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.

The Second Plenary Meeting in Munich

The FORTRESS consortium gathered on 11–12 February for its second face-to-face plenary meeting, hosted by the Research Institute CODE at the Universität der Bundeswehr München. Bringing partners together in person created a valuable environment for in-depth technical discussions, strategic alignment, and coordinated planning. It was encouraging to see the steady progress achieved across all work packages, along with productive exchanges on the project's architectural direction and practical implementation challenges. These sessions further strengthened the connection between research, experimentation, and real-world deployment.

Alongside these efforts, we are also preparing an introductory project video featuring insights from our consortium partners, offering a clear and accessible overview of FORTRESS's goals and expected impact. Building on the momentum of this meeting, the consortium is committed to maintaining regular face-to-face interactions to foster closer collaboration and drive even more tangible results. We look forward to sharing further updates as the project continues to evolve.

For more information: https://pq-fortress.eu/2026/02/13/strong-momentum-at-our-second-plenary-meeting-in-munich/

Comcast's Cybersecurity Research Colloquium

Axel Poschmann (PQShield) recently delivered a talk at Comcast's Cybersecurity Research Colloquium as part of the Comcast PQC Center of Excellence Monthly Research Presentation, titled "PQ/T Hybrid Secure Boot: Why You Need a Fortress to Achieve It" on February 27, 2026. The presentation highlighted the growing complexity of secure boot in the post-quantum era, where traditional cryptographic schemes such as RSA and ECC are no longer sufficient. Key challenges were discussed across the secure boot lifecycle, including the lack of a one-size-fits-all approach for PQ/T hybrid signature verification due to evolving regulatory requirements, as well as practical difficulties in signature generation, such as key management and the absence of fully mature end-to-end quantum-safe solutions.

The talk introduced the FORTRESS project (Fully Optimized Root of Trust for Robust Embedded Secure Systems) as a strategic response to these challenges. FORTRESS aims to develop a scalable, efficient hybrid secure boot architecture based on a flexible Root of Trust that integrates both traditional and post-quantum algorithms. By leveraging hardware-software co-design and carefully balancing security, performance, and cost, the project seeks to enable seamless adoption of quantum-resistant secure boot across embedded systems, edge devices, and critical infrastructure. The presentation outlined FORTRESS's research direction and emphasized its role in bridging current gaps toward practical and deployable PQ/T hybrid secure boot solutions.

For more information: https://pq-fortress.eu/2026/02/27/fortress-takes-the-stage-at-comcasts-cybersecurity-research-colloquium/

From Pitfalls to Progress: ML-DSA

Benchmarking Accepted at MAgiCS

The FORTRESS project continues to advance the state of the art in post-quantum secure systems with new research on ML-DSA benchmarking. The paper “Apples, Oranges, and Signatures: Pitfalls and Methodology in ML-DSA Benchmarking” by Sebastien Riou, Jong-Yeon Park, Liga Anwar, Axel Poschmann, and Michael Hutter has been accepted for presentation at the MAgiCS workshop (co-located with IACR Eurocrypt 2026) in …

Apples, Oranges, and Signatures
Pitfalls and Methodology in ML-DSA Benchmarking

Sebastien Riou[1], Jong-Yeon Park[2], Liga Anwar[2], Axel Poschmann[1], and Michael Hutter[1,2]

[1] PQShield Inc.,
Prama House, 267 Banbury Rd, Oxford, UK
{sebastien.riou,axel.poschmann}@pqshield.com
[2] University of the Bundeswehr Munich,
Werner-Heisenberg-Weg 39, 85579 Neubiberg, Germany
{jongyoun.park,liga.anwar,michael.hutter}@unibw.de

Abstract. Cryptographic migration, particularly in the post-quantum setting, poses significant practical challenges and requires reliable performance data to support sound engineering decisions. For ML-DSA, however, existing benchmarking practices often produce misleading or non-comparable results, complicating migration and cryptographic agility efforts. This paper analyzes common pitfalls in benchmarking ML-DSA signature operations, including subtle inconsistencies when comparing security levels. We show that execution-time variability of the ML-DSA signing algorithm—an inherent property due to rejection sampling and

Read more

Consortium Partners

Eurescom ensures strong project coordination and effective execution across all activities including dissemination & communication, while PQShield contributes world-leading post-quantum cryptography expertise and direct involvement in shaping NIST PQC standards. CyberHive strengthens the project with high-performance, industry-ready cybersecurity technologies, and Codasip brings deep hardware-software co-design capabilities as Europe’s leading RISC-V provider. eShard adds essential chip-level security testing and vulnerability analysis through its advanced evaluation platforms, and Universität der Bundeswehr München provides rigorous academic research and critical infrastructure expertise.

EURESCOM
Innovation through Collaboration

PQ SHIELD

cyberhive

Codasip

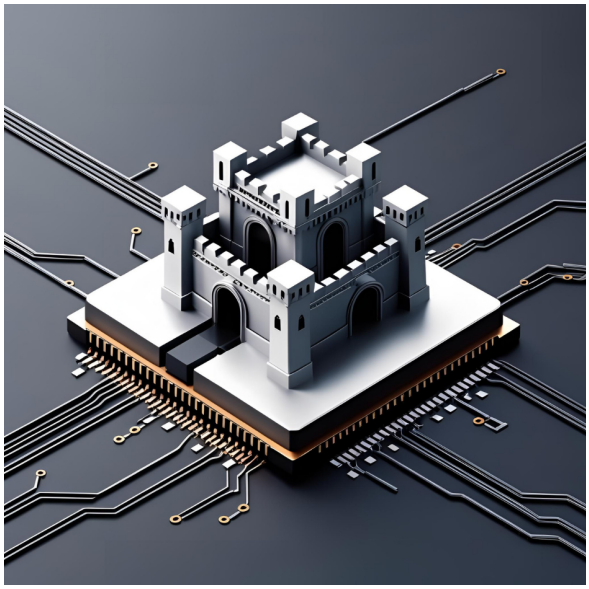
eShard

der Bundeswehr
Universität München

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