GB

中华人民共和国国家标准

2000年制定

中 国 国 家 标 准 汇 编

269

GB 17964～17975

（2000 年制定）

中 国 标 准 出 版 社

2001

中国国家标准汇编

269

GB 17964～17975

（2000 年制定）

中国标准出版社总编室　编

*

中国标准出版社出版

北京复兴门外三里河北街 16 号

邮政编码：100045

电　　话：68523946　68517548

中国标准出版社秦皇岛印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

开本 880×1230　1/16　印张 45¾　字数 1 399 千字

2001 年 6 月第一版　2001 年 6 月第一次印刷

*

ISBN7-5066-2425-7/TB・698

印数 1—3 000　定价 120.00 元

网址 www.bzcbs.com

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。本《汇编》在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2. 本《汇编》收入我国正式发布的全部国家标准。各分册中如有顺序号缺号的，除特殊情况注明外，均为作废标准号或空号。

3. 由于本《汇编》的出版时间与新国家标准的发布时间已达到基本同步，我社将在每年出版前一年发布的新制定的国家标准，便于读者及时使用。出版的形式不变，分册号继续顺延。

4. 由于标准不断修订，修订信息不能在本《汇编》中得到充分和及时的反映，根据多年来读者的要求，自1995年起，在本《汇编》汇集出版前一年发布的新制定的国家标准的同时，新增出版前一年发布的被修订的标准的汇编版本，视篇幅分设若干分册。这些修订标准汇编的正书名、版本形式与《中国国家标准汇编》相同，但不占总的分册号，仅在封面和书脊上注明“19××年修订-1，-2，-3，…”字样，作为本《汇编》的补充。读者配套购买则可收齐前一年制定和修订的全部国家标准。

5. 由于读者需求的变化，自第201分册起，仅出版精装本。

鉴于国家标准GB 17940～17989制定于2000年，将相应分册结构调整如下：

《中国国家标准汇编》267　GB 17920～17939，GB 17990～18020(1999年制定)；

《中国国家标准汇编》268　GB 17940～17963(2000年制定)；

《中国国家标准汇编》269　GB 17964～17975(2000年制定)；

《中国国家标准汇编》270　GB 17976～17989(2000年制定)。

从第271分册开始将恢复正常的编号顺序，请读者在购买时注意以上变化。

本分册为第269分册，收入国家标准GB 17964～17975的最新版本。

中国标准出版社

2001年2月

目　　录

前　言

本标准等同采用国际标准 ISO/IEC 10116:1997《信息技术　安全技术　n 位块密码算法的操作方式》。

本标准描述 n 位块密码算法的四种操作方式，即：电子密本(ECB)方式、密码块链接(CBC)方式、密码反馈(CFB)方式和输出反馈(OFB)方式。

本标准在技术内容上与国际标准保持一致。

本标准的附录 A、附录 B、附录 C 和附录 D 均是提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位：中国电子技术标准化研究所。

本标准主要起草人：罗韧鸿、向维良。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系和其他官方和非官方国际组织也可参与标准的制定工作。

对于信息技术领域,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的标准草案需分发给国家成员体进行表决。发布一项标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 10116 是 ISO/IEC JTC1"信息技术"联合技术委员会的 SC27"安全技术"分委员会制定的。

该第 2 版替代第 1 版(ISO/IEC 10116:1991)。

附录 A 至附录 D 均为提示的附录。

中华人民共和国国家标准

信息技术　安全技术
n 位块密码算法的操作方式

GB/T 17964—2000
idt ISO/IEC 10116:1997

Information technology—Security techniques—
Modes of operation for an n-bit block cipher

1　范围

本标准描述 n 位块密码算法的四种操作方式。

注：附录 A 包含了对每一种操作方式的性质的说明。

本标准确定了四种规定的操作方式，以便在 n 位块密码的应用中（例如数据传输的保护、数据存储、鉴别），本标准将对诸如操作方式规范和适用的参数值提供一个有用的参照。

2　定义

下列定义适用于本标准。

2.1　块链接　block chaining
一种信息加密方法，每一密文块在密码上依赖于前一个密文块。

2.2　密文　ciphertext
经过变换，信息内容被隐藏起来的数据。

2.3　密码同步　cryptographic synchronization
加密与解密过程的协调一致。

2.4　解密　decipherment
一个相应加密过程的逆。

2.5　加密　encipherment
为了产生密文，即隐藏数据，由密码算法对数据进行的（可逆）变换。

2.6　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 SV。

2.7　初始化值　initialization value
用于定义一个加密过程的启动点的值。

2.8　密钥　key
控制密码变换操作（例如加密、解密）的符号序列。

2.9　n 位块密码　n-bit block cipher
明文块和密文块的长度均为 n 位的块密码。

2.10　明文　plaintext
未加密的信息。

2.11　启动变量（SV）　starting variable (SV)
确定操作方式的启动点的变量。

注：本标准未规定从初始化值导出启动变量的方法。这种方法需在操作方式的应用中描述。

国家质量技术监督局 2000-01-03 批准　　2000-08-01 实施

3 记法

3.1 加密

本标准中，由块密码规定的函数关系记作：

$$C=eK(P)$$

其中：P 是明文块；

C 是密文块；

K 是密钥。

eK 是使用密钥 K 的加密运算。

3.2 解密

对应的解密函数记作：

$$P=dK(C)$$

dK 是使用密钥 K 的解密运算。

3.3 位阵列

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。

3.4 模 2 加

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：

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

3.5 位的选择

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。

3.6 移位运算

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：

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

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

其作用是将阵列 X 的各位左移 k 个位置，舍弃 $X_1,\cdots,X_k$，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，其作用是用 F 完全取代 X。

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

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

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

其中最左边的 m−k 位均为“1”。

4 要求

对于某些所描述的方式来说，可能需要对明文变量进行填充。填充技术不属于本标准的范围。

对于密码反馈(CFB)操作方式(见第 7 章)，定义了三个参数：r、j 和 k。对于输出反馈(OFB)操作方式(见第 8 章)，定义了一个参数：j。当使用这些操作方式中的某一种时，所有通信方都要选择并使用同样的参数值。

5 电子密本(ECB)方式

5.1 用于ECB加密方式的变量是：

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

b) 密钥K。

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

5.2 ECB加密方式描述如下：

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

5.3 ECB解密方式描述如下：

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

6 密码块链接(CBC)方式

6.1 用于CBC加密方式的变量是：

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

b) 密钥K。

c) n位启动变量SV。

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

6.2 CBC加密方式描述如下：

对第1个明文块进行加密：

$$C_1=eK(P_1\oplus SV) \qquad \cdots\cdots (3)$$

随后：

$$C_i=eK(P_i\oplus C_{i-1}) \quad i=2,3,\cdots,q \qquad \cdots\cdots (4)$$

此过程如图1的上半部分所示。启动变量SV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。

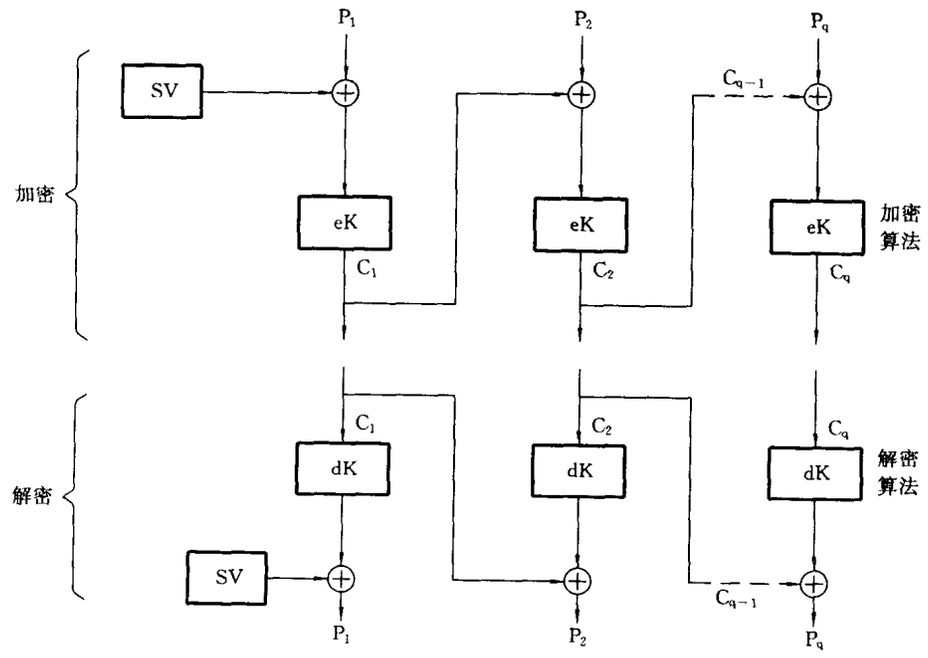

图1 密码块链接(CBC)操作方式

6.3 CBC 解密方式描述如下：

对第 1 个密文块进行解密：

$$P_1=dK(C_1)\oplus SV \qquad \cdots\cdots (5)$$

随后：

$$P_i=dK(C_i)\oplus C_{i-1} \quad i=2,3,\cdots,q \qquad \cdots\cdots (6)$$

此过程如图 1 的下半部分所示。

7 密码反馈(CFB)方式

7.1 下列三个参数定义了 CFB 操作方式：

——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

1 $r-k$ 可小于 n。图 2 示出了 $r-k>n$ 的特殊情形。

2 如果 $r=n$，则此方式与本标准上一版本中所描述的 CFB 方式兼容。

用于 CBC 操作方式的变量是：

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 位启动变量 SV。

b) 中间结果

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

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

3) q 个变量 $E_1,E_2,\cdots,E_q$ 所组成的序列，每个块都为 j 位。

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

7.2 反馈缓存 FB 的初始值置为：

$$FB_1=SV \qquad \cdots\cdots (7)$$

对每个明文变量进行加密的操作采用以下六个步骤：

a)

$$X_i=FB_i\sim n \qquad \cdots\cdots (8)$$

b) 使用块密码：

$$Y_i=eK(X_i) \qquad \cdots\cdots (9)$$

c) 选择最左边 j 位：

$$E_i=Y_i\sim j \qquad \cdots\cdots (10)$$

d) 产生密文变量：

$$C_i=P_i\oplus E_i \qquad \cdots\cdots (11)$$

e) 产生反馈变量：

$$F_i=S_j(I(k)|C_i) \qquad \cdots\cdots (12)$$

f) 在 FB 上进行移位函数操作：

$$FB_{i+1}=S_k(FB_i|F_i) \qquad \cdots\cdots (13)$$

对 $i=1,2,\cdots,q$，重复上述步骤，最后一个循环结束于式(11)。此过程如图 2 的左半部分所示。块密码的输出块 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”位放到明文变量的最左边位置上，将明文变量扩展成 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。

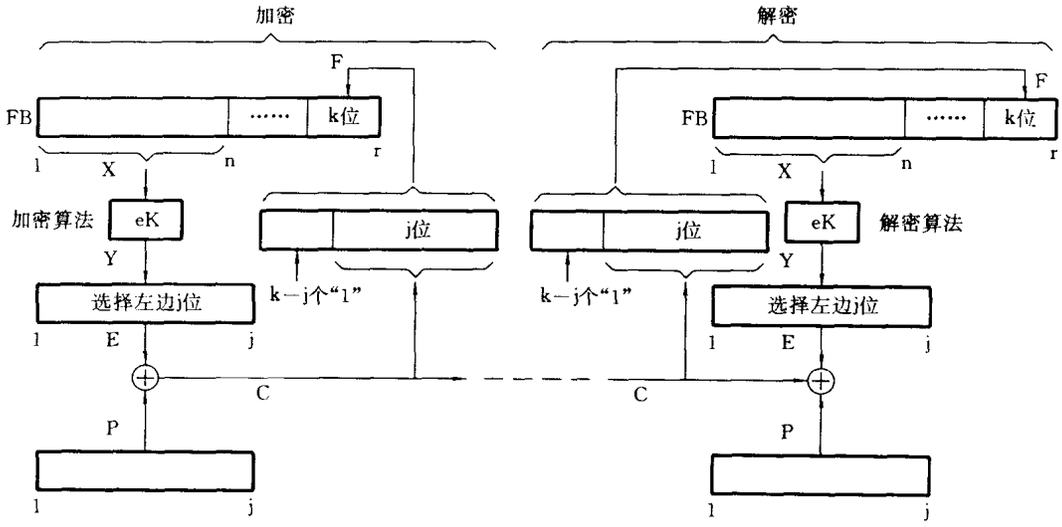

图 2　密码反馈(CFB)操作方式

7.3　用于解密的变量与用于加密的变量是相同的。

反馈缓存 FB 被置成初始值：

$$FB_1=SV \qquad \cdots\cdots (14)$$

对每个密文变量进行解密的操作采用以下六个步骤：

a)　$$X_i=FB_i\sim n \qquad \cdots\cdots (15)$$

b) 使用块密码：

$$Y_i=eK(X_i) \qquad \cdots\cdots (16)$$

c) 选择最左边 j 位：

$$E_i=Y_i\sim j \qquad \cdots\cdots (17)$$

d) 产生明文变量：

$$P_i=C_i\oplus E_i \qquad \cdots\cdots (18)$$

e) 产生反馈变量：

$$F_i=S_j(I(k)\,|\,C_i) \qquad \cdots\cdots (19)$$

f) 在 FB 上进行移位功能操作：

$$FB_{i+1}=S_k(FB_i\,|\,F_i) \qquad \cdots\cdots (20)$$

对 i＝1，2，…，q，重复上述步骤，最后一个循环结束于式(18)。此过程如图 2 的右半部分所示。块密码的输出块 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 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。

7.4　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)，等式(12)和(19)可以写成：

$$F_i=C_i(\text{当 } j=k)$$

8 输出反馈(OFB)方式

8.1 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($1 \leqslant j \leqslant n$)。

用于 OFB 操作方式的变量是：

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 位启动变量 SV。

b) 中间结果

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

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

3) q 个变量 $E_1, E_2, \cdots, E_q$ 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。

8.2 输入块 X 置成初始值：

$$X_1 = SV \qquad \cdots\cdots (21)$$

对每个明文变量进行加密的操作采用以下四个步骤：

a) 使用块密码：

$$Y_i = eK(X_i) \qquad \cdots\cdots (22)$$

b) 选择最左边 j 位：

$$E_i = Y_i \sim j \qquad \cdots\cdots (23)$$

c) 产生密文变量：

$$C_i = P_i \oplus E_i \qquad \cdots\cdots (24)$$

d) 反馈操作：

$$X_{i+1} = Y_i \qquad \cdots\cdots (25)$$

对 $i = 1, 2, \cdots, q$，重复上述步骤，最后一个循环结束于式(24)。此过程如图 3 的左半部分所示。每次使用块密码所产生的结果 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。

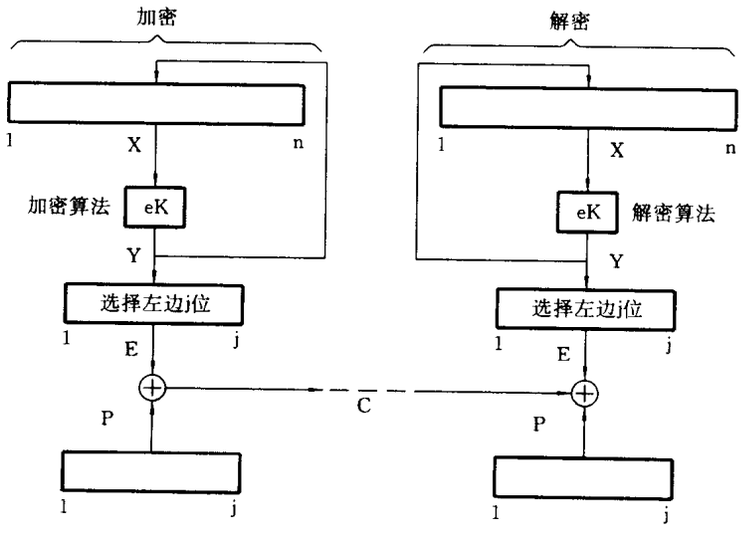

图 3 输出反馈(OFB)操作方式

8.3 用于解密的变量与用于加密的变量是相同的。反馈缓存 FB 被置成初值：

$$X_1 = SV$$

对每个密文变量进行解密的操作采用以下四个步骤：

a）使用块密码：

$$Y_i = eK(X_i) \quad \cdots\cdots (26)$$

b）选择最左边 j 位：

$$E_i = Y_i \sim j \quad \cdots\cdots (27)$$

c）产生明文变量：

$$P_i = C_i \oplus E_i \quad \cdots\cdots (28)$$

d）反馈操作：

$$X_{i+1} = Y_i \quad \cdots\cdots (29)$$

对 $i = 1, 2, \cdots, q$，重复上述步骤，最后一个循环结束于式(28)。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；仅有式(28)是不同的。

附 录 A
（标准的附录）
操作方式的性质

A1 电子密本(ECB)操作方式的性质

A1.1 环境

在各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是共同使用的序列。在ECB方式中，相同的明文块(对于相同的密钥)产生相同的密文块。

A1.2 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块进行；

b) 对密文块的重排将导致明文块的相应重排；

c) 相同的明文块(对于相同的密钥)总是产生相同的密文块，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块构成的。

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。

A1.3 填充要求

只有n位的倍数才能被加密或解密。其他长度需要被填充至n位边界。

A1.4 差错扩散

在ECB方式中，在一个密文块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块的解密将导致对应的明文块中每个明文位出错的概率为50%。

A1.5 块边界

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

A2 密码块链接(CBC)操作方式的性质

A2.1 环境

只要使用同样的密钥和启动变量对相同的明文进行加密，CBC方式应将产生相同的密文。关心这种性质的用户需要采用某种办法来改变明文的开始、密钥或启动变量。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，它使用诸如启动变量的某个值，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)。

A2.2 性质

CBC的性质有：

a) 链接操作使得密文块依赖于当前的和所有以前的明文块，因此对密文块的重新安排不会导致对相应的明文块的重新安排；

b) 使用不同的SV值从而防止同一明文加密成同一密文。

A2.3 填充要求

只有n位的倍数才能被加密或解密。其他长度需填充至n位边界。如果这是不可接受的，可以按一种特殊的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最后变量(即：一个$j<n$位的变量P_q，其中q应大于1)的可能的办法是

按下面的描述的 OFB 方式对它进行加密：

a) 加密

$$C_q=P_q\oplus(eK(C_{q-1})\sim j) \quad \cdots\cdots (30)$$

b) 解密

$$P_q=C_q\oplus(eK(C_{q-1})\sim j) \quad \cdots\cdots (31)$$

但是，如果 SV 不是秘密的或者与同一个密钥一起被多次使用(见 A4)，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 位块，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}导出的密文块。令

$$C_q=eK(S_j(C_{q-1}|P_q)) \quad \cdots\cdots (32)$$

因此最后两个密文变量是 C_{q-1}和 C_q。

b) 解密

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

$$S_j(C_{q-1}|P_q)=dK(C_q) \quad \cdots\cdots (33)$$

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。

A2.4 差错扩散

在 CBC 方式中，在一个密文块中的一个或多个位差错将会影响对两个块(即发生差错的块和随后的块)的解密。第 i 个密文块中的一个差错对于所产生的明文有以下影响：第 i 个明文块每位出错的概率为 50%。第 i+1 个明文块的差错模式与第 i 个密文块的相同。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。

A2.5 块边界

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

A3 密码反馈(CFB)操作方式的性质

A3.1 环境

只要使用同样的密钥和启动变量对相同的明文进行加密，CFB 方式应将产生相同的密文。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、密钥或启动变量。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，它使用诸如启动变量的某个值，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)。

A3.2 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 SV 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≥n+k 使得能对块密码进行流水线式连续操作。

A3.3 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。

A3.4 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。在所有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%。

A3.5 同步

如果加密和解密之间的块边界丢失了(例如由于一个位滑动)，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 位之后将自动重新建立同步。

A4 输出反馈(OFB)操作方式的性质

A4.1 环境

只要使用同样的密钥和启动变量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 SV 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 SV 只应使用一次。

A4.2 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 SV 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块密码的加密操作；

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块密码操作，因而引起更大的处理开销。

A4.3 填充要求

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

A4.4 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。

A4.5 同步

OFB 方式不是自同步的。如果加密和解密两个操作不同步，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位所引起。

每次重新初始化应使用一个 SV 值，它不同于与同一个密钥一起使用的以前的 SV 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。”