

size\_t



num\_bits  
s

libff::Fp\_model< n,  
modulus >