ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 18238.3—2024
代替 GB/T 18238.3—2002

网络安全技术　杂凑函数
第3部分：专门设计的杂凑函数

Cybersecurity technology—Hash-functions—Part 3：Dedicated hash-functions

2024-09-29 发布　　2025-04-01 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 18238《网络安全技术　杂凑函数》的第 3 部分。GB/T 18238 已经发布了以下部分：

——第 1 部分：总则；

——第 2 部分：采用分组密码的杂凑函数；

——第 3 部分：专门设计的杂凑函数。

本文件代替 GB/T 18238.3—2002《信息技术　安全技术　散列函数　第 3 部分：专用散列函数》，与 GB/T 18238.3—2002 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语“块”“散列函数标识符”“循环函数”“字”及其定义（见 2002 年版的第 3 章）；

b) 增加了术语“字节”（见第 3 章）；

c) 删除了专用散列函数 1、专用散列函数 2 和专用散列函数 3（见 2002 年版的第 7 章、第 8 章和第 9 章）；

d) 增加了杂凑函数 SM3（见第 7 章）；

e) 更改了附录 A 实例为附录 A 对象标识符（见附录 A，2002 年版的附录 A）。

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。

本文件由全国网络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：中电科网络安全科技股份有限公司、国家密码管理局商用密码检测中心、中国电子技术标准化研究院、中国科学院大学、山东大学、中国科学院软件研究所、西安西电捷通无线网络通信股份有限公司、北京银联金卡科技有限公司、中国电子科技集团公司第十五研究所、格尔软件股份有限公司、北京信安世纪科技股份有限公司、山东得安信息技术有限公司、华为技术有限公司、智巡密码（上海）检测技术有限公司、北京江南天安科技有限公司、北京海泰方圆科技股份有限公司。

本文件主要起草人：张立廷、罗鹏、赵新强、李世敏、毛颖颖、黄晶晶、孙思维、王薇、眭晗、李琴、杨波、李艳俊、林阳荟晨、郑强、赵礼鹏、龚晓燕、马洪富、曾光、韩玮、李雪雁、潘文伦、熊云、贾世杰、王跃武、王现方、陈奕言、王月辉。

本文件及其所代替文件的历次版本发布情况为：

——2002 年首次发布为 GB/T 18238.3—2002；

——本次为第一次修订。

引　言

杂凑函数使用特定的算法将任意长度(通常设有上限)的位串映射到固定长度的位串。专门设计的杂凑函数是指在设计过程中不依赖其他密码原语(如分组密码等),直接设计形成的杂凑函数。

GB/T 18238《网络安全技术　杂凑函数》由3个部分构成。

——第1部分:总则。目的在于规定杂凑函数的要求和通用模型,用于指导GB/T 18238的其他部分。

——第2部分:采用分组密码的杂凑函数。目的在于规定采用分组密码的杂凑函数。

——第3部分:专门设计的杂凑函数。目的在于规定专门设计的杂凑函数。

网络安全技术　杂凑函数
第3部分：专门设计的杂凑函数

1　范围

本文件规定了专门设计的杂凑函数的要求和模型。

本文件适用于专门设计的杂凑函数的设计、开发和检测。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 18238.1—2024　网络安全技术　杂凑函数　第1部分：总则（ISO/IEC 10118-1：2016，MOD）

GB/T 25069　信息安全技术　术语

GB/T 32905—2016　信息安全技术　SM3密码杂凑算法

3　术语和定义

GB/T 25069和GB/T 18238.1—2024界定的以及下列术语和定义适用于本文件。

3.1

字节　byte

由8个连续位构成的位串。

4　符号

下列符号适用于本文件。

B_i：B的第i个字节。

D：数据。

H：杂凑值。

IV：初始化值。

L_X：位串X的位长度。

L_1：输入到轮函数ϕ的两个位串中，第一个位串的位长度。

L_2：输入到轮函数ϕ的两个位串中，第二个位串的位长度，也是轮函数ϕ输出值的位长度，以及初始化值IV的位长度。

r：填充方法中预留位串的位长度。

5　要求

使用本文件中的杂凑函数的用户应选择：