

# 力旺電子 Briefing .

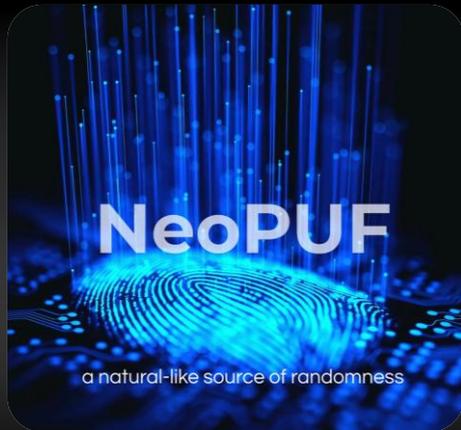
**ememory**

# 智慧財產權 聲明 ■

All rights, titles and interests contained in this information, texts, images, figures, tables or other files herein, including, but not limited to, its ownership and the intellectual property rights, are reserved to eMemory Technology Incorporated and PUFsecurity Corporation. This information may contain privileged and confidential information. Any and all information provided herein shall not be disclosed, copied, distributed, reproduced or used in whole or in part without prior written permission of eMemory Technology Incorporated or PUFsecurity Corporation.

# 未來創新成果展示

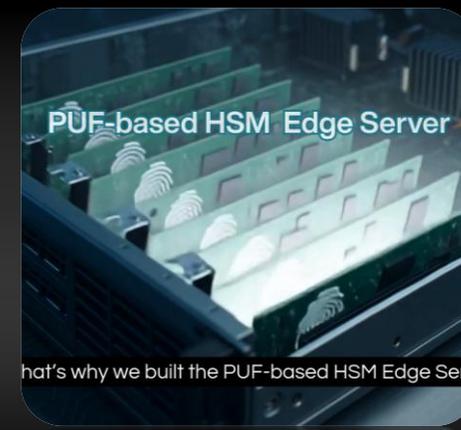
Click on the image to watch the video.



## NeoPUF – The Holy Grail of Security

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

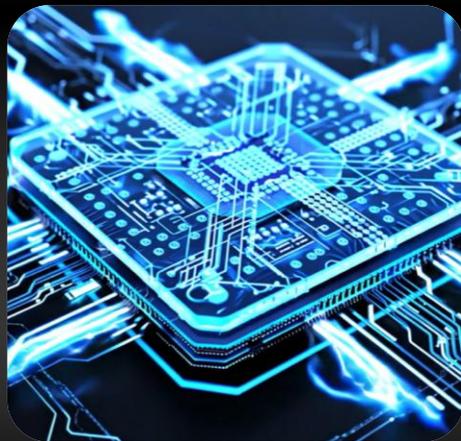
Click on the image to watch the video.



## 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

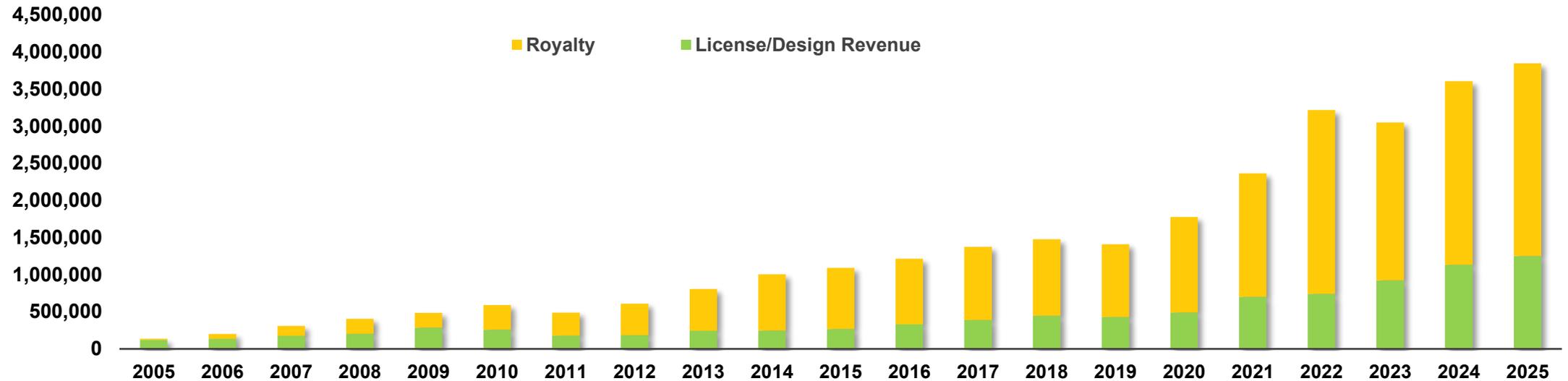
Powering the trusted core of next-generation defense security.

# 公司介紹

- eMemory is the global leader of embedded non-volatile memory IP

## Revenue Trend

(Unit: NT\$ 1,000)



**Founded**  
In 2000

Based in Hsinchu, Taiwan.  
IPO in 2011. Over 74M wafers shipped.

**1350+**  
Patents Issued

228 pending patents. 342 employees with 73% R&D personnel.

**Best IP Partner**  
With TSMC

TSMC Best IP Partner Award since 2010.

# 公司產品技術



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.

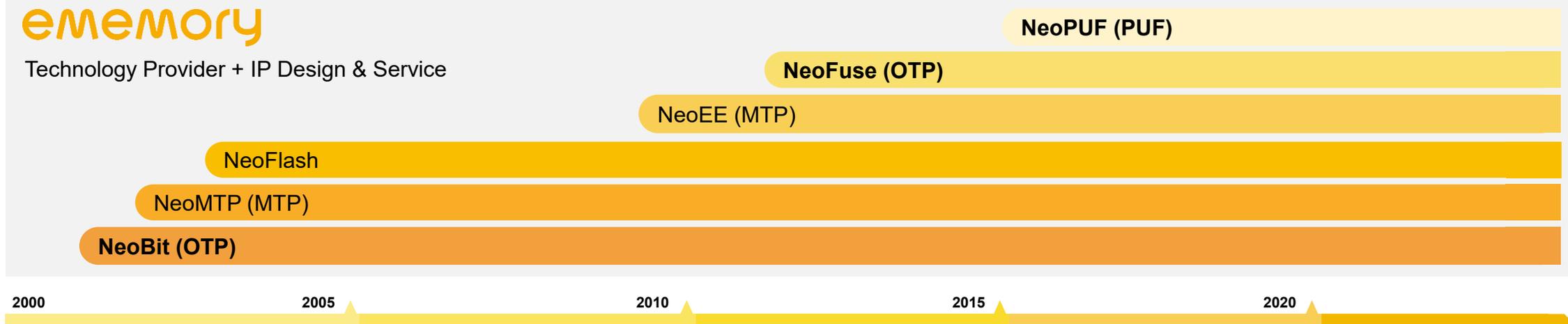
## PUFsecurity

PUF-based Security IP Design & Service



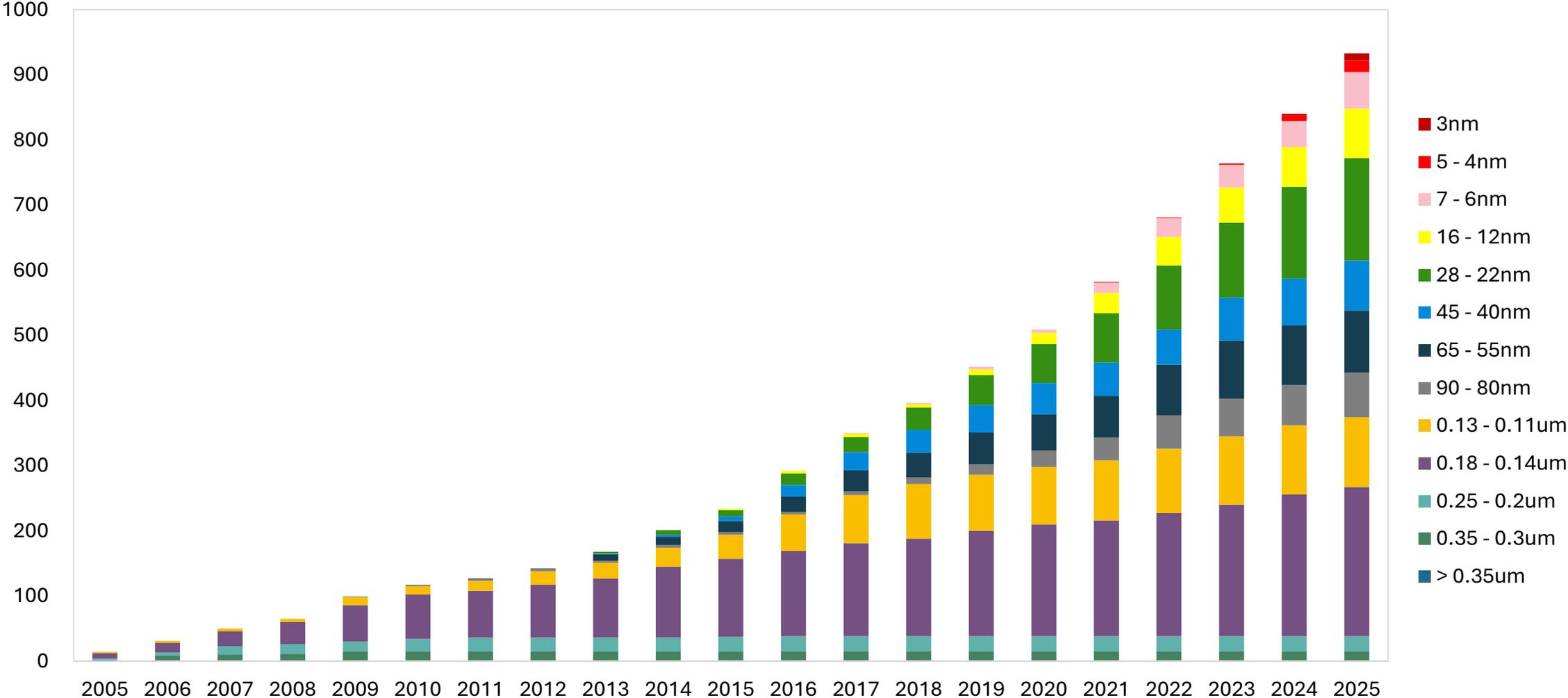
## eMemory

Technology Provider + IP Design & Service



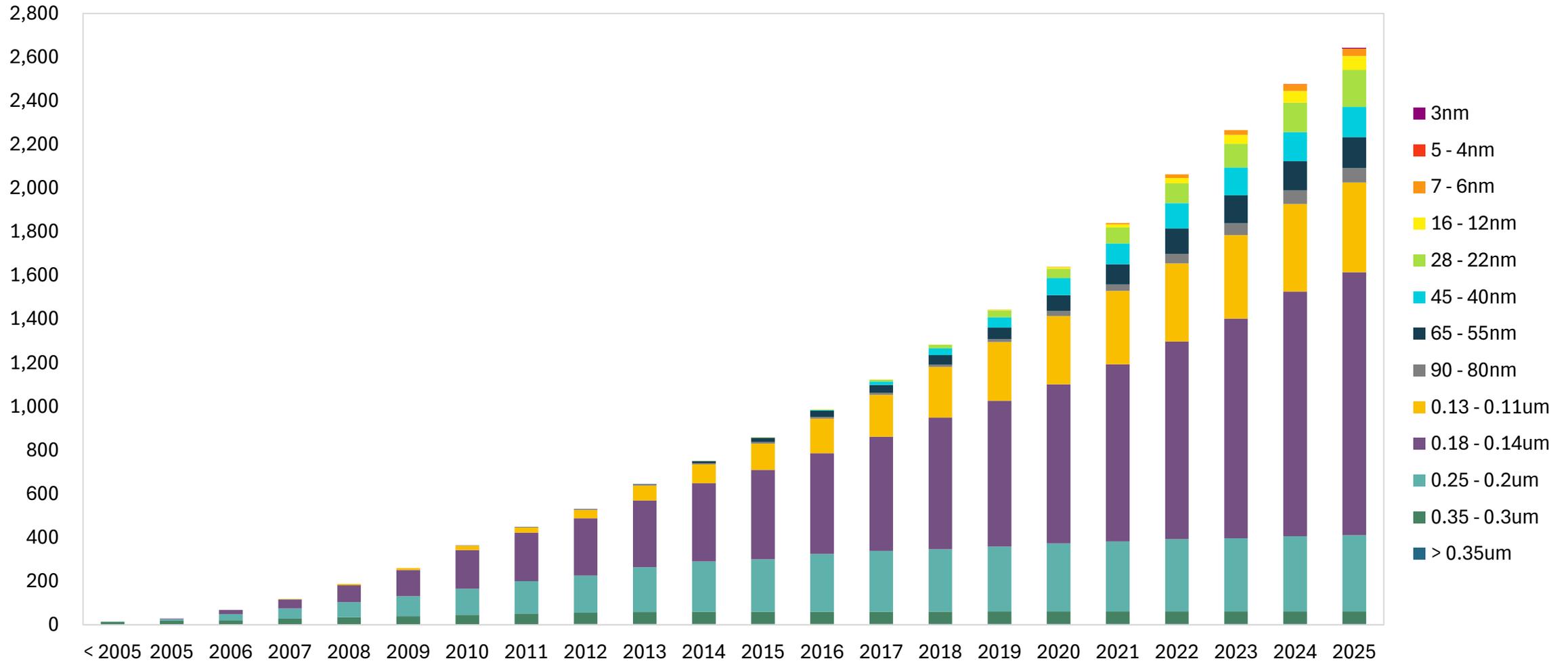
# Registered IPs at TSMC

## Registered IP > 850



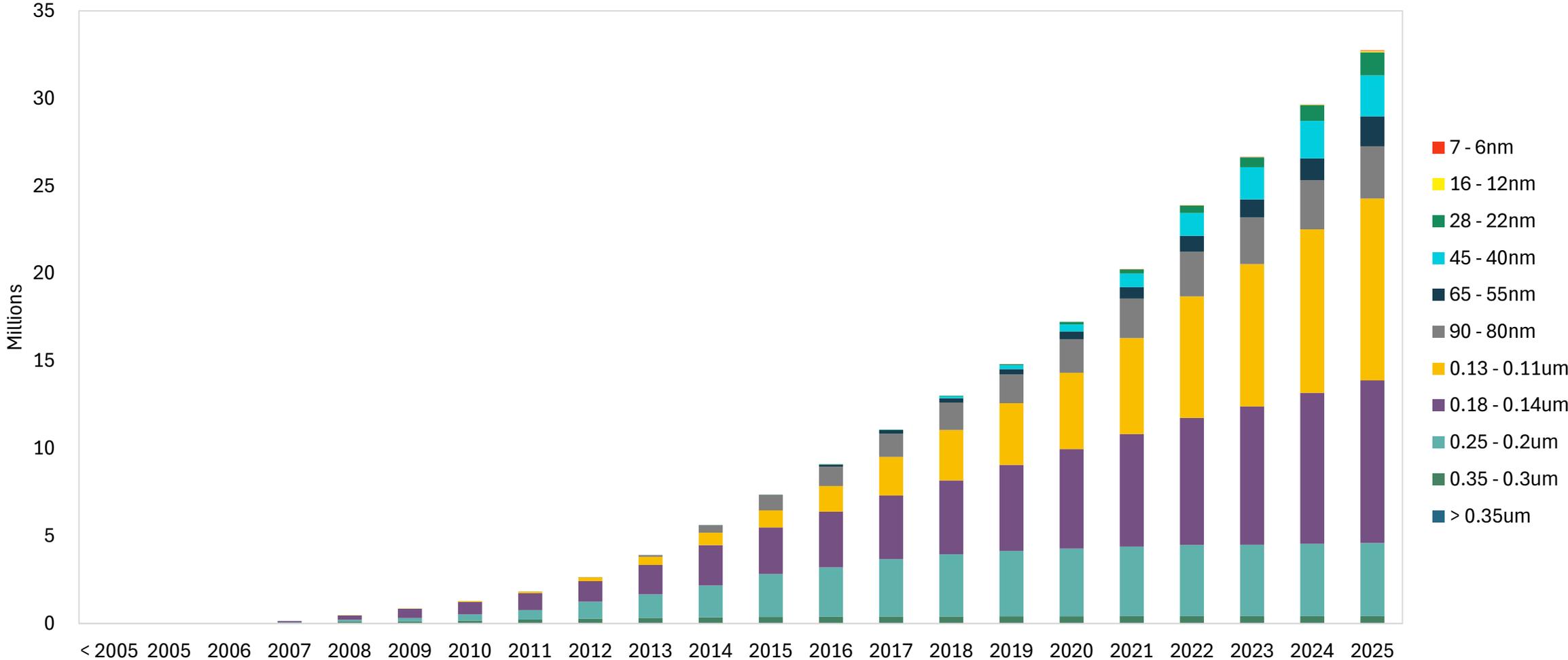
# NTOs at TSMC

## New Tape Out Contribution > 2600



# Wafer Contribution at TSMC

## 8" Wafer Contribution > 25M



# Revenue and Tape-out by Technology

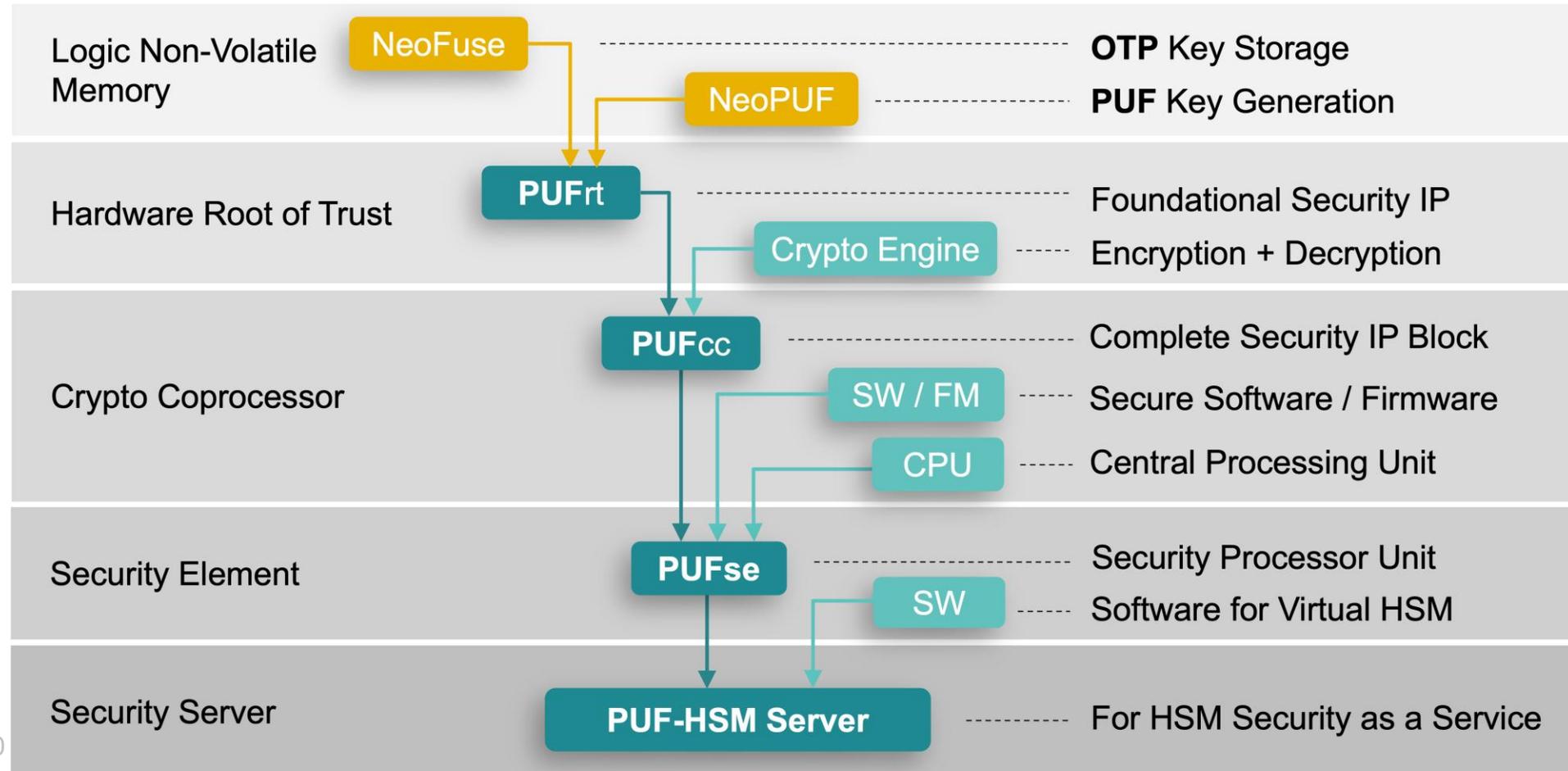
Year	NTO		Revenue (USD)		
	NeoBit	NeoFuse	NeoBit	NeoFuse	PUF-based
2002	3				
2003	29				
2004	40				
2005	68		\$ 4,217,380		
2006	133		\$ 6,202,270		
2007	220		\$ 9,402,479		
2008	253		\$ 12,896,211		
2009	268		\$ 11,695,587		
2010	284		\$ 15,873,331		
2011	254		\$ 15,399,098		
2012	270		\$ 19,620,768		
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
<b>Total</b>	<b>5,382</b>	<b>1,730</b>	<b>\$ 482,412,457</b>	<b>\$ 384,164,465</b>	<b>\$ 23,383,735</b>

\*NTO stands for **New Tape-Out**  
page 9

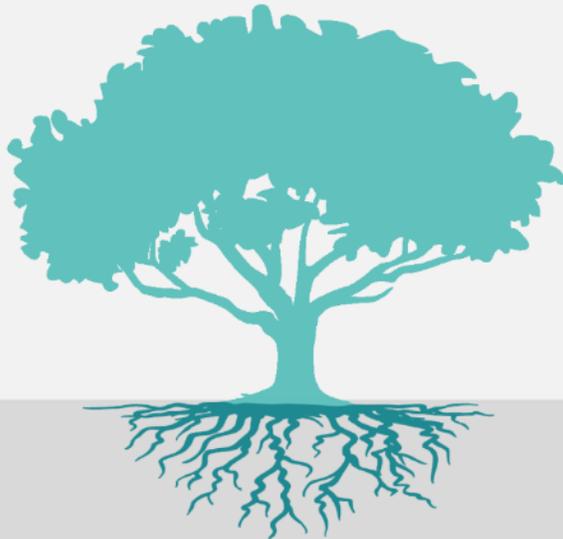
\* Revenue includes both **licensing** and **royalty**

# 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



# The Foundation of the Security Ecosystem ■



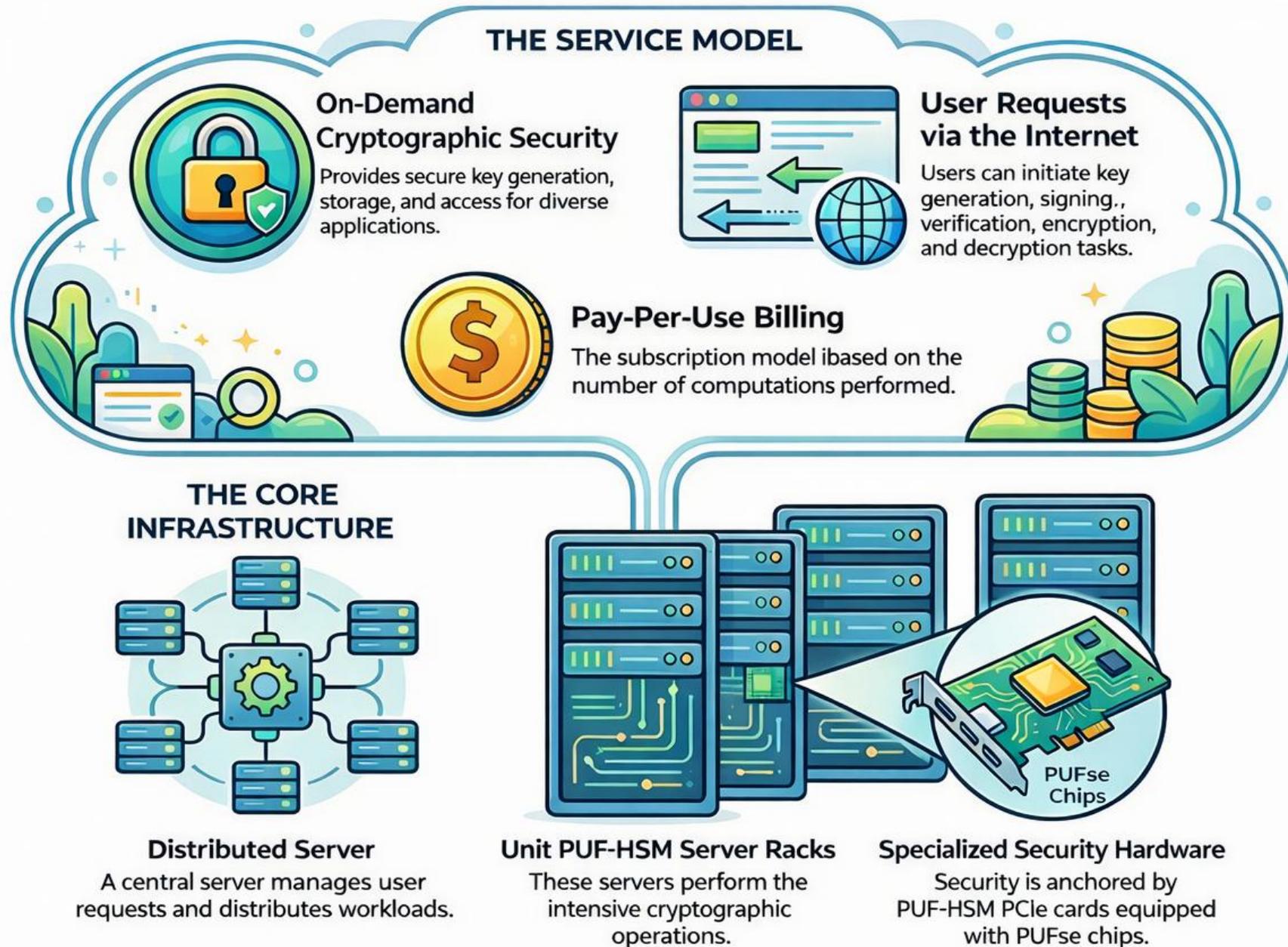
## ← Software Security Ecosystem

- 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

# How Distributed PUF-HSM as a Service Works



# 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

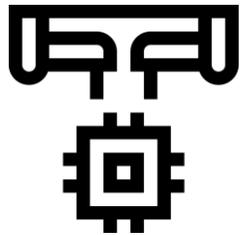


IoT

# 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

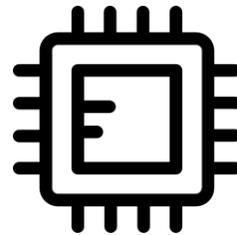
## Foundry Platforms



TSMC, Intel, UMC, GF, etc.

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

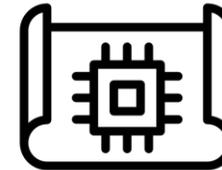
## CPU Partners



Arm, RISC-V, Cadence, etc.

- SoC customers looking for both CPU and security subsystems

## CSP



More to come

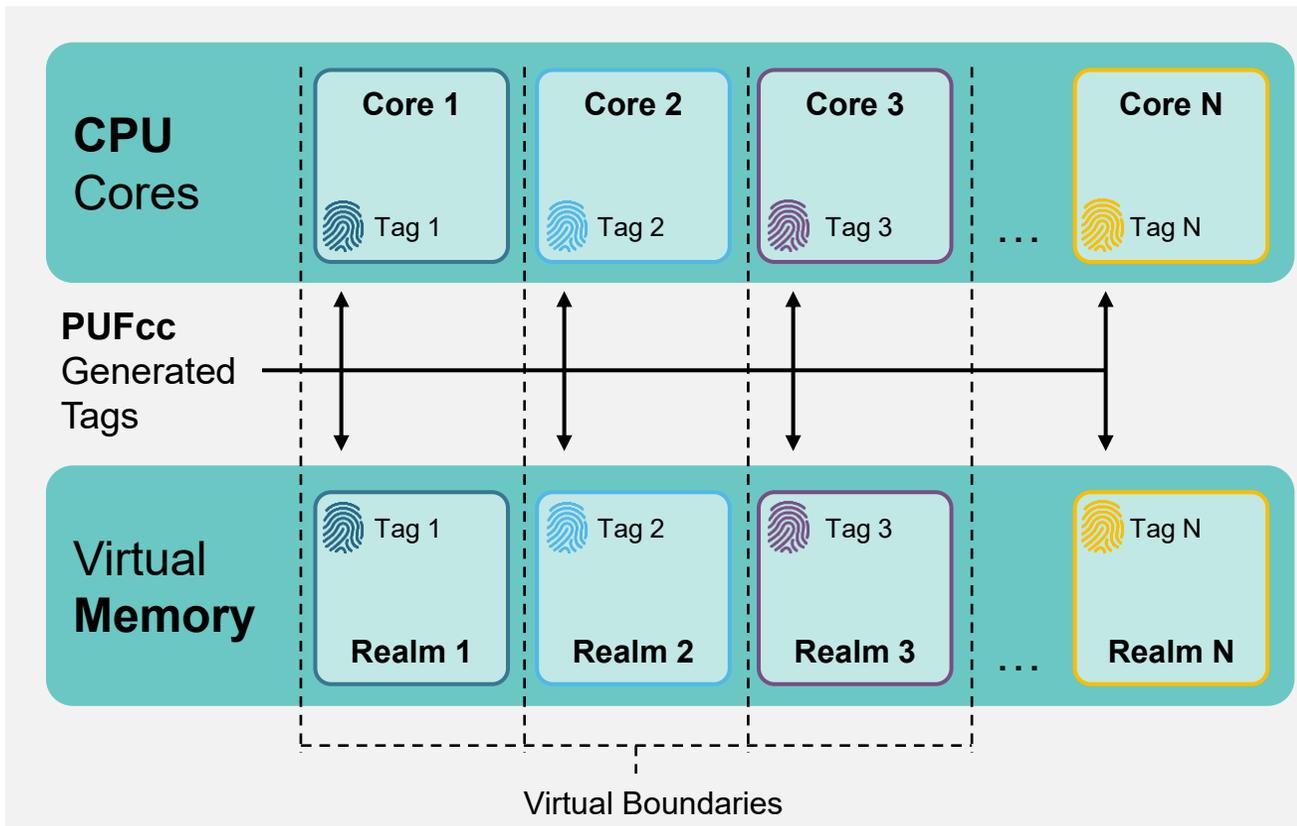
- Work with CSP and system companies for embedded security on a chip level

# Market Application ■

- Customers with many different applications will begin to adopt **PUF-based Security Solutions**

CPU	AI	SSD
DPU	DTV/STB	Wi-Fi
FPGA	ISP	And More.

# Next Computing: Confidential Computing

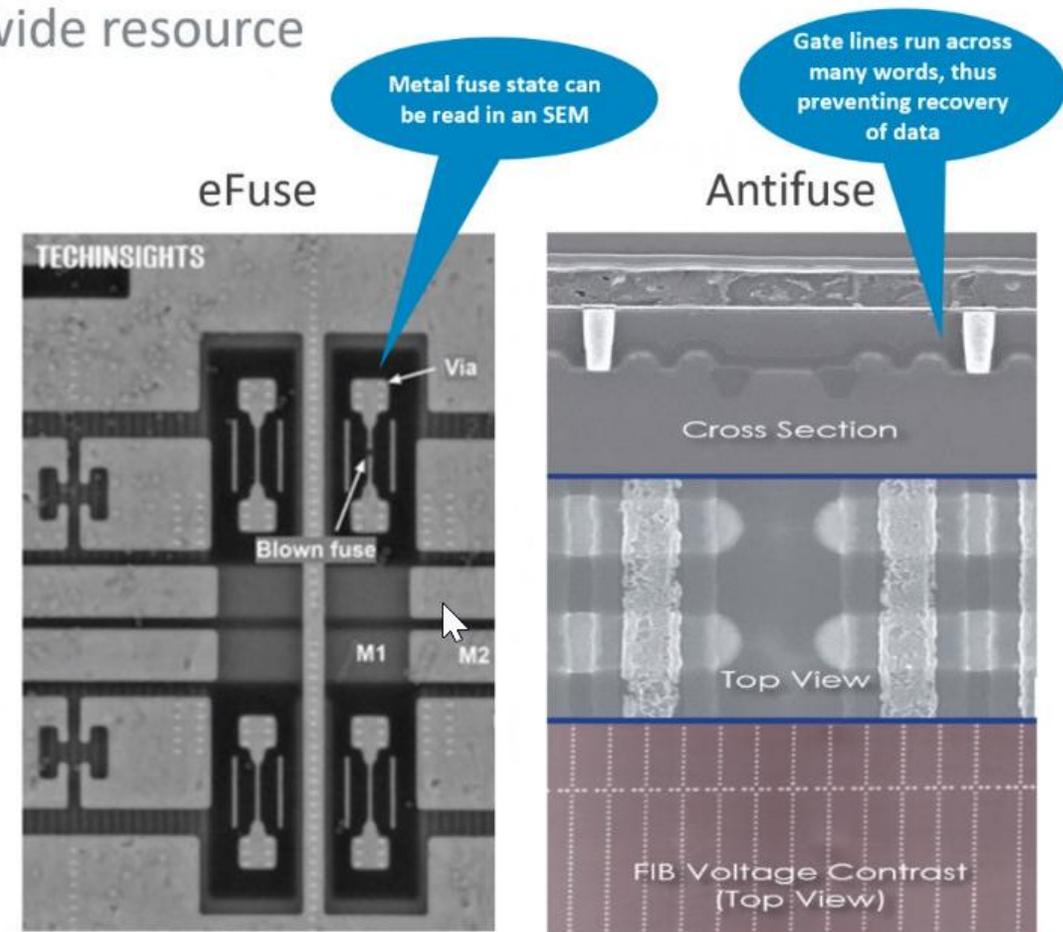


- **Protect data** in the Virtual Memory of Multi-Core CPUs
- CPU Cores and Virtual Memory have unique corresponding **tag numbers**
- Tag numbers are internally **randomly generated** by **PUFcc** (Crypto Coprocessor IP)

# AntiFuse OTP vs. eFuse

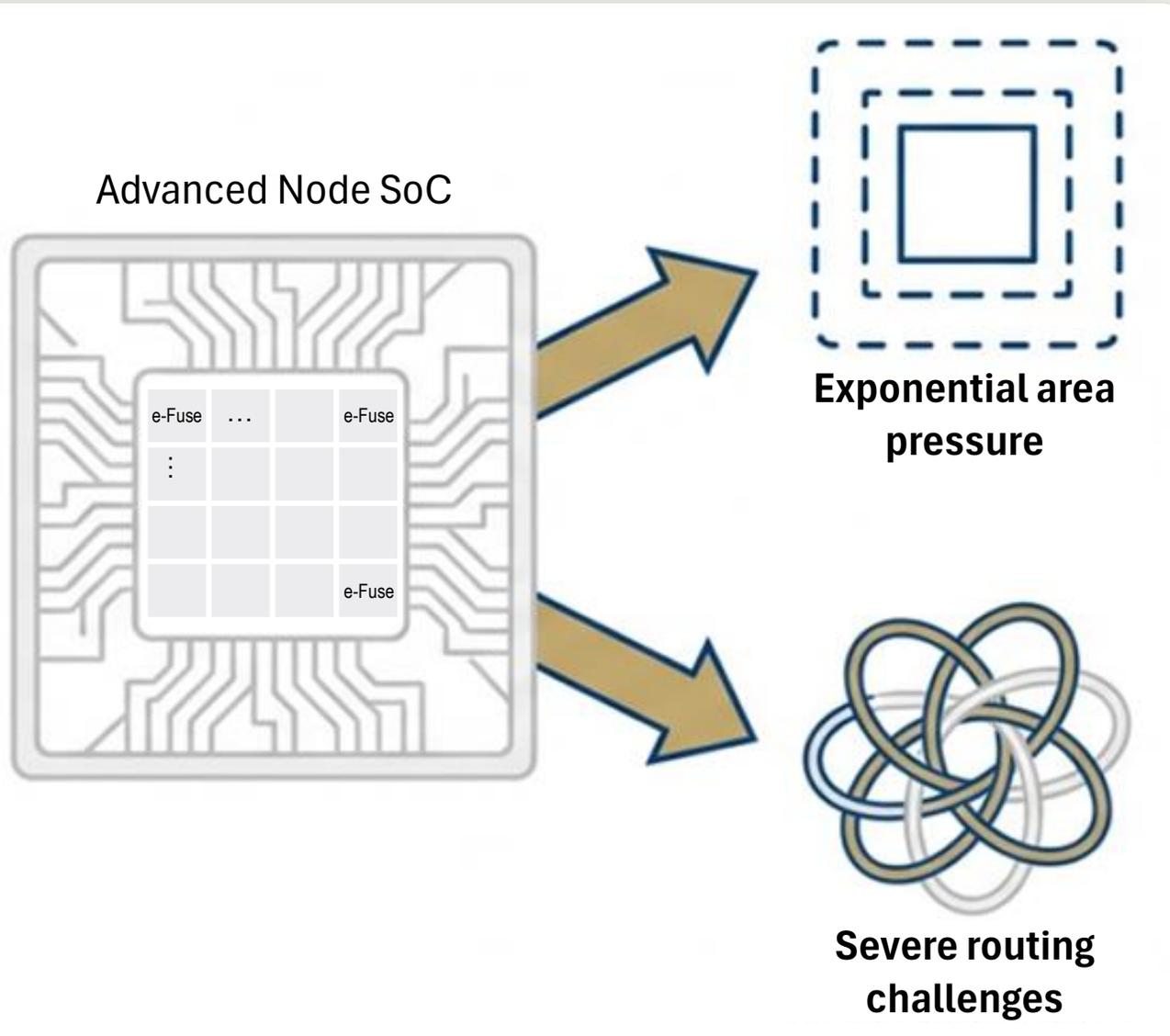
One Time Programmable (OTP) memory is a SoC-wide resource

- 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
    - ~0.04mm<sup>2</sup> on 7nm for 128x32 bit PUF



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

# Advanced Nodes Amplify the Structural Limitations of e-Fuse



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.

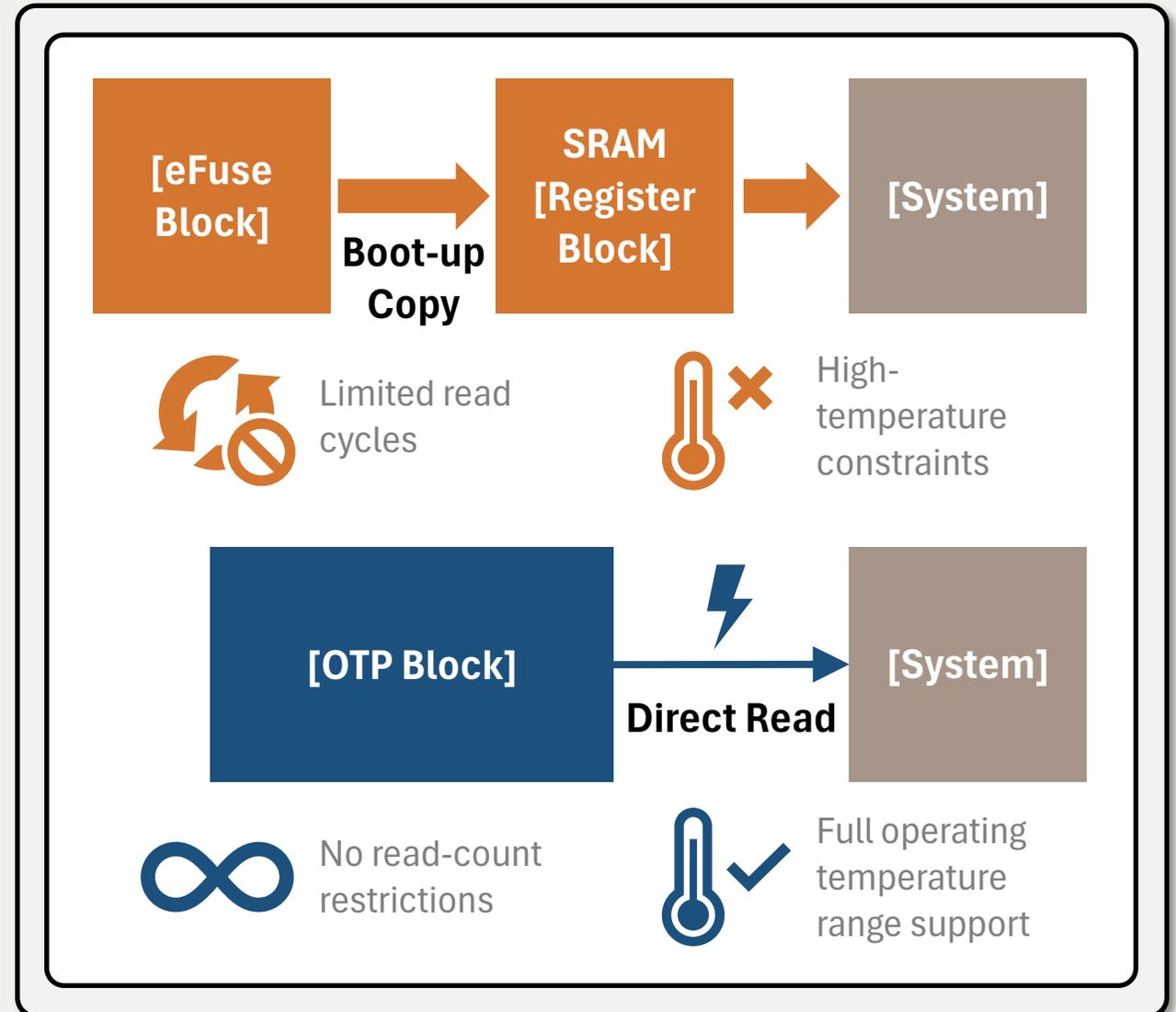
# Multi-e-Fuse Architectures Impose High Costs in Area, Power, and Efficiency

## 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**



16 x 2Kx8 e-Fuse

**OTP**

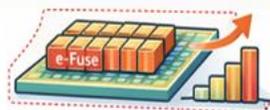
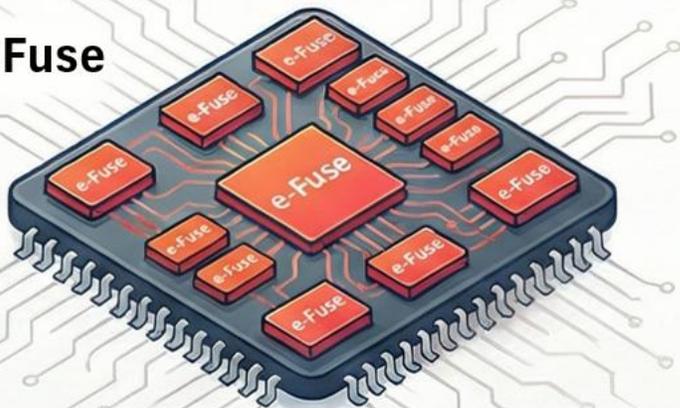


1 x 32Kx8 OTP

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 mm <sup>2</sup>	0.33 mm <sup>2</sup>	-
Total area	~1.92 mm <sup>2</sup>	0.33 mm <sup>2</sup>	<b>&gt;80% area reduction with OTP</b>
Additional SRAM / registers	Required	Not required	Further savings in area and power

# 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

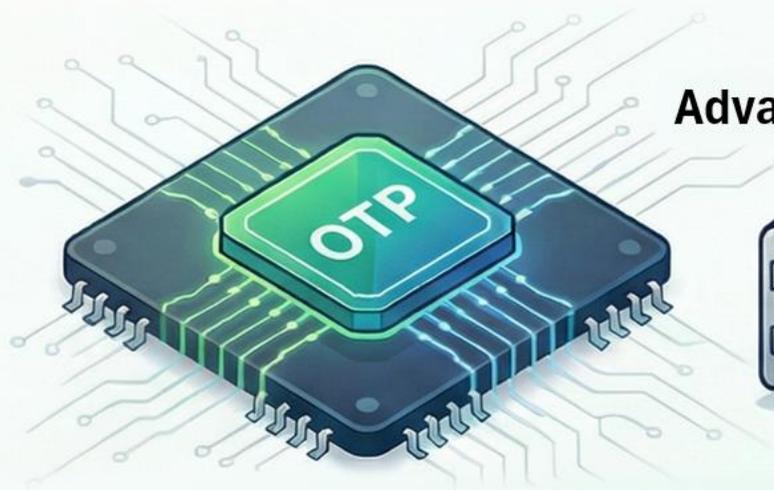
- Limited read cycles
- High-temperature operating constraints
- Mandatory boot-time data copy to SRAM



### Weaker native security

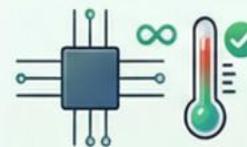
Sensitive data typically requires additional encryption mechanisms, increasing system complexity.

## Advantages of OTP



### Lower area and cost

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

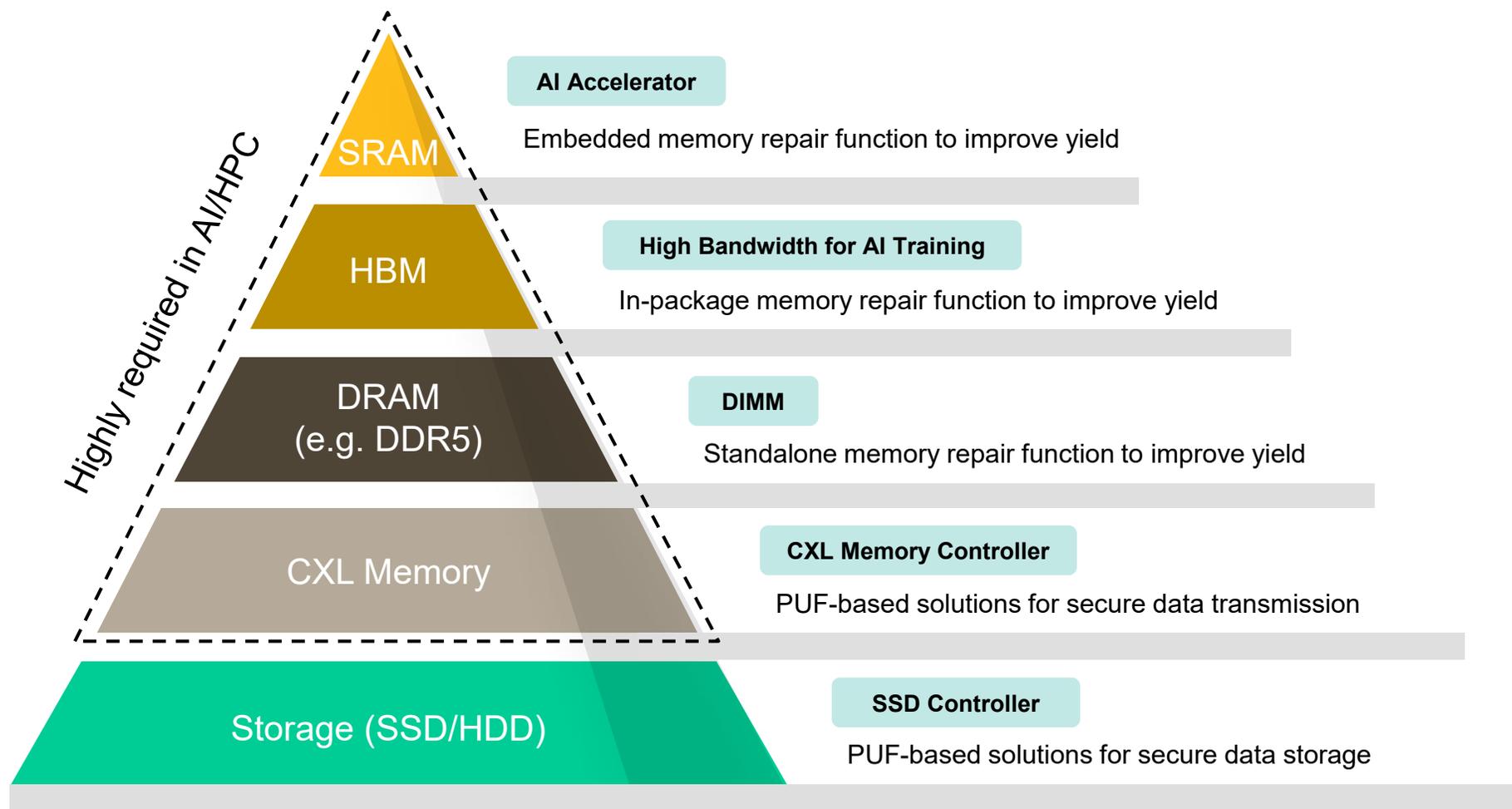


### Integrated security capabilities

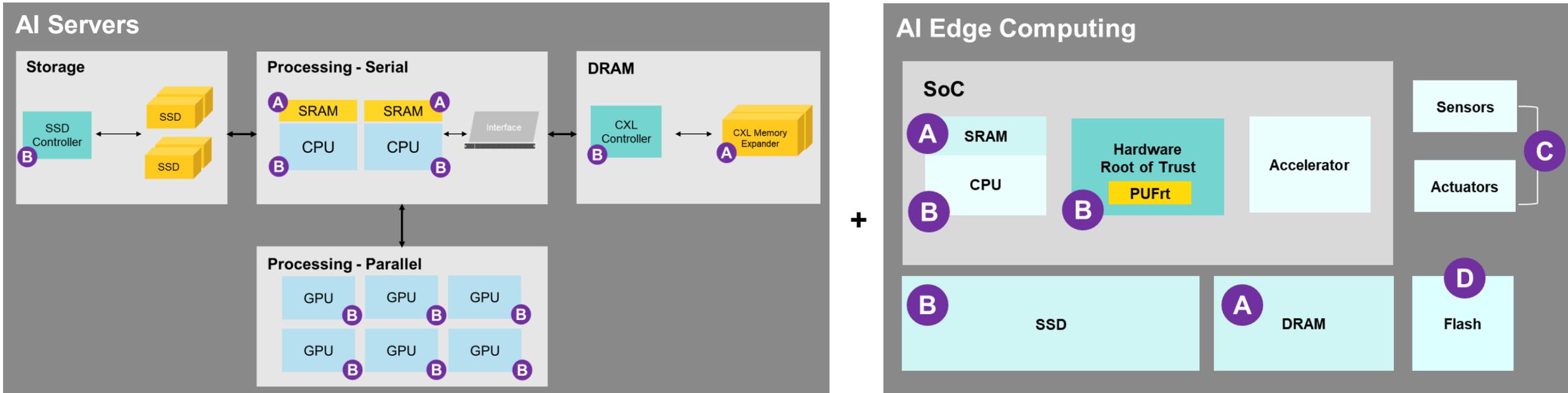
OTP can be natively combined with **PUF and TRNG**, enabling a more **complete hardware-root-of-trust solution**.

# eMemory Helps Memory.

- eMemory's security IP and OTP/MTP IP 1) ensure data security and 2) improve yield for SRAM, HBM and DRAM.



# eMemory for AI Servers and Edge Devices



**A Memory Repair**

**B Root of Trust** provides:

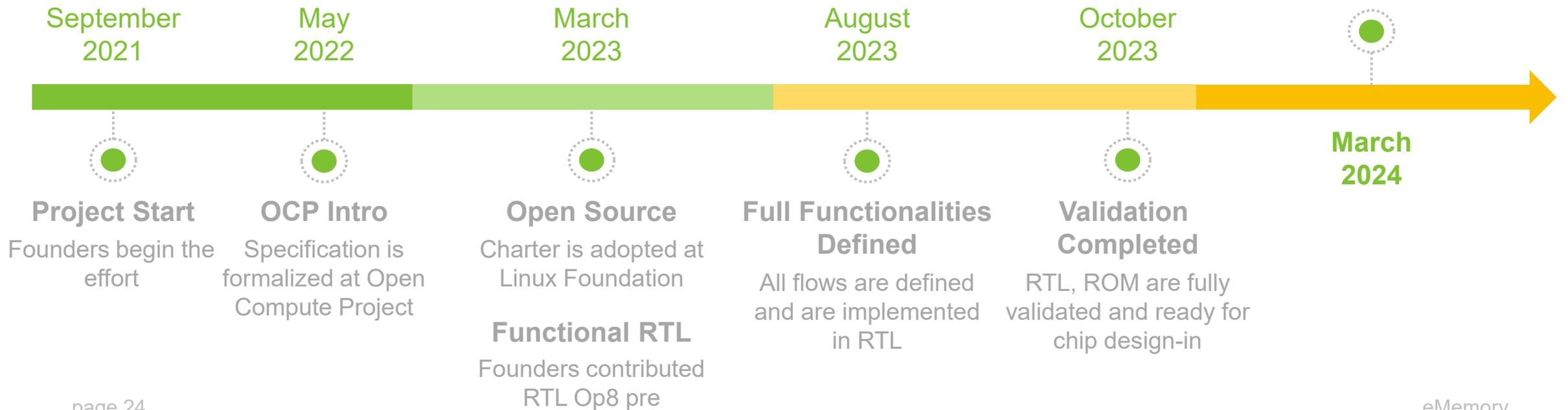
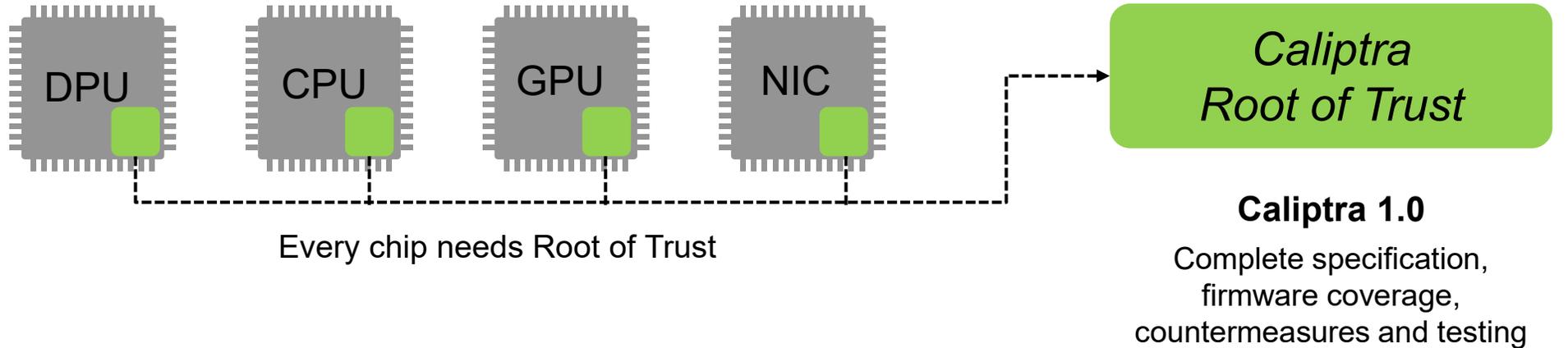
1. Key storage/generation
2. Cryptographic processing to protect AI models, input data and output results
3. Confidential Computing

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

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

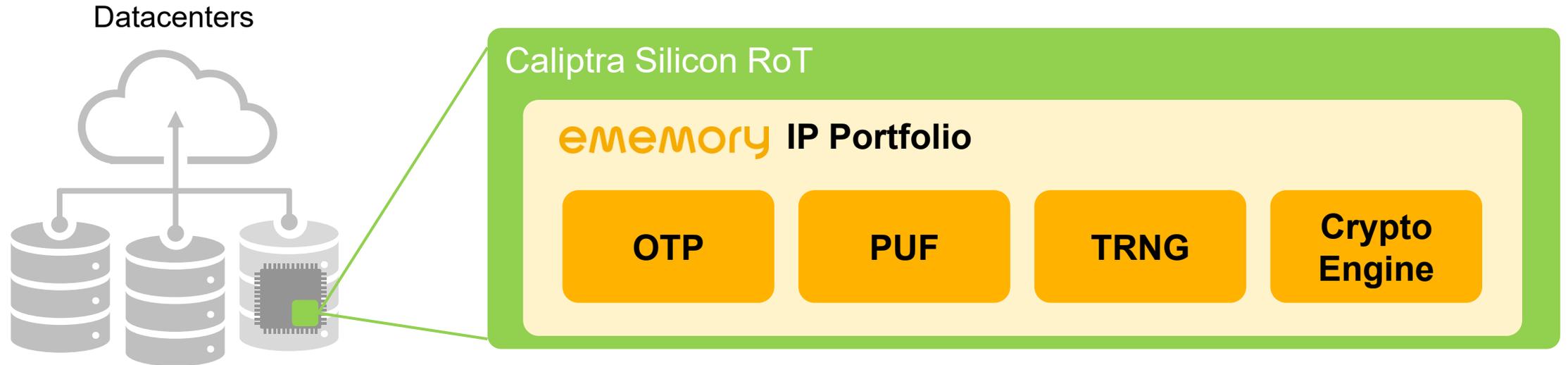
# Why is Caliptra so Important? ■

## Datacenter Chips



# What is the Important Role of eMemory in Caliptra?

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



## Unique Chip Identity



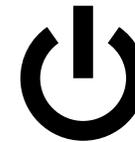
Chip Fingerprint

## Secure Attestation



Device Certificate

## Secure Boot

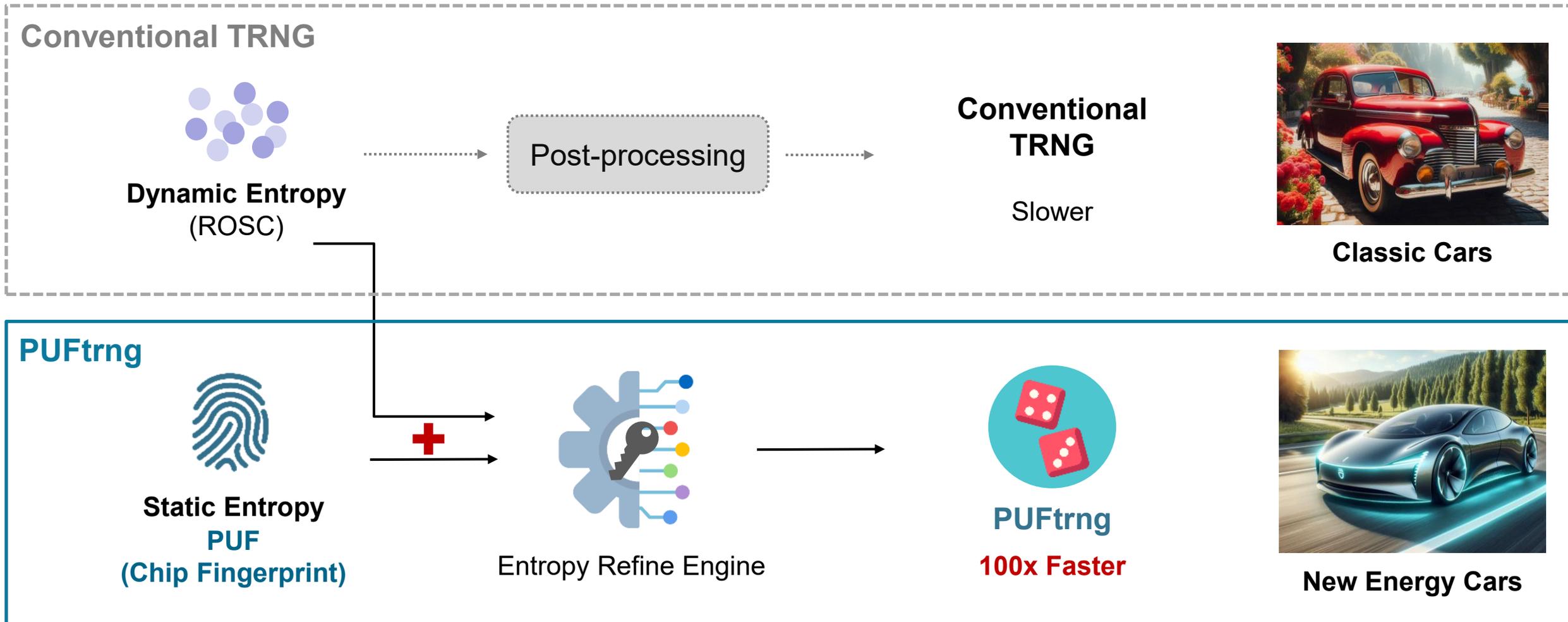


Boot into Trusted Operating System

# PUFtrng: 100 Times Faster than Conventional TRNG

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

*Similar to...*



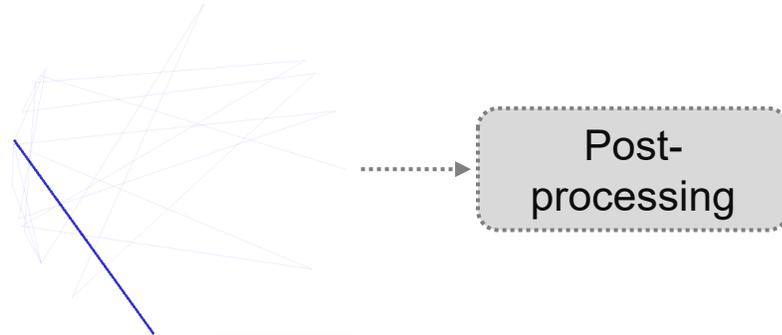
# PUFtrng: 100 Times Faster than Conventional TRNG

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

*Similar to...*

## Conventional TRNG

**Figure 1:**  
Dynamic Entropy



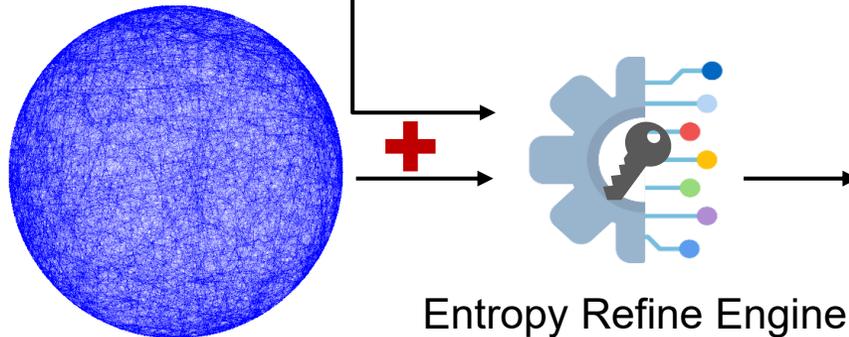
**Figure 2:**  
Conventional TRNG  
→ Low throughput random bits  
→ Slower



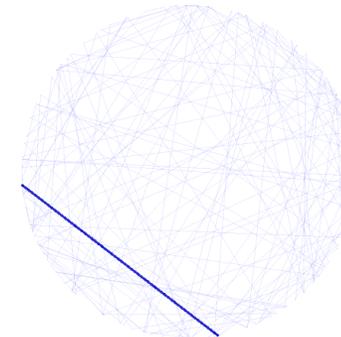
**Classic Cars**

## PUFtrng

**Figure 3:**  
Static Entropy  
→ **PUF**  
(chip fingerprint)



**Figure 4:**  
**PUFtrng**  
→ High throughput random bits  
→ **100x Faster**



**New Energy Cars**

# Why is **High-Density SRAM** needed in AI? ■

- To increase the speed of AI accelerators, **high-density SRAM** is needed for use in:

## Buffer Memory

- High-density SRAM helps improve data transfer speed and reduce energy costs by acting as a fast **intermediate storage** between different processing stages.

## AI Model Training

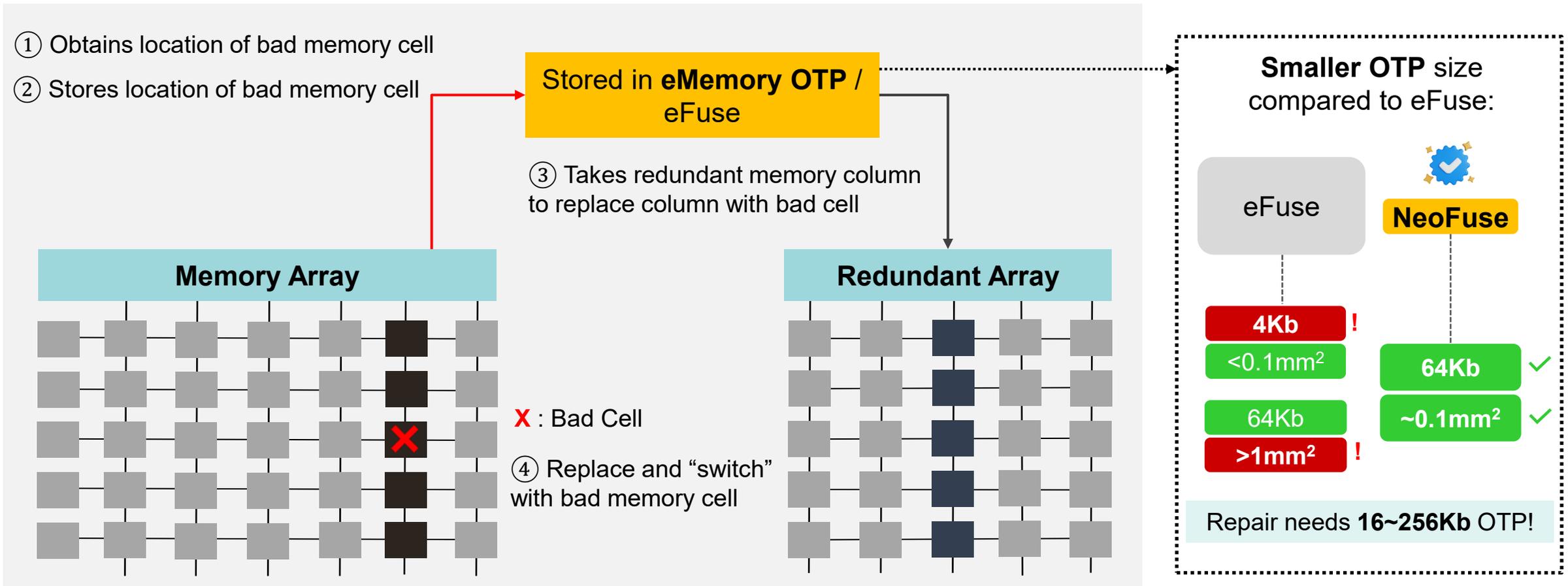
- High-density SRAM helps **store** vast amounts of data for AI accelerators to access quickly to speed up training.

## Computing in Memory (CIM) for Inference

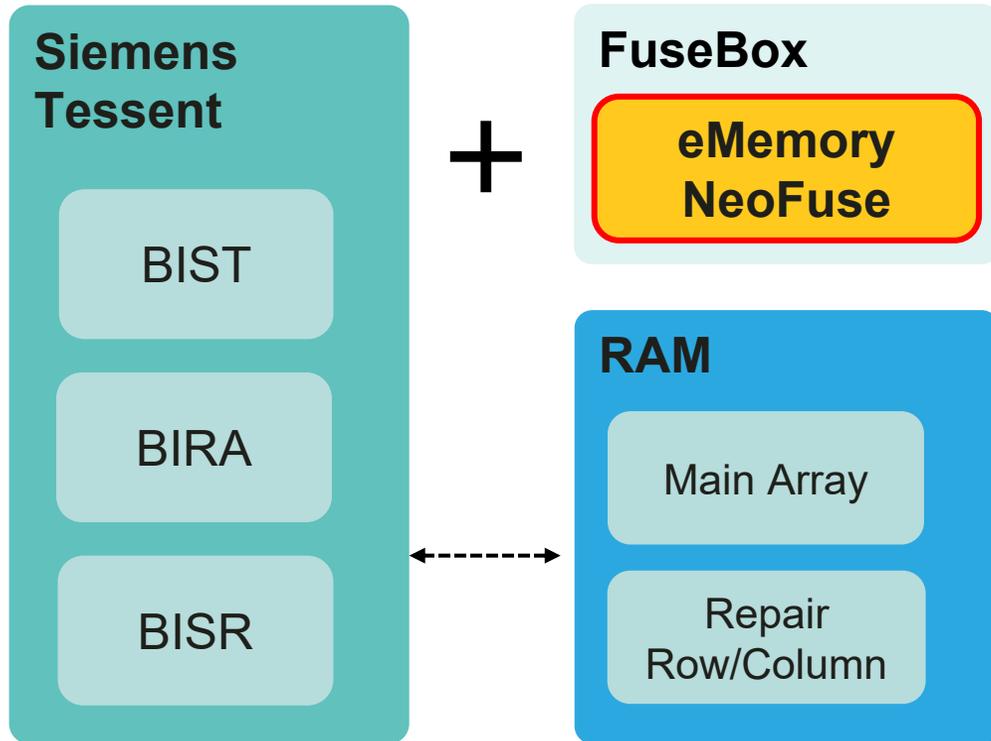
- High-density SRAM enables **in-memory computation** by storing large datasets and performing computations on them without transferring data to separate processors.

# eMemory enables High-Yielding SRAM

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



# Partnering for Success: eMemory and Siemens



*BIST = Built-in Self Test*

*BIRA = Built-In Redundancy Analysis*

*BISR = Memory Built-in Self Repair*

eMemory provides OTP with interface for Siemens MBIST:

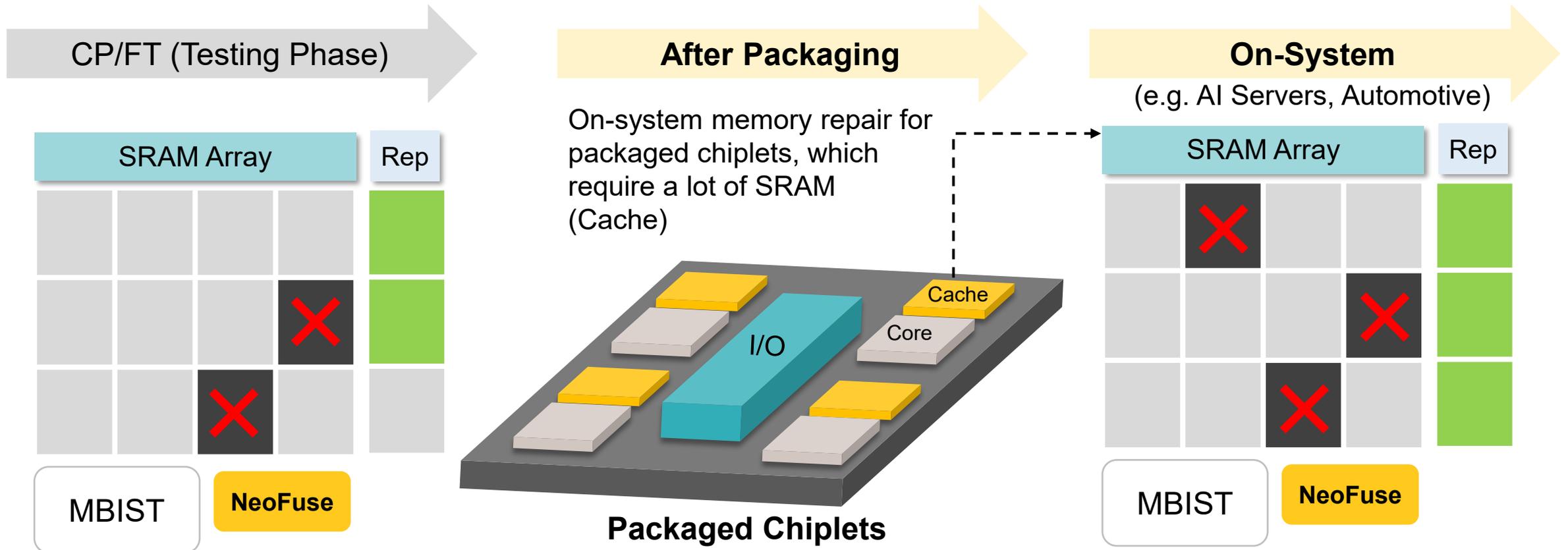
- **Tessent** provides memory BISR functions with BIST and BIRA
- **NeoFuse OTP** provides defect-free OTP using BIRA, BISR and adapter to Tessent
- **New MBISR**: Tessent MBISR + NeoFuse, scanning defective SRAM by word/column and logging to the OTP



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.

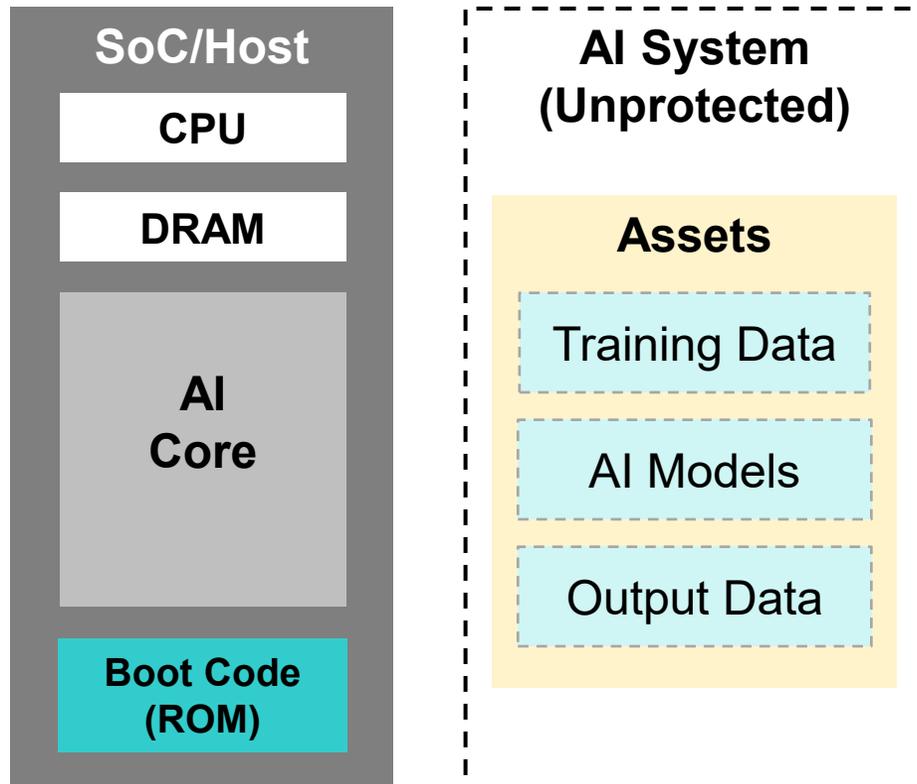


Made possible with MBIST

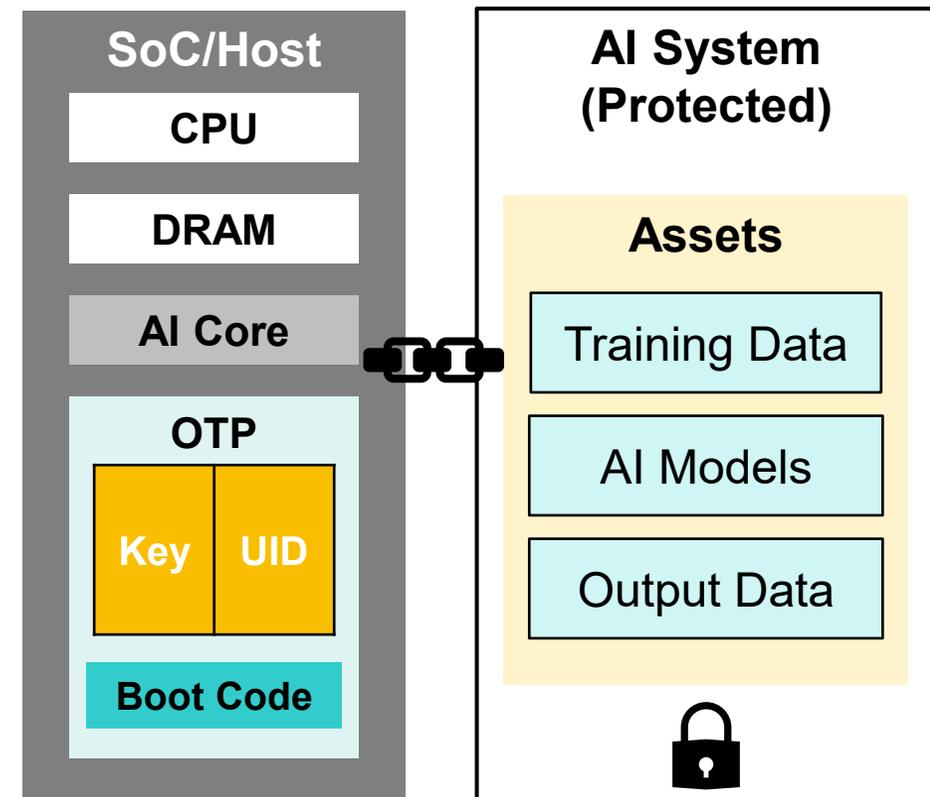
# eMemory enables HPC in AI Applications

- eMemory's OTPs can also store boot codes, root key and unique ID for the root of trust in AI systems.

Without eMemory OTP



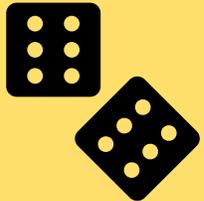
With eMemory OTP



# Why **PQC** Needs **PUF**? ■



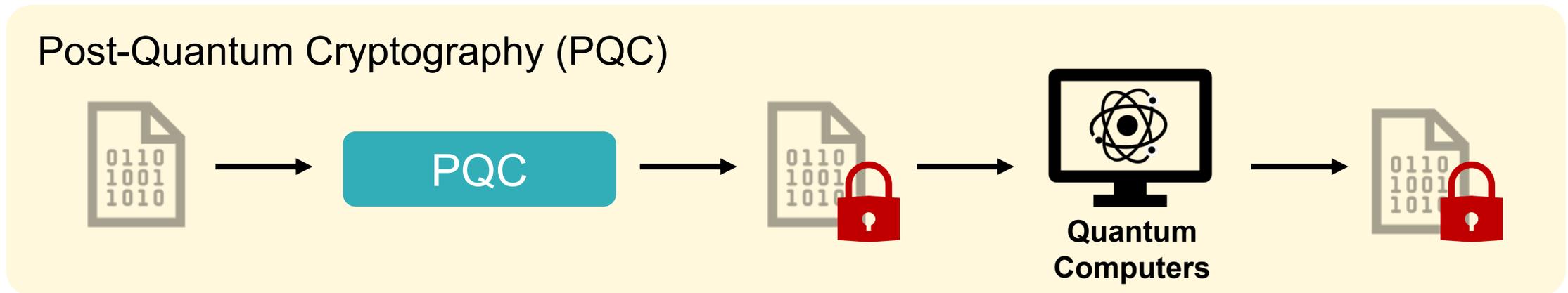
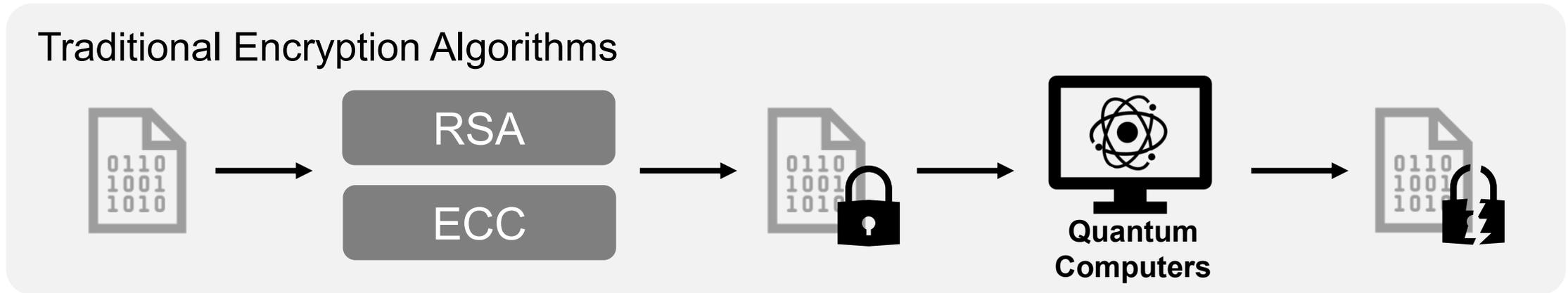
**PUF** can **efficiently generate keys with long length**, which is needed for PQC.



**PUF** can **efficiently provide random numbers**, which are needed for **anti-tampering** in PQC.

# What is PQC? ■

- PQC aims to create cryptographic systems that can withstand attacks from quantum computers.



# Why is PQC Needed? ■

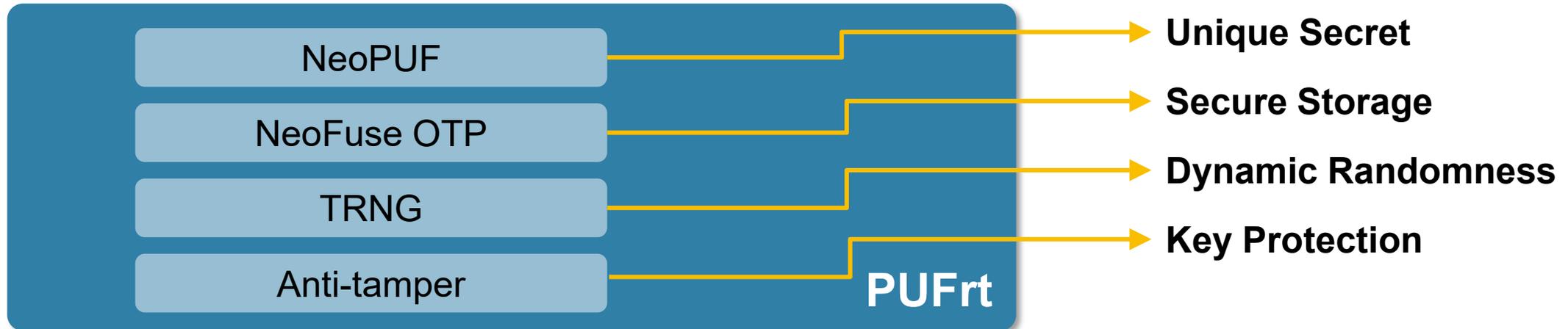
- As quantum computing progresses, the demand for encryption capable of resisting quantum attacks becomes critical.
- The sooner we implement PQC, the sooner we can guarantee the security of our data in a quantum future.



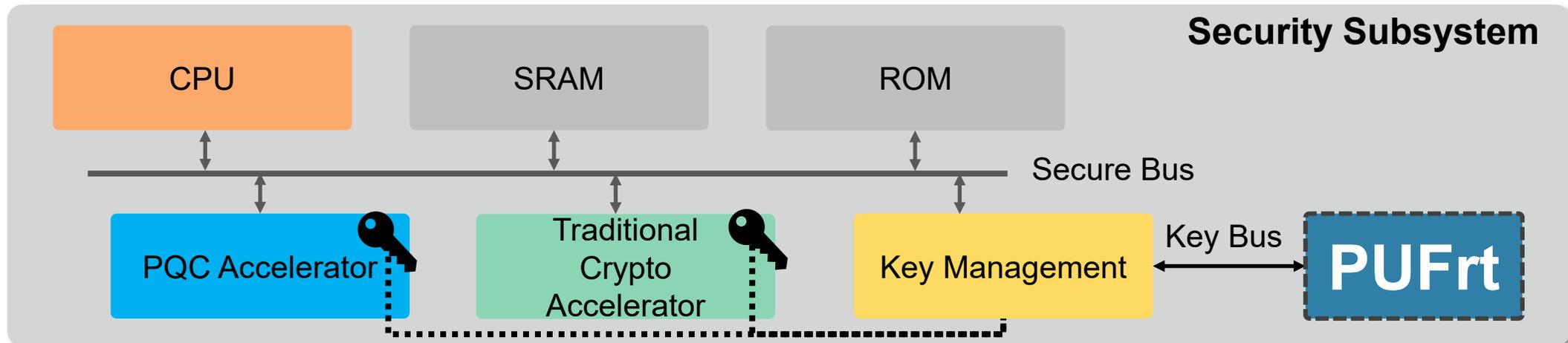
- In 2024, NIST officially announced three standards for PQC:
  - FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
  - FIPS 204, Module-Lattice-Based Digital Signature Standard
  - FIPS 205, Hash-Based Digital Signature Standard

# 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

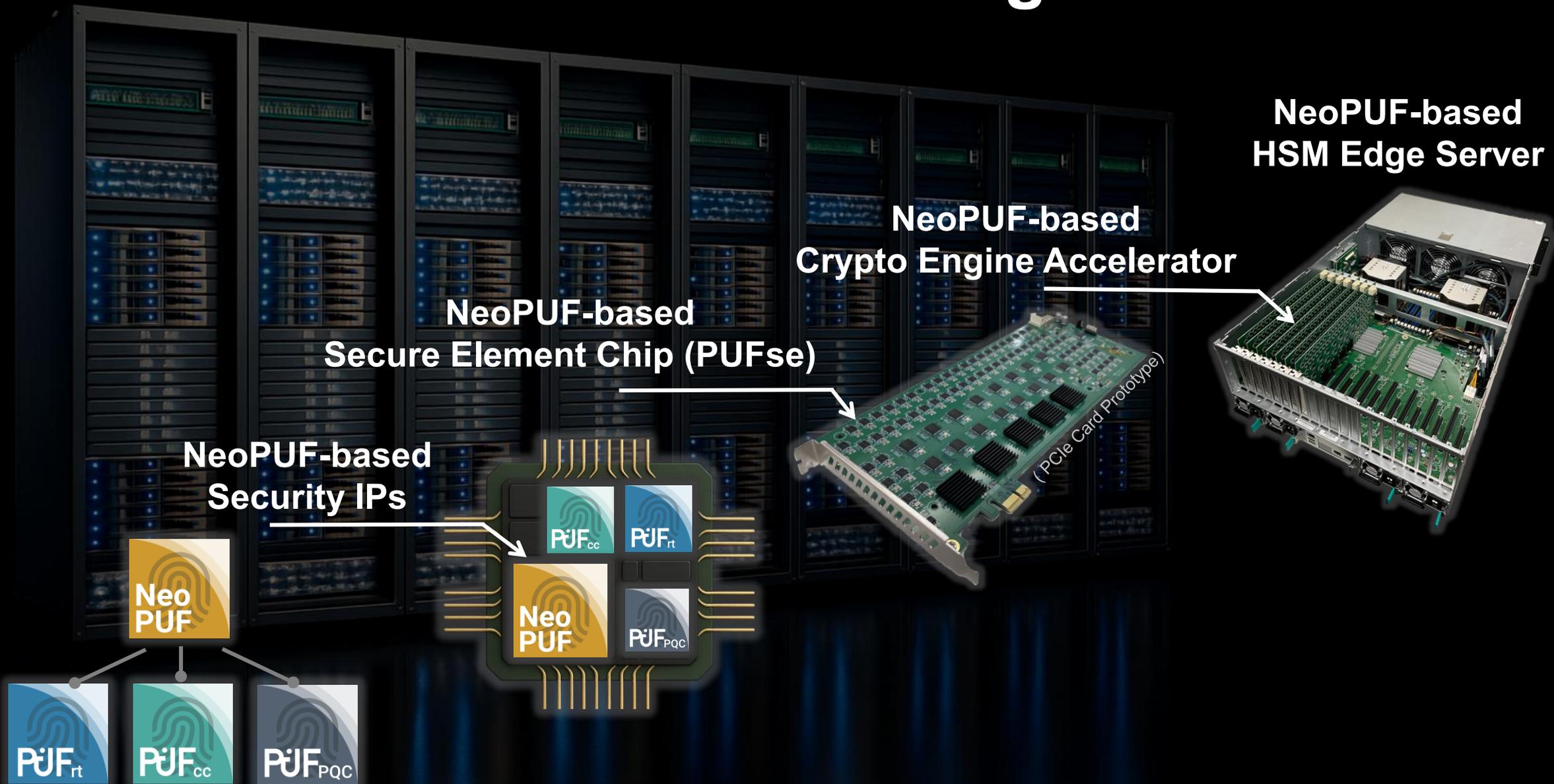
Monitor

Identify key databases and prioritize upgrades

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

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

# NeoPUF-based HSM Edge Server



# NeoPUF-based HSM Edge Server Applications



Financial Services & Banking



E-Commerce & Retail



Healthcare & Pharmaceuticals



Government & Public Sector



Telecommunications

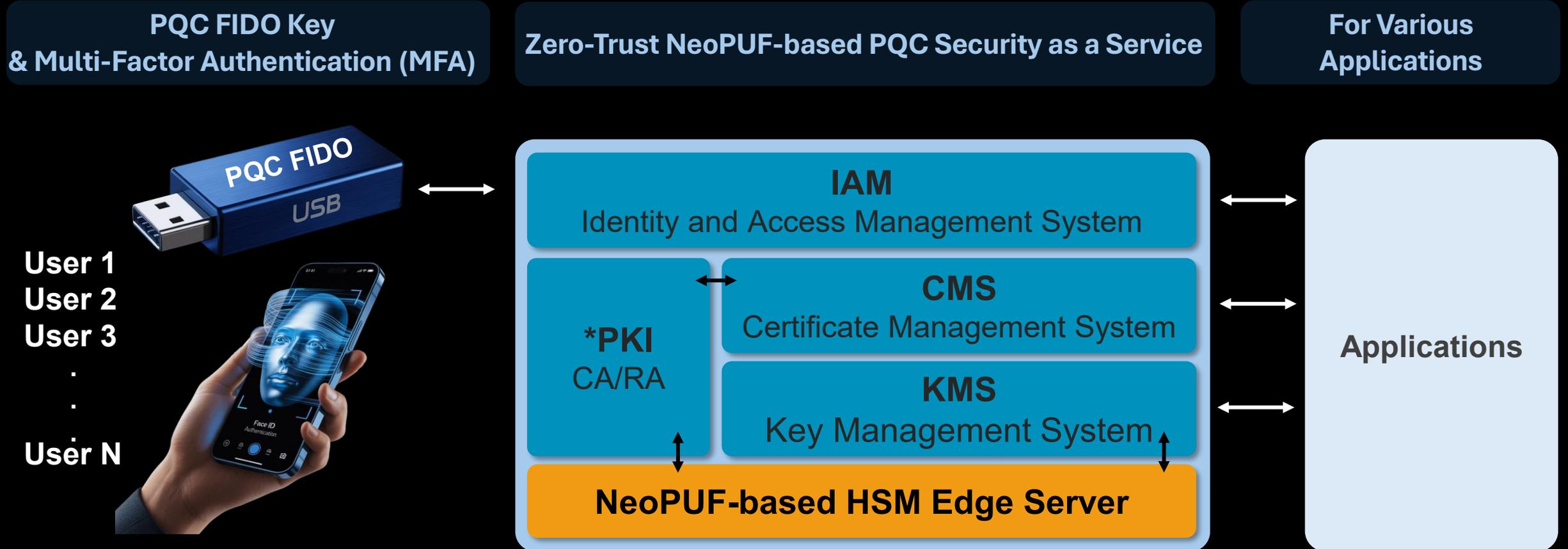


Cloud & Data Centers



Automotive & Manufacturing

# NeoPUF-based PQC Security as a Service



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

# Security Challenges in Chiplets

## Chiplet Supply Chain

### IP Piracy

IP theft

01

### Malicious Parts

“Trojan” chiplets may exist

02

### Counterfeit Parts

Unauthorized chiplets can be inserted

03

## Authentication between Chiplets

### Primary Components

e.g. Core / Accelerator

01

### Enabling Components

e.g. I/O

02

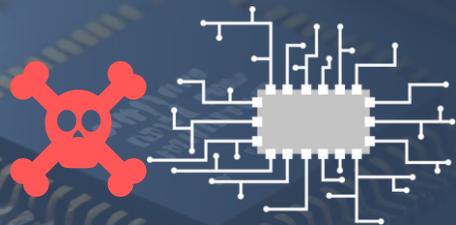
### Supportive Components

e.g. Memory

03

# NeoPUF for Supply Chain Security

## Design



**IP Piracy**



Built-in HUK, eliminating the need for key injection

## Fab./ Packaging



**Malicious Parts**



Each component carries a PUF UID for device management

## Deployment



**Counterfeit Parts**



Keys & certificates generated by the PUF assist in supply chain management

# Authentication between Chiplets

		Security Requirement	Hardware Root of Trust	Authentication Scheme
✓	Primary Components	High	<ul style="list-style-type: none"><li>• Anti-Tampering</li><li>• Secure Storage</li><li>• Unique ID</li><li>• TRNG</li></ul>	<ul style="list-style-type: none"><li>• Two-way Authentication</li><li>• Asymmetric Crypto</li></ul>
✓	Enabling Components	Moderate	<ul style="list-style-type: none"><li>• Anti-Tampering</li><li>• Secure Storage</li><li>• Unique ID</li><li>• TRNG</li></ul>	<ul style="list-style-type: none"><li>• One-way Authentication</li><li>• Symmetric Crypto</li></ul>
✓	Supportive Components	Basic	<ul style="list-style-type: none"><li>• Anti-Tampering</li><li>• Secure Storage</li></ul>	<ul style="list-style-type: none"><li>• One-way Authentication</li><li>• Symmetric Crypto</li></ul>

# NeoPUF-based Solutions for Chiplet Security



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



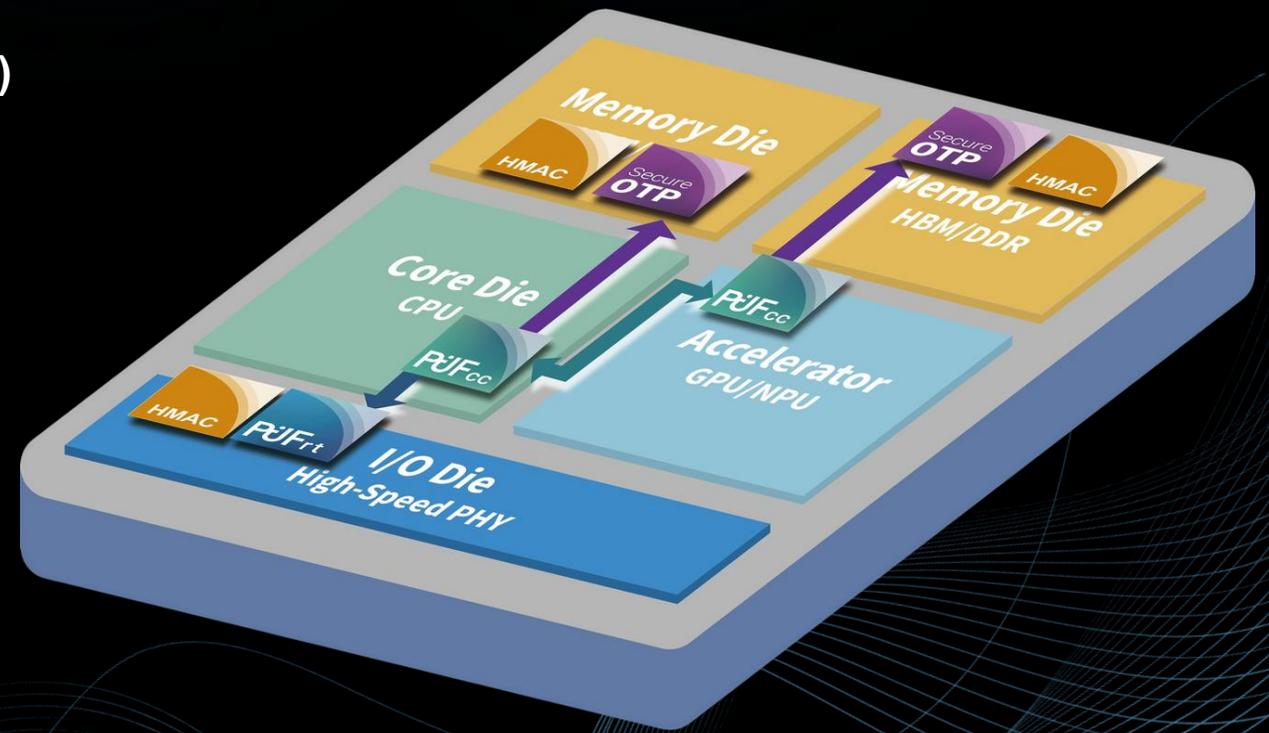
**Secure Storage**  
(For key / certificates)



**Hardware Root of Trust**  
(UID / Key)



**Crypto Coprocessor**  
(Two-way asymmetric authentication)



# Thank You for your time ■

For more information, please visit:

eMemory Website: <https://www.ememory.com.tw/>

PUFsecurity Website: <https://www.pufsecurity.com/>

The logo for eMemory, featuring the word "eMemory" in a white, lowercase, sans-serif font. The background of the slide is a blurred image of a circuit board with a yellowish-green glow on the left side.

eMemory