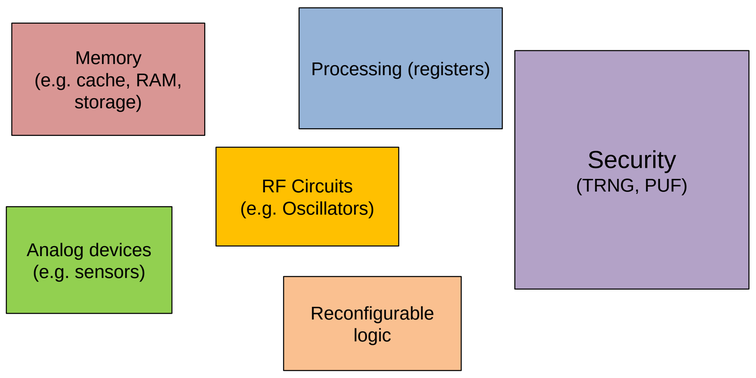
TAS-MTJ based True Random Number Generator

Frederic Ouattara, Lionel Torres

CONTEXT & MOTIVATION

Magnetic Tunnel Junction (MTJ)
is suitable for a wide range of applications



Physical Unclonable Function (PUF)

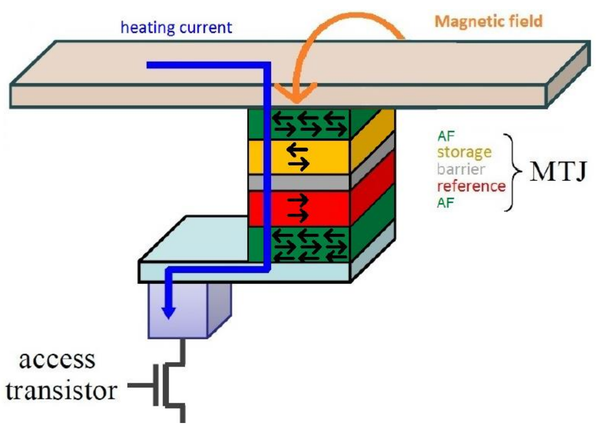
Magnetic Tunnel Junction (MTJ)
is suitable for two mains hardware security primitives

True Random Number Generator (TRNG)

- **Physical Unclonable Function (PUF)**
  - **Application**
    - Secure authentication
  - **Manufacturing variability exploitation**
    - Variability of electrical resistance of MTJ
- **True Random Number Generator (TRNG)**
  - **Application**
    - Random cryptographic keys
    - Statistical sampling
  - **Source of randomness**
    - Writing process of MTJ

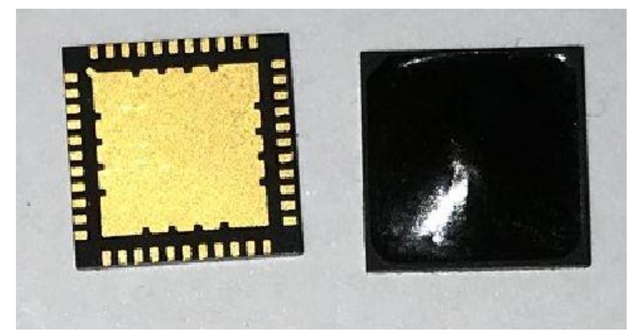
THERMALLY ASSISTED SWITCHING MAGNETIC RANDOM ACCESS MEMORY (TAS-MRAM) DUT

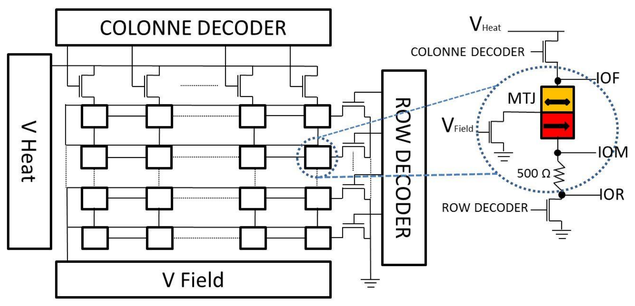
Thermally Assisted Switching (TAS)



- FM layers' magnetization is blocked at room temp.
- Heating the junction unblocks the free layer

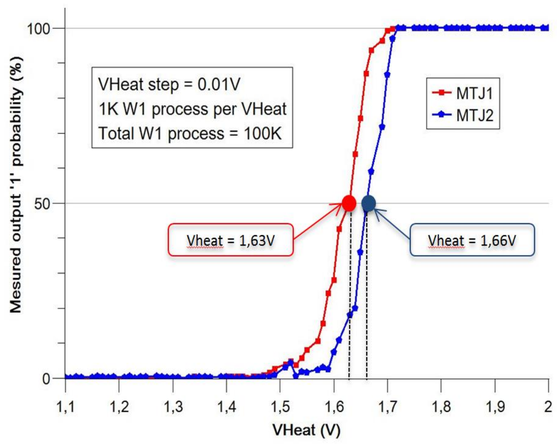
1Kbit TAS-MRAM device



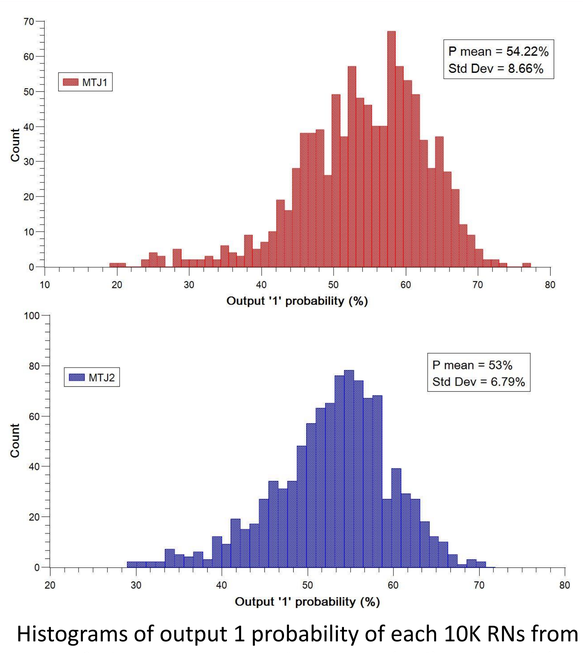


TAS-MTJ Writing '1' characterisation

- RESET by writing '0' (W0)
- SET by writing '1' (W1)



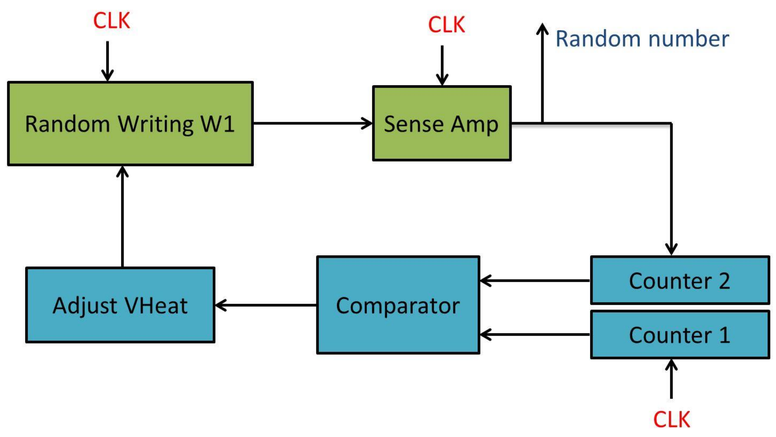
Raw random number distribution



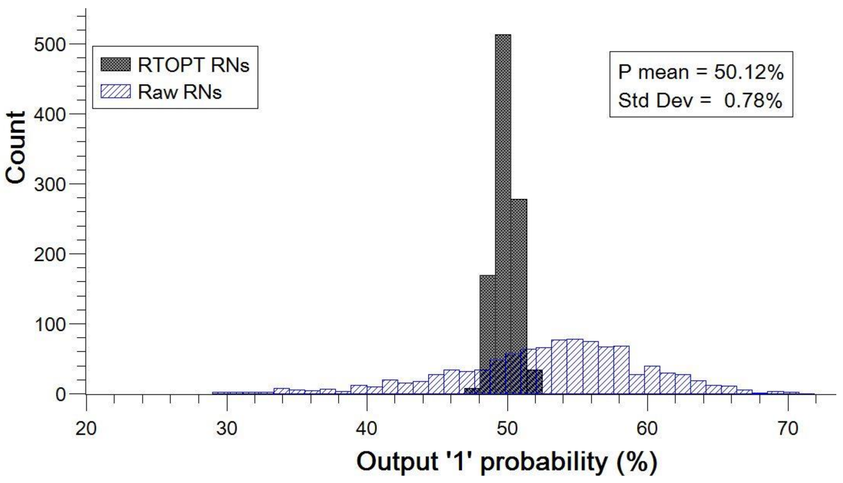
Histograms of output 1 probability of each 10K RNs from a total of 10M RNs generated by MTJ1 (red) and MTJ2 (blue)

TAS – MTJ BASED TRNG

Real Time Output Probability Tracking

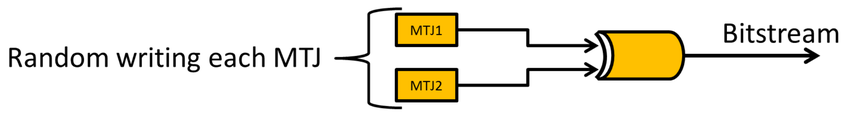


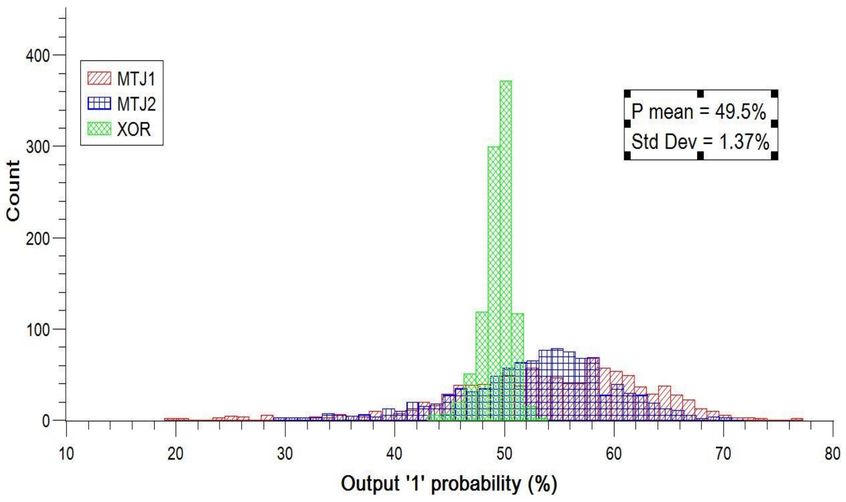
- Architecture of real-time output probability tracking (RTOPT)



- Histograms of output 1 probability of RNs generated with a RTOPT (dark) compare to the raw RNs (blue)

XOR post processing

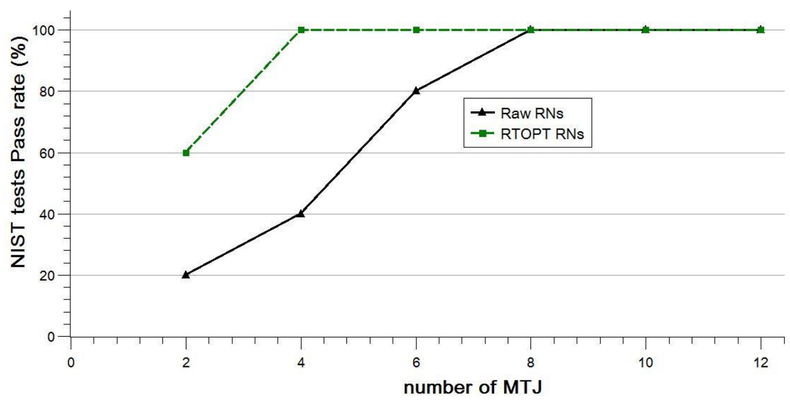




- Histogram of output 1 probability after a XOR post processing on two MTJs (MTJ1 and MTJ2)

NIST Randomness Tests Results

Test name	Raw	RTOPT	Von Neu-mann	XOR^3 on Raw	XOR^2 on RTOPT
Frequency	Fail	Pass	Pass	Pass	Pass
Block Frequency	Fail	Fail	Pass	Pass	Pass
Run	Fail	Pass	Pass	Pass	Pass
Longuest Run	Fail	Fail	Pass	Pass	Pass
Cumulative Sums	Fail	Fail	Pass	Pass	Pass
Binary Rank	Fail	Fail	Pass	Pass	Pass
FFT	Fail	Fail	Pass	Pass	Pass
Serial	Fail	Fail	Pass	Pass	Pass
Approximate entropy	Fail	Fail	Pass	Pass	Pass
Non-overlapping Template	Fail	Fail	Pass	Pass	Pass



- The ten appicable tests of NIST pass rate as a function of the numbers of MTJs with XOR processing on raw RNs and RNs generated with a real time output probability tracking (RTOPT)

Laboratoire d'Informatique, Robotique et Microélectronique de Montpellier
Université Montpellier / CNRS (French National Center for Scientific Research)
Address: 161, rue Ada - 34095 Montpellier, France
E-mail: fredreic.ouattara@ lirmm.fr, lionel.torres@lirmm.fr