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。

3.1.8

密码同步　cryptographic synchronization

使密码系统正确处理而进行的协作机制。

3.1.9

解密　decipherment/decryption

加密过程对应的逆过程。

3.1.10

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，明文分组直接作为加密算法的输入，对应的输出作为密文分组。

3.1.11

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.1.12

反馈缓存（FB）　feedback buffer（FB）

用于为加密过程存储输入数据的变量。在启动点，FB 的值为 IV。

3.1.13

初始化向量/值　initialization vector/initialization value（IV）

在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

3.1.14

密钥　key

控制密码变换操作的关键信息或参数。

3.1.15

带非线性函数的输出反馈模式　output feedback with a nonlinear function（OFBNLF）operation mode

分组密码算法的一种工作模式，是 OFB 和 ECB 的变体，它的密钥随着每一个分组而改变。

3.1.16

输出反馈工作模式　output feedback（OFB）operation mode

分组密码算法用于构造序列密码的一种工作模式，用该算法当前时刻的输出作为下一时刻的输入。

3.1.17

明文　plain text/clear text

待加密的数据。

3.2　定义

3.2.1　加密表达式

本标准中，由分组密码规定的函数关系记作：

$$C=E_K(P)$$

其中：P 是明文分组；

C 是密文分组；

K 是密钥；

E_K 是使用密钥 K 的加密运算。

3.2.2　解密表达式

对应的解密函数记作：

$$P=D_K(C)$$

D_K 是使用密钥 K 的解密运算。

3.2.3 位阵列表达式

由一个大写字母表示的变量，如上面的 P 和 C，它表示一个一维的位阵列。例如：

$$A=(a_1,a_2,\cdots,a_m)\text{和 }B=(b_1,b_2,\cdots,b_m)$$

便是两个 m 位阵列，其位从 1 到 m 编号。所有位阵列的记法都是以下标为 1 的位处于最左边。

3.2.4 模 2 加表达式

模 2 加操作，也称作“异或”运算，用符号⊕表示，应用到阵列 A 和 B 的运算定义为：

$$A\oplus B=(a_1\oplus b_1,a_2\oplus b_2,\cdots,a_m\oplus b_m)$$

3.2.5 位选择表达式

选择 A 的最左边 j 个位以产生一个 j 位阵列的操作记作：

$$A\sim j=(a_1,a_2,\cdots,a_j)$$

仅当 $1\leqslant j\leqslant m$（m 是 A 中的位数）时此操作才有定义。

3.2.6 移位运算表达式

移位函数 S_k 定义如下：

已知 m 位变量 X 和 k 位变量 F，其中 $1\leqslant k\leqslant m$，移位函数 $S_k(X|F)$ 的作用是产生以下的 m 位变量（| 是连接运算符，下同）：

$$S_k(X|F)=(X_{k+1},X_{k+2},\cdots,X_m,f_1,f_2,\cdots,f_k)\quad(k<m)$$

$$S_k(X|F)=(f_1,f_2,\cdots,f_k)\quad(k=m)$$

其作用是将阵列 X 的各位左移 k 个位置，舍弃 $X_1,X_2,\cdots,X_k$，并将阵列 F 放置在阵列 X 的最右边的 k 个位置上。当 $k=m$ 时，其作用是 F 完全取代 X。

此函数的一个特例是以全“1”的 m 位变量 I(m) 开始，并将 k 位变量 F 移到其中。结果为：

$$S_k(I(m)|F)=(1,1,\cdots,1,f_1,f_2,\cdots,f_k)\quad(k<m)$$

$$S_k(I(m)|F)=(f_1,f_2,\cdots,f_k)\quad(k=m)$$

其中最左边的 $m-k$ 位均为“1”。

4 缩略语和符号

AES	高级数据加密标准(advanced encryption standard)
BC	分组链接(block chaining)
CBC	密码分组链接(cipher block chaining)
CFB	密码反馈(cipher feedback)
CTR	计数器(counter)
DEA	数据加密算法(data encryption algorithm)
ECB	电码本(electronic codebook)
IV	初始值(initialization value)
OFB	输出反馈(output feedback)
OFBNLF	带非线性函数的输出反馈(output feedback with a nonlinear function)

5 电码本(ECB)模式

5.1 变量定义

a) q 个明文分组 $P_1,P_2,\cdots,P_q$ 所组成的序列，每个块都为 n 位。

b) 密钥 K。

c) q 个密文分组 $C_1,C_2,\cdots,C_q$ 所组成的结果序列，每个块都为 n 位。

5.2 ECB 的加密方式描述

$$C_i=E_K(P_i)\quad i=1,2,\cdots,q$$

5.3 ECB 的解密方式描述

$$P_i = D_K(C_i) \quad i=1,2,\cdots,q$$

注：ECB 模式的工作性质见附录 A。

示例：ECB 模式的示例参考附录 B。

6 密码分组链接(CBC)模式

6.1 变量定义

a) q 个明文分组 $P_1,P_2,\cdots,P_q$ 所组成的序列，每个块都为 n 位。

b) 密钥 K。

c) n 位初始值 IV。

d) q 个密文分组 $C_1,C_2,\cdots,C_q$ 所组成的结果序列，每个块都为 n 位。

6.2 CBC 的加密方式描述

对第一个明文分组进行加密：

$$C_1 = E_K(P_1 \oplus IV)$$

随后：

$$C_i = E_K(P_i \oplus C_{i-1}) \quad i=2,3,\cdots,q$$

此过程如图 1 的上半部分所示。初始值 IV 用于产生第 1 个密文输出。之后，在加密之前，这个密文与下一个明文进行模 2 加。

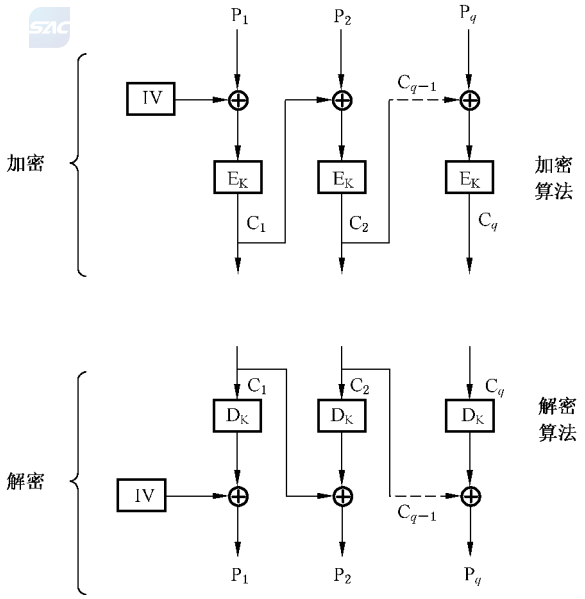

图 1 密码分组链接(CBC)操作方式

6.3 CBC 的解密方式描述

对第 1 个密文分组进行解密：

$$P_1 = D_K(C_1) \oplus IV$$

随后：

$$P_i = D_K(C_i) \oplus C_{i-1} \quad i=2,3,\cdots,q$$

此过程如图 1 的下半部分所示。

注：CBC 模式的工作性质见附录 A。

示例：CBC 模式的示例参考附录 B。

7 密码反馈(CFB)模式

7.1 参数定义

- 反馈缓存的大小 $r(n\leqslant r\leqslant 2n)$；
- 反馈变量的大小 $k(1\leqslant k\leqslant n)$；
- 明文变量的大小 $j(1\leqslant j\leqslant k)$。

注：$r-k$ 可小于 n。图 2 示出了 $r-k>n$ 的特殊情形。

7.2 变量定义

a) 输入变量

1) q 个明文变量 $P_1,P_2,\cdots,P_q$ 所组成的序列，每个块都为 j 位。

2) 密钥 K。

3) r 位初始值 IV。

b) 中间结果

1) q 个密码输入块 $X_1,X_2,\cdots,X_q$ 所组成的序列，每个块都为 n 位。

2) q 个密码输出块 $Y_1,Y_2,\cdots,Y_q$ 所组成的序列，每个块都为 n 位。

3) q 个变量 $Z_1,Z_2,\cdots,Z_q$ 所组成的序列，每个变量都为 j 位。

4) $q-1$ 个反馈变量 $F_1,F_2,\cdots,F_{q-1}$ 所组成的序列，每个变量都为 k 位。

5) $q-1$ 个反馈缓存内容 $FB_1,FB_2,\cdots,FB_{q-1}$ 所组成的序列，每个块都为 n 位。

c) 输出变量

q 个密文变量 $C_1,C_2,\cdots,C_q$ 所组成的序列，每个块都为 j 位。

7.3 CFB 的加密方式描述

反馈缓存 FB 的初始值为：

$$FB_1=IV$$

对每个明文变量进行加密的运算采用以下六个步骤：

a) 产生输入变量：

$$X_i=FB_i\sim n$$

b) 使用分组密码：

$$Y_i=E_K(X_i)$$

c) 选择最左边的 j 位：

$$Z_i=Y_i\sim j$$

d) 产生密文变量：

$$C_i=P_i\oplus Z_i$$

e) 产生反馈变量：

$$F_i=S_j(I(k)\,|\,C_i)$$

f) FB 移位运算：

$$FB_{i+1}=S_k(FB_i\,|\,F_i)$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 d)。此过程如图 2 左半部分所示。分组密码的输出块 Y 的最左边 j 位用来通过模 2 加来加密 j 位明文变量。Y 的其他位被舍弃。明文和密文变量的各位从 1 到 j 编号。

通过把 $k-j$ 个“1”位放到密文变量的最左边位置上，将密文变量扩展成 k 位反馈变量 F，然后将反馈缓存 FB 的各位左移 k 个位置，并将 F 插到最右边的 k 个位置上，就产生了新的反馈缓存 FB 值。在此移位操作中，FB 的最左边 k 位被舍弃。FB 最左边的新的 n 位用作加密过程的下一个输入 X。

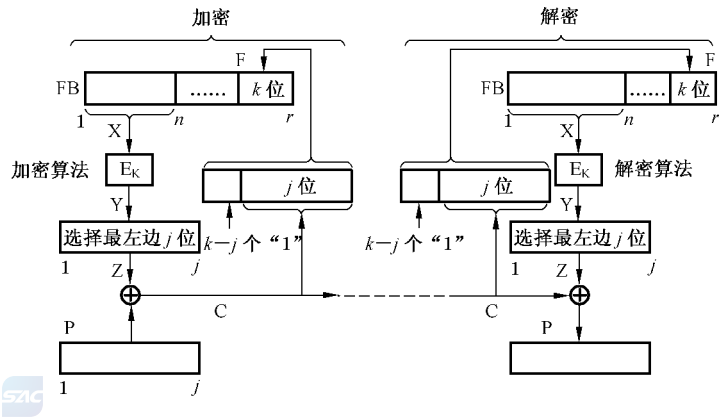

图 2　密码反馈(CFB)工作模式

7.4　CFB 的解密方式描述

用于解密变量与用于加密变量是相同的。

反馈缓存 FB 被置成初始值：

$$FB_1 = IV$$

对每个密文变量进行解密的操作采用以下六个步骤：

a)　产生输入变量：

$$X_i = FB_i \sim n$$

b)　使用分组密码：

$$Y_i = E_K(X_i)$$

c)　选择最左边的 j 位：

$$Z_i = Y_i \sim j$$

d)　产生明文变量：

$$P_i = C_i \oplus Z_i$$

e)　产生反馈变量：

$$F_i = S_j(I(k) \mid C_i)$$

f)　FB 移位运算：

$$FB_{i+1} = S_k(FB_i \mid F_i)$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 d)。此过程如图 2 右半部分所示。分组密码的输出块 Y 的最左边 j 位用来通过模 2 加来解密 j 位密文变量。Y 的其他位被舍弃。明文和密文变量的各位从 1 到 j 编号。

通过把 $k-j$ 个“1”位放到密文变量的最左边位置上，将密文变量扩展成 k 位反馈变量 F，然后将反馈缓存 FB 的各位左移 k 个位置，并将 F 放到最右边的 k 个位置上，就产生了新的反馈缓存 FB 值。在此移位操作中，FB 的最左边 k 位被舍弃。FB 最左边的新的 n 位用作加密过程的下一个输入 X。

注：CFB 模式的工作性质见附录 A。

示例：CFB 模式的示例参考附录 B。

7.5　建议

建议使用 j 和 k 的值相等的 CFB 方式。按照这种建议形式($j=k$)，加密操作和解密操作的步骤 e)可以写成：

$$F_i = C_i \quad (\text{当 } j=k)$$

8 输出反馈(OFB)模式

8.1 参数定义

OFB 操作方式由一个参数来定义,该参数为明文变量的大小 j($1 \leqslant j \leqslant n$)。

8.2 变量定义

a) 输入变量

1) q 个明文变量 $P_1, P_2, \cdots, P_q$ 所组成的序列,每个块都为 j 位。

2) 密钥 K。

3) n 位初始值 IV。

b) 中间结果

1) q 个密码输入块 $X_1, X_2, \cdots, X_q$ 所组成的序列,每个块都为 n 位。

2) q 个密码输出块 $Y_1, Y_2, \cdots, Y_q$ 所组成的序列,每个块都为 n 位。

3) q 个变量 $Z_1, Z_2, \cdots, Z_q$ 所组成的序列,每个块都为 j 位。

c) 输出变量

q 个密文变量 $C_1, C_2, \cdots, C_q$ 所组成的序列,每个块都为 j 位。

8.3 OFB 的加密方式描述

输入块 X 置成初始值:

$$X_1 = IV$$

对每个明文变量进行加密的运算采用以下四个步骤:

a) 使用分组密码:

$$Y_i = E_K(X_i)$$

b) 选择最左边的 j 位:

$$Z_i = Y_i \sim j$$

c) 产生密文变量:

$$C_i = P_i \oplus Z_i$$

d) 反馈操作:

$$X_{i+1} = Y_i$$

对 $i = 1, 2, \cdots, q$,重复上述步骤,最后一个循环结束于步骤 c)。此过程如图 3 的左半部分所示。每次使用分组密码所产生的结果 Y_i 被用来反馈并成为 X 的下一个值,即 X_{i+1}。Y_i 的最左边 j 位用来加密输入变量。

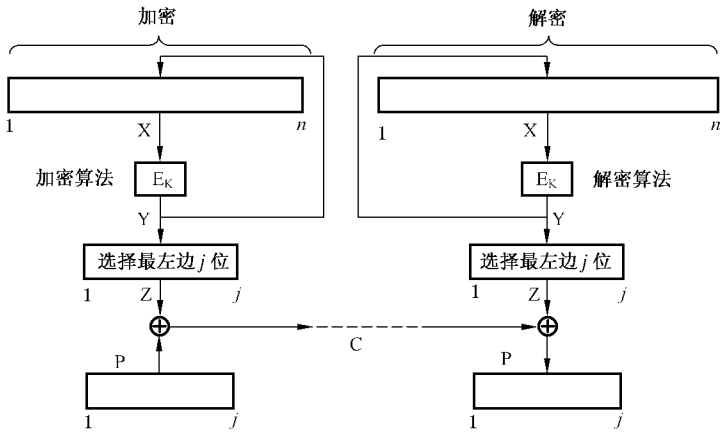

图 3 输出反馈(OFB)工作模式

8.4 OFB 的解密方式描述

用于解密的变量与用于加密的变量是相同的。输入块被置成初始值：

$$X_1 = IV$$

对每个密文变量进行解密的运算采用以下四个步骤：

a) 使用块密文：

$$Y_i = E_K(X_i)$$

b) 选择最左边的 j 位：

$$Z_i = Y_i \sim j$$

c) 产生明文变量：

$$P_i = C_i \oplus Z_i$$

d) 反馈操作：

$$X_{i+1} = Y_i$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 c)。此过程如图 3 的右半部分所示。值 X_i 和 Y_i 与加密过程中相应的值是相同的；仅有步骤 c)是不同的。

注：OFB 模式的工作性质见附录 A。

示例：OFB 模式的示例参考附录 B。

9 计数器(CTR)模式

9.1 变量定义

a) 输入变量

1) q 个明文变量 $P_1,P_2,\cdots,P_q$ 所组成的序列(其中，$P_1,P_2,\cdots P_{q-1}$ 都为 n 位，P_q 为 k 位)。

2) 密钥 K。

3) q 个计数序列 $T_1,\cdots,T_{q-1},T_q$，每个块都为 n 位。

b) 中间结果

1) q 个密码输出块 $X_1,X_2,\cdots,X_q$ 所组成的序列，每个块都为 n 位。

2) k 位密码输出块 Z。

c) 输出变量

q 个密文变量 $C_1,C_2,\cdots,C_q$ 所组成的序列(其中，$C_1,C_2,\cdots C_{q-1}$ 都为 n 位，C_q 为 k 位)。

9.2 CTR 的加密方式描述

a) 对计数序列加密：

$$X_i = E_K(T_i) \quad i=1,2,\cdots,q$$

b) 产生密文变量：

$$C_i = P_i \oplus X_i \quad i=1,2,\cdots,q-1$$

c) 选择最左边的 k 位：

$$Z = X_q \sim k$$

d) 处理最后的分组

$$C_q = P_q \oplus Z$$

对 $i=1,2,\cdots,q-1$，重复步骤 b)，最后结束于步骤 d)。此过程如图 4 的上半部分所示。

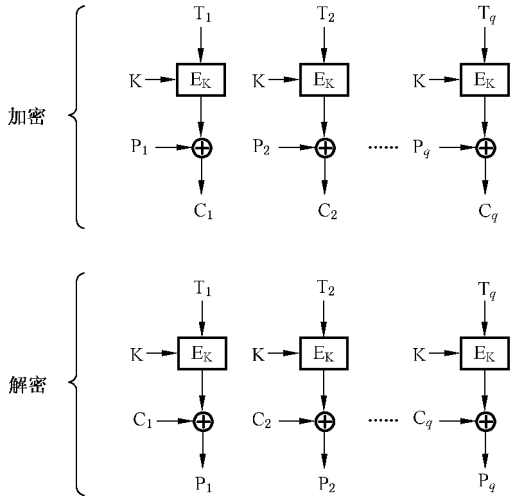

图 4　计数器(CTR)工作模式

9.3　CTR 的解密方式描述

a)　对计数序列加密：

$$X_i = E_K(T_i) \quad i=1,2,\cdots,q$$

b)　产生明文变量：

$$P_i = C_i \oplus X_i \quad i=1,2,\cdots,q-1$$

c)　选择最左边的 k 位：

$$Z = X_q \sim k$$

d)　处理最后的分组

$$P_q = C_q \oplus Z$$

对 $i=1,2,\cdots,q-1$，重复步骤 b)，最后结束于步骤 d)。此过程如图 4 的下半部分所示。

注：CTR 模式的工作性质见附录 A。

示例：CTR 模式的示例参考附录 B。

10　分组链接(BC)模式

10.1　变量定义

a)　q 个明文分组 $P_1,P_2,\cdots,P_q$ 所组成的序列，每个块都为 n 位。

b)　密钥 K。

c)　n 位初始值 IV。

d)　q 个反馈变量 $F_1,F_2,\cdots,F_q$ 所组成的序列，每个块都为 n 位。

e)　q 个密文分组 $C_1,C_2,\cdots,C_q$ 所组成的结果序列，每个块都为 n 位。

10.2　BC 的加密方式描述

a)　反馈变量初始值为：

$$F_1 = IV$$

b)　产生密文变量：

$$C_i = E_K(P_i \oplus F_i)$$

c)　产生反馈变量：

$$F_{i+1} = F_i \oplus C_i$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 b)。此过程如图 5 的上半部分所示。初始值 IV 用于产生第 1 个密文输出。之后，在加密之前，这个密文与当前反馈变量进行模 2 加，产生下一

个反馈变量。

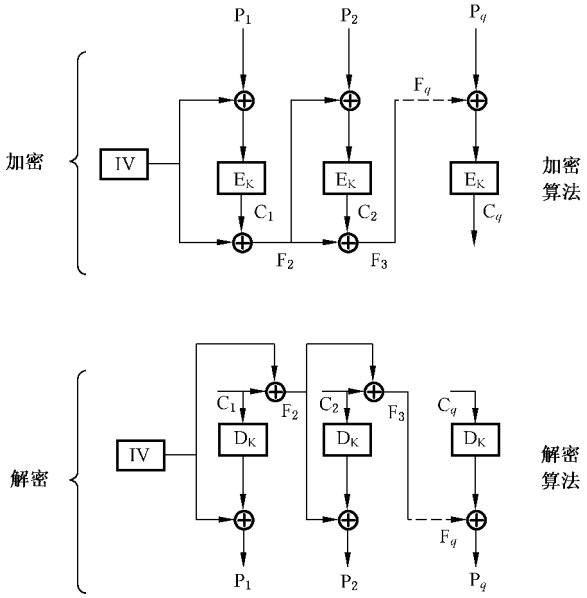

图 5　分组链接(BC)操作方式

10.3　BC 的解密方式描述

a)　反馈变量初始值为：

$$F_1 = IV$$

b)　产生明文变量：

$$P_i = F_i \oplus D_K(C_i)$$

c)　产生反馈变量：

$$F_{i+1} = F_i \oplus C_i$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 b)。此过程如图 5 的下半部分所示。

注：BC 模式的工作性质见附录 A。

11　带非线性函数的输出反馈(OFBNLF)模式

11.1　变量定义

a)　输入变量

1)　q 个明文变量 $P_1,P_2,\cdots,P_q$ 所组成的序列，每个块都为 n 位。

2)　密钥 K。

3)　n 位初始值 IV。

b)　中间结果

$q+1$ 个密钥输入块 $K_0,K_1,\cdots,K_q$ 所组成的序列，每个块都为 n 位。

c)　输出变量

q 个密文变量 $C_1,C_2,\cdots,C_q$ 所组成的序列，每个块都为 n 位。

11.2　OFBNLF 的加密方式描述

a)　输入变量置成初始值：

$$K_0 = IV$$

b)　产生密钥变量：

$$K_i = E_K(K_{i-1})$$

c)　产生密文变量：

$$C_i = E_{K_i}(P_i)$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 c)。此过程如图 6 的上半部分所示。每次使用的密钥 K_i 被密钥 K 加密并成为下一个分组的密钥，即 K_{i+1}。

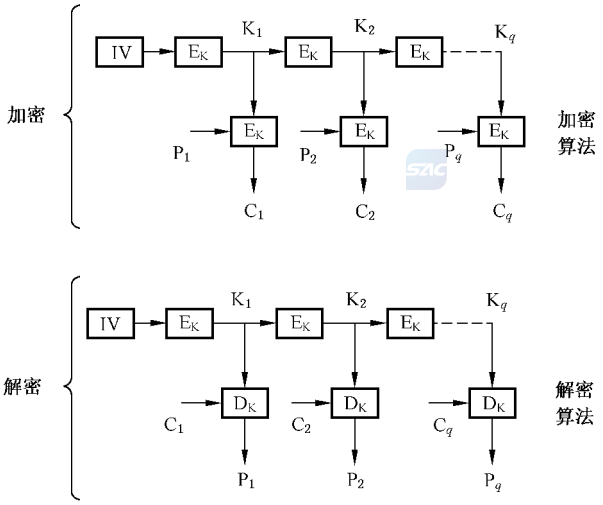

图 6　带非线性函数的输出反馈(OFBNLF)工作模式

11.3　OFBNLF 的解密方式描述

a)　输入变量置成初始值：

$$K_0 = IV$$

b)　产生密钥变量：

$$K_i = E_K(K_{i-1})$$

c)　产生明文变量：

$$P_i = D_{K_i}(C_i)$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于步骤 c)。此过程如图 6 的下半部分所示。每次使用的密钥 K_i 被密钥 K 加密并成为下一个分组的密钥，即 K_{i+1}。K_i 与加密过程中相应的值是相同的。

注：OFBNLF 模式的工作性质见附录 A。

附 录 A
（规范性附录）
工作模式的性质

A.1 电码本（ECB）工作模式的性质

A.1.1 环境

在各种计算机之间或人与人之间所交换的二进制数据可能会有重复或者是共同使用的序列。在ECB方式中，相同的明文分组（对于相同的密钥）产生相同的密文分组。

A.1.2 性质

ECB方式的性质有：

a） 对某一块的加密或解密可独立于其他进行；

b） 对密文的重排将导致明文分组的相应重排；

c） 相同的明文分组（对于相同的密钥）总是产生相同的密文分组，这使得它容易遭受一种“字典攻击”，这种字典是由对应的明文和密文分组构成的。

对于超过一个块的消息一般建议不使用ECB方式，对于可接受重复性或必须单独访问各个块的那些特殊使用情况，ECB的用法可以在未来的标准中规定。

A.1.3 填充要求

只有分组长度的倍数才能被加密或解密。其他长度需要被填充至分组长度边界。

A.1.4 差错扩散

在ECB方式中，在一个密文分组中的一个或多个位差错只会影响对发生差错的那一块的解密。对于有一个或多个错误位的密文分组的解密将导致对应的明文分组中每个明文位出错的概率为50%。

A.1.5 块边界

如果加密或解密之间的块边界丢失了（例如由于一个位的滑动），则在重新建立正确的块边界之前，加密与解密之间将失去同步。如果块边界丢失，则所有解密操作的结果都是不正确的。

A.2 密码分组链接（CBC）工作模式的性质

A.2.1 环境

只要使用同样的密钥和初始值对相同的明文进行加密，CBC方式将产生相同的密文。关心这种性质的用户需要采用某种方法来改变明文的开始、密钥或初始值。一种可能的办法是将一个唯一的标识符（例如一个递增计数器）加到每个CBC消息的开始处。在对大小不能增加的记录进行加密时可采用另一种办法，它使用诸如初始值的某个值，这个值能从记录中计算出来且不用知道其内容（例如它的按随机访问存储方式的地址）。

A.2.2 性质

CBC方式的性质有：

a） 链接操作使得密文分组依赖于当前的和以前的明文分组，因此对密文分组的重新安排不会导致对相应明文分组的重新安排；

b） 使用不同的IV从而防止同一明文加密成同一密文。

A.2.3 填充要求

只有分组长度的倍数才能被加密或解密。其他长度需要被填充至分组长度边界。如果这是不可接受的，可以按一种特殊方式来处置最后一个变量。下面给出两个特殊处理的例子。

第一种处理一个不完整的变量（即：一个 $j<n$ 位的变量 P_q，其中 q 应大于1）的可能办法是按下面

的描述的 OFB 方式对它进行加密：

a） 加密

$$C_q = P_q \oplus (eK(C_{q-1}) \sim j) \quad \cdots\cdots(50)$$

b） 解密

$$P_q = C_q \oplus (eK(C_{q-1}) \sim j) \quad \cdots\cdots(51)$$

但是，如果 IV 不是秘密的或者与同一个密钥一起被多次使用（见 A.4），那么最后的变量容易受到“选择明文攻击”。

第二种办法称作“密文窃取”。假设最后两个明文变量为 P_{q-1} 和 P_q，P_{q-1} 是一个 n 位分组，P_q 是一个 $j<n$ 位的变量，q 应大于 1。

a） 加密

设 C_{q-1} 为使用 5.2 所描述的方法由 P_{q-1} 导出的密文分组。令

$$C_q = eK(S_j(C_{q-1} \mid P_q)) \quad \cdots\cdots(52)$$

因此最后两个密文变量是 C_{q-1} 和 C_q

b） 解密

首先需要对 C_q 进行解密，从而产生变量 P_q 和 C_{q-1} 的右边 $n-j$ 位：

$$S_j(C_{q-1}) \mid P) = dK(C_q) \quad \cdots\cdots(53)$$

进而得到完整的块 C_{q-1}，并且使用 5.3 所描述的方法能导出 P_{q-1}。

两个紧随着的变量是按逆序进行解密的，这使得这种方法不太适合于硬件实现。

A.2.4 差错扩散

在 CBC 方式中，在一个密文分组中的一个或多个位差错会影响对两个块（即发生差错的块和随后的块）的解密。第 i 个密文分组中的一个差错对于所产生的明文有以下影响：第 i 个明文分组每位出错的概率为 50%。第 $i+1$ 个明文分组的差错模式与第 i 个密文分组相同。如果在一个不到 n 位的变量中出现差错，差错扩散取决于所选择的特殊处理方法。在第一个例子中，被解密的较短的块中与明文中出错的位直接对应的那些位也会出错。

A.2.5 块边界

如果解密或解密之间的块边界丢失了（例如由于一个位的滑动），则在重新建立正确的块边界之前，加密与解密之间将失去同步。如果块边界丢失，所有解密操作的结果都是不正确的。

A.3 密码反馈（CFB）工作模式的性质

A.3.1 环境

只要使用同样的密钥和初始值对相同的明文进行加密，CFB 方式将产生相同的密文。关心这种特性的用户需要采用某种办法来改变明文的开始、密钥或初始值。一种可能的办法是将一个唯一的标识符（例如一个递增计数器）加到每个 CFB 消息的开始处。在对大小不能增加的记录进行加密时可采用另一种办法，它使用诸如初始值的某个值，这个值能从记录中计算出来且不用知道其内容（例如它的按随机访问存储方式的地址）。

A.3.2 性质

CFB 的性质有：

a） 链接操作使得密文变量依赖于当前的和除一确定数目以外的所有以前的明文变量，该数目取决于 r、k 和 j 的选择（见图 2）。因此对 j 位密文变量的重新安排不会导致对相应的 j 位明文变量的重新安排；

b） 使用不同的 IV 值从而防止同一明文加密成同一密文；

c） CFB 方式的加密和解密过程都使用块密码的加密操作；

d） CFB 方式的强度依赖于 k 的大小（$j=k$ 时最大）以及 j、k、n 和 r 的相对大小；

注：$j<k$ 将导致输入块的值重复出现的概率增加。这种重复出现将会泄露明文位之间的线性关系。

e) 选择一个较小的 j 值对于每个明文单位将要求更多次的块密码操作，因而引起更大的处理开销；

f) 选择 $r \geqslant n+k$ 使得能对块密码进行流水线式连续操作。

A.3.3 填充要求

只有 j 位的倍数才能被加密或解密。其他长度需要填充至 j 位边界。但是，经常对 j 的大小的选择是要使得其无需进行填充，例如对于明文的最后部分，j 能被修改。

A.3.4 差错扩散

CFB 方式中，任一 j 位密文单位的差错都将影响对随后密文的解密，直到出错的位移出 CFB 反馈缓存为止。第 i 个密文变量中的差错对产生的明文有下列影响：第 i 个明文变量与第 i 个密文变量有相同的差错模式。在所以不正确接收的位被移出反馈缓存之前，随后的明文变量的每一位出错的概率为 50%。

A.3.5 同步

如果加密和解密之间的分组边界丢失了(例如由于一个位的滑动)，则在 j 位边界重新建立的 r 位之后，密码同步将被重新建立。如果丢失 j 位的倍数，则在 r 位之后将重新建立同步。

A.4 输出反馈(OFB)工作模式的性质

A.4.1 环境

只要使用同样的密钥和初始值对相同的明文进行加密，OFB 方式应将产生相同的密文。此外，当使用相同的密钥和 IV 时，OFB 方式中将会产生相同的密钥流，因此，为了保密起见，对于一个给定的密钥，一个特定的 IV 只能使用一次。

A.4.2 性质

OFB 的性质有：

a) 没有链接操作会使得 OFB 更容易受到主动的攻击；

b) 使用不同的 IV 值，通过产生不同的密钥流，从而防止同一明文加密成同一密文；

c) OFB 方式的加密和解密过程都使用分组密码的加密运算；

d) OFB 方式不依赖明文来产生用于对明文进行模 2 加的密钥流；

e) 选择一个较小的 j 值对于每个明文单位将要求更多次的分组密码操作，因而引起更大的处理开销。

A.4.3 填充要求

只有 j 位的倍数才能被加密或解密。其他长度需要填充至 j 位边界。但是，经常对 j 的大小的选择是要使得其无需进行填充，例如对于明文的最后部分，j 能被修改。

A.4.4 差错扩散

OFB 方式不在产生的明文输出扩散密文差错。密文中每一差错位只会引起被解密的明文中出现一个差错位。

A.4.5 同步

OFB 方式不是自动同步的。如果加密和解码两个操作不同步，系统需要重新初始化。这种同步丢失可能由于插入或丢失任何数目的密文所引起。

每次重新初始化应使用一个新的 IV 值，它不同于与同一个密钥一起使用的以前的 IV 值。其原因是对于相同的参数，每次都要产生相同的位流。这将易于受到“已知的明文攻击”。

A.5 计数器(CTR)工作模式的性质

A.5.1 环境

计数模式下的分组密码算法使用序列号作为算法的输入。不是用加密算法的输出填充寄存器，而

是将一个计数器输入到寄存器中。每一个分组完成加密后，计数器都要增加某个常数，典型值是 1。没有什么是专供计数器用的，它不必根据可能的输入计数。可以随机序列发生器作为分组算法的输入，而不必考虑其密码上是否安全。

A.5.2 性质

CTR 的性质有：

a) 加密运算可并行处理，吞吐量仅受可使用并行数量的限制；

b) 使用不同的计数器，通过产生不同的密钥流，从而防止同一明文加密成同一密文；

c) CTR 方式的加密和解密过程都使用分组密码的加密运算；

d) CTR 方式不依赖明文来产生用于对明文进行模 2 加的密钥流。

A.5.3 填充要求

计数模式解决了 OFB 模式小于分组长度的 n 比特输出问题，可以处理任意长度的信息，不需要填充。

A.5.4 差错扩散

CTR 方式不在产生的明文输出扩散密文差错。密文中每一差错位只会引起被解密的明文中出现一个差错位。

A.5.5 同步

CTR 方式不是自动同步的。如果加密和解码两个操作不同步，系统需要重新初始化。这种同步丢失可能由于插入或丢失任何数目的密文所引起。

每次重新初始化应使用一个新的计数器值，它不同于与同一个密钥一起使用的以前的计数器值。其原因是对于相同的参数，每次都要产生相同的密钥流。这将易于受到“已知的明文攻击”。

A.6 分组链接(BC)工作模式的性质

A.6.1 环境

为了在分组链接(BC)模式中使用分组算法，可以简单地将分组密码算法的输入跟所有前面密文分组的异或值相异或。就像 CBC 算法一样，过程要从一个初始向量 IV 开始。

只要使用同样的密钥和初始值对相同的明文进行加密，BC 方式将产生相同的密文。关心这种性质的用户需要采用某种方法来改变明文的开始、密钥或初始值。

A.6.2 性质

BC 方式的性质有：

a) 链接操作使得密文分组依赖于当前的和以前的明文分组，因此对密文分组的重新安排不会导致对相应明文分组的重新安排；

b) 使用不同的 IV 从而防止同一明文加密成同一密文。

A.6.3 填充要求

只有分组长度的倍数才能被加密或解密。其他长度需要被填充至分组长度边界。

A.6.4 差错扩散

BC 模式的反馈过程具有扩散明文错误的性质，这个问题是由于密文分组的解密依赖于所有前面的密文分组而引起的，密文中单一的错误都将导致所有后续密文分组在解密中出错。

A.6.5 同步

如果解密或解密之间的块边界丢失了(例如由于一个位的滑动)，则在重新建立正确的块边界之前，加密与解密之间将失去同步。如果块边界丢失，所有解密操作的结果都是不正确的。

A.7 带非线性函数的输出反馈(OFBNLF)工作模式的性质

A.7.1 环境

带非线性函数的输出反馈(OFBNLF)是 OFB 和 ECB 的一个变体，它的密钥随每一个分组而改变。

只要使用同样的密钥和初始值对相同的明文进行加密，OFBNLF 方式应将产生相同的密文。此外，当使用相同的密钥和 IV 时，OFBNLF 方式中将会产生相同的密钥流，因此，为了保密起见，对于一个给定的密钥，一个特定的 IV 只能使用一次。

A.7.2 性质

OFBNLF 的性质有：

a) 使用不同的 IV 值，通过产生不同的密钥流，从而防止同一明文加密成同一密文；

b) OFBNLF 方式的加密和解密过程都使用分组密码的加密运算；

c) OFBNLF 方式不依赖明文来产生用于对明文进行加密的密钥流。

A.7.3 填充要求

只有分组长度的倍数才能被加密或解密。其他长度需要被填充至分组长度边界。

A.7.4 差错扩散

密文的一个比特错误扩散到一个明文分组。然而，如果一位丢失或增加，那就有无限的错误扩散。

A.7.5 同步

OFBNLF 方式不是自动同步的。如果加密和解码两个操作不同步，系统需要重新初始化。这种同步丢失可能由于插入或丢失任何数目的密文所引起。

每次重新初始化应使用一个新的 IV 值，它不同于与同一个密钥一起使用的以前的 IV 值。其原因是对于相同的参数，每次都要产生相同的位流。这将易于受到“已知的明文攻击”。

附 录 B
（资料性附录）
工作模式举例

B.1 概述

本附录举例说明使用本标准所规定的工作模式对消息的加密和解密。这些例子使用下列参数：

使用的分组密码是数据加密算法(DEA)，分组长度为 64。

密码密钥为 0123456789ABCDEF。

初始值为 1234567890ABCDEF。

明文是“Now is the time for all”的 7 位 GB1988/ASCII 代码(十六进制形式：4E6F772069732074 68652074696D6520 666F7220616C6C20)。对于 CFB 方式，明文是“Now”的 7 位 GB1988/ASCII 代码(十六进制形式：4E6F77)。

B.2 ECB 方式

表 B.1 和表 B.2 分别给出 ECB 方式加密和解密的例子。

表 B.1 ECB 方式加密

i	明文 P_i	分组密码输入分组	分组密码输出分组	密文 C_i
1	4E6F772069732074	4E6F772069732074	3FA40E8A984D4815	3FA40E8A984D4815
2	68652074696D6520	68652074696D6520	6A271787AB8883F9	6A271787AB8883F9
3	666F7220616C6C20	666F7220616C6C20	893D51EC4B563B53	893D51EC4B563B53

表 B.2 ECB 方式解密

i	密文 C_i	分组密码输入分组	分组密码输出分组	明文 P_i
1	3FA40E8A984D4815	3FA40E8A984D4815	4E6F772069732074	4E6F772069732074
2	6A271787AB8883F9	6A271787AB8883F9	68652074696D6520	68652074696D6520
3	893D51EC4B563B53	893D51EC4B563B53	666F7220616C6C20	666F7220616C6C20

B.3 CBC 方式

表 B.3 和表 B.4 分别给出 CBC 方式加密和解密的例子。

表 B.3 CBC 方式加密

i	明文 P_i	分组密码输入分组	分组密码输出分组	密文 C_i
1	4E6F772069732074	5C5B2158F9D8ED9B	E5C7CDDE872BF27C	E5C7CDDE872BF27C
2	68652074696D6520	8DA2EDAAEE46975C	43E934008C389C0F	43E934008C389C0F
3	666F7220616C6C20	25864620ED54F02F	683788499A7C05F6	683788499A7C05F6

表 B.4 CBC 方式解密

i	密文 C_i	分组密码输入分组	分组密码输出分组	明文 P_i
1	E5C7CDDE872BF27C	E5C7CDDE872BF27C	5C5B2158F9D8ED9B	4E6F772069732074
2	43E934008C389C0F	43E934008C389C0F	8DA2EDAAEE46975C	68652074696D6520
3	683788499A7C05F6	683788499A7C05F6	25864620ED54F02F	666F7220616C6C20

B.4 CFB 方式

表 B.5 和表 B.6 分别给出 CFB 方式加密和解密的例子。此例所选的参数为：$j=k=8$ 且 $r=n$。k 位反馈以斜体形式给出。

表 B.5 CFB 方式加密

i	明文 P_i	分组密码输入分组	分组密码输出分组	密文 C_i
1	4E	1234567890ABCDEF	BD661569AE874E25	F3
2	6F	34567890ABCDEF*F3*	7039546F9A0F6330	1F
3	77	567890ABCDEFF3*1F*	AD1B78B0BB371BE7	DA

表 B.6 表 C6 CFB 方式解密

i	密文 C_i	分组密码输入分组	分组密码输出分组	明文 P_i
1	F3	1234567890ABCDEF	BD661569AE874E25	4E
2	1F	34567890ABCDEF*F3*	7039546F9A0F6330	6F
3	DA	567890ABCDEFF3*1F*	AD1B78B0BB371BE7	77

B.5 OFB 方式

表 B.7 和表 B.8 分别给出 OFB 方式加密和解密的例子。此例所选的参数为：$j=64$。

表 B.7 OFB 方式加密

i	明文 P_i	分组密码输入分组	分组密码输出分组	密文 C_i
1	4E6F772069732074	1234567890ABCDEF	BD661569AE874E25	F3096249C7F46E51
2	68652074696D6520	8DA2EDAAEE46975C	5D976A504786581F	35F24A242EEB3D3F
3	666F7220616C6C20	25864620ED54F02F	5B0229C3443694E3	3D6D5BE3255AF8C3

表 B.8 OFB 方式解密

i	密文 C_i	分组密码输入分组	分组密码输出分组	明文 P_i
1	F3096249C7F46E51	1234567890ABCDEF	BD661569AE874E25	4E6F772069732074
2	35F24A242EEB3D3F	8DA2EDAAEE46975C	5D976A504786581F	68652074696D6520
3	3D6D5BE3255AF8C3	25864620ED54F02F	5B0229C3443694E3	666F7220616C6C20

B.6 CTR 方式

表 B.9 和表 B.10 分别给出 CTR 方式加密和解密的例子。此例所选的参数为：

使用的分组密码是高级数据加密标准(AES)，密钥长度为 128 位。

密码密钥为(十六进制)2B7E151628AED2A6ABF7158809CF4F3C。

初始计数器为(十六进制)F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF。

明文是(十六进制)6BC1BEE22E409F96E93D7E117393172A

AE2D8A571E03AC9C9EB76FAC45AF8E51

30C81C46A35CE411E5FBC1191A0A52EF

F69F2445DF4F9B17AD2B417BE66C3710

表 B.9 CTR 方式加密

i	明文 P_i	分组密码输入分组	分组密码输出分组	密文 C_i
1	6BC1BEE22E409F96 E93D7E117393172A	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFEFF	EC8CDF7398607CB0 F2D21675EA9EA1E4	874D6191B620E326 1BEF6864990DB6CE
2	AE2D8A571E03AC9C 9EB76FAC45AF8E51	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF00	362B7C3C67735163 18A077D7FC5073AE	9806F66B7970FDFF 8617187BB9FFFDFF
3	30C81C46A35CE411 E5FBC1191A0A52EF	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF01	6A2CC3787889374F BEB4C81B17BA6C44	5AE4DF3EDBD5D35E 5B4F09020DB03EAB
4	F69F2445DF4F9B17 AD2B417BE66C3710	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF02	E89C399FF0F198C6 D40A31DB156CABFE	1E031DDA2FBE03D1 792170A0F3009CEE

表 B.10 CTR 方式解密

i	密文 C_i	分组密码输入分组	分组密码输出分组	明文 P_i
1	874D6191B620E326 1BEF6864990DB6CE	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFEFF	EC8CDF7398607CB0 F2D21675EA9EA1E4	6BC1BEE22E409F96 E93D7E117393172A
2	9806F66B7970FDFF 8617187BB9FFFDFF	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF00	362B7C3C67735163 18A077D7FC5073AE	AE2D8A571E03AC9C 9EB76FAC45AF8E51
3	5AE4DF3EDBD5D35E 5B4F09020DB03EAB	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF01	6A2CC3787889374F BEB4C81B17BA6C44	30C81C46A35CE411 E5FBC1191A0A52EF
4	1E031DDA2FBE03D1 792170A0F3009CEE	F0F1F2F3F4F5F6F7 F8F9FAFBFCFDFF02	E89C399FF0F198C6 D40A31DB156CABFE	F69F2445DF4F9B17 AD2B417BE66C3710

参 考 文 献

[1] ANSI X 3.92(1981)美国国家标准 信息系统 数据加密算法
[2] FIPS-197(2001)联邦信息处理标准 高级数据加密标准

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
分组密码算法的工作模式
GB/T 17964—2008
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 44 千字
2008 年 9 月第一版 2008 年 9 月第一次印刷
*
书号:155066·1-33626

GB/T 17964-2008