



中华人民共和国国家标准

GB/T 15852.2—2024

代替 GB/T 15852.2—2012

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

Cybersecurity technology—Message authentication codes
(MACs)—Part 2: Mechanisms using a dedicated hash-function

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	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号	3
5 用户使用要求	4
6 MAC 算法 1(MD _x -MAC)	4
6.1 通则	4
6.2 MAC 算法 1 的描述	4
6.2.1 通则	4
6.2.2 步骤 1(密钥扩展)	5
6.2.3 步骤 2(修改常数和初始值)	5
6.2.4 步骤 3(杂凑操作)	5
6.2.5 步骤 4(输出变换)	5
6.2.6 步骤 5(截断操作)	5
6.3 效率	5
7 MAC 算法 2(HMAC)	6
7.1 通则	6
7.2 MAC 算法 2 的描述	6
7.2.1 通则	6
7.2.2 步骤 1(密钥扩展)	6
7.2.3 步骤 2(杂凑操作)	6
7.2.4 步骤 3(输出变换)	6
7.2.5 步骤 4(截断操作)	6
7.3 效率	6
8 MAC 算法 3(MD _x -MAC 的变种)	7
8.1 通则	7
8.2 MAC 算法 3 的描述	7
8.2.1 通则	7
8.2.2 步骤 1(密钥扩展)	7
8.2.3 步骤 2(修改常数和初始值)	7
8.2.4 步骤 3(填充)	7

8.2.5	步骤 4(应用轮函数)	8
8.2.6	步骤 5(截断操作)	8
8.3	效率	8
9	常数的计算	8
9.1	概述	8
9.2	SM3 密码杂凑函数	8
附录 A (资料性)	MAC 算法的安全性分析	9
附录 B (规范性)	对象标识符	11
附录 C (资料性)	测试向量	13
参考文献	17

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 15852 的第 2 部分。GB/T 15852 已经发布了以下部分：

- 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制；
- 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；
- 信息技术 安全技术 消息鉴别码 第 3 部分：采用泛杂凑函数的机制。

本文件代替 GB/T 15852.2—2012《信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制》，与 GB/T 15852.2—2012 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加了术语“熵”“输入数据位串”“安全性强度”及定义，更改了术语“杂凑函数”“填充”“初始值”“轮函数”“分组”“字”的定义，删除了术语“抗碰撞杂凑函数”“消息比特串”（见第 3 章，2012 年版的第 3 章）；
- b) 删除了符号 D' ，更改了符号 \bar{h} 、 K' 、 K_0 、 K_1 、 K_2 、 \bar{K} 、 \bar{K}_1 、 \bar{K}_2 、 R 、 S_0 、 S_1 、 S_2 、 T_0 、 T_1 、 T_2 、 U_0 、 U_1 、 U_2 、 ϕ' 、 $K_1[i]$ 、 H 的定义，增加了符号 ω 、 $\lceil \rceil$ （见第 4 章，2012 年版的第 4 章）；
- c) 更改了可选的杂凑函数的范围，并更改了算法描述中采用专门设计的杂凑函数的说明和常数的计算（见第 5 章～第 9 章，2012 年版的第 5 章～第 9 章）；
- d) 增加了关于 MAC 值和输入数据串长度限制的说明（见第 5 章）；
- e) 增加了 MAC 算法通则，增加了 MAC 算法密钥长度、输入数据位串长度的说明（见 6.1、7.1、8.1）；
- f) 增加了 MAC 算法描述的通则和步骤标注（见 6.2、7.2、8.2）；
- g) 增加了采用 SM3 密码杂凑算法的 MAC 算法 1 和 MAC 算法 3 的描述和相应的常数计算（见第 6 章～第 9 章）；删除了采用其他专门设计的杂凑函数的描述和相应的常数计算（见 2012 年版的第 6 章～第 9 章）
- h) 更改了关于 MAC 算法 2 的安全证明的说明（见附录 A，2012 年版的附录 B）。

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：中国科学院软件研究所、中电科网络安全科技股份有限公司、中国科学院大学、国家密码管理局商用密码检测中心、桂林电子科技大学、广西网信信息技术有限公司、格尔软件股份有限公司、兴唐通信科技有限公司、郑州信大捷安信息技术股份有限公司、北京时代新威信息技术有限公司、北京时代亿信科技股份有限公司、长扬科技（北京）股份有限公司、中国电子科技集团公司第十五研究所、浙江大华技术股份有限公司、陕西省信息化工程研究院、华为技术有限公司。

本文件主要起草人：吴文玲、眭晗、张立廷、刘丽敏、孙思维、罗鹏、毛颖颖、张蕾、郑雅菲、韦永壮、韦博华、郑强、蔡子凡、刘为华、王连强、刘伟丰、赵华、李艳俊、魏东、赵晓荣、曾光。

本文件及其所代替文件的历次版本发布情况为：

- 2012 年首次发布为 GB/T 15852.2—2012；
- 本次为第一次修订。

引 言

消息鉴别码能够保护数据的完整性,也能够验证数据的来源。采用专门设计的杂凑函数的消息鉴别码是指:在设计过程中,以专门设计的杂凑函数(如 SM3 等)或其轮函数为主要部件,通过一定的迭代机制形成的消息鉴别码。

GB/T 15852 拟分为以下部分。

- 第 1 部分:采用分组密码的机制。目的在于规定采用分组密码的消息鉴别码。
- 第 2 部分:采用专门设计的杂凑函数的机制。目的在于规定采用专门设计的杂凑函数的消息鉴别码。
- 第 3 部分:采用泛杂凑函数的机制。目的在于规定采用泛杂凑函数的消息鉴别码。

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

1 范围

本文件规定了采用专门设计的杂凑函数的消息鉴别码(MAC)的用户使用要求,提供了 3 种采用专门设计的杂凑函数的消息鉴别码算法。

注 1: 这些消息鉴别码算法能用于数据完整性检验,检验数据是否被非授权地改变。

本文件适用于安全体系结构、过程及应用的安全服务。

注 2: 本文件定义的第一个 MAC 算法通常被称作 MD_x-MAC。它调用一次完整的杂凑函数,但对其中的轮函数做了细微的修改,把一个密钥加到了轮函数的附加常数上。第二个 MAC 算法通常被称作 HMAC,它调用两次完整的杂凑函数。第三个 MAC 算法是 MD_x-MAC 的一个变种,它限制输入长度不大于 256 位。在只处理较短输入的情况下,它有更好的性能。

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 18238.3—2024 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 25069—2022 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—2022 界定的以及下列术语和定义适用于本文件。

3.1

熵 **entropy**

封闭系统中无序性、随机性或可变性的度量。

注: 随机变量 X 的熵是观察 X 所获得的信息量的量化度量。

[来源:ISO/IEC 18031:2011,3.11]

3.2

杂凑函数 **hash-function**

将任意长的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,有修改]

3.3

输入数据位串 **input data string**

输入 MAC 算法的位串。