# Design of Novel Physical Unclonable Function for Hardware Security Application

Paul Flammarion, Kevin-Andres Vicuna-Barriga, Lionel Trojman

## Introduction

This study investigates a new methodology for implementing Physically Unclonable Functions (PUFs) in Field-Programmable Gate Arrays (FPGAs) using Ring Oscillator (RO). PUF represents a sophisticated hardware security technology that is gaining importance with the increasing ubiquity of electronic devices.

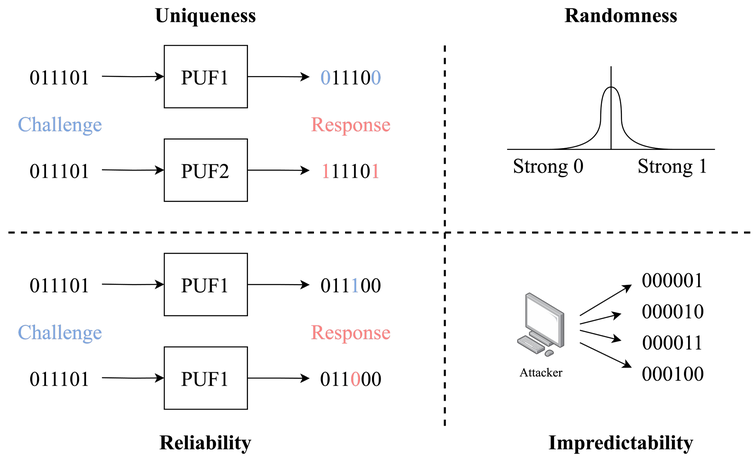


Figure 1: PUF Device Evaluation Metrics

The PUF's metrics shown in Fig. 1 come from the natural variances in silicon processing, rendering each Integrated Circuit (IC) physically unique. This uniqueness facilitates the generation of a distinct encryption key using challenge-response authentication mechanism for each IC, derived directly from its physical properties.

## Methodology

To propose a novel architecture, we have carefully reviewed the literature. The method suggested is based on the concept of a collapse RO, as illustrated in Fig. 2. This base structure allows generation of high entropy, low power consumption, and resilience to temporal noise. Furthermore, it allows for the evaluation of the proposed method with the Cycle To Collapse (CTC) metric. In addition, it has been shown that this weak PUF type is sensitive to environmental factors such as temperature variation.

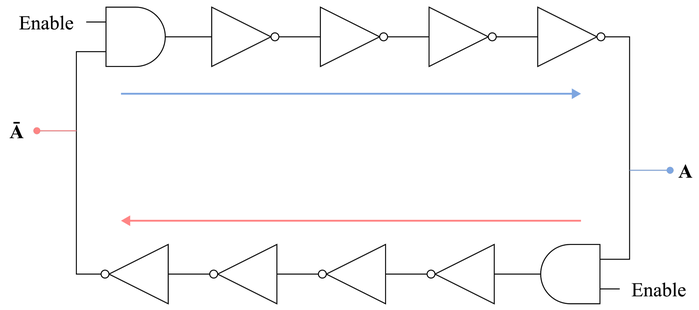


Figure 2: Classic Collapse Ring Oscillator Structure

Following the literature review, we designed a novel architecture for RO-based PUFs, integrating configurable paths to enhance security and variability. This design phase involved careful consideration of circuit topology, component selection as larger logic cells, and layout optimization. We implemented this structure in a Intel MAX 10 FPGA, with the most symmetric row approach for each 128 bits. Moreover, our methodology implements the use of reconfigurable paths using tristate buffers.

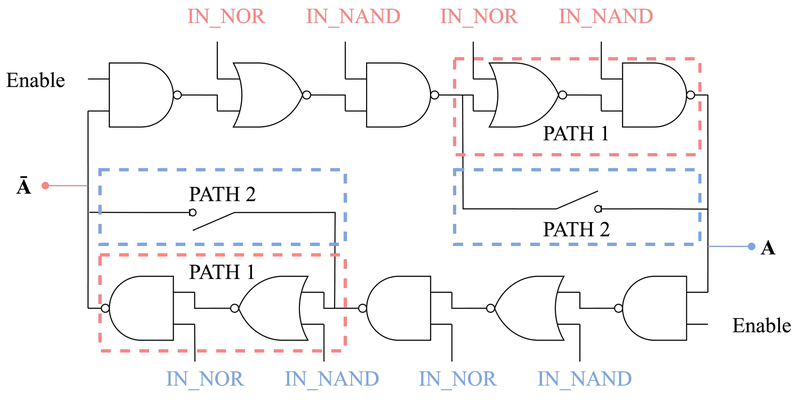


Figure 3: Proposed Ring Oscillator

Since the tristate buffer acts as a switch, we are able to dynamically select the path used by the body voltage. Moreover, Fig. 3 shows the symmetry in the RO implementation for both the upper and lower paths, using NAND and NOR logic cells.

## Results and Discussion

To evaluate our methodology, we have generated five hundred keys of 128-bits for each calibration, on two distinct FPGAs. The calibration refers to the path used by the body voltage for the PUF's output. All data have been generated at a temperature of 25°C for subsequent analysis.

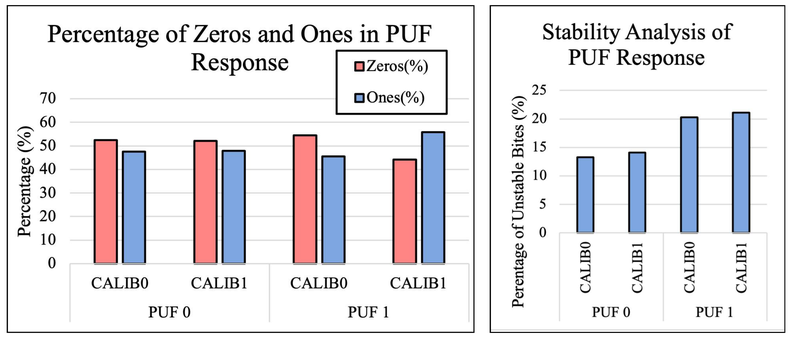


Figure 4: Ring Oscillator Randomness and Stability Responses

Fig. 4 shows a high degree of randomness, variations on calibration changes and a normal level of stability.

To further improve our method, we want to perform more tests with a higher number of FPGAs, measure the variation under different environmental condition and limit the parameter variation to point out the best way to improve the PUF's implementation in an FPGA.

## Conclusion

In our work, we have proposed a novel PUF architecture to enhance the hardware security of FPGAs. This architecture has demonstrated a good response to our first experiments with the use of four new patterns that are very promising: tristate buffer, larger gates, row approach, and configurability.

As a future work, we want to investigate the possibility of dynamic configuration for each bit based on its previous response. This method has potential to significantly enhance our results, thereby strengthening the PUF implementation.