



# 中华人民共和国国家标准

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

Information security technology—Public key cryptographic algorithm SM2  
based on elliptic curves—Part 2: Digital signature algorithm

2016-08-29 发布

2017-03-01 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 .....	I
引言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号和缩略语 .....	1
5 数字签名算法 .....	2
5.1 综述 .....	2
5.2 椭圆曲线系统参数 .....	2
5.3 用户密钥对 .....	2
5.4 辅助函数 .....	3
5.5 用户其他信息 .....	3
6 数字签名的生成算法及流程 .....	3
6.1 数字签名的生成算法 .....	3
6.2 数字签名生成算法流程 .....	3
7 数字签名的验证算法及流程 .....	4
7.1 数字签名的验证算法 .....	4
7.2 数字签名验证算法流程 .....	5
附录 A (资料性附录) 数字签名与验证示例 .....	7
A.1 综述 .....	7
A.2 $F_p$ 上的椭圆曲线数字签名 .....	7
A.3 $F_{2^m}$ 上的椭圆曲线数字签名 .....	8
参考文献 .....	10

## 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 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

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 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 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 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 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 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。

本部分为 GB/T 32918 的第 2 部分，描述了基于椭圆曲线的数字签名算法。

# 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

## 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数字签名算法,包括数字签名生成算法和验证算法,并给出了数字签名与验证示例及其相应的流程。

本部分适用于商用密码应用中的数字签名和验证,可满足多种密码应用中的身份鉴别和数据完整性、真实性的安全需求。

## 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 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 32905—2016 信息安全技术 SM3 密码杂凑算法

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**消息 message**

任意有限长度的比特串。

### 3.2

**签名消息 signed message**

由消息以及该消息的签名部分所组成的一组数据项。

### 3.3

**签名密钥 signature key**

在数字签名生成过程中由签名者专用的秘密数据项,即签名者的私钥。

### 3.4

**签名生成过程 signature generation process**

输入消息、签名密钥和椭圆曲线系统参数,并输出数字签名的过程。

### 3.5

**可辨别标识 distinguishing identifier**

可以无歧义辨别某一实体身份的信息。

## 4 符号和缩略语

下列符号和缩略语适用于本文件。

A, B 使用公钥密码系统的两个用户。