash())))))))))))))))))))))))))))) a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),((a_7, (id(pk(sk_4),exp(g,ltdh_3)),(sign((sSignature1, id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4),(a_8,edhoc_kdf(hkdfextract(hash((wrap(a_6),)))))),(ph(sh_1),(a_6),odh(od_1)),(wrap(a_6),odh(od_2)),(wrap(a_6),wrap(hash((wrap(a_4),a_5))))))), exp(a_6,X_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)), (hash((wrap(a_6),wrap(hash((wrap(method_zero), (wrap(a 3), (wrap(exp(g, X 1)), (wrap(a 4), a 5))))))), (pk(sk 4), a 8))), hash_length))))), a 9, sk 4), a 8))), $pk(sk_4)))),((id(pk(sk_5),exp(g,ltdh_4)),(sign(sSignature2,(id(pk(sk_5),exp(g,ltdh_4)),(hash(ssignature2))))))))$ hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4),(a_8,edhoc_kdf(hkdfextract(hash((wrap(a_6),)))))),(pk(sk_1),(a_6),cdffoc_kdf) (wrap(a_3),(wrap(a_6),wrap(hash((wrap(method_zero), exp(a_6,X_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)), (hash((wrap(a_6),wrap(hash((wrap(method_zero), (wrap(a 3), (wrap(exp(g, X 1)), (wrap(a 4), a 5)))))), (pk(sk 4), a 8))), hash_length))))), a 9, sk 4), a 8))), pk(sk_4)))),(pk(sk_5),(EAD_1,edhoc_kdf(hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))), exp(a_6,X_1)),ssix,(id(pk(sk_5),exp(g,ltdh_4)), $(hash((wrap(hash((wrap(a_6),wrap(hash((wrap(method_zero), wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),\\ ((a_7,(id(pk(sk_4),exp(g,ltdh_3)),(sign((sSignature1, (id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(a_6),wrap$ hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, X_1)),(wrap(a_4),a_5))))))))),(pk(sk_4),(a_8,edhoc_kdf(hkdfextract(hash((wrap(a_6),)))))),(ph(sh_1),(a_6),odh(ob), land)
(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),
exp(a_6,X_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)),
(hash((wrap(a_6),wrap(hash((wrap(method_zero),

(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))), (pk(sk_4),a_8))),hash_length)))))),a_9,sk_4),a_8))), pk(sk_4)))),(pk(sk_5),EAD_1))),hash_length))))), srep,sk_5),EAD_1)),pk(sk_5)))),hash_length),X_1,