**Abbreviations** 

~M\_19 = senc(secretB,h2(exp(exp(g,eadd(x\_1,eadd(skA\_1,emul(s\_1,h1(idA,exp(g,skA\_1)))))),eadd(eadd(skB\_1,emul(h1(idB,exp(g,skB\_1)),s\_1)),y\_3)),exp(exp(g,x\_1),y\_3)))

~M\_20 = senc(secretA,h2(exp(exp(g,eadd(y\_3,eadd(skB\_1,emul(s\_1,h1(idB,exp(g,skB\_1))))))),eadd(eadd(skA\_1,emul(h1(idA,exp(g,skA\_1)),s\_1)),x\_1)),exp(exp(g,y\_3),x\_1)))

A trace has been found.

