现代密码学

第十讲 线性反馈移位寄存器

信息与软件工程学院

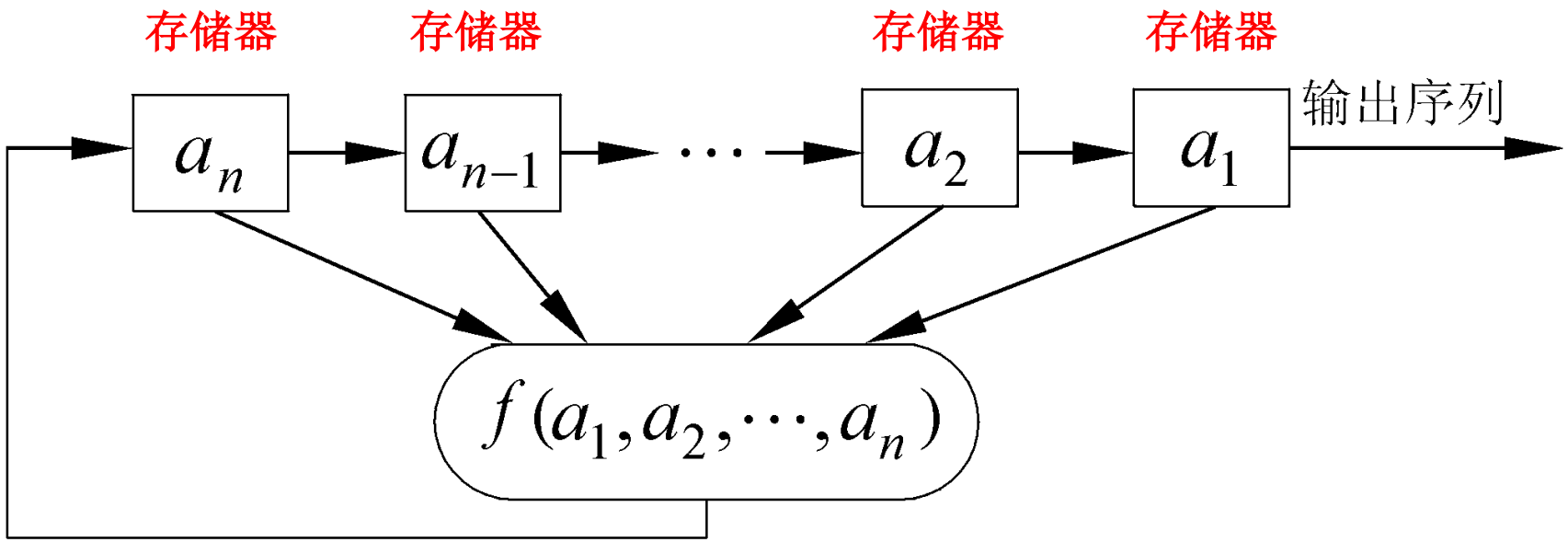
第十讲 线性反馈移位寄存器

- 反馈移位寄存器
- 线性反馈移位寄存器

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$f(a_1,a_2,\ldots,a_n)$组成，如下图所示。



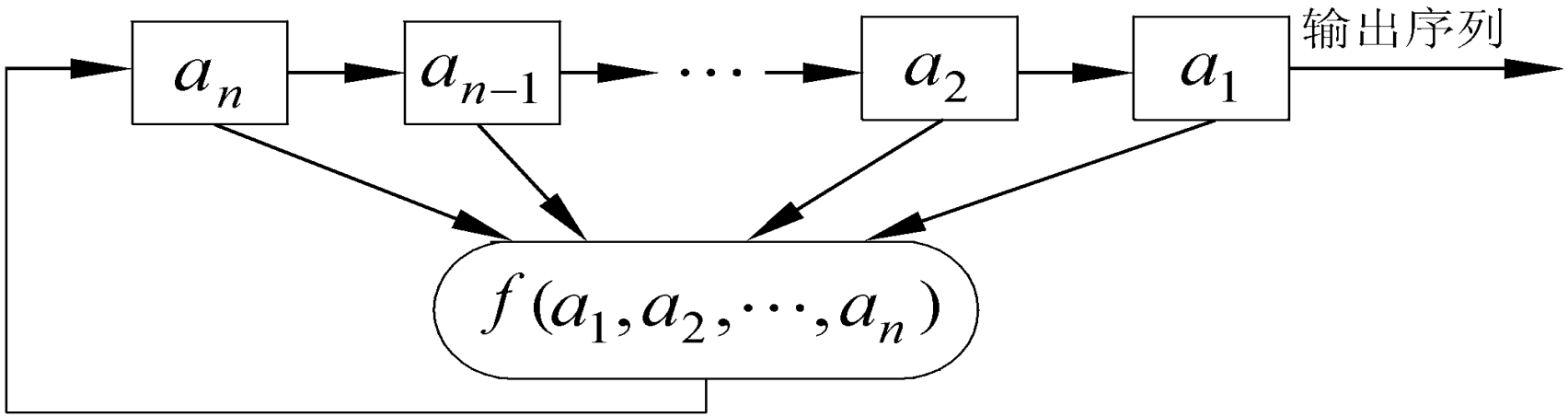
反馈移位寄存器的状态

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

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

表示，其中a_i是第i级存储器的内容。

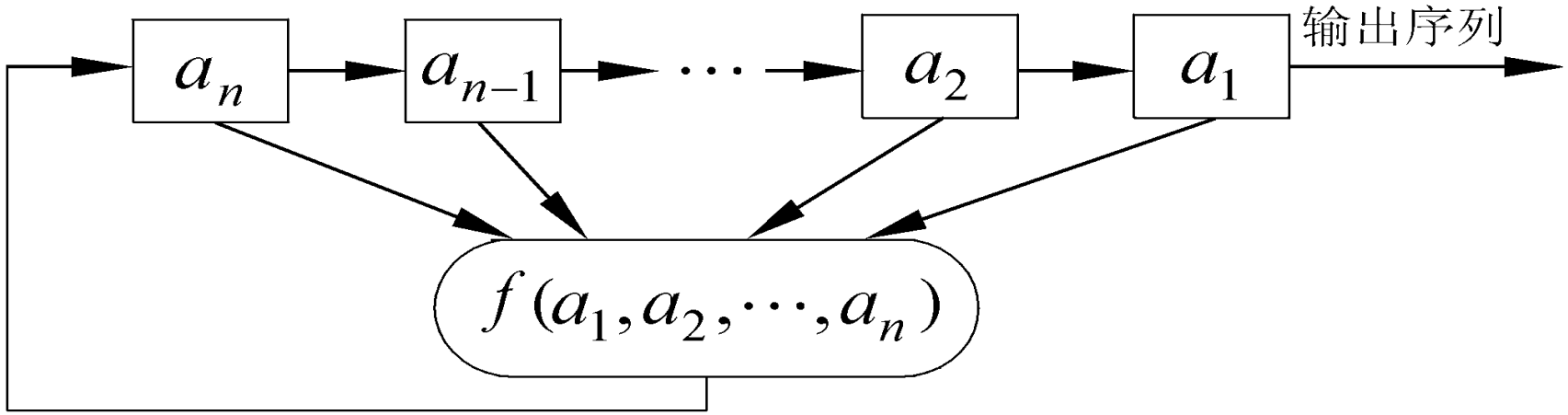


反馈函数

初始状态由用户确定。

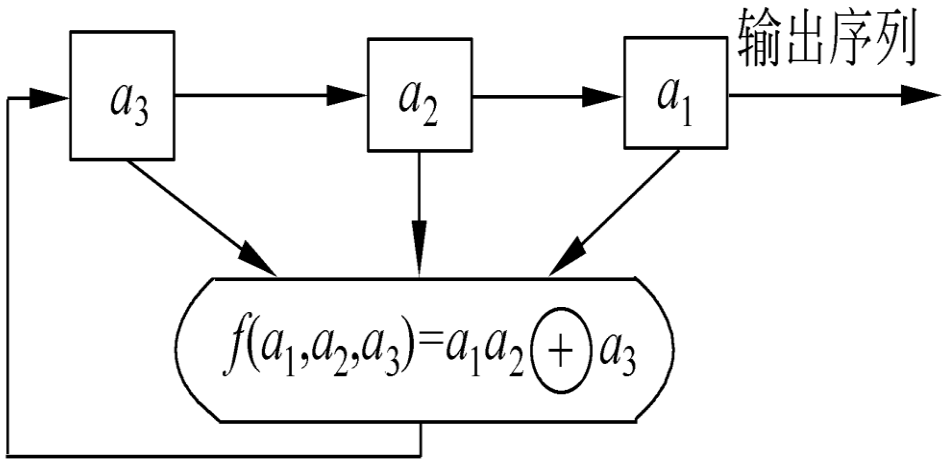
反馈函数$f(a_1,a_2,\ldots,a_n)$是n元布尔函数，即函数的自变量和因变量只取0和1这两个可能的值。

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$(a_1,a_2,a_3)=(1,0,1)$，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101110111011…，周期为4。

一个3级反馈移位寄存器的状态和输出

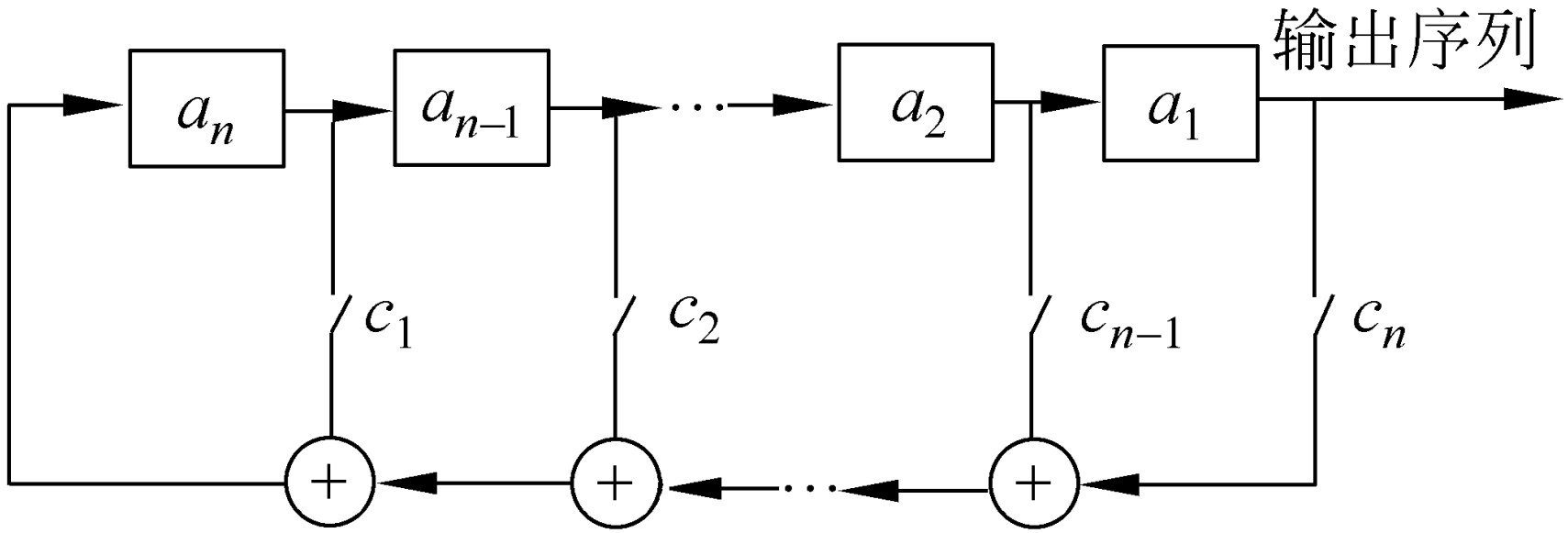
状态 (a_3,a_2,a_1)	输出
1 0 1	1
1 1 0	0
1 1 1	1
0 1 1	1
1 0 1	1
1 1 0	0

第十讲 线性反馈移位寄存器

- 反馈移位寄存器
- 线性反馈移位寄存器

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



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

LFSR的反馈函数

输出序列$\{a_t\}$满足：

$$f(a_1,a_2,\cdots,a_n)=c_1a_n\oplus c_2a_{n-1}\oplus\cdots\oplus c_na_1$$

$$a_{n+1}=c_1a_n\oplus c_2a_{n-1}\oplus\cdots\oplus c_na_1$$

$$a_{n+2}=c_1a_{n+1}\oplus c_2a_n\oplus\cdots\oplus c_na_2$$

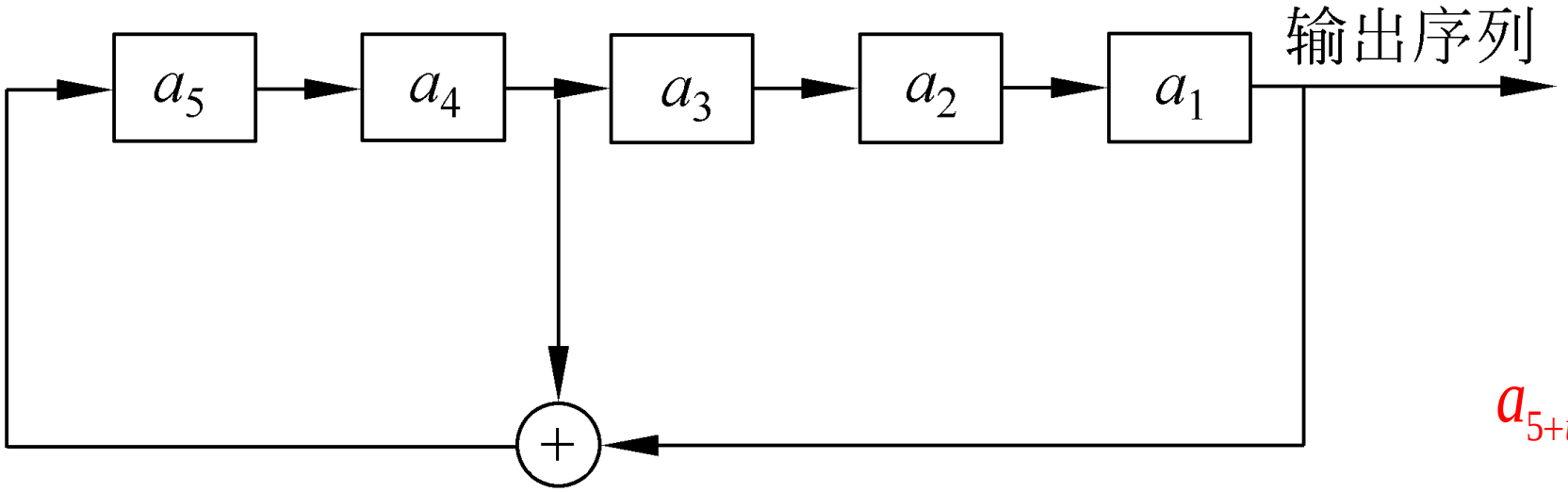
$$\cdots\cdots$$

$$a_{n+t}=c_1a_{n+t-1}\oplus c_2a_{n+t-2}\oplus\cdots\oplus c_na_t,t=1,2,\cdots$$

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最重要的部件之一。

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

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

可求出输出序列为

1001101001000010101110110001111100110…

周期为31。

密钥流的周期

- 给定密钥流 $\{a_i\}=a_1,a_2,a_3,\cdots,a_n,\cdots$ ，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$c_1, c_2, \ldots, c_n$中至少有一个不为0，否则$f(a_1, a_2, \ldots, a_n) \equiv 0$。

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。

感 谢 聆 听!

xynie@uestc.edu.cn