

size_t

num_bits
s

libff::Fp_model< edwards
_q_limbs, edwards_modulus_q >

P_XY
P_XZ
P_ZZplusYZ

libff::edwards_at
_G1_precomp