Report

在本项目中一共复刻了关于SM2的4种pitfall：

leaking k

- Compute d_A with $\sigma = (r, s)$ and k ：
  - $s = \left((1 + d_A)^{-1} \cdot (k - r \cdot d_A)\right) mod\ n$
  - $s(1 + d_A) = (k - r \cdot d_A)\ mod\ n$
  - $d_A = (s + r)^{-1} \cdot (k - s)\ mod\ n$

reusing k

- Signing message M_1 with d_A
  - Randomly select $k \in [1, n - 1]$, compute $kG = (x, y)$
  - $r_1 = (Hash(Z_A || M_1) + x)\ mod\ n$
  - $s_1 = \left((1 + d_A)^{-1} \cdot (k - r_1 \cdot d_A)\right) mod\ n$
- Signing message M_2 with d_A
  - Reuse the same k, $kG = (x, y)$
  - $r_2 = (Hash(Z_A || M_2) + x)\ mod\ n$
  - $s_2 = \left((1 + d_A)^{-1} \cdot (k - r_2 \cdot d_A)\right) mod\ n$
- Recovering d_A with 2 signatures $(r_1, s_1), (r_2, s_2)$
  - $s_1(1 + d_A) = (k - r_1 \cdot d_A)\ mod\ n$
  - $s_2(1 + d_A) = (k - r_2 \cdot d_A)\ mod\ n$
  - $d_A = \frac{s_2 - s_1}{s_1 - s_2 + r_1 - r_2}\ mod\ n$

reusing k by different users

- Alice signed message M_1 with $d_A, \sigma_A = (r_1, s_1)$
  - Randomly select $k \in [1, n-1]$, compute $kG = (x, y)$
  - $r_1 = (Hash(Z_A||M_1) + x) \, mod \, n$
  - $s_1 = \left((1 + d_A)^{-1} \cdot (k - r_1 \cdot d_A)\right) mod \, n$
- Bob signed message M_2 with $d_B, \sigma_B = (r_2, s_2)$
  - Reuse the same k, $kG = (x, y)$
  - $r_2 = (Hash(Z_B||M_2) + x) \, mod \, n$
  - $s_2 = \left((1 + d_B)^{-1} \cdot (k - r_2 \cdot d_B)\right) mod \, n$
- Alice can deduce Bob secret key
  - $d_B = \frac{k - s_2}{s_2 + r_2} \, mod \, n$
- Bob can deduce Alice secret key
  - $d_A = \frac{k - s_1}{s_1 + r_1} \, mod \, n$

same d and k with ECDSA

- ECDSA signing with private key d
  - Randomly select k, $R = kG = (x, y)$
  - $e_1 = hash(m)$
  - $r_1 = x \, mod \, n, s_1 = (e_1 + r_1 d) k^{-1} mod \, n$
  - Signature (r_1, s_1)
- SM2 signing with private key d
  - Reuse the same k as ECDSA, $(x, y) = kG$
  - $e_2 = h(Z_A||m)$
  - $r_2 = (e_2 + x) \, mod \, n$
  - $s_2 = (1 + d)^{-1} \cdot (k - r_2 d) mod \, n$
  - Signature (r_2, s_2)
- With the two sigs, private key d can be recovered:
  - $d \cdot r_1 = k s_1 - e_1 \, mod \, n$
  - $d \cdot (s_2 + r_2) = k - s_2 \, mod \, n$
  - $d = \frac{s_1 s_2 - e_1}{(r_1 - s_1 s_2 - s_1 r_2)} mod \, n$

在代码中我复现了这些pitfalls，最终结果如下所示：

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local
leaking k leads to leaking of d 验证成功
reusing k leads to leaking of d 验证成功
Alice got the leaking d of Bob 验证成功
Bob got the leaking d of Alice 验证成功
SM2 using same d and k with ECDSA leads to leaking of d 验证成功
```