Abbreviations \sim M 3 = exp(g,Y 1) \sim M 4 = encxor((a 3,(id(pk(sk 3),exp(g,ltdh 1)),(sign((sSignature1,(id(pk(sk 3),exp(g,ltdh 1)),(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two), $(wrap(a 7),(wrap(a_8),(wrap(a_9),a_10))))))),$ (pk(sk 3),(a 4,edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10))))))),exp(a 8, Y 1)), stwo, (id(pk(sk 3), exp(g, ltdh 1)), (hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10))))))),(pk(sk 3),a 4))),hash length)))))),srep,sk 3),a 4))), edhoc kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))),exp(a 8,Y 1)),stzero,hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two), (wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))plaintext length)) \sim M 5 = a 3 $(wrap(a 7),(wrap(a_8),(wrap(a_9),a_10))))))),$

 $\sim X 1 = (\sim M, (hash((wrap(\sim M 3), wrap(hash((wrap(method two), lange))))))$ $(\sim M 1,(a 4,(edhoc kdf(hkdfextract(hash((wrap(\sim M 3),$ wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), $(hash((wrap(\sim M 3), wrap(hash((wrap(method two),$ (wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))(~M 1,a 4))),hash length),mangle(1-proj-2-tuple(2-proj-2-tuple(2-proj-2-tuple(decxor(~M 4,edhoc kdf(hkdfextract(hash((wrap(~M 3),wrap(hash((wrap(method two), (wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))exp(a 8,~M 6)),stzero,hash((wrap(~M 3),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))),plaintext length))))),a 11))))) (id(pk(sk 3),exp(g,ltdh 1)),(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7), (wrap(a 8),(wrap(a 9),a 10))))))),(pk(sk 3),(a 4,(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), $pk(sk_3), exp(g,ltdh_1)), (hash((wrap(exp(g,Y 1)),$ wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), sign((sSignature1,(id(pk(sk 3),exp(g,ltdh 1)),

(pk(sk 3),(a 4,edhoc kdf(hkdfextract(hash(wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10))))))),exp(a 8, Y 1), stwo, (id(pk(sk 3), exp(g, ltdh 1)), (hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10))))))),(pk(sk_3),a_4))),hash_length)))))),a_11,sk_3))))) \sim X 2 = (\sim M,(hash((wrap(\sim M 3),wrap(hash((wrap(method two), (wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))(~M 1,(a 4,(edhoc kdf(hkdfextract(hash((wrap(~M_3), wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), $(hash((wrap(\sim M 3), wrap(hash((wrap(method two),$ (wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))(~M 1,a 4))),hash_length),mangle(1-proj-2-tuple(2-proj-2-tuple(2-proj-2-tuple(decxor(~M 4,edhoc kdf($hkdfextract(hash((wrap(\sim M 3), wrap(hash((wrap(method two),$ $(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),$

exp(a 8,~M 6)),stzero,hash((wrap(~M 3),wrap(hash(

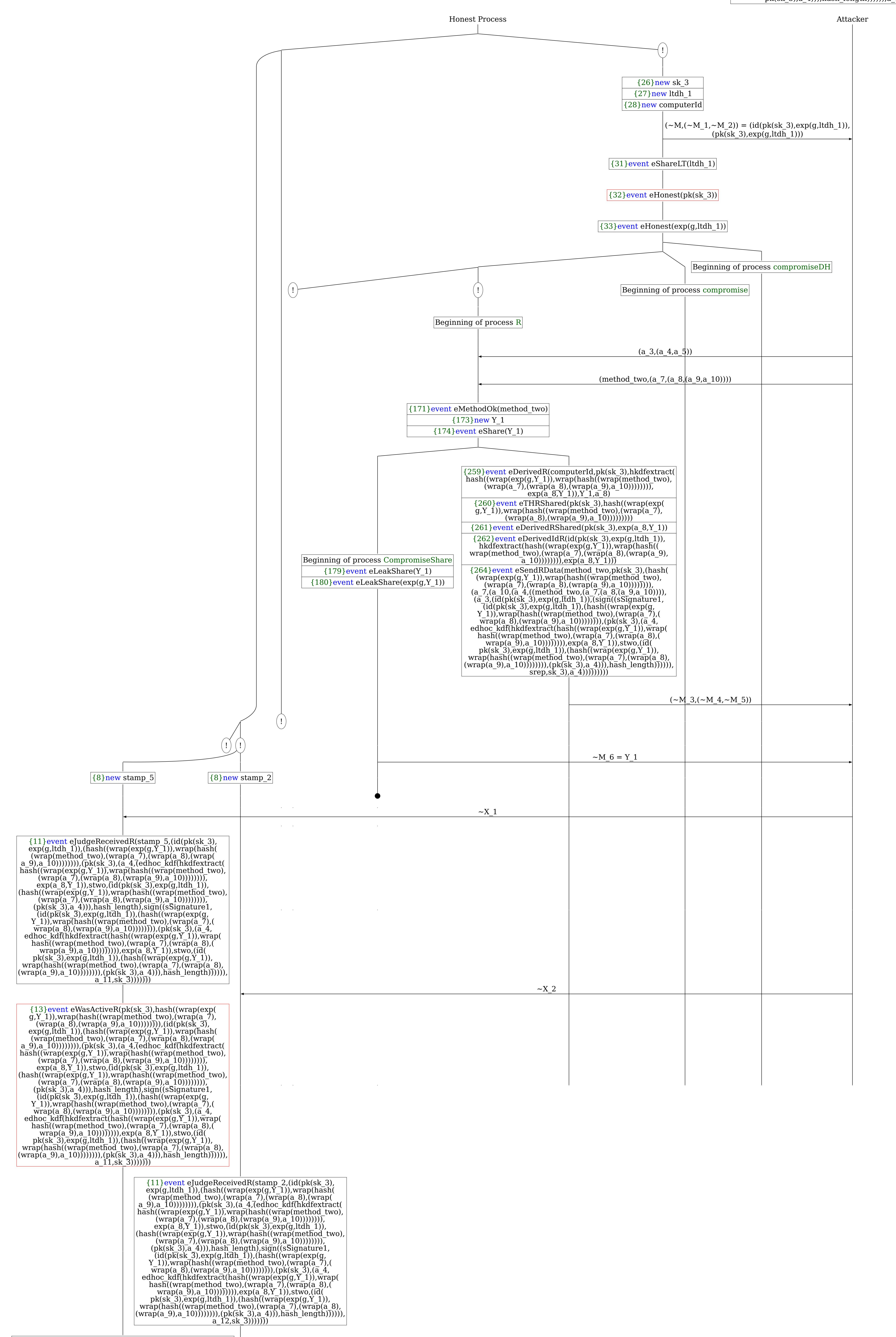
(wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(

a 9),a 10))))))),plaintext length))))),a 12)))))

(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),

(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10)))))))

(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method_two),(wrap(a_7), (wrap(a 8),(wrap(a 9),a 10))))))),(pk(sk 3),(a_4,(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)), wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), $(wrap(a_9),a_10))))))), exp(a_8,Y_1)), stwo, (id($ $pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y 1)),$ wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8), sign((sSignature1,(id(pk(sk 3),exp(g,ltdh 1)), (hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method two), $(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),$ (pk(sk 3),(a 4,edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7),(wrap(a 8),(wrap(a 9),a 10))))))),exp(a 8, \overline{Y} 1)),stwo,($\overline{id}(pk(sk_3),exp(g,ltdh_1))$,(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),($wrap(a_7),(wrap(a_8),(wrap(a_9),a_10)))))),($ pk(sk 3),a 4))),hash length)))))),a_12,sk_3)))))



A trace has been found.

{14}event eJudgeProcessedR((id(pk(sk_3),exp(g, ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))), (pk(sk_3),(a_4,(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8, Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10)))))))),(pk(sk_3),a_4))),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_7),(wrap(a_8),(wrap(a_9),a_10)))))))),(pk(sk_3),(a_4,edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10)))))))),exp(a_8,Y_1)),stwo,(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10)))))))),exp(a_8,Y_1)),hash_length)))))),exp(a_9,a_10))))))),exp(sk_3),a_4))),hash_length)))))),exp(a_9,a_10))))))),exp(a_8,Y_1),hash_length)))))),exp(a_9,a_10))))))),exp(a_8,Y_1),hash_length)))))),exp(a_9,a_10))))))),exp(a_8,Y_1),hash_length)))))),exp(a_9,a_10))))))),exp(a_11,sk_3)))))))

{13}event eWasActiveR(pk(sk 3),hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method two),(wrap(a 7), $(\overline{w}rap(a_8),(\overline{w}rap(a_9),a_10)))))),(id(pk(sk_3),a_10))))$ $\exp(g, ltdh_1)$, $(hash(wrap(exp(g, Y_1)), wrap(hash(g, Y_2)))$ (wrap(method two), (wrap(a 7), (wrap(a 8), (wrap(hāsh((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two)), (wrap(a_7),(wrap(a_8),(wrap(a_9),a_10)))))), $\exp(a^{1}8,\overline{Y}1)$),stwo, $(id(pk(sk^{1}3),exp(g,ltdh^{1}))$, $(\text{hash}((\text{wrap}(\text{exp}(\text{g,Y}_1)),\text{wrap}(\text{hash}((\text{wrap}(\text{method}_{\text{two}}),$ (wrap(a 7), (wrap(a 8), (wrap(a 9), a 10)))))), $(pk(sk_3), a_4)), hash_length, sign((sSignature1), sign((sSignat$ (id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g, Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(\overline{w} rap(a_8),(wrap(a_9),a_10))))))),(pk(sk_3),(a_4, edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),(wrap(a_9),a_10))))))),exp(a_8,Y_1)),stwo,(id(
pk(sk_3),exp(g,ltdh_1)),(hash((wrap(exp(g,Y_1)),
wrap(hash((wrap(method_two),(wrap(a_7),(wrap(a_8),
(wrap(a_9),a_10)))))),(pk(sk_3),a_4))),hash_length)))))),
a_12,sk_3))))))