Chapter 2

CRYPTOGRAPHIC DEVICES

For the discussion of power analysis attacks and countermeasures, it is helpful to have some basic knowledge about cryptographic devices. In particular, it is helpful to have a basic understanding of how they are built. This chapter provides this information in compact form. It is intended for readers without a background in hardware design.

First, we sketch the typical components of cryptographic devices. Second, we talk about the design flow that is used to build them. This means, we discuss the sequence of steps that are necessary to get from the specification of a device to the actual device. Last, we focus on logic cells. In particular, we give a brief introduction to complementary CMOS, which is the most popular technique to implement logic cells for digital circuits. This exposition follows the notation that is used in [RCN03], which is a popular book about the design of digital circuits.

2.1 Components

Cryptographic devices usually consist of several components. Each of these components implements a specific functionality, such as the encryption of data or the storage of cryptographic keys. The components of cryptographic devices can essentially be divided into two groups. The components in the first group perform cryptographic operations, e.g. a digital circuit that performs encryptions. The components in the second group handle data of the cryptographic operations, e.g. non-volatile memory that provides an encryption key. Below we list the most important components of typical cryptographic devices.

- **Dedicated Cryptographic Hardware:** This component includes all hardware that is solely dedicated to performing cryptographic operations, e.g. a dedicated cryptographic circuit that implements AES.

Figure 2.1. AES encryption chip in a PLCC package.

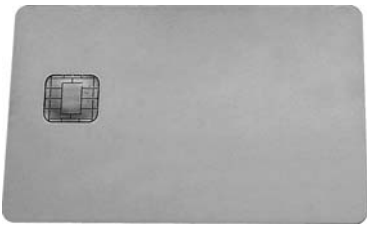

Figure 2.2. Cryptographic smart card.

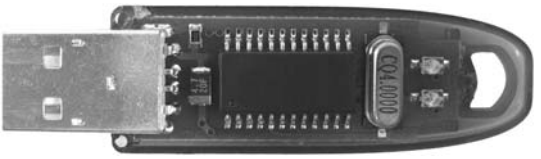

Figure 2.3. Cryptographic device in a USB token.

- **General-Purpose Hardware:** This component includes all general-purpose hardware that is used to perform cryptographic operations, e.g. a microcontroller that is programmed to perform AES encryptions.
- **Cryptographic Software:** This component consists of any type of software that implements cryptographic operations, e.g. software that implements AES.
- **Memory:** This component stores data of cryptographic operations, e.g. AES encryption keys.
- **Interface:** This component handles the data transfer to and from a cryptographic device. Cryptographic applications impose special demands on the interface. It is for example crucial that the interface prevents sensitive data, like a cryptographic key, from unauthorized access from the outside.

The components of cryptographic devices can be implemented either on separate chips or on a single chip. If they are implemented on separate chips, the chips need to be mounted on a printed circuit board (PCB). Suitable packages for chips that are mounted on a PCB are for example the dual in-line package (DIP) or the plastic-leaded chip carrier (PLCC) as shown in Figure 2.1. Examples of cryptographic devices that are built based on multiple chips are cryptographic acceleration cards or hardware security modules (HSMs).