A Day without Safe Cryptography

Presented by the Quantum Safe Security Working Group

TABLE OF CONTENTS

ABOUT CSA

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at www.cloudsecurityalliance.org and follow us on Twitter @cloudsa.

ACKNOWLEDGMENTS

Lead Author:

Jeffrey Ritter

Quantum Safe Security Working Group Co-Chairs:

Bruno Huttner
Jane Melia

Cloud Security Alliance:

Hillary Baron
Ryan Bergsma
Victor Chin
Kendall Scoboria

Contributors:

Jon-Michael Brook
Marcelo Carvalho
Edward Chiu
Moshe Ferber
Vishal Patel
John Rauser
DeLora Rosario

INTRODUCTION

Over the past fifty years, the digital age has sparked the creation of a remarkable infrastructure through which a nearly infinite variety of digital transactions and communications are executed, enabling businesses, education, governments, and communities to thrive and prosper. Millions of new devices are connecting to the Internet, creating, processing, and transferring digital information in greater volumes and with greater velocity than ever imagined.[1]

The momentum and success of this global transformation is largely due to advances in engineering and deployment of encryption tools and services. As digital information has become more valued, talented mathematicians and scientists have used cryptography and mathematics to build multiple generations of stronger, more effective security to protect against possible breaches.

When properly designed and launched, encryption services enable institutions, nations, companies, and individuals to trust the global digital infrastructure as an indispensable resource for improving the quality of their lives. Despite the breaches that receive public attention, we know that malicious conduct often succeeds only when cryptography has not been properly deployed. Countless investigations confirm that human errors, or uses of encryption that is not of sufficient strength for the value of the protected data assets, are the original causations; the science and mathematics behind the security are sound.

But what if, on any particular morning, the encryption tools we rely on were suddenly ineffective? What if a fundamental advance in computing occurred that rendered our current encryption tools and services unable to protect data assets and systems from unwanted intrusion, interference, or surveillance? The outcome would surely entail a catastrophic collapse of trust, endangering the stability and reliability of the global infrastructure and, ultimately, all transactions and services.

That possibility is now on the horizon as a consequence of the continuing advancements in quantum computing. Indeed, a large segment of the mathematic and scientific community that enabled today's success in encryption is now prioritizing how to engineer new encryption services to ensure quantum computing can succeed. Even before quantum computers mature into machines that can support "general purpose" computing, scientists have realized that quantum computing, when used with malicious intent, has the capacity to overwhelm existing cryptographic tools and services.

The lesson in the evolution of today's digital infrastructure is clear: priority must be placed on engineering security into each generation of new innovations rather than deferring security investments to later points in the development process.

This brief white paper serves to illuminate the importance of building and using encryption tools as quantum computing quickly becomes a reality. The intended goal is to put in place "quantum-safe" encryption tools and services before quantum computing becomes real, and *before* its capabilities become available to bad actors for malicious or criminal purposes.[2] In this paper, we answer the following questions:

- What is quantum computing?
- How will quantum computing place existing cryptography and encryption at risk?
- What would our digital lives look like if existing encryption services were broken by quantum-capable bad actors?
- What will quantum-safe encryption look like? What are the next steps forward?

[1] See https://www.vanityfair.com/news/2008/07/internet200807.

[2] For our purposes, "bad actor" can be any entity acting adversely to a company's interests or intentions.

WHAT IS QUANTUM COMPUTING?

Quantum computing introduces an entirely new engineering design for computers. Built on quantum mechanics, when released, quantum computing will transform and magnify achievable computing power and efficiency. Quantum computers will be capable of calculating solutions for computational problems and exercises that existing "classical" computers cannot solve. Quantum computers will also alter the amount of time and resources required to execute existing computational exercises and processes that are, today, both complex and intensive.

Working, small-scale quantum computers exist today.[3] Engineering and fabrication techniques required to construct large "general purpose" computers are advancing much faster than previously imagined. Combined with distributed cloud services and advances in artificial intelligence computing, quantum computing may achieve commercial operations sooner than earlier estimates of 2022.[4] In addition, investments to build quantum capabilities are accelerating, and many of those investments focus on building and launching quantum-safe security solutions and services. The momentum is truly global, and the competition is extraordinary—China, Switzerland, and United States are all hosting significant research and development initiatives.

Quantum computing employs qubits—the quantum analog for a classical bit. Qubits possess certain properties that, when assembled into quantum systems, can process and execute enormously complex calculations as electrical energy passes through them. This is achieved by enabling qubits to sustain superposition, something existing computing cannot accomplish.

Quantum computing transforms supercomputing capabilities in material science, physics, chemistry, medicine, automated systems and robots. Quantum systems are hard to build, and even harder to operate for long periods of time, yet their power, and their potential, continues to gain momentum.

HOW WILL QUANTUM COMPUTING PLACE EXISTING CRYPTOGRAPHY & ENCRYPTION AT RISK?

Existing cryptography uses mathematical processes to create keys which are then used to encrypt digital content. At every level of computing, encryption protects vital assets: userIDs, passwords, IP addresses, electronic mail, digital signatures, credit card transactions, securities trading, electronic commerce, government benefit services, intellectual property, consumer media, websites, social media, and much more. A key is a mathematical algorithm that is used to scramble the content (far more complex than replacing "A" with "M" and "B" with "N"!). Keys are variable in length and can be up to 256 bits or longer!

Once a key is applied, the encrypted content (called ciphertext) can be transmitted and received by two parties. The ciphertext can only be decrypted by a receiving party using a suitable key—either a key that is paired to the original encryption key (asymmetric cryptography) or is the same key used for the encryption (symmetric cryptography). With either method, the required key is separately transmitted and exchanged, usually also in an encrypted form.

There are many variations of both asymmetric and symmetric cryptography in commercial use. Most computer scientists

[3] In November 2017, IBM announced they have built a 50-qubit quantum computer. https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/ (Last Visited December 4, 2017). Others are racing to achieve even more. See https://www.nytimes.com/2017/11/13/technology/quantum-computing-research.html?_r=0 (Last Visited December 4, 2017).

[4] https://www.wired.com/2017/03/race-sell-true-quantum-computers-begins-really-exist/ (Last visited November 10, 2017). IBM has announced offering the first commercial quantum service by the end of 2017. https://techcrunch.com/2017/11/10/ibm-passes-major-milestone-with-20-and-50-qubit-quantum-computers-as-a-service/ (Last visited December 5, 2017).

and engineers are familiar with these variations by their names or acronyms. Asymmetric algorithms include RSA, EEC, and Diffie-Hellman (the latter is used to exchange keys for use in symmetric encryption). Symmetric algorithms include Triple DES (authorized by NIST, a US government agency, for use through 2030) and AES (the Advanced Encryption Standard, a subset of what is known as the Rijndael cipher).

The only way bad actors can decrypt any encrypted content is to obtain or guess the key with which the ciphertext was created. Existing cryptography works because it is mathematically infeasible for a bad actor to guess the precise key with which the original content was encrypted. They will try, often using "brute force", which is merely machine-generated guesses of all the possible combinations for any single key. But that approach only succeeds when very poor, commercially inadequate keys have been used; for virtually all modern commercial uses of existing cryptography, the encryption works.

But this is exactly where quantum computing, in the control of bad actors as a strategic weapon, is so concerning. Quantum computing will have the computational power to solve, and dramatically decrease the breaking resistance of the cryptographic solutions used today to encrypt billions and billions of digital information assets. Once those keys are calculated, the encrypted content can be decrypted and made accessible to anyone. In fact, computer scientists have already figured out how to do so—they are just waiting on quantum computing to catch up.

One solution for "cracking" all commonly used asymmetric cryptographic keys is called Shor's Algorithm. Scientists project that Shor's Algorithm, running on a sufficiently large quantum computer, will be able to break any ciphertext that is encrypted using current asymmetric cryptography. In other words, the complexity of the related algorithms will be overcome by the computational power of the machines applying that algorithm.

For symmetric cryptography, one solution is called Grover's Algorithm. It is believed that Grover's Algorithm will be able to break any symmetric key currently in use, for which the maximum key length is 128 bits. Scientists have calculated, however, that if the key length for a symmetric key is doubled to 256 bits, the mathematical complexity will not be overcome within the foreseeable future of quantum computing.[5]

So quantum computing, once scaled into use, threatens current cryptographic tools (absent the current use of 256-bit encryption). That is, in itself, an unsettling reality of the momentum toward functional quantum computing. As promising as its future to critical questions now beyond our reach, in the wrong hands, quantum becomes a viable weapon.

The threat is so promising that companies are quietly reporting that bad actors who achieve unauthorized access to commercial systems are copying and retaining vast quantities of encrypted databases and stored digital assets with the expectation they will soon be able to break the related keys and examine and exploit the previously secured content.[6]

WHAT WOULD OUR DIGITAL LIVES LOOK LIKE IF EXISTING ENCRYPTION SERVICES WERE BROKEN BY QUANTUM-CAPABLE BAD ACTORS?

Imagining the impact of broken encryption tools and services is difficult to understate. Cryptography serves many defensive goals, among which are to:

- Protect systems and networks from access by unauthorized users.

[5] Merely extending the key length may not fully protect authenticated, encrypted content. Other algorithms, such as Simon's Algorithm, also threaten the utility of existing cryptography post-quantum. See https://arxiv.org/pdf/1602.05973.pdf.

[6] See https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/.

- Safeguard website connections (such as https://) to assure users of the authenticity of the website content and the security of any transaction involving personal information or financial data.
- Enable online approvals, digital signatures, and other procedures that work only when the authenticity of the user, and the integrity of their action, can be validated and assured.
- Expedite the installation of software code updates, patches, and new releases.
- Restrict connections to business IT networks only to mobile devices (such as laptops, tablets, and phones) that are authorized and validated as those of authorized users.
- Assure only authorized medical professionals (and their patients) access and rely upon medical health information.

What happens if these defensive objectives are defeated by bad actors using quantum computing to break the related encryption keys and services? The adverse effects can threaten our daily social, business, and government activities, perhaps catastrophically. To illustrate, here is a partial summary focusing on your individual interactions with systems, devices, and information assets that are, today, protected by encryption services:

At the Start of Your Day

- Attempts to access your work email via your phone prove unsuccessful; the mail server has been compromised and existing password files have been wiped clean.
- Using your laptop to read the news, you see an astounding story on a major news site and headlines on other sites reporting the news site server has been hijacked, rendering all of the news stories available there to be unreliable.
- Phone calls and text messages from your colleagues cascade into your phone, all reporting similar issues accessing work-related servers.
- Alarmed, you decide to shift your major securities investments into fixed income mutual funds but discover that the brokerage website is not available; bad actors have gained control of the encryption keys at a related cloud service provider, disabling the interface to the public website.

The Morning at Work

- Major disruptions are being reported on the transportation systems today. The entire transportation system has switched to manual operations, with only a few trains operating. Your short commute to work has turned into a solid two-hour nightmare. Many of your colleagues cannot even make it into the office.
- Arriving at the office, you learn that the entire electronic supply chain management network is not reporting tracking and status updates. Initial security reports indicate the cloud service provider's server network has been overwhelmed by queries for tracking data from authorized users (for which the bad actors have obtained and decrypted related encrypted access codes). Deliveries at seven national warehouses are backing up as the notifications of inbound deliveries are not being received.

Lunch Break

- You go out for lunch and are embarrassed to be told your secure "chipped" credit card is maxed out; the private key embedded on the card has been derived by attackers and a forged card has already been created and used to the full amount of the available balance. Of course, you are not the only one affected. In fact, to protect their customers against the breaches, banks have frozen all of their customer assets and stopped all ATMs. You are lucky enough to able to withdraw some funds from your own branch, after manual identification and a few hours wait at the teller.

The Afternoon at Work

- An emergency meeting of your executive team shares the devastating news that the key management system for the encryption controls on all of your enterprise systems has been compromised and virtually all keys managed by the company must be reissued and exchanged before any additional customer orders or supplier payments can be processed. No one knows if the reissued keys will stand for any length of time.

The Evening

- Returning home early, you receive a text message from the security team on your phone. The message alerts you to access and download from an external website a code update patch for any laptop or phone used to conduct business. The message, the website, and the code update all appear genuine; however, bad actors have generated malicious code and used stolen encryption keys to “sign” the code in order for it to appear genuine to any of the devices.

Of course, no one knows today where bad actors will strike first. The many publicized incidents involving consumer information targets are likely relatively small compared to the economic and strategic value of attacking infrastructures and valued corporate and governmental assets. But if any of these attacks succeed, and they will, the operational and economic impact of the resulting loss of trust in your company may take years to rebuild.

WHAT WILL QUANTUM-SAFE ENCRYPTION LOOK LIKE? WHAT ARE THE NEXT STEPS FORWARD?

Quantum-resistant cryptographic algorithms and innovations, such as a new method for distributing quantum-based keys (called Quantum Key Distribution or QKD), already exist today. As noted earlier, increasing the key length of symmetric keys to 256 bits will be enormously useful to resisting those using Grover’s Algorithm (and related computing machines) to break them. So often, business executives delay decisions to improve security, waiting to see if the new technology is worth the investment. In this case, the path forward is now known and visible. Quantum-safe encryption is available. This means that those questioning whether to proceed can no longer wait for the technology.

But availability requires more than simply “plug-and-play.” The last 25+ years of computing innovation confirm that retooling cryptographic solutions is intensely time-intensive in execution. Solutions must be identified, selected, tested (including for interoperability across the complex digital ecosystems in which any business now operates), and deployed.

Within most companies, the most challenging retooling work requires updating cryptographic libraries and frameworks that support enterprise-level, internally developed applications. Large, multinational businesses may have thousands of these applications; merely discovering them and integrating them into the necessary evolutionary updates promises to be a daunting task.

The final steps will entail structured, well-disciplined, and measured training, vendor selection, alignment and retooling of both suppliers and customers, contracting amendments, and possible legal reforms to adjust the responsibilities and allocation of risk.

Balancing and planning that level of effort to improve security against the risks of current security services being compromised will be challenging. But the pace of quantum computing, and its potential to be misused by bad actors, largely invalidate the historical calculations with which industries and governments have previously decided to “take the risks.” As highlighted above, the risks of delay can be catastrophic to businesses and consumers.

In 2015, Michele Mosca, co-founder of the Institute for Quantum Computing, emphasized that the main challenges to achieve quantum-safe computing will not be technical; instead, organizations must grapple with the numerous business and policy decisions required to move forward. In her view, deploying quantum-safe cryptography must occur before quantum computers become available for general commercial use.[7] In other words, unless security is in place, quantum computing will be more dangerous than trustworthy.

Since 2014, the Cloud Security Alliance has maintained a Quantum-Safe Working Group to focus on what will be required to adapt or replace existing encryption tools and services with quantum-safe encryption solutions. Their work, including this white paper, emphasizes building the methodologies and standard-facing processes for doing so.

What are the next steps? The Working Group welcomes your engagement and contributions. Quantum-safe security is not simply another task item for corporate security teams; it is a vital and strategic priority for companies to sustain their competitive capability in global markets. Those nations, economies, and companies that are first to implement quantum-safe security will experience dramatically reduced costs in insurance and security defenses while enjoying the functional and computing benefits that quantum computing will deliver.

There is one further compelling truth about the power of quantum computing and the importance of quantum-safe security: a single company will only be as secure as every business system with which that company connects. Advancing toward effective quantum-safe security will require a company's full business ecosystem to be engaged and invested. There can be no weak link among trading partners, customers, suppliers, or contractors. The time to begin is now.

[7] See https://pdfs.semanticscholar.org/b4ac/17c649bc8dc4653ce6c114d4eeae3d6ed66f.pdf.