**一、算法概述**

SM2 是中国国家密码算法，基于椭圆曲线密码体制（ECC），采用与 ECDSA 类似的思路，但引入了用户标识（ZA）参与签名，提升安全性。签名算法用于验证消息的完整性与身份真实性。

**二、数学背景**

**1. 椭圆曲线定义**

在有限域 Fp上的椭圆曲线为：

文本, 信件

AI 生成的内容可能不正确。

**2. 基本参数**

* p：素数，定义有限域 Fp\mathbb{F}\_pFp​
* a,b：曲线参数
* G=(xG,yG)：基点，生成子群
* n：G 的阶（满足 nG= O）
* dA∈[1,n−1]：签名者私钥
* PA=dA⋅G：签名者公钥

**三、用户身份标识 ZA 的计算**

为了防止不同用户间的签名重用攻击，SM2 引入 ZA（用户绑定摘要）：



 ID\_A​：签名者身份标识

 ENTL\_A ​：标识长度（以比特为单位）

 (x\_A,y\_A)：用户公钥坐标

 Hash 通常使用 SM3

**四、签名过程**

输入：私钥 d\_A​、消息 M、系统参数 (p,a,b,G,n)

**步骤：**

1. **预处理**  
    计算 ZA，然后：



1. **随机数生成**

选取 k∈[1,n−1]

**计算点**

图片包含 文本

AI 生成的内容可能不正确。

若 r=0 或 r+k=n，重新生成 k

1. 计算 s



若 s=0，重新生成 k

**五、验签过程**

输入：消息 MMM、签名 (r,s)、签名者公钥 P\_A

**步骤：**

1. **检查合法性**  
    验证 r,s∈[1,n−1]
2. 计算 e



1. 计算 t

若 t=0，验签失败图示

AI 生成的内容可能不正确。

1. 计算椭圆曲线点
2. 计算 r'图片包含 文本

   AI 生成的内容可能不正确。

文本

AI 生成的内容可能不正确。

1. 比对 r' 和 r,验签成功当且仅当 r′=r

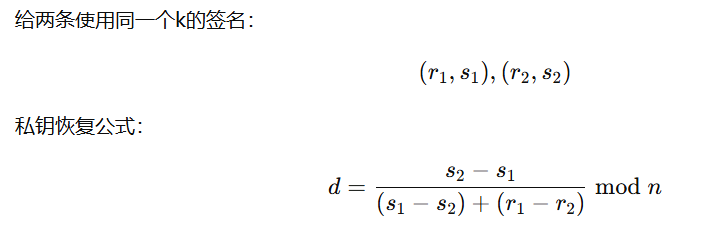
攻击推导式：

1. k值泄露恢复私钥

文本

AI 生成的内容可能不正确。

1. 两条签名重复k恢复私钥

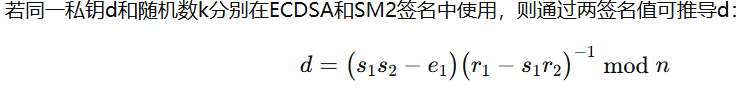


1. 跨用户重复k（不同私钥，重复k）

文本, 信件

AI 生成的内容可能不正确。

1. ECDSA与SM2使用同一d,k



实验结果：



文本

AI 生成的内容可能不正确。

