

derive\_ipa\_round\_challenge

secp256k1\_mpt\_scalar  
\_reduce32