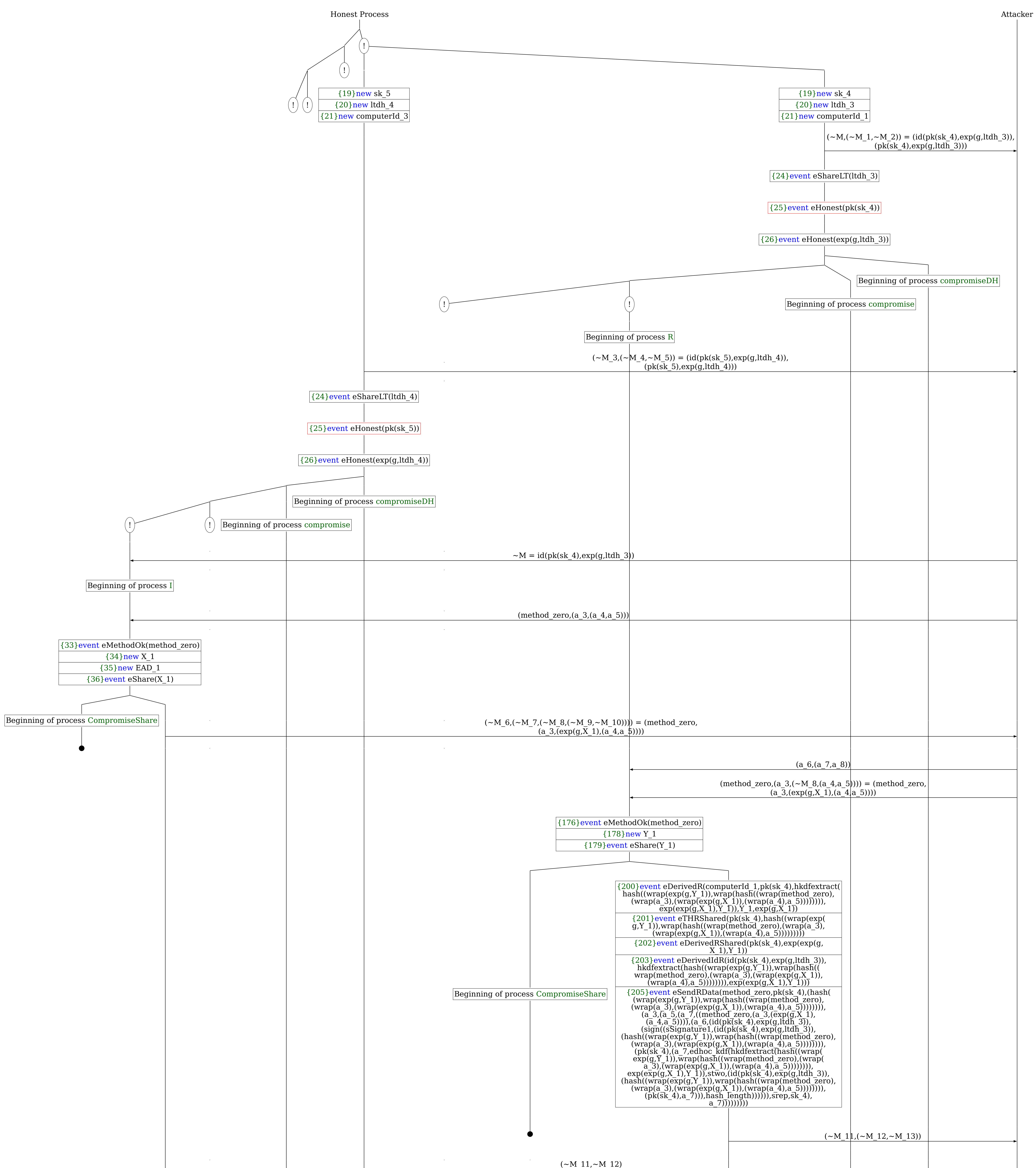
Abbreviations $\sim M_111 = \exp(g, Y_1)$ $\sim M_12 = encxor((a_6,(id(pk(sk_4),exp(g,ltdh_3)),($ sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)), (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero), $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),$ (pk(sk_4),(a_7,edhoc_kdf(hkdfextract(hash((wrap($\exp(g,\overline{Y} \ 1))$, \overline{w} $\exp(hash((wrap(method zero),(wrap(method zero))))$ a_3 ,(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))), $\exp(\exp(g,X_1),Y_1)$, stwo, $(id(pk(sk_4), \exp(g,ltdh_3))$, A trace has been found. (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero), $(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ (pk(sk_4),a_7))),hash_length)))))),srep,sk_4), a 7))),edhoc kdf(hkdfextract(hash((wrap(exp(g, Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), $g,X_1),Y_1),stzero,hash((wrap(exp(g,Y_1)),wrap($ hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, $X_1)$,(wrap(a_4),a_5))))))),plaintext_length)) \sim M 13 = a 6



{62}event eDerivedIShared(pk(sk_5),exp(exp(g,Y_1), {64} event eVerified(sign((sSignature1,(id(pk(sk_4), exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5)))))))),(pk(sk_4),(a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash(wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5))))))),exp(exp(g,Y_1),X_1)),stwo, (id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1),X_1)),wrap(b,ash((wrap(mathod_zero)),(wrap(a_2)))))))),wrap(b,ash((wrap(mathod_zero)),(wrap(a_2))))))) Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4), a_7))),hash_length)))))),srep,sk_4),e1(sign((sSignature1, (id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g, Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4), (a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero)),wrap(a_3), wrap(hash((wrap(method_zero)),wrap(a_3), wrap(hash((wrap(method_zero)),wrap(a_3),wrap(a_3))))))))) wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),exp(exp(g,Y_1),X_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero), (wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))), (pk(sk_4),a_7))),hash_length)))))),srep,sk_4)), e3(sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)), $(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3), (wrap(exp(g,X_1)), (wrap(a_4), a_5)))))))),$ (pk(sk 4),(a 7,edhoc kdf(hkdfextract(hash((wrap($\exp(g, \overline{Y} 1))$, wrap(hash((wrap(method_zero),(wrap($(wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3), (wrap(exp(g,X_1)), (wrap(a_4), a_5))))))))$ (pk(sk_4),(a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(3), $\overline{(wrap(exp(g,X 1)), (wrap(a 4), \overline{a} 5)))))))),$ $\exp(e\overline{x}p(g,Y_1),X_1))$, $\operatorname{stwo}(id(pk(sk_4),e\overline{x}p(g,ltdh_3)))$, $(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3), (wrap(exp(g,X_1)), (wrap(a_4), a_5)))))))),$ $(pk(sk_4),a_7)),hash_length))))),pk(sk_4),sigtrue)$ {66}<mark>event</mark> eTHIShared(pk(sk 5),hash((wrap(hash($(wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3), (wrap(exp(g,X_1)), (wrap(a_4), a_5)))))))),$ ((a_6,(id(pk(sk_4),exp(g,ltdh_3)),(sign((sSignature1, id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g, Y_1)), wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4), (a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),exp(exp(g,Y_1), X_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)),(hash(($wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ (pk(sk_4),a_7))),hash_length)))))),srep,sk_4), a_7))),pk(sk_4))))

{76} event eAcceptI(computerId 3,method zero,pk(sk_5),pk(sk_4),hkdfextract(hash((wrap(exp(g,Y_1))), wrap(hash((wrap(method_zero),(wrap(a_3),(wrap($\exp(g,X_1)$, $(wrap(a_4),a_5)))))), <math>\exp(\exp(g,Y_1),X_1)$, $(wrap(a_4),a_5)))))), exp(exp(g,Y_1), <math>(wrap(exp(g,Y_1)), wrap(exp(g,Y_1))))$ hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, X_1)),(wrap(a_4),a_5))))))),exp(exp(g,Y_1),X_1)), edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g, X_1)),(wrap(a_4),a_5))))))),exp(exp(g,Y_1),X_1)), sseven,hash((wrap(hash((wrap(hash((wrap(exp(g, X_1), X_2))))))) Y_1)),wrap(hash((wrap(method_zero)),(wrap(a_3), $(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))))),(a_6,a_7)$ (id(pk(sk_4),exp(g,ltdh_3)),(sign((sSignature1, id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g, Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),(pk(sk_4), (a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), (a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero),(wrap(a_3),(wrap($\exp(g,X_1)$, $(wrap(a_4),a_5)))))), <math>\exp(\exp(g,Y_1)$, $X_1)$, stwo, $(id(pk(sk_4),exp(g,ltdh_3))$, (hash(($wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero), (wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),$ (wrap(a_5),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))), (pk(sk_4),a_7))), hash_length)))))), srep,sk_4), a_7))), pk(sk_4)))), (id(pk(sk_5), exp(g,ltdh_4)), (sign((sSignature2,(id(pk(sk_5), exp(g,ltdh_4)), (hash((wrap(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5))))))))), ((a_6,(id(pk(sk_4), exp(a_4),a_5)))))))))), ((a_6,(id(pk(sk_4), exp(a_4),a_5)))))))), ((a_6,(id(pk(sk_4), exp(a_4),a_5))))))))))))) g,ltdh_3)),(sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5))))))),(pk(sk_4),(a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),exp(exp(g,Y_1),X_1)),stwo, (id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1),X_2),X_1)))) Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),(pk(sk_4), a_7))),hash_length)))))),srep,sk_4),a_7))),pk(sk_4)))),(pk(sk_5),(EAD_1,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero), (wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))))))) exp(exp(g,Y_1),X_1)),ssix,(id(pk(sk_5),exp(g,ltdh_4)), (hash((wrap(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5))))))),((a_6,(id(pk(sk_4),exp(g,ltdh_3)),(sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(exp(g,1_1)),wrap(nash() wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5)))))))),(pk(sk_4),(a_7,edhoc_kdf() hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash(() wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)), (wrap(a_4),a_5)))))))),exp(exp(g,Y_1),X_1)),stwo, (id(pk(sk_4),exp(g,ltdh_3)),(hash((wrap(exp(g,Y_1)),wrap(a_3)), (wrap(a_3)))))))),exp(exp(g,Y_1),X_2)),wrap(a_3) Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3), (wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),(pk(sk_4), a_7))),hash_length))))),srep,sk_4),a_7))),pk(sk_5),EAD_1))),hash_length))))),

srep,sk_5),EAD_1)),pk(sk_5)))),hash_length),X_1, exp(g,Y_1))