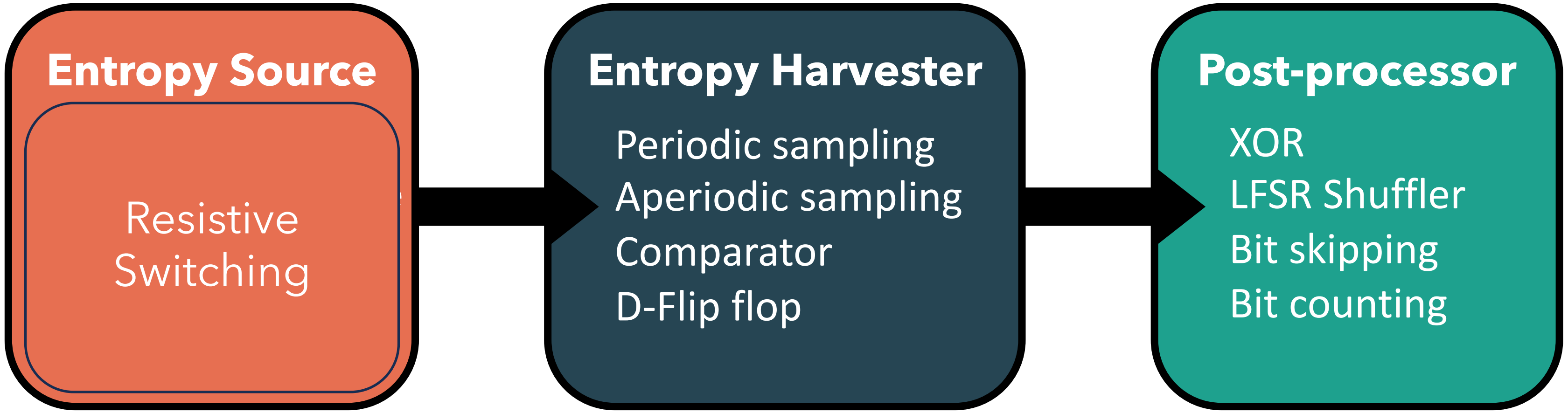
Generating Random Numbers with Emerging Memory Devices

Elena Ioana Vãtãjelu
CR CNRS

Basic PTRNG Representation



Entropy Source

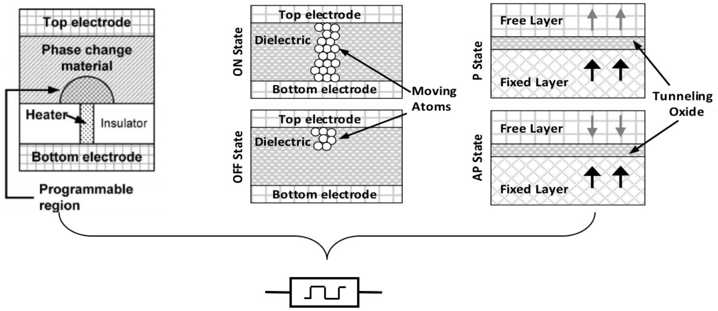
Resistive Switching

Entropy Harvester

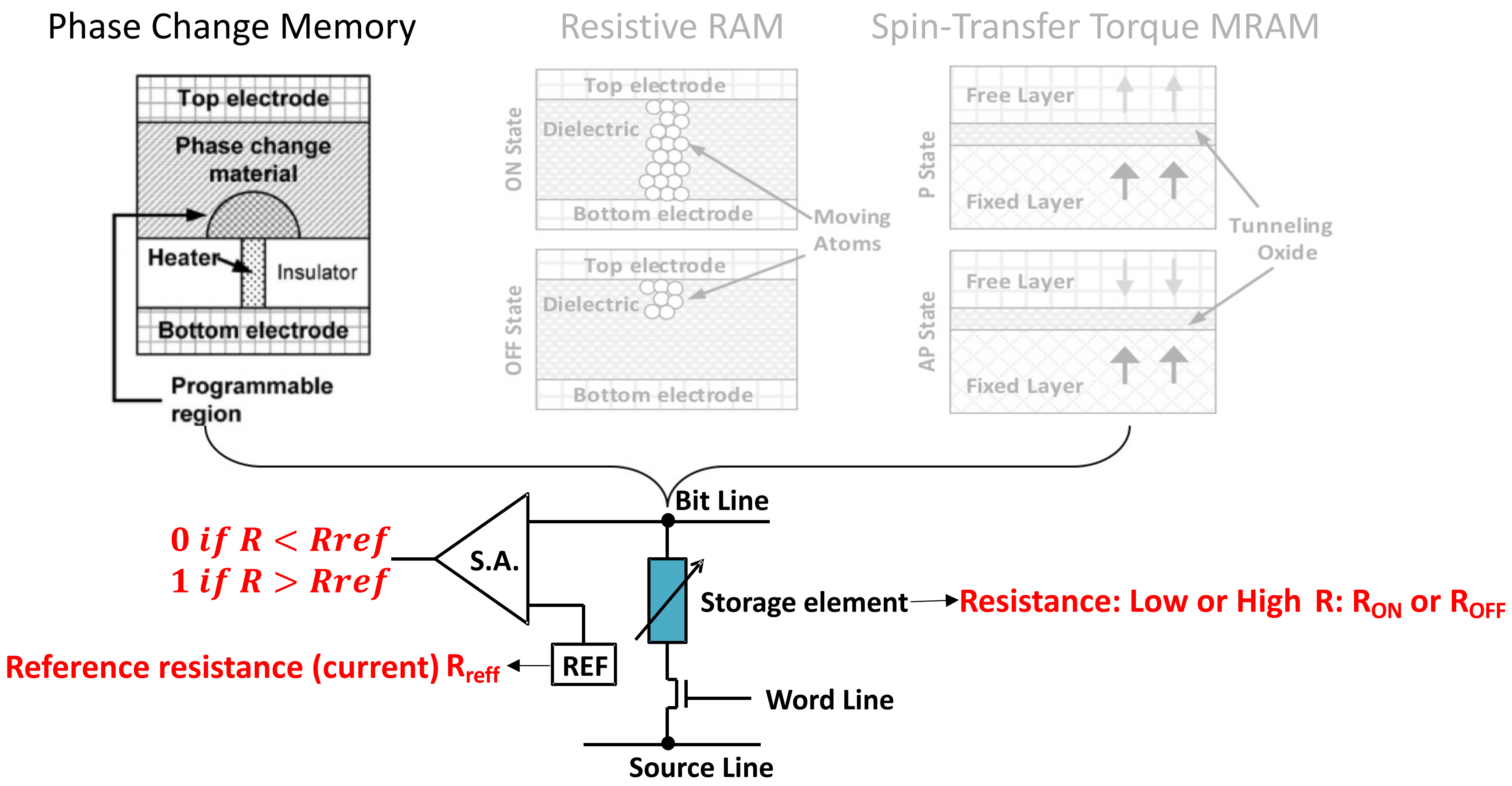
- Periodic sampling
- Aperiodic sampling
- Comparator
- D-Flip flop

Post-processor

- XOR
- LFSR Shuffler
- Bit skipping
- Bit counting



Presentation Outline



Phase Change Memory

Resistive RAM

Spin-Transfer Torque MRAM

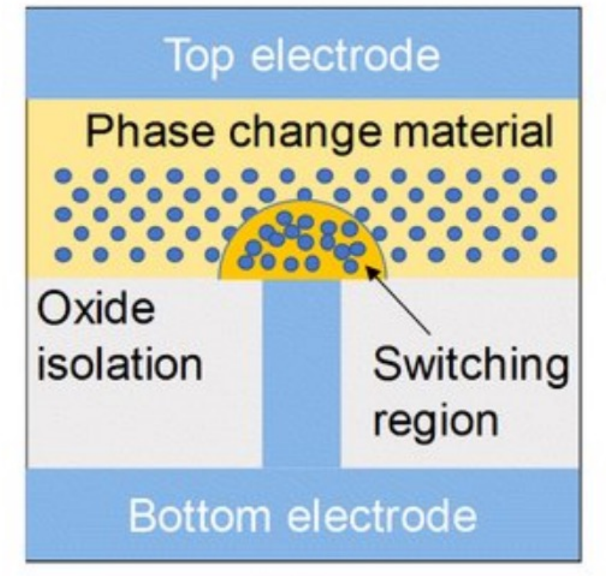
$0\ if\ R < Rref$

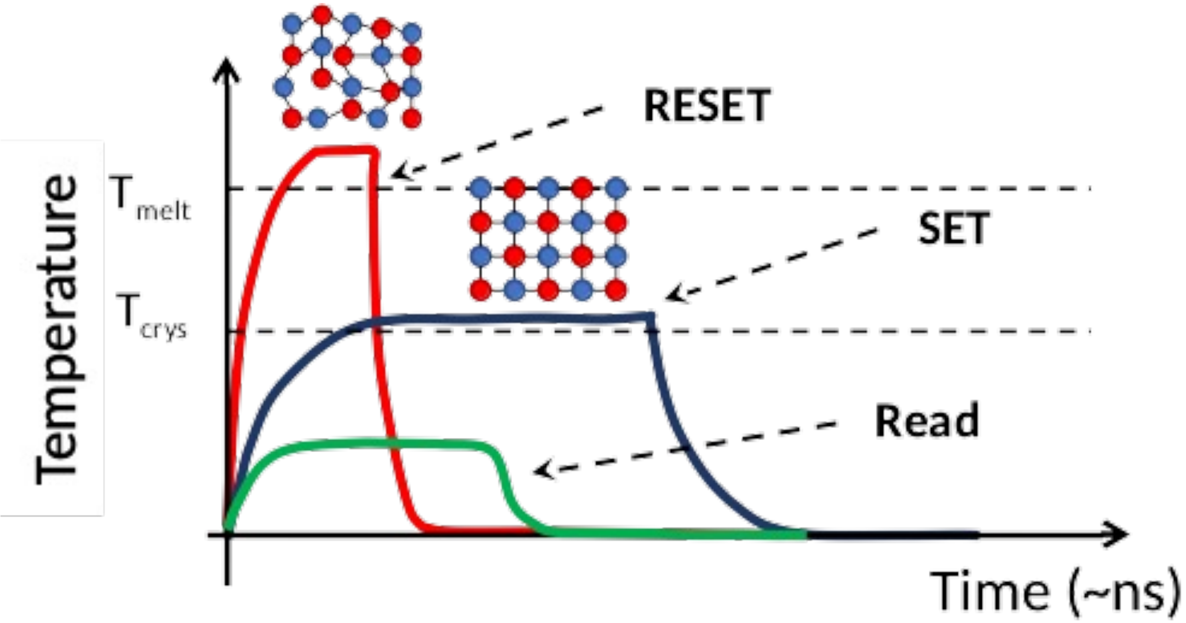
$1\ if\ R > Rref$

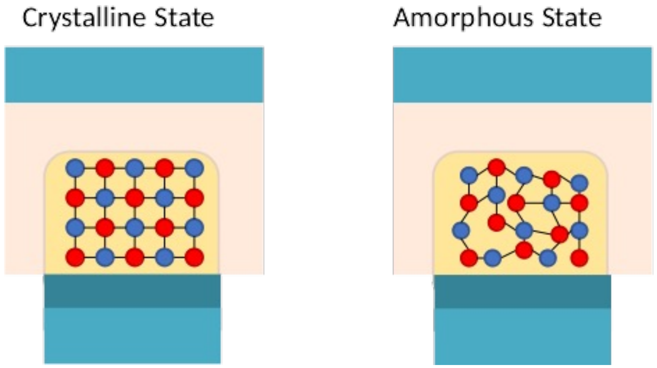
Resistance: Low or High R: R_{ON} or R_{OFF}

Reference resistance (current) R_{reff}

PCM (Phase Change Memory)







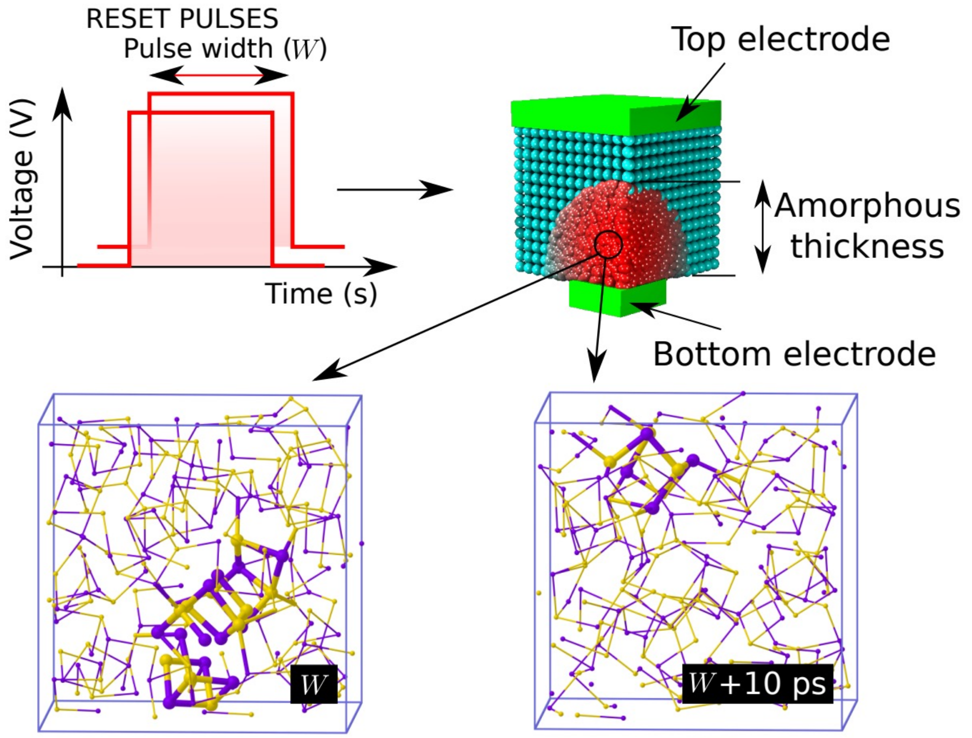
◆ Electrode

◆ Heater

◇ Chalcogenide Glass (GeSbTe)

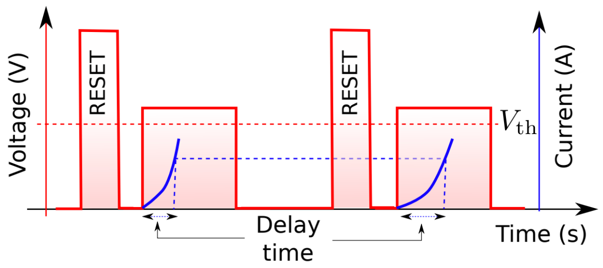
◆ Programmable Volume

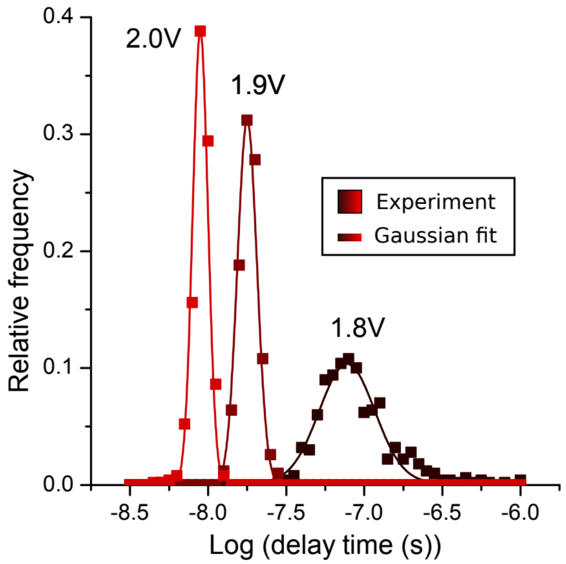
PCM (Phase Change Memory)
- Stochasticity -



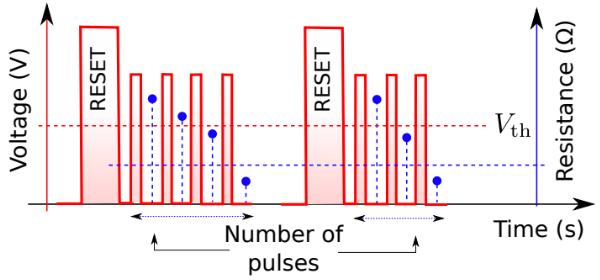
Cycle-to-cycle variation of the thickness and atomic configuration of the amorphous state

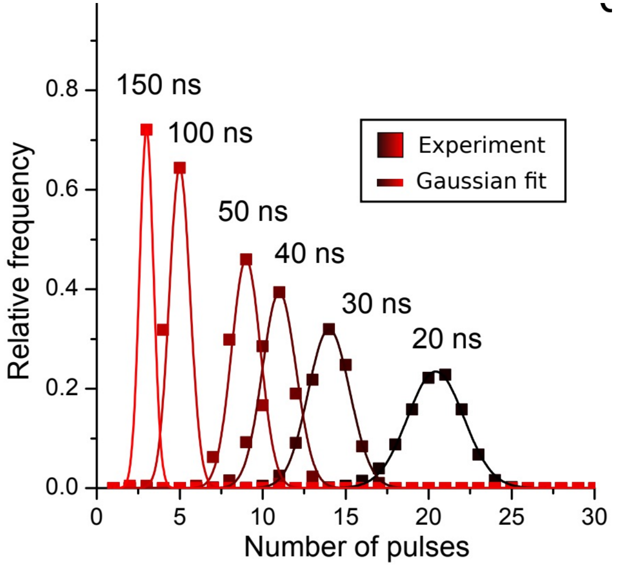
Threshold Switching





Memory Switching

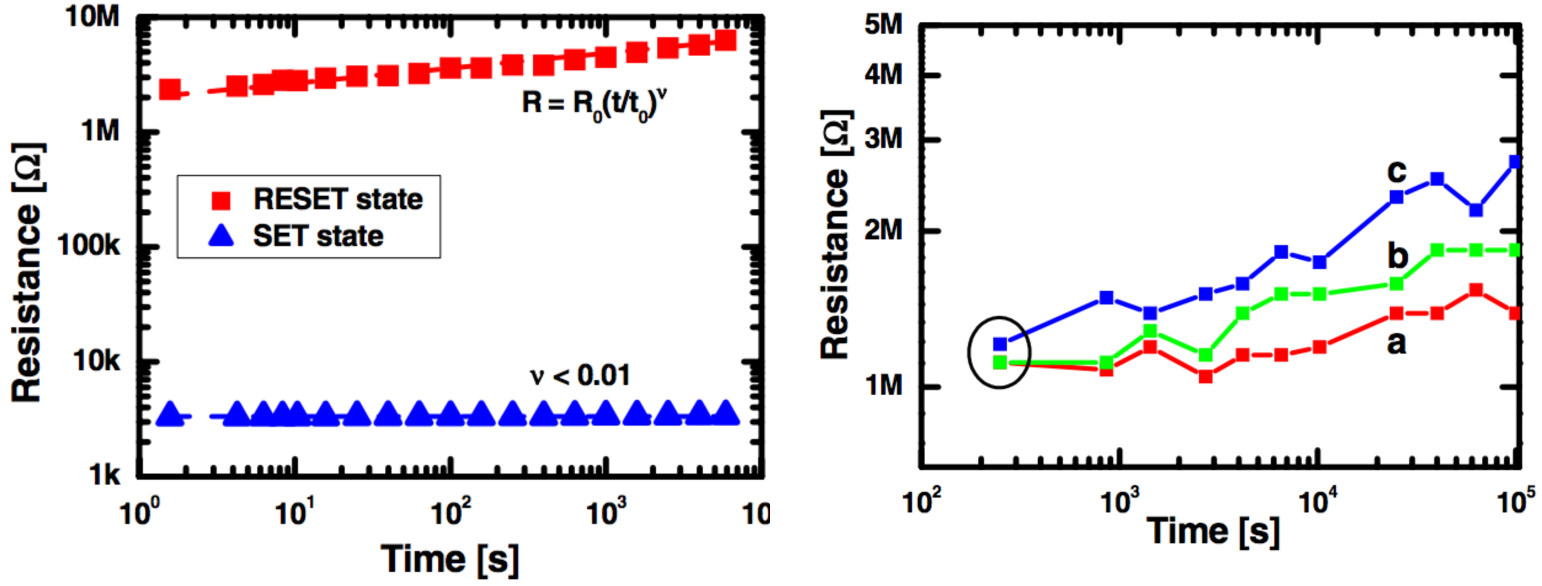




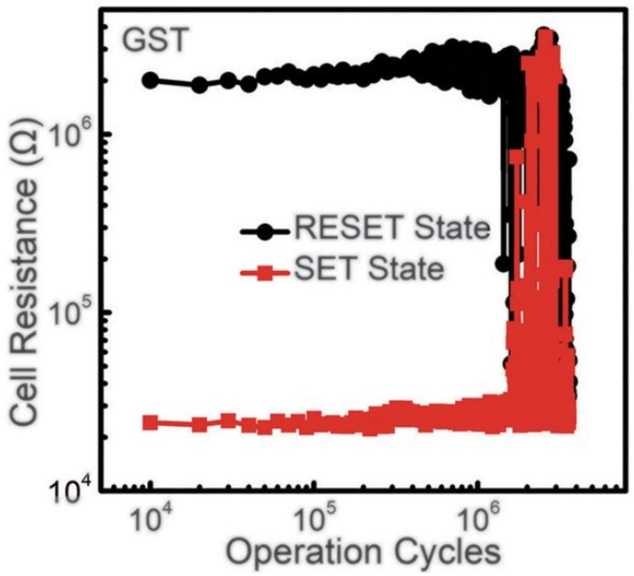
M. Le Gallo, T. Tuma, F. Zipoli, A. Sebastian and E. Eleftheriou, "Inherent stochasticity in phase-change memory devices," *2016 ESSDERC*, Lausanne, Switzerland, 2016

PCM (Phase Change Memory)
- Issues -

Resistance Drift

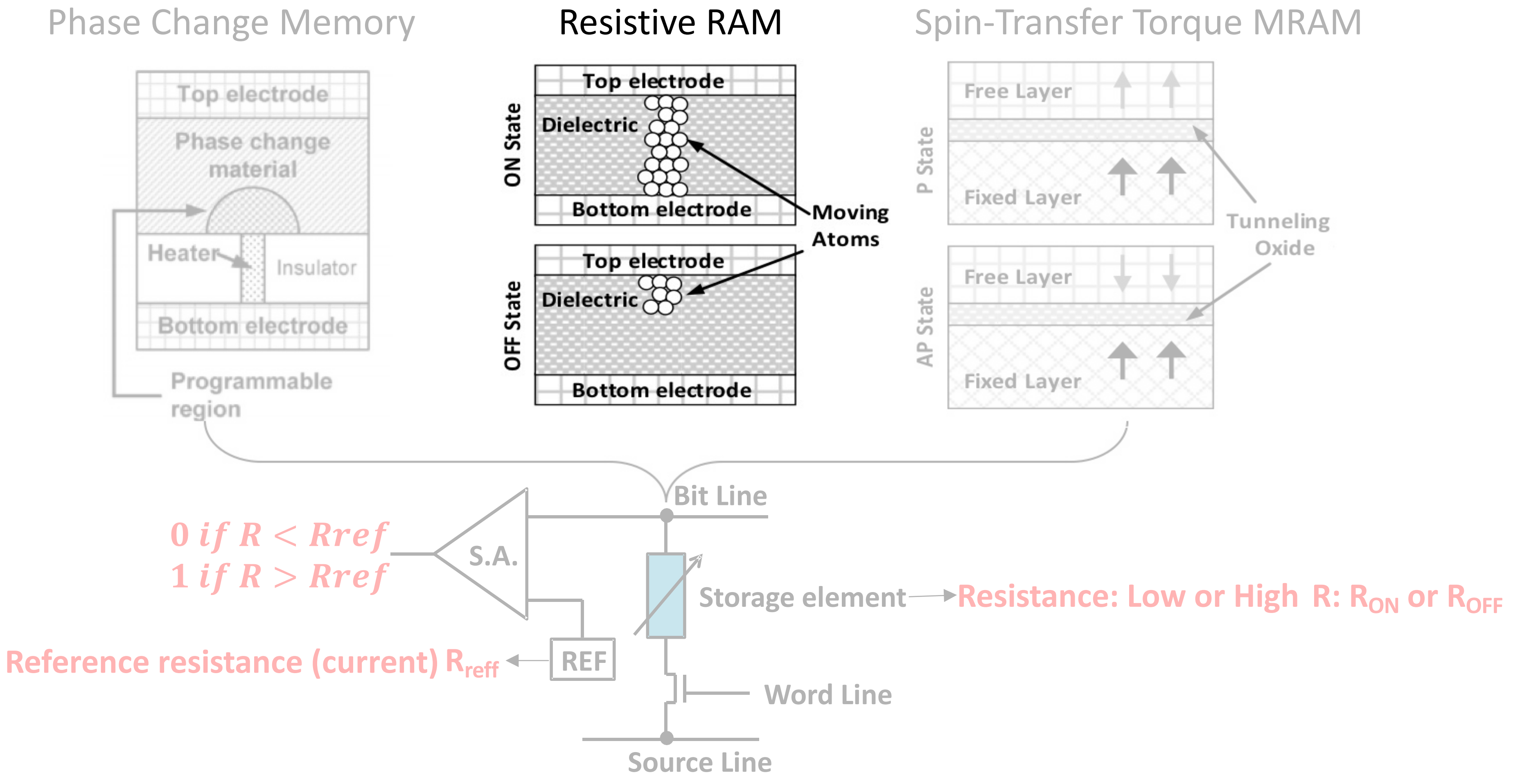


Cycling endurance



Keyuan Ding et al., Phase-change heterostructure enables ultralow noise and drift for memory operation.*Science*, 366,210-215(2019)
Boniardi, Mattia et al. “Statistics of Resistance Drift Due to Structural Relaxation in Phase-Change Memory Arrays.” IEEE Transactions on Electron Devices 57 (2010): 2690-2696.

Presentation Outline



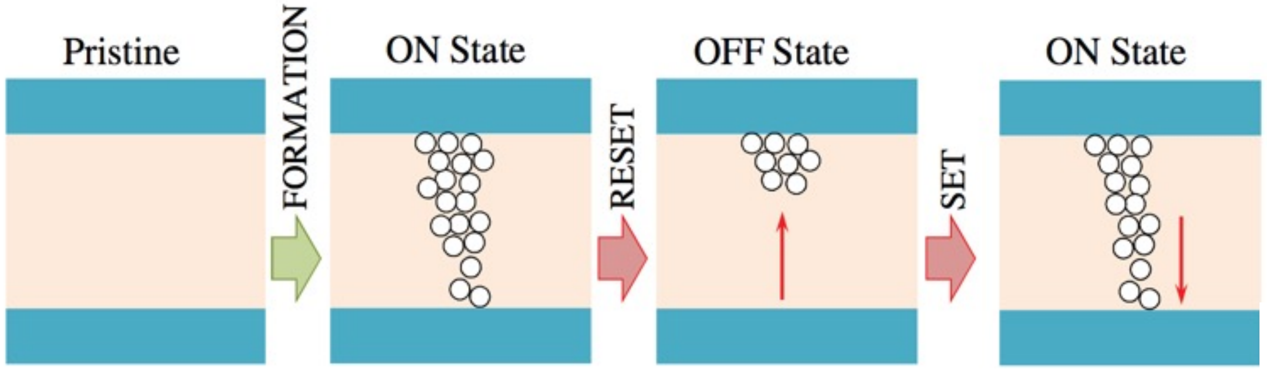
$0\ if\ R < Rref$

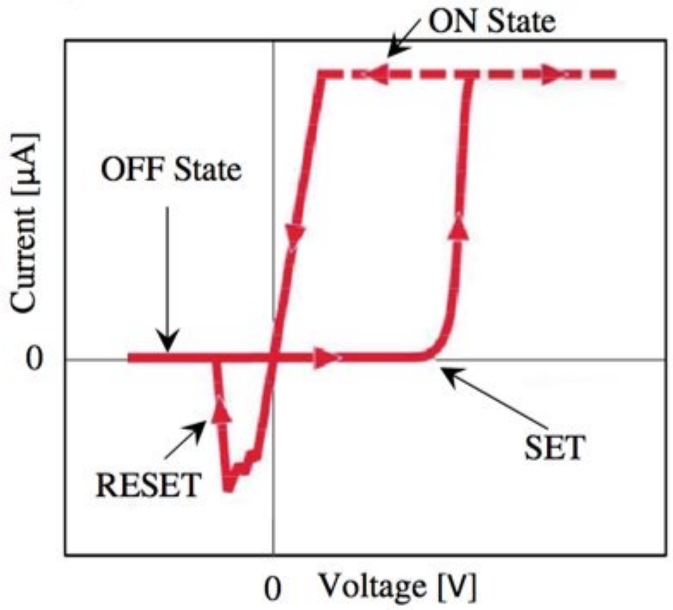
$1\ if\ R > Rref$

Storage element → Resistance: Low or High R: R_{ON} or R_{OFF}

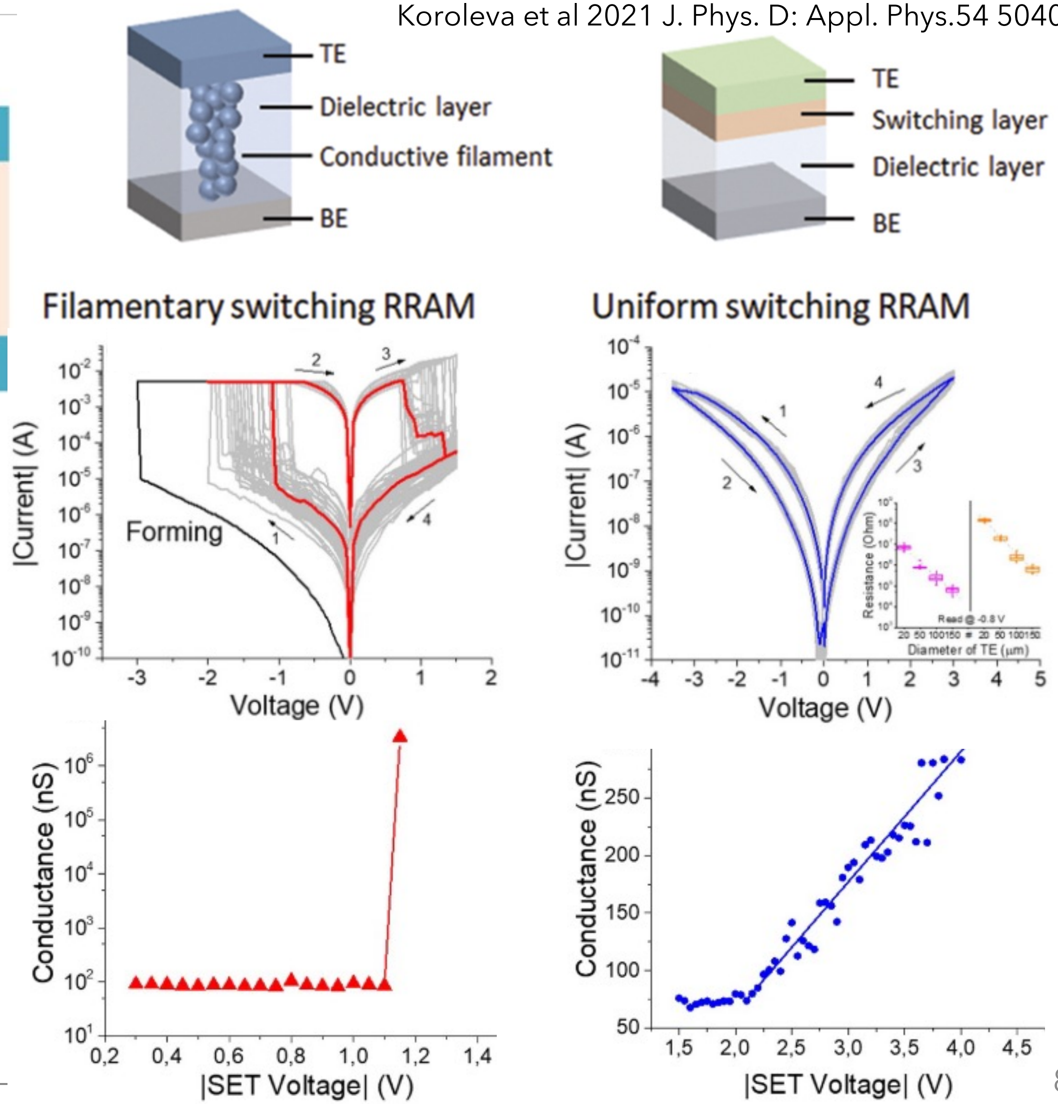
Reference resistance (current) R_{reff} ← REF

RRAM (Resistive Memory)

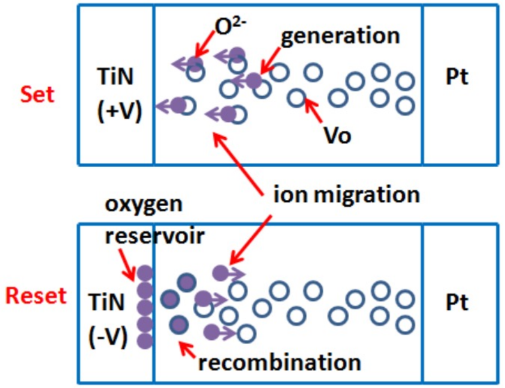


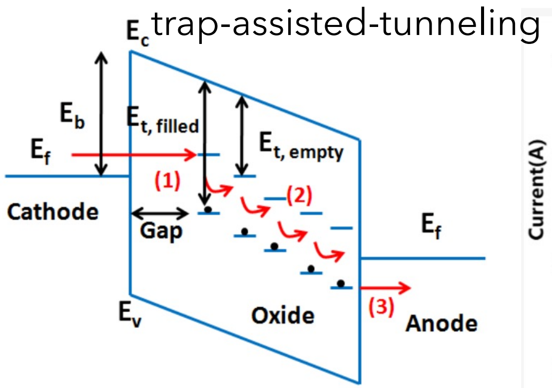


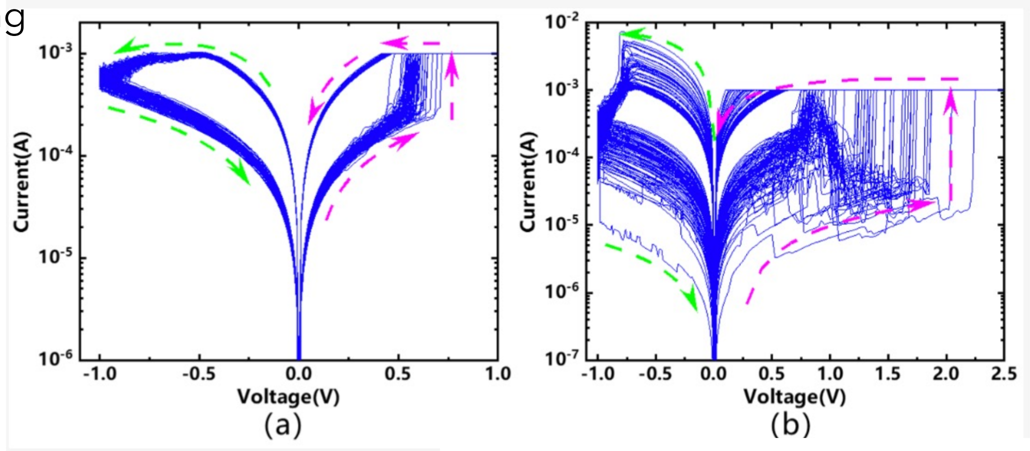
Koroleva et al 2021 J. Phys. D: Appl. Phys.54 504004



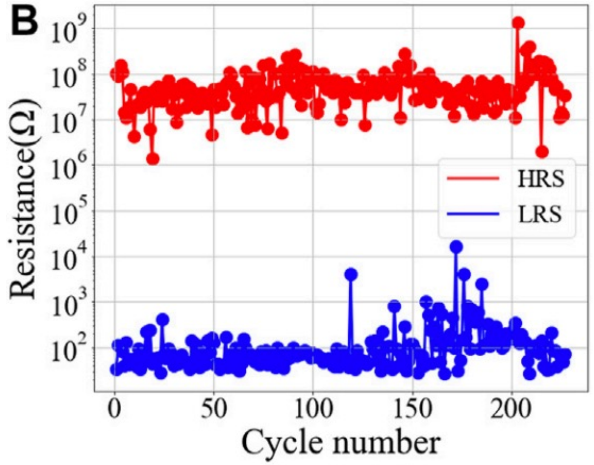
RRAM (Resistive Memory) - Stochasticity -







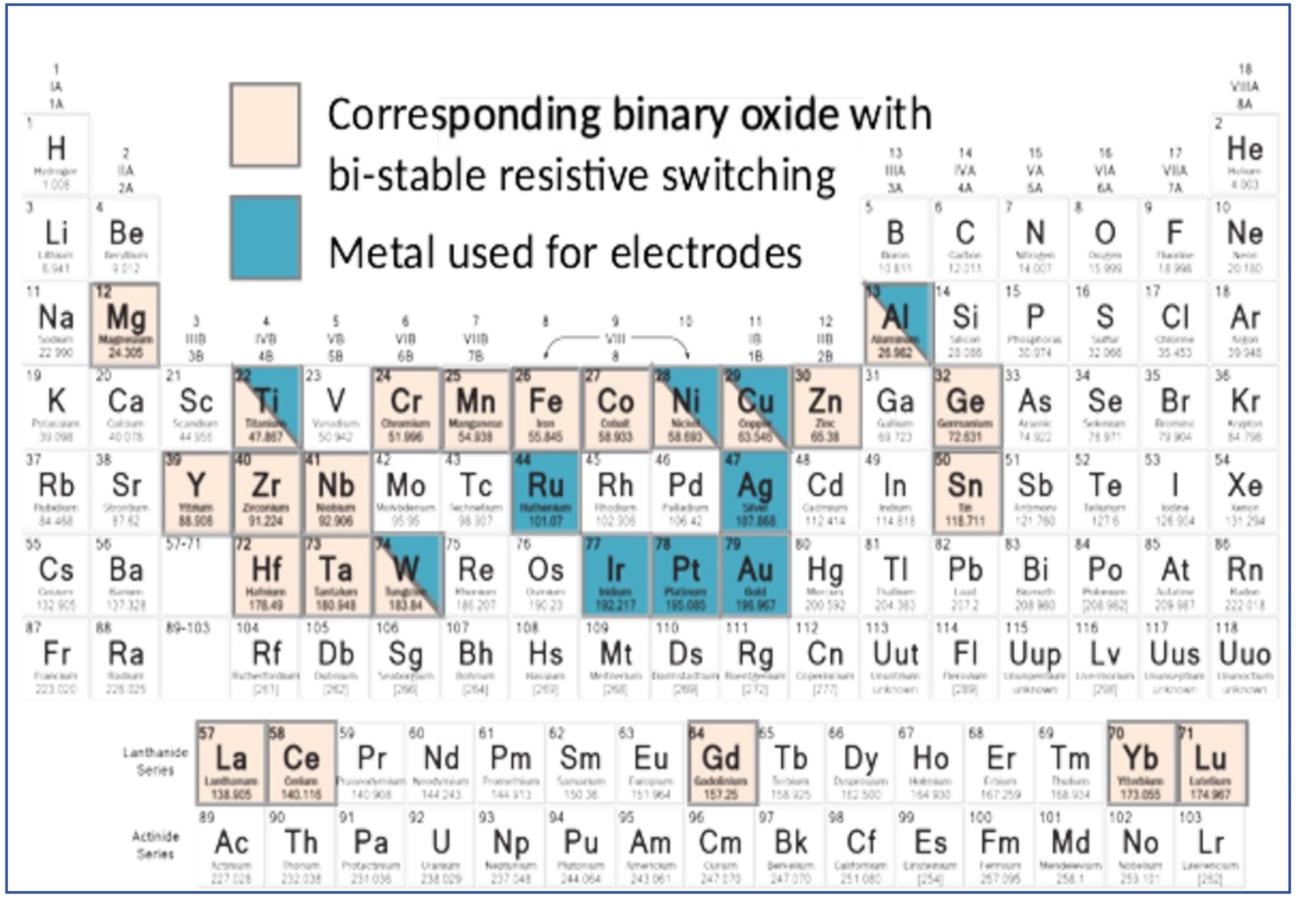
Stochastic process of moving atoms in a dielectric due to discrete displacements ('hopping') of atoms which will occur with a certain probability



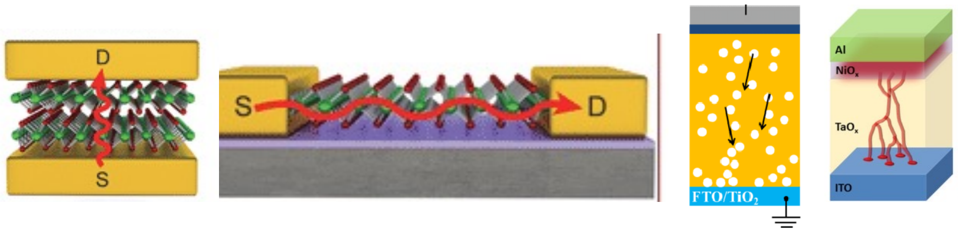
Huang, Yifu et al. ReSe2-Based RRAM and Circuit-Level Model for Neuromorphic Computing. Frontiers in Nanotechnology. 3. 10.3389/fnano.2021.782836.

S. Yu, et al, "On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, monte carlo simulation, and experimental characterization," *2011* IEDM

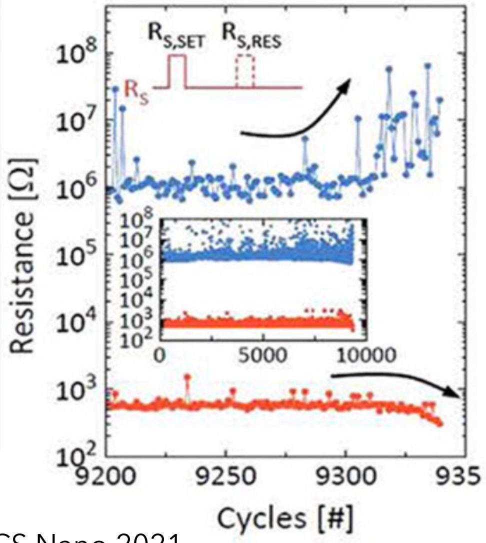
RRAM (Resistive Memory)
- Issues -



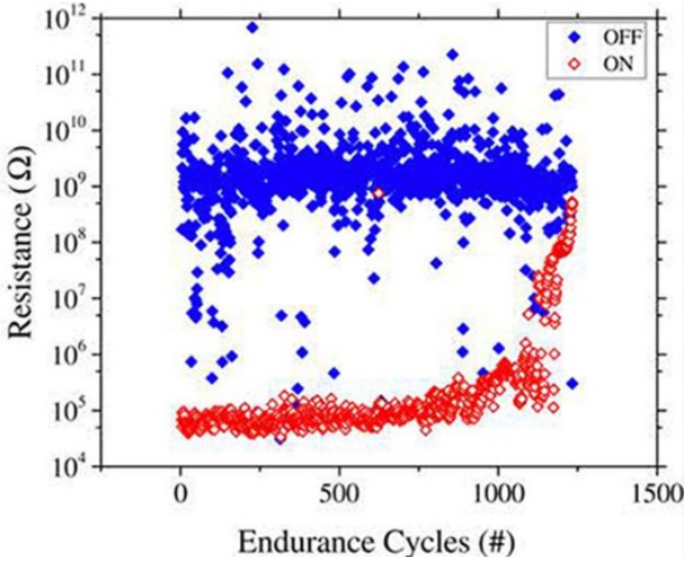
Versatility



Resistance Drift

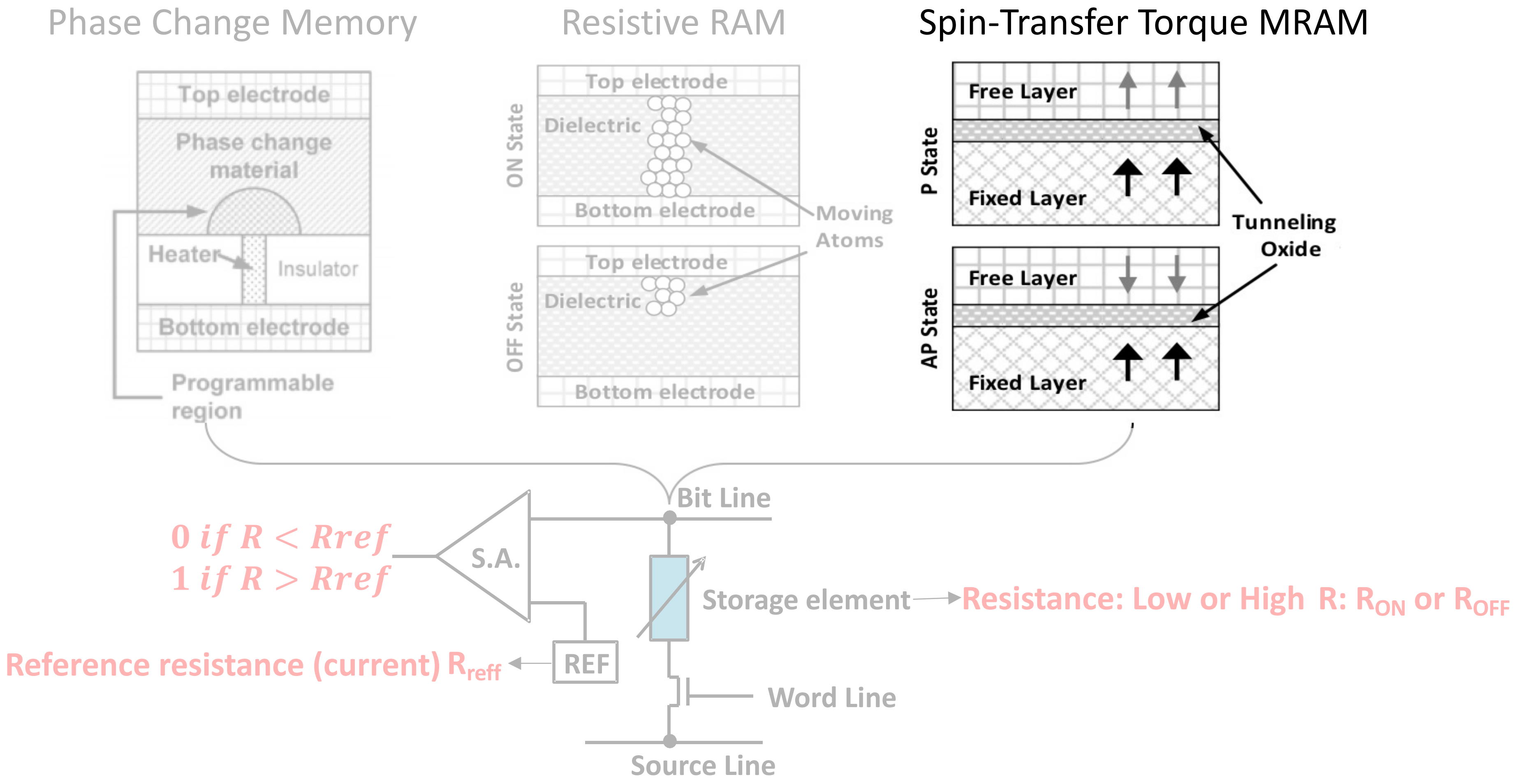


Cycling Endurance



Mario Lanza et al. Standards for the Characterization of Endurance in Resistive Switching Devices. ACS Nano 2021

Presentation Outline



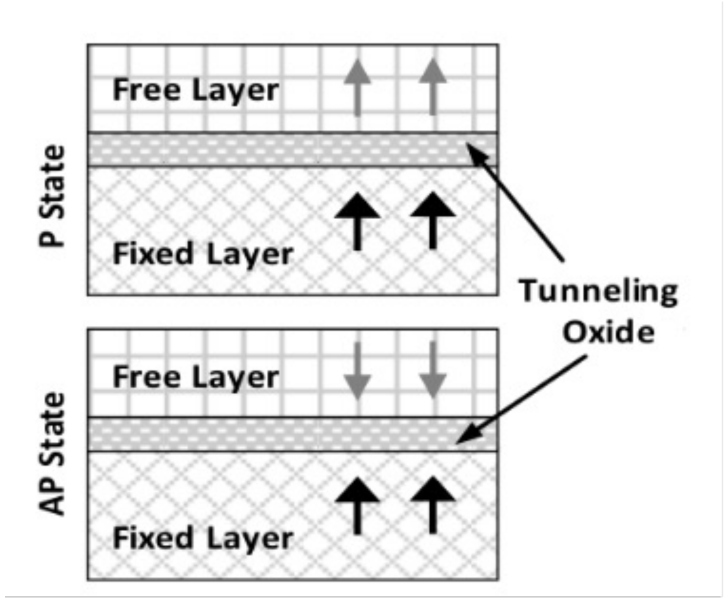
$0 \ if \ R < Rref$

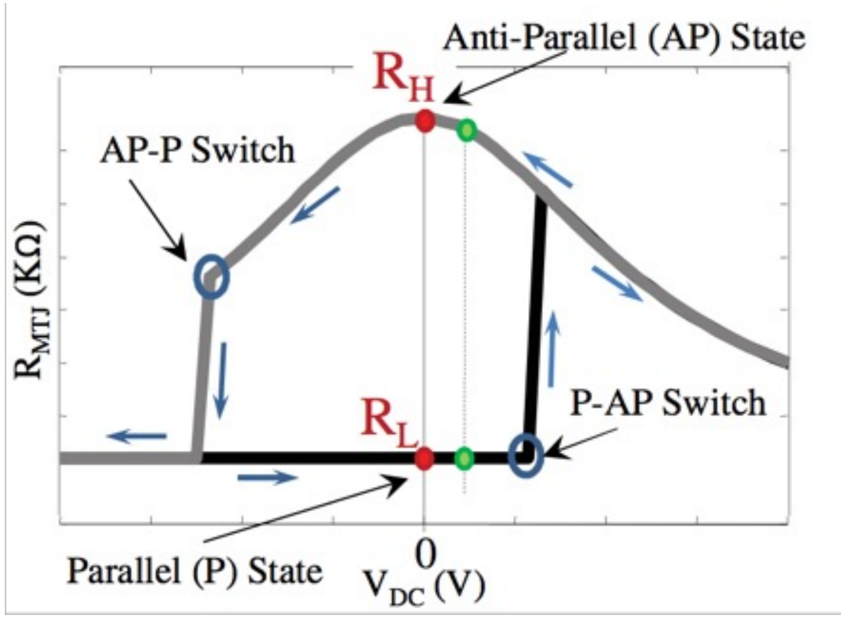
$1 \ if \ R > Rref$

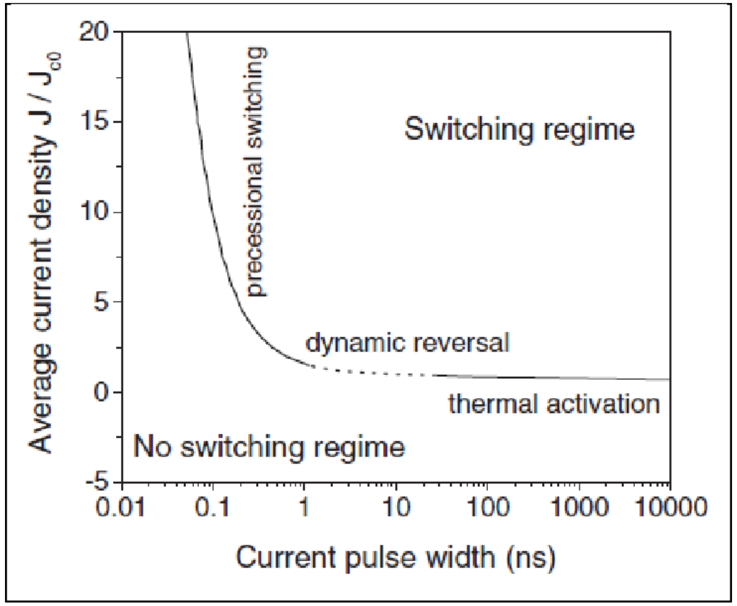
Reference resistance (current) R_{reff}

Resistance: Low or High R: R_{ON} or R_{OFF}

MRAM (Magnetic Memory)







TiMA

MRAM (Magnetic Memory)
- Stochasticity -

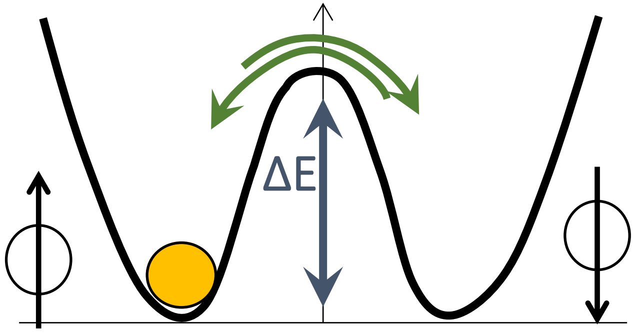
Néel-Brown: at finite temperature, there is a finite probability for the magnetization to flip and reverse its direction.

Néel-Brown model:
$P(t) = \exp(t/\tau)$ → source of entropy
$\tau = \tau_0 \exp(\Delta E / k_B T)$

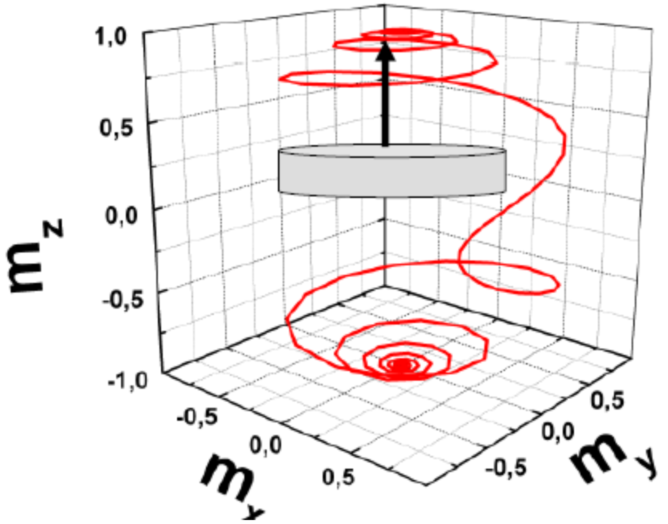
$$P_{wr} = \exp\left(\frac{-\pi^2 \cdot \Delta \cdot \left(\enclose{circle}{\frac{I_W}{I_{c0}}} - 1\right)/4}{\frac{I_W}{I_{c0}} \cdot \exp\left(2 \cdot \alpha \cdot \gamma \cdot H_k \cdot \enclose{circle}{tw} \cdot \frac{\enclose{circle}{\frac{I_W}{I_{c0}}} - 1}{1 + \alpha^2}\right) - 1} \right)$$

$\Delta E = f(K,M) \cdot (A \cdot t_f / k_B T)$

K = anisotropy,
M = demagnetization energy,
A = area of free layer,
t_f = thickness of free layer

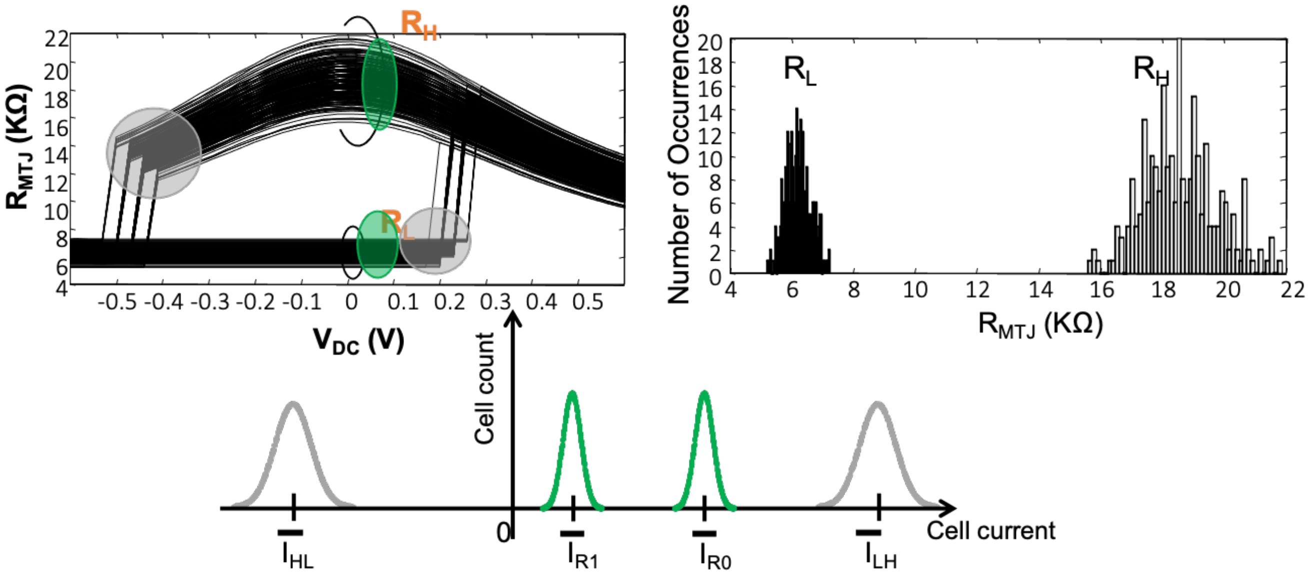


Digitalization

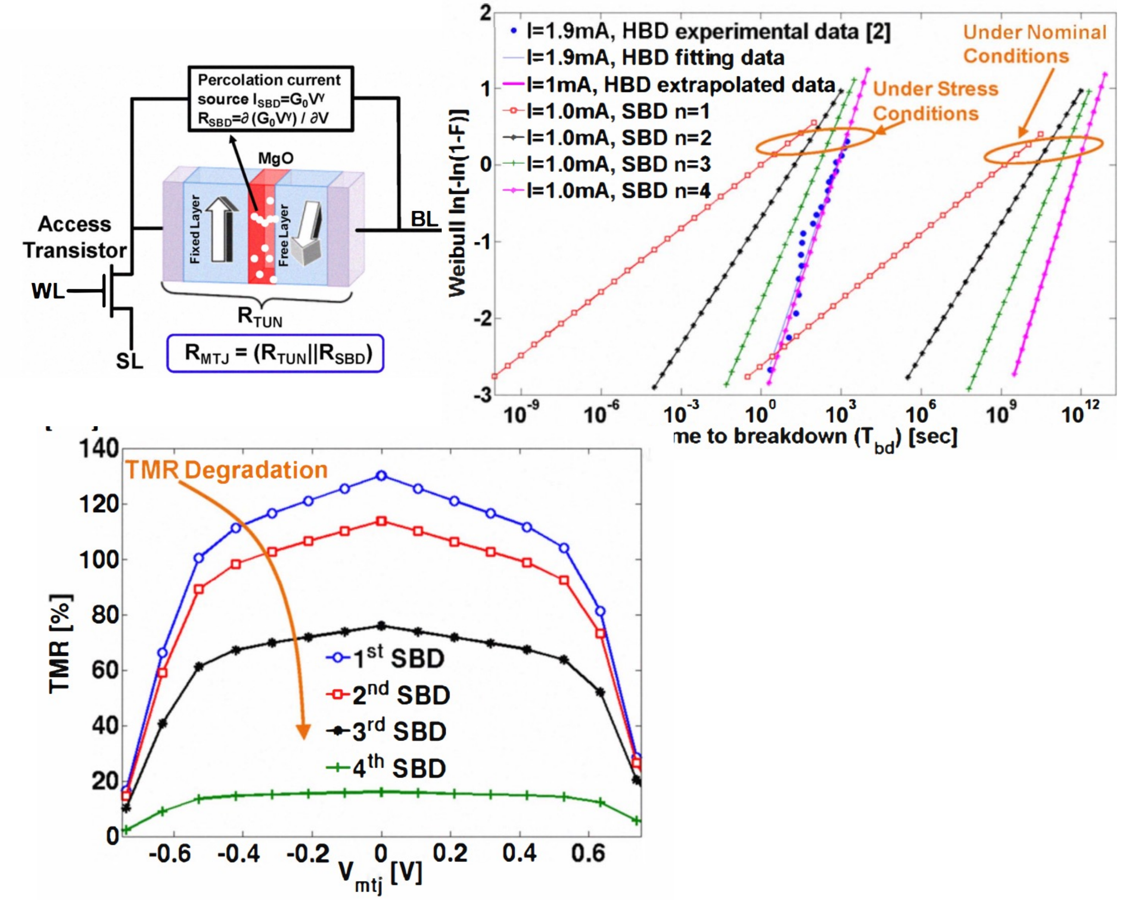


MRAM (Magnetic Memory)
- Issues -

Process Variability



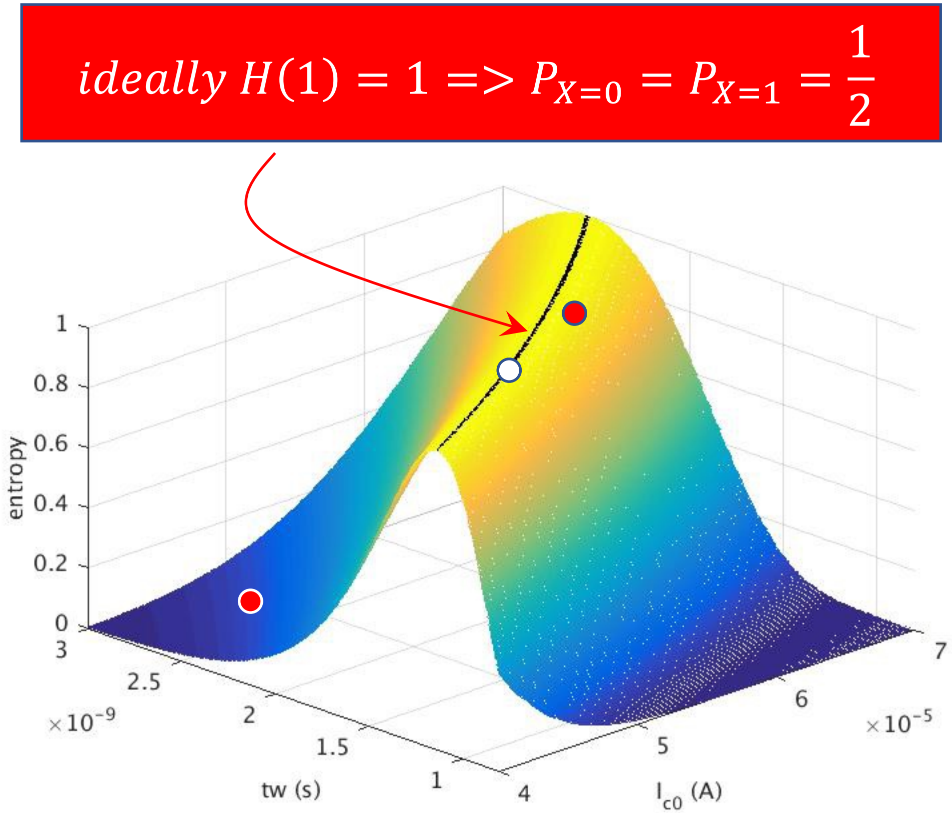
Time-dependent Dielectric Breakdown



G. Panagopoulos, C. Augustine and K. Roy, "Modeling of dielectric breakdown-induced time-dependent STT-MRAM performance degradation," *69th Device Research Conference*, 2011
E. I. Vatajelu, et al, STT-MRAM-Based PUF Architecture Exploiting Magnetic Tunnel Junction Fabrication-Induced Variability. J. Emerg. Technol. Comput. Syst. 13, 1, Article 5 (January 2017)

MRAM (Magnetic Memory)
- A TRNG Example -

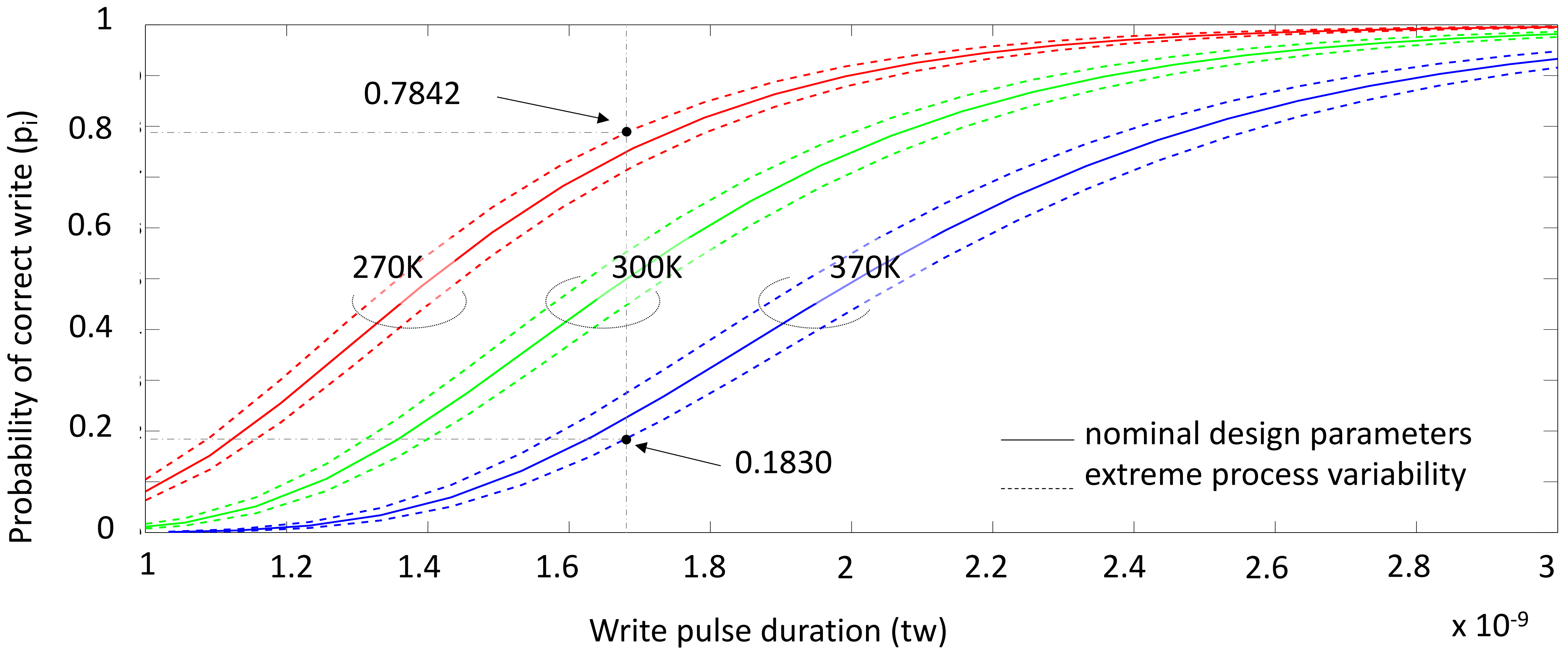
- based on the stochasticity of MTJ write operation as source of entropy: $H(X) = -P_{X=0}log_2(P_{X=0}) - P_{X=1}log_2(P_{X=1})$



$ideally\ H(1) = 1 => P_{X=0} = P_{X=1} = \frac{1}{2}$

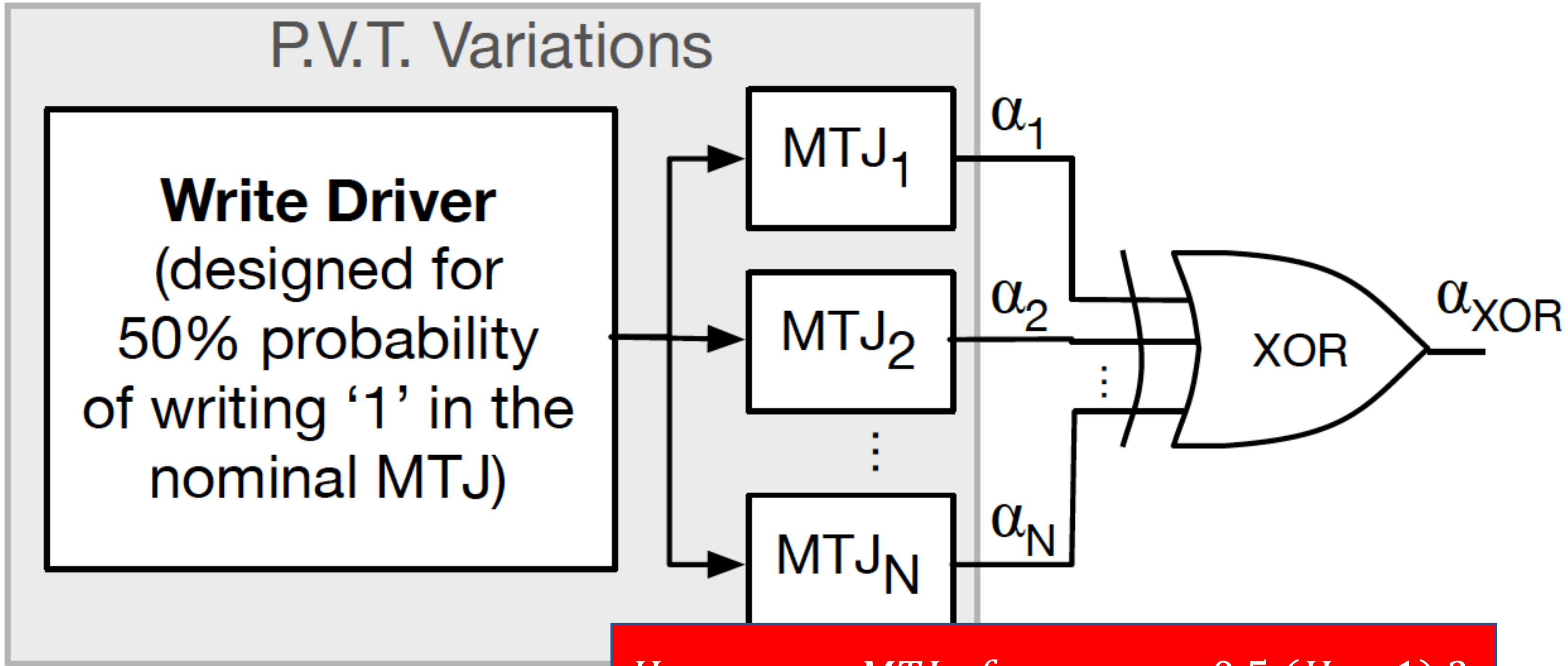
E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

MRAM (Magnetic Memory) - A TRNG Example -



E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

MRAM (Magnetic Memory)
- A TRNG Example -



How many MTJs for $\alpha_{XOR} = 0{,}5\ (H = 1)$?

$$with\ \alpha_i = \left|\frac{1}{2} - P_i^{MTJ}\right|$$

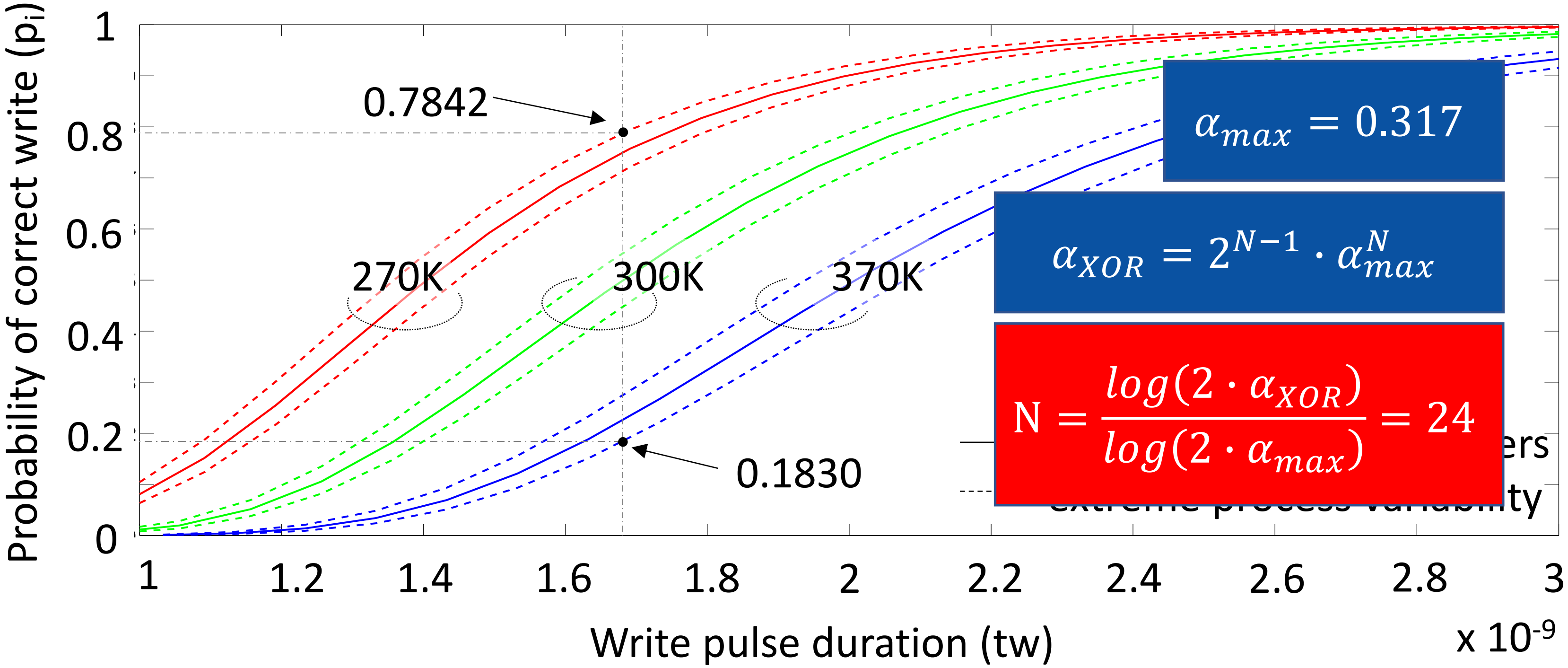
$$P_{XOR} = P_1^{MTJ} \cdot \left(1 - P_2^{MTJ}\right) + P_2^{MTJ} \cdot \left(1 - P_1^{MTJ}\right)$$

=> $\alpha_{XOR} = 2^{N-1} \cdot \alpha_1 \cdots \alpha_N$

E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

MRAM (Magnetic Memory)
- A TRNG Example -

- Question: how many MTJs for high entropy?



$$\alpha_{max} = 0.317$$

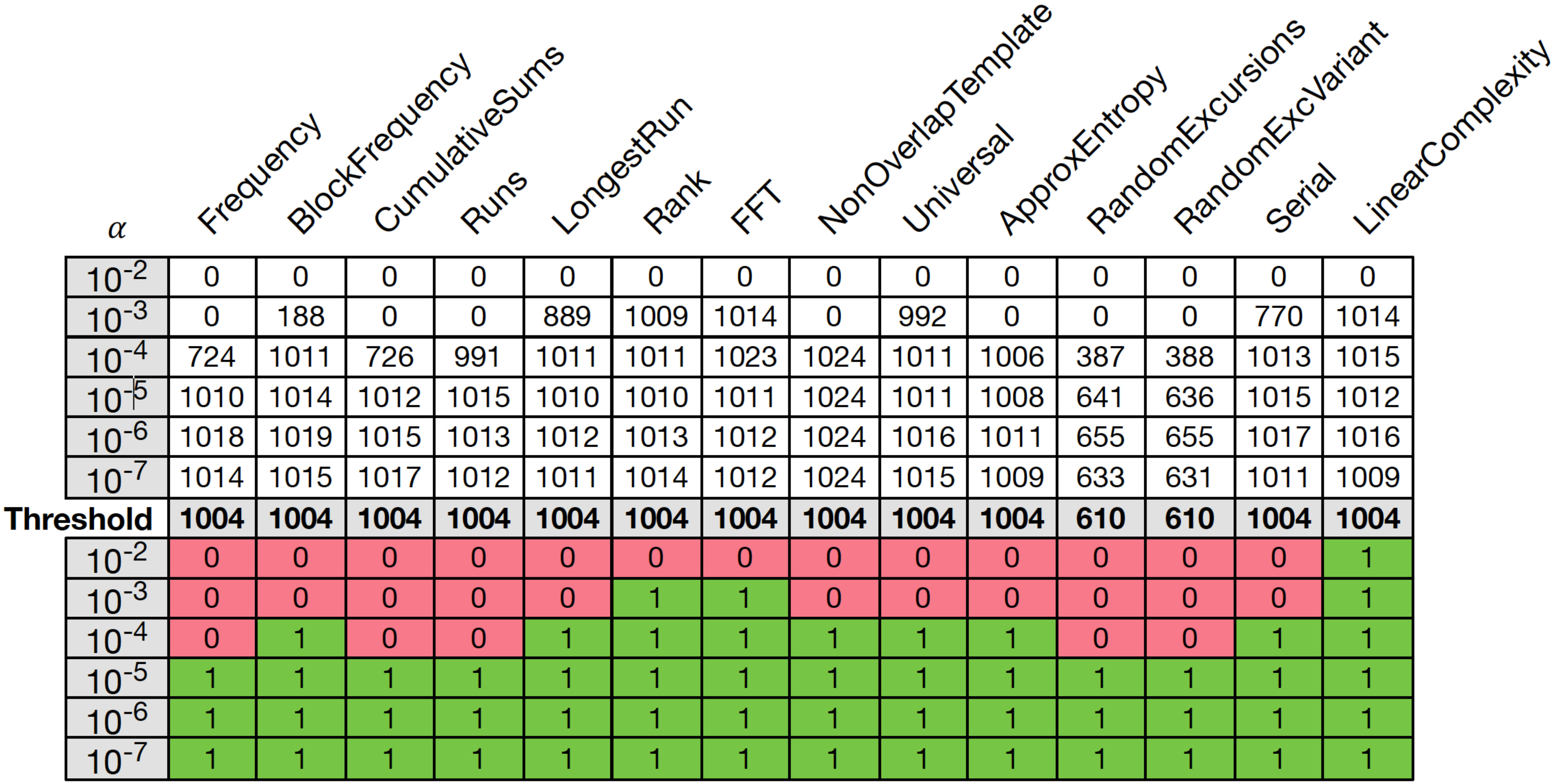
$$\alpha_{XOR} = 2^{N-1} \cdot \alpha_{max}^{N}$$

$$\mathrm{N} = \frac{log(2 \cdot \alpha_{XOR})}{log(2 \cdot \alpha_{max})} = 24$$

E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

MRAM (Magnetic Memory)
- A TRNG Example -

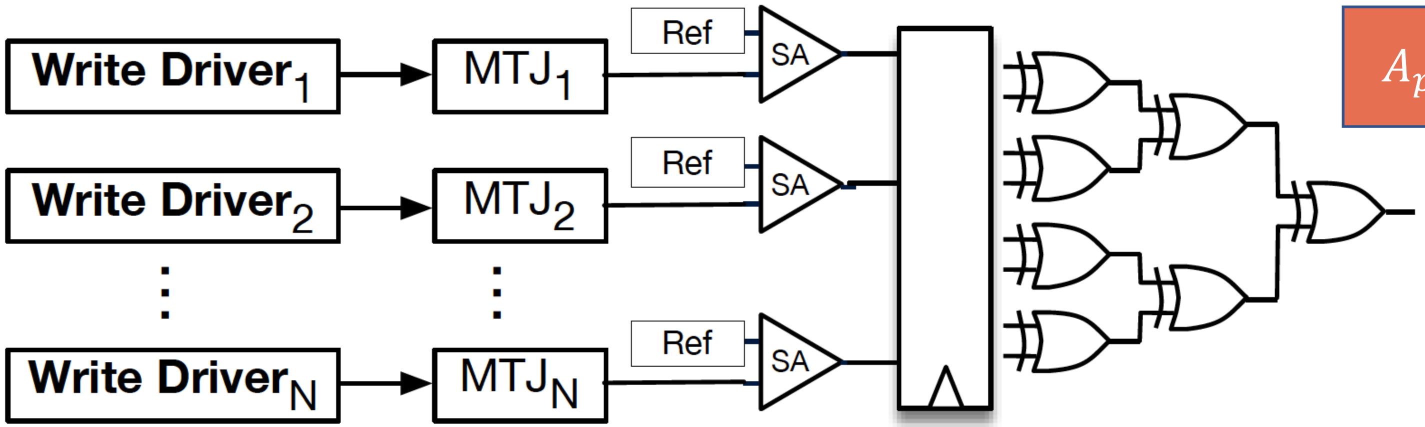
NIST test results assuming various values of α_{XOR}



α	Frequency	BlockFrequency	CumulativeSums	Runs	LongestRun	Rank	FFT	NonOverlapTemplate	Universal	ApproxEntropy	RandomExcursions	RandomExcVariant	Serial	LinearComplexity
10^{-2}	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10^{-3}	0	188	0	0	889	1009	1014	0	992	0	0	0	770	1014
10^{-4}	724	1011	726	991	1011	1011	1023	1024	1011	1006	387	388	1013	1015
10^{-5}	1010	1014	1012	1015	1010	1010	1011	1024	1011	1008	641	636	1015	1012
10^{-6}	1018	1019	1015	1013	1012	1013	1012	1024	1016	1011	655	655	1017	1016
10^{-7}	1014	1015	1017	1012	1011	1014	1012	1024	1015	1009	633	631	1011	1009
Threshold	**1004**	**1004**	**1004**	**1004**	**1004**	**1004**	**1004**	**1004**	**1004**	**1004**	**610**	**610**	**1004**	**1004**
10^{-2}	0	0	0	0	0	0	0	0	0	0	0	0	0	1
10^{-3}	0	0	0	0	0	1	1	0	0	0	0	0	0	1
10^{-4}	0	1	0	0	1	1	1	1	1	1	0	0	1	1
10^{-5}	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10^{-6}	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10^{-7}	1	1	1	1	1	1	1	1	1	1	1	1	1	1

E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

MRAM (Magnetic Memory)
- A TRNG Example -

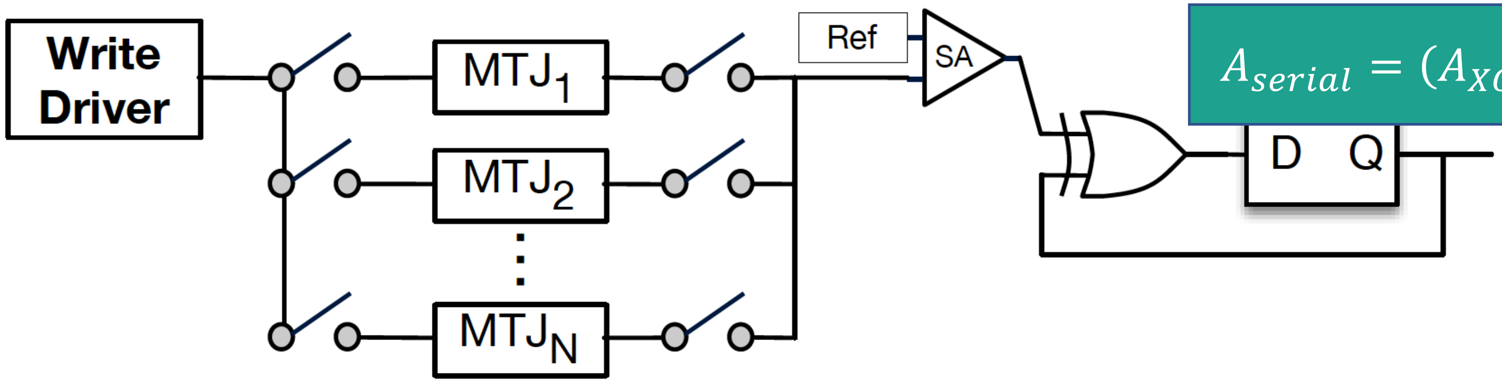


(a) Parallel Implementation

$$A_{parallel} = N(A_{XOR} + A_{FF} + A_{SA} + A_{WD})$$

$$t_{parallel} = t_{wr0} + t_{wr1} + t_{rd}$$

(b) Serial Implementation



$$A_{serial} = (A_{XOR} + A_{FF} + A_{SA} + A_{WD}) + 2 \cdot N \cdot A_{TG}$$

$$t_{serial} = N \cdot (t_{wr0} + t_{wr1} + t_{rd})$$

E. I. Vatajelu and G. Di Natale, "High-Entropy STT-MTJ-Based TRNG," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 491-495, Feb. 2019

Conclusions & Discussions

- Many devices – very varied phisics – all with intrinsic stochasticity
- Challenging evaluation for new devices
- Many frameworks developing in parallel
- Material/Device engineering today mitigates stochasticity

- Device/Technology co-optimization (DTCO) needed!

Generating Random Numbers with Spintronic and Memristive Devices

Elena Ioana Vãtãjelu
CR CNRS