

# Open source platform for digital simulation, characterization and modeling attacks on delay based Physical Unclonable Functions (PUFs)

Rodrigo C. Surita (IC), Mario L. Côrtes (PQ), Diego F. Aranha (PQ), Guido Araujo (PQ)

## Abstract

PUFs rely on manufacture variations in integrated circuits for providing security properties such as authentication without the need explicitly storing cryptographic keys. More specifically, delay-based PUFs depend on signal delays in digital circuits. This work proposes an open source platform to simulate the digital behavior of delay-based PUF models, measure performance according to security metrics and apply machine learning techniques on an attempt to predict their responses.

*Key words: embedded security, Physical Unclonable Functions, modeling attacks*

## Introduction

Designs that combine security and small silicon area are of great interest in IoT devices. delay-based Physical Unclonable Functions (PUFs) are devices where signals run among different circuit paths defined by an input (challenge) [1]. As each path has distinct delays, the response signals arrive at different moments at the end of the circuit paths and are captured by an arbiter, which builds the output. The delays may vary between instances produced, thus creating different functions.

Although effective in size and power consumption, many low-cost PUF designs have revealed security weaknesses such as susceptibility to modeling attacks [2]. In this scenario, testing cryptographic metrics and modelling resistance of new PUF proposals is crucial.

## Results and Discussion

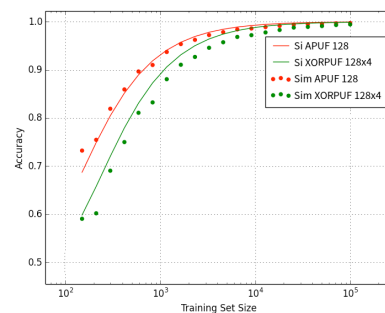
For circuit simulations, the platform discussed uses a versatile standalone Python / VHDL Testbench, also compatible IEEE 1164 VHDL simulators. The physical parameters are defined by a random function, which is by default a Gaussian distribution within  $[-3\sigma, +3\sigma]$  range from an AMS 350nm Standard Cell Design Kit. Some PUF design examples, such as the classical Arbiter PUF XOR PUF [1,2] are included. New designs can be described using VHDL or Python.

**Table 1:** simulated and silicon APUF 64 Metrics.

Metric	Simulated	Silicon [1]
Hamming Weight	0.46	0.40
Hamming Distance	0.44	0.47
Entropy	0.090	0.07
min-Entropy	0.011	0.01

For the design characterization, scripts to compute the metrics used on related work were

included, such as Hamming weight, entropy, min-entropy and between-instance Hamming distance [1]. Discussed methods for modelling attacks such as logistic regressions, SVMs and neural networks [2] are also available for testing.



**Figure 1.** Accuracy of SVM model for simulated and silicon (regressions obtained in [2]) for 128 bits APUF and 4 line 128 bits XORPUF.

## Conclusions

Although using a simplified model, the software was able to precisely reproduce some key experiments on silicon implementations described in literature using only simulations. That represents a possibility of speedup and cost reduction on development techniques. It is now in use as a development tool for PUF designs at University of Campinas Computer Systems Laboratory and is freely available at Github [3].

## Acknowledgement

Intel Project “Physical Unclonable Functions for SoC Devices”.

<sup>1</sup> Katzenbeisser, S et. all. PUFs: Myth, Fact or Busted? *Proceedings of the 14th International Cryptographic Hardware and Embedded Systems*, v. 7428, p.283–301. 2012;

<sup>2</sup> Ruhrmair U. et all. Modeling attacks on physical unclonable functions. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, p. 237–249. 2010.

<sup>3</sup> Surita R. C. FreePUF Simulator and Attacker. Available at <https://github.com/rodrigossurita/freepuf>