Post-Quantum Cryptography

Benchmarking for a Quantum Secure Future

Graduate

Lukas Kellenberger

Introduction: Quantum computing has emerged as a rapidly advancing field, driven by substantial global investment and research. Some estimates suggest that powerful quantum computers could be produced as early as the early 2030s. While this technological breakthrough promises significant advancements, it also introduces serious security challenges due to its ability to compromise widely used encryption standards. In response, the National Institute of Standards and Technology launched the Post-Quantum Cryptography project in 2016, aiming to standardize cryptographic algorithms that remain secure against quantum computers. After multiple evaluation rounds, new standards have been published for key exchange and digital signature schemes. This paper presents a technical analysis of these emerging standards and offers a benchmarking framework for evaluating their performance. The goal is to provide support for a smooth and secure transition to a quantum-resistant world.

Approach: The objective of this paper is to highlight the practical use of the newly published post-quantum algorithms, with a focus on their real-world applicability. The study begins with an evaluation of recent developments in quantum computing and an analysis of the technical foundations of the selected post-quantum standards. This is followed by the design and implementation of a benchmarking framework to support the planning and transition to secure post-quantum cryptographic solutions. The different standards are compared, and based on the results, key insights, actionable recommendations, and necessary adaptations are derived to guide the transition.

Result: The results from the benchmark demonstrate that National Institute of Standards and Technology's quantum-secure standardized key exchange algorithms exhibit robust performance and, depending on the key size, can be competitive with traditional algorithms. For hybrid algorithms, a decrease in performance is to be expected; however, this decline remains within acceptable limits for typical use cases. In the context of digital signature algorithms, the performance implications are more pronounced due to the substantially larger signature sizes involved. The findings indicate that post-quantum cryptographic algorithms offer a viable path toward a quantum-secure future. Nevertheless, each system requires a well-considered and thoroughly prepared migration strategy.

Advisor
Dr. Daniel Tschudi

Co-Examiner
Dr. Alexandru Caracas, Rüti ZH, ZH

Subject Area
Computer Science