IMSE-cnm Instituto de Microelectrónica de Sevilla

DCIS21 XXXVI CONFERENCE

Design Flow to Evaluate the Performance of Ring Oscillator PUFs on FPGAs

M.C. Martínez-Rodríguez, E. Camacho-Ruiz, S. Sánchez-Solano and P. Brox

26th November 2021

SPIRS Project with Grant Agreement No. 952622 under the EU H2020 research and innovation programme

Grant PID2020-116664RBI00 funded by MCIN/AEI/10.13039/501100011033

LINKA20216 from CSIC

Post-doc grant supported by the Andalusian government under EU PO. FSE.

SPIRS

Outline

1. Introduction
2. Design flow of RO PUFs using SysGen
3. Performance evaluation of RO PUFS
4. Experimental results
5. Conclusions

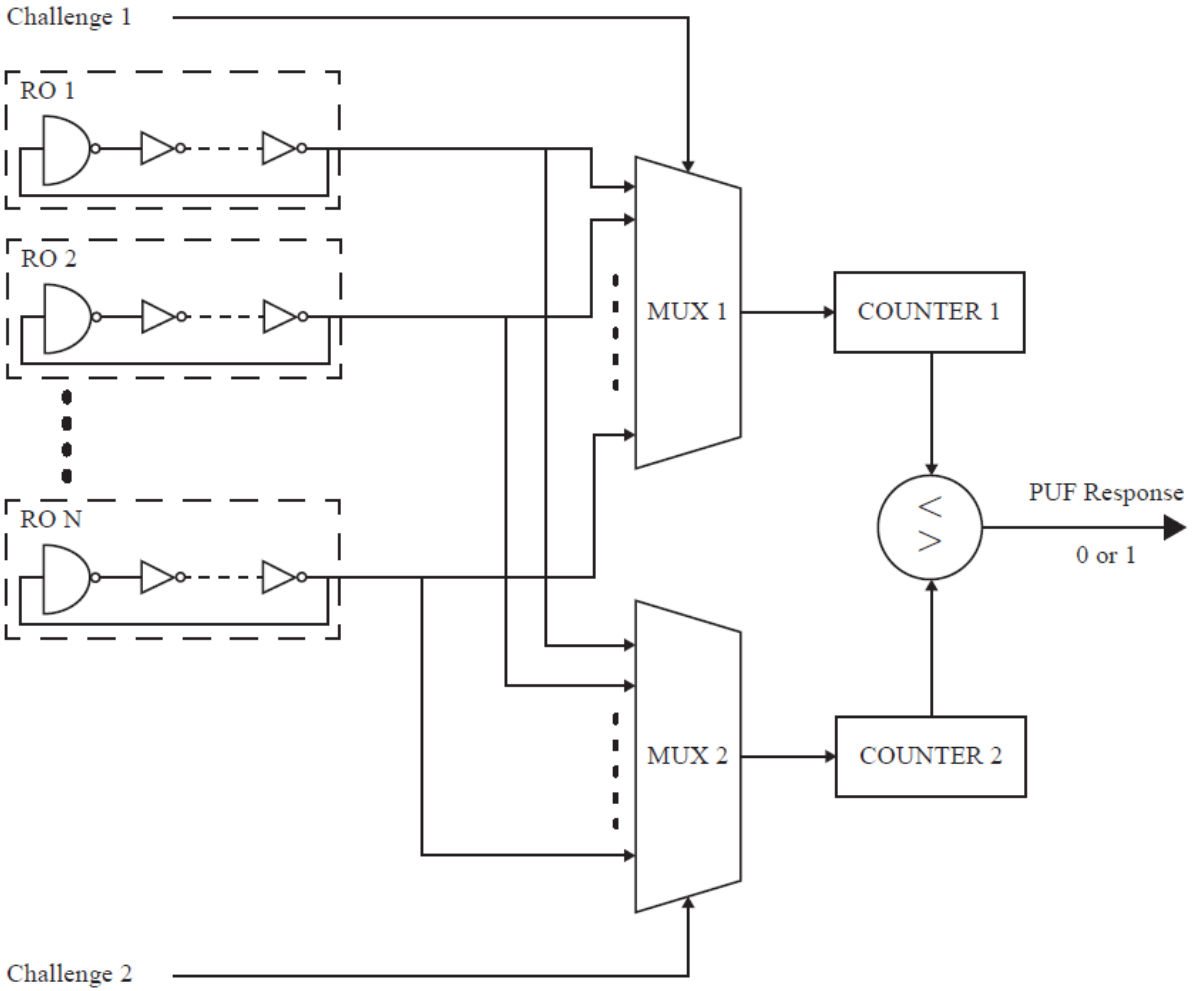
PUF properties

- **Uniqueness:** different PUF instances should return different responses when the same challenge is applied
- **Reliability:** a PUF instance should return a response as unchanged as possible when the same challenge is applied
- **Unpredictability**: there is no way to predict an output PUF response, even the PUF designer can not guess it.

- PUF responses can be used to derive a unique digital identity (PUF ID) inherent to the electronic device in which the PUF circuitry is inserted.

Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. Proc. IEEE 2014, 102, 1126–1141.

Conventional RO PUF

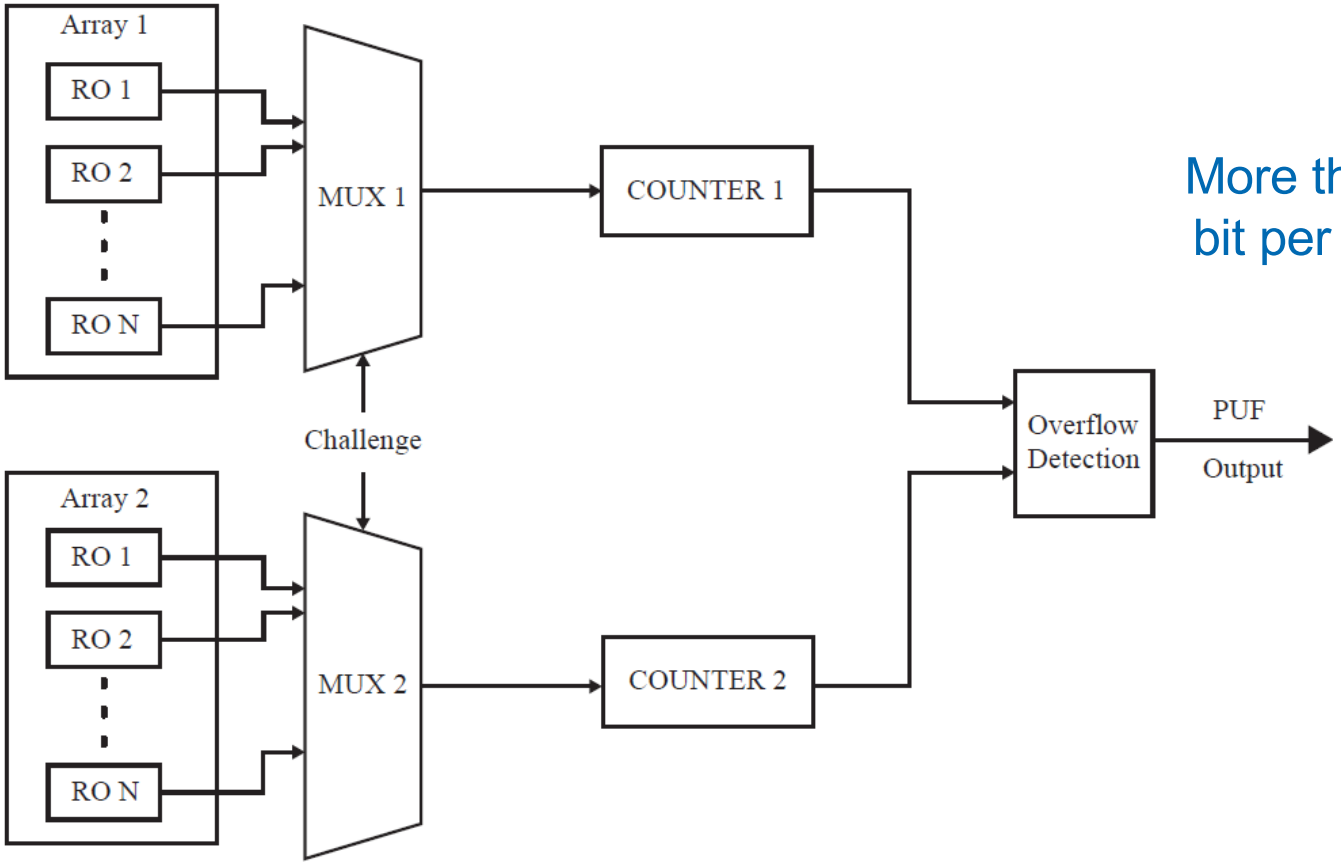


$$f_{RO} = \frac{1}{nstages \times \tau_{INV}}$$

All the ROs are the same by construction, but their frequency is not the same due to variability of technological parameters and certain physical phenomena (such as jitter, transistor-level noise sources, etc.)

Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. Proc. IEEE 2014, 102, 1126–1141.

RO PUF principle

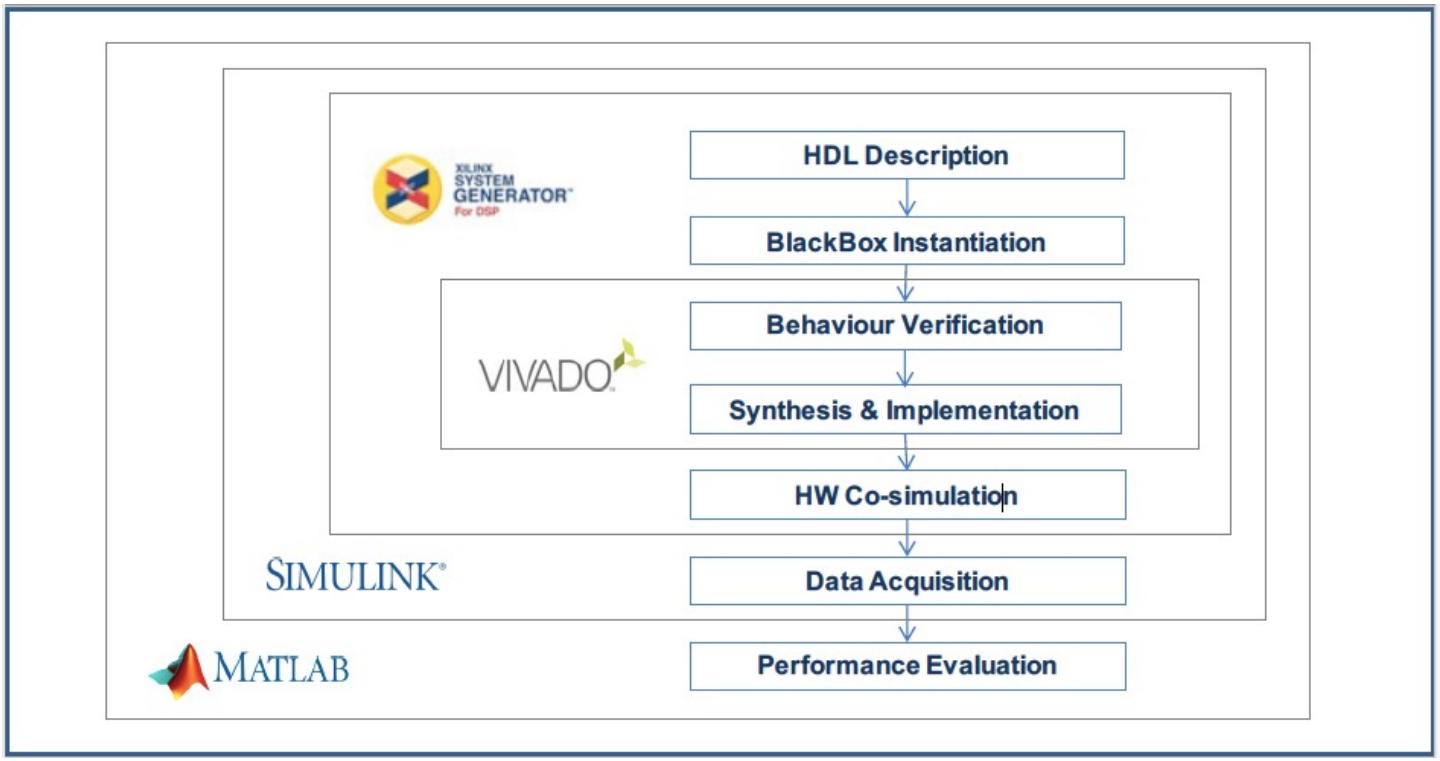


More than one bit per output!!

For each pair of ROs, the output is the value of the counter of the ROs with the lower frequency

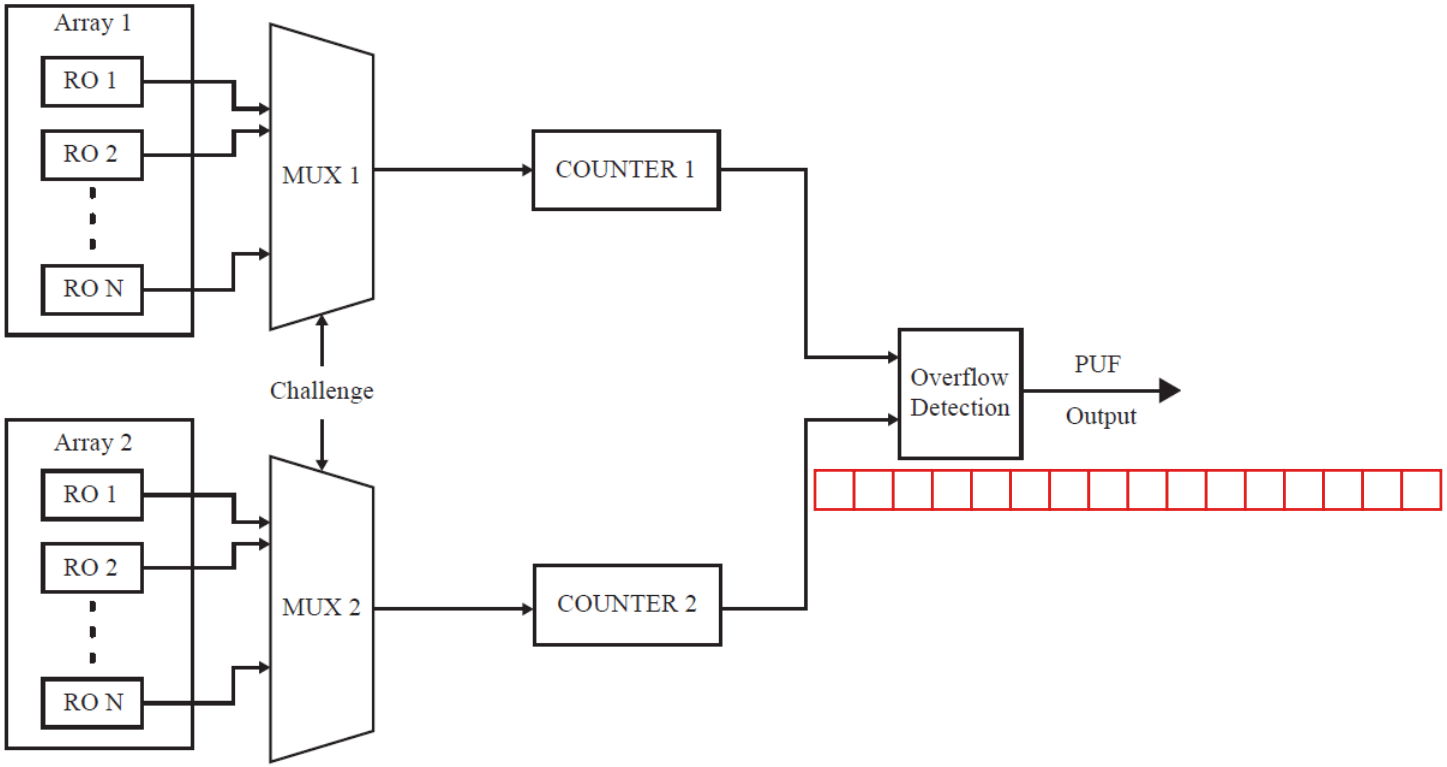
Kodýtek, F.; Lórencz, R. A Design of Ring Oscillator Based PUF on FPGA. 2015 IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits Systems, 2015, pp. 37–42. doi:10.1109/DDECS.2015.21.
Kodtek, F.; Lrencz, R.; Buek, J. Improved Ring Oscillator PUF on FPGA and Its Properties. Microprocess. Microsyst. 2016, 47, 55–63. doi:10.1016/j.micpro.2016.02.005.

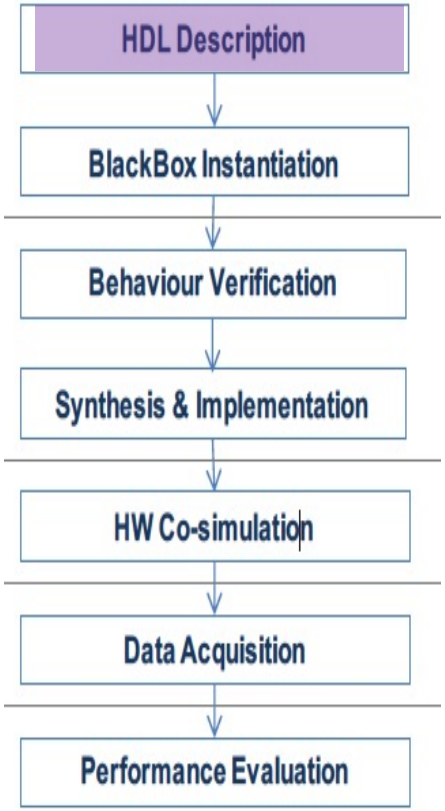
Design flow of RO PUFs using SysGen (I)



- HW co-simulation enables that the PUF is working on the FPGA while the challenges/responses are generated/processed with Matlab.
- Analysis of a silicon PUF since the variations of CMOS manufacturing process are exploited **only** when the PUF is implemented. An analysis of the PUF behavior based on simulations would be useless.
- To ensure PUF properties: analysis of a huge number of PUF responses.

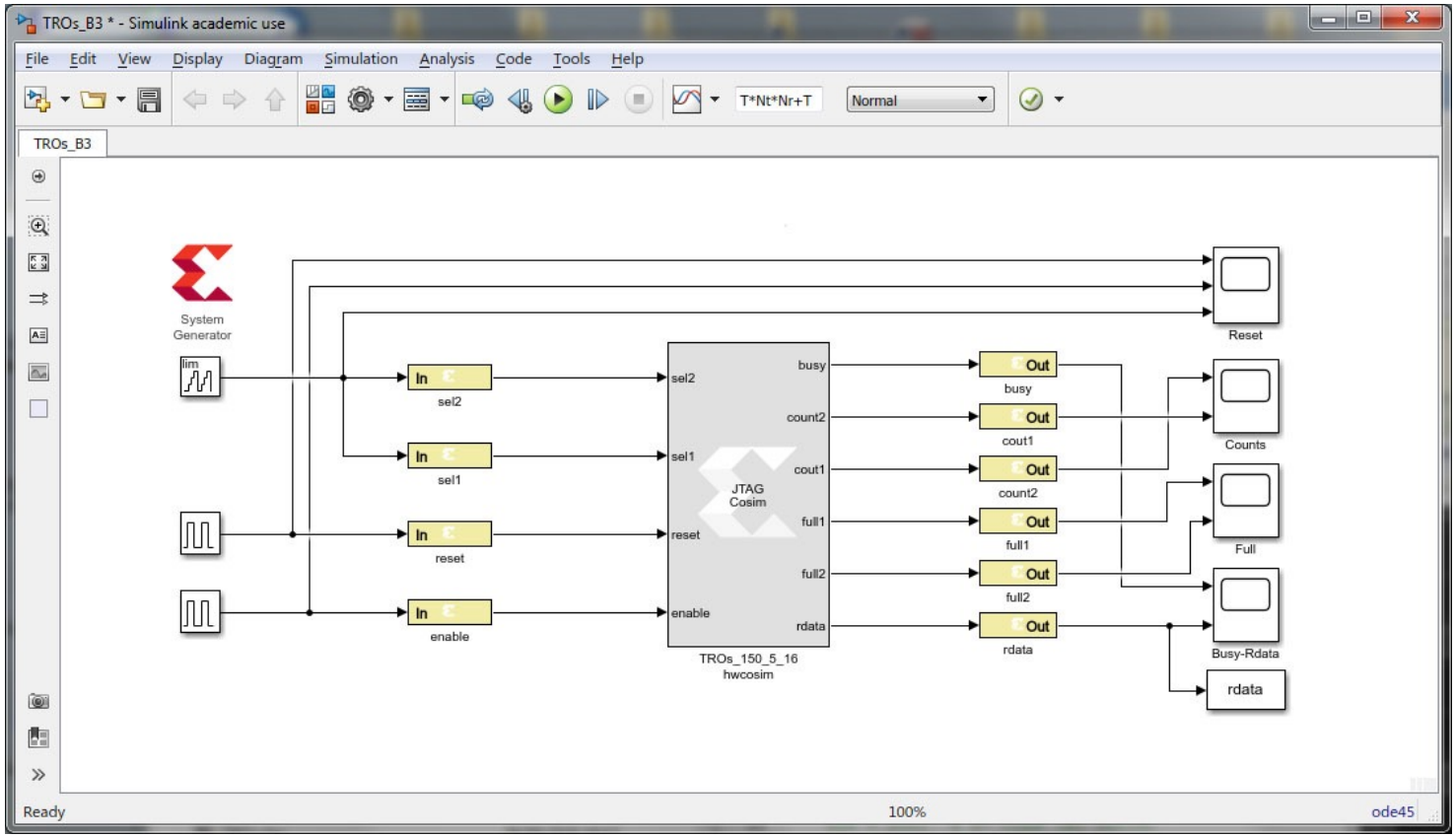
Design flow of RO PUFs using SysGen (II)

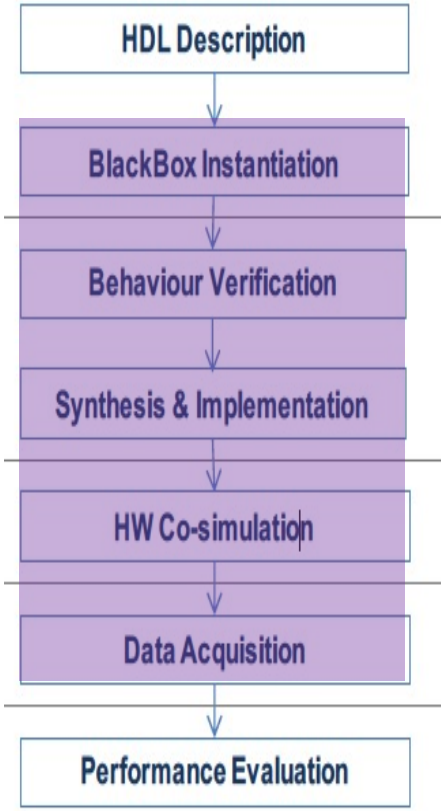




Challenge RO pair response: the value of the counter of the RO with the lower frequency

Design flow of RO PUFs using SysGen (III)





Performance evaluation of RO PUFS (I)

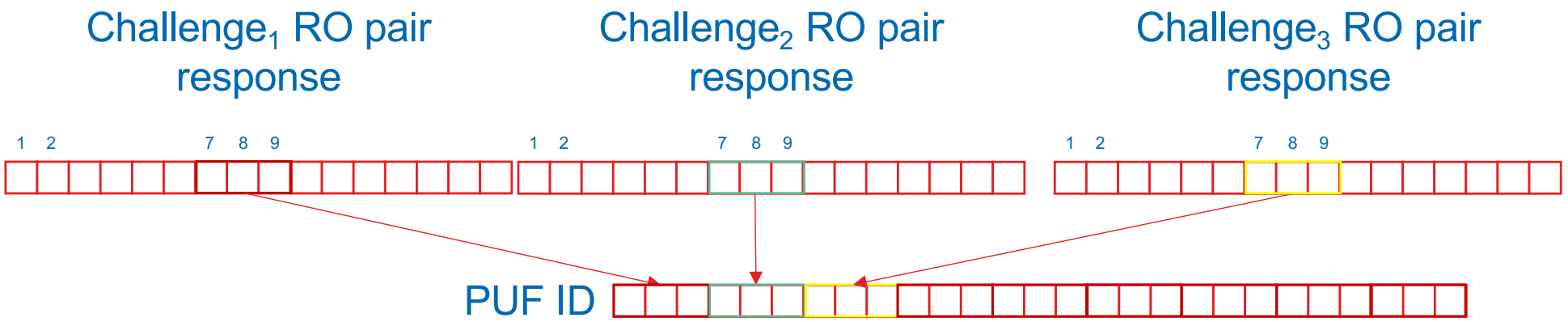
Challenge-response RO PUF bit performance

Not all the bits provided by the overflow detection block satisfies the PUF properties. For each bit, reliability, unpredictability and entropy is analyzed.

- **Reliability** is measured by the average bit stability, the more stable, the more reliable.
- **Unpredictability** is measured by the average bit probability. Ideal value: 50%.
- Entropy will determine the **uniqueness.** Ideal values: Hintra=1 and Hinter=1.

Performance evaluation of RO PUFS (II)

RO PUF performance



Challenge$_i$ RO pair response: the value of the counter of the RO with the lower frequency
PUF ID: Concatenation of the **selected bits** of each challenge for all possible challenges.

- Intra-Hamming distance (HDintra) determines the **similarity** between responses.

Ideal value: HDIntra=0, which means that the RO PUF ID is always the same when the same sequence of challenges is applied to the same device.

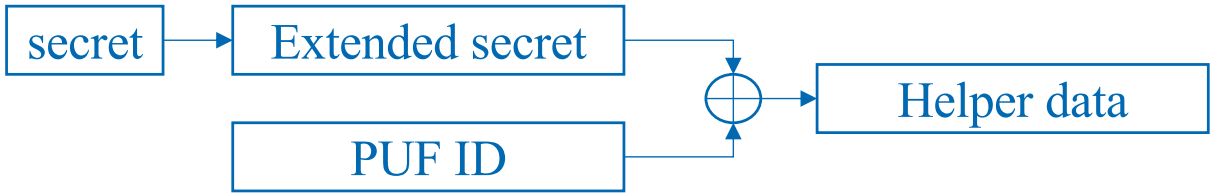
- Inter-Hamming distance (HDinter) determines the **uniqueness** of the responses generated among different devices

  Ideal value: HDinter=50%

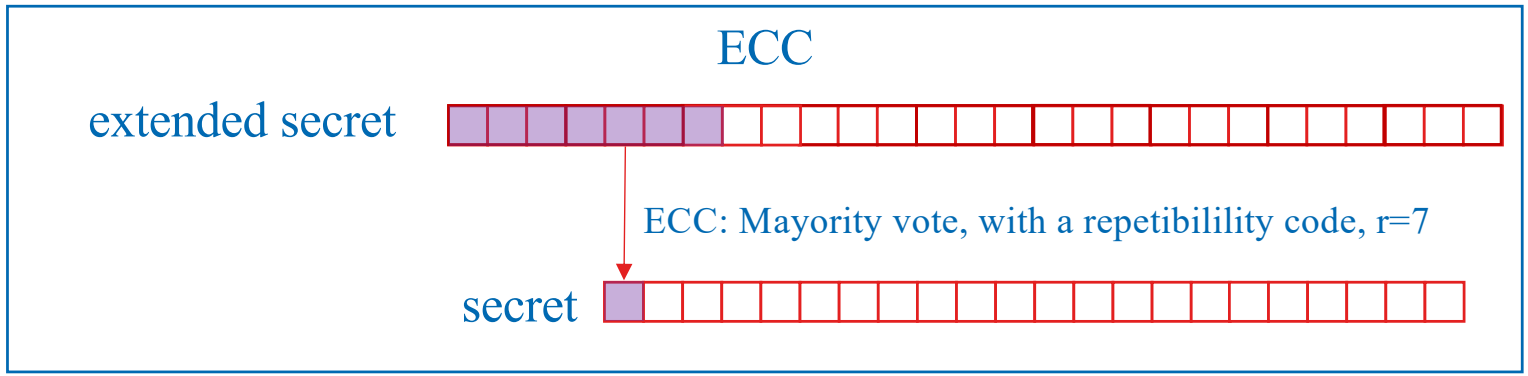
Performance evaluation of RO PUFS (III)

Obfuscation and recovery of a secret using RO PUFs

- Enrolment: we want to obfuscate a secret without storing it



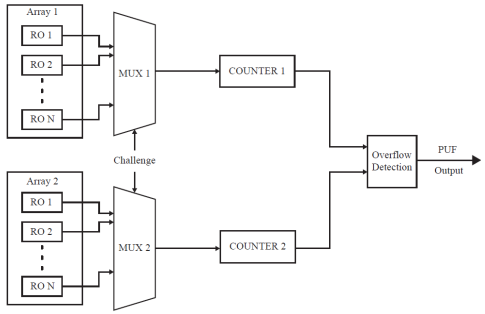
- Reconstruction: we want to recovery the secret



Suh, G.E.; Devadas, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9–14.
Delvaux, J.; Gu, D.; Schellekens, D.; Verbauwhede, I. Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2015, 34, 889–902. doi:10.1109/TCAD.2014.2370531
Hiller, M.; Kürzinger, L.; Sigl, G. Review of error correction for PUFs and evaluation on state-of-the-art FPGAs. Journal of Cryptographic Engineering 2020, 10, 229–247. doi:10.1007/s13389-020-00223-w.

Experimental results (I)

- **Design:**
  - Two arrays of 150 ROs each.
  - Each RO has 5 stages composed by 4 inverters and 1 NAND gate.
  - The size of the output counters is 16 bits.
  - Directives must be included in the HDL description:
    - (*ALLOW COMBINATORIAL LOOPS = “true”, KEEP = “true” *)
    - (DONT TOUCH = “yes”) wire <wire name >;

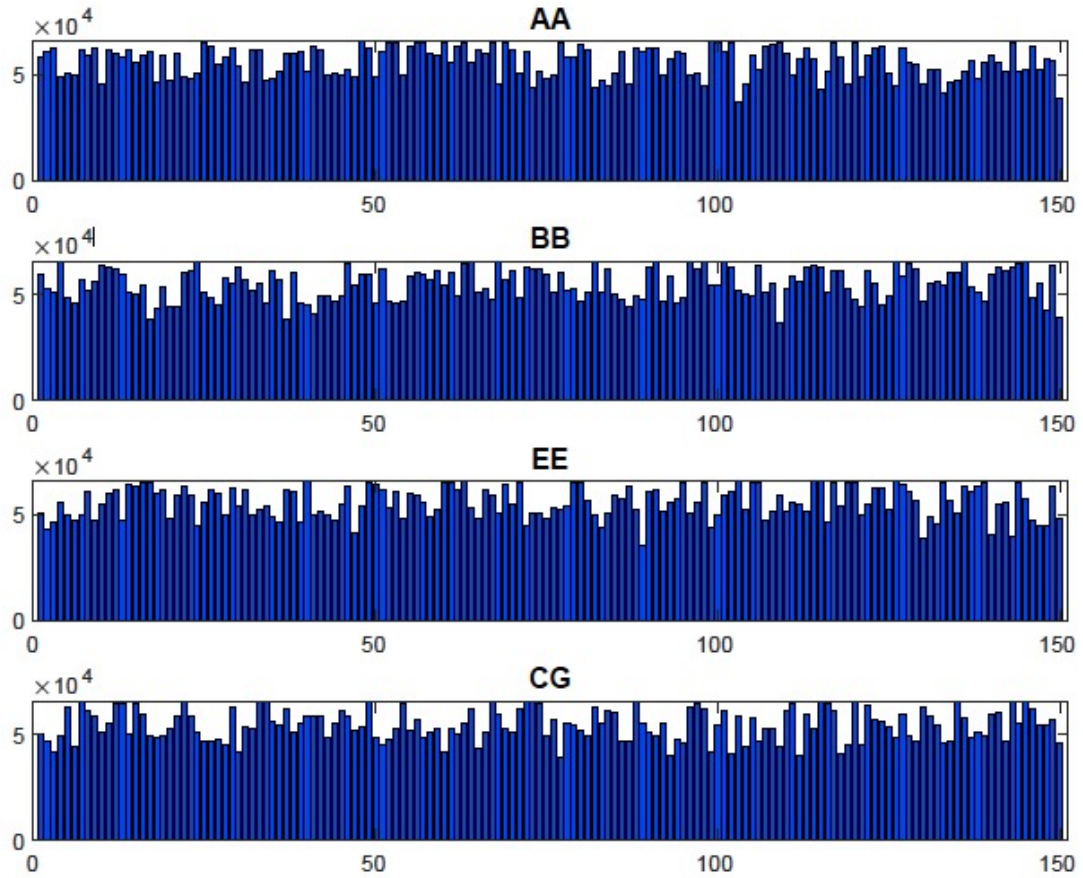


- Synthesis and implementation strategies

Code	Synthesis strategy	Implementation strategy
A	Default	Default
B	Flow AreaOptimized high	Area Explore
C	Flow AlternateRoutability	Performance ExplorePostRoutePhysOpt
D	Flow PerfOptimized high	Performance Explore
E	Flow RuntimeOptimized	Flow RuntimeOptimized
G		Congestion SpreadLogic high

Experimental results (II)

- 17 Basys 3 Artix-7 FPGA Boards
- **Matlab R2018a**
- Systen Generator in **Xilinx Vivado 2018.2.**



Mean values 1000 responses

Experimental results (III)

Challenge-response RO PUF bit performance

For **1000 different responses** for the **same challenge**, for 150 different challenges, and 4 strategies (AA, BB, EE, CG) *17 boards = **68 different RO PUF.**

	Average stability					Average probability					Hintra					Hinter				
	AA	BB	EE	CG	All	AA	BB	EE	CG	All	AA	BB	EE	CG	All	AA	BB	EE	CG	All
1	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
2	1,000	0,999	0,999	1,000	1,000	0,761	0,760	0,758	0,753	0,757	0,7208	0,8300	0,7454	0,8756	0,7930	0,0508	0,0404	0,0266	0,0528	0,5862
3	0,999	0,999	0,999	0,999	0,999	0,662	0,652	0,658	0,658	0,657	0,8794	0,9314	0,9487	0,9388	0,9246	0,0871	0,0675	0,0632	0,0800	0,7375
4	0,999	0,999	0,998	0,998	0,998	0,567	0,574	0,574	0,584	0,574	0,9984	0,9807	0,9714	0,9678	0,9796	0,1975	0,1546	0,1482	0,1858	0,7828
5	0,997	0,997	0,996	0,996	0,997	0,529	0,537	0,542	0,538	0,536	0,9987	0,9951	0,9853	0,9941	0,9933	0,3854	0,4262	0,3817	0,4254	0,8902
6	0,993	0,993	0,993	0,993	0,993	0,567	0,578	0,570	0,561	0,568	0,9886	0,9876	0,9845	0,9628	0,9809	0,7324	0,8062	0,7571	0,7332	0,9374
7	0,985	0,986	0,984	0,986	0,985	0,521	0,512	0,518	0,523	0,517	0,9937	0,9949	0,9982	0,9904	0,9943	0,9496	0,9471	0,9417	0,9280	0,9825
8	0,967	0,970	0,968	0,967	0,968	0,510	0,508	0,518	0,513	0,511	0,9975	0,9934	0,9954	0,9935	0,9950	0,9553	0,9525	0,9576	0,9528	0,9888
9	0,934	0,941	0,936	0,937	0,937	0,509	0,493	0,520	0,501	0,505	0,9951	0,9968	0,9940	0,9938	0,9949	0,9550	0,9570	0,9515	0,9496	0,9891
10	0,869	0,876	0,871	0,871	0,872	0,499	0,491	0,493	0,504	0,496	0,9955	0,9935	0,9942	0,9981	0,9953	0,9540	0,9512	0,9603	0,9557	0,9898
11	0,739	0,741	0,741	0,742	0,741	0,504	0,506	0,507	0,494	0,502	0,9952	0,9959	0,9967	0,9961	0,9960	0,9580	0,9640	0,9530	0,9539	0,9884
12	0,562	0,561	0,563	0,563	0,562	0,500	0,502	0,503	0,500	0,501	0,9973	0,9958	0,9950	0,9958	0,9960	0,9530	0,9618	0,9542	0,9516	0,9897
13	0,513	0,513	0,513	0,513	0,513	0,500	0,500	0,501	0,500	0,500	0,9933	0,9982	0,9939	0,9942	0,9949	0,9601	0,9587	0,9510	0,9654	0,9882
14	0,513	0,513	0,513	0,513	0,513	0,499	0,500	0,501	0,500	0,500	0,9966	0,9930	0,9945	0,9968	0,9952	0,9532	0,9621	0,9515	0,9585	0,9889
15	0,513	0,513	0,513	0,513	0,513	0,500	0,500	0,501	0,500	0,500	0,9959	0,9948	0,9924	0,9939	0,9942	0,9662	0,9608	0,9535	0,9535	0,9886
16	0,513	0,513	0,513	0,513	0,513	0,500	0,500	0,500	0,499	0,500	0,9947	0,9976	0,9913	0,9966	0,9950	0,9603	0,9551	0,9544	0,9548	0,9908

Trade-off: MSB more reliable, LSB more unpredictable

Experimental results (IV)

RO PUF performance

Concatenation of selected bits of all the responses using all the possible challenges.

	PUF 6 - 8			
	HDInter	HDIntra	HDIntra_min	HDIntra_max
AA	45,1209	1,8522	0,8873	2,6367
BB	46,4804	1,7317	1,0176	2,2249
EE	45,5980	1,6682	1,0816	2,1707
CG	44,8268	1,8614	1,2282	2,9862
All	48,6667	1,7784	0,8873	2,9862

$3 \times 150 = 450$ bits

	PUF 6 - 7			
	HDInter	HDIntra	HDIntra_min	HDIntra_max
AA	42,7500	1,0979	0,4580	1,5963
BB	44,8235	1,0926	0,6447	1,7967
EE	43,3578	0,9951	0,5473	1,5030
CG	42,3529	1,1313	0,4113	2,3470
All	48,0187	1,0792	0,4113	2,3470

$2 \times 150 = 300$ bits

	PUF 7 - 8			
	HDInter	HDIntra	HDIntra_min	HDIntra_max
AA	49,7255	2,4211	1,1880	3,3220
BB	49,5882	2,2157	1,3583	2,9950
EE	49,5588	2,1963	1,4753	2,9507
CG	48,9559	2,4438	1,7233	3,6150
All	49,7464	2,3192	1,1880	3,6150

$2 \times 150 = 300$ bits

Experimental results (IV)

Obfuscation and recovery of a secret using RO PUFs

False negative Rate (FNR) and False positive Rate (FPR) after recovering a 32-secret key using PUF 6-7 responses and different-length repetition codes

	AA		BB		EE		CG	
r	FNR	FPR	FNR	FPR	FNR	FPR	FNR	FPR
3	0,641	0,000	0,000	0,000	0,392	0,000	0,711	0,000
5	0,000	0,000	0,034	0,000	0,230	0,000	0,216	0,000
7	0,000	0,000	0,001	0,000	0,006	0,000	0,216	0,000
9	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

FNR and FPR after recovering a 32-bit secret key using r=9 for all boards and strategies

	AA	BB	EE	CG	all
FNR	0,0001	0,000	0,000	0,0144	0,000
FPR	0,000	0,000	0,000	0,000	0,000

Conclusions

- This work presents a design flow to evaluate the performance of RO PUFs on FPGAs based on a DSP tool for FPGAs that provides HW co-simulation.
- HW co-simulation enables that the PUF is working on the FPGA while the challenges/responses are generated/processed with Matlab.
- Analysis of a silicon PUF since the variations of CMOS manufacturing process are exploited **only** when the PUF is implemented.
- To ensure PUF properties: analysis of a huge number of PUF responses. Several scripts and functions were developed to evaluate the properties of the PUFs.
- After extensive experimental results, 2-bits per each CRP can be used to generate the PUF response obtaining a good performance in terms of entropy, probability and stability.
- The reliability of the PUF in the obfuscation and recovery of a secret key is corroborated with experimental results. No counterfeit device is able to retrieve a secret in any of the studied scenarios.

IMSE -cnm Instituto de Microelectrónica de Sevilla

DCIS21 XXXVI CONFERENCE

Thank you for your attention!
Questions?

macarena@imse-cnm.csic.es

SPIRS Project with Grant Agreement No. 952622 under the EU H2020 research and innovation programme

Grant PID2020-116664RBI00 funded by MCIN/AEI/10.13039/501100011033

LINKA20216 from CSIC

Post-doc grant supported by the Andalusian government under EU PO. FSE.

SPIRS