ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17964—2021
代替 GB/T 17964—2008

信息安全技术
分组密码算法的工作模式

Information security technology—Modes of operation for a block cipher

2021-10-11 发布　　2022-05-01 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

本文件按照 GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 17964—2008《信息安全技术　分组密码算法的工作模式》，与 GB/T 17964—2008 相比，除了结构调整和编辑性改动外，主要技术变化如下：

a) 删除了“分组密码”等常见术语，增加了“XEX 结构”等多个术语（见第3章，2008年版的3.1）；

b) 删除了“位阵列表达式”等多个定义（见2008年版的3.2）；

c) 增加了 bit(S,i)等多个符号（见4.1）；

d) 增加了“HCTR”“XTS”等缩略语（见4.2）；

e) 增加了 ECB 工作模式加密算法和解密算法的示意图（见第5章）；

f) 删除了7.1和8.1，将相关参数定义增加到4.1符号中（见2008年版的第7章、第8章）；

g) 将第10章“分组链接（BC）模式”调整到新增加的第12章，增加了“带密文挪用的 XEX 可调分组密码工作模式”为第10章（见第10章、第12章，2008年版的第10章）；

h) 将第11章“带非线性函数的输出反馈（OFBNLF）工作模式”调整到新增加的第13章，增加了“带泛杂凑函数的计数器工作模式”为第11章（见第11章、第13章，2008年版的第11章）；

i) 更改了规范性附录 A 为资料性附录 A（见附录 A，2008年版的附录 A）；

j) 更改了密文窃取的具体方法，增加了示意图，并将“密文窃取”更名为“密文挪用”（见附录 A，2008年版的附录 A）；

k) 增加了 XTS 工作模式的性质和 HCTR 工作模式的性质（见附录 A）；

l) 更改了产生工作模式示例的分组密码为 SM4 算法（见附录 B，2008年版的附录 B）；

m) 增加了 XTS 工作模式的示例和 HCTR 工作模式的示例（见附录 B）；

n) 增加了资料性附录 C，列举了三种常见的填充方法，并给出了举例（见附录 C）。

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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：成都卫士通信息产业股份有限公司、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、国家密码管理局商用密码检测中心、格尔软件股份有限公司、西安西电捷通无线网络通信股份有限公司、上海信息安全工程技术研究中心。

本文件主要起草人：张立廷、眭晗、涂彬彬、李世敏、罗俊、王鹏、毛颖颖、郑强、张国强、徐明翼。

本文件及其所代替文件的历次版本发布情况为：

——2000年首次发布为 GB/T 17964—2000；2008年第一次修订；

——本次为第二次修订。

信息安全技术
分组密码算法的工作模式

1 范围

本文件描述了九种分组密码算法的工作模式，给出了参数和方法。

本文件适用于指导分组密码算法在加解密数据时的使用。

本文件描述的工作模式仅适用于保护数据的机密性，不适用于保护数据的完整性。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069—2010 信息安全技术 术语

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 25069—2010 和 GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

分组密码算法工作模式 block cipher operation mode

分组密码算法的使用方式，主要包括电码本工作模式、密文分组链接工作模式、密文反馈工作模式、输出反馈工作模式、计数器工作模式、带密文挪用的 XEX 可调分组密码工作模式、带泛杂凑函数的计数器工作模式、分组链接工作模式、带非线性函数的输出反馈工作模式等。

[来源：GM/Z 4001—2013，2.26，有修改]

3.2

电码本工作模式 electronic codebook(ECB)operation mode

分组密码算法的一种工作模式，其特征是将明文分组直接作为算法的输入，对应的输出作为密文分组。

[来源：GM/Z 4001—2013，2.10]

3.3

密文分组链接工作模式 cipher block chaining(CBC)operation mode

分组密码算法的一种工作模式，其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

[来源：GM/Z 4001—2013，2.62]

3.4

密文反馈工作模式 cipher feedback(CFB)operation mode

用分组密码算法构造序列密码的一种工作模式。其特征是，使用分组算法当前输出的若干比特，与