A Comprehensive Post-Quantum Cryptography (PQC) Solution based on Physical Unclonable Function (PUF)

Securing SoCs for the Quantum Computing Era

WHITE PAPER - Security IP

eMemory Technology Inc.
PUFsecurity Corp.
January 2026

Introduction

The official release of the FIPS 203, 204, and 205 standards by the National Institute of Standards and Technology (NIST) marks the finalization of Post-Quantum Cryptography (PQC) standards [1-3]. This milestone not only heralds a new era but also initiates the most fundamental security architecture migration for the global semiconductor industry since the advent of RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). While this transition aims to mitigate the threats posed by future quantum computing, the intrinsic characteristics of PQC algorithms – particularly the complex matrix and polynomial operations associated with lattice-based cryptography, along with substantial key sizes – impose unprecedented challenges on system-on-chip (SoC) designs regarding **performance, power, and area** (**PPA**).

Spanning from resource-constrained IoT devices to high-performance computing (HPC) platforms demanding extreme throughput, how can designers achieve an optimal trade-off between performance and cost? In response, PUFsecurity and eMemory have introduced the PUF-PQC solution, anchored by a design philosophy of "modular thinking." By offering two distinct architectural strategies, PUF-PQC facilitates a seamless transition for clients addressing post-quantum requirements.

This article provides an in-depth analysis of the specific PPA challenges introduced by PQC and elucidates how PUF-PQC leverages its unique dual-track strategy to deliver a robust and flexible Hardware Root of Trust (HRoT) across diverse application scenarios. Furthermore, it demonstrates the integration of Physical Unclonable Function (PUF) with a NIST SP 800-90B compliant True Random Number Generator (TRNG) to serve as critical components of PUFrt (Root of Trust), ensuring the security of post-quantum key generation starting from the entropy source.

1. Engineering Challenges of PQC Integration

While traditional public-key cryptography relies on the hardness of integer factorization or discrete logarithm problems, the PQC standards selected by NIST encompasses lattice-based cryptography (e.g., ML-KEM [1] and ML-DSA [2]) and hash-based cryptography (e.g., SLH-DSA) [3]. A thorough analysis of the impact of PQC on SoC design constitutes the strategic first step in comprehending next-generation security architectures. The severe challenges PQC algorithms pose to PPA metrics stem from two interconnected core characteristics, algorithmic complexity and data volume. These factors create a causal chain that directly impacts three critical SoC design metrics:

- *Performance*: PQC algorithms, particularly lattice-based schemes, involve extensive Number Theoretic Transform (NTT) and polynomial arithmetic. These highly intensive matrix operations consume significant processor cycles. Consequently, a pure software implementation would severely degrade the execution efficiency of the system's main applications.

- *Power & Bandwidth*: concurrently, compared to legacy RSA and ECC, PQC public and private key sizes can be orders of magnitude larger. Handling substantially larger keys sizes during encryption and decryption imposes extreme demands on memory access bandwidth. This not only increases system power consumption but also creates critical performance bottlenecks that may partially offset the benefits gained from hardware acceleration.

- *Area*: to mitigate the performance bottlenecks, hardware acceleration becomes imperative. However, constructing a hardware engine capable of efficiently executing complex PQC operations requires a substantial number of logic gates and memory circuits. This necessity drives a significant increase in silicon die area, thereby escalating chip manufacturing costs.

Under the triple constraints of PPA, a monolithic, "one-size-fits-all" solution is no longer viable for diverse application scenarios. From cost-sensitive microcontrollers (MCUs) to AI servers demanding extreme computational power, the market requires flexible strategies. This specific need serves as the entry point for the modular design philosophy behind the PUF-PQC solution by eMemory and PUFsecurity.

[1] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203)*. U.S. Department of Commerce, Aug. 2024.

[2] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard (FIPS 204)*. U.S. Department of Commerce, Aug. 2024.

[3] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard (FIPS 205)*. U.S. Department of Commerce, Aug. 2024.

2. The Modular Strategy of PUF-PQC

To address diverse application scenarios ranging from ultra-lightweight devices to high-performance computing, PUF-PQC offers two distinct architectural approaches to hardware integration.

Architecture Option 1, PUF-PQC Engine (PSCE_1300 series): Ultra-Lightweight Pure Hardware Acceleration

- **Target applications**: IoT endpoint devices, smart cards, and low-cost MCUs.

The PUF-PQC Engine is a pure hardware accelerator developed according to the design philosophy of “lean architecture”. This architecture (**Fig. 1**) offloads high-level instruction scheduling to the host CPU to minimize silicon footprint. Secure Hash Algorithm (SHA) and Support / Polynomial Logic (SPL) components are also included in this Engine.

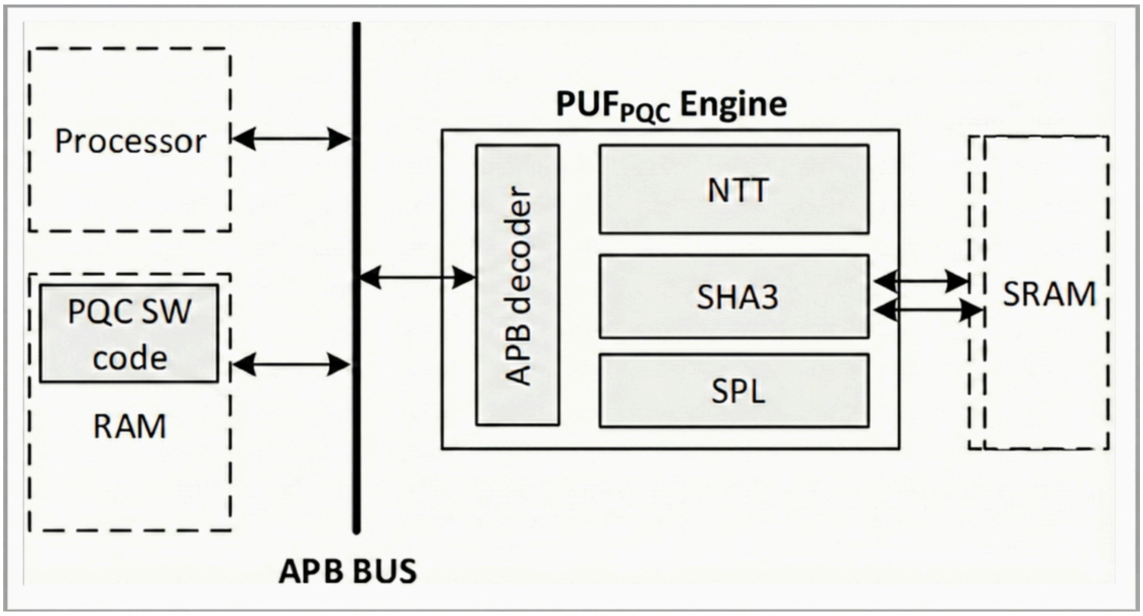


Figure 1. PUF-PQC Engine architecture.

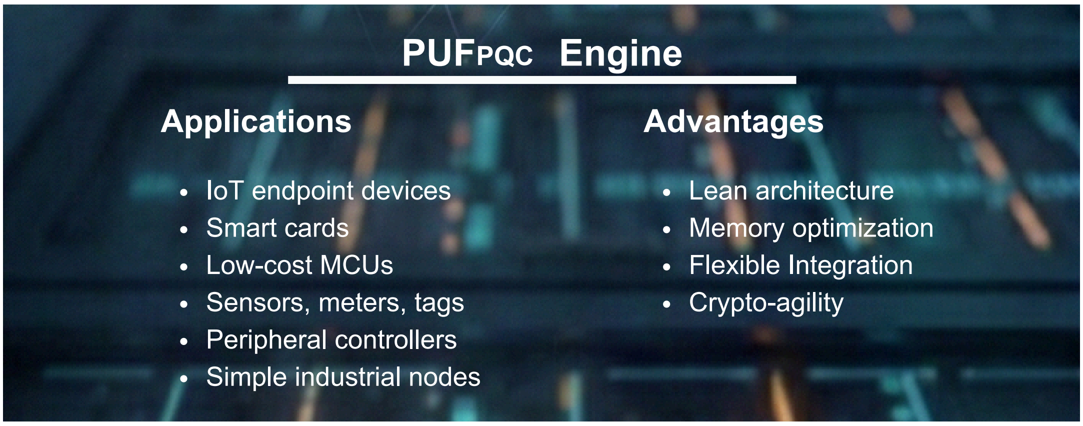
Advantages of the PUF-PQC Engine:

- *Lean architecture design*: the design eliminates the embedded CPU core, retaining only the core arithmetic units and essential control logic. This approach significantly reduces the total gate count.

- *Memory optimization*: the engine adopts a multi-bank single-port SRAM architecture paired with conflict-free scheduling techniques. Compared to traditional dual-port designs, this solution substantially reduces memory area while maintaining the high memory access bandwidth required for Number Theoretic Transform (NTT) operations. Furthermore, it supports configurable SRAM size, allowing designers to precisely tailor the memory footprint based on the selected algorithm parameter sets (e.g., ML-KEM-512 vs. ML-KEM-1024).

- *Flexible integration*: the engine integrates seamlessly via standard bus interfaces (e.g., APB or AHB), attaching directly to the system interconnect. This architecture is highly suitable for cost-constrained and area-sensitive design projects.

- *Crypto-agility*: the PUF-PQC engine is capable of adapting to future algorithm fine-tuning, standard extensions, or parameter modifications through updates to the supporting firmware architecture.



PUFPQC Engine

Applications

- IoT endpoint devices
- Smart cards
- Low-cost MCUs
- Sensors, meters, tags
- Peripheral controllers
- Simple industrial nodes

Advantages

- Lean architecture
- Memory optimization
- Flexible Integration
- Crypto-agility

Architecture Option 2, PUF-PQC Subsystem (PSHSM_180 series): Host CPU Offloading and Heterogeneous Integration

- **Target applications**: high-performance computing (HPC), automotive electronics (ADAS/V2X), and edge AI servers.

The PUF-PQC Subsystem functions as a "security island" aligned with architectural concepts of PSA certified levels 3 and 4. The system integrates a dedicated RISC-V processor (MCU), embedded firmware, and hardware acceleration units, establishing an isolated and secure computational environment (**Fig. 2**).

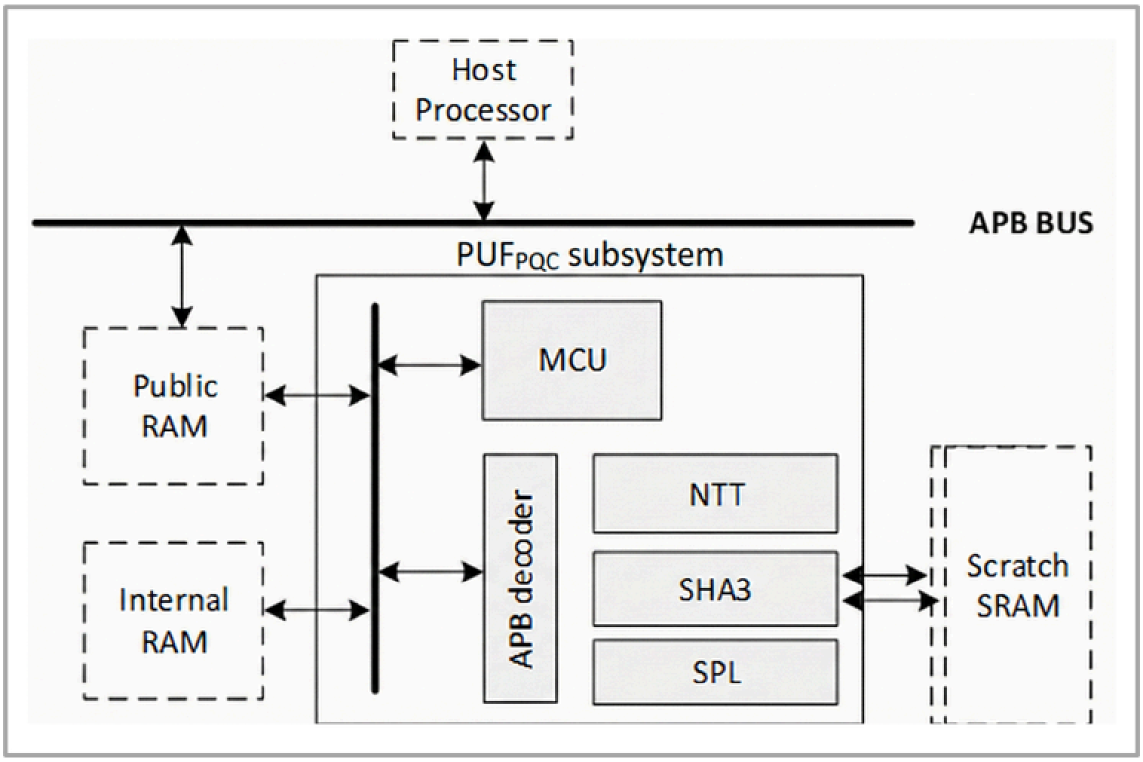


Figure 2. PUF-PQC Subsystem architecture.

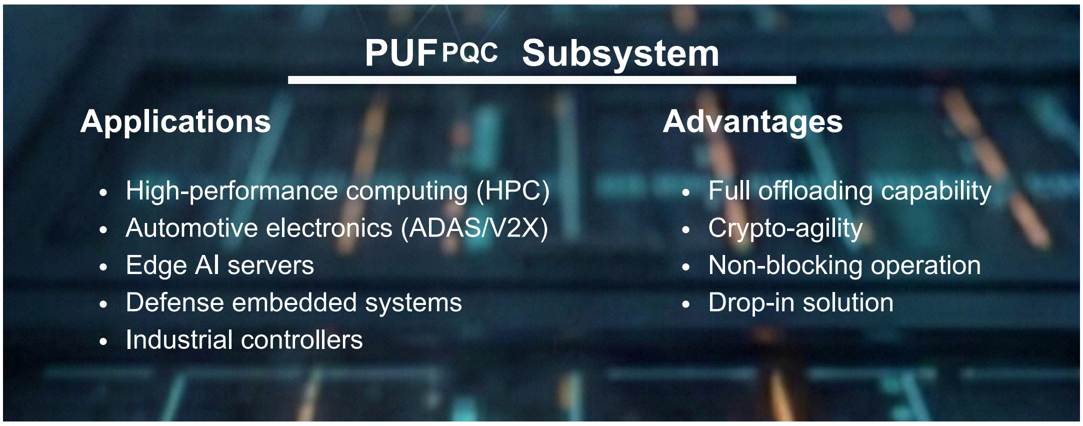
Advantages of the PUF-PQC Subsystem:

- *Full offloading capability*: this represents the subsystem's core value proposition. It autonomously executes complete PQC protocols (including keygen, encapsulate, decapsulate, sign, and verify) as well as SHA3/SHAKE hash operations. The host CPU issues high-level commands via the bus interface without intervening in the underlying complex mathematical computations, effectively offloading the main processor.

- *Crypto-agility*: leveraging the built-in RISC-V core and an updatable firmware architecture, the PUF-PQC Subsystem is engineered to accommodate future algorithm fine-tuning, standard extensions, or parameter modifications. This capability not only extends the product lifecycle but also provides clients with the flexibility for future field updates.

- *Non-blocking operation*: communication is facilitated via shared memory and a mailbox mechanism. The host CPU can resume other tasks immediately after dispatching a request, preventing system pipeline stalls and thereby enhancing overall system throughput.

- *Drop-in solution*: since the complex algorithmic logic is fully encapsulated within the subsystem's firmware, the complexity of integrating the SoC software stack and the associated verification time are significantly reduced, accelerating time-to-market.



PUF PQC Subsystem

Applications

- High-performance computing (HPC)
- Automotive electronics (ADAS/V2X)
- Edge AI servers
- Defense embedded systems
- Industrial controllers

Advantages

- Full offloading capability
- Crypto-agility
- Non-blocking operation
- Drop-in solution

3. Selecting Suitable PQC Solution for Your Application

When selecting a PUF-PQC architecture, trade-offs between the following key metrics that must be considered:

Product / Feature	PSCE_1300 series	PSHSM_180 series
Architecture	PUF-PQC Engine	PUF-PQC Subsystem
Algorithm Support	FIPS 203, FIPS 204	FIPS 203, FIPS 204
Silicon Area	minimal	larger (Includes CPU & extra SRAM)
HOST CPU Loading	high (responsible for instruction scheduling)	very Low (full offloading)
Integration Complexity	host CPU must integrate IP API/FW	simple (high-level API)
Flexibility	both feature crypto-agility, supporting firmware updates to comply with future algorithmic standards	
System Performance	depends on host capability	optimal (parallel processing)
Deliverables	HW: RTL SW: FW/API	HW: RTL SW: HOST FW/API, ROM

For SoCs running complex operating systems like Linux/Android, although the PUF-PQC Subsystem increases area cost, it frees up valuable host processor power and isolates the security boundary, making it the preferred choice for high-end applications.

4. Hardware Root of Trust for PUF-PQC: Integration of PUFrt

While PQC algorithms guarantee the quantum resistance of the computational process, the security of the system is compromised if the entropy source of the key generation lacks randomness. The PUF-PQC solution deeply integrates the PUFrt HRoT [4] developed by PUFsecurity and eMemory. By anchoring security in the physical essence of the silicon, it establishes an immutable chain of trust for key generation.

The importance of entropy sources

The NIST SP 800-90A/B/C standard series emphasizes the critical role of high-quality entropy sources in cryptographic systems. If the random number seed is predictable or reproducible, attackers can derive the private key without needing to break the PQC algorithm itself, rendering the encryption futile.

Synergistic integration of PUFrt and PUF-PQC

Integration of PUFrt employs the following mechanisms to ensure robust and hardware-rooted key generation (**Fig. 3**):

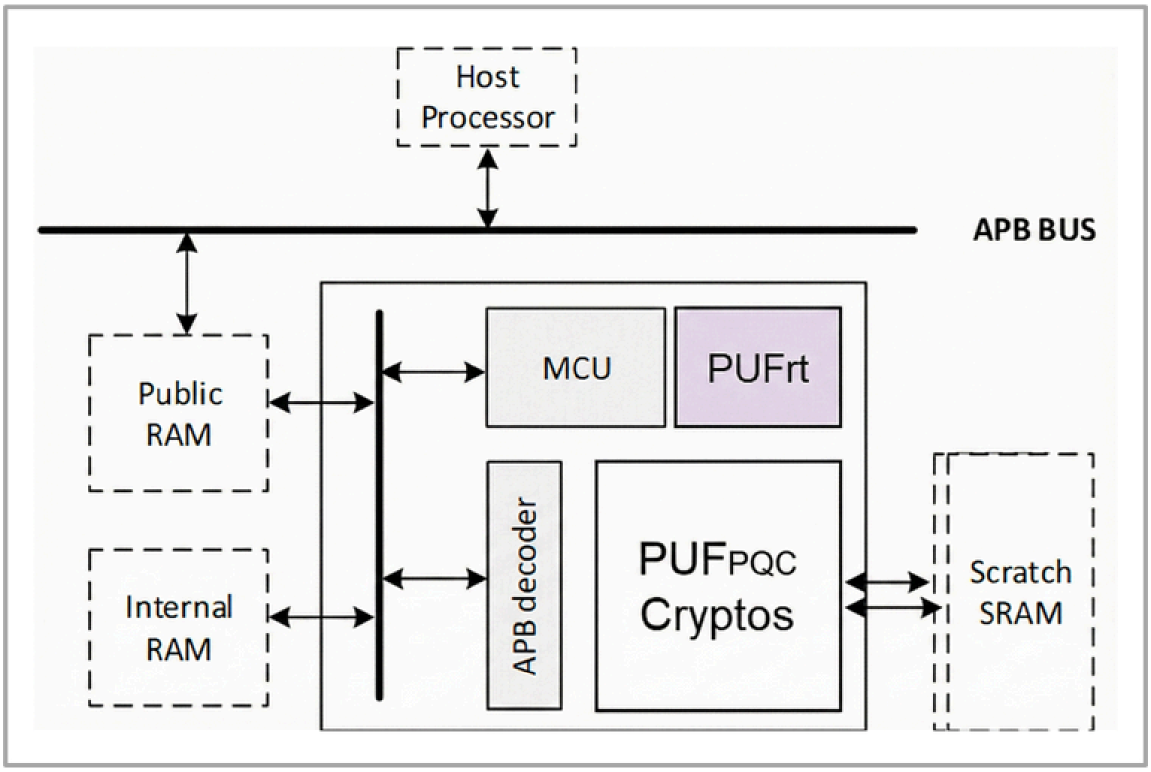


Figure 3. PUF-PQC Subsystem with PUFrt, offering a one-stop PQC solution.

- ***Intrinsic Unique Device Secret** (UDS)*: leveraging eMemory's **NeoPUF** technology [5], the system extracts microscopic process variations inherent in the silicon manufacturing process to generate a unique device identifier. This UDS is utilized to protect the storage and recovery of keys-at-rest.

- ***True Random Number Generator** (TRNG)*: integrating a TRNG compliant with NIST SP 800-90B specifications, delivering high-bandwidth and high-entropy random numbers [6].

- *Secure seeding*: true random numbers generated by the TRNG are directly injected as seeds into the PUF-PQC Engine, ensuring the path remains within the secure boundary.

- *Ephemeral key generation*: utilizing high-quality seeds, the PUF-PQC Engine performs Deterministic Random Bit Generator (DRBG) expansion to compute the ephemeral public-private key pairs (session keys) required for PQC protocols.

- ***NeoFuse One-Time Programmable Memory*** (OTP): Provides highly reliable non-volatile memory for secure storage of sensitive data and cryptographic material, establishing a complete and trusted chain of security.

- *Comprehensive integration*: the fully integrated configuration empowers the system to independently execute PQC secure boot and secure authentication.

This workflow ensures that every PQC key possesses physical-layer unpredictability and is generated entirely within the hardware security boundary. Through PUFrt's robust hardware-level anti-tamper design, the solution significantly mitigates the risks of side-channel attacks (SCA) targeting entropy sources and secure storage, thereby constructing a defense-in-depth architecture for the SoC.

4. eMemory Technology Inc. *PUF-Based Root of Trust (PUFrt) for High-Security AI Application*. eMemory, Sept. 2020,
5. Wu, Ming-Yang, et al. "*A PUF Scheme Using Competing Oxide Rupture with Bit Error Rate Approaching Zero.*" 2018 IEEE International Solid-State Circuits Conference (ISSCC) Digest of Technical Papers, Feb. 2018, pp. 130–132.
6. Turan, Meltem Sönmez, et al. *Recommendation for the Entropy Sources Used for Random Bit Generation*. National Institute of Standards and Technology, Jan. 2018. NIST Special Publication 800-90B.

5. Conclusion

The central challenge of the quantum computing era lies in the absence of a "one-size-fits-all" PQC standardized solution applicable to all scenarios. Market heterogeneity necessitates next-generation security architectures that possess unprecedented flexibility and customization capabilities.

PUFsecurity leverages a dual-track strategy comprising the **PUF-PQC Engine** and the **PUF-PQC Subsystem** to deliver precise solutions tailored for distinct market segments. For either endpoint devices that demand extreme cost-efficiency or edge computing platforms that require peak performance and future agility, PUF-PQC assists clients in constructing a robust, customized security defense system that aligns with their PPA requirements while strictly satisfying PQC compliance.

- The **PUF-PQC Engine**: suitable for projects that are cost-sensitive with its high configurability and compact silicon footprint.

- The **PUF-PQC Subsystem**: ideal for projects requiring a comprehensive security boundary and crypto-agility. Specifically, when integrated with PUFrt that provides complete entropy source and secure storage, the subsystem facilitates the immediate realization of PQC secure boot and secure authentication. This allows clients to benefit from host CPU offloading while deploying a NIST FIPS-compliant post-quantum HRoT.

By virtue of its modular design philosophy and unshakeable HRoT, PUF-PQC stands not merely as a tool to address current engineering challenges, but as a blueprint for leading the industry in establishing a sustainable and scalable trust architecture in the quantum computing era.

eMemory & PUFsecurity IP Solutions

PUFsecurity Corp., a subsidiary of eMemory Technology Inc., is a leading provider of hardware root-of-trust technologies, specializing in security IP solutions based on Physically Unclonable Function (PUF) technology. Leveraging eMemory's NeoPUF and NeoFuse OTP technologies, PUFsecurity focuses on developing and deploying native key generation and full-stack security architectures to address the challenges of the quantum era.

Core IP solutions for security

- **PUF$_{\text{PQC}}$** (Post-Quantum Cryptography)
- **PUFcc** (Crypto Coprocessor)
- **PUFrt** (Root of Trust)
- **PUFhsm** (Hardware Security Module)

PUFsecurity is currently constructing a PUF-based Security-as-a-Service ecosystem to provide protection and authentication for the next generation of connected devices.

For more information on the complete product portfolio of eMemory and PUFsecurity IP solutions, please visit, **https://www.ememory.com.tw/en-US/Products/Security/Overview**