PQC4eMRTD: Post-Quantum Cryptography for electronic Machine-Readable Travel Documents

Description

Quantum computing is ante portas . Research in the field of quantum computers is very active and many countries and privatecompanies are investing millions. IBM Quantum announced a 433-qubit processor on November 9th, 2022 and they anticipate devices with more than 4000 qubits to be available by the year 2025. Meanwhile, research activities also demonstrate that less and less qubits are needed to break classical asymmetric cryptography. The European digital security industry represented by Eurosmart on the other hand also highlights the importance to start transitioning towards quantum-resistant (QR) infrastructure as of today.

In the particular case of electronic machine-readable traveldocuments (eMRTDs), Eurosmart has thoroughly analysed all the security risks stemming from the advent of quantum computers, and all the challenges that should be solved to entirely transition to a QR infrastructure: (1) redesigning privacy oriented cryptographic protocols, (2) designing PKIs based on QR cryptography, (3) updating the standards which are instrumental to reach international interoperability, (4) deploying the new infrastructure (electronic passport, PKI,&), and (5) waiting for the renewal of the former generation of electronic passports on the field only supporting classical cryptography (the typical lifetime of an electronicpassport is ten years).

This analysis shows that the transition towards QR infrastructure for electronic passports will take time. Therefore, the security of electronic passports is particularly at risk. Thus, clear measures shall be taken as of now. The vision of the PQC4eMRTD project is to join forces with world leading European players in the field of security, as well as PQCexperts from academia to push previous PQC research results towards the international standardization working groups in order to unlock the implementation of QR protocols, mainly in the fields of digital identities and eMRTDs.

Barcelona Supercomputing Center - Centro Nacional de Supercomputación