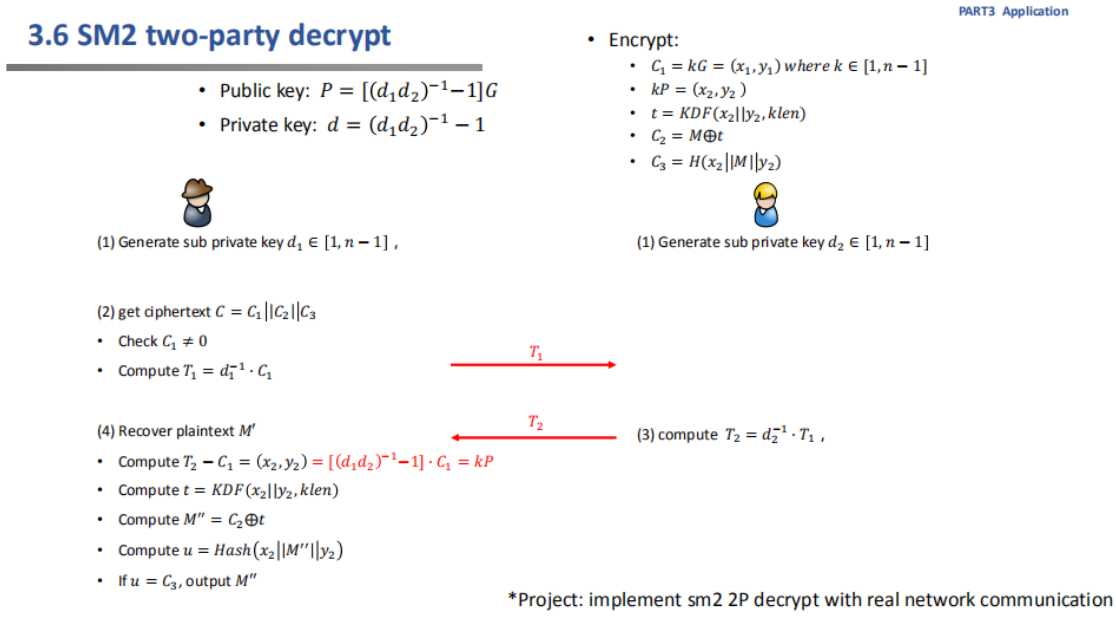
Report

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



在上图中还缺步骤，和之前的sign方案相同，通过d1，d2，协商出公钥，然后由右边的Alice 发给左边的Bob

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) 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 decrypt\正确性证明.py"
C3= bdc69099343244a41ce36387cc3e610e3478ebf09d022dd559c77de91d44eb0d
u = bdc69099343244a41ce36387cc3e610e3478ebf09d022dd559c77de91d44eb0d
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，并且完成了解密

```
u = bdc69099343244a41ce36387cc3e610e3478ebf09d022dd559c77de91d44eb0d
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 decrypt\Alice.py"
这里是Alice，等待接入.....
接收到数据为： 91afdfe17a3c7bfcbdbbb52a7be7432b3c1ea242ffd55da0cbc1f81bdb3a63055327d4a74bcf54c7c7b27261e096355515d6f39a3d64da63befab8fead8d355f
此时可以恢复出公钥为： 58792adda73c8d5c9b90b9cd5a36cd2bbfa27023be94fe3bccd539921b4900fdd1c92bd5aa0458dbc3cb046ed9c053b20297957a51d4a9245039a8899bcd2779
接下来将通过公钥计算出来的密文传给Bob
这里是Alice，等待接入.....
发送的数据为： 1b2454d7e884bdfe3f48725d0ace3fa877f79da37f0ce4824c6a48192ff166deeb32a62c2b414f054a15de943d74225cdcfc52579ba43fd361945b5bf818bc39
这里是Alice，等待接入.....
发送的数据为： e52cb0c9aa398e013138a88a
这里是Alice，等待接入.....
发送的数据为： 7da5f03a5f2abc5ff4952ac4b32fc4926d7df58ee41d8031e793510c15e7770e
这里是Alice，等待接入.....
接收到数据为： ef5ba8904a9ed8139b0090285c8a0c583cb63b93c596fa99154efcfdf2ca24af487b5101735c4ed7a550a54848d911a2909027453854917306 4c22642ca97f4
这里是Alice，等待接入.....
发送的数据为： b71aaa0ad72e9872472c032adf681a180fd7d2997d6a64e32657a1f5cbb86700d6aee02b3a6ab74402f3e3f1a889c2eefd4b30393 96fe5e20b8aba42afb3badf
12
这里是Alice，等待接入.....
发送的数据为： 12

C:\Users\86180>
```

```
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 decrypt\Bob.py"
这里是Bob，连接成功!!
发送的数据为： 91afdfe17a3c7bfcbdbbb52a7be7432b3c1ea242ffd55da0cbc1f81bdb3a63055327d4a74bcf54c7c7b27261e096355515d6f39a3d64da63befab8fead8d355f
这里是Bob，连接成功!!
接收到数据为： 1b2454d7e884bdfe3f48725d0ace3fa877f79da37f0ce4824c6a48192ff166deeb32a62c2b414f054a15de943d74225cdcfc52579ba43fd361945b5bf818bc39
这里是Bob，连接成功!!
接收到数据为： e52cb0c9aa398e013138a88a
这里是Bob，连接成功!!
接收到数据为： 7da5f03a5f2abc5ff4952ac4b32fc4926d7df58ee41d8031e793510c15e7770e
这里是Bob，连接成功!!
发送的数据为： ef5ba8904a9ed8139b0090285c8a0c583cb63b93c596fa99154efcfdf2ca24af487b5101735c4ed7a550a54848d911a2909027453285491730 64c22642ca97f4
这里是Bob，连接成功!!
接收到数据为： b71aaa0ad72e9872472c032adf681a180fd7d2997d6a64e32657a1f5cbb86700d6aee02b3a6ab74402f3e3f1a889c2eefd4b3039396fe5e20b8aba42afb3badf
这里是Bob，连接成功!!
接收到数据为： 12
C3= 7da5f03a5f2abc5ff4952ac4b32fc4926d7df58ee41d8031e793510c15e7770e
u = 7da5f03a5f2abc5ff4952ac4b32fc4926d7df58ee41d8031e793510c15e7770e
恢复的明文为：(16进制) 46656e67205869616e676469
转化为字符串为： Feng Xiangdi

C:\Users\86180>
```