An energy and area efficient, all digital entropy source compatible with modern standards based on jitter pipelining

2022 Conference on Cryptographic Hardware and Embedded Systems

Adriaan Peetermans Ingrid Verbauwhede

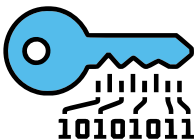
imec-COSIC, KU Leuven, Leuven, Belgium

September 21, 2022

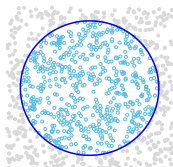
Random numbers

How are they used?

- Cryptography



- Statistical simulations

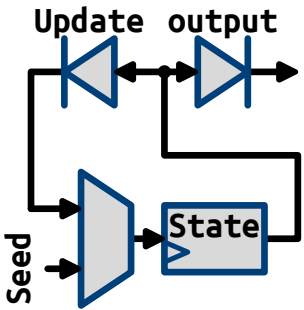


- Gambling/games

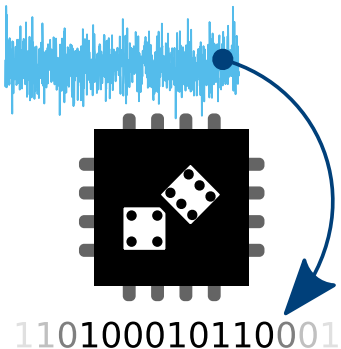
Random numbers

How are they generated?

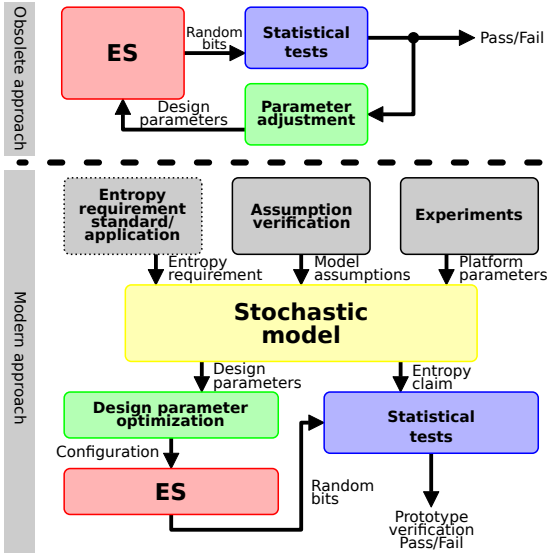
- Pseudo Random Number Generator (PRNG)



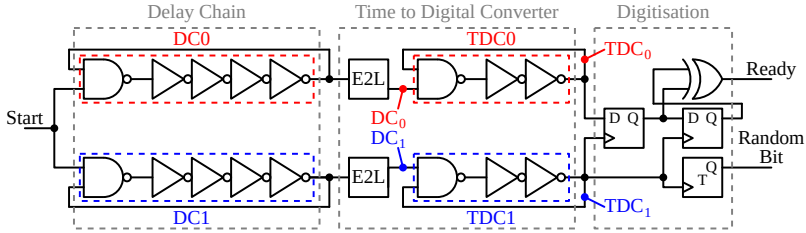
- True Random Number Generator (TRNG)



RNG verification

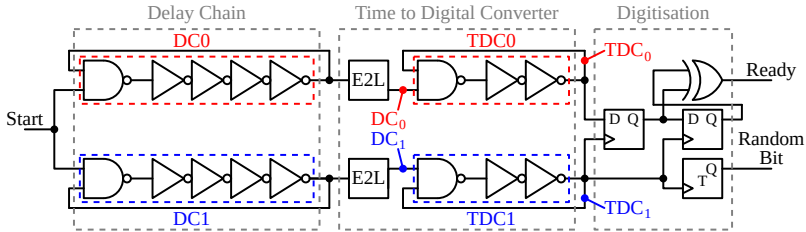


TRNG architecture



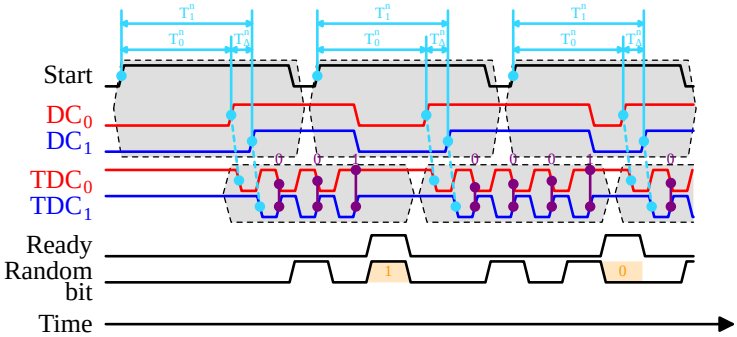
- **Delay Chain (DC)**
  - Propagate start edge through two independent paths
  - Timing jitter accumulation
- **Time to Digital Converter (TDC)**
  - Resolve timing difference created by DCs
  - Timing jitter accumulation
- **Digitisation**
  - Convert resolved timing difference into digital format
  - Notifies controller output is valid

TRNG architecture



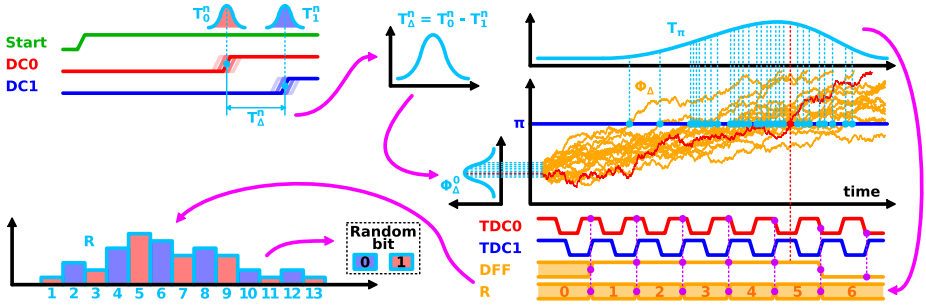
- Throughput optimisation:
  - Reduced TDC resolution requires less jitter accumulation time
    - TDC frequency matching
  - Concurrent jitter accumulation both in DC and TDC
    - Jitter pipelining

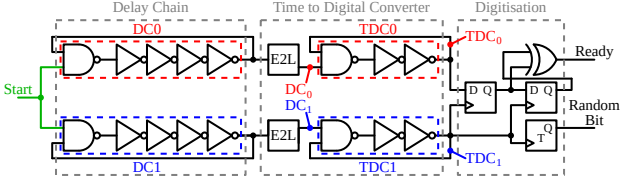
Jitter pipeline



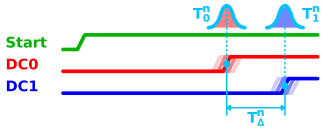
- Jitter pipeline with two stages
  - DC-stage
  - TDC-stage
- First bit is resolved while second one is already started
- Pipeline timing balance should be maintained

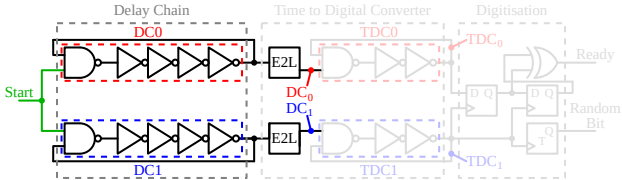
Stochastic model, overview



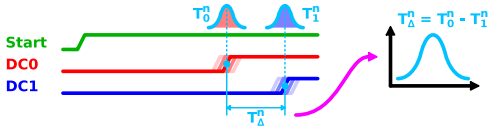


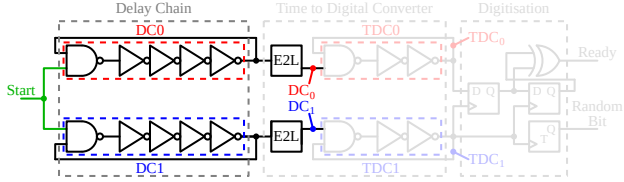
Stochastic model, overview



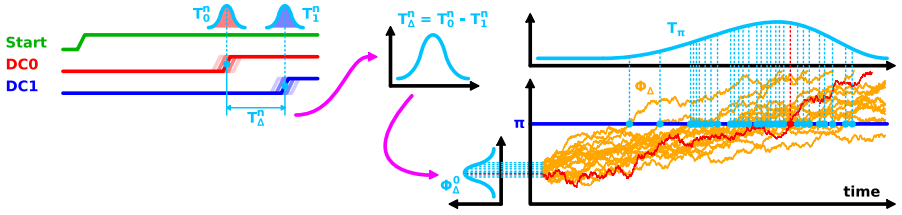


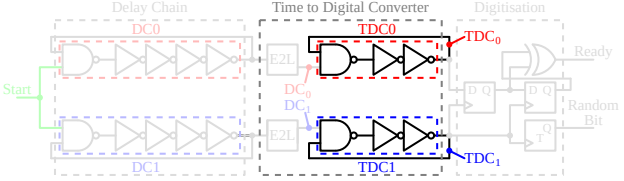
Stochastic model, overview



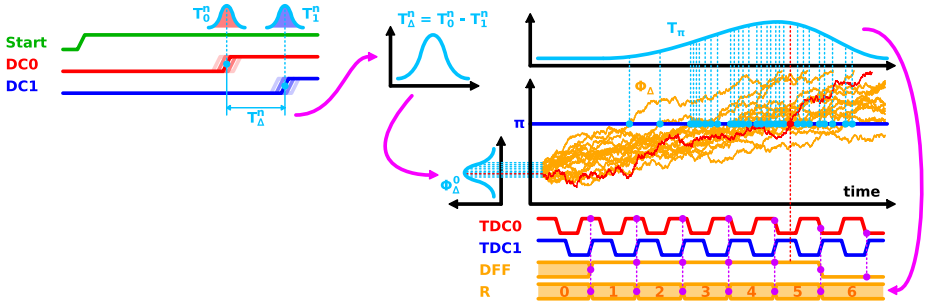


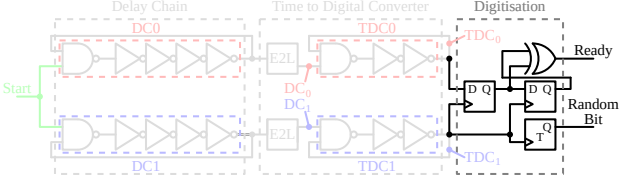
Stochastic model, overview



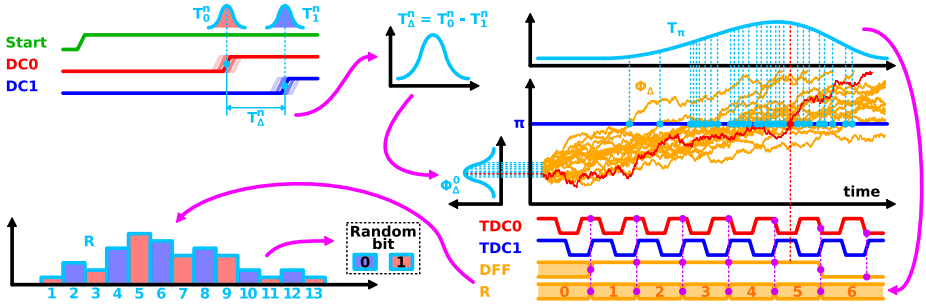


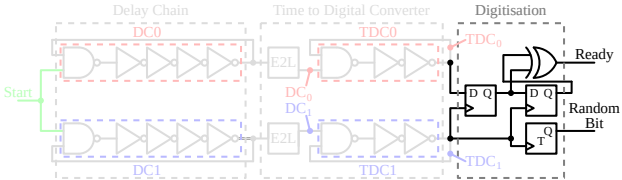
Stochastic model, overview



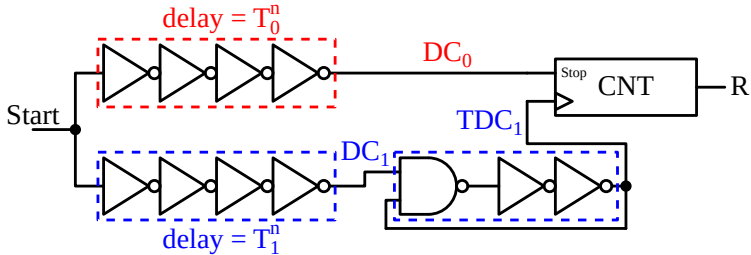


Stochastic model, overview



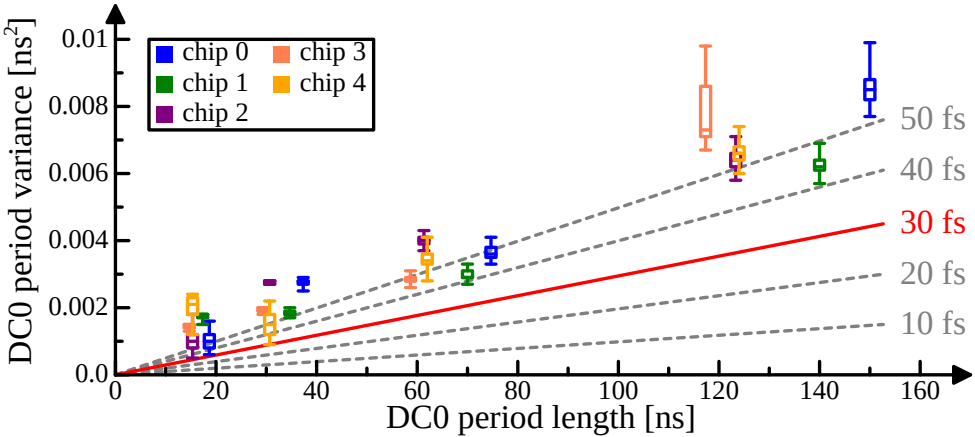


On-chip jitter measurement

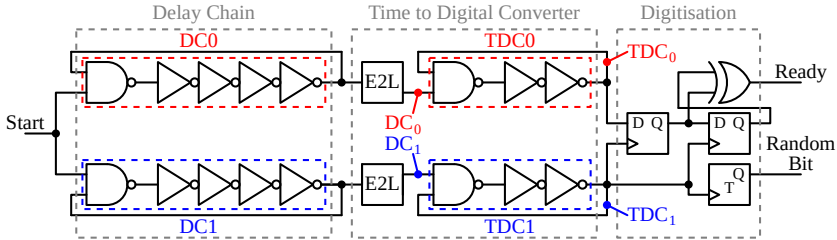


- Experimentally determine platform dependent jitter parameter
- Conservative estimation method avoids overestimation
  - Overestimation could lead to false entropy claim
  - Measurement errors give positive bias
- On-chip and differential to avoid external influences
- Reuse existing TRNG hardware

On-chip jitter measurement, results

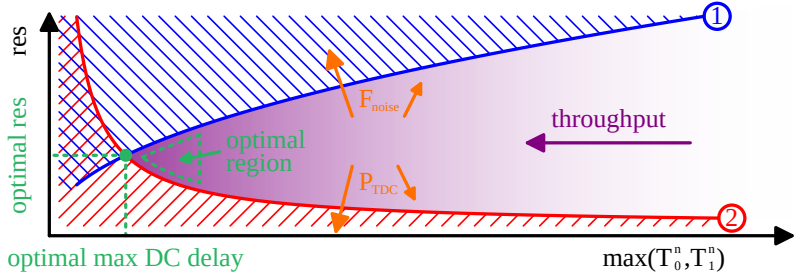


Design parameter selection criteria



- Four design parameters can be freely chosen: μ_{DC_0}, μ_{DC_1}, μ_{TDC_0} and μ_{TDC_1}
  - Represent DC, TDC oscillation frequencies
- Selection criteria:
  - Pipeline balance
  - Entropy density
  - Throughput

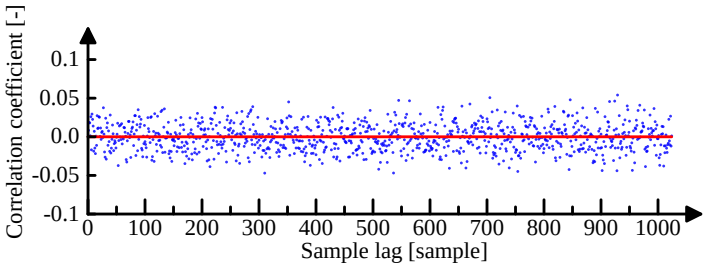
Design parameter selection criteria



- Resolution versus accumulation time bounded by:
  - Entropy density (1)
  - Pipeline balance (2)
  - Throughput (colour gradient)
- TRNG throughput improved by:
  - Larger jitter strength (shifts (1))
  - Faster TDC oscillation speed (shifts (2))

Experimental results

- IID claim verification
  - Correlation analysis
    - 4096 consecutively generated counter values



    - No correlation observed
  - NIST SP 800-90B IID test
    - 5 devices, 1 Mbit consecutively generated random bits per device
    - All devices pass

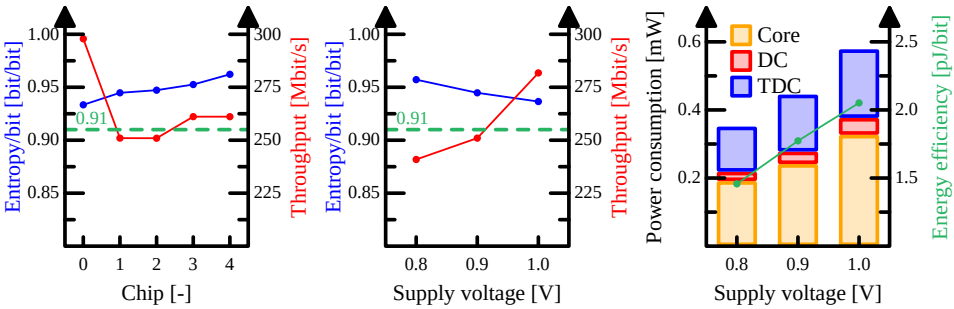
Experimental results

- Entropy validation
  - Standards require minimally 0.91 bit/bit min-entropy density
  - ES design parameters have been optimised to output at least the required entropy density
  - Higher entropy density levels possible at lower throughput
  - 5 devices, 1 Mbit consecutively generated random bits per device
  - All devices reach required entropy density

Chip	0	1	2	3	4
Model estimate	0.99988	0.99861	0.99811	0.99895	0.99963
Test estimate	0.93341	0.94475	0.94722	0.95255	0.96221
Minimum	0.93341	0.94475	0.94722	0.95255	0.96221

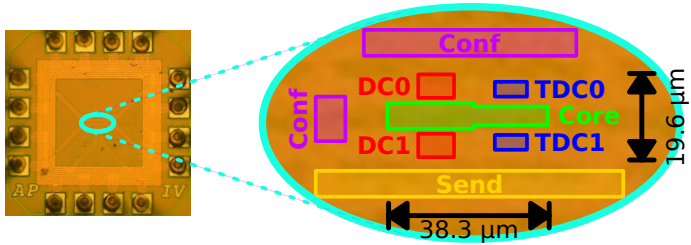
Experimental results

- Power and throughput



- All devices have a throughput higher than 250 Mbit/s (highest for jitter-based)
- Output min-entropy density above 0.91 bit/bit over all voltage levels tested
- Best energy efficiency at 0.8 V supply: 1.46 pJ/bit

Conclusion



- ES architecture design, verification, and fabrication in a 28 nm technology compatible with modern standards
- Jitter pipelining allows for efficient entropy generation
- All-digital structure benefits scaling and design integration
- Stochastic model estimating generated output entropy
- On-chip jitter measurements
- Optimisation scheme guides parameter selection

Thank you for your attention

Design parameter selection criteria

- Four design parameters can be freely chosen: μ_{DC_0}, μ_{DC_1}, μ_{TDC_0} and μ_{TDC_1}
  - Represent DC, TDC oscillation frequencies
- Selection criteria:
  - Pipeline balance

$$res > \frac{P_{TDC_0} P_{TDC_1}}{2 \max(T_0^n, T_1^n)}. \tag{1}$$

  - Entropy density

$$res < \alpha \sqrt{F_{noise} \max(T_0^n, T_1^n)}, \tag{2}$$

  - Throughput

$$throughput = \frac{1}{\max(T_0^n, T_1^n)}. \tag{3}$$