# An algorithmic optimization for HQC on the ARM m4 MCU

Ridwane Aissaoui*[1], Jean-Christophe Deneuville[2], Alain Pirovano[2], and Christophe Guerber[3]

[1]Fédération ENAC ISAE-SUPAERO ONERA - Equipe télécommunications – Ecole Nationale de l'Aviation Civile – France

[2]Fédération ENAC ISAE-SUPAERO ONERA - Equipe télécommunications – Ecole Nationale de l'Aviation Civile – France

[3]Direction de la technique et de l'innovation de la DGAC – Direction Générale de l'Aviation Civile – France

**Résumé**

This article presents a work in progress that aims to improve the performance of the code-based HQC post-quantumKey Encapsulation Mechanism (KEM) algorithm. Many con-strained systems with limited computational and memory resources, such as Internet of Things (IoT) devices, small Unmanned Aerial Vehicles (UAVs), or medical devices, struggle to use cryptographic algorithms efficiently. They still need to be provided with information security, and the wireless nature of the communications with these systems means that this security has to rely on cryptography. In particular, an end-to-end encryption scheme can provide confidentiality and authentication. KEMs are vital in this process. Several propositions for quantum-resistant KEMs have been chosen by the National Institute of Standards and Technology (NIST) for standardization. One of these schemes, Hamming Quasi-Cyclic (HQC), has not yet been provided with an optimized implementation for constrained devices. This article details the work in progress for the algorithmic optimization of HQC, using properties in the costly polynomial operations to reduce computational load and memory usage during the process. Anticipated results are an improvement in computational complexity, going from O(nˆlog2(3))to O(n). We also expect an improvement in memory usage during the process, reducing the memory consumption.

*Intervenant