Chapter 3

POWER CONSUMPTION

Digital circuits consume power whenever they perform computations. They draw current from a power supply and then dissipate the received energy as heat. The power consumption of digital circuits is a very important topic. The power consumption determines whether a chip needs to be cooled or not, it determines which kind of power supply is necessary and, in case of cryptographic devices, it determines whether a device can be attacked or not. Obviously, this is the most important property of the power consumption in the context of this book.

In this chapter, we discuss the power consumption of cryptographic devices in detail and we show how it can be measured in practice. Our discussion starts with an analysis of the power consumption of CMOS circuits in general. Subsequently, different simulation techniques and power models for digital circuits are introduced. Finally, we discuss setups to measure the power consumption of cryptographic devices. In particular, we elaborate on the quality criteria of such measurement setups.

3.1 Power Consumption of CMOS Circuits

The total power consumption of a CMOS circuit is the sum of the power consumptions of the logic cells making up the circuit. Hence, the total power consumption essentially depends on the number of logic cells in a circuit, the connections between them, and the fact how the cells are built. These properties are a result of design decisions that are taken at the system level (overall system architecture, used algorithms, hardware/software splitting, *etc.*), the architecture level (specific implementation of hardware and software components), the cell level (design of the logic cells), and the transistor level (semiconductor technology used to implement the MOS transistors of the logic cells).

When operating a CMOS circuit, the circuit is provided with the constant supply voltage V_{DD} and with input signals, as shown in Figure 3.1. The logic

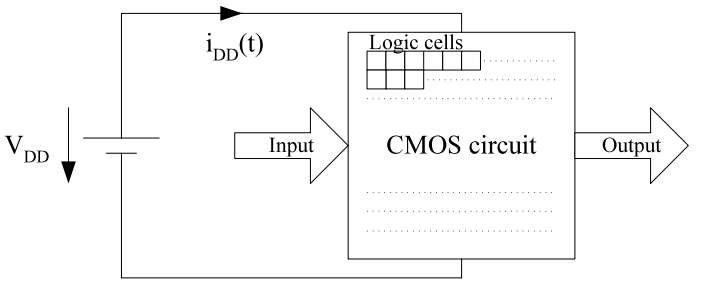

Figure 3.1. Power consumption of CMOS circuits.

cells in the circuit process the input signals and draw current from the power supply. We denote the total instantaneous current by $i_{DD}(t)$ and the instantaneous power consumption by $p_{cir}(t)$. Hence, the average power consumption P_{cir} of the circuit over time T can be calculated according to (3.1).

$$P_{cir} = \frac{1}{T}\int_0^T p_{cir}(t)dt = \frac{V_{DD}}{T}\int_0^T i_{DD}(t)dt \tag{3.1}$$

As pointed out in Section 2.3.2, logic cells are usually implemented using complementary CMOS. We now use the simplest CMOS cell, the CMOS inverter, to describe when and why CMOS cells dissipate power. The discussion of the inverter is representative for all other cells, because all CMOS cells are built based on complementary pull-up and pull-down networks. In case of an inverter, these networks consist of the two transistors $P1$ and $N1$, see Figure 3.2. In case of more complex gates, more PMOS and NMOS transistors are necessary for these networks.

The power consumption of an inverter can essentially be divided into two parts. The first part is the static power consumption P_{stat}. This is the power that is consumed if there is no switching activity in a cell. The second part of the power consumption is the dynamic power consumption P_{dyn}. In addition to the static power, a cell consumes dynamic power if an internal signal or an output signal of a cell switches. The total power consumption of a cell is the sum of P_{stat} and P_{dyn}.

3.1.1 Static Power Consumption

CMOS cells are built in such a way that their pull-up network and their pull-down network are never conducting at the same time for constant input signals. For example, in case of the CMOS inverter shown in Figure 3.2, $P1$ is conducting and $N1$ is insulating if the input a is set to GND. Vice versa, $P1$ is insulating and $N1$ is conducting if the input a is set to V_{DD}. In both cases, there is no direct connection between the V_{DD} line and the GND line.