GAO
Science, Technology Assessment, and Analytics

SCIENCE & TECH SPOTLIGHT:

SECURING DATA FOR A POST-QUANTUM WORLD

Accessible Version

MARCH 2023

WHY THIS MATTERS

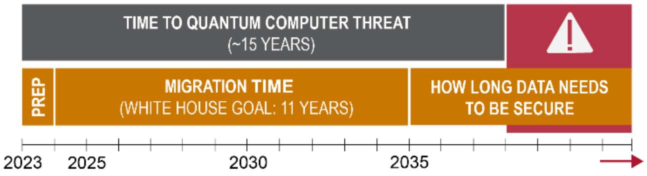
While the emergence of quantum computers offers potential benefits, these computers could undermine the security of current encryption methods that protect sensitive information. If encryption methods able to withstand the capabilities of quantum computing are not developed and deployed soon, secure data could be decrypted as soon as the 2030s.

/// THE TECHNOLOGY

What is it? Quantum computing poses risks to the security of sensitive data, which researchers are working to address. Governments, organizations, and individuals rely on cryptography to keep sensitive and personally identifiable information secure. Cryptography protects information by transforming it using mathematical functions, collectively referred to as encryption. Current, widely used encryption methods rely on complex mathematics that are nearly impossible for normal, or classical, computers to break in reasonable time frames.

Quantum computers, in contrast, could break certain types of widely used encryption methods, such as those used for secure website connections, in exponentially shorter times because of key differences in information processing. As described in an earlier GAO report, classical computers process information through bits that can only be 0 or 1 (like an on/off switch). A quantum computer, however, processes information using quantum bits, or qubits, which can be any combination of 0s and 1s simultaneously due to properties of nature at small scales.

Quantum computers that could break current encryption methods—known as cryptographically relevant quantum computers (CRQCs)—may not exist for another 10 to 20 years, according to some experts. The largest quantum computer currently developed only has a small fraction of the necessary qubits for a CRQC. However, data encrypted with current methods can be downloaded and saved for future decryption by CRQCs. For example, technology designs relevant for long periods are at risk if a bad actor steals them and later decrypts them with a CQRC. In other words, if the migration time plus the time data must be securely retained is longer than the time it takes for CRQC development, then data will be unprotected (see fig. 1).



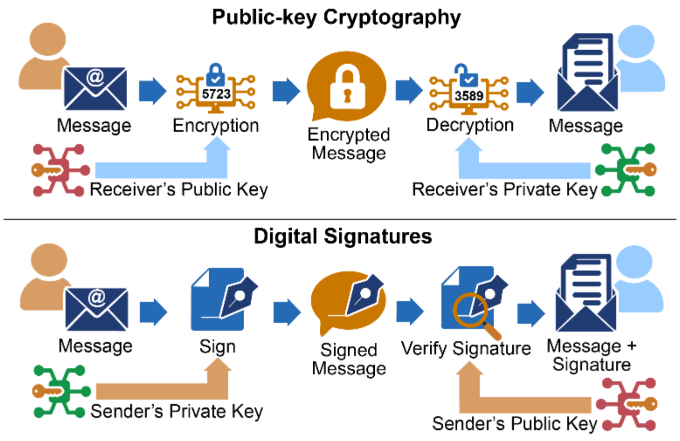
🟥 Data unprotected

Source: GAO adaptation of Mosca's theorem. | GAO-23-106559

Figure 1. A possible scenario of how migration to post-quantum cryptography may affect the safety of sensitive information. The faster this migration occurs; the sooner data can be secured.

To combat the threat of CRQCs, researchers are developing and standardizing new encryption methods collectively referred to as post-quantum cryptography (PQC). These new methods are intended to withstand attacks from both quantum and classical computers.

How does it work? Cryptography protects sensitive data using a series of characters called a "key" which can be public or private. Senders and receivers use keys to lock (encrypt) and unlock (decrypt) the transmitted data. There are three main types of cryptography: private-key, public-key, and digital signatures. Experts generally agree that encryption methods for private-key cryptography are less susceptible to attack by CRQCs and easier to make more secure by using larger key sizes. In contrast, experts generally agree that current encryption methods commonly used for public-key cryptography and digital signatures are susceptible to attack by CRQCs. Public-key cryptography includes the encryption of e-mail and other digital transactions and digital signatures include the virtual signing and authentication of documents (see fig. 2).



Source: GAO (adaptation), National Academies of Sciences, Engineering, and Medicine, © *Cryptography and the Intelligence Community: The Future of Encryption,* Figures S.1.2 and S.1.3, 2022, https://doi.org/10.17226/26168 (analysis), icons-studio/stock.adobe.com (images). | GAO-23-106559

Figure 2. Illustration of the two types of cryptography most susceptible to cryptographically relevant quantum computers.

The mathematical structure underlying current encryption methods commonly used for public-key cryptography and digital signatures could be broken with a CRQC. For example, the Rivest-Shamir-Adleman (RSA) algorithm—a widely used public-key encryption method for exchanging of sensitive information, such as bank transfers—would take billions of years for a classical computer to decrypt, but only hours or days for a CRQC.

Options for replacing current public-key encryption methods fall under different families of challenging mathematical problems that should not be susceptible to decryption by classical or quantum computers. Latticebased encryption, for example, relies on geometry in a highly multidimensional space. This results in a system that should be much more difficult to decrypt, according to experts.

How mature is it? PQC methods have been developed and are undergoing standardization for implementation. A National Institute of Standards and Technology (NIST) public initiative has been developing replacements for at-risk encryption methods since 2016. In July 2022, NIST selected four PQC algorithms the agency will standardize. The National Security Agency plans to incorporate the algorithms into its commercial national security algorithm suite once NIST releases the standards, anticipated in 2024. NIST is also collaborating with expert and standards groups, such as the International Organization for Standardization, which are developing their own PQC standards. Other countries are also working on their own PQC methods.

Why now? While experts do not agree on when a CRQC will be developed, they do agree that the time to prepare for PQC is now. The Office of Management and Budget issued guidance in 2022 on how to identify and prioritize at-risk encryption methods and information for an efficient transition to PQC once the NIST standards are available. For example, sensitive information with long security lifetimes, such as personally identifiable information, would be prioritized in the transition.

Organizations that are unaware of the extent of cryptography use in their systems may need to make unexpected infrastructural changes. For example, PQC may require upgraded microprocessors. Further, in a 2022 national security memorandum, the White House outlined the need for growing an informed PQC workforce in the U.S., as well as the need for ensuring interoperability between federal agencies during the PQC transition. The White House has called for federal agencies to complete the transition to PQC by 2035, but this may not be soon enough to keep data safe from future decryption.

/// OPPORTUNITIES

- **Enhanced data security.** Even if a CRQC is never developed, creating more complex encryption methods could make sensitive and personally identifiable information more secure.
- **Modernized infrastructure.** The technology updates needed for transition to PQC may result in modernized infrastructure that is more agile for future updates than systems that have encryption methods incorporated into their hardware.

/// CHALLENGES

- **Lengthy transition.** Identifying and replacing affected technologies may take a long time, and the longer the transition to PQC takes, the more that sensitive information will be at risk.
- **Cost and complexity.** Transitioning to infrastructure supportive of new encryption methods will be expensive and complex. Organizations may face challenges in planning for incurred costs and in remaining operational during the infrastructure changeover.
- **Workforce gaps.** The U.S. requires more data security and quantum computing expertise than is currently available. For example, one study predicts that fewer than 50 percent of quantum computing jobs may be filled by 2025.
- **Information sharing.** As organizations adopt PQC, some—such as those in law enforcement and national security—may hesitate to share information with those that have not transitioned to PQC.

/// POLICY CONTEXT AND QUESTIONS

- What additional steps could policymakers take to protect against decryption of sensitive data by quantum computers?
- What additional planning may be needed to upgrade infrastructure to support PQC?
- What actions could help build a workforce capable of understanding, implementing, and advancing PQC as needed?

/// SELECTED GAO WORK

Quantum Computing and Communications: Status and Prospects, GAO-22-104422.

Science & Tech Spotlight: Quantum Technologies, GAO-20-527SP.

/// SELECTED REFERENCES

G. Alagic, et al., *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. July 2022.

M. Mosca and M. Piani. *2021 Quantum Threat Timeline Report.* January 2022. https://globalriskinstitute.org/mp-files/2021-quantum-threat-timeline-report-short-report.pdf/.

National Academies of Sciences, Engineering, and Medicine. *Cryptography and the Intelligence Community: The Future of Encryption.* Washington, D.C.: 2022.

GAO SUPPORT:

The Government Accountability Office (GAO) meets congressional information needs in several ways, including by providing oversight, insight, and foresight on science and technology issues. GAO staff are available to brief on completed bodies of work or specific reports and answer follow-up questions. GAO also provides targeted assistance on specific science and technology topics to support congressional oversight activities and provide advice on legislative proposals.

For more information, contact: Brian Bothwell at (202) 512-6888 or bothwellb@gao.gov and Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov

Staff Acknowledgments: Katrina Pekar-Carpenter (Assistant Director), Kristen Pinnock (Analyst-in-Charge), Bradley Becker, Jehan Chase, Louise Fickel, Nicole Jarvis, Curtis Martin, and Kristen Watts.

This document is not an audit product and is subject to revision based on continued advances in science and technology. It contains information prepared by GAO to provide technical insight to legislative bodies or other external organizations. This document has been reviewed by Karen L. Howard, PhD, GAO's Acting Chief Scientist.

This work of the United States may include copyrighted material, details at www.gao.gov/copyright.

Congressional Relations: A. Nicole Clowers, Managing Dir.,(202) 512-4400, clowersa@gao.gov

Public Affairs: Charles Young, Managing Dir., (202) 512-4800, youngc1@gao.gov