

ICS 35.030
CCS L 80



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

GB/T 15852.2-2024

Replacing GB/T 15852.2-2012

**Cybersecurity technology - Message authentication
codes(MACs) - Part 2: Mechanisms using a dedicated
hash-function**

(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 User Requirements	
6 MAC algorithm 1 (MDx-MAC)	
6.1 General	
6.2 Description of MAC Algorithm 1	
6.2.1 General	
6.2.2 Step 1 (Key Expansion)	
6.2.3 Step 2 (Modify constants and initial values)	
6.2.4 Step 3 (Hash Operation)	
6.2.5 Step 4 (Output Transformation)	
6.2.6 Step 5 (Truncation Operation)	
6.3 Efficiency	
7 MAC algorithm 2 (HMAC)	
7.1 General	
7.2 Description of MAC Algorithm 2	
7.2.1 General	
7.2.2 Step 1 (Key Expansion)	
7.2.3 Step 2 (Hash Operation)	
7.2.4 Step 3 (Output Transformation)	
7.2.5 Step 4 (Truncation Operation)	
7.3 Efficiency	
8 MAC algorithm 3 (variant of MDx-MAC)	
8.1 General	
8.2 Description of MAC Algorithm 3	
8.2.1 General	
8.2.2 Step 1 (Key Expansion)	
8.2.3 Step 2 (Modify constants and initial values)	

8.2.4 Step 3 (Filling)
8.2.5 Step 4 (applying the round function)
8.2.6 Step 5 (Truncation Operation)
8.3 Efficiency
9 Calculation of constants
9.1 Overview
9.2 SM3 cryptographic hash function
Appendix A (Informative) Security Analysis of MAC Algorithm
Appendix B (Normative) Object Identifiers
Appendix C (Informative) Test Vector
Reference

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 15852. GB/T 15852 has been published in the following parts.

- Information technology security techniques Message authentication code Part 1: Mechanisms using block ciphers;
- Network security technology Message authentication code Part 2: Mechanism using specially designed hash functions;
- Information technology security techniques Message authentication code Part 3: Mechanisms using generalized hash functions.

This document replaces GB/T 15852.2-2012 "Information technology security technology message authentication code Part 2: Using dedicated hash Compared with GB/T 15852.2-2012, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

- a) Added the terms "entropy", "input data bit string", "security strength" and their definitions, and changed the terms "hash function", "padding", "initialization" and "initialization" the definitions of "value", "round function", "group", and "word" have been changed, and the terms "collision-resistant hash function" and "message bit string" have been deleted (see Chapter 3, 2012 Chapter 3 of the 2001 edition);
- b) The symbol D' was deleted, and the symbols h , K' , K_0 , K_1 , K_2 , K , K_1 , K_2 , R , S_0 , S_1 , S_2 ,

T0, T1, T2, U0, U1, the definitions of U2, ϕ_i' , $K1[i]$, and H are updated with the symbol w, (see Chapter 4, Chapter 4 of the 2012 edition);

c) Changed the range of optional hash functions, and changed the description and constants of specially designed hash functions in the algorithm description Calculation (see Chapters 5 to 9, Chapters 5 to 9 of the 2012 edition);

d) Added instructions on MAC value and input data string length limit (see Chapter 5);

e) Added the general rules for MAC algorithm, added the description of MAC algorithm key length and input data bit string length (see 6.1, 7.1, 8.1);

f) Added general rules and step annotations for MAC algorithm description (see 6.2, 7.2, 8.2);

g) Added descriptions of MAC Algorithm 1 and MAC Algorithm 3 using the SM3 cryptographic hash algorithm and the corresponding constant calculations (see Chapters 6 to 9); Deleted the description of other specially designed hash functions and the corresponding constant calculations (see 2012 Chapter 6 to Chapter 9 of the version)

h) Changed the description of the security proof of MAC algorithm 2 (see Appendix A, Appendix B of the 2012 edition).

Introduction

Message authentication codes can protect the integrity of data and verify the source of data.

The code is. in the design process, a specially designed hash function (such as SM3, etc.) or its round function is used as the main component, through a certain number of iterations the message authentication code formed by the mechanism.

GB/T 15852 is intended to be divided into the following parts.

--- Part 1: Mechanisms using block ciphers. The purpose is to specify message authentication codes using block ciphers.

--- Part 2: Mechanisms using specially designed hash functions. The purpose is to specify the message using specially designed hash functions Identification code.

--- Part 3: Mechanisms using generalized hash functions. The purpose is to specify message authentication codes using generalized hash functions.

Network security technology message authentication code Part 2: Mechanisms using specially designed hash functions

1 Scope

This document specifies the user requirements for message authentication codes (MACs) using specially designed hash functions.

A message authentication code algorithm based on a hash function designed by the gate.

NOTE 1 These message authentication algorithms can be used to verify data integrity and to check whether data has been altered in an unauthorized manner.

This document applies to security architectures, processes and application security services.

Note 2: The first MAC algorithm defined in this document is usually called MDx-MAC. It calls the complete hash function once, but does a the second MAC algorithm is usually called HMAC, which calls the third MAC algorithm is a variant of MDx-MAC, which limits the input length to no more than 256 bits.

In case of short input, it has better performance.

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 18238.3-2024 Network security technology hash functions Part 3: Specially designed hash functions GB/T 25069-2022 Information Security Technical Terminology GB/T 32905-2016 Information security technology SM3 cryptographic hash algorithm

3 Terms and definitions

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

Entropy

A measure of disorder, randomness, or variability in a closed system.

Note: The entropy of a random variable X is a quantitative measure of the amount of information obtained by observing X .

[Source. ISO/IEC 18031:2011, 3.11] 3.2 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