PQC4eMRTD

**Post-Quantum Cryptography for electronic Machine-Readable Travel Documents**

# Post Quantum Cryptography for RISC-V Space Systems

Dr. Leonidas Kosmidis

12/06/2026

Advancing RISC-V Adoption in HPC and Cloud Environments Workshop

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

# Outline

- The need for Post Quantum Cryptography
- PQC4eMRTD project
- Cryptography in the Computing Continuum
- PQC in Existing and upcoming space systems
- Conclusion

# Introduction

- Conventional cryptographic algorithms are vulnerable to quantum computing attacks
- A 2048-bit RSA key can be broken in 177 days using 13.500 physical qubits [1]
- This is much less than previous estimates which was 8 hours using 20 million qubits
- Migration to Post Quantum Cryptographic algorithms is required

[1] E. Gouzien and N. Sangouard, “Factoring 2048-bit RSA Integers in 177 Days with 13 436 qubits and a Multimode Memory,” Phys. Rev. Lett., vol. 127, p. 140503, Sep 2021

# Introduction

- Quantum Computing Technology advances fast
- IBM Quantum announced a 433-qubit chip in 2022 [1] and estimated devices with 4000-qubits to be available by 2025 [2]
- Migration to Post Quantum Cryptography is required and needs to be implemented within a few years, before it is late
- Government initiatives are underway in many countries
- Quantum resilience is a European Commission priority

[1] IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two, https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[2] "IBM Unveils New Roadmap to Practical Quantum Computing Era; Plans to Deliver 4,000+ Qubit System, https://newsroom.ibm.com/2022-05-10-IBM-Unveils-New-Roadmapto-Practical-Quantum-Computing-Era-Plans-to-Deliver-4,000-Qubit-System

# The PQC4eMRTD project

- Post Quantum Cryptography for electronic Machine Readable Travel Documents
- Coordination and Support Action (CSA) project funded by the European Commission
- January 2025 - December 2026
- Monitor the standardization landscape in eMRTDs and PQC, as well as in other domains with similar requirements such as aerospace and participate in standardization
  - RISC-V PQC TG, HAC (High Assurance Crypto) TG, Crypto TG etc.
  - Ensure that the adopted solutions are appropriate also for resource constrained systems
- Prepare the migration of European eMRTDs to PQC

# Where is cryptography used in the Computing Continuum?

PQC4eMRTD

- Everywhere!
- Cryptography is ubiquitous:
  - authentication, encryption, handshake (TLS/SSL)
- It used in many different functionalities
  - Networking, storage, software updates
- Across different devices in the continuum
  - Personal computers, Cloud servers, edge devices and IoT
  - All can be addressed with a single, free instruction set

RISC-V®

# How about Space Systems?

- Cybersecurity is an increasing concern in space systems
- A recent study found that 50% of GEO satellite traffic is unencrypted [1]
- Possible threats:
  - Eavesdropping of sensitive information
  - Unauthorised access to space or ground stations
  - Manipulation of telecommands
  - Malicious software updates
- Certain classes of space systems have higher risk:
  - Sensitive observation data and critical infrastructure such as global positioning and telecommunications

[1] Zhang et al, Don't Look Up: There Are Sensitive Internal Links in the Clear on GEO Satellites, ACM SIGSAC Conference on Computer and Communications Security, 2025, https://dl.acm.org/doi/10.1145/3719027.3765198

# Functionalities that rely on Cryptography

- Authentication:
  - Users: affects their access to the system
  - Administrator: affects the integrity and availability of the entire system

- Networking:
  - Secure communications
  - Encrypt transmitted data
  - TLS/SSL

- Storage:
  - Data encryption

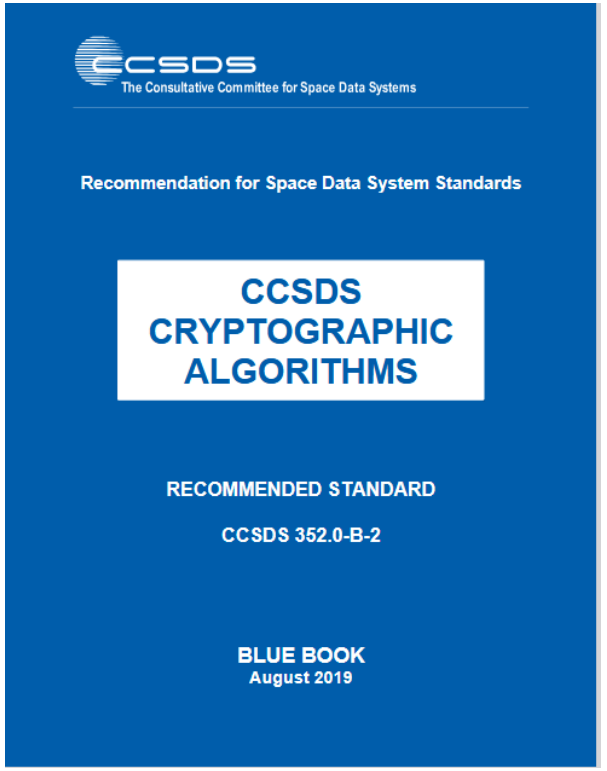
# Functionalities that rely on Cryptography

- Secure Boot:
  - Ensure that the bootloader and operating system are not modified
  - Secure software updates

- Multi-tenancy
  - Multiple Users share the hardware
  - Memory isolation is not enough
  - Memory encryption
  - Not even the hypervisor is able to see the memory contents

# Encryption in existing space systems

- The Consultative Committee for Space Data Systems (CCSDS) has long ago acknowledged the importance of cybersecurity and recommends the use of cryptographic algorithms for **all** space systems communications
  - Both Telecommands and downlink communications need to be encrypted
- Currently CCSDS adopts conventional cryptographic algorithms
  - AES: 128-bit, 192-bit, 256-bit
  - RSA: 2048-bit, 4096-bit

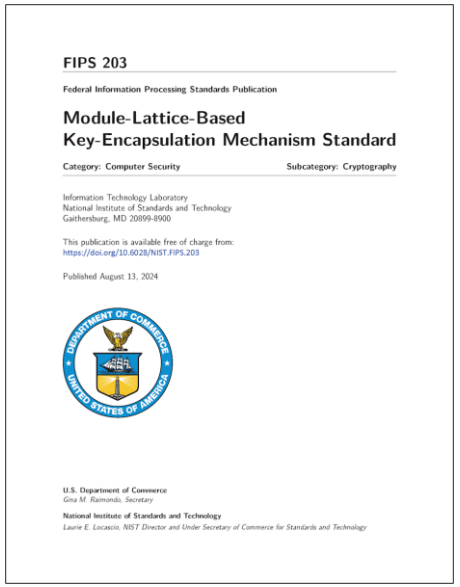


# Encryption in existing space systems

- Cryptographic accelerators for conventional algorithms are already included in several COTS processors used in space:
  - ARM, x86
- RSA is vulnerable to quantum computing attacks
- Space systems lifetimes can be very long
  - >10 or 20 years
  - We need to engineer space systems to remain secure until the end of their operational timeline

# Encryption in upcoming space systems

- In 2024 NIST has approved a series of Post Quantum Resilient cryptographic algorithms based on different types of mathematical operations such as Algebraic Lattices


FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

**FIPS 203**
Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

**FIPS 204**
Module-Lattice-Based Digital Signature Standard (ML-DSA)

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

**FIPS 205**
Stateless Hash-Based Digital Signature Standard (SLH-DSA)

# Encryption in upcoming space systems

PQC4eMRTD

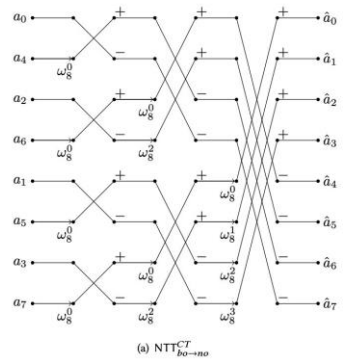
- PQC algorithms use larger key sizes than conventional cryptographic algorithms
- Deployed systems or systems under development with existing space processors can use software implementations of PQC algorithms
- Reference software implementations exist
- We have successfully ported them on FrontGrade Gaisler’s GR740 (LEON4) as well as LEON3 and NOEL-V
- We have added PQC support in NASA's CryptoLib

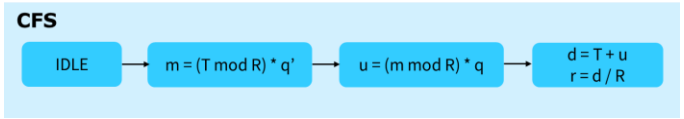
# Encryption in upcoming space systems

- Due to hardware complexity PQC algorithms can benefit from hardware acceleration
- Already considered in upcoming RISC-V based space processors
- Microchip's HPSC includes a vector unit
  - Vector instructions can be used to accelerate PQC algorithms
  - Long vector registers can be used to store the long keys
  - Reference PQC implementations using RISC-V vector intrinsics
- Frontgrade Gaisler's GR765 includes a PQC hardware crypto accelerator for secure boot
  - SIMD feature similar to the SPARROW accelerator can also be used to accelerate PQC algorithms

# Encryption in upcoming space systems

- We are exploring additional acceleration possibilities [1]:
  - Custom instructions to accelerate PQC algorithm building blocks such as the Number Theoretic Transform (NTT)
  - Study trade-offs and implications of integrating different parts of the algorithm in the processor's critical path
  - Experiment with different RISC-V processors:
    - BSC Sargantana
    - Chips Alliance VeeR
    - NeoRV32
  - Custom instruction for Montgomery Reduction in ML-KEM decapsulation (decryption) in NeoRV:
    - 20% of decryption execution time
    - 10x speedup considering frequency reduction in non pipelined implementation
    - 31% speedup in the full application






| | Freq(MHz) | # cycles | Exec time (µs) | Speedup |
|---|---|---|---|---|
| **CPU** | 109.35 | 720 | **6.59** | |
| **Combinatorial** | 87.09 | 55 | **0.63** | **10.46x** |
| **Multi-stage** | 109.35 | 66 | **0.60** | **10.98x** |

[1] L. Kosmidis et al, RISC-V PQC Hardware Implementations for Safe and Secure Systems: A Design Exploration, RISC-V Summit North America 2025

# Post Quantum Security Standardisation within RISC-V

## Security Groups

- Memory Tagging – RVG-161 Task Group (TG):
- Runtime Integrity - RVG 60 Special Interest Group (SIG)
- Trusted Computing – RVG-74 (SIG)
- SmMTT (Supervisor Domain Isolation) – RVG-65 (TG)
- Application-Processor Trusted Execution Environment (CoVE) – RVG-76 (TG)
- I/O Physical Memory Protection Unit (IOPMP) – RVG-56 (TG)
- Security Model - RVG-79 (TG)
- Security Response Team – RVG-73 (SIG)
- CHERI – RVG-70 (SIG)
- Control Flow Integrity – RVG-71 (SIG)
- Application-Processor Trusted Execution Environment I/O (CoVE-IO) – RV-144 (TG)
- Microarchitecture Side Channels – RVG-72 (SIG)
- World Guard RVS-2940 (Specification Task Group)
- External Debug Security – RVG-136 (TG)
- Timing Fences – RVG-83 (TG)
- S-mode Physical Memory Protection (SPMP) – RVG-100 (TG)
- Crypto GOST-R – RVG-81 (TG)
- Post-Quantum Cryptography (PQC) - RVG-84 (TG)
- High Assurance Cryptography (HAC) -RVG-145 (TG)
- Cryptographic Extensions – RVG-82 (TG)

© 2025 Consortium Confidential

# Other Related RISC-V WG/TG/SIG

## Groups

- Automotive
- Functional Safety
- Space SIG
- RVM Microcontroller specification (RVM26)
  elected Vice Chair

© 2025 Consortium Confidential

# Additional Work on Standardisation

## Space

- ELISA – Enable Linux in Safety Critical Systems

- Aero and Space WGs

© 2025 Consortium Confidential

# Additional Work on Standardisation

## Safety Critical Systems

- Khronos

- SYCL SC WG
  - High level programming model for GPUs
  - WG Co-Chair and Outreach Officer

- Member of the OpenGL SC, Vulkan SC, OpenCL and Safety Critical Advisory Forum

- Consideration of PQC acceleration in GPUs

© 2025 Consortium Confidential

# Additional Work on Standardisation

## Space

- ADHA Standardisation Group
  - Standard interface for the interconnection of space processing elements
  - Includes networking, storage etc
  - Ensure that PQC is included

- Auto-coding of Hardware Design Languages for Space FPGAs
  - Evaluation of PQC algorithms with high level synthesis

© 2025 Consortium Confidential

# Conclusion

- Cybersecurity is very important in upcoming space systems
- Post Quantum Cryptography Migration is required
- PQC algorithms can be implemented in software on existing space processors
- Upcoming space processors will have hardware acceleration for PQC
- Significant work on standardisation is under way
- Will benefit several different domains

© 2025 Consortium Confidential

# PQC4eMRTD

**https://pqc4emrtd-project.eu/**

https://www.linkedin.com/company/pqc4emrtd-project

https://x.com/pqc4emrtd

This project has received funding from the European Union's DIGITAL research and innovation programme under Grant Project number 101190400.