

size_t

num_bits
s

libff::Fp_model< edwards
_q_limbs, edwards_modulus_q >

T
X
Y
Z

libff::extended_edwards
_G1_projective