ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15852.2—2012

信息技术　安全技术　消息鉴别码 第2部分：采用专用杂凑函数的机制

Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2: Mechanisms using a dedicated hash-function

(ISO/IEC 9797-2:2002, MOD)

2012-12-31 发布　　2013-06-01 实施

中华人民共和国国家质量监督检验检疫总局
中国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》由如下部分组成：

——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。

本部分是GB/T 15852的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分修改采用ISO/IEC 9797-2：2002《信息技术　安全技术　消息鉴别码　第2部分：采用专用杂凑函数的机制》。增加了基于专用杂凑函数WHIRLPOOL的MAC生成方法及例子，更新了附录和参考文献，并将ISO/IEC 9797-2：2002中计算常数的6.3条调整到本部分的第9章。

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、信息安全国家重点实验室。

本部分主要起草人：吴文玲、张立廷、王鹏、吴双、张文涛、陈华、眭晗。

引　言

本部分规定的第一个 MAC 算法通常被称作 MDx-MAC。它调用一次完整的杂凑函数，但是对其中的轮函数做了细微的修改，把一个密钥加到了轮函数的附加常数上。第二个 MAC 算法通常被称作 HMAC，它调用两次完整的杂凑函数。第三个 MAC 算法是 MDx-MAC 的一个变种，它限制输入长度不大于 256 比特。在只处理较短输入的情况下，它有更好的性能。

本部分规定的三种 MAC 算法采用四种专用杂凑函数；其中，专用杂凑函数 1、2、3 和 4 分别是 ISO/IEC 10118-3：2004 中规定的专用杂凑函数 1、2、3 和 7。使用的专用杂凑函数也可以为国家密码管理部门批准的相应专用杂凑函数。

信息技术　安全技术　消息鉴别码
第2部分:采用专用杂凑函数的机制

1　范围

GB/T 15852的本部分规定了三种采用专用杂凑函数的消息鉴别码算法。这些消息鉴别码算法可用作数据完整性检验,检验数据是否被非授权地改变。同样这些消息鉴别码算法也可用作消息鉴别,保证消息源的合法性。数据完整性和消息鉴别的强度依赖于密钥的长度及其保密性、杂凑函数的算法强度及其输出长度、消息鉴别码的长度和具体的消息鉴别码算法。

本部分适用于任何安全体系结构、进程或应用的安全服务。

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 1988—1998　信息技术　信息交换用七位编码字符集(eqv ISO/IEC 646:1991)

ISO/IEC 10118-3:2004　信息技术　安全技术　杂凑函数　第3部分:专用杂凑函数(Information technology—Security techniques—Hash-functions—Part 3:Dedicated hash-functions)

3　术语和定义

下列术语和定义适用于本文件。

3.1

消息鉴别码　message authentication code;MAC

利用对称密码技术,以密钥为参数,由消息导出的数据项。任何持有这一密钥的实体,都可利用消息鉴别码检查消息的完整性和始发者。

3.2

消息鉴别码(MAC)算法密钥　MAC algorithm key

一种用于控制消息鉴别码算法运算的密钥。

3.3

消息鉴别码算法　message authentication code algorithm

消息鉴别码算法简称MAC算法,其输入为密钥和消息,输出为一个固定长度的比特串,满足下面两个性质:

——对于任何密钥和消息,MAC算法都能够快速地计算。

——对于任何固定的密钥,攻击者在没有获得密钥信息的情况下,即使获得了一些(消息,MAC)对,对任何新的消息预测其MAC在计算上是不可行的。

注:一个MAC算法有时被称作一个密码校验函数。计算不可行性依赖于使用者具体的安全要求及其环境。

3.4

输出变换　output transformation

应用在算法中,对迭代操作的输出所进行的变换。