WORKING GROUP PAPER

APRIL 2019

Implications of Quantum Computing for Encryption Policy

Encryption Working Group

Implications of Quantum Computing for Encryption Policy

Encryption Working Group

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This paper and its companion piece on user-controlled encryption were prepared by Princeton University's Center for Information Technology Policy at the request of the Carnegie Encryption Working Group as briefings to provide insight into future trends related to encryption policy. The papers do not take a position on encryption policy, rather they provide analysis of the future trends related to encryption and how they will shape the issues that policymakers must address.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate around the world.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, The Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

Introduction

Quantum computing is still in its infancy, but its future development could reshape many aspects of computing, including encryption. Although the impact of quantum computing on encryption has been widely discussed, there has been less attention to how quantum computing would affect proposals for exceptional access to encrypted data, including key escrow, the most commonly suggested approach.

How Quantum Computers Differ From Traditional Computers

Unlike ordinary classical computers, quantum computers are constructed on different underlying mechanisms of physics. Rather than relying on classical bits of information, which take on a value of either zero or one, a quantum computer is built on quantum bits (or qubits) that can be in states that combine aspects of zero and one, according to the rules of quantum mechanics. Because quantum computers rely on different physical mechanisms, they in principle can perform some computations much more quickly than classical computers can. There is a rich, detailed theory of what quantum computers can and cannot do, and how they compare to classical computers.

Quantum computers, in principle, can do some computations much faster than classical computers, some computations only modestly faster, and some at the same speed. So the arrival of practical quantum computers would change some of the tradeoffs involved in designing algorithms, including cryptographic algorithms. As described below, cryptography experts in government, industry, and academia have been working for years to prepare for the potential arrival of quantum computers, although much work remains to be done.

Quantum computers are very difficult to build. As of yet, nobody has succeeded in building a quantum computer that is large enough or fast enough to offer any practical advantages over (or even parity with) classical computers. Although substantial gains have been made in theory, materials, and measurement, since 2001 the size of quantum computers has increased to only seventy-two physical qubits. There has been no demonstration of a single logical qubit that could

serve as the building block of a large-scale quantum computer, and thousands of such qubits would be needed for applications to cryptanalysis.

But research is advancing rapidly. And although there is substantial uncertainty about the future pace of improvements to quantum computers, and some experts question whether quantum computers large enough to impact cryptography can ever be built, it is realistically possible that a practical quantum computer could become available over the next ten to twenty years that would be sufficiently large to place many encryption systems at risk.[1] Even before fully quantum systems become practical, many experts predict that the anticipated transition to quantum computing will likely involve the use of hybrid systems that combine limited quantum computing functionality with classical supercomputers to reach significantly higher effective processing speeds than classical-only devices. Early quantum systems, whether hybrid or pure quantum, would likely be very expensive and rare.

Regardless, current data collection could pose risks if an adversary is recording encrypted communications, or acquiring or breaking into systems to collect encrypted stored data. If that is the case, and if such an adversary were to acquire a quantum computer in ten to twenty years, they would be in a position to quickly decrypt all the data they had collected to date.

Why Quantum Computing Matters for Encryption

The security of encryption systems relies on the use of operations that can be done quickly by someone who knows a secret key but requires vastly more time for someone who does not know it. An encryption algorithm typically has an adjustable key size, and the algorithm is designed so that a modest increase in the key size causes a modest increase in decryption time for those who know the key, but a massive increase in decryption time for those who don't know it. This ensures that the key size can be made large enough so that decryption becomes massively, prohibitively expensive for those who do not know the key, but remains very practical for keyholders. The security of a cryptographic algorithm depends on maintaining a very large gap between the effect of a key size increase on those that know the key versus those that do not know it.

Decryption without knowing the key amounts, in practice, to a kind of brute-force search: it requires searching an extremely large space of possible secret keys, trying different keys in turn until finding one that unlocks the encrypted data. On a classical computer, the expected time required to do this is proportional to the number of possible keys that exist—the searcher must try half of the possible keys to have a fifty-fifty chance of trying the correct one.

The effect of quantum computing on the security of an encryption algorithm depends on how large of an effect quantum computing will have on the time required for nonkeyholders to find the secret key.

Encryption Algorithms That Quantum Will Thoroughly Compromise

For some encryption algorithms, quantum computing might allow those without the key to sidestep entirely the need to do brute-force search by, for example, enabling a key extraction algorithm that can find the decryption key directly without a blind search. For instance, the popular Rivest-Shamir-Adleman (RSA) encryption algorithm relies on the assumption that factoring a large number is very difficult. In RSA, the secret key is essentially a pair of large prime numbers, P and Q. The product of multiplying P and Q is published, but it is assumed that an adversary who knows the product of P and Q cannot derive the factors P and Q from that product except by a variant of brute-force search. Factoring appears to be very time-consuming for classical computers, but a quantum computer could quickly extract the factors P and Q by using a method called Shor's Algorithm. In a world with large quantum computers, RSA would not be secure because someone without the key who knows the publicly available product of P and Q could quickly recover the secret key.

Encryption Algorithms That Can Be Kept Secure By Increasing Key Size

Other encryption algorithms are not prone to being defeated so thoroughly by a method like Shor's Algorithm. For these methods, quantum computing is not a fatal threat, because an adversary must still engage in brute-force search. But there is a quantum shortcut, called Grover's Algorithm, that can speed up any brute-force search substantially, allowing a space of a given size to be searched in an amount of time proportional to the square root of that size. This approach would be enough to defeat many encryption methods if they are not adjusted.

In this case, it is possible to compensate for the effect of quantum computing by increasing the key size, expanding the space that must be searched by brute force, so as to counteract the effect of Grover's Algorithm. For many encryption algorithms, doubling the key size, say from 128 bits to 256 bits, has the effect of squaring the size of the key space that someone without the key would have to search. This countermeasure exactly offsets the square-root effect of Grover's Algorithm, restoring the security level of the pre-quantum algorithm.

One consequence is that data that was encrypted before the emergence of viable quantum computing—with the original smaller key size—will become susceptible to decryption when quantum computing does become available, but data encrypted with the larger quantum-safe key size will continue to be secure. (Like classical computers, quantum computers would be expected to get faster over time, necessitating the same kinds of generational increases in key size that have been necessary in the pre-quantum computing era.)

The Transition to Quantum-Safe Encryption

As the emergence of practical quantum computers approaches, organizations must update their systems to use quantum-safe encryption. Encryption methods that can be defeated by quantum computing must be replaced by methods that withstand quantum computing, and encryption methods that remain viable must have their key sizes increased. Refinement and adoption of these methods could take a long time. Experience indicates that phasing out an endangered encryption algorithm can take a decade or more.[2] Given the possibility of large-scale quantum computers in the next two decades, and the legal requirements to protect some forms of classified data for at least two decades, government agencies should begin using quantum-safe encryption for security-critical data. In fact, any users who need data to remain secure for more than a decade should start switching over to quantum-safe encryption as soon as possible.

A critical consideration in this adaptation process is the need to know in advance, with high confidence, that the new encryption method one wishes to use is quantum-safe as well as secure against classical computing attacks. This is a difficult challenge, since the capabilities of future

quantum computers are poorly understood, and new quantum algorithms are likely to be discovered in the future.

Cryptographers have been working for years to prepare for the potential arrival of quantum computers by developing quantum-safe encryption methods. Companies and consortia in the United States, Europe, Asia, and elsewhere have active research programs. The U.S. government is also striving to adapt to a future with quantum computers. Government agencies, including the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), have been working for years on quantum-safe encryption methods for government use. NIST also launched a post-quantum cryptography standards process in 2016 to develop standards for quantum-safe encryption of nonclassified government information, standards that private sector actors are also likely to use. The second round of NIST's competitive selection process includes twenty-six proposals submitted by companies and universities in the United States and elsewhere.

Predicting the Arrival of Quantum Computers

If cryptographically relevant quantum computers become feasible, experts will probably have several years of advance warning. Current quantum computing architectures do not scale well, so new approaches would probably need to be proposed and evaluated to reach the necessary scale. Still, if the goal is to protect secrets for twenty years or more, then quantum-resistant encryption should probably be used today for more data.

The prevalence of quantum computing is another salient factor. Will quantum computing be available initially to only a few actors or will it soon become widely available? The gap between the leading industry or academic lab and the second-place lab is probably just a few months.[3] This suggests that knowledge of how to build a quantum computer, once it existed, would be widely available before long. But the first encryption-relevant quantum computers would likely be very costly (and would probably be hybrid systems that relied on the support of very large, expensive classical computers), so cost would be an impediment to wide availability in the early years. In any case, most analysts believe that if anyone does develop a viable quantum computer, that innovation would be next to impossible to keep under wraps. Experts assess that it is unlikely that a large-scale quantum computer could be developed secretly.

Effect of Quantum Computing on Key Escrow

Proposals involving key escrow, a commonly cited potential approach to exceptional access, typically rely on public-key encryption, that is, an encryption method that uses separate keys for encrypting and decrypting. (This allows a device to encrypt an escrow package in such a way that the device itself cannot decrypt what it previously encrypted, because the device would know the encryption key but would not know the decryption key. The decryption key would be more closely held.)

Most public-key encryption systems deployed today in new devices and services are not quantum-safe. To achieve parity with the security of these systems, a key escrow system would not require quantum-safe encryption. But if a higher degree of security is sought for key escrow systems to maintain data security for decades, then these systems would need to rely on a public-key encryption method that is quantum-safe. If it is not quantum-safe, then data stored on the device can be recovered later by any adversary who has a sufficiently large quantum computer. The adversary could record an image of the encrypted storage today, along with the escrow package, and then later use their assumed access to a quantum computer to defeat the encryption that protects the escrow package, thereby gaining access to the information needed to decrypt the stored image of all the data on the device.

That said, in the early years of quantum computing, encryption-breaking capabilities would probably be scarce and expensive, so actors with such capabilities would be expected to reserve them for the highest-value targets. Accordingly, widespread breaking of escrow packages would be unlikely in the early years of quantum computing. In the long run, however, the cost of breaking legacy escrow packages would likely continue to decrease.

Accordingly, the main impact of quantum computing on key escrow is that the potential emergence of large quantum computers would force escrow methods to switch to encryption methods that have undergone far less vetting for their general security than the encryption methods used today. This increases the technical risk associated with key escrow (along with most other applications of public-key encryption). In the coming years, experts and practitioners will continue to grapple with the challenge of shoring up encryption methods to contend with advances in quantum computing.

Acknowledgments

This publication benefited greatly from the suggestions and feedback of several members of the Encryption Working Group.

Notes

1 This and other time estimates later in the piece are based on assessments by the authors.
2 Based on the assessment of the authors.
3 Based on the assessment of the authors.

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org