Reliability analysis of digital sensors against perturbations of FPGAs

Sylvain Guilley[1,2], Richard Newell[3] and Thibault Porteboeuf[2]

[1] TELECOM-ParisTech
[2] Secure-IC S.A.S.
[3] Microsemi Corp.

This paper discusses the *digital sensor* [2, 1], a detection technology against perturbations, that are the priviledged attacks paths for fault injection attacks. It has been valided in various FPGAs and on ASICs. The digital sensor aims at providing a binary alarm signal indicating potential fault injection attempt. As such this IP acts as a binary classifier whose ROC (Receiver Operating Characteristics) curves can be plotted to illustrate its performance. In order to compute the ROC curves, we first need to be able to compute the true/false positive and true/false negative probabilities. In our case, we consider three random variables. First, the critical path delay which is supposed to vary from chip to chip or from instance to instance while being constant over time. Then the sensor alarm threshold which is supposed to follow the same rule as the critical path. Both have a standard deviation that depends on the fabrication process. Their mean value is controlled by the chip designer, and more precisely their spacing. The third variable is the clock period, which changes according to its distribution at every clock cycle. Its standard deviation and mean value are specified by the chip designer but can be modified by the attacker. In this article, we will consider that the attacker can influence the spacing between the mean clock period and the critical path mean delay.

References

[1] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger. Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks. *IET Information Security*, 5(4):181–190, December 2011. DOI: 10.1049/iet-ifs.2010.0238.

[2] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger. WDDL is Protected Against Setup Time Violation Attacks. In *FDTC*, pages 73–83. IEEE Computer Society, September 6th 2009. In conjunction with CHES'09, Lausanne, Switzerland. DOI: 10.1109/FDTC.2009.40; Online version: http://hal.archives-ouvertes.fr/hal-00410135/en/.