现代密码学

第七讲 流密码的基本概念

信息与软件工程学院

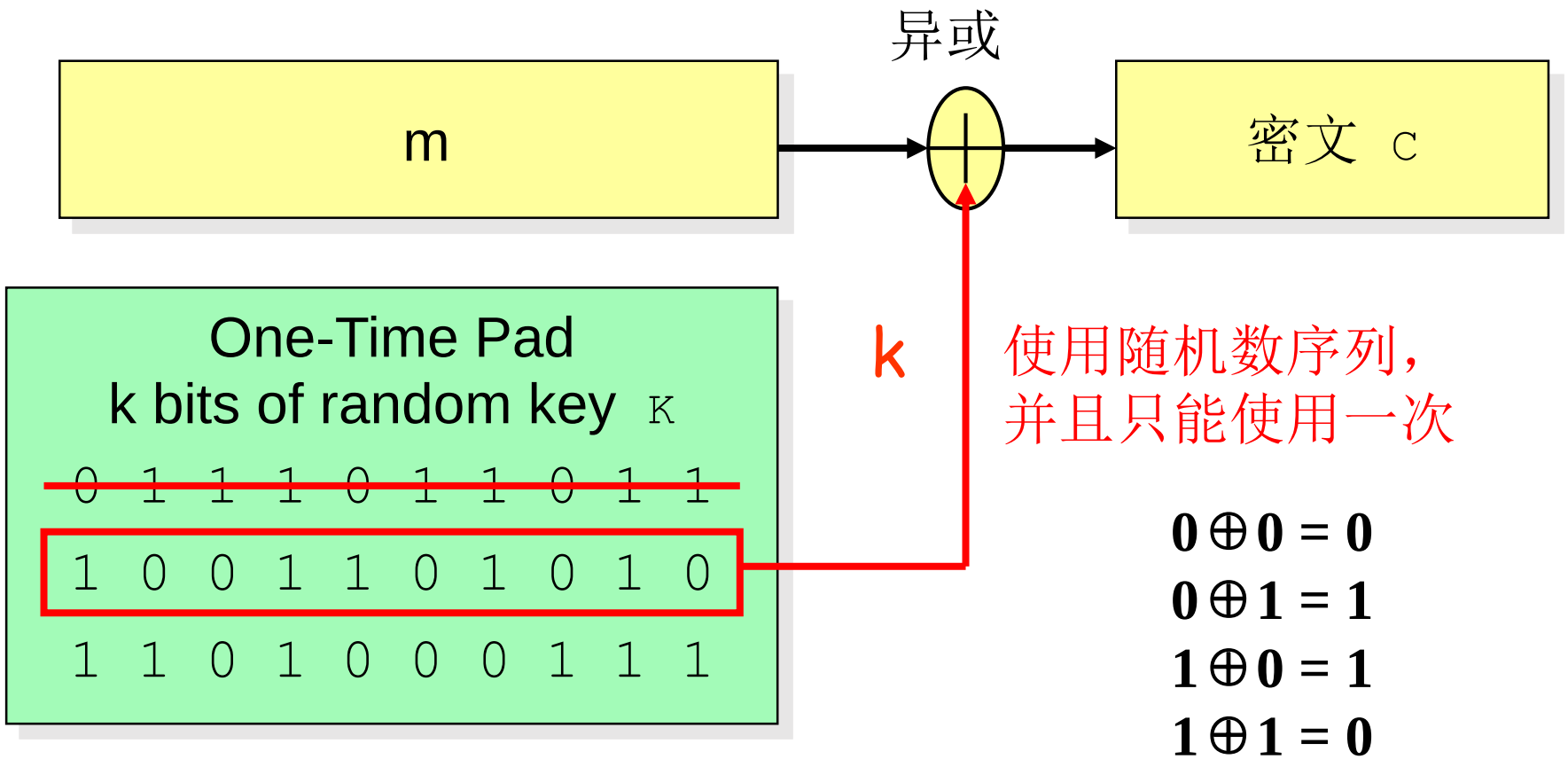
第七讲 流密码的基本概念

- 一次一密
- 流密码的定义
- 同步流密码

一次一密密码

- 一种理想的加密方案，叫做一次一密密码（**one-time pad**），由**Major Joseph Mauborgne**和**AT&T**公司的**Gilbert Vernam1917**年发明的
- 明文：$x=x_0\,x_1\,x_2\cdots$
- 密钥：$k=k_0k_1k_2\ \cdots$
- 密文：$y=y_0y_1y_2\ \cdots$
- 加密函数：$y_i=x_i+k_i(\mathrm{mod}26)$
- 解密函数：$x_i=y_i-k_i(\mathrm{mod}26)$
- 注：密钥为随机产生的，而且只使用一次

一次一密密码


异或
m
密文 C
One-Time Pad
k bits of random key K
0 1 1 1 0 1 1 0 1 1
1 0 0 1 1 0 1 0 1 0
1 1 0 1 0 0 0 1 1 1
k
使用随机数序列，
并且只能使用一次
0⊕0 = 0
0⊕1 = 1
1⊕0 = 1
1⊕1 = 0

一次一密密码的特点

- 优点：
  - 密钥随机产生，仅使用一次
  - 无条件安全
  - 加密和解密为加法运算，效率较高
- 缺点：
  - 密钥长度至少与明文长度一样长，密钥共享困难，不太实用

第七讲 流密码的基本概念

- 一次一密
- 流密码的定义
- 同步流密码

流密码概况

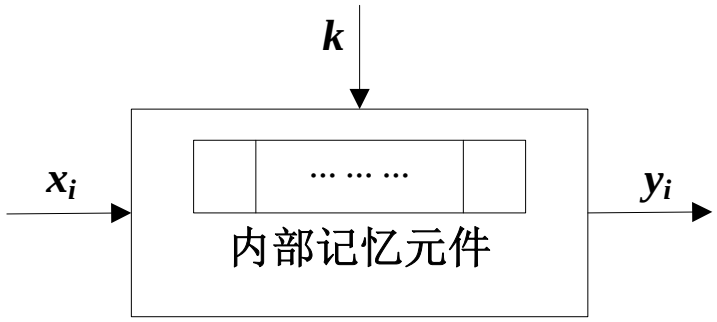
- 流密码(stream cipher)是一种重要的密码体制
  - 明文消息按字符或比特逐位加密
  - 流密码也称为序列密码(Sequence Cipher)
- 流密码在20世纪50年代得到飞跃式发展
  - 密钥流可以用移位寄存器电路来产生，也促进了线性和非线性移位寄存器发展
  - 流密码主要是基于硬件实现

流密码的基本思想

- 流密码的基本思想
  - 利用密钥k产生一个密钥流$z=z_0z_1z_2\ldots$，并使用如下规则对明文串$x=x_0x_1x_2\ldots$加密：

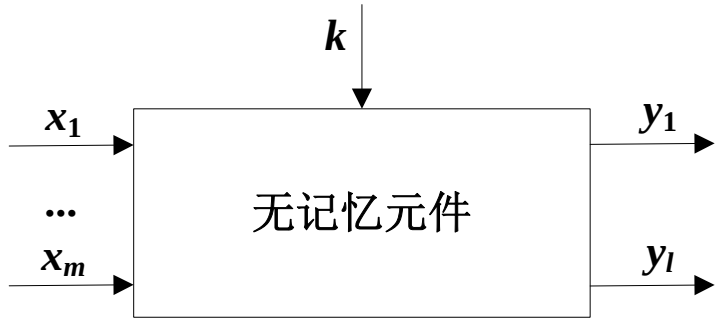
$$y=y_0y_1y_2\ldots=Ez_0(x_0)Ez_1(x_1)\,Ez_2(x_2)\ldots,$$

- 密钥流
  - 由密钥流发生器f产生：$z_i=f(k,\sigma_i)$
  - σ_i是加密器中的记忆元件在时刻i的状态
  - f是由k,σ_i产生的函数



$y_i=Ez_i(x_i)$

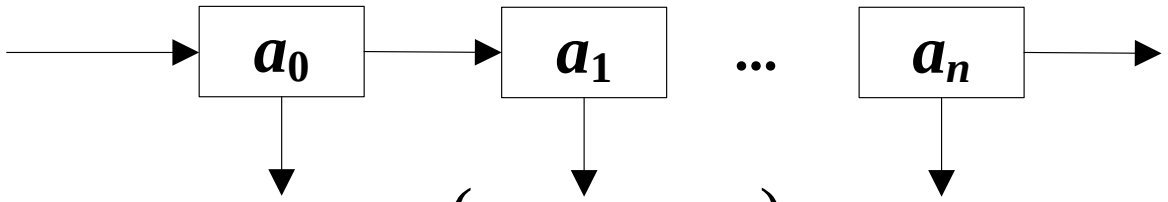
流密码



$y=E_k(x)$

分组密码

- 内部记忆元件由一组移位寄存器构成



$\sigma_i=(a_0,a_1,\cdots,a_n)$

第七讲 流密码的基本概念

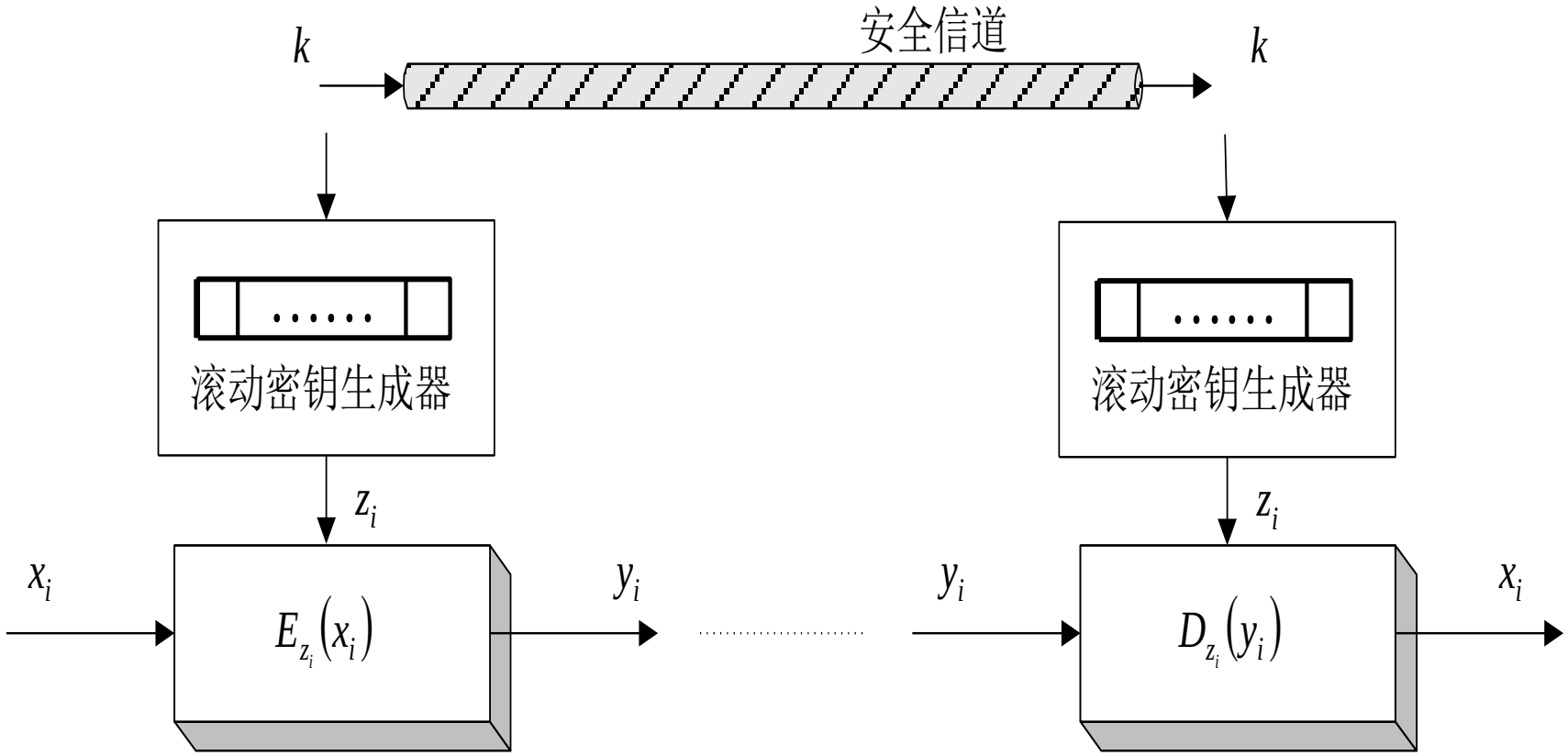
- 一次一密
- 流密码的定义
- 同步流密码

同步流密码

- 内部记忆元件的状态σ_i独立于明文字符的叫做同步流密码，否则叫做自同步流密码。

- 在同步流密码中，由于$z_i=f(k,\sigma_i)$与明文字符无关，因而此时密文字符$y_i=E_{zi}(x_i)$也不依赖于此前的明文字符。因此，可将同步流密码的加密器分成密钥流产生器和加密变换器两个部分。

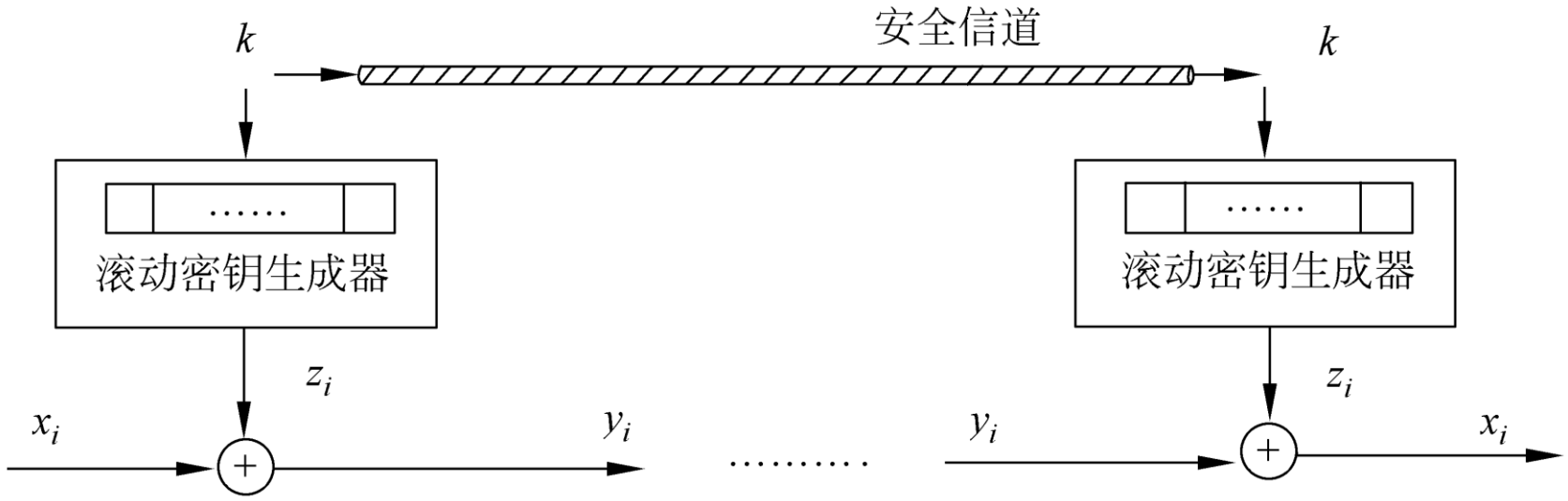
同步流密码体制模型



同步流密码体制模型

加法流密码体制模型

二元加法流密码是目前最为常用的流密码体制，其加密变换可表示为$y_i=z_i \oplus x_i$。



加法流密码体制模型

流密码的需求

- 一次一密密码是加法流密码的原型
  - 如果密钥用作滚动密钥流，则加法流密码就退化成一次一密密码。
- 密码设计者的最大愿望是设计出一个滚动密钥生成器，使得密钥经其扩展成的密钥流序列具有如下性质：
  - 极大的周期
  - 良好的统计特性
  - 抗线性分析

感 谢 聆 听!

xynie@uestc.edu.cn