Chapter 11

CONCLUSIONS

When we started writing this book, we thought that the final manuscript would have about 200 pages. However, after having finished the first couple of chapters, we realized that the final manuscript would get significantly longer. Power analysis attacks are a very interdisciplinary topic. Hence, these attacks have attracted the attention of people with very different backgrounds. This has lead to a large number and a great variety of publications that discuss power analysis attacks from many different points of view.

The different views on power analysis attacks can essentially be categorized into two groups. On the one hand, power analysis attacks can be viewed as a mathematical problem. The goal is to find mathematical models that describe the leakage of cryptographic devices in order to build secure systems based on these models. This line of thinking has lead to countermeasures like masking. On the other hand, power analysis attacks can be viewed as an engineering problem that can be solved by decreasing the leaking signal or by increasing the noise. This line of thinking has lead to the different hardware countermeasures including DPA-resistant logic styles. It has been very fruitful during the last years that there is more than one approach to model and to counteract power analysis attacks. The two approaches have continuously stimulated new research on attacks and countermeasures.

The motivation for writing this book was to provide a comprehensive overview of the research on this topic. Furthermore, our goal was also to provide an introduction to power analysis attacks for people who start working in this field. Obviously, it is not possible to do an in-depth discussion of every aspect of power analysis attacks in a single book. However, we have tried to put together the aspects that we consider to be the most important ones. We now provide specific conclusions for the attacks and countermeasures that have been explained in this book. Subsequently, we provide some general conclusions.

11.1 Specific Conclusions

In the introduction of this book we have pointed out that cryptographic devices have become essential building blocks of many security-sensitive systems. Consequently, it is important to study their resistance against power analysis attacks. The example provided in Chapter 1 has shown that conducting power analysis attacks is simple, although expertise from many different fields is required. Using an off-the-shelf oscilloscope and following the original paper of Kocher *et al.* allows performing DPA attacks on unprotected implementations of AES without actually knowing the details of the implementation.

However, in order to improve power analysis attacks and in order to develop countermeasures it is necessary to understand how cryptographic devices work, how they are built, and how they consume power. This is why Chapters 2 and 3 have introduced these topics. Based on these chapters we have discussed many aspects of power analysis attacks and countermeasures in this book. The following paragraphs summarize the most important issues concerning measurement setups, characteristics of power traces, SPA attacks, DPA attacks, template attacks, software countermeasures, hardware countermeasures, and DPA-resistant logic styles.

Measurement Setups. Building a measurement setup is the first task that is needed in order to perform power analysis attacks in practice. However, although this task is crucial, there exist almost no publications on this topic. In Chapter 3, we have put together the experiences we have gained about measurement setups during the last years. We hope that this contribution stimulates a broader discussion of this topic. Such a discussion would help to make fair comparisons of attack results that have been obtained using different measurement setups.

In Chapter 3, we have distinguished two kinds of noise that account for the quality of a measurement setup. There is electronic noise on the one hand and switching noise on the other hand. The main part of electronic noise is typically caused by conducted and radiated emissions of other devices than the attacked one, e.g. clock generators, PCs, LCDs, *etc.* Hence, this kind of noise can be reduced by shielding. Switching noise is caused by cells of the attacked circuit that are not relevant for the attack. It can be reduced by using low clock frequencies and by using small probes that only measure the power consumption of a part of the attacked device.

As a general strategy to perform power analysis attacks, we recommend to characterize the noise characteristics of the measurement setup before performing power analysis attacks. The electronic noise should be analyzed right after having built the setup. Knowing the electronic noise of the setup is necessary for decisions like the number of traces that are used to build templates and for the calculation of the correlation coefficient occurring in DPA attacks.