

secp256k1_mpt_prove
_same_plaintext



generate_random_scalar