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。

引　言

匿名数字签名机制是一种特殊类型的数字签名机制，该类数字签名机制中，非授权的实体不能获得签名方的身份标识，但可验证合法的签名方产生了合法的签名。

采用群组公钥的匿名数字签名机制具有提供签名方更多信息的能力。一些签名机制拥有连接能力，其中由同一个签名方产生的两个签名是可连接的。一些签名机制拥有打开能力，其中签名可以被特殊的实体打开来揭露签名方的身份。一些签名机制既具有连接能力也具有打开能力。

对于每个机制，本部分规定了打开、连接和/或撤销过程。

本部分规定的机制使用了 GB/T 32905 中规范的抗碰撞密码杂凑函数去计算整个消息。

本文件的发布机构提请注意，声明符合本文件时，可能涉及与 8.3 相关的 CN201810207503.4、CN201810207564.0、CN201810207571.0 等专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利持有人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

本文件的发布机构提请注意，本文件修改采用 ISO/IEC 20008-2:2013，因此，除上述声明外，韩国电子通信研究院、英特尔公司以及日本 NEC 公司针对 ISO/IEC 20008-2:2013 所作出的“专利持有人愿意基于无歧视、合理条件和条款与其他方协商许可”的声明适用于本文件。相关信息可通过以下联系方式获得：

专利持有人：Electronics and Telecommunications Research Institute

地址：161，Gajeong-dong，Yuseong-gu，Daejeon，305-700，KOREA

联系人：Hanchul Shin

电子邮件：vip123@etri.ke.kr

电话：+82-042-860-5797

传真：+82-042-860-3831

网址：http://www.etri.re.kr

专利持有人：Intel Corporation

地址：Intel Legal and Corporation Affairs 2200 Mission College Blvd.，RNB-150，Santa Clara，CA 95054

联系人：James Kovacs

电子邮件：Standards.Licensing@intel.com

电话：408-765-1170

传真:408-613-7292
网址:http://www.intel.com/standards/licensing.html

专利持有人:NEC Corporation
地址:7-1 Shiba 5-chome Minato-Ku TokyoJapan 108-8001 Japan
联系人:Yoshinobu Matsumoto
电子邮件:y-matsumoto@cp.jp.nec.com
电话:+81-3-3798-2452
传真:+81-3-3798-6394
网址:http://www.nec.com/

请注意除上述专利外,本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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

1　范围

GB/T 38647的本部分规定了采用群组公钥的匿名数字签名机制的一般模型和要求、具有连接能力的机制、具有打开功能的机制、具有打开和连接功能的机制。

本部分给出了:

a)　采用群组公钥签名的匿名数字签名机制的概述;

b)　多种提供这类匿名数字签名的机制。

对于每个机制,本部分规定了:

a)　群组成员签名密钥和群组公钥的生成过程;

b)　生成签名的过程;

c)　验证签名的过程;

d)　群组成员打开过程(可选);

e)　群组签名连接过程(可选);

f)　撤销群组签名的过程。

本部分适用于指导采用群组公钥的匿名数字签名机制的设计、实现与应用。

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　信息安全技术　SM3密码杂凑算法

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 34953.2—2018　信息技术　安全技术　匿名实体鉴别　第2部分:基于群组公钥签名的机制(ISO/IEC 20009-2:2013,IDT)

GB/T 38647.1　信息技术　安全技术　匿名数字签名　第1部分:总则(GB/T 38647.1—2020,ISO/IEC 20008-1:2013,MOD)

ISO/IEC 10118(所有部分)　信息技术　安全技术　杂凑函数(Information technology—Security techniques—Hash-functions)

ISO/IEC 15946-1　信息技术　安全技术　基于椭圆曲线的密码技术　第1部分:通用要求(Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 1:General)

ISO/IEC 15946-5　信息技术　安全技术　基于椭圆曲线的密码技术　第5部分:椭圆曲线生成(Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 5:Elliptic curve generation)

3　术语和定义

GB/T 38647.1界定的以及下列术语和定义适用于本文件。