Chapter 4

STATISTICAL CHARACTERISTICS OF POWER TRACES

After having discussed different measurement setups and their most important quality criteria in Chapter 3, we now analyze power traces from a statistical point of view. Power traces are vectors of voltage values that have been recorded with a digital sampling oscilloscope. The measured voltage values are proportional to the power consumption of a cryptographic device because the oscilloscope is connected to an appropriate measurement circuit or EM probe. The settings of the oscilloscope determine the length of the power traces and the number of points that are recorded per second.

In this chapter, we present statistical models for the individual points of power traces and for power traces as a whole. These models describe power traces in a way that power analysis attacks can be explained and analyzed relatively easily. We introduce these models by first presenting the most important components of power traces, *i.e.* we discuss which factors influence the power consumption most. Subsequently, we characterize these dependencies based on probability distributions and we introduce a notation for side-channel leakage. Using the conclusions gained from these discussions, we present different methods to compress power traces. In the last section of this chapter, we provide a brief introduction to confidence intervals and hypothesis testing.

4.1 Composition of Power Traces

Power analysis attacks exploit the fact that the power consumption of cryptographic devices depends on the operations they perform and on the data they process. These two dependencies are therefore the most interesting properties of the power consumption in the context of this book. This is also why we introduce a dedicated notation for the operation-dependent and the data-dependent components of power traces. For each single point of a power trace, we refer to

the operation-dependent component of the point as P_{op}. With P_{data}, we refer to the data-dependent component of the point.

Besides P_{op} and P_{data}, each point of a power trace also depends on two additional factors. As already pointed out in Section 3.5.1, there is electronic noise in every power measurement in practice. When a power measurement of a fixed operation on some fixed data is repeated, the measurement is different for every repetition. We denote this noise component of the power consumption by $P_{el.\,noise}$. Besides the noise, each point of a power trace has also a constant component. Constant components are for example caused by leakage currents and by transistor switchings that occur independently of the performed operation and the processed data. We refer to this constant power consumption as P_{const}. The components P_{op}, P_{data}, $P_{el.\,noise}$, and P_{const} are additive. Therefore, it is possible to model each point of a power trace as the sum of these four components.

Each point of a power trace can be modeled as the sum of an operation-dependent component P_{op}, a data-dependent component P_{data}, electronic noise $P_{el.\,noise}$, and a constant component P_{const}.

$$P_{total} = P_{op} + P_{data} + P_{el.\,noise} + P_{const} \tag{4.1}$$

Note that the four components P_{op}, P_{data}, $P_{el.\,noise}$, and P_{const} are functions of the time. For each point of a power trace, these components are potentially different. We do not write these components explicitly as a function of time as we usually only analyze single points based on this model.

In the context of power analysis attacks, the components P_{op}, P_{data}, and $P_{el.\,noise}$ are the most important ones. The component P_{const} is not relevant for power analysis attacks because it does not provide any exploitable information for an attacker. An attacker can only learn information about the key of a cryptographic device by analyzing P_{op} and P_{data}. This analysis becomes the more difficult, the bigger the noise component $P_{el.\,noise}$ is. In the following sections, we discuss the characteristics of the different additive components of the power consumption.

4.2 Characteristics of Single Points

We start the characterization of the different components of power traces by only looking at a single point of a power trace, *i.e.* we look at the power consumption of a cryptographic device at a fixed moment of time. For this fixed moment of time, we determine the probability distribution of $P_{el.\,noise}$, P_{data}, and P_{op}.