现代密码学

第二十五讲 分组密码的工作模式2

信息与软件工程学院

第二十五讲 分组密码的工作模式

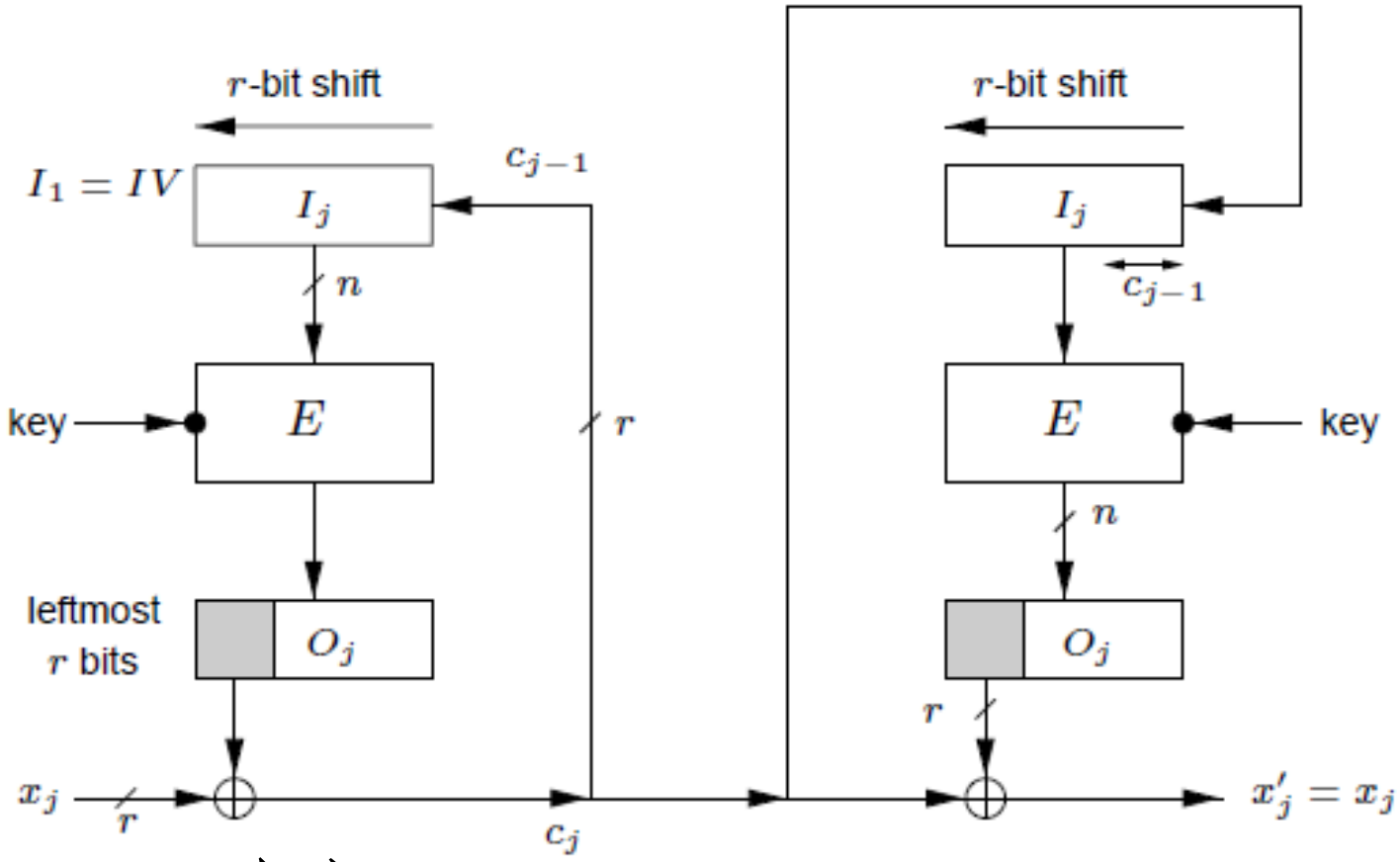
- 密码反馈(CFB)模式
- 输出反馈(OFB)模式
- 计数器模式

密码反馈CFB（Cipher Feedback）模式

- 若待加密消息需按字符、字节或比特处理时，可采用**CFB**模式。并称待加密消息按 ***r*** 比特处理的**CFB**模式为 ***r*** 比特CFB模式。
- 适用范围:
  - 适用于每次处理***r***比特明文块的特定需求的加密情形,能灵活适应数据各格式的需要
  - 例如,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为单位进行加密

CFB的加密解密

- 若记$IV=c_{-l+1}\ldots c_{-1}\,c_0$，$|c_i|=r$，则加密过程可表示为：$c_i = x_i \oplus left_r(E_k(c_{i-l}\cdots c_{i-2}c_{i-1}))$



CFB模式的特点

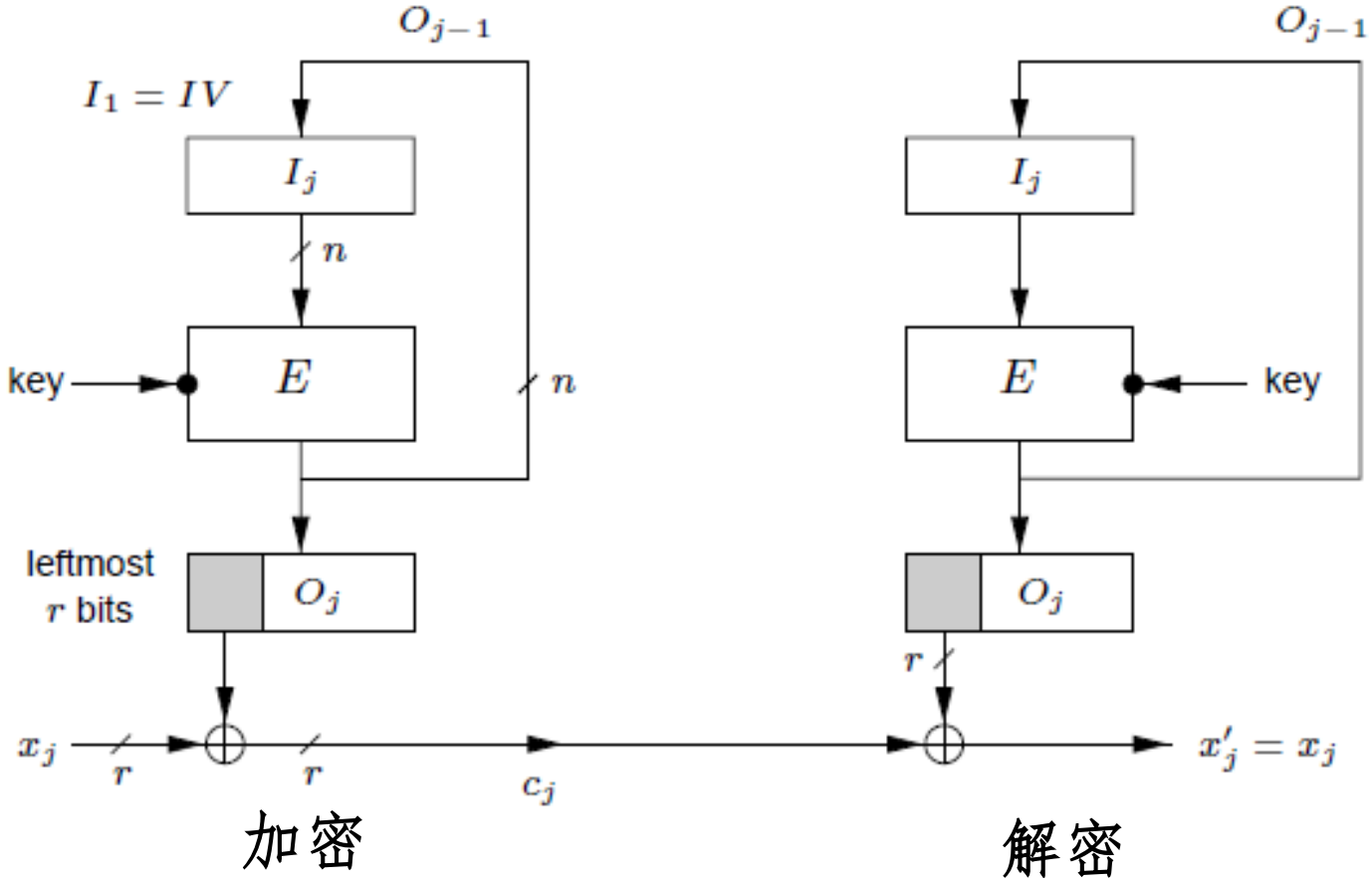
- 相同明文：和按**CBC**模式加密一样，改变***IV***同样会导致相同的明文输入得到不同的加密输出。***IV***无需保密（虽在某些应用中**IV**须是不可预测的）。
- 链接依赖性：类似**CBC**加密，链接机制致使密文组依赖于当前明文组和其前面的明文组；因此，重排密文组会影响解密。
- 错误的传播：一个或多个比特错误出现在任一个**r**比特的密文组中会影响这个组和后继$\lceil n/r \rceil$个密文组的解密。
- 错误恢复：**CFB**和**CBC**相似，也是自同步的，但它需有$\lceil n/r \rceil$个密文组才能还原

第二十五讲 分组密码的工作模式

- 密码反馈(CFB)模式
- 输出反馈(OFB)模式
- 计数器模式

输出反馈OFB(Output Feedback)模式

- **OFB模式在结构上类似于CFB模式，但反馈的内容是DES的输出而不是密文！**



OFB工作模式的特点

- 相同明文：和**CBC**及**CFB**一样，改变***IV***同样会导致相同的明文输入得到不同的加密输出。
- 链接依赖性：密钥流是独立于明文的。
- 错误传播：有一个或多个比特错误的任一密文字符仅会影响该字符的解密， 密文字符的某比特位置出错将致使还原明文的相应位置也出错。
- 错误恢复：**OFB**模式能从密文比特错误中得以恢复，但在丢失密文比特后就无法实现自同步了，这是因为丢失密文比特会破坏密钥流的编排。

四类工作模式比较和选用

（1）ECB模式简单、高速，但最弱，易受重放和替换攻击，一般用于加密长度小于等于分组长度的消息。

（2）CBC，CFB，OFB模式的选用取决于实际的特殊需求。

① 明文不易丢信号，对明文的格式没有特殊要求的环境可选用CBC模式。需要完整性认证功能时也可选用该模式。

② 容易丢信号的环境，或对明文格式有特殊要求的环境，可选用CFB模式。

③ 不易丢信号，但信号特别容易错，且明文冗余特别多，可选用OFB模式。

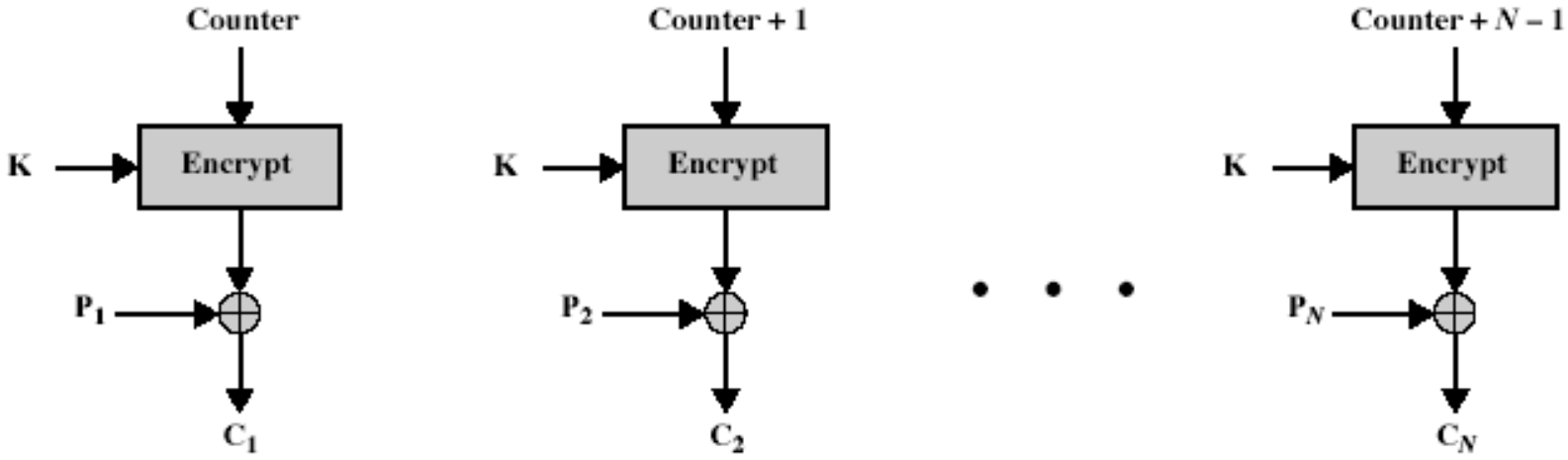
第二十五讲 分组密码的工作模式

- 密码反馈(CFB)模式
- 输出反馈(OFB)模式
- 计数器模式

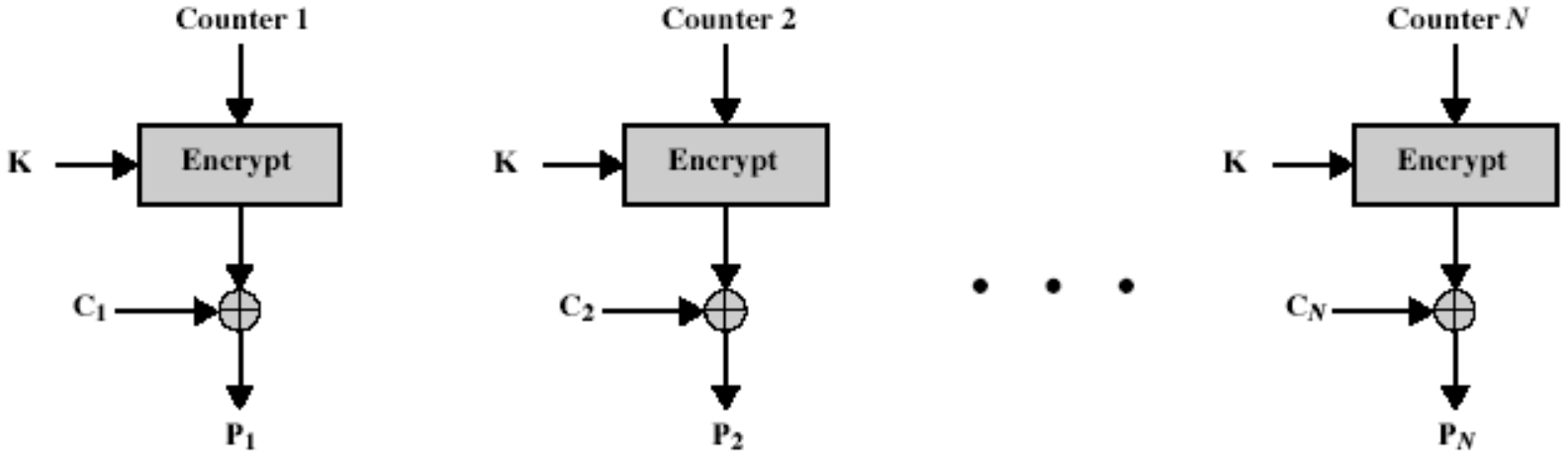
计数器模式

- 利用固定密钥**k**对自然数序列**1,2,3,…,n, …**加密，将得到的密文分组序列看作密钥流序列，按加法密码的方式与明文分组逐位异或的一种方式
- 利用这种方式可以产生伪随机数序列,其伪随机特性远比计算机产生的随机数的性质好

计数器模式的结构



(a) Encryption



(b) Decryption

CTR的优点

- 效率
  - 可并行加密
  - 预处理
  - 吞吐量仅受可使用并行数量的限制
- 加密数据块的随机访问
- 可证明安全
- 简单性（只要求实现加密算法）

感 谢 聆 听!

xynie@uestc.edu.cn