Exploiting Emerging Memory Technologies for Hardware Security

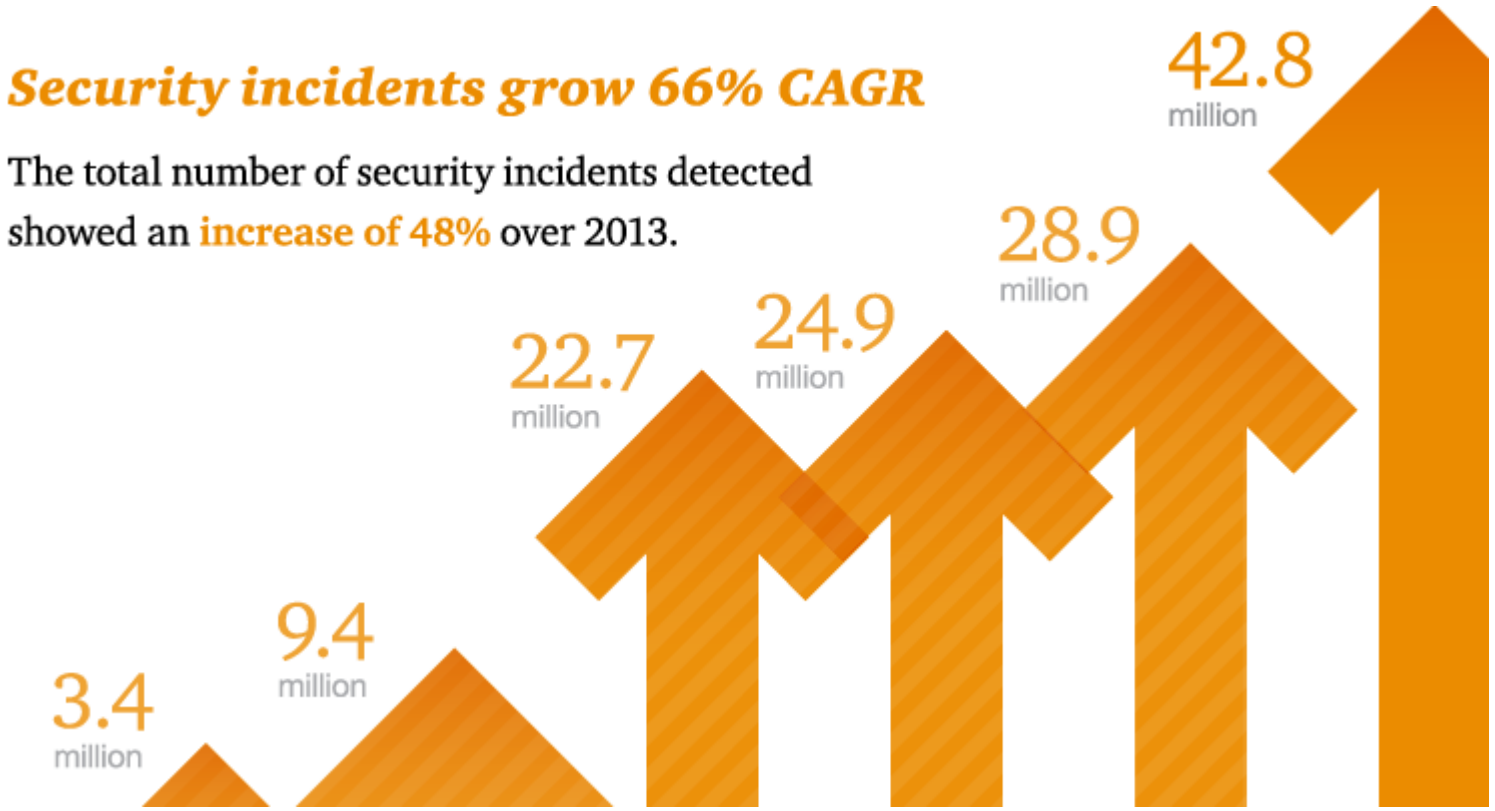
Dr. Swaroop Ghosh

School of Electrical Engineering and Computer Science, The Pennsylvania State University

PennState

Lab of Green & Secure Integrated Circuit Systems (LOGICS)

Why We Should Care?



Why We Should Care?

Banking

Aviation

consumer

automobile

Government

Critical infrastructure

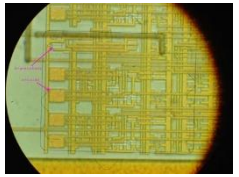
finance

The New Trend

- Software level security policies assume hardware to be secure
  - Not the case anymore

Motivational Examples

Hacking PIC uC




Vulnerability: UV-EPROM

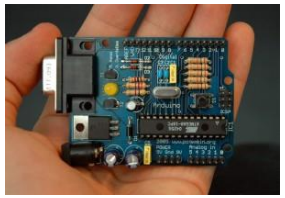
Hacking Apple battery

Vulnerability: hardcoded passwords

RFID snooping&cloning

Vulnerability: unencrypted communication

Hacking hotel key



Vulnerability: unprotected key

Hacking smart meter

Vulnerability: unprotected key

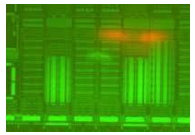
Outline

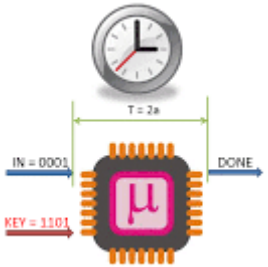
- Basics of hardware security
- CMOS security primitives
- Emerging technologies
- Application in security
- Conclusions

Side Channel Attacks

Voltage, current

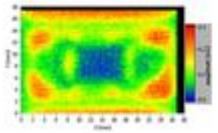
light



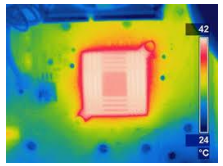


time

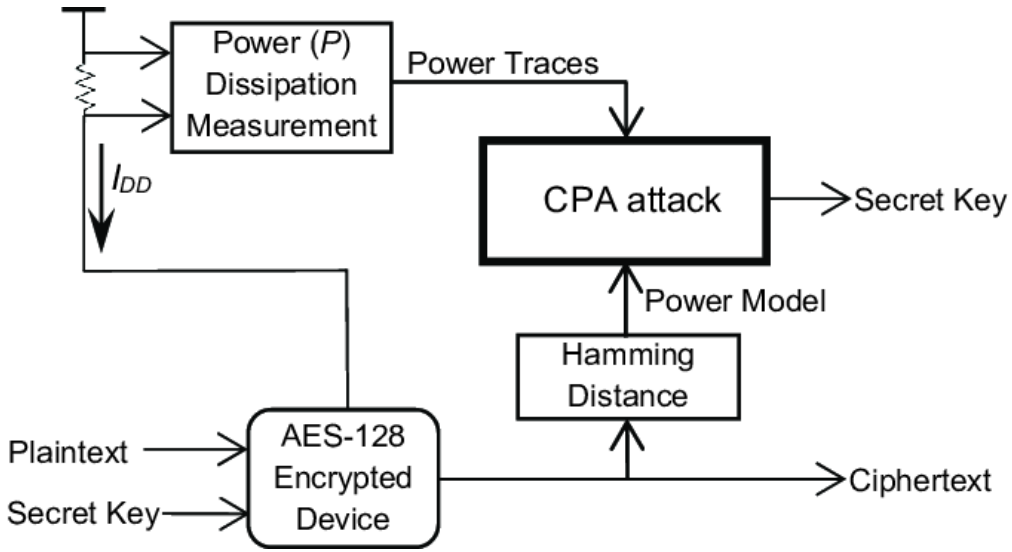
EM



heat

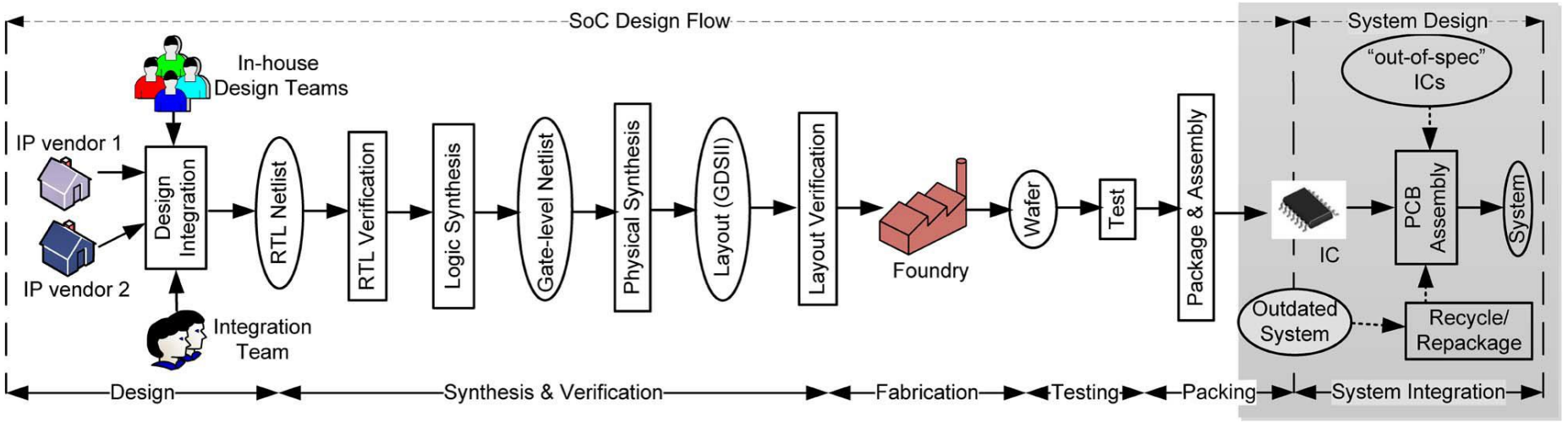


sound



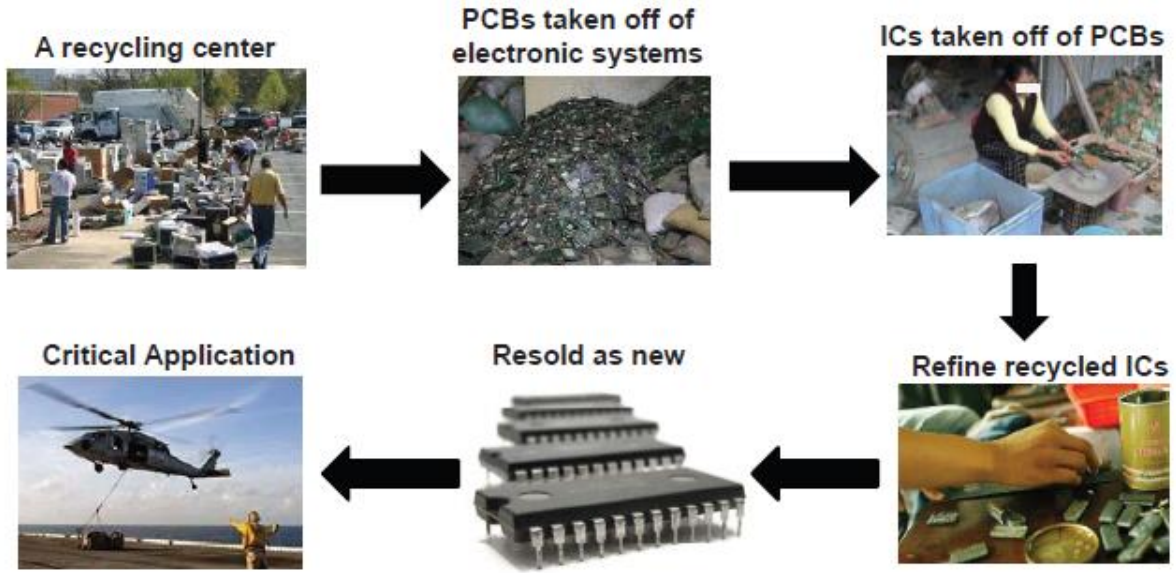
- Possible sources: electrical, ambient, acoustical, temporal…
- Objective: extract valuable information

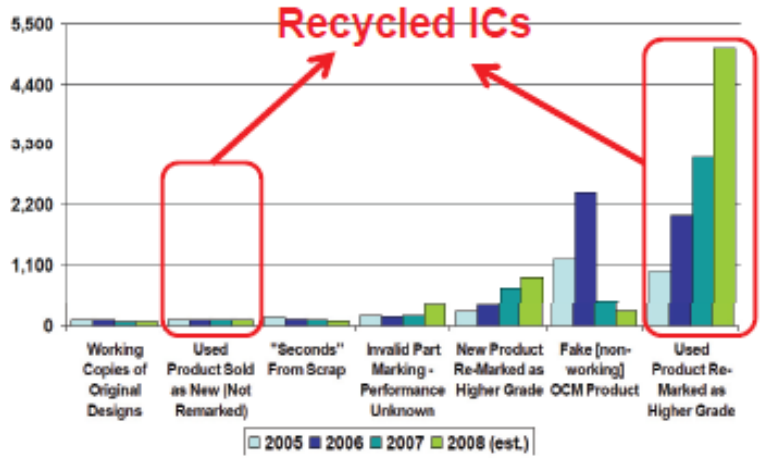
Semiconductor Supply Chain



- Profit driven business model that relies on outsourcing
  - Security vulnerabilities present at many stages of design and manufacturing process
- Attacks
  - Counterfeiting
  - Hardware Trojan Horses
  - Cloning
  - Overproduction
  - Reverse engineering
  - Non-invasive tampering

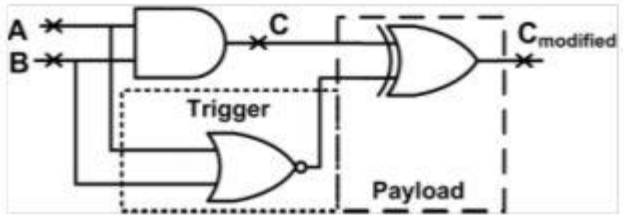
IC Recycling/Counterfeiting



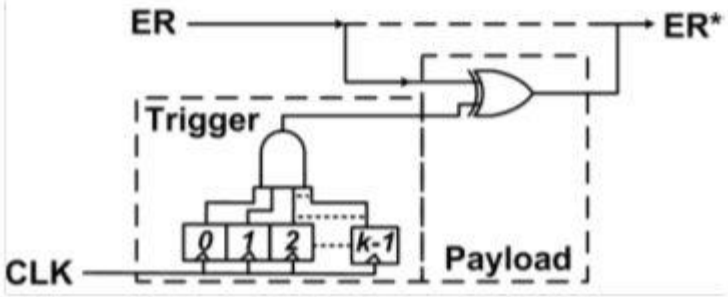


Hardware Trojans

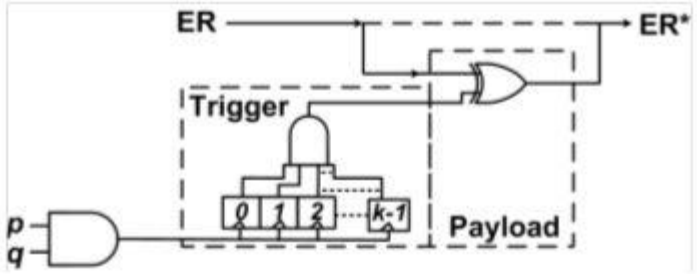
- Undesirable/ unintended design features to
  - Bypass security features
  - Bypasses convention test methods
  - Triggers in-field failures



(a) Combinationally triggered Trojan

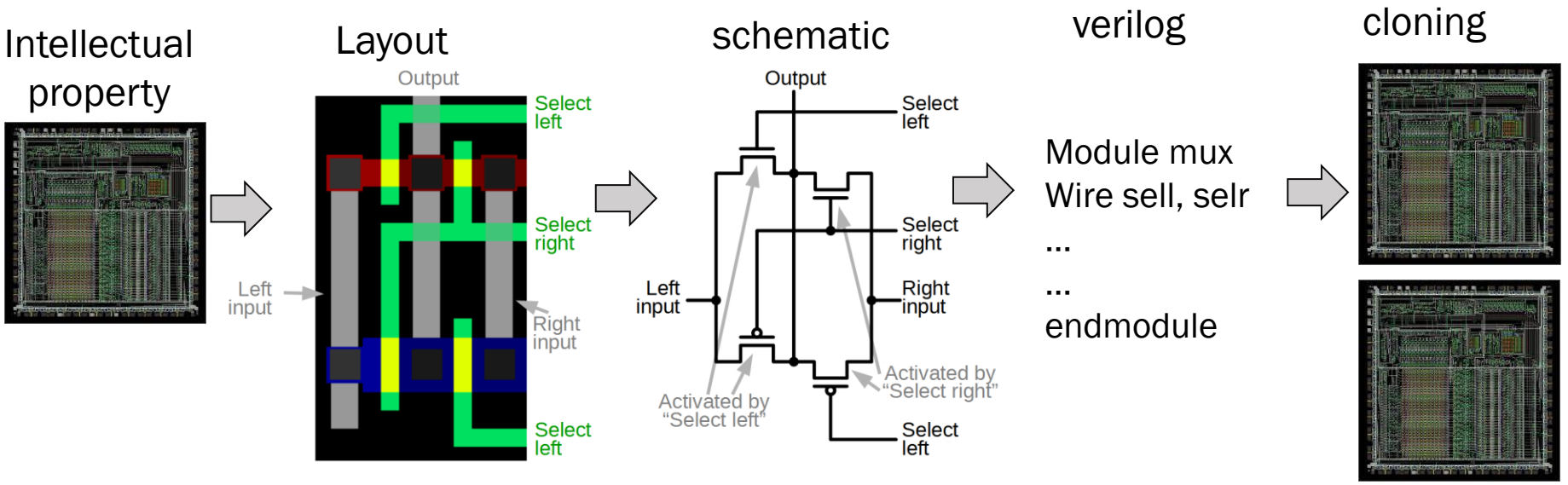


(b) Synchronous counter ("time-bomb") Trojan



(c) Asynchronous counter Trojan

Reverse Engineering and Cloning



- Delayering of chip, identification of gates and their connectivity information, and, reconstruction of netlist
  - Goals: competitive analysis, cloning and overproduction, siphoning profit

Non-Invasive Tampering

laser

X-ray gun

magnet

UV light

heat

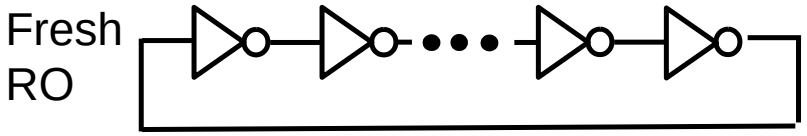
Ion gun

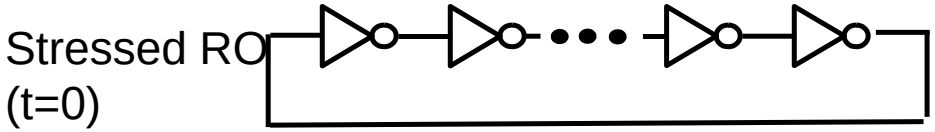
- Objective is to
  - Bypass security features
  - Launch denial-of-service attack
  - Extract valuable information

Outline

- Basics of hardware security
- CMOS security primitives
- Emerging technologies
- Application in security
- Conclusions

Recycling Sensor





Case-1

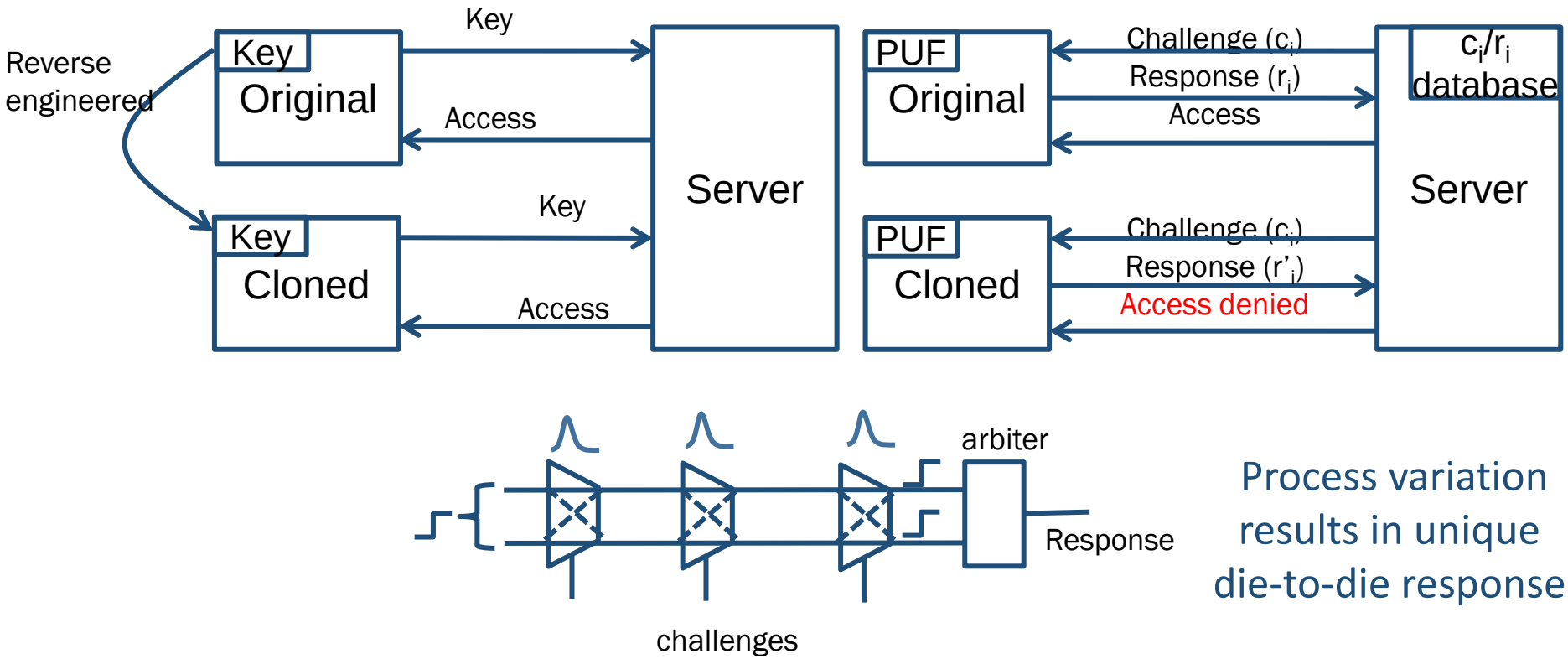
Shaded chips are flagged recycled

Case-2

Recycling of shaded chips are masked

- Aged RO is compared with fresh RO
- Challenges
  - Process variation results in wrong decision or masking
  - Limited by aging of RO and delay sensitivity of RO on aging
- Prevents recycling/counterfeit ICs

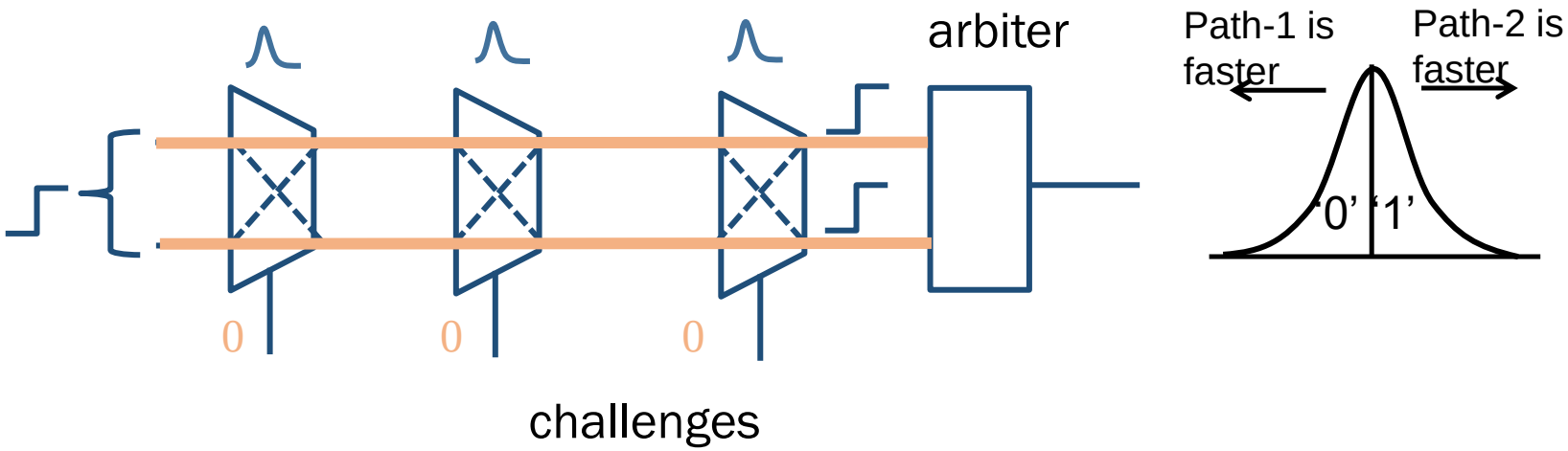
Physically Unclonable Functions



Process variation results in unique die-to-die response

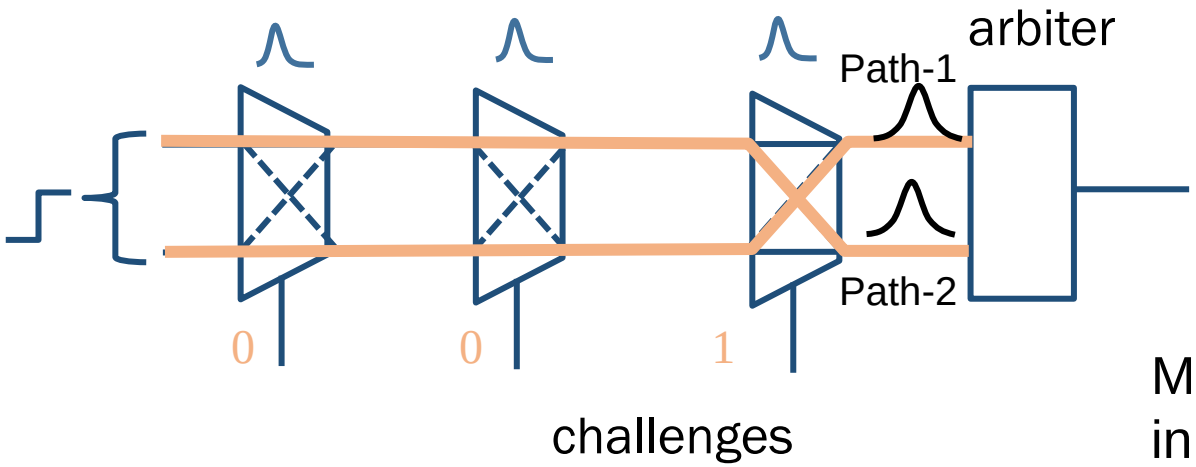
- PUF replaces the hardcoded key with a challenge response system
  - Response is generated from physical properties of the chip
  - Cannot be cloned
- Prevents cloning, counterfeit IC

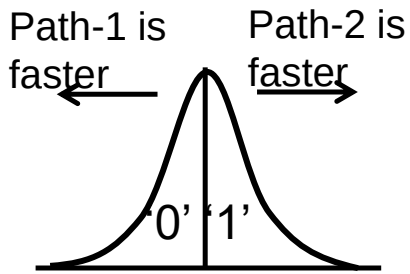
Physically Unclonable Functions



- Different chips produce different responses for same challenge

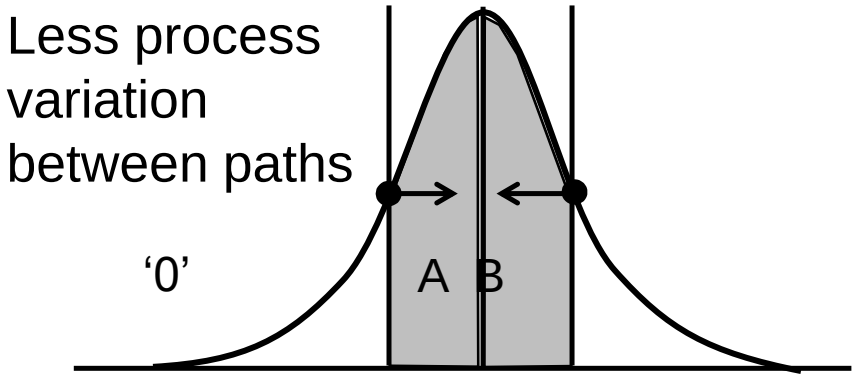
Physically Unclonable Functions





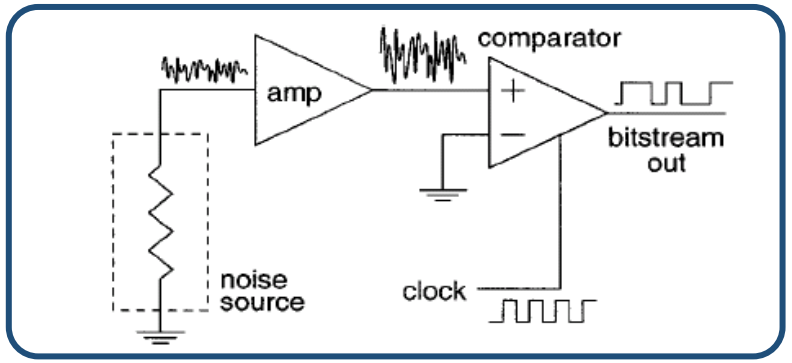
- Process variation is good

More responses in shaded area

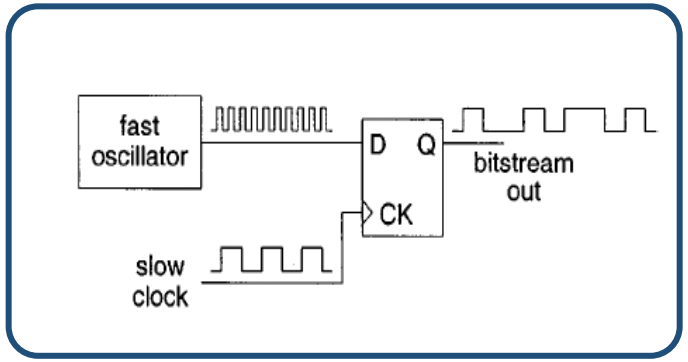


True Random Number Generator

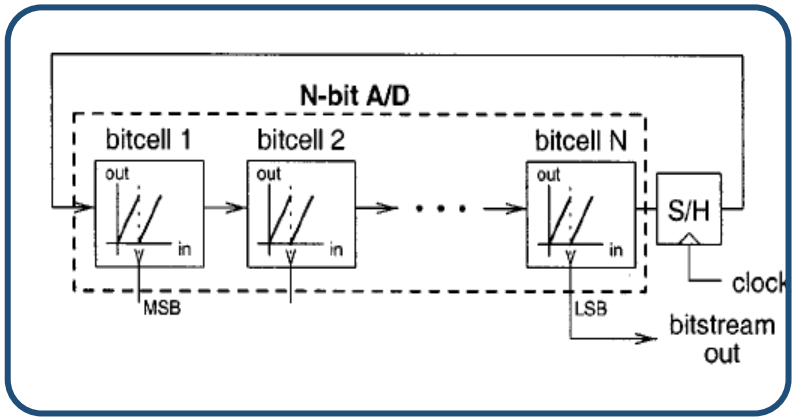
Direct amplification



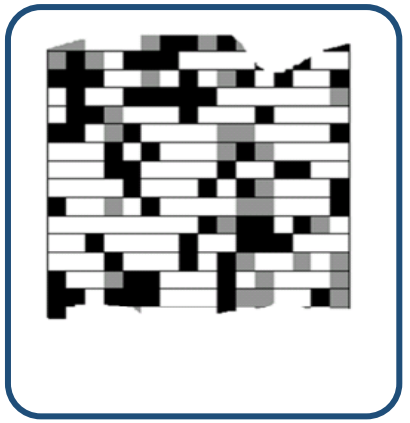
Oscillator sampling



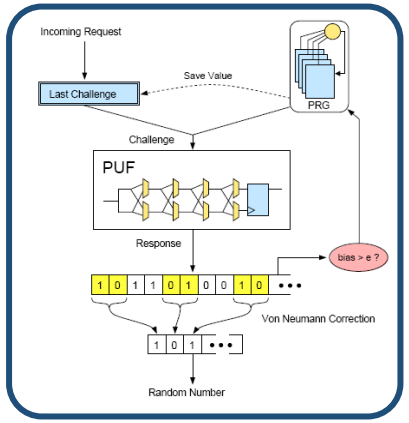
Discrete time chaos



SRAM PUF



PUF

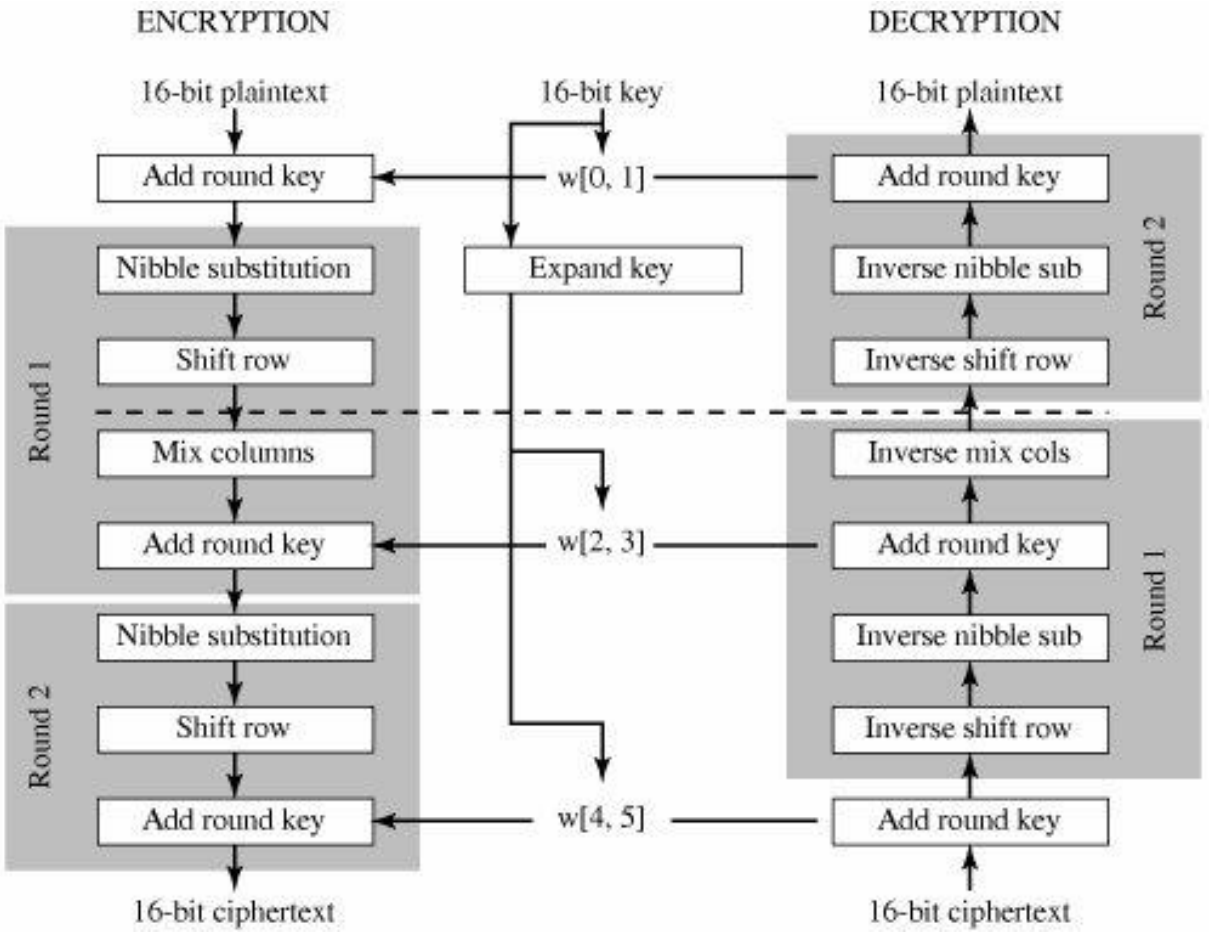


- Key generation and seed generation for authentication, secure communication

Petrie, Craig S., and Alvin Connelly. "A noise-based IC random number generator for applications in cryptography." Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on 47, no. 5 (2000): 615-621.

Encryption Engines

- Ensures privacy in communication
- Requires extensive shift, XOR and addition operation
  - Prone to side channel attack



Hardware Security Primitives- Key Requirements

Security primitive	Key Requirements
Recycling sensor	Low process variation, high sensitivity to usage
PUF	High process variation, nonlinearity
TRNG	High entropy
Encryption	Recursive shift, multiplication, addition
Miscellaneous	Sensitivity to ambient parameters

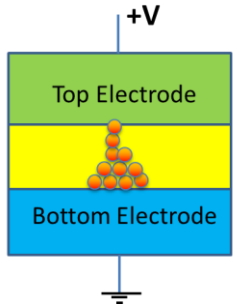
Outline

- Basics of hardware security
- CMOS security primitives
- Emerging technologies
- Application in security
- Conclusions

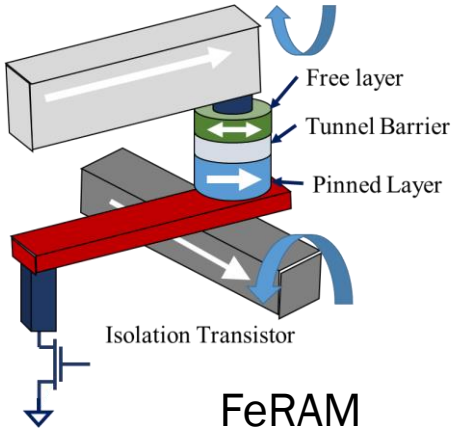
Emerging Technologies

- Opportunities
  - Non-volatility, electroforming, asymmetric read/write, retention, magnetization noise, stochastic resistance, non-linearity, random DW dynamics…
- Challenges
  - Vulnerabilities
- Need deeper understanding for right application

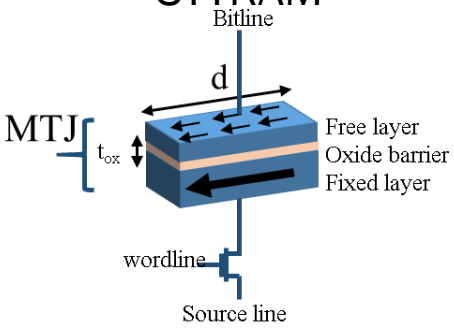
ReRAM



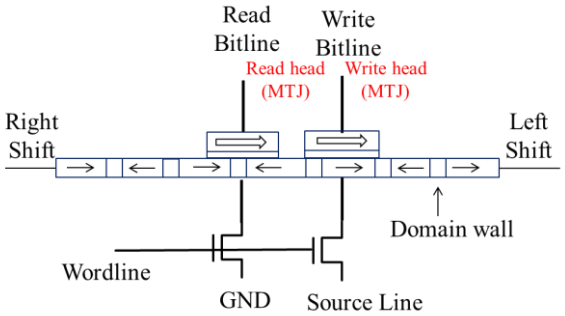
MRAM



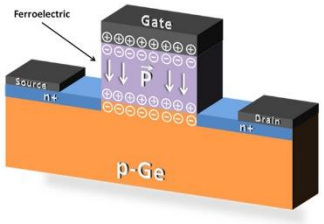
STTRAM



DWM



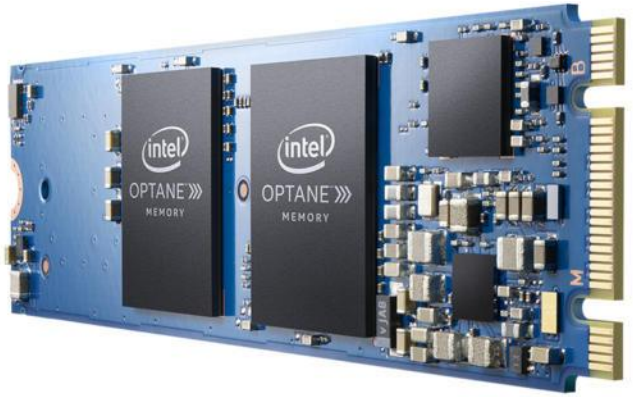
FeRAM



PCRAM

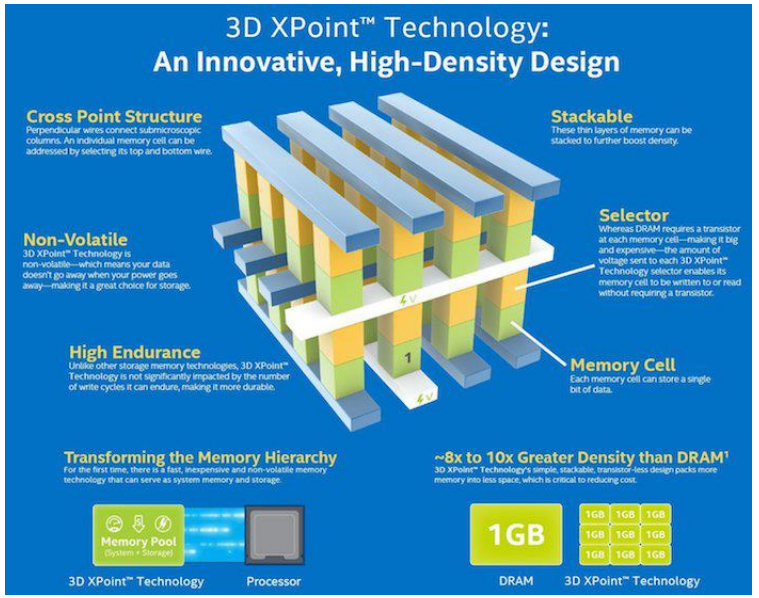
Recent Commercialization of Emerging NVMs

Phase Change RAM*

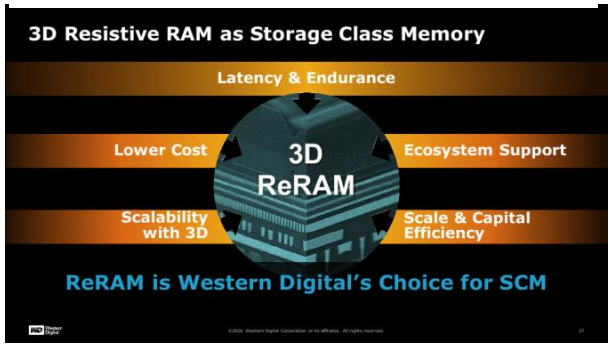


Intel unveils its Optane hyperfast memory

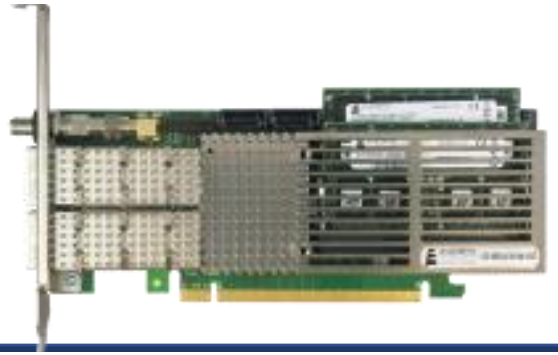
Intel released few key details around its new non-volatile memory



ReRAM



STT- MRAM



Published: *March 9, 2017*

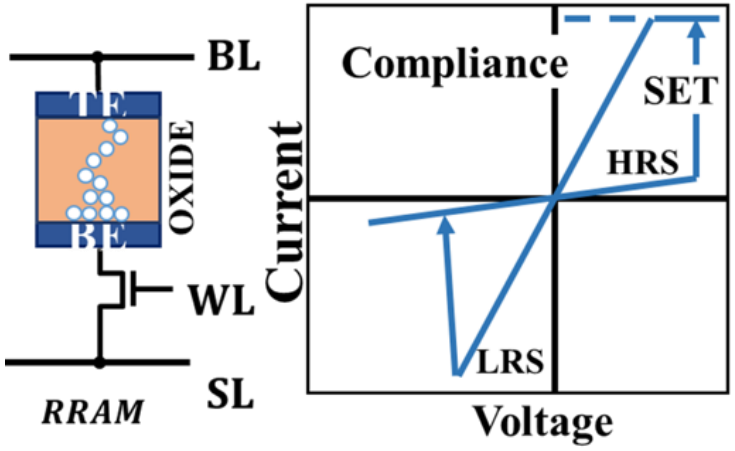
Everspin unveils a new low latency, PCIe NVMe card based on Spin Torque MRAM

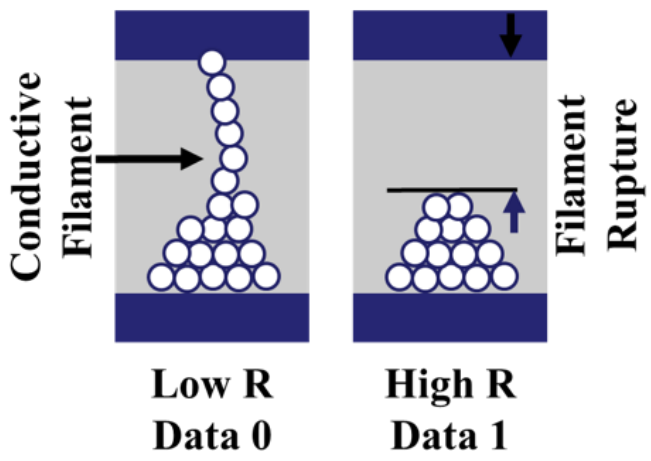
Western Digital to Use 3D ReRAM as Storage Class Memory for Special-Purpose SSDs

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

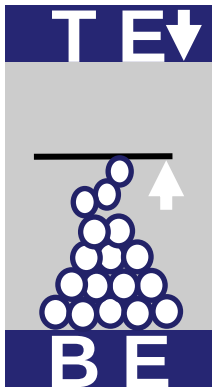
NVM: Resistive RAM (ReRAM)

- ReRAM Features
  - Bits stored as resistance state
  - Low R ⟶ Data “0”, High R ⟶ Data “1”
  - Possible Oxides: HfO_2, TiO_2, TaO_x,WO_x
- Offers lowest footprint ($4F^2$ for xpoint)



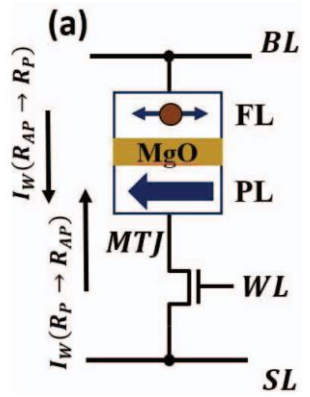


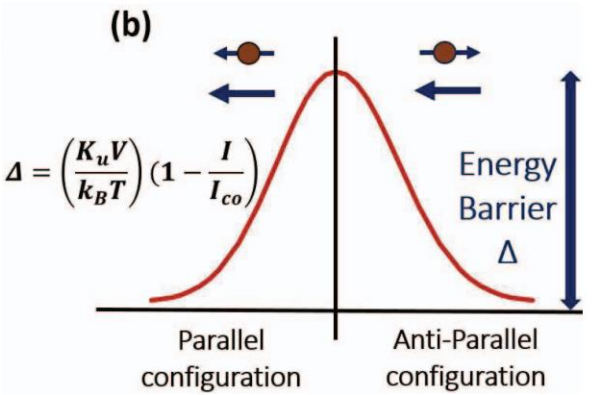
Many Possible Resistance Levels



NVM: Spin Torque Transfer RAM (STTRAM)

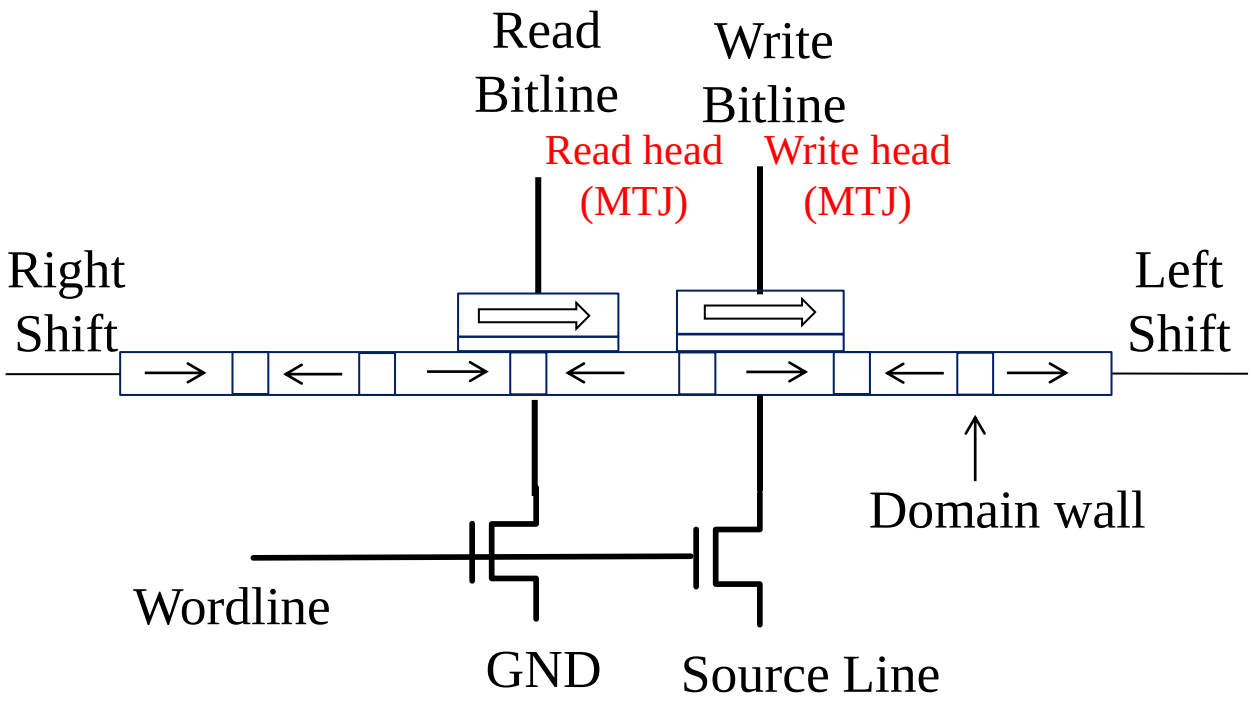
- STTRAM Features
  - Magnetic Tunnel Junction (MTJ) as Storage element
  - MTJ consists of free (FL) and pinned (PL) magnetic layer
  - Bits stored as resistance state
  - Magnetic Orientation
    - **Data "0"**: Parallel (Low resistance)
    - **Data "1":** Anti-parallel (High resistance)





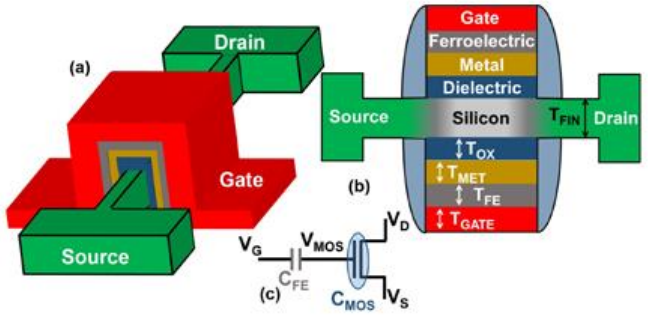
Domain Wall Memory

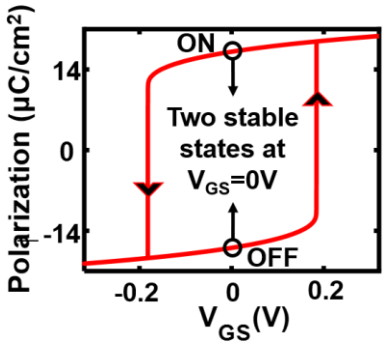
- DWM Features
  - Three components: Read MTJ, Write MTJ, Nanowire
  - Bits are stored in nanowire that acts like a shift register
  - Access mechanism is serial

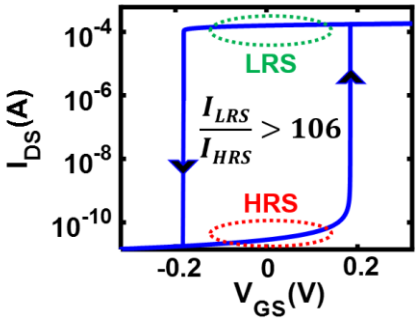


NVM: Ferroelectric FET (FeFET)

- FeFET features
  - Ferroelectric (FE) layer between metal gate and dielectric layer
  - Stores data as polarization state (+ve or -ve) of FE layer
  - Inherent 3-terminal structure allows isolation of read and write ports
  - If +ve V_{GS} > gate critical voltage ⟶ polarization switches to positive



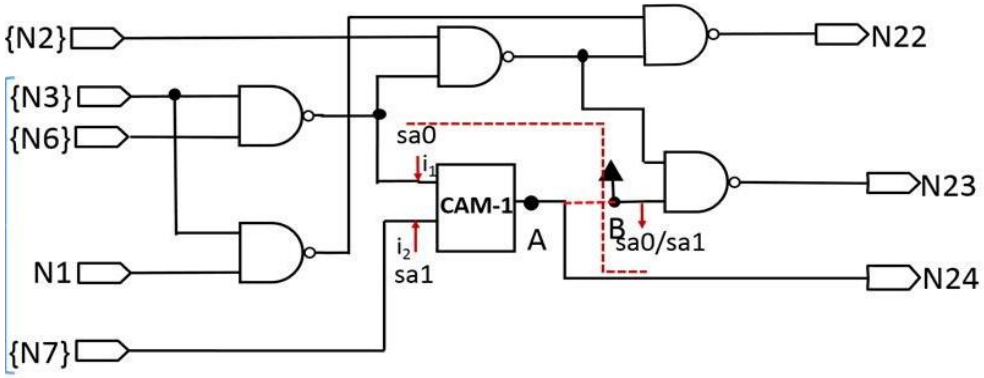


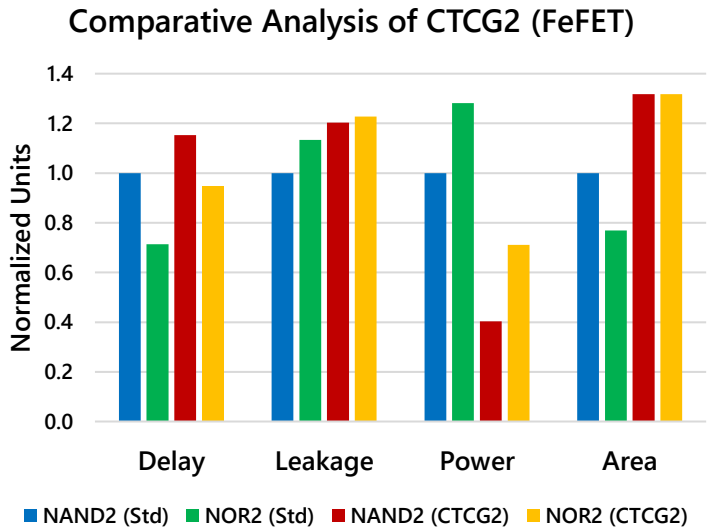


Outline

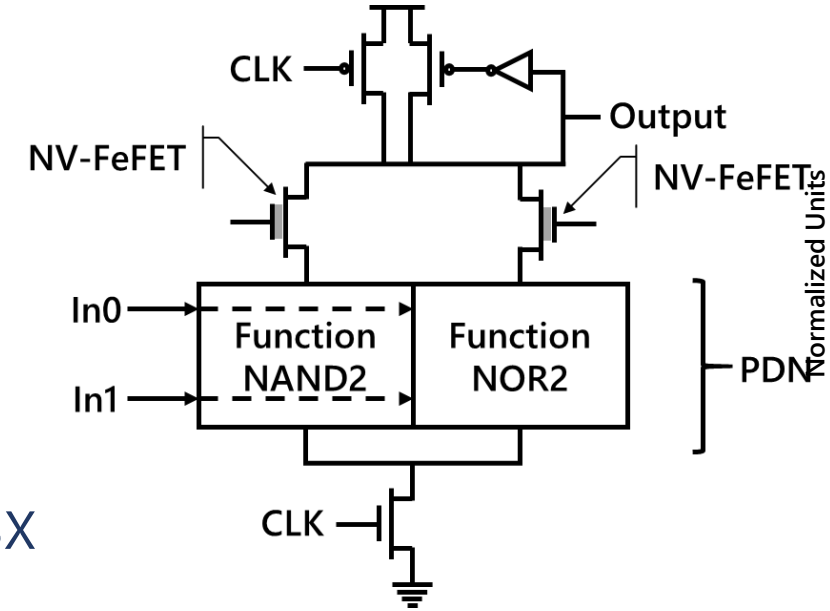
- Basics of hardware security
- CMOS security primitives
- Emerging technologies
- Application in security
- Conclusions

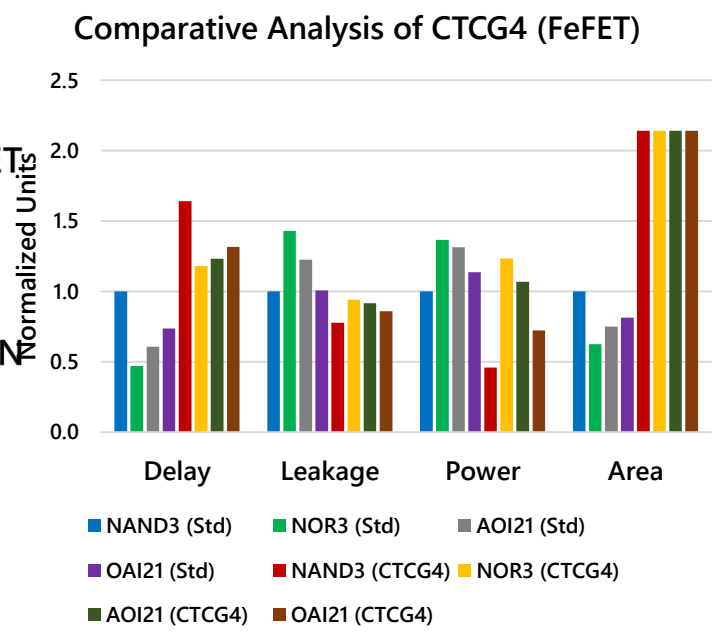
Exploiting Persistence-Obfuscation





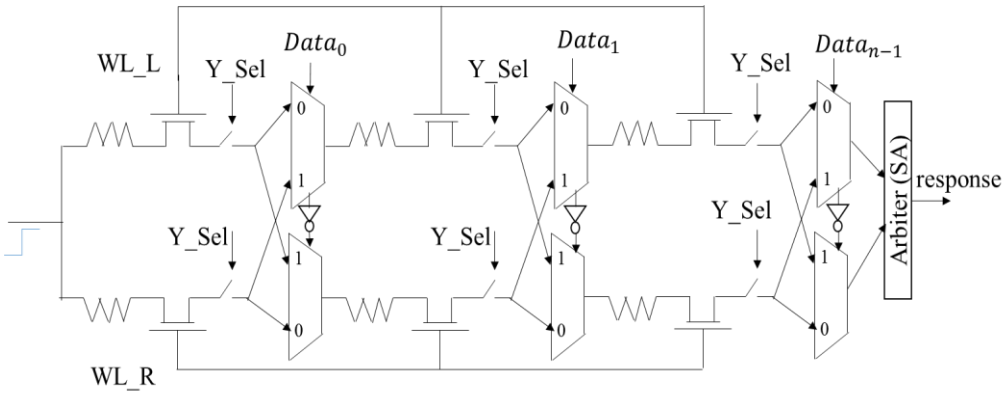
- Average delay overhead: 1.7X
- Average leakage overhead: 0.9X
- Average total power overhead: 0.6X
- Average area overhead: 2.3X

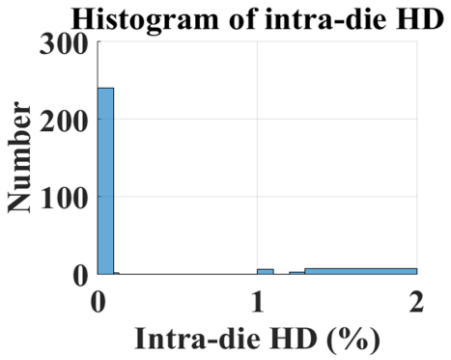


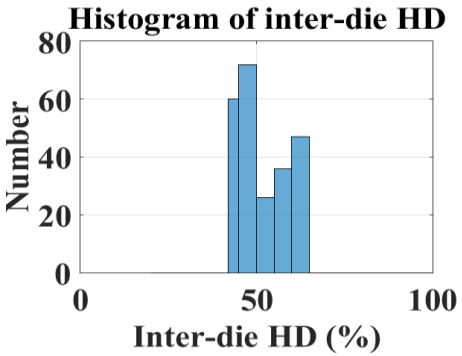


Exploiting Variations- Physically Unclonable Functions

- Design
  - PV in emerging NVM
  - RRAM based design using RC signal delay to generate PUF response

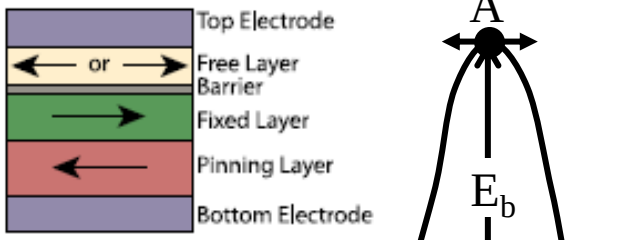


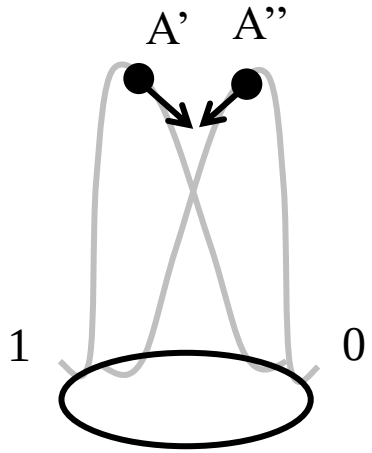




MRAM PUF

- Employs random initialization of the MTJ due to physical variations in the MTJ
- Variations create random tilt of energy barrier
- MTJ free layer is prone to prefer certain initial orientation much similar to SRAM PUF
- Intra-die HD of 0.0225 and an entropy of 0.99
- Decreasing the aspect ratio at constant volume and increasing the volume at constant aspect ratio is proposed to increase the tilt angle variation and enhance the stability of the PUF

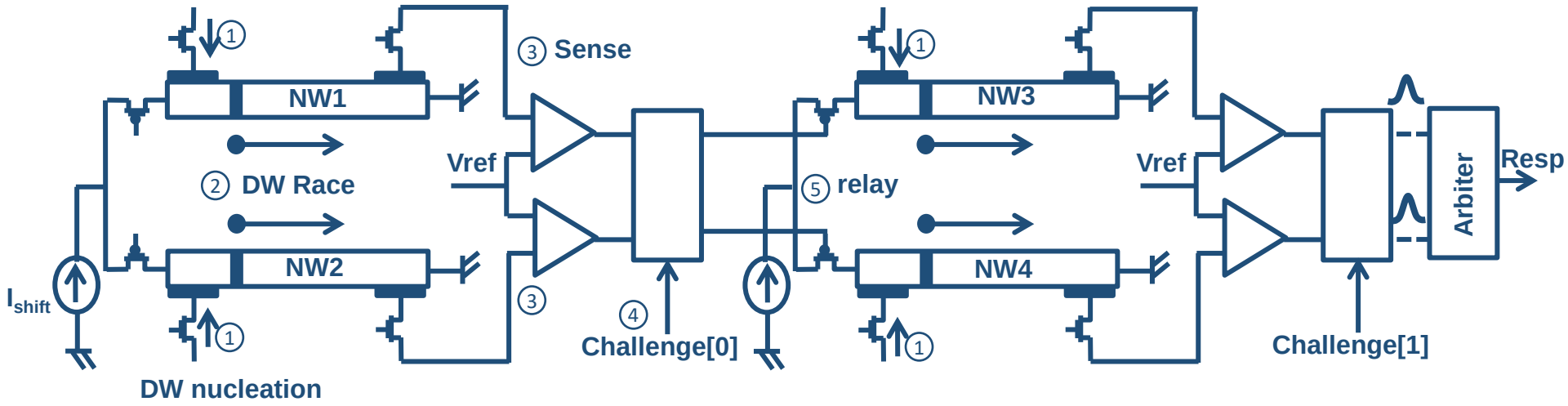




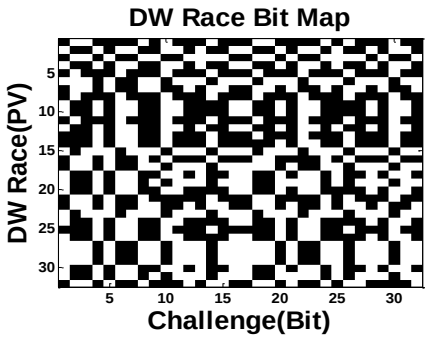
PUF Types	$\mathcal{D}_{intra}$	$\mathcal{D}_{inter}$	$\rho(Y^n) \leq$	area (μm^2)
SRAM	0.078	0.49	0.94	51.99
Latch	0.26	0.3	0.71	531.25
D flip-flop	0.19	0.39	0.81	765.63
Arbiter	0.07	0.46	0.5-0.9	690.56
Ring Oscillator	0.099	0.46	0.86	7774.2
Memristor *	-	$\simeq 0.5$	-	-
STT-PUF *	$\sim$ 10e-6	$\simeq 0.5$	0.985	6.79
MRAM	0.0225	0.47	0.99	6.74

Das, Jayita, Kevin Scott, Srinath Rajaram, Drew Burgett, and Sanjukta Bhanja. "MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS." (2015).

DWM-Relay PUF



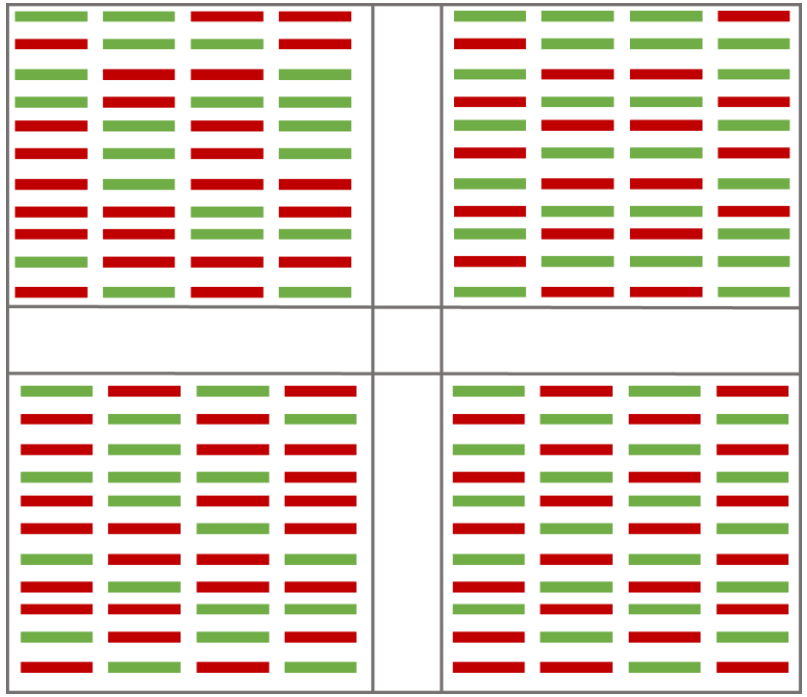
- Operation of relay-PUF
  - DW nucleation
  - Race
  - Sense
  - Relay
  - Race…
- Variation in DW velocity due to variation is exploited
- Hamming distance=50%

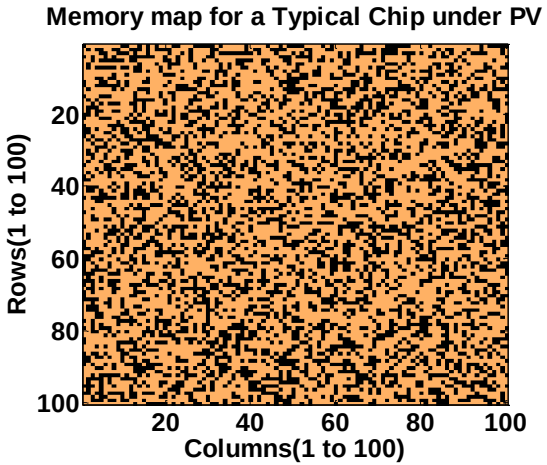


Anirudh Iyengar, Swaroop Ghosh and Kenneth Ramclam, "Domain wall magnet for embedded memory and hardware security", Special Issue of Journal of Emerging Topics on Circuits and Systems (JETCAS Special Issue), 2015

Memory PUF

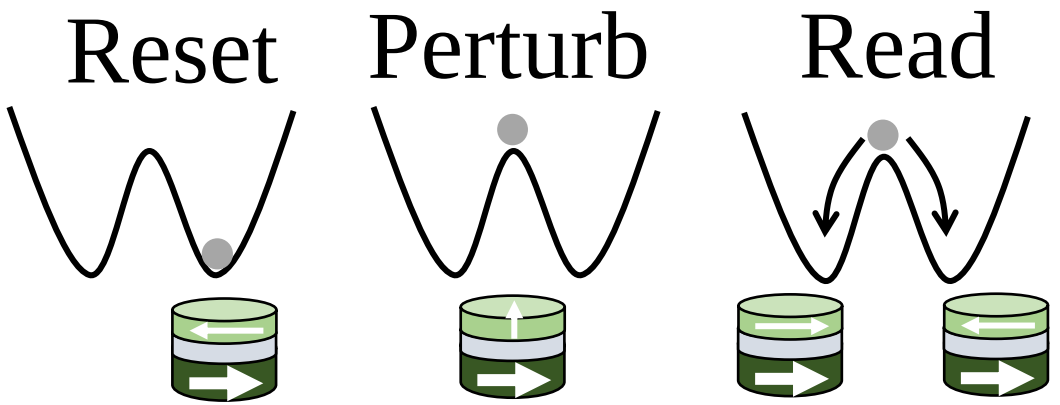
- DW is raced in memory array (pinned: ‘0’ (red), remaining: ‘1’ (green))
- Uneven number of ‘0’s and ‘1’s at high voltage
- Temperature variation changes response
- Hamming distance is ~44%





Spintronic TRNG

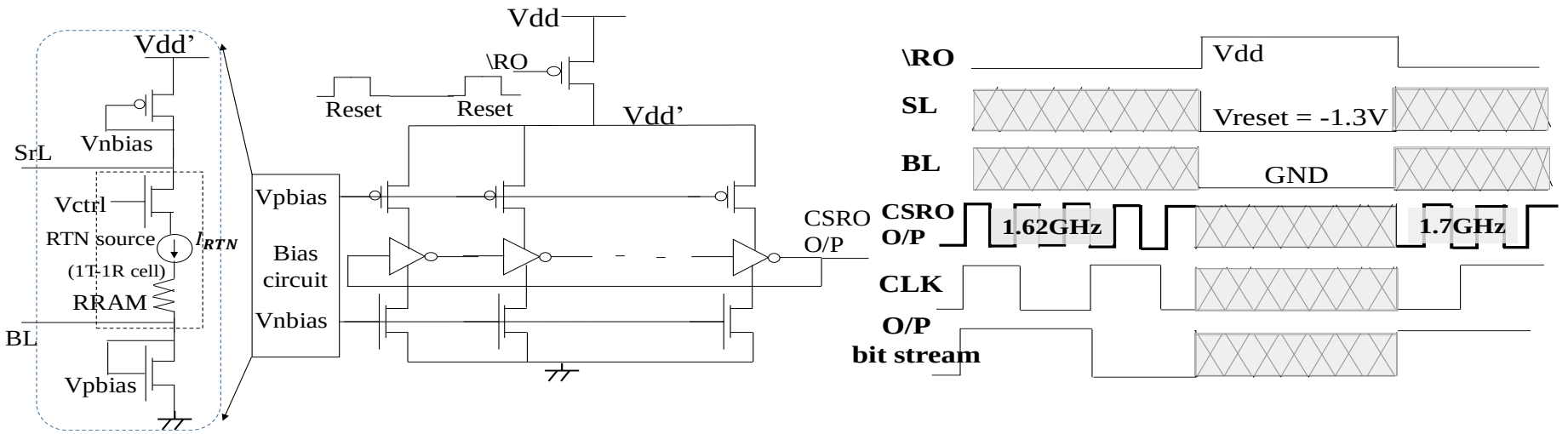
- Key ideas:
  - Reset the MTJ to AP state
  - Excite the free layer of the MTJ to the bifurcation point by applying a current pulse
  - Magnetization settle in random state due to thermal noise
  - To improve randomness and kill correlation bits are XOR'ed with each other
- Reset pulse is detrimental to MTJ reliability
- Sharing of reset and sense circuit makes sense MTJ susceptible to read disturb



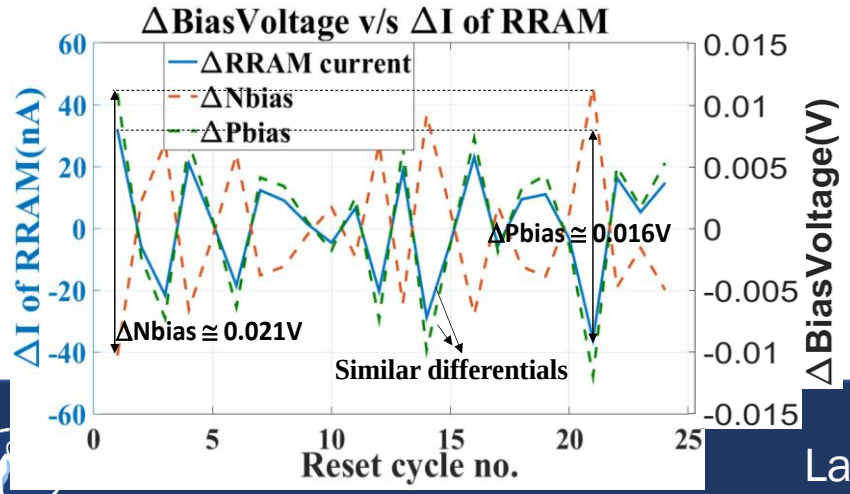
Choi, Won Ho, L. V. Yang, Jongyeon Kim, Abhishek Deshpande, Gyuseong Kang, Jian-ping Wang, and Chris H. Kim. "A Magnetic Tunnel Junction based True Random Number Generator with conditional perturb and real-time output probability tracking." In Electron Devices Meeting (IEDM), 2014 IEEE International, pp. 12-5. IEEE, 2014.

RRAM TRNG

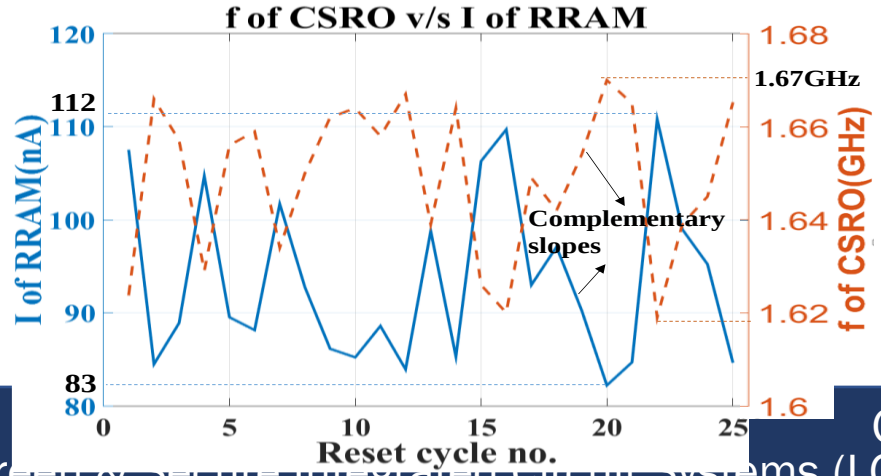
- RTN to generate random bit strings



Bias voltage differentials

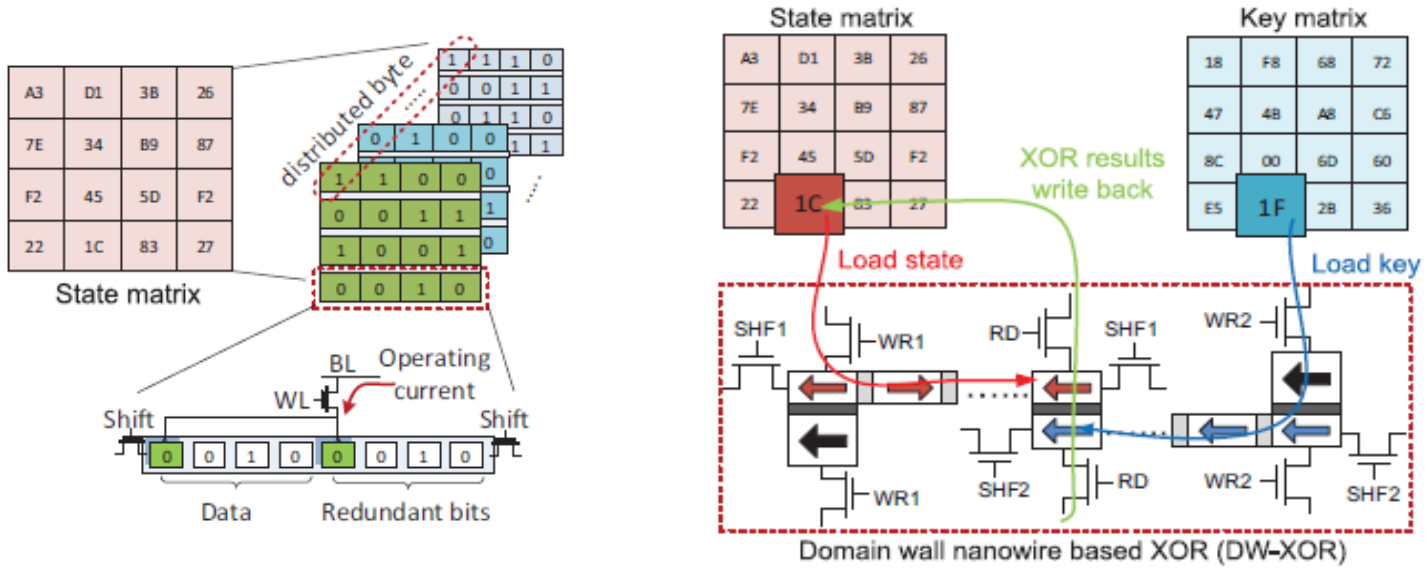


Frequency of CSRO oscillations



Spintronic Encryption Engine

- SubByte: The DW-based Look-Up Table (LUT) is used to save leakage power
- ShiftRows: To mimic cyclic rotation in nanowire, redundant bits are employed in DW nanowire
- MixColumns: multiplication by shift and addition. For addition domain wall XOR gate is employed
- AddRoundKey: This step XORs the SM with the round key



] Wang, Yuhao, Hao Yu, Dennis Sylvester, and Pingfan Kong. "Energy efficient in-memory aes encryption based on nonvolatile domain-wall nanowire." In Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014, pp. 1-4. IEEE, 2014.

Open Research Problems

- Various new flavors of devices
  - SOT-MRAM
  - PMA-MTJ
  - Skyrmionic memory
- Application areas of hardware primitives
  - Data non-repudiation
  - System security issues e.g., buffer overflow
  - Machine learning

Conclusions

- Hardware supply chain presents several new attack surfaces
- Conventional CMOS technologies offer limited randomness, variations and noise sources
- Emerging NVMs possess novel ingredients suitable for security
- We reviewed multiple techniques and their security applications
- We also covered open problems in the area

Thank you!

- Acknowledgements
  - Collaborators: Anupam Chattopadhyay, Shivam Bhasin, Jongsun Park, Rashmi Jha