AMCL

Generated by Doxygen 1.8.13

Contents

Chapter 1

Apache Milagro Crypto Library (AMCL)

AMCL is a standards compliant C cryptographic library with no external dependencies, specifically designed to support the Internet of Things (IoT).

AMCL is provided in *C* language but includes a `Python` wrapper.for some components as an aid for development work.

1.1 Project page

The official project page is hosted at `Apache Milagro (incubating)`

1.2 License

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to you under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

`http://www.apache.org/licenses/LICENSE-2.0`

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

1.3 Platforms

The software can be compiled and installed for these operating systems;

- Linux
- Windows
- Mac OS

1.4 Downloads

The source code is available from here;

git clone `https://github.com/milagro-crypto/milagro-crypto-c`

1.5 Installation

There are instructions for building for Linux, Mac OS and Windows.

Chapter 2

Linux

Software dependencies

CMake is required to build the library and can usually be installed from the operating system package manager.

- sudo apt-get install cmake

If not, then you can download it from www.cmake.org

In order to use the Python language wrapper install `Python`

The C Foreign Function Interface for Python `CFFI` module is also required if you wish to use the Python module.

- sudo pip install cffi

In order to build the documentation `doxygen` is required.

Quick Start

A Makefile is present at the project root that reads the options defined in config.mk. Change these options and then type `make` to build and test the library.

If `docker` is installed then type `make dbuild` to build and test the library in a docker container.

Manual build

The default build is for 64 bit machines, Elliptic curve BN254CX and curve type Weierstrass

1. mkdir target/build
2. cd target/build
3. cmake -D CMAKE_INSTALL_PREFIX=/opt/amcl ../..
4. export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:./
5. make
6. make test
7. make doc
8. sudo make install

The build can be configured using by setting flags on the command line i.e.

1. cmake -D CMAKE_INSTALL_PREFIX=/opt/amcl -D WORD_LENGTH=32 ../..

list available CMake options

1. cmake -LH

Uninstall software

- sudo make uninstall

Building an installer

After having built the libraries you can build a binary installer and a source distribution by running this command

- make package

Chapter 3

Mac OS

Software dependencies

Install Homebrew

- ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"

Install cmake

- brew install cmake

In order to use the Python language wrapper install Python

The C Foreign Function Interface for Python CFFI module is also required if you wish to use the Python module.

- brew install pkg-config libffi
- sudo pip install cffi

In order to build the documentation doxygen is required.

- brew install doxygen

Build Instructions

The default build is for 64 bit machines, Elliptic curve BN254CX and curve type Weierstrass

1. mkdir -p target/build
2. cd target/build
3. cmake ../..
4. make
5. make test
6. make doc
7. sudo make install

The build can be configured using by setting flags on the command line i.e.

1. cmake -DWORD_LENGTH=32 ../..

Uninstall software

- sudo make uninstall

Chapter 4

Windows

Software dependencies

Minimalist GNU for Windows MinGW provides the tool set used to build the library and should be installed. When the MinGW installer starts select the mingw32-base and mingw32-gcc-g++ components. From the menu select "Installation" -> "Apply Changes", then click "Apply". Finally add C:\MinGW\bin to the PATH variable.

CMake is required to build the library and can be downloaded from www.cmake.org

In order to use the Python language wrapper install Python

The C Foreign Function Interface for Python CFFI module is also required, if you wish to use the Python module.

- pip install cffi

In order to build the documentation doxygen is required.

Build Instructions

Start a command prompt as an administrator

The default build is for 64 bit machines, Elliptic curve BN254CX and curve type Weierstrass

1. mkdir target\build
2. cd target\build
3. cmake -G "MinGW Makefiles" -D WORD_SIZE=64 ..\..
4. mingw32-make
5. mingw32-make test
6. mingw32-make doc
7. mingw32-make install

Post install append the PATH system variable to point to the install ./lib.

My Computer -> Properties -> Advanced > Environment Variables

The build can be configured using by setting flags on the command line i.e.

1. cmake -G "MinGW Makefiles" -D WORD_SIZE=64 -D BUILD_PYTHON=on ..\..

Uninstall software

- mingw32-make uninstall

Building an installer

After having built the libraries you can build a Windows installer using this command

- sudo mingw32-make package

In order for this to work `NSIS` has to have been installed

Chapter 5

Data Structure Index

5.1 Data Structures

Here are the data structures with brief descriptions:

Chapter 6

File Index

6.1 File List

Here is a list of all documented files with brief descriptions:

Chapter 7

Data Structure Documentation

7.1 amcl_aes Struct Reference

AES instance.

```
#include <amcl.h>
```

Data Fields

- int Nk
- int Nr
- int mode
- unsign32 fkey [60]
- unsign32 rkey [60]
- char f [16]

7.1.1 Field Documentation

7.1.1.1 f

```
char amcl_aes::f[16]
```

buffer for chaining vector

7.1.1.2 fkey

```
unsign32 amcl_aes::fkey[60]
```

subkeys for encrypton

7.1.1.3 mode

```
int amcl_aes::mode
```

AES mode of operation

7.1.1.4 Nk

```
int amcl_aes::Nk
```

AES Key Length

7.1.1.5 Nr

```
int amcl_aes::Nr
```

AES Number of rounds

7.1.1.6 rkey

```
unsign32 amcl_aes::rkey[60]
```

subkeys for decrypton

The documentation for this struct was generated from the following file:

- amcl.h

7.2 csprng Struct Reference

Cryptographically secure pseudo-random number generator instance.

```
#include <amcl.h>
```

Data Fields

- unsign32 ira [NK]
- int rndptr
- unsign32 borrow
- int pool_ptr
- char pool [32]

7.2.1 Field Documentation

7.2.1.1 borrow

```
unsign32 csprng::borrow
```

borrow as a result of subtraction

7.2.1.2 ira

```
unsign32 csprng::ira[NK]
```

random number array

7.2.1.3 pool

```
char csprng::pool[32]
```

random pool

7.2.1.4 pool_ptr

```
int csprng::pool_ptr
```

pointer into random pool

7.2.1.5 rndptr

```
int csprng::rndptr
```

pointer into array

The documentation for this struct was generated from the following file:

- amcl.h

7.3 ECP2_BLS381 Struct Reference

ECP2 Structure - Elliptic Curve Point over quadratic extension field.

```
#include <ecp2_BLS381.h>
```

Data Fields

- FP2_BLS381 x
- FP2_BLS381 y
- FP2_BLS381 z

7.3.1 Field Documentation

7.3.1.1 x

`FP2_BLS381 ECP2_BLS381::x`

x-coordinate of point

7.3.1.2 y

`FP2_BLS381 ECP2_BLS381::y`

y-coordinate of point

7.3.1.3 z

`FP2_BLS381 ECP2_BLS381::z`

z-coordinate of point

The documentation for this struct was generated from the following file:

- ecp2_BLS381.h

7.4 ECP_BLS381 Struct Reference

ECP structure - Elliptic Curve Point over base field.

```
#include <ecp_BLS381.h>
```

Data Fields

- FP_BLS381 x
- FP_BLS381 y
- FP_BLS381 z

7.4.1 Field Documentation

7.4.1.1 x

`FP_BLS381 ECP_BLS381::x`

x-coordinate of point

7.4.1.2 y

`FP_BLS381 ECP_BLS381::y`

y-coordinate of point. Not needed for Montgomery representation

7.4.1.3 z

`FP_BLS381 ECP_BLS381::z`

z-coordinate of point

The documentation for this struct was generated from the following file:

- ecp_BLS381.h

7.5 FP12_BLS381 Struct Reference

FP12 Structure - towered over three FP4.

`#include <fp12_BLS381.h>`

Data Fields

- FP4_BLS381 a
- FP4_BLS381 b
- FP4_BLS381 c
- int type

7.5.1 Field Documentation

7.5.1.1 a

`FP4_BLS381 FP12_BLS381::a`

first part of FP12

7.5.1.2 b

`FP4_BLS381 FP12_BLS381::b`

second part of FP12

7.5.1.3 c

`FP4_BLS381 FP12_BLS381::c`

third part of FP12

7.5.1.4 type

`int FP12_BLS381::type`

Type

The documentation for this struct was generated from the following file:

- fp12_BLS381.h

7.6 FP2_BLS381 Struct Reference

FP2 Structure - quadratic extension field.

`#include <fp2_BLS381.h>`

Data Fields

- FP_BLS381 a
- FP_BLS381 b

7.6.1 Field Documentation

7.6.1.1 a

`FP_BLS381 FP2_BLS381::a`

real part of FP2

7.6.1.2 b

`FP_BLS381 FP2_BLS381::b`

imaginary part of FP2

The documentation for this struct was generated from the following file:

- fp2_BLS381.h

7.7 FP4_BLS381 Struct Reference

FP4 Structure - towered over two FP2.

`#include <fp4_BLS381.h>`

Data Fields

- FP2_BLS381 a
- FP2_BLS381 b

7.7.1 Field Documentation

7.7.1.1 a

`FP2_BLS381 FP4_BLS381::a`

real part of FP4

7.7.1.2 b

`FP2_BLS381 FP4_BLS381::b`

imaginary part of FP4

The documentation for this struct was generated from the following file:

- fp4_BLS381.h

7.8 FP_BLS381 Struct Reference

FP Structure - quadratic extension field.

`#include <fp_BLS381.h>`

Data Fields

- BIG_384_58 g
- sign32 XES

7.8.1 Field Documentation

7.8.1.1 g

```
BIG_384_58 FP_BLS381::g
```

Big representation of field element

7.8.1.2 XES

```
sign32 FP_BLS381::XES
```

Excess

The documentation for this struct was generated from the following file:

- fp_BLS381.h

7.9 gcm Struct Reference

GCM mode instance, using AES internally.

```
#include <amcl.h>
```

Data Fields

- unsign32 table [128][4]
- uchar stateX [16]
- uchar Y_0 [16]
- unsign32 lenA [2]
- unsign32 lenC [2]
- int status
- amcl_aes a

7.9.1 Field Documentation

7.9.1.1 a

`amcl_aes gcm::a`

Internal Instance of AMCL_AES cipher

7.9.1.2 lenA

`unsign32 gcm::lenA[2]`

GCM 64-bit length of header

7.9.1.3 lenC

`unsign32 gcm::lenC[2]`

GCM 64-bit length of ciphertext

7.9.1.4 stateX

`uchar gcm::stateX[16]`

GCM Internal State

7.9.1.5 status

`int gcm::status`

GCM Status

7.9.1.6 table

`unsign32 gcm::table[128][4]`

2k byte table

7.9.1.7 Y_0

`uchar gcm::Y_0[16]`

GCM Internal State

The documentation for this struct was generated from the following file:

- amcl.h

7.10 hash256 Struct Reference

SHA256 hash function instance.

```
#include <amcl.h>
```

Data Fields

- unsign32 length [2]
- unsign32 h [8]
- unsign32 w [80]
- int hlen

7.10.1 Field Documentation

7.10.1.1 h

```
unsign32 hash256::h[8]
```

Internal state

7.10.1.2 hlen

```
int hash256::hlen
```

Hash length in bytes

7.10.1.3 length

```
unsign32 hash256::length[2]
```

64-bit input length

7.10.1.4 w

```
unsign32 hash256::w[80]
```

Internal state

The documentation for this struct was generated from the following file:

- amcl.h

7.11 hash512 Struct Reference

SHA384-512 hash function instance.

```
#include <amcl.h>
```

Data Fields

- unsign64 length [2]
- unsign64 h [8]
- unsign64 w [80]
- int hlen

7.11.1 Field Documentation

7.11.1.1 h

```
unsign64 hash512::h[8]
```

Internal state

7.11.1.2 hlen

```
int hash512::hlen
```

Hash length in bytes

7.11.1.3 length

```
unsign64 hash512::length[2]
```

64-bit input length

7.11.1.4 w

```
unsign64 hash512::w[80]
```

Internal state

The documentation for this struct was generated from the following file:

- amcl.h

7.12 octet Struct Reference

Portable representation of a big positive number.

```
#include <amcl.h>
```

Data Fields

- int len
- int max
- char * val

7.12.1 Field Documentation

7.12.1.1 len

```
int octet::len
```

length in bytes

7.12.1.2 max

```
int octet::max
```

max length allowed - enforce truncation

7.12.1.3 val

```
char* octet::val
```

byte array

The documentation for this struct was generated from the following file:

- amcl.h

7.13 PAILLIER_private_key Struct Reference

Paillier Private Key.

```
#include <paillier.h>
```

Data Fields

- BIG_1024_58 p [HFLEN_2048]
- BIG_1024_58 q [HFLEN_2048]
- BIG_1024_58 lp [HFLEN_2048]
- BIG_1024_58 lq [HFLEN_2048]
- BIG_1024_58 invp [FFLEN_2048]
- BIG_1024_58 invq [FFLEN_2048]
- BIG_1024_58 p2 [FFLEN_2048]
- BIG_1024_58 q2 [FFLEN_2048]
- BIG_1024_58 mp [HFLEN_2048]
- BIG_1024_58 mq [HFLEN_2048]

7.13.1 Field Documentation

7.13.1.1 invp

```
BIG_1024_58 PAILLIER_private_key::invp[FFLEN_2048]
```

Precomputed $p^{-1} \pmod{2^m}$

7.13.1.2 invq

```
BIG_1024_58 PAILLIER_private_key::invq[FFLEN_2048]
```

Precomputed $q^{-1} \pmod{2^m}$

7.13.1.3 lp

```
BIG_1024_58 PAILLIER_private_key::lp[HFLEN_2048]
```

Private Key modulo p (Euler totient of p)

7.13.1.4 lq

```
BIG_1024_58 PAILLIER_private_key::lq[HFLEN_2048]
```

Private Key modulo q (Euler totient of q)

7.13.1.5 mp

```
BIG_1024_58 PAILLIER_private_key::mp[HFLEN_2048]
```

Precomputed $L(g^{lp} \pmod{p^2})^{-1}$

7.13.1.6 mq

`BIG_1024_58 PAILLIER_private_key::mq[HFLEN_2048]`

Precomputed $L(g^{lq} \pmod{q^2})^{-1}$

7.13.1.7 p

`BIG_1024_58 PAILLIER_private_key::p[HFLEN_2048]`

Secret Prime

7.13.1.8 p2

`BIG_1024_58 PAILLIER_private_key::p2[FFLEN_2048]`

Precomputed p^2

7.13.1.9 q

`BIG_1024_58 PAILLIER_private_key::q[HFLEN_2048]`

Secret Prime

7.13.1.10 q2

`BIG_1024_58 PAILLIER_private_key::q2[FFLEN_2048]`

Precomputed q^2

The documentation for this struct was generated from the following file:

- paillier.h

7.14 PAILLIER_public_key Struct Reference

Paillier Public Key.

```
#include <paillier.h>
```

Data Fields

- BIG_512_60 n [FFLEN_4096]
- BIG_512_60 g [FFLEN_4096]
- BIG_512_60 n2 [FFLEN_4096]

7.14.1 Field Documentation

7.14.1.1 g

```
BIG_512_60 PAILLIER_public_key::g[FFLEN_4096]
```

Public Base - $g = n + 1$

7.14.1.2 n

```
BIG_512_60 PAILLIER_public_key::n[FFLEN_4096]
```

Paillier Modulus - $n = pq$

7.14.1.3 n2

```
BIG_512_60 PAILLIER_public_key::n2[FFLEN_4096]
```

Precomputed n^2

The documentation for this struct was generated from the following file:

- paillier.h

7.15 pktype Struct Reference

Public key type.

```
#include <x509.h>
```

Data Fields

- int type
- int hash
- int curve

7.15.1 Field Documentation

7.15.1.1 curve

```
int pktype::curve
```

elliptic curve used or RSA key length in bits

7.15.1.2 hash

```
int pktype::hash
```

hash type

7.15.1.3 type

```
int pktype::type
```

signature type (ECC or RSA)

The documentation for this struct was generated from the following file:

- x509.h

7.16 rsa_private_key_2048 Struct Reference

Integer Factorisation Private Key.

```
#include <rsa_2048.h>
```

Data Fields

- BIG_1024_58 p [FFLEN_2048/2]
- BIG_1024_58 q [FFLEN_2048/2]
- BIG_1024_58 dp [FFLEN_2048/2]
- BIG_1024_58 dq [FFLEN_2048/2]
- BIG_1024_58 c [FFLEN_2048/2]

7.16.1 Field Documentation

7.16.1.1 c

```
BIG_1024_58 rsa_private_key_2048::c[FFLEN_2048/2]
```

1/p mod q

7.16.1.2 dp

```
BIG_1024_58 rsa_private_key_2048::dp[FFLEN_2048/2]
```

decrypting exponent mod (p-1)

7.16.1.3 dq

```
BIG_1024_58 rsa_private_key_2048::dq[FFLEN_2048/2]
```

decrypting exponent mod (q-1)

7.16.1.4 p

```
BIG_1024_58 rsa_private_key_2048::p[FFLEN_2048/2]
```

secret prime p

7.16.1.5 q

```
BIG_1024_58 rsa_private_key_2048::q[FFLEN_2048/2]
```

secret prime q

The documentation for this struct was generated from the following file:

- rsa_2048.h

7.17 rsa_public_key_2048 Struct Reference

Integer Factorisation Public Key.

```
#include <rsa_2048.h>
```

Data Fields

- sign32 e
- BIG_1024_58 n [FFLEN_2048]

7.17.1 Field Documentation

7.17.1.1 e

```
sign32 rsa_public_key_2048::e
```

RSA exponent (typically 65537)

7.17.1.2 n

```
BIG_1024_58 rsa_public_key_2048::n[FFLEN_2048]
```

An array of BIGs to store public key

The documentation for this struct was generated from the following file:

- rsa_2048.h

7.18 sha3 Struct Reference

SHA3 hash function instance.

```
#include <amcl.h>
```

Data Fields

- unsign64 length
- unsign64 S [5][5]
- int rate
- int len

7.18.1 Field Documentation

7.18.1.1 len

```
int sha3::len
```

Hash length in bytes

7.18.1.2 length

```
unsign64 sha3::length
```

64-bit input length

7.18.1.3 rate

```
int sha3::rate
```

TODO

7.18.1.4 S

```
unsign64 sha3::S[5][5]
```

Internal state

The documentation for this struct was generated from the following file:

- amcl.h

Chapter 8

File Documentation

8.1 arch.h File Reference

Architecture Header File.

Macros

- #define CHUNK 64
- #define byte unsigned char
- #define sign32 __int32
- #define sign8 signed char
- #define sign16 short int
- #define sign64 long long
- #define unsign32 unsigned __int32
- #define unsign64 unsigned long long
- #define uchar unsigned char
- #define chunk __int64

8.1.1 Detailed Description

Author

Mike Scott

Date

23rd February 2016 Specify Processor Architecture

8.1.2 Macro Definition Documentation

8.1.2.1 byte

```
#define byte unsigned char
```

8-bit unsigned integer

8.1.2.2 CHUNK

```
#define CHUNK 64
```

size of chunk in bits = wordlength of computer = 16, 32 or 64. Note not all curve options are supported on 16-bit processors - see rom.c

8.1.2.3 chunk

```
#define chunk __int64
```

C type corresponding to word length Note - no 128-bit type available

8.1.2.4 sign16

```
#define sign16 short int
```

16-bit signed integer

8.1.2.5 sign32

```
#define sign32 __int32
```

32-bit signed integer

8.1.2.6 sign64

```
#define sign64 long long
```

64-bit signed integer

8.1.2.7 sign8

```
#define sign8 signed char
```

8-bit signed integer

8.1.2.8 uchar

```
#define uchar unsigned char
```

Unsigned char

8.1.2.9 unsign32

```
#define unsign32 unsigned __int32
```

32-bit unsigned integer

8.1.2.10 unsign64

```
#define unsign64 unsigned long long
```

64-bit unsigned integer

8.2 big_1024_58.h File Reference

BIG Header File.

```
#include <stdio.h>
#include <stdlib.h>
#include <inttypes.h>
#include "arch.h"
#include "amcl.h"
#include "config_big_1024_58.h"
```

Macros

- #define BIGBITS_1024_58 (8*MODBYTES_1024_58)
- #define NLEN_1024_58 (1+((8*MODBYTES_1024_58-1)/BASEBITS_1024_58))
- #define DNLEN_1024_58 2*NLEN_1024_58
- #define BMASK_1024_58 (((chunk)1<<BASEBITS_1024_58)-1)
- #define NEXCESS_1024_58 (1<<(CHUNK-BASEBITS_1024_58-1))
- #define HBITS_1024_58 (BASEBITS_1024_58/2)
- #define HMASK_1024_58 (((chunk)1<<HBITS_1024_58)-1)

Typedefs

- typedef chunk BIG_1024_58[NLEN_1024_58]
- typedef chunk DBIG_1024_58[DNLEN_1024_58]

Functions

- int BIG_1024_58_iszilch (BIG_1024_58 x)

    Tests for BIG equal to zero.
- int BIG_1024_58_isunity (BIG_1024_58 x)

    Tests for BIG equal to one.
- int BIG_1024_58_diszilch (DBIG_1024_58 x)

    Tests for DBIG equal to zero.
- void BIG_1024_58_output (BIG_1024_58 x)

    Outputs a BIG number to the console.
- void BIG_1024_58_rawoutput (BIG_1024_58 x)

    Outputs a BIG number to the console in raw form (for debugging)
- void BIG_1024_58_cswap (BIG_1024_58 x, BIG_1024_58 y, int s)

    Conditional constant time swap of two BIG numbers.
- void BIG_1024_58_cmove (BIG_1024_58 x, BIG_1024_58 y, int s)

    Conditional copy of BIG number.
- void BIG_1024_58_dcmove (BIG_1024_58 x, BIG_1024_58 y, int s)

    Conditional copy of DBIG number.
- void BIG_1024_58_toBytes (char ∗a, BIG_1024_58 x)

    Convert from BIG number to byte array.
- void BIG_1024_58_fromBytes (BIG_1024_58 x, char ∗a)

    Convert to BIG number from byte array.
- void BIG_1024_58_fromBytesLen (BIG_1024_58 x, char ∗a, int s)

    Convert to BIG number from byte array of given length.
- void BIG_1024_58_dfromBytesLen (DBIG_1024_58 x, char ∗a, int s)

    Convert to DBIG number from byte array of given length.
- void BIG_1024_58_doutput (DBIG_1024_58 x)

    Outputs a DBIG number to the console.
- void BIG_1024_58_drawoutput (DBIG_1024_58 x)

    Outputs a DBIG number to the console.
- void BIG_1024_58_rcopy (BIG_1024_58 x, const BIG_1024_58 y)

    Copy BIG from Read-Only Memory to a BIG.
- void BIG_1024_58_copy (BIG_1024_58 x, BIG_1024_58 y)

    Copy BIG to another BIG.
- void BIG_1024_58_dcopy (DBIG_1024_58 x, DBIG_1024_58 y)

    Copy DBIG to another DBIG.
- void BIG_1024_58_dsucopy (DBIG_1024_58 x, BIG_1024_58 y)

    Copy BIG to upper half of DBIG.
- void BIG_1024_58_dscopy (DBIG_1024_58 x, BIG_1024_58 y)

    Copy BIG to lower half of DBIG.
- void BIG_1024_58_sdcopy (BIG_1024_58 x, DBIG_1024_58 y)

    Copy lower half of DBIG to a BIG.
- void BIG_1024_58_sducopy (BIG_1024_58 x, DBIG_1024_58 y)

    Copy upper half of DBIG to a BIG.
- void BIG_1024_58_zero (BIG_1024_58 x)

    Set BIG to zero.
- void BIG_1024_58_dzero (DBIG_1024_58 x)

    Set DBIG to zero.
- void BIG_1024_58_one (BIG_1024_58 x)

    Set BIG to one (unity)
- void BIG_1024_58_invmod2m (BIG_1024_58 x)

Set BIG to inverse mod 2^256.
- void BIG_1024_58_add (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z)

  Set BIG to sum of two BIGs - output not normalised.
- void BIG_1024_58_or (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z)

  Set BIG to logical or of two BIGs - output normalised.
- void BIG_1024_58_inc (BIG_1024_58 x, int i)

  Increment BIG by a small integer - output not normalised.
- void BIG_1024_58_sub (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z)

  Set BIG to difference of two BIGs.
- void BIG_1024_58_dec (BIG_1024_58 x, int i)

  Decrement BIG by a small integer - output not normalised.
- void BIG_1024_58_dadd (DBIG_1024_58 x, DBIG_1024_58 y, DBIG_1024_58 z)

  Set DBIG to sum of two DBIGs.
- void BIG_1024_58_dsub (DBIG_1024_58 x, DBIG_1024_58 y, DBIG_1024_58 z)

  Set DBIG to difference of two DBIGs.
- void BIG_1024_58_imul (BIG_1024_58 x, BIG_1024_58 y, int i)

  Multiply BIG by a small integer - output not normalised.
- chunk BIG_1024_58_pmul (BIG_1024_58 x, BIG_1024_58 y, int i)

  Multiply BIG by not-so-small small integer - output normalised.
- int BIG_1024_58_div3 (BIG_1024_58 x)

  Divide BIG by 3 - output normalised.
- void BIG_1024_58_pxmul (DBIG_1024_58 x, BIG_1024_58 y, int i)

  Multiply BIG by even bigger small integer resulting in a DBIG - output normalised.
- void BIG_1024_58_mul (DBIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z)

  Multiply BIG by another BIG resulting in DBIG - inputs normalised and output normalised.
- void BIG_1024_58_smul (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z)

  Multiply BIG by another BIG resulting in another BIG - inputs normalised and output normalised.
- void BIG_1024_58_sqr (DBIG_1024_58 x, BIG_1024_58 y)

  Square BIG resulting in a DBIG - input normalised and output normalised.
- void BIG_1024_58_monty (BIG_1024_58 a, BIG_1024_58 md, chunk MC, DBIG_1024_58 d)

  Montgomery reduction of a DBIG to a BIG - input normalised and output normalised.
- void BIG_1024_58_shl (BIG_1024_58 x, int s)

  Shifts a BIG left by any number of bits - input must be normalised, output normalised.
- int BIG_1024_58_fshl (BIG_1024_58 x, int s)

  Fast shifts a BIG left by a small number of bits - input must be normalised, output will be normalised.
- void BIG_1024_58_dshl (DBIG_1024_58 x, int s)

  Shifts a DBIG left by any number of bits - input must be normalised, output normalised.
- void BIG_1024_58_shr (BIG_1024_58 x, int s)

  Shifts a BIG right by any number of bits - input must be normalised, output normalised.
- int BIG_1024_58_ssn (BIG_1024_58 r, BIG_1024_58 a, BIG_1024_58 m)

  Fast time-critical combined shift by 1 bit, subtract and normalise.
- int BIG_1024_58_fshr (BIG_1024_58 x, int s)

  Fast shifts a BIG right by a small number of bits - input must be normalised, output will be normalised.
- void BIG_1024_58_dshr (DBIG_1024_58 x, int s)

  Shifts a DBIG right by any number of bits - input must be normalised, output normalised.
- chunk BIG_1024_58_split (BIG_1024_58 x, BIG_1024_58 y, DBIG_1024_58 z, int s)

  Splits a DBIG into two BIGs - input must be normalised, outputs normalised.
- chunk BIG_1024_58_norm (BIG_1024_58 x)

  Normalizes a BIG number - output normalised.
- void BIG_1024_58_dnorm (DBIG_1024_58 x)

  Normalizes a DBIG number - output normalised.

- int BIG_1024_58_comp (BIG_1024_58 x, BIG_1024_58 y)

    Compares two BIG numbers. Inputs must be normalised externally.
- int BIG_1024_58_dcomp (DBIG_1024_58 x, DBIG_1024_58 y)

    Compares two DBIG numbers. Inputs must be normalised externally.
- int BIG_1024_58_nbits (BIG_1024_58 x)

    Calculate number of bits in a BIG - output normalised.
- int BIG_1024_58_dnbits (DBIG_1024_58 x)

    Calculate number of bits in a DBIG - output normalised.
- void BIG_1024_58_mod (BIG_1024_58 x, BIG_1024_58 n)

    Reduce x mod n - input and output normalised.
- void BIG_1024_58_sdiv (BIG_1024_58 x, BIG_1024_58 n)

    Divide x by n - output normalised.
- void BIG_1024_58_dmod (BIG_1024_58 x, DBIG_1024_58 y, BIG_1024_58 n)

    x=y mod n - output normalised
- void BIG_1024_58_ddiv (BIG_1024_58 x, DBIG_1024_58 y, BIG_1024_58 n)

    x=y/n - output normalised
- int BIG_1024_58_parity (BIG_1024_58 x)

    return parity of BIG, that is the least significant bit
- int BIG_1024_58_bit (BIG_1024_58 x, int i)

    return i-th of BIG
- int BIG_1024_58_lastbits (BIG_1024_58 x, int n)

    return least significant bits of a BIG
- void BIG_1024_58_random (BIG_1024_58 x, csprng *r)

    Create a random BIG from a random number generator.
- void BIG_1024_58_randomnum (BIG_1024_58 x, BIG_1024_58 n, csprng *r)

    Create an unbiased random BIG from a random number generator, reduced with respect to a modulus.
- void BIG_1024_58_modmul (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z, BIG_1024_58 n)

    *Calculate x=y*z mod n.*
- void BIG_1024_58_moddiv (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 z, BIG_1024_58 n)

    Calculate x=y/z mod n.
- void BIG_1024_58_modsqr (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 n)

    Calculate x=y^2 mod n.
- void BIG_1024_58_modneg (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 n)

    Calculate x=-y mod n.
- int BIG_1024_58_jacobi (BIG_1024_58 x, BIG_1024_58 y)

    Calculate jacobi Symbol (x/y)
- void BIG_1024_58_invmodp (BIG_1024_58 x, BIG_1024_58 y, BIG_1024_58 n)

    Calculate x=1/y mod n.
- void BIG_1024_58_mod2m (BIG_1024_58 x, int m)

    Calculate x=x mod 2^m.
- void BIG_1024_58_dmod2m (DBIG_1024_58 x, int m)

    Calculate x=x mod 2^m.

8.2.1 Detailed Description

Author

Mike Scott

8.2.2 Macro Definition Documentation

8.2.2.1 BIGBITS_1024_58

```
#define BIGBITS_1024_58 (8*MODBYTES_1024_58)
```

Length in bits

8.2.2.2 BMASK_1024_58

```
#define BMASK_1024_58 (((chunk)1<<BASEBITS_1024_58)-1)
```

Mask = 2^BASEBITS-1

8.2.2.3 DNLEN_1024_58

```
#define DNLEN_1024_58 2*NLEN_1024_58
```

Double length in bytes

8.2.2.4 HBITS_1024_58

```
#define HBITS_1024_58 (BASEBITS_1024_58/2)
```

Number of bits in number base divided by 2

8.2.2.5 HMASK_1024_58

```
#define HMASK_1024_58 (((chunk)1<<HBITS_1024_58)-1)
```

Mask = 2^HBITS-1

8.2.2.6 NEXCESS_1024_58

```
#define NEXCESS_1024_58 (1<<(CHUNK-BASEBITS_1024_58-1))
```

2^(CHUNK-BASEBITS-1) - digit cannot be multiplied by more than this before normalisation

8.2.2.7 NLEN_1024_58

```
#define NLEN_1024_58 (1+((8*MODBYTES_1024_58-1)/BASEBITS_1024_58))
```

length in bytes

8.2.3 Typedef Documentation

8.2.3.1 BIG_1024_58

```
typedef chunk BIG_1024_58[NLEN_1024_58]
```

Define type BIG as array of chunks

8.2.3.2 DBIG_1024_58

```
typedef chunk DBIG_1024_58[DNLEN_1024_58]
```

Define type DBIG as array of chunks

8.2.4 Function Documentation

8.2.4.1 BIG_1024_58_add()

```
void BIG_1024_58_add (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z )
```

Parameters

x	BIG number, sum of other two
y	BIG number
z	BIG number

8.2.4.2 BIG_1024_58_bit()

```
int BIG_1024_58_bit (
            BIG_1024_58 x,
            int i )
```

Parameters

x	BIG number
i	the bit of x to be returned

Returns

0 or 1

8.2.4.3 BIG_1024_58_cmove()

```
void BIG_1024_58_cmove (
            BIG_1024_58 x,
            BIG_1024_58 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a BIG number
y	another BIG number
s	copy takes place if not equal to 0

8.2.4.4 BIG_1024_58_comp()

```
int BIG_1024_58_comp (
            BIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	first BIG number to be compared
y	second BIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.2.4.5 BIG_1024_58_copy()

```
void BIG_1024_58_copy (
            BIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	BIG number
y	BIG number to be copied

8.2.4.6 BIG_1024_58_cswap()

```
void BIG_1024_58_cswap (
            BIG_1024_58 x,
            BIG_1024_58 y,
            int s )
```

Conditionally swaps parameters in constant time (without branching)

Parameters

x	a BIG number
y	another BIG number
s	swap takes place if not equal to 0

8.2.4.7 BIG_1024_58_dadd()

```
void BIG_1024_58_dadd (
            DBIG_1024_58 x,
            DBIG_1024_58 y,
            DBIG_1024_58 z )
```

Parameters

x	DBIG number, sum of other two - output not normalised
y	DBIG number
z	DBIG number

8.2.4.8 BIG_1024_58_dcmove()

```
void BIG_1024_58_dcmove (
            BIG_1024_58 x,
            BIG_1024_58 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a DBIG number
y	another DBIG number
s	copy takes place if not equal to 0

8.2.4.9 BIG_1024_58_dcomp()

```
int BIG_1024_58_dcomp (
            DBIG_1024_58 x,
            DBIG_1024_58 y )
```

Parameters

x	first DBIG number to be compared
y	second DBIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.2.4.10 BIG_1024_58_dcopy()

```
void BIG_1024_58_dcopy (
            DBIG_1024_58 x,
            DBIG_1024_58 y )
```

Parameters

x	DBIG number
y	DBIG number to be copied

8.2.4.11 BIG_1024_58_ddiv()

```
void BIG_1024_58_ddiv (
            BIG_1024_58 x,
            DBIG_1024_58 y,
            BIG_1024_58 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y/n
y	DBIG number
n	Modulus

8.2.4.12 BIG_1024_58_dec()

```
void BIG_1024_58_dec (
            BIG_1024_58 x,
            int i )
```

Parameters

x	BIG number to be decremented
i	integer

8.2.4.13 BIG_1024_58_dfromBytesLen()

```
void BIG_1024_58_dfromBytesLen (
            DBIG_1024_58 x,
            char * a,
            int s )
```

Parameters

x	DBIG number
a	byte array
s	byte array length

8.2.4.14 BIG_1024_58_diszilch()

```
int BIG_1024_58_diszilch (
            DBIG_1024_58 x )
```

Parameters

x	a DBIG number

Returns

1 if zero, else returns 0

8.2.4.15 BIG_1024_58_div3()

```
int BIG_1024_58_div3 (
            BIG_1024_58 x )
```

Parameters

x	BIG number

Returns

Remainder

8.2.4.16 BIG_1024_58_dmod()

```
void BIG_1024_58_dmod (
            BIG_1024_58 x,
            DBIG_1024_58 y,
            BIG_1024_58 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y mod n
y	DBIG number
n	Modulus

8.2.4.17 BIG_1024_58_dmod2m()

```
void BIG_1024_58_dmod2m (
            DBIG_1024_58 x,
            int m )
```

Truncation

Parameters

x	DBIG number, on reduced mod 2^m
m	new truncated size

8.2.4.18 BIG_1024_58_dnbits()

```
int BIG_1024_58_dnbits (
            DBIG_1024_58 x )
```

Parameters

x	DBIG number

Returns

Number of bits in x

8.2.4.19 BIG_1024_58_dnorm()

```
void BIG_1024_58_dnorm (
        DBIG_1024_58 x )
```

All digits of the input DBIG are reduced mod 2^BASEBITS

Parameters

x	DBIG number to be normalised

8.2.4.20 BIG_1024_58_doutput()

```
void BIG_1024_58_doutput (
        DBIG_1024_58 x )
```

Parameters

x	a DBIG number

8.2.4.21 BIG_1024_58_drawoutput()

```
void BIG_1024_58_drawoutput (
        DBIG_1024_58 x )
```

Parameters

x	a DBIG number

8.2.4.22 BIG_1024_58_dscopy()

```
void BIG_1024_58_dscopy (
            DBIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.2.4.23 BIG_1024_58_dshl()

```
void BIG_1024_58_dshl (
            DBIG_1024_58 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.2.4.24 BIG_1024_58_dshr()

```
void BIG_1024_58_dshr (
            DBIG_1024_58 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.2.4.25 BIG_1024_58_dsub()

```
void BIG_1024_58_dsub (
            DBIG_1024_58 x,
            DBIG_1024_58 y,
            DBIG_1024_58 z )
```

Parameters

x	DBIG number, difference of other two - output not normalised
y	DBIG number
z	DBIG number

8.2.4.26 BIG_1024_58_dsucopy()

```
void BIG_1024_58_dsucopy (
            DBIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.2.4.27 BIG_1024_58_dzero()

```
void BIG_1024_58_dzero (
            DBIG_1024_58 x )
```

Parameters

x	DBIG number to be set to zero

8.2.4.28 BIG_1024_58_fromBytes()

```
void BIG_1024_58_fromBytes (
            BIG_1024_58 x,
            char * a )
```

Parameters

x	BIG number
a	byte array

8.2.4.29 BIG_1024_58_fromBytesLen()

```
void BIG_1024_58_fromBytesLen (
            BIG_1024_58 x,
            char * a,
            int s )
```

Parameters

x	BIG number
a	byte array
s	byte array length

8.2.4.30 BIG_1024_58_fshl()

```
int BIG_1024_58_fshl (
            BIG_1024_58 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Overflow bits

8.2.4.31 BIG_1024_58_fshr()

```
int BIG_1024_58_fshr (
            BIG_1024_58 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Shifted out bits

8.2.4.32 BIG_1024_58_imul()

```
void BIG_1024_58_imul (
            BIG_1024_58 x,
            BIG_1024_58 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

8.2.4.33 BIG_1024_58_inc()

```
void BIG_1024_58_inc (
            BIG_1024_58 x,
            int i )
```

Parameters

x	BIG number to be incremented
i	integer

8.2.4.34 BIG_1024_58_invmod2m()

```
void BIG_1024_58_invmod2m (
            BIG_1024_58 x )
```

Parameters

x	BIG number to be inverted

8.2.4.35 BIG_1024_58_invmodp()

```
void BIG_1024_58_invmodp (
```

```
BIG_1024_58 x,
BIG_1024_58 y,
BIG_1024_58 n )
```

Modular Inversion - This is slow. Uses binary method.

Parameters

x	BIG number, on exit = 1/y mod n
y	BIG number
n	The BIG Modulus

8.2.4.36 BIG_1024_58_isunity()

```
int BIG_1024_58_isunity (
            BIG_1024_58 x )
```

Parameters

x	a BIG number

Returns

1 if one, else returns 0

8.2.4.37 BIG_1024_58_iszilch()

```
int BIG_1024_58_iszilch (
            BIG_1024_58 x )
```

Parameters

x	a BIG number

Returns

1 if zero, else returns 0

8.2.4.38 BIG_1024_58_jacobi()

```
int BIG_1024_58_jacobi (
            BIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	BIG number
y	BIG number

Returns

Jacobi symbol, -1,0 or 1

8.2.4.39 BIG_1024_58_lastbits()

```
int BIG_1024_58_lastbits (
            BIG_1024_58 x,
            int n )
```

Parameters

x	BIG number
n	number of bits to return. Assumed to be less than BASEBITS.

Returns

least significant n bits as an integer

8.2.4.40 BIG_1024_58_mod()

```
void BIG_1024_58_mod (
            BIG_1024_58 x,
            BIG_1024_58 n )
```

Slow but rarely used

Parameters

x	BIG number to be reduced mod n
n	The modulus

8.2.4.41 BIG_1024_58_mod2m()

```
void BIG_1024_58_mod2m (
            BIG_1024_58 x,
            int m )
```

Truncation

Parameters

x	BIG number, on reduced mod 2^m
m	new truncated size

8.2.4.42 BIG_1024_58_moddiv()

```
void BIG_1024_58_moddiv (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z,
            BIG_1024_58 n )
```

Slow method for modular division

Parameters

x	BIG number, on exit = y/z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.2.4.43 BIG_1024_58_modmul()

```
void BIG_1024_58_modmul (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z,
            BIG_1024_58 n )
```

brief return NAF (Non-Adjacent-Form) value as +/- 1, 3 or 5, inputs must be normalised

Given x and 3∗x extracts NAF value from given bit position, and returns number of bits processed, and number of trailing zeros detected if any param x BIG number param x3 BIG number, three times x param i bit position param nbs pointer to integer returning number of bits processed param nzs pointer to integer returning number of trailing 0s return + or - 1, 3 or 5Slow method for modular multiplication

Parameters

x	BIG number, on exit = y∗z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.2.4.44 BIG_1024_58_modneg()

```
void BIG_1024_58_modneg (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 n )
```

Modular negation

Parameters

x	BIG number, on exit = -y mod n
y	BIG number
n	The BIG Modulus

8.2.4.45 BIG_1024_58_modsqr()

```
void BIG_1024_58_modsqr (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 n )
```

Slow method for modular squaring

Parameters

x	BIG number, on exit = y^2 mod n
y	BIG number
n	The BIG Modulus

8.2.4.46 BIG_1024_58_monty()

```
void BIG_1024_58_monty (
            BIG_1024_58 a,
            BIG_1024_58 md,
            chunk MC,
            DBIG_1024_58 d )
```

Parameters

a	BIG number, reduction of a BIG
md	BIG number, the modulus
MC	the Montgomery Constant
d	DBIG number to be reduced

8.2.4.47 BIG_1024_58_mul()

```
void BIG_1024_58_mul (
            DBIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z )
```

Parameters

x	DBIG number, product of other two
y	BIG number
z	BIG number

8.2.4.48 BIG_1024_58_nbits()

```
int BIG_1024_58_nbits (
            BIG_1024_58 x )
```

Parameters

x	BIG number

Returns

Number of bits in x

8.2.4.49 BIG_1024_58_norm()

```
chunk BIG_1024_58_norm (
            BIG_1024_58 x )
```

All digits of the input BIG are reduced mod 2^BASEBITS

Parameters

x	BIG number to be normalised

8.2.4.50 BIG_1024_58_one()

```
void BIG_1024_58_one (
            BIG_1024_58 x )
```

Parameters

x	BIG number to be set to one.

8.2.4.51 BIG_1024_58_or()

```
void BIG_1024_58_or (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z )
```

Parameters

x	BIG number, or of other two
y	BIG number
z	BIG number

8.2.4.52 BIG_1024_58_output()

```
void BIG_1024_58_output (
            BIG_1024_58 x )
```

Parameters

x	a BIG number

8.2.4.53 BIG_1024_58_parity()

```
int BIG_1024_58_parity (
            BIG_1024_58 x )
```

Parameters

x	BIG number

Returns

0 or 1

8.2.4.54 BIG_1024_58_pmul()

```
chunk BIG_1024_58_pmul (
            BIG_1024_58 x,
            BIG_1024_58 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

Returns

Overflowing bits

8.2.4.55 BIG_1024_58_pxmul()

```
void BIG_1024_58_pxmul (
            DBIG_1024_58 x,
            BIG_1024_58 y,
            int i )
```

Parameters

x	DBIG number, product of other two
y	BIG number
i	small integer

8.2.4.56 BIG_1024_58_random()

```
void BIG_1024_58_random (
            BIG_1024_58 x,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
r	A pointer to a Cryptographically Secure Random Number Generator

8.2.4.57 BIG_1024_58_randomnum()

```
void BIG_1024_58_randomnum (
            BIG_1024_58 x,
            BIG_1024_58 n,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
n	The modulus
r	A pointer to a Cryptographically Secure Random Number Generator

8.2.4.58 BIG_1024_58_rawoutput()

```
void BIG_1024_58_rawoutput (
            BIG_1024_58 x )
```

Parameters

x	a BIG number

8.2.4.59 BIG_1024_58_rcopy()

```
void BIG_1024_58_rcopy (
            BIG_1024_58 x,
            const BIG_1024_58 y )
```

Parameters

x	BIG number
y	BIG number in ROM

8.2.4.60 BIG_1024_58_sdcopy()

```
void BIG_1024_58_sdcopy (
            BIG_1024_58 x,
            DBIG_1024_58 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.2.4.61 BIG_1024_58_sdiv()

```
void BIG_1024_58_sdiv (
            BIG_1024_58 x,
            BIG_1024_58 n )
```

Slow but rarely used

Parameters

x	BIG number to be divided by n
n	The Divisor

8.2.4.62 BIG_1024_58_sducopy()

```
void BIG_1024_58_sducopy (
            BIG_1024_58 x,
            DBIG_1024_58 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.2.4.63 BIG_1024_58_shl()

```
void BIG_1024_58_shl (
            BIG_1024_58 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.2.4.64 BIG_1024_58_shr()

```
void BIG_1024_58_shr (
            BIG_1024_58 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.2.4.65 BIG_1024_58_smul()

```
void BIG_1024_58_smul (
            BIG_1024_58 x,
            BIG_1024_58 y,
            BIG_1024_58 z )
```

Note that the product must fit into a BIG, and x must be distinct from y and z

Parameters

x	BIG number, product of other two
y	BIG number
z	BIG number

8.2.4.66 BIG_1024_58_split()

```
chunk BIG_1024_58_split (
            BIG_1024_58 x,
            BIG_1024_58 y,
            DBIG_1024_58 z,
            int s )
```

Internal function. The value of s must be approximately in the middle of the DBIG. Typically used to extract z mod 2^MODBITS and z/2^MODBITS

Parameters

x	BIG number, top half of z
y	BIG number, bottom half of z
z	DBIG number to be split in two.
s	Bit position at which to split

Returns

carry-out from top half

8.2.4.67 BIG_1024_58_sqr()

```
void BIG_1024_58_sqr (
            DBIG_1024_58 x,
            BIG_1024_58 y )
```

Parameters

x	DBIG number, square of a BIG
y	BIG number to be squared

8.2.4.68 BIG_1024_58_ssn()

```
int BIG_1024_58_ssn (
            BIG_1024_58 r,
            BIG_1024_58 a,
            BIG_1024_58 m )
```

Parameters

r	BIG number normalised output
a	BIG number to be subtracted from
m	BIG number to be shifted and subtracted

Returns

sign of r

8.2.4.69 BIG_1024_58_sub()

```
void BIG_1024_58_sub (
            BIG_1024_58 x,
```

```
            BIG_1024_58 y,
            BIG_1024_58 z )
```

Parameters

x	BIG number, difference of other two - output not normalised
y	BIG number
z	BIG number

8.2.4.70 BIG_1024_58_toBytes()

```
void BIG_1024_58_toBytes (
            char * a,
            BIG_1024_58 x )
```

Parameters

a	byte array
x	BIG number

8.2.4.71 BIG_1024_58_zero()

```
void BIG_1024_58_zero (
            BIG_1024_58 x )
```

Parameters

x	BIG number to be set to zero

8.3 big_384_58.h File Reference

BIG Header File.

```
#include <stdio.h>
#include <stdlib.h>
#include <inttypes.h>
#include "arch.h"
#include "amcl.h"
#include "config_big_384_58.h"
```

Macros

- #define BIGBITS_384_58 (8∗MODBYTES_384_58)
- #define NLEN_384_58 (1+((8∗MODBYTES_384_58-1)/BASEBITS_384_58))
- #define DNLEN_384_58 2∗NLEN_384_58
- #define BMASK_384_58 (((chunk)1<<BASEBITS_384_58)-1)
- #define NEXCESS_384_58 (1<<(CHUNK-BASEBITS_384_58-1))
- #define HBITS_384_58 (BASEBITS_384_58/2)
- #define HMASK_384_58 (((chunk)1<<HBITS_384_58)-1)

Typedefs

- typedef chunk BIG_384_58[NLEN_384_58]
- typedef chunk DBIG_384_58[DNLEN_384_58]

Functions

- int BIG_384_58_iszilch (BIG_384_58 x)

  Tests for BIG equal to zero.
- int BIG_384_58_isunity (BIG_384_58 x)

  Tests for BIG equal to one.
- int BIG_384_58_diszilch (DBIG_384_58 x)

  Tests for DBIG equal to zero.
- void BIG_384_58_output (BIG_384_58 x)

  Outputs a BIG number to the console.
- void BIG_384_58_rawoutput (BIG_384_58 x)

  Outputs a BIG number to the console in raw form (for debugging)
- void BIG_384_58_cswap (BIG_384_58 x, BIG_384_58 y, int s)

  Conditional constant time swap of two BIG numbers.
- void BIG_384_58_cmove (BIG_384_58 x, BIG_384_58 y, int s)

  Conditional copy of BIG number.
- void BIG_384_58_dcmove (BIG_384_58 x, BIG_384_58 y, int s)

  Conditional copy of DBIG number.
- void BIG_384_58_toBytes (char ∗a, BIG_384_58 x)

  Convert from BIG number to byte array.
- void BIG_384_58_fromBytes (BIG_384_58 x, char ∗a)

  Convert to BIG number from byte array.
- void BIG_384_58_fromBytesLen (BIG_384_58 x, char ∗a, int s)

  Convert to BIG number from byte array of given length.
- void BIG_384_58_dfromBytesLen (DBIG_384_58 x, char ∗a, int s)

  Convert to DBIG number from byte array of given length.
- void BIG_384_58_doutput (DBIG_384_58 x)

  Outputs a DBIG number to the console.
- void BIG_384_58_drawoutput (DBIG_384_58 x)

  Outputs a DBIG number to the console.
- void BIG_384_58_rcopy (BIG_384_58 x, const BIG_384_58 y)

  Copy BIG from Read-Only Memory to a BIG.
- void BIG_384_58_copy (BIG_384_58 x, BIG_384_58 y)

  Copy BIG to another BIG.
- void BIG_384_58_dcopy (DBIG_384_58 x, DBIG_384_58 y)

Copy DBIG to another DBIG.

- void BIG_384_58_dsucopy (DBIG_384_58 x, BIG_384_58 y)

  Copy BIG to upper half of DBIG.
- void BIG_384_58_dscopy (DBIG_384_58 x, BIG_384_58 y)

  Copy BIG to lower half of DBIG.
- void BIG_384_58_sdcopy (BIG_384_58 x, DBIG_384_58 y)

  Copy lower half of DBIG to a BIG.
- void BIG_384_58_sducopy (BIG_384_58 x, DBIG_384_58 y)

  Copy upper half of DBIG to a BIG.
- void BIG_384_58_zero (BIG_384_58 x)

  Set BIG to zero.
- void BIG_384_58_dzero (DBIG_384_58 x)

  Set DBIG to zero.
- void BIG_384_58_one (BIG_384_58 x)

  Set BIG to one (unity)
- void BIG_384_58_invmod2m (BIG_384_58 x)

  Set BIG to inverse mod 2^256.
- void BIG_384_58_add (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z)

  Set BIG to sum of two BIGs - output not normalised.
- void BIG_384_58_or (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z)

  Set BIG to logical or of two BIGs - output normalised.
- void BIG_384_58_inc (BIG_384_58 x, int i)

  Increment BIG by a small integer - output not normalised.
- void BIG_384_58_sub (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z)

  Set BIG to difference of two BIGs.
- void BIG_384_58_dec (BIG_384_58 x, int i)

  Decrement BIG by a small integer - output not normalised.
- void BIG_384_58_dadd (DBIG_384_58 x, DBIG_384_58 y, DBIG_384_58 z)

  Set DBIG to sum of two DBIGs.
- void BIG_384_58_dsub (DBIG_384_58 x, DBIG_384_58 y, DBIG_384_58 z)

  Set DBIG to difference of two DBIGs.
- void BIG_384_58_imul (BIG_384_58 x, BIG_384_58 y, int i)

  Multiply BIG by a small integer - output not normalised.
- chunk BIG_384_58_pmul (BIG_384_58 x, BIG_384_58 y, int i)

  Multiply BIG by not-so-small small integer - output normalised.
- int BIG_384_58_div3 (BIG_384_58 x)

  Divide BIG by 3 - output normalised.
- void BIG_384_58_pxmul (DBIG_384_58 x, BIG_384_58 y, int i)

  Multiply BIG by even bigger small integer resulting in a DBIG - output normalised.
- void BIG_384_58_mul (DBIG_384_58 x, BIG_384_58 y, BIG_384_58 z)

  Multiply BIG by another BIG resulting in DBIG - inputs normalised and output normalised.
- void BIG_384_58_smul (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z)

  Multiply BIG by another BIG resulting in another BIG - inputs normalised and output normalised.
- void BIG_384_58_sqr (DBIG_384_58 x, BIG_384_58 y)

  Square BIG resulting in a DBIG - input normalised and output normalised.
- void BIG_384_58_monty (BIG_384_58 a, BIG_384_58 md, chunk MC, DBIG_384_58 d)

  Montgomery reduction of a DBIG to a BIG - input normalised and output normalised.
- void BIG_384_58_shl (BIG_384_58 x, int s)

  Shifts a BIG left by any number of bits - input must be normalised, output normalised.
- int BIG_384_58_fshl (BIG_384_58 x, int s)

  Fast shifts a BIG left by a small number of bits - input must be normalised, output will be normalised.

- void BIG_384_58_dshl (DBIG_384_58 x, int s)

  Shifts a DBIG left by any number of bits - input must be normalised, output normalised.
- void BIG_384_58_shr (BIG_384_58 x, int s)

  Shifts a BIG right by any number of bits - input must be normalised, output normalised.
- int BIG_384_58_ssn (BIG_384_58 r, BIG_384_58 a, BIG_384_58 m)

  Fast time-critical combined shift by 1 bit, subtract and normalise.
- int BIG_384_58_fshr (BIG_384_58 x, int s)

  Fast shifts a BIG right by a small number of bits - input must be normalised, output will be normalised.
- void BIG_384_58_dshr (DBIG_384_58 x, int s)

  Shifts a DBIG right by any number of bits - input must be normalised, output normalised.
- chunk BIG_384_58_split (BIG_384_58 x, BIG_384_58 y, DBIG_384_58 z, int s)

  Splits a DBIG into two BIGs - input must be normalised, outputs normalised.
- chunk BIG_384_58_norm (BIG_384_58 x)

  Normalizes a BIG number - output normalised.
- void BIG_384_58_dnorm (DBIG_384_58 x)

  Normalizes a DBIG number - output normalised.
- int BIG_384_58_comp (BIG_384_58 x, BIG_384_58 y)

  Compares two BIG numbers. Inputs must be normalised externally.
- int BIG_384_58_dcomp (DBIG_384_58 x, DBIG_384_58 y)

  Compares two DBIG numbers. Inputs must be normalised externally.
- int BIG_384_58_nbits (BIG_384_58 x)

  Calculate number of bits in a BIG - output normalised.
- int BIG_384_58_dnbits (DBIG_384_58 x)

  Calculate number of bits in a DBIG - output normalised.
- void BIG_384_58_mod (BIG_384_58 x, BIG_384_58 n)

  Reduce x mod n - input and output normalised.
- void BIG_384_58_sdiv (BIG_384_58 x, BIG_384_58 n)

  Divide x by n - output normalised.
- void BIG_384_58_dmod (BIG_384_58 x, DBIG_384_58 y, BIG_384_58 n)

  x=y mod n - output normalised
- void BIG_384_58_ddiv (BIG_384_58 x, DBIG_384_58 y, BIG_384_58 n)

  x=y/n - output normalised
- int BIG_384_58_parity (BIG_384_58 x)

  return parity of BIG, that is the least significant bit
- int BIG_384_58_bit (BIG_384_58 x, int i)

  return i-th of BIG
- int BIG_384_58_lastbits (BIG_384_58 x, int n)

  return least significant bits of a BIG
- void BIG_384_58_random (BIG_384_58 x, csprng ∗r)

  Create a random BIG from a random number generator.
- void BIG_384_58_randomnum (BIG_384_58 x, BIG_384_58 n, csprng ∗r)

  Create an unbiased random BIG from a random number generator, reduced with respect to a modulus.
- void BIG_384_58_modmul (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z, BIG_384_58 n)

  Calculate x=y∗z mod n.
- void BIG_384_58_moddiv (BIG_384_58 x, BIG_384_58 y, BIG_384_58 z, BIG_384_58 n)

  Calculate x=y/z mod n.
- void BIG_384_58_modsqr (BIG_384_58 x, BIG_384_58 y, BIG_384_58 n)

  Calculate x=y^2 mod n.
- void BIG_384_58_modneg (BIG_384_58 x, BIG_384_58 y, BIG_384_58 n)

  Calculate x=-y mod n.
- int BIG_384_58_jacobi (BIG_384_58 x, BIG_384_58 y)

Calculate jacobi Symbol (x/y)
- void BIG_384_58_invmodp (BIG_384_58 x, BIG_384_58 y, BIG_384_58 n)

  Calculate x=1/y mod n.
- void BIG_384_58_mod2m (BIG_384_58 x, int m)

  Calculate x=x mod 2^m.
- void BIG_384_58_dmod2m (DBIG_384_58 x, int m)

  Calculate x=x mod 2^m.

8.3.1 Detailed Description

Author

Mike Scott

8.3.2 Macro Definition Documentation

8.3.2.1 BIGBITS_384_58

```
#define BIGBITS_384_58 (8*MODBYTES_384_58)
```

Length in bits

8.3.2.2 BMASK_384_58

```
#define BMASK_384_58 (((chunk)1<<BASEBITS_384_58)-1)
```

Mask = 2^BASEBITS-1

8.3.2.3 DNLEN_384_58

```
#define DNLEN_384_58 2*NLEN_384_58
```

Double length in bytes

8.3.2.4 HBITS_384_58

```
#define HBITS_384_58 (BASEBITS_384_58/2)
```

Number of bits in number base divided by 2

8.3.2.5 HMASK_384_58

```
#define HMASK_384_58 (((chunk)1<<HBITS_384_58)-1)
```

Mask = 2^HBITS-1

8.3.2.6 NEXCESS_384_58

```
#define NEXCESS_384_58 (1<<(CHUNK-BASEBITS_384_58-1))
```

2^(CHUNK-BASEBITS-1) - digit cannot be multiplied by more than this before normalisation

8.3.2.7 NLEN_384_58

```
#define NLEN_384_58 (1+((8*MODBYTES_384_58-1)/BASEBITS_384_58))
```

length in bytes

8.3.3 Typedef Documentation

8.3.3.1 BIG_384_58

```
typedef chunk BIG_384_58[NLEN_384_58]
```

Define type BIG as array of chunks

8.3.3.2 DBIG_384_58

```
typedef chunk DBIG_384_58[DNLEN_384_58]
```

Define type DBIG as array of chunks

8.3.4 Function Documentation

8.3.4.1 BIG_384_58_add()

```
void BIG_384_58_add (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z )
```

Parameters

x	BIG number, sum of other two
y	BIG number
z	BIG number

8.3.4.2 BIG_384_58_bit()

```
int BIG_384_58_bit (
            BIG_384_58 x,
            int i )
```

Parameters

x	BIG number
i	the bit of x to be returned

Returns

0 or 1

8.3.4.3 BIG_384_58_cmove()

```
void BIG_384_58_cmove (
            BIG_384_58 x,
            BIG_384_58 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a BIG number
y	another BIG number
s	copy takes place if not equal to 0

8.3.4.4 BIG_384_58_comp()

```
int BIG_384_58_comp (
            BIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	first BIG number to be compared
y	second BIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.3.4.5 BIG_384_58_copy()

```
void BIG_384_58_copy (
            BIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	BIG number
y	BIG number to be copied

8.3.4.6 BIG_384_58_cswap()

```
void BIG_384_58_cswap (
            BIG_384_58 x,
            BIG_384_58 y,
            int s )
```

Conditionally swaps parameters in constant time (without branching)

Parameters

x	a BIG number
y	another BIG number
s	swap takes place if not equal to 0

8.3.4.7 BIG_384_58_dadd()

```
void BIG_384_58_dadd (
            DBIG_384_58 x,
            DBIG_384_58 y,
            DBIG_384_58 z )
```

Parameters

x	DBIG number, sum of other two - output not normalised
y	DBIG number
z	DBIG number

8.3.4.8 BIG_384_58_dcmove()

```
void BIG_384_58_dcmove (
            BIG_384_58 x,
            BIG_384_58 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a DBIG number
y	another DBIG number
s	copy takes place if not equal to 0

8.3.4.9 BIG_384_58_dcomp()

```
int BIG_384_58_dcomp (
            DBIG_384_58 x,
            DBIG_384_58 y )
```

Parameters

x	first DBIG number to be compared
y	second DBIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.3.4.10 BIG_384_58_dcopy()

```
void BIG_384_58_dcopy (
            DBIG_384_58 x,
            DBIG_384_58 y )
```

Parameters

x	DBIG number
y	DBIG number to be copied

8.3.4.11 BIG_384_58_ddiv()

```
void BIG_384_58_ddiv (
            BIG_384_58 x,
            DBIG_384_58 y,
            BIG_384_58 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y/n
y	DBIG number
n	Modulus

8.3.4.12 BIG_384_58_dec()

```
void BIG_384_58_dec (
            BIG_384_58 x,
            int i )
```

Parameters

x	BIG number to be decremented
i	integer

8.3.4.13 BIG_384_58_dfromBytesLen()

```
void BIG_384_58_dfromBytesLen (
            DBIG_384_58 x,
            char * a,
            int s )
```

Parameters

x	DBIG number
a	byte array
s	byte array length

8.3.4.14 BIG_384_58_diszilch()

```
int BIG_384_58_diszilch (
            DBIG_384_58 x )
```

Parameters

x	a DBIG number

Returns

1 if zero, else returns 0

8.3.4.15 BIG_384_58_div3()

```
int BIG_384_58_div3 (
            BIG_384_58 x )
```

Parameters

x	BIG number

Returns

Remainder

8.3.4.16 BIG_384_58_dmod()

```
void BIG_384_58_dmod (
            BIG_384_58 x,
            DBIG_384_58 y,
            BIG_384_58 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y mod n
y	DBIG number
n	Modulus

8.3.4.17 BIG_384_58_dmod2m()

```
void BIG_384_58_dmod2m (
            DBIG_384_58 x,
            int m )
```

Truncation

Parameters

x	DBIG number, on reduced mod 2^m
m	new truncated size

8.3.4.18 BIG_384_58_dnbits()

```
int BIG_384_58_dnbits (
            DBIG_384_58 x )
```

Parameters

x	DBIG number

Returns

Number of bits in x

8.3.4.19 BIG_384_58_dnorm()

```
void BIG_384_58_dnorm (
            DBIG_384_58 x )
```

All digits of the input DBIG are reduced mod 2^BASEBITS

Parameters

x	DBIG number to be normalised

8.3.4.20 BIG_384_58_doutput()

```
void BIG_384_58_doutput (
            DBIG_384_58 x )
```

Parameters

x	a DBIG number

8.3.4.21 BIG_384_58_drawoutput()

```
void BIG_384_58_drawoutput (
            DBIG_384_58 x )
```

Parameters

x	a DBIG number

8.3.4.22 BIG_384_58_dscopy()

```
void BIG_384_58_dscopy (
            DBIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.3.4.23 BIG_384_58_dshl()

```
void BIG_384_58_dshl (
            DBIG_384_58 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.3.4.24 BIG_384_58_dshr()

```
void BIG_384_58_dshr (
```

```
            DBIG_384_58 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.3.4.25 BIG_384_58_dsub()

```
void BIG_384_58_dsub (
            DBIG_384_58 x,
            DBIG_384_58 y,
            DBIG_384_58 z )
```

Parameters

x	DBIG number, difference of other two - output not normalised
y	DBIG number
z	DBIG number

8.3.4.26 BIG_384_58_dsucopy()

```
void BIG_384_58_dsucopy (
            DBIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.3.4.27 BIG_384_58_dzero()

```
void BIG_384_58_dzero (
            DBIG_384_58 x )
```

Parameters

x	DBIG number to be set to zero

8.3.4.28 BIG_384_58_fromBytes()

```
void BIG_384_58_fromBytes (
            BIG_384_58 x,
            char * a )
```

Parameters

x	BIG number
a	byte array

8.3.4.29 BIG_384_58_fromBytesLen()

```
void BIG_384_58_fromBytesLen (
            BIG_384_58 x,
            char * a,
            int s )
```

Parameters

x	BIG number
a	byte array
s	byte array length

8.3.4.30 BIG_384_58_fshl()

```
int BIG_384_58_fshl (
            BIG_384_58 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Overflow bits

8.3.4.31 BIG_384_58_fshr()

```
int BIG_384_58_fshr (
            BIG_384_58 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Shifted out bits

8.3.4.32 BIG_384_58_imul()

```
void BIG_384_58_imul (
            BIG_384_58 x,
            BIG_384_58 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

8.3.4.33 BIG_384_58_inc()

```
void BIG_384_58_inc (
            BIG_384_58 x,
            int i )
```

Parameters

x	BIG number to be incremented
i	integer

8.3.4.34 BIG_384_58_invmod2m()

```
void BIG_384_58_invmod2m (
            BIG_384_58 x )
```

Parameters

x	BIG number to be inverted

8.3.4.35 BIG_384_58_invmodp()

```
void BIG_384_58_invmodp (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 n )
```

Modular Inversion - This is slow. Uses binary method.

Parameters

x	BIG number, on exit = 1/y mod n
y	BIG number
n	The BIG Modulus

8.3.4.36 BIG_384_58_isunity()

```
int BIG_384_58_isunity (
            BIG_384_58 x )
```

Parameters

x	a BIG number

Returns

1 if one, else returns 0

8.3.4.37 BIG_384_58_iszilch()

```
int BIG_384_58_iszilch (
            BIG_384_58 x )
```

Parameters

x	a BIG number

Returns

1 if zero, else returns 0

8.3.4.38 BIG_384_58_jacobi()

```
int BIG_384_58_jacobi (
            BIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	BIG number
y	BIG number

Returns

Jacobi symbol, -1,0 or 1

8.3.4.39 BIG_384_58_lastbits()

```
int BIG_384_58_lastbits (
            BIG_384_58 x,
            int n )
```

Parameters

x	BIG number
n	number of bits to return. Assumed to be less than BASEBITS.

Returns

least significant n bits as an integer

8.3.4.40 BIG_384_58_mod()

```
void BIG_384_58_mod (
            BIG_384_58 x,
            BIG_384_58 n )
```

Slow but rarely used

Parameters

x	BIG number to be reduced mod n
n	The modulus

8.3.4.41 BIG_384_58_mod2m()

```
void BIG_384_58_mod2m (
            BIG_384_58 x,
            int m )
```

Truncation

Parameters

x	BIG number, on reduced mod 2^m
m	new truncated size

8.3.4.42 BIG_384_58_moddiv()

```
void BIG_384_58_moddiv (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z,
            BIG_384_58 n )
```

Slow method for modular division

Parameters

x	BIG number, on exit = y/z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.3.4.43 BIG_384_58_modmul()

```
void BIG_384_58_modmul (
            BIG_384_58 x,
            BIG_384_58 y,
```

```
            BIG_384_58 z,
            BIG_384_58 n )
```

brief return NAF (Non-Adjacent-Form) value as +/- 1, 3 or 5, inputs must be normalised

Given x and 3*x extracts NAF value from given bit position, and returns number of bits processed, and number of trailing zeros detected if any param x BIG number param x3 BIG number, three times x param i bit position param nbs pointer to integer returning number of bits processed param nzs pointer to integer returning number of trailing 0s return + or - 1, 3 or 5Slow method for modular multiplication

Parameters

x	BIG number, on exit = y*z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.3.4.44 BIG_384_58_modneg()

```
void BIG_384_58_modneg (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 n )
```

Modular negation

Parameters

x	BIG number, on exit = -y mod n
y	BIG number
n	The BIG Modulus

8.3.4.45 BIG_384_58_modsqr()

```
void BIG_384_58_modsqr (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 n )
```

Slow method for modular squaring

Parameters

x	BIG number, on exit = y^2 mod n
y	BIG number
n	The BIG Modulus

8.3.4.46 BIG_384_58_monty()

```
void BIG_384_58_monty (
            BIG_384_58 a,
            BIG_384_58 md,
            chunk MC,
            DBIG_384_58 d )
```

Parameters

a	BIG number, reduction of a BIG
md	BIG number, the modulus
MC	the Montgomery Constant
d	DBIG number to be reduced

8.3.4.47 BIG_384_58_mul()

```
void BIG_384_58_mul (
            DBIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z )
```

Parameters

x	DBIG number, product of other two
y	BIG number
z	BIG number

8.3.4.48 BIG_384_58_nbits()

```
int BIG_384_58_nbits (
            BIG_384_58 x )
```

Parameters

x	BIG number

Returns

Number of bits in x

8.3.4.49 BIG_384_58_norm()

```
chunk BIG_384_58_norm (
            BIG_384_58 x )
```

All digits of the input BIG are reduced mod 2^BASEBITS

Parameters

x	BIG number to be normalised

8.3.4.50 BIG_384_58_one()

```
void BIG_384_58_one (
            BIG_384_58 x )
```

Parameters

x	BIG number to be set to one.

8.3.4.51 BIG_384_58_or()

```
void BIG_384_58_or (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z )
```

Parameters

x	BIG number, or of other two
y	BIG number
z	BIG number

8.3.4.52 BIG_384_58_output()

```
void BIG_384_58_output (
            BIG_384_58 x )
```

Parameters

x	a BIG number

8.3.4.53 BIG_384_58_parity()

```
int BIG_384_58_parity (
            BIG_384_58 x )
```

Parameters

x	BIG number

Returns

0 or 1

8.3.4.54 BIG_384_58_pmul()

```
chunk BIG_384_58_pmul (
            BIG_384_58 x,
            BIG_384_58 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

Returns

Overflowing bits

8.3.4.55 BIG_384_58_pxmul()

```
void BIG_384_58_pxmul (
            DBIG_384_58 x,
            BIG_384_58 y,
            int i )
```

Parameters

x	DBIG number, product of other two
y	BIG number
i	small integer

8.3.4.56 BIG_384_58_random()

```
void BIG_384_58_random (
            BIG_384_58 x,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
r	A pointer to a Cryptographically Secure Random Number Generator

8.3.4.57 BIG_384_58_randomnum()

```
void BIG_384_58_randomnum (
            BIG_384_58 x,
            BIG_384_58 n,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
n	The modulus
r	A pointer to a Cryptographically Secure Random Number Generator

8.3.4.58 BIG_384_58_rawoutput()

```
void BIG_384_58_rawoutput (
            BIG_384_58 x )
```

Parameters

x	a BIG number

8.3.4.59 BIG_384_58_rcopy()

```
void BIG_384_58_rcopy (
```

```
            BIG_384_58 x,
            const BIG_384_58 y )
```

Parameters

x	BIG number
y	BIG number in ROM

8.3.4.60 BIG_384_58_sdcopy()

```
void BIG_384_58_sdcopy (
            BIG_384_58 x,
            DBIG_384_58 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.3.4.61 BIG_384_58_sdiv()

```
void BIG_384_58_sdiv (
            BIG_384_58 x,
            BIG_384_58 n )
```

Slow but rarely used

Parameters

x	BIG number to be divided by n
n	The Divisor

8.3.4.62 BIG_384_58_sducopy()

```
void BIG_384_58_sducopy (
            BIG_384_58 x,
            DBIG_384_58 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.3.4.63 BIG_384_58_shl()

```
void BIG_384_58_shl (
            BIG_384_58 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.3.4.64 BIG_384_58_shr()

```
void BIG_384_58_shr (
            BIG_384_58 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.3.4.65 BIG_384_58_smul()

```
void BIG_384_58_smul (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z )
```

Note that the product must fit into a BIG, and x must be distinct from y and z

Parameters

x	BIG number, product of other two
y	BIG number
z	BIG number

8.3.4.66 BIG_384_58_split()

```
chunk BIG_384_58_split (
```

```
            BIG_384_58 x,
            BIG_384_58 y,
            DBIG_384_58 z,
            int s )
```

Internal function. The value of s must be approximately in the middle of the DBIG. Typically used to extract z mod 2^MODBITS and z/2^MODBITS

Parameters

x	BIG number, top half of z
y	BIG number, bottom half of z
z	DBIG number to be split in two.
s	Bit position at which to split

Returns

carry-out from top half

8.3.4.67 BIG_384_58_sqr()

```
void BIG_384_58_sqr (
            DBIG_384_58 x,
            BIG_384_58 y )
```

Parameters

x	DBIG number, square of a BIG
y	BIG number to be squared

8.3.4.68 BIG_384_58_ssn()

```
int BIG_384_58_ssn (
            BIG_384_58 r,
            BIG_384_58 a,
            BIG_384_58 m )
```

Parameters

r	BIG number normalised output
a	BIG number to be subtracted from
m	BIG number to be shifted and subtracted

Returns

sign of r

8.3.4.69 BIG_384_58_sub()

```
void BIG_384_58_sub (
            BIG_384_58 x,
            BIG_384_58 y,
            BIG_384_58 z )
```

Parameters

x	BIG number, difference of other two - output not normalised
y	BIG number
z	BIG number

8.3.4.70 BIG_384_58_toBytes()

```
void BIG_384_58_toBytes (
            char * a,
            BIG_384_58 x )
```

Parameters

a	byte array
x	BIG number

8.3.4.71 BIG_384_58_zero()

```
void BIG_384_58_zero (
            BIG_384_58 x )
```

Parameters

x	BIG number to be set to zero

8.4 big_512_60.h File Reference

BIG Header File.

```
#include <stdio.h>
#include <stdlib.h>
#include <inttypes.h>
#include "arch.h"
#include "amcl.h"
#include "config_big_512_60.h"
```

Macros

- #define BIGBITS_512_60 (8∗MODBYTES_512_60)
- #define NLEN_512_60 (1+((8∗MODBYTES_512_60-1)/BASEBITS_512_60))
- #define DNLEN_512_60 2∗NLEN_512_60
- #define BMASK_512_60 (((chunk)1<<BASEBITS_512_60)-1)
- #define NEXCESS_512_60 (1<<(CHUNK-BASEBITS_512_60-1))
- #define HBITS_512_60 (BASEBITS_512_60/2)
- #define HMASK_512_60 (((chunk)1<<HBITS_512_60)-1)

Typedefs

- typedef chunk BIG_512_60[NLEN_512_60]
- typedef chunk DBIG_512_60[DNLEN_512_60]

Functions

- int BIG_512_60_iszilch (BIG_512_60 x)

  Tests for BIG equal to zero.
- int BIG_512_60_isunity (BIG_512_60 x)

  Tests for BIG equal to one.
- int BIG_512_60_diszilch (DBIG_512_60 x)

  Tests for DBIG equal to zero.
- void BIG_512_60_output (BIG_512_60 x)

  Outputs a BIG number to the console.
- void BIG_512_60_rawoutput (BIG_512_60 x)

  Outputs a BIG number to the console in raw form (for debugging)
- void BIG_512_60_cswap (BIG_512_60 x, BIG_512_60 y, int s)

  Conditional constant time swap of two BIG numbers.
- void BIG_512_60_cmove (BIG_512_60 x, BIG_512_60 y, int s)

  Conditional copy of BIG number.
- void BIG_512_60_dcmove (BIG_512_60 x, BIG_512_60 y, int s)

  Conditional copy of DBIG number.
- void BIG_512_60_toBytes (char ∗a, BIG_512_60 x)

  Convert from BIG number to byte array.
- void BIG_512_60_fromBytes (BIG_512_60 x, char ∗a)

  Convert to BIG number from byte array.
- void BIG_512_60_fromBytesLen (BIG_512_60 x, char ∗a, int s)

  Convert to BIG number from byte array of given length.
- void BIG_512_60_dfromBytesLen (DBIG_512_60 x, char ∗a, int s)

  Convert to DBIG number from byte array of given length.
- void BIG_512_60_doutput (DBIG_512_60 x)

Outputs a DBIG number to the console.
- void BIG_512_60_drawoutput (DBIG_512_60 x)

  Outputs a DBIG number to the console.
- void BIG_512_60_rcopy (BIG_512_60 x, const BIG_512_60 y)

  Copy BIG from Read-Only Memory to a BIG.
- void BIG_512_60_copy (BIG_512_60 x, BIG_512_60 y)

  Copy BIG to another BIG.
- void BIG_512_60_dcopy (DBIG_512_60 x, DBIG_512_60 y)

  Copy DBIG to another DBIG.
- void BIG_512_60_dsucopy (DBIG_512_60 x, BIG_512_60 y)

  Copy BIG to upper half of DBIG.
- void BIG_512_60_dscopy (DBIG_512_60 x, BIG_512_60 y)

  Copy BIG to lower half of DBIG.
- void BIG_512_60_sdcopy (BIG_512_60 x, DBIG_512_60 y)

  Copy lower half of DBIG to a BIG.
- void BIG_512_60_sducopy (BIG_512_60 x, DBIG_512_60 y)

  Copy upper half of DBIG to a BIG.
- void BIG_512_60_zero (BIG_512_60 x)

  Set BIG to zero.
- void BIG_512_60_dzero (DBIG_512_60 x)

  Set DBIG to zero.
- void BIG_512_60_one (BIG_512_60 x)

  Set BIG to one (unity)
- void BIG_512_60_invmod2m (BIG_512_60 x)

  Set BIG to inverse mod 2^256.
- void BIG_512_60_add (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z)

  Set BIG to sum of two BIGs - output not normalised.
- void BIG_512_60_or (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z)

  Set BIG to logical or of two BIGs - output normalised.
- void BIG_512_60_inc (BIG_512_60 x, int i)

  Increment BIG by a small integer - output not normalised.
- void BIG_512_60_sub (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z)

  Set BIG to difference of two BIGs.
- void BIG_512_60_dec (BIG_512_60 x, int i)

  Decrement BIG by a small integer - output not normalised.
- void BIG_512_60_dadd (DBIG_512_60 x, DBIG_512_60 y, DBIG_512_60 z)

  Set DBIG to sum of two DBIGs.
- void BIG_512_60_dsub (DBIG_512_60 x, DBIG_512_60 y, DBIG_512_60 z)

  Set DBIG to difference of two DBIGs.
- void BIG_512_60_imul (BIG_512_60 x, BIG_512_60 y, int i)

  Multiply BIG by a small integer - output not normalised.
- chunk BIG_512_60_pmul (BIG_512_60 x, BIG_512_60 y, int i)

  Multiply BIG by not-so-small small integer - output normalised.
- int BIG_512_60_div3 (BIG_512_60 x)

  Divide BIG by 3 - output normalised.
- void BIG_512_60_pxmul (DBIG_512_60 x, BIG_512_60 y, int i)

  Multiply BIG by even bigger small integer resulting in a DBIG - output normalised.
- void BIG_512_60_mul (DBIG_512_60 x, BIG_512_60 y, BIG_512_60 z)

  Multiply BIG by another BIG resulting in DBIG - inputs normalised and output normalised.
- void BIG_512_60_smul (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z)

  Multiply BIG by another BIG resulting in another BIG - inputs normalised and output normalised.

- void BIG_512_60_sqr (DBIG_512_60 x, BIG_512_60 y)

  Square BIG resulting in a DBIG - input normalised and output normalised.
- void BIG_512_60_monty (BIG_512_60 a, BIG_512_60 md, chunk MC, DBIG_512_60 d)

  Montgomery reduction of a DBIG to a BIG - input normalised and output normalised.
- void BIG_512_60_shl (BIG_512_60 x, int s)

  Shifts a BIG left by any number of bits - input must be normalised, output normalised.
- int BIG_512_60_fshl (BIG_512_60 x, int s)

  Fast shifts a BIG left by a small number of bits - input must be normalised, output will be normalised.
- void BIG_512_60_dshl (DBIG_512_60 x, int s)

  Shifts a DBIG left by any number of bits - input must be normalised, output normalised.
- void BIG_512_60_shr (BIG_512_60 x, int s)

  Shifts a BIG right by any number of bits - input must be normalised, output normalised.
- int BIG_512_60_ssn (BIG_512_60 r, BIG_512_60 a, BIG_512_60 m)

  Fast time-critical combined shift by 1 bit, subtract and normalise.
- int BIG_512_60_fshr (BIG_512_60 x, int s)

  Fast shifts a BIG right by a small number of bits - input must be normalised, output will be normalised.
- void BIG_512_60_dshr (DBIG_512_60 x, int s)

  Shifts a DBIG right by any number of bits - input must be normalised, output normalised.
- chunk BIG_512_60_split (BIG_512_60 x, BIG_512_60 y, DBIG_512_60 z, int s)

  Splits a DBIG into two BIGs - input must be normalised, outputs normalised.
- chunk BIG_512_60_norm (BIG_512_60 x)

  Normalizes a BIG number - output normalised.
- void BIG_512_60_dnorm (DBIG_512_60 x)

  Normalizes a DBIG number - output normalised.
- int BIG_512_60_comp (BIG_512_60 x, BIG_512_60 y)

  Compares two BIG numbers. Inputs must be normalised externally.
- int BIG_512_60_dcomp (DBIG_512_60 x, DBIG_512_60 y)

  Compares two DBIG numbers. Inputs must be normalised externally.
- int BIG_512_60_nbits (BIG_512_60 x)

  Calculate number of bits in a BIG - output normalised.
- int BIG_512_60_dnbits (DBIG_512_60 x)

  Calculate number of bits in a DBIG - output normalised.
- void BIG_512_60_mod (BIG_512_60 x, BIG_512_60 n)

  Reduce x mod n - input and output normalised.
- void BIG_512_60_sdiv (BIG_512_60 x, BIG_512_60 n)

  Divide x by n - output normalised.
- void BIG_512_60_dmod (BIG_512_60 x, DBIG_512_60 y, BIG_512_60 n)

  x=y mod n - output normalised
- void BIG_512_60_ddiv (BIG_512_60 x, DBIG_512_60 y, BIG_512_60 n)

  x=y/n - output normalised
- int BIG_512_60_parity (BIG_512_60 x)

  return parity of BIG, that is the least significant bit
- int BIG_512_60_bit (BIG_512_60 x, int i)

  return i-th of BIG
- int BIG_512_60_lastbits (BIG_512_60 x, int n)

  return least significant bits of a BIG
- void BIG_512_60_random (BIG_512_60 x, csprng ∗r)

  Create a random BIG from a random number generator.
- void BIG_512_60_randomnum (BIG_512_60 x, BIG_512_60 n, csprng ∗r)

  Create an unbiased random BIG from a random number generator, reduced with respect to a modulus.
- void BIG_512_60_modmul (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z, BIG_512_60 n)

Calculate x=y∗z mod n.
- void BIG_512_60_moddiv (BIG_512_60 x, BIG_512_60 y, BIG_512_60 z, BIG_512_60 n)

  Calculate x=y/z mod n.
- void BIG_512_60_modsqr (BIG_512_60 x, BIG_512_60 y, BIG_512_60 n)

  Calculate x=y^2 mod n.
- void BIG_512_60_modneg (BIG_512_60 x, BIG_512_60 y, BIG_512_60 n)

  Calculate x=-y mod n.
- int BIG_512_60_jacobi (BIG_512_60 x, BIG_512_60 y)

  Calculate jacobi Symbol (x/y)
- void BIG_512_60_invmodp (BIG_512_60 x, BIG_512_60 y, BIG_512_60 n)

  Calculate x=1/y mod n.
- void BIG_512_60_mod2m (BIG_512_60 x, int m)

  Calculate x=x mod 2^m.
- void BIG_512_60_dmod2m (DBIG_512_60 x, int m)

  Calculate x=x mod 2^m.

8.4.1 Detailed Description

Author

Mike Scott

8.4.2 Macro Definition Documentation

8.4.2.1 BIGBITS_512_60

```
#define BIGBITS_512_60 (8*MODBYTES_512_60)
```

Length in bits

8.4.2.2 BMASK_512_60

```
#define BMASK_512_60 (((chunk)1<<BASEBITS_512_60)-1)
```

Mask = 2^BASEBITS-1

8.4.2.3 DNLEN_512_60

```
#define DNLEN_512_60 2*NLEN_512_60
```

Double length in bytes

8.4.2.4 HBITS_512_60

```
#define HBITS_512_60 (BASEBITS_512_60/2)
```

Number of bits in number base divided by 2

8.4.2.5 HMASK_512_60

```
#define HMASK_512_60 (((chunk)1<<HBITS_512_60)-1)
```

Mask = 2^HBITS-1

8.4.2.6 NEXCESS_512_60

```
#define NEXCESS_512_60 (1<<(CHUNK-BASEBITS_512_60-1))
```

2^(CHUNK-BASEBITS-1) - digit cannot be multiplied by more than this before normalisation

8.4.2.7 NLEN_512_60

```
#define NLEN_512_60 (1+((8*MODBYTES_512_60-1)/BASEBITS_512_60))
```

length in bytes

8.4.3 Typedef Documentation

8.4.3.1 BIG_512_60

```
typedef chunk BIG_512_60[NLEN_512_60]
```

Define type BIG as array of chunks

8.4.3.2 DBIG_512_60

```
typedef chunk DBIG_512_60[DNLEN_512_60]
```

Define type DBIG as array of chunks

8.4.4 Function Documentation

8.4.4.1 BIG_512_60_add()

```
void BIG_512_60_add (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z )
```

Parameters

x	BIG number, sum of other two
y	BIG number
z	BIG number

8.4.4.2 BIG_512_60_bit()

```
int BIG_512_60_bit (
            BIG_512_60 x,
            int i )
```

Parameters

x	BIG number
i	the bit of x to be returned

Returns

0 or 1

8.4.4.3 BIG_512_60_cmove()

```
void BIG_512_60_cmove (
            BIG_512_60 x,
            BIG_512_60 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a BIG number
y	another BIG number
s	copy takes place if not equal to 0

8.4.4.4 BIG_512_60_comp()

```
int BIG_512_60_comp (
            BIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	first BIG number to be compared
y	second BIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.4.4.5 BIG_512_60_copy()

```
void BIG_512_60_copy (
            BIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	BIG number
y	BIG number to be copied

8.4.4.6 BIG_512_60_cswap()

```
void BIG_512_60_cswap (
            BIG_512_60 x,
            BIG_512_60 y,
            int s )
```

Conditionally swaps parameters in constant time (without branching)

Parameters

x	a BIG number
y	another BIG number
s	swap takes place if not equal to 0

8.4.4.7 BIG_512_60_dadd()

```
void BIG_512_60_dadd (
            DBIG_512_60 x,
            DBIG_512_60 y,
            DBIG_512_60 z )
```

Parameters

x	DBIG number, sum of other two - output not normalised
y	DBIG number
z	DBIG number

8.4.4.8 BIG_512_60_dcmove()

```
void BIG_512_60_dcmove (
            BIG_512_60 x,
            BIG_512_60 y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	a DBIG number
y	another DBIG number
s	copy takes place if not equal to 0

8.4.4.9 BIG_512_60_dcomp()

```
int BIG_512_60_dcomp (
            DBIG_512_60 x,
            DBIG_512_60 y )
```

Parameters

x	first DBIG number to be compared
y	second DBIG number to be compared

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.4.4.10 BIG_512_60_dcopy()

```
void BIG_512_60_dcopy (
            DBIG_512_60 x,
            DBIG_512_60 y )
```

Parameters

x	DBIG number
y	DBIG number to be copied

8.4.4.11 BIG_512_60_ddiv()

```
void BIG_512_60_ddiv (
            BIG_512_60 x,
            DBIG_512_60 y,
            BIG_512_60 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y/n
y	DBIG number
n	Modulus

8.4.4.12 BIG_512_60_dec()

```
void BIG_512_60_dec (
            BIG_512_60 x,
            int i )
```

Parameters

x	BIG number to be decremented
i	integer

8.4.4.13 BIG_512_60_dfromBytesLen()

```
void BIG_512_60_dfromBytesLen (
            DBIG_512_60 x,
            char * a,
            int s )
```

Parameters

x	DBIG number
a	byte array
s	byte array length

8.4.4.14 BIG_512_60_diszilch()

```
int BIG_512_60_diszilch (
            DBIG_512_60 x )
```

Parameters

x	a DBIG number

Returns

1 if zero, else returns 0

8.4.4.15 BIG_512_60_div3()

```
int BIG_512_60_div3 (
            BIG_512_60 x )
```

Parameters

x	BIG number

Returns

Remainder

8.4.4.16 BIG_512_60_dmod()

```
void BIG_512_60_dmod (
            BIG_512_60 x,
            DBIG_512_60 y,
            BIG_512_60 n )
```

Slow but rarely used. y is destroyed.

Parameters

x	BIG number, on exit = y mod n
y	DBIG number
n	Modulus

8.4.4.17 BIG_512_60_dmod2m()

```
void BIG_512_60_dmod2m (
            DBIG_512_60 x,
            int m )
```

Truncation

Parameters

x	DBIG number, on reduced mod 2^m
m	new truncated size

8.4.4.18 BIG_512_60_dnbits()

```
int BIG_512_60_dnbits (
            DBIG_512_60 x )
```

Parameters

x	DBIG number

Returns

Number of bits in x

8.4.4.19 BIG_512_60_dnorm()

```
void BIG_512_60_dnorm (
            DBIG_512_60 x )
```

All digits of the input DBIG are reduced mod 2^BASEBITS

Parameters

x	DBIG number to be normalised

8.4.4.20 BIG_512_60_doutput()

```
void BIG_512_60_doutput (
```

```
            DBIG_512_60 x )
```

Parameters

x	a DBIG number

8.4.4.21 BIG_512_60_drawoutput()

```
void BIG_512_60_drawoutput (
            DBIG_512_60 x )
```

Parameters

x	a DBIG number

8.4.4.22 BIG_512_60_dscopy()

```
void BIG_512_60_dscopy (
            DBIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.4.4.23 BIG_512_60_dshl()

```
void BIG_512_60_dshl (
            DBIG_512_60 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.4.4.24 BIG_512_60_dshr()

```
void BIG_512_60_dshr (
            DBIG_512_60 x,
            int s )
```

Parameters

x	DBIG number to be shifted
s	Number of bits to shift

8.4.4.25 BIG_512_60_dsub()

```
void BIG_512_60_dsub (
            DBIG_512_60 x,
            DBIG_512_60 y,
            DBIG_512_60 z )
```

Parameters

x	DBIG number, difference of other two - output not normalised
y	DBIG number
z	DBIG number

8.4.4.26 BIG_512_60_dsucopy()

```
void BIG_512_60_dsucopy (
            DBIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	DBIG number
y	BIG number to be copied

8.4.4.27 BIG_512_60_dzero()

```
void BIG_512_60_dzero (
            DBIG_512_60 x )
```

Parameters

x	DBIG number to be set to zero

8.4.4.28 BIG_512_60_fromBytes()

```
void BIG_512_60_fromBytes (
            BIG_512_60 x,
            char * a )
```

Parameters

x	BIG number
a	byte array

8.4.4.29 BIG_512_60_fromBytesLen()

```
void BIG_512_60_fromBytesLen (
            BIG_512_60 x,
            char * a,
            int s )
```

Parameters

x	BIG number
a	byte array
s	byte array length

8.4.4.30 BIG_512_60_fshl()

```
int BIG_512_60_fshl (
            BIG_512_60 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Overflow bits

8.4.4.31 BIG_512_60_fshr()

```
int BIG_512_60_fshr (
            BIG_512_60 x,
            int s )
```

The number of bits to be shifted must be less than BASEBITS

Parameters

x	BIG number to be shifted
s	Number of bits to shift

Returns

Shifted out bits

8.4.4.32 BIG_512_60_imul()

```
void BIG_512_60_imul (
            BIG_512_60 x,
            BIG_512_60 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

8.4.4.33 BIG_512_60_inc()

```
void BIG_512_60_inc (
            BIG_512_60 x,
            int i )
```

Parameters

x	BIG number to be incremented
i	integer

8.4.4.34 BIG_512_60_invmod2m()

```
void BIG_512_60_invmod2m (
            BIG_512_60 x )
```

Parameters

x	BIG number to be inverted

8.4.4.35 BIG_512_60_invmodp()

```
void BIG_512_60_invmodp (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 n )
```

Modular Inversion - This is slow. Uses binary method.

Parameters

x	BIG number, on exit = 1/y mod n
y	BIG number
n	The BIG Modulus

8.4.4.36 BIG_512_60_isunity()

```
int BIG_512_60_isunity (
            BIG_512_60 x )
```

Parameters

x	a BIG number

Returns

1 if one, else returns 0

8.4.4.37 BIG_512_60_iszilch()

```
int BIG_512_60_iszilch (
            BIG_512_60 x )
```

Parameters

x	a BIG number

Returns

1 if zero, else returns 0

8.4.4.38 BIG_512_60_jacobi()

```
int BIG_512_60_jacobi (
            BIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	BIG number
y	BIG number

Returns

Jacobi symbol, -1,0 or 1

8.4.4.39 BIG_512_60_lastbits()

```
int BIG_512_60_lastbits (
            BIG_512_60 x,
            int n )
```

Parameters

x	BIG number
n	number of bits to return. Assumed to be less than BASEBITS.

Returns

least significant n bits as an integer

8.4.4.40 BIG_512_60_mod()

```
void BIG_512_60_mod (
            BIG_512_60 x,
            BIG_512_60 n )
```

Slow but rarely used

Parameters

x	BIG number to be reduced mod n
n	The modulus

8.4.4.41 BIG_512_60_mod2m()

```
void BIG_512_60_mod2m (
            BIG_512_60 x,
            int m )
```

Truncation

Parameters

x	BIG number, on reduced mod 2^m
m	new truncated size

8.4.4.42 BIG_512_60_moddiv()

```
void BIG_512_60_moddiv (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z,
            BIG_512_60 n )
```

Slow method for modular division

Parameters

x	BIG number, on exit = y/z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.4.4.43 BIG_512_60_modmul()

```
void BIG_512_60_modmul (
            BIG_512_60 x,
            BIG_512_60 y,
```

```
BIG_512_60 z,
BIG_512_60 n )
```

brief return NAF (Non-Adjacent-Form) value as +/- 1, 3 or 5, inputs must be normalised

Given x and 3∗x extracts NAF value from given bit position, and returns number of bits processed, and number of trailing zeros detected if any param x BIG number param x3 BIG number, three times x param i bit position param nbs pointer to integer returning number of bits processed param nzs pointer to integer returning number of trailing 0s return + or - 1, 3 or 5Slow method for modular multiplication

Parameters

x	BIG number, on exit = y∗z mod n
y	BIG number
z	BIG number
n	The BIG Modulus

8.4.4.44 BIG_512_60_modneg()

```
void BIG_512_60_modneg (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 n )
```

Modular negation

Parameters

x	BIG number, on exit = -y mod n
y	BIG number
n	The BIG Modulus

8.4.4.45 BIG_512_60_modsqr()

```
void BIG_512_60_modsqr (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 n )
```

Slow method for modular squaring

Parameters

x	BIG number, on exit = y^2 mod n
y	BIG number
n	The BIG Modulus

8.4.4.46 BIG_512_60_monty()

```
void BIG_512_60_monty (
            BIG_512_60 a,
            BIG_512_60 md,
            chunk MC,
            DBIG_512_60 d )
```

Parameters

a	BIG number, reduction of a BIG
md	BIG number, the modulus
MC	the Montgomery Constant
d	DBIG number to be reduced

8.4.4.47 BIG_512_60_mul()

```
void BIG_512_60_mul (
            DBIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z )
```

Parameters

x	DBIG number, product of other two
y	BIG number
z	BIG number

8.4.4.48 BIG_512_60_nbits()

```
int BIG_512_60_nbits (
            BIG_512_60 x )
```

Parameters

x	BIG number

Returns

Number of bits in x

8.4.4.49 BIG_512_60_norm()

```
chunk BIG_512_60_norm (
            BIG_512_60 x )
```

All digits of the input BIG are reduced mod 2^BASEBITS

Parameters

x	BIG number to be normalised

8.4.4.50 BIG_512_60_one()

```
void BIG_512_60_one (
            BIG_512_60 x )
```

Parameters

x	BIG number to be set to one.

8.4.4.51 BIG_512_60_or()

```
void BIG_512_60_or (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z )
```

Parameters

x	BIG number, or of other two
y	BIG number
z	BIG number

8.4.4.52 BIG_512_60_output()

```
void BIG_512_60_output (
            BIG_512_60 x )
```

Parameters

x	a BIG number

8.4.4.53 BIG_512_60_parity()

```
int BIG_512_60_parity (
            BIG_512_60 x )
```

Parameters

x	BIG number

Returns

0 or 1

8.4.4.54 BIG_512_60_pmul()

```
chunk BIG_512_60_pmul (
            BIG_512_60 x,
            BIG_512_60 y,
            int i )
```

Parameters

x	BIG number, product of other two
y	BIG number
i	small integer

Returns

Overflowing bits

8.4.4.55 BIG_512_60_pxmul()

```
void BIG_512_60_pxmul (
            DBIG_512_60 x,
            BIG_512_60 y,
            int i )
```

Parameters

x	DBIG number, product of other two
y	BIG number
i	small integer

8.4.4.56 BIG_512_60_random()

```
void BIG_512_60_random (
            BIG_512_60 x,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
r	A pointer to a Cryptographically Secure Random Number Generator

8.4.4.57 BIG_512_60_randomnum()

```
void BIG_512_60_randomnum (
            BIG_512_60 x,
            BIG_512_60 n,
            csprng * r )
```

Assumes that the random number generator has been suitably initialised

Parameters

x	BIG number, on exit a random number
n	The modulus
r	A pointer to a Cryptographically Secure Random Number Generator

8.4.4.58 BIG_512_60_rawoutput()

```
void BIG_512_60_rawoutput (
            BIG_512_60 x )
```

Parameters

x	a BIG number

8.4.4.59 BIG_512_60_rcopy()

```
void BIG_512_60_rcopy (
```

```
            BIG_512_60 x,
            const BIG_512_60 y )
```

Parameters

x	BIG number
y	BIG number in ROM

8.4.4.60 BIG_512_60_sdcopy()

```
void BIG_512_60_sdcopy (
            BIG_512_60 x,
            DBIG_512_60 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.4.4.61 BIG_512_60_sdiv()

```
void BIG_512_60_sdiv (
            BIG_512_60 x,
            BIG_512_60 n )
```

Slow but rarely used

Parameters

x	BIG number to be divided by n
n	The Divisor

8.4.4.62 BIG_512_60_sducopy()

```
void BIG_512_60_sducopy (
            BIG_512_60 x,
            DBIG_512_60 y )
```

Parameters

x	BIG number
y	DBIG number to be copied

8.4.4.63 BIG_512_60_shl()

```
void BIG_512_60_shl (
            BIG_512_60 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.4.4.64 BIG_512_60_shr()

```
void BIG_512_60_shr (
            BIG_512_60 x,
            int s )
```

Parameters

x	BIG number to be shifted
s	Number of bits to shift

8.4.4.65 BIG_512_60_smul()

```
void BIG_512_60_smul (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z )
```

Note that the product must fit into a BIG, and x must be distinct from y and z

Parameters

x	BIG number, product of other two
y	BIG number
z	BIG number

8.4.4.66 BIG_512_60_split()

```
chunk BIG_512_60_split (
```

```
            BIG_512_60 x,
            BIG_512_60 y,
            DBIG_512_60 z,
            int s )
```

Internal function. The value of s must be approximately in the middle of the DBIG. Typically used to extract z mod 2^MODBITS and z/2^MODBITS

Parameters

x	BIG number, top half of z
y	BIG number, bottom half of z
z	DBIG number to be split in two.
s	Bit position at which to split

Returns

carry-out from top half

8.4.4.67 BIG_512_60_sqr()

```
void BIG_512_60_sqr (
            DBIG_512_60 x,
            BIG_512_60 y )
```

Parameters

x	DBIG number, square of a BIG
y	BIG number to be squared

8.4.4.68 BIG_512_60_ssn()

```
int BIG_512_60_ssn (
            BIG_512_60 r,
            BIG_512_60 a,
            BIG_512_60 m )
```

Parameters

r	BIG number normalised output
a	BIG number to be subtracted from
m	BIG number to be shifted and subtracted

Returns

sign of r

8.4.4.69 BIG_512_60_sub()

```
void BIG_512_60_sub (
            BIG_512_60 x,
            BIG_512_60 y,
            BIG_512_60 z )
```

Parameters

x	BIG number, difference of other two - output not normalised
y	BIG number
z	BIG number

8.4.4.70 BIG_512_60_toBytes()

```
void BIG_512_60_toBytes (
            char * a,
            BIG_512_60 x )
```

Parameters

a	byte array
x	BIG number

8.4.4.71 BIG_512_60_zero()

```
void BIG_512_60_zero (
            BIG_512_60 x )
```

Parameters

x	BIG number to be set to zero

8.5 bls_BLS381.h File Reference

BLS Header file.

```
#include "pair_BLS381.h"
```

Macros

- #define BGS_BLS381 MODBYTES_384_58
- #define BFS_BLS381 MODBYTES_384_58
- #define BLS_OK 0
- #define BLS_FAIL 41
- #define BLS_INVALID_G1 42
- #define BLS_INVALID_G2 43

Functions

- int BLS_BLS381_KEY_PAIR_GENERATE (csprng ∗RNG, octet ∗S, octet ∗W)
  Generate Key Pair.
- int BLS_BLS381_SIGN (octet ∗SIG, octet ∗M, octet ∗S)
  Calculate a signature.
- int BLS_BLS381_VERIFY (octet ∗SIG, octet ∗M, octet ∗W)
  Verify a signature.
- int BLS_BLS381_ADD_G1 (octet ∗R1, octet ∗R2, octet ∗R)
  Add two members from the group G1.
- int BLS_BLS381_ADD_G2 (octet ∗W1, octet ∗W2, octet ∗W)
  Add two members from the group G2.
- int BLS_BLS381_MAKE_SHARES (int k, int n, csprng ∗RNG, octet ∗X, octet ∗Y, octet ∗SKI, octet ∗SKO)
  Use Shamir's secret sharing to distribute BLS secret keys.
- int BLS_BLS381_RECOVER_SECRET (int k, octet ∗X, octet ∗Y, octet ∗SK)
  Use Shamir's secret sharing to recover a BLS secret key.
- int BLS_BLS381_RECOVER_SIGNATURE (int k, octet ∗X, octet ∗Y, octet ∗SIG)
  Use Shamir's secret sharing to recover a BLS signature.

8.5.1 Detailed Description

Author

Mike Scott

Date

28th Novemebr 2018 Allows some user configuration defines structures declares functions

8.5.2 Macro Definition Documentation

8.5.2.1 BFS_BLS381

```
#define BFS_BLS381 MODBYTES_384_58
```

BLS Field Size

8.5.2.2 BGS_BLS381

```
#define BGS_BLS381 MODBYTES_384_58
```

BLS Group Size

8.5.2.3 BLS_FAIL

```
#define BLS_FAIL 41
```

Invalid signature

8.5.2.4 BLS_INVALID_G1

```
#define BLS_INVALID_G1 42
```

Not a valid G1 point on the curve

8.5.2.5 BLS_INVALID_G2

```
#define BLS_INVALID_G2 43
```

Not a valid G2 point on the curve

8.5.2.6 BLS_OK

```
#define BLS_OK 0
```

Function completed without error

8.5.3 Function Documentation

8.5.3.1 BLS_BLS381_ADD_G1()

```
int BLS_BLS381_ADD_G1 (
            octet * R1,
            octet * R2,
            octet * R )
```

Parameters

R1	member of G1
R2	member of G1
R	member of G1. R = R1+R2

Returns

Zero for success or else an error code

8.5.3.2 BLS_BLS381_ADD_G2()

```
int BLS_BLS381_ADD_G2 (
            octet * W1,
            octet * W2,
            octet * W )
```

Parameters

W1	member of G2
W2	member of G2
W	member of G2. W = W1+W2

Returns

Zero for success or else an error code

8.5.3.3 BLS_BLS381_KEY_PAIR_GENERATE()

```
int BLS_BLS381_KEY_PAIR_GENERATE (
            csprng * RNG,
            octet * S,
            octet * W )
```

Parameters

RNG	Pointer to a cryptographically secure random number generator
S	Private key. Generated externally if RNG set to NULL
W	Public Key. W = S∗G, where G is fixed generator

Returns

Zero for success or else an error code

8.5.3.4 BLS_BLS381_MAKE_SHARES()

```
int BLS_BLS381_MAKE_SHARES (
            int k,
```

```
int n,
cspring * RNG,
octet * X,
octet * Y,
octet * SKI,
octet * SKO )
```

Parameters

k	Threshold
n	Number of shares
RNG	Pointer to a cryptographically secure random number generator
X	X values
Y	Y values. Valid BLS secret keys
SKI	Input secret key to be shared. Ignored if set to NULL
SKO	Secret key that is shared

Returns

Zero for success or else an error code

8.5.3.5 BLS_BLS381_RECOVER_SECRET()

```
int BLS_BLS381_RECOVER_SECRET (
    int k,
    octet * X,
    octet * Y,
    octet * SK )
```

Parameters

k	Threshold
X	X values
Y	Y values. Valid BLS secret keys
SK	Secret key that is recovered

Returns

Zero for success or else an error code

8.5.3.6 BLS_BLS381_RECOVER_SIGNATURE()

```
int BLS_BLS381_RECOVER_SIGNATURE (
    int k,
    octet * X,
    octet * Y,
    octet * SIG )
```

Parameters

k	Threshold
X	X values
Y	Y values. Valid BLS signatures
SIG	Signature that is recovered

Returns

Zero for success or else an error code

8.5.3.7 BLS_BLS381_SIGN()

```
int BLS_BLS381_SIGN (
            octet * SIG,
            octet * M,
            octet * S )
```

Parameters

SIG	signature
M	message to be signed
S	Private key

Returns

Zero for success or else an error code

8.5.3.8 BLS_BLS381_VERIFY()

```
int BLS_BLS381_VERIFY (
            octet * SIG,
            octet * M,
            octet * W )
```

Parameters

SIG	signature
M	message whose signature is to be verified.
W	Public key

Returns

Zero for success or else an error code

8.6 config_big_1024_58.h File Reference

Config BIG Header File.

```
#include "amcl.h"
```

Macros

- #define MODBYTES_1024_58 128
- #define BASEBITS_1024_58 58

8.6.1 Detailed Description

Author

Mike Scott

8.6.2 Macro Definition Documentation

8.6.2.1 BASEBITS_1024_58

```
#define BASEBITS_1024_58 58
```

Numbers represented to base 2*BASEBITS

8.6.2.2 MODBYTES_1024_58

```
#define MODBYTES_1024_58 128
```

Number of bytes in Modulus

8.7 config_big_384_58.h File Reference

Config BIG Header File.

```
#include "amcl.h"
```

Macros

- #define MODBYTES_384_58 48
- #define BASEBITS_384_58 58

8.7.1 Detailed Description

Author

Mike Scott

8.7.2 Macro Definition Documentation

8.7.2.1 BASEBITS_384_58

```
#define BASEBITS_384_58 58
```

Numbers represented to base 2*BASEBITS

8.7.2.2 MODBYTES_384_58

```
#define MODBYTES_384_58 48
```

Number of bytes in Modulus

8.8 config_big_512_60.h File Reference

Config BIG Header File.

```
#include "amcl.h"
```

Macros

- #define MODBYTES_512_60 64
- #define BASEBITS_512_60 60

8.8.1 Detailed Description

Author

Mike Scott

8.8.2 Macro Definition Documentation

8.8.2.1 BASEBITS_512_60

```
#define BASEBITS_512_60 60
```

Numbers represented to base 2*BASEBITS

8.8.2.2 MODBYTES_512_60

```
#define MODBYTES_512_60 64
```

Number of bytes in Modulus

8.9 config_ff_2048.h File Reference

COnfig FF Header File.

```
#include "amcl.h"
#include "config_big_1024_58.h"
```

Macros

- #define FFLEN_2048 2

8.9.1 Detailed Description

Author

Mike Scott

8.9.2 Macro Definition Documentation

8.9.2.1 FFLEN_2048

```
#define FFLEN_2048 2
```

2^n multiplier of BIGBITS to specify supported Finite Field size, e.g 2048=256*2^3 where BIGBITS=256

8.10 config_ff_4096.h File Reference

COnfig FF Header File.

```
#include "amcl.h"
#include "config_big_512_60.h"
```

Macros

- #define FFLEN_4096 8

8.10.1 Detailed Description

Author

Mike Scott

8.10.2 Macro Definition Documentation

8.10.2.1 FFLEN_4096

```
#define FFLEN_4096 8
```

2^n multiplier of BIGBITS to specify supported Finite Field size, e.g 2048=256*2^3 where BIGBITS=256

8.11 ecdh_BLS381.h File Reference

ECDH Header file for implementation of standard EC protocols.

```
#include "ecp_BLS381.h"
#include "ecdh_support.h"
```

Macros

- #define EGS_BLS381 MODBYTES_384_58
- #define EFS_BLS381 MODBYTES_384_58
- #define ECDH_OK 0
- #define ECDH_INVALID_PUBLIC_KEY -2
- #define ECDH_ERROR -3
- #define ECDH_INVALID -4

Functions

- int ECP_BLS381_KEY_PAIR_GENERATE (csprng *R, octet *s, octet *W)

  Generate an ECC public/private key pair.
- int ECP_BLS381_PUBLIC_KEY_VALIDATE (octet *W)

  Validate an ECC public key.
- int ECP_BLS381_SVDP_DH (octet *s, octet *W, octet *K)

  Generate Diffie-Hellman shared key.
- void ECP_BLS381_ECIES_ENCRYPT (int h, octet *P1, octet *P2, csprng *R, octet *W, octet *M, int len, octet *V, octet *C, octet *T)

  ECIES Encryption.
- int ECP_BLS381_ECIES_DECRYPT (int h, octet *P1, octet *P2, octet *V, octet *C, octet *T, octet *U, octet *M)

  ECIES Decryption.
- int ECP_BLS381_SP_DSA (int h, csprng *R, octet *k, octet *s, octet *M, octet *c, octet *d)

  ECDSA Signature.
- int ECP_BLS381_VP_DSA (int h, octet *W, octet *M, octet *c, octet *d)

  ECDSA Signature Verification.

8.11.1 Detailed Description

Author

Mike Scott

8.11.2 Macro Definition Documentation

8.11.2.1 ECDH_ERROR

```
#define ECDH_ERROR -3
```

ECDH Internal Error

8.11.2.2 ECDH_INVALID

```
#define ECDH_INVALID -4
```

ECDH Internal Error

8.11.2.3 ECDH_INVALID_PUBLIC_KEY

```
#define ECDH_INVALID_PUBLIC_KEY -2
```

Public Key is Invalid

8.11.2.4 ECDH_OK

```
#define ECDH_OK 0
```

Function completed without error

8.11.2.5 EFS_BLS381

```
#define EFS_BLS381 MODBYTES_384_58
```

ECC Field Size in bytes

8.11.2.6 EGS_BLS381

```
#define EGS_BLS381 MODBYTES_384_58
```

ECC Group Size in bytes

8.11.3 Function Documentation

8.11.3.1 ECP_BLS381_ECIES_DECRYPT()

```
int ECP_BLS381_ECIES_DECRYPT (
            int h,
            octet * P1,
            octet * P2,
            octet * V,
            octet * C,
            octet * T,
            octet * U,
            octet * M )
```

IEEE-1363 ECIES Decryption

Parameters

h	is the hash type
P1	input Key Derivation parameters
P2	input Encoding parameters
V	component of the input ciphertext
C	the input ciphertext
T	the input HMAC tag, part of the ciphertext
U	the input private key for decryption
M	the output plaintext message

Returns

1 if successful, else 0

8.11.3.2 ECP_BLS381_ECIES_ENCRYPT()

```
void ECP_BLS381_ECIES_ENCRYPT (
            int h,
            octet * P1,
            octet * P2,
            csprng * R,
            octet * W,
            octet * M,
            int len,
            octet * V,
            octet * C,
            octet * T )
```

IEEE-1363 ECIES Encryption

Parameters

h	is the hash type
P1	input Key Derivation parameters
P2	input Encoding parameters
R	is a pointer to a cryptographically secure random number generator
W	the input public key of the recieving party
M	is the plaintext message to be encrypted
len	the length of the HMAC tag
V	component of the output ciphertext
C	the output ciphertext
T	the output HMAC tag, part of the ciphertext

8.11.3.3 ECP_BLS381_KEY_PAIR_GENERATE()

```
int ECP_BLS381_KEY_PAIR_GENERATE (
            csprng * R,
            octet * s,
            octet * W )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
s	the private key, an output internally randomly generated if R!=NULL, otherwise must be provided as an input
W	the output public key, which is s.G, where G is a fixed generator

Returns

0 or an error code

8.11.3.4 ECP_BLS381_PUBLIC_KEY_VALIDATE()

```
int ECP_BLS381_PUBLIC_KEY_VALIDATE (
            octet * W )
```

Parameters

W	the input public key to be validated

Returns

0 if public key is OK, or an error code

8.11.3.5 ECP_BLS381_SP_DSA()

```
int ECP_BLS381_SP_DSA (
            int h,
            csprng * R,
            octet * k,
            octet * s,
            octet * M,
            octet * c,
            octet * d )
```

IEEE-1363 ECDSA Signature

Parameters

h	is the hash type
R	is a pointer to a cryptographically secure random number generator
k	Ephemeral key. This value is used when R=NULL
s	the input private signing key
M	the input message to be signed
c	component of the output signature
d	component of the output signature

8.11.3.6 ECP_BLS381_SVDP_DH()

```
int ECP_BLS381_SVDP_DH (
            octet * s,
```

```
octet * W,
octet * K )
```

IEEE-1363 Diffie-Hellman shared secret calculation

Parameters

s	is the input private key,
W	the input public key of the other party
K	the output shared key, in fact the x-coordinate of s.W

Returns

0 or an error code

8.11.3.7 ECP_BLS381_VP_DSA()

```
int ECP_BLS381_VP_DSA (
            int h,
            octet * W,
            octet * M,
            octet * c,
            octet * d )
```

IEEE-1363 ECDSA Signature Verification

Parameters

h	is the hash type
W	the input public key
M	the input message
c	component of the input signature
d	component of the input signature

Returns

0 or an error code

8.12 ecdh_support.h File Reference

ECDH Support Header File.

```
#include "amcl.h"
```

Functions

- void ehashit (int sha, octet ∗p, int n, octet ∗x, octet ∗w, int pad)

    general purpose hash function w=hash(p|n|x|y)
- void HASH (int h, octet ∗I, octet ∗O)

    hash an octet into another octet
- int HMAC (int h, octet ∗M, octet ∗K, int len, octet ∗tag)

    HMAC of message M using key K to create tag of length len in octet tag.
- void KDF2 (int h, octet ∗Z, octet ∗P, int len, octet ∗K)

    Key Derivation Function - generates key K from inputs Z and P.
- void PBKDF2 (int h, octet ∗P, octet ∗S, int rep, int len, octet ∗K)

    Password Based Key Derivation Function - generates key K from password, salt and repeat counter.
- void AES_CBC_IV0_ENCRYPT (octet ∗K, octet ∗P, octet ∗C)

    AES encrypts a plaintext to a ciphtertext.
- int AES_CBC_IV0_DECRYPT (octet ∗K, octet ∗C, octet ∗P)

    AES encrypts a plaintext to a ciphtertext.

8.12.1 Detailed Description

Author

Mike Scott

8.12.2 Function Documentation

8.12.2.1 AES_CBC_IV0_DECRYPT()

```
int AES_CBC_IV0_DECRYPT (
            octet * K,
            octet * C,
            octet * P )
```

IEEE-1363 AES_CBC_IV0_DECRYPT function. Decrypts in CBC mode with a zero IV.

Parameters

K	AES key
C	input ciphertext octet
P	output plaintext octet

Returns

0 if bad input, else 1

8.12.2.2 AES_CBC_IV0_ENCRYPT()

```
void AES_CBC_IV0_ENCRYPT (
            octet * K,
            octet * P,
            octet * C )
```

IEEE-1363 AES_CBC_IV0_ENCRYPT function. Encrypts in CBC mode with a zero IV, padding as necessary to create a full final block.

Parameters

K	AES key
P	input plaintext octet
C	output ciphertext octet

8.12.2.3 ehashit()

```
void ehashit (
            int sha,
            octet * p,
            int n,
            octet * x,
            octet * w,
            int pad )
```

Parameters

sha	is the hash type
p	first octect involved in the hash
n	integer involved in the hash
x	second octect involved in the h ash
w	output
pad	padding

8.12.2.4 HASH()

```
void HASH (
            int h,
            octet * I,
            octet * O )
```

Parameters

h	is the hash type
I	input octet
O	output octet - H(I)

8.12.2.5 HMAC()

```
int HMAC (
        int h,
        octet * M,
        octet * K,
        int len,
        octet * tag )
```

IEEE-1363 MAC1 function. Uses SHA256 internally.

Parameters

h	is the hash type
M	input message octet
K	input encryption key
len	is output desired length of HMAC tag
tag	is the output HMAC

Returns

0 for bad parameters, else 1

8.12.2.6 KDF2()

```
void KDF2 (
        int h,
        octet * Z,
        octet * P,
        int len,
        octet * K )
```

IEEE-1363 KDF2 Key Derivation Function. Uses SHA256 internally.

Parameters

h	is the hash type
Z	input octet
P	input key derivation parameters - can be NULL
len	is output desired length of key
K	is the derived key

8.12.2.7 PBKDF2()

```
void PBKDF2 (
            int h,
            octet * P,
            octet * S,
            int rep,
            int len,
            octet * K )
```

PBKDF2 Password Based Key Derivation Function. Uses SHA256 internally.

Parameters

h	is the hash type
P	input password
S	input salt
rep	Number of times to be iterated.
len	is output desired length
K	is the derived key

8.13 ecp2_BLS381.h File Reference

ECP2 Header File.

```
#include "fp2_BLS381.h"
#include "config_curve_BLS381.h"
```

Data Structures

- struct ECP2_BLS381

  ECP2 Structure - Elliptic Curve Point over quadratic extension field.

Functions

- int ECP2_BLS381_isinf (ECP2_BLS381 *P)

  Tests for ECP2 point equal to infinity.
- void ECP2_BLS381_copy (ECP2_BLS381 *P, ECP2_BLS381 *Q)

  Copy ECP2 point to another ECP2 point.
- void ECP2_BLS381_inf (ECP2_BLS381 *P)

  Set ECP2 to point-at-infinity.
- int ECP2_BLS381_equals (ECP2_BLS381 *P, ECP2_BLS381 *Q)

  Tests for equality of two ECP2s.
- void ECP2_BLS381_affine (ECP2_BLS381 *P)

  Converts an ECP2 point from Projective (x,y,z) coordinates to affine (x,y) coordinates.
- int ECP2_BLS381_get (FP2_BLS381 *x, FP2_BLS381 *y, ECP2_BLS381 *P)

  Extract x and y coordinates of an ECP2 point P.

- void ECP2_BLS381_output (ECP2_BLS381 ∗P)

  Formats and outputs an ECP2 point to the console, converted to affine coordinates.
- void ECP2_BLS381_outputxyz (ECP2_BLS381 ∗P)

  Formats and outputs an ECP2 point to the console, in projective coordinates.
- void ECP2_BLS381_toOctet (octet ∗S, ECP2_BLS381 ∗P)

  Formats and outputs an ECP2 point to an octet string.
- int ECP2_BLS381_fromOctet (ECP2_BLS381 ∗P, octet ∗S)

  Creates an ECP2 point from an octet string.
- void ECP2_BLS381_rhs (FP2_BLS381 ∗r, FP2_BLS381 ∗x)

  Calculate Right Hand Side of curve equation y^2=f(x)
- int ECP2_BLS381_set (ECP2_BLS381 ∗P, FP2_BLS381 ∗x, FP2_BLS381 ∗y)

  Set ECP2 to point(x,y) given x and y.
- int ECP2_BLS381_setx (ECP2_BLS381 ∗P, FP2_BLS381 ∗x)

  Set ECP to point(x,[y]) given x.
- void ECP2_BLS381_neg (ECP2_BLS381 ∗P)

  Negation of an ECP2 point.
- int ECP2_BLS381_dbl (ECP2_BLS381 ∗P)

  Doubles an ECP2 instance P.
- int ECP2_BLS381_add (ECP2_BLS381 ∗P, ECP2_BLS381 ∗Q)

  Adds ECP2 instance Q to ECP2 instance P.
- void ECP2_BLS381_sub (ECP2_BLS381 ∗P, ECP2_BLS381 ∗Q)

  Subtracts ECP instance Q from ECP2 instance P.
- void ECP2_BLS381_mul (ECP2_BLS381 ∗P, BIG_384_58 b)

  Multiplies an ECP2 instance P by a BIG, side-channel resistant.
- void ECP2_BLS381_frob (ECP2_BLS381 ∗P, FP2_BLS381 ∗f)

  Multiplies an ECP2 instance P by the internal modulus p, using precalculated Frobenius constant f.
- void ECP2_BLS381_mul4 (ECP2_BLS381 ∗P, ECP2_BLS381 ∗Q, BIG_384_58 ∗b)

  Calculates P=b[0]∗Q[0]+b[1]∗Q[1]+b[2]∗Q[2]+b[3]∗Q[3].
- void ECP2_BLS381_mapit (ECP2_BLS381 ∗P, octet ∗w)

  Maps random BIG to curve point of correct order.
- void ECP2_BLS381_generator (ECP2_BLS381 ∗G)

  Get Group Generator from ROM.

Variables

- const int CURVE_A_BLS381
- const int CURVE_B_I_BLS381
- const BIG_384_58 CURVE_B_BLS381
- const BIG_384_58 CURVE_Order_BLS381
- const BIG_384_58 CURVE_Cof_BLS381
- const BIG_384_58 CURVE_Bnx_BLS381
- const BIG_384_58 Fra_BLS381
- const BIG_384_58 Frb_BLS381
- const BIG_384_58 CURVE_Gx_BLS381
- const BIG_384_58 CURVE_Gy_BLS381
- const BIG_384_58 CURVE_Pxa_BLS381
- const BIG_384_58 CURVE_Pxb_BLS381
- const BIG_384_58 CURVE_Pya_BLS381
- const BIG_384_58 CURVE_Pyb_BLS381

8.13.1 Detailed Description

Author

Mike Scott

8.13.2 Function Documentation

8.13.2.1 ECP2_BLS381_add()

```
int ECP2_BLS381_add (
            ECP2_BLS381 * P,
            ECP2_BLS381 * Q )
```

Parameters

P	ECP2 instance, on exit =P+Q
Q	ECP2 instance to be added to P

8.13.2.2 ECP2_BLS381_affine()

```
void ECP2_BLS381_affine (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance to be converted to affine form

8.13.2.3 ECP2_BLS381_copy()

```
void ECP2_BLS381_copy (
            ECP2_BLS381 * P,
            ECP2_BLS381 * Q )
```

Parameters

P	ECP2 instance, on exit = Q
Q	ECP2 instance to be copied

8.13.2.4 ECP2_BLS381_dbl()

```
int ECP2_BLS381_dbl (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance, on exit =2∗P

8.13.2.5 ECP2_BLS381_equals()

```
int ECP2_BLS381_equals (
            ECP2_BLS381 * P,
            ECP2_BLS381 * Q )
```

Parameters

P	ECP2 instance to be compared
Q	ECP2 instance to be compared

Returns

1 if P=Q, else returns 0

8.13.2.6 ECP2_BLS381_frob()

```
void ECP2_BLS381_frob (
            ECP2_BLS381 * P,
            FP2_BLS381 * f )
```

Fast point multiplication using Frobenius

Parameters

P	ECP2 instance, on exit = p∗P
f	FP2 precalculated Frobenius constant

8.13.2.7 ECP2_BLS381_fromOctet()

```
int ECP2_BLS381_fromOctet (
            ECP2_BLS381 * P,
            octet * S )
```

The octet string is in the form x|y The real and imaginary parts of the x and y coordinates are in big-endian base 256 form.

Parameters

P	ECP2 instance to be created from the octet string
S	input octet string return 1 if octet string corresponds to a point on the curve, else 0

8.13.2.8 ECP2_BLS381_generator()

```
void ECP2_BLS381_generator (
            ECP2_BLS381 * G )
```

Parameters

G	ECP2 instance

8.13.2.9 ECP2_BLS381_get()

```
int ECP2_BLS381_get (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            ECP2_BLS381 * P )
```

If x=y, returns only x

Parameters

x	FP2 on exit = x coordinate of point
y	FP2 on exit = y coordinate of point (unless x=y)
P	ECP2 instance (x,y)

Returns

-1 if P is point-at-infinity, else 0

8.13.2.10 ECP2_BLS381_inf()

```
void ECP2_BLS381_inf (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance to be set to infinity

8.13.2.11 ECP2_BLS381_isinf()

```
int ECP2_BLS381_isinf (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 point to be tested

Returns

1 if infinity, else returns 0

8.13.2.12 ECP2_BLS381_mapit()

```
void ECP2_BLS381_mapit (
            ECP2_BLS381 * P,
            octet * w )
```

Parameters

P	ECP2 instance of correct order
w	OCTET byte array to be mapped

8.13.2.13 ECP2_BLS381_mul()

```
void ECP2_BLS381_mul (
            ECP2_BLS381 * P,
            BIG_384_58 b )
```

Uses fixed sized windows.

Parameters

P	ECP2 instance, on exit =b∗P
b	BIG number multiplier

8.13.2.14 ECP2_BLS381_mul4()

```
void ECP2_BLS381_mul4 (
            ECP2_BLS381 * P,
            ECP2_BLS381 * Q,
            BIG_384_58 * b )
```

Parameters

P	ECP2 instance, on exit = b[0]∗Q[0]+b[1]∗Q[1]+b[2]∗Q[2]+b[3]∗Q[3]
Q	ECP2 array of 4 points
b	BIG array of 4 multipliers

8.13.2.15 ECP2_BLS381_neg()

```
void ECP2_BLS381_neg (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance, on exit = -P

8.13.2.16 ECP2_BLS381_output()

```
void ECP2_BLS381_output (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance to be printed

8.13.2.17 ECP2_BLS381_outputxyz()

```
void ECP2_BLS381_outputxyz (
            ECP2_BLS381 * P )
```

Parameters

P	ECP2 instance to be printed

8.13.2.18 ECP2_BLS381_rhs()

```
void ECP2_BLS381_rhs (
            FP2_BLS381 * r,
            FP2_BLS381 * x )
```

Function f(x)=x^3+Ax+B Used internally.

Parameters

r	FP2 value of f(x)
x	FP2 instance

8.13.2.19 ECP2_BLS381_set()

```
int ECP2_BLS381_set (
            ECP2_BLS381 * P,
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Point P set to infinity if no such point on the curve.

Parameters

P	ECP2 instance to be set (x,y)
x	FP2 x coordinate of point
y	FP2 y coordinate of point

Returns

1 if point exists, else 0

8.13.2.20 ECP2_BLS381_setx()

```
int ECP2_BLS381_setx (
            ECP2_BLS381 * P,
            FP2_BLS381 * x )
```

Point P set to infinity if no such point on the curve. Otherwise y coordinate is calculated from x.

Parameters

P	ECP instance to be set (x,[y])
x	BIG x coordinate of point

Returns

1 if point exists, else 0

8.13.2.21 ECP2_BLS381_sub()

```
void ECP2_BLS381_sub (
            ECP2_BLS381 * P,
            ECP2_BLS381 * Q )
```

Parameters

P	ECP2 instance, on exit =P-Q
Q	ECP2 instance to be subtracted from P

8.13.2.22 ECP2_BLS381_toOctet()

```
void ECP2_BLS381_toOctet (
            octet * S,
            ECP2_BLS381 * P )
```

The octet string is created in the form x|y. Convert the real and imaginary parts of the x and y coordinates to big-endian base 256 form.

Parameters

S	output octet string
P	ECP2 instance to be converted to an octet string

8.13.3 Variable Documentation

8.13.3.1 CURVE_A_BLS381

```
const int CURVE_A_BLS381
```

Elliptic curve A parameter

8.13.3.2 CURVE_B_BLS381

```
const BIG_384_58 CURVE_B_BLS381
```

Elliptic curve B parameter

8.13.3.3 CURVE_B_I_BLS381

```
const int CURVE_B_I_BLS381
```

Elliptic curve B parameter

8.13.3.4 CURVE_Bnx_BLS381

```
const BIG_384_58 CURVE_Bnx_BLS381
```

Elliptic curve parameter

8.13.3.5 CURVE_Cof_BLS381

```
const BIG_384_58 CURVE_Cof_BLS381
```

Elliptic curve cofactor

8.13.3.6 CURVE_Gx_BLS381

```
const BIG_384_58 CURVE_Gx_BLS381
```

x-coordinate of generator point in group G1

8.13.3.7 CURVE_Gy_BLS381

```
const BIG_384_58 CURVE_Gy_BLS381
```

y-coordinate of generator point in group G1

8.13.3.8 CURVE_Order_BLS381

```
const BIG_384_58 CURVE_Order_BLS381
```

Elliptic curve group order

8.13.3.9 CURVE_Pxa_BLS381

```
const BIG_384_58 CURVE_Pxa_BLS381
```

real part of x-coordinate of generator point in group G2

8.13.3.10 CURVE_Pxb_BLS381

```
const BIG_384_58 CURVE_Pxb_BLS381
```

imaginary part of x-coordinate of generator point in group G2

8.13.3.11 CURVE_Pya_BLS381

```
const BIG_384_58 CURVE_Pya_BLS381
```

real part of y-coordinate of generator point in group G2

8.13.3.12 CURVE_Pyb_BLS381

```
const BIG_384_58 CURVE_Pyb_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.13.3.13 Fra_BLS381

```
const BIG_384_58 Fra_BLS381
```

real part of BN curve Frobenius Constant

8.13.3.14 Frb_BLS381

```
const BIG_384_58 Frb_BLS381
```

imaginary part of BN curve Frobenius Constant

8.14 ecp_BLS381.h File Reference

ECP Header File.

```
#include "fp_BLS381.h"
#include "config_curve_BLS381.h"
```

Data Structures

- struct ECP_BLS381

    ECP structure - Elliptic Curve Point over base field.

Functions

- int ECP_BLS381_isinf (ECP_BLS381 ∗P)

  Tests for ECP point equal to infinity.
- int ECP_BLS381_equals (ECP_BLS381 ∗P, ECP_BLS381 ∗Q)

  Tests for equality of two ECPs.
- void ECP_BLS381_copy (ECP_BLS381 ∗P, ECP_BLS381 ∗Q)

  Copy ECP point to another ECP point.
- void ECP_BLS381_neg (ECP_BLS381 ∗P)

  Negation of an ECP point.
- void ECP_BLS381_inf (ECP_BLS381 ∗P)

  Set ECP to point-at-infinity.
- void ECP_BLS381_rhs (FP_BLS381 ∗r, FP_BLS381 ∗x)

  Calculate Right Hand Side of curve equation y^2=f(x)
- int ECP_BLS381_set (ECP_BLS381 ∗P, BIG_384_58 x, BIG_384_58 y)

  Set ECP to point(x,y) given x and y.
- int ECP_BLS381_get (BIG_384_58 x, BIG_384_58 y, ECP_BLS381 ∗P)

  Extract x and y coordinates of an ECP point P.
- void ECP_BLS381_add (ECP_BLS381 ∗P, ECP_BLS381 ∗Q)

  Adds ECP instance Q to ECP instance P.
- void ECP_BLS381_sub (ECP_BLS381 ∗P, ECP_BLS381 ∗Q)

  Subtracts ECP instance Q from ECP instance P.
- int ECP_BLS381_setx (ECP_BLS381 ∗P, BIG_384_58 x, int s)

  Set ECP to point(x,y) given just x and sign of y.
- void ECP_BLS381_cfp (ECP_BLS381 ∗Q)

  Multiplies Point by curve co-factor.
- void ECP_BLS381_mapit (ECP_BLS381 ∗Q, octet ∗w)

  Maps random BIG to curve point of correct order.
- void ECP_BLS381_affine (ECP_BLS381 ∗P)

  Converts an ECP point from Projective (x,y,z) coordinates to affine (x,y) coordinates.
- void ECP_BLS381_outputxyz (ECP_BLS381 ∗P)

  Formats and outputs an ECP point to the console, in projective coordinates.
- void ECP_BLS381_output (ECP_BLS381 ∗P)

  Formats and outputs an ECP point to the console, converted to affine coordinates.
- void ECP_BLS381_rawoutput (ECP_BLS381 ∗P)

  Formats and outputs an ECP point to the console.
- void ECP_BLS381_toOctet (octet ∗S, ECP_BLS381 ∗P, bool c)

  Formats and outputs an ECP point to an octet string The octet string is normally in the standard form 0x04|x|y Here x (and y) are the x and y coordinates in left justified big-endian base 256 form. For Montgomery curve it is 0x06|x If c is true, only the x coordinate is provided as in 0x2|x if y is even, or 0x3|x if y is odd.
- int ECP_BLS381_fromOctet (ECP_BLS381 ∗P, octet ∗S)

  Creates an ECP point from an octet string.
- void ECP_BLS381_dbl (ECP_BLS381 ∗P)

  Doubles an ECP instance P.
- void ECP_BLS381_pinmul (ECP_BLS381 ∗P, int i, int b)

  Multiplies an ECP instance P by a small integer, side-channel resistant.
- void ECP_BLS381_mul (ECP_BLS381 ∗P, BIG_384_58 b)

  Multiplies an ECP instance P by a BIG, side-channel resistant.
- void ECP_BLS381_mul2 (ECP_BLS381 ∗P, ECP_BLS381 ∗Q, BIG_384_58 e, BIG_384_58 f)

  Calculates double multiplication P=e∗P+f∗Q, side-channel resistant.
- void ECP_BLS381_generator (ECP_BLS381 ∗G)

  Get Group Generator from ROM.

Variables

- const int CURVE_A_BLS381
- const int CURVE_Cof_I_BLS381
- const int CURVE_B_I_BLS381
- const BIG_384_58 CURVE_B_BLS381
- const BIG_384_58 CURVE_Order_BLS381
- const BIG_384_58 CURVE_Cof_BLS381
- const BIG_384_58 CURVE_Gx_BLS381
- const BIG_384_58 CURVE_Gy_BLS381
- const BIG_384_58 CURVE_Pxa_BLS381
- const BIG_384_58 CURVE_Pxb_BLS381
- const BIG_384_58 CURVE_Pya_BLS381
- const BIG_384_58 CURVE_Pyb_BLS381
- const BIG_384_58 CURVE_Pxaa_BLS381
- const BIG_384_58 CURVE_Pxab_BLS381
- const BIG_384_58 CURVE_Pxba_BLS381
- const BIG_384_58 CURVE_Pxbb_BLS381
- const BIG_384_58 CURVE_Pyaa_BLS381
- const BIG_384_58 CURVE_Pyab_BLS381
- const BIG_384_58 CURVE_Pyba_BLS381
- const BIG_384_58 CURVE_Pybb_BLS381
- const BIG_384_58 CURVE_Pxaaa_BLS381
- const BIG_384_58 CURVE_Pxaab_BLS381
- const BIG_384_58 CURVE_Pxaba_BLS381
- const BIG_384_58 CURVE_Pxabb_BLS381
- const BIG_384_58 CURVE_Pxbaa_BLS381
- const BIG_384_58 CURVE_Pxbab_BLS381
- const BIG_384_58 CURVE_Pxbba_BLS381
- const BIG_384_58 CURVE_Pxbbb_BLS381
- const BIG_384_58 CURVE_Pyaaa_BLS381
- const BIG_384_58 CURVE_Pyaab_BLS381
- const BIG_384_58 CURVE_Pyaba_BLS381
- const BIG_384_58 CURVE_Pyabb_BLS381
- const BIG_384_58 CURVE_Pybaa_BLS381
- const BIG_384_58 CURVE_Pybab_BLS381
- const BIG_384_58 CURVE_Pybba_BLS381
- const BIG_384_58 CURVE_Pybbb_BLS381
- const BIG_384_58 CURVE_Bnx_BLS381
- const BIG_384_58 CURVE_Cru_BLS381
- const BIG_384_58 Fra_BLS381
- const BIG_384_58 Frb_BLS381
- const BIG_384_58 CURVE_W_BLS381 [2]
- const BIG_384_58 CURVE_SB_BLS381 [2][2]
- const BIG_384_58 CURVE_WB_BLS381 [4]
- const BIG_384_58 CURVE_BB_BLS381 [4][4]

8.14.1 Detailed Description

Author

Mike Scott

8.14.2 Function Documentation

8.14.2.1 ECP_BLS381_add()

```
void ECP_BLS381_add (
            ECP_BLS381 * P,
            ECP_BLS381 * Q )
```

Parameters

P	ECP instance, on exit =P+Q
Q	ECP instance to be added to P

8.14.2.2 ECP_BLS381_affine()

```
void ECP_BLS381_affine (
            ECP_BLS381 * P )
```

Parameters

P	ECP instance to be converted to affine form

8.14.2.3 ECP_BLS381_cfp()

```
void ECP_BLS381_cfp (
            ECP_BLS381 * Q )
```

Parameters

Q	ECP instance

8.14.2.4 ECP_BLS381_copy()

```
void ECP_BLS381_copy (
            ECP_BLS381 * P,
            ECP_BLS381 * Q )
```

Parameters

P	ECP instance, on exit = Q
Q	ECP instance to be copied

8.14.2.5 ECP_BLS381_dbl()

```
void ECP_BLS381_dbl (
            ECP_BLS381 * P )
```

Parameters

P	ECP instance, on exit =2∗P

8.14.2.6 ECP_BLS381_equals()

```
int ECP_BLS381_equals (
            ECP_BLS381 * P,
            ECP_BLS381 * Q )
```

Parameters

P	ECP instance to be compared
Q	ECP instance to be compared

Returns

1 if P=Q, else returns 0

8.14.2.7 ECP_BLS381_fromOctet()

```
int ECP_BLS381_fromOctet (
            ECP_BLS381 * P,
            octet * S )
```

The octet string is normally in the standard form 0x04|x|y Here x (and y) are the x and y coordinates in left justified big-endian base 256 form. For Montgomery curve it is 0x06|x If in compressed form only the x coordinate is provided as in 0x2|x if y is even, or 0x3|x if y is odd

Parameters

P	ECP instance to be created from the octet string
S	input octet string return 1 if octet string corresponds to a point on the curve, else 0

8.14.2.8 ECP_BLS381_generator()

```
void ECP_BLS381_generator (
            ECP_BLS381 * G )
```

Parameters

G	ECP instance

8.14.2.9 ECP_BLS381_get()

```
int ECP_BLS381_get (
            BIG_384_58 x,
            BIG_384_58 y,
            ECP_BLS381 * P )
```

If x=y, returns only x

Parameters

x	BIG on exit = x coordinate of point
y	BIG on exit = y coordinate of point (unless x=y)
P	ECP instance (x,y)

Returns

sign of y, or -1 if P is point-at-infinity

8.14.2.10 ECP_BLS381_inf()

```
void ECP_BLS381_inf (
            ECP_BLS381 * P )
```

Parameters

P	ECP instance to be set to infinity

8.14.2.11 ECP_BLS381_isinf()

```
int ECP_BLS381_isinf (
            ECP_BLS381 * P )
```

Parameters

P	ECP point to be tested

Returns

1 if infinity, else returns 0

8.14.2.12 ECP_BLS381_mapit()

```
void ECP_BLS381_mapit (
            ECP_BLS381 * Q,
            octet * w )
```

Parameters

Q	ECP instance of correct order
w	OCTET byte array to be mapped

8.14.2.13 ECP_BLS381_mul()

```
void ECP_BLS381_mul (
            ECP_BLS381 * P,
            BIG_384_58 b )
```

Uses Montgomery ladder for Montgomery curves, otherwise fixed sized windows.

Parameters

P	ECP instance, on exit =b∗P
b	BIG number multiplier

8.14.2.14 ECP_BLS381_mul2()

```
void ECP_BLS381_mul2 (
            ECP_BLS381 * P,
```

```
ECP_BLS381 * Q,
BIG_384_58 e,
BIG_384_58 f )
```

Parameters

P	ECP instance, on exit =e∗P+f∗Q
Q	ECP instance
e	BIG number multiplier
f	BIG number multiplier

8.14.2.15 ECP_BLS381_neg()

```
void ECP_BLS381_neg (
    ECP_BLS381 * P )
```

Parameters

P	ECP instance, on exit = -P

8.14.2.16 ECP_BLS381_output()

```
void ECP_BLS381_output (
    ECP_BLS381 * P )
```

Parameters

P	ECP instance to be printed

8.14.2.17 ECP_BLS381_outputxyz()

```
void ECP_BLS381_outputxyz (
    ECP_BLS381 * P )
```

Parameters

P	ECP instance to be printed

8.14.2.18 ECP_BLS381_pinmul()

```
void ECP_BLS381_pinmul (
            ECP_BLS381 * P,
            int i,
            int b )
```

Parameters

P	ECP instance, on exit =i*P
i	small integer multiplier
b	maximum number of bits in multiplier

8.14.2.19 ECP_BLS381_rawoutput()

```
void ECP_BLS381_rawoutput (
            ECP_BLS381 * P )
```

Parameters

P	ECP instance to be printed

8.14.2.20 ECP_BLS381_rhs()

```
void ECP_BLS381_rhs (
            FP_BLS381 * r,
            FP_BLS381 * x )
```

Function f(x) depends on form of elliptic curve, Weierstrass, Edwards or Montgomery. Used internally.

Parameters

r	BIG n-residue value of f(x)
x	BIG n-residue x

8.14.2.21 ECP_BLS381_set()

```
int ECP_BLS381_set (
            ECP_BLS381 * P,
            BIG_384_58 x,
            BIG_384_58 y )
```

Point P set to infinity if no such point on the curve.

Parameters

P	ECP instance to be set (x,y)
x	BIG x coordinate of point
y	BIG y coordinate of point

Returns

1 if point exists, else 0

8.14.2.22 ECP_BLS381_setx()

```
int ECP_BLS381_setx (
            ECP_BLS381 * P,
            BIG_384_58 x,
            int s )
```

Point P set to infinity if no such point on the curve. If x is on the curve then y is calculated from the curve equation. The correct y value (plus or minus) is selected given its sign s.

Parameters

P	ECP instance to be set (x,[y])
x	BIG x coordinate of point
s	an integer representing the "sign" of y, in fact its least significant bit.

8.14.2.23 ECP_BLS381_sub()

```
void ECP_BLS381_sub (
            ECP_BLS381 * P,
            ECP_BLS381 * Q )
```

Parameters

P	ECP instance, on exit =P-Q
Q	ECP instance to be subtracted from P

8.14.2.24 ECP_BLS381_toOctet()

```
void ECP_BLS381_toOctet (
            octet * S,
```

```
ECP_BLS381 * P,
bool c )
```

Parameters

c	compression required, true or false
S	output octet string
P	ECP instance to be converted to an octet string

8.14.3 Variable Documentation

8.14.3.1 CURVE_A_BLS381

```
const int CURVE_A_BLS381
```

Elliptic curve A parameter

8.14.3.2 CURVE_B_BLS381

```
const BIG_384_58 CURVE_B_BLS381
```

Elliptic curve B parameter

8.14.3.3 CURVE_B_I_BLS381

```
const int CURVE_B_I_BLS381
```

Elliptic curve B_i parameter

8.14.3.4 CURVE_BB_BLS381

```
const BIG_384_58 CURVE_BB_BLS381[4][4]
```

BN curve constant for GS decomposition

8.14.3.5 CURVE_Bnx_BLS381

```
const BIG_384_58 CURVE_Bnx_BLS381
```

BN curve x parameter

8.14.3.6 CURVE_Cof_BLS381

```
const BIG_384_58 CURVE_Cof_BLS381
```

Elliptic curve cofactor

8.14.3.7 CURVE_Cof_I_BLS381

`const int CURVE_Cof_I_BLS381`

Elliptic curve cofactor

8.14.3.8 CURVE_Cru_BLS381

`const BIG_384_58 CURVE_Cru_BLS381`

BN curve Cube Root of Unity

8.14.3.9 CURVE_Gx_BLS381

`const BIG_384_58 CURVE_Gx_BLS381`

x-coordinate of generator point in group G1

8.14.3.10 CURVE_Gy_BLS381

`const BIG_384_58 CURVE_Gy_BLS381`

y-coordinate of generator point in group G1

8.14.3.11 CURVE_Order_BLS381

`const BIG_384_58 CURVE_Order_BLS381`

Elliptic curve group order

8.14.3.12 CURVE_Pxa_BLS381

`const BIG_384_58 CURVE_Pxa_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.13 CURVE_Pxaa_BLS381

`const BIG_384_58 CURVE_Pxaa_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.14 CURVE_Pxaaa_BLS381

`const BIG_384_58 CURVE_Pxaaa_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.15 CURVE_Pxaab_BLS381

`const BIG_384_58 CURVE_Pxaab_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.16 CURVE_Pxab_BLS381

`const BIG_384_58 CURVE_Pxab_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.17 CURVE_Pxaba_BLS381

`const BIG_384_58 CURVE_Pxaba_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.18 CURVE_Pxabb_BLS381

`const BIG_384_58 CURVE_Pxabb_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.19 CURVE_Pxb_BLS381

`const BIG_384_58 CURVE_Pxb_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.20 CURVE_Pxba_BLS381

`const BIG_384_58 CURVE_Pxba_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.21 CURVE_Pxbaa_BLS381

`const BIG_384_58 CURVE_Pxbaa_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.22 CURVE_Pxbab_BLS381

`const BIG_384_58 CURVE_Pxbab_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.23 CURVE_Pxbb_BLS381

`const BIG_384_58 CURVE_Pxbb_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.24 CURVE_Pxbba_BLS381

`const BIG_384_58 CURVE_Pxbba_BLS381`

real part of x-coordinate of generator point in group G2

8.14.3.25 CURVE_Pxbbb_BLS381

`const BIG_384_58 CURVE_Pxbbb_BLS381`

imaginary part of x-coordinate of generator point in group G2

8.14.3.26 CURVE_Pya_BLS381

`const BIG_384_58 CURVE_Pya_BLS381`

real part of y-coordinate of generator point in group G2

8.14.3.27 CURVE_Pyaa_BLS381

`const BIG_384_58 CURVE_Pyaa_BLS381`

real part of y-coordinate of generator point in group G2

8.14.3.28 CURVE_Pyaaa_BLS381

`const BIG_384_58 CURVE_Pyaaa_BLS381`

real part of y-coordinate of generator point in group G2

8.14.3.29 CURVE_Pyaab_BLS381

`const BIG_384_58 CURVE_Pyaab_BLS381`

imaginary part of y-coordinate of generator point in group G2

8.14.3.30 CURVE_Pyab_BLS381

`const BIG_384_58 CURVE_Pyab_BLS381`

imaginary part of y-coordinate of generator point in group G2

8.14.3.31 CURVE_Pyaba_BLS381

```
const BIG_384_58 CURVE_Pyaba_BLS381
```

real part of y-coordinate of generator point in group G2

8.14.3.32 CURVE_Pyabb_BLS381

```
const BIG_384_58 CURVE_Pyabb_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.14.3.33 CURVE_Pyb_BLS381

```
const BIG_384_58 CURVE_Pyb_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.14.3.34 CURVE_Pyba_BLS381

```
const BIG_384_58 CURVE_Pyba_BLS381
```

real part of y-coordinate of generator point in group G2

8.14.3.35 CURVE_Pybaa_BLS381

```
const BIG_384_58 CURVE_Pybaa_BLS381
```

real part of y-coordinate of generator point in group G2

8.14.3.36 CURVE_Pybab_BLS381

```
const BIG_384_58 CURVE_Pybab_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.14.3.37 CURVE_Pybb_BLS381

```
const BIG_384_58 CURVE_Pybb_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.14.3.38 CURVE_Pybba_BLS381

```
const BIG_384_58 CURVE_Pybba_BLS381
```

real part of y-coordinate of generator point in group G2

8.14.3.39 CURVE_Pybbb_BLS381

```
const BIG_384_58 CURVE_Pybbb_BLS381
```

imaginary part of y-coordinate of generator point in group G2

8.14.3.40 CURVE_SB_BLS381

```
const BIG_384_58 CURVE_SB_BLS381[2][2]
```

BN curve constant for GLV decomposition

8.14.3.41 CURVE_W_BLS381

```
const BIG_384_58 CURVE_W_BLS381[2]
```

BN curve constant for GLV decomposition

8.14.3.42 CURVE_WB_BLS381

```
const BIG_384_58 CURVE_WB_BLS381[4]
```

BN curve constant for GS decomposition

8.14.3.43 Fra_BLS381

```
const BIG_384_58 Fra_BLS381
```

real part of BN curve Frobenius Constant

8.14.3.44 Frb_BLS381

```
const BIG_384_58 Frb_BLS381
```

imaginary part of BN curve Frobenius Constant

8.15 ff_2048.h File Reference

FF Header File.

```
#include "big_1024_58.h"
#include "config_ff_2048.h"
```

Macros

- #define HFLEN_2048 (FFLEN_2048/2)
- #define P_MBITS_2048 (MODBYTES_1024_58∗8)
- #define P_TBITS_2048 (P_MBITS_2048%BASEBITS_1024_58)
- #define P_EXCESS_2048(a) (((a[NLEN_1024_58-1])>>(P_TBITS_2048))+1)
- #define P_FEXCESS_2048 ((chunk)1<<(BASEBITS_1024_58∗NLEN_1024_58-P_MBITS_2048-1))

Functions

- void FF_2048_copy (BIG_1024_58 ∗x, BIG_1024_58 ∗y, int n)
  Copy one FF element of given length to another.
- void FF_2048_init (BIG_1024_58 ∗x, sign32 m, int n)
  Initialize an FF element of given length from a 32-bit integer m.
- void FF_2048_zero (BIG_1024_58 ∗x, int n)
  Set FF element of given size to zero.
- int FF_2048_iszilch (BIG_1024_58 ∗x, int n)
  Tests for FF element equal to zero.
- int FF_2048_parity (BIG_1024_58 ∗x)
  return parity of an FF, that is the least significant bit
- int FF_2048_lastbits (BIG_1024_58 ∗x, int m)
  return least significant m bits of an FF
- void FF_2048_one (BIG_1024_58 ∗x, int n)
  Set FF element of given size to unity.
- int FF_2048_comp (BIG_1024_58 ∗x, BIG_1024_58 ∗y, int n)
  Compares two FF numbers. Inputs must be normalised externally.
- void FF_2048_add (BIG_1024_58 ∗x, BIG_1024_58 ∗y, BIG_1024_58 ∗z, int n)
  addition of two FFs
- void FF_2048_sub (BIG_1024_58 ∗x, BIG_1024_58 ∗y, BIG_1024_58 ∗z, int n)
  subtraction of two FFs
- void FF_2048_inc (BIG_1024_58 ∗x, int m, int n)
  increment an FF by an integer,and normalise
- void FF_2048_dec (BIG_1024_58 ∗x, int m, int n)
  Decrement an FF by an integer,and normalise.
- void FF_2048_norm (BIG_1024_58 ∗x, int n)
  Normalises the components of an FF.
- void FF_2048_shl (BIG_1024_58 ∗x, int n)
  Shift left an FF by 1 bit.
- void FF_2048_shr (BIG_1024_58 ∗x, int n)
  Shift right an FF by 1 bit.
- void FF_2048_output (BIG_1024_58 ∗x, int n)
  Formats and outputs an FF to the console.
- void FF_2048_rawoutput (BIG_1024_58 ∗x, int n)
  Formats and outputs an FF to the console, in raw form.
- void FF_2048_toOctet (octet ∗S, BIG_1024_58 ∗x, int n)
  Formats and outputs an FF instance to an octet string.
- void FF_2048_fromOctet (BIG_1024_58 ∗x, octet ∗S, int n)
  Populates an FF instance from an octet string.
- void FF_2048_mul (BIG_1024_58 ∗x, BIG_1024_58 ∗y, BIG_1024_58 ∗z, int n)
  Multiplication of two FFs.
- void FF_2048_mod (BIG_1024_58 ∗x, BIG_1024_58 ∗p, int n)

Reduce FF mod a modulus.
- void FF_2048_sqr (BIG_1024_58 ∗x, BIG_1024_58 ∗y, int n)

  Square an FF.
- void FF_2048_dmod (BIG_1024_58 ∗x, BIG_1024_58 ∗y, BIG_1024_58 ∗z, int n)

  Reduces a double-length FF with respect to a given modulus.
- void FF_2048_invmodp (BIG_1024_58 ∗x, BIG_1024_58 ∗y, BIG_1024_58 ∗z, int n)

  Invert an FF mod a prime modulus.
- void FF_2048_invmod2m (BIG_1024_58 U[ ], BIG_1024_58 a[ ], int n)

  Invert an FF mod 2^(n∗BIGBITS)
- void FF_2048_random (BIG_1024_58 ∗x, csprng ∗R, int n)

  Create an FF from a random number generator.
- void FF_2048_randomnum (BIG_1024_58 ∗x, BIG_1024_58 ∗y, csprng ∗R, int n)

  Create a random FF less than a given modulus from a random number generator.
- void FF_2048_skpow (BIG_1024_58 ∗r, BIG_1024_58 ∗x, BIG_1024_58 ∗e, BIG_1024_58 ∗p, int n, int en)

  Calculate r=x^e mod p, side channel resistant.
- void FF_2048_skspow (BIG_1024_58 ∗r, BIG_1024_58 ∗x, BIG_1024_58 e, BIG_1024_58 ∗p, int n)

  Calculate r=x^e mod p, side channel resistant.
- void FF_2048_skpow2 (BIG_1024_58 ∗r, BIG_1024_58 ∗x, BIG_1024_58 ∗e, BIG_1024_58 ∗y, BIG_1024↩_58 ∗f, BIG_1024_58 ∗p, int n, int en)

  Calculate r=x^e.y^f mod p for big e and f, side channel resistant.
- void FF_2048_power (BIG_1024_58 ∗r, BIG_1024_58 ∗x, int e, BIG_1024_58 ∗p, int n)

  Calculate r=x^e mod p.
- void FF_2048_pow (BIG_1024_58 ∗r, BIG_1024_58 ∗x, BIG_1024_58 ∗e, BIG_1024_58 ∗p, int n)

  Calculate r=x^e mod p.
- void FF_2048_pow2 (BIG_1024_58 ∗r, BIG_1024_58 ∗x, BIG_1024_58 e, BIG_1024_58 ∗y, BIG_1024_58 f, BIG_1024_58 ∗m, int n)

  Calculate r=x^e.y^f mod m.
- int FF_2048_cfactor (BIG_1024_58 ∗x, sign32 s, int n)

  Test if an FF has factor in common with integer s.
- int FF_2048_prime (BIG_1024_58 ∗x, csprng ∗R, int n)

  Test if an FF is prime.
- void FF_2048_crt (BIG_1024_58 ∗r, BIG_1024_58 ∗rp, BIG_1024_58 ∗rq, BIG_1024_58 ∗p, BIG_1024_58 ∗q, int n)

  Combine rp and rq using the Chinese Remainder Theorem.

8.15.1 Detailed Description

Author

Mike Scott

8.15.2 Macro Definition Documentation

8.15.2.1 HFLEN_2048

```
#define HFLEN_2048 (FFLEN_2048/2)
```

Useful for half-size RSA private key operations

8.15.2.2 P_EXCESS_2048

```
#define P_EXCESS_2048(
               a ) (((a[NLEN_1024_58-1])>>(P_TBITS_2048))+1)
```

TODO

8.15.2.3 P_FEXCESS_2048

```
#define P_FEXCESS_2048 ((chunk)1<<(BASEBITS_1024_58*NLEN_1024_58-P_MBITS_2048-1))
```

TODO

8.15.2.4 P_MBITS_2048

```
#define P_MBITS_2048 (MODBYTES_1024_58*8)
```

Number of bits in modulus

8.15.2.5 P_TBITS_2048

```
#define P_TBITS_2048 (P_MBITS_2048%BASEBITS_1024_58)
```

TODO

8.15.3 Function Documentation

8.15.3.1 FF_2048_add()

```
void FF_2048_add (
             BIG_1024_58 * x,
             BIG_1024_58 * y,
             BIG_1024_58 * z,
             int n )
```

Parameters

x	FF instance, on exit = y+z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.15.3.2 FF_2048_cfactor()

```
int FF_2048_cfactor (
            BIG_1024_58 * x,
            sign32 s,
            int n )
```

Parameters

x	FF instance to be tested
s	the supplied integer
n	size of FF in BIGs

Returns

1 if gcd(x,s)!=1, else return 0

8.15.3.3 FF_2048_comp()

```
int FF_2048_comp (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            int n )
```

Parameters

x	first FF number to be compared
y	second FF number to be compared
n	size of FF in BIGs

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.15.3.4 FF_2048_copy()

```
void FF_2048_copy (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            int n )
```

Parameters

x	FF instance to be copied to, on exit = y
y	FF instance to be copied from
n	size of FF in BIGs

8.15.3.5 FF_2048_crt()

```
void FF_2048_crt (
            BIG_1024_58 * r,
            BIG_1024_58 * rp,
            BIG_1024_58 * rq,
            BIG_1024_58 * p,
            BIG_1024_58 * q,
            int n )
```

Parameters

r	FF instance, on exit the solution of the system
rp	FF instance, solution modulo p
rq	FF instance, solution modulo q
p	FF instance, MUST be coprime with q
q	FF instance, MUST be coprime with p
n	size of p and q in BIGs

8.15.3.6 FF_2048_dec()

```
void FF_2048_dec (
            BIG_1024_58 * x,
            int m,
            int n )
```

Parameters

x	FF instance, on exit = x-m
m	an integer to be subtracted from x
n	size of FF in BIGs

8.15.3.7 FF_2048_dmod()

```
void FF_2048_dmod (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            BIG_1024_58 * z,
            int n )
```

This is slow

Parameters

x	FF instance, on exit = y mod z
y	FF instance, of double length 2∗n
z	FF modulus
n	size of FF in BIGs

8.15.3.8 FF_2048_fromOctet()

```
void FF_2048_fromOctet (
            BIG_1024_58 * x,
            octet * S,
            int n )
```

Creates FF from big-endian base 256 form.

Parameters

x	FF instance to be created from an octet string
S	input octet string
n	size of FF in BIGs

8.15.3.9 FF_2048_inc()

```
void FF_2048_inc (
            BIG_1024_58 * x,
            int m,
            int n )
```

Parameters

x	FF instance, on exit = x+m
m	an integer to be added to x
n	size of FF in BIGs

8.15.3.10 FF_2048_init()

```
void FF_2048_init (
            BIG_1024_58 * x,
            sign32 m,
            int n )
```

Parameters

x	FF instance to be copied to, on exit = m
m	integer
n	size of FF in BIGs

8.15.3.11 FF_2048_invmod2m()

```
void FF_2048_invmod2m (
            BIG_1024_58 U[ ],
            BIG_1024_58 a[ ],
            int n )
```

Parameters

U	FF instance, on exit 1/a mod 2^(n∗BIGBITS)
a	FF instance
n	size of FF in BIGs

8.15.3.12 FF_2048_invmodp()

```
void FF_2048_invmodp (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            BIG_1024_58 * z,
            int n )
```

Parameters

x	FF instance, on exit = 1/y mod z
y	FF instance
z	FF prime modulus
n	size of FF in BIGs

8.15.3.13 FF_2048_iszilch()

```
int FF_2048_iszilch (
            BIG_1024_58 * x,
            int n )
```

Parameters

x	FF number to be tested
n	size of FF in BIGs

Returns

1 if zero, else returns 0

8.15.3.14 FF_2048_lastbits()

```
int FF_2048_lastbits (
            BIG_1024_58 * x,
            int m )
```

Parameters

x	FF number
m	number of bits to return. Assumed to be less than BASEBITS.

Returns

least significant n bits as an integer

8.15.3.15 FF_2048_mod()

```
void FF_2048_mod (
            BIG_1024_58 * x,
            BIG_1024_58 * p,
            int n )
```

This is slow

Parameters

x	FF instance to be reduced mod p - on exit = x mod p
p	FF modulus
n	size of FF in BIGs

8.15.3.16 FF_2048_mul()

```
void FF_2048_mul (
            BIG_1024_58 * x,
```

```
BIG_1024_58 * y,
BIG_1024_58 * z,
int n )
```

Uses Karatsuba method internally

Parameters

x	FF instance, on exit = y∗z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.15.3.17 FF_2048_norm()

```
void FF_2048_norm (
        BIG_1024_58 * x,
        int n )
```

Parameters

x	FF instance to be normalised
n	size of FF in BIGs

8.15.3.18 FF_2048_one()

```
void FF_2048_one (
        BIG_1024_58 * x,
        int n )
```

Parameters

x	FF instance to be set to unity
n	size of FF in BIGs

8.15.3.19 FF_2048_output()

```
void FF_2048_output (
        BIG_1024_58 * x,
        int n )
```

Parameters

x	FF instance to be printed
n	size of FF in BIGs

8.15.3.20 FF_2048_parity()

```
int FF_2048_parity (
            BIG_1024_58 * x )
```

Parameters

x	FF number

Returns

0 or 1

8.15.3.21 FF_2048_pow()

```
void FF_2048_pow (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            BIG_1024_58 * e,
            BIG_1024_58 * p,
            int n )
```

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	FF exponent
p	FF modulus
n	size of FF in BIGs

8.15.3.22 FF_2048_pow2()

```
void FF_2048_pow2 (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            BIG_1024_58 e,
```

```
BIG_1024_58 * y,
BIG_1024_58 f,
BIG_1024_58 * m,
int n )
```

Parameters

r	FF instance, on exit = x^e.y^f mod p
x	FF instance
e	BIG exponent
y	FF instance
f	BIG exponent
m	FF modulus
n	size of FF in BIGs

8.15.3.23 FF_2048_power()

```
void FF_2048_power (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            int e,
            BIG_1024_58 * p,
            int n )
```

For very short integer exponent

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	integer exponent
p	FF modulus
n	size of FF in BIGs

8.15.3.24 FF_2048_prime()

```
int FF_2048_prime (
            BIG_1024_58 * x,
            csprng * R,
            int n )
```

Uses Miller-Rabin Method

Parameters

x	FF instance to be tested
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

Returns

1 if x is (almost certainly) prime, else return 0

8.15.3.25 FF_2048_random()

```
void FF_2048_random (
            BIG_1024_58 * x,
            csprng * R,
            int n )
```

Parameters

x	FF instance, on exit x is a random number of length n BIGs with most significant bit a 1
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

8.15.3.26 FF_2048_randomnum()

```
void FF_2048_randomnum (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            csprng * R,
            int n )
```

Parameters

x	FF instance, on exit x is a random number $<$ y
y	FF instance, the modulus
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

8.15.3.27 FF_2048_rawoutput()

```
void FF_2048_rawoutput (
            BIG_1024_58 * x,
            int n )
```

Parameters

x	FF instance to be printed
n	size of FF in BIGs

8.15.3.28 FF_2048_shl()

```
void FF_2048_shl (
            BIG_1024_58 * x,
            int n )
```

Parameters

x	FF instance to be shifted left
n	size of FF in BIGs

8.15.3.29 FF_2048_shr()

```
void FF_2048_shr (
            BIG_1024_58 * x,
            int n )
```

Parameters

x	FF instance to be shifted right
n	size of FF in BIGs

8.15.3.30 FF_2048_skpow()

```
void FF_2048_skpow (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            BIG_1024_58 * e,
            BIG_1024_58 * p,
            int n,
            int en )
```

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	FF exponent
p	FF modulus
n	size of FF in BIGs
en	size of the exponent in BIGs

8.15.3.31 FF_2048_skpow2()

```
void FF_2048_skpow2 (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            BIG_1024_58 * e,
            BIG_1024_58 * y,
            BIG_1024_58 * f,
            BIG_1024_58 * p,
            int n,
            int en )
```

Parameters

r	FF instance, on exit = x^e.y^f mod p
x	FF instance
e	FF exponent
y	FF instance
f	FF exponent
p	FF modulus
n	size of FF in BIGs
en	size of the exponent in BIGs

8.15.3.32 FF_2048_skspow()

```
void FF_2048_skspow (
            BIG_1024_58 * r,
            BIG_1024_58 * x,
            BIG_1024_58 e,
            BIG_1024_58 * p,
            int n )
```

For short BIG exponent

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	BIG exponent
p	FF modulus
n	size of FF in BIGs

8.15.3.33 FF_2048_sqr()

```
void FF_2048_sqr (
            BIG_1024_58 * x,
```

```
            BIG_1024_58 * y,
            int n )
```

Uses Karatsuba method internally

Parameters

x	FF instance, on exit = y^2
y	FF instance to be squared
n	size of FF in BIGs

8.15.3.34 FF_2048_sub()

```
void FF_2048_sub (
            BIG_1024_58 * x,
            BIG_1024_58 * y,
            BIG_1024_58 * z,
            int n )
```

Parameters

x	FF instance, on exit = y-z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.15.3.35 FF_2048_toOctet()

```
void FF_2048_toOctet (
            octet * S,
            BIG_1024_58 * x,
            int n )
```

Converts an FF to big-endian base 256 form.

Parameters

S	output octet string
x	FF instance to be converted to an octet string
n	size of FF in BIGs

8.15.3.36 FF_2048_zero()

```
void FF_2048_zero (
            BIG_1024_58 * x,
            int n )
```

Parameters

x	FF instance to be set to zero
n	size of FF in BIGs

8.16 ff_4096.h File Reference

FF Header File.

```
#include "big_512_60.h"
#include "config_ff_4096.h"
```

Macros

- #define HFLEN_4096 (FFLEN_4096/2)
- #define P_MBITS_4096 (MODBYTES_512_60∗8)
- #define P_TBITS_4096 (P_MBITS_4096%BASEBITS_512_60)
- #define P_EXCESS_4096(a) (((a[NLEN_512_60-1])>>(P_TBITS_4096))+1)
- #define P_FEXCESS_4096 ((chunk)1<<(BASEBITS_512_60∗NLEN_512_60-P_MBITS_4096-1))

Functions

- void FF_4096_copy (BIG_512_60 ∗x, BIG_512_60 ∗y, int n)

  Copy one FF element of given length to another.
- void FF_4096_init (BIG_512_60 ∗x, sign32 m, int n)

  Initialize an FF element of given length from a 32-bit integer m.
- void FF_4096_zero (BIG_512_60 ∗x, int n)

  Set FF element of given size to zero.
- int FF_4096_iszilch (BIG_512_60 ∗x, int n)

  Tests for FF element equal to zero.
- int FF_4096_parity (BIG_512_60 ∗x)

  return parity of an FF, that is the least significant bit
- int FF_4096_lastbits (BIG_512_60 ∗x, int m)

  return least significant m bits of an FF
- void FF_4096_one (BIG_512_60 ∗x, int n)

  Set FF element of given size to unity.
- int FF_4096_comp (BIG_512_60 ∗x, BIG_512_60 ∗y, int n)

  Compares two FF numbers. Inputs must be normalised externally.
- void FF_4096_add (BIG_512_60 ∗x, BIG_512_60 ∗y, BIG_512_60 ∗z, int n)

  addition of two FFs
- void FF_4096_sub (BIG_512_60 ∗x, BIG_512_60 ∗y, BIG_512_60 ∗z, int n)

subtraction of two FFs
- void FF_4096_inc (BIG_512_60 ∗x, int m, int n)
  increment an FF by an integer,and normalise
- void FF_4096_dec (BIG_512_60 ∗x, int m, int n)
  Decrement an FF by an integer,and normalise.
- void FF_4096_norm (BIG_512_60 ∗x, int n)
  Normalises the components of an FF.
- void FF_4096_shl (BIG_512_60 ∗x, int n)
  Shift left an FF by 1 bit.
- void FF_4096_shr (BIG_512_60 ∗x, int n)
  Shift right an FF by 1 bit.
- void FF_4096_output (BIG_512_60 ∗x, int n)
  Formats and outputs an FF to the console.
- void FF_4096_rawoutput (BIG_512_60 ∗x, int n)
  Formats and outputs an FF to the console, in raw form.
- void FF_4096_toOctet (octet ∗S, BIG_512_60 ∗x, int n)
  Formats and outputs an FF instance to an octet string.
- void FF_4096_fromOctet (BIG_512_60 ∗x, octet ∗S, int n)
  Populates an FF instance from an octet string.
- void FF_4096_mul (BIG_512_60 ∗x, BIG_512_60 ∗y, BIG_512_60 ∗z, int n)
  Multiplication of two FFs.
- void FF_4096_mod (BIG_512_60 ∗x, BIG_512_60 ∗p, int n)
  Reduce FF mod a modulus.
- void FF_4096_sqr (BIG_512_60 ∗x, BIG_512_60 ∗y, int n)
  Square an FF.
- void FF_4096_dmod (BIG_512_60 ∗x, BIG_512_60 ∗y, BIG_512_60 ∗z, int n)
  Reduces a double-length FF with respect to a given modulus.
- void FF_4096_invmodp (BIG_512_60 ∗x, BIG_512_60 ∗y, BIG_512_60 ∗z, int n)
  Invert an FF mod a prime modulus.
- void FF_4096_invmod2m (BIG_512_60 U[ ], BIG_512_60 a[ ], int n)
  Invert an FF mod 2^(n∗BIGBITS)
- void FF_4096_random (BIG_512_60 ∗x, csprng ∗R, int n)
  Create an FF from a random number generator.
- void FF_4096_randomnum (BIG_512_60 ∗x, BIG_512_60 ∗y, csprng ∗R, int n)
  Create a random FF less than a given modulus from a random number generator.
- void FF_4096_skpow (BIG_512_60 ∗r, BIG_512_60 ∗x, BIG_512_60 ∗e, BIG_512_60 ∗p, int n, int en)
  Calculate r=x^e mod p, side channel resistant.
- void FF_4096_skspow (BIG_512_60 ∗r, BIG_512_60 ∗x, BIG_512_60 e, BIG_512_60 ∗p, int n)
  Calculate r=x^e mod p, side channel resistant.
- void FF_4096_skpow2 (BIG_512_60 ∗r, BIG_512_60 ∗x, BIG_512_60 ∗e, BIG_512_60 ∗y, BIG_512_60 ∗f, BIG_512_60 ∗p, int n, int en)
  Calculate r=x^e.y^f mod p for big e and f, side channel resistant.
- void FF_4096_power (BIG_512_60 ∗r, BIG_512_60 ∗x, int e, BIG_512_60 ∗p, int n)
  Calculate r=x^e mod p.
- void FF_4096_pow (BIG_512_60 ∗r, BIG_512_60 ∗x, BIG_512_60 ∗e, BIG_512_60 ∗p, int n)
  Calculate r=x^e mod p.
- void FF_4096_pow2 (BIG_512_60 ∗r, BIG_512_60 ∗x, BIG_512_60 e, BIG_512_60 ∗y, BIG_512_60 f, BIG_512_60 ∗m, int n)
  Calculate r=x^e.y^f mod m.
- int FF_4096_cfactor (BIG_512_60 ∗x, sign32 s, int n)
  Test if an FF has factor in common with integer s.

- int FF_4096_prime (BIG_512_60 *x, csprng *R, int n)

  Test if an FF is prime.
- void FF_4096_crt (BIG_512_60 *r, BIG_512_60 *rp, BIG_512_60 *rq, BIG_512_60 *p, BIG_512_60 *q, int n)

  Combine rp and rq using the Chinese Remainder Theorem.

8.16.1 Detailed Description

Author

Mike Scott

8.16.2 Macro Definition Documentation

8.16.2.1 HFLEN_4096

```
#define HFLEN_4096 (FFLEN_4096/2)
```

Useful for half-size RSA private key operations

8.16.2.2 P_EXCESS_4096

```
#define P_EXCESS_4096(
              a ) (((a[NLEN_512_60-1])>>(P_TBITS_4096))+1)
```

TODO

8.16.2.3 P_FEXCESS_4096

```
#define P_FEXCESS_4096 ((chunk)1<<(BASEBITS_512_60*NLEN_512_60-P_MBITS_4096-1))
```

TODO

8.16.2.4 P_MBITS_4096

```
#define P_MBITS_4096 (MODBYTES_512_60*8)
```

Number of bits in modulus

8.16.2.5 P_TBITS_4096

```
#define P_TBITS_4096 (P_MBITS_4096%BASEBITS_512_60)
```

TODO

8.16.3 Function Documentation

8.16.3.1 FF_4096_add()

```
void FF_4096_add (
            BIG_512_60 * x,
            BIG_512_60 * y,
            BIG_512_60 * z,
            int n )
```

Parameters

x	FF instance, on exit = y+z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.16.3.2 FF_4096_cfactor()

```
int FF_4096_cfactor (
            BIG_512_60 * x,
            sign32 s,
            int n )
```

Parameters

x	FF instance to be tested
s	the supplied integer
n	size of FF in BIGs

Returns

1 if gcd(x,s)!=1, else return 0

8.16.3.3 FF_4096_comp()

```
int FF_4096_comp (
            BIG_512_60 * x,
            BIG_512_60 * y,
            int n )
```

Parameters

x	first FF number to be compared
y	second FF number to be compared
n	size of FF in BIGs

Returns

-1 is x<y, 0 if x=y, 1 if x>y

8.16.3.4 FF_4096_copy()

```
void FF_4096_copy (
            BIG_512_60 * x,
            BIG_512_60 * y,
            int n )
```

Parameters

x	FF instance to be copied to, on exit = y
y	FF instance to be copied from
n	size of FF in BIGs

8.16.3.5 FF_4096_crt()

```
void FF_4096_crt (
            BIG_512_60 * r,
            BIG_512_60 * rp,
            BIG_512_60 * rq,
            BIG_512_60 * p,
            BIG_512_60 * q,
            int n )
```

Parameters

r	FF instance, on exit the solution of the system
rp	FF instance, solution modulo p
rq	FF instance, solution modulo q
p	FF instance, MUST be coprime with q
q	FF instance, MUST be coprime with p
n	size of p and q in BIGs

8.16.3.6 FF_4096_dec()

```
void FF_4096_dec (
            BIG_512_60 * x,
            int m,
            int n )
```

Parameters

x	FF instance, on exit = x-m
m	an integer to be subtracted from x
n	size of FF in BIGs

8.16.3.7 FF_4096_dmod()

```
void FF_4096_dmod (
            BIG_512_60 * x,
            BIG_512_60 * y,
            BIG_512_60 * z,
            int n )
```

This is slow

Parameters

x	FF instance, on exit = y mod z
y	FF instance, of double length 2∗n
z	FF modulus
n	size of FF in BIGs

8.16.3.8 FF_4096_fromOctet()

```
void FF_4096_fromOctet (
            BIG_512_60 * x,
            octet * S,
            int n )
```

Creates FF from big-endian base 256 form.

Parameters

x	FF instance to be created from an octet string
S	input octet string
n	size of FF in BIGs

8.16.3.9 FF_4096_inc()

```
void FF_4096_inc (
            BIG_512_60 * x,
            int m,
            int n )
```

Parameters

x	FF instance, on exit = x+m
m	an integer to be added to x
n	size of FF in BIGs

8.16.3.10 FF_4096_init()

```
void FF_4096_init (
            BIG_512_60 * x,
            sign32 m,
            int n )
```

Parameters

x	FF instance to be copied to, on exit = m
m	integer
n	size of FF in BIGs

8.16.3.11 FF_4096_invmod2m()

```
void FF_4096_invmod2m (
            BIG_512_60 U[ ],
            BIG_512_60 a[ ],
            int n )
```

Parameters

U	FF instance, on exit 1/a mod 2^(n∗BIGBITS)
a	FF instance
n	size of FF in BIGs

8.16.3.12 FF_4096_invmodp()

```
void FF_4096_invmodp (
            BIG_512_60 * x,
            BIG_512_60 * y,
            BIG_512_60 * z,
            int n )
```

Parameters

x	FF instance, on exit = 1/y mod z
y	FF instance
z	FF prime modulus
n	size of FF in BIGs

8.16.3.13 FF_4096_iszilch()

```
int FF_4096_iszilch (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF number to be tested
n	size of FF in BIGs

Returns

1 if zero, else returns 0

8.16.3.14 FF_4096_lastbits()

```
int FF_4096_lastbits (
            BIG_512_60 * x,
            int m )
```

Parameters

x	FF number
m	number of bits to return. Assumed to be less than BASEBITS.

Returns

least significant n bits as an integer

8.16.3.15 FF_4096_mod()

```
void FF_4096_mod (
            BIG_512_60 * x,
            BIG_512_60 * p,
            int n )
```

This is slow

Parameters

x	FF instance to be reduced mod p - on exit = x mod p
p	FF modulus
n	size of FF in BIGs

8.16.3.16 FF_4096_mul()

```
void FF_4096_mul (
            BIG_512_60 * x,
            BIG_512_60 * y,
            BIG_512_60 * z,
            int n )
```

Uses Karatsuba method internally

Parameters

x	FF instance, on exit = y∗z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.16.3.17 FF_4096_norm()

```
void FF_4096_norm (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF instance to be normalised
n	size of FF in BIGs

8.16.3.18 FF_4096_one()

```
void FF_4096_one (
              BIG_512_60 * x,
              int n )
```

Parameters

x	FF instance to be set to unity
n	size of FF in BIGs

8.16.3.19 FF_4096_output()

```
void FF_4096_output (
              BIG_512_60 * x,
              int n )
```

Parameters

x	FF instance to be printed
n	size of FF in BIGs

8.16.3.20 FF_4096_parity()

```
int FF_4096_parity (
              BIG_512_60 * x )
```

Parameters

x	FF number

Returns

0 or 1

8.16.3.21 FF_4096_pow()

```
void FF_4096_pow (
              BIG_512_60 * r,
              BIG_512_60 * x,
              BIG_512_60 * e,
              BIG_512_60 * p,
              int n )
```

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	FF exponent
p	FF modulus
n	size of FF in BIGs

8.16.3.22 FF_4096_pow2()

```
void FF_4096_pow2 (
            BIG_512_60 * r,
            BIG_512_60 * x,
            BIG_512_60 e,
            BIG_512_60 * y,
            BIG_512_60 f,
            BIG_512_60 * m,
            int n )
```

Parameters

r	FF instance, on exit = x^e.y^f mod p
x	FF instance
e	BIG exponent
y	FF instance
f	BIG exponent
m	FF modulus
n	size of FF in BIGs

8.16.3.23 FF_4096_power()

```
void FF_4096_power (
            BIG_512_60 * r,
            BIG_512_60 * x,
            int e,
            BIG_512_60 * p,
            int n )
```

For very short integer exponent

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	integer exponent
p	FF modulus
n	size of FF in BIGs

8.16.3.24 FF_4096_prime()

```
int FF_4096_prime (
            BIG_512_60 * x,
            csprng * R,
            int n )
```

Uses Miller-Rabin Method

Parameters

x	FF instance to be tested
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

Returns

1 if x is (almost certainly) prime, else return 0

8.16.3.25 FF_4096_random()

```
void FF_4096_random (
            BIG_512_60 * x,
            csprng * R,
            int n )
```

Parameters

x	FF instance, on exit x is a random number of length n BIGs with most significant bit a 1
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

8.16.3.26 FF_4096_randomnum()

```
void FF_4096_randomnum (
            BIG_512_60 * x,
            BIG_512_60 * y,
            csprng * R,
            int n )
```

Parameters

x	FF instance, on exit x is a random number $<$ y

Parameters

y	FF instance, the modulus
R	an instance of a Cryptographically Secure Random Number Generator
n	size of FF in BIGs

8.16.3.27 FF_4096_rawoutput()

```
void FF_4096_rawoutput (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF instance to be printed
n	size of FF in BIGs

8.16.3.28 FF_4096_shl()

```
void FF_4096_shl (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF instance to be shifted left
n	size of FF in BIGs

8.16.3.29 FF_4096_shr()

```
void FF_4096_shr (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF instance to be shifted right
n	size of FF in BIGs

8.16.3.30 FF_4096_skpow()

```
void FF_4096_skpow (
            BIG_512_60 * r,
            BIG_512_60 * x,
            BIG_512_60 * e,
            BIG_512_60 * p,
            int n,
            int en )
```

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	FF exponent
p	FF modulus
n	size of FF in BIGs
en	size of the exponent in BIGs

8.16.3.31 FF_4096_skpow2()

```
void FF_4096_skpow2 (
            BIG_512_60 * r,
            BIG_512_60 * x,
            BIG_512_60 * e,
            BIG_512_60 * y,
            BIG_512_60 * f,
            BIG_512_60 * p,
            int n,
            int en )
```

Parameters

r	FF instance, on exit = x^e.y^f mod p
x	FF instance
e	FF exponent
y	FF instance
f	FF exponent
p	FF modulus
n	size of FF in BIGs
en	size of the exponent in BIGs

8.16.3.32 FF_4096_skspow()

```
void FF_4096_skspow (
            BIG_512_60 * r,
```

```
            BIG_512_60 * x,
            BIG_512_60 e,
            BIG_512_60 * p,
            int n )
```

For short BIG exponent

Parameters

r	FF instance, on exit = x^e mod p
x	FF instance
e	BIG exponent
p	FF modulus
n	size of FF in BIGs

8.16.3.33 FF_4096_sqr()

```
void FF_4096_sqr (
            BIG_512_60 * x,
            BIG_512_60 * y,
            int n )
```

Uses Karatsuba method internally

Parameters

x	FF instance, on exit = y^2
y	FF instance to be squared
n	size of FF in BIGs

8.16.3.34 FF_4096_sub()

```
void FF_4096_sub (
            BIG_512_60 * x,
            BIG_512_60 * y,
            BIG_512_60 * z,
            int n )
```

Parameters

x	FF instance, on exit = y-z
y	FF instance
z	FF instance
n	size of FF in BIGs

8.16.3.35 FF_4096_toOctet()

```
void FF_4096_toOctet (
            octet * S,
            BIG_512_60 * x,
            int n )
```

Converts an FF to big-endian base 256 form.

Parameters

S	output octet string
x	FF instance to be converted to an octet string
n	size of FF in BIGs

8.16.3.36 FF_4096_zero()

```
void FF_4096_zero (
            BIG_512_60 * x,
            int n )
```

Parameters

x	FF instance to be set to zero
n	size of FF in BIGs

8.17 fp12_BLS381.h File Reference

FP12 Header File.

```
#include "fp4_BLS381.h"
```

Data Structures

- struct FP12_BLS381

    FP12 Structure - towered over three FP4.

Functions

- int FP12_BLS381_iszilch (FP12_BLS381 ∗x)

    Tests for FP12 equal to zero.
- int FP12_BLS381_isunity (FP12_BLS381 ∗x)

    Tests for FP12 equal to unity.
- void FP12_BLS381_copy (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Copy FP12 to another FP12.
- void FP12_BLS381_one (FP12_BLS381 ∗x)

    Set FP12 to unity.
- void FP12_BLS381_zero (FP12_BLS381 ∗x)

    Set FP12 to zero.
- int FP12_BLS381_equals (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Tests for equality of two FP12s.
- void FP12_BLS381_conj (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Conjugation of FP12.
- void FP12_BLS381_from_FP4 (FP12_BLS381 ∗x, FP4_BLS381 ∗a)

    Initialise FP12 from single FP4.
- void FP12_BLS381_from_FP4s (FP12_BLS381 ∗x, FP4_BLS381 ∗a, FP4_BLS381 ∗b, FP4_BLS381 ∗c)

    Initialise FP12 from three FP4s.
- void FP12_BLS381_usqr (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Fast Squaring of an FP12 in "unitary" form.
- void FP12_BLS381_sqr (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Squaring an FP12.
- void FP12_BLS381_smul (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Fast multiplication of two sparse FP12s that arises from ATE pairing line functions.
- void FP12_BLS381_ssmul (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Fast multiplication of what may be sparse multiplicands.
- void FP12_BLS381_mul (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Full unconditional Multiplication of two FP12s.
- void FP12_BLS381_inv (FP12_BLS381 ∗x, FP12_BLS381 ∗y)

    Inverting an FP12.
- void FP12_BLS381_pow (FP12_BLS381 ∗r, FP12_BLS381 ∗x, BIG_384_58 b)

    Raises an FP12 to the power of a BIG.
- void FP12_BLS381_pinpow (FP12_BLS381 ∗x, int i, int b)

    Raises an FP12 instance x to a small integer power, side-channel resistant.
- void FP12_BLS381_compow (FP4_BLS381 ∗c, FP12_BLS381 ∗x, BIG_384_58 e, BIG_384_58 r)

    Raises an FP12 instance x to a BIG power, compressed to FP4.
- void FP12_BLS381_pow4 (FP12_BLS381 ∗r, FP12_BLS381 ∗x, BIG_384_58 ∗b)

    Calculate x[0]^b[0].x[1]^b[1].x[2]^b[2].x[3]^b[3], side-channel resistant.
- void FP12_BLS381_frob (FP12_BLS381 ∗x, FP2_BLS381 ∗f)

    Raises an FP12 to the power of the internal modulus p, using the Frobenius.
- void FP12_BLS381_reduce (FP12_BLS381 ∗x)

    Reduces all components of possibly unreduced FP12 mod Modulus.
- void FP12_BLS381_norm (FP12_BLS381 ∗x)

    Normalises the components of an FP12.
- void FP12_BLS381_output (FP12_BLS381 ∗x)

    Formats and outputs an FP12 to the console.
- void FP12_BLS381_toOctet (octet ∗S, FP12_BLS381 ∗x)

    Formats and outputs an FP12 instance to an octet string.
- void FP12_BLS381_fromOctet (FP12_BLS381 ∗x, octet ∗S)

Creates an FP12 instance from an octet string.
- void FP12_BLS381_trace (FP4_BLS381 *t, FP12_BLS381 *x)

  Calculate the trace of an FP12.
- void FP12_BLS381_cmove (FP12_BLS381 *x, FP12_BLS381 *y, int s)

  Conditional copy of FP12 number.

Variables

- const BIG_384_58 Fra_BLS381
- const BIG_384_58 Frb_BLS381

8.17.1 Detailed Description

Author

Mike Scott

8.17.2 Function Documentation

8.17.2.1 FP12_BLS381_cmove()

```
void FP12_BLS381_cmove (
            FP12_BLS381 * x,
            FP12_BLS381 * y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	FP12 instance, set to y if s!=0
y	another FP12 instance
s	copy only takes place if not equal to 0

8.17.2.2 FP12_BLS381_compow()

```
void FP12_BLS381_compow (
            FP4_BLS381 * c,
            FP12_BLS381 * x,
            BIG_384_58 e,
            BIG_384_58 r )
```

Parameters

c	FP4 instance, on exit = x^(e mod r) as FP4
x	FP12 input
e	BIG exponent
r	BIG group order

8.17.2.3 FP12_BLS381_conj()

```
void FP12_BLS381_conj (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

If y=(a,b,c) (where a,b,c are its three FP4 components) on exit x=(conj(a),-conj(b),conj(c))

Parameters

x	FP12 instance, on exit = conj(y)
y	FP12 instance

8.17.2.4 FP12_BLS381_copy()

```
void FP12_BLS381_copy (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = y
y	FP12 instance to be copied

8.17.2.5 FP12_BLS381_equals()

```
int FP12_BLS381_equals (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance to be compared
y	FP12 instance to be compared

Returns

1 if x=y, else returns 0

8.17.2.6 FP12_BLS381_frob()

```
void FP12_BLS381_frob (
            FP12_BLS381 * x,
            FP2_BLS381 * f )
```

Parameters

x	FP12 instance, on exit = x^p
f	FP2 precalculated Frobenius constant

8.17.2.7 FP12_BLS381_from_FP4()

```
void FP12_BLS381_from_FP4 (
            FP12_BLS381 * x,
            FP4_BLS381 * a )
```

Sets first FP4 component of an FP12, other components set to zero

Parameters

x	FP12 instance to be initialised
a	FP4 to form first part of FP4

8.17.2.8 FP12_BLS381_from_FP4s()

```
void FP12_BLS381_from_FP4s (
            FP12_BLS381 * x,
            FP4_BLS381 * a,
            FP4_BLS381 * b,
            FP4_BLS381 * c )
```

Parameters

x	FP12 instance to be initialised
a	FP4 to form first part of FP12
b	FP4 to form second part of FP12
c	FP4 to form third part of FP12

8.17.2.9 FP12_BLS381_fromOctet()

```
void FP12_BLS381_fromOctet (
            FP12_BLS381 * x,
            octet * S )
```

De-serializes the components of an FP12 to create an FP12 from big-endian base 256 components.

Parameters

x	FP12 instance to be created from an octet string
S	input octet string

8.17.2.10 FP12_BLS381_inv()

```
void FP12_BLS381_inv (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = 1/y
y	FP12 instance

8.17.2.11 FP12_BLS381_isunity()

```
int FP12_BLS381_isunity (
            FP12_BLS381 * x )
```

Parameters

x	FP12 number to be tested

Returns

1 if unity, else returns 0

8.17.2.12 FP12_BLS381_iszilch()

```
int FP12_BLS381_iszilch (
            FP12_BLS381 * x )
```

Parameters

x	FP12 number to be tested

Returns

1 if zero, else returns 0

8.17.2.13 FP12_BLS381_mul()

```
void FP12_BLS381_mul (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = x*y
y	FP12 instance, the multiplier

8.17.2.14 FP12_BLS381_norm()

```
void FP12_BLS381_norm (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance to be normalised

8.17.2.15 FP12_BLS381_one()

```
void FP12_BLS381_one (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance to be set to one

8.17.2.16 FP12_BLS381_output()

```
void FP12_BLS381_output (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance to be printed

8.17.2.17 FP12_BLS381_pinpow()

```
void FP12_BLS381_pinpow (
            FP12_BLS381 * x,
            int i,
            int b )
```

Parameters

x	FP12 instance, on exit = x^i
i	small integer exponent
b	maximum number of bits in exponent

8.17.2.18 FP12_BLS381_pow()

```
void FP12_BLS381_pow (
            FP12_BLS381 * r,
            FP12_BLS381 * x,
            BIG_384_58 b )
```

Parameters

r	FP12 instance, on exit = y^b
x	FP12 instance
b	BIG number

8.17.2.19 FP12_BLS381_pow4()

```
void FP12_BLS381_pow4 (
            FP12_BLS381 * r,
            FP12_BLS381 * x,
            BIG_384_58 * b )
```

Parameters

r	FP12 instance, on exit = x[0]^b[0].x[1]^b[1].x[2]^b[2].x[3]^b[3]
x	FP12 array with 4 FP12s
b	BIG array of 4 exponents

8.17.2.20 FP12_BLS381_reduce()

```
void FP12_BLS381_reduce (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance, on exit reduced mod Modulus

8.17.2.21 FP12_BLS381_smul()

```
void FP12_BLS381_smul (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = x*y
y	FP12 instance, of special form

8.17.2.22 FP12_BLS381_sqr()

```
void FP12_BLS381_sqr (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = y^2
y	FP12 instance

8.17.2.23 FP12_BLS381_ssmul()

```
void FP12_BLS381_ssmul (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = x*y
y	FP12 instance, of special form

8.17.2.24 FP12_BLS381_toOctet()

```
void FP12_BLS381_toOctet (
            octet * S,
            FP12_BLS381 * x )
```

Serializes the components of an FP12 to big-endian base 256 form.

Parameters

S	output octet string
x	FP12 instance to be converted to an octet string

8.17.2.25 FP12_BLS381_trace()

```
void FP12_BLS381_trace (
            FP4_BLS381 * t,
            FP12_BLS381 * x )
```

Parameters

t	FP4 trace of x, on exit = tr(x)
x	FP12 instance

8.17.2.26 FP12_BLS381_usqr()

```
void FP12_BLS381_usqr (
            FP12_BLS381 * x,
            FP12_BLS381 * y )
```

Parameters

x	FP12 instance, on exit = y^2
y	FP4 instance, must be unitary

8.17.2.27 FP12_BLS381_zero()

```
void FP12_BLS381_zero (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance to be set to zero

8.17.3 Variable Documentation

8.17.3.1 Fra_BLS381

```
const BIG_384_58 Fra_BLS381
```

real part of BN curve Frobenius Constant

8.17.3.2 Frb_BLS381

```
const BIG_384_58 Frb_BLS381
```

imaginary part of BN curve Frobenius Constant

8.18 fp2_BLS381.h File Reference

FP2 Header File.

```
#include "fp_BLS381.h"
```

Data Structures

- struct FP2_BLS381

  FP2 Structure - quadratic extension field.

Functions

- int FP2_BLS381_iszilch (FP2_BLS381 ∗x)
  Tests for FP2 equal to zero.
- void FP2_BLS381_cmove (FP2_BLS381 ∗x, FP2_BLS381 ∗y, int s)
  Conditional copy of FP2 number.
- int FP2_BLS381_isunity (FP2_BLS381 ∗x)
  Tests for FP2 equal to one.
- int FP2_BLS381_equals (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Tests for equality of two FP2s.
- void FP2_BLS381_from_FPs (FP2_BLS381 ∗x, FP_BLS381 ∗a, FP_BLS381 ∗b)
  Initialise FP2 from two FP numbers.
- void FP2_BLS381_from_BIGs (FP2_BLS381 ∗x, BIG_384_58 a, BIG_384_58 b)
  Initialise FP2 from two BIG integers.
- void FP2_BLS381_from_FP (FP2_BLS381 ∗x, FP_BLS381 ∗a)
  Initialise FP2 from single FP.
- void FP2_BLS381_from_BIG (FP2_BLS381 ∗x, BIG_384_58 a)
  Initialise FP2 from single BIG.
- void FP2_BLS381_copy (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Copy FP2 to another FP2.
- void FP2_BLS381_zero (FP2_BLS381 ∗x)
  Set FP2 to zero.
- void FP2_BLS381_one (FP2_BLS381 ∗x)
  Set FP2 to unity.
- void FP2_BLS381_neg (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Negation of FP2.
- void FP2_BLS381_conj (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Conjugation of FP2.
- void FP2_BLS381_add (FP2_BLS381 ∗x, FP2_BLS381 ∗y, FP2_BLS381 ∗z)
  addition of two FP2s
- void FP2_BLS381_sub (FP2_BLS381 ∗x, FP2_BLS381 ∗y, FP2_BLS381 ∗z)
  subtraction of two FP2s
- void FP2_BLS381_pmul (FP2_BLS381 ∗x, FP2_BLS381 ∗y, FP_BLS381 ∗b)
  Multiplication of an FP2 by an FP.
- void FP2_BLS381_imul (FP2_BLS381 ∗x, FP2_BLS381 ∗y, int i)
  Multiplication of an FP2 by a small integer.
- void FP2_BLS381_sqr (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Squaring an FP2.
- void FP2_BLS381_mul (FP2_BLS381 ∗x, FP2_BLS381 ∗y, FP2_BLS381 ∗z)
  Multiplication of two FP2s.
- void FP2_BLS381_output (FP2_BLS381 ∗x)
  Formats and outputs an FP2 to the console.
- void FP2_BLS381_rawoutput (FP2_BLS381 ∗x)
  Formats and outputs an FP2 to the console in raw form (for debugging)
- void FP2_BLS381_inv (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Inverting an FP2.
- void FP2_BLS381_div2 (FP2_BLS381 ∗x, FP2_BLS381 ∗y)
  Divide an FP2 by 2.
- void FP2_BLS381_mul_ip (FP2_BLS381 ∗x)
  Multiply an FP2 by (1+sqrt(-1))
- void FP2_BLS381_div_ip2 (FP2_BLS381 ∗x)

Divide an FP2 by (1+sqrt(-1))/2 -.
- void FP2_BLS381_div_ip (FP2_BLS381 *x)

  Divide an FP2 by (1+sqrt(-1))
- void FP2_BLS381_norm (FP2_BLS381 *x)

  Normalises the components of an FP2.
- void FP2_BLS381_reduce (FP2_BLS381 *x)

  Reduces all components of possibly unreduced FP2 mod Modulus.
- void FP2_BLS381_pow (FP2_BLS381 *x, FP2_BLS381 *y, BIG_384_58 b)

  Raises an FP2 to the power of a BIG.
- int FP2_BLS381_sqrt (FP2_BLS381 *x, FP2_BLS381 *y)

  Square root of an FP2.
- void FP2_BLS381_times_i (FP2_BLS381 *x)

  Multiply an FP2 by sqrt(-1)

8.18.1 Detailed Description

Author

Mike Scott

8.18.2 Function Documentation

8.18.2.1 FP2_BLS381_add()

```
void FP2_BLS381_add (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            FP2_BLS381 * z )
```

Parameters

x	FP2 instance, on exit = y+z
y	FP2 instance
z	FP2 instance

8.18.2.2 FP2_BLS381_cmove()

```
void FP2_BLS381_cmove (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	FP2 instance, set to y if s!=0
y	another FP2 instance
s	copy only takes place if not equal to 0

8.18.2.3 FP2_BLS381_conj()

```
void FP2_BLS381_conj (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

If y=(a,b) on exit x=(a,-b)

Parameters

x	FP2 instance, on exit = conj(y)
y	FP2 instance

8.18.2.4 FP2_BLS381_copy()

```
void FP2_BLS381_copy (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = y
y	FP2 instance to be copied

8.18.2.5 FP2_BLS381_div2()

```
void FP2_BLS381_div2 (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = y/2
y	FP2 instance

8.18.2.6 FP2_BLS381_div_ip()

```
void FP2_BLS381_div_ip (
            FP2_BLS381 * x )
```

Note that (1+sqrt(-1)) is irreducible for FP4

Parameters

x	FP2 instance, on exit = x/(1+sqrt(-1))

8.18.2.7 FP2_BLS381_div_ip2()

```
void FP2_BLS381_div_ip2 (
            FP2_BLS381 * x )
```

Note that (1+sqrt(-1)) is irreducible for FP4

Parameters

x	FP2 instance, on exit = 2x/(1+sqrt(-1))

8.18.2.8 FP2_BLS381_equals()

```
int FP2_BLS381_equals (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance to be compared
y	FP2 instance to be compared

Returns

1 if x=y, else returns 0

8.18.2.9 FP2_BLS381_from_BIG()

```
void FP2_BLS381_from_BIG (
            FP2_BLS381 * x,
            BIG_384_58 a )
```

Imaginary part is set to zero

Parameters

x	FP2 instance to be initialised
a	BIG to form real part of FP2

8.18.2.10 FP2_BLS381_from_BIGs()

```
void FP2_BLS381_from_BIGs (
            FP2_BLS381 * x,
            BIG_384_58 a,
            BIG_384_58 b )
```

Parameters

x	FP2 instance to be initialised
a	BIG to form real part of FP2
b	BIG to form imaginary part of FP2

8.18.2.11 FP2_BLS381_from_FP()

```
void FP2_BLS381_from_FP (
            FP2_BLS381 * x,
            FP_BLS381 * a )
```

Imaginary part is set to zero

Parameters

x	FP2 instance to be initialised
a	FP to form real part of FP2

8.18.2.12 FP2_BLS381_from_FPs()

```
void FP2_BLS381_from_FPs (
            FP2_BLS381 * x,
```

```
              FP_BLS381 * a,
              FP_BLS381 * b )
```

Parameters

x	FP2 instance to be initialised
a	FP to form real part of FP2
b	FP to form imaginary part of FP2

8.18.2.13 FP2_BLS381_imul()

```
void FP2_BLS381_imul (
              FP2_BLS381 * x,
              FP2_BLS381 * y,
              int i )
```

Parameters

x	FP2 instance, on exit = y*i
y	FP2 instance
i	an integer

8.18.2.14 FP2_BLS381_inv()

```
void FP2_BLS381_inv (
              FP2_BLS381 * x,
              FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = 1/y
y	FP2 instance

8.18.2.15 FP2_BLS381_isunity()

```
int FP2_BLS381_isunity (
              FP2_BLS381 * x )
```

Parameters

x	FP2 instance to be tested

Returns

1 if x=1, else returns 0

8.18.2.16 FP2_BLS381_iszilch()

```
int FP2_BLS381_iszilch (
            FP2_BLS381 * x )
```

Parameters

x	FP2 number to be tested

Returns

1 if zero, else returns 0

8.18.2.17 FP2_BLS381_mul()

```
void FP2_BLS381_mul (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            FP2_BLS381 * z )
```

Parameters

x	FP2 instance, on exit = y∗z
y	FP2 instance
z	FP2 instance

8.18.2.18 FP2_BLS381_mul_ip()

```
void FP2_BLS381_mul_ip (
            FP2_BLS381 * x )
```

Note that (1+sqrt(-1)) is irreducible for FP4

Parameters

x	FP2 instance, on exit = x∗(1+sqrt(-1))

8.18.2.19 FP2_BLS381_neg()

```
void FP2_BLS381_neg (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = -y
y	FP2 instance

8.18.2.20 FP2_BLS381_norm()

```
void FP2_BLS381_norm (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance to be normalised

8.18.2.21 FP2_BLS381_one()

```
void FP2_BLS381_one (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance to be set to one

8.18.2.22 FP2_BLS381_output()

```
void FP2_BLS381_output (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance

8.18.2.23 FP2_BLS381_pmul()

```
void FP2_BLS381_pmul (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            FP_BLS381 * b )
```

Parameters

x	FP2 instance, on exit = y∗b
y	FP2 instance
b	FP residue

8.18.2.24 FP2_BLS381_pow()

```
void FP2_BLS381_pow (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            BIG_384_58 b )
```

Parameters

x	FP2 instance, on exit = y^b
y	FP2 instance
b	BIG number

8.18.2.25 FP2_BLS381_rawoutput()

```
void FP2_BLS381_rawoutput (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance

8.18.2.26 FP2_BLS381_reduce()

```
void FP2_BLS381_reduce (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance, on exit reduced mod Modulus

8.18.2.27 FP2_BLS381_sqr()

```
void FP2_BLS381_sqr (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = y^2
y	FP2 instance

8.18.2.28 FP2_BLS381_sqrt()

```
int FP2_BLS381_sqrt (
            FP2_BLS381 * x,
            FP2_BLS381 * y )
```

Parameters

x	FP2 instance, on exit = sqrt(y)
y	FP2 instance

8.18.2.29 FP2_BLS381_sub()

```
void FP2_BLS381_sub (
            FP2_BLS381 * x,
            FP2_BLS381 * y,
            FP2_BLS381 * z )
```

Parameters

x	FP2 instance, on exit = y-z
y	FP2 instance
z	FP2 instance

8.18.2.30 FP2_BLS381_times_i()

```
void FP2_BLS381_times_i (
            FP2_BLS381 * x )
```

Note that -1 is QNR

Parameters

x	FP2 instance, on exit = x∗sqrt(-1)

8.18.2.31 FP2_BLS381_zero()

```
void FP2_BLS381_zero (
            FP2_BLS381 * x )
```

Parameters

x	FP2 instance to be set to zero

8.19 fp4_BLS381.h File Reference

FP4 Header File.

```
#include "fp2_BLS381.h"
#include "config_curve_BLS381.h"
```

Data Structures

- struct FP4_BLS381

  FP4 Structure - towered over two FP2.

Functions

- int FP4_BLS381_iszilch (FP4_BLS381 ∗x)

  Tests for FP4 equal to zero.
- int FP4_BLS381_isunity (FP4_BLS381 ∗x)

  Tests for FP4 equal to unity.
- int FP4_BLS381_equals (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Tests for equality of two FP4s.
- int FP4_BLS381_isreal (FP4_BLS381 ∗x)

  Tests for FP4 having only a real part and no imaginary part.
- void FP4_BLS381_from_FP2s (FP4_BLS381 ∗x, FP2_BLS381 ∗a, FP2_BLS381 ∗b)

Initialise FP4 from two FP2s.
- void FP4_BLS381_from_FP2 (FP4_BLS381 ∗x, FP2_BLS381 ∗a)

  Initialise FP4 from single FP2.
- void FP4_BLS381_from_FP2H (FP4_BLS381 ∗x, FP2_BLS381 ∗a)

  Initialise FP4 from single FP2.
- void FP4_BLS381_copy (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Copy FP4 to another FP4.
- void FP4_BLS381_zero (FP4_BLS381 ∗x)

  Set FP4 to zero.
- void FP4_BLS381_one (FP4_BLS381 ∗x)

  Set FP4 to unity.
- void FP4_BLS381_neg (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Negation of FP4.
- void FP4_BLS381_conj (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Conjugation of FP4.
- void FP4_BLS381_nconj (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Negative conjugation of FP4.
- void FP4_BLS381_add (FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP4_BLS381 ∗z)

  addition of two FP4s
- void FP4_BLS381_sub (FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP4_BLS381 ∗z)

  subtraction of two FP4s
- void FP4_BLS381_pmul (FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP2_BLS381 ∗a)

  Multiplication of an FP4 by an FP2.
- void FP4_BLS381_qmul (FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP_BLS381 ∗a)

  Multiplication of an FP4 by an FP.
- void FP4_BLS381_imul (FP4_BLS381 ∗x, FP4_BLS381 ∗y, int i)

  Multiplication of an FP4 by a small integer.
- void FP4_BLS381_sqr (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Squaring an FP4.
- void FP4_BLS381_mul (FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP4_BLS381 ∗z)

  Multiplication of two FP4s.
- void FP4_BLS381_inv (FP4_BLS381 ∗x, FP4_BLS381 ∗y)

  Inverting an FP4.
- void FP4_BLS381_output (FP4_BLS381 ∗x)

  Formats and outputs an FP4 to the console.
- void FP4_BLS381_rawoutput (FP4_BLS381 ∗x)

  Formats and outputs an FP4 to the console in raw form (for debugging)
- void FP4_BLS381_times_i (FP4_BLS381 ∗x)

  multiplies an FP4 instance by irreducible polynomial sqrt(1+sqrt(-1))
- void FP4_BLS381_norm (FP4_BLS381 ∗x)

  Normalises the components of an FP4.
- void FP4_BLS381_reduce (FP4_BLS381 ∗x)

  Reduces all components of possibly unreduced FP4 mod Modulus.
- void FP4_BLS381_pow (FP4_BLS381 ∗x, FP4_BLS381 ∗y, BIG_384_58 b)

  Raises an FP4 to the power of a BIG.
- void FP4_BLS381_frob (FP4_BLS381 ∗x, FP2_BLS381 ∗f)

  Raises an FP4 to the power of the internal modulus p, using the Frobenius.
- void FP4_BLS381_xtr_A (FP4_BLS381 ∗r, FP4_BLS381 ∗w, FP4_BLS381 ∗x, FP4_BLS381 ∗y, FP4_BL←S381 ∗z)

  Calculates the XTR addition function r=w∗x-conj(x)∗y+z.
- void FP4_BLS381_xtr_D (FP4_BLS381 ∗r, FP4_BLS381 ∗x)

*Calculates the XTR doubling function r=x^2-2*conj(x)*
- void FP4_BLS381_xtr_pow (FP4_BLS381 *r, FP4_BLS381 *x, BIG_384_58 b)

 Calculates FP4 trace of an FP12 raised to the power of a BIG number.
- void FP4_BLS381_xtr_pow2 (FP4_BLS381 *r, FP4_BLS381 *c, FP4_BLS381 *d, FP4_BLS381 *e, FP4_↵ BLS381 *f, BIG_384_58 a, BIG_384_58 b)

 Calculates FP4 trace of c^a.d^b, where c and d are derived from FP4 traces of FP12s.
- void FP4_BLS381_cmove (FP4_BLS381 *x, FP4_BLS381 *y, int s)

 Conditional copy of FP4 number.
- int FP4_BLS381_sqrt (FP4_BLS381 *r, FP4_BLS381 *x)

 Calculate square root of an FP4.
- void FP4_BLS381_div_i (FP4_BLS381 *x)

 Divide FP4 number by QNR.
- void FP4_BLS381_div_2i (FP4_BLS381 *x)

 Divide an FP4 by QNR/2.
- void FP4_BLS381_div2 (FP4_BLS381 *x, FP4_BLS381 *y)

 Divide an FP4 by 2.

8.19.1 Detailed Description

Author

Mike Scott

8.19.2 Function Documentation

8.19.2.1 FP4_BLS381_add()

```
void FP4_BLS381_add (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP4_BLS381 * z )
```

Parameters

x	FP4 instance, on exit = y+z
y	FP4 instance
z	FP4 instance

8.19.2.2 FP4_BLS381_cmove()

```
void FP4_BLS381_cmove (
            FP4_BLS381 * x,
```

```
FP4_BLS381 * y,
int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	FP4 instance, set to y if s!=0
y	another FP4 instance
s	copy only takes place if not equal to 0

8.19.2.3 FP4_BLS381_conj()

```
void FP4_BLS381_conj (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

If y=(a,b) on exit x=(a,-b)

Parameters

x	FP4 instance, on exit = conj(y)
y	FP4 instance

8.19.2.4 FP4_BLS381_copy()

```
void FP4_BLS381_copy (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance, on exit = y
y	FP4 instance to be copied

8.19.2.5 FP4_BLS381_div2()

```
void FP4_BLS381_div2 (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance, on exit = y/2
y	FP4 instance

8.19.2.6 FP4_BLS381_div_2i()

```
void FP4_BLS381_div_2i (
            FP4_BLS381 * x )
```

Divide FP4 by the QNR/2

Parameters

x	FP4 instance

8.19.2.7 FP4_BLS381_div_i()

```
void FP4_BLS381_div_i (
            FP4_BLS381 * x )
```

Divide FP4 by the QNR

Parameters

x	FP4 instance

8.19.2.8 FP4_BLS381_equals()

```
int FP4_BLS381_equals (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance to be compared
y	FP4 instance to be compared

Returns

1 if x=y, else returns 0

8.19.2.9 FP4_BLS381_frob()

```
void FP4_BLS381_frob (
            FP4_BLS381 * x,
            FP2_BLS381 * f )
```

Parameters

x	FP4 instance, on exit = x^p
f	FP2 precalculated Frobenius constant

8.19.2.10 FP4_BLS381_from_FP2()

```
void FP4_BLS381_from_FP2 (
            FP4_BLS381 * x,
            FP2_BLS381 * a )
```

Imaginary part is set to zero

Parameters

x	FP4 instance to be initialised
a	FP2 to form real part of FP4

8.19.2.11 FP4_BLS381_from_FP2H()

```
void FP4_BLS381_from_FP2H (
            FP4_BLS381 * x,
            FP2_BLS381 * a )
```

real part is set to zero

Parameters

x	FP4 instance to be initialised
a	FP2 to form imaginary part of FP4

8.19.2.12 FP4_BLS381_from_FP2s()

```
void FP4_BLS381_from_FP2s (
            FP4_BLS381 * x,
```

FP2_BLS381 * *a*,
FP2_BLS381 * *b*)

Parameters

x	FP4 instance to be initialised
a	FP2 to form real part of FP4
b	FP2 to form imaginary part of FP4

8.19.2.13 FP4_BLS381_imul()

```
void FP4_BLS381_imul (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            int i )
```

Parameters

x	FP4 instance, on exit = y*i
y	FP4 instance
i	an integer

8.19.2.14 FP4_BLS381_inv()

```
void FP4_BLS381_inv (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance, on exit = 1/y
y	FP4 instance

8.19.2.15 FP4_BLS381_isreal()

```
int FP4_BLS381_isreal (
            FP4_BLS381 * x )
```

Parameters

x	FP4 number to be tested

Returns

1 if real, else returns 0

8.19.2.16 FP4_BLS381_isunity()

```
int FP4_BLS381_isunity (
            FP4_BLS381 * x )
```

Parameters

x	FP4 number to be tested

Returns

1 if unity, else returns 0

8.19.2.17 FP4_BLS381_iszilch()

```
int FP4_BLS381_iszilch (
            FP4_BLS381 * x )
```

Parameters

x	FP4 number to be tested

Returns

1 if zero, else returns 0

8.19.2.18 FP4_BLS381_mul()

```
void FP4_BLS381_mul (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP4_BLS381 * z )
```

Parameters

x	FP4 instance, on exit = y*z
y	FP4 instance
z	FP4 instance

8.19.2.19 FP4_BLS381_nconj()

```
void FP4_BLS381_nconj (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

If y=(a,b) on exit x=(-a,b)

Parameters

x	FP4 instance, on exit = -conj(y)
y	FP4 instance

8.19.2.20 FP4_BLS381_neg()

```
void FP4_BLS381_neg (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance, on exit = -y
y	FP4 instance

8.19.2.21 FP4_BLS381_norm()

```
void FP4_BLS381_norm (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance to be normalised

8.19.2.22 FP4_BLS381_one()

```
void FP4_BLS381_one (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance to be set to one

8.19.2.23 FP4_BLS381_output()

```
void FP4_BLS381_output (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance to be printed

8.19.2.24 FP4_BLS381_pmul()

```
void FP4_BLS381_pmul (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP2_BLS381 * a )
```

Parameters

x	FP4 instance, on exit = y∗a
y	FP4 instance
a	FP2 multiplier

8.19.2.25 FP4_BLS381_pow()

```
void FP4_BLS381_pow (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            BIG_384_58 b )
```

Parameters

x	FP4 instance, on exit = y^b
y	FP4 instance
b	BIG number

8.19.2.26 FP4_BLS381_qmul()

```
void FP4_BLS381_qmul (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP_BLS381 * a )
```

Parameters

x	FP4 instance, on exit = y∗a
y	FP4 instance
a	FP multiplier

8.19.2.27 FP4_BLS381_rawoutput()

```
void FP4_BLS381_rawoutput (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance to be printed

8.19.2.28 FP4_BLS381_reduce()

```
void FP4_BLS381_reduce (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance, on exit reduced mod Modulus

8.19.2.29 FP4_BLS381_sqr()

```
void FP4_BLS381_sqr (
            FP4_BLS381 * x,
            FP4_BLS381 * y )
```

Parameters

x	FP4 instance, on exit = y^2
y	FP4 instance

8.19.2.30 FP4_BLS381_sqrt()

```
int FP4_BLS381_sqrt (
            FP4_BLS381 * r,
            FP4_BLS381 * x )
```

Square root

Parameters

r	FP4 instance, on exit = sqrt(x)
x	FP4 instance

Returns

1 x is a QR, otherwise 0

8.19.2.31 FP4_BLS381_sub()

```
void FP4_BLS381_sub (
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP4_BLS381 * z )
```

Parameters

x	FP4 instance, on exit = y-z
y	FP4 instance
z	FP4 instance

8.19.2.32 FP4_BLS381_times_i()

```
void FP4_BLS381_times_i (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance, on exit = sqrt(1+sqrt(-1)*x

8.19.2.33 FP4_BLS381_xtr_A()

```
void FP4_BLS381_xtr_A (
            FP4_BLS381 * r,
            FP4_BLS381 * w,
            FP4_BLS381 * x,
            FP4_BLS381 * y,
            FP4_BLS381 * z )
```

Parameters

r	FP4 instance, on exit = w∗x-conj(x)∗y+z
w	FP4 instance
x	FP4 instance
y	FP4 instance
z	FP4 instance

8.19.2.34 FP4_BLS381_xtr_D()

```
void FP4_BLS381_xtr_D (
            FP4_BLS381 * r,
            FP4_BLS381 * x )
```

Parameters

r	FP4 instance, on exit = x^2-2∗conj(x)
x	FP4 instance

8.19.2.35 FP4_BLS381_xtr_pow()

```
void FP4_BLS381_xtr_pow (
            FP4_BLS381 * r,
            FP4_BLS381 * x,
            BIG_384_58 b )
```

XTR single exponentiation

Parameters

r	FP4 instance, on exit = trace(w^b)
x	FP4 instance, trace of an FP12 w
b	BIG number

8.19.2.36 FP4_BLS381_xtr_pow2()

```
void FP4_BLS381_xtr_pow2 (
            FP4_BLS381 * r,
            FP4_BLS381 * c,
            FP4_BLS381 * d,
            FP4_BLS381 * e,
            FP4_BLS381 * f,
            BIG_384_58 a,
            BIG_384_58 b )
```

XTR double exponentiation Assumes c=tr(x^m), d=tr(x^n), e=tr(x^(m-n)), f=tr(x^(m-2n))

Parameters

r	FP4 instance, on exit = trace(c^a.d^b)
c	FP4 instance, trace of an FP12
d	FP4 instance, trace of an FP12
e	FP4 instance, trace of an FP12
f	FP4 instance, trace of an FP12
a	BIG number
b	BIG number

8.19.2.37 FP4_BLS381_zero()

```
void FP4_BLS381_zero (
            FP4_BLS381 * x )
```

Parameters

x	FP4 instance to be set to zero

8.20 fp_BLS381.h File Reference

FP Header File.

```
#include "big_384_58.h"
#include "config_field_BLS381.h"
```

Data Structures

- struct FP_BLS381

  FP Structure - quadratic extension field.

Macros

- #define MODBITS_BLS381 MBITS_BLS381
- #define TBITS_BLS381 (MBITS_BLS381%BASEBITS_384_58)
- #define TMASK_BLS381 (((chunk)1<<TBITS_BLS381)-1)
- #define FEXCESS_BLS381 (((sign32)1<<MAXXES_BLS381)-1)
- #define OMASK_BLS381 (-((chunk)(1)<<TBITS_BLS381))

Functions

- int FP_BLS381_iszilch (FP_BLS381 ∗x)

  Tests for FP equal to zero mod Modulus.
- void FP_BLS381_zero (FP_BLS381 ∗x)

  Set FP to zero.
- void FP_BLS381_copy (FP_BLS381 ∗y, FP_BLS381 ∗x)

  Copy an FP.
- void FP_BLS381_rcopy (FP_BLS381 ∗y, const BIG_384_58 x)

  Copy from ROM to an FP.
- int FP_BLS381_equals (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Compares two FPs.
- void FP_BLS381_cswap (FP_BLS381 ∗x, FP_BLS381 ∗y, int s)

  Conditional constant time swap of two FP numbers.
- void FP_BLS381_cmove (FP_BLS381 ∗x, FP_BLS381 ∗y, int s)

  Conditional copy of FP number.
- void FP_BLS381_nres (FP_BLS381 ∗y, BIG_384_58 x)

  Converts from BIG integer to residue form mod Modulus.
- void FP_BLS381_redc (BIG_384_58 x, FP_BLS381 ∗y)

  Converts from residue form back to BIG integer form.
- void FP_BLS381_one (FP_BLS381 ∗x)

  Sets FP to representation of unity in residue form.
- void FP_BLS381_mod (BIG_384_58 r, DBIG_384_58 d)

  Reduces DBIG to BIG exploiting special form of the modulus.
- void FP_BLS381_mul (FP_BLS381 ∗x, FP_BLS381 ∗y, FP_BLS381 ∗z)

  Fast Modular multiplication of two FPs, mod Modulus.
- void FP_BLS381_imul (FP_BLS381 ∗x, FP_BLS381 ∗y, int i)

  Fast Modular multiplication of an FP, by a small integer, mod Modulus.
- void FP_BLS381_sqr (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Fast Modular squaring of an FP, mod Modulus.
- void FP_BLS381_add (FP_BLS381 ∗x, FP_BLS381 ∗y, FP_BLS381 ∗z)

  Modular addition of two FPs, mod Modulus.
- void FP_BLS381_sub (FP_BLS381 ∗x, FP_BLS381 ∗y, FP_BLS381 ∗z)

  Modular subtraction of two FPs, mod Modulus.
- void FP_BLS381_div2 (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Modular division by 2 of an FP, mod Modulus.
- void FP_BLS381_pow (FP_BLS381 ∗x, FP_BLS381 ∗y, BIG_384_58 z)

  Fast Modular exponentiation of an FP, to the power of a BIG, mod Modulus.
- void FP_BLS381_sqrt (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Fast Modular square root of a an FP, mod Modulus.
- void FP_BLS381_neg (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Modular negation of a an FP, mod Modulus.
- void FP_BLS381_output (FP_BLS381 ∗x)

Outputs an FP number to the console.
- void FP_BLS381_rawoutput (FP_BLS381 ∗x)

  Outputs an FP number to the console, in raw form.
- void FP_BLS381_reduce (FP_BLS381 ∗x)

  Reduces possibly unreduced FP mod Modulus.
- void FP_BLS381_norm (FP_BLS381 ∗x)

  normalizes FP
- int FP_BLS381_qr (FP_BLS381 ∗x)

  Tests for FP a quadratic residue mod Modulus.
- void FP_BLS381_inv (FP_BLS381 ∗x, FP_BLS381 ∗y)

  Modular inverse of a an FP, mod Modulus.

Variables

- const BIG_384_58 Modulus_BLS381
- const BIG_384_58 R2modp_BLS381
- const chunk MConst_BLS381

8.20.1 Detailed Description

Author

Mike Scott

8.20.2 Macro Definition Documentation

8.20.2.1 FEXCESS_BLS381

```
#define FEXCESS_BLS381 (((sign32)1<<MAXXES_BLS381)-1)
```

2^(BASEBITS∗NLEN-MODBITS)-1 - normalised BIG can be multiplied by less than this before reduction

8.20.2.2 MODBITS_BLS381

```
#define MODBITS_BLS381 MBITS_BLS381
```

Number of bits in Modulus for selected curve

8.20.2.3 OMASK_BLS381

```
#define OMASK_BLS381 (-((chunk)(1)<<TBITS_BLS381))
```

for masking out overflow bits

8.20.2.4 TBITS_BLS381

```
#define TBITS_BLS381 (MBITS_BLS381%BASEBITS_384_58)
```

Number of active bits in top word

8.20.2.5 TMASK_BLS381

```
#define TMASK_BLS381 (((chunk)1<<TBITS_BLS381)-1)
```

Mask for active bits in top word

8.20.3 Function Documentation

8.20.3.1 FP_BLS381_add()

```
void FP_BLS381_add (
            FP_BLS381 * x,
            FP_BLS381 * y,
            FP_BLS381 * z )
```

Parameters

x	FP number, on exit the modular sum = y+z mod Modulus
y	FP number
z	FP number

8.20.3.2 FP_BLS381_cmove()

```
void FP_BLS381_cmove (
            FP_BLS381 * x,
            FP_BLS381 * y,
            int s )
```

Conditionally copies second parameter to the first (without branching)

Parameters

x	an FP number
y	another FP number
s	copy takes place if not equal to 0

8.20.3.3 FP_BLS381_copy()

```
void FP_BLS381_copy (
            FP_BLS381 * y,
            FP_BLS381 * x )
```

Parameters

y	FP number to be copied to
x	FP to be copied from

8.20.3.4 FP_BLS381_cswap()

```
void FP_BLS381_cswap (
            FP_BLS381 * x,
            FP_BLS381 * y,
            int s )
```

Conditionally swaps parameters in constant time (without branching)

Parameters

x	an FP number
y	another FP number
s	swap takes place if not equal to 0

8.20.3.5 FP_BLS381_div2()

```
void FP_BLS381_div2 (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Parameters

x	FP number, on exit =y/2 mod Modulus
y	FP number

8.20.3.6 FP_BLS381_equals()

```
int FP_BLS381_equals (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Parameters

x	FP number
y	FP number

Returns

1 if equal, else returns 0

8.20.3.7 FP_BLS381_imul()

```
void FP_BLS381_imul (
            FP_BLS381 * x,
            FP_BLS381 * y,
            int i )
```

Parameters

x	FP number, on exit the modular product = y∗i mod Modulus
y	FP number, the multiplicand
i	a small number, the multiplier

8.20.3.8 FP_BLS381_inv()

```
void FP_BLS381_inv (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Parameters

x	FP number, on exit = 1/y mod Modulus
y	FP number

8.20.3.9 FP_BLS381_iszilch()

```
int FP_BLS381_iszilch (
            FP_BLS381 * x )
```

Parameters

x	BIG number to be tested

Returns

1 if zero, else returns 0

8.20.3.10 FP_BLS381_mod()

```
void FP_BLS381_mod (
            BIG_384_58 r,
            DBIG_384_58 d )
```

This function comes in different flavours depending on the form of Modulus that is currently in use.

Parameters

r	BIG number, on exit = d mod Modulus
d	DBIG number to be reduced

8.20.3.11 FP_BLS381_mul()

```
void FP_BLS381_mul (
            FP_BLS381 * x,
            FP_BLS381 * y,
            FP_BLS381 * z )
```

Uses appropriate fast modular reduction method

Parameters

x	FP number, on exit the modular product = y∗z mod Modulus
y	FP number, the multiplicand
z	FP number, the multiplier

8.20.3.12 FP_BLS381_neg()

```
void FP_BLS381_neg (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Parameters

x	FP number, on exit = -y mod Modulus
y	FP number

8.20.3.13 FP_BLS381_norm()

```
void FP_BLS381_norm (
            FP_BLS381 * x )
```

Parameters

x	FP number, on exit normalized

8.20.3.14 FP_BLS381_nres()

```
void FP_BLS381_nres (
            FP_BLS381 * y,
            BIG_384_58 x )
```

Parameters

x	BIG number to be converted
y	FP result

8.20.3.15 FP_BLS381_one()

```
void FP_BLS381_one (
            FP_BLS381 * x )
```

Parameters

x	FP number to be set equal to unity.

8.20.3.16 FP_BLS381_output()

```
void FP_BLS381_output (
            FP_BLS381 * x )
```

Converts from residue form before output

Parameters

x	an FP number

8.20.3.17 FP_BLS381_pow()

```
void FP_BLS381_pow (
            FP_BLS381 * x,
            FP_BLS381 * y,
            BIG_384_58 z )
```

Parameters

x	FP number, on exit = y^z mod Modulus
y	FP number
z	BIG number exponent

8.20.3.18 FP_BLS381_qr()

```
int FP_BLS381_qr (
            FP_BLS381 * x )
```

Parameters

x	FP number to be tested

Returns

1 if quadratic residue, else returns 0 if quadratic non-residue

8.20.3.19 FP_BLS381_rawoutput()

```
void FP_BLS381_rawoutput (
            FP_BLS381 * x )
```

Parameters

x	a BIG number

8.20.3.20 FP_BLS381_rcopy()

```
void FP_BLS381_rcopy (
```

```
            FP_BLS381 * y,
            const BIG_384_58 x )
```

Parameters

y	FP number to be copied to
x	BIG to be copied from ROM

8.20.3.21 FP_BLS381_redc()

```
void FP_BLS381_redc (
            BIG_384_58 x,
            FP_BLS381 * y )
```

Parameters

y	FP number to be converted to BIG
x	BIG result

8.20.3.22 FP_BLS381_reduce()

```
void FP_BLS381_reduce (
            FP_BLS381 * x )
```

Parameters

x	FP number, on exit reduced mod Modulus

8.20.3.23 FP_BLS381_sqr()

```
void FP_BLS381_sqr (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Uses appropriate fast modular reduction method

Parameters

x	FP number, on exit the modular product = y^2 mod Modulus
y	FP number, the number to be squared

8.20.3.24 FP_BLS381_sqrt()

```
void FP_BLS381_sqrt (
            FP_BLS381 * x,
            FP_BLS381 * y )
```

Parameters

x	FP number, on exit = sqrt(y) mod Modulus
y	FP number, the number whose square root is calculated

8.20.3.25 FP_BLS381_sub()

```
void FP_BLS381_sub (
            FP_BLS381 * x,
            FP_BLS381 * y,
            FP_BLS381 * z )
```

Parameters

x	FP number, on exit the modular difference = y-z mod Modulus
y	FP number
z	FP number

8.20.3.26 FP_BLS381_zero()

```
void FP_BLS381_zero (
            FP_BLS381 * x )
```

Parameters

x	FP number to be set to 0

8.20.4 Variable Documentation

8.20.4.1 MConst_BLS381

```
const chunk MConst_BLS381
```

Constant associated with Modulus - for Montgomery = 1/p mod 2^BASEBITS

8.20.4.2 Modulus_BLS381

```
const BIG_384_58 Modulus_BLS381
```

Actual Modulus set in romf_yyy.c

8.20.4.3 R2modp_BLS381

```
const BIG_384_58 R2modp_BLS381
```

Montgomery constant

8.21 mpin_BLS381.h File Reference

M-Pin Header file.

```
#include "pair_BLS381.h"
#include "pbc_support.h"
```

Macros

- #define PGS_BLS381 MODBYTES_384_58
- #define PFS_BLS381 MODBYTES_384_58
- #define MPIN_OK 0
- #define MPIN_INVALID_POINT -14
- #define MPIN_BAD_PIN -19
- #define MPIN_PAS 16
- #define MAXPIN 10000
- #define PBLEN 14
- #define MESSAGE_SIZE 256
- #define M_SIZE_BLS381 (MESSAGE_SIZE+2∗PFS_BLS381+1)

Functions

- void MPIN_BLS381_GET_Y (int h, int t, octet ∗O, octet ∗Y)

  Generate Y=H(s,O), where s is epoch time, O is an octet, and H(.) is a hash function.
- int MPIN_BLS381_EXTRACT_FACTOR (int h, octet ∗ID, int factor, int facbits, octet ∗CS)

  Extract a PIN number from a client secret.
- int MPIN_BLS381_RESTORE_FACTOR (int h, octet ∗ID, int factor, int facbits, octet ∗CS)

  Extract a PIN number from a client secret.
- int MPIN_BLS381_EXTRACT_PIN (int h, octet ∗ID, int pin, octet ∗CS)

  Extract a PIN number from a client secret.
- int MPIN_BLS381_CLIENT (int h, int d, octet ∗ID, csprng ∗R, octet ∗x, int pin, octet ∗T, octet ∗V, octet ∗U, octet ∗UT, octet ∗TP, octet ∗MESSAGE, int t, octet ∗y)

  Perform client side of the one-pass version of the M-Pin protocol.
- int MPIN_BLS381_CLIENT_1 (int h, int d, octet ∗ID, csprng ∗R, octet ∗x, int pin, octet ∗T, octet ∗S, octet ∗U, octet ∗UT, octet ∗TP)

Perform first pass of the client side of the 3-pass version of the M-Pin protocol.

- int MPIN_BLS381_RANDOM_GENERATE (csprng ∗R, octet ∗S)

  Generate a random group element.
- int MPIN_BLS381_CLIENT_2 (octet ∗x, octet ∗y, octet ∗V)

  Perform second pass of the client side of the 3-pass version of the M-Pin protocol.
- int MPIN_BLS381_SERVER (int h, int d, octet ∗HID, octet ∗HTID, octet ∗y, octet ∗SS, octet ∗U, octet ∗UT, octet ∗V, octet ∗E, octet ∗F, octet ∗ID, octet ∗MESSAGE, int t, octet ∗Pa)

  Perform server side of the one-pass version of the M-Pin protocol.
- void MPIN_BLS381_SERVER_1 (int h, int d, octet ∗ID, octet ∗HID, octet ∗HTID)

  Perform first pass of the server side of the 3-pass version of the M-Pin protocol.
- int MPIN_BLS381_SERVER_2 (int d, octet ∗HID, octet ∗HTID, octet ∗y, octet ∗SS, octet ∗U, octet ∗UT, octet ∗V, octet ∗E, octet ∗F, octet ∗Pa)

  Perform third pass on the server side of the 3-pass version of the M-Pin protocol.
- int MPIN_BLS381_RECOMBINE_G1 (octet ∗Q1, octet ∗Q2, octet ∗Q)

  Add two members from the group G1.
- int MPIN_BLS381_RECOMBINE_G2 (octet ∗P1, octet ∗P2, octet ∗P)

  Add two members from the group G2.
- int MPIN_BLS381_KANGAROO (octet ∗E, octet ∗F)

  Use Kangaroos to find PIN error.
- int MPIN_BLS381_ENCODING (csprng ∗R, octet ∗TP)

  Encoding of a Time Permit to make it indistinguishable from a random string.
- int MPIN_BLS381_DECODING (octet ∗TP)

  Encoding of an obfuscated Time Permit.
- int MPIN_BLS381_GET_G1_MULTIPLE (csprng ∗R, int type, octet ∗x, octet ∗G, octet ∗W)

  Find a random multiple of a point in G1.
- int MPIN_BLS381_GET_G2_MULTIPLE (csprng ∗R, int type, octet ∗x, octet ∗G, octet ∗W)

  Find a random multiple of a point in G1.
- int MPIN_BLS381_GET_CLIENT_SECRET (octet ∗S, octet ∗ID, octet ∗CS)

  Create a client secret in G1 from a master secret and the client ID.
- int MPIN_BLS381_GET_CLIENT_PERMIT (int h, int d, octet ∗S, octet ∗ID, octet ∗TP)

  Create a Time Permit in G1 from a master secret and the client ID.
- int MPIN_BLS381_GET_SERVER_SECRET (octet ∗S, octet ∗SS)

  Create a server secret in G2 from a master secret.
- int MPIN_BLS381_PRECOMPUTE (octet ∗T, octet ∗ID, octet ∗CP, octet ∗g1, octet ∗g2)

  Precompute values for use by the client side of M-Pin Full.
- int MPIN_BLS381_SERVER_KEY (int h, octet ∗Z, octet ∗SS, octet ∗w, octet ∗p, octet ∗I, octet ∗U, octet ∗UT, octet ∗K)

  Calculate Key on Server side for M-Pin Full.
- int MPIN_BLS381_CLIENT_KEY (int h, octet ∗g1, octet ∗g2, int pin, octet ∗r, octet ∗x, octet ∗p, octet ∗T, octet ∗K)

  Calculate Key on Client side for M-Pin Full.
- int MPIN_BLS381_GET_DVS_KEYPAIR (csprng ∗R, octet ∗Z, octet ∗Pa)

  Generates a random public key for the client z.Q.

8.21.1 Detailed Description

Author

Mike Scott

8.21.2 Macro Definition Documentation

8.21.2.1 M_SIZE_BLS381

```
#define M_SIZE_BLS381 (MESSAGE_SIZE+2*PFS_BLS381+1)
```

Signature message size and G1 size

8.21.2.2 MAXPIN

```
#define MAXPIN 10000
```

max PIN

8.21.2.3 MESSAGE_SIZE

```
#define MESSAGE_SIZE 256
```

Signature message size

8.21.2.4 MPIN_BAD_PIN

```
#define MPIN_BAD_PIN -19
```

Bad PIN number entered

8.21.2.5 MPIN_INVALID_POINT

```
#define MPIN_INVALID_POINT -14
```

Point is NOT on the curve

8.21.2.6 MPIN_OK

```
#define MPIN_OK 0
```

Function completed without error

8.21.2.7 MPIN_PAS

```
#define MPIN_PAS 16
```

MPIN Symmetric Key Size

8.21.2.8 PBLEN

```
#define PBLEN 14
```

max length of PIN in bits

8.21.2.9 PFS_BLS381

```
#define PFS_BLS381 MODBYTES_384_58
```

MPIN Field Size

8.21.2.10 PGS_BLS381

```
#define PGS_BLS381 MODBYTES_384_58
```

MPIN Group Size

8.21.3 Function Documentation

8.21.3.1 MPIN_BLS381_CLIENT()

```
int MPIN_BLS381_CLIENT (
            int h,
            int d,
            octet * ID,
            csprng * R,
            octet * x,
            int pin,
            octet * T,
            octet * V,
            octet * U,
            octet * UT,
            octet * TP,
            octet * MESSAGE,
            int t,
            octet * y )
```

If Time Permits are disabled, set d = 0, and UT is not generated and can be set to NULL. If Time Permits are enabled, and PIN error detection is OFF, U is not generated and can be set to NULL. If Time Permits are enabled, and PIN error detection is ON, U and UT are both generated.

Parameters

h	is the hash type
d	is input date, in days since the epoch. Set to 0 if Time permits disabled
ID	is the input client identity
R	is a pointer to a cryptographically secure random number generator

Parameters

x	an output internally randomly generated if R!=NULL, otherwise must be provided as an input
pin	is the input PIN number
T	is the input M-Pin token (the client secret with PIN portion removed)
V	is output = -(x+y)(CS+TP), where CS is the reconstructed client secret, and TP is the time permit
U	is output = x.H(ID)
UT	is output = x.(H(ID)+H(d|H(ID)))
TP	is the input time permit
MESSAGE	is the message to be signed
t	is input epoch time in seconds - a timestamp
y	is output H(t|U) or H(t|UT) if Time Permits enabled

Returns

0 or an error code

8.21.3.2 MPIN_BLS381_CLIENT_1()

```
int MPIN_BLS381_CLIENT_1 (
            int h,
            int d,
            octet * ID,
            csprng * R,
            octet * x,
            int pin,
            octet * T,
            octet * S,
            octet * U,
            octet * UT,
            octet * TP )
```

If Time Permits are disabled, set d = 0, and UT is not generated and can be set to NULL. If Time Permits are enabled, and PIN error detection is OFF, U is not generated and can be set to NULL. If Time Permits are enabled, and PIN error detection is ON, U and UT are both generated.

Parameters

h	is the hash type
d	is input date, in days since the epoch. Set to 0 if Time permits disabled
ID	is the input client identity
R	is a pointer to a cryptographically secure random number generator
x	an output internally randomly generated if R!=NULL, otherwise must be provided as an input
pin	is the input PIN number
T	is the input M-Pin token (the client secret with PIN portion removed)
S	is output = CS+TP, where CS=is the reconstructed client secret, and TP is the time permit
U	is output = x.H(ID)
UT	is output = x.(H(ID)+H(d|H(ID)))
TP	is the input time permit

Returns

0 or an error code

8.21.3.3 MPIN_BLS381_CLIENT_2()

```
int MPIN_BLS381_CLIENT_2 (
            octet * x,
            octet * y,
            octet * V )
```

Parameters

x	an input, a locally generated random number
y	an input random challenge from the server
V	on output = -(x+y).V

Returns

0 or an error code

8.21.3.4 MPIN_BLS381_CLIENT_KEY()

```
int MPIN_BLS381_CLIENT_KEY (
            int h,
            octet * g1,
            octet * g2,
            int pin,
            octet * r,
            octet * x,
            octet * p,
            octet * T,
            octet * K )
```

Parameters

h	is the hash type
g1	precomputed input
g2	precomputed input
pin	is the input PIN number
r	is an input, a locally generated random number
x	is an input, a locally generated random number
p	is an input, hash of the protocol transcript
T	is the input Server-side Diffie-Hellman component
K	is the output calculated shared key

Returns

0 or an error code

8.21.3.5 MPIN_BLS381_DECODING()

```
int MPIN_BLS381_DECODING (
            octet * TP )
```

Parameters

TP	is the input obfuscated time permit, restored on output

Returns

0 or an error code

8.21.3.6 MPIN_BLS381_ENCODING()

```
int MPIN_BLS381_ENCODING (
            csprng * R,
            octet * TP )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
TP	is the input time permit, obfuscated on output

Returns

0 or an error code

8.21.3.7 MPIN_BLS381_EXTRACT_FACTOR()

```
int MPIN_BLS381_EXTRACT_FACTOR (
            int h,
            octet * ID,
            int factor,
            int facbits,
            octet * CS )
```

Parameters

h	is the hash type
ID	is the input client identity
factor	is an input factor
facbits	is the number of bits in the factor
CS	is the client secret from which the factor is to be extracted

Returns

0 or an error code

8.21.3.8 MPIN_BLS381_EXTRACT_PIN()

```
int MPIN_BLS381_EXTRACT_PIN (
            int h,
            octet * ID,
            int pin,
            octet * CS )
```

Parameters

h	is the hash type
ID	is the input client identity
pin	is an input PIN number
CS	is the client secret from which the PIN is to be extracted

Returns

0 or an error code

8.21.3.9 MPIN_BLS381_GET_CLIENT_PERMIT()

```
int MPIN_BLS381_GET_CLIENT_PERMIT (
            int h,
            int d,
            octet * S,
            octet * ID,
            octet * TP )
```

Parameters

h	is the hash type
d	is input date, in days since the epoch.
S	is an input master secret
ID	is the input client identity
TP	is a Time Permit for the given date = s.H(d|H(ID))

Returns

0 or an error code

8.21.3.10 MPIN_BLS381_GET_CLIENT_SECRET()

```
int MPIN_BLS381_GET_CLIENT_SECRET (
            octet * S,
            octet * ID,
            octet * CS )
```

Parameters

S	is an input master secret
ID	is the input client identity
CS	is the full client secret = s.H(ID)

Returns

0 or an error code

8.21.3.11 MPIN_BLS381_GET_DVS_KEYPAIR()

```
int MPIN_BLS381_GET_DVS_KEYPAIR (
            csprng * R,
            octet * Z,
            octet * Pa )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
Z	an output internally randomly generated if R!=NULL, otherwise it must be provided as an input
Pa	the output public key for the client

8.21.3.12 MPIN_BLS381_GET_G1_MULTIPLE()

```
int MPIN_BLS381_GET_G1_MULTIPLE (
            csprng * R,
            int type,
            octet * x,
            octet * G,
            octet * W )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
type	determines type of action to be taken
x	an output internally randomly generated if R!=NULL, otherwise must be provided as an input
G	if type=0 a point in G1, else an octet to be mapped to G1
W	the output =x.G or x.M(G), where M(.) is a mapping

Returns

0 or an error code

8.21.3.13 MPIN_BLS381_GET_G2_MULTIPLE()

```
int MPIN_BLS381_GET_G2_MULTIPLE (
            csprng * R,
            int type,
            octet * x,
            octet * G,
            octet * W )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
type	determines type of action to betaken
x	an output internally randomly generated if R!=NULL, otherwise must be provided as an input
G	a point in G2
W	the output =x.G or (1/x).G

Returns

0 or an error code

8.21.3.14 MPIN_BLS381_GET_SERVER_SECRET()

```
int MPIN_BLS381_GET_SERVER_SECRET (
            octet * S,
            octet * SS )
```

Parameters

S	is an input master secret
SS	is the server secret = s.Q where Q is a fixed generator of G2

Returns

0 or an error code

8.21.3.15 MPIN_BLS381_GET_Y()

```
void MPIN_BLS381_GET_Y (
            int h,
            int t,
            octet * O,
            octet * Y )
```

Parameters

h	is the hash type
t	is epoch time in seconds
O	is an input octet
Y	is the output octet

8.21.3.16 MPIN_BLS381_KANGAROO()

```
int MPIN_BLS381_KANGAROO (
            octet * E,
            octet * F )
```

Parameters

E	a member of the group GT
F	a member of the group GT = E^e

Returns

0 if Kangaroos failed, or the PIN error e

8.21.3.17 MPIN_BLS381_PRECOMPUTE()

```
int MPIN_BLS381_PRECOMPUTE (
            octet * T,
            octet * ID,
            octet * CP,
            octet * g1,
            octet * g2 )
```

Parameters

T	is the input M-Pin token (the client secret with PIN portion removed)
ID	is the input client identity
CP	is Public Key (or NULL)
g1	precomputed output
g2	precomputed output

Returns

0 or an error code

8.21.3.18 MPIN_BLS381_RANDOM_GENERATE()

```
int MPIN_BLS381_RANDOM_GENERATE (
            csprng * R,
            octet * S )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
S	is the output random octet

Returns

0 or an error code

8.21.3.19 MPIN_BLS381_RECOMBINE_G1()

```
int MPIN_BLS381_RECOMBINE_G1 (
            octet * Q1,
            octet * Q2,
            octet * Q )
```

Parameters

Q1	an input member of G1
Q2	an input member of G1
Q	an output member of G1 = Q1+Q2

Returns

0 or an error code

8.21.3.20 MPIN_BLS381_RECOMBINE_G2()

```
int MPIN_BLS381_RECOMBINE_G2 (
            octet * P1,
            octet * P2,
            octet * P )
```

Parameters

P1	an input member of G2
P2	an input member of G2
P	an output member of G2 = P1+P2

Returns

0 or an error code

8.21.3.21 MPIN_BLS381_RESTORE_FACTOR()

```
int MPIN_BLS381_RESTORE_FACTOR (
            int h,
            octet * ID,
            int factor,
            int facbits,
            octet * CS )
```

Parameters

h	is the hash type
ID	is the input client identity
factor	is an input factor
facbits	is the number of bits in the factor
CS	is the client secret to which the factor is to be added

Returns

0 or an error code

8.21.3.22 MPIN_BLS381_SERVER()

```
int MPIN_BLS381_SERVER (
            int h,
            int d,
            octet * HID,
            octet * HTID,
```

```
octet * y,
octet * SS,
octet * U,
octet * UT,
octet * V,
octet * E,
octet * F,
octet * ID,
octet * MESSAGE,
int t,
octet * Pa )
```

If Time Permits are disabled, set d = 0, and UT and HTID are not generated and can be set to NULL. If Time Permits are enabled, and PIN error detection is OFF, U and HID are not needed and can be set to NULL. If Time Permits are enabled, and PIN error detection is ON, U, UT, HID and HTID are all required.

Parameters

h	is the hash type
d	is input date, in days since the epoch. Set to 0 if Time permits disabled
HID	is output H(ID), a hash of the client ID
HTID	is output H(ID)+H(d|H(ID))
y	is output H(t|U) or H(t|UT) if Time Permits enabled
SS	is the input server secret
U	is input from the client = x.H(ID)
UT	is input from the client= x.(H(ID)+H(d|H(ID)))
V	is an input from the client
E	is an output to help the Kangaroos to find the PIN error, or NULL if not required
F	is an output to help the Kangaroos to find the PIN error, or NULL if not required
ID	is the input claimed client identity
MESSAGE	is the message to be signed
t	is input epoch time in seconds - a timestamp
Pa	is input from the client z.Q or NULL if the key-escrow less scheme is not used

Returns

0 or an error code

8.21.3.23 MPIN_BLS381_SERVER_1()

```
void MPIN_BLS381_SERVER_1 (
    int h,
    int d,
    octet * ID,
    octet * HID,
    octet * HTID )
```

Parameters

h	is the hash type
d	is input date, in days since the epoch. Set to 0 if Time permits disabled
ID	is the input claimed client identity
HID	is output H(ID), a hash of the client ID
HTID	is output H(ID)+H(d|H(ID))

Returns

0 or an error code

8.21.3.24 MPIN_BLS381_SERVER_2()

```
int MPIN_BLS381_SERVER_2 (
            int d,
            octet * HID,
            octet * HTID,
            octet * y,
            octet * SS,
            octet * U,
            octet * UT,
            octet * V,
            octet * E,
            octet * F,
            octet * Pa )
```

If Time Permits are disabled, set d = 0, and UT and HTID are not needed and can be set to NULL. If Time Permits are enabled, and PIN error detection is OFF, U and HID are not needed and can be set to NULL. If Time Permits are enabled, and PIN error detection is ON, U, UT, HID and HTID are all required.

Parameters

d	is input date, in days since the epoch. Set to 0 if Time permits disabled
HID	is input H(ID), a hash of the client ID
HTID	is input H(ID)+H(d|H(ID))
y	is the input server's randomly generated challenge
SS	is the input server secret
U	is input from the client = x.H(ID)
UT	is input from the client= x.(H(ID)+H(d|H(ID)))
V	is an input from the client
E	is an output to help the Kangaroos to find the PIN error, or NULL if not required
F	is an output to help the Kangaroos to find the PIN error, or NULL if not required
Pa	is the input public key from the client, z.Q or NULL if the client uses regular mpin

Returns

0 or an error code

8.21.3.25 MPIN_BLS381_SERVER_KEY()

```
int MPIN_BLS381_SERVER_KEY (
            int h,
            octet * Z,
            octet * SS,
            octet * w,
            octet * p,
            octet * I,
            octet * U,
            octet * UT,
            octet * K )
```

Uses UT internally for the key calculation, unless not available in which case U is used

Parameters

h	is the hash type
Z	is the input Client-side Diffie-Hellman component
SS	is the input server secret
w	is an input random number generated by the server
p	is an input, hash of the protocol transcript
I	is the hashed input client ID = H(ID)
U	is input from the client = x.H(ID)
UT	is input from the client= x.(H(ID)+H(d|H(ID)))
K	is the output calculated shared key

Returns

0 or an error code

8.22 paillier.h File Reference

Paillier declarations.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>
#include "ff_4096.h"
#include "ff_2048.h"
```

Data Structures

- struct PAILLIER_public_key

  Paillier Public Key.
- struct PAILLIER_private_key

  Paillier Private Key.

Macros

- #define FS_4096 MODBYTES_512_60*FFLEN_4096
- #define FS_2048 MODBYTES_1024_58*FFLEN_2048
- #define HFS_4096 MODBYTES_512_60*HFLEN_4096
- #define HFS_2048 MODBYTES_1024_58*HFLEN_2048

Functions

- void PAILLIER_KEY_PAIR (csprng *RNG, octet *P, octet *Q, PAILLIER_public_key *PUB, PAILLIER_private_key *PRIV)

  Generate the key pair.
- void PAILLIER_PRIVATE_KEY_KILL (PAILLIER_private_key *PRIV)

  Clear private key.
- void PAILLIER_ENCRYPT (csprng *RNG, PAILLIER_public_key *PUB, octet *PT, octet *CT, octet *R)

  Encrypt a plaintext.
- void PAILLIER_DECRYPT (PAILLIER_private_key *PRIV, octet *CT, octet *PT)

  Decrypt ciphertext.
- void PAILLIER_ADD (PAILLIER_public_key *PUB, octet *CT1, octet *CT2, octet *CT)

  Homomorphic addition of plaintexts.
- void PAILLIER_MULT (PAILLIER_public_key *PUB, octet *CT1, octet *PT, octet *CT)

  Homomorphic multipication of plaintexts.
- void PAILLIER_PK_fromOctet (PAILLIER_public_key *PUB, octet *PK)

  Read a public key from its octet representation.
- void PAILLIER_PK_toOctet (octet *PK, PAILLIER_public_key *PUB)

  Write a public key to an octet.

8.22.1 Macro Definition Documentation

8.22.1.1 FS_2048

```
#define FS_2048 MODBYTES_1024_58*FFLEN_2048
```

2048 field size in bytes

8.22.1.2 FS_4096

```
#define FS_4096 MODBYTES_512_60*FFLEN_4096
```

4096 field size in bytes

8.22.1.3 HFS_2048

```
#define HFS_2048 MODBYTES_1024_58*HFLEN_2048
```

Half 2048 field size in bytes

8.22.1.4 HFS_4096

```
#define HFS_4096 MODBYTES_512_60*HFLEN_4096
```

Half 4096 field size in bytes

8.22.2 Function Documentation

8.22.2.1 PAILLIER_ADD()

```
void PAILLIER_ADD (
            PAILLIER_public_key * PUB,
            octet * CT1,
            octet * CT2,
            octet * CT )
```

$E(m1 + m2) = E(m1) * E(m2)$

1. $ct = ct1 * ct2 \pmod{n^2}$

Parameters

PUB	Public key
CT1	Ciphertext one
CT2	Ciphertext two
CT	Ciphertext

Returns

Returns 0 or else error code

8.22.2.2 PAILLIER_DECRYPT()

```
void PAILLIER_DECRYPT (
            PAILLIER_private_key * PRIV,
```

```
            octet * CT,
            octet * PT )
```

These are the decryption steps modulo n. The computations are carried out modulo p and q and combined using the CRT.

1. $ctl = ct^l \pmod{n^2} - 1$
2. $ctln = ctl/n$
3. $pt = ctln * m \pmod{n}$

Parameters

PRIV	Private key
CT	Ciphertext
PT	Plaintext

8.22.2.3 PAILLIER_ENCRYPT()

```
void PAILLIER_ENCRYPT (
            csprng * RNG,
            PAILLIER_public_key * PUB,
            octet * PT,
            octet * CT,
            octet * R )
```

These are the encryption steps.

1. $m < n$
2. $r < n$
3. $c = g^m.r^n \pmod{n^2}$

Parameters

RNG	Pointer to a cryptographically secure random number generator
PUB	Public key
PT	Plaintext
CT	Ciphertext
R	R value for testing. If RNG is NULL then this value is read.

8.22.2.4 PAILLIER_KEY_PAIR()

```
void PAILLIER_KEY_PAIR (
```

```
csprng * RNG,
octet * P,
octet * Q,
PAILLIER_public_key * PUB,
PAILLIER_private_key * PRIV )
```

Pick large prime numbers of the same size p and q

1. $n = pq$
2. $g = n + 1$
3. $l = (p - 1)(q - 1)$
4. $m = l^{-1} \pmod n$

Parameters

RNG	Pointer to a cryptographically secure random number generator
P	Prime number. If RNG is NULL then this value is read
Q	Prime number. If RNG is NULL then this value is read
PUB	Public key
P↩ RIV	Private key

8.22.2.5 PAILLIER_MULT()

```
void PAILLIER_MULT (
    PAILLIER_public_key * PUB,
    octet * CT1,
    octet * PT,
    octet * CT )
```

$E(m1 * m2) = E(m1)^{m2}$

1. $ct = ct1^{m2} \pmod{n^2}$

Parameters

PUB	Public key
CT1	Ciphertext one
PT	Plaintext constant
CT	Ciphertext

8.22.2.6 PAILLIER_PK_fromOctet()

```
void PAILLIER_PK_fromOctet (
            PAILLIER_public_key * PUB,
            octet * PK )
```

Parameters

PUB	Public key
PK	Octet representation of the public key

8.22.2.7 PAILLIER_PK_toOctet()

```
void PAILLIER_PK_toOctet (
            octet * PK,
            PAILLIER_public_key * PUB )
```

Parameters

PK	Destination octet
PUB	Public key

8.22.2.8 PAILLIER_PRIVATE_KEY_KILL()

```
void PAILLIER_PRIVATE_KEY_KILL (
            PAILLIER_private_key * PRIV )
```

Parameters

P↩ RIV	Private key to clean

8.23 pair_BLS381.h File Reference

PAIR Header File.

```
#include "fp12_BLS381.h"
#include "ecp2_BLS381.h"
#include "ecp_BLS381.h"
```

Functions

- void PAIR_BLS381_another (FP12_BLS381 r[ ], ECP2_BLS381 ∗PV, ECP_BLS381 ∗QV)

    Precompute line functions for n-pairing.
- void PAIR_BLS381_ate (FP12_BLS381 ∗r, ECP2_BLS381 ∗P, ECP_BLS381 ∗Q)

    Calculate Miller loop for Optimal ATE pairing e(P,Q)
- void PAIR_BLS381_double_ate (FP12_BLS381 ∗r, ECP2_BLS381 ∗P, ECP_BLS381 ∗Q, ECP2_BLS381 ∗R, ECP_BLS381 ∗S)

    Calculate Miller loop for Optimal ATE double-pairing e(P,Q).e(R,S)
- void PAIR_BLS381_fexp (FP12_BLS381 ∗x)

    Final exponentiation of pairing, converts output of Miller loop to element in GT.
- void PAIR_BLS381_G1mul (ECP_BLS381 ∗Q, BIG_384_58 b)

    Fast point multiplication of a member of the group G1 by a BIG number.
- void PAIR_BLS381_G2mul (ECP2_BLS381 ∗P, BIG_384_58 b)

    Fast point multiplication of a member of the group G2 by a BIG number.
- void PAIR_BLS381_GTpow (FP12_BLS381 ∗x, BIG_384_58 b)

    Fast raising of a member of GT to a BIG power.
- int PAIR_BLS381_GTmember (FP12_BLS381 ∗x)

    Tests FP12 for membership of GT.
- int PAIR_BLS381_nbits (BIG_384_58 n3, BIG_384_58 n)

    Prepare Ate parameter.
- void PAIR_BLS381_initmp (FP12_BLS381 r[ ])

    Initialise structure for multi-pairing.
- void PAIR_BLS381_miller (FP12_BLS381 ∗res, FP12_BLS381 r[ ])

    Miller loop.

Variables

- const BIG_384_58 CURVE_Bnx_BLS381
- const BIG_384_58 CURVE_Cru_BLS381
- const BIG_384_58 CURVE_W_BLS381 [2]
- const BIG_384_58 CURVE_SB_BLS381 [2][2]
- const BIG_384_58 CURVE_WB_BLS381 [4]
- const BIG_384_58 CURVE_BB_BLS381 [4][4]

8.23.1 Detailed Description

Author

Mike Scott

8.23.2 Function Documentation

8.23.2.1 PAIR_BLS381_another()

```
void PAIR_BLS381_another (
            FP12_BLS381 r[ ],
            ECP2_BLS381 * PV,
            ECP_BLS381 * QV )
```

Parameters

r	array of precomputed FP12 products of line functions
PV	ECP2 instance, an element of G2
QV	ECP instance, an element of G1

8.23.2.2 PAIR_BLS381_ate()

```
void PAIR_BLS381_ate (
            FP12_BLS381 * r,
            ECP2_BLS381 * P,
            ECP_BLS381 * Q )
```

Parameters

r	FP12 result of the pairing calculation e(P,Q)
P	ECP2 instance, an element of G2
Q	ECP instance, an element of G1

8.23.2.3 PAIR_BLS381_double_ate()

```
void PAIR_BLS381_double_ate (
            FP12_BLS381 * r,
            ECP2_BLS381 * P,
            ECP_BLS381 * Q,
            ECP2_BLS381 * R,
            ECP_BLS381 * S )
```

Faster than calculating two separate pairings

Parameters

r	FP12 result of the pairing calculation e(P,Q).e(R,S), an element of GT
P	ECP2 instance, an element of G2
Q	ECP instance, an element of G1
R	ECP2 instance, an element of G2
S	ECP instance, an element of G1

8.23.2.4 PAIR_BLS381_fexp()

```
void PAIR_BLS381_fexp (
            FP12_BLS381 * x )
```

Here p is the internal modulus, and r is the group order

Parameters

x	FP12, on exit = x^((p^12-1)/r)

8.23.2.5 PAIR_BLS381_G1mul()

```
void PAIR_BLS381_G1mul (
            ECP_BLS381 * Q,
            BIG_384_58 b )
```

May exploit endomorphism for speed.

Parameters

Q	ECP member of G1.
b	BIG multiplier

8.23.2.6 PAIR_BLS381_G2mul()

```
void PAIR_BLS381_G2mul (
            ECP2_BLS381 * P,
            BIG_384_58 b )
```

May exploit endomorphism for speed.

Parameters

P	ECP2 member of G1.
b	BIG multiplier

8.23.2.7 PAIR_BLS381_GTmember()

```
int PAIR_BLS381_GTmember (
            FP12_BLS381 * x )
```

Parameters

x	FP12 instance

Returns

1 if x is in GT, else return 0

8.23.2.8 PAIR_BLS381_GTpow()

```
void PAIR_BLS381_GTpow (
            FP12_BLS381 * x,
            BIG_384_58 b )
```

May exploit endomorphism for speed.

Parameters

x	FP12 member of GT.
b	BIG exponent

8.23.2.9 PAIR_BLS381_initmp()

```
void PAIR_BLS381_initmp (
            FP12_BLS381 r[] )
```

Parameters

r	FP12 array, to be initialised to 1

8.23.2.10 PAIR_BLS381_miller()

```
void PAIR_BLS381_miller (
            FP12_BLS381 * res,
            FP12_BLS381 r[] )
```

Parameters

res	FP12 result
r	FP12 precomputed array of accumulated line functions

8.23.2.11 PAIR_BLS381_nbits()

```
int PAIR_BLS381_nbits (
```

```
            BIG_384_58 n3,
            BIG_384_58 n )
```

Parameters

n	BIG parameter
n3	BIG paramter = 3∗n

Returns

number of nits in n3

8.23.3 Variable Documentation

8.23.3.1 CURVE_BB_BLS381

```
const BIG_384_58 CURVE_BB_BLS381[4][4]
```

BN curve constant for GS decomposition

8.23.3.2 CURVE_Bnx_BLS381

```
const BIG_384_58 CURVE_Bnx_BLS381
```

BN curve x parameter

8.23.3.3 CURVE_Cru_BLS381

```
const BIG_384_58 CURVE_Cru_BLS381
```

BN curve Cube Root of Unity

8.23.3.4 CURVE_SB_BLS381

```
const BIG_384_58 CURVE_SB_BLS381[2][2]
```

BN curve constant for GLV decomposition

8.23.3.5 CURVE_W_BLS381

```
const BIG_384_58 CURVE_W_BLS381[2]
```

BN curve constant for GLV decomposition

8.23.3.6 CURVE_WB_BLS381

```
const BIG_384_58 CURVE_WB_BLS381[4]
```

BN curve constant for GS decomposition

8.24 pbc_support.h File Reference

Auxiliary functions for Pairing-based protocols.

```
#include "amcl.h"
```

Macros

- #define TIME_SLOT_MINUTES 1440

Functions

- void mhashit (int sha, int n, octet ∗x, octet ∗w)

    general purpose hash function w=hash(n|x)
- unsign32 today (void)

    Supply today's date as days from the epoch.
- void HASH_ALL (int h, octet ∗I, octet ∗U, octet ∗CU, octet ∗Y, octet ∗V, octet ∗R, octet ∗W, octet ∗H)

    Hash the session transcript.
- void HASH_ID (int h, octet ∗ID, octet ∗HID)

    Hash an M-Pin Identity to an octet string.
- unsign32 GET_TIME (void)

    Get epoch time as unsigned integer.
- void AES_GCM_ENCRYPT (octet ∗K, octet ∗IV, octet ∗H, octet ∗P, octet ∗C, octet ∗T)

    AES-GCM Encryption.
- void AES_GCM_DECRYPT (octet ∗K, octet ∗IV, octet ∗H, octet ∗C, octet ∗P, octet ∗T)

    AES-GCM Decryption.

8.24.1 Detailed Description

Author

Mike Scott

8.24.2 Macro Definition Documentation

8.24.2.1 TIME_SLOT_MINUTES

```
#define TIME_SLOT_MINUTES 1440
```

Time Slot = 1 day

8.24.3 Function Documentation

8.24.3.1 AES_GCM_DECRYPT()

```
void AES_GCM_DECRYPT (
            octet * K,
            octet * IV,
            octet * H,
            octet * C,
            octet * P,
            octet * T )
```

Parameters

K	AES key
IV	Initialization vector
H	Header
P	Plaintext
C	Ciphertext
T	Checksum

8.24.3.2 AES_GCM_ENCRYPT()

```
void AES_GCM_ENCRYPT (
            octet * K,
            octet * IV,
            octet * H,
            octet * P,
            octet * C,
            octet * T )
```

Parameters

K	AES key
IV	Initialization vector
H	Header
P	Plaintext
C	Ciphertext
T	Checksum

8.24.3.3 GET_TIME()

```
unsign32 GET_TIME (
            void  )
```

Returns

current epoch time in seconds

8.24.3.4 HASH_ALL()

```
void HASH_ALL (
            int h,
            octet * I,
            octet * U,
            octet * CU,
            octet * Y,
            octet * V,
            octet * R,
            octet * W,
            octet * H )
```

Parameters

h	is the hash type
I	is the hashed input client ID = H(ID)
U	is the client output = x.H(ID)
CU	is the client output = x.(H(ID)+H(T|H(ID)))
Y	is the server challenge
V	is the client part response
R	is the client part response
W	is the server part response
H	the output is the hash of all of the above that apply

8.24.3.5 HASH_ID()

```
void HASH_ID (
            int h,
            octet * ID,
            octet * HID )
```

Parameters

h	is the hash type
ID	an octet containing the identity
HID	an octet containing the hashed identity

8.24.3.6 mhashit()

```
void mhashit (
            int sha,
            int n,
            octet * x,
            octet * w )
```

Parameters

sha	is the hash type
n	integer involved in the hash
x	octect involved in the h ash
w	output

8.24.3.7 today()

```
unsign32 today (
            void )
```

Returns

today's date, as number of days elapsed since the epoch

8.25 randapi.h File Reference

PRNG API File.

```
#include "amcl.h"
```

Functions

- void CREATE_CSPRNG (csprng ∗R, octet ∗S)

  Initialise a random number generator.
- void KILL_CSPRNG (csprng ∗R)

  Kill a random number generator.

8.25.1 Detailed Description

Author

Mike Scott

8.25.2 Function Documentation

8.25.2.1 CREATE_CSPRNG()

```
void CREATE_CSPRNG (
            csprng * R,
            octet * S )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
S	is an input truly random seed value

8.25.2.2 KILL_CSPRNG()

```
void KILL_CSPRNG (
            csprng * R )
```

Deletes all internal state

Parameters

R	is a pointer to a cryptographically secure random number generator

8.26 rsa_2048.h File Reference

RSA Header file for implementation of RSA protocol.

```
#include "ff_2048.h"
#include "rsa_support.h"
```

Data Structures

- struct rsa_public_key_2048

  Integer Factorisation Public Key.
- struct rsa_private_key_2048

  Integer Factorisation Private Key.

Macros

- #define HASH_TYPE_RSA_2048 SHA256
- #define RFS_2048 MODBYTES_1024_58*FFLEN_2048

Functions

- void RSA_2048_KEY_PAIR (csprng *R, sign32 e, rsa_private_key_2048 *PRIV, rsa_public_key_2048 *P↩ UB, octet *P, octet *Q)

  RSA Key Pair Generator.
- void RSA_2048_ENCRYPT (rsa_public_key_2048 *PUB, octet *F, octet *G)

  RSA encryption of suitably padded plaintext.
- void RSA_2048_DECRYPT (rsa_private_key_2048 *PRIV, octet *G, octet *F)

  RSA decryption of ciphertext.
- void RSA_2048_PRIVATE_KEY_KILL (rsa_private_key_2048 *PRIV)

  Destroy an RSA private Key.
- void RSA_2048_fromOctet (BIG_1024_58 *x, octet *S)

  Populates an RSA public key from an octet string.

8.26.1 Detailed Description

Author

Mike Scott declares functions

8.26.2 Macro Definition Documentation

8.26.2.1 HASH_TYPE_RSA_2048

```
#define HASH_TYPE_RSA_2048 SHA256
```

Chosen Hash algorithm

8.26.2.2 RFS_2048

```
#define RFS_2048 MODBYTES_1024_58*FFLEN_2048
```

RSA Public Key Size in bytes

8.26.3 Function Documentation

8.26.3.1 RSA_2048_DECRYPT()

```
void RSA_2048_DECRYPT (
            rsa_private_key_2048 * PRIV,
            octet * G,
            octet * F )
```

Parameters

PRIV	the input RSA private key
G	is the input ciphertext
F	is output plaintext (requires unpadding)

8.26.3.2 RSA_2048_ENCRYPT()

```
void RSA_2048_ENCRYPT (
            rsa_public_key_2048 * PUB,
            octet * F,
            octet * G )
```

Parameters

PUB	the input RSA public key
F	is input padded message
G	is the output ciphertext

8.26.3.3 RSA_2048_fromOctet()

```
void RSA_2048_fromOctet (
            BIG_1024_58 * x,
            octet * S )
```

Creates RSA public key from big-endian base 256 form.

Parameters

x	FF instance to be created from an octet string
S	input octet string

8.26.3.4 RSA_2048_KEY_PAIR()

```
void RSA_2048_KEY_PAIR (
            csprng * R,
            sign32 e,
            rsa_private_key_2048 * PRIV,
            rsa_public_key_2048 * PUB,
            octet * P,
            octet * Q )
```

Parameters

R	is a pointer to a cryptographically secure random number generator
e	the encryption exponent
P↔ RIV	the output RSA private key
PUB	the output RSA public key
P	Input prime number. Used when R is equal to NULL for testing
Q	Inpuy prime number. Used when R is equal to NULL for testing

8.26.3.5 RSA_2048_PRIVATE_KEY_KILL()

```
void RSA_2048_PRIVATE_KEY_KILL (
            rsa_private_key_2048 * PRIV )
```

Parameters

P↔ RIV	the input RSA private key. Destroyed on output.

8.27 rsa_support.h File Reference

RSA Support Header File.

```
#include "amcl.h"
```

Macros

- #define MAX_RSA_BYTES 512

Functions

- int PKCS15 (int h, octet ∗M, octet ∗W)

  PKCS V1.5 padding of a message prior to RSA signature.
- int OAEP_ENCODE (int h, octet ∗M, csprng ∗R, octet ∗P, octet ∗F)

  OAEP padding of a message prior to RSA encryption.
- int OAEP_DECODE (int h, octet ∗P, octet ∗F)

  OAEP unpadding of a message after RSA decryption.

8.27.1 Detailed Description

Author

Mike Scott

8.27.2 Macro Definition Documentation

8.27.2.1 MAX_RSA_BYTES

```
#define MAX_RSA_BYTES 512
```

Maximum of 4096

8.27.3 Function Documentation

8.27.3.1 OAEP_DECODE()

```
int OAEP_DECODE (
            int h,
            octet * P,
            octet * F )
```

Unpadding is done in-place

Parameters

h	is the hash type
P	are input encoding parameter string (could be NULL)
F	is input padded message, unpadded on output

Returns

0 if OK, else 1

8.27.3.2 OAEP_ENCODE()

```
int OAEP_ENCODE (
            int h,
            octet * M,
            csprng * R,
            octet * P,
            octet * F )
```

Parameters

h	is the hash type

Parameters

M	is the input message
R	is a pointer to a cryptographically secure random number generator
P	are input encoding parameter string (could be NULL)
F	is the output encoding, ready for RSA encryption

Returns

0 if OK, else 1

8.27.3.3 PKCS15()

```
int PKCS15 (
            int h,
            octet * M,
            octet * W )
```

Parameters

h	is the hash type
M	is the input message
W	is the output encoding, ready for RSA signature

Returns

1 if OK, else 0

8.28 utils.c File Reference

AMCL Support functions for M-Pin servers.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include "amcl.h"
#include "utils.h"
```

Functions

- void amcl_hex2bin (const char *src, char *dst, int src_len)

  Decode hex value.
- void amcl_bin2hex (char *src, char *dst, int src_len)

  Encode binary string.

- void amcl_print_hex (char *src, int src_len)

  Print encoded binary string in hex.
- int generateOTP (csprng *RNG)

  Generate a random six digit one time password.
- void generateRandom (csprng *RNG, octet *randomValue)

  Generate a random Octet.

8.28.1 Detailed Description

Author

Mike Scott
Kealan McCusker

Date

28th July 2016 LICENSE

8.28.2 Function Documentation

8.28.2.1 amcl_bin2hex()

```
void amcl_bin2hex (
             char * src,
             char * dst,
             int src_len )
```

Encode binary string.

Parameters

src	Binary string
dst	Hex encoded string
src_len	length binary string

8.28.2.2 amcl_hex2bin()

```
void amcl_hex2bin (
            const char * src,
            char * dst,
            int src_len )
```

Decode hex value.

Parameters

src	Hex encoded string
dst	Binary string
src_len	length Hex encoded string

8.28.2.3 amcl_print_hex()

```
void amcl_print_hex (
            char * src,
            int src_len )
```

Print encoded binary string in hex.

Parameters

src	Binary string
src_len	length binary string

8.28.2.4 generateOTP()

```
int generateOTP (
            csprng * RNG )
```

Generates a random six digit one time password.

Parameters

RNG	random number generator

Returns

OTP One Time Password

8.28.2.5 generateRandom()

```
void generateRandom (
            csprng * RNG,
            octet * randomValue )
```

Generate a random Octet.

Parameters

RNG	random number generator
randomValue	random Octet

8.29 utils.h File Reference

Utility functions Header File.

```
#include "amcl.h"
```

Functions

- void amcl_hex2bin (const char *src, char *dst, int src_len)
  Decode hex value.
- void amcl_bin2hex (char *src, char *dst, int src_len)
  Encode binary string.
- void amcl_print_hex (char *src, int src_len)
  Print encoded binary string in hex.
- void generateRandom (csprng *RNG, octet *randomValue)
  Generate a random Octet.
- int generateOTP (csprng *RNG)
  Generate a random six digit one time password.

8.29.1 Detailed Description

Author

Kealan McCusker

8.29.2 Function Documentation

8.29.2.1 amcl_bin2hex()

```
void amcl_bin2hex (
            char * src,
            char * dst,
            int src_len )
```

Encode binary string.

Parameters

src	Binary string
dst	Hex encoded string
src_len	length binary string

8.29.2.2 amcl_hex2bin()

```
void amcl_hex2bin (
            const char * src,
            char * dst,
            int src_len )
```

Decode hex value.

Parameters

src	Hex encoded string
dst	Binary string
src_len	length Hex encoded string

8.29.2.3 amcl_print_hex()

```
void amcl_print_hex (
            char * src,
            int src_len )
```

Print encoded binary string in hex.

Parameters

src	Binary string
src_len	length binary string

8.29.2.4 generateOTP()

```
int generateOTP (
            csprng * RNG )
```

Generates a random six digit one time password.

Parameters

RNG	random number generator

Returns

OTP One Time Password

8.29.2.5 generateRandom()

```
void generateRandom (
            csprng * RNG,
            octet * randomValue )
```

Generate a random Octet.

Parameters

RNG	random number generator
randomValue	random Octet

8.30 version.c File Reference

AMCL version support function.

```
#include "version.h"
```

Functions

- void amcl_version (void)

  Print version number and information about the build.

8.30.1 Detailed Description

Author

Mike Scott
Kealan McCusker

Date

28th April 2016 LICENSE

8.30.2 Function Documentation

8.30.2.1 amcl_version()

```
void amcl_version (
            void )
```

Print version number and information about the build.

8.31 wcc_BLS381.h File Reference

WCC Header File.

```
#include "pair_BLS381.h"
#include "pbc_support.h"
```

Macros

- #define WCC_PGS_BLS381 MODBYTES_384_58
- #define WCC_PFS_BLS381 MODBYTES_384_58
- #define WCC_OK 0
- #define WCC_INVALID_POINT -51
- #define TIME_SLOT_MINUTES 1440
- #define PIV 12
- #define PTAG 16

Functions

- int WCC_BLS381_RANDOM_GENERATE (csprng *RNG, octet *S)

  Generate a random integer.
- void WCC_BLS381_Hq (int sha, octet *A, octet *B, octet *C, octet *D, octet *h)

  Hash EC Points and Id to an integer.
- int WCC_BLS381_GET_G2_MULTIPLE (octet *S, octet *HID, octet *VG2)

  Calculate value in G2 multiplied by an integer.
- int WCC_BLS381_GET_G1_MULTIPLE (octet *S, octet *HID, octet *VG1)

  Calculate value in G1 multiplied by an integer.
- int WCC_BLS381_SENDER_KEY (int sha, octet *xOct, octet *piaOct, octet *pibOct, octet *PbG2Oct, octet *PgG1Oct, octet *AKeyG1Oct, octet *IdBOct, octet *AESKeyOct)

  Calculate the sender AES key.
- int WCC_BLS381_RECEIVER_KEY (int sha, octet *yOct, octet *wOct, octet *piaOct, octet *pibOct, octet *PaG1Oct, octet *PgG1Oct, octet *BKeyG2Oct, octet *IdAOct, octet *AESKeyOct)

  Calculate the receiver AES key.
- int WCC_BLS381_RECOMBINE_G1 (octet *R1, octet *R2, octet *R)

  Add two members from the group G1.
- int WCC_BLS381_RECOMBINE_G2 (octet *W1, octet *W2, octet *W)

  Add two members from the group G2.

8.31.1 Detailed Description

Author

Mike Scott
Kealan McCusker

8.31.2 Macro Definition Documentation

8.31.2.1 PIV

```
#define PIV 12
```

AES-GCM Initialization Vector Size

8.31.2.2 PTAG

```
#define PTAG 16
```

AES-GCM MAC Size

8.31.2.3 TIME_SLOT_MINUTES

```
#define TIME_SLOT_MINUTES 1440
```

Time Slot = 1 day

8.31.2.4 WCC_INVALID_POINT

```
#define WCC_INVALID_POINT -51
```

Point is NOT on the curve

8.31.2.5 WCC_OK

```
#define WCC_OK 0
```

Function completed without error

8.31.2.6 WCC_PFS_BLS381

```
#define WCC_PFS_BLS381 MODBYTES_384_58
```

WCC Field Size

8.31.2.7 WCC_PGS_BLS381

```
#define WCC_PGS_BLS381 MODBYTES_384_58
```

WCC Group Size

8.31.3 Function Documentation

8.31.3.1 WCC_BLS381_GET_G1_MULTIPLE()

```
int WCC_BLS381_GET_G1_MULTIPLE (
            octet * S,
            octet * HID,
            octet * VG1 )
```

Calculate a value in G1. VG1 = s*H1(ID) where ID is the identity.

1. VG1 = s*H1(ID)

Parameters

S	integer modulus curve order
HID	Hash of ID padded with zeros to the field size
VG1	EC point VG1 = s*H1(ID)

Returns

rtn Returns 0 if successful or else an error code

8.31.3.2 WCC_BLS381_GET_G2_MULTIPLE()

```
int WCC_BLS381_GET_G2_MULTIPLE (
            octet * S,
            octet * HID,
            octet * VG2 )
```

Calculate a value in G2. VG2 = s∗H2(ID) where ID is the identity.

1. VG2 = s∗H2(ID)

Parameters

S	integer modulus curve order
HID	Hash of ID padded with zeros to the field size
VG2	EC Point VG2 = s∗H2(ID)

Returns

rtn Returns 0 if successful or else an error code

8.31.3.3 WCC_BLS381_Hq()

```
void WCC_BLS381_Hq (
            int sha,
            octet * A,
            octet * B,
            octet * C,
            octet * D,
            octet * h )
```

Perform sha256 of EC Points and Id. Map to an integer modulo the curve order.

1. x = toInteger(sha256(A,B,C,D))
2. h = x % q where q is the curve order

Parameters

sha	Hash type
A	EC Point
B	EC Point
C	EC Point
D	Identity
h	Integer result

8.31.3.4 WCC_BLS381_RANDOM_GENERATE()

```
int WCC_BLS381_RANDOM_GENERATE (
            csprng * RNG,
            octet * S )
```

Generate a random number modulus the group order.

Parameters

RNG	cryptographically secure random number generator
S	Returned random integer modulus the group order

8.31.3.5 WCC_BLS381_RECEIVER_KEY()

```
int WCC_BLS381_RECEIVER_KEY (
            int sha,
            octet * yOct,
            octet * wOct,
            octet * piaOct,
            octet * pibOct,
            octet * PaG1Oct,
            octet * PgG1Oct,
            octet * BKeyG2Oct,
            octet * IdAOct,
            octet * AESKeyOct )
```

Calculate the receiver AES key.

1. j=e(pia.AG1+PaG1,(y+pib).BKeyG2)
2. K=H(j,w.PaG1)

Parameters

sha	Hash type
yOct	Random y $<$ q where q is the curve order
wOct	Random w $<$ q where q is the curve order
piaOct	Hq(PaG1,PbG2,PgG1)
pibOct	Hq(PbG2,PaG1,PgG1)
PaG1Oct	x.AG1 where x $<$ q
PgG1Oct	w.AG1 where w $<$ q
BKeyG2Oct	Receiver key
IdAOct	Sender identity
AESKeyOct	AES key returned

Returns

rtn Returns 0 if successful or else an error code

8.31.3.6 WCC_BLS381_RECOMBINE_G1()

```
int WCC_BLS381_RECOMBINE_G1 (
            octet * R1,
            octet * R2,
            octet * R )
```

Add two members from the group G1.

Parameters

R1	member of G1
R2	member of G1
R	returns member of G1 = R1+R2

Returns

Returns 0 if successful or else an error code

8.31.3.7 WCC_BLS381_RECOMBINE_G2()

```
int WCC_BLS381_RECOMBINE_G2 (
            octet * W1,
            octet * W2,
            octet * W )
```

Add two members from the group G2.

Parameters

W1	member of G2
W2	member of G2
W	returns member of G2 = W1+W2

Returns

Returns 0 if successful or else an error code

8.31.3.8 WCC_BLS381_SENDER_KEY()

```
int WCC_BLS381_SENDER_KEY (
            int sha,
            octet * xOct,
            octet * piaOct,
            octet * pibOct,
            octet * PbG2Oct,
            octet * PgG1Oct,
            octet * AKeyG1Oct,
            octet * IdBOct,
            octet * AESKeyOct )
```

Calculate the sender AES Key.

1. j=e((x+pia).AKeyG1,pib.BG2+PbG2)
2. K=H(j,x.PgG1)

Parameters

sha	Hash type
xOct	Random x < q where q is the curve order
piaOct	Hq(PaG1,PbG2,PgG1)
pibOct	Hq(PbG2,PaG1,PgG1)
PbG2Oct	y.BG2 where y < q
PgG1Oct	w.AG1 where w < q
AKeyG1Oct	Sender key
IdBOct	Receiver identity
AESKeyOct	Returned AES key

Returns

rtn Returns 0 if successful or else an error code

8.32 x509.h File Reference

X509 function Header File.

Data Structures

- struct pktype

    Public key type.

Functions

- pktype X509_extract_cert_sig (octet ∗c, octet ∗s)

  Extract certificate signature.
- int X509_extract_cert (octet ∗sc, octet ∗c)
- pktype X509_extract_public_key (octet ∗c, octet ∗k)
- int X509_find_issuer (octet ∗c)
- int X509_find_validity (octet ∗c)
- int X509_find_subject (octet ∗c)
- int X509_find_entity_property (octet ∗c, octet ∗S, int s, int ∗f)
- int X509_find_start_date (octet ∗c, int s)
- int X509_find_expiry_date (octet ∗c, int s)

8.32.1 Detailed Description

Author

Mike Scott

8.32.2 Function Documentation

8.32.2.1 X509_extract_cert()

```
int X509_extract_cert (
            octet * sc,
            octet * c )
```

Parameters

sc	a signed certificate
c	the extracted certificate

Returns

0 on failure

8.32.2.2 X509_extract_cert_sig()

```
pktype X509_extract_cert_sig (
            octet * c,
            octet * s )
```

Parameters

c	an X.509 certificate
s	the extracted signature

Returns

0 on failure, or indicator of signature type (ECC or RSA)

8.32.2.3 X509_extract_public_key()

```
pktype X509_extract_public_key (
            octet * c,
            octet * k )
```

Parameters

c	an X.509 certificate
k	the extracted key

Returns

0 on failure, or indicator of public key type (ECC or RSA)

8.32.2.4 X509_find_entity_property()

```
int X509_find_entity_property (
            octet * c,
            octet * S,
            int s,
            int * f )
```

Parameters

c	an X.509 certificate
S	is OID of property we are looking for
s	is a pointer to the section of interest in the cert
f	is pointer to the length of the property

Returns

0 on failure, or pointer to the property

8.32.2.5 X509_find_expiry_date()

```
int X509_find_expiry_date (
            octet * c,
            int s )
```

Parameters

c	an X.509 certificate
s	is a pointer to the start of the validity field

Returns

0 on failure, or pointer to the expiry date

8.32.2.6 X509_find_issuer()

```
int X509_find_issuer (
            octet * c )
```

Parameters

c	an X.509 certificate

Returns

0 on failure, or pointer to issuer field in cert

8.32.2.7 X509_find_start_date()

```
int X509_find_start_date (
            octet * c,
            int s )
```

Parameters

c	an X.509 certificate
s	is a pointer to the start of the validity field

Returns

0 on failure, or pointer to the start date

8.32.2.8 X509_find_subject()

```
int X509_find_subject (
            octet * c )
```

Parameters

c	an X.509 certificate

Returns

0 on failure, or pointer to subject field in cert

8.32.2.9 X509_find_validity()

```
int X509_find_validity (
            octet * c )
```

Parameters

c	an X.509 certificate

Returns

0 on failure, or pointer to validity field in cert

Index