A trace has been found.

| Abbreviations |
| --- |
| ~M = AES_enc((rand2,(seed,rand2)),derive_key(encryption_key, privacy_const),privacyIV) |
| ~M_1 = Mode_E2E |
| ~M_2 = AES_enc((AES_enc((rand2,(seed,rand2)),derive_key( encryption_key,privacy_const),privacyIV),Mode_E2E), derive_key(encryption_key,signature_const),privacyIV) |
| ~M_3 = adv |
| ~M_4 = AES_enc((rand2_2,(seed,rand2_2)),derive_key( encryption_key,privacy_const),privacyIV) |
| ~M_5 = Mode_E2E |
| ~M_6 = AES_enc((AES_enc((rand2_2,(seed,rand2_2)), derive_key(encryption_key,privacy_const),privacyIV), Mode_E2E),derive_key(encryption_key,signature_const), privacyIV) |
| ~M_7 = adv |