SECURING COMMUNICATIONS IN THE QUANTUM COMPUTING AGE

MANAGING THE RISKS TO ENCRYPTION

APPENDIXES C AND D

MICHAEL J. D. VERMEER | EVAN D. PEET

For more information on this publication, visit www.rand.org/t/RR3102

Published by the RAND Corporation, Santa Monica, Calif.

Preface

Quantum computing, a nascent technology that promises to provide powerful new computing capabilities, also presents a potential threat to our communication infrastructure. In its current form, our means of securing communications across the internet—public key cryptography—is widely expected to possess weaknesses that could be exploited by quantum computing. New forms of public key cryptography are being developed that are expected to be secure, but if they are not widely used by the time quantum computers arrive, wide-scale, we would expect disruptive cyber vulnerabilities.

A mixed-method research approach was employed to evaluate the risks and create policy recommendations. While significant variation exists in expert assessments, it is likely quantum computers capable of breaking current encryption will exist before the U.S. communication infrastructure has completely prepared. Moreover, the risk will grow the longer organizations wait to transition to new cryptography. Overall, it was assessed that the threat from quantum computing is urgent, and swift action is necessary to mitigate the risk. The recently begun National Quantum Initiative Program is an important first step, but additional action is needed from the U.S. government. The authors recommend that the executive branch ensure adequate priority is given to this issue and that the chosen coordinating body begin organizing action across the federal government. Congress should also consider beginning to hold hearings to establish oversight over standardization and transition efforts. Finally, individual organizations should take steps to prepare for the coming cryptographic transition and adapt their systems to incorporate greater cryptographic agility.

This online appendix to *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption* (Michael J. D. Vermeer and Evan D. Peet, Santa Monica, Calif.: RAND Corporation, RR-3102-RC, 2020) contains the expert elicitation protocol and consumer survey used in the research.

About the RAND Center for Global Risk and Security

The Center for Global Risk and Security (CGRS) works across the RAND Corporation to develop multidisciplinary research and policy analysis dealing with systemic risks to global security. The center draws on RAND's expertise to complement and expand RAND research in many fields, including security, economics, health, and technology. A board of distinguished business leaders, philanthropists, and former policymakers advises and supports the center activities, which are increasingly focused on global security trends and the impact of disruptive technologies on risk and security. For more information about the RAND Center for Global Risk and Security, visit www.rand.org/international/cgrs.

Security 2040

This report is part of a RAND Ventures initiative to envision critical security challenges in the world of 2040, considering the effects of political, technological, social, and demographic trends that will shape those security challenges in the coming decades. The research was conducted within the RAND Center for Global Risk and Security.

Funding for this project was provided by gifts from RAND supporters and income from operations.

Contents

Appendix C: Expert Elicitation Protocol

Interview Protocol: Quantum Computing and the Future of Encryption

Part I. Introduction:

The goal of this project is to assess any security risks that will result from the future realization of a quantum computer able to break our current public key encryption infrastructure. We are interviewing experts in the domains of quantum computing, cryptography, and industry cybersecurity to gain their insight on the expected future state of quantum computing and post-quantum cryptography (PQC) and the way industry security professionals will adapt to this new reality.

We hope to:

- Identify a timeline for the likely realization of both universal quantum computing and PQC
- Assess security risks resulting from vulnerabilities in our encryption infrastructure in a few possible future scenarios.

The immediate product of this elicitation will be a publication that summarizes the results of a literature review on the subject, the results of this expert elicitation, and the results of a consumer survey. In reporting the results of this study, the experts who contribute will be listed but will not be identified with their specific responses.

We understand that if you have access to classified information, your expert opinion could include knowledge of that information. For that reason, we want to reiterate that you are free to choose not to answer any question for any reason.

Thank you for your participation.

Part II. Background information

It is expected that the creation of a quantum computer will create a threat to the information security of any system that relies upon current public key encryption methods. These encryption methods are relied upon to secure many critical sectors of our digital infrastructure including email, financial transactions, e-commerce, and most internet-based communications. Quantum computers are widely expected to "break" the public key encryption infrastructure as currently implemented, and in so doing nullify much of the security of our current digital infrastructure. In 2016, the National Institute of Standards and Technology (NIST) began an initiative to evaluate ideas for the creation and standardization of public key encryption methods that are secure against quantum computers, so-called post-quantum cryptography (PQC). This year they held the first workshop to examine submitter's presentations and are now in an analysis phase while they consider proposed methods. Their timeline suggests draft standards will be ready in five to seven years (2023–2025).[1] After this time there is expected to be a deployment period during which the new standards are incrementally adopted. Historically, full deployment of new algorithms has often lasted a decade or more. Figure 1 below gives an example of expected industry adoption patterns for new technologies. Adoption of both quantum computing and post-quantum cryptography after their introduction may follow a similar pattern. In the interim, the NSA has suggested that organizations as much as possible make use of algorithms that are believed to already have a measure of quantum-resistance.[2]

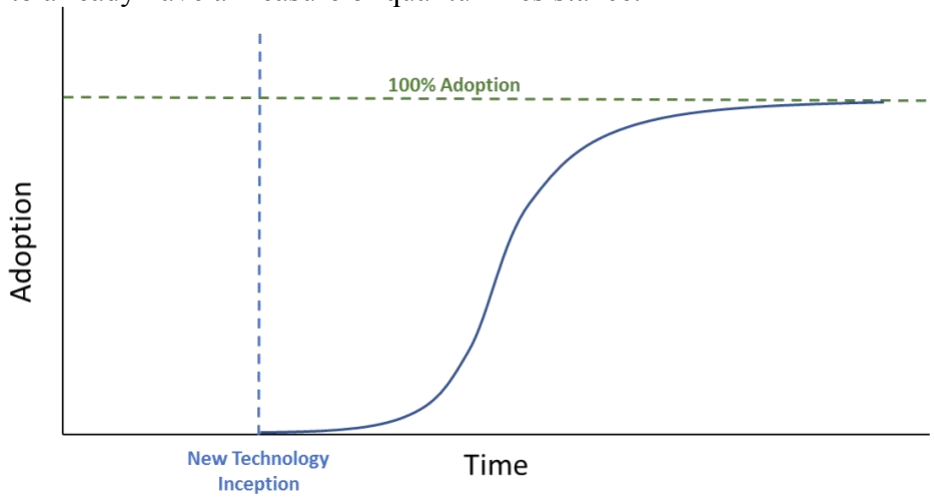


Figure 1. Industry technology adoption curve.[3] Industry adoption of new technologies and security tends to follow a known pattern after a new technology is introduced. Adoption begins slowly with a few early adopters, accelerates, then is followed by a tail of late adopters before near-universal adoption is achieved.

1 "Post-quantum cryptography," National Institute of Standards and Technology, 3 January 2017. Available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

2 Symmetric key and hash-based algorithms are widely considered to be quantum-resistant, *i.e.*, with a moderate increase in key length they can provide equivalent security against a quantum attack.

3 Adapted from Reilly, Michael, "Tech maturity S-curve for insurers," Accenture, 8 November 2016. Available at: https://insuranceblog.accenture.com/tech-maturity-s-curve-for-insurers

Part III. Expected Security Risks

Before we assess your expectations for the timelines of quantum computing and post-quantum cryptography and the consequences of different timelines, we'd like to begin by broadly assessing your expectations regarding the future security risks of these technologies with the following open-ended question:

1. Please discuss any thoughts that you have regarding the security risks that may result from the development of a quantum computer capable to break our current public key encryption infrastructure.

Part IV. Expected State of Quantum Computing and Post-Quantum Cryptography

First, we will ask you to assess the risks to various categories of organizations in three future scenarios. We will describe a range of potential consequences on information security from the creation of a quantum computer capable of breaking public key encryption, then ask you to give your opinion of the likelihood of those consequences occurring.

We would like to learn your view of the security risks to 1) the U.S. defense and intelligence establishment, 2) non-defense U.S. government agencies, 3) advanced tech private sector industries including the information technologies, financial services, and the defense industrial base, and 4) mid-tech private sector industries including telecommunications, healthcare services, and manufacturing. In each of these scenarios, we will ask you to consider the following potential consequence categories. In each case, consider the consequence in a given scenario **if no additional measures were taken to address any security vulnerability presented by quantum computers other than eventual adoption of PQC.**

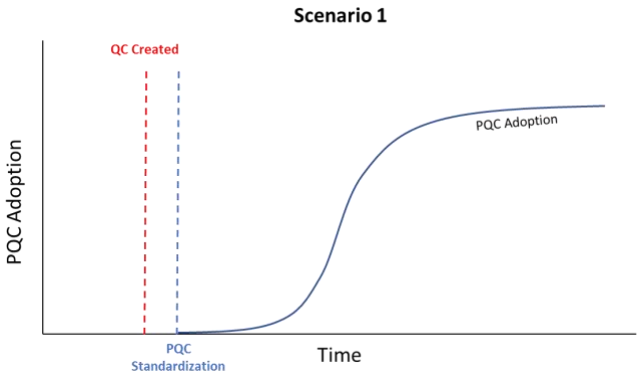
Consequences: If no mitigation measures other than eventual adoption of PQC are taken to address security vulnerabilities . . .

1	Malicious actors are occasionally able to obtain sensitive information.
2	Malicious actors have frequent access to sensitive information.
3	Malicious actors have complete control of information systems.

For each scenario, please give us your opinion of the likelihood of each consequence being realized for each category of organization. To do this, please write a number between 0 (no chance) and 100 (absolutely certain) in the boxes below. The sum of the 3 boxes should add up to 100 for each category of organization. After reporting your opinions of the likelihood of each consequence for each sector, we will ask you to examine your responses and whether you would like to make any revisions. If you would like to revise, please do so.

Scenario 1

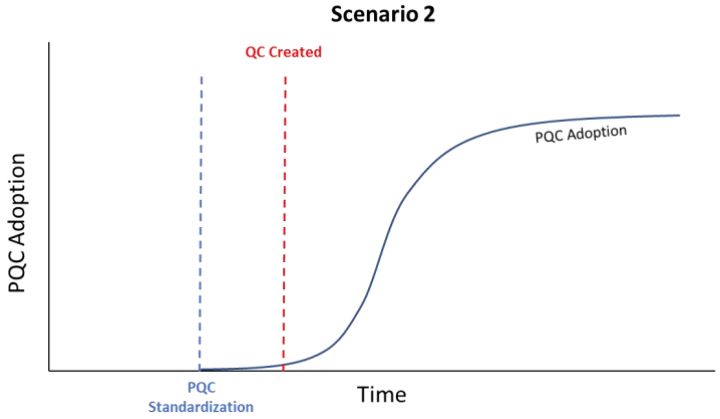
A quantum computer capable of breaking current public key encryption is created before post-quantum cryptography is standardized. Assume that while some organizations and government agencies will have moved to incorporate quantum resistant methods in their security where possible, no fully quantum-safe protocol standards are available for adoption. ***Do you understand this scenario and what we are asking you to do?***



	Occasional access Score = 1	Frequent access Score = 2	Complete control Score = 3	Reason(s) for most likely consequence
U.S. defense & intelligence establishment				
Non-defense U.S. government agencies				
Adv. Tech (info tech, fin services, def. ind)				
Mid. Tech (telecom, healthcare, mfg.)				

Scenario 2

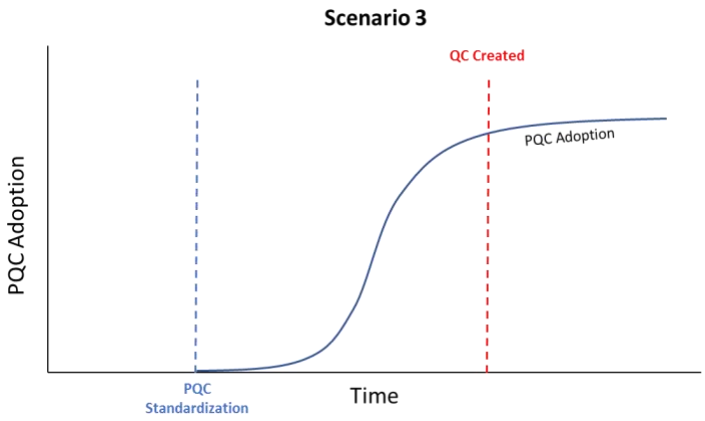
A quantum computer capable of breaking current public key encryption is created within 3 years following the standardization of post-quantum cryptography. Assume that most (but not all) government agencies will have followed NSA directives to begin transitioning to quantum-safe cryptography, but many industry sectors continue to have gaps in the transition to PQC. ***Do you understand this scenario and what we are asking you to do?***



	Occasional access Score = 1	Frequent access Score = 2	Complete control Score = 3	Reason(s) for most likely consequence
U.S. defense & intelligence establishment				
Non-defense U.S. government agencies				
Adv. Tech (info tech, fin services, def. ind)				
Mid. Tech (telecom, healthcare, mfg.)				

Scenario 3

A quantum computer capable of breaking current public key encryption is created 10 or more years after the release of standards for post-quantum cryptography. Assume that government agencies and many critical industry sectors have universally transitioned to PQC, and other industry sectors have followed historical patterns for the adoption of security to protect against known vulnerabilities. ***Do you understand this scenario and what we are asking you to do?***



	Occasional access Score = 1	Frequent access Score = 2	Complete control Score = 3	Reason(s) for most likely consequence
U.S. defense & intelligence establishment				
Non-defense U.S. government agencies				
Adv. Tech (info tech, fin services, def. ind)				
Mid. Tech (telecom, healthcare, mfg.)				

Part V. Quantum Computing and Post-Quantum Cryptography Timeline

We would like to ask you your opinion on the likely timeline for creation and adoption of quantum computing, post-quantum cryptography and some associated technologies. Please give us your opinion of the timeline of each development or event occurring by providing a year estimate. To make this part of the survey tenable, we will not be able to cover every technological path within these categories. Instead, please select what you consider to be the single most promising path within each major category as the "best representative" for answering the following questions.

As we walk through these questions, we will ask that you fill in your responses in the following way:

1. First, please report the earliest possible year that this technology could be developed or the event could occur.
2. Then ask yourself if you can imagine any possible circumstance under which the event could occur earlier. If you can think of such a circumstance, then please revise your estimate accordingly.
3. Next, please report the latest possible year that this technology could be developed or the event could occur.
4. Again, ask yourself if you can imagine any possible circumstance under which the event could occur later. If you can think of such a circumstance, then please revise your estimate accordingly.
5. Once you have made and refined your estimates of lower and upper bounds, *then* please report your best estimated year when the event will occur.

For each of the technologies or events, we will first define and describe each. Please use this definition when responding. If you have an alternative definition or understanding, please inform us after responding.

Quantum Computing Technologies:

Quantum computer capable of breaking public key encryption: The creation of a computing system capable of breaking the encryption algorithms used in current public key infrastructure.

QC Tech	Earliest possible year	Latest possible year	Best estimated year	Reason(s)
Overall: Quantum computer capable of breaking public key encryption				

Quantum Computing Adoption:

Government adoption of QC: The first use by any U.S. government agency of a quantum computer capable of using algorithms to break public key encryption.

Adoption of QC by state-level malicious actor: The first use by an organization acting on behalf of an adversary state of a quantum computer capable of using algorithms to break public key encryption.

Adoption of QC by individual malicious actor: The first use by an individual malicious actor for personal use of a quantum computer capable of using algorithms to break public key encryption.

QC Adoption	Earliest possible year	Latest possible year	Best estimated year	Reason(s)
First government adoption of QC				
First adoption of QC by state-level malicious actor				
First adoption of QC by an individual malicious actor				

Post-quantum Cryptography and Adoption:

Creation of quantum-safe security suite: The first creation of a full security suite that is secure against quantum attack via the use of post-quantum public key encryption methods.

Near-universal U.S. defense establishment adoption of PQC: >95% adoption by U.S. defense and intelligence agency systems of post-quantum cryptography into their security.

Near-universal U.S. government adoption of PQC: >95% adoption by all U.S. government agencies of post-quantum cryptography into their security.

Near-universal adoption of PQC by advanced technology industry sectors: >95% adoption by advanced technology private sector industries including the information technologies, financial services, and the defense industrial base of post-quantum cryptography into their security.

Near-universal adoption of PQC by mid-technology industry sectors: >95% adoption by mid-technology private sector industries including telecommunications, healthcare services, and manufacturing of post-quantum cryptography into their security.

		Earliest possible year	Latest possible year	Best estimated year	Reason(s)
PQC Adoption	Creation of quantum-safe security suite				
	Near-universal U.S. defense establishment adoption of PQC				
	Near-universal U.S. gov't adoption of PQC				
	Near-universal adoption of PQC by advanced tech industry sectors.				
	Near-universal adoption of PQC by mid-tech industry sectors.				

Part VI. Discussion questions

Open-ended questions on other factors that may impact security risks presented by quantum computing.

1. Is there anything else that we didn't ask you that we should have in order to better understand timelines for QC, PQC, adoption, and the implications for security?

2. What do you expect the impact to be from data with a long intelligence lifetime that could be intercepted now and decrypted later by a quantum computer? How significant is this vulnerability?

3. Other than scalable qubit fabrication, controllable quantum logic, readout capability, and scalable error correction, are there other key technological breakthroughs that will be needed to create a quantum computer capable of breaking public key encryption?

4. What are some of the mitigation measures you would expect organizations to take in addition to or in lieu of implementation of post-quantum cryptography if they were vulnerable to attack by a quantum computer?

5. What are some examples of the consequences of systems being vulnerable to quantum attack after quantum computers arrive?

Appendix D: Consumer Survey

1. How knowledgeable are you about quantum computing?
   SCALE: LOW END [1]: Not at all knowledgeable
   HIGH END [10]: Extremely knowledgeable
2. How knowledgeable are you about how quantum computing may affect cybersecurity?
   SCALE: LOW END [1]: Not at all knowledgeable
   HIGH END [10]: Extremely knowledgeable
3. How knowledgeable are you about how encryption is used on the internet?
   SCALE: LOW END [1]: Not at all knowledgeable
   HIGH END [10]: Extremely knowledgeable
4. In 2013 the credit and debit card information of 40 million customers was stolen from the retail organization, Target. How concerned were you?
   SCALE: LOW END [1]: Unconcerned or did not know this happened
   HIGH END [10]: Extremely concerned
5. Following the theft of credit/debit card information from Target in 2013, how did you respond?
   a. I did nothing
   b. I checked how my information was affected
   c. I froze my credit reports
   d. I began using an identity protection service
   e. I limited my shopping at Target for a while
   f. I stopped shopping at Target for a while
   g. Other
6. In 2017 the social security numbers and other personal information of 143 million Americans was stolen from the credit reporting agency, Equifax. How concerned were you?
   SCALE: LOW END [1]: Unconcerned or did not know this happened
   HIGH END [10]: Extremely concerned
7. Following the theft from Equifax of social security numbers and other personal information in 2017, how did you respond?
   a. I did nothing
   b. I checked how my information was affected
   c. I froze my Equifax credit report
   d. I froze all three of my credit reports
   e. I began using an identity protection service
   f. Other

8. Imagine a tech that lets hackers control smart phones is **nearly developed** and your phone maker (e.g. Apple) has **not** installed new security **but** others have. What do you do?
    a. I don't currently use a smart phone
    b. I keep my smart phone and use it the same
    c. I keep my smart phone but remove private things
    d. I plan to buy a new, more secure phone
    e. I immediately buy a new, more secure phone
    f. I stop using smart phones altogether
9. Now imagine hackers **have the tech** to control smart phones, and some phones have been hacked. Your phone maker has **not installed new security**. What do you do?
    a. I don't currently use a smart phone
    b. I keep my smart phone and use it the same
    c. I keep my smart phone but remove private things
    d. I plan to buy a new, more secure phone
    e. I immediately buy a new, more secure phone
    f. I stop using smart phones altogether
10. Now imagine hackers have used the new tech to **hack your smart phone maker** and now **can** see and control everything on **your** smart phone. What do you do?
    a. I don't currently use a smart phone
    b. I keep my smart phone and use it the same
    c. I keep my smart phone but remove private things
    d. I plan to buy a new, more secure phone
    e. I immediately buy a new, more secure phone
    f. I stop using smart phones altogether