Monday,
7 March 2022

Daily Wire

Latest news and updates

Technology
Special

Jennifer Robinson

China Reaches Quantum Advantage

What now?

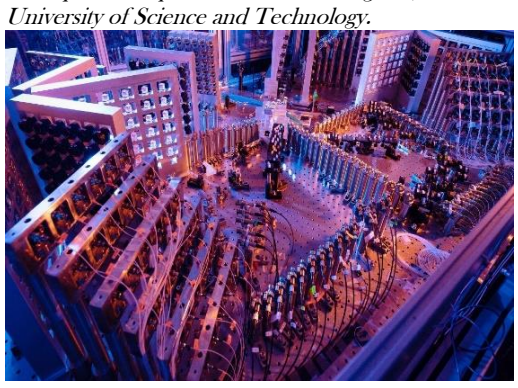
Last week, Chinese researchers have publicly presented their latest developments of the quantum computer Jiuzhang 2.0. In this demonstration, Jiuzhang 2.0 and the state-of-the-art supercomputer had to solve a computational challenge specifically designed for this test. The result: the quantum computer reached a conclusion, while the supercomputer did not. The Chinese researchers claim that their photon-based quantum computer Jiuzhang 2.0, which works at room temperature, computed the specific challenge 1 septillion (a thousand, raised to the seventh power) times faster than the supercomputer. In other words, they have demonstrated quantum advantage.

Three years ago, Google and NASA reported the achievement of quantum advantage for the first time, in their case with the superconducting quantum computer Sycamore, operable at very low temperatures. Since then, development of quantum computers has skyrocketed. While Sycamore was equipped with 53 qubits, the photon-based quantum computer Jiuzhang 2.0 reaches 113 qubits. This may remind one of the well-known Moore's law of conventional computing, the doubling of transistor numbers in an integrated circuit every two years - yet this is not optimistic enough. Based on in-house observations at Google, Neven's law has been proposed as a Moore's law for quantum computers, stating that the computational capacity of quantum computers grows doubly exponentially relative to conventional capacity. This implies a growth by the powers of powers of two (i.e. 2^2 (4), 2^4 (16), 2^8 (256), 2^{16} (65.536), etc.), meaning that quantum computing is expected to grow exponentially faster than conventional computing. For comparison, if this would apply to conventional computing methods, we would have had today's laptops and computers in 1975.

To say that the developments by the Chinese towards a quantum computer is an endpoint, is a mistake. Jiuzhang 2.0 has demonstrated that it can do this specific challenge faster, but this does not extend to any computational challenge. To deliver on its potential and become fully programmable like a conventional computer, quantum computers must be developed further. Yet, considering Neven's law and the fast-paced development of quantum computers in the past three years, useable quantum computers are expected within a decade.

Quantum computers promise to be a gamechanger in scientific research involving highly complex simulations, in the pharmaceutical industry to find compounds used as medicine, for financial modelling to predict market trends or for the entertainment sector to develop more exciting experiences. Another sector which quantum computers are expected to impact is the communication sector, especially with a focus on secure communication. By applying quantum mechanical principles to data encryption and transmission it will be possible to create high encryption standards to secure digital communication from hackers and eavesdroppers.

The Chinese quantum computer Jiuzhang 2.0 based on a photonic processor. Chao-Yang Lu, Chinese University of Science and Technology.



COLUMN

The Unfinished Race

The Netherlands is being outrun by China and the US

Anyone with a little foresight could have seen this situation coming, China has outrun Western countries in the race towards quantum computing. This race has started in 1980 and only received considerable investment from the Dutch government when it launched Quantum Delta NL in 2020. Now we can see that this is too little, but maybe it is not too late.

This demonstration of Chinese researchers is impressive and is an important milestone in the race of building a quantum computer. However, this potential computational capacity poses a threat to our communication networks, since our current encryption standards can easily be cracked by such superior computing power. It is only a matter of time until the superior quantum computing power can be utilised for large-scale intervention in networks relying on conventional computing and establishing a communication network of far superior encryption. This is a threat not only to governmental sensitive information, but also will impact the privacy of all citizens.

The European Union has expressed its concern about the sovereignty of member states in the context of the increasing technological capacity of the US and China, rightly so. Investments that have been made earlier are not enough, the Dutch government is faced with the need to respond now. Faced with the same decision, Japan put priority on effective encryption of their communications and independence of other countries by prioritising domestic development of the necessary technology, vastly increasing its commitment once again.

This shows that the race is not yet finished. Now, it is up to the Dutch government and its EU partners to increase investment quickly and ride out this challenging competition in quantum computing and (post-quantum) cryptography or abandon the race and brace themselves for what is to come. I would say: catch up, the potential of this technology and the looming insecurities are too great to not act now. The Dutch government must prove its worth.

***Rosalie Prümm**, International relations and quantum technology expert*

Alexander Preston

Quantum-what?

Quantum computers, quantum advantage and post-quantum cryptography spelled out

A quantum computer is a new and powerful computer which can analyse large amounts of data and run detailed simulations – tasks a conventional computer is not capable of. Conventionally, a computer encodes information in bits as '0's or '1's. A quantum computer encodes information in qubits which, based on the principles of quantum theory, can have the states of 0 and 1 at the same time. This is called superposition. Qubits have the property that they cannot be copied, which makes it possible to keep the stored data private.

Quantum advantage describes the scientific goal to demonstrate that a quantum computer can solve a specific problem a conventional computer cannot solve – regardless of whether the problem is useful or not. Since quantum advantage is mainly an intermediate, scientific goal towards the creation of a powerful quantum computer, the clear application or societal relevance of this research field is not yet clear.

Post-quantum cryptography refers to algorithms used for the encryption of information which cannot be cracked by a quantum computer. Currently, research efforts focus on the development of post-quantum cryptographic standards to improve existing encryption standards and secure today's data against a quantum computer attack decades in the future.

Time to bundle forces

Minister Vos invites stakeholders to discuss next steps

Mirjam Nilsson

In response to the recent advances in the field of quantum technology and the resulting opportunities and challenges regarding quantum encryption, the minister of Education, Culture and Science, Peter Vos, has invited various stakeholders to discuss next steps. National and international pressure for more funding requires a decision on how to invest in quantum communication technologies. Should we invest in quantum computing to develop quantum encryption standards for secure future communication or should we focus on the safety of our current encryption? "In the Netherlands, we have a vivid quantum environment with great potential. It is time now, that we bundle our forces and resources to increase our competitive capacity and to contribute to an economic, inclusive and societally desirable development of quantum communication technologies.", Vos said. The meeting will be held in The Hague on April 14th.