Recent Progress in Quantum Computing Relevant to Internet Security

Hilarie Orman
hilarie@purplestreak.com

March 6, 2024

Abstract

Quantum computers at some future date might be able to factor large numbers, and this poses a threat to some public key and key exchange systems in use today. This overview of recent progress in devising quantum algorithms and building quantum computing devices is meant to help technologists understand the difficult problems that quantum engineers are working on, where advances have been made, and how those things affect estimates of if and when large scale quantum computation might happen.

1 Introduction: Looking to Leapfrog

A few years ago, summarizing the state of factoring using logical quantum computing was relatively easy because the field was still barely even nascent [Orm21]. There were a few groups producing qubit chips for demonstrations, and all used the same technology based on superconducting transmon qubits. Today, there is much more innovative variety in hardware, and the scaling challenges are more clearly evident. Given the rapid increase in people who are skilled in the physics and engineering of quantum devices, and given the results they have produced recently, it seems more likely that there will be useful quantum computers within the next 5 - 10 years. Although the RSA public key system is not in imminent danger, in 10 years there might be devices with enough raw qubits to start approaching the problem of factoring numbers with 2048 bits. By that time we should know if quantum devices will ever have the speed and reliability necessary for succeeding.

Technology for quantum computing has a rate of improvement that is beginning to look like the general rule that has been seen in many economically useful manufacturing, in which production rates increase slowly and then become quite rapid. The perceived exponential improvements in the products are due to a set of improvements in each aspect of the process. One of those sets is "people skilled in the art," and the number of those people can rise exponentially during the early stages of development of a new technology, much like the emergence of semiconductor experts in the 1950s and 1960s. Because of the increasing investment in quantum computation, there are many more people today who can build quantum devices than there were 3 years ago. That translates into more improvements in the engineering of more types of devices, and this leads to steady increases in the number of qubits per device. Still, we are in early days of an obscure future.

There are over 70 companies engaged in developing or supporting quantum computers [Dar23], which seems remarkable given that the technology has yet to demonstrate any compelling uses. Research and engineering activities have moved beyond simply demonstrating a large number of usable qubits. Scalability, coherence time, error correction, and gate implementations, all of which are crucial to large-scale computation, are getting attention, but no single approach has yet demonstrated major strides. Instead, different groups are trying different types of physical implementation of qubits, and thus each group has a different learning curve and different rates of progress on the various dimensions of merit for quantum devices.

The industry seems to be entering a time of foment and possible disruption, which is exciting, but gives little indication when, if ever, quantum computing at scale might be achieved. We can say confidently that if the goal is feasible at all, then we are closer than we were a few years back.

About 45 years ago, artificial intelligence was in much the same state. Computer science focused on AI, research conferences published thousands of papers, small companies arose and flourished. A few prescient observers [Mor76] opined that nothing important could be done unless there were many more orders of magnitude in computing technology available for experimentation. The field of AI subdued, turned from clever tricks to large-scale graph analysis, and finally emerged into the current era of massive computation and large models. Although it was foreseen, no one could have predicted the timeline that would lead to the convergence of massive computation and huge neural nets. If quantum computing can reach the point of being able to produce cheap machines with tens or hundreds of thousands logical qubits, if the coherence times can be extended, if the qubit interconnection graph is dense, and if the gate times are in the subnanosecond range, then security mechanisms that depend on large integers problems will fall to the new machines, and many other hard problems in science will be solved. Each “if” is a big problem for physicists and engineers, and we cannot predict a timeline with what we know today.

2 Algorithms

Quantum algorithms that have clear speed advantages over classical algorithms, even in theory, if not practice, are few. In order to be advantageous, a quantum algorithm must be substantially faster than its corresponding classical algorithm, and that generally means that the quantum version should run in polynomial time compared to subexponential or exponential time for the classical version. Shor’s algorithm for factoring large integers remains the clearest example. There are advantageous quantum methods for investigating large random states (random circuits, arrays of spin states, some random coding problems, etc.), but their utility is questionable at this time. There is also a scaling issue in that improvements in classical algorithms keep moving the cross-over point to larger problems. Any practical advantage in quantum computing is still obscured in the fog of quantum engineering.

There are some theoretical reasons that indicate that we are unlikely to see a deluge of quantum algorithms. For one, quantum memory devices are limited, whereas today’s classical computers are loaded with memory, and for another, quantum algorithms are circuits that operate on a superposition of states without feedback. The theory of quantum computing has been acquiring some interesting results and perspectives [Aar22], [BMN$^+$21] that bear watching. For example, although Grover’s algorithm for quantum searching has little advantage over classical methods, there is a search method over pseudorandom data [YZ22] that is quantum polynomial versus exponential for classical.

Of the algorithms being pursued today, matching them to available quantum hardware for solving significant problems is in itself a difficult issue. Just as with a classical computer, the devil is in the details, and maximum performance comes from meticulous attention to using the machine capabilities optimally. However, for quantum computers, the hardware is a moving target, so compilers and code optimization on a per machine basis are important parts of the solutions. For example, IonQ was able to achieve one of their demonstration goals by improving their compiler. This resulted in a 95% reduction in 2-qubit gates for one of their core functions.

The known zone of computational advantage for quantum computing remains in flux and will remain so for some time. At the current time, the only promising algorithms are statistically oriented problems of distinctly limited size. If there are theoretical discoveries that can result in reducing quantum resources for important algorithms, we might obtain quantum usefulness soon, but theoretical discoveries are unpredictable.

2.1 Regev's version of Shor's quantum factoring algorithm

Along the lines of simplification, there has been an interesting discovery applicable to factoring. Oded Regev is an expert on the problem of lattice reduction, and he saw a way to improve quantum factoring by computing points in a multidimensional lattice. In contrast to Shor's algorithm which computes many different powers of 2 modulo the target number N, Regev's method [Reg24] computes the products of many small primes that are raised to many different large powers modulo N. Those products can be viewed as points in a multidimensional space in which the dimension is the number of small primes and the coordinates are the exponents of the powers. The quantum FFT algorithm is computed on those points, and when this quantum state is measured, it yields a randomly selected multidimensional vector related to the group period (and thus, the factors of N). Given enough of these estimates, a lattice reduction on a classical computer can efficiently and with high probability find the group period. Regev found that the lattice reduction, when used for this purpose, is "surprisingly good".

For a number N of n bits, Shor's algorithm uses about $(n^3)/3$ gates; Regev's method uses about $n^{3/2}$ *for large* n; for n in the range of a few thousand the number is $n^{5/2}$. Regev's method uses substantially more qubits than Shor. (A subsequent paper [RV23] showed that the number of qubits could be reduced to some small multiple of n, but that comes at the cost of a great increase in gates).

In the asympototic case for large N, the reduced number of gates would mean that the state coherence times could be substantially shorter than Shor's algorithm requires. Regev initially thought that his method would be advantageous for numbers as small as 2000 bits, but in his revised paper of January 2024, this supposition was weakened, noting that actual coded implementations are necessary before asserting an improvement. Our rough calculations indicate that Regev's method probably uses 30% *more* gates that Shor's does (noting that the quantum machine would have to be reinitialized to rerun the algorithm about 45 times in order to get enough samples for the lattice reduction). NB: we concentrate on 2048 bit numbers because that is at beginning of the range that cannot be attacked by classical computers, and it was considered "safe" until rumblings of quantum computing were heard. Data guarded by 2048 bit keys would be the first to suffer if quantum factoring met all of its wild expectations for error-free computation.

It is worthwhile to understand why fewer gates and sampled data are so helpful when designing a quantum algorithm. The advantage of using small numbers for multiplication is that the quantum circuits for working with them have fewer operations than do the large numbers in Shor's algorithm. Smaller circuits, in general, mean that the coherence time required for the qubits is smaller, and that in turn may mean that the engineering requirements for a factoring quantum computer are more easily achieved. The lattice reduction step for Regev's multidimensional method requires about $sqrt(n)$ sample to assure that the lattice reduction algorithm has a very high probability of finding the period of the group. It would seem that the algorithm's shorter circuit times are for naught because the whole system has to be run so many times.

This brings us to the second interesting aspect of Regev's method — independent quantum estimates. The independence refers to the fact that the algorithm runs, produces a measured result for one vector, and then is reinitialized and run again for another vector, producing another measured result, etc. This means that the small circuits only have to hold their results for the time to compute the exponentiations and one multidimensional quantum FFT per each run of the algorithm. The fact that the samples can be post-processed on a classical computer is the novel property that makes it a likely improvement for very large numbers (assuming that a quantum supercomputer with some trillions of qubits is ever built).

Regev's algorithm illustrates two points that might be useful in further quantum methods for number theoretic computations. The first is that a handful of small numbers with small exponents can be used in place of one number raised to large exponents, and the second is that a multidimensional algorithm can be run several times to collect samples for analysis on a classical computer (this is similar to doing quantum Gaussian Boson Sampling). The combination of the two ideas yields a novel improvement for quantum factoring. It is worth noting that the quantum measurement is a way to do a truly random selection without incurring any computational cost. Quantum is random for free.

Regev notes that if there are major improvements in lattice reduction, then his method becomes even more effective, and furthermore, the world of "post-quantum" cryptography would be largely devoid of safe algorithms. To date, people have worried quite a bit about whether or not there will be a breakthrough in factoring, and lattice solutions have emerged as the intractable problem on which to base public key cryptography. It would be surprising and ironic if the two kinds of problems were at heart, deeply related.

But, expectations should not run ahead of the full reality of building a quantum computer of sufficient size to tackle a large number. When we say "qubit", we mean an error corrected or logical qubit, and that is, in turn, implemented by many physical qubits, many fast, high fidelity gates, and many interconnections. We have yet to see even a single logical qubit demonstrated, let alone several thousand. Nevertheless, Regev's algorithm could be a notable step along the way to eventual (far future) success in quantum factoring.

2.1.1 More detail on Regev's algorithm

Showing that multidimensional lattice computations can be done accurately for a 2000 bit number by computing with fewer than 50 small primes is non-obvious, and Regev's paper is largely concerned with proving the error bounds that relate the dimension of the computational space to the probability of solving the problem in the post-quantum processing step. That step is the well-studied LLL lattice reduction algorithm [LLL82], a piece of magic that takes a set of n dimensional vectors and very efficiently finds a reduced representation

Shor's algorithm also has a post-processing step, albeit a very simple one. The algorithm computes a number R that is related to the factors of the target number, but that calculation need only be approximated to a certain accuracy. R is a rational number of length $2L$ bits where L is the bit length of the number to be factored. R is related to the period of an element in the multiplication group of the number to be factored. The period of a non-trivial element is a factor of the size of the group, it is easy (in time L^2) to use that information to find a factor of the target number. Where does this important number R come from? It is the QFFT of the powers of a group element reduced modulo N, the number to be factored. Those powers can be calculated in parallel using a quantum computer with $2N$ qubits, and the FFT can be calculated on that superposition of powers of small primes. Asympototically, this can be done in time n^2, but for practical purposes, the running time is proportional to n^3.

Regev realized that rather than calculating the powers of one element of the group, the quantum computer could use several elements (small primes), and calculate the products of powers of those elements modulo the target number N. Those products have a periodic repetition pattern in the multidimensional space defined by the small primes. A multidimensional FFT applied to the superposition of those powers yields the multidimensional value R, and R has a repetition pattern in the multidimensional lattice that can be described by a set of basis vectors. Those vectors are related to the group order, and thus to the prime factors of N.

In Shor's algorithm, it is fairly simply to compute the group order from R. The multidimensional counterpart is more complicated, yet entirely tractable in the classical computing domain. Finding the basis vectors for the repetition is done by a classical computer using the LLL algorithm, the workhorse of modern lattice reduction. The running time of LLL scales by approximately $(1.01)^d$, where d is the dimension of the space. In order to compute R with high probability for a 2048 bit number, one needs several dozen distinct, small primes.

Does Regev's method work for discrete logarithms modulo a prime? Apparently it does, according to a recent paper by Martin Ekera and Joel Gartner [EG23]. The Diffie-Hellman key exchange method, which depends on the difficulty of this problem, is frequently used in Internet protocols such as SSL.

Does this method work with elliptic curve fields? According to Ekera, probably not. There is no useful analogy between the small primes for the lattice construction and the elliptic curve points. However, there is a possibly more efficient quantum algorithm outlined by Litinski [Lit23] at PsiQuantum that would break 256-bit EC keys with "only" 50M gates. It assumes that a photonic quantum computer can execute many gate operations in parallel with "non-local" qubit connections. This has not been implemented.

3 Hardware

After nearly 25 years of development, the clear answer to "what is the physical realization of qubits for computing?" is: superconducting qubits, trapped ions, neutral atoms, spin qubits, or photons. The interconnection topology is linear, 2D mesh, 3D, or dynamic. For quantum, we see a widening bleeding edge.

The search for the best quantum technology has become as much about breadth as depth. Researchers need to make qubit devices that are easy to initialize and operate, that are scalable by orders of magnitude while being fast and stable, and that have topological options that support error correction. As each group announces successes in these various aspects, their hopes hinge on a "leapfrog" moment in which they surpass and pull away from competitors. It is still a game that anyone might win.

The variety of technologies is actually good news, because it means that the physicists and engineers are beginning to get a serious grasp on how build and control quantum devices, and many design options are being explored. Several quantum computing devices are available online, and the software design space is being explored in parallel.

One might wonder why this is turning out to be such a hard problem. There are many things in the physical world that exhibit quantum phenomena, from atoms to electrons to atomic nuclei, and to light. These things are at nanometer scale, and they are not easy to fabricate nor to control. Much of the history of modern physics has concentrated on devising methods to simply demonstrate that the theory matches reality.

Given these difficulties, it is amazing that any kind of quantum computer has been built. A computer is all about control of states. In classical computing the states are binary, zero or one, and at each time step all states of the billions of entities in the computer are determined and measurable. But in a quantum computer, the qubits are in a fragile superposition of many states.

At a detailed level, a qubit "state" is based on some fundamental physical property. For photons, it is the polarization or path, for electrons it can be energy or spin or position, for atomic nuclei it can be nuclear spin, for molecules it can be vibrational modes. For each type, there are different important properties. One is the size of the qubit. Although electrons are very small, the fabrication techniques use up a lot of space to ensure so that they can be held still and controlled. For example, superconducting transmon qubits use square micrometers of silicon area, and IBMs quantum chip sets currently have about 200 qubits per chip. That's a far cry from the 100 billions of transistors that make up modern CPU chips. Another consideration is the time that a qubit can maintain its state, and yet another is the difficulty of creating connections to other qubits and to the control circuitry. These things together affect what kinds of error correction can be achieved. All in all, each technology influences the architecture of the resulting quantum computer.

A few years ago, the measure of progress for quantum computing was the number of usable qubits in a quantum computer. Today, the various companies tout their achievements and plans in terms that are more related to the amount of computing that the platform can deliver. One useful measure is "quantum volume" (QV), a well-defined benchmark that is adaptable to any logical quantum processor. In general terms, QV is a measure of how reliably an ensemble of qubits can carry out a computation over multiple levels of quantum gates. The gates take two input qubits and produce two output qubits. Each gate and its inputs are chosen randomly at the start of the benchmark test. There is a mathematically based measure that determines how well the quantum computer performed. IBM's 133 qubit processor has demonstrated a QV of 7, while the record of 19 is held by Quantinuum's H1-2 machine (note that although the QV measure is technically the logarithm base two of the measurement success, it is fairly common for a company to state it in terms of the base, e.g. QV of 128 instead of 7).

The QV measure is good for judging the reliability of the quantum device, but it does not include gate speed in its measure. Most devices have a fast single qubit gate operation (submicrosecond, as low as a few nanoseconds), but the two-qubit gates are slower. If the qubits are not fully interconnected, then the input states have to be manipulated to bring them into a placement that supports the gate operation. This can increase the time for the gate operation by an order of magnitude or more. Qubit interconnection is much easier for some technologies (e.g., neutral atoms) than others.

Not all players in the game use QV as their figure of merit. QuEra has a set of useful algorithms that they use for benchmarks, the AQ series that are scalable to different numbers of qubits. Because Intel has no announced benchmarks, their current or expected QV is unknown today. Microsoft has suggested the reliable operations per second (rQOPS) is the best measure of usefulness.

The following sections show the variety of approaches and the varying degrees of maturity in the devices. Because there are so many difficult problems in the engineering of a quantum computer, it is hard to know if any approach is going to succeed, or when. The accomplishments logged in the past 12 months illustrate that progress is ongoing, but any of the approaches could hit a roadblock or leapfrog the others. Although none of the approaches would be capable of factoring large scale numbers within a decade, this still bears watching. If a major breakthrough in error correction were to occur for any of these technologies, and if they could scale up to millions of interconnected physical qubits, factoring numbers of 2048 bits might come within reach.

Several companies have demonstrated topological qubits or "non-Abelian anyons". These oddities of quantum theory had not even been observed before a couple of years ago, but now they have been demonstrated over a variety of qubit types, and they are seen as a promising basis for error-corrected quantum computation. In brief, quantum particles have, as part of their state, a memory of where they have been with respect to other particles with which they are entangled. The information is in the "phase" of the quantum state, and it is fairly long-lived. The “non-Abelian” aspect of it refers to the mathematical structure of the motions in space that the particles can take; the algebraic group of possible motions is, in general, non-Abelian, and that means that the information about the motion history is not easily collapsed into a simple variable. Because error correcton for qubits has not yet been demonstrated, and because it seems to need a lot of extra qubits and measurements, any physical principle that can simplify the problem will be a major advance in the field. Anyons might be the key to error-correction.

Some of the data in the following sections is from [Fei22] and [Swa24].

3.1 Superconducting Transmon Qubits: IBM

IBM is staying the course for superconducting transmon qubits, possibly the best understood quantum technology today. These qubits use superconducting charge devices in which the quantum state is determined by the energy level of the electrons in a small region of a circuit. Typical qubit coherence times (T1 is state coherence, T2 is phase coherence) are 288 μsec for T1 and 127 μsec for T2. The superconductivity occurs only in a very low energy environment, i.e., a cryostat operating in the milliKelvin region. The devices can be fabricated using ordinary silicon wafers.

IBM is furthest along the pathway for producing logical quantum processors. They are fabricating chips with 133 physical qubits today, and they have one demonstration chip with over a thousand qubits. Each qubit is a few square micrometers in area. The newer chip has a qubit density about 50% higher than the 133 qubit chips. The density is important because silicon wafers have limited area, as do cryochambers, and smaller devices will ease the problems of scaling to millions of qubits in some future world.

Creating gates for controlling sets of qubits requires a lot of signal routing, and that has led IBM engineers to use 3 layers of wiring for their 133-bit chip and 5 layers for the 1000 qubit chip. The smaller chip is superior to previous chips because of improvements in gate fidelity and performance [Fad23].

IBM has made gate operations a priority for their roadmap. They want to have a machine that can execute 100M gates during a single coherence time. That is the scale at which a quantum computer can become “useful” in the sense that it is clearly superior to classical computers for some classes of problems. From [Nay23]: “reliable Quantum Operations Per Second (rQOPS), which measures how many reliable operations can be executed in a second. A quantum supercomputer will need at least one million rQOPS. . . . In order to solve the most challenging commercial chemistry and materials science problems, a supercomputer will need to continue to scale to one billion rQOPS and beyond, with an error rate of at most 10-18 or one for every quintillion operations. At one billion rQOPS, chemistry and materials science research will be accelerated by modeling new configurations and interactions of molecules."

IBM is also working on methods for interconnecting chips. Soon they be connecting chips in the cryostat for ordinary signaling, and in the future they might have quantum interconnection lines between chips. IBM has the most mature notion of a quantum computer "system" and the collection of problems that make upwards scaling so challenging.

Along with most other developers of quantum computers, IBM expects topological qubits to be important for implementing error correction, and IBM researchers have demonstrated these odd particles [Aea23a], though not in their quantum chips: "This demonstration is a prerequisite for experiments involving fusion and braiding of Majorana zero modes" (which would be the non-Abelian anyons that could implement high-fidelity quantum operations)." Promising as these are, it is important to note that this phenomenon occurs when qubits can be controllably moved to new positions, and this has not been a primary design feature for transmon qubits.

3.2 Stealth Mode?: Microsoft

A few years ago Microsoft identified error-correction as the main problem for their quantum project. At that time they were using superconducting qubits, and they showed some innovative plans for qubit interconnections using a "heavy hexagon" layout that would facilitate error correction gates. They also announced that they had demonstrated non-Abelian anyons and would incorporate topological phase into their future qubit designs. Since then, they have not announced any new processors, though their recent work indicates they are pursuing the same paths.

The following information about plans for using topological qubits was taken from Microsoft's website in early February of 2024; the content is no longer available.

"Microsoft engineered devices allow us to induce and control topological phase creating Majorana Zero Modes. . . . This innovation starts our path to engineering the world's first hardware protected qubit, a new type of stable qubit. . . . Our protected qubit, with built-in error protection, extends our first breakthrough by changing qubit technology from analog to digital control. . . . To scale operations and reduce errors, digitally controlled hardware-protected qubits can be entangled and braided with a series of quality advances."

Their roadmap today emphasizes that fast and reliable qubits and gates are essential for doing useful work. Their roadmap talks of running 1 million reliable quantum operations per second (rQOPS) with an error rate of less than 1 every trillion steps, and then they will gradually scale up to reach 100 million reliable rQOPS per second This sounds more aspirational than realistic, but they may have something grand in the works.

3.3 Logical Qubits: Google

Once a frontrunner in demonstrating advanced qubit devices, Google has settled into more of research and demonstration role. Recently they were able to implement topological qubits [Aea23b] using superconducting qubits.

Google is working on building "useful error-corrected logical qubits" and scaling up the number of physical qubits by a factor of 10 each year [NK23]. In 2023 they demonstrated a prototype with 100 physical qubits, and that puts them on "the precipice" of a true logical qubit, and their plan for 2025 is "1 long-lived logical qubit", to be followed by a "tilable module" for a logical gate. After that, it's all "scale up".

3.4 Trapped Ions: IonQ and Quantinuum

Ions held in a shaped electromagnetic field can be used as qubits if they are first cooled enough to keep them from jostling out of the field. To set up an array of trapped ions, lasers are used to cool them in a vacuum chamber. The state coherence does not require super low temperatures, but the array still has to be kept in a cryostat for measurement. However, the temperature is much higher (4K) than for superconducting qubits. A big advantage of trapped ions is the long coherence times: seconds to minutes. The gate times are few μsec. Moreover, full qubit connectivity is a basic property.

The usual way of constructing the "trap" for ions is called a Paul trap. It uses an oscillating quadrapole field to confine the ions. The field potential can be up to several electronvolts, which is sufficient to hold the ions in place for a long time with respect to gate times.

For an overview of literature regarding control systems for trapped ion devices see [Cas23]. There are two companies that have demonstrated non-trivial computations with trapped ions technology.

3.4.1 Quantinuum

Last year Quantinuum demonstrated quantum volume (QV) of 19 on a 15 qubit machine (their H1-1) [Sta23b]. Their press release indicated that they are on a line of development in which their improvements in technology are incorporated into their production line without the need for fundamental redesign. Their model H2 machine excels in qubit connectivity and gate fidelity [ITV+24]:
32 fully-connected qubits
65,536 (2^{16}) QV
99.997% single-qubit gate fidelity
99.8% two-qubit gate fidelity
demonstration of topological qubits.

3.4.2 IonQ

IonQ's Forte machine underwent improvements last year to add more qubits, upping it to 36 from 20. Their compiler was also improved, as previously mentioned. The improvements helped them carry out operations on an ensemble of 35 qubits using circuits with depths between about 243 and 335 gates [Sta24], demonstrating the ability to hold coherence long enough to compute well-known algorithms like the quantum Fourier transform. They are projecting 1024 qubit devices within 5 years.

IonQ has also announced their Tempo machines, to be available in 2024, with many improvements over Forte, though details are lacking.

From their announcement in 2023 in which they set the 35 qubit benchmark: "IonQ co-founder Chris Monroe, advisor Kenneth Brown, and their academic collaborators recently (in 2020) demonstrated the first fault tolerant error corrected operation using a trapped ion system, with an overhead of just 13:1. Other technologies, because of their poor gate fidelity and qubit connectivity, might need 1,000, 10,000 or even 1,000,000 qubits to create a single error-corrected qubit." This design is promising, but they have not yet demonstrated an error-corrected qubit.

IonQ partners with Honeywell for manufacturing the quantum processors.

IonQ's basic quantum parameters:
T1, T2 lifetimes: many seconds, one second
Gate speed: 1-3 μsec.

3.5 Neutral Atoms: QuEra, Atom Computing, Pasqal

Neutral atom technology, further behind on the curve than superconducting qubits or ion traps, seems to be developing rapidly and making use of the novel way of holding the atoms in place with “optical tweezers” (intersecting laser beams). To date, the neutral atom computers have mainly been used for analog computations (seeking low energy states), but the companies doing the work are simultaneously working on programmability and universal logic gates. Useful background information about this relatively new qubit technology can be found in [WDE^{+}23].

The assemblage of atoms needs extreme cooling in a vacuum as part of state preparation. Much like trapped ions, lasers are used to calm the atoms into place in the laser beam array; after that it can operate at room temperature, but keeping it cooled to about 4K increases the coherence times. The coherence time for T2 is a leisurely 1-10 sec. Gate times are on the order of 400 nsec to 2 μsec. Each atom occupies a small space, from a few microns to less than one, depending on the beam spacing.

The quantum state for neutral atoms is based on the spin state of an outer electron. The atoms are in the Rydberg state, meaning that only one of the electrons are in an outer (high energy) shell. Such atoms have a simple interaction model, similar to an ideal hydrogen atom, and the inner electrons can be ignored for most interactions.

The kind of atom to use for these machines is still not clear. Akali metals, such as rubidium, are being used currently by QuEra, and Atom Computing (atom-computing.com) is using ytterbium. The fact that there is no obvious consensus on which element is best shows that the physicists and engineers are still experimenting with materials, perhaps echoing the early days of semiconductors when the doping materials were still the subject of experiments.

3.5.1 QuEra

QuEra has produced interesting quantum computers, with a small number of qubits, but with full interconnection through atom movement. Due to the small number of qubits, they expect their machines to be useful as analog devices for the time being, but they do support a programmable logic mode as well.

Quera has 256 qubit devices today. Their projections are:
256 qubits with 10 logical qubits in 2024
3000 qubits with 30 logical qubits in 2025

10K qubits with 1K logical qubits in 2026

From their January 2024 press release: “Transversal gates are crucial in quantum computing for their ability to prevent error propagation across qubits, making them inherently error-resistant. They simplify quantum error correction by allowing errors to be corrected independently for each qubit.”

3.5.2 Atom Computing

Atom Computing announced in October of 2023 that they had a one thousand qubit machine [Wil23, Tim23] using ytterbium for their neutral atoms. The machine will be available for public use sometime in 2024. Their current priorities focus on novel ways of preparing and maintaining a fully populated qubit array [Nea24], up to 1200 atoms, using “spares” that can be moved into the array when an atom escapes the laser cells (this is the only mention I’ve seen of maintenance for a quantum computer).

In late 2023, Harvard research physicists announced that they had reached a milestone by implementing critical elements for error corrected qubits in a programmable, neutral atom quantum computer with 280 qubits [Bea24]. This achievement used movable atoms. Should this technology continue to advance quickly, it might indeed surpass superconducting transmon qubits in terms of quantum volume. This work has DARPA support, and although the program is for “noisy” quantum computing, their program manager notes that they have been able to advance technology for error-corrected large-scale QC [Sta23a].

3.5.3 Pasqal

Pasqal (www.pasqal.com) is also in the neutral atom QC game, weighing at 100 qubits today, 200 qubits “soon”, and “on track” for 1000 qubits in their next generation processor.

3.6 Spin

3.6.1 HRL Laboratories

Quantum dot TV displays have been in production for several years, but quantum dot computing devices are also a possibility. They work by holding single electrons in silicon charge traps, and the spin of the electron is used as the qubit state. These spin qubits have fast gate times.

HRL Laboratories announced that they have been able to implement a universal set of gates for their spin qubits [HRL23a, HRL23b, Wea23]. This puts them just barely on the map, but spin qubits are being used by Intel, too, and this technology area might move quickly now that they have the gate sets.

3.7 Spin? Stealth?: Intel

Having produced a few demonstrations of quantum computing, Intel may have entered stealth mode. They announced their committment to topological qubits in order to achieve robust error correction, but they have not touted recent developments.

In 2020 they announced a chip for controlling quantum operations within the cryostat. The "Horse Ridge II" controller can cut down on the wiring that goes into a cryostat by allowing some measurements and qubit gate signals to be carried out inside the cold chamber. This seems like a necessary component for scaling up to millions of qubits, but Intel has not announced any follow-ons to the device.

In June of 2023, Intel announced a small (12 qubit) quantum computer called Tunnel Falls [Int23] . It is a spin qubit device, with the advantage very small silicon based qubits. The qubit is only 50 nm on a side, and that density is not approached by any other quantum technology.

3.8 Light: PsiQuantum, Xanadu

On basic principles, photons would seem to be the ideal quantum devices. They are fast, they have long coherence times because they do not interact with one another, industry has been building communication systems based on light for a few decades, quantum advantage has been demonstrated on a photonic quantum computer, and photonic devices can operate at room temperature. Why haven't they taken over the industry?

Unfortunately, physics research thus far withholds a few necessities. Although the photon interactions can be done at room temperature, the measurement apparatus for sensing the photons must be kept at cryonic temperatures in the 4 Kelvin range. Photons are free spirits, and building the gates for controlled entanglement is difficult. It is not clear if anyone has yet implemented a set of photonic gates for universal logic, though they have been described in theory [HTD15].

Nonetheless, photon entanglement is an interesting phenomenon that involves pathways as part of the state. In classic experiments with light and half-silvered mirrors, photons can exhibit the property of both having gone through a pathway and not having gone through it. This superposition of position states is very counterintuitive, but very real, and it is a basis for computing with photons. A fairly recent overview of the state of photonic computation and its pros and cons [CCY+22] explains the why it has the potential to excel, despite lagging in programmability.

3.8.1 PsiQuantum

PsiQuantum has described a photonic gate architecture that they call "fusion based quantum computation" [BBB+23], but this has not been built.

PsiQuantum is building a photonic quantum computer, the Q1, but little information about it has been made public. They have some funding from the DARPA Underexplored Systems for Utility-Scale Quantum Computing (US2QC) program. In 2022, Forbes magazine [SG22] reported that PsiQuantum was building an optical switch to enable interconnections between ten of thousands of quantum processors. Their goal was to have a million qubit processor.

The only part of the Q1 that needs cooling is the superconducting single photon detectors. However, it operates in the 4 Kelvin range rather than the milliKelvin range of dilution refrigerators. It may not sound like a big difference, but it requires 1000x less power.

3.8.2 Xanadu

The Canadian company Xanadu Quantum Technologies reported a benchmark result demonstrating quantum advantage for a photonic computer running Gaussian Boson Sampling in June 2022 [Mea22].

3.9 Quantum Circuits (QCI)

This venture aims to have error-correction "built-in" to their quantum devices. They use superconducting transmons, but they add "dual resonator qubits" [Tea24] to the circuit. They can move a microwave photon between two resonator regions, or have it exist spookily in both regions at once. This is an interesting combination of two kinds of quantum mechanisms combined into one qubit device.

4 The Race to Advantage

When will someone say “the only way to solve (this important problem) in a timely/cost-effective manner is to use (an existing logical quantum computer)”? That day might come, but much water will flow under many bridges before then.

There’s no agreement on predicting such a moment. There are some computations known today that might be solved with a quantum computer in the future and will never be solved by a classical computer, but they are not important problems. It needs a real world problem and a time or cost limit. Perhaps there are situations where lives depend on data that is locked behind an RSA public key of 2048 bits, and if a quantum supercomputers can be built, then a nation will spend the money to solve the RSA problem.

In the meantime, existing quantum computers merely suggest that logical quantum computing might be useful for some problems in a decade or more. Or, perhaps they will be cheaper than corresponding classical supercomputers. But, there are not many algorithms for which quantum computing is both useful and necessary. One reason is the lack of quantum memory, something that was not lacking in the early days of semiconductor computers. “Generally, quantum computers will be practical for ‘big compute’ problems on small data, not big data problems” [HHT23].

Other discussion of why quantum computers need an exponential advantage to exceed the computational capabilities of classical computers is in: [BMN^{+}21]

Specifically, with respect to Internet security, when will it be feasible to factor a given 2048-bit RSA modulus? This is a problem too hard for a classical computer limited to planetary resources, so a quantum computer is the only possible approach. We take as a given constraint that even if we could double the amount of energy that the sun bathes on the earth, the planet could not sustain human life. That’s the minimum of what it would take to factor a 2048 bit number or to use brute force computing to find a 128 bit symmetric key. Technically, all computation could be reversible, and most of the energy could be recovered, but the Second Law of Thermodynamics leads to the conclusion that a goodly percentage of the energy would end up as wasted heat, further hastening the demise of our planet. Perhaps, if there were fusion reactors on asteroids powering supercomputers, such large computations would be feasible, but that is unlikely to happen in the next 50 years.

Bitcoin mining uses a great deal of energy, a few per cent of the total US consumption [dV24]. Although that may seem like a lot of computation, it is many orders of magnitude short of being able to factor a 2048-bit number or to guess a 128 bit key.

4.1 Advantage Claims

There have been several claims that quantum computers or similar quantum devices have carried out computations that are far beyond the capabilities of current classical computers. It is important to note that all such computations to date are based on statistical sampling. The quantum computers generate a complicated entangled state with a distribution based on a programmed random configuration. Sequentially, a million or so samples are gathered by repeated measurement of the state. This yields a random samples over an "interesting" distribution. Researchers can investigate the samples using classical computing for further structure and use it to confirm or deny hypotheses about the distribution.

The demonstrations can be used to show that a quantum processor is able to use all its qubits and to carry out quantum operations over the ensemble. Although this sounds straightforward, the devil is in the details of what constitutes a "random" hard problem and how one demonstrates that the answers are actually from the solution space.

There are two problems that are generally agreed to be suitable for demonstrating that a quantum computer can solve a really hard problem. Gaussian Boson Sampling (GBS) is an algorithm for calculating a function of a matrix, similar to a determinant but much more difficult computationally. In a photonic quantum device, beam splitters and mirrors implement the function, and it is applied to a superposition of photons that represent the input matrix. Each run yields a sample value, and these are combined in a final step using a classical computer. Random Circuit Sampling (RCS) [BFNV17], in contrast, is not an algorithm for calculating a function, it is for verifiably generating random instances of the output of a randomly chosen logic circuit.

Despite the hype and hoopla of claims and counter claims of immense computational advantage, there are some arguments over the scope and scaling of the advantage and the details of selecting a random configuration. Nonetheless, each of the demonstrations shows that there is steady improvement in building controllable and usable quantum computing devices of increasing size and complexity. The number of qubits, interconnections, gate fidelities, and measurement apparatus are getting better, and those improvements can be used in building more capable computing devices. It is also important to note that there is no claim of importance of the computations per se – they do not make the case for financial advantage.

An overview of several of the following quantum advantage demonstrations can be found in [CCY$^+$22].

A brief history of quantum advantage:

- 2019 – Google implements “random circuit sampling” (RCS) using 53-qubit Sycamore processor [Aea19] with a claim of substantial computational advantage over classical computers.
- 2020 – Chinese researchers built a photonic device to carry out Gaussian Boson Sampling [ZWD$^+$20]. They estimated that a supercomputer would take 10^{14} years to carry out the computation that their device did in 200 seconds.
- 2021 – A follow-on project by the same group claims a 10^{24} time advantage for GBS.
- 2021 – IBM publishes result that their 127 qubit computer can outperform classical computers in evaluating symmetric logic expressions when the number of classical bits is limited a few and only one qubit is used [MKB$^+$21]. They demonstrated 93% accuracy for a computation, and that even that unimpressive number was far better than a classical computer (with severely limited compute space) could achieve.
- 2022 – A photonic computer implemented GBS for a problem of significant size. From [Mea22]: “We carry out Gaussian boson sampling (GBS) on 216 squeezed modes entangled with three-dimensional connectivity, using a time-multiplexed and photon-number-resolving architecture. On average, it would take more than 9000 years for the best available algorithms and supercomputers to produce, using exact methods, a single sample from the programmed distribution, whereas Borealis [the photonic computer] requires only 36 μs.”
- 2022 – Researchers claim that classical solutions to RCS on existing supercomputers with optimized code would be faster than the Google Sycamore processor [PCZ22].
- 2023 – Mathematicians comparing quantum solutions to RCS versus classical computers [ZVBL23] found that quantum advantage would be overcome by errors as the problem size increased. This shows the importance of error correction for quantum computation; without it, the useful region for QC is greatly constrained. Other researchers

claim that the precise definition of "random" can affect the results, and that not all of the demonstrations used the same statistics for the circuit generation [OK23, KRS23]. More research is needed.

- 2023 – Google uses a 70 qubit Sycamore processor for another RCS problem [AC23]; speedup claim is that best existing classical supercomputer would take 47 years.
- 2023 – IBM achieves "pretty good quantum" by demonstrating solutions to 2D Ising spin state models using their 127-qubit processor [KEA$^+$23]. Ising models have elements arranged in a lattice and with randomly chosen 1-bit states. The elements interact over time and settle into an annealed low-energy state. This is quite complicated for non-trivial lattices, and IBM used the topology of their quantum processor as the lattice for the Ising state. Their algorithm had an impressive computation scale of "60 layers of two-qubit gates, a total of 2,880 CNOT gates." Their paper claims that the accuracy of their results was surprisingly good given the error rates of their machine, and they achieved this by back-fitting measured errors and using them to correct further results. They suggest that a hybrid computation model of error mitigation with limited error correction might be the operational mode for "utilitarian" quantum computation in the near future.

4.2 Factoring Prospects

The big question for Internet security is if and/or when quantum computers will be able to factor numbers with 2000 or more bits (or solve discrete logarithms in that range). These numbers are completely out of range for classical computers, but given enough advances in fast and reliable quantum computing, the 2000 bit range could be conquered, but even a wildly optimistic estimate would put that at nearly 25 years from now.

The necessary quantum resources for factoring numbers of 2000 bits are not hard to estimate. Shor's algorithm needs 4000 logical qubits to store the exponent variable, a 2000 qubit register for the accumulating result, and a working register of 2000 qubits. The total is 8000 qubits. It is hard to estimate the total number of physical qubits needed, because quantum error correction proposals use anywhere from 20 to 1000 physical qubits to implement each logical (error-corrected) qubit. For purposes of estimation, we will assume a ratio of 500 physical to logical. In support of this, we note that Google is currently working with 100 qubits to implement subcomponents of what may soon be one logical qubit. If gate fidelities improve by orders of magnitude, error correction will be easier, but current progress favors qubit production over gate improvements. Thus, the 2000 bit factorization problem requires about 4 million physical qubits.

Several companies are working towards the million qubit mark today: [Bro23]: "IBM is not the first to aim big. Google has said it is targeting a million qubits by the end of the decade, though error correction means only 10,000 will be available for computations. Maryland-based IonQ is aiming to have 1,024 'logical qubits,' each of which will be formed from an error-correcting circuit of 13 physical qubits, performing computations by 2028. Palo Alto–based PsiQuantum, like Google, is also aiming to build a million-qubit quantum computer, but it has not revealed its time scale or its error-correction requirements."

The arithmetic for the modular exponentiations for Shor's algorithm needs about 2.7 billion Toffoli gate operations. Regev's algorithm needs about 3.5 billion for computing each sample lattice point (in total, 45 sample points are needed). Although Regev's algorithm would need fewer gates than Shor's for much larger numbers, in the 2000 bit range Regev needs to carry out about 70 modular squarings, and that is a substantial amount of arithmetic. Shor's algorithm, in contrast, is doing modular multiplications by fixed constants, and that has simpler arithmetic circuits than squaring does. For the purposes of estimating, we will use the 2.7 billion gates for our estimation.

Let us assume that the coherence times, T1 and T2, are 10 seconds, which is quite long in today's quantum world. It follows that the time to execute one fully corrected gate must be less than 4 nanoseconds. Almost all quantum devices today range from msec to μsec gate times [Rud23, Mal22] which are far too slow for factoring. They would have to improve those times by factors of 1000 to 100000. Is that even possible? One factor that limits quantum control is the Heisenberg uncertainty principle. When trying to focus a beam onto an exceedingly tiny area, one can encounter the problem that the actual effect is over a wider area because the particle momenta become larger. If gates times cannot be increased, then the only hope for massive computation is longer coherence times. There is not much data on progress in that direction, except for IBM's roadmap.

IBM projects much better coherence in its next generation of processors, and their goal is to support 100M operations by 2033. However, the chips that they predict for this will be of a completely different design than that what they are using today for their quantum "advantage" or "utility" demonstrations today. A wildly optimistic exponential extrapolation of progress in this dimension, from thousands of gates today to 100M in 10 years, would lead a prediction that there will be enough quantum computing power to factor 2000 bit numbers by the late 2040s.

It is even possible that new qubit technologies will overtake today's efforts. PsiQuantum implies that their photonic computing devices today have nanosecond gate times, and they are touting an architecture with "non-local" connections that could increase quantum computing effectivity by orders of magnitude [LN22]. Their new idea in this is to increase the number of gates that can operate in parallel, thus keeping the qubits busier. It is an interesting idea that might apply to other qubit technologies. If their gate times truly are that fast, and if their new architecture enables denser computation, and if their coherence times are in the minute range, then 2000 bit factorizations could come sooner. But, photonics is the least mature quantum technology, and no predictions can be made based on the limited achievements thus far.

5 Predictions, Projections, and Damned Lies

So, when should we throw out the RSA public key algorithm and all security methods that use modular exponentiation? When should we eschew methods based on lattice reduction? The advice can vary as widely as the field of quantum computing devices is growing. The key takeaway is to be aware of how knowledge and development are coalescing in this moving landscape.

A visual depiction of the threshholds for RSA computations and quantum relationships is shown in this multidimensional "quantum landscape" chart created by Sam Jacques for 2023:
`http://sam-jaques.appspot.com/quantum_landscape_2023`.
The overview is helpful, though recent accomplishments have already exceeded the summary: number of qubits is now at one thousand, for example. The red line showing "RSA-1024 is broken" is superfluous because it is generally agreed that any of the top supercomputers today could factor a 1024 bit number in about a month (note that an 829 bit number was factored using fairly ordinary machines in 2020). The chart also suggests that we are close to having usable surface codes; that seems doubtful, and I think that the technology will remain stuck in the lower, unadvantageous, part of the chart for some time to come.

There is a huge question looming over the future of quantum computing: is it physically possible to achieve advantage over classical computing for an important problem? It seems clear that quantum computers can be built, it seems clear that for some problems involving randomness they can exceed classical computers, but it is not clear that they will be large enough or fast enough to really deliver on “advantage” for problems of interest to science and industry. It seems more likely that as quantum devices approach that threshhold, they will also hit some physical limit that impedes further improvement.

There is also the uncertainty about the relevance of current research and development. Although the recent accomplishments in quantum engineering are striking and promising, each one seems to reveal the edge of some deeper problem lurking around the corner. No technology layer seems to a stable platform for building the next layer, no one has a vision for a commodity quantum supercomputer. All the announcements have to be viewed within the context of the limitations of the technology at hand. Some things may move quickly, but as a whole, the field may be failing to cohere.

There might not be much clarity during the next few years, but undoubtedly there will be an increasing number of demonstrations, new benchmark results, and many more research papers. We have some information today about where things are moving and where major breakthroughs are needed, and as prognosticators, those will have to be our guides as the landscape unfolds.

6 Thanks

The author gratefully acknowledges financial support from the Internet Corporation for Assigned Names and Numbers (ICANN) for this work. Richard Schroeppel contributed valuable insights on algorithms and resource estimates.

References

[Aar22] Scott Aaronson. How much structure is needed for huge quantum speedups? scottaaronson.com, September 2022.

[AC23] Google Quantum AI and Collaborators. Phase transitions in random circuit sampling. arxiv.org, December 2023. `https://arxiv.org/pdf/2304.11119.pdf`.

[Aea19] Frank Arute and et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, Oct 2019. https://doi.org/10.1038/s41586-019-1666-5.

[Aea23a] Morteza Aghaee and et al. InAs-Al hybrid devices passing the topological gap protocol. *Phys. Rev. B*, 107:245423, Jun 2023.

[Aea23b] T. I. Andersen and et al. Non-abelian braiding of graph vertices in a superconducting processor. *Nature*, 618(7964):264–269, Jun 2023. https://doi.org/10.1038/s41586-023-05954-4.

[BBB$^+$23] Sara Bartolucci, Patrick Birchall, Hector Bombín, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, Fernando Pastawski, Terry Rudolph, and Chris Sparrow. Fusion-based quantum computation. *Nature Communications*, 14(1):912, Feb 2023. https://doi.org/10.1038/s41467-023-36493-1.

[Bea24] Dolev Bluvstein and et al. Logical quantum processor based on reconfigurable atom arrays. *Nature*, 626(7997):58–65, Feb 2024. https://doi.org/10.1038/s41586-023-06927-3.

[BFNV17] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *NIST Publication*, 2017. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927073.

[BMN$^+$21] Ryan Babbush, Jarrod R. McClean, Michael Newman, Craig Gidney, Sergio Boixo, and Hartmut Neven. Focus beyond quadratic speedups for error-corrected quantum advantage. *PRX Quantum*, 2(1), March 2021.

[Bro23] Michael Brooks. IBM wants to build a 100,000-qubit quantum computer, May 2023. https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/.

[Cas23] Stefanie Castillo. The electronic control system of a trapped-ion quantum processor: A systematic literature review. *IEEE Access*, 11:65775–65786, 2023.

[CCY$^+$22] Yen-Hung Chen, Chien-Hung Cho, Wei Yuan, Yin Ma, Kai Wen, and Ching-Ray Chang. Photonic quantum computers enlighten the world: A review of their development, types, and applications. *IEEE Nanotechnology Magazine*, 16(4):4–9, 2022.

[Dar23] James Dargan. Quantum computing companies: A full 2024 list. *The Quantum Insider*, December 2023.

[dV24] Alex de Vries. Bitcoin energy consumption index. *Digiconomist*, 2024. `https://digiconomist.net/bitcoin-energy-consumption`, 150 terawatt hours per year as of Feb 2024,.

[EG23] Martin Ekerå and Joel Gärtner. Extending Regev's factoring algorithm to compute discrete logarithms. *arXiv*, 11 2023. arxiv.org/pdf/2311.05545.pdf.

[Fad23] Ingrid Fadelli. Exclusive: A closer look at IBM's heron and condor quantum processors. *All About Circuits*, December 2023. `https://www.allaboutcircuits.com/news/closer-look-at-ibms-heron-and-condor-quantum-processors/`.

[Fei22] Russ Fein. Quantum computing modalities – a qubit primer revisited. *The Quantum Leap Blog*, October 2022. `https://quantumtech.blog/2022/10/20/quantum-computing-modalities-a-qubit-primer-revisited/`.

[HHT23] Torsten Hoefler, Thomas Haner, and Matthias Troyer. Disentangling hype from practicality: On realistically achieving quantum advantage. *Communications of the ACM*, 66(5):82–87, May 2023.

[HRL23a] News HRL. Quantum computing breakthrough: Silicon encoded spin qubits achieve universality. *HRL Laboratories*, March 2023. `https://scitechdaily.com/`, quantum-computing-breakthrough-silicon-encoded, -spin-qubits-achieve-universality/.

[HRL23b] News HRL. Silicon encoded spin qubits achieve universality. *HRL Laboratories*, 2023. `https://www.hrl.com/news/2023/03/05/`, hrl-laboratories-silicon-encoded, -spin-qubits-achieve-universality.

[HTD15] Ming Hua, Ming-Jie Tao, and Fu-Guo Deng. Fast universal quantum gates on microwave photons with all-resonance operations in circuit QED. *Scientific Reports*, 5(1):9274, Mar 2015. `https://doi.org/10.1038/srep09274`.

[Int23] News Intel. Intel's new chip to advance silicon spin qubit research for quantum computing. Intel.com, 2023. `https://www.intel.com/content/www/us/en/newsroom/news/quantum-computing-chip-to-advance-research.html#gs.55xm94`, Intel makes new quantum chip available to university and federal research labs to grow the quantum computing research community.

[ITV$^+$24] Mohsin Iqbal, Nathanan Tantivasadakarn, Ruben Verresen, Sara L. Campbell, Joan M. Dreiling, Caroline Figgatt, John P. Gaebler, Jacob Johansen, Michael Mills, Steven A. Moses, Juan M. Pino, Anthony Ransford, Mary Rowe, Peter Siegfried, Russell P. Stutz, Michael Foss-Feig, Ashvin Vishwanath, and Henrik Dreyer. Non-Abelian topological order and anyons on a trapped-ion processor. *Nature*, 626(7999):505–511, February 2024. `http://dx.doi.org/10.1038/s41586-023-06934-4`.

[KEA$^+$23] Youngseok Kim, Andrew Eddins, Sajant Anand, Ken Xuan Wei, Ewout van den Berg, Sami Rosenblatt, Hasan Nayfeh, Yantao Wu, Michael Zaletel, Kristan Temme, and Abhinav Kandala. Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618(7965):500–505, Jun 2023. `https://doi.org/10.1038/s41586-023-06096-3`.

[KRS23] Gil Kalai, Yosef Rinott, and Tomer Shoham. Questions and concerns about Google's quantum supremacy claim. arxiv.org/pdf/2305.01064.pdf, May 2023. `https://arxiv.org/pdf/2305.01064.pdf`.

[Lit23] Daniel Litinski. How to compute a 256-bit elliptic curve private key with only 50 million toffoli gates. arxiv.org/abs/2306.08585, 2023.

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, and László Miklós Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982. `https://api.semanticscholar.org/CorpusID:5701340`.

[LN22] Daniel Litinski and Naomi Nickerson. Active volume: An architecture for efficient fault-tolerant quantum computers with limited non-local connections, November 2022. `https://arxiv.org/pdf/2211.15465.pdf`.

[Mal22] Maciej Malinowski. How fast are quantum computers (part 2: clock speeds). GitHub blog, December 2022. `https://m-malinowski.github.io/2022/12/04/how-fast-are-quantum-computers-part-2.html`.

[Mea22] Lars S. Madsen and et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, Jun 2022. `https://doi.org/10.1038/s41586-022-04725-x`.

[MKB$^+$21] Dmitri Maslov, Jin-Sung Kim, Sergey Bravyi, Theodore J. Yoder, and Sarah Sheldon. Quantum advantage for computations with limited space. *Nature Physics*, 17(8):894–897, Aug 2021. `https://doi.org/10.1038/s41567-021-01271-7`, `https://arxiv.org/abs/2008.06478`.

[Mor76] Hans Moravec. The role of raw power in intelligence, May 1976. `https://web.archive.org/web/20160303232511/,http://www.frc.ri.cmu.edu/users/hpm/project.archive/general.articles/1975/Raw.Power.html`.

[Nay23] Chetan Nayak. Microsoft achieves first milestone towards a quantum supercomputer. Technical report, Microsoft Azure Quantum Blog, June 2023. `https://cloudblogs.microsoft.com/quantum/2023/06/21/microsoft-achieves-first-milestone-towards`, -a-quantum-supercomputer/.

[Nea24] M. A. Norcia and et al. Iterative assembly of ^{171}yb atom arrays in cavity-enhanced optical lattices, 2024.

[NK23] Hartmut Neven and Julian Kelly. Suppressing quantum errors by scaling a surface code logical qubit. Technical report, Google Research, February 2023.

[OK23] Sangchul Oh and Sabre Kais. Comparison of quantum advantage experiments using random circuit sampling. *Phys. Rev. A*, 107:022610, Feb 2023.

[Orm21] Hilarie Orman. Internet security and quantum computing. Cryptology ePrint Archive, Paper 2021/1637, 2021. `https://eprint.iacr.org/2021/1637`.

[PCZ22] Feng Pan, Keyang Chen, and Pan Zhang. Solving the sampling problem of the sycamore quantum circuits. *Phys. Rev. Lett.*, 129:090502, Aug 2022.

[Reg24] Oded Regev. An efficient quantum factoring algorithm, 2024. `https://arxiv.org/abs/2308.06572`.

[Rud23] Terry Rudolph. What is the logical gate speed of a photonic quantum computer?, June 2023. `https://quantumfrontiers.com/2023/06/21/`, what-is-the-logical-gate-speed-of-a-photonic-quantum-computer/.

[RV23] Seyoon Ragavan and Vinod Vaikuntanathan. Space-efficient and noise-robust quantum factoring. Cryptology ePrint Archive, Paper 2023/1501, 2023. `https://eprint.iacr.org/2023/1501`.

[SG22] Paul Smith-Goodson. Psiquantum has a goal for its million qubit photonic quantum computer to outperform every supercomputer on the planet. *Forbes Magazine*, September 2022. `https://www.forbes.com/sites/moorinsights/2022/09/21/`, psiquantum-has-a-goal-for-its-million-qubit-photonic, -quantum-computer-to-outperform-every-supercomputer, -on-the-planet/?sh=131da0958db3.

[Sta23a] Staff. DARPA-funded research leads to quantum computing breakthrough, December 2023. `https://www.darpa.mil/news-events/2023-12-06`.

[Sta23b] News Staff. Quantinuum H-series quantum computer accelerates through 3 more performance records for quantum volume: 217, 218, and 219. *Quantinuum.com*, June 2023. `https://www.quantinuum.com/news/`, quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219.

[Sta24] IonQ Staff. How we achieved our 2024 performance target of #AQ 35. Technical report, IonQ.com, January 2024.

[Swa24] Matt Swayne. Harnessing the power of neutrality: Comparing neutral-atom quantum computing with other modalities. *Quantum Computing*, February 2024.

`https://thequantuminsider.com/2024/02/22/`, harnessing-the-power-of-neutrality-comparing-neutral-atom-quantum-computing-with-other-modalities/.

[Tea24] Quantum Circuits Team. What are quantum circuits' dual resonator qubits and why are they a breakthrough? Technical report, Quantum Circuit, February 2024. `https://quantumcircuits.com/dual-resonator-qubits-breakthrough/`.

[Tim23] John Timmer. Atom computing is the first to announce a 1,000+ qubit quantum computer. *Ars Technica*, October 2023.

[WDE+23] Karen Wintersperger, Florian Dommert, Thomas Ehmer, Andrey Hoursanov, Johannes Klepsch, Wolfgang Mauerer, Georg Reuber, Thomas Strohm, Ming Yin, and Sebastian Luber. Neutral atom quantum computing hardware: performance and end-user perspective. *EPJ Quantum Technology*, 10(1):32, Aug 2023. `https://doi.org/10.1140/epjqt/s40507-023-00190-1`.

[Wea23] Aaron J. Weinstein and et al. Universal logic with encoded spin qubits in silicon. *Nature*, 615(7954):817–822, Mar 2023. `https://doi.org/10.1038/s41586-023-05777-3`.

[Wil23] Alex Wilkins. Record-breaking quantum computer has more than 1000 qubits. *New Scientist*, October 2023. `https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/`.

[YZ22] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. IACR eprint, June 2022.

[ZVBL23] Alexander Zlokapa, Benjamin Villalonga, Sergio Boixo, and Daniel A. Lidar. Boundaries of quantum supremacy via random circuit sampling. *npj Quantum Information*, 9(1):36, Apr 2023. `https://doi.org/10.1038/s41534-023-00703-x`.

[ZWD+20] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao-Yan Yang, Wei-Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai-Le Liu, Chao-Yang Lu, and Jian-Wei

Pan. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.