

ICS 35.030
CCS L 80



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

GB/T 18238.2-2024

Replacing GB/T 18238.2-2002

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

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

(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 Use of the general model	
6 Hash function 1	
6.1 Overview	
6.2 Parameter Selection	
6.3 Filling method	
6.4 Initialization Value	
6.5 Round Function	
6.6 Output Transformation	
7 Hash function 2	
7.1 Overview	
7.2 Parameter Selection	
7.3 Filling Method	
7.4 Initialization Value	
7.5 Round Function	
7.6 Output Transformation	
8 Hash function 3	
8.1 Overview	
8.2 Parameter selection	
8.3 Filling method	
8.4 Initialization Value	
8.5 Round Function	
8.6 Output Transformation	
Appendix A (Informative) Definition of initialization value and transformation u10	
Appendix B (Informative) Example	
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 2 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 18238.2-2002 "Information technology security techniques - Hash functions - Part 2: Hash functions using n-bit block ciphers" Compared with GB/T 18238.2-2002, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

- a) Added the term "group" (see 3.1);
- b) Added an overview of hash functions (see 6.1);
- c) Change hash function 3 to hash function 2, change hash function 4 to hash function 3, and delete hash function 2 (see Chapter 7, 8 of the 2002 edition, and Chapters 7, 8, and 9 of the 2002 edition).

This document is modified to adopt ISO/IEC 10118-2:2010 "Information technology security techniques - Hash functions - Part 2: Using n-bit Hash Functions for Block Ciphers.

This document has the following structural adjustments compared to ISO/IEC 10118-2:2010.

- Chapter 7 corresponds to Chapter 8 of ISO/IEC 10118-2:2010;
- Chapter 8 corresponds to Chapter 9 of ISO/IEC 10118-2:2010.

The technical differences between this document and ISO/IEC 10118-2:2010 and their reasons are as follows.

- Added normative reference document GB/T 25069-2022 (see Chapter 3);
- Changed the term "n-bit block cipher" to "block cipher" and deleted the term "round function" (see Chapter 3);
- Added D, Di, H, Hi, IV, L1, L2, LX, n, q, T, X||Y, X (+)Y, ., =, phi, and improved the symbol definitions (see Chapter 4);
- Deleted the hash function 2 specified in ISO/IEC 10118-2:2010, because the hash

function has been found to have security issues; and Change the hash functions 3 and 4 specified in ISO/IEC 10118-2:2010 to hash functions 2 of this document.

(see Chapter 7) and hash function 3 (see Chapter 8), and optimized description logic (see Chapters 7 and 8);

--- Deleted the normative Appendix C because the code given in this appendix is not applicable to my country.

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 was changed to "Network Security Technology Hash Function Part 2: Using Segmentation Hash functions for group ciphers";

--- Incorporated ISO/IEC 10118-2:2010/Cor1.2011;

--- Added the note for the term "group" (see 3.1);

--- Added notes on the security of hash functions (see 7.1, 8.1);

--- Corrected the typo in ISO/IEC Chapter 9 Round Function, changing "For the specific definition of beta related to the hash function, see 8.1" to "The specific definition of beta associated with this hash function is given in 7.5" (see Chapter 9);

--- Changed the informative Appendix A, replaced the AES block cipher algorithm with the SM4 block cipher algorithm to guide the SM4 algorithm in Table A.1, "sub-function i" is changed to "the first 3 bits of the key", and in Table A.2, "sub-function i" is changed to "the first 3 bits of the key".

The first 4 digits" (see Appendix A);

--- Changed the informative Appendix B, and gave examples of three hash functions using the SM4 block cipher algorithm (see Appendix B);

--- Added the informative reference document GB/T 32907-2016 (see Appendix B);

--- Adjusted some statements (see 7.5, 8.5), changed some data to table format for easier reading, and added table numbers (see Appendix Record B);

---Adjusted references.

Introduction

The 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.

The hash function of the code refers to. in the design process, the block cipher algorithm (such as SM4, etc.) is used as the main component, and a certain iterative mechanism is used to form the hash function of.

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 2: Hash functions using block ciphers

1 Scope

This document specifies three hash functions for use with (n-bit) block ciphers. The first hash function provides a hash of length no greater than n bits.

The first hash function provides a 2n-bit hash value, the second hash function provides a 2n-bit hash value, and the third hash function provides a 3n-bit hash value.

This document applies to the design, development, and testing of hash functions employed in block ciphers.

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) Note. There is no technical difference between the referenced content of GB/T 18238.1-2024 and the referenced content of ISO/IEC 10118-1:2000.

GB/T 25069-2022 Information Security Technical Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and GB/T 18238.1-2024 and the following apply to this document.

Grouping blocks

A sequence of elements recorded or transmitted as a unit.

Note: Here, elements are characters, words or records.