

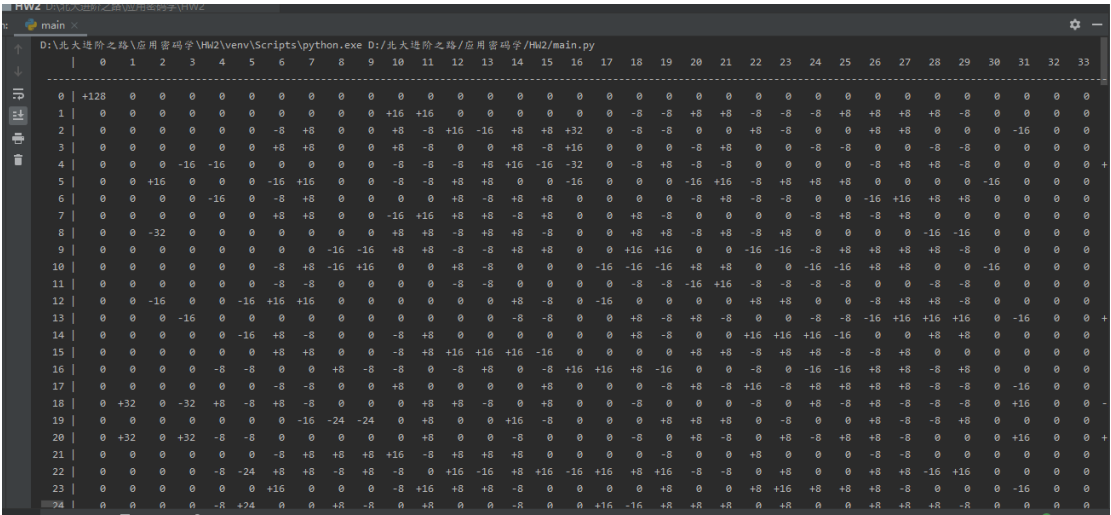
# 密码学第三次作业

## 输出 ZUC 加密算法的线性分析表：

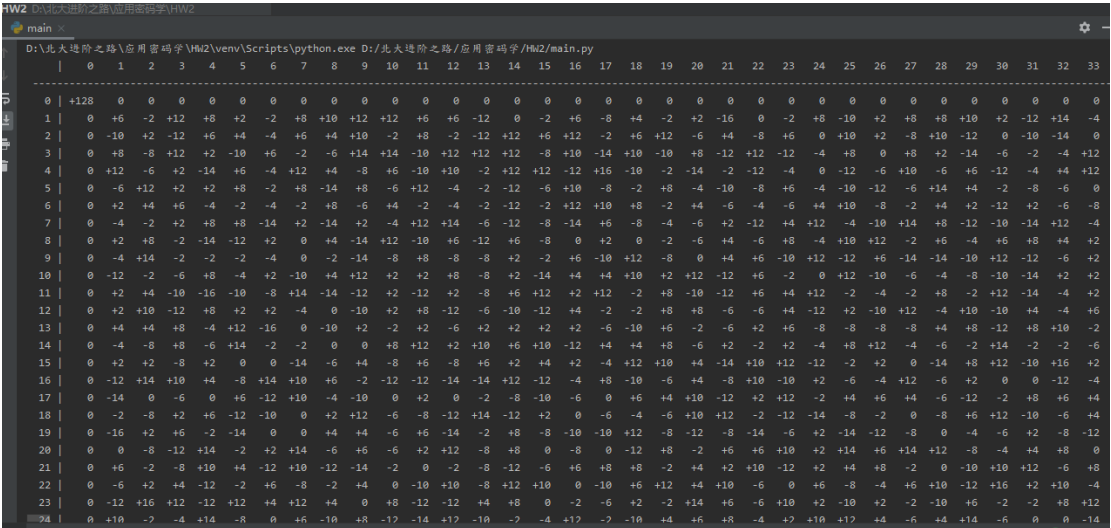
线性分析表的原理：在一个分布均匀的情况下，每一组明-密文对在表中应该是分布均匀的，即概率都为  $1/2$ ，而实际上 S 盒的变换中，并不能使明-密文呈现均匀的分布。线性分析表则是记录每一个明-密文对在 S 盒的变换中关于  $1/2$  的偏差值的一个表。

ZUC 算法又称为祖冲之算法，他是一个面向字的流式加密算法，每一轮中有 4 个 S 盒进行加密：S0,S1,S2,S3。其中 S0=S2,S1=S3。每一个 S 盒一次可以对 16 位的数据进行加密，故每一个 S 盒的对应一个  $256 \times 256$  的线性分析表

S0-box 的线性分析表部分截图如下：



S1-box 的线性分析表部分截图如下：



输出 ZUC 加密算法的差分分析表:

差分分析表的原理：在一个分布均匀的情况下，我们将具有相同异或值的输入对中的输入值分别通过 S 盒进行加密得到两个输出值，这两个输出值的异或值应该均匀的分布在各种取值。而差分分析表就是为了通过记录这些输出值的分布情况对密码进行差分分析而存在的。

这些输出异或分布,引入如下定义。对  $m$  长的比特串  $x'$  和  $n$  长的比特串  $y'$ ,定义:

$$N_n(x', \gamma') = |\{(x, x^*) \in \Delta(x') : \pi_S(x) \oplus \pi_S(x^*) = \gamma'\}|$$

换言之,  $N_p(x', y')$  记下了输入异或等于  $x'$ , 输出异或等于  $y'$  的对数 (对某一给定的 S 盒)。图

由上一个实验可知，ZUC 加密算法的每一个 S 盒对应的差分分析表都是一个 256\*256 的表格。

S0-box 的差分分析表部分截图如下:

[illegible]

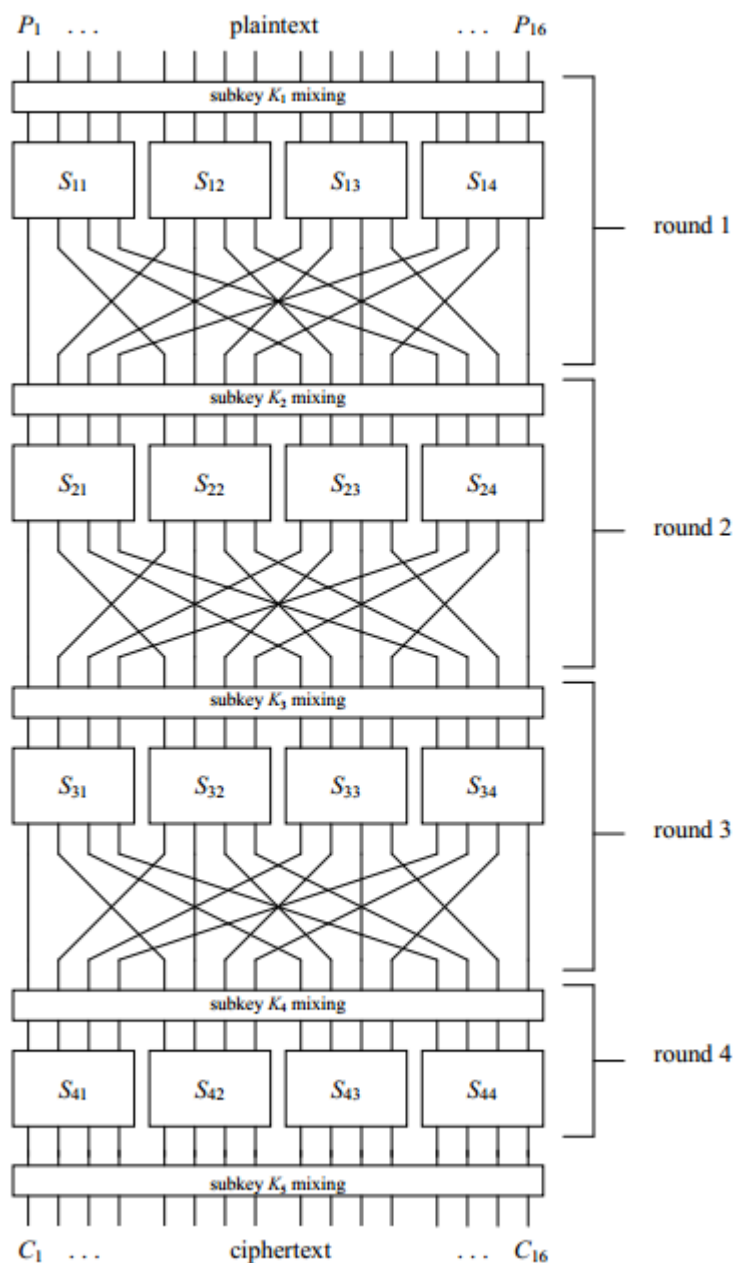
S1-box 的差分分析表部分截图如下:

[illegible]

简答题：

- Answer why a final key mixing is required by a cipher (you can take Basic SPN as an example) ?

答：



图中为我们展示的是一

个基本的 SPN 结构，可以看出每一轮中都含有 key-mixing（轮密钥加）、permutation（置换）、substitution（代替）三个步骤，而且每一轮中的步骤都有相同的先后顺序，依次是 key-mixing、permutation、substitution。除此之外，在末轮结束以后还额外加上了一轮的 key-mixing。从我们对于密码线性分析以及密码差分分析的学习我们可以发现，如果缺少了最后

一轮的轮密钥加密，我们就可以通过线性分析或是差分分析的方式，以较大的成功率，从密文推出倒数第二轮的内容。

**结论：**末轮的轮密钥加可以更加有效的抵御密码分析攻击。