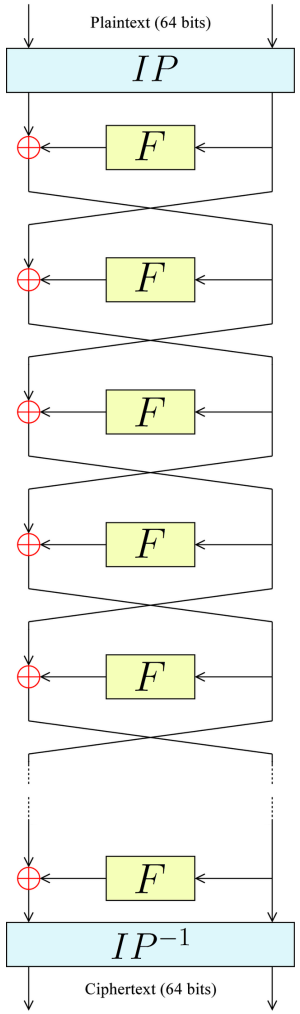
DES S-box 4 is not like the others

Stian Fauskanger

University of Bergen
Department of Informatics
The Selmer Center

October 14, 2014

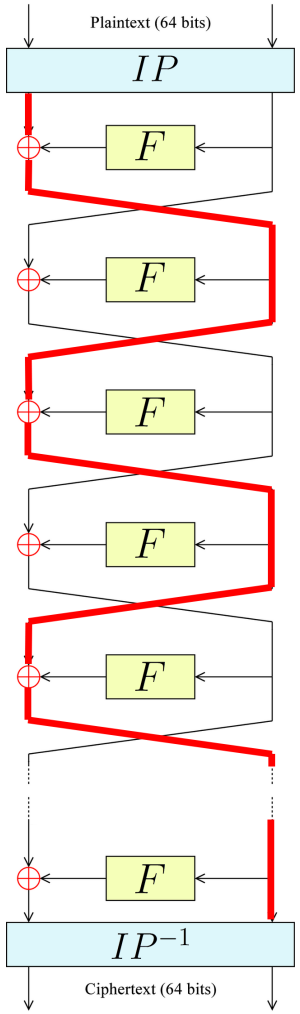
DES



Data Encryption Standard

Image source: Wikipedia.org

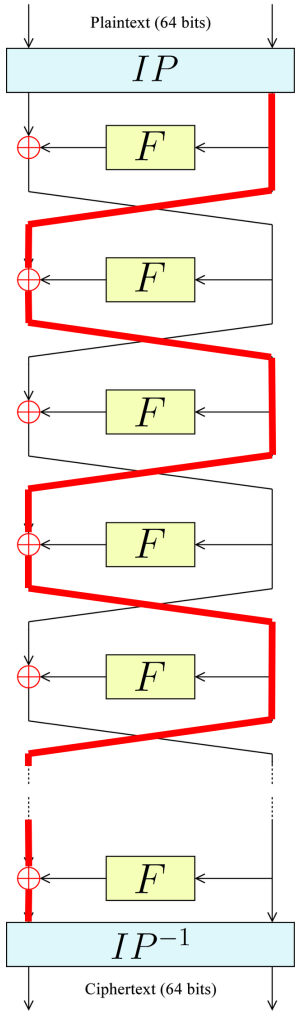
DES



$$C_L = P_H \oplus F_1 \oplus \cdots \oplus F_{15}$$
$$C_H = P_L \oplus F_2 \oplus \cdots \oplus F_{16}$$

Image source: Wikipedia.org

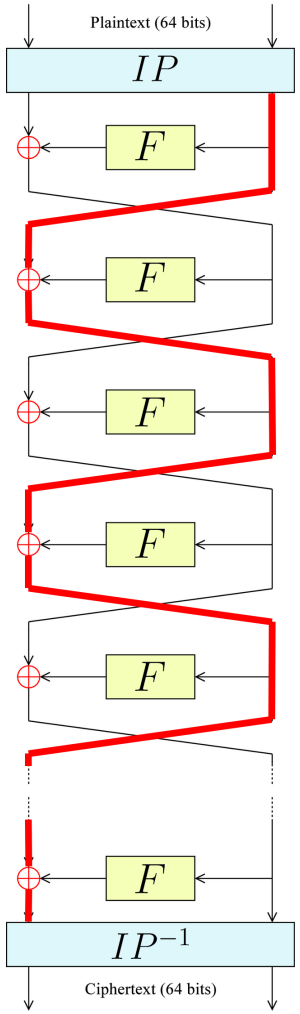
DES



$$C_L = P_H \oplus F_1 \oplus \cdots \oplus F_{15}$$
$$C_H = P_L \oplus F_2 \oplus \cdots \oplus F_{16}$$

Image source: Wikipedia.org

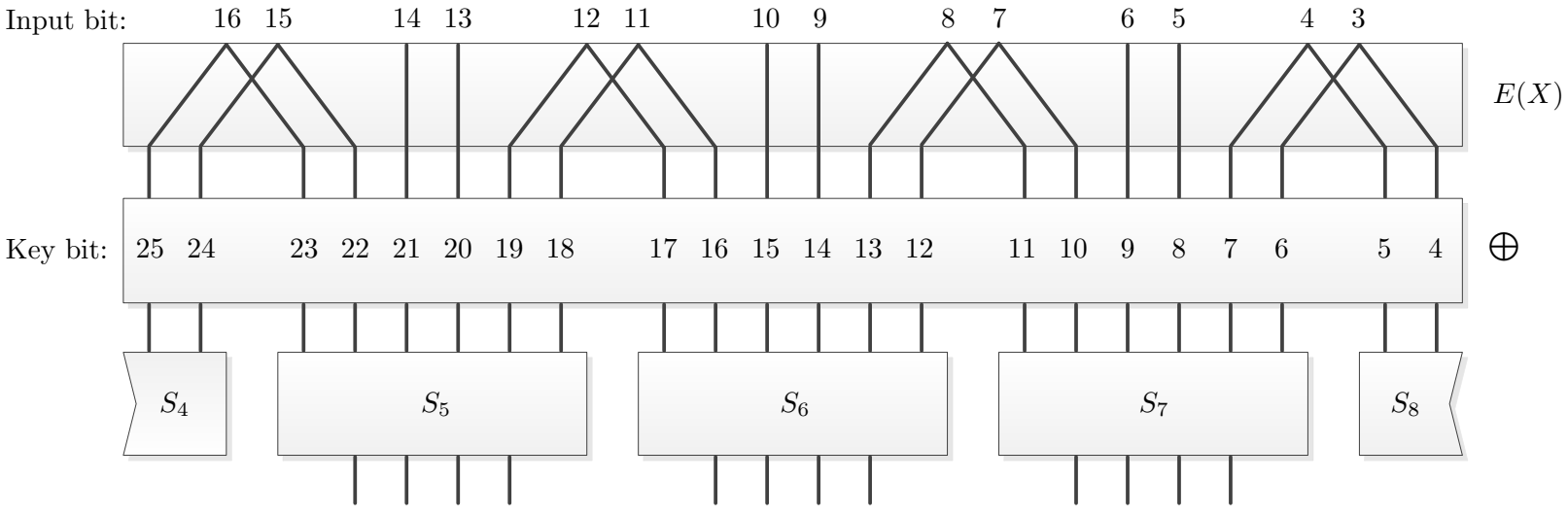
DES



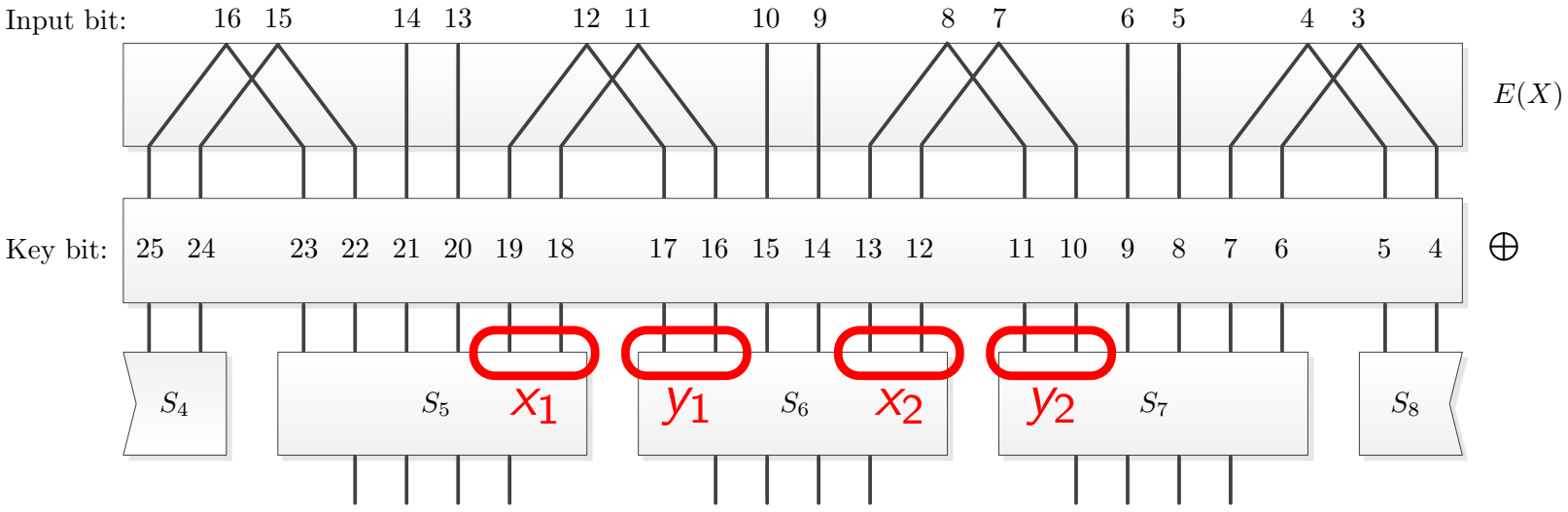
$$C_L \oplus P_H = F_1 \oplus \cdots \oplus F_{15}$$
$$C_H \oplus P_L = F_2 \oplus \cdots \oplus F_{16}$$

Image source: Wikipedia.org

F repeats input-bits to adjacent S-boxes



F repeats input-bits to adjacent S-boxes



$$x_1 \oplus y_1 = k \qquad \text{and} \qquad x_2 \oplus y_2 = k'$$

Distribution on XOR of 8 outputs

$$k_1 k_1' \ldots k_8 k_8' \begin{pmatrix} & rst \\ & \vdots \\ \cdots & x \\ & \end{pmatrix}$$

$$x = \mathbf{Pr}(rst \mid k_1 k_1' \ldots k_8 k_8')$$

Number of different distributions

n	Upper bound	123	234	345	456	567	678	781	812
1	16	16	16	16	16	16	16	16	16
2	40	40	40	40	**24**	40	40	40	40
3	80	80	80	80	**32**	80	80	80	80
4	140	140	140	140	**40**	140	140	140	140
5	224	224	224	224	**48**	224	224	224	224
6	336	336	336	336	**56**	336	336	336	336
7	480	480	480	480	**64**	480	480	480	480
8	660	660	660	660	**72**	660	660	660	660

Rank of distributions

n	Upper bound	123	234	345	456	567	678	781	812
1	6	6	6	6	6	6	6	6	6
2	9	9	9	9	**7**	9	9	9	9
3	13	13	13	13	**8**	13	13	13	13
4	18	18	18	18	**9**	18	18	18	18
5	24	24	24	24	**10**	24	24	24	24
6	31	30	31	29	**11**	31	31	31	31
7	39	36	39	34	**12**	39	39	39	39
8	48	42	48	39	**13**	48	48	48	48

Right and left distribution

An S-box is a mapping $S(x_5, x_4, x_3, x_2, x_1, x_0) = (y_3, y_2, y_1, y_0)$

Definition

The right distribution is the distribution of $(x_1, x_0, y_3, y_2, y_1, y_0)$.

What's special about S-box 4?

Definition

The right distribution is the distribution of $(x_1, x_0, y_3, y_2, y_1, y_0)$.

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

$$\sum_a f_{r_1}(c) f_{r_2}(c \oplus a)$$

What's special about S-box 4?

Definition

The right distribution is the distribution of $(x_1, x_0, y_3, y_2, y_1, y_0)$.

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

$$\sum_a f_{r_1}(c) f_{r_2}(c \oplus a) = \sum_a f_{(r_1 \oplus s)}(c) f_{(r_2 \oplus s)}(c \oplus a)$$

Thanks

Thank you!