eMemory Briefing ▪

ememory

IPR Notice

Company Overview

- eMemory is the global leader of Logic NVM and Security IP

Revenue Trend
(Unit: NT$ 1,000)

Chart legend: ■ Royalty ■ License/Design Revenue

Y-axis values: 0, 500,000, 1,000,000, 1,500,000, 2,000,000, 2,500,000, 3,000,000, 3,500,000, 4,000,000, 4,500,000

X-axis years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025
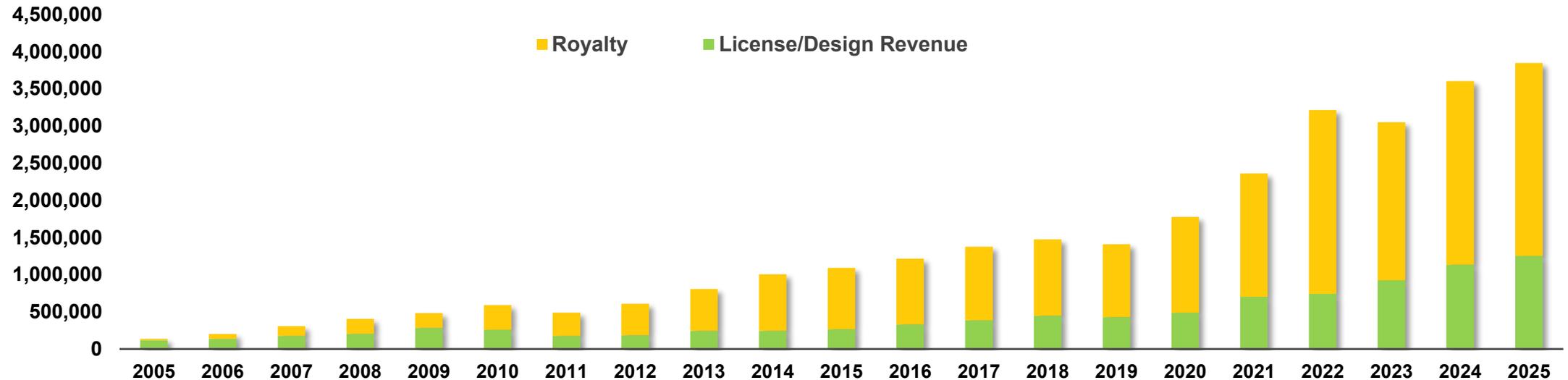
74M+
Cumulative Wafers Shipped
Spanning 740 production processes from 0.5μm to 2nm, and 9.8M wafers (8''-equi.) shipped in 2025.

1350+
Patents Issued
Expanding our IP footprint with 228 pending patents, driven by a 342-member team with 73% 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.
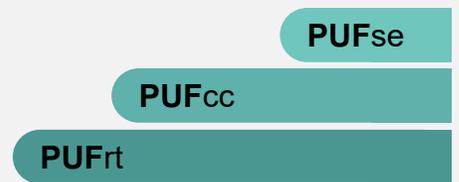
Technology Portfolio

With access to eMemory's widely verified IP process platform, PUFsecurity is uniquely positioned to provide **OTP and PUF-based** Security IP Solutions with **extensive availability** across various foundries and process nodes.

PUFsecurity
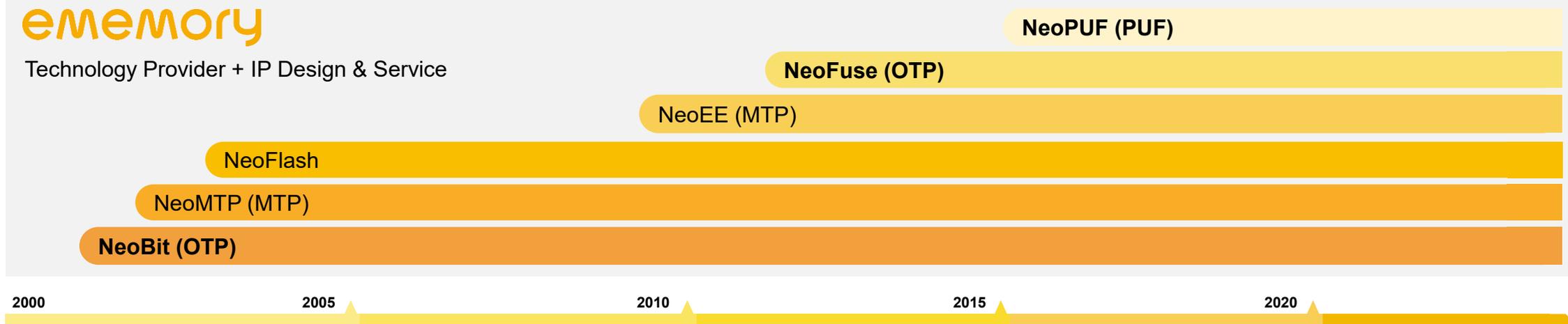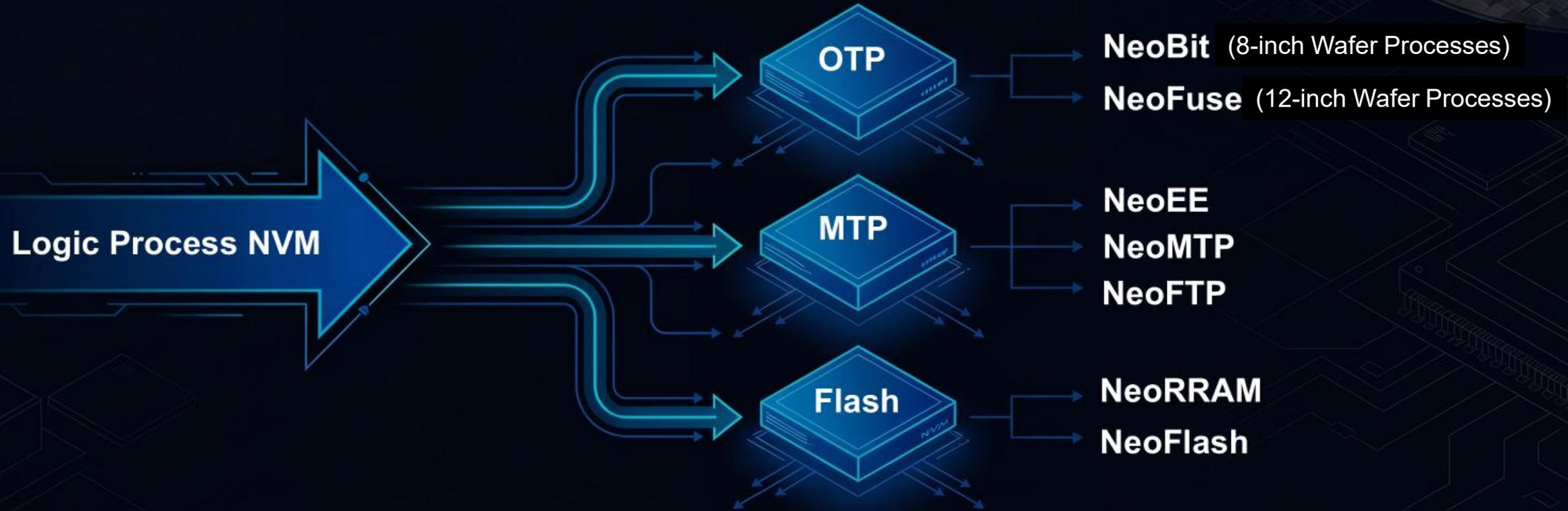PUF-based Security IP Design & Service

- PUFse
- PUFcc
- PUFrt

ememory
Technology Provider + IP Design & Service

- NeoPUF (PUF)
- NeoFuse (OTP)
- NeoEE (MTP)
- NeoFlash
- NeoMTP (MTP)
- NeoBit (OTP)

2000   2005   2010   2015   2020

Core Technology: Logic Process NVM

Logic Process NVM →

OTP →
- NeoBit (8-inch Wafer Processes)
- NeoFuse (12-inch Wafer Processes)

MTP →
- NeoEE
- NeoMTP
- NeoFTP

Flash →
- NeoRRAM
- NeoFlash

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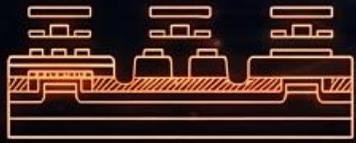- Image sensor recovery
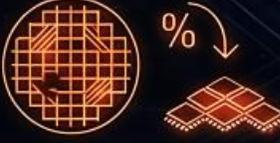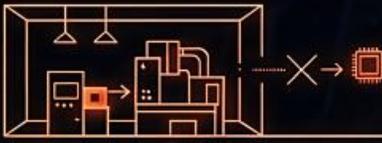- Analog circuits trimming

Performance Flexibility
- Code storage & execution
- Product differentiation & version control

Fundamental Security
- Hardware-rooted, unalterable key storage

Logic NVM
Solving the Pain Points of Traditional NVM

	Traditional NVM	Logic NVM
Process Complexity	Requires 10+ additional masks.	Standard logic process. Zero additional masks.
Cost Efficiency	High manufacturing cost (long process).	Low cost (streamlined production).
Yield Rate	Lower yield (complex processing).	High yield (standard maturity).
Development Cycle	Long lead time. New transistor models required.	Rapid deployment. Uses existing logic models.
Scalability	Limited capacity. Requires new equipment.	Highly scalable. No new equipment needed.

eMemory
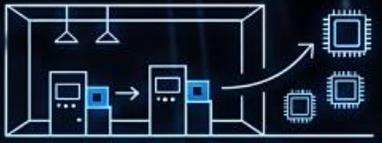
PUF-Based Hardware Security

From OTP to PUF

Root of Trust
- Secure OTP
- TRNG
- NeoPUF
- PUFrt

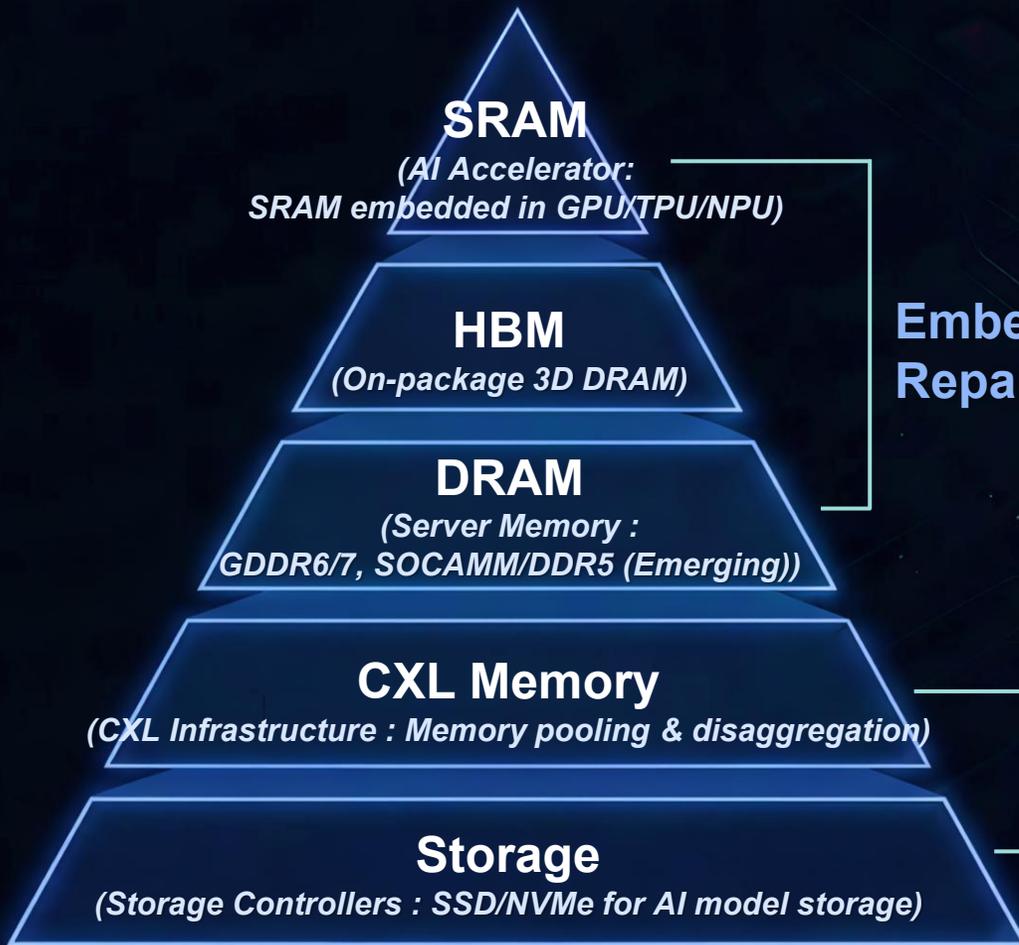**Crypto-processors**
- PUFcc
- PUFhsm

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

Certifications
- NIST CAVP (PQC)
  (FIPS 203/204/205, SP 800-208)
- NIST CAVP/ESV
- PSA L3 RoT, L2 ready
- SESIP L3

**PUF evolves from OTP technology
— the invisible, unique, unclonable hardware key**

eMemory

Where eMemory Fits: AI Memory System

SRAM
(AI Accelerator:
SRAM embedded in GPU/TPU/NPU)

HBM
(On-package 3D DRAM)

DRAM
(Server Memory :
GDDR6/7, SOCAMM/DDR5 (Emerging))

CXL Memory
(CXL Infrastructure : Memory pooling & disaggregation)

Storage
(Storage Controllers : SSD/NVMe for AI model storage)

Embedded Memory Repair

PUF-based Solutions

High Yield, Low Cost
- OTP repair for embedded memory (SRAM/HBM/DRAM)
- MTP-based updateable DIMM configuration (DDR5/SOCAMM)
- Cost-effective AI chip mass production

High Reliability
- Embedded memory repair ensures HBM stack integrity
- OTP redundancy guarantees long-term data retention
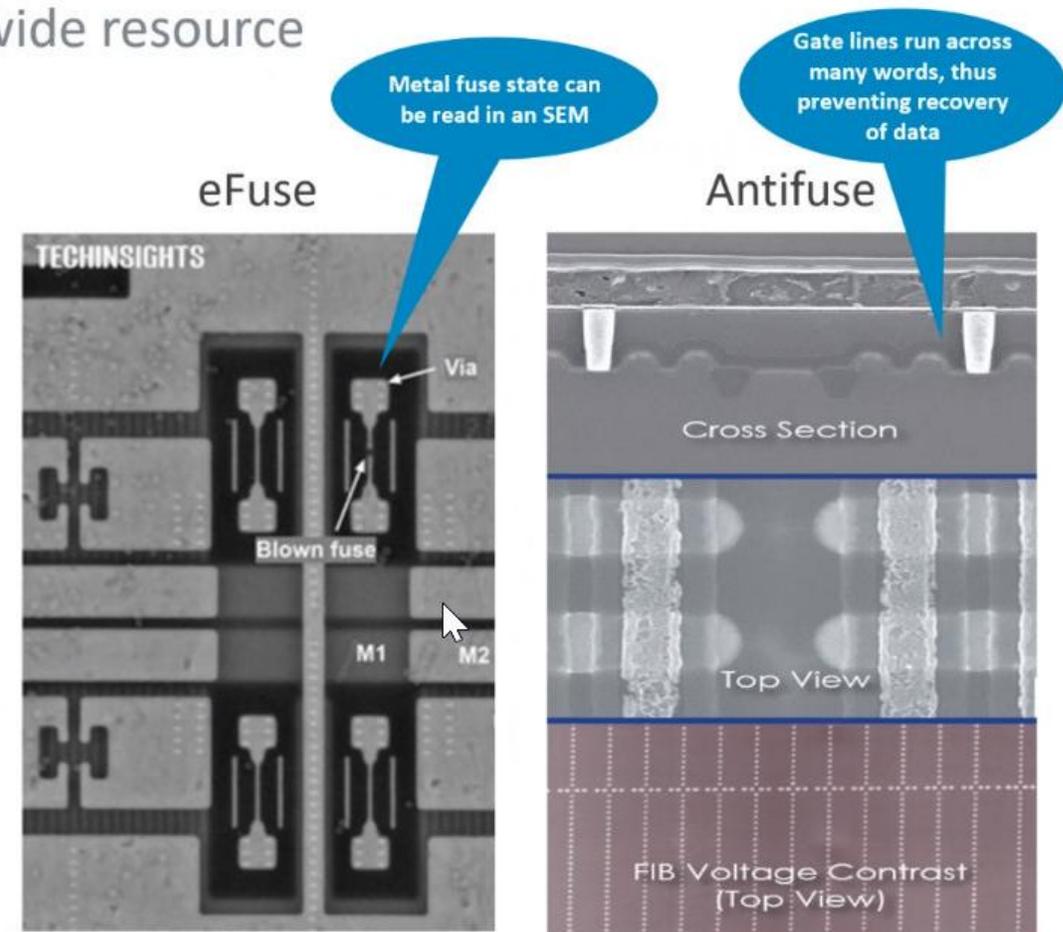- Operational stability under extreme AI workloads

High Security
- PUF-based Root of Trust (PUFrt) establishes a hardware-anchored trust foundation
- Secure data transmission across CXL memory pools
- Protect data storage within NVMe/SSD controllers to safeguard AI models
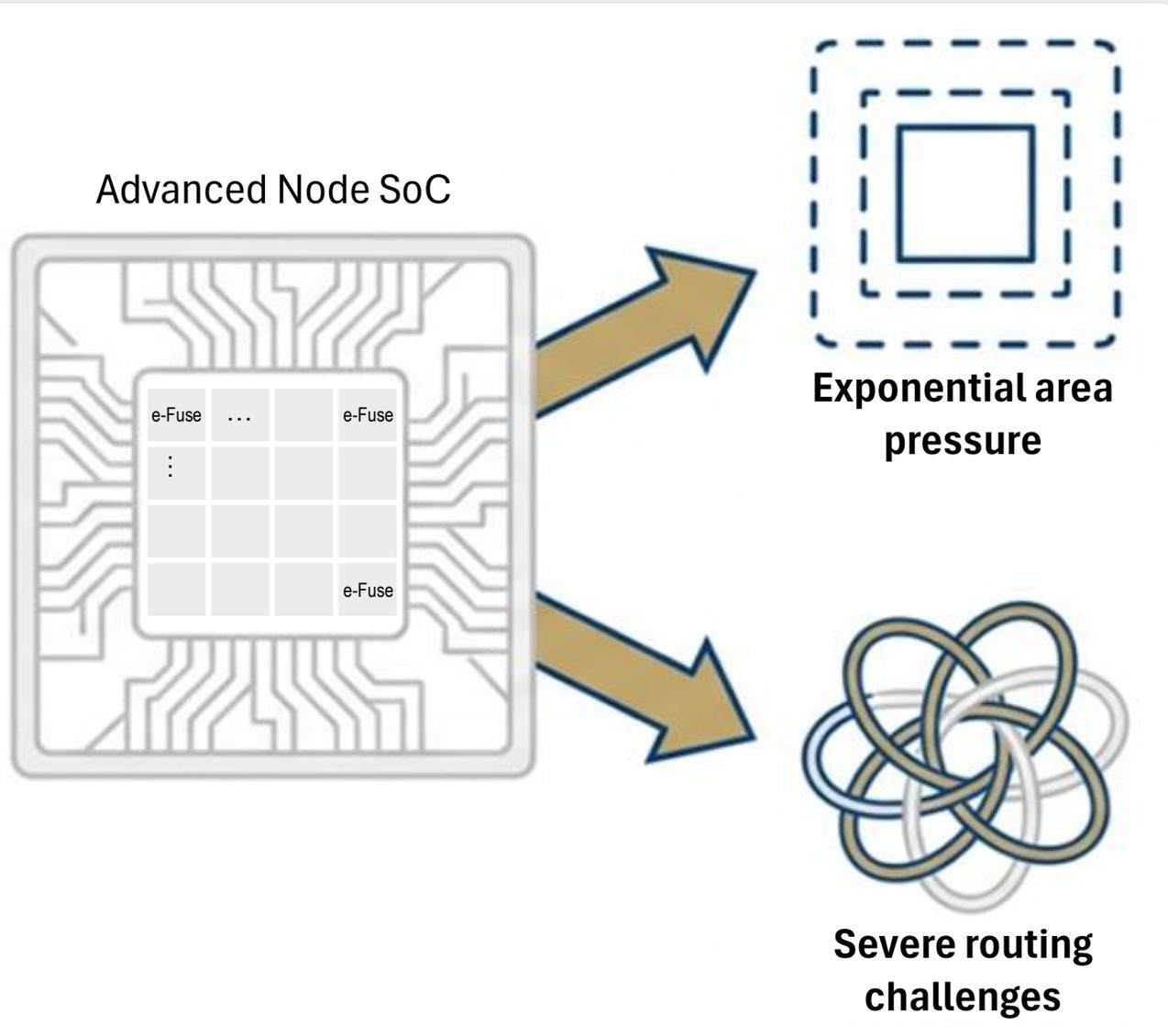
AntiFuse OTP vs. eFuse

One Time Programable (OTP) memory is a SoC-wide resource

- RSS supports OTP as field-programmable to store confidential code and data
- eFuse:
  - Area efficient for smaller arrays
  - Typically not field programmable
  - Can be easily read by delayering SoC (a few $k cost)
    - The secure channel key can be compromised
    - The device can then be cloned
- Antifuse OTP:
  - Cannot be read using a scanning electron microscope
  - Dense bit cells, efficient for large arrays
    - Macro periphery is large versus eFuse
  - Integrated charge pump enables field programming
  - PUF can be included for a small additional area
    - ~0.04mm2 on 7nm for 128x32 bit PUF

eFuse — Metal fuse state can be read in an SEM

Antifuse — Gate lines run across many words, thus preventing recovery of data

https://semiengineering.com/the-benefits-of-antifuse-otp/

Rainer Herberholz

arm

Advanced Nodes Amplify the Structural Limitations of e-Fuse

Advanced Node SoC

| e-Fuse | … | e-Fuse |

e-Fuse

Exponential area pressure

Severe routing challenges

As SoC functionality grows more complex, the number of e-Fuse blocks typically increases to 8–16 per SoC, significantly **amplifying area and routing pressure**, while also **requiring larger SRAM to compensate for e-Fuse limitations**.

Challenge

At advanced nodes, growing functional requirements (e.g., code storage, configuration data, SRAM repair) drive the deployment of multiple e-Fuse blocks per SoC.

Impact

This not only increases silicon area consumption, but also creates severe backend routing challenges and additional SRAM overhead.

Multi-e-Fuse Architectures Impose High Costs in Area, Power, and Efficiency

Area Overhead

- e-Fuse data must be copied to SRAM at boot due to limited read cycles and high-temperature constraints.
- This duplication increases **boot time and doubles the memory footprint** for configuration data.

Design Complexity

- Distributed placement of 8–16 e-Fuse blocks significantly **complicates routing**.
- Programming e-Fuse requires **high current**, adding constraints to power planning and IR drop management.
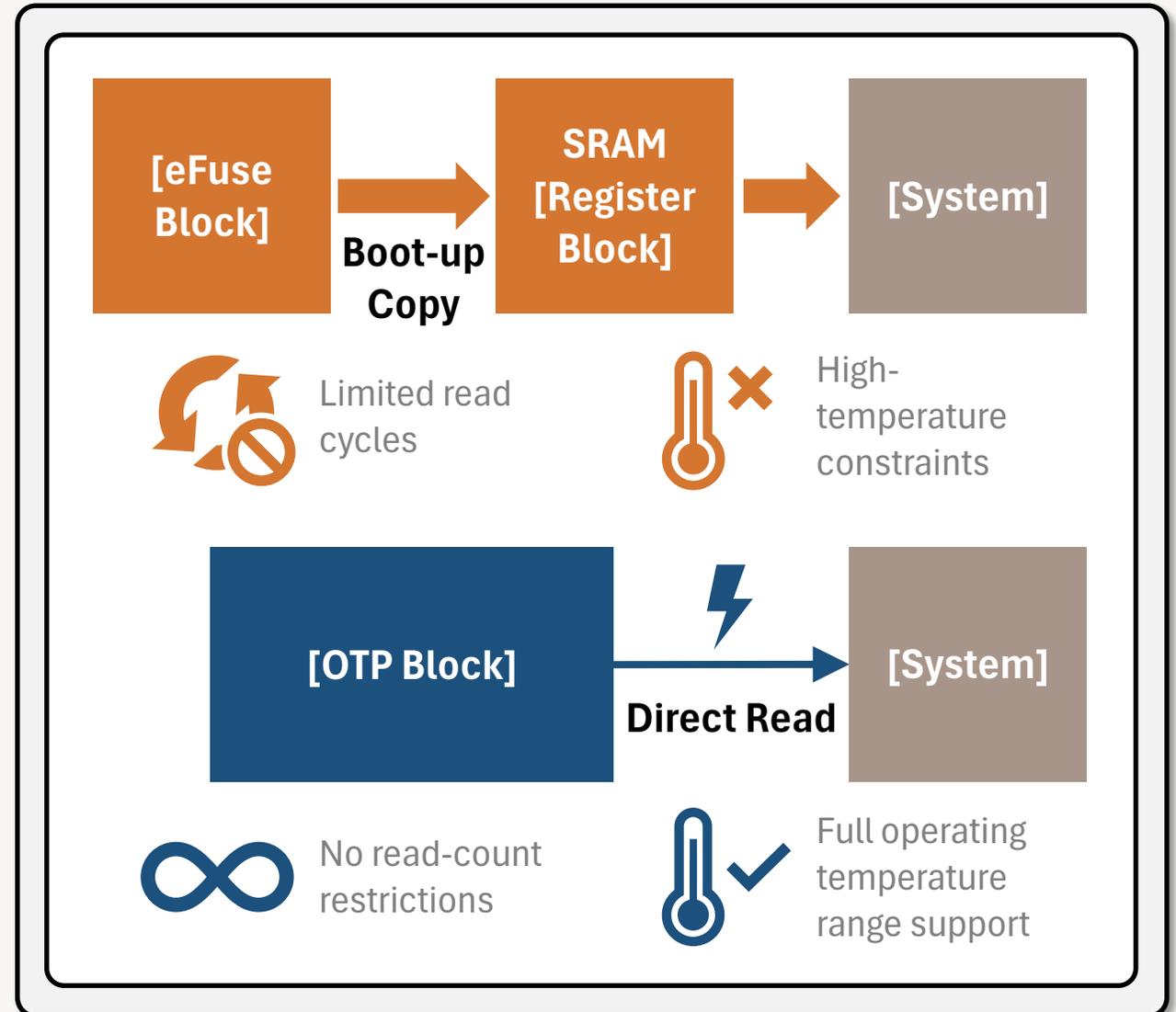
OTP Delivers a Clear Area Advantage Beyond 4K × 8 Density

e-Fuse

Total area: 1.92 mm^2
(excluding SRAM)

16 x 2Kx8 e-Fuse

OTP

Total area:
0.33 mm^2

1 x 32Kx8 OTP

Item	e-Fuse Solution (16 × 2K×8)	OTP Solution (1 × 32K×8)	Conclusion
Total storage capacity	32K × 8	32K × 8	Same
Area per macro	0.12 mm²	0.33 mm²	-
Total area	~1.92 mm²	0.33 mm²	>80% area reduction with OTP
Additional SRAM / registers	Required	Not required	Further savings in area and power

eMemory

e-Fuse vs. OTP: A Critical Choice for Advanced Nodes

Challenges with e-Fuse
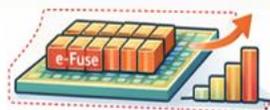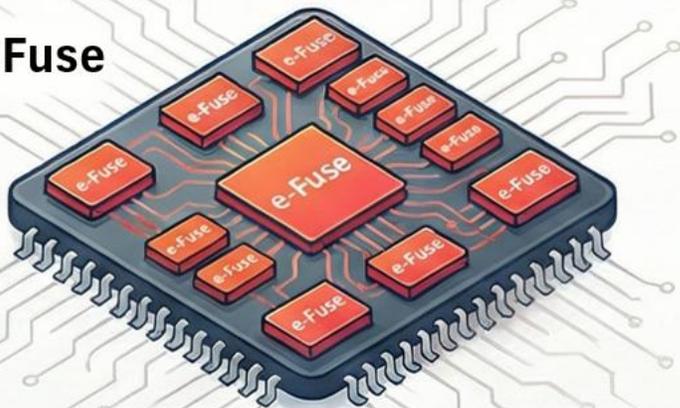
Excessive silicon footprint
Advanced nodes often require 8–16 e-Fuse blocks, significantly inflating die area.
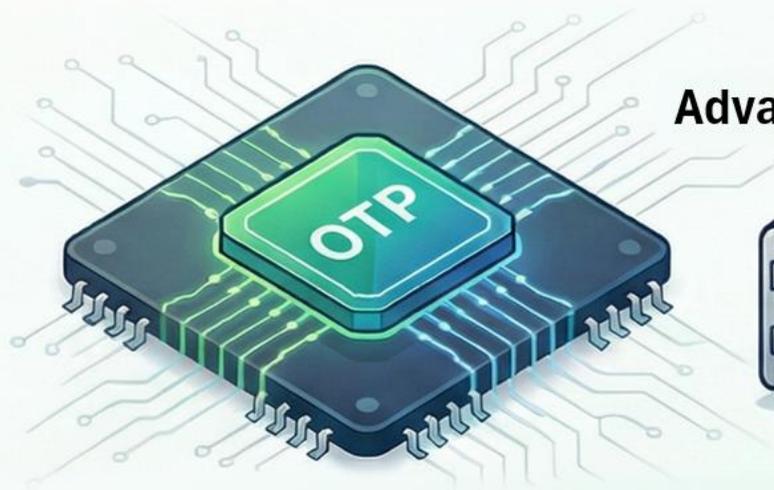
High design complexity
- Limited read cycles
- High-temperature operating constraints
- Mandatory boot-time data copy to SRAM

Weaker native security
Sensitive data typically requires additional encryption mechanisms, increasing system complexity.

Additional Encryption

Advantages of OTP

Lower area and cost
3%~6% Cost Reduction
Transitioning from e-Fuse to OTP can reduce total SoC cost by **approximately 3–6%**.
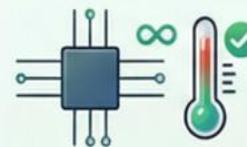
Simplified system design
- Direct read access
- No read-count or temperature limitations
- Reduced boot-time overhead

Integrated security capabilities
PUF/TRNG Integration
OTP can be natively combined with **PUF and TRNG**, enabling a more **complete hardware-root-of-trust solution**.

eMemory Technology Inc.

Registered IPs at TSMC
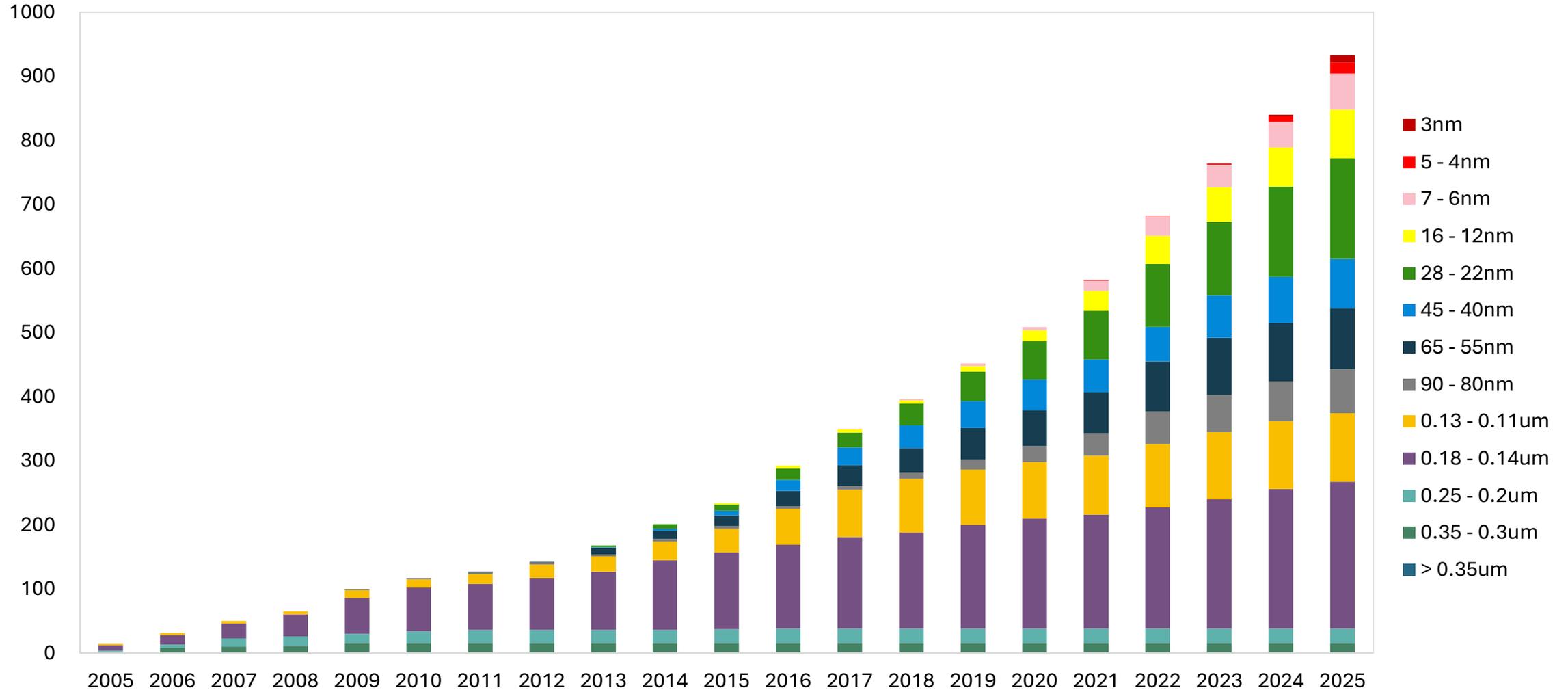
Registered IP > 850
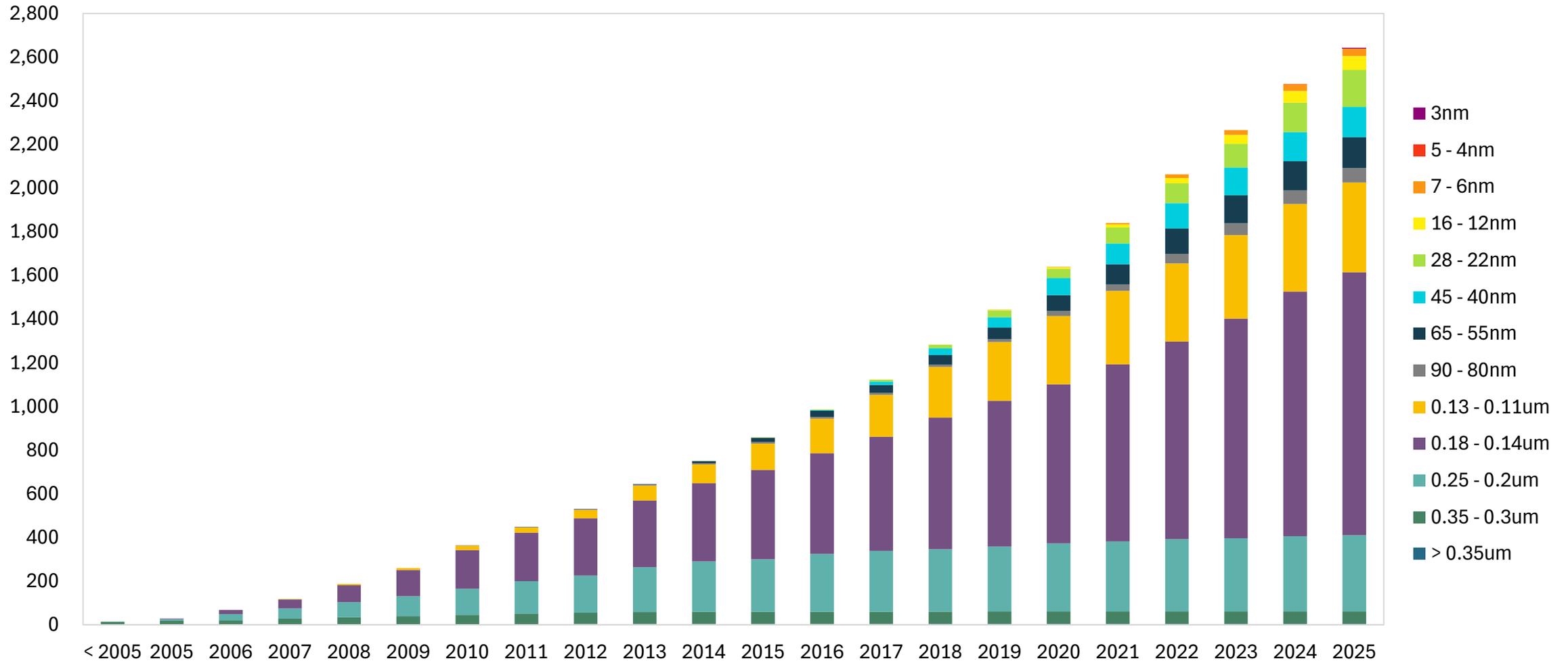
Wafer Contribution at TSMC

8"-Equivalent Wafer Contribution > 25M

Legend:
- 7 - 6nm
- 16 - 12nm
- 28 - 22nm
- 45 - 40nm
- 65 - 55nm
- 90 - 80nm
- 0.13 - 0.11um
- 0.18 - 0.14um
- 0.25 - 0.2um
- 0.35 - 0.3um
- > 0.35um

Y-axis: Millions (0 to 35)

X-axis: < 2005, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025
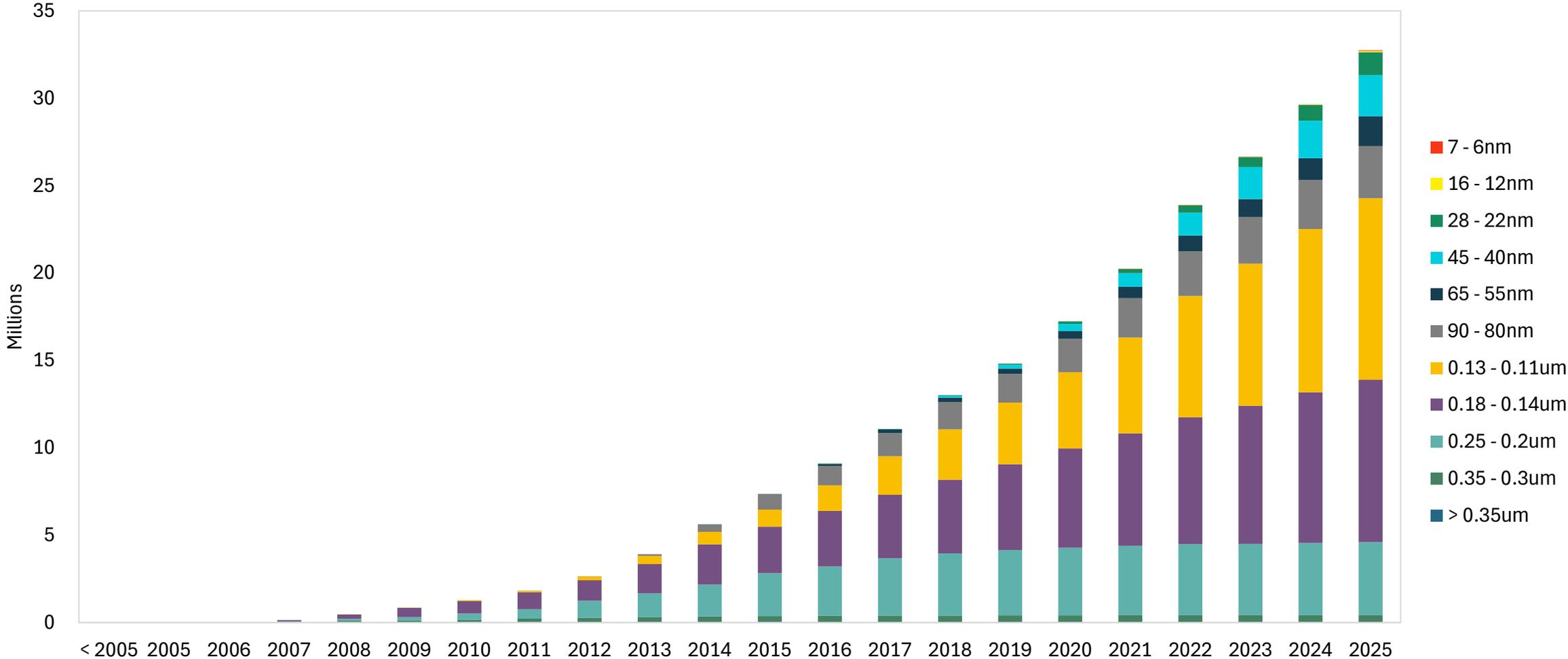
Advanced-Node Tape-out Landscape

Leading-Edge Nodes (3nm–7nm)

55 TOTAL TAPE-OUTS

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

18	
9	
7	
21	

■ Defense-related ■ AI SoC ■ SSD Controller ■ Others
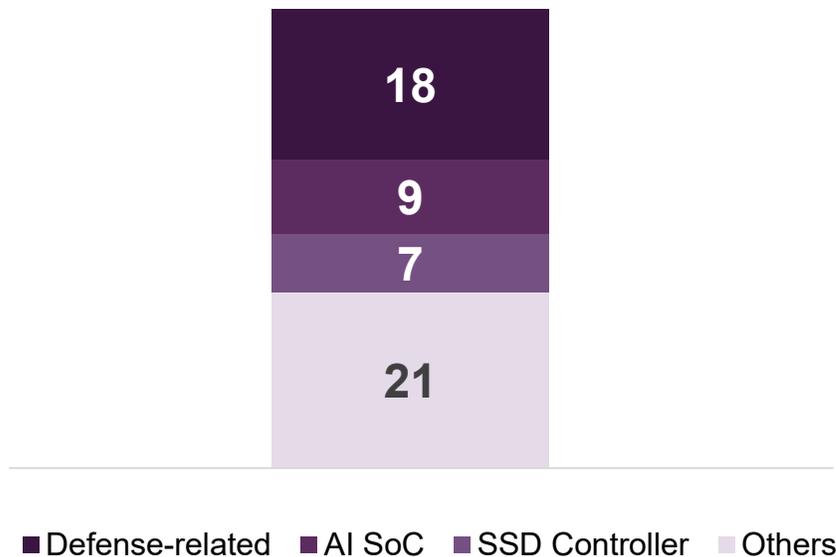
Mainstream Advanced Nodes (12nm/16nm)

77 TOTAL TAPE-OUTS

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

15	
13	
11	
38	

■ Multimedia ■ Network IC ■ SSD Controller ■ Others

eMemory
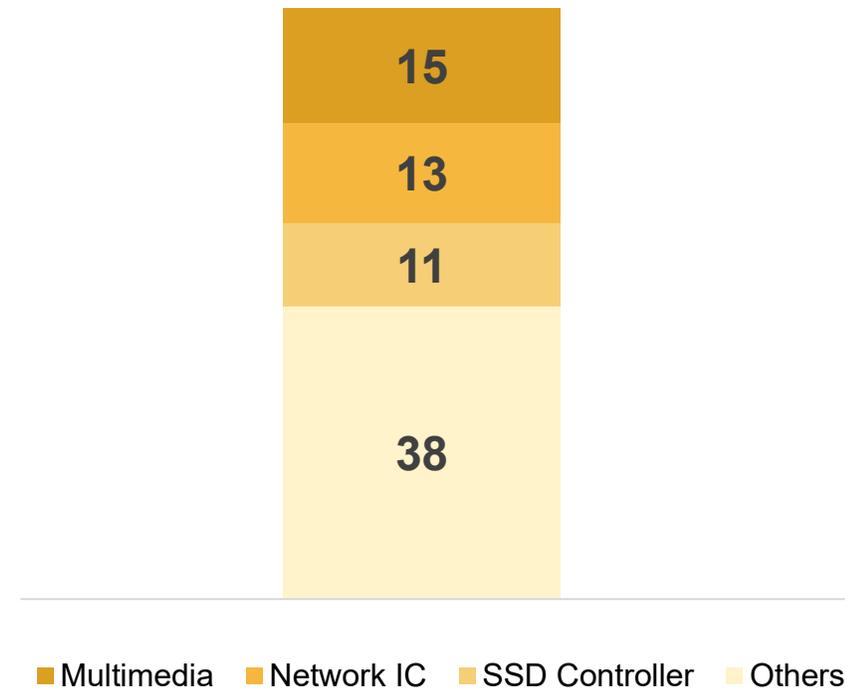
Revenue and Tape-out by Technology

| Year	NTO		Revenue (USD)		
	NeoBit	NeoFuse	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	$ 31,834,860	$ 10,773,223	$ 85,000
2019	226	109	$ 27,602,332	$ 14,466,279	$ 195,000
2020	248	182	$ 30,378,346	$ 26,437,660	$ 434,998
2021	252	259	$ 32,367,560	$ 44,011,223	$ 1,160,702
2022	264	231	$ 35,327,060	$ 63,762,480	$ 4,207,209
2023	226	241	$ 23,251,721	$ 64,276,058	$ 4,375,409
2024	266	270	$ 25,952,137	$ 71,649,123	$ 5,279,985
2025	253	248	$ 27,312,244	$ 78,122,682	$ 7,645,293
Total	**5,382**	**1,730**	**$ 482,412,457**	**$ 384,164,465**	**$ 23,383,735**

*NTO stands for **New Tape-Out**

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

eMemory

Evolution from **OTP** to **PUF-HSM**

- Based on OTP technologies, many different security function IPs have evolved
- Hardware Security has evolved from SecureOTP to a full PUF-Based Security Subsystem

eMemory
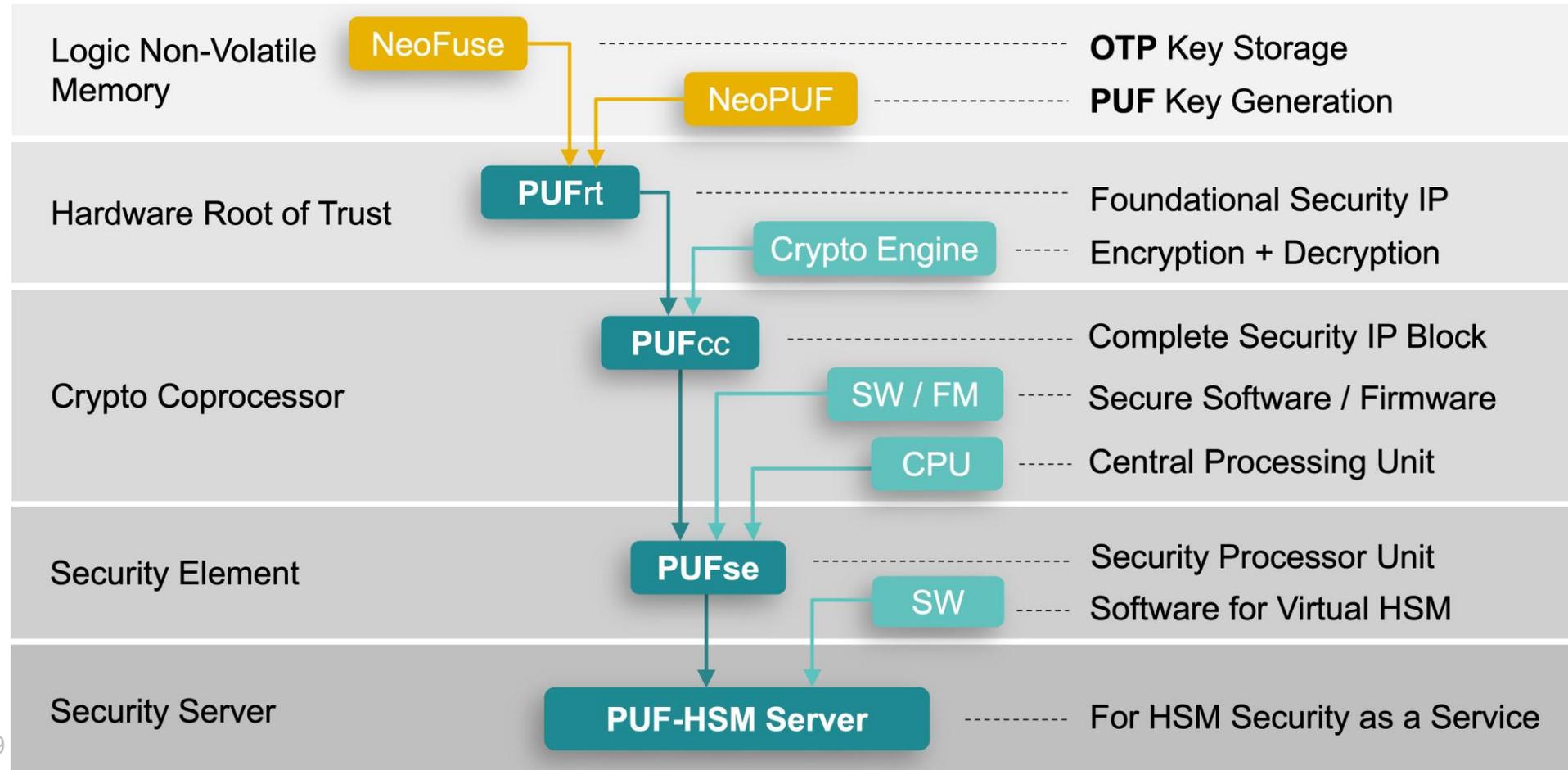
The Foundation of the Security Ecosystem
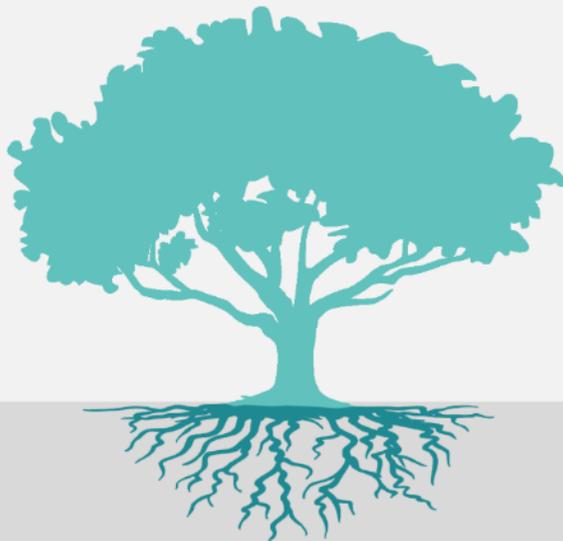
Software Security Ecosystem
- Continually changing and adapting to new threats
- Relies on immutable Hardware Root of Trust

PUFsecurity
- Hardware Security For the entire lifespan of the Chip
- Foundational **Hardware Root of Trust** for Software

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

Data Center

IoT

Security Business Development

- As eMemory is an established IP company, there are different **platforms** that we can leverage for sales in security IPs and sub-systems

Foundry Platforms
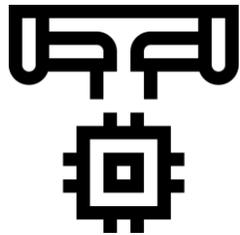
TSMC, Intel, UMC, GF, etc.

- Licensed our security technology to major foundries
- Co-promotional activities

CPU Partners

Arm, RISC-V, Cadence, etc.

- SoC customers looking for both CPU and security subsystems

CSP

More to come

- Work with CSP and system companies for embedded security on a chip level

eMemory

eMemory for **AI Servers** and **Edge Devices**

AI Servers

- **Storage**
  - SSD Controller (B)
  - SSD
  - SSD
- **Processing - Serial**
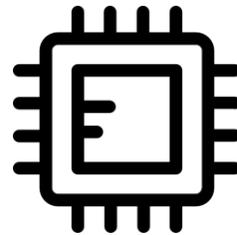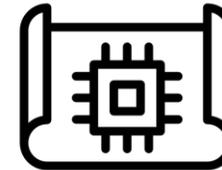 - (A) SRAM (A) SRAM
  - CPU (B) CPU (B)
  - Interface
- **DRAM**
  - CXL Controller (B)
  - CXL Memory Expander (A)
- **Processing - Parallel**
  - GPU (B) GPU (B) GPU (B)
  - GPU (B) GPU (B) GPU (B)

+

AI Edge Computing

- **SoC**
  - (A) SRAM
  - CPU (B)
  - (B) Hardware Root of Trust — PUFrt
  - Accelerator
- (B) SSD
- (A) DRAM
- (D) Flash
- Sensors
- Actuators (C)
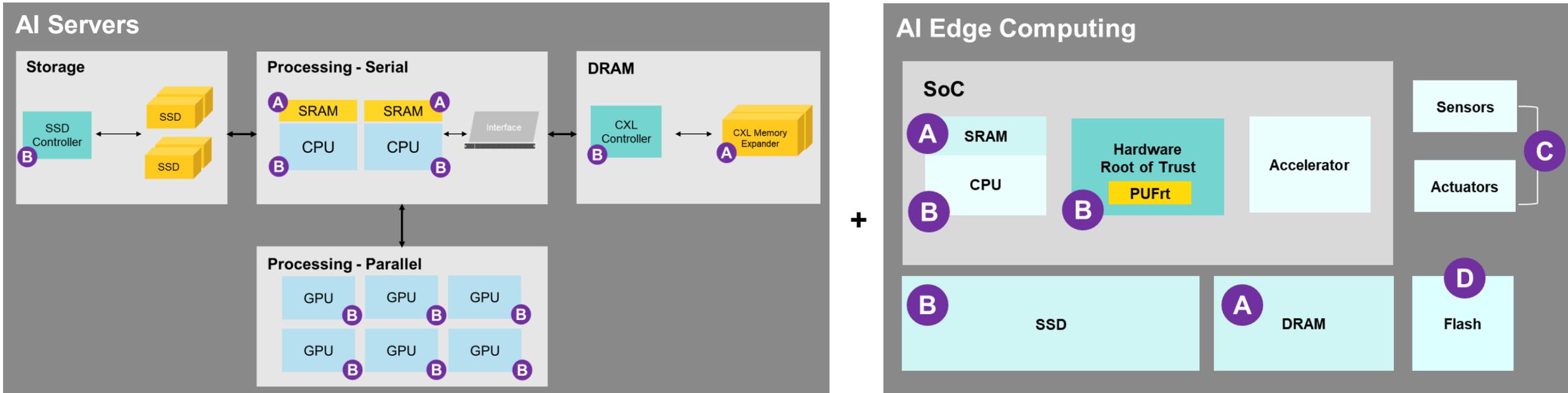
(A) Memory Repair

(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

Why is **Caliptra** so Important?

Datacenter Chips

DPU CPU GPU NIC

Every chip needs Root of Trust

Caliptra Root of Trust
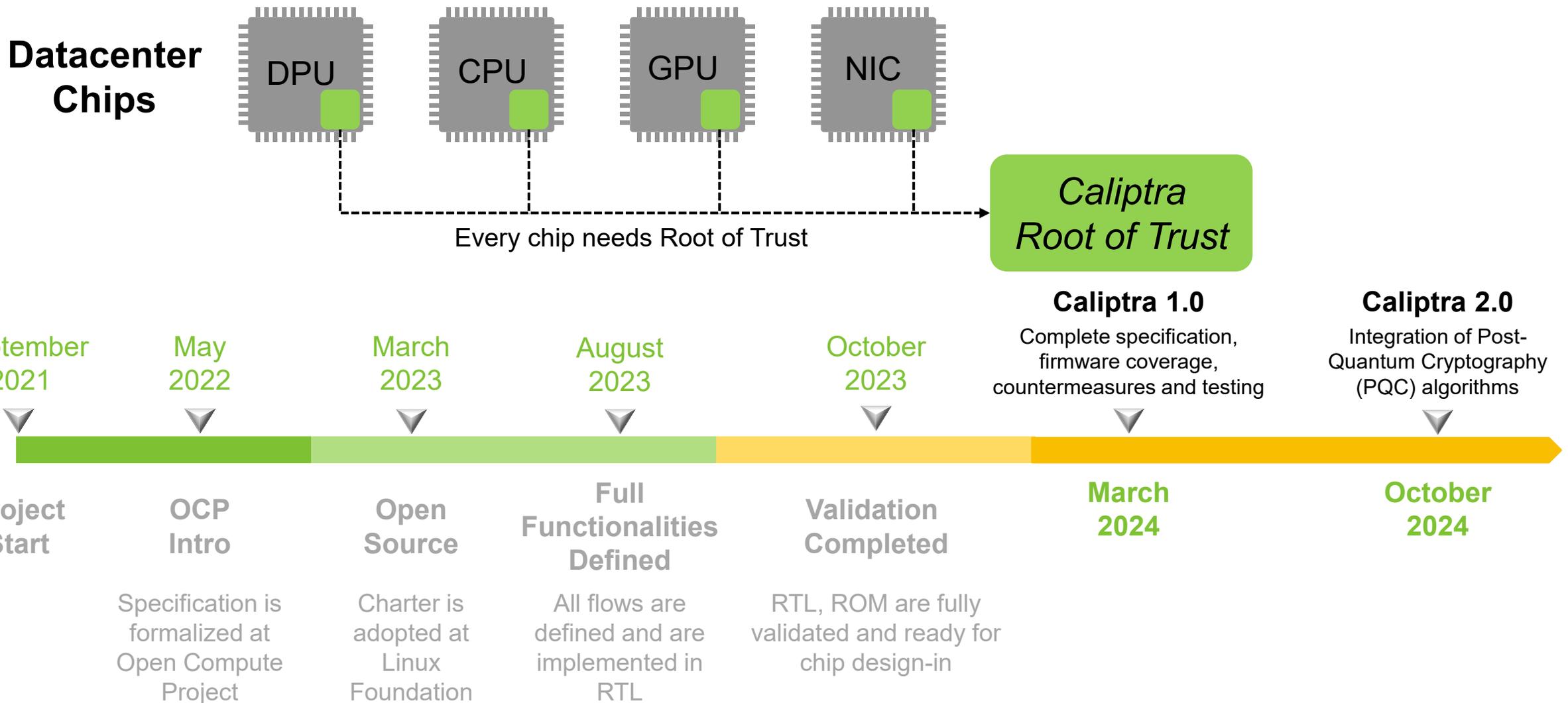
Caliptra 1.0
Complete specification, firmware coverage, countermeasures and testing

Caliptra 2.0
Integration of Post-Quantum Cryptography (PQC) algorithms

September 2021	May 2022	March 2023	August 2023	October 2023		

Project Start

OCP Intro

Specification is formalized at Open Compute Project

Open Source

Charter is adopted at Linux Foundation

Full Functionalities Defined

All flows are defined and are implemented in RTL

Validation Completed

RTL, ROM are fully validated and ready for chip design-in

March 2024

October 2024

eMemory

What is the Important Role of **eMemory** in **Caliptra**?

- eMemory's root of trust IP is ready to meet Caliptra's requirements.

Datacenters

Caliptra Silicon RoT

ememory IP Portfolio

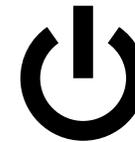| OTP	PUF	TRNG	Crypto-processors	Cryptography (PQC)
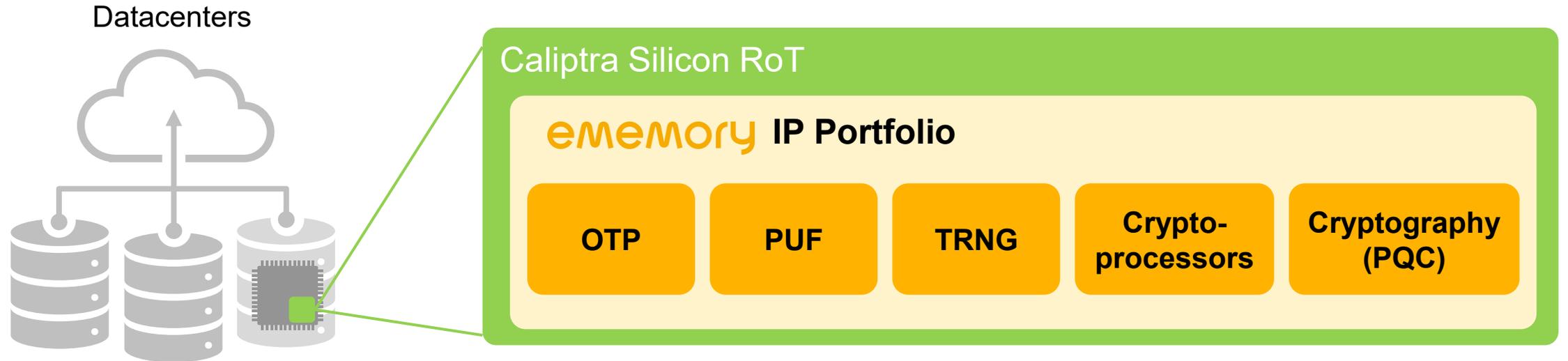
Unique Chip Identity

Chip Fingerprint

Secure Attestation

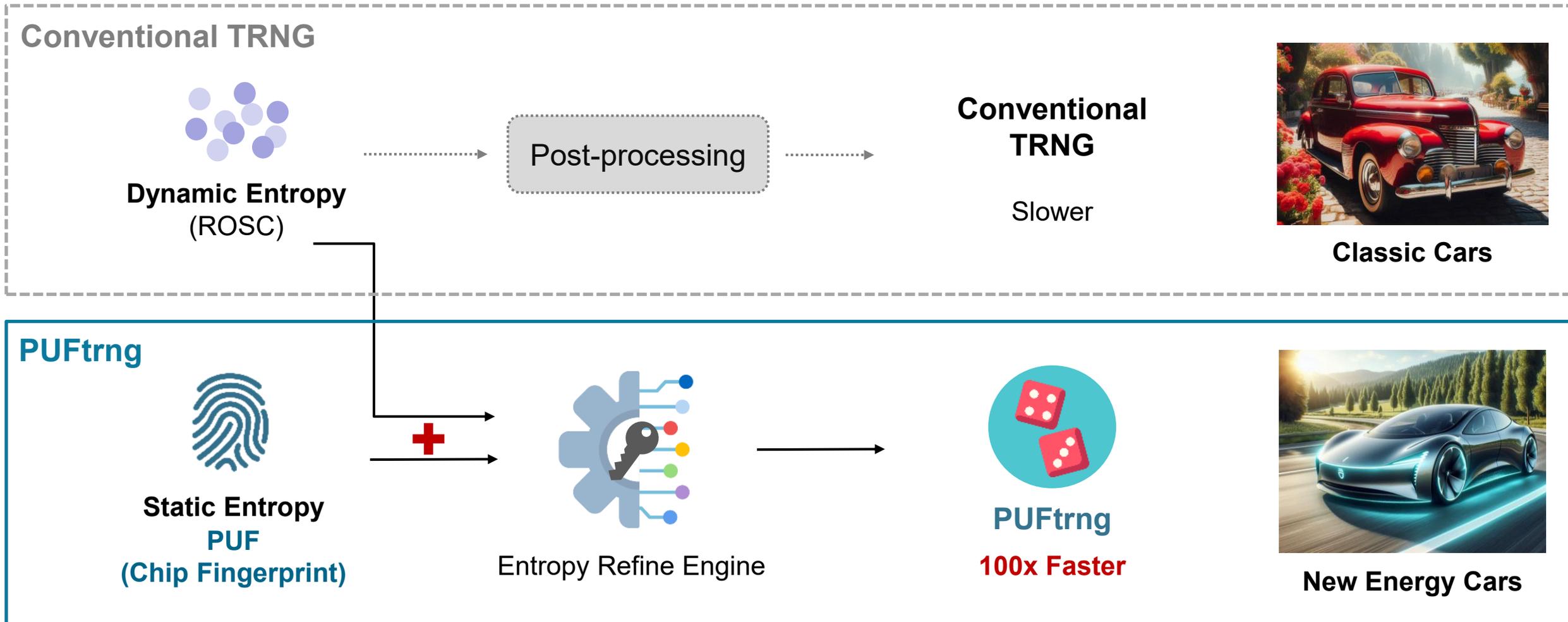Device Certificate

Secure Boot

Boot into Trusted Operating System

PUFtrng: 100 Times Faster than Conventional TRNG

- PUF-based conditioning algorithm provides high-throughput and high entropy quality

Similar to…

Conventional TRNG

Dynamic Entropy
(ROSC)

Post-processing

Conventional TRNG

Slower

Classic Cars

PUFtrng

Static Entropy
PUF
(Chip Fingerprint)

Entropy Refine Engine

PUFtrng

100x Faster

New Energy Cars

eMemory

PUFtrng: 100 Times Faster than Conventional TRNG

- PUF-based conditioning algorithm provides high-throughput and high-quality entropy

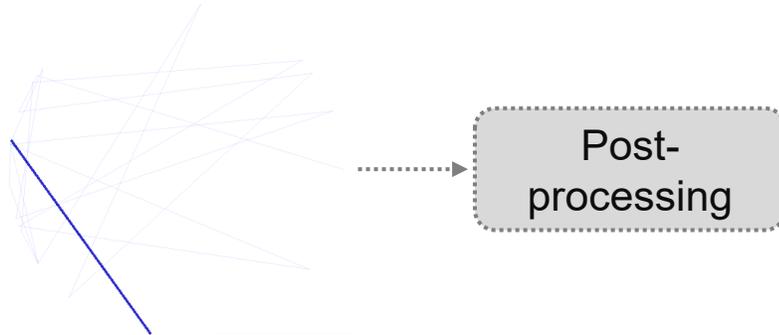*Similar to…*

Conventional TRNG

Figure 1:

Dynamic Entropy

Post-processing

Figure 2:

Conventional TRNG
→ Low throughput random bits
→ Slower

Classic Cars

PUFtrng

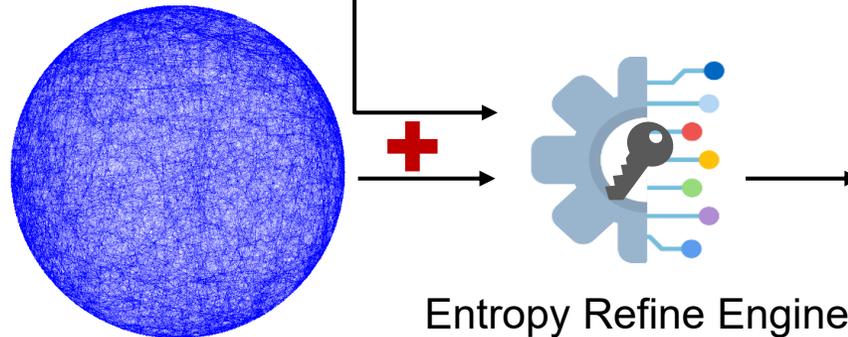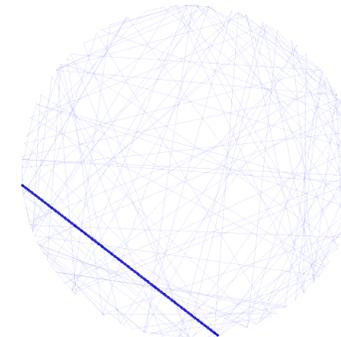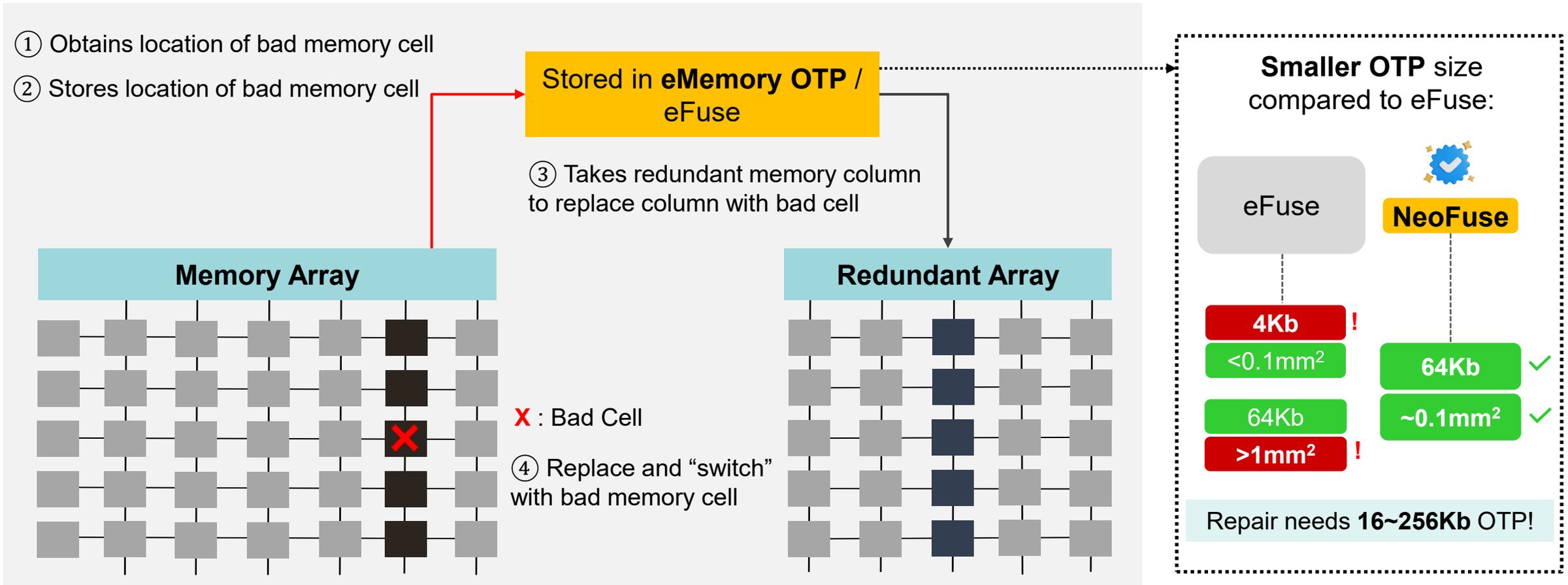**Figure 3:**

Static Entropy
→ **PUF**
(chip fingerprint)

Entropy Refine Engine

Figure 4:

PUFtrng
→ **High** throughput random bits
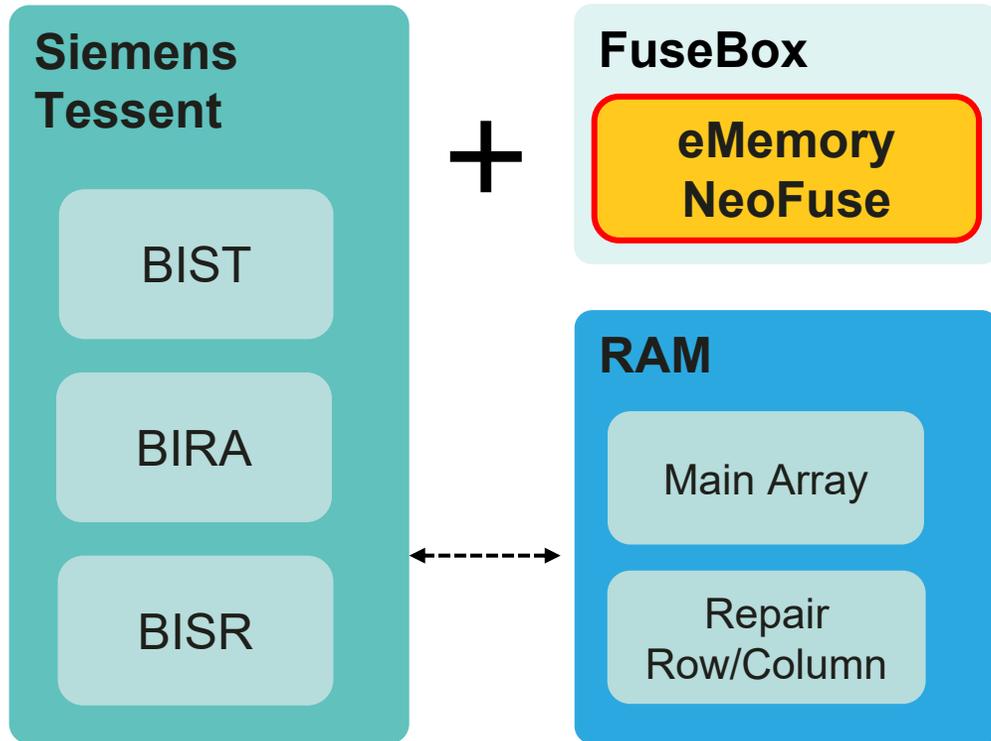→ **100x Faster**

New Energy Cars

eMemory

eMemory enables **High-Yielding** SRAM

- SRAM yield decreases as technology is scaled due to smaller dimensions. To **increase yield**, **eMemory's OTP** is required.

① Obtains location of bad memory cell

② Stores location of bad memory cell

Stored in eMemory OTP / eFuse

③ Takes redundant memory column to replace column with bad cell

Memory Array

Redundant Array

X : Bad Cell

④ Replace and "switch" with bad memory cell

Smaller OTP size compared to eFuse:

eFuse	NeoFuse
4Kb !	
<0.1mm^2	**64Kb** ✓
64Kb	~0.1mm^2 ✓
>1mm^2 !	

Repair needs **16~256Kb** OTP!

Partnering for Success: **eMemory and Siemens** ▪

Siemens Tessent

BIST

BIRA

BISR

+

FuseBox

eMemory NeoFuse

RAM

Main Array

Repair Row/Column

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

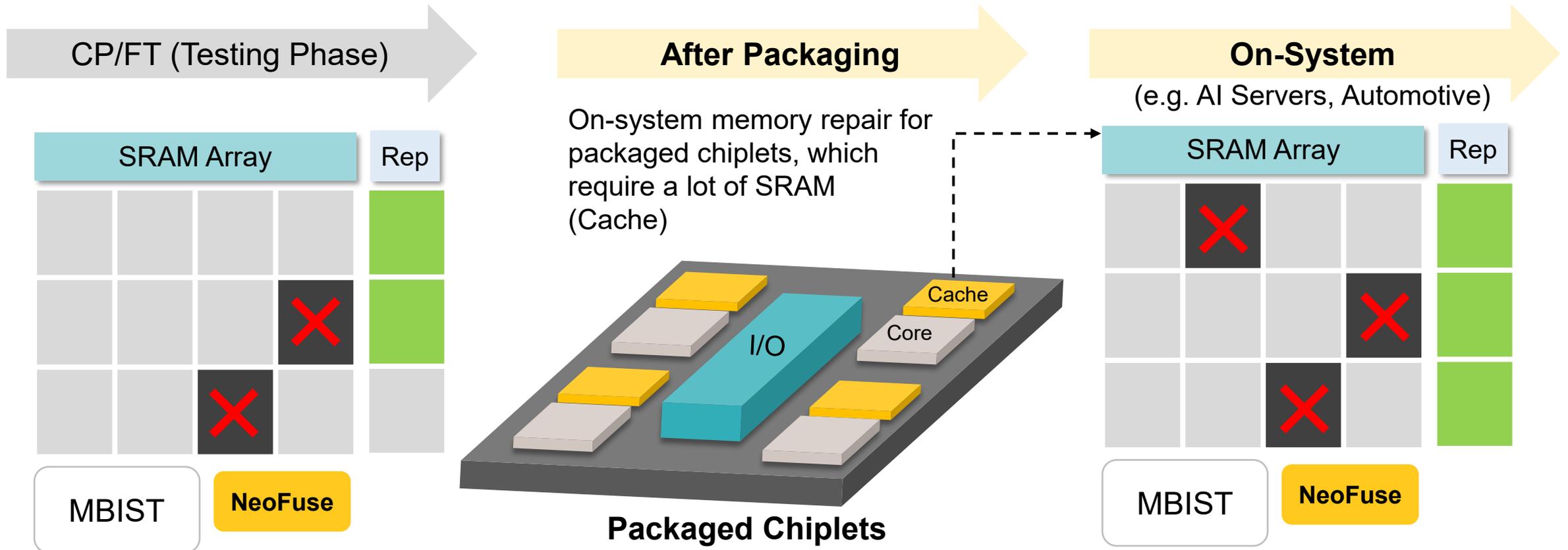eMemory provides OTP with interface for Siemens MBIST:

- **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**

On-System Repair for AI Accelerators

- Memory Built-in Self-Test (MBIST) offers **on-system repair** capabilities, which are essential for high-speed high-reliability applications and chiplet **architecture** or **after system** packaging.

CP/FT (Testing Phase) → **After Packaging** → **On-System** (e.g. AI Servers, Automotive)

On-system memory repair for packaged chiplets, which require a lot of SRAM (Cache)

SRAM Array | Rep

MBIST | NeoFuse

Packaged Chiplets

I/O · Core · Cache
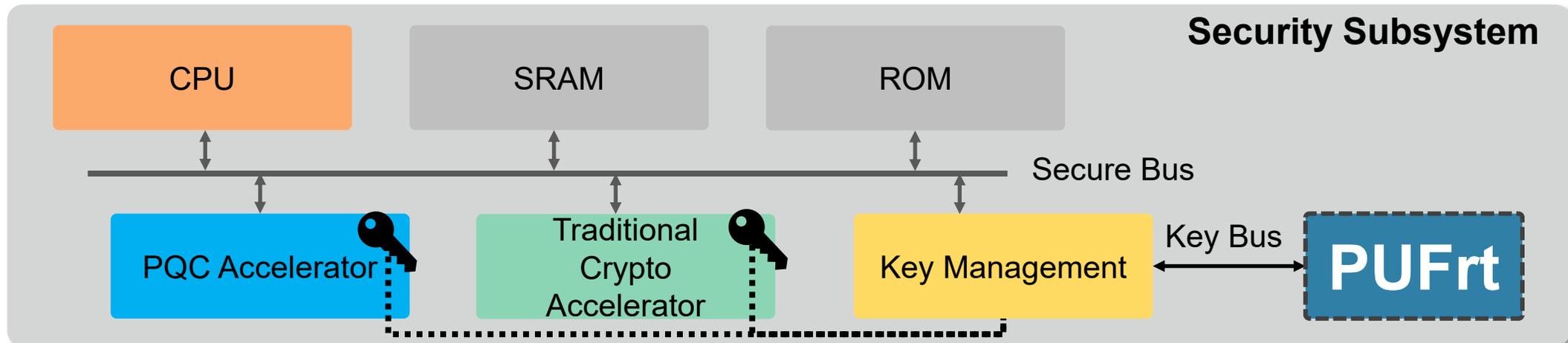
SRAM Array | Rep

MBIST | NeoFuse

Made possible with MBIST

How **PUF-based Solutions** Help **PQC?**

- Our PUF-based Root of Trust (PUFrt) can help PQC:
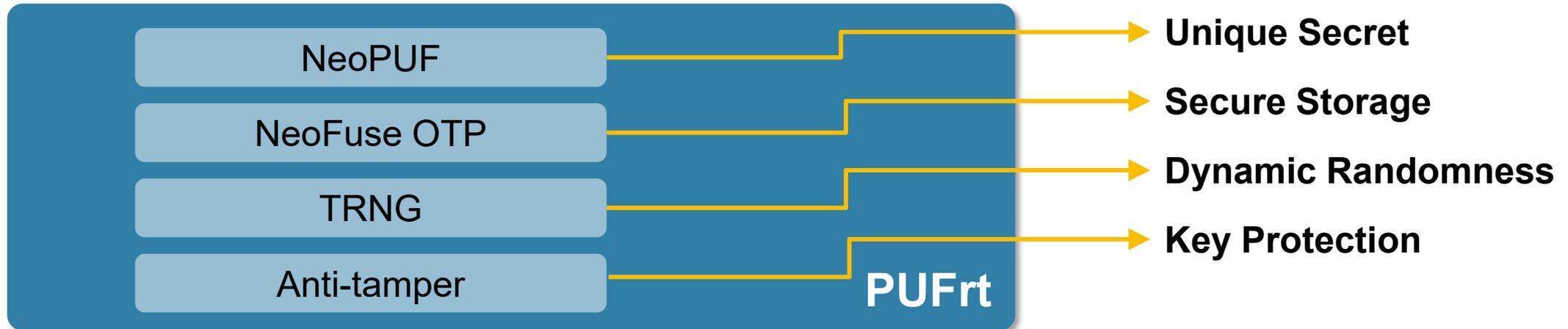
- By integrating the PUFrt into the security subsystem, it can effectively manage the long and complex keys required for PQC algorithms.

PQC Migration Steps & Scope

Key Principles:
- Execute Clear Migration Steps
- Prioritize Critical Digital Assets
- Deploy PQC-ready HSM Edge Servers

Select from FIPS 203/204/205
for key exchange & signatures

Validate PQC integration
via software

Track new database
and key system to ensure stability

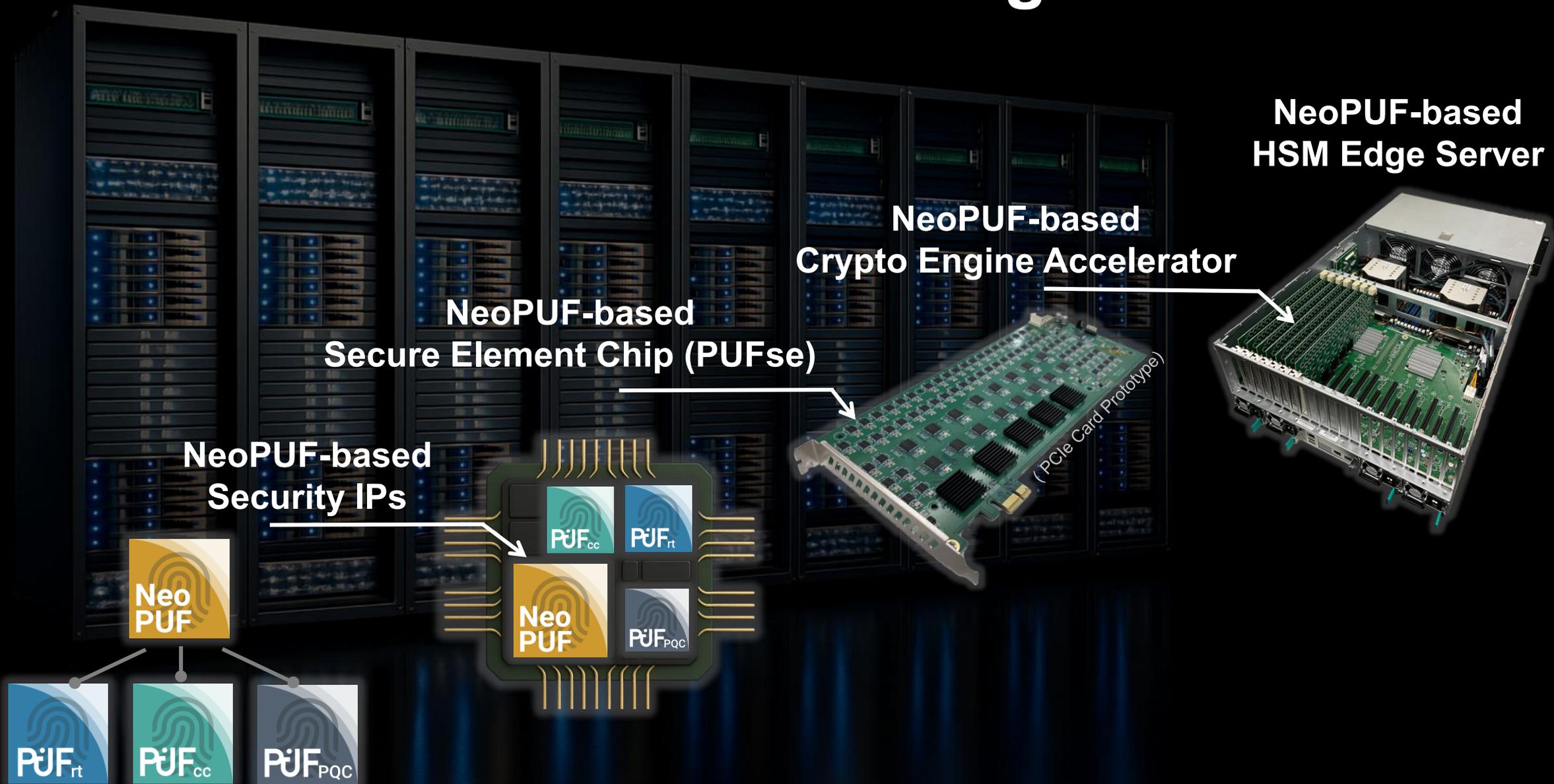| Assess | Choose PQC | Ensure Agility | PQC Testing | Migration | Monitor |

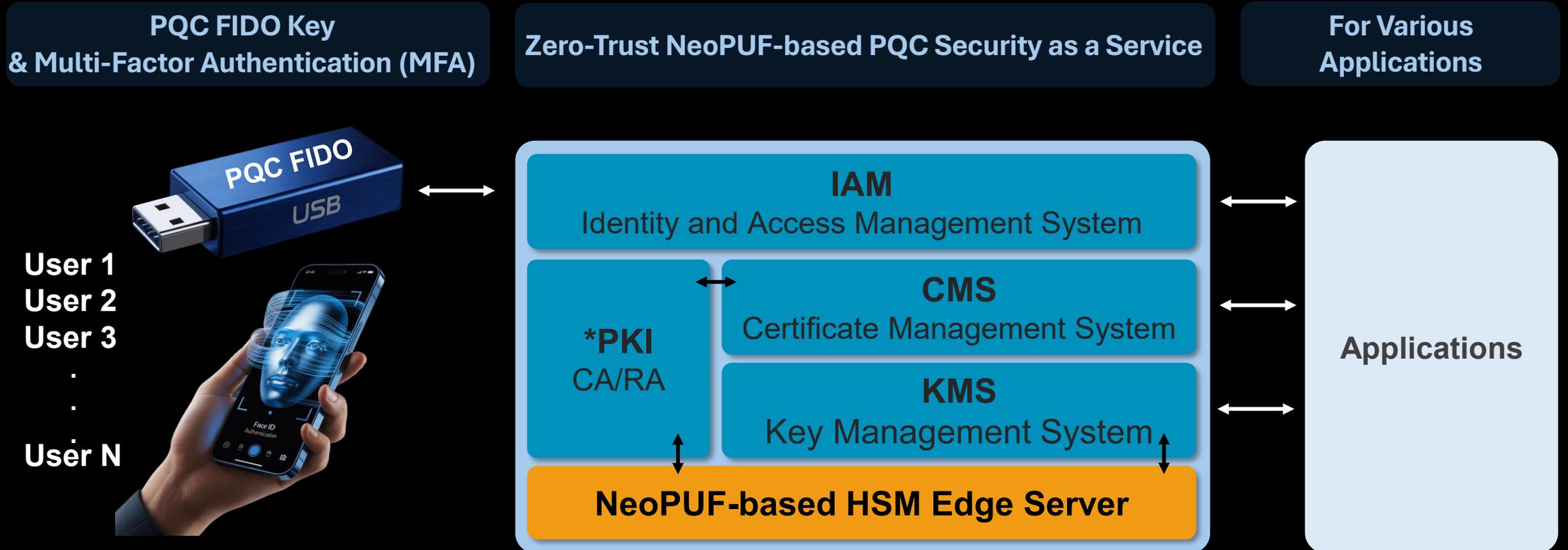Identify key databases
and prioritize upgrades

HSM must support PQC, ECC, RSA
(e.g., TLS, IPSec)

- **RSA → PQC**
- **ECC → PQC**
- **AES128 → AES256**

ememory

NeoPUF-based HSM Edge Server

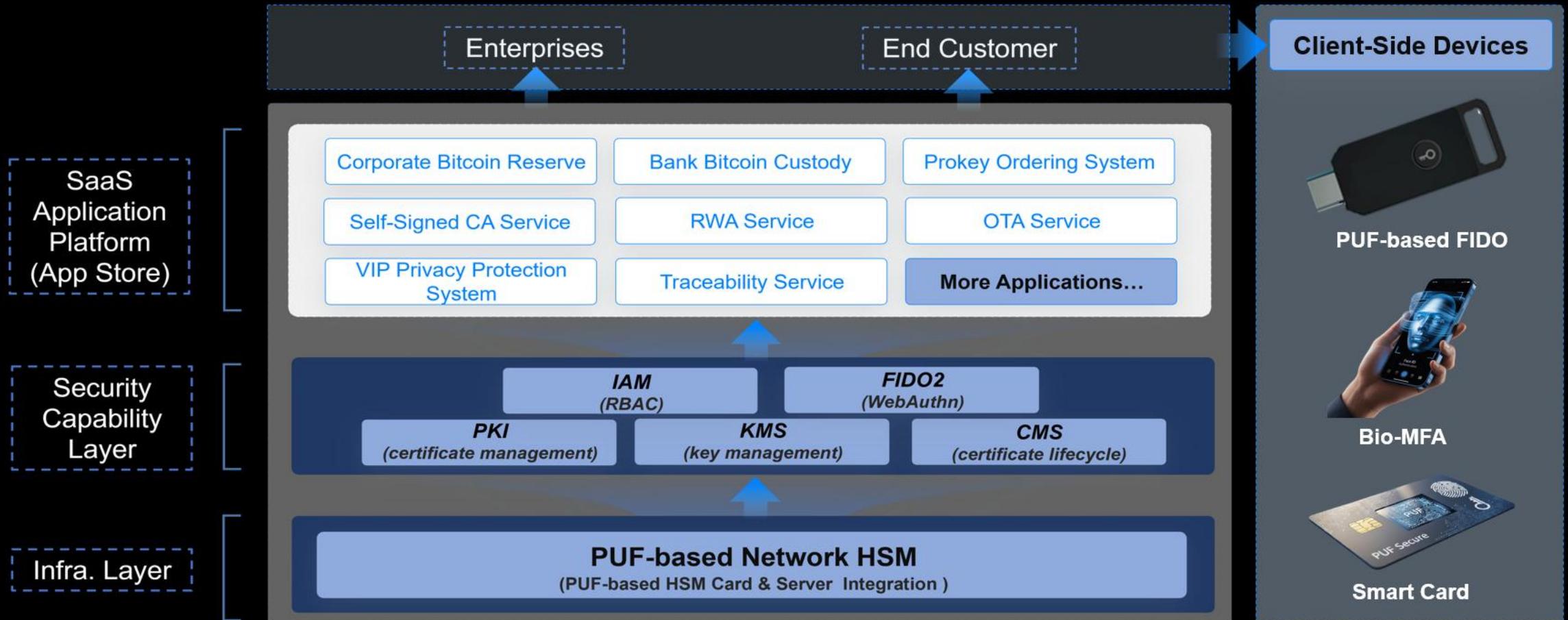NeoPUF-based
HSM Edge Server

NeoPUF-based
Crypto Engine Accelerator

NeoPUF-based
Secure Element Chip (PUFse)

(PCIe Card Prototype)

NeoPUF-based
Security IPs

Neo PUF

PÜF_cc   PÜF_rt

Neo PUF   PÜF_PQC

PÜF_rt   PÜF_cc   PÜF_PQC

33

ememory

NeoPUF-based PQC Security as a Service

PQC FIDO Key
& Multi-Factor Authentication (MFA)

Zero-Trust NeoPUF-based PQC Security as a Service

For Various
Applications

PQC FIDO

USB

User 1
User 2
User 3
.
.
.
User N

IAM
Identity and Access Management System

CMS
Certificate Management System

PKI
CA/RA

KMS
Key Management System

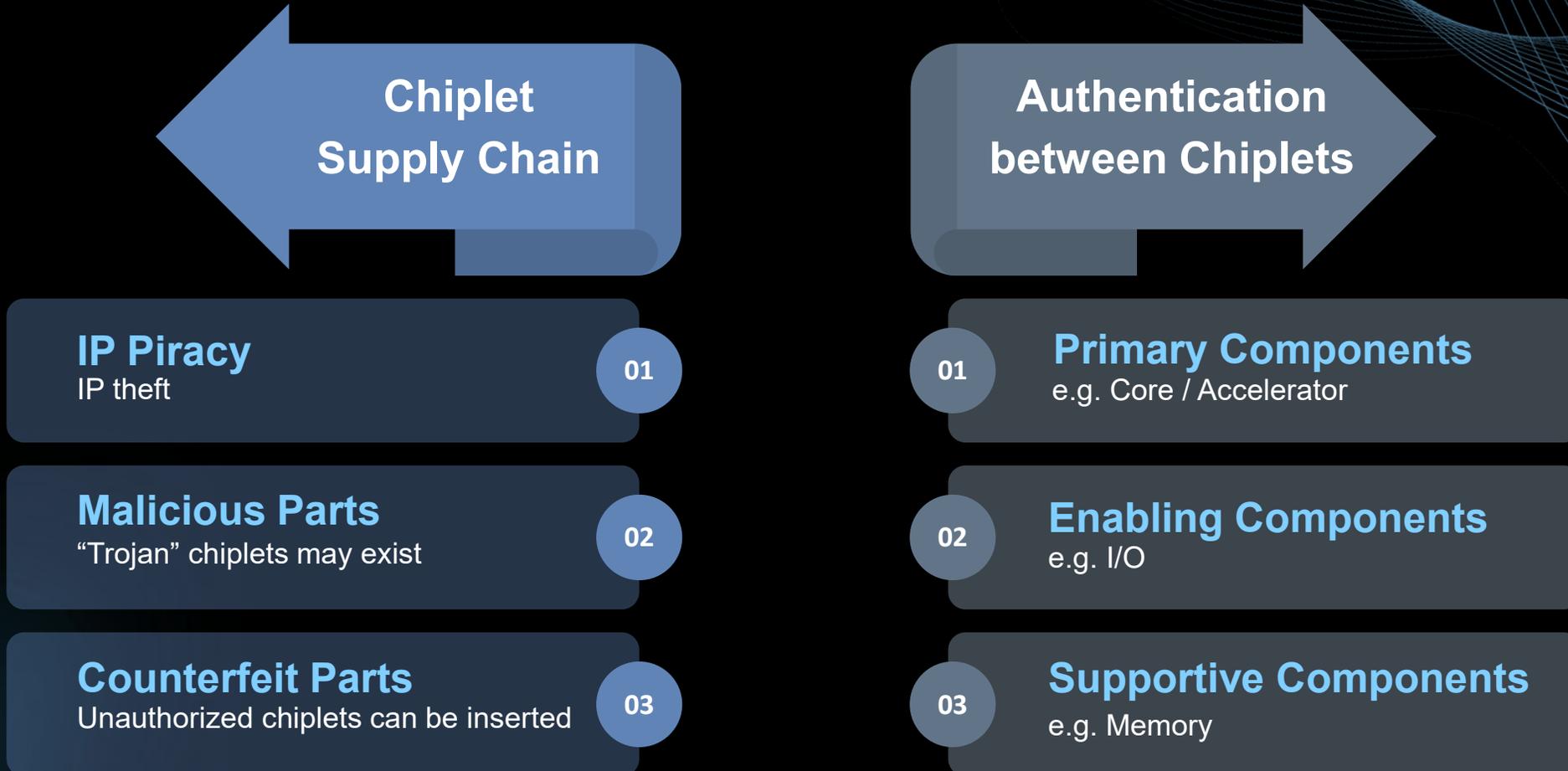**NeoPUF-based HSM Edge Server**

Applications

*Note — PKI: public key infrastructure / CA: certificate authority / RA: registration authority

34

ememory

NeoPUF-based Hardware Security as a Service Ecosystem

- Starting from a hardware-secure foundation and a software-secure platform, we unlock value by embedding security natively in every service workflow.
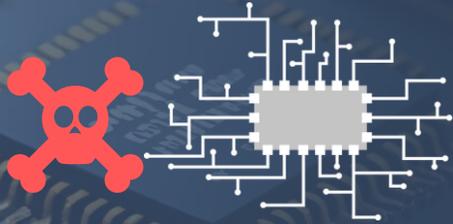
Enterprises **End Customer** **Client-Side Devices**

SaaS Application Platform (App Store)

Corporate Bitcoin Reserve	Bank Bitcoin Custody	Prokey Ordering System
Self-Signed CA Service	RWA Service	OTA Service
VIP Privacy Protection System	Traceability Service	More Applications…

PUF-based FIDO

Security Capability Layer

IAM *(RBAC)* **FIDO2** *(WebAuthn)*

PKI *(certificate management)* **KMS** *(key management)* **CMS** *(certificate lifecycle)*

Bio-MFA

Infra. Layer

PUF-based Network HSM
(PUF-based HSM Card & Server Integration)

Smart Card

ememory

Security Challenges in Chiplets

Chiplet Supply Chain

Authentication between Chiplets

IP Piracy
IP theft
01

01
Primary Components
e.g. Core / Accelerator

Malicious Parts
"Trojan" chiplets may exist
02

02
Enabling Components
e.g. I/O

Counterfeit Parts
Unauthorized chiplets can be inserted
03

03
Supportive Components
e.g. Memory

NeoPUF for Supply Chain Securiy

Design	Fab./ Packaging	Deployment
IP Piracy	**Malicious Parts**	**Counterfeit Parts**
NeoPUF	NeoPUF	NeoPUF
Built-in HUK, eliminating the need for key injection	Each component carries a PUF UID for device management	Keys & certificates generated by the PUF assist in supply chain management
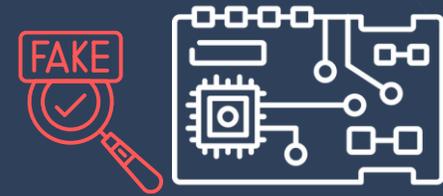
Authentication between Chiplets

	Security Requirment	Hardware Root of Trust	Authentication Scheme
✔ Primary Components	**High**	• Anti-Tampering • Secure Storage • Unique ID • TRNG	• Two-way Authentication • Asymmetric Crypto
✔ Enabling Components	**Moderate**	• Anti-Tampering • Secure Storage • Unique ID • TRNG	• One-way Authentication • Symmetric Crypto
✔ Supportive Components	**Basic**	• Anti-Tampering • Secure Storage	• One-way Authentication • Symmetric Crypto

NeoPUF-based Solutions
for Chiplet Security

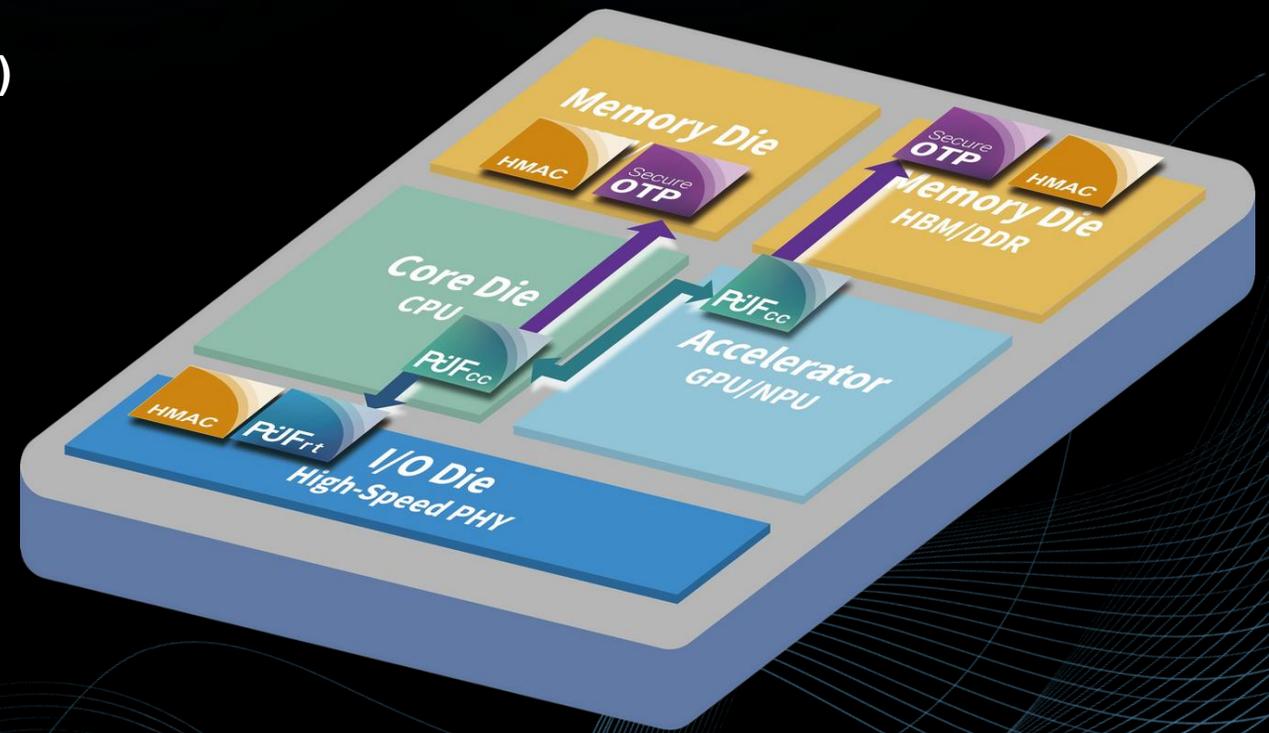**Cryptographic Accelerator**
 (One-way symmetric authentication)

Secure Storage
 (For key / certificates)
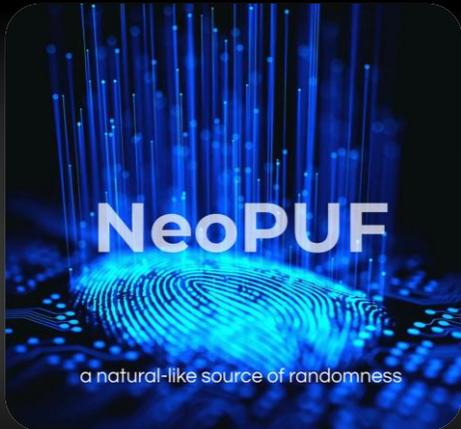
Hardware Root of Trust
 (UID / Key)

Crypto Coprocessor
(Two-way asymmetric authentication)
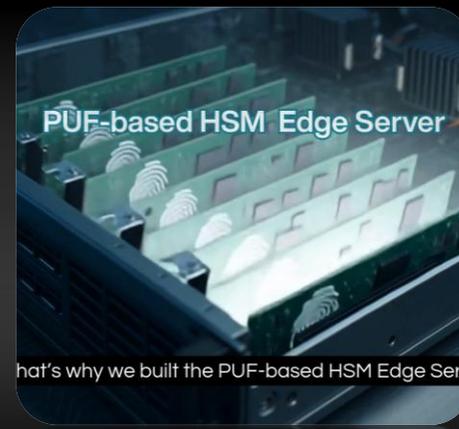
Video Showcase of Our Future Innovation .

👇 **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.**
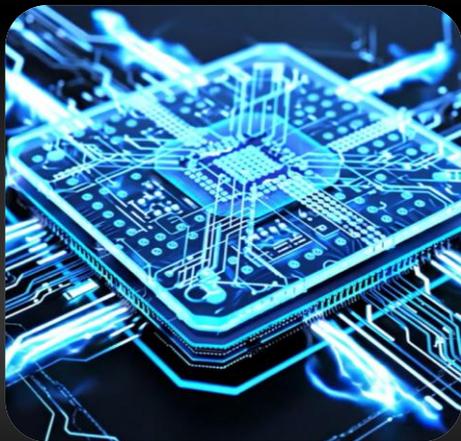
Chiplet Supply Chain Secured by NeoPUF

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/

ememory