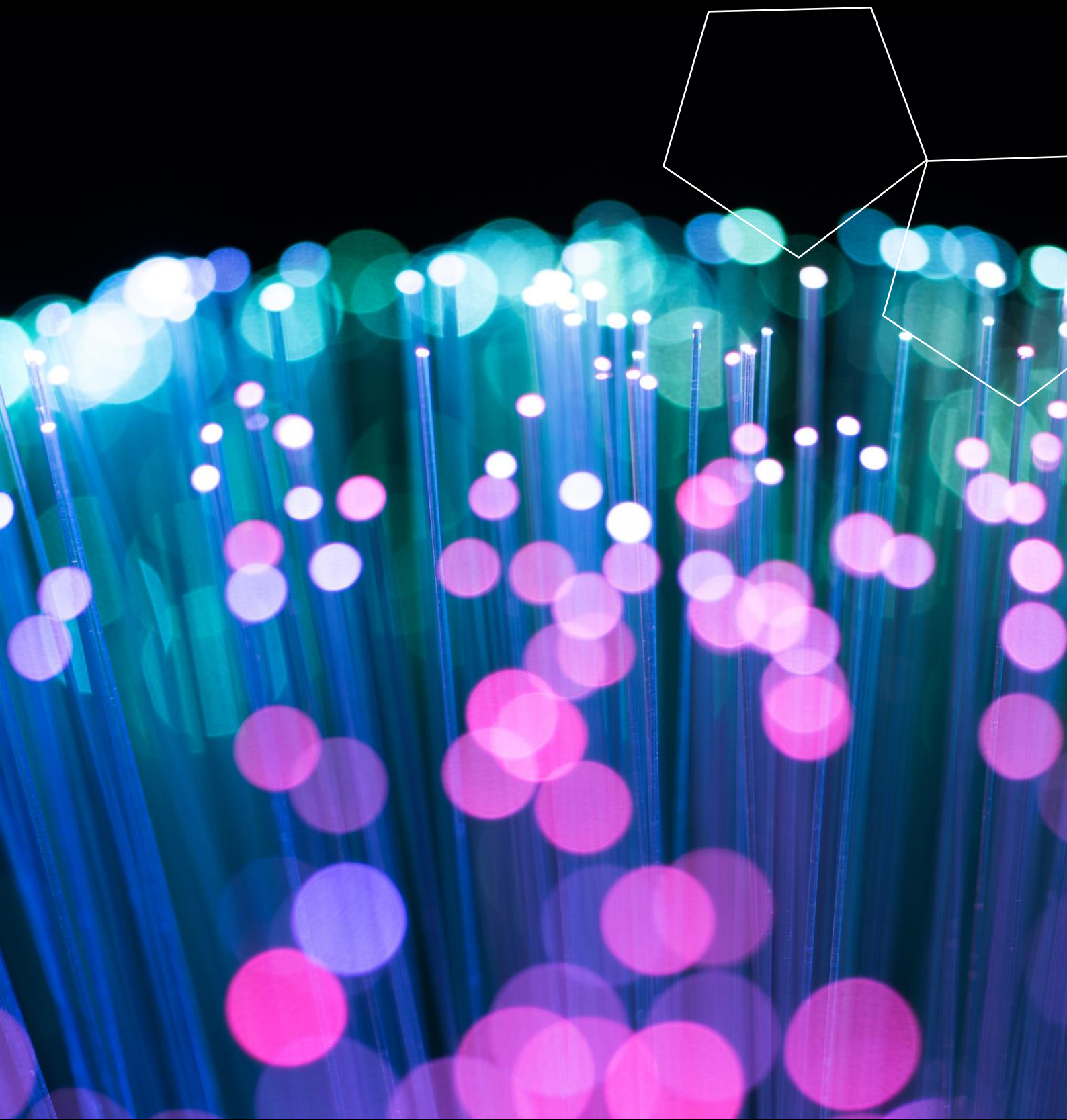
ARQIT

Quantum Speed Up

David Williams, Founder Chairman and CEO, Arqit Ltd.



When is Quantum Attack Relevant?

A question we are sometimes asked by people new to cryptography and quantum technology is: do I have to worry about quantum attack now?

Cyber-attacks are now ever present in our news cycles. They are mainly possible because of the deficiencies of PKI encryption. Partly invented by one of my own Board Directors, it did a great job for a long while, but was never designed to universally protect a hyper connected world. That is why every major state cyber agency in the world is deep in planning to migrate away from PKI right now.

The world needs stronger, simpler encryption, and that is what Arqit has invented. A little like using a pathogen to create its antidote, we use some transformational quantum encryption techniques to create keys that are safe from quantum attack. These are one-time keys, created in the moment they are needed, in a trustless manner.

There is huge innovation in this Platform-as-a-Service, with over 1,300 patent claims filed in a system that is unlike anything that the world has seen before and solving deep tech problems that have persisted for decades. But, that also means that these keys can prevent many of the cyber-attacks that are made today, regardless of the timing of quantum computing. So, we have a solution for customers today, and have them covered for the time when quantum attack is real. That is why so many blue-chip customers and governments are engaging with Arqit today, with platform revenues expected to flow this year.

The US agency, given the task of leading the global response to the threat, NIST[i] has urged all parties to urgently begin work to migrate to new protections, because whilst the timetable of quantum computing attack is uncertain, PKI is already failing us and it is certain that total network upgrade cycles take a long time.

We can however start to put more data around the timing of quantum attack. Anyone who still quotes estimates that were around five years ago has not been paying attention to the enormous advances that have occurred and the vast investment poured into the race for Universal quantum computing. Basic architecture, error correction and algorithm improvement have all resulted in a dramatic increase in the efficiency of quantum computing - physical qubit numbers are not the only determinant of the schedule and with an increase in the ratio of logical to physical qubits, the timetable is accelerating. The vast resources and talent pouring into this area means that the innovation can only intensify.

But Arqit's customer decisions are not driven by that consideration. Arqit has a simple, low-cost method to make all connected devices secure against most current forms of cyber-attack with one time pad keys delivered trustlessly - the holy grail of cyber security - and quantum safety is baked in. Here is our analysis of the data on the timing of development of universal quantum computing.

The exponential increase in quantum computing power

The Global Risk Institute published a report "Quantum Threat Timeline" [ii] in 2019 which surveyed 22 academics on the likely forecast timetable for a quantum computer to break PKI. The majority consensus was around 15 years. Since then, the weight of investment has moved quantum computing out of the conservative realm of academia where small, fixed budgets and an absence of economic incentive do not spur rapid innovation and into the commercial market.

Looking at the rate of growth in physical qubits over the last few years, it's clear that the huge volume of investment is starting to result in impressive leaps in capability. Several companies (Google, Rigetti, IBM) already quote physical qubits of more than 100 qubits, and our analysis shows a rapid doubling of qubit numbers across the sector. IBM are themselves targeting an increase from around 100 qubits today to around 1000 by the end of 2023[iii], which roughly means a doubling every 7–8 months. Honeywell is also on target to double their computing power every 6 months.[iv] By that measure, it seems likely that quantum computers with qubit numbers on the order of 10,000 qubits will appear within the next 5–10 years. If PsiQuantum is able to meet its own aspirations, we could even see a 1-million-qubit machine by then[v].

The opinion that quantum computing will advance faster than the 2019 consensus suggests it is neither rare nor limited to marginal commentators. Sundar Pichai, CEO of Google, announced at the World Economic Forum in 2020 that quantum computing could end the usefulness of PKI encryption by 2025.[vi] Research by the Global Risk Institute in 2020 surveyed 44 deep experts in quantum computing and the majority thought that there was a probability to break encryption before 2030.[vii] A July report published this week by Boston Consulting Group[viii] underlines the rate of investment in quantum computing and how that will act as a catalyst for rapid improvement as it has in many other sectors. The sheer number of quantum start-ups (estimated at 193 across the world by the FT[ix]) will also catalyse developments and lead to step-changes in capability that can't be foreseen today.

A reduction in the required number of qubits

Experts in this area know that it's not just about physical qubits, but logical qubits, which are the error-corrected collection of physical qubits that results in a single, robust and usable quantum bit. For example, Google's approach to quantum computing results in only 1 logical qubit for every 1000 physical qubits, but IBM's work[x] is leading them towards 1 in 100 or perhaps even 1 in 10 in the next few years, and the rate of improvement appears to be exponential. There are also emerging technologies to create physical qubits which are inherently robust to errors[xi] and could lead to an order-of-magnitude reduction in the error rate in a single bound. The most exciting advances announced in recent months have been around error-correction.

This drastically reduces the resources to run a quantum algorithm and crucially, this is rarely taken into account when assessing the qubit numbers required to break encryption. A recent article from Häner et al[xii] showed that RSA-2048 could be broken with as few as 2,000 logical qubits, which would mean only 20,000 physical qubits with better error correction. This is compared with an estimated 20 million physical qubits from a paper published only last year[xiii] and this estimate itself had dropped from 1 billion in 2012 by tailoring the algorithm to the quantum hardware being used. This rapid change demonstrates just how far we can reduce the numbers of qubits once error correction improves.

There are also interesting advances in quantum memory. Whilst it's not a technology suitable for operations at distance, using entanglement-based quantum memories we can potentially network quantum computers together in the same location, generating rapid scale up in capability.

Protecting yourself today from the threat tomorrow

Organisations need to act now, even before a quantum computer is available, due to harvest-now-decrypt-later attacks, such as the data theft from Saudi Aramco.[xiv] Government organisations like NIST have already said "it is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks."[xv] The World Economic Forum agrees, saying "addressing this issue requires action at the national and global levels - now."[xvi]

Innovation continuing at pace

Taken together, these threads of research activity and volume of investment make it likely that we'll see a quantum computer able to break encryption within a decade, and perhaps in only five years.

- Improvements in error correction and the implementation of Shor's algorithm means that the number of qubits will be reduced to perhaps only 20,000 within the same period.
- The number of physical qubits per machine are increasing at around 2x every six months, meaning we're likely to see a 10,000-qubit quantum computer between 2025–2030.

It's only with this holistic view that we can start to form a realistic picture of when the threat will emerge. Given the possibility that it could happen within five years, there's no reason for enterprise or governments to delay migration to quantum-secure technology.

I remember working on a financing for a UK mobile phone network in 1996. We had to work very hard to persuade the syndicate of banks that one day mobile phone penetration would reach 20%. Of course, by 2001 it was treble that level. Investment levels, technology, costs and features all changed. Thus, it will be with quantum computing in 2021 that the volume of capital available to early-stage companies is breathtakingly large on a global scale by comparison with earlier eras. The hyperscalers also have almost unlimited capital to deploy in generating competitive advantage.

Using assumptions that are years out of date to predict the future of the fastest moving technological revolution in our history is not well grounded in history or economics. Happily, for Arqit, the very fruitful pursuit of solutions to the major problems of quantum encryption means that in fact our technology solves major problems that are splashed across our headlines today, and we ***also*** have your back covered against the quantum threat, whenever it materialises.

References

[i] https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final

[ii] https://globalriskinstitute.org/publications/quantum-threat-timeline/

[iii] https://techcrunch.com/2020/09/15/ibm-publishes-its-quantum-roadmap-says-it-will-have-a-1000-qubit-machine-in-2023/?guccounter=2

[iv] https://thequantumdaily.com/2021/03/09/honeywell-sets-new-record-for-quantum-computing-performance/

[v] https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/moorinsights/2021/05/10/last-weeks-big-technology-reveal-psiquantums-previously-secret-q1-photonic-quantum-computer-with-globalfoundries/amp/

[vi] https://www.telegraph.co.uk/technology/2020/01/22/googles-sundar-pichai-quantum-computing-could-end-encryption/

[vii] https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

[viii] https://www.bcg.com/publications/2021/building-quantum-advantage

[ix] https://www.ft.com/content/a5af3039-abbf-4b25-92e2-c40e5957c8cd

[x] https://www.sciencemag.org/news/2020/07/biggest-flipping-challenge-quantum-computing

[xi] https://spectrum.ieee.org/tech-talk/computing/hardware/amazon-quantum.amp.html

[xii] https://arxiv.org/abs/2001.09580

[xiii] https://arxiv.org/abs/1905.09749

[xiv] https://www.bleepingcomputer.com/news/security/saudi-aramco-data-breach-sees-1-tb-stolen-data-for-sale/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

[xv] https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

[xvi] https://www.weforum.org/agenda/2020/06/quantum-computers-security-challenges/