ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15851.3—2018
代替 GB/T 15851—1995

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

Information technology—Security techniques—Digital signature schemes giving message recovery—Part 3：Discrete logarithm based mechanisms

（ISO/IEC 9796-3：2006，MOD）

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国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　缩略语和符号、约定 …… 3
4.1　缩略语和符号 …… 3
4.2　转换函数和掩码生成函数 …… 5
4.3　附图说明 …… 5
5　签名机制和杂凑函数之间的绑定 …… 6
6　带消息恢复的数字签名框架 …… 6
6.1　过程 …… 6
6.2　参数生成过程 …… 7
6.3　签名生成过程 …… 7
6.4　签名验证过程 …… 7
7　带消息恢复的数字签名总体模型 …… 8
7.1　要求 …… 8
7.2　函数和过程总结 …… 8
7.3　用户密钥生成过程 …… 8
7.4　签名生成过程 …… 9
7.5　签名验证过程 …… 11
8　NR(Nyberg-Rueppel 消息恢复签名) …… 13
8.1　域参数和用户密钥 …… 13
8.2　签名生成过程 …… 13
8.3　签名验证过程 …… 14
9　ECNR(椭圆曲线 Nyberg-Rueppel 消息恢复签名) …… 15
9.1　域参数和用户密钥 …… 15
9.2　签名生成过程 …… 15
9.3　签名验证过程 …… 16
10　ECMR(椭圆曲线 Miyaji 消息恢复签名) …… 17
10.1　域参数和用户密钥 …… 17
10.2　签名生成过程 …… 17
10.3　签名验证过程 …… 18
11　ECPV(椭圆曲线 Pintsov-Vanstone 消息恢复签名) …… 18
11.1　域参数和用户参数 …… 18

11.2 签名生成过程 …… 19
11.3 签名验证过程 …… 20
12 ECKNR(椭圆曲线 KCDSA/Nyberg-Rueppel 消息恢复签名) …… 21
12.1 域参数和用户参数 …… 21
12.2 签名生成过程 …… 21
附录 A(资料性附录) 数学转换 …… 24
附录 B(规范性附录) 转换函数 …… 26
附录 C(规范性附录) 掩码生成函数(密钥导出函数) …… 29
附录 D(资料性附录) 数据输入生成方式实例 …… 30
附录 E(资料性附录) ASN.1 模块 …… 31
附录 F(资料性附录) 算例 …… 33
附录 G(资料性附录) 机制特点总结 …… 45
附录 H(资料性附录) 方案的对应性 …… 47
参考文献 …… 48

前　言

GB/T 15851《信息技术　安全技术　带消息恢复的数字签名方案》目前分为以下部分：

——第2部分：基于大数分解的机制；

——第3部分：基于离散对数的机制。

本部分为GB/T 15851的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 15851—1995《信息技术　安全技术　带消息恢复的数字签名方案》，与GB/T 15851—1995相比，主要技术差异如下：

——补充规定了密钥生成过程；

——除带消息恢复的数字签名框架外，新定义了五种数字签名方案，并规定了每种签名方案的签名和验证方法；

——补充规定了杂凑函数的用法；

——部分签名方案增加使用椭圆曲线或有限域；

——新增对完全和部分消息恢复的说明；

——新增规范性引用文件；

——使用8个新增附录替换原附录A和附录B，用于描述密钥导出函数及数字签名方案的说明实例等。

本部分使用重新起草法修改采用ISO/IEC 9796-3:2006《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》及其勘误。

本部分与ISO/IEC 9796-3:2006相比存在结构变化，删除了第11章，将第12章改为第11章，第13章改为第12章，增加8.3.6、9.3.6、10.3.6、11.3.6和12.3.6。

本部分与ISO/IEC 9796-3:2006的技术性差异及其原因如下：

——删除了第11章及其相关内容，以与我国技术水平相适应。

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、中国电子技术标准化研究院、重庆邮电大学、中国电子科技集团公司第三十研究所、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、北京大学深圳研究生院、天津市无线电监测站、中国人民解放军信息安全测评认证中心、北京计算机技术及应用研究所、福建省无线电监测站、国家信息技术安全研究中心、北京数字认证股份有限公司、中国电信股份有限公司上海研究院、工业和信息化部宽带无线IP标准工作组等。

本部分主要起草人：王月辉、杜志强、李琴、曹军、黄振海、李大为、宋起柱、许玉娜、张璐璐、龙昭华、李明、铁满霞、张变玲、李楠、朱跃生、李广森、颜湘、张国强、童伟刚、万洪涛、朱正美、陈志宇、葛培勤、侯鹏亮、许福明、高波、郑骊。

本部分所代替标准的历次版本发布情况为：

——GB/T 15851—1995。

引　言

数字签名机制可以提供实体鉴别、数据源鉴别、不可抵赖和数据完整性服务。

数字签名机制满足以下要求：

——如果只有公开验证密钥，没有私有签名密钥，对任何给定的消息生成一个有效的签名在计算上是不可行的；

——签名方已生成的签名既不能用来为一个新消息生成一个有效的签名，也不能用来恢复签名密钥；

——对于签名者，找到带有相同签名的两个不同的消息在计算上是不可行的。

大部分签名机制是基于非对称密码技术，包括下列三个基本操作：

——生成密钥对的过程，每个密钥对包括一个私有签名密钥和相对应的公开验证密钥；

——使用私有签名密钥的过程，称作签名生成过程；

——使用公开验证密钥的过程，称作签名验证过程。

数字签名机制有两类：

——对于给定的私有签名密钥，签名者对相同消息的签名是相同的，这种机制称为非随机的（或确定的）[参见 ISO/IEC 14888-1]；

——对于给定的消息和给定的私有签名密钥，每个签名处理过程生成的签名是不同的，这种机制称为随机的。

本部分规定了随机的数字签名机制。

数字签名方案也可以分成下列两类：

——当整个消息需要存储和/或随着签名一起传输时，该方案称作“带附录的签名方案”[参见 ISO/IEC 14888]；

——从签名中可以恢复整个或者部分消息时，该方案称作“带消息恢复的签名方案”。

如果消息足够短，则整个消息可包括在签名里并通过签名验证过程从签名中恢复；否则消息的一部分可包括在签名里，余下部分存储起来或随着签名一起传输。本部分规定的机制提供完整或者部分恢复，目的在于降低存储和传输管理。

本部分包括五个签名方案。本部分规定的方案使用杂凑函数对整个消息进行运算。ISO/IEC 10118 规定了杂凑函数。在本部分中规定的一些方案使用有限域上的椭圆曲线一个群。ISO/IEC 15946-1:2002 描述了基于有限域上的椭圆曲线实现密码系统的数学背景和基本技术。本部分所定义机制的特点参见附录 G，这些机制与 ISO/IEC 9796-3:2000 以及 ISO/IEC 15946-4:2004 所定义机制的对应关系参见附录 H。

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

1　范围

GB/T 15851的本部分规定了五种带消息恢复功能的数字签名方案。这些方案的安全性是基于定义在有限域或有限域上的椭圆曲线的离散对数问题的难度。

本部分也定义了在杂凑权标里的一个可选控制字段，其能够增强签名的安全性。

本部分规定了随机机制。

在本部分中规定的机制能够完全或者部分恢复消息。

注：带附录的基于离散对数的数字签名方案参见ISO/IEC 14888-3。

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。

ISO/IEC 10118(所有部分)　信息技术　安全技术　散列函数(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：总则(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

下列术语和定义适用于本文件。

3.1

数据输入　data input

取决于完整消息或部分消息的八位位组串，其组成了签名生成过程的一部分输入。

3.2

域参数　domain parameter

常见且已知的或者可以被域中所有实体访问的数据项。

[ISO/IEC 14888-1：1998]

注：域参数集合可以包括数据项，诸如杂凑函数标识、杂凑权标的长度、消息中可恢复部分的最大长度、有限域参数、椭圆曲线参数或者其他能够表明域的安全策略的参数。