True Random Number Generator based on RO-PUF

Luis F. Rojas Muñoz, Santiago Sánchez Solano,

Macarena C. Martínez-Rodríguez, Piedad Brox

XXXVII Conference on Design of Circuits and Integrated Systems - DCIS 2022

IMSE-cnm Instituto de Microelectrónica de Sevilla

CSIC Consejo Superior de Investigaciones Científicas

Universidad de Sevilla

OUTLINE

- Introduction
- PUF/TRNG Design
- PUF Characterization
- TRNG Validation Process
- State-of-the-art
- Conclusions
- References

- Hardware Security Primitives

  - PUF
    - Unique response
    - Authentication
    - Secure Communication
  - TRNG
    - Unpredictable response
    - Key generation
    - Encryption

- Variability/Entropy Unit

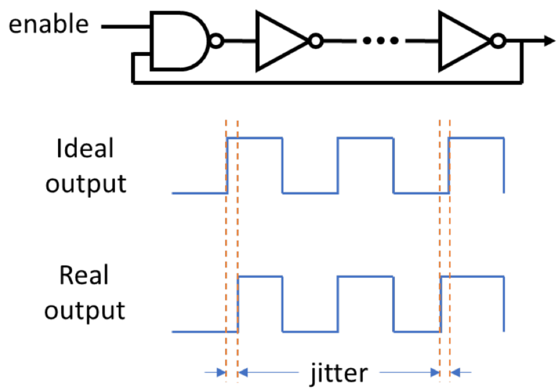


Figure 1. A generic ring oscillator scheme with enable stage and its jitter representation.

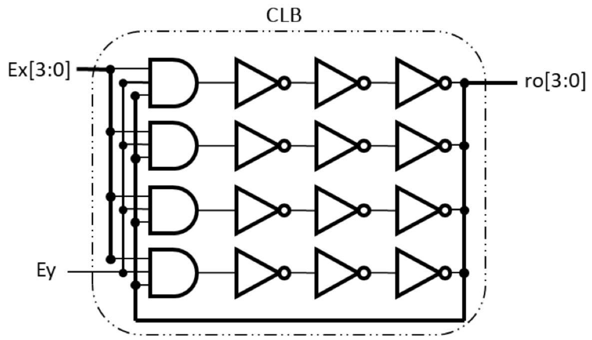


Figure 2. Implementation scheme of 4 ROs of 4 stages in a CLB.

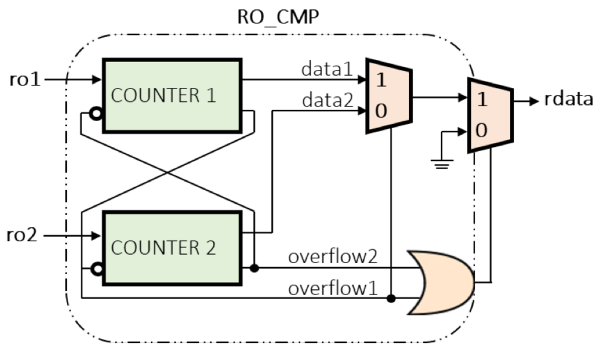


Figure 3. RO pair comparison module.

<u>Binary/Gray counters</u>

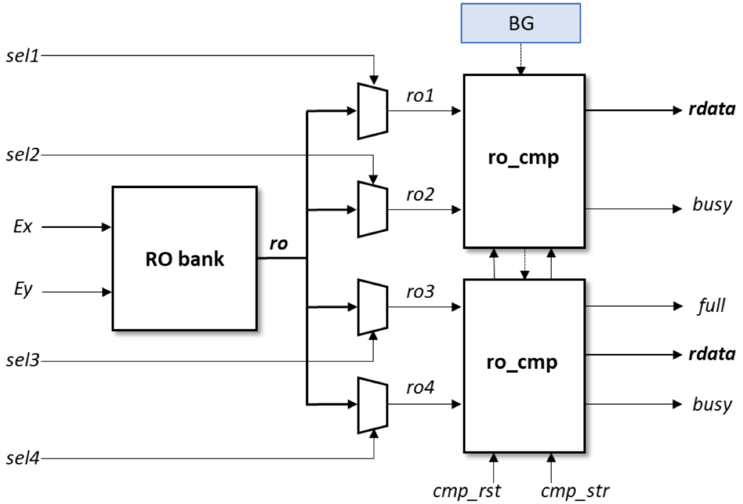
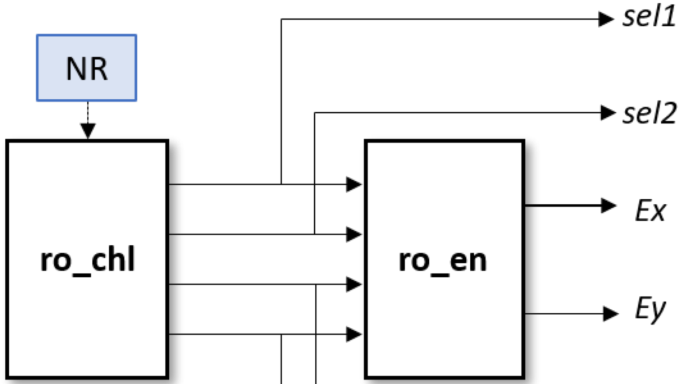


Figure 4. Variability/Entropy block diagram.

- RO-pair Selection Strategy



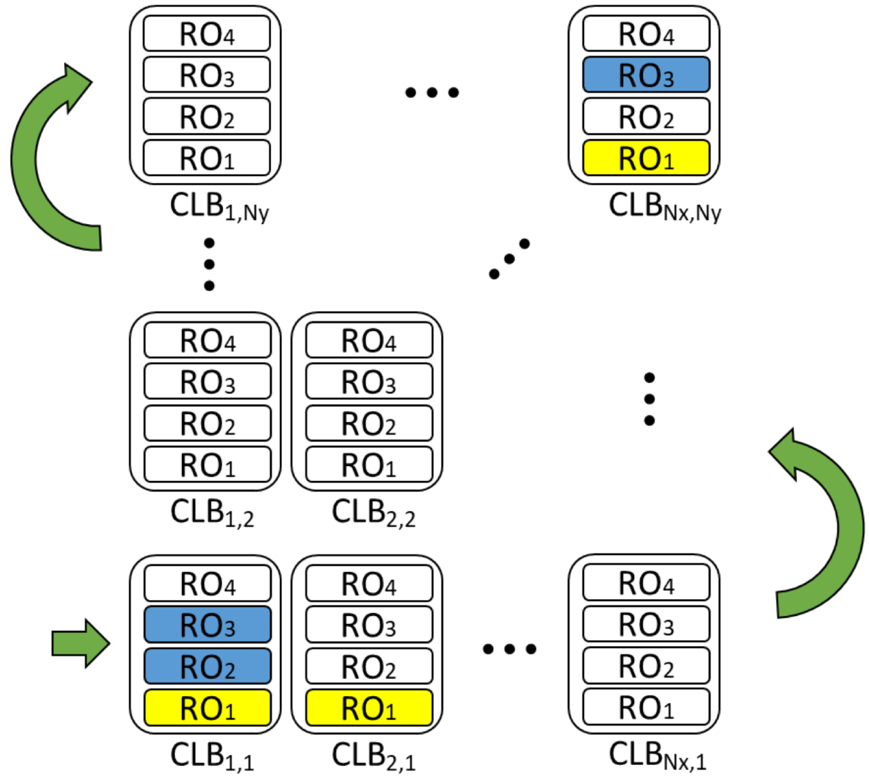


Figure 5. RO-pair Selection Strategy block diagram.

Same position, different CLB

Different position, same or different CLB

Closest/Farthest configuration.

- Output Bit Repository

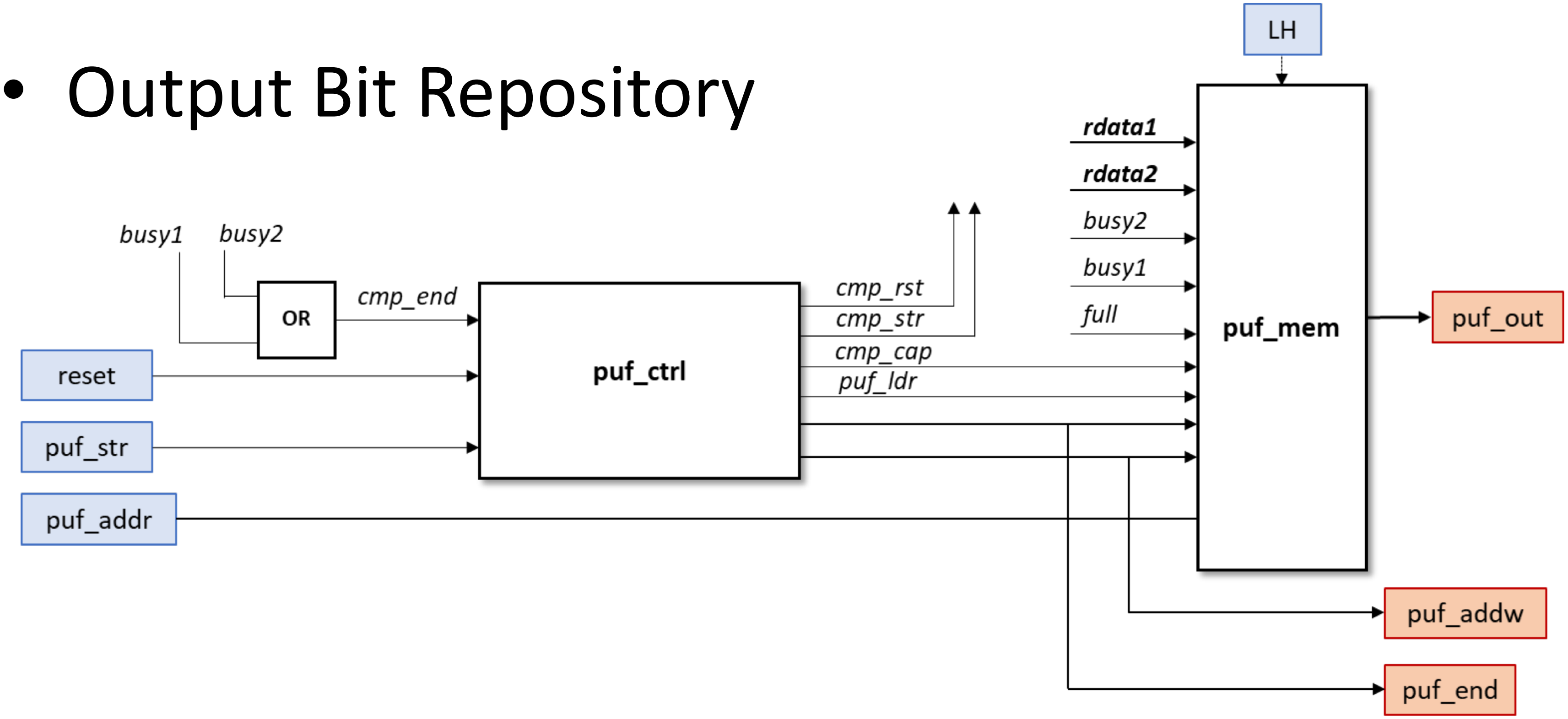
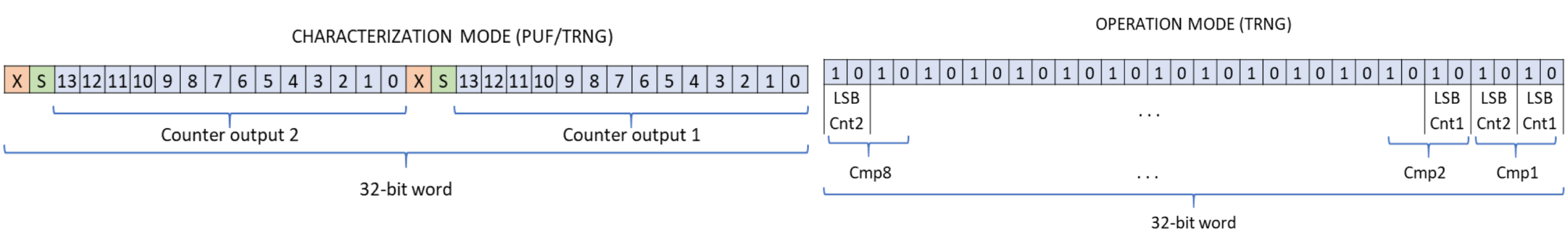


Figure 6. Output bit repository block diagram. Operation/Characterization mode.



- IP integration

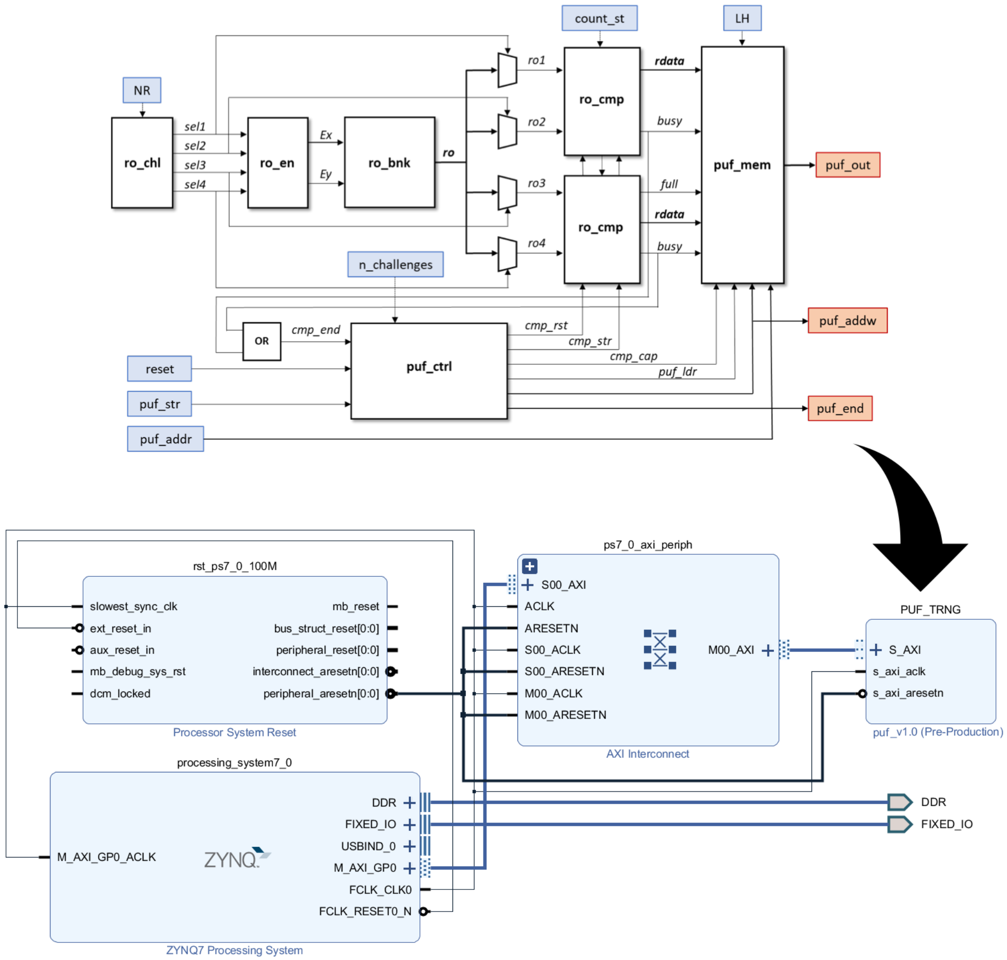


Figure 7. PUF/TRNG IP Integrator schematic

- IP Configurability
  - Implementation
    - Parameterized RO bank size and position.
    - Operation Mode (4bits)
    - Characterization Mode (32bits)
  - Usage
    - No. RO Competitions
    - PUF/TRNG
    - Configurations
      - Binary/Gray
      - Closest/Farthest
      - Lower Higher

- Bit Selection

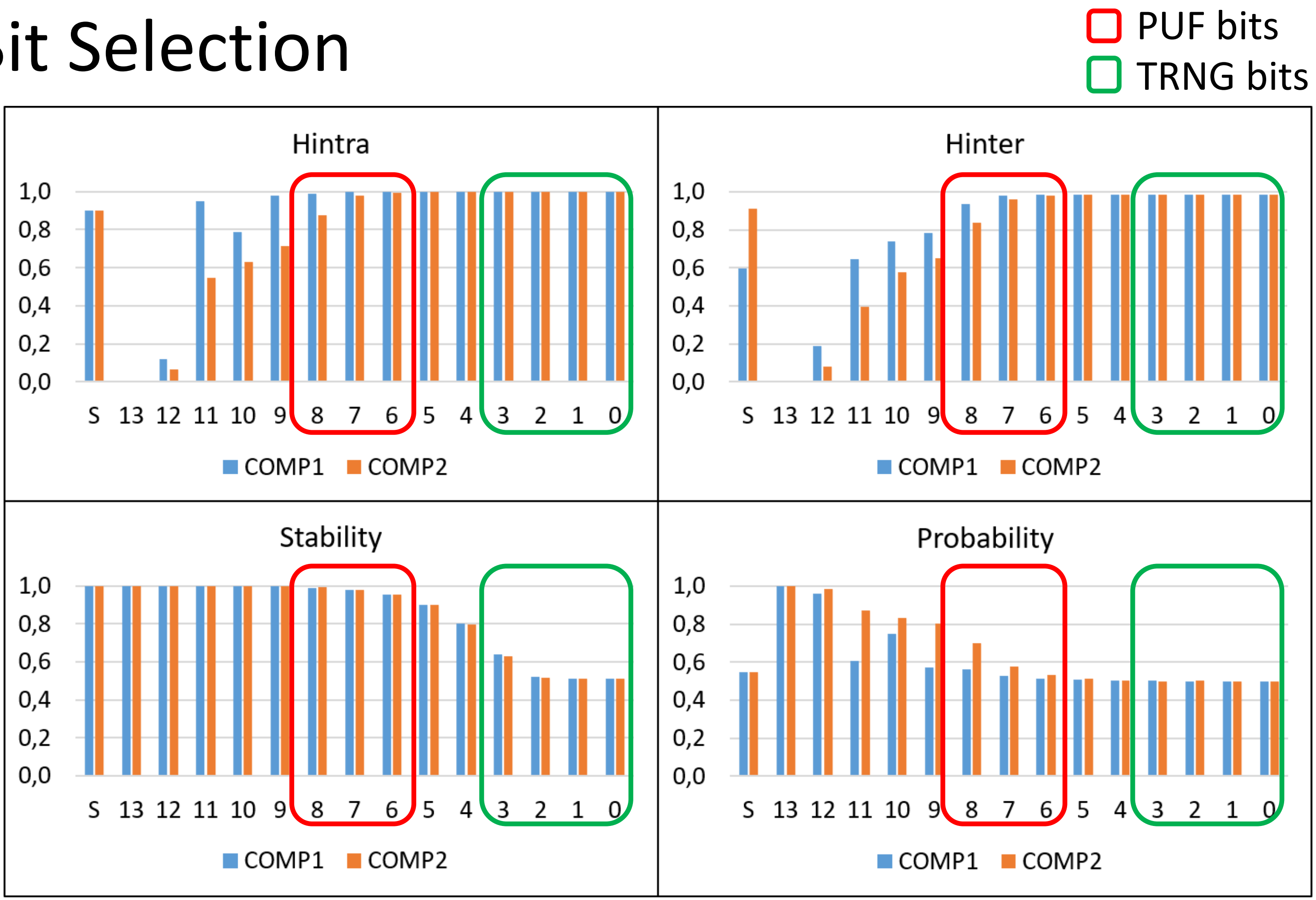


Figure 8. Stability, probability and entropy metrics calculated for each bit of the counters under the binary-closest RO-PUF/TRNG configuration.

- Validation Scheme

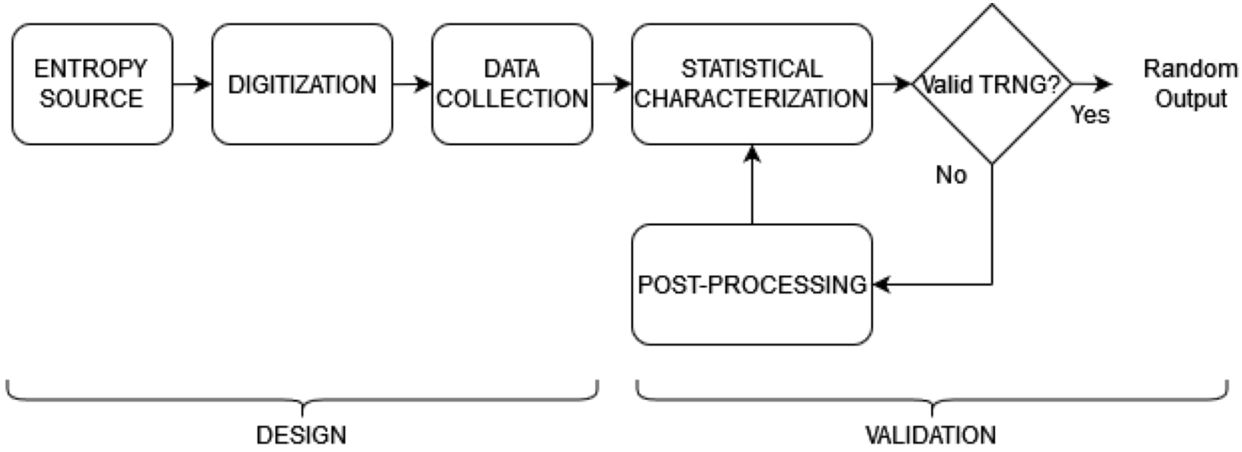


Figure 9. Flowchart of the design and validation processes of a TRNG.

- Entropy source
  - Variability/Entropy Unit
- Digitization
  - RO-Pair Selection Strategy
- Data Collection
  - Output Bit Repository
- Statistical Characterization
  - NIST 800-22
  - NIST 800-90B
- Post-Processing
  - XOR
  - Von Nuemann

4. TRNG VALIDATION PROCESS

- Statistical Characterization
  - NIST 800-22
    - 15 Tests
  - NIST 800-90B
    - Identical and Independent Distribution (IID) tests
    - Non-IID tests
    - 2 Health check tests
- Post-Processing
  - XOR corrector
  - Von Nuemann corrector

- NIST 800-22 standard
  - First Assessment: preliminary results
    - 7/15 tests: short bitstream length required
    - Randomness degree of 1, 2 and 4 LSB per counter
    - Configurations: Closest/Farthest + Binary/Gray
    - Total of 24 TRNG possibilities
  - Data collection strategy
    - Generate sequences of 480 bits
    - Generate 100 bit sequences for each TRNG.
    - Collect data from the 10 IP modules implemented in a test system.

– First Statistical Assessment

LSBs	1								2								4							
Loc.	CLOSEST				FARTHEST				CLOSEST				FARTHEST				CLOSEST				FARTHEST			
Code	G		B		G		B		G		B		G		B		G		B		G		B	
Cntr	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
PUF 0	5	7	7	7	7	7	7	7	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
PUF 1	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	6	7	7	7	7	7	7	7
PUF 2	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	5	7	7	7
PUF 3	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	4	7	7	6
PUF 4	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	2	5	7	7
PUF 5	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	6	7	7	7	7
PUF 6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
PUF 7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	3	7	7	7	7	7	7	7
PUF 8	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	6	7	7	7
PUF 9	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	6	7	7	7

G : Gray code. B : Binary code.

Table 1. Count of NIST 800-22 subset tests successfully passed by the random bit sequences extracted from the 24 feature combinations derived from the RO-PUF/TRNG desing.

LSBs	4								4†			
Location	CLOSEST				FARTHEST				CLOSEST		FARTHEST	
Counter Code	G		B		G		B		G	B	G	B
Counter	1	2	1	2	1	2	1	2	1 & 2	1 & 2	1 & 2	1 & 2
PUF 0	7	7	7	7	7	7	7	7	7	7	7	7
PUF 1	6	7	7	7	7	7	7	7	7	7	7	7
PUF 2	7	7	7	7	5	7	7	7	7	7	7	7
PUF 3	7	7	7	7	4	7	7	6	7	7	7	7
PUF 4	7	7	7	7	2	5	7	7	7	7	7	7
PUF 5	7	7	7	6	7	7	7	7	7	7	7	7
PUF 6	7	7	7	7	7	7	7	7	7	7	7	7
PUF 7	3	7	7	7	7	7	7	7	7	7	7	7
PUF 8	7	7	7	7	6	7	7	7	7	7	7	7
PUF 9	7	7	7	7	6	7	7	7	7	7	7	7

†: 2 LSBs concatenated from each counter. G: Gray code. B: Binary code.

Table 2. Comparison of tests successfully approved by 4 LSBs collected from each entropy source against 4 LSBs concatenated from each counter whitin the NIST 800-22 subset.

- NIST 800-22 standard
  - Second Assessment:
    - 15/15 tests
    - Randomness degree of 2 LSBs concatenated from each counter.
    - Configurations: Closest/Farthest + Binary/Gray
    - Total of 4 TRNG possibilities
  - Data collection strategy
    - Generate sequences of 1M bits
    - Generate 100 bit sequences for each TRNG.
    - Collect data from the 10 IP modules implemented in a test system.

– Second Assessment

LSBs	4†			
Counter Code	Gray		Binary	
Location	Closest	Farthest	Closest	Farthest
Counter	1 & 2	1 & 2	1 & 2	1 & 2
PUF 0	9	11	11	15
PUF 1	10	13	12	15
PUF 2	10	13	11	15
PUF 3	10	12	12	15
PUF 4	9	12	11	15
PUF 5	10	12	12	15
PUF 6	10	11	13	15
PUF 7	10	11	12	15
PUF 8	11	12	10	15
PUF 9	8	10	10	15

†: 2 LSBs concatenated from each counter.

Table 3. Count of NIST 800-22 subset tests successfully approved by the 4 TRNGs configurations.

4. TRNG VALIDATION PROCESS

- NIST 800-22 standard
  - Third Assessment:
    - 15/15 tests
    - Randomness degree of 2 LSBs concatenated from each counter.
    - Configurations: Closest/Farthest + Binary/Gray
    - Post-processing:
      - XOR corrector
      - Von Nuemann corrector
    - Total of 3/4 TRNG possibilities
  - Data collection strategy
    - Generate sequences of 1M bits
    - Generate 100 bit sequences for each TRNG
    - Collect data from the 10 IP modules implemented in a test system

- Post-processing

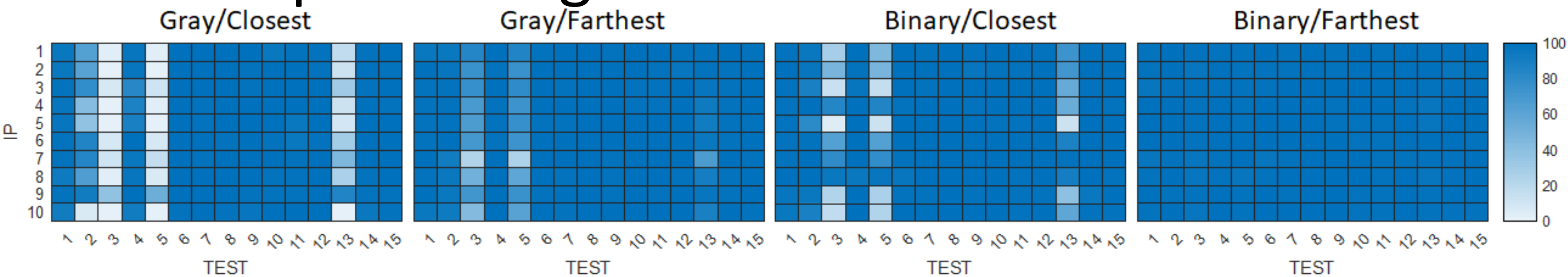


Figure 10. Color map of the rate of NIST 800-22 tests passed by each RO-PUF/TRNG implementation (the darker the color, the higher the pass rate) assessing raw data.

LSBs	**4†**					
Corrector	**Von Neumann**			**XOR**		
Counter Code	**Gray**		**Binary**	**Gray**		**Binary**
Location	**Closest**	**Farthest**	**Closest**	**Closest**	**Farthest**	**Closest**
Counter	**1 & 2**	**1 & 2**	**1 & 2**	**1 & 2**	**1 & 2**	**1 & 2**
PUF 1	10	12	13	15	15	15
PUF 2	13	15	13	15	15	15
PUF 3	13	10	13	15	15	15
PUF 4	11	11	11	15	15	15
PUF 5	11	11	10	15	15	15
PUF 6	12	11	13	15	15	15
PUF 7	10	11	11	15	15	15
PUF 8	12	13	13	15	15	15
PUF 9	13	13	15	15	15	15
PUF 10	10	11	11	15	15	15

†: 2 LSBs concatenated from each counter.

Tabla 4. Test pass rate obtained using Von Neuman and XOR correctors.

- NIST 800-90b recommendation
  - IDD & Non-IID tests

		XOR			RAW
	TEST	GC	GF	BC	BF
IID	IID Permutation	Pass	Pass	Pass	Pass
	Chi-square Independence	Pass	Pass	Pass	Pass
	Chi-square Goodness-of-fit	Pass	Pass	Pass	Pass
	LRS Test	Pass	Pass	Pass	Pass
Non-IID	Most Common Value Estimate	0.995915	0.995351	0.995543	0.993609
	Collision Estimate	0.917535	0.905876	0.896818	0.895582
	Markov Estimate	0.999247	0.999097	0.997907	0.998003
	Compresion Estimate	0.836274	0.830815	0.882088	0.843385
	t-Tuple Estimate	0.931433	0.921623	0.921623	0.93978
	LRS Estimate	0.919974	0.996316	0.989705	0.986412
	MultiMCW Predictoin Estimate	0.998528	0.998482	0.996301	0.994446
	Lag Prediction Estimate	0.995447	0.99642	0.99543	0.994662
	MultiMMC Prediction Estimate	0.995224	0.99653	0.994583	0.996677
	LZ78Y Prediction Estimate	0.997862	0.998061	0.996336	0.994705

Table 5. Entropy estimation of 4 TRNGs using the NIST 800-90b recomendation

  - Health Check tests
    - Adaptive Proportion test: PASS
    - Repetition Count test: PASS

- Comparison Table – NIST 800-22

No. Test	PUF/TRNG proposal				[2]		[3]	[4]	[5]	
	XOR			RAW	RAW	Post-Proc			XOR	VN
	GC	GF	BC	BF					3LSB	3LSB
1	98	98	98	97	98	98	100	98	98	95
2	99	98	98	99	99	99	95	100	99	99
3	98	98	98	97	98	98	95	99	98	99
4	98	98	99	98	99	99	100	98	100	100
5	99	98	99	97	99	99	95	99	99	99
6	99	98	98	98	98	98	100	99	98	99
7	99	99	99	98	98	99	100	98	99	100
8	99	99	99	99	99	99	100	99	98	94
9	98	98	99	98	98	99	100	99	95	97
10	98	98	98	98	98	99	100	99	99	99
11	98	98	98	98	98	98	100	99	98	99
12	99	99	99	98	99	99	100	99	100	99
13	99	98	99	97	98	98	100	98	100	100
14	98	98	98	98	98	99	100	99	100	99
15	98	98	98	98	99	99	95	99	100	100
μ	98,5	98,2	98,5	97,9	98,4	98,7	98,7	98,8	98,7	98,5

Table 6. Average test pass rate of 4 TRNGs using the NIST 800-22 statistical test suite against related works.

6. CONCLUSIONS

- The configurability levels of the original PUF design allows to derive four TRNG configurations based on the relative location of the competing rings and the type of counter.
- The statistical results of the randomness level of the four TRNG configurations satisfy the NIST 800-22 standard and the NIST 800-90b recommendation.
- The design includes the capability of generating true random numbers without any post-processing stage (Binary/Farthest configuration).
- The proposed PUF/TRNG design incorporates two security primitives in a compact design, thus optimizing both resource and power consumption.

REFERENCES

[1] Martínez-Rodríguez, M.C.; Rojas-Muñoz, L.F.; Camacho-Ruiz, E.; Sánchez-Solano, S.; Brox, P. Efficient RO-PUF for Generation of Identifiers and Keys in Resource-Constrained Embedded Systems. Cryptography 2022, 6.

[2] Anandakumar, N.N.; Sanadhya, S.K.; Hashmi, M.S. FPGA-based true random number generation using programmable delays in oscillator-rings. IEEE Transactions on Circuits and Systems II: Express Briefs 2019, 67, 570–574.

[3] Cao, Y.; Zhao, X.; Zheng, W.; Zheng, Y.; Chang, C.H. A new energy-efficient and high throughput two-phase multi-bit per cycle ring oscillator-based true random number generator. IEEE Transactions on Circuits and Systems I: Regular Papers 2021, 69, 272–283.

[4] Acar, B.; Ergün, S. A robust digital random number generator based on transient effect of ring oscillator. In Proceedings of the 2020 IEEE 11th Latin American Symposium on Circuits & Systems (LASCAS). IEEE, 2020, pp. 1–4.

[5] Buchovecká, S.; Lórencz, R.; Kodýtek, F.; Buˇcek, J. True random number generator based on ring oscillator PUF circuit.
Microprocessors and Microsystems 2017, 53, 33–41

Thanks for your attention!