

secp256k1_mpt_pok_sk
_prove



generate_random_scalar