现代密码学

第八讲 有限状态自动机

信息与软件工程学院

第八讲 有限状态自动机

- 有限状态自动机
- 密钥流生成器

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$S=\{ s_i \mid i=1,2,\ldots,l \}$。

② 有限输入字符集$A_1=\{ A^{(1)}_j \mid j=1,2,\ldots,m\}$和有限输出字符集

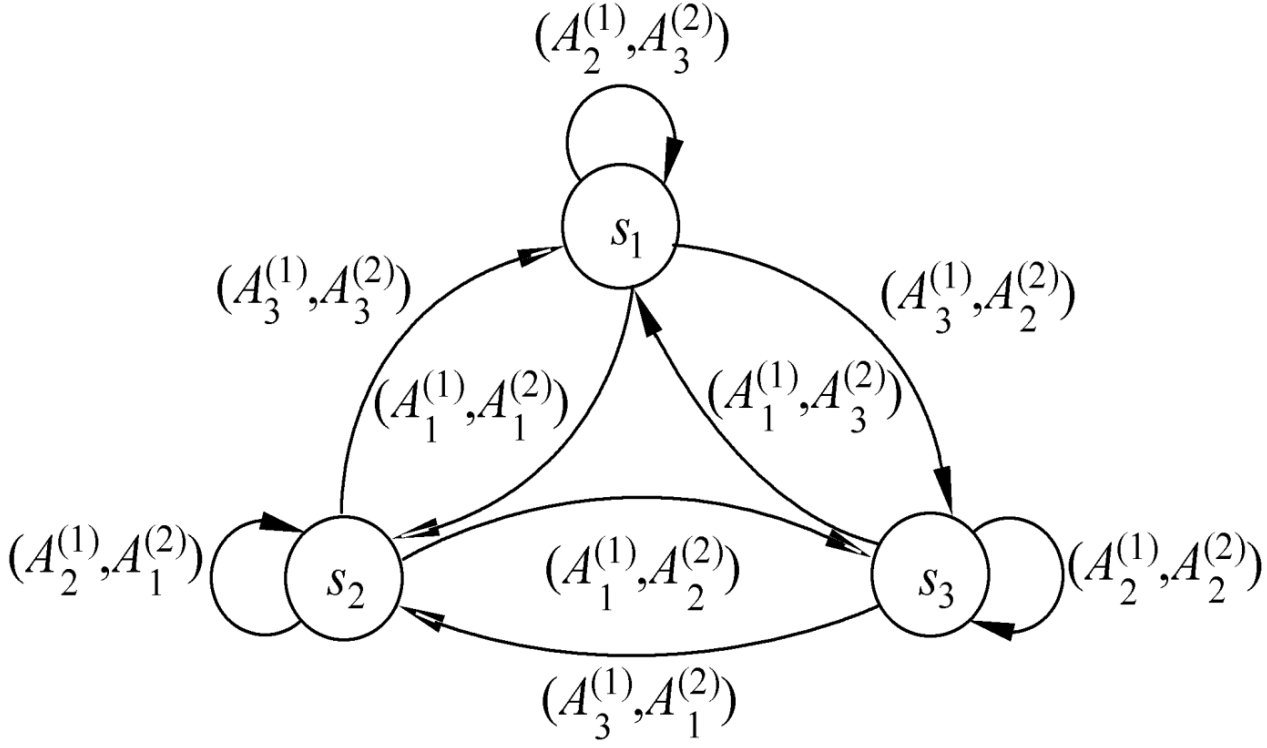
$$A_2=\{A^{(2)}_k \mid k=1,2,\ldots,n\}。$$

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

$A^{(1)}{}_1\ A^{(1)}{}_2\ A^{(1)}{}_1\ A^{(1)}{}_3\ A^{(1)}{}_3\ A^{(1)}{}_1$

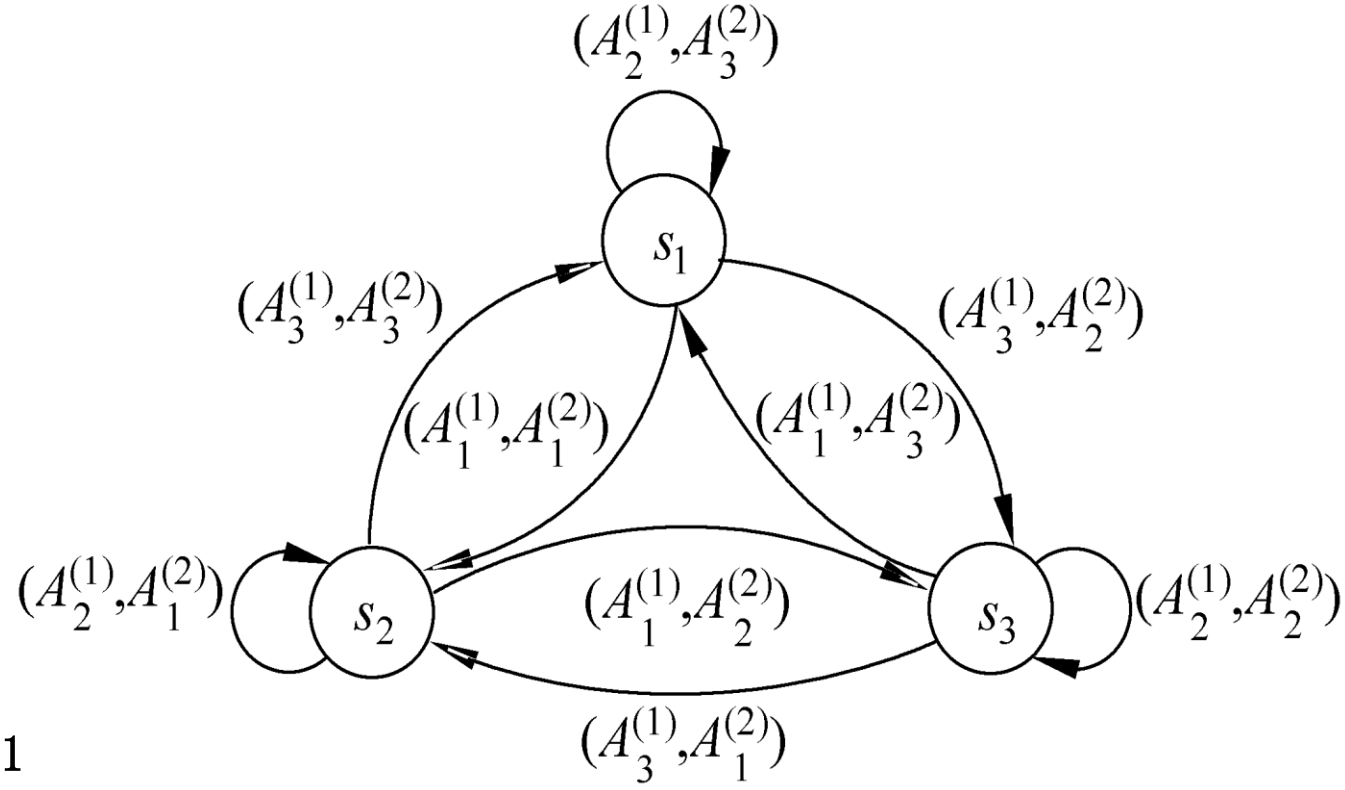
初始状态为s_1，

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

$A^{(2)}{}_1\ A^{(2)}{}_1\ A^{(2)}{}_2\ A^{(2)}{}_1\ A^{(2)}{}_3\ A^{(2)}{}_1$



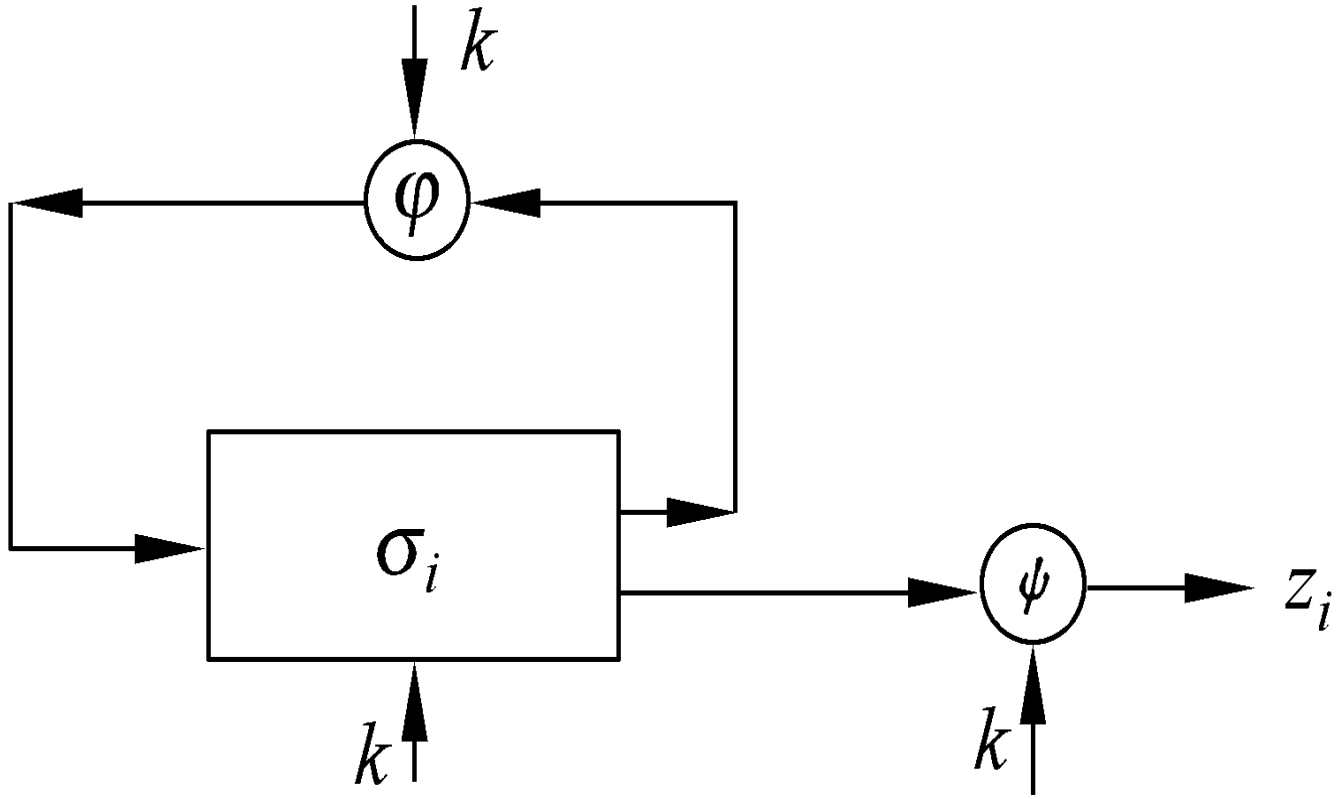
第八讲 有限状态自动机

- 有限状态自动机
- 密钥流生成器

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$\sum$、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$\sigma_i$变为一个新状态$\sigma_{i+1}$，
- 输出函数$\psi:\sigma_i \rightarrow z_i$，当前状态$\sigma_i$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



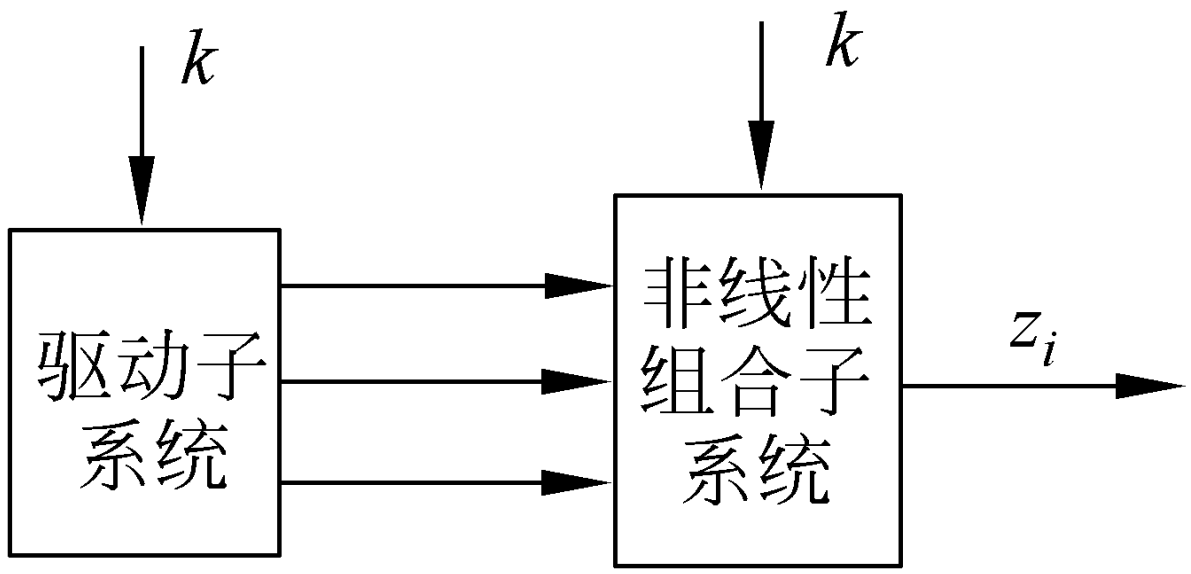
作为有限状态自动机的密钥流生成器

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，并且要求在设备上是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

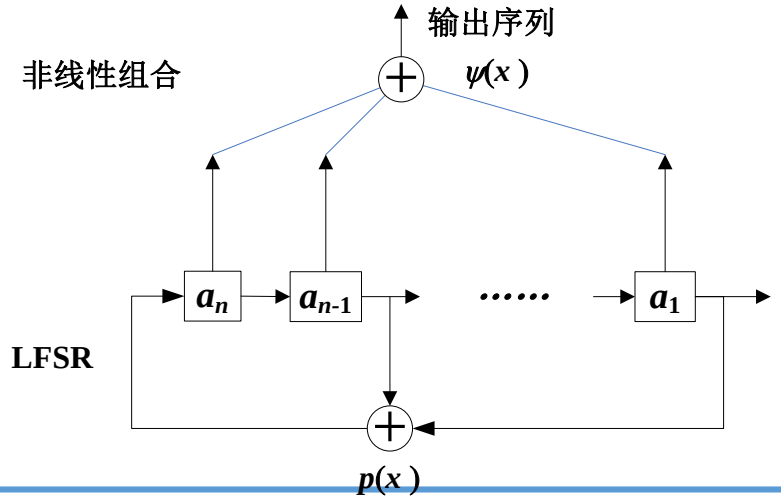
密钥流生成器的分解

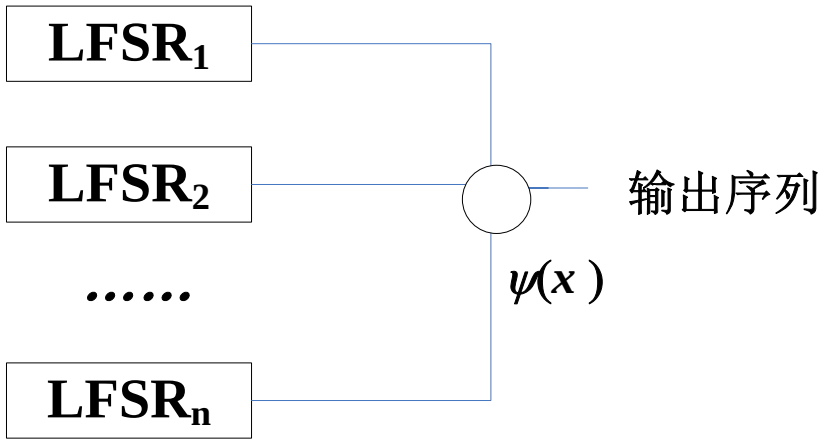
- 密钥流生成器可分成驱动部分和非线性组合部分
- 驱动部分控制生成器的状态转移，并为非线性组合部分提供统计性能好的序列
- 非线性组合部分要利用这些序列组合出满足要求的密钥流序列



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





感 谢 聆 听!

xynie@uestc.edu.cn