ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36624—2018

信息技术　安全技术　可鉴别的加密机制

Information technology—Security techniques—Authenticated encryption

(ISO/IEC 19772:2009,MOD)

2018-09-17 发布　　2019-04-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法修改采用 ISO/IEC 19772:2009《信息技术　安全技术　可鉴别的加密机制》。

本标准与 ISO/IEC 19772:2009 的技术性差异及其原因如下：

——关于规范性引用文件，本标准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(见 8.4)；
- 用 GB/T 17964—2008 代替了 ISO/IEC 10116(见 9.3)；
- 用 GB/T 32907—2016 代替了 ISO/IEC 18033-3(见第 5 章)；
- 增加引用了 GB/T 25069—2010(见第 3 章)；

——第 3 章中，直接采用现行国家标准中已定义的术语定义，删除了部分常见的通用定义。

与 ISO/IEC 19772:2009 相比在结构上有较大调整，具体如下：

——对 ISO/IEC 19772:2009 范围一节内容进行修改，其中部分内容移至第 5 章概述；

——考虑到我国国情及技术的实际应用范围，本标准采用了 ISO/IEC 19772:2009 中第 7 章至第 11 章规定的五种可鉴别加密机制，删除 ISO/IEC 19772:2009 中第 6 章规定的可鉴别加密机制；

——将 ISO/IEC 19772:2009 中规范性附录 C 调整为附录 A，相应的，ISO/IEC 19772:2009 中资料性附录 A 和附录 B 分别调整为附录 B 和附录 C；

——附录 C 中给出的数据示例，修改为采用 SM4 算法作为示例。

本标准做了下列编辑性修改：

——纳入了 ISO/IEC 19772:2009 勘误版本的内容。

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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国科学院数据与通信保护研究教育中心、中国科学院软件研究所、北京江南天安科技有限公司。

本标准主要起草人：王琼霄、蔡权伟、张颖君、赵宇航、宋利、吴鹏一、闻楠、林璟锵、荆继武、王明月、宋天林。

信息技术　安全技术　可鉴别的加密机制

1　范围

本标准规定了五种可鉴别的加密机制，通过定义数据串的处理方法来实现以下安全目标：

——数据保密性，保护数据不会向非授权者泄露；

——数据完整性，确保数据接收者能够验证数据是否被修改；

——数据源鉴别，确保数据接收者能够验证数据始发者的身份。

本标准给出了五种可鉴别的加密机制 ASN.1 定义。

本标准适用于需对数据进行保密性、完整性保护及数据源鉴别的应用和系统。

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 17964—2008　信息安全技术　分组密码算法的工作模式

GB/T 25069—2010　信息安全技术　术语

GB/T 32907—2016　信息安全技术　SM4 分组密码算法

3　术语和定义

GB/T 15852.1—2008、GB/T 17964—2008、GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

可鉴别的加密　authenticated encryption

一种可逆的数据转换，利用密码算法产生数据对应的密文，非授权实体无法在不被发现的情况下对该密文进行修改，同时提供了数据保密性、数据完整性与数据源鉴别。

3.2

可鉴别的加密机制　authenticated encryption mechanism

用于实现数据保密性保护并提供数据完整性和数据源鉴别的密码技术，包括加密和解密两个处理过程。

3.3

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069—2010，定义 2.1.36]

3.4

分组密码　block cipher

又称块密码算法，一种对称密码算法，将明文划分成固定长度的分组进行加密。