Physically Secure Cryptographic Computations
From Micro to Nano Electronic Devices

Jean-Jacques Quisquater and François-Xavier Standaert
UCL Crypto Group, Université Catholique de Louvain
e-mail: `jjq@dice.ucl.ac.be,fstandae@uclouvain.be`

Abstract - A recent branch of cryptography focuses on the physical constraints that a real-life cryptographic device must face, and attempts to exploit these constraints to expose the devices secrets. This gave birth to implementation-specific attacks, which often turned out to be much more efficient than the best known cryptanalytic attacks against the underlying primitive as an idealized object. This talk aims to review some of the physical weaknesses of present technologies and to discuss how future technological scalings may affect these physical security issues.

Physical attacks - The classical cryptographic setting only considers abstract computational adversaries, modeled as Turing machines. By contrast, the aim of physical cryptography is to include adversaries taking the specificities of actual cryptographic implementations into account. Side-channel and fault attacks are typical examples of such techniques. In side-channel attacks, an adversary monitors the physical leakages of a device (such as its power consumption [8] or electromagnetic radiation [1]) in order to learn about its internal configuration. In fault attacks [2], he tries to affect a devices's proper behavior (*e.g.* by the use of glitches or lasers) in order to obtain the result of some faulty computations. Both side-channels and fault insertion provide adversaries with enhanced capabilities that can be turned into very powerful attacks. Their efficiency depends on the physical strength and granularity of the adversary. That is: "*How precisely can he monitor the leakages / insert a fault?*".

Technology scalings - For four decades, the semiconductor industry has progressively scaled its devices down to the nanometer size. But the end of scaled CMOS devices (presently 45-nm large) predicted by the International Technology Roadmap for Semiconductors [6] underlines the need of alternative (nano) technologies to extend Moore's law beyond 2016. Just as for present digital circuits, alternative (*e.g.* optical, electromechanical, quantum) technologies not only raise performance issues, but security ones. For example, side-channel and fault attacks are worth being re-considered in these new contexts.

As far as side-channel attacks are concerned, it is noticeable that certain physical leakages are inherently attached to the notion of computation. Computing takes some time and, up to a certain extent (*e.g.* the possibility to carry out reversible computers [5]), requires some power. The execution time [7] or power consumption of a device can consequently be exploited as side-channels, whatever the (possibly nano) technology considered. By contrast, the actual representation and scale of these physical leakages is technology-dependent. For example, the dynamic power consumption in former CMOS devices could be exploited by side-channel adversaries through very simple leakage models (based on the switching activity). Technologies with little (or constant) dynamic power consumption would result in different needs for the adversary. Similarly, fault attacks are an issue for any cryptographic implementation, but technology scalings may affect the difficulty of inserting a fault within a device. For example, default and fault tolerance are generally more critical for smaller technologies [3]. Importantly, just as technologies are scaling down, *the means of physical adversaries are evolving too*. More precise measurement apparatus are developed for side-channel attacks (possibly at a lower price), higher computational powers are available to exploit the side-channel leakages or faulty computations via enhanced strategies.

Distributed information - While the very existence of physical threats for micro and nano electronic devices remains mainly unchanged with technology scalings, an important difference relates to the applications taking advantage of these technologies. Small embedded devices allow the distribution of digital information over a continuously larger spectrum of applications. Copyrighted medias, intellectual properties, medical or private identification data, . . . although protected by powerful cryptographic techniques, may be the target of various physical attacks. Radio Frequency Identification Devices and sensor networks raise additional privacy issues. As a matter of fact, with this "embedded systems everywhere" paradigm comes an "embedded security everywhere" question that is far from being answered by present technologies. Physical attacks are particularly critical with this respect.

Towards a physical cryptography - From a theoretical point of view, side-channel or fault attacks are less generic than classical cryptanalysis in the sense that they target a specific implementation rather than an abstract algorithm. This also makes their evaluation and analysis more difficult. "How to properly assess the security of a cryptographic implementation" has been a long standing open question. Consequently, the definition of sound evaluation criteria is an important aspect in the understanding of physical security issues. From sound criteria and methodologies directly derive properly understood tradeoffs. For example, *physical security generally has to be balanced with implementation cost in real world applications*. It requires to have a clear idea of what hardware cost and physical security actually mean. In this context, the building of concrete foundations for a physical cryptography appears as an important research challenge for the coming years. Separate attempts to model certain parts of the physical reality (*e.g.* fault or side-channel attacks [9], [10]) have been introduced. Their application to different technologies, combination within a unified framework and the design of implementations with provable security against various types of physical adversaries are interesting cryptographic research problems.

Conclusion - Physical attacks pose a serious threat to the security of cryptographic implementations. They have been largely applied to various algorithms implemented on CMOS devices [4]. But technology scalings are not expected to remove the theoretical threat of side-channel or fault attacks (although they could result in different constraints for the adversaries). Due to the proliferation of small embedded devices, the investigation of these physical security issues is particularly critical for future technologies and could serve as an evaluation criteria, just as cost and efficiency. For these purposes, it is important to develop good foundations for the understanding of physical cryptography. This requires to extend the classical cryptographic setting in order to establish a relation between the digital information and its physical representation.

Acknowledgements: François-Xavier Standaert is a postdoctoral researcher of the Belgian Fund for Scientific Research (F.N.R.S. - F.S.R.).

REFERENCES

[1] D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, *The EM Side-Channel(s)*, in the proceedings of CHES 2002, Lecture Notes in Computer Science, vol 2523, pp 29-45, Redwood City, CA, USA, August 2002.

[2] D. Boneh, R. DeMillo, R. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, proceedings of Eurocrypt 1997, Lecture Notes in Computer Science, vol 1233, pp 37-51.

[3] G. Bourianoff, *The Future of Nanocomputing*, in IEEE Computer, vol 36, num 8, pp 44-53, August 2003.

[4] ECRYPT Network of Excellence in Cryptology, *The Side-Channel Cryptanalysis Lounge* , http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html.

[5] B. Hayes, *Reverse Engineering*, in American Scientist, vol 94, num 2, pp 107-111, March-April 2006.

[6] International Sematech, *The International Technology Roadmap for Semiconductors*, 2001 Edition.

[7] P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*, in the proceedings of Crypto 1996, Lecture Notes in Computer Science, vol 1109, pp 104-113, Santa Barbara, California, USA, August 1996.

[8] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in the proceedings of Crypto 1999, Lecture Notes in Computer Science, vol 1666, pp 398-412, Santa-Barbara, California, USA, August 1999.

[9] S. Micali, L. Reyzin, *Physically Observable Cryptography*, in the proceedings of TCC 2004, Lecture Notes in Computer Science, vol 2951, pp 278-296, Cambridge, Massachusetts, USA, February 2004.

[10] F.-X. Standaert, T.G. Malkin, M. Yung, *A Formal Practice-Oriented Model for the Analysis of Side-Channel Attacks*, Cryptology ePrint Archive, Report 2006/139, 2006, http://eprint.iacr.org/2006/139