Abbreviations
~X_1 = (derive_encryption_key(Curve25519(Curve25519(gen, derive_prikey_from_sn(serial_number)),pri_c_1), rand_3),Curve25519(gen,pri_c_1))
~M_3 = AES_enc(smartthings,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),bleAuthentication), n1_2)
~X_2 = AES_enc(serial_number,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2) = AES_enc(serial_number,derive_key(derive_encryption_key(Curve25519(Curve25519(gen, pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n1_2),n1_2)
~X_3 = (AES_dec(AES_enc(serial_number,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),n1_2),n1_2),derive_key(derive_encryption_key(Curve25519(Curve25519(gen, derive_prikey_from_sn(serial_number)),pri_c_1), rand_3),n1_2),n1_2),derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)), pri_c_1),rand_3))
~M_4 = AES_enc(privacy_iv_5,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),n1_2),n1_2)
~M_5 = AES_enc(privacy_seed_5,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),n1_2),n1_2)
~M_6 = AES_enc(poolsize,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),n1_2),n1_2)
~M_7 = AES_enc(time_sync_3,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),n1_2),n1_2)
~X_4 = AES_enc(smartthings,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),bleAuthentication),~M_9) = AES_enc(smartthings, derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),bleAuthentication),n2_2)
~M_10 = AES_enc(smartthings,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),bleAuthentication),a)
~M_11 = AES_enc(serial_number,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),n2_2),n2_2)
~X_5 = (AES_enc(AES_dec(~M_4,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2),derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_9),~M_9),AES_enc(AES_dec(~M_5,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)),~M),~M_2),~M_2),derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_9),~M_9),AES_enc(poolsize,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_9),~M_9),a_1) = (AES_enc(privacy_iv_5,derive_key(derive_encryption_key(Curve25519(Curve25519(gen, pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n2_2),n2_2),AES_enc(privacy_seed_5,derive_key(derive_encryption_key(Curve25519(Curve25519(gen, pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n2_2),n2_2),AES_enc(poolsize,derive_key(derive_encryption_key(Curve25519(Curve25519(gen, pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n2_2),n2_2),a_1)
~X_6 = get_id(derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize)
~X_7 = get_id(derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize)
~M_12 = SHA256(concat(get_id(derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize),a_2))
~X_8 = SHA256(concat(get_id(derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),privacy),AES_dec(~M_4,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2),AES_dec(~M_5,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2),poolsize),~M_13)) = SHA256(concat(get_id(derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize),salt2_2))

A trace has been found.