ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38647.1—2020

信息技术　安全技术　匿名数字签名　第1部分：总则

Information technology—Security techniques—Anonymous digital signatures—Part 1：General

（ISO/IEC 20008-1：2013，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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号 …… 7
5　群组公钥和多公钥的选择 …… 7
6　总体要求 …… 10
7　采用群组公钥的机制 …… 11
7.1　一般模型 …… 11
7.2　实体 …… 11
7.3　密钥生成过程 …… 12
7.4　群组签名过程 …… 13
7.5　群组签名验证过程 …… 13
7.6　群组成员打开过程 …… 13
7.7　群组签名连接过程 …… 14
7.8　群组签名撤销过程 …… 14
8　采用多公钥的机制 …… 17
8.1　一般模型 …… 17
8.2　实体 …… 17
8.3　密钥产生过程 …… 17
8.4　环签名过程 …… 17
8.5　环签名验证过程 …… 17
参考文献 …… 18

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1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 20008-1：2013《信息技术　安全技术　匿名数字签名　第1部分：总则》。

本部分与ISO/IEC 20008-1：2013相比结构上有调整，增加了第2章，其他条编号依次修改。

本部分与ISO/IEC 20008-1：2013相比存在技术性差异，这些差异涉及的条款已通过在其外侧页边空白位置的垂直单线(|)进行了标示，具体技术性差异及其原因如下：

——增加了第2章规范性引用文件(见第2章)；

——删除了缩略语“DAA”和“TPM”，与我国技术水平相适应(见ISO/IEC 20008-1：2013的第3章)；

——第6章第4段段尾增加了不同类型的数字签名技术所支撑的不同类型的实体鉴别机制，并给出了规范这些实体鉴别机制的国家标准(见第6章)。

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、天津市无线电监测站、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、李琴、黄振海、颜湘、曹军、刘科伟、赵晓荣、张国强、李志勇、李冬、陶洪波、刘景莉、赵旭东、李冰、许玉娜、傅强、龙昭华、彭潇、熊克琦、铁满霞、方华、林德欣、黄奎刚、于光明、吴冬宇、高德龙、张变玲、朱正美、王月辉、赵慧。

引　言

GB/T 38647 规定的机制使用了各种标准规定的密码算法，例如：

a) 可以使用抗碰撞密码杂凑函数来对已签名消息进行密码杂凑运算并计算签名；

b) 需要证书验证公钥时，可以使用传统的数字签名机制；

c) 如果实体在执行该机制时需要数据通信作为其机制的一部分被鉴别，可能需要使用传统的实体鉴别机制；

d) 如果在匿名数字签名的机制中某些实体的信息需要被加密，可能需要使用传统的非对称加密机制来实现保护隐私和保密。

匿名数字签名机制可用于提供诸如实体鉴别、数据源鉴别、抗抵赖性和数据完整性服务。数字签名机制可以使私钥的拥有者(或持有人)单独或共同生成数字签名消息。其对应的验证密钥(或多个密钥)可以被用于验证该消息的签名有效性。数字签名机制满足：

a) 攻击者需要拥有下列的一项或两项：

1) 验证密钥而不是签名密钥；

2) 攻击者适应性选择的一系列消息的签名集合。

b) 在以下情形下攻击者在计算上是不可行的：

1) 产生对新消息的有效的签名；

2) 恢复签名密钥；

3) 在某些情况下，在之前已签消息上产生不同的有效的签名。

匿名数字签名是一种特殊类型的数字签名机制。在匿名数字签名机制里，给定数字签名，一个包括验证方在内的未经授权的实体不能恢复签名方的标识或身份。然而，这样的机制仍然具有只有合法签名方能够产生有效签名的特性。对于参与匿名签名机制的授权实体，有四种不同的情况：

a) 授权的实体能够验证签名方的签名的机制；

b) 授权的实体只能具有连接同一个签名方创建的两个签名的能力但不能验证签名方身份的机制；

c) 包含两个授权实体并符合前两种情况的机制；

d) 包含两个授权实体并不符合前两种情况的机制。

匿名数字签名的示例应用是实现匿名的实体鉴别。GB/T 34953.2 中规定了匿名实体鉴别机制。

不同于传统的数字签名机制，匿名数字签名机制是基于非对称密码技术，并且涉及三个基本操作：

a) 生成签名密钥和验证密钥的过程；

b) 使用签名密钥创建匿名数字签名的过程；

c) 使用验证密钥验证匿名数字签名的过程。

传统的数字签名和匿名数字签名之间的主要差异之一就是利用公钥进行签名验证的方法。要验证一个传统的数字签名，验证者利用绑定签名方身份的验证密钥，验证匿名数字签名时，验证方使用的任一群组公钥或多公钥，它们不绑定于单个签名方。采用群组公钥的匿名签名通常被称为群组签名，而采用多公钥的匿名签名通常被称为环签名。匿名签名机制提供的匿名强度(即不愿透露姓名的程度)取决于群组的大小和公钥的数量。

在使用群组公钥的匿名数字签名的机制中，可以对一个实体或一群组实体进行三个不同授权级别

的撤销，包括以下三种可能：

a） 整组撤销，即整个群组被撤销。

b） 撤销某一群组成员的成员资格。其结果是已撤销的成员不能再授权代表群组去创建群签名；

c） 签名验证方可以撤销群组成员创建的某种匿名签名类型的权限。经过这种撤销后，已被申请撤销的成员仍能够代表群组去创建其他匿名签名。

信息技术　安全技术　匿名数字签名
第1部分:总则

1　范围

GB/T 38647的本部分规定了匿名签名机制的定义、选择和总体要求,以及以下两种匿名签名机制的通用模型、实体集和部分流程:

a)　采用群组公钥的签名机制;

b)　采用多公钥的签名机制。

本部分适用于指导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 15843(所有部分)　信息技术　安全技术　实体鉴别

GB/T 34953.2　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

GB/T 38647.2　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

3　术语和定义

下列术语和定义适用于本文件。

3.1

匿名数字签名　anonymous digital signature

可以使用一个群组公钥或多个公钥进行验证的签名,未经授权的实体不能通过该签名(包括签名的验证方)追踪到签名方的可区分标识符。

注:匿名数字签名也可称为匿名签名或简称为数字签名或签名。

3.2

匿名强度　anonymity strength

由未经授权的实体可以从给定签名来确定真实签名方的概率导出的数字。

注:匿名强度为 n 意味着未经授权的实体可以以 $1/n$ 的概率从一个签名正确猜测真实签名方。

3.3

抗碰撞密码杂凑函数　collision-resistant hash-function

满足下列特性的密码杂凑函数:找到可以映射到同一个输出的任意两个不同的输入在计算上是不可行的。

注:计算上的可行性取决于特定的安全需求和环境。

3.4

数据元素　data element

整数、比特串、整数的集合或比特串的集合。