《密码学》课程习题

执笔 张焕国

第四章习题

1、设 $g(x)=x^4+x^3+1$，以其为连接多项式组成线性移位寄存器。画出逻辑图，写出输出序列及状态变迁。

2、设 $g(x)=x^4+x^3+x^2+x+1$，以其为连接多项式组成线性移位寄存器。画出逻辑图，写出输出序列及状态变迁。并分析与习题 1 的输出序列有什么不同？

3、令 $n=3$，$f(s_0,s_1,s_2)=s_0 \oplus s_2 \oplus 1 \oplus s_1 s_2$，以其为反馈函数构成非线性移位寄存器。求出非线性移位寄存器的状态变迁及输出。

4、令 $n=3$，$f(s_0,s_1,s_2)=1 \oplus s_0 \oplus s_1 \oplus s_2 \oplus s_0 s_1 \oplus s_1 s_2 \oplus s_2 s_3$，以其为反馈函数构成非线性移位寄存器。画出逻辑图，求出非线性移位寄存器的状态变迁及输出。

5、证明：GF（2）上的 n 级移位寄存器有 2^n 个状态，有种 2^{2^n} 不同的反馈函数，其中线性反馈函数只有 2^{n-1} 种，其余均为非线性反馈函数。

6、说明为什么在 A5 算法中每一时刻至少有两个 LSR 移位。

7、用 MCS-51 单片机实现有限状态自动机密码。

8、说明在 RC4 算法中 S 表初始化的作用。

9、令 n=3，仿照 RC4 设计构造一个类似的密码，并手工演算其加解密过程。

10、编程实现 RC4 密码。