

ICS 35.030
CCS L 80



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

GB/T 18238.1-2024

Replacing GB/T 18238.1-2000

Cybersecurity technology - Hash-functions - Part 1: General

网络安全技术 杂凑函数 第1部分：总则

(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	
4.1 General symbols	
4.2 Coding Conventions	
5 Requirement	
6 General Model of Hash Function	
6.1 Overview	
6.2 Hash Operation	
6.2.1 General	
6.2.2 Step 1 (filling)	
6.2.3 Step 2 (Segmentation)	
6.2.4 Step 3 (Iteration)	
6.2.5 Step 4 (Output Transformation)	
6.3 Use of the general model	
Appendix A (Normative) Filling Method	
Appendix B (Informative) Safety Precautions	
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 1 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 18238.1-2000 "Information technology security techniques - Hash functions - Part 1: Overview" and Compared with GB/T 18238.1-2000, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

- a) Changed the term "collision-free hash function" to "collision-resistant hash function" (see 3.4, 2.1 of the 2000 edition);
- b) Changed the term "hash code" to "hash value" (see 3.3, 2.3 of the 2000 edition);
- c) Added terms such as "output transformation" and "round function" (see Chapter 3);
- d) Added symbols B_i , D_i , H_i , h , L_1 , L_2 , n , q , T , ϕ (see Chapter 4);
- e) Added "General Model of Hash Functions" (see Chapter 6);
- f) Change Filling Method 2 to Filling Method 1, add Filling Method 2; and delete Filling Method 1 (see A.3, 2000 Edition) Appendix B).

This document is modified to adopt ISO/IEC 10118-1:2016 "Information technology security techniques - Hash functions - Part 1: General principles".

This document has the following structural adjustments compared to ISO/IEC 10118-1:2016.

- Adjusted the order of the terms "hash function" and "anti-collision hash function" (see Chapter 3);
- 4.1 corresponds to 4.1 and 4.2 of ISO/IEC 10118-1:2016;
- Deleted Appendix B of ISO/IEC 10118-1:2016 and adjusted Appendix C to Appendix B.

The technical differences between this document and ISO/IEC 10118-1:2016 and their reasons are as follows.

- Move the introduction about hash functions in "Scope" to "Introduction";
- Added normative reference document GB/T 25069-2022 (see Chapter 3);
- Added the symbol n to represent the block length of the block cipher and q to represent the number of blocks of the input data bit string (see Chapter 4);
- Move the note to 3.4 of ISO/IEC 10118-1:2016 to Chapter 5 and change it to the main text;
- Deleted the normative Annex B "Principles for adopting hash functions in ISO/IEC 10118 (all parts)" because this principle is the principles considered by ISO in adopting algorithm proposals from various countries are not directly applicable to the algorithms that specific countries regulate themselves.

The following editorial changes were made to this document.

- In order to coordinate with my country's technical standard system, the name of the standard is changed to "Network Security Technical Hash Function Part 1: General Principles";
- Incorporated the contents of ISO/IEC 10118-1:2016/Amd.1.2021;
- Added the source standard for the terms "collision-resistant hash function", "hash value", "hash function", "initialization value" and "padding" (see Section 3 chapter);
- Deleted the notes to the terms "hash function", "hash value" and "initialization value", and changed the note to the term "round function" (see Chapter 3);
- Replaced ISO/IEC 10118 (all parts) with the informative reference GB/T 18238 (all parts), GB/T 18238.2 and GB/T 18238.3 replace other parts of ISO/IEC 10118;
- Deleted Example 1 of B.3 in informative Appendix B (see Appendix C of ISO/IEC 10118-2:2016);
- Deleted the padding method 3 of ISO/IEC 10118-1:2016/Amd.1.2021, because the hash function specified in this series of documents this fill method is not used.
- Changed references.

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.

Commonly used for.

- Compress the message into a digest for input into the digital signature mechanism;
- Promise a given bit string to the user without revealing the bit string.

Note: The hash functions specified in GB/T 18238 (all parts) do not involve the use of keys. However, these hash functions are used in conjunction with keys to construct messages.

GB/T 15852.2 provides the technology of calculating MAC using hash function.

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 1: General

1 Scope

This document specifies the requirements and general model for hash functions, describes the four steps of hashing, and gives the use of the general model.

method.

This document contains the definitions, symbols and requirements common to GB/T 18238 (all parts).

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 25069-2022 Information Security Technical Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

Hash-function

A function that maps a bit string of arbitrary length to a bit string of fixed length satisfies the following properties.

---Given an output bit string, it is computationally infeasible to find an input bit string that produces the output bit string;

---Given an input bit string, it is computationally infeasible to find another different input bit string that produces the same output bit string.

[Source. GB/T 25069-2022, 3.505] 3.2 data string the input bit string to the hash function.

Hash value

The result of a cryptographic hash operation.

[Source. GB/T 25069-2022, 3.764] 3.4 collision-resistant hash-function A hash function that satisfies the property that it is computationally infeasible to find any two different inputs that map to the same output.

NOTE: Computational feasibility depends on specific safety requirements and environment.