Physical Security

François-Xavier Standaert & Jean-Jacques Quisquater

UCL Crypto Group
Laboratoire de Microélectronique
Université catholique de Louvain
Place du Levant, 3, B-1348 Louvain-La-Neuve, Belgium
fstandae;jjq@uclouvain.be

A cryptographic primitive can be considered from two points of view: on the one hand, it can be viewed as an abstract mathematical object or black box (i.e. a transformation, possibly parameterized by a key, turning some input into some output); on the other hand, this primitive will in fine have to be implemented in a program that will run on a given processor, in a given environment, and will therefore present specific characteristics. The first point of view is that of classical cryptanalysis; the second one is that of physical security. Physical attacks on cryptographic devices take advantage of implementation specific characteristics to recover the secret parameters involved in the computation. They are therefore much less general, since specific to a given implementation, but often much more powerful than classical cryptanalysis, and are considered very seriously by cryptographic devices implementors.

Physical attacks can be classified in many ways. The literature usually sorts them along two orthogonal axes.

Invasive vs. non-invasive: invasive attacks require depackaging the chip to get direct access to its inside components; a typical example of this is the connection of a wire on a data bus to see the data transfers. A non-invasive attack only exploits externally available information (the emission of which is however often unintentional) such as running time, power consumption, ... One can go further along this axis by distinguishing local and distant attacks: a local attack requires close but external, i.e. non-invasive, proximity to the device under concern, for example by a direct connection to its power supply. As opposed, a distant attack can operate at a larger distance, for example by measuring electromagnetic field several meters (or hundreds of meters) away, or by interacting with the device through an internet connection.

Active vs. passive: active attacks try to tamper with the devices proper functioning; for example, fault-induction attacks will try to induce errors in the computation. As opposed, passive attacks will simply observe the device's behavior during its processing, without disturbing it.

Note that these two axes are well orthogonal: an invasive attack may completely avoid disturbing the device's behavior, and a passive attack may require a preliminary depackaging for the required information to be observable. These attacks are of course not mutually exclusive: an invasive attack may for example serve as a preliminary step for a non-invasive one, by giving a detailed description of the chip's architecture that helps to find out where to put external probes.

In parallel, physical attacks can also be classified according to the cost of the equipment and expertise required to carry out an attack. For example, a taxonomy for

physical adversaries has been proposed in [1]. Such classifications are typically provided by standardization bodies. Methodologies allowing to evaluate these cost issues are described in the FIPS 140-2 documentation [2] or the Common Criteria application of attack potential to smart cards [3, 4].

Eventually, some of the most frequently considered types of physical attacks include:

1. Tampering attacks (e.g. discussed in [5]).
2. Timing attacks (introduced in [6]).
3. Fault attacks (introduced in [7]).
4. Power analysis attacks (introduced in [8]).
5. Electromagnetic analysis attacks (introduced in [9, 10]).
6. Cold boot attacks (introduced in [11]).

References

1. D.G. Abraham, G.M. Dolan, G.P. Double, J.V. Stevens, *Transaction Security System*, in IBM Systems Journal, vol 30, num 2, pp 206- 229, 1991.
2. FIPS 140-2, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, December 3, 2002.
3. *Application of Attack Potential to Smart Cards*, Common Criteria Supporting Document, Version 2.1, April 2006, http://www.commoncriteriaportal.org
4. http://www.ssi.gouv.fr/archive/en/confidence/evalcertif.html
5. R.J. Anderson, M.G. Kuhn, *Tamper Resistance - a Cautionary Note*, USENIX Workshop on Electronic Commerce, pp 18-21, Oakland, California, November 1996.
6. 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.
7. D. Boneh, R.A. DeMillo, R.J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract)*, in the proceedings of EUROCRYPT 1997, Lecture Notes in Computer Science, vol 1233, pp 37-51, Konstanz, Germany, May 1997.
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. K. Gandolfi, C. Mourtel, F. Olivier, *Electromagnetic Analysis: Concrete Results*, in the proceedings of CHES 2001, Lecture Notes in Computer Science, vol 2162, pp 251-261, Paris, France, May 2001.
10. J.-J. Quisquater, D. Samyde, *ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards*, in the proceedings of E-smart 2001, Lecture Notes in Computer Science, vol 2140, pp 200-210, Cannes, France, September 2001.
11. J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, E.W. Felten, *Lest We Remember: Cold Boot Attacks on Encryption Keys*, USENIX Security Symposium 2008, pp 45-60, San Jose, California, USA, August 2008.