IST-2002-507932

ECRYPT

European Network of Excellence in Cryptology

Network of Excellence

Information Society Technologies

D.VAM.15
Theoretical Models for Side-Channel Attacks

Due date of deliverable: 31 July 2007
Actual submission date: 30 June 2008

Start date of project: 1 February 2004 Duration: 4 years

Lead contractor: UCL Crypto Group

Revision 1

Project co-funded by the European Commission within the 6th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Theoretical Models for Side-Channel Attacks

Editor
François-Xavier Standaert (UCL)

Contributors
Lejla Batina (KUL), Thomas Eisenbarth (RUB), Benedikt Gierlichs (KUL),
François Koeune (UCL), Elisabeth Oswald (BRIS), Stefan Tillich (IAIK).

30 June 2008
Revision 1

The work described in this report has in part been supported by the Commission of the European Communities through the IST program under contract IST-2002-507932. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Side-channel attacks are an important class of cryptanalytic techniques in which an adversary exploits the physically observable features of a target device in order to recover secret information. They are therefore less general - since specific to a given implementation - but often much more powerful than classical cryptanalysis, and are considered very seriously by cryptographic devices manufacturers. Because of their intrinsic relation with the physical specificities of microelectronic circuits, such attacks are also difficult to evaluate, prevent and model. As a consequence, research in this field has first been oriented towards ad hoc countermeasures and security evaluations. This resulted in a succession of attacks, protections and attacks against protected designs. Such results summarized in [**?**] typically exhibit the recent and rapidly evolving nature of physically observable cryptography.

By opposition to the combination of ad hoc solutions for the analysis of side-channel attacks, the goal of theoretical models in physically observable cryptography is to provide a sound framework allowing to evaluate cryptographic devices in a fair manner. But arguably because of the difficulty to connect physical leakages with classical security notions, the first attempts to model and provably address side-channel attacks have shown limitations in their application to practice. Such limitations are mainly caused by two types of reasons. First, cryptographic devices have to be reasonably efficient, which prevents from implementing side-channel countermeasures of which the cost is prohibitive. Second, the notion of physical leakage is highly device-dependent which makes general conclusions difficult to obtain. For example, Micali and Reyzin initiated an analysis of side-channels taking the modularity of physically observable computations into account. It notably defines the notion of *physical computer* that is the combination of an abstract computer (*i.e.* a Turing machine) and a leakage function. The model in [**?**] is very general, capturing almost any conceivable form of physical leakage. But because of the great generality of the assumptions, the obtained positive results (*i.e.* leading to useful constructions) are quite restricted in nature, and it is not clear how they apply to practice. This is especially true for primitives such as modern block ciphers for which even the black box security cannot be proven. As a consequence of this state-of-the art, the goal of the present deliverable is to consider the possibility to develop a specialized model for side-channel attacks that could lead to theoretically meaningful and practically useful conclusions. Due to the challenging nature of the question, no definitive answer will be provided. Rather, we browse the different type of works that have been published during the ECRYPT project and relate to the question of sound models for side-channel attacks.

First and directly related to the modeling of side-channel attacks, the framework in [**?**] formally considers the problem of side-channel key recovery that is the most frequently found in practice. It discusses how basic (but practically essential) questions such as "*how to compare two implementations?*" and "*how to compare two side-channel adversaries?*" are central in the understanding of physically observable devices. In order to answer these questions, [**?**] proposes a methodological division between implementations and adversaries. That is, it extends the model of Micali and Reyzin in order to quantify both the implementation issue (*i.e.* "*how good is my implementation?*") and the adversarial issue (*i.e.* "*how strong is my adversary?*") in the physically observable setting. It is then argued that such a methodological separation of both concerns brings essential insights and avoids previous confusions in the analysis of side-channel attacks. As a consequence, two types of evaluation metrics are introduced. First, an information theoretic metric is used to measure the amount of information that is provided by a given implementation. Second, an actual security metric is used to

measure how this information can be turned into a successful attack. Actual candidates for the metrics are introduced and shown to allow comparing different implementations or adversaries. Some important connections between the metrics are also demonstrated. Eventually, a unified evaluation methodology for side-channel attacks is provided. First applications of this framework to the analysis of cryptographic hardware implementations can be found in [**?**, **?**].

Following this framework, a first important open problem is the efficient computation of the various metrics introduced to evaluate cryptographic hardware devices. As far as the comparison of implementations is concerned, the evaluation of an information theoretic metric implies the approximation of the leakage probability density functions. But in practice, the number of samples in the side-channel leakages and the number of plaintexts and keys[1] for which these distributions have to be estimated can be very large and lead to unrealistic complexities. As a consequence, different methods have been introduced to handle such problems in a systematic manner. Namely, data dimensionality reduction techniques such as the Principal Component Analysis can be used to select the actual time samples for which the leakage distributions are to be approximated [**?**]. Similarly, the stochastic models in [**?**] can be used to reduce the number of distributions to estimate in an optimal manner, *i.e.* leading to a minimum loss of information. In both cases, the inherent complexity of the side-channel problem implies to combine sound theoretical principles with good heuristics.

In parallel to the evaluation of implementations in a strong adversarial complex, another important theoretical question relates to the development of flexible side-channel adversaries. That is, side-channel attacks frequently require some knowledge about the target device in order to efficiently exploit the leakages. As a typical example, attacks such as in [**?**] assume a so-called "Hamming distance" leakage model. Since such models are not always available to the adversary, in particular when countemeasures against side-channel attacks are implemented, an interesting research direction is the development of attacks that are successful without doing assumptions on the leakage model. In this context, the goal is not to be efficient anymore (in general, the better one knows about a leakage model, the better one can attack) but to be generic. Interestingly, the conditional entropy that can be used as an evaluation metric also has interesting properties when used in such generic attacks. The mutual information analysis introduced in [**?**] is a first example of such side-channel disctinguisher.

Finally, next to the evaluation of implementations and development of attacks, a final goal of theoretical models for side-channel attacks is to design and argue about the security of new constructions. The pseudo random number generator in [**?**] is an example of such designs. It shows how security arguments for cryptographic devices can be devised if one combines limited information leakage and limited computational power for the adversaries.

In summary, various contributions of the ECRYPT Network of Excellence can be related to the formal analysis of side-channel attacks, including [**?**, **?**, **?**, **?**, **?**, **?**, **?**]. This list is not claimed to be exhaustive and several other proposals coexist in the literature. Due to the recent nature of the research topic, these works also constitute directions for future investigations and research. We believe that the aforementioned elements are important in the understanding of physically observable cryptography and contain reasonable starting points for a more theoretical discussion on physically observable cryptography.

[1] And possibly other parameters, *e.g.* masks in protected designs such as in [**?**].

Bibliography

[1] Cédric Archambeau, Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template attacks in principal subspaces. In Goubin and Matsui [**?**], pages 1–14.

[2] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.

[3] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis - a generic side-channel distinguisher. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442, Washington DC,US, 2008. Springer-Verlag.

[4] Louis Goubin and Mitsuru Matsui, editors. *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*. Springer, 2006.

[5] Louis Goubin and Jacques Patarin. Des and differential power analysis (the "duplication" method). In Çetin Kaya Koç and Christof Paar, editors, *CHES*, volume 1717 of *Lecture Notes in Computer Science*, pages 158–172. Springer, 1999.

[6] François Macé, François-Xavier Standaert, and Jean-Jacques Quisquater. Information theoretic evaluation of side-channel resistant logic styles. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 427–442. Springer, 2007.

[7] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks - Revealing the Secrets of Smartcards*. Springer, April 2007.

[8] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004.

[9] Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal Malkin, and Moti Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In Masayuki Abe and Virgil D. Gligor, editors, *ASIACCS*, pages 56–65. ACM, 2008.

[10] Werner Schindler, Kerstin Lemke, and Christof Paar. A stochastic model for differential side channel cryptanalysis. In Josyula R. Rao and Berk Sunar, editors, *CHES*, volume 3659 of *Lecture Notes in Computer Science*, pages 30–46. Springer, 2005.

[11] François-Xavier Standaert, Eric Peeters, Cédric Archambeau, and Jean-Jacques Quisquater. Towards security limits in side-channel attacks. In Goubin and Matsui [**?**], pages 30–45.

[12] Francois-Xavier Standaert, Tal G. Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. Cryptology ePrint Archive, Report 2006/139, 2006. `http://eprint.iacr.org/`.