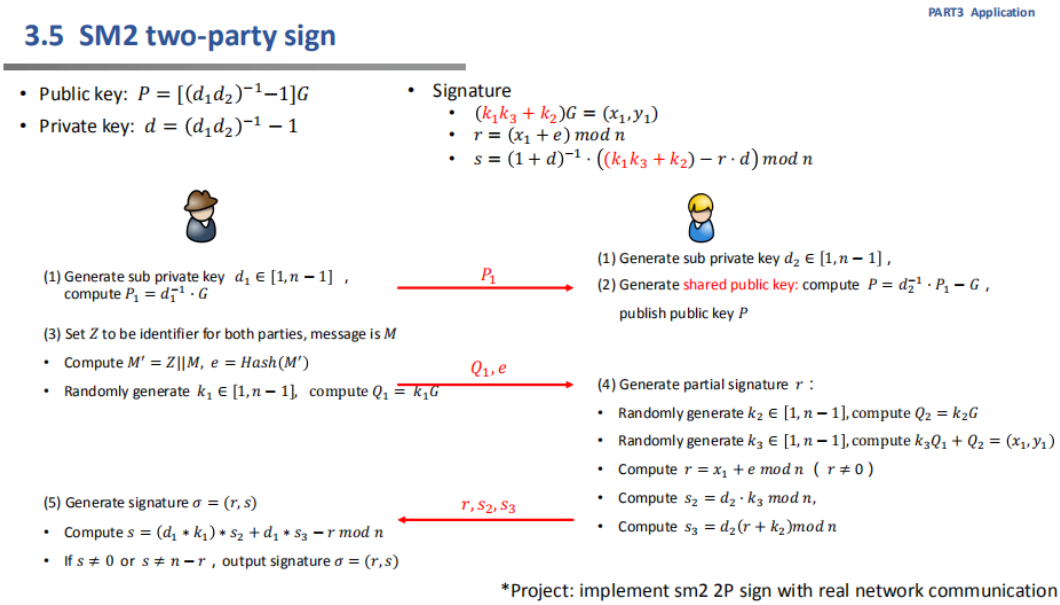
Report

本项目实现的是SM2-two party sign ,采用的SM2为Gmssl库中的实现方式，实验原理如下所示：



采用的网络通信方式为python 中的socket套接字，采用tcp协议完成，关于策略实现的正确性如下所示：

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\SM2-two-party sign\正确性证明.py"
计算通过分步计算得到的s为：66151618728396126077616228615048692101429082212705988056651975304801562121181
计算通过私钥直接计算的s为：66151618728396126077616228615048692101429082212705988056651975304801562121181
算法正确性验证成功!
```

随后网络通信的结果如下所示，可以看到通信成功建立，并且完成了签名

```
计算通过私钥直接计算的s为：66151618728396126077616228615048692101429082212705988056651975304801562121181
算法正确性验证成功!

C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\SM2-two-party sign\Alice.py"
这里是Alice，等待接入.....
接收到数据为： 69629972d6838185d93ba8208dc74f7fb93f6d0a36aab1d6eb0ff05413cb8457c7bbbf59caef2bf19ddaaca691411d847b772066bb853c0ab2cdd519b8b2628d
此时可以恢复出公钥为： 9a487a9d334b418593a73426ac09f3929e4ead2215e2200e9b95deda3ef0a27ee8c52a111f23bc435a7a68835881ccfd83d7beb59495c71ec391433deef12a55
这里是Alice，等待接入.....
接收到数据为： 4d9b8c295950c3793db1fce14695f2eddb52d33d9c9a31715b6677b780484efe425a553da35f0b59aaec3d5d1c4d5e43a811ea4e3e617603ddc6c8249bc6e1c8
这里是Alice，等待接入.....
接收到数据为： 4dfc424de2567f6eaf773ea1c388d0dd8e2870fe1b0219a62555c41c24e4ceff
这里是Alice，等待接入.....
发送的数据为：76343171079462152962204425928851893514410384944773357002700423046165479365915
这里是Alice，等待接入.....
发送的数据为：79440272969842601167418308122088488833447739420182831281833698859175388552636 4
这里是Alice，等待接入.....
发送的数据为：21773151190808431922874254609271921595501410549095017474300020001248469855324
```

```
Microsoft Windows [版本 10.0.19044.1826]
(c) Microsoft Corporation。保留所有权利。

C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\SM2-two-party sign\Bob.py"
这里是Bob，连接成功!!
发送的数据为： 69629972d6838185d93ba8208dc74f7fb93f6d0a36aab1d6eb0ff05413cb8457c7bbbf59caef2bf19ddaaca691411d847b772066bb853c0ab2cdd519b8b2628d
这里是Bob，连接成功!!
发送的数据为： 4d9b8c295950c3793db1fce14695f2eddb52d33d9c9a31715b6677b780484efe425a553da35f0b59aaec3d5d1c4d5e43a811ea4e3e617603ddc6c8249bc6e1c8
这里是Bob，连接成功!!
发送的数据为： 4dfc424de2567f6eaf773ea1c388d0dd8e2870fe1b0219a62555c41c24e4ceff
这里是Bob，连接成功!!
接收到数据为： 76343171079462152962204425928851893514410384944773357002700423046165479365915
这里是Bob，连接成功!!
接收到数据为： 79440272969842601167418308122088488833447739420182831281833698859175388552636 4
这里是Bob，连接成功!!
接收到数据为： 21773151190808431922874254609271921595501410549095017474300020001248469855324
最终得到的签名值为： a8c8b41d4f29c0bffb3473820beb0c6a5c7331047e5b9adfb99963be80ad1d1ba03e53b8edb997841f6d35c1ad2d495b30fccad45e56aeb649be284bc299bd81
```