ICS 35.040
L 80

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
国家标准化管理委员会　发布

目　　次

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。