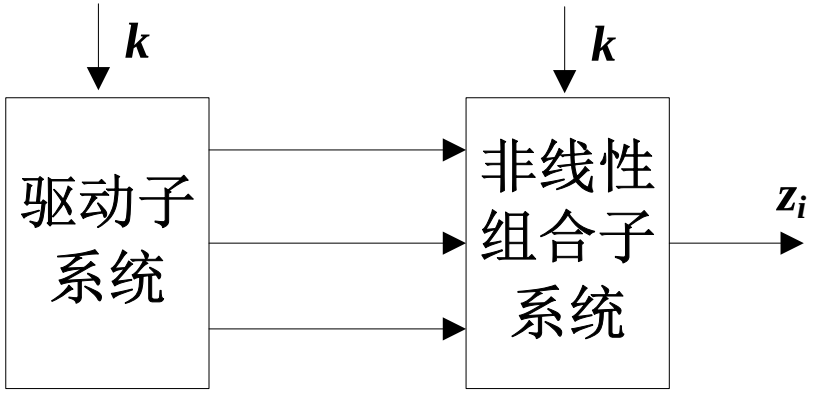
现代密码学

第十四讲 非线性序列1

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

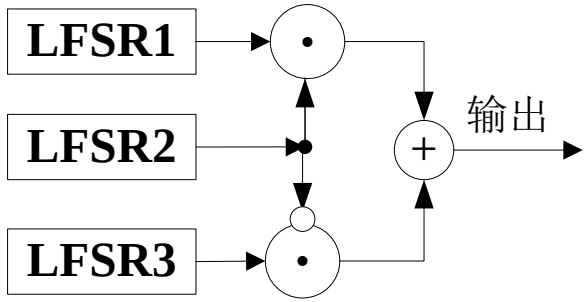
- 驱动子系统常用一个或多个线性反馈移位寄存器来实现
- 非线性组合子系统用非线性组合函数F来实现
- 为了使密钥流生成器输出的二元序列尽可能复杂，也应保证其周期尽可能大、线性复杂度和不可预测性尽可能高

第十四讲 非线性序列1

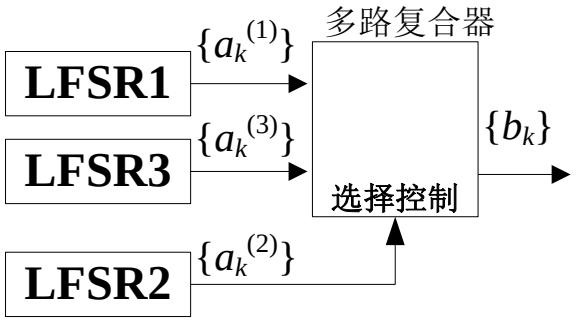
- Geffe序列生成器
- J-K触发器
- Pless生成器

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



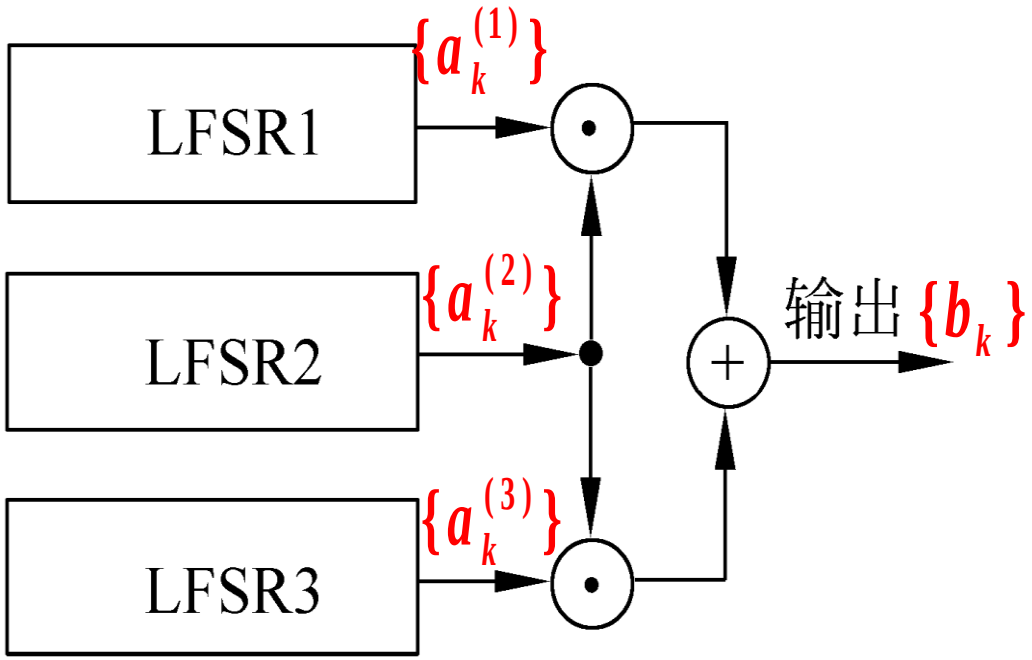
Geffe序列生成器



多路复合器表示Geffe序列生成器

- 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LFSRi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LFSRi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= $\prod_{i=1}^{3}\left(2^{n_i}-1\right)$

线性复杂度= $\left(n_1+n_3\right)n_2+n_3$

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。

第十四讲 非线性序列1

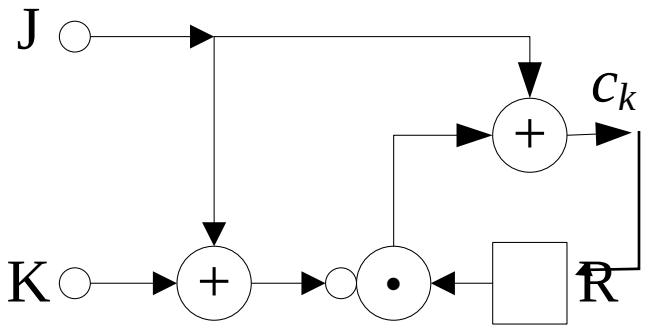
- Geffe序列生成器
- J-K触发器
- Pless生成器

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

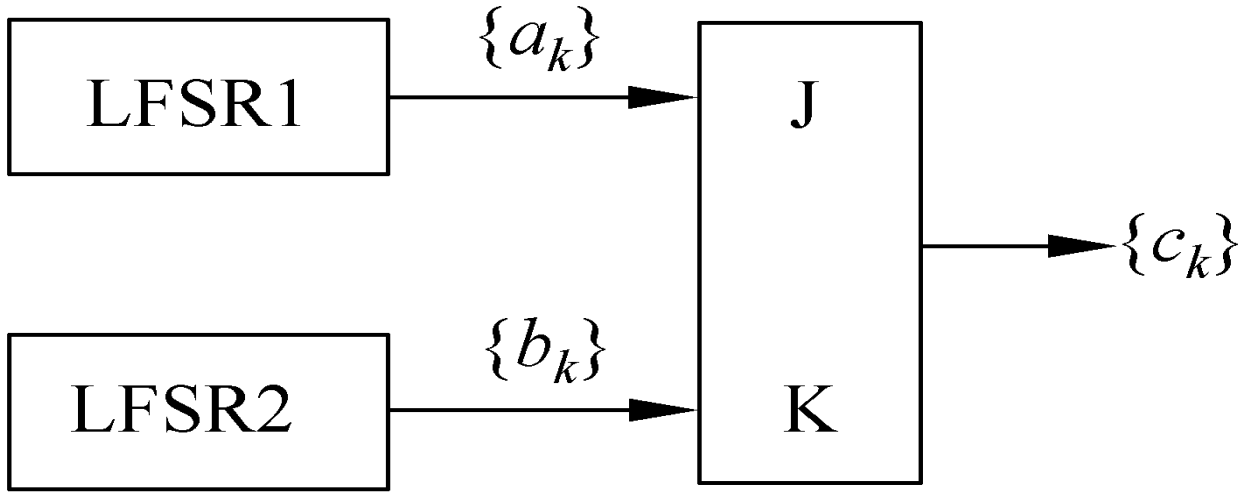


J-K触发器

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

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

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

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

例2.7 令m=2,n=3，两个驱动m序列分别为

$\{a_k\}$=0,1,1,…

和

$\{b_k\}$=1,0,0,1,0,1,1,…

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,…,

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

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

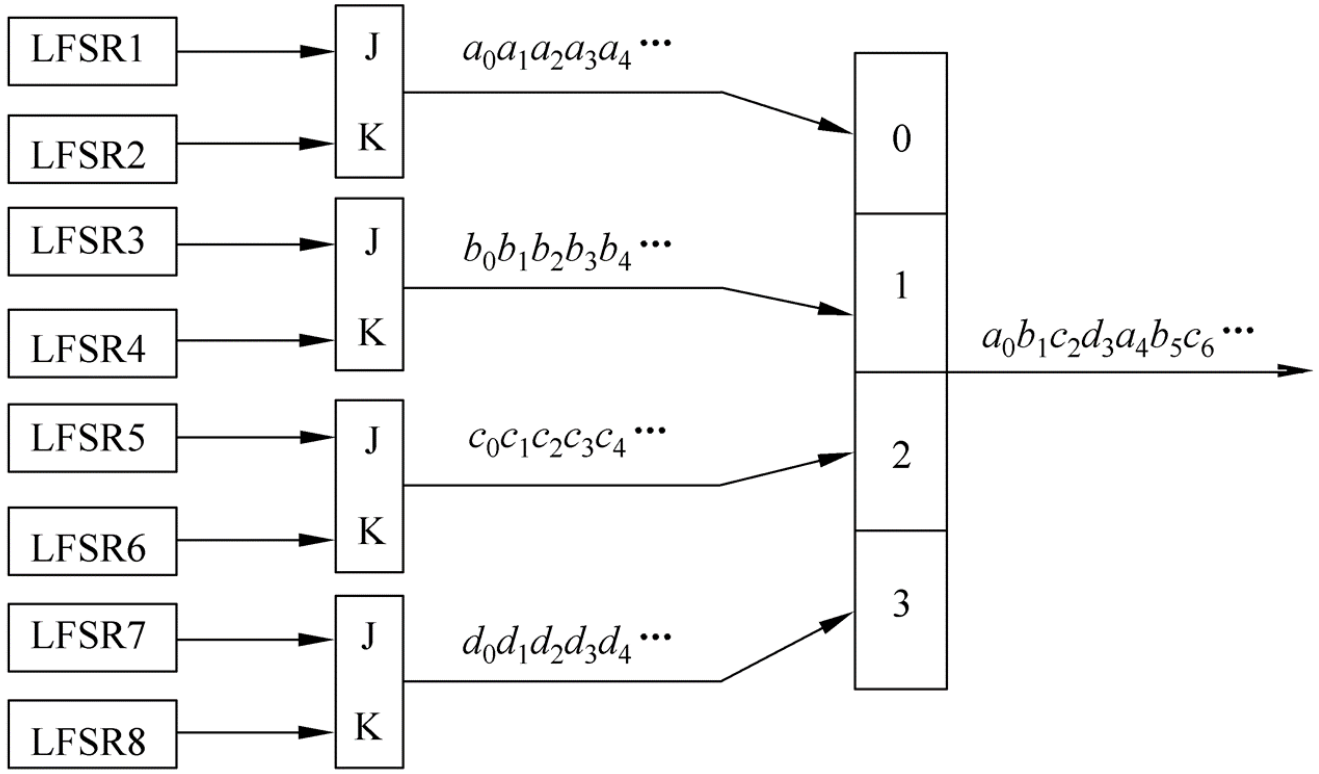
- 如果知道$\{c_k\}$中相邻位的值c_{k-1}和c_k，就可以推断出a_k和b_k中的一个。而一旦知道足够多的这类信息，就可通过密码分析的方法得到序列$\{a_k\}$和$\{b_k\}$。
- 为了克服上述缺点，Pless提出了由多个J-K触发器序列驱动的多路复合序列方案，称为Pless生成器。

第十四讲 非线性序列1

- Geffe序列生成器
- J-K触发器
- 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。



感 谢 聆 听!

xynie@uestc.edu.cn