SM2椭圆曲线密码算法原理与推导

1. 概述

SM2是中国国家密码管理局发布的椭圆曲线公钥密码算法标准（GB/T 32905-2016），适用于数字签名、密钥交换和公钥加密等场景。其安全性基于椭圆曲线离散对数问题（ECDLP）的计算困难性，具有比RSA更高的效率。

2. 数学基础

2.1 椭圆曲线定义

SM2使用的椭圆曲线定义在有限域GF(p)上，其方程为：

$$y^2 = x^3 + ax + b \mod p$$

其中：

- p是一个大质数
- a和b是曲线参数，满足$4a^3 + 27b^2 \neq 0 \mod p$（确保曲线非奇异）

SM2推荐的曲线参数为：

- p = 0x8542D69E4C044F18E8B92435BF6FF7DE457283915C45517D722EDB8B08F1DFC3
- a = 0x787968B4FA32C3FD2417842E73BBFEFF2F3C848B6831D7E0EC65228B3937E498
- b = 0x63E4C6D3B23B0C849CF84241484BFE48F61D59A5B16BA06E6E12D1DA27C5249A

2.2 椭圆曲线点运算

椭圆曲线上的点组成一个加法群，满足群的所有性质。群运算定义如下：

1. **点加法**：对于曲线上的两点$P(x_1,y_1)$和$Q(x_2,y_2)$，它们的和$R(x_3,y_3)$定义为：
   - 若$P \neq Q$且$x_1 \neq x_2$：

$$k = \frac{y_2 - y_1}{x_2 - x_1} \mod p$$

$$x_3 = k^2 - x_1 - x_2 \mod p$$

$$y_3 = k(x_1 - x_3) - y_1 \mod p$$

   - 若P = Q：

$$k = \frac{3x_1^2 + a}{2y_1} \mod p$$

$$x_3 = k^2 - 2x_1 \mod p$$

$$y_3 = k(x_1 - x_3) - y_1 \mod p$$

2. **点乘法**：对于整数k和曲线上的点P，kP定义为P自身相加k次：

$$kP = \underbrace{P + P + \cdots + P}_{k次}$$

   实际计算中使用快速幂算法（double-and-add）优化计算。

3. **单位元**：无穷远点O，满足对任意点P，有P + O = P。

4. **逆元**：对于点P(x,y)，其逆元为-P(x,-y mod p)，满足P + (-P) = O。

2.3 椭圆曲线离散对数问题

SM2的安全性基于椭圆曲线离散对数问题（ECDLP）的计算困难性：

给定椭圆曲线上的点P和Q = kP，其中k是整数，求k的值在计算上是困难的。

SM2使用的基点G及其阶n为：

- Gx = 0x421DEBD61B62EAB6746434EBC3CC315E32220B3BADD50BDC4C4E6C147FEDD43D
- Gy = 0x0680512BCBB42C07D47349D2153B70C4E5D7FDFCBFA36EA1A85841B9E46E09A2
- n = 0x8542D69E4C044F18E8B92435BF6FF7DD297720630485628D5AE74EE7C32E79B7

其中n是基点G的阶，即nG = O，且n是一个大质数。

3. SM2数字签名算法

3.1 密钥对生成

1. 随机生成私钥d，满足1 < d < n-1
2. 计算公钥P = dG，其中G是基点

3.2 Z值计算

Z值是用户ID和公钥的哈希值，用于增强签名的安全性：

$$Z = SM3(ENTLA||ID||a||b||Gx||Gy||Px||Py)$$

其中：

- ENTLA是ID长度（比特数），用2字节表示
- ID是用户标识
- a, b是曲线参数
- Gx, Gy是基点坐标

- Px, Py是公钥坐标

3.3 签名生成

对于消息M，签名过程如下：

1. 计算e = SM3(Z || M)，将e转换为整数
2. 随机生成k，满足1 < k < n-1
3. 计算kG = (x_1, y_1)
4. 计算r = $(e + x_1) \bmod n$，若r = 0或r + k = n，则返回步骤2
5. 计算s = $[(1 + d)^{-1} (k - r d)] \bmod n$，若s = 0，则返回步骤2
6. 签名结果为(r, s)

3.4 签名验证

对于消息M和签名(r, s)，验证过程如下：

1. 检查r和s是否满足$1 \le r, s \le n-1$，若不满足则验证失败
2. 计算e = SM3(Z || M)，将e转换为整数
3. 计算$t = (r + s) \bmod n$，若t = 0则验证失败
4. 计算$sG + tP = (x_1, y_1)$，若结果为O则验证失败
5. 计算$R = (e + x_1) \bmod n$
6. 若R = r则验证通过，否则失败

4. 算法安全性分析

SM2的安全性基于以下几点：

1. 椭圆曲线离散对数问题（ECDLP）的计算困难性
2. 每次签名使用不同的随机数k
3. Z值的引入将签名与用户ID绑定，防止跨用户的签名重用
4. 签名生成过程中的各种检查（如$r, s \neq 0$等）

与RSA相比，SM2在相同安全级别下具有更短的密钥长度，例如：

- 256位椭圆曲线（SM2）提供与3072位RSA相当的安全性
- 这使得SM2在存储和传输效率上具有优势