Abbreviations \sim M 3 = exp(g,Y 1) \sim M_4 = encxor((a_1,(id(pk(sk_3),exp(g,ltdh_1)),(edhoc_kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5), $(wrap(a_6),(wrap(a_7),a_8))))))),exp(a_6,Y_1)),$ stone,hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7),a 8))))))),hash length), $\exp(a 6, ltdh 1)), stwo, (id(pk(sk 3), exp(g, ltdh 1)),$ (hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method_one), (wrap(a 5),(wrap(a 6),(wrap(a 7),a 8))))))),(exp(g,ltdh 1),a 2))),hash length),a 2))),edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7), a 8)))))))),exp(a 6,Y 1)),stzero,hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5), (wrap(a 6),(wrap(a 7),a 8))))))),plaintext length)) \sim M 5 = a 1 \sim X 1 = aeadenc((id(a 9,a 10),(a 11,a 12)),a 13,edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(~M 3), wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6), (wrap(~M 3),wrap(hash((wrap(method one),(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),hash_length), $\exp(a 6, \sim M 7))$, $sthree, hash((wrap(hash((wrap(<math>\sim M 3)$), wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6), edhoc kdf(hkdfextract(hash((wrap(~M 3),wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7),a 8))))))), $\exp(a 6,\sim M 6)$),stone,hash((wrap(~M 3),wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6), (wrap(a 7), a 8))))))), hash length), $\exp(a 6, \sim M 7)$), $stwo, (\sim M, (hash((wrap(\sim M 3), wrap($ hash((wrap(method one),(wrap(a 5),(wrap(a 6),(

wrap(a 7), a 8))))))), (~M 2, a 2))), hash length),

a_2))),~M_2))),key_length),edhoc kdf(hkdfextract(

edhoc kdf(hkdfextract(hash((wrap(~M 3),wrap(hash(

(wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(

a 7),a 8))))))), $\exp(a 6,\sim M 6)$),stone,hash((wrap(

~M 3),wrap(hash((wrap(method one),(wrap(a 5),(

wrap(a 6),(wrap(a 7),a 8))))))),hash length),

 $\exp(a 6, \sim M 7))$, sfour, $hash((wrap(hash((wrap(\sim M 3), \sim M 5))))$

wrap(hash((wrap(method one),(wrap(a 5),(wrap(a 6),

(wrap(a 7),a 8)))))))))))((a 1,(~M,(edhoc kdf(hkdfextract(

edhoc kdf(hkdfextract(hash((wrap(~M 3),wrap(hash(

(wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(

a 7),a 8))))))), $\exp(a 6,\sim M 6)$),stone,hash((wrap(

~M 3),wrap(hash((wrap(method one),(wrap(a 5),(

wrap(a 6), (wrap(a 7), a 8))))))), hash length),

 $\exp(a 6,\sim M 7))$, $stwo,(\sim M,(hash((wrap(\sim M 3),wrap($

hash((wrap(method one),(wrap(a 5),(wrap(a 6),(

wrap(a 7), a 8))))))), (~M 2, a 2))), hash length),

a 2))), \sim M 2))),iv length))

= aeadenc((id(a 9,a 10),

(a_11,a_12)),a_13,edhoc_kdf(hkdfextract(edhoc kdf(

hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((

wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7),

a 8))))))))exp(a 6,Y 1)),stone,hash((wrap(exp(

g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),

(wrap(a 6), (wrap(a 7), a 8))))))), hash length),

exp(a 6,ltdh 1)),sthree,hash((wrap(hash((wrap(

exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(

a 5),(wrap(a 6),(wrap(a 7),a 8))))))),((a 1,

(id(pk(sk 3),exp(g,ltdh 1)),(edhoc kdf(hkdfextract(

edhoc kdf(hkdfextract(hash((wrap(exp(g,Y_1)),wrap(

hash((wrap(method one),(wrap(a 5),(wrap(a 6),(

wrap(a 7), a 8))))))), exp(a 6, Y 1)), stone, hash(

(wrap(exp(g,Y 1)), wrap(hash((wrap(method one),

 $(wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))), hash length),$

 $\exp(a 6, ltdh 1)), stwo, (id(pk(sk 3), exp(g, ltdh 1)),$

(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),

(wrap(a 5),(wrap(a 6),(wrap(a 7),a 8))))))),(

 $\exp(g, ltdh 1), a 2)), hash length), a 2)), \exp(g, ltdh 1), a 2)), hash length), a 2)), exp(g, ltdh 1), a 2))$

ltdh 1)))),key length),edhoc kdf(hkdfextract(edhoc kdf(

hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((

wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7),

a 8))))))))exp(a 6,Y 1)),stone,hash((wrap(exp(

g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),

(wrap(a 6), (wrap(a 7), a 8))))))), hash length),

exp(a 6,ltdh 1)),sfour,hash((wrap(hash((wrap(exp(

g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),

(wrap(a_6),(wrap(a 7),a 8)))))))),((a 1,(id(pk(

sk 3),exp(g,ltdh 1)),(edhoc kdf(hkdfextract(edhoc kdf(

hkdfextract(hash((wrap(exp(g,Y 1)),wrap(hash((

wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7),

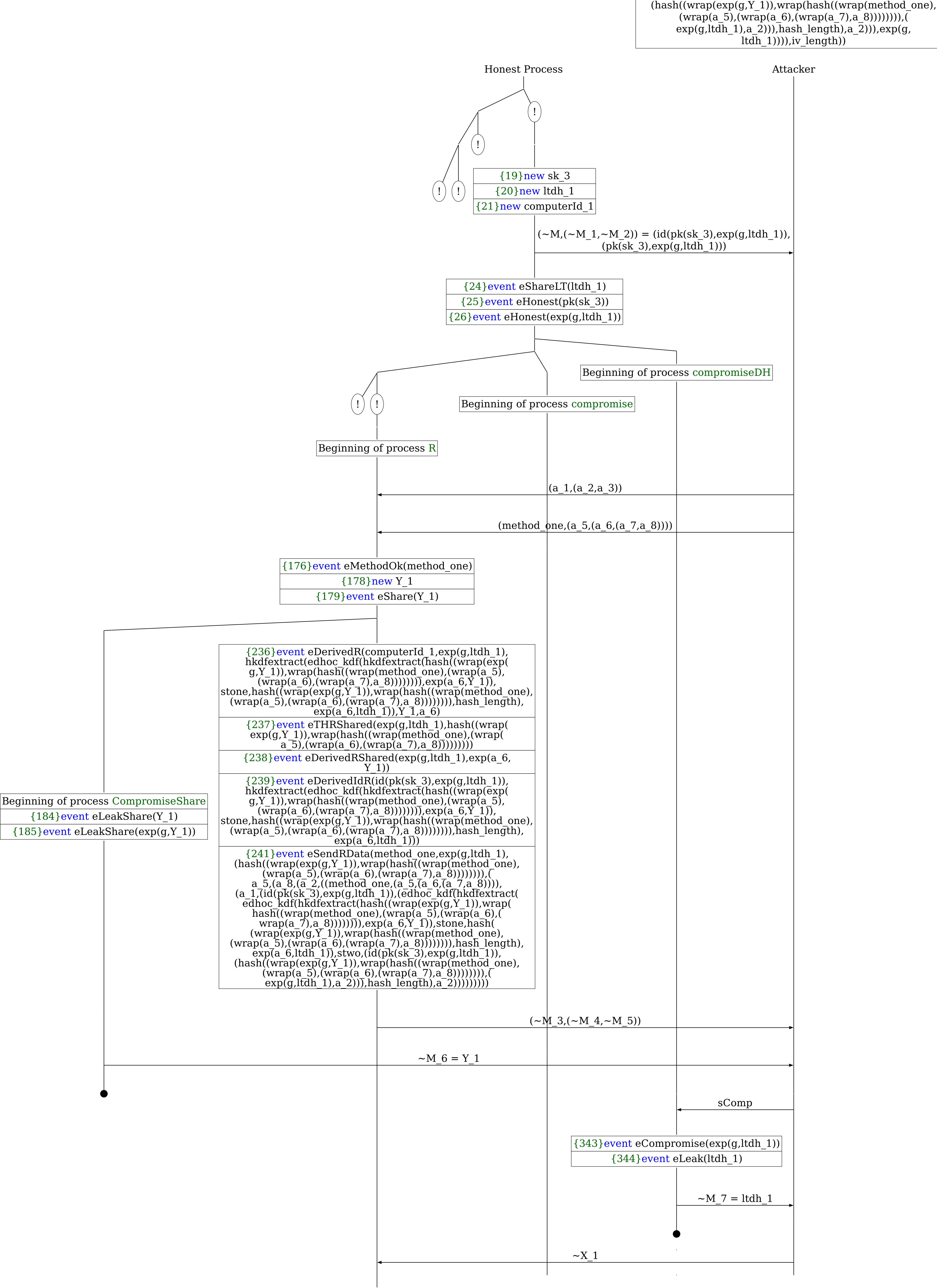
a 8))))))))exp(a 6,Y 1)),stone,hash((wrap(exp(

g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5),

(wrap(a 6), (wrap(a 7), a 8)))))))), hash length),

 $\exp(a 6, ltdh 1)), stwo, (id(pk(sk 3), exp(g, ltdh 1)),$

A trace has been found.



 $\{253\}$ event eVerified(a 11,e1(a 11),e3(a 11),(sSignature2, $(id(a_9,a_10),(hash(wrap(hash(wrap(exp(g,Y_1))),$ wrap(hash(wrap(method one),(wrap(a 5),(wrap(a 6), $(wrap(a_7),a_8))))))),((a_1,(id(pk(sk_3),exp(sk_3))))))))$ g,ltdh 1)),(edhoc kdf(hkdfextract(edhoc_kdf(hkdfextract(hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method one),(wrap(a 5), (wrap(a 6), (wrap(a 7), a 8))))))), exp(a_6,Y_1)), stone, hash ((wrap($\exp(g,Y_1)$), wrap(hash((wrap(method_one),(wrap(a_5),(wrap(a_6),(wrap(a $\overline{7}$),a 8)))))))),hash length),exp(a <math>6, $\overline{1}$ tdh 1)), $stw\overline{o}$,($id(\overline{p}k(sk_3),exp(\overline{g},ltdh_1))$,($hash((wra\overline{p}(exp(\overline{g},ltdh_1)))$),($hash((wra\overline{p}(exp(\overline{g},ltdh_1)))$) g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5), $(\overline{w}rap(a_6),(\overline{w}rap(a_7),a_8)))))),(exp(g,ltdh_1),$ $(a_2)), hash_length, a_2)), exp(g, ltdh_1))), (a_9, a_1)), a_2))$ (a 12,edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)), wrap(hash((wrap(method one),(wrap(a 5), (wrap(a 6), (wrap(a 7), a 8)))))), exp(a $6,Y_1)$, stone, hash ((wrap(exp(g,Y_1)), wrap(hash($(\overline{wrap}(method_one),(\overline{wrap}(a_5),(\overline{wrap}(a_6),(\overline{wrap}(a_6))))$ a $\overline{7}$),a $8)))))))),hash length),exp(a <math>\overline{6}$, $\overline{1}$ tdh 1)), ssix,(id(a 9,a 10),(hash((wrap(hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5), (wrap(a_6),(wrap(a_7),a_8)))))))),((a_1,(id(pk(sk_3),exp(g,ltdh_1)),(edhoc_kdf(hkdfextract(edhoc_kdf($hkdfextract(\overline{h}ash((wrap(exp(g,Y 1)),wrap(hash(($ wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7), $[a, 8)))))), exp(a_6, Y_1)), stone, hash((wrap(exp($ $g,Y^{-}1)$, wrap(hash((wrap(method one),(wrap(a 5), $(\overline{w}rap(a 6),(wrap(a 7),a 8)))))),hash length),$ $\exp(a^{-}6,l\bar{t}dh 1)),\bar{s}tw\bar{o},(id(\bar{p}k(sk 3),exp(\bar{g},ltdh 1)),\bar{s}tw\bar{o})$ (hash((wrap(exp(g,Y 1)),wrap(hash((wrap(method one),(wrap(a 5), (wrap(a 6), (wrap(a 7), a 8))))))), ($\exp(g, ltdh_1), a_2)), hash_length), a_2)), exp(g, ltdh_1), a_2)), exp(g, ltdh_1), a_2)), exp(g, ltdh_1), a_2)), a_2)$ ltdh 1)))),(a_9,a_12))),hash_length)))))),a_9, sigtrue)

{256}event eAcceptR(computerId 1,method one,a 9, exp(g,ltdh 1),hkdfextract(edhoc kdf(hkdfextract($hash(wrap(exp(g,Y_1)),wrap(hash(wrap(method_one),$ $(wrap(\bar{a} \ 5), (wrap(a \ 6), (wrap(a \ 7), a \ \bar{8}))))))), exp($ a $6,Y^{1}$), stone, hash ((wrap(exp(g,Y $\overline{1}$)), wrap(hash($(\overline{w}, \overline{q})$ (wrap(a 5), $(\overline{w}, \overline{q})$), $(\overline{w}, \overline{q})$ a $\overline{7}$),a $8)))))))),hash length),exp(a <math>\overline{6}$, $\overline{1}$ tdh $\overline{1}$)), edhoc kdf(hkdfextract(edhoc kdf(hkdfextract(hash((wrap(exp(g,Y 1)), wrap(hash(wrap(method one), $(wrap(a_5), (wrap(a_6), (wrap(a_7), a_8)))))), exp(a_7)$ a 6,Y 1)), stone, hash (wrap(exp(g,Y_1)), wrap(hash($(\overline{w}, \overline{q})$ (wrap(a 5), $(\overline{w}, \overline{q})$), $(\overline{w}, \overline{q})$ a 7), a 8))))))), hásh_length), exp(a_6, ltdh_1)), sseven, hash((wrap(hash((wrap(hash((wrap(exp(g, Y 1)), wrap(hash((wrap(method one), (wrap(a 5), ($\overline{\text{wrap}}(a^{-1}6),(\overline{\text{wrap}}(a^{-1}7),a^{-1}8))))),((a^{-1}1,(\overline{\text{id}}(\overline{\text{pk}}))))))$ sk 3),exp(g, Ttdh 1)),(edhoc kdf(hkdfextract(edhoc kdf($hkdfextract(\overline{h}ash((wrap(exp(g,Y_1)),wrap(hash(($ wrap(method one),(wrap(a 5),(wrap(a 6),(wrap(a 7), [a, 8)))))), exp(a, 6, Y, 1)), stone, hash (wrap(exp(g,Y^{-1}), wrap(hash((wrap(method one),(wrap(a 5), $(\overline{w}rap(a 6), (wrap(a 7), a 8))))))), hash length),$ $\exp(a_6, l\bar{t}dh_1)$), $stw\bar{o}$, $(id(\bar{p}k(sk_3), \exp(\bar{g}, ltdh_1))$, (hash((wrap(exp(g,Y_1)),wrap(hash((wrap(method_one), (wrap(a_5),(wrap(a_6),(wrap(a_7),a_8))))))),(exp(g,ltdh_1),a_2))),hash_length),a_2))),exp(g, ltdh_1)))),((id(a_9,a_10),(a_11,a_12)),a_9))), hash_length),Y_1,a_6)