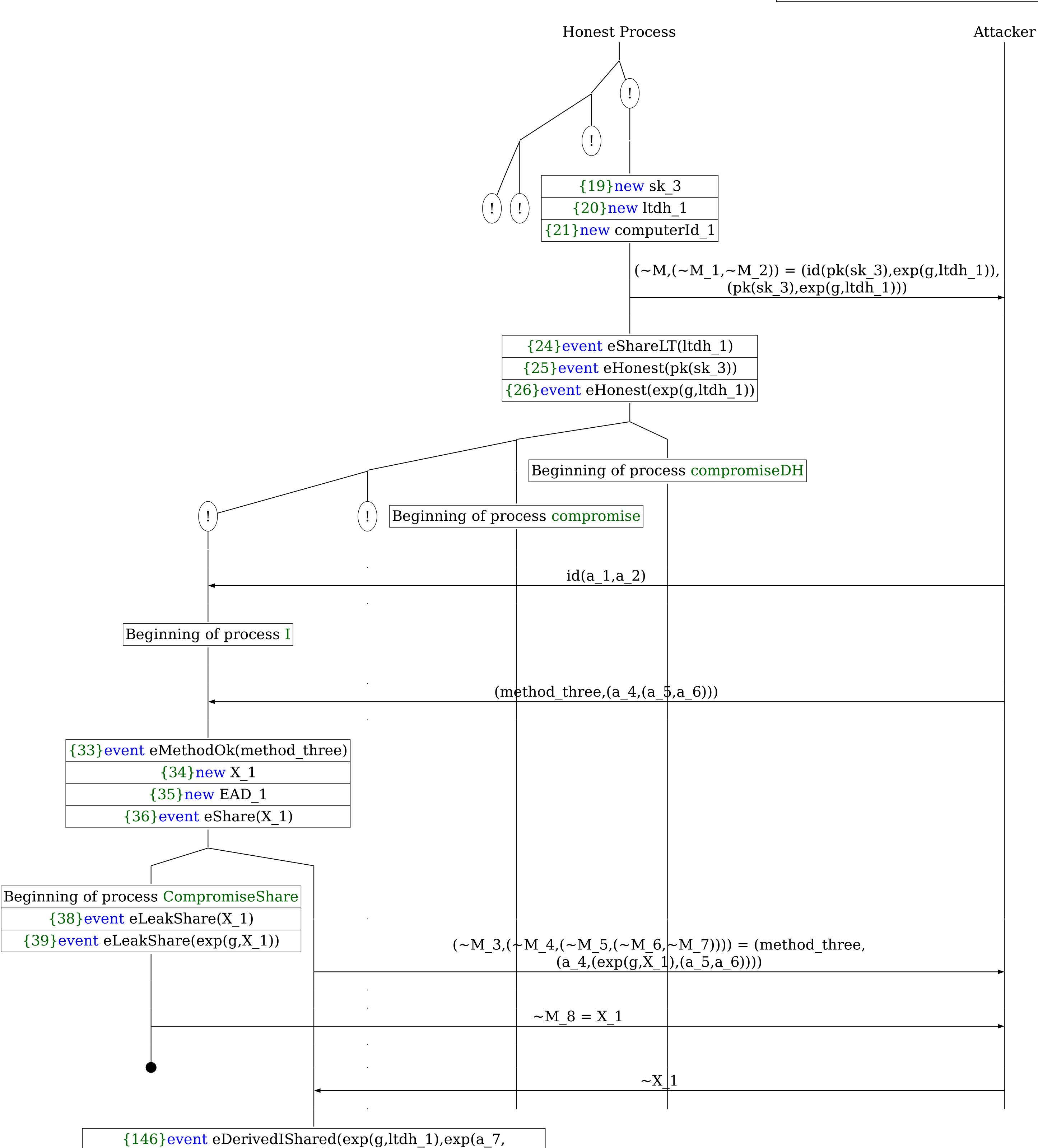
Abbreviations $\sim X_1 = (a_7, encxor((a_8, (id(a_1, a_2), (edhoc_kdf(hkdfextract(a_1, a_2), (edhoc_kdf(hkdfe$

edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6))))))),exp(a_7,~M_8)),stone,hash((wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4), (wrap(~M_5),(wrap(a_5),a_6)))))))),hash_length),exp(a_2,~M_8)),stwo,(id(a_1,a_2),(hash((wrap(a_7), wrap(hash((wrap(method_three),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length),a_9))),edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4),(wrap(~M_5), (wrap(a_5),a_6)))))))),exp(a_7,~M_8)),stzero,hash((wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4),(wrap(a_7),wrap(a_4),(wrap(~M_5), (wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4),(wrap(~M_5),(wrap(a_5),a_6)))))))),plaintext_length)))

(a_7,encxor((a_8,(id(a_1,a_2),(edhoc_kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(a_7),wrap(hash(wrap(method_three),(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_three),(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_three),(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_three),(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_three),(wrap(a_7),wrap(hash((wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),plaintext_length)))

A trace has been found.



{150}event eTHIShared(exp(g,ltdh_1),hash((wrap(hash((wrap(a_7),wrap(hash((wrap(method_three),(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_three),(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_three),(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_three),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))),(a_2,a_9))),hash_length), a 9))),a 2))))

{162} event eAcceptI(computerId 1, method three, exp(g,ltdh_1),a_2,hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a⁷),wrap(hash((wrap(method three), $(wrap(a_4), (wrap(exp(g,X_1)), (wrap(a_5), a_6))))))),$ $\exp(a^{-7}X 1)$, stone, has $h(wrap(a^{-7}X n + b))$, wrap(hash($(wrap(\overline{method three}), (wrap(a 4), (\overline{wrap(exp(g,X 1))}),$ hkdfextract(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract($hash((wrap(a \overline{7}), wrap(hash((wrap(method three)),$ (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 three),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a 5),a^{-}6)))))))),hash length),exp(a^{-}2,X 1)),$ sfive, hash((wrap(hash((wrap(a_7), wrap(hash((wrap($method_three$),($wrap(a_4)$,($wrap(exp(g,X_1))$),($wrap(exp(g,X_1))$)) $[a_5], \overline{a}_6)))))))),(\overline{[a_8],(id(a_1,a_2),(edhoc_kdf(a_1,a_2)),(edhoc_kdf(a_1,a_2)$ hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash((wrap(method three),(wrap(a 4),(wrap($\exp(g,X 1)$, $(wrap(a 5), \bar{a} 6))))))), <math>\exp(a 7,X 1)$, stone, $hash(\overline{w}rap(a_{\overline{7}}), \overline{w}rap(\overline{h}ash(\overline{w}rap(\overline{m}e\overline{t}hod_{\overline{t}}hree))$, $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),$ hash_length), $\exp(a_2, X_1)$), stwo, $(id(a_1, a_2), (a_2, x_1))$ $hash((\overline{w}rap(a 7), \overline{w}rap(ha\overline{s}h((\overline{w}rap(method three)))))$ $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))),$ $(a_2,a_9))$, hash length), \bar{a} 9)), a 2)), \bar{b} ash length), exp(a 7,ltdh 1)),edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a 7),wrap(hash((wrap(method three),(wrap(a 4),(wrap($\exp(g(X 1)), (wrap(a 5), a 6))))))), \exp(a 7, X 1)),$ stone, $hash(\overline{w}rap(a \overline{7}), \overline{w}rap(\overline{h}ash((\overline{w}rap(\overline{m}e\overline{t}hod three)), \overline{u}))$ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))hash length), $exp(a_2,X_1)$, sfive, hash (wrap(hash) (wrap(a 7), wrap(hash((wrap(method three), (wrap(a_4), $(wrap(exp(g,X_1)), (wrap(a_5), a_6)))))))),$ ((a 8, (id(a 1, a 2), (edhōc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash((wrap(method three), $(wrap(a 4),(wrap(ex\overline{p}(g,X 1)),(wrap(a 5),a 6)))))))))$ $\exp(a^{-7},X^{-1})$, stone , $\operatorname{hash}((\operatorname{wrap}(a_{-7}),\operatorname{wrap}(\operatorname{hash}($ $(wrap(\overline{m}eth\overline{o}d three),(wrap(a 4),(\overline{wrap}(exp(g,X 1)),$ $(wrap(a_5),a_6)))))))),hash_length),exp(a_2,X_1)),$ stwo,(id(a 1,a 2),($hash((\overline{w}rap(a 7),wrap(hash(($ wrap(method three),(wrap(a $\overline{4}$),(wrap(exp(g,X 1)), $(wrap(a 5), \bar{a} 6))))))))(a 2, \bar{a} 9))), hash length),$ $(a_9)), (a_2)), (a_8), (a_7), (a_7)$ hash((wrap(hash((wrap(hash((wrap(a 7), wrap(hash($(wrap(method_three),(wrap(a_4),(wrap(exp(g,X_1)),$ (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 three),(wrap(a 4),(wrap($\exp(g,X 1)$, $(wrap(a 5), \bar{a} 6)))))), <math>\exp(\bar{a} 7,X 1)$, stone, $hash(\overline{w}rap(a 7), \overline{w}rap(\overline{h}ash((\overline{w}rap(me\overline{t}hod three)), \overline{w}rap(\overline{h}ash((\overline{w}rap(me\overline{t}hod thr$ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))hash length), $\exp(a^2, \overline{X} 1)$, stwo, $(id(a^2, \overline{X} 2), (id(a^2, \overline{X} 2))$ hash((wrap(a 7), wrap(hash((wrap(method three), (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6))))))),(a 2, a 9)), hash_length, a 9)), a 2))), (id(pk(sk 3),exp(g,ltdh 1)),(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a⁷)), wrap(hash((wrap(method three),(wrap(a 4),(wrap($\exp(g,X 1)$, $(wrap(a 5), \bar{a} 6)))))), <math>\exp(\bar{a} 7,X 1)$, stone, $hash(\overline{w}rap(a \overline{7}), \overline{w}rap(\overline{h}ash((\overline{w}rap(\overline{m}e\overline{t}hod three)), \overline{u}))$ $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6)))))))$ hash length), exp(a 2, X 1)), sfive, hash(wrap(hash((wrap(a 7), wrap(hash((wrap(method three), (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 three), (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))), $\exp(a 7, X 1)$, $\operatorname{stone}_{hash}((\operatorname{wrap}(a 7), \operatorname{wrap}(\operatorname{hash}($ $(wrap(\overline{m}eth\overline{o}d\ three),(wrap(a\ 4),(\overline{wrap}(exp(g,X\ 1)),$ $(wrap(a 5), a \overline{6})))))))), hash length), exp(a 2, X 1)),$ stwo,(id(a 1,a 2),($hash((\overline{w}rap(a 7), \overline{w}rap(hash)($ wrap(method three),(wrap(a $\overline{4}$),(wrap(exp(g,X 1)), $(wrap(a_5), a_6)))))))),(a_2, a_9)),hash_length),$ a 9)), $(\overline{2})$, $(\overline{2})$ $(id(pk(sk_3),exp(g,ltdh_1)),(hash((wrap(hash(($ wrap(a 7), wrap(hash((wrap(method three), (wrap($a^{\overline{4}}$, $\overline{(wrap(exp(g,X 1)), (wrap(a 5), a 6)))))))),$ ((a 8, (id(a 1, a 2), (edhōc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash((wrap(method three), (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 three),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a 5),a \overline{6}))))))),hash length),exp(a 2,X 1)),$ stwo,(id(a_1,a_2),(hash((wrap(a 7),wrap(hash((wrap(method three),(wrap(a_4),(wrap($exp(g,X_1)$),

 $(wrap(a 5), \bar{a} 6)))))))), (a 2, \bar{a} 9))), hash length),$

a \hat{g})), \hat{g} , \hat{g} ,

 \overline{EAD} 1),exp(\overline{g} ,ltdh 1))),hash \overline{length} ,X 1,a 7)