IV. Feistel-Chiffren und DES

Entwurfsprinzipien moderner Blockchiffren

- Einfache Operationen, aber nicht nur linear (Effizienz)
- Mehrere Runden um Sicherheit zu garatieren (Konfusion und Diffusion)
- 2 wesentliche Strukturen
  - Feistel-Chiffren (DES)
  - Substitution-Permutations Netzwerke (AES).

IV.1 Feistel-Chiffren

Feistel Chiffre definiert durch

1. **Klartextraum $P = \{0,1\}^n$, Chiffretextraum $C = \{0,1\}^n$, Schlüsselraum $K \subseteq \{0,1\}^m$, wobei n gerade ist, n=2t.**

2. **Rundenzahl r > 1.**

3. **Methode zur Erzeugung von Rundenschlüsseln**

   KeySchedule: $\{0,1\}^m \rightarrow \{0,1\}^{r \cdot l}$

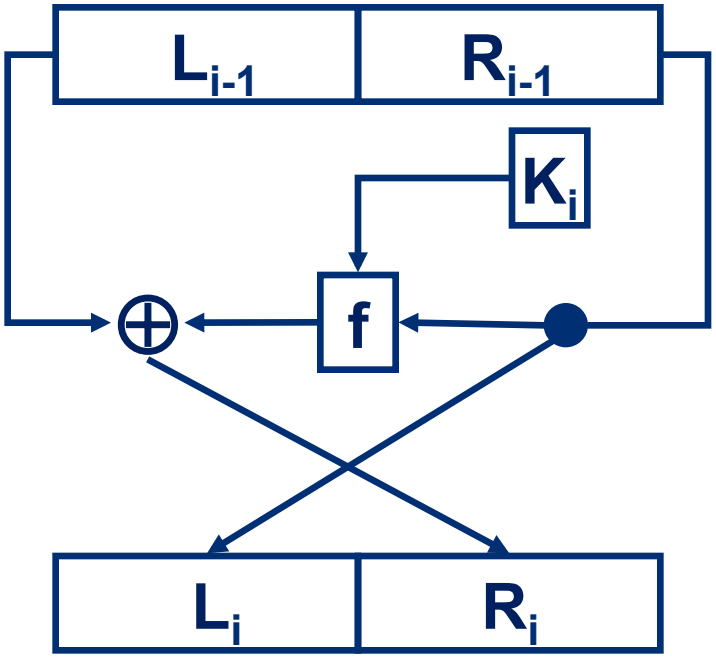
   $K \mapsto K_1 \ldots K_r$

4. **Rundenfunktion** $f : \{0,1\}^l \times \{0,1\}^t \rightarrow \{0,1\}^t$

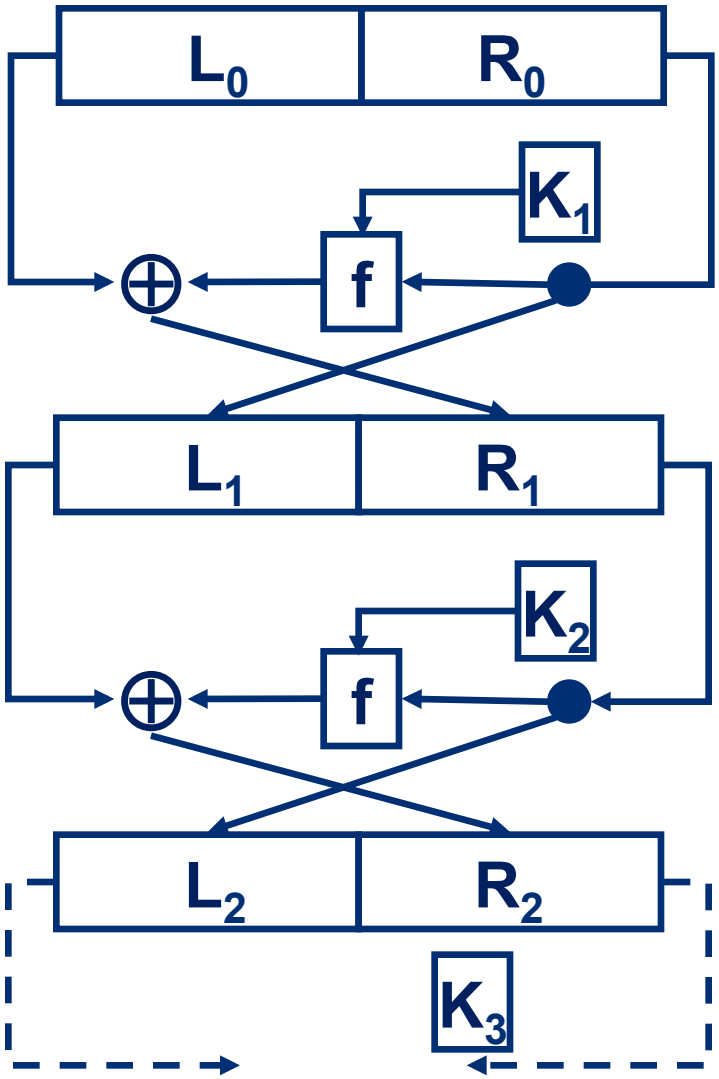
Feistel-Chiffren – eine Runde

$(L_{i-1}, R_{i-1}) \mapsto (L_i, R_i)$, **wobei**

- $L_{i-1}, L_i, R_{i-1}, R_i \in \{0,1\}^t$
- $L_i = R_{i-1}, R_i = L_{i-1} \oplus f(K_i, R_{i-1})$

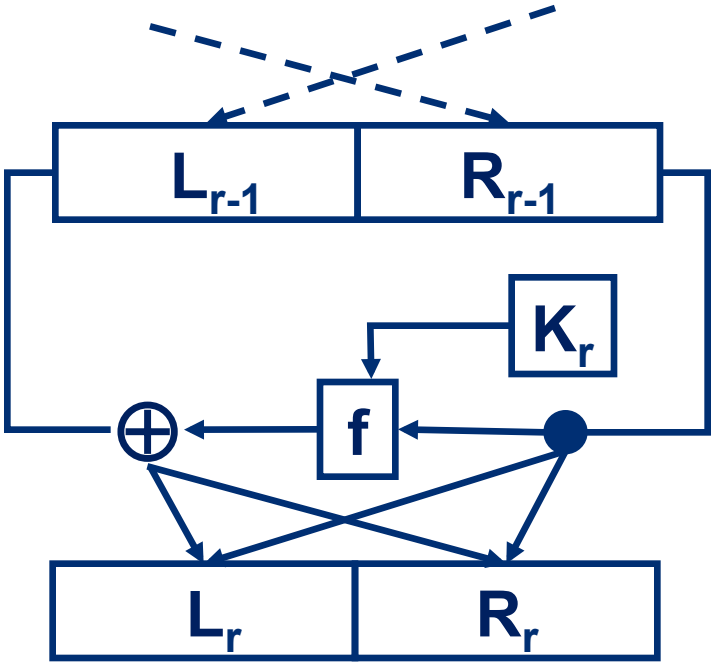


Feistel-Chiffren



Klartext $p=(L_0,R_0)$

Chiffretext $c=(R_r,L_r)$



IV.2 Data Encryption Standard DES

- DES entworfen 1973/74 von NSA und IBM
- 1975 als Standard der NIST festgelegt.
- 1999 DeepCrack bricht DES Schlüssel in 22 Stunden.
- DES wird durch 3DES als Standard ersetzt.
- 2001 wird DES durch AES (Advanced Encryption Standard) als Standard der NIST ersetzt.
- DES in Form von 3DES auch heute noch im Einsatz.

DES - Parameter

DES ist Feistel-Chiffre mit

1. Klartextraum $P = \{0,1\}^{64}$, Chiffretextraum $C = \{0,1\}^{64}$, Schlüssselraum $K \subseteq \{0,1\}^{64}$.

2. Rundenzahl r = 16.

3. Methode zur Erzeugung von Rundenschlüssel
   KeySchedule: $\{0,1\}^{64} \rightarrow \{0,1\}^{16 \cdot 48}$
   $K \mapsto K_1,\ldots,K_{16}$

4. Rundenfunktion $f : \{0,1\}^{48} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$

DES - Schlüsselraum

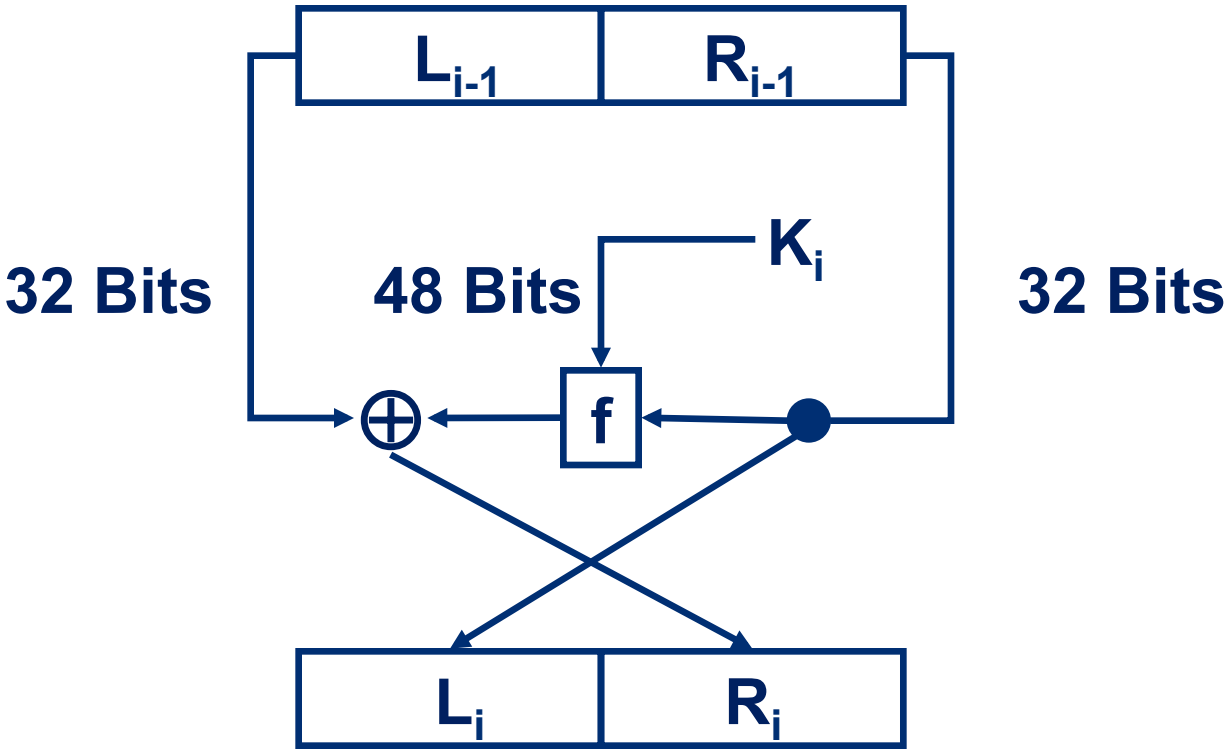
$$K = \left\{ (b_1, \ldots, b_{64}) \in \{0,1\}^{64} : \sum_{i=1}^{8} b_{8u+i} = 1 \mod 2, 0 \le u \le 7 \right\}$$

Damit $|K| = 2^{56}$.

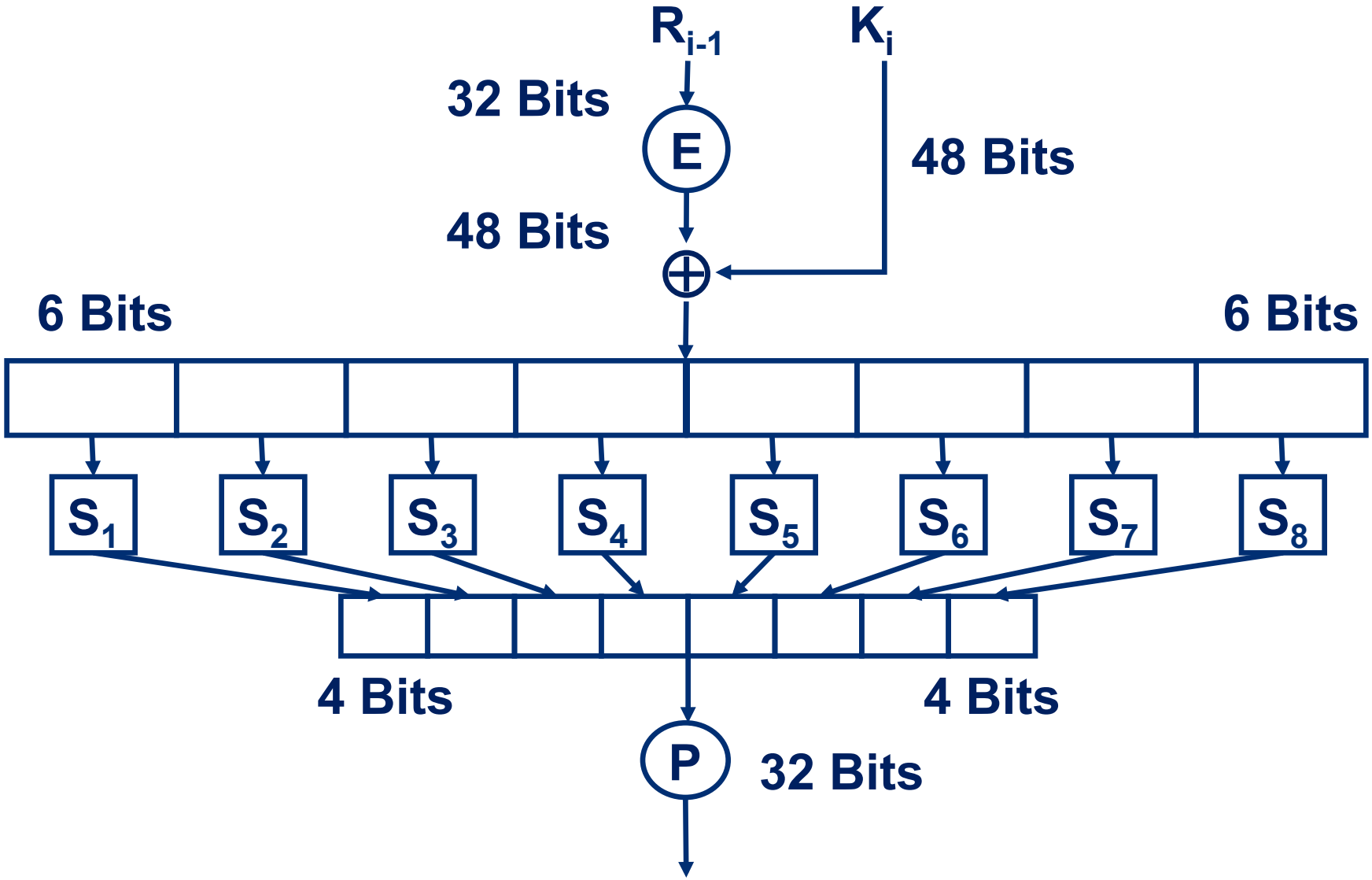
Gültiger DES-Schlüssel

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

DES – eine Runde



DES Rundenfunktion



$$f(K_i,R_{i-1}) = P(S(E(R_{i-1}) \oplus K_i))$$

Expansion und Permutation

Expansion

$$E: \{0,1\}^{32} \rightarrow \{0,1\}^{48}$$
$$R_1 \cdots R_{32} \mapsto R_{32} R_1 \cdots R_{32} R_1$$

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Permutation

$$P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$
$$R_1 \cdots R_{32} \mapsto R_{16} \cdots R_{25}$$

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES S-Boxen

$$S_i: \{0,1\}^6 \rightarrow \{0,1\}^4 \qquad ,i = 1,\ldots,8$$
$$b_1 \ldots b_6 \mapsto S_i(b_1 b_6, b_2 b_3 b_4 b_5)$$

1. Interpretiere $b_1 b_6$ als Zeilenindex, $b_2 b_3 b_4 b_5$ als Spaltenindex.
2. Ausgabe ist Binärdarstellung des Eintrags an Position $(b_1 b_6, b_2 b_3 b_4 b_5)$ der i-ten S-Box.

S_1

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

DES S-Boxen

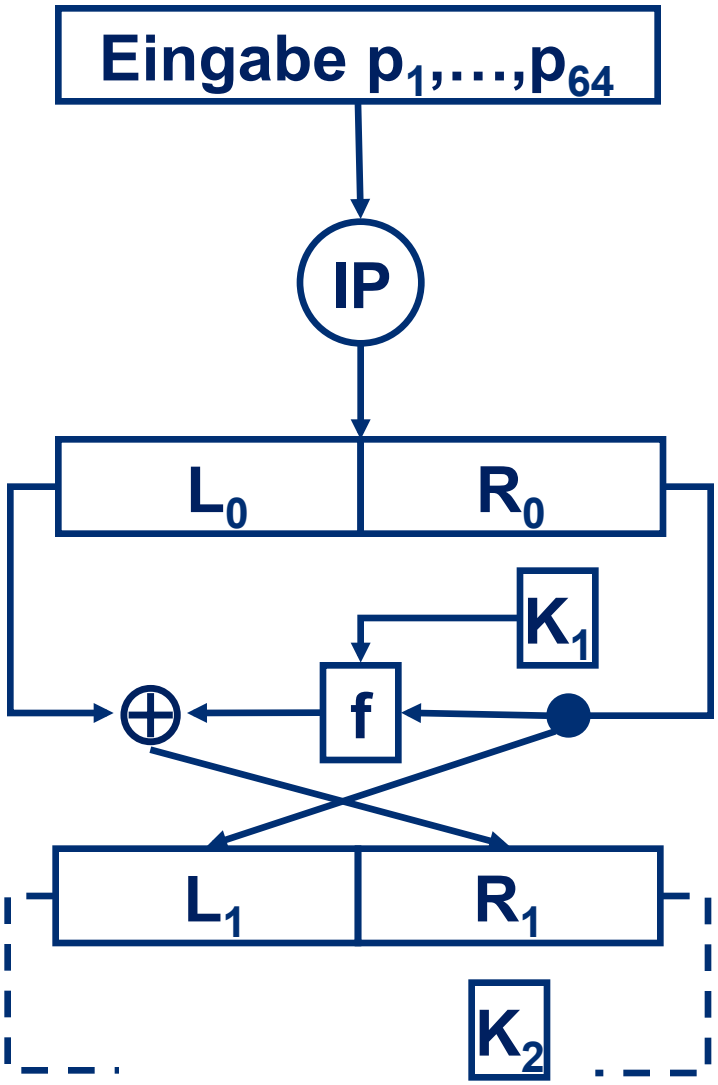
Beispiel $S_1(101101) = S_1(11,0110) = S_1(3,6)$

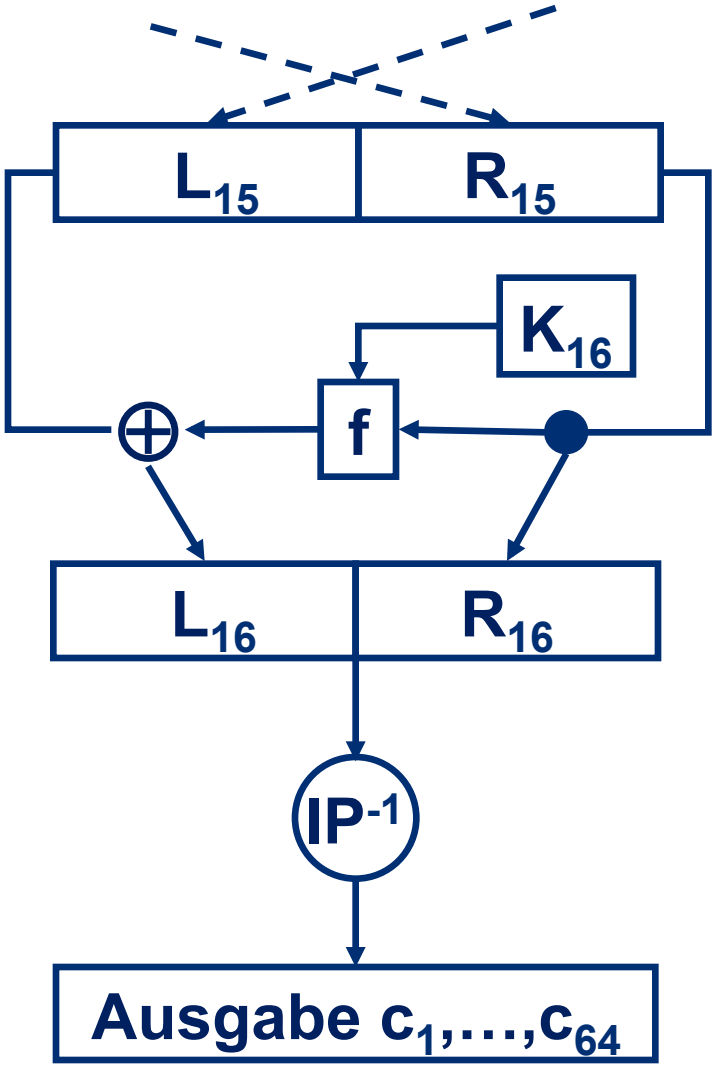
$= 0001$

S_1

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

DES


Eingabe $p_1,\ldots,p_{64}$
IP
L_0
R_0
K_1
f
L_1
R_1
K_2


L_{15}
R_{15}
K_{16}
f
L_{16}
R_{16}
IP^{-1}
Ausgabe $c_1,\ldots,c_{64}$

Initiale Permutation

$$IP: \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$

$$p_1 \cdots p_{64} \mapsto p_{58} p_{50} \cdots p_7$$

$$IP^{-1}: \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$

$$v_1 \cdots v_{64} \mapsto v_{40} v_8 \cdots v_{25}$$

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES – KeySchedule

… ist nicht sehr erhellend!

DES S-Boxen

Lemma 4.1 Für $i = 1,\ldots,8$ und alle $u,v \in \{0,1\}^6$, die sich an genau einer Position unterscheiden, gilt, dass sich $S_i(u)$ und $S_i(v)$ an mindestens zwei Positionen unterscheiden.

Beispiel $i = 1, u = 101101, v = 111101$

$$S_1(u) = 0001, S_1(v) = 0110$$

S_1

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

Permutation P

Lemma 4.2 Betrachte jedes $u \in \{0,1\}^{32}$ als Folge von acht 4-Bitfolgen. Unterscheiden sich u,v an zwei Positionen innerhalb einer 4-Bitfolge, so unterscheiden sich $P(u)$ und $P(v)$ in zwei 4-Bitfolgen.

Beispiel $u = 0^{32}, v = 110^{30}$

$P(u) = 0^{32}$

$P(v) = 0^8 10^7 10^{15}$

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES Diffusion

Diffusion Die Diffusion einer Blockchiffre ist groß, wenn jedes Bit des Klartextes und jedes Bit des Schlüssels möglichst viele Bits des Chiffretexts beeinflusst.

Lemma 4.1 Für $i = 1,\ldots,8$ und alle $u,v \in \{0,1\}^6$, die sich an genau einer Position unterscheiden, gilt, dass sich $S_i(u)$ und $S_i(v)$ an mindestens zwei Positionen unterscheiden.

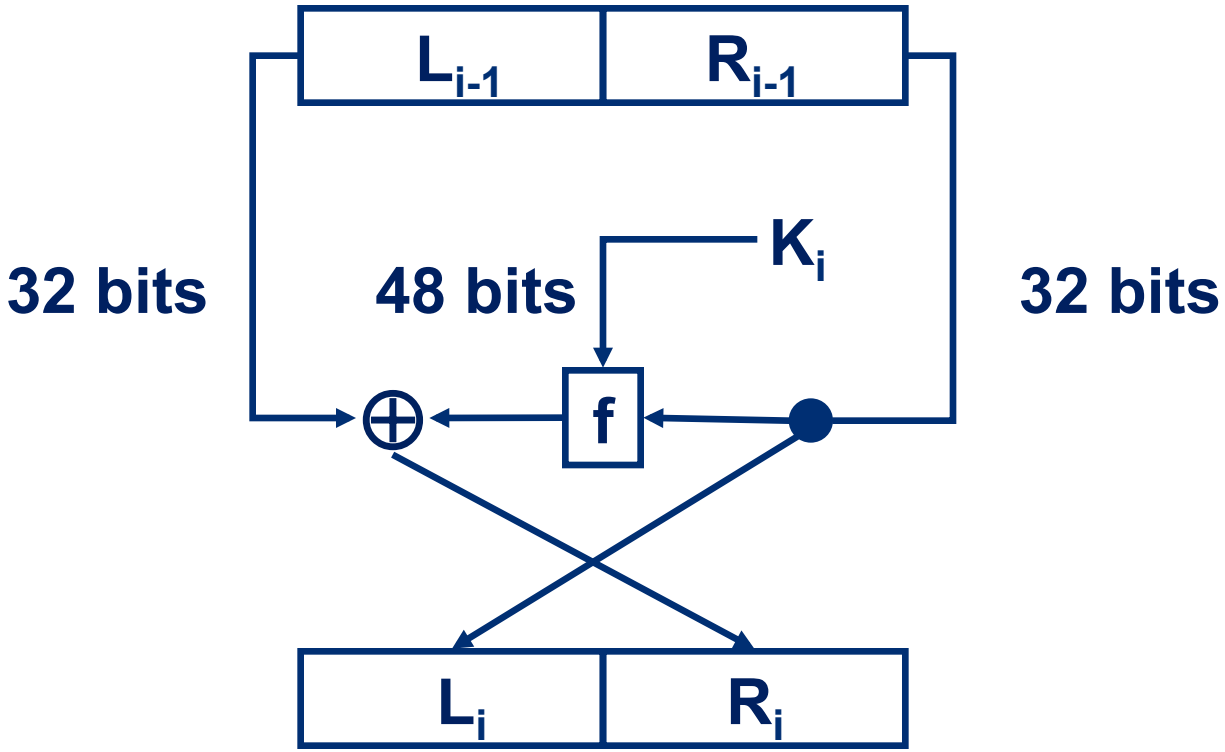
Lemma 4.2 Betrachte jedes $u \in \{0,1\}^{32}$ als Folge von acht 4-Bitfolgen. Unterscheiden sich u,v an zwei Positionen innerhalb einer 4-Bitfolge, so unterscheiden sich $P(u)$ und $P(v)$ in zwei 4-Bitfolgen.

Diffusion und der Lawinneneffect in DES

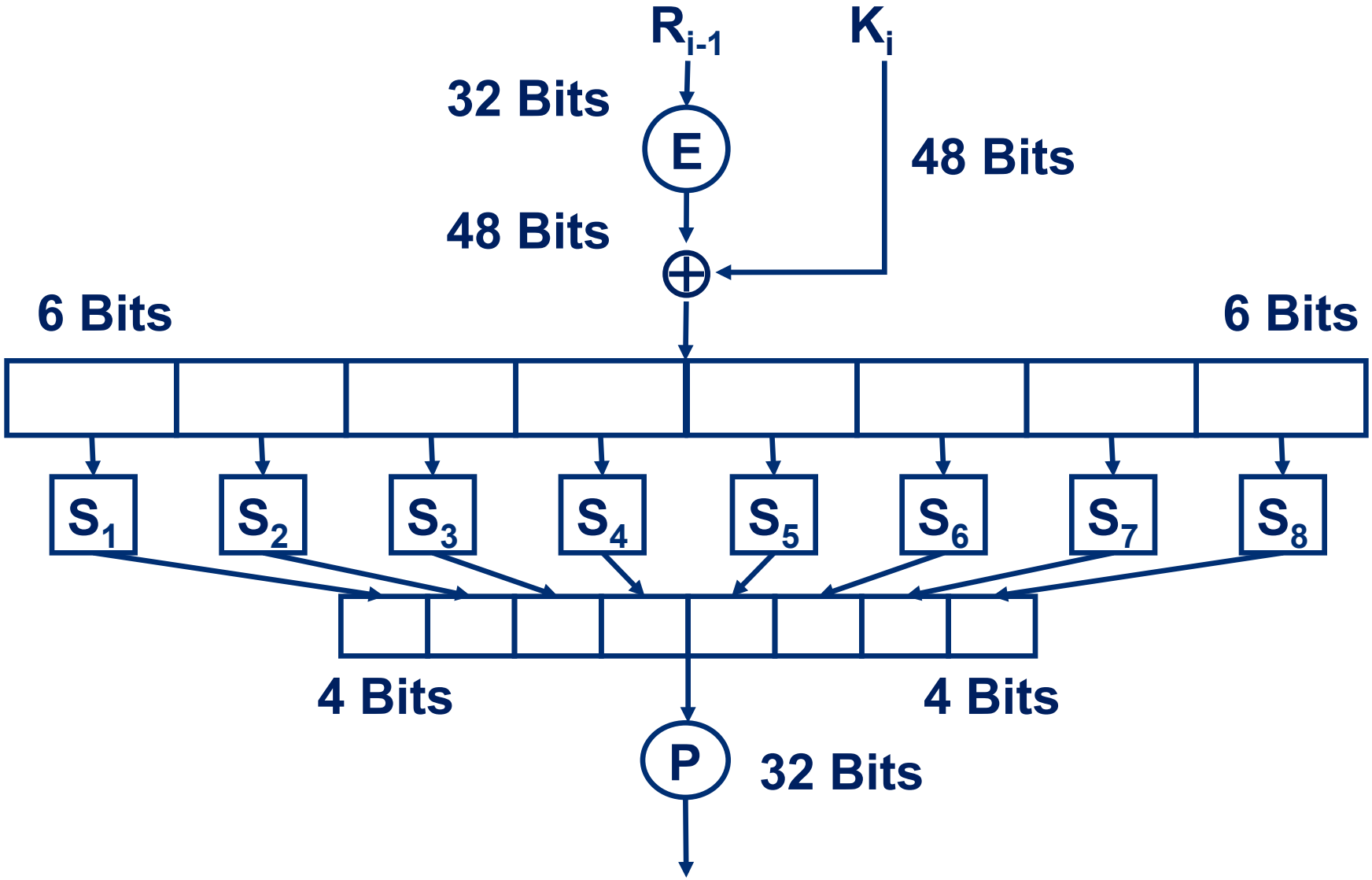
Klartexte p und p´ unterscheiden sich an Δ=1 Positionen, Unterschied in der linken Hälfte

Δ=1	Δ=0	Eingabe
Δ=0	Δ=1	nach Runde 1
Δ=1	Δ=2	nach Runde 2
Δ=2	Δ=4	nach Runde 3
Δ=4	Δ=8	nach Runde 4

DES – eine Runde



DES Rundenfunktion



$$f(K_i,R_{i-1}) = P(S(E(R_{i-1}) \oplus K_i))$$

DES-Entschlüsselung

DES-Entschlüsselung erfolgt wie Verschlüsselung mit Rundenschlüsseln in umgekehrter Reihenfolge.

Beweis Übung.

DES-Varianten

2DES $P = C = \{0,1\}^{64}, K \subseteq \{0,1\}^{64} \times \{0,1\}^{64}$

$k \in K, k = (k_1, k_2)$

$2DES_k(p) = DES_{k_2}(DES_{k_1}(p))$

3DES $P = C = \{0,1\}^{64}, K \subseteq \{0,1\}^{64} \times \{0,1\}^{64} \times \{0,1\}^{64}$

$k \in K, k = (k_1, k_2, k_3)$

$3DES_k(p) = DES_{k_3}(DES^{-1}_{k_2}(DES_{k_1}(p)))$

- 2DES nicht so sicher, wie Schlüssellänge erwarten lässt.
- 3DES gilt immer noch als sicher, ist aber zu langsam.