



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

订单号: 0109250410403126 防伪编号: 2025-0409-1127-1518-2143 购买单位: 豪密科技

豪密科技 专用

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 符号 1

5 要求 1

6 专门设计的杂凑函数的模型 2

 6.1 通用模型的使用 2

 6.2 轮函数模型 2

7 杂凑函数 SM3 2

 7.1 概述 2

 7.2 参数选择 2

 7.3 填充方法 2

 7.4 初始化值 2

 7.5 轮函数 2

 7.6 输出变换 2

附录 A(规范性) 对象标识符 3

参考文献..... 4

订单号：0109250410403126 防伪编号：2025-0409-1127-1518-2143 购买单位：豪密科技

订单号: 0109250410403126 防伪编号: 2025-0409-1127-1518-2143 购买单位: 豪密科技

豪密科技 专用

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。

豪密科技
防伪编号: 2025-0409-1127-1518-2143

订单号: 0109250410403126 防伪编号: 2025-0409-1127-1518-2143 购买单位: 豪密科技

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：

购买单位：豪密科技
2025-0409-1127-1518-2143
防伪编号：0109250410403126
订单号：0109250410403126

- 本文件规定的杂凑函数；
- 杂凑值 H 的长度 L_H 。

注 1：本文件定义的所有杂凑函数的输入和输出均为一个位串；这与每个杂凑函数内部字节顺序的约定无关。

注 2： L_H 的选择影响杂凑函数的安全性。本文件规定的所有杂凑函数均被认为是抗碰撞安全的。其中，执行 $2^{L_H/2}$ 次杂凑运算被认为是计算上不可行的。

附录 A 定义的对象标识符用于标识本文件规定的杂凑函数。

6 专门设计的杂凑函数的模型

6.1 通用模型的使用

专门设计的杂凑函数应采用 GB/T 18238.1—2024 中定义的基于轮函数的通用模型。

6.2 轮函数模型

本文件规定的杂凑函数默认要求，填充后的数据串以字节串形式作为输入。如果填充后的数据串是 $8n$ 位串 $x_0, x_1, \dots, x_{8n-1}$ ，则将其看作 n 字节序列 B_0, B_1, \dots, B_{n-1} 。其中，每组连续 8 位为一个字节，每组的第一位为该字节的最高有效位。因此，对任意 $i (0 \leq i < n)$ ， $B_i = 2^7 x_{8i} + 2^6 x_{8i+1} + \dots + x_{8i+7}$ 。

本文件规定的杂凑函数的输出变换为：截取最终输出 H_q (长度为 L_2 位) 的最左侧 L_H 位，作为杂凑值 H 。

7 杂凑函数 SM3

7.1 概述

本章以 GB/T 32905—2016 规定的 SM3 密码杂凑算法作为示例，展示 6.2 规定的轮函数模型的使用方法，介绍其中的参数选取、填充方法、初始化值、轮函数和输出变换。

杂凑函数 SM3 可应用于所有长度不超过 $2^{64} - 1$ 位的数据串 D 。

7.2 参数选择

杂凑函数 SM3 的参数 $L_1 = 512, L_2 = 256, L_H = 256$ 。具体按 GB/T 32905—2016 中 5.3。

7.3 填充方法

杂凑函数 SM3 的填充方法应采用 GB/T 18238.1—2024 中 A.3 规定的方法 2，取 $r = 64$ 。具体按 GB/T 32905—2016 中 5.2。

7.4 初始化值

初始化值按 GB/T 32905—2016 中 4.1。

7.5 轮函数

轮函数按 GB/T 32905—2016 中 5.3.2 和 5.3.3。

7.6 输出变换

输出变换为恒等变换，即杂凑值 $H = H_q$ 。具体按 GB/T 32905—2016 中 5.4。

附录 A

(规范性)

对象标识符

本附录列出了本文件引用的杂凑函数 SM3 的对象标识符。

```
DedicatedHashFunctions {
iso(1) standard(0) hash-functions(10118) part3(3)
asn1-module(1) dedicated-hash-functions(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER -- alias
-- Synonyms --
id-scctc-algorithm OID ::= {iso(1) member-body(2) cn(156) scctc(10197) algorithm(1) }
id-sm3 OID ::= {id-scctc-algorithm sm3(401)}
-- Assignments --
id-dhf-sm3 OID ::= {id-scctc-algorithm sm3(401)}
HashFunctions ::= SEQUENCE {
algorithm ALGORITHM, &.id({HashFunctionAlgs}),
parameters ALGORITHM, &.Type({HashFunctionAlgs}{@algorithm}) OPTIONAL
}
HashFunctionAlgsALGORITHM ::= {
dhf-sm3,
... -- Expect additional algorithms --
}
dhf-sm3 ALGORITHM ::= { OID id-dhf-sm3 PARMS NullParms }
NullParms ::= NULL
-- Cryptographic algorithm identification --
ALGORITHM ::= CLASS {
&.id OBJECT IDENTIFIER UNIQUE,
&.Type OPTIONAL
}
WITH SYNTAX { OID&.id [PARMS &.Type] }
END -- DedicatedHashFunctions --
```

参 考 文 献

- [1] GB/T 15852.2 网络安全技术 消息鉴别码 第2部分:采用专门设计的杂凑函数的机制
 - [2] ISO/IEC 11770-6 Information technology—Security techniques—Key management—Part 6:
Key derivation
-

豪密科技 专用



版权声明

中国标准在线服务网(www.spc.org.cn)是中国标准出版社委托北京标科网络技术有限公司负责运营销售正版标准资源的网络服务平台,本网站所有标准资源均已获得国内外相关版权方的合法授权。未经授权,严禁任何单位、组织及个人对标准文本进行复制、发行、销售、传播和翻译出版等违法行为。版权所有,违者必究!

中 华 人 民 共 和 国
国 家 标 准
网络安全技术 杂凑函数
第 3 部分:专门设计的杂凑函数
GB/T 18238.3—2024

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)

网址: www.spc.net.cn

服务热线: 400-168-0010

2024 年 9 月第一版

*

书号: 155066 • 1-77541

版权专有 侵权必究

购买者: 豪密科技
时 间: 2025-04-09
定 价: 29 元



GB/T 18238.3-2024