Chapter 5

Cryptanalysis of Bitblock Ciphers

For cryptanalyzing bitblock ciphers we know some basic approaches:

1. exhaustion = brute-force searching the complete key space
2. algebraic attack, see Chapter 2
3. statistical attacks against hidden linearity:
    (a) linear cryptanalysis (Matsui/Yamagishi 1992), the subject of the following sections
    (b) differential cryptanalysis (Murphy, Shamir, Biham 1990)
    (c) generalizations and mixtures of (a) and (b)

Differential cryptanalysis was known at IBM and NSA already in 1974 when designing DES. In contrast apparently linear cryptanalysis—though conceptually simpler—was unknown to the designers of DES. Accordingly the resistance of DES against linear cryptanalysis is suboptimal. However an important design criterion was:

- *The S-boxes should be as nonlinear as possible.*

In the following years many people developed generalizations and combinations of linear and differential cryptanalysis:

- related keys attack (Biham 1992, Schneier)
- differentials of higher order (Harpes 1993, Biham 1994, Lai 1994)
- differential-linear cryptanalysis (Langford/Hellman 1994)
- partial differentials (Knudsen 1995)

- I/O-sum analysis (Harpes/Kramer/Massey 1995)
- S-box-pair analysis (Davies/Murphy 1995, Mirza 1996)
- boomerang attack (Wagner 1999)
- slide attack against (maybe hidden) periodicity in ciphers or key schedules (Biryukov/Wagner 1999)
- impossible differentials (Biham/Biryukov/Shamir 1999)

All these statistical attacks—including linear and differential cryptanalysis—hardly break a cipher in the sense of classical cryptanalysis. They usually assume lots of known plaintexts, much more than an attacker could gather in a realistic scenario. Therefore a more adequate term is "analysis" instead of "attack". The analyses make sense for finding measures for some partial aspects of security of bitblock ciphers. They measure security for example by the number of known plaintext blocks needed for the attack. If a cipher resists an attacker even with exaggerated assumptions on her capabilities, then we feel safe to trust it in real life.

Given an SP-network the analysis starts with the nonlinear components of the single rounds, in particular with the S-boxes. The next step extends the potential attack over several rounds. This shows how the cost of the attack grows with the number of rounds. In this way we find criteria for the number of rounds for which the cipher is "secure"—at least from this special attack.

By the way we should never forget that the attack always relates to a certain fixed algebraic structure; in most cases to the structure of the plaintext space as a vector space over $\mathbb{F}_2$. Of course a similar attack could relate to another structure. A seemingly complex map could look simple if considered with the structure as cyclic group $\mathbb{Z}/n\mathbb{Z}$ in mind—or even with "exotic" structures invented for the analysis of this single map. In the following however we only consider the structure as a vector space over $\mathbb{F}_2$, the structure that is best understood.

Security Criteria for Bitblock Ciphers

To escape attacks bitblock ciphers, or their round maps, or their S-boxes, should fulfill some requirements. For background theory see the mathematical Appendix D.

- **Balance** All preimages have the same number of elements, or in other words, the values of the map are uniformly distributed. Irregularities of the distribution would provide hooks for statistical cryptanalysis.

- **Diffusion/avalanche effect** If a single plaintext bit changes, about 50% of the ciphertext bits change. This effect conceals similarity of plaintexts.

- **Algebraic complexity** The determination of preimages or parts thereof should lead to equations whose solution is as difficult as possible. This requirement is related to the algebraic degree of the map, but only in an indirect way. A suitable measure is "algebraic immunity".

- **Nonlinearity** We know several criteria that measure linearity, also "hidden" linearity, and are relatively easy to describe and to handle. For example they quantify how susceptible Boolean maps are for linear or differential cryptanalysis.

  - The "linear potential" should be as low as possible, the "linear spectrum" (or "linear profile") as balanced as possible.
  - The "differential potential" should be as low as possible, the "differential spectrum" (or "differential profile") as balanced as possible.
  - The "nonlinearity" (in a narrow sense as the HAMMING distance from affine maps) should be as large as possible.
  - The "linearity distance", the HAMMING distance from maps with "linear structure", should be as large as possible.

Some of these criteria are compatible with each other, some criteria contradict other ones. Therefore the design of a bitblock cipher requires a balance between different criteria. Instead of optimizing a map for a single criterion the designer should aim at a uniformly high level for all criteria.

Cipher designers usually decide the conflict between balance and nonlinearity in favour of balance. But there is no really convincing reason for this—the psychological reason seems to be that statistical attacks that use the nonuniform distribution of the output of non-balanced maps are easier to understand and therefore taken more seriously. The trade-off for nonlinearity is then handled by increasing the number of rounds.

In this section we freely use the notations and results from the mathematical appendices A to E—often without explicit reference.

5.1 The Idea of Linear Cryptanalysis

Consider a bitblock cipher F of block length n and key length l,

$$F\colon \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n.$$

Imagine the arguments of F as plain texts $a \in \mathbb{F}_2^n$ and keys $k \in \mathbb{F}_2^l$, the values of F as cipher texts $c \in \mathbb{F}_2^n$. A **linear relation** between a plaintext $a \in \mathbb{F}_2^n$, a key $k \in \mathbb{F}_2^l$, and a ciphertext $c = F(a,k) \in \mathbb{F}_2^n$ is described by three linear forms

$$\alpha\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2, \quad \beta\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2, \quad \text{and} \quad \kappa\colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2$$

as an equation

$$\kappa(k) = \alpha(a) + \beta(c). \tag{1}$$

If $I = (i_1, \ldots, i_r)$ is the index set that corresponds to the linear form κ—that is $\kappa(k) = k_{i_1} + \cdots + k_{i_r}$—, then writing (1) more explicitly we get an equation for the sum of the involved key bits $k_{i_1}, \ldots, k_{i_r}$:

$$k_{i_1} + \cdots + k_{i_r} = \alpha(a) + \beta(c),$$

For an attack with known plaintext a this reduces the number of unknown key bits to $l-1$ by elimination of one of these bits.

In general the odds of the relation (1) for concrete random values of k, a, and c are about fifty-fifty: both sides evaluate to 0 or 1 with probability $\frac{1}{2}$. Best for security is a frequency of 50% plaintexts a that make the relation true for a fixed key k, where $c = F(a,k)$ is the corresponding ciphertext. This would make the relation indistinguishable from a pure accidental one. If the probability of the relation,

$$p_{F,\alpha,\beta,\kappa}(k) := \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \kappa(k) = \alpha(a) + \beta(F(a,k))\},$$

is conspicuously larger than $\frac{1}{2}$, this reveals a biased probability for the values of the bits of k, and would result in a small advantage for the cryptanalyst. If on the other hand the probability is noticeably smaller than $\frac{1}{2}$, then the complementary relation $\kappa(k) = \alpha(a) + \beta(c) + 1$ is true more often than by pure chance. This also is a weakness. Because the situation concerning the deviation of the probabilities from the ideal value $\frac{1}{2}$ is symmetric (and because the I/O-correlation and the potential are multiplicative, see Proposition 6) it makes sense to consider symmetric quantities, the **input-output correlation**:

$$\tau_{F,\alpha,\beta,\kappa}(k) := 2p_{F,\alpha,\beta,\kappa}(k) - 1$$

(in short: I/O-correlation) and the **potential** of a linear relation:

$$\lambda_{F,\alpha,\beta,\kappa}(k) := \tau_{F,\alpha,\beta,\kappa}(k)^2.$$

The I/O-correlation takes values between -1 and 1. It is the correlation of two Boolean functions on $\mathbb{F}_2^n$, namely $\alpha + \kappa(k)$ and $\beta \circ F_k$. (For fixed k the value of $\kappa(k)$ is constant, i. e. 0 or 1.) The first of these functions picks input bits, the second one, output bits. In general the correlation of Boolean functions $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is the difference

$$c(f,g) := \frac{1}{2^n} \cdot [\#\{x \in \mathbb{F}_2^n \mid f(x) = g(x)\} - \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}] \,.$$

The potential takes values between 0 and 1, and measures the deviation of the probability from $\frac{1}{2}$. In the best case it is 0, in the worst, 1. This "bad" extreme case would provide an exact and directly useable relation for the key bits. Figure 5.1 illustrates the connection.

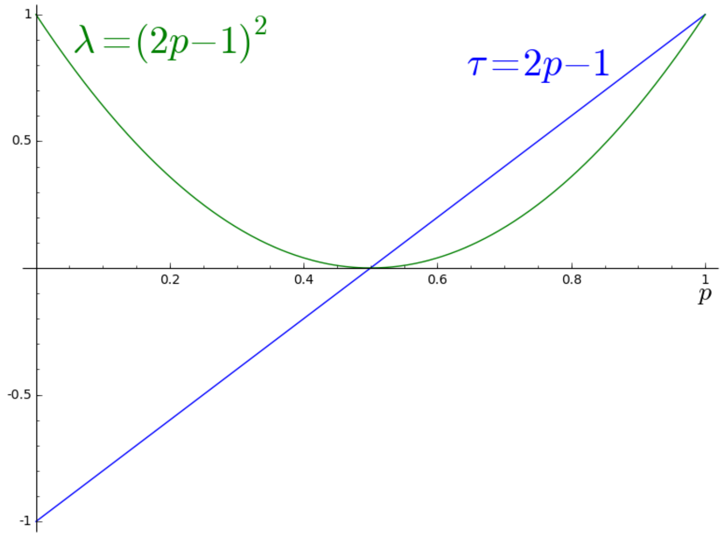

Figure 5.1: Connection between probability p, I/O-correlation τ, and potential λ

Note that the key k is the target of the attack. As long as it is unknown, the value of $p_{F,\alpha,\beta,\kappa}(k)$ is also unknown. Thus for cryptanalysis it makes sense to average the probabilities of a linear relation over all keys:

$$p_{F,\alpha,\beta,\kappa} := \frac{1}{2^{n+l}} \#\{(a,k) \in \mathbb{F}_2^n \times \mathbb{F}_2^l \mid \kappa(k) = \alpha(a) + \beta(F(a,k))\}. \qquad (2)$$

This average probability is determined by the definition of the cipher F alone, at least theoretically, neglecting efficiency. Calculating it however amounts to an exhaustion of all plaintexts and keys, and thus is unrealistic for a realistic cipher with large block lengths. We extend the definition for the "average case" also to I/O-correlation and potential:

$$\tau_{F,\alpha,\beta,\kappa} := 2p_{F,\alpha,\beta,\kappa} - 1,$$

$$\lambda_{F,\alpha,\beta,\kappa} := \tau^2_{F,\alpha,\beta,\kappa}.$$

Note that the I/O-correlation is also a mean value, but the potential is not!

SHAMIR already in CRYPTO 85 noticed that the S-boxes of DES admit linear relations with conspicuous probabilities. However it took another seven years until MATSUI (after first attempts by GILBERT and CHASSÉ 1990 with the cipher FEAL) succeeded in making systematic use of this observation. For estimating $\kappa(k)$ he proceeded as follows (in the case $p_{F,\alpha,\beta,\kappa} > \frac{1}{2}$; in the case $p_{F,\alpha,\beta,\kappa} < \frac{1}{2}$ take the bitwise complement, in the case $p_{F,\alpha,\beta,\kappa} = \frac{1}{2}$ the method is useless):

1. **Collect** N pairs of plaintexts and corresponding ciphertexts $(a_1, c_1), \ldots, (a_N, c_N)$.
2. **Count** the number
$$t := \#\{i = 1, \ldots, N \mid \alpha(a_i) + \beta(c_i) = 0\}.$$
3. **Decide** by majority depending on t:
   - If $t > \frac{N}{2}$, estimate $\kappa(k) = 0$.
   - If $t < \frac{N}{2}$, estimate $\kappa(k) = 1$.

The case $t = \frac{N}{2}$ is worthless, however scarce—we might randomize the decision between 0 and 1.

If we detect a linear relation whose probability differs from $\frac{1}{2}$ in a sufficient way, then this procedure will have a good success probability for sufficiently large N. This allows to reduce the number of unknown key bits by 1, applying elimination.

As a theoretical result from these considerations we'll get a connection between the number N of needed plaintext blocks and the success probability, see Table 5.4.

The more linear relations with sufficiently high certainty the attacker finds, the more she can reduce the size of the remaining key space until finally an exhaustion becomes feasible. A concrete example in Section 5.7 will illustrate this.

Example

For a concrete example with $n = l = 4$ we consider the BOOLEAN map f that is given by the values in Table 5.1—by the way this is the S-box S_0 of LUCIFER—and define the bitblock cipher

$$F\colon \mathbb{F}_2^4 \times \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4 \quad \text{by } F(a,k) := f(a+k).$$

x	$y = f(x)$	x_4	$y_1 + y_2 + y_4$
0 0 0 0	1 1 0 0	0	0
0 0 0 1	1 1 1 1	1	1
0 0 1 0	0 1 1 1	0	0
0 0 1 1	1 0 1 0	1	1
0 1 0 0	1 1 1 0	0	0
0 1 0 1	1 1 0 1	1	1
0 1 1 0	1 0 1 1	0	0
0 1 1 1	0 0 0 0	1	0
1 0 0 0	0 0 1 0	0	0
1 0 0 1	0 1 1 0	1	1
1 0 1 0	0 0 1 1	0	1
1 0 1 1	0 0 0 1	1	1
1 1 0 0	1 0 0 1	0	0
1 1 0 1	0 1 0 0	1	1
1 1 1 0	0 1 0 1	0	0
1 1 1 1	1 0 0 0	1	1

Table 5.1: An S-box for $f\colon \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$ and two linear forms (the S-box S_0 of Lucifer)

a	$a+k$	c	$\alpha(a)$	$\beta(c)$	$\alpha(a) + \beta(c)$
0010	1010	0011	0	1	1
0101	1101	0100	1	1	0
1010	0010	0111	0	0	0

Table 5.2: Estimating a key bit after Matsui

We encrypt using the key $k = \texttt{1000}$ (that we'll attack later as a test case). For a linear relation we consider the linear forms

$$\alpha(a) = a_4, \quad \beta(c) = c_1 + c_2 + c_4, \quad \kappa(k) = k_4.$$

In Section 5.2 we'll see that with these linear forms the relation $\kappa(k) = \alpha(a)+\beta(c)$ for F has a quite large probability. Table 5.2 shows the ciphertexts belonging to three plaintexts a (that later we'll assume as known plaintexts). The values of c are taken from Table 5.1. The number t of observed values 0 of $\alpha(a) + \beta(c)$ is $t = 2$. Hence the majority decision gives the estimate $k_4 = 0$ (being in cheat mode we know it's correct).

How successful will this procedure be in general? We have to analyse the problems:

1. How to find linear relations of sufficiently high probabilities?

2. Since in general bitblock ciphers consist of several rounds we ask:

   (a) How to find useful linear relations for the round function of an iterated bitblock cipher?

   (b) How to combine these over the rounds as a linear relation for the complete cipher?

   (c) How to calculate the probability of a combined linear relation for the complete cipher from the probabilities for the single rounds?

The answer to the first question and part (a) of the second one is: from the linear spectrum, see Section 5.3, that is by Fourier analysis, see Appendix D. The following partial questions lead to the analysis of linear paths, see Section 5.5, and the cumulation of probabilities, see Proposition 7. For (c) finally we only find a coarse rule of thumb.

Fourier analysis is quite efficient if the cost (time and space) is considered as function of the input size. Unfortunately this grows exponentially with the dimension. Therefore Fourier analysis soon becomes infeasible for dimensions more than 10. For serious block ciphers we have dimensions, or block and key sizes, of 64 or 128 bits, far out of reach.

At first sight this objection concerns also question 2 (a). However the single rounds usually consist of processing much smaller pieces, the S-boxes, in parallel. Hence one tries to reduce the problem to the analysis of the S-boxes, and this is feasible: Even AES uses S-boxes of dimension 8 only.

$$\begin{tikzcd}
 & \mathbb{F}_2^n \arrow[d, "\oplus"'] & & & k \arrow[d, mapsto] & \\
\mathbb{F}_2^n \arrow[r] & \mathbb{F}_2^n \arrow[r, "f"] & \mathbb{F}_2^n & a \arrow[r, mapsto] & b \arrow[r, mapsto, "\boxed{\mathrm{S}}" description] & c
\end{tikzcd}$$

Figure 5.2: A (much too) simple example—The graphics here and later represent the map f sometimes by the S-box S in the elementwise assignments.

5.2 Example A: A One-Round-Cipher

We consider examples that are much too simple for real world applications but illustrate the principles of linear cryptanalysis in an easily intelligible way. We always assume round functions of the type $f(a+k)$, that is we add the key—or an n-bit part of it—to the plaintext before applying a bijective S-box $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$. This is a quite special method of bringing the key into play but nevertheless realistic. The paradigmatic sample ciphers LUCIFER, DES, and AES do so, the term used with AES [1] is “key-alternating cipher structure”.

The simplest model is encryption by the formula

$$c = f(a+k),$$

see Figure 5.2. This example is pointless because one block of known plaintext gives a solution for k:

$$k = f^{-1}(c) + a.$$

Note that the attacker knows the inverse map f^{-1} that is part of the decryption algorithm. (One-way encryption methods that assume that f^{-1} is not efficiently deducible from f are the subject of another part of cryptography, see Part III, Chapter 6, of these lecture notes.)

The somewhat more involved example A stops this attack:

$$c = f(a + k^{(0)}) + k^{(1)}$$

(see Figure 5.3). This is the simplest example for which the method of linear cryptanalysis makes sense: Let (α, β) be a pair of linear forms with

$$\beta \circ f(x) \overset{p}{\approx} \alpha(x), \tag{3}$$

where the symbol $\overset{p}{\approx}$ reads as “equal with probability p”, or in other words

$$p = p_{f,\alpha,\beta} := \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \beta \circ f(x) = \alpha(x)\}.$$

$$\begin{tikzcd}
& \mathbb{F}_2^n \arrow[d, "\bigoplus"'] & & \mathbb{F}_2^n \arrow[d, "\bigoplus"'] \\
\mathbb{F}_2^n \arrow[r] & \mathbb{F}_2^n \arrow[r, "f"] & \mathbb{F}_2^n \arrow[r] & \mathbb{F}_2^n \\
& k^{(0)} \arrow[d, mapsto] & & k^{(1)} \arrow[d, mapsto] \\
a \arrow[r, mapsto] & b \arrow[r, mapsto, "\boxed{S}" description] & b' \arrow[r, mapsto] & c
\end{tikzcd}$$

Figure 5.3: Example A

$$\begin{tikzcd}
\mathbb{F}_2^n \arrow[rr, "f"] \arrow[dr, "\alpha"'] & {} \arrow[d, phantom, "\overset{p}{\approx}"] & \mathbb{F}_2^n \arrow[dl, "\beta"] \\
& \mathbb{F}_2 &
\end{tikzcd}$$

Figure 5.4: Diagram for an "approximative" linear relation

The diagram in Figure 5.4 illustrates Formula (3). Note that the linear form κ of the general theory is implicit in the present context: Since the key bits are simply added to plaintext and ("intermediary") ciphertext we have $\kappa = \alpha$ for $k^{(0)}$, and $\kappa = \beta$ for $k^{(1)}$, hence $\kappa(k^{(0)}, k^{(1)}) = \alpha(k^{(0)}) + \beta(k^{(1)})$.

How does this scenario fit the general situation from Chapter 2? In example A we have

- key length $l = 2n$, key space $\mathbb{F}_2^{2n}$, and keys of the form $k = (k^{(0)}, k^{(1)})$ with $k^{(0)}, k^{(1)} \in \mathbb{F}_2^n$.
- The cipher is defined by the map
$$F\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n, \quad (a, k^{(0)}, k^{(1)}) \mapsto f(a + k^{(0)}) + k^{(1)}.$$
- The linear form $\kappa\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is $\kappa(k^{(0)}, k^{(1)}) = \alpha(k^{(0)}) + \beta(k^{(1)})$.

Hence the probability of a linear relation for a fixed key $k = (k^{(0)}, k^{(1)})$ is

$$\begin{aligned}
p_{F,\alpha,\beta,\kappa}(k) &= \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \kappa(k) = \alpha(a) + \beta(F(a,k))\} \\
&= \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \alpha(k^{(0)}) + \beta(k^{(1)}) = \alpha(a) + \beta(f(a + k^{(0)}) + k^{(1)})\} \\
&= \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \alpha(k^{(0)}) = \alpha(a) + \beta(f(a + k^{(0)}))\},
\end{aligned}$$

where we omitted $\beta(k^{(1)})$ that occurs on both sides of the equation inside the curly set brackets.

This expression is independent of $k^{(1)}$, and the slightly rewritten equation

$$p_{F,\alpha,\beta,\kappa}(k) = \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \alpha(a + k^{(0)}) = \beta(f(a + k^{(0)}))\}$$

shows that it assumes the same value for all $k^{(0)}$: With a also $a + k^{(0)}$ runs through all of $\mathbb{F}_2^n$ for a fixed $k^{(0)}$. Therefore this value must agree with the mean value over all k:

$$p_{F,\alpha,\beta,\kappa}(k) = p_{F,\alpha,\beta,\kappa} = \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \alpha(x) = \beta(f(x))\} = p.$$

This consideration shows:

Proposition 3 *In the scenario of example A the probability $p_{F,\alpha,\beta,\kappa}(k)$ assumes the same value*

$$p = \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \alpha(x) = \beta(f(x))\}$$

for all keys $k \in \mathbb{F}_2^{2n}$. In particular p coincides with the mean value from Equation (2)*.*

Using the notations from Figure 5.3 we have

$$\begin{aligned} \beta(c) &= \beta(b' + k^{(1)}) = \beta(b') + \beta(k^{(1)}) \\ &\overset{p}{\approx} \alpha(b) + \beta(k^{(1)}) = \alpha(a + k^{(0)}) + \beta(k^{(1)}) = \alpha(a) + \alpha(k^{(0)}) + \beta(k^{(1)}). \end{aligned}$$

This yields a linear relation for the bits of the key $k = (k_1, k_2)$:

$$\alpha(k^{(0)}) + \beta(k^{(1)}) \overset{p}{\approx} \alpha(a) + \beta(c).$$

Treating the complementary relation

$$\beta \circ f(x) \overset{1-p}{\approx} \alpha(x) + 1$$

in an analoguous way we get:

Proposition 4 *In the scenario of example A let (α, β) be a pair of linear forms for f with probability p as in Formula* (3)*. Then $\hat{p} = \max\{p, 1 - p\}$ is the success probability for determing a single key bit by this linear relation given* one *known plaintext block.*

a	b	b'	c	$\alpha(a) + \beta(c)$
0000	1000	0010	0011	1
0001	1001	0110	0111	1
0010	1010	0011	0010	0
0011	1011	0001	0000	1
0100	1100	1001	1000	1
0101	1101	0100	0101	1
0110	1110	0101	0100	1
0111	1111	1000	1001	1
1000	0000	1100	1101	1
1001	0001	1111	1110	1
1010	0010	0111	0110	1
1011	0011	1010	1011	1
1100	0100	1110	1111	1
1101	0101	1101	1100	1
1110	0110	1011	1010	1
1111	0111	0000	0001	0

Table 5.3: A linear relation for the key bits

Example

Take $n = 4$, and for f take the S-box S_0 of LUCIFER. As the two rightmost columns of Table 5.1 show the linear relation defined by (α, β), where $\alpha(x) = x_4$ and $\beta(y) = y_1 + y_2 + y_4$, has probability $p_{f,\alpha,\beta} = \frac{14}{16} = \frac{7}{8}$ (providing strong evidence that the designers of LUCIFER weren't aware of linear cryptanalysis).

As concrete round keys take $k_0 = \texttt{1000}$ and $k_1 = \texttt{0001}$. Table 5.3, running through all possible 16 plaintexts, shows that $\alpha(a) + \beta(c)$ assumes the value $1 = \alpha(k_0) + \beta(k_1)$ for this partial sum of key bits exactly 14 times—as expected.

How large is the success probability p_N of correctly estimating this partial sum, assuming $N = 1, 2, \ldots$ random known plaintexts from the set of 2^n possible plaintexts? (For given linear forms α and β with $p = p_{f,\alpha,\beta}$.) This is exactly the scenario of the hypergeometric distribution (for an explanation of the hypergeometric distribution see Appendix E). Therefore we have:

Proposition 5 *In example A let (α, β) be a pair of linear forms that defines a linear relation for f with probability p. Then the success probability for determining a key bit by this linear relation from N known plaintexts is the cumulated probability $p_N = p_N^{(s)}$ of the hypergeometric distribution with parameters 2^n, $s = \hat{p} \cdot 2^n$, and N where $\hat{p} = \max\{p, 1-p\}$.*

If we neglect exact mathematical reasoning and work with asymptotic

$N\lambda$	1	2	3	4	...	8	9
p_N	84, 1%	92, 1%	95, 8%	97, 7%	...	99, 8%	99, 9%

Table 5.4: Dependence of the success probability on the number of known plaintexts

approximations (as is common in applied statistics), then we can replace the hypergeometric distribution by the normal distribution. The usual (quite vaguely stated) conditions for this approximation are "p not too different from $\frac{1}{2}$, $N \ll 2^n$, but N not too small." This gives the formula

$$p_N \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\sqrt{N\lambda}} e^{-t^2/2}\, dt, \tag{4}$$

where $\lambda = (2p-1)^2$ is the potential of the linear relation. The values associated with the normal distribution are well-known and yield Table 5.4. Instead of the approximation by the normal distribution we could directly use the hypergeometric distribution. This would, in particular for small N, give a more precise value but not a closed formula as simple as (4).

To get a success probability of about 95% we need $N \approx \frac{3}{\lambda}$ known plaintexts according to the table. In the concrete example above we had $p = \frac{7}{8}$, hence $\lambda = \frac{9}{16}$, and the number of known plaintexts needed for a 95% success probability is $N \approx 5$. Using Table 5.2 we succeeded with only $N = 3$ plaintexts. This is not a great surprise because the a-priori probability of this success is about 90% (for $N\lambda = \frac{27}{16} \approx 1,68\ldots$).

> In this example the condition "N not too small" for the approximation by the normal distribution is more than arguable. However determining the exact values for the hypergeometric distribution is easy: Consider an urn containing 16 balls, 14 black ones and 2 white ones, and draw 3 balls by random. Then the probability of all of them being black is $\frac{26}{40}$, the probability of two being black and one being white is $\frac{13}{40}$. Hence the probability of at least two balls being black is $\frac{39}{40} = 97,5\%$. This is clearly more than the 90% from the approximation (4). The remaining probabilities are $\frac{1}{40}$ for exactly one black ball, and 0 for three white balls.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	6	6	8	8	6	6	8	8	6	6	8	8	14	6	8
2	8	10	8	6	4	6	8	6	6	12	6	8	10	8	6	8
3	8	12	10	6	12	8	10	6	6	6	8	8	10	10	8	8
4	8	8	4	8	8	8	8	4	10	6	6	6	10	6	10	10
5	8	10	10	12	8	10	6	8	10	8	4	10	10	8	8	6
6	8	10	8	10	8	10	8	10	8	10	8	2	8	10	8	10
7	8	8	10	6	8	8	2	6	8	8	10	6	8	8	10	6
8	8	8	6	10	6	10	8	8	4	8	10	10	10	10	12	8
9	8	10	8	10	6	4	10	8	8	6	8	6	6	8	10	4
10	8	6	10	8	6	8	8	10	6	4	8	6	12	6	6	8
11	8	12	8	8	6	6	6	10	10	6	10	10	8	8	8	12
12	8	8	10	10	6	10	8	4	6	6	8	8	4	8	6	10
13	8	6	12	6	6	8	10	8	10	8	6	8	8	10	12	8
14	8	6	10	12	10	4	8	6	8	10	10	8	10	8	8	10
15	8	8	8	8	10	6	6	10	4	8	4	8	6	6	10	10

Table 5.5: Approximation table of the S-box S_0 of Lucifer. Row and column indices are linear forms represented by integers. To get the probabilities divide by 16.

5.3 Approximation Table, Correlation Matrix, and Linear Spectrum of a Boolean Map

Linear relations for a Boolean map (or S-box) $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ are true with certain frequencies (or probabilities). We collect these frequencies in a matrix of size $2^n \times 2^q$, called the **approximation table** of f. This table gives, for each pair (α, β) of linear forms, the number of arguments x where $\beta \circ f(x) = \alpha(x)$. Table 5.5 shows the approximation table of the S-box S_0 of Lucifer. The entry 16 in the upper left corner says that the relation $0 = 0$ is true in all 16 possible cases. At the same time 16 is the common denominator by which we have to divide all other entries to get the probabilities. In the general case the upper left corner would be 2^n. The remaining entries of the first column (corresponding to $\beta = 0$) are 8 because each non-zero linear form α takes the value 0 in exactly half of all cases, that is 8 times. (In the language of linear algebra we express this fact as: The kernel of a linear form $\neq 0$ is a subspace of dimension $n - 1$.) For the first row an analogous argument is true—provided that f is bijective (or balanced).

The **correlation matrix** and the **linear spectrum** (also called linear profile or linearity profile—not to be confused with the linear complexity profile of a bit sequence that is defined by linear feedback shift registers and

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{3}{4}$	$-\frac{1}{4}$	0
2	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{2}$	$-\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0
3	0	$\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0	0
4	0	0	$-\frac{1}{2}$	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
5	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$
6	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	2	0	$\frac{1}{4}$	0	$\frac{1}{4}$
7	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	0	2	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$
8	0	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
9	0	$\frac{1}{4}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	$-\frac{1}{2}$
10	0	$-\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0
11	0	$\frac{1}{2}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	0	$\frac{1}{2}$
12	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{4}$
13	0	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{2}$	0
14	0	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$
15	0	0	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

Table 5.6: Correlation matrix of the S-box S_0 of Lucifer. Row and column indices are linear forms represented by integers.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{9}{16}$	$\frac{1}{16}$	0
2	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0
3	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0
4	0	0	$\frac{1}{4}$	0	0	0	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
5	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$
6	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{9}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$
7	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{9}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$
8	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0
9	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$
10	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0
11	0	$\frac{1}{4}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	0	$\frac{1}{4}$
12	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$
13	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$
14	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$
15	0	0	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

Table 5.7: Linear spectrum of the S-box S_0 of Lucifer. Row and column indices are linear forms represented by integers.

sometimes also called linearity profile) are the analogous matrices whose entries are the I/O-correlations or the potentials of the corresponding linear relations. The correlation matrix arises from the approximation table by first dividing the entries by 2^n (getting the probabilities p) and then transforming the probabilities to I/O-correlations by the formula $\tau = 2p - 1$. To get the linear spectrum we have to square the single entries of the correlation matrix.

For S_0 Table 5.6 shows the correlation matrix, and Table 5.7, the linear spectrum. Here again the first rows and columns hit the eye: The zeroes tell that a linear relation involving the linear form 0 has potential 0, hence is useless. The 1 in the upper left corner says that the relation $0 = 0$ holds for any arguments, but is useless too. In the previous subsection we picked the pair (α, β) where $\alpha(x) = x_4$ (represented by `0001` $\hat{=}\, 1$) and $\beta(y) = y_1 + y_2 + y_4$ (represented `1101` $\hat{=}\, 13$) in row 1, column 13. It assumes the maximum value $\frac{9}{16}$ for the potential that moreover also occurs at the coordinates $(6, 11)$ and $(7, 6)$. (We ignore the true, but useless, maximum value 1 in the upper left corner.)

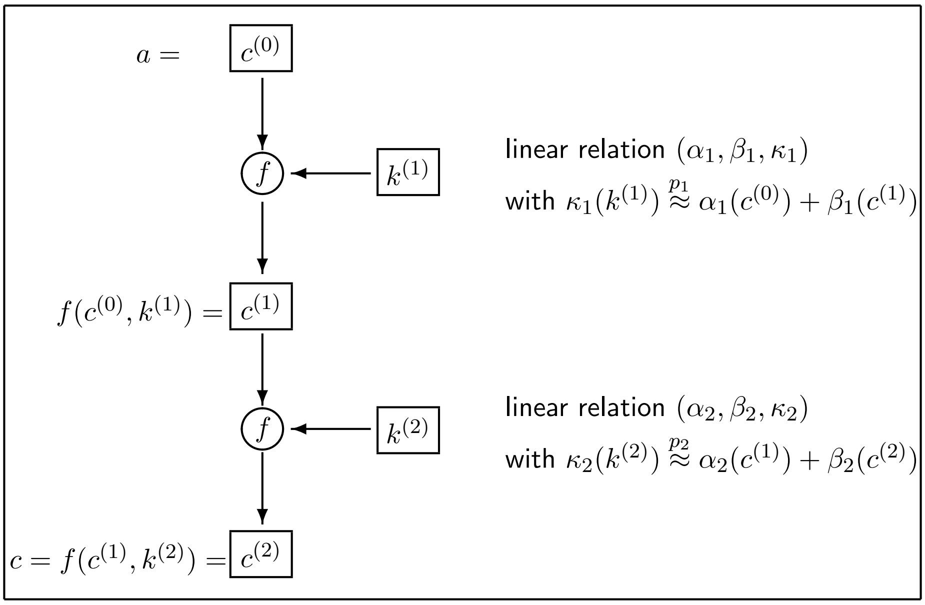
$a = c^{(0)}$
f
$k^{(1)}$
linear relation $(\alpha_1, \beta_1, \kappa_1)$
with $\kappa_1(k^{(1)}) \overset{p_1}{\approx} \alpha_1(c^{(0)}) + \beta_1(c^{(1)})$
$f(c^{(0)}, k^{(1)}) = c^{(1)}$
f
$k^{(2)}$
linear relation $(\alpha_2, \beta_2, \kappa_2)$
with $\kappa_2(k^{(2)}) \overset{p_2}{\approx} \alpha_2(c^{(1)}) + \beta_2(c^{(2)})$
$c = f(c^{(1)}, k^{(2)}) = c^{(2)}$

Figure 5.5: General two-round cipher

5.4 Example B: A Two-Round Cipher

As a next step we iterate the round map

$$f\colon \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^n$$

of a bitblock cipher over two rounds using round keys $k^{(i)} \in \mathbb{F}_2^q$ as illustrated in Figure 5.5.

Remark In a certain sense example A already was a two-round cipher since we used two partial keys. Adding one more S-box at the right side of Figure 5.3 would be cryptologically irrelevant, because this non-secret part of the algorithm would be known to the cryptanalyst who simply could “strip it off” (that is, apply its inverse to the cipher text) and be left with example A. In a similar way we could interpret example B as a three-round cipher. However this would be a not so common counting of rounds.

We consider linear relations

$$\kappa_1(k^{(1)}) \overset{p_1}{\approx} \alpha_1(c^{(0)}) + \beta_1(c^{(1)})$$

with probability p_1, I/O-correlation $\tau_1 = 2p_1 - 1$, and potential $\lambda_1 = \tau_1^2$, and

$$\kappa_2(k^{(2)}) \overset{p_2}{\approx} \alpha_2(c^{(1)}) + \beta_2(c^{(2)})$$

with probability p_2, I/O-correlation $\tau_2 = 2p_2 - 1$, and potential $\lambda_2 = \tau_2^2$. We can combine these two linear relations if $\alpha_2 = \beta_1$, thereby getting a linear relation for some key bits expressed by the (known) plaintext $c^{(0)} = a$ and the ciphertext $c^{(2)} = c$,

$$\kappa_1(k^{(1)}) + \kappa_2(k^{(2)}) \overset{p}{\approx} \alpha_1(c^{(0)}) + \beta_2(c^{(2)}),$$

that holds with a certain probability p, and has I/O-correlation τ and potential λ, that in general depend on $k = (k^{(1)}, k^{(2)})$ and are difficult to determine. Therefore we again consider a simplified example B, see Figure 5.6. Encryption is done step by step by the formulas

$$b^{(0)} = a+k^{(0)}, a^{(1)} = f_1(b^{(0)}), b^{(1)} = a^{(1)}+k^{(1)}, a^{(2)} = f_2(b^{(1)}), c = a^{(2)}+k^{(2)}.$$

(Here f_1 is given by the S-box S_0, and f_2, by the S-box S_1 that could be identical with S_0. Note that we allow that the round functions of the different rounds differ. The reason is that usually the round function consists of several parallel S-boxes and the permutations direct an input bit through different S-boxes on its way through the rounds, see Section 5.7.)

As for example A adding some key bits after the last round prevents the "stripping off" of f_2. Comparing example B with the general settings in Chapter 2 we have:

- key length $l = 3n$, key space $\mathbb{F}_2^{3n}$, and keys of the form $k = (k^{(0)}, k^{(1)}, k^{(2)})$ with $k^{(0)}, k^{(1)}, k^{(2)} \in \mathbb{F}_2^n$.
- Encryption is defined by the map
$$\begin{array}{rcl} F\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n, \\ (a, k^{(0)}, k^{(1)}, k^{(2)}) & \mapsto & f_2(f_1(a + k^{(0)}) + k^{(1)}) + k^{(2)}. \end{array}$$
- The linear form κ: $\mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is given by
$$\kappa(k^{(0)}, k^{(1)}, k^{(2)}) = \alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)}).$$

Here (α, β) is a linear relation for f_1 with probability p_1, I/O-correlation τ_1, and potential λ_1, and (β, γ), a linear relation for f_2 with probability p_2, I/O-correlation τ_2, and potential λ_2 (the same β since we want to combine the linear relations), where

$$\begin{array}{rcl} p_1 & = & \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \beta \circ f_1(x) = \alpha(x)\} \\ p_2 & = & \frac{1}{2^n} \cdot \#\{y \in \mathbb{F}_2^n \mid \gamma \circ f_2(y) = \beta(y)\} \end{array}$$

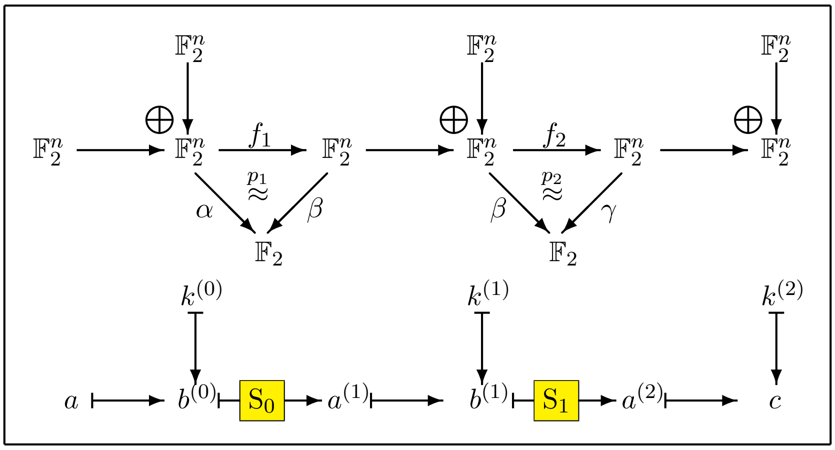

Figure 5.6: Example B

With the notations of Figure 5.6 we have

$$\begin{aligned}\gamma(c) = \gamma(a^{(2)}) + \gamma(k^{(2)}) &\overset{p_2}{\approx} \beta(b^{(1)}) + \gamma(k^{(2)}) = \beta(a^{(1)}) + \beta(k^{(1)}) + \gamma(k^{(2)})\\ &\overset{p_1}{\approx} \alpha(b^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)}) = \alpha(a) + \alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)})\end{aligned}$$

Hence we get a linear relation for the key bits as a special case of Equation (1) in the form

$$\alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)}) \overset{p}{\approx} \alpha(a) + \gamma(c)$$

with a certain probability p that is defined by the formula

$$\begin{aligned} p &= p_{F,\alpha,\beta,\gamma}(k)\\ &= \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)}) = \alpha(a) + \gamma(F(a,k))\}.\end{aligned}$$

We try to explicitly determine p. As for the one-round case we first ask how p depends on k. Insert the definition of $F(a,k)$ into the defining equation inside the set brackets. Then $\gamma(k^{(2)})$ cancels out and we are left with

$$p_{F,\alpha,\beta,\gamma}(k) = \frac{1}{2^n} \cdot \#\{a \in \mathbb{F}_2^n \mid \alpha(k^{(0)}+a)+\beta(k^{(1)}) = \gamma(f_2(k^{(1)}+f_1(k^{(0)}+a)))\}.$$

This is independent of $k^{(2)}$, and for all $k^{(0)}$ assumes the same value

$$p_{F,\alpha,\beta,\gamma}(k) = \frac{1}{2^n} \cdot \#\{x \in \mathbb{F}_2^n \mid \alpha(x) = \beta(k^{(1)}) + \gamma(f_2(k^{(1)} + f_1(x)))\}$$

because $x = k^{(0)} + a$ runs through $\mathbb{F}_2^n$ along with a. This value indeed depends on k, but only on the middle component $k^{(1)}$. Now form the mean value $\bar{p} := p_{F,\alpha,\beta,\gamma}$ over all keys:

$$\bar{p} = \frac{1}{2^{2n}} \cdot \#\{(x, k^{(1)}) \in \mathbb{F}_2^{2n} \mid \alpha(x) = \beta(k^{(1)}) + \gamma(f_2(k^{(1)} + f_1(x)))\}.$$

Inside the brackets we see the expression $\gamma(f_2(k^{(1)} + f_1(x)))$, and we know:

$$\gamma(f_2(k^{(1)} + f_1(x))) = \begin{cases} \beta(k^{(1)} + f_1(x)) & \text{with probability } p_2, \\ 1 + \beta(k^{(1)} + f_1(x)) & \text{with probability } 1 - p_2. \end{cases}$$

Here "probability p_2" means that the statement is true for $p_2 \cdot 2^{2n}$ of all possible $(x, k^{(1)}) \in \mathbb{F}_2^{2n}$. Substituting this we get

$$\bar{p} = \frac{1}{2^{2n}} \cdot \Big[p_2 \cdot \#\{(x, k^{(1)}) \in \mathbb{F}_2^{2n} \mid \alpha(x) = \beta(f_1(x))\}$$

$$+ (1 - p_2) \cdot \#\{(x, k^{(1)}) \in \mathbb{F}_2^{2n} \mid \alpha(x) \neq \beta(f_1(x))\} \Big]$$

where now the defining equations of both sets are also independent of $k^{(1)}$. We recognize the definition of p_1 and substitute it getting

$$\bar{p} = p_1 p_2 + (1 - p_1)(1 - p_2) = 2p_1 p_2 - p_1 - p_2 + 1.$$

This formula looks much more beautiful if expressed in terms of the I/O-correlations $\bar{\tau} = 2\bar{p} - 1$ and $\tau_i = 2p_i - 1$ for $i = 1$ and 2:

$$\bar{\tau} = 2\bar{p} - 1 = 4p_1 p_2 - 2p_1 - 2p_2 + 1 = (2p_1 - 1)(2p_2 - 1) = \tau_1 \tau_2.$$

In summary we have proved:

Proposition 6 *For example B we have:*

(i) *The probability $p_{F,\alpha,\beta,\gamma}(k)$ depends only on the middle component $k^{(1)}$ of the key $k = (k^{(0)}, k^{(1)}, k^{(2)}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n$.*

(ii) *The mean value of these probabilities over all keys k is $p_{F,\alpha,\beta,\gamma} = \bar{p} = 2p_1 p_2 - p_1 - p_2 + 1$.*

(iii) *The I/O-correlations and the potentials are multiplicative:*

$$\tau_{F,\alpha,\beta,\gamma} = \tau_1 \tau_2 \quad \textit{and} \quad \lambda_{F,\alpha,\beta,\gamma} = \lambda_1 \lambda_2.$$

In Matsui's test we face the decision whether to use the linear relation or its negation for estimating a bit. We can't do better than use the mean value $p_{F,\alpha,\beta,\gamma}$ since the key and the true probability $p_{F,\alpha,\beta,\gamma}(k)$ are unknown. This could be an error since these two probabilities might lie on different sides of $\frac{1}{2}$.

Example

Let $n = 4$, S_0 as in example A, and S_1 as given in Table 5.8 (in different order) as transition from column $b^{(1)}$ to column $a^{(2)}$. (By the way this is the second S-box of LUCIFER.) Consider the linear forms $\alpha \mathrel{\hat{=}} \texttt{0001}$ and $\beta \mathrel{\hat{=}} \texttt{1101}$ as before with $p_1 = \frac{7}{8}$, $\tau_1 = \frac{3}{4}$, $\lambda_1 = \frac{9}{16}$. Furthermore let $\gamma \mathrel{\hat{=}} \texttt{1100}$. Then the linear relation for f_2 defined by (β, γ) (see Table 5.9, row index

a	$b^{(0)}$	$a^{(1)}$	$b^{(1)}$	$a^{(2)}$	c	$\beta(b^{(1)})$	$\gamma(a^{(2)})$	$\alpha(a)+\gamma(c)$
0000	1000	0010	0011	1001	1111	1	1	0
0001	1001	0110	0111	0100	0010	0	1	1
0010	1010	0011	0010	1110	1000	0	0	1
0011	1011	0001	0000	0111	0001	0	1	1
0100	1100	1001	1000	1100	1010	1	0	1
0101	1101	0100	0101	1011	1101	0	1	1
0110	1110	0101	0100	0011	0101	1	0	1
0111	1111	1000	1001	1101	1011	0	0	0
1000	0000	1100	1101	1111	1001	1	0	1
1001	0001	1111	1110	1000	1110	0	1	1
1010	0010	0111	0110	0000	0110	1	0	1
1011	0011	1010	1011	1010	1100	0	1	1
1100	0100	1110	1111	0101	0011	1	1	0
1101	0101	1101	1100	0110	0000	0	1	1
1110	0110	1011	1010	0001	0111	1	0	1
1111	0111	0000	0001	0010	0100	1	0	0

Table 5.8: The data flow in the concrete example for B, and some linear forms

13, column index 12) has probability $p_2 = \frac{1}{4}$, I/O-correlation $\tau_2 = -\frac{1}{2}$, and potential $\lambda_2 = \frac{1}{4}$, the maximum possible value by Table 5.10. (Note that the linear profile of S_1 is more uniform than that of S_0.)

As concrete round keys take $k^{(0)} =$ `1000`, $k^{(1)} =$ `0001`—as before—, and $k^{(2)} =$ `0110`. We want to gain the bit $\alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)})$ (that in cheat mode we know is 0). Since $\tau_1\tau_2 < 0$ in the majority of cases $\alpha(a)+\gamma(c)$ should give the complementary bit 1. Table 5.8 shows that in 12 of 16 cases this prediction is correct. Therefore $1 - p = \frac{3}{4}$, $p = \frac{1}{4}$, $\tau = -\frac{1}{2}$, $\lambda = \frac{1}{4}$. Remember that this value depends on the key component $k^{(1)}$. In fact it slightly deviates from the mean value

$$\bar{p} = 2 \cdot \frac{7}{8} \cdot \frac{1}{4} - \frac{7}{8} - \frac{1}{4} + 1 = \frac{7}{16} - \frac{14}{16} - \frac{4}{16} + \frac{16}{16} = \frac{5}{16}.$$

Calculating the variation of the probability as function of the partial key $k^{(1)}$ we get the values $\frac{1}{4}$ and $\frac{3}{8}$ each 8 times, all lying on the "correct side" of $\frac{1}{2}$ and having the correct mean value $\frac{5}{16}$.

There are other "paths" from α to γ—we could insert any β in between. Calculating the mean probabilities yields—besides the already known $\frac{5}{16}$—three times $\frac{15}{32}$, eleven times exactly $\frac{1}{2}$, and even a single $\frac{17}{32}$ that lies on the "wrong" side of $\frac{1}{2}$. Thus only the one case we explicitly considered is really good.

As an alternative concrete example take $\beta \,\hat{=}\,$ `0001`. Here $\lambda_1 = \frac{1}{16}$, $p_1 = \frac{3}{8}$,

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	10	8	10	8	6	12	10	10	4	6	8	10	8	10	8
2	8	6	4	10	6	8	6	8	8	10	4	6	10	8	10	8
3	8	8	8	8	6	6	6	6	10	6	6	10	4	8	8	12
4	8	8	8	4	8	8	8	4	6	6	6	10	10	10	10	6
5	8	6	8	10	4	6	8	6	8	6	12	6	8	10	8	6
6	8	10	12	10	6	12	6	8	10	8	6	8	8	10	8	6
7	8	8	8	12	10	10	10	6	4	8	8	8	6	10	10	10
8	8	8	6	10	10	6	8	8	10	10	8	12	8	12	6	6
9	8	6	6	8	6	12	8	10	8	6	10	12	10	8	8	10
10	8	6	6	8	12	10	6	8	10	4	8	6	6	8	8	6
11	8	4	10	10	8	8	10	6	8	8	6	10	8	4	6	6
12	8	8	6	6	6	10	12	8	8	8	6	6	6	10	4	8
13	8	10	6	8	6	8	8	10	6	8	8	10	4	6	10	4
14	8	10	6	8	8	10	10	4	12	10	10	8	8	6	10	8
15	8	4	10	6	8	8	10	10	10	10	8	8	6	10	12	8

Table 5.9: Approximation table of the S-box S_1 of LUCIFER. Row and column indices are linear forms represented by integers. For the probabilities divide by 16.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0
2	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0
3	0	0	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	0	$\frac{1}{4}$
4	0	0	0	$\frac{1}{4}$	0	0	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
5	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$
6	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$	0	$\frac{1}{16}$
7	0	0	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
8	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$
9	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$
10	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	$\frac{1}{4}$	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$
11	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$
12	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0
13	0	$\frac{1}{16}$	$\frac{1}{16}$	0	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$
14	0	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	0
15	0	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	0	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$	0

Table 5.10: Linear profile of the S-box S_1 of LUCIFER. Row and column indices are linear forms represented by integers.

$\tau_1 = -\frac{1}{4}$, and $\lambda_2 = \frac{1}{16}$, $p_2 = \frac{5}{8}$, $\tau_2 = \frac{1}{4}$. Hence $\tau = -\frac{1}{16}$ and $p = \frac{15}{32}$. The target bit is $\alpha(k^{(0)}) + \beta(k^{(1)}) + \gamma(k^{(2)}) + 1 = 1$, and the success probability is $1 - p = \frac{17}{32}$. The mean value of p over all keys is $\frac{15}{32}$ for this β in coincidence with the key-specific value.

$$\begin{tikzcd}
 & \mathbb{F}_2^n \arrow[d, "\oplus"'] & & & & \mathbb{F}_2^n \arrow[d, "\oplus"'] & & & \mathbb{F}_2^n \arrow[d, "\oplus"'] \\
\mathbb{F}_2^n \arrow[r] & \mathbb{F}_2^n \arrow[rr, "f_1"] \arrow[rr, phantom, "\overset{p_1}{\approx}"'] \arrow[dr, "\beta_0"'] & & \mathbb{F}_2^n \arrow[r] \arrow[dl, "\beta_1"] & \cdots \arrow[r] & \mathbb{F}_2^n \arrow[rr, "f_r"] \arrow[rr, phantom, "\overset{p_r}{\approx}"'] \arrow[dr, "\beta_{r-1}"'] & & \mathbb{F}_2^n \arrow[r] \arrow[dl, "\beta_r"] & \mathbb{F}_2^n \\
 & & \mathbb{F}_2 & & & & \mathbb{F}_2 & &
\end{tikzcd}$$

Figure 5.7: Example C

5.5 Linear Paths

Consider the general case where the round map $f: \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^n$ 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

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

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

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

and the assertion follows by induction on r. ◇

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.

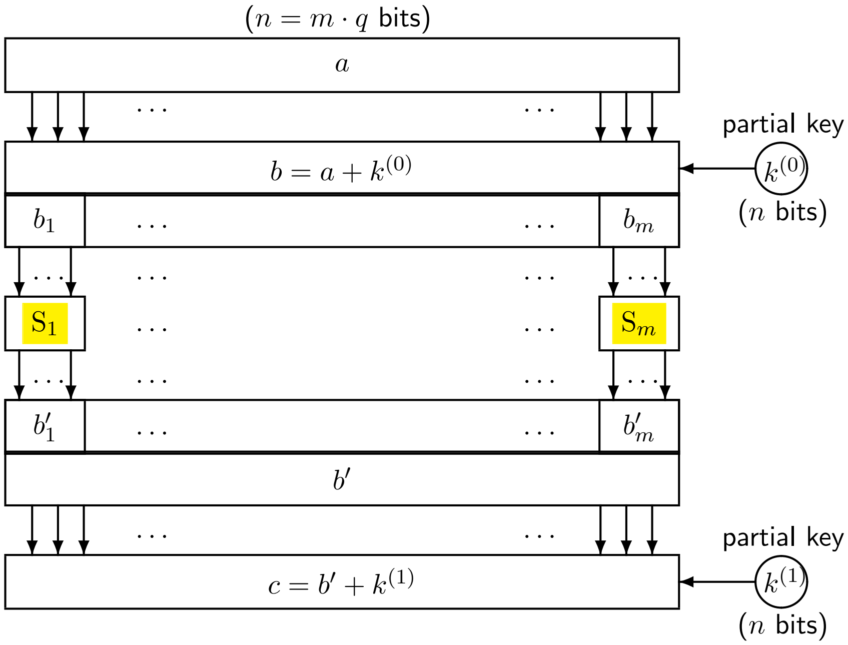

Figure 5.8: Example D, parallel arrangement of m S-boxes $S_1, \ldots, S_m$ of width q

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

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.

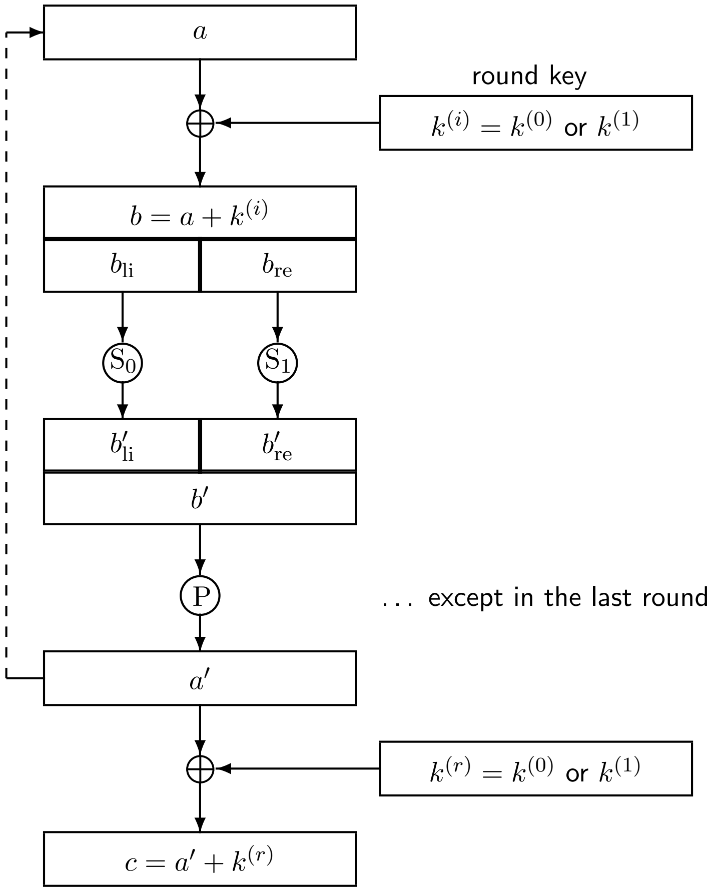

Figure 5.9: Mini-Lucifer

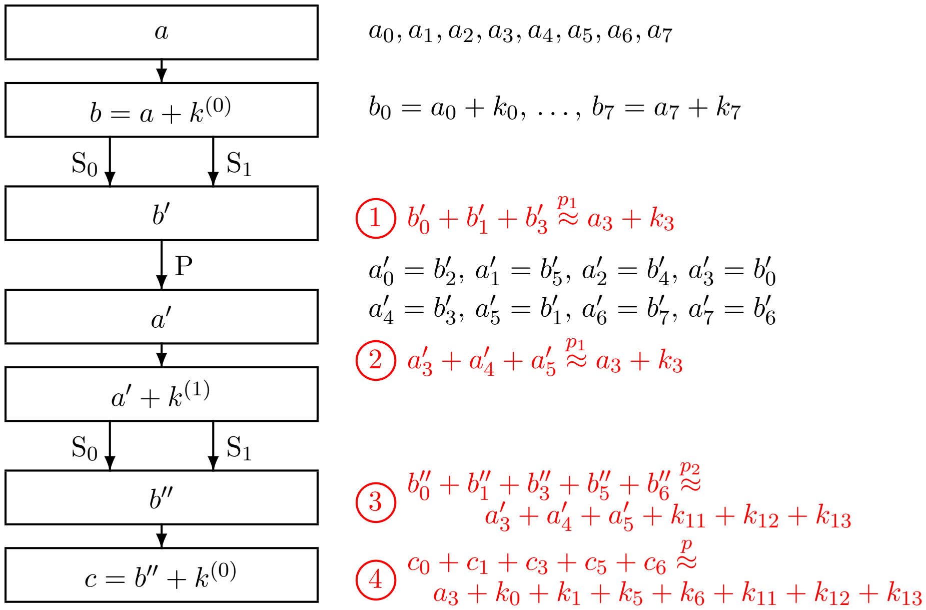
a
$a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7$
$b = a + k^{(0)}$
$b_0 = a_0 + k_0,\ \ldots,\ b_7 = a_7 + k_7$
S_0
S_1
b'
$\boxed{1}\ b'_0 + b'_1 + b'_3 \overset{p_1}{\approx} a_3 + k_3$
P
$a'_0 = b'_2,\ a'_1 = b'_5,\ a'_2 = b'_4,\ a'_3 = b'_0$
$a'_4 = b'_3,\ a'_5 = b'_1,\ a'_6 = b'_7,\ a'_7 = b'_6$
a'
$\boxed{2}\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

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 $\beta_1' \mathrel{\hat{=}} \texttt{0001} \mathrel{\hat{=}} 1$, on the right-hand side, for S_1, we have $\beta_2' \mathrel{\hat{=}} \texttt{1100} \mathrel{\hat{=}} 12$. 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 $\gamma_1 \mathrel{\hat{=}} 13 \mathrel{\hat{=}} \texttt{1101}$.

For β_2' the maximum potential is $\lambda_2'' = \frac{1}{4}$. Having two choices we choose $\gamma_2 \mathrel{\hat{=}} 6 \mathrel{\hat{=}} \texttt{0110}$ 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.

5.8 Systematic Search for Linear Relations

The search for useful linear relations over several rounds has no general elegant solution. The published examples often use linear paths that more or less appear from nowhere, and it is not evident that they are the best ones.

Let n be the block length of the cipher, and r, the number of rounds. Then for each round the choice is between 2^n linear formes, making a total of $2^{n(r+1)}$ choices. This number also specifies the cost of determining the best relation by complete search. There are some simplifications that however don't reduce the order of magnitude of the cost:

- In the first round consider only linear forms that activate only one S-box.
- Then choose the next linear form such that it activates the least possible number of S-boxes of the next round (with high, but not necessarily maximum potential).
- If one of the relations in a linear path has probability $\frac{1}{2}$, or I/O-correlation 0, then the total I/O-correlation is 0 by multiplicativity, and this path may be neglected. The same is true componentwise if the linear forms split among the S-boxes of the respective round. However this negligence could introduce errors since we deal with average probabilities not knowing the key-dependent ones.

For our 2-round example with Mini-Lucifer the systematic search is feasible by pencil and paper or by a Sage or Python script. Our example has the following characteristics:

- $\alpha = (\alpha_1, \alpha_2)$ with $\alpha_1 \hat{=} 1 \hat{=} \texttt{0001}$ and $\alpha_2 \hat{=} 0 \hat{=} \texttt{0000}$ (α_1 was formerly denoted α. Now for uniformity we make both components of all linear forms explicit and index them by 1 and 2.)
- $\beta = (\beta_1, \beta_2)$ with $\beta_1 \hat{=} 13 \hat{=} \texttt{1101}$ and $\beta_2 \hat{=} 0 \hat{=} \texttt{0000}$
- $\beta' = (\beta'_1, \beta'_2)$ with $\beta'_1 \hat{=} 1 \hat{=} \texttt{0001}$, $\beta'_2 \hat{=} 12 \hat{=} \texttt{1100}$
- $\gamma = (\gamma_1, \gamma_2)$ with $\gamma_1 \hat{=} 13 \hat{=} \texttt{1101}$, $\gamma_2 \hat{=} 6 \hat{=} \texttt{0110}$
- $\tau_1 = \frac{3}{4}$, $\tau'_2 = \frac{3}{4}$, $\tau''_2 = \frac{1}{2}$, $\tau_2 = \frac{3}{8}$, $\tau = \frac{9}{32}$, $p = \frac{41}{64} = 0,640625$
- $c_0 + c_1 + c_3 + c_5 + c_6 \overset{p}{\approx} a_3 + k_0 + k_1 + k_5 + k_6 + k_{11} + k_{12} + k_{13}$

An alternative choice of γ_2 is $\gamma_2 \hat{=} 14 \hat{=} \texttt{1110}$; this yields a linear path with the characteristics

- $\alpha \hat{=} (1, 0)$, $\beta \hat{=} (13, 0)$, $\beta' \hat{=} (1, 12)$, $\gamma \hat{=} (13, 14)$

  - $\tau = -\frac{9}{32}$, $p = \frac{23}{64} = 0,359375$
  - $c_0+c_1+c_3+c_4+c_5+c_6 \overset{p}{\approx} a_3+k_0+k_1+k_4+k_5+k_6+k_{11}+k_{12}+k_{13}$

The systematic search finds two even "better" linear paths, characterized by

- $\alpha \hat{=} (8,0)$, $\beta \hat{=} (8,0)$, $\beta' \hat{=} (1,0)$, $\gamma \hat{=} (13,0)$
  - $\tau = -\frac{3}{8}$, $p = \frac{5}{16} = 0,3125$
  - $c_0 + c_1 + c_3 \overset{p}{\approx} a_0 + k_1 + k_3 + k_{11}$
- $\alpha \hat{=} (15,0)$, $\beta \hat{=} (8,0)$, $\beta' \hat{=} (1,0)$, $\gamma \hat{=} (13,0)$
  - $\tau = -\frac{3}{8}$, $p = \frac{5}{16} = 0,3125$
  - $c_0 + c_1 + c_3 \overset{p}{\approx} a_0 + a_1 + a_2 + a_3 + k_2 + k_{11}$

that do not completely exhaust the potential of the single S-boxes but on the other hand activate only one S-box of the second round, and thereby show the larger potential $\lambda = \frac{9}{64}$. Thus we get a 95% success probability with only

$$N = \frac{3}{\lambda} = \frac{64}{3} \approx 21$$

known plaintexts for determining one bit.

The designer of a cipher should take care that in each round the active bits fan out over as many S-boxes as possible. The inventors of AES, Daemen and Rijmen call this design approach "wide-trail strategy". The design of AES strengthens this effect by involving a linear map instead of a mere permutation, thereby replacing the "P" of an SP-network by an "L".

Figure 5.11 shows an example of a linear path with all its ramifications.

Example (Continued)

For an illustration of the procedure we generate 25 pairs of known plaintexts and corresponding ciphertexts using the key $k \hat{=}$ `1001011000101110`. The target key bits are

$$\begin{aligned}
b_0 &= k_0 + k_1 + k_5 + k_6 + k_{11} + k_{12} + k_{13} \\
b_1 &= k_0 + k_1 + k_4 + k_5 + k_6 + k_{11} + k_{12} + k_{13} \\
b_2 &= k_1 + k_3 + k_{11} \\
b_3 &= k_2 + k_{11}
\end{aligned}$$

that we know in cheat mode are $b_0 = 1$, $b_1 = 1$, $b_2 = 1$, $b_3 = 0$. We use all four good relations at the same time without fearing the possible reduction of the success probability. All of these relations assert the probable equality of the bits

$$\begin{aligned} b_0 &\overset{p}{\approx} c_0 + c_1 + c_3 + c_5 + c_6 + a_3 \\ b_1 &\overset{p}{\approx} 1 + c_0 + c_1 + c_3 + c_4 + c_5 + c_6 + a_3 \\ b_2 &\overset{p}{\approx} 1 + c_0 + c_1 + c_3 + a_0 \\ b_3 &\overset{p}{\approx} 1 + c_0 + c_1 + c_3 + a_0 + a_1 + a_2 + a_3 \end{aligned}$$

each with its individual corresponding probability p. For the last three of these sums we have to take the complementary bits since the corresponding I/O-correlations are negative (the probabilities are $< \frac{1}{2}$). This is done by adding the bit `1`.

Table 5.13 shows the results for these plaintext-ciphertext pairs. As we see our guess is correct for all four bits.

As a consequence of our analysis we get a system of four linear equations for the 16 unknown key bits:

$$\begin{aligned} 1 &= k_0 + k_1 + k_5 + k_6 + k_{11} + k_{12} + k_{13} \\ 1 &= k_0 + k_1 + k_4 + k_5 + k_6 + k_{11} + k_{12} + k_{13} \\ 1 &= k_1 + k_3 + k_{11} \\ 0 &= k_2 + k_{11} \end{aligned}$$

that allow us to reduce the number of keys for an exhaustion from $2^{16} = 65536$ to $2^{12} = 4096$. Note the immediate simplifications of the system: $k_{11} = k_2$ from the last equation, and $k_4 = 0$ from the first two.

As a cross-check we run some more simulations. The next four yield

- $15, 16, 19, 16$
- $15, 16, 13, 17$
- $15, 20, 19, 17$
- $19, 19, 20, 18$

correct guesses, and so on. Only run number 10 produced a wrong bit (the second one):

- $17, 12, 14, 17$

then again run number 25. Thus empirical evidence suggests a success probability of at least 90% in this scenario.

nr	plaintext	ciphertext	b_0	b_1	b_2	b_3
1	`00001111`	`00001010`	1	1	1	1
2	`00010001`	`11001110`	1	1	1	0
3	`00010110`	`11001001`	1	1	1	0
4	`00111101`	`10110010`	0	1	1	1
5	`01000000`	`11100111`	0	1	1	0
6	`01001000`	`01010111`	0	1	1	0
7	`01001100`	`11101010`	1	1	1	0
8	`01001101`	`01011100`	1	1	1	0
9	`01001111`	`01111010`	1	1	1	0
10	`01100111`	`00110011`	0	1	0	0
11	`10000011`	`11110100`	0	1	1	1
12	`10010011`	`01101011`	1	1	1	0
13	`10011000`	`01100111`	0	1	1	0
14	`10101011`	`11011001`	1	1	1	0
15	`10110001`	`11001000`	1	1	0	0
16	`10110010`	`10100100`	1	0	1	1
17	`10110110`	`11000100`	0	1	0	0
18	`10111001`	`11000001`	1	0	0	0
19	`10111101`	`10111111`	1	1	0	0
20	`11000100`	`01001111`	1	1	1	0
21	`11000111`	`00111111`	1	1	1	0
22	`11011111`	`11011010`	1	1	1	1
23	`11100000`	`11101110`	0	0	0	0
24	`11100100`	`01110011`	1	0	0	0
25	`11110101`	`11110101`	1	0	1	0

true bit:	1	1	1	0
correct guesses:	17	20	18	20

Table 5.13: Plaintext/ciphertext pairs for Mini-Lucifer

Analysis over Four Rounds

Now let's explore how an increasing number of rounds impedes linear cryptanalysis.

Consider the toy cipher Mini-Lucifer over four rounds. Searching an optimal linear path over four rounds is somewhat expensive, so we content ourselves with extending the best example from the two round case, the third one, over two additional rounds. Slightly adapting the notation we get:

- for the first round $\beta_0 = \alpha \hat{=} (8,0)$ and $\beta_1 \hat{=} (8,0)$ (the "old" β) with $\tau_1 = -\frac{1}{2}$,
- for the second round (applying the permutation P to β_1) $\beta_1' \hat{=} (1,0)$ and $\beta_2 \hat{=} (13,0)$ (the "old" γ) with $\tau_2 = \frac{3}{4}$,
- for the third round $\beta_2' \hat{=} (1,12)$ and $\beta_3 \hat{=} (13,6)$ with $\tau_3 = \frac{3}{8}$,
- for the fourth round $\beta_3' \hat{=} (5,13)$ and $\beta = \beta_4 \hat{=} (3,12)$ (the "new" β) with $\tau_4 = -\frac{1}{4}$.

Figure 5.11 shows this linear path with its ramifications.

The repeated round keys we used are not independent. Therefore multiplicativity of I/O-correlations is justified by the rule of thumb only yielding an approximate value for the I/O-correlation of the linear relation (α, β) over all of the four rounds:

$$\tau \approx \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{3}{8} \cdot \frac{1}{4} = \frac{9}{256} \approx 0,035.$$

The other characteristics are

$$p \approx \frac{265}{512} \approx 0,518, \quad \lambda \approx \frac{81}{65536} \approx 0,0012, \quad N \approx \frac{65536}{27} \approx 2427,$$

the last one being the number of needed known plaintexts for a 95% success probability.

Comparing this with the cost of exhaustion over all 65536 possible keys we seem to have gained an advantage. However there are only 256 different possible plaintexts all together. So linear cryptanalysis completely lost its sense by the increased number of rounds.

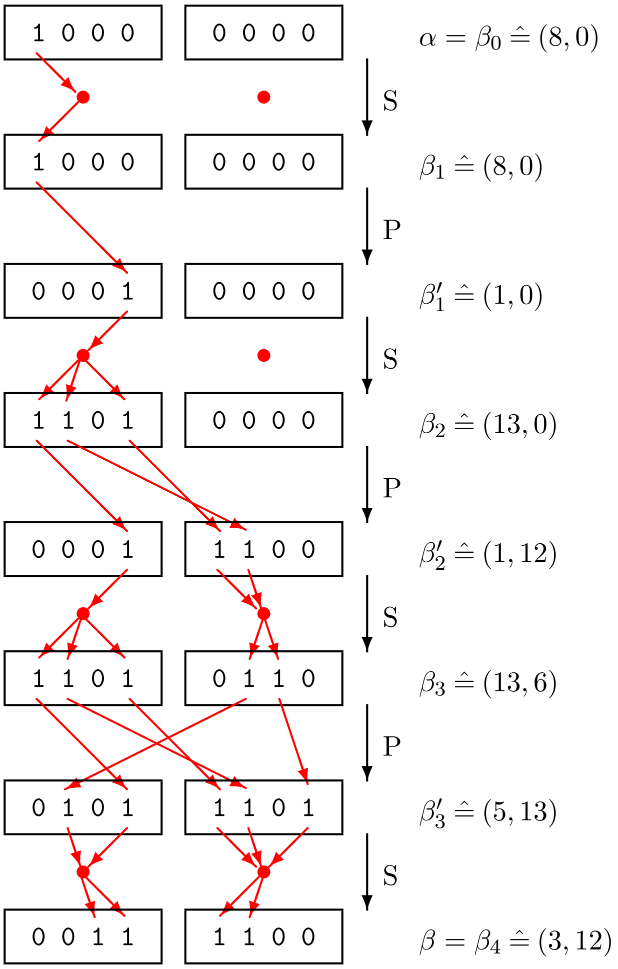
1 0 0 0
0 0 0 0
$\alpha = \beta_0 \mathrel{\hat{=}} (8,0)$
S
1 0 0 0
0 0 0 0
$\beta_1 \mathrel{\hat{=}} (8,0)$
P
0 0 0 1
0 0 0 0
$\beta_1' \mathrel{\hat{=}} (1,0)$
S
1 1 0 1
0 0 0 0
$\beta_2 \mathrel{\hat{=}} (13,0)$
P
0 0 0 1
1 1 0 0
$\beta_2' \mathrel{\hat{=}} (1,12)$
S
1 1 0 1
0 1 1 0
$\beta_3 \mathrel{\hat{=}} (13,6)$
P
0 1 0 1
1 1 0 1
$\beta_3' \mathrel{\hat{=}} (5,13)$
S
0 0 1 1
1 1 0 0
$\beta = \beta_4 \mathrel{\hat{=}} (3,12)$

Figure 5.11: A linear path with ramifications ("trail"). For S the linear form in the range is *chosen* (for high potential), indicated by a red dot. For P the linear form in the range results by applying the permutation.

5.9 The Idea of Differential Cryptanalysis

Differential cryptanalysis has some similarities with linear cryptanalysis but instead of linear relations it uses approximations of Boolean maps by linear structures (see Appendix C). The idea is to consider a difference vector before applying a round map, and its possible values thereafter. Sequences of difference vectors that fit together over all the rounds of an iterated bitblock cipher are called a **differential path** or a **characteristic** [Biham/Shamir 1990]. The potential of a differential path is approximated by the product of the potentials of the single steps. A **differential hull** or a **differential** [Lai/Massey/Murphy 1991] is the collection of all paths between a given input difference (of the entire cipher) and a given output difference. The success of differential cryptanalysis relies on an analoguous rule of thumb:

> *Along a differential path the differential potentials are multiplicative. The potential of a differential hull is approximated by the potential of a dominant differential path.*

This potential reflects the probability for getting an equation for some key bits.