密码分析——ZUC 算法（祖冲之序列密码算法）

一、S 盒

32 比特 S 盒 S 由 4 个小的 8×8 的 S 盒并置而成，即 $S=(S_0，S_1，S_2，S_3)$,其中 $S_0=S_2$，$S_1=S_3$。S_0 和 S_1 的定义分别见表 1 和表 2。设 S_0 (或 S_1)的 8 比特输入为 x， 将 x 视作两个 16 进制数的连接，即 $x=h\|l$,则表 1(或表 2)中第 h 行和第 l 列交叉的元素即为 S_0 (或 S_1)的输出 $S_0(x)$（或 $S_1(x)$）。

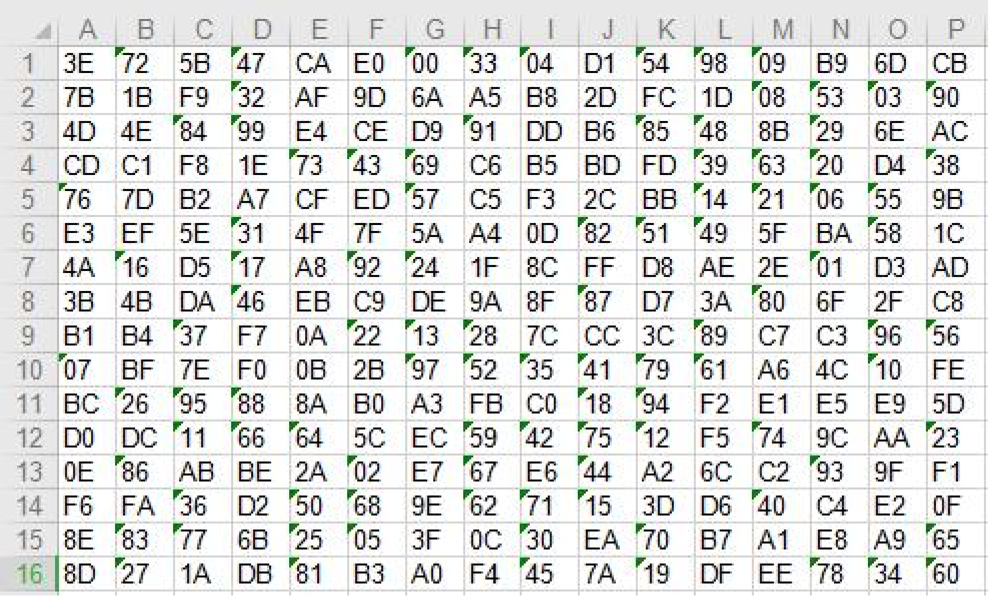
设 S 盒 S 的 32 比特输入 X 和 32 比特输出 Y 分别为：

$$X=x_0\|x_1\|x_2\|x_3$$

$$Y=y_0\|y_1\|y_2\|y_3$$

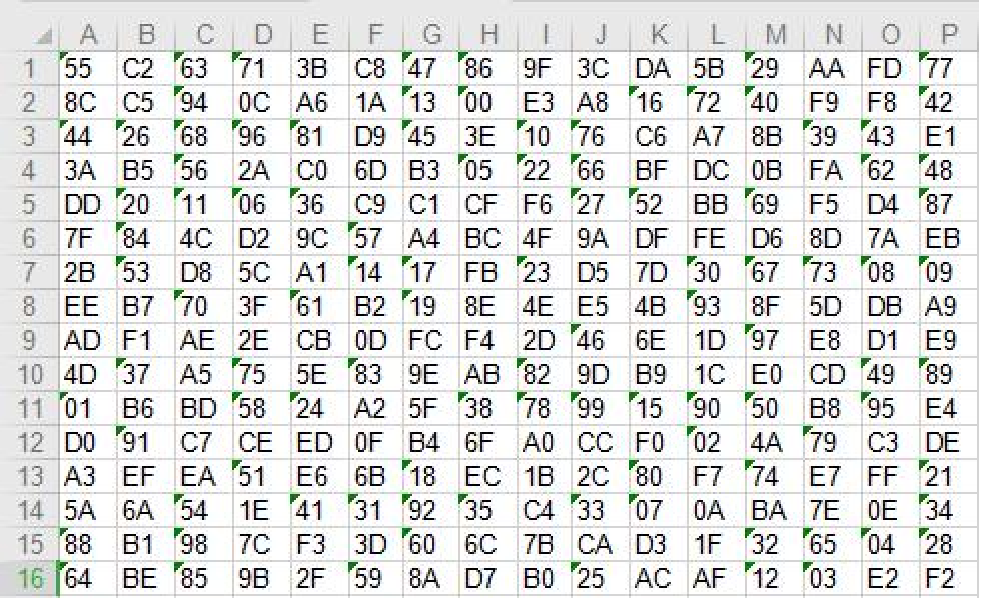
其中 x_i 和 y_i 均为 8 比特字节，$i=0,1,2,3$，则有 $y_i=S_i(x_i)$，$i=0,1,2,3$。

表 1 S_0 盒



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	3E	72	5B	47	CA	E0	00	33	04	D1	54	98	09	B9	6D	CB
2	7B	1B	F9	32	AF	9D	6A	A5	B8	2D	FC	1D	08	53	03	90
3	4D	4E	84	99	E4	CE	D9	91	DD	B6	85	48	8B	29	6E	AC
4	CD	C1	F8	1E	73	43	69	C6	B5	BD	FD	39	63	20	D4	38
5	76	7D	B2	A7	CF	ED	57	C5	F3	2C	BB	14	21	06	55	9B
6	E3	EF	5E	31	4F	7F	5A	A4	0D	82	51	49	5F	BA	58	1C
7	4A	16	D5	17	A8	92	24	1F	8C	FF	D8	AE	2E	01	D3	AD
8	3B	4B	DA	46	EB	C9	DE	9A	8F	87	D7	3A	80	6F	2F	C8
9	B1	B4	37	F7	0A	22	13	28	7C	CC	3C	89	C7	C3	96	56
10	07	BF	7E	F0	0B	2B	97	52	35	41	79	61	A6	4C	10	FE
11	BC	26	95	88	8A	B0	A3	FB	C0	18	94	F2	E1	E5	E9	5D
12	D0	DC	11	66	64	5C	EC	59	42	75	12	F5	74	9C	AA	23
13	0E	86	AB	BE	2A	02	E7	67	E6	44	A2	6C	C2	93	9F	F1
14	F6	FA	36	D2	50	68	9E	62	71	15	3D	D6	40	C4	E2	0F
15	8E	83	77	6B	25	05	3F	0C	30	EA	70	B7	A1	E8	A9	65
16	8D	27	1A	DB	81	B3	A0	F4	45	7A	19	DF	EE	78	34	60

表 2 S_1 盒



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	55	C2	63	71	3B	C8	47	86	9F	3C	DA	5B	29	AA	FD	77
2	8C	C5	94	0C	A6	1A	13	00	E3	A8	16	72	40	F9	F8	42
3	44	26	68	96	81	D9	45	3E	10	76	C6	A7	8B	39	43	E1
4	3A	B5	56	2A	C0	6D	B3	05	22	66	BF	DC	0B	FA	62	48
5	DD	20	11	06	36	C9	C1	CF	F6	27	52	BB	69	F5	D4	87
6	7F	84	4C	D2	9C	57	A4	BC	4F	9A	DF	FE	D6	8D	7A	EB
7	2B	53	D8	5C	A1	14	17	FB	23	D5	7D	30	67	73	08	09
8	EE	B7	70	3F	61	B2	19	8E	4E	E5	4B	93	8F	5D	DB	A9
9	AD	F1	AE	2E	CB	0D	FC	F4	2D	46	6E	1D	97	E8	D1	E9
10	4D	37	A5	75	5E	83	9E	AB	82	9D	B9	1C	E0	CD	49	89
11	01	B6	BD	58	24	A2	5F	38	78	99	15	90	50	B8	95	E4
12	D0	91	C7	CE	ED	0F	B4	6F	A0	CC	F0	02	4A	79	C3	DE
13	A3	EF	EA	51	E6	6B	18	EC	1B	2C	80	F7	74	E7	FF	21
14	5A	6A	54	1E	41	31	92	35	C4	33	07	0A	BA	7E	0E	34
15	88	B1	98	7C	F3	3D	60	6C	7B	CA	D3	1F	32	65	04	28
16	64	BE	85	9B	2F	59	8A	D7	B0	25	AC	AF	12	03	E2	F2

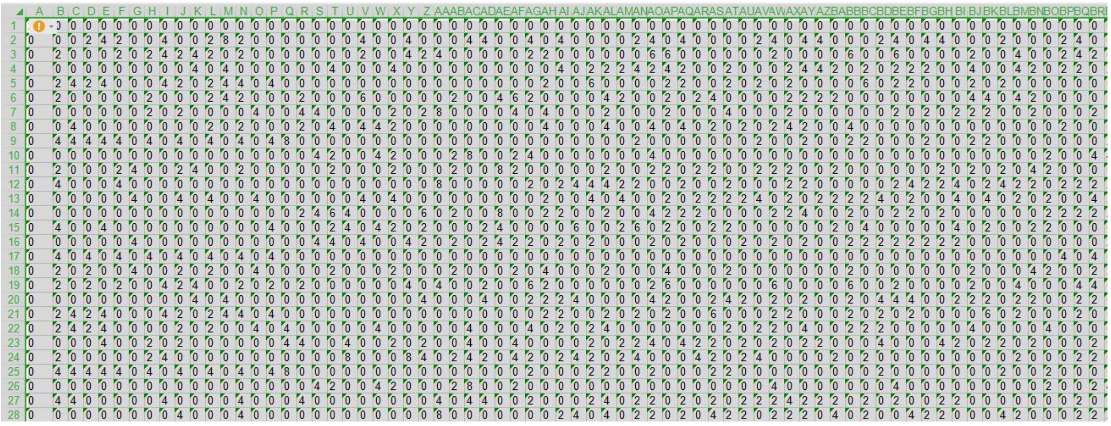
二、差分分布表

设计思路：由于 ZUC 算法的 S 盒是并置的，输入 X 中的各部分 x_i 经过对应 S_i 盒置换变换后得到各部分输出 $y_i = S_i(x_i)$， $i = 0,1,2,3$ 。因此，计算 S 盒的差分分布表即计算各小 S 盒的差分分布表即可。

对于每一小 S 盒，输入差分 Δx_i 的取值为 0x00-0xff，共 256 种。而每一差分取值又对应 256 种值分别为 0x00-0xff 的输入 x_i ，通过异或运算得到另一输入 $x_i' = x_i \oplus \Delta x_i$ 。再分别计算两输入对应的输出 $y_i = S_i(x_i)$和 $y_i' = S_i'(x_i)$，以及其对应的差分值 $\Delta y_i = y_i \oplus y_i'$ ，统计各 Δy_i 出现的频数，记录在表中对应的$(\Delta x_i，\Delta y_i)$位置。每个小 S 盒对应的差分分布表的大小为 256*256。

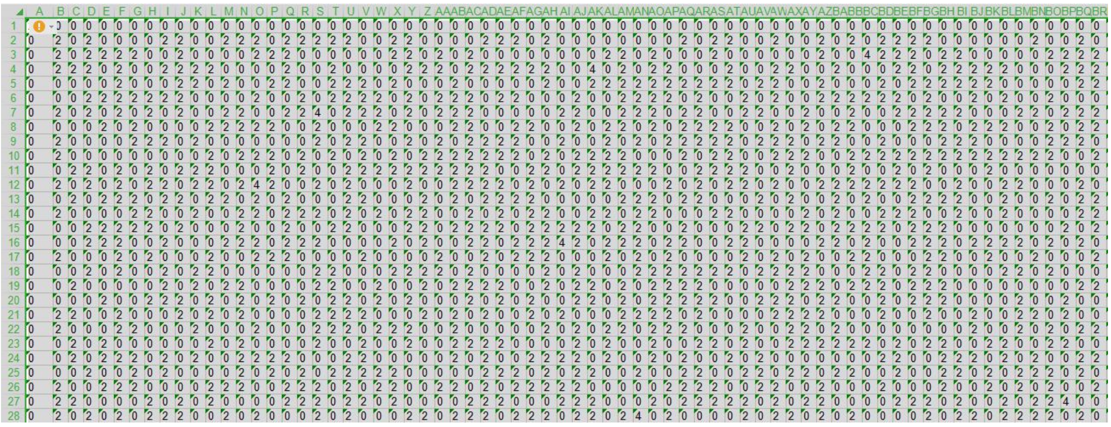
运算结果如表 3 和表 4 所示。

表 3 S_0 盒 DDT（部分）



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR
1	[illegible]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	2	4	2	0	0	4	0	0	2	8	2	0	0	0	0	0	0	0	4	0	0	4	0	0	0	4	4	0	0	4	0	4	0	0	0	0	2	4	0	4	0	0	0	0	2	4	0	4	4	0	0	0	2	4	0	4	4	0	0	0	2	0	0	0	2	4	0
3	0	2	0	0	0	2	0	2	4	2	4	2	0	2	0	0	0	0	0	0	0	2	0	0	4	2	4	0	0	0	0	0	2	2	0	0	0	0	0	0	6	6	0	0	0	0	0	0	2	0	0	0	0	6	0	0	6	0	0	0	0	2	0	0	4	0	0	2	4	2
4	0	0	0	0	0	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	0	0	4	0	0	0	0	0	0	0	0	0	0	4	0	2	2	2	4	2	4	2	0	0	2	0	0	0	2	4	4	2	0	2	0	2	2	2	0	0	4	0	0	4	2	0	2	2	0
5	0	2	4	2	4	0	0	0	4	2	0	2	4	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	6	0	0	0	0	2	2	0	0	2	0	2	0	2	0	0	0	0	6	0	2	2	0	0	0	2	0	2	0	0	0	0	0	0
6	0	2	0	0	0	0	0	2	0	0	0	2	4	2	0	0	0	2	0	0	0	6	0	0	0	0	0	2	0	0	4	6	2	0	0	0	0	4	2	0	0	2	0	2	4	0	0	0	0	2	2	2	2	0	0	0	0	0	0	0	0	4	4	0	4	2	0	0	0	0
7	0	0	0	0	0	0	0	2	0	2	0	0	0	0	4	0	0	4	4	0	0	0	0	2	0	2	8	0	0	0	0	4	0	4	0	0	0	2	0	0	0	2	0	0	0	4	0	0	0	2	0	0	0	0	0	0	2	0	2	0	2	2	2	0	0	2	0	0	0	2
8	0	0	4	0	0	0	0	0	0	0	0	2	0	2	0	0	0	2	0	4	0	4	4	2	0	0	0	0	0	0	0	0	0	4	0	0	0	4	0	0	4	0	4	0	2	0	2	0	2	4	2	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
9	0	4	4	4	4	4	0	4	0	4	0	4	0	4	0	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	0	0	2	0	0	2	2	0	0	0	2	0	0	2	2	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	0	4	2	0	0	0	2	8	0	0	2	4	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	4
11	0	2	0	0	0	2	4	0	0	2	4	0	0	2	0	0	0	0	0	2	0	0	0	2	0	0	0	2	0	0	8	2	0	0	0	0	0	2	0	0	2	2	0	2	2	0	0	2	2	2	0	0	2	0	0	0	0	0	0	2	0	2	0	2	0	4	2	0	0	0
12	0	4	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	2	0	2	4	4	4	2	2	0	0	2	0	0	2	0	0	0	2	2	0	0	0	0	0	2	4	2	2	4	0	2	4	2	2	0	2	2	2
13	0	0	0	0	0	0	4	0	0	4	0	4	0	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0	0	0	0	0	0	2	0	0	4	0	4	0	0	2	0	2	2	2	2	4	0	2	0	2	2	2	2	4	0	2	0	0	4	0	4	0	2	0	2	0	0	4
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	4	6	4	0	0	0	0	6	0	2	0	0	8	0	0	2	2	0	0	2	0	0	4	2	2	2	0	0	0	0	2	2	4	0	0	2	0	0	2	2	0	2	0	0	0	0	0	0	2	2	2	2
15	0	4	0	0	4	0	0	0	0	0	0	0	0	0	0	4	0	0	0	2	4	0	4	2	0	2	0	0	0	2	4	0	0	0	0	6	0	0	2	6	0	2	0	0	2	2	0	0	0	0	0	0	2	0	4	0	0	0	0	0	4	0	2	0	0	2	2	0	0	0
16	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	4	4	0	4	0	0	4	2	0	2	0	2	4	2	2	0	2	0	2	0	0	0	2	0	2	0	0	0	2	0	2	0	2	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	0
17	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	4
18	0	2	0	2	0	0	4	0	0	2	0	2	0	0	4	0	0	0	0	2	0	0	0	2	0	0	0	2	0	0	0	2	0	4	0	0	0	2	0	0	0	4	0	0	0	2	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	0	0	0	4	2	0	0	2
19	0	2	0	2	0	2	0	0	4	2	4	0	0	2	0	2	0	2	0	0	0	0	0	0	4	0	4	0	0	2	0	0	6	2	0	0	0	0	0	0	2	6	0	0	0	0	0	0	6	0	0	0	0	6	0	0	2	0	0	0	0	2	0	0	4	0	0	0	4	4
20	0	0	0	0	0	0	0	0	0	0	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	4	0	0	2	2	2	4	0	0	0	0	4	2	0	0	2	4	2	0	2	0	2	0	0	2	0	4	4	4	0	0	2	2	2	0	2	2	0	0	2	2
21	0	2	4	2	4	0	0	0	4	2	0	2	4	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	0	2	0	2	0	2	0	0	6	0	0	0	2	2	0	0	0	2	0	2	0	2	0	0	0	0	6	0	2	0	0	0	2	0
22	0	2	4	2	4	0	0	0	0	2	0	2	0	0	4	0	4	0	0	0	0	0	4	0	0	0	0	0	4	0	0	0	4	0	2	0	2	4	0	0	0	0	0	0	0	2	0	2	2	0	4	0	0	2	2	2	0	0	0	0	0	4	0	0	0	0	4	0	0	0
23	0	0	0	0	4	0	0	2	0	2	0	0	0	0	0	0	4	4	0	0	4	0	0	2	0	2	0	0	4	0	0	4	0	0	0	0	2	0	2	2	4	0	4	2	2	0	2	0	2	0	2	2	0	0	0	4	0	0	0	4	2	0	2	2	0	2	0	0	0	2
24	0	2	0	0	0	0	0	2	4	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	8	4	0	2	4	2	0	4	2	0	2	4	2	0	2	4	0	0	0	4	2	0	2	4	0	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	2	0	0	0	2	2
25	0	4	4	4	4	4	0	4	0	4	0	4	0	4	0	4	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2	2	0	0	2	0	0	0	2	2	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	0	0	2	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	0	4	2	0	0	0	2	8	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	2	0	0	2
27	0	4	4	0	0	0	0	0	4	0	0	0	0	4	0	0	0	4	0	0	0	0	0	0	0	0	4	0	4	4	0	0	2	0	0	0	2	4	0	2	2	0	2	0	2	0	2	2	2	4	2	2	2	0	2	0	2	0	2	2	0	0	0	0	0	0	0	0	2	0
28	0	0	0	0	0	0	0	0	0	4	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	2	4	0	4	0	2	2	0	2	0	4	2	2	0	2	2	2	0	4	0	2	0	0	4	2	2	0	0	0	4	2	0	0	0	2	2

表 4 S_1 盒 DDT（部分）



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR
1	[illegible]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	2	0	2	0	0	0	0	2	2	0	0	2	2	2	0	2	2	2	2	2	0	0	2	2	0	0	0	0	2	2	2	0	2	0	0	0	0	0	0	0	0	2	0	2	2	0	0	2	0	0	2	0	2	0	2	2	2	2	0	0	0	0	0	0	2	0	0	2	0
3	0	2	0	2	2	2	2	0	0	2	0	0	0	0	2	2	2	0	0	0	0	0	0	2	2	0	2	0	2	0	0	0	0	0	0	0	0	2	2	0	2	0	0	0	2	0	0	0	0	0	0	2	0	0	4	2	2	2	0	2	2	0	0	0	0	0	2	2	2	2
4	0	2	2	2	0	2	0	0	2	2	2	2	0	0	0	0	2	0	0	2	0	0	0	0	2	2	2	0	2	2	2	2	2	2	0	0	4	0	2	0	2	2	0	0	0	2	0	0	2	2	0	0	2	0	0	0	2	2	0	2	2	2	2	2	0	0	0	2	2	2
5	0	0	0	0	0	2	0	0	0	2	2	0	2	0	0	2	2	0	0	2	2	2	0	2	0	0	0	2	0	0	0	0	0	2	0	0	2	2	2	2	2	2	2	2	2	2	0	2	2	0	0	2	0	0	0	2	0	2	2	2	2	2	2	0	0	0	0	0	2	2
6	0	0	0	2	2	2	2	2	2	2	0	0	0	0	2	0	0	2	0	2	2	2	2	0	2	0	2	2	2	0	2	2	0	0	0	2	0	0	2	2	2	2	0	2	0	0	2	0	2	0	0	2	2	2	2	2	2	0	2	0	0	2	0	2	0	0	2	0	0	0
7	0	2	0	2	0	2	0	2	0	2	0	0	2	2	0	0	2	2	4	0	2	2	2	0	2	0	2	2	2	0	0	0	0	0	2	2	0	0	2	2	2	0	2	2	0	0	2	2	0	0	2	0	0	2	0	0	2	2	2	2	2	0	0	0	2	2	0	2	2	2
8	0	0	0	0	2	0	2	0	0	0	0	2	2	2	2	2	0	0	2	0	0	0	2	2	0	0	0	2	2	0	0	2	2	0	0	2	0	2	2	0	2	0	2	2	2	2	0	0	2	0	2	0	2	2	0	0	0	2	2	2	0	2	2	2	0	0	2	0	2	2
9	0	2	0	0	0	0	2	2	2	0	2	0	0	0	0	0	0	0	2	0	2	2	0	0	2	0	2	0	2	2	2	2	0	0	2	0	0	2	0	2	0	2	2	2	2	2	0	2	2	2	0	2	2	0	0	2	0	0	0	2	2	2	0	0	0	0	2	2	2	0
10	0	2	0	0	0	0	0	0	0	0	0	2	0	2	2	2	0	2	0	2	0	2	0	2	0	2	2	2	2	2	2	2	0	2	0	2	2	2	2	0	0	0	2	0	2	2	0	0	2	2	2	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	2
11	0	0	2	2	0	2	0	2	0	2	2	2	0	0	0	2	0	2	0	0	2	2	2	2	2	2	2	2	2	2	0	0	2	2	0	2	2	2	2	2	2	0	0	2	2	2	2	0	0	2	0	0	0	2	0	0	2	0	2	0	0	0	2	0	0	0	0	0	0	0
12	0	2	0	2	0	2	0	2	2	0	2	2	0	2	4	2	0	0	2	0	2	0	0	0	2	0	0	2	2	2	2	0	2	0	2	0	2	2	0	0	0	2	0	2	0	2	2	0	2	0	0	2	2	2	2	2	2	2	0	0	2	0	0	2	2	0	0	0	2	0
13	0	0	2	0	2	2	2	0	2	2	0	2	2	0	2	0	2	0	0	0	2	2	0	0	0	2	0	2	0	2	2	2	2	0	0	0	0	0	2	2	2	0	2	2	0	0	0	2	0	2	0	0	2	0	2	0	0	2	2	2	2	0	0	2	0	0	2	0	2	2
14	0	2	0	0	0	0	2	2	0	0	2	0	0	2	2	0	2	2	2	0	2	0	2	0	2	2	0	0	2	0	2	0	2	2	0	0	2	2	0	2	2	0	0	0	2	2	0	0	0	0	2	0	2	0	0	2	2	2	0	0	2	0	0	2	0	0	0	0	2	2
15	0	0	0	2	2	2	2	2	0	2	0	0	0	2	0	0	2	0	0	2	2	0	0	0	2	2	0	2	2	2	2	0	2	2	2	2	2	0	2	2	0	0	2	0	0	0	2	2	0	2	2	0	2	2	2	2	0	2	2	2	0	0	0	0	0	0	0	2	0	2
16	0	0	0	2	2	2	0	0	2	0	0	0	2	2	2	0	2	2	2	0	0	0	0	2	0	2	0	0	2	2	0	2	2	2	4	2	0	2	2	2	0	2	2	0	0	2	2	0	0	0	0	2	2	0	2	0	0	2	2	2	0	2	2	2	2	0	2	0	2	0
17	0	2	0	0	0	2	0	2	0	0	0	2	0	0	2	2	2	0	0	0	0	2	0	0	0	0	2	0	0	2	0	2	2	2	0	0	0	2	0	2	0	2	0	0	0	0	2	0	2	0	2	0	0	2	2	0	0	0	2	2	0	0	2	0	0	2	0	0	0	2
18	0	0	0	2	0	2	0	0	2	0	2	2	0	0	0	0	0	0	2	2	0	0	0	2	2	2	2	0	2	0	0	0	0	2	0	2	0	0	0	2	2	2	2	2	2	2	0	2	2	2	2	0	0	0	2	2	0	2	2	0	0	0	0	2	2	0	2	0	0	0
19	0	0	2	0	0	0	0	0	2	0	2	0	2	2	0	0	0	0	2	2	0	0	2	0	0	2	0	2	2	2	2	0	0	2	0	2	2	0	2	0	2	2	2	2	0	0	0	0	0	2	2	2	0	2	2	2	0	2	2	2	0	0	0	0	0	0	0	0	2	2
20	0	0	0	0	2	0	0	2	2	2	0	2	0	2	0	2	0	2	0	2	2	0	2	0	2	0	0	0	2	0	2	0	2	0	0	2	2	0	2	0	2	2	2	2	2	0	0	2	2	2	0	2	2	0	0	2	0	2	2	2	0	0	0	0	2	0	0	2	0	0
21	0	2	2	0	0	2	0	0	0	2	0	2	0	2	0	0	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	0	2	0	2	0	0	0	2	2	2	2	0	2	0	0	0	0	2	2	2	2	0	0	0	2	0	0	2	0	0	2	0	0	2	2	0	2	0	0
22	0	2	0	0	0	2	2	0	0	0	2	0	0	0	2	0	0	0	2	2	2	0	2	2	2	0	0	2	0	0	0	0	0	2	0	2	0	2	2	0	2	2	2	0	0	0	2	0	0	2	2	0	2	0	0	0	0	0	0	0	0	2	0	0	2	0	2	0	2	2
23	0	0	2	0	2	0	0	0	0	0	0	2	0	2	0	0	0	0	2	0	0	2	0	0	2	0	0	2	2	2	2	0	0	0	0	2	0	2	0	0	2	0	0	2	2	0	2	0	0	2	2	2	2	2	2	0	2	0	2	2	0	0	2	2	0	0	2	2	0	0
24	0	0	2	0	2	2	2	0	2	0	2	0	0	2	2	2	2	0	0	0	2	2	0	0	0	0	0	2	0	2	0	0	2	2	2	2	0	2	0	0	2	0	2	0	0	2	0	2	0	0	0	0	0	0	0	2	2	0	0	2	2	2	0	2	0	2	0	0	2	2
25	0	0	0	2	0	0	2	0	2	0	0	0	0	2	0	2	0	2	0	2	2	2	2	2	0	0	0	0	0	2	2	2	0	2	0	2	2	0	0	2	0	0	2	2	0	0	2	2	0	2	2	0	2	2	0	0	2	0	0	2	2	0	2	0	2	2	2	0	2	0
26	0	2	0	0	2	2	2	0	0	0	0	2	2	2	0	0	2	2	2	0	2	0	2	2	0	0	2	2	0	2	0	2	2	2	2	2	0	0	0	0	0	2	2	2	2	0	0	2	2	0	0	2	0	0	0	2	0	0	0	2	0	0	2	0	2	0	2	0	0	2
27	0	2	2	0	0	0	0	2	0	2	0	2	0	0	0	0	2	2	2	0	2	2	0	2	0	0	0	0	2	2	2	0	0	0	2	2	2	0	0	0	2	0	2	2	2	2	2	0	2	0	2	2	0	0	0	0	2	2	2	0	2	0	0	2	0	2	2	4	0	0
28	0	2	0	2	0	2	0	2	2	2	0	0	2	0	2	0	0	0	2	0	2	0	0	0	2	2	0	2	2	2	0	2	2	2	0	2	2	0	2	4	0	2	0	0	0	0	2	0	2	2	0	2	0	2	0	0	0	0	2	0	2	2	0	2	2	2	2	0	2	0

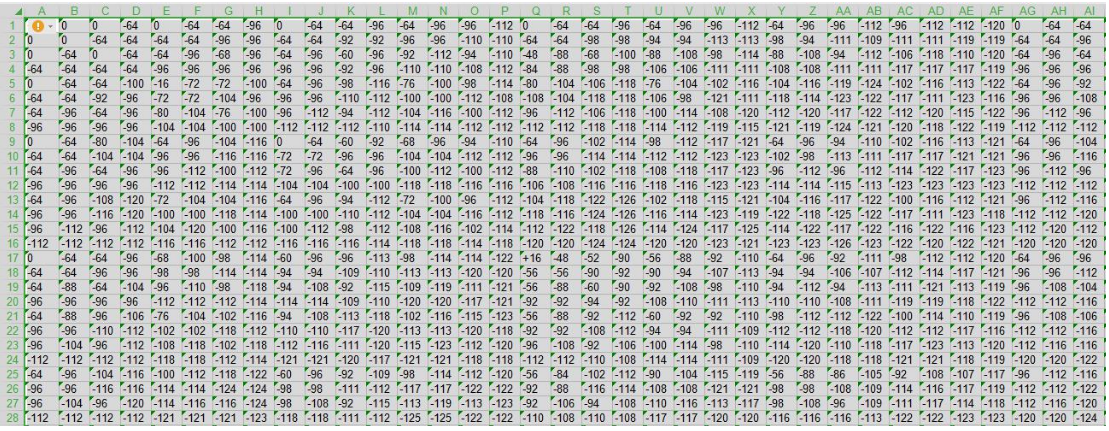
三、线性渐进表

设计思路：与差分分析表相似，计算 ZUC S 盒的线性渐进表仅需计算各小 S 盒的线性渐进表即可。

对于每一小 S 盒，输入 x_i 的组合可表示为 $c_0x_0 \oplus c_1x_1 \oplus ... \oplus c_7x_7$，其中 c_0，c_1，…，c_7 的取值为 0 或 1，共对应 2^8=256 种情况。同理，对于输出 y_i 来说，也存在着 $d_0y_0 \oplus d_1y_1 \oplus ... \oplus d_7y_7\left(d_0，d_1，d_2，d_3 = 0\text{或}1\right)$共 256 种情况，统计满足每一种输入组合与输出组合相等 $c_0x_0 \oplus c_1x_1 \oplus ... \oplus c_7x_7 = d_0y_0 \oplus d_1y_1 \oplus ... \oplus d_7y_7$ 的频数，并计算其偏差值（频数-256/2），将偏差值记录在对应的表项$\left(c_0c_1c_2c_3，d_0d_1d_2d_3\right)$中。每个小 S 盒对应的线性渐进表的大小为 256*256。

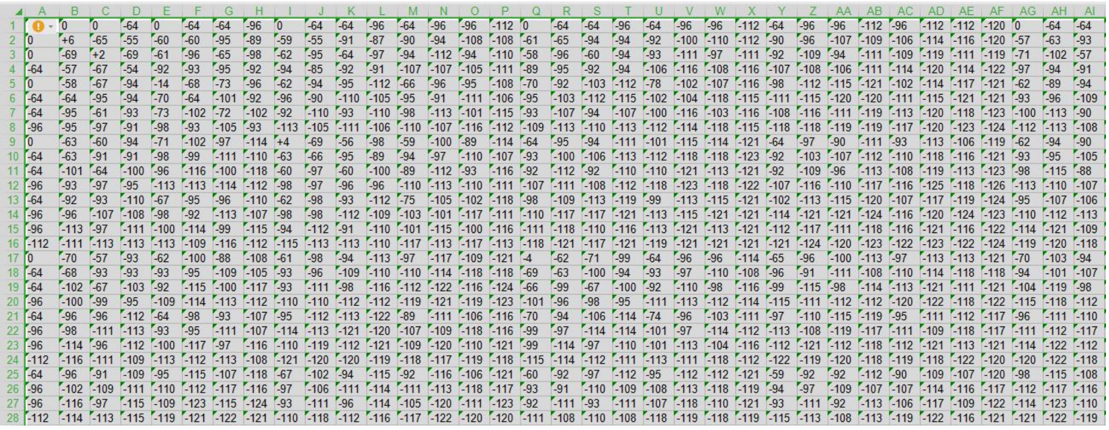
运算结果如表 5 和表 6 所示。

表 5 S_0 盒 LAT（部分）



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1		0	0	-64	0	-64	-64	-96	0	-64	-64	-96	-64	-96	-96	-112	0	-64	-64	-96	-64	-96	-96	-112	-64	-96	-96	-112	-96	-112	-112	-120	0	-64	-64
2	0	0	-64	-64	-64	-64	-96	-96	-64	-64	-92	-92	-96	-96	-110	-110	-64	-64	-98	-98	-94	-94	-113	-113	-98	-94	-111	-109	-111	-111	-119	-119	-64	-64	-96
3	0	-64	0	-64	-64	-96	-68	-96	-64	-96	-60	-96	-92	-112	-94	-110	-48	-88	-68	-100	-88	-108	-98	-114	-88	-108	-94	-112	-106	-118	-110	-120	-64	-96	-64
4	-64	-64	-64	-64	-96	-96	-96	-96	-96	-96	-92	-96	-110	-110	-108	-112	-84	-88	-98	-98	-106	-106	-111	-111	-108	-108	-111	-111	-117	-117	-117	-119	-96	-96	-96
5	0	-64	-64	-100	-16	-72	-72	-100	-64	-96	-98	-116	-76	-100	-98	-114	-80	-104	-106	-118	-76	-104	-102	-116	-104	-116	-119	-124	-102	-116	-113	-122	-64	-96	-92
6	-64	-64	-92	-96	-72	-72	-104	-96	-96	-96	-110	-112	-100	-100	-112	-108	-108	-104	-118	-118	-106	-98	-121	-111	-118	-114	-123	-122	-117	-111	-123	-116	-96	-96	-108
7	-64	-96	-64	-96	-80	-104	-76	-100	-96	-112	-94	-112	-104	-116	-100	-112	-96	-112	-106	-118	-100	-114	-108	-120	-112	-120	-117	-122	-112	-120	-115	-122	-96	-112	-96
8	-96	-96	-96	-96	-104	-104	-100	-100	-112	-112	-112	-110	-114	-114	-112	-112	-112	-112	-118	-118	-114	-112	-119	-115	-121	-119	-124	-121	-120	-118	-122	-119	-112	-112	-112
9	0	-64	-80	-104	-64	-96	-104	-116	0	-64	-60	-92	-68	-96	-94	-110	-64	-96	-102	-114	-98	-112	-117	-121	-64	-96	-94	-110	-102	-116	-113	-121	-64	-96	-104
10	-64	-64	-104	-104	-96	-96	-116	-116	-72	-72	-96	-96	-104	-104	-112	-112	-96	-96	-114	-114	-112	-112	-123	-123	-102	-98	-113	-111	-117	-117	-121	-121	-96	-96	-116
11	-64	-96	-64	-96	-96	-112	-100	-112	-72	-96	-64	-96	-100	-112	-100	-112	-88	-110	-102	-118	-108	-118	-117	-123	-96	-112	-96	-112	-114	-122	-117	-123	-96	-112	-96
12	-96	-96	-96	-96	-112	-112	-114	-114	-104	-104	-100	-100	-118	-118	-116	-116	-106	-108	-116	-116	-118	-116	-123	-123	-114	-114	-115	-113	-123	-123	-123	-123	-112	-112	-112
13	-64	-96	-108	-120	-72	-104	-104	-116	-64	-96	-94	-112	-72	-100	-96	-112	-104	-118	-122	-126	-102	-118	-115	-121	-104	-116	-117	-122	-100	-116	-112	-121	-96	-112	-116
14	-96	-96	-116	-120	-100	-100	-118	-114	-100	-100	-110	-112	-104	-104	-116	-112	-118	-116	-124	-126	-116	-114	-123	-119	-122	-118	-125	-122	-117	-111	-123	-118	-112	-112	-120
15	-96	-112	-96	-112	-104	-120	-100	-116	-100	-112	-98	-112	-108	-116	-102	-114	-112	-122	-118	-126	-114	-124	-117	-125	-114	-122	-117	-122	-116	-122	-116	-123	-112	-120	-112
16	-112	-112	-112	-112	-116	-116	-112	-112	-116	-116	-116	-114	-118	-118	-114	-118	-120	-120	-124	-124	-120	-120	-123	-121	-123	-123	-126	-123	-122	-120	-122	-121	-120	-120	-120
17	0	-64	-64	-96	-68	-100	-98	-114	-60	-96	-96	-113	-98	-114	-114	-122	+16	-48	-52	-90	-56	-88	-92	-110	-64	-96	-92	-111	-98	-112	-112	-120	-64	-96	-96
18	-64	-64	-96	-96	-98	-98	-114	-114	-94	-94	-109	-110	-113	-113	-120	-120	-56	-56	-90	-92	-90	-94	-107	-113	-94	-94	-106	-107	-112	-114	-117	-121	-96	-96	-112
19	-64	-88	-64	-104	-96	-110	-98	-118	-94	-108	-92	-115	-109	-119	-111	-121	-56	-88	-60	-90	-92	-108	-98	-110	-94	-112	-94	-113	-111	-121	-113	-119	-96	-108	-104
20	-96	-96	-96	-96	-112	-112	-112	-114	-114	-114	-109	-110	-120	-120	-117	-121	-92	-92	-94	-92	-108	-110	-111	-113	-110	-110	-108	-111	-119	-119	-118	-122	-112	-112	-116
21	-64	-88	-96	-106	-76	-104	-102	-116	-94	-108	-113	-118	-102	-116	-115	-123	-56	-88	-92	-112	-60	-92	-92	-110	-98	-112	-112	-122	-100	-114	-110	-119	-96	-108	-106
22	-96	-96	-110	-112	-102	-102	-118	-112	-110	-110	-117	-120	-113	-113	-120	-118	-92	-92	-108	-112	-94	-94	-111	-109	-112	-112	-118	-120	-112	-112	-117	-116	-112	-112	-116
23	-96	-104	-96	-112	-108	-118	-102	-118	-112	-116	-111	-120	-115	-123	-112	-120	-96	-108	-92	-106	-100	-114	-98	-110	-114	-120	-110	-118	-117	-123	-113	-120	-112	-116	-116
24	-112	-112	-112	-112	-118	-118	-112	-114	-121	-121	-120	-117	-121	-121	-118	-118	-112	-112	-110	-108	-114	-114	-111	-109	-120	-120	-118	-118	-121	-121	-118	-119	-120	-120	-122
25	-64	-96	-104	-116	-100	-112	-118	-122	-60	-96	-92	-109	-98	-114	-112	-120	-56	-84	-102	-112	-90	-104	-115	-119	-56	-88	-86	-105	-92	-108	-107	-117	-96	-112	-116
26	-96	-96	-116	-116	-114	-114	-124	-124	-98	-98	-111	-112	-117	-117	-122	-122	-92	-88	-116	-114	-108	-108	-121	-121	-98	-98	-108	-109	-114	-116	-117	-119	-112	-112	-122
27	-96	-104	-96	-120	-114	-116	-116	-124	-98	-108	-92	-115	-113	-119	-113	-123	-92	-106	-94	-108	-110	-116	-113	-117	-98	-108	-96	-109	-111	-117	-114	-118	-112	-116	-120
28	-112	-112	-112	-112	-121	-121	-121	-123	-118	-118	-111	-112	-125	-125	-122	-122	-110	-108	-110	-108	-117	-117	-120	-120	-116	-116	-116	-113	-122	-122	-123	-123	-120	-120	-124

表 4 S_1 盒 LAT（部分）



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1		0	0	-64	0	-64	-64	-96	0	-64	-64	-96	-64	-96	-96	-112	0	-64	-64	-96	-64	-96	-96	-112	-64	-96	-96	-112	-96	-112	-112	-120	0	-64	-64
2	0	+6	-65	-55	-60	-60	-95	-89	-59	-55	-91	-87	-90	-94	-108	-108	-61	-65	-94	-94	-92	-100	-110	-112	-90	-96	-107	-109	-106	-114	-116	-120	-57	-63	-93
3	0	-69	+2	-69	-61	-96	-65	-98	-62	-95	-64	-97	-94	-112	-94	-110	-58	-96	-60	-94	-93	-111	-97	-111	-92	-109	-94	-111	-109	-119	-111	-119	-71	-102	-57
4	-64	-57	-67	-54	-92	-93	-95	-92	-94	-85	-92	-91	-107	-107	-105	-111	-89	-95	-92	-94	-106	-116	-108	-116	-107	-108	-106	-111	-114	-120	-114	-122	-97	-94	-91
5	0	-58	-67	-94	-14	-68	-73	-96	-62	-94	-95	-112	-66	-96	-95	-108	-70	-92	-103	-112	-78	-102	-107	-116	-98	-112	-115	-121	-102	-114	-117	-121	-62	-89	-94
6	-64	-64	-95	-94	-70	-64	-101	-92	-96	-90	-110	-105	-95	-91	-111	-106	-95	-103	-112	-115	-102	-104	-118	-115	-111	-115	-120	-120	-111	-115	-121	-121	-93	-96	-109
7	-64	-95	-61	-93	-73	-102	-72	-102	-92	-110	-93	-110	-98	-113	-101	-115	-93	-107	-94	-107	-100	-116	-103	-116	-108	-116	-111	-119	-113	-120	-118	-123	-100	-113	-90
8	-96	-95	-97	-91	-98	-93	-105	-93	-113	-105	-111	-106	-110	-107	-116	-112	-109	-113	-110	-113	-112	-114	-118	-115	-118	-118	-119	-119	-117	-120	-123	-124	-112	-113	-108
9	0	-63	-60	-94	-71	-102	-97	-114	+4	-69	-56	-98	-59	-100	-89	-114	-64	-95	-94	-111	-101	-115	-114	-121	-64	-97	-90	-111	-93	-113	-106	-119	-62	-94	-90
10	-64	-63	-91	-91	-98	-99	-111	-110	-63	-66	-95	-89	-94	-97	-110	-107	-93	-100	-106	-113	-112	-118	-118	-123	-92	-103	-107	-112	-110	-118	-116	-121	-93	-95	-105
11	-64	-101	-64	-100	-96	-116	-100	-118	-60	-97	-60	-100	-89	-112	-93	-116	-92	-112	-92	-110	-110	-121	-113	-121	-92	-109	-96	-113	-108	-119	-113	-123	-98	-115	-88
12	-96	-93	-97	-95	-113	-113	-114	-112	-98	-97	-96	-96	-110	-113	-110	-111	-107	-111	-108	-112	-118	-123	-118	-122	-107	-116	-110	-117	-116	-125	-118	-126	-113	-110	-107
13	-64	-92	-93	-110	-67	-95	-96	-110	-62	-98	-93	-112	-75	-105	-102	-118	-98	-109	-113	-119	-99	-113	-115	-121	-102	-113	-115	-120	-107	-117	-119	-124	-95	-107	-106
14	-96	-96	-107	-108	-98	-92	-113	-107	-98	-98	-112	-109	-103	-101	-117	-111	-110	-117	-117	-121	-113	-115	-121	-121	-114	-121	-121	-124	-116	-120	-124	-123	-110	-112	-113
15	-96	-113	-97	-111	-100	-114	-99	-115	-94	-112	-91	-110	-101	-115	-100	-116	-111	-118	-110	-116	-113	-121	-113	-121	-112	-117	-111	-118	-116	-121	-116	-122	-114	-121	-109
16	-112	-111	-113	-113	-113	-109	-116	-112	-115	-113	-113	-110	-117	-113	-117	-113	-118	-121	-117	-121	-119	-121	-121	-121	-121	-124	-120	-123	-122	-123	-122	-124	-119	-120	-118
17	0	-70	-57	-93	-62	-100	-88	-108	-61	-98	-94	-113	-97	-117	-109	-121	-4	-62	-71	-99	-64	-96	-96	-114	-65	-96	-100	-113	-97	-113	-113	-121	-70	-103	-94
18	-64	-68	-93	-93	-93	-95	-109	-105	-93	-96	-109	-110	-110	-114	-118	-118	-69	-63	-100	-94	-93	-97	-110	-108	-96	-91	-111	-108	-110	-114	-118	-118	-94	-101	-107
19	-64	-102	-67	-103	-92	-115	-100	-117	-93	-111	-98	-116	-112	-122	-116	-124	-66	-99	-67	-100	-92	-110	-98	-116	-99	-115	-98	-114	-113	-121	-111	-121	-104	-119	-98
20	-96	-100	-99	-95	-109	-114	-113	-112	-110	-110	-112	-112	-119	-121	-119	-123	-101	-96	-98	-95	-111	-113	-112	-114	-115	-111	-112	-112	-120	-122	-118	-122	-115	-118	-112
21	-64	-96	-96	-112	-64	-98	-93	-107	-95	-112	-113	-122	-89	-111	-106	-116	-70	-94	-106	-114	-74	-96	-103	-111	-97	-110	-115	-119	-95	-111	-112	-117	-96	-111	-110
22	-96	-98	-111	-113	-93	-95	-111	-107	-114	-113	-121	-120	-107	-109	-118	-116	-99	-97	-114	-114	-101	-97	-114	-112	-113	-108	-119	-117	-111	-109	-118	-117	-111	-112	-117
23	-96	-114	-96	-112	-100	-117	-97	-116	-110	-119	-112	-121	-109	-120	-110	-121	-99	-114	-97	-110	-101	-113	-104	-116	-112	-121	-112	-118	-112	-121	-113	-121	-114	-122	-112
24	-112	-116	-111	-109	-113	-112	-113	-108	-121	-120	-120	-119	-118	-117	-119	-118	-115	-114	-112	-111	-113	-111	-118	-112	-122	-119	-120	-118	-119	-118	-122	-120	-120	-122	-118
25	-64	-96	-91	-109	-95	-115	-107	-118	-67	-102	-94	-115	-92	-116	-106	-121	-60	-92	-97	-112	-95	-112	-112	-121	-59	-92	-92	-112	-90	-109	-107	-120	-98	-115	-108
26	-96	-102	-109	-111	-110	-112	-117	-116	-97	-106	-111	-114	-111	-113	-118	-117	-93	-91	-110	-109	-108	-113	-118	-119	-94	-97	-109	-107	-107	-114	-116	-117	-112	-117	-116
27	-96	-116	-97	-115	-109	-123	-115	-124	-93	-111	-96	-114	-105	-120	-111	-123	-92	-111	-93	-111	-107	-118	-110	-121	-93	-111	-92	-113	-106	-117	-109	-122	-114	-123	-110
28	-112	-114	-113	-115	-119	-121	-122	-121	-110	-118	-112	-116	-117	-122	-120	-120	-111	-108	-110	-108	-118	-119	-118	-119	-115	-113	-108	-113	-119	-122	-116	-121	-121	-122	-119