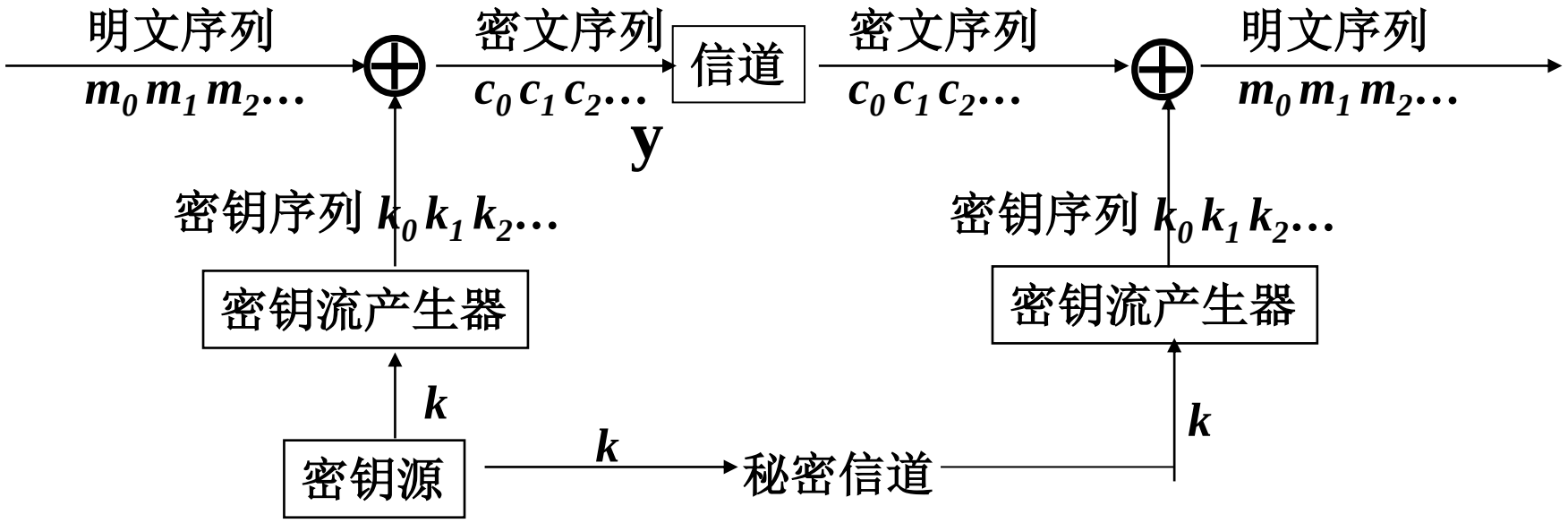
§3.1 序列密码

一种对称密码体制，是一种对明文消息字符逐位加密的私钥密码体制。序列密码的基本原理：



序列加密变换：$c_i = m_i \oplus k_i \pmod 2$，$i \geq 0$

序列解密变换：$m_i = c_i \oplus k_i \pmod 2$，$i \geq 0$

§3.1 序列密码

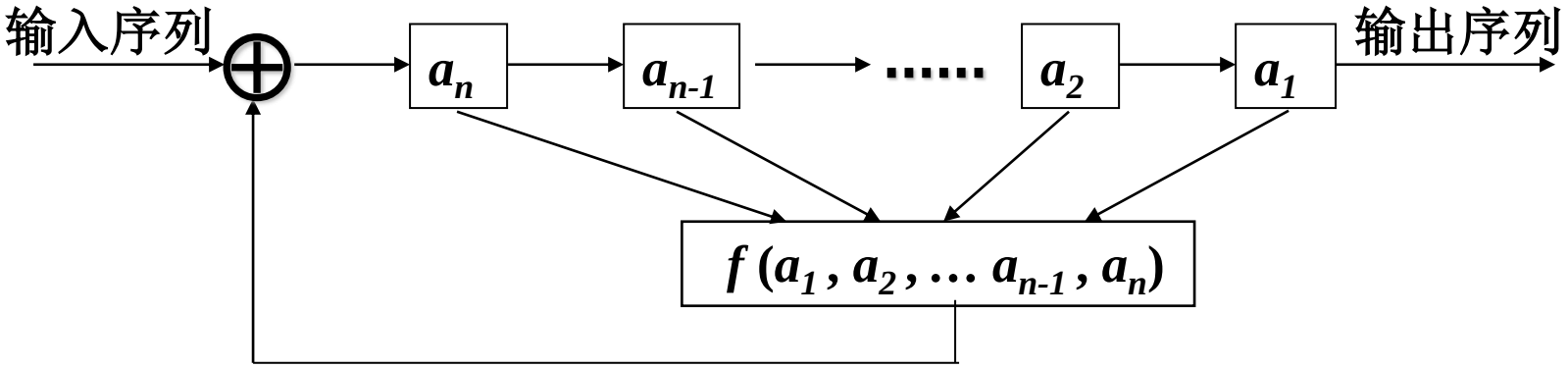
序列密码体制安全性取决于密钥序列，一个真正具有良好随机特性的密钥序列是设计序列密码的关键。实际操作中，序列密码是依靠一个短密钥（种子密钥）来产生一个长密钥序列，但此密钥序列不是真正的随机序列，我们称其为伪随机序列。

序列密码启蒙于“一次一密”的密码方案，其核心在于如何产生随机序列或伪随机序列。

密钥序列的产生主要是基于移位寄存器。

§3.1 序列密码

线性反馈移位寄存器序列的结构模型：



若t 时刻状态为$S_t=(a_t, a_{t+1}, \ldots, a_{t+n-1})$

则$t+1$ 时刻状态为$S_{t+1}=(a_{t+1}, a_{t+2}, \ldots, a_{t+n})$

其中$a_{t+n}= f(a_t, a_{t+1}, \ldots, a_{t+n-1})$

一般的线性反馈移位寄存器的反馈函数表示为：

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

其中c_i为0或1。

§3.1 序列密码

例：GF(2)上的4阶线性反馈移位寄存器的反馈函数为

$$f(a_1, a_2, a_3, a_4) = a_1 \oplus a_2$$

时刻t	状态 a_4	a_3	a_2	a_1	输出(k_i)	时刻t	状态 a_4	a_3	a_2	a_1	输出(k_i)
0	0	0	0	1	1	8	0	1	0	1	1
1	1	0	0	0	0	9	1	0	1	0	0
2	0	1	0	0	0	10	1	1	0	1	1
3	0	0	1	0	0	11	1	1	1	0	0
4	1	0	0	1	1	12	1	1	1	1	1
5	1	1	0	0	0	13	0	1	1	1	1
6	0	1	1	0	0	14	0	0	1	1	1
7	1	0	1	1	1	15	0	0	0	1	1

§3.1 序列密码

典型的序列密码算法：

- A5是用于GSM加密的序列密码，用于加密从电话到基站的连接，其他部分是不加密的，电话公司容易窃听用户会话。
- RC4是Ron Rivest在1987年为RSA数据安全公司开发的可变密钥长度的序列密码。