UDC 681.3.06：003.26
L 80

中华人民共和国国家标准

GB/T 15277—94

信 息 处 理
64bit 分组密码算法的工作方式

Information processing—Modes of operation for a 64-bit block cipher algorithm

1994-12-07 发布　　1995-08-01 实施

国家技术监督局　发布

中华人民共和国国家标准

信 息 处 理
64bit 分组密码算法的工作方式

GB/T 15277—94

Information processing—Modes of operation for a 64-bit block cipher algorithm

本标准等效采用国际标准 ISO 8372—1987《信息处理 64bit 分组密码算法的工作方式》。

1 主题内容与适用范围

本标准描述了采用秘密密钥的任意一种 64bit 分组密码算法的四种工作方式。

注：附录 A(参考件)包含了对每一种工作方式性质的简要评述。

本标准规定了四种确定的工作方式，以便在 64bit 分组密码的任何应用(例如数据传输，数据存储，鉴别)中，对诸如工作方式的详细说明、启动变量的生成以及参数值的选定提供一个有用的参照。

注：对密文反馈(CFB)工作方式(见第 6 章)，要确定两个参数 j 和 k；对输出反馈(OFB)工作方式(见第 7 章)，要确定一个参数 j。在使用其中一种工作方式时，相应参数要由通信的所有各方选定和使用。

2 术语

2.1 明文 plaintext

未加密的信息。

2.2 密文 ciphertext

已加密的信息。

2.3 分组链接 block chaining

一种信息加密方法，每一个密文分组在密码上依赖于前一个密文分组。

2.4 初始化值(IV) initializing value(IV)

用来确定加密过程的启动点的值。

2.5 启动变量(SV) starting variable(SV)

由初始化值导出的且用来确定工作方式启动点的变量。

注：本标准没有规定由初始化值导出启动变量的方法。这需要在应用这些工作方式时另行描述。

2.6 密码同步 cryptographic synchronization

加密与解密过程的协调一致。

3 记法

本标准中，由分组密码算法定义的函数关系记为

$$C = eK(P)$$

式中：P——明文分组；

C——密文分组；

K——密钥。

国家技术监督局 1994-12-07 批准　　1995-08-01 实施