4.4 Die Schlüsselauswahl

Zur Beschreibung der Runden gehört noch die Beschreibung der Schlüsselauswahl. Zunächst wird der 56-Bit-Schlüssel auf 64 Bit aufgebläht, indem nach je 7 Bits ein Paritätsbit eingefügt wird; welches, ist egal, man kann sogar beliebige Bits einfügen, da die zusätzlichen Bits nicht weiter verwendet werden. Jedenfalls ist der erste Schritt eine Abbildung

$$\mathrm{Par}\colon \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{64}.$$

Im zweiten Schritt werden die ursprünglichen 56 Bits wieder extrahiert, allerdings in der Reihenfolge der folgenden Tabelle.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Das ist eine Abbildung

$$\mathrm{PC}_1\colon \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{56}$$

('Permuted Choice 1'). Nun werden die 56 Bits in zwei 28-Bit-Hälften geteilt und diese jeweils zyklisch nach links geschoben, insgesamt 16 mal. Das sind also 16 Abbildungen

$$\mathrm{LS}_i\colon \mathbb{F}_2^{28} \longrightarrow \mathbb{F}_2^{28} \quad (i = 1, \ldots 16);$$

wie weit geschoben wird, zeigt die Tabelle:

1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Die ersten beiden Male wird also um ein Bit geschoben, dann 6 mal um zwei Bits usw. Für die i-te Schlüsselauswahl A_i wird nach der i-ten Verschiebung noch die 'Permuted Choice 2',

$$\mathrm{PC}_2\colon \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{48}$$

ausgeführt, wobei die Auswahl in der Reihenfolge der folgenden Tabelle geschieht (die Bits 9, 18, 22, 25, 35, 38, 43, 54 entfallen dabei).

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Insgesamt ist

$$A_i = \mathrm{PC}_2 \circ \mathrm{LS}_i \circ \cdots \circ \mathrm{LS}_1 \circ \mathrm{PC}_1 \circ \mathrm{Par}\,.$$

Diese Konstruktion wird noch einmal in dieser Abbildung zusammengefasst: