ICS 35.040
L 80
备案号：36826—2012

GM

中华人民共和国密码行业标准

GM/T 0003.1—2012

SM2 椭圆曲线公钥密码算法
第 1 部分：总则

Public key cryptographic algorithm SM2 based on elliptic curves—Part 1：General

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发 布

目　　次

前　言

GM/T 0003—2012《SM2 椭圆曲线公钥密码算法》分为 5 个部分：

——第 1 部分：总则；

——第 2 部分：数字签名算法；

——第 3 部分：密钥交换协议；

——第 4 部分：公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0003 的第 1 部分。

本部分依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分的附录 A、附录 B、附录 C 和附录 D 为资料性附录。

本部分由国家密码管理局提出并归口。

本部分起草单位：北京华大信安科技有限公司、中国人民解放军信息工程大学、中国科学院数据与通信保护研究教育中心。

本部分主要起草人：陈建华、祝跃飞、叶顶峰、胡磊、裴定一、彭国华、张亚娟、张振峰。

引　言

N. Koblitz 和 V. Miller 在 1985 年各自独立地提出将椭圆曲线应用于公钥密码系统。椭圆曲线公钥密码所基于的曲线性质如下：

——有限域上椭圆曲线在点加运算下构成有限交换群，且其阶与基域规模相近；

——类似于有限域乘法群中的乘幂运算，椭圆曲线多倍点运算构成一个单向函数。

在多倍点运算中，已知多倍点与基点，求解倍数的问题称为椭圆曲线离散对数问题。对于一般椭圆曲线的离散对数问题，目前只存在指数级计算复杂度的求解方法。与大数分解问题及有限域上离散对数问题相比，椭圆曲线离散对数问题的求解难度要大得多。因此，在相同安全程度要求下，椭圆曲线密码较其他公钥密码所需的密钥规模要小得多。

本部分描述必要的数学基础知识与一般技术，以帮助实现其他各部分所规定的密码机制。

SM2 椭圆曲线公钥密码算法
第 1 部分:总则

1 范围

GM/T 0003 的本部分给出了 SM2 椭圆曲线公钥密码算法涉及的必要数学基础知识与相关密码技术,以帮助实现其他各部分所规定的密码机制。

本部分适用于基域为素域和二元扩域的椭圆曲线公钥密码算法。

2 符号和缩略语

下列符号和缩略语适用于本部分。

a,b:F_q中的元素,它们定义 F_q上的一条椭圆曲线 E。

B:MOV 阈。正数 B,使得求取 F_{q^B}上的离散对数至少与求取 F_q上的椭圆曲线离散对数一样困难。

$deg(f)$:多项式 $f(x)$的次数。

E:有限域上由 a 和 b 定义的一条椭圆曲线。

$E(F_q)$:F_q上椭圆曲线 E 的所有有理点(包括无穷远点 O)组成的集合。

$ECDLP$:椭圆曲线离散对数问题。

F_p:包含 p 个元素的素域。

F_q:包含 q 个元素的有限域。

F_q^*:由 F_q中所有非零元构成的乘法群。

F_{2^m}:包含 2^m个元素的二元扩域。

G:椭圆曲线的一个基点,其阶为素数。

$\gcd(x,y)$:x 和 y 的最大公因子。

h:余因子,$h=\sharp E(F_q)/n$,其中 n 是基点 G 的阶。

$LeftRotate()$:循环左移运算。

$l_{\max}$:余因子 h 的最大素因子的上界。

m:二元扩域 F_{2^m}关于 F_2 的扩张次数。

$\bmod f(x)$:模多项式 $f(x)$的运算。若 $f(x)$是二元域上的多项式,则所有系数执行模 2 运算。

$\bmod n$:模 n 运算。例如,$23 \bmod 7=2$。

n:基点 G 的阶(n 是 $\sharp E(F_q)$的素因子)。

O:椭圆曲线上的一个特殊点,称为无穷远点或零点,是椭圆曲线加法群的单位元。

P:$P=(x_P,y_P)$是椭圆曲线上除 O 之外的一个点,其坐标 x_P,y_P满足椭圆曲线方程。

P_1+P_2:椭圆曲线 E 上两个点 P_1 与 P_2 的和。

p:大于 3 的素数。

q:有限域 F_q中元素的数目。

$r_{\min}$:基点 G 的阶 n 的下界。

$Tr()$:迹函数。

x_P:点 P 的 x 坐标。

$x^{-1} \bmod n$:使得 $x \cdot y \equiv 1 (\bmod n)$成立的唯一整数 y,$1 \leqslant y \leqslant n-1$,$\gcd(x,n)=1$。