A Perspective on Security and Trust Requirements for the Future

Dr. Kenneth Plaks

International Symposium on Physical Design

April 14-17, 2019

Hardware Security in the Field

US Air Force

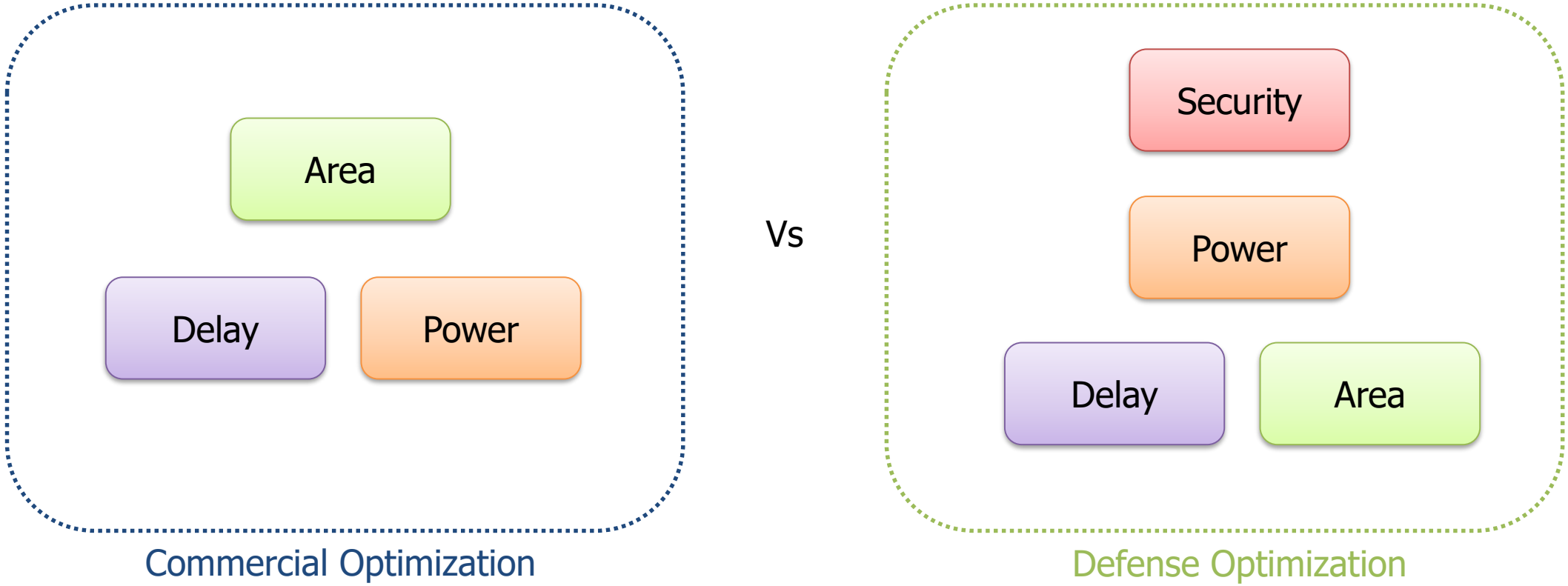
The importance of electronics

US Air Force

Commercial and Military have similar needs…

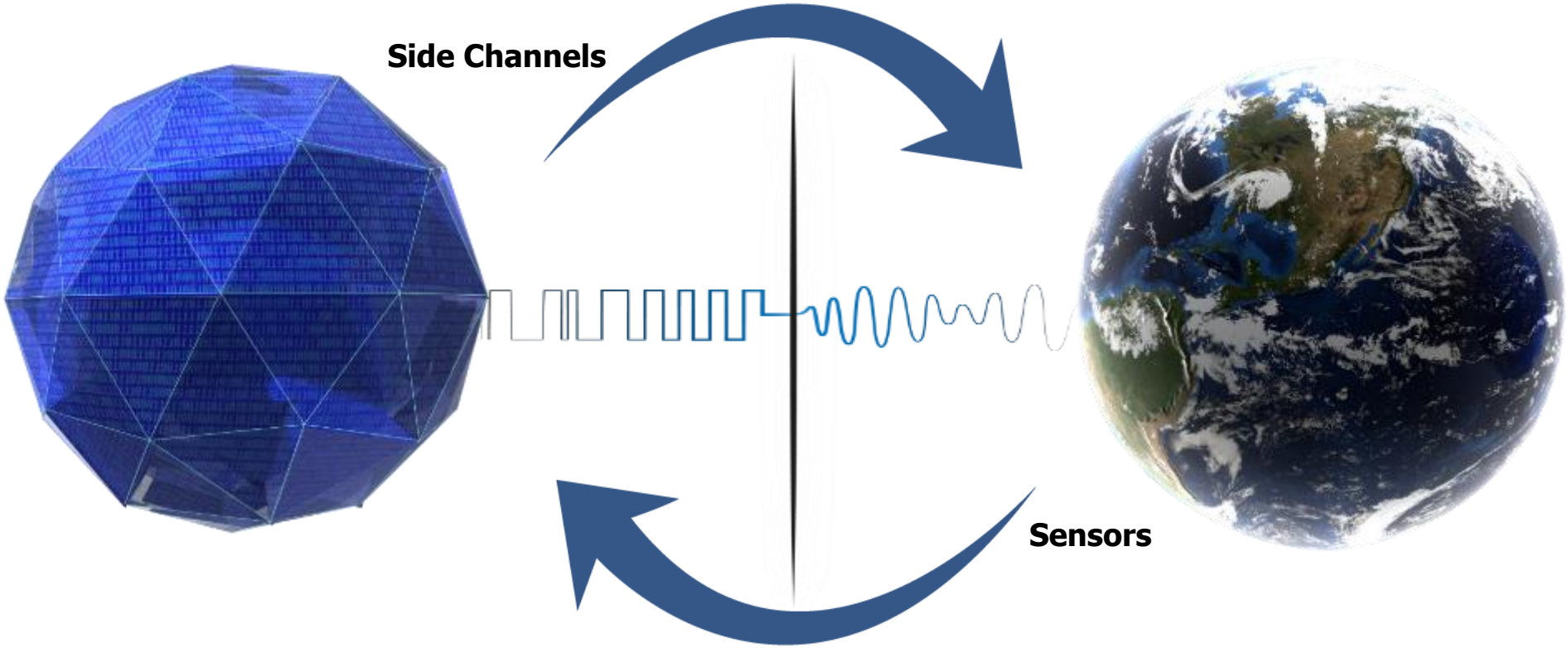
Commercial	Military
• IP protection and overproduction	• Export leakage – ITAR concerns
• License Enforcement	• Anti Tamper
• Brand identity and dependability	• Trust – reliability and no malicious insertions

But we place a much higher priority on security



What would physical design look like if we optimized for security, instead of area?

(U) Physical design and security



Digital World | **Physical Design** | **Real World**

Sensors

- For this talk, sensors are things that provide data from the real world to the digital world
  - Military uses sensors to determine where a chip has been
  - Military uses sensors as a root of trust
- We will use the DARPA SHIELD project as an example

Image courtesy of Northrop Grumman

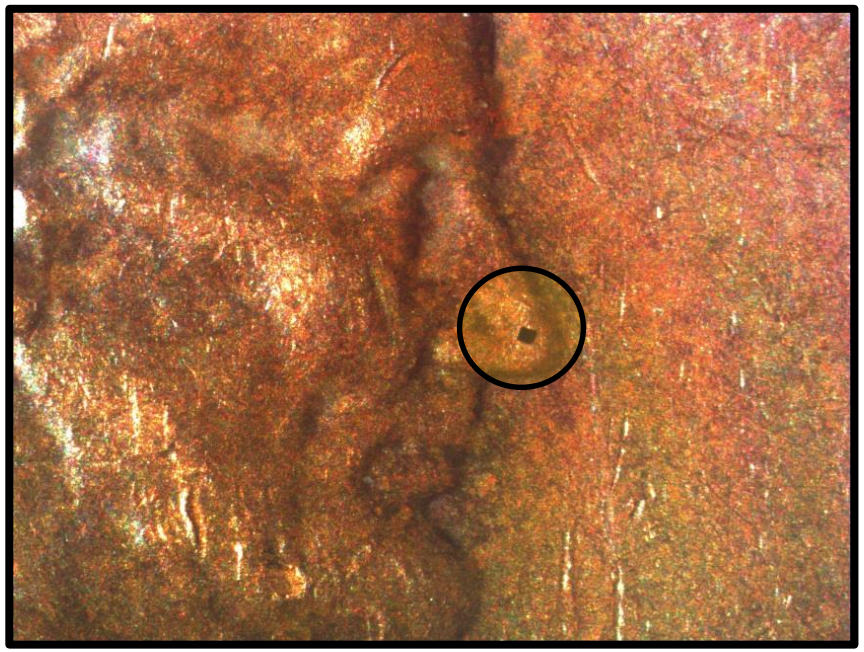
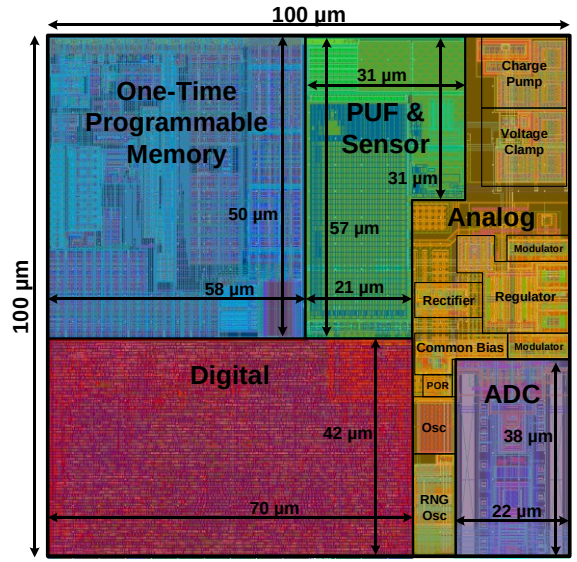


Image courtesy of SRI International

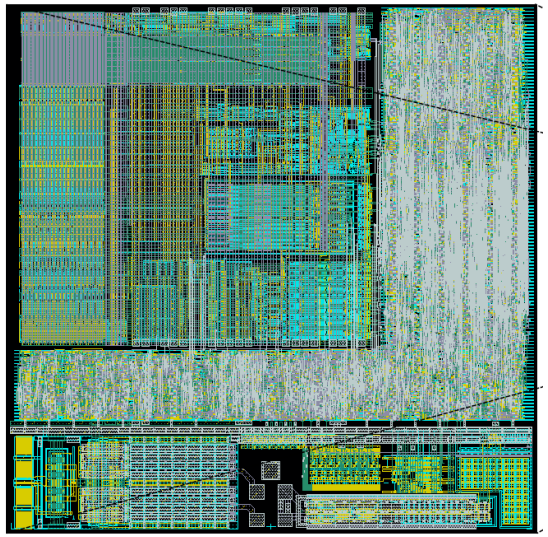
Sensor Example: DARPA SHIELD



Dielet floorplan (Northrop Grumman)
14nm CMOS

Key SHIELD Specifications

- Unique Key Storage
- Full 256-bit AES encryption engine
- Unpowered, passive intrusion sensors
- RF power and communication
- Transfer fragility
- 100µm x 100µm
- 50 µW Total Power
- Operating temp < 120°C
- Cost < $0.01 per dielet



Prototype dielet layout (SRI)
28nm CMOS

Asymmetric Security

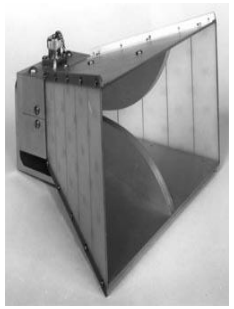
- Non-resettable, "always on" intrusion sensors on dielet
- On-board encryption symmetric key that cannot be "coaxed" from dielet
- ID and Key are unique to the individual host IC (not just the part number)
- Interrogation history (date, time, location) stored on secure server
- Built-in fragility structures kill dielet if removal from host is attempted

SHIELD makes counterfeiting too expensive and too hard to do.

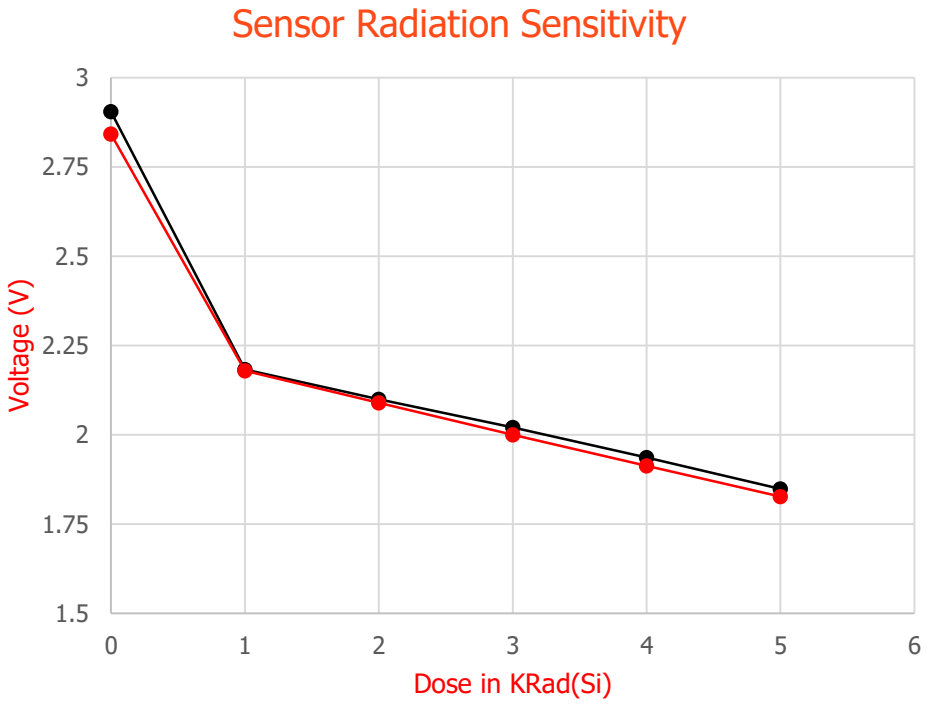
Images courtesy of Northrop Grumman and SRI International

SHIELD – Xray and RF Sensor Testing

Mini-x-ray test fixture in Draper's Radiation Effects Lab



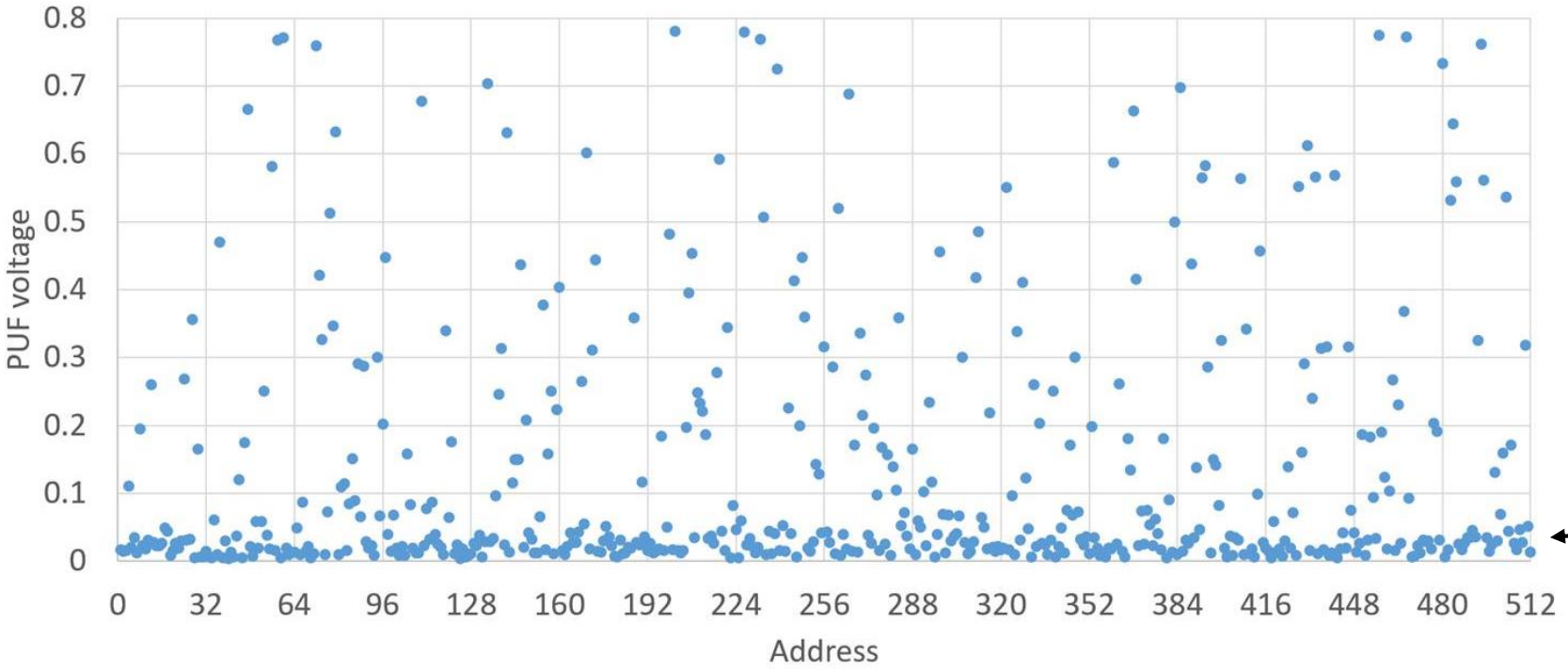
Stock photos of anechoic chamber, antenna & probe. RF testing was carried out in a secure lab at Draper

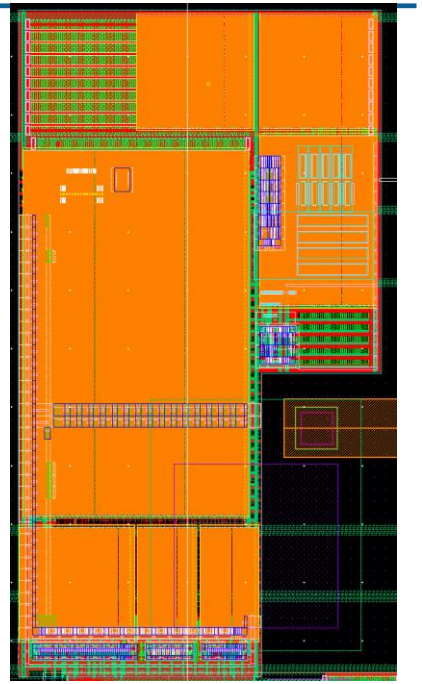


Physical Vulnerabilities of PUFs

The 1st silicon iteration of a DoD PUF failed due to its output voltages being severely skewed in the negative direction (toward 0V)

The root cause of the voltage skew was the layout proximity effect which is a dominant effect in nanoscale devices





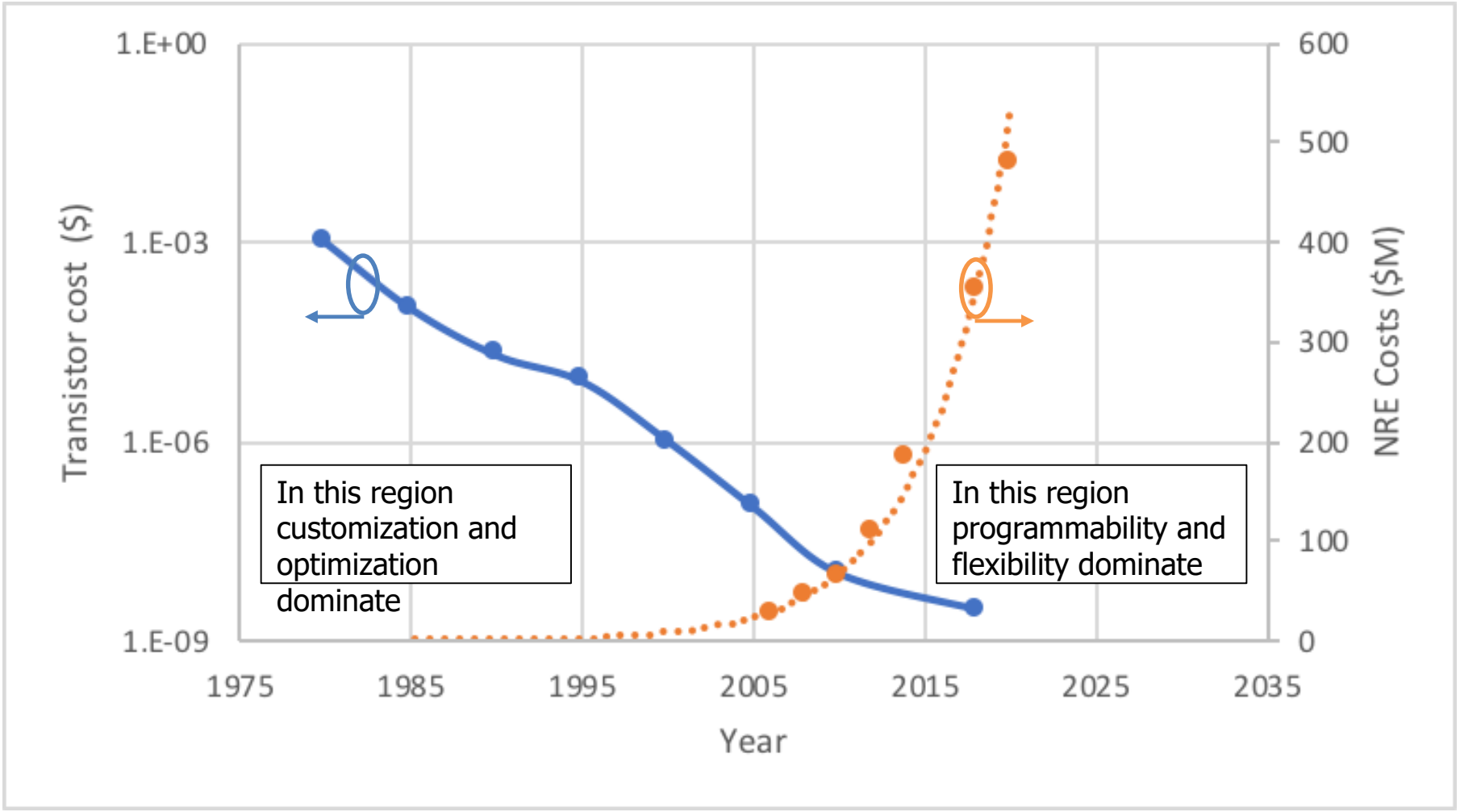
SHIELD, DARPA

The PUF voltages should have been uniformly distributed; however, testing revealed that most of the voltages were skewed negatively toward 0V.

Side channels

- For this talk, side channels are ways of getting data from the digital world to the real world
  - Not talking about SPECTER and MELTDOWN
  - Military uses side channels to find malicious circuits
- How can we interrogate a circuit for malice, when we don’t trust the circuit in the first place?
- What aspects of physical design could enhance security?

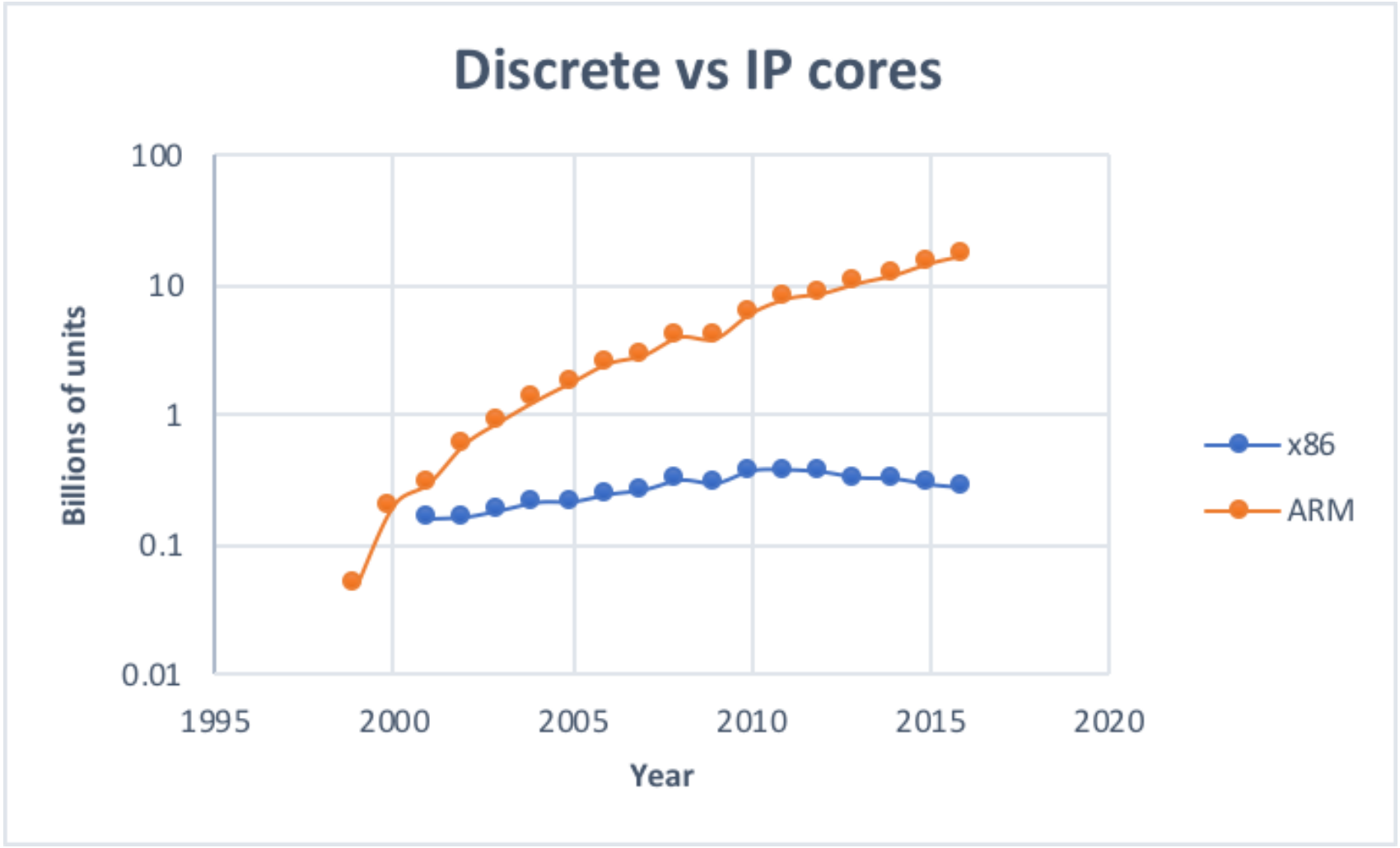
The trojan challenge in three charts



Sources: IBS; A. Olofsson, "Silicon Compilers - Version 2.0", keynote, Proc. ISPD, 2018

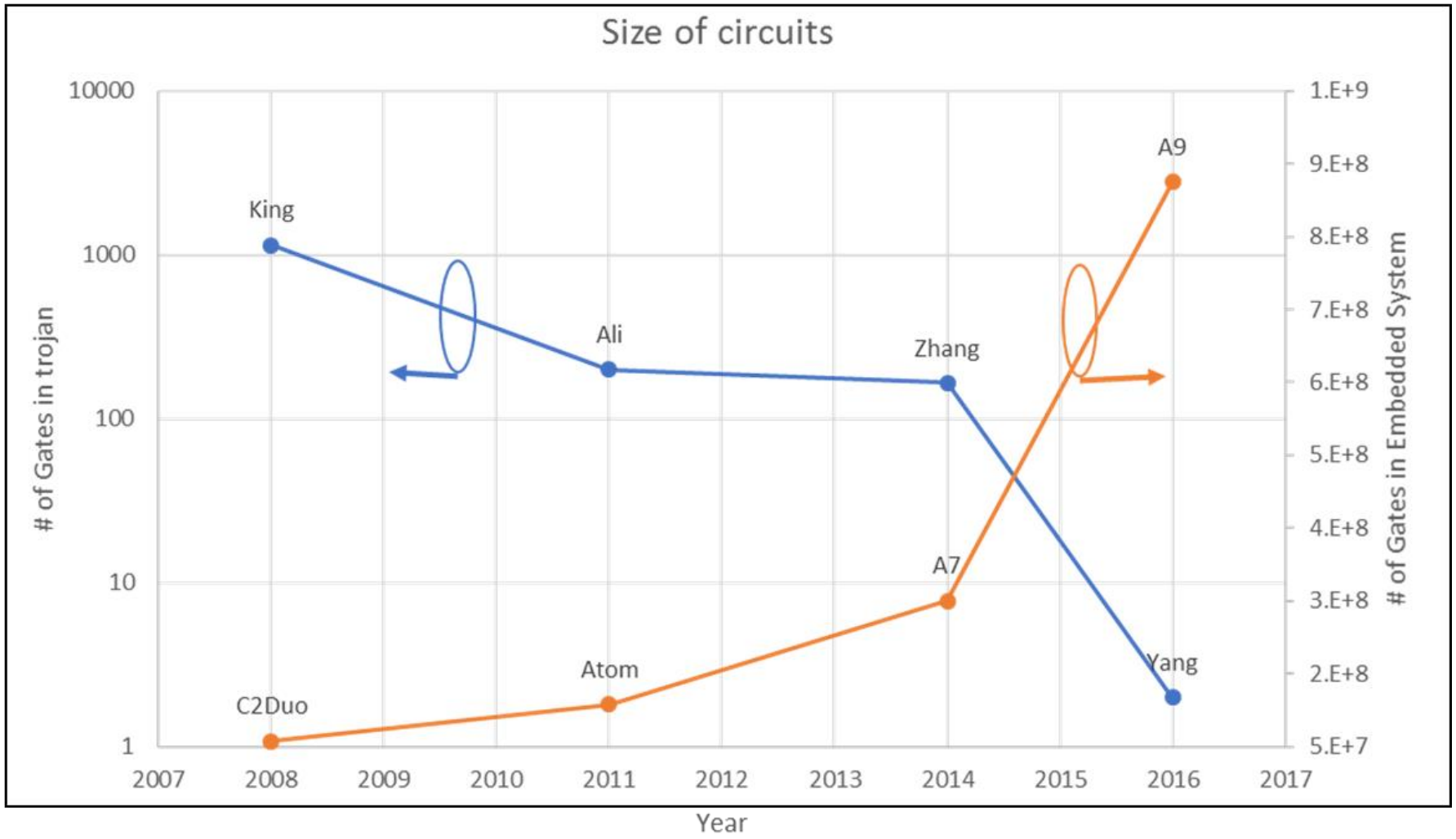
Moore's law makes SOC's possible

Technical Observation



But we have lost herd immunity

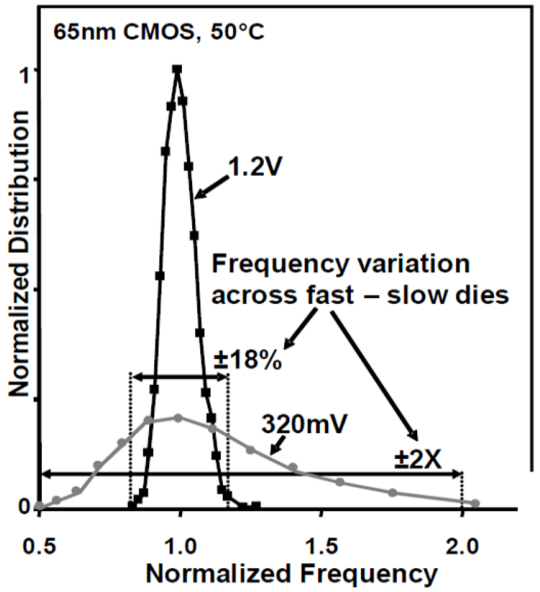
Hardware Trojans



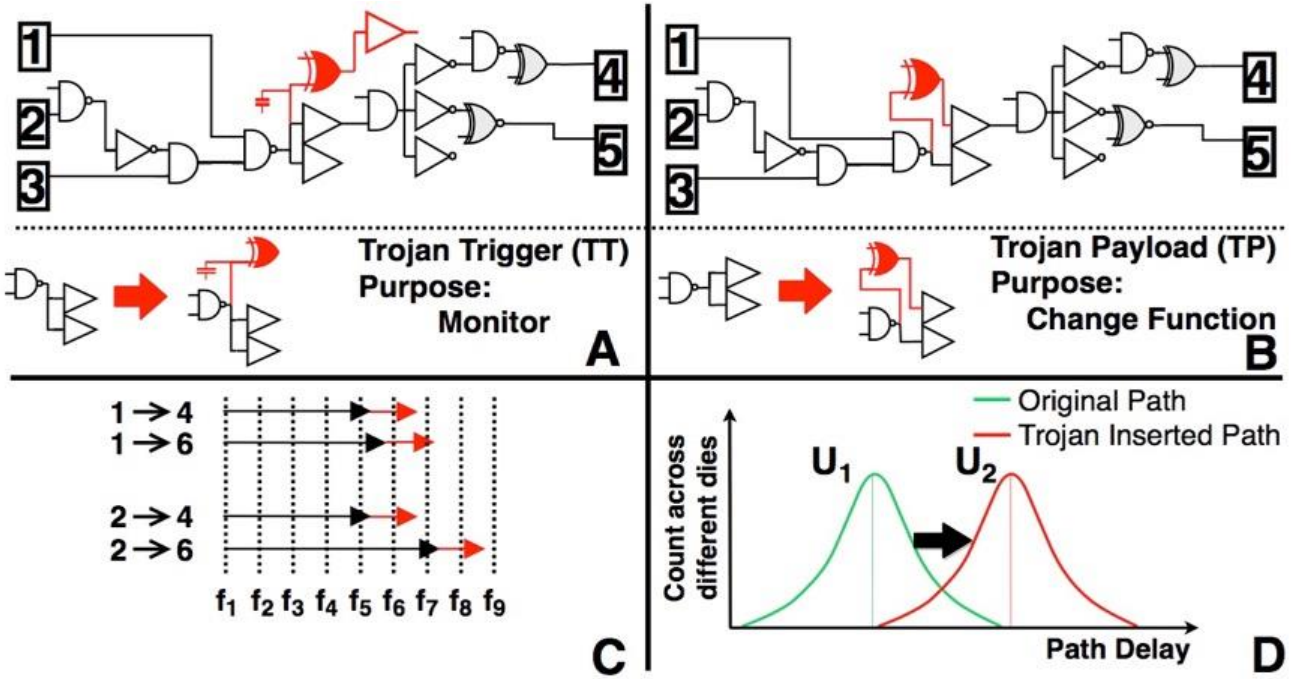
Moore's law also makes defense even harder

One possible approach: physical timing side channels

- Trojan impact on timing should be observable even without activating the trojan
  - But voltage variation makes that hard to measure

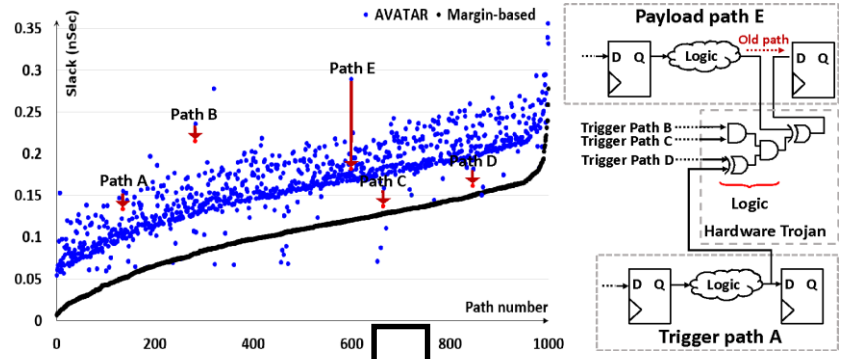


H. Kaul, M. Anders, S. Hsu, A. Agarwal, R. Krishnamurthy and S. Borkar, "Near-threshold voltage (NTV) design — Opportunities and challenges," DAC Design Automation Conference 2012 , San Francisco, CA, 2012, pp. 1149-1154.



Solution to Complications:

- **Voltage Noise**



IR Annotated Timing Analysis

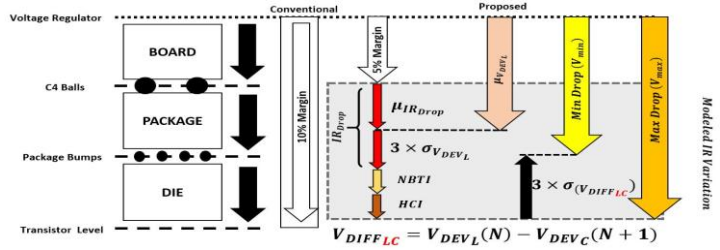
Model	Stage 1	Stage 2	• • •	Stage n
DEV delay model	(V_{DEV}, d_1)	(V_{DEV}, d_2)	• • •	(V_{DEV}, d_n)
Physical delay model	(V_1, D_1)	(V_2, D_2)	• • •	(V_n, D_n)

① $\sum_{i=1}^{N} D_i = \sum_{i=1}^{N} d_i$ ② $D_i \approx \frac{k_i V_i}{(V_i - V_{th(i)})^{\alpha}}$

③ $dD_i = -\frac{k_i - \frac{\alpha k_i V_i}{V_i - V_{th(i)}}}{(V_i - V_{th(i)})^{\alpha}} dV_i$ ④ $dV_i = V_{DEV} - V_i$

⑤ $\Delta d_{path} = \sum_{i=1}^{N} dD_i = \sum_{i=1}^{N} -\frac{(k_i - \frac{\alpha k_i V_i}{V_i - V_{th(i)}}) \times (V_{DEV} - V_i)}{(V_i - V_{th(i)})^{\alpha}} = 0$

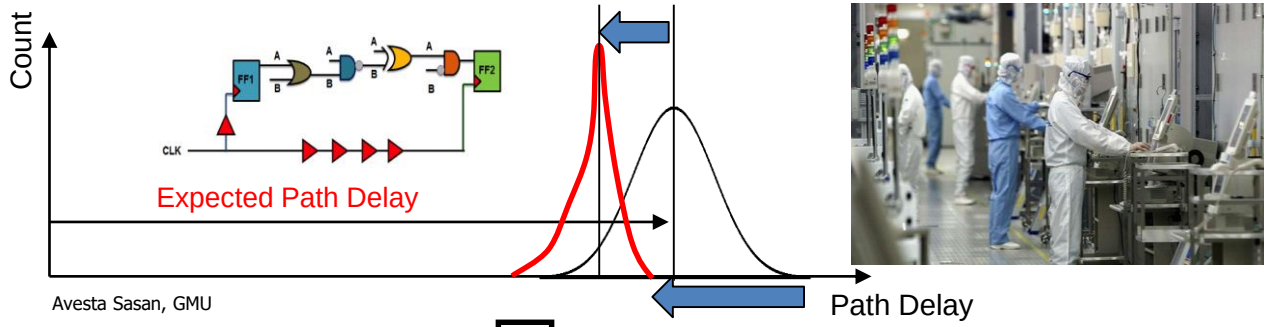
⑥ $\Omega_i = \frac{V_i}{V_{th(i)}}$ ⑦ $V_{DEV} = \frac{\sum_{i=1}^{N} \frac{D_i[\Omega_i(1-\alpha)-1]}{\Omega_i - 1}}{\sum_{i=1}^{N} \frac{D_i[\Omega_i(1-\alpha)-1]}{V_i(\Omega_i - 1)}}$



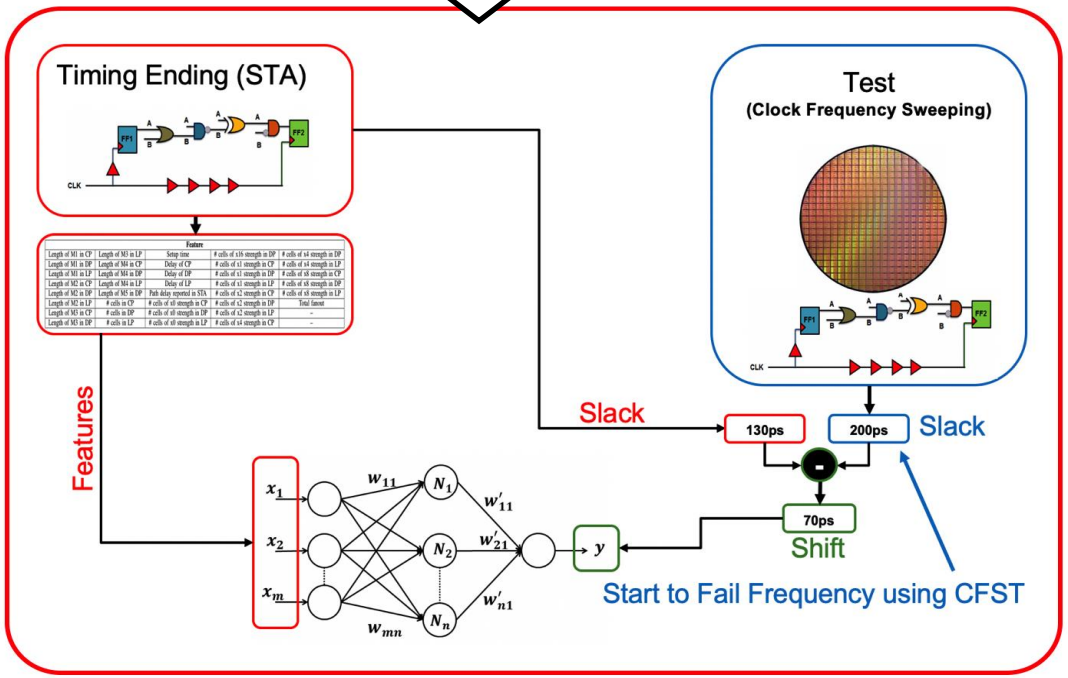
A. Vakil, H. Homayoun, and A. Sasan, Proceedings of the 24th Asia and South Pacific Design Automation Conference. ACM, 2019, pp. 152–159.

https://dl.acm.org/citation.cfm?id=3287683

- **Process Drift**

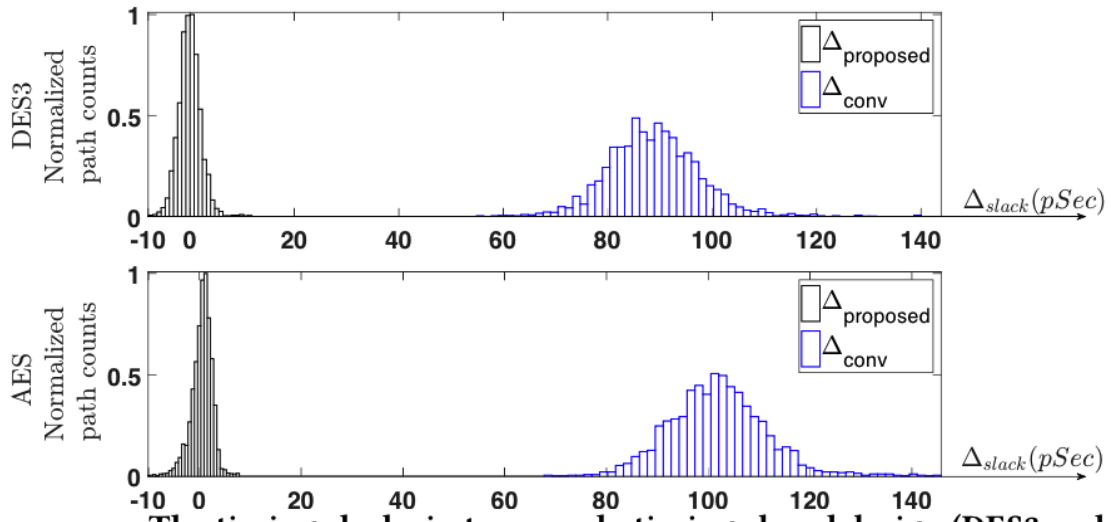


NN Process Watchdog



AVATAR (IR-ATA): Annotating the Timing Impact of Voltage drop and Noise

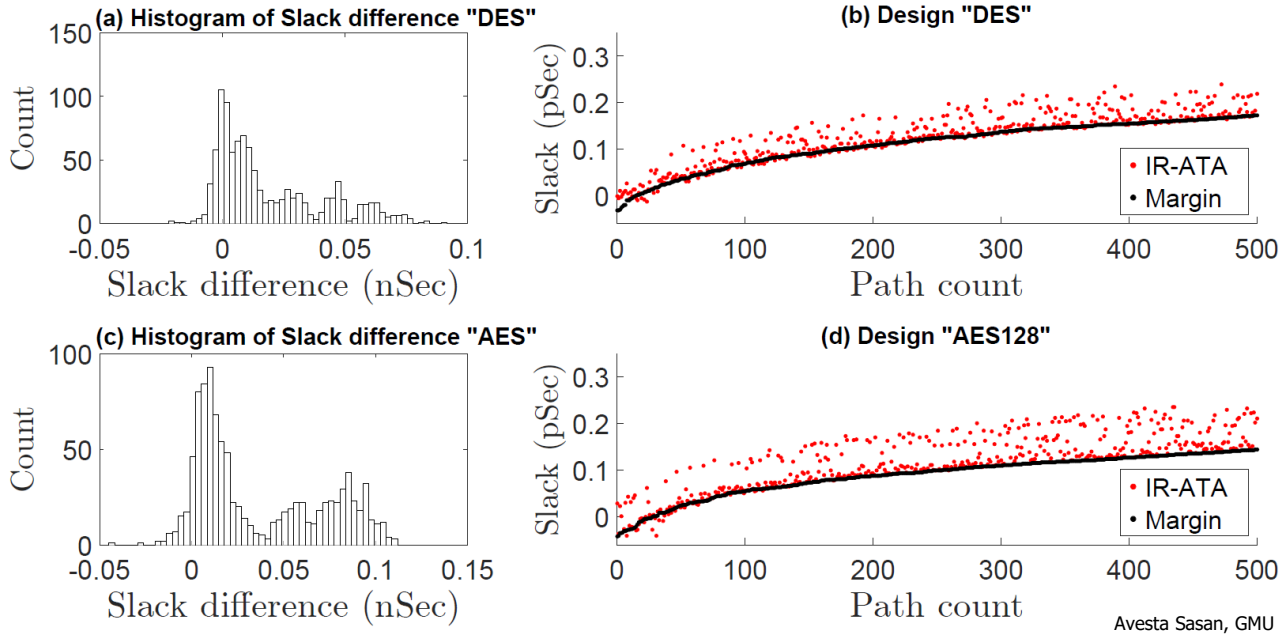
Spice Verification: the improved accuracy of AVATAR (IR-ATA) in capturing the timing impact of Voltage drop (STA versus Spice)



The timing slacks in two nearly timing closed design (DES3 and AES) using conventional margin based and AVATAR flow for generation of GTM.

STA Improvement: Impact of using AVATAR(IR-ATA) for reporting the timing slack:

- The released slack could be used for PPA improvement.



Avesta Sasan, GMU

PPA Improvement

Power reduction: The released slack (from using AVATAR for voltage drop and voltage noise modeling) is used for ECOs targeting the reduction of leakage and dynamic power.

- Reduces Dynamic power
- Reduces Leakage power
- Reduces area

Summary of power & area improvement in the investigated benchmarks when STA is updated with IR-ATA flow, followed by incremental application of power and timing ECOs.

Benchmark	Percentage Reduction			Fixed Timing Violations
	Dynamic P	Leakage P	Area	
DES3	1.9	13	0.32	27
AES	2.3	11	0.75	43
b19	1.6	19	0.81	87
MSP430	2.4	18	0.61	76
ETHERNET	2.3	13	0.90	12
s38417	1.9	21	0.52	47

Performance boost: The released slack (from using AVATAR for voltage drop and voltage noise modeling) in critical timing paths, allow the physical designer to shorten the clock cycle time, leading to a higher performance design.

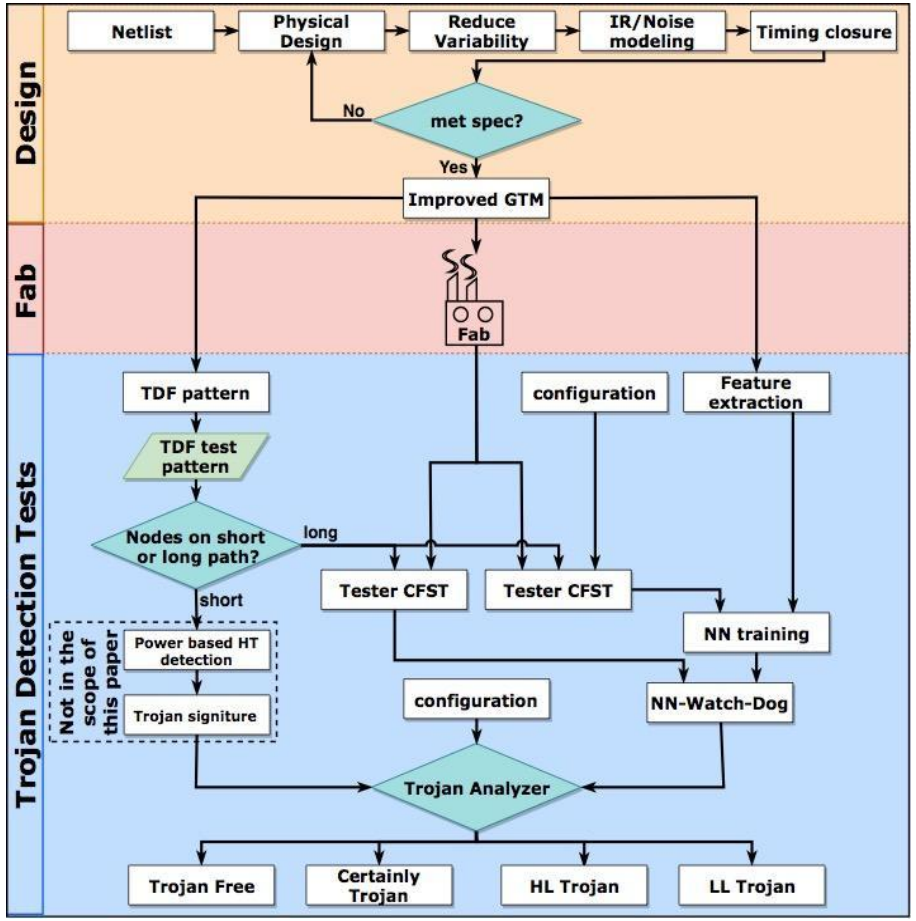
- Increases max frequency

Summary of improvement in the performance (maximum frequency) of investigated benchmark when STA is updated with IR-ATA and increase in total available slack in top 10K timing paths (to be used for dynamic power, leakage & area recovery).

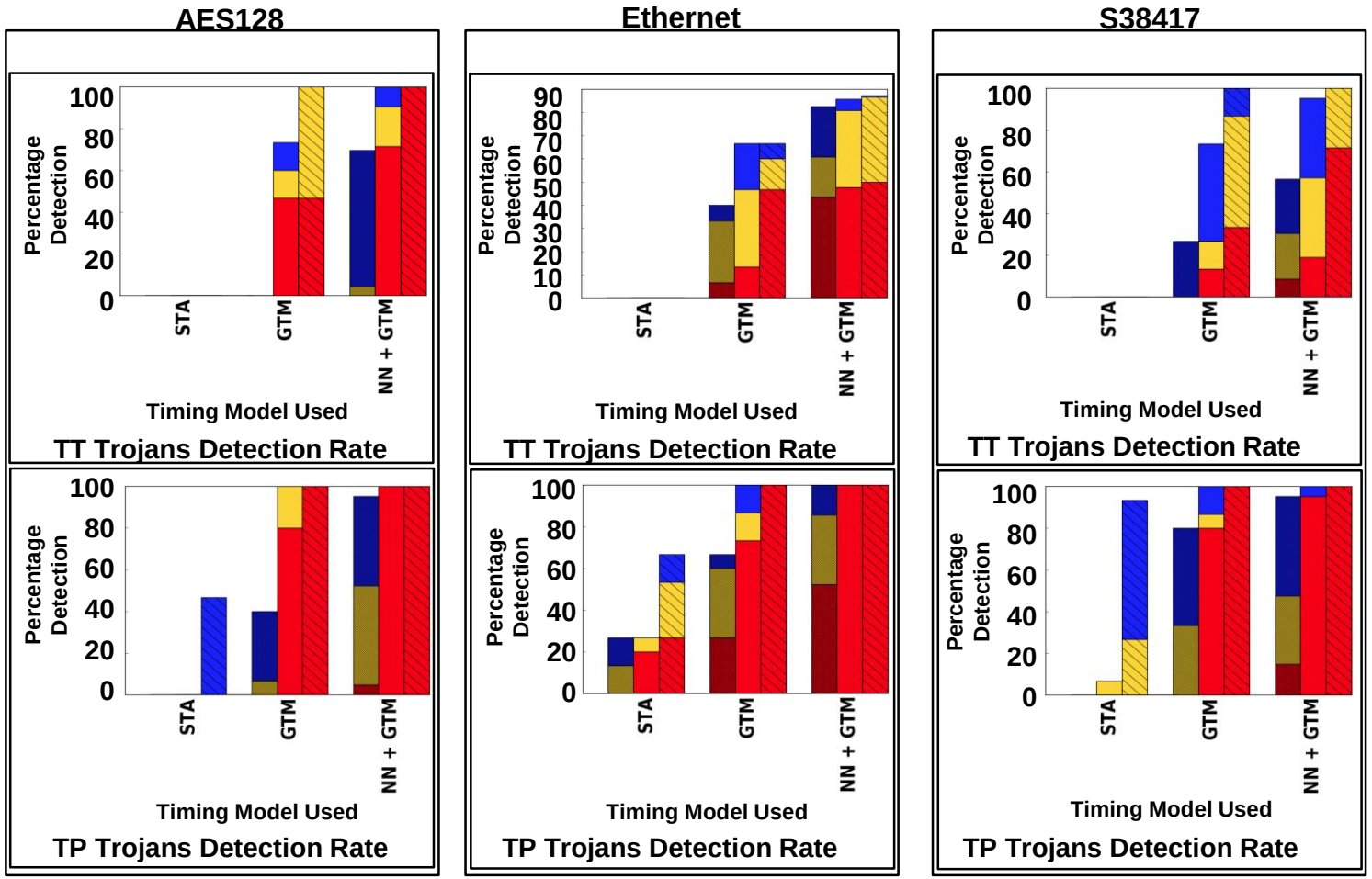
Benchmark	Total Available Slack (ns)		Max Freq (GHz)	
	Before	After	Before	After
DES3	8351.26	8859.78	0.72	0.76
AES	3033.56	33045.42	1.05	1.09
b19	1608.30	1720.31	0.46	0.48
MSP430	842.51	903.09	0.33	0.34
ETHERNET	8347.31	8905.58	0.53	0.54
s38417	499.07	576.16	1.07	1.12

Trojan Detection Rate

The new voltage variation aware timing model (GTM) along with NN process watch dog can significantly improve the chances of Trojan detection without having access to a Golden IC.



Design and test Flow

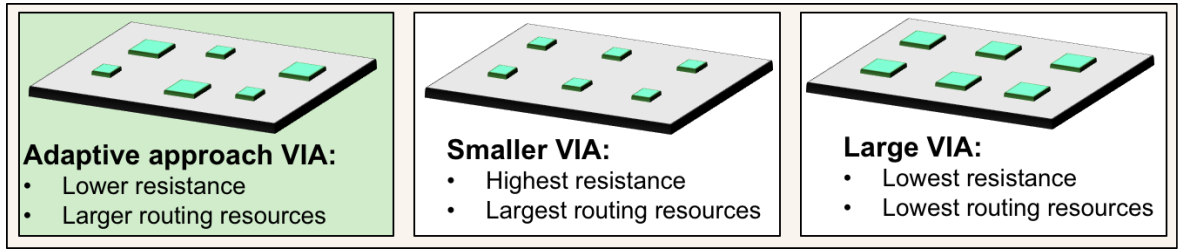


Trojan Detection

Avesta Sasan, GMU

Security aware physical design

Routing VIA: Adapt via size to help enhance power estimation accuracy



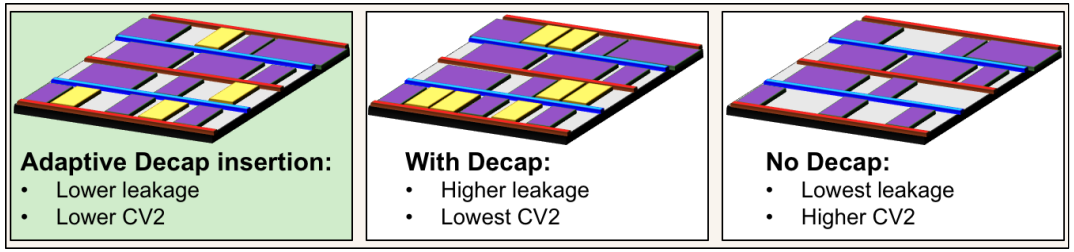
- Upsize critical VIAs
- Adds less routing violations

Summary of change in Vmax, number of routing violations, and percentage of upsized via stacks when using IR-ATA enabled via stack re-sizing in Algorithm 2.

Design (DES3)	Vmax	Routing Violations	% via upsized
(1× 2) Vias	0.895	7	0
IR-ATA-Adaptive Via	0.909	9	14.34
(4× 2) Vias	0.910	2651	100

Decap: Insert decaps to help stabilize power estimate

Avesta Sasan, GMU



- Leakage reduction
- Lower space overhead

IR-ATA enabled Decap insertion uses only half of empty spaces, but reaches similar V_{max} to the design fully packed by decaps, resulting in 2.6% reduction in leakage.

Design (DES)	V_{max}	Leakage Reduction	% empty space used
With Decap	0.912	0	98.84
Proposed ECO	0.911	2.15%	42.53
No Decap	0.897	3.85%	0

Conclusion

- Physical design is where the digital becomes real
- There are several opportunities to enhance security
  - Or inadvertently break it…
- By adding security considerations to physical design offers the opportunity to make better chips, with lower security risk

www.darpa.mil