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

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。

3.5

可区分标识符 distinguishing identifier

用来明确区分实体的信息。

3.6

域 domain

在单一安全策略下操作的实体的集合。

示例：由单一机构或使用同一安全策略的一组机构创建的公钥证书。

3.7

域参数 domain parameter

域内所有实体通用的、已知的和可访问的数据元素。

3.8

绑定证据 evidence of binding

用来呈现证明签名方和签名之间密码绑定的数据元素，它是群组成员打开过程的输出。

3.9

证据评估过程 evidence evaluation process

输入绑定证据、群组签名和群组公钥，输出证据评估结果(有效的或无效的)的过程。

注：输入到证据评估过程中的群组签名是有效的，已被群组签名验证过程成功验证过。

3.10

证据评估方 evidence evaluator

检查绑定证据有效性的实体。

3.11

群组 group

在单一成员管理策略下操作的实体集合。

注：一个群组包括多个群组成员，每个群组成员都有一个成员证书，该证书是在群组成员发布过程中由群组成员发布方创建的。

3.12

群组成员 group member

拥有群组成员证书并能代表群组创建群组签名的实体。

3.13

群组成员私钥 group member private key

作为群组成员签名密钥一部分的私有数据元素，该元素特定于群组成员并且只能在群组成员发布过程和群组签名过程中使用。

3.14

群组成员签名密钥 group member signature key

规定了群组成员的数据元素的集合，包含群组成员私钥和群组成员证书，仅由群组成员在群组签名过程中使用。

3.15

群组成员证书 group membership credential

特定于群组成员的数据元素，通过使用群组成员发布密钥而具有不可伪造性，由群组成员在群组签名过程使用。

注 1：群组成员证书也称群组证书。

注 2：群组成员证书是群组成员签名密钥的一部分。

3.16

群组成员发布方 group membership issuer

创建群组成员证书的实体。

注：群组成员发布方也称群组发布方或发布方。

3.17

群组成员发布密钥 group membership issuing key

群组成员发布方专有的私有数据元素，并且在群组发布过程中只能够由发布方使用。

注：群组成员发布密钥也称为群组发布密钥或发布密钥。

3.18

群组成员发布过程 group membership issuing process

输入群组成员发布密钥、群组公钥、群组公共参数和可区分标识符(可选的)同时输出群组成员签名密钥的过程。

注1：群组成员发布过程也称发布过程。

注2：群组成员发布过程在文献中也被称为群组成员加入过程或简称为加入过程。

3.19

全局撤销 global revocation

群组签名撤销过程，通过更新群组公钥、其他的群组公共参数和/或群组中使用的撤销列表，使某些之前合法的群组成员变为非法，达到撤销签名密钥的效果。

注1：使用全局撤销的撤销列表也称为群组全局撤销列表。

注2：群组成员签名密钥可以在全局撤销列表中被更新。

3.20

群组成员打开方 group membership opener

从一个群组签名来确定签名方标识的实体。

注：群组成员打开方也称为群组打开方或打开方。

3.21

群组成员打开密钥 group membership opening key

特定于群组成员打开方的私有数据元素，并且只由打开方在群组成员打开过程中使用。

注：群组成员打开密钥也称为群组打开密钥或打开密钥。

3.22

群组成员打开过程 group membership opening process

输入群组签名、群组成员打开密钥、群组公钥和群组公共参数同时输出签名方可区分标识符的过程，可选的还可以输出签名方和签名之间绑定的证据。

注1：群组成员打开过程也叫打开过程。

注2：需要打开过程中输入有效的群组签名，这意味着该签名已经通过群组签名验证过程被成功验证。

3.23

群组公钥 group public key

与群组成员发布密钥数学上相关的公共数据元素，它涉及群组成员发布过程、群组签名过程、群组签名验证过程和采用群组公钥的匿名签名机制的其他过程(可选)。

注：在一些启用撤销功能的机制里群组公钥可能要被更新。

3.24

群组公共参数 group public parameter

特定于群组并且可以被群组内所有实体访问的数据元素，它涉及采用群组公钥的匿名签名机制的所有过程。

3.25

群组签名 group signature

群组签名过程产生的数据元素。

3.26

群组签名连接方 group signature linker

确定两个匿名签名是否连接的实体，即它们是否由同一个签名方创建。

注 1：群组签名连接方也称连接方。

注 2：根据该机制，连接方可能拥有也可能不拥有连接密钥。

3.27

群组签名连接基 group signature linking base

特定于群组签名连接方的公共数据元素(可选的)，如果需要使用这个数据元素去连接由同一个签名方创建的多个签名，则该数据元素将参与群组签名的过程。

注 1：群组签名连接基也称连接基。

注 2：连接基有时在文献中称为基。连接基用于 GB/T 38647.2 中规范的直接匿名验证技术。

3.28

群组签名连接密钥 group signature linking key

特定于群组签名连接方的私有数据元素并且只能由连接方在群组签名连接过程使用。

注：群组签名连接密钥也称连接密钥。

3.29

群组签名连接过程 group signature linking process

输入两个匿名签名、群组公共参数和群组签名连接密钥(可选的)并且输出签名连接结果(连接或不连接)的过程。

注 1：群组签名连接过程也叫连接过程。

注 2：在一些标准中，例如 GB/T 38647.2，使用群组签名连接密钥的连接过程提供了本地连接能力。

注 3：在同一个签名密钥下创建的不同的签名是连接的；在两个不同的签名密钥下创建的不同签名是不连接的，未使用同一连接过程需要的参数创建的两个的签名也是不连接的，例如，它们是由两个不同的群组签名连接基创建的。

3.30

群组签名过程 group signature process

输入消息、群组成员签名密钥、群组公钥、群组公共参数和连接基(可选的)并且输出群组签名的过程。

注：群组签名过程也称为签名过程。

3.31

群组签名验证过程 group signature verification process

输入群组签名消息、群组公钥和群组公共参数同时输出群组签名验证结果(有效或无效)的过程。

注：群组签名验证过程也称为验证过程。

3.32

群组签名撤销列表 group signature revocation list

可以用来识别由未授权的群组成员所创建匿名签名的签名方身份的数据元素。

注 1：群组签名撤销列表包括内容类型的范围、撤销的群组成员私钥、撤销的群组成员证书的组件和之前创建的部分或全部的签名。

注 2：根据该机制，群组签名撤销列表可以作为群组公钥撤销列表、群组全局撤销列表或验证方局部撤销列表。

3.33

群组签名撤销过程 group signature revocation process

撤销授权群组成员创建特定类型群组签名的过程。

注：群组签名撤销过程包括整个群组的撤销、群组等级的全局撤销或群组签名验证方的局部撤销。

3.34

群组签名消息 group signed message

签名本身是群组签名并且可选的包含连接基的签名消息。

3.35

杂凑码 hash-code

密码杂凑函数输出的比特串。

注：关于该术语的文献包含了与密码杂凑代码具有相同或相似含义的各种术语。例如，修改检测代码、操作检测代码、摘要、密码杂凑结果、密码杂凑值和版权标记。

3.36

杂凑函数 hash-function

将比特串映射为固定长度的比特串的函数，该函数满足下列两个特性：

a) 对于给定输出，找到映射为该输出的输入，在计算上是不可行的；

b) 对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

3.37

密钥 key

控制密码变换操作的符号序列。

注：操作的实例包括加密、解密、密码校验函数计算、签名生成或签名验证。

3.38

局部撤销 local revocation

使签名验证方根据群组签名撤销列表拒绝无效群组签名的群组签名撤销过程。

注 1：本地撤销过程中使用的群组签名撤销列表可以由验证方本身或者由其他资源(例如，它可能是验证方采用的群组全局撤销列表的一部分)生成。

注 2：在本地撤销过程中使用的群组签名撤销列表也称为验证方本地撤销列表。

3.39

消息 message

任意长度的比特串。

3.40

参数 parameter

整数、比特串或函数。

3.41

潜在签名方 potential signer

在环签名过程中公钥被真实的签名方使用的实体。

3.42

环 ring

由真实签名方和潜在签名方(或签名方)组成的实体集合。

3.43

环公共参数 ring public parameter

特定于环的数据元素，可供采用多公钥的匿名签名机制所有过程中涉及的所有实体访问。

3.44

环签名 ring signature

环签名过程产生的数据元素。

3.45

环签名过程 ring signature process

输入消息、真实签名方的签名密钥、潜在签名方的公钥以及环公共参数，输出环签名的过程。

3.46

环签名验证过程 ring signature verification process

输入环签名消息、真实签名方的公钥、潜在签名方以及环公共参数，输出环签名验证结果为有效或无效的过程。

3.47

环签名消息 ring singed message

采用环签名产生的签名消息。

3.48

安全强度 security strength

衡量破解密码算法或系统所需工作量(运算的数量)的数字。

注：安全强度用比特来表示。安全强度为 b 比特意味着破解系统需要阶为 2^b 的运算。安全强度的常用值为 80 比特、112 比特、128 比特、192 比特和 256 比特。

3.49

签名 signature

签名生成过程产生的一个或多个数据元素。

注：签名也称为数字签名。

3.50

签名密钥 signature key

特定于一个实体的一套私有数据元素，仅由该实体在签名过程使用。

注：签名密钥有时也称为个人签名密钥。在 GB/T 38647 和其他标准如 ISO/IEC 9796-2 和 GB/T 15851.3—2018 中两者存在的意义相同。

3.51

签名密钥对 signature key pair

由一个签名密钥和一个验证密钥组成的密钥对，其中：

a) 签名密钥应该部分或完全保密，并且只能由签名方使用；

b) 验证密钥可以是公开的，并且可以由任意验证方使用。

3.52

签名过程 signature process

输入消息、签名密钥和域参数，输出签名的过程。

3.53

签名消息 signed message

由签名、不能由签名来恢复的部分消息和可选文本字段组成的数据元素集合。

3.54

签名方 signer

生成数字签名的实体。

3.55

真实签名方 true signer

代表环创建环签名的实体。

注：真实签名方也叫签名方。

3.56

验证密钥 verification key

与实体签名密钥数学上相关的公共数据元素集合并且由验证方在验证过程中使用。

注：验证密钥有时也被称为公共验证密钥，在 GB/T 38647 和其他标准如 ISO/IEC 9796-2 和 GB/T 15851.3—2018 中两者存在的意义相同。

3.57

验证过程 verification process

输入签名消息、验证密钥和域参数，输出签名验证结果(有效或无效)的过程。

3.58

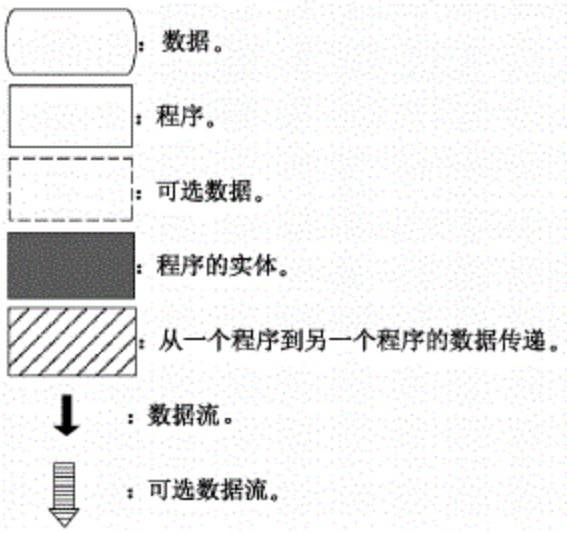
验证方 verifier

检查签名有效性的实体。

注：验证方也称为签名验证方。

4 符号

下列符号适用于本文件。



5 群组公钥和多公钥的选择

在传统数字签名机制中，如图 1 所示，一个签名私钥和一个验证公钥形成签名密钥对。在签名过程中，签名方使用签名私钥去创建给定消息的签名。在验证过程中，验证方使用公开验证密钥去验证这个签名是否为对应的私钥签署的。如果验证方确认签名确实是对应于验证密钥的签名密钥创建的，则验证方输出：有效；否则输出：无效。因此，从验证方角度来看，签名是通过验证公钥与签名方绑定的，验证公钥作为签名方的可区分标识符。

在匿名数字签名机制中，一个签名密钥和一个验证密钥形成签名密钥对，其中一个用在签名过程而另一个用在验证过程的方式并不是必要的。在本部分中规定了两类采用不同验证密钥的匿名签名机制的原则和要求，一类是采用群组公钥的机制，另一类是采用多公钥的机制。

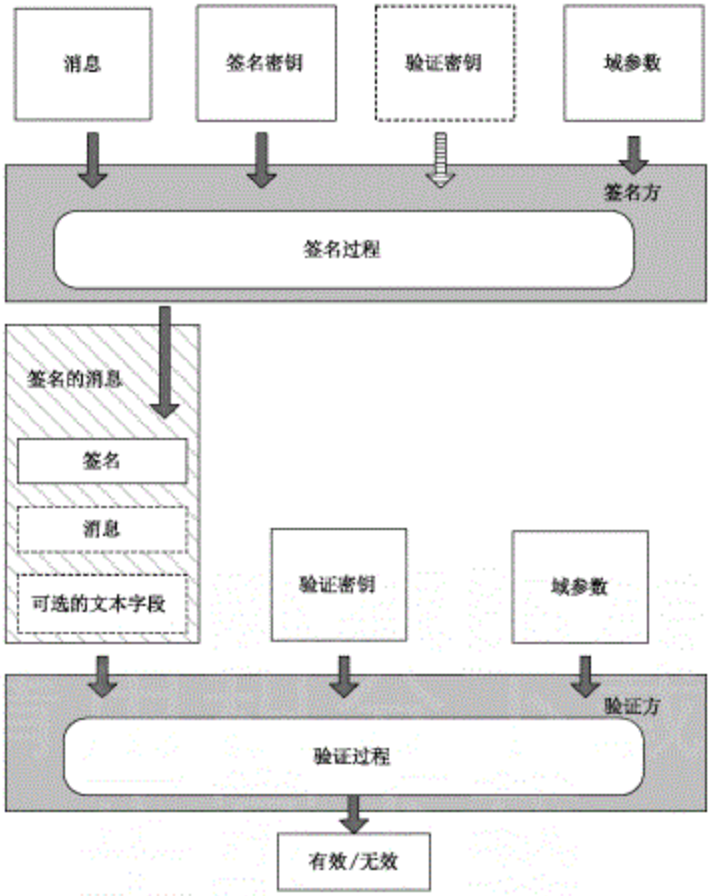


图 1　传统签名机制中的签名和验证过程

在采用群组公钥的匿名签名机制中，如图 2 所示，签名方是一个群组成员。该群组只有一个群组公钥。每个群组成员都有由群组成员的私钥和相应的成员证书组成的唯一的群组成员签名密钥。签名过程中，签名方使用群组成员签名密钥对给定的消息创建群组签名。在验证过程中，验证方使用群组公钥来检查该签名是否为群组成员的签名密钥签署的群组签名，并且不能透露是用哪一个群组签名密钥创建的签名。如果验证方验证签名是使用对应于该群组公钥的群组成员签名密钥创建的，则验证通过；否则，验证不通过。其结果是：从验证方的角度来看，该群组签名不是绑定于单个签名方，而是通过群组公钥绑定到该群组。其匿名强度取决于该群组的大小。

注：某些机制需要将验证方生成的随机数输入到群组签名和签名验证的过程中。在图 2 中，该随机数被视为消息的一部分。

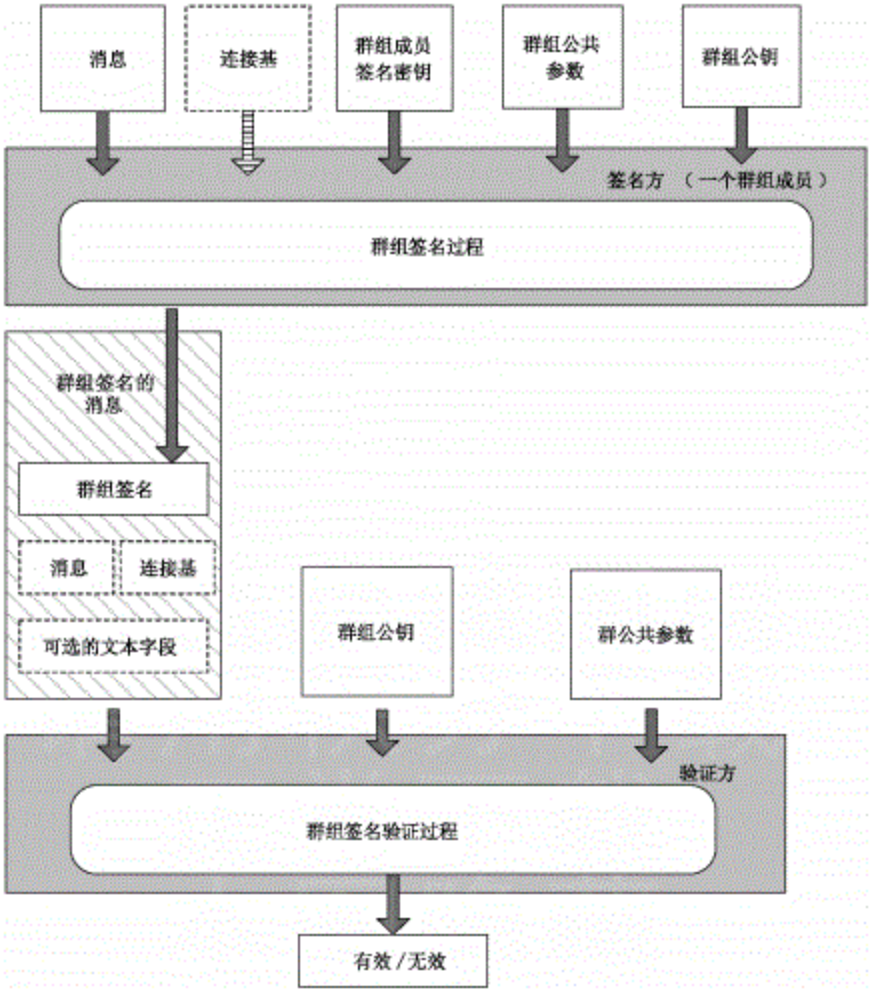


图 2　采用群组公钥的匿名签名机制中的签名和验证过程

在采用多公钥的匿名签名机制(也称为环签名机制)中,如图 3 所示,每个签名方,包括真实的签名方和每个潜在签名方,和传统的数字签名机制一样有一个签名私钥和一个验证公钥形成签名密钥对。在签名过程中,真正的签名方用其签名密钥连同公钥(或公钥集)对给定的消息创建签名,该公钥(公钥集)属于潜在的签名方(或潜在的签名方集合)。在验证过程中,验证方使用包含真实签名方和所有潜在签名方的公开密钥来检查签名是否是由公开密钥对应的签名密钥创建的,并且不透露是何人签署。其结果是:从验证方的角度来看,该签名没有绑定一个单独的签名方,而是绑定到该公钥所有者的集合。匿名强度取决于公钥的数量。

如图 1～图 3 所示,输入到签名过程的消息可以分割也可以不分割为两部分。如果分割,一部分可以从签名中恢复而另一部分不能从签名恢复。其中,包含在已签消息中的部分是那些不能从签名中恢复的消息。

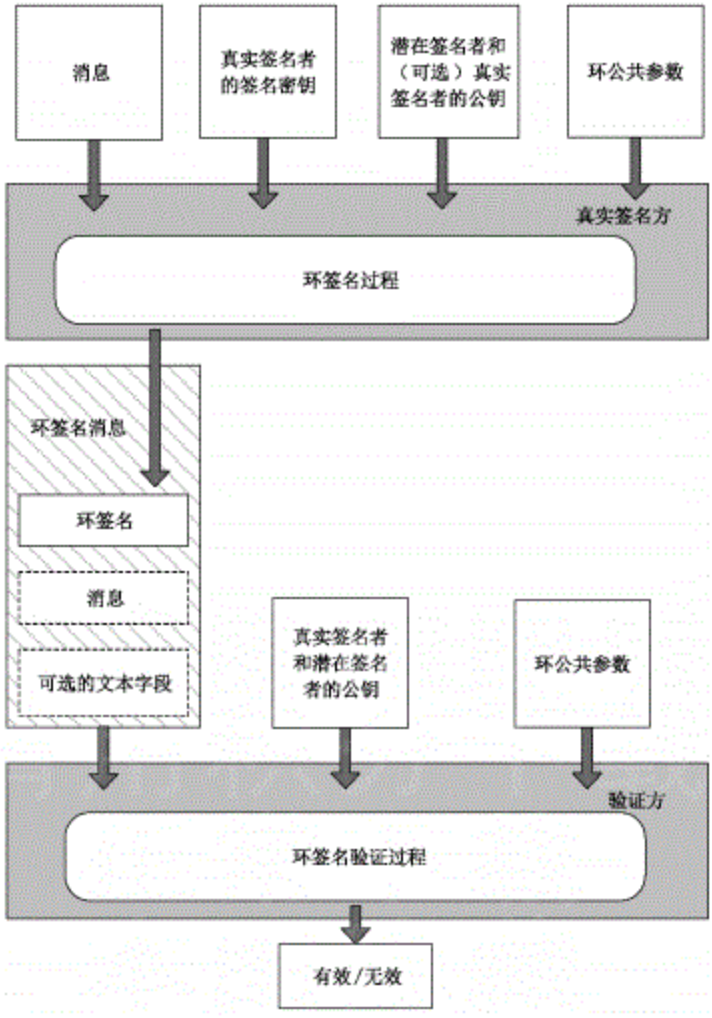


图 3　环签名机制的签名和验证过程

6　总体要求

匿名数字签名机制涉及的每一个实体应首先获取公共的域参数集，用于计算匿名签名机制中的各种函数。在采用群组公钥的匿名签名机制中，该域与一个群组相关联。其中，域参数也被称为群组公共参数。在采用多公钥的匿名签名机制中，域与环相关联，域参数（也称为环公共参数）包括所有与公钥集合及相应的签名和验证过程相关的参数。

每个签名验证方都应有权访问所需公钥的真实副本。在采用群组公钥的匿名签名机制中，该公钥属于签名方所在的群组而不是单个签名方。在采用多公钥的匿名签名机制中，这些公钥是多个单独公钥的集合。其中，每个公钥属于一个真实签名方或潜在的签名方。验证方无法区分潜在的签名方还是真实签名方。

每一个签名方都具有可区分标识符，其标识明确地绑定到签名方的私钥。执行机制的过程中，此信息应能够被相关的实体访问到。在采用多公钥的匿名签名机制中，签名方的可区分标识符可以是签名方的验证密钥。在采用群组公钥的匿名签名机制中，签名方的可区分标识符可以采用多种形式。

在采用群组公钥的匿名签名机制中，实体鉴别机制可以用于群组成员（作为签名方）和群组成员发布方以可信的方式执行的群组成员发布过程。这可确保群组成员发布方只给合法群组成员提供群组成员证书。当这个实体鉴别机制不是匿名时，使用在 GB/T 15843 中规定的机制，当该实体的鉴别机制是

匿名时，使用 GB/T 34953.2 规定的机制。

本部分不指定密钥管理机制或群组公钥和多个个人公钥的鉴别机制。有多种方法可用于获得可靠的公钥副本，例如公钥证书。密钥和证书管理的技术超出本部分的范围。

注：更多信息参见 ISO/IEC 9594-8、ISO/IEC 11770-2、ISO/IEC 11770-3 和 ISO/IEC 15945。

对于采用群组公钥的匿名签名机制，本部分没有规定群组成员发布方如何鉴别群组成员，以及在何种情况下进行群组成员的打开过程或群组签名连接过程。此外，没有规定群组成员发布方、群组成员打开方或任何其他实体如何决定一个群组成员不再被授权去创建特定类型的群组签名。然而，当使用撤销机制时，就要求每个签名验证方能够获得最新的群组公钥和任何必要的群组公共参数，且如果使用群组签名撤销列表，签名验证方有权访问它。

本部分凡涉及密码算法相关的内容，按国家有关法规实施；凡涉及采用密码技术解决机密性、完整性、真实性、抗抵赖需求的需遵循密码相关国家标准和行业标准。

7 采用群组公钥的机制

7.1 一般模型

采用群组公钥的匿名数字签名机制也被称为群组签名机制。这种类型的机制包括群组与群组成员的集合以及群组成员发布方。另外，如果需要追溯签名的签名方，群组成员打开方也是必需的。该机制的匿名强度取决于合法群组成员的数目。

根据该机制，可连接同一个签名方创建的两个签名。一个具有连接能力的实体被称为群组签名连接方；这种实体不一定是群组的成员。在一些机制中，任何人都可以是连接方；在这种情况下，连接基通常包含在一个签名里。在其他机制中，连接方应持有群组签名连接密钥；在这种情况下，对应于该连接密钥的公开参数也包含在签名里。

根据该机制，可以撤销群组成员的私钥或群组成员的证书；在以上任何一种情况下，群组成员签名密钥都将被撤销。由撤销的群组成员签名密钥创建的群组签名在群组签名验证过程中将被拒绝。

采用群组公钥的匿名数字签名机制规定了以下过程：

a) 密钥生成过程(包括群组成员发布过程)；
b) 群组签名过程；
c) 群组签名验证过程；
d) 群组签名打开过程(可选)；
e) 群组签名连接过程(可选)；
f) 群组签名撤销过程(可选)。

采用群组公钥的匿名签名机制的情况在 GB/T 38647.2 中列出。

7.2 实体

如下面列出的，在匿名签名机制中所涉及的许多类型的实体都使用一个群组公钥。某些类型的实体存在于每一个机制里，而另一些实体仅在提供可选功能的机制中涉及。

签名方：签名方是生成数字签名的一个群组成员。签名方拥有可区分标识符和群组成员签名密钥，该签名密钥由群组私钥和成员证书组成。

注：该群组成员的签名密钥有时也被称为签名方的签名密钥。

在一些机制中，签名方的角色在多个实体之间拆分。例如，在 GB/T 38647.2 中规定，在直接匿名证明(DAA)机制中，签名方角色可在可具有有限计算和存储能力的主签名方和具有更多计算能力但安全容忍性差的辅助签名方之间拆分，例如硬件签名模块，辅助签名方是具有安全性的一般的计算机平台(也称为包含嵌入式的主机)。

验证方：验证方是验证数字签名的实体。

群组成员发布方：群组成员发布方是给签名方发布群组成员证书的实体。这种实体存在于GB/T 38647.2 规定的所有机制中。

群组成员打开方：群组成员打开方是可以确定一个签名的签名方的实体。这个实体存在于GB/T 38647.2 的一些机制中。在某些特定的机制中，群组成员发布方和群组成员打开方是相同的实体。根据这种机制，群组成员打开方可输出绑定的证据，即绑定签名到签名方的可标识身份。

证据评估方：证据评估方检查绑定证据的有效性。

群组签名连接方：群组签名连接方是能够连接同一个签名方生成的两个签名的实体。这个实体存在于GB/T 38647.2 中。在某些特定的机制中，连接方也是验证方。在不同匿名签名机制中连接方的数量可能会发生变化。

7.3 密钥生成过程

密钥生成过程包括密钥生成算法，密钥生成算法用于创建该群组成员发布密钥，如果在机制中需要，还用于创建群组成员打开密钥和群组签名连接密钥(或值)。典型的密钥生成算法是输入一个取决于该机制的安全性强度的安全参数，并输出公私钥对。

密钥生成过程还包括群组成员发布过程。根据机制规定，如图 4 的群组成员发布过程可能涉及也可能不涉及一个在希望成为群组成员的用户和群组成员发布方之间的协议。

若需要上述协议，群组成员和群组成员发布方都应参与群组成员签名密钥的生成过程。在协议完成后，群组成员拥有群组成员签名密钥，该密钥由成员的群组成员私钥和成员证书组成；该群组成员发布方会知晓成员证书和相关的成员的可区分标识符。该可区分标识符的格式取决于机制，并且它可以是也可以不是群组成员发布过程的输入。

另外，群组成员发布方应单独生成群组成员签名密钥，并把它分发至群组成员。在这种情况下，群组成员的私钥和成员证书的归属是不明确的，并且成员和发布方都将拥有签名密钥的值。

注：如果群组成员发布方知道签名方的群组成员签名密钥，该群组成员发布方必须是可信任的非冒充的群组成员。否则，群组签名机制将不具备抗抵赖性。

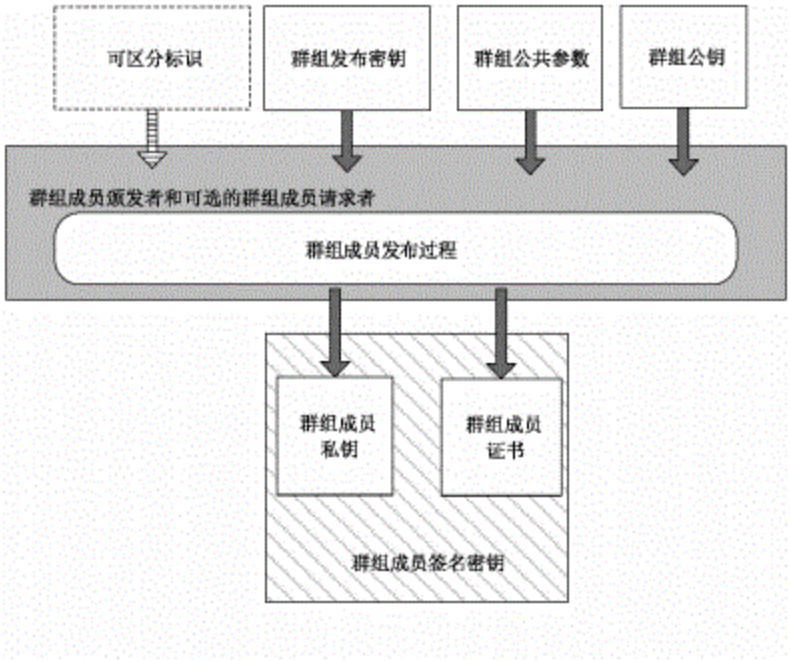


图 4 群组成员发布过程

7.4 群组签名过程

签名过程是由作为签名方的群组成员执行。签名方使用其成员签名密钥来计算给定消息的群组签名。

如果该机制支持群组成员打开，签名过程中会在签名中嵌入可区分标识符，通过这样的方式，该群组成员打开方可以恢复可区分标识符，但无法恢复其他部分。这可以通过在签名前使用群组打开方的公钥对可区分标识符进行非对称加密来实现。

如果该机制支持群组签名连接，当生成可连接的两个签名时，签名过程将使用相同的连接基或连接密钥，通过这样的方式，该群组签名的连接方用连接密钥只能连接两个签名，但无法连接其他部分。根据该机制，连接方可以是也可以不是签名的验证方。

如果机制允许签名方被撤销，签名过程应包含可确保验证方验证出签名是由一个未撤销的签名方创建的功能。

7.5 群组签名验证过程

验证过程由验证方执行，验证方能够将签名关联到正确的群组公钥，但不能从签名来确定签名方的身份。

根据机制的不同，验证过程可以独立于也可以不独于签名连接过程和/或签名的撤销过程。

7.6 群组成员打开过程

如图 5 所示，打开过程由群组成员打开方执行，使打开方确定匿名签名的签名方的可区分标识符。

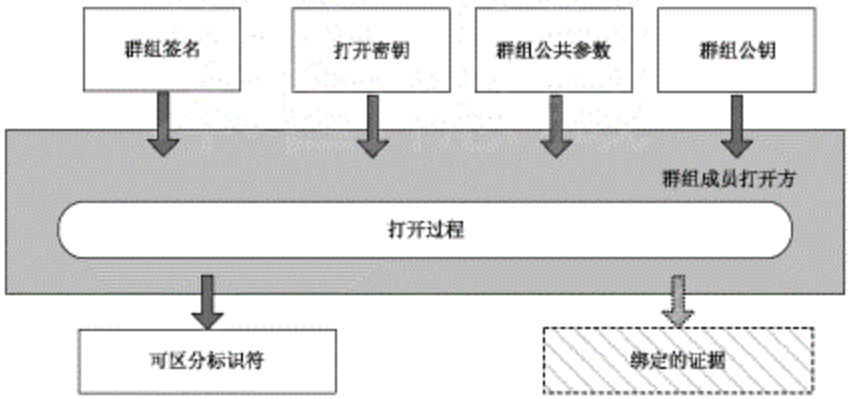


图 5 群组成员打开过程

根据机制，它可以涉及或可以不涉及一个证据评估过程。如果需要证据评估，在打开过程中群组成员打开方将创建绑定的证据，表明给定的签名与签名方的可区分标识符具有密码学绑定关系。如图 6 所示，所示证据评估过程由证据评估方执行，其中，基于绑定的证据检查打开方从给定的消息是否正确识别了签名方的身份。如果证据评估确信签名匹配绑定信息，则评估方输出有效；否则，评估方输出无效。

注：由于各种原因的存在，打开过程可以包括或不包括证据评估过程。一般来说，如果打开过程的结果需要由外部评估方验证，则采用证据评估过程。如何确定是否将证据评估过程作为打开过程的一部分，不在本部分范围之内。

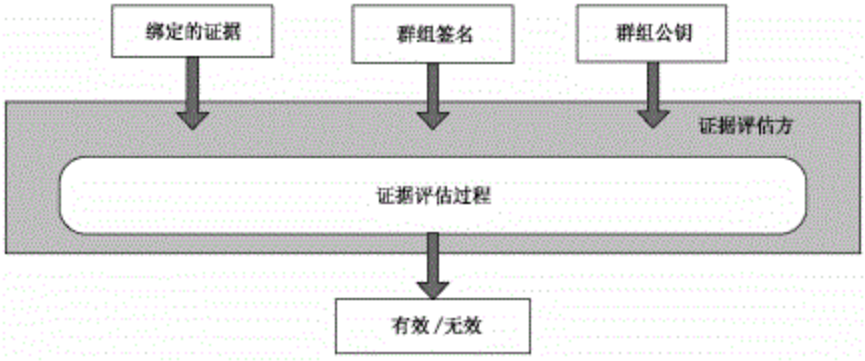


图 6　证据评估过程

7.7　群组签名连接过程

群组签名连接过程，如图 7 所示，是由群组签名连接方执行，检查给定的两个有效签名是否是由同一个签名方创建的。根据该机制，该群组签名连接方可以也可以不拥有连接密钥；同时，该群组签名连接过程可以包括也可以不包括连接基，连接基可能会也可能不会由签名连接方创建。当存在该连接基时，它一般是在群组签名过程中创建两个签名时使用。

注：具有连接过程的机制被认为拥有用户控制连接能力或可控连接能力(参见参考文献[7])。

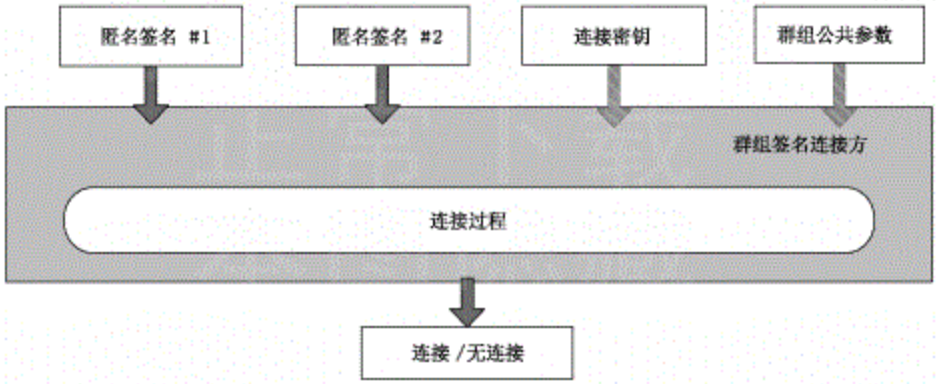


图 7　群组签名连接过程

7.8　群组签名撤销过程

7.8.1　概述

采用群组公钥的匿名数字签名机制定义了三个不同“等级”的撤销。这三个等级允许不同类型的授权被撤销。

7.8.2　1 级撤销

整个群组被撤销。如果整个群组的授权需要被撤销，相应的群组公钥应添加到群组公钥撤销列表中。任何与撤销群组公钥相关的匿名数字签名将被拒绝。这种撤销方法与使用传统的数字签名方案是相同的。

注：这种类型撤销的机制未在 GB/T 38647.2 中规定。

7.8.3　2 级撤销

撤销指定群组成员的成员资格，结果为已撤销的成员不再被授权代表群组创建群组的签名。有下列两种方法来实现：

a) 群组成员发布方更新群组公钥(这可能会也可能不会涉及更新它的私钥和/或该群组的公共参数)。发布方随后使用新的群组公钥更新所有合法签名方的证书。在后续群组签名过程、验证过程、打开过程和连接的过程中,将使用更新后的密钥和证书。根据该机制,该更新方法可以定期执行,或者群组成员发布方希望撤销群组成员的任何时候执行,或者以上两种情况同时发生时执行。

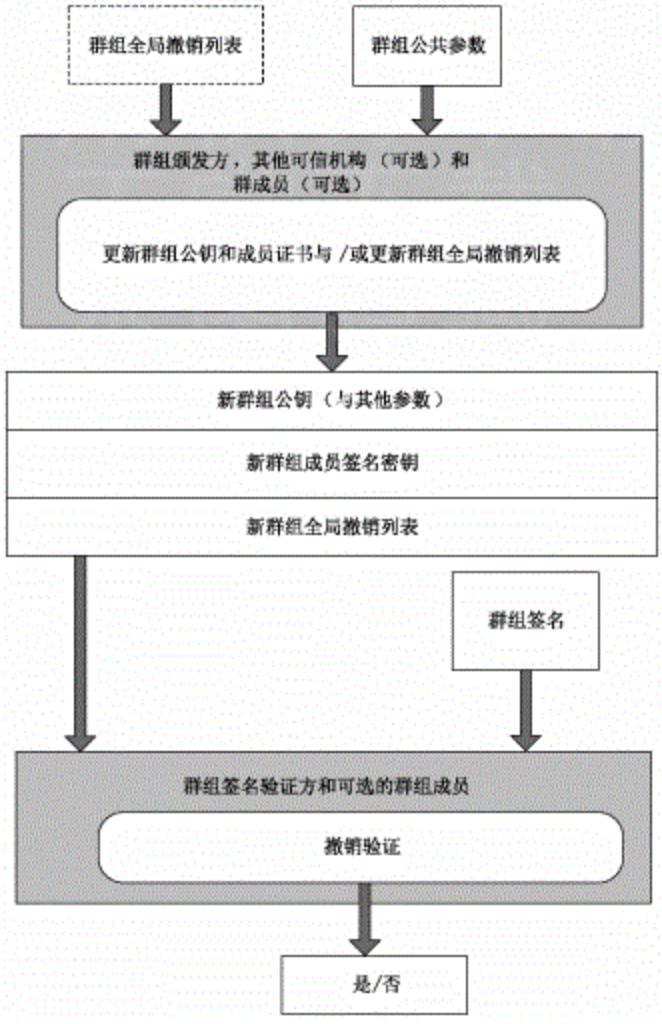
注 1:此撤销方法被称为基于密钥更新的撤销或证书更新撤销。

注 2:根据该机制,以下两个途径可作为撤销方法。第一,群组发布方与每个合法群组成员进行交互,以更新成员群组成员的签名密钥。第二,群组发布方创建特定的公共信息,然后每个合法的群组成员根据这些信息相应地更新自己的群组成员签名密钥。

b) 另一种方法是利用群组全局撤销列表。撤销列表的内容列表依赖于机制,将在下面指定一些常见的情况。一个在群组撤销列表中列出的授权相关的匿名数字签名应被群组签名验证方拒绝。

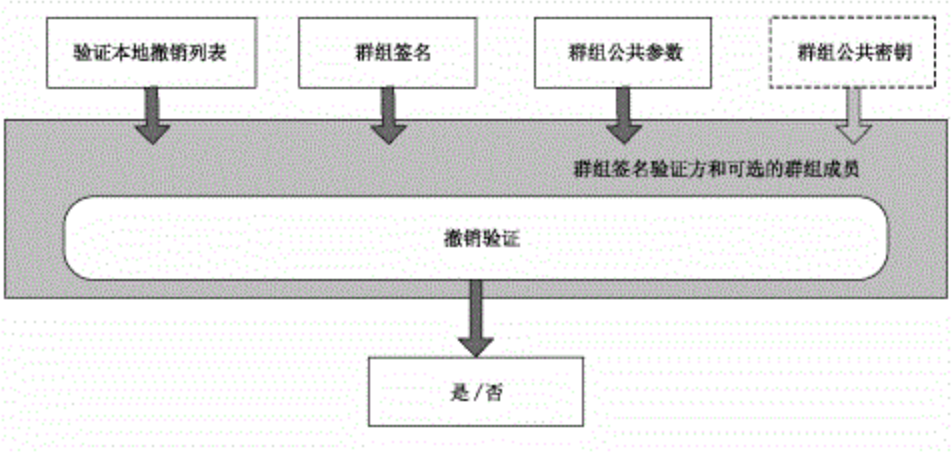
如图 8 a)所示,这个级别的撤销被称为全局撤销。一些全局撤销机制在 GB/T 38647.2 中规定。

注 3:根据该机制,这个级别中的两种撤销方法可以一起使用:例如,群组公钥和群组成员证书的信息更新可以被包括在群组全局撤销列表中。群组全局撤销列表被验证方用来更新群组公钥和/或由签名方更新其群组成员签名密钥。



a) 全局撤销

图 8 群组签名撤销过程



b) 局部撤销

图 8（续）

7.8.4 3 级撤销

群组成员授权创建的特定类型的匿名签名由签名验证方撤销。验证方可以通过利用验证方局部撤销列表来实现这个等级撤销。与验证方局部撤销列表中相关的匿名数字签名应被群组签名验证方拒绝。

这个级别的撤销，如图 8 b)所示，被称为局部撤销。一些局部撤销机制是在 GB/T 38647.2 规定的。

注 1：这种类型的撤销也被称为验证方局部撤销。

注 2：在这种类型的撤销，虽然验证方执行撤销机制，但验证方可能不知道被撤销的签名方是谁。

7.8.5 撤销列表

7.8.5.1 一般而言，撤销列表是由列表中用户都信赖的用户或者由用户自己创建。撤销列表用于识别创建已被撤销的数字签名的特定授权。使用撤销列表来检查一个签名的有效性通常是签名验证的一部分。根据撤销列表，一些撤销机制需要签名方在签名时证明其有权基于撤销列表创建签名，其他的验证机制只需要验证方在签名验证过程中检查撤销列表。根据机制的不同，撤销列表可被“压缩”为耽搁参数来实现有效性的验证。该证明不得泄露任何签名方隐私的敏感信息。

注：将撤销列表压缩为单个参数的机制也被称为累加器。

7.8.5.2 有三种类型的撤销列表分别对应三个撤销等级：

a) 群组公钥撤销列表。该名单由受信任的机构创建，并包含撤销的群组公钥。根据机制的不同，可将检查该列表可以作为采用群组公钥的每个过程的一个构成部分。

b) 群组全局撤销列表。该列表应由群组发布方或其他群组级别可信机构创建，由群组签名验证方所使用，撤销列表的内容取决于不同的机制；还包括一些特殊情况的存在，比如，私钥撤销列表、群组成员证书撤销列表以及群组签名撤销列表。

c) 验证方局部撤销列表。该列表可以由验证方自己或由其他实体创建，只能由验证方使用。该撤销列表的内容依赖于机制，一般情况下包括一个验证方黑名单撤销列表和一个群组签名撤销列表。根据不同机制，验证方可以采用全局撤销列表作为部分或全部验证方局部撤销列表。

7.8.5.3 撤销列表的内容可以有所不同，如以下示例所示：

a) 在“私钥撤销”里，撤销列表列出撤销签名方的私有签名密钥，验证方可以检查给定的签名是否由该密钥所创建。该列表可以在全局撤销中使用，也可以在局部撤销中使用。

b) 在“成员证书撤销”里，撤销列表列出撤销签名方的群组成员证书，签名方可能需要提供证明签名方的成员证书不在列表内。根据该机制，此列表可以在全局撤销中使用。

c) 在“验证方黑名单撤销”里，撤销列表包括对应于群组签名连接基的签名(或其部分签名)，并且验证方可以检查是否给定的签名是由列表中签名的签名方创建的。此列表可以在局部撤销中使用。

d) 在“签名撤销”里，签名(或其部分签名)包含在撤销列表中，验证方可以检查给定的签名是否包含在列表中，以及由签名方提供的一项由列表中的签名方所创建的证据。根据该机制，此列表可以在全局撤销中使用也可以在局部撤销中使用。

8 采用多公钥的机制

8.1 一般模型

采用多公钥的匿名签名机制也称为环签名机制。环签名机制涉及一个可能签名方的集合。每一个可能的签名方拥有和传统签名机制相同形式的签名密钥对。这些可能的签名方是彼此独立的，在某种程度上它们不需要就参与同一个签名过程达成一致。其中一方是真实的签名方，另一方(或其他的)就是潜在的签名方。真实的签名方选择潜在的签名方并且形成一个环。

环签名机制由下列过程组成：

a) 密钥产生过程；

b) 环签名过程；

c) 环签名验证过程。

8.2 实体

在使用多公钥的匿名数字机制中包含以下三种类型的实体：

a) 真实的签名方：真实的签名方是产生数字签名的实体；

b) 潜在的签名方：潜在的签名方是其公钥被用来创建数字签名的实体，这意味着该公钥既被用在签名过程也被用在验证过程，尽管潜在的签名方没有参与这两个过程；

c) 验证方：验证方是验证数字签名的实体。

8.3 密钥产生过程

密钥产生过程包含了一系列签名和验证密钥的产生过程，签名密钥对是彼此独立产生的。

8.4 环签名过程

在签名过程中，真实的签名方选择潜在的签名方(或潜在签名方的集合)，并且通过使用它自己的私有签名密钥和潜在签名方的验证密钥(不需要潜在签名方的同意和辅助)对消息进行签名。

8.5 环签名验证过程

在环签名验证过程中，验证方利用在签名过程中涉及的真实签名方和潜在签名方的公钥来验证签名。验证方在不知道谁是真实签名方的情况下检查签名是否是由签名方中的任意一个进行签署的。

参 考 文 献

[1] GB/T 15851.3—2018 信息技术 安全技术 带消息恢复的数字签名方案 第3部分:基于离散对数的机制

[2] ISO/IEC 9594-8:2008 Information technology—Open systems interconnection—The directory: Public-key and attribute certificate frameworks

[3] ISO/IEC 9796-2 Information technology—Security techniques—Digital signature schemes giving message recovery—Part 2: Integer factorization based mechanisms

[4] ISO/IEC 11770-2:2008 Information technology—Security techniques—Key management—Part 2: Mechanisms using symmetric techniques

[5] ISO/IEC 11770-3:2008 Information technology—Security techniques—Key management—Part 3: Mechanisms using asymmetric techniques

[6] ISO/IEC 15945:2002 Information technology—Security techniques—Specification of TTP services to support the application of digital signatures

[7] E. Brickell, L. Chen and J. Li, Simplified security notions of direct anonymous attestation and a concrete scheme from pairings. International Journal of Information Security, 8(5): 315-330, 2009.