

secp256k1_ec_pubkey
_tweak_mul



memset