Quantum computing risks and opportunities: how to become post-quantum ready

Augustinus Mohn PhD CISM
is a manager at KPMG Cyber & Privacy.

Marijn Pronk M.Int.
is a consultant at KPMG Cyber & Privacy.

Ir. Thijs Timmerman MBA CISM CRISC
is a partner at KPMG Cyber & Privacy.

The advance of quantum computing brings new risks and opportunities that decision-makers need to consider to make their organizations "quantum ready". Traditional cybersecurity measures such as cryptographic keys or encryption of sensitive information need to be re-evaluated to identify potential weaknesses. In addition to taking practical steps today, it is important to build the right strategy for the long term, bringing together today's actions with tomorrow's risk landscape.

INTRODUCTION

Quantum computing is an upcoming technology that will have major implications for society and organizations of any sector and size. It brings new opportunities that can be leveraged as well as new risks that need to be managed. One area that is expected to be especially affected by quantum computers is cryptography, i.e. the encryption of information through algorithms. The recent steep development of quantum computing capabilities in lab environments is only a "warming-up" phase before the technology will hit the market at a larger scale. This means that decision makers should start taking the right steps now to prepare their organization for the future.

Organizations should future-proof their cryptographic data protection controls ([Baum22]) and strengthen their security of access control measures in both the IT and Operational Technology (OT) domain. They should also re-think how they can leverage quantum technology to improve their service offering. To provide practical advice, this article elaborates on the key trends and implications of quantum computing in the cybersecurity area of cryptography, both on the risk and opportunity side, equipping decision makers with the right context and next steps to take.

QUANTUM COMPUTING SIGNIFICANTLY IMPROVES CALCULATION SPEED

Quantum computers are computers based on quantum technology. They make use of the mechanics of particles at a sub-atomic level and have the potential to outperform traditional computers by miles. Although a quantum computer has outperformed a traditional (albeit very powerful) computer for the first time only recently, in 2019 ([Oliv19]), the race for ever better quantum computers is picking up fast. Tech giants such as IBM ([IBM23]), Microsoft ([Micr23]), Honeywell ([Hone23]), Google ([Goog23]) and Intel ([Inte23]) are heavily investing in quantum technology, working on ever more efficient and scalable solutions. For example, IBM's first quantum computing system produced in 1998 had 2-qubits (quantum-bits ([IBMQ23])). In 2022, IBM introduced their 433-qubit quantum computer Osprey. For reference: the break-through in 2019 was achieved by a quantum computer with only 53 qubits ([Arut19]).

While the number of qubits in itself is not sufficient as a performance indicator ([Smit22]), the exponential growth in complexity demonstrates the potential computing power that quantum computers may hold in the future ([Feld19]). Proof of concepts from the lab give a promising outlook towards the potential capabilities of mature quantum technology. Once mature, quantum technology will significantly speed up calculations, yielding advantages in e.g. data lake analysis, modelling of industrial processes or optimization of network traffic flows. Additionally, its computing power will significantly reduce the time required to break a cryptographic key based on large number factorization – a tough problem today that will become relatively easy to crack in the future. With their advanced computing power, quantum computers will pose a threat to widely used cryptographic solutions like RSA ([MIT19]).

> Although a quantum computer may be necessary for breaking an encryption in the future, that same computer is not needed for acquiring the encrypted data today

ADDRESSING THE RISKS AND OPPORTUNITIES OF QUANTUM COMPUTING

Understanding how to work today to be prepared for tomorrow

With the advancement of the Internet of Things (IoT), i.e. internet-connected devices in both domestic and industrial settings, the world is increasingly interconnected. This implies two things: an exponentially growing pool of data, and increasing dependencies between digital and traditional/non-digital technology. While an exponentially growing pool of data can add true value to organizations and individuals, it also increases the exposure to security risks. Sensitive personal data, business critical knowledge stored in a digital format and digital systems in general, contain a pool of information that needs to be protected. Similarly, access to digital systems that are used to manage non-digital technology (e.g. an electricity grid) needs to be controlled in a way that prevents malicious actors from abusing those systems, with potentially drastic consequences.

Traditional IT security measures have matured to a level where they can reliably act against traditional cybersecurity threats – for example by encrypting data with long and complex digital keys that would take a traditional computer many years to decrypt. A prominent capability of quantum computing is to eventually be able to decrypt – by today's standards – securely encrypted information. Hence, a sufficiently advanced quantum computer could easily break traditional security measures (within seconds to minutes and hours – compared to the millions or even billions of years it would take a traditional computer).

Although a quantum computer may be necessary for breaking an encryption in the future, that same computer is not needed for acquiring the encrypted data today. Malicious actors can intercept a data flow (data harvesting), store it, and keep the data until quantum technology is ready to break the encryption (a problem also known as "harvest now – decrypt later").

Data loss can happen through a variety of reasons, such as human mistakes and social engineering. Therefore, implementing security measures to prevent data loss today are an important step in becoming post-quantum secure in the future.

Identifying key risk areas

What we should consider today is what kind of data is valuable to an adversary. The data should have long-term value in order to retain its benefit for the hacker in the future when quantum computers are available. Think about data to protect confidentiality, availability or integrity for a period of time to prevent significant consequences if decrypted or otherwise compromised down the line.

For a post-quantum risk assessment, it is therefore necessary to identify types of electronic data that contain sensitive or critical information for an organization and require special protection. As a next step, security measures should be identified and implemented to prevent that the data in question is stolen or leaked – through raising awareness within the organization and ensuring that data is shared only on a need-to-know basis.

Additionally, organizations should consider the risks quantum computers pose to security, not only of traditional IT, but also internet-connected Operational Technology (OT) or the so-called Internet of Things (IoT). In case access to the control of OT is compromised, attackers may take over devices and control them for their purposes. At a small scale, this can mean intrusion of privacy through e.g. home cameras connected to the internet. On a larger scale, it can mean the disruption of critical infrastructure networks (electricity grids, nuclear facilities, water management and many more). Individuals as well as governments and businesses need to prepare for these eventualities.

Any good security strategy does not wait until an issue arises, but prepares for the future to provide long-term value

Building the right strategy and mitigating (future) risks

Implementing new security measures – e.g. security awareness campaigns on how to handle sensitive data – takes effort and time. So in addition to taking practical steps today, it is important to build the right strategy for the long term, bringing together today's actions with tomorrow's risk landscape. Any good security strategy does not wait until an issue arises, but prepares for the future to provide long-term value. It is important to understand today's risks (e.g. data leakage), how they relate to future risks (e.g. the decryption of leaked data through quantum computers), and what can be done today to reduce the overall risk profile in the future. The Dutch Ministry of Defense has included quantum computing in their 5-year research and technology agenda (2021-2025) to start understanding its impact on society ([MinD20]). Organizations should do the same to stay ahead of malicious actors.

Apart from traditional security actions, such as awareness measures or limitation of data access on the need-to-know principle, it is equally important to identify and consider embedding future-proof security measures. For example, there are cryptographic solutions available today that are likely to withstand even the most powerful quantum computers ([NIST22]). Migrating from current encryption standards to quantum resistant schemes should therefore be on the priority list of a post-quantum security strategy. With this in mind, it is not surprising that the US government, for example, is trying to pass laws that will mandate government

agencies to use Post Quantum Cryptography (PQC) algorithms for public keys. The execution of these plans can differ in implementation strategies (e.g. hybrid use of PQC and standard encryption), and, as is the case with every cyber implementation strategy, these choices will be dependent on a trade-off between security, performance (especially reach) and costs.

The Dutch National Security Agency AIVD has recently published the Post Quantum Crypto Migration Handbook, established in collaboration with TNO and CWI and edited by various representatives from industry, including KPMG ([MBZK23]), which provides guidance on such a strategy. Building on the directions of the Handbook, we recommend a four-step approach (see Figure 1): (1) identify which security measures are currently implemented at your organization, (2) assess to what extent those are quantum ready, (3) perform a risk assessment by identifying if today's measures are sufficient to protect what is important for your organization (crown jewels, critical data, etc.) against quantum computing threats (incl. the "harvesting" of data by malicious actors today), and (4) plan and execute the modification of security measures to post-quantum proof solutions.

Figure 1. A four-step approach to becoming post-quantum ready.

Source: KPMG: Security Risks of Quantum Computing, 2020.

OPPORTUNITIES

While organizations should definitely think about the risks that quantum computing poses, it is important to note that accelerated technological advancement in quantum computing also offers a lot of opportunities for business and research. For example, quantum computing as a service is already gaining traction in the form of cloud services ([Paut21]). A traditional computer sends a command to a quantum computer hosted on the cloud, where it performs the necessary computations on high speeds and sends the processed data back in "classical" binary form. These advances make quantum computing power accessible to a broader range of organizations and can speed up processes, without the need for a quantum computer.

These opportunities might be very valuable to organizations that need high computational capabilities. It is important, however, to take the envisioned commercial applicability with a grain of salt. Even though the quantum promises are that they will help businesses to solve computational problems that they cannot solve themselves with traditional computers, most use cases are highly hypothetical and experimental ([McKi21]). On top of that, there are still sizable margins of error that have to be applied to calculations made by quantum computing. Fluctuations in temperature, electromagnetic fields, or mechanical vibrations can alter the process within quantum computers and impact the reliability of their calculations ([Broo19]).

CONCLUSION: PROVIDE LONG-TERM SECURITY TO YOUR ORGANIZATION AND CLIENTS

Naturally, it will depend on the resources, nature and needs of your organization how you decide to adopt practical and viable countermeasures to threats posed by quantum computing. A risk-based, tailor-made approach to an organization's specific use-case seems to be the most viable option at this point. Large-scale deployment of solutions such as Quantum Key Distribution (QKD) might be cost effective in the short term, but will not be proven effective if it doesn't offer long-term and high-level solutions. Short-term risk reduction and long-term post-quantum security is the preferred two-tiered strategy to provide proper long-lasting security to your organization and its clients.

References

[Arut19] Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 2019*(574), 505–510. Retrieved from: https://www.nature.com/articles/s41586-019-1666-5

[Baum22] Baumgärtner, L. et al. (2022). When—and how—to prepare for post-quantum cryptography. *McKinsey Digital.* Retrieved from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

[Broo19] Brooks, M. (2019. Beyond quantum supremacy: the hunt for useful quantum computers. *Nature.* Retrieved from: https://www.nature.com/articles/d41586-019-02936-3

[Feld19] Feldman, S. (2019). 20 Years of Quantum Computing Growth. *Statista.* Retrieved from: https://www.statista.com/chart/17896/quantum-computing-developments/

[Goog23] Google (2023). *Explore the possibilities of quantum.* Retrieved from: https://quantumai.google/

[Hone23] Honeywell (2023). *Honeywell Quantum Solutions.* Retrieved from: https://www.honeywell.com/us/en/company/quantum

[IBM23] IBM (2023). *Highlights of the IBM Quantum Summit 2022.* Retrieved from: https://www.ibm.com/quantum

[IBMQ23] IBM Quantum (2023). *The qubit.* Retrieved from: https://quantum-computing.ibm.com/composer/docs/iqx/guide/the-qubit

[Inte23] Intel (2023). *Quantum Computing.* Retrieved from: https://www.intel.com/content/www/us/en/research/quantum-computing.html

[MBZK23] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2023). *Het PQC-migratie handboek.* Retrieved from: https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek

[McKi21] McKinsey & Company (2021). *Quantum computing: An emerging ecosystem and industry use cases.* Retrieved from: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf

[Micr23] Microsoft (2023). *Azure Quantum.* Retrieved from: https://azure.microsoft.com/en-us/solutions/quantum-computing/#quantum-impact

[MinD20] Ministerie van Defensie (2020). *Strategische Kennis- en Innovatieagenda (SKIA) 2021-2025.* Retrieved from: https://www.defensie.nl/downloads/publicaties/2020/11/25/strategische-kennis--en-innovatieagenda-2021-2025

[MIT19] MIT (2019). How a quantum computer could break 2048-bit RSA encryption in 8 hours. *MIT Technology Review.* Retrieved from: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

[NIST22] NIST (2022). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.* Retrieved from: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[Oliv19] Oliver, W. D. (2019). Quantum computing takes flight. *Nature.* Retrieved from: https://www.nature.com/articles/d41586-019-03173-4

[Paut21] Pautasso, L. et al. (2021). The current state of quantum computing: Between hype and revolution. *McKinsey Digital.* Retrieved from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/the-current-state-of-quantum-computing-between-hype-and-revolution

[Smit22] Smith-Goodson, P. et al. (2022). IBM Announces New 400+ Qubit Quantum Processor Plus Plans For A Quantum-Centric Supercomputer. *Forbes.* Retrieved from: https://www.forbes.com/sites/moorinsights/2022/11/09/ibm-announces-new-400-qubit-quantum-processor-plus-plans-for-a-quantum-centric-supercomputer/

About the authors

Augustinus Mohn PhD CISM is a manager at KPMG Cyber & Privacy. He obtained his PhD in strategic studies and international law at the University of Aberdeen, Scotland, in 2018. In addition to his role at KPMG, he is a project fellow at the World Economic Forum's Centre for the Fourth Industrial Revolution (C4IR).

Marijn Pronk M.Int. is a consultant at KPMG Cyber & Privacy. For the past years she has been studying emerging technologies and their risks and has provided capacity building consultancy on topics such as mis- and disinformation.

Ir. Thijs Timmerman MBA CISM CRISC is a partner at KPMG Cyber & Privacy. He supports clients in optimizing their security strategy, clarifying their risk posture, building of the business case for cyber investments, fulfilling improvement programs and conducting quality assurance activities. Thijs completed an MSc in Industrial and Applied Mathematics at Eindhoven University of Technology, with a focus on discrete mathematics and cryptographic applications.