

secp256k1_mpt_prove
_equality_shared_r



generate_random_scalar