SM2 签名算法的数学推导

1. 签名生成过程

假设消息 M 和私钥 d_A，签名结果为 (r, s)，签名生成过程如下：

1. 计算消息 M 和标识符 Z_A 的哈希值：

$$e = H(Z_A \parallel M) \mod n$$

2. 选择一个随机数 $k \in [1, n-1]$，计算点 $kG = (x_1, y_1)$。

3. 计算签名中的 r 值：

$$r = (e + x_1) \mod n$$

如果 $r = 0$ 或 $r + k = n$，则重新选择 k。

4. 计算签名中的 s 值：

$$s = (1 + d_A)^{-1} \cdot (k - r \cdot d_A) \mod n$$

如果 $s = 0$，则重新选择 k。

签名结果为 (r, s)。

2. 签名验证过程

给定公钥 P_A，签名 (r, s)，以及消息 M，验证过程如下：

1. 计算消息 M 和标识符 Z_A 的哈希值：

$$e' = H(Z_A \parallel M) \mod n$$

2. 计算验证中的 t 值：

$$t = (r + s) \mod n$$

如果 $t = 0$，则验证失败。

3. 计算点 (x_1', y_1')：

$$(x_1', y_1') = s \cdot G + t \cdot P_A$$

4. 计算验证值 R：

$$R = (e' + x_1') \mod n$$

如果 $R = r$，则签名有效，否则无效。