

Quantum Computing

Sylvia Le

Connecticut College

### Quantum Computing

Moore's law, which states that the number of transistors on an integrated circuit will double every two years, has been able to accurately predict the advancement in processor and computer design for more than half of a century. Currently, in the year of 2020, the size of a transistor has shrunk to about 10-20 nm. It could have gone down further, but a lot of things start to behave differently when it's the size of a few atoms, which may topple the basis of modern-day computers. With all the weird phenomenon that could happen at the quantum scale, the error rate will soon be too high that it's not efficient to fix them all. Moreover, the smaller the transistors get, the higher the clock frequencies it can run at, hence the higher the power consumption. The higher the power consumption, the more heat it creates, which raises another problem: heat dissipation. These two barriers lead many people to think that Moore's law is coming to an end. While chip manufacturers have cleverly found a way to solve the problem but still make computers faster by pipelining, superscalar, and multiprocessors, scientists and top tech companies have to look at other possibilities of the future: quantum computing and quantum computer. According to Wikipedia, the definition of quantum computing is "the use of quantum phenomena such as superposition and entanglement to perform computation. Computers that perform quantum computations are known as quantum computers."

As normal computers' basic data unit is a bit, which can take two values 0 or 1, quantum computers' basic unit is the qubit, which behaves differently from normal bit: it takes two 0 or 1, or 0 and 1 at the same time. To correctly understand qubits, one must understand two quantum physics concept: superposition and quantum entanglement.

The concept of superposition was derived from the famous thought experiment of the physicist Erwin Schrödinger. In this experiment, a cat is placed into a box, inside which has a device that has a 50% chance of killing the cat within 1 hour. The question is, after 1 hour, is the cat alive or dead? Normally, the answer would be, it either alive or dead; however, Schrödinger stated that in the quantum world, the very moment before one opens the box, the cat is being alive and dead at the same time. In other words, the cat is in a superposition. Only when the

box is opened, the state of the cat will 'collapse' into a definite state, alive or dead. Apply this idea to a particle, consider an electron orbits around an atom core. The electron location is in a superposition, which means that it can be at any space at the same time, with a certain area has a higher probability of finding the electron. Only when a scientist decides to measure the location, the electron's location will be definite

If the experiment above is repeated with two cats and two boxes, there can be four possible outcomes: both cats are alive, both cats are dead, one alive and one dead, and vice versa. The system of two cats is also in a superposition state, in which all four results can exist at the same time. However, in quantum mechanics, it's possible to know the properties of one particle just by looking at the other's state, and that changes made to one will instantly affect the other, no matter how far away they are. The two particles are said to be 'entangled'. In the cats' example, if one of the box is opened and the cats in there is alive, you know that the other cat is dead, without having to open the other box. In reality, multiple particles can be entangled. Entangled particles can be disentangled due to interactions with the surroundings, which may happen faster than entanglement can be created, thus make the process of entangling particles much more challenging. New methods are being created to achieve a higher entangling rate with a lower entanglement decay rate.

A qubit can be any particle that exhibits quantum behavior: an electron with spin, a photon with polarization, etc. Each can either hold the value 0, 1, or 0 and 1 at the same time due to superposition. When the qubit is measured, it will return the value 0 or 1. Which state has a higher probability will be returned. This is possible due as a result of the particle-wave duality, where different waves can be added up to reveal the regions with high peaks, means greater probability, and plateau region, which means low probabilities. In classical computers, a group of four-bit can represent  $2^4 = 16$  different values, one at a time. A group of four qubits, however, can represent all 16 values at the same time. This allows quantum computers to process a great number of potential outcomes to a problem simultaneously, giving it the potential to solve the current computationally infeasible problem. Qubits can 'communicate' with each other through quantum entanglement. Every additional qubit will double the number of possible entangled states, making the possible superposition states grow exponentially.

## QUANTUM COMPUTING

Besides, researches have shown that the ability to form entanglement between qubits greatly speeds up the processing ability.

Quantum computers also have their own set of quantum logic gates. Due to principles of quantum mechanics, quantum logic gates are reversible, mean that it's possible to get the state of the two input qubits given the resulting output state. Though most classical logic gates are not reversible, it's possible to perform classical computing and Boolean functions using quantum logic gates.














Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Figure 1: Quantum logic gates

Figure 1 illustrates some suggested quantum logic gates. Currently, there is no agreement on a fixed set of gates. Pauli-X gate function like NOT gate in classical computers: it maps values 0 to 1 and 1 to 0. Hadamard gate acts on one qubit and produce a superposition from the qubit value. SWAP gate acts on two qubits and swap the value of the two qubits. The

## QUANTUM COMPUTING

controlled gate acts on two or more qubits, and use one qubit as a control to determine other qubits state. The controlled gates, particularly the CNOT gate, can be used with the Hadamard gate to produce entangled states. Generally, quantum logic gates manipulate the qubits' superposition states and produce new superposition, then base on probability, collapse it into meaningful strings of 0 and 1. Since the result is probabilistic, it's often a good idea to repeat the calculation several times to be sure about the result. Despite having to double-check the process, it's indeed still a lot faster than performing the process on a classical computer.

Since qubits are technically quantum particles, they are sensitive and fragile to environmental disturbances, such as light, temperature, radiation, quantum vibration, etc. Therefore, quantum behavior can decay and eventually disappear before existing for a long enough time to do any computation. In the quantum computer research lab, the qubits are placed in vacuum tubes freeze to almost absolute zero degrees to protect them. Algorithms are also designed to make up for this loss of efficiency, but too many qubits are still used just for error detection and correction. The cost to maintain such a delicate system and the qubits' property of being prone to error presents great challenges to building a reliable quantum computer.

One potential use of quantum computers is modeling quantum processes, such as chemical reaction and physics processes. To model a chemical reaction precisely, the scientists need to know the quantum state of all electrons involve. Electrons in reality stay in a superposition; a system of around 20 electrons can easily have a million or more possible states. Therefore, for a complex molecule, the number of possible configurations is too large for a classical computer to handle. Quantum computer, on the other hand, operates on the principles of quantum mechanics. With enough qubits, it can have more computational power than what is required to simulate complex natural processes. The behavior of the electrons strictly reflects the reaction conditions, help the scientist understand the reaction mechanism. This can be a breakthrough in many fields, such as developing new drugs, understanding how the human brain works, etc. In August 2020, Google successfully simulated a chemical reaction involving a molecule with 12 hydrogen atoms and nitrogen atoms with 12 qubits, each represents an electron. The problem can indeed be calculated using a classical computer, but

scientists consider this can be a milestone in quantum chemistry, and hint at the potential of more simulating ability with the development of more qubits in the future. More research on both hardware and software is required before desired goals can be achieved.

Quantum computers also present promising potential and a threat to cryptography. Indeed, the hype about quantum computers stems partly from its ability to render modern cryptography schemes no longer insecure. RSA algorithm, for example, the security goal is to make it easy to calculate the pair of public and private keys, but infeasible to calculate one given the other, or get the private key when knowing the public key. A part of the public key,  $N$ , is the product of two prime numbers. These two primes are also used later to calculate the public and private exponent value of the public and private keys. Therefore, if one has the value of the primes that make up  $N$ , the encryption keys are broken. In reality, the primes are big, normally hundreds of digits, lead to  $N$  is also a big number. This makes it hard to calculate the factorization of  $N$ . For a classical computer, the time it would take can easily scale up to thousands or millions of years for a 1024-bit key. Theoretically, a quantum computer has the potential to perform this process within minutes or hours. The presence of quantum computers also makes it possible to use more advanced and efficient algorithms to do the job, like Shor's algorithm for factorization. This great reduction in speed pose a threat to network security once quantum computers are available.

However, quantum computer is a double edge sword. If it can be used to break the current cryptography schemes, it can also be a tool for a better encryption algorithm. Researchers have come up with some quantum cryptography protocol in place of the old algorithms. The BB84 protocol, for example, uses a stream of photons as the key. Each photon can have four different polarization states of 0, 45, 90, or 135 degrees, and can be encoded into 0 or 1 using either a rectilinear basis or a diagonal basis.

	0	1
Rectilinear	↑	→
Diagonal	↗	↖

*Table 1.* Binary encoding of polarized photon going through rectilinear and diagonal basis

## QUANTUM COMPUTING

In a key exchange session between two entities, say, Alice and Bob, Alice generates a random string of binary, and 'encodes' by randomly choosing a basis above. After the encryption, Alice now has a sequence of polarization state for each of the binary bit. She then sends Bob a stream of photons, each has the polarization state corresponding to the one calculated. On the other side, Bob receives the photons and chooses a random basis for each of the photons. Theoretically, if the photons weren't altered during transmission, if the basis Bob chooses for a particular photon match the basis Alice chose, it should return the correct binary bit. By probability, Bob has a 50% chance of choosing the right basis. A correct basis is chosen when a 0 or 90 degrees polarized photon is filtered through a rectilinear basis, and 45 and 135 degrees through a diagonal basis. Alice and Bob then compare the basis they use through a public channel, and for any mismatch basis, the corresponding binary bit is discarded. The remaining string of bit is used as the secret key.

Two quantum mechanics principles make this form of cryptography secure from eavesdropping. First, the Heisenberg Uncertainty Principle states that the act of measuring a particle changes the state of that particle. Suppose a third person, Eve, wants to intercept the key exchange session, tries to decrypts the photons stream first, then transmit it to Bob. Eve, like the case of Bob, described above, also has a 50% chance of choosing the right basis. For every basis that she chooses wrongly, she changes the photon's polarization state. The stream of photons, with some whose state has changed comparing to the original, is then sent to Bob. Later when Alice and Bob check the secret key, if there is any mismatching bit, it's the sign of an eavesdropper. Second, the No-Cloning theorem proves that it's impossible to create a completely identical copy of a quantum state. This implies that the third party Eve can't make a copy of the photons stream to try and break the key.

With its remarkable processing power, quantum computer also shows potential in artificial intelligence research. It has the power to churn through large data set within a small amount of time to spot patterns, and the potential to enhance and enlarge the data set. This can lead to the development of a new machine learning model. Natural Language Processing also benefits from the availability of quantum computers. With a quantum computer, it's can now be possible to devise a model that captures all the nuances and properties of a language.

## QUANTUM COMPUTING

With a better model, computers might now be aware of the overall meaning of a sentence or a paragraph rather than single words. The probabilistic nature of the output of quantum computers may also hint at its potential in problems that are more unintuitive and random. Given the potential in the field of research, in May 2013, Google Research in partnership with NASA launch Quantum AI Lab to research how can quantum computing can be applied to machine learning and other complex science problem.

Theoretically, a quantum computer can solve every problem that can be solved with a classical computer. Also, according to the Church-Turing thesis, the vice versa must be true. Hence, it means that besides the ability to provide better time complexities, technically quantum computer provides no additional advantage. This runtime advantage lead to the coining of the term 'quantum supremacy'. Quantum supremacy is the goal of showing that a quantum computer can solve a problem that a classical computer cannot solve within a practical amount of time. There are several experiments proposed to prove quantum supremacy, including integers factorization, Boson sampling, sampling distribution of random quantum circuits, etc. In 2017, IBM showed that it's possible to simulate up to 56 qubits on a supercomputer, hint at the need for more qubits to achieve supremacy. Later research suggests that an array of 7x7 qubits with 40 cycles is enough, provided that the error rate is pushed low. In August 2019, Google claimed to have achieved quantum supremacy with 54 qubits (one of which was not functional) used to perform a series of operations within 200 seconds. A classical computer would take 10,000 years to complete this task. The examined operations fall into the quantum circuit sampling experiment: researchers pick a quantum circuit, simulate it on a quantum computer, then simulate what the quantum computer was doing on a classical computer. These steps are repeated until the classical computer is no longer able to catch up with quantum computers in terms of time complexities. IBM research team disagreed with the result and demonstrated that the same problem can be complete in 2.5 days. The debate shows some problems with the definition of the term 'supremacy'. First, there is currently no fixed standard for classical computer performance, since there are still advancements in CPU architecture. Second, many put forward the question of what is defined as impractical time. 200 seconds is still a thousand times faster than 2.5 days, so is 2.5 days considered impractical?



## QUANTUM COMPUTING

Third, the term 'supremacy' is quite misleading. It's worth noting that quantum supremacy is not that quantum computer can outperform classical computers on all tasks. Many people now prefer using 'quantum advantage', but it's considered a weaker version of the previous term.

Research in quantum computer still has a long way to go. Some skeptics turn down the idea of a quantum computer on a large scale, for current problems in noise-canceling and system maintenance. However, generally speaking, we are at a point where we can be optimistic about the future of quantum computers. Besides, let's remind ourselves of classical computers in the 1950s. It can fill several rooms, use a tremendous amount of power, and is only used in scientific and military research. But years by years, it's getting smaller, yet more powerful. Quantum computer, likewise, is taking its first baby steps. Progress might not be significant, but it's still being made.

Reference

ColdFusion. "Quantum Computers - FULLY Explained!" *YouTube*, 27 May 2019,

[www.youtube.com/watch?v=PzL-oXxNGVM&list=PLNYP8Gh5s-](https://www.youtube.com/watch?v=PzL-oXxNGVM&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDRXrH&index=71&t=2s&ab_channel=ColdFusion)

[ruwk5YP67Z9JvqGNNDRXrH&index=71&t=2s&ab\\_channel=ColdFusion](https://www.youtube.com/watch?v=PzL-oXxNGVM&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDRXrH&index=71&t=2s&ab_channel=ColdFusion). Accessed 2 Nov.

2020.

Frame of Essence. "Will Quantum Computers Break Encryption?" *YouTube*, 5 Apr. 2017,

[www.youtube.com/watch?v=6H\\_9l9N3IXU&list=PLNYP8Gh5s-ruwk5YP-](https://www.youtube.com/watch?v=6H_9l9N3IXU&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=17&t=804s&ab_channel=FrameofEssence)

[67Z9JvqGNNDRXrH&index=17&t=804s&ab\\_channel=FrameofEssence](https://www.youtube.com/watch?v=6H_9l9N3IXU&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=17&t=804s&ab_channel=FrameofEssence). Accessed 2 Nov.

2020.

Google. "Demonstrating Quantum Supremacy." *YouTube*, 23 Oct. 2019,

[www.youtube.com/watch?v=-ZNEzzDclIU&list=PLNYP8Gh5s-ruwk5YP-](https://www.youtube.com/watch?v=-ZNEzzDclIU&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=64&t=84s&ab_channel=Google)

[67Z9JvqGNNDRXrH&index=64&t=84s&ab\\_channel=Google](https://www.youtube.com/watch?v=-ZNEzzDclIU&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=64&t=84s&ab_channel=Google). Accessed 2 Nov. 2020.

Haitjema, Mart. "Quantum Key Distribution - QKD." *Wustl.Edu*, 2 Dec. 2007,

[www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/](http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/).

Martinis, John. "Quantum Supremacy Using a Programmable Superconducting

Processor." *Google AI Blog*, 23 Oct. 2019, [ai.googleblog.com/2019/10/quantum-](https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html)

[supremacy-using-programmable.html](https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html)

minutephysics. "How Quantum Computers Break Encryption | Shor's Algorithm

Explained." *YouTube*, 30 Apr. 2019,

[www.youtube.com/watch?v=lvTqbM5Dq4Q&list=PLNYP8Gh5s-ruwk5YP-](https://www.youtube.com/watch?v=lvTqbM5Dq4Q&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=18&ab_channel=minutephysics)

[67Z9JvqGNNDRXrH&index=18&ab\\_channel=minutephysics](https://www.youtube.com/watch?v=lvTqbM5Dq4Q&list=PLNYP8Gh5s-ruwk5YP-67Z9JvqGNNDRXrH&index=18&ab_channel=minutephysics). Accessed 2 Nov. 2020.

## QUANTUM COMPUTING

Pednault, Edwin. "On 'Quantum Supremacy' | IBM Research Blog." *IBM Research Blog*, 22 Oct. 2019, [www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/](http://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/).

Savage, Neil. "Google's Quantum Computer Achieves Chemistry Milestone." *Scientific American*, 4 Sept. 2020, [www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/](http://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/).

TED-Ed. "Schrödinger's Cat: A Thought Experiment in Quantum Mechanics - Chad Orzel." *YouTube*, 14 Oct. 2014, [www.youtube.com/watch?v=UjaAxUO6-Uw&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=43&t=182s&ab\\_channel=TED-Ed](http://www.youtube.com/watch?v=UjaAxUO6-Uw&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=43&t=182s&ab_channel=TED-Ed). Accessed 2 Nov. 2020.

TED-Ed. "What Can Schrödinger's Cat Teach Us about Quantum Mechanics? - Josh Samani." *YouTube*, 21 Aug. 2014, [www.youtube.com/watch?v=z1GCnycbMeA&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=45&ab\\_channel=TED-Ed](http://www.youtube.com/watch?v=z1GCnycbMeA&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=45&ab_channel=TED-Ed). Accessed 2 Nov. 2020.

Thomas, Arun C. "Quantum Computing Explained!" *Medium*, 20 Jan. 2020, [towardsdatascience.com/quantum-computing-explained-a114999299ca](https://towardsdatascience.com/quantum-computing-explained-a114999299ca).

Veritasium. *Quantum Entanglement & Spooky Action at a Distance*. 12 Jan. 2015, [www.youtube.com/watch?v=ZuvK-od647c&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=46&t=117s&ab\\_channel=Veritasium](http://www.youtube.com/watch?v=ZuvK-od647c&list=PLNYP8Gh5s-ruwk5YP67Z9JvqGNNDXRrH&index=46&t=117s&ab_channel=Veritasium).

Wikipedia. "Quantum Computing." *Wikipedia*, 12 June 2020, [en.wikipedia.org/wiki/Quantum\\_computing#:~:text=Quantum%20computing%20is%20the%20use](https://en.wikipedia.org/wiki/Quantum_computing#:~:text=Quantum%20computing%20is%20the%20use). Accessed 2 Nov. 2020.

## QUANTUM COMPUTING

창하김. "BB84 Protocol of Quantum Key Distribution." *YouTube*, 8 Oct. 2019,

[www.youtube.com/watch?v=44G9UuB2RWI&t=173s&ab\\_channel=%EC%B0%BD%ED%9](https://www.youtube.com/watch?v=44G9UuB2RWI&t=173s&ab_channel=%EC%B0%BD%ED%9)

[5%98%EA%B9%80](#).