Abbreviations
~X_1 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,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))

A trace has been found.