CC-06-01

Post-quantum cryptography (PQC) today, tomorrow, and challenges

Atsushi Yamada

ISARA Corporation

Abstract

In August 2024, the (US) National Institute of Standards and Technology (NIST) standardized several post-quantum cryptography (PQC) algorithms. Although these specifications are greatly important, PQC standardization is still far from over. NIST is now developing a standard for the post-quantum signature algorithm FN-DSA (based on the FALCON algorithm), and has also began an "onramp" process to identify and standardize additional signature algorithms. And these are just the basic building blocks. The systems and protocols which will eventually utilize these algorithms need standards as well. For example, the standards for protocols such as TLS, SSH and IKEv2 will need to be updated before they can consume the PQC algorithms.

This talk will cover the status of post-quantum standards and their implementations. We will also review guidelines to migrate cybersecurity infrastructures to PQC. We will discuss the path to PQC, some potential challenges along the way, and of how cryptography inventories are critical to successful migrations. Finally, we will highlight additional benefits of assessing your cryptography posture and conclude that cryptography posture management should be a cybersecurity best practice today.