Chaos in Fully Digital Circuits: a Novel Approach to the Design of Entropy Sources

Tommaso Addabbo, Ada Fort, Riccardo Moretti,
Marco Mugnaini, Hadis Takaloo, Valerio Vignoli

Department of Information Engineering and Mathematics
University of Siena, Italy

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

UNIVERSITÀ
DI SIENA 1240

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

Presentation Outline

- Sources of entropy in ‘fully digital’ True Random Number Generators
- A novel class of ‘full digital’ circuits: Digital Nonlinear Oscillators (DNOs)
- A Novel Chaotic DNO Topology in Programmable Logic: study, analysis and experiments
- Design of a True Random Number Generator based on ‘fully digital’ chaos
- Conclusion

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

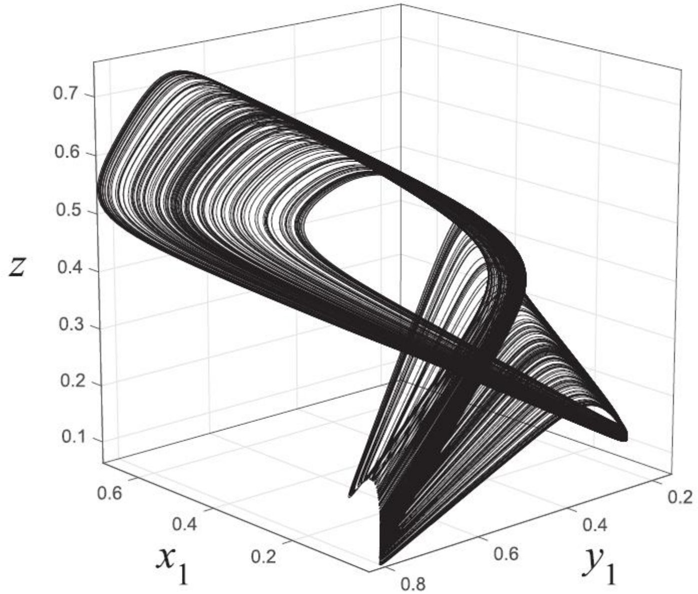
Source of Randomness in Fully Digital TRNGs

Known sources of entropy in ‘fully digital’ True Random Number Generators (TRNGs) are based on the following physical phenomena:

1. **Digital Metastability**;
2. **Random Jitter** (phase noise in periodic oscillators);
3. **Combination** of the above.

We introduce a novel class of circuits, defined as **Digital Nonlinear Oscillators (DNOs),** as possible candidates for a new class of ‘fully-digital’ entropy sources, suitable for cryptographic applications.

We adopt a **nonlinear dynamical system analysis** point of view, discussing theoretical models and proposing numerical investigation techniques to provide evidence that, for specific circuit topologies, the actual source of randomness is due to **deterministic chaos**.



2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

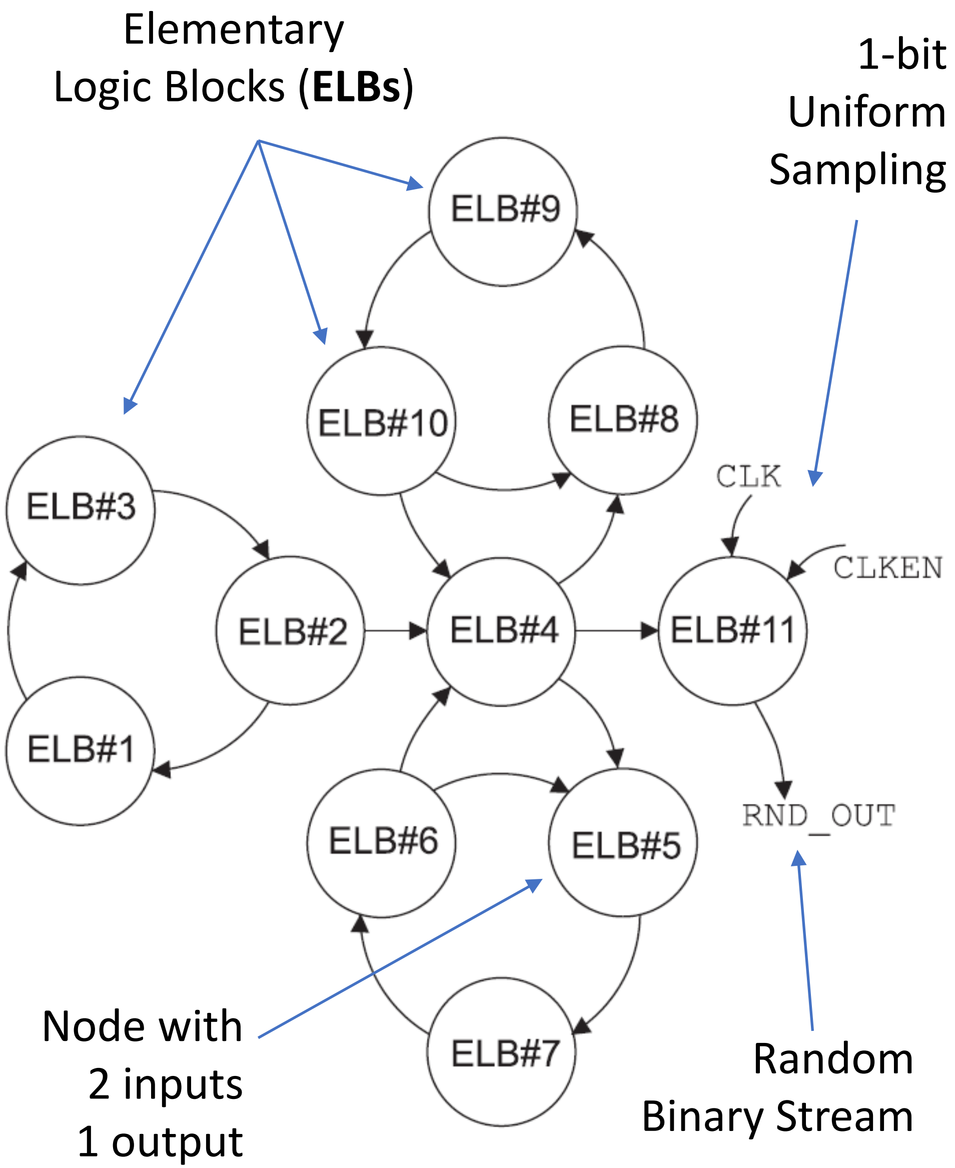
Digital Nonlinear Oscillators (DNOs)

(Informal) Definition:

A Digital Nonlinear Oscillator (DNO) is a ***network of electronic circuits***, each one originally designed to behave as a digital logic gate, implementing an autonomous nonlinear dynamical system exhibiting oscillations in the time-continuous domain.

Each node in the network is an electronic circuit originally designed to implement a Boolean function of the form

$$f : \{0,1\}^k \rightarrow \{0,1\}$$



IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

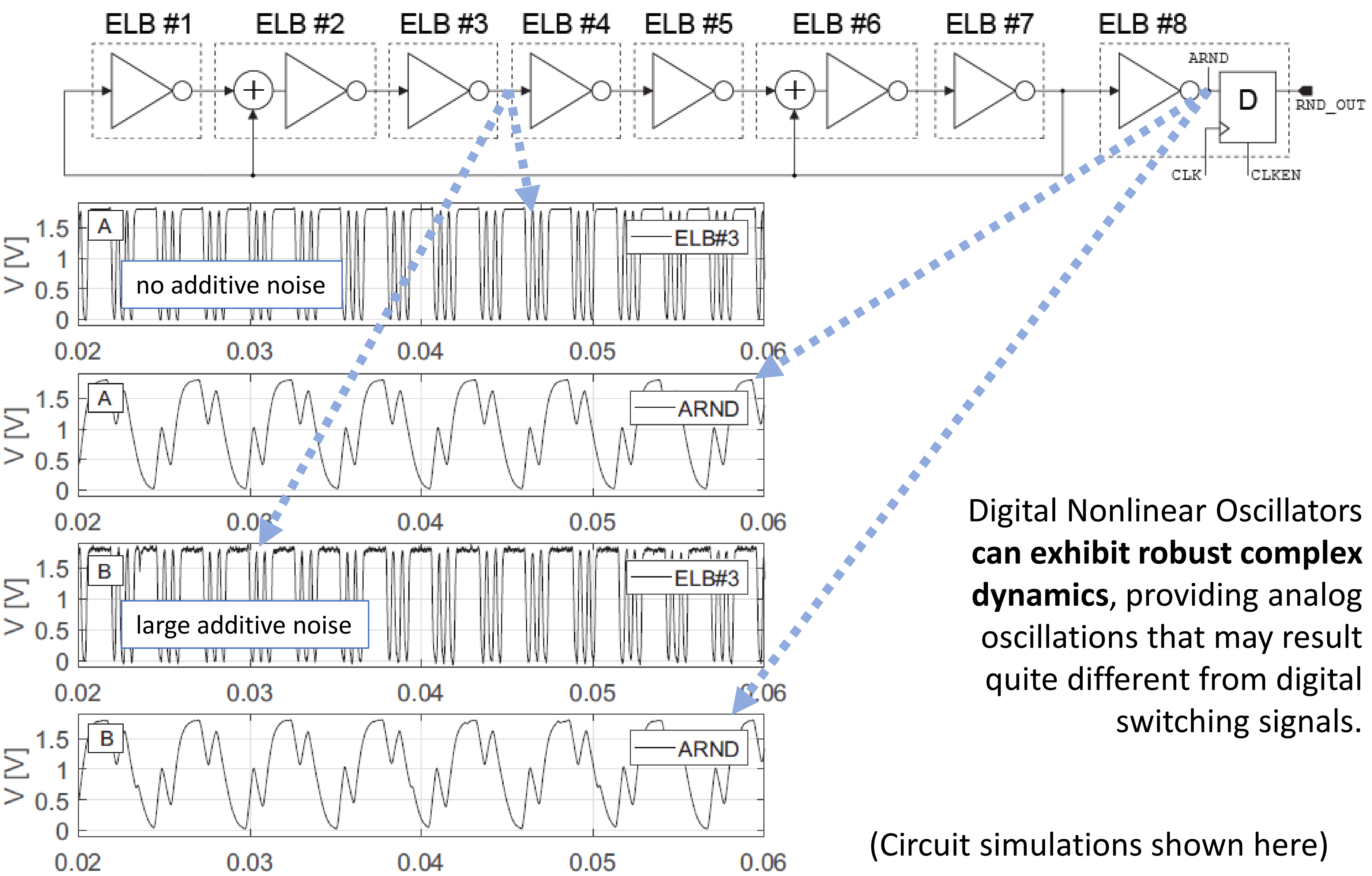
CAS

UNIVERSITÀ DI SIENA 1240

Prof. Tommaso Addabbo

Digital Nonlinear Oscillators (DNOs)

Golic Galois Ring Oscillator (7 nodes)



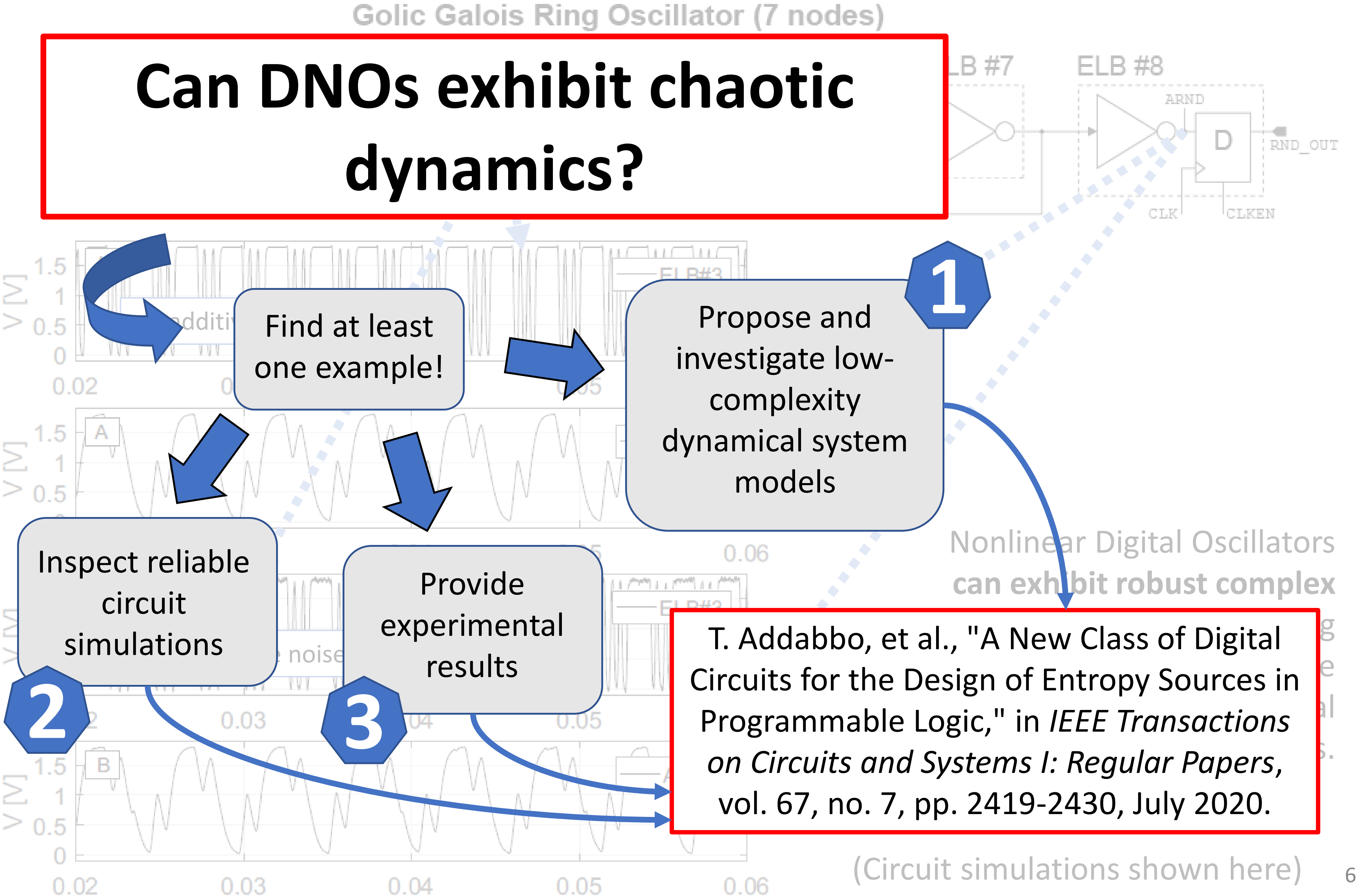
Digital Nonlinear Oscillators **can exhibit robust complex dynamics**, providing analog oscillations that may result quite different from digital switching signals.

(Circuit simulations shown here)

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

Digital Nonlinear Oscillators (DNOs)



Can DNOs exhibit chaotic dynamics?

Find at least one example!

1 Propose and investigate low-complexity dynamical system models

2 Inspect reliable circuit simulations

3 Provide experimental results

Nonlinear Digital Oscillators can exhibit robust complex ...g ...e ...al ...s.

T. Addabbo, et al., "A New Class of Digital Circuits for the Design of Entropy Sources in Programmable Logic," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 7, pp. 2419-2430, July 2020.

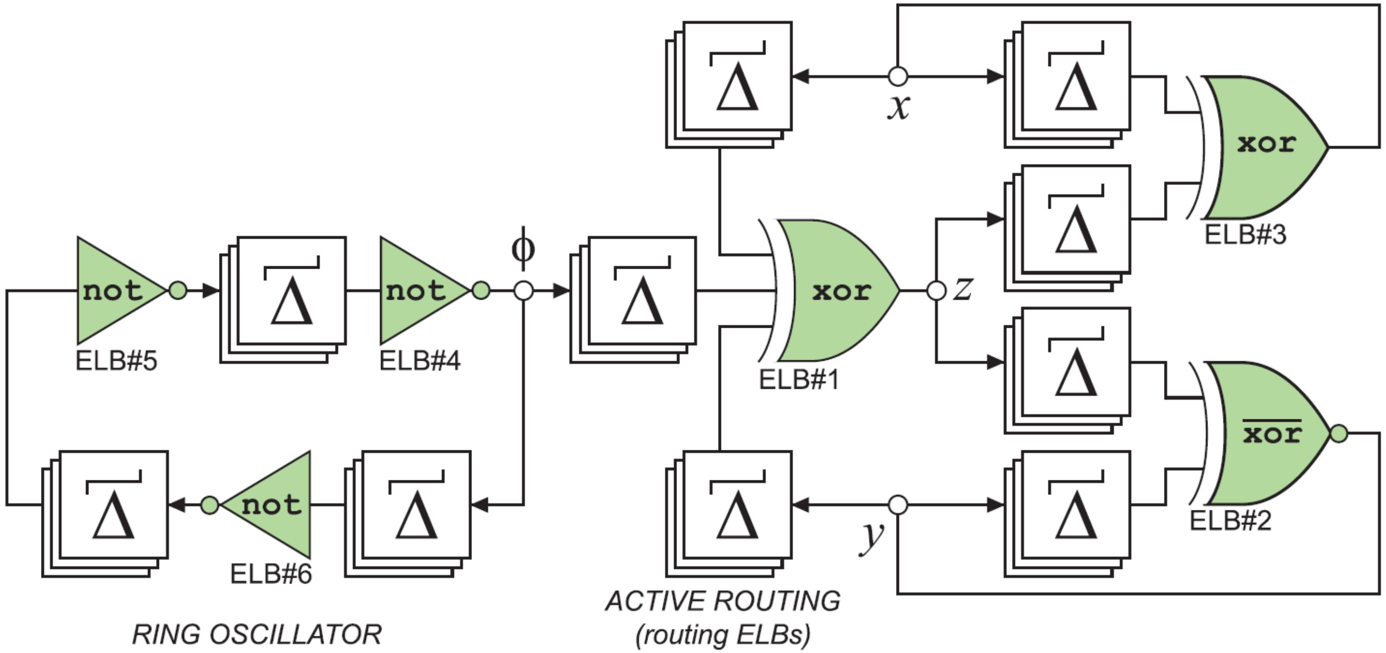
(Circuit simulations shown here)

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

A Novel Chaotic DNO Topology in PLDs

We investigated low-complexity solutions suitable for being implemented in Programmable Logic Devices (PLDs), as FPGAs, without loss of generality.



The circuit is made of 6 Look Up Tables (LUTs, green gates) interconnected using the FPGA active digital routing elements (connection/switch boxes). As shown by the authors, **this circuit admits robust chaotic dynamics**, and can be used to design reliable and efficient entropy sources for true random number generation.

IEEE Xplore® Digital Library

ISCAS 2020

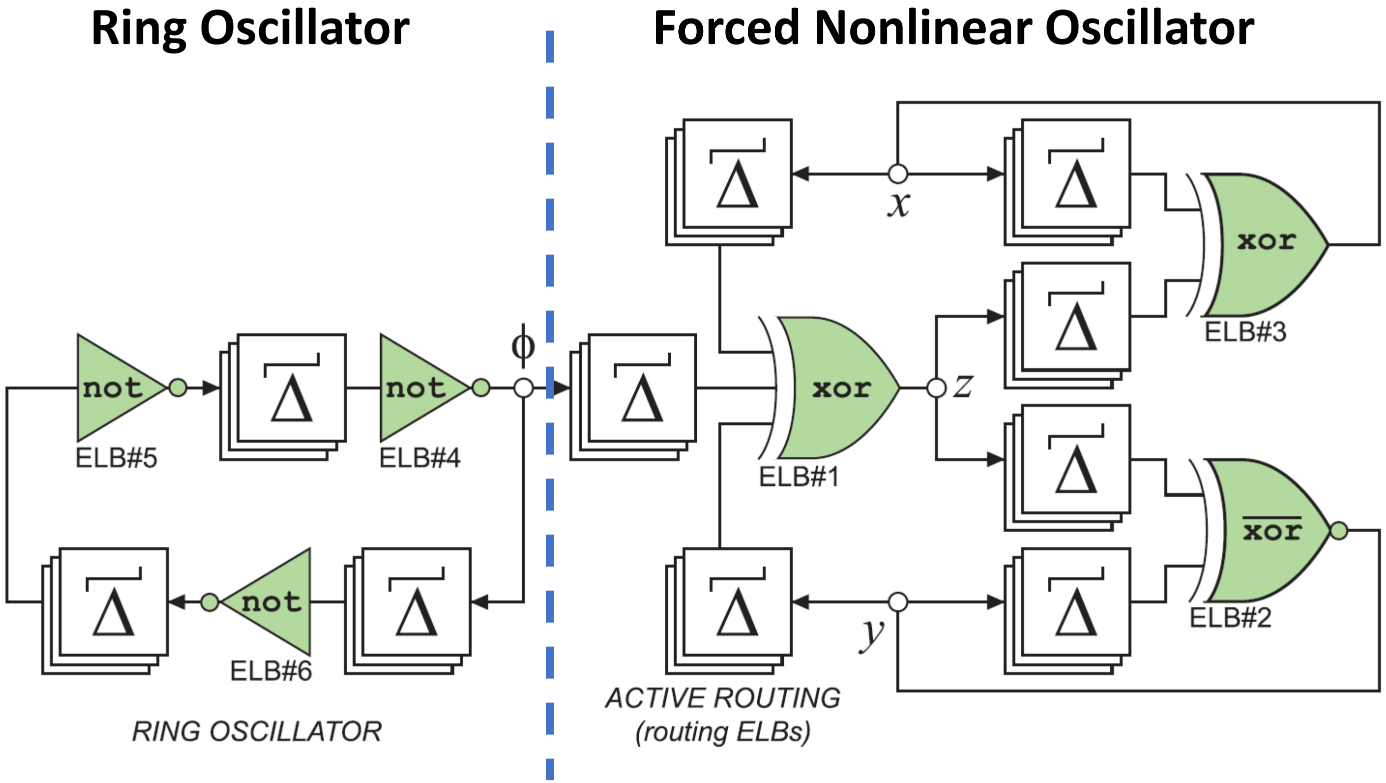
2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

CAS

UNIVERSITÀ DI SIENA 1240

Prof. Tommaso Addabbo

A Novel Chaotic DNO Topology in PLDs



At a first approximation, we assumed to study the proposed DNOs as a **Forced Nonlinear Oscillator** driven by a periodic excitation, provided by a **Ring Oscillator**.

This assumption was used to investigate both **low-dimension theoretical models** and **high-dimension dynamical systems**, resulting from CMOS circuits defined at the transistor level, by means of advanced circuit simulators (Cadence, UMC 180nm technology).

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

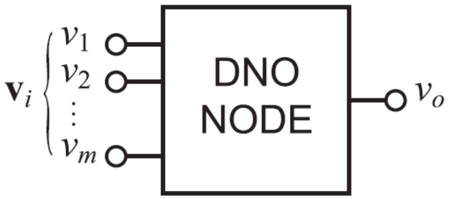
Prof. Tommaso Addabbo

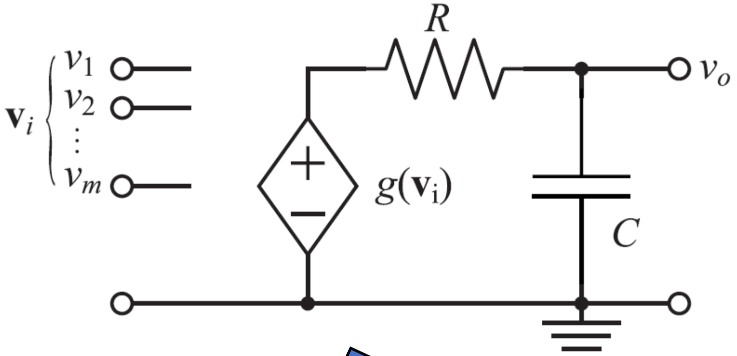
Low-Dimension Theoretical Models

We assumed to relate each DNO node to a first-order cell, such that

$$\frac{dv_o}{dt} = \frac{g(\mathbf{v}_i) - v_o}{RC}$$

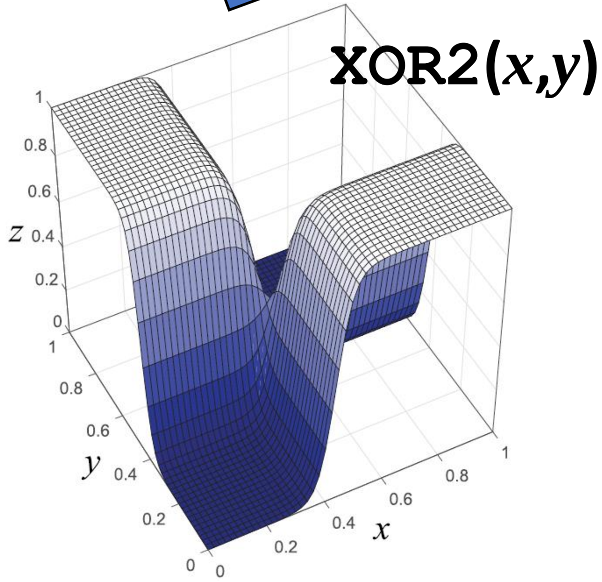
being $g(vi)$ a nonlinear function describing the DC analog transfer function of the digital gate.





$$x_i(v_i) = x_i = \frac{1}{1 + e^{-a(v_i - b)}}$$
$$\bar{x}_i(v_i) = \bar{x}_i = \frac{1}{1 + e^{a(v_i - b)}}$$

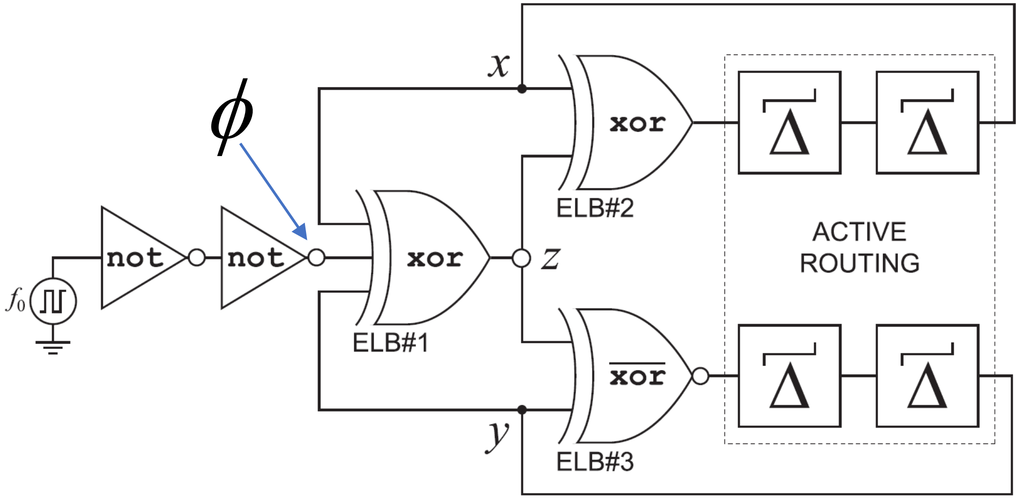
$$\mathtt{del}(v_i) = x_i, \quad \mathtt{xor2}(v_i, v_j) = x_i\bar{x}_j + \bar{x}_i x_j,$$
$$\mathtt{nxor2}(v_i, v_j) = x_i x_j + \bar{x}_i\bar{x}_j,$$
$$\mathtt{xor3}(v_i, v_j, v_k) = (x_i x_j + \bar{x}_i\bar{x}_j)x_k + (x_i\bar{x}_j + \bar{x}_i x_j)\bar{x}_k$$



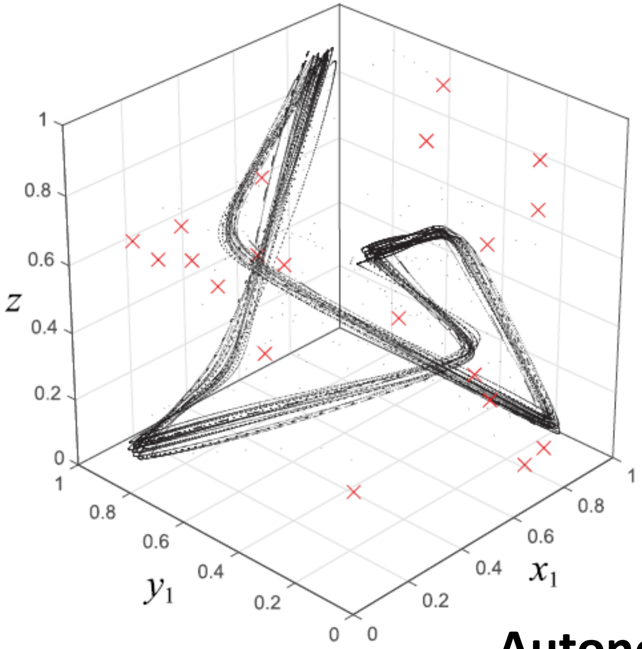
2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

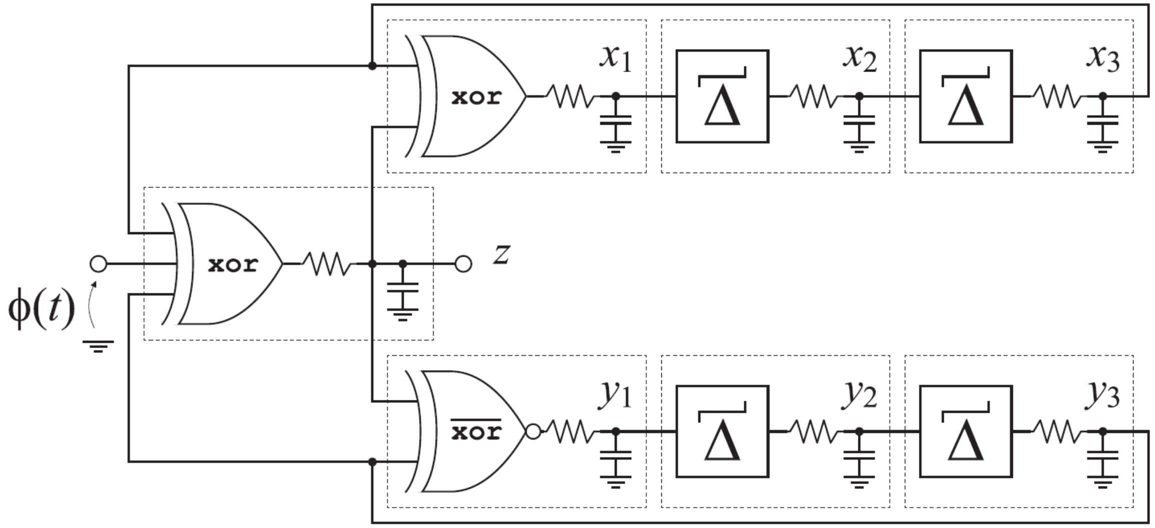
Prof. Tommaso Addabbo

Low-Dimension Theoretical Models



Forced Nonlinear Oscillator





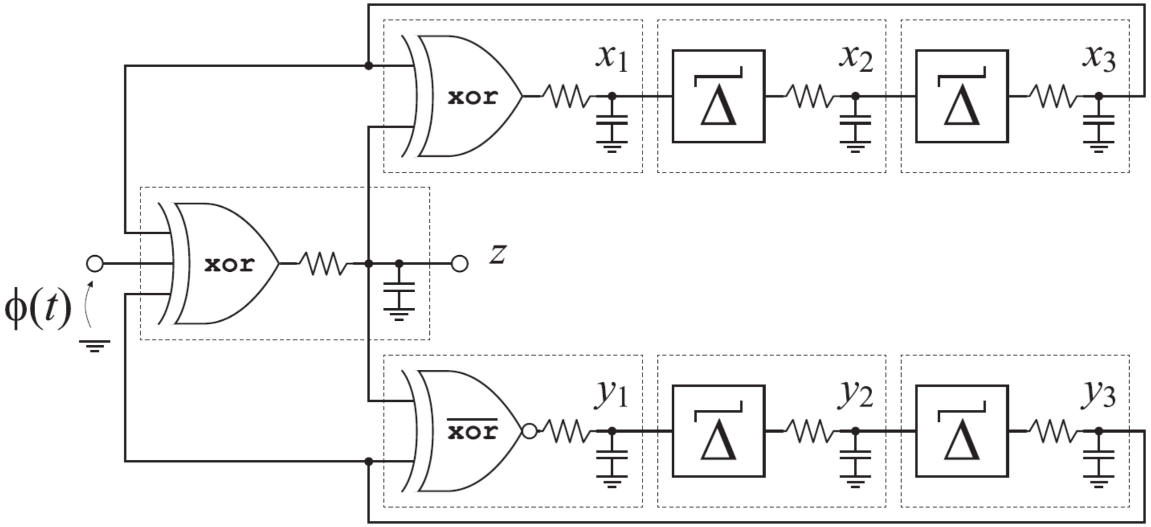
Autonomous Nonlinear Periodic Oscillator, if ϕ = 0V

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

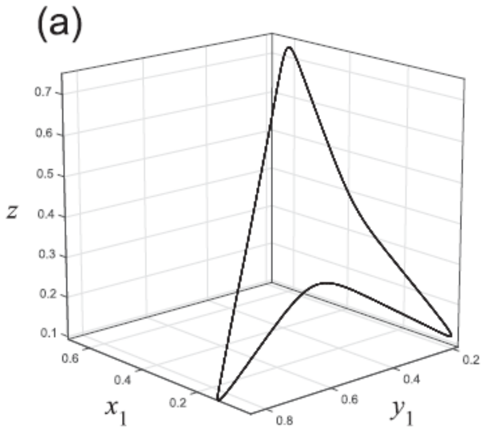
Prof. Tommaso Addabbo

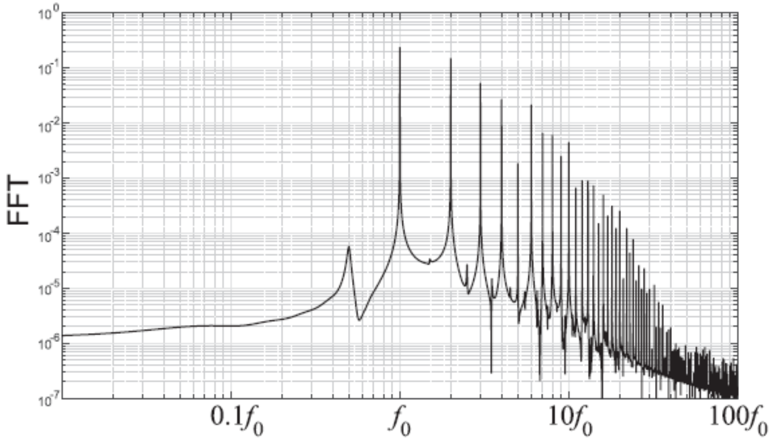
Low-Dimension Theoretical Models

By varying the frequency f_0 of the periodic excitation $\phi(t)$, period doubling cascades and routes to chaos were clearly detected.



$Q = 1/f_0RC = 18.43$





IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

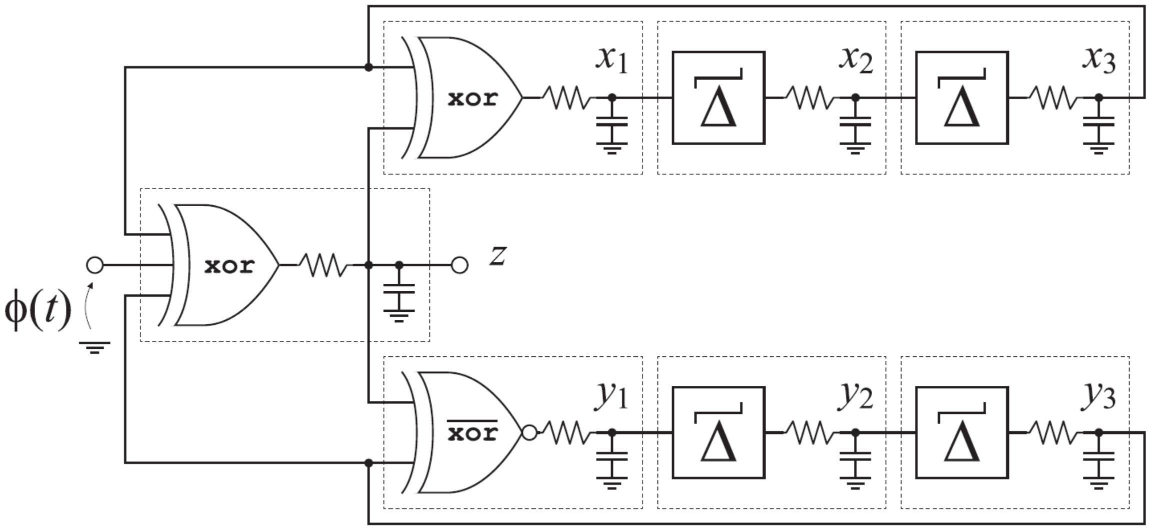
CAS

UNIVERSITÀ DI SIENA 1240

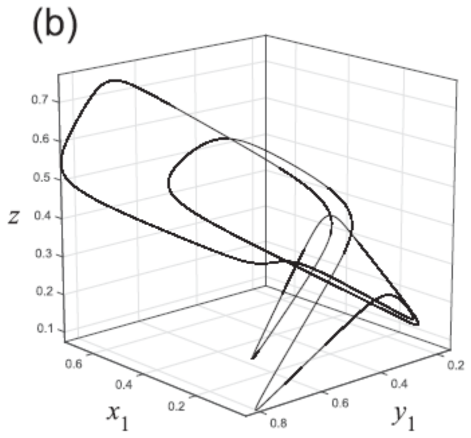
Prof. Tommaso Addabbo

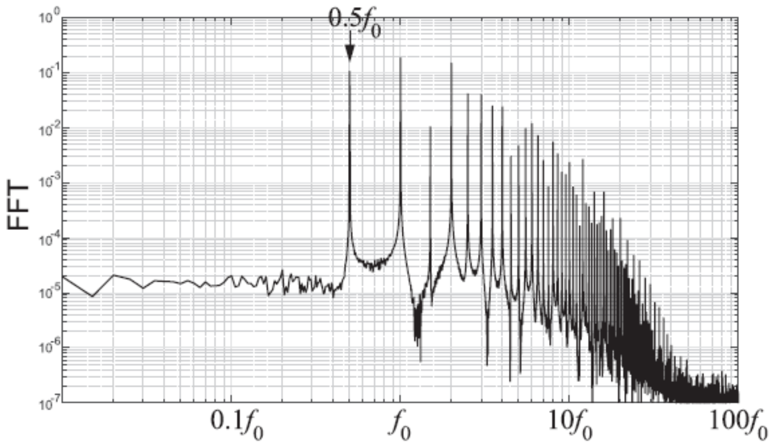
Low-Dimension Theoretical Models

By varying the frequency f_0 of the periodic excitation $\phi(t)$, period doubling cascades and routes to chaos were clearly detected.



$$Q = 1/f_0RC = 19.42$$





IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

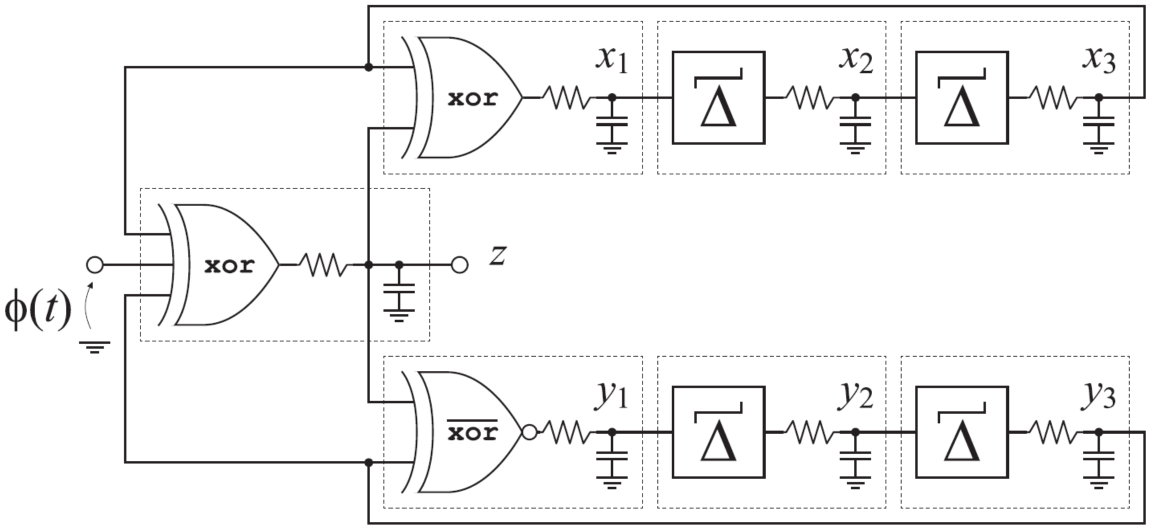
CAS

UNIVERSITÀ DI SIENA 1240

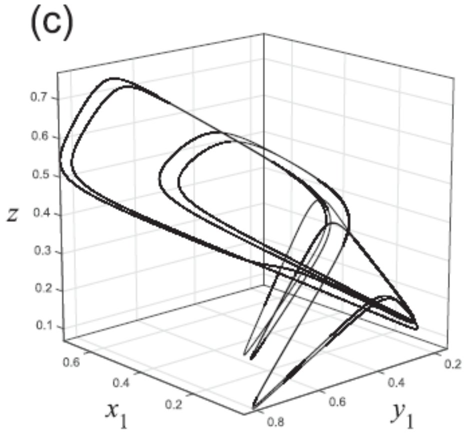
Prof. Tommaso Addabbo

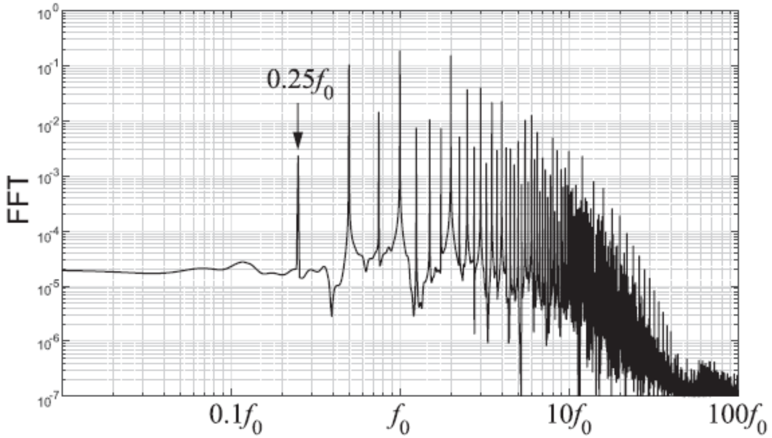
Low-Dimension Theoretical Models

By varying the frequency f_0 of the periodic excitation $\phi(t)$, period doubling cascades and routes to chaos were clearly detected.



$$Q = 1/f_0RC = 19.58$$



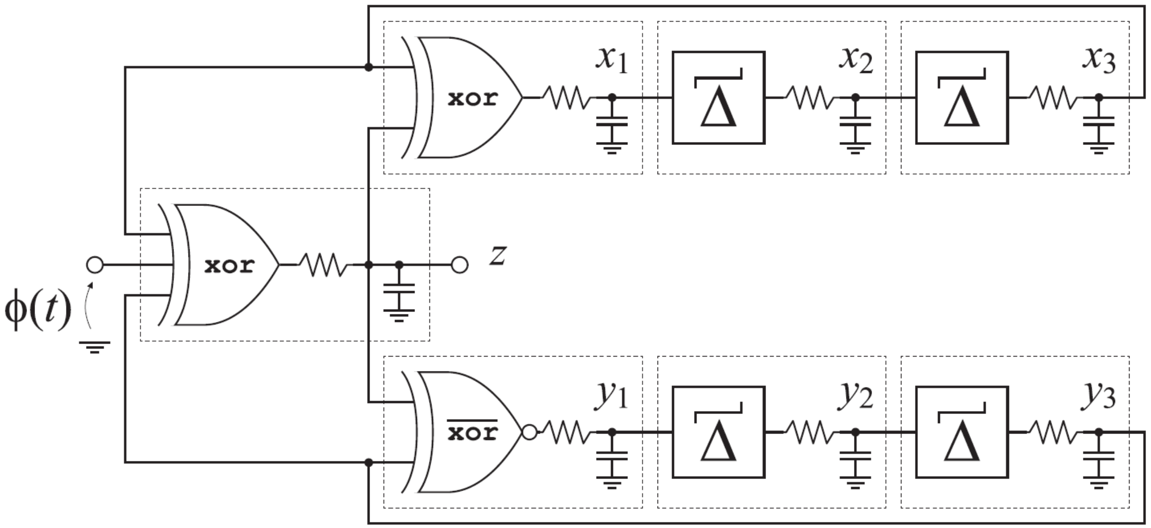


2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

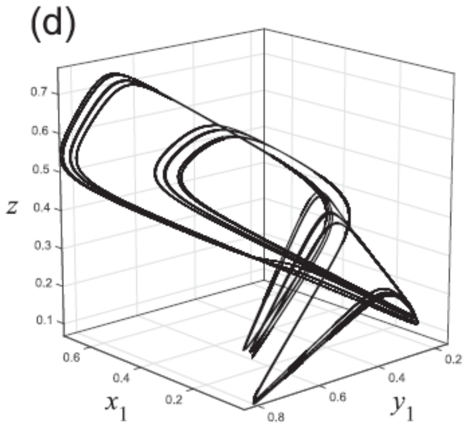
Prof. Tommaso Addabbo

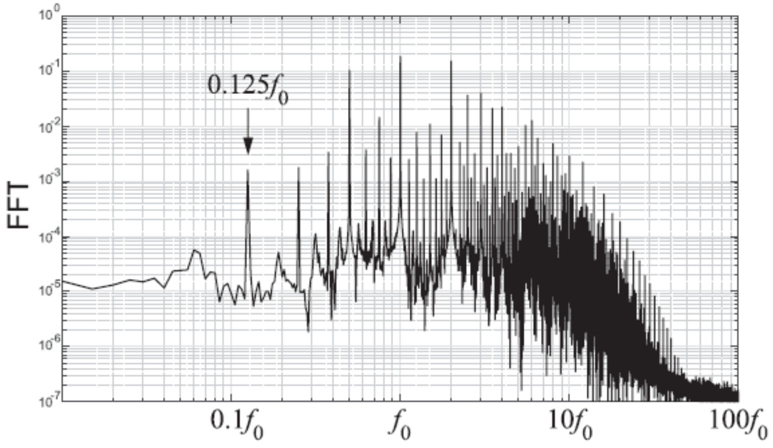
Low-Dimension Theoretical Models

By varying the frequency f_0 of the periodic excitation $\phi(t)$, period doubling cascades and routes to chaos were clearly detected.



$$Q = 1/f_0RC = 19.61$$





IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

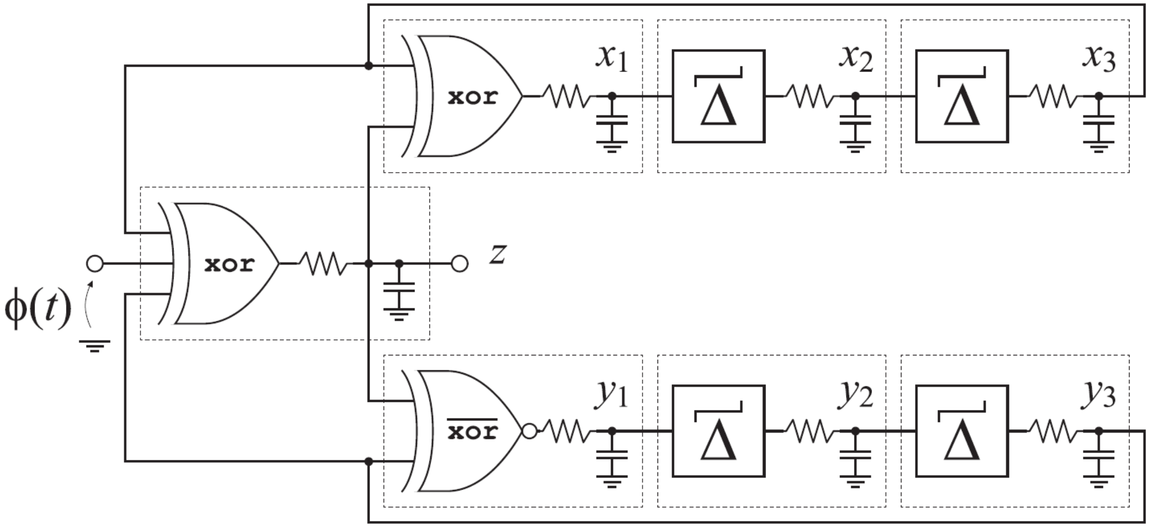
CAS

UNIVERSITÀ DI SIENA 1240

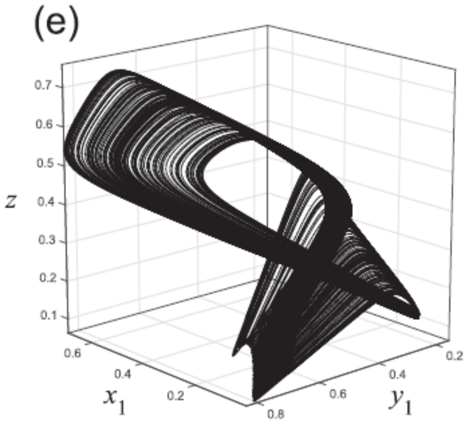
Prof. Tommaso Addabbo

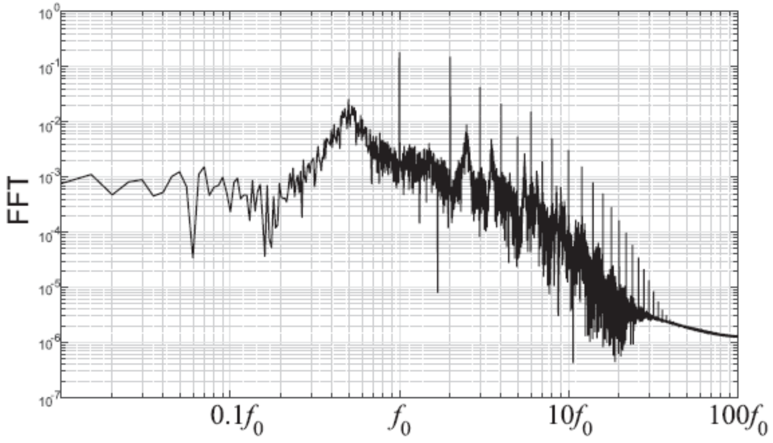
Low-Dimension Theoretical Models

By varying the frequency f_0 of the periodic excitation $\phi(t)$, period doubling cascades and routes to chaos were clearly detected.



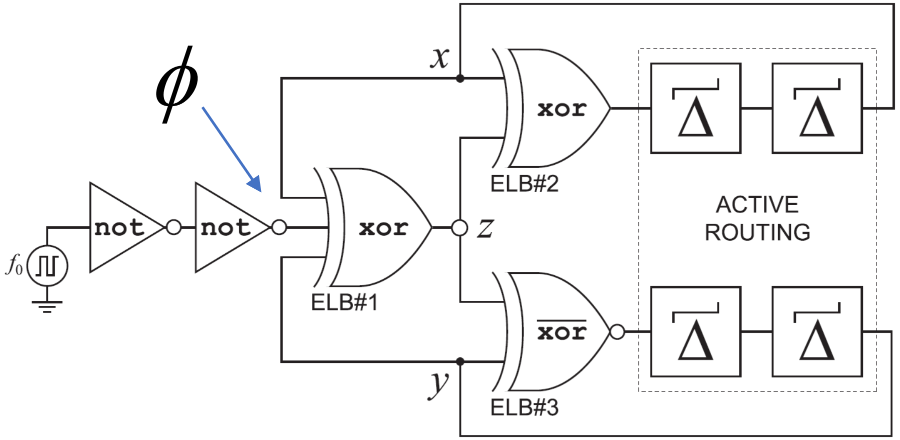
$$Q = 1/f_0RC = 19.90$$





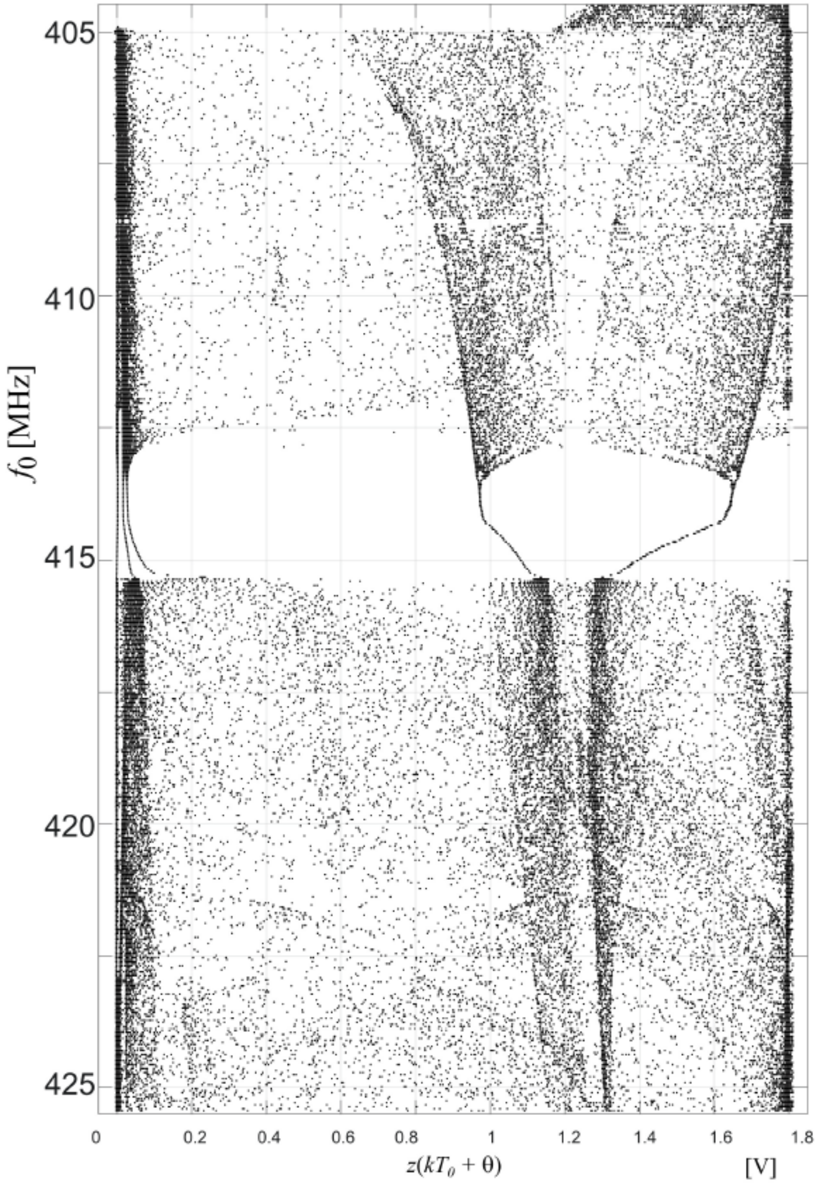
Prof. Tommaso Addabbo

Accurate CMOS Circuit Transient Simulations



Similar results were obtained resorting to exhaustive circuit simulations based on advanced CMOS transistor models. Also in this case, bifurcation diagrams showing periodic and chaotic windows were clearly detected.

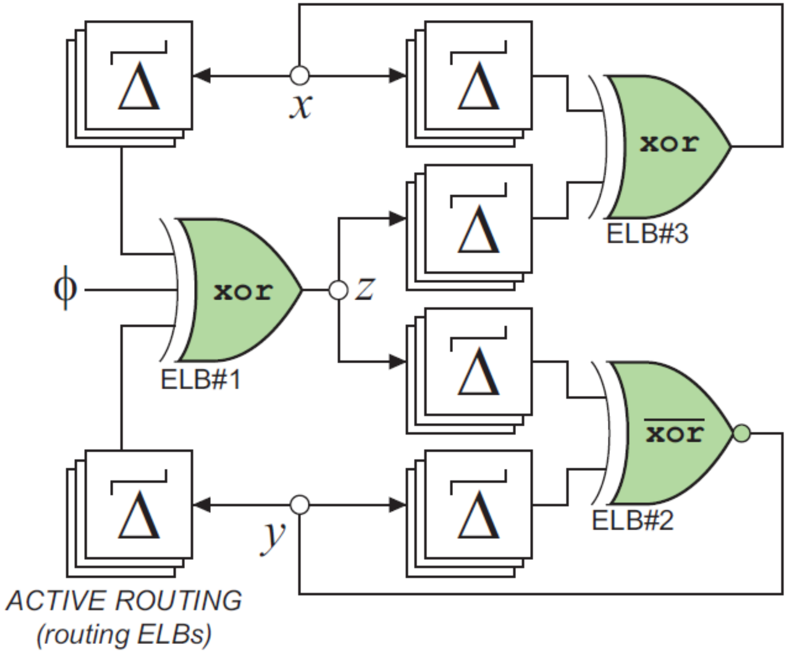
Most importantly, **chaotic windows resulted robust with respect to small circuit parametric perturbations**.



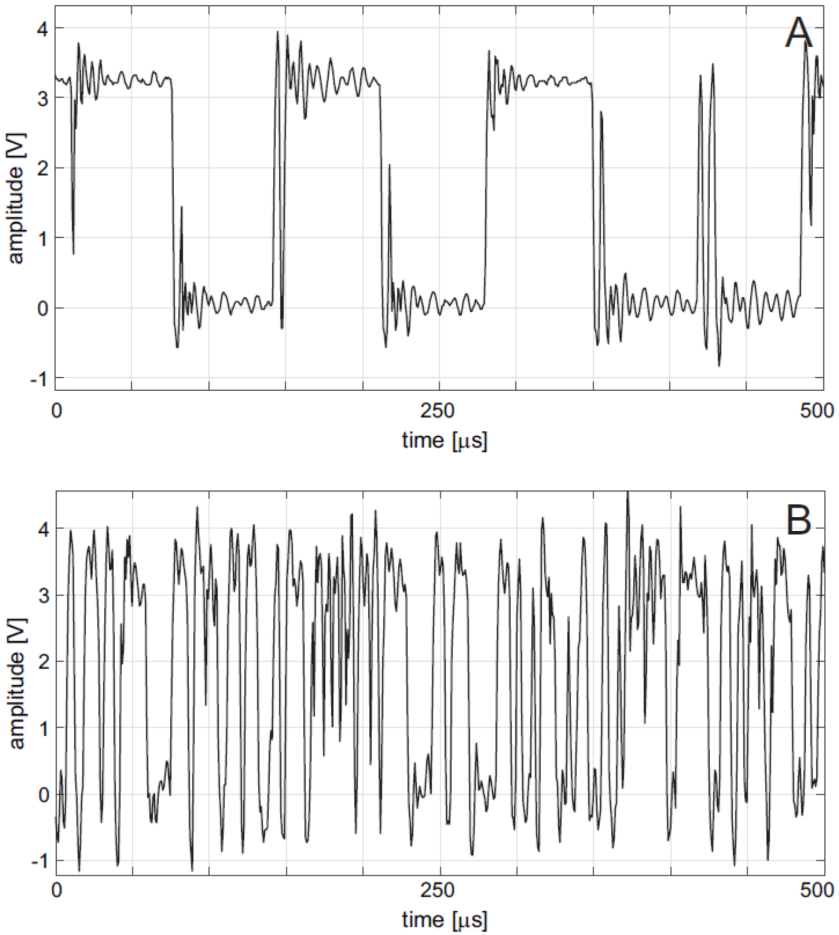
2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

Evidence of Chaos: Experimental Results



We implemented the forced nonlinear oscillator, based on the presented topology, in a Xilinx Artix 7 xc7a35 FPGAs, providing an external square-wave excitation signal ϕ (i.e., a clock signal) through a FPGA I/O pin.



Periodic excitation frequencies: 1.208MHz (A) and 1.160MHz (B)

IEEE Xplore® Digital Library

ISCAS 2020

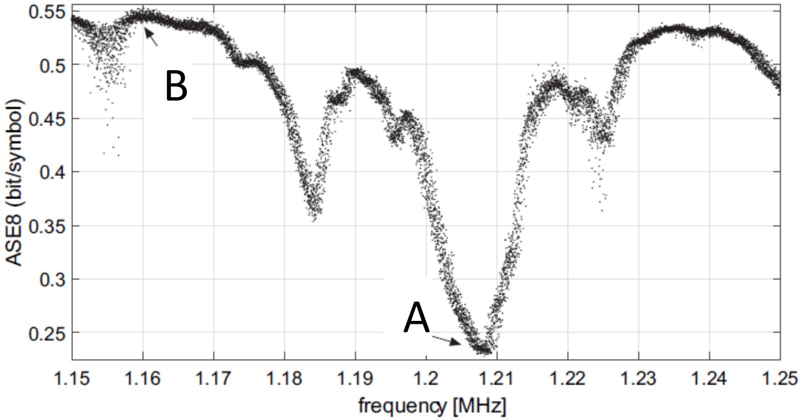
2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

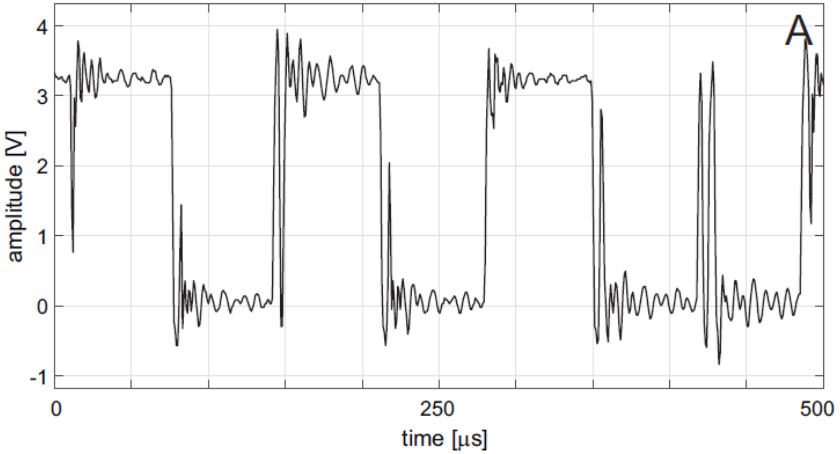
CAS

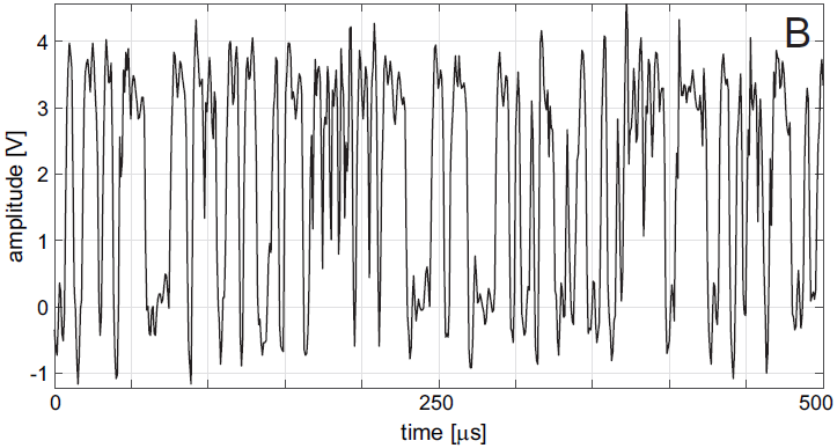
UNIVERSITÀ DI SIENA 1240

Evidence of Chaos: Experimental Results

Average Shannon Entropy







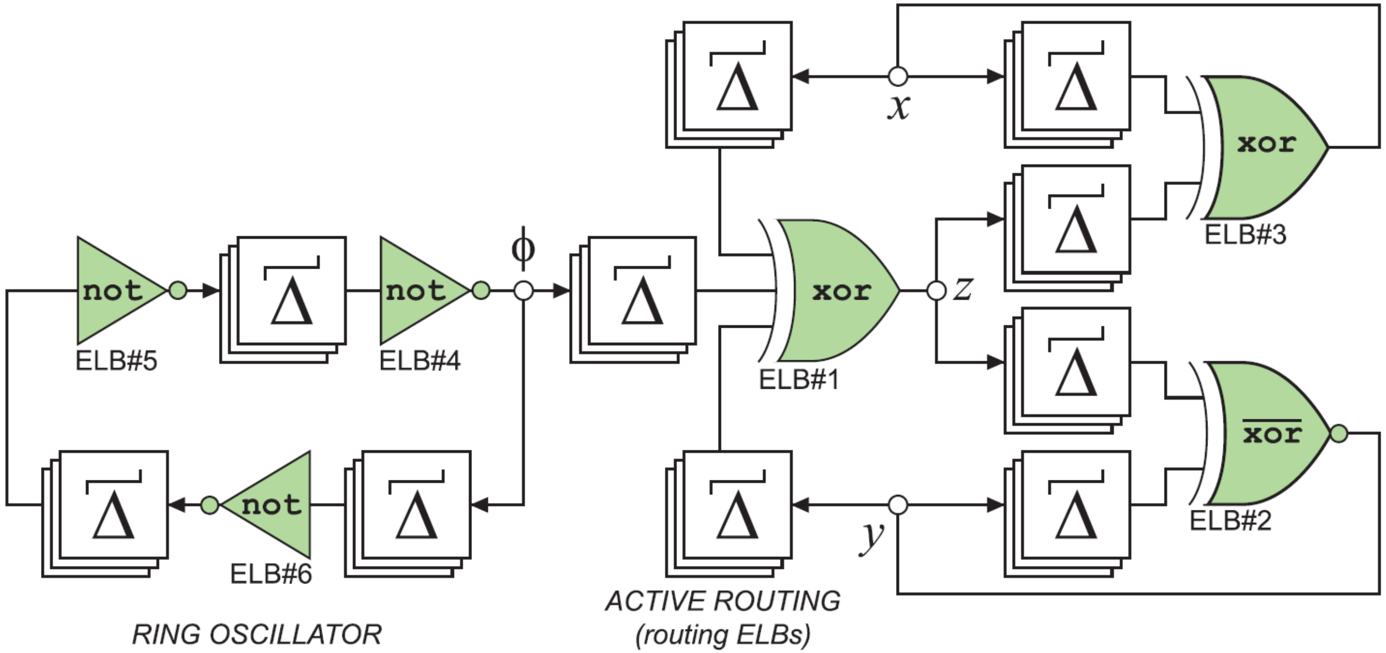
The dynamics complexity was also evaluated estimating the Average Shannon Entropy, as a function of the input excitation frequency, based on binary sequences extracted from the FPGA, revealing different regions of dynamical behavior, as suggested by the investigated models.

Periodic excitation frequencies: 1.208MHz (A) and 1.160MHz (B)

Prof. Tommaso Addabbo

A Novel Chaotic DNO Topology in PLDs

The final circuit was obtained substituting the external excitation source with a ring oscillator, obtaining an autonomous dynamical system.



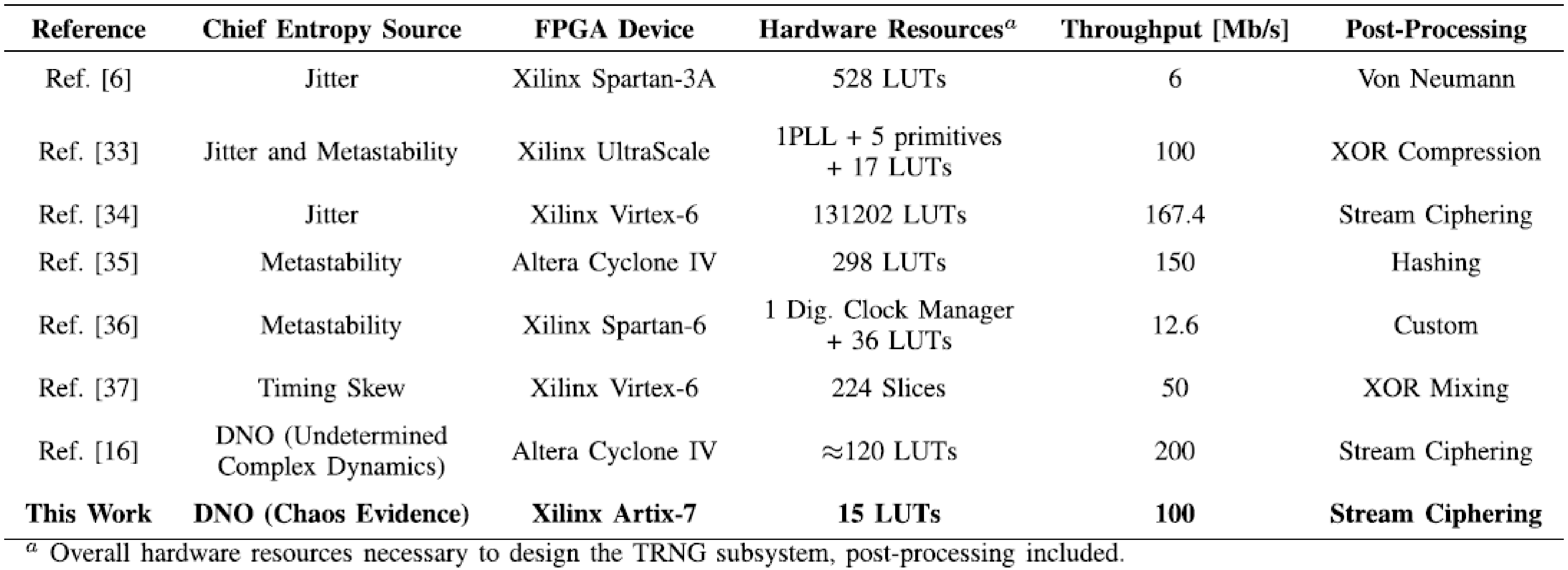
Experiments have been performed designing the proposed DNO in six Xilinx Artix 7 FPGA chips. To assess the impact of intra-device variability on the circuit performance, in each chip 16 DNO copies were designed in different chip areas, reaching a total of 96 DNO instances.

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

14

Prof. Tommaso Addabbo

A TRNG based on ‘Fully Digital’ Chaos



Reference	Chief Entropy Source	FPGA Device	Hardware Resources[a]	Throughput [Mb/s]	Post-Processing
Ref. [6]	Jitter	Xilinx Spartan-3A	528 LUTs	6	Von Neumann
Ref. [33]	Jitter and Metastability	Xilinx UltraScale	1PLL + 5 primitives + 17 LUTs	100	XOR Compression
Ref. [34]	Jitter	Xilinx Virtex-6	131202 LUTs	167.4	Stream Ciphering
Ref. [35]	Metastability	Altera Cyclone IV	298 LUTs	150	Hashing
Ref. [36]	Metastability	Xilinx Spartan-6	1 Dig. Clock Manager + 36 LUTs	12.6	Custom
Ref. [37]	Timing Skew	Xilinx Virtex-6	224 Slices	50	XOR Mixing
Ref. [16]	DNO (Undetermined Complex Dynamics)	Altera Cyclone IV	≈120 LUTs	200	Stream Ciphering
This Work	**DNO (Chaos Evidence)**	**Xilinx Artix-7**	**15 LUTs**	**100**	**Stream Ciphering**

[a] Overall hardware resources necessary to design the TRNG subsystem, post-processing included.

The designed TRNG, based on the proposed DNO required only 15 LUTs in a FPGA (including post-processing!), providing an **outstanding throughput of 6.66 Mbit/s per LUT**.

The result is justified by the simplicity of the topology, enhancing the dynamical speed of the resulting nonlinear dynamical system, that **the design set to operate in structurally stable chaotic regions in any tested case**.

The generated random sequences were **exhaustively tested statistically, and passed the NIST 800.22 standard for cryptographic applications**.

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Prof. Tommaso Addabbo

IEEE Xplore® Digital Library

ISCAS 2020

2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

CAS

UNIVERSITÀ DI SIENA 1240

Prof. Tommaso Addabbo

Conclusion

We have proposed a novel class of Digital Nonlinear Oscillators (DNOs) **supporting complex dynamics, including chaos, suitable for the definition of high-performance and low-complexity entropy sources** in Programmable Logic Devices (PLDs).

The study led the authors to the design of a **fully digital True Random Number Generator consuming only two slices of a Xilinx FPGA, including post-processing**, passing the NIST standard tests for randomness in any case experimentally tested by the authors (6 chips, 96 generators, different environmental temperatures).

The solution has been compared with others published in the literature, confirming the validity of the proposal.