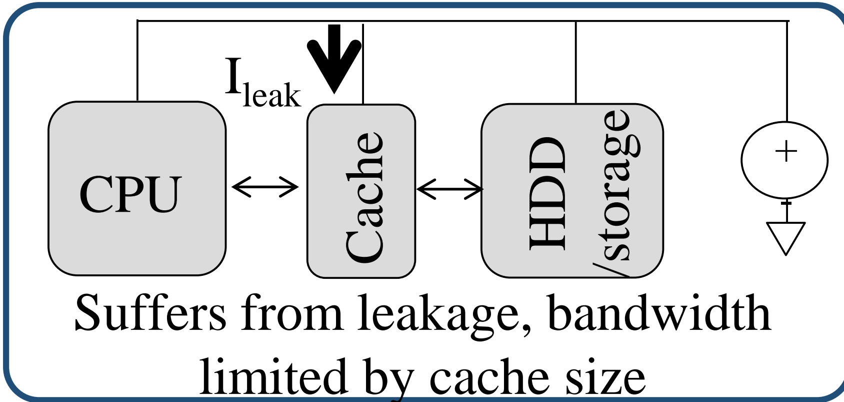
Fault Injection Attacks on Emerging Non-Volatile Memories

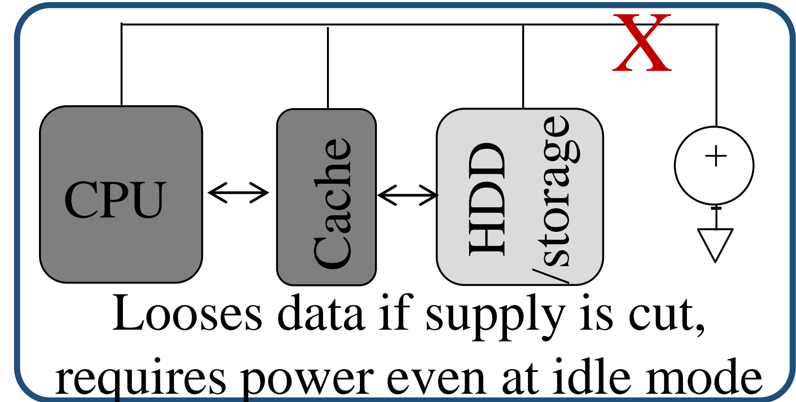
Mohammad Nasim Imtiaz Khan and Swaroop Ghosh

School of Electrical Engineering and Computer Science
The Pennsylvania State University

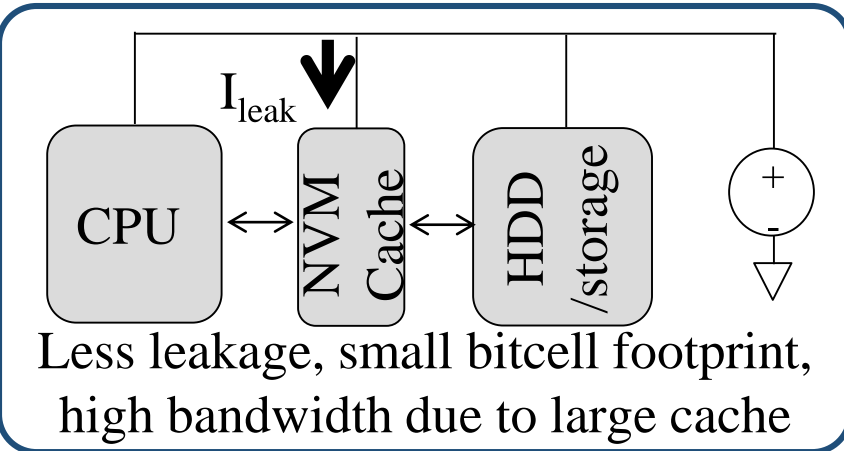
Why Emerging NVMs?

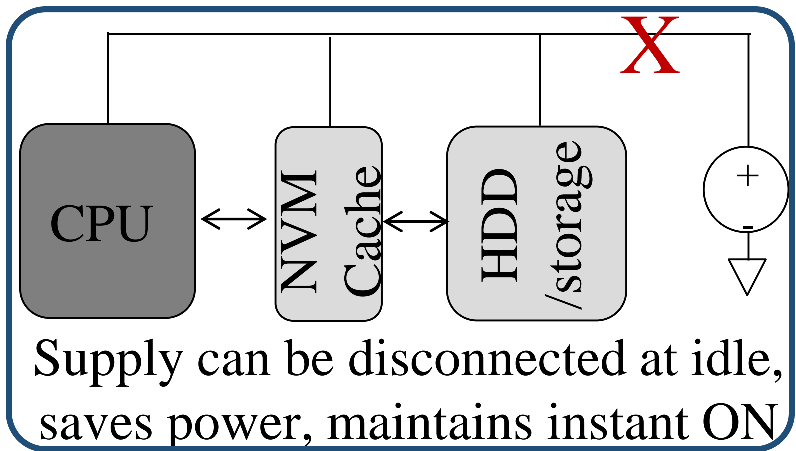
Conventional





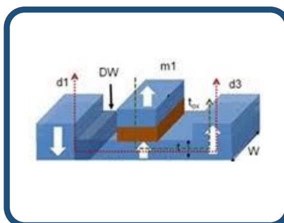
Emerging NVM



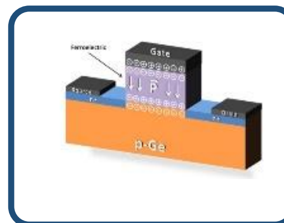


PCRAM

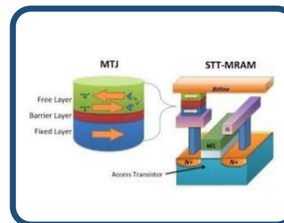
DWM



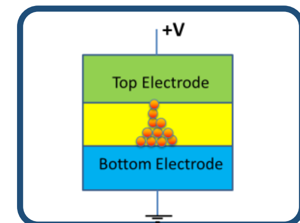
FeRAM



STTRAM

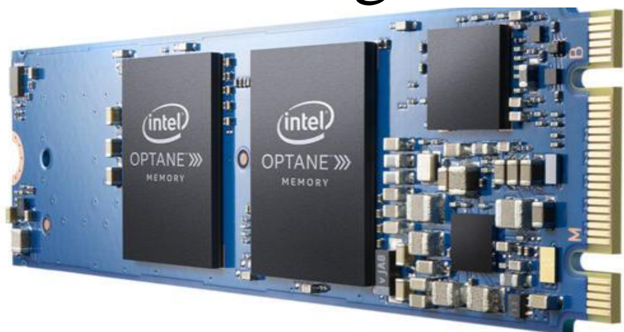


ReRAM



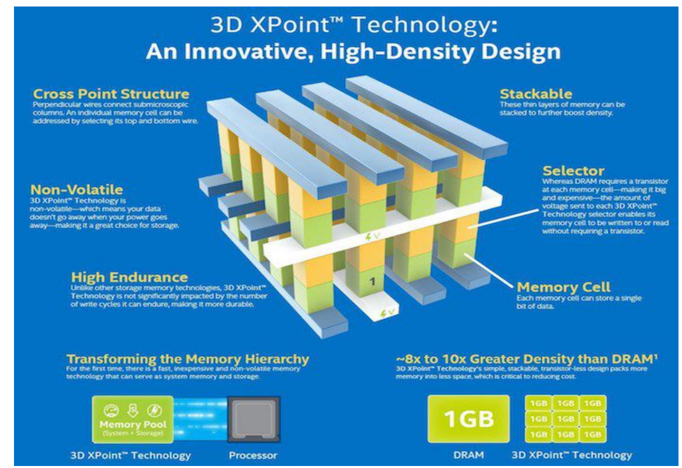
Recent Commercialization of Emerging NVMs

Phase Change RAM



Intel unveils its Optane hyperfast memory

Intel released few key details around its new non-volatile memory

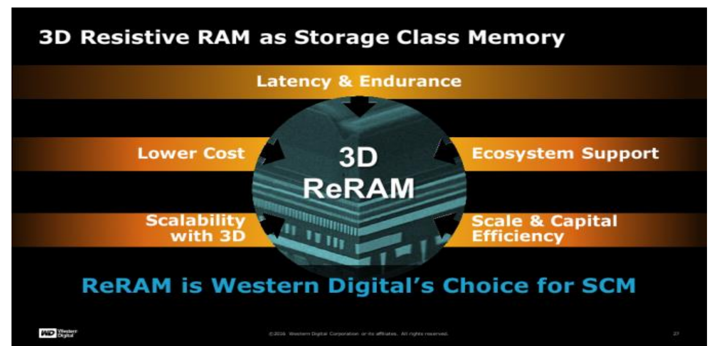


STT- MRAM

Published: *March 9, 2017*

Everspin unveils a new low latency, PCIe NVMe card based on Spin Torque MRAM

ReRAM

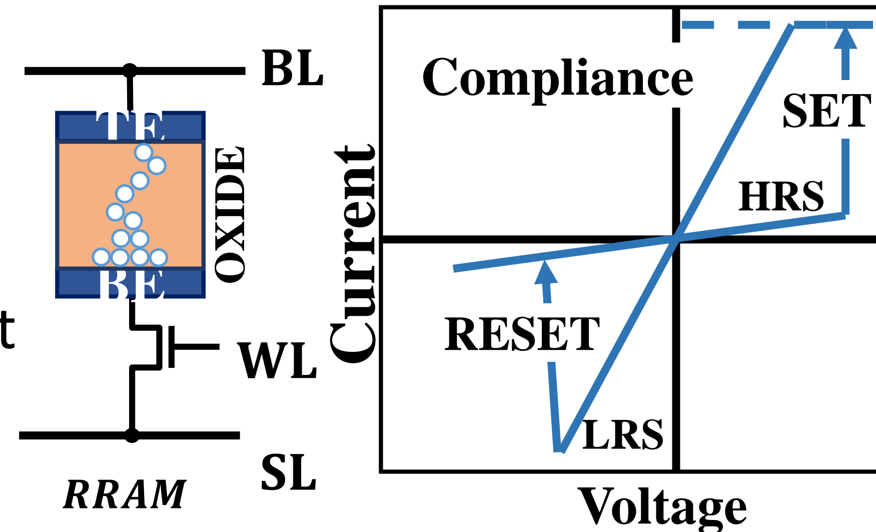


Western Digital to Use 3D ReRAM as Storage Class Memory for Special-Purpose SSDs

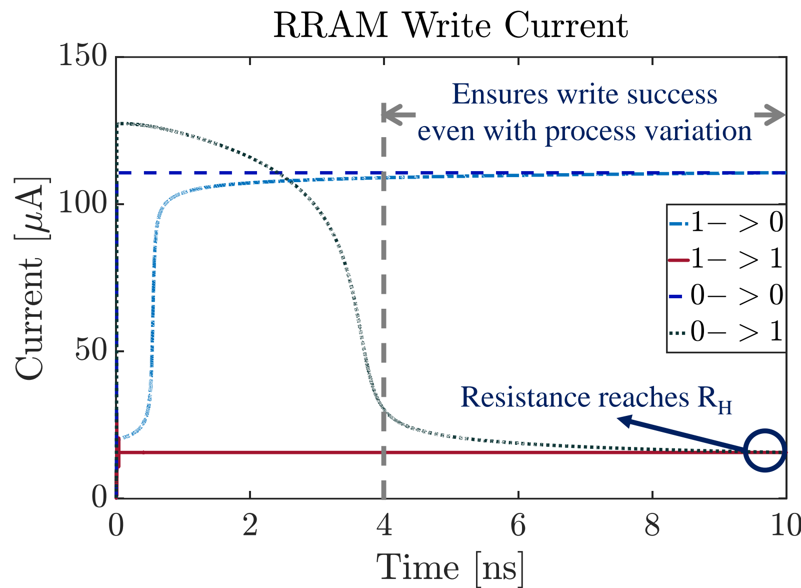
by Anton Shilov on August 12, 2016 8:00 AM EST

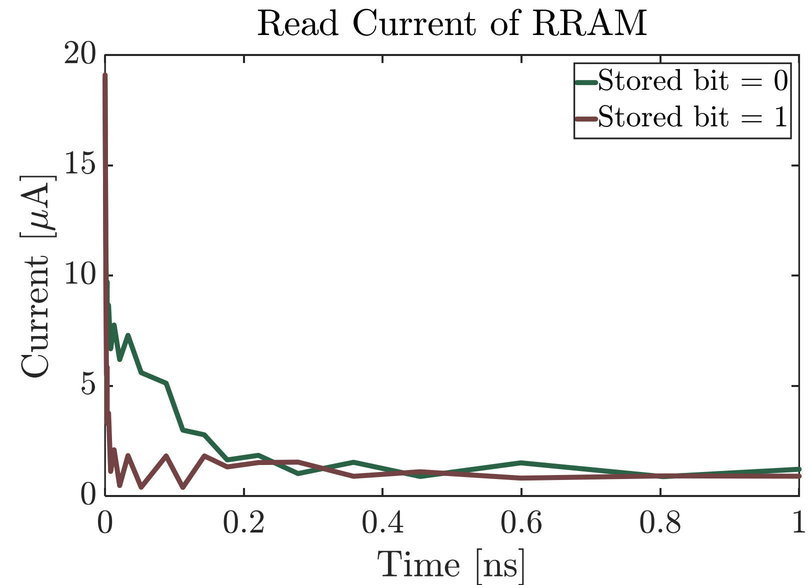
NVM: RRAM

- Read/write latency
  - Read/write of RRAM
- Read/write
  - Sensing RRAM resistance
  - Write: Conduction Filament
- Features
  - Footprint = ~12-24F^2
  - Random access
- Suitable for LLC/Main Memory



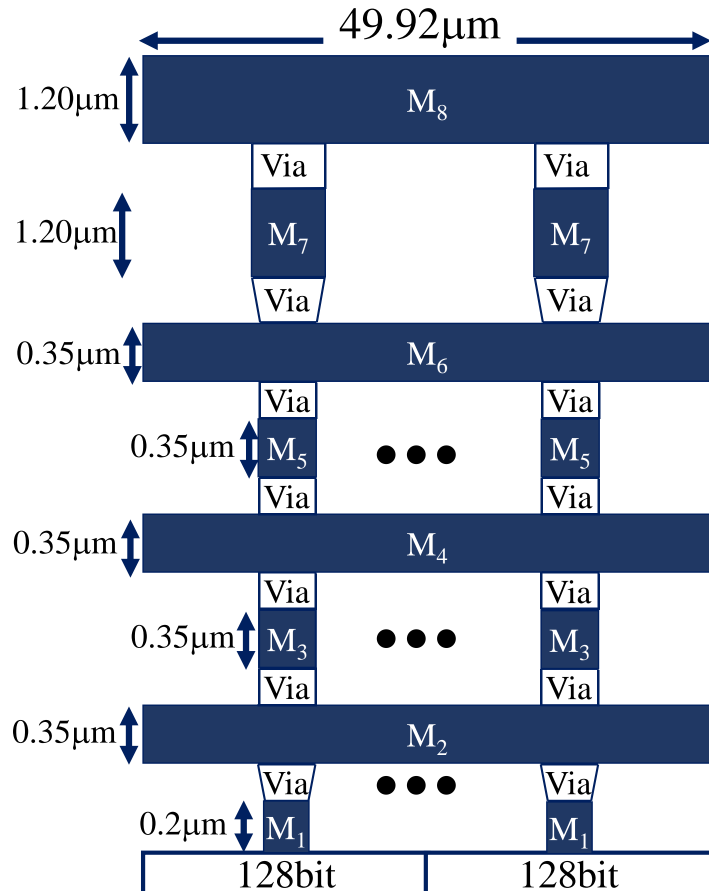
NVM Characteristics-Long Latency/High Current





- Long read/write latency (1ns/10ns for RRAM)
- Latency varies with process and temperature variation
- High write current (~100µA/bit)
- High read current (~10µA/bit)
- V_{dd} Droop/Gnd bounce due to high current

Supply Noise: Ground Bounce Modeling



R_1 Estimation

Number of Via (tapping) per 128bit (24.96µm):

M_8-M_7 = 1, M_7-M_6 = 2
M_6-M_5 = 4, M_5-M_4 = 4
M_4-M_3 = 8, M_3-M_2 = 8
M_2-M_1 = 8

$$R_1 = R_{Contact} + R_{Metal} + R_{Via}$$

$$R_{Metal} = \sum_{x=1}^{8} \frac{R_{Mx} * Metal\ Length}{Via\ Number} = 14.3867\Omega$$

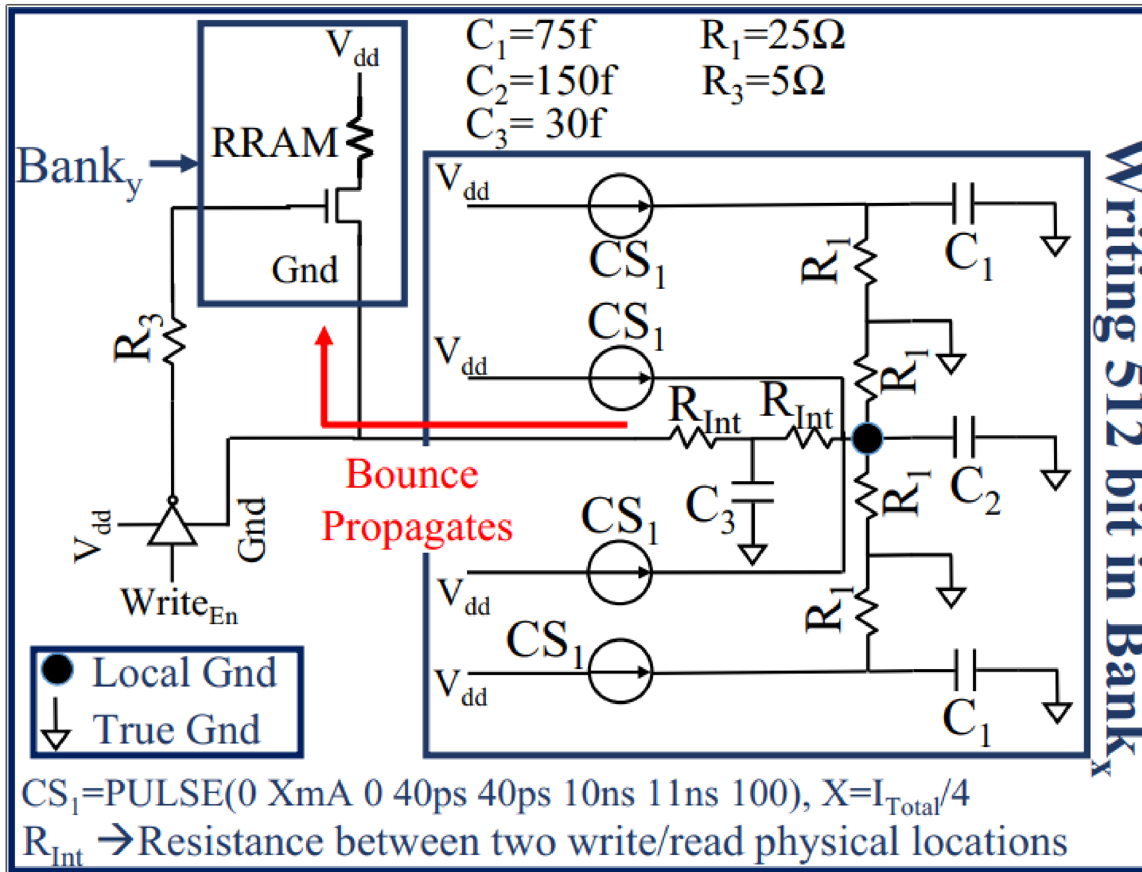
$$R_{Via} = \sum_{x=1, y=x+1}^{8} \frac{Via\ Resistance_{x-y}}{Via\ Numberx_{_y}} = 5\Omega$$

$$R_1 = 5 + 14.3867 + 5 = \sim 25\Omega$$

Supply line modeled for 65nm technology

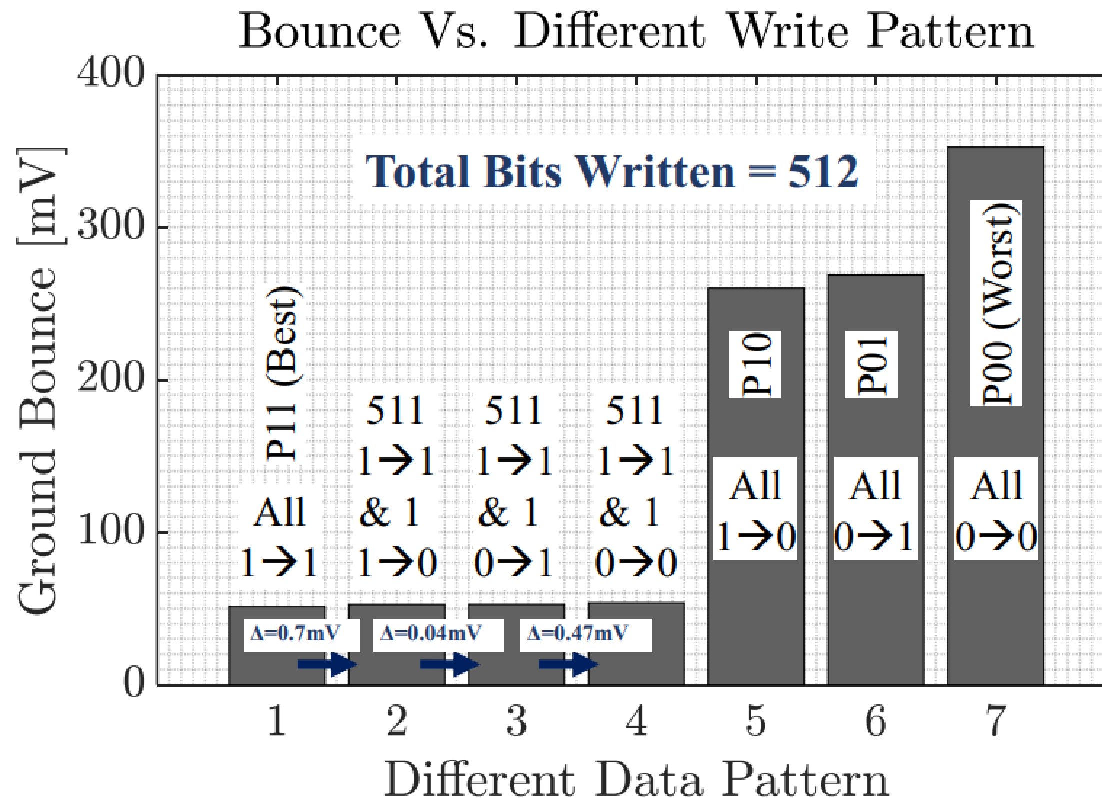
[1] "Interconnect: Capacitance and Resistance for 65nm technology." http://ptm.asu.edu/, 2005.
[2] "Wire Capacitance and Resistance Calculator for 65nm." http://users.ece.utexas.edu/~mcdermot/vlsi-2/Wire_Capacitance_and_Resistance_65nm.xls, 2008.

Supply Noise: Ground Bounce Modeling (Contd.)



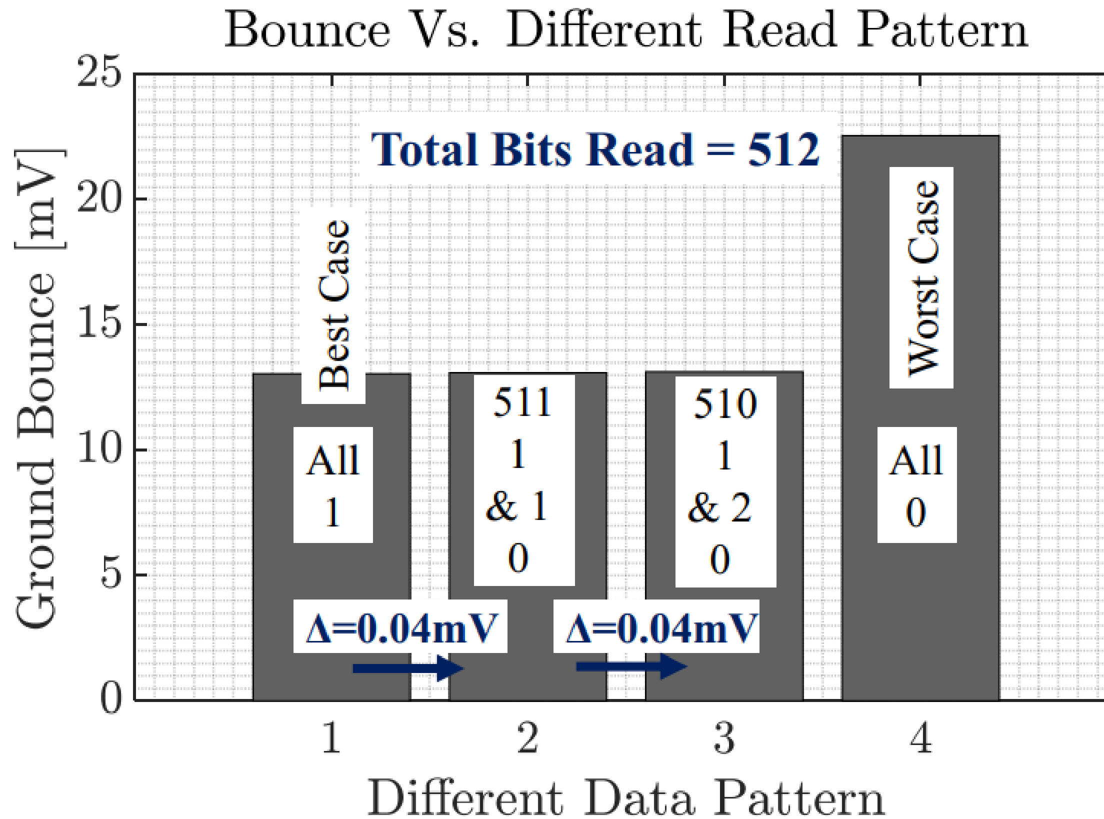
- R_1 : Resistance from M_8 to M_1
- CS: Constant Current Source
  - Each one represents read/write current of 128bits

Supply Noise: Ground Bounce Vs Write Data Pattern



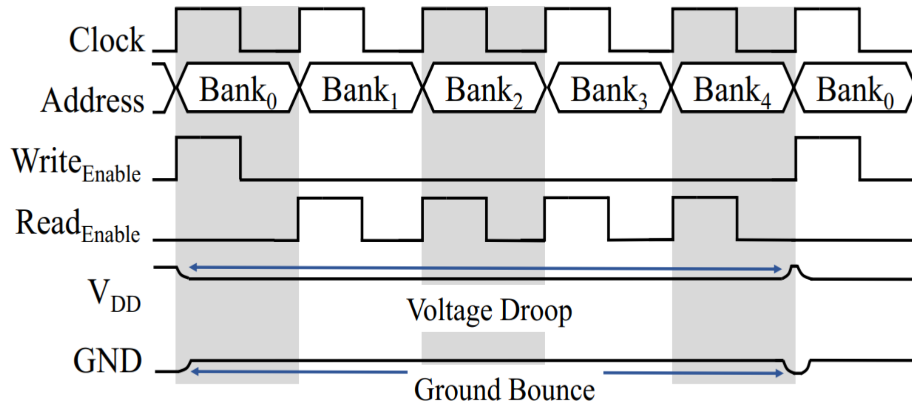
- Depends on write data pattern
- Lowest/highest ~51mV/~352mV
- Can be controlled at the granularity of 1mV

Supply Noise: Ground Bounce Vs Read Data Pattern

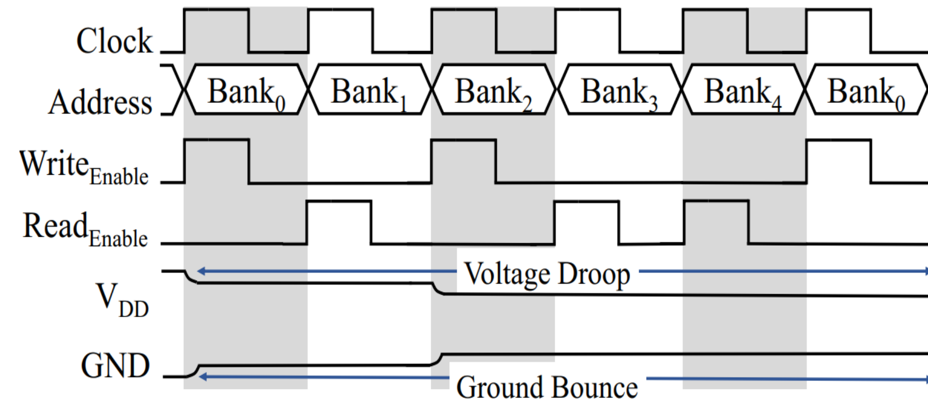


- Depends on read data pattern
- Lowest/highest ~13mV/~23mV
- Can be controlled at the granularity of 0.04mV

Parallel Accesses



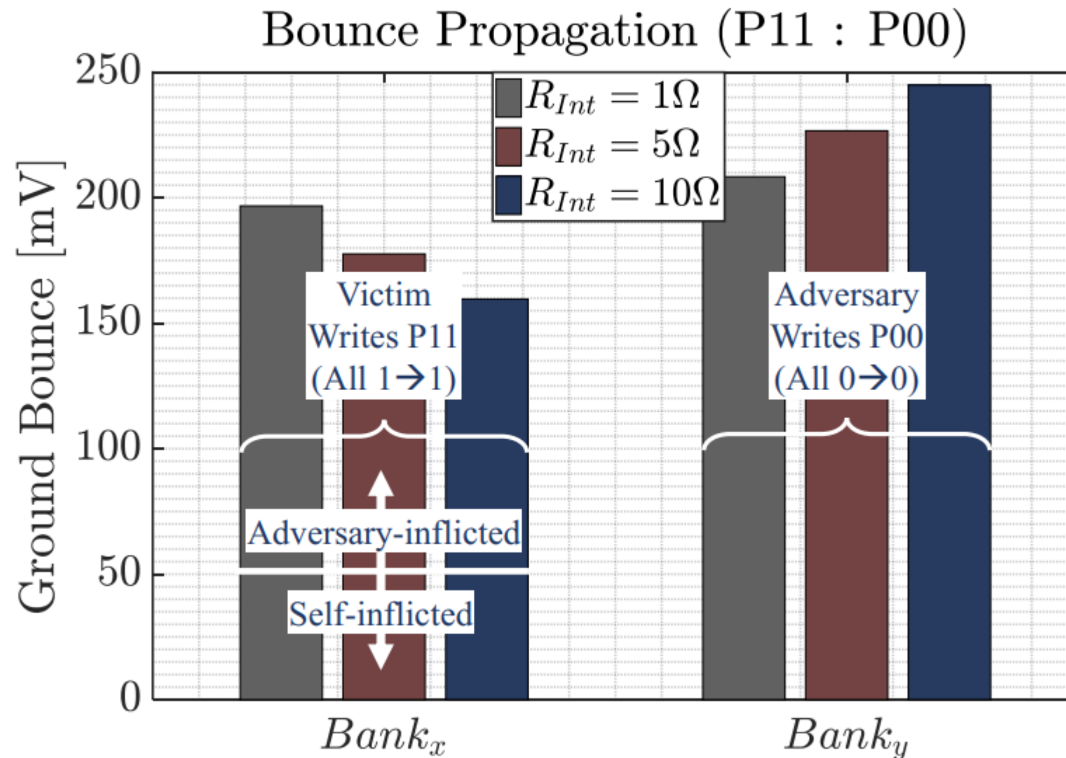
1X Write



2X Write

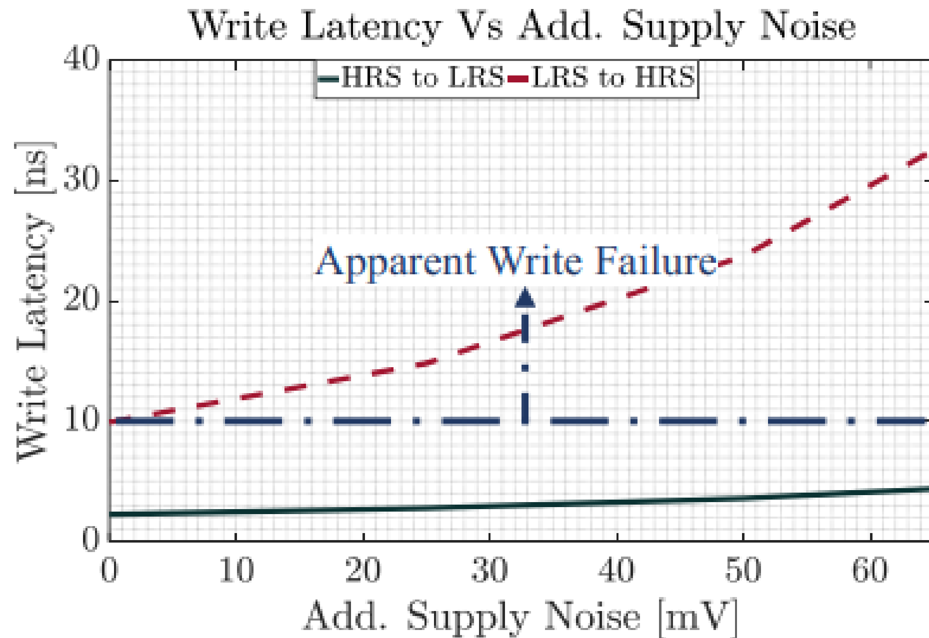
- Read/write takes multiple clock cycles
- Parallel operations on independent banks
  - Increases throughput
- Worsen supply noise
- Operations can affect each other

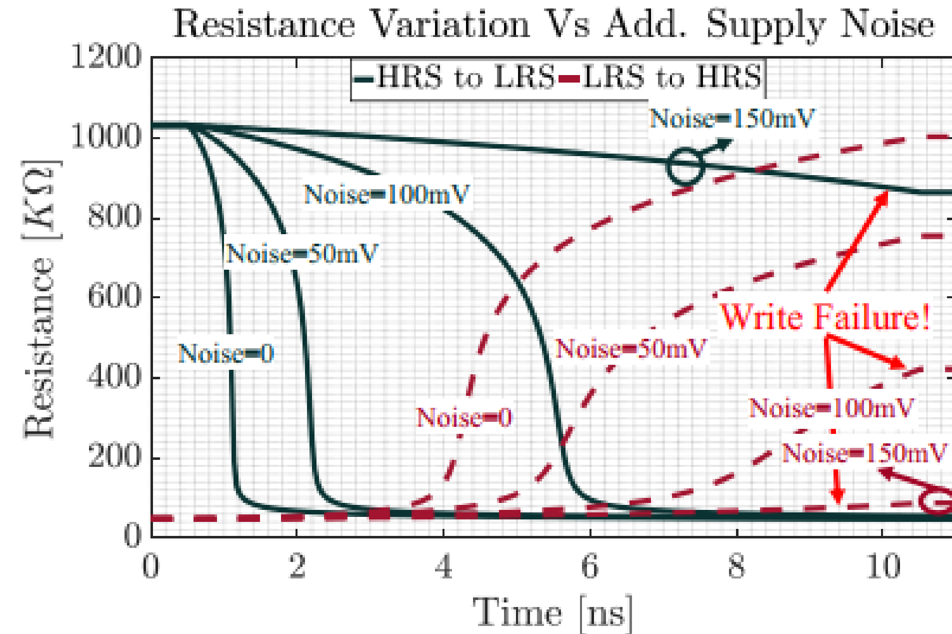
Supply Noise: Ground Bounce Propagation



- Victim/adversary writes P11/P00 in $Bank_x$/$Bank_y$ simultaneously
- Victim incurs both
  - Self inflicted bounce
  - Adversary inflicted bounce
- Adversary Inflicted bounce reduces as distance increases

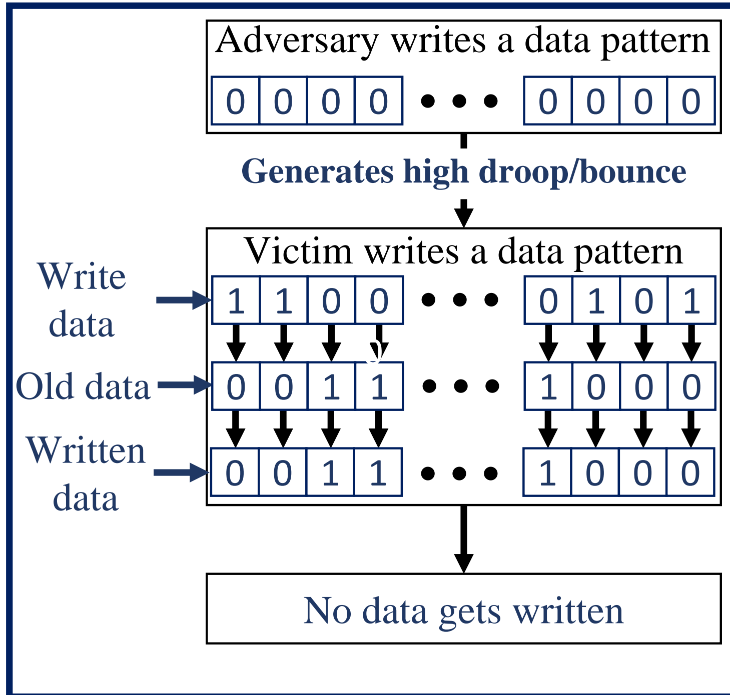
Impact of Supply Noise on Write Operation



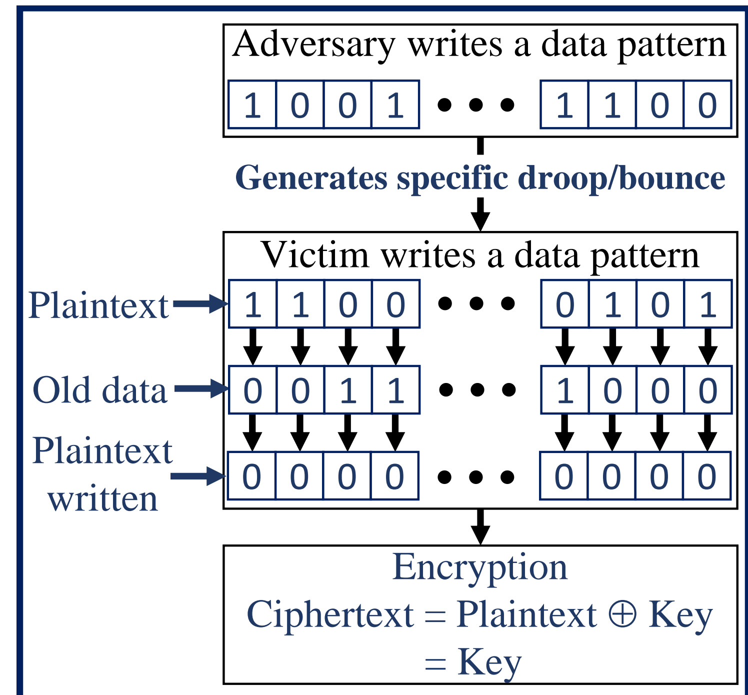


- Supply noise:
  - 0 to 50mV: No failure
  - 50 to 120mV: 0→1 write fails
  - >120mV: both write polarity fails

Fault Injection Attacks

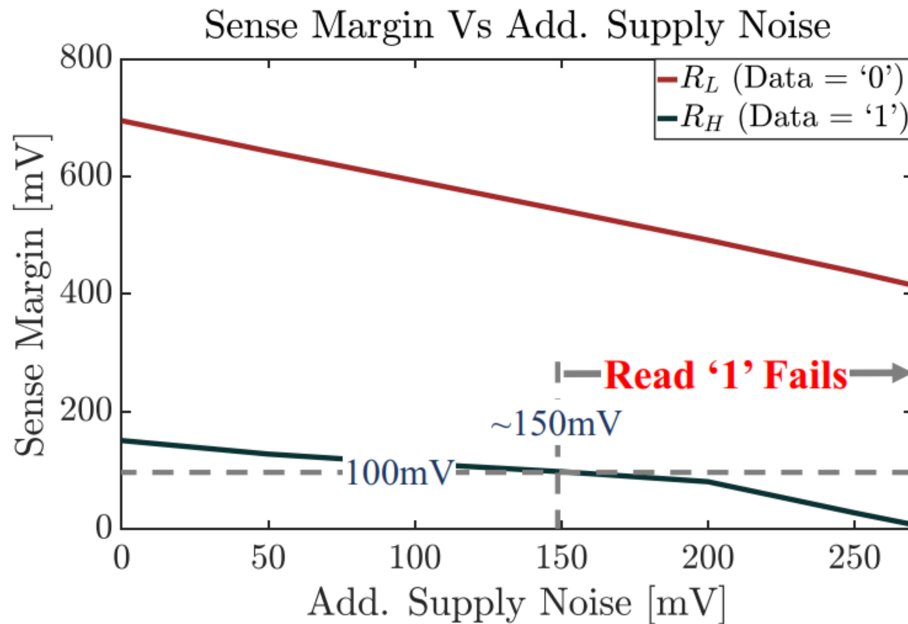


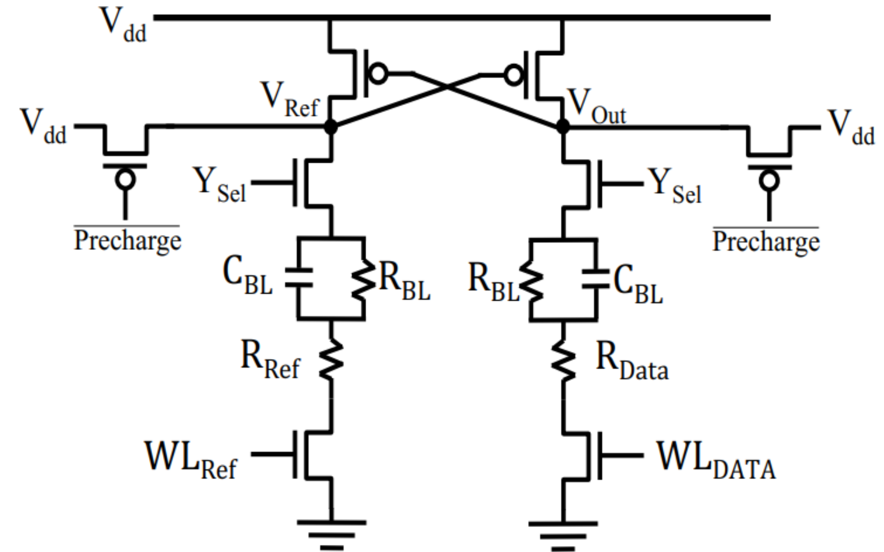
DoS Attack



Specific Polarity Fault Injection

Impact of Supply Noise on Read Operation





- Supply noise:
  - 0 to 150mV : No failure
  - >150mV : Read '1' Fails

Detection of Victim's Write Operation

1. Keep reading predefined store data at different location

2. Sense read failure

3. If read failure found at one address

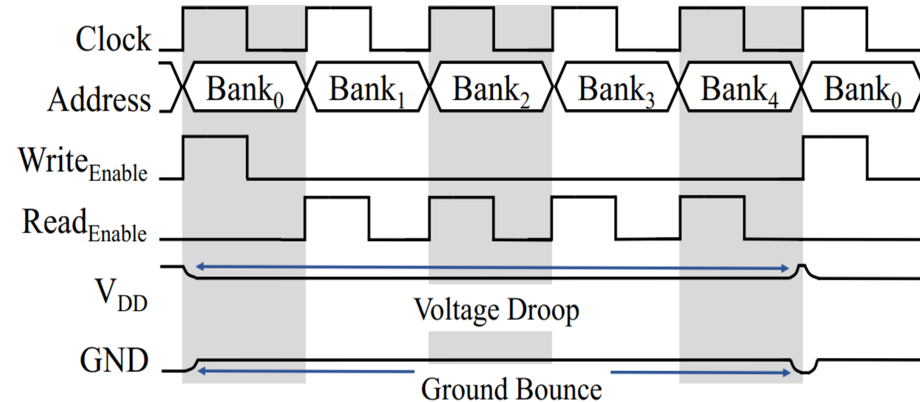
    - Victim writes in nearby location

    - Write detected!

4. Adversary writes to the nearby address (where read failure)

    - Generates supply noise

    - Can cause DoS/Fault injection based on noise generation



Details to appear in ISLPED 2018

Mitigation

- Only sequential accesses
  - Hurts throughput
- Novel architecture
  - Parallel accesses with highest physical distance
  - Alleviates the issue to some extent
- Good quality power grid
  - Incurs area-overhead
  - Alleviates the issue to some extent
- Power rail separation for each bank
  - Incurs area-overhead
  - Alleviates the issue to some extent
- Slow down the system clock
  - Hurts the throughput
- Memory Testing
  - Exhausted testing incurs high test time
  - Weak bits still vulnerable to attacks specially unspecified temp. ranges

Conclusion

- We discussed new fault models specific to NVMs
- We modeled supply noise
- We discussed impact of supply noise on read/write
- We described fault injection attacks on NVMs
- We presented countermeasures

Acknowledgements

This work was supported in part by

National Science Foundation (NSF) CNS- 1722557, CCF-1718474 and DGE-1723687

Defense Advanced Research Projects Agency (DARPA) Young Faculty Award [#D15AP00089]

Thank You!

Contact:

Md Nasim Imtiaz Khan (muk392@psu.edu) Dr Swaroop Ghosh (szg212@psu.edu)