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.

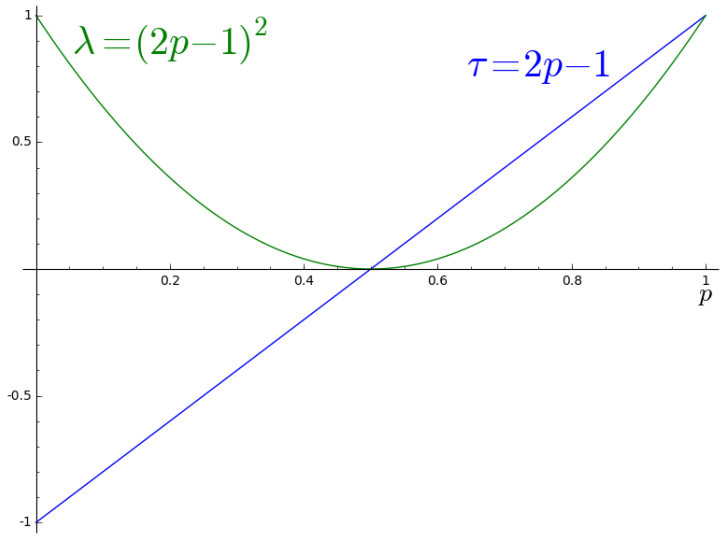

Figure 5.1: Connection between probability p, I/O-correlation τ, and potential λ

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 $k =$ `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.