力旺電子Briefing .

ememory

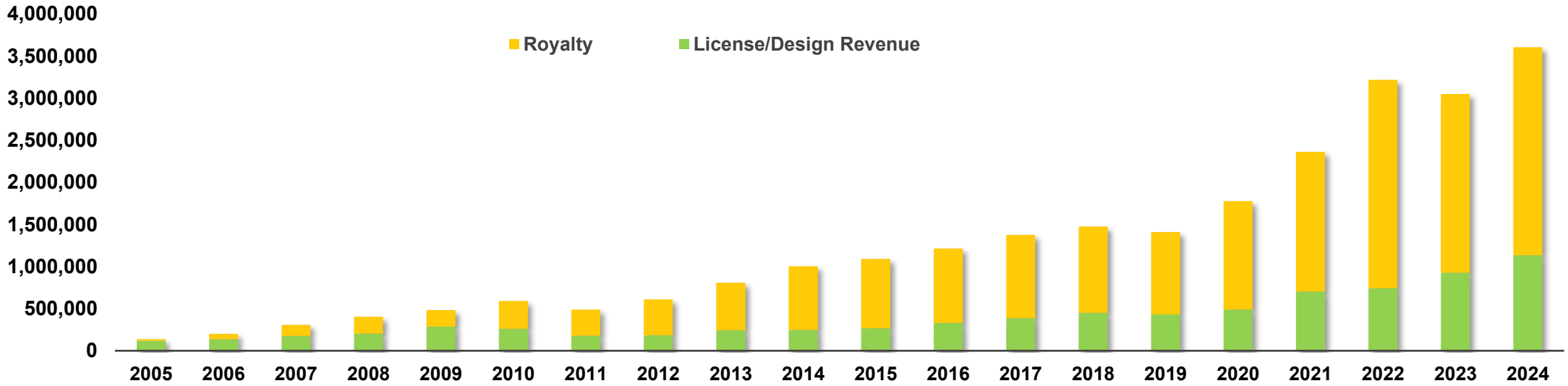
IPR Notice

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 69M wafers shipped.

1300+
Patents Issued

214 pending patents. 360 employees with 69% 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

- **PUF**se
- **PUF**cc
- **PUF**rt

eMemory

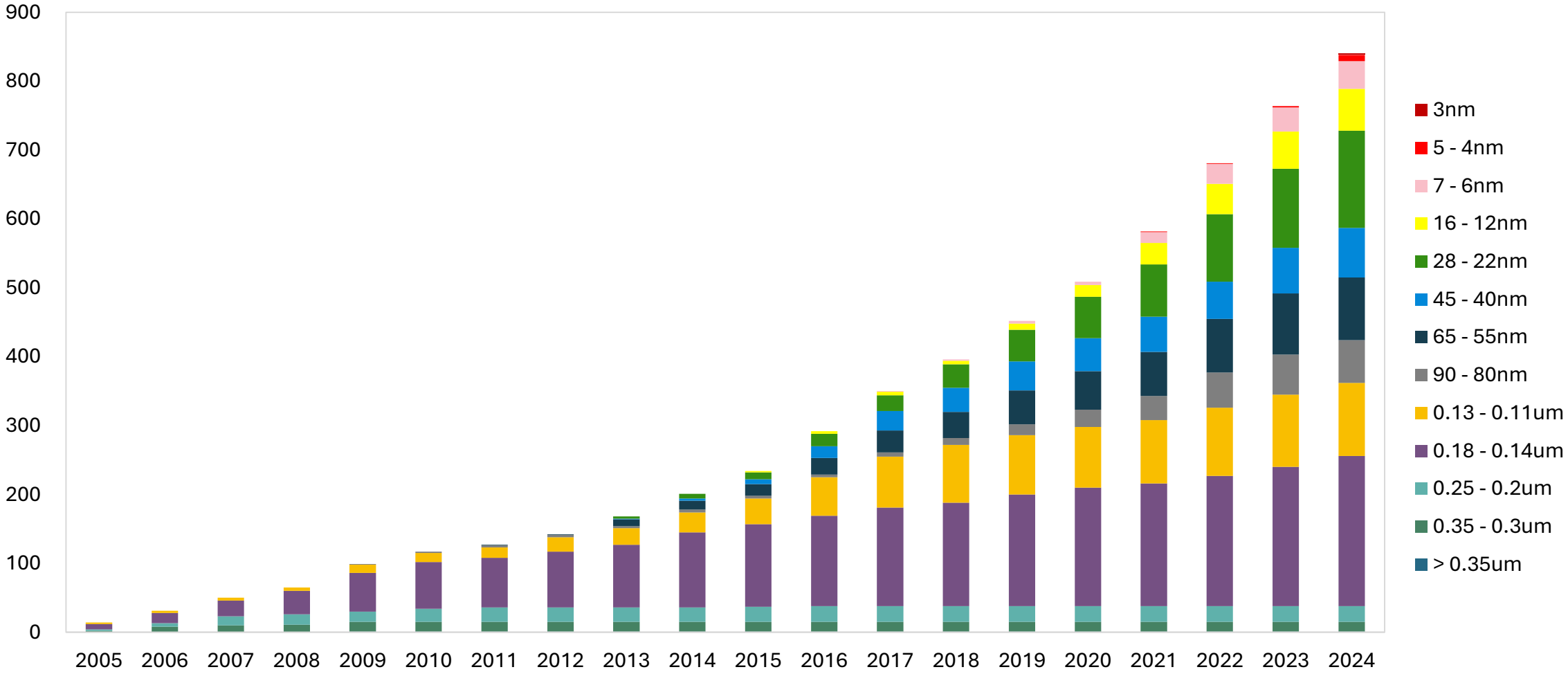
Technology Provider + IP Design & Service

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

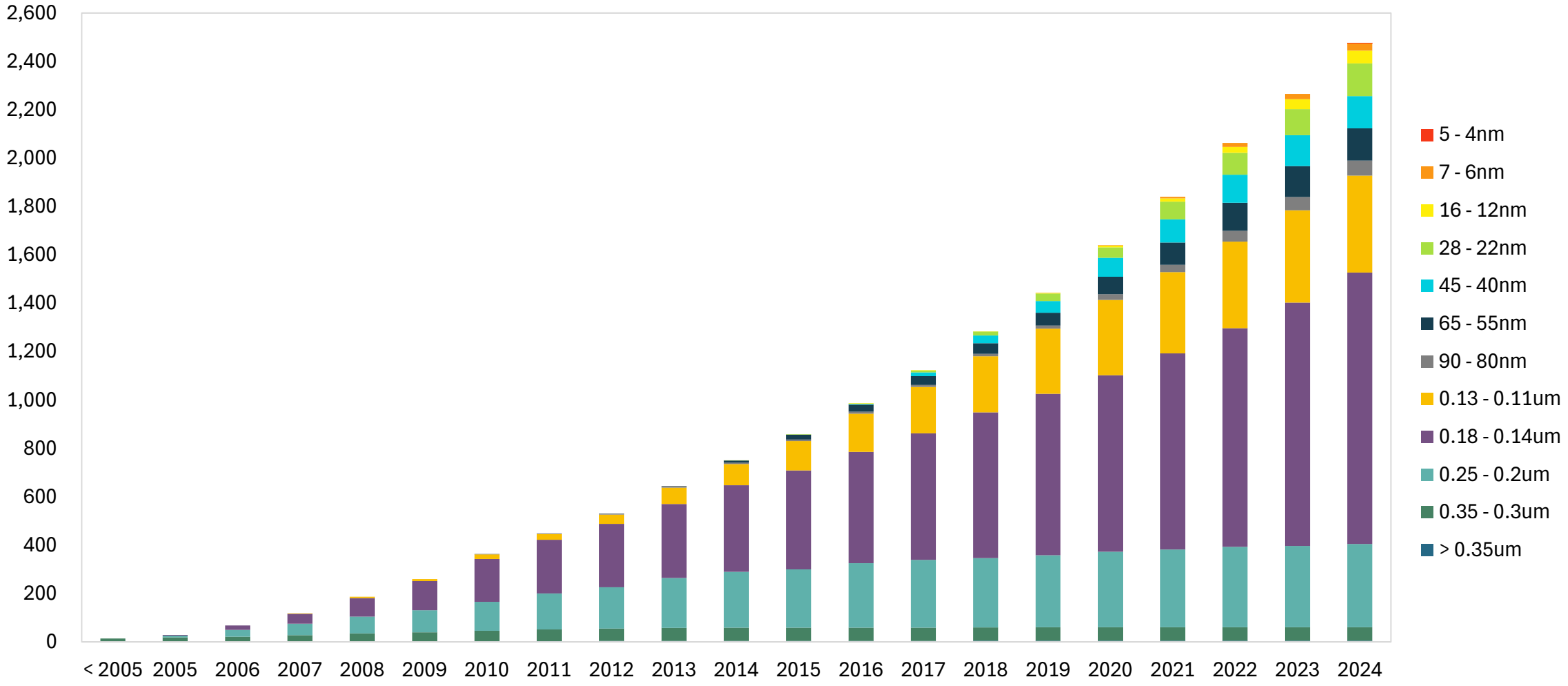
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

Registered IPs at TSMC

Registered IP > 750

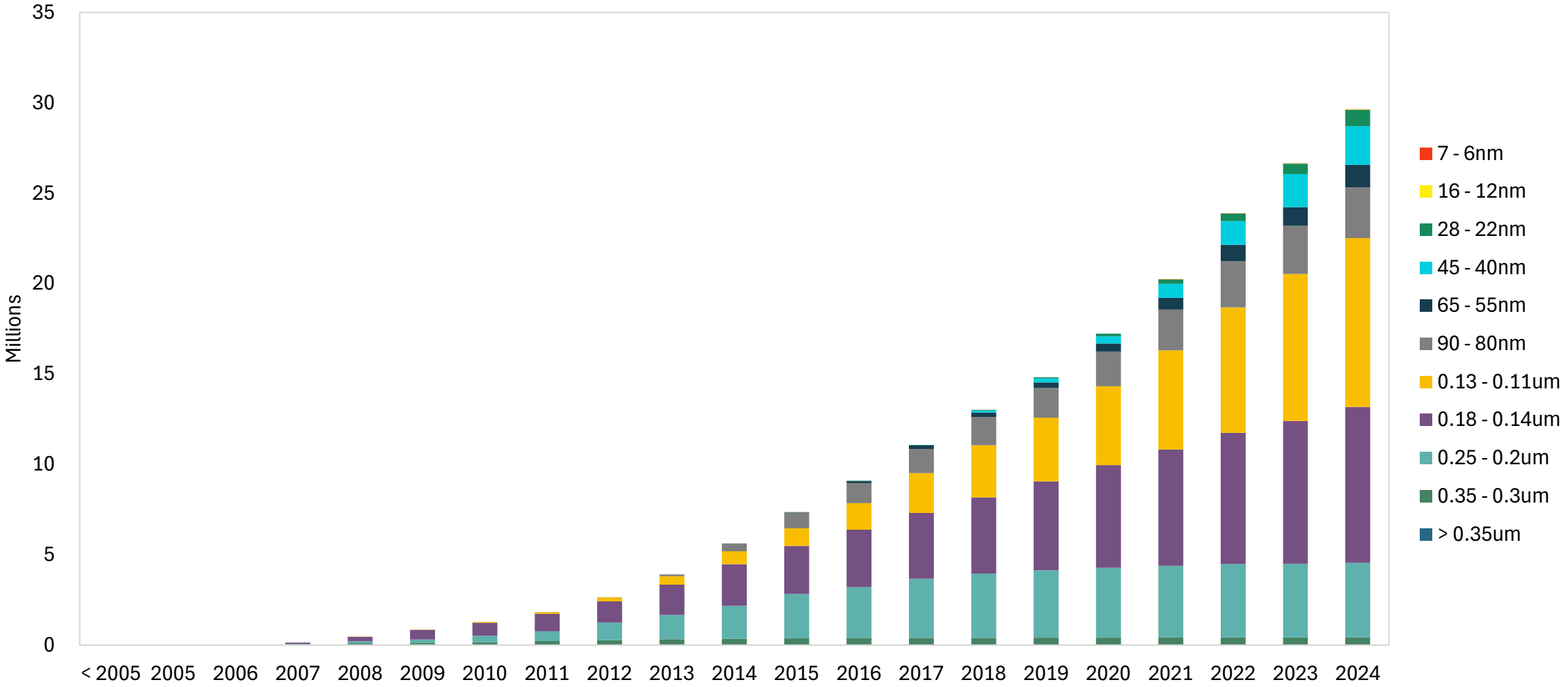


New Tape Out Contribution > 2400



Wafer Contribution at TSMC

8” Wafer Contribution > 25M



Revenue and Tape-out by Technology

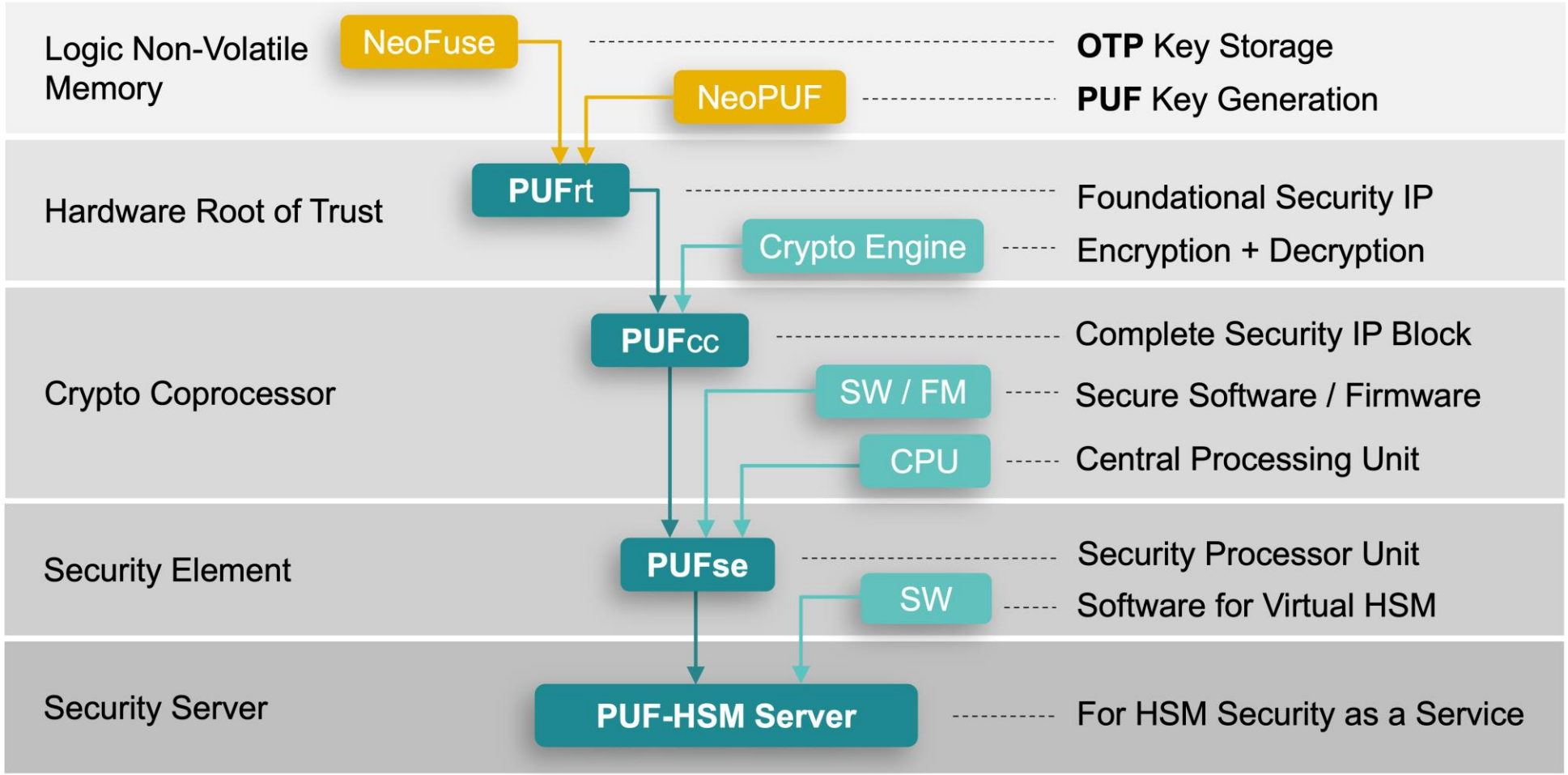
	NTO		Revenue (USD)		
Year	**NeoBit**	**NeoFuse**	**NeoBit**	**NeoFuse**	**PUF-based**
2002	3				
2003	29				
2004	40				
2005	68		$ 4,217,380		
2006	133		$ 6,202,270		
2007	220		$ 9,402,479		
2008	253		$ 12,896,211		
2009	268		$ 11,695,587		
2010	284		$ 15,873,331		
2011	254		$ 15,399,098		
2012	270		$ 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
Total	**5,129**	**1,482**	**$ 455,100,213**	**$ 306,041,783**	**$ 15,738,303**

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

* 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

Distributed **PUF-HSM as a Service**

Various applications require **secure cryptographic operations** and **secret key storage/access**.

Internet

Key Generation
Sign
Verify
Encryption
Decryption

SUBSCRIBE

Billing based on the number of computations

Distributed PUF-HSM as a Service

Distributed PUF-HSM Server

Unit PUF-HSM Server

PUF-HSM PCIe Card

PUFse chip

Distributed Virtual HSM Software

PUF-HSM Service Billing Counter

PUFse API

Unit HSM Software

Standards Drive Hardware-Based Security

OPEN Compute Project® Caliptra

Driving an open standard for silicon root of trust

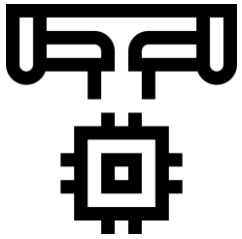
fido™ ALLIANCE

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

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

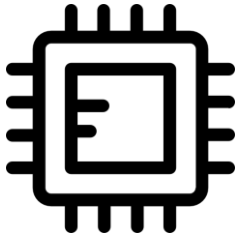
Foundry Platforms



TSMC, Intel, UMC, GF, etc.

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

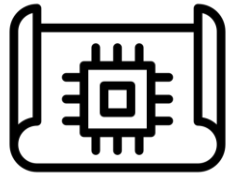
CPU Partners



Arm, RISC-V, Cadence, etc.

- SoC customers looking for both CPU and security subsystems

CSP



More to come

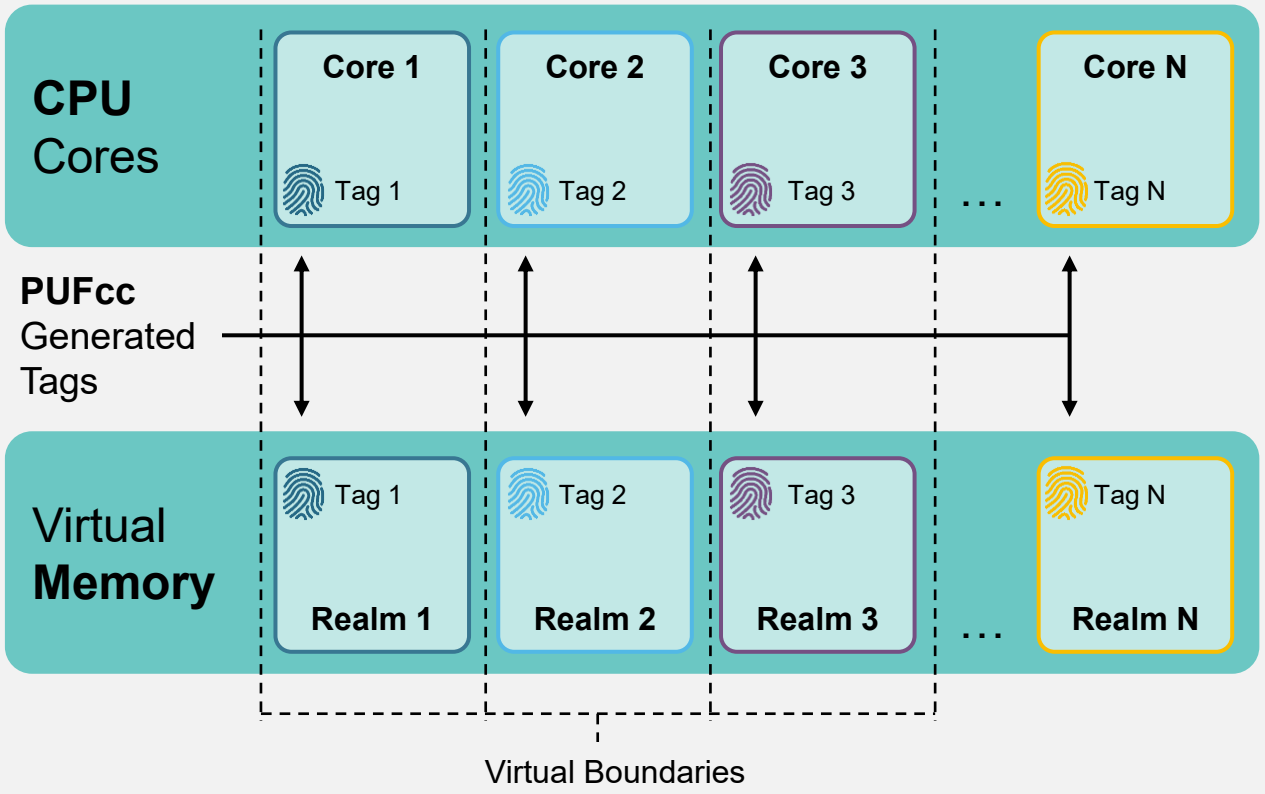
- Work with CSP and system companies for embedded security on a chip level

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**

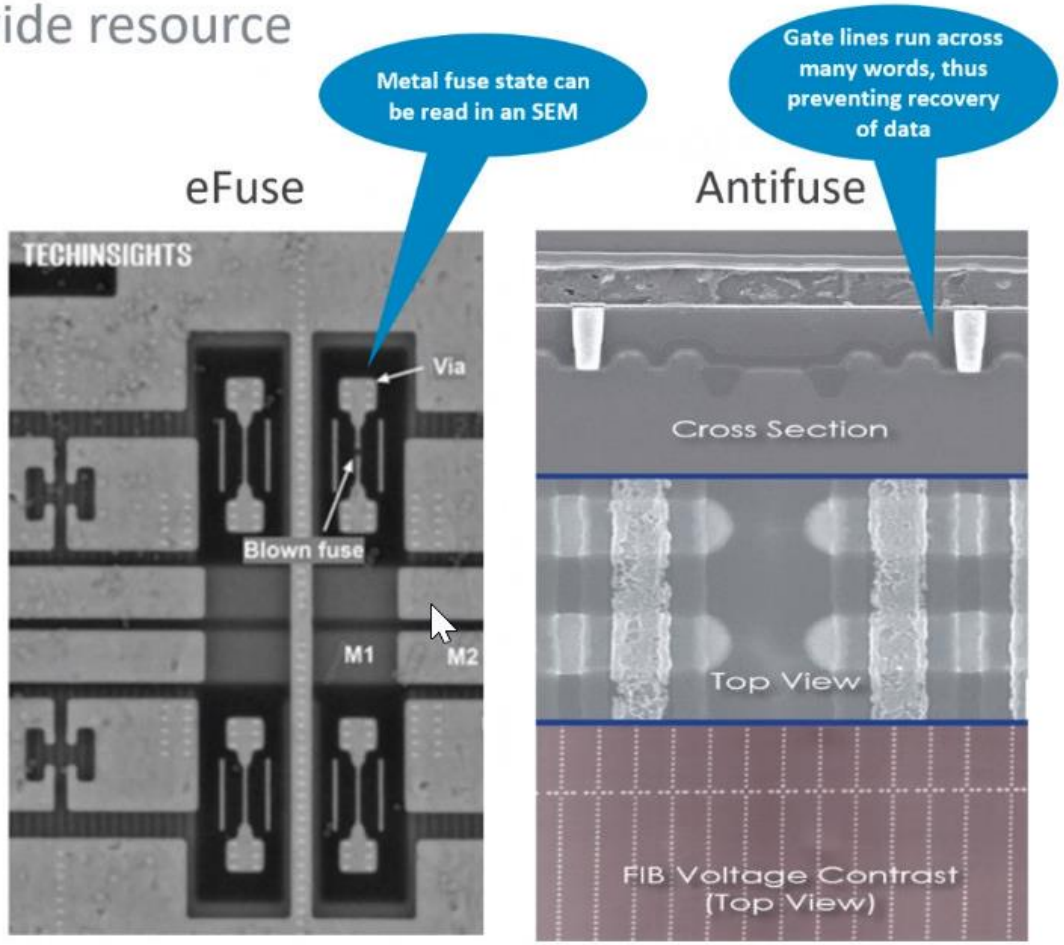


- **Protect data** in the Virtual Memory of Multi-Core CPUs
- CPU Cores and Virtual Memory have unique corresponding **tag numbers**
- Tag numbers are internally **randomly generated** by **PUFcc** (Crypto Coprocessor IP)

AntiFuse OTP vs. **eFuse**

One Time 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



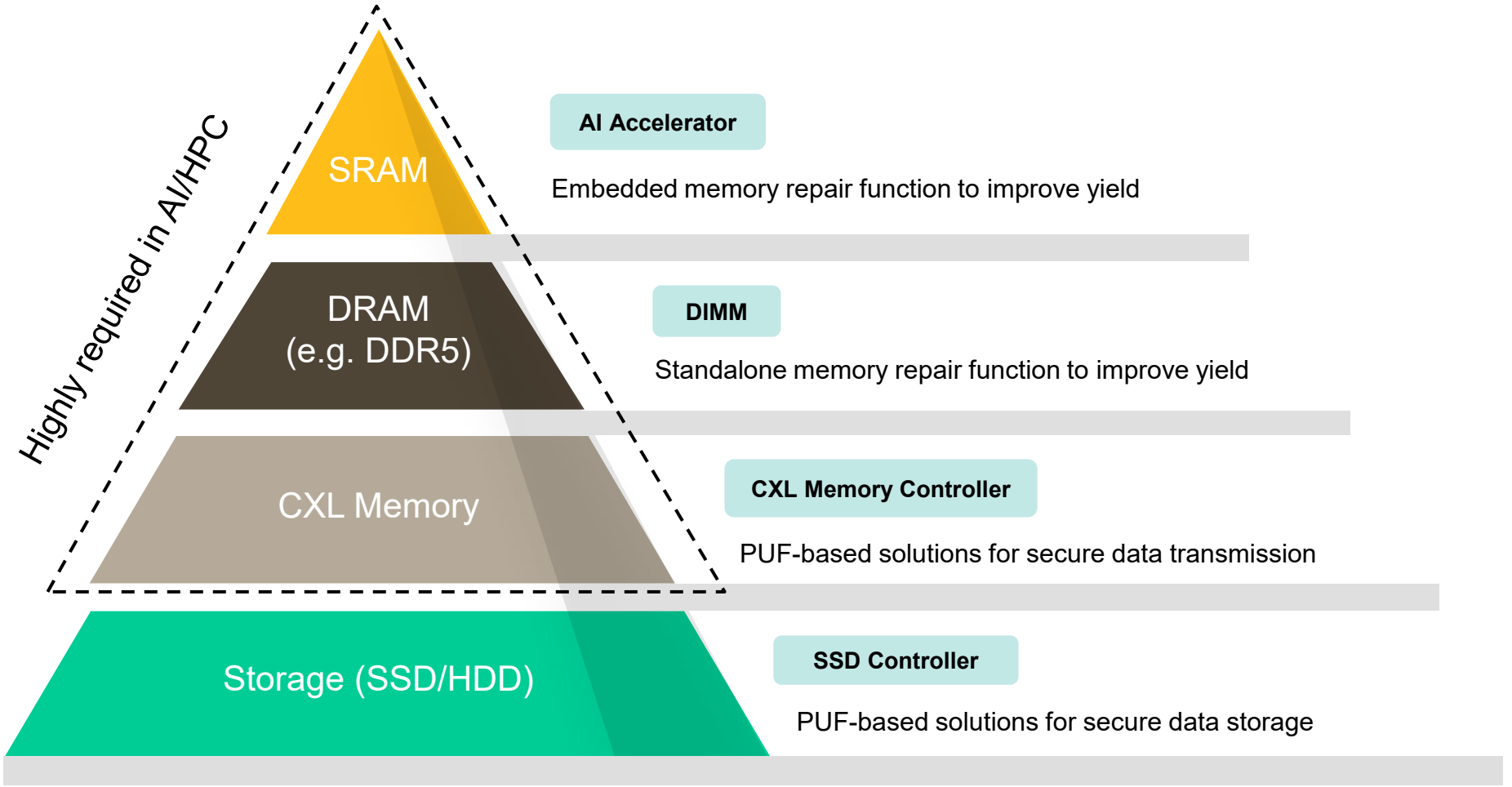
https://semiengineering.com/the-benefits-of-antifuse-otp/

Rainer Herberholz

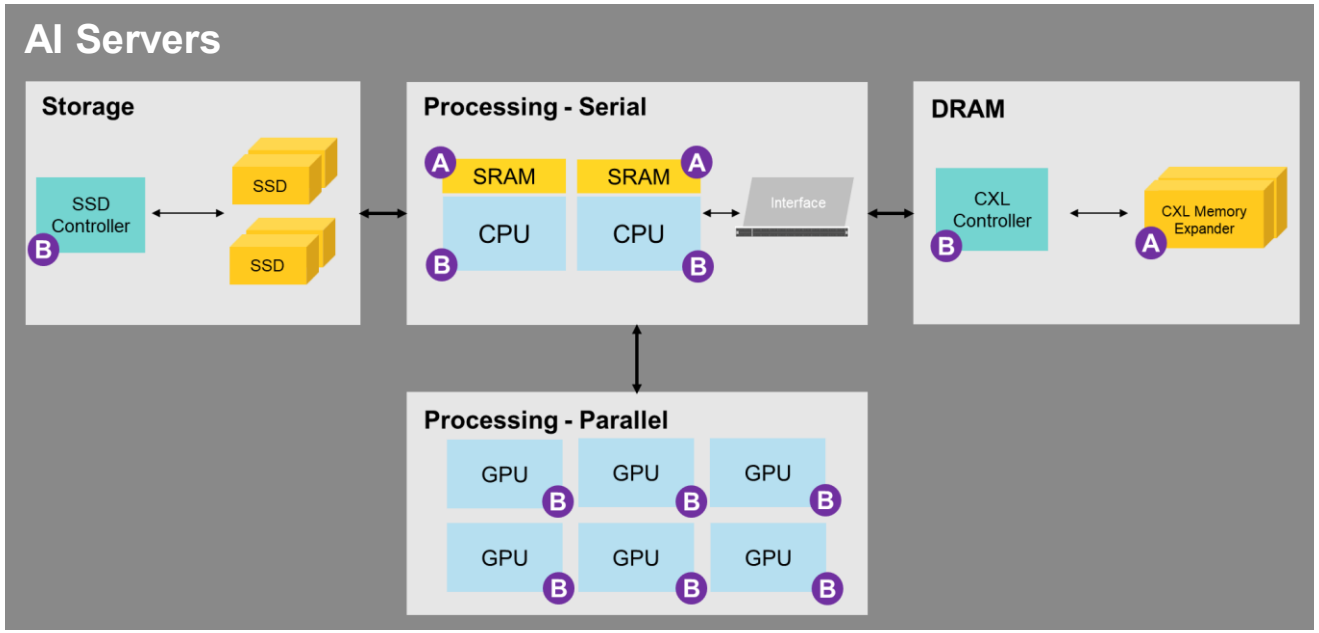
arm

Example: **eMemory** Helps Memory.

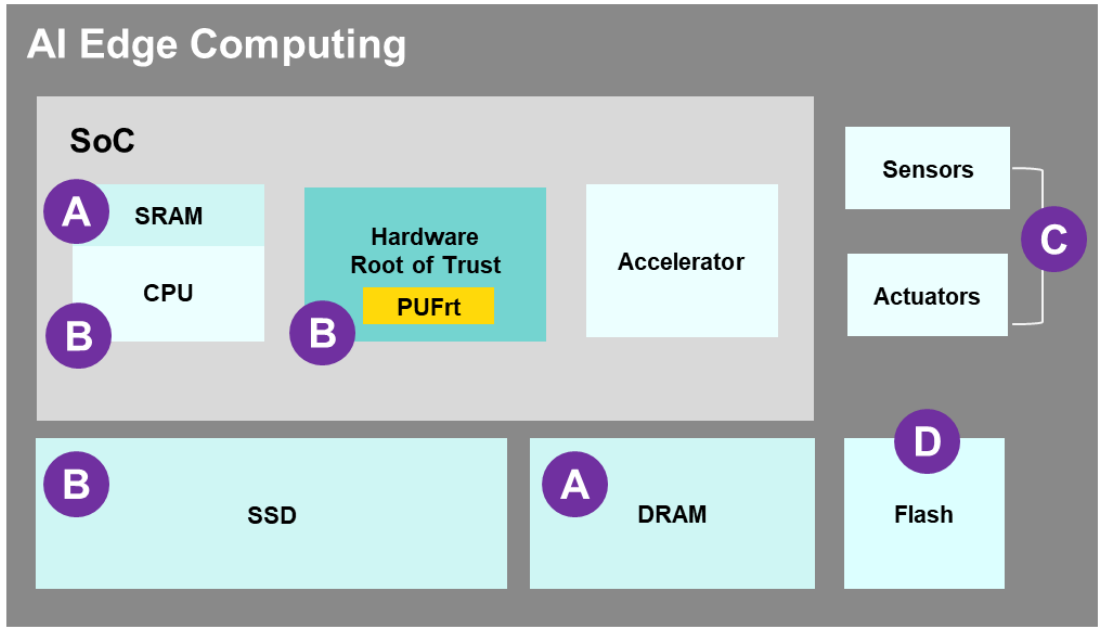
- eMemory's security IP and OTP/MTP IP 1) ensure data security and 2) improve yield for SRAM and DRAM.



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



+



A **Memory Repair**

B **Root of Trust** provides:

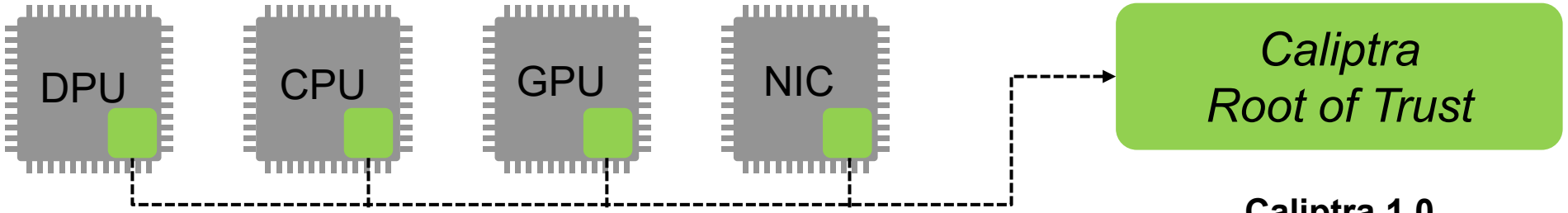
1. Key storage/generation
2. Cryptographic processing to protect AI models, input data and output results
3. Confidential Computing

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?

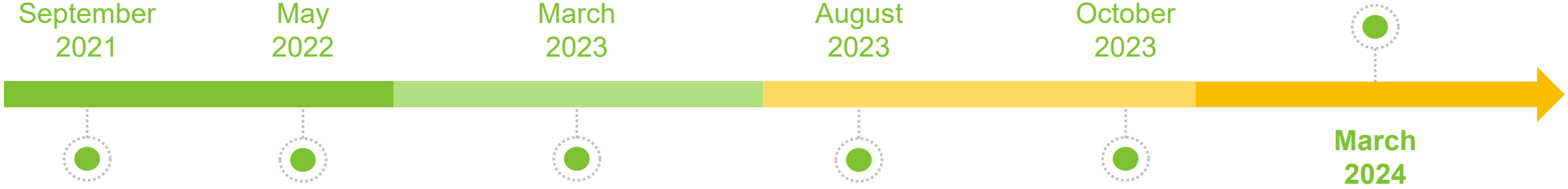
Datacenter Chips



Every chip needs Root of Trust

Caliptra 1.0

Complete specification, firmware coverage, countermeasures and testing



Project Start

Founders begin the effort

OCP Intro

Specification is formalized at Open Compute Project

Open Source

Charter is adopted at Linux Foundation

Functional RTL

Founders contributed RTL Op8 pre

Full Functionalities Defined

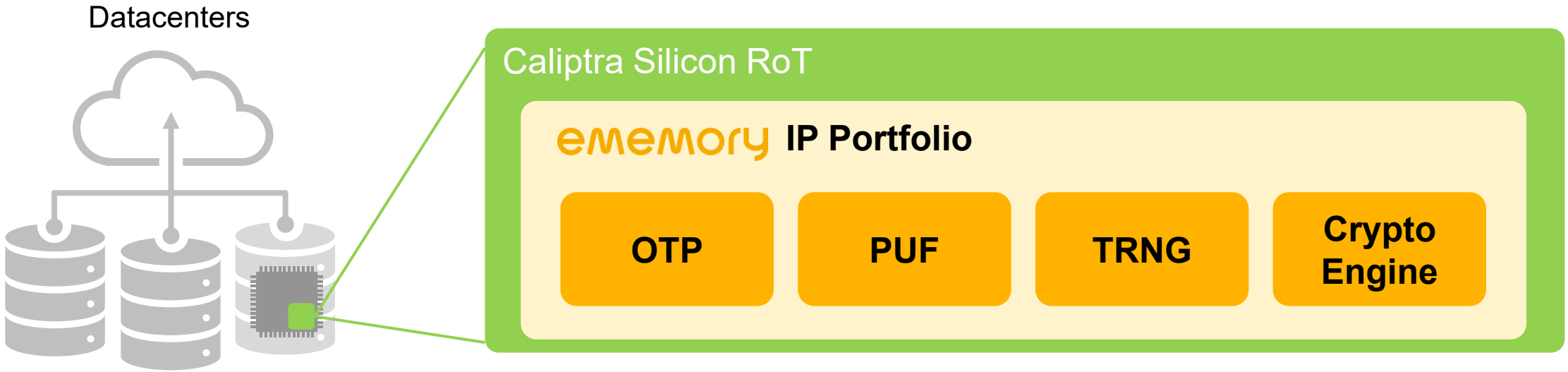
All flows are defined and are implemented in RTL

Validation Completed

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

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…

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

PUFtrng: 100 Times Faster than Conventional TRNG

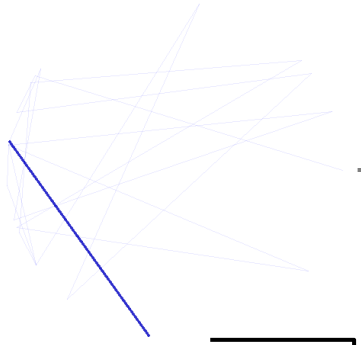
- PUF-based conditioning algorithm provides high-throughput and high-quality entropy

Similar to…

Conventional TRNG

Figure 1:

Dynamic Entropy



Post-processing

Figure 2:

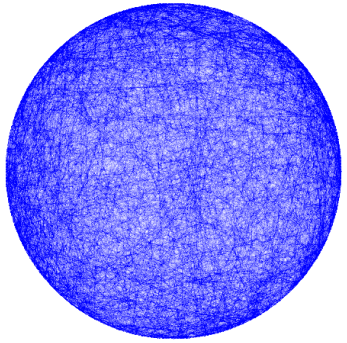
Conventional TRNG
→ Low throughput random bits
→ Slower

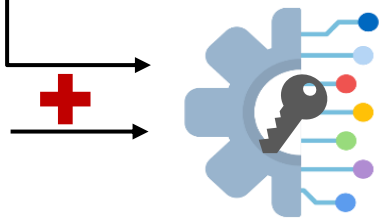
Classic Cars

PUFtrng

Figure 3:

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

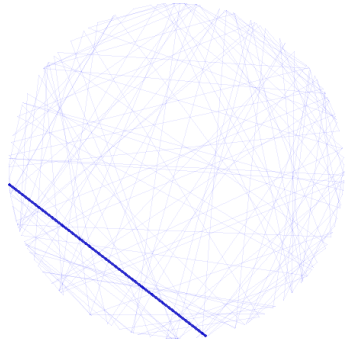




Entropy Refine Engine

Figure 4:

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



New Energy Cars

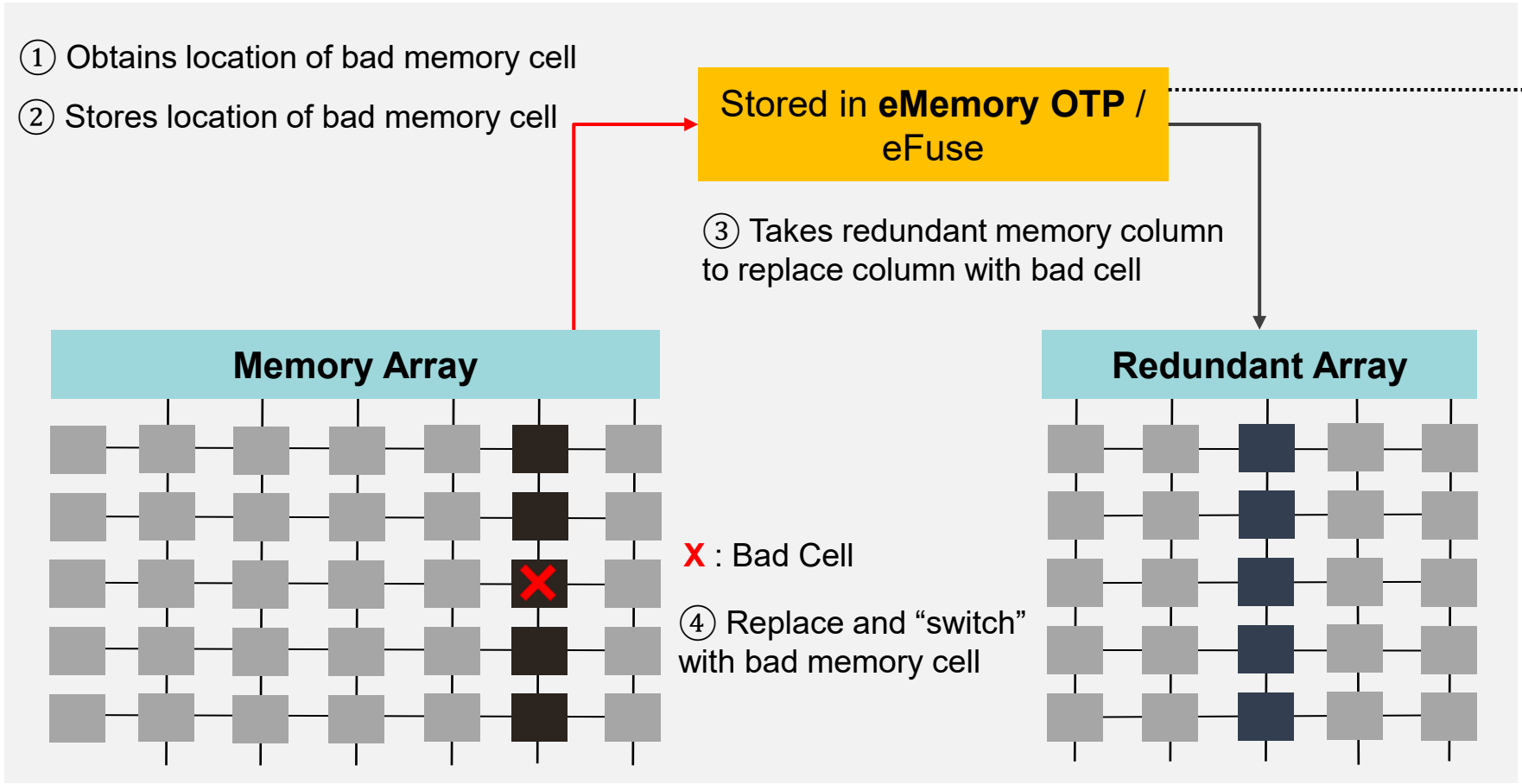
Why is **High-Density SRAM** needed in **AI?**

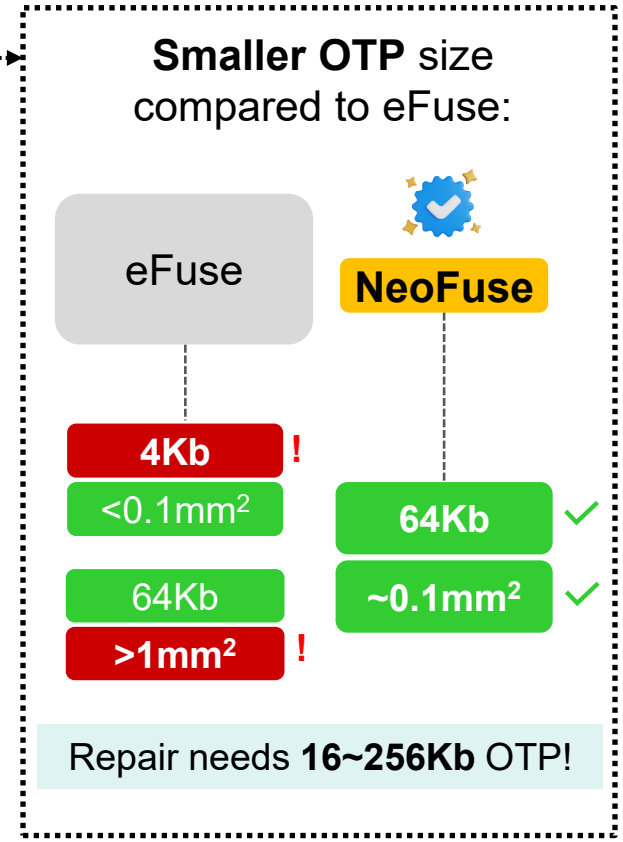
- To increase the speed of AI accelerators, **high-density SRAM** is needed for use in:

Buffer Memory	AI Model Training	Computing in Memory (CIM) for Inference
• High-density SRAM helps improve data transfer speed and reduce energy costs by acting as a fast **intermediate storage** between different processing stages.	• High-density SRAM helps **store** vast amounts of data for AI accelerators to access quickly to speed up training.	• High-density SRAM enables **in-memory computation** by storing large datasets and performing computations on them without transferring data to separate processors.

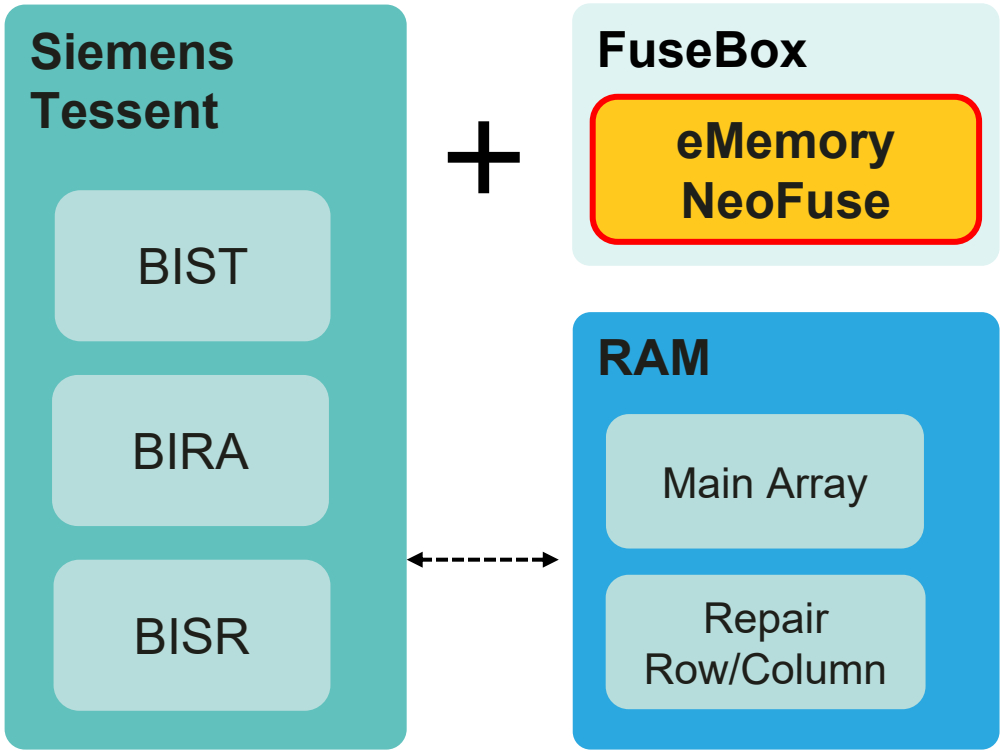
eMemory enables **High-Yielding** SRAM

- 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

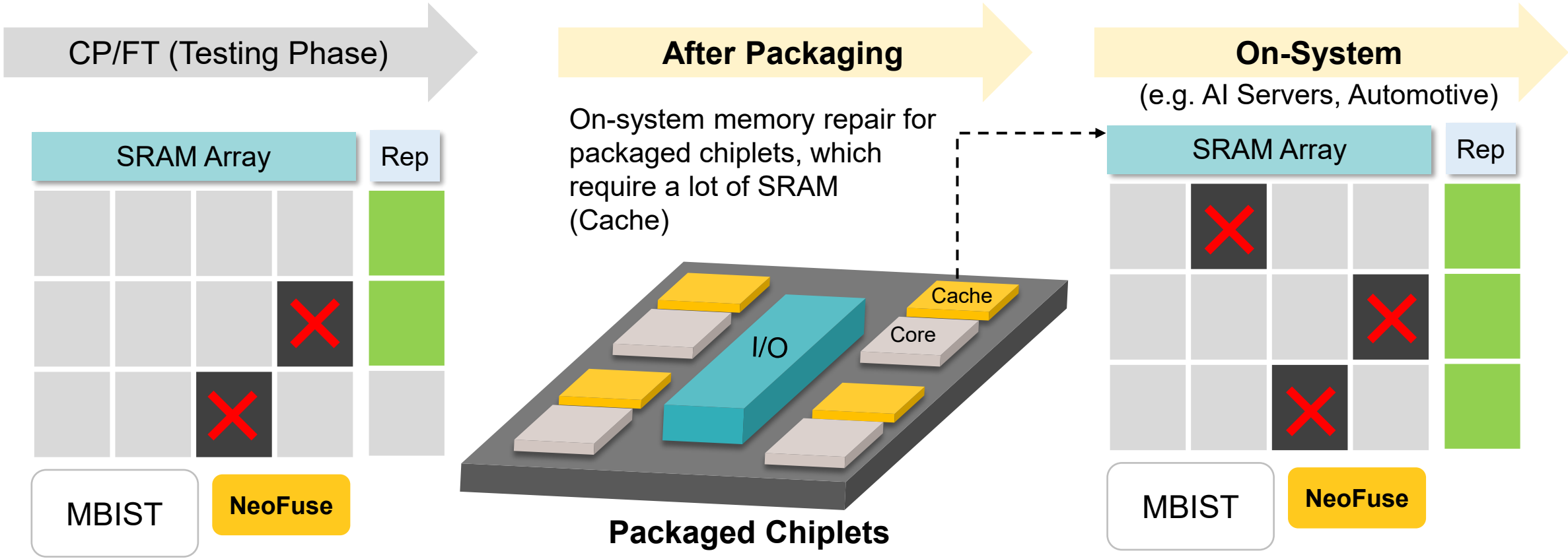
eMemory provides OTP with interface for Siemens MBIST:

- **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

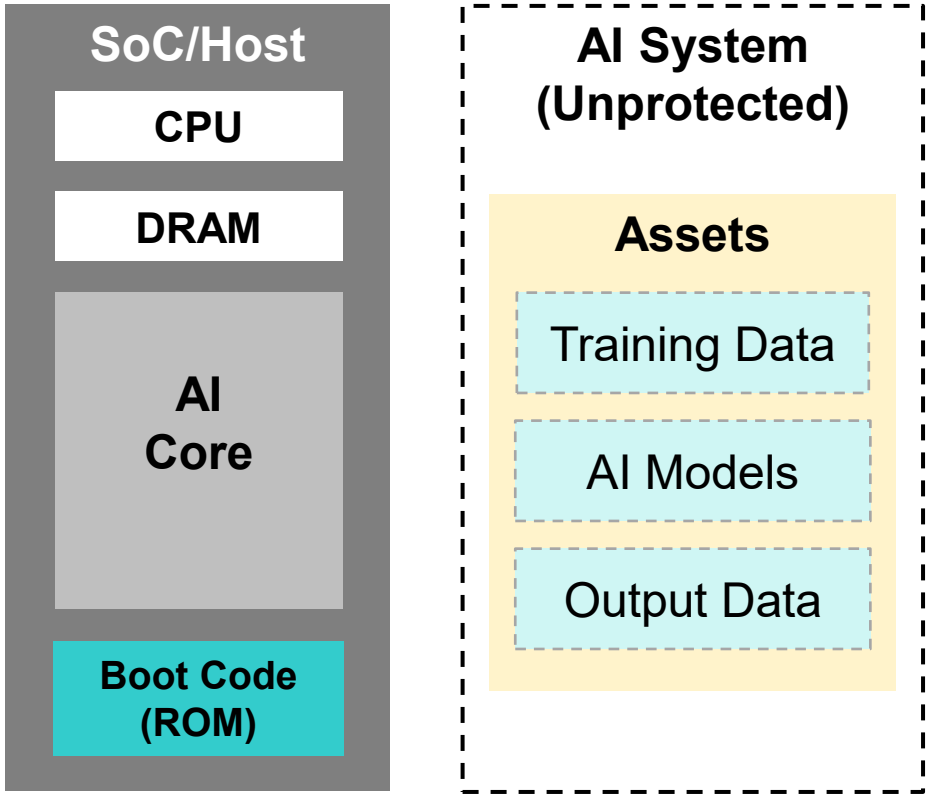
- Memory Built-in Self-Test (MBIST) offers **on-system repair** capabilities, which are essential for high-speed high-reliability applications and chiplet **architecture** or **after system** packaging.



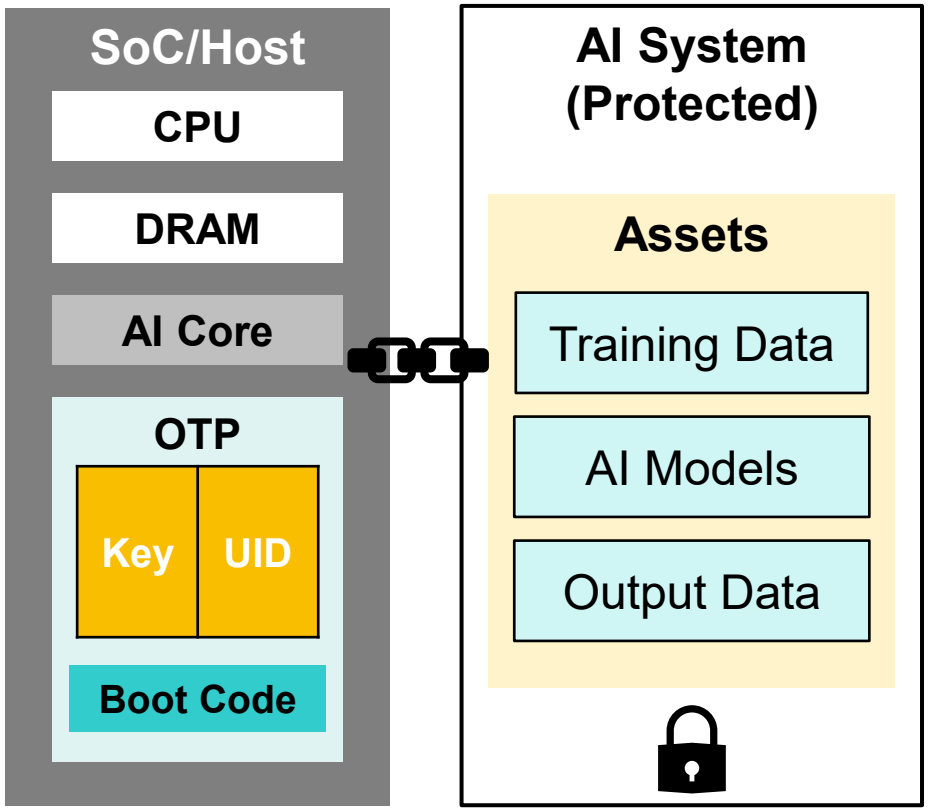
eMemory enables HPC in **AI Applications**

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

Without eMemory OTP

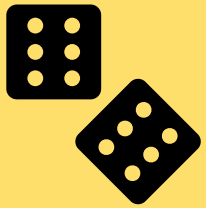


With eMemory OTP



Why **PQC** Needs **PUF**?

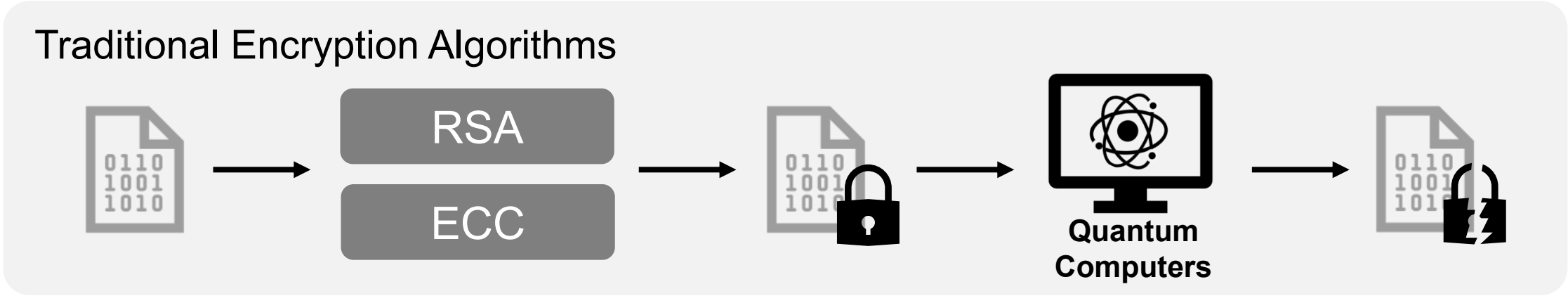
PUF can **efficiently generate keys with long length**, which is needed for PQC.



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.



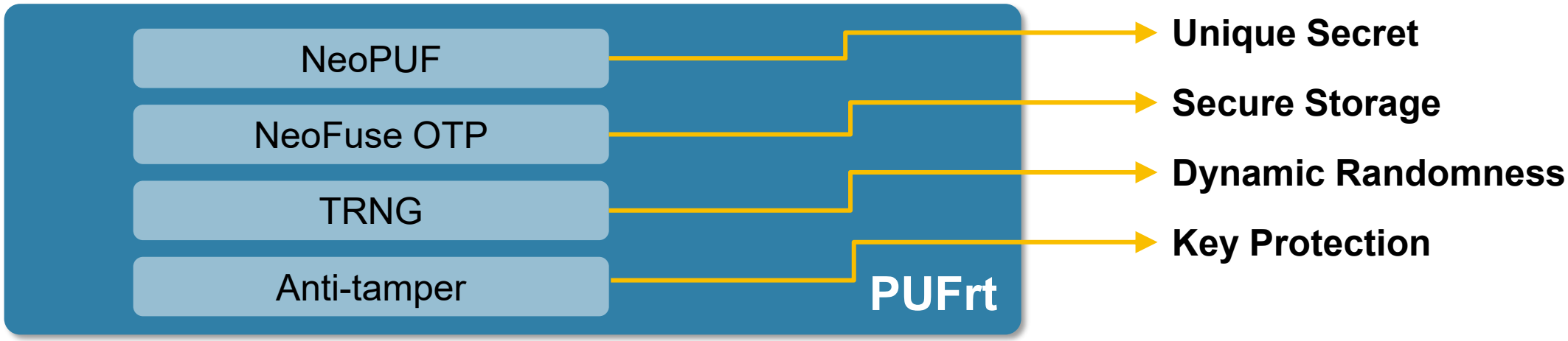
Why is **PQC** Needed?

- 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.

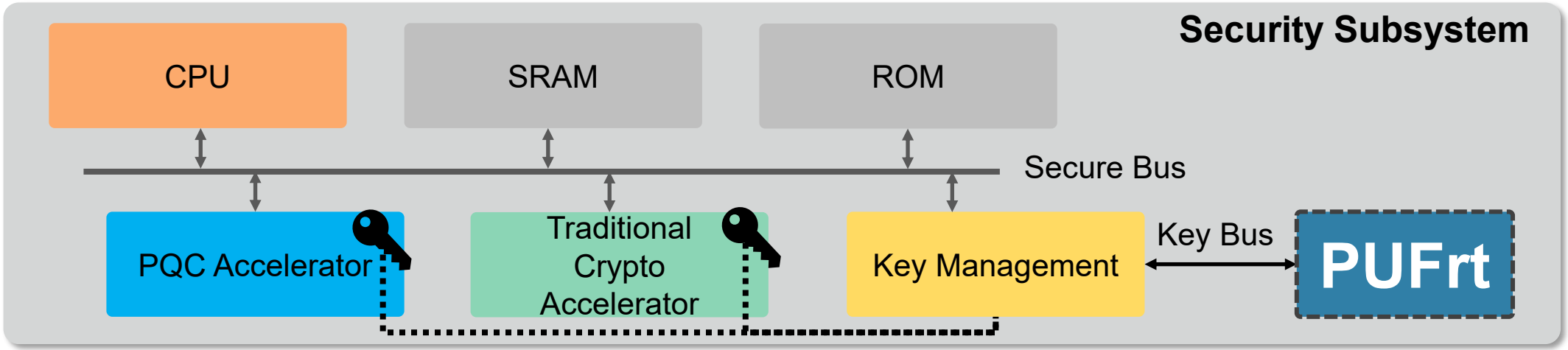
- In 2024, NIST officially announced three standards for PQC:
  - FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
  - FIPS 204, Module-Lattice-Based Digital Signature Standard
  - FIPS 205, Hash-Based Digital Signature Standard

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.



Why Migrate to PQC ?

Future-Proof Security for the Quantum Era

Eliminate risks posed by quantum computing threats

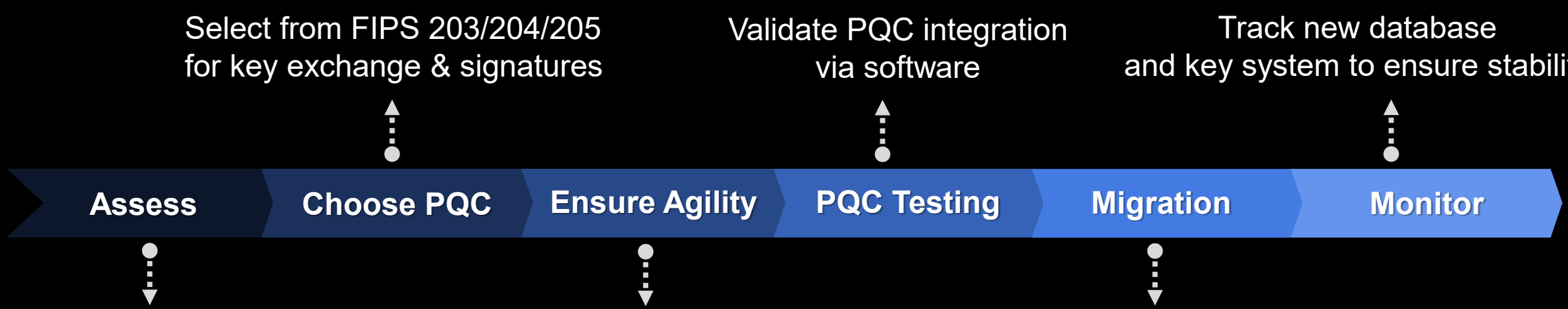
Adopt PQC-Ready HSM Edge Servers

Support both RSA/ECC and PQC crypto algorithms

PQC Migration Steps & Scope

Key Principles:

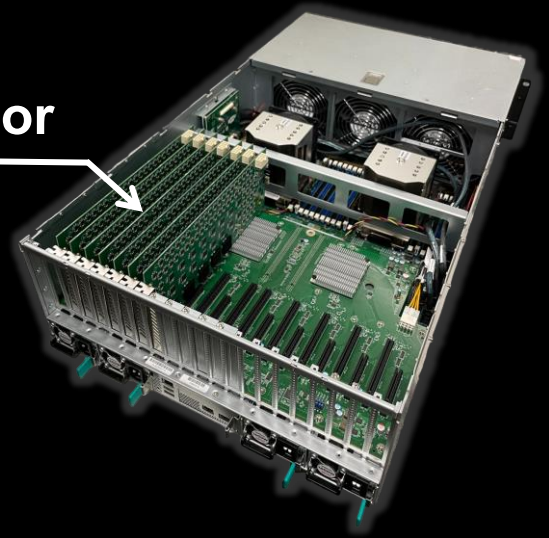
- Execute Clear Migration Steps
- Prioritize Critical Digital Assets
- Deploy PQC-ready HSM Edge Servers



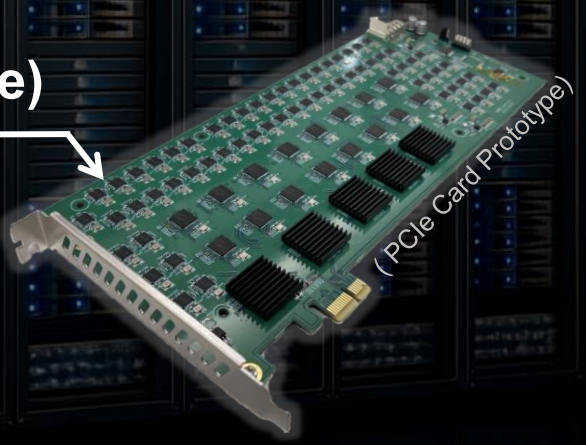
ememory

NeoPUF-based HSM Edge Server

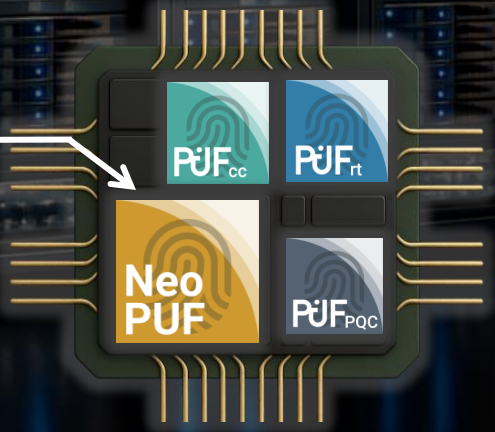
NeoPUF-based
HSM Edge Server



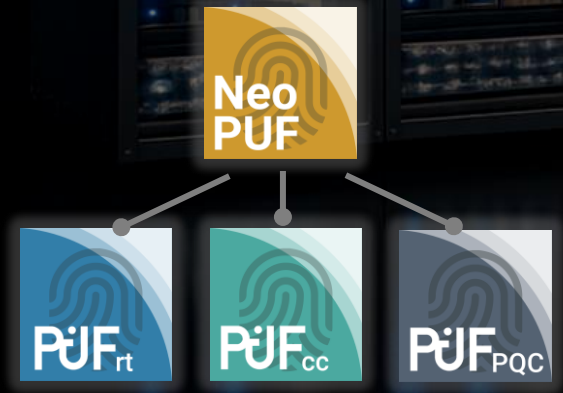
NeoPUF-based
Crypto Engine Accelerator



NeoPUF-based
Secure Element Chip (PUFse)



NeoPUF-based
Security IPs



ememory

NeoPUF-based HSM Edge Server Applications

Financial Services & Banking

E-Commerce & Retail

Healthcare & Pharmaceuticals

Government & Public Sector

Telecommunications

Cloud & Data Centers

Automotive & Manufacturing

ememory

NeoPUF-based PQC Security as a Service

PQC FIDO Key & Multi-Factor Authentication (MFA)

User 1
User 2
User 3
.
.
.
User N

Zero-Trust NeoPUF-based PQC Security as a Service

IAM
Identity and Access Management System

***PKI**
CA/RA

CMS
Certificate Management System

KMS
Key Management System

NeoPUF-based HSM Edge Server

For Various Applications

Applications

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

ememory

Security Challenges in Chiplets

Chiplet Supply Chain

IP Piracy 01
IP theft

Malicious Parts 02
“Trojan” chiplets may exist

Counterfeit Parts 03
Unauthorized chiplets can be inserted

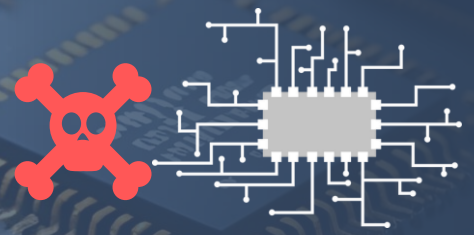
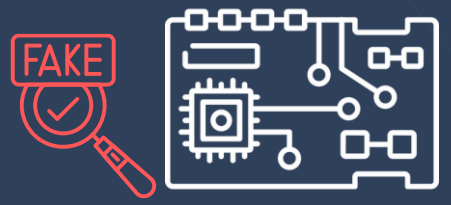
Authentication between Chiplets

01 **Primary Components**
e.g. Core / Accelerator

02 **Enabling Components**
e.g. I/O

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

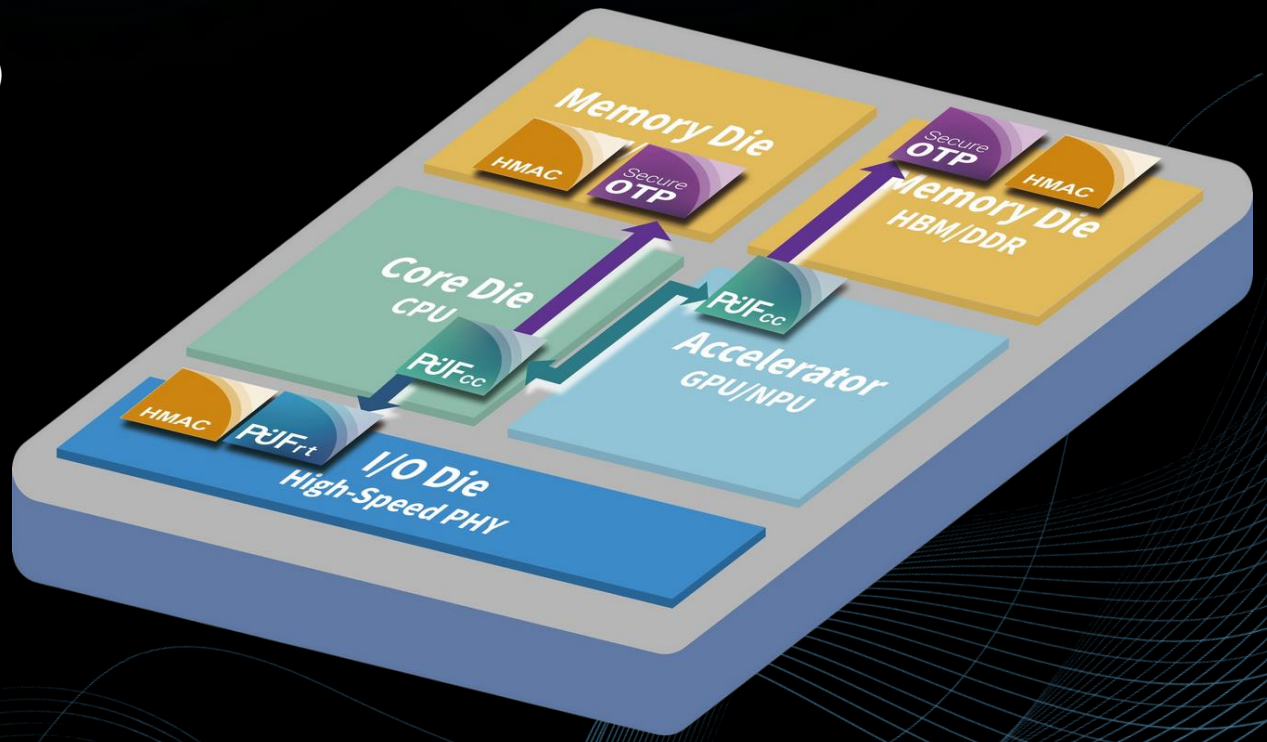
NeoPUF-based Solutions for Chiplet Security

Cryptographic Accelerator
(One-way symmetric authentication)

Secure Storage
(For key / certificates)

Hardware Root of Trust
(UID / Key)

Crypto Coprocessor
(Two-way asymmetric authentication)



Thank You for your time .

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