ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17902.1—2023/ISO/IEC 14888-1:2008
代替 GB/T 17902.1—1999

信息技术　安全技术　带附录的数字签名　第1部分:概述

Information technology—Security techniques—Digital signatures with appendix—Part 1:General

（ISO/IEC 14888-1:2008,IDT）

2023-03-17 发布　　2023-10-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 17902《信息技术　安全技术　带附录的数字签名》的第1部分。GB/T 17902已经发布了以下部分:

——第1部分:概述;

——第2部分:基于身份的机制;

——第3部分:基于证书的机制。

本文件代替GB/T 17902.1—1999《信息技术　安全技术　带附录的数字签名　第1部分:概述》,与GB/T 17902.1—1999相比,除结构调整和编辑性改动外,主要技术变化如下:

——将原"概述"部分调整至第5章(见第5章,1999年版的第3章);

——删除了"赋值""无碰撞散列函数""确定性的""散列权标""散列代码""预签名""随机化""随机值""签名方程""签名函数"及"赋值"等术语(见1999年版的第4章),增加了"抗碰撞杂凑函数""数据元""域""杂凑码""密钥对"及"消息"等术语(见第3章);

——删除了"重新计算的散列权标""准备好的部分消息""赋值""预签名""重新计算的预签名"等符号以及"比较"的图例(见1999年版的第5章),增加了"可选数据"的图例(见4.3),并增加了"惯例"内容(见4.2);

——增加了"签名机制和杂凑函数的绑定选项"一章,描述了签名机制和杂凑函数绑定的几类选项(见第7章);

——将签名过程内容合并至第9章,并用通用模型,统一描述现有机制,较原内容更具有普适性(见第9章,1999年版的第8章、第9章);

——将验证过程合并至第10章,并更新了通用模型描述现有机制,较原内容更具有普适性(见第10章,1999年版的第9章)。

本文件等同采用ISO/IEC 14888-1:2008《信息技术　安全技术　带附录的数字签名　第1部分:概述》。

本文件做了下列最小限度的编辑性改动:

——第10章验证签名部分增加了注,便于理解。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国科学院软件研究所、成都卫士通信息产业股份有限公司、北京数字认证股份有限公司、中国电子技术标准化研究院、中国信息通信研究院。

本文件主要起草人:张振峰、何双羽、张严、白琨鹏、郝春亮、张立廷、王现方、傅大鹏、王惠莅、王榕。

本文件及其所代替文件的历次版本发布情况为:

——1999年首次发布为GB/T 17902.1—1999;

——本次为第一次修订。

引　言

数字签名机制是一类非对称密码机制，被广泛用于实体鉴别、数据来源鉴别、数据完整性和抗抵赖服务。有两种数字签名机制：

——若在验证过程中，需要消息作为输入的一部分，则此类机制称为“带附录的数字签名”，附录计算需要使用杂凑函数；

——若在验证过程中，披露全部或是部分消息，则此类机制称为“带消息恢复的数字签名”，签名生成和验证也会使用到杂凑函数。

带附录的数字签名在GB/T 17902中进行了规范，带消息恢复的数字签名在ISO 10118中进行了规范，杂凑函数则是在GB/T 18238(所有部分)中进行了规范。

GB/T 17902《信息技术　安全技术　带附录的数字签名》由三个部分组成。

——第1部分：概述。目的在于规范通用的带附录数字签名的整体框架和通用模型。

——第2部分：基于身份的机制。目的在于规范基于身份的带附录数字签名机制。

——第3部分：基于证书的机制。目的在于规范基于证书的数字签名机制。

信息技术　安全技术　带附录的数字签名
第1部分:概述

1　范围

GB/T 17902规定了几种对任意长度消息进行签名的带附录的数字签名机制。

本文件包括带附录的数字签名的一般原理与要求,同时也包括GB/T 17902各部分用到的定义与符号。

证书和密钥管理等相关技术不在本文件的规范范围内。更多此类信息见GB/T 16264.8—2005[2],ISO/IEC 11770-3[8]以及ISO/IEC 15945:2002[9]。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

附录　appendix

由签名和一个可选文本字段构成的比特串。

3.2

抗碰撞杂凑函数　collision-resistant hash-function

抗碰撞散列函数

满足如下性质的杂凑函数:找出映射到同一输出的任何两个不同输入在计算上不可行。

注:计算是否可行依赖于具体的安全需求和环境。

[来源:ISO/IEC 10118-1:2016,3.1]

3.3

数据元　data element

整数、比特串、整数集合或比特串集合。

3.4

域　domain

在单一安全策略下运行的一组实体。

示例:由单一机构或一组采用同一安全策略的机构创建的公钥证书。

3.5

域参数　domain parameter

对域中所有实体都是公共的且已知或可访问的数据元。

3.6

杂凑码 hash-code

散列码

杂凑函数输出的比特串。

[来源:ISO/IEC 10118-1:2016, 3.3]

3.7

杂凑函数 hash-function

散列函数

将任意比特串映射到固定长度比特串的函数,满足下面两个特征:

——对于给定输出,找出映射为该输出的输入,在计算上是不可行的;

——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 1:计算上的可行性取决于特定安全要求和环境。

注 2:该杂凑函数的定义也被称为单向杂凑函数。

[来源:ISO/IEC 10118-1:2016, 3.4]

3.8

标识数据 identification data

分配给某一实体,用于对其标识的数据元序列(包括实体的可区分标识符)。

注:标识数据能额外包含数据元,例如,签名过程标识符、签名密钥标识符、签名密钥有效期、对密钥用法的限制、关联的安全策略参数、密钥系列号或域参数。

3.9

密钥对 key pair

由一个签名密钥和一个验证密钥组成的对,即:

——签名密钥是完全或部分保密的、只由被签名者使用的数据元集合;

——验证密钥是能够完全公开、供任何验证者使用的数据元集合。

3.10

消息 message

任意长度的比特串。

3.11

参数 parameter

整数、比特串或杂凑函数。

3.12

签名 signature

签名过程产生的一个或多个数据元。

3.13

签名密钥 signature key

签名过程中实体所特有的且只能由该实体使用的私有数据元集合。

注:有时在其他标准中也被称为"私有签名密钥",例如 ISO/IEC 9796-2,GB/T 15851.3 和 ISO/IEC 9798-3。

3.14

签名过程 signature process

以消息、签名密钥和域参数作为输入,给出签名作为输出的过程。

3.15

已签消息 signed message

由签名、无法从签名恢复的消息部分和一个可选文本字段组成的一组数据元。

注：在本文件中，整个消息被包含在已签消息中并且消息的任何部分都不能从签名中恢复。

3.16

验证密钥 verification key

在数学上与实体的签名密钥相关，并由验证方在验证过程中使用的公开数据元集合。

注：在其他标准中也被称“公开验证密钥”，例如 ISO/IEC 9796-2，GB/T 15851.3，ISO/IEC 9798-3。

3.17

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。

4 符号、惯例和图例

4.1 符号

下列符号适用于 GB/T 17902 的所有部分。

H	杂凑码
K	随机数发生器
M	消息
R	签名的第一部分

注：R 也被称为证据。

$\overline{R}$	重新计算的签名第一部分
S	签名的第二部分
X	签名密钥
Y	验证密钥
Z	域参数集合
Σ	签名
$A \bmod N$	在 0 到 $N-1$ 中的唯一整数 B，使得 N 能整除 $A-B$
$A \equiv B \pmod N$	整数 A 与整数 B 模 N 相等，即 $(A-B) \bmod N = 0$

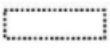
4.2 惯例

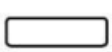
在 GB/T 17902 所有部分中的整数(或位、字节)以最左侧为最高有效位。

4.3 图例

下列图例适用于 GB/T 17902 的所有部分。


数据


可选数据


过程


主过程

可选主过程

数据流

可选数据流

另一个可选数据流

两条数据流，其中至少一条是必备的

5 通则

GB /T 17902 描述的机制基于非对称密码技术。非对称数字签名机制由以下三个基本操作组成。

a) 生成密钥对的过程，称为密钥生成过程。每一个密钥对都由一个签名密钥和对应的一个验证密钥组成。

b) 使用签名密钥签名的过程，也被称为签名过程：

1) 对一个给定消息和签名密钥，若获得两个相同签名的概率是可忽略的，则称运算是概率性的；

2) 对一个给定消息和签名密钥，生成的所有签名都相同，则称运算是确定性的。

c) 使用验证密钥验证签名的过程，也被称为验证过程。

验证一个数字签名需要使用签名者的验证密钥。因此，验证者要能将正确的验证密钥与签名者关联起来，或是要和签名者的(部分)标识数据关联起来。这种关联由验证密钥自身提供的，称这种机制是“基于身份的”。这种关联由包含验证密钥的证书提供，这种机制被称为“基于证书的”。

6 通用模型

带附录的数字签名机制包含以下过程：

——密钥生成过程；

——签名过程；

——验证过程。

在签名过程中，签名者对一个给定的消息计算数字签名。这个数字签名和一个可选的文本字段构成附录，附录附加在消息上形成已签消息，如图 1 所示。

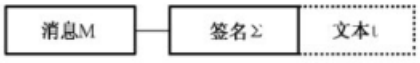


图 1 已签消息

根据实际应用，有多种生成附录并附加在消息上的方法。这些方法能使验证者将消息和正确签名关联起来。

验证者在验证签名之前，获得签名对应的正确的签名验证密钥。这对于成功验证签名非常重要。可选的文本字段可用于向验证者传递签名者的标识数据，或是用于鉴别验证密钥信息的数据。某些情况下，签名者的标识数据可作为消息 M 的一部分，以获得签名的保护。

数字签名机制应满足以下的要求：

a) 只给定验证密钥，而不给定签名密钥，产生任一消息的有效签名在计算上是不可行的；

b) 签名者产生的签名不能用于生成新消息及其对应的有效签名，也不可用来恢复签名密钥；

c) 找到签名相同但内容不同的两个消息在计算上是不可行的，即使对签名者在计算上也是不可

行的。

注：计算上的可行性依赖于用户的具体安全要求和环境

7 签名机制和杂凑函数绑定方式的选项

使用本文件中的数字签名机制需要选择一个抗碰撞杂凑函数。在使用中应将杂凑函数与签名机制绑定使用。否则，攻击者可使用一个弱杂凑函数(不是实际使用的)伪造签名。

已有一系列方式实现此类绑定。以下方法按照伪造签名风险从低到高排列。

a) 当使用特定签名机制时要求使用特定的杂凑函数。在签名验证过程中应只使用此杂凑函数。

b) 允许使用一套杂凑函数，在证书的域参数里明确指定使用的杂凑函数。在证书管理域内，验证者在签名验证过程中只使用证书指定的杂凑函数进行签名验证。但是在域外，会因为证书机构不遵循用户的策略而产生风险。例如，域外的证书机构签发一个允许使用其他杂凑函数的证书，签名伪造的问题可能出现。在这种情况下，一个被误导的验证者将无法确定采用何种杂凑函数进行验证。

c) 允许使用一组可选的杂凑函数，并通过除 b)之外的方式指定使用哪一个杂凑函数。例如，通过消息或是双方协商指定杂凑函数。验证过程应只使用由该方式指定的杂凑函数。然而，存在攻击者通过使用其他杂凑函数伪造签名的风险(具体攻击方法见附录 A)。

注：在 c)中提及的“除 b)之外的方式”包括通过杂凑函数标识符的方式。杂凑函数标识符与杂凑码拼接成杂凑令牌包含在签名中。在此方式下，即使验证者接受的签名使用了弱杂凑函数(能够通过杂凑码找到对应输入的杂凑函数)，对于不同的消息，攻击者也不能重用这个签名。但是，正如参考文献[9]中所述(见附录 A)，使用该类弱杂凑函数，攻击者依然能够通过针对包含此弱杂凑函数标识符的签名，找到对应的消息。

数字签名机制的用户宜综合考虑不同绑定方式的技术优势和开销，进行风险评估。风险评估还宜考虑伪造签名的开销。

8 密钥生成

数字签名机制的密钥生成过程包括以下两个步骤：

a) 生成域参数；

b) 生成签名密钥和验证密钥。

第一个步骤只在建立域时执行一次。第二个步骤，针对域内的每个签名者分别执行，密钥生成过程的输出是签名密钥 X 和验证密钥 Y。对于一组指定的域参数，避免 X 的值与之前使用的值相同。

注：域参数和密钥的有效性验证不在本文件的规定范畴内。

9 签名过程

9.1 通则

签名过程需要以下数据元：

——域参数集合 Z；

——签名密钥 X；

——消息 M；

——杂凑函数标识符 hid(可选)；

——其他文本 t(可选)。

杂凑函数的标识符能够用于绑定签名机制和杂凑函数,具体内容见第 7 章。

带附录的数字签名机制的签名过程由以下步骤组成:

——计算签名;

——构建附录;

——构建已签消息。

9.2 计算签名

该过程的输入为消息 M,签名密钥 X 以及域参数集合 Z。输出为签名 Σ,Σ 由第一部分 R 和第二部分 S 组成,第二部分是否存在取决于签名机制,见图 2。

9.3 构建附录

附录由签名和可选文本字段构成,记为(Σ,t)。文本字段可包含一个证书,该证书的作用是用密码机制关联验证密钥和签名者的标识数据。

注:根据应用的不同,附录有多种不同的生成并将其附加在消息上的方式。附录确保验证者能够关联正确的消息和对应签名。验证者能够关联签名的正确验证密钥是成功完成验证的前提。

9.4 构建已签消息

已签消息由消息 M 和附录构成,即 M,(Σ,t)。

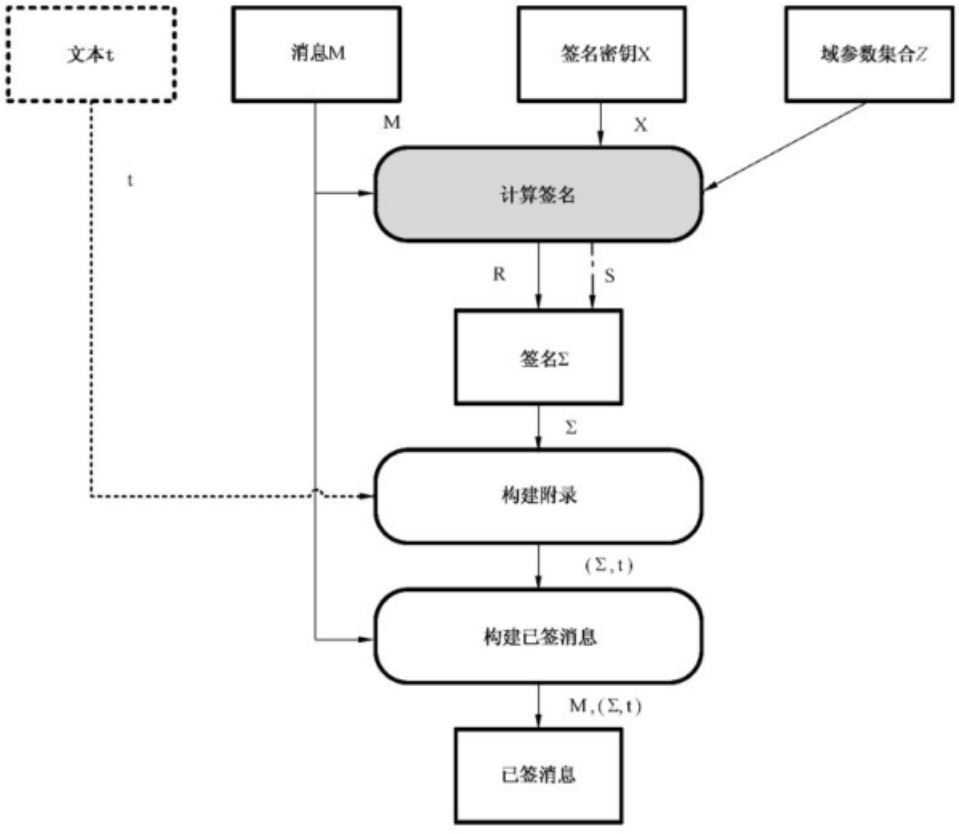


图 2 签名过程

10 验证过程

验证过程需包含以下数据元：

——域参数集合 Z；

——验证密钥 Y；

——消息 M；

——签名 Σ；

——标识数据 Id(可选)；

——使用中的杂凑函数标识符 hid [若没有使用其他方式确定(见第 7 章)]；

——其他文本 t(可选)。

验证过程的输入为消息 M，域参数 Z，验证密钥 Y，签名 Σ 以及与签名机制对应的标识数据 Id。验证过程的输出是验证签名结果的布尔值：是(接受)/否(拒绝)。整个过程见图 3。整个验证过程由以下函数组合之一构成：

a) 签名打开、计算杂凑值并比较；

b) 签名打开、恢复消息代表和验证恢复的消息代表；

注 1：消息代表是指由消息转化生成的比特串，用于与签名密钥结合产生签名。

c) 恢复证据、恢复赋值、重新计算预签名、重新计算证据、验证证据。

注 2：证据是预签名和部分消息的值经过证据函数计算后的输出，是签名的第一部分。

注 3：赋值是证据和部分消息经过赋值函数计算后的一组数据元。

注 4：预签名是对签名过程中生成的随机数进行运算的结果，与消息无关。

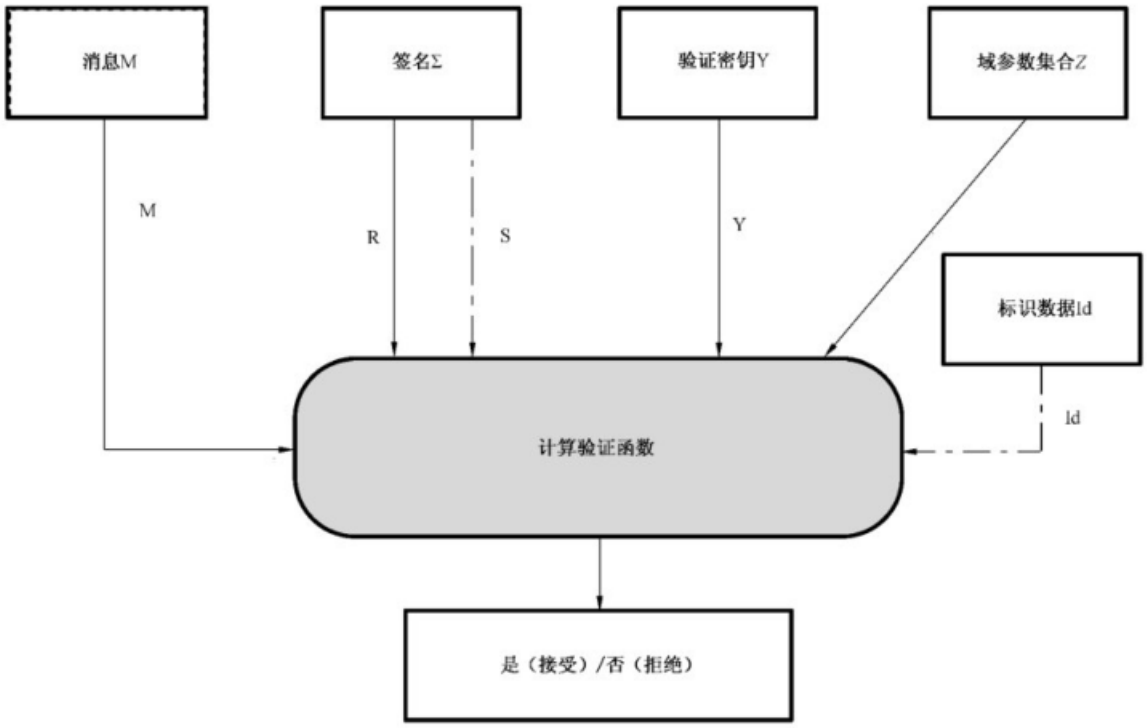


图 3 验证过程

附 录 A
（资料性）
关于杂凑函数标识符

如第 7 章所述，使用 GB/T 17902 中描述的数字签名机制宜选择抗碰撞杂凑函数。为保证验证过程能够被安全执行，对验证者而言，确定签名生成时采用的杂凑函数非常重要。如果恶意的第三方使验证者相信在生成签名时使用了一个“弱”杂凑函数（例如，缺乏单向性的杂凑函数），此第三方能够欺骗验证者接受一个“错误”消息的合法签名。

GB/T 17902 允许通过“杂凑令牌”指定一个签名所使用的杂凑函数。该令牌由一个杂凑函数标识符与一个杂凑码拼接组成，用于绑定杂凑函数与数字签名机制。如果杂凑函数标识符通过此类方式包含杂凑令牌中，对于不同的消息，攻击者无法重用一个已存在的合法签名，即便验证者接受的签名使用了弱到能够找到原象的杂凑函数，此类攻击也不起效。这被认为是解决上段中提到攻击的有效手段。

然而，正如在参考文献[10]中详细讨论的，如果一个验证者被欺骗并相信签名生成时采用了某个“弱”杂凑函数，即使将杂凑函数标识符用“杂凑令牌”的方式包含在签名中，依然可能存在其他攻击。此处的“弱”的是指杂凑函数缺乏单向性，即找到一个输入使其输出是某个给定的杂凑码在计算上是可行的。（缺乏单向性的杂凑函数可能引起的安全风险，促使将杂凑函数标识符以杂凑令牌的形式包含在签名中予以保护。）

在参考文献[10]中描述了两类攻击方法。

a) 在攻击者能够完全控制签名中的杂凑令牌值的情况下，攻击者在某个随机生成的签名中嵌入弱杂凑函数的杂凑函数标识符。攻击者通过弱杂凑函数反向计算获得消息 M，从而形成消息 M 和它的签名。在此种情况中，即使弱杂凑函数只是对一部分杂凑码存在脆弱性，依然有可能伪造该部分杂凑码对应消息的签名。

b) 在某些允许使用长杂凑函数标识符的情况下，攻击者生成一个随机签名并尝试计算信息代表 T（正常情况下，信息代表 T 是利用验证密钥从签名中计算出的比特串）。如果攻击者找到一个满足条件的 T，使得 T 的形式满足 T=Pad||HID||H（其中 Pad 是一个常量的比特串，HID 是随机生成的杂凑函数标识符但是在结构上与杂凑函数标识符相同，H 是消息输出的杂凑码）。攻击者通过攻击弱杂凑函数，从 H 中反算出某个消息 M。当 Pad 的长度不足且签名机制允许长 HID 存在时，攻击者通过尝试不同 Pad 值找到符合条件 T 的概率就是不可忽略的。在此类攻击中，攻击成功的前提是攻击者能够使验证者相信签名使用了某个新随机生成但符合语法结构的杂凑函数标识符。

给定这样一个“签名”，攻击者获得嵌在签名中或是嵌在恢复出的消息代表中的杂凑码，并利用弱杂凑函数找到一个对应此杂凑码的消息。由此，攻击者成功伪造了一个新签名。因此除了拼接杂凑函数标识符和杂凑码的方式外，有时验证者也需要有安全独立的途径知晓签名验证时使用的杂凑函数。

在 GB/T 17902 中的大多数的数字签名机制需要在域参数中指定所使用的杂凑函数[如第 7 章 a)项中所描述]，或者签名机制自身指定可供选择的杂凑函数[如第 7 章 b)项中所描述]。数字签名机制的使用者宜综合考虑不同方式的开销和优势，进行风险评估。此项评估包含评估伪造签名的开销。

参 考 文 献

[1] GB/T 15851.3 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(GB/T 15851.3—2018,ISO 9796-3:2006,MOD)

[2] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

[3] GB/T 18238(所有部分) 信息技术 安全技术 散列函数[ISO/IEC 10118(所有部分)]

[4] GB/T 25069—2022 信息安全技术 术语

[5] ISO/IEC 9796-2:2010 Information technology—Security techniques—Digital signature schemes giving message recovery—Part 2: Integer factorization based mechanisms

[6] ISO/IEC 9798-3 IT Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques

[7] ISO/IEC 10118-1:2016 Information technology—Security techniques—Hash-functions—Part 1: General

[8] ISO/IEC 11770-3 Information security—Key management—Part 3: Mechanisms using asymmetric techniques

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

[10] B. Kaliski, On hash function firewalls in signature scheme, in Proc. Cryptographers Track RSA Conference 2002, Preneel, Ed, Lecture Notes in Computer Science. Vol. 2271, pp.1-16, Berlin Springer-verlag,2002.