《密码学》课程设计实验报告

实验序号：05　　实验项目名称：序列密码

学　　号		姓　　名		专业、班	18信安3-4班
实验地点	网安基地新珈楼B308	指导教师	王张宜	时间	2020.12.01

一、　实验目的及要求

教学目的：

(1) 掌握序列密码的基本概念；

(2) 掌握线性移位寄存器的结构及其序列的伪随机性；

(3) 熟悉非线性序列的概念与基本产生方法；

(4) 了解常用伪随机性评价方法；

(5) 掌握一种典型流密码（如RC4或ZUC等）。

实验要求：

(1) 掌握序列密码的实现方案；

(2) 掌握线性移位寄存器的构造；

(3) 熟悉序列伪随机性的基本测试方法；

(4) 实现RC4或ZUC算法。

二、实验设备（环境）及要求

Windows操作系统，高级语言开发环境

三、实验内容与步骤

1．序列密码的实现方案

（1）种子密钥K输入到密钥流发生器；

（2）产生一系列密钥流；

（3）通过与同一时刻的一个字节或者一位明文流进行异或操作产生密文流。

2．线性移位寄存器的构造

（1）选择连接多项式（一般选择本原多项式作为连接多项式）

（2）根据连接多项式的反馈系数得出反馈函数

（3）根据反馈函数得出每个节拍的寄存器状态

（必做题：实验 1-5）

实验（1）使用本原多项式 $g_1(x)=x^4+x+1$ 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。

实验（2）使用本原多项式 $g_2(x)=x^4+x^3+1$ 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。

试对比以上两组输出序列的关系。

提示：（1）与（2）中的多项式是互反多项式，所谓互反多项式是指 f(x)与 $x^n f\left(\frac{1}{x}\right)$

实验（3）使用多项式 $g(x)=x^4+x^3+x^2+x+1$ 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（1）、（2）的输出序列有什么不同？

提示：上述多项式是不可约多项式，但不是本原多项式

分别采用初值 1111、1000、0010 穷举状态变迁。

3．非线性移位寄存器

实验（4）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。画出逻辑图，求出非线性移位寄存器的状态变迁及输出。

实验（5）令 n =3，$f(s_0,s_1,s_2)=1\oplus s_0\oplus s_1\oplus s_2\oplus s_0s_1\oplus s_1 s_2\oplus s_2 s_0$ ，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。

4. 随机性测试（选作）

Golomb 随机性假设测试准则

准则 1（频率测试）：在 S 的周期 SN 中，1 的个数与 0 的个数至多相差 1。

准则 2（游程测试）：在 S 的周期 SN 中，至少有 1/2 的游程长度为 1，至少有 1/4 的游程长度为 2，至少有 1/8 的游程长度为 3，以此类推，并且 0 和 1 游程的个数近似相等。

准则 3（自相关测试）：自相关函数 R(t)是双值的。即对某个整数 K，有：

$$N\cdot R(t)=\sum_{i=0}^{N-1}(2s_i-1)(2s_{i+t}-1)=\begin{cases}N, t=0\\ K, 1\le t\le N-1\end{cases}$$

对于实验（1）-（5）产生的随机序列进行上述测试。

5. 编程实现 RC4、A5、ZUC 算法（选作）

6. 思考与扩展阅读（选作）

（1）定理：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；

（2）定理：GF（2）上的 n 级移位寄存器中线性反馈函数只有 2^{n-1} 种；

（3）定理：n 次本原多项式的个数是 $[\phi(2^n-1)]/n$，其中 ϕ 是欧拉函数；（欧拉函数：小于或等于 x 的数中与 x 互质的数的数目）

例如对于 n=4，$[\phi(2^4-1)]/4=[\phi(15)]/4=2$，因此对于 4 元的线性移位寄存器，只有 2 个 LFSR 可以生成 m 序列，即实验（1）和（2）

（4）在实际的序列密码设计中，人们往往选择项数较少的本原多项式构造 LFSR，例如三项式或五项式。试分析选择的原因。

（5）本原多项式一定是不可约多项式；反之则不一定成立。

例如 GF（2）上的 1-4 元不可约多项式有（黄色标注的是本原多项式，互反多项式略去）：

n=1 时，x、x+1

n=2 时，x^2+x+1

n=3 时，x^3+x+1

n=4 时，x^4+x+1、$x^4+x^3+x^2+x+1$（T=5）

为了书写简便，5-8 元不可约多项式写成系数的形式，如 111 代表 x^2+x+1

n=5 时，100101、101111、110111

n=6 时，1000011、1001001（T=9）、1010111（T=21）、1011011、1100111

n=7 时，10000011、10001001、10001111、10011101、10100111、10101011、10111111、11001011、11101111

n=8 时，100011011（T=51）、100011101、100101011、100101101。。。。。

（6）常用的判定 GF（2）上的不可约多项式的方法：

（a）如果 f(x)的常数项为 0，除 f(x)=x 之外，f(x)一定可约；

（b）如果 f(x)的项数为偶数，除 f(x)=x+1 之外，f(x)一定可约；

（c）如果 f(x)中各项的 x 的幂次都是 2 的倍数，f(x)一定可约；

（d）如果 gcd（f(x), f’(x)）≠1，f(x)一定可约；

（e）如果 f(x+1)可约，f(x)一定可约；

（f）如果 $x^n f\left(\frac{1}{x}\right)$ 可约，f(x)一定可约；等等。。。。。

（7）密码设计的初步尝试：

（a）设计 AES 类的 S 盒

选择不同的不可约多项式，按照 AES S 盒的相同计算过程即可

（b）生成 m 序列

选择不同的本原多项式，按照 LFSR 的构造过程即可。

四、实验结果与数据处理

五、分析与讨论

六、教师评语

签名：

日期：

成绩