Abbreviations
~X_1 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),~M_4),prck),concat(a_3,zero)) = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),p256(gen,exp_D_1)),prck),concat(a_3,zero))
~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),p256(gen,exp_D_1)),prck),concat(rand_dev_2,zero))
~X_2 = AES_CCM(a_4,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(~M,~M_1),~M_2),gen),~M_4)),a_3),~M_6)),~M_4),prsn)) = AES_CCM(a_4,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk),AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))
~M_7 = AES_CCM(p_complete,AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsk),AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),a_3),rand_dev_2)),p256(gen,exp_D_1)),prsn))

A trace has been found.