

secp256k1_xonly_pubkey
_tweak_add



memset