A trace has been found.

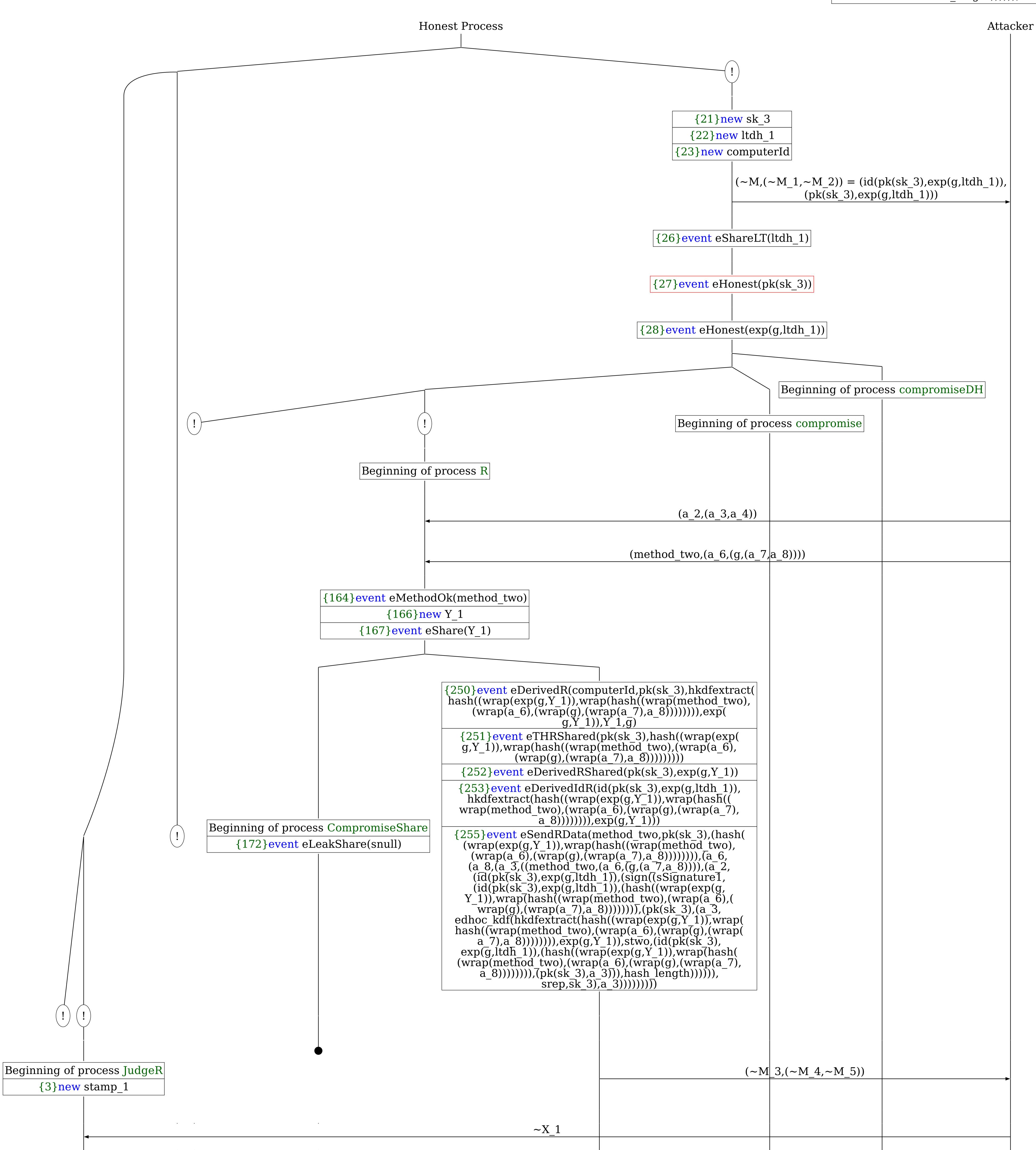
Abbreviations $\sim M \ 3 = \exp(g, Y \ 1)$

 $\sim X_1 = (\sim M, (hash((wrap(\sim M_3), wrap(hash((wrap(method_two), (wrap(a_6), (wrap(g), (wrap(a_7), a_8))))))), (\sim M_1, (a_3, (edhoc_kdf(hkdfextract(hash((wrap(\sim M_3), wrap(hash((wrap(method_two), (wrap(a_6), (wrap(g), (wrap(a_7), a_8))))))), \sim M_3), stwo, (\sim M, (hash((wrap(\sim M_3), wrap(hash((wrap(method_two), (wrap(a_6), (wrap(g), (wrap(a_7), a_8))))))), (\sim M_1, a_3))), hash_length), 1-proj-2-tuple(2-proj-2-tuple(2-proj-2-tuple(decxor(\sim M_4, edhoc_kdf(hkdfextract(hash((wrap(\sim M_3), wrap(hash((wrap(method_two), (wrap(a_6), (wrap(g), (wrap(a_7), a_8))))))), \sim M_3), stzero, hash((wrap(\sim M_3), wrap(hash((wrap(method_two), (wrap(a_6), (wrap(g), (wrap(a_7), a_8))))))))), plaintext_length))))))))))))$

(wrap(g),(wrap(a 7),a 8))))))),plaintext length))

 \sim M 5 = a 2

 $(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp($ g,Y 1)),wrap(hash((wrap(method two),(wrap(a 6), (wrap(g),(wrap(a 7),a 8)))))),(pk(sk 3),(a 3,(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method two),(wrap(a 6),(wrap(g), (wrap(a 7), a 8))))))), exp(g,Y 1)), stwo, (id(pk(sk 3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method two),(wrap(a_6),(wrap(g),(wrap(a 7),a 8))))))),(pk(sk 3),a 3))),hash length), sign((sSignature1,(id(pk(sk 3),exp(g,ltdh 1)), $(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method_two),$ $(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))),(pk($ sk 3),(a 3,edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 6), $(wrap(g),(wrap(a_7),a_8)))))),exp(g,Y_1)),stwo,$ $(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(u))),(hash((wrap(exp(u))),(hash((wrap(exp(u))),(hash((wrap(exp(u))),(hash((wrap(exp(u))),(hash((wrap(exp(u))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w)),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),(hash((w))),($ Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),($wrap(g),(wrap(a_7),a_8))))))),(pk(sk_3),a_3))),$ hash length)))))),srep,sk 3)))))



{6}event eJudgeReceivedR(stamp_1,(id(pk(sk_3), exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7), a_8))))))),(pk(sk_3),(a_3,(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))),exp(g,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two), (wrap(a_6),(wrap(g),(wrap(a_7),a_8)))))),dpk(sk_3),a_3)),hash_length),sign((sSignature1,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g), (wrap(a_7), a_8))))))),pk(sk_3),(a_3,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7), a_8))))))),exp(g,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7), a_8))))))),fpk(sk_3),a_3)),hash_length))))),srep,sk_3)))))))

{8}event eWasActiveR(pk(sk_3),hash((wrap(exp(g, Y_1)),wrap(hash((wrap(method two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))), (id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))), (pk(sk_3),(a_3,(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))), exp(g,Y_1)), stwo, (id(pk(sk_3),exp(g,ltdh_1)), (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8)))))), (pk(sk_3),a_3)), hash length), sign((sSignature1,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))), (pk(sk_3),(a_3,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8))))))), exp(g,Y_1)), stwo, (id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_6),(wrap(g),(wrap(a_7),a_8)))))))), exp(g,X_1)), hash_length))))), srep,sk_3))))))), exp(g,x_3))), hash_length))))),