ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32918.5—2017

信息安全技术
SM2 椭圆曲线公钥密码算法
第 5 部分:参数定义

Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 5:Parameter definition

2017-05-12 发布　　2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 32918《信息安全技术　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 GB/T 32918 的第 5 部分。

本部分按照 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。

本部分由国家密码管理局提出。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)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。

SM2 是国家密码管理局组织制定并提出的椭圆曲线密码算法标准。GB/T 32918 的主要目标如下：

——GB/T 32918.1—2016 定义和描述了 SM2 椭圆曲线密码算法的相关概念及数学基础知识，并概述了该部分同其他部分的关系。

——GB/T 32918.2—2016 描述了一种基于椭圆曲线的签名算法，即 SM2 签名算法。

——GB/T 32918.3—2016 描述了一种基于椭圆曲线的密钥交换协议，即 SM2 密钥交换协议。

——GB/T 32918.4—2016 描述了一种基于椭圆曲线的公钥加密算法，即 SM2 加密算法，该算法需使用 GB/T 32905—2016 定义的 SM3 密码杂凑算法。

——GB/T 32918.5—2017 给出了 SM2 算法使用的椭圆曲线参数，以及使用椭圆曲线参数进行 SM2 运算的示例结果。

信息安全技术
SM2 椭圆曲线公钥密码算法
第 5 部分:参数定义

1 范围

GB/T 32918 的本部分规定了 SM2 椭圆曲线公钥密码算法的曲线参数。

本部分适用于数字签名与验证(参见附录 A)、密钥交换与验证(参见附录 B)、消息加解密示例(参见附录 C)。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分:总则

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分:密钥交换协议

GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法

3 符号

下列符号适用于本文件。

p 大于 3 的素数。

a,b F_q 中的元素,它们定义 F_q 上的一条椭圆曲线 E。

n 基点 G 的阶[n 是 $\sharp\ E(F_q)$ 的素因子]。

x_G 生成元的 x 坐标

y_G 生成元的 y 坐标

4 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