| | 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 $(\alpha, \beta)$ 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 $\alpha$ 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 $(\alpha, \beta)$ 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.)