Report

这个项目完成的是想办法推断出一个公钥，并且用到尽可能少的信息。

在算法层面，采用的是由优化后的SM2类修改而成的ECDSA算法，采用了SM2类中的一些点乘，点加运算等，同时实现了ECDSA的签名和验签，ECDSA的具体原理过程如下图所示：

- Key Gen: $P = dG$, n is order
- Sign(m)
  - $k \leftarrow Z_n^*, R = kG$
  - $r = R_x \bmod n, r \neq 0$
  - $e = hash(m)$
  - $s = k^{-1}(e + dr) \bmod n$
  - Signature is (r, s)
- Verify (r, s) of m with P
  - $e = hash(m)$
  - $w = s^{-1} \bmod n$
  - $(r', s') = e \cdot wG + r \cdot wP$
  - Check if $r' == r$
  - Holds for correct sig since
  - $es^{-1}G + rs^{-1}P = s^{-1}(eG + rP) =$
  - $k(e + dr)^{-1}(e + dr)G = kG = R$

因为要推断公钥信息，因为如果知道（r，s）和e，另外还知道之前的随机数k，就可以算出公钥：

$$d_a = r^{-1}(sk - e) \bmod n$$

根据这个等式，如果我们想知道公钥的话，代入得：

$$\mathrm{Q_a = d_a G = r^{-1}(sk - e) \cdot G = r^{-1}(\,s \cdot kG - eG) = r^{-1}(sK - eG)}$$

可以发现，点K的坐标是关键，只要能知道点K的坐标x1,y1。已知

$$r = x1 \bmod n, n < p < 2n$$

因此，x1一共有两种可能： x1=r 或 x1 =r+n 所以在这里我们要花1bit的信息来告诉推断公钥的函数x1的取值

同时，对于一个确定的x1，y1也有正负两种可能，在模p的背景下，因为p是奇数，所以可以通过y1的奇偶性来判断y1的值，如果y1和计算出来的y1'奇偶性不符，那么y1=p-y1。

综上所示，有了这两个信息，我们就能推断出公钥的值

同时，在恢复公钥的时候，我们还需要用到费马小定理：

$$y^p \equiv y \bmod p \rightarrow y^{p+1} \equiv y^2 \bmod p$$

设

$$Y = y^2 \bmod p$$

则有：

$$\mathrm{Y}^{\frac{\mathrm{p}+1}{2}} \equiv \mathrm{Y} \pmod{\mathrm{p}} \Rightarrow \mathrm{y} = \pm \mathrm{Y}^{\frac{\mathrm{p}+1}{4}} \bmod \mathrm{p}$$

综上，我们可以设置一个2bit的flag来确定公钥具体的值，因此需要多添加2bit的信息，具体的执行结果如下所示，可以看到，成功恢复了公钥，完成了验签过程：

```
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\ECDSA-deduce publickey\ecdsa-dp.py"
恢复出来的公钥为：  b9c9a6e04e9c91f7ba880429273747d7ef5ddeb0bb2ff6317eb00bef331a83081a6994b8993f3f5d6eadddb81872266c87c018fb4162f5af347b483e24620207
初始公钥为：  B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDDB81872266C87C018FB4162F5AF347B483E24620207
恢复成功

发送信息为  r: 350097128238088702891899054022661985834199872870904616357639903269165687244 58 s: 72036904842761814129573801613593767656499875116423882386752590618376779426599 flag: 01 msg: Feng Xiangdi
验签成功

C:\Users\86180>
```