Chapter 6

# DIFFERENTIAL POWER ANALYSIS

Differential power analysis (DPA) attacks are the most popular type of power analysis attacks. This is due to the fact that DPA attacks do not require detailed knowledge about the attacked device. Furthermore, they can reveal the secret key of a device even if the recorded power traces are extremely noisy.

In contrast to SPA attacks, DPA attacks require a large number of power traces. It is therefore usually necessary to physically possess a cryptographic device for some time in order to mount a DPA attack on it. Consider for example an owner of an electronic purse. This person can record a large number of power traces by transferring small amounts of money to and from the purse. These traces could then be used to reveal the cryptographic key that is used by the purse.

In this chapter, we provide a comprehensive introduction to DPA attacks. We discuss and compare different kinds of DPA attacks and we also illustrate them based on several examples. For this purpose, we use the software and the hardware implementation of AES that are described in Appendix B. We also elaborate on issues like the simulation of DPA attacks and the calculation of the number of traces that are needed to perform successful DPA attacks.

## 6.1 General Description

The goal of DPA attacks is to reveal secret keys of cryptographic devices based on a large number of power traces that have been recorded while the devices encrypt or decrypt different data blocks. The main advantage of DPA attacks compared to SPA attacks is that no detailed knowledge about the cryptographic device is necessary. In fact, it is usually sufficient to know the cryptographic algorithm that is executed by the device.

Another important difference between the two kinds of attacks is that the recorded traces are analyzed in a different way. In SPA attacks, the power

consumption of a device is mainly analyzed along the time axis. The attacker tries to find patterns or tries to match templates in a single trace. In case of DPA attacks, the shape of the traces along the time axis is not so important. DPA attacks analyze how the power consumption at fixed moments of time depends on the processed data. Hence, DPA attacks focus exclusively on the data dependency of the power traces.

> DPA attacks exploit the data dependency of the power consumption of cryptographic devices. They use a large number of power traces to analyze the power consumption at a fixed moment of time as a function of the processed data.

We now discuss in detail how such an analysis reveals secret keys of cryptographic devices. In contrast to SPA attacks, there exists a general attack strategy that is used by all DPA attacks. This strategy consists of five steps.

**Step 1: Choosing an Intermediate Result of the Executed Algorithm.** The first step of a DPA attack is to choose an intermediate result of the cryptographic algorithm that is executed by the attacked device. This intermediate result needs to be a function $f(d, k)$, where $d$ is a known non-constant data value and $k$ is a small part of the key. Intermediate results that fulfill this condition can be used to reveal $k$. In most attack scenarios, $d$ is either the plaintext or the ciphertext.

**Step 2: Measuring the Power Consumption.** The second step of a DPA attack is to measure the power consumption of the cryptographic device while it encrypts or decrypts $D$ different data blocks. For each of these encryption or decryption runs, the attacker needs to know the corresponding data value $d$ that is involved in the calculation of the intermediate result chosen in step 1. We write these known data values as vector $\mathbf{d} = (d_1, \ldots, d_D)'$, where $d_i$ denotes the data value in the $i^{\text{th}}$ encryption or decryption run.

During each of these runs the attacker records a power trace. We refer to the power trace that corresponds to data block $d_i$ as $\mathbf{t}_i' = (t_{i,1}, \ldots, t_{i,T})$, where $T$ denotes the length of the trace. The attacker measures a trace for each of the $D$ data blocks, and hence, the traces can be written as matrix $\mathbf{T}$ of size $D \times T$. It is important for DPA attacks that the measured traces are correctly aligned. This means that the power consumption values of each column $\mathbf{t}_j$ of the matrix $\mathbf{T}$ need to be caused by the same operation. In order to obtain aligned power traces, the trigger signal for the oscilloscope needs to be generated in such a way that the oscilloscope records the power consumption of exactly the same sequence of operations during each encryption or decryption run. In case such a trigger signal is not available, the power traces need to be aligned using the techniques described in Section 8.2.2.