PSEC-KEM over GF(2^283)

This directory contains source code for PSEC-KEM over GF(2^283), and the this document describes steps to run it. For further details please refer to the design document.

Platform Requirements

---
1 Hardware : Standard 64 bit desktop/server system. Does not support 32 bit machine.

2 Software : Linux OS, gcc-4.x, gmp library

Compilation

To compile, execute the command

gcc -lgmp -lrt psec-kem.c -o psec-kem

Execution

After executing the program, a choice menue will appear. The required steps are described using screenshots.

```
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
x^283 + x^12 + x^7 + x^5 + x^0
PSEC-KEM options are :
1. 256 bit Private Key Generation
2. Public key W(x,y) generation
3. Encryption operation of PSEC-KEM
4. Decryption operation of PSEC-KEM

Your choice :  1
Private key (256 bit) : 1fe63ffc71a29953 376272bfb1f65b24 3921a33a1a21ac61 316081497e8125ab
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
x^283 + x^12 + x^7 + x^5 + x^0
PSEC-KEM options are :
1. 256 bit Private Key Generation
2. Public key W(x,y) generation
3. Encryption operation of PSEC-KEM
4. Decryption operation of PSEC-KEM

Your choice :  2
Select Curve type :
1. Random Curve
2. Koblitz Curve
1
Enter 256 bit private key : 1fe63ffc71a29953 376272bfb1f65b24 3921a33a1a21ac61 316081497e8125ab

Public key W(x) is : 208466f f5447936a7b52a71 34710fc515d49ffa abacfb88a04f506e 6a80e55ffeb6683f
Public key W(y) is : 41916c7 3c8e248e413f9de6 dc9839c43681cd12 b5f29dbda2e435d5 bfc0a9dc9eb83b5d
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
x^283 + x^12 + x^7 + x^5 + x^0
PSEC-KEM options are :
1. 256 bit Private Key Generation
2. Public key W(x,y) generation
3. Encryption operation of PSEC-KEM
4. Decryption operation of PSEC-KEM

Your choice :  3
```

```
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
x^283 + x^12 + x^7 + x^5 + x^0
PSEC-KEM options are :
1. 256 bit Private Key Generation
2. Public key W(x,y) generation
3. Encryption operation of PSEC-KEM
4. Decryption operation of PSEC-KEM

Your choice :  3
Select Curve type :
1. Random Curve
2. Koblitz Curve
1

 Session key :
b1a170a04ea1d0b7822d94dec80c6272018c3b01fe91a9d11a15ec870ce044cb
Send it to other party:
003b763a
3630e9b77e4bc1d6
b26ee36d1a72850f
2d8e46912935bf4b
30eca5e95cbf8825
045c5b35
9e063cd6271a90ea
bb9c91b96f6f55ba
e823daf11cea26d3
f503ffe14ea0b34a
58257d7aa2550377
f6d35431d0310a94
dafdbc80a93f4494
adb710bee095924d

sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
```

```
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$ ./psec-kem
x^283 + x^12 + x^7 + x^5 + x^0
PSEC-KEM options are :
1. 256 bit Private Key Generation
2. Public key W(x,y) generation
3. Encryption operation of PSEC-KEM
4. Decryption operation of PSEC-KEM

Your choice :  4
Select Curve type :
1. Random Curve
2. Koblitz Curve
1
Enter First received strings : 003b763a
3630e9b77e4bc1d6
b26ee36d1a72850f
2d8e46912935bf4b
30eca5e95cbf8825
045c5b35
9e063cd6271a90ea
bb9c91b96f6f55ba
e823daf11cea26d3
f503ffe14ea0b34a
58257d7aa2550377
f6d35431d0310a94
dafdbc80a93f4494
adb710bee095924d
Enter private key in hex form :1fe63ffc71a29953 376272bfb1f65b24 3921a33a1a21ac61 316081497e8125ab

Session key :
b1a170a04ea1d0b7822d94dec80c6272018c3b01fe91a9d11a15ec870ce044cb
Verification returns 0
sujoy@iit-desktop:/media/Book/MS/CD/Finite_Field_Softs_Anup/NTT_software_PSEC$
```