分组密码的工作模式

Modes of Operation for Block Ciphers

可厉害的土豆

01 电码本模式（Electronic Codebook，ECB）

02 密文分组链接模式（Cipher Block Chaining，CBC）

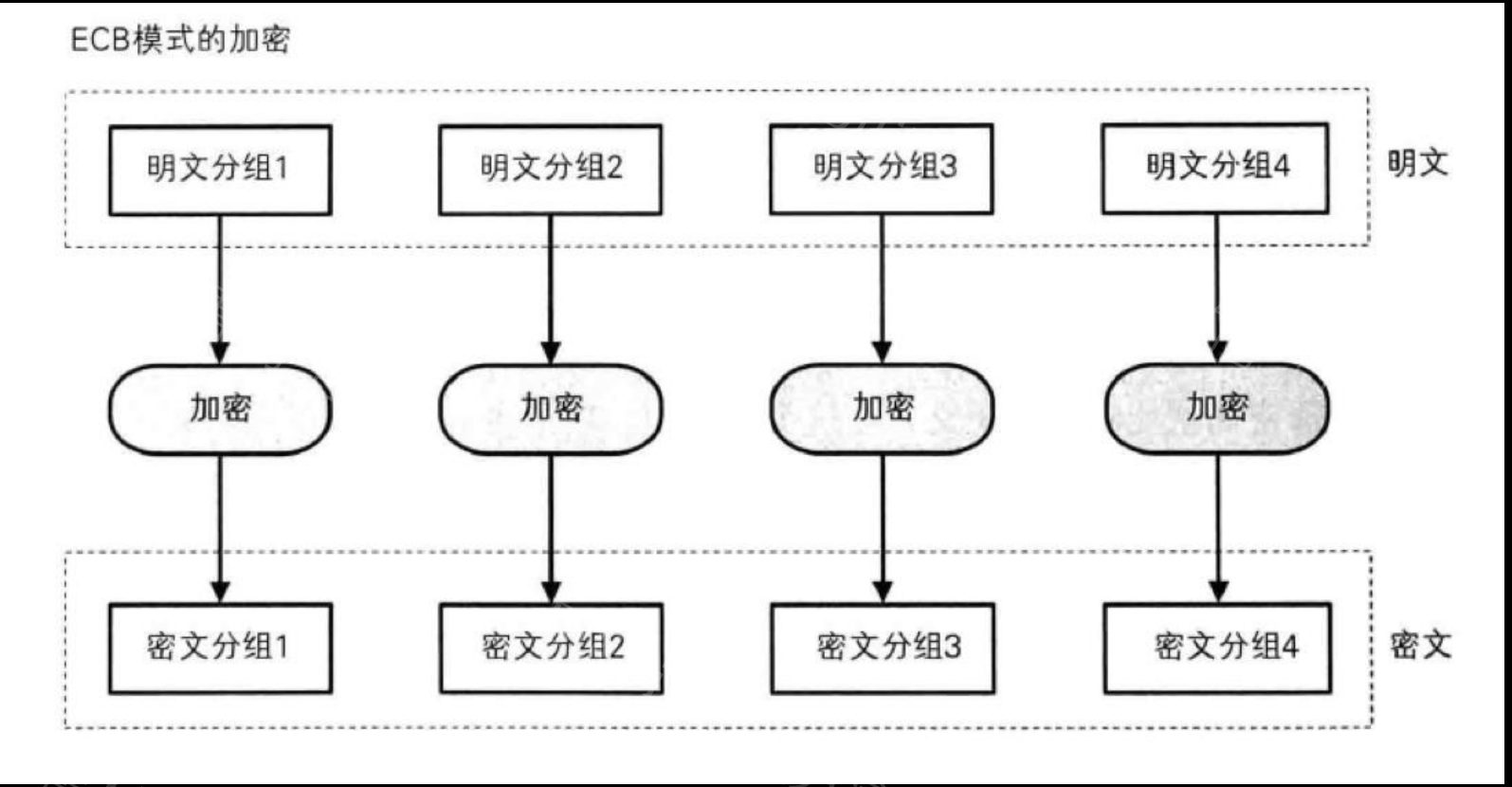
03 密文反馈模式（Cipher Feedback，CFB）

04 输出反馈模式（Output Feedback，OFB）

05 计数器模式（Counter，CTR）

01 电码本模式(ECB)
Electronic Codebook

- 用**相同的密钥**分别对明文分组**单独加密**。



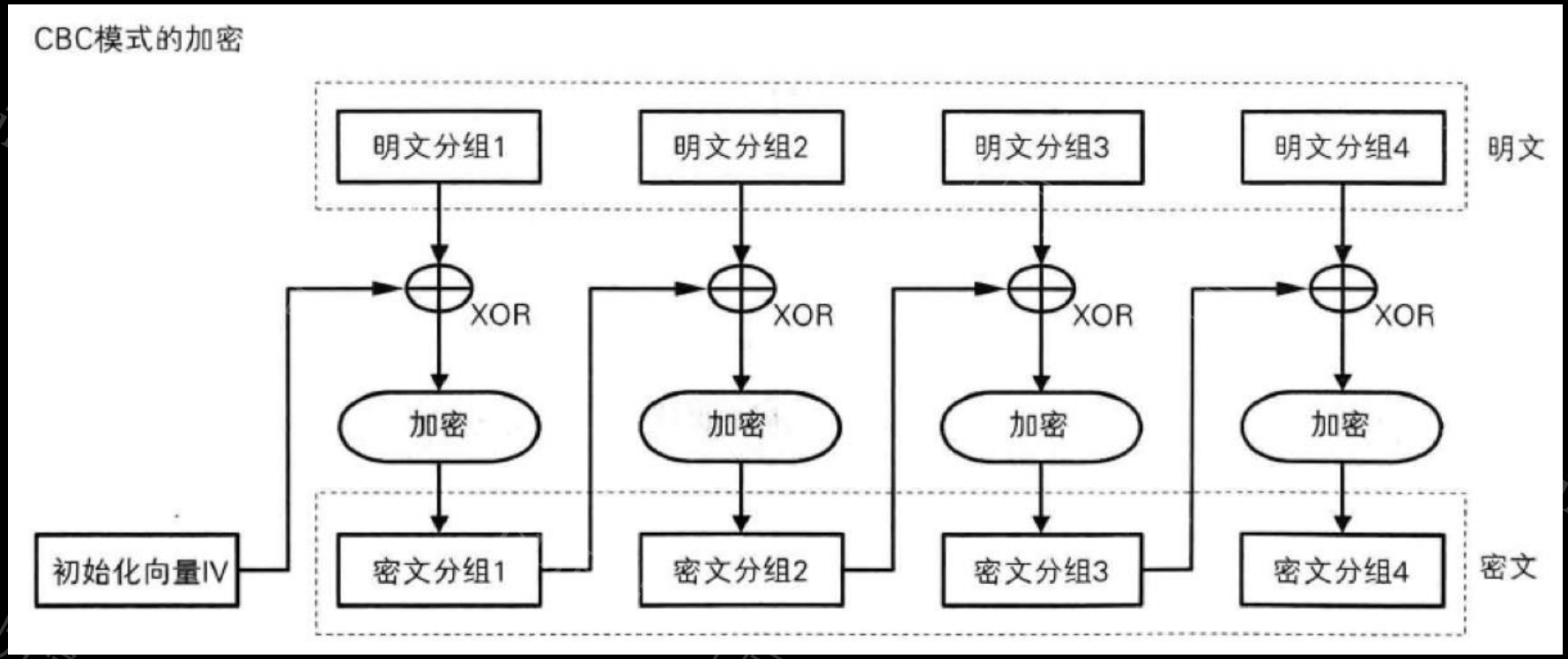
01 电码本模式(ECB)
Electronic Codebook

- 优点：每个数据块独立加密，可并行加密，实现简单
- 缺点：相同明文会产生相同密文，不具备数据完整保护性

适用于短消息的加密传输（如一个加密密钥）

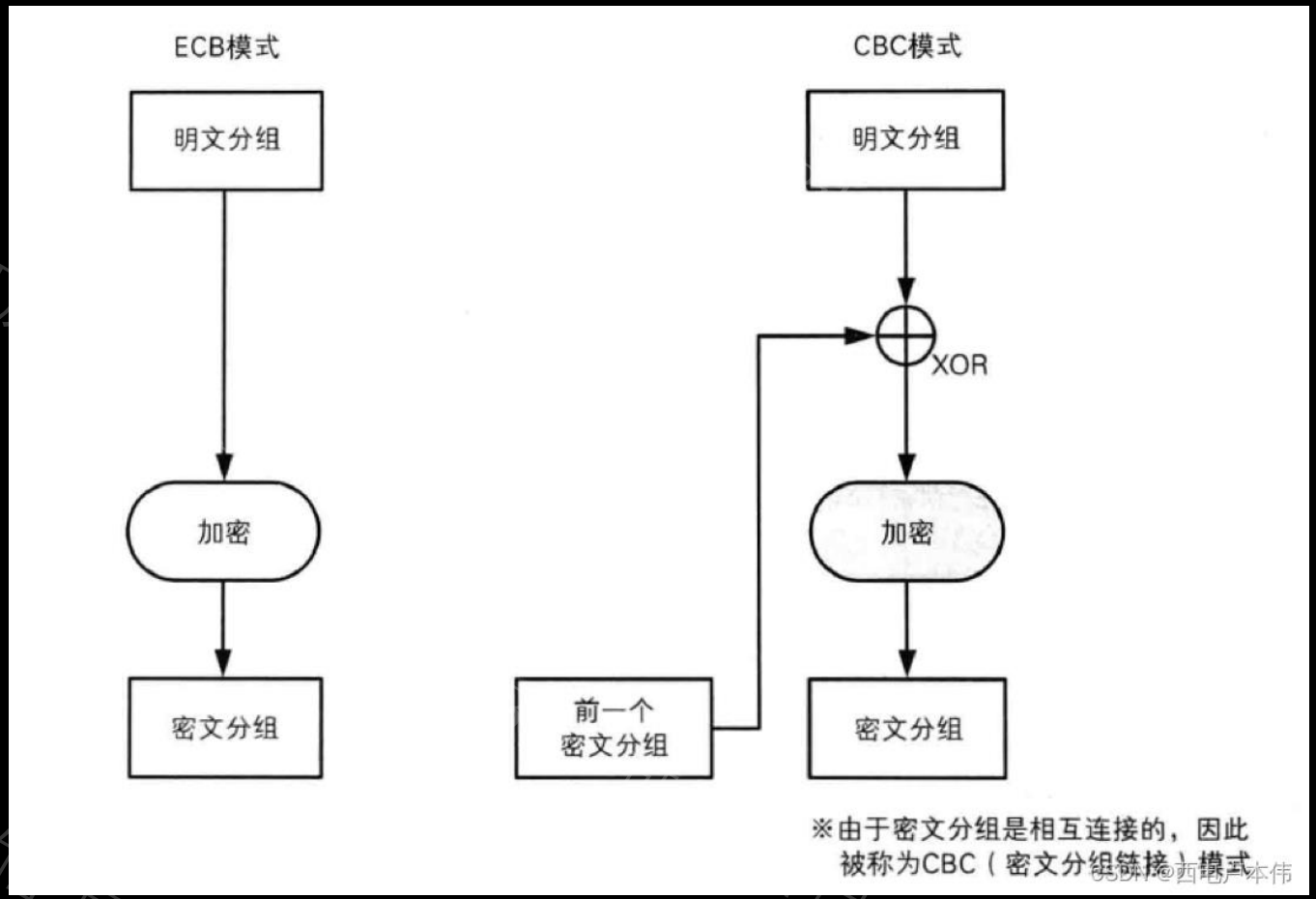
02 密文分组链接模式(CBC)
Cipher Block Chaining

- 将前一个密文块与当前明文块进行异或运算后再加密
- 初始向量 (IV) 用于第一个块的加密。



02 密文分组链接模式(CBC)
Cipher Block Chaining

- 加密算法的**输入**是**上一个密文分组**和**下一个明文分组**的**异或**。



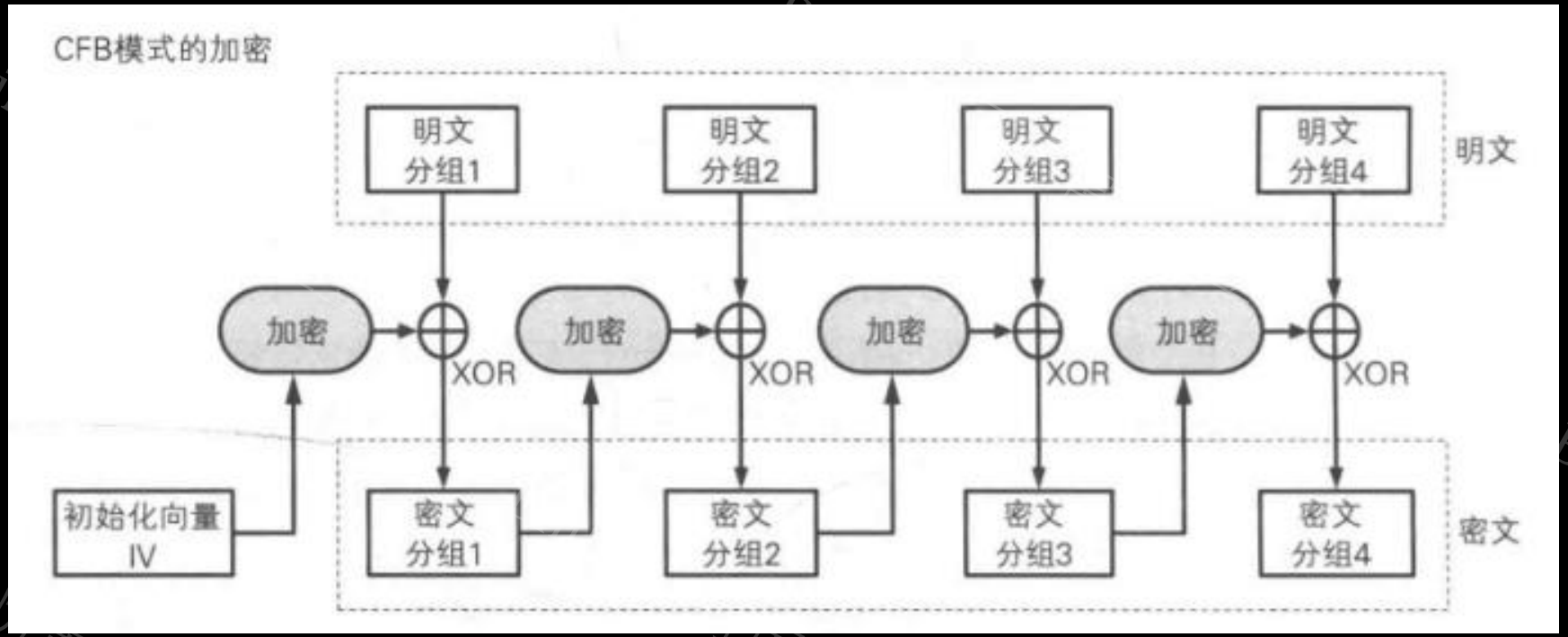
02 密文分组链接模式(CBC)
Cipher Block Chaining

- 优点：每个密文块的加密**依赖**前一个密文块，具备数据完整性保护
- 缺点：错误**传播**、不适合**并行**处理、

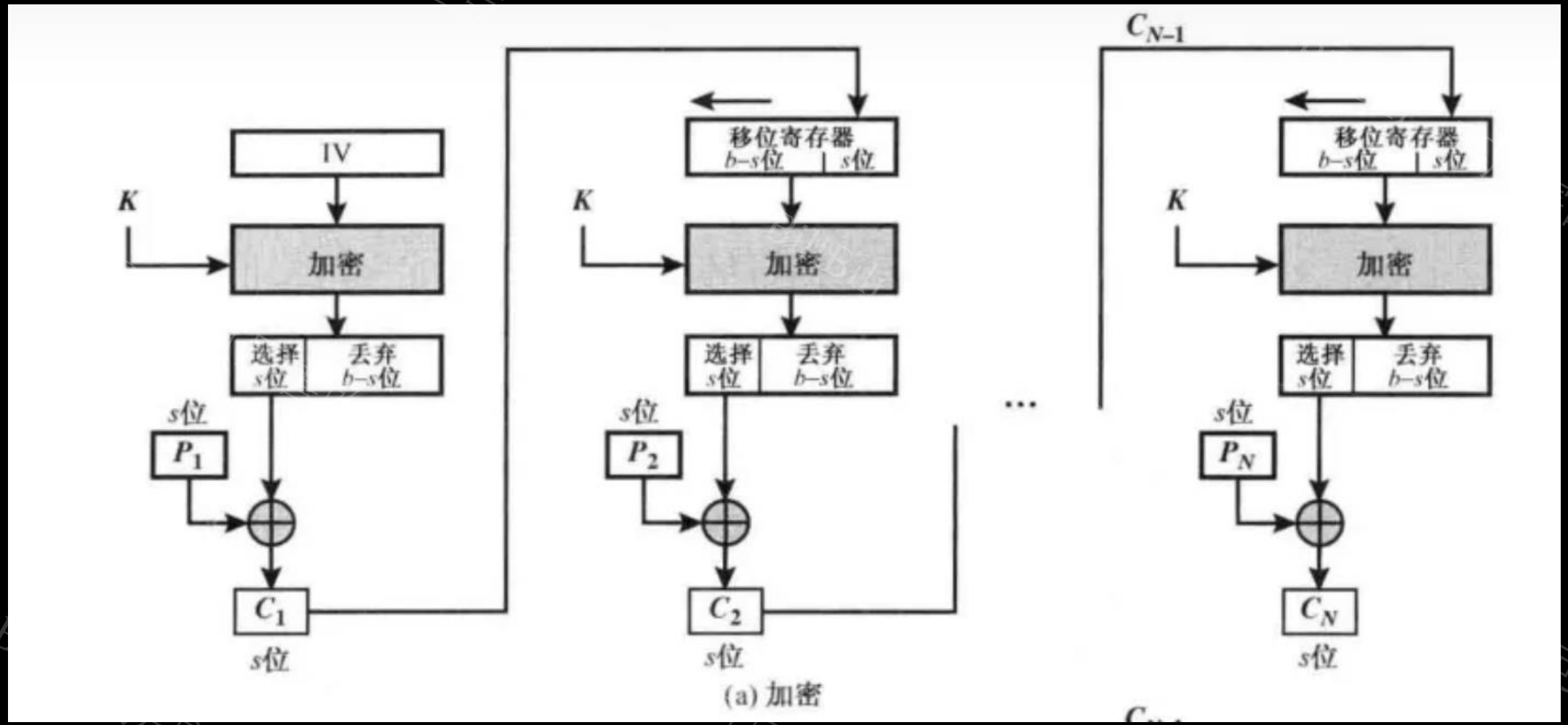
适用于常规**文件**加密、**非实时**加密等场景

03 密文反馈模式(CFB)
Cipher Feedback

- 将**前一个密文块**作为**输入**进行加密，生成一个**密钥流**，再与**当前明文块**进行**异或**运算得到密文块。



03 密文反馈模式(CFB)
Cipher Feedback



(a) 加密

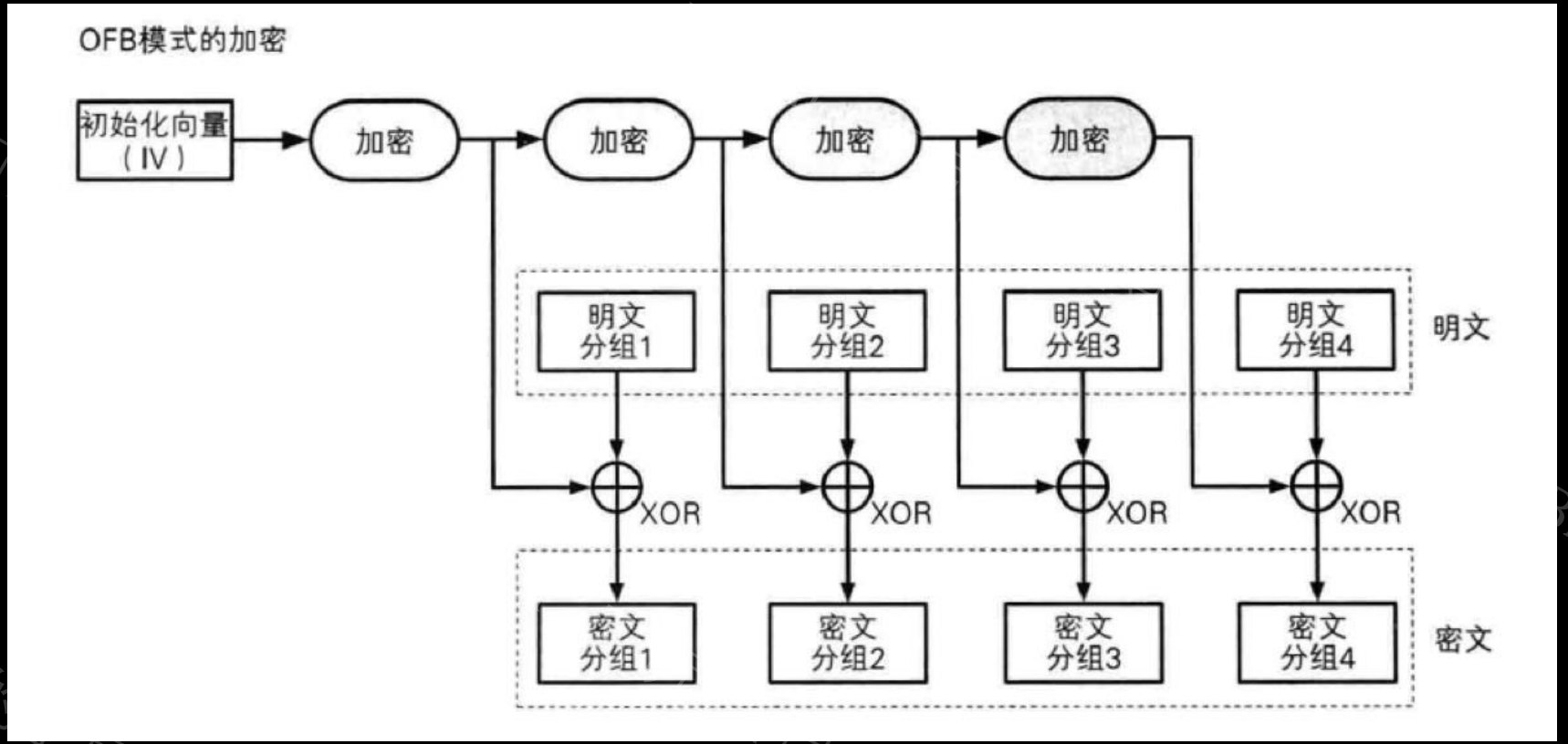
03 密文反馈模式(CFB)
Cipher Feedback

- **优点**
  - 可变长度的加密操作
  - 实时性
  - 可以部分解密数据
- **缺点：**
  - 密文分组的错误传播敏感
  - 不适合并行处理的场景
  - 需要保证初始向量的唯一性和完整性

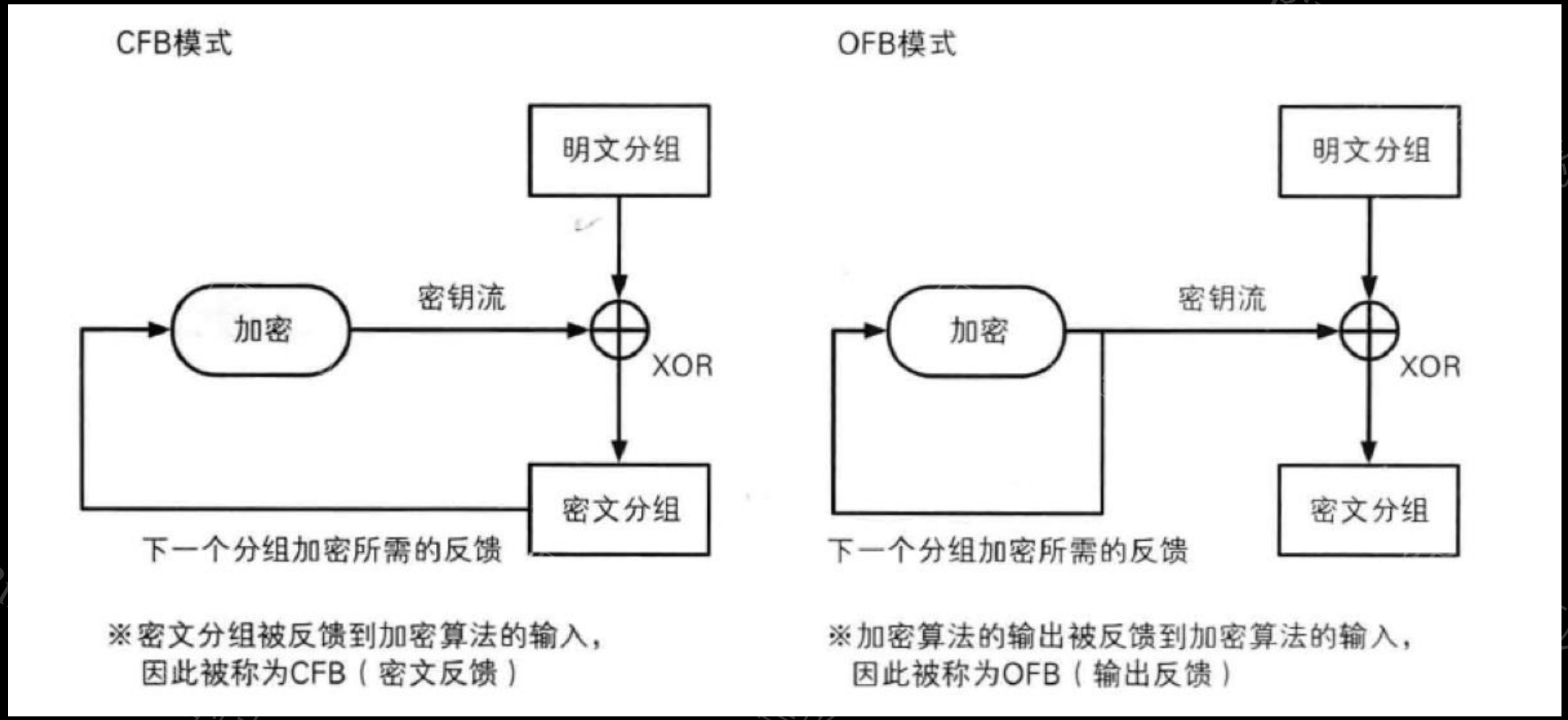
适用于流加密和对特定部分数据进行随机访问的场景

04 输出反馈模式（OFB）
Output Feedback

- 将**前一个加密算法的输出**作为**输入**进行**加密**，生成一个**密钥流**，再与**当前明文块**进行**异或**运算得到密文块。



04 输出反馈模式（OFB）
Output Feedback



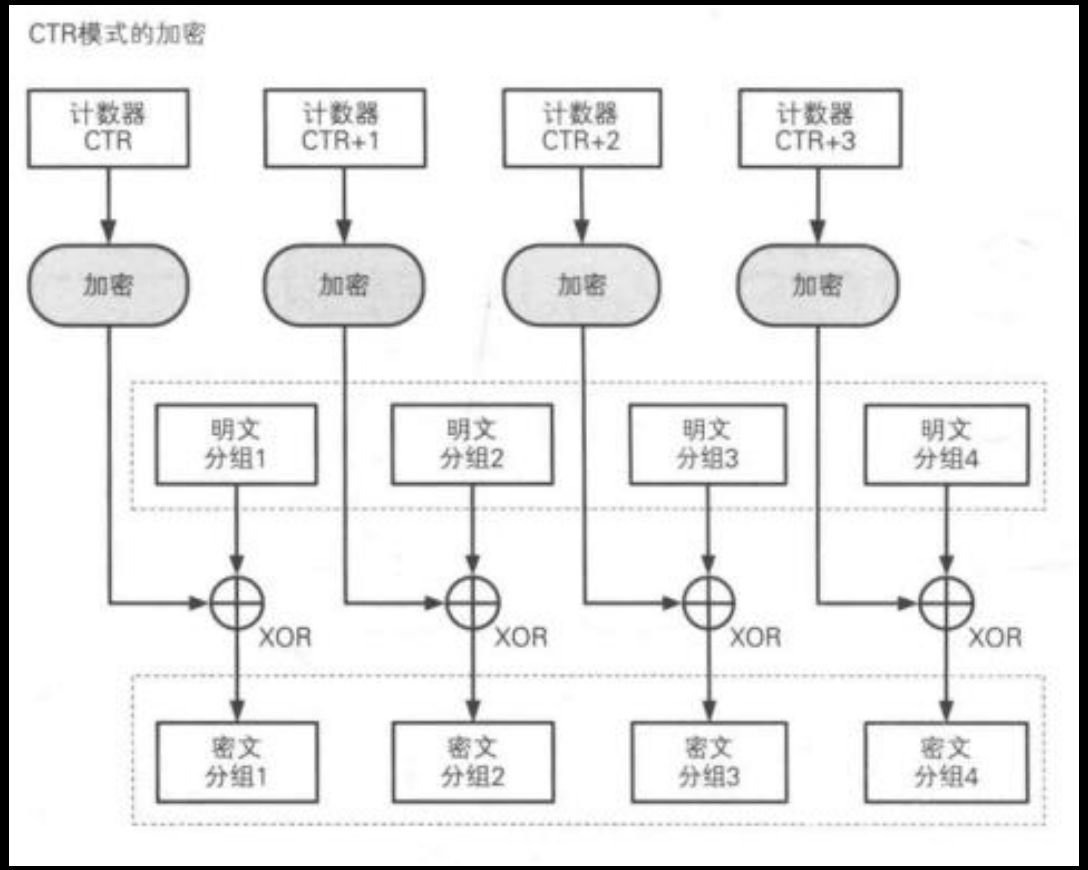
04 输出反馈模式（OFB）
Output Feedback

- **优点：**
  - 可变长度的加密操作
  - 实时性
  - 对密文分组的错误不敏感
- **缺点：**
  - 传输错误不可恢复
  - 无法提供数据完整性保护
  - 不支持并行加密

适用于实时数据流加密和随机访问的场景

05 计数器模式（CTR）
Counter

- 每一个明文分组都与一个**经过加密**的**计数器异或**。对每个后续的分组，计数器增1。



05 计数器模式（CTR）
Counter

- **优点：**
  - 并行处理
  - 随机访问
  - 不受错误传播影响
- **缺点：**
  - 计数器必须唯一
  - 密钥流和明文相关性较弱

适用于并行加密、随机访问和实时加密的场景

工作模式	描述	优点	缺点	典型应用
电码本模式（Electronic Codebook，ECB）	用相同的密钥分别对明文分组单独加密	简单直观的加密模式； 可以进行并行加密操作； 可以随机访问任意块	相同的明文块会生成相同的密文块； 缺乏混淆和扩散	单个数据的安全传输
密文分组链接模式（Cipher Block Chaining，CBC）	加密算法的输入是上一个密文分组和下一个明文分组的异或	密文之间的依赖性增加了安全性； 可处理任意长度的数据； 可抵抗明文和密文的修改	不适合并行处理； 需要处理初始向量； 算法之间可能存在差异	面向分组的通用传输； 认证
密文反馈模式（Cipher Feedback，CFB）	一次处理输入的s位，上一个密文分组作为加密算法的输入，产生的伪随机数输出与明文异或后作为下一个单元的密文	可变长度的加密操作; 实时性; 可以部分解密数据	错误传播敏感； 不适合并行处理； 保证初始向量的唯一性和完整性	面向数据流的通用传输； 认证
输出反馈模式（Output Feedback，OFB）	与CFB类似，只是加密算法的输入是上一次加密的输出，并且使用整个分组	可变长度的加密操作; 实时性; 对密文分组的错误不敏感	传输错误不可恢复； 无法提供数据完整性保护； 不支持并行加密	噪声信道上的数据流传输（如卫星通信）
计数器模式（Counter，CTR）	每个明文分组都与一个经过加密的计数器异或。 对每个后续的分组，计数器增1	并行处理; 随机访问; 不受错误传播影响	计数器必须唯一; 密钥流和明文相关性较弱	面向分组的通用传输； 用于高速需求

参考资料

[1] Stallings, W. 密码编码学与网络安全——原理与实践（第八版）[M]. 北京: 电子工业出版社, 2015.

[2] 知乎用户W2GxGb. （七）分组密码的五大工作模式[EB/OL]. 2021-04-17.2023-05-31. https://zhuanlan.zhihu.com/p/364772865.

[3] 西电卢本伟. 分组密码的五种模式[EB/OL].2022-04-20.2023-05.31. https://blog.csdn.net/lbwnbnbnbnbnbnbn/article/details/124302153.

感谢观看

祝你

每顿吃饱

每晚睡好

身体健康

学业有成

工作顺利

——可厉害的土豆