RISC-V Solutions for Post Quantum Computing for Machine Readable Travel Documents

Leonidas Kosmidis[1,2] Matina Maria Trompouki[1] Eric Rufart[1]
Jannis Wolf[1] Guillermo Vidal[2,1] Marc Solé[2,1]

[1]Barcelona Supercomputing Center (BSC)
[2] Universitat Politècnica de Catalunya (UPC)

Abstract

The PQC4eMRTD (Post-Quantum Cryptography for electronic Machine-Readable Travel Documents) European Project has started in January 2025. The purpose of this Coordination and Support Action (CSA) project is to monitor and influence Post Quantum Computing solutions related to the security of identity documents with biometric data. RISC-V is the perfect candidate for the exploration of these solutions, therefore in addition to the standardisation involvement, we are working towards various implementations related to this domain.

Introduction

Nowadays, government issued digital identity cards, driver licenses and travel documents such as passports include secure microprocessor technologies which are used to retrieve highly sensitive personal information such as biometrics.

With the technology evolution of quantum computers, the long term security of this information stored and protected with traditional security methods is at risk, especially considering the long validity period of such documents.

For this reason, there is a global effort for the development of Post Quantum Computing and Quantum Resistant security solutions.

In fact, in 2017, the US National Institute of Standards and Technology (NIST) started its post-quantum cryptography project and asked for submissions of post-quantum key exchange, public-key encryption, and signature schemes to a competition-like standardization effort. In 2022, the first algorithms chosen for standardization were announced, with finalized written standards published in 2024.

At this important time, Europe has a unique opportunity to influence upcoming standardisation efforts and lead the development of secure solutions for the post-quantum era.

RISC-V offers a unique opportunity to experiment with different implementations of these solutions, so that efficient hardware implementations are devised. Moreover, the identification of common programming patterns and operations used in post quantum cryptography allows the extension of the ISA with new extensions that over significant acceleration.

For this reason, the PQC4eMRTD project, coordinated by Infineon, is performing the following tasks:

- Monitoring PQC and travel document standardisation activities. This includes identifying relevant working groups and study the work that has been performed so far. RISC-V with its High Assurance Cryptography (HAC) and Post-Quantum Cryptography (PQC) Task Groups have been identified and project members will participate in them, studying the work performed so far.
- Active Participation in the identified PQC and travel document standardisation activities. The project members will join and actively participate in the aforementioned RISC-V TGs, contributing in the discussions and bringing practical feedback from their own experimentation with PQC algorithms and their acceleration.
- Increase awareness and promote the wide spread use of the upcoming PQC solutions. This abstract and presentation opportunity either in a talk or a poster form at the RISC-V Summit Europe 2025 is part of this effort, allowing to reach the European RISC-V community and facilitate adoption.

Project Status and Information

The project is coordinated by Infineon, and the consortium consists of Barcelona Supercomputing Center (BSC), Thales, University of Ljubljana and CryptoNext and has a duration of 2 years.

The project is currently at its very early stages, with the kick-off taking place in January and identifying the working groups of interest.

The project partners are in the process of joining the identified working groups and task groups, and started analysing the performed work so far.

In parallel, BSC investigates the implementation of several PQC algorithms on RISC-V architectures, and more importantly the ones developed in-house, such as in the Sargantana RISC-V core. In addition, the implementation of PQC accelerators for the candidate algorithms submitted to the NIST post-quantum cryptography project such as Dilithium is on-going, as well as their integration with BSC developed RISC-V Systems on Chip. Special attention is paid in low area and low power consumption, given that the processors included in IDs and passports are extremely resource limited.

This work is not only focused on hardware but on softwar implementations, too. For example, the use of formally proven implementations on top of Ada SPARK, which is supported in the RISC-V cores used in BSC's research platforms.

Given that the RISC-V Summit takes place several months from now when substantial work will have been performed, the final version of the abstract as well as the presentation material (slides/poster) will include the most up-to-date status of the project.

Acknowledgments

The work presented in this paper has received funding from the European Union's DIGITAL research and innovation programme under Grant Project No 101190400 (PQC4eMRTD).