$(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),\\ (wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),\\ (pk(sk_4),(a_7,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),\\ exp(exp(g,X_1),Y_1)),stwo,(id(pk(sk_4),exp(g,ltdh_3)),\\ (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5))))))),\\ (pk(sk_4),a_7))),hash_length))))),srep,sk_4),\\ a_7))),edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,X_1)),(wrap(a_4),a_5)))))))),exp(exp(g,X_1),Y_1)),stzero,hash((wrap(exp(g,Y_1)),wrap($

hash((wrap(method_zero),(wrap(a_3),(wrap(exp(g,

 $X_1)$,(wrap(a_4),a_5))))))),plaintext_length))

 \sim M 13 = a 6

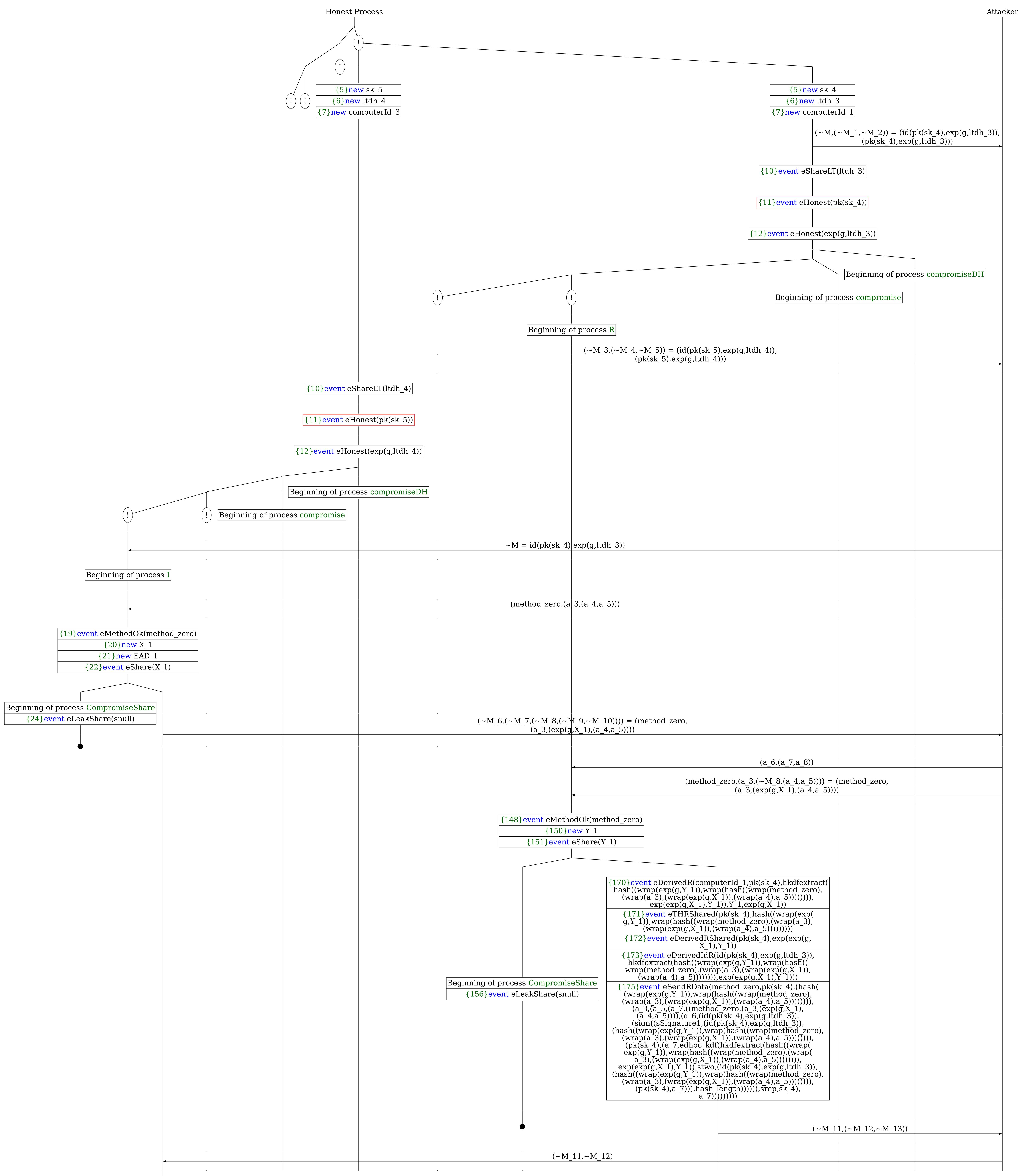
Abbreviations

 $\sim M_111 = \exp(g, Y_1)$

 $\sim M_12 = encxor((a_6,(id(pk(sk_4),exp(g,ltdh_3)),($

 $sign((sSignature1,(id(pk(sk_4),exp(g,ltdh_3)),$

A trace has been found.



{46} event eDerivedIShared(pk(sk_5),exp(exp(g,Y_1), X_1))

{50} event 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 [ength)))))),srep,sk_4), a_7))),pk(sk_4)))))

{60} 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))))))), exp(exp(g,Y 1), X 1)), hkdfextract(hash((wrap(exp(g,Y 1)), wrap(a hash((wrap(exp(g,Y 1)), wrap(hash((wrap(exp(g,Y 1)), wrap(a hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method zero), (wrap(a 3), (wrap(exp(g,X 1)), wrap(a hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method zero), (wrap(a 3), (wrap(exp(g,X 1)), wrap(a hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method zero), (wrap(a 3), (wrap(exp(g,Y 1)), wrap(hash((wrap(exp(g,X 1)), wrap(hash((wrap(exp(g,X 1)), wrap(hash((wrap(exp(g,X 1)), wrap(a 4),a 5))))))), exp(exp(g,Y 1), x 1)), stwo, (id(pk(sk 4), exp(g,tlth 3)), (hash((wrap(exp(g,X 1)), wrap(hash((wrap(exp(g,X 1)), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1)), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(exp(g,X 1)), (wrap(a 4),a 5))))))), exp(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1), wrap(hash((wrap(exp(g,Y 1