

secp256k1\_ec\_pubkey  
\_tweak\_mul



memset