Hudson Institute

MAY 2020

The Executive's Guide to Quantum Cryptography: Security in a Post-Quantum World

BY ARTHUR HERMAN

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, **www.hudson.org**

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

We would like to acknowledge ID Quantique for their generous support.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

+1.202.974.2400
info@hudson.org
www.hudson.org

Cover: Creative rendering of a circuit padlock in network space. (Getty Images)

Hudson Institute

APRIL 2020

The Executive's Guide to Quantum Cryptography: Security in a Post-Quantum World

BY ARTHUR HERMAN

INTRODUCTION

CEOs and CIOs are accountable for protecting their company, their investors, their customers, and their employees from cyber-threats that endanger the company's private information and financial well-being.

Today the most serious of these is the threat to the integrity and confidentiality of data and information that are vital to a company's success. This does not come only from current cyber-attacks and hackers, which according to 2018 estimates by cyber-research firm Accenture, cost organizations globally an average of $13 million a year. It also includes the future threat posed by quantum computers, which will render public-key cryptographic systems helpless and enable competitors, adversaries, and possibly foreign entities to steal a company's most precious information without leaving a trace behind.

In October 2018, global research and advisory firm Gartner elevated the quantum computer threat to the top of its list of digital disruptions for which CIOs may not be prepared. It noted that "quantum computers have the potential to run massive amounts of calculations in parallel in seconds," including cracking the complicated math problems on which today's encryption systems depend.

At the same time, considerable confusion exists, even among experts, about the true potential of the quantum threat, the timeline for its advent, and the steps needed to protect a company's future.

This guidebook answers key questions about how quantum technology itself, in the form of quantum random-number generators (QRNG) and quantum-key distribution (QKD), can provide secure solutions for addressing the quantum computer threat.

After explaining how QRNG and QKD work, the guidebook recommends that executives combine these quantum cryptographic solutions with other software-based, quantum-resistant applications that can deter future quantum computer attacks.

Finally, the guide shows how quantum science will determine the future of communication technology by making it safe, secure, and ready for the twenty-first century.

Business management guru Peter Drucker once posed the question, "Will the corporation survive?" One thing is certain: no corporation, agency, or enterprise can survive if its most important data and information are constantly and systematically vulnerable to attack and/or theft.

Employees, shareholders, investors, and the general public need to trust that company executives have made every effort to secure that data and information, now and in the future.

It is to help senior executives fulfill that trust and ensure peace of mind that this guidebook was written.

I. WHAT IS QUANTUM SUPREMACY?

On October 23, 2019, Google published a paper in the journal Nature entitled “Quantum Supremacy Using a Programmable Superconducting Processor.” The tech giant announced its achievement of a much-vaunted goal: quantum supremacy.

That means that a quantum computer solved in a matter of minutes a problem that would take even the fastest supercomputer ten thousand years.

This milestone, which some prefer to call quantum advantage, was a major stepping-stone to the quantum computers of the future, which may become serious threats to encryption systems. In fact, Google’s CEO later predicted that the end of encryption could come in as little as five years.

II. HOW DO QUANTUM COMPUTERS POSE A THREAT TO TODAY'S ENCRYPTION?

What is threatening is that today's cryptography largely depends on supposedly hard math problems, based on the factorization of large numbers into their prime factors.* Why "supposedly"? Because before 1994, factoring was truly thought to be a hard math problem, but that year, Peter Shor invented an algorithm (now named after him) that factorizes large numbers easily. The only caveat is that this algorithm must run on a quantum computer, meaning that the very problem at the heart of cryptography will be solved by a large-scale quantum computer. This was the first instance where the astonishing computing power of a quantum computer was shown to have practical applications.

Shor's discovery changed our perception of the quantum computer and started the rush towards the physical realization of a quantum computer and the discovery of new algorithms that will exploit their power.

* How does this work? A prime number is an integer, which cannot be factorized into smaller ones. For example, 23 is a prime number; 21 is not, even though its prime factors are 3 and 7. It is easy to multiply numbers, but much harder to invert this operation and find the prime factors, especially for large enough numbers. This difference, and the resulting difficulty in factorizing those large numbers, lies at the heart of current public-key cryptography.

III. HOW SOON WILL THE THREAT BECOME A REALITY?

Estimates vary, but growing expert consensus says a large-scale quantum computer will be available within the next decade. In fact, Google's CEO, Sundar Pichai, was quoted as predicting at the World Economic Forum in Davos that quantum computers will spell the end of standard encryption within five to ten years.[1]

Either way, time is short for developing a quantum-safe response. This is particularly true if you have data that needs to remain confidential for years to come. Records of financial transactions and medical data, for example, need to be kept secure for decades, meaning that the systems storing them should be reinforced now against future advances. There is also a serious risk that data transmitted over open channels, such as the internet, could be harvested today and stored until it could eventually be decrypted by a quantum computer.

Is the quantum threat real? Cybersecurity experts certainly think so. A 2019 DigiCert survey of IT directors, IT security managers, and IT "generalists" working for some 400 firms in the United States, Europe, and Japan found that 55 percent saw the quantum computing threat as "somewhat to extremely large" today, and 71 percent as "somewhat to extremely large" in the future. Surprisingly, only 35 percent have any budget today for making their systems quantum-safe, and only 59 percent anticipated a "large to somewhat large" budget sometime in the future.[2]

[1] Hannah Boland, "Quantum Computing Could End Encryption within Five Years, says Google Boss, Telegraph, January 22, 2020, https://www.telegraph.co.uk/technology/2020/01/22/googles-sundar-pichai-quantum-computing-could-end-encryption/.

[2] DigiCert, Quantum's Promise and Peril:2019 DigiCert Post-Quantum Crypto Survey, https://www.digicert.com/resources/industry-report/2019-Post-Quantum-Crypto-Survey.pdf.

The bottom line is, the risk is well understood today. Unfortunately, the commitment to offset that risk is still inadequate.

IV. WHAT ARE MY OPTIONS TO PROTECT MY DATA AND NETWORKS?

One option is to use post-quantum cryptography. Researchers are working on methods to improve the security of software-based signatures and key-exchange methods using post-quantum cryptography—methods that should continue to be effective after quantum computers are powerful enough to break existing public -key cryptosystems. A number of products that mix different algorithms, known as hybrids, are already in operation. The National Institute of Standards and Technology (NIST) is working on a set of standards for quantum-resistant algorithms (QRA), which it hopes to complete by 2024. The real test will come when quantum computers arrive on the scene.

However, post-quantum cryptography rests on the unprovable assumption that these new algorithms are difficult to reverse. But the question that remains is, difficult for whom? How do we know that a solution to these problems has not been discovered, even if it is unpublished? And if this solution does not exist yet, how do we know that it will not be found in the future, once more and more clever computer scientists develop the next generations of quantum computers? The answer is simple: we do not.

There are, however, tools that use quantum technology that can already improve security: quantum random number generators (QRNG) and quantum-key distribution (QKD).

V. HOW CAN THE RANDOMNESS OF QUANTUM RANDOM NUMBER GENERATION HELP ENCRYPT DATA?

A random number is a number generated by a process whose outcome is completely unpredictable and which cannot be reliably reproduced. Random numbers are required in many applications, from cryptosystems to gaming. In fact, almost every cryptographic process starts with the generation of random numbers. Poor randomness has been linked to several significant faulty implementations and hacks.

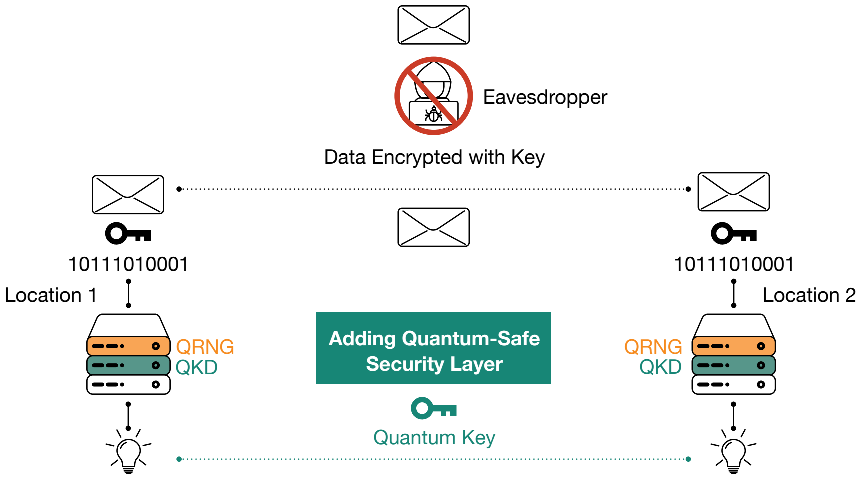
Quantum physics is fundamentally random, unlike classical physics, which is deterministic. Quantum Random Number Generators, or QRNGs, integrate the randomness of quantum physics to generate truly random numbers for encrypting messages and for other cryptographic applications.

The Swiss company ID Quantique, for example, is manufacturing a range of quantum-generated random communication products known as Quantis. An important feature of these products is that they are already certified by national bodies such as Germany's BSI (the counterpart of NIST), which delivered the AIS31 certification for some Quantis systems. A new QRNG chip, with reduced form factor and power consumption, is AEC-Q100 certified and is compliant with the NIST 800-90A/B/C standard. These certifications are often required by end customers for real-world implementations.

An Australian company, Quintessence Labs, has a QRNG-based Qstream product suite that is being used to secure billions of highly sensitive legal documents in the cloud. Many other start-up companies are also active in this field.

Improving randomness generation with QRNGs, which can easily be added to current security solutions, is the first way to improve security today. The second solution, QKD, represents a new way to distribute these random numbers and generate secure keys between different locations.

Figure 1: Adding Quantum-safe Security Layers with QRNG and QKD



SOURCE: ID QUANTIQUE (MARCH 2020), HTTP://WWW.IDQUANTIQUE.COM/

VI. WHAT IS QUANTUM-KEY DISTRIBUTION?

Quantum-Key Distribution, or QKD, can offer long-term security against a future quantum computer attack. That is because it rests on fundamental physical principles rather than specific mathematical assumptions. Ultimately, provable secure communication boils down to distribution of a unique secret key, used to encrypt a message, which like QRNGs is completely random and used only once. QKD can establish such a key remotely between two distinct parties, and it is essentially immune to hacking by both conventional hackers and quantum computers. This is because if anyone tries to tamper with the data, the two QKD parties will immediately know.

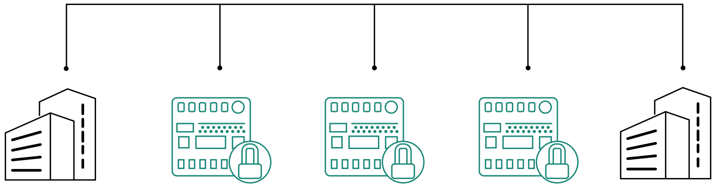
In short, quantum cryptography is the only known method for transmitting a secret key over long distances that is provably secure in accordance with the fundamental properties of quantum physics.

This exchange of encryption keys via QKD will eventually become the cornerstone of network security for all high-value data, but it is also a way to protect high-value data today.

VII. HOW DO I IMPLEMENT QKD SOLUTIONS TO PROTECT MY DATA?

Current technological breakthroughs are pushing the distance over which quantum signals can be sent. Trials using laboratory-grade hardware and "dark fibers"—optical fibers laid by telecommunications companies but lying unused—have sent quantum signals up to four hundred kilometers. Practical systems that can be easily deployed over an existing infrastructure are currently limited to distances of about one hundred kilometers. A scalable architecture that includes trusted nodes to link successive QKD systems can extend the practical range of this technology and allow keys to be securely shared over a wide-ranging network, making large-scale implementation possible and practical. Some are doing this now. Korean ICT giant SK Telecom is applying QRNGs to the subscriber authentication center of its 5G network. It is already adding the ID Quantique QKD technology to the Seoul-Daejeon section of its LTE and 5G networks to prevent hacking and eavesdropping. Its plan is to strengthen security for 5G and LTE data transmission and reception over the whole network, to provide an extra value to their customers using their network by mitigating the risk of network intrusion and exploitation of user's data. Implementing these measures into your network now protects against the future costs of rebuilding security and repairing

Figure 2: QKD in a 5G Network



SOURCE: ID QUANTIQUE (MARCH 2020), HTTP://WWW.IDQUANTIQUE.COM/

customer reputation in a post-quantum world.

An American company, Quantum Xchange, is using QKD to provide point-to-multipoint transmissions for financial markets on Wall Street.

We must acknowledge that the United States is not alone in this field and is probably not even the leader today. China has already built a QKD network running for two thousand kilometers between Shanghai and Beijing and is working on an extension running eleven thousand kilometers that will cover most of eastern China. They are also actively deploying satellites that use QKD technology in space.

Europe is also active in this arena and is currently planning for a quantum communication infrastructure that should encompass most of the EU.

The bottom line is that QKD offers the ultimate solution against quantum computer attack in the future, while QRNG provides a provable and guaranteed confidentiality link that is available now.

VIII. WHAT IS THE FUTURE OF QKD?

As QKD technology grows and matures, it will form the basis of a global quantum communications network that will include space-based networks. A global network of spacecraft and ground stations, distributing secret encryption keys by means of quantum technology, will be able to meet emerging and long-term threats to data security.

This is not science fiction. On September 29, 2017, the first intercontinental video conference using quantum cryptography took place between the presidents of the Austrian and Chinese academies of science. The cryptographic key pair used by the stations in Vienna and Beijing had been generated using an optical QKD payload aboard the Chinese satellite Micius.

That event gives us all a glimpse of the quantum future, especially quantum communications. But we can expect more. The development of quantum repeaters will transform a QKD network, which only transports keys, to a full quantum internet, which will link clusters of quantum computers working together to perform computations we cannot even think about today. In short, there is a brave new world taking shape thanks to quantum technology, and not all of it is frightening or dangerous.

CONCLUSION: WHAT DO I NEED TO KNOW TO MAKE A READINESS PLAN?

As noted earlier, information is a critical asset for today's businesses, which must protect proprietary information as zealously as defense agencies guard classified information. Therefore, any CEO or CIO who needs to know where that protection should go in the future, and how, must understand the current state of cyber and other IT security protections.

It is vital to develop a checklist for a readiness or quantum risk-assessment plan, which should include the following:

First, find out how data and other information is stored, and who has access to the most critical information.

Every CEO and CIO needs to remember: data breaches occur because someone has deemed the targeted information to be critical. If executives do not know what information is critical in their company or agency, it is important for them to find out.

Second, catalog where cryptography is used in your existing networks and data systems and determine how long current cyber-protections will last.

Even if current protections have a long shelf life, in less than a decade no networks or data systems will be safe unless steps are taken to render them quantum-secure. On the other hand, if protections for important platforms have expired or are about to expire, this offers an opportunity to implement a security reset by incorporating hybrid tools and other solutions that can be progressively upgraded and made future-proof, including quantum cryptography.

Third, decide which critical data are your company's or agency's most important assets, and determine whether they have the best possible protection today as well as tomorrow.

The general rule for all cybersecurity solutions is that the "crown jewels"—

your company's or agency's data and systems—deserve the best and most immediate protection. That means they deserve quantum-safe solutions that can be sustained over time, especially over the anticipated time line for the advent of quantum computers. This is where QKD should be able to help, starting today.

Finally, ask whether the vendors and suppliers with whom you share data and information have quantum-safe encryption, and if they do not, find out when they will begin quantum-proofing their critical systems.

No company is an island unto itself. This means no amount of quantum-proofing at home will protect data and information shared with companies or entities that are themselves vulnerable to quantum attack. Opening this dialogue with vendors and suppliers will alert them to the need to quantum-proof their own data and networks and offer them the opportunity to look at the latest quantum-safe technologies available today, including quantum cryptography solutions.

Check the following websites for additional information:

https://www.idquantique.com

https://www.hudson.org/policycenters/36-quantum-alliance-initiative https://csrc.nist.gov/projects/post-quantum-cryptography

https://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

https://quantumcomputingreport.com/

https://www.abiresearch.com/market-research/product/1028952-cryptography-in-the-quantum-computing-era/

Hudson Institute
1201 Pennsylvania Avenue, Fourth Floor, Washington, D.C. 20004
+1.202.974.2400 www.hudson.org