index i	0	1	2	3	4	5	6	7
$\mathrm{P}(i)$	2	5	4	0	3	1	7	6

Table 5.12: Lucifer's permutation P

5.7 Mini-Lucifer

As a slightly more complex example we define a toy cipher "Mini-Lucifer" that employs the S-boxes and a permutation of the true Lucifer. Here is the construction, see Figure 5.9:

- Before and after each round map we add a partial key. We use two keys $k^{(0)}$ and $k^{(1)}$ in alternating order. They consist of the first or last 8 bits of the 16 bit master key. In particular for $r \geq 3$ the round keys are not independent.
- The round function consists of a parallel arrangement of the two S-boxes, as in the example of Section 5.6, followed by the permutation P.
- The permutation P maps a single byte (octet) to itself as defined in Table 5.12. As usual for SP-networks we omit it in the last round.

Up to now we ignored permutations in linear cryptanalysis. How do they influence the analysis?

Well, let f be a Boolean map, (α, β), a linear relation for f with probability p, and P, a permutation of the range of f. Then we set $\beta' = \beta \circ \mathrm{P}^{-1}$, a linear form, and immediately see that (α, β') is a linear relation for $\mathrm{P} \circ f$ with the same probability p:

$$\begin{aligned} p &= \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \beta(f(x)) = \alpha(x)\} \\ &= \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid (\beta \circ \mathrm{P}^{-1})(\mathrm{P} \circ f(x)) = \alpha(x)\}. \end{aligned}$$

The assignment $\beta \mapsto \beta'$ simply permutes the linear forms β. In other words: appending a permutation to f permutes the columns of the approximation table, of the correlation matrix, and of the linear profile.

> *Inserting a permutation into the round function of an SP-network affects linear cryptanalysis in a marginal way only.*

We'll verify this assertion for a concrete example, and see how "marginal" the effect really is. By the way the same argument holds if we replace the permutation by a more general bijective linear map L: also $\beta \mapsto \beta \circ \mathrm{L}^{-1}$ permutes the linear forms.

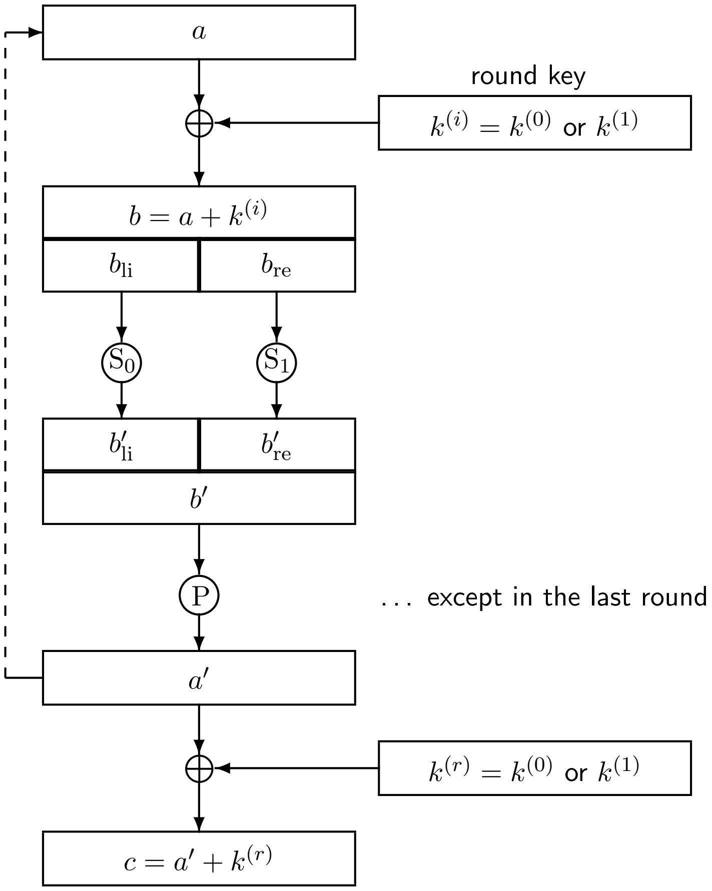

Figure 5.9: Mini-Lucifer

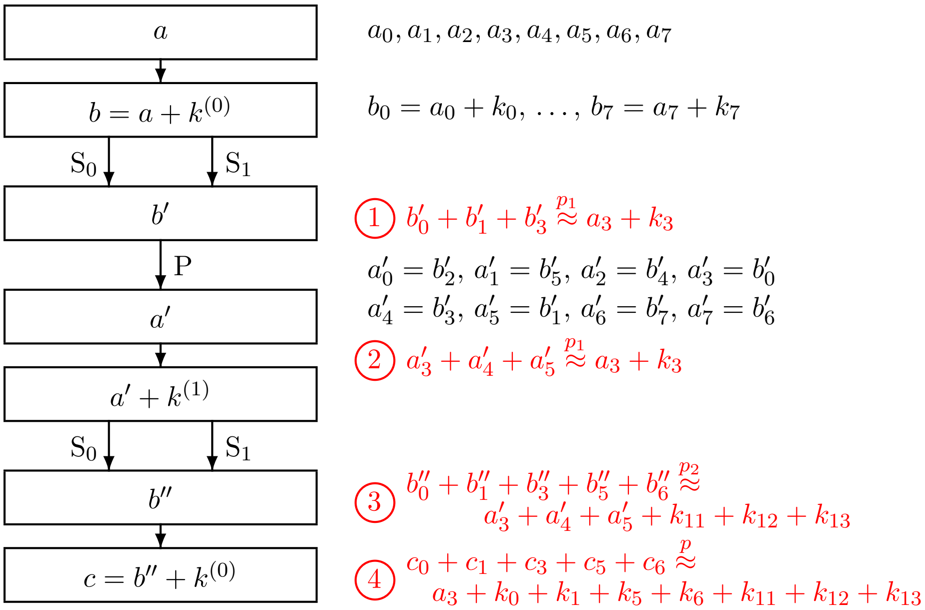
a
$a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7$
$b = a + k^{(0)}$
$b_0 = a_0 + k_0,\ \ldots,\ b_7 = a_7 + k_7$
S_0
S_1
b'
1 $b'_0 + b'_1 + b'_3 \overset{p_1}{\approx} a_3 + k_3$
P
$a'_0 = b'_2,\ a'_1 = b'_5,\ a'_2 = b'_4,\ a'_3 = b'_0$
$a'_4 = b'_3,\ a'_5 = b'_1,\ a'_6 = b'_7,\ a'_7 = b'_6$
a'
2 $a'_3 + a'_4 + a'_5 \overset{p_1}{\approx} a_3 + k_3$
$a' + k^{(1)}$
S_0
S_1
b''
3 $b''_0 + b''_1 + b''_3 + b''_5 + b''_6 \overset{p_2}{\approx}$
$a'_3 + a'_4 + a'_5 + k_{11} + k_{12} + k_{13}$
$c = b'' + k^{(0)}$
4 $c_0 + c_1 + c_3 + c_5 + c_6 \overset{p}{\approx}$
$a_3 + k_0 + k_1 + k_5 + k_6 + k_{11} + k_{12} + k_{13}$

Figure 5.10: Mini-Lucifer with 2 rounds

Example

The concrete example is specified in Figure 5.10. The relation 1, namely

$$\beta(b') \overset{p_1}{\approx} \alpha(a + k^{(0)})$$

holds with probability $p_1 = \frac{7}{8}$ between $\alpha \mathrel{\hat{=}} \texttt{0001}$ and $\beta \mathrel{\hat{=}} \texttt{1101}$. The permutation P transforms it to the relation 2, namely

$$\beta \circ \mathrm{P}^{-1}(a') \overset{p_1}{\approx} \alpha(a + k^{(0)}) = \alpha(a) + \alpha(k^{(0)}).$$

But P also distributes the bits from the left-hand side of the relation over the two S-boxes of the next round. So the cryptanalytic trick of letting only one S-box per round become active works only for the first round.

> *Inserting a permutation into the round function of an SP-network has the effect that linear cryptanalysis has to deal with more than one parallel S-box becoming active in later rounds.*

We'll soon see in the example that this effect reduces the potential. The relevant bits a'_3, a'_4, a'_5, or, after adding the key, $a'_3 + k_{11}$, $a'_4 + k_{12}$, $a'_5 + k_{13}$, split as input to the left S-box S_0 of the second round (namely $a'_3 + k_{11}$), and to the right one, S_1 (namely $a'_4 + k_{12}$ and $a'_5 + k_{13}$).

On the left-hand side, for S_0, the linear form for the input is $\beta'_1 \mathrel{\hat{=}}$ `0001` $\mathrel{\hat{=}} 1$, on the right-hand side, for S_1, we have $\beta'_2 \mathrel{\hat{=}}$ `1100` $\mathrel{\hat{=}} 12$. From the linear profile of S_0 we see that the maximum possible potential for β'_1 is $\lambda'_2 = \frac{9}{16}$ with $p'_2 = \frac{7}{8}$, assumed for $\gamma_1 \mathrel{\hat{=}} 13 \mathrel{\hat{=}}$ `1101`.

For β'_2 the maximum potential is $\lambda''_2 = \frac{1}{4}$. Having two choices we choose $\gamma_2 \mathrel{\hat{=}} 6 \mathrel{\hat{=}}$ `0110` with probability $p''_2 = \frac{3}{4}$. The combined linear relation with $\beta'(x) = \beta'_1(x_0, \ldots, x_3) + \beta'_2(x_4, \ldots, x_7)$ and, on the output side, $\gamma(y) = \gamma_1(y_0, \ldots, y_3) + \gamma_2(y_4, \ldots, y_7)$ has I/O-correlation

$$2p_2 - 1 = (2p'_2 - 1)(2p''_2 - 1) = \frac{3}{8}$$

by Proposition 8, hence $p_2 = \frac{11}{16}$, $\lambda_2 = \frac{9}{64}$.

The relation between $\beta'(a'+k^{(1)})$ and $\gamma(b'')$ is labelled by 3 in Figure 5.10, namely

$$\gamma(b'') \overset{p_2}{\approx} \beta'(a' + k^{(1)}) = \beta'(a') + \beta'(k^{(1)}).$$

Combining 2 and 3 (and cancelling k_3) yields the relation

$$\gamma(c) + \gamma(k^{(0)}) = \gamma(c + k^{(0)}) = \gamma(b'') \overset{p}{\approx} \alpha(a) + \alpha(k^{(0)}) + \beta'(k^{(1)}),$$

labelled by 4 in the figure, whose probability p is given by Proposition 7 since the two round keys are independent. We get

$$2p - 1 = (2p_1 - 1)(2p_2 - 1) = \frac{3}{4} \cdot \frac{3}{8} = \frac{9}{32},$$

whence $p = \frac{41}{64}$. The corresponding potential is $\lambda = \frac{81}{1024}$.

The number N of needed plaintexts for a 95% success probability follows from the approximation in Table 5.4:

$$N = \frac{3}{\lambda} = \frac{1024}{27} \approx 38.$$

Note that there are only 256 possible plaintexts at all.

In the example the success probability derived from the product of the I/O-correlations (or of the potentials) of all active S-boxes. We had luck since in this example the involved partial keys were independent. In the general case this is not granted. Nevertheless the cryptanalyst relies on the empirical evidence and ignores the dependencies, trusting the rule of thumb:

> *The success probability of linear cryptanalysis is (approximately) determined by the multiplicativity of the I/O-correlations (or of the potentials) of all the active S-boxes along the considered path (including all of its ramifications).*

The restriction in this rule of thumb concerns the *success probability* of linear cryptanalysis but not the *course of action.* The cryptanalyst is right if and only if she succeeds, no matter whether her method had an exact mathematical foundation for all details.

Now we obtained a single bit. So what?

Of course we may find more relations, and detect more key bits. However we have to deal with smaller and smaller potentials, and face an increasing danger of hitting a case where the probability for the concrete (target) key lies on the "wrong" side of $\frac{1}{2}$. Moreover we run into a multiple test situation reusing the same known plaintexts several times. This enforces an unpleasant adjustment of the success probabilities.