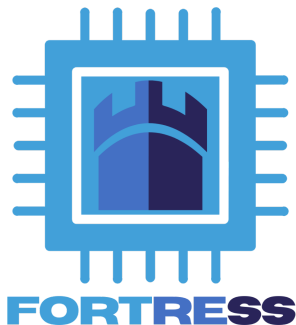




FORTRESS NEWSLETTER #3

FORTRESS aims to develop a scalable and efficient hybrid secure boot architecture.



FULLY OPTIMISED ROOT OF TRUST FOR ROBUST EMBEDDED SECURITY SYSTEMS

FORTRESS project focuses on hardware-software co-design principles, enabling diverse platforms – embedded systems, edge devices, and Critical National Infrastructure – to transition to quantum-resistant architectures seamlessly. Additionally, the project will engage industry stakeholders to align with regulatory and standardisation efforts, ensuring practical deployment and maximum impact.

Secure Boot and the challenges of Post-Quantum Cryptography

In today's digital systems, secure boot is a fundamental cornerstone of security architecture. By leveraging a dedicated subsystem, the Root of Trust (RoT), a trust chain is established in which each software component, starting from the boot ROM, verifies the authenticity and integrity of the next stage. This trust is anchored in a verification key securely stored within the RoT. To serve as a system's trust anchor, a RoT must fulfill three fundamental properties: it must be constrained, fixed, and trustworthy. Each property presents a distinct challenge during the transition to Post-Quantum Cryptography (PQC).

First Property: Constrained. A RoT is isolated from other system elements, accessible only via a restricted API, and should be limited in resource consumption. For the transition to PQC, implementations must remain compact and hardware-efficient while maintaining execution performance. Here, different PQC signing algorithms offer different trade-offs. For secure boot, LMS (Leighton-Micali Signatures) is an ideal candidate because it offloads complex computations to an offline signing infrastructure that operates sporadically. A broader solution is

hardware/software co-design, which considers the entire execution stack simultaneously to enable dedicated performance tweaks.

Second Property: Fixed. A RoT is intentionally immutable to resist attacks. However, long deployment lifecycles require systems to adapt to evolving threats, e.g. the potential advent of cryptographic-relevant quantum computers. To address this, European agencies (such as BSI and ANSSI) mandate post-quantum/traditional hybrid cryptography, where firmware images are signed with both post-quantum and traditional signature schemes and accepted only if both are valid. Long-term adaptability also relies on crypto-agility, allowing algorithms to be swapped post-deployment through architectural software separation and/or hardware redundancy.

Third Property: Trustworthy. A RoT must thwart powerful attacks while remaining simple enough for comprehensive security analysis. PQC transition demands implementing new algorithms alongside convincing security assurances. The attack surface spans two main areas: First, algorithmic vulnerabilities, where NIST standardization provides high confidence. Second, implementation-specific vulnerabilities (such as fault-injection attacks), which still require dedicated work to achieve the same level of assurance. Furthermore, hardware/software co-design and crypto-agility add system complexity, inherently complicating security analysis.

Project FORTRESS sets out to solve all three challenges. We explore dedicated hardware/software co-design for efficiency, deploy post-quantum/traditional hybrid signatures for long-term security, focus on implementations with physical attacks in mind, and perform extensive security analyses to ensure trustworthiness.

The RoT Has Set In | FORTRESS Expert Review #1

Introduction Welcome to the first edition of the FORTRESS Expert Review series, where, we delve into the world of embedded post-quantum cryptography to provide you with detailed analyses on the matter. Hash functions play an important role in making many Post-Quantum Cryptography (PQC) schemes secure and efficient enough. In particular, the NIST-standardized ML-KEM (FIPS 203) and ML-DSA (FIPS 204) post-quantum cryptographic ...

[Read more](#)

FORTRESS takes the center stage at the CODE-Jahrestagung 2026: From Post-Quantum Research to

Real-World Deployment

FORTRESS participated in CODE-Jahrestagung 2026, held on 14 and 15 July 2026 at the University of the Bundeswehr Munich. Under the theme "Cryptography as a Strategic Key to Digital Defence," this two-day event brought together representatives from research, industry, public authorities, and the cybersecurity community. The programme featured expert presentations, keynotes, panel discussions, interactive workshops, and a specialist exhibition covering ...

[Read more](#)



FORTRESS Explained #5

FORTRESS Explained #5: What is ML-DSA, and why is it the new standard for digital signatures? ML-DSA, the Module-Lattice-Based Digital Signature Algorithm, is stepping up to become the new global standard for digital signatures. Standardized by NIST as FIPS 204 in August 2024, it is a mathematical tool used to create digital signatures, which prove that a file, message, or ...

[Read more](#)



FORTRESS Paper accepted at CHES 2026

"SHARMONY: Composing SHA-2 and SHA-3 Hardware for Crypto-Agile PQC", by Liga Anwar, Carlos Andres Lara-Nino, Jong-Yeon Park and Michael Hutter (Universität der Bundeswehr

München), has been accepted to IACR Transactions on Cryptographic Hardware and Embedded Systems and will be presented at CHES 2026 in Antalya, Türkiye, on 11–15 October.

The post-quantum standards are split across two hash families: ML-KEM and ML-DSA build on SHA-3 and SHAKE, while the hash-based signatures LMS and SLH-DSA are each specified with both SHA-2 and SHAKE parameter sets. A Root of Trust that is to stay crypto-agile needs both, and building them separately means paying for two engines. SHARMONY combines them into one, so that a single accelerator serves either family while taking up considerably less room than two separate designs would. For a Root of Trust that must stay constrained, that turns crypto-agility from an expensive option into an affordable one.

Third Plenary meeting



On 17–18 June 2026, the consortium gathered in Bordeaux for its third plenary meeting, kindly hosted by eShard. The meeting kicked off with updates from project coordinator Uwe Herzog (Eurescom) and a technical progress by Dr. Axel Y. Poschmann (PQShield). In addition, day 1 covered updates by Work Package 1, under the leadership of Universität der Bundeswehr München, which handles the RoT through benchmarking and trade-off analyses, and Work Package 2, led by PQShield, developing hybrid RoT architectures that keep the intentionally fixed trust anchor adaptable. A guided visit to eShard's laboratories gave first-hand insights into hardware security evaluation and side-channel analysis.

Day two turned to Work Packages 3 and 4, covering integration, validation, and the test evidence on which trustworthiness ultimately rests, alongside dissemination and stakeholder engagement in Work Package 5, led by Pooja Mohnani (Eurescom).

Our thanks to all partners, and to eShard for the organisation and hospitality.

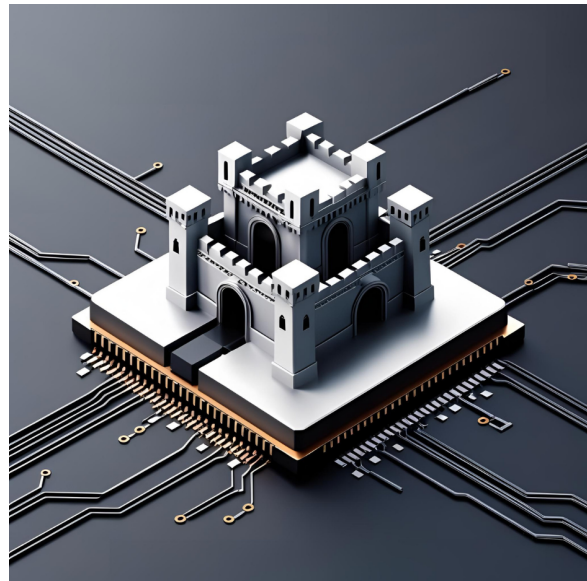
For more information: <https://pq-fortress.eu/2026/06/22/fortress-consortium-advances-post-quantum-security-at-bordeaux-plenary-meeting/>



Ambition and Impact

FORTRESS advances the **state of the art** by combining **post-quantum cryptography** with **hardware-enforced security** to deliver trusted systems that remain secure in the quantum era. The project contributes to **EU leadership in PQC standardisation**, ensures the **resilience of critical infrastructures**, and enables a **secure digital transition** for industries and public services across Europe.

[Read more](#)



FORTRESS has received funding from the EU Horizon Europe research and innovation programme under grant agreement 101225722. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

About your data

This mail is generated from registered subscribers who are interested to keep themselves updated about the project activities and sent by MailPoet under the General Data Protection Regulation of the EU, learn more about our [DPD](#).

[View this in your browser.](#)

Contact at: info@pq-fortress.eu



[Unsubscribe](#) | [Manage your subscription](#)

FORTRESS Newsletter powered by MailPoet.