ICS 35.040
L 80
备案号:36830—2012

GM

中华人民共和国密码行业标准

GM/T 0003.5—2012

SM2 椭圆曲线公钥密码算法
第 5 部分:参数定义

**Public key cryptographic algorithm SM2 based on elliptic curves—
Part 5:Parameter definition**

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 5 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 和附录 C 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。

SM2 椭圆曲线公钥密码算法
第 5 部分:参数定义

1 范围

GM/T 0003 的本部分规定了 SM2 椭圆曲线公钥密码算法的曲线参数,并给出了数字签名与验证、密钥交换与验证、消息加解密示例。

2 参数定义

SM2 使用素数域 256 位椭圆曲线。

椭圆曲线方程:$y^2=x^3+ax+b$

曲线参数:

p=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

a=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

b=28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

n=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

x_G=32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

y_G=BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0