PhD Proposal

Laboratory (location): Grenoble INP-LCIS (Valence)
Thesis Advisor: Vincent BEROULLE
Co-advisor: David HELY

Subject: Design and emulation of new robust architectures for UHF RFID Tags

RFID tags are more and more used for critical applications within harsh environments (aeronautics, railways…) or for secure applications such as identification, countermeasure against counterfeiting…However, such low cost systems, initially designed for non critical applications with a high volume, are not robust by themselves. For critical applications, a malfunction of RFID chip may have serious consequences or induce a severe security breach for hackers. Dysfunctions can have many origins: for instance, hardware issues can be due to aging effects or can also be due to hackers attack such as optical or electromagnetic fault injection [HUT08]. It is thus a common practice for critical applications to increase the robustness of RFID system thanks to hardware redundancy. Such a method has some drawbacks: it increases the global system cost and adds more and more complexity to the protocol and the associated middleware. Robust tags would then allow limiting the use of redundancy.

The main purpose of this PhD Thesis is to increase UHF tags robustness by proposing new digital architectures of RFID chips which would be resilient against both hardware attacks and natural defects.

Usual design techniques for robust VLSI consist in evaluating the design robustness by simulation and to do this independently of the design validation. The main technique for robustness evaluation is the simulation based faults injection. Within the RFID context such an approach only based on simulation has several drawbacks. In fact, simulations often are inaccurate because the system behavior relies on several parameters such as the global electromagnetic environment, the number of tags present in the reader field, the RFID protocol parameters… Hence, we propose for this project (1) to develop a design method dedicated to RFID system based on hardware prototyping in order to avoid time consuming simulations and then (2) to evaluate the design within a real environment. The hardware prototyping will be based on FPGA which will allow the design to be validated in a real environment. Moreover, using instrumentation techniques for fault injection within FPGA [SER07], it will be then possible to analyze the effects of faulty tag on the global system in terms of safety and security and then to propose countermeasures.

In a first time, the PhD candidate will design an RFID tag prototype made of an FPGA for the digital part and of an off-the-shelf RF front end. Then, he will instrument the prototype in order to perform fault injection campaigns within the global RFID system. Afterwards, the system robustness evaluation in presence of faults will be done. The result of this evaluation will then serve as basis for proposing new architectures of RFID tags which will be designed and validated using the same environment.

The prototyping system designed by the candidate will also be used in order to propose and demonstrate new attacks against RFID system based on malicious tags. It will also be used for the evaluation of RFID methods aiming at detecting faulty tags and reconfiguring the global RFID system accordingly [FRI10].

Experiments requiring a complex RFID environment and its associated specific tools will be performed within the RFTLAB, a Grenoble Institute of Technology lab dedicated to RFID experiments.

The PhD candidate will be based in the LCIS a Grenoble Institute of Technology Research lab located in Valence (connected directly by high speed train to Lyon (30 mins) and (Paris 2h10mins).

Contact and Application by email to:
David HELY david.hely@lcis.grenoble-inp.fr
Please join to your application:

- Covers letters
- Resume
- Master marks and ranking
- References

References:

[FRI10] G. Fritz, V. Beroulle, O. Aktouf, M. D. Nguyen, D. Hély, “RFID System On-line Testing Based on the Evaluation of the Tags Read-Error-Rate”, JOURNAL OF ELECTRONIC TESTING, (DOI: 10.1007/s10836-010-5191-6), pp 1-10, december 2010.
[Hut08] M. Hutter, J. Schmidt, T. Plos, « RFID and its vulnerability to Faults », CHES 2008, LNCS 5154, pp 363-369, 2008.
[SER07] Y. Serrestou, V. Beroulle, C. Robach, “Impact of Hardware Emulation on the Verification Quality Improvement”, WG 10.5 International Conference on Very Large Scale Integration, pp. 206-211, 218-223, 15-17 October, Georgia Institute of Technology, Atlanta, GA, 2007