

secp256k1\_bulletproof  
\_prove\_agg

secp256k1\_bulletproof  
\_verify\_agg

derive\_ipa\_binding  
\_challenge

