KU LEUVEN

High Throughput TRNGs on FPGAs

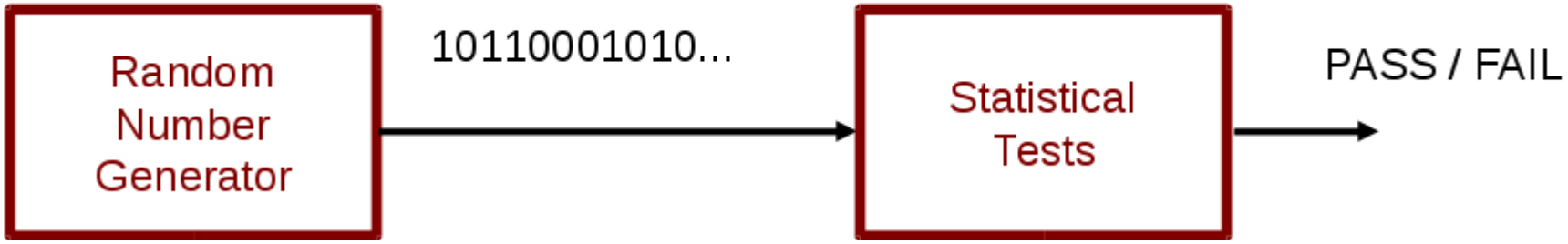
Vladimir Rožić, Bohan Yang and Ingrid Verbauwhede
ESAT-COSIC and iMinds, KU Leuven

Outline

- Design and Evaluation Requirements
- Entropy Extraction
- General Architecture
- Stochastic Model
- Platform Parameters
- Design Decisions
- Results
- Conclusions and Future Work

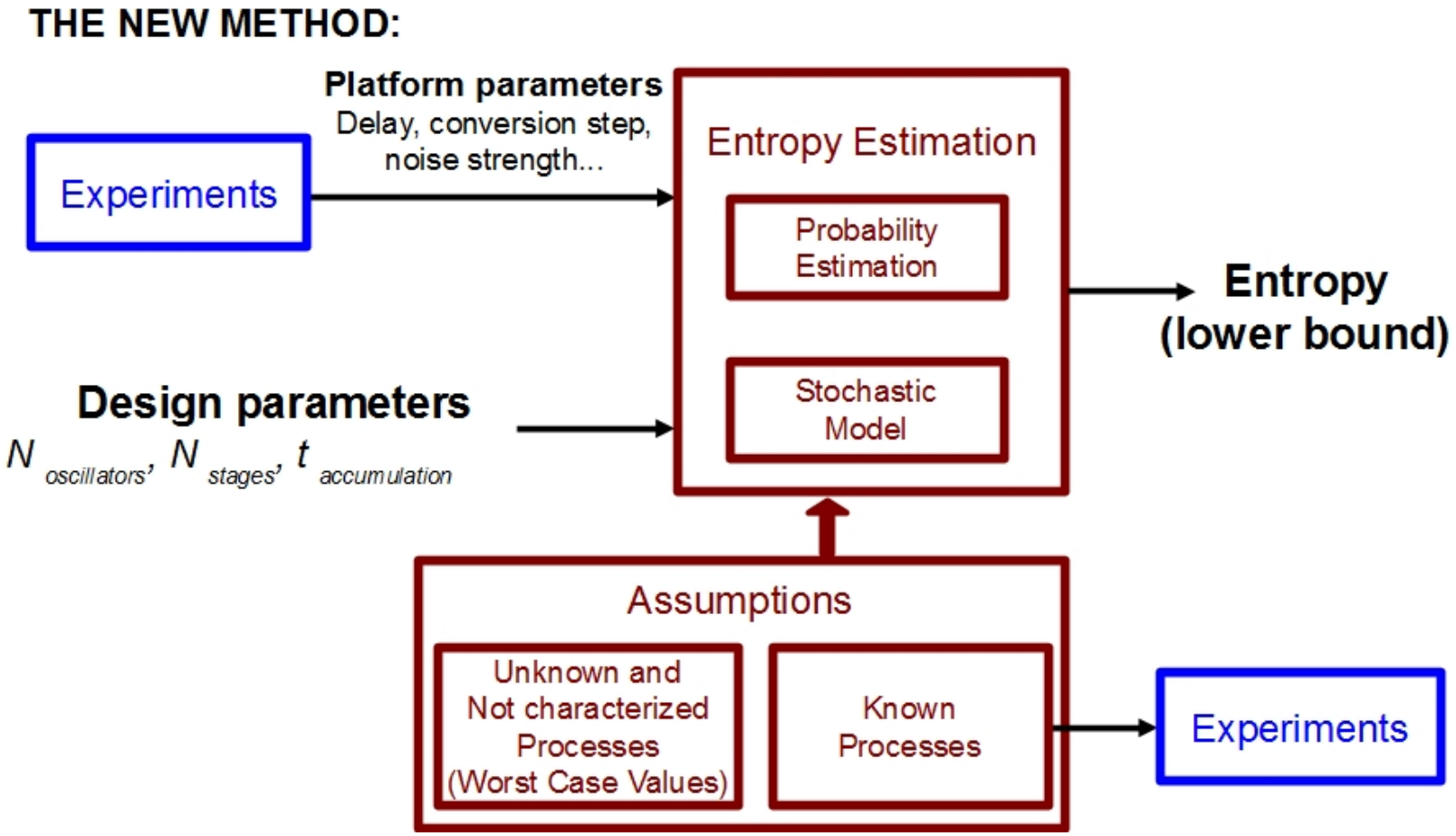
Security Evaluation

THE OLD METHOD:



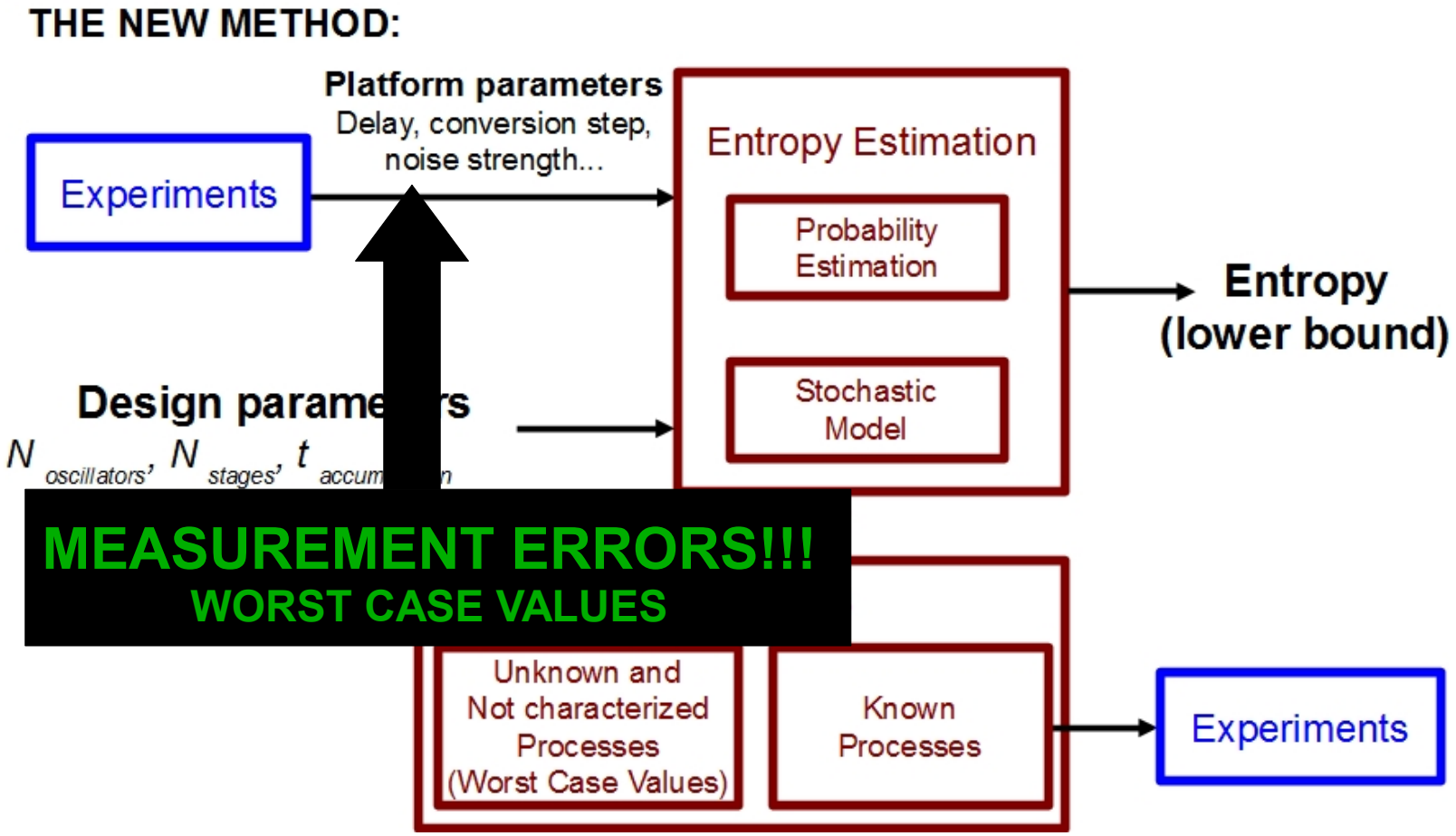
KU LEUVEN

Security Evaluation



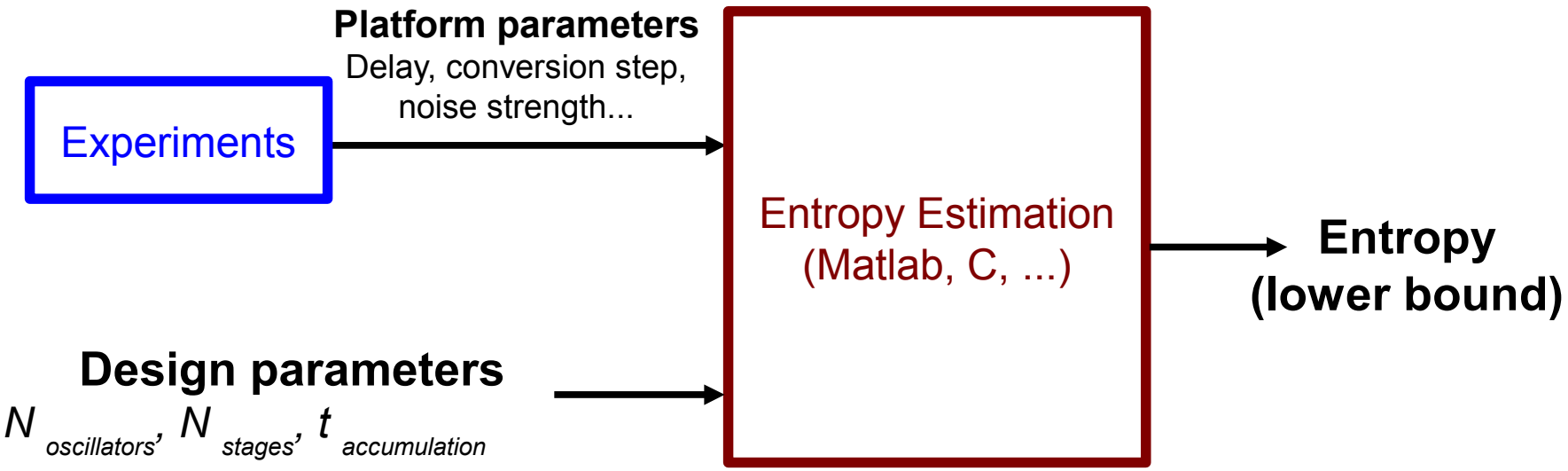
KU LEUVEN

Security Evaluation



KU LEUVEN

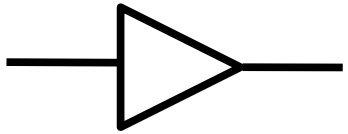
Design Procedure



- STEP1: Build the mathematical model for estimating entropy
- STEP2: Measure the relevant platform parameters
- STEP3: Tune design parameters to make trade-offs

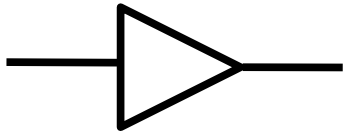
Timing Jitter

Delay=d0+Δd



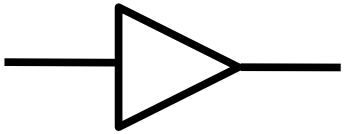
Timing Jitter

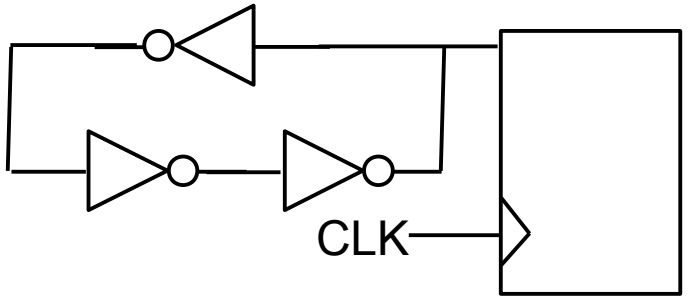
Delay=d0+Δd RANDOM

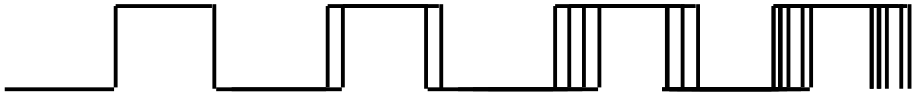


Timing Jitter

Delay=d0+Δd RANDOM



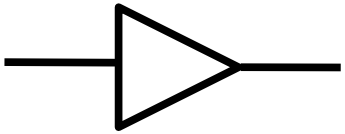


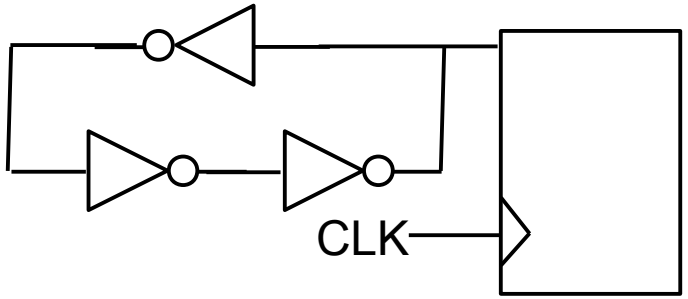


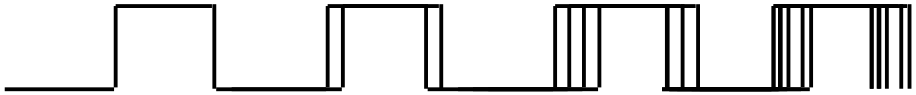
KU LEUVEN

Timing Jitter

Delay=d0+Δd RANDOM



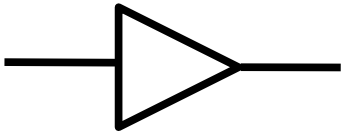


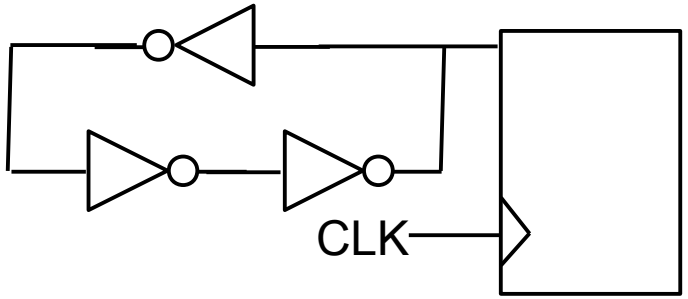


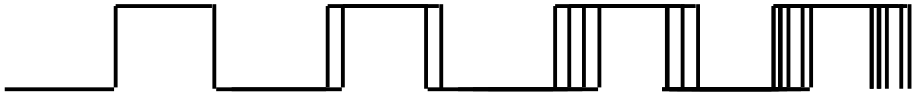
More
Oscillators

Timing Jitter

Delay=d0+Δd RANDOM





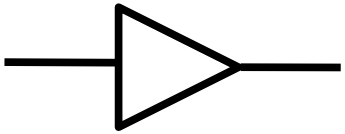


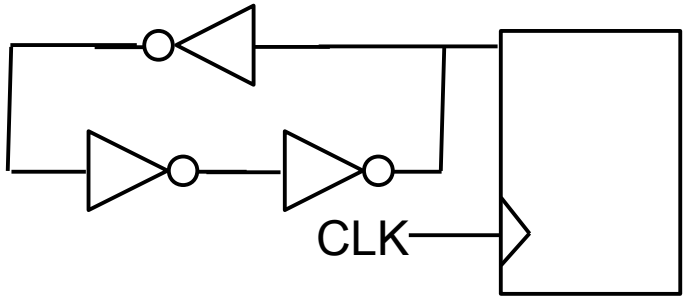
More Oscillators

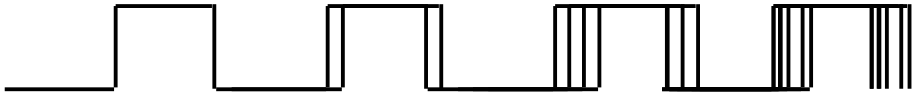
More Transitions

Timing Jitter

Delay=d0+Δd RANDOM







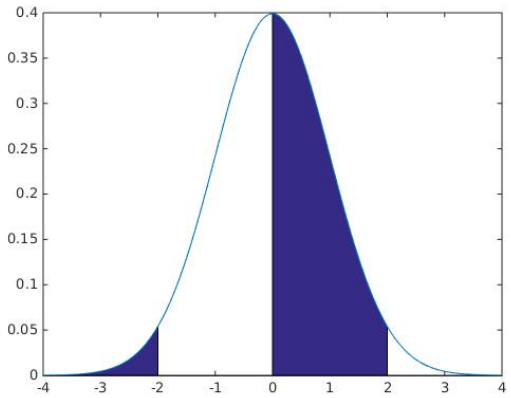
More Oscillators

More Transitions

Efficient Entropy Extraction

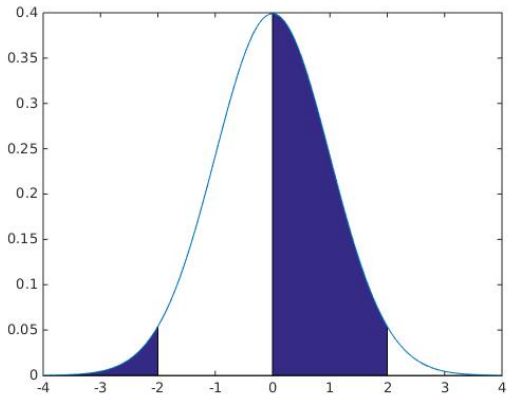
KU LEUVEN

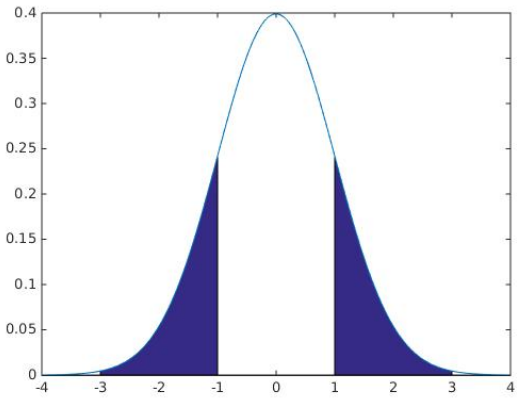
Entropy Extraction



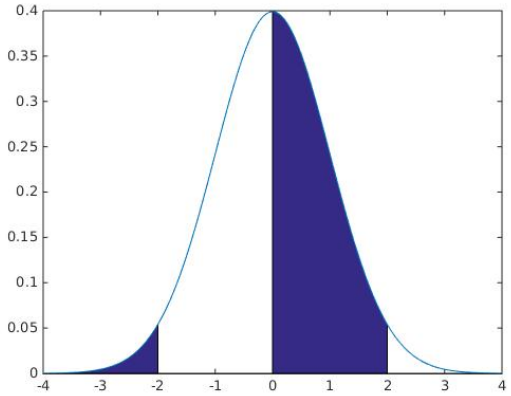
KU LEUVEN

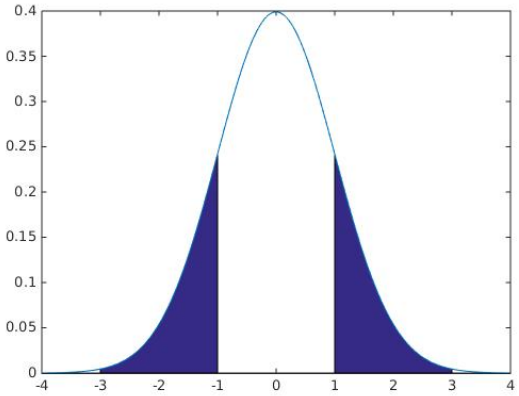
Entropy Extraction

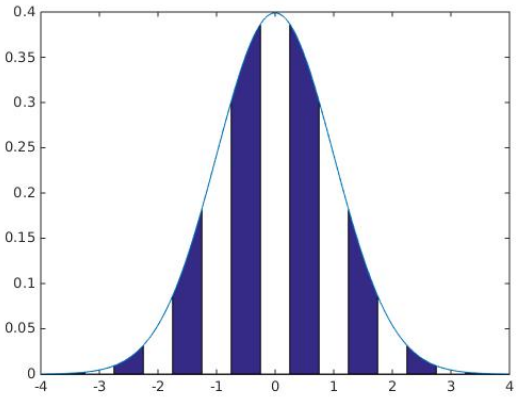




Entropy Extraction

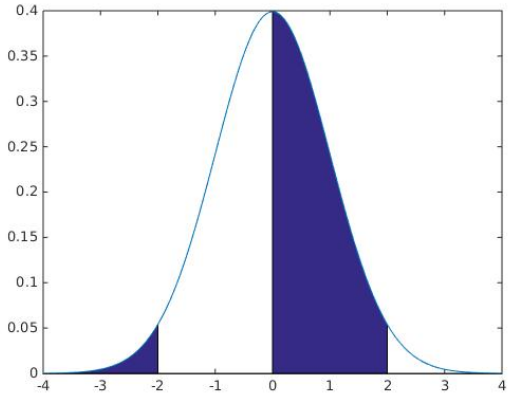


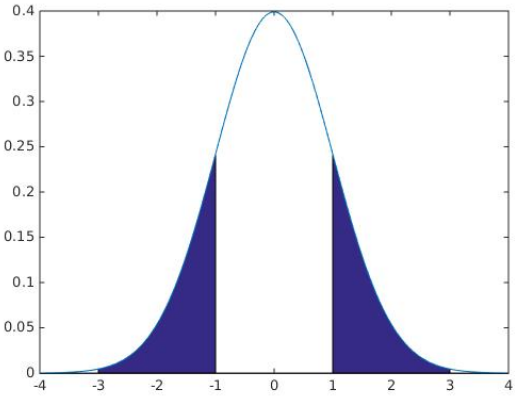


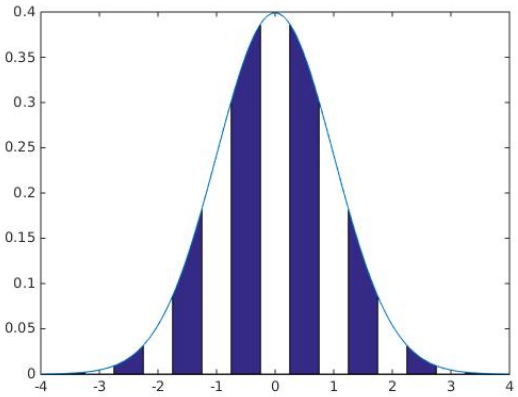


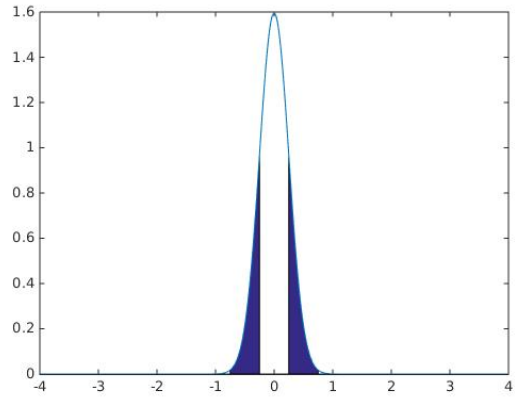
KU LEUVEN

Entropy Extraction



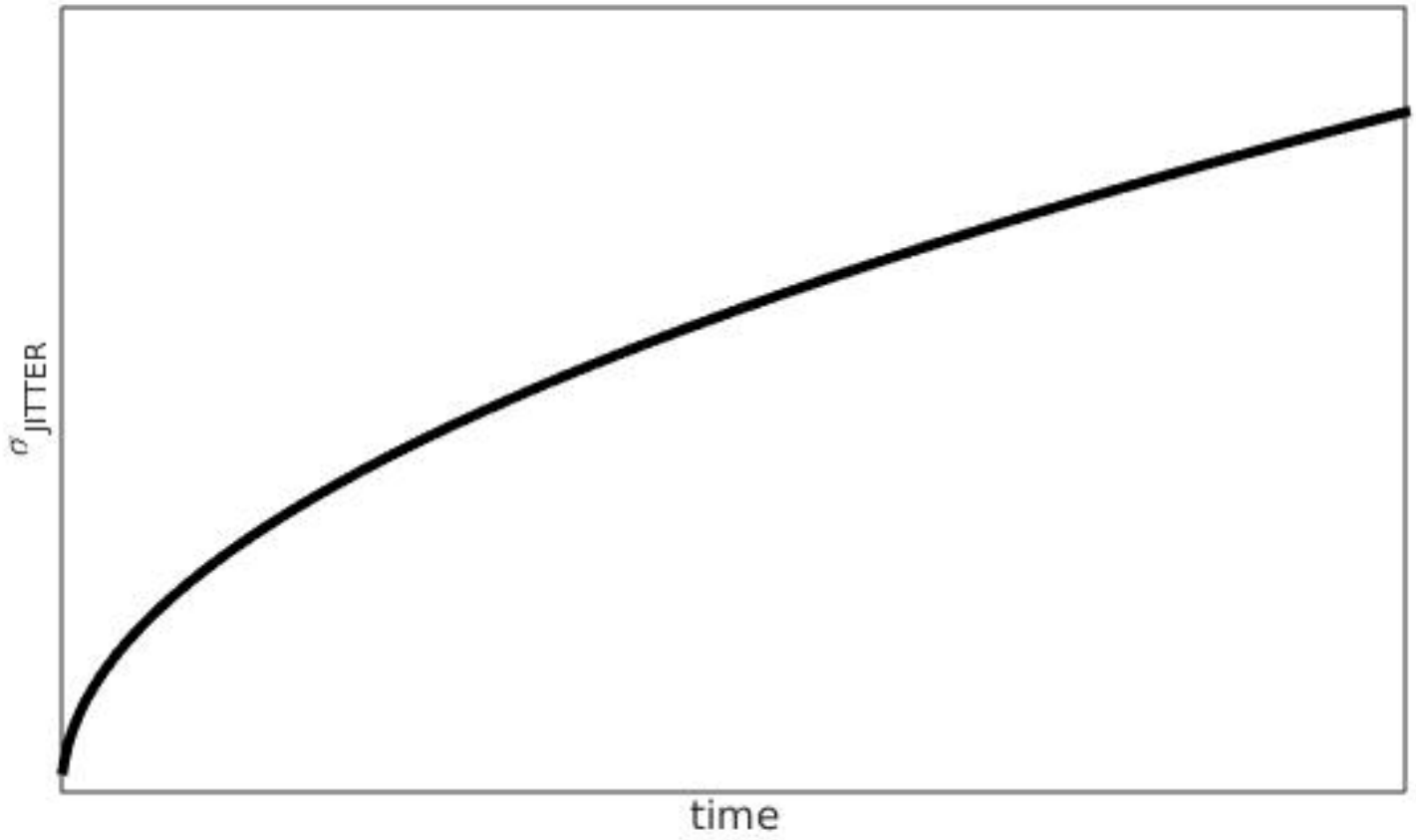






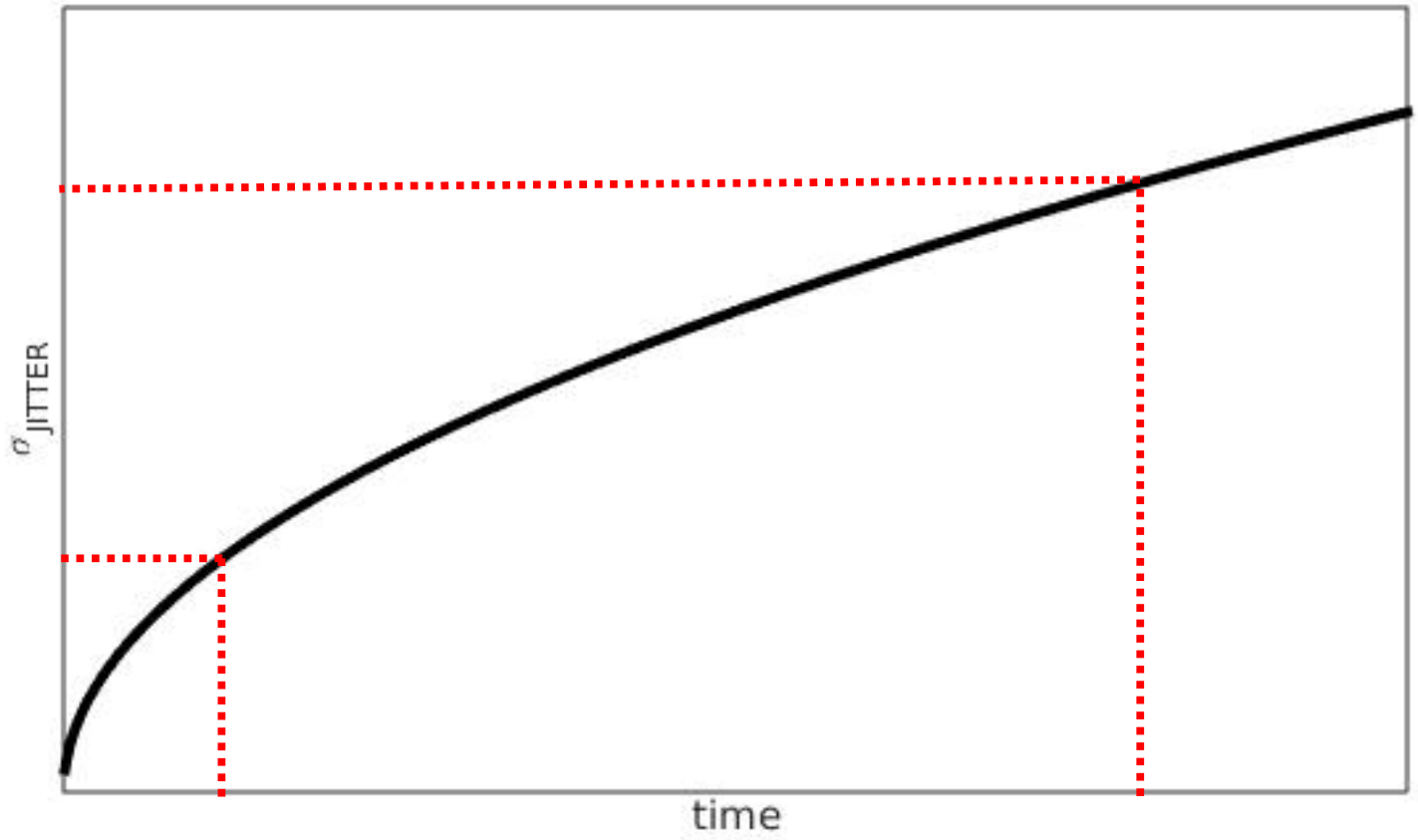
KU LEUVEN

Jitter Accumulation



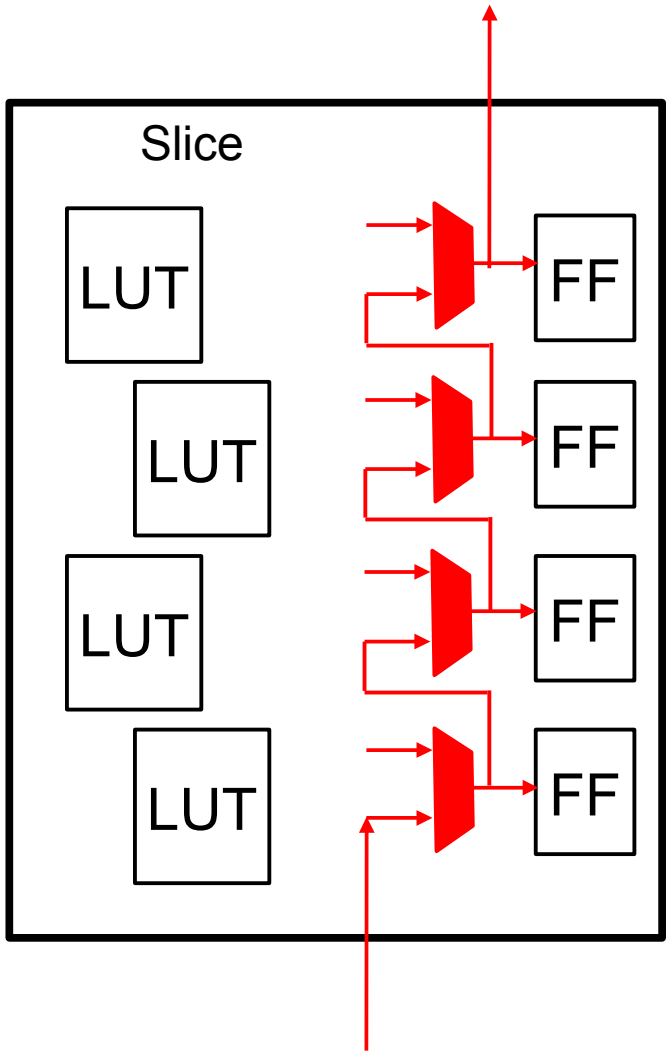
KU LEUVEN

Jitter Accumulation



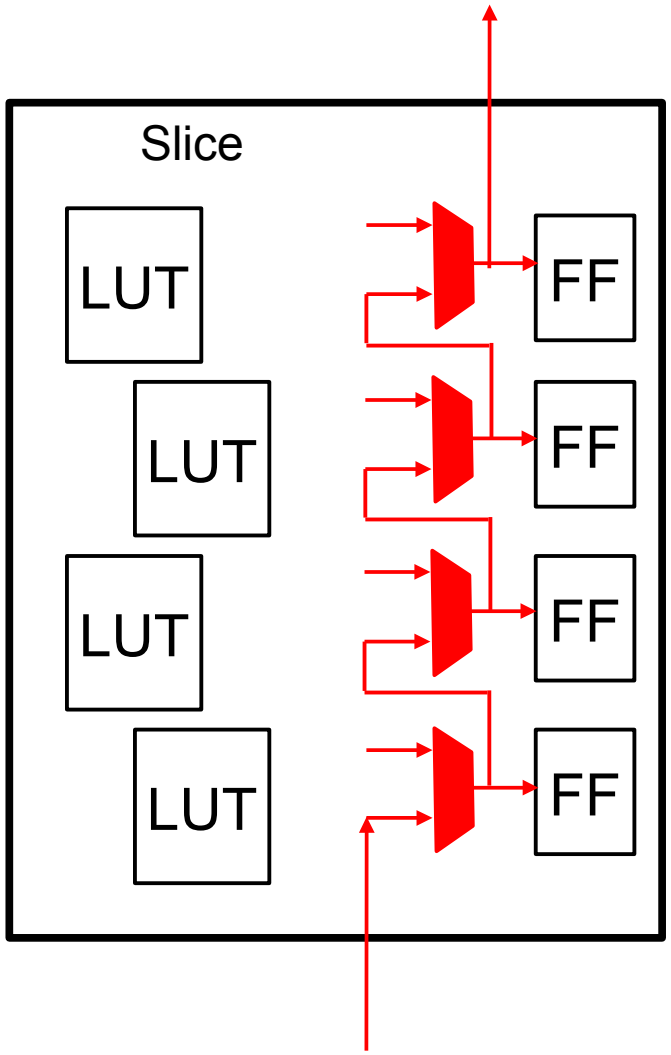
KU LEUVEN

Entropy Extraction on FPGA



KU LEUVEN

Entropy Extraction on FPGA



d_{step}=16ps to 17ps

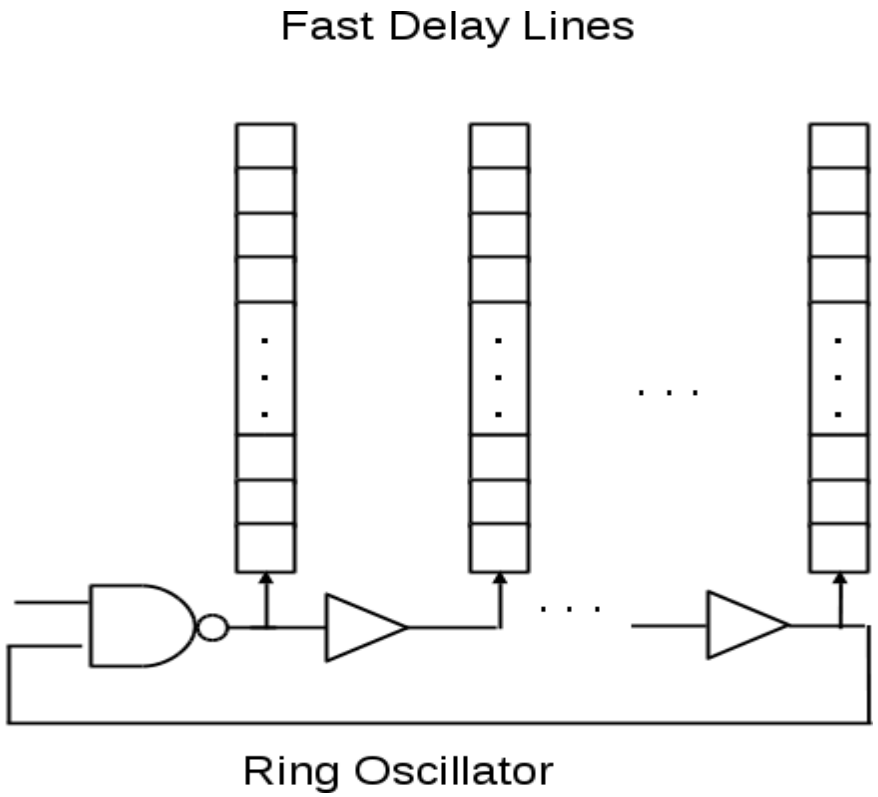
d_{LUT}=480ps

$(d_{LUT}/d_{step})^2$=797.2

KU LEUVEN

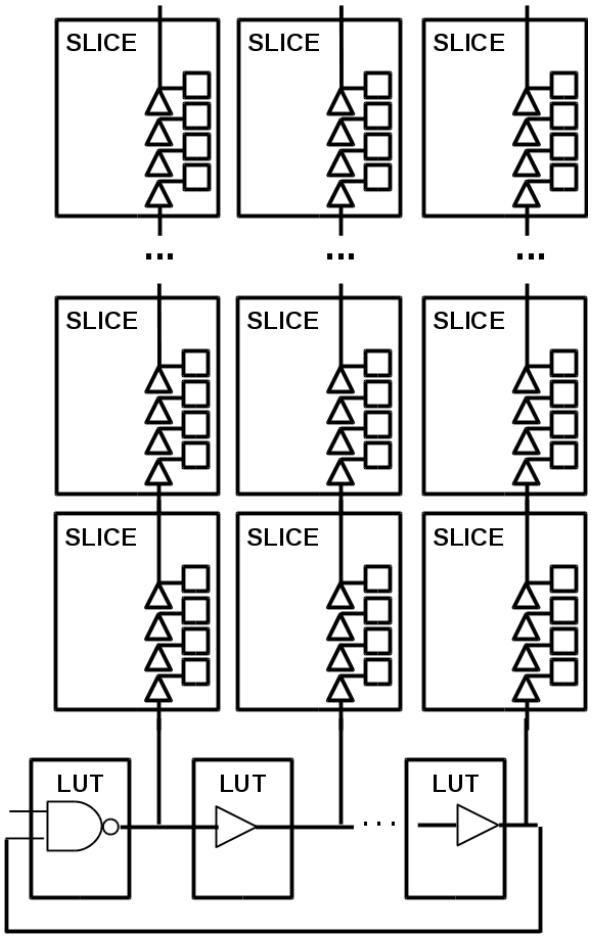
Entropy Source

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



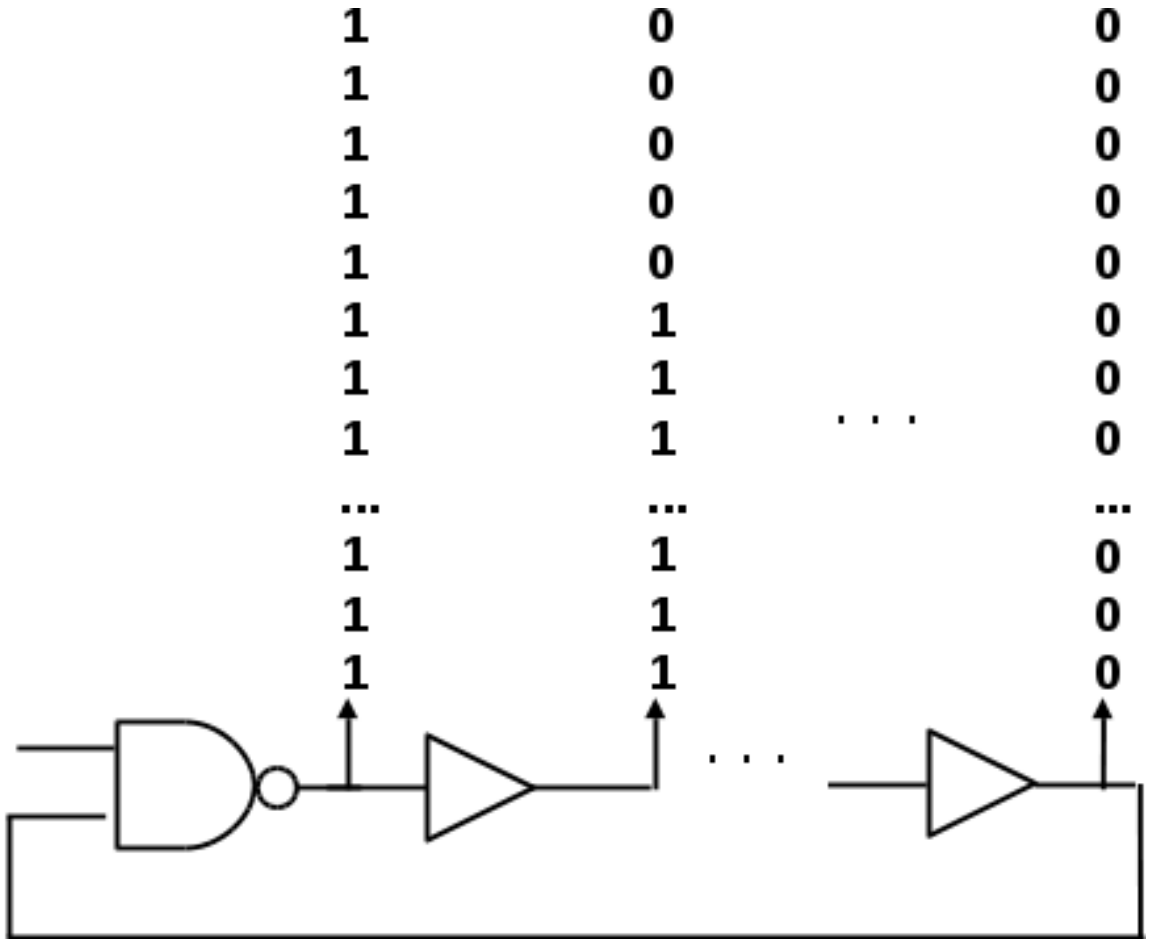
KU LEUVEN

Entropy Source - Implementation



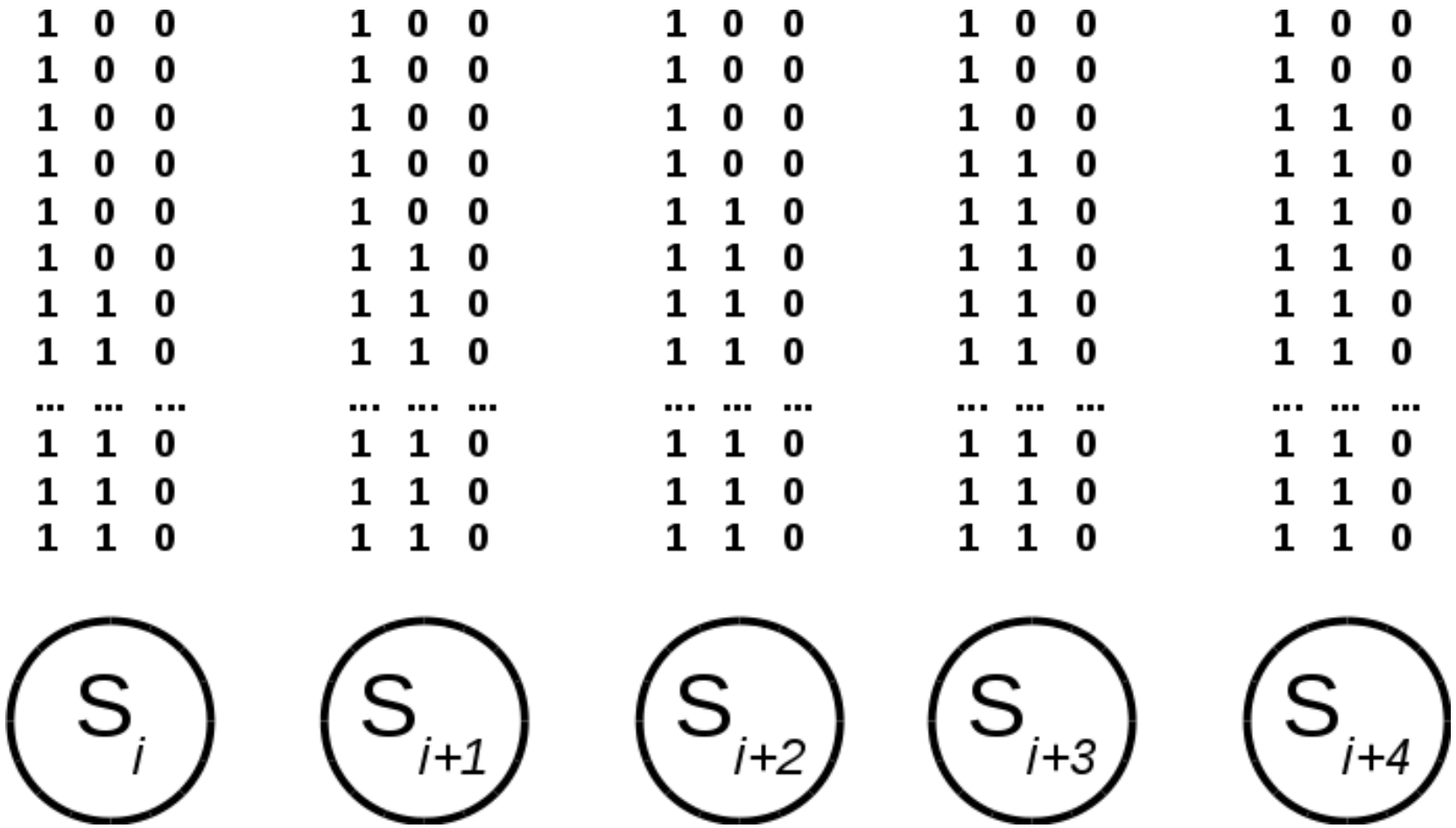
KU LEUVEN

Jitter Snapshot



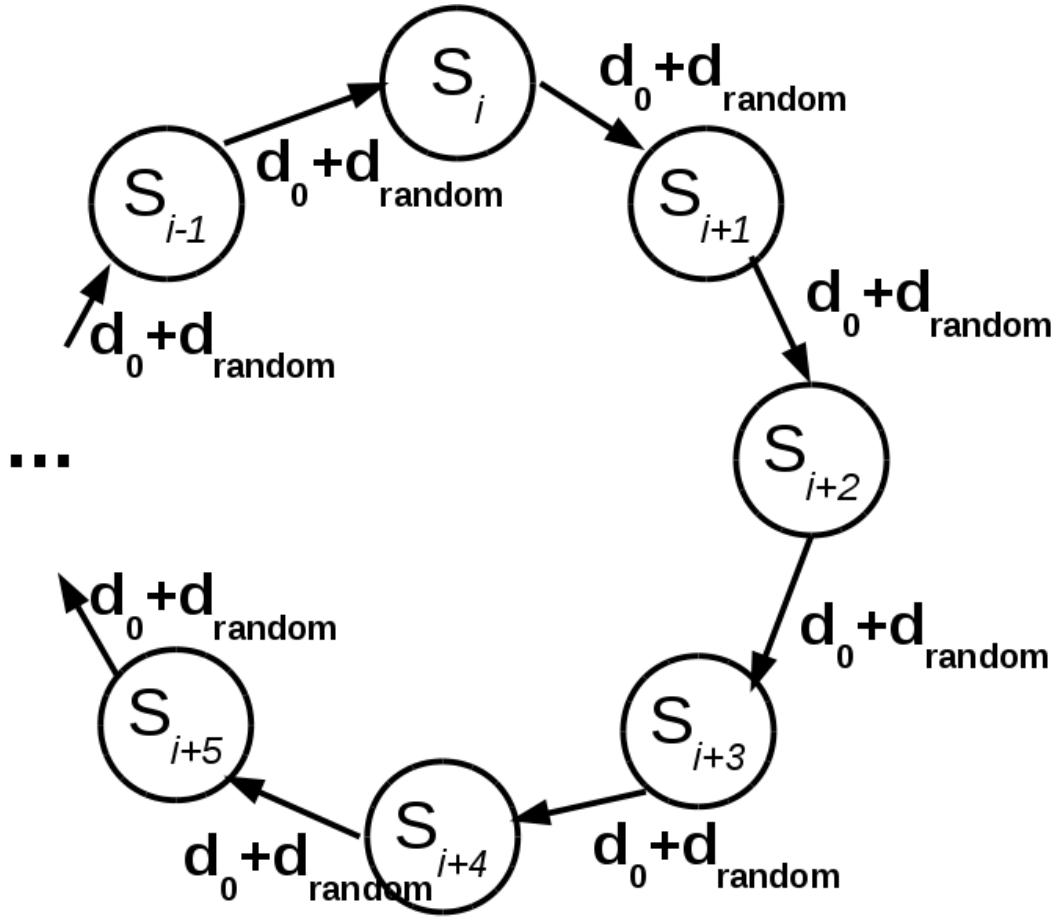
KU LEUVEN

Stochastic Model - FSM



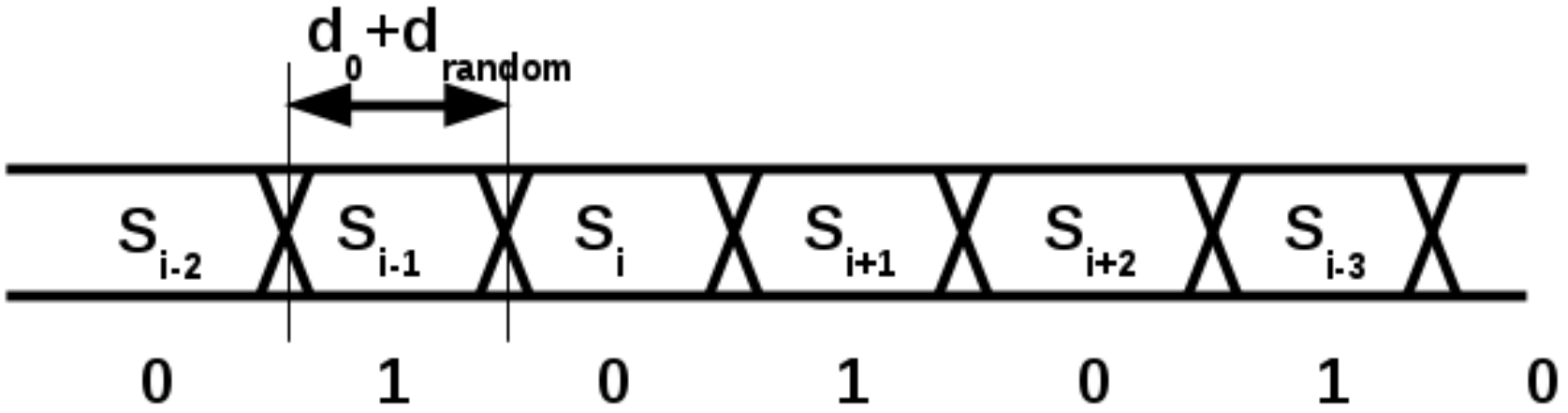
KU LEUVEN

Stochastic Model - FSM



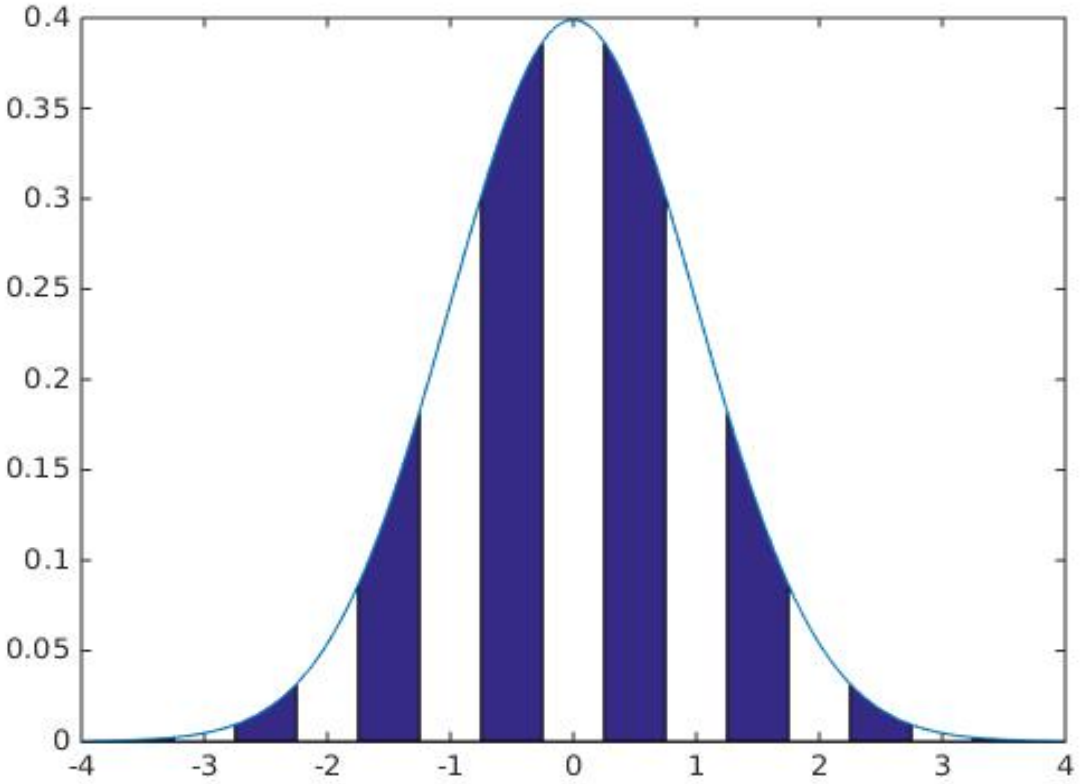
KU LEUVEN

Stochastic Model - FSM



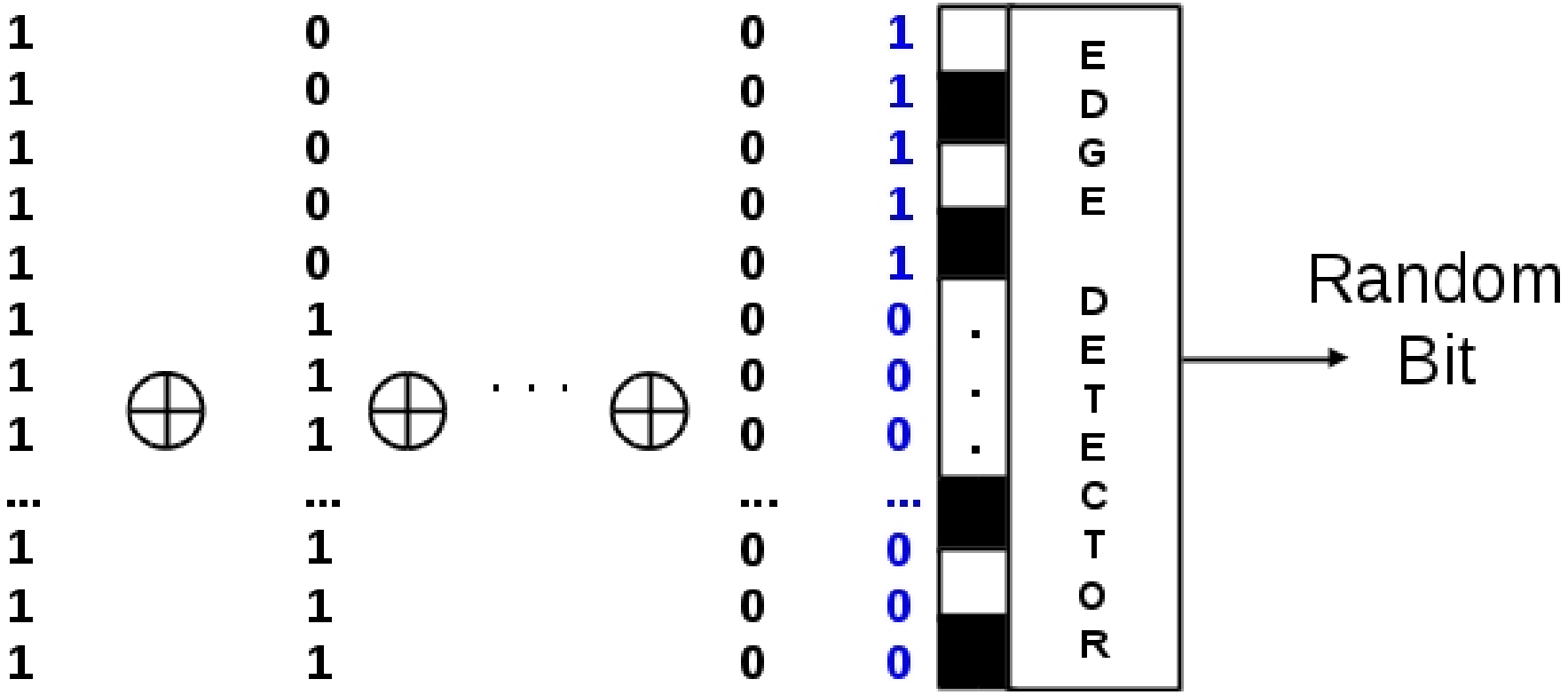
KU LEUVEN

Binary Probability



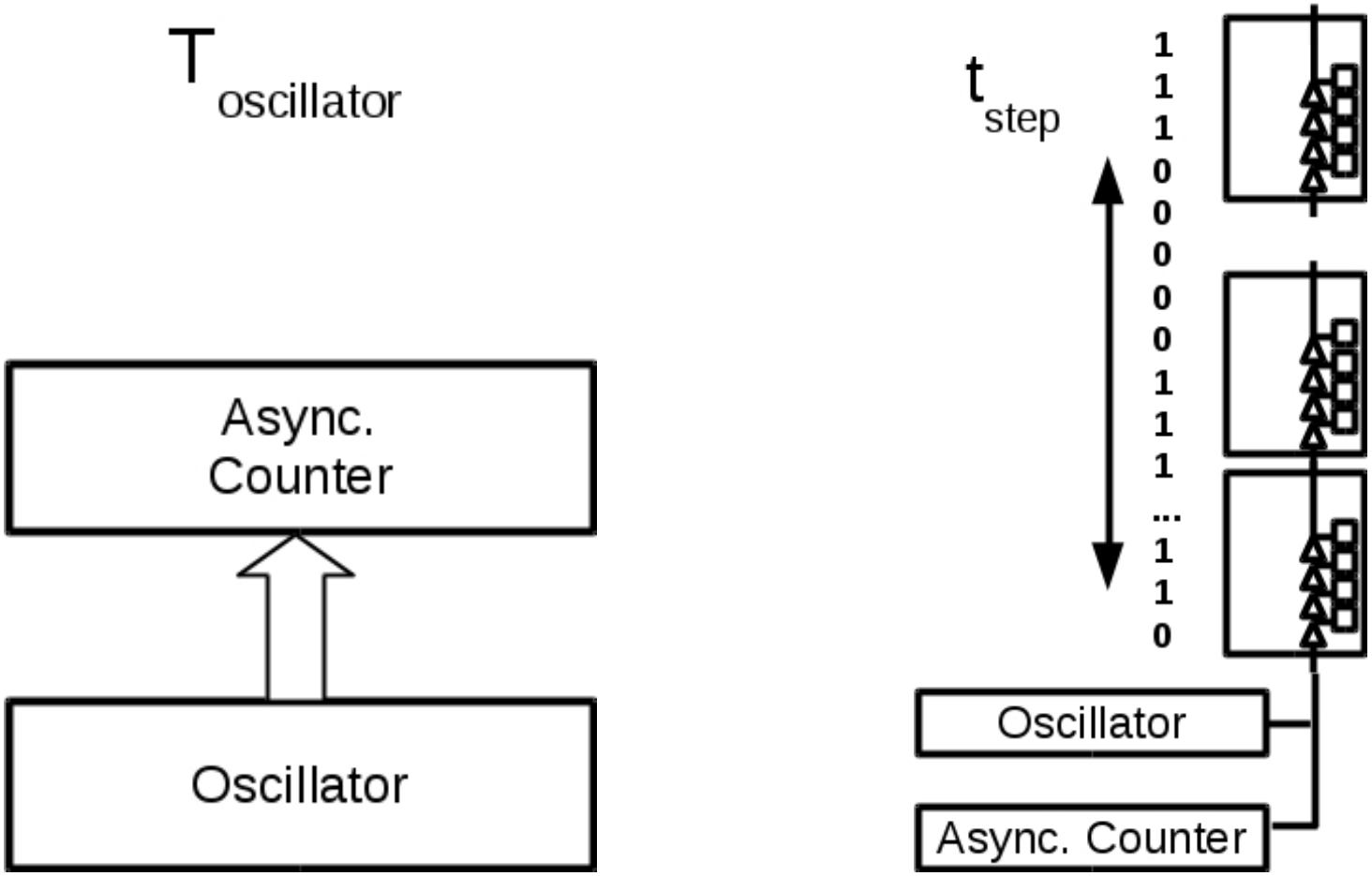
KU LEUVEN

Entropy Extraction - Edge Position Decoding



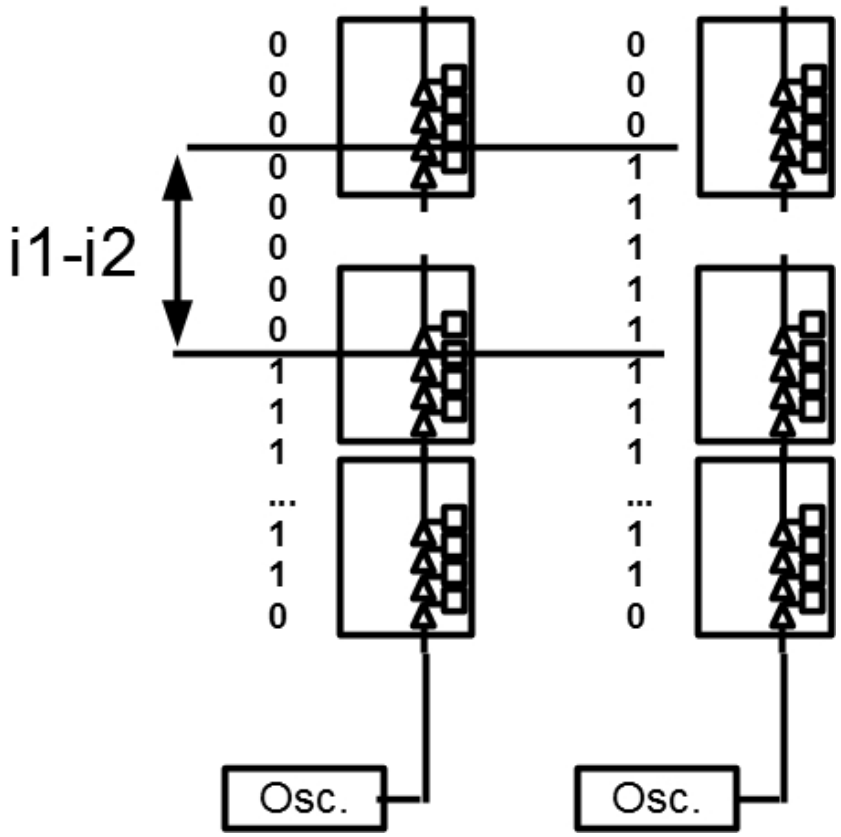
KU LEUVEN

Platform Parameters



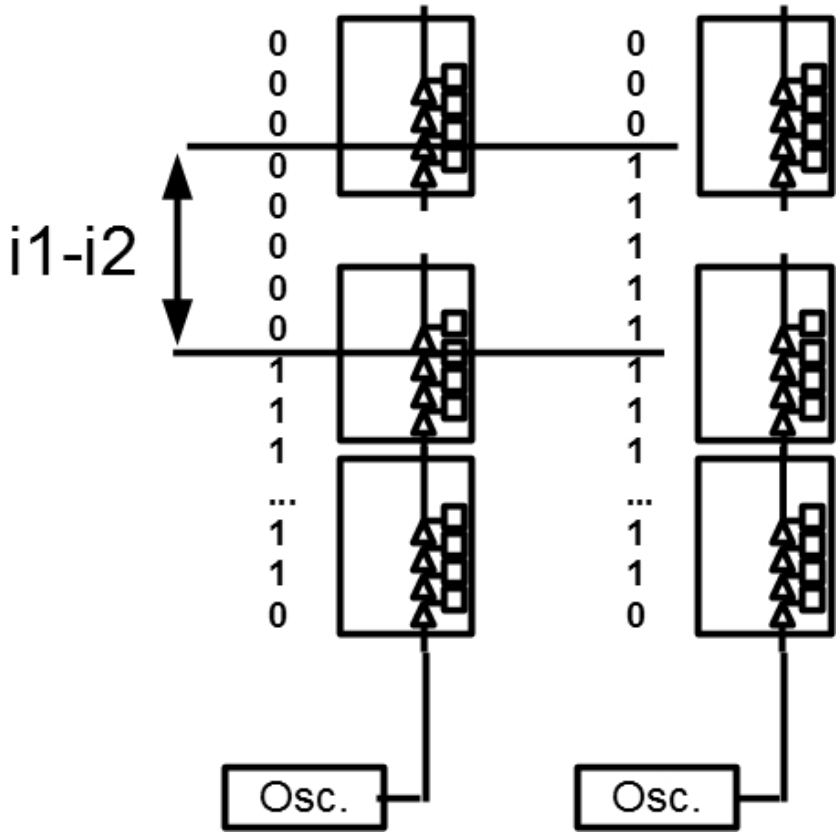
KU LEUVEN

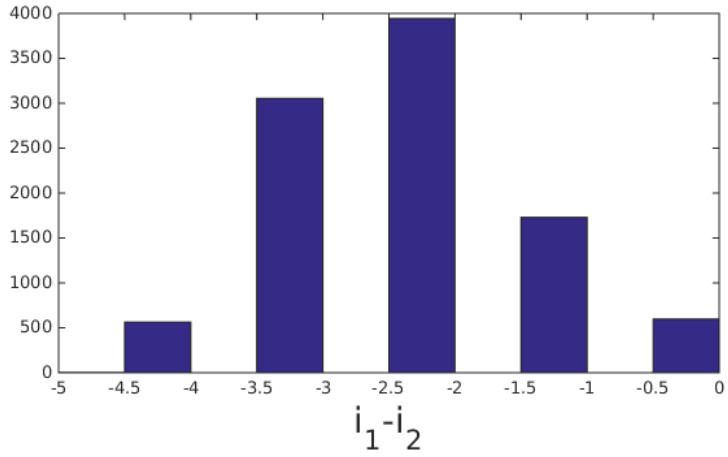
Platform Parameters-Jitter



KU LEUVEN

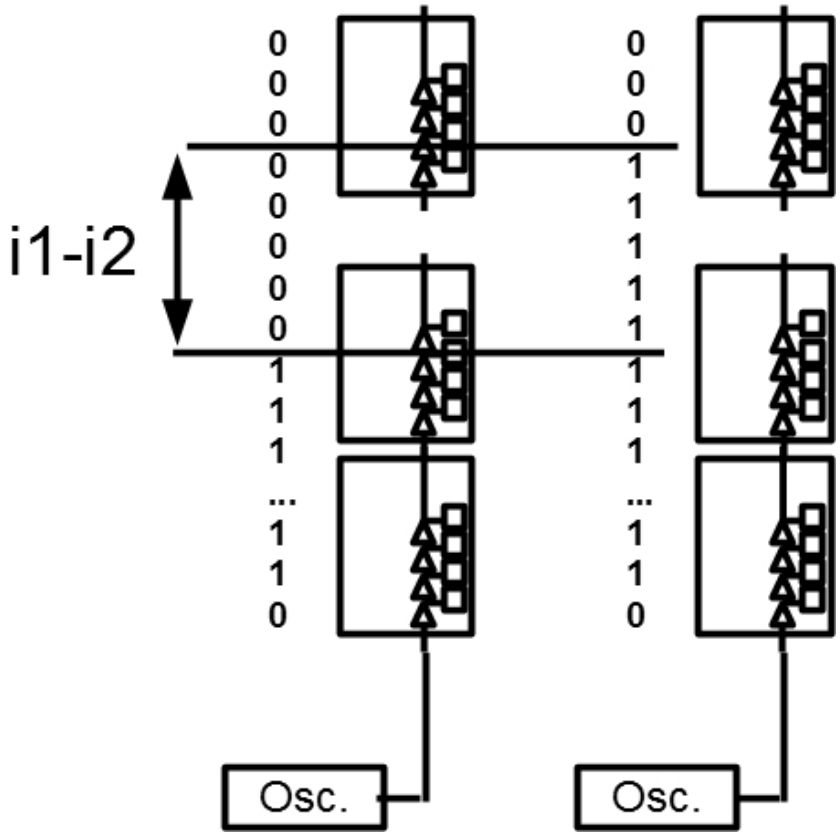
Platform Parameters-Jitter

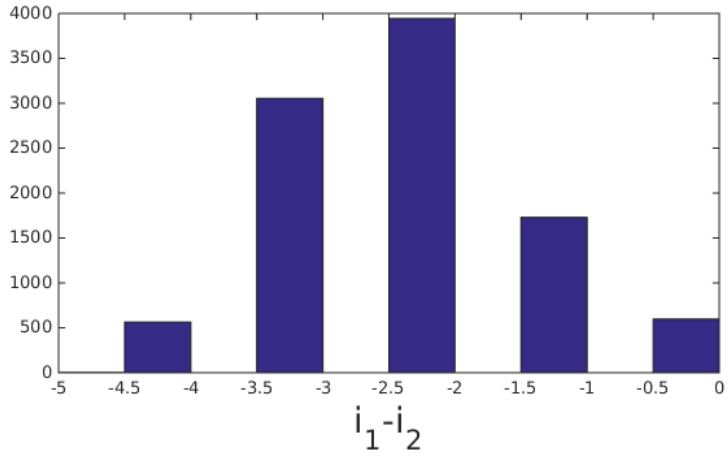




KU LEUVEN

Platform Parameters-Jitter



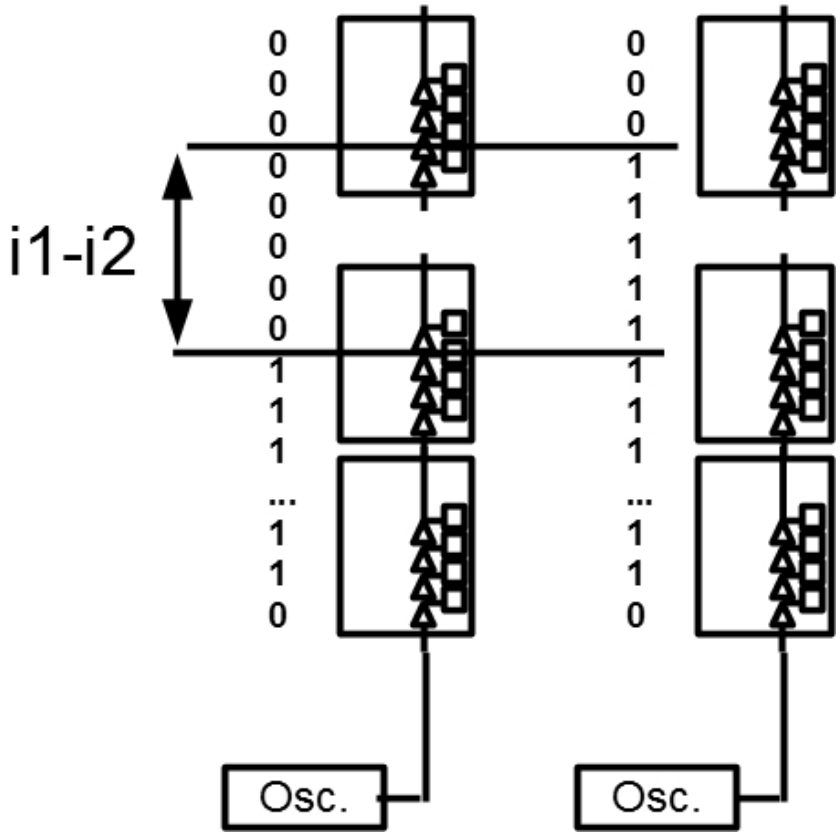


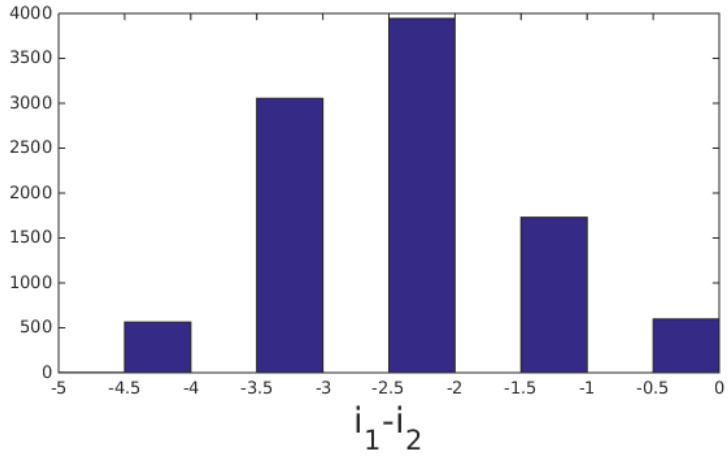
t=20ns

σ_{jitter}=0.97 * 16ps = 15.5 ps

KU LEUVEN

Platform Parameters-Jitter





t=20ns

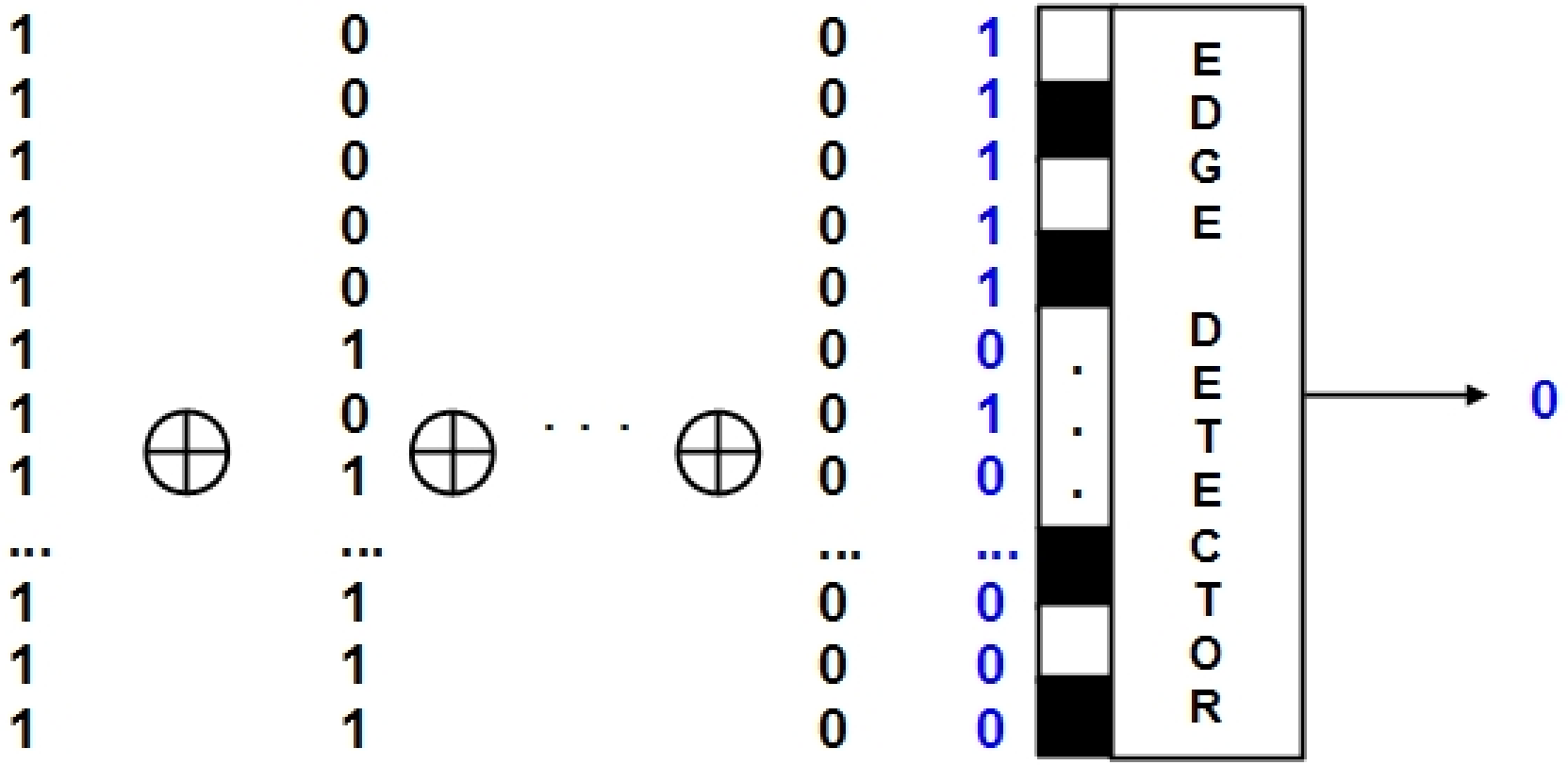
σ_{jitter}=0.97 * 16ps = 15.5 ps

-20%

12.5 ps

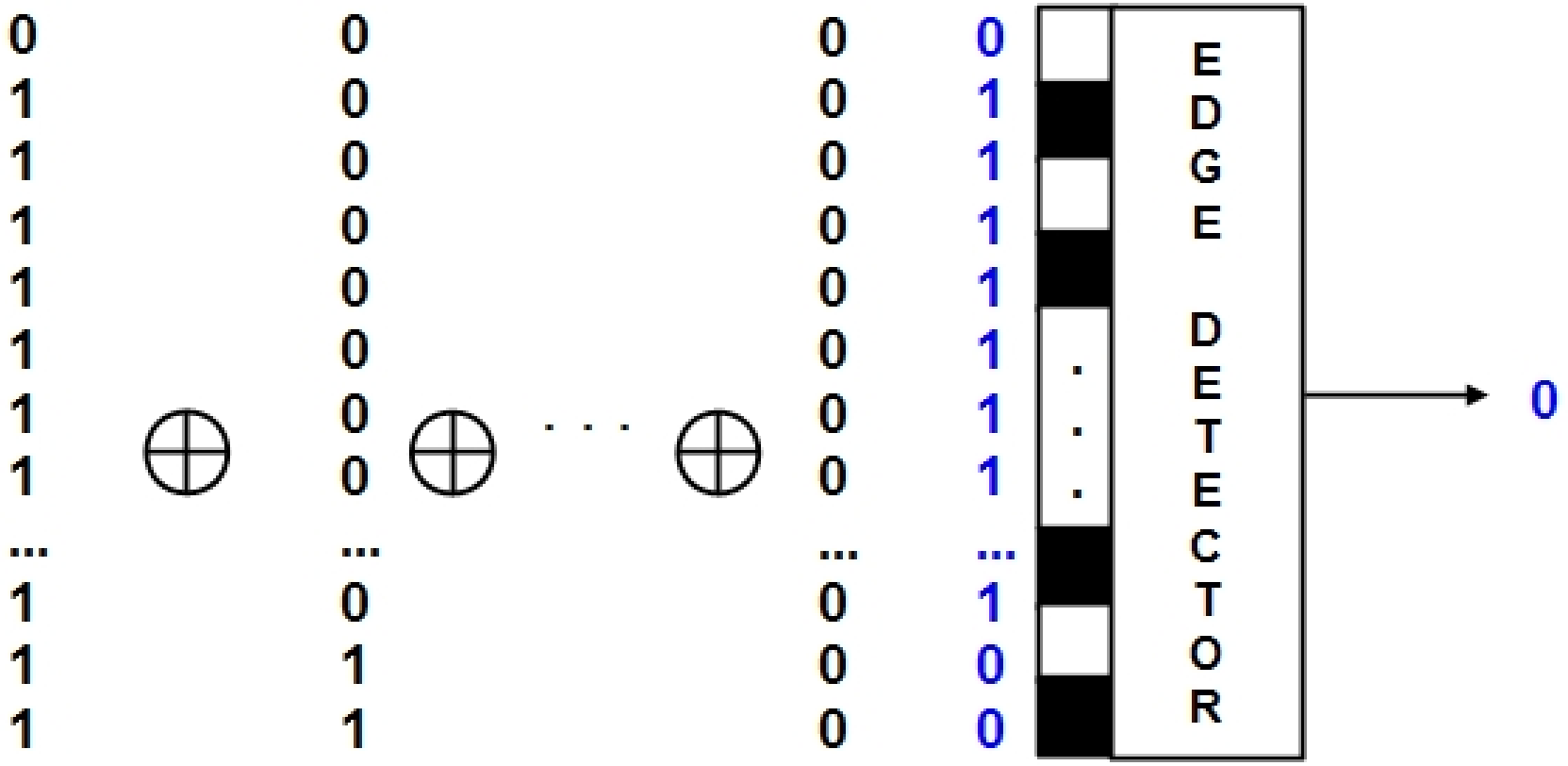
KU LEUVEN

Entropy Extraction - Bubbles in the Code



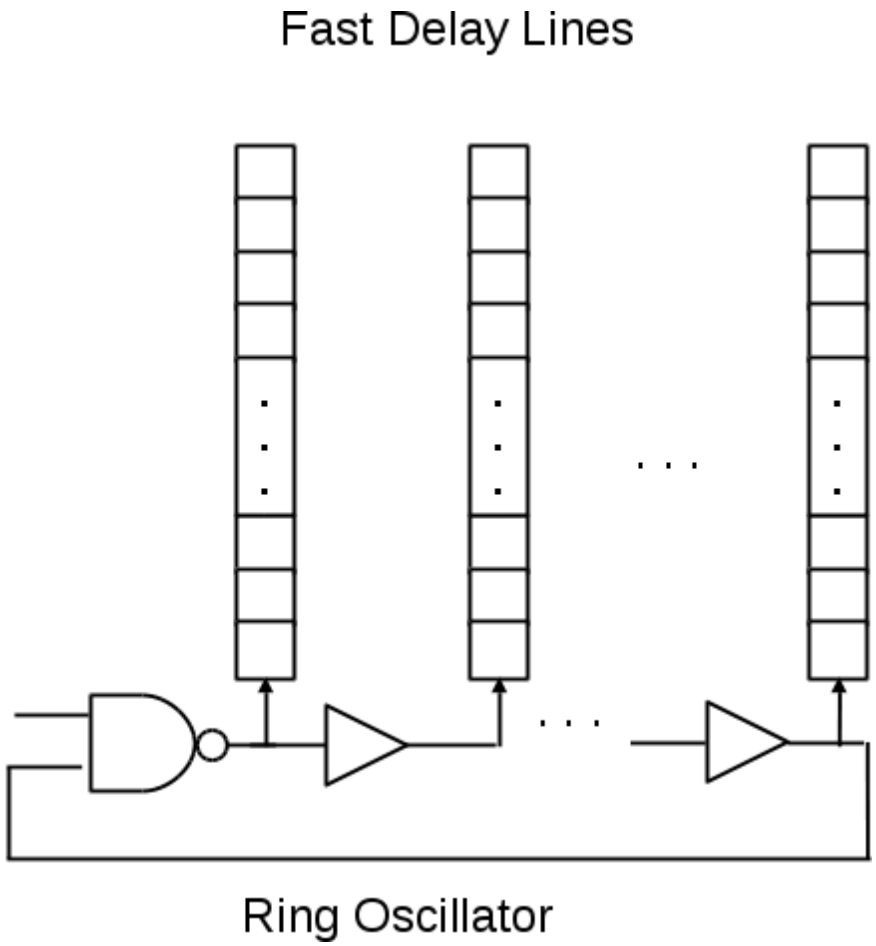
KU LEUVEN

Entropy Extraction – Double Edges



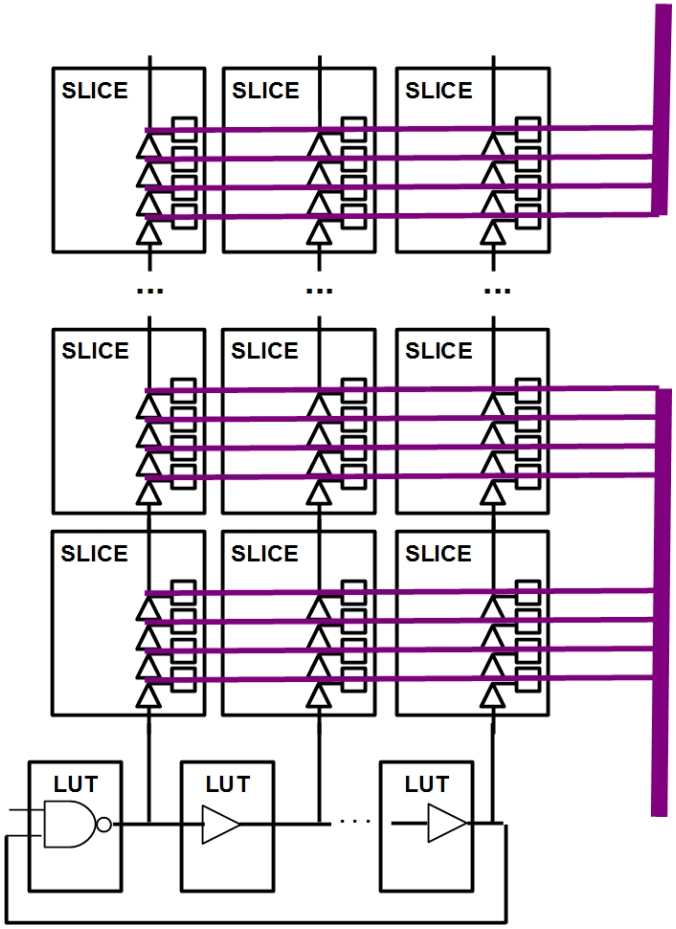
KU LEUVEN

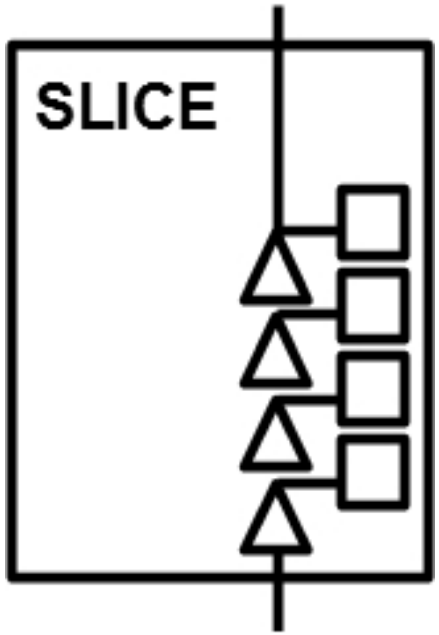
Design Parameters



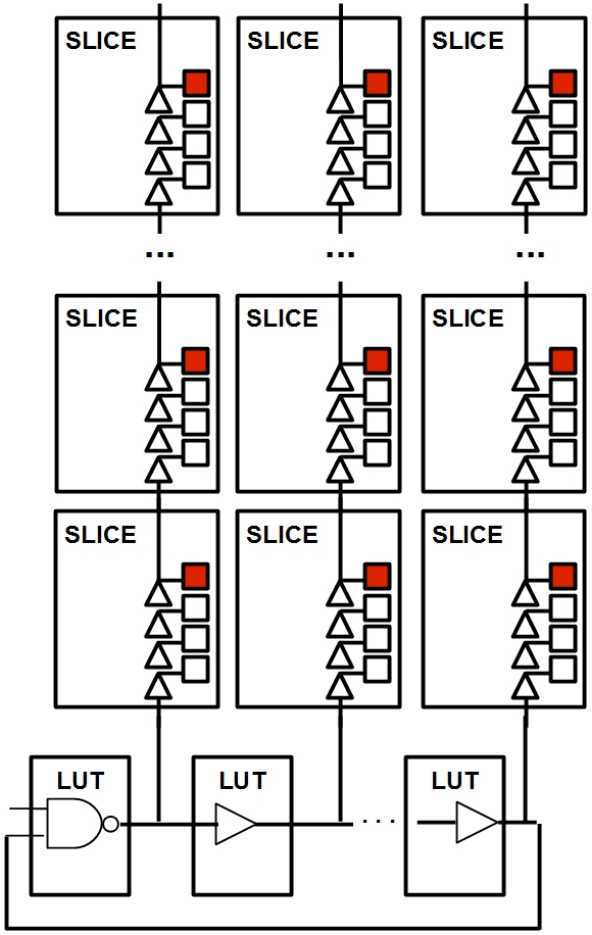
- n=3
- m=36
- t=N*10ns

Non-Linearity





Non-Linearity – Downsampling



KU LEUVEN

Results

Na	k	H	n_{pf}	Throughput1 [Mbps]	H_{min}	Throughput2 [Mbps]
1	1	0.917	3	33.33	0.58	28
2	1	0.994	2	25	0.88	22
3	1	0.999	1	33.33	0.96	16
5	4	0.42	15	1.33	0.13	1.3
10	4	0.77	5	2	0.36	1.82
15	4	0.9	3	2.22	0.55	1.83
20	4	0.95	2	2.5	0.68	1.7
25	4	0.98	2	2	0.78	1.56

Results - resources

k	Platform	Resources
1	Spartan6	64 slices
4	Spartan6	40 slices

Conclusions and Future Work

- Carry-chain primitives provide high-precision measurements of accumulated jitter
- Highly efficient entropy extraction on FPGAs
- High throughput (>MHz) with low resources (<70 slices)
- Future work
  - Improve arithmetic post-processing
  - Modify stochastic model to account for non-linearities
  - On-the-fly testing

Thank You

Questions? Comments?

KU LEUVEN