Securing The IoT Against Fault Injection Attacks Using Digital Sensors

Roukoz Nabhan*, Jean-Max Dutertre*, Jean-Baptiste Rigaud*, Jean-Luc Danger‡, Laurent Sauvage‡

*Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France

Email: {roukoz.nabhan, dutertre, rigaud}@emse.fr

‡LTCI, Télécom Paris, Institut Mines-Télécom, 91120 Palaiseau, France

Email: {jean-luc.danger, laurent.sauvage}@telecom-paris.fr

Abstract

The connected objects exchange sensitive data such as passwords or personal information with each other through the internet. The confidentiality and security of these data are vulnerable to physical threats like Fault Injection Attacks (FIA). The French-German project **APRIORI**† provides an Application Programming Interface (API) for the secure element of the Internet Of Things (IoT). It is based on the generation of an array of digital sensors ensuring privacy for connected objects.

Different constraints must be respected to select the best detector, fully digital, easy to implement and low-cost at the silicon area.

In this work, we first test the effectiveness of the fully digital detector designed by D. El-Baze et al.[1] against ElectroMagnetic Fault Injection (EMFI). We implement this sensor on Nexys video 7 Field Programmable Gate Array (FPGA) board which is equipped with an Artix-7(XC7A200T). We deeply analyze the impact of FIA on the behavior of sensors at several clock frequencies.

Besides the modeling and simulating of the EMFI proposed by M. Dumont et al.[2], no research work has yet demonstrated precisely the mechanism of different fault models after experimental tests. Our results illustrate both sampling and timing fault models. We also propose an improved design of this sensor to cover both fault models. It should be suitable for FPGA and Application-Specific Integrated Circuit (ASIC) implementation for future work.

References

[1] David El-Baze, Jean-Baptiste Rigaud, and Philippe Maurine. "A fully-digital EM pulse detector". In: *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2016, pp. 439–444.

[2] Mathieu Dumont, Philippe Maurine, and Mathieu Lisart. "Modeling of Electromagnetic Fault Injection". In: *2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*. 2019, pp. 246–248.

† APRIORI: Advanced PRivacy of IOt devices through Robust hardware Implementation. `https://anr.fr/Project-ANR-20-CYAL-0007`