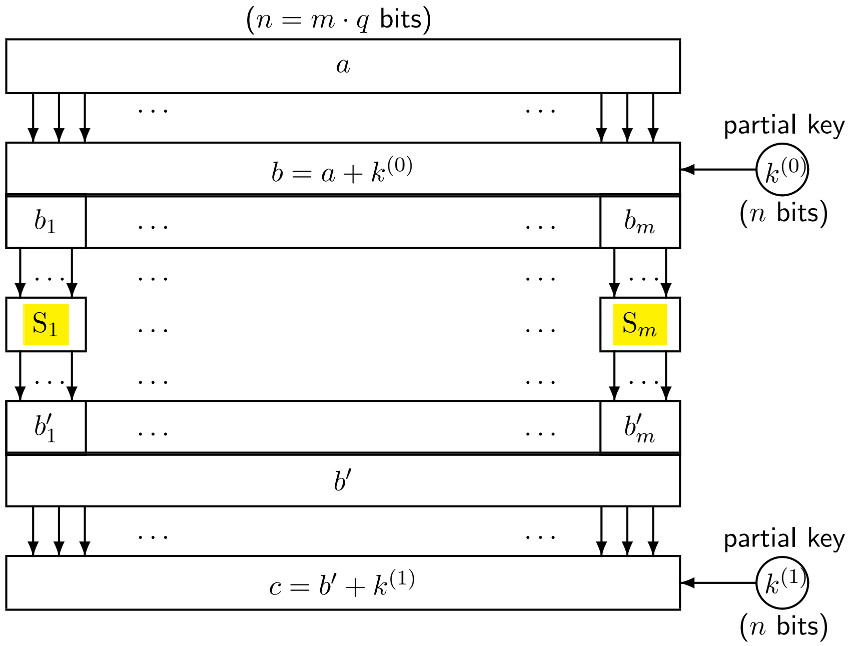

Figure 5.8: Example D, parallel arrangement of m S-boxes $\mathrm{S}_1, \ldots, \mathrm{S}_m$ of width q

5.6 Parallel Arrangement of S-Boxes

The round map of an SP-network usually involves several "small" S-boxes in a parallel arrangement. On order to analyze the effect of this construction we again consider a simple example D, see Figure 5.8.

Proposition 8 *Let* $S_1, \ldots, S_m \colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^q$ *be Boolean maps,* $n = m \cdot q$*, and* f*, the Boolean map*

$$f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n, \;\; f(x_1, \ldots, x_m) = (S_1(x_1), \ldots, S_m(x_m)) \text{ for } x_1, \ldots, x_m \in \mathbb{F}_2^q.$$

Let (α_i, β_i) *for* $i = 1, \ldots, m$ *be linear relations for* S_i *with probabilities* p_i*. Let*

$$\begin{aligned} \alpha(x_1, \ldots, x_m) &= \alpha_1(x_1) + \cdots + \alpha_m(x_m) \\ \beta(y_1, \ldots, y_m) &= \beta_1(y_1) + \cdots + \beta_m(y_m) \end{aligned}$$

Then (α, β) *is a linear relation for* f *with probability* p *given by*

$$2p - 1 = (2p_1 - 1) \cdots (2p_m - 1).$$

Proof. We consider the case $m = 2$ only; the general case follows by a simple induction as for Proposition 7.

In the case $m = 2$ we have $\beta \circ f(x_1, x_2) = \alpha(x_1, x_2)$ if and only if

- *either* $\beta_1 \circ \mathrm{S}_1(x_1) = \alpha_1(x_1)$ and $\beta_2 \circ \mathrm{S}_2(x_2) = \alpha_2(x_2)$
- *or* $\beta_1 \circ \mathrm{S}_1(x_1) = 1 + \alpha_1(x_1)$ and $\beta_2 \circ \mathrm{S}_2(x_2) = 1 + \alpha_2(x_2)$.

Hence $p = p_1p_2 + (1-p_1)(1-p_2)$, and the assertion follows as for Proposition 6. $\diamond$

As a consequence the I/O-correlations and the potentials are multiplicative also for a parallel arrangement. At first view this might seem a strengthening of the security, but this appearance is deceiving! We cannot detain the attacker from choosing all linear forms as zeroes except the "best" one. And the zero forms have probabilities $p_i = 1$ and potentials 1. Hence the attacker picks a pair (α_j, β_j) with maximum potential, and then sets $\alpha(x_1, \ldots, x_m) = \alpha_j(x_j)$ and $\beta(y_1, \ldots, y_m) = \beta_j(y_j)$. In a certain sense she turns the other S-boxes, except S_j, "inactive". Then the complete linear relation inherits exactly the probability and the potential of the "active" S-box S_j.

Example

Once again we consider a concrete example with $m = 2$ and $q = 4$, hence $n = 8$. As S-boxes we take the ones from LUCIFER, S_0 at the left, and S_1 at the right, see Figure 5.8. For the left S-box S_0 we take the linear relation with $\alpha \mathrel{\hat{=}} \texttt{0001}$ and $\beta \mathrel{\hat{=}} \texttt{1101}$, that we know has probability $p_1 = \frac{7}{8}$, for the right S-Box S_1 we take the relation $(0,0)$ with probability 1. The combined linear relation for $f = (\mathrm{S}_0, \mathrm{S}_1)$ then also has probability $p = \frac{7}{8}$ and potential $\lambda = \frac{9}{16}$, and we know that linear cryptanalysis with $N = 5$ pairs of plaintext and ciphertext has 95% success probability. We decompose all relevant bitblocks into bits:

plaintext: $a = (a_0, \ldots, a_7) \in \mathbb{F}_2^8$,

ciphertext: $c = (c_0, \ldots, c_7) \in \mathbb{F}_2^8$,

key: $k = (k_0, \ldots, k_{15}) \in \mathbb{F}_2^{16}$ where $(k_0, \ldots, k_7)$ serves as "initial key" (corresponding to $k^{(0)}$ in Figure 5.8), and $(k_8, \ldots, k_{15})$ as "final key" (corresponding to $k^{(1)}$).

Then $\alpha(a) = a_3$, $\beta(c) = c_0 + c_1 + c_3$, and $\kappa(k) = \alpha(k_0, \ldots, k_7) + \beta(k_8, \ldots, k_{15}) = k_3 + k_8 + k_9 + k_{11}$. Hence the target relation is

$$k_3 + k_8 + k_9 + k_{11} = a_3 + c_0 + c_1 + c_3.$$

We use the key $k = \texttt{1001011000101110}$ whose relevant bit is $k_3 + k_8 + k_9 + k_{11} = 1$, and generate five random pairs of plaintext and ciphertext, see Table 5.11. We see that for this example Matsui's algorithm guesses the relevant key bit correctly with no dissentient.

a	a_3	c	$c_0 + c_1 + c_3$	estimate
00011110	1	00000010	0	1
00101100	0	00111111	1	1
10110010	1	01011101	0	1
10110100	1	01010000	0	1
10110101	1	01010111	0	1

Table 5.11: Calculations for example D