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

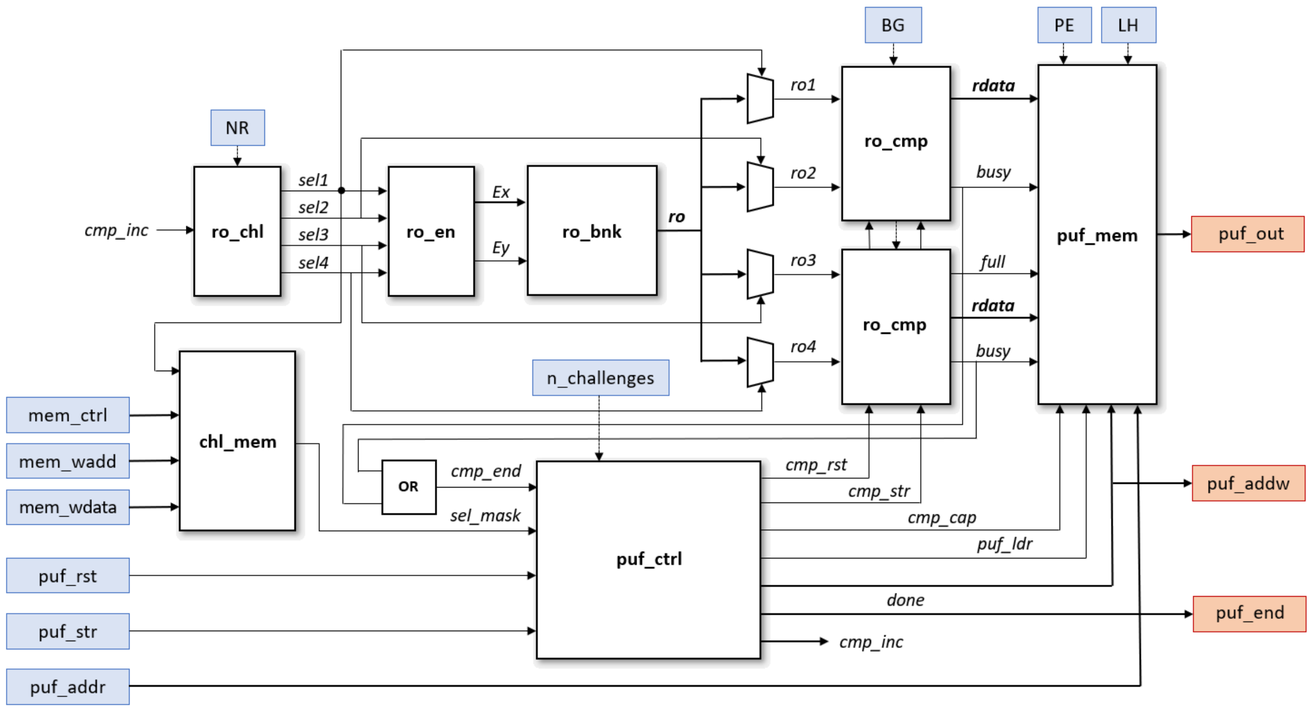
IMSE-cnm Instituto de Microelectrónica de Sevilla
CSIC Consejo Superior de Investigaciones Científicas
Universidad de Sevilla
SPIRS

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

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 Software Development Kit (SDK) for online characterization, validation, and performance monitoring of PUF and TRNG quality metrics was also developed.

RO-PUF/TRNG IP module design



- **Design core components:**
  - **ro_bank** : Matrix of ROs (Four 4-stage ROs per CLB)
  - **ro_comp** : 2 blocks for simultaneous RO-pair comparisons
  - **ro_chl** : Challenge generation mechanism
  - **chl_mem** : Challenge selection mask (PUF operation)
  - **puf_mem** : Store and retrieve the output
  - **puf_ctrl** : Control of system operation

- **Features pre-synthesis:**
  - Configurable IP encapsulation
    - CLB matrix dimensions
    - Matrix location in PL
    - Effective length of the counters
    - Operating mode
      - Operation
      - Characterization
  - 32/64-bit AXI4-Lite bus interface

- **Features post-implementation:**
  - Selection of the main function
    - PUF
    - TRNG
  - RO-pair comparison strategy
    - Close
    - Far
  - Counter coding
    - Gray
    - Binary
  - Selected counter bits
    - Low
    - High

Test System Implementation and Validation

Test System

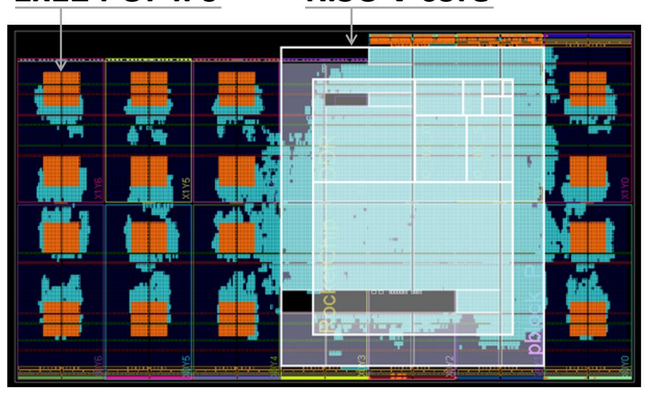
- **Genesys 2 board** (Kintex FPGA)
  - 64-bit Rocket RISC-V core (Linux OS)
  - 32/64 AXI4-Lite interface
  - 16/12 PUF/TRNG IPs (32/64-bit)
    - → 640 ROs
    - → 14-bit counters

Resource Consumption

AXI	Mode	LUTs	Registers	Block RAM	DSPs
32-bit	C	46.45%	10.16%	6.97%	1.79%
	O	46.40%	10.16%	5.17%	1.79%
64-bit	C	48.56%	14.39%	6.07%	1.79%
	O	48.50%	14.31%	6.07%	1.79%

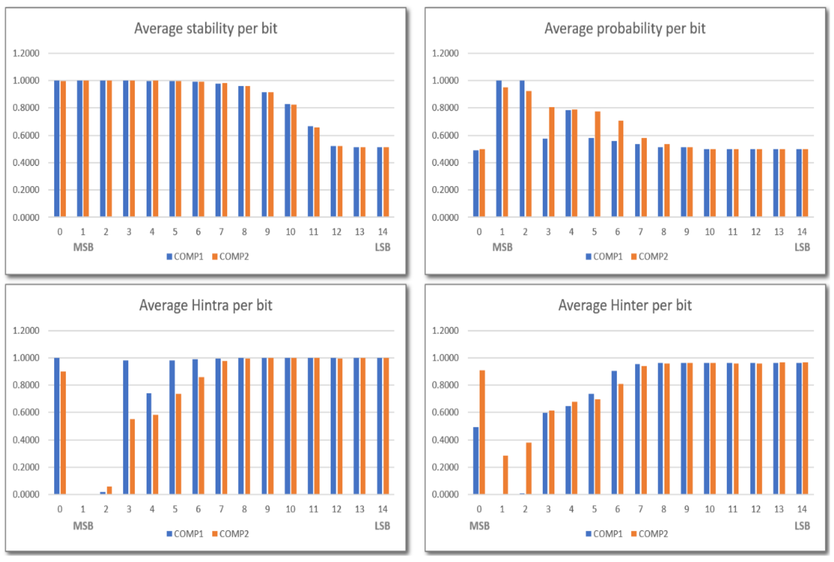
SDK (High-level functions)

- puf_getdata
- puf_bitselect
- puf_enrollment
- puf_HDintra
- puf_reliability
- puf_HDinter
- puf_uniqueness
- puf_test
- trng_getdata
- trng_validation

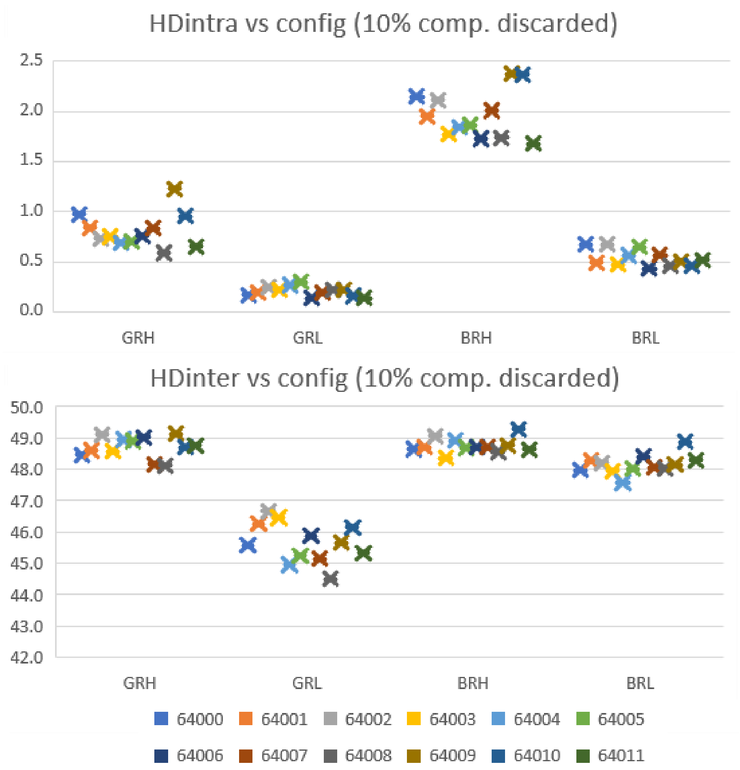


Post-implementation layout of the test system with 32-bit AXI4-Lite interface

PUF – Assessment and Validation



Average bit counter metrics - Binary/Close configuration



Performance evaluation for PUF operation

TRNG – Assessment and Validation

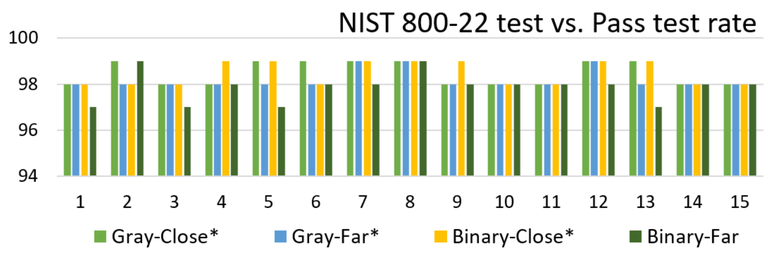
- **Evaluation strategy**
  - 1 million bits per string
  - 4 TRNG configurations
    - → Extraction of 2 LSBs
    - → Combined counters
    - → 4 Configuration options

- **Randomness Assessment**
  - 15 tests of NIST 800-22
  - 100 bit strings per IP

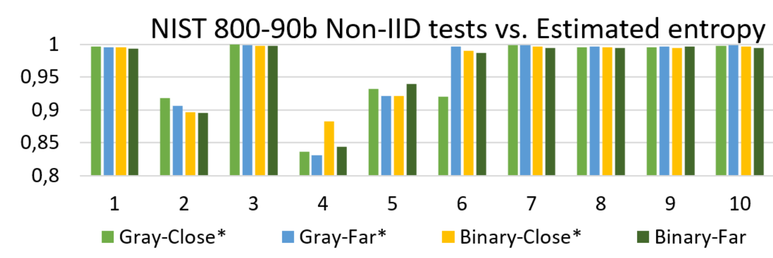
  Approved randomness

- **Entropy source validation**
  - 10 tests of NIST 800-90b
  - 1 bit string per IP

  Validated Entropy



Results of statistical evaluation of randomness



Results of entropy estimation. *XOR post-processing

Conclusiones

- A security primitive with **dual PUF/TRNG functionality**, efficient in terms of resource consumption and speed of operation, was designed and provided with a standard AXI4 interface for easy integration in embedded systems implemented on Xilinx Series-7 and Zynq-7000 devices.
- The C-coded functions included in the **SDK** provide the RO-PUF/TRNG design with a **self-assessment system** to test and guarantee its performance by monitoring the respective metrics of both of its functionalities.
- The evaluation results demonstrate that the design achieves **excellent performance**, making it suitable for inclusion into the RoT of **RISC-V-based SoCs**.

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.