密 码 学

第六讲　分组密码的应用技术

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

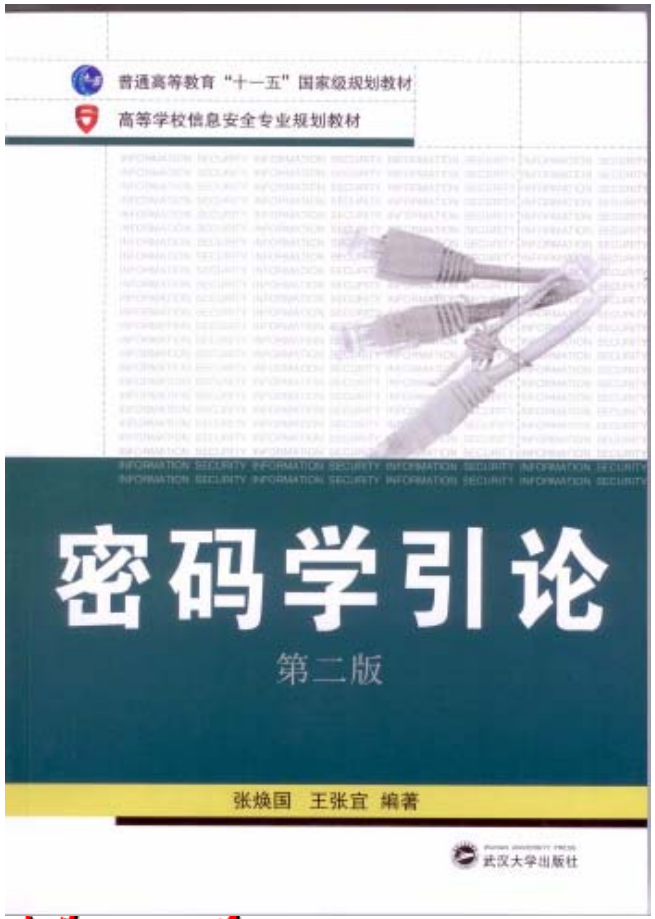
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

内容简介

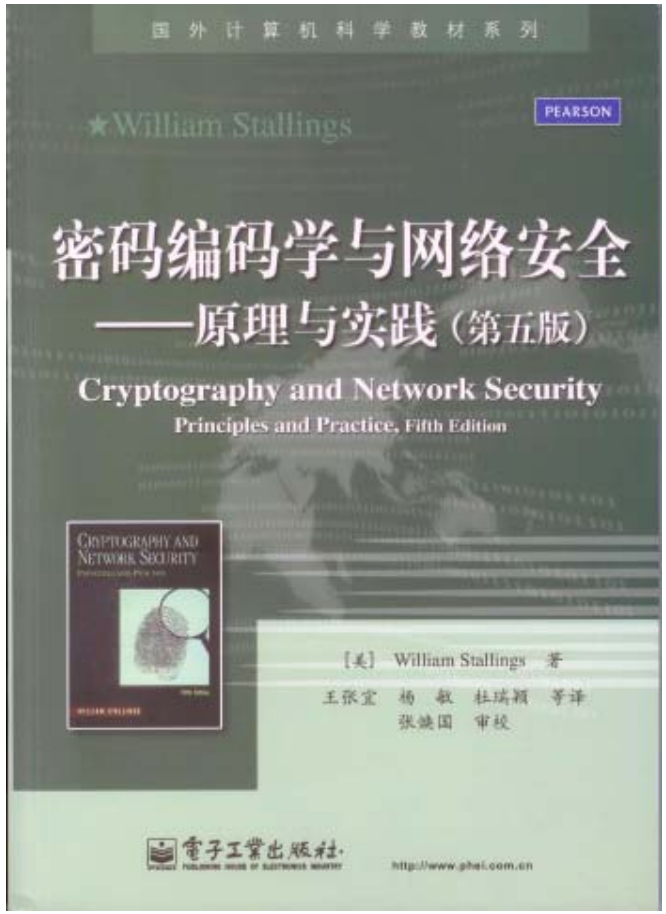
第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

教材与主要参考书

教材



参考书



一、计算机数据的特殊性

1、存在明显的数据模式

- 许多数据都具有某种固有的模式。这主要是由数据冗余和数据结构引起的。
- 各种计算机语言的语句和指令都十分有限，因而在程序中便表现为少量的语句和指令的大量重复。
- 各种语言程序往往具有某种固定格式。
- 数据库的记录也往往具有某种固定结构。
- 操作系统和网络协议也有同样的问题。

一、计算机数据的特殊性

1、存在明显的数据模式：

- 根据明文相同、密钥相同，则密文相同的道理，这些固有的数据模式将在密文中表现出来。
- 掩盖明文数据模式的方法：
  - ■随机掩盖技术：
    - ◆使用一个随机序列掩盖明文数据，从而消除明文中的数据模式。
    - ◆缺点：通信双方必须共享该随机序列，带来许多麻烦。
  - ■链接技术
    - ◆使前后明文块及密文块彼此关联起来，从而消除明文中的数据模式
- 如果不能掩盖数据模式，既使采用安全的密码算法也是徒劳的。

一、计算机数据的特殊性

2、分组密码用于数据加密存在短快问题：

- 设明文M长度为n_1，分组密码的明文分组长度为n_2，如果n_1不是n_2的整数倍，则最后一块要加密的数据块的长度必然小于明文分组长度n_2，称此数据块为短块。
- 分组密码不能直接加密短块数据，必须采取特殊的方法处理短块。

二、分组密码的工作模式

1977年DES颁布，1981年美国政府针对DES的应用，制定了DES的四种基本工作模式：

- 电码本模式（ECB）
- 密文反馈链接模式（CBC）
- 密码反馈模式（CFB）
- 输出反馈模式（OFB）

二、分组密码的工作模式

2000年美国在征集AES的同时又公开征集AES的工作模式，共征集到 15个候选工作模式。

- 经过评审选定了几个新的工作模式。
- 这些新的工作模式将为AES的应用作出贡献。

二、分组密码的工作模式

1、电码本模式（ECB）

- 直接利用分组密码对明文的各分组进行加密。
- 设　明文　$M=(M_1, M_2, \ldots, M_n)$，
  密钥为K，
  密文　$C=(C_1, C_2, \ldots, C_n)$，
  其中　$C_i=E(M_i, K)$，$i=1,2,\ldots,n$
- 电码本方式是分组密码的基本工作模式。
- 缺点：
  - 可能出现短块，这时需要特殊处理。
  - 密钥K固定，如果$M_i=M_j$，则$C_i=C_j$，从而暴露明文的数据模式。
- 应用：适合加密密钥等短数据

二、分组密码的工作模式

2、密文反馈链接模式（CBC）

①明密文链接方式（Plaintext and Ciphertext Block Chaining）

● 设　明文 $M=(M_1, M_2, \ldots, M_n)$，

密钥为K,

密文 $C=(C_1, C_2, \ldots, C_n)$,

其中

$$C_i=\begin{cases} E(M_i \oplus Z, K), & i=1 \\ E(M_i \oplus M_{i-1} \oplus C_{i-1}, K), & i=2,\ldots,n \end{cases}$$

Z为初始化向量。

二、分组密码的工作模式

2、密文反馈链接模式（CBC）

①明密文链接方式

- 错误传播
  - ◆加密时，明文或密文发生错误引起对应密文及其后续密文发生错误
  - ◆解密时，密文或明文发生错误引起对应明文及其后续明文发生错误
  - ◆如果密码算法的输入数据错误只引起对应的几个输出数据错误，则成称为错误传播有界
  - ◆如果密码算法的输入数据错误引起对应的输出数据及其后续的输出数据全部错误，则称为错误传播无界

二、分组密码的工作模式

2、密文反馈链接模式（CBC）

①明密文链接方式

- 对于CBC模式，即使$M_i=M_j$，但因一般都有$M_{i-1}\oplus C_{i-1}\neq M_{j-1}\oplus C_{j-1}$，从而使$C_i\neq C_j$，从而掩盖了明文中的数据模式。
- 加密时错误传播无界，当M_i或C_i中发生一位错误时，自此后的密文全都发生错误。
- 解密时也是错误传播无界。

$$\begin{cases} M_i = E(C_i, K)\oplus Z, & i=1 \\ M_i = E(C_i, K)\oplus M_{i-1}\oplus C_{i-1}, & i=2,\ldots,n \end{cases}$$

Z为初始化向量。

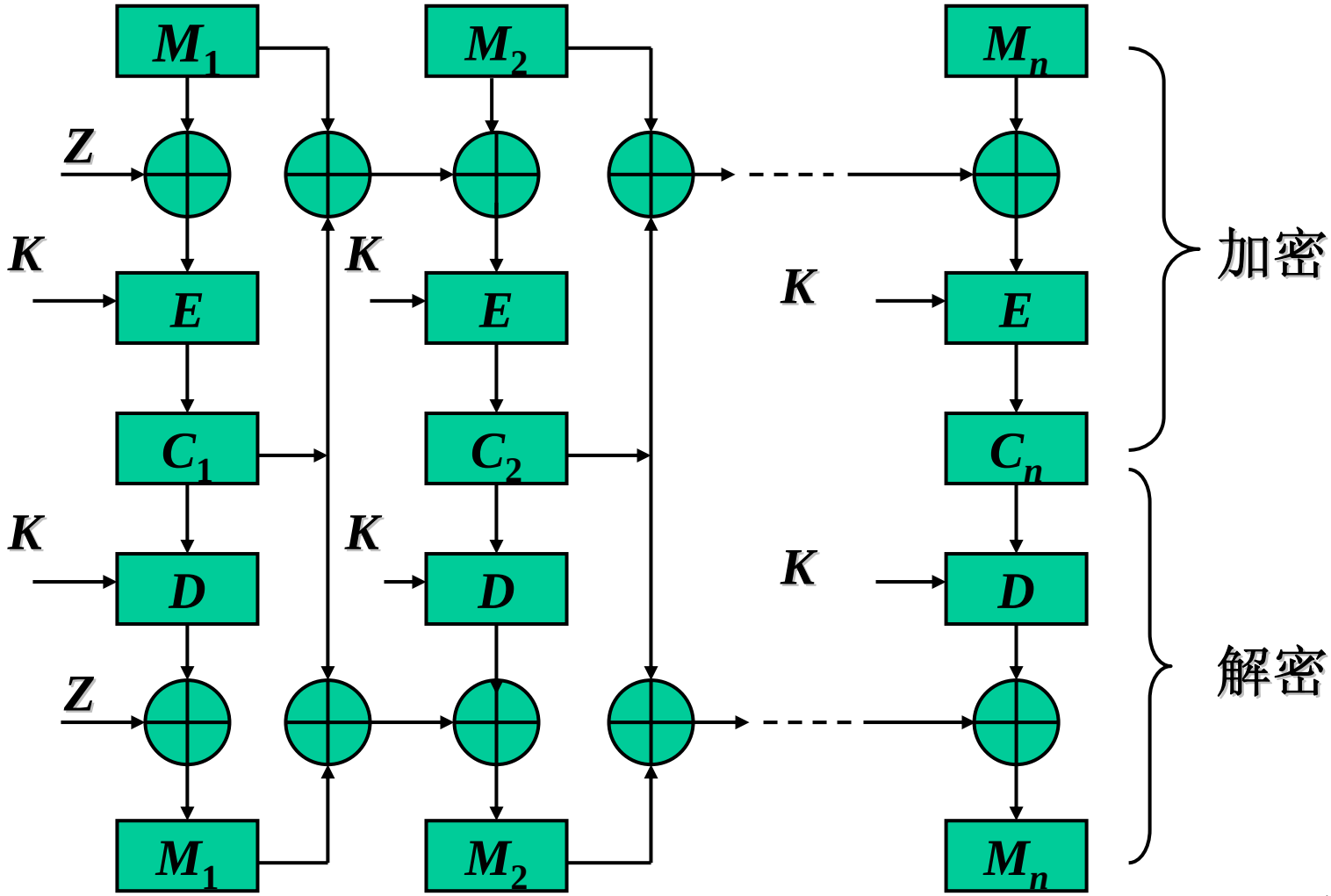
二、分组密码的工作模式

2、密文反馈链接模式（CBC）

①明密文链接方式

- 加密是在发送端进行的，加密时明文和密文发生错误的概率较小。
- 解密是在接收端进行的，解密时明文和密文发生错误的概率较小。
- 但是，密文是经过信道传输的，因此密文在信道中受干扰而发生错误的概率较大。
- 错误传播无界的缺点：当磁盘发生一点损坏时将导致整个密文文件无法解密。
- 错误传播无界的优点：可用于数据完整性、真实性认证。

二、分组密码的工作模式



二、分组密码的工作模式

2、密文反馈链接模式（CBC）

- 明密文链接方式具有加解密错误传播无界的特性，而磁盘文件加密和通信加密通常希望解密错误传播有界，这时可采用密文链接方式。

②密文链接方式（ Ciphertext Block Chaining）

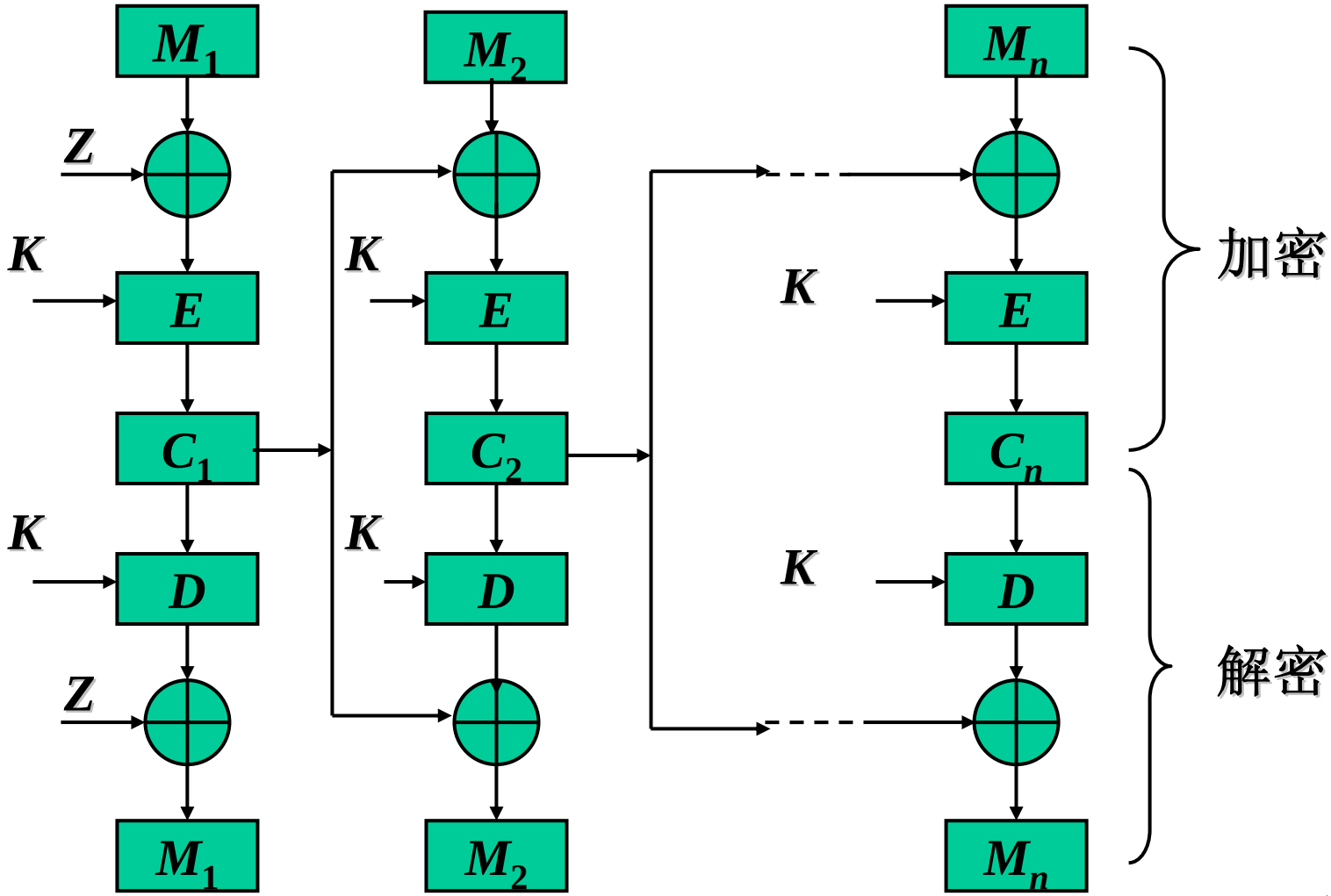
- 设　明文 $M=(M_1, M_2, \ldots, M_n)$，

  密钥为K,

  密文 $C=(C_1, C_2, \ldots, C_n)$,

其中 $$C_i=\begin{cases} E(M_i \oplus Z, K), & i=1 \\ E(M_i \oplus C_{i-1}, K), & i=2,\ldots,n \end{cases}$$

二、分组密码的工作模式



武漢大学

二、分组密码的工作模式

2、密文反馈链接模式（CBC）

②密文链接方式

- 加密：错误传播无界
  - M_i 或C_{i-1}错误，将影响C_i及其以后的密文全错。

- 解密时：错误传播有界

$$M_i=\begin{cases} D(C_i, K)\oplus Z, & i=1 \\ D(C_i, K)\oplus C_{i-1}, & i=2,\ldots,n \end{cases}$$

  - C_{i-1} 发生了错误，则只影响M_{i-1} 和M_i 发生错误，其余不错，因此错误传播有界。
  - 解密错误传播有界有利于提高密码处理的可用性。

二、分组密码的工作模式

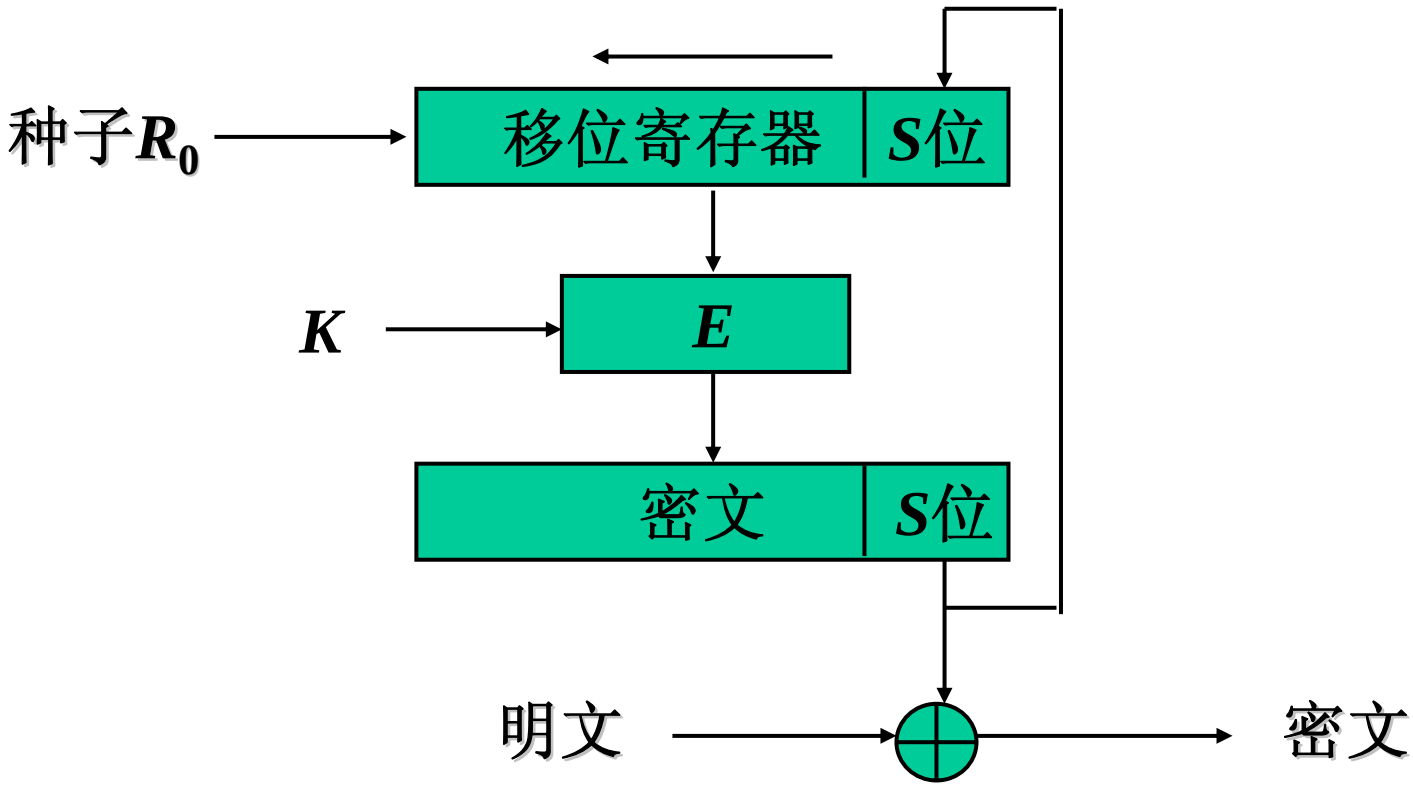
3、输出反馈模式 (OFB)

- 将一个分组密码转换为一个密钥序列产生器。从而可以实现用分组密码按流密码的方式进行加解密。

  - 采用一个移位寄存器，R_0是初始内容，称为种子。
  - E 是DES、AES、SMS4 等强密码，加密移位寄存器的内容，输出密文最右边的s（ $s \geq 1$）位作密钥，与明文摸2加加密。
  - 移位寄存器左移s位，密文最右边的s位 反馈到移位寄存器的右s位。E再加密，再输出密钥。
  - 如此继续，把分组密码转变成了序列密码。

二、分组密码的工作模式

3、输出反馈模式 (OFB)



二、分组密码的工作模式

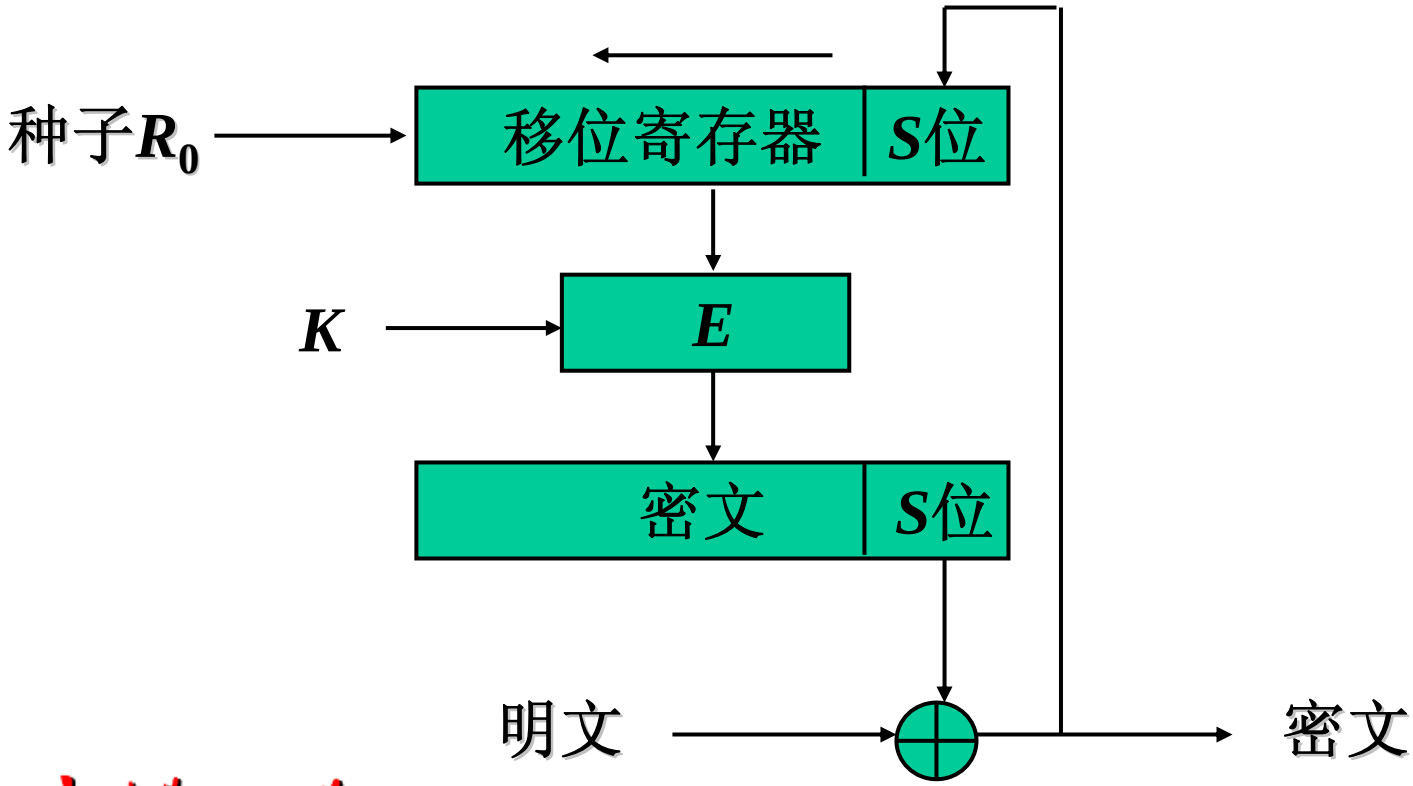
3、输出反馈模式 (OFB)

- 如果分组密码是安全的，则产生的密钥序列也是安全的。
- 加解密都没有错误传播。
- 适于加密冗余度较大的数据，如语音和图象数据。
- 为了提高速度可输出最右边的 8位。
- 因无错误传播，所以对密文的篡改难以检测。

二、分组密码的工作模式

4、密码反馈模式 CFB（Cipher Feedback）

- CFB模式也是用分组密码产生密钥序列。



二、分组密码的工作模式

4、密码反馈模式 (CFB)

- 与OFB的不同是，把密文反馈到移位寄存器。
- 加密时若明文错了一位，则影响相应的密文错，这一错误反馈到移位寄存器后将影响到后续的密钥序列错，导致后续的密文都错。
- 解密时若密文错了一位，不仅影响相应的明文错，而且密文的这一错误反馈到移位寄存器后将影响到后续的密钥序列错，导致后续的明文都错。
- 因错误传播无界，可用于检查发现对明密文的篡改。

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- 2000年美国学者John Black和Phllip Rogaway提出X CBC模式，作为CBC模式的扩展，推荐为AES的工作模式，被美国政府采纳作为标准。
- X CBC主要是解决了CBC要求明文数据的长度是码分组长度的整数倍的限制，可以处理任意长的数据。如果用分组密码是安全的，则密钥序列就是安全的。

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- 设明文$M=(M_1, M_2, \ldots, M_{n-1}, M_n)$，相应的密文$C=(C_1, C_2, \ldots, C_{n-1}, C_n)$，而$M_n$可能是短块。
- 使用3个密钥K_1，K_2，K_3进行加密。
- 使用填充函数$Pad(X)$对短块数据进行填充。

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- 填充函数*Pad*（*X*）定义如下：

$$\text{Pad}(X)=\begin{cases} X, & \text{当}X\text{不是短块;} \\ X10\ldots0, & \text{当}X\text{是短块。} \end{cases}$$

- 经填充函数 *Pad*（*X*）填充后的数据块一定是标准块。

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- 令$Z=0$，以Z作为初始化向量。加密过程如下：

$$C_i = \begin{cases} E(M_i \oplus Z, K_1), & i=1 \\ E(M_i \oplus C_{i-1}, K_1), & i=2,\ldots,n-1 \end{cases}$$

$$C_n = \begin{cases} E(M_n \oplus C_{n-1} \oplus K_2, K_1), & \text{当} M_n \text{不是短块；} \\ E(\mathrm{PAD}(M_n) \oplus C_{n-1} \oplus K_3, K_1), & \text{当} M_n \text{是短块。} \end{cases}$$

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- X CBC与CBC的区别：
  - CBC要求最后一个数据块是标准块，不是短块。
  - X CBC既允许最后一个数据块是标准块，也允许是短块。
  - 最后一个数据块的加密方法与 CBC不同。
  - 因为有填充，需要传输填充长度信息。

二、分组密码的工作模式

5、X CBC (Extended Cipher Block Chaining Encryption)模式

- X CBC模式的主要优点：
  - 可以处理任意长度的数据。
  - 适于计算产生检测数据完整性的消息认证码MAC。
- X CBC模式的主要缺点：
  - 有填充，不适合文件和数据库加密。
  - 使用3个密钥，需要传输填充长度，控制复杂。

二、分组密码的工作模式

6、CTR（Counter Mode Encryption）模式

- CTR模式是Diffie和Hellman于1979年提出的，在征集AES工作模式的活动中由California大学的Phillip Rogaway等人的推荐。
- 设T_1，T_2，…，T_{n-1}，T_n 是一给定的计数序列，M_1，M_2，…，M_{n-1}，M_n 是明文，其中M_1，M_2，…，M_{n-1}是标准块，M_n 的可能是标准块，也可能是短块。设M_n 的长度等于u，$u \leqslant$ 分组长度。

二、分组密码的工作模式

6、CTR（Counter Mode Encryption）模式

- CTR的工作模式的加密过程如下：

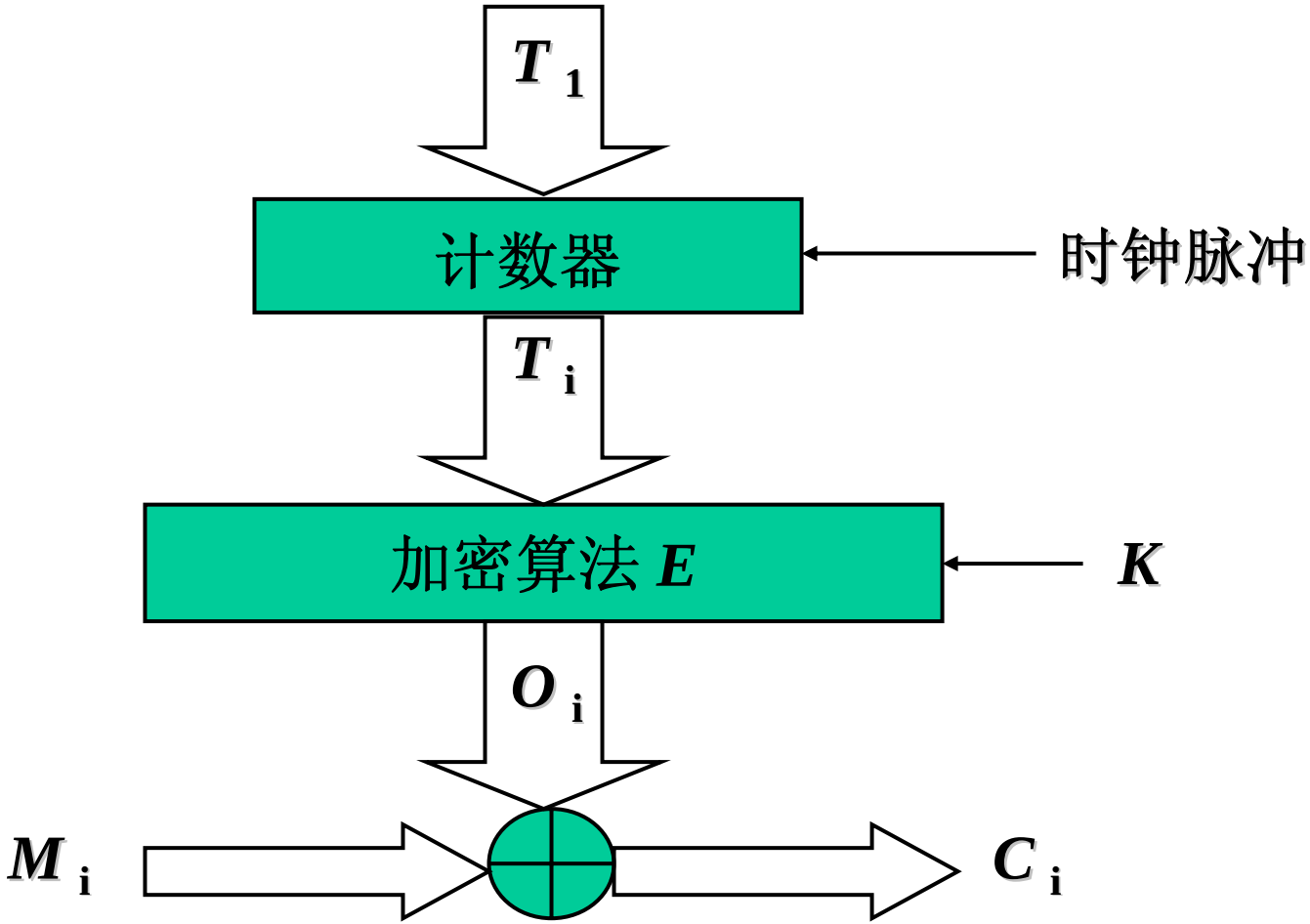
$$O_i = E(T_i, K),\ i=1,2,\ldots,n.$$

$$C_i = M_i \oplus O_i,\ i=1,2,\ldots,n-1.$$

$$C_n = M_n \oplus MSB_u(O_n).$$

其中$MSB_u(O_n)$表示O_n中的高u位。

二、分组密码的工作模式



二、分组密码的工作模式

6、CTR（Counter Mode Encryption）模式

- CTR的工作模式的解密过程如下：

$$O_i = E(T_i, K),\ i=1,2,\ldots,n.$$

$$M_i = C_i \oplus O_i,\ i=1,2,\ldots,n-1.$$

$$M_n = C_n \oplus MSB_u(O_n).$$

其中$MSB_u(O_n)$表示O_n中的高u位。

二、分组密码的工作模式

6、CTR（Counter Mode Encryption）模式

- CTR的工作模式的优点：
  - CTR模式的优点是安全、高效、可并行、适合任意长度的数据；
  - O_i的计算可预处理高速进行；
  - 由于采用了摸2加实现加密，是对合运算，解密运算与加密运算相同。
  - 适合随机存储数据的解密。
- CTR模式的缺点：
  - 没有错误传播，因此不易确保数据完整性。

三、短块加密

- 分组密码一次只能对一个固定长度的明文（密文）块进行加（解）密。
- 称长度小于分组长度的数据块为短块。
- 必须采用合适的技术解决短块加密问题。
- 短块处理技术：
  - 填充技术
  - 密文挪用技术
  - 序列加密

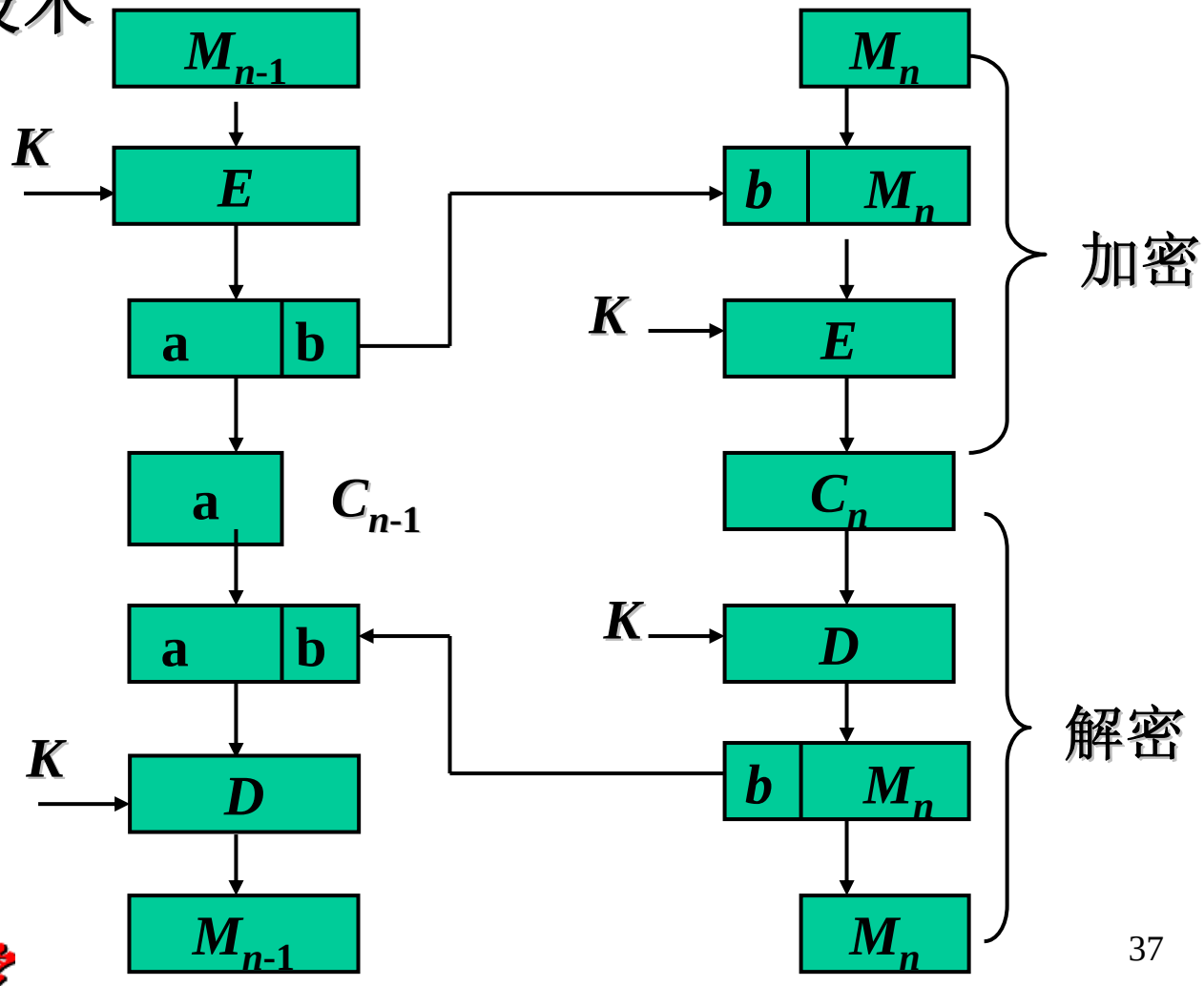
三、短块加密

1、填充技术

- 用无用的数据填充短块，使之成为标准块。
- 为了确保加密强度，填充数据应是随机的。
- 但是收信者如何知道哪些数字是填充的呢？这就需要增加指示信息，通常用最后8位作为填充指示符。
- 填充可能引起存储器溢出，因而可能不适于文件和数据库加密。

三、短块加密

2、密文挪用技术



三、短块加密

- 密文挪用法也需要指示挪用位数的指示符，否则收信者不知道挪用了多少位，从而不能正确解密。

- 密文挪用加密短块的优点是不引起数据扩展。

- 缺点是解密时要先解密C_n 、还原挪用后再解密C_{n-1}，从而使控制复杂。

三、短块加密

3、序列加密

- 对于最后一块短块数据，直接使用密钥K与短块数据模2相加。
- 序列加密方法的优点是简单。
- 但是如果短块太短，则加密强度不高。

作 业 题

1、p115第32题。

自 选 实 践 题

1、 p114第8题，26题，29题。

谢　谢！