ZUC 密码分析实验

1901210446—刘华兴

第一部分：差分分析及线性分析表

1 整体思路：

实验要求是计算祖冲之密码算法两个 S 盒的差分分布表和线性逼近表。通过使用老师上传的 zuc_core.c 中的 S 盒数据，并使用python实现

2 差分分析表的实现思路

ZUC 密码算法的 S 盒的输入有 8 个比特，其中前四个表示行数，后四个表示列数，置换时将输入换成 S 盒中相应位置的值。要构造差分分析表，我们需要两个明文x 和 x*，其中 x xor x* 为一个定值 x'，再将 x 和 x*分别输入S 盒运算，得到输出为 y 和 y*。计算 y xor y*的值 y'，统计 y'中值的分布情况。在实验中，我们让 x'取遍 00000000 到 11111111 的所有值，对于每一个 x'，让 x 也从 00000000 取到 11111111，计算相应的 x*，再计算 y 和 y*，最终得到 y'，统计从 00000000 到 11111111 中的每个值在 y'中的出现次数，最终将所有结果汇总，形成差分分析表。

3 线性逼近表的实现思路

线性逼近表是用于线性分析的表，和差分分析表稍有不同。线性逼近表分析的是明文X 和 X 经过 S 盒的输出 Y 的某些位组成的随机变量。

表中有 a 和 b 两种元素，a 表示 X 的某些位组成的数，b 表示 Y 的某些位组成的数。比如 a 为 3 则表示 X_7 和 X_8 为 1，b 为 4 则表示 Y_6 为 1，则此时的随机变量即为 X_7 xor X_8 xor Y_6 我们首先统计从 00000000 到 11111111 的 S 盒输出的值，再逐条统计满足 X_7 xor X_8 xor Y_6 =0 的个数并记录。和差分分析表一样，我们仍然要遍历所有的值，将所有结果汇总起来，最后形成一张 256*256 的表。

在实现中，我们先将整数转换成 8 位的二进制数，找出为 1 的位置，在 S 盒置换表中将这些位置上的值进行异或，如果结果为 0，则计数器加 1，直到统计完所有的值。

最后，我们可以将生成结果写入 csv 或 excel 中，以便展示。本次实验我将其写入了 excel 中

4 代码见连接

5 实验结果部分截图

S0_ddt.xlsx

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf	0x10
0x0	256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	2	4	2	0	0	4	0	0	2	8	2	0	0	0
0x2	0	2	0	0	0	2	0	2	4	2	4	2	0	2	0	0	0
0x3	0	0	0	0	0	0	0	0	0	0	4	0	4	0	0	0	0
0x4	0	2	4	2	4	0	0	0	4	2	0	2	4	4	0	4	0
0x5	0	2	0	0	0	0	0	2	0	0	0	2	4	2	0	0	0
0x6	0	0	0	0	0	0	0	2	0	2	0	0	0	0	4	0	0
0x7	0	0	4	0	0	0	0	0	0	0	0	2	0	2	0	0	0
0x8	0	4	4	4	4	4	0	4	0	4	0	4	0	4	0	4	8
0x9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0xa	0	2	0	0	0	2	4	0	0	2	4	0	0	2	0	0	0
0xb	0	4	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0
0xc	0	0	0	0	0	0	4	0	0	4	0	4	0	0	4	0	0
0xd	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0xe	0	4	0	0	4	0	0	0	0	0	0	0	0	0	0	4	0
0xf	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0
0x10	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0
0x11	0	2	0	2	0	0	4	0	0	2	0	2	0	0	4	0	0
0x12	0	2	0	2	0	2	0	0	4	2	4	0	0	2	0	2	0
0x13	0	0	0	0	0	0	0	0	0	0	4	0	4	0	0	0	0
0x14	0	2	4	2	4	0	0	0	4	2	0	2	4	4	0	4	0
0x15	0	2	4	2	4	0	0	0	0	2	0	2	0	0	4	0	4
0x16	0	0	0	0	4	0	0	2	0	2	0	0	0	0	0	0	4
0x17	0	2	0	0	0	0	0	2	4	0	0	0	0	0	0	0	0

S1_ddt.xlsx

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf	0x10
0x0	256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	2	0	2	0	0	0	0	2	2	0	0	2	2	2	0	2
0x2	0	2	0	2	2	2	2	0	0	2	0	0	0	0	2	2	2
0x3	0	2	2	2	0	2	0	0	2	2	2	2	0	0	0	0	2
0x4	0	0	0	0	0	2	0	0	0	2	2	0	2	0	0	2	2
0x5	0	0	0	2	2	2	2	2	2	2	0	0	0	0	2	0	0
0x6	0	2	0	2	0	2	0	2	0	2	0	0	2	2	0	0	2
0x7	0	0	0	0	2	0	2	0	0	0	0	2	2	2	2	2	0
0x8	0	2	0	0	0	0	2	2	2	0	2	0	0	0	0	0	0
0x9	0	2	0	0	0	0	0	0	0	0	0	2	0	2	2	2	0
0xa	0	0	2	2	0	2	0	2	0	2	2	2	0	0	0	2	0
0xb	0	2	0	2	0	2	0	2	2	0	2	2	0	2	4	2	0
0xc	0	0	2	0	2	2	2	0	2	2	0	2	2	0	2	0	2
0xd	0	2	0	0	0	0	2	2	0	0	2	0	0	2	2	0	2
0xe	0	0	0	2	2	2	2	2	0	2	0	0	0	2	0	0	2
0xf	0	0	0	2	2	2	0	0	2	0	0	0	2	2	2	0	2
0x10	0	2	0	0	0	2	0	2	0	0	0	2	0	0	2	2	2
0x11	0	0	0	2	0	2	0	0	2	0	2	2	0	0	0	0	0
0x12	0	0	2	0	0	0	0	0	2	0	2	0	2	2	0	0	0
0x13	0	0	0	0	2	0	0	2	2	2	0	2	0	2	0	2	0
0x14	0	2	2	0	0	2	0	0	0	2	0	2	0	2	0	0	0
0x15	0	2	0	0	0	2	2	0	0	0	2	0	0	0	2	0	0
0x16	0	0	2	0	2	0	0	0	0	0	0	2	0	2	0	0	0
0x17	0	0	2	0	2	2	2	0	2	0	2	0	0	2	2	2	2

S0_lat.xlsx

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf	0x10
0x0	256	256	256	128	256	128	128	128	256	128	128	128	128	128	128	128	256
0x1	128	128	128	128	128	128	128	128	128	128	144	144	128	128	128	128	128
0x2	128	128	128	128	128	128	120	136	128	128	136	120	144	112	136	136	160
0x3	128	128	128	128	128	128	136	136	128	128	136	120	128	128	136	120	144
0x4	128	128	128	112	112	128	128	128	128	128	120	120	120	136	144	112	96
0x5	128	128	144	128	128	128	112	144	128	128	120	120	136	136	128	128	112
0x6	128	128	128	128	112	128	120	136	128	128	128	128	136	120	136	136	128
0x7	128	128	128	128	128	128	136	136	128	128	112	144	136	136	120	136	128
0x8	128	128	96	128	128	128	128	128	128	128	136	136	120	136	136	120	128
0x9	128	128	128	128	128	128	128	128	112	112	136	136	120	120	136	136	128
0xa	128	128	128	128	128	128	120	136	112	144	128	128	136	120	128	128	128
0xb	128	128	128	128	128	128	120	120	128	128	128	128	120	120	128	128	128
0xc	128	128	112	128	128	112	144	144	128	128	128	128	128	128	136	120	128
0xd	128	128	128	112	128	128	128	128	128	128	128	128	128	128	120	120	128
0xe	128	128	128	128	128	112	136	120	128	128	120	136	128	128	128	128	128
0xf	128	128	128	128	128	128	136	136	128	128	120	136	144	144	144	112	128
0x10	128	128	128	128	120	120	128	128	136	120	120	128	120	136	128	120	144
0x11	128	128	128	128	128	128	120	120	128	128	136	128	128	128	128	136	128
0x12	128	160	128	96	136	120	136	120	128	128	128	136	136	120	128	136	128
0x13	128	128	128	128	128	128	128	112	104	104	128	136	128	128	144	120	128
0x14	128	160	128	160	120	120	128	128	128	128	128	136	128	128	120	128	128
0x15	128	128	128	128	128	128	120	136	136	136	144	120	136	136	136	128	128
0x16	128	128	128	128	128	120	104	136	136	120	136	120	128	144	112	136	144	112
0x17	128	128	128	128	128	128	144	128	128	128	120	144	136	136	120	128	128

S1_lat.xlsx

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf	0x10
0x0	256	256	256	128	256	128	128	128	256	128	128	128	128	128	128	128	256
0x1	128	134	126	140	136	130	126	136	138	140	140	134	134	116	128	126	134
0x2	128	118	130	116	134	132	124	134	132	138	126	136	126	116	140	134	140
0x3	128	136	120	140	130	118	134	126	122	142	142	118	140	140	140	120	138
0x4	128	140	122	130	114	134	124	140	132	120	134	118	138	126	140	140	116
0x5	128	122	140	130	130	136	126	136	114	136	122	140	124	126	116	122	138
0x6	128	130	132	134	124	126	124	126	136	122	132	126	124	126	116	126	140
0x7	128	124	126	130	136	136	114	130	114	130	124	140	142	122	116	120	114
0x8	128	130	136	126	114	116	130	128	132	114	140	118	134	116	134	120	128
0x9	128	124	142	126	126	126	124	128	126	114	120	136	120	120	130	126	134
0xa	128	116	126	122	136	124	130	118	132	140	130	130	136	120	130	114	132
0xb	128	130	132	118	112	118	120	142	114	116	130	116	130	120	134	140	130
0xc	128	130	138	116	136	130	130	124	128	118	130	136	116	122	118	116	132
0xd	128	132	132	136	124	140	112	128	118	130	126	130	122	130	130	130	130
0xe	128	124	120	136	122	142	126	126	128	128	136	140	130	138	134	138	116
0xf	128	130	130	120	130	128	128	114	122	132	120	134	120	134	130	132	130
0x10	128	116	142	138	132	120	142	138	134	126	116	116	114	114	140	116	124
0x11	128	114	128	122	128	134	116	138	124	118	128	130	128	126	120	118	122
0x12	128	126	120	130	134	116	118	128	130	140	122	120	116	142	116	130	128
0x13	128	112	130	134	126	114	128	128	132	132	122	134	114	126	136	120	118
0x14	128	128	120	116	142	126	130	142	122	134	122	130	140	120	136	128	120
0x15	128	134	126	120	138	132	116	138	116	114	126	128	126	120	116	122	134
0x16	128	122	130	132	116	126	134	120	126	132	128	118	138	120	140	138	128
0x17	128	116	144	140	116	140	132	140	132	128	136	116	116	132	136	128	126

第二部分：为什么最后还需要进行异或轮密钥操作？

当密码的第一步和最后一步都是异或轮密钥时可以保证攻击者在不知道密钥的情况下无法开始加密和解密操作。而没有这一步的话，

那么攻击者拿到密文即可通过 S 盒进行第一步解密，增加了密码被破解的风险。

换句话说，最后进行异或轮密钥操作可以使密码更难被破解