A trace has been found.

| Abbreviations |
| --- |
| ~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),a_2)),p256(a_2,exp_P_1)),prck),concat(rand_prov_2,auth_val_3)) |