A Comparative Study of Cryptographically Secure Random Number Generators

Felicia Guo, Jingyi Xu
EE241B Final Project
May 6, 2021

Berkeley
UNIVERSITY OF CALIFORNIA

Overview

- Background
- PRNG vs TRNG
  - Blum Blum Shub
  - TRNG with Markov Chain de-correlation and IVN bias correction
- Results
- Summary

Berkeley
UNIVERSITY OF CALIFORNIA

Background

- Increasing need for (cryptographically secure) random numbers
  - Private data transfers
- How do we generate random numbers?
  - True random: use device noise as entropy source
    - Need debiasing
  - Pseudorandom: take a seed and run it through algorithms
    - Has limited period
    - Easier to predict
- How do we know if a stream of numbers is ‘random’?
  - Statistical tests
- How do we know if it’s cryptographically secure?
  - Next-bit test: there is no polynomial time algorithm which, given the first L bits of the output sequences, can predict the L+1th bit with a probability significantly greater than 50%

Berkeley
UNIVERSITY OF CALIFORNIA

Blum Blum Shub

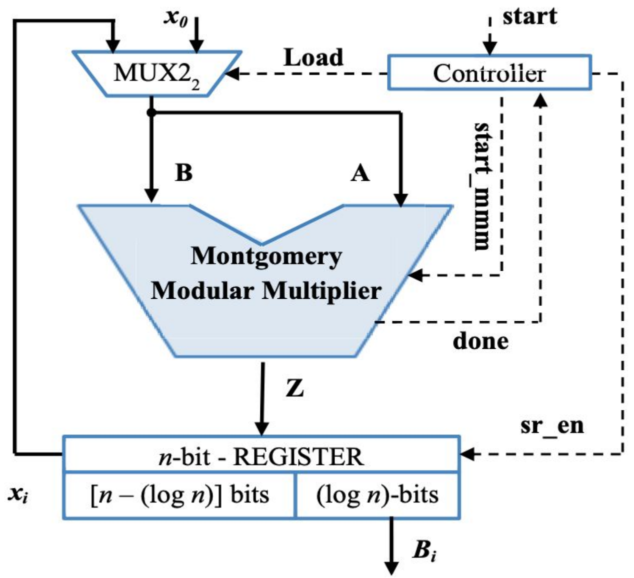
- Find M

$$M = p \cdot q$$
$$p = 4p1 + 3$$
$$q = 4q1 + 3$$

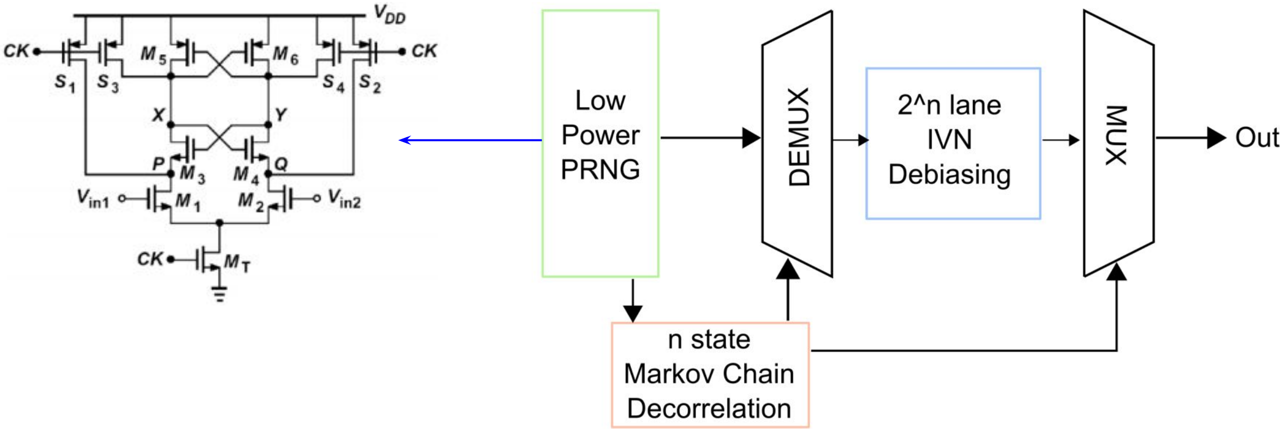
- Find seed: gcd(seed, M) = 1
- Repeat:

$$x_{n+1} = x_n^2 \, mod \, M$$

- Can use least significant $\log_2(\log_2 M)$ bits for output



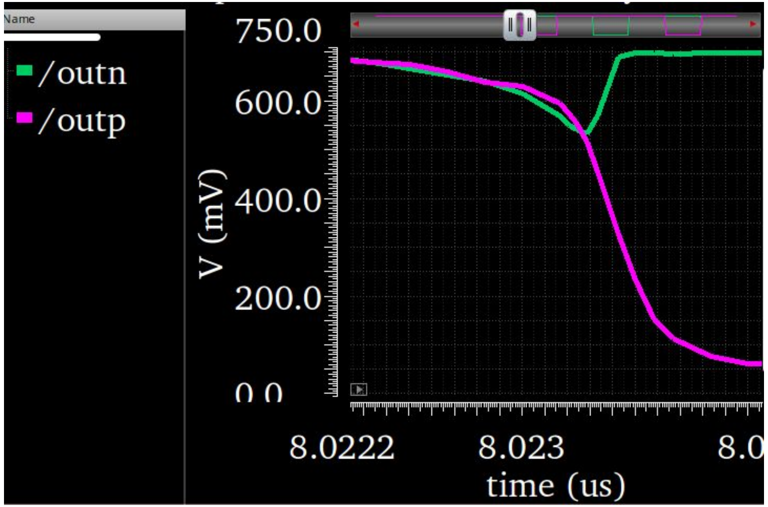
TRNG - Overview



- Input bitstream produced by strongARM latch utilizing noise
- Shift register “Markov Chain” assigns bits to IVN lane based on past bit history

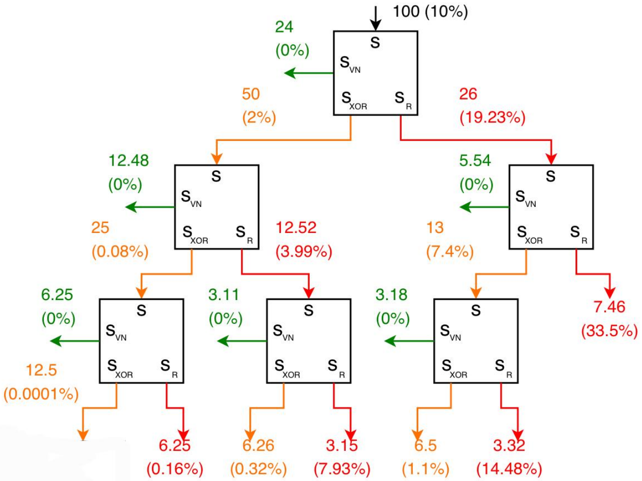
TRNG - StrongARM Bit Generation

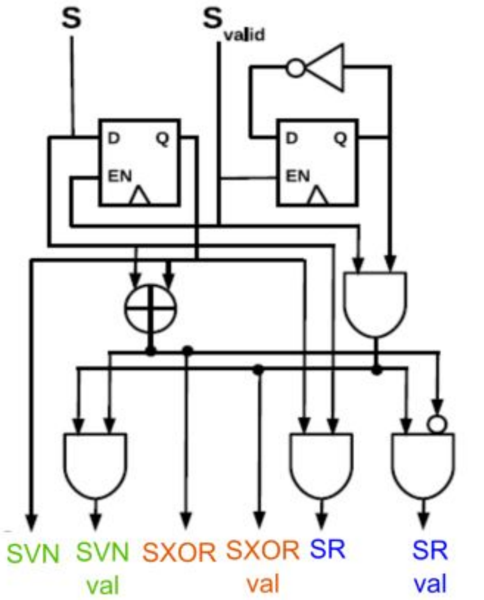
- Set outputs to same voltage
- Use device noise to differentiate outputs in strongARM
- Tested for VDD of 0.63V, 0.7V, 0.77V



TRNG - Iterative Von Neumann Debiasing

- Extracts entropy from input sequence by discarding sequences of all 1s or all 0s
- Iterative tree to limit hit to throughput from bit discarding



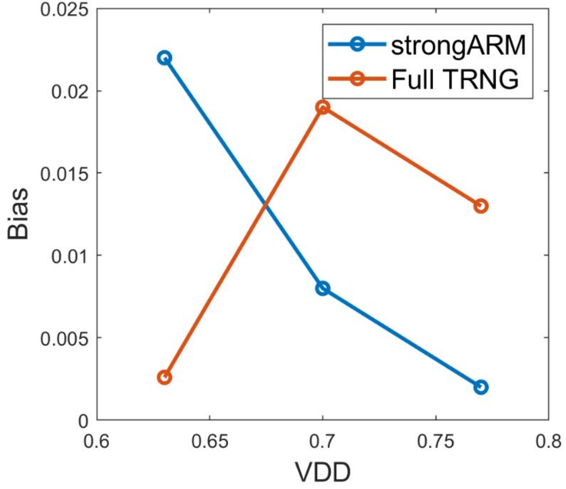


S	10	11	01	10	00	01	11	10	10	10
SVN	0		1	0		1		0	0	0
SXOR	1	0	1	0	0	1	0	1	1	1
SR		1			0		1			

Berkeley
UNIVERSITY OF CALIFORNIA

Results - Statistical Quality

- Post processing potentially helps with bias in TRNG (below)
- NIST SP 800-22 test results on right



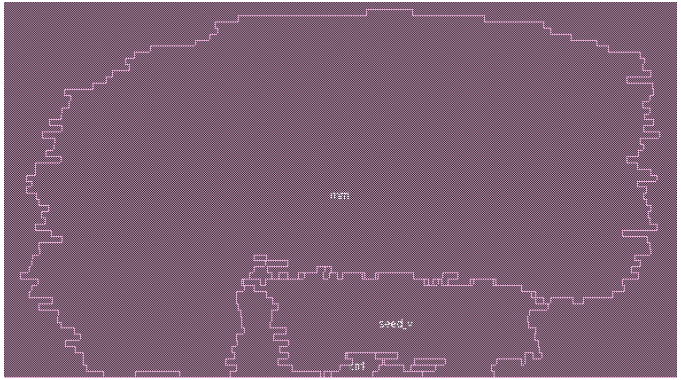
	Pass Rate	
	BBS	TRNG
Runs	10/10	8/10
Block Frequency	10/10	10/10
Approx. Entropy	10/10	8/10
FFT	9/10	10/10
Serial	10/10	10/10

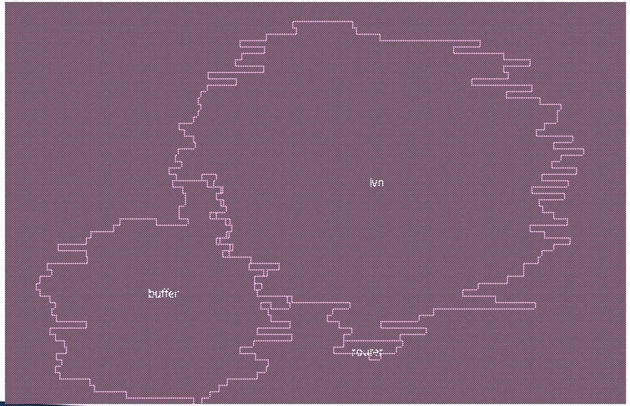
Berkeley
UNIVERSITY OF CALIFORNIA

Results-Area

Area in um^2

BBS		TRNG	
Modular multiplier	3112.18	IVN	1757.06
Seed validation	646.18	Buffer	715.46
Control	30.55	MC router	32.19
Total	4153.55	Total	2535.28





Results-Power & Throughput

Power in mV

	BBS	TRNG
Internal	0.551	0.273
Switching	0.956	0.225
Leakage	0.167	0.079
Internal	1.675	0.577

	BBS	TRNG
Max clock frequency(GHz)	0.66	1.25
bitrate(Gbit/s)	1.332	1.25

Berkeley
UNIVERSITY OF CALIFORNIA

Summary

- It’s a trade-off
  - BBS has better bit statistical quality
  - TRNG has better energy and area efficiency
  - Comparable throughput
- Next steps:
  - More extensive testbenches with at least 100 runs and longer bitstreams
  - Better sources of colored noise to test the debiasing capabilities of IVN

Berkeley
UNIVERSITY OF CALIFORNIA