Root of Trust Components to Increase Security of RISC-V Based Systems on Chips

Luis F. Rojas-Muñoz[1*], Macarena C. Martínez-Rodríguez[1], Santiago Sánchez-Solano[1] and Piedad Brox[1]

[1] Instituto de Microelectrónica de Sevilla, IMSE-CNM, CSIC/Universidad de Sevilla

Abstract

This work presents the design and validation of a compact and efficient RO-PUF/TRNG module, which combines ID generation and entropy source functionalities, and can be used as an essential primitive of a hardware RoT for RISC-V based SoCs. The design was encapusalted as an IP core to provide it with a high level of configurability, flexibility, and reusability. A comprehensive SDK for online characterization, validation, and performance monitoring of PUF and TRNG quality metrics was also developed. The experimental results show that the proposed RO-PUF/TRNG IP is suitable for increasing the security of IoT applications.

Introduction

Nowadays, the security of processing and information exchange systems has become one of the main concerns of many companies and organizations, posing demanding challenges for system designers and developers. The situation is especially critical for many IoT devices, where limited resources and the requirement for fast time-to-market have sometimes pushed security issues to the back burner. The growing interest, both at the industry and at the academic levels, in incorporating the free and open RISC-V ISA standard into the processing systems implemented by many IoT devices has made it necessary to explore different solutions to increase the security of these systems [1].

Hardware-based security solutions are becoming increasingly popular due to their ability to provide a higher level of protection for sensitive data and avoid counterfeiting. These solutions rely on a set of primitives that establish a trusted foundation, known as Root-of-Trust (RoT), which provides a common anchor point for the system security. Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs) are two basic primitives of a RoT. By generating unique identifiers and truly random numbers, both based on the physical properties of a device, these primitives help establish trust in the system and enhance the security of cryptographic operations. PUFs and TRNGs based on ring oscillators (ROs) have proven to be effective alternatives for implementation in programmable devices. Also, the integration of both functionalities in a single design allows to achieve an optimal cost-benefit trade-off [2].

This work describes an RO-PUF/TRNG module capable of providing identifiers and random numbers with a high bit-per-resource rate, as well as the methodology used for the online evaluation of quality metrics (both for PUF and TRNG functionalities) obtained when incorporated into a RISC-V-based System-on-Chip (SoC).

RO-PUF/TRNG IP Module Design

The block diagram of the RO-PUF/TRNG module is shown in Figure 1. Using two reported design techniques (sign bit and counter bits), the design simultaneously compares two RO pairs and extracts two bits from each comparison. The design takes advantage of the internal structure of Xilinx Series-7 devices to achieve a compact and efficient implementation that integrates four 4-stage ROs per CLB. The core components of the design are a matrix of ROs (RO_bank) and two blocks to perform simultaneous RO-pair comparisons (cmp1 & cmp2) using binary or Gray-code counters. It also includes a challenge generation mechanism (chll_gen) that allows discarding the most unfavorable ones (chll_mem) to enhance PUF response reliability, as weel as blocks to store and retrieve the output (out_mem) and to control system operation (ctrl).

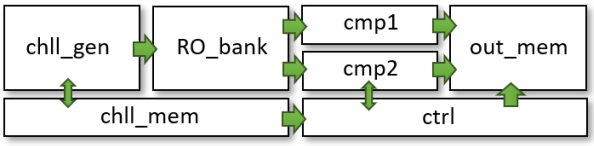

Figure 1: *RO-PUF/TRNG simplified block diagram*

To facilitate its interaction with general-purpose processor systems to build SoC solutions, many design features have been parameterized to be fixed prior to synthesis. The design has been encapsulated as a configurable IP module provided with a standard communication interface based on the AXI4-Lite bus to facilitate its interaction with other components. Once the system containing the IP core has been implemented, application programs running in the processor allow users to set the operating mode by choosing the main function (PUF/TRNG) and different configuration options: RO-pair comparison strategy (Close/Far); counter coding (Gray/Binary); and selected bits (Low/High) [3].

*Corresponding author: rojas@imse-cnm.csic.es

Test Systems Implementation and Validation

With the objective of verifying its correct operation and evaluating the quality indices to validate our proposal, several test systems were implemented, including different instances of the PUF/TRNG IP module using 32- and 64-bit AXI4-Lite interfaces. The design of these test systems was carried out using the facilities provided in the vivado-risc-v repository [4], which allow bridging the gap between the chisel-based tools developed by the University of Berkeley to generate SoCs that incorporate in-order (Rocket) and out-of-order (BOOM) cores using the open RISC-V ISA [5], and the Vivado IP Integrator tool that facilitates its implementation in development boards with Xilinx FPGAs.

The test systems incorporate a 64-bit RISC-V (rocket64b) core whose implementation consumes 37% of the LUTs and 8.5% of the registers available in the Kintex-7 FPGA of a Genesys 2 development board, leaving enough room to instantiate 16 IP modules, as shown in Figure 2. Placement directives were used to separate the locations of the processing system and the different PUF/TRNG replicas, so as to distribute the latter homogeneously among the clock zones of the programmable device.

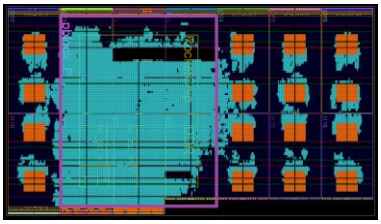

Figure 2: *Test system with RISC-V and 16 IPs*

The support of Linux operating system by the RISC-V core, and the availability of a large number of copies of the IP module on the same device, made possible the development and online execution of a series of routines to obtain the metrics that determine the quality of the proposal according to its dual functionality. The software development kit (SDK) includes low- and high-level drivers to facilitate access to the primitives and control their operation, as well as functions and applications to facilitate the tasks of characterization (during the development phase), validation (as a step prior to product deployment), and periodic monitoring (during device operation) to detect security breaches caused by changes in operating conditions or attempts to attack the device.

PUF – Assessment and Validation

The reliability of always returning the same response to the same sequence of challenges and the uniqueness of this response compared to those provided by other implementations of the module in the same or a different device are the two main quality indices of a PUF, which can be estimated by the HDintra and HDinter Hamming distances, respectively. Table 1 shows the average values of these metrics for four different IP configurations with 640 ROs (2560 output bits), before and after completing an enrollment process and applying the challenge selection mechanism to eliminate 10% of the comparisons. As can be seen, using this feature it is possible to achieve a reliability improvement between 40.8% and 79% without adversely affecting uniqueness.

Table 1: *PUF HDintra and HDinter metrics*.

Config.	HDintra		HDinter	
BH	3.31	1.96	48.80	48.74
GH	1.81	0.81	48.77	48.70
BL	1.62	0.54	48.11	48.14
GL	0.97	0.20	45.66	45.64

TRNG – Assessment and Validation

Design configurability allows four TRNG configurations to be derived based on the RO-pair comparison strategy and the type of counter. The NIST-800-22 statistical tests were used to evaluate the level of randomness of the TRNGs. All of them successfully passed the approval threshold (96) in each of the tests (Fig. 3, top). The successful entropy estimation of the four TRNGs using the non-IID statistical tests from NIST 800-90b recommendation (Fig. 3, bottom), validates the entropy source inherent to the design.

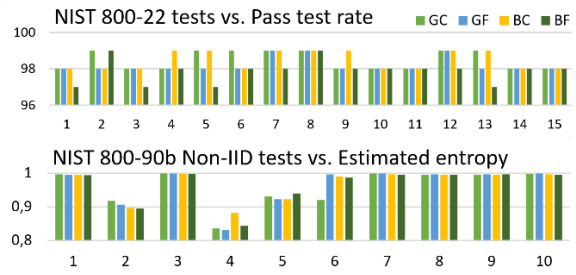

Figure 3: *TRNG pass test rate and estimated entropy*

The evaluation results demonstrate that the design achieves excellent performance, making it suitable for inclusion into the RoT of RISC-V-based SoCs.

Acknowledgments

This research was supported in part by the SPIRS Project with Grant Agreement No. 952622 under the EU H2020 research and innovation programme M.C.M.R. holds a postdoc fellowship from the Andalusia Government with support from PO FSE of EU.

References

[1] T. Lu. "A Survey on RISC-V Security: Hardware and Architecture". arXiv:2107.04175 [cs.CR] (Jul. 2021), doi: **10.48550/arXiv.2107.04175**

[2] V. K. Rai et al. "TRGP: A Low-Cost Re-Configurable TRNG-PUF Architecture for IoT". In *22nd Int. Seem. on Quality Electronic Design*, pp. 420-425, (April 2021).

[3] M. C. Martínez-Rodríguez et al. "Efficient RO-PUF for Generation of Identifiers and Keys in Resource-Constrained Embedded Systems". In: *Cryptography* 6(4): 51 (Oct. 2022), doi: **10.3390/cryptography6040051**.

[4] E. Tarassov "Vivado-risc-V Repository". url: https://github.com/eugene-tarassov/vivado-risc-v.

[5] K. Asanović et al. "The Rocket Chip Generator". Technical Report UCB/EECS-2016-17, EECS Department, University of California, Berkeley, April 2016. url: https://github.com/chipsalliance/rocket-chip