Review of the book

"Power Analysis Attacks: Revealing the Secrets of Smart Cards"
by Stefan Mangard, Elisabeth Oswald and Thomas Popp
Springer, 2007

ISBN: 978-0-387-30857-9

Arnaud Tisserand
CNRS, IRISA Laboratory, Lannion, France

Abstract: This book provides a very clear, complete and highly illustrated presentation of power analysis methods used to extract secret information from cryptosystems such as smart cards. All concepts are progressively introduced, mathematically analyzed and illustrated using many real attacks results. The main attack methods and some variants are presented. Standard countermeasures used to protect cryptosystems against power analysis attacks are also presented. Limitations and efficiency aspects of attacks and protections methods are discussed. Both software and hardware implementations on smart cards are targeted.

1 What the book is about

The security of a cryptosystem (cryptographic algorithms and protocols, cryptographic keys and cryptographic device used for implementation) does not only depend on its theoretical quality (e.g. use of robust algorithms and parameters, certified protocols and long enough cryptographic keys). Physical attacks can be used to break a system. Side channel attacks exploit the dependency between secret information used in the cryptosystem and some physical values measured on/around the cryptosystem (e.g. power consumption, electromagnetic radiation, timing information) to break the system. A well-known example of side channel attack is the case a thief attempting to open a safety box using a stethoscope. The analysis of the clicking sound may, hopefully, reveal the secret lock combination.
This book deals with a specific kind of side channel attack used to extract secret information from a cryptosystem using an appropriate analysis of its power consumption. Those attacks are called *power analysis attacks*. Power consumption traces are recorded during the execution of the cryptosystem using a high-speed oscilloscope. The analysis of the power traces may provide information on the secret key. A typical example is the case of a program line such as the following:

$$\texttt{if} \quad b = 0 \quad \texttt{then} \quad r = op_1(x) \quad \texttt{else} \quad r = op_2(x)$$

If the power consumptions for operations op_1 and op_2 are different (amplitude/duration), the recorded power traces show differences for $b = 0$ and $b = 1$. If b is a secret key bit, the power trace directly "shows" the value of b on the oscilloscope. This is the idea behind *simple power analysis* (SPA). One problem is where the attacker should look at a difference in the trace (timing aspects are very important).
When differences are too small (weak signal and/or noisy environment), simple power analysis does not work anymore. Then, statistical methods have to be used to extract secret information using a large amount of power traces. This is the idea behind *differential power analysis* (DPA). The set of power traces is analyzed and compared to a theoretical power model of the cryptosystem (or parts of it). Those attacks are very efficient in practice.
This book also deals with some protection methods, called *countermeasures*, used to protect cryptosystems against some power analysis attacks at software and hardware levels. The principle of several basic countermeasures is described. Countermeasures make the power consumption of the device independent

of the secret information used in the cryptosystem. Protected versions can also be attacked if the independence is not perfect. The analysis of power attacks on protected cryptosystems shows limitations and efficiency aspects for both attacks and countermeasures.
This book provides numerous and highly illustrated examples (numerical values, specific equations, figures) from real attacks, and countermeasures, on an AES algorithm implemented in smart card context. A first implementation is done in software using an 8051-compatible microcontroller. The second implementation is done in hardware for a dedicated AES core which can be used as a coprocessor in the smart card. Some references to power attacks and countermeasures for asymmetric cryptography are provided in several chapters of the book.

2 Summary of the book

The structure of the book is as follows:

First pages: foreword (2 pages), preface (4 pages), notations (3 pages), glossary (3 pages)

Chapter 1: Introduction (pages 1–14)

A brief overview on cryptographic algorithms and cryptographic devices is provided. Power analysis attacks are introduced, defined and placed in the common categorization of physical attacks. A basic attack example is provided for a software implementation of AES on an 8051-compatible microcontroller. This simple example clearly illustrates the dependency of the secret data used in the microcontroller and the instantaneous power consumption of the microcontroller. This dependency is the central point for power analysis attacks. Countermeasure principles are introduced.

Chapter 2: Cryptographic Devices (pages 15–26)

The basic elements used in cryptographic circuits are introduced. Their basic behavior with respect to their power consumption is summarized. Those elements are the fundamental blocks of cryptographic devices in dedicated hardware implementations but also for software implementations (cryptographic codes run on a processor implemented in a circuit). The typical design process — the design flow — of a digital integrated circuit is also summarized. A good knowledge of this process is important to design and use efficient attacks and countermeasures.

Chapter 3: Power Consumption (pages 27–60)

The power consumption sources in CMOS digital integrated circuits are described, analyzed and modeled at different levels: transistor, gate and circuit. Standard power simulation methods are described. The main power models, Hamming weight and Hamming distance models, are described in the context of power attacks. Typical power measurements setups are presented. The setups used for all the examples provided in the book are described. Noise sources and noise models for power consumption and power measurement are described and used to define quality criteria for power measurement setups.

Chapter 4: Statistical Characteristics of Power Traces (pages 61–100)

The elements or components of power traces are introduced in the attack context. What components can be used for an attack? What components limit the attack or reduce its efficiency? Basic statistical definitions, distribution models, distribution test methods are recalled and illustrated using complete numerical examples. This part is very clear and complete, it allows to understand all details given in the book without having to read maths books. For teaching and attack implementation point of views, this is a noticeable effort. The data dependency and the operation dependency to power consumption are presented and widely illustrated using statistical analysis examples. Signal and noise characteristics, from signal processing field, are described and used to model the efficiency and the limits of power attacks. For instance, the number of traces required to allow efficient attacks is deduced from statistical parameters. This number should not be too large for attack duration and cost purpose, but large enough to ensure the attack success with a high probability.

Chapter 5: Simple Power Analysis (pages 101–118)

The basic power attack is presented: simple power analysis. It directly exploits the dependency between the power consumption (i.e. patterns in the power trace) and secret information. If the patterns in the power trace can be directly correlated to some operations and/or values depending on secret information (e.g. key bits), then this attack is very efficient. Standard improvements on SPA are presented: template attacks and collision attacks. Only SPA attack examples on AES (and mainly for software implementation) are provided in this chapter. Some references are cited for SPA attacks against asymmetric cryptography algorithms.

Chapter 6: Differential Power Analysis (pages 119–166)

This is the biggest chapter of the book, and there is a good reason for that. Differential power analysis is the most efficient and most used method in practice. It is also the base for many variants and improvements. The authors provide a very complete and highly illustrated description of all steps of a DPA attack. The mathematical formulation for all steps is also described. This complete description makes it usable for the software implementation of the complete attack. Several variants for various statistical parameters are defined, analyzed and illustrated using real attack examples. The efficiency of DPA attacks is studied using the computation of the number of required traces (derived from statistical models). Many numerical examples are provided and clearly illustrated.

Chapter 7: Hiding (pages 167–200)

The principle of this type of countermeasure is to make the power consumption independent of the intermediate values manipulated and intermediate operations performed in the device. This can be done using a device and/or algorithms with a random power consumption (e.g. random dummy operations, random shuffling of operations). This can also be done using a device, algorithms and data representations where the power consumption is always the same for all operations and for all manipulated values. Several countermeasures are described to make the power consumption constant. The authors analyze and discuss the cost and the practical applicability of those countermeasures.

Chapter 8: Attacks on Hiding (pages 201–222)

Implementing perfect hiding countermeasures is not possible. So, some power attacks are still possible, but maybe their cost is very high. For several countermeasures and attacks methods, the authors discuss the effectiveness of the attack and the quality of the countermeasure.

Chapter 9: Masking (pages 223–244)

The principle of this type of countermeasure is to make random the intermediate values processed by the cryptosystem. Intermediate values are combined (using more or less advance mathematical operations) with a random mask which changes from execution to execution. The cryptosystem has to be modified to integrate masking and unmasking operations. If the masks are random, there is no correlation between the power consumption and the secret information. Several masking solutions for hardware and software implementations are described and compared.

Chapter 10: Attacks on Masking (pages 245–272)

A perfect masking scheme requires that each intermediate value must be masked using a single-use mask. In practice, this is not possible for cost reasons. Not all operations are masked, some masks are shared and reused, etc. Then some correlations between masked intermediate values may be found. Several attacks specific to masked systems are described and compared.

Chapter 10: Conclusions (pages 273–282)

Specific conclusions are presented for power measurements setups, statistical characteristics of power traces, the major attack methods (SPA, DPA, template) and for some countermeasures (in software, in hardware and for specific logic styles resistant to DPA attacks). Then general conclusions are given.

Appendix A: DPA Article by Kocher *et al.* (pages 283–294)

Reprint of the foundation paper "*Differential Power Analysis*" by Paul Kocher, Joshua Jaffe and Benjamin Jun. This paper was published in the proceedings of CRYPTO conference in 1999 (LNCS vol. 1666, pp. 388–397).

Appendix B: The Advanced Encryption Standard (pages 295–306)

Short overview of the AES algorithm and basic software implementation. A very quick description of basic hardware implementation is also provided. This AES overview is very short but sufficient to understand attack "points" used in previous chapters. For a more complete reference on AES see, for instance, the book "The Design of Rijndael: AES - The Advanced Encryption Standard" by J. Daemen and V. Rijmen, 2002.

Last pages: references (pages 307–328), author index (pages 329–334), topic index (pages 335–337)

Many chapters end with comments and references to research works in a useful section entitled "Notes and Further Reading".

3 What is the book like (style)?

The book is decomposed into self-sufficient and highly illustrated chapters for each concept or method. The concepts and methods are progressively introduced and analyzed. This makes the book a very good reference for learning and teaching.
The authors cover all relevant aspects of the field: concepts, definitions, mathematical models and developments, numerous real examples with details, clear illustrations, references to foundation works, discussions on the cost and efficiency of the presented solutions.
The book has been carefully written. It clearly and rigorously describes all required tools from theory to practical aspects. The numerous examples and illustrations make the reading of the book very pleasant.

4 Would you recommend this book?

I highly recommend this very nice book.

There are several ways to read it and several possible audience levels. Each chapter presents, in a self-sufficient description, one specific aspect of power analysis attacks. One can quickly find answers to specific questions by reading parts of just one or two chapters. The complete book can be used for teaching with step-by-step guidance and clearly defined lessons. Technical descriptions and references can be used to mount power analysis attacks.

The reviewer is a CNRS researcher at IRISA laboratory in Lannion, France.