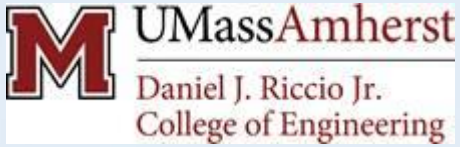
Efficient and Secure AI at the Edge: Two Tales

Wayne Burleson
Professor and Graduate Program Director
Electrical and Computer Engineering
University of Massachusetts Amherst, MA, USA

MPSOC 2026
Victoria, BC, Canada
June 21-26, 2026



Two Tales:

1. Analog Computing for RF ML Classification using Memristor Crossbar Arrays: Security Issues
    - Sponsor: US Army Research Lab
    - Collaborators: Qiangfei Xia, UMass Amherst
    - Students: Faheem Rahman, Negin Mohajeri, Aarushi Mahajan
2. Neuro-device Security
    - Sponsor: US National Science Foundation: Smart and Connected Communities
    - Collaborators:
        - Kevin Fu, Silvia Zhang, Northeastern University
        - Jenny Amos, UIUC
        - Erika Peterson MD, U. Arkansas
        - Julian Goldman MD, Harvard and Mass General Hospital
    - Students: Mortaza Hassani

Analog computing: old idea, new applications and constraints

From wartime control systems to energy-constrained edge AI

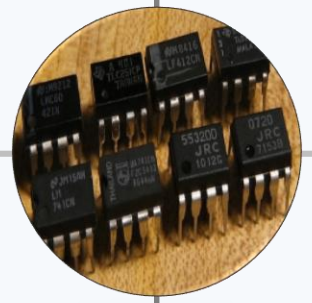
Differential analyzers
mechanical integration of ODEs

1930s

WWII control
fire-control, radar, trajectory

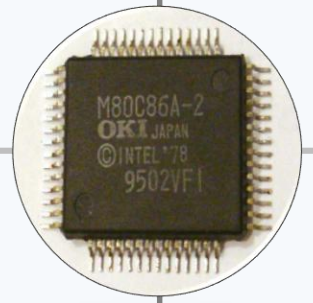
1940s

Op-amp era
summers, integrators, filters



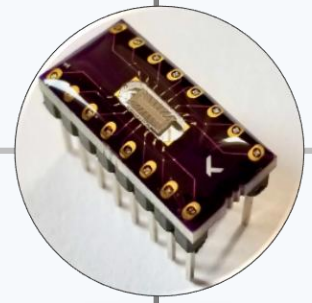
1950s–60s

Digital dominance
software, memory, repeatability



1970s–2000s

Analog revival
edge AI accelerators



Today

Why analog computing faded

- Heat, size, and continuous bias power
- Programming by patching and calibration
- Limited precision, repeatability, and memory

Why it matters again

- Edge workloads need low latency and low energy
- Sensing tasks can tolerate approximate compute
- CMOS/memristors add density and programmability

[1] CHM, “Vannevar Bush’s Differential Analyzer”; [2] CHM, “Choosing Analog”; [3] Analog Devices, Op Amp Applications Handbook, Sec. H.
Image credits: CHM Differential Analyzer; MIT News antenna; Wikimedia Op-amps; Wikimedia Oki 80C86A; Knowm Memristor Crossbar.

A/D Conversion Has Advanced in Efficiency and Performance/Bit

What improved

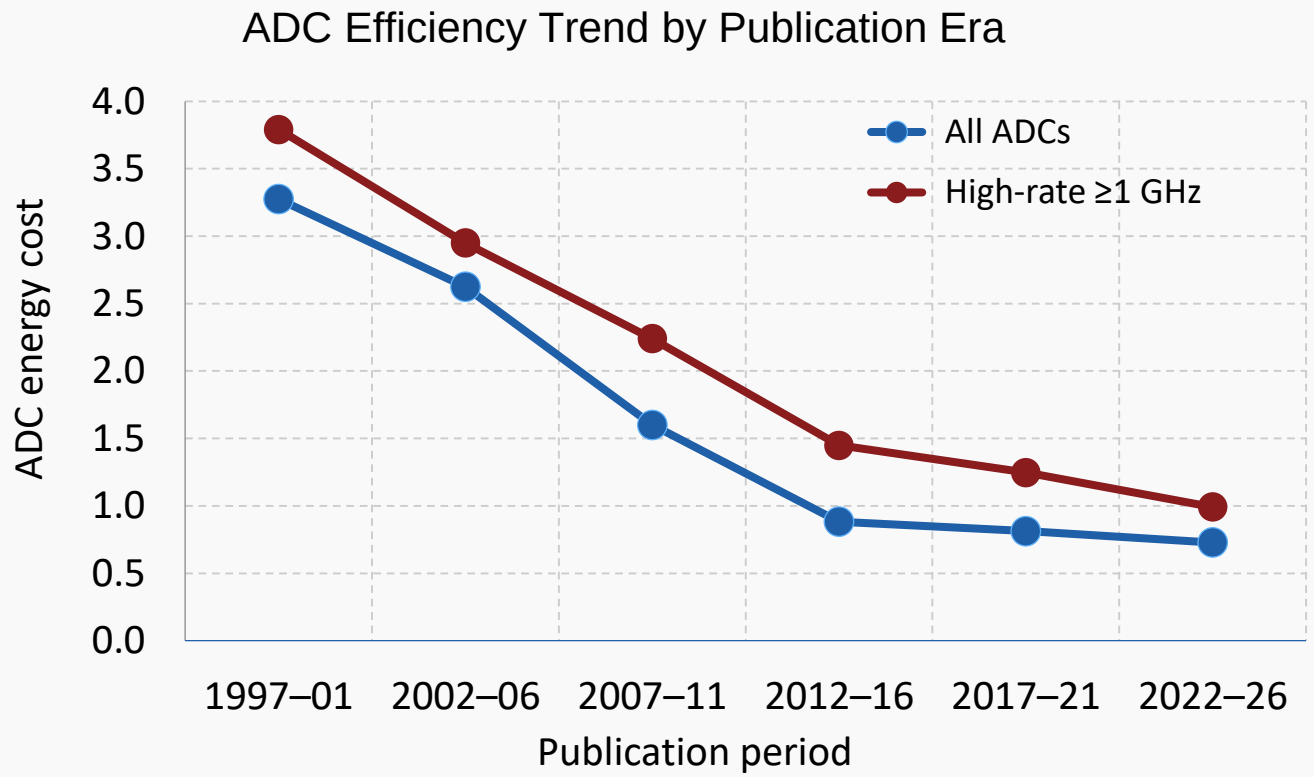
Energy per conversion step fell by orders of magnitude. (note log scale)

What still hurts

- High-rate ADCs show higher ADC energy cost than the All ADCs trends
- Wide RF bandwidth also creates downstream data movement

Design implication

Do not digitize everything first when the edge task only needs selected RF features



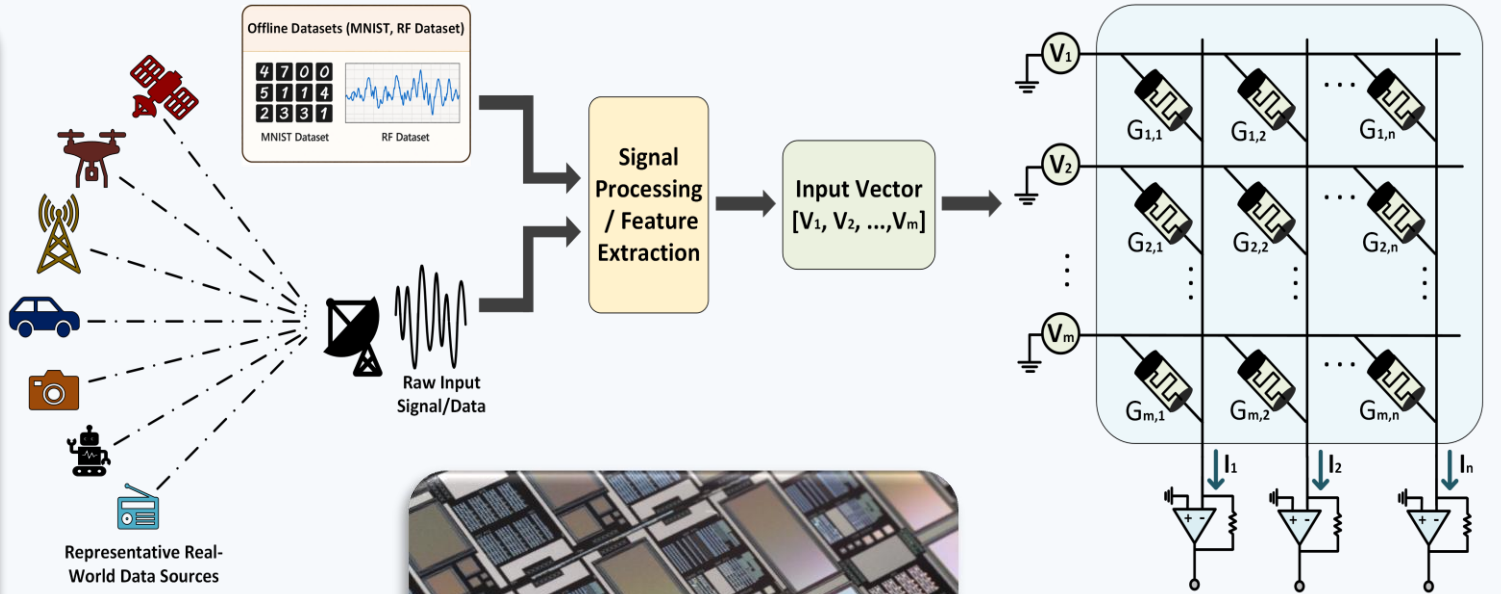
Walden FoM, log10(fJ/conversion-step); **lower is better**

High-rate ADC cost motivates analog edge processing before full-rate DSP

[7] B. Murmann, “ADC Performance Survey 1997–2026,” ISSCC/VLSI data set.

Why analog edge processing for RF signals?

- **Edge constraint:** RF edge sensing requires fast, private, low-energy processing.
- **SDR bottleneck:** Conventional SDR often digitizes before classification-oriented feature extraction, increasing A/D cost and latency.
- **Research hypothesis:** Analog Memristive Crossbar Array (MCA) accelerators can process RF features **earlier** and **more efficiently** in the sensing chain.



Fabricated memristive SoC for RF analog in-memory processing.
Nature Electronics, 2025. Image credit: Yi Huang, UMass Amherst.

RF Signal wideband, analog → **Analog front end** filter / mix / sample → **MCA accelerator** current-domain VMM → **Classifier** low-latency decision → **Secure output** protected model IP

Analog accelerators can be used along with SDR to provide earlier response

Memristive crossbars: compute where the weights are stored

Analog vector-matrix multiplication (VMM) through Ohm's law and KCL current summation

MCA Definition

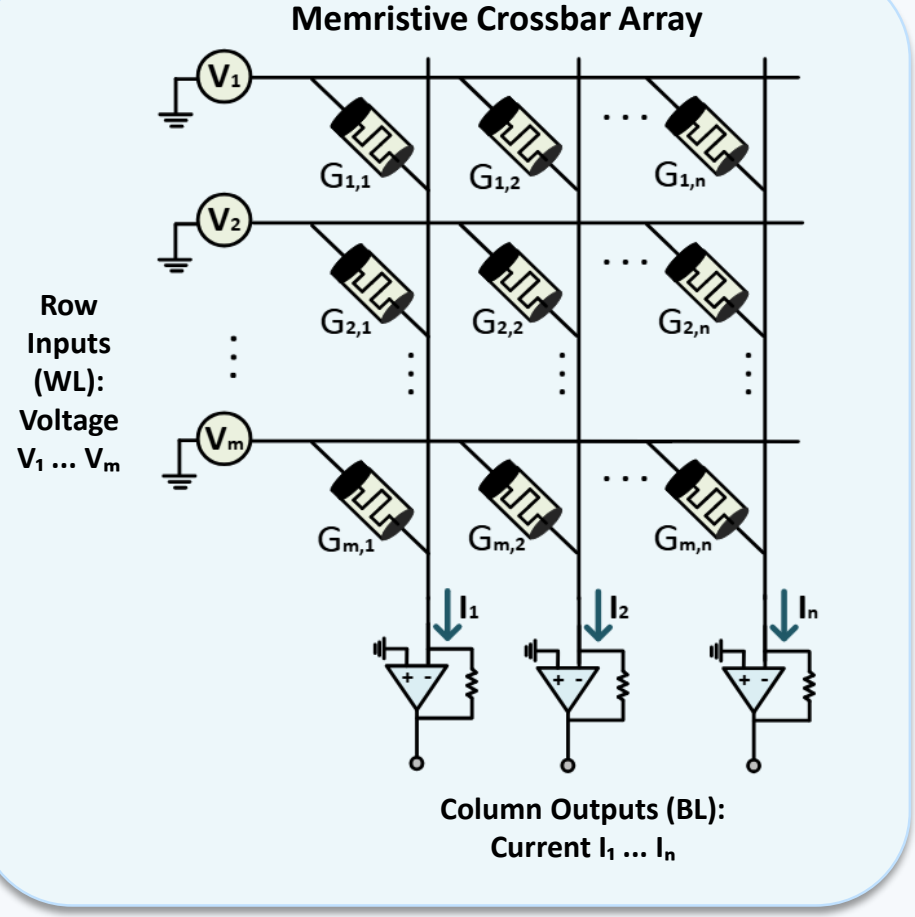
- Grid of WL and BL with memristive devices at each cross-point
- Store weights as conductances
- Row voltages produce column currents
- Enables analog Vector Matrix Multiplication: $(I_j = \sum_i V_i G_{ij})$

Advantages

- Highly parallel with low data movement
- Low latency and high energy efficiency
- Good conductance precision (11 bits) and CMOS compatibility
- RF/AI Fit: Analog input and compute are naturally compatible

Applications

- AI/ML acceleration
- Neuromorphic and in-memory computing
- Signal Processing



[8] A. Sebastian, "Memory devices and applications for in-memory computing," Nat. Nanotechnol., 2020.
[9] D. Ielmini, "In-memory computing with resistive switching devices," Nat. Electron., 2018.

Memristive Crossbar Array Security: Attacker's Objective?

Analog weights, inputs, and outputs are physically observable and vulnerable

Confidentiality risk

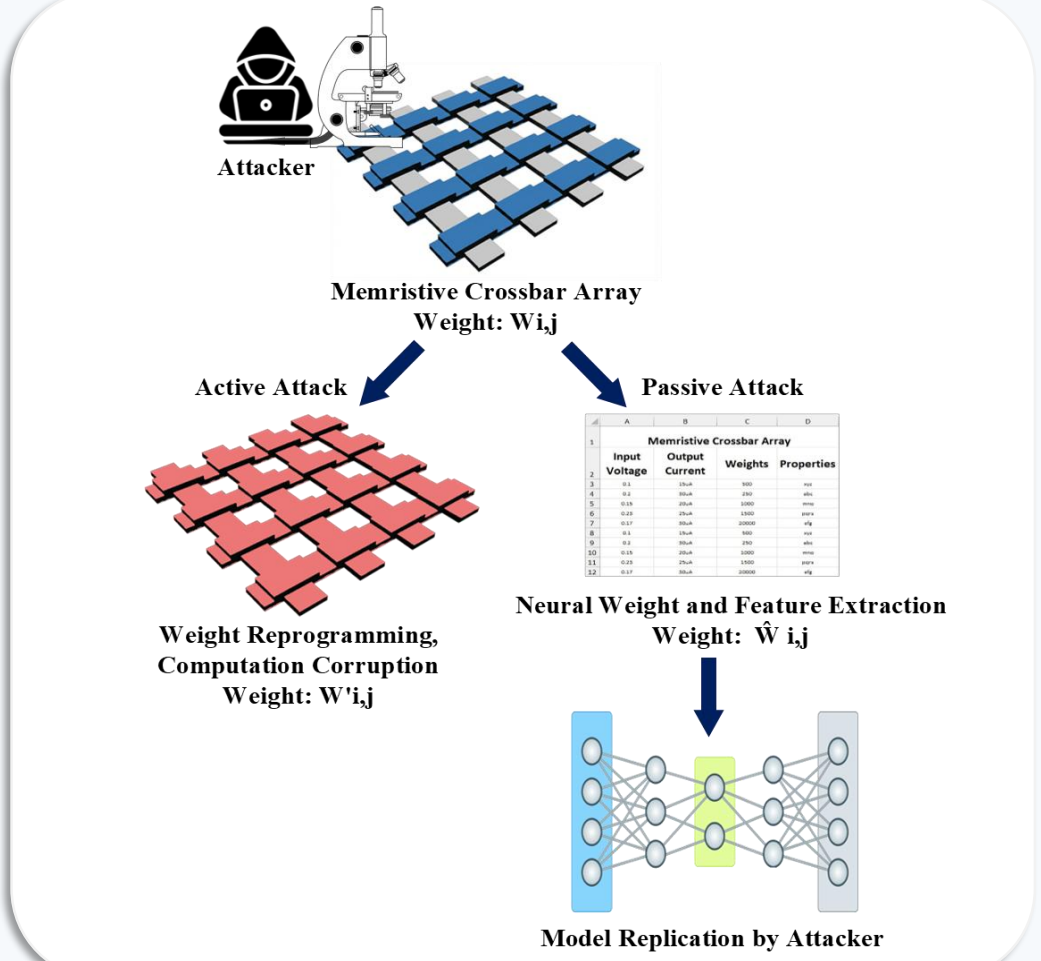
- **Weight leakage**
- **Current-based observation**
- **Model extraction**

Integrity risk

- **Weight tampering**
- **Fault-induced disturbance**
- **Corrupted output**

System-level impact

- **Model theft or cloning**
- **Wrong inference decisions**
- **Need for protection and detection**



MCA efficiency and vulnerability both come from physical conductance-stored weights

[10] Lillis, W., W. Burleson, et al., "Survey of Security Issues in Memristor-Based Machine Learning Accelerators for RF Analysis," Chips, 2024.

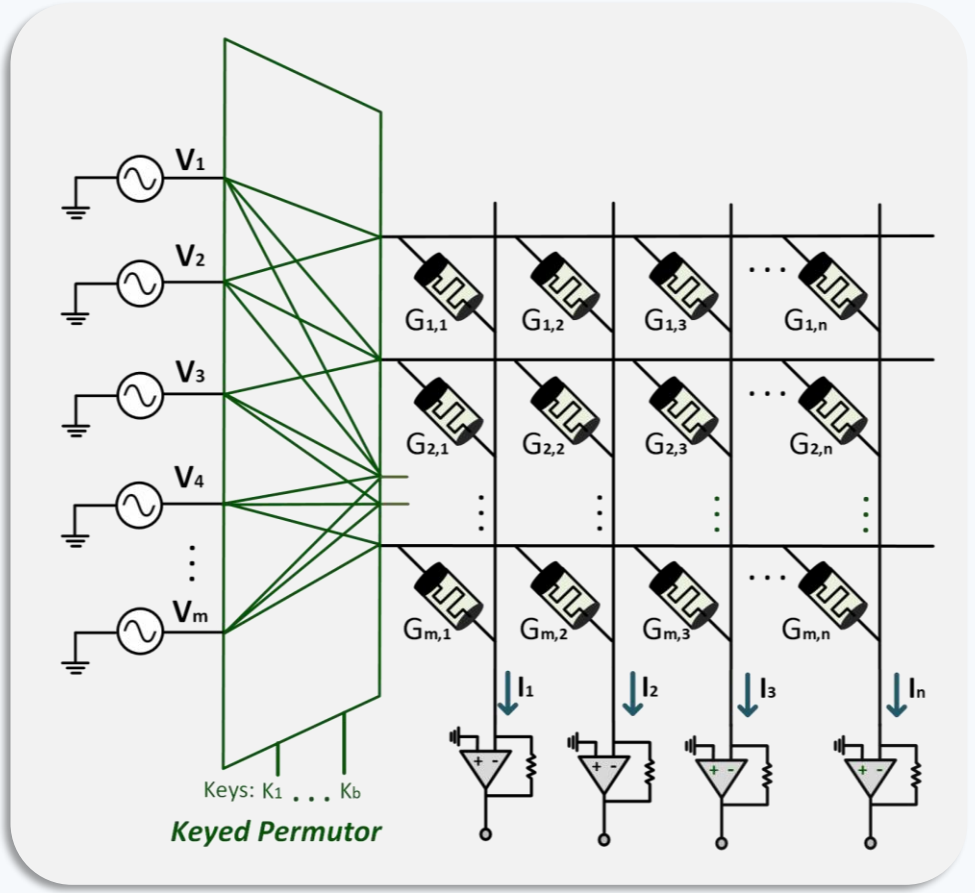
Memristive Crossbar Arrays: Protecting Weight Access

Addresses Threat Model 1: input access + output observation

Keyed Permutor

- Scrambles input-to-row mapping using a secret key
- Preserves correct computation for authorized users
- Also supports row sparing by remapping faulty rows to healthy spare rows

Configuration n=256 input rows	Permutor Fan-in (m)	Approx. Key space	Area Overhead	Remark
Pairwise Swap	2	$(m!)^{\frac{n}{m}} = 2^{128}$	~3.13%	Limited key space
Triplet Swap	**3**	$(\mathbf{m!})^{\frac{n}{m}} \approx 2^{220}$	**~4.67%**	**Compromise of key space and routing**
Quadruplet swap	4	$(\mathrm{m!})^{\frac{n}{m}} \approx 2^{293}$	~6.25%	More routing complexity



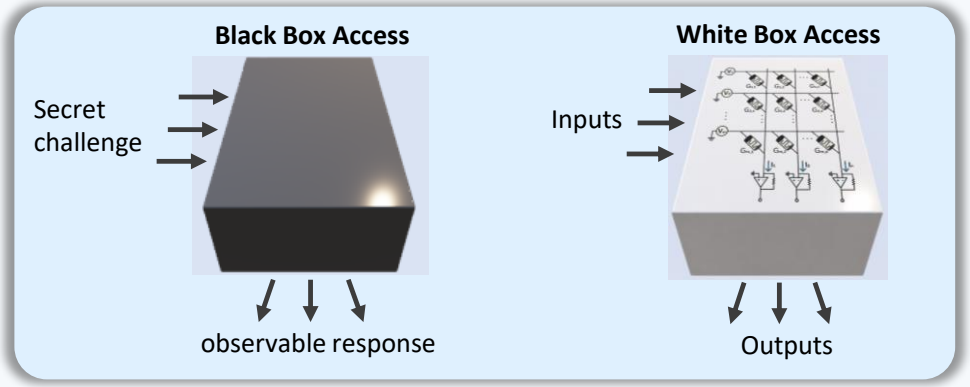
[11] M. F. Rahman and W. Burleson, "Integrated Security Mechanisms for Weight Protection in Memristive Crossbar Arrays," IEEE ASAP, 2025.

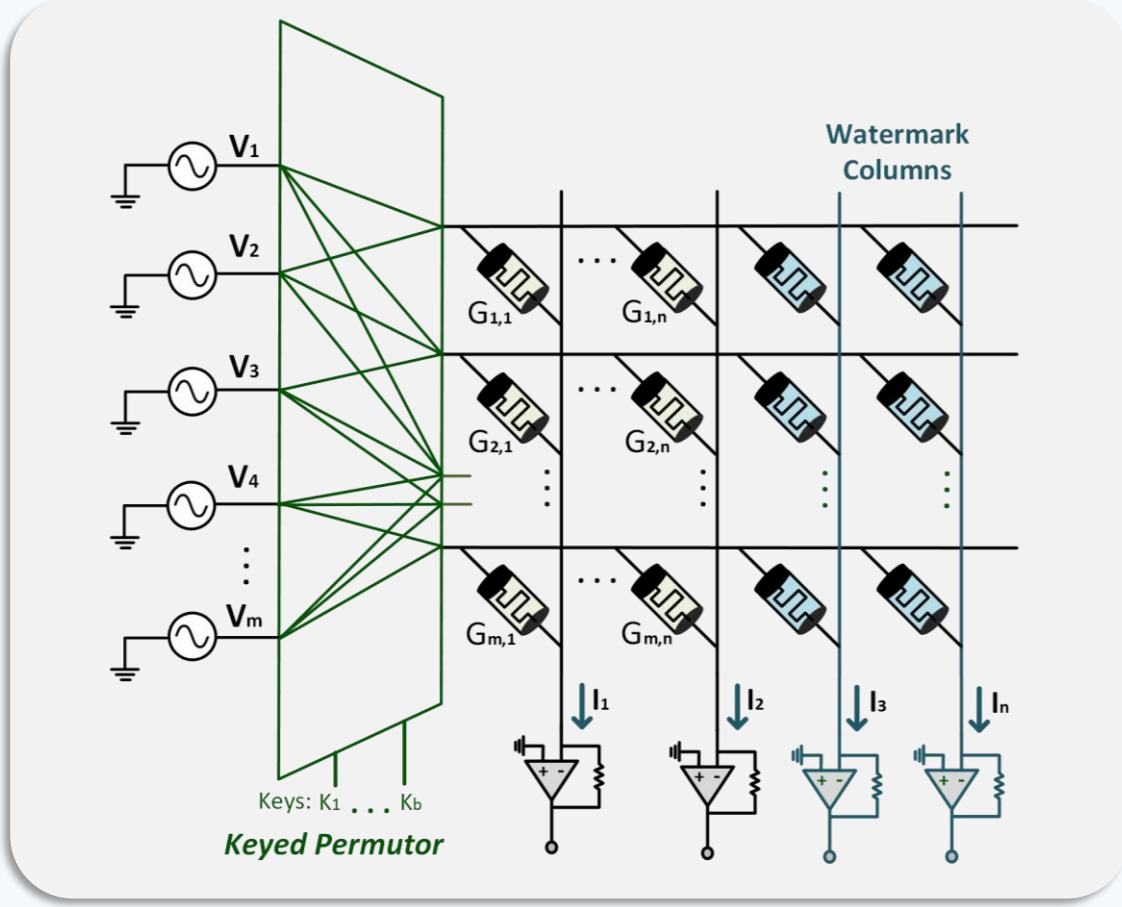
Watermark Columns for Ownership Verification

Ownership authentication and theft identification, rather than direct attack prevention

Watermark Columns: Security role

- Store owner-specific secret signatures
- Secret challenges activate watermark columns
- Do not affect normal computation
- **White-box:** Columns should resemble regular columns
- **Black-box:** Verification uses a secret challenge and observable response





Watermark Columns placement may vary by design

The Keyed Permutor makes extraction harder; Watermarking helps authenticate ownership after copying

[11] M. F. Rahman and W. Burleson, "Integrated Security Mechanisms for Weight Protection in Memristive Crossbar Arrays," IEEE ASAP, 2025.

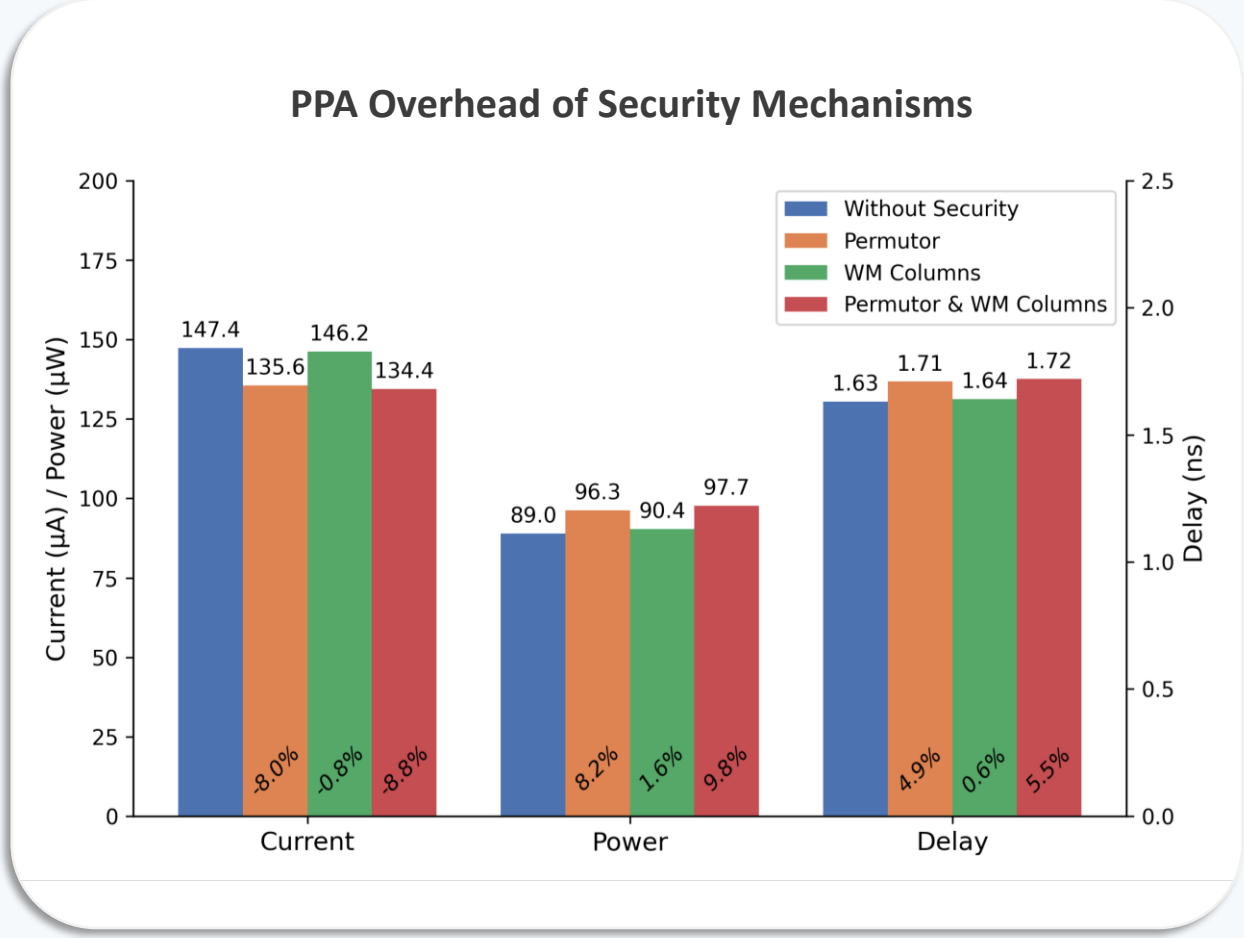
Weight Obfuscation and Watermarking Add Security to MCAs with Low Overhead

Simulation setup

- HSPICE 1T1R memristive crossbar model
- 45 nm GPDK; 22 nm and 12 nm PTM studies
- Parasitic-aware interconnect
- Large-scale 256 × 128 benchmark array

Key findings

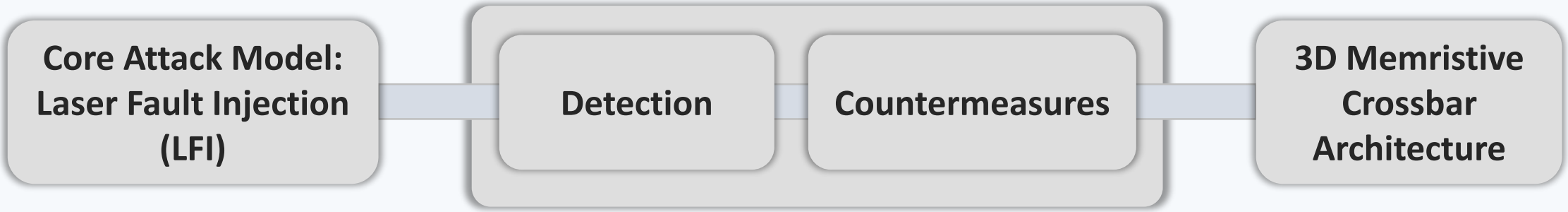
- Watermark columns add very small overhead
- Keyed Permutor contributes most of the overhead
- Watermark columns: ~1.6% power, ~0.6% delay
- Keyed Permutor: ~8.2% power, ~4.9% delay



Combined security impact remains below 10% for current, power, and delay

Memristive Crossbar Arrays: Protecting the Core

Addressing Threat Model 2: crossbar-core probing, fault injection, detection, and countermeasures



Core-level threat model

- Model injected faults inside the crossbar core
- Study **LFI** as a core-level attack on MCA
- Faults can leak or alter stored weights

Detection mechanism

- VDD droop provides a supply-side disturbance signature
- Enables runtime monitoring near the array rails

Built-in countermeasures

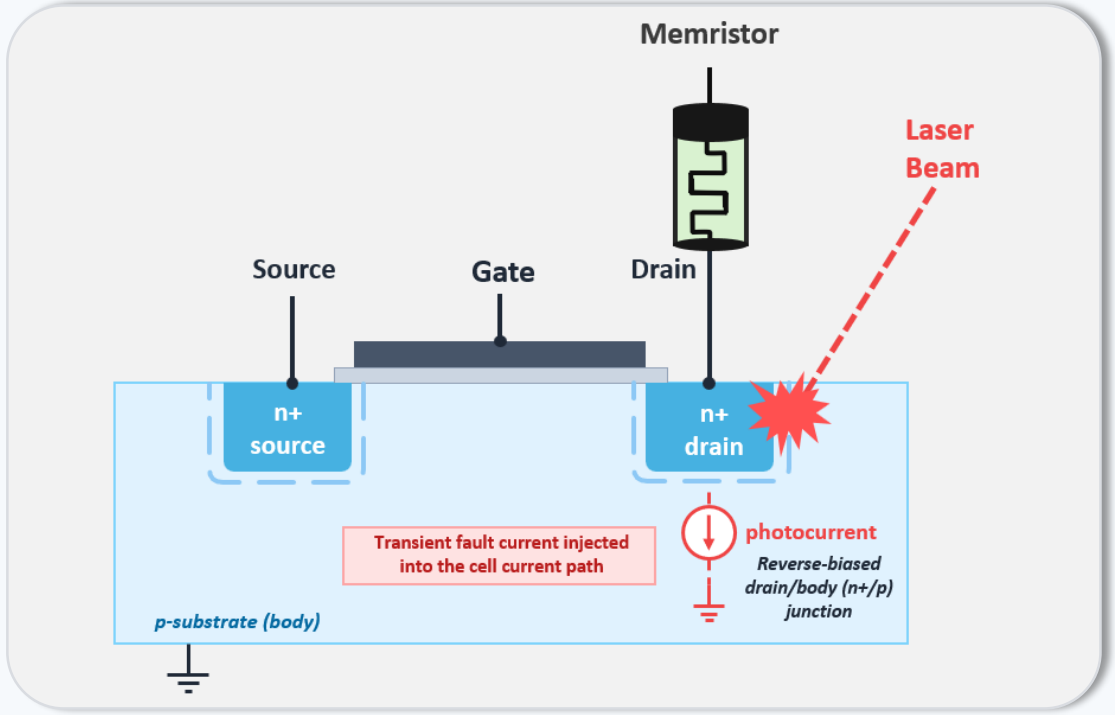
- Replica and canary columns support anomaly detection
- Complementary to VDD-droop sensing

Broader architecture direction

- 3D MCA provides architecture-level protection for core weights

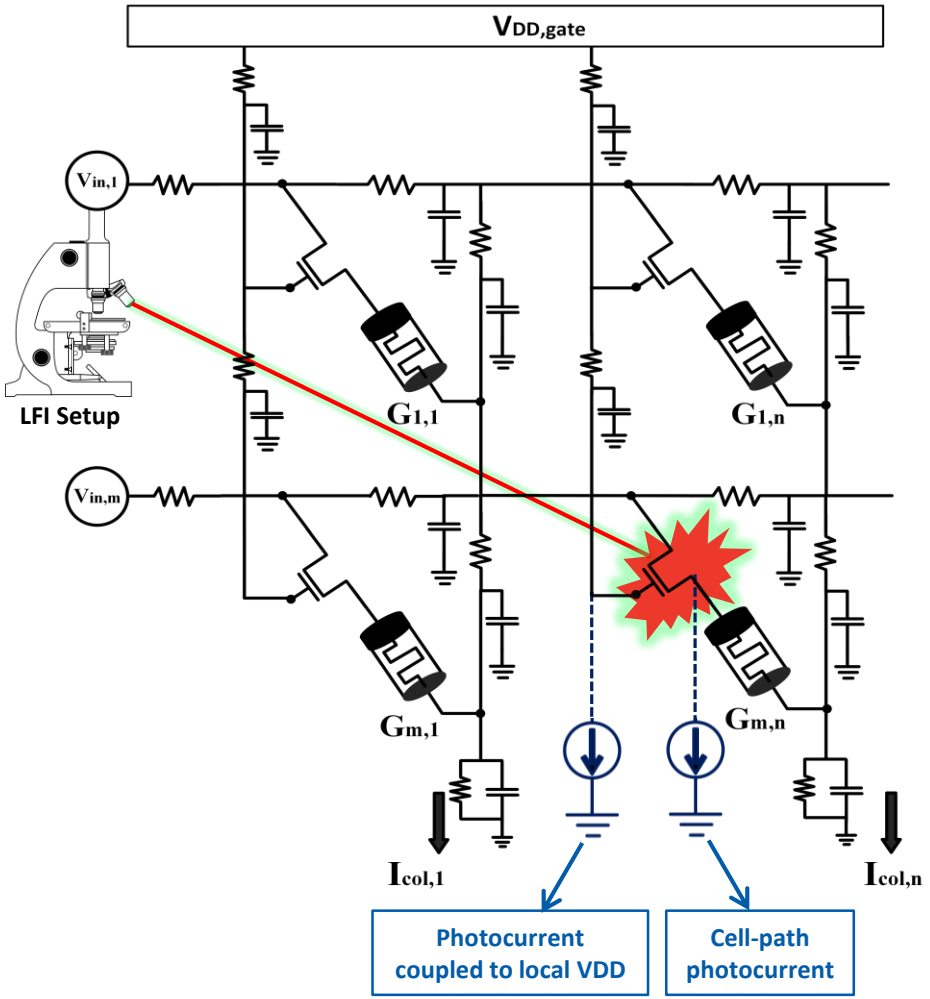
Attack Model: How LFI Becomes Analog Current Injection

Laser-generated carriers at reverse-biased junctions create a parasitic current path



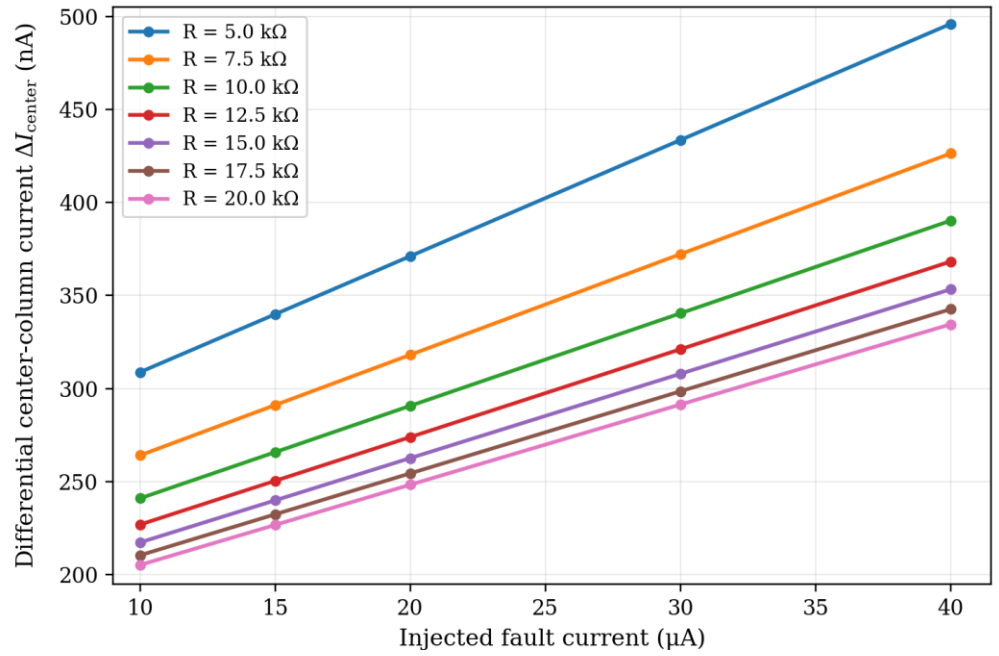
- Laser illumination generates electron–hole pairs
- Collected carriers appear as an injected analog photocurrent
- Cell-path coupling perturbs the output column current
- Supply-side coupling creates local VDD droop
- $I_{col,j}^{(LFI)}(t) = I_{col,j}^{(Nom.)}(t) + \Delta I_{col,j}(t)$

Circuit-level view of LFI in a 1T1R memristive crossbar

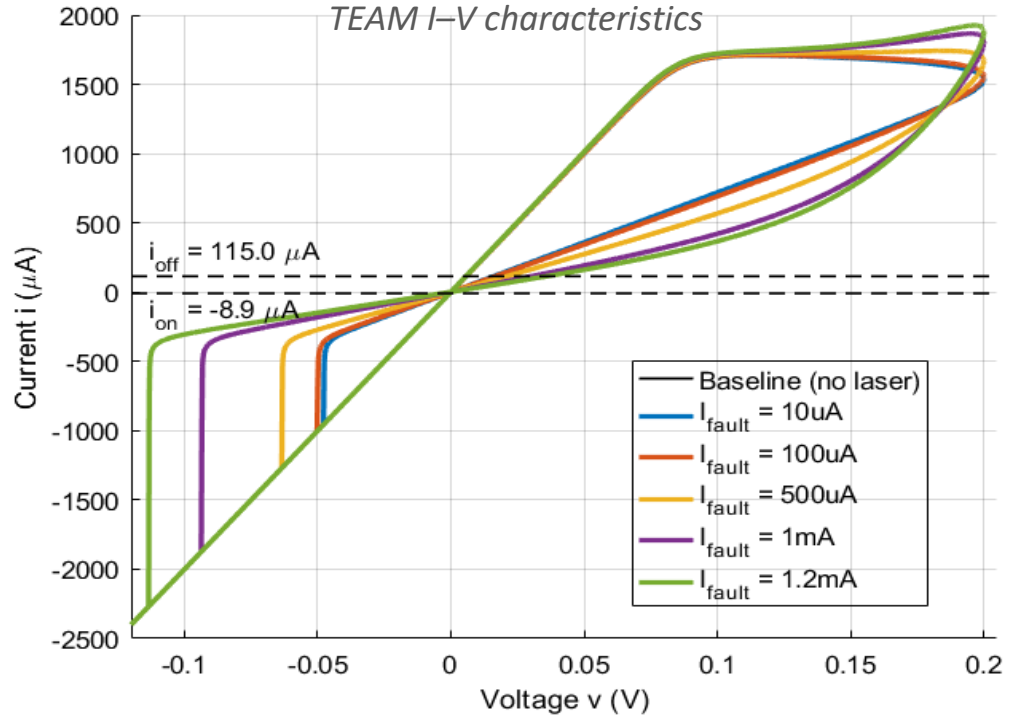


[12] V. Beroulle et al., "Laser-induced fault effects in security-dedicated circuits," VLSI-SoC, Springer, 2015.
[13] K. Yamashita et al., "Redshift: Manipulating signal propagation delay via continuous-wave lasers," IACR TCHES 2022.

LFI Results: Weight Extraction vs. State Alteration



Differential center-column current vs. injected fault current



Low-injection regime: weight extraction

- Laser injection perturbs the struck column current.
- Sweeping fault current gives a near-linear **differential** response.
- Regression maps fault response to conductance:

$$G_{est}(\mu S) = 77.74 \times slope(nA/\mu A) - 285.97$$

High-injection regime: weight alteration

- Small injections cause transient perturbations only.
- Large injections cross the effective switching threshold.
- At high injected current, the TEAM device state shifts ~140%.

[14] S. Kvatinsky et al., "TEAM: ThrEshold Adaptive Memristor Model," IEEE Trans. Circuits Syst. I, 2013.

Detecting Core Faults: VDD Droop and Reference Columns

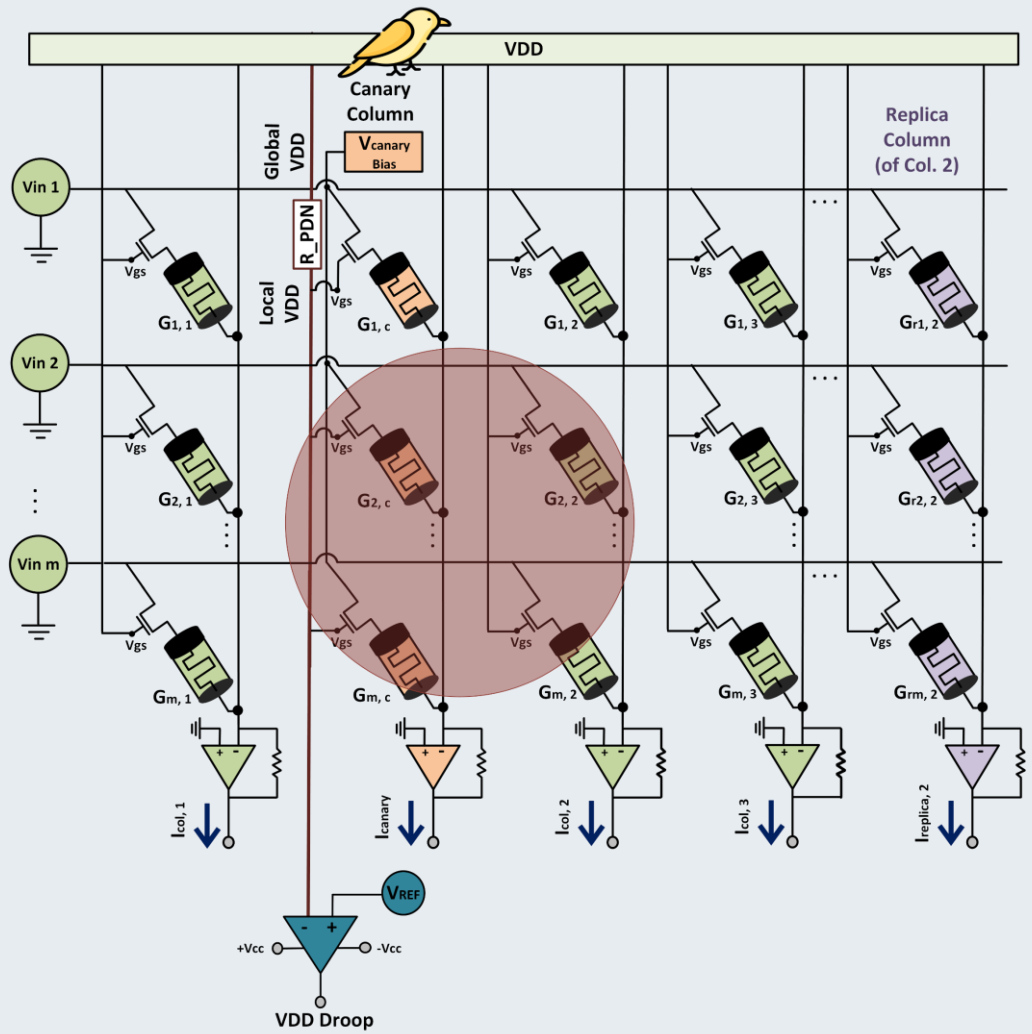
Optical/current disturbances leave both supply-side and column-current signatures

Why VDD droop detection is useful

- LFI can disturb the local VDD rail, not only the target-cell current.
- Sensor continually compares VDD with a reference threshold.
- Excessive droop provides a fast, weight-independent LFI alert.

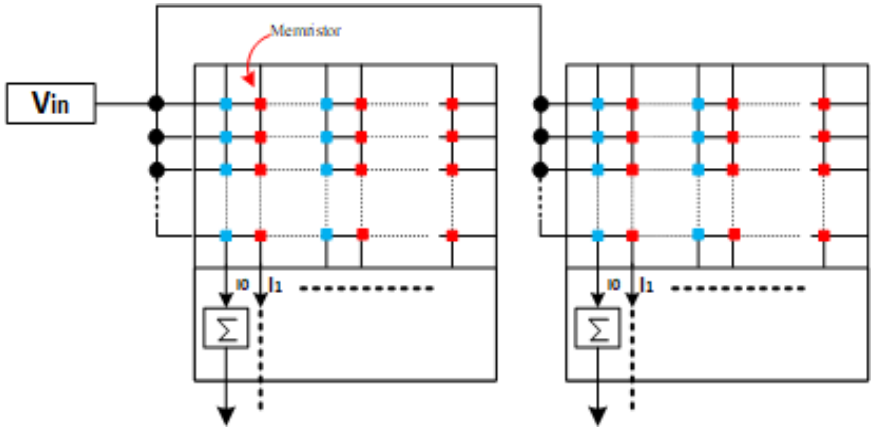
Built-in countermeasures

- **Canary column:** Fixed bias and conductances produce a stable current. Deviation beyond a threshold indicates disturbance.
- **Replica column:** Stores the same weights and inputs as a protected column. A current mismatch indicates localized LFI.
- **Local VDD-droop detection**, along with column monitoring, improves coverage and reduces false alarms.

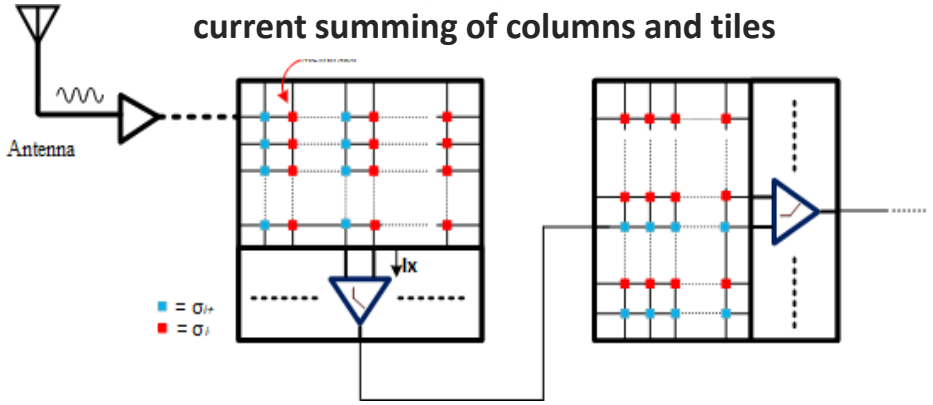


Canary-column, replica-column, and local VDD-droop based LFI detection in a 1T1R memristive crossbar array.

From a Single MCA to a Fully Analog Neural Net Processor



Multiple Tiles using Amplifiers for differential current summing of columns and tiles



Multiple Layers using Amplifiers to convert to voltage, activation function and driving next layer

Array (power, delay) per tile across 10 kΩ/100µS :

- **Small Scale (32×32): 0.65mW, 805.11ps**
- **Large Scale (512×512): 8.15mW, 1109.3ps**

Amplifier Requirements

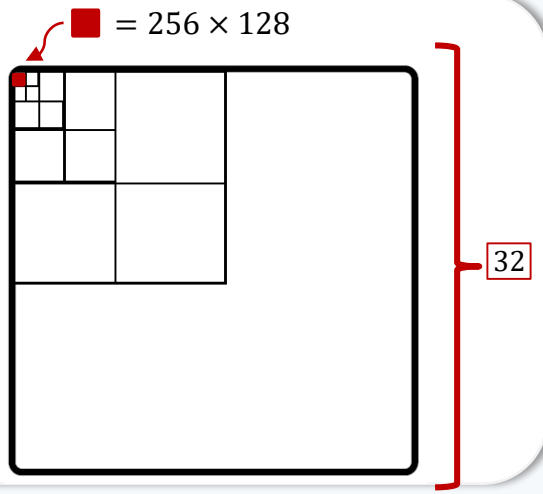
- Column-current sensing and summation
- Current-to-voltage conversion and rectification
- Output buffering and voltage amplification
- High linearity

Design Challenges

- Low-voltage operation and noise
- Long wires and parasitic density
- Signal degradation and resistive loading
- Cascaded-layer interfacing

Example: ResNet34 for RF Dataset

- 22 Million parameters (weights in 34 layers) ~2^25
- 32×32 array of subarrays. Each subarray 256×128
- HSPICE model of full-parallel N×N MCA in 45 nm technology with L-model parasitics and high-impedance loads
- **10-100 W and 1msec estimates**

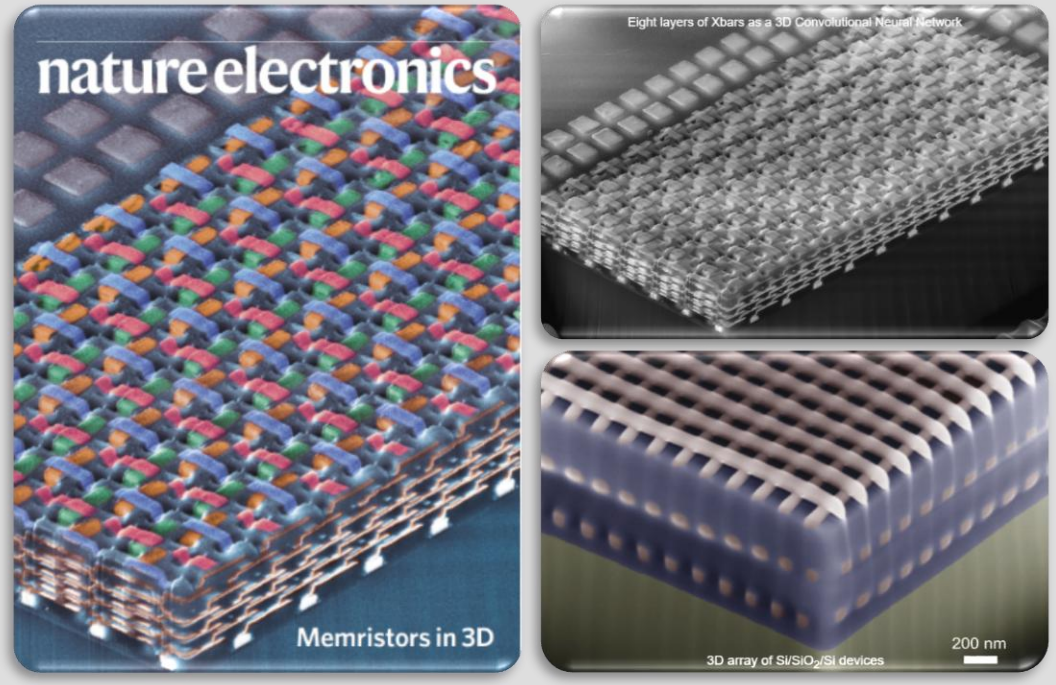


[13] N. Mohajeri and W. Burleson, "Fully Analog and Scalable Memristive Crossbar Arrays," in preparation, 2026.

Why 3D Memristive Crossbar Arrays?

From multi-tile scaling to multi-tier 3D integration

- Multi-tile MCA scales large systems modularly
- Rows/columns can be flexibly connected due to summation associativity (allowing large TSV pitch)
- Multi-tier 3D memristor arrays have already been experimentally demonstrated,
- 2nm length and 6nm pitch using novel Finfet technology.
- 3D integration enables higher density, lower latency, and better energy efficiency
- 3D memory and packaging are already commercialized (3D NAND, HBM)
- **Thermal challenges remain!**



Source: P. Lin et al., Nature Electronics, 2020.
Image credit: Peng Lin and Qiangfei Xia Research Group, UMass Amherst

3D Memristive Crossbar Arrays: Core and Output Confidentiality

Addressing Threat Models 2 and 3: localized core probing and output-only observation

- Split effective weights across multiple tiers
- Store conductance as a cross-tier sum: $G_{eff} = G_1 + G_2 + \ldots$
- A single physical layer reveals only partial model information
- Output observation is incomplete without cross-tier aggregation
- HSPICE simulations compare 2D and multi-tier 3D MCA baselines with TSV/interconnect parasitics.

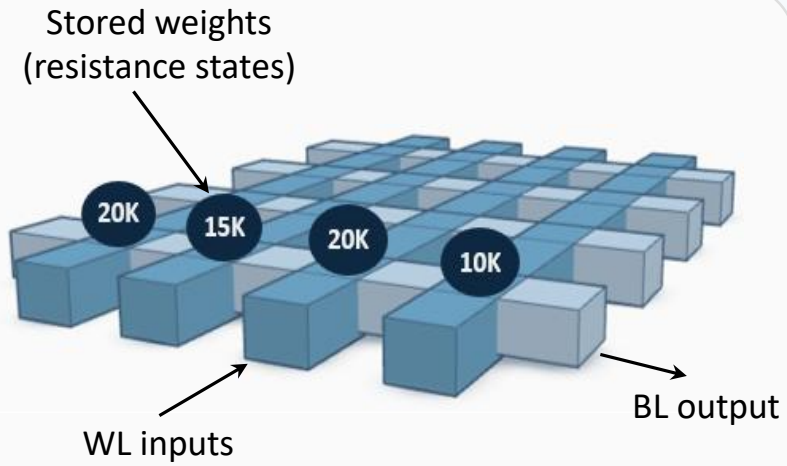
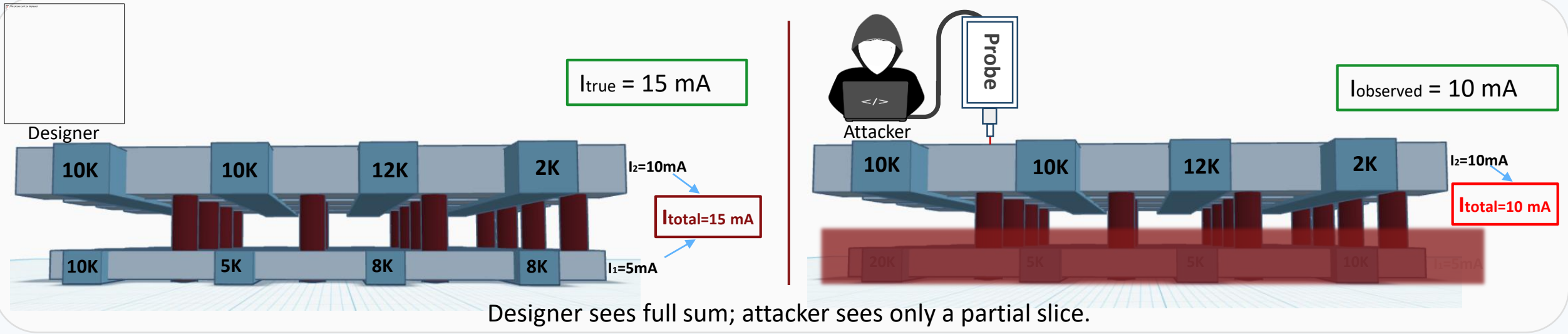


Fig. 2D baseline: a single-layer view exposes the full weight pattern.

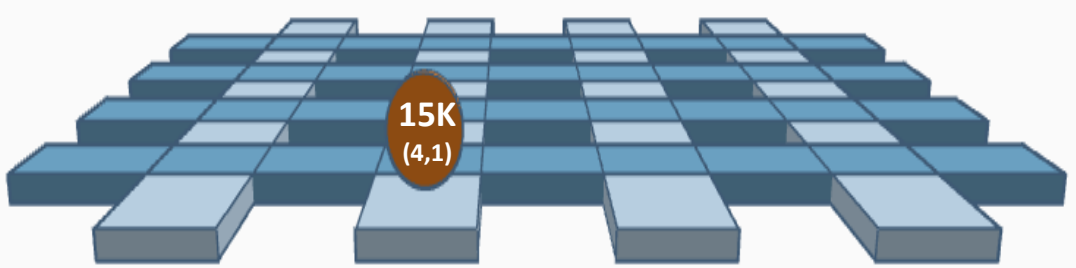


Designer sees full sum; attacker sees only a partial slice.

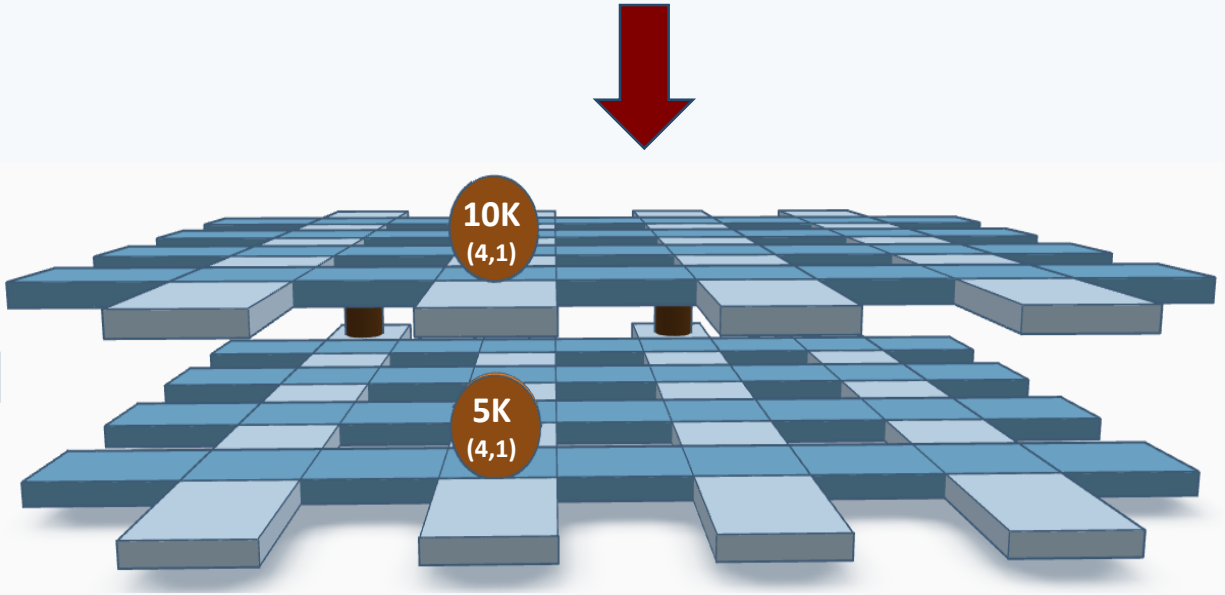
Cross-Tier Mapping Obfuscation for 3D Memristive Crossbars

Splitting weights is not enough without the mapping key

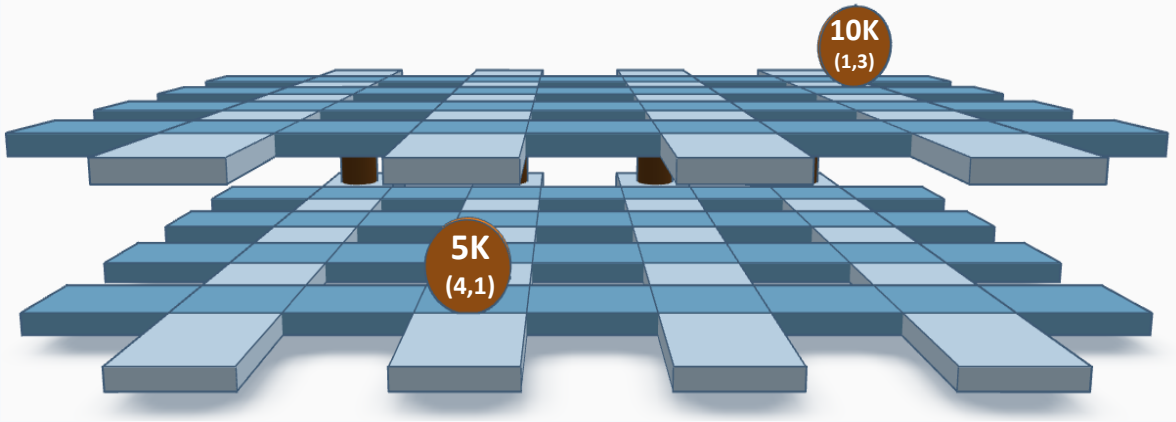
- Split weight shares are not necessarily aligned across tiers
- Secret mapping hides the physical-to-logical weight locations
- Time-varying mapping can hinder repeated profiling attacks



2D baseline: full weight in one visible location



Plain split: aligned locations across tiers

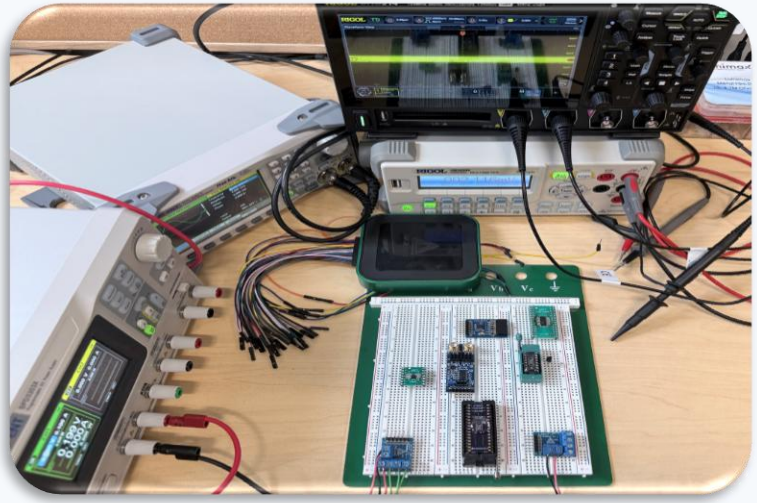


Obfuscated split: remapped across rows, columns, or tiers

Ongoing Hardware Validation: From SPICE to discrete Devices

Why Physical Validation Matters

- Confirms simulation concepts on real devices
- Captures device-to-device variation and programming history
- Reveals wiring, contact, loading, and instrument effects
- Tests repeatability, calibration, and readout robustness
- Guides practical security thresholds and countermeasure design



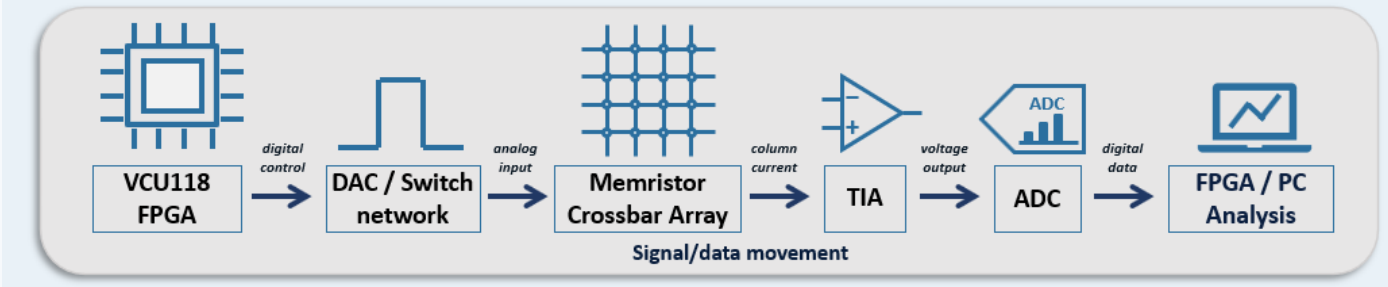
Experimental Hardware Setup with Knowm Discrete Memristors and 8x8 MCA

Goal and Setup

- Establish hardware platform for MCA security research
- FPGA + DAC/switch network + MCA + TIA + ADC

Security Extension Measurements

1. Input-row obfuscation and watermark verification
2. Weight inference from current traces
3. Electrical emulation of LFI-style attacks
4. Disturbance detection using canary columns and VDD droop
5. Split-weight confidentiality through multi-array emulation



Tale #2:
From Technology to Humans:
Protecting Users of Neural and Medical Implant Technologies Through Resilience and Safety Engineering

Prof. Wayne Burleson
Professor and Graduate Program Director
Electrical and Computer Engineering
University of Massachusetts Amherst, MA, USA

NeuroSec: Transdisciplinary

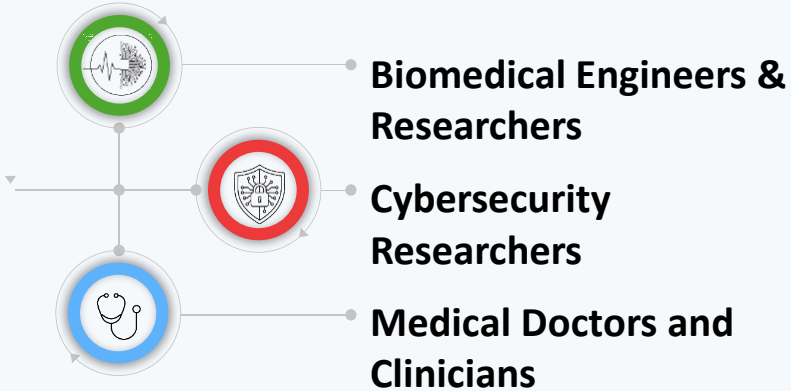
PROJECT LEADERSHIP

Kevin Fu - **Northeastern Univ. (PI)**
Wayne Burleson - **UMass Amherst (Co-PI)**
Xuan (Silvia) Zhang **- Northeastern Univ. (Co-PI)**
Jennifer Amos **- Univ. of Illinois UC (Co-PI)**
Erika Petersen MD **- Univ. of Arkansas (Co-PI)**
Julian Goldman MD **– Harvard, Mass General Hospital**

Industry Partners:
Medtronic, Boston Scientific, St. Jude, Nevro, +25…

NSF Award #2531225

$3.5M – 5 Year Award



Biomedical Engineers & Researchers

Cybersecurity Researchers

Medical Doctors and Clinicians

Northeastern University · HARVARD MEDICAL SCHOOL · UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN · MGH 1811 · UAMS University of Arkansas for Medical Sciences · University of Massachusetts Amherst · Archimedes Neuro Cybersecurity Community Project

Implanted Neuro Devices: Statistics & Trends

Market Size (2025)	Forecast (2034)	CAGR (2026-2034)	Base Year
$11.31B	$29.08B	11.2%	2025

Implantable Neuromodulation Device Market Outlook 2025-2034

https://marketintelo.com/report/implantable-neuromodulation-device-market

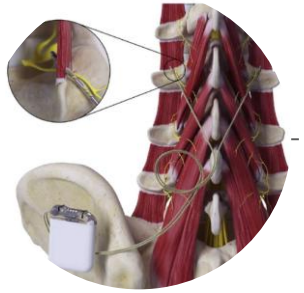
10% **Of Americans will have a device implanted into their bodies during their lifetimes**

https://journalofethics.ama-assn.org/issue/implantable-material-and-device-regulation

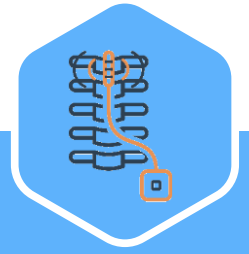
54% **Of the U.S. population has a neurological disorder**

https://news.yale.edu/2025/12/09/massive-hidden-burden-neurological-disorders

- Parkinson's disease
- Essential tremor
- Epilepsy
- Amyotrophic Lateral Sclerosis (ALS)
- Chronic neuropathic pain
- Major Depressive Disorder (MDD)
- Obsessive-Compulsive Disorder (OCD)
- Brain-Computer Interface (BCI)



Neuro-stimulation Treatment Modalities



Spinal Cord Stimulation (SCS)

Chronic back pain, Failed Back Surgery Syndrome (FBSS), Neuropathic pain

Frequency: **40–60 Hz**
Pulse width: **200–500 µs**
Amplitude: **1–10 mA**
High-frequency: **1–10 kHz**
Pulse width: **20–50 µs**

Deep Brain Stimulation (DBS)

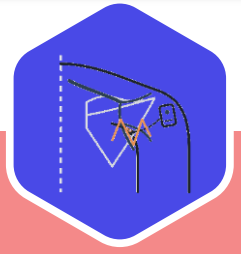
Parkinson's Disease (PD), Essential Tremor, Dystonia, Obsessive-Compulsive Disorder (OCD)

Frequency: typically, **100–185 Hz**
Pulse width: **60–210 µs**
Amplitude: **1–5 V**

Vagus Nerve Stimulation (VNS)

Drug-resistant Epilepsy, Treatment-resistant Depression

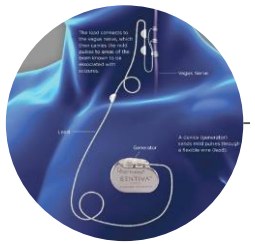
Frequency: **20–30 Hz**
Pulse width: **250–500 µs**
Current: **0.25–3.5 mA**



Peripheral Nerve Stimulation (PNS)

Peripheral neuropathy, localized chronic pain, CRPS, Diabetic Neuropathy

Frequency: **10–100 Hz**
Pulse width: **50–400 µs**
Amplitude: commonly **mA range**



[2] Neuromodulationjournal.org
[3] doi:10.1001/jamaneurol.2021.0538
[4] https://www.brainfacts.org/diseases-and-disorders/therapies/2017/the-past-and-promise-of-deep-brain-stimulation-062817
[5] https://neurology.ufl.edu/divisions/epilepsy/neuromodulation-vns-rns-dbs/
[6] https://painandspinespecialists.com/treatments/peripheral-nerve-stimulation/

2000's to 2020's
Cardio to Insulin Pumps to Neuro

TECHNOLOGY

My Pacemaker Is Tracking Me From Inside My Body

Cloud-connected medical devices save lives, but also raise questions about privacy, security, and oversight. An Object Lesson.

By Neta Alexander

https://www.theatlantic.com/technology/archive/2018/01/my-pacemaker-is-tracking-me-from-inside-my-body/551681/

Hacked terminals capable of causing pacemaker deaths

By Darren Pauli

Oct 17 2012 12:33PM

https://www.itnews.com.au/news/hacked-terminals-capable-of-causing-pacemaker-mass-murder-319508

FDA reports potential cybersecurity risk with insulin pump system

Sep 20, 2022 - 03:24 PM

https://www.aha.org/news/headline/2022-09-20-fda-reports-potential-cybersecurity-risk-insulin-pump-system

The Switch

Yes, terrorists could have hacked Dick Cheney's heart

October 21, 2013 More than 12 years ago

https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/

LILY HAY NEWMAN SECURITY JUL 16, 2019 2:13 PM

These Hackers Made an App That Kills to Prove a Point

Medtronic and the FDA left an insulin pump with a potentially deadly vulnerability on the market—until researchers who found the flaw showed how bad it could be.

https://www.wired.com/story/medtronic-insulin-pump-hack-app/

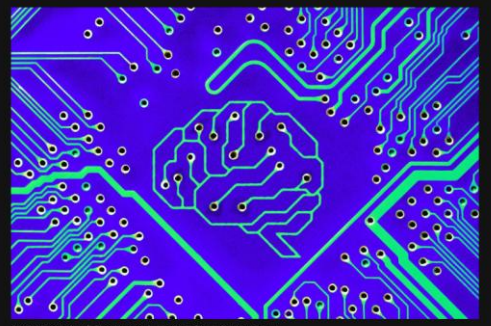
FDA recalls close to half-a-million pacemakers over hacking fears

Security concerns over connected health devices are once again in the spotlight.

by Saqib Shah • Aug. 31, 2017 6:45 am EST

https://www.engadget.com/2017-08-31-fda-pacemakers-abbott-hacking.html

Neurotech companies are selling your brain data, senators warn



/ Neurotech companies have access to some of users' most sensitive data – and few regulations on what they can do with it.

by Gaby Del Valle

Apr 28, 2025, 1:00 PM EDT

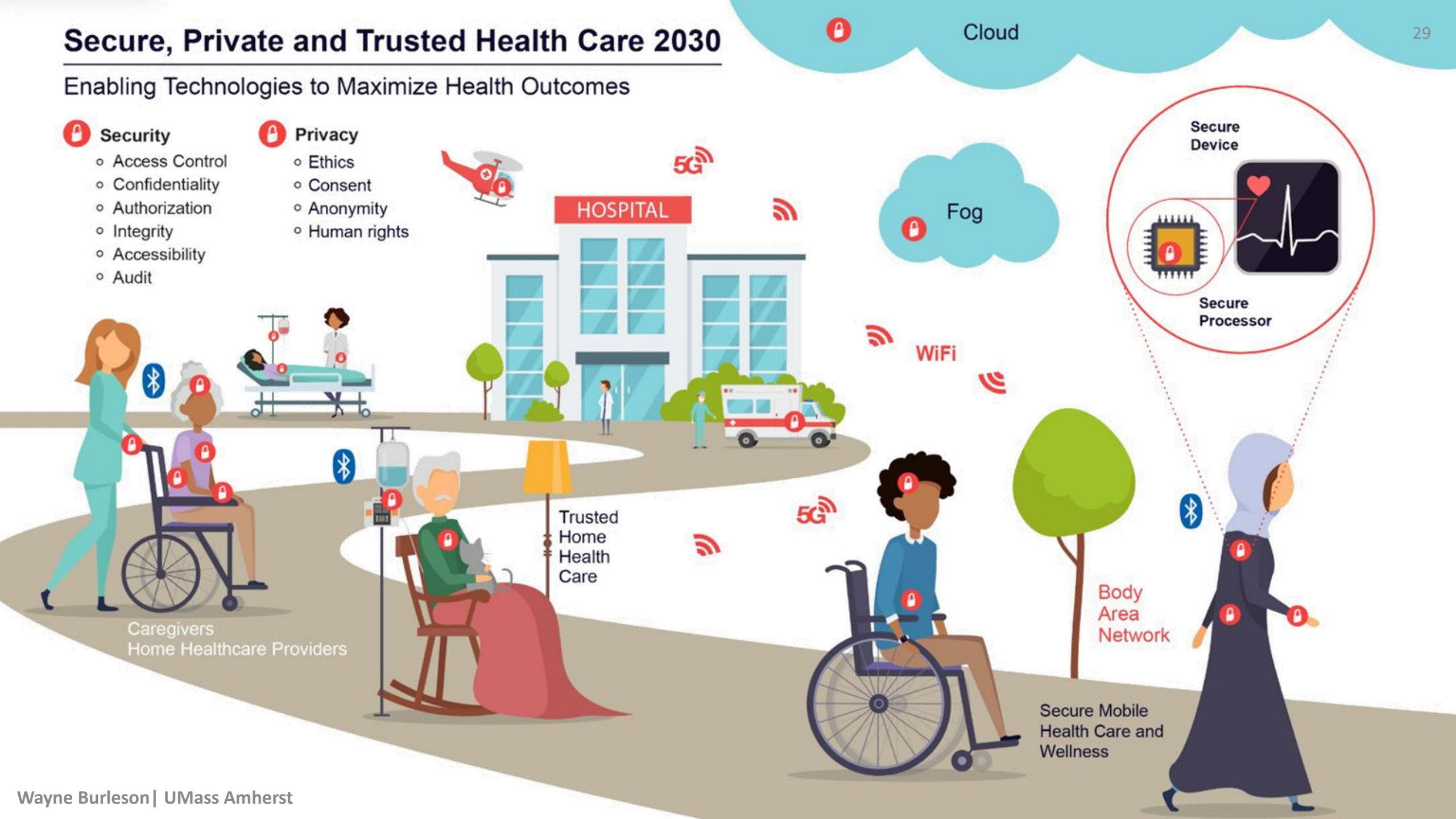
2 Comments (All New)

Cath Virginia / The Verge | Photos from Getty Images

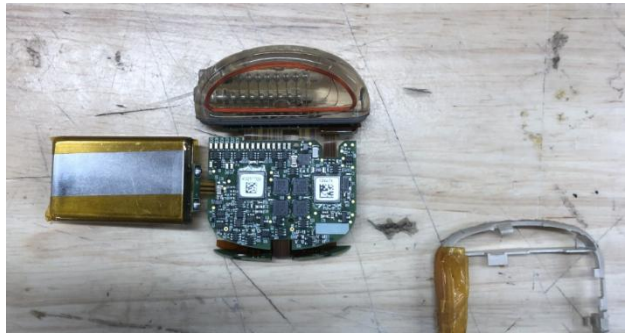
https://www.theverge.com/policy/657202/ftc-letter-senators-neurotech-companies-brain-computer-interface

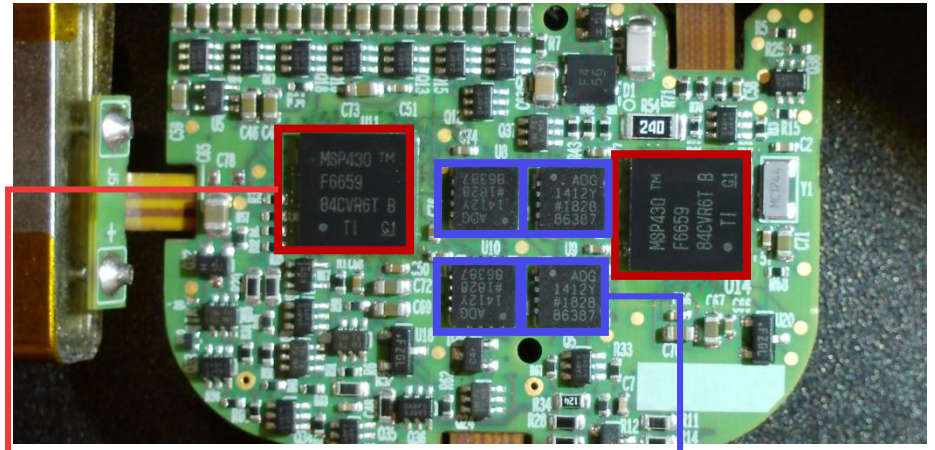
Secure, Private and Trusted Health Care 2030

Enabling Technologies to Maximize Health Outcomes



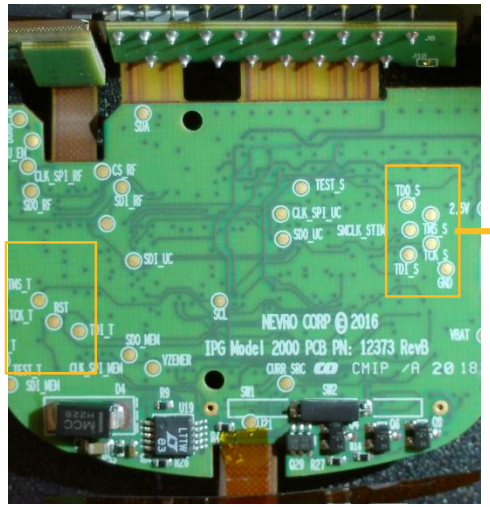
Implantable Neurostimulator Hardware Teardown





MSP430F6659:Microcontrollers

ADG1412Y: Analog Switches



JTAG

Hardware Teardown and Reverse Engineering Team

- Mortaza Hassani, UMass
- Kevin Fu NEU
- Hui Zhuang, NEU
- Takeshi Sugawara, UEC Japan

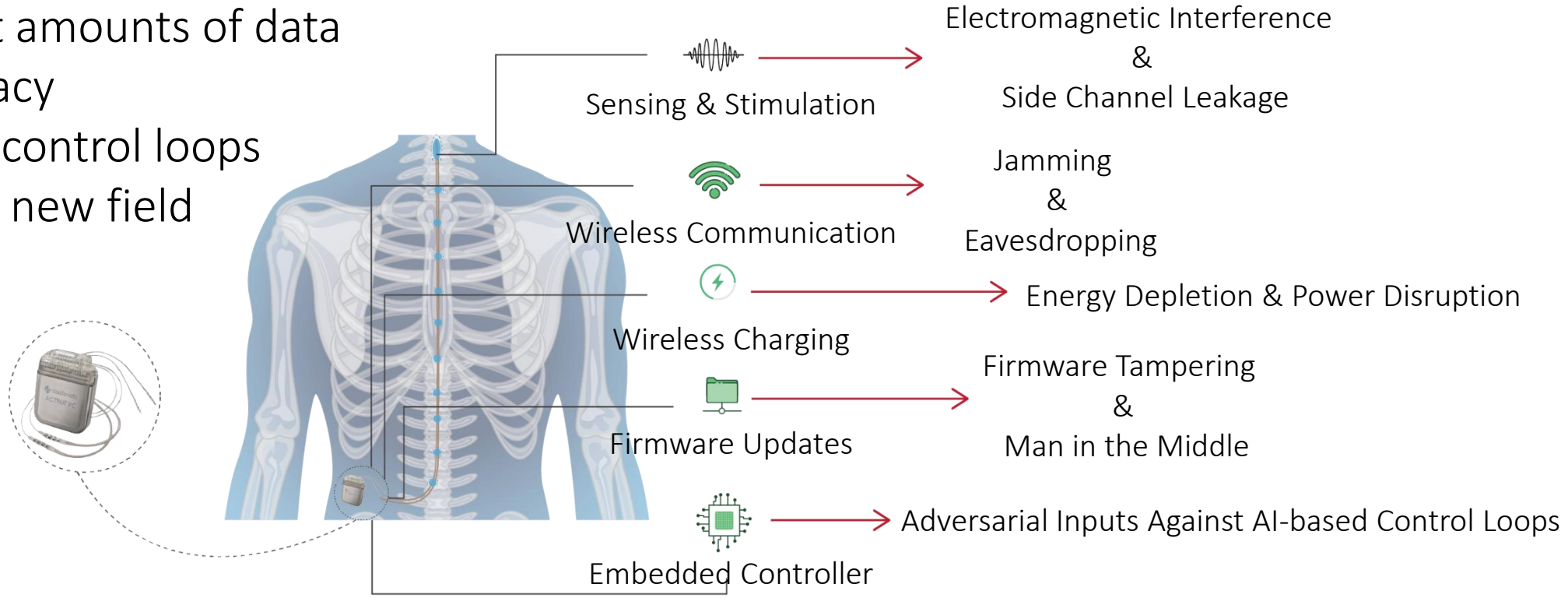
Targets:

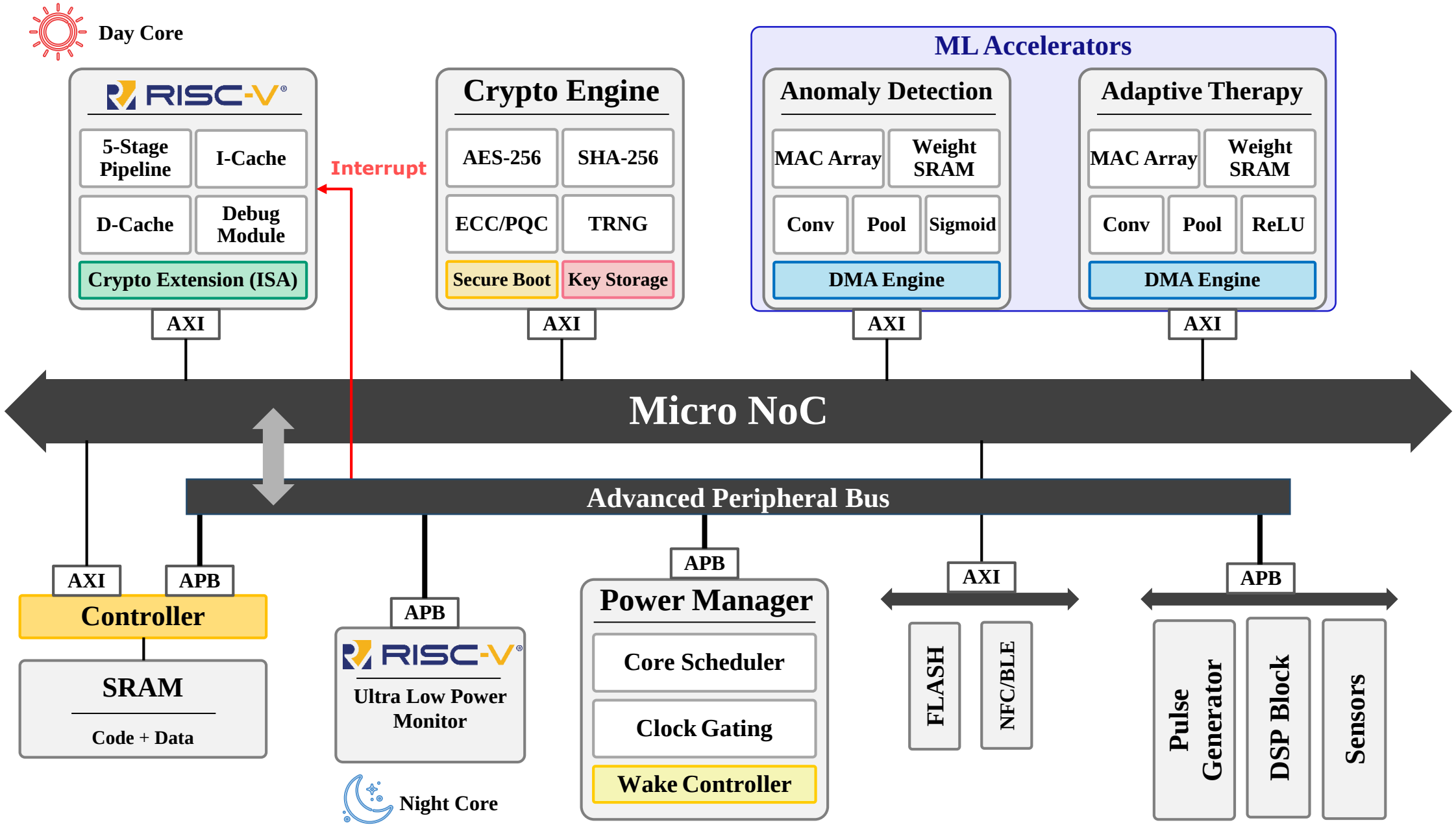
- Firmware updates
- Therapy “recipes”
- RF interface (BT/NFC)
- RF powering and battery

Potential Threat Vectors For Neural Implants

What is **different** than other IMD Security & Privacy?

- Significant amounts of data
- Brain privacy
- Real-time control loops
- Neuro is a new field



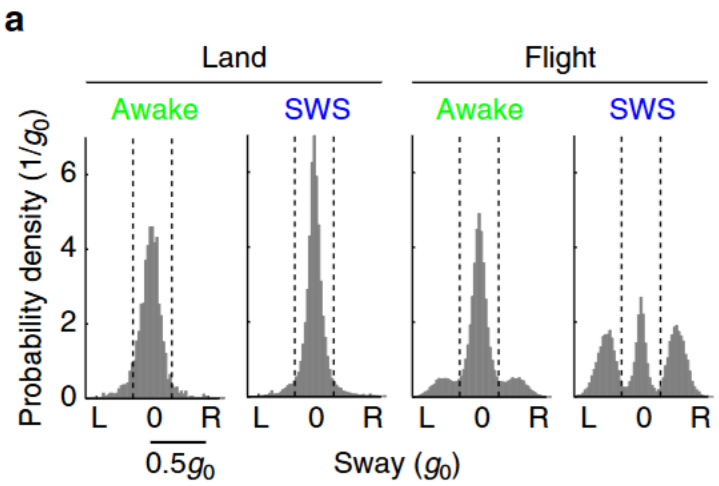

Day Core
RISC-V
5-Stage Pipeline
I-Cache
D-Cache
Debug Module
Crypto Extension (ISA)
Interrupt
Crypto Engine
AES-256
SHA-256
ECC/PQC
TRNG
Secure Boot
Key Storage
ML Accelerators
Anomaly Detection
MAC Array
Weight SRAM
Conv
Pool
Sigmoid
DMA Engine
Adaptive Therapy
MAC Array
Weight SRAM
Conv
Pool
ReLU
DMA Engine
AXI
AXI
AXI
AXI
Micro NoC
Advanced Peripheral Bus
AXI
APB
Controller
SRAM
Code + Data
APB
RISC-V
Ultra Low Power Monitor
Night Core
APB
Power Manager
Core Scheduler
Clock Gating
Wake Controller
AXI
FLASH
NFC/BLE
APB
Pulse Generator
DSP Block
Sensors

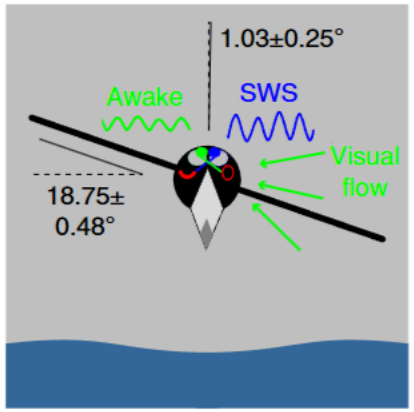
Biological Inspiration for Day/Night Core

Great frigatebirds (Fregata minor)

Unihemispheric slow wave sleep (USWS)

- One cerebral hemisphere exhibits deep slow-wave sleep while the other maintains wakefulness.
- The eye opposite the awake hemisphere remains open for continuous environmental monitoring.
- This state allows marine mammals to maintain voluntary motor control to breathe and avoid drowning.
- The evolutionary adaptation is observed primarily in cetaceans, eared seals, manatees, and birds.
- Sleep drive is regulated independently within each hemisphere by localized neural circuits.





[7] Evidence that birds sleep in mid-flight | Nature 2016 | https://doi.org/10.1038/ncomms12468
[8] https://pmc.ncbi.nlm.nih.gov/articles/PMC4763353/
[9] DOI: 10.1016/s0165-5876(00)00376-1

PQC Communication Enc/Decryption

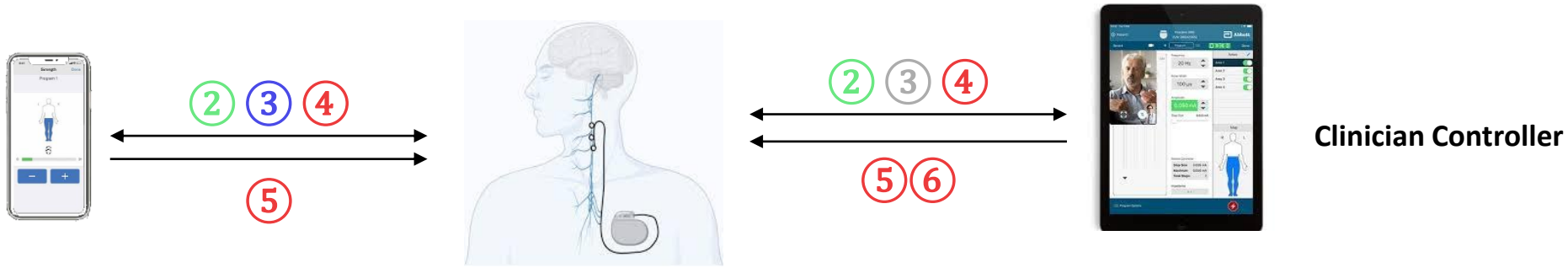
01 Manufacturing Provisioning (KeyGen)

Initial Pairing (Sign + Verify) [Trust Relationship Established] 02

03 Session Establishment (Encaps + Decaps)

AES/ASCON Protected Session (Telemetry | Therapy Commands | Firmware Updates) 04-6

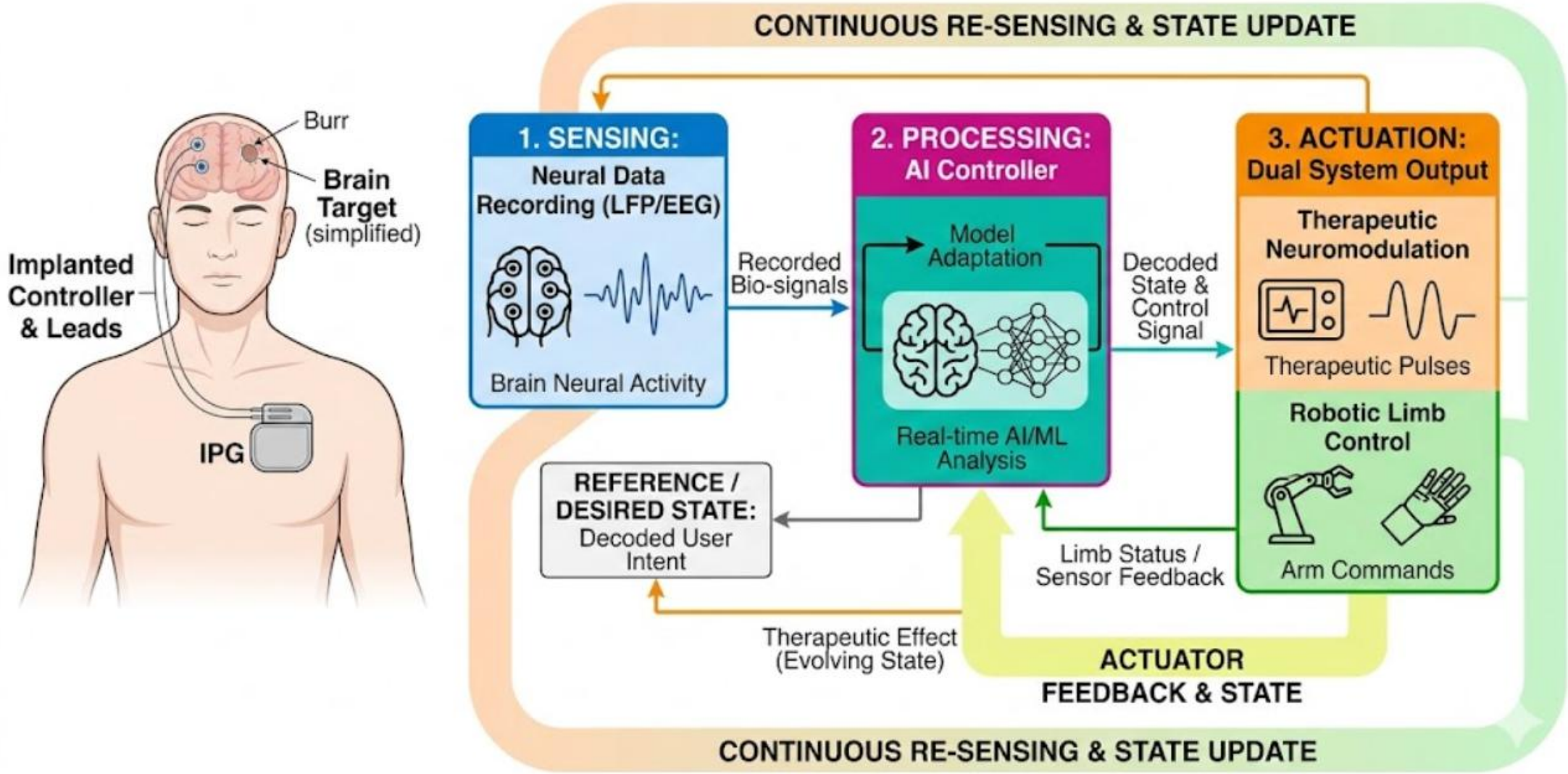
#.	Data Flow	PQC Operation	Symmetric Crypto	Threat if Missing
1	Manufacturing Provisioning	DSA. KeyGen, KEM. KeyGen	-	No Root of Trust/Identity
2	Pairing (New Device, Lost Device)	DSA. Sign, DSA. Verify	-	Fake Controller, Fake Implant, MITM
3	Session Establishment	KEM. Encaps, KEM. Decaps	-	No Secure/Confidential Session
4	Telemetry (Within Session)	-	AES/ASCON	Information Leakage, Telemetry Tampering
5	Therapy Command (Within Session)	-	AES/ASCON	Unauthorized Therapy Change
6	Firmware Update (Within Session)	DSA. Sign, DSA. Verify	AES/ASCON	Malicious Firmware, Rollback Attack



Scenarios: Feature Vs. Component Matrix

	Day CPU	Night CPU	Anomaly Detection	Therapy	Crypto	DSP Block	Sensors	Pulse Generator	SRAM	Flash	NFC/ BLE
Anomaly Detection	✓	✓	✓			✓	✓		✓		
Therapy Update	✓	✓		✓	✓	✓		✓	✓		
Physiological Alarms	✓	✓		✓		✓	✓			✓	✓
Model Update	✓		✓		✓	✓			✓	✓	✓
Firmware Update	✓	✓			✓			✓	✓	✓	✓
Credential Update	✓				✓				✓	✓	✓
Safe Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Data Upload	✓				✓	✓			✓	✓	✓

Closed-loop Control



Google Gemini, Nano Banana Pro 2026

Efficient and Secure AI at the Edge: Two Tales
Overall Takeaways

- Fully Analog VLSI for RF Neural ML Classification
  - Analog imprecision is ok for soft compute like ML
  - Dense and precise memristors allow fast and low-power VMM
  - Fully analog is enabled by novel amplifier designs
  - New threat models to protect model IP and analog compute
  - Remaing challenges: VLSI, CMOS Manufacturing, Test, AI Accuracy…
- Neuro devices enable therapies for numerous neuro diseases
  - Alternative to pharmacological solutions
  - New threat models due to Brain wave sensing and neuro-stimulation
  - RISC-V MPSoC with AI accelerators and Post-quantum Crypto
  - Remaining challenges: Community acceptance, full life-cycle, AI safety…