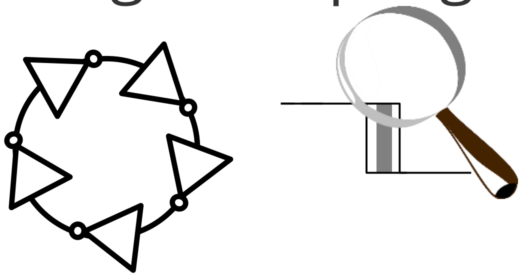
ES-TRNG

A High-throughput, Low-area True Random Number Generator based on Edge Sampling



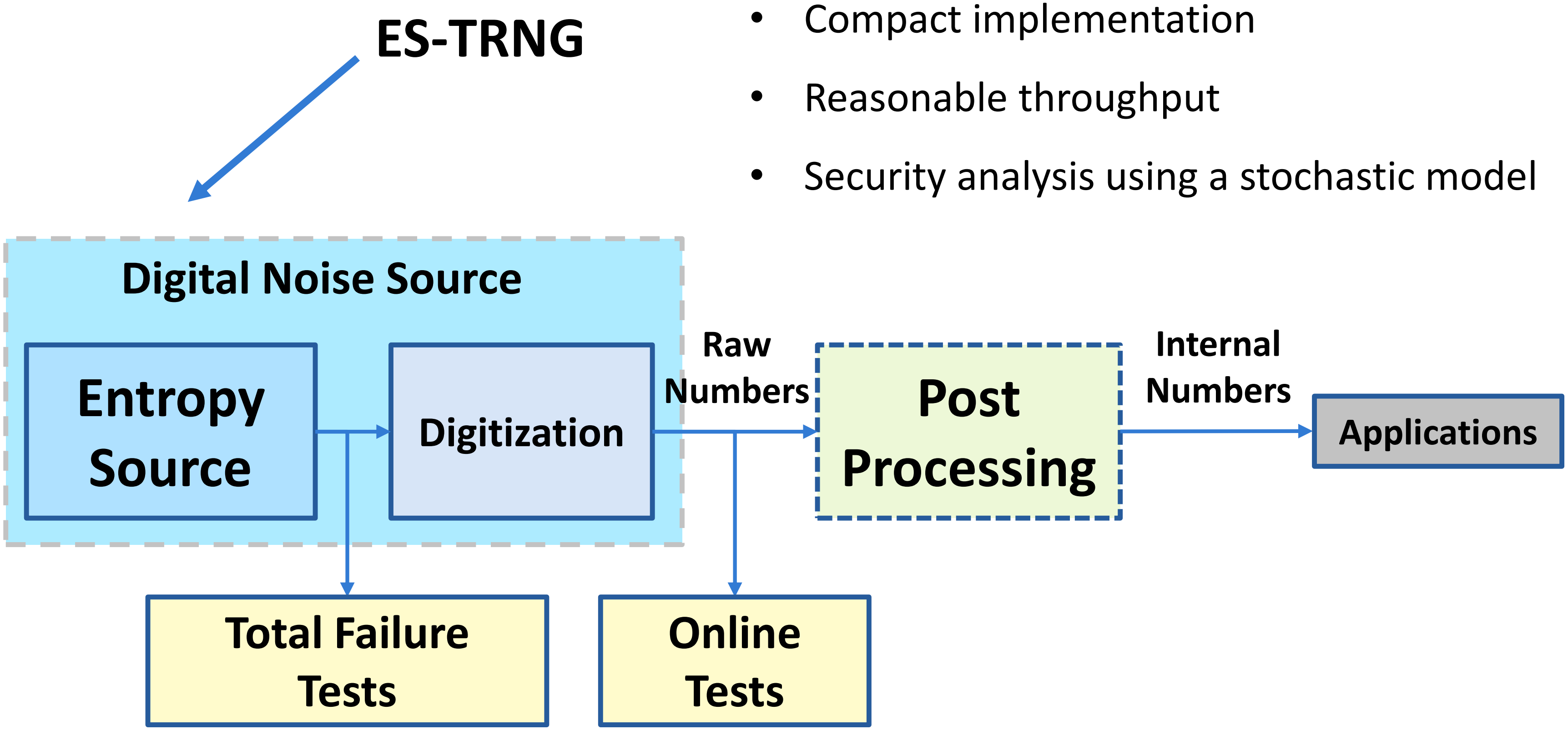
Bohan Yang, Vladimir Rožić, Miloš Grujić

Nele Mentens and Ingrid Verbauwhede

COSIC, KU Leuven

Generic TRNG Architecture

- Timing jitter based TRNG
- Compact implementation
- Reasonable throughput
- Security analysis using a stochastic model



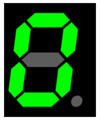
Stochastic model oriented security analysis

For Cryptographic Applications:

Initialization

Vectors

The **SECURITY** of a TRNG depends on its unpredictability.



which

NIST800-22

DIEHARD

FIPS 140-1

cannot be measured by statistical tests

can be estimated by stochastic model

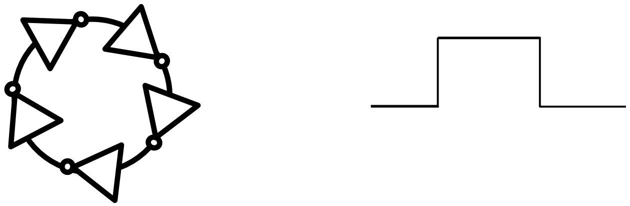
AIS-31

NIST800-90B ?

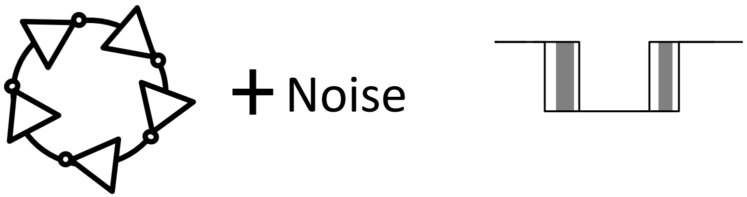
?

Timing jitter based TRNG

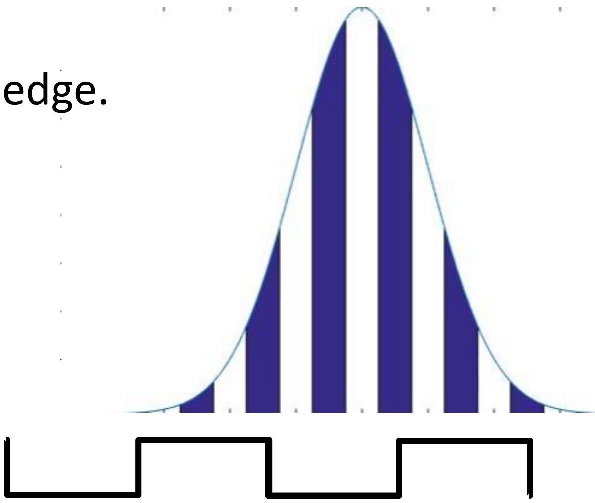
Noise Free

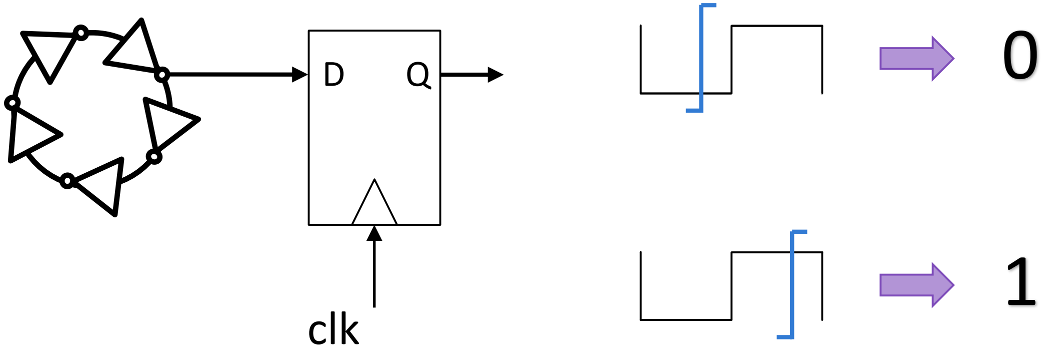


Noise Free



A random bit is generated only when measuring the position of a edge.





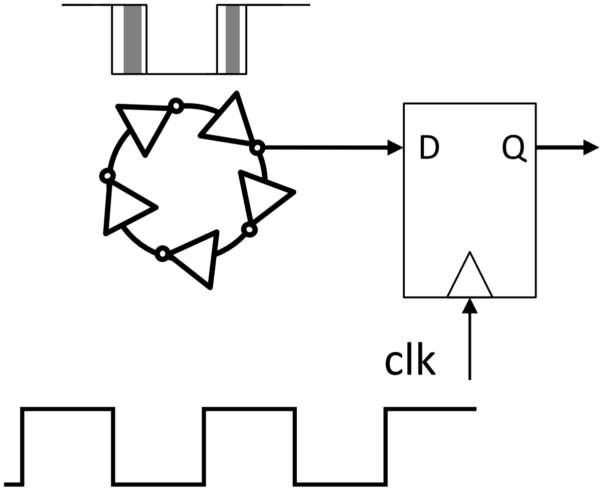
Elementary TRNG

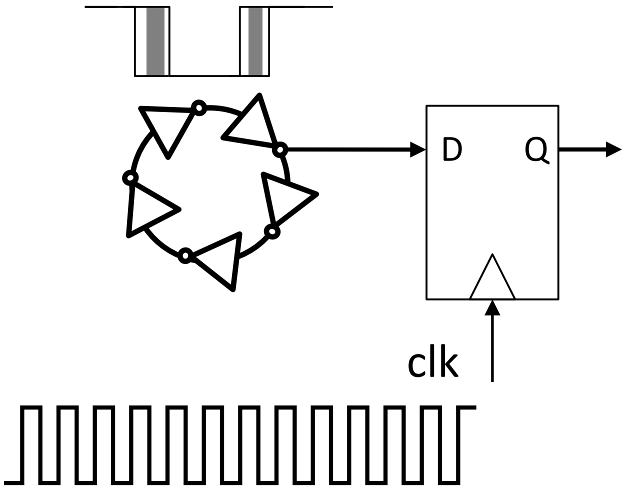
Timing Jitter accumulation is slow → Low throughput

Solution: increasing the sampling resolution!

How to increase the sampling resolution

Sampling at a higher frequency ?



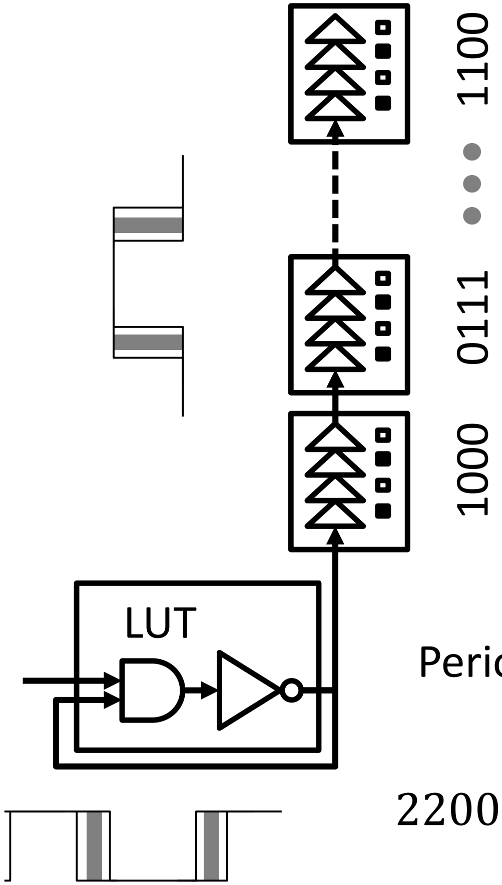


Highest sampling frequency is limited by technology, platform, system, power, energy….

How to increase the sampling resolution

Using high resolution TDC (Time-to-Digital Converter)

DC-TRNG



Resolution: ~ 17 ps

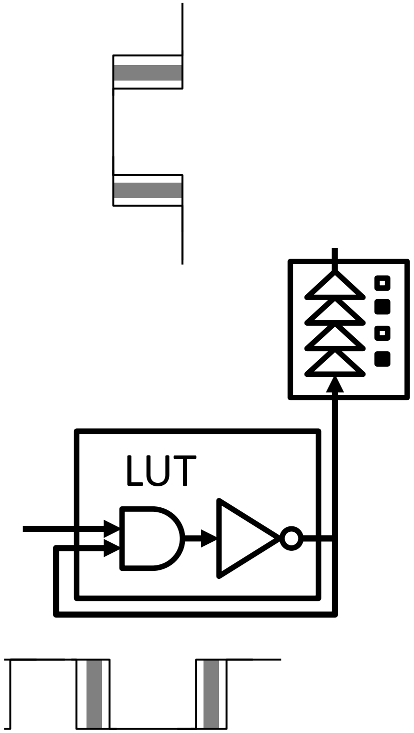
(@~60 GHz)

Period: ~ 2.2 ns

$$2200\,ps \div 2 \div 17\,ps \div 4 \approx 17$$

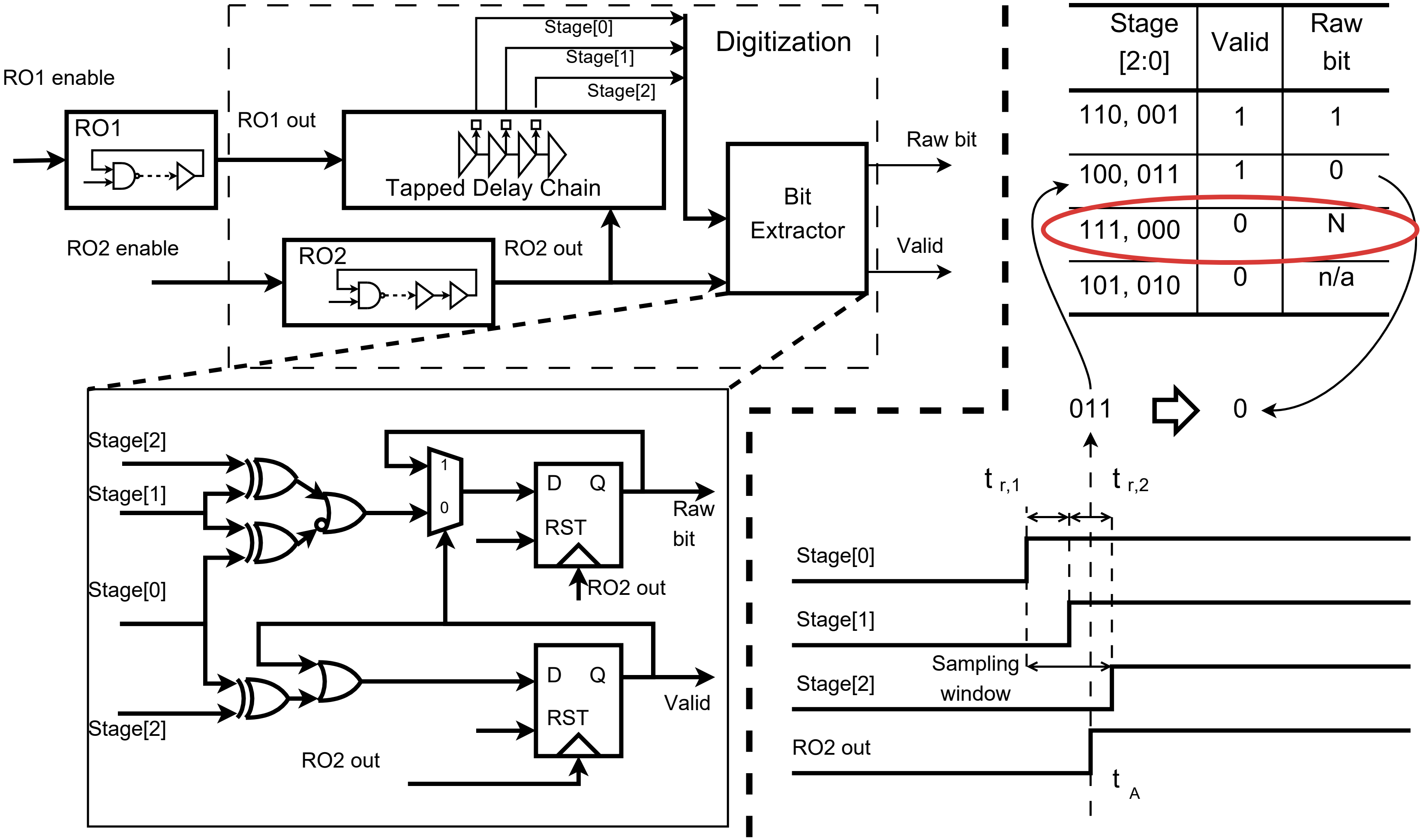
20

ES-TRNG



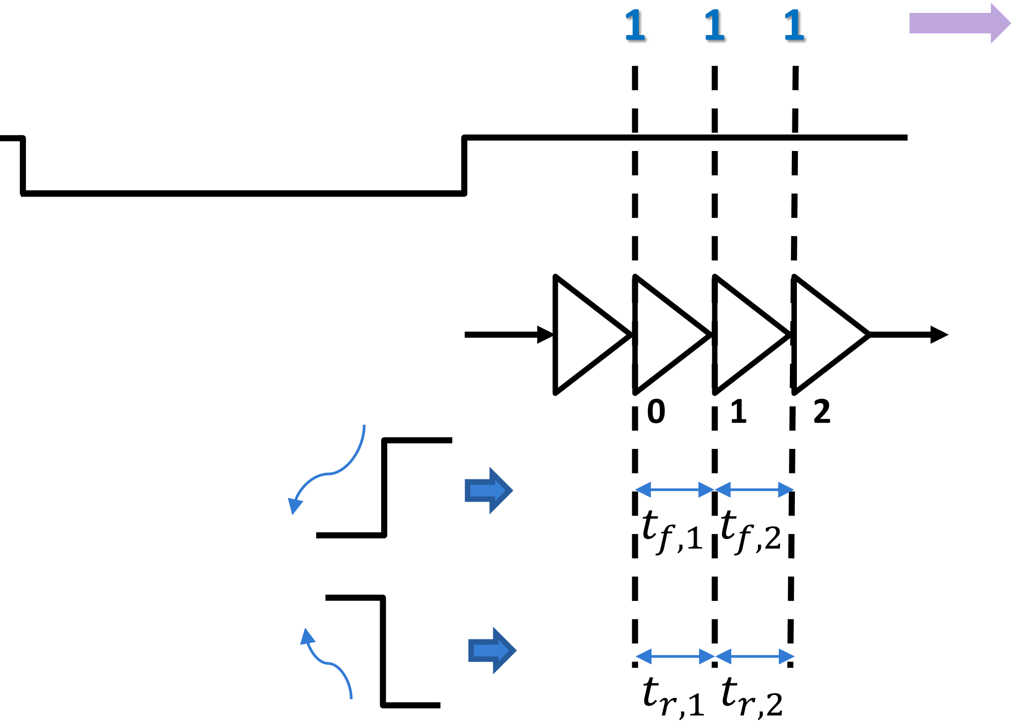
V. Rozic, B. Yang, W. Dehaene, and I. Verbauwhede, "Highly Efficient Entropy Extraction for True Random Number Generators on FPGAs," In DAC 2015

A closer look at ES-TRNG architecture



Stage [2:0]	Valid	Raw bit
110, 001	1	1
100, 011	1	0
111, 000	0	N
101, 010	0	n/a

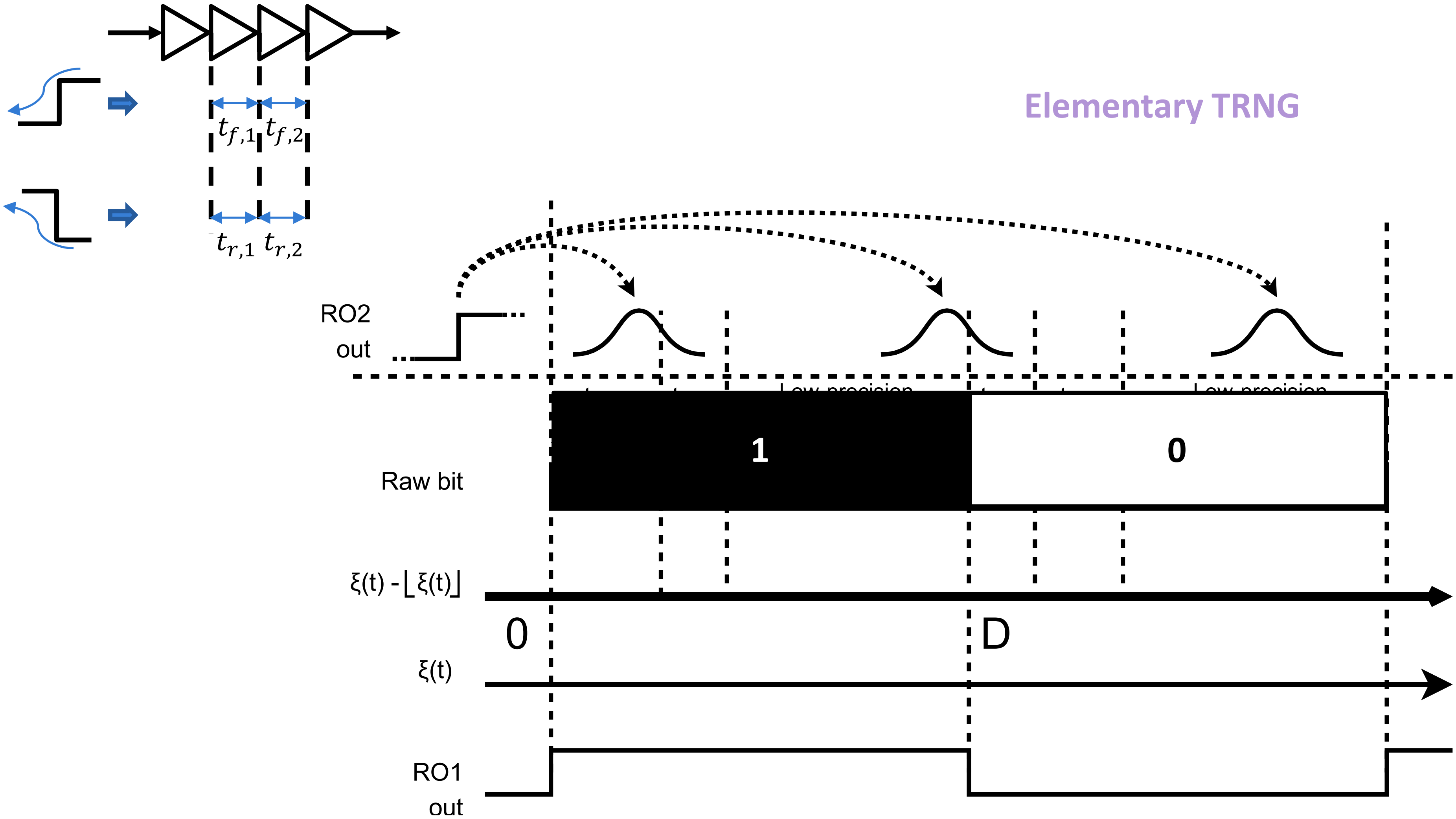
Technique 1: variable-precision phase encoding



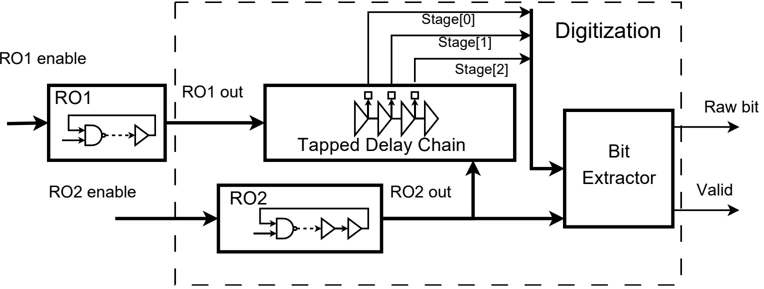
Stages [2:0]	Valid	Raw bit
110,001	1	1
100,011	1	0
111,000	0	N
101,010	0	n/a

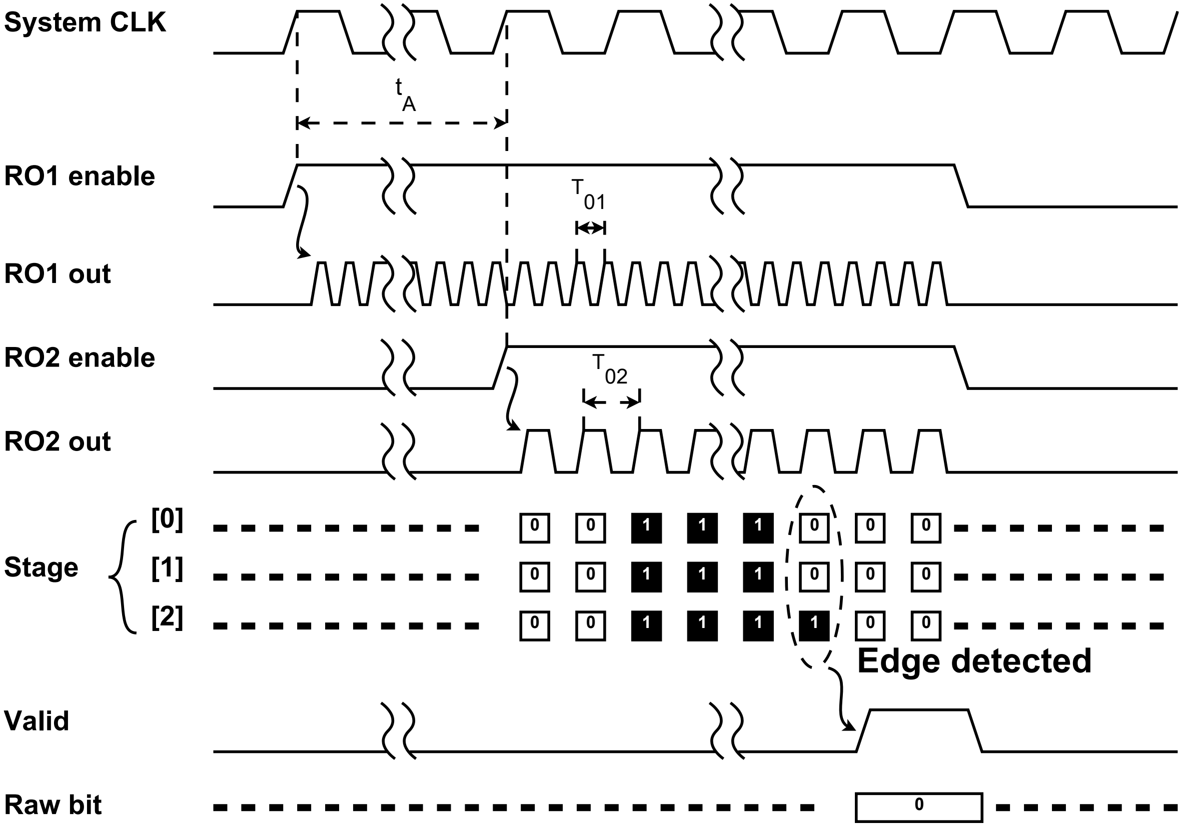
Technique 1: variable-precision phase encoding

Elementary TRNG



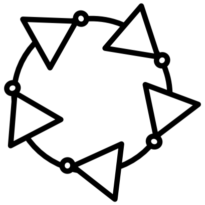
Technique 2: repetitive sampling



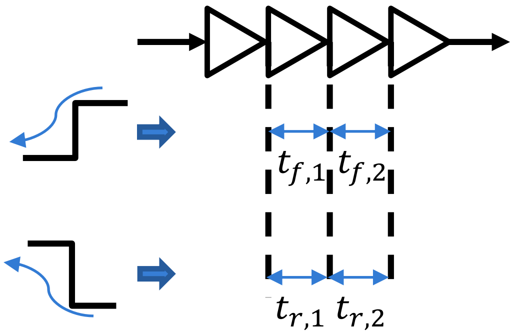


Dependency between each samples

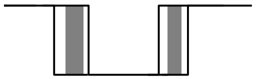
ES-TRNG: platform parameters



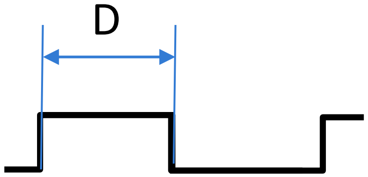
RO 1	2.172 ns	RO 2	2.740 ns



$t_{f,1}$	35.93 ps	$t_{f,2}$	40.90 ps
$t_{r,1}$	22.25 ps	$t_{r,2}$	24.12 ps

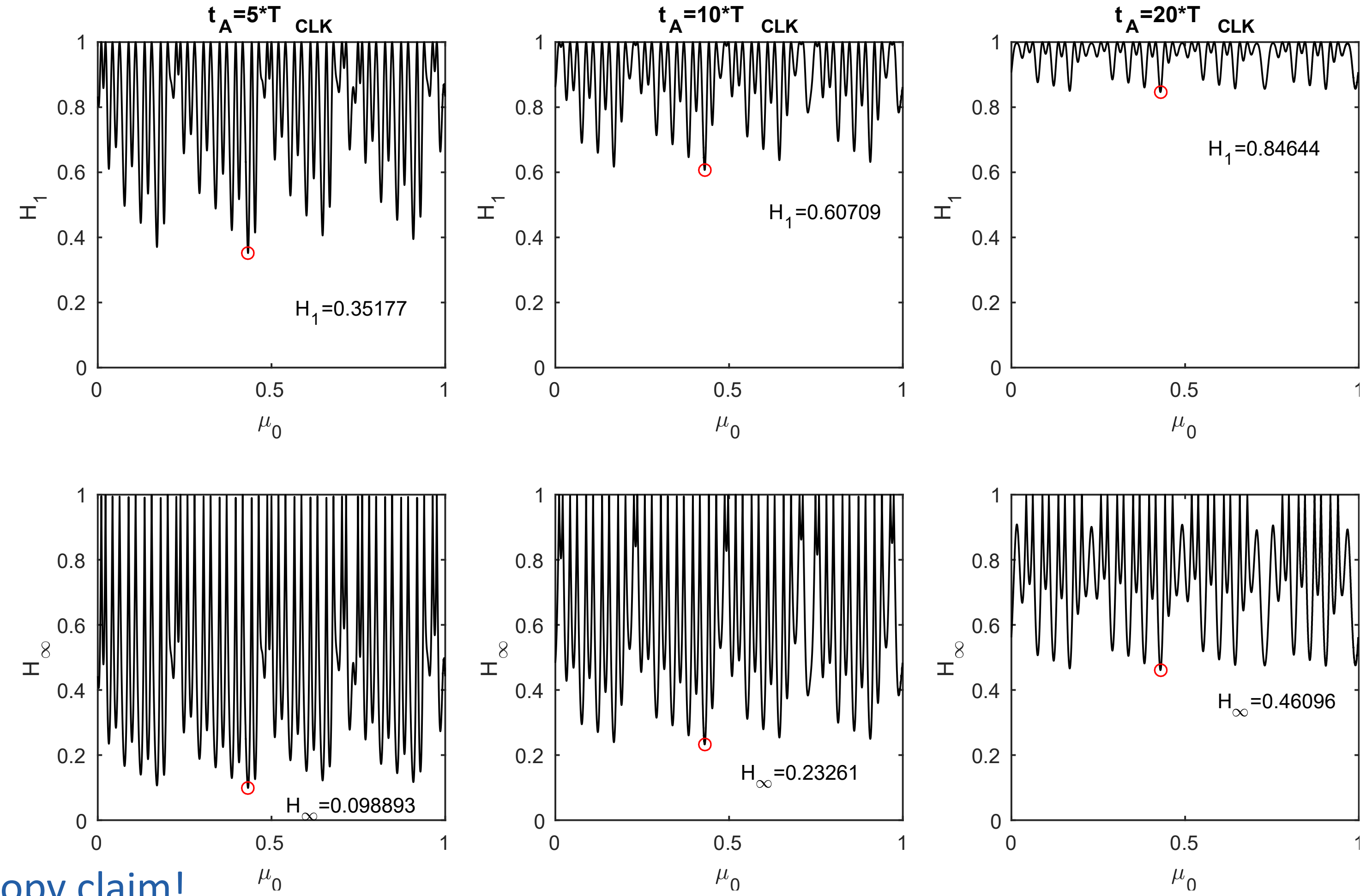


$\frac{\sigma_m^2}{t_m}$ 2.9 fs



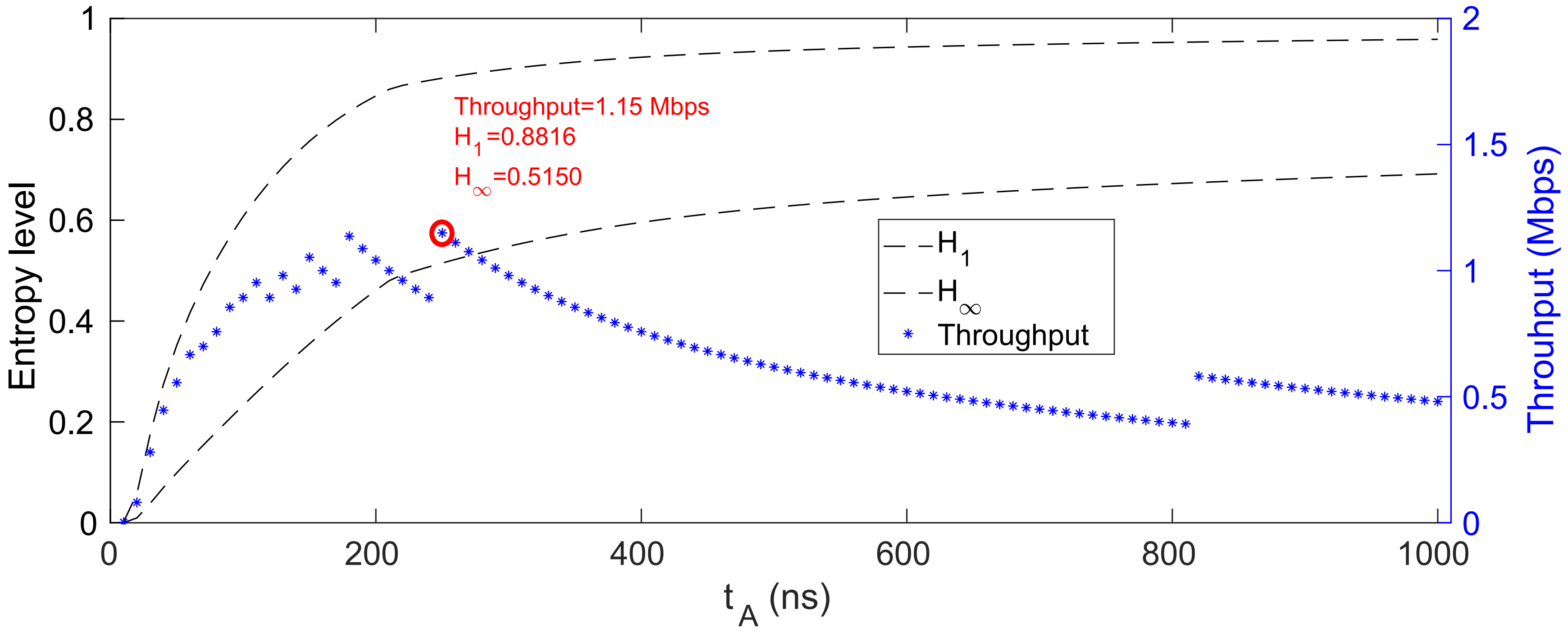
0.43

ES-TRNG: design parameters



Entropy claim!

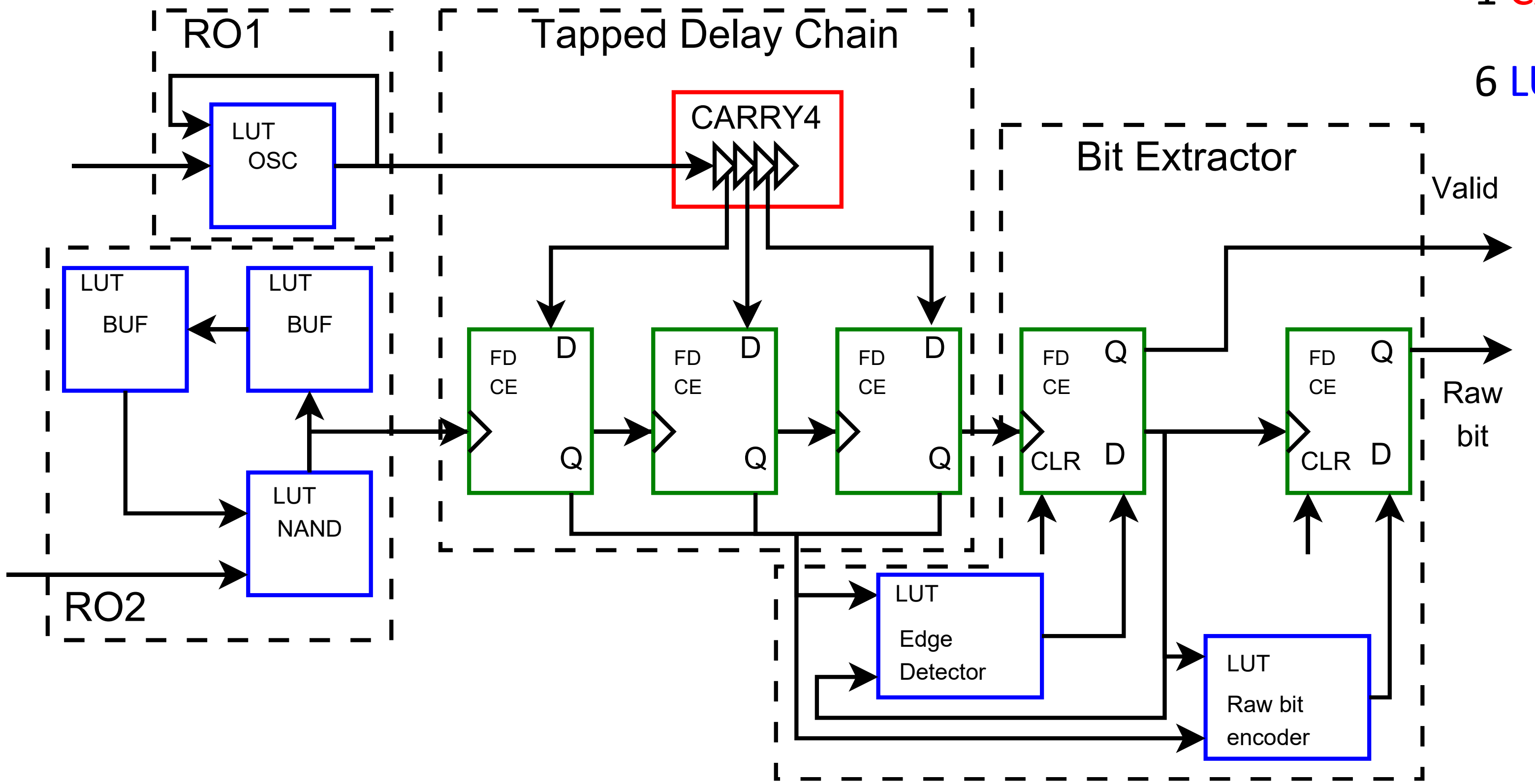
ES-TRNG: design parameters



Entropy claim!

Implementation of ES-TRNG on Xilinx FPGA

Compact!



5 DFFs

1 CARRY4

6 LUTs + 4 LUTs

Conclusion

ES-TRNG

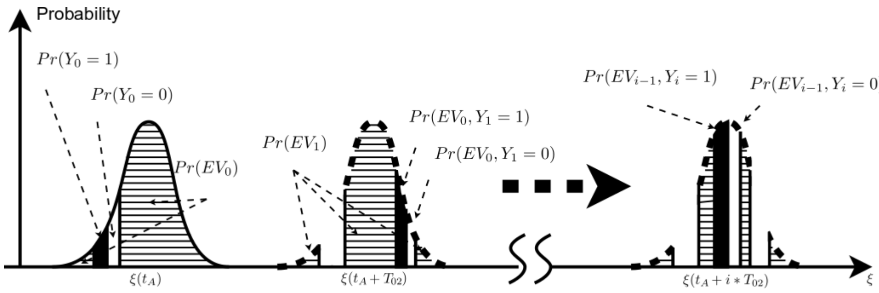
Compact Hardware: 10 LUTs + 5 FFs @ Xilinx Spartan-6

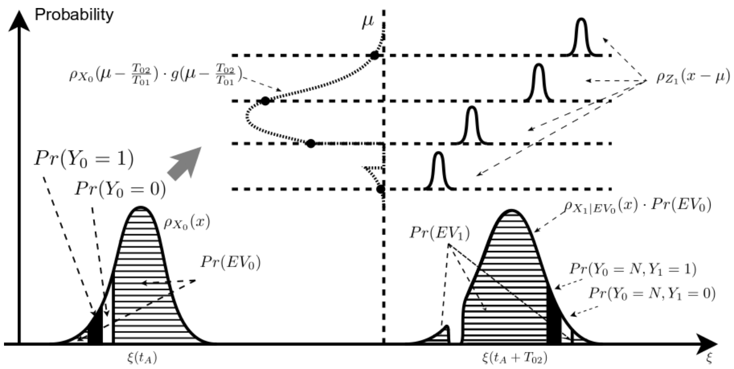
or 10 LUTs + 6 FFs @ Intel Cyclone-V

Relative High Throughput: 1.15 Mbps @ Xilinx Spartan-6

or 1.07 Mbps @ Intel Cyclone-V

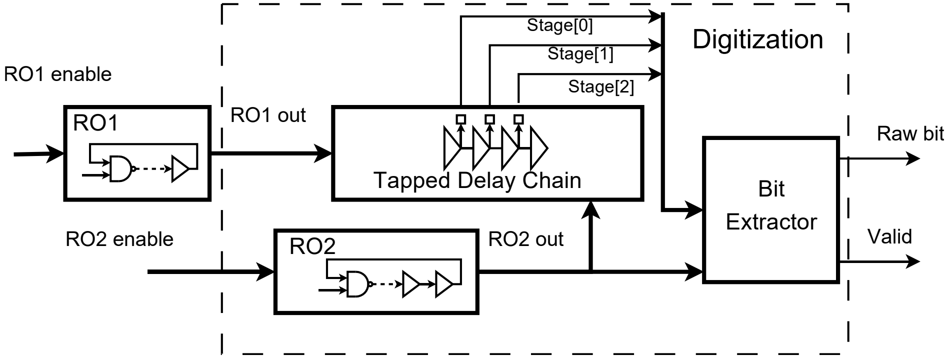
Security analysis supported by stochastic model





DC-TRNG & ES-TRNG resources (in progress):
https://github.com/ybhphoenix/DC-ES-TRNG

Q&A


RO1 enable
RO1
RO1 out
Tapped Delay Chain
Stage[0]
Stage[1]
Stage[2]
Digitization
RO2 enable
RO2
RO2 out
Bit
Extractor
Raw bit
Valid