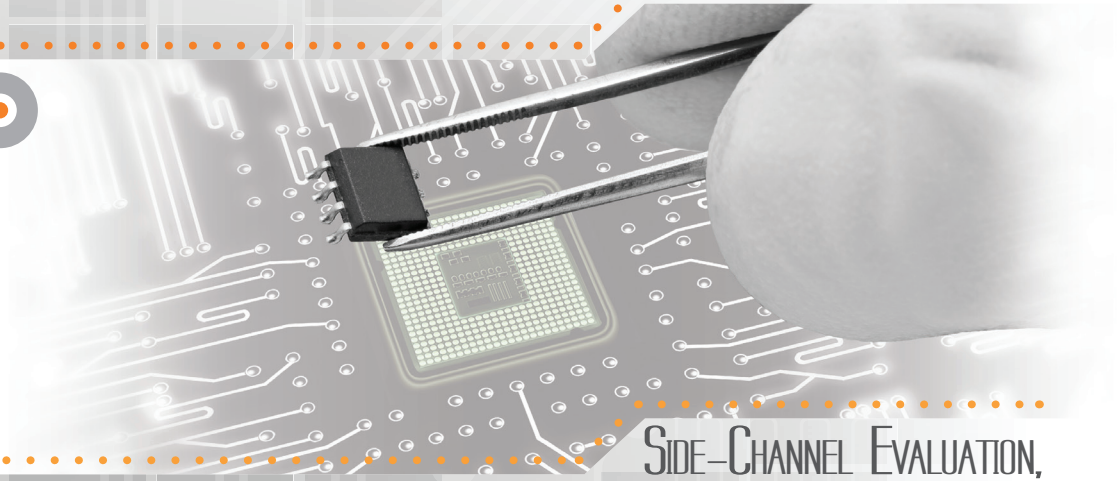
SCEPTIC



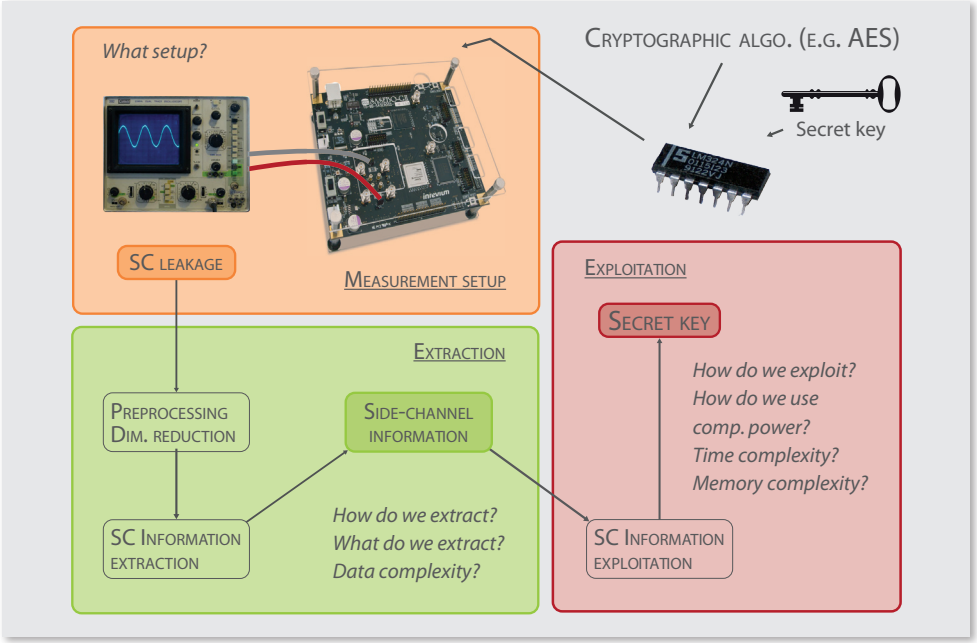
Side-Channel Evaluation, Protection and Tests for Integrated Circuits

RÉGION WALLONNE

UCL Université catholique de Louvain

Embedded devices are now ubiquitous in everyday applications: smartcards, RFID tags, electronic car keys... These applications raise many privacy and security concerns and require a protection using cryptographic primitives.

Exploiting unintended features, side-channel attacks can completely break an unprotected cryptographic device



For the last 20 years however, new attacks, specific to embedded devices, have been proposed and intensively studied. These attacks are called side-channel attacks as they make use of unintended features of the device, like its power consumption, to break its security.

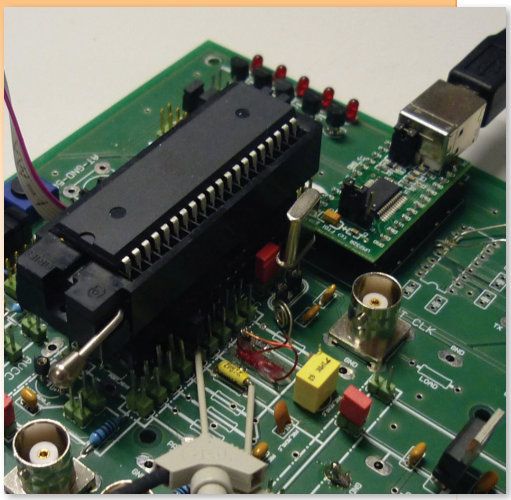
The industry devotes considerable efforts to protect devices with specific countermeasures

Side-channel attacks proved to be a very practical threat, sometimes needing only a few hundred measurements to break a secure token. They are taken very seriously by the industry where considerable efforts are dedicated to protect devices with specific countermeasures. Unfortunately, side-channel countermeasures are always a trade-off between cost and security. Evaluating the real security gain is important when looking for the best counter-measure to implement in a constrained environment like a smartcard.

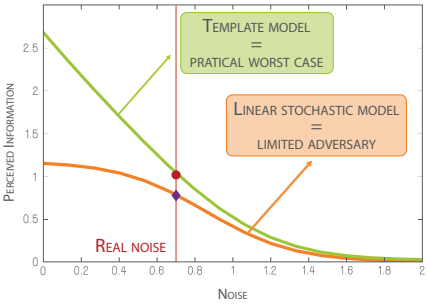
Evaluating the security of a protected device against side-channel attacks is not a trivial task. Indeed, many parameters can have an impact: the measurement setup, the computational power available, the attack used by the adversary...

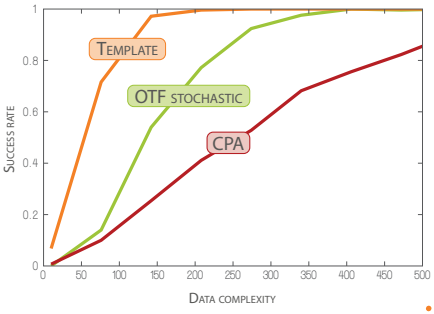
The most common mistake an evaluator can make is to assess the cleverness of the adversary instead of the security of the device.....

using suboptimal attacks or not taking advantage of the available computational power corresponds to evaluating the security for a limited adversary. Although considering limited adversaries can be reasonable in some cases, it can also lead to a false sense of security. Performing a fair evaluation of side-channel security requires thus an appropriate methodology in order to be sure of what we actually evaluate.



Comparing different adversaries and attack strategies





What we developed

Thanks to Walloon Region funding, we developed:

1) A **METHODOLOGY** for the evaluation of side-channel security. One of the goals of this methodology is to make a distinction between the evaluation of the electronic device and that of the adversary. We applied this methodology in published scientific papers[2,3].

2) An implementation of this methodology. This implementation consists in two parts: first a **MEASUREMENT BOARD**, used for the acquisition of side-channel leakages, and second a **DEMONSTRATION SOFTWARE**, used to automatically compute various side-channel security metrics. This software, developed in Java, is available for industrial exploitation (to be negociated).

3) In order to confirm its relevance, we applied our methodology to various **COUNTERMEASURES**[1]. We studied them to find out the most effective attacks in order to avoid overestimating the security gain.

References

[1] F.-X. Standaert, N. Veyrat-Charvillon, E. Oswald, B. Gierlichs, M. Medwed, M. Kasper, S. Mangard, The World is Not Enough: Another Look on Second-Order DPA, in the proceedings of Asiacrypt 2010, Lecture Notes in Computer Science, vol 6477, pp 112-129, Singapore, December 2010.

[2] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, D. Flandre, A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices, in the proceedings of Eurocrypt 2011, Lecture Notes in Computer Science, vol 6632, pp 109-128, Tallinn, Estonia, May 2011, Springer.

[3] M. Renauld, D. Kamel, F.-X. Standaert, D. Flandre, Information Theoretic and Security Analysis of a 65-nanometer DDSLL AES S-box, in the proceedings of CHES 2011, Lecture Notes in Computer Science, vol 6917, pp 223-239, Nara, Japan, September 2011, Springer.

Partnership We are looking for partners to undertake the production and exploitation of this new technology.

UCL Crypto Group
Place du Levant, 3 - 1348 Louvain-la-neuve
(+32) 10 47 81 41 - uclcryptogroup@listes.uclouvain.be