力旺電子 Briefing

智慧財產權聲明.

eMemory: Embedded NVM with Logic Process

Part 1. The Core Concept

Volatile Memory
(e.g., RAM)

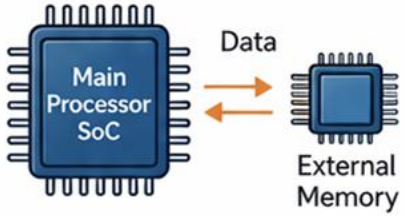
Power Off
Data Lost

Non-Volatile Memory
(e.g., Flash/Storage)

Power Off
Data Stays

2. eNVM vs. External Memory

External Memory



Slower, Higher Power

Embedded NVM (eNVM)

Faster, More Efficient, Saves Space

Part 2: What eMemory Does

Logic-Compatible eNVM IP

License IPs to Foundries and Chip Designers
Key: Enables eNVM in standard logic processes, **WITHOUT** extra costly steps.
(Cost-Effective, Scalable)

Part 3: Key Technology Types

1. ONE-TIME PROGRAMMABLE (OTP)

NeoBit (8-inch)
NeoFuse (12-inch)

Key Uses:
- Memory repair for DRAM/ SRAM
- Image sensor recovery
- Analog circuits trimming

2. MULTIPLE-TIME PROGRAMMABLE (MTP)

NeoFlash
NeoMTP
NeoEE
Embedded ReRAM
ASIC Memory

Key Uses:
- Firmware Updates
- Data Logging
- Flexible Product Configuration

Part 4: Advanced Security

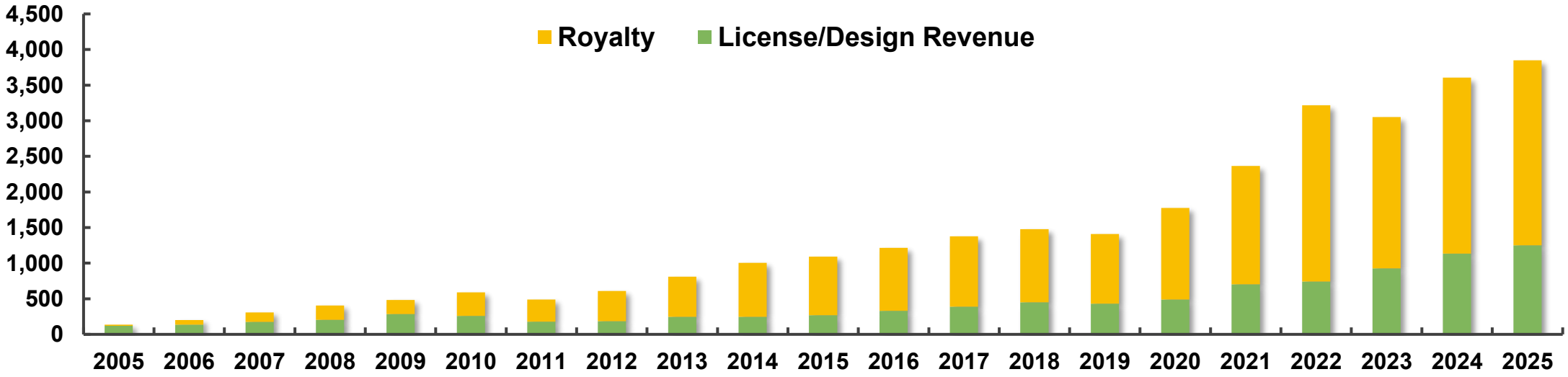
Anti-Fuse Technology (OTP)
Permanent, difficult-to-tamper connection (better than standard fuse). Highest security.

NeoPUF (Physical Unclonable Function)
Uses unique microscopic variations to generate keys ON-DEMAND, not stored. Ultimate root of trust.

Company Overview

- eMemory leads the global market in **Logic NVM and PUF-Based Security IPs**.

Revenue Trend
(Unit: NT$ in Million)



77M+
Cumulative Wafers Shipped
Spanning 756 production processes from 0.5μm to 2nm, and 2.6M wafers (8″-equivalent) shipped in 2026 Q1.

1360+
Patents Issued
Expanding our IP footprint with 225 pending patents, driven by a 338-member team with 72% R&D focus.

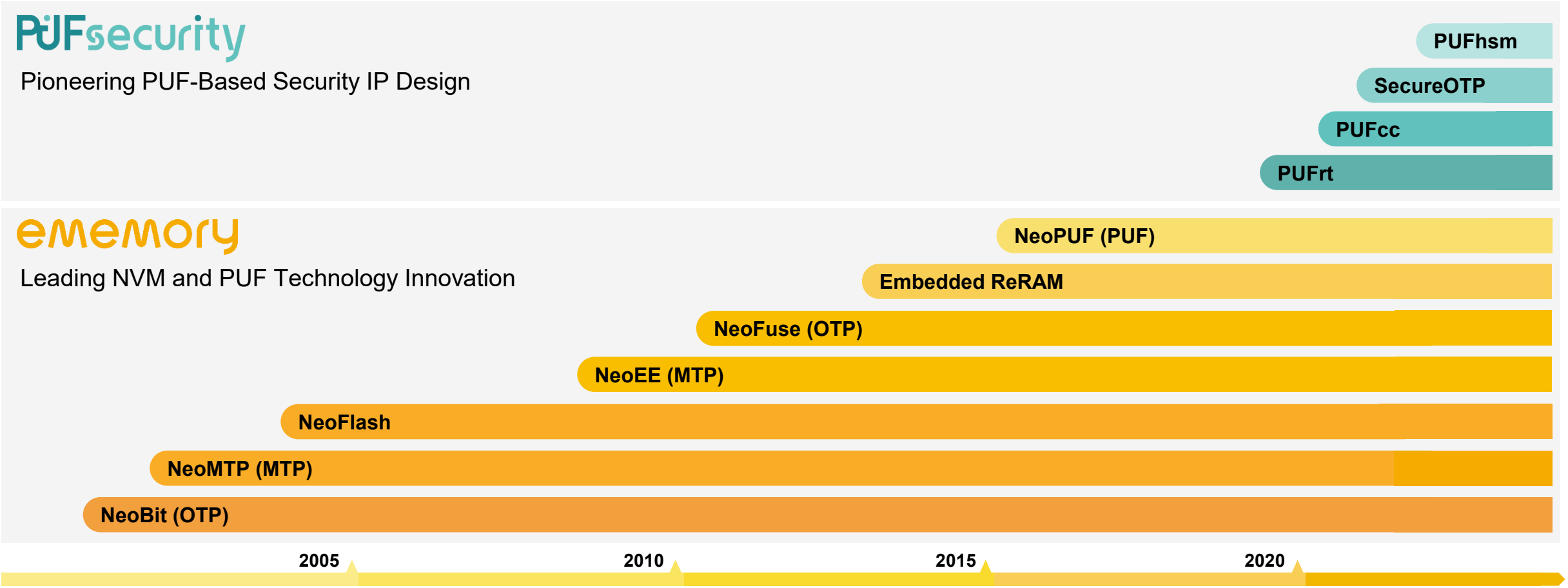
16-Year
Best IP Partner with TSMC
Founded in 2000 and IPO in 2011. Recognized as TSMC's Best IP Partner every year since 2010.

Technology Portfolio

- eMemory's IP portfolio is built on two pillars: **OTP** as the foundation and **MTP** for scalable integration.

PUFsecurity

Pioneering PUF-Based Security IP Design



Leading NVM and PUF Technology Innovation

One-Time Programmable (OTP) Memory

- eMemory advances silicon security from foundational OTP to **next-gen NeoPUF-Based solutions**.

OTP
- **NeoBit** (8″ Wafer Processes)
- **NeoFuse** (12″ Wafer Processes)

PUF
- **NeoPUF**
- **PUFrt**
- **SecureOTP**

Crypto -processors
- **PUFcc**
- **PUFhsm**

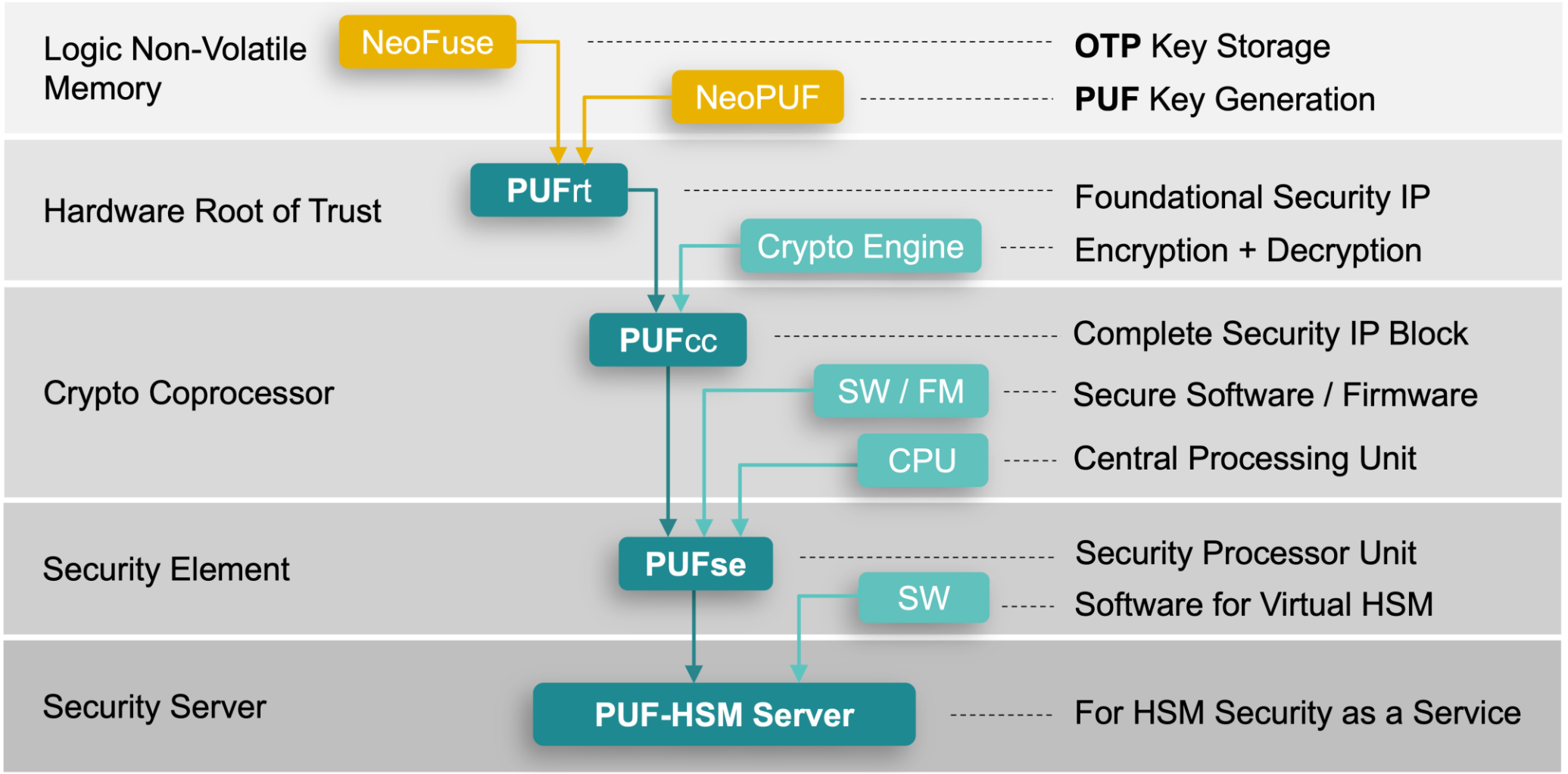
Cryptography
- **RSA**
- **ECC**
- **AES**
- **SHA**
- **PQC**
- **etc.**

Yield Enhancement
- Memory repair for DRAM/SRAM
- Image sensor recovery
- Analog circuits trimming

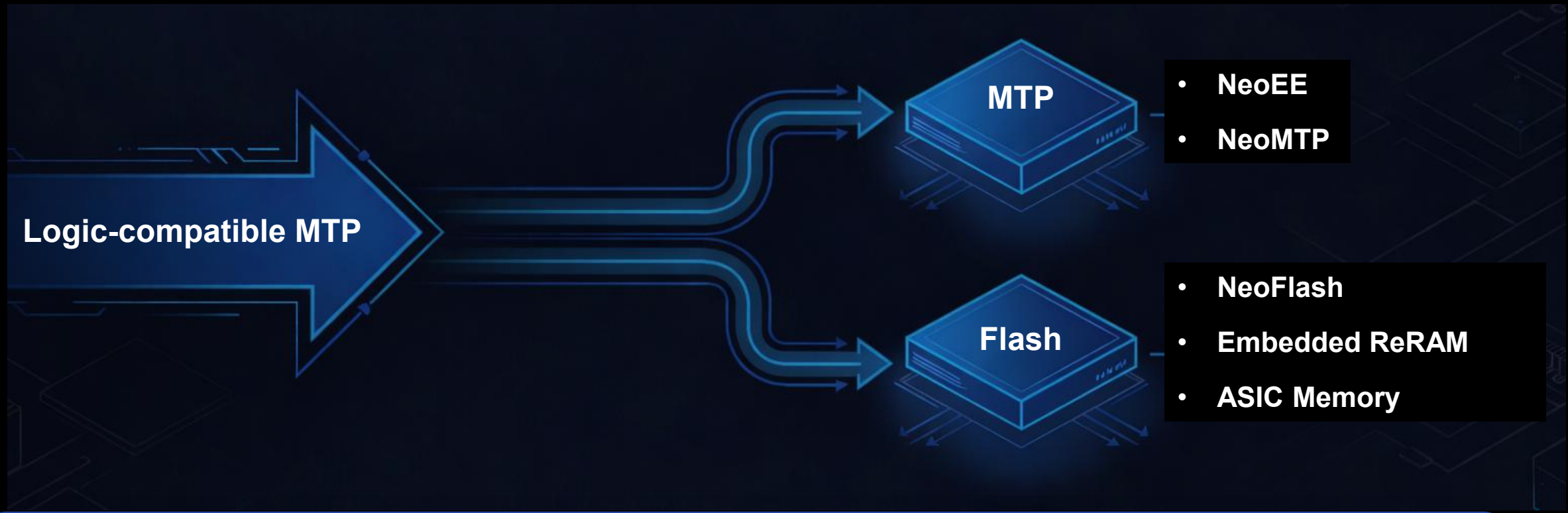
Fundamental Security
- Hardware root-of-trust
- Unalterable key storage
- Silicon-level identity protection

Evolution from OTP to PUF-HSM

- eMemory evolves from OTP technology into integrated **PUF-based security subsystem**.



Multiple-Time Programmable (MTP) Memory

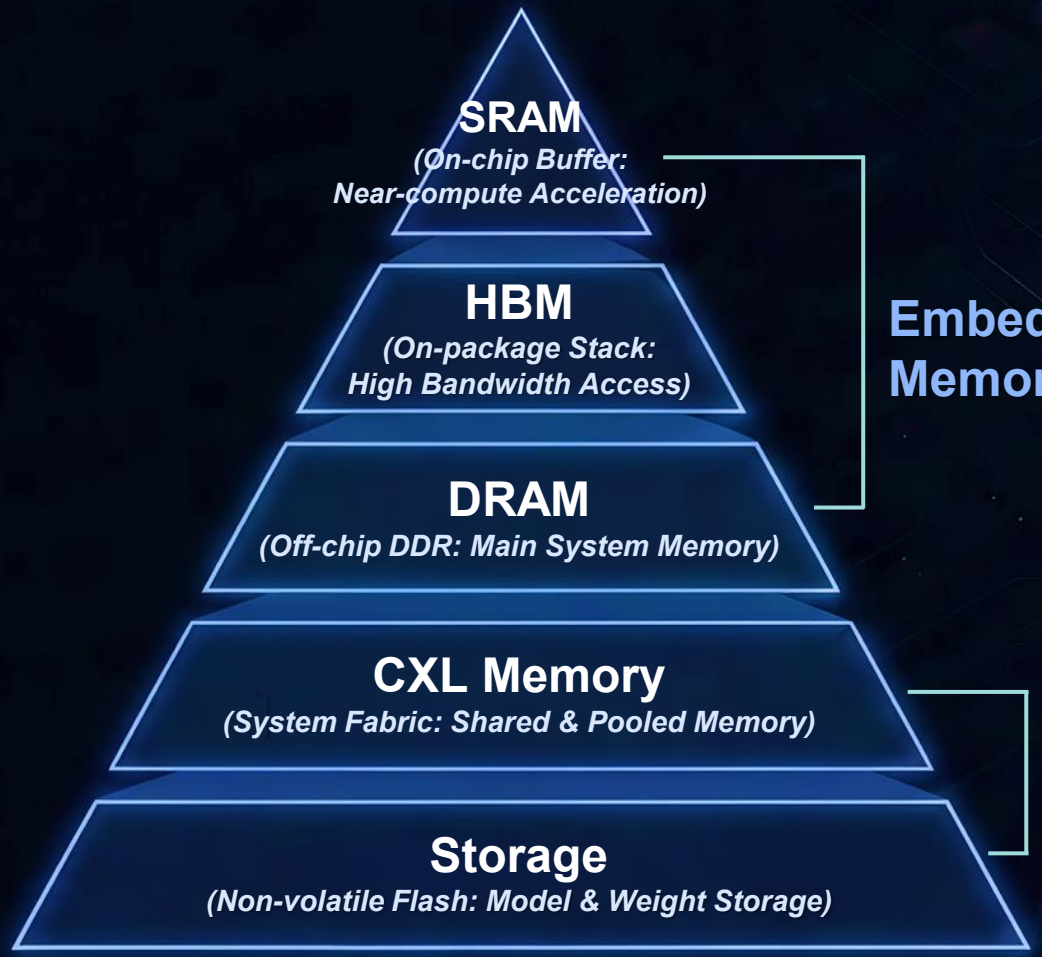


Density Variety
- Scalable storage configurations
- Optimized silicon footprint
- Versatile capacity range (Bits to Mb)

High Endurance
- Optimized write/erase cycles
- Enhanced data retention reliability
- Extended application operational lifespan

Process Integration
- Seamless standard logic embedding
- Foundry-ready ASIC integration
- Zero-mask overhead implementation

eMemory Enabling AI Memory Systems



High Yield, Low Cost

- **OTP Repair:** Enhances SRAM/HBM/DRAM production yield
- **MTP Configuration:** Optimizes updateable DDR5/SOCAMM DIMMs
- **Cost Reduction:** Enables cost-effective AI chip mass production

High Reliability

- **Repair Integration:** Ensures HBM stack and DRAM integrity
- **Data Retention:** Guarantees long-term stability via OTP redundancy
- **Workload Stability:** Supports operational uptime under extreme AI tasks

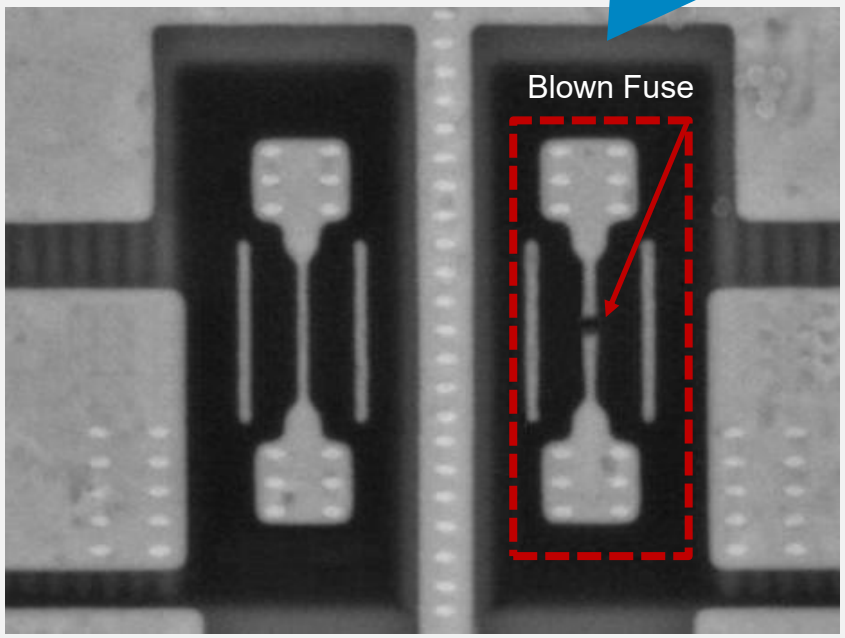
High Security

- **PUF-Based Root of Trust:** Establishes hardware-anchored trust foundation
- **Secure Transmission:** Protects data integrity across CXL memory pools
- **Storage Protection:** Safeguards AI models within NVMe/SSD controllers

Anti-Fuse OTP vs. e-Fuse

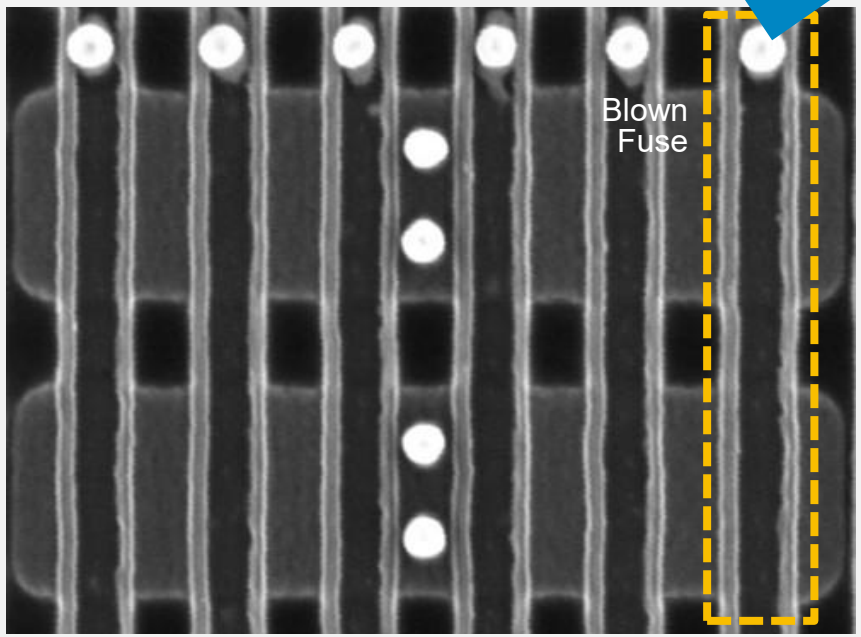
e-Fuse

Physically Visible: Vulnerable to Reverse Engineering



Anti-Fuse OTP (NeoFuse)

Physically Invisible: Resistant to Physical Attacks

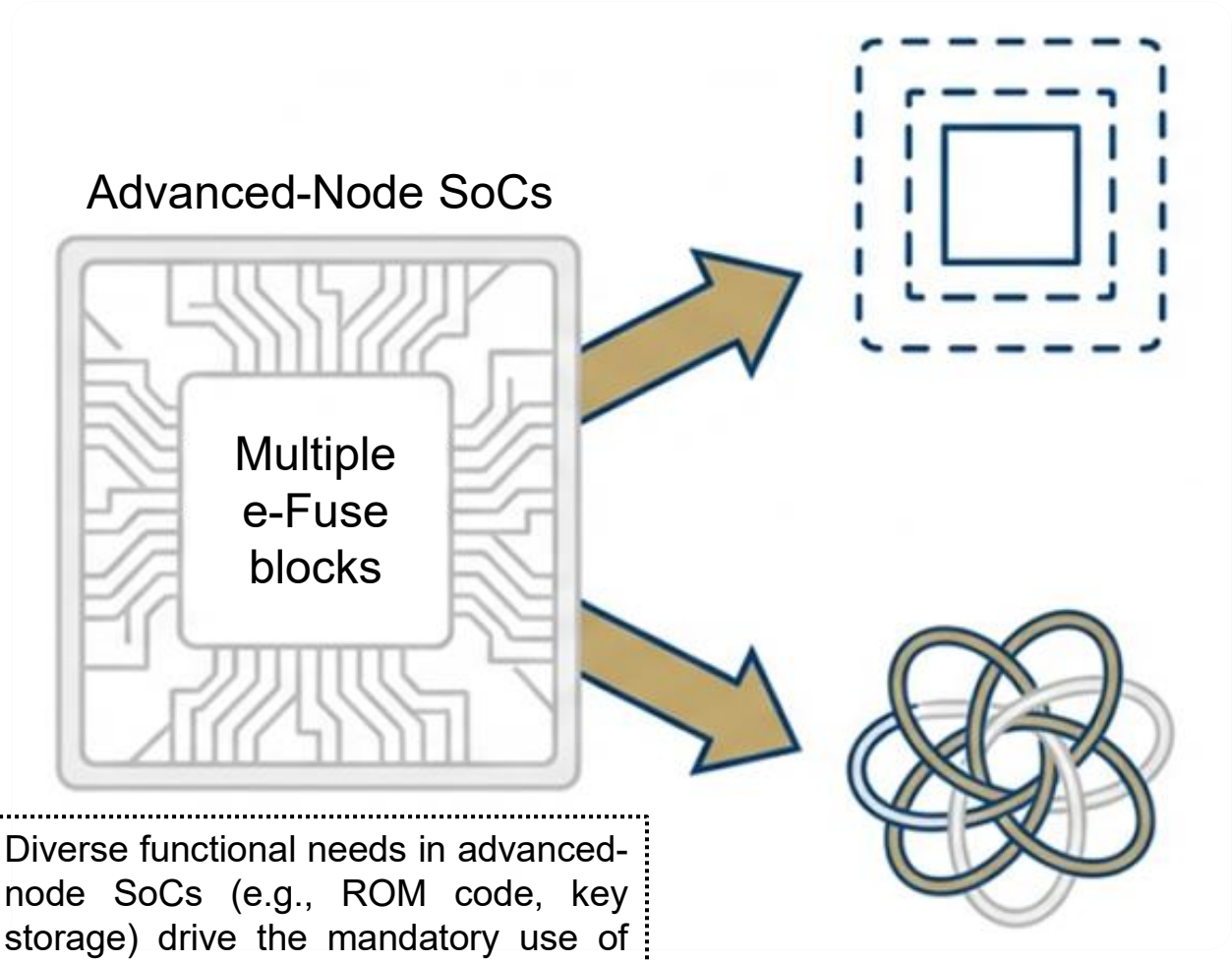


- Display Driver
- PMIC
- Sensor IC
- Camera
- MCU
- Multi-Media
- Automotive
- RFID Tag
- DRAM
- Connectivity

Arm RSS (Runtime Security Subsystem) Endorsement

- **Field-Programmable RSS Support:** Enables secure storage of confidential code and data within the Runtime Security Subsystem.
- **High-Density Efficiency:** Optimizes area for large arrays with seamless, low-overhead PUF integration.

e-Fuse Bottlenecks



Diverse functional needs in advanced-node SoCs (e.g., ROM code, key storage) drive the mandatory use of multiple e-Fuse blocks.

Area Overhead

Mandatory SRAM buffering **doubles the memory footprint** due to read limitations.

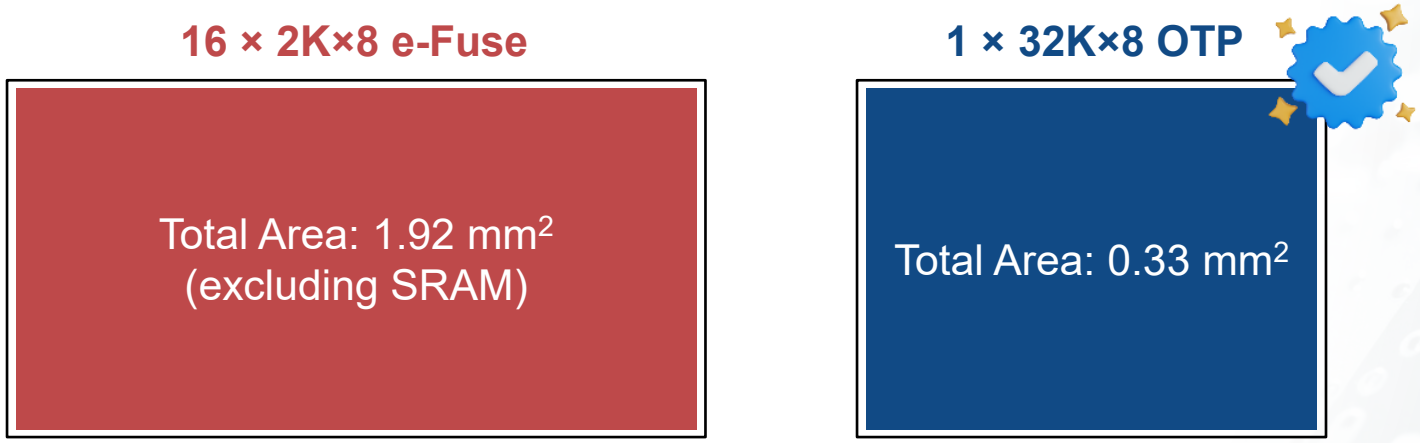
Design Complexity

Scattered multiple e-Fuse block layouts trigger **severe routing and power grid challenges**.

OTP Area Efficiency

- eMemory's OTP outperforms e-Fuse in area efficiency **beyond 4K×8 densities**.

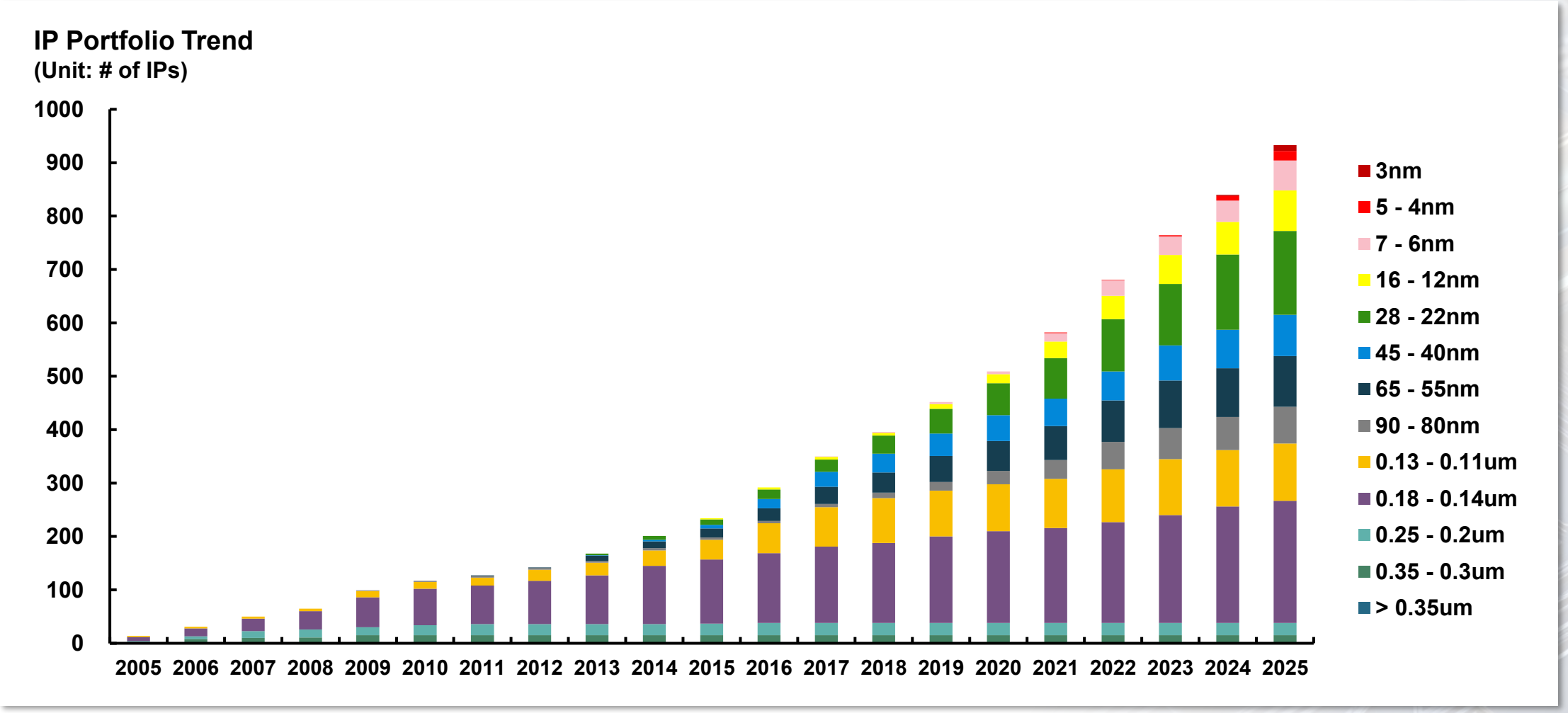
Example:
32K x 8 Density



Item	e-Fuse Solution	OTP Solution	OTP Advantages
Number of Macros	16 Macros	1 Macro	**Single-macro simplicity**
Total Area	~1.92 mm²	0.33 mm²	**>80% Area reduction**
Additional SRAM	Required	Not required	**Zero buffer SRAM requirement**
Design Effort	High (Scattered)	Low (Centralized)	**Simplified layout & routing**

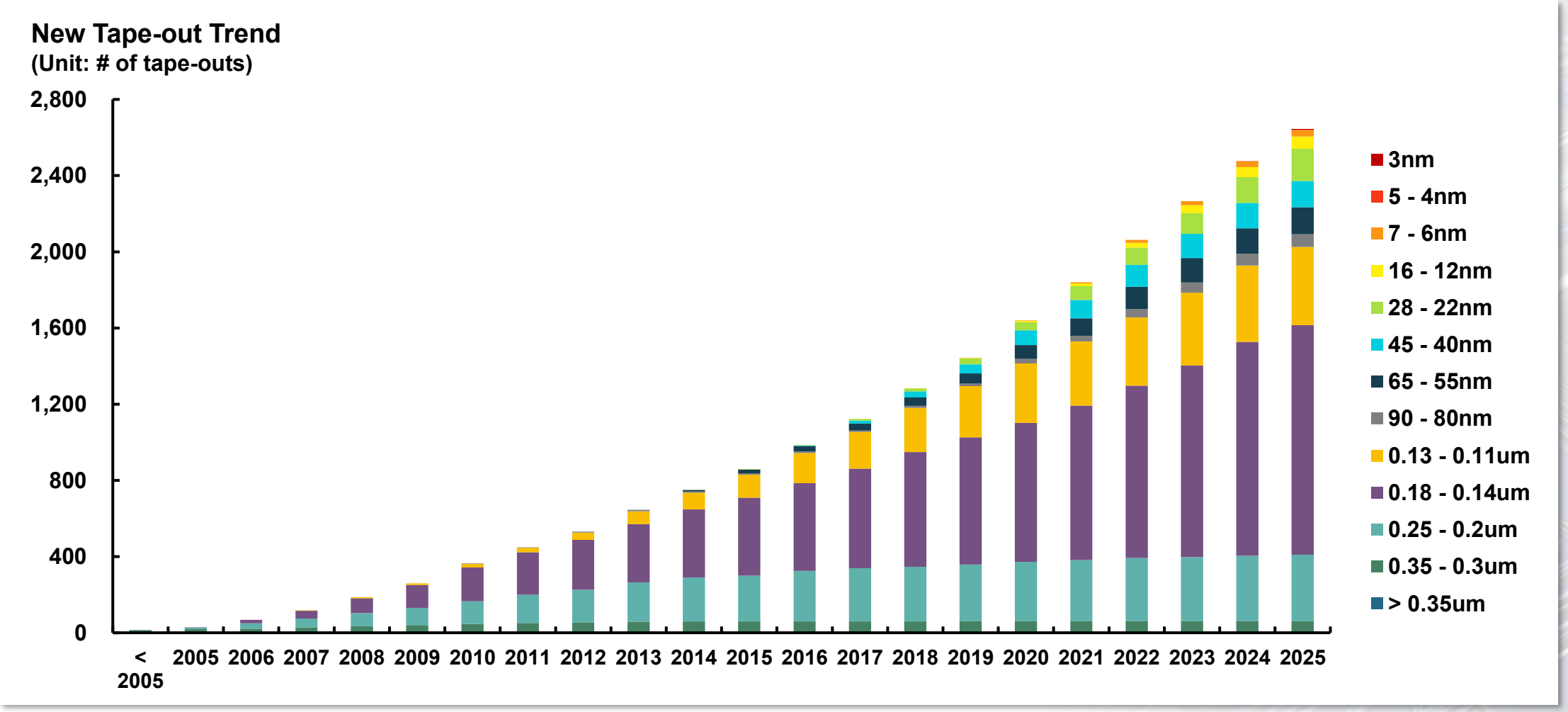
Registered IPs at TSMC

- eMemory integrates widely across TSMC process nodes with **over 850 registered IPs** to enable broad customer adoption.



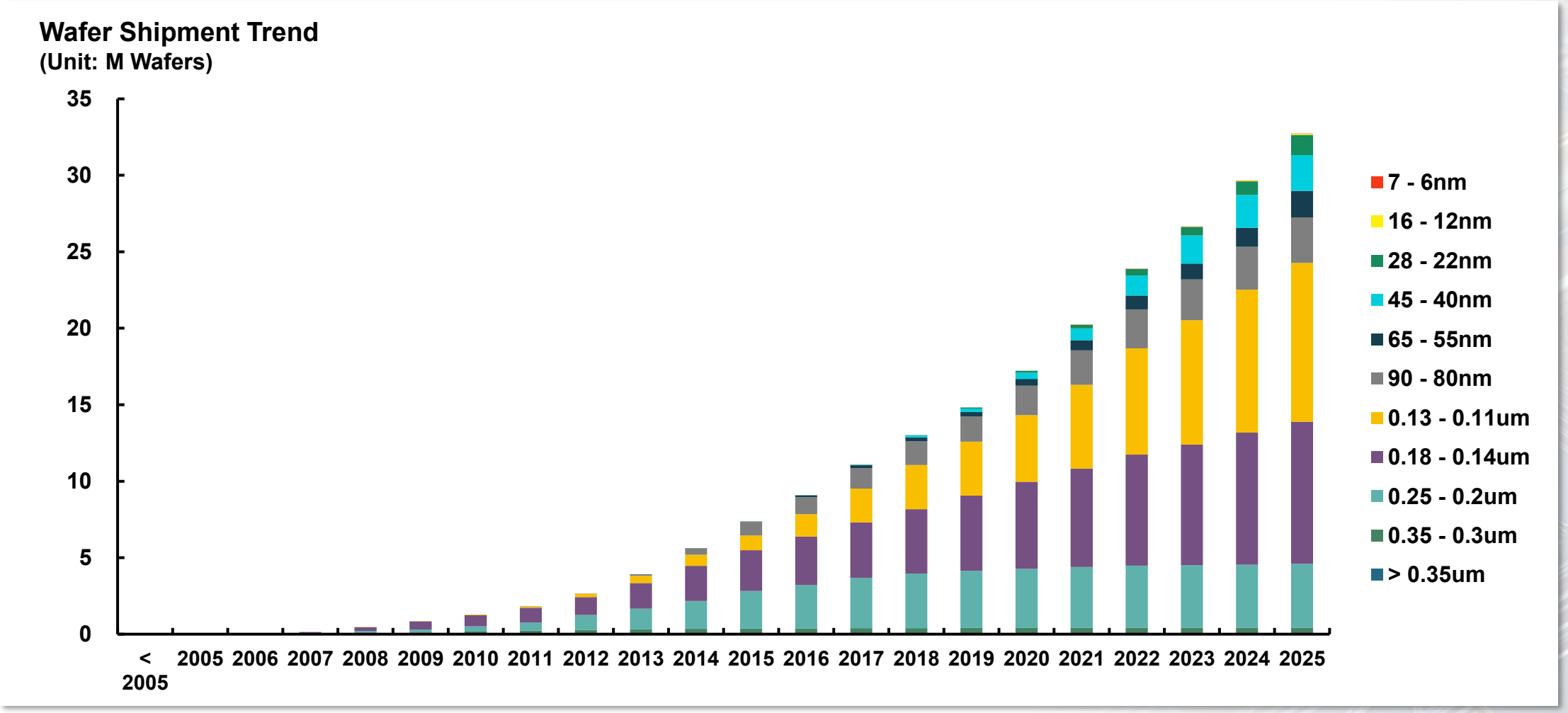
New Tape-Outs at TSMC

- eMemory secures continuous success with **over 2,600 new tape-outs (NTOs)** across all leading-edge and mature process nodes.



Wafer Shipment at TSMC

- eMemory translates **over 25M wafer shipments (8″-equivalent)** into recurring royalty revenue with long-term visibility.



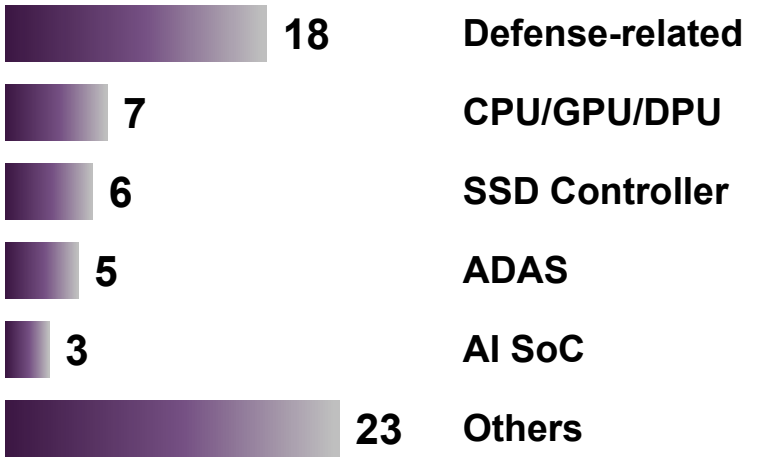
Accumulated Advanced-Node Licensed NTOs

- eMemory secures future growth with **over 140 advanced-node tape-out licenses**, building a high-value royalty pipeline driven by increasing adoption.

Leading-Edge Nodes (3nm–7nm)

62 TOTAL TAPE-OUTS

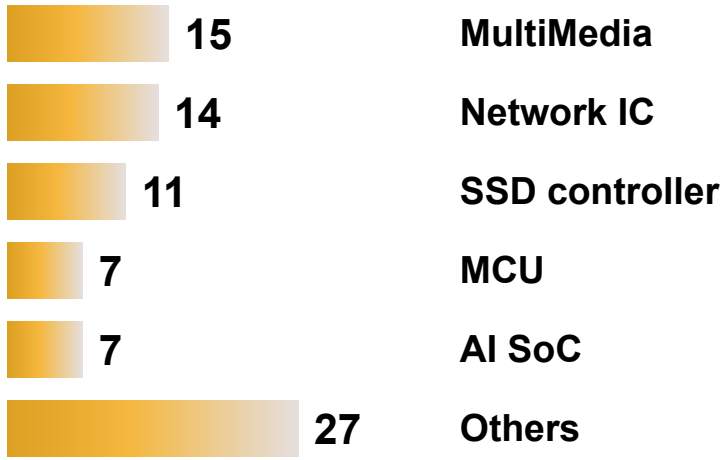
Driven primarily by AI and Advanced System-on-Chip (SoC) technologies.



Mainstream Advanced Nodes (12nm/16nm)

81 TOTAL TAPE-OUTS

Driven by demand in High-end Multimedia Processing and Networking sectors.



Tape-outs and Revenue by Technology

	NTO			Revenue (USD)		
Year	NeoBit	NeoFuse	PUF-Based	NeoBit	NeoFuse	PUF-Based
2002	3					
2003	29					
2004	40					
2005	68			$ 4,217,380		
2006	133			$ 6,202,270		
2007	220			$ 9,402,479		
2008	253			$ 12,896,211		
2009	268			$ 11,695,587		
2010	284			$ 15,873,331		
2011	254			$ 15,399,098		
2012	270			$ 19,620,768		
2013	363	1		$ 25,436,669	$ 382,084	
2014	371	3		$ 31,831,985	$ 328,787	
2015	311	11		$ 30,943,426	$ 1,080,373	
2016	270	28		$ 30,247,340	$ 3,636,142	
2017	257	61		$ 34,619,653	$ 5,238,351	
2018	253	86	1	$ 31,834,860	$ 10,773,223	$ 85,000
2019	226	109	2	$ 27,602,332	$ 14,466,279	$ 195,000
2020	248	182	3	$ 30,378,346	$ 26,437,660	$ 434,998
2021	252	259	6	$ 32,367,560	$ 44,011,223	$ 1,160,702
2022	264	231	33	$ 35,327,060	$ 63,762,480	$ 4,207,348
2023	226	241	29	$ 23,251,721	$ 64,276,058	$ 4,375,409
2024	266	270	32	$ 25,952,137	$ 71,649,123	$ 5,279,985
2025	253	248	54	$ 27,312,244	$ 78,122,682	$ 7,645,293
Total	**5,382**	**1,730**	**160**	**$ 482,412,457**	**$ 384,164,465**	**$ 23,383,735**

*Revenue includes both **licensing** and **royalty**

Hardware Root of Trust (HRoT)

- eMemory provides the **foundational Hardware Root of Trust** that secures the entire software stack throughout the chip's lifespan.

Software Security Stack
- **Core Function:** Dynamic adaptation to new threats
- **Key Attribute:** Continuous evolution

Hardware Root of Trust
- **Core Function:** Foundational trust for software
- **Key Attribute:** Immutable permanence

Security Business Development

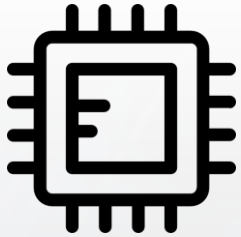
- eMemory drives security IP adoption by collaborating with **leading foundry, processor, and cloud service providers.**

Foundry Platforms

TSMC, Intel, UMC, GF, etc.

- **Technology Licensing:** Providing security IPs to leading global foundries.
- **Co-marketing Activities:** Reaching diverse customer bases through joint promotional efforts.

CPU Partners



Arm, RISC-V, Cadence, etc.

- **System Integration:** Addressing SoC customer needs for pre-integrated CPU and security subsystems.
- **Architectural Alignment:** Collaborating with major processor providers like Arm and RISC-V.

Cloud Service Providers (CSPs)

Microsoft, Meta, Google, Amazon, etc.

- **Hardware-to-Cloud Security:** Working with CSPs on embedded security requirements at the chip level.
- **Root of Trust Solutions:** Developing foundational security for systems like AWS, Meta, and Azure.

Standards Drive Hardware-Based Security

Driving an open standard for silicon root of trust.

Using asymmetric public/private key encryption technology and device ID to achieve fast and secure access to the network.

Caliptra Open-Source HRoT

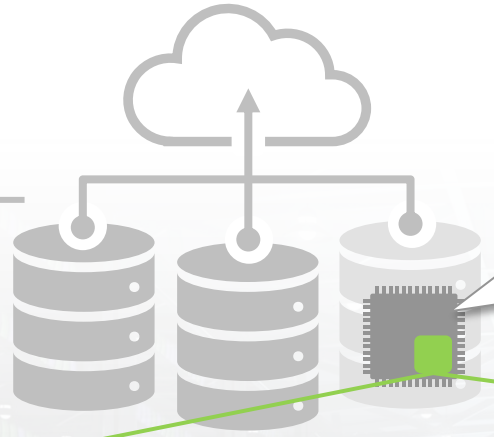
- eMemory's **Root of Trust IP is fully ready to** meet the hardware security requirements of the **Caliptra specification.**

OPEN Compute Project

Project Start
Sep-21

Caliptra 1.0
Mar-24

Caliptra 2.0 (+PQC)
Oct-24



Caliptra-compliant IPs are designed to be integrated into a wide range of high-performance **Data Center and Edge components**:

- **Compute:** CPUs, GPUs (Accelerators)
- **Storage:** SSD Controllers
- **Networking:** NICs (Network Interface Cards), SmartNICs, DPU
- **Custom Silicon:** ASICs, SoCs

Caliptra HRoT 1.0 » **Caliptra HRoT 2.0**

eMemory IP Portfolio

- OTP
- TRNG
- PUF
- Crypto-processors
- Cryptography (PQC)

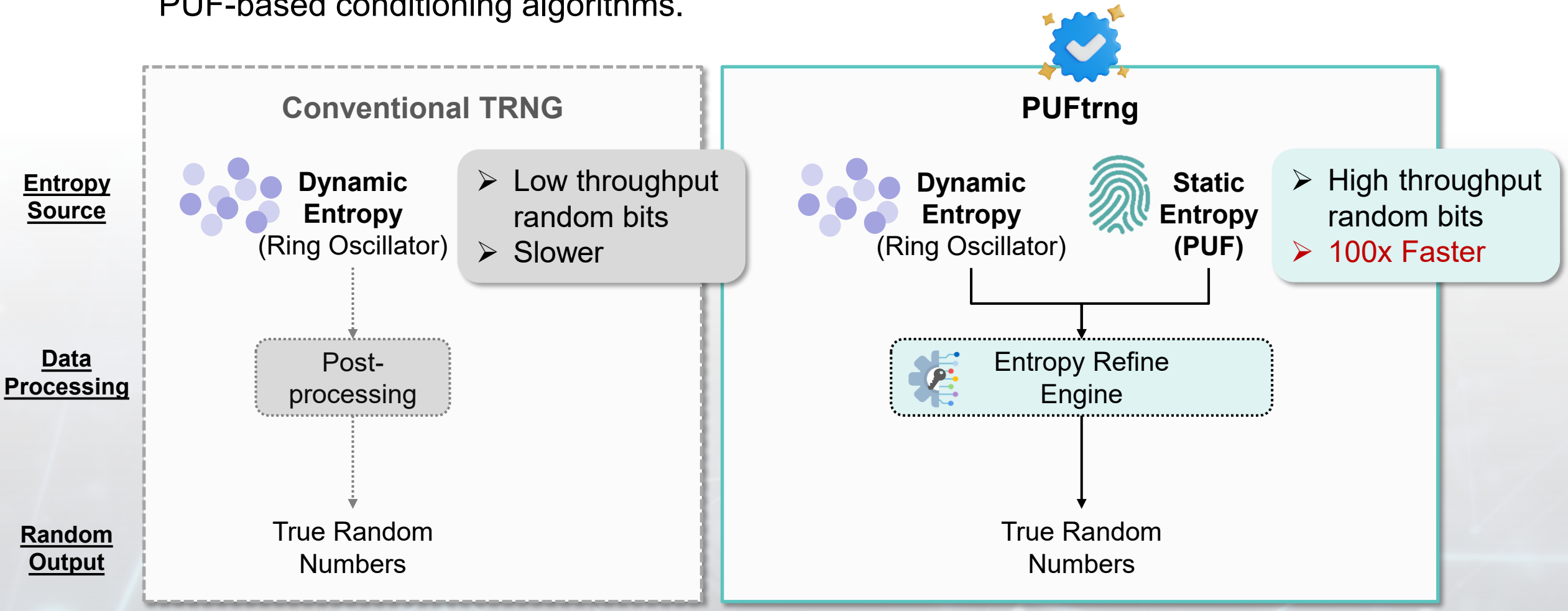
eMemory

Core Security Capabilities:

- Unique Chip Identity
- Secure Attestation
- Secure Boot

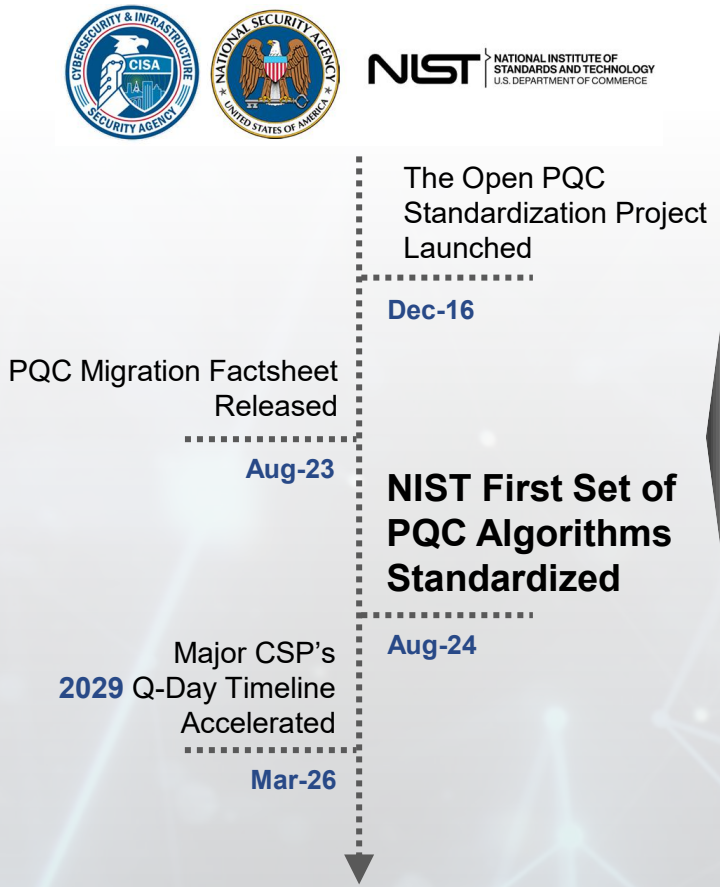
True Random Number Generator (TRNG)

- eMemory's **PUFtrng** delivers **100x faster performance** and superior entropy quality via PUF-based conditioning algorithms.



Post-Quantum Cryptography (PQC)

- eMemory provides **NIST-compliant hardware foundations** to secure data against future quantum computing threats.

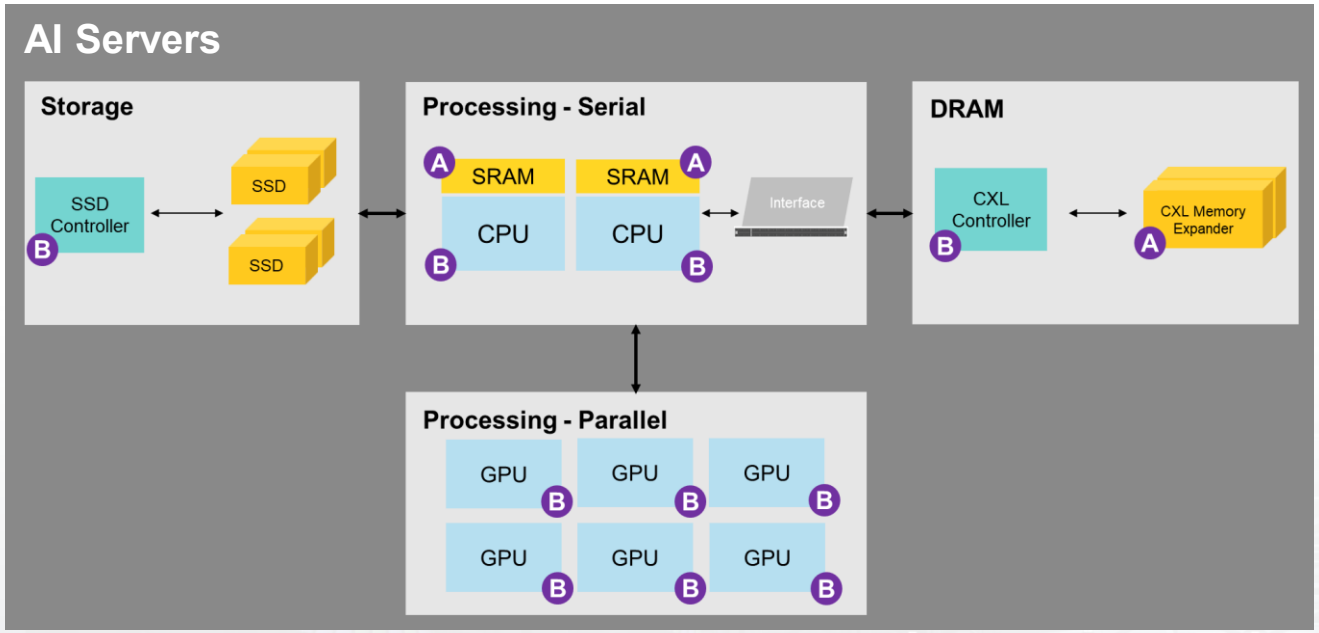


Quantum Threat: Conventional RSA and ECC encryption are vulnerable to future Shor's algorithm attacks by quantum computers.

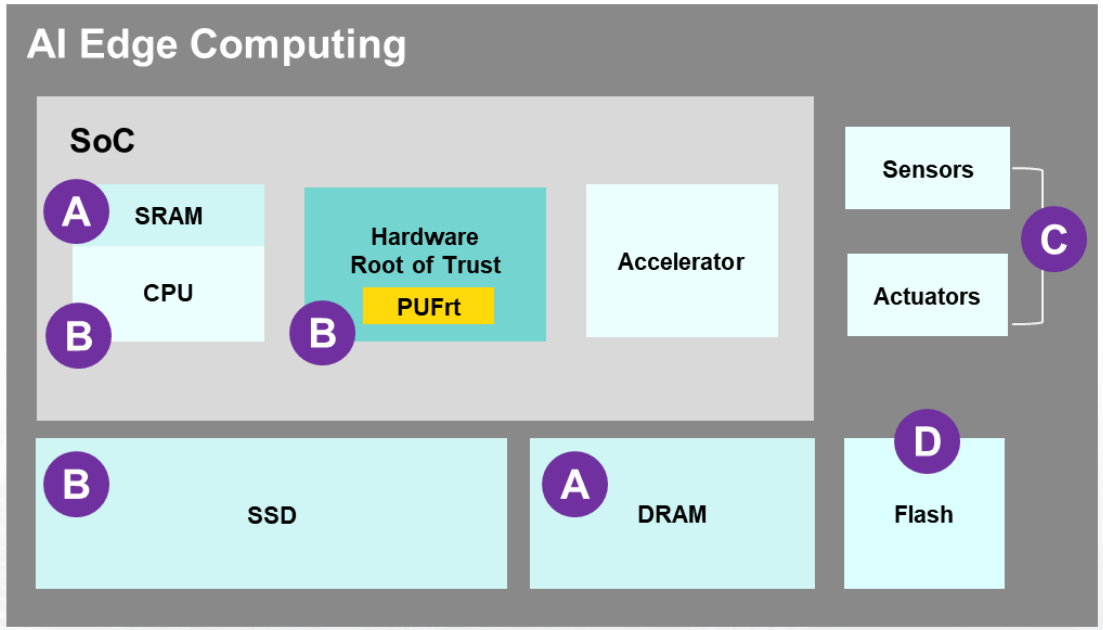
NIST Standards: Official FIPS 203/204/205 and SP 800-208 define the mandatory PQC baseline for global industries.

eMemory Achievements: Our PUF$_{PQC}$ attains **full NIST coverage**, securing the chain of trust from physical PUF to PQC algorithms.

eMemory for AI Servers and Edge Devices



+



A **Memory Repair**

B **Root of Trust** provides:

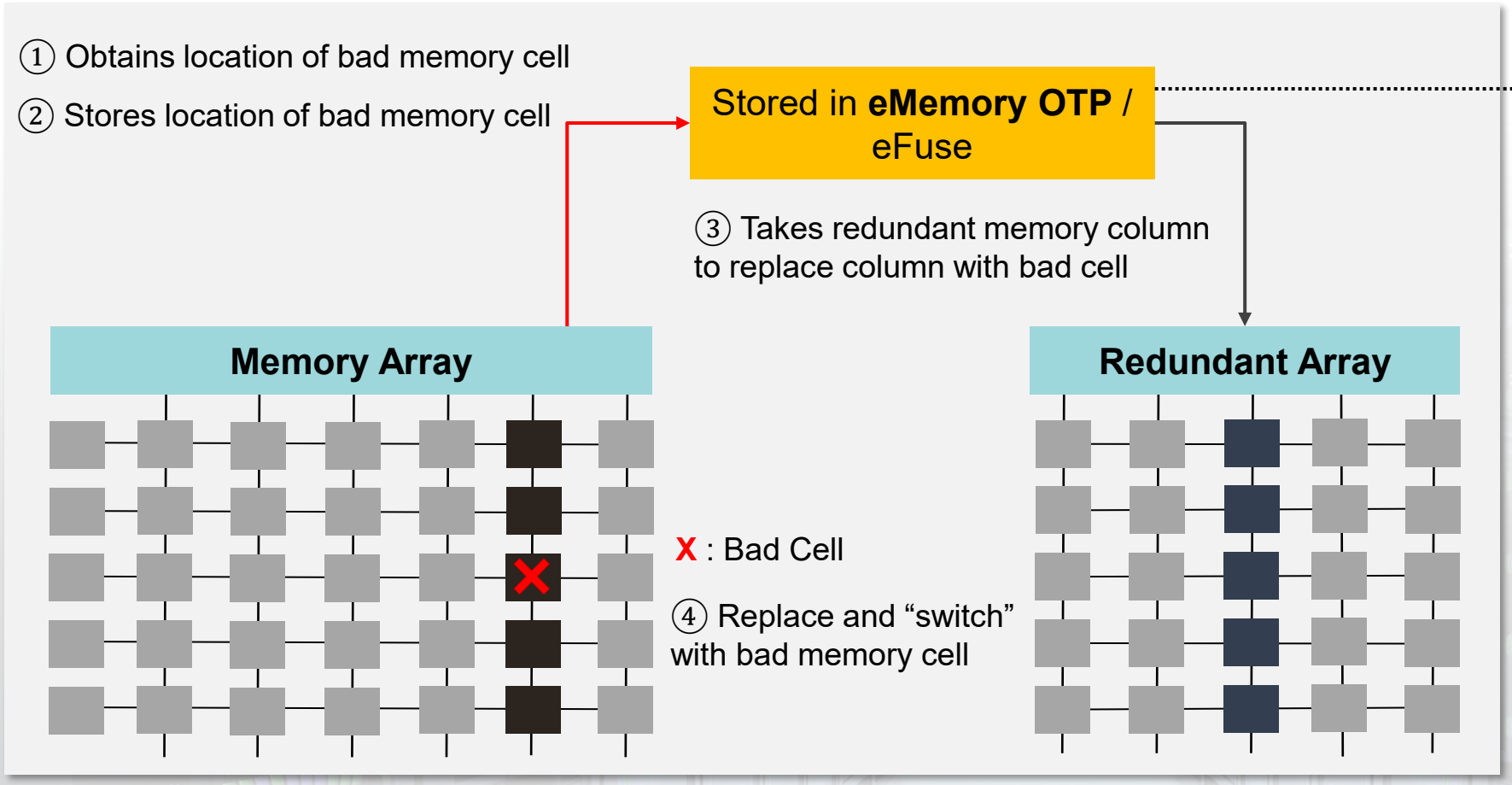
1. Key storage/generation
2. Cryptographic processing to protect AI models, input data and output results
3. Confidential Computing

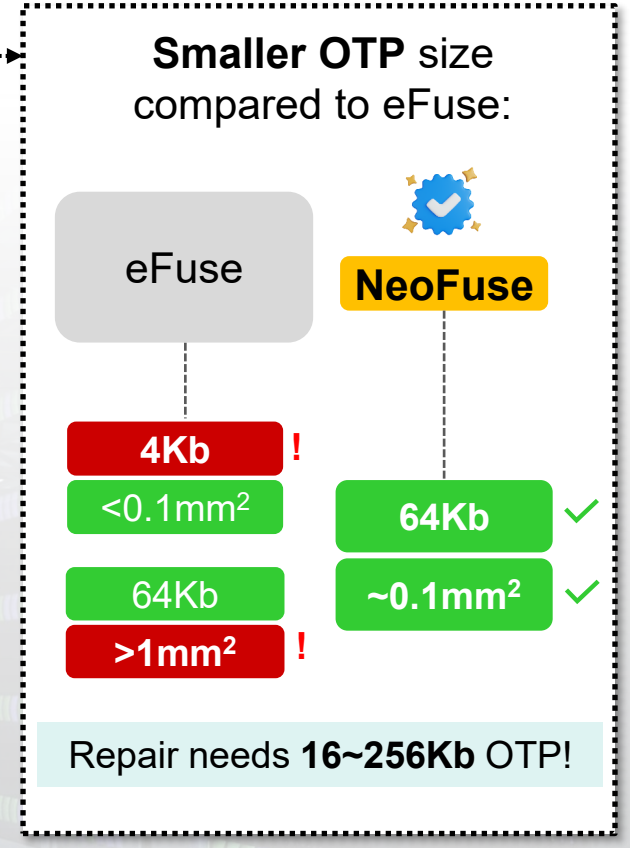
C **OTP** needed for trimming analog circuits in Sensors and Actuators

D **NeoFlash** to replace conventional eFlash for a much lower cost

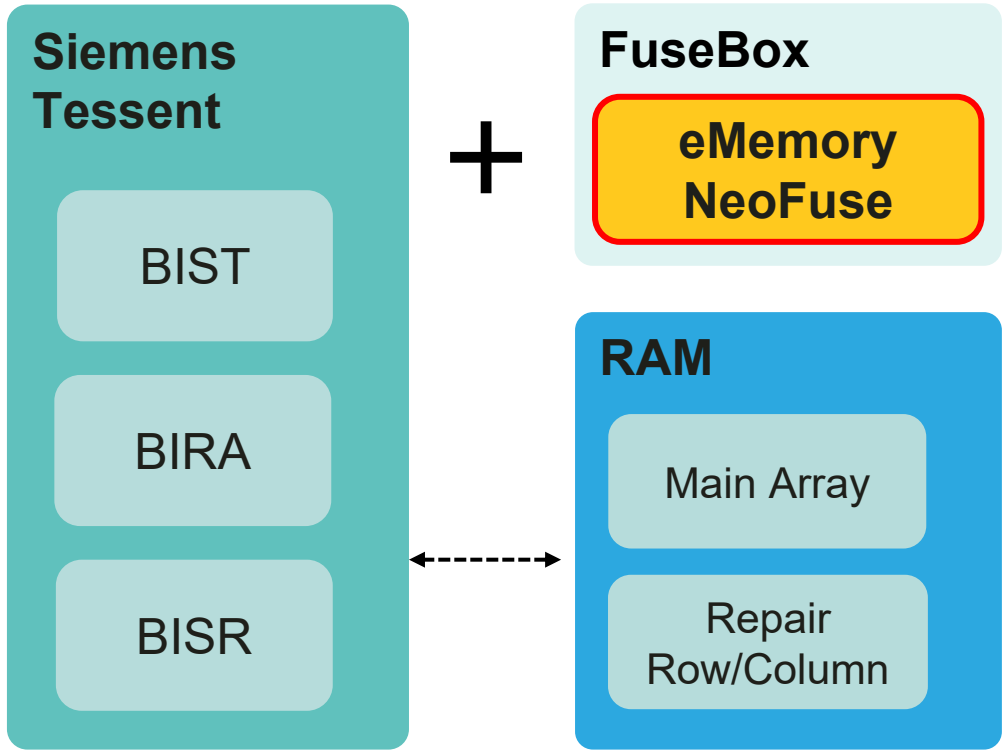
eMemory enables High-Yielding SRAM

- eMemory's OTP enables high-density SRAM Repair, addressing scaling challenges at advanced nodes.





eMemory and Siemens: Partnering for Success



BIST = Built-in Self Test
BIRA = Built-In Redundancy Analysis
BISR = Memory Built-in Self Repair

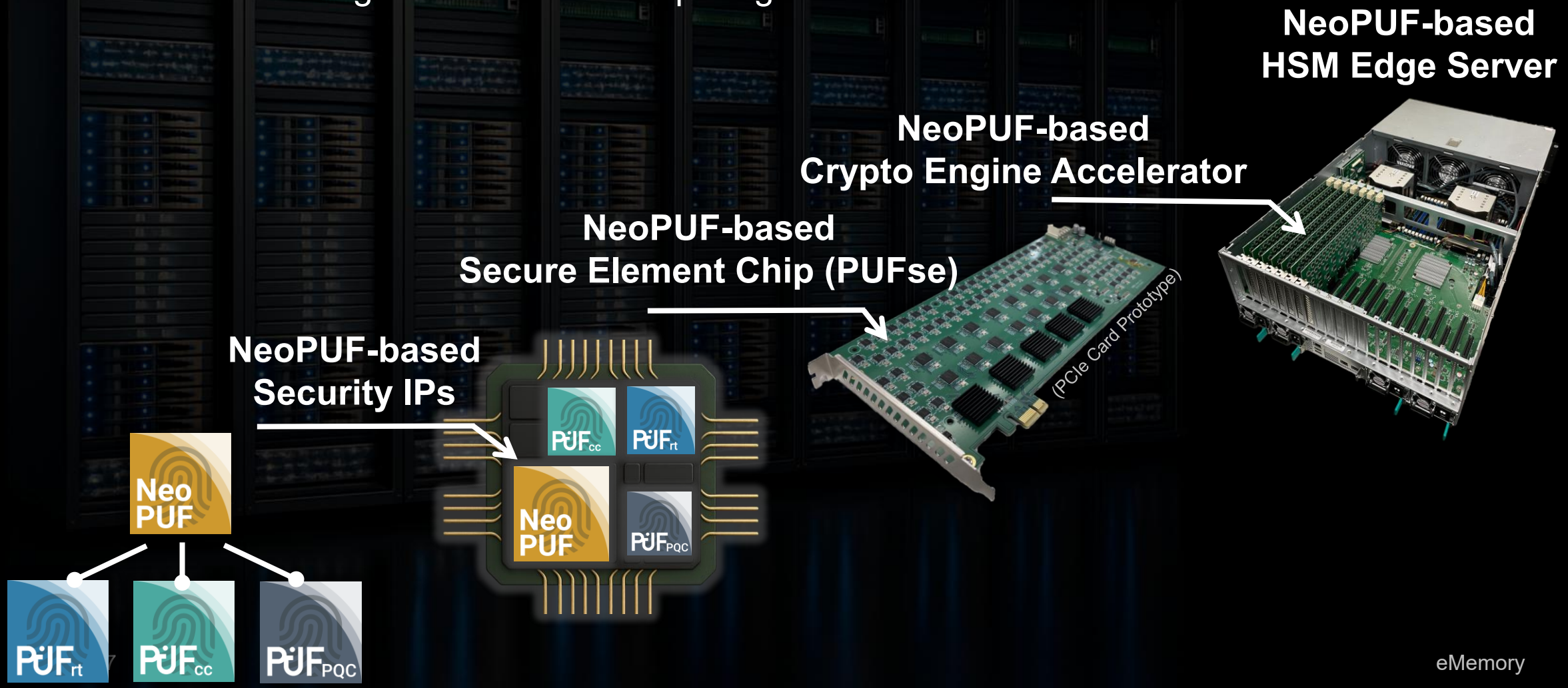
eMemory provides OTP with interface for Siemens MBIST:

- **Tessent** provides memory BISR functions with BIST and BIRA
- **NeoFuse OTP** provides defect-free OTP using BIRA, BISR and adapter to Tessent
- **New MBISR**: Tessent MBISR + NeoFuse, scanning defective SRAM by word/column and logging to the OTP

1. **Compact**
2. **Flexible**
3. **Robust**

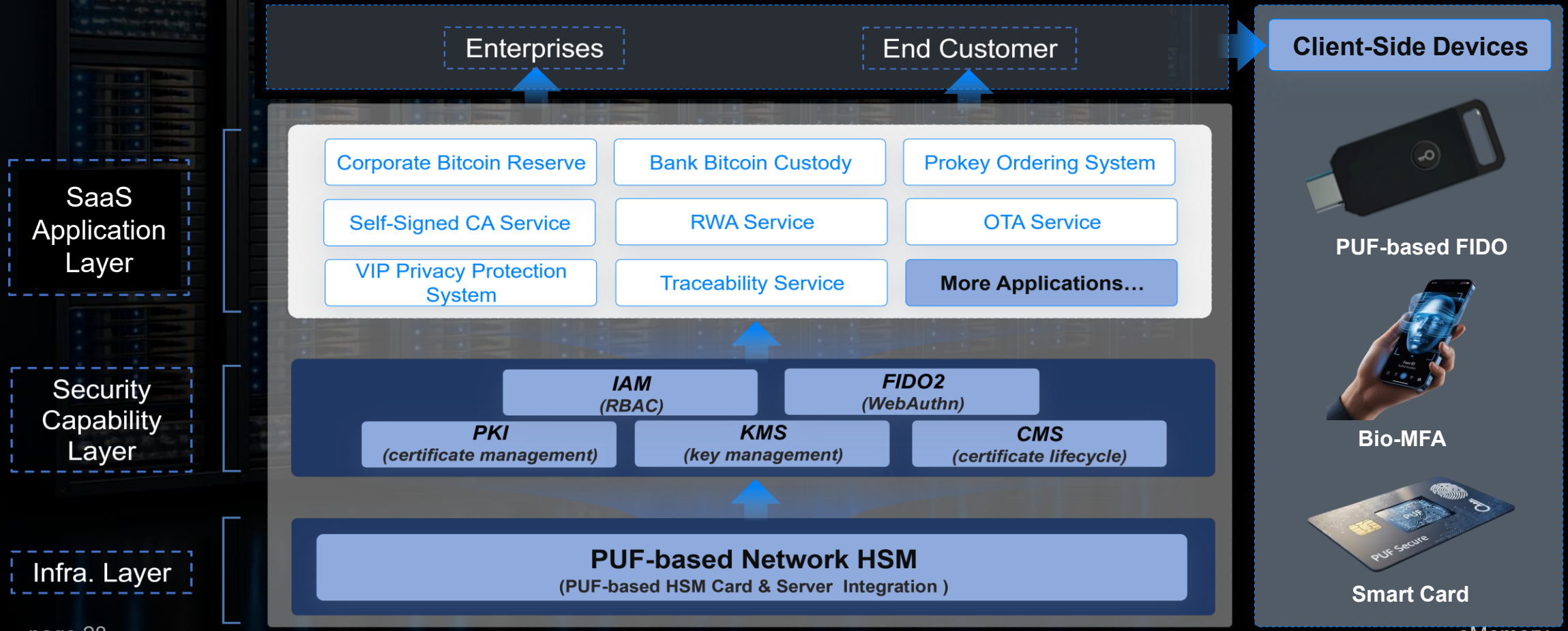
NeoPUF-based HSM Edge Server

- eMemory embeds a physical unclonable root to secure hardware security module (HSM) infrastructure against hardware tampering and insider threats.



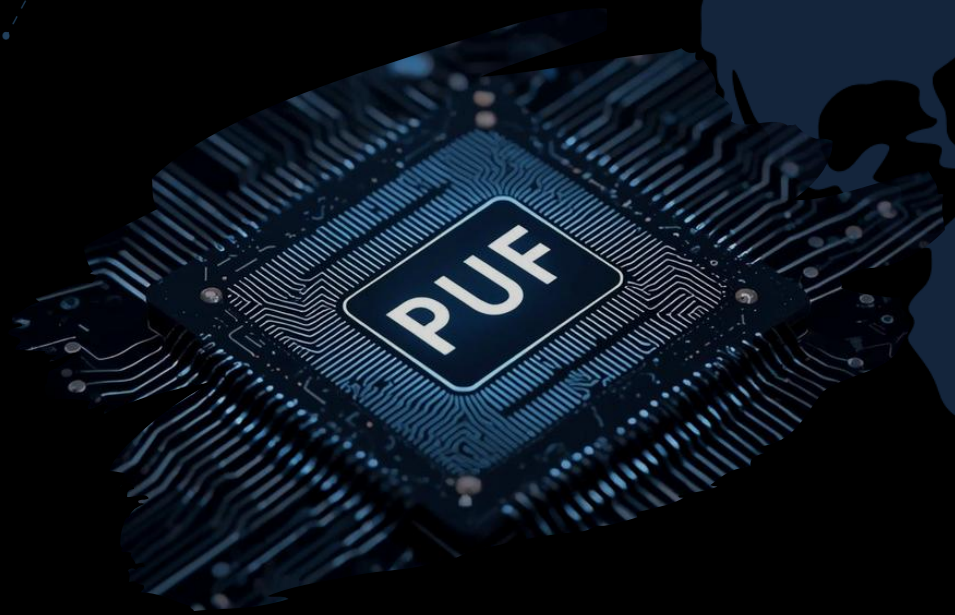
NeoPUF-Based Hardware Security as a Service

- eMemory extends the physical root of trust to software platforms, enabling automated security provisioning for service workflows.



NeoPUF Safeguards National Security

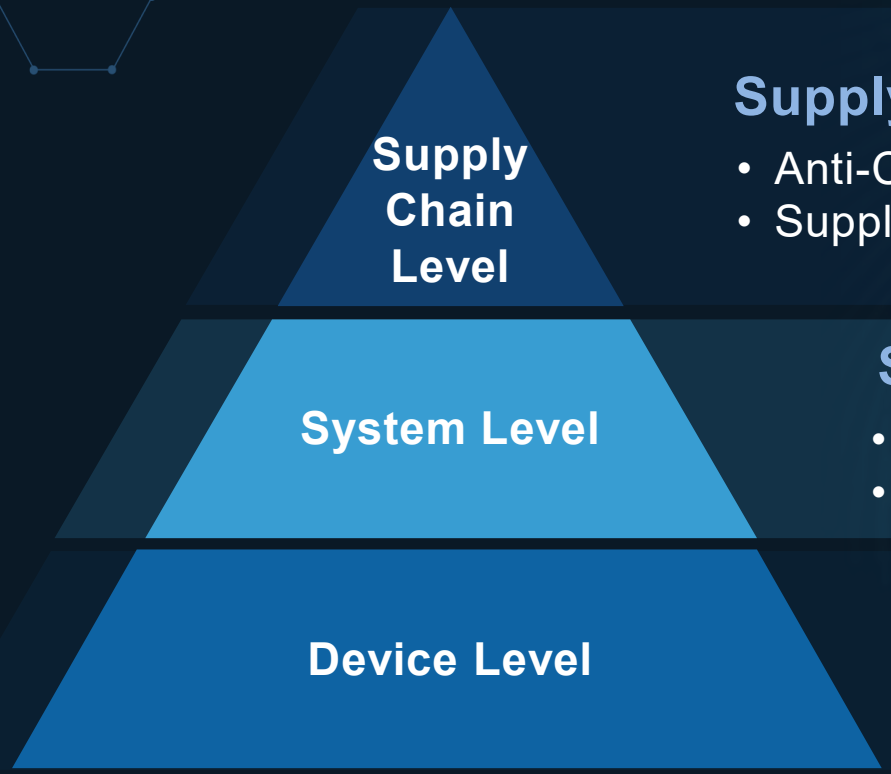
- eMemory establishes a non-replicable hardware identity to protect mission-critical defense supply chains.



- **Create a unique and unclonable hardware identity for every chip**
- **Establish a hardware root-of-trust, enabling secure key generation and device authentication**
- **Transform drones, radios, and satellites into trusted and traceable elements of the mission system**

NeoPUF Authenticates Defense Applications

- eMemory deploys multi-level hardware security to ensure operational integrity from devices to global supply chains.



Supply Chain Level: Enforces Global Traceability

- Anti-Counterfeiting for Military Electronics
- Supply Chain Security

System Level: Guarantees Operational Integrity

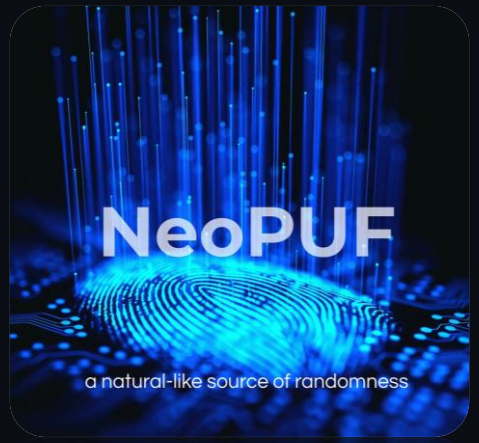
- Secure Boot & Firmware Integrity
- IoT & Sensor Network Security

Device Level: Establishes Hardware Root-of-Trust

- Device Authentication & Identification
- Secure Key Generation

eMemory Video Insight: Security in Action .

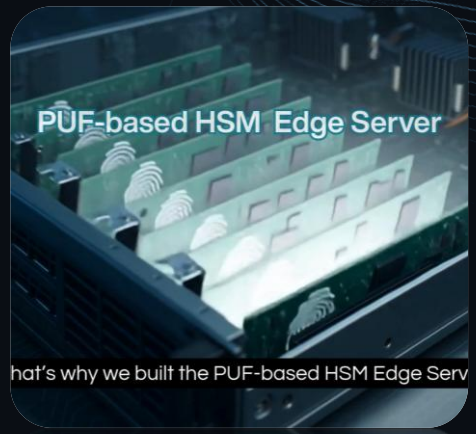
Click on the image to watch the video.



NeoPUF – The Holy Grail of Security

Establishing an unforgeable identity for every chip, creating the ultimate foundation for zero-trust security.

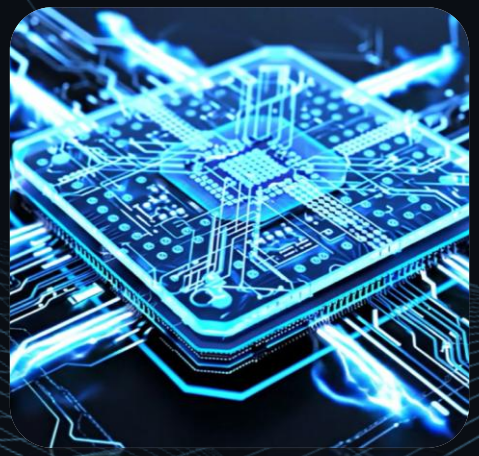
Click on the image to watch the video.



Quantum-Proof Security: PUF based HSM Edge Server for PQC Migration

Transforming hardware security into a scalable service, protecting critical data and infrastructure from cloud to edge.

Click on the image to watch the video.



Chiplet Supply Chain Secured by NeoPUF

Extending trust boundaries to secure the future of heterogeneous computing and integration.

Click on the image to watch the video.

NeoPUF: The Hardware Trust Anchor Powering Tomorrow's Defense Systems

Powering the trusted core of next-generation defense security.

Thank You for your time .

For more information, please visit:
eMemory Website: https://www.ememory.com.tw/
PUFsecurity Website: https://www.pufsecurity.com/