Quantum Computing

Dr Wayne Crump, intern from the MacDiarmid Institute, 2019

Summary

Quantum computing is said to be an important future technology, but how important and how far away that future might be is unclear. It could be a catalyst to breakthroughs in the R&D of new materials, as well as providing value to other areas – however, at this stage it has not shown any commercially viable application. The technology is still immature with significant challenges impeding its development. The kind of quantum computer needed to break public key encryption is still considered to be a long way off but "quantum-safe" encryption standards are being developed. Recently there has been at least 2.5 billion USD investment into the space from both governments and industry in the USA, EU and China.

What is Quantum Computing?

In a classical computer, "bits" are used to represent information and can be in the ONE or ZERO state. Calculations are performed by operating on the bits using logic gates such as AND, OR and NOT. Using these elements one can build up to the complex computations we have today such as facial recognition. A quantum computer uses "qubits" instead which still can be in the ZERO or ONE state, but can also in a sense be in both these states at the same time. Quantum logic gates operate on the qubits to perform calculations and the computation is fundamentally different from the classical case because of the different properties of the qubits. This new paradigm in computing has resulted in the development of several "quantum" algorithms which show theoretical speedups over classical algorithms seeking to do the same task.

Potential applications

The potential here is in accelerating development of new materials, chemicals and drugs due to the speedup over a classical computer in simulating these systems [1]. This could have far reaching impacts for many industries. Artificial intelligence and machine learning might also benefit from quantum computing, with companies like Google, IBM and D-Wave active in this area. Quantum computers have also shown capability with optimisation problems like the travelling salesman problem and may also be useful in pattern recognition. One of the potentially significant areas of application is that of cyber security.

Cyber security concerns

Public key cryptosystems are pervasive in our ecosystem and are used, for example, in email, secure web browsing, setting up a secure channel and authenticating software updates [2]. Shor's algorithm provides a way for quantum computers to break current public key cryptosystems. A quantum computer capable of doing this does not exist yet and experts believe it will not exist for some time. There are significant problems that inhibit the development of this class of quantum computer.

Even so, the potential threat has been enough to spur into action work by both the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI) in setting up new "Quantum-safe" public key cryptography standards [3] [4]. The NIST program is in its second round of testing proposals and draft standards are expected to be available by 2022-2024.

Current public key cryptosystems are deeply embedded and so implementing new standards is expected to take time. Experts have said it is difficult to predict this time with 7 years as a possible minimum. Regardless, NIST encourages the adoption of "crypto agility" which is the ability to change cryptosystems, so that any needed changes will be easier to undertake in the future [5].

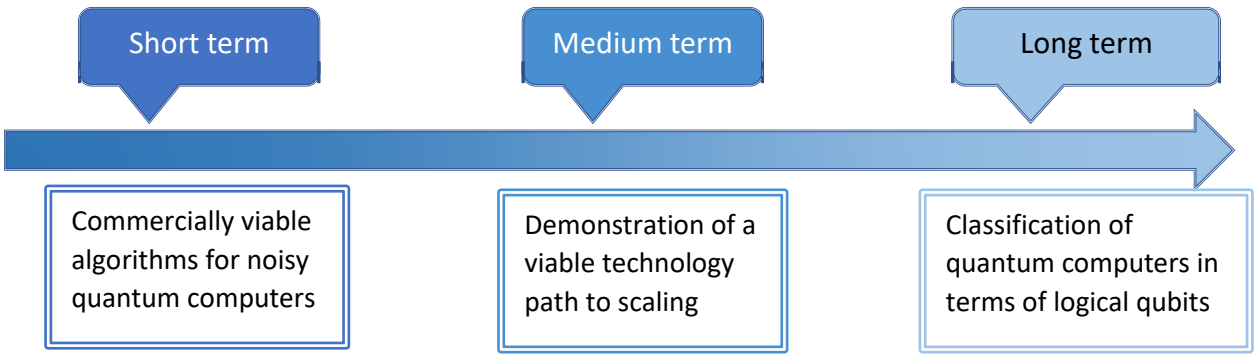
What is the current state of the technology?

Quantum computers are still in their infancy with serious hurdles in their way. The biggest hurdle is the problem of decoherence which gets worse as the system increases in size. The computer needs to maintain its quantum state throughout a calculation for the result to be accurate, however, the quantum state is very sensitive to any unwanted noise which causes the state to "decohere" and introduce errors into a calculation.

Quantum error correction can be used to overcome this problem by combining several physical qubits into one "logical" qubit, but it requires gate and qubit error rates below a threshold. The other drawback is that one logical qubit can require many physical qubits as the system scales up. To break current public key cryptography, it's thought that more than 2,000 logical qubits or 2,000,000 physical qubits are required [6].

Some technologies like ion traps are able to produce qubits and gates with errors below the threshold, however there is no obvious way to scale them up. Other technologies like superconducting circuits seem easier to scale up, but the errors are not low enough for quantum error correction to work [6]. At present, it seems there is no feasible technology path to scale-up and build a large-scale error corrected quantum computer. There are some sceptics who believe that it may be impossible to build a large-scale quantum computer. Current quantum computers are only in the 10s of bits and these are noisy systems where the number of gate operations in a calculation must be limited to reduce errors [6]. D-Waves system is the exception with 2000 qubits, however theirs is a specialised machine which operates a slightly different model of computing [6].

An important milestone to look out for then would be for the development of a feasible technology path. It is likely that scale-up would follow quickly due to the amount of money going into the space. Another milestone would be quantum computer designers talking about their machines in terms of logical qubits as this would indicate they have come to grips with error correction.



Commercial activity

Despite being a young industry, there is a large amount of investment in the space. Experts have attributed some of this to hype as well as fear of a competitor having a technological advantage. Google, Microsoft and Intel all have ongoing programs with IBM offering cloud access to its current quantum computers.

A significant company is D-Wave Systems (Canada) which has been around since 1999 and has built and sold several models of their quantum computer to Lockheed Martin, Los Alamos National Laboratory and a collaboration between Google, NASA and the Universities Space Research Association (USRA). They also offer cloud services. Two notable start-ups are Rigetti (USA) who offer cloud services and IonQ (USA) which are close to offering their system for research.

International activity

Several countries are funding research programs into quantum technologies, of which quantum computing is a part:

- **United Kingdom:** Their Quantum Technologies Program began in 2013 with current funding at 47 million GBP (59.92 million USD) per year till 2024 [7].
- **European Union:** They recently established a Quantum Technologies Flagship in 2018 with funding of 100 million EUR (113.8 million USD) per year till 2028 (ten years of funding) [8].
- **USA:** They recently announced their investment into quantum information science of 1.2 billion USD over 5 years which will bring their funding to around 440-490 million USD per year [9].
- **China:** Building of the National Laboratory for Quantum Information Science is underway which has received 7 billion RMB (1 billion USD) at this point and is slated to receive a further 100 billion RMB (14.5 billion USD) over the next five years. In 2016 and 2017, the National Key Research and Development plan alone has funded around 1 billion RMB (15 million USD) of projects each year. Up to billions of RMB may be provided by China's National Natural Sciences Foundation to the space as well [10].
- **Australia:** The Centre for Quantum Computation and Communication Technology (CQC2T) received 33.7 million AUD to launch it as a centre of excellence in 2019 [11].
- **Aotearoa New Zealand:** There are currently no NZ researchers working directly on building a quantum computer. There is a small amount of people working on developing algorithms such as Professor Cristian Calude and Dr Michael Dinneen and others looking at post-quantum cryptography such as Professor Steven Galbraith at the University of Auckland. There are others who work in fields on the periphery of quantum computing such as Dr Maarten Hoogerland, Professor Howard Carmichael and Associate Professor Scott Parkins at the University of Auckland and Associate Professor Jevon Longdell at the University of Otago.

Opportunities for Aotearoa New Zealand

Currently there is free access to IBM's quantum computer via the cloud, and there are a few online simulators of quantum computers. New Zealanders can access these to familiarise themselves with the technology and potential find if they can make some use of it.

Aotearoa New Zealand would be behind in any effort to build a quantum computer due to our late starting point; however, the expertise in quantum systems that already exists here might find opportunity to collaborate with overseas efforts such as in Australia.

We thank the following individuals for comment:

- Professor Cristian Calude, Department of Computer Science, University of Auckland
- Professor Howard Carmichael, Department of Physics, University of Auckland
- Professor Steven Galbraith, Department of Mathematics, University of Auckland
- Dr Maarten Hoogerland, Department of Physics, University of Auckland
- Jeremy Jones, Theta Cyber Security
- Associate Professor Jevon Longdell, Department of Physics, University of Otago
- Paul Macpherson, Reserve Bank of New Zealand
- Associate Professor Scott Parkins, Department of Physics, University of Auckland

We would like to especially thank Dr Kirsten Edgar, Professor Cristian Calude and Associate Professor Scott Parkins for their comments on this work.

Bibliography

[1] A. M. Lewis, C. Ferigato, M. Travagnin and E. Florescu, "The Impact of quantum technologies on the EU's Future Policies: Part 3 Perspectives for Quantum Computing," European Commission, Ispra, Italy, 2018. Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/impact-quantum-technologies-eus-future-policies-part-3-perspectives-quantum-computing.

[2] European Telecommunications Standards Institute, "Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges.," European Telecommunications Standards Institute, Sophia Antipolis CEDEX, France, 2015. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[3] National Institute of Standards and Technology, "Post-Quantum Cryptography," [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. [Accessed 1 June 2019].

[4] European Telecommunications Standards Institute, "Quantum-Safe Cryptography," [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 1 June 2019].

[5] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, USA, 2016. Available: https://www.nist.gov/publications/report-post-quantum-cryptography.

[6] National Academies of Sciences, Engineering, and Medicine, "Quantum Computing: Progress and Prospects," The National Academies Press, Washington, DC, 2019. Available: https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects.

[7] P. Vallance, "Building an ecosystem for breakthroughs," New Statesman America, 11 April 2019. [Online]. Available: https://www.newstatesman.com/spotlight/emerging-technologies/2019/04/building-ecosystem-breakthroughs.

[8] PressRelease, "EC launches € 1 billion Quantum Technologies Flagship," ERA Portal Austria, 30 October 2018. [Online]. Available: https://era.gv.at/object/news/4393.

[9] M. Giles, "President Trump has signed a $1.2 billon law to boost US quantum tech," MIT Technology Review, 22 December 2018. [Online]. Available: https://www.technologyreview.com/f/612679/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/.

[10] E. B. Kania and J. K. Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," Centre for a New American Security, Washington, DC, 2018. Available: https://www.cnas.org/publications/reports/quantum-hegemony.

[11] M. Johnston, "Federal govt funnels $33.7 million towards UNSW's quantum research," IT News, 18 February 2019. [Online]. Available: https://www.itnews.com.au/news/federal-govt-funnels-337-million-towards-unsws-quantum-research-519393.

Further reading

- Think Academy explaining quantum computing: https://www.youtube.com/watch?v=WVv5OAR4Nik
- Interesting articles on quantum computing: https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/, https://www.gizmodo.com.au/2019/06/when-will-quantum-computers-outperform-regular-computers/
- A technical report on the current state of quantum computing: National Academies of Sciences, Engineering, and Medicine, "Quantum Computing: Progress and Prospects," The National Academies Press, Washington, DC, 2019. Available: https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects.
- Web based quantum computer simulator: http://www.quantumplayground.net/#/home
- Gibbons Lecture Series on quantum computing by University of Auckland: https://www.cs.auckland.ac.nz/en/about/ourdepartment/gibbons-lectures.html

➲Curated List of Resources