ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15852.3—2019

信息技术　安全技术　消息鉴别码 第3部分:采用泛杂凑函数的机制

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

(ISO/IEC 9797-3:2011, MOD)

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 2
4.1　符号 …… 2
4.2　缩略语 …… 4
5　一般模型 …… 4
6　机制 …… 5
6.1　概述 …… 5
6.2　UMAC …… 5
6.3　Badger …… 10
6.4　Poly1305 …… 13
6.5　GMAC …… 15
附录 A（资料性附录）　测试向量 …… 17
附录 B（资料性附录）　泛杂凑函数的安全性信息 …… 20
附录 C（资料性附录）　ZUC 和 SM4 算法的抗攻击能力 …… 21
参考文献 …… 22

前　言

GB/T 15852《信息技术　安全技术　消息鉴别码》分为以下3个部分：

——第1部分：采用分组密码的机制；

——第2部分：采用专用杂凑函数的机制；

——第3部分：采用泛杂凑函数的机制。

本部分为GB/T 15852的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 9797-3:2011《信息技术　安全技术　消息鉴别码　第3部分：采用泛杂凑函数的机制》。

本部分与ISO/IEC 9797-3:2011相比存在结构变化，将6.3.3.1调整为6.3.3，6.5.3.1调整为6.5.3。

本部分与ISO/IEC 9797-3:2011的主要技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的GB/T 15852.1—2008代替了ISO/IEC 9797-1；
- 删除了ISO/IEC 18031、ISO/IEC 18033-3、ISO/IEC 18033-4；
- 增加了GB/T 32907—2016、GB/T 33133.1—2016、GB/T 36624—2018。

——在第3章中删除了密钥、素数两个常规性术语和定义。

——在第4章中增加缩略语部分。

——在6.3.1中根据ZUC算法对初始向量的要求，将Badger的64位全1初始向量修改为128位全1初始向量。

——删除规范性附录A对象标识符(因为缺少国内相关对象标识符定义)。

本部分做了下列编辑性修改：

——调整资料性附录B为资料性附录A，列举了在底层采用ZUC或SM4算法的MAC算法所生成的测试向量；

——调整资料性附录C为资料性附录B，介绍了泛杂凑函数的安全性信息；

——增加资料性附录C，介绍了ZUC和SM4算法的抗攻击能力。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：中国科学院软件研究所、中国科学院数据与通信保护研究教育中心、北京邮电大学、成都卫士通信息产业股份有限公司。

本部分主要起草人：张立廷、吴文玲、张蕾、眭晗、温巧燕、王鹏、金正平、彭真、秦体红。

信息技术　安全技术　消息鉴别码
第3部分：采用泛杂凑函数的机制

1　范围

GB/T 15852的本部分规定了4种采用泛杂凑函数的消息鉴别码算法：UMAC、Badger、Poly1305和GMAC。这些算法基于GB/T 33133.1—2016中规定的序列密码算法和GB/T 32907—2016中规定的分组密码算法，或符合国家规定的其他序列密码算法和分组密码算法，使用一个密钥和一个泛杂凑函数处理一个长度为 m 位的比特串，输出一个长度为 n 位的比特串作为MAC。

本部分适用于安全体系结构、进程及应用的安全服务。这些算法可以作为数据完整性机制，用于检验数据是否在未经授权的方式下被更改。也可以作为消息鉴别机制，确保消息来自于拥有密钥的实体。数据完整性机制和消息鉴别机制的强度由以下指标决定：密钥的长度（按比特）与保密性、泛杂凑函数产生的杂凑码的长度（按比特）、泛杂凑函数的强度、MAC的长度（按比特），以及具体的机制。

注：提供完整性服务的一般框架在ISO/IEC 10181-6[7]中指定。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 15852.1—2008　信息技术　安全技术　消息鉴别码　第1部分：采用分组密码的机制（ISO/IEC 9797-1：1999，IDT）

GB/T 32907—2016　信息安全技术　SM4分组密码算法

GB/T 33133.1—2016　信息安全技术　祖冲之序列密码算法　第1部分：算法描述

GB/T 36624—2018　信息技术　安全技术　可鉴别的加密机制

3　术语和定义

GB/T 15852.1—2008界定的以及下列术语和定义适用于本文件。

3.1

空串　empty string

长度为零的比特串。

3.2

临时值　nonce

使用一次的值，用于向MAC算法提供新鲜输入。

3.3

标签　tag

MAC算法的结果，附加一个可能的加密消息以提供完整性保护。

3.4

泛杂凑函数　universal hash-function

由密钥确立的映射，将一定范围内任意长比特串映射到定长比特串，满足：对于所有不同的输入，其