



中华人民共和国国家标准

GB/T 18238.1—2024

代替 GB/T 18238.1—2000

网络安全技术 杂凑函数 第 1 部分：总则

Cybersecurity technology—Hash-functions—Part 1: General

(ISO/IEC 10118-1:2016, Information technology—Security techniques—
Hash-functions—Part 1: General, MOD)

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	III
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号	2
4.1 一般符号	2
4.2 编码约定	2
5 要求	2
6 杂凑函数的通用模型	3
6.1 概述	3
6.2 杂凑运算	3
6.2.1 通则	3
6.2.2 步骤 1(填充)	3
6.2.3 步骤 2(分割)	3
6.2.4 步骤 3(迭代)	3
6.2.5 步骤 4(输出变换)	3
6.3 通用模型的使用	4
附录 A(规范性) 填充方法	5
附录 B(资料性) 安全性注意事项	6
参考文献	7

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 1 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 18238.1—2000《信息技术 安全技术 散列函数 第 1 部分：概述》，与 GB/T 18238.1—2000 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了术语“无碰撞散列函数”为“抗碰撞杂凑函数”(见 3.4, 2000 年版的 2.1)；
- b) 更改了术语“散列码”为“杂凑值”(见 3.3, 2000 年版的 2.3)；
- c) 增加了“输出变换”“轮函数”等术语(见第 3 章)；
- d) 增加了符号 B_i 、 D_i 、 H_i 、 h 、 L_1 、 L_2 、 n 、 q 、 T 、 ϕ (见第 4 章)；
- e) 增加了“杂凑函数的通用模型”(见第 6 章)；
- f) 更改填充方法 2 为填充方法 1, 增加了填充方法 2; 并删除了填充方法 1(见 A.3, 2000 年版的附录 B)。

本文件修改采用 ISO/IEC 10118-1:2016《信息技术 安全技术 杂凑函数 第 1 部分：总则》。

本文件与 ISO/IEC 10118-1:2016 相比做了下述结构调整：

- 调整了术语“杂凑函数”和“抗碰撞杂凑函数”的顺序(见第 3 章)；
- 4.1 对应 ISO/IEC 10118-1:2016 的 4.1 和 4.2；
- 删除了 ISO/IEC 10118-1:2016 的附录 B, 将附录 C 调整为附录 B。

本文件与 ISO/IEC 10118-1:2016 的技术差异及其原因如下：

- 将“范围”中关于杂凑函数的介绍内容移至“引言”；
- 增加了规范性引用文件 GB/T 25069—2022(见第 3 章)；
- 增加了符号 n 表示分组密码的分组长度、 q 表示输入数据位串的分组个数(见第 4 章)；
- 将 ISO/IEC 10118-1:2016 中 3.4 的注移至第 5 章, 改为正文；
- 删除了规范性附录 B“ISO/IEC 10118(所有部分)采纳杂凑函数的原则”，因为该原则是 ISO 采纳各国算法提案所考虑的原则, 并不直接适用于具体各国规范自身的算法。

本文件做了下列编辑性改动：

- 为与我国技术标准体系协调, 标准名称更改为《网络安全技术 杂凑函数 第 1 部分：总则》；
- 纳入了 ISO/IEC 10118-1:2016/Amd.1:2021 的内容；
- 增加了术语“抗碰撞杂凑函数”“杂凑值”“杂凑函数”“初始化值”及“填充”的来源标准(见第 3 章)；
- 删除了术语“杂凑函数”“杂凑值”及“初始化值”的注, 更改了术语“轮函数”的注(见第 3 章)；
- 用资料性引用的 GB/T 18238(所有部分)替换了 ISO/IEC 10118(所有部分), 用 GB/T 18238.2 和 GB/T 18238.3 替换了 ISO/IEC 10118 的其他部分；
- 删除了资料性附录 B 中 B.3 的示例 1(见 ISO/IEC 10118-2:2016 的附录 C)；
- 删除了 ISO/IEC 10118-1:2016/Amd.1:2021 的填充方法 3, 因为本系列文件规定的杂凑函数

未使用该填充方法。

——更改了参考文献。

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、电子技术标准化研究院、中国电子科技集团公司第十五研究所、中国科学院信息工程研究所、中国科学院软件研究所、中国科学院大学、山东大学、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、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、北京江南天安科技有限公司、智巡密码(上海)检测技术有限公司等、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、李彦峰、李艳俊、毛颖颖、李世敏、黄晶晶、史丹萍、睦晗、孙思维、王鹏、王薇、王丹丹、杜志强、王提、杨波、郑强、龚晓燕、马洪富、曾光、李雪雁、韩玮、潘文伦、贾世杰、熊云、杨慧慧。

本文件及其所代替文件的历次版本发布情况为:

——2000年首次发布为GB/T 18238.1—2000;

——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。杂凑函数通常用于:

- 将消息压缩为摘要,用于数字签名机制的输入;
- 向用户承诺一个给定的位串,而不泄露该位串。

注: GB/T 18238(所有部分)中规定的杂凑函数不涉及密钥的使用。但是,这些杂凑函数与密钥搭配使用,以构建消息鉴别码(Message Authentication Code, MAC)。消息鉴别码提供数据源鉴别和消息完整性保护。

GB/T 15852.2给出了杂凑函数计算 MAC 的技术。

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 1 部分：总则

1 范围

本文件规定了杂凑函数的要求和通用模型,描述了杂凑运算的四个步骤,并给出了通用模型的使用方法。

本文件包含 GB/T 18238(所有部分)所共用的定义、符号和要求。

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 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

杂凑函数 **hash-function**

将任意长位串映射为定长位串的函数,满足下列性质:

- 给定一个输出位串,寻找一个输入位串来产生该输出位串,在计算上不可行;
- 给定一个输入位串,寻找另一个不同的输入位串来产生相同的输出位串,在计算上不可行。

[来源:GB/T 25069—2022,3.505]

3.2

数据串 **data string**

杂凑函数的输入位串。

3.3

杂凑值 **hash value**

密码杂凑运算的结果。

[来源:GB/T 25069—2022,3.764]

3.4

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

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是不可行的。

注:计算可行性依赖于特定安全要求和环境。

[来源:GB/T 25069—2022,3.322,有修改]

3.5

初始化值 **initialization value**

在密码变换中,为增强安全性或使密码设备同步而引入的用于数据变换的起始数据。