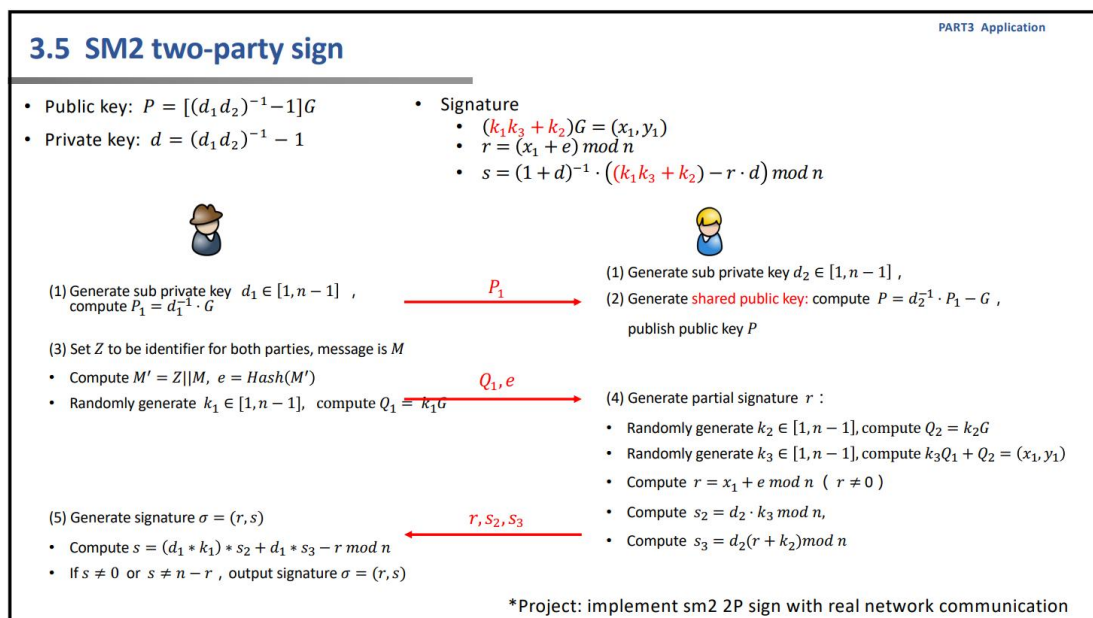


Project15: implement sm2 2P sign with real network communication



算法简介:

为了实现 SM2 曲线上的 2P 签名并进行真实的网络通信，我们需要对 SM2 算法进行一些增强。步骤之一包括：

调整所使用的椭圆曲线参数，将 SM2 的参数设置为你选择的 SM2 曲线参数。

利用 Python 的 socket 模块来实现网络通信。需要编写适当的代码来创建 UDP 客户端或服务器，从而能够发送和接收数据。请注意，发送和接收数据时，需要对数据进行适当的编码和解码，例如：

```
1. client.sendto(x.encode('utf-8'), address)
2. client.sendto(y.encode('utf-8'), address)
```

同时修改代码，以便可以根据 SM2 的签名结果和已知的参数来推导 SM2 公钥。

实现方式：python

结果:

服务端:

```
===== RESTART: E:\project15\服务端  
===  
等待建立连接...  
连接已关闭
```

客户端:

```
连接建立  
Signature : 0x9f52618fe491272aefed7c5e647b2665d1e08eb0674cafed65a79141028a52d8  
0x629bdlc74656c7311bd63c7531e71fb25c56324b376c70ad7a95087462aa1f76
```

分工: 自己独立完成