## 密码分析学

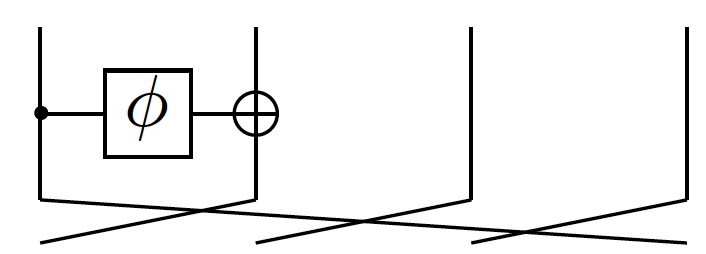
第4次作业：

1）根据课上介绍的方法，对5轮CipherFour（注意，课上是CIPHERD算法）算法进行线性分析。（明密文对应关系同作业二的txt文件，该文件依次列出了明文从0开始对应的密文取值）。

提交资料：线性分析过程说明文档，包含S盒线性近似表，每轮线性特征，偏差，攻击采用的线性壳轮数及概率*p*，密钥恢复攻击过程及数据（分别测试已知2|p-1/2|-2、8|p-1/2|-2个明密文时可恢复的密钥集合）；代码。

2）找出如下图所示的非平衡Feistel结构的最长轮数的零相关线性壳，其中函数可逆。

提交资料：结果及理由说明文档。



3）提交日期：2021-11-19

提交资料：实验报告+可读性较好的程序源代码

提交邮箱：mimafenxixue2021@163.com

要求同作业一。