# 第三次作业

## 设计思路

### 差分密码分析

差分密码分析是迄今已知的攻击迭代密码最有效的方法之一，其基本思想实：通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特。

ZUC算法的S-Box 是8 × 8 的 输入，所以x 和 y的差分取值在[0, 255]区间。DDT的计算用python3实现，如下所示：

SBOX to DDT

for p1 in range(256)

for p2 in range(256)

XOR\_IN = p1 ^ p2

XOR\_OUT = sbox[p1] ^ sbox[p2]

DDT[XOR\_IN][XOR\_OUT] += 1

### 线性密码分析

线性密码分析是对迭代密码的一种已知明文攻击，它利用的是密码算法中的”不平衡（有效）的线性逼近“。

ZUC算法的S-Box 是8 × 8 的 输入，所以x 和 y的差分取值在[0, 255]区间。LAT的计算用python3实现，如下所示：

SBOX to LAT

for a in range(256)

for b in range(256)

for i in range(256)

LAT[a][b] += a.i ^ b.sbox\_val[i]

LAT[a][b]=256-LAT[a][b] LAT[a][b] = LAT[a][b] - 128

## 实验结果

S0 DDT在当前目录ZUC\_S0\_LAT.txt里。

S1 DDT在当前目录ZUC\_S1\_DDT.txt里。

S0 LAT在当前目录ZUC\_S0\_LAT.txt里。

S1 LAT在当前目录ZUC\_S1\_LAT.txt里。

## 为什么加密最后一轮key mixing,substition后不是用permutation而是再用一次key mixing?

Permutation不安全，攻击者不需要密钥也能能够还原它一轮，降低了密码破解的复杂度。