All Actuaries Summit
New age, new actuary

11-13 June 2025, Sydney

Quantum Computing

Prepared by Dr Anthony Lowe and Dr Michael Walker

Presented to the Actuaries Institute
2025 All-Actuaries Summit
11-13 June 2025

Actuaries Institute
ABN 69 000 423 656
Level 2, 50 Carrington Street, Sydney NSW 2000
P +61 (0) 2 9239 6100 | actuaries.asn.au

Quantum Computing

Anthony Lowe and Michael Walker

Abstract

Quantum computing is expected to revolutionise the way we use data and computation – from breaking current cybersecurity keys used in banking and other applications to enormously speeding up computationally intensive calculations such as optimising investment portfolios.

But given how far away we are from working quantum computers, a decade or more, should we already be concerned that quantum computers will be able to break current encryption protocols? What sorts of actuarial calculations are most likely to benefit from quantum computing?

In this paper, we explore the key concepts of quantum computing – superposition, entanglement, no cloning, and quantum error correction; discuss the various approaches to and practical challenges of building working quantum computers; cover quantum algorithms and the future of programming quantum computers; and discuss the immediate implications of quantum computing on cybersecurity.

Keywords: quantum computing, quantum algorithms, cybersecurity, data science

Key concepts of quantum computing

Introduction

From a practical perspective it is sufficient to understand that quantum computing is based on different mathematical principles from conventional, or classical, computing. Quantum computers represent data differently from classical ones and perform different operations on them. We elaborate on this below. These differences in data representation and manipulation allow quantum computers to run different algorithms, algorithms not available to classical computers, and some of these quantum algorithms are useful. It is not the case that quantum computers do everything faster or even better, but they may perform certain specific tasks better or faster where a quantum algorithm is known.

Classical computing

In classical computing, which actuaries are familiar with, information (e.g., a number or letter) is represented by bits which have the value 0 or 1. A modern PC uses 64 bits in parallel. The bits are manipulated by logic gates to perform calculations. The gates are boolean operators, e.g., AND, OR and NOT, and the manipulations are performed sequentially, thousands of millions of times a second. The computer is built using billions of transistors and other components fabricated on small semiconductor chips.

Qubits and superposition

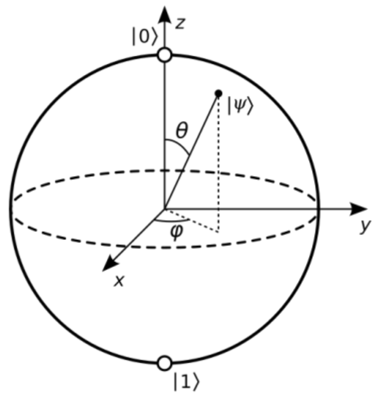
In quantum computers, information is represented by qubits which are quantum states of a system that can have two values. Common examples are electrons which have a quantum property called spin that is either -1/2 (down) or +1/2 (up), and photons, which have either vertical (V) or horizontal (H) polarisation.

The electron's state |ψ> can be represented mathematically as the linear combination of the down and up states as follows:

|ψ> = α |↓> + β |↑>

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$.

A qubit's state space can be visualised as a sphere, known as the Bloch sphere:



The linear combination is known as a superposition of the two states. In some sense, the electron is simultaneously in the down and up states. However, when we measure which state the electron is in, we will either get the answer down with probability $|\alpha|^2$ or up with probability $|\beta|^2$.

This is the same as the famous Schrödinger's Cat thought experiment where in some sense the cat in the box is simultaneously alive and dead but, when we open the box to take a look, the cat must be *either* alive *or* dead. Schrödinger originally developed this thought experiment to show that the standard, or Copenhagen, interpretation of quantum mechanics led to an absurd result, but it is now used to illustrate that quantum systems behave in very different ways to classical ones.

Quantum entanglement

An important feature of quantum systems called entanglement is also a feature of quantum computers. We can illustrate entanglement using the following example: suppose we have a neutral, spinless elementary particle – say a pion – which is stationary, and that the pion decays into an electron and positron. The electron and positron will fly away from each other in opposing directions.

$$e^- \longleftarrow \pi^0 \longrightarrow e^+$$

To conserve angular momentum, one must have spin down and the other spin up so that the combined system has zero spin like the pion before it decayed. If we measure the spin of the electron and find it is down and then immediately measure the spin of the positron, it must be up, and vice versa. In other words, entanglement ensures that the electron and positron are always found to have opposite spins.

Entanglement can also occur between qubits. Consider two qubits in the state $|\psi\rangle = \alpha\,|{\downarrow\downarrow}\rangle + \beta\,|{\uparrow\uparrow}\rangle$. We see that the state of the two qubits is restricted to components where the qubits have the same spin, so knowing the measured value of one qubit immediately gives us the measured value of the other. Indeed, measuring the state of one qubit without disturbing the other, which is possible with some quantum computing technologies, would still leave the unmeasured qubit in a pure state corresponding to the outcome of the measured qubit.

Interestingly, the effects of measurement between entangled particles are apparently instantaneous since the measurement correlations will always hold no matter how far apart the particles/qubits are in space and no matter how close in time.

Einstein didn't like this at all – he called it "spooky action at a distance" – and argued that the spin states of the electron and positron must be determined at the time of the decay by so-called hidden variables. Unfortunately for Einstein, experiments have shown that quantum entanglement is real and that hidden variables do not exist. Entanglement is important because it allows qubits to control operations on other qubits, permitting fine control over which components are included in qubits' states.

No cloning

A third important aspect of quantum computing is that it is impossible to make an independent and identical copy of a qubit unless its state is already known. This is quite different to classical computing where it is common to create identical copies of bits, e.g., the intermediate result of a calculation. No cloning has important implications for error correction in quantum computing.

Quantum gates and circuits

Qubits are manipulated using quantum gates – such as the controlled NOT (CNOT), Hadamard (H), and Toffoli (CCNOT) gates – which are analogous to classical gates. For example, the Hadamard gate manipulates a qubit in a known down or up state into a superposition which is equally up and down:

$$|{\downarrow}\rangle \;\text{——}\; H \longrightarrow \; 1/\sqrt{2}\,(|{\downarrow}\rangle + |{\uparrow}\rangle)$$
$$|{\uparrow}\rangle \;\text{——}\; H \longrightarrow \; 1/\sqrt{2}\,(|{\downarrow}\rangle - |{\uparrow}\rangle)$$

i.e., if we measure the known down or up qubit after it has passed through the Hadamard gate, the result will be down half the time and up half the time.

However, there are two key differences between classical and quantum gates. First, quantum gates are reversible which means that we can deduce the input from the output. Some classical gates such as NOT are reversible (if we know the output is 1 then the input is 0 and vice versa) but others, such as AND, are not (if we know the output is 0, we have no way of knowing if the input was 0,0; 0,1 or 1,0). Reversing the calculation helps with error correction and optimising calculation efficiency.

The second difference is that the operation of certain gates can lead to entanglement of the output qubits speeding up the computation.

Most quantum computers use circuits based on quantum gates like the electronic circuits based on boolean gates used in classical computers. Quantum algorithms use quantum circuits to manipulate qubits and perform calculations, but it should be noted this not the only approach discussed by researchers.

Adiabatic quantum computing

Another approach called adiabatic quantum computing defines an energy operator, called a Hamiltonian, which describes the problem and has the desired solution as its lowest energy state. The quantum computer is initialised to be all zeros and then the Hamiltonian is applied with gradually more strength so that the qubits move into the lowest energy state over time. This approach was one of the first to be made commercially available as a cloud service by D-Wave[1]. It is an effective approach for some problems but is a bit slow.

How do quantum computers provide an advantage over classical computers?

Quantum computers do not run faster than classical computers, in fact if we measure in operations per second they are typically slower. Their ability to complete certain tasks in less time or better in some other way comes from their representation of data, and the operations they can perform on it, being more general. By this we mean that the classical bit values of 0 and 1 are special cases of the states available to a qubit which are not only |0> and |1> but everything in between as represented by the superposition equation. Furthermore, because the coefficients α and β are complex, this introduces an additional degree of freedom which makes the space of possible values a Bloch sphere, instead of a line segment. Readers with a physics or engineering background may recognise this as a phase.

The generalisation of operations possible with a quantum computer follows from this. Whereas a classical computer can only flip values, perhaps conditionally, between 0 and 1 the quantum computer can rotate the Bloch sphere arbitrarily to perform partial swaps, as well as rotations about the z-axis corresponding to phase changes. These additional operations acting in a more general space allow quantum computers to follow algorithmic paths unavailable to classical computers, effectively taking shortcuts. Some of these shortcuts can be interpreted as parallelism, often referred to as quantum parallelism when a multitude of values in superposition are acted on simultaneously. Others lack such an intuitive picture despite being equally important.

Computational complexity

In computing, calculations – irrespective of the hardware on which they are made – can be classified in terms of difficulty by the number of steps (or, equivalently, time) required to complete the calculation.

Suppose we have a calculation with input length n. If the calculation can be completed in $\leq kn^p$ steps for every value of n, then it is said to be polynomial (complexity class P) and is regarded as tractable by classical computers. Calculations that require more steps or time than this are said to be intractable. For an important class of calculations the number of steps grows in proportion to the number required already. Such calculations are said to be exponential.

If we have n qubits all in the down state

$$|\psi_n\rangle = |\downarrow\downarrow \ldots \downarrow\rangle$$

and apply the Hadamard gate to each, then we create a new state with 2^n combinations – i.e., a linear combination of operators produces a state with an exponential number of values.

If we apply this concept to a calculation, each potential state can represent a solution to our problem, i.e., quantum superpositions (and entanglement) enable quantum parallel processing. Although, of course, if we measure the state, then we will get a single result with a certain probability, and the other states will be lost.

Actuarial calculations most likely to benefit from quantum parallelism are those involving sparse matrices and combinatoric calculations. Solving the Black-Scholes equation is also likely to benefit for reasons discussed below. Quantum machine learning is beginning to look promising.

Approaches and challenges to building a working quantum computer

Up to this point, everything we have discussed has been theory developed by mathematicians and theoretical physicists, such as Richard Feynman, who first proposed the idea of quantum computing.

But how do we go about building a working quantum computer? The field is still very experimental, and a wide range of approaches are currently being explored. The two most common physical properties which are exploited are spin and polarisation.

The most well-known approaches in Australia are quantum dots, pioneered by Professor Michelle Simmons and her group at UNSW, and that of US photonics company, PsiQuantum. Recently, the Commonwealth and Queensland governments invested A$940 million in PsiQuantum to build a quantum computer in Brisbane.

Photonics quantum computers are based on the polarisation of light (photons). Another approach utilises the spin of trapped ions. Ions are atoms that are missing or have an additional electron which can then be confined using electromagnetic fields and manipulated using lasers.

Unfortunately, qubits don’t just interact with each other, they interact with the wider environment, degrading the quantum states and introducing errors in a process known as decoherence.

Decoherence increases with temperature and time, both of which pose substantial challenges. Most current quantum computers operate at a temperature close to absolute zero (-273 Celsius) to reduce thermal noise and maintain the coherence of the qubits. The practical implication is that whilst qubits themselves may be small, the equipment currently needed to set up and manipulate them is large and expensive.

Another implication of decoherence is that error correction will be important for quantum computers, and this is a major area of research. Error correction allows clusters of qubits to correct errors and reduce the impacts of decoherence. In practice this means that every logical or effective qubit, as conceived in the design of a quantum algorithm, requires many, perhaps hundreds or even a thousand physical qubits.

Currently, the most advanced quantum computers have 10s of physical qubits and are large and expensive. To be of practical use, they would need many times this number, perhaps millions of physical qubits, equating to thousands of logical qubits.

There is a lot of investment going into research and development of quantum computers, but it is difficult to predict when a key breakthrough may occur. However, it will likely be many decades before we have quPhones in our pockets!

The data loading bottleneck

One of the most practical challenges for actuarial applications of quantum computing is efficiently loading classical data into quantum systems. Actuarial work often involves very large datasets that would need to be encoded into quantum states.

Current approaches like Quantum Random Access Memory (QRAM) remain theoretical, and existing data loading methods require time proportional to dataset size, resulting in decoherence of the qubits and potentially negating quantum speedups. This means that even if quantum algorithms offer exponential advantages for computation, the practical benefits may be limited by data transfer constraints.

Promising strategies to address this include:

- Hybrid classical-quantum systems where data preparation occurs classically
- Quantum feature maps that efficiently encode only the most relevant features
- Compression techniques optimised for actuarial datasets.

Classical machine learning might also be used to ameliorate this problem[2].

Until these challenges are resolved, quantum applications may need to focus on problems with smaller data requirements or those where data can be generated within the quantum system itself.

Quantum Algorithms

Historical context

Actuaries are familiar with coding on PCs in high-level programming languages such as Python, but it wasn’t always like that.

The first digital programmable computer, Colossus, built in the UK in 1944, used thermionic valves and was programmed using switches and patch wiring – there were no programming languages as such back then. It occupied almost a whole room at Bletchley Park where it was assembled.

Fast forward 80 years to today and most of us carry a computer many times more powerful than Colossus in our pocket in the form of smartphones. Incidentally, they are also far more advanced than those onboard the Apollo spacecraft that took astronauts to the moon in the 1960s and 1970s.

The present situation with quantum computers is analogous to Colossus. They are currently large, not very powerful and don’t have high-level, general purpose programming languages. However, just as with classical computers, we can reasonably expect that all that will change over time, and we will eventually have much more powerful (quantum) computers than we do today.

We are also still at the beginning of knowing how to program quantum computers. Programming languages for quantum computers, qiskit and QASM being the best known, currently require the coder to think at the level of qubits and explicitly apply gates to them, unlike classical computing languages where the coder need only declare a variable and act on that, knowing that the allocation of bits and the actions upon them are taken care of by the compiler. That being said, quantum computing libraries increasingly contain well known quantum algorithms and even quantum machine learning methods as declared methods which the coder may call instead of having to code them from scratch.

Many quantum algorithms are concerned with optimisation problems, offering improvements in either speed or accuracy. Quantum optimisation algorithms typically avoid local minima/maxima naturally and effectively explore the entire solution space in parallel. Quantum algorithms offering improvements in runtime include the optimisation of database queries, where the time taken by the query is very sensitive to the order in which the forms are accessed. Quantum query optimisation algorithms are expected to offer a quadratic speedup over classical ones[3].

The best-known quantum algorithms are the first two to be developed, Shor's and Grover's algorithms:

Shor's algorithm

In 1994, mathematician Peter Shor devised an algorithm[4] that exponentially speeds up the factorisation of large semiprime numbers relative to the fastest known classical algorithm. Shor's algorithm was the first to show that quantum computers could, in theory, exponentially speed up certain calculations and has been a major driver behind interest and investment in quantum computing.

Shor's algorithm is based on a technique called quantum Fourier transforms. These are the quantum analogues of the discrete Fourier transforms that are used extensively in digital signal and image processing and many other fields. An application that most of us are familiar with is processing and editing images taken with digital cameras. The Fourier transform gives the frequency distribution of a signal or image – similar to analysing the harmonics of a note played on a musical instrument.

Grover's algorithm

In 1996, computer scientist Lov Grover devised an algorithm[4] for searching unsorted databases; for example, searching a database of names in random order to find the email address of a colleague. Grover's algorithm uses a technique called quantum amplification in which the state we are looking for (the colleague's name in our example) is amplified so that it has a high probability when we make the measurement of the quantum system.

Grover's algorithm quadratically speeds up the search. When used in a brute force attack to break an encryption the length of the key or hash is effectively halved. However, given the time taken to set up the initial qubits, this may mean, in practice, that it doesn't find the answer faster than a classical computer. In fact, the algorithm's true value is that it can extract a desired result from a superposition, thus making a range of quantum algorithms useful which would not be otherwise.

It is important to note from these two examples that quantum algorithms don't uniformly increase calculation speed over classical computing, and for some calculations may not improve it at all. Other calculations will, however, be completed much faster on quantum computers.

Other quantum algorithms

The QUBO (Quadratic Unconstrained Binary Optimisation) algorithm will efficiently solve quadratic optimisation problems, of great importance in portfolio optimisation[5].

The branch-and-bound algorithm is used for optimising subject to constraint. It does this by constructing a binary tree of possible solutions subject to strict ordering conditions. Its quantum version[6] uses a quantum tree algorithm to enhance the search and has been shown to reduce the runtime by a power of approximately one half, (square root).

Quantum annealing is a potentially general method for solving functions in which the register starts in a |0> state and is subjected to a Hamiltonian whose final solution is the optimal input for the function of interest[7]. This is conceptually similar to adiabatic quantum computing with the important difference that annealing is gate-based with operations occurring at discrete times while adiabatic quantum computing is inherently slow, gradual and does not use discrete gates.

No discussion of optimisation or equation solving is complete without solving linear equations. One quantum algorithm, HHL (named for its discoverers), will solve sparse linear equations with exponential speedup over classical methods. If we define the equation A|x> = |b> where A is a sparse matrix and |b> is a vector of known values, then the HHL algorithm will find |x>.

There are two caveats, however. The first is that this assumes prior construction of the state vector |b>, which can be demanding for a quantum computer. The other is the complement of this, that the output of HHL is a quantum state vector and only one component is returned upon measurement. This is fine if sampling from the solution is acceptable or for applications which then feed |x> to another algorithm but encoding |b> at the beginning and sampling the entirety of |x> are each capable of offsetting this advantage so useful applications are limited[8].

For graph-theoretic and other combinatorial optimisation problems, of which the best known is the travelling salesman problem, there is QAOA (Quantum Approximate Optimisation Algorithm)[4]. QAOA offers faster runtimes compared to conventional methods and currently receives a lot of attention because its hardware-efficient nature gives it a better chance of being useful on nearer term quantum computers.

Interestingly, the Black-Scholes equation, the stock tool for pricing derivatives and similar financial products, can be interpreted as a special case of the Schrödinger equation, which describes the behaviour of fundamental particles, and numerically solved on a quantum computer, yielding more accurate results than conventional calculations[9].

Partial differential equations

Solving partial differential equations is central to finance and to many areas of science. An efficient quantum algorithm for solving PDEs has been published with a one-hundred-fold improvement in accuracy over classical methods[10].

Quantum Machine Learning

Current conventional machine learning algorithms all have their quantum computing equivalents, early work in quantum machine learning being driven by the hope of faster performance. However, while fewer training runs are typically needed for the models to converge this is effectively offset by the slower gate times and the advantages of quantum machine learning over classical lie in greater accuracy and stability of out against perturbations in the testing data[11].

The development of machine learning models was impeded for several years by so-called barren plateaus, regions in parameter space where the parameter gradients vanish too rapidly for the model to optimise them. This may be understood as the catch of the internal space doubling in capacity with every additional qubit. The problem was tamed by learning to see a quantum circuit as a sequence of operators which combine to form an algebra which characterises the circuit. A simple approach to avoiding barren plateaus is to add more parameters than there are generators in the characteristic algebra[12]. Indeed, results indicate that quantum algorithms tolerate and even benefit from over-parameterisation while classical ones will either overfit or, as is the case with deep multi-layer networks, need large amounts of data to train.

Results in quantum machine learning research indicate resistance to over-fitting and trainability on fewer samples for circuits of similar complexity and models with the same number of parameters. Another approach is to construct the quantum circuit in such a way that its generating operators respect the symmetry of the input data[13]. While effective, this approach limits the generality of the model.

Techniques like these, and others yet to be developed, may ultimately lead to more generalised approaches to quantum programming.

Cybersecurity

Whilst commercially useful quantum computers are still a decade away by most expert estimates, that does not mean organisations can afford to wait to act. Organisations that do not start preparing now will face significant cybersecurity risks in the future.

Almost all the transactions routinely taking place over the internet rely on encryption to protect privacy and sensitive data. Modern encryption relies on mathematical problems which are difficult to solve but easy to verify. For example, a commercial website encrypts credit card details to prevent third parties reading them. This particular encryption, called public key or asymmetric encryption, involves a large prime number which is kept as a private key while one of its large multiples combined with other data form a key which is shared publicly. The encryption can be broken by factoring the large multiple to identify the private key, but this is too difficult for a conventional computer to do in reasonable time. Even if a sufficiently powerful computer is built, the keys need only be made a bit larger to render decryption too difficult again. In fact, the larger the key the greater the effect of increasing its size so that currently the advantage always lies with the encryptor.

All this will change when hackers gain access to sufficiently powerful quantum computers. The properties of quantum computers allow them to run algorithms not accessible to conventional computers. Shor’s algorithm, and its subsequent refinements, allow a large number to be factored into prime numbers with a relatively small number of steps which increases only slowly as we move to larger encryption keys. It therefore provides an exponential speedup over classical algorithms.

A lot of modern encryption will consequently be breakable in the not-so-distant future when cryptographically relevant quantum computers become available. Fortunately, “post-quantum” encryption algorithms have already been developed based on different mathematical problems which neither conventional nor quantum computers can solve efficiently.

The US National Institute of Standards and Technology has recommended four standards (Federal Information Processing Standards 203, 204, 205 and 206) based on new post-quantum encryption methods believed to be secure against quantum computers to be implemented by 2035[14]. These new standards are designed for different types of secure digital transactions. It should be noted that the new standards will require more processing power than current methods to avoid significantly degrading transaction speeds. Similar recommendations have been made by the Australian Signals Directorate to be implemented by 2030[15] and the European Commission has encouraged Member States to develop coordinated standards[16].

However, there is considerable debate about whether the mandated implementation time frames are too lenient.

Few organisations outside of the cybersecurity industry appreciate that transitioning to new encryption standards will be a long, time-consuming process which cannot be completed at short notice. Previous mandated encryption upgrades have taken many years and ran over time. Post-quantum cryptography (often referred to as PQC) will need to be implemented before the availability of quantum computers if sensitive data is to be protected.

The early availability of quantum computers is likely to follow a similar pattern to that of conventional computers, with a few expensive-yet-primitive models available only to the well-resourced with availability and cost improving slowly over time. And while progress on commercially developed quantum computers is loudly announced the acquisition of a cryptographically relevant quantum computer by a rogue government or organisation will not be. They will simply use it, leaving the data breach undetectable until after its harm has been done.

The situation is particularly urgent for organisations whose data is likely to remain sensitive up to 7 to 15 years into the future. Aspiring hackers, typically supported by rogue states and similar, are already running harvest-now-decrypt-later attacks. As the name suggests, this means copying data in transit and storing it until the advent of cryptographically relevant quantum computing. If your organisation uses data sensitive for that long, then your transition to post-quantum cryptography is already running late!

The process of upgrading to post-quantum cryptography begins with a thorough audit of all the encryption-related processes and encrypted data throughout the organisation. Most organisations have never performed such an audit or even have a checklist to work through. Achieving this level of cyber-maturity in an organisation is worth the post-quantum cryptography update alone, even if no encryption processes are changed. Software tools exist which can scan systems and identify the encryption-related processes and the types of encryption they use.

There are three types of encryption endangered by quantum computing. The chief danger comes from Shor’s algorithm with the asymmetric encryption described above. There is also a theoretical risk for encryption based on either of symmetric key exchange or hashing due to Grover’s algorithm, which can search through unstructured values with quadratic speedup over classical methods.

Organisations need to assess the risk and cost associated with upgrading encryption methods, taking into account the sensitivity of the data they protect and the difficulty of upgrading them. Where encryption is upgraded careful planning and testing are required to detect unexpected effects on system performance due to latency and compatibility issues.

Conclusion

Commercially useful quantum computers are still a decade away by most expert estimates but will offer significant computational advantages to those who are ready when they arrive. Quantum algorithms relevant to optimisation offer improved performance with large calculations while quantum machine learning methods offer improved accuracy with less data. Organisations seeking to take advantage of this technology will need to consider the pros and cons of different approaches.

Most quantum computing technologies require cryogenic cooling down to temperatures approaching absolute zero, requiring bulky and sophisticated cooling equipment. They are therefore kept in specially adapted facilities and made available over the cloud. While this is fine for many applications it may introduce a problematic latency for high-speed applications.

Field deployable approaches are under development, such as the diamond-based technology of Quantum Brilliance[17] or the neutral atom technology of Pasqal[18] or QuEra[19]. These approaches are less advanced than cryogenic methods and organisations seeking to cut their teeth may prefer to access facilities over the cloud such as D-Wave[1] or IBM Quantum Experience[20] for a commercial subscription fee.

There is also the option of running quantum algorithms on a simulation. Indeed, some data centres are also making quantum simulations and even hardware available to their users. This would probably not allow commercially useful calculations as the effective capacity of a simulated quantum computer is inherently limited, but enough to refine and understand useful algorithms in time for so-called “Q-day”.

Each organisation has its own needs and priorities, both now and going forward, but rewards exist for those who prepare for the arrival of quantum computers ahead of time.

References

[1] https://www.dwavesys.com/
[2] https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.5.030320
[3] https://dl.acm.org/doi/abs/10.1145/3514221.3520257
[4] https://quantumpositioned.com/what-are-quantum-algorithms/#google_vignette
[5] https://learn.quantumcomputinginc.com/learn/module/understanding-qubos/qubo-formulation
[6] Montanaro, Ashley. "Quantum speedup of branch-and-bound algorithms." *Physical Review Research* 2, no. 1 (2020): 013056
[7] https://quantumzeitgeist.com/what-is-quantum-annealing/#google_vignette
[8] Harrow, Aram W., Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations." *Physical review letters* 103, no. 15 (2009): 150502
[9] https://journals.sagepub.com/doi/full/10.1177/29767032231211902
[10] https://www.nature.com/articles/s41598-023-34966-3
[11] https://arxiv.org/abs/2405.10360
[12] West, Maxwell T., Azar C. Nakhl, Jamie Heredge, Floyd M. Creevey, Lloyd CL Hollenberg, Martin Sevior, and Muhammad Usman. "Drastic circuit depth reductions with preserved adversarial robustness by approximate encoding for quantum machine learning." *Intelligent Computing* 3 (2024): 0100
[13] Larocca, Martin, Nathan Ju, Diego García-Martín, Patrick J. Coles, and Marco Cerezo. "Theory of overparametrization in quantum neural networks." *Nature Computational Science* 3, no. 6 (2023): 542-551
[14] National Institute of Standards and Technology. (2024, August). NIST releases first 3 finalized post-quantum encryption standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards retrieved 12 January 2025
[15] Australian Cyber Security Centre. (2025). Guidelines for cryptography. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography retrieved 12 January 2025
[16] European Commission. (2025). Recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography retrieved 12 January 2025
[17] https://quantumbrilliance.com
[18] https:///www.pasqal.com
[19] https://www.quera.com/
[20] https://www.ibm.com/quantum