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

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