A low-cost EM glitch detector

David El-baze[1], Jean-Baptiste Rigaud[1] and Philippe Maurine[2]

[1]SAS-ENSM-SE, {david.el-baze,rigaud}@emse.fr
[2]SAS-CEA, philippe.maurine@cea.fr
[2]LIRMM, philippe.maurine@lirmm.fr

March 31, 2015

Abstract

The method, using ElectroMagnetic Pulses (EMP), has recently been demonstrated to be an efficient fault injection technique [1]. If one can find voltage glitch detectors [2] in the literature, there is no proposal which puts forward the idea of detecting EM injection.

Within this context, we introduce, in this presentation, a fully digital and low cost sensors allowing detecting EM pulses. This detector was developped following the results of [3]. That shows that EMP can produce bit sets and bit resets, i.e. disrupting the behavior of DFF.

To validate the operating principe of this detector, but also to demonstrate its efficiency, we mapped it as a hard-macro FPGA and evaluate their performances under various operating conditions. To that end a testchip was designed. It features a 128 bits AES, an uART (RS232) and a mesh of detectors. This testchip was subjected to EMP produced at different positions above its surface. This allowed us measuring the EM susceptibilities of the AES but also of the mesh. 80% of EM injections were detected by the mesh for an area overhead of 5%. This demonstrates the validity of the concept and the efficiency of the detector.

References

[1] A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria, "Injection of transient faults using electromagnetic pulses-Practical results on a cryptographic system-." *IACR Cryptology ePrint Archive*, vol. 2012, p. 123, 2012. [Online]. Available: http://www.feng.pucrs.br/ vargas/Disciplinas/HW-Reconfiguravel/FI-Techniques/CEA-LETI/Injection-of-transient-faults-using-EM-pulse.pdf

[2] L. Zussa, "Étude des techniques d'injection de fautes par violation de contraintes temporelles permettant la cryptanalyse physique de circuits sécurisés," Ph.D. dissertation, Saint-Etienne, EMSE, 2014. [Online]. Available: http://www.theses.fr/2014EMSE0757

[3] S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine, "Evidence of a larger EM-induced fault model," in *Smart Card Research and Advanced Application Conference (CARDIS)*, Paris, France, Nov. 2014. [Online]. Available: http://hal-emse.ccsd.cnrs.fr/emse-01099037