Supplementary material

Our GitHub not only contains our source code (client.cpp, server.cpp, pairing_1.h), but we also uploaded our compiled demo software (Compiledprogram.zip). If you want to verify quickly, just unzip and run the demo program we have compiled. If you want to compile yourself, please follow the instructions below.

Code compilation guide

1. Compile the library miracle.lib according to the open source project Miracl (https://github.com/miracl/MIRACL).
2. Then replace the pairing_1.h file in the open source project with the pairing_1.h file in this folder. We add the two constructor functions that we need in our code in this new file. You can read the code for details, which I have annotated.
3. Then you can open the VS**** x** compiler in the Visual Studio Tools folder to compile the source code, because we are in vs2013 development of the 32-bit program, so we open is VS2013 x86 compiler, you can compile according to your needs and environment.
4. The compile commands for our code on the client and server are “cl /O2 /GX client.cpp ssp_pair.cpp ecn.cpp zzn2.cpp zzn.cpp big.cpp miracl.lib” and “cl /O2 /GX server.cpp ssp_pair.cpp ecn.cpp zzn2.cpp zzn.cpp big.cpp miracl.lib” respectively.

Demo software usage guide

To make the demo software easier to understand, our program prints out all the key information, and we will demonstrate our software below. Detailed algorithms can refer to our paper.

1. First open two terminal windows and run the server.exe and client.exe programs respectively. They will print the public parameters that have been initialized.

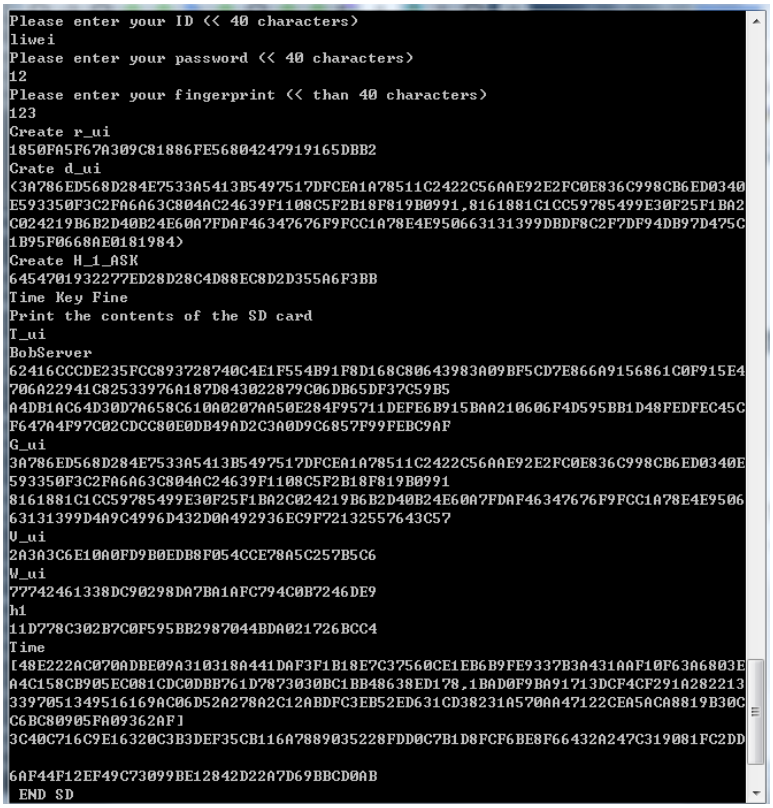
```
C:\Users\Administrator\Desktop\ALL\miracl2>server.exe
Verifty Pulib Params
[51FD78661D94186CFD3FE19BCB90FCB69DE2F1DEE978B8B499427F3E8FC4F88E8467311FA330176
C2CB4A6BD3A76B66BE0F451EA500E90C7DC9A12BCA371A409,F0C26D2BBE07D264C1610C1B244BBC
E240B7EFE024BAA2DB35135EB81EC37C0FB3103AFF28717C4C101040A6F51CD476C56ECA767AAF18
8B2C0D7DC2D7373F0]
[A1C7A2DA2FA0D9F9AE47472AC260D1BE2328E9F09E3779E92FCEBE5A5EDB3F03AD293E4CC033090
2BE70C4230B0C86272F7C333D90F31018C2280BFCAABBC708,16EF1137BF083E5DA3BED0BD435A9D
30F816A08156930A29C7FE6859902EBD0B5144C3B168E9338A1549C849352F335762ADA03DB7C31D
49CB16B2C862AA3AE9]
(30ADC99A4936991179D9B8FB0382799346832DA926D950FDA5C50590808E06EEB6641C12E5BF622
AE510915152BFC83E6436AF7ABE8DFE5993A4A6678C76F5BA,7844CD595F1DFFA1C109A78EEF9A07
E1A75A31004C641D39AA45D45119CE6F4923D31C4BDB4F0B284ABEC74C78DBA518810D763D065BA7
763F2D253AEE747080)
(B3246A9D3D6526208925EE80787CD1F90D35EC7939B2FDAF32BB4D3E6EDE19DD63CEFF15B0779F9
F046D0F98240A0FAA838D1A22B80C9CB2AFB417EAEDAE9B14,B067F61DF3431F919FFA403F4A3E0B
D1986A04E3B9BE1F1DFDBA726D4D8BE12910046503070A322A9646F5104BD39E8B6B02E13916D929
72D4660B06607FC3EF)
1234567890
4B27AA7BC8BBC22583EF30FFAF0884240FE6590C
7A724F4454587FD1F32948073972D3720A6CED02
Verifty Pulib Params End
Enter 1 --> Authentication and Key Agreement
Enter 2 -->Create a New Server
Enter 3 --> Termination Process
```

```
C:\Users\Administrator\Desktop\ALL\miracl2>client.exe
Verifty Pulib Params
[51FD78661D94186CFD3FE19BCB90FCB69DE2F1DEE978B8B499427F3E8FC4F88E8467311FA330176
C2CB4A6BD3A76B66BE0F451EA500E90C7DC9A12BCA371A409,F0C26D2BBE07D264C1610C1B244BBC
E240B7EFE024BAA2DB35135EB81EC37C0FB3103AFF28717C4C101040A6F51CD476C56ECA767AAF18
8B2C0D7DC2D7373F0]
[A1C7A2DA2FA0D9F9AE47472AC260D1BE2328E9F09E3779E92FCEBE5A5EDB3F03AD293E4CC033090
2BE70C4230B0C86272F7C333D90F31018C2280BFCAABBC708,16EF1137BF083E5DA3BED0BD435A9D
30F816A08156930A29C7FE6859902EBD0B5144C3B168E9338A1549C849352F335762ADA03DB7C31D
49CB16B2C862AA3AE9]
(30ADC99A4936991179D9B8FB0382799346832DA926D950FDA5C50590808E06EEB6641C12E5BF622
AE510915152BFC83E6436AF7ABE8DFE5993A4A6678C76F5BA,7844CD595F1DFFA1C109A78EEF9A07
E1A75A31004C641D39AA45D45119CE6F4923D31C4BDB4F0B284ABEC74C78DBA518810D763D065BA7
763F2D253AEE747080)
(B3246A9D3D6526208925EE80787CD1F90D35EC7939B2FDAF32BB4D3E6EDE19DD63CEFF15B0779F9
F046D0F98240A0FAA838D1A22B80C9CB2AFB417EAEDAE9B14,B067F61DF3431F919FFA403F4A3E0B
D1986A04E3B9BE1F1DFDBA726D4D8BE12910046503070A322A9646F5104BD39E8B6B02E13916D929
72D4660B06607FC3EF)
1234567890
4B27AA7BC8BBC22583EF30FFAF0884240FE6590C
7A724F4454587FD1F32948073972D3720A6CED02
Verifty Pulib Params End
Enter 0 --> User Registration Phase
Enter 1 --> Login And Exchanging
Enter 2 --> Change New Password And Fingerprint
Enter 3 --> Updata New Server
Enter 4 --> Termination Process
```

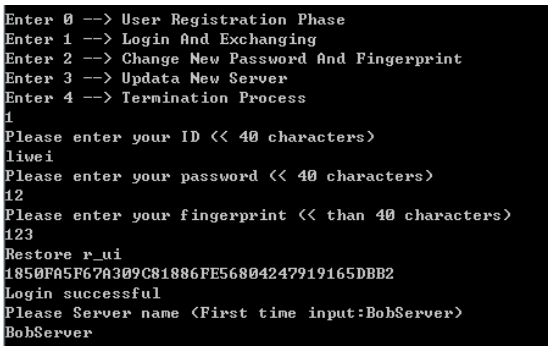
To complete a quick certification experiment, we have initialized a BobServer service on the server side. We enter 1 in the service program and press Enter, then enter the name of our default service. At this time, the network initialization of the server has been completed, and the local 8000 port is monitored.

```
Verifty Pulib Params End
Enter 1 --> Authentication and Key Agreement
Enter 2 -->Create a New Server
Enter 3 --> Termination Process
1
Enter a name for the server to use for authentication.
If you are not registered new server, please enter: BobServer .
Otherwise enter name of the server you registered
BobServer
Server side has been initialized. Waiting for connection
```

Next, we need to enter 0 to complete a user registration. When you enter the ID, password, and biometric information, an SD card is generated. Finally, we print out the contents of the SD card.



Next, we can complete a login and authentication. Enter 1 and follow the prompts to enter your registration information and the name of the authentication server (if you don't add the new of the server, default to BobServer), it will automatically complete the next work.



We also print out the process of restoring authentication information from the network communication string in the server and client respectively.

Finally, we saw that they not only successfully authenticated each other, but also negotiated the session key.

2. You can also enter 2 to modify the user password and biometric information, but make sure the user is already registered. Then you can use the new password and biometric information to complete the login, authentication and other work.

```
Enter 0 --> User Registration Phase
Enter 1 --> Login And Exchanging
Enter 2 --> Change New Password And Fingerprint
Enter 3 --> Updata New Server
Enter 4 --> Termination Process
2
Please enter your ID (< 40 characters)
liwei
Please enter your password (< 40 characters)
12
Please enter your fingerprint (< than 40 characters)
123
Login successful
Please Enter New Password
23
Please Enter New Fingerprint
234
Has been successful change password and fingerprint
Enter 0 --> User Registration Phase
Enter 1 --> Login And Exchanging
Enter 2 --> Change New Password And Fingerprint
Enter 3 --> Updata New Server
Enter 4 --> Termination Process
```

3. You can also enter 2, 3 to add a new server on the server and client respectively. If you want to use a new server to authenticate and agreement keys, make sure that the same server is updated on both sides.

```
Enter 1 --> Authentication and Key Agreement
Enter 2 -->Create a New Server
Enter 3 --> Termination Process
2
Input new server name ( <40 characters)
Alice
Enter 1 --> Authentication and Key Agreement
Enter 2 -->Create a New Server
Enter 3 --> Termination Process
```

```
Enter 0 --> User Registration Phase
Enter 1 --> Login And Exchanging
Enter 2 --> Change New Password And Fingerprint
Enter 3 --> Updata New Server
Enter 4 --> Termination Process
3
Make sure the updated server is already registered
Enter new Server name ( <40 characters )
Alice
Please enter your ID (< 40 characters)
liwei
Please enter your password (< 40 characters)
23
Please enter your fingerprint (< than 40 characters)
234
Restore d_ui
(3A786ED568D284E7533A5413B5497517DFCEA1A78511C2422C56AAE92E2FC0E836C998CB6ED0340
E593350F3C2FA6A63C804AC24639F1108C5F2B18F819B0991.8161881C1CC59785499E30F25F1BA2
C024219B6B2D40B24E60A7FDAF46347676F9FCC1A78E4E950663131399DBDF8C2F7DF94DB97D475C
1B95F0668AE0181984)
Enter 0 --> User Registration Phase
Enter 1 --> Login And Exchanging
Enter 2 --> Change New Password And Fingerprint
Enter 3 --> Updata New Server
Enter 4 --> Termination Process
```