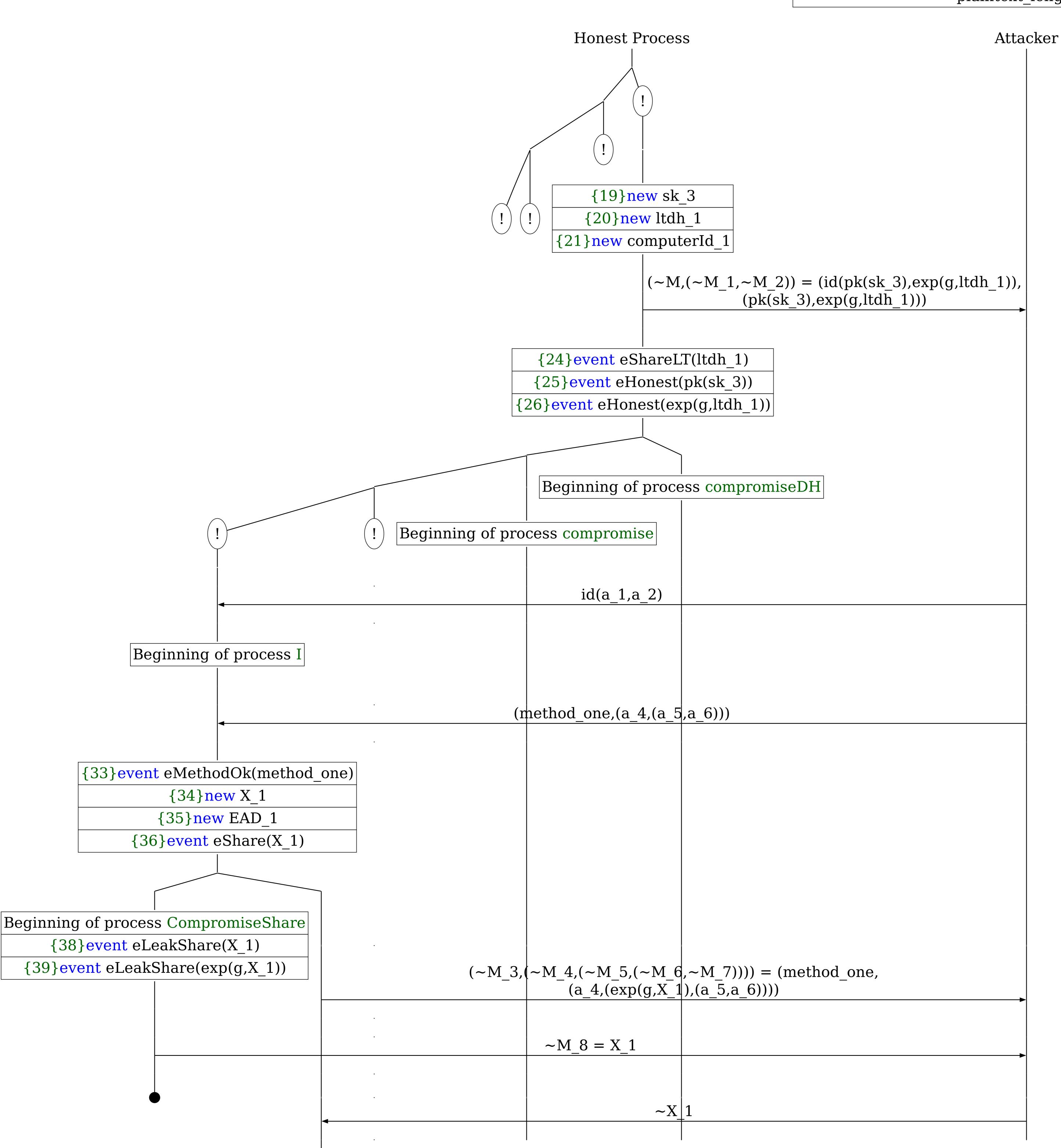
Abbreviations

A trace has been found.



{90}event eDerivedIShared(pk(sk\_3),exp(a\_7,X\_1))

{94}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))))

{104}event eAcceptI(computerId 1,method one,pk( sk 3),a 2,hkdfextract(edhoc kdf(hkdfextract(hash(  $(wrap(a \overline{7}), wrap(hash((wrap(method one), (wrap(a 4),$  $(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))),exp(a_7,X_1)),stone,hash((wrap(a_7),wrap(hash((wrap(method_one),x_1)),stone)))$  $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),$ 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))))))) $\exp(a^{7},X^{1})$ ,  $\operatorname{stone}$ ,  $\operatorname{hash}((\operatorname{wrap}(a^{7}),\operatorname{wrap}(\operatorname{hash}($ (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(a<sup>7</sup>), 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)