The ship has sailed: the NIST Post-Quantum Cryptography ”competition”

Dustin Moody

Computer Security Division
National Institute of Standards and Technology

Abstract. In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms. In particular, quantum computers would completely break many public-key cryptosystems, including those standardized by NIST and other standards organizations.

Due to this concern, many researchers have begun to investigate post-quantum cryptography (also called quantum-resistant cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. A significant effort will be required to develop, standardize, and deploy new post-quantum algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs.

NIST has taken several steps in response to this potential threat. In 2015, NIST held a public workshop and later published NISTIR 8105, Report on Post-Quantum Cryptography, which shares NIST’s understanding of the status of quantum computing and post-quantum cryptography. NIST also decided to develop additional public-key cryptographic algorithms through a public standardization process, similar to the development processes for the hash function SHA-3 and the Advanced Encryption Standard (AES). To begin the process, NIST issued a detailed set of minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms, available at http://www.nist.gov/pqcrypto. The deadline for algorithms to be submitted was November 30, 2017.

In this talk, I will share the rationale on the major decisions NIST has made, such as excluding hybrid and (stateful) hash-based signature schemes. I will also talk about some open research questions and their potential impact on the standardization effort, in addition to some of the practical issues that arose while creating the API. Finally, I will give some preliminary information about the submitted algorithms, and discuss what we’ve learned during the first part of the standardization process.