力旺電子Briefing

ememory

IPR Notice

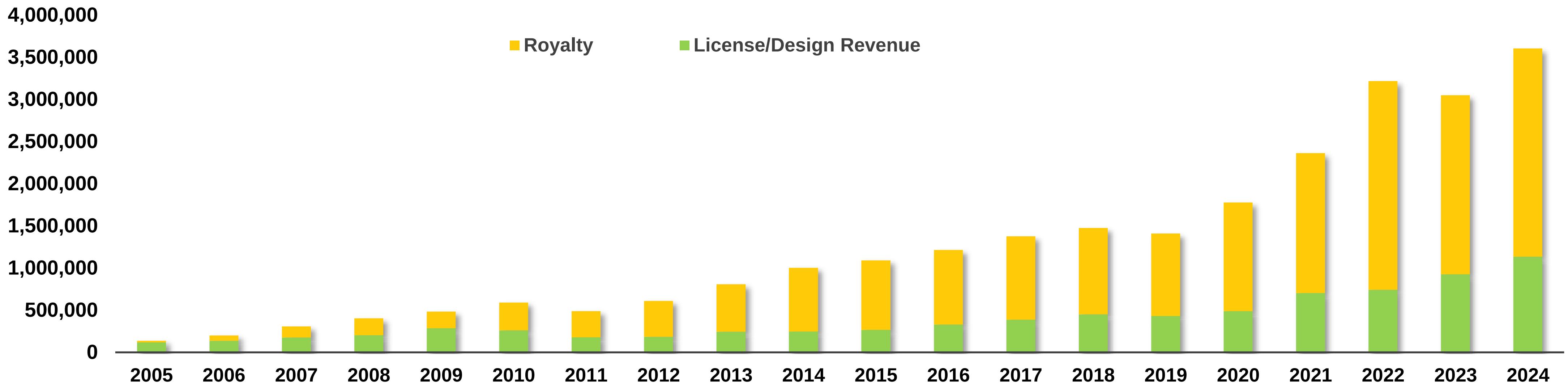
All rights, titles and interests contained in this information, texts, images, figures, tables or other files herein, including, but not limited to, its ownership and the intellectual property rights, are reserved to eMemory Technology Incorporated and PUFsecurity Corporation. This information may contain 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.

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 65M wafers shipped.

1260+
Patents Issued

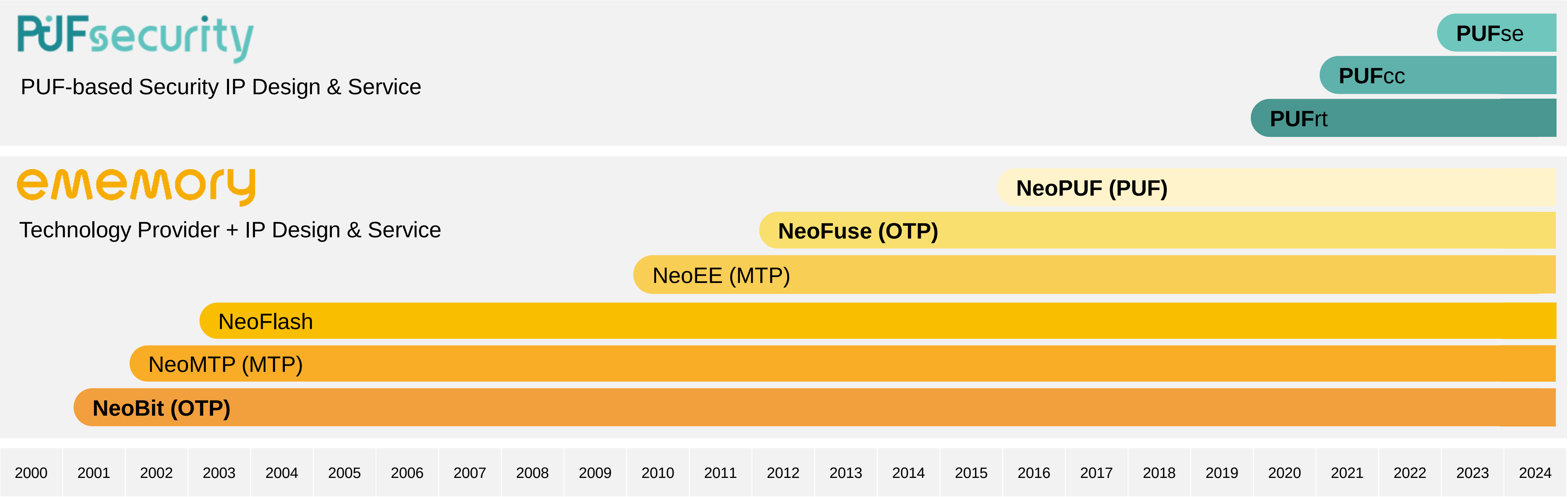
203 pending patents. 360 employees with 68% R&D personnel.

Best IP Partner
With TSMC

TSMC Best IP Partner Award since 2010.

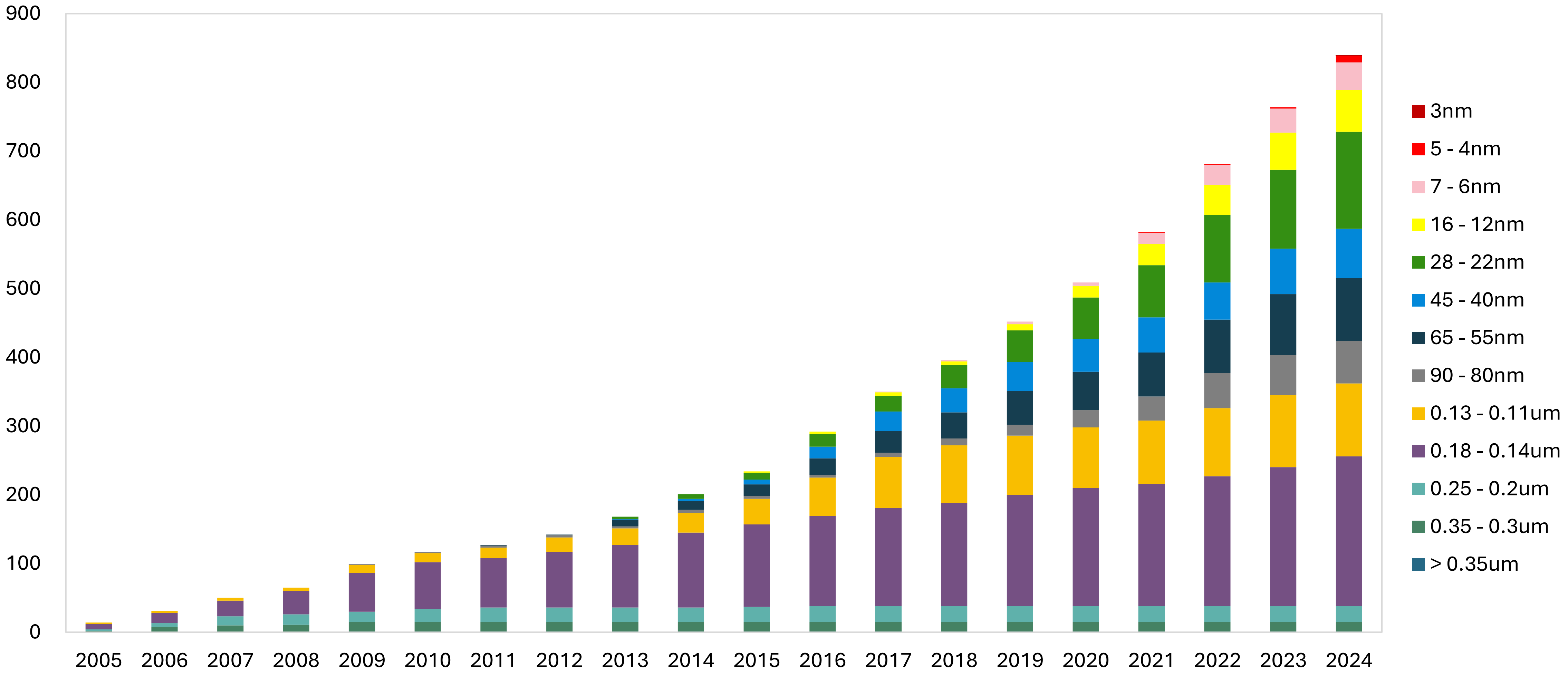
公司產品技術

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.



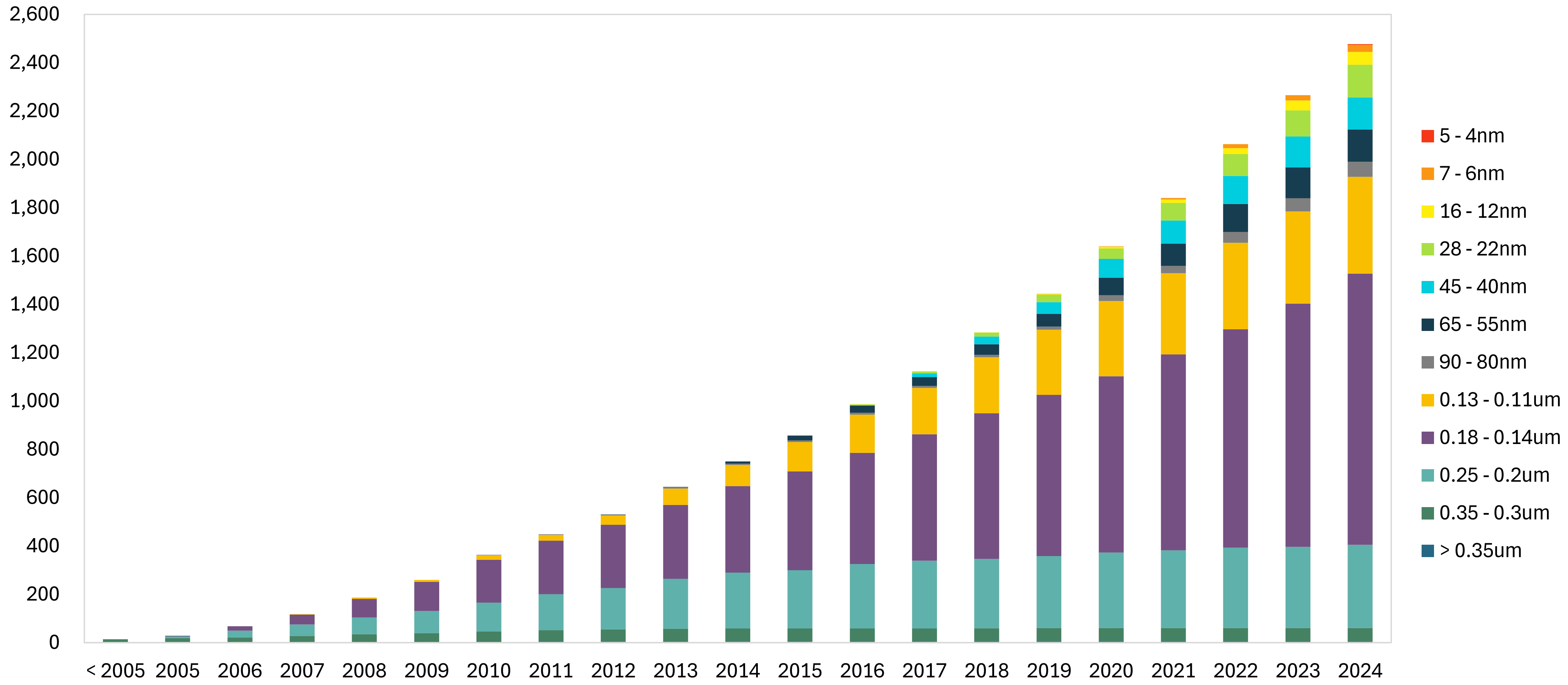
Registered IPs at TSMC .

Registered IP > 750



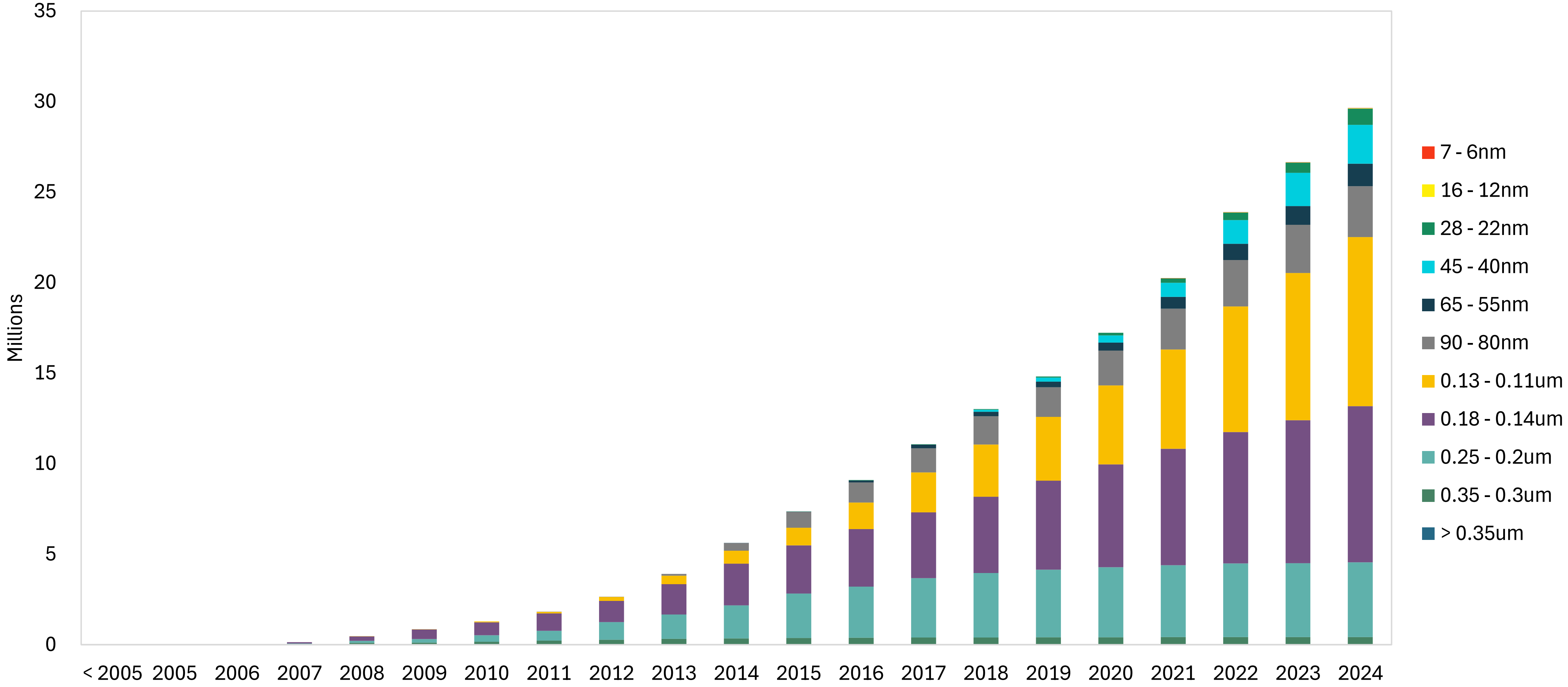
NTOs at TSMC

New Tape Out Contribution > 2400



Wafer Contribution at TSMC

8” Wafer Contribution > 25M



Revenue and Tape-out by Technology

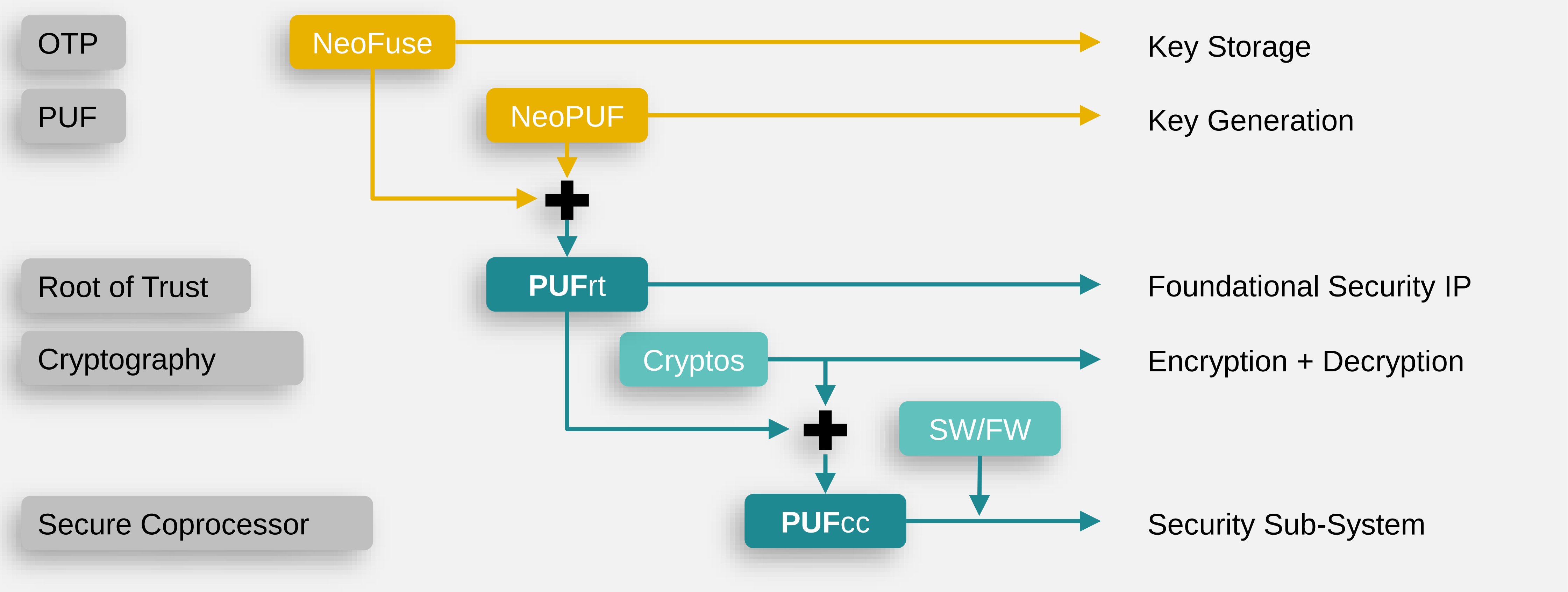
	NTO		Revenue (USD)		
Year	**NeoBit**	**NeoFuse**	**NeoBit**	**NeoFuse**	**PUF-based**
2002	3				
2003	29				
2004	40				
2005	68		$ 4,217,380		
2006	133		$ 6,202,270		
2007	220		$ 9,402,479		
2008	253		$ 12,896,211		
2009	268		$ 11,695,587		
2010	284		$ 15,873,331		
2011	254		$ 15,399,098		
2012	270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

PUF-based Security Solutions

- Based on OTP Technologies, many different security functions IPs have evolved
- Regulations, such as TPM 2.0, now require Hardware Root of Trust



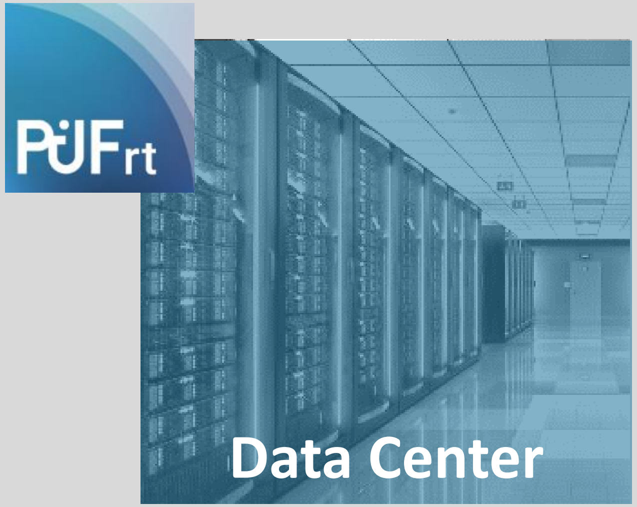
Standards Drive Hardware-Based Security .

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

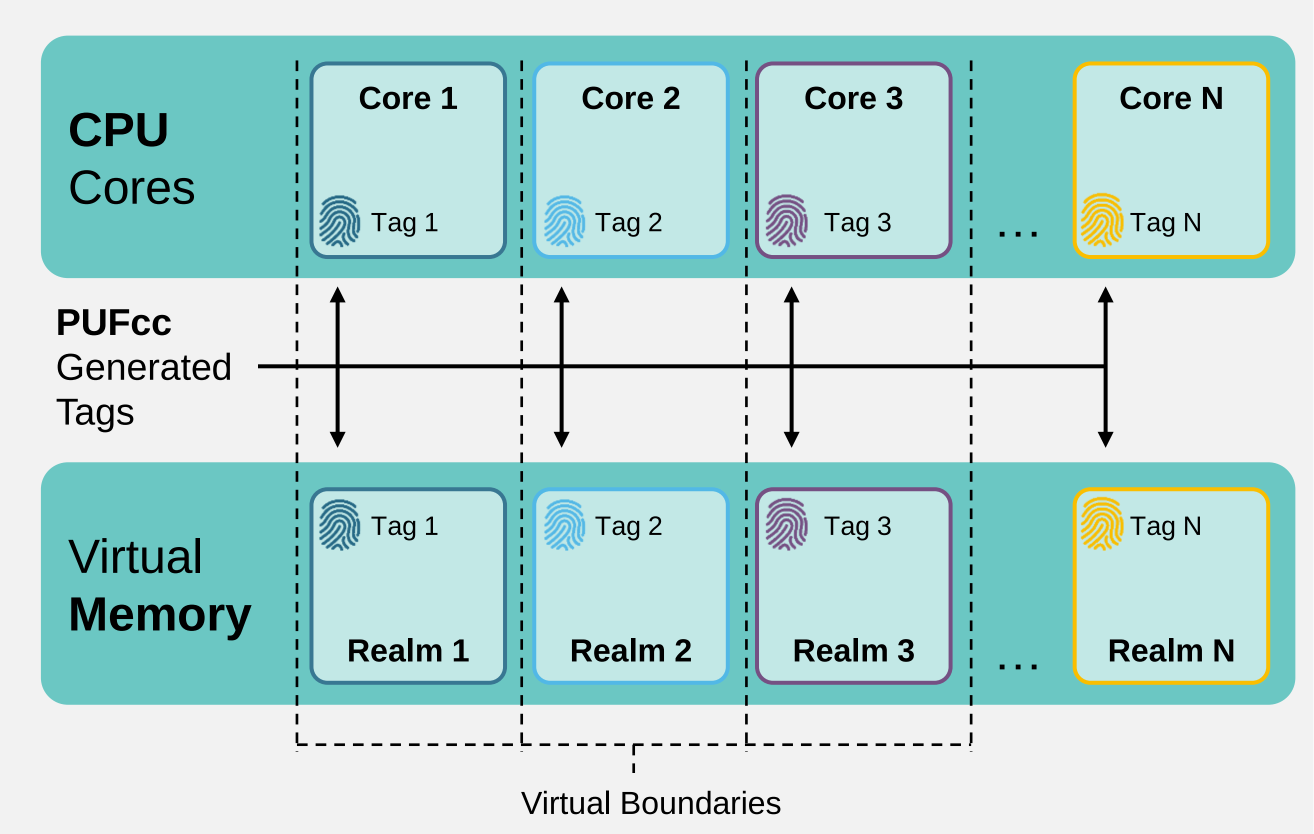
- Work with CSP and system companies for embedded security on a chip level

Market **Application** .

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

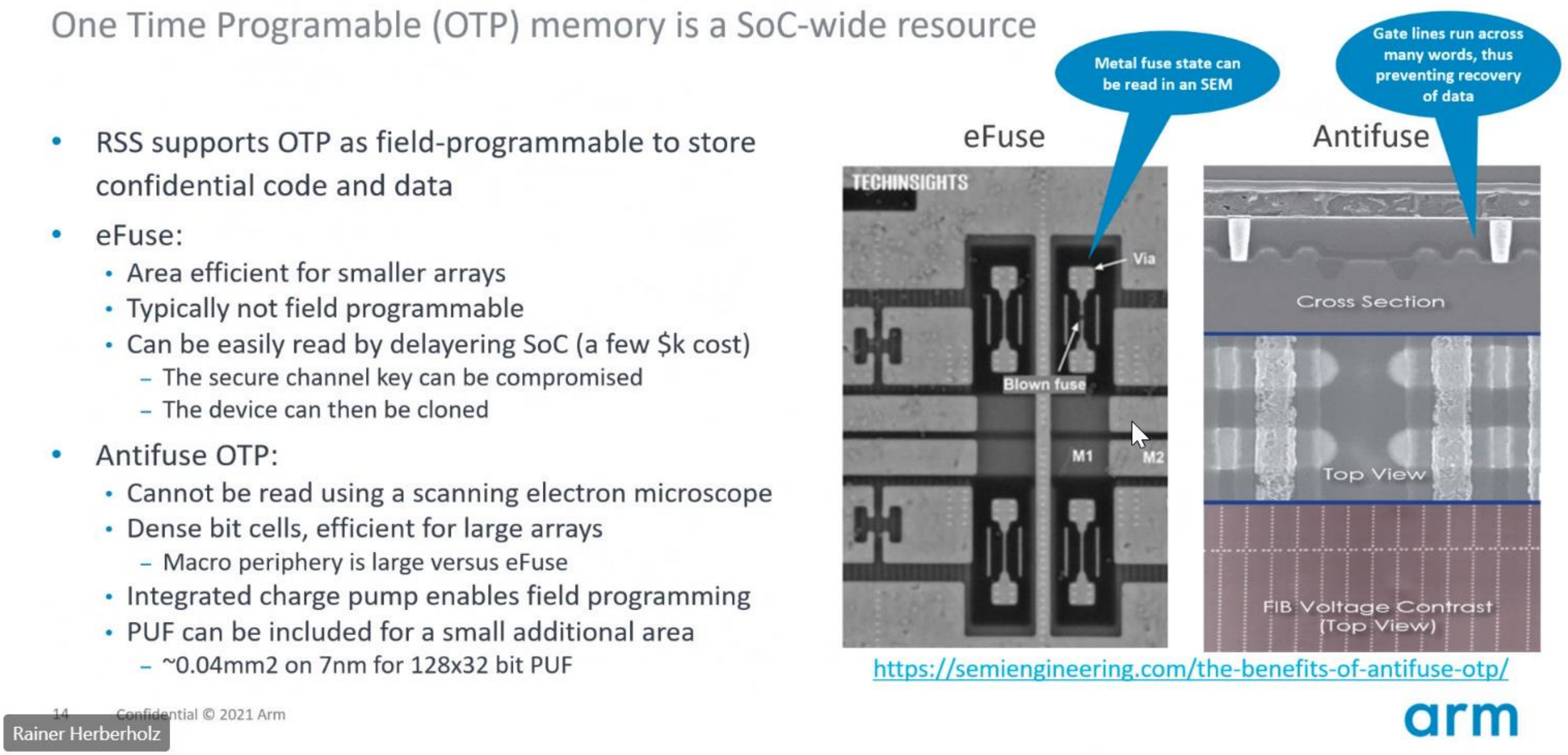
CPU	AI	SSD
DPU	DTV/STB	Wi-Fi
FPGA	ISP	And More.

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

Metal fuse state can be read in an SEM

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

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

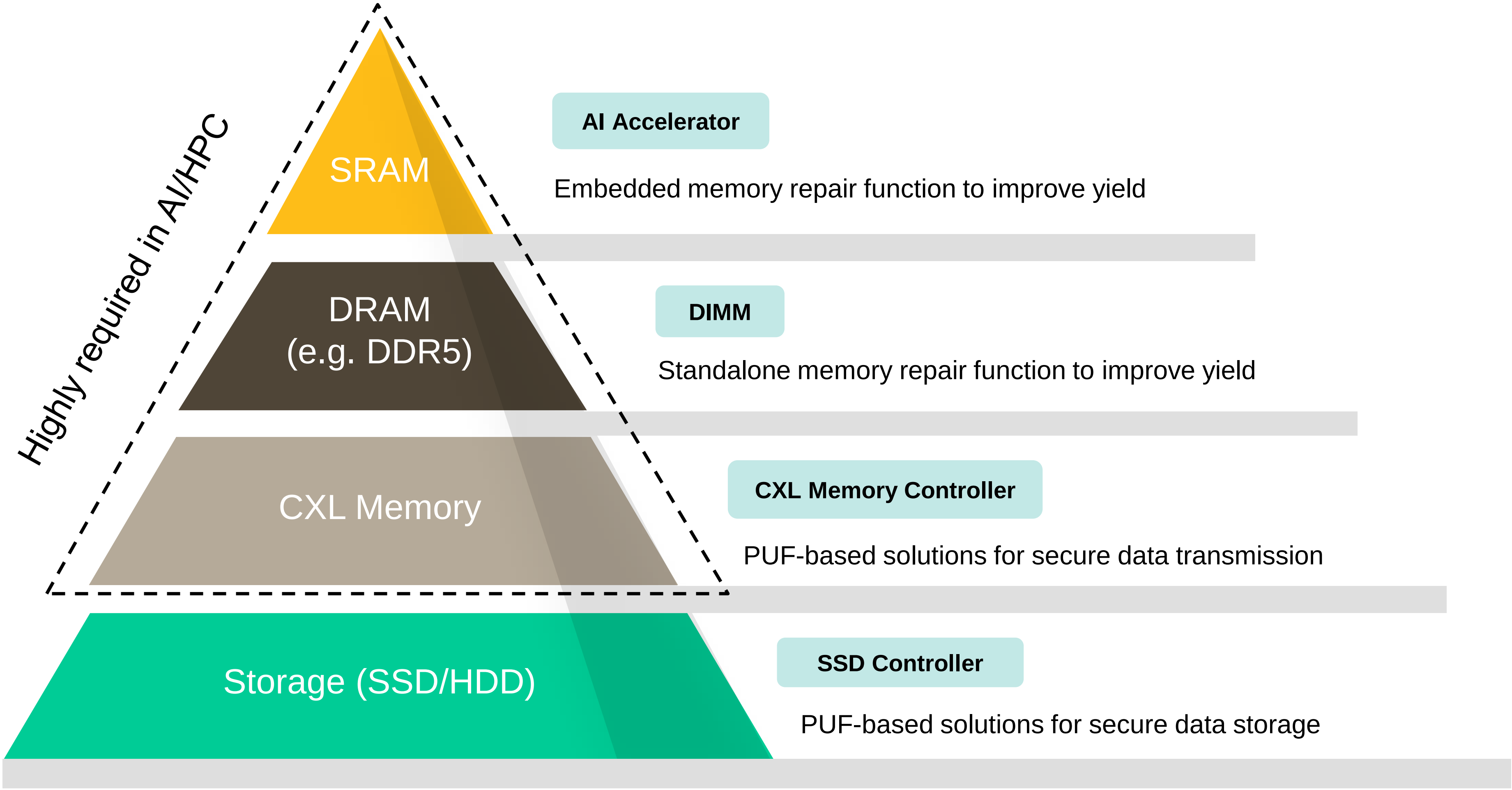
14 Confidential © 2021 Arm

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.



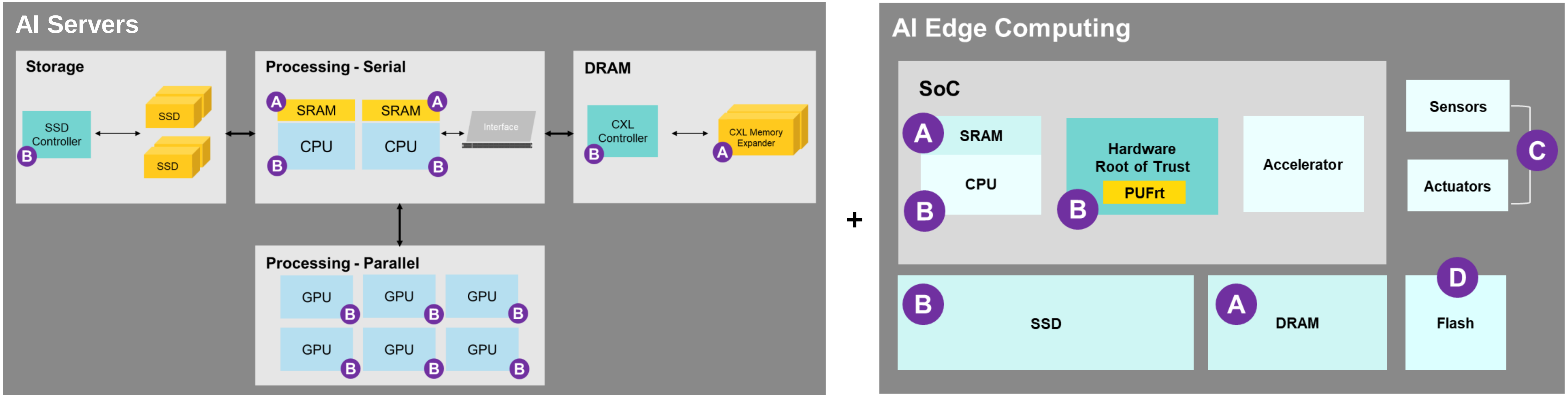
Embedded memory repair function to improve yield

Standalone memory repair function to improve yield

PUF-based solutions for secure data transmission

PUF-based solutions for secure data storage

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



A **Memory Repair**

B **Root of Trust** provides:

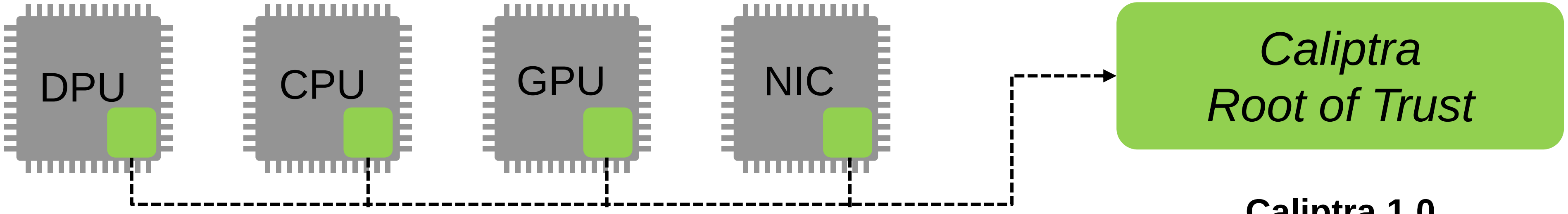
1. Key storage/generation
2. Cryptographic processing to protect AI models, input data and output results
3. Confidential Computing

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?

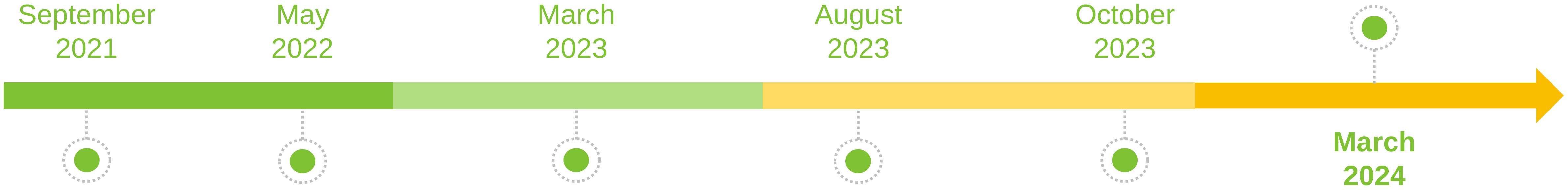
Datacenter Chips



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

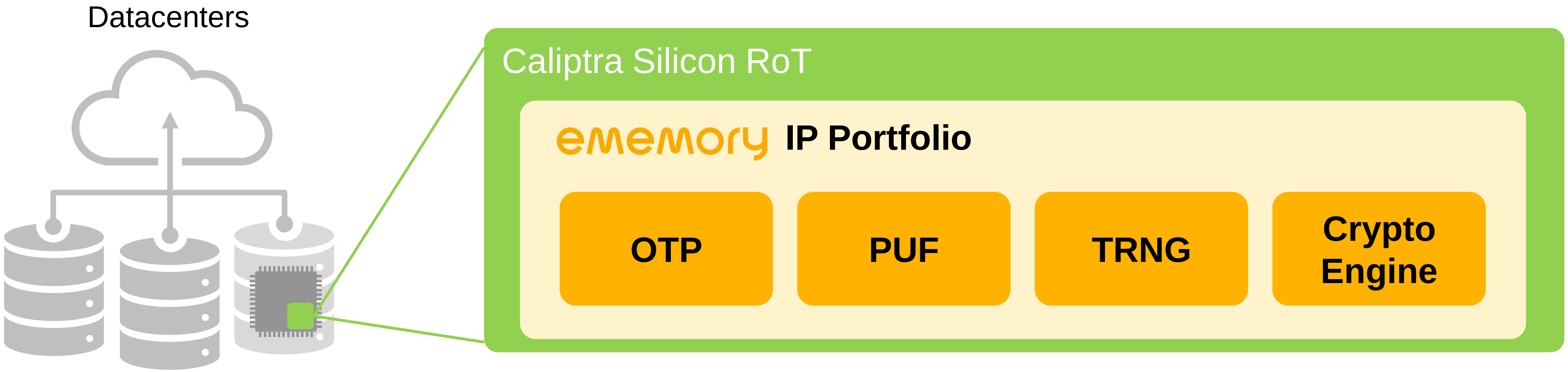
All flows are defined and are implemented in RTL

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.



Datacenters

Caliptra Silicon RoT

ememory **IP Portfolio**

OTP

PUF

TRNG

Crypto Engine

Unique Chip Identity

Chip Fingerprint

Secure Attestation

Device Certificate

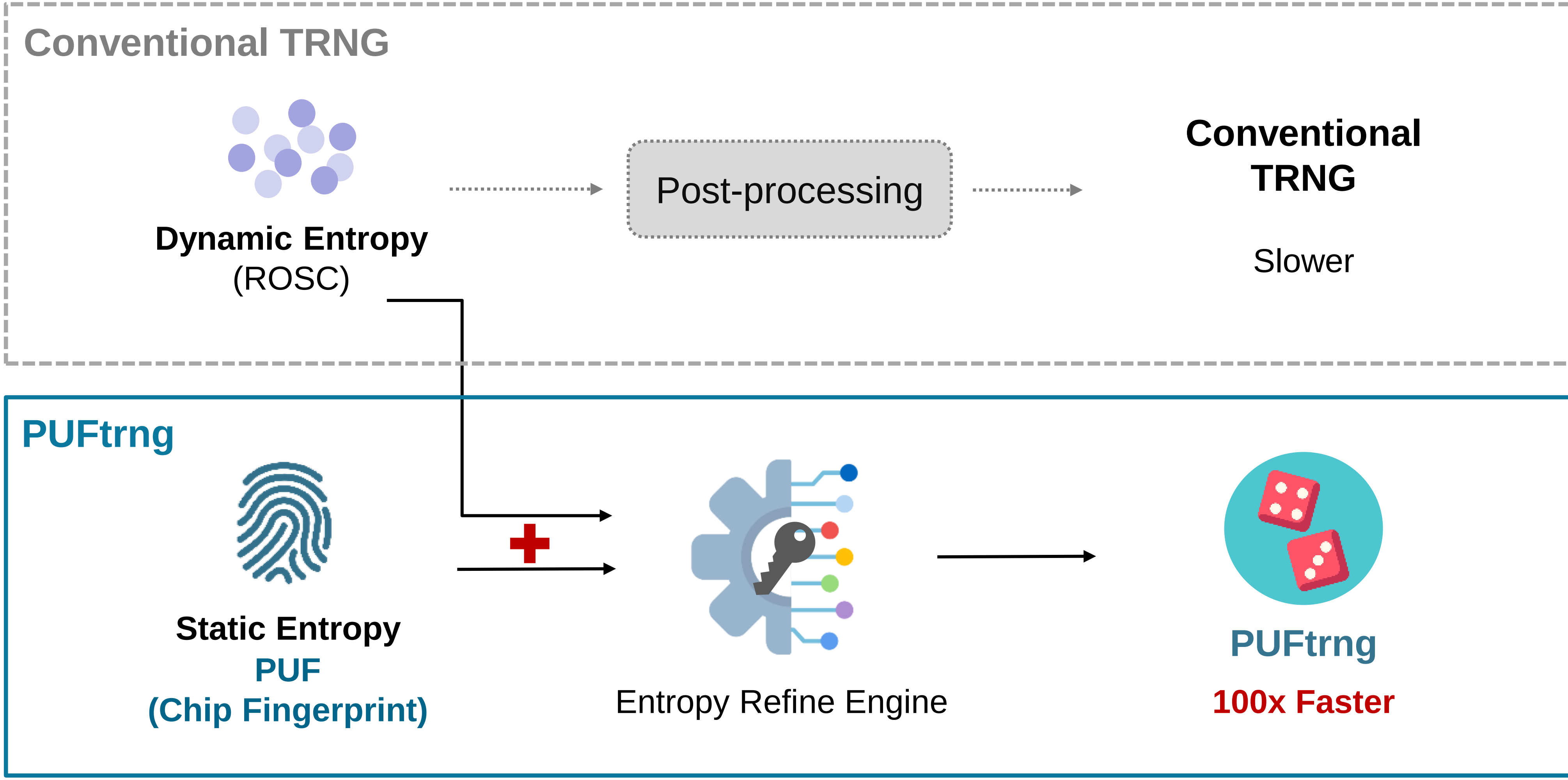
Secure Boot

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

PUFtrng

Static Entropy
PUF
(Chip Fingerprint)

Entropy Refine Engine

PUFtrng

100x Faster

Classic Cars

New Energy Cars

PUFtrng: 100 Times Faster than Conventional TRNG

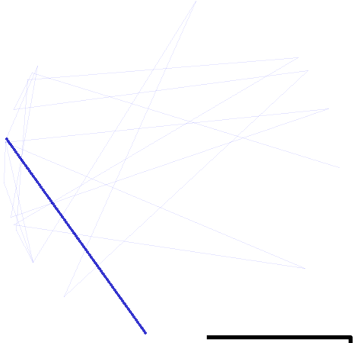
- PUF-based conditioning algorithm provides high-throughput and high-quality entropy

Similar to…

Conventional TRNG

Figure 1:

Dynamic Entropy



Post-processing

Figure 2:

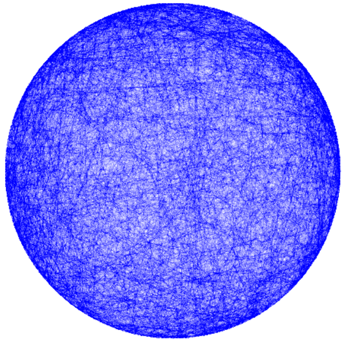
Conventional TRNG
→ Low throughput random bits
→ Slower

Classic Cars

PUFtrng

Figure 3:

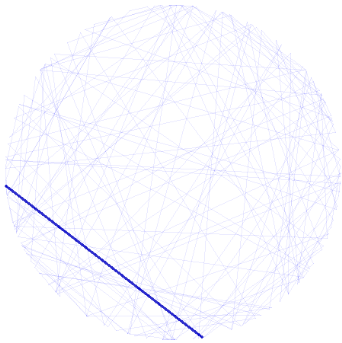
Static Entropy
→ **PUF**
(chip fingerprint)



Entropy Refine Engine

Figure 4:

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



New Energy Cars

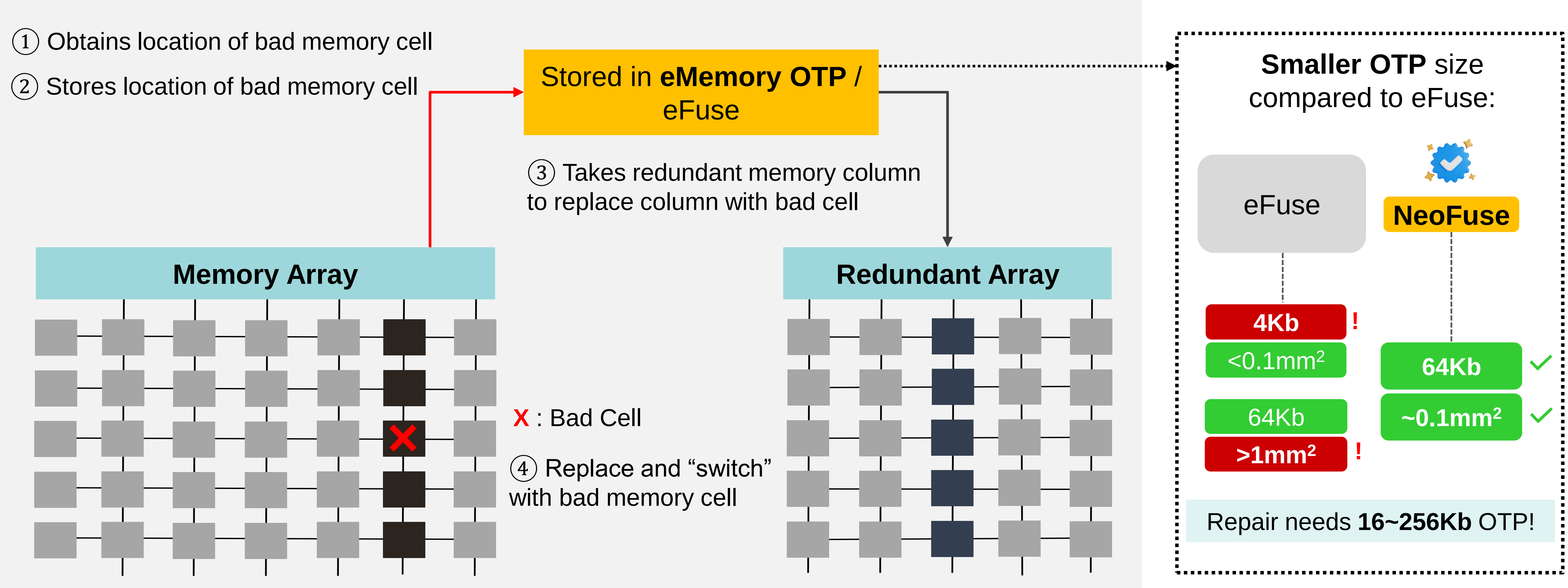
Why is **High-Density SRAM** needed in **AI?**

- 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.



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

X : Bad Cell

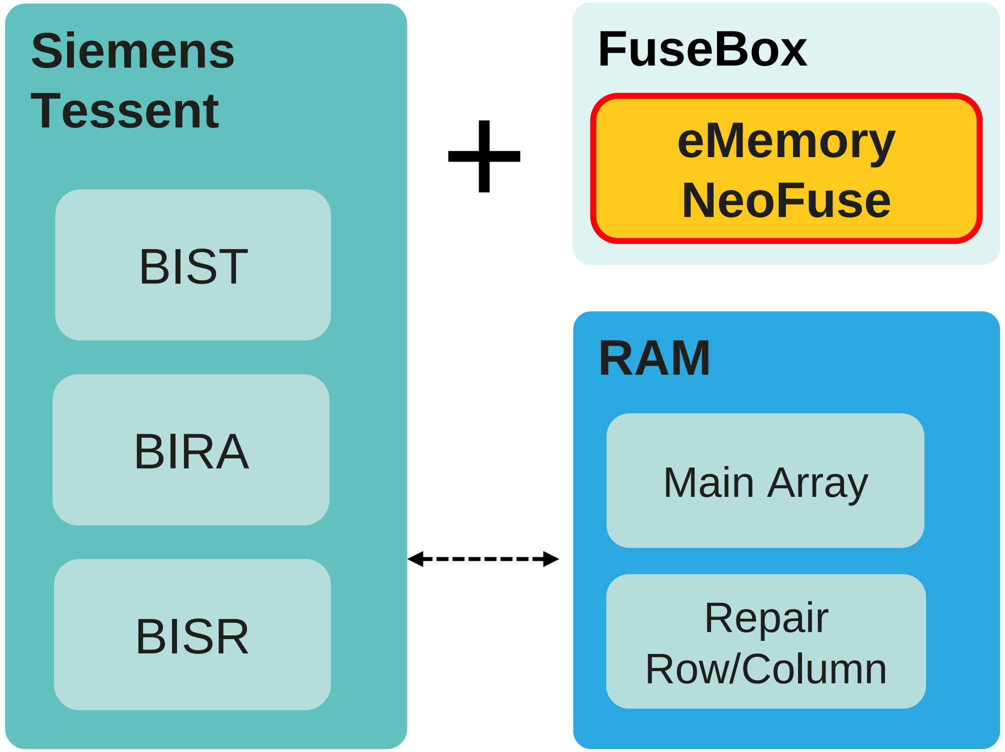
④ Replace and "switch" with bad memory cell

Smaller OTP size compared to eFuse:

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

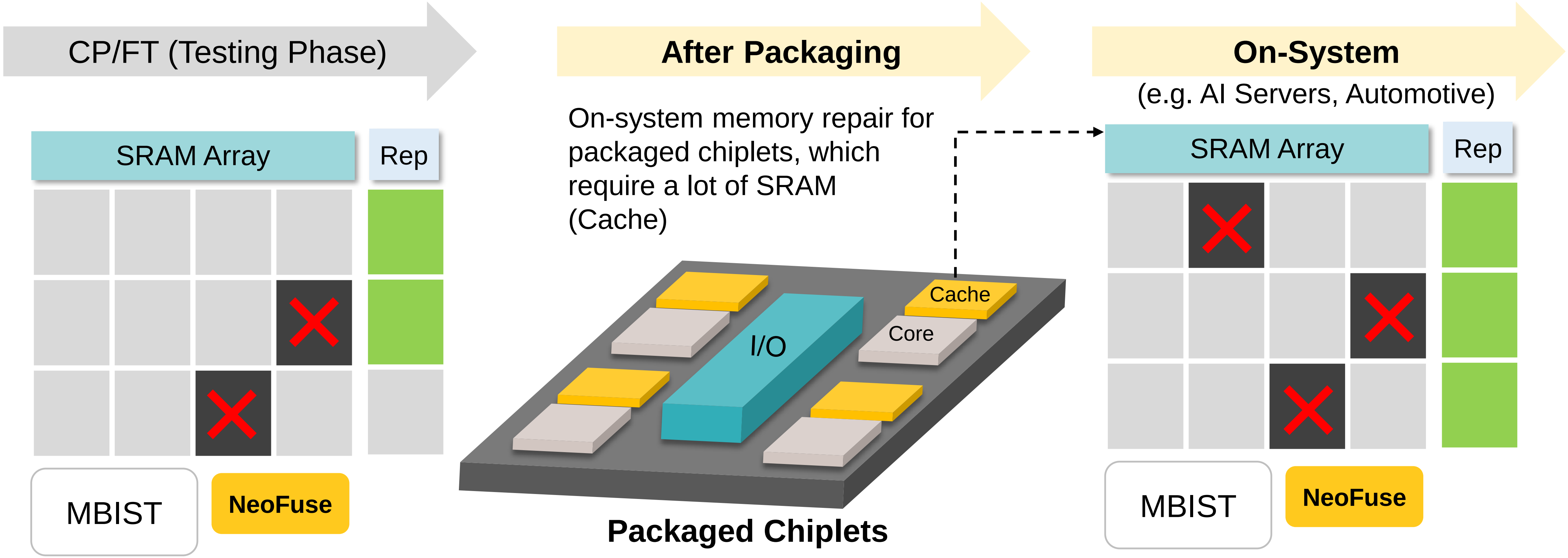
eMemory provides OTP with interface for Siemens MBIST:

- **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, scann ing defective SRAM by word/column and loggin g 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.



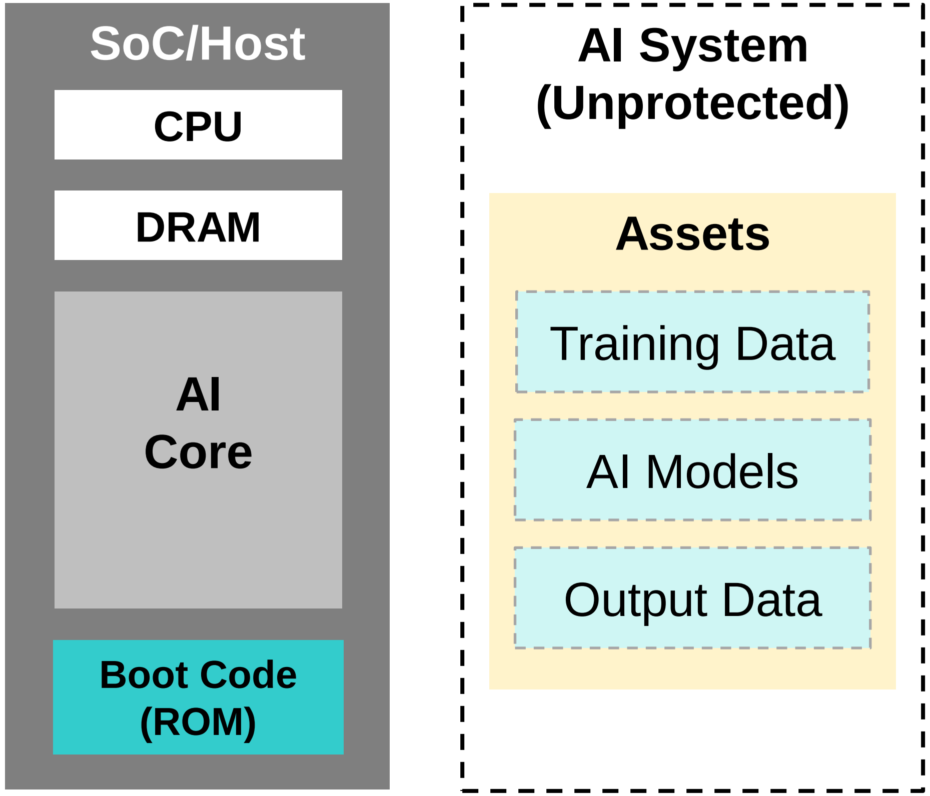
On-system memory repair for packaged chiplets, which require a lot of SRAM (Cache)

Made possible with MBIST

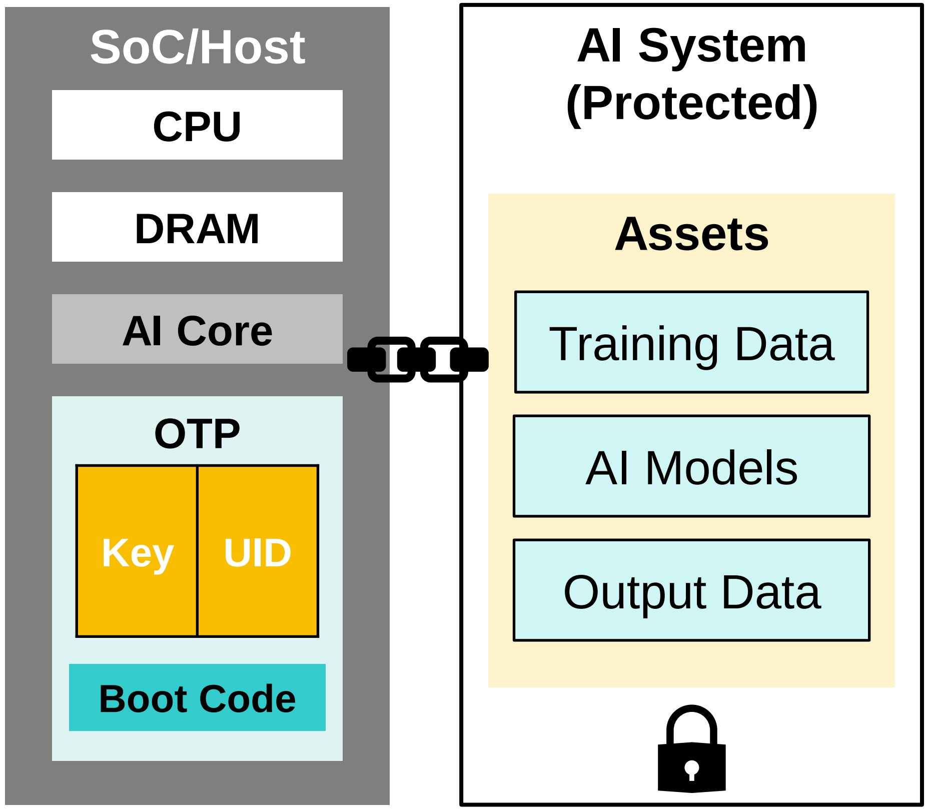
eMemory enables HPC in **AI Applications**

- **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



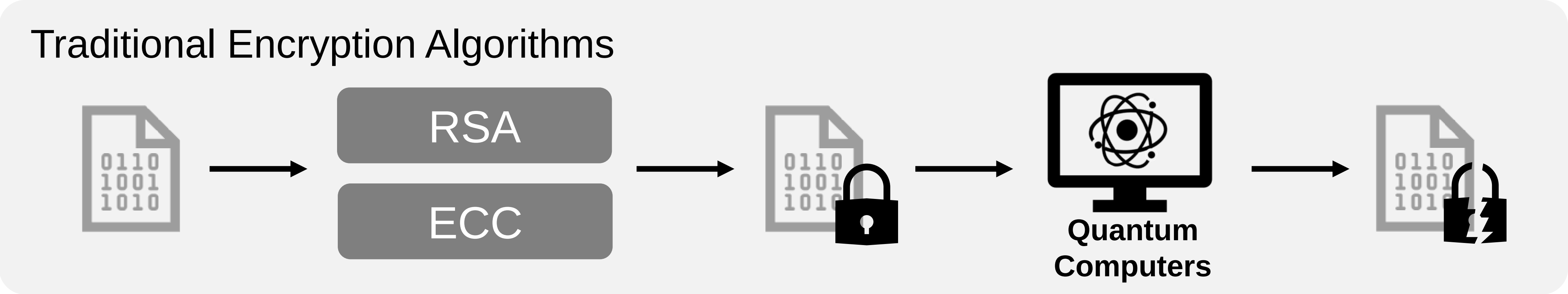
Why **PQC** Needs **PUF**?

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.

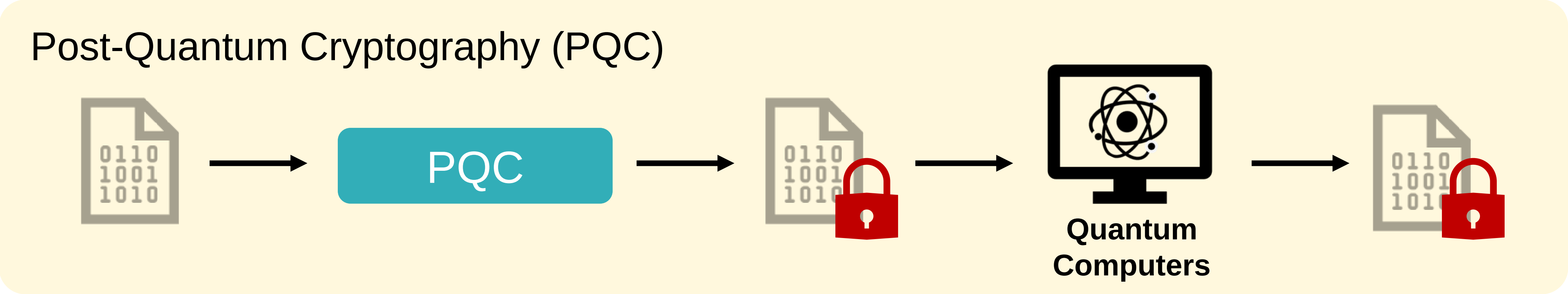


Traditional Encryption Algorithms

RSA

ECC

Quantum Computers



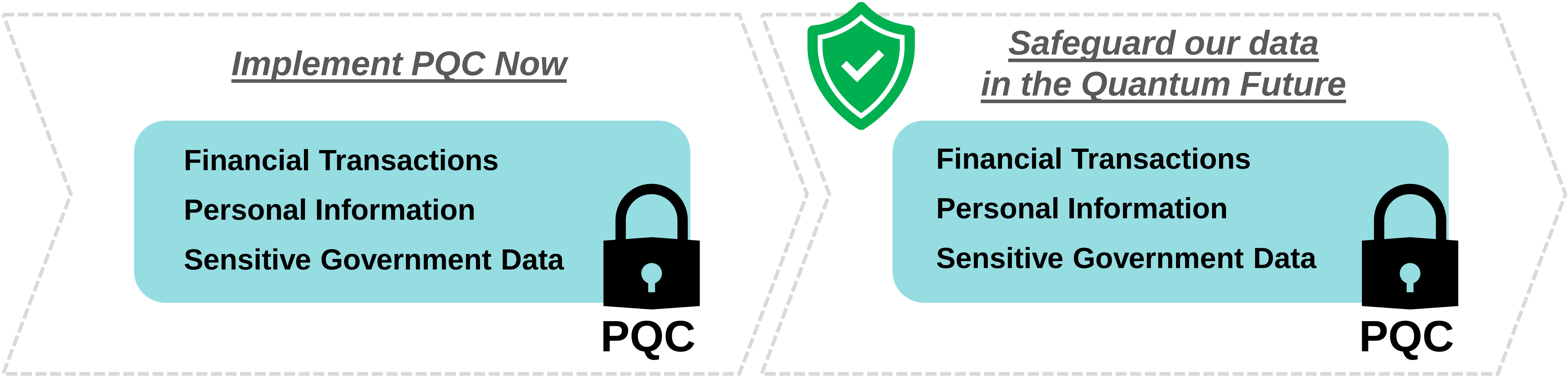
Post-Quantum Cryptography (PQC)

PQC

Quantum Computers

Why is **PQC** Needed?

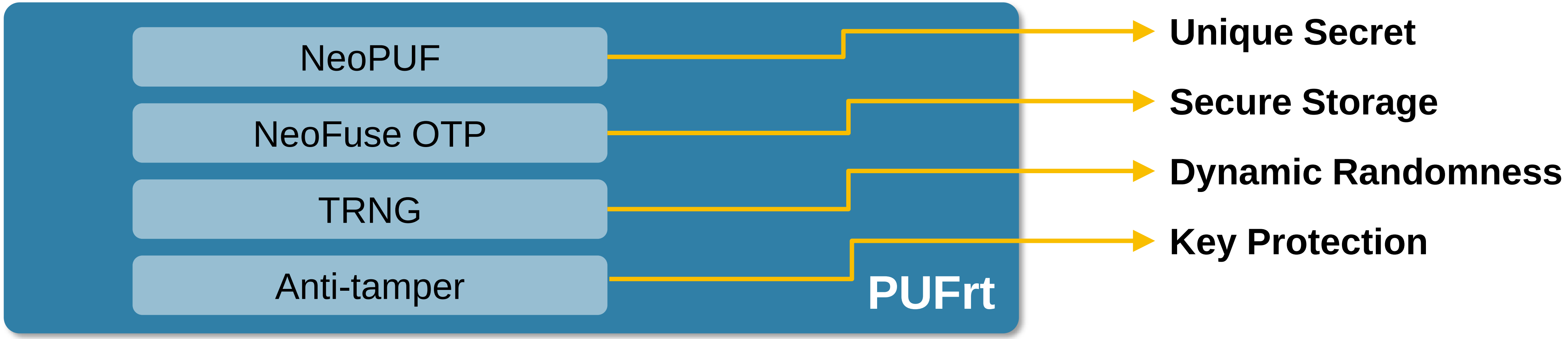
- As quantum computing progresses, the demand for encryption capable of resisting quantum attacks becomes critical.
- The sooner we implement PQC, the sooner we can guarantee the security of our data in a quantum future.



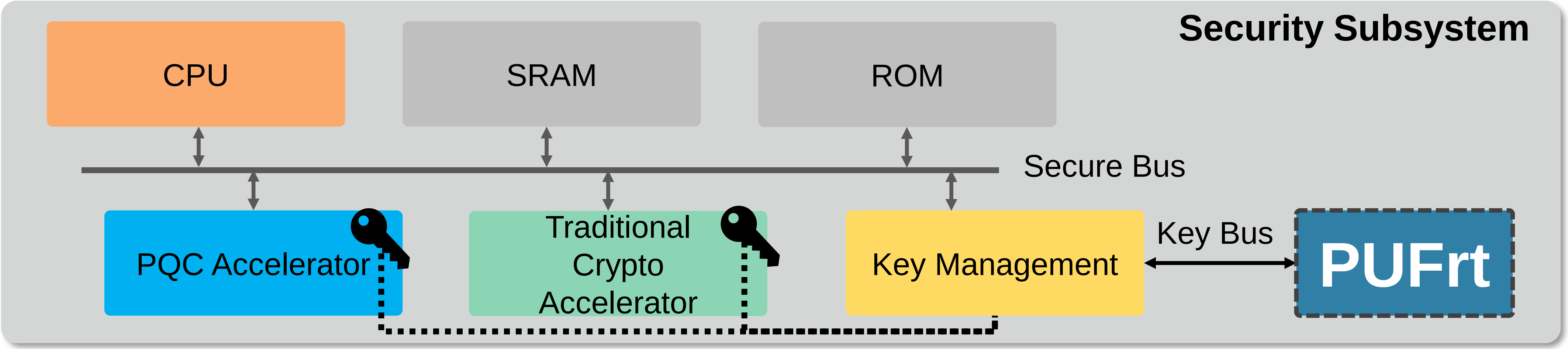
- In 2024, NIST officially announced three standards for PQC:
  - FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
  - FIPS 204, Module-Lattice-Based Digital Signature Standard
  - FIPS 205, Hash-Based Digital Signature Standard

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.



Thank You for your time

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