Chapter 1

INTRODUCTION

Smart cards are frequently used as cryptographic devices to provide strong authentication of users and to store secret information securely. Smart cards are among the most critical components of modern security systems.

When Kocher *et al.* [KJJ99] showed in 1998 that power analysis attacks can efficiently reveal the secrets of smart cards, the belief in the security of cryptographic devices was shattered. This book describes why power analysis attacks work, how they can be conducted, and how they can be counteracted.

In this chapter, we briefly explain the use of cryptographic devices and cryptography in modern security systems. We survey different kinds of attacks on cryptographic devices, and we present a concrete example of a power analysis attack. Furthermore, we provide an overview of countermeasures against power analysis attacks.

1.1 Cryptography and Cryptographic Devices

Modern security systems use cryptographic algorithms to provide confidentiality, integrity, and authenticity of data. Cryptographic algorithms are mathematical functions that typically take two input parameters: a message (which is also called plaintext) and a cryptographic key. The cryptographic algorithm maps these parameters to an output, which is called ciphertext. This process is called encryption. In modern cryptography, the cryptographic algorithm itself is assumed to be known. This means that all details about it are publicly available and only the cryptographic key is kept secret. This important principle goes back to Auguste Kerckhoffs who was a Dutch cryptographer of the 19th century.

We distinguish between symmetric and asymmetric cryptography. In symmetric cryptography, the entities that communicate share a common secret key. A well-known example for a symmetric encryption algorithm is the *Advanced*

Encryption Standard (AES) [Nat01]. It is a block cipher, which means that it encrypts blocks of texts of a fixed size. In the case of AES, the block size is defined to be 128 bits. The key size can be 128, 192, or 256 bits. The versions of AES are called accordingly: AES-128, AES-192, and AES-256. In this book we use the abbreviation AES to refer to AES-128. An overview of the working principle of AES is given in Appendix B. Due to its widespread use, all examples of power analysis attacks in this book target implementations of AES.

In asymmetric cryptography, every user has a key pair. The key pair consists of a public parameter, which is called the public key, and a secret parameter, which is called the private key. There are many asymmetric cryptographic algorithms in use today. The most popular algorithm is the *Rivest-Shamir-Adleman* (RSA) algorithm [RSA78]. RSA keys have at least $1\,024$ bits in today's applications. This prevents practical attacks on RSA.

Breaking a cryptographic algorithm typically means finding the secret key based on some public information, which can be for instance pairs of plaintexts and ciphertexts. A cryptographic algorithm is considered to be secure in practice if there is no attack known that can break it within a reasonable amount of time and with a reasonable amount of computing power. A cryptographic algorithm is considered to be computationally secure if breaking it requires computing power that is not available in practice. Many algorithms are designed such that the effort of breaking them grows exponentially with the number of bits of the key. Consequently, the length of the key is an important factor in the security of a cryptographic algorithm. The notion of computational security is stronger than the notion of practical security. Algorithms that are popular today are considered to be computationally secure.

One property of modern symmetric and asymmetric cryptographic algorithms is that they can be efficiently performed by a computer. This implies that the key that is used for such an algorithm needs to be stored on the computer as well. However, typical personal computers (PCs) are rather insecure platforms. Viruses and worms spread via the Internet and frequently infect a large number of PCs within a short time. Hence, unless special attention is paid to its configuration, a PC is not an adequate platform to store valuable assets. Cryptographic keys are such valuable assets. For instance, knowing somebody's secret key might allow someone to pose as that person. Closed platforms such as smart cards are more suitable for storing cryptographic keys. Typical smart cards are not connected to the Internet and do not allow software to be installed. They can be considered as a protected environment that stores keys and that performs cryptographic operations. A smart card is an example of a cryptographic device. Other examples of cryptographic devices are USB (Universal Serial Bus) tokens or contactless devices such as RFID (Radio-Frequency Identification) tags.