

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 18238.3-2024

Replacing GB/T 18238.3-2002

**Cybersecurity technology - Hash-functions - Part 3: Dedicated
hash-functions**

网络安全技术 杂凑函数 第3部分：专门设计的杂凑函数

(English Translation)

Issued on: September 29, 2024

Implemented on: April 1, 2025

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Symbols
5 Requirements
6 Model of specially designed hash functions
6.1 Use of the general model
6.2 Round Function Model
7 Hash function SM3
7.1 Overview
7.2 Parameter Selection
7.3 Filling method
7.4 Initialization Value
7.5 Round Function
7.6 Output Transformation
Appendix A (Normative) Object Identifier
References

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document is part 3 of GB/T 18238 "Network Security Technology Hash Function". GB/T 18238 has published the following part.

--- Part 1: General;

--- Part 2: Hash functions using block ciphers;

--- Part 3: Specially designed hash functions.

This document replaces GB/T 18238.3-2002 "Information technology security techniques - Hash functions - Part 3: Special hash functions Compared with GB/T 18238.3-2002, in

addition to structural adjustments and editorial changes, the main technical changes are as follows.

- a) The terms "block", "hash function identifier", "round robin function", "word" and their definitions (see Chapter 3 of the 2002 edition) are deleted;
- b) Added the term "byte" (see Chapter 3);
- c) Deleted Special Hash Function 1, Special Hash Function 2 and Special Hash Function 3 (see Chapter 7, Chapter 8 and Chapter 9);
- d) Added hash function SM3 (see Chapter 7);
- e) Changed Appendix A Instance to Appendix A Object Identifier (see Appendix A, Appendix A of the 2002 Edition).

Introduction

A hash function uses a specific algorithm to map a bit string of arbitrary length (usually with an upper limit) to a bit string of fixed length.

A hash function refers to a hash function that is directly designed during the design process without relying on other cryptographic primitives (such as block ciphers, etc.).

GB/T 18238 "Network Security Technology Hash Function" consists of three parts.

--- Part 1: General. The purpose is to specify the requirements and general model of hash functions to guide other part.

--- Part 2: Hash functions for block ciphers. The purpose is to specify hash functions for block ciphers.

--- Part 3: Specially designed hash functions. The purpose is to specify specially designed hash functions.

Network security technology hash function Part 3: Specially designed hash functions

1 Scope

This document specifies the requirements and models for specially designed hash functions.

This document applies to the design, development, and testing of specially designed hash functions.

2 Normative references

The contents of the following documents constitute essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

GB/T 18238.1-2024 Network security technology hash functions Part 1: General (ISO/IEC 10118-1:2016, MOD) GB/T 25069 Information security technical terms GB/T 32905-2016 Information security technology SM3 cryptographic hash algorithm

3 Terms and definitions

The terms and definitions defined in GB/T 25069 and GB/T 18238.1-2024 and the following apply to this document.

byte

A bit string consisting of 8 consecutive bits.

4 Symbols

The following symbols apply to this document.

B_i . the i -th byte of B .

D . Data.

H . hash value.

IV . Initialization value.

LX . The length of bit string X in bits.

$L1$. The length of the first bit string in the two bit strings input to the round function ϕ .

$L2$. The bit length of the second bit string of the two bit strings input to the round function ϕ , which is also the bit length of the output value of the round function ϕ , and the initial the bit length of the initialization value IV .

r . The bit length of the reserved bit string in the padding method.

5 Requirements

Users of the hash functions in this document should choose.