WORKSHOP OVERVIEW: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

POST-QUANTUM CRYPTOGRAPHY

Background

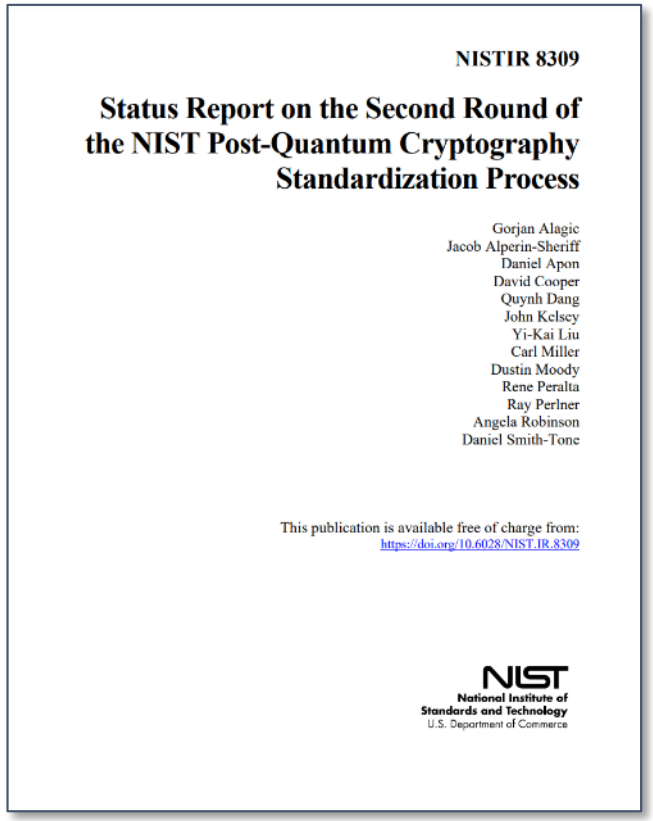
- Quantum computing running Shor's algorithm will render common public key algorithms ineffective

Problem

- Algorithm replacement can be extremely disruptive and often takes decades to complete

Status

- Algorithm selection is not expected before late 2021



NISTIR 8309

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Jacob Alperin-Sheriff
Daniel Apon
David Cooper
Quynh Dang
John Kelsey
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8309

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

REPLACEMENT PREREQUISITES

- Identify the presence of legacy algorithms
- Understand the formats and APIs of cryptographic libraries to support necessary changes/replacements
- Develop implementation validation tools
- Discover the hardware that implements or accelerates algorithm performance
- Determine OS or applications code that uses the algorithm
- Identify all communications devices with vulnerable protocols
- Update the processes/ procedures by developers, implementers, and users

SIGNIFICANT TECHNICAL CHALLENGE

The new algorithms will not likely be drop-in replacements

Differences in the following could affect performance and reliability:

- Key size
- Signature size
- Error handling properties
- Number of execution steps needed to perform the algorithm
- Key establishment process complexity

OPERATIONAL CONSIDERATIONS

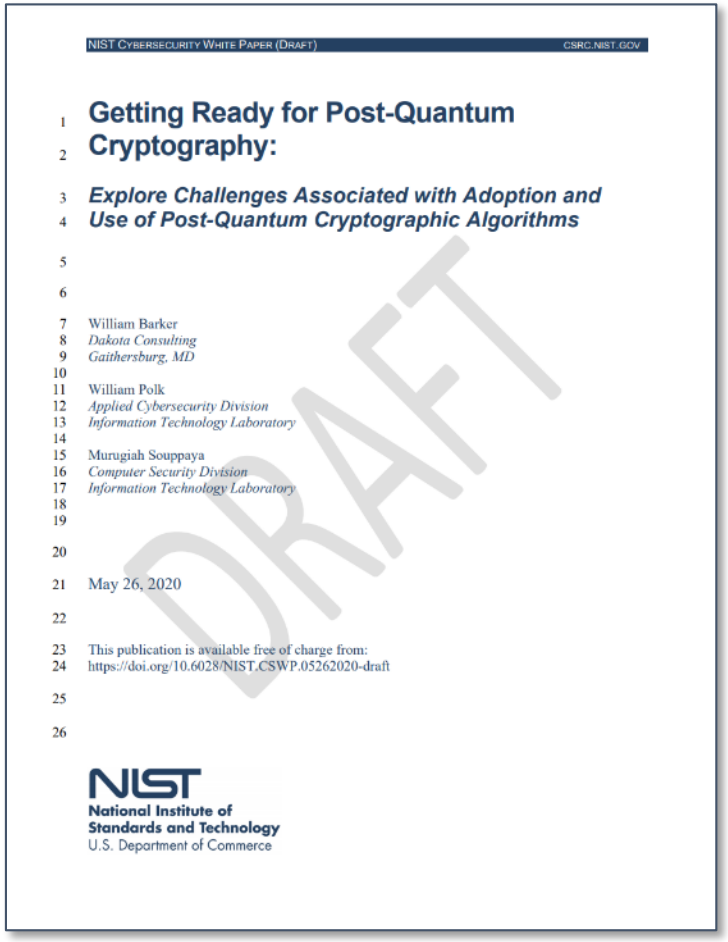
Accelerating adoption of replacement algorithms relies on:

- Developing a risk-based approach
- Establishing a communication plan
- Identifying a migration timeline and resources
- Updating or replacing security standards and procedures
- Providing installation, configuration, and administration documentation
- Testing and validating the new processes and procedures

NCCOE SUPPORT

Initiate development of practices to ease migration

- White papers
- Playbooks
- Demonstrable implementations
- Virtual workshops (planned for October 7, 2020)



NIST CYBERSECURITY WHITE PAPER (DRAFT) CSRC.NIST.GOV

Getting Ready for Post-Quantum Cryptography:

Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms

William Barker
Dakota Consulting
Gaithersburg, MD

William Polk
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

May 26, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.05262020-draft

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT

WORKSHOP PURPOSE/OBJECTIVE

Purpose:

- Discuss the challenges and investigate the practical and implementable approaches to ease the migration from the current set of public key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks.

Objective:

- Provide an opportunity for participants provide feedback on all aspects of the planned activities to include: impacted protocols, relevant standards, guidelines, recommended practices, use cases and technologies to be considered, and sources of specifications and guidance. NIST will use the resulting prioritized list of activities to help accelerate the development of a playbook for migration to post-quantum cryptography.

Today's Agenda

11:00 – 11:10 EDT	NIST and NCCoE Overview
11:10 – 11:20 EDT	Workshop Overview & Background
11:25 – 11:45 EDT	Status of NIST PQC Activity
11:45 – 11:55 EDT	Moderated Q&A
11:55 – 12:00 EDT	Break
12:00 – 13:00 EDT	Challenges Session •Standard Developing Organizations •Integration Challenge •Customer Challenges •Government Perspective
13:00 – 13:10 EDT	Moderated Q & A
13:10 – 13:15 EDT	Break
13:15 – 14:25 EDT	Five Minute Participant Lightning Talk Session
14:25 – 14:35 EDT	Moderated Q & A
14:35 – 14:45 EDT	Next Steps/Wrap-up (NCCoE)

Wrap-up

CALL TO ACTION

Help us shape the NCCoE's crypto migration project planning and execution!

- Provide feedback post October 7 Workshop
- Share approaches and tools for discovering public key cryptography
- Share approaches and tools for discovering algorithm migration
- Read the white paper and provide recommendations regarding the various aspects of crypto migration
- Share list of prioritized activities NIST should consider