

Appendix C

Functions used in Performance testing

C.1 Large Integers

Table Large Integer Functions

Multiplication Function	
CLN	Operator *
CryptoPP	Integer::Times
GMP	mpz_mul
LiDIA	multiply
MIRACL	multiply
NTL	mul
OpenSSL	BN_mul
PIOLOGIE	Operator *
Modular Exponential	
CLN	expt
CryptoPP	a_exp_b_mod_c
GMP	mpz_powm_ui (unsigned long), mpz_powm
LiDIA	power_mod
MIRACL	powmod
NTL	PowerMod
OpenSSL	BN_mod_exp
PIOLOGIE	pow
GCD Functions	
CLN	gcd
CryptoPP	Integer::Gcd
GMP	mpz_gcd
LiDIA	gcd
MIRACL	egcd
NTL	GCD
OpenSSL	BN_gcd
PIOLOGIE	gcd
xGCD Functions	
CLN	cl_modint_ring ::recip
CryptoPP	Integer::InverseMod
GMP	mpz_invert
LiDIA	xgcd_left
MIRACL	xgcd
NTL	InvMod
OpenSSL	BN_mod_inverse
PIOLOGIE	inverse

C.2 EC Points

Table EC Functions

Addition		
Library	EC2	ECP
CryptoPP	EC2N::Add	ECP::Add
LiDIA	add	multiply
MIRACL	ecurve2_add	ecurve2_mult
OpenSSL	EC_POINT_add	EC_POINT_mul
Scalar Multiplication		
Library	EC2	ECP
CryptoPP	EC2N::Multiply	ECP::Multiply
LiDIA	add	multiply
MIRACL	ecurve_add	ecurve_mult

C.3 Primality Testing Functions

Table Primality testing Functions

Primality Functions	
CLN	isprobprime
CryptoPP	IsPrime
GMP	mpz_probab_prime_p
LiDIA	is_prime
MIRACL	isprime
NTL	ProbPrime
OpenSSL	BN_is_prime
PIOLOGIE	isprime
