差分分析表的实现

祖冲之密码算法的 S 盒的输入有 8 个比特，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，需要两个明文x 和 x*，其中 x⊕ x* 为一个定值 x′，再将 x 和 x*分别输入S 盒运计算，得到输出为 y 和 y*。计算 y ⊕y*的值 y′，统计 y′中值的分布情况。遍历 x′，x 和 y*，最终将所有结果汇总，

线性分析表的实现

线性分析表分析的是明文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。首先遍历 S 盒输出的值，再统计满足随机变量为 0 的概率并记录。

部分结果截图如下：

256	0	0	0	0	0	0	0	0	0
0	0	0	2	4	2	0	0	4	0
0	2	0	0	0	2	0	2	4	2
0	0	0	0	0	0	0	0	0	0
0	2	4	2	4	0	0	0	4	2
0	2	0	0	0	0	0	2	0	0
0	0	0	0	0	0	0	2	0	2
0	0	4	0	0	0	0	0	0	0
0	4	4	4	4	4	0	4	0	4
0	0	0	0	0	0	0	0	0	0
0	2	0	0	0	2	4	0	0	2
0	4	0	0	0	4	0	0	0	0
0	0	0	0	0	0	4	0	0	4
0	0	0	0	0	0	0	0	0	0
0	4	0	0	4	0	0	0	0	0
0	0	0	0	0	0	4	0	0	0
0	4	0	4	0	4	0	4	0	4
0	2	0	2	0	0	4	0	0	2
0	2	0	2	0	2	0	0	4	2
0	0	0	0	0	0	0	0	0	0

0	2	4	2	4	0	0	0	4	2
0	2	4	2	4	0	0	0	0	2
0	0	0	0	4	0	0	2	0	2
0	2	0	0	0	0	0	2	4	0
0	4	4	4	4	4	0	4	0	4
0	0	0	0	0	0	0	0	0	0
0	4	4	0	0	0	0	0	4	0
0	0	0	0	0	0	0	0	0	4

256	0	0	0	0	0	0	0	0	0
0	2	0	2	0	0	0	0	2	2
0	2	0	2	2	2	2	0	0	2
0	2	2	2	0	2	0	0	2	2
0	0	0	0	0	2	0	0	0	2
0	0	0	2	2	2	2	2	2	2
0	2	0	2	0	2	0	2	0	2
0	0	0	0	2	0	2	0	0	0
0	2	0	0	0	0	2	2	2	0
0	2	0	0	0	0	0	0	0	0
0	0	2	2	0	2	0	2	0	2
0	2	0	2	0	2	0	2	2	0
0	0	2	0	2	2	2	0	2	2
0	2	0	0	0	0	2	2	0	0
0	0	0	2	2	2	2	2	0	2
0	0	0	2	2	2	0	0	2	0
0	2	0	0	0	2	0	2	0	0
0	0	0	2	0	2	0	0	2	0
0	0	2	0	0	0	0	0	2	0
0	0	0	0	2	0	0	2	2	2
0	2	2	0	0	2	0	0	0	2
0	2	0	0	0	2	2	0	0	0
0	0	2	0	2	0	0	0	0	0
0	0	2	0	2	2	2	0	2	0
0	0	0	2	0	0	2	0	2	0
0	2	0	0	2	2	2	0	0	0
0	2	2	0	0	0	0	2	0	2
0	2	0	2	0	2	0	2	2	2
0	0	0	2	0	0	0	2	0	0
0	2	2	2	2	0	2	0	0	0
0	2	0	2	0	2	2	0	0	0

0	0	0	2	2	2	0	0	0	0
256	256	256	128	256	128	128	128	256	128
128	128	128	128	128	128	128	128	128	128
128	128	128	128	128	128	120	136	128	128
128	128	128	128	128	128	136	136	128	128
128	128	128	112	112	128	128	128	128	128
128	128	144	128	128	128	112	144	128	128
128	128	128	128	112	128	120	136	128	128
128	128	128	128	128	128	136	136	128	128
128	128	96	128	128	128	128	128	128	128
128	128	128	128	128	128	128	128	112	112
128	128	128	128	128	128	120	136	112	144
128	128	128	128	128	128	120	120	128	128
128	128	112	128	128	112	144	144	128	128
128	128	128	112	128	128	128	128	128	128
128	128	128	128	128	112	136	120	128	128
128	128	128	128	128	128	136	136	128	128
128	128	128	128	120	120	128	128	136	120
128	128	128	128	128	128	120	120	128	128
128	160	128	96	136	120	136	120	128	128
128	128	128	128	128	128	128	112	104	104
128	160	128	160	120	120	128	128	128	128
128	128	128	128	128	128	120	136	136	136
128	128	128	128	120	104	136	136	120	136
128	128	128	128	128	128	144	128	128	128
128	128	128	128	120	152	128	128	136	120
128	128	128	128	128	128	120	120	128	128
128	160	128	96	120	136	120	136	128	128
128	128	128	128	128	128	144	128	104	104
128	96	128	96	120	120	128	128	128	128
128	128	128	128	128	128	136	120	120	120
128	128	128	128	136	120	136	136	136	120
128	128	128	128	128	128	128	112	128	128
128	128	112	128	128	128	128	120	136	136
128	128	112	128	128	128	144	136	120	120
128	128	128	128	128	128	128	120	120	136
128	128	128	128	128	128	144	120	136	120

256	256	256	128	256	128	128	128	256	128
128	134	126	140	136	130	126	136	138	140
128	118	130	116	134	132	124	134	132	138
128	136	120	140	130	118	134	126	122	142
128	140	122	130	114	134	124	140	132	120
128	122	140	130	130	136	126	136	114	136
128	130	132	134	124	126	124	126	136	122
128	124	126	130	136	136	114	130	114	130
128	130	136	126	114	116	130	128	132	114
128	124	142	126	126	126	124	128	126	114
128	116	126	122	136	124	130	118	132	140
128	130	132	118	112	118	120	142	114	116
128	130	138	116	136	130	130	124	128	118
128	132	132	136	124	140	112	128	118	130
128	124	120	136	122	142	126	126	128	128
128	130	130	120	130	128	128	114	122	132
128	116	142	138	132	120	142	138	134	126
128	114	128	122	128	134	116	138	124	118
128	126	120	130	134	116	118	128	130	140
128	112	130	134	126	114	128	128	132	132
128	128	120	116	142	126	130	142	122	134
128	134	126	120	138	132	116	138	116	114
128	122	130	132	116	126	134	120	126	132
128	116	144	140	116	140	132	140	132	128
128	138	126	124	142	120	128	134	118	136
128	116	120	136	134	142	138	126	132	116
128	120	132	124	128	128	116	140	142	142
128	142	126	124	124	118	114	124	144	122
128	122	136	130	132	126	136	122	138	116
128	124	134	130	124	124	126	126	116	140
128	128	126	130	130	138	128	132	138	130
128	126	140	118	118	128	130	120	136	122
128	128	124	120	116	120	124	116	122	126
128	130	126	116	116	118	134	124	120	130