



现代密码学

第二章 流密码

信息与软件工程学院



流密码的基本概念

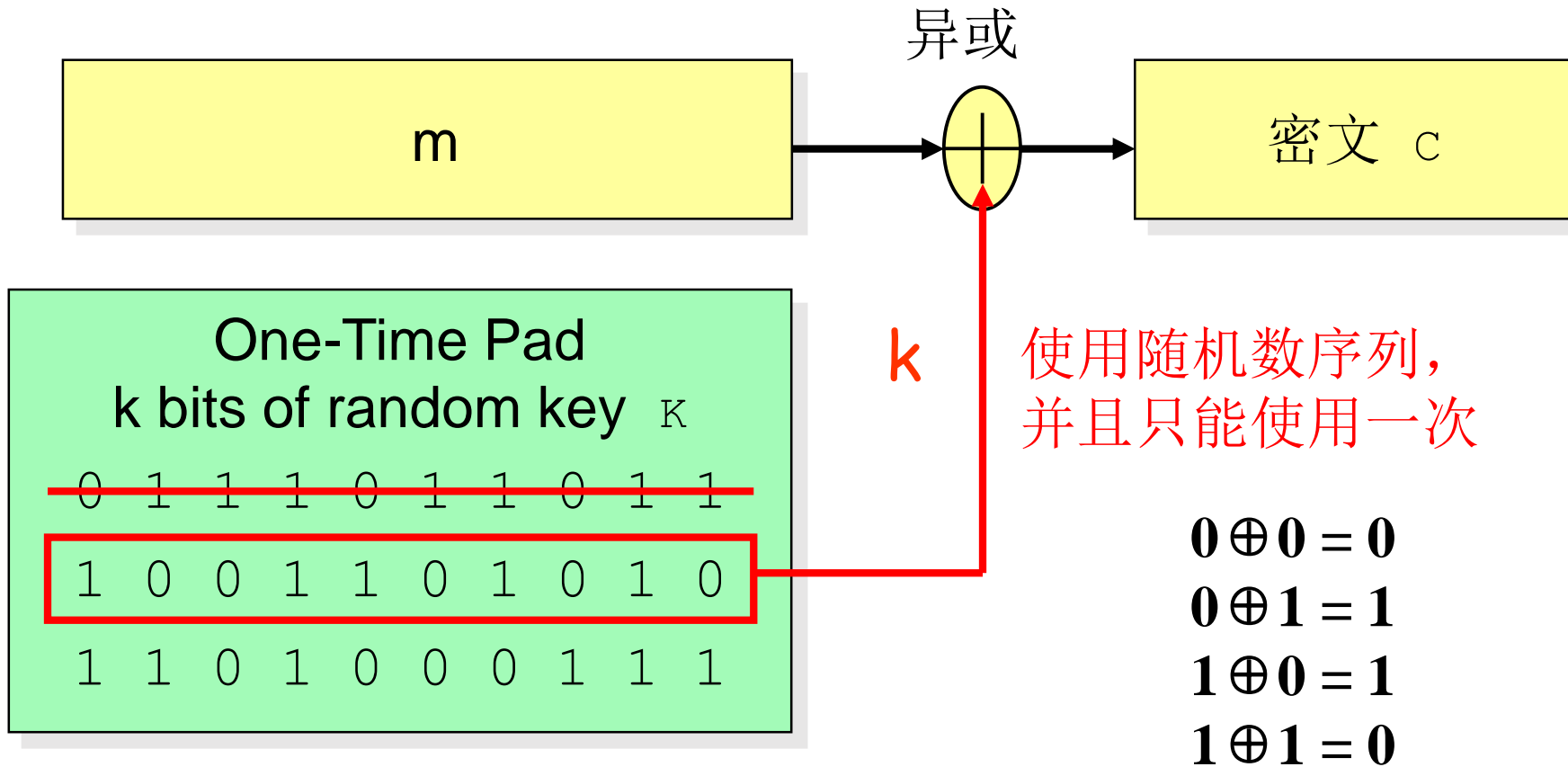


A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

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： $x=x_0x_1x_2\ldots$
- 密钥： $k=k_0k_1k_2\ldots$
- 密文： $y=y_0y_1y_2\ldots$
- 加密函数： $y_i=x_i+k_i(\text{mod}26)$
- 解密函数： $x_i=y_i-k_i(\text{mod}26)$
- 注： 密钥为随机产生的，而且只使用一次

一次一密密码



A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the title.

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
-

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

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

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

流密码的基本思想

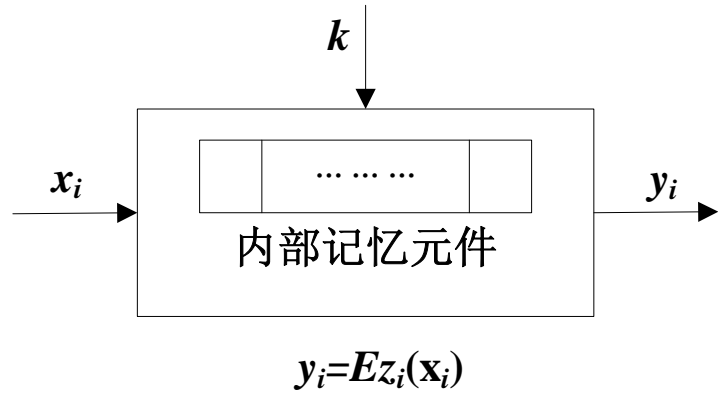
- 流密码的基本思想

- 利用密钥 k 产生一个密钥流 $z=z_0z_1z_2\dots$ ，并使用如下规则对明文串 $x=x_0x_1x_2\dots$ 加密：

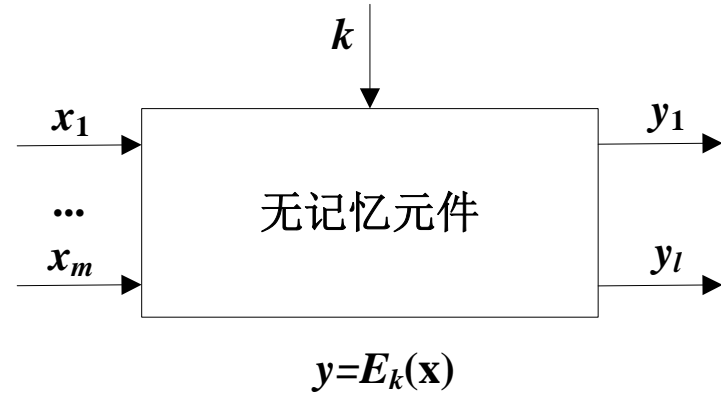
$$y=y_0y_1y_2\dots=Ez_0(x_0)Ez_1(x_1)Ez_2(x_2)\dots,$$

- 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
-

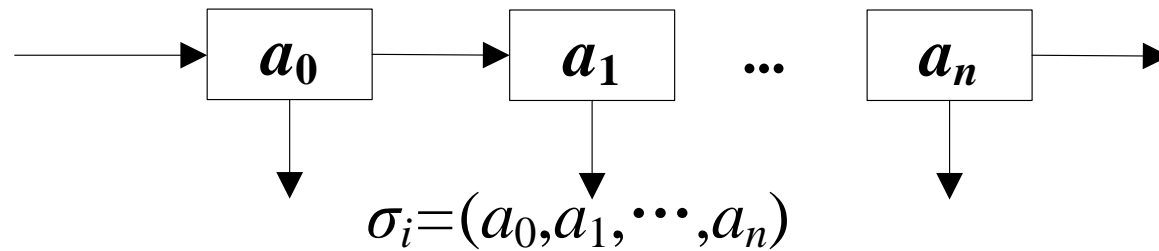


流密码



分组密码

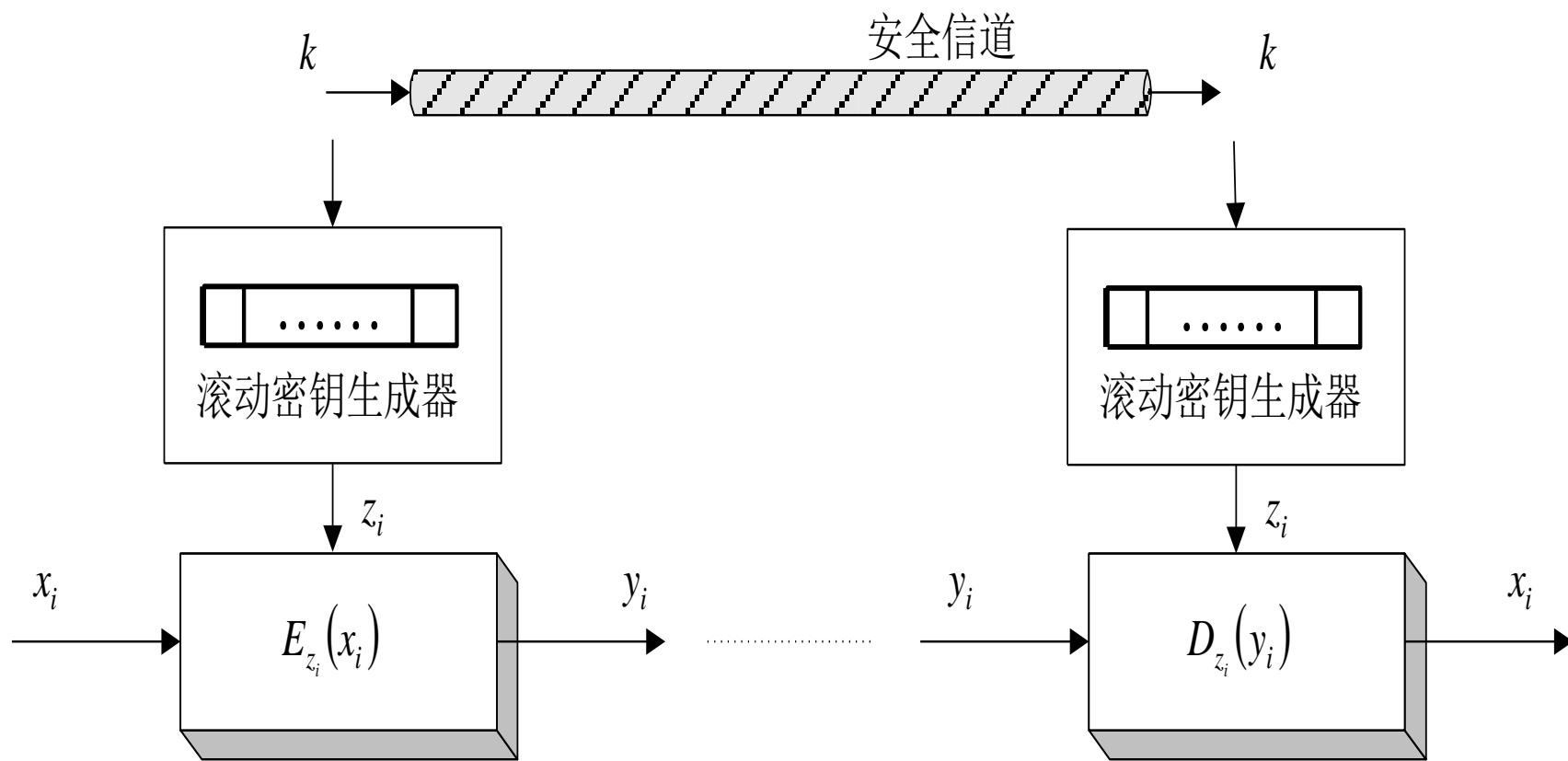
- 内部记忆元件由一组移位寄存器构成



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 $y_i=E_{z_i}(x_i)$ 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。

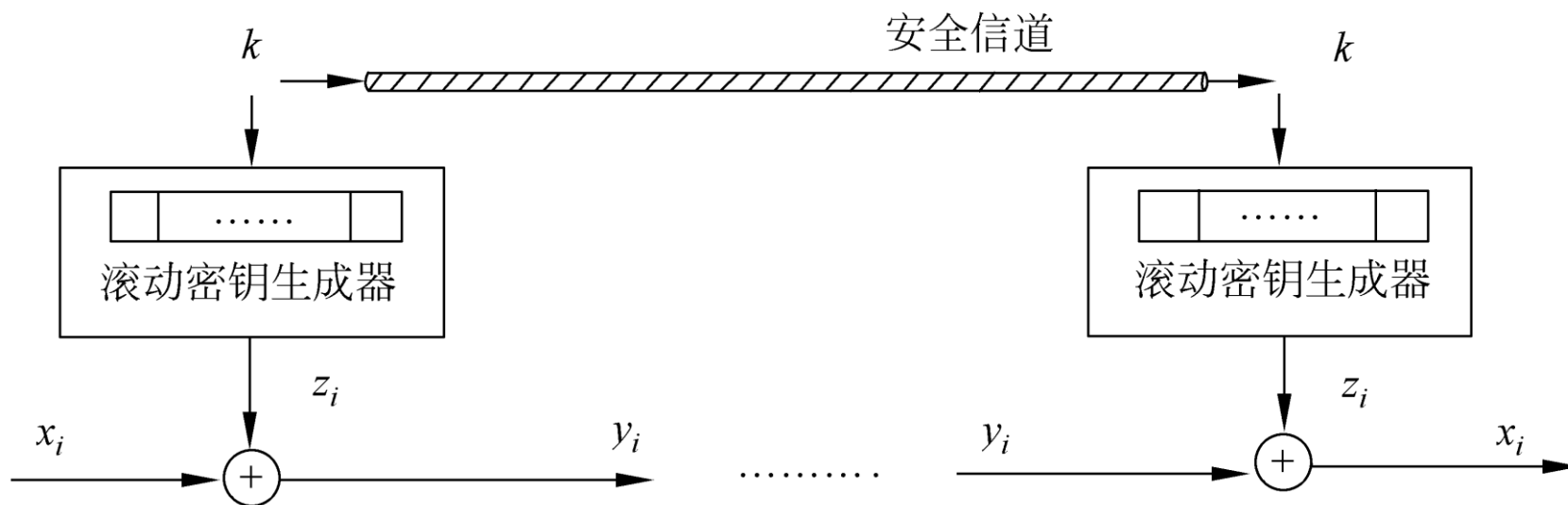
同步流密码体制模型



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

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

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



现代密码学

有限状态自动机

信息与软件工程学院

有限状态自动机的模型

➤ 有限状态自动机是具有离散输入和输出（输入集和输出集均有限）的一种数学模型，由以下3部分组成：

① 有限状态集 $S = \{ s_i \mid i=1,2,\dots,l \}$ 。

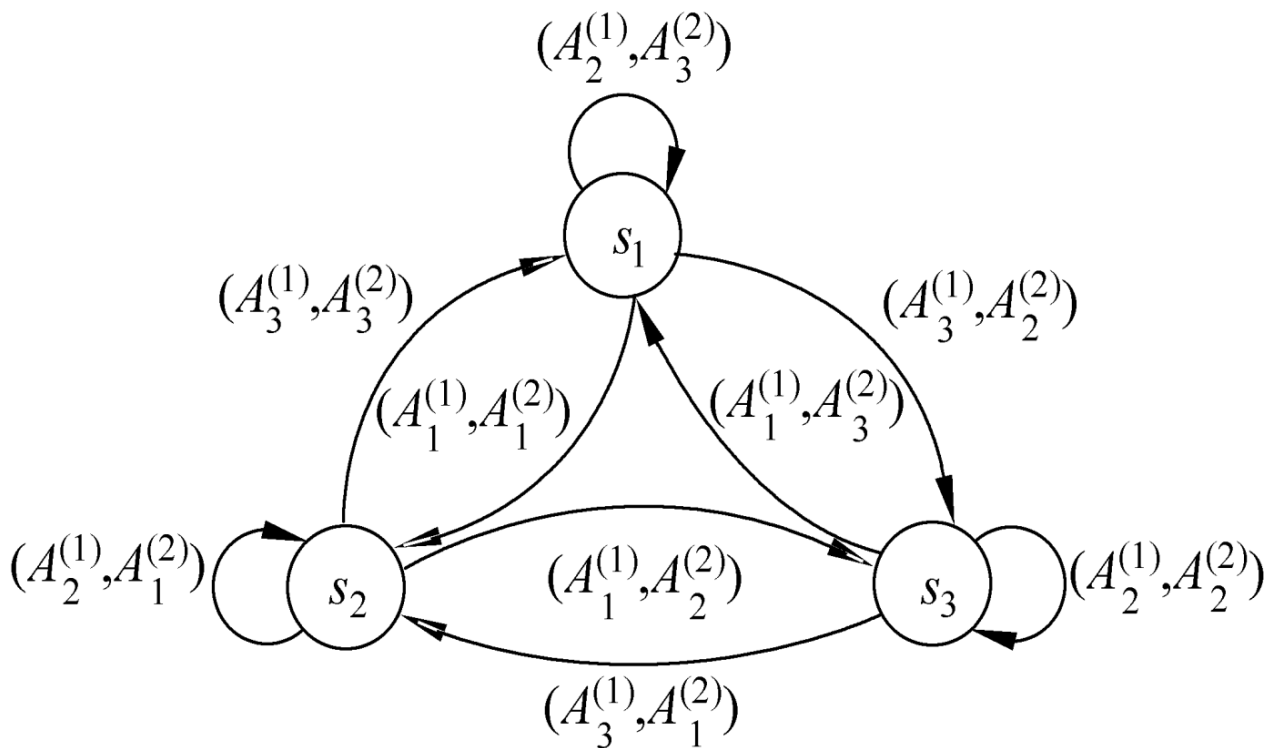
② 有限输入字符集 $A_1 = \{ A^{(1)}_j \mid j=1,2,\dots,m \}$ 和有限输出字符集 $A_2 = \{ A^{(2)}_k \mid k=1,2,\dots,n \}$ 。

③ 转移函数 $A^{(2)}_k = f_1(s_i, A^{(1)}_j)$, $s_h = f_2(s_i, A^{(1)}_j)$

即在状态为 s_i ，输入为 $A^{(1)}_j$ 时，输出为 $A^{(2)}_k$ ，而状态转移为 s_h 。

有限状态自动机的有向图表示

- 有限状态自动机可用有向图表示，称为**转移图**。
- 转移图的顶点对应于自动机的状态，若状态 s_i 在输入 $A^{(1)}_i$ 时转为状态 s_j ，且输出一字符 $A^{(2)}_j$ ，则在转移图中，从状态 s_i 到状态 s_j 有一条标有 $(A^{(1)}_i, A^{(2)}_j)$ 的弧线



有限状态自动机的矩阵表示

- 设 $S=\{s_1,s_2,s_3\}$, $A_1=\{A_1^{(1)},A_2^{(1)},A_3^{(1)}\}$, $A_2=\{A_1^{(2)},A_2^{(2)},A_3^{(2)}\}$, 则该有限状态自动机的矩阵表示如下

f_1	$A_1^{(1)}$	$A_2^{(1)}$	$A_3^{(1)}$
s_1	$A_1^{(2)}$	$A_3^{(2)}$	$A_2^{(2)}$
s_2	$A_2^{(2)}$	$A_1^{(2)}$	$A_3^{(2)}$
s_3	$A_3^{(2)}$	$A_2^{(2)}$	$A_1^{(2)}$
f_2	$A_1^{(1)}$	$A_2^{(1)}$	$A_3^{(1)}$
s_1	s_2	s_1	s_3
s_2	s_3	s_2	s_1
s_3	s_1	s_3	s_2

有限状态自动机的实例

若输入序列为

$A_1^{(1)} A_2^{(1)} A_1^{(1)} A_3^{(1)} A_3^{(1)} A_1^{(1)}$

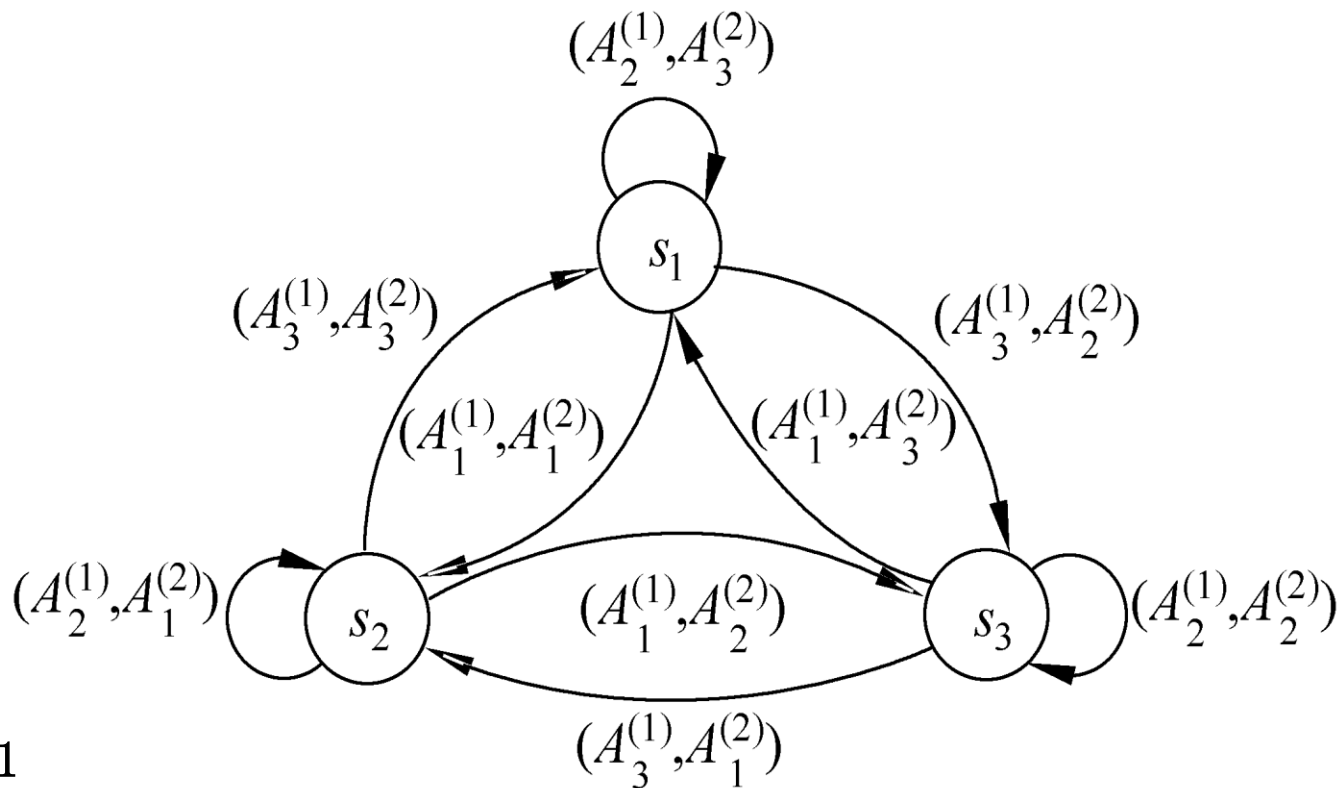
初始状态为 s_1 ,

则得到状态序列

$s_1 s_2 s_2 s_3 s_2 s_1 s_2$

输出字符序列

$A_1^{(2)} A_1^{(2)} A_2^{(2)} A_1^{(2)} A_3^{(2)} A_1^{(2)}$

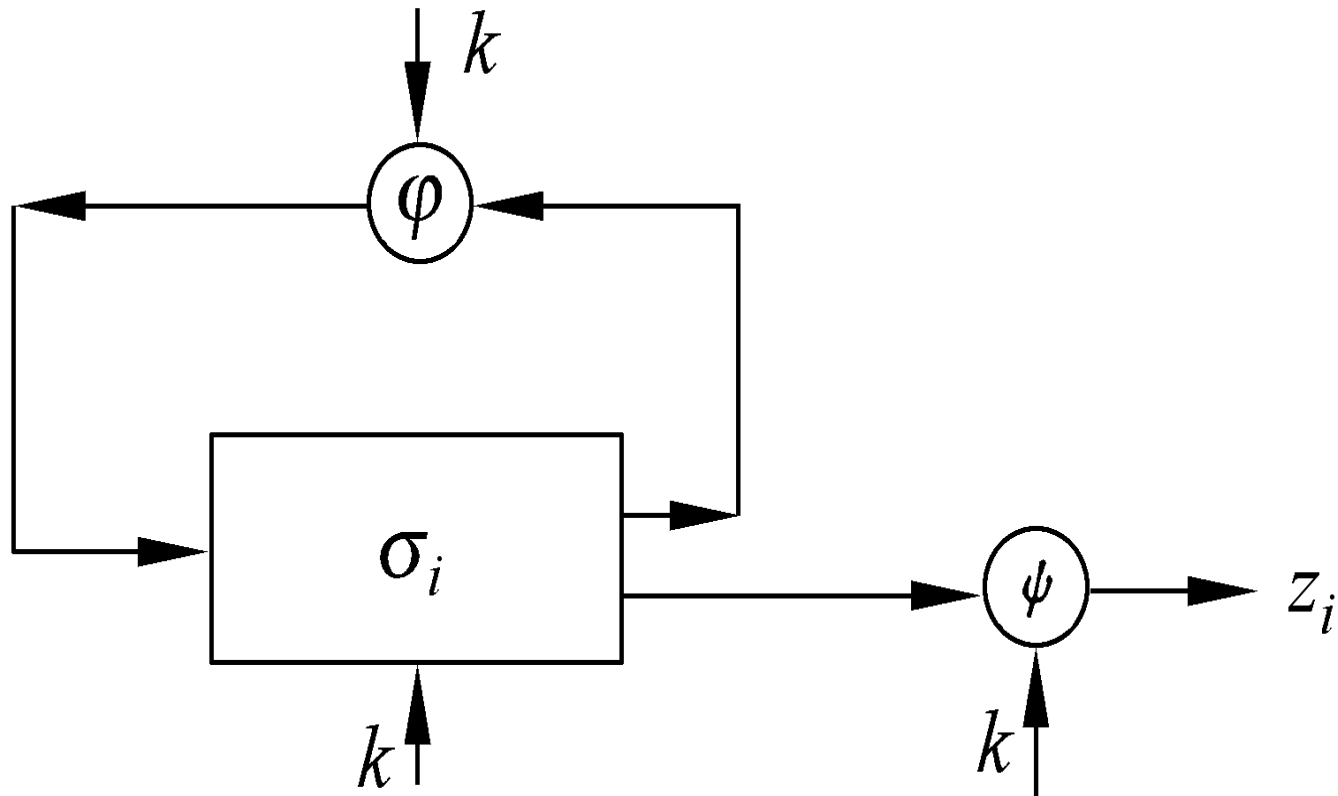


A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

密钥流产生器

- 密钥流产生器: 参数为 k 的有限状态自动机,
 - 一个输出符号集 Z 、一个状态集 Σ 、两个函数 φ 和 ψ 以及一个初始状态 σ_0 组成。
 - 状态转移函数 $\varphi: \sigma_i \rightarrow \sigma_{i+1}$, 将当前状态 σ_i 变为一个新状态 σ_{i+1} ,
 - 输出函数 $\psi: \sigma_i \rightarrow z_i$, 当前状态 σ_i 变为输出符号集中的一个元素 z_i 。
-

作为有限状态自动机的密钥流生成器



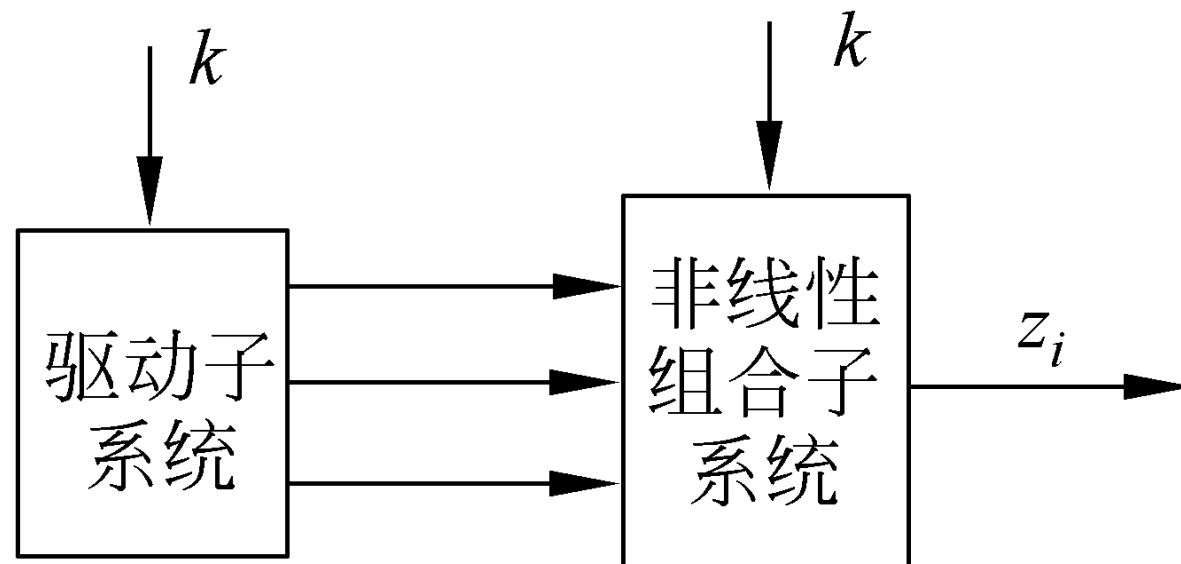
作为有限状态自动机的密钥流生成器

密钥流生成器设计的关键

- 关键在于：找出适当的状态转移函数 φ 和输出函数 ψ ，使得输出序列 z 满足密钥流序列 z 应满足的随机性条件，并且要求在设备上节省的和容易实现的。
- 一般采用线性的 φ 和非线性的 ψ ，这样将能够进行深入的分析并可以得到好的生成器

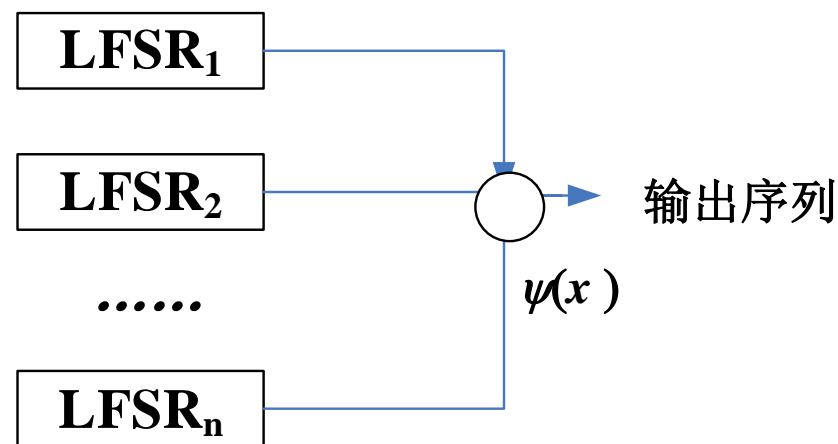
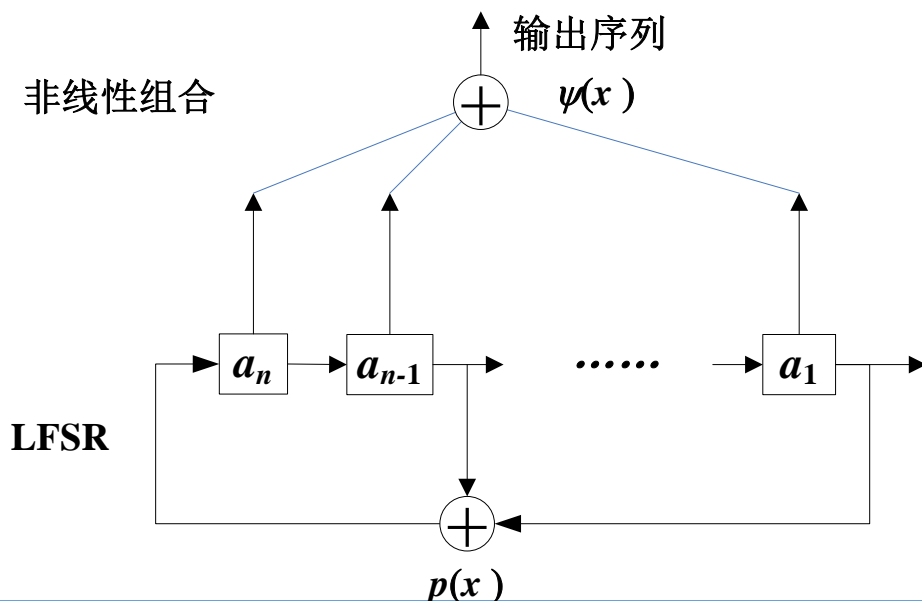
密钥流生成器的分解

- 密钥流生成器可分成**驱动部分**和**非线性组合部分**
- 驱动部分控制生成器的状态转移，并为非线性组合部分提供统计性能好的序列
- 非线性组合部分要利用这些序列组合出满足要求的密钥流序列



常见的两种密钥流产生器

- 目前最为流行和实用的密钥流产生器，其驱动部分是一个或多个线性反馈移位寄存器。
- 前者称为滤波生成器，或前馈生成器
- 后者称为非线性组合生成器
- 还有钟控生成器，缩减生成器，停走生成器等



现代密码学

二元序列的伪随机性

信息与软件工程学院

二元序列的伪随机性

- GF (2) 上的一个无限序列

$$\underline{a} = (a_1, a_2, \dots, a_n, \dots)$$

称为二元序列，若 $a_i \in GF(2)$ 。

- 周期：对于二元序列 \underline{a} ，如果存在正整数 l ，使得对于一切正整数 k 都有

$$a_k = a_{k+l}$$

则称 \underline{a} 是周期的。

满足上述条件的最小正整数称为 \underline{a} 的周期记为 $p(\underline{a})$

周期的性质

- 设GF (2) 上的一个无限序列 $\underline{a} = (a_1, a_2, \dots, a_n, \dots)$ 是周期为 $p(\underline{a})$ 的二元序列，并设正整数 l 对任何非负整数 k 都有 $a_k = a_{k+l}$ ，则一定有

$$p(\underline{a}) \mid l$$

- 证明：

设 $l = qp(\underline{a}) + r$ ，其中 q, r 为正整数，且 $0 \leq r < p(\underline{a})$ ，则有

$$a_k = a_{k+l}$$

$$\Rightarrow a_k = a_{qp(\underline{a})+r+k}$$

$$\Rightarrow a_k = a_{r+k}$$

又由于 $0 \leq r < p(\underline{a})$ ，根据 $p(\underline{a})$ 的极小性可知 $r = 0$ ，因此 $p(\underline{a}) \mid l$ 。

游程的定义

设 \underline{a} 是 GF (2) 上周期为 $p(\underline{a})$ 的周期序列。将 \underline{a} 的一个周期

$$(a_1, a_2, \dots, a_{p(\underline{a})})$$

依次排列在一个圆周上使 $a_{p(\underline{a})}$ 与 a_1 相连, 把这个圆周上形如

$$\underbrace{011 \cdots 110}_{\text{都是1}} \text{ 或 } \underbrace{100 \cdots 001}_{\text{都是0}}$$

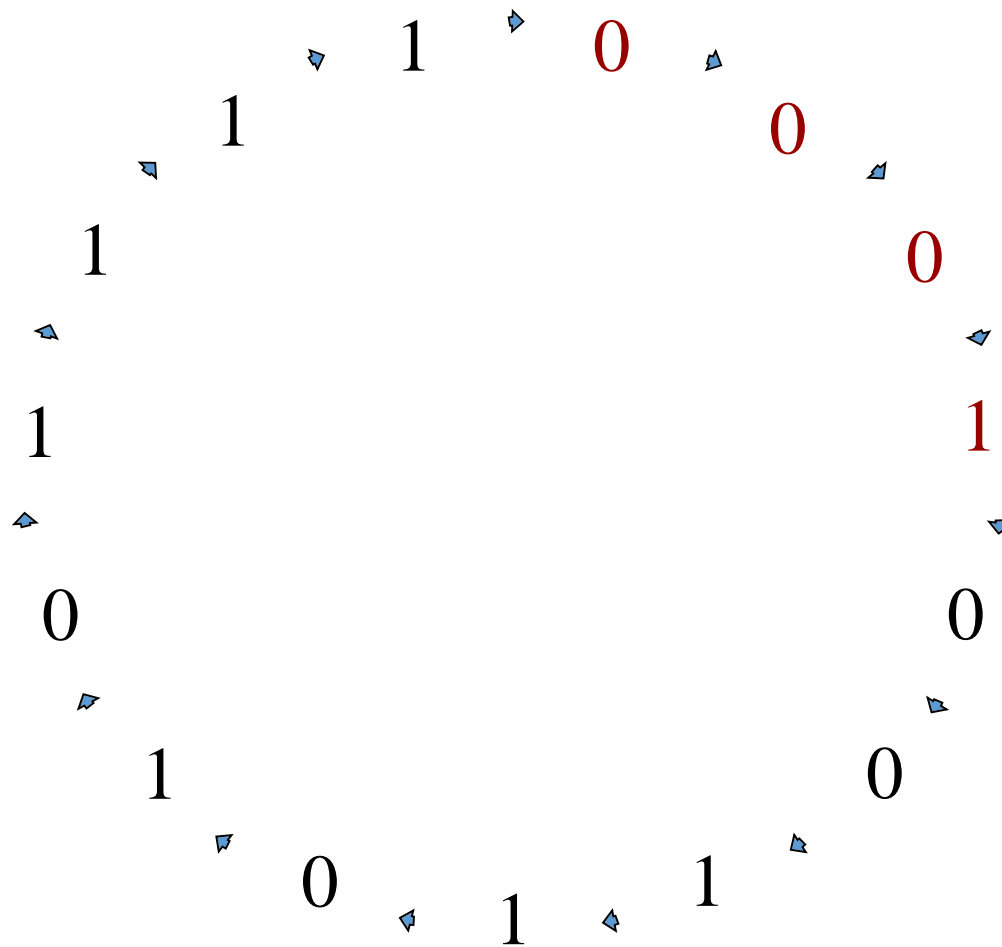
的一连串两两相邻的项分别称为 \underline{a} 的一个周期中一个 1 游程或一个 0 游程。而 1 游程中 1 的个数或 0 游程中 0 的个数称为游程的长度。



游程的例子

周期为15的二元序列
100010011010111

011110为1的4游程
10001为0的3游程



自相关函数

GF(2)上周期为**T**的序列**{a_i}**的**自相关函数**定义为

$$R(t) = \sum_{k=1}^T (-1)^{a_k} (-1)^{a_{k+t}}, 0 \leq t \leq T-1$$

当**t=0**时，**R(t)=T**；当**t≠0**时，称**R(t)**为**异相自相关函数**。

Golomb伪随机公设

3个随机性公设:

① 在序列的一个周期内，0与1的个数相差至多为1。

- 说明 $\{a_i\}$ 中0与1出现的概率基本上相同

② 在序列的一个周期内，长为 i 的游程占游程总数的 $1/2^i$ ($i=1,2,\dots$)，且在等长的游程中0的游程个数和1的游程个数相等。

- 说明0与1在序列中每一位置上出现的概率相同

③ 异相自相关函数是一个常数。

- 意味着通过对序列与其平移后的序列做比较，不能给出其他任何信息

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

伪随机序列的定义

设 $\underline{a} = (a_1, a_2, \dots, a_{p(\underline{a})}, \dots)$ 是 GF (2) 上一个周期等于 $p(\underline{a})$ 的周期序列。

如果对于一切 $t \not\equiv 0 \pmod{p(\underline{a})}$, 有

$$R(t) = -1$$

则称序列 $\underline{a} = (a_1, a_2, \dots, a_{p(\underline{a})}, \dots)$ 为伪随机序列。

- 可以证明上述定义满足Golomb三个伪随机公设, 详情参考
 - 万哲先著。代数和编码 (第三版)。高等教育出版社, 2007.
-

伪随机序列还应满足的条件

- C1. 周期 p 要足够大，如大于 10^{50} ;
- C2. 序列 $\{a_i\}_{i \geq 1}$ 产生易于高速生成;
- C3. 当序列 $\{a_i\}_{i \geq 1}$ 的任何部分暴露时，要分析整个序列，提取产生它的电路结构信息，在计算上是不可行的，称此为不可预测性。

C3决定了密码的强度，是流密码理论的核心。它包含了流密码要研究的许多主要问题，如线性复杂度、相关免疫性、不可预测性等等。

现代密码学

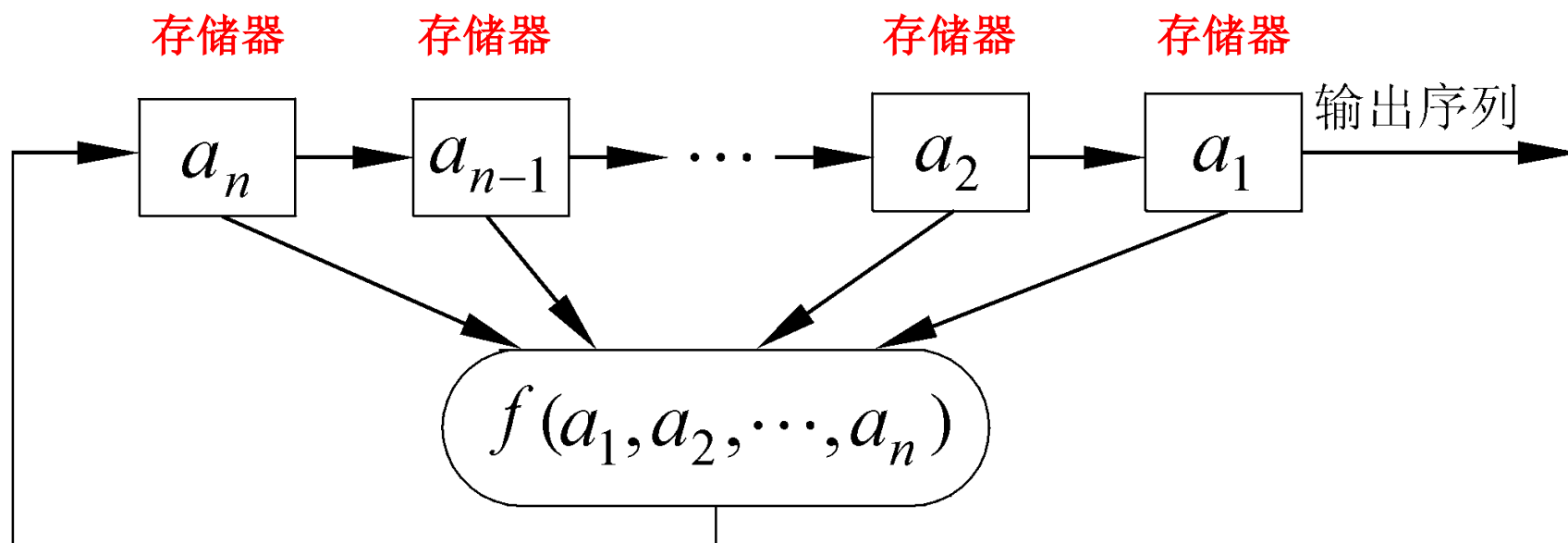
线性反馈移位寄存器

信息与软件工程学院

反馈移位寄存器

移位寄存器是流密码产生密钥流的一个主要组成部分。

GF(2) 上一个n级反馈移位寄存器由n个二元存储器与一个反馈函数 $f(a_1, a_2, \dots, a_n)$ 组成，如下图所示。



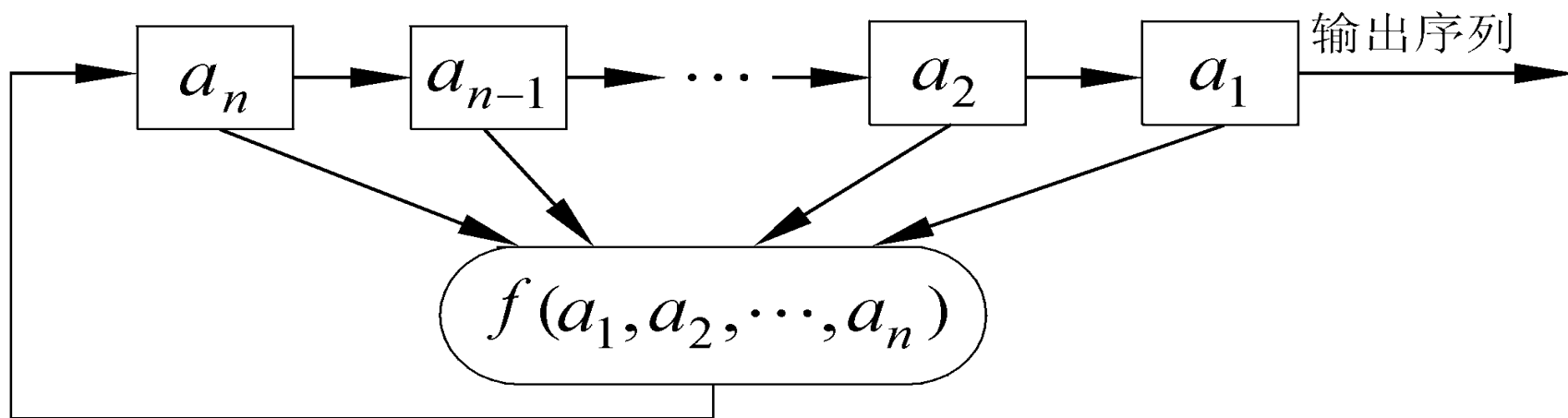
反馈移位寄存器的状态

在任一时刻，这些级的内容构成该反馈移位寄存器的状态，每一状态对应于GF(2)上的一个n维向量，共有 2^n 种可能的状态。

每一时刻的状态可用n维向量

$$(a_1, a_2, \dots, a_n)$$

表示，其中 a_i 是第i级存储器的内容。

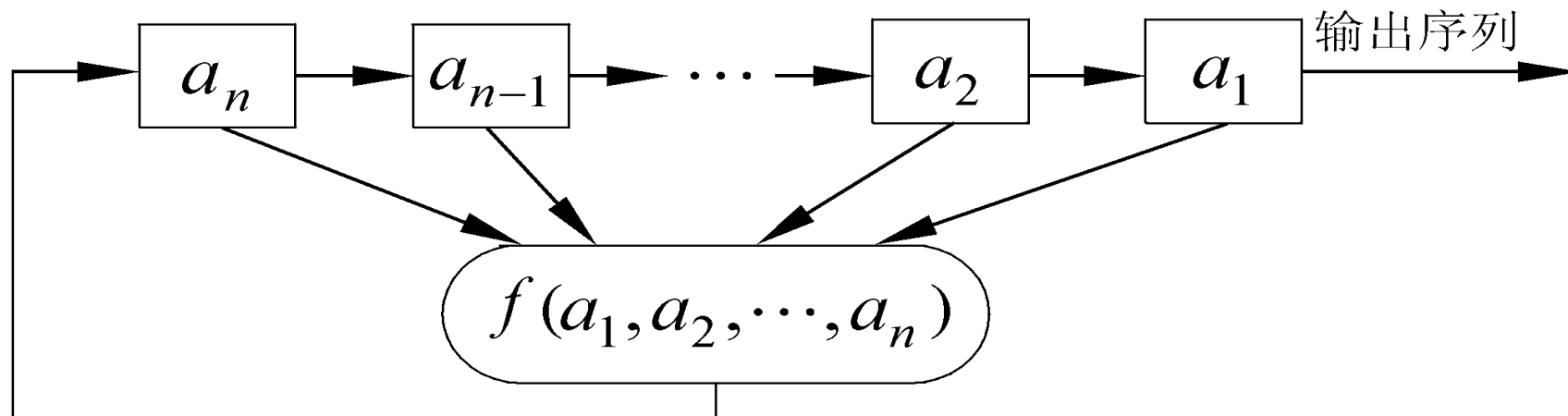


反馈函数

初始状态由用户确定。

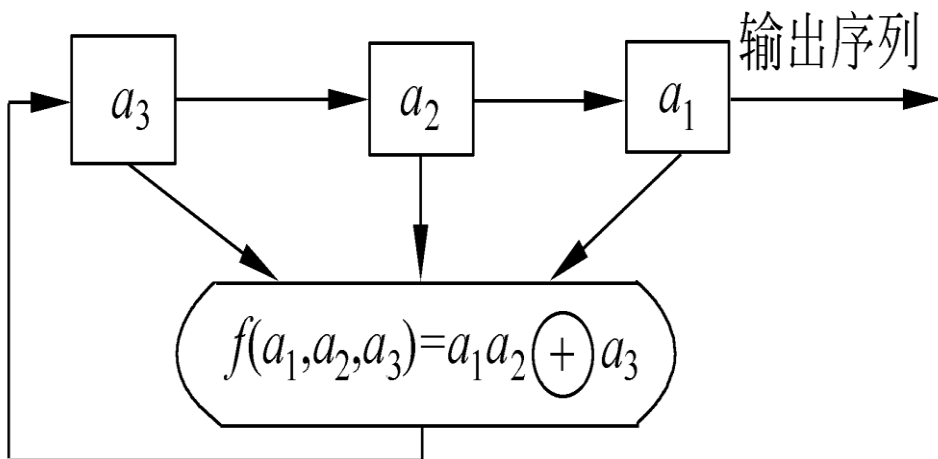
反馈函数 $f(a_1, a_2, \dots, a_n)$ 是 n 元布尔函数，即函数的自变量和因变量只取0和1这两个可能的值。

函数中的运算有逻辑与、逻辑或、逻辑补、异或等运算。



反馈移位寄存器的例子

如图是一个3级反馈移位寄存器，其初始状态为 $(a_1, a_2, a_3) = (1, 1, 0)$ ，输出可由右表给出。



一个3级反馈移位寄存器

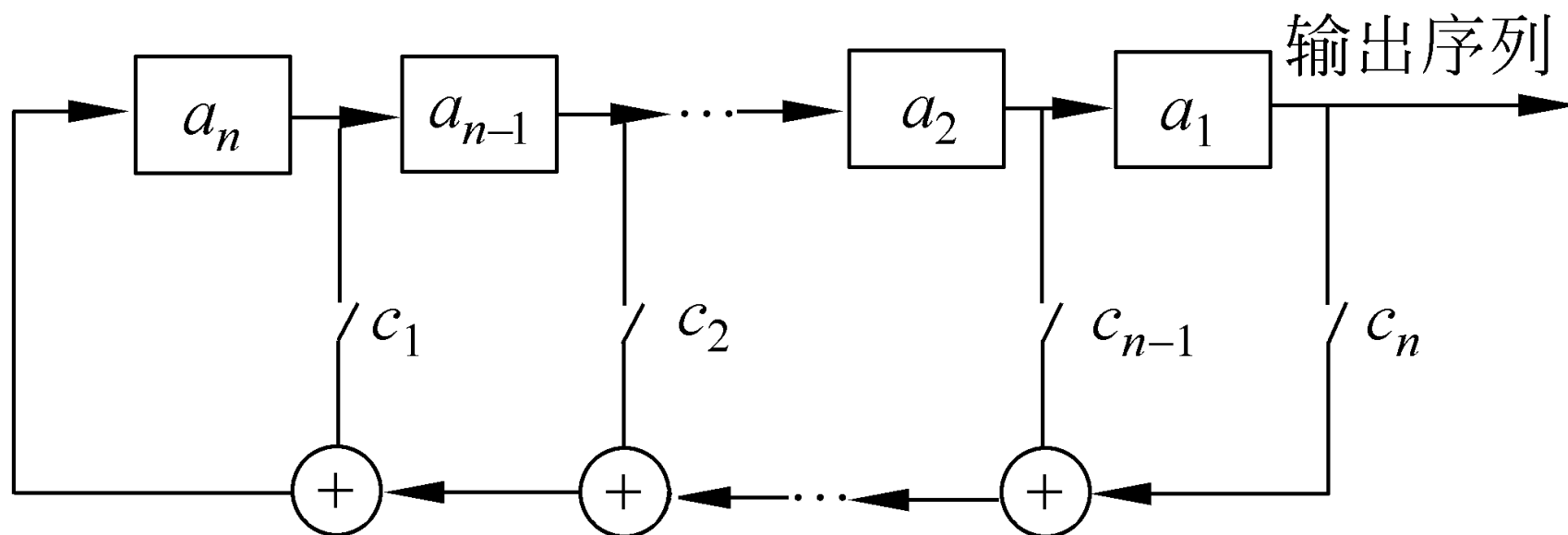
即输出序列为110111011101..., 周期为4。

一个3级反馈移位寄存器的状态和输出

状态 (a_3, a_2, a_1)	输出
0 1 1	1
1 0 1	1
1 1 0	0
1 1 1	1
0 1 1	1
1 0 1	1

线性反馈移位寄存器LFSR (linear feedback shift register)

GF(2) 上的n级线性反馈移位寄存器



$$f(a_1, a_2, \dots, a_n) = c_1 a_n \oplus c_2 a_{n-1} \oplus \dots \oplus c_n a_1$$

LFSR的反馈函数

输出序列 $\{a_t\}$ 满足：

$$f(a_1, a_2, \dots, a_n) = c_1 a_n \oplus c_2 a_{n-1} \oplus \dots \oplus c_n a_1$$

$$a_{n+1} = c_1 a_n \oplus c_2 a_{n-1} \oplus \dots \oplus c_n a_1$$

$$a_{n+2} = c_1 a_{n+1} \oplus c_2 a_n \oplus \dots \oplus c_n a_2$$

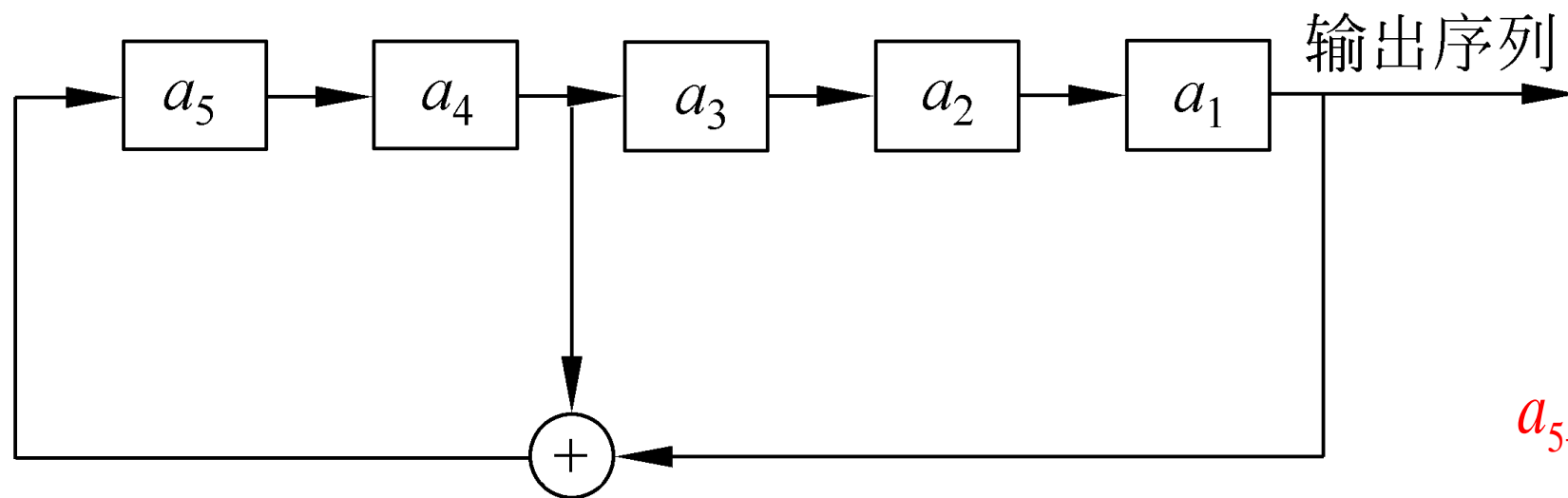
.....

$$a_{n+t} = c_1 a_{n+t-1} \oplus c_2 a_{n+t-2} \oplus \dots \oplus c_n a_t, t = 1, 2, \dots$$

线性反馈移位寄存器：实现简单、速度快、有较为成熟的理论，成为构造密钥流生成器的重要组成部分之一。

LFER的实例

例 下图是一个5级线性反馈移位寄存器，其初始状态为 $(a_1, a_2, a_3, a_4, a_5) = (1, 0, 0, 1, 1)$



反馈函数

$$a_{5+t} = a_{t+3} \oplus a_t, t = 1, 2, \dots$$

可求出输出序列为

1001101001000010101110110001111100110...

周期为**31**。

密钥流的周期

- 给定密钥流 $\{a_i\} = a_1, a_2, a_3, \dots, a_n, \dots$ ，如果存在整数 r ，使得对于任意 a_i ，都有 $a_{i+r} = a_i$ ，则称 r 为该密钥流的一个周期，称满足 $a_{i+r} = a_i$ 的**最小正整数**为该密钥流的最小周期或简称**周期**。

LFSR的性质

总是假定 c_1, c_2, \dots, c_n 中至少有一个不为0，否则 $f(a_1, a_2, \dots, a_n) \equiv 0$ 。

总是假定 $c_n=1$ 。

- LFSR输出序列的性质：完全由其反馈函数决定。
- n 级LFSR状态数：最多有 2^n 个
- n 级LFSR的状态周期： $\leq 2^n - 1$
- 输出序列的周期=状态周期， $\leq 2^n - 1$
- 选择合适的反馈函数可使序列的周期达到最大值 $2^n - 1$ ，周期达到最大值的序列称为m序列。



现代密码学

m-序列

信息与软件工程学院

线性移位寄存器的一元多项式表示

定义2.1 设n级线性移位寄存器的输出序列满足递推关系

$$a_{n+k} = c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \dots \oplus c_n a_k \quad (*)$$

用延迟算子 D ($Da_k = a_{k-1}$) 作为未定元, 给出的反馈多项式为:

$$p(D) = 1 + c_1 D + \dots + c_{n-1} D^{n-1} + c_n D^n$$

这种递推关系可用一个一元高次多项式

$$p(x) = 1 + c_1 x + \dots + c_{n-1} x^{n-1} + c_n x^n$$

表示, 称这个多项式为LFSR的特征多项式。

关于特征多项式的解释

$$\begin{aligned} a_{n+k} &= c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \cdots \oplus c_n a_k \\ \Leftrightarrow a_{n+k} \oplus c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \cdots \oplus c_n a_k &= 0 \end{aligned}$$

$D(a_k) = a_{k-1}$ ，用 $p(D) = 1 + c_1 D + \cdots + c_n D^n$ 作用于 a_{n+k} 后恰好就是上式的左边，

即

$$\begin{aligned} p(D)(a_{n+k}) &= (1 + c_1 D + \cdots + c_n D^n)(a_{n+k}) \\ &= a_{n+k} + c_1 D(a_{n+k}) + \cdots + c_n D^n(a_{n+k}) \\ &= a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_n a_k \end{aligned}$$

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

生成函数

定义2.2 给定序列 $\{a_i\}$ ，幂级数

$$A(x) = \sum_{i=1}^{\infty} a_i x^{i-1}$$

称为该序列的生成函数。

生成函数的性质

定理2.1 设 $p(x)=1+c_1x+\dots+c_{n-1}x^{n-1}+c_nx^n$ 是 $GF(2)$ 上的多项式， $G(p(x))$ 中任一序列 $\{a_i\}$ 的生成函数 $A(x)$ 满足：

$$A(x) = \frac{\phi(x)}{p(x)}$$

其中

$$\phi(x) = \sum_{i=1}^n (c_{n-i} x^{n-i} \sum_{j=1}^i a_j x^{j-1})$$

定理2.1的证明

证明： 在等式

$$a_{n+1} = c_1 a_n \oplus c_2 a_{n-1} \oplus \dots \oplus c_n a_1$$

$$a_{n+2} = c_1 a_{n+1} \oplus c_2 a_n \oplus \dots \oplus c_n a_2$$

...

两边分别乘以 x^n, x^{n+1}, \dots , 再求和, 可得

$$A(x) - (a_1 + a_2 x + \dots + a_n x^{n-1})$$

$$= c_1 x [A(x) - (a_1 + a_2 x + \dots + a_{n-1} x^{n-2})]$$

$$+ c_2 x^2 [A(x) - (a_1 + a_2 x + \dots + a_{n-2} x^{n-3})] + \dots + c_n x^n A(x)$$

移项
整理

$$\begin{aligned} & (1 + c_1 x + \dots + c_{n-1} x^{n-1} + c_n x^n) A(x) \\ &= (a_1 + a_2 x + \dots + a_n x^{n-1}) + c_1 x (a_1 + a_2 x + \dots + a_{n-1} x^{n-2}) \\ &+ c_2 x^2 (a_1 + a_2 x + \dots + a_{n-2} x^{n-3}) + \dots + c_{n-1} x^{n-1} a_1 \end{aligned}$$

定理2.1 证明 (续)

移项
整理

$$\begin{aligned} & (1+c_1x+\dots+c_{n-1}x^{n-1}+c_nx^n)A(x) \\ &= (a_1+a_2x+\dots+a_nx^{n-1})+c_1x(a_1+a_2x+\dots+a_{n-1}x^{n-2}) \\ &+ c_2x^2(a_1+a_2x+\dots+a_{n-2}x^{n-3})+\dots+c_{n-1}x^{n-1}a_1 \end{aligned}$$

$$p(x)A(x) = \sum_{i=1}^n (c_{n-i}x^{n-i} \sum_{j=1}^i a_jx^{j-1}) = \phi(x)$$

证毕。

注意： $A(x) = \frac{\phi(x)}{p(x)}$

$$\deg \phi(x) \leq n-1$$



- ※ $\phi(x)$ 的次数小于 n
 - 因此共有 $2^n - 1$ 个不同的非0表达式
 - 而每一个初态都对应不同的 $\phi(x)$, 共有 $2^n - 1$ 个初态
 - 所以初态和 $\phi(x)$ 是一一对应的

一些定理和定义

根据初始状态的不同，由递推关系(*)生成的非恒零的序列有 2^n-1 个，记这 2^n-1 个非零序列的全体为 $G(p(x))$ 。

定理2.2 $p(x)|q(x)$ 的充要条件是 $G(p(x)) \subseteq G(q(x))$ 。

——该定理说明：可用 n 级LFSR产生的序列，也可用级数更多的LFSR来产生。

定义2.3 设 $p(x)$ 是 $GF(2)$ 上的多项式，使 $p(x)|(x^p-1)$ 成立的最小正整数 p 称为 $p(x)$ 的周期或阶。

定理2.3 若序列 $\{a_i\}$ 的特征多项式 $p(x)$ 定义在 $GF(2)$ 上， p 是 $p(x)$ 的周期，则 $\{a_i\}$ 的周期 $r|p$ 。

——该定理说明： n 级LFSR输出序列的周期 r ，不依赖于初始条件，而依赖于特征多项式 $p(x)$ 。

• 定理2.2 $p(x)|q(x)$ 的充要条件是 $G(p(x))\subset G(q(x))$

• 证明：若 $p(x)|q(x)$ ，可设 $q(x)=p(x)r(x)$ ，因此

$$\bullet \quad A(x) = \frac{\phi(x)}{p(x)} = \frac{\phi(x)r(x)}{p(x)r(x)} = \frac{\phi(x)r(x)}{q(x)}$$

• 而 $\phi(x)$ 次数小于等于 $n-1$ ， $r(x)$ 次数为 n_q-n ，所以 $\phi(x)r(x)$ 次数小于等于 $n_q-n+(n-1)=n_q-1$ 。

• 根据定理2.1的推导过程，可知 $\phi(x)r(x)$ 唯一对应一个 $q(x)$ 生成的序列，而显然有

• $q(x)A(x)=p(x)r(x)A(x)=\phi(x)r(x)$ ，即该序列为 $A(x)$ 。

• 所以若 $\{a_i\}\in G(p(x))$ ，则也有 $\{a_i\}\in G(q(x))$ ，即 $G(p(x))\subset G(q(x))$

- 反之，若 $G(p(x)) \subset G(q(x))$ ，则对于次数小于 n 的多项式 $\phi(x)$ ，存在序列 $\{a_i\} \in G(p(x))$ ，以

$$A(x) = \frac{\phi(x)}{p(x)}$$

为生成函数

根据定理2.1的推导过程，当 $\phi(x)=1$ 时，当然也存在序列 $\{a_i\} \in G(p(x))$ 以 $A(x) = \frac{1}{p(x)}$ 为生成函数

由于 $G(p(x)) \subset G(q(x))$ ，序列 $\{a_i\} \in G(q(x))$ ，所以存在函数 $r(x)$ ，使得 $\{a_i\}$ 的生成函数也等于 $\frac{r(x)}{q(x)}$ ，

从而 $A(x) = \frac{1}{p(x)} = \frac{r(x)}{q(x)}$ ，即 $q(x) = p(x)r(x)$ ，所以 $p(x) | q(x)$ 。
证毕

定理2.3 若序列 $\{a_i\}$ 的特征多项式 $p(x)$ 定义在 $GF(2)$ 上,
 p 是 $p(x)$ 的周期, 则 $\{a_i\}$ 的周期 $r|p$ 。

证明:

$$\because p(x) | (x^p - 1)$$

$$\therefore \exists q(x), \text{使 } x^p - 1 = p(x)q(x)$$

$$\text{又 } p(x)A(x) = \phi(x)$$

$$\text{得 } p(x)q(x)A(x) = \phi(x)q(x)$$

$$\therefore (x^p - 1)A(x) = \phi(x)q(x)$$

$$\text{由于 } \deg(q(x)) = p - n, \deg(\phi(x)) \leq n - 1$$

$$\text{得 } \deg((x^p - 1)A(x)) \leq p - 1$$

$$\text{故 } a_{i+p} = a_i, i = 1, 2, 3, \dots$$

$$\text{设 } p = kr + t, 0 \leq t < r,$$

$$\text{则 } a_{i+p} = a_{i+kr+t} = a_{i+t} = a_i, \text{所以 } t = 0$$

$$\therefore r | p.$$

定义2.3 设 $p(x)$ 是
 $GF(2)$ 上的多项式,
 使 $p(x) | (x^p - 1)$ 成
 立的最小正整数 p 称
 为 $p(x)$ 的周期或阶。

不可约多项式

定理2.4 设 $p(x)$ 是 n 次不可约多项式，周期为 m ，序列 $\{a_i\} \in G(p(x))$ ，则 $\{a_i\}$ 的周期为 m 。

证明：设 $\{a_i\}$ 的周期为 r ，由定理2.3有 $r|m$ ，所以 $r \leq m$ 。

设 $A(x)$ 为 $\{a_i\}$ 的生成函数， $A(x) = \phi(x)/p(x)$ ，即 $p(x)A(x) = \phi(x) \neq 0$ ， $\phi(x)$ 的次数不超过 $n-1$ 。而

$$\begin{aligned} A(x) &= \sum a_i x^{i-1} = a_1 + a_2 x + \dots + a_r x^{r-1} + x^r (a_1 + a_2 x + \dots + a_r x^{r-1}) \\ &\quad + (x^r)^2 (a_1 + a_2 x + \dots + a_r x^{r-1}) + \dots \\ &= a_1 + a_2 x + \dots + a_r x^{r-1} / (1 - x^r) \\ &= a_1 + a_2 x + \dots + a_r x^{r-1} / (x^r - 1) \end{aligned}$$



$$A(x) = \frac{a_1 + a_2x + \cdots + a_rx^{r-1}}{x^r - 1} = \frac{\phi(x)}{p(x)}$$

$$p(x)(a_1 + a_2x + \cdots + a_rx^{r-1}) = \phi(x)(x^r - 1)$$

$$p(x) \mid \phi(x)(x^r - 1)$$

$$\gcd(p(x), \phi(x)) = 1$$

$$p(x) \mid (x^r - 1), \text{ 因此 } m \leq r$$

$$\text{故 } m = r$$

n 级LFSR输出序列的周期 r 不依赖于初始条件，而依赖于特征多项式 $p(x)$ 。

m-序列产生的必要条件

定理2.5 n 级LFSR产生的序列有最大周期 2^n-1 的必要条件是其特征多项式为不可约的。

证明：设 n 级LFSR产生的序列周期达到最大 2^n-1 。

反证法：设特征多项式为 $p(x)$ ，若 $p(x)$ 可约，可设为 $p(x)=g(x)h(x)$ ，其中 $g(x)$ 不可约，且次数 $k < n$ 。由于 $G(g(x)) \subsetneq G(p(x))$ ，而 $G(g(x))$ 中序列的周期一方面不超过 2^k-1 ，另一方面又等于 2^n-1 ，这是矛盾的，所以 $p(x)$ 不可约。

该定理的逆不成立，即LFSR的特征多项式为不可约多项式时，其输出序列不一定是 m 序列。

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the section header.

定理2.5 的反例

例2.4 $f(x)=x^4+x^3+x^2+x+1$ 为GF(2)上的不可约多项式，这可由 $x, x+1, x^2+x+1$ 都不能整除 $f(x)$ 得到。以 $f(x)$ 为特征多项式的LFSR的输出序列可由

$$a_k=a_{k-1}\oplus a_{k-2}\oplus a_{k-3}\oplus a_{k-4}(k\geq 4)$$

和给定的初始状态求出，设初始状态为**0001**，则输出序列为**000110001100011...**，周期为5，不是m序列。

m-序列产生的充要条件

定义2.4 若 n 次不可约多项式 $p(x)$ 的阶为 2^n-1 ，则称 $p(x)$ 是 n 次本原多项式。

定理2.6 设 $\{a_i\} \in G(p(x))$ ， $\{a_i\}$ 为 m 序列的充要条件是 $p(x)$ 为本原多项式。

证明：若 $p(x)$ 是本原多项式，则其阶为 2^n-1 ，得 $\{a_i\}$ 的周期等于 2^n-1 ，即 $\{a_i\}$ 为 m 序列。

反之，若 $\{a_i\}$ 为 m 序列，即其周期等于 2^n-1 ，由定理2.5知 $p(x)$ 是不可约的。由定理2.3知 $\{a_i\}$ 的周期 2^n-1 整除 $p(x)$ 的阶，而 $p(x)$ 的阶不超过 2^n-1 ，所以 $p(x)$ 的阶为 2^n-1 ，即 $p(x)$ 是本原多项式。

对于任意的正整数 n ，至少存在一个 n 次本原多项式。所以对于任意的 n 级LFSR，至少存在一种连接方式使其输出序列为 m 序列

m-序列举例

例2.5 设 $p(x)=x^4+x+1$ ，若LFSR以 $p(x)$ 为特征多项式，则输出序列的递推关系为

$$a_k = a_{k-1} \oplus a_{k-4} (k \geq 4)$$

若初始状态为1001，则输出为

100100011110101100100011110101...

周期为 $2^4-1=15$ 。

若初始状态为1000，则输出为

100011110101100100011110101...

100100011110101100100011110101...

现代密码学

m-序列的伪随机性

信息与软件工程学院

随机序列的一般特性

游程： 设 $\{a_i\} = (a_1 a_2 a_3 \cdots)$ 为二元序列，例如 **00110111**，其前两个数字是00，称为0的2游程；接着是11，是1的2游程；再下来是0的1游程和1的3游程。

自相关函数： GF(2) 上周期为 T 的序列 $\{a_i\}$ 的自相关函数定义为

$$R(t) = \sum_{k=1}^T (-1)^{a_k} (-1)^{a_{k+t}}, 0 \leq t \leq T-1$$

当 $t=0$ 时， $R(t)=T$ ；当 $t \neq 0$ 时，称 $R(t)$ 为 **异相自相关函数**。

Golomb伪随机公设

3个随机性公设:

① 在序列的一个周期内，0与1的个数相差至多为1。

- 说明 $\{a_i\}$ 中0与1出现的概率基本上相同

② 在序列的一个周期内，长为 i 的游程占游程总数的 $1/2^i$ ($i=1, 2, \dots$)，且在等长的游程中0的游程个数和1的游程个数相等。

- 说明0与1在序列中每一位置上出现的概率相同

③ 异相自相关函数是一个常数。

- 意味着通过对序列与其平移后的序列做比较，不能给出其他任何信息

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

伪随机序列的定义

设 $\underline{a} = (a_1, a_2, \dots, a_{p(\underline{a})}, \dots)$ 是 GF (2) 上一个周期等于 $p(\underline{a})$ 的周期序列。

如果对于一切 $t \not\equiv 0 \pmod{p(\underline{a})}$, 有

$$R(t) = -1$$

则称序列 $\underline{a} = (a_1, a_2, \dots, a_{p(\underline{a})}, \dots)$ 为伪随机序列。

m序列的随机性

m序列满足Golomb的3个随机性公设。

定理2.7 GF(2)上的n长m序列 $\{a_i\}$ 具有如下性质:

- ① 在一个周期内, 0、1出现的次数分别为 $2^{n-1}-1$ 和 2^{n-1} 。
- ② 在一个周期内, 总游程数为 2^{n-1} ; 对 $1 \leq i \leq n-2$, 长为i的游程有 2^{n-i-1} 个, 且0、1游程各半; 长为n-1的0游程一个, 长为n的1游程一个。
- ③ $\{a_i\}$ 的自相关函数为

$$R(t) = \begin{cases} 2^n - 1, & t = 0 \\ -1, & 0 < t \leq 2^n - 2 \end{cases}$$

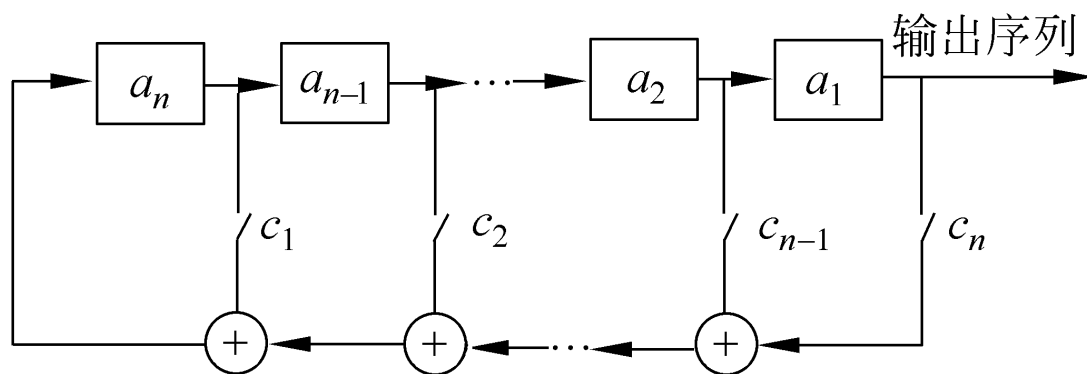
定理2.7的证明

证明：① 在 n 长 m 序列的一个周期内，除了全0状态外，**每个 n 长状态（共 2^n-1 个）都恰好出现一次。**

LFSR的输出为每个状态的 a_1 ，因此输出为1的状态必然是 $(**\cdots*1)$ 的形式，

而 m 序列这类状态共有 2^{n-1} 个，所以输出中1的个数为 **2^{n-1} 个**。

输出为0的状态必然是 $(**\cdots*0)$ 的形式，而 m 序列这类状态共有 $2^{n-1}-1$ 个（因为不能有全零状态），所以输出中0的个数为 **$2^{n-1}-1$ 个**。



定理2.7的证明（续）

证明：

② 对 $n=1,2$ ，易证结论成立。

对 $n>2$ ，当 $1 \leq i \leq n-2$ 时， n 长 m 序列的一个周期内，长为 i 的0游程数目等于序列中如下形式的状态数目： $100\dots 01*\dots *$ ，其中 $n-i-2$ 个 $*$ 可任取0或1。这种状态共有 2^{n-i-2} 个。同理可得长为 i 的1游程数目也等于 2^{n-i-2} ，所以长为 i 的游程总数为 2^{n-i-1} 。

定理2.7的证明（续）

由于寄存器中不会出现全0状态，所以不会出现0的 n 游程，但必有一个1的 n 游程，而且1的游程不会更大，因为若出现1的 $n+1$ 游程，就必然有两个相邻的全1状态，但这是不可能的。这就证明了1的 n 游程必然出现在如下的串中：

$$0 \quad \underbrace{11 \cdots 1}_{n \text{ 个 } 1} \quad 0$$

当这 $n+2$ 位通过移位寄存器时，便依次产生以下状态：

$$0 \quad \underbrace{11 \cdots 1}_{n-1 \text{ 个 } 1} \quad \underbrace{11 \cdots 1}_{n \text{ 个 } 1} \quad \underbrace{11 \cdots 1}_{n-1 \text{ 个 } 1} \quad 0$$

定理2.7的证明 (续)

由于 $0 \underbrace{11 \dots 1}_{n-1 \text{ 个 } 1}$, $\underbrace{11 \dots 1}_{n-1 \text{ 个 } 1} 0$ 这两个状态只能各出现一次, 所以不会再有1的n-1游程。

0的n-1游程只有一个:

$$\underbrace{100 \dots 01}_{n-1 \text{ 个 } 0}$$

于是在一个周期内, 总游程数为

$$1 + 1 + \sum_{i=1}^{n-2} 2^{n-i-1} = 2^{n-1}$$

定理2.7的证明 (续)

③ $\{a_i\}$ 是周期为 2^n-1 的 m 序列, 对于任一正整数 $t(0 < t < 2^n-1)$, $\{a_i\} + \{a_{i+t}\}$ 在一个周期内为 0 的位数正好是序列 $\{a_i\}$ 和 $\{a_{i+t}\}$ 对应位相同的位数。设序列 $\{a_i\}$ 满足递推关系:

$$a_{h+n} = c_1 a_{h+n-1} \oplus c_2 a_{h+n-2} \oplus \cdots \oplus c_n a_h$$

$$\text{故 } a_{h+n+t} = c_1 a_{h+n+t-1} \oplus c_2 a_{h+n+t-2} \oplus \cdots \oplus c_n a_{h+t}$$

$$a_{h+n} \oplus a_{h+n+t} = c_1 (a_{h+n-1} \oplus a_{h+n+t-1}) \oplus c_2 (a_{h+n-2} \oplus a_{h+n+t-2}) \oplus \cdots \oplus c_n (a_h \oplus a_{h+t})$$

$$\text{令 } b_j = a_j \oplus a_{j+t}, \text{ 序列 } \{b_j\} \text{ 满足: } b_{h+n} = c_1 b_{h+n-1} \oplus c_2 b_{h+n-2} \oplus \cdots \oplus c_n b_h$$

因为对应同样的特征多项式, 所以 $\{b_i\}$ 也是 m 序列。

$$\text{所以 } R(t) = \sum_{k=1}^T (-1)^{a_k} (-1)^{a_{k+t}} = \sum_{k=1}^T (-1)^{b_k} = 2^{n-1} - 1 - 2^{n-1} = -1$$

现代密码学

m-序列的安全性

信息与软件工程学院

m-序列的安全性

- 寻找m序列的递推关系式。
 - 已知一段序列，如果知道其反馈多项式，就可以将其后的序列依次求出
 - 已知序列能否获得相应的反馈多项式(或线性递推式)呢？
 - 解方程方法——已知序列 $\{a_i\}$ 是由n级线性移存器产生的，并且知道 $\{a_i\}$ 的连续 $2n$ 位，可用解线性方程组的方法得到反馈多项式
 - 线性反馈移位寄存器综合解——Berlekamp-Massey算法

例1 设序列 $a = (01111000\dots)$ 是由4级线性移存器所产生序列的连续8个信号，求该移存器的线性递推式。

解：设该4级移存器的线性递推式为：

$$a_n = c_1 a_{n-1} \oplus c_2 a_{n-2} \oplus c_3 a_{n-3} \oplus c_4 a_{n-4} \quad (n \geq 4)$$

由于知道周期序列的连续8个信号，不妨设为开头的8个信号，即

$$a_0 a_1 a_2 a_3 a_4 a_5 a_6 a_7 = 01111000$$

当 $n=4$ 时，由递归式可得： $a_4 = c_1 a_3 \oplus c_2 a_2 \oplus c_3 a_1 \oplus c_4 a_0$

即：

$$c_1 \oplus c_2 \oplus c_3 = 1 \quad (1)$$

同理可得：

$$c_1 \oplus c_2 \oplus c_3 \oplus c_4 = 0 \quad (2)$$

$$c_2 \oplus c_3 \oplus c_4 = 0 \quad (3)$$

$$c_3 \oplus c_4 = 0 \quad (4)$$

解方程组得 $c_1 = 0, c_2 = 0, c_3 = 1, c_4 = 1$

故所求移存器递推式为：

$$a_n = a_{n-3} \oplus a_{n-4} \quad (n \geq 4)$$

例 设敌手得到密文串: **101101011110010**

和相应的明文串: **011001111111001**

因此, 可得相应的密钥流: **110100100001011**

进一步假定敌手还知道密钥流是使用5级线性反馈移位寄存器产生的, 那么敌手可分别用密钥流中的前10个比特建立如下方程

$$(a_6 \ a_7 \ a_8 \ a_9 \ a_{10}) = (c_5 \ c_4 \ c_3 \ c_2 \ c_1) \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_7 \\ a_4 & a_5 & a_6 & a_7 & a_8 \\ a_5 & a_6 & a_7 & a_8 & a_9 \end{pmatrix}$$



即

$$(0 \ 1 \ 0 \ 0 \ 0) = (c_5 \ c_4 \ c_3 \ c_2 \ c_1) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

而

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$



从而得到

$$(c_5 \ c_4 \ c_3 \ c_2 \ c_1) = (0 \ 1 \ 0 \ 0 \ 0) \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

所以

$$(c_5 \ c_4 \ c_3 \ c_2 \ c_1) = (1 \ 0 \ 0 \ 1 \ 0)$$

密钥流的递推关系为

$$a_{i+5} = c_5 a_i \oplus c_2 a_{i+3} = a_i \oplus a_{i+3}$$

A decorative graphic consisting of a series of horizontal blue lines of varying lengths, creating a stepped or staircase effect, is positioned in the top left corner.

第十三讲 m -序列的安全性

A vertical line with two white circles is positioned on the left side of the slide. The top circle is connected to a blue horizontal bar, and the bottom circle is connected to another blue horizontal bar. The line extends above the top circle and below the bottom circle.

解方程方法

线性反馈移位寄存器综合

线性综合解

设 $\underline{a} = (a_0, a_1, \dots, a_{N-1})$ 是 F_2 上的长度为 N 的序列，而

$f(x) = c_0 + c_1x + c_2x^2 + \dots + c_lx^l$ 是 F_2 上的多项式， $c_0=1$.

如果序列中的元素满足递推关系：

$$a_k = c_1a_{k-1} \oplus c_2a_{k-2} \oplus \dots \oplus c_la_{k-l}, k = l, l+1, \dots, N-1 \quad (2)$$

则称 $\langle f(x), l \rangle$ 产生二元序列 \underline{a} 。其中 $\langle f(x), l \rangle$ 表示以 $f(x)$ 为特征多项式的 l 级线性移位寄存器。

如果 $f(x)$ 是一个能产生 \underline{a} 并且级数最小的线性移位寄存器的特征多项式， l 是该寄存器的级数，则称 $\langle f(x), l \rangle$ 为序列 \underline{a} 的线性综合解。

线性移位寄存器的综合问题

线性移位寄存器的综合问题可表述为：给定一个 N 长二元序列 \underline{a} ，如何求出产生这一序列的最小级数的线性移位寄存器，即最短的线性移存器。

1、特征多项式 $f(x)$ 的次数 $\leq l$ 。因为产生 \underline{a} 且级数最小的线性移位寄存器可能是退化的，在这种情况下 $f(x)$ 的次数 $< l$ ；并且此时 $f(x)$ 中的 $c_l=0$ ，因此在特征多项式 $f(x)$ 中仅要求 $c_0=1$ ，但不要要求 $c_l=1$ 。

2、规定：0级线性移位寄存器是以 $f(x)=1$ 为特征多项式的线性移位寄存器，且 n 长($n=1, 2, \dots, N$)全零序列，仅由0级线性移位寄存器产生。事实上，以 $f(x)=1$ 为反馈特征多项式的递归关系式是： $a_k=0, k=0, 1, \dots, n-1$ 。因此，这一规定是合理的。

3、给定一个 N 长二元序列 \underline{a} ，求能产生 \underline{a} 并且级数最小的线性移位寄存器，就是求 \underline{a} 的线性综合解。利用B-M算法可以有效的求出。

Berlekamp-Massey算法 (B-M算法)

用归纳法求出一系列线性移位寄存器:

$$\langle f_n(x), l_n \rangle \quad \partial^0 f_n(x) \leq l_n, \quad n = 1, 2, \dots, N$$

每一个 $\langle f_n(x), l_n \rangle$ 都是产生序列 \mathbf{a} 的前 n 项的最短线性移位寄存器, 在 $\langle f_n(x), l_n \rangle$ 的基础上构造相应的 $\langle f_{n+1}(x), l_{n+1} \rangle$, 使得是 $\langle f_{n+1}(x), l_{n+1} \rangle$ 产生给定序列前 $n+1$ 项的最短移存器, 则最后得到的 $\langle f_N(x), l_N \rangle$ 就是产生给定 N 长二元序列 \mathbf{a} 的最短的线性移位寄存器。

B-M算法（续）

任意给定一个 N 长序列 $\underline{a} = (a_0, a_1, \dots, a_{N-1})$ ，按 n 归纳定义

$$\langle f_n(x), l_n \rangle \quad n = 0, 1, 2, \dots, N-1$$

1、取初始值： $f_0(x) = 1, \quad l_0 = 0$

2、设 $\langle f_0(x), l_0 \rangle, \langle f_1(x), l_1 \rangle, \dots, \langle f_n(x), l_n \rangle$ ($0 \leq n < N$) 均已求得，

且 $l_0 \leq l_1 \leq \dots \leq l_n$

记： $f_n(x) = c_0^{(n)} + c_1^{(n)}x + \dots + c_{l_n}^{(n)}x^{l_n}, c_0^{(n)} = 1$ ，再计算：

$$d_n = c_0^{(n)}a_n + c_1^{(n)}a_{n-1} + \dots + c_{l_n}^{(n)}a_{n-l_n}$$

称 d_n 为第 n 步差值。然后分两种情形讨论：

B-M算法（续）

（ i ） 若 $d_n = 0$ ，则令：

$$f_{n+1}(x) = f_n(x), \quad l_{n+1} = l_n。$$

（ ii ） 若 $d_n = 1$ ，则需区分以下两种情形：

① 当： $l_0 = l_1 = \cdots = l_n = 0$ 时，

$$\text{取： } f_{n+1}(x) = 1 + x^{n+1}, l_{n+1} = n + 1。$$

② 当有 \mathbf{m} ($0 \leq m < n$)，使： $l_m < l_{m+1} = l_{m+2} = \cdots = l_n$ 。

$$\text{便置： } f_{n+1}(x) = f_n(x) + x^{n-m} f_m(x), l_{n+1} = \max\{ l_n, n + 1 - l_n \}$$

最后得到的 $\langle f_N(x), l_N \rangle$ 便是产生序列 \underline{a} 的最短线性移位寄存器。



B-M算法举例

输入： $S^8=10101111$

n	d_n	f_n	L_n	m	f_m
0	1	1	0		
1	1	$1+x$	1	0	1
2	1	1	1	0	1
3	0	$1+x^2$	2		
4	0	$1+x^2$	2		
5	1	$1+x^2$	2	2	1
6	0	$1+x^2+x^3$	4		
7	1	$1+x^2+x^3$	4	5	$1+x^2$
8		$1+x^3+x^4$	4		

输出： $\langle 1+x^3+x^4, 4 \rangle$

$$f_n(x) = c_0^{(n)} + c_1^{(n)}x + \cdots + c_{l_n}^{(n)}x^{l_n}, c_0^{(n)} = 1,$$

$$d_n = c_0^{(n)}a_n + c_1^{(n)}a_{n-1} + \cdots + c_{l_n}^{(n)}a_{n-l_n}$$

(i) 若 $d_n=0$, 则令:

$$f_{n+1}(x) = f_n(x), \quad l_{n+1} = l_n.$$

(ii) 若 $d_n=1$, 则需区分以下两种情形:

① 当: $l_0 = l_1 = \cdots = l_n = 0$ 时,

$$\text{取: } f_{n+1}(x) = 1 + x^{n+1}, l_{n+1} = n + 1.$$

② 当有 m ($0 \leq m < n$), 使:

$$\text{③ } l_m < l_{m+1} = l_{m+2} = \cdots = l_n.$$

$$\text{便置: } f_{n+1}(x) = f_n(x) + x^{n-m}f_m(x), \\ l_{n+1} = \max\{ l_n, n + 1 - l_n \}$$



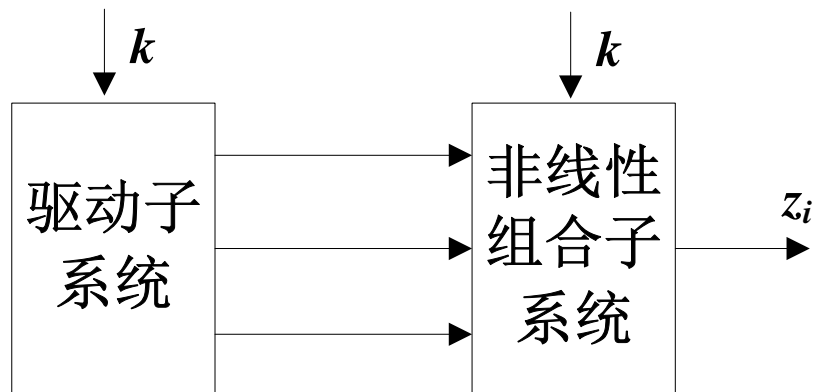
现代密码学

非线性序列

信息与软件工程学院

非线性序列

- 密钥流生成器可分解为驱动子系统和非线性组合子系统，如图所示

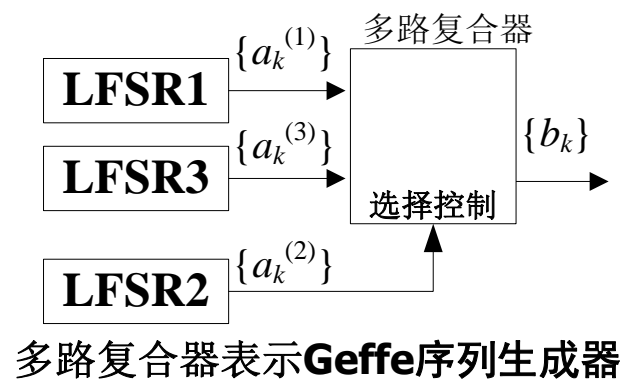
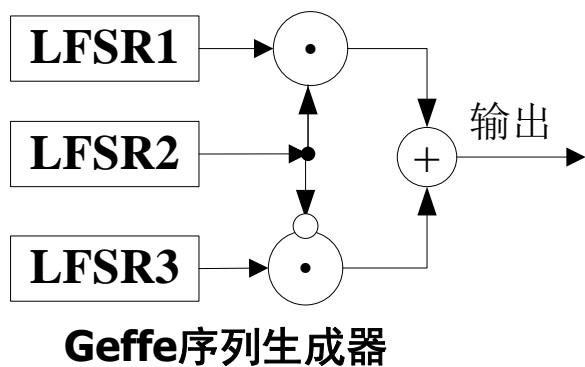


密钥流生成器的分解

- 驱动子系统常用一个或多个线性反馈移位寄存器来实现
- 非线性组合子系统用非线性组合函数 F 来实现
- 为了使密钥流生成器输出的二元序列尽可能复杂，也应保证其周期尽可能大、线性复杂度和不可预测性尽可能高

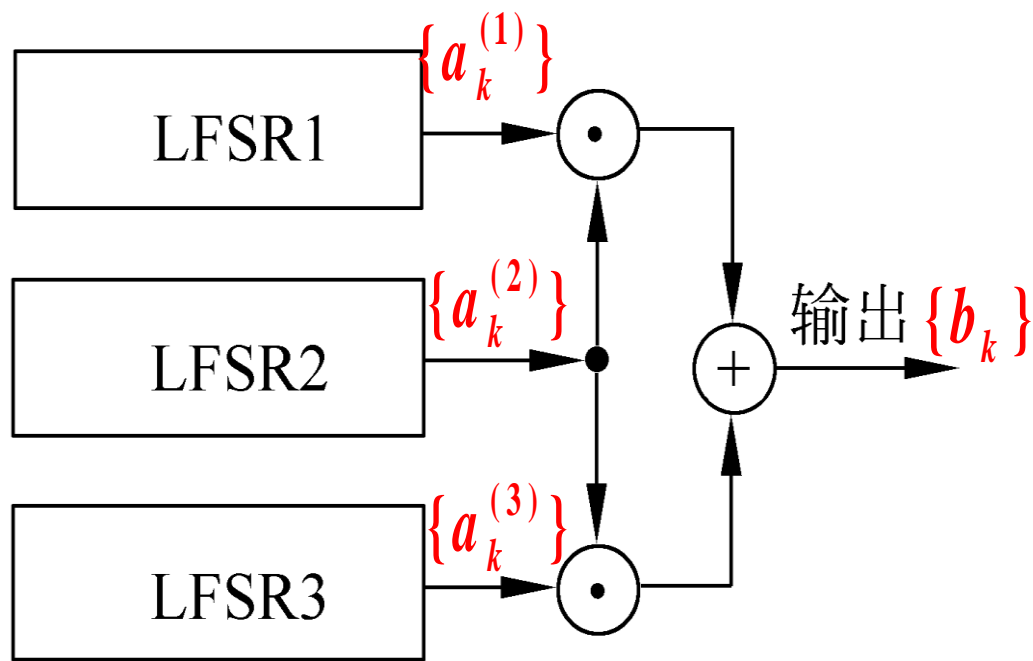
• Geffe序列生成器

- Geffe序列生成器由3个LFSR组成，其中LFSR2作为控制生成器使用，如图所示



- 当LFSR2输出1时，LFSR2与LFSR1相连接
- 当LFSR2输出0时，LFSR2与LFSR3相连接

Geffe序列生成器（续）



若设LFSR i 的输出序列为 $\{a_k^{(i)}\}$ ($i=1,2,3$),
则输出序列 $\{b_k\}$ 可以表示为

$$b_k = a_k^{(1)} a_k^{(2)} + a_k^{(3)} \overline{a_k^{(2)}} = a_k^{(1)} a_k^{(2)} + a_k^{(3)} a_k^{(2)} + a_k^{(3)}$$

设LFSR i 的特征多项式分别为 n_i 次本原多项式, 且 n_i **两两互素**

则Geffe序列的**周期**=
$$\prod_{i=1}^3 (2^{n_i} - 1)$$

Geffe序列的周期实现了**极大化**,
且**0**与**1**之间的分布大体上是**平衡**的。

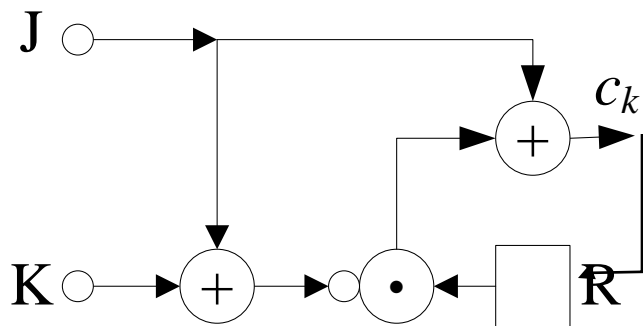
线性复杂度=
$$(n_1 + n_3) n_2 + n_3$$

J-K触发器

J-K触发器如图所示，它的两个输入端分别用J和K表示，其输出 c_k 不仅依赖于输入，还依赖于前一个输出位 c_{k-1} ，即

$$c_k = \overline{(x_1 + x_2)} c_{k-1} + x_1$$

其中 x_1 和 x_2 分别是J和K端的输入。由此可得J-K触发器的真值表，如下表所示

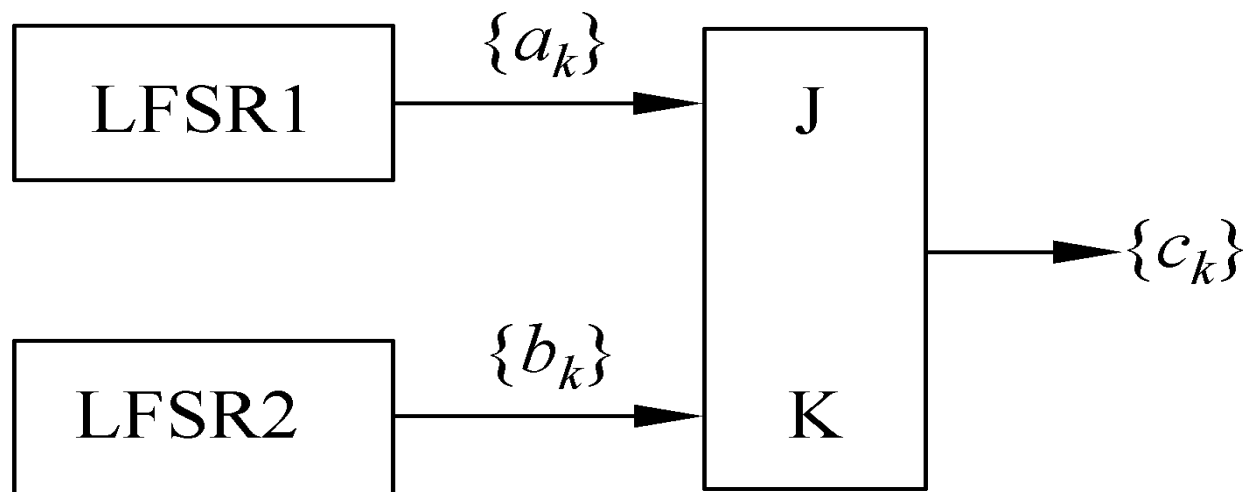


J-K触发器

J	K	c_k
0	0	c_{k-1}
0	1	0
1	0	1
1	1	$\overline{c_{k-1}}$

J-K触发器真值表

利用J-K触发器的非线性序列生成器



$\{a_k\}$: m级m序列

$\{b_k\}$: n级m序列

$$c_k = \overline{(a_k + b_k)} \quad c_{k-1} + a_k = (a_k + b_k + 1) \quad c_{k-1} + a_k$$

当m与n互素且 $a_0 + b_0 = 1$ 时，序列 $\{c_k\}$ 的周期为 $(2^m - 1)(2^n - 1)$ 。

利用J-K触发器的非线性序列生成器的实例

$$c_k = \overline{(a_k + b_k)} \quad c_{k-1} + a_k = (a_k + b_k + 1) \quad c_{k-1} + a_k$$

例2.7 令 $m=2, n=3$, 两个驱动 m 序列分别为

$$\{a_k\}=0,1,1,\dots$$

和

$$\{b_k\}=1,0,0,1,0,1,1,\dots$$

于是, 输出序列 $\{c_k\}$ 是 $0,1,1,0,1,0,0,1,1,1,0,1,0,1,0,0,1,0,0,1,0,\dots$,

其周期为 $(2^2-1)(2^3-1)=21$ 。

弱点

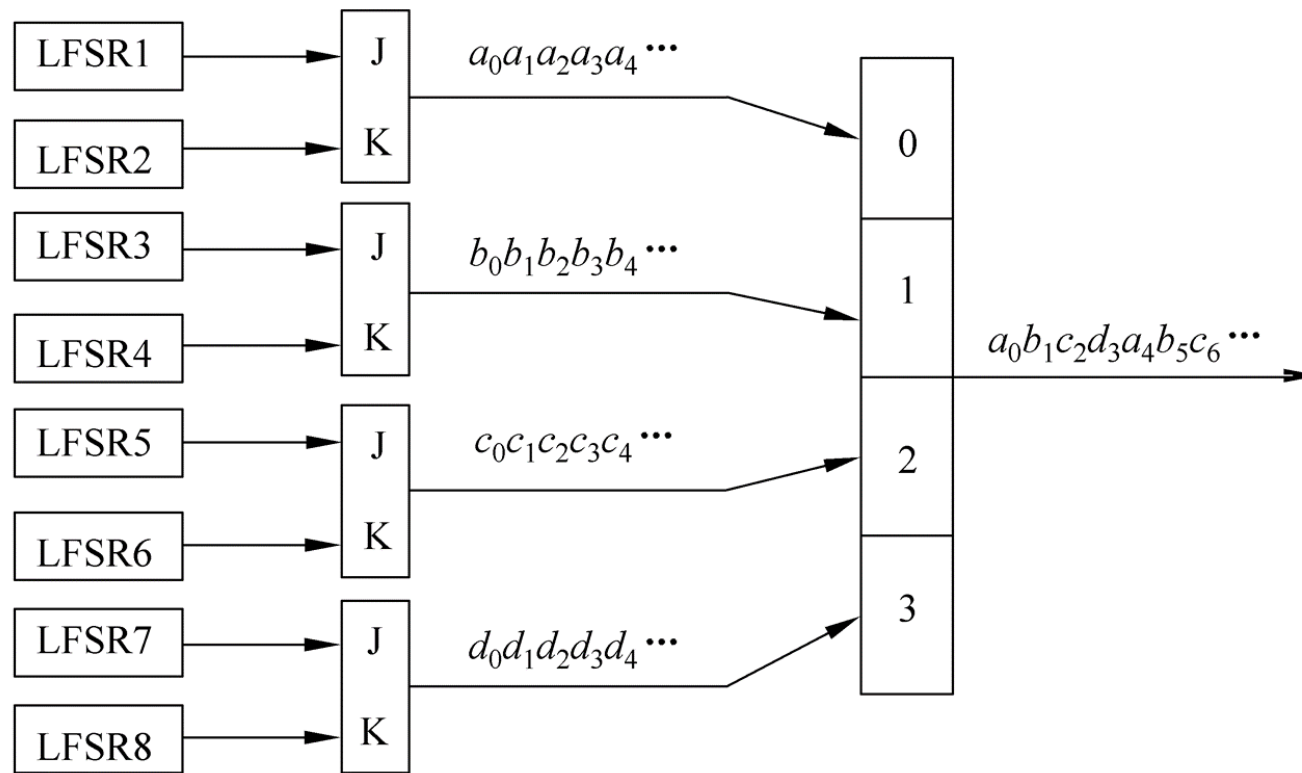
由 $c_k = (a_k + b_k + 1)c_{k-1} + a_k$ 可得

$$c_k = \begin{cases} a_k, & c_{k-1} = 0 \\ \overline{b_k}, & c_{k-1} = 1 \end{cases}$$

- 如果知道 $\{c_k\}$ 中相邻位的值 c_{k-1} 和 c_k ，就可以推断出 a_k 和 b_k 中的一个。而一旦知道足够多的这类信息，就可通过密码分析的方法得到序列 $\{a_k\}$ 和 $\{b_k\}$ 。
- 为了克服上述缺点，Pless 提出了由多个 J-K 触发器序列驱动的多路复合序列方案，称为 Pless 生成器。

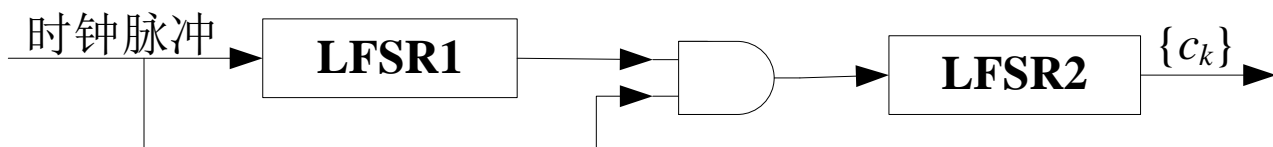
Pless生成器

Pless生成器由8个LFSR、4个J-K触发器和1个循环计数器构成，由循环计数器进行选通控制，如图所示。



钟控序列生成器模型

- 钟控序列最基本的模型是用一个LFSR控制另外一个LFSR的移位时钟脉冲，如图所示，一个最简单钟控序列生成器



- 假设LFSR1和LFSR2分别输出序列 $\{a_k\}$ 和 $\{b_k\}$ ，其周期分别为 p_1 和 p_2 。
- 当LFSR1输出1时，移位时钟脉冲通过与门使LFSR2进行一次移位，从而生成下一位。
- 当LFSR1输出0时，移位时钟脉冲无法通过与门影响LFSR2。因此LFSR2重复输出前一位。

钟控序列的周期

- 假设LFSR1和LFSR2分别输出序列 $\{a_k\}$ 和 $\{b_k\}$ ，其周期分别为 p_1 和 p_2 。假设钟控序列 $\{c_k\}$ 的周期为 p ，可得如下关系：

- $$p = \frac{p_1 p_2}{\gcd(w_1, p_2)}, \quad \text{其中 } w_1 = \sum_{i=0}^{p_1-1} a_i$$

- c_k 的一个周期至少是LFSR1和LFSR2同时回到初始状态的时刻
- 显然当运行 $p_1 \times p_2$ 个节拍后两个LFSR必然回到初态，因此周期至多是 $p_1 \times p_2$
- LFSR1运行一个周期，LFSR2运行 $w_1 = dt$ 拍， $d = \gcd(w_1, p_2)$
- 则LFSR1运行 (p_2/d) 个周期后，LFSR2刚好运行 $dt \times p_2/d = tp_2$ 拍，即 t 个周期，于是两个LFSR都回到初态，这时运行了 $(p_2/d) \times p_1$ 个节拍

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the section header.

钟控序列的周期（续）

- 若 $\{a_k\}$ 和 $\{b_k\}$ 的极小特征多项式分别为 $\text{GF}(2)$ 上的 m 和 n 次本原多项式 $f_1(x)$ 和 $f_2(x)$ ，且 $m|n$ 。
 - 则 $p_1=2^m-1$, $p_2=2^n-1$ 。
 - 而 w_1 为 $\{a_k\}$ 一个周期内 1 的个数，因此 $w_1=2^{m-1}$
 - 故 $\gcd(w_1, p_2)=1$ ，所以 $p=p_1p_2=(2^m-1)(2^n-1)$ 。
-

钟控序列的线性复杂度

- 可推导出 $\{c_k\}$ 的线性复杂度为 $n(2^m-1)$ ，极小特征多项式为 $f_2(x^{2^m-1})$
 - 其对应的LFSR2的抽头每隔周期 $p_1=2^m-1$ 一个，这样，参与运算的每个抽头对应的状态的节奏相同，从而相当于对LFSR2序列进行每 2^m-1 拍的抽样序列(不计由于LFSR1的0游程而产生的重复)，这个序列只是LFSR2的平移和按照LFSR1中的0游程进行迟延，而抽头应该与LFSR2的节奏一致，所以其极小多项式和线性复杂度如上

钟控序列的例子

- 例： 设LFSR1为3级m序列生成器，其特征多项式为 $f_1(x)=1+x+x^3$ 。设初态为 $a_0=a_1=a_2=1$ ，于是输出序列为 $\{a_k\}=1,1,1,0,1,0,0,\dots$
- 又设LFSR2为3级m序列生成器，且记其状态向量为 σ_k ，则在上图的构造下 σ_k 的变化情况如下：
 - $\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_3, \sigma_4, \sigma_4, \sigma_4,$
 - $\sigma_5, \sigma_6, \sigma_0, \sigma_0, \sigma_1, \sigma_1, \sigma_1,$
 - $\sigma_2, \sigma_3, \sigma_4, \sigma_4, \sigma_5, \sigma_5, \sigma_5,$
 - $\sigma_6, \sigma_0, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_2,$
 - $\sigma_0, \sigma_1, \sigma_2, \sigma_2, \sigma_3, \sigma_3, \sigma_3,$
 - $\sigma_4, \sigma_5, \sigma_6, \sigma_6, \sigma_0, \sigma_0, \dots$
- $\{c_k\}$ 的周期为 $(2^3-1)^2=49$ ，在它的的一个周期内，每个 σ_k 恰好出现7次

例（续）

- 设 $f_2(x)=1+x^2+x^3$ 为 LFSR2 的特征多项式，且初态为 $b_0=b_1=b_2=1$ ，则 $\{b_k\}=1,1,1,0,0,1,0,1,1,1\dots$

- 由 σ_k 的变化情况得 $\{c_k\}=1,1,1,0,0,0,0,0, 1,0,1,1,1,1,1, 1,0,0,0,1,1,1, 0,1,1,1,1,1,1, 0,0,1,1,0,0,0, 1,1,1,1,0,0,0, 0,1,0,0,1,1,\dots$

$\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_3, \sigma_4, \sigma_4, \sigma_4,$

- $\sigma_5, \sigma_6, \sigma_0, \sigma_0, \sigma_1, \sigma_1, \sigma_1,$

- $\sigma_2, \sigma_3, \sigma_4, \sigma_4, \sigma_5, \sigma_5, \sigma_5,$

- $\sigma_6, \sigma_0, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_2,$

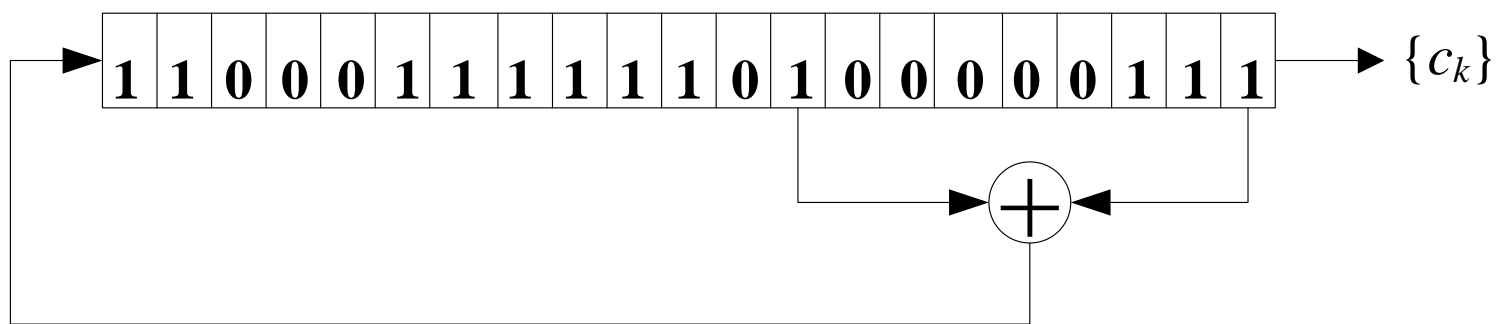
- $\sigma_0, \sigma_1, \sigma_2, \sigma_2, \sigma_3, \sigma_3, \sigma_3,$

- $\sigma_4, \sigma_5, \sigma_6, \sigma_6, \sigma_0, \sigma_0, \dots$

状态 (b_3, b_2, b_1)	输出
σ_0 1 1 1	1
σ_1 0 1 1	1
σ_2 0 0 1	1
σ_3 1 0 0	0
σ_4 0 1 0	0
σ_5 1 0 1	1
σ_6 1 1 0	0



- $\{c_k\}$ 的极小特征多项式为 $1+x^{14}+x^{21}$ ，其线性复杂度为 $3(2^3-1)=21$ ，下图是其线性等价生成器。





感谢聆听!

xynie@uestc.edu.cn
