ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 15852.3-2019

Information technology -- Security techniques -- Message authentication codes (MACs) -- Part 3: Mechanisms using a universal hash-function

Issued on: August 30, 2019 **Implemented on: March 1, 2020**

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

Table of Contents

Foreword

GB/T 15852 "Information Technology Security Technology Message Authentication Code" is divided into the following three parts.

--- Part 1. The mechanism of using block ciphers;

--- Part 2. Mechanisms using dedicated hash functions;

--- Part 3. The mechanism of using a ubiquitous function.

This part is the third part of GB/T 15852.

This part is drafted in accordance with the rules given in GB/T 1.1-2009.

This section uses the redrafting method to modify the use of ISO /IEC 9797-3.2011 "Information Technology Security Technology Message Authentication Code No. 3

Part. The mechanism of using a general hash function.

This section has a structural change compared to ISO /IEC 9797-3.2011, adjusting 6.3.3.1 to 6.3.3 and 6.5.3.1 to 6.5.3.

The main technical differences between this part and ISO /IEC 9797-3.2011 and their reasons are as follows.

---About the normative reference documents, this part has made technical adjustments to adapt to China's technical conditions, adjustments

The situation is reflected in Chapter 2, "Regulatory Citations", and the specific adjustments are as follows.

* Replace ISO /IEC 9797-1 with GB/T 15852.1-2008 equivalent to the international standard;

* Removed ISO /IEC 18031, ISO /IEC 18033-3, ISO /IEC 18033-4;

* Added GB/T 32907-2016, GB/T 33133.1-2016, GB/T 36624-2018.

--- In Chapter 3, two general terms and definitions of keys and prime numbers have been

removed.

--- Add abbreviations in Chapter 4.

--- In 6.3.1, according to the ZUC algorithm's requirement for the initial vector, the Badger's 64-bit all-one initial vector is modified to 128 bits.

All 1 initial vector.

--- Remove the canonical Appendix A object identifier (because the lack of a domestic related object identifier definition).

This section has made the following editorial changes.

---Adjustment of informative Appendix B is informative Appendix A, listing the MAC algorithm based on the ZUC or SM4 algorithm at the bottom.

Test vector

---Adjustment of informative Appendix C is informative Appendix B, introducing the security information of the general hash function;

--- Increase the informative Appendix C, introducing the anti-attack capabilities of the ZUC and SM4 algorithms.

1 Scope

This part of GB/T 15852 specifies four message authentication code algorithms using the ubiquitous function. UMAC, Badger, Poly1305

And GMAC. These algorithms are based on the sequence cipher algorithm specified in GB/T 33133.1-2016 and the provisions of GB/T 32907-2016.

a block cipher algorithm, or other sequence cipher algorithm and block cipher algorithm that conforms to national regulations, using a key and a general hash function

The number is processed into a bit string of length m bits, and a bit string of length n bits is output as a MAC.

This section applies to security services for security architectures, processes, and applications. These algorithms can be used as data integrity mechanisms for inspection

Check if the data has been changed in an unauthorized manner. It can also be used as a message authentication mechanism to ensure that the message comes from the entity that owns the key.

The strength of the data integrity mechanism and the message authentication mechanism is determined by the following criteria. the length of the key (in bits) and the confidentiality, the hash function

The length of the raw hash code (in bits), the strength of the hash function, the length of the MAC (in bits), and the specific mechanism.

Note. The general framework for providing integrity services is specified in ISO /IEC 10181-6 [7].

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article.

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 15852.1-2008 Information technology security technology message authentication code - Part 1.

(ISO /IEC 9797-1.1999, IDT)

GB/T 32907-2016 Information Security Technology SM4 Block Cipher Algorithm

GB/T 33133.1-2016 Information security technology Zu Chongzhi sequence cipher algorithm Part 1. Algorithm description

GB/T 36624-2018 Information technology security technology identifiable encryption mechanism

3 Terms and definitions

The following terms and definitions as defined in GB/T 15852.1-2008 apply to this document.

3.1

Empty string emptystring

A bit string of zero length.

3.2

Temporary value nonce

A value that is used once to provide fresh input to the MAC algorithm.

3.3

Tag tag

As a result of the MAC algorithm, a possible encrypted message is appended to provide integrity protection.

3.4

Pan-heavy function universalhash-function

A mapping established by a key, mapping a arbitrarily long bit string within a certain range to a fixed length bit string, satisfying. for all different inputs,