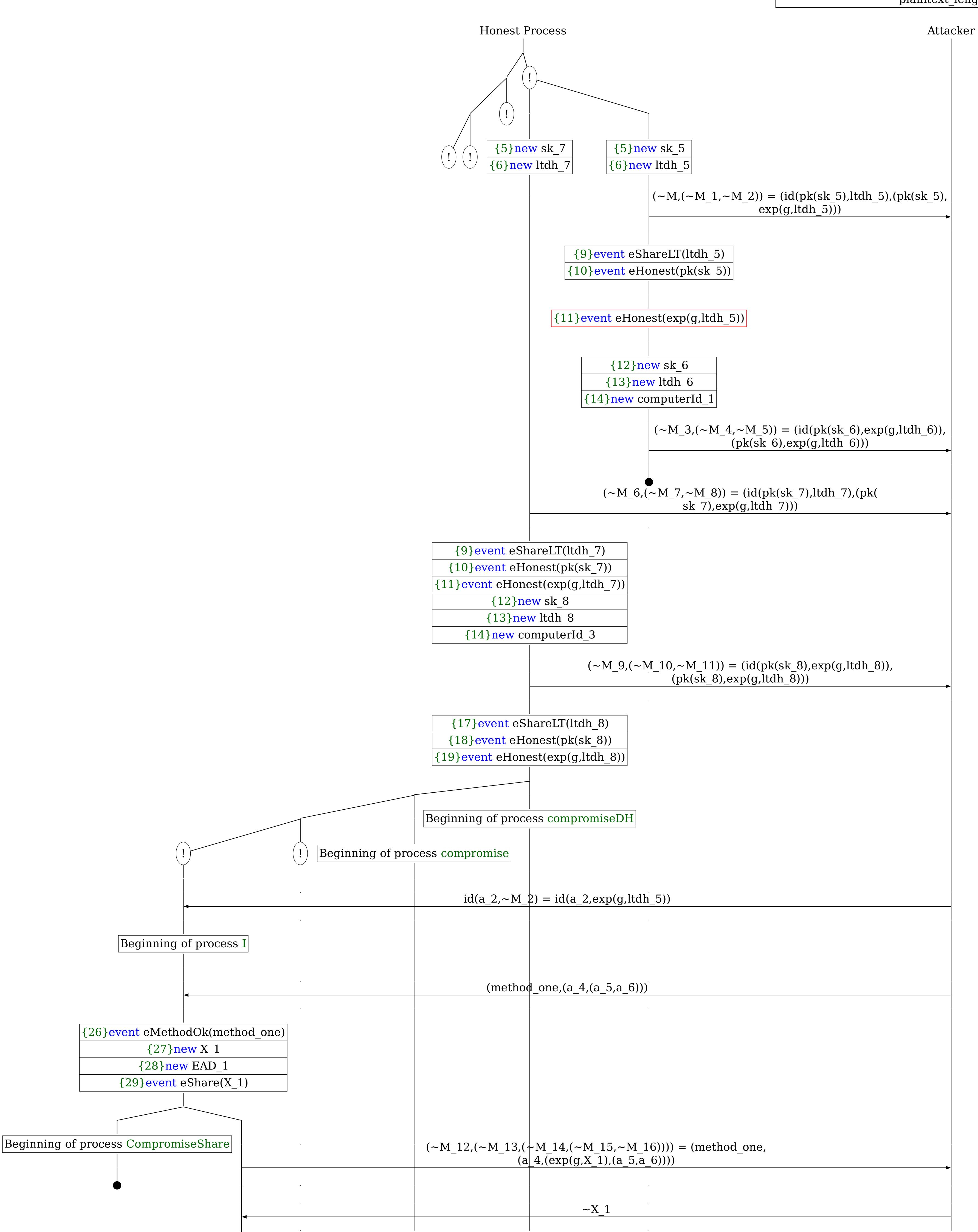
~X_1 = (g,encxor((a_7,(id(a_2,~M_2),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(g),wrap(hash(wrap(method_one),(wrap(a_4),(wrap(~M_14),(wrap(a_5),a_6))))))),~M_14),stone,hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(~M_14),(wrap(a_5),a_6))))))),hash_length),exp(~M_14, get_DH_cred(~M))),stwo,(id(a_2,~M_2),(hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(method_one),(wrap(a_4),(wrap(a_4),(wrap(method_one),(wrap(a_4)

Abbreviations

 $get_DH_cred(\sim M))), stwo, (id(a_2,\sim M_2), (hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(\sim M_14),(wrap(a_5),a_6)))))))), (\sim M_2,a_8))), hash_length), a_8))), edhoc_kdf(hkdfextract(hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(\sim M_14),(wrap(a_5),a_6))))))), \sim M_14), stzero, hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(\sim M_14),(wrap(a_5),a_6)))))))), plaintext_length)))$

(g,encxor((a 7,(id(a 2,exp(g,ltdh 5)),(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(g), wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp($g(X 1), (wrap(a 5), a_6)))))), exp(g(X_1)), stone,$ hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a 4), (wrap(exp(g,X 1)), (wrap(a 5),a 6))))))),hash_length),exp(exp(g,ltdh_5),X_1)),stwo,(id(a_2,exp(g,ltdh_5)),(hash((wrap(g),wrap(hash((wrap(method one), (wrap(a 4), (wrap(exp(g,X 1)), (wrap(exp(g,X 1)))) $a_5),a_6))))))),(exp(g,ltdh_5),a_8))),hash_length),$ a 8))),edhoc kdf(hkdfextract(hash((wrap(g),wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g, X = 1),(wrap(a 5),a 6))))))),exp(g,X 1)),stzero, hash((wrap(g), wrap(hash((wrap(method one), (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))), plaintext length)))



{79}event eDerivedIShared(pk(sk_8),exp(g,X_1))

{83}event eTHIShared(pk(sk_8),hash((wrap(hash(wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),((a_7,(id(a_2,exp(g,Itdh_5)),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),exp(g,X_1)),stone,hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),hash_length),exp(exp(g,ltdh_5),X_1)),stwo,(id(a_2,exp(g,ltdh_5)),(hash((wrap(g),wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),(exp(g,ltdh_5),a_8))),hash_length),a_8))),exp(g,ltdh_5),in_8))),hash_length),a_8))),exp(g,ltdh_5)))))

{93}event eAcceptI(computerId_3,method_one,pk(sk_8),exp(g,ltdh_5),hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(g), wrap(hash((wrap(method_one), (wrap(a_4), $(wrap(exp(g,X_1)), (wrap(a_5), a_6)))))))),$ $\exp(g,X_1)$, stone, hash((wrap(g), wrap(hash((wrap(method_one), (wrap(a_4), (wrap(exp(g,X_1)), (wrap(exp(g,X a_5),a_6)))))))),hash_length),exp(exp(g,ltdh_5), X_1)),hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(g),wrap(hash(wrap(method_one),(wrap(a_4), $(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),exp(g,X_1)),stone,hash((wrap(g),wrap(hash((wrap(method_one),$ (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),
 hash_length),exp(exp(g,Itdh_5),X_1)),edhoc_kdf(
 hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(g), wrap(hash((wrap(method_one),(wrap(a_4),(wrap(exp($g,X_1)$, $(wrap(a_5),a_6))))))), <math>exp(g,X_1)$, stone, hash((wrap(g), wrap(hash((wrap(method_one), (wrap(a 4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))), hash_length),exp(exp(g,ltdh_5),X_1)),sseven,hash($(wrap(hash((wrap(hash((wrap(g), \overline{wrap(hash((wrap(g), \overline{wrap(hash((wrap(f), \overline{wrap(f), \overline{wrap(f), \overline{wrap(f)}})})))}))))))))))))))))))))$ $method_one)$, $(wrap(a_4), (wrap(exp(g,X_1)), (wrap(exp(g,X_1))))$ a 5), a 6))))))), $((a_7, (id(a_2, exp(g, ltdh_5)), exp(g, ltdh_5)))$ (edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash($(wrap(\overline{g}), wrap(hash((wrap(me\overline{t}hod one), (wrap(a 4),$ $(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),exp(g,X_1)),stone,hash((wrap(g),wrap(hash((wrap(method_one),$ (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))), hash_length),exp(exp(g,ltdh_5),X_1)),stwo,(id(a_2,exp(g,ltdh_5)),(hash((wrap(g),wrap(hash((wrap(\overline{m} ethod one), $\overline{(wrap(a_4), (wrap(exp(g,X_1)), (wrap(exp(g,X_1))$ a_5),a_6))))))),(exp(g,ltdh_5),a_8))),hash_length), a $\overline{8}$)), $\overline{\exp}(g, \text{ltdh } 5\bar{)})))), ((id(\overline{pk}(sk 8), \exp(g, \text{ltdh } 8)), exp(g, \text{ltdh } 8)))))))$ (sign((sSignature2,(id(pk(sk_8),exp(g,ltdh_8)), (hash((wrap(hash((wrap(g), wrap(hash((wrap(method_one), (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))), ((a 7,(id(a 2,exp(g,ltdh 5)),(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(g),wrap(hash($(wrap(method_one),(wrap(a_4),(wrap(exp(g,X_1)),$ $(wrap(a_5),a_6))))))), exp(g,X_1)), stone, hash(wrap(g), wrap(hash((wrap(method_one), (wrap(a_4), a_5))))))))))))))))))))))$ $(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),hash_length),$ $\exp(\exp(\hat{g}, \hat{t}dh_5))$, $(id(a_2), \exp(g, \hat{t}dh_5))$, (hash((wrap(g), wrap(hash((wrap(method_one), (wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))), $(exp(g,ltdh_5),a_8)),hash_length),a_8)),exp($ g,ltdh 5)))),(pk(sk 8),(ÉAD 1,edhoc kdf(hkdfextract(edhōc kdf(hkdfextract(hash((wrap(g),wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a_5), \overline{a}_6))))))))), exp(\overline{g}, X_1)), stone, hash($ (wrap(g), wrap(hash((wrap(method one), (wrap(a 4), $(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),hash_length), exp(exp(g,ltdh_5),X_1)),ssix,(id(pk(sk_8),exp($ g,ltdh 8)),(hash(wrap(hash(wrap(g),wrap(hash((wrap(method one),(wrap(a 4),(wrap(exp(g,X 1)),(wrap(a_5),a_6))))))))),((a_7,(id(a_2,exp(g,ltdh_5)), (edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash($(wrap(\overline{g}), wrap(hash((wrap(me\overline{t}hod one), (wrap(a 4),$ $(\overline{wrap}(\exp(g,X 1)),(\overline{wrap}(a 5),a \overline{6})))))),\exp(g,\overline{g})$ $X_1)$, stone, hash((wrap(g), wrap(hash((wrap(method one), (wrap(a_4), (wrap(exp(g, X_1)), (wrap(a_5), a_6))))))), hash_length),exp(exp(g,ltdh_5),X_1)),stwo,(id(a_2,exp(g,ltdh_5)),(hash((wrap(g),wrap(hash((wrap(g method one),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),(exp(g,ltdh_5),a_8))),hash_length), a_8))), $exp(\overline{g}, ltdh_5))), (pk(sk_8), EAD_1)), hash_length))))),$ $(srep,sk_8), EAD_1), pk(sk_8))), hash_length), X_1,$

A trace has been found.