ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17964—2008
代替 GB/T 17964—2000

信息安全技术
分组密码算法的工作模式

**Information technology—Security techniques—
Modes of operation for a block cipher**

2008-06-26 发布　　2008-11-01 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

本标准代替 GB/T 17964—2000《信息技术　安全技术　n 位块密码算法的操作方式》。

本标准与 GB/T 17964—2000 相比主要变化如下：

——修改了标准的名称；

——修改了部分术语的定义；

——修改了加密解密的关系表达式；

——增加了分组算法的计数器(CTR)、分组链接(BC)和带非线性函数的输出反馈(OFBNLF)三种工作模式及其说明；

——在资料性附录 B 中增加了计数器(CTR)工作模式的加密解密实例说明；

——修改了部分描述性文字的语法。

本标准的附录 A 是规范性附录，附录 B 是资料性附录。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：无锡江南信息安全工程技术中心、卫士通信息产业股份有限公司、兴唐通信科技股份有限公司、济南得安计算机技术有限公司、上海格尔软件股份有限公司。

本标准主要起草人：徐强、李元正、谢永泉、李玉峰、高志权、谭武征。

本标准所代替标准的历次版本发布情况为：

——GB/T 17964—2000。

引　言

本标准中对于某些所描述的工作模式来说，可能需要对明文变量进行填充，具体填充技术不属于本标准的范围。

某些工作模式需要用到初始值 IV，IV 的定义不属于本标准范围。

当使用这些工作模式中的某一种时，所有通信方都要选择并使用同样的参数值。

本标准编制过程中得到了国家商用密码应用技术体系总体工作组的指导。

信息安全技术
分组密码算法的工作模式

1 范围

本标准描述了分组密码算法的七种工作模式，以便规范分组密码的使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

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)

3 术语和定义

下列术语和定义适用于本标准。

3.1 术语

3.1.1

分组链接工作模式 block chaining (BC) operation mode

分组密码算法的一种工作模式，当前的明文分组与所有前面密文分组的异或值相异或运算后再进行加密得到当前的密文分组。

3.1.2

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。

3.1.3

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，主要包括电码本模式(ECB)、密码分组链接模式(CBC)、密码反馈模式(CFB)、输出反馈模式(OFB)、计数器模式(CTR)等。

3.1.4

密码分组链接工作模式 cipher block chaining (CBC) operation mode

分组密码算法的一种工作模式，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。

3.1.5

密码反馈工作模式 cipher feedback (CFB) operation mode

分组密码算法用于构造序列密码的一种工作模式，用密文依次更新存储该密码算法启动变量的反馈缓冲器。

3.1.6

计数器工作模式 counter (CTR) operation mode

分组密码算法用于构造序列密码的一种工作模式，通过加密不断变化的计数器来产生密钥序列。

3.1.7

密文 ciphertext

加密后的数据。