7TUNNELS

PRIMER

QUANTUM COMPUTING

THE BASICS

7TUNNELS®

Park City · Utah · USA info@7Tunnels.com

7TUNNELS PRIMER

QUANTUM COMPUTING

1994

Peter Shor formulates his quantum integer factorization algorithm

2004

China successfully entangles five qubits

2018

U.S. Senate unanimously passes the National Quantum Initiative Act

2019

IBM launches its Q System One commercial quantum computer

2019

Google's quantum processor takes 210 seconds to run a calculation that the fastest supercomputer would need 10,000 years to perform

Classical vs. Quantum Computers

Alan Turing and Konrad Zuse designed the first programmable computers in the 1930s and, in the process, laid the foundation of modern computation: a binary system in which all data is represented in bits of either one or zero. Although simple, this classical binary system allows for a vast universe of programming potential, as evidenced by the capability of today's computers compared to the machines of even a decade ago.

Yet despite their immense speed and power, classical computers are inherently limited by the binary system's Boolean 'True/False' logic paradigm: a supercomputer may be able to run 200 quadrillion calculations per second, but it still must consider each solution independently.

A quantum computer, however, is based on quantum mechanics—the world of subatomic particles like quarks and photons that is beyond the laws of classical physics. Its fundamental unit is a quantum bit, or qubit, which can be a one, a zero, or critically, a probabilistic mixture of both—a state known as superposition. When qubits are linked, they achieve entanglement—a physical phenomenon that occurs when pairs or groups of particles are generated, interact, or share spatial proximity in which the quantum state of each particle cannot be described independently of the state of the others—and their processing power grows exponentially.

The difference between quantum and classical computers lies in that exponential power. If a classical computer can be thought of as a train traveling from Point A to Point B, a quantum computer is like a fleet of jets capable of traveling from the same Point A to many points at the same time.

Consider a computer program designed to find the seven of hearts in a deck of cards laid face down. Today's fastest computer would find the card in an instant but would use the same underlying process as Zuse's Z1: it would turn over each card in sequence until it found its target. A quantum computer, however, would simply turn over every cards at the same time.

In numerical terms, 50 entangled qubits could represent one quadrillion output states and it is theorized that 300 perfectly entangled qubits could map all the known information in the history of the universe.[1]

The Current State of Quantum Computers

The theoretical concept of quantum computation was first posited by physicist Richard Feynman in 1959. Two decades later, Feynman openly called for the development of quantum computers saying, "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."

The first pair of qubits was successfully linked in 1998 by a team of physicists in Oxford.[2] Since then, the pace of quantum computer advancement has tracked closely with Moore's law, which observes that processing power for classical computers can be expected to effectively double every two years. For quantum computers, that advancement is measured in two ways: width—the number of successfully linked qubits—and depth, which measures the coherence time of those qubits.

With each new benchmark reached, we near the advent of Quantum Supremacy—the tipping point when quantum computers functionally outperform binary supercomputers. (One point of clarity—a quantum computer must still be controlled by a classical computer that requests and evaluates the processes the quantum core runs. As such, there will continue to be a need for advances in binary processor speed and power.)

Building quantum computer cores is both expensive and difficult. Qubits can be created using photons, ions, atoms, electrons or even electrical currents, but all of these are unstable and difficult to manipulate into superposition. They are also extremely susceptible to noise from the slightest temperature change or vibrations from sources as small as nearby atoms.

Noise leads to decoherence (loss of superposition) which in turn creates calculating errors. As a result, some qubit processors need to be housed in dilution refrigerators that reach temperatures of less than 50 millikelvin (-459 °F, which is several degrees colder than space.) Factor in other hard-to-source components like niobium/titanium superconducting wires and helium-3, a supercooling gas that is a byproduct of nuclear research, and the challenges of building quantum computers become daunting.[3]

As such, some have dismissed the race for Quantum Supremacy as a meaningless stunt, one without near-term impact on industry and security. But those skeptics are betting against some of the biggest, smartest and wealthiest companies on Earth: Google, Alibaba, IBM, Microsoft and Intel,[4] not to mention the governments of the United States, China and Russia, who combined have already invested nearly a trillion dollars in quantum computer research and development.

Potential Applications

Eventually, large-scale quantum computers will be capable of solving the most complex computer and mathematical problems known to man. They offer the potential to unlock the most vexing mysteries in fields ranging from chemistry and biology to astronomy and economics and, of course, computer science. Moreover, quantum computers will help us in ways we haven't even thought of yet; they'll solve problems that are beyond the realm of our collective imagination. Maybe those solutions will take the form of new disease-curing drugs. Perhaps they will come as monumental advances in Artificial Intelligence. But like all new technology, quantum computers will inevitably be used for criminal purposes, and the most imminent threat quantum computers pose is the ability to break all known methods of digital encryption.[5]

Consider TSL, the widely used cryptographic protocol that protects digital communications. When an internet user visits a website, the client (user) and server (website) negotiate a secure link through which to communicate. This process, known as a "handshake," takes milliseconds and is commonly done using an algorithm based upon the mathematical difficulty of factoring the product of two large prime numbers.

Without the decryption key, a hacker would need to try every possible combination of numbers to break the handshake and view the data being transmitted. For 256-bit encryption, this would require trying 2^{256} (two to the 256th power) different combinations. For perspective, that is larger than the number of atoms in the observable universe.[6]

It would take the fastest computer in the world millions of years to brute force hack 256-bit encryption, but a quantum computer, using an existing algorithm created by Peter Shor that shortens the process, could conceivably solve RSA's integer factorization problem in a matter of minutes.[7]

While it stands to reason that quantum computers will also be used to develop new encryption standards, today's encrypted communications will still be vulnerable. As Rep. Will Hurd of Texas pointed out, Chinese and Russian bad actors are known to be intercepting encrypted communications (ciphertext) knowing full well quantum computers will soon be able to decrypt it.[8] The reality is that many others are vacuuming up communications and data in bulk, counting on future decryption and the leverage that exposed information will provide.

This means that every single piece of data—from trade secrets and financial documents to health records and patented formulas—encrypted and transmitted using today's standards will be vulnerable and potentially exposed and exploited in the very near future.

The only solution, according to the National Institute of Standards and Technology, is to "begin now to prepare our information security systems to be able to resist quantum computing."[9]

Looking Forward

Quantum computing represents the most significant and revolutionary technological advance since the creation of the microprocessor. And while we don't know who will reach Quantum Supremacy first or when it will happen, it grows nearer every day.[10]

What cannot be disputed, though, is that both the public and private sectors are heavily incentivized to withhold information about quantum computing progress. As NSA general counsel Glenn Gerstell stated, "The strategic advantage here would be for one country to surreptitiously acquire such a capability and maintain it for perhaps several years or more. Other countries would not realize that everything from their weapons systems to financial transactions would be vulnerable during that period; and that would include not only current activity but also the historic, encrypted communications collected and retained by the winner in anticipation of this very capability."[11]

In September of 2019, a research paper briefly appeared on an official NASA website. Authored by Google researchers working in partnership with the space agency, the paper announced that a quantum computer had successfully performed a calculation in 210 seconds that Summit, the most powerful supercomputer on Earth, based at Tennessee's Oak Ridge National Laboratories, would require 10,000 years to match.[12]

The announcement, which was viewed by a reporter from London's Financial Times before disappearing from the site, illustrates not only the rapid acceleration of quantum computing technology (which those same Google researchers predict will grow double exponentially, or twice the rate of Moore's Law)[13] but also the secrecy desired by those on the threshold of acquiring such powerful, world-changing new technology.

[1] *Science Magazine*, December 1, 2016 https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one
[2] *The Age of the Qubit: A New Era of Quantum Information in Science and Technology*, Institute of Physics, 2011 https://www.iop.org/publications/iop/2011/file_52078.pdf
[3] *MIT Technology Review*, January 17, 2019 https://www.technologyreview.com/s/612760/quantum-computers-component-shortage/
[4] *Wired Magazine*, May 19, 2018 https://www.wired.com/story/google-alibaba-spar-over-timeline-for-quantum-supremacy/
[5] *Network World, March 20, 2019 https://www.networkworld.com/article/3373550/quantum-computing-will-break-your-encryption-in-a-few-years.html*
[6] *IBM Security Intelligence*, June 12, 2014 https://securityintelligence.com/moores-law-and-cryptography-for-business-do-we-need-a-larger-key-space/
[7] National Security Agency – *Information Assurance Directorate*, January 2016 https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf
[8] Official Website of Congressman Will Hurd, June 23, 2018 https://hurd.house.gov/media-center/in-the-news/best-piece-legislation-dc-about-quantum-computing
[9] NIST Government Website, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[10] *Wired Magazine*, May 19, 2018 https://www.wired.com/story/google-alibaba-spar-over-timeline-for-quantum-supremacy/
[11] *New York Times*, September 10, 2019 https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html
[12] *Financial Times*, September 20, 2019 https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17
[13] *Financial Times*, September 20, 2019 https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17