



# 中华人民共和国国家标准

GB/T 38647.2—2020

---

## 信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制

Information technology—Security techniques—Anonymous digital signatures—  
Part 2: Mechanisms using a group public key

(ISO/IEC 20008-2:2013, MOD)

2020-04-28 发布

2020-11-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会

# 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 .....	2
5 一般模型和要求 .....	3
6 具有连接能力的机制 .....	4
6.1 概述 .....	4
6.2 机制 1 .....	4
6.3 机制 2 .....	8
6.4 机制 3 .....	13
6.5 机制 4 .....	16
7 具有打开功能的机制 .....	19
7.1 概述 .....	19
7.2 机制 5 .....	19
7.3 机制 6 .....	22
8 具有打开和连接功能的机制 .....	24
8.1 概述 .....	24
8.2 机制 7 .....	24
8.3 机制 8 .....	28
附录 A (规范性附录) 对象标识符 .....	33
附录 B (规范性附录) 密码杂凑函数 .....	35
附录 C (资料性附录) 采用群组公钥的匿名签名机制的安全指南 .....	37
附录 D (资料性附录) 撤销机制的比较 .....	40
附录 E (资料性附录) 数值实例 .....	43
附录 F (资料性附录) 机制 5 的正确性证明 .....	95
参考文献 .....	99

## 前 言

GB/T 38647《信息技术 安全技术 匿名数字签名》拟分为两个部分：

——第 1 部分：总则；

——第 2 部分：采用群组公钥的机制。

本部分为 GB/T 38647 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用 ISO/IEC 20008-2:2013《信息技术 安全技术 匿名数字签名 第 2 部分：采用群组公钥的机制》。

本部分与 ISO/IEC 20008-2:2013 的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 删除了 ISO/IEC 18031 和 ISO/IEC 18032；
- 增加了 GB/T 32905、GB/T 32918.2—2016、GB/T 34953.2—2018 和 ISO/IEC 15946-1；
- 用修改采用国际标准的 GB/T 38647.1 代替了 ISO/IEC 20008-1。

——第 5 章采用了我国密码算法国家标准 GB/T 32905，以与我国技术水平相适应。

——第 8 章增加了机制 8(见 8.3)，该机制基于 GB/T 32918.2—2016，是与我国商用密码算法相适应的匿名数字签名技术。

——增加了与机制 8 的数学假设和安全参数选取相关的内容(见附录 C)。

——增加了与机制 8 的撤销机制相关的内容(见附录 D)。

——增加了 E.8，给出了机制 8 的数值实例(见附录 E)。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、中关村无线网络安全产业联盟、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、国家信息技术安全研究中心、中国通用技术研究院、中国电子技术标准化研究院、天津市电子机电产品检测中心、重庆邮电大学、北京计算机技术及应用研究所、工业和信息化部宽带无线 IP 标准工作组。

本部分主要起草人：杜志强、曹军、张国强、李琴、李志勇、李冬、赵晓荣、黄振海、李冰、陶洪波、刘科伟、颜湘、刘景莉、赵旭东、王月辉、张璐璐、吕春梅、许玉娜、傅强、龙昭华、彭潇、熊克琦、林德欣、铁满霞、吴冬宇、郑骊、高德龙、张变玲、于光明、朱正美、赵慧、黄奎刚。