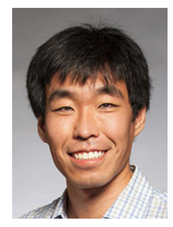
Computationally Enabled, Robust, Low-Power True Random Number Generation (TRNG)

Tyler Terhune, Akshat Boora, Xun Sun, Wenbing Zhang, Rajesh Pamula, Sung Min Kim, **Baosen Zhang** and **Visvesh Sathe**

Electrical and Computer Engineering, University of Washington



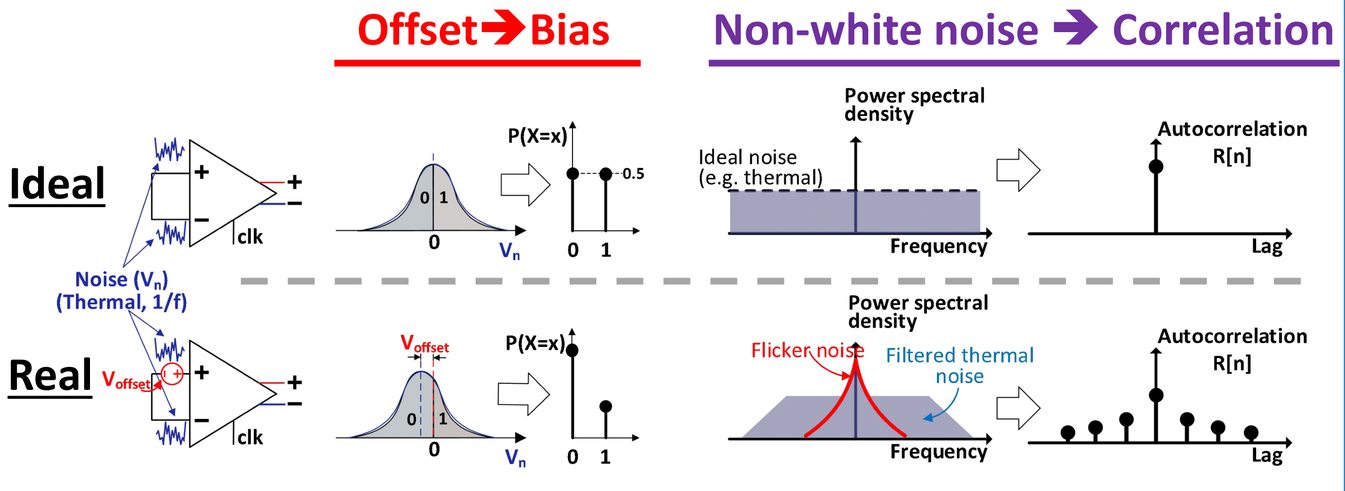
Key TRNG Metrics

- Randomness Quality (entropy rate H)
- Robustness (PVT/attack resistance)
- Efficiency (pJ/output-bit)
- Throughput/Bitrate (Gbps)

Existing Approach: Circuit Design Driven

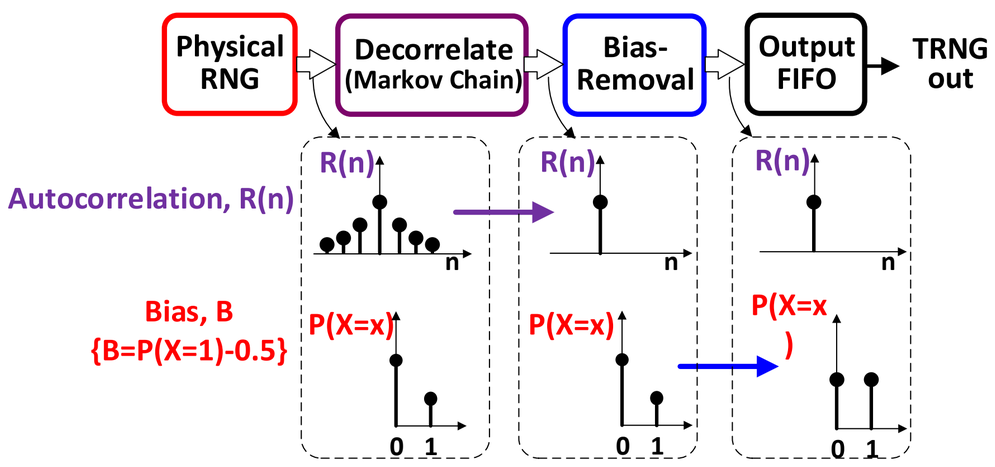
- Minimize bias B=P(X=1) - 0.5 (ideally 0)
- Autocorrelation ignored or an afterthought
- Fundamental limiter to Randomness
  - PVT Variation induced Bias
  - Finite Bandwidth, 1/f noise induced correlation between bits

Example: Metastability-based TRNGs



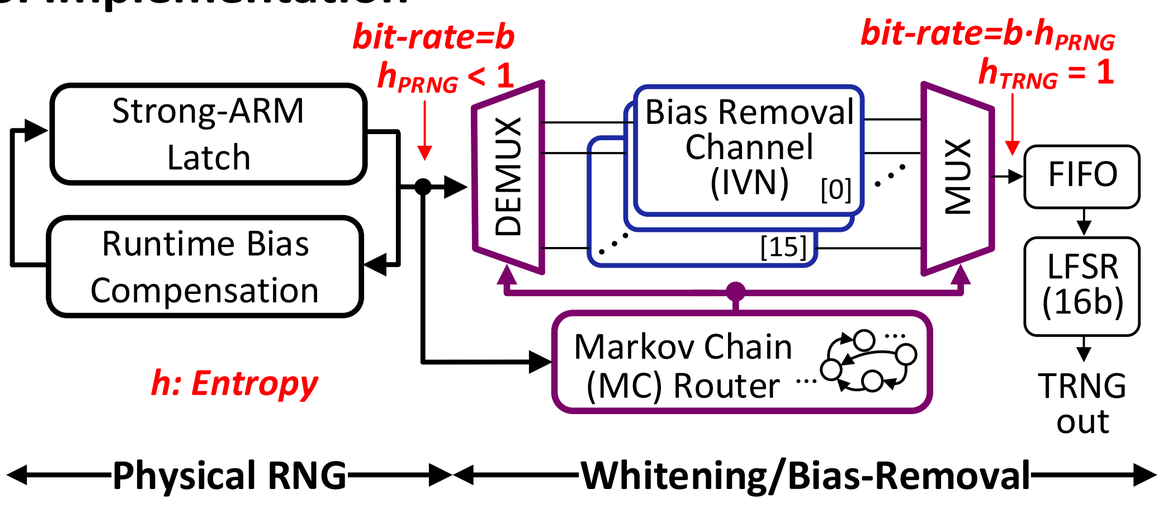
- Limit bias ➔µV resolution offset cancellation ➔ ↓robustness)
- Limit Correlation ➔ High bandwidth circuits ➔↑power, ↓ bitrate)
- No clear approach to address 1/f noise

Computationally enabled TRNG design[1,2]



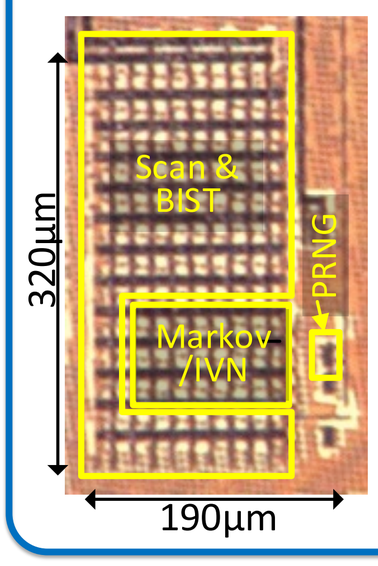
- Design "good-enough" physical RNGs (PhyRNGs)
- Integrated post-processing first whitens bitstream (correlation removal), then **<u>eliminates</u>** bias

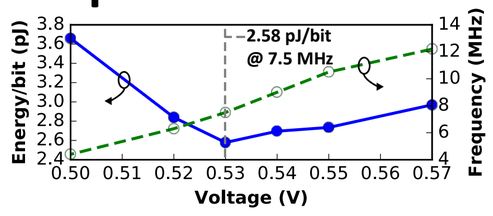
VLSI Implementation



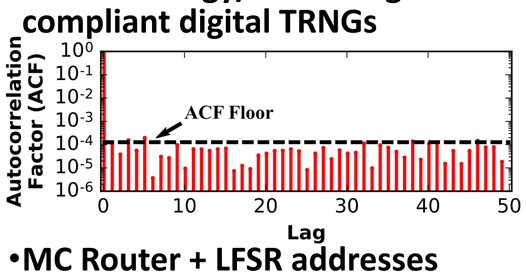
- MC whitening: Bits within channel have identical statistics
- Bias Removal using Iterative vonNeumann (IVN) correction[3]
- Whitening MUST precede IVN to better meet iid requirement

65nm CMOS Test-Chip Measurements

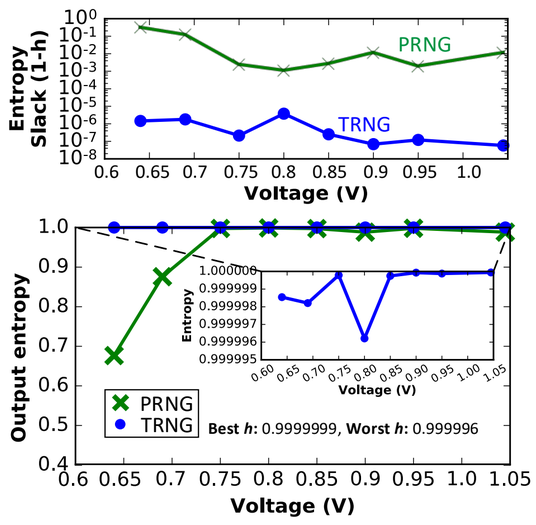




- **Lowest Energy/bit among NIST-compliant digital TRNGs**



- **MC Router + LFSR addresses bitstream autocorrelation**



- **PVT Robust. TRNG quality maintained despite Phy-RNG degradation**

Pass Rate for NIST Pub 800-22 Tests (All "PASS")*				
	Nominal		Min. Energy	
Voltage (V)	1.0		0.53	
Temperature (°C)	-20	100	-20	100
NIST benchmark				
Frequency	0.98	0.98	1.0	0.99
Block Frequency	1.0	1.0	0.99	1.0
Cumulative Sums	0.98	0.98	1.0	0.99
Runs	1.0	0.99	0.98	0.97
Longest Run	0.98	0.96	1.0	1.0
Rank	1.0	1.0	1.0	1.0
FFT	1.0	0.99	0.99	0.97
Non-Overlap. Template	0.98	0.98	0.98	0.97
Overlap. Template	0.98	1.0	0.99	1.0

NIST Pub 800-90B Entropy Assessment (All "PASS")	
Test	Results on 1Mb bitstream (score,DOF)
IID Permutation	PASS (NA,NA)
Chi-square Independence	PASS (1892, 2047)
Chi-square Goodness of fit	PASS (5.83, 9)
LRS Test	PASS (NA, NA)
Min. Entropy	0.996
Restart Test	PASS (NA, NA)
DOF: degrees of freedom, NA: Not applicable	

<u>NIST-Compliant</u>

- **Validated in the -20C-100C and 0.58V-1.0V range**

Challenges

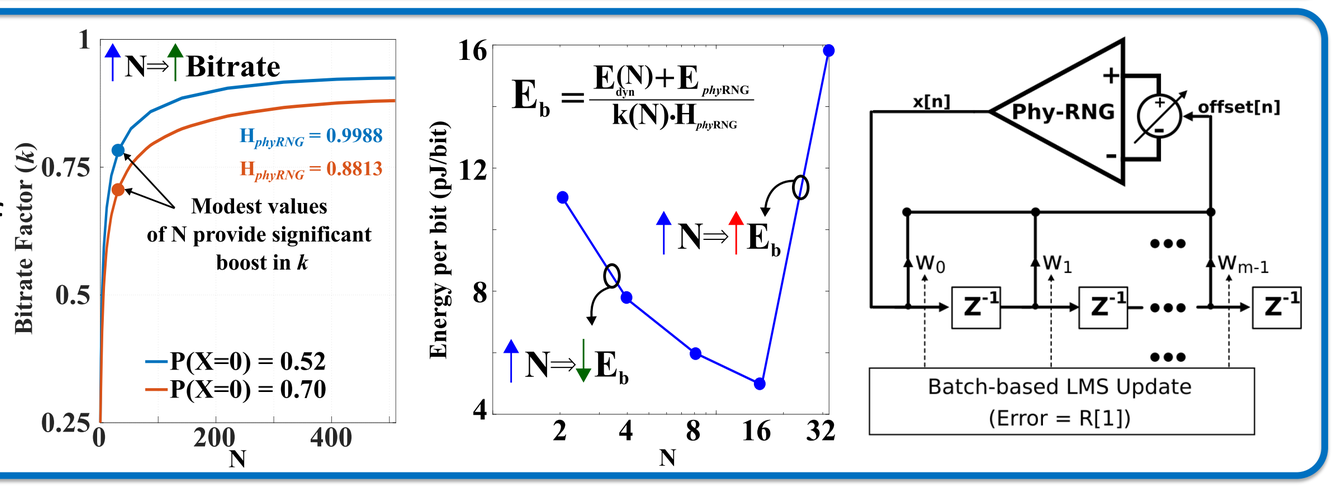
- Proposed TRNG architecture achieves quality, robustness, efficiency and bitrate
- Significant advance in correlation, **BUT** significant room for improvement
  - MC-Router does not scale well (2^n lanes required for lag-n decorrelation
  - MC-based whitening addresses stationary autocorrelation sources, not non-stationary ones (e.g. 1/f noise). LFSR still required to achieve robust NIST compliance

Broader Impact

- Robust and balanced architecture applicable broadly applicable across TRNG implementations: (FPGA/ASIC/SoCs)
- Findings covered as part of a week-long module in the Advanced VLSI design course at the University of Washington

Future Work

- **<u>Adaptive</u>** TRNGs
- Runtime trade-off management for optimal quality and efficiency



References

1.V. Pamula et al., "An all-digital true-random-number generator with integrated de-correlation and bias correction at 3.2-to-86 Mb/s, 2.58 pJ/bit in 65-nm CMOS", *In 2018 IEEE Symposium on VLSI Circuits 2018,* Jun. 18

2.V. Pamula et al.,"A 65-nm CMOS 3.2-to-86 Mb/s 2.58 pJ/bit Highly Digital True-Random-Number Generator With Integrated De-Correlation and Bias Correction." IEEE Solid-State Circuits Letters. 2018 Dec;1(12);237-240

3.Y. Peres "Iterating Von Neumann's Procedure for Extracting Random Bits", *The Annals of Statistics*. 20. 10.1214/aos/1176348543.