A Robust True Random Number Generator Using Voltage-Controlled MTJ in 65nm CMOS

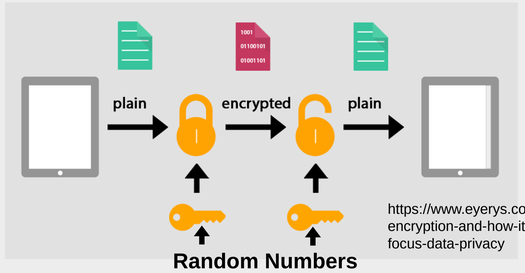
Jiyue Yang, Di Wu, Albert Lee, Seyed Armin Razavi, Puneet Gupta, Kang L. Wang, Sudhakar Pamarti, University of California, Los Angeles.

ERI SUMMIT & MTO Symposium 2020 | Seattle, WA | August 18-20

Foundation Required for Novel Compute (FRANC)

Security and Access

Background



https://www.eyerys.com/articles/end-end-encryption-and-how-it-highlights-growing-focus-data-privacy

A True Random Number Generator (RNG) has several applications:

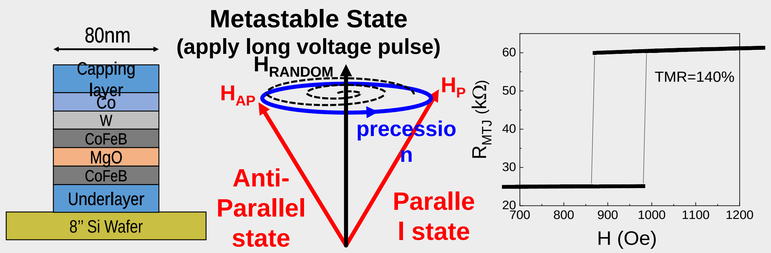
- As secret keys for data encryption, communications, digital content protection
- As random bit streams for a non-von Neumann (stochastic) computing architecture

Requirements

- Highly random, independent, entropy source
- Low energy, high density

Approach

Voltage-Controlled Magnetic Tunneling Junction (VC-MTJ) as Entropy Source

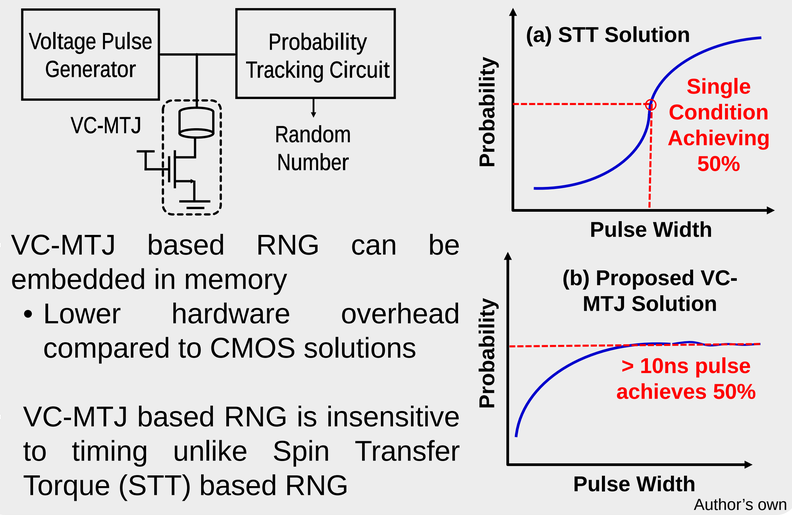


VC-MTJ Film Stack | Precessional Switching | Hysteresis Loop

Author's own

- VC-MTJ's magnetic (H) field exhibits damped precession upon voltage application
  - After precession, thermal noise randomly switches the H field into a parallel (P) or anti-parallel (AP) state with equal probability
  - Effectively, a 1 or 0 is randomly stored in the VC-MTJ
- H-field switching offers low energy, high density random number generation
- True RNG unlike pseudorandom number generators

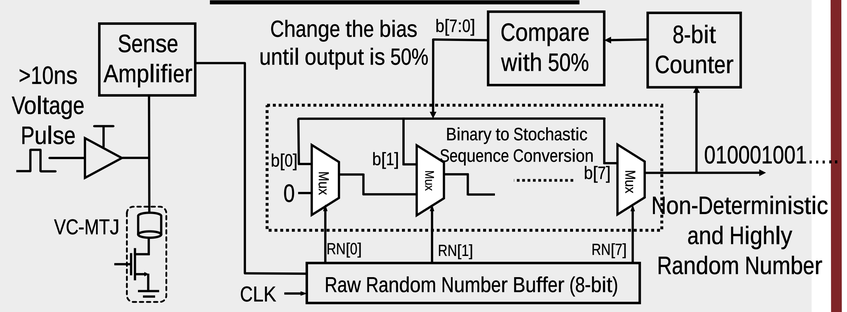
Comparison to Prior State-of-the-Art



- VC-MTJ based RNG can be embedded in memory
  - Lower hardware overhead compared to CMOS solutions
- VC-MTJ based RNG is insensitive to timing unlike Spin Transfer Torque (STT) based RNG

Author's own

VC-MTJ based RNG



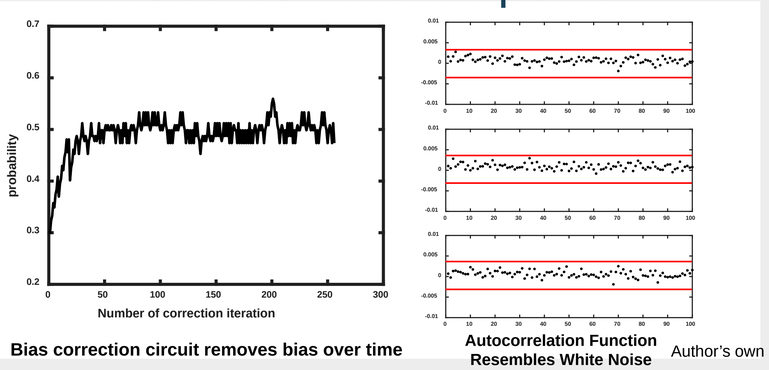
Raw Random Numbers from VC-MTJ

Monitor Probability and Remove Any Bias

Author's own

- VC-MTJ generates raw random numbers
- Lightweight bias correction circuit removes any bias
- Can be embedded into a dense memory array for efficient random vector generation

Results and Impact



Author's own

Results and Impact

	NIST 800-22 Test	MTJ1	MTJ 2	MTJ 3
		Pass Rate	Pass Rate	Pass Rate
1	Frequency	100%	100%	100%
2	Block Frequency	100%	100%	100%
3	Cumulative Sum	100%	100%	100%
4	Runs	97.5%	95%	95%
5	Longest Run	97.5%	100%	100%
6	Rank	100%	100%	100%
7	FFT	95%	100%	95%
8	Nonoverlap Template	Pass	Pass	Pass
9	Overlap Template	95%	95%	Pass
10	Universal	95%	100%	95%
11	Approximate Entropy	97.5%	100%	95%
12	Random Excursion	Pass	Pass	Pass
13	Random Excursion Variant	Pass	Pass	Pass
14	Serial	100%	100%	100%
15	Linear Complexity	97.5%	95%	95%

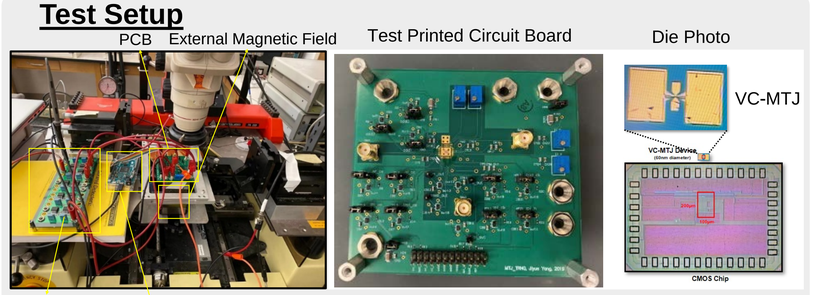
1) 90% pass rate is required to be qualified as random.
2) Pass means that the tests of all subcategories are passed

Multiple VC-MTJs pass National Institute of Standards and Technology (NIST) randomness tests

Author's own

Impact: Enable VC-MTJ's application to cryptography and for a non-von Neumann (stochastic) computing architecture

Test Setup



Author's own

Comparison to Prior State-of-the-Art

	This Work		VLSI' 18, [5]	IEDM'14, [4]	VLSI'11, [3]
	With VC-MTJ Wire bonded to CMOS Chip	Expected After VC-MTJ Integrated with CMOS			
Entropy Source	VC MTJ Switching		STT MRAM Switching Time	STT MRAM Switching	Soft Oxide Breakdown
Technology	65nm		28nm	Not Integrated	65nm
Endurance	> 10^12 (Expected)		N/A	N/A	N/A
MRAM Density(μm^2/bit)	$0.02\mu m^2$		$0.05\mu m^2$ [1]*	$0.05\mu m^2$ [1] *	N/A
Robust to H Field Attack	Yes		N/A	N/A	N/A
Bit Rate (Mb/s)	0.4	100	66	N/A	0.011
Energy/Bit	135pJ/bit	6.7pJ/bit	18pJ/bit	N/A	181810pJ/bit
Area(μm^2)	2600	200	180	0.0085 (MTJ Size)	1200
NIST Test	ALL		ALL	10	ALL

[1] L. Wei, et al., *ISSCC*,2019.

Author's own

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.
Distribution Statement A – Approved for Public Release, Distribution Unlimited.