分组密码的工作模式

西安邮电大学

2021/6/20

主要内容

1 电码本(ECB)模式

2 密码分组链接(CBC)模式

3 密码反馈(CFB)模式

4 输出反馈(OFB) 模式

5 计数器(CTR) 模式

- **分组密码算法：只能加密固定长度的明文。**

  如：DES可以对一个64比特的明文分组进行加密，

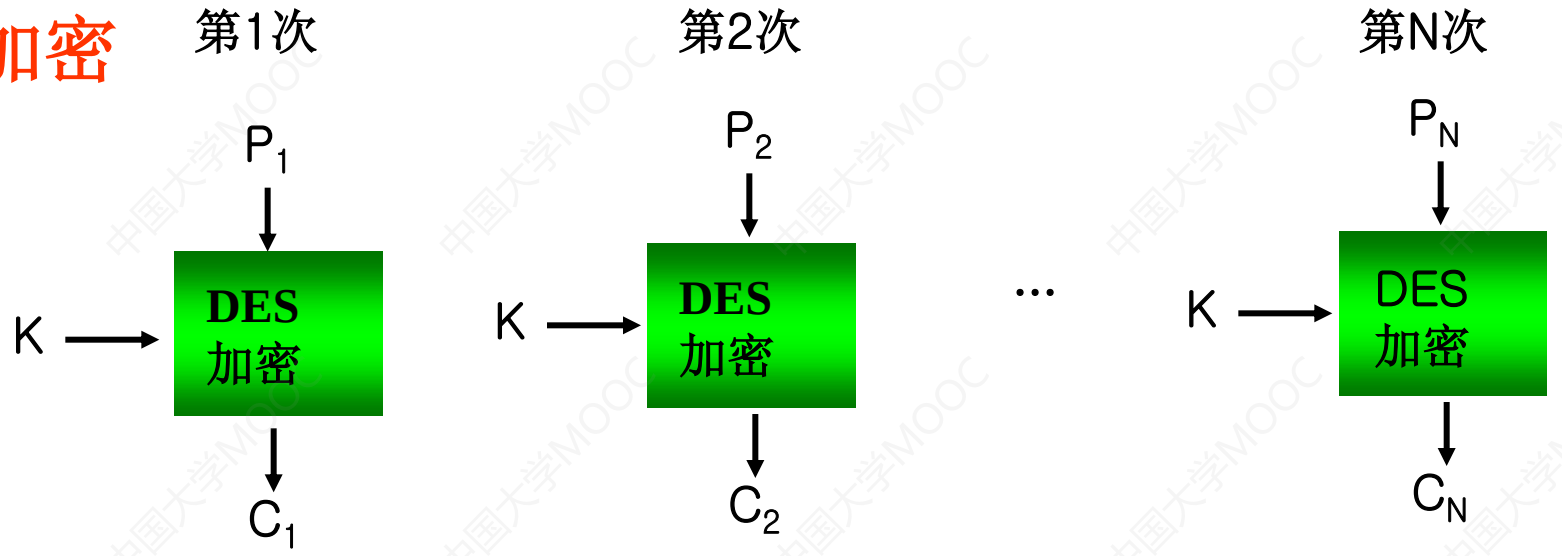
  AES可以对一个128比特的明文分组进行加密

- **分组密码的工作模式：使用分组密码算法（如DES、AES等），对任意长度的明文进行加密的密码方案。**

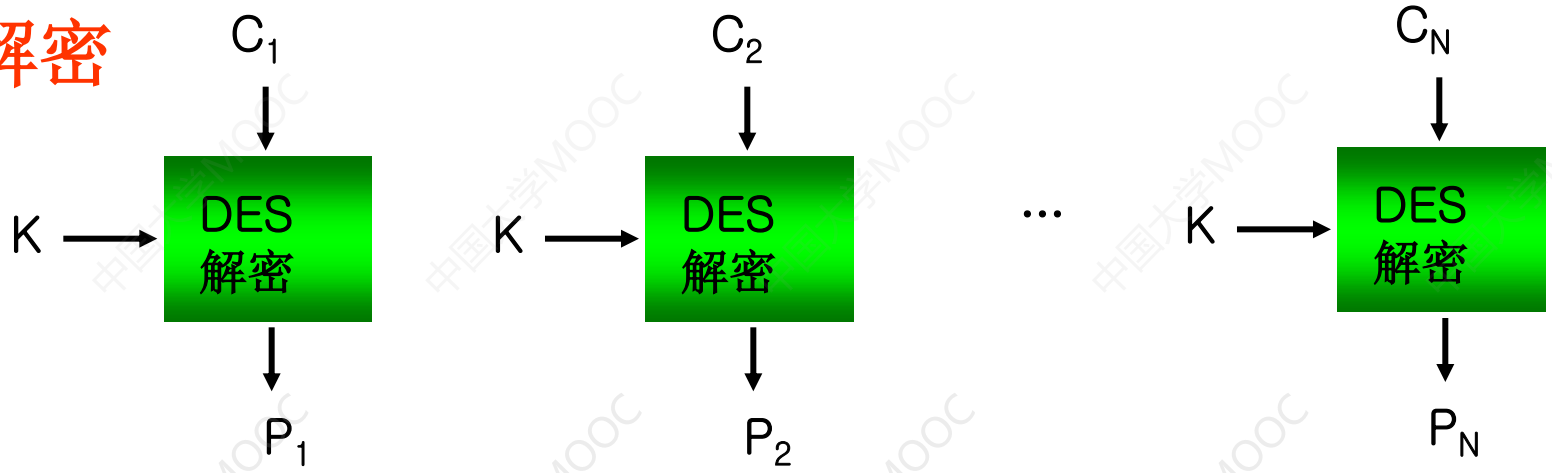
1.电码本(ECB)模式

- ECB模式是将明文的各个分组独立地使用同一密钥k加密。由于这种工作模式类似于电报密码本中指定码字的过程，所以被形象地称为电码本模式。

ECB加密



ECB解密



ECB模式的优、缺点及应用

优点：(1) 实现简单;

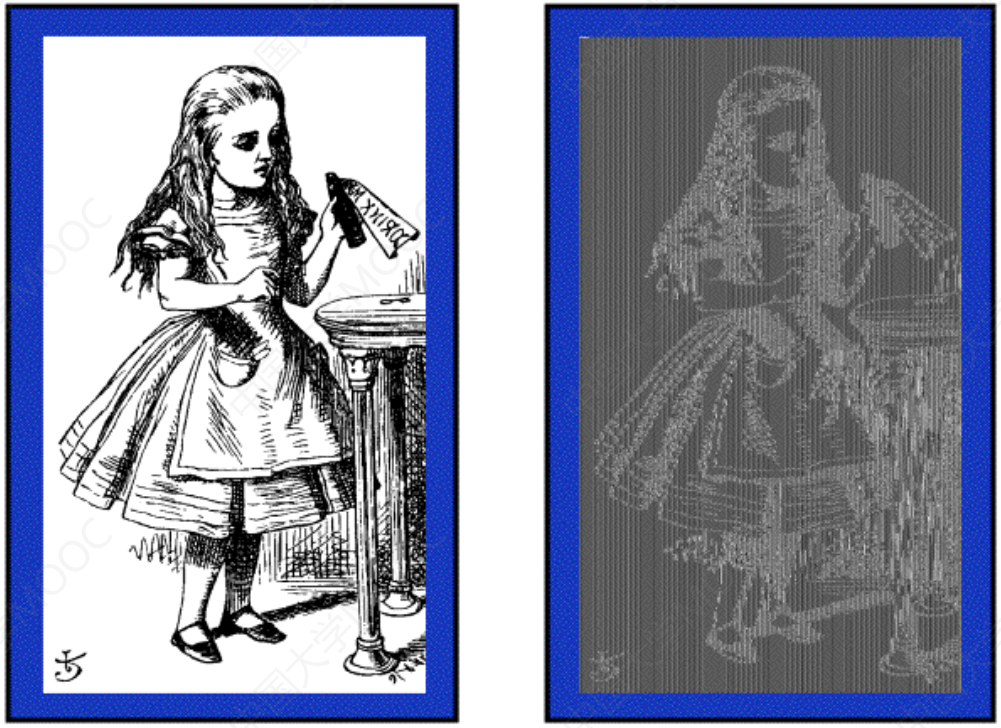
(2) 不同明文分组的加密可并行实施,尤其是硬件实现时速度很快.

缺点：不同的明文分组之间的加密独立进行,故保留了单表代替缺点,造成相同明文分组对应相同密文分组,因而不能隐蔽明文分组的统计规律和结构规律,不能抵抗替换攻击.

典型应用：（1）用于随机数的加密保护；

（2）用于单分组明文的加密。

ECB模式不能隐蔽明文分组的**数据格式。**



ECB模式加密的图像

ECB容易受到替换攻击

例：假设分组长度为128比特,对于某银行，有转账请求“从A-5374账户向B-6671账户转账1亿元”，明文用16进制表示为：

- 明文分组1=41 2D 35 33 37 34 20 20 20 20 20 20 20 20 20 20 (付款人：A-5374)
- 明文分组2=42 2D 36 36 37 31 20 20 20 20 20 20 20 20 20 20（收款人：B-6671）
- 明文分组3=31 30 30 30 30 30 30 30 30 20 20 20 20 20 20 20（转帐金额：100000000）

下面我们用ECB模式进行加密，从加密后的数据看不出明文分组的内容。

- 密文分组1=59 7D DE CC EF EC BA 9B BF 83 99 CF 60 D2 59 B9 (付款人：？？？？)
- 密文分组2=DF 49 2A 1C 14 8E 18 B6 53 1F 38 BD 5A A9 D7 D7（收款人：？？？？）
- 密文分组3=CD AF D5 9E 39 FE FD 6D 64 8B CC CB 52 56 8D 79（转帐金额：？？？？）

接下来，攻击者将密文分组1和2的内容对调：

- 密文分组1=DF 49 2A 1C 14 8E 18 B6 53 1F 38 BD 5A A9 D7 D7(付款人：？？？？)
- 密文分组2=59 7D DE CC EF EC BA 9B BF 83 99 CF 60 D2 59 B9 （收款人：？？？？）
- 密文分组3=CD AF D5 9E 39 FE FD 6D 64 8B CC CB 52 56 8D 79（转帐金额：？？？？）

银行对上述信息解密后，就会变成下面这样

- 明文分组2=42 2D 36 36 37 31 20 20 20 20 20 20 20 20 20 20(付款人： B-6671)
- 明文分组1=41 2D 35 33 37 34 20 20 20 20 20 20 20 20 20 20 （收款人： A-5374）
- 明文分组3=31 30 30 30 30 30 30 30 30 20 20 20 20 20 20 20（转帐金额：100000000）

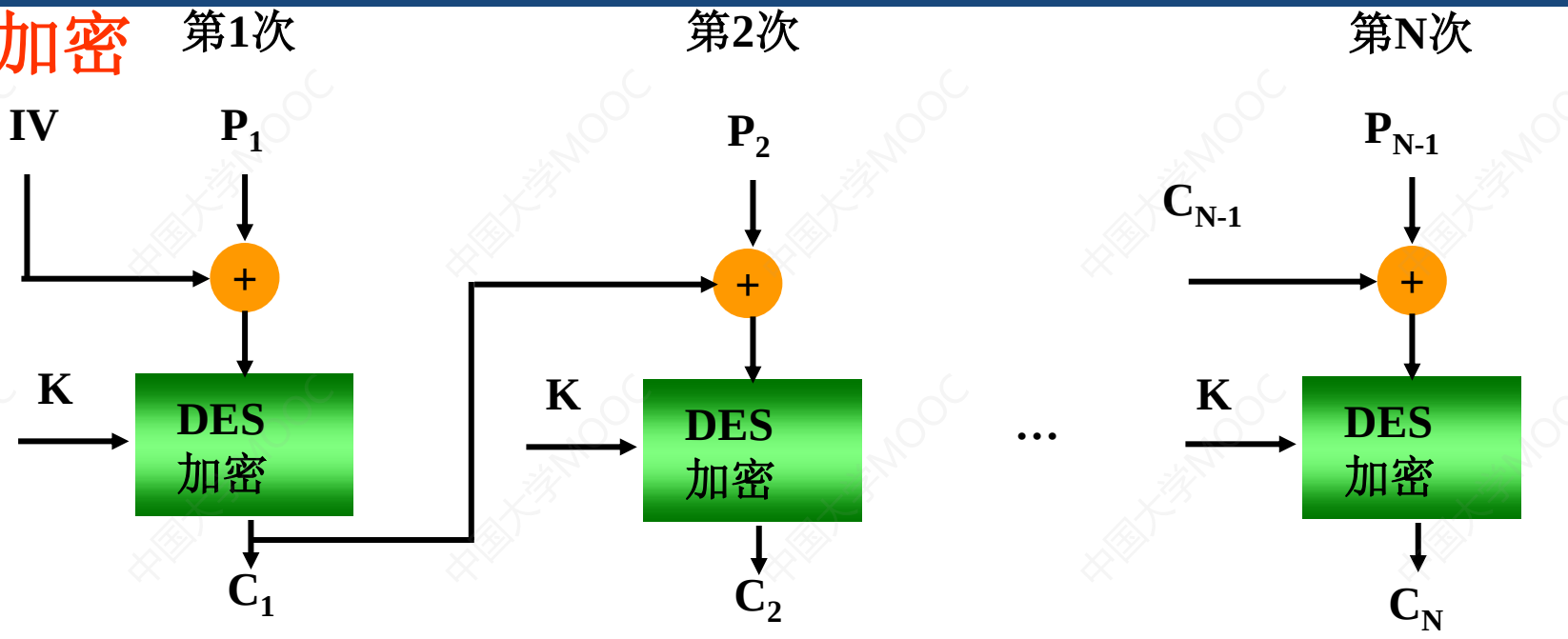
原本请求的内容是从：A-5374 账户向B-6671账户转帐1亿元，现在变成从B-6671账户向A-5374账户转帐1亿元，完全相反。

通过这个例子可以看出，ECB模式的一个弱点就是可以在不破译密文的情况下操纵明文。

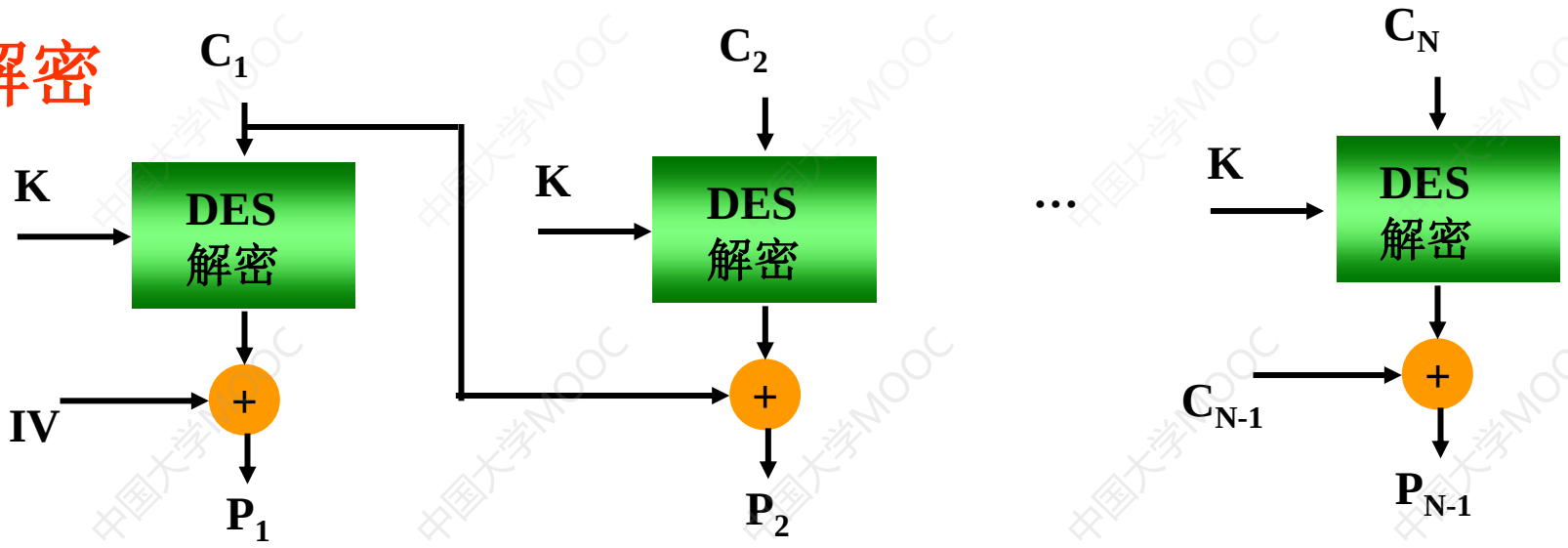
2.密码分组链接(CBC)模式

- CBC模式的加密：将当前明文分组与前一个密文分组进行异或后在进行加密操作。第一个明文分组之前没有密文分组，需要将第一个明文分组与一个初始向量IV进行异或。
- CBC模式的解密：将当前密文分组解密操作，然后与前一个密文分组进行异或。

CBC加密


第1次
第2次
第N次
IV
P_1
P_2
P_{N-1}
C_{N-1}
+
K
DES
加密
…
C_1
C_2
C_N

CBC解密


C_1
C_2
C_N
K
DES
解密
…
IV
+
C_{N-1}
P_1
P_2
P_{N-1}

CBC模式中的IV（初始向量）

- 随机数。每次加密前随机产生，使得相同的明文，加密后得到不同的密文。
- 为了解密能够顺利进行，发送方和接受方都应该知道IV。
- IV 无须保密，可以以明文形式传输。

CBC模式的特点

- **1. 明文块的统计特性得到了隐蔽。** 由于在密文CBC模式中，各密文块不仅与当前明文块有关，而且还与以前的明文块及初始化向量有关，从而使明文的统计规律在密文中得到了较好的隐蔽。
- **2. 具有有限的(两步)错误传播特性。** 一个密文块的错误将导致两个密文块不能正确解密。
- **3. 具有自同步功能。** 密文出现丢块和错块不影响后续密文块的脱密. 若从第t块起密文块正确,则第t+1个明文块就能正确求出。

CBC模式的典型应用

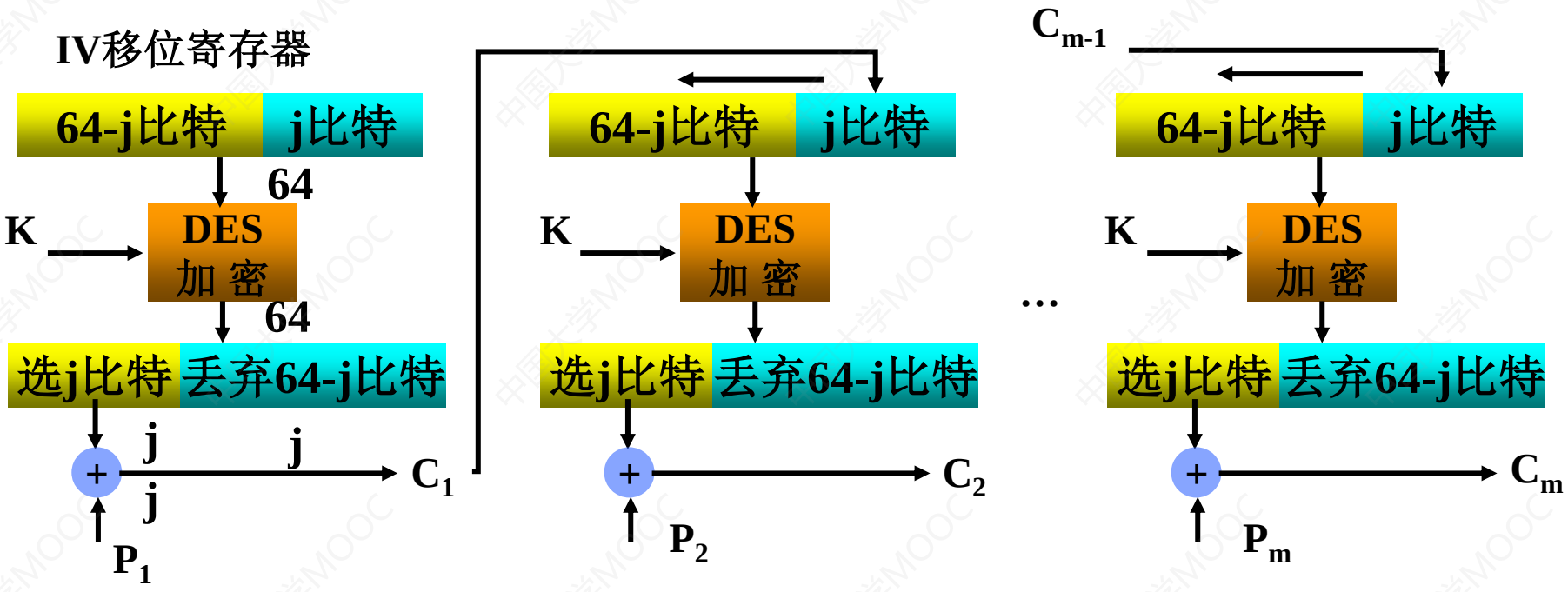
(1) 数据加密;

(2) 完整性认证和身份认证;

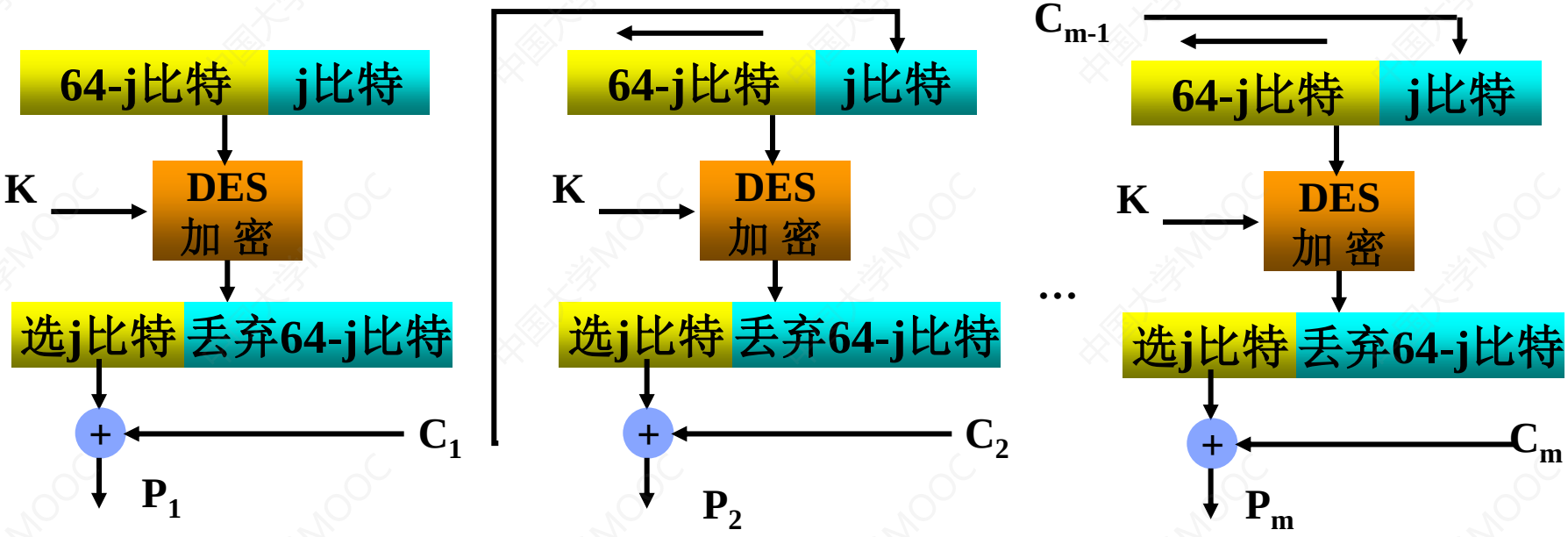
3．密码反馈(CFB)模式

- CFB模式中，使用分组密码 E（如DES和AES等）对大小为 n 的移位寄存器内容进行加密，对其输出结果选取最右边的 j 比特作为密钥序列。其中当前移位寄存器的内容是上一次移位寄存器的内容向左移位j比特后，接着用前一个密文序列补齐最右边的j比特得到。
- j比特CFB模式的加密：加密是 j 比特明文序列异或 j 比特密钥序列来得到密文序列。
- j比特CFB模式的解密： j 比特密文序列异或 j 比特密钥序列来得到明文序列。

CFB加密


IV移位寄存器
64-j比特
j比特
64
K
DES
加 密
64
选j比特
丢弃64-j比特
j
j
j
+
C1
P1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C2
P2
Cm-1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
Cm
Pm
…

CFB解密


64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C1
P1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C2
P2
Cm-1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
Cm
Pm
…

CFB模式的优、缺点及应用

优点：

1.隐藏明文的数据格式。

2.每一次可以加密j比特明文块，因此灵活适应各种数据格式的需求。比如，数据库加密要求加密时不能改变明文的字节长度，这时就要以明文字节长度为单位进行加密。

缺点：

1.加解密效率低：一次只能完成 j个比特明密文数据的加解密。

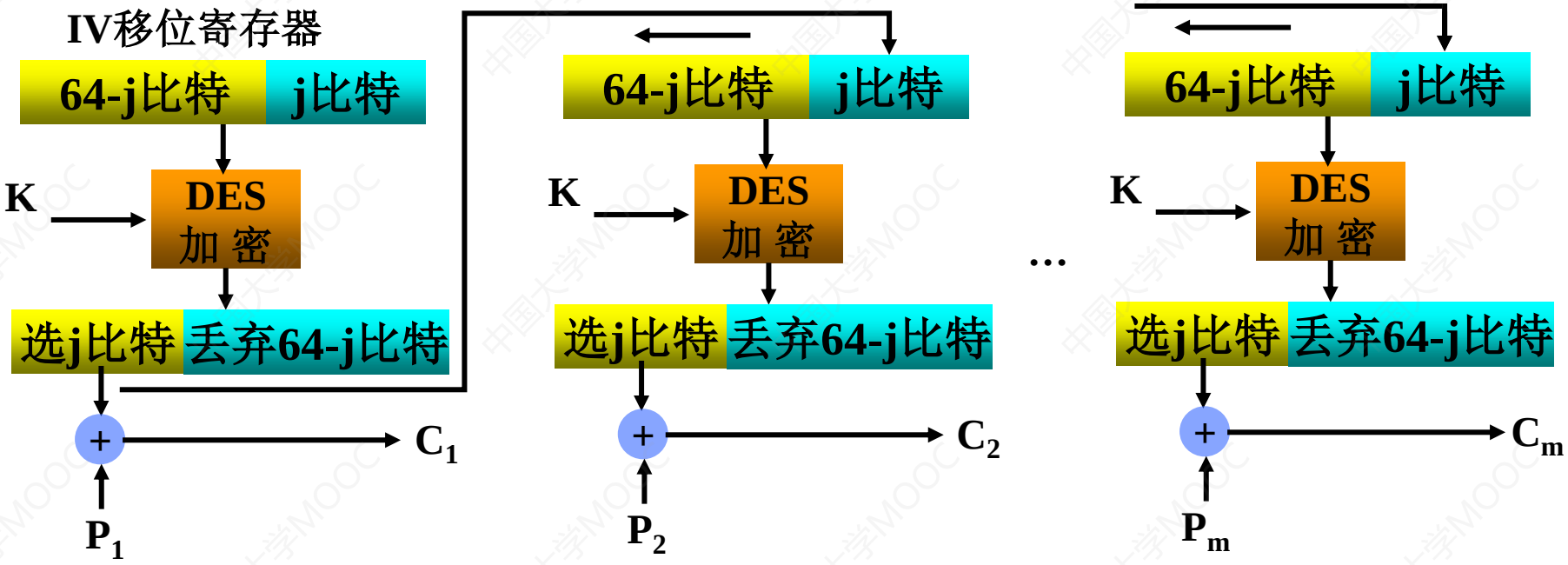
2.会造成错误传播：因为CFB是自同步序列密码：密钥序列依赖于密文。所以，密文某个比特错误，解密后不仅可以导致在明文相同位置产生一个单比特错误；同时，只要这一密文错误还在移位寄存器中，就会造成相应密钥序列和明文序列的错误。

应用：数据库加密等对数据格式有特殊要求的应用环境。

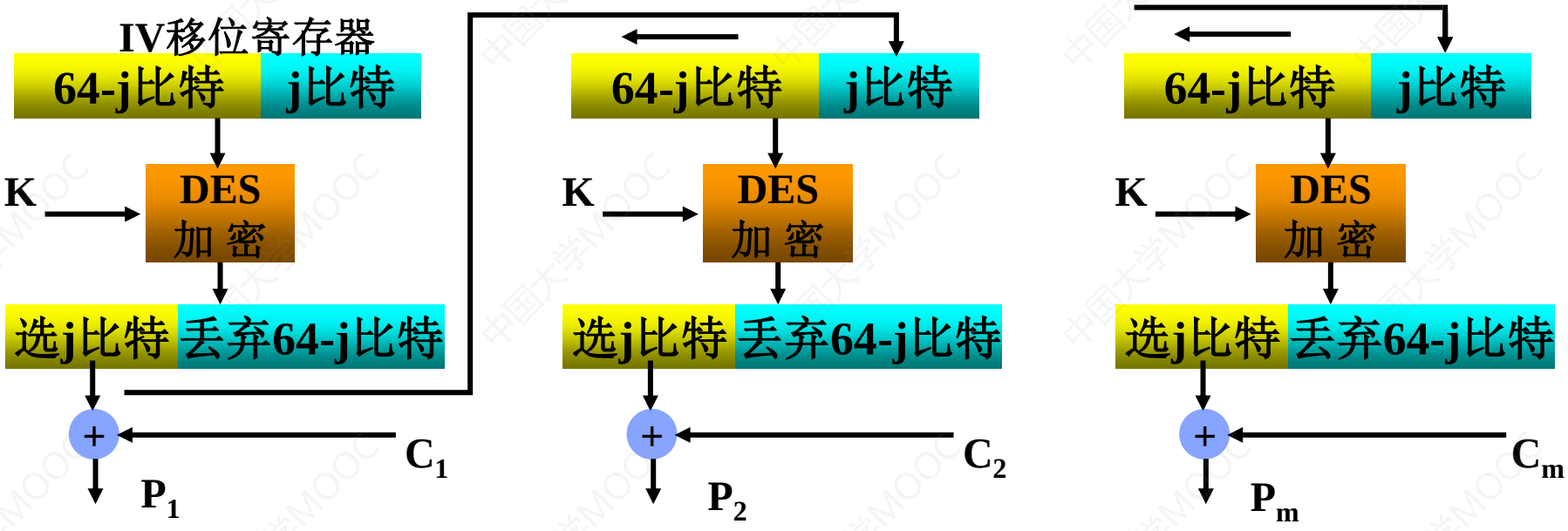
4. 输出反馈(OFB)模式

- **OFB 模式在结构上类似于CFB 模式，但反馈的内容是分组密码算法 E 输出的密钥序列（最左边 j 比特）而不是密文！j比特CFB模式的加密：加密是 j 比特明文序列异或 j 比特密钥序列来得到密文序列。**
- **j比特OFB模式的加密： j 比特明文序列异或 j 比特密钥序列得到 j 比特密文序列。**
- **j比特OFB模式解密： j 比特密文序列异或 j 比特密钥序列得到 j 比特明文序列。**

OFB加密


IV移位寄存器
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C1
P1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C2
P2
…
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
Cm
Pm

OFB解密


IV移位寄存器
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C1
P1
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
C2
P2
64-j比特
j比特
K
DES
加 密
选j比特
丢弃64-j比特
+
Cm
Pm

CFB模式的优、缺点及应用

优点：

1.不具有错误传播特性。因为OFB是同步序列密码：密钥序列的产生独立于密文，所以，密文某个比特错误，解密后仅会导致在明文相同位置产生一个单比特错误。

2.隐蔽明文的数据格式 。

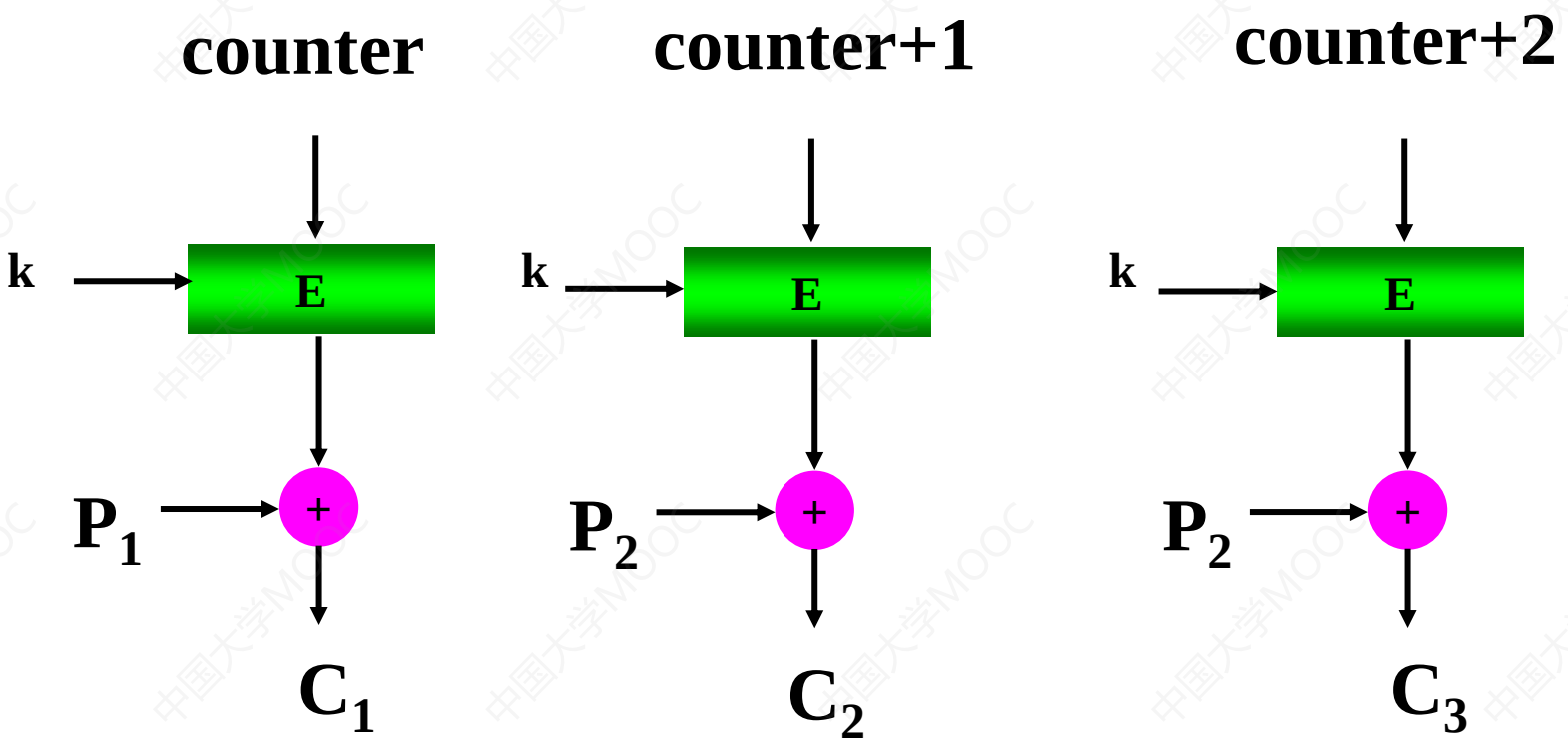
缺点： 加解密效率低。

应用： 图像加密、语音加密。

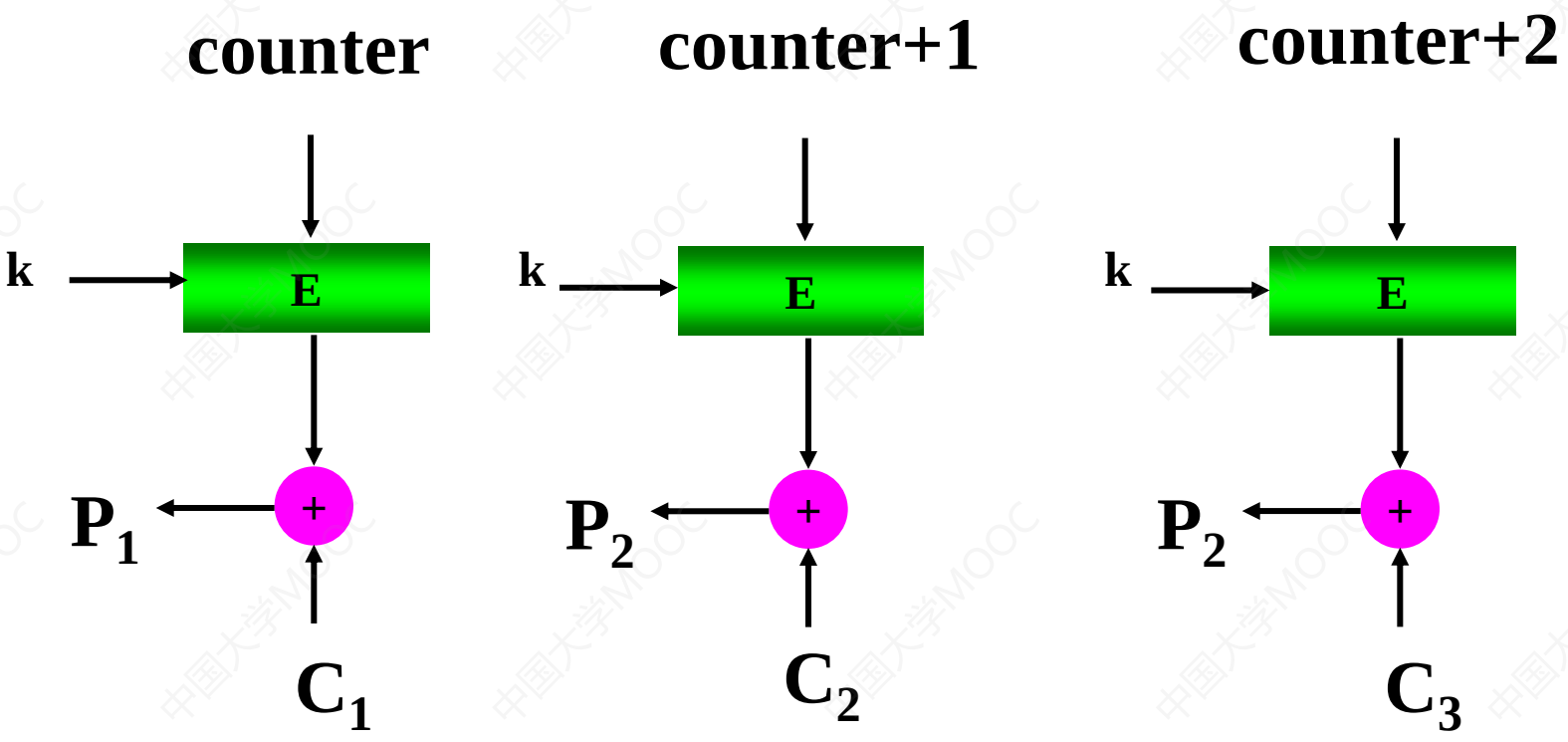
5. 计数器 (CTR) 模式

- CTR模式中，每个分组对应一个逐次累加的计数器，并使用分组密码 E（如DES和AES等）对计数器进行加密来生成密钥序列。
- CTR的加密：明文序列异或密钥序列得到密文序列。
- CTR解密：密文序列异或密钥序列得到明文序列。

CTR加密



CTR解密



CTR模式的优点及应用

优点：

1.可并行 执行： 因为计数器模式各块儿可单独处理。

2.可预处理： 明文不参与密钥产生。

应用： 随机存取数据的加密。