《现代密码学》第四讲

分组密码（四）

《现代密码学》第四讲

分组密码算法的运行模式

本节主要内容

- SMS4 加 / 解密算法
- SMS4 密钥编排算法
- 分组密码算法的运行模式

分组密码的运行模式

分组密码在加密时，明文分组的长度是固定的，而实际应用中待加密消息的数据量是不定的，数据格式多种多样.

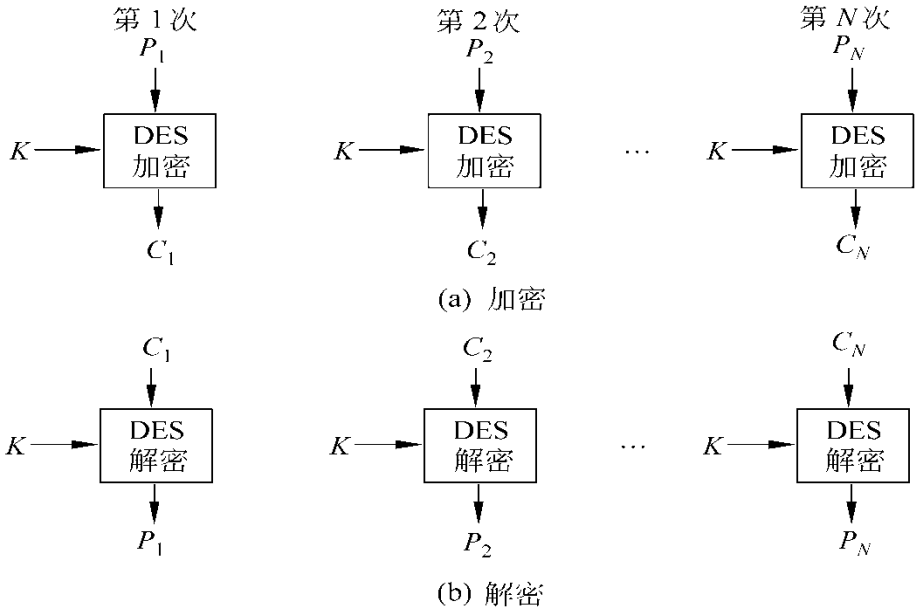
1） 为了能在各种应用场合使用 DES，美国在 FIPS PUS 74 和 81 中定义了 DES 的 4 种运行模式：ECB, CBC, CFB, OFB

2） FIPS PUB 140-2 推荐了 AES 的另外一种运行模式：CTR

分组密码的运行模式

- 1 ECB（electronic codebook）模式

最简单的运行模式，首先将明文分为64比特（调用的分组密码算法的分组长度）的明文块，它一次对一个64比特长的明文分组加密，每次的加密密钥都相同



分组密码的运行模式

- 如果明文长于 64 比特，首先将其分为长为 64 比特的分组； 若最后一个分组如果不够 64 比特，则需要填充；
- 明文加密过程和解密过程分别调用加密算法和解密算法 .
- 不需要额外的初始向量 .

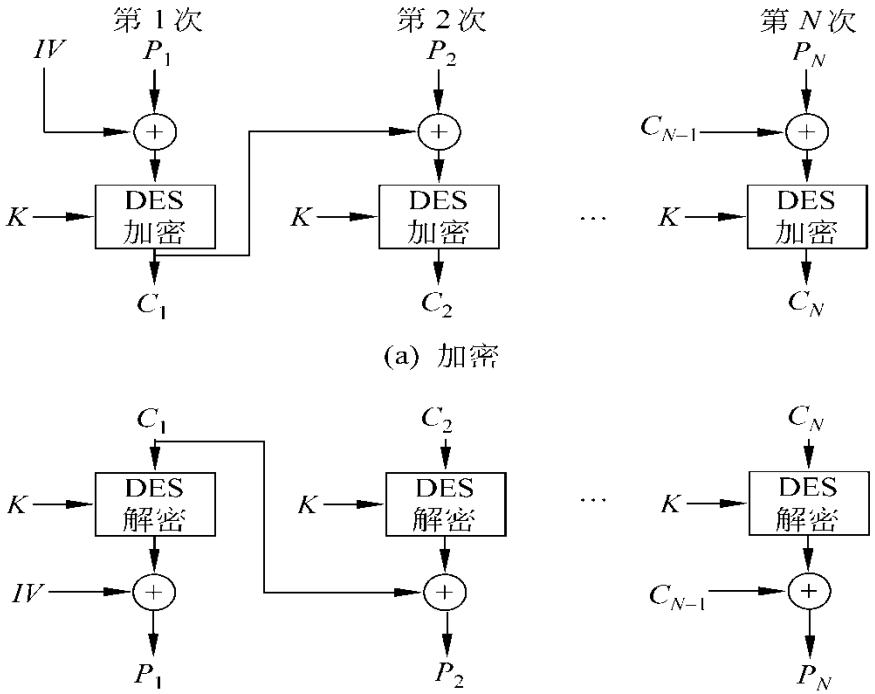
分组密码的运行模式

- 密文块可以分别独立解密，无顺序要求．
- 密钥相同时，明文中相同的 64 比特分组产生相同的 64 比特密文块；
- 不存在错误传播，一块密文传送错误只导致对应明文解密错误；
- 主要用于发送少数量的分组数据．

分组密码的运行模式

- 2 CBC（cipher block chaining）模式

首先对明文分组，它一次对一个明文分组加密，加密算[illegible]和前一次密文分组的



分组密码的运行模式

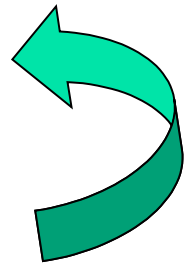
注：在产生第 1 个密文分组时，需要有一个初始向量 IV 与第 1 个明文分组异或． 解密时， IV 和解密算法对第 1 个密文分组的输出进行异或以恢复第 1 个明文分组． IV 对于收发双方都应是已知的，为使安全性最高， IV 应像密钥一样被保护 （可使用 ECB 加密模式来发送 IV)． 如果敌手能欺骗接收方使用不同的 IV 值，则接收方收到的 P1 中相应的比特也发生了变化

$$C_1 = E_K[IV \oplus P_1] \qquad P_1(i) = IV(i) \oplus D_K[C_1](i)$$

$$P_1 = IV \oplus D_K[C_1] \qquad P_1(i) = IV(i) \oplus D_K[C_1](i)$$

分组密码的运行模式

- 如果消息长于 64 比特，首先将其分为长为 64 比特的分组，最后一个分组如果不够 64 比特，则需要填充 .
- 明文加密过程和解密过程分别调用加密算法和解密算法 .
- 需要额外的初始向量，若初始向量公开，攻击者可以通过篡改，使第 1 块明文解密错误
- 密文块需按顺序逐一解密 .



分组密码的运行模式

- 密钥相同时，明文中相同的 64 比特分组产生不相同的 64 比特密文块；
- 存在错误传播，一块密文传输错误会导致下一块密文解密失败
- 适合加密长度大于 64 比特的消息

分组密码的运行模式

- 3 CFB（cipher feedback）模式

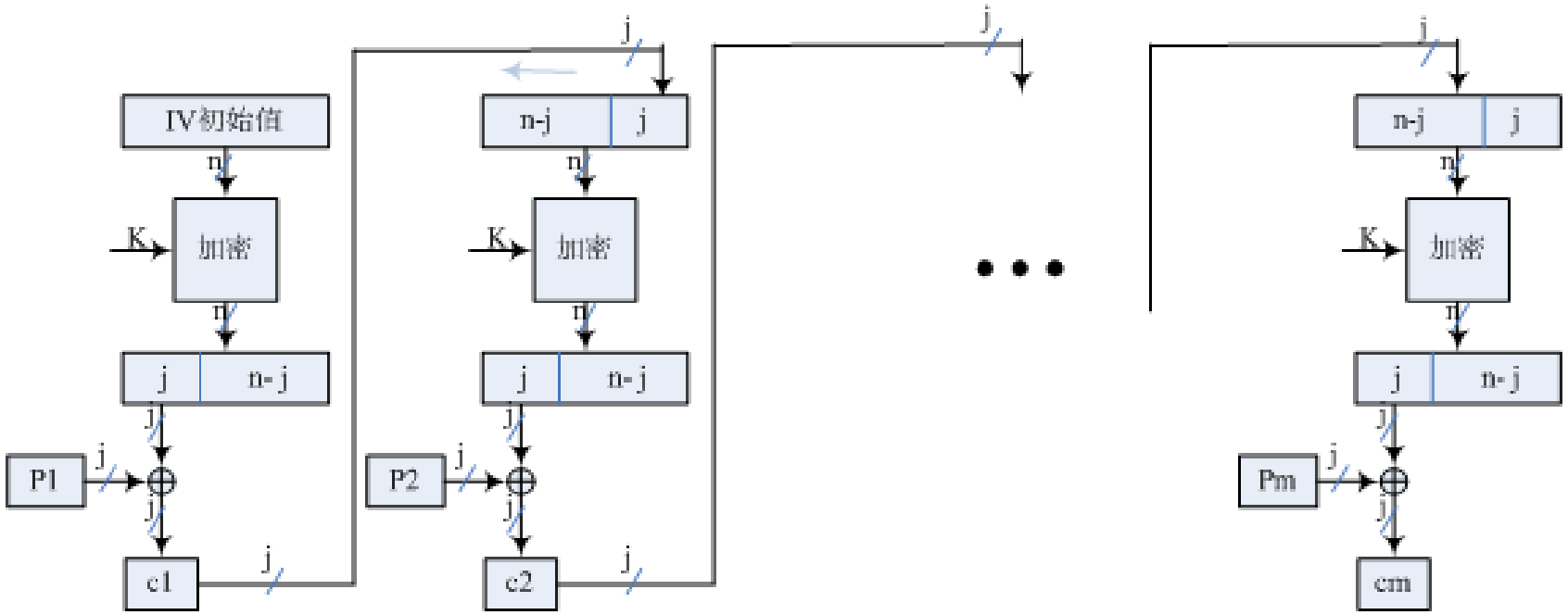
设传送的每个单元（如一个字符）是 j 比特，0<j<64 长，通常取 j=8.

加密时，设加密算法的输入是 64 比特移位寄存器，其初值为某个初始向量 IV. 加密算法输出的最左（最高有效位）j 比特与明文的第一个单元 P_1 进行异或，产生出密文的第 1 个单元 C_1. 传送该单元并将输入寄存器的内容左移 j 位，用 C_1 补齐最右边（最低有效位）j 位. 这一过程继续到明文的所有单元都被加密为止.

解密时，将加密算法输出的最左（最高有效位）j 比特与密文的相应单元异或，产生明文. 反馈到输入寄存器的值为密文单元.

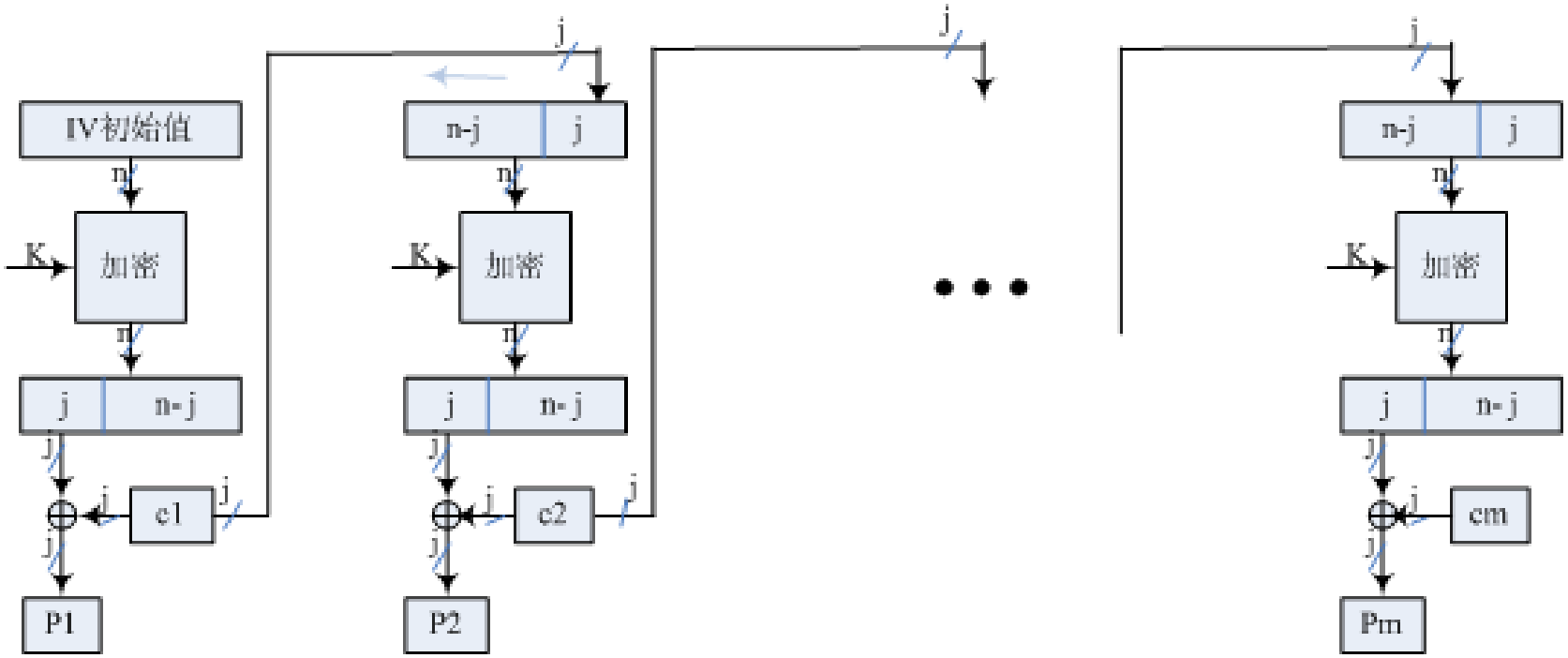
分组密码的运行模式

- CFB 加密模式



分组密码的运行模式

- CFB 解密模式



分组密码的运行模式

- 消息被看作bit流，无须分组填充；适合数据以比特或字节为单位出现标准允许反馈任意比特 （1,8 or 64 or whatever）记作CFB-1，CFB-8，CFB-64
- 只使用DES加密算法，且所有加密都使用同一密钥.
- 需要额外的初始向量，若初始向量公开，攻击者可以通过篡改，使前几块（与错误比特几次移出寄存器有关）明文解密错误.

分组密码的运行模式

- 密文块需按顺序逐一解密 .
- 密钥相同时，明文中相同的 64 比特分组产生不相同的 64 比特密文块 .
- 存在错误传播（只传播后面的几块） .

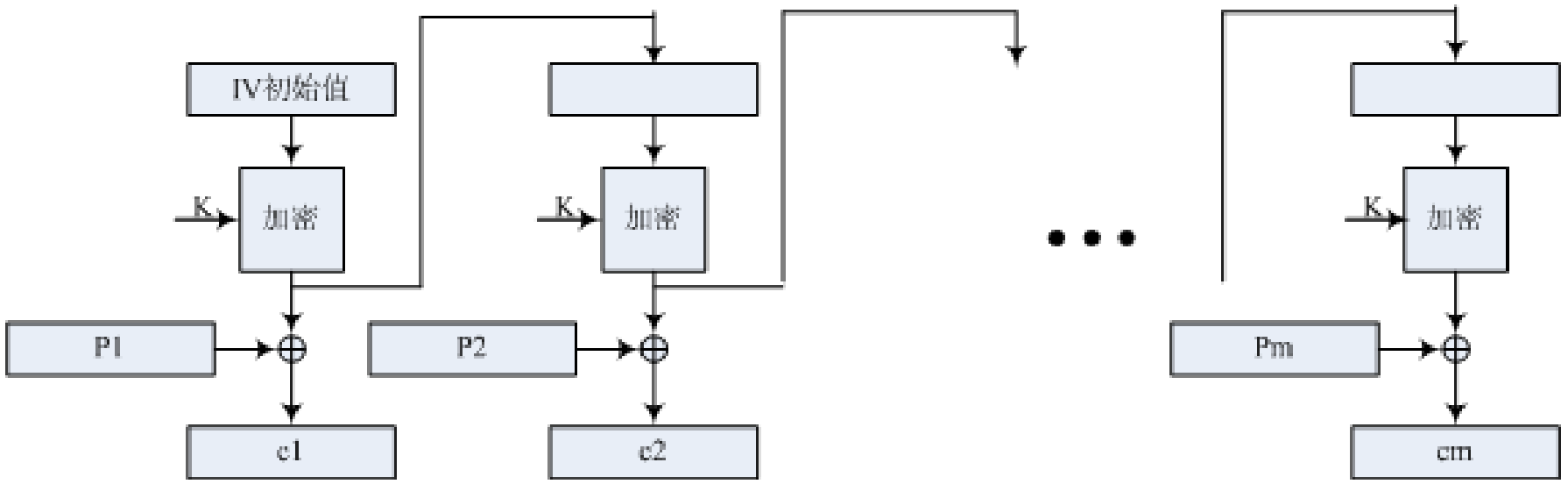
分组密码的运行模式

- 4 OFB （output feedback）模式

类似于 CFB， 不同之处在于 OFB 模式是将加密算法的输出反馈到移位寄存器，而 CFB 模式中是将密文单元反馈到移位寄存器。

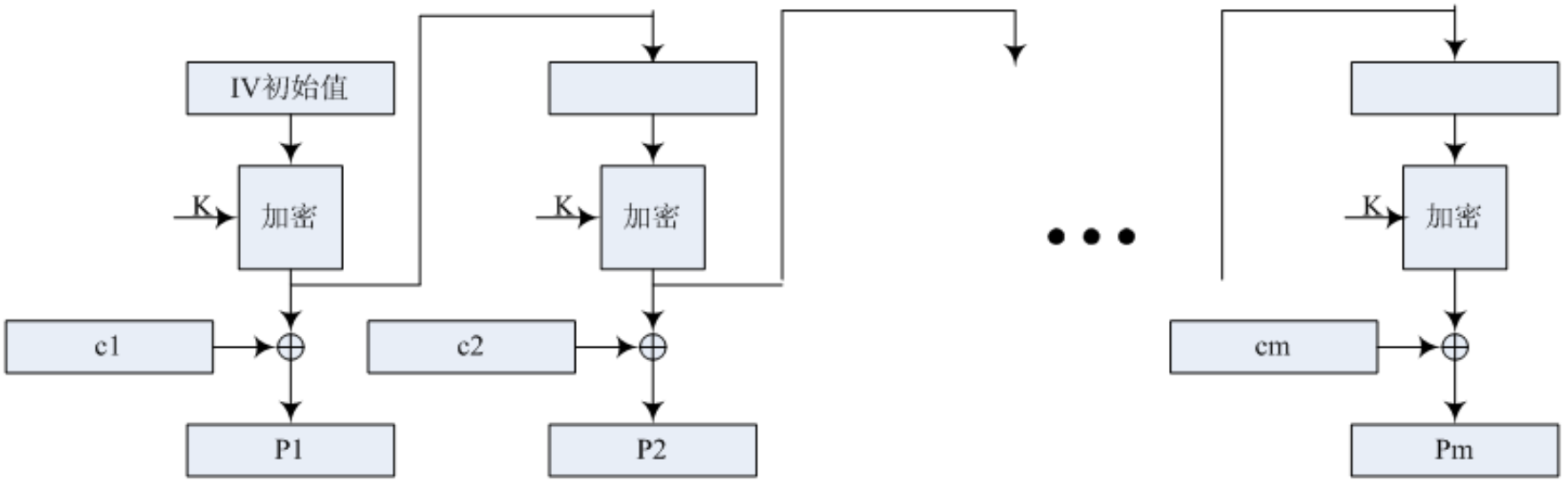
分组密码的运行模式

加密模式



分组密码的运行模式

解密模式



分组密码的运行模式

- 消息被看作比特流，无须分组填充．
- 只使用 DES 加密算法，且所有加密都使用同一密钥．
- 需要额外的初始向量，若初始向量公开，攻击者可以通过篡改，使所有明文解密错误．
- 密钥流可以在已知消息之前计算，不需要按顺序解密．
- 密钥相同时，明文中相同的 64 比特分组产生不相同的 64 比特密文块．
- 不存在比特错误传播．
- 发送者和接收者必须保持同步．

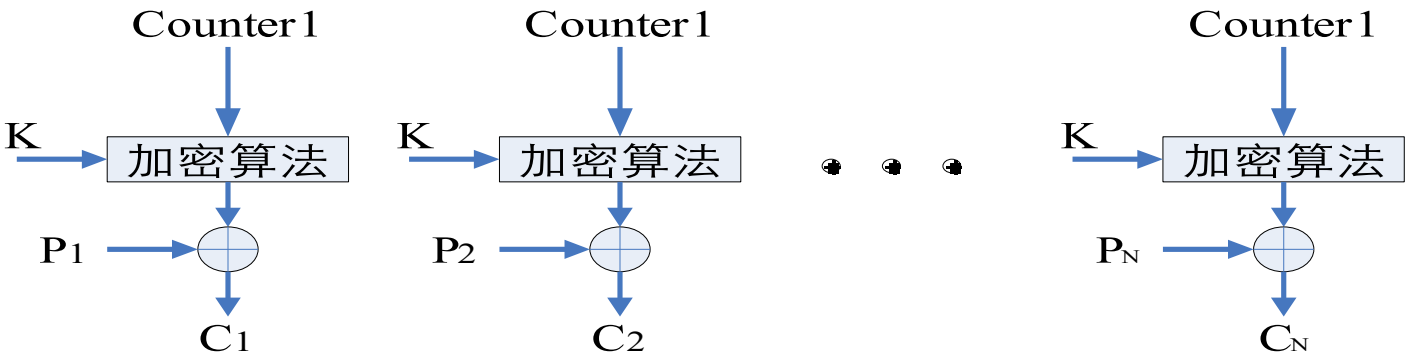
分组密码的运行模式

- Vernam 密码的改进版，(key+IV) 不能重复使用 .

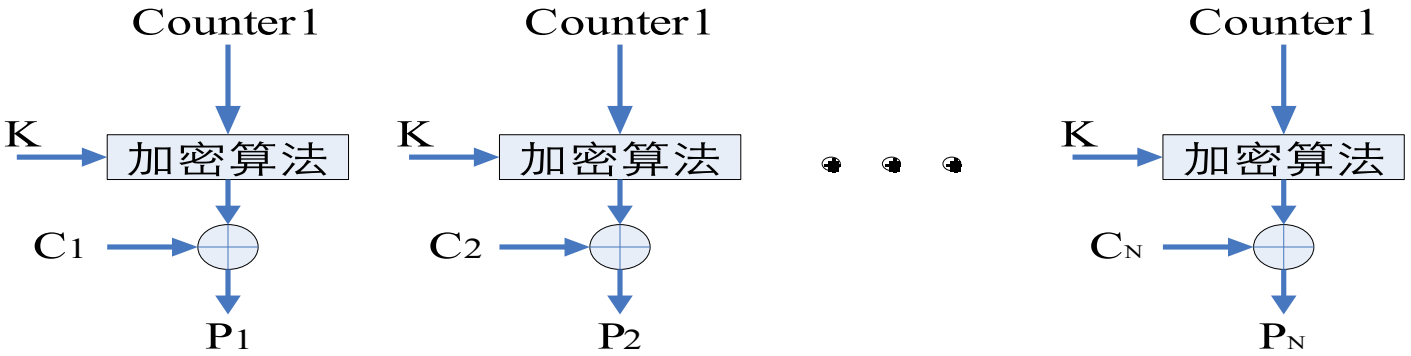
- OFB 的缺点是它比 CFB 模式更易受到对消息流的篡改攻击，比如在密文中取 1 比特的补，那么在恢复的明文中相应位置的比特也为原比特的补 . 因此使得敌手有可能通过对消息校验部分的篡改和对数据部分的篡改，而以纠错码不能检测的方式篡改密文 .

分组密码的运行模式

计数器模式 Counter(CTR)



加密过程



解密过程

分组密码的运行模式

- **Block Modes**
  - **ECB, CBC**
- **Stream Modes**
  - **CFB, OFB, CTR Mode**

主要知识点小结

- SMS4 加 / 解密算法
- SMS4 密钥编排算法
- 分组密码算法的运行模式

THE END !