ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 18238.2—2024
代替 GB/T 18238.2—2002

网络安全技术　杂凑函数
第 2 部分:采用分组密码的杂凑函数

Cybersecurity technology—Hash-functions—Part 2: Hash-functions using a block cipher

(ISO/IEC 10118-2:2010, Information technology—Security techniques—Hash-functions—Part 2: Hash-functions using an n-bit block cipher, 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

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2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 18238.2—2002《信息技术　安全技术　散列函数　第2部分：采用n位块密码的散列函数》，与GB/T 18238.2—2002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“分组”（见3.1）；

b) 增加了杂凑函数的概述（见6.1）；

c) 更改散列函数3为杂凑函数2，更改散列函数4为杂凑函数3，并删除散列函数2（见第7章、第8章，2002年版的第7章、第8章、第9章）。

本文件修改采用ISO/IEC 10118-2:2010《信息技术　安全技术　杂凑函数　第2部分：采用n位块密码的杂凑函数》。

本文件与ISO/IEC 10118-2:2010相比做了下述结构调整：

——第7章对应ISO/IEC 10118-2:2010的第8章；

——第8章对应ISO/IEC 10118-2:2010的第9章。

本文件与ISO/IEC 10118-2:2010的技术差异及其原因如下：

——增加了规范性引用文件GB/T 25069—2022（见第3章）；

——更改了术语“n位分组密码”为“分组密码”，删除术语“轮函数”（见第3章）；

——增加了D、D_i、H、H_i、IV、L_1、L_2、L_X、n、q、T、$X \| Y$、$X \oplus Y$、$:=$、ϕ，完善了符号定义（见第4章）；

——删除了ISO/IEC 10118-2:2010规定的杂凑函数2，因该杂凑函数已被发现存在安全问题；并将ISO/IEC 10118-2:2010规定的杂凑函数3和杂凑函数4依次更改为本文件的杂凑函数2（见第7章）及杂凑函数3（见第8章），同时优化了描述逻辑（见第7章、第8章）；

——删除了规范性附录C，因为该附录给出的代码不适用于我国情况。

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2部分：采用分组密码的杂凑函数》；

——纳入了ISO/IEC 10118-2:2010/Cor 1:2011；

——增加了术语“分组”的注（见3.1）；

——增加了关于杂凑函数安全性提示的注释（见7.1、8.1）；

——更改了ISO/IEC第9章轮函数中笔误，将“与该杂凑函数相关的β的具体定义见8.1”更改为“与该杂凑函数相关的β的具体定义见7.5”（见第9章）；

——更改了资料性附录A，使用SM4分组密码算法替换了AES分组密码算法，以指导SM4算法的使用，将表A.1中“子函数i”更改为“密钥的前3位”，将表A.2中“子函数i”更改为“密钥的前4位”（见附录A）；

——更改了资料性附录 B,使用 SM4 分组密码算法给出了三种杂凑函数的示例(见附录 B);

——增加了资料性引用文件 GB/T 32907—2016(见附录 B);

——调整了部分语句(见 7.5、8.5),为方便阅读,对部分数据改用表格形式,并增加了表编号(见附录 B);

——调整了参考文献。

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、中国电子技术标准化研究院、中国科学院软件研究所、中国电子科技集团公司第十五研究所、山东大学、西安西电捷通无线网络通信股份有限公司、中国科学院信息工程研究所、中国科学院大学、北京银联金卡科技有限公司、山东得安信息技术有限公司、华为技术有限公司、格尔软件股份有限公司、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、北京信安世纪科技股份有限公司、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、李彦峰、眭晗、毛颖颖、李艳俊、李世敏、王薇、黄晶晶、张国强、史丹萍、王鹏、孙思维、孙晓峰、杨波、谭亦夫、王秉政、马洪富、曾光、郑强、韩玮、李雪雁、龚晓燕、潘文伦、贾世杰、熊云、张雪、刘赣秦、魏曼。

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 18238.2—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。采用分组密码的杂凑函数是指:在设计过程中,以分组密码算法(如 SM4 等)为主要部件,通过一定的迭代机制形成的杂凑函数。

GB/T 18238《网络安全技术　杂凑函数》由 3 个部分组成。

——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2部分：采用分组密码的杂凑函数

1　范围

本文件规定了三种采用(n 位)分组密码的杂凑函数。第一种杂凑函数提供长度不大于 n 位的杂凑值，第二种杂凑函数提供 $2n$ 位的杂凑值，第三种杂凑函数提供 $3n$ 位的杂凑值。

本文件适用于采用分组密码的杂凑函数的设计、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)

注：GB/T 18238.1—2024 被引用的内容与 ISO/IEC 10118-1：2000 被引用的内容没有技术上的差异。

GB/T 25069—2022　信息安全技术　术语

3　术语和定义

GB/T 25069—2022 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

分组　block

作为一个单位记录或传输的元素序列。

注：这里的元素是字符、字或记录。

[来源：GB/T 25069—2022，3.354]

3.2

分组密码　block cipher

加密算法在明文分组(即界定了长度的位串)上运算，以此产生密文分组的对称加密系统。

[来源：GB/T 25069—2022，3.161]

4　符号

下列符号适用于本文件。

B^L：当 n 为偶数时，n 位串 B 的最左边的 $n/2$ 位位串；当 n 为奇数时，n 位串 B 的最左边 $(n+1)/2$ 位位串。

B^R：当 n 为偶数时，n 位串 B 的最右边的 $n/2$ 位位串；当 n 为奇数时，n 位串 B 的最右边 $(n-1)/2$ 位位串。

B_i：当 B 是由多个 m 位字构成的序列时，B_i $(i\geqslant 0)$ 表示 B 的第 i 个 m 位字。特别地，当 $m=8$