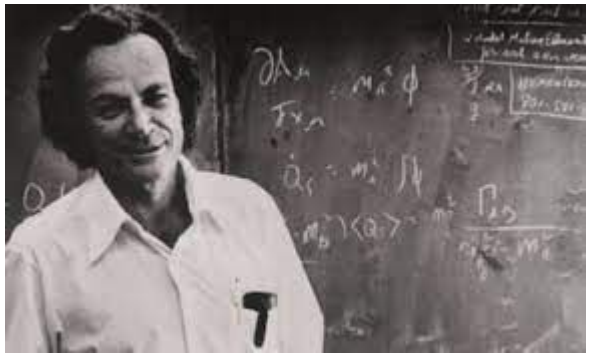
TA4

Arun Kumar Rajasekaran

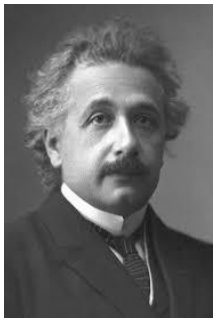
50 years ago, Nobel Prize-winner Richard Feynman argued that “nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical.”

Let’s look at a very short history of the evolution of quantum computing.



1905

Albert Einstein explains the photoelectric effect—shining light on certain materials can function to release electrons from the material—and suggests that light itself consists of individual quantum particles or photons.

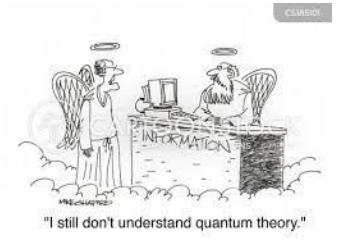


1924

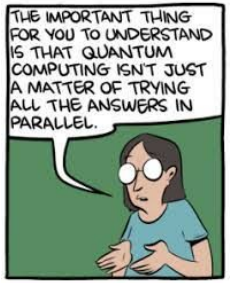
The term quantum mechanics is first used in a paper by Max Born

1925

Werner Heisenberg, Max Born, and Pascual Jordan formulate matrix mechanics, the first conceptually autonomous and logically consistent formulation of quantum mechanics



"I still don't understand quantum theory."



1925 to 1927

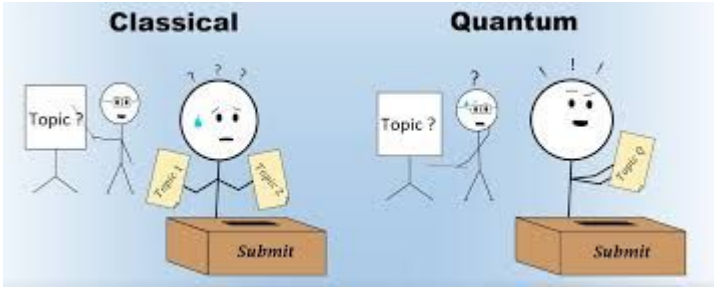
Niels Bohr and Werner Heisenberg develop the Copenhagen interpretation, one of the earliest interpretations of quantum mechanics which remains one of the most commonly taught

1930

Paul Dirac publishes The Principles of Quantum Mechanics, a textbook that has become a standard reference book that is still used today

1935

Albert Einstein, Boris Podolsky, and Nathan Rosen publish a paper highlighting the counterintuitive nature of quantum superpositions and arguing that the description of physical reality provided by quantum mechanics is incomplete



1935

Erwin Schrödinger, discussing quantum superposition with Albert Einstein and critiquing the Copenhagen interpretation of quantum mechanics, develops a thought experiment in which a cat (forever known as Schrödinger's cat) is simultaneously dead and alive; Schrödinger also coins the term "quantum entanglement"

1947

Albert Einstein refers for the first time to quantum entanglement as "spooky action at a distance" in a letter to Max Born

1976

Roman Stanisław Ingarden of the Nicolaus Copernicus University in Toruń, Poland, publishes one of the first attempts at creating a quantum information theory

1980

Paul Benioff of the Argonne National Laboratory publishes a paper describing a quantum mechanical model of a Turing machine or a classical computer, the first to demonstrate the possibility of quantum computing

1981

In a keynote speech titled Simulating Physics with Computers, Richard Feynman of the California Institute of Technology argues that a quantum computer had the potential to simulate physical phenomena that a classical computer could not simulate

1985

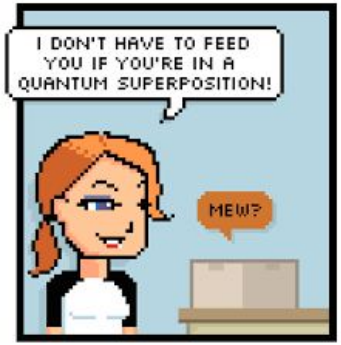
David Deutsch of the University of Oxford formulates a description for a quantum Turing machine

1992

The Deutsch–Jozsa algorithm is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm

1993

The first paper describing the idea of quantum teleportation is published



1994

Peter Shor of Bell Laboratories develops a quantum algorithm for factoring integers that has the potential to decrypt RSA-encrypted communications, a widely-used method for securing data transmissions

1994

The National Institute of Standards and Technology organizes the first US government-sponsored conference on quantum computing

1996

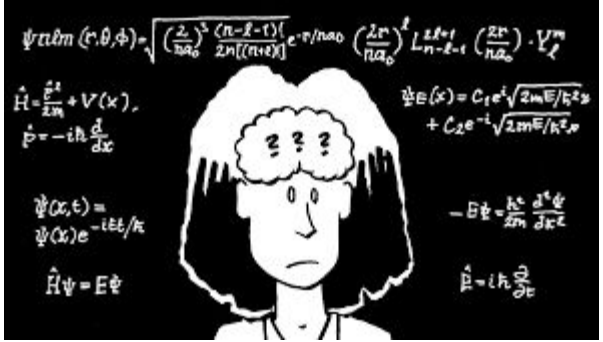
Lov Grover of Bell Laboratories invents the quantum database search algorithm

1998

First demonstration of quantum error correction; first proof that a certain subclass of quantum computations can be efficiently emulated with classical computers

1999

Yasunobu Nakamura of the University of Tokyo and Jaw-Shen Tsai of Tokyo University of Science demonstrate that a superconducting circuit can be used as a qubit



2002

The first version of the Quantum Computation Roadmap, a living document involving key quantum computing researchers, is published

2004

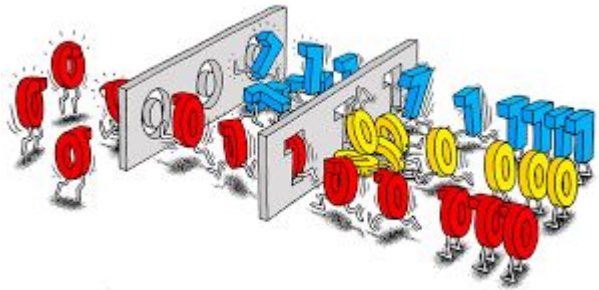
First five-photon entanglement demonstrated by Jian-Wei Pan's group at the University of Science and Technology in China

2011

The first commercially available quantum computer is offered by D-Wave Systems

2012

1QB Information Technologies (1QBit), the first dedicated quantum computing software company, is founded

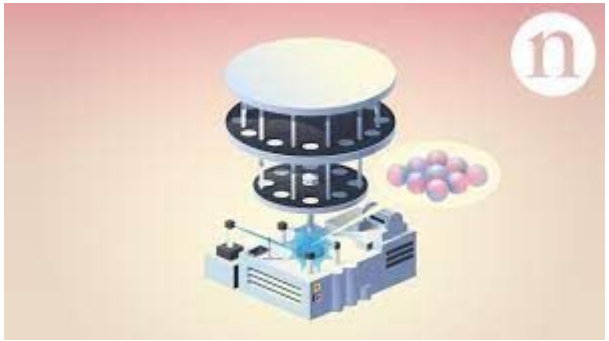


2014

Physicists at the Kavli Institute of Nanoscience at the Delft University of Technology, The Netherlands, teleport information between two quantum bits separated by about 10 feet with zero percent error rate

2017

Chinese researchers report the first quantum teleportation of independent single-photon qubits from a ground observatory to a low Earth orbit satellite with a distance of up to 1400 km



2018

The National Quantum Initiative Act is signed into law by President Donald Trump, establishing the goals and priorities for a 10-year plan to accelerate the development of quantum information science and technology applications in the United States

2019

Google claims to have reached quantum supremacy by performing a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete; IBM responds by suggesting it could take 2.5 days instead of 10,000 years, highlighting techniques a supercomputer may use to maximize computing speed

Importance of QC

“Everything we call real is made of things that cannot be regarded as real.”

Niels Bohr

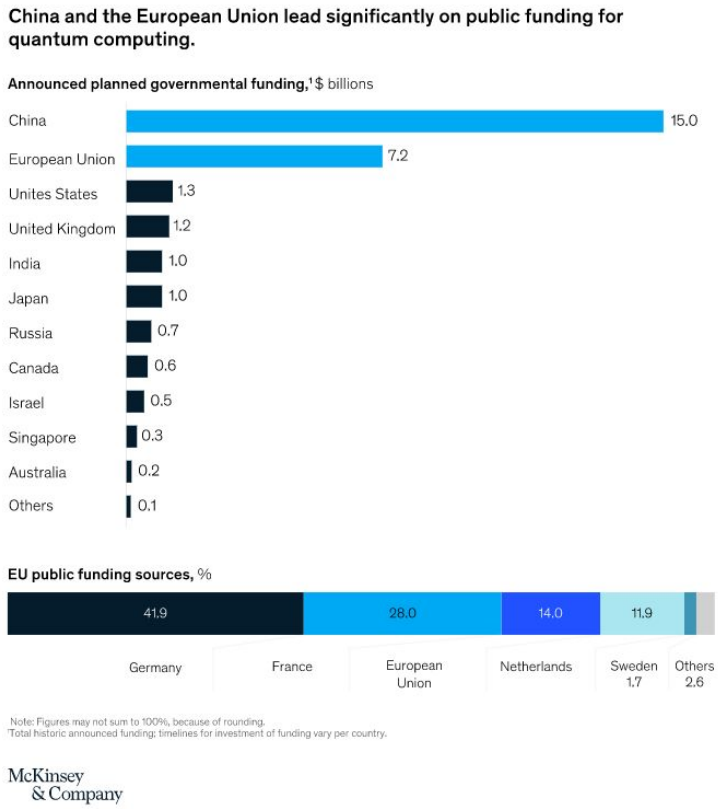
“I like to think the moon is there even if I am not looking at it.”

Albert Einstein

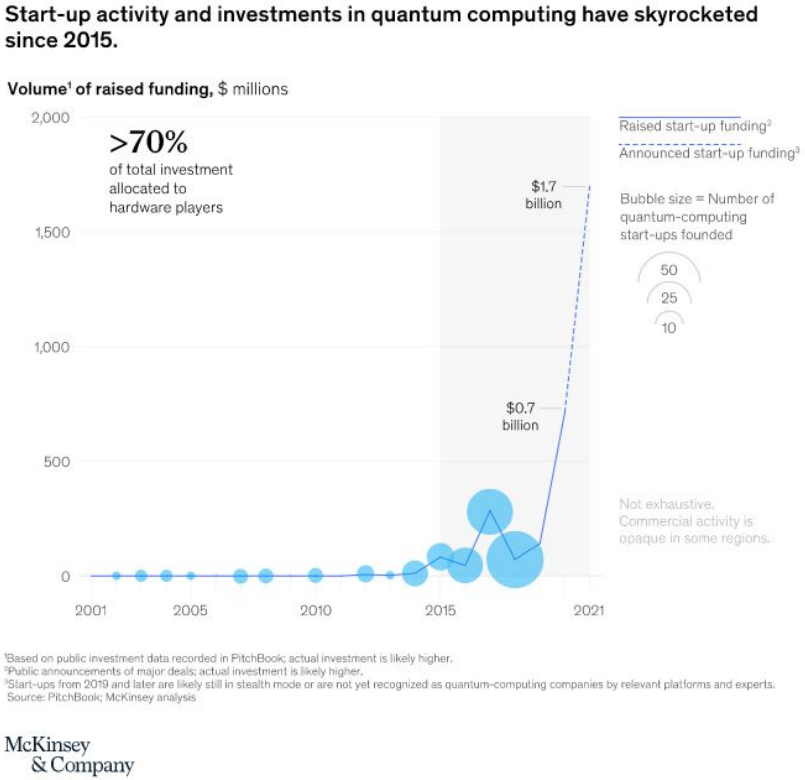
“The way we have to describe Nature is generally incomprehensible to us.”

Richard Feynman

Importance of QC

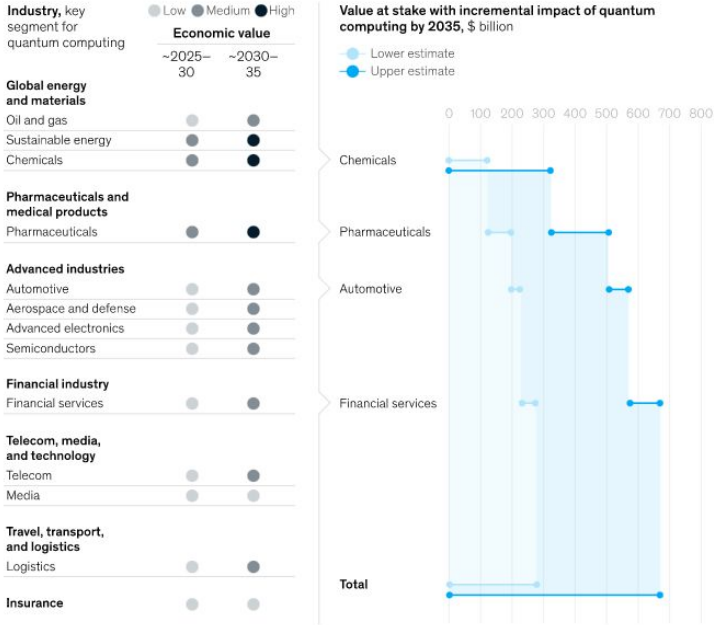


Importance of QC



Importance of QC

Conservatively, we estimate that the value at stake in pharmaceuticals, chemicals, automotive, and finance use cases could be up to nearly $700 billion.



Note: Viability and value of use cases is uncertain due to the immaturity of quantum-computing technology and the industry; given that business-value estimates are speculative and on the conservative side, they are intended to guide research toward areas of quantum applications with a high value potential, rather than to serve as definitive projections for business value.
Source: McKinsey analysis

Features of Quantum Computing

Features of Quantum Computing

Superposition and entanglement are two features of quantum physics on which quantum computing is based. They empower quantum computers to handle operations at speeds exponentially higher than conventional computers and with much less energy consumption.

- Superposition
- Entanglement
- Decoherence

Superposition

A qubit places the quantum information that it contains into a state of superposition. This refers to a combination of all possible configurations of the qubit. "Groups of qubits in superposition can create complex, multidimensional computational spaces. Complex problems can be represented in new ways in these spaces."

Entanglement

Entanglement is integral to quantum computing power. Pairs of qubits can be made to become entangled. This means that the two qubits then exist in a single state. In such a state, changing one qubit directly affects the other in a manner that's predictable.

Quantum algorithms are designed to take advantage of this relationship to solve complex problems. While doubling the number of bits in a classical computer doubles its processing power, adding qubits results in an exponential upswing in computing power and ability.

Decoherence

Decoherence occurs when the quantum behavior of qubits decays. The quantum state can be disturbed instantly by vibrations or temperature changes. This can cause qubits to fall out of superposition and cause errors to appear in computing. It's important that qubits be protected from such interference by, for instance, supercooled refrigerators, insulation, and vacuum chambers.

Limitations

- Decoherence, or decay, can be caused by the slightest disturbance in the qubit environment. This results in the collapse of computations or errors to them. As noted above, a quantum computer must be protected from all external interference during the computing stage.

- Error correction during the computing stage hasn't been perfected. That makes computations potentially unreliable. Since qubits aren't digital bits of data, they can't benefit from conventional error correction solutions used by classical computers.

- Retrieving computational results can corrupt the data. Developments such as a particular database search algorithm that ensures that the act of measurement will cause the quantum state to decohere into the correct answer hold promise.

- Security and quantum cryptography is not yet fully developed.

- A lack of qubits prevents quantum computers from living up to their potential for impactful use. Researchers have yet to produce more than 128.

Simulating Qubits

Qubits are the basic units of the quantum memory which, in contrast to classical bits that can be either 0 or 1, can hold both 0 and 1 state thanks to superposition. For example, 8 classical bits are enough to represent any number between 0 and 255. On the other hand 8 qubits can represent all numbers between 0 and 255 at the same time.

There are different approaches with different pros & cons to simulate qubits. These include:

1. Photonics

Photons have a natural isolation property due to their weak interactions with the surrounding environment, which makes them a great candidate to carry information, represent qubits, and operate at room temperature. Another advantage is that photonic quantum computers can be integrated into existing fiber optic-based telecommunications infrastructure.

However, one of the challenges that face photonic quantum computing is the limitations in fault tolerance and error correction.

Current companies developing photonic quantum computing technology include PsiQuantum, Xanadu, and the Amazon Quantum Solutions Lab.

2. Trapped ions

Quantum hardware that uses trapped ion qubits typically rely upon microwave or optical signals transmitted through free space or waveguides and delivered to the location of the qubits. Current QC prototypes of trapped-ion consist of a chain of 5 to 20 static ions in a single potential well. Challenges that face trapped-ion systems are:

the difficulty of isolating individual ion motions as chain length increases

the number of ions one can individually address with gate laser beams

measuring individual qubits

Current companies that work on ion-trapped quantum technologies include Honeywell and IonQ,

3. Semiconducting material

Qubits can be simulated by manipulating individual electrons in semiconducting materials such as selenium or germanium, or defected materials such as diamonds, aluminum nitride or silicon carbide. Applying microwaves and magnetic fields to these materials will allow them to exhibit superposition, entanglement, and other quantum properties.

Companies that rely on semiconducting technology for their QCs include Intel, Google, and IBM

4. Superconducting material

Superconducting qubit systems are controlled using microwave and low-frequency electrical signals, both of which are communicated through wires that run into cooling refrigerators to reach the qubits inside the controlled environment. In 2018, Intel announced the construction of a 49 qubit superconducting chip called Tangle Lake.

Some more related terms: 1. Quantum reversible gates

A reversible gate is the one whose input can be reconstructed just by looking at the output. For example, in classical computation the NOT inverter gate is reversible, whereas the XOR gate is irreversible because inputs cannot be identified by looking at the output. It is necessary for quantum gates to be reversible because quantum mechanics is reversible and quantum operations are unitary. Unitary operations are such that their inverses are also their conjugates.

Logical reversibility allows for:

Reversing quantum circuits: by applying the sequence of ’inverse’ quantum gates in reverse order to the output.

Reducing computational power: since each input is associated with a unique output, no qubit can be erased. Therefore, no energy would be lost during computation.

QPU

A quantum processing unit (QPU) is a computational unit that relies on quantum principles to perform a task. the QPU includes the:

QRAM (register + gates)

Quantum control unit (QCU) which drives the system to the desired state.

Classical controller interface which defines the interaction between the host CPU and the QPU

How to interact with the quantum computer?

To program a quantum computer, the programmer will send the algorithms via a host system, typically called “host processor”. A host processor is a classical computer which has a high bandwidth connection to the QCU. The host runs a conventional operating system to allow the user interaction with the quantum processor.

List of companies involved

https://builtin.com/hardware/quantum-computing-companies

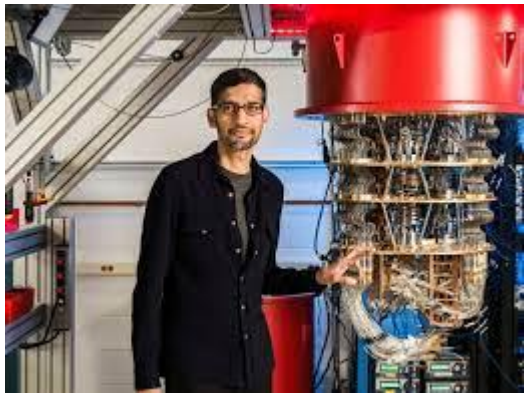
https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication

Key players

Google

Google is spending billions of dollars to build its quantum computer by 2029. The company opened a campus in California called Google AI to help it meet this goal. Once developed, Google could launch a quantum computing service via the cloud.

Cirq



Key players

IBM

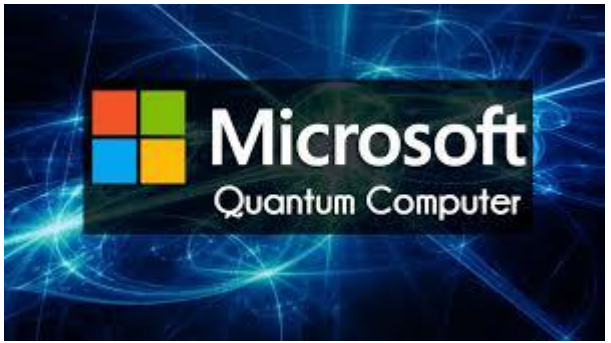
IBM plans to have a 1,000-qubit quantum computer in place by 2023. For now, IBM allows access to its machines for those research organizations, universities, and laboratories that are part of its Quantum Network.

Qiskit

Key players

Microsoft

Microsoft offers companies access to quantum technology via the Azure Quantum platform.



Quantum Computer vs. Classical Computer

Quantum computers and classical computers process information differently. A quantum computer uses qubits to run multidimensional quantum algorithms. Their processing power increases exponentially as qubits are added. A classical processor uses bits to operate various programs. Their power increases linearly as more bits are added. Classical computers have much less computing power.

Quantum Computer vs. Classical Computer

Quantum computers have a more basic structure than classical computers. They have no memory or processor. All a quantum computer uses is a set of superconducting qubits.

Quantum Computer vs. Classical Computer

Classical computers are best for everyday tasks and have low error rates. Quantum computers are ideal for a higher level of task, e.g., running simulations, analyzing data (such as for chemical or drug trials), creating energy-efficient batteries. They can also have high error rates.

Quantum Computer vs. Classical Computer

Quantum computers are more expensive and difficult to build than classical computers.

Quantum Computer vs. Classical Computer

Classical computers don't need extra-special care. They may use a basic internal fan to keep from overheating. Quantum processors need to be protected from the slightest vibrations and must be kept extremely cold. Super-cooled superfluids must be used for that purpose.

Applications

Chemistry and Chemical engineering

Chemical and biological engineering involve the discovery and manipulation of molecules. Doing so involves the motion and interaction of subatomic particles. In other words, it involves quantum mechanics.

As molecules get more complex, the number of possible configurations grows exponentially. It becomes a combinatorics calculation, suitable for a quantum computer.

This ability means that quantum computers will play an important role in accelerating current efforts in materials discovery and drug development.

Chemical and biological engineering

Cao, Yudong, et al. "Quantum chemistry in the age of quantum computing." Chemical reviews 119.19 (2019): 10856-10915.

Ajagekar, Akshay, and Fengqi You. "New frontiers of quantum computing in chemical engineering." Korean Journal of Chemical Engineering 39.4 (2022): 811-820.

Andersson, Martin P., et al. "Quantum computing for chemical and biomolecular product design." Current Opinion in Chemical Engineering 36 (2022): 100754.

Yuan, Xiao. "A quantum-computing advantage for chemistry." Science 369.6507 (2020): 1054-1055.

Biomedical engineering

Parsons, Donald Frederick. "Possible medical and biomedical uses of quantum computing." Neuroquantology 9.3 (2011).

Marchetti, Laura, et al. "Quantum computing algorithms: getting closer to critical problems in computational biology." Briefings in Bioinformatics 23.6 (2022): bbac437.

Ragab, Mahmoud, et al. "Mathematical Modelling of Quantum Kernel Method for Biomedical Data Analysis." Computers, Materials & Continua 71.3 (2022).

Physics

Meyer, David A. "Quantum computing classical physics." Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 360.1792 (2002): 395-405.

Nakahara, Mikio. Lectures on quantum computing, thermodynamics and statistical physics. Vol. 8. World Scientific, 2013.

Vandersypen, Lieven MK, and Mark A. Eriksson. "Quantum computing with semiconductor spins." Physics Today 72.8 (2019): 38-45.

Cyber security

Combinatorics have been central to encryption for over a thousand years. Al-Khalil's 8th century Book of Cryptographic Messages looked at permutations and combinations of words. Today's encryption is still built on combinatorics, emphasizing the assumption that combinatoric calculations are essentially unmanageable.

With quantum computing, however, cracking encryption becomes much easier, which poses a threat to data security. A new industry is growing that helps companies prepare for upcoming vulnerabilities in their cybersecurity.

Cyber security

Today's RSA encryption, a widely used form of encryption, particularly for sending sensitive data over the internet, is based on 2048-bit numbers. Experts estimate that a quantum computer would need to be as large as 70 million qubits to break that encryption. Considering the largest quantum computer today is IBM's 53-qubit quantum computer, it could be a long time before we're breaking that encryption.

As the pace of quantum research continues to accelerate, though, the development of such a computer within the next 3-5 years cannot be discounted. As an example, earlier this year, Google and the KTH Royal Institute of Technology in Sweden reportedly found "a more efficient way for quantum computers to perform the code-breaking calculations, reducing the resources they require by orders of magnitude." Their work, highlighted in the MIT Technology Review, demonstrated that a 20 million-qubit computer could break a 2048-bit number – in a mere 8 hours.

Cyber security

Brijwani, Geeta N., Prafulla E. Ajmire, and Pragati V. Thawani. "Future of Quantum Computing in Cyber Security." Handbook of Research on Quantum Computing for Smart Environments. IGI Global, 2023. 267-298.

Ali, Arshad. "A Pragmatic Analysis of Pre-and Post-Quantum Cyber Security Scenarios." 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST). IEEE, 2021.

Kaur, Jagpreet, and K. R. Ramkumar. "The recent trends in cyber security: A review." Journal of King Saud University-Computer and Information Sciences 34.8 (2022): 5766-5781.

Good Blogs/Articles to explore

- Quantum Computing for the Very Curious, Andy Mathushak & Micheal Nielsen

(https://quantum.country/qcvc)

- Qiskit textbook, IBM

(https://qiskit.org/textbook/content/ch-ex/)

- Guide to Quantum Computing, WIRED

(https://www.wired.com/story/wired-guide-to-quantum-computing/)

- Quantum Computing, IBM

(https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/)

Good Blogs/Articles to explore

- Quantum-Computation and Applications, Bhupesh Bishnoi, 2020, arXiv preprint

(https://arxiv.org/abs/2006.02799)

- Quantum Computing: Lecture Notes, Ronald de Wolf, 2019

(https://arxiv.org/abs/1907.09415)

- A Gentle Introduction to Quantum Computing Algorithms with Applications to Universal Prediction, Elliot Catt and Marcus Hutter, 2020

(https://arxiv.org/abs/2005.03137)

- Quantum computing from a mathematical perspective: a description of the quantum circuit model, J. Ossorio-Castillo and José M. Tornero, 2018

(https://arxiv.org/abs/1810.08277)

- A course in Quantum Computing, Michael Loceff, 2015

(https://lapastillaroja.net/wp-content/uploads/2016/09/Intro_to_QC_Vol_1_Loceff.pdf)