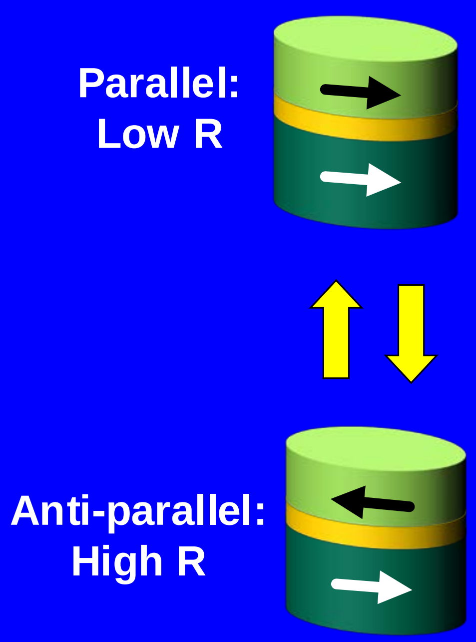
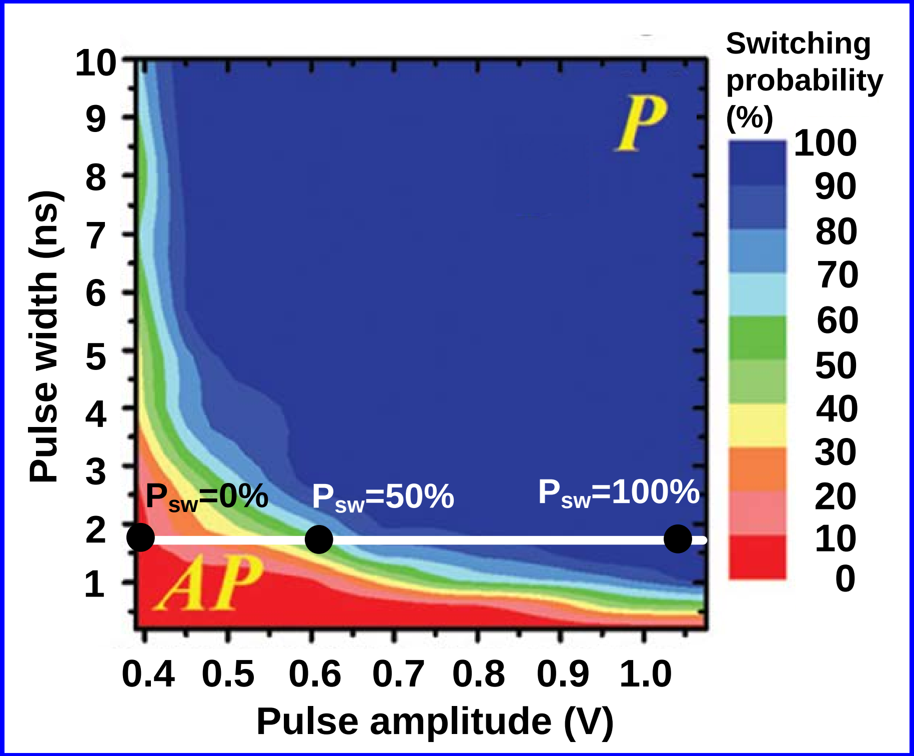
MTJ based Random Number Generation and Analog-to-Digital Conversion

Chris H. Kim
University of Minnesota

Workshop on the Future of Spintronics, June 5, 2016

Switching Probability of an MTJ



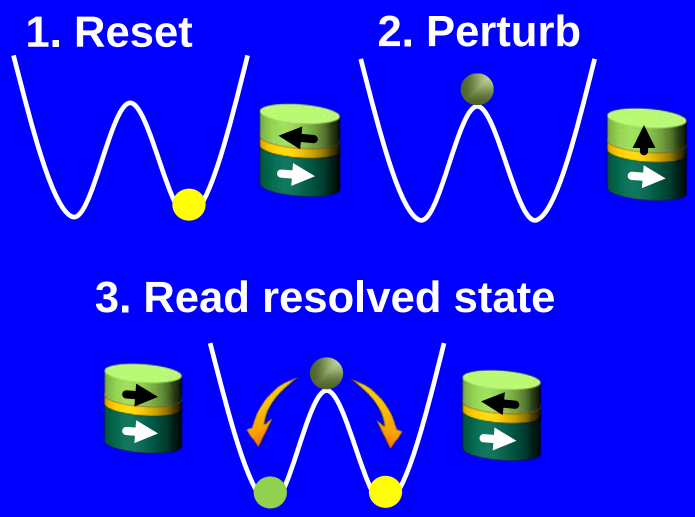


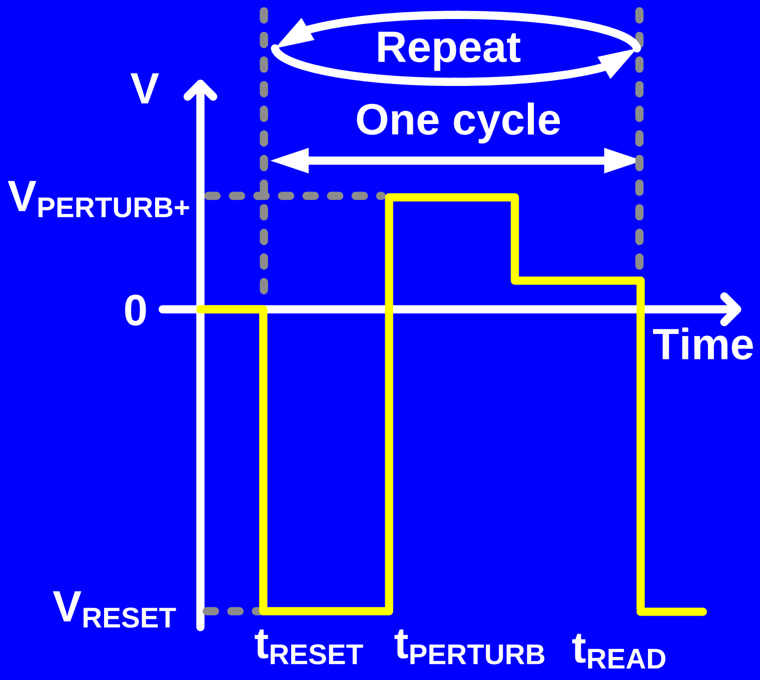
H. Zhao, JP Wang, JAP, 2011

- P_{sw}=100% (write) or 0% (read) : STT-MRAM
- P_{sw}=50% switching: Random number generation
- 0%<P_{sw}<100%: Analog to digital conversion, time to digital conversion

MTJ based TRNG

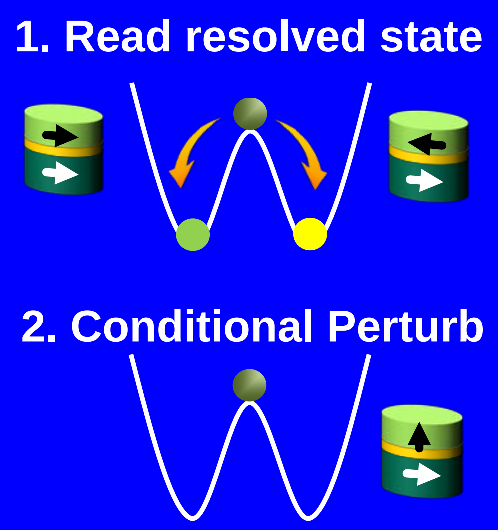
- Unconditional Reset Scheme -

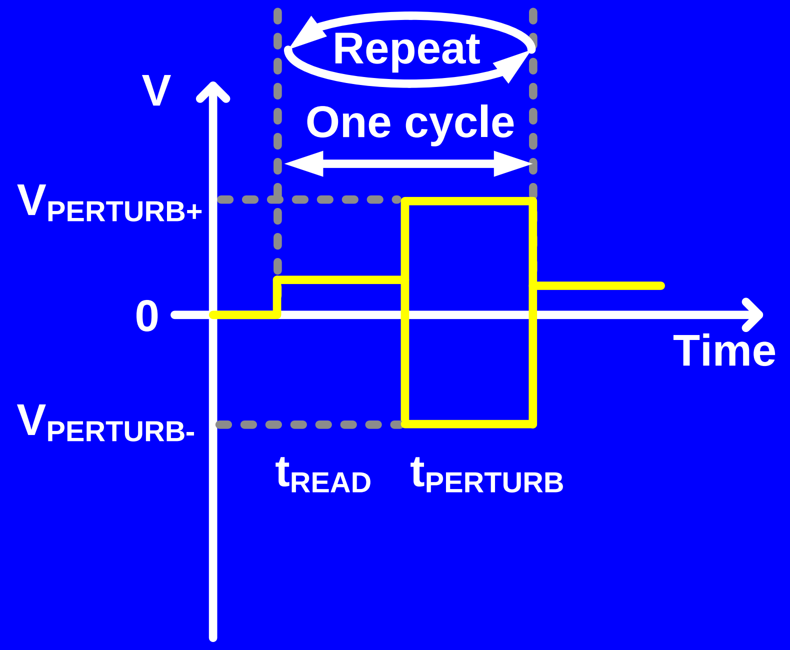




- 50% switching utilized for generating random bits
- Large reset voltage required every cycle → slow, high power, short lifetime

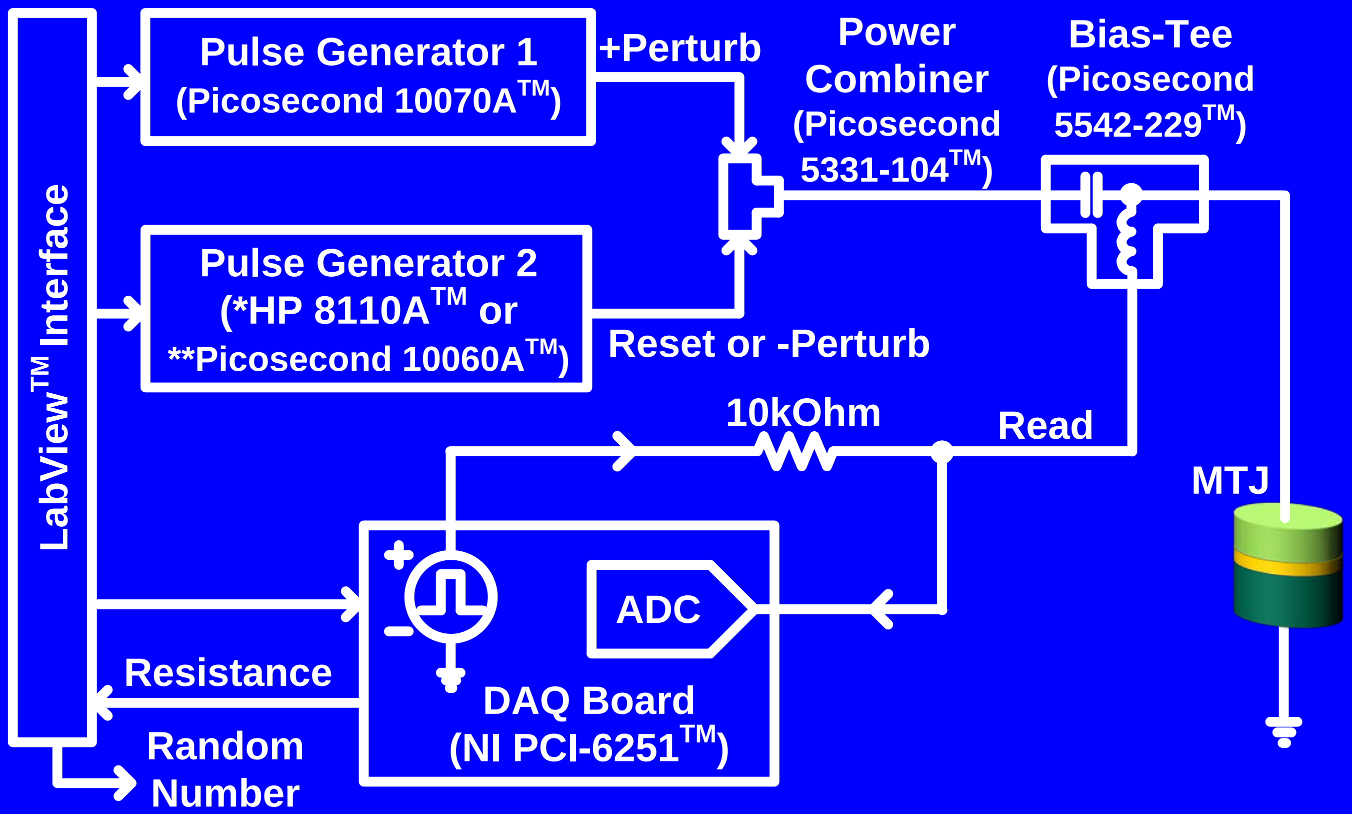
New Conditional Perturb Scheme

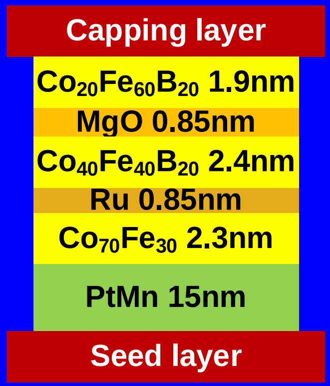


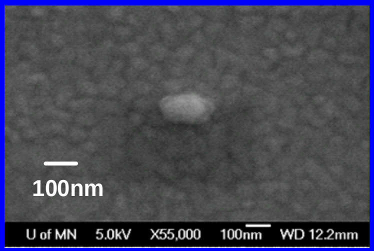


- Perturbs MTJ according to the previously sampled MTJ state, thereby eliminating the reset phase → fast, low power, long lifetime

MTJ Measurement Setup







Dimension	170x50nm^2
RA	5.26 Ω·μm^2
TMR	107%
Thermal stability	61

- **Random number generator measurement setup with sub-50 ps pulse width resolution**

W. Choi, Y. Lv, JP Wang, C. Kim, IEDM 2014

NIST Randomness Test Results

Unconditional reset scheme

# of segments: 55

	Test	Pass/Fail
1	Frequency	Fail
2	Block frequency	Pass
3	Cumulative Sums	Fail
4	Runs	Pass
5	Longest-Run-of-Ones	Pass
6	Rank	Pass
7	FFT	Pass
8	Non-overlapping Template Matching	Pass
9	Serial	Pass
10	Approximate Entropy	Pass

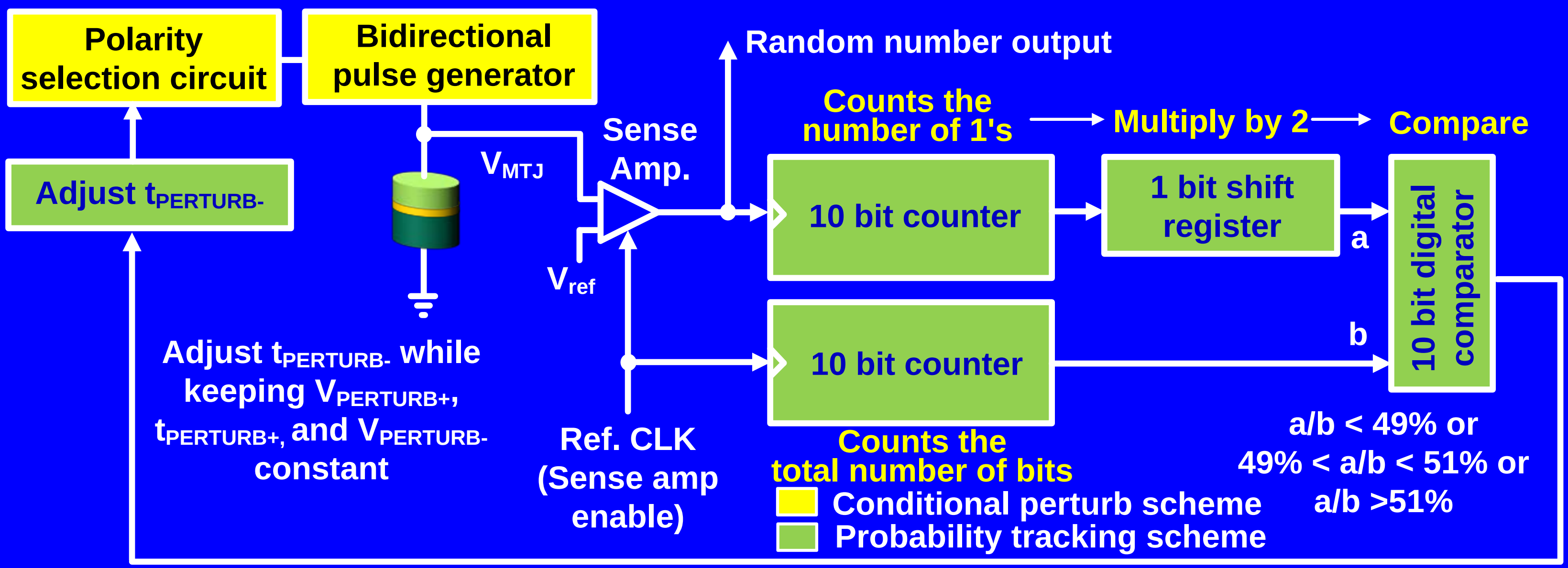
Conditional perturb scheme

# of segments: 55

	Test	Pass/Fail
1	Frequency	Fail
2	Block frequency	Pass
3	Cumulative Sums	Fail
4	Runs	Pass
5	Longest-Run-of-Ones	Pass
6	Rank	Pass
7	FFT	Pass
8	Non-overlapping Template Matching	Pass
9	Serial	Pass
10	Approximate Entropy	Pass

- Both schemes show similar level of randomness
- The output data fail to pass the frequency and cumulative sums tests

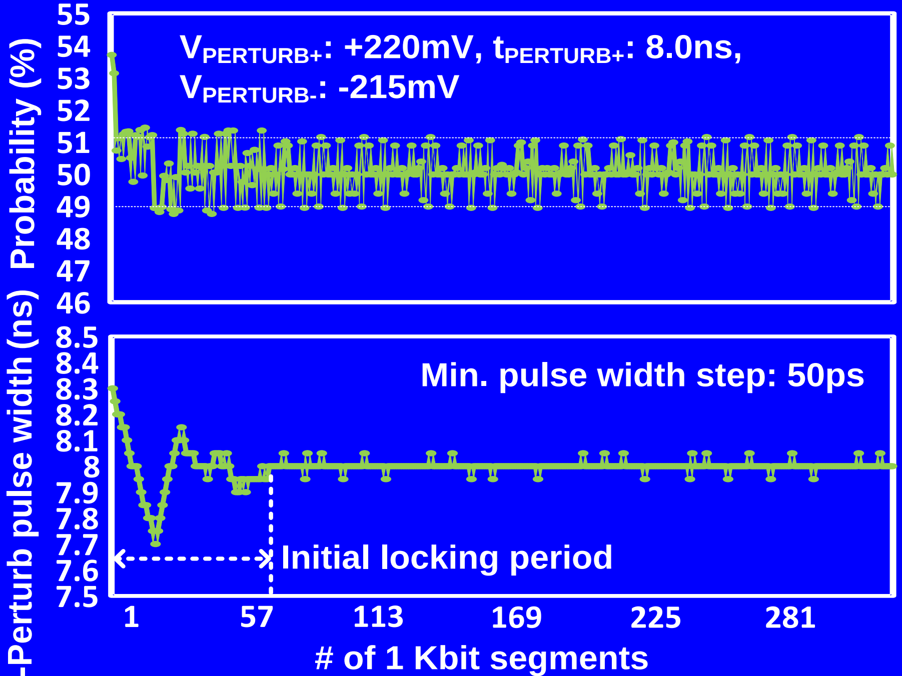
Real-Time Output Probability Tracking



- Simple single-parameter feedback control
- The proposed techniques were implemented in a real-time feedback loop

W. Choi, Y. Lv, JP Wang, C. Kim, IEDM 2014

Measured Probability and Randomness
- Real-Time Output Probability Tracking-



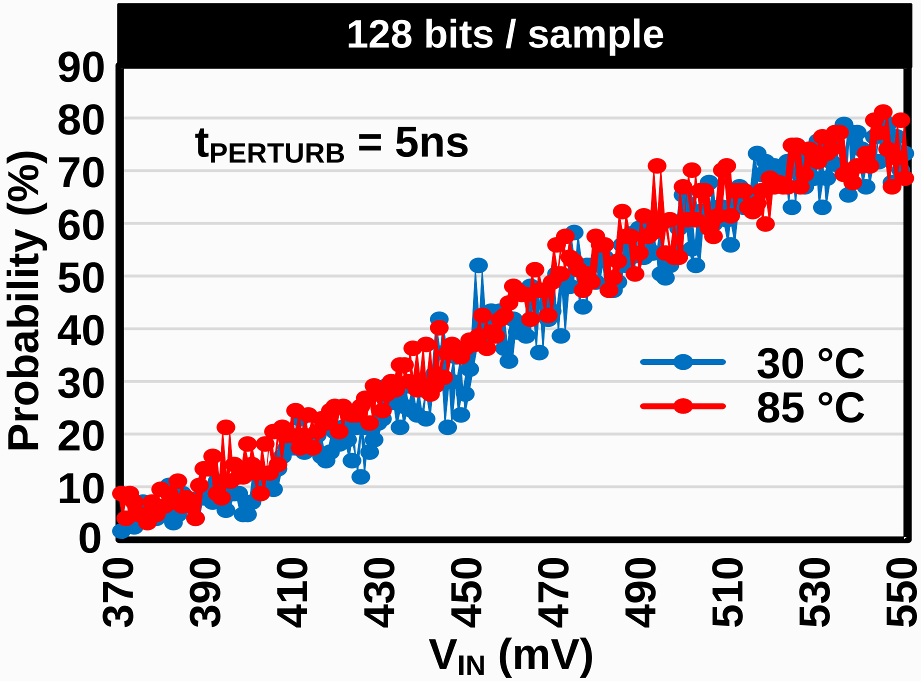
Raw data after probability tracking

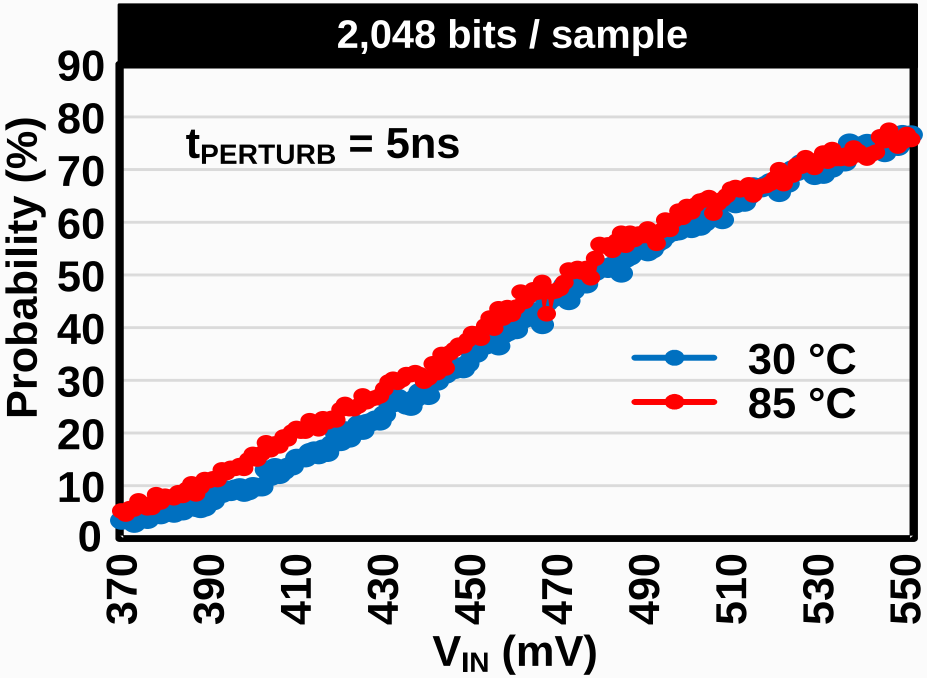
Conditional perturb scheme, # of segments: 55

	Test	Pass/Fail
1	Frequency	Pass
2	Block frequency	Pass
3	Cumulative Sums	Pass
4	Runs	Pass
5	Longest-Run-of-Ones	Pass
6	Rank	Pass
7	FFT	Pass
8	Non-overlapping Template Matching	Pass
9	Serial	Pass
10	Approximate Entropy	Pass

- **Proposed conditional perturb and real-time probability tracking provides good randomness while improving reliability, speed, and power**

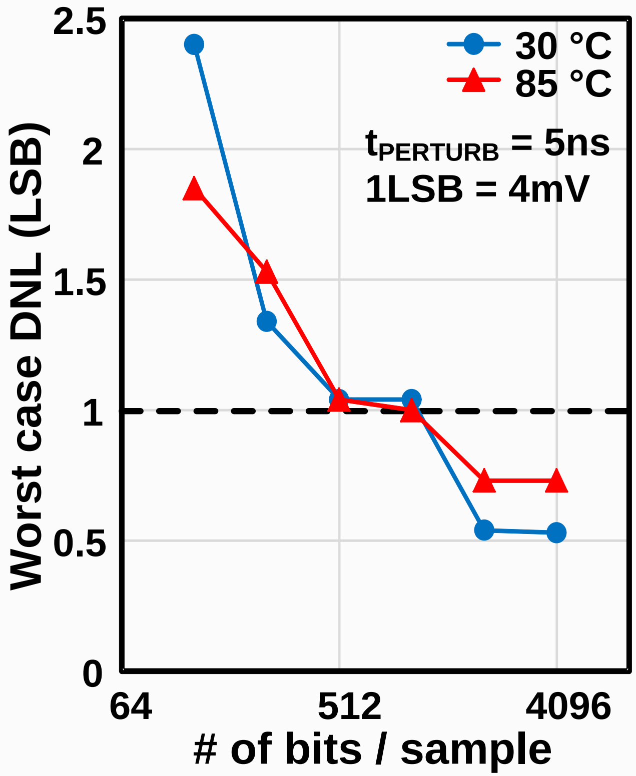
MTJ based ADC

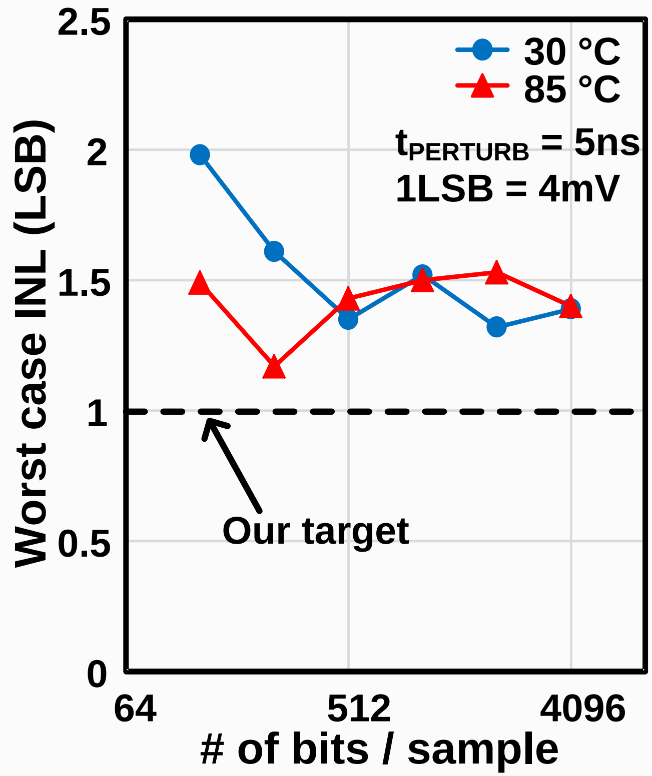




- **A short 5ns $t_{PERTURB}$ used for suppressing thermal activation switching**
- **Averaging more bits gives a smoother and more accurate probability curve (128 bits vs. 2,048 bits)**
- **Temperature sensitivity is acceptably low**

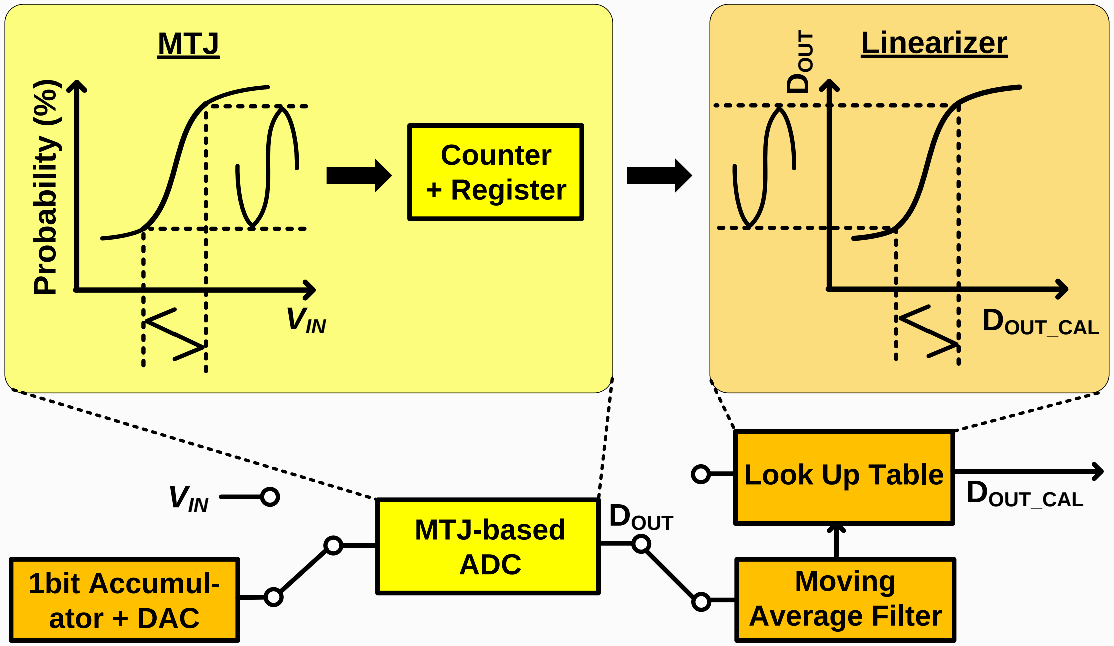
Measured Worst Case DNL and INL





- A 5-bit ADC resolution is assumed (i.e. 1LSB = 4mV)
- DNL of 1 LSB can be achieved by averaging more random bits (e.g. 2,048 bits)
- INL cannot be improved by simply averaging more bits

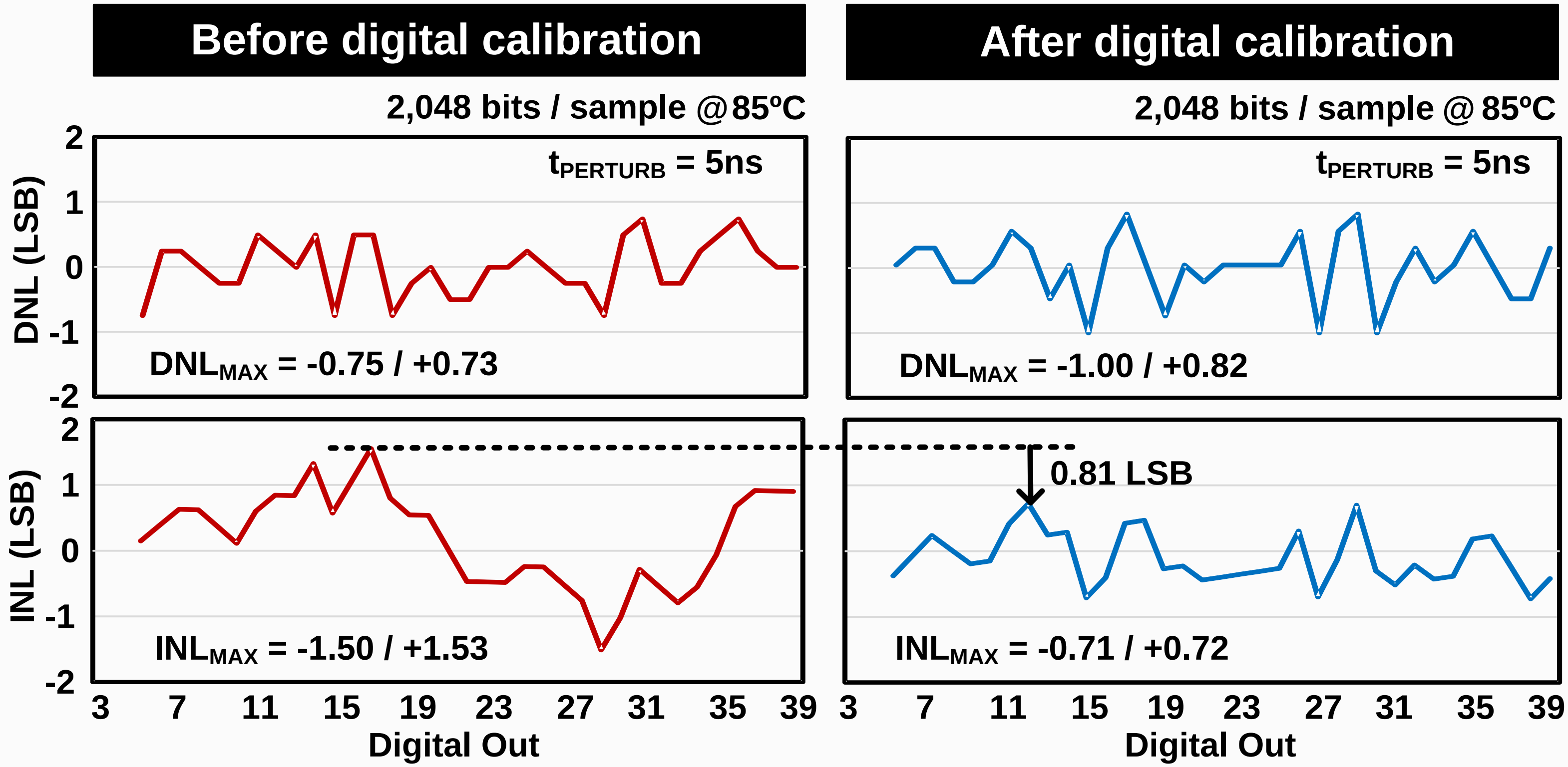
One-time Digital Calibration for Improving INL



J. Kim, et al., TCAS-I, 2010, J. Daniels, et al., VLSI Circuits Symposium, 2010.

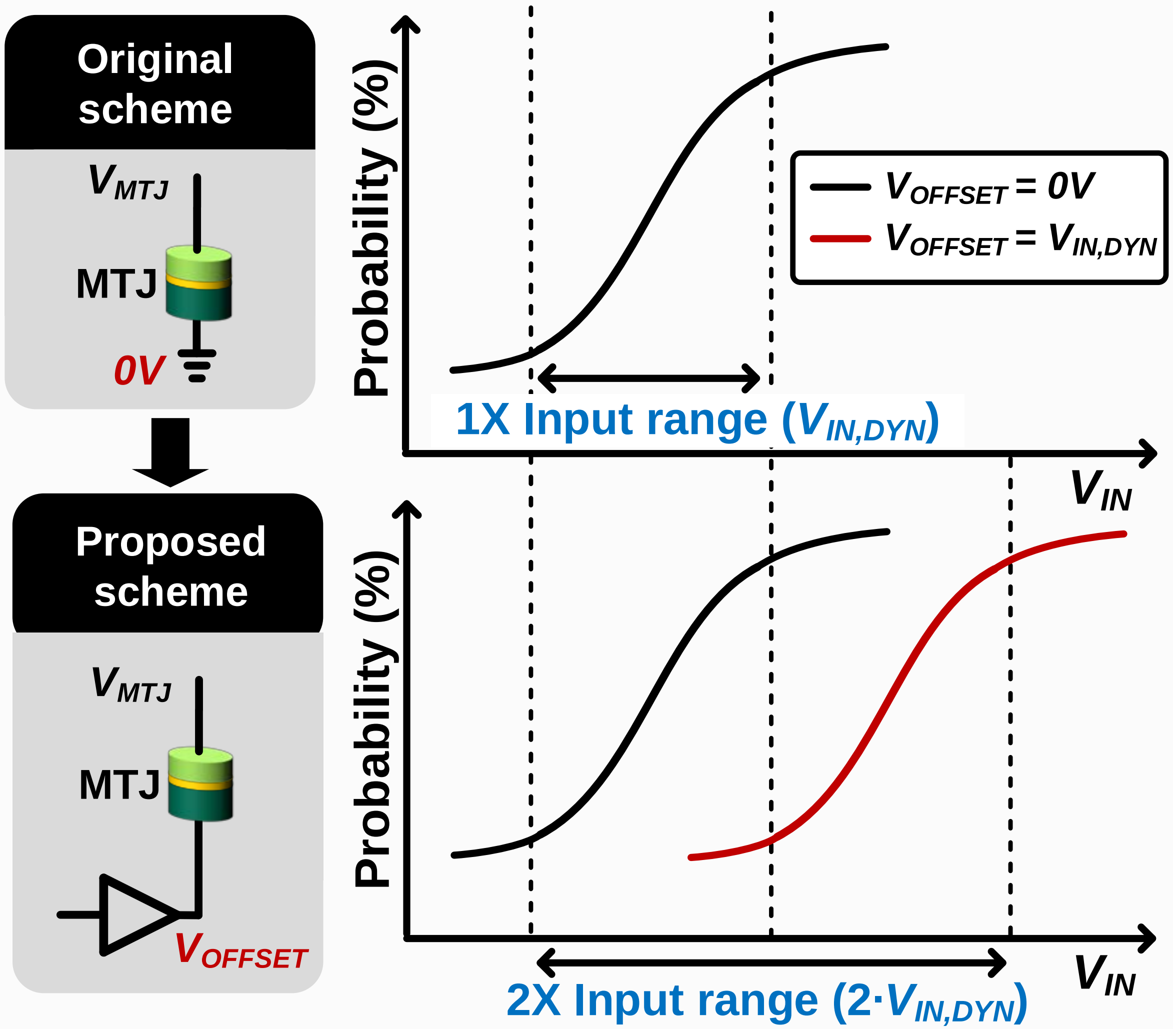
- **Basic idea: Pre-calibrate MTJ transfer curve and store the inverse function in a look-up table to compensate for inherent non-linearity**

Measured DNL and INL @ 85℃

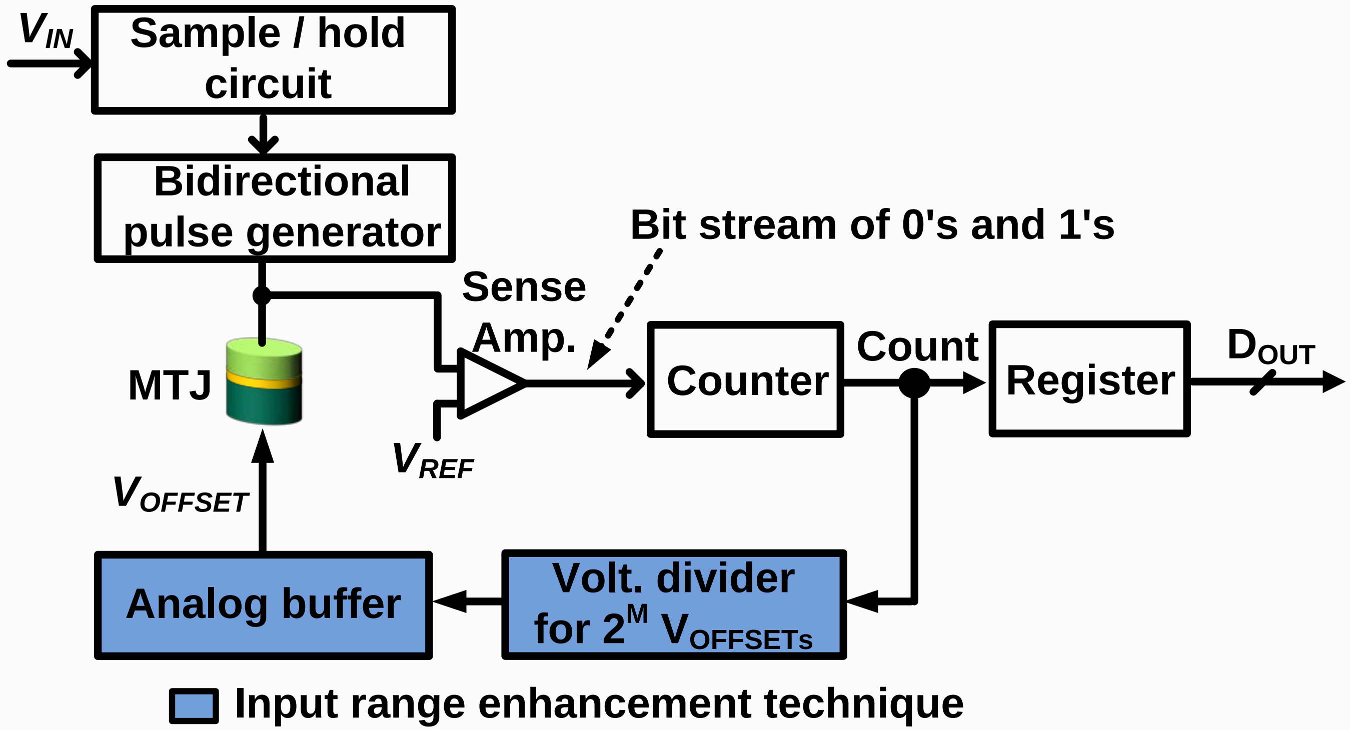


- Target DNL / INL of 1 LSB can be met after one-time calibration
- ADC resolution limited to 5-bit due to narrow input voltage range

Proposed Input Range Enhancement Technique

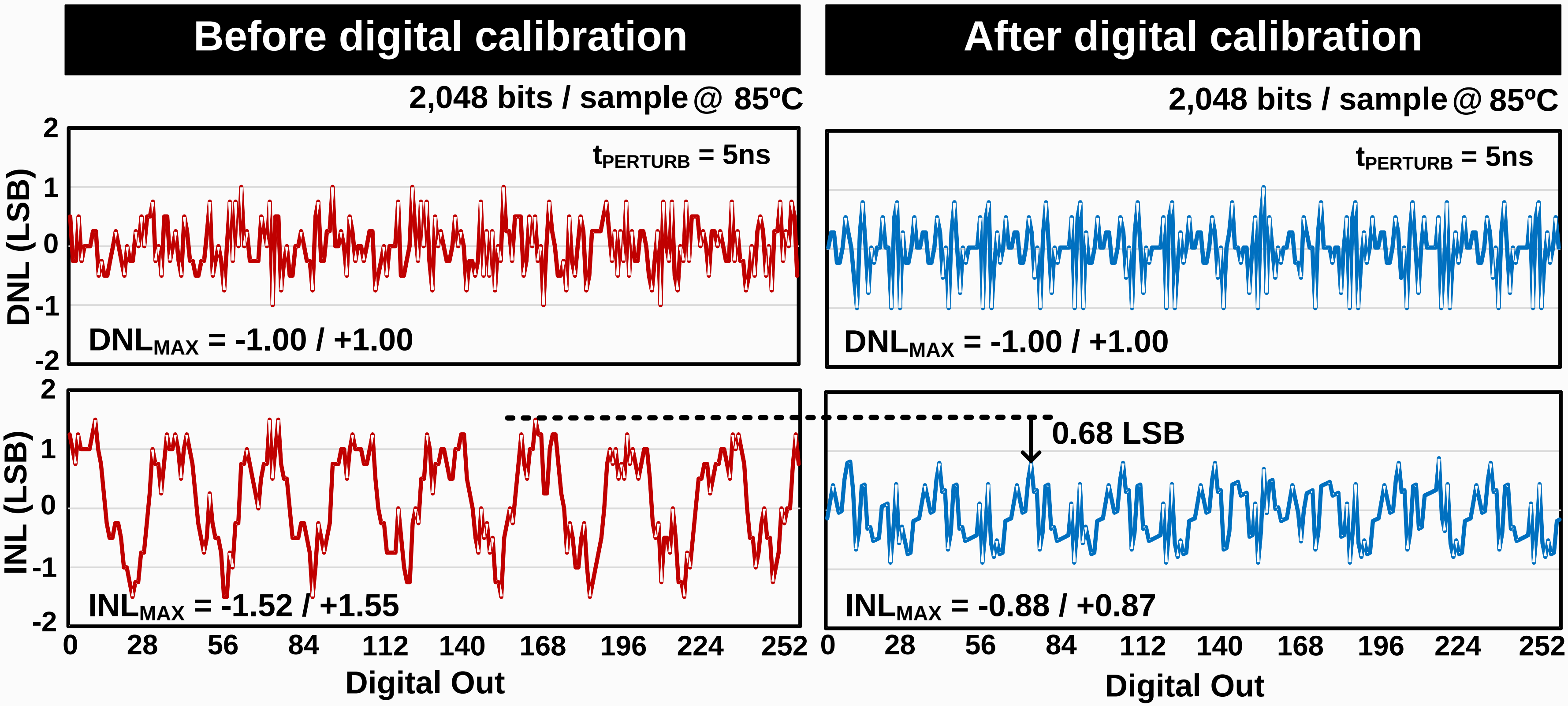


Implementation of Input Range Enhancement Technique



- A voltage divider and an analog buffer control the MTJ bottom node voltage

Measured DNL and INL @ 85℃



- **Target DNL / INL of 1 LSB can be met after calibration**
- **8-bit ADC resolution with good linearity is achieved**

ADC Performance Summary

2,048 bits / sample

		30 ºC			85 ºC		
	Input range	DNL_{MAX} (LSB)	INL_{MAX} (LSB)	Bits	DNL_{MAX} (LSB)	INL_{MAX} (LSB)	Bits
Original MTJ-based ADC	128mV (X1)	0.74	1.32	5	0.75	1.53	5
+ Digital calibration	128mV (X1)	1.00	0.76	5	1.00	0.72	5
+ Digital calibration + Input range enhancement	1024mV (X8)	1.00	0.84	8	1.00	0.88	8

- **ADC resolution (=8 bit) was limited by the minimum voltage step (=1mV) of pulse generator**
- **Ideally, resolution could be as high as 14 bits**

Summary

- **MTJ-based TRNG**
  - First demonstration of TRNG based on the random switching probability of MTJ
  - Conditional perturb and real-time output probability tracking → improved lifetime, speed, and power

- **MTJ-based ADC**
  - Digital calibration for improved linearity and input range enhancement technique
  - 2,048 bits averaged to generate one ADC sample
  - Insensitive to temperature using a 5ns pulse width