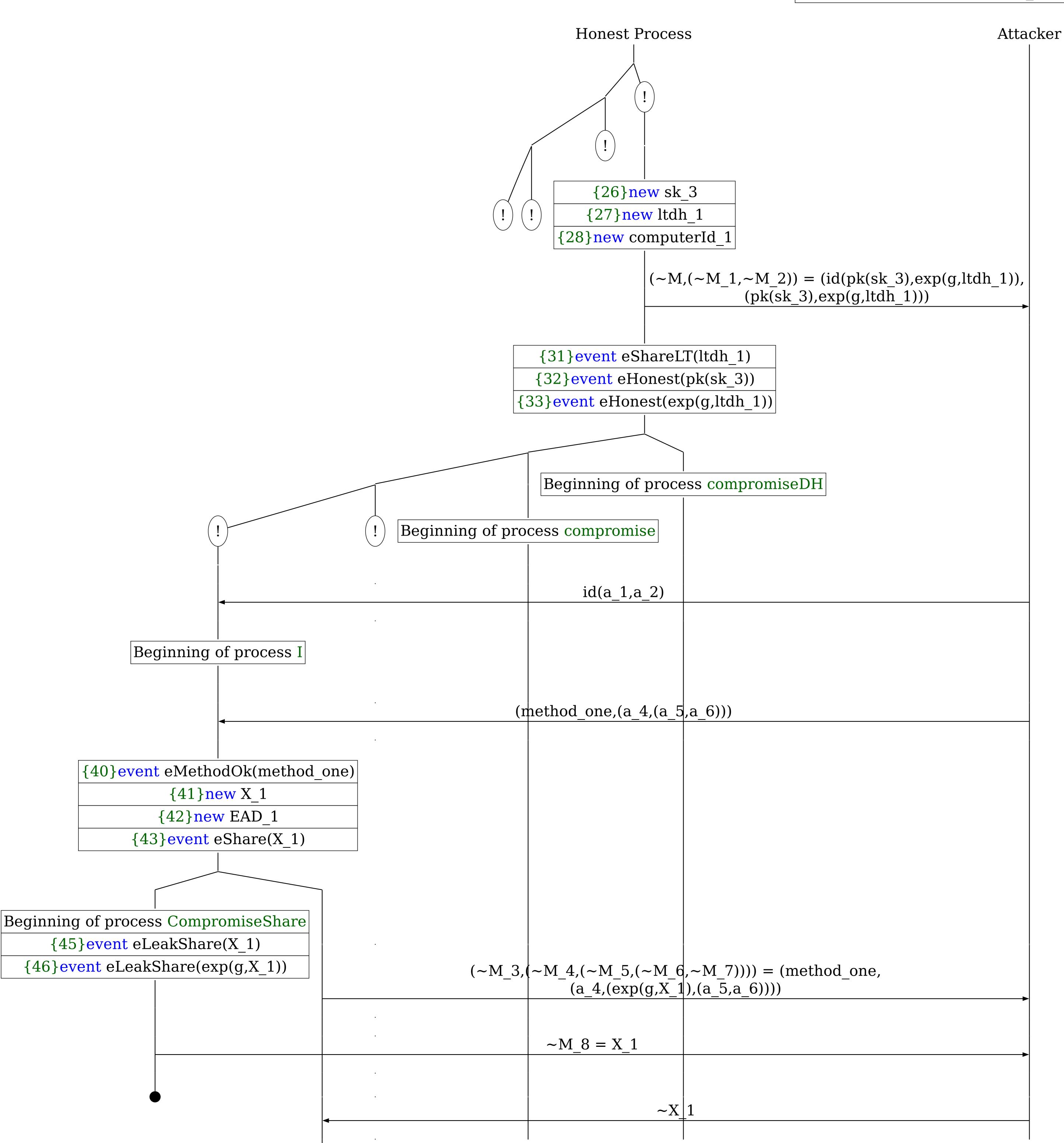
Abbreviations

$$\begin{split} \sim & X_1 = (a_7, encxor((a_8, (id(a_1, a_2), (edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7), wrap(hash(ewrap(method_one), (wrap(a_4), (wrap(\sim M_5), (wrap(a_5), a_6))))))), exp(a_7, \sim M_8)), stone, hash((wrap(e_3, wrap(hash((wrap(method_one), (wrap(a_4), (wrap(\sim M_5), (wrap(a_5), a_6))))))), hash_length), exp(e_3, \sim M_8)), stwo, (id(e_1, e_3, e_2), (hash((wrap(e_3, e_3), ewrap(hash((wrap(method_one), (wrap(e_4), (wrap(\sim M_5), (wrap(e_5), e_3))))))), (e_3, e_2, e_3))), hash_length), ewrap(e_5), ewrap(e_3, e_3))), hash_length), ewrap(e_5), ewrap(e_6, e_3), ewrap(e_4), (wrap(\sim M_5), (wrap(e_5), e_3)))))))), exp(e_7, \sim M_8)), stzero, hash(ewrap(e_3, e_3), ewrap(e_3, e_3), ewrap(e_4), (wrap(e_4), (wrap(e_4), (wrap(e_5), e_3), ewrap(e_5), ew$$

 $(a_7, encxor((a_8, (id(a_1, a_2), (edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6))))))), exp(a_7, X_1)), stone, hash((wrap(a_7), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6))))))), hash_length), exp(a_2, X_1)), stwo, (id(a_1, a_2), (hash((wrap(a_7), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6))))))), (a_2, a_9))), hash_length), a_9))), edhoc_kdf(hkdfextract(hash((wrap(a_7), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6))))))))), exp(a_7, X_1)), stzero, hash((wrap(a_7), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6)))))))), plaintext_length)))$

A trace has been found.



{94}event eDerivedIShared(pk(sk_3),exp(a_7,X_1))

{98}event eTHIShared(pk(sk_3),hash((wrap(hash(wrap(a_7),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),
exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),
stwo,(id(a_1,a_2),(hash((wrap(a_7),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))),(a_2,a_9))),hash_length),
a_9))),a_2))))

{108}event eAcceptI(computerId 1,method one,pk(sk 3),a 2,hkdfextract(edhoc kdf(hkdfextract(hash($(wrap(a \overline{7}), wrap(hash((wrap(method one), (wrap(a 4),$ (wrap(exp(g,X_1)),(wrap(a_5),a_6)))))), exp(a_7, X_1)), stone, hash((wrap(a_7), wrap(hash((wrap(method_one), $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),$ hash length), exp(a 2,X 1), hkdfextract(edhoc_kdf($hkdfextract(hash((wrap(a_7), wrap(hash((wrap(method_one), a_7), wrap(hash((wrap(meth$ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6))))))) $\exp(a^{7},X^{1})$, stone , $\operatorname{hash}((\operatorname{wrap}(a^{7}),\operatorname{wrap}(\operatorname{hash}($ (wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), (wrap(a 5),a 6)))))))),hash [ength],exp(a 2,X 1)), edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash) $(wrap(\bar{a} 7), wrap(hash((wrap(\bar{m}ethod one), (wrap(a 4),$ $(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),exp(a_7,$ X 1)), stone, hash ((wrap(a 7), wrap(hash)(wrap(method one)), (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6))))))),hash_length), $\exp(a_2,X_1)$, $\sin(a_1,x_2)$, $\sin(a_2,X_1)$, $\sin(a_1,x_2)$, (wrap(hash((wrap(a⁷), wrap(hash((wrap(method one), $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),$ ((a 8,(id(a 1,a 2),(edhoc kdf(hkdfextract(edhoc kdf($hkdfextract(hash((wrap(a_7), wrap(hash((wrap(method_one), a_7)))))$ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6))))))) $\exp(a^{-7},X^{-1})$, stone, hash((wrap(a_7), wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a_5),a_6))))))),hash_Tength),exp(a_2,X_1)),$ stwo,(id(a 1,a 2),(hash((wrap(a 7),wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a 5), \bar{a} 6)))))))), (a 2, \bar{a} 9))), hash length),$ $(a_9)), ((id(pk(sk_3), exp(g, ltdh_1)), (sign(g, ltdh_1)), (sign(g,$ $(\overline{s}\operatorname{Signa}\overline{t}\operatorname{ure}2,(\operatorname{id}(\operatorname{pk}(\operatorname{sk}\overline{3}),\operatorname{exp}(g,\operatorname{ltdh}\overline{1})),(\operatorname{hash}(\operatorname{sk}\overline{3}),\operatorname{exp}(g,\operatorname{ltdh}\overline{3})))$ (wrap(hash((wrap(a 7), wrap(hash((wrap(method one)), wrap(hash((wwa))), wrap(hash((wwa)), wrap(hash((wwa)), wrap(hash((wwa)) $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),$ ((a 8,(id(a 1,a 2),(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash((wrap(method one), $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))),$ $\exp(a^{7}X 1)$, stone, $hash(wrap(a^{7}X n), wrap(hash(n))$ $(wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),$ $(wrap(a 5), a \overline{6})))))))), hash Tength), exp(a 2, X 1)),$ stwo,(id(a 1,a 2),(hash((wrap(a 7),wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), (wrap(a_5),a_6))))))))))),(a_2,a_9))),hash_length), a_9))),a_2))),(pk(sk_3),(EAD_1,edhoc_kdf(hkdfextract(ēdhoc kdf(hkdfextract(hash((wrap(ā 7), wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a_5),a_6))))))), exp(a_7,X_1)), stone, hash($ (wrap(a 7), wrap(hash((wrap(method one), (wrap(a 4), $(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),hash_length), exp(a_2,X_1)),ssix,(id(pk(sk_3),exp(g,ltdh_1)),$ (hash((wrap(hash((wrap(a 7), wrap(hash((wrap(method one), $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))$ ((a 8,(id(a 1,a 2),(edhoc kdf(hkdfextract(edhoc kdf($hkdfex\overline{t}ract(hash((\overline{w}rap(a 7), \overline{w}rap(hash((\overline{w}rap(method one),$ $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),$ $\exp(a^{7}X 1)$, stone, $hash(wrap(a^{7}), wrap(hash($ (wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), (wrap(a 5),a 6))))))),hash_length),exp(a 2,X 1)), stwo,(id(a 1,a 2),(hash((wrap(a 7),wrap(hash((wrap(method one),(wrap(a $4\bar{)}$,(wrap(exp(g,X 1)), (wrap(a_5),a_6))))))))),(a_2,a_9))),hash_length), a_9))),a_2))),(pk(sk_3),EAD_1))),hash_length))))),

 $srep.(sk_3), EAD_1), pk(sk_3))), hash_Tength), X_1,$

a 7)