DDT 和 LAT 表计算

1901210443 刘高原

1.祖冲之 S 盒的介绍

根据国密祖冲之算法的介绍可以知道，祖冲之算法的 S 盒共分四个小 S 盒，分别为 S0、S1、S2、S3，其中 S2=S0、S3=S1.

本次作业让计算的就是其中两个小盒 S0 和 S1 的 DDT 表和 ACT 表。

S 盒的输入输出是 4 字节，即 32 位，每个小盒输入输出为 8 位。

设 S0 的 8 比特输入为 X，将 X 视作两个 16 进制数的连接，即 X=H||L,则 S0 盒中第 H 行和第 L 列交叉的元素即为 S0 的输出 S0(X)

设 S 盒 S 的 32 比特输入 X 和 32 比特输出 Y 分别为：

X= x0 || x1 || x2 || x3

Y= y0 || y1 || y2 || y3

其中 xi 和 yi 均为 8 比特,i=0,1,2,3。

则有则有 yi=Si(xi),i=0,1,2,3。

由于我们仅要求 S0 盒和 S1 盒的 DDT 表和 ACT 表，因此输入时有 8 位。

2.DDT 的计算

1. $\Delta X=X1 \oplus X2$
2. 根据 X1 和 X2 查表可以得到 Y1 和 Y2(X 用 16 进制表示,共八位，高四位对应表中的行，低四位对应表中的列，由此可以找到 Y)

3. ΔY=Y1⊕Y2

4. ΔX 为 DDT 表的行， ΔY 为 DDT 表的列

运算过程：

循环输入 X1，循环指定 ΔX，由 X1 和 ΔX 算出 X2，然后查表分别得到 Y1 和 Y2，由 Y1 和 Y2 计算出 ΔY，统计所有 DDT[ΔX][ΔY]。

表的大小 256*256

3. LAT 的计算

X 和 Y 进行不同的位运算进行匹配。

运算为挑选 X 或 Y(二进制表示)中不同的位置上的数进行异或

Y 由 X 查表得到(X 用 16 进制表示，共八位，高四位对应表中的行，低四位对应表中的列，由此可以找到 Y)

在 X 的同一个位计算模式和 Y 同一个计算模式下，所有 X 以及其对应的 Y 进行此匹配运算有多少满足相等的条件，统计满足的次数，并将其表示为对 128 的偏移。

LAT 表的行为 X 中的参加运算的位(X 的二进制表示，若该位参加运算即为 1，不参加 即为 0)，列为 Y 中参加运算的位(Y 的二进制表示，若该位参加运算即为 1，不参加即为 0)，行列对应的值为所有满足此运算的总数相对于 128 的偏移量。

表的大小 256*256