Evaluation flow for information leakage via the leakage current of an ASIC integrated circuit

Keywords : Side Chanel Attacks, digital circuits, leakage current

Context :
When implementing secure integrated circuits, the designer must take into account the robustness of his design against potential leakage sources for privileged data. These leakage sources can be exploited in different ways, with the assistance of mathematical methods. Guessing or retrieving a secret data is not impossible. The adversary may for example observe the power consumption of a circuit, or observe its magnetic emissions in order to have a deeper understanding of the circuit. In the context of our project, we are interested in the information contained in the leakage current, these leakage currents are a major concern for sub 100 nm technologies. Our approach is to verify the possibility of improving this type of attacks which exploit the leakage current.

Description of the internship :
The goal of this internship is to develop a characterization flow for the leakage current, The student at first, will have to perform an ASIC implementation of an AES [1] block-cipher using a Cadence set of tools (Xcellium, Genus, Voltus for power analysis). Then he will introduce modifications to the design in order to simulate a localized change in the leakage current. The last step is dedicated to the development of a python script in order to automate the whole process of modifying and measuring the leakage currents and power consumption. We will use the script in order to perform an attack to retrieve the encryption key of the synthesized AES using a leakage current analysis method called LPA [2][3]. The usability of the flow, if well defined, can be extended to modeling the magnetic emissions of an integrated circuit, since the current and the generated magnetic field are dependent and bound the Biot-Savart law.

[1] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001.
[2] M. Alioto, L. Giancane, G. Scotti and A. Trifiletti, "Leakage Power Analysis attacks: Well-defined procedure and first experimental results," 2009 International Conference on Microelectronics - ICM, 2009, pp. 46-49, doi: 10.1109/ICM.2009.5418592.
[3] Moradi, A. (2014). Side-Channel Leakage through Static Power. In: Batina, L., Robshaw, M. (eds) Cryptographic Hardware and Embedded Systems – CHES 2014. CHES 2014. Lecture Notes in Computer Science, vol 8731. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44709-3_31

Profile :
- Microelectronics background (Digital and analog)
- VHDL, Verilog, SPICE
- Knowledge in scripting using TCL/Bash
- Knowledge in at least one scripting/programming language : Python(preferable), Matlab, …

Profil : 2A internship
Duration : 2 to 3 months
Remuneration : about 560€/month

To apply, please send your CV and latest transcript to :
- nasr-eddine.ouldei-tebina@univ-grenoble-alpes.fr
- paolo.maistri@univ-grenoble-alpes.fr
- alain.zergainoh@univ-grenoble-alpes.fr

Our team welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as strength and an asset.

Laboratoire TIMA
46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE
Tél : 04 76 57 50 79
E-mail : tima-direction@univ-grenoble-alpes.fr
Web : http://tima.univ-grenoble-alpes.fr

TIMA Laboratory
46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE
Tel: (+33) (0) 476 57 50 79
E-mail: tima-direction@univ-grenoble-alpes.fr
Website: http://tima.univ-grenoble-alpes.fr