Live Demonstration: Generating FPGA Fingerprints utilizing Full-Chip Characterization with Ring-Oscillator PUFs

Andreas Herkle, Holger Mandry, Joachim Becker, Maurits Ortmanns
University of Ulm, Institute of Microelectronics, Ulm, Germany
{andreas.herkle, holger.mandry, joachim.becker, maurits.ortmanns}@uni-ulm.de

Abstract—This demo shows the automated characterization of Xilinx Zynq FPGAs on the Digilent Zybo with the help of a framework based on Partial Reconfiguration. Fine-granular measurements of the whole chip area reveals several aspects which have to be taken into account for PUF system design on these devices. In this demo, the visitor will get to know the general measurement approach and explanations about the provided results. With the help of a python based tool, the visitor can experience the workflow first-hand, generate their own measurements and use them to differentiate a single board from a set of multiple other boards. Further in-sight can be gained by analysis of the different statistical metrics and by combining measurements from multiple boards.

I. INTRODUCTION

Physical Unclonable Functions (PUF) are dedicated circuits for generating hardware specific fingerprints of individual devices. They come in a variety of implementations but all of them utilize the uncontrollable deviations resulting from manufacturing in order to facilitate a device specific and unpredictable yet repeatable behavior. A specific implementation is designed identically for all devices and generates a response on-demand based only on its specific variations. Thus, PUFs especially excel as alternatives for non-volatile memory storing secret keys in hardware cryptographic systems, which requires not only specialized and expensive hardware for intrusion prevention but also constant power supply.

One example of a PUF is the ring-oscillator (RO-PUF), whose mean oscillation frequency slightly varies between different instances. RO-PUFs are well-known as the most preferable choice on FPGAs due to their easy implementation, their small size and their outstanding statistical metrics.

In a recent publication [1], a full-chip characterization of Xilinx Zynq FPGAs based on RO-PUF in-depth analysis was presented. With the help of Partial Reconfiguration, the complete reconfigurable chip area was successively covered with ring-oscillators. Further improvements of the ring-oscillators themselves and their respective measurement logic were applied and allowed to identify and solve many issues regarding the readout stability. One result of this work is the possibility to generate fine-granular heatmaps of the frequency distribution on-chip as illustrated in Fig. 1. Consequently, device specific fingerprints can be easily extracted while also maintaining precautions about disturbances identified by the different types of heatmaps generated from all devices.

Fig. 1. Heatmap for the on-chip distribution of the (a) mean and (b) standard deviation of the ring-oscillator frequencies on a single device

II. VISITOR EXPERIENCE

This live demonstration will provide the visitor with insight about the methodology of measuring the FPGA chip area on multiple Digilent Zybo boards with the help of the publicly available framework [2]. A python based graphical user interface allows the visitors to set the different constraints like readout mode, number of measurements and evaluation times. Visualization of the measurement is provided in various way. The visitors can interact themselves with the measurement setup on a provided computer with detailed explanation and guidance. Hereby, they can select from the provided boards to be measured (and bring their own Zybo). By comparing the real-time results to a given list, they can identify boards solely on the frequency fingerprint. The visitors can also generate an on-chip view averaged over multiple devices and identify spots and areas with critical influence of nearby logic. More statistical metrics can be extracted and illustrated, which provide the visitors a deeper insight about selective PUF placement. A normalization algorithm based on grouping the logic elements can fine-tune the granularity of the measurements and provide further in-sight on a logic independent level.

ACKNOWLEDGMENT

This work was funded by the German National Science Foundation DFG under Grant Number FI 982/15-1.

REFERENCES

- [1] A. Herkle, H. Mandry, J. Becker, and M. Ortmanns, "In-depth analysis and enhancements of ro-pufs with a partial reconfiguration framework on xilinx zynq-7000 soc fpgas," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2019, pp. 238–247.
- [2] A. Herkle, "Framework based on partial reconfiguration for chip characterization utilizing ring-oscillator pufs," 2019. [Online]. Available: <https://github.com/IFM-Ulm/ro-pr-fw>