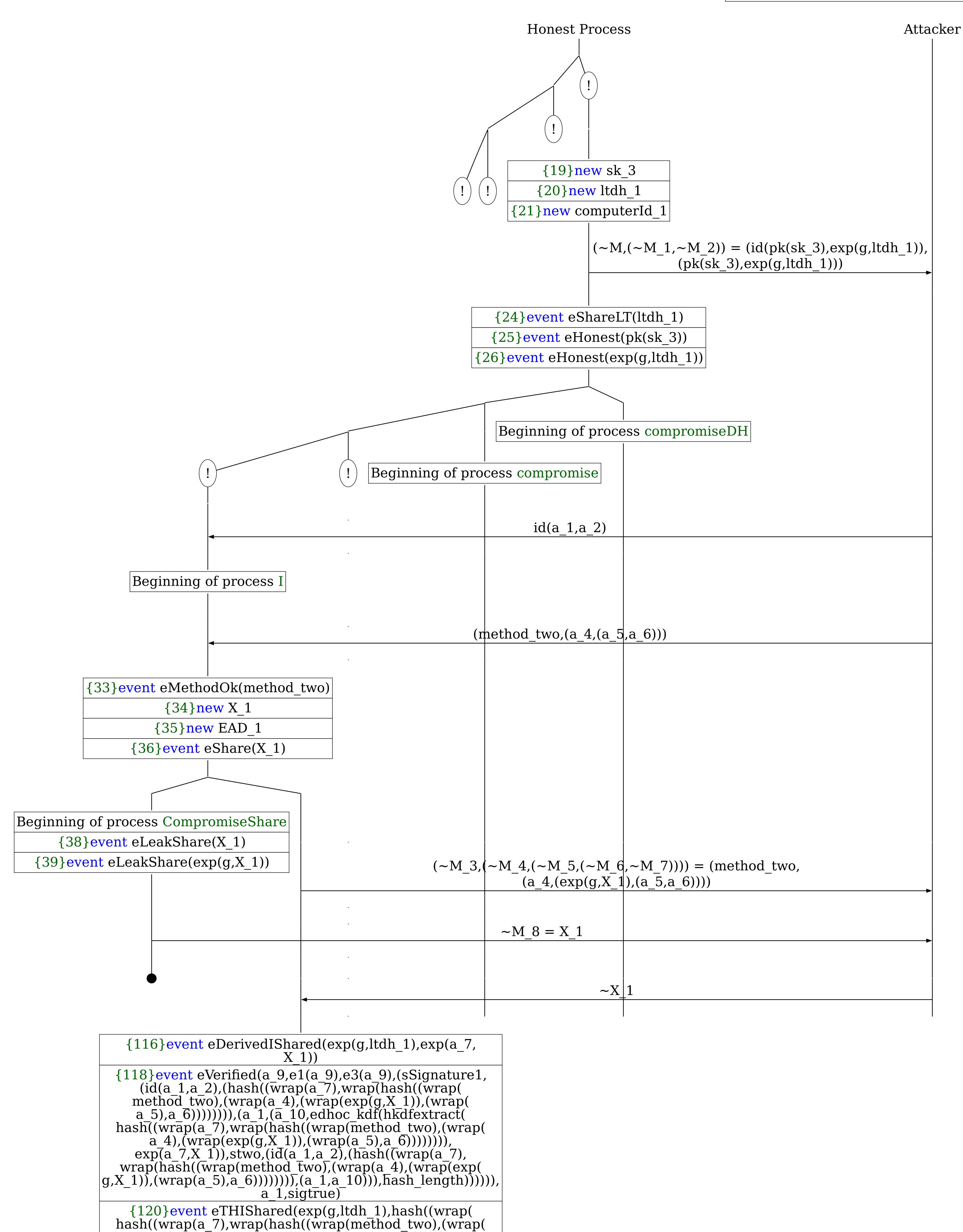
Abbreviations

 $\begin{array}{l} \sim & X_1 = (a_7, encxor((a_8, (id(a_1, a_2), (a_9, a_10))), edhoc_kdf(\\ & hkdfextract(hash((wrap(a_7), wrap(hash((wrap(method_two),\\ & (wrap(a_4), (wrap(\sim M_5), (wrap(a_5), a_6))))))),\\ & exp(a_7, \sim M_8)), stzero, hash((wrap(a_7), wrap(hash(\\ & (wrap(method_two), (wrap(a_4), (wrap(\sim M_5), (wrap(a_5), a_6))))))), plaintext_length)))\\ & = (a_7, encxor(\\ \end{array}$

(a_8,(id(a_1,a_2),(a_9,a_10))),edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))), exp(a_7,X_1)),stzero,hash((wrap(a_7),wrap(hash(wrap(method_two),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),plaintext_length)))

A trace has been found.



{132}event eAcceptI(computerId_1,method_two,exp(g,ltdh_1),a_1,hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_two),(wrap(a_4),(wrap(exp(g, X 1)), $(wrap(a_5), a_6)))))))), exp(a_7, X_1)), hkdfextract($ edhoc kdf(hkdfextract(hash(wrap(a 7),wrap(hash((wrap(method two),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a 5),a^{\overline{6}}))))))))exp(\overline{a} 7,X 1)),sfive,hash($ (wrap(hash((wrap(a 7), wrap(hash((wrap(method_two), (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))))((a 8,(id(a 1,a 2),(a 9,a 10))),a 1))),hash length), exp(a 7,ltdh 1)),edhoc kdf(hkdfextract(edhoc kdf($hkdfextract(hash(wrap(a 7), wrap(hash(wrap(method_two),$ $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))$ exp(a 7,X 1)), sfive, hash ((wrap(hash ((wrap(a 7), $wrap(ha\overline{s}h((\overline{w}rap(method\ two),(wrap(a\ 4),(wrap(exp($ $g_{X_1}(wrap(a_5),a_6))))))),((a_8,(id(a_1,a_5),a_6))))))))$ a 2), (a 9, a $1\overline{0}$)), a 1)), hash length, exp(\overline{a} 7) ltdh 1)),sseven,hash((wrap(hash((wrap(hash((wrap(a 7), wrap(hash((wrap(method two),(wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))))))((a 8,(id) a 1,a 2),(a 9,a 10))),a_1))),((id(pk(sk_3),exp(g,ltdh_1)),(edhoc_kdf(hkdfextract(edhoc kdf(hkdfextract(hash(wrap(a 7), wrap(hash((wrap(method two), (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a 5),a 6))))))), $\exp(a 7, X 1)$, sfive, hash((wrap(hash((wrap(a 7), yrap(a 7)))) $wrap(ha\overline{s}h((\overline{w}rap(method\ two),(wrap(a\ 4),(wrap(exp($ $g_{X_1}(x_1), (wrap(a_5), a_6))))))), (a_8, (id(a_1, a_1)), (a_8, a_6))))))))$ a 2),(a 9,a 10))),a 1))),hash length),exp(a 7, ltdh 1), ssix, (id(pk(sk 3), exp(g, ltdh 1)), (hash(g, ltdh 1))(wrap(hash((wrap(a 7), wrap(hash((wrap(method_two), (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))), ((a_8,(id(a_1,a_2),(a_9,a_10))),a_1))),(exp(g, ltdh_1),EAD_1))),hash_length),EAD_1)),exp(g,ltdh_1))), hash_length),X_1,a_7)

à_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))), ((a_8,(id(a_1,a_2),(a_9,a_10))),a_1))))