## 密码分析学

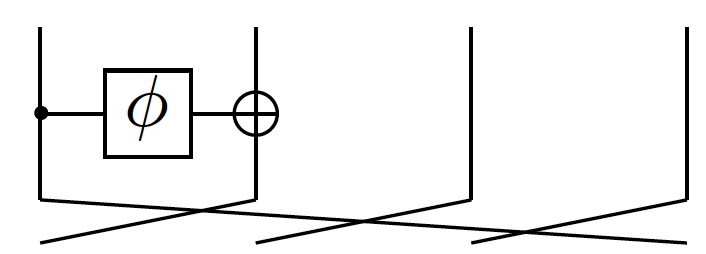
第4次作业：

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三的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）**选做**：仿照不可能差分的自动化搜索技术，结合线性掩码传播规则和相关度为零的充分条件，设计并实现零相关线性壳的自动化搜索算法，并对2）进行验证。

提交资料：自动化搜索算法设计文档+代码。

4）提交日期：2020-11-18，做完后请尽快提交，**同等结果下优先选择提交日期早的小组**。

12周（**11月24日**）择优进行课上演示。