Rethinking Cybersecurity in a Quantum World

pwc

Tomorrow's Cyber Security, Today

IRONCAP

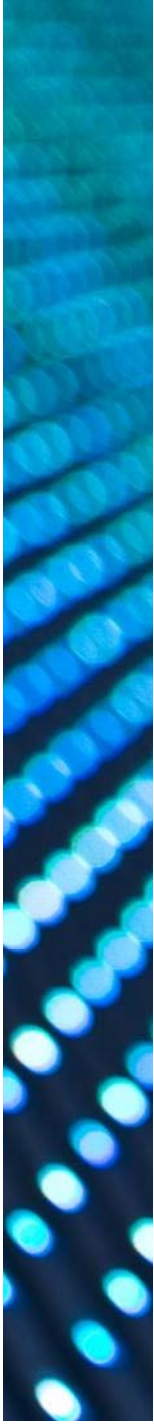
Table of Contents:

Quantum mechanics and computing, an odd pair?

Although quantum physics as a theory has existed since early in the last century, the idea of using quantum mechanics to fuel computing power was not an obvious idea – in fact, it was counterintuitive. Indeed, it is hard to imagine how quantum theory, fundamentally based on the language of probability, can possibly be related to computing.

It was not until 1982 that the idea of simulating a quantum mechanical system with a computer was introduced. This revolutionary idea was first shown in Richard Feynman's speech and accompanying paper "Simulating Physics with Computers" in 1982[1], where he explicitly discussed the construction of a machine that would operate on quantum mechanical principles. He was the first to coin the term quantum computer. With more attention on this subject, more ideas followed. The most notable was from David Deutsch[2], whose theory was regarded as the start of the epoch of quantum computing, when he showed that a universal quantum computer was in fact possible.

Ironically, what makes quantum computing unique is exactly this counterintuitive concept behind quantum information processing, i.e., uncertainty. Unlike classical computers, which are effectively pre-programmed calculators based on binary (i.e. bits that can equal 0 or 1), quantum bits (qubits) have some likelihood of being a 1 and some likelihood of being 0 at the same time. This revolutionary fuzzy logic of superposition, with 0 and 1 co-existing, provides a brand-new lever to turbo-charge computing power that is significantly faster at certain tasks (a million or more times) than today's classical computers. It is precisely this new-found computing power that makes quantum computers work in a completely different way from the computers of today.



[1] 1_00_QIC_Feynman.pdf (whu.edu.cn)

[2] deutsch85.dvi (daviddeutsch.org.uk)

What does the future hold?

Imagine we venture into an entirely new realm of computation in the quantum era, using new applications that we cannot possibly foresee. The transformation is similar to how classical computers revolutionised our world in just a few decades, only this time quantum's extraordinary capabilities not only make the world move faster, but will reshape our world by solving the unsolvable.

Quantum computers are not intended to replace classical computers. For instance, quantum computers will not support our email and they are probably too expensive to be used for word processing. A practical way to imagine a likely future is having quantum processors working alongside our classical computers to focus on specific problems where quantum computers outperform. Such problems typically involve complex mathematical issues like optimisation, where further increases in classical computational capability just won't work. To draw an analogy, bicycles used to be the main form of transport before motor cars were invented. The creation of motor cars brought revolutionary capabilities and a transformative experience to transportation by achieving the previously unachievable. However, they have not fully replaced bicycles, which continue to co-exist alongside motor cars. But it was obvious that we had to rethink how to protect bikers from being runover by motor cars. Likewise, quantum computers are best described as doing something very specific, very fast, and very efficiently. Quantum computing will create new potentials and unimaginable opportunities, but will also give rise to new cybersecurity risks with its ability to crack the cryptographic systems in use today. Like bicycles, classical computers will be here for good. We need to rethink how to protect our data from this new breed of computing power so that both classical and quantum computers can co-exist peacefully.

Overview of cryptography

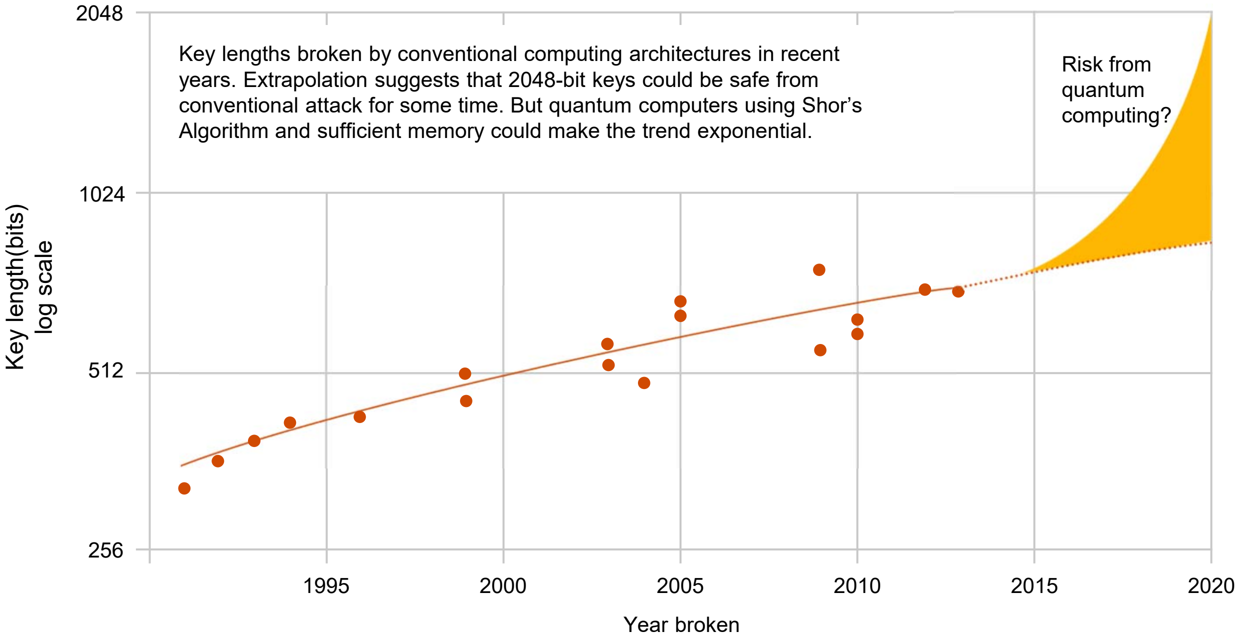
Cryptography is based on two-way functions, whereby it is easy to solve in one direction but is nearly impossible to solve in the reverse direction. Depending on the one-way function, classical computers need to spend hundreds of years to solve cryptographic functions in reverse. Data encrypted will therefore remain safe against hacking from the strongest classical super computers due to the inherited limitation of their binary operations.

However, scientists have demonstrated quantum computers' ability to crack factor-based cryptographic systems in a fraction of the time it would take a classical computer. The cryptographic systems at risk from attack by a quantum computer are those based on factorisation. This type of technology is used extensively on the Internet, for example, in key exchange. Over the last two decades, the risk was largely regarded as theoretical because quantum computers were the stuff of fiction. However, this perception has changed drastically in the last few years.

The quantum threat is real

The race to "quantum supremacy" (a term to describe the point where quantum computers can do things that classical computers can't) has intensified in recent years, with billions of dollars pouring into quantum R&D from global tech firms. National policies and strategies to build quantum technology R&D capabilities are well under way. Major geopolitical players have already developed their quantum initiatives, with an increasing number of countries joining the race. Indeed, this will significantly compress quantum computer development – repeating the growth rate of its distant relative, the classical computer, in an even more aggressive fashion. While classical computers armed with powerful hardware can break certain RSA encryption with smaller key length, RSA 1024 and beyond is believed to be unrealistic for today's most powerful supercomputers to break. According to a study by the European Telecommunications Standards Institute (ESTI) as indicated in the below diagram, RSA 1024-bit keys are considered as safe from adversaries using classical computers.

Figure 1 – Breaks in the RSA cryptosystem in recent years using conventional computation



Source: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

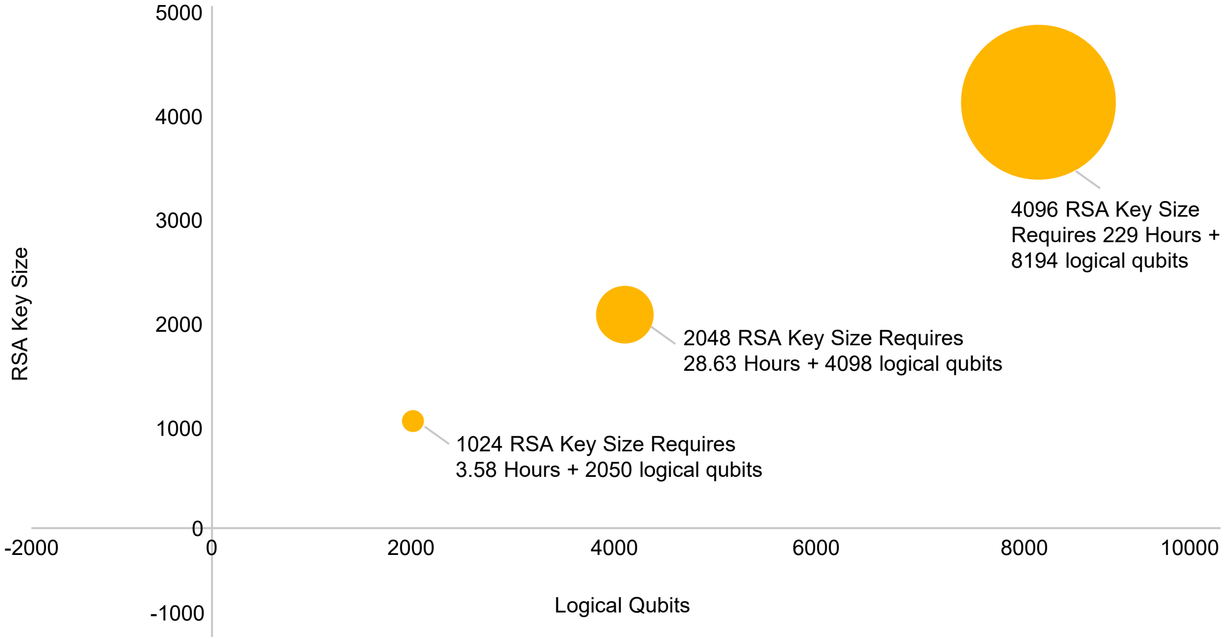
It is anticipated that quantum computers could break widely used factor-based public-key cryptography schemes, such as RSA 1024 and ECC, or weaken standardised symmetric encryption algorithms. When a "working quantum computer" is available (i.e. one having a sufficient number of Qubits that is resistant to quantum noise and other quantum-decoherence), and economically viable and practically operational, reliance on RSA 2048 may not be sustainable.

[3] Report on Post-Quantum Cryptography (nist.gov)

The quantum threat is real

While there are debates over when such time will arrive, one should note that not all quantum developments are allowed or are intended to be made public. Some experts have even stated that Q-Day has already arrived. It is therefore down to us to be fully prepared, because our stakeholders, who entrust us with their data and digital assets, expect no less in any situation: full protection and diligent security against any adversary, known or unknown, at all times!

Figure 2 – RSA Key Size vs Qubits required to break a code



Source: Quantum Computing: Progress & Prospects (2019) Emily Grumbling and Mark Horowitz

Fortunately, non-factor-based cryptosystems have long existed, with a good track record of resilience. We need to identify those cryptosystems that are based on mathematical building blocks other than factor-based, and which incorporate mathematical operations that are robust against attacks from quantum computers.

There need to be sufficient and convincing proof to conclude in a crypto-analysis that the right Post-Quantum Cryptography (PQC) is safe for both quantum and classical computers, and that it can interoperate with existing communication protocols and networks. At the same time it must be able to protect the future state, where both classical computers and quantum computers will co-exist. Such initiatives have already started.

[3] Report on Post-Quantum Cryptography (nist.gov)

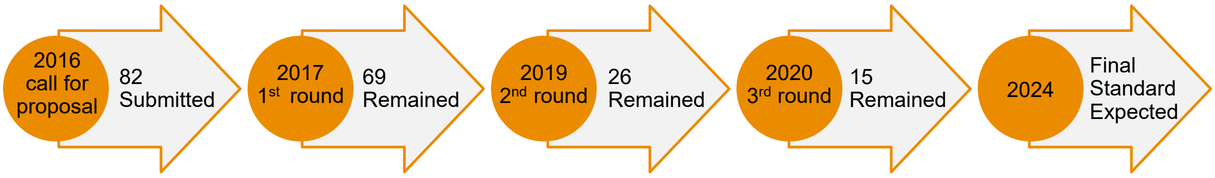
In search of Post-Quantum Cryptography (PQC)

In 2017, the National Institute of Standards and Technology (NIST) in the US started selecting one or more public-key cryptographic algorithms[4] for use on key facilities through a public competition. The intention is to find the algorithms that are "capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers."

NIST was upfront in indicating that only a handful of "families of cryptographic primitives" are likely to fit:

- code-based cryptography
- lattice-based cryptography
- multivariate polynomial cryptography
- hash-based signatures
- other, including isogeny-based

A total of 82 initial proposals were received. After nearly four years of stringent review and assessment, NIST announced the 3rd Round[5] candidates in July 2020. It is generally anticipated that NIST will announce the final standard by 2024:



Source: NISTIR 8309 Status Report on Second Round of the NIST Post-Quantum Cryptography Standardization Process

[4] Post-Quantum Cryptography | CSRC (nist.gov)

[5] Status Report on the Second Round of the NIST PQC Standardization Process

NIST’s 3rd round results

A total of fifteen candidates remained in the 3rd Round. Out of these, NIST selected seven final candidates as “the most promising to fit the majority of use cases and most likely to be ready for standardisation soon after the end of the third round”. The other six candidates are regarded by NIST as “potential candidates for future standardisation, most likely after another round of evaluation”[6] [7].

It is NIST’s intention to select only one scheme from each “family” for standardization. Interestingly, the 3rd Round results have already produced “sure-winners” in some of the “in-family” race, as highlighted in the table below. For example, Classic McEliece Goppa code is a clear winner for public-key encryption, since it is the only candidate left in the Code-based cryptography family. However, more time is needed to identify the right candidate from the Lattice-based cryptographic family.

Cryptography “family”	**Final Candidates (7)**		**Alternate Candidates (8)**		**Total**
	Public-key Encryption/KEM	Digital Signature	Public-key Encryption/KEM	Digital Signature	
Code-based	1	0	2	0	3
Lattice-based	3	2	2	0	7
Hash-based	0	0	0	1	1
Multivariate-based	0	1	0	1	2
Others (Isogenies &symmetric crypto)	0	0	1	1	2
Total	**4**	**3**	**5**	**3**	**15**

[6] PQC Third Round Candidate Announcement | CSRC (nist.gov)

[7] NISTIR 8309, PQC Project Second Round Report | CSRC

Good progress, but will it be ready in time?

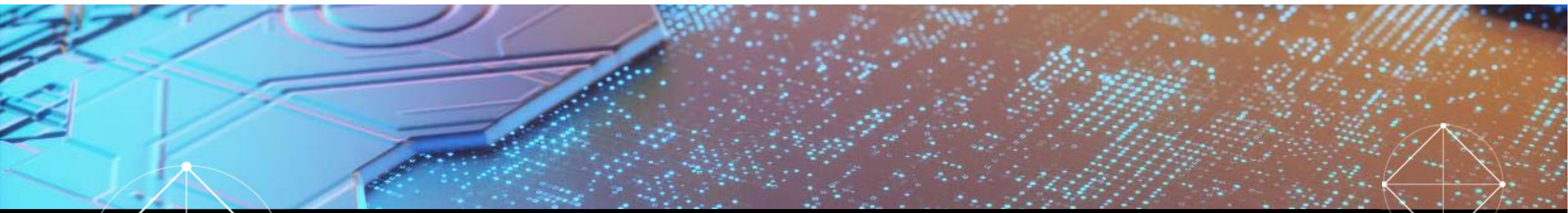
Will NIST’s targeted announcement time frame for PQC keep up with the acceleration in quantum computing? If these developments outstrip cryptographic key technology, data suddenly becomes compromised. To make it worse, cyber criminals are already capable of intercepting encrypted and strategically important confidential information and storing it. Encrypted data that needs to be kept confidential for a long period of time is particularly vulnerable. Attackers could gain access to the ciphertext and store it. As quantum computing develops and becomes commercially viable, they will be able to use the technology to break the encryption that is protecting the stolen data.

More time is needed for digital change and readiness, even if standards are available by 2024. A rapid transition to new information security technologies, tools and methodologies is simply unrealistic because it requires significant infrastructural, cultural and procedural change, as well as funding. Transformation on this scale takes time, as indicated by the timeline below based on NIST’s own projection. With critical activities adding to the time window, it is much narrower than it first appears.

NIST finalises selection		Standards & guidelines		Implementation of standards under normal circumstances		Implementation of Post Quantum Cryptography standards
1/2 years*	+	“proceed expeditiously”*	+	5 to 15 years*	+	Decades*
2022/23		2024/25		2030 Very Optimistic 2040 Optimistic		> 2040 Realistic

Source: NIST’s April 28 2021 publication, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms | NIST

* “Algorithm selection is expected to be completed in the next year or two, and work on standards and implementation guidelines will proceed expeditiously….in the best case, 5 to 15 or more years will elapse…before a full implementation of those standards is completed. Unfortunately, the implementation of post-quantum public-key standards is likely to be more problematic…it may be decades before the community replaces most of the vulnerable public-key systems currently in use.”



Embrace change and act now

Rapid technological progress in recent years has created a new business reality: the digital economy. Companies today interact with each other, their partners, customers and even regulators via digital channels that send and receive data. For a company to be trusted digitally, it is essential to ensure that sensitive data and information are secure. Encryption technology is a critical component of today's information security infrastructure that protects data transmitted via the Internet.

Quantum computer development is progressing at a faster pace than ever expected. Alongside the successful initiatives of IBM and Google, research teams from Harvard and the University of Maryland have almost simultaneously implemented two new 51- and 53-qubit quantum computing systems. In Dec 2020, a team of Chinese physicists developed a prototype quantum computer based on a new photonic design and, in May 2021, two technology companies in the US announced plans to construct a full-scale quantum computer with over 1 million qubits.

With these technological advances, it is likely that the eagerly-awaited Q-Day will arrive earlier than expected. For this reason, the Quantum threat is an issue that business leaders should address at the earliest opportunity. It is also important to recognise that rapid transition to new information security technologies, tools and methodologies is unrealistic because much of our infrastructure and network systems today are inter-connected, often on a global level. Therefore, responding to the Quantum threat will require significant infrastructural, cultural and procedural change, as well as funding on a scale not seen since the Y2K threat.

To address the Quantum challenge, PwC China has formulated a methodology incorporating global information security best practices and the knowledge and experience of subject matter specialists. Our approach comprises six key steps:

Assessment

The Quantum Threat will impact entities differently. It is therefore necessary to first ascertain the technologies and infrastructure of the entity, as well as the data assets that need to be protected.

Analysis

The business impact of the Quantum Threat is determined by analysing specific attributes relating to the entity's infrastructure and its data assets.

Strategy

Select and determine the actions to enhance the cryptographic tools, taking into consideration business impact, cost efficiency and performance. Develop a strategic plan, addressing risk prioritization, implementation approach, and cost estimation.

Pilot

Given the technological complexity, and the need to address components outside of the organisation (e.g. business partners and service providers), it is essential to start with a pilot project. Based on the pilot results, the proposed solutions and action plan can be modified and tailored to better fit the entity's needs.

Rollout

This includes rolling out a successful solution (as tested and refined during the pilot) across the entire entity to protect critical data and information.

Continuous Update

Enhancing data protection systems with quantum-safe technologies is a continuous process, given the evolving technological and potential regulatory landscape. It is important to be informed of the latest developments in the field and to update the entity's action plan accordingly, ideally every six months.

The accelerating pace of digitalisation presents an opportunity for business leaders to tackle the quantum threat as part of their digital transformation strategy. Recognising every entity is unique in its own way, PwC China will work alongside business and system owners to develop an optimal solution for your specific needs and requirements. Our solutions include exclusive use of innovative products to ensure uninterrupted cryptographic security as we transition from the pre-quantum to the post-quantum world. Our agile approach is designed to cater for the fluidity of emerging PQC standards and certification requirements, ensuring your business can land solidly on the future quantum soil!

[8] This Is Why Quantum Computing Is More Dangerous Than You Realize

[9] Physicists in China challenge Google's 'quantum advantage': Photon-based quantum computer does a calculation that ordinary computers might never be able to do

[10] PsiQuantum and GLOBALFOUNDRIES to Build the World's First Full-scale Quantum Computer

Contact us

William Gee
Partner, Digitalisation Office
PwC China
william.gee@hk.pwc.com

Andrew Cheung
President and CEO
01 Communique
andrew.cheung@01com.com

Samuel Sinn
Partner, Cybersecurity and Privacy
PwC China
samuel.sinn@cn.pwc.com

Sergey Strakhov
CTO
01 Communique
strakhov@01com.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.