CIFellows 2020-2021

Soheil Salehi, Ph.D.

Computing Innovation Fellows

Electrical and Computer Engineering Department, University of California, Davis

Towards Hardware and AI-assisted Security: A Defense-In-Depth Approach

❑ ICs are more complex compared to decades ago:

- Design and fab are not handled by same entity anymore!

❑ High Cost of ASIC Manufacturing:

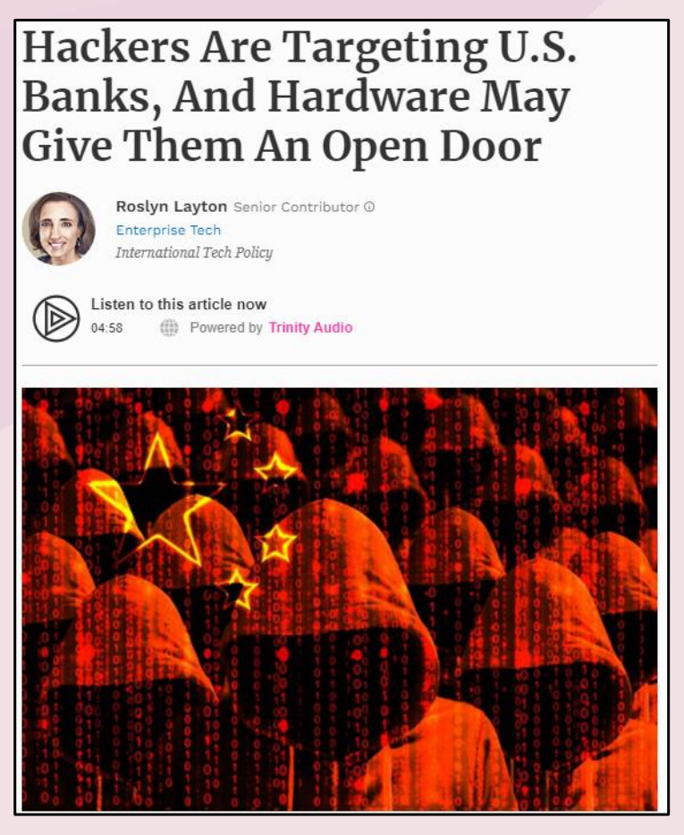
- Major U.S. Tech are Fabless: AMD, Nvidia, Qualcomm, Broadcom, etc.

❑ Hardware security is questioned:

- Emerging hardware security attacks
- Globalized fabrication and supply chain

Bloomberg Businessweek
The Big Hack
How China used a tiny chip to infiltrate America's top companies

The Bloomberg Businessweek. 2018. The Big Hack. Technical Report retrieved from: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.



Hackers Are Targeting U.S. Banks, And Hardware May Give Them An Open Door

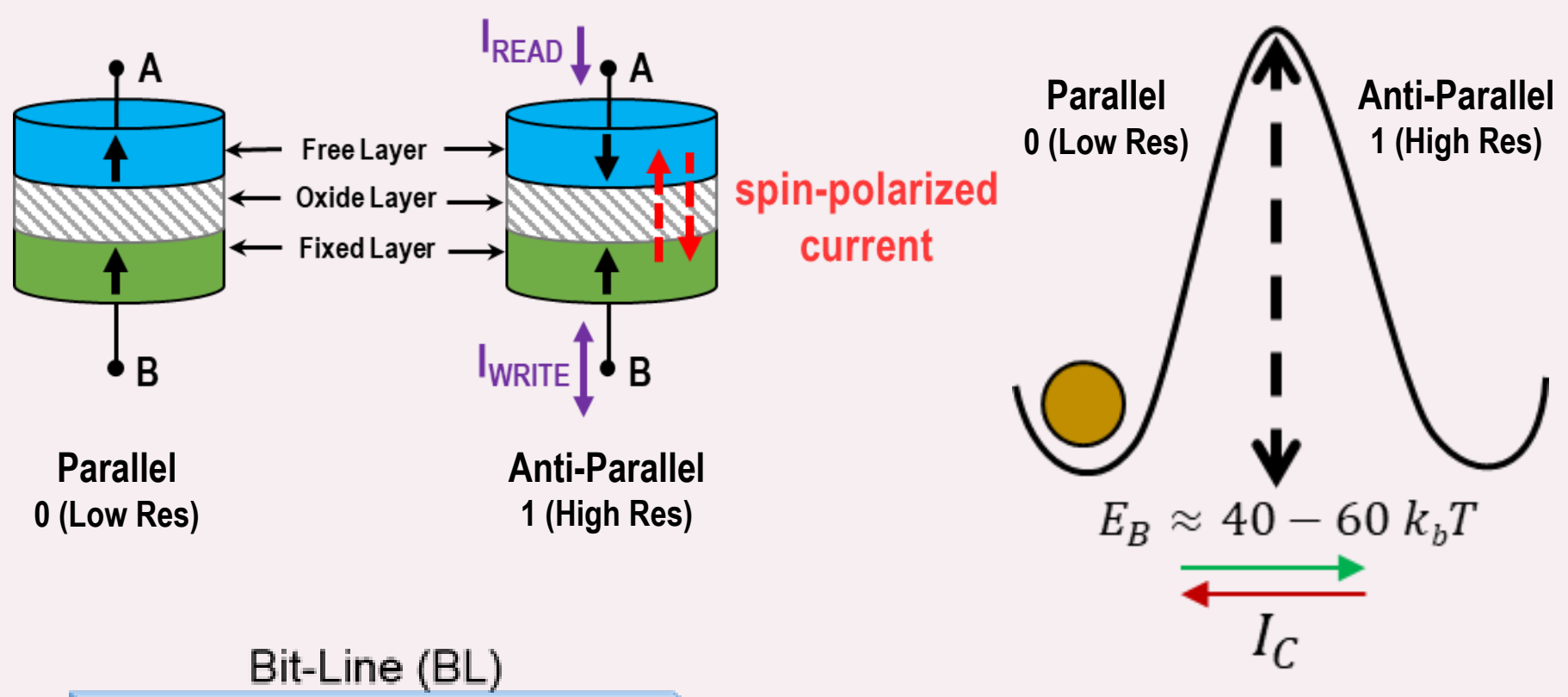
Roslyn Layton Senior Contributor
Enterprise Tech
International Tech Policy

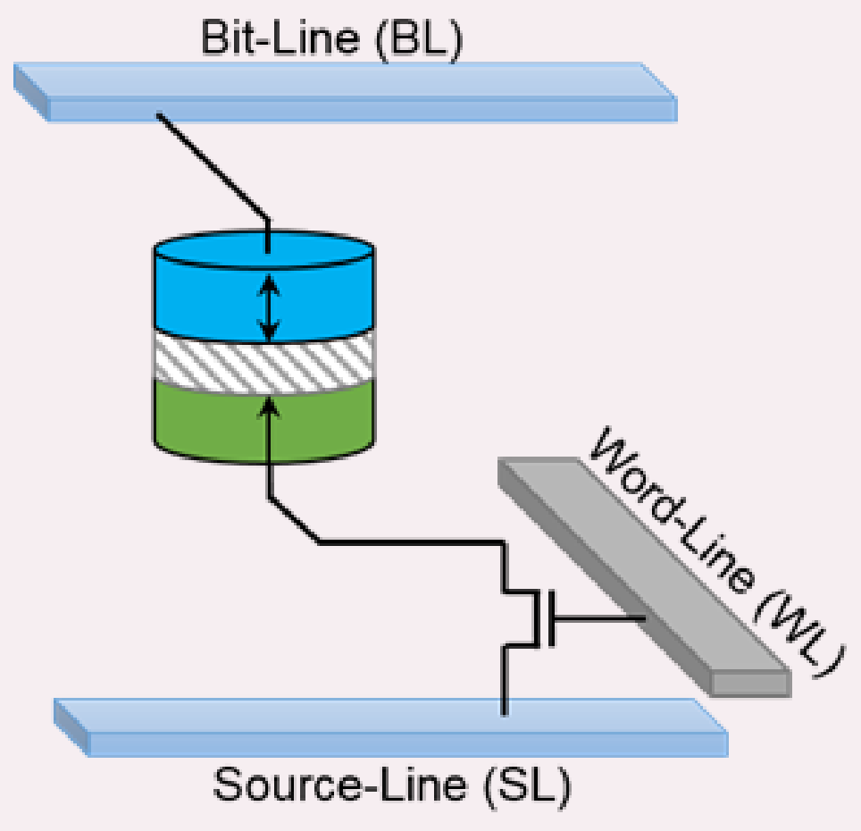
Listen to this article now
04:58 Powered by Trinity Audio

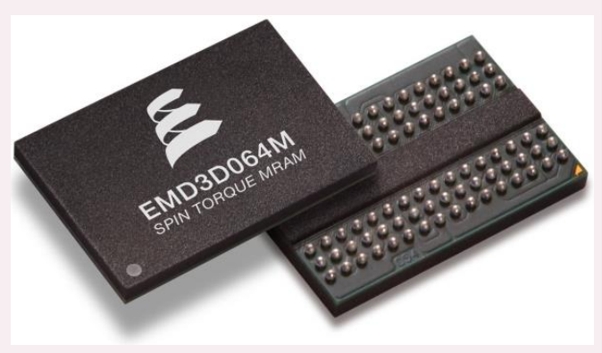
Forbes. 2021. Hackers Are Targeting U.S. Banks, And Hardware May Give Them An Open Door. https://www.forbes.com/sites/roslynlayton/2021/03/17/hackers-are-targeting-us-banks-and-hardware-may-give-them-an-open-door/?sh=6e3d8e8814dc

❑ Magnetic Tunnel Junctions (MTJs):

- A tunneling oxide layer sandwiched between two ferromagnetic layers
- Magnetization of free layer can be modified using a current or voltage





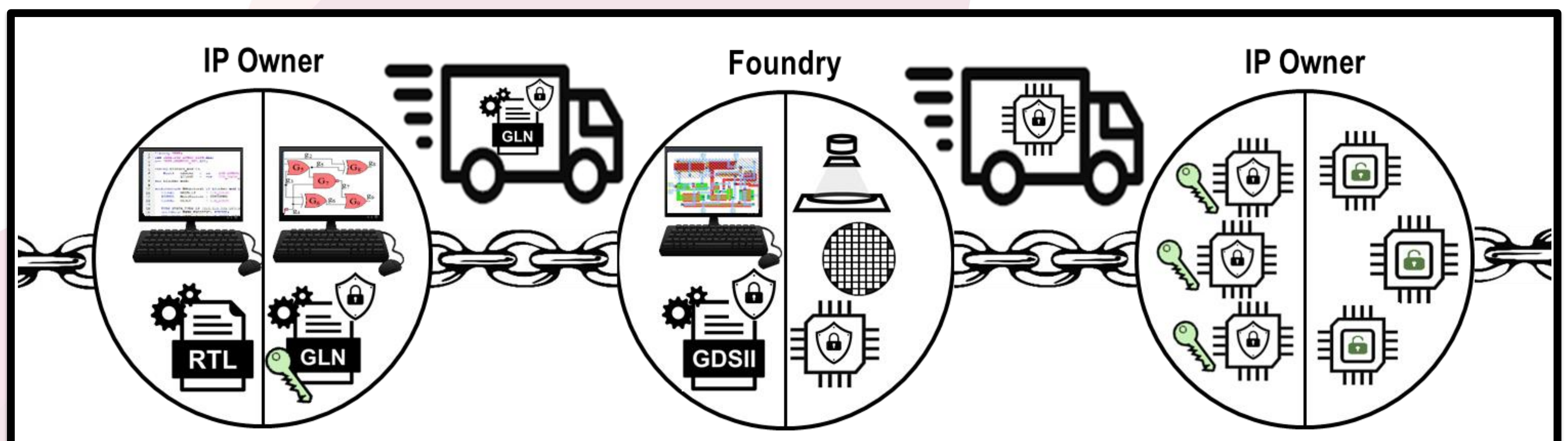


https://www.everspin.com/spin-transfer-torque-mram-products

https://www.theregister.co.uk/2019/03/08/samsung_mram/

❑ Advantages:

✓ Non-Volatile
✓ Near-zero standby power
✓ Area efficient
✓ Fast read operation



Key Contributions:

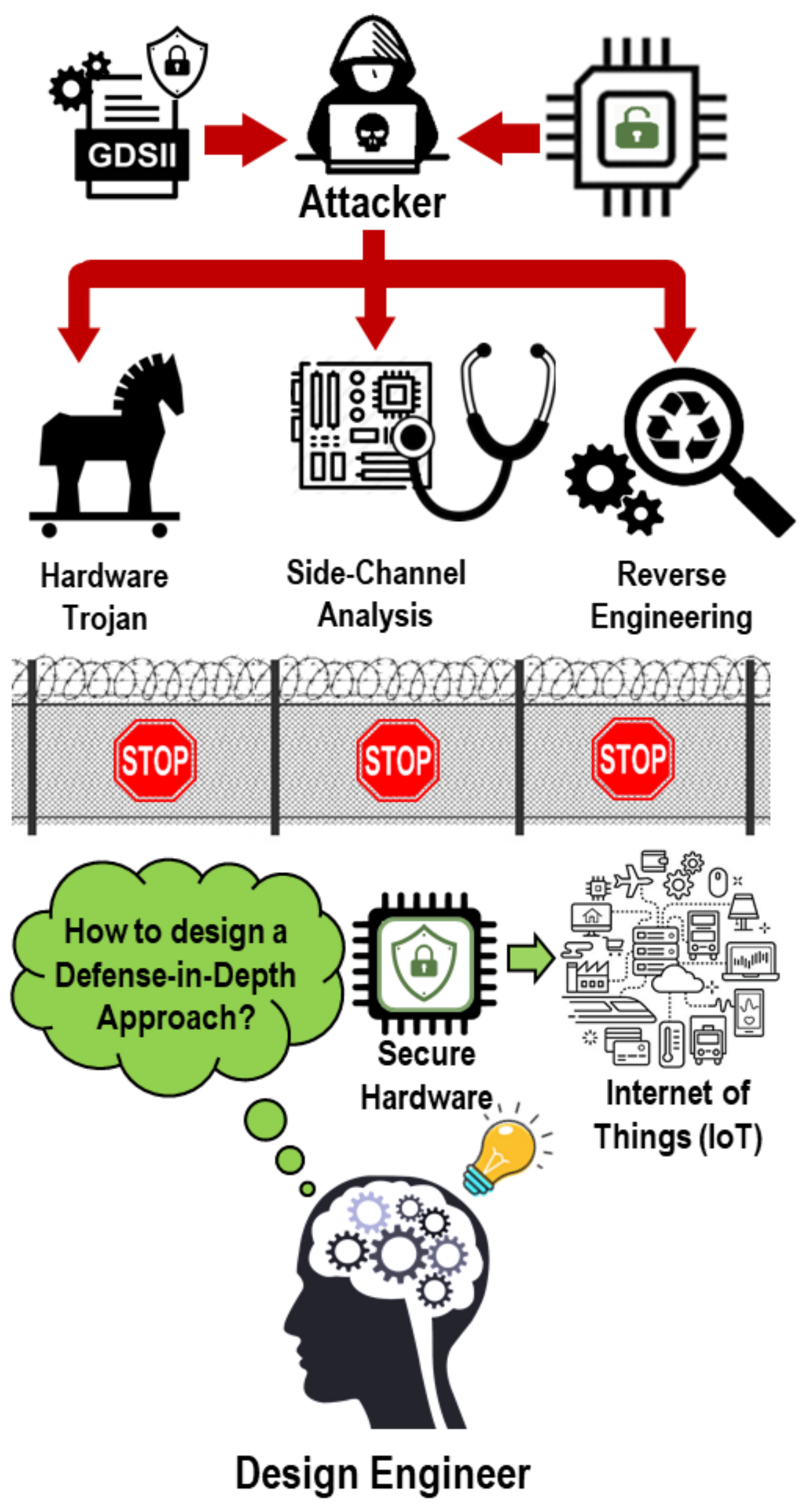
✓ **Defense-in-Depth for Hardware Security**

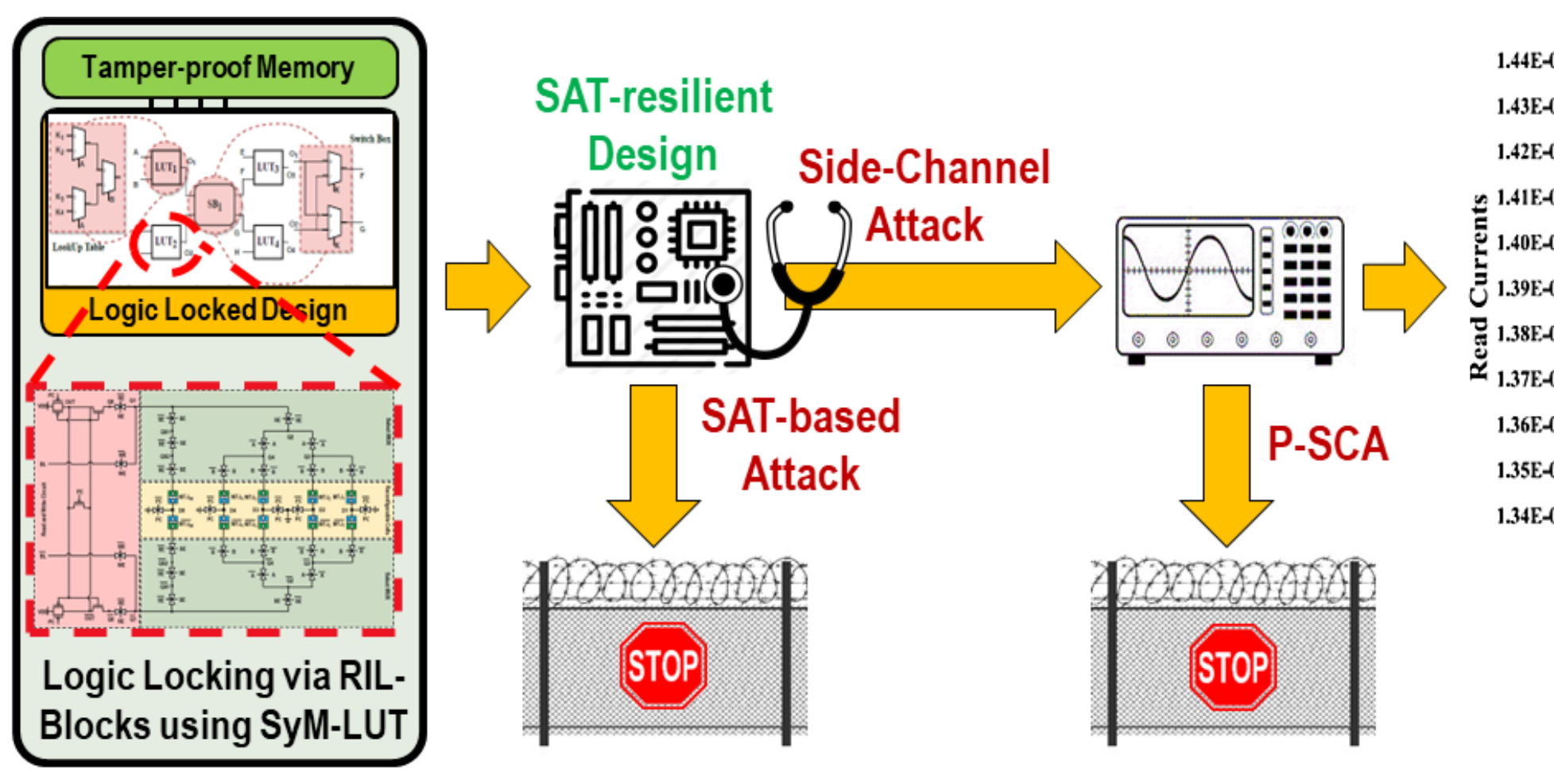
✓ **Symmetrical MRAM-LUT (SyM-LUT):**
- Utilize emerging post-CMOS devices
- Low power variation mitigates P-SCAs
- Scan Obfuscation Mechanism (SOM)
- Reliable in presence of Process Variation

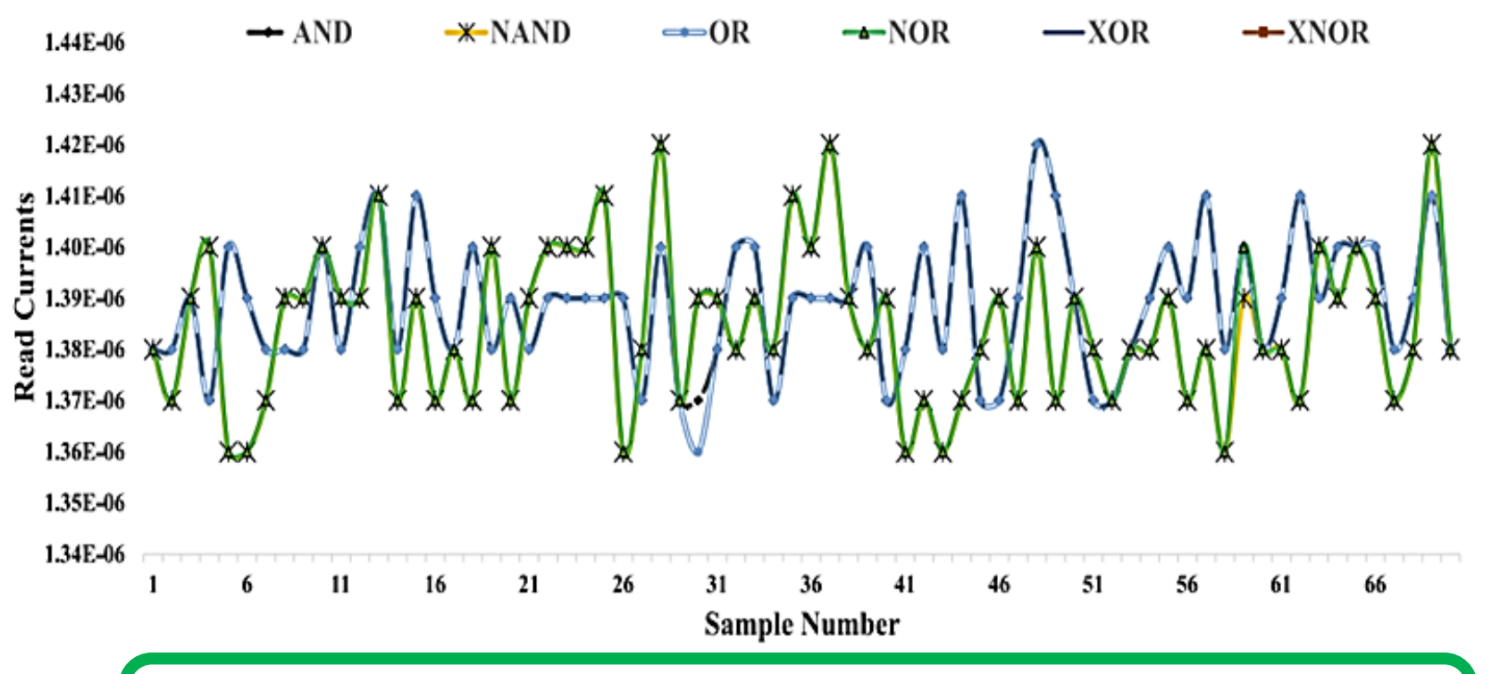
✓ **Reconfigurable Interconnect and Logic-Blocks (RIL-Blocks):**
- Combination of LUTs and logarithmic network
- High output corruptibility for SAT-resiliency
- SAT-resiliency with few 8×8×8 RIL-blocks
- Low overhead using 2-input SyM-LUTs

✓ **Thwarts bypass and removal attacks**

✓ **Dynamic morphing capability**







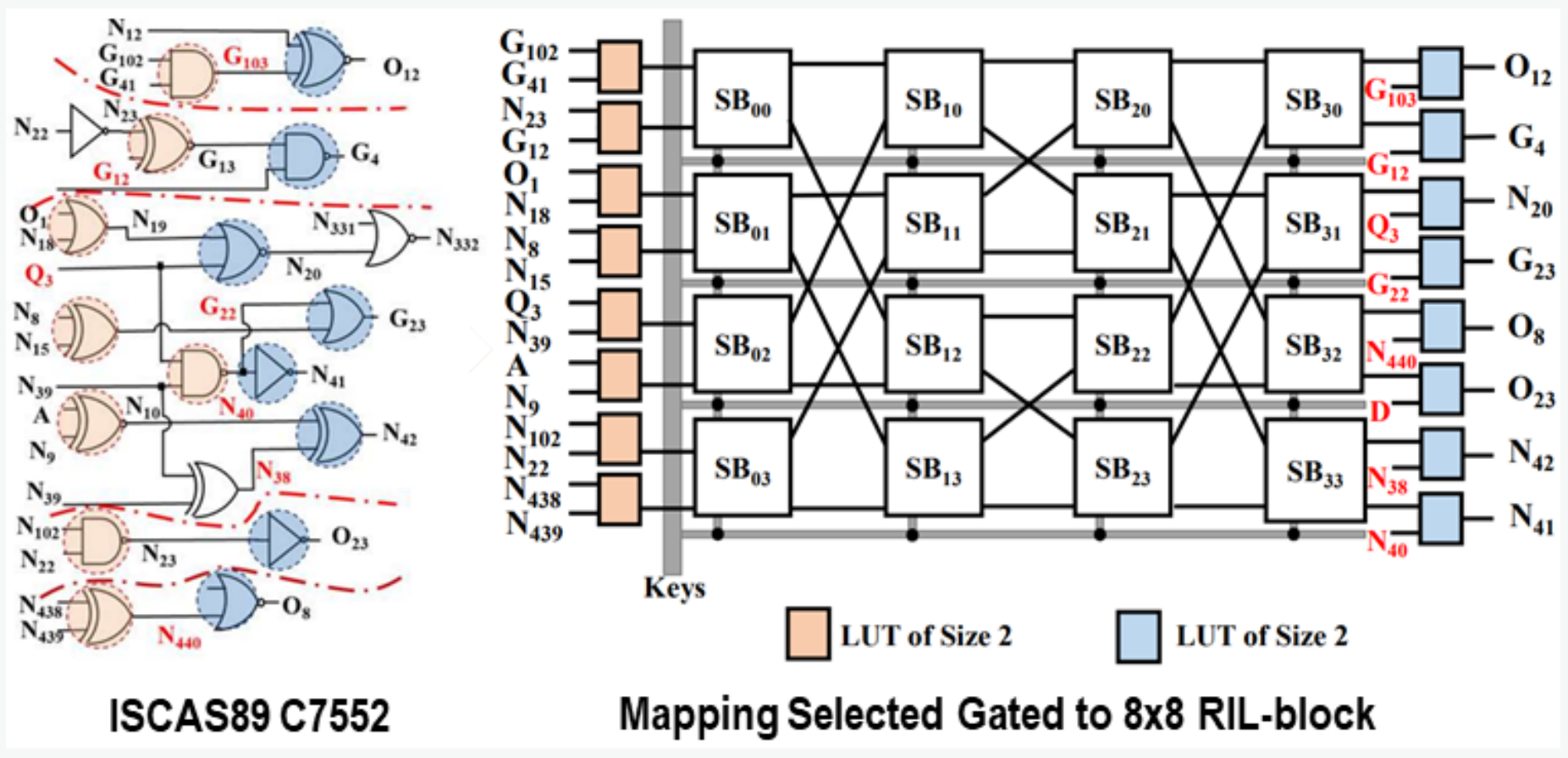
Sample read current traces for the proposed 2-input SyM-LUT configured to implement different logic functions.

Comparison of Security Coverage with state-of-the-art attacks

Attacks	SFLL [1]	GSHE/MESO [2,3]	InterLock [4]	CAS-Lock [5]	LUT [6]	Proposed
SAT-attack	✓	✗	✓	✓	✓	✓
AppSAT	✓	✓	✓	✓	✓	✓
Power side channel attack	–	–	–	–	–	✓
Removal attack	✓	–	✓	✓	✓	✓
ScanSAT	–	–	–	–	✓	✓
Shift and Scan attack	–	–	–	–	✓	✓
Features	[1]	[2,3]	[4]	[5]	[6]	Proposed
Dynamic morphing	✗	✓	✗	✗	✗	✓
Application	–	Limited	–	–	–	–

❑ RIL-Blocks:

- Combination of LUTs with almost non-blocking Banyan network with $(N/2)\,log_2\,N$ switching blocks for SAT resiliency.



❑ Design Questions:

- **Insertion Policy**: Can be inserted randomly
- **Design Complexity**: as low as 3 RIL-blocks
- **LUT Complexity**: LUT-2 for small overhead

Size and Quantity of RIL-blocks for ISCAS C7552 Benchmark for SAT-resiliency

RIL Blocks	Size of RIL Blocks			RIL Blocks	Size of RIL Blocks		
	2x2	8x8	8x8x8		2x2	8x8	8x8x8
1	0.31	0.63	23.53	10	1.16	∞	∞
2	0.35	6.33	198.556	25	34.5	∞	∞
3	0.405	20.422	∞	50	102.319	∞	∞
4	0.55	180.938	∞	75	∞	∞	∞
5	0.67	316.231	∞	100	∞	∞	∞

❑ SAT-Attack:

- State-of-the-art SAT-Attacks with CaDiCaL[1]
- **Benchmarks:** ISCAS-89[2] and DoD's Common Evaluation Platform (CEP)[3]

Comparison of ML-assisted P-SCAs on SyM-LUT with SOM

Benchmark Suite	Benchmark Circuit	Number of RIL-Block			AppSAT Success
		1	2	3	
ISCAS-89	b15	124.25	546.2	∞	✗
	s35932	105.1	1864.2	∞	✗
	s38584	345.2	∞	∞	✗
	b20	240.4	2454.26	∞	✗
CEP	AES	1060.56	∞	∞	✗
	SHA-256	846.87	∞	∞	✗
	MD5	1450.1	∞	∞	✗
	GPS	∞	∞	∞	✗

❑ Machine Learning-Assisted P-SCA:

- **Dataset:** 640,000 power traces for 16 labels
  - 16(Gates)x4(Keys/Gate)x10,000 instances
- **Evaluation metric:** Accuracy and F1-score
- **Feature scaling and outlier filtering:** z-scores for data pre-processing

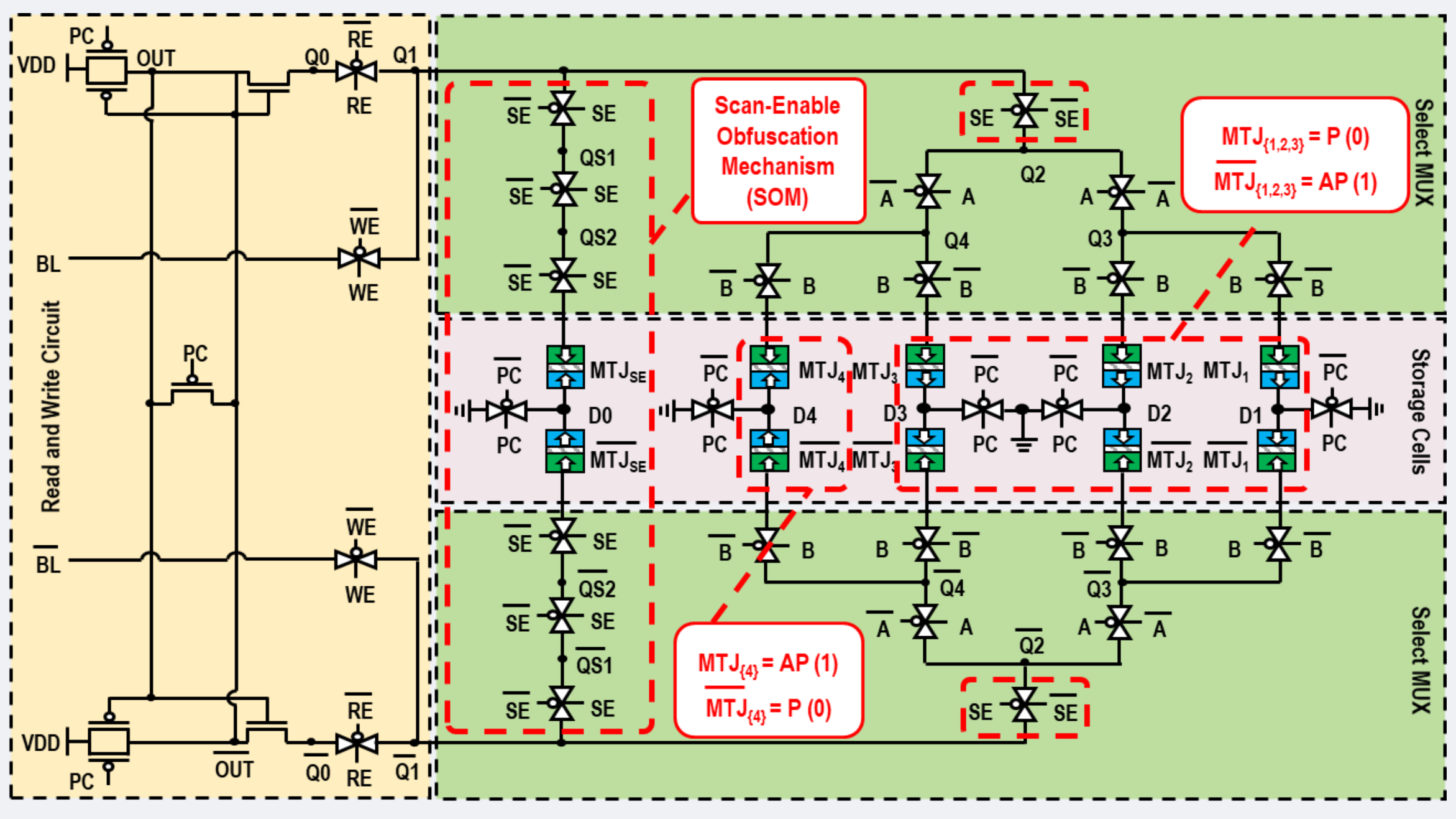
Comparison of ML-assisted P-SCAs on SyM-LUT with SOM

Algorithm	Accuracy	F1-Score
Random Forest	31.6%	0.322
Logistic Regression	30.93%	0.310
SVM	26.36%	0.284
DNN	35.01%	0.357

1. Armin Biere. SAT Competition-2018.
2. Available at: https://pld.ttu.ee/~maksim/benchmarks/
3. CEP is a system on a chip design that is representative of typical microelectronics used by the body of the Department of Defense (DoD) and includes instrumentation and government-specific benchmarks.

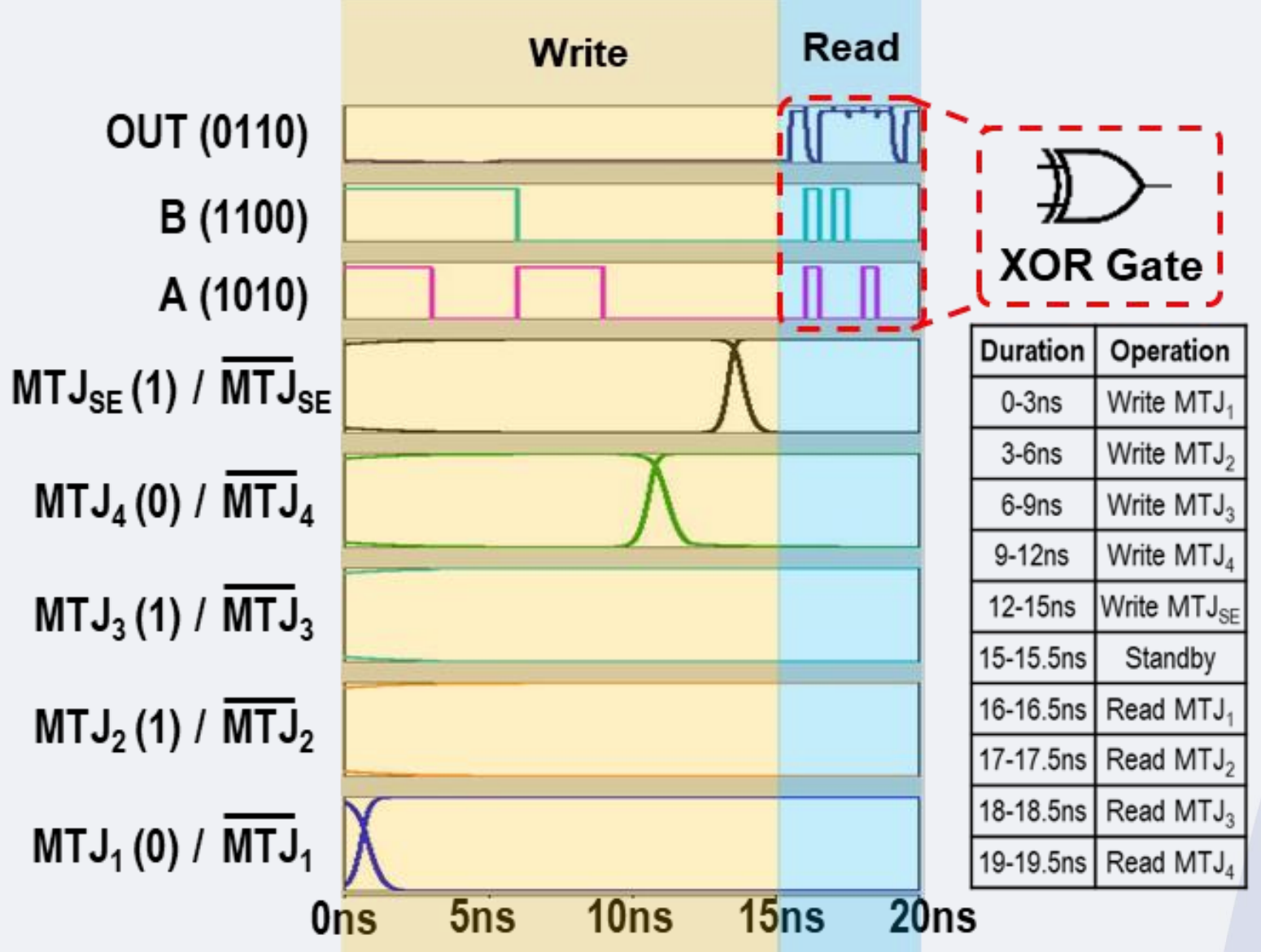
❑ Symmetrical MRAM-LUTs (SyM-LUT):

- P-SCA resiliency using emerging spin-based devices
- Scan Obfuscation Mechanism (SOM)



❑ HSPICE Simulation:

- 45nm PTM CMOS Technology[1]
- STT-MRAM Verilog A Model[2]
- 10,000 MC for PV analysis[3]



Duration	Operation
0-3ns	Write MTJ_1
3-6ns	Write MTJ_2
6-9ns	Write MTJ_3
9-12ns	Write MTJ_4
12-15ns	Write MTJ_{SE}
15-15.5ns	Standby
16-16.5ns	Read MTJ_1
17-17.5ns	Read MTJ_2
18-18.5ns	Read MTJ_3
19-19.5ns	Read MTJ_4

❑ Energy of 2-input SyM-LUT:

- **Standby Energy:** 20aJ
- **Write Energy:** 33fJ
- **Read Energy:** 4.6fJ

❑ Reliability of 2-input SyM-LUT:

- 640,000 error-free read/write
- P (M=32.7KΩ) << AP (M=57.7KΩ)

❑ Area vs. 2-input SRAM-LUT:

- **Select MUX:** +12 transistors
- **Storage Cell:** -20 transistors
- **SOM:** +18 transistors

1. 45nm Predictive Technology Model (PTM), Available at: http://ptm.asu.edu/.
2. J. Kim, et al., "A technology-agnostic MTJ SPICE model with user-defined dimensions for STT-MRAM scalability studies," IEEE Custom Integrated Circuits Conference (CICC), 2015, pp. 1-4.
3. S. Salehi, et al., "Clockless Spin-based Look-Up Tables with Wide Read Margin," Great Lakes Symposium on VLSI (GLSVLSI), 2019, pp. 363-366.

References:

[1] M. Yasin, et al., "SFLL-HLS: Stripped-functionality logic locking meets high-level synthesis," in 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2019, pp. 1–4.

[2] B. Shakya, et al., "CAS-Lock: A security-corruptibility trade-off resilient logic locking scheme," ACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 175-202, 2020.

[3] N. Rangarajan, et al., "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," IEEE Transactions on Emerging Topics in Computing (TETC), p. 1–1, 2020.

[4] H. M. Kamali, et al., "Interlock: An intercorrelated logic and routing locking," in IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2020.

[5] G. Kolhe, et al., "Security and complexity analysis of LUT-based obfuscation: From blueprint to reality," in IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2019, pp. 1–8.

[6] S. P.et al., "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in 2018 Design, Automation Test in Europe Conference Exhibition (DATE), 2018, pp. 97–102.

CRA
Computing Research Association

CCC
Computing Community Consortium
Catalyst

NSF

Acknowledgement:
This material is based upon work supported by the National Science Foundation (NSF) under grant Computing Research Association for CIFellows Project 2030859. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.