ICS 35.040
L 80
备案号:55617—2016

GM

中华人民共和国密码行业标准

GM/T 0044.5—2016

SM9 标识密码算法
第 5 部分:参数定义

**Identity-based cryptographic algorithms SM9—
Part 5:Parameter definition**

2016-03-28 发布　　2016-03-28 实施

国家密码管理局　　发 布

目　　次

前　言

GM/T 0044《SM9 标识密码算法》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：密钥封装机制和公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0044 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。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：国家信息安全工程技术研究中心。

本部分主要起草人：陈晓、马宁、张青坡、袁文恭、刘平、李增欣、王学进、杨恒亮、熊荣华、马艳丽、浦雨三、唐英、孙移盛、安萱。

SM9 标识密码算法
第 5 部分:参数定义

1 范围

GM/T 0044 的本部分规定了 SM9 标识密码算法的曲线参数,并给出了数字签名算法、密钥交换协议、密钥封装机制、公钥加密算法示例。

本部分适用于 SM9 算法实现中每个步骤运算正确性的验证。

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。

GM/T 0004—2012 SM3 密码杂凑算法

GM/T 0002—2012 SM4 分组密码算法

GM/T 0044.1—2016 SM9 标识密码算法 第 1 部分:总则

GM/T 0044.2—2016 SM9 标识密码算法 第 2 部分:数字签名算法

GM/T 0044.3—2016 SM9 标识密码算法 第 3 部分:密钥交换协议

GM/T 0044.4—2016 SM9 标识密码算法 第 4 部分:密钥封装机制和公钥加密算法

3 参数定义

3.1 系统参数

本部分使用 256 位的 BN 曲线。

椭圆曲线方程:$y^2=x^3+b$。

曲线参数:

参数 t :60000000 0058F98A

迹 $\mathrm{tr}(t)=6t^2+1$:D8000000 019062ED 0000B98B 0CB27659

基域特征 $q(t)=36t^4+36t^3+24t^2+6t+1$:

B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

方程参数 b:05

群的阶 $N(t)=36t^4+36t^3+18t^2+6t+1$:

B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

余因子 cf:1

嵌入次数 k:12

扭曲线的参数 β:$\sqrt{-2}$

k 的因子 $d_1=1, d_2=2$

曲线识别符 cid:0x12

群 G_1 的生成元 $P_1=(x_{P1}, y_{P1})$: