生成规则分析:

P0:每一行是 0-15 的置换
P1:传输函数非线性
P2:输入一位，改变两位。当 abcdef 中 af 变化时变现为在行间跳动(L0-L1 L0-L2 L2-L3 L3-L1)，bcde 变化时变现为行内的卡诺图相邻位置移动。
P3:S(X) 与 S(X^001100)输出两位不同。行内限制。
P4:S(X) 与 S(X^11yz00)不同。行间限制（L0-L2; L1-13）

	00	01	11	10
00	0	1	3	2
01	4	5	7	6
11	12	13	15	14
10	8	9	11	10

算法简要说明:

采取分行步骤生成，共四行构成一个 sBox。采用候选方法来生成，在生成新元素时根据已经生成了的元素间的限制关系来删除掉不可用的元素，然后从可用的元素中选取生成。

算法过程分析：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
L0																
L1																
L2																
L3																

0. 生成一行

生成一行时，影响的主要是 p0,p2,p3。生成元素后

p0 部分 p2 p3	所有元素候选值中删除相同的
P2	卡诺图相邻位置删除相差一位的
P3	异或 0110 位置删除相差一位的

1. 生成 L0

第一个生成。正常生成。

2. 生成 L1

依据行间关系限制 p2，在生成一行时，提前上出不满足行间限制的候选值。

部分 p2	与 L0 同位置删除相同的，相差一位的

3. 生成 L2

依据行间关系限制 p2 p4，在生成一行时，提前上出不满足行间限制的候选值。

部分 p2	与 L0 同位置删除相同的，相差一位的
P4	与 L0^1yz0 位置删除相同的

4. 生成 L3

类似 L2

这样依据限制关系，不断的从候选值中随机取元素生成便可以生成所需要的 S 盒。

数据结构说明：

T_dif1 ： 相邻位置表 即变化一位位置可能变化的值

T_1yz0：p4 规则中 中间四位 bcde ^1yz0 取值表

T_candi：可选元素候选表 **-1**：不可选

例：

```
[[ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0 -1  2  3 -1 -1  6 -1  8  9 10 11 12 -1 14 15]
 [ 0 -1  2  3 -1 -1  6 -1  8  9 10 11 12 -1 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0 -1  2  3 -1 -1  6 -1  8  9 10 11 12 -1 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0 -1  2  3 -1 -1  6 -1  8  9 10 11 12 -1 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
 [ 0  1  2  3  4 -1  6  7  8  9 10 11 12 13 14 15]
```

[0 1 2 3 4 -1 6 7 8 9 10 11 12 13 14 15]]

T_num：可选择的元素数量表 **inf:**已经填充选择了

例：

[inf, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16]

slct_pos：每次填充选择的位置

slct_num：每次填充的数

函数调用表: