Post-quantum key agreement for small devices

Benjamin Smith, Inria/LIX

15/09/2025

An IPP Cybersecurity M2 research project proposal

Contact

Benjamin Smith (smith@lix.polytechnique.fr)

Context

The anticipated rise of quantum computing will, at some point, render most currently-deployed public-key cryptography (in particular, elliptic-curve cryptography and RSA) insecure, with disastrous consequences for communications security. Over the last decade, cryptographers have been working on the design and analysis of *post-quantum* cryptosystems, which are designed to resist future adversaries equipped with powerful conventional *and* quantum computers. The first wave of international standards has just appeared, and the next challenge is putting these new cryptosystems into practice.

HQC [1] is a post-quantum key agreement scheme (a *Key Encapsulation Mechanism*, or KEM) whose security is based on supposedly hard computational problems from the theory of error-correcting codes. In March 2025, HQC was selected by NIST (the US national technical standards agency) as a future standard for post-quantum KEMs [2], as an alternative to the lattice-based ML-KEM (defined in FIPS 203) [3]. While ML-KEM has been the subject of much analysis in recent years, HQC has seen alarmingly little work on implementation techniques (or on its security!).

Objectives

The first goal of this project is to provide a clean and portable software implementation of HQC, starting from its specification [4], with a view to finding practical improvements, and identifying (and fixing) points of vulnerability to side-channel analysis.

The second goal of this project is to study the performance of HQC in constrained devices, using RIOT OS [5] (or its Rust-based successor Ariel OS [6]) as a platform

for development and experimentation on a range of low-end IoT devices. RIOT supports literally hundreds of different platforms, so this will give us a good idea (and probably some hard lessons) on the extent to which the new standard is actually deployable in low-end environments. In any case, adapting the algorithms of HQC to 32-bit architectures with hard constraints on RAM will be a very interesting challenge.

References

Contact Benjamin Smith (smith@lix.polytechnique.fr) for discussion and further references.

- [1] HQC https://pqc-hqc.org/
- [2] HQC standardization announcement: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption
- [3] HQC specification: https://pqc-hqc.org/doc/hqc_specifications_2025_08_22.pdf
- [4] FIPS 203 (ML-KEM standard specification): https://csrc.nist.gov/pubs/fips/203/final
- [5] RIOT OS: https://www.riot-os.org/
- [6] Ariel OS: https://github.com/ariel-os/ariel-os