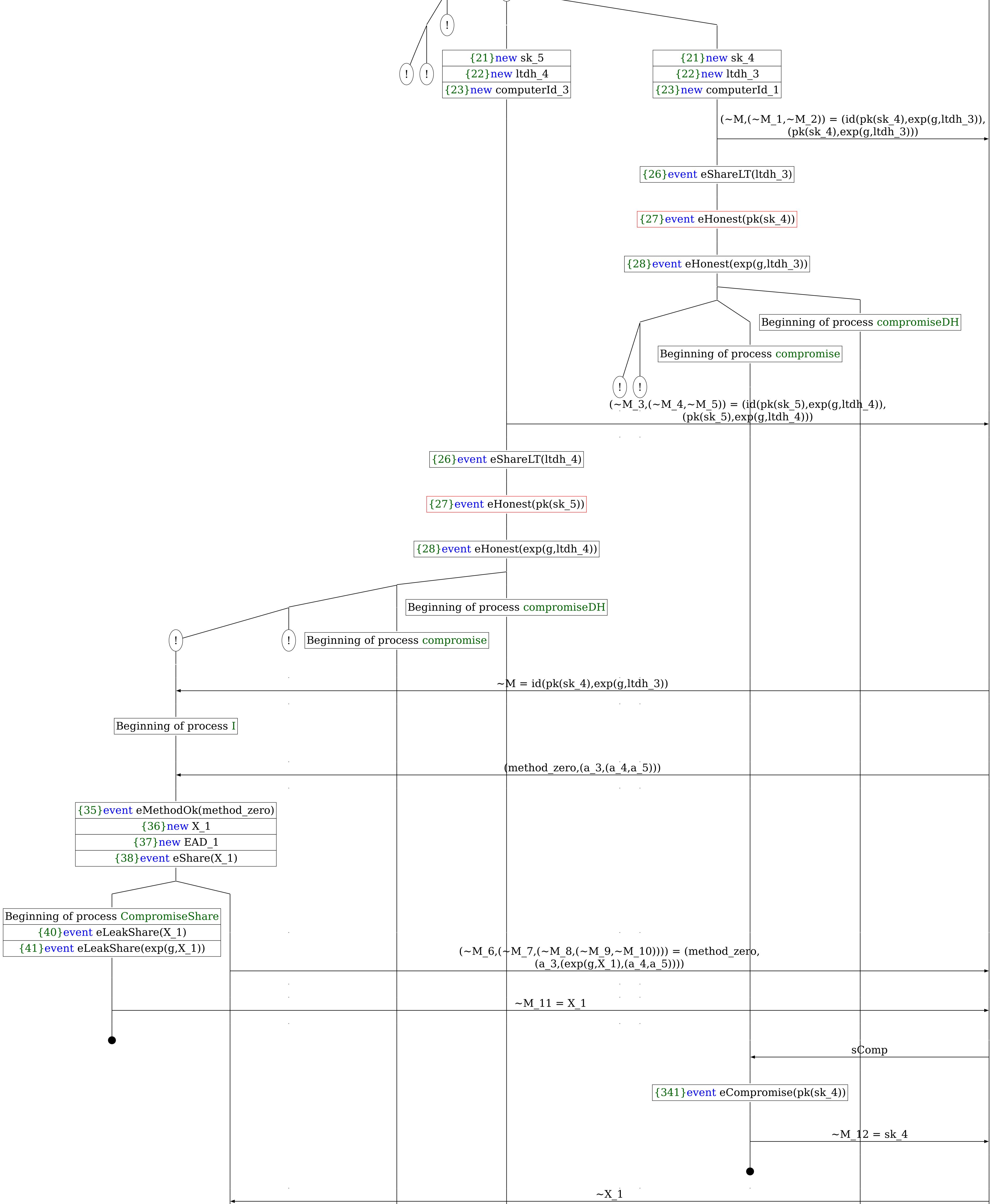
Abbreviations

 $\sim X_1 = (a_6, encxor((a_7, (\sim M, (sign((sSignature1, (\sim M, (hash($ (wrap(a 6), wrap(hash((wrap(method zero), (wrap(a 3), $(wrap(\sim M 8),(wrap(a 4),a 5)))))),(\sim M 1,$ (a 8,edhoc kdf(hkdfextract(hash((wrap(a 6),wrap(hash((wrap(method zero),(wrap(a 3),(wrap(~M 8), $(wrap(a 4), a 5)))))))))exp(a 6, \sim M 11)),stwo,(\sim M,$ (hash((wrap(a 6), wrap(hash((wrap(method zero), $(wrap(a 3),(wrap(\sim M 8),(wrap(a 4),a 5))))))),$ (~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))))))), $\exp(a 6,\sim M 11)$),stzero,hash((wrap(a 6),wrap(hash((wrap(method zero),(wrap(a 3),

(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), (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(($(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))))))(pk(sk_4),$ a 8))),hash length)))))),a 9,sk 4),a 8))),edhoc kdf(exp(a 6,X 1)),stzero,hash((wrap(a 6),wrap(hash(

A trace has been found.

 $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ wrap(a_6),wrap(hash((wrap(method_zero),(wrap(a_3), hkdfextract(hash((wrap(a_6),wrap(hash((wrap(method_zero), $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ $(wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),$ Attacker **Honest Process** {21}new sk 5 {21}new sk 4 {22}new ltdh 3 {23}new computerId 1 $(\sim M, (\sim M_1, \sim M_2)) = (id(pk(sk_4), exp(g, ltdh_3)),$ $(pk(sk_4),exp(g,ltdh_3)))$



{64}event eDerivedIShared(pk(sk_5),exp(a_6,X_1)) {68} event eTHIShared(pk(sk_5),hash((wrap(hash({68}event eTHIShared(pk(sk_5),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),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))),
pk(sk_4))))

{78} 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,