ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15852.1—2020
代替 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

Information technology—Security techniques—Message authentication codes—Part 1: Mechanisms using a block cipher

[ISO/IEC 9797-1:2011,Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms using a block cipher,MOD]

2020-12-14 发布　　2021-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

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1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替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》。

与GB/T 15852.1—2008相比，主要技术变化如下：

——删除了消息鉴别码算法用途的说明(见2008年版的第1章)；

——增加了MAC算法的常用名称指代(见第5章、第7章)；

——删除了规范性引用文件GB/T 9387.2—1995和GB/T 15843.1—2008(见2008年版的第2章)；

——增加了术语“初始变换”(见3.13)，修改了术语“输出变换”的定义，以适应修改后的MAC算法的一般模型(见3.14，2008年版的3.2.7)；

——增加了16个符号，修改了3个符号(见4.1，2008年版的第4章)；增加了“缩略语”(见4.2)；

——修改了第5章的标题，将“要求”改为“用户要求”；修改了用户选择密钥诱导方法的要求(见第5章，2008年版的第5章)；

——增加了使用MAC算法4时数据串长度的要求及使用MAC算法7时MAC的长度要求(见第5章)；

——修改了MAC算法的一般模型及“MAC算法模型”图，增加了密钥诱导和最终迭代操作，以适用于本部分规定的所有MAC算法(见6.1，2008年版的第6章)；

——增加了密钥诱导操作的概述与方法、最终迭代操作的概述与方法(见6.2、6.7)；增加了填充方法4、初始变换3(见6.3.5、6.5.4)；修改了迭代应用分组密码操作(见6.6，2008年版的6.4)；增加了截断操作的概述和截断操作2(见6.9)；修改和增加了操作方法在本部分所规定的MAC算法中的应用情况说明(见6.3.1、6.5.1、6.7.1、6.8.1、6.9.1，2008年版的6.1、6.3、6.5)；

——修改了MAC算法4的常用名称的注释，删除了采用DEA时密钥长度的说明(见7.5，2008年版的7.4)；

——修改了MAC算法5，替换为CMAC(见7.6，2008年版的7.5)；修改了MAC算法6，替换为LMAC(见7.7，2008年版的7.6)；

——增加了MAC算法7(TrCBC)和MAC算法8(CBCR)(见7.8、7.9)；

——修改了附录A“例子”的标题为“测试向量”；修改了使用的分组密码算法，将DEA修改为SM4分组密码算法；修改了明文、密钥、结果(见附录B，2008年版的附录A)；增加了MAC算法7和MAC算法8的测试向量(见B.8、B.9)；

——修改了表C.1中编号为1.2和4.2的算法效率；增加了MAC算法7和MAC算法8的安全性说明、算法的特性、安全强度估计(见附录C)。

本部分使用重新起草法修改采用 ISO/IEC 9797-1:2011《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》。

本部分与 ISO/IEC 9797-1:2011 相比在结构上有较多调整,附录 A 列出了本部分与 ISO/IEC 9797-1:2011 的章条编号对照一览表。

本部分与 ISO/IEC 9797-1:2011 的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:

- 删除引用 ISO 18033-3;
- 增加引用了 GB/T 17964—2008;

——修改了术语"消息鉴别码"的定义,增加了术语"初始变换"和定义(见第 3 章,ISO/IEC 9797-1:2011 的第 3 章);

——增加了"初始变换"等 4 个符号,以适应修改后的 MAC 算法的一般模型和第 7 章中定义的所有 MAC 算法(见 4.1);修改了赋值符号的定义,以简化描述(见 4.1,ISO/IEC 9797-1:2011 的第 4 章);增加了"缩略语",列举了本部分使用的 3 个缩略语(见 4.2);

——增加了 MAC 算法的常用名称指代,以便于管理和沟通(见第 5 章、第 7 章);

——修改了用户选择分组密码算法的要求,以适应我国密码管理的要求;修改了用户选择密钥诱导方法的要求,纠正国际标准中的错误;增加了使用 MAC 算法 7 时 MAC 长度的要求;修改关于密钥管理的信息为注释(见第 5 章,ISO/IEC 9797-1:2011 的第 5 章);

——修改了 MAC 算法的一般模型,增加了初始变换操作,并修改了"MAC 算法模型"图,修改后的一般模型可适用于本部分定义的所有 MAC 算法,解决了一般模型不适用于 MAC 算法 4 的问题(见 6.1,ISO/IEC 9797-1:2011 的 6.1);

——增加了初始变换的概述和方法,对应于一般模型的修改(见 6.5);修改了迭代应用分组密码操作的起始位置,以衔接初始变换,并删除不再适用的注释(见 6.6,ISO/IEC 9797-1:2011 的6.5);增加了最终迭代 4,用于 MAC 算法 8(见 6.7.5);增加了截断操作的概述和截断操作 2,用于 MAC 算法 7,并保持操作描述方式一致(见 6.9);

——修改了 MAC 算法在一般模型下的描述,以适应修改后的一般模型(见第 7 章,ISO/IEC 9797-1:2011 的第 7 章)

——删除了关于 MAC 算法采用非我国标准规定的分组密码算法时的说明,以适应我国密码管理要求(见 7.4、7.5,ISO/IEC 9797-1:2011 的 7.4、7.5);

——增加了 MAC 算法 7(TrCBC)和 MAC 算法 8(CBCR),补充性能良好的新算法(见 7.8、7.9)。

本部分做了下列编辑性修改:

——删除了 ISO/IEC 9797-1:2011 第 1 章中的关于密钥管理机制及对象标识符有关范围的说明;

——删除了 ISO/IEC 9797-1:2011 的附录 A"对象标识符";

——在附录 B.1 增加了资料性引用文件 GB/T 32907—2016;

——删除了 ISO/IEC 9797-1:2011 的附录 B 中关于 MAC 算法采用非我国标准规定的分组密码算法时的说明;

——修改了附录"例子"的标题为"测试向量";修改了使用的分组密码算法、明文、密钥、结果,使用我国标准规定的密码算法生成 MAC 算法的测试向量(见附录 B,ISO/IEC 9797-1:2011 的附录 B);增加了 MAC 算法 7 和 MAC 算法 8 的测试向量(见 B.8、B.9);

——修改了表 C.1 编号为 1.2 和 4.2 的算法效率,纠正国际标准中的错误(见附录 C,ISO/IEC

9797-1:2011 的附录 C);增加了 MAC 算法 7 和 MAC 算法 8 的安全性说明、算法的特性、安全强度估计(见附录 C);

——删除了 ISO/IEC 9797-1:2011 的 C.2,因方法及建议存在安全问题;

——删除了 ISO/IEC 9797-1:2011 的附录 D“与以前的 MAC 算法标准的比较”。

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、成都卫士通信息产业股份有限公司、桂林电子科技大学、国家密码管理局商用密码检测中心。

本部分主要起草人:吴文玲、眭晗、张立廷、张蕾、韦永壮、毛颖颖、郑雅菲、涂彬彬、刘仁章、丁勇、王玉珏、张众。

本部分所代替标准的历次版本发布情况为:

——GB/T 15852—1995;

——GB/T 15852.1—2008。

引　言

本部分定义了8种采用n比特分组密码的消息鉴别码算法(MAC算法):CBC-MAC、EMAC、ANSI retail MAC、MacDES、CMAC、LMAC、TrCBC、CBCR。

本部分定义的第一个MAC算法通常被称作CBC-MAC。其余七个MAC算法是CBC-MAC的变种。其中,MAC算法2、MAC算法3、MAC算法5、MAC算法6和MAC算法8在操作的末尾应用了特殊的变换。MAC算法4在操作的起始和末尾各应用了一个特殊的变换。MAC算法7在截取MAC值时使用特殊的规则。当MAC算法的密钥长度是分组密码密钥长度的两倍的时候,宜使用MAC算法4。MAC算法5和MAC算法7使用加密的次数最少。MAC算法5只需要一次分组密码密钥设置,但需要一个较长的中间密钥。MAC算法6是MAC算法2的可选变种。MAC算法7和MAC算法8不需要中间密钥和密钥设置,当存储空间受限时,建议使用MAC算法7和MAC算法8。

本部分凡涉及密码算法的相关内容,按国家有关法规实施;凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的宜遵循密码相关国家标准和行业标准。

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

1　范围

GB/T 15852的本部分规定了采用分组密码的消息鉴别码(MAC)的用户使用要求、算法一般模型,提供了8种采用分组密码的消息鉴别码算法。

本部分适用于安全体系结构、过程及应用的安全服务。

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 17964—2008　信息安全技术　分组密码算法的工作模式

3　术语和定义

下列术语和定义适用于本文件。

3.1

分组　block

长度为 n 的比特串。

3.2

密钥　key

控制密码变换操作的符号序列。

注:密码变换操作,例如加密、解密、密码校验函数计算、签名生成、签名验证。

[GB/T 15843.1—2017,定义3.16]

3.3

明文　plaintext

未加密的信息。

3.4

密文　ciphertext

为隐藏信息内容进行变换后的数据。

[GB/T 15843.1—2017,定义3.7]

3.5

分组密码密钥　block cipher key

控制分组密码运算的密钥。

3.6

***n* 比特分组密码　*n*-bit block cipher**

分组长度为 n 比特的分组密码。