

Preface

This book has been written to provide more in-depth details to any user about how to analyze the security of an embedded device. Around two decades ago, the security of those devices was still only relying on mathematical complexity and computational infeasibility to force cryptographic systems. Unfortunately, during the execution of cryptographic algorithms, unintentional leakage may be observed. Indeed, the power consumption or the electromagnetic emanations of the device are correlated to the encryption/decryption process. Those unintended channels are called *side-channel*. Our work was not targeted at the discovery of new *side-channel* sources but rather at a thorough investigation of two of them: the power consumption and the electromagnetic emanation in the near-field domain. In this respect, we dealt with three different aspects of the problem:

- We carried out many experiments on small microcontrollers but also on FPGAs in order to provide an explanation on the sources and on the set up of an efficient measurement process. Moreover, we provide the XY scanning pictures of the electromagnetic field radiated by a small microcontroller.
- Obtaining several measures of the observed side-channel, how is it possible to statistically analyze these observations? We detail here the different methods available and we introduce an enhancement in the Template Attack process with Principal Component Analysis.
- Finally, on the basis of this experience, we tried to answer the following question: *Is it possible to provide a theoretical tool to evaluate secure implementations?* The idea was to follow the notion of *Physical Computer* introduced by Micali and Reyzin. In this respect, we provide here two metrics that we consider necessary to evaluate both the strength of the adversary and the information held in the leakage. Respectively, we choose the average success rate and the Shannons mutual information.

Frisco, TX, September 2012

Eric Peeters

Advanced DPA Theory and Practice
Towards the Security Limits of Secure Embedded
Circuits

Peeters, E.

2013, XVI, 139 p., Hardcover

ISBN: 978-1-4614-6782-3