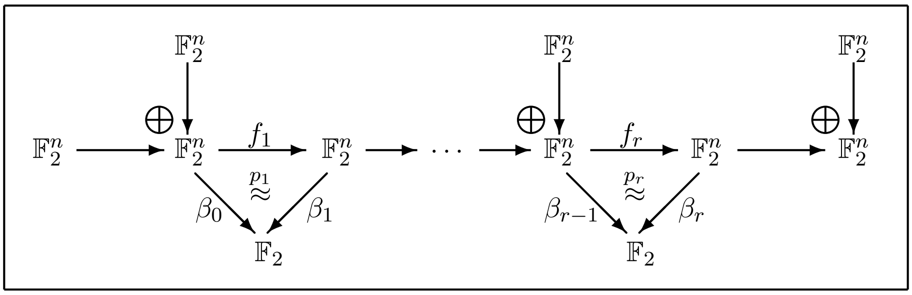

Figure 5.7: Example C

5.5 Linear Paths

Consider the general case where the round map $f\colon \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^n$ is iterated for r rounds with round keys $k^{(i)} \in \mathbb{F}_2^q$, in analogy with Figure 5.5. Let $(\alpha_i, \beta_i, \kappa_i)$ be a linear relation for round i. Let $\alpha_i = \beta_{i-1}$ for $i = 2, \ldots, r$. Set $\beta_0 := \alpha_1$. Then the chain $\beta = (\beta_0, \ldots, \beta_r)$ is called a **linear path** for the cipher.

For a simplified scenario, let's call it example C as a generalization of example B, again we'll derive a useful result on the probabilities. So we consider the special but relevant case where the round keys enter the algorithm in an additive way, see Figure 5.7.

Given a key $k = (k^{(0)}, \ldots, k^{(r)}) \in \mathbb{F}_2^{n\cdot(r+1)}$ we compose the encryption function F successively with the intermediate results

$$a^{(0)} = a \mid b^{(0)} = a^{(0)} + k^{(0)} \mid a^{(1)} = f_1(b^{(0)}) \mid b^{(1)} = a^{(1)} + k^{(1)} \mid \ldots$$

$$b^{(r-1)} = a^{(r-1)} + k^{(r-1)} \mid a^{(r)} = f_r(b^{(r-1)}) \mid b^{(r)} = a^{(r)} + k^{(r)} = c =: F(a,k)$$

The general formula is

$$b^{(i)} = a^{(i)} + k^{(i)} \text{ for } i = 0, \ldots, r,$$

$$a^{(0)} = a \text{ and } a^{(i)} = f_i(b^{(i-1)}) \text{ for } i = 1, \ldots, r.$$

We consider a linear relation

$$\kappa(k) \overset{p}{\approx} \beta_0(a) + \beta_r(c),$$

where

$$\kappa(k) = \beta_0(k^{(0)}) + \cdots + \beta_r(k^{(r)}),$$

and p is the probability

$$p_{F,\beta}(k) = \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \sum_{i=0}^{r} \beta_i(k^{(i)}) = \beta_0(a) + \beta_r(F(a,k))\}$$

that depends on the key k. Denote the mean value of these probabilities over all k by q_r. It depends on $(f_1, \ldots, f_r)$ and on the linear path β:

$$q_r := \frac{1}{2^{n\cdot(r+2)}} \cdot \#\{a, k^{(0)}, \ldots, k^{(r)} \in \mathbb{F}_2^n \mid \sum_{i=0}^{r} \beta_i(k^{(i)}) = \beta_0(a) + \beta_r(F(a,k))\}.$$

Substitute $F(a,k) = a^{(r)} + k^{(r)} = f_r(b^{(r-1)}) + k^{(r)}$ into the defining equation of this set. Then $\beta_r(k^{(r)})$ cancels out, and we see that the count is independent of $k^{(r)}$. The remaining formula is

$$q_r = \frac{1}{2^{n\cdot(r+1)}} \cdot \#\{a, k^{(0)}, \ldots, k^{(r-1)} \in \mathbb{F}_2^n \mid \sum_{i=0}^{r-1} \beta_i(k^{(i)}) = \beta_0(a) + \beta_r(f_r(b^{(r-1)}))\}.$$

In this formula the probability p_r is hidden: We have

$$\beta_r(f_r(b^{(r-1)})) = \begin{cases} \beta_{r-1}(b^{(r-1)}) & \text{with probability } p_r, \\ 1 + \beta_{r-1}(b^{(r-1)}) & \text{with probability } 1 - p_r, \end{cases}$$

where "with probability p_r" means: in $p_r \cdot 2^{n\cdot(r+1)}$ of the $2^{n\cdot(r+1)}$ possible cases. Hence

$$\begin{aligned} q_r &= \frac{1}{2^{n\cdot(r+1)}} \cdot \Big[p_r \cdot \#\{a, k^{(0)}, \ldots, k^{(r-1)} \mid \sum_{i=0}^{r-1} \beta_i(k^{(i)}) = \beta_0(a) + \beta_{r-1}(b^{(r-1)})\} \\ &\quad + (1 - p_r) \cdot \#\{a, k^{(0)}, \ldots, k^{(r-1)} \mid \sum_{i=0}^{r-1} \beta_i(k^{(i)}) = 1 + \beta_0(a) + \beta_{r-1}(b^{(r-1)})\} \Big] \\ &= p_r \cdot q_{r-1} + (1 - p_r) \cdot (1 - q_{r-1}), \end{aligned}$$

for the final counts exactly correspond to the probabilities for $r - 1$ rounds.

This is the perfect entry to a proof by induction, showing:

Proposition 7 (Matsuis Piling-Up Theorem) *In example C the mean value $p_{F,\beta}$ of the probabilities $p_{F,\beta}(k)$ over all keys $k \in \mathbb{F}_2^{n(r+1)}$ fulfills*

$$2p_{F,\beta} - 1 = \prod_{i=1}^{r} (2p_i - 1).$$

In particular the I/O-correlations and the potentials are multiplicative.

Proof. The induction starts with the trivial case $r = 1$ (or with the case $r = 2$ that we proved in Proposition 6).

From the previous consideration we conclude

$$2q_r - 1 = 4p_r q_{r-1} - 2p_r - 2q_{r-1} + 1 = (2p_r - 1)(2q_{r-1} - 1),$$

and the assertion follows by induction on r. $\diamond$

For real ciphers in general the round keys are *not* independent but derive from a “master key” by a specific key schedule. In practice however this effect is negligeable. The method of linear cryptanalysis follows the rule of thumb:

> *Along a linear path the potentials are multiplicative.*

Proposition 7, although valid only in a special situation and somewhat imprecise for real life ciphers, gives a good impression of how the cryptanalytic advantage (represented by the potential) of linear approximations decreases with an increasing number of rounds; note that the product of numbers smaller than 1 (and greater than 0) decreases with the number of factors. This means that the security of a cipher against linear cryptanalysis is the better, the more rounds it involves.