# SM2 算法及安全漏洞分析

## 一、算法概述

SM2 是我国自主研发的椭圆曲线密码算法，基于椭圆曲线离散对数问题（ECDLP）构建，具备签名、加密、密钥交换等功能。与国际主流的 ECC 算法相比，SM2 在参数选择、签名流程等方面进行了优化，更适合国内密码应用场景。其安全性依赖于有限域上椭圆曲线点运算的数学复杂性，同等安全强度下，密钥长度远短于 RSA 算法，具有更高的计算效率。

## 二、核心数学基础

### 2.1 椭圆曲线基础

* **曲线方程**：SM2 采用的椭圆曲线方程为，定义在有限域 上，其中 q 为素数（文档中给定 q = 0x8542D69E4C044F18E8B92435BF6FF7DE457283915C45517D722EDB8B08F1DFC3 ）。
* **点运算特性**：曲线上的点对 “加法” 和 “数乘” 运算封闭，满足交换律和结合律。利用该特性可实现密钥生成与加密签名的核心逻辑，例如点乘运算 （ k 为标量， P 为曲线上的点）。

### 2.2 有限域与参数

* **有限域** ：包含 q 个元素的集合，支持加减乘除运算（除零外），是椭圆曲线定义的基础。
* **系统参数**：SM2 定义了一组固定参数，包括曲线参数 a, b 、基点 G 、阶 n 、余因子 h 等，所有运算均基于这些参数展开。

## 三、核心功能流程

### 3.1 签名与验证

1. **签名生成（Sign）**：
   * 预处理：计算
   * 计算签名：。
2. **签名验证（Verify）**：
   * 校验 r, s 范围，计算
   * 计算

### 3.2 加密与解密

1. **加密（Encrypt）**：
   * 生成随机数 k ，计算
   * 派生密钥，计算 。
2. **解密（Decrypt）**：
   * 计算，派生
   * 解密得 ，验证 。

## 四、安全漏洞分析

### 4.1 随机数 k 泄露

* **风险**：若签名过程中随机数 k 泄露，攻击者可通过公式 推导私钥
* **案例**：重复使用 k 对不同消息签名时，攻击者可联立两个签名方程求解私钥。

### 4.2 多用户密钥泄露

* **风险**：不同用户若使用相同 k 签名，可相互推导对方私钥，例如 Alice 可通过 Bob 的签名计算

### 4.3 与 ECDSA 兼容性风险

* **风险**：同一私钥 d 和随机数 k 若同时用于 SM2 和 ECDSA 签名，攻击者可通过联立两种算法的签名公式破解私钥。