ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17902.2—2005/ISO/IEC 14888-2:1999

信息技术　安全技术　带附录的数字签名　第2部分:基于身份的机制

Information technology—Security techniques—Digital signatures with appendix—Part 2:Identity-based mechanisms

(ISO/IEC 14888-2:1999,IDT)

2005-04-19 发布　　2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 带附录的数字签名
第 2 部分:基于身份的机制
GB/T 17902.2—2005/ISO/IEC 14888-2:1999
*
中 国 标 准 出 版 社 出 版 发 行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
电话:63787337、63787447
2005 年 8 月第一版 2005 年 8 月电子版制作
*
书号:155066·1-23069

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　概述 …… 1
4　术语和定义 …… 1
5　符号 …… 2
6　密钥生成过程 …… 2
6.1　生成域参数 …… 2
6.2　生成验证密钥和签名密钥 …… 3
7　签名过程 …… 3
7.1　生成预签名 …… 3
7.2　准备消息 …… 4
7.3　计算证据 …… 4
7.4　计算签名 …… 4
8　验证过程 …… 5
8.1　准备消息 …… 6
8.2　检索证据 …… 6
8.3　计算验证函数 …… 7
8.4　验证证据 …… 7
9　Guillou-Quisquater 签名机制 …… 7
9.1　公钥导出函数 …… 8
9.2　准备消息 …… 8
9.3　计算证据 …… 8
9.4　计算签名的第一部分 …… 8
9.5　计算赋值 …… 8
10　带短赋值的基于身份的签名 …… 8
10.1　准备消息 …… 8
10.2　计算证据 …… 8
10.3　计算赋值 …… 8
11　带消息散列码检索的基于身份的签名 …… 8
11.1　计算证据 …… 9
11.2　计算签名的第一部分 …… 9
附录 A(资料性附录)　数值例子 …… 10
A.1　密钥生成过程的数值例子 …… 10
A.1.1　生成域参数 …… 10
A.1.2　生成验证密钥和签名密钥 …… 11
A.2　在第 9 章中描述的 Guillou-quisquater 签名机制的数值例子 …… 11
A.2.1　签名过程 …… 11

A.2.2 验证过程 …… 12
A.3 在第 10 章中描述的带有短赋值的基于身份的签名的数值例子 …… 13
A.3.1 签名过程 …… 13
A.3.2 验证过程 …… 14
A.4 在第 11 章中描述的给出消息散列代码检索的基于身份的签名的数值例子 …… 14
A.4.1 签名过程 …… 14
A.4.2 验证过程 …… 15
附录 B(资料性附录) 专利信息 …… 17
参考文献 …… 18

图 1 带确定性证据的签名过程 …… 4
图 2 带随机化证据的签名过程 …… 5
图 3 带确定性证据的验证过程 …… 6
图 4 带随机化证据的验证过程 …… 7

前　言

GB/T 17902《信息技术　安全技术　带附录的数字签名》由以下几个部分组成：

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。

本部分为GB/T 17902的第2部分，等同采用国际标准ISO/IEC 14888-2:1999《信息技术　安全技术　带附录的数字签名　第2部分：基于身份的机制》(英文版)。

本部分的附录A和附录B是资料性附录。

本部分由中华人民共和国信息产业部提出；

本部分由全国信息安全标准化技术委员会归口；

本部分由中国电子技术标准化研究所、信息安全国家重点实验室起草。

本部分主要起草人：叶茅枫、陈星、罗锋盈、胡磊、叶顶锋、张振峰、黄家英。

信息技术　安全技术　带附录的数字签名
第2部分:基于身份的机制

1　范围

GB/T 17902规定了任意长度消息的带附录的各种数字签名机制。它适用于提供实体鉴别、数据始发鉴别、抗抵赖和数据完整性的方案。

GB/T 17902的本部分规定了任意长度消息的带附录的基于身份的数字签名机制的签名和验证过程的总的结构和基本过程。

2　规范性引用文件

下列文件中的条款通过GB/T 17902的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB 15851—1995　信息技术　安全技术　带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

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

3　概述

数字签名的验证需要签名实体的验证密钥。所以,验证方必须把正确的验证密钥与签名实体,或更准确地讲,与签名实体的(部分)标识数据关联起来。如果这种联系是验证密钥自身所固有的,这种方案被称作“基于身份的”。

本部分中定义的基于身份的方案的密钥生成过程包括一个可信第三方。这个可信第三方有个秘密参数——密钥生成指数,它用于导出其他实体的签名密钥。签名密钥的秘密性无条件地依赖于密钥生成指数的秘密性。

在基于身份的签名的验证中,需要两个参数。第一个参数为域验证指数,它对所有实体来说是共同的;而第二个参数为签名实体的验证密钥,它对每个实体而言是特定的。本部分定义的基于身份的机制中,实体的验证密钥是使用一个公共函数直接从实体的标识数据中得到的。

带附录的基于身份的签名机制是个随机化机制的例子,如GB/T 17902.1—1999所描述。数字签名和验证过程描述遵循GB/T 17902.1—1999第10章定义的一般过程。特别地,本标准使用了GB/T 17902.1—1999提供的一般需求条件、定义和符号。

在下列过程的详细说明中定义了带附录的基于身份的数字签名机制。它们是:

a)　密钥生成过程;

b)　签名过程;

c)　验证过程。

4　术语和定义

下列术语和定义适用于GB/T 17902的本部分: