ICS 35.030
CCS L 80

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

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$\overline{h}$、K'、K_0、K_1、K_2、$\overline{K}$、$\overline{K_1}$、$\overline{K_2}$、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w、$\lceil\ \rceil$（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MDx-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MDx-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。