EasyChair Preprint

№ 1571

Demonstration of Differential Circuit (DiffC)-PUF Addressing and Readout Platform

Alexander Scholz, Lukas Zimmermann, Axel Sikora, Mehdi Tahoori and Jasmin Aghassi-Hagmann

October 1, 2019

Demonstration of Differential Circuit (DiffC)-PUF Addressing and Readout Platform

Alexander Scholz[‡,$], Lukas Zimmermann[†,$], Axel Sikora[†], Mehdi B. Tahoori[§] and Jasmin Aghassi-Hagmann[‡,$]
[‡]Institute for Applied Research, Offenburg University of Applied Sciences, Germany
[†]Institute of Reliable Embedded Systems and Communication Electronics, Offenburg University of Applied Sciences, Germany
[$]Institute of Nanotechnology, Karlsruhe Institute of Technology, Germany
[§]Chair of Dependable Nano Computing, Karlsruhe Institute of Technology, Germany

1 Hardware Demo Objectives

This Demo presents a complete platform for a discrete board-level analog PUF including the addressing and readout in both hardware and software infrastructures. The Differential Circuit (DiffC)-PUF is assembled using discrete components, as shown in Figure 1. With the current setup, 28-bit PUF responses can be generated. The used approach allows non-linear bit width scaling with physical expansion. The DiffC-PUF platform enables access to a reliable PUF in a full board-level SoC system including software for security analysis in R&D settings.

2 Introduction

A Physical Unclonable Function (PUF) describes a hardware-based security primitive that can be utilized for authentication, identification and secure key generation [1][2][3]. As proposed in literature, analog PUFs, exploiting transistor mismatch, are usually complex and costly prototype ICs [4][5]. Unfortunately, this limits the direct physical access for the research community. With the herein demonstrated DiffC-PUF, which exploits variation mismatch in the manner of analog PUF circuits, the community can get full access to a reliable PUF in a real hardware system.

3 Attack Model

Not applicable

4 Experimental Results

The entire DiffC-PUF evaluation platform consists of the DiffC-PUF (highlighted with green background on Figure 1) and a commercial, off the shelf microcontroller (EFM32 Leopard Gecko development board) for PC communication, challenge generation and response readout. The DiffC-PUF's control logic, for addressing and readout routing and the DiffC-PUF core, as intrinsic variability source, are custom PCB designs. The DiffC-PUF core is designed such that single core entities are detachable, allowing interchangeability of core circuits for large-scale characterization.

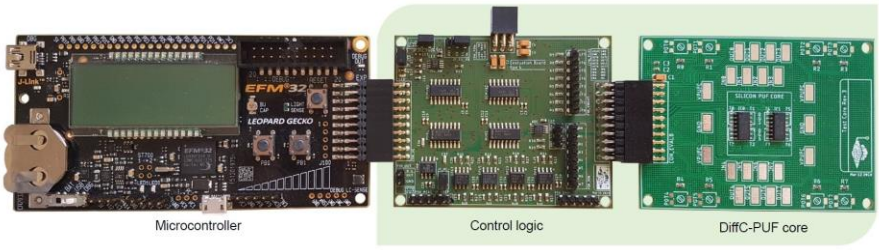

Figure 1: DiffC-PUF evaluation platform with microcontroller (left) and the DiffC-PUF (highlighted with green background), consisting of the control logic and the detachable DiffC-PUF core.

The system is tested with regards to PUF metrics such as reliability and uniqueness. Furthermore, each DiffC-PUF response was read out over 125 cycles to observe bit errors.

5 Key Observations and Outcomes

The experimental results of the fabricated DiffC-PUF core instances show an average reliability of 99.20% and a uniqueness value of 48.84%. The interchangeability of DiffC-PUF cores can be seen in the demonstration.

6 List of Equipment

To power the platform, we used two power supplies of the type HP E3631A. The communication interface between the PC and microcontroller is controlled via Python script.

7 References

[1] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security, pages 148–160. ACM, 2002.

[2] G Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In Design Automation Conference, 2007. DAC'07. 44th ACM/IEEE, pages 9–14. IEEE, 2007.

[3] Blaise Gassend, Daihyun Lim, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice and Experience, 16(11):1077–1098, 2004.

[4] Keith Lofstrom, W Robert Daasch, and Donald Taylor. Ic identification circuit using device mismatch. In Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International, pages 372–373. IEEE, 2000.

[5] Daniele Puntin, Stefano Stanzione, and Giuseppe Iannaccone. Cmos unclonable system for secure authentication based on device variability. In Solid-State Circuits Conference, 2008. ESSCIRC 2008. 34th European, pages 130–133. IEEE, 2008.