A Survey of AIS-20/31 Compliant TRNG Cores Suitable for FPGA Devices

Oto PEŤURA, Ugo MUREDDU, Nathalie BOCHARD, Viktor FISCHER, Lilian BOSSUET

Univ Lyon, UJM-Saint-Etienne, CNRS
Laboratoire Hubert Curien UMR 5516
F-42023, SAINT-ETIENNE, France

oto.petura@univ-st-etienne.fr

FPL 2016, Lausanne, Switzerland, August 2016

HECTOR

LABORATOIRE HUBERT CURIEN

Outline

LABORATOIRE HUBERT CURIEN

Goals of the TRNG evaluation

Fair comparison of different TRNG principles in terms of:

- feasibility and reproducibility
- area (cost)
- speed (bitrate)
- power consumption
- entropy

LABORATOIRE HUBERT CURIEN

Selected TRNG principles

Based on the selection criteria:

- AIS-31 compliance
- Feasibility in FPGAs

The next TRNGs were selected and implemented:

- Elementary oscillator based TRNG (ELO-TRNG)
- Coherent sampling oscillator based TRNG (COSO-TRNG)
- Multiple ring oscillator based TRNG (MURO-TRNG)
- Phase locked loop based TRNG (PLL-TRNG)
- Transient effect ring oscillator based TRNG (TERO-TRNG)
- Self timed ring based TRNG (STR-TRNG)

LABORATOIRE HUBERT CURIEN

Outline

LABORATOIRE HUBERT CURIEN

Methodology to achieve a fair comparison

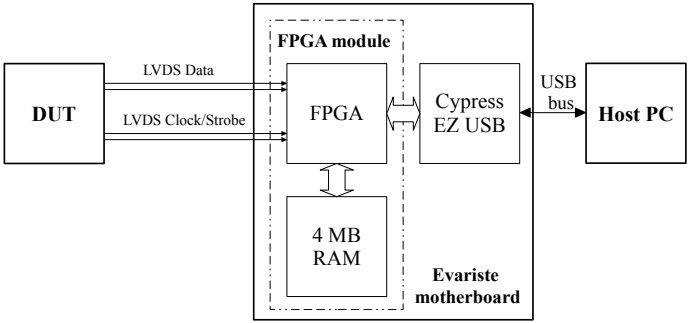
- Unified external interface
  (as simple as possible)
- Reduced complexity of the design
  (just the TRNG core, no post-processing)
- All designs implemented in all the devices
  (Xilinx Spartan 6 FPGA, Altera Cyclone V FPGA, Microsemi SmartFusion2 FPGA)
- Statistical properties (entropy) evaluated using the procedure B of the AIS-20/31 statistical test suite

LABORATOIRE HUBERT CURIEN

Hardware configuration

DUT

- FPGA module with the RNG core
- Simple serial data interface
- Two LVDS lines (data, clock/strobe)



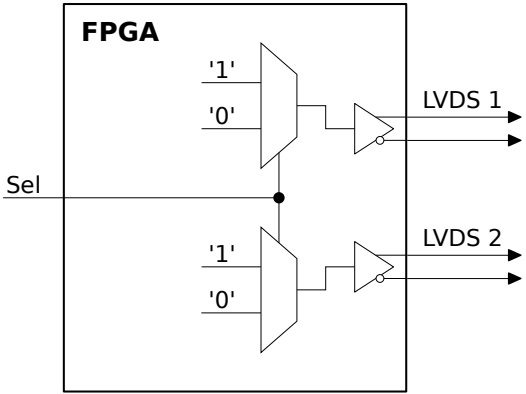
Acquisition card

- Evariste motherboard and Cyclone III FPGA module
- Can store up to 4 MB of continuous data at 0 – 400 Mbits/s

LABORATOIRE HUBERT CURIEN

Power consumption measurement strategy

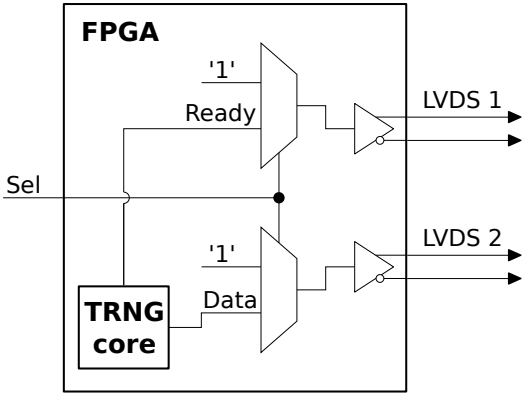
A reference design is used to measure the power consumption of an FPGA with no logic inside (about 4 mW)



Power consumption measurement strategy

The power consumption of the TRNG core is computed by subtracting the consumption of the ‘empty’ project from the total power consumption

The multiplexers are used to eliminate an impact of output drivers on the power consumption measurement.



Evaluated parameters

- Area
  in terms of LUTs and registers
- Net power consumption
- Output bit rate
- Entropy
  evaluated using test T8 of the AIS-20/31 test suite

Newly defined parameters:

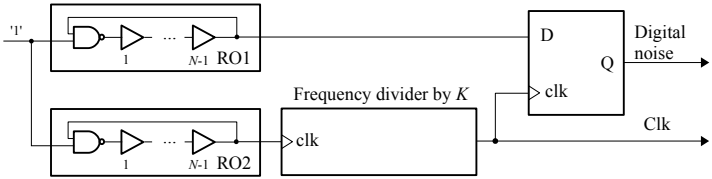
- Energy efficiency
  number of bits generated consuming one μWs of energy
- Entropy & bit rate product
  bit rate with full entropy

LABORATOIRE HUBERT CURIEN

Outline

LABORATOIRE HUBERT CURIEN

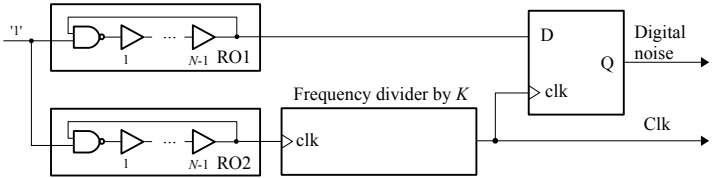
ERO-TRNG core [1]



Family	N	K [$\cdot 10^3$]	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	3	80	46/19	2.16	0.0042	0.999
Cyclone V	5	135	34/20	3.24	0.0027	0.990
SmartFusion 2	5	20	45/19	4	0.014	0.980

[1] M. Baudet, D. Lubicz, J. Micolond, and A. Tassiaux, "On the security of oscillator-based random number generators," Journal of Cryotology, vol. 24, no. 2, pp. 398–425, 2011.

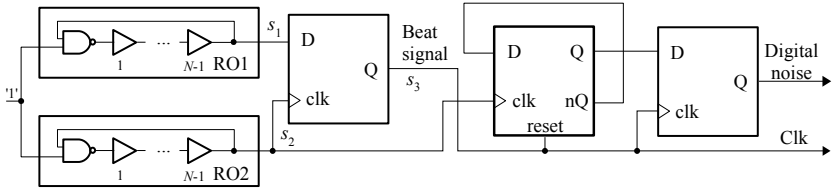
ERO-TRNG core



Observations:

- Easy to implement – no placement or routing constraints needed
- Very good reproducibility
- Based on the jitter size, the K value might be very high, the size of the counter ($\leq$ 20 bits) can affect scalability

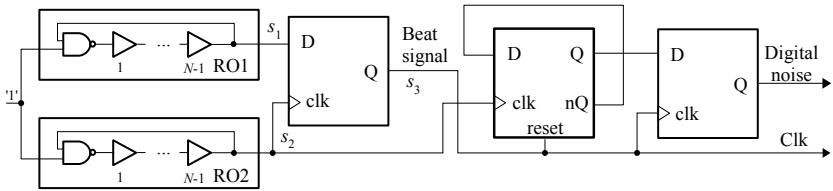
COSO-TRNG core [1]



Family	N	RO freq. [MHz]	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	8	144.5	18/3	1.22	0.54	0.999
Cyclone V	6	315.5	13/3	0.9	1.44	0.999
SmartFusion 2	10	185.2	23/3	1.94	0.328	0.999

[1] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays. ACM, 2004, pp. 71–78.

COSO-TRNG core



Observations:

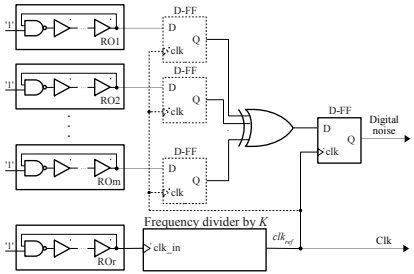
- The difference in periods has to be very small – difficult to achieve
- Disadvantage: Finding a suitable configuration requires long time (several hours) and the same configuration is not guaranteed to work on another device
- Placement and routing constraints are required

LABORATOIRE HUBERT CURIEN

MURO-TRNG core [1]

Family	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	521/131	54.72	2.57	0.999
Cyclone V	525/130	34.93	2.2	0.999
SmartFusion 2	545/130	66.41	3.62	0.999

$m = 120$
$K = 100$

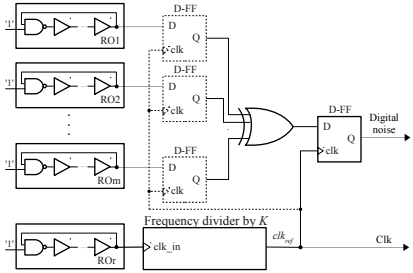


[1] B. Sunar, W. Martin, and D. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance ti Active Attacks," IEEE Transactions on Computers, pp. 109–119, 2007.

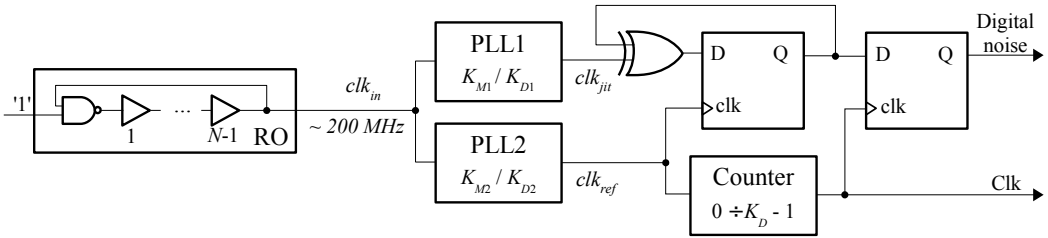
MURO-TRNG core

Observations:

- The generator requires a large number of identical rings to be implemented
- The rings might lock which is extremely hard to detect given their number
- No need of manual place and route



PLL-TRNG core [1]

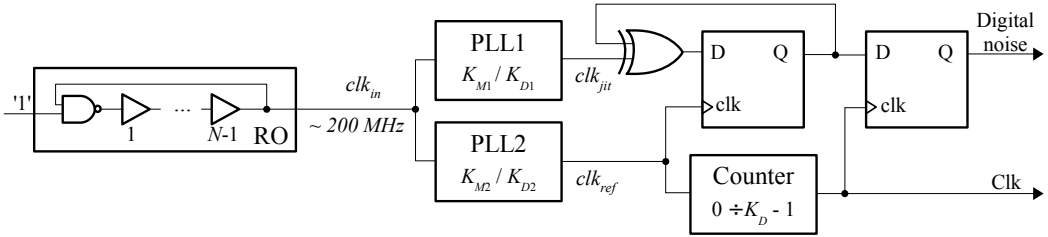


Family	clk_{jit} [MHz]	clk_{ref} [MHz]	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	435.3	485.7	34/14	10.6	0.44	0.431
Cyclone V	213.8	255.6	24/14	23	0.6	0.592
SmartFusion 2	90.4	163.6	30/15	19.7	0.37	0.340

[1] V. Fischer and M. Drutarovsky, "True random number generator embedded in reconfigurable hardware," in Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), ser. LNCS, vol. 2523, Redwood Shores, CA, USA. Springer Verlag, 2002, pp. 415–430.

LABORATOIRE HUBERT CURIEN

PLL-TRNG core

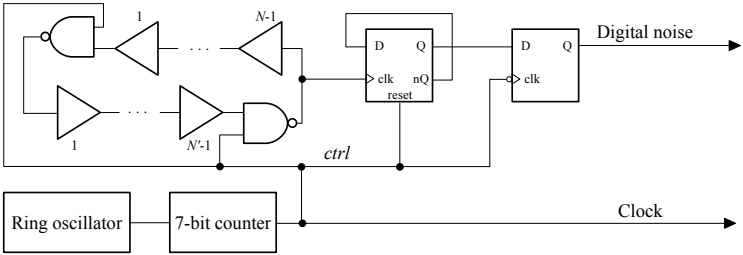


Observations:

- The PLL setup is not straightforward for some families (Spartan 6: PLL outputs go to different clock domains)
- Once the PLLs are setup, the results are reproducible within the same device family (type of the device)
- PLLs are very well isolated from the rest of the device

LABORATOIRE HUBERT CURIEN

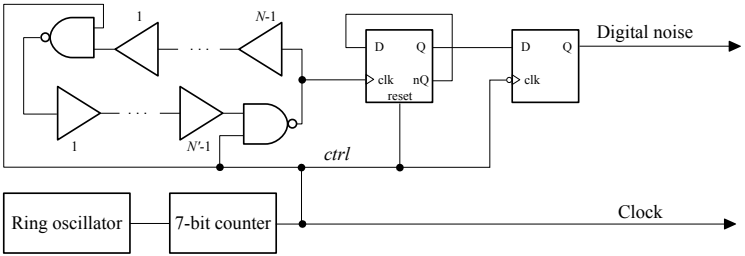
TERO-TRNG core [1]



Family	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	39/12	3.312	0.625	0.999
Cyclone V	46/12	9.36	1	0.987
SmartFusion 2	46/12	1.23	1	0.999

[1] M. Varchola and M. Drutarovsky, "New high entropy element for FPGA based true random number generators," in Cyptographic Hardware and Embedded Systems, CHES 2010. Springer, 2010, pp. 351–365.

TERO-TRNG core



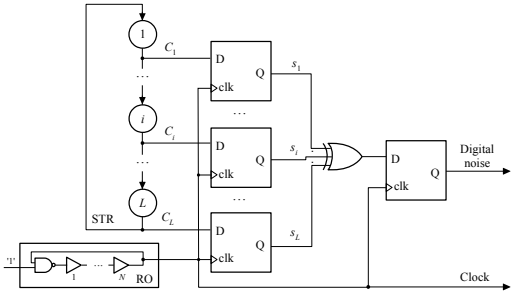
Observations:

- The placement and routing constraints must be enforced in the TERO loop design
- The two TERO branches must be well unbalanced to get between 100 and 200 oscillations
- Difficult to obtain repeatable results on different devices

STR-TRNG core [1]

Family	Area (LUT/L&R)	Power cons. [mW]	Bit rate [Mbits/s]	Entropy per bit
Spartan 6	346/256	65.9	154	0.998
Cyclone V	352/256	49.4	245	0.999
SmartFusion 2	350/256	82.52	188	0.999

$L = 255$

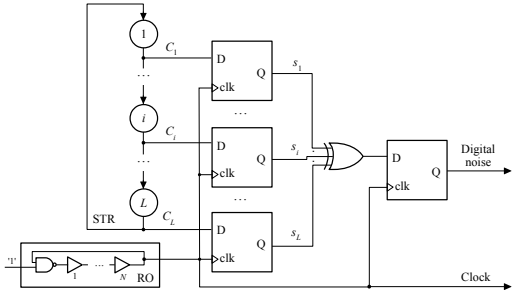


[1] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet, "A self-timed ring based true random number generator," in IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2013), 2013, pp. 99–106.

STR-TRNG core

Observations:

- The ring must have a huge number of cells
- Each cell must be initialized at the beginning and number of events must be verified continuously
- The topology is important – manual placement needed



Summary of implementation results

TRNG type	FPGA device	Area (LUT/Reg)	Power cons. [mW]	Bit rate [Mbits/s]	Efficiency [bits/μWs]	Entropy per bit	Entropy * Bit rate	Feasib. & Repeat.
ERO	Spartan 6	46/19	2.16	0.0042	1.94	0.999	0.004	**5**
	Cyclone V	34/20	3.24	0.0027	0.83	0.990	0.003	
	SmartFusion 2	45/19	4	0.014	3.5	0.980	0.013	
COSO	Spartan 6	**18/3**	**1.22**	0.54	442.6	0.999	0.539	1
	Cyclone V	**13/3**	**0.9**	1.44	**1 600**	0.999	1.438	
	SmartFusion 2	**23/3**	**1.94**	0.328	169	0.999	0.327	
MURO	Spartan 6	521/131	54.72	2.57	46.9	0.999	2.567	4
	Cyclone V	525/130	34.93	2.2	62.9	0.999	2.197	
	SmartFusion 2	545/130	66.41	3.62	54.5	0.999	3.616	
PLL	Spartan 6	34/14	10.6	0.44	41.5	0.981	0.431	3
	Cyclone V	24/14	23	0.6	43.4	0.986	0.592	
	SmartFusion 2	30/15	19.7	0.37	18.7	0.921	0.340	
TERO	Spartan 6	39/12	3.312	0.625	188.7	0.999	0.624	1
	Cyclone V	46/12	9.36	1	106.8	0.987	0.985	
	SmartFusion 2	46/12	1.23	1	813	0.999	0.999	
STR	Spartan 6	346/256	65.9	**154**	**2 343.2**	0.998	**154.121**	2
	Cyclone V	352/256	49.4	**245**	**4 959.1**	0.999	**244.755**	
	SmartFusion 2	350/256	82.52	**188**	**2 286.7**	0.999	**188.522**	

LABORATOIRE HUBERT CURIEN

Outline

Conclusions

- All the presented TRNG cores are feasible in all major FPGA families
- COSO and TERO TRNGs are impractical in their current state
  (They both require per device placement and routing)
- Each TRNG has its pros and cons
- Presented implementations are not fully optimized
  (Final optimization is a question of the target application)
- Quality of the TRNG design depends not only on the principle used
  (Hardware used and implementation itself are very important too)
- VHDL source code is available at:
  `https://labh-curien.univ-st-etienne.fr/cryptarchi/HECTOR_TRNG_designs`

LABORATOIRE HUBERT CURIEN

Acknowledgments

This work was performed in the framework of the project

HECTOR

Hardware Enabled Crypto and Randomness

The HECTOR project has received funding from the
European Union's Horizon 2020 research and innovation programme
under grant agreement number 644052 starting from March 2015

www.hector-project.eu

LABORATOIRE HUBERT CURIEN

Thank you for your attention