2020 Research Day

STT-ANGIE: Asynchronous True Random Number Generator using STT-MTJ

Ben Perach, Shahar Kvatinsky

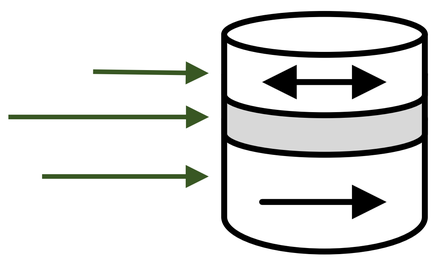
1. TRNG: True Random Number Generator

- Generates secret cryptographic keys
- Based on a physical random process

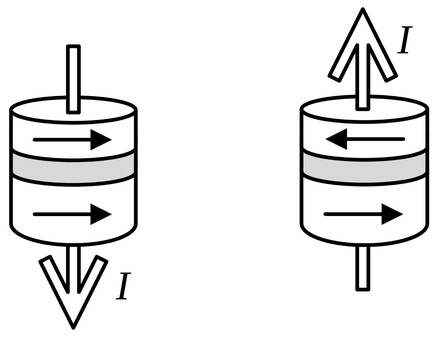
2. STT-MTJ: Spin Transfer Torque Magnetic Tunnel Junction

- Composed of three layers:

1. **Free:** dynamic magnetization direction
2. **Barrier:** Creating potential barrier
3. **Fixed:** fixed magnetization direction



P - Parallel AP - Anti Parallel

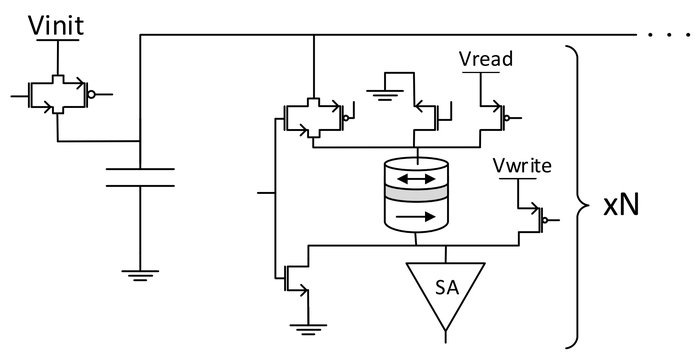


- Two stable states: P & AP
- State depended resistance:

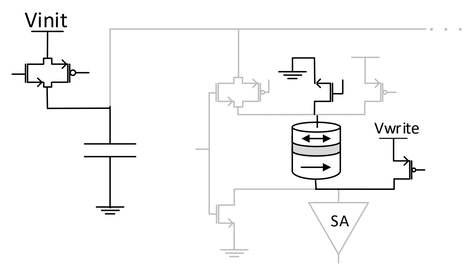
$$R_P < R_{AP}$$

- Physically modeled by stochastic differential equations

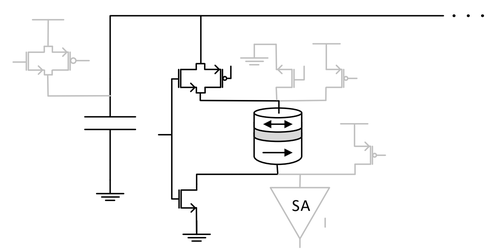
3. Proposed TRNG



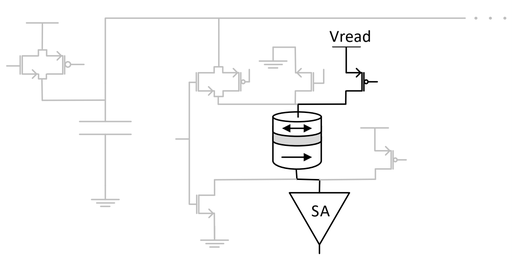
1. Reset step: Charge capacitor. Switch MTJs to AP



2. Enable step: Discharge capacitor parallelly through all MTJs for a constant time. The MTJs will switch with some probability



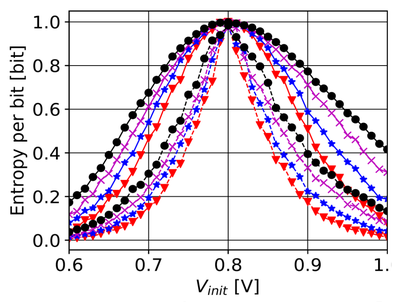
3. Read step: Read the state of the MTJs

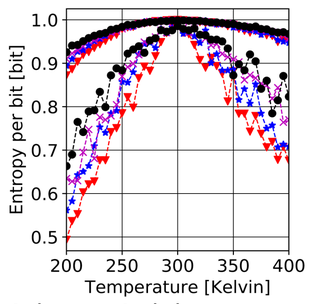


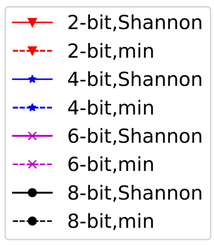
Enable step time does not have to be accurate

- When the capacitor is discharged the MTJs will not switch
- Enables to embed in low-frequency (low-power) devices

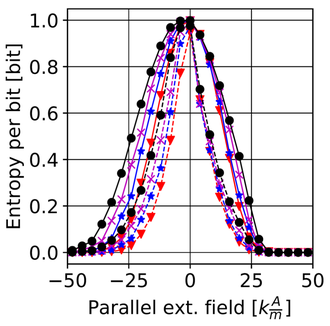
4. Entropy Simulations Results

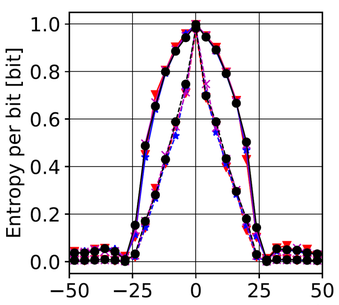


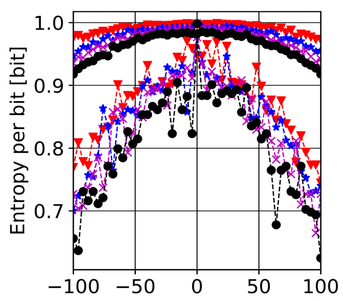




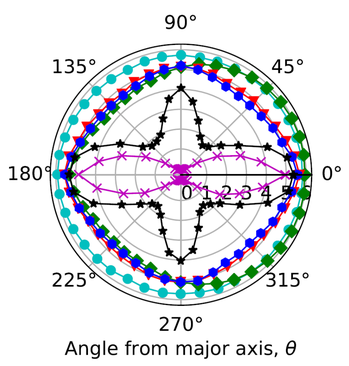
- External magnetic field with variable magnitude:

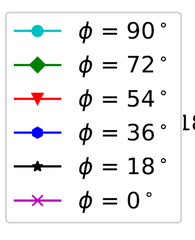


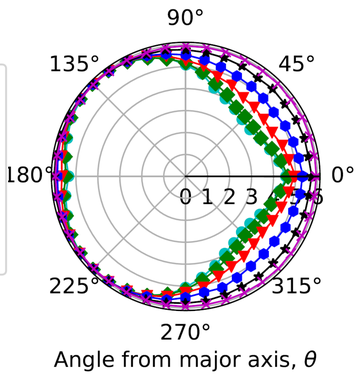




- External magnetic field with variable direction and frequency on 6-bit TRNG:







5. Process Variation [Entropy per bit]

N	Average	Standard Deviation	Median	10th percentile
2	0.74	0.19	0.76	0.46
4	0.79	0.12	0.80	0.4
6	0.82	0.08	0.83	0.72
8	0.86	0.06	0.86	0.78

6. Rate, Power & Area

	Entropy Rate [Mb/s]	Area [μm^2]	Energy [pJ/bit]
2-bit	16.2-35.1	402	8.4-18.3
4-bit	43.1-67.3	404	6.8-10.6
6-bit	70.6-98.0	406	6.3-8.7
8-bit	**99.7-127.8**	**408**	**6-7.7**
Yang et al.	23.16	375	23
Srinivansan et al.	2400	4004	2.9

Conclusion:

High entropy rate & low energy for the given area

Yang *et al.*, "16.3 A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS", ISSCC'14
Srinivasan *et al.*, "2.4GHz 7mW All-Digital PVT-Variation Tolerant True Random Number Generator in 45nm CMOS", VLSIC'10