Scientific Research Publishing

Journal of Applied Mathematics and Physics, 2025, 13(12), 4341-4354
https://www.scirp.org/journal/jamp
ISSN Online: 2327-4379
ISSN Print: 2327-4352

Quantum Computing and Quantum Sensing: A Pedagogical Introduction to Emerging Quantum Technologies

Andy Ling[1], Neil Pandya[2]

[1]Syosset High School, Syosset, USA
[2]Physic Department, Stevens Institute of Technology, Hoboken, USA
Email: andyling928@gmail.com

How to cite this paper: Ling, A. and Pandya, N. (2025) Quantum Computing and Quantum Sensing: A Pedagogical Introduction to Emerging Quantum Technologies. *Journal of Applied Mathematics and Physics*, **13**, 4341-4354.
https://doi.org/10.4236/jamp.2025.1312239

Received: October 15, 2025
Accepted: December 16, 2025
Published: December 19, 2025

Abstract

Quantum technologies, mainly quantum computing and quantum sensing are emerging as new applications of quantum mechanics for practical use. Two notable advancements in quantum computing and quantum sensing respectively are Shor's algorithm and nitrogen vacancy centers in diamond lattices. Shor's algorithm leverages certain properties of quantum computers to factor large numbers faster than any classical algorithm. Nitrogen vacancy centers leverage spin defects to sense even very small signatures of magnetic fields. This review article aims to provide a pedagogical introduction and overview of these emerging platforms for quantum technology.

Keywords

Quantum Technologies, Quantum Computing, Quantum Sensing, Shor's Algorithm, Nitrogen Vacancy Centers

1. Introduction

Following the discovery of quantum mechanics in the early 20th century, efforts have been made to find potential applications using the unusual properties of quantum particles to improve technology. The most well known of these applications is quantum computing. In quantum computation, the non-classical nature exhibited by quantum systems is leveraged to more rapidly compute the solutions to certain problems compared to the systems in classical computers. One such problem is integer factorization. While factoring small integers is a trivial process, it quickly becomes an extremely difficult problem to solve computationally for very large numbers. In fact, the best algorithms run in sub-exponential time [1].

The General Number Field Sieve (GNFS) is the fastest known classical algorithm for factoring integers. To better appreciate the comparison of the time it takes to run GNFS with the time it takes to run a quantum algorithm that accomplishes the same end, we briefly explain big-O notation. Saying that an algorithm runs in time $O\left(f\left(N\right)\right)$ is saying that the time that it takes the algorithm to run is directly proportional to a function f of the integer being factored, N, when that integer is very large. Thus, the number of steps it takes to run GNFS can be expressed as

$$\exp\left(\left(\left(64/9\right)^{1/3}+o\left(1\right)\right)\left(\ln N\right)^{1/3}\left(\ln\ln N\right)^{2/3}\right),$$

where $o\left(1\right)$ is a term that approaches 0 as N goes to infinity. Compare that with the polynomial time that Peter Shor proved it would take with a quantum computer [2]:

$$O\left(\left(\ln N\right)^{3}\right)$$

This run time is the basis for most modern public key cryptographic systems. However, using the power of quantum mechanics, an algorithm that can rapidly factor large integers has been discovered, which is known as Shor's algorithm. In fact, this is why the National Institute of Standards and Technology is currently hosting a competition to find a new method of public key cryptography. While quantum computers show great promise for being able to perform computations in minutes that would take classical computers decades if not centuries, there is one major hurdle: The qubits used by quantum computers as of now are too faulty to be able to perform the large amount of calculations required for anything useful. This is because quantum systems are extremely sensitive to external influences and as a result, they must be isolated from all external physical agents that can influence their state. These factors include electromagnetic radiation, interaction with other particles, and in some cases temperatures. The latter is the reason why many quantum technologies require cryogenic control.

While this sensitivity of quantum systems to external influence might seem like a curse, it may actually be a blessing in disguise. A lesser known application of quantum mechanics seeks to use this sensitivity that plagues quantum systems to detect very small signatures of environmental conditions including electromagnetic fields, pressure, etc. This field of quantum technology goes under the name, "quantum sensing". Surprisingly, this technology is not new as the most notable application of quantum sensing is the atomic clock, which uses the oscillating behavior of atoms as they interact with light of a specific frequency to keep track of time to extremely high degrees of accuracy. Newer applications of quantum sensing include detecting subtle changes in magnetic fields, which have applications in medical imaging and material science.

2. Background

To understand these new quantum technologies, we first must understand the fundamentals of quantum physics. In the macroscopic world of physics, entities

are modeled as either particles or waves, but not both. Particles have three properties: position, mass, and velocity (or, equivalently, momentum, which is the product of mass and velocity). Waves also have two properties, wavelength and frequency, which describe how their oscillations occur in space and time, respectively. In the quantum world, all entities exhibit properties of both particles and waves, an idea known as wave-particle duality. An example of an entity that is both a wave and a particle is light. Light is reflected when it bounces off objects, which suggests that light is a particle, but light also exhibits interference patterns, something that only waves can do in classical physics.

One of the pillars of quantum mechanics is the De Broglie hypothesis, which stipulates that all matter exhibits wave-like properties, and the momentum of an object can be derived from an object's wavelength using the following equation:

$$p = \frac{h}{\lambda}$$

where p is the momentum of the object, h is Planck's constant, a fundamental constant of nature equal to approximately 6.62610−31J s, and λ is the wavelength.

A fundamental aspect of classical systems is that they all have deterministic evolution, meaning that you can predict the future, as well as the past, of a system by applying the necessary equations of motion once its initial conditions are known. Quantum systems also have deterministic evolution, however, due to the Heisenberg uncertainty principle, it is impossible to measure all the variables of a quantum system with arbitrary precision, meaning that the way in which we measure a quantum system is probabilistic.

The way we describe a quantum particle, is with the wavefunction, denoted $\Psi(x)$, which is a complex valued function that takes in a position, represented by x, and outputs a complex number whose square magnitude $|\Psi(x)|^2$ represents the probability of finding the quantum particle at the position.

Two other aspects of quantum mechanics are entanglement and superposition. Entanglement is the property exhibited when two particles interact; they behave in a way such that the states of both particles are dependent. In fact, this dependency persists even if both particles are brought many kilometers apart. When a system is in a superposition state, this means the system is in a single quantum state that is a weighted sum of possibilities.

The spin of a quantum particle is a fundamental property that is essential for the understanding and control of quantum systems, and will be covered in more detail later in the article. Contrary to its name, it has nothing to do with the actual spinning motion of a particle. What it actually represents is the intrinsic angular momentum of a particle, a quantum analogue of a magnetic moment, much like the one of a compass needle. Electrons are fairly simple particles, and they only have two spin states—up or down. Note that this is not the same as the North/South poles on a magnet. Particles such as electrons can only have a half integer spin. Electrons, more specifically, can only have spin $+\frac{1}{2}$ or $-\frac{1}{2}$

because a quantum particle's spin is intrinsic to that particle, but it can be flipped.

The quantum systems used in both quantum computing and quantum sensing have two energy levels, anything more is too complicated, which is why we only use a binary system for all computers. The two levels are usually one ground state and one excited state. A way to represent these two-level systems geometrically is on the unit sphere. Because of superposition, a vector, which represents the quantum system, on the Bloch Sphere can be represented as follows: (Note that both $|0\rangle$ and $|1\rangle$ represent the vectors [1, 0] and [0, 1], respectively).

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex numbers such that $|\alpha|^2$ and $|\beta|^2$ represent the probability that the quantum state collapses into $|0\rangle$ or $|1\rangle$ respectively when measured. The particle must be in either one of these states, a condition called normalization, which implies that

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

Because all complex numbers have a polar representation in the form of $re^{i\phi}$, where ϕ is the angle of the polar representation of the complex number and r is the magnitude, we can rewrite this equation as follows:

$$|\Psi\rangle = |\alpha|\exp(i\phi_\alpha)|0\rangle + |\beta|\exp(i\phi_\beta)|1\rangle \tag{3}$$

Next, we introduce the concept of the "global phase". To do that, we contrast it with "relative phase." Consider a qubit for example:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

One may change the phase of one component, but not the other by multiplying that component by a phase factor, $e^{i\pi}$, for example:

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

As you can see, $|\Psi\rangle$ and $|\Psi'\rangle$ are physically different, *i.e.*, they give different measurement probabilities. However, if one instead chooses to multiply the *whole* state by a phase factor:

$$e^{i\pi}|\Psi\rangle = -|\Psi\rangle.$$

$|\Psi\rangle$ and $-|\Psi\rangle$ are physically indistinguishable, since all measurable quantities depend only on relative ratios between components, and not the overall scale. When multiplying the *whole* state by a phase factor, the phase factor is called a "global phase". In summary,

$$|\Psi\rangle = e^{i\phi}|\Psi\rangle. \tag{4}$$

For a two-level system to be representable on the Bloch sphere, it must meet two criteria:

1) The wavefunction has to be normalized, Equation (3), such that $|\Psi|^2 = 1$.

2) A global phase does not matter, Equation (4), meaning $|\Psi\rangle$ and $e^{i\phi}|\Psi\rangle$

represent the same quantum state.

The reason the above criteria is important is because it allows us to reduce the number of variables from four to two as follows:

Let $\phi = \phi_\beta - \phi_\alpha$.

$$|\Psi\rangle = e^{-i\phi_\alpha}|\Psi\rangle = e^{-i\phi_\alpha}\left(|\alpha|e^{i\phi_\alpha}|0\rangle + |\beta|e^{i\phi_\beta}|1\rangle\right)$$

$$= |\alpha||0\rangle + |\beta|e^{i(\phi_\beta - \phi_\alpha)}|1\rangle = |\alpha||0\rangle + |\beta|e^{i\phi}|1\rangle$$

(From Equation (4); substituting Equation (3). Furthermore, because of Equation (2), which matches the pythagorean identity, we might as well construct an angle θ such that $\alpha = \cos\left(\frac{\theta}{2}\right)$ and. That leaves us with

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle \quad \text{with } 0 \le \theta \le \pi, 0 \le \phi < 2\pi. \tag{5}$$

To understand why we choose $\frac{\theta}{2}$ and not just θ, we must understand the Bloch sphere, Figure 1.

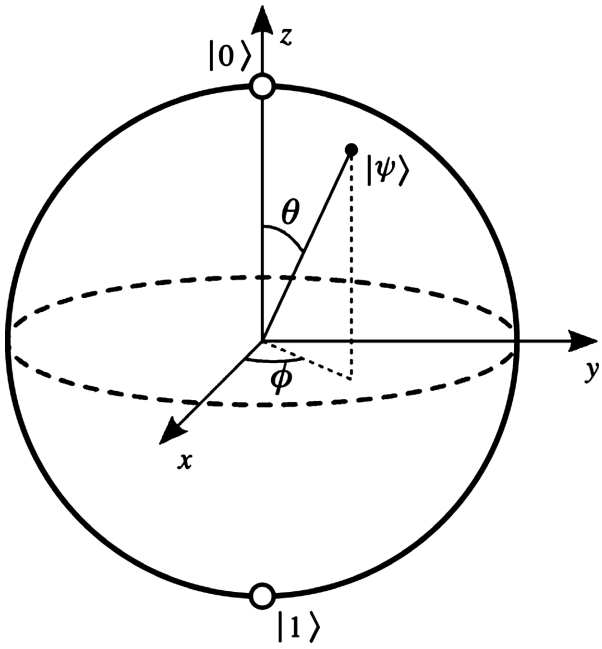


Figure 1. Bloch sphere representation of a qubit state [3].

The "north pole" of the sphere represents $|0\rangle$ while the "south pole" represents $|1\rangle$. If state vector $|\Psi\rangle$ points directly north, it has a probability of 1 of being in $|0\rangle$. Likewise, if state vector $|\Psi\rangle$ points directly south, it has a probability of 1 of being in $|1\rangle$. Points on the surface of the sphere correspond to different superpositions of $|0\rangle$ and $|1\rangle$. Looking at Equation (5), we use $\frac{\theta}{2}$ and not θ so that an angle of 0 points to $|0\rangle$ since $\cos\left(\frac{0}{2}\right) = 1$ and $\sin\left(\frac{0}{2}\right) = 0$,

while an angle of π points to $|1\rangle$ since $\cos\left(\frac{\pi}{2}\right)=0$ and $\sin\left(\frac{\pi}{2}\right)=1$.

3. Quantum Sensing

The ability to sense very weak magnetic fields has important applications in a wide variety of contexts. These include navigation in remote areas where GPS does not work; detecting rock and minerals underground for mining; and sensing brain activity down to even the faintest neuron impulse for biomedical applications. Such problems call for a new type of sensor, one that uses a quantum system that is especially sensitive to magnetic fields, but not too strongly affected by its immediate environment. Examples of such environments include other atoms or particles in the structure that hosts the quantum system. In such cases, the energy levels of the quantum system are sensitive mostly to the physical quantity one is trying to measure. A very good candidate for realizing such quantum systems is defect states in what would otherwise be perfect crystalline materials. A prime example are nitrogen vacancy defects in diamond, which have attracted great interest in the area of quantum sensing.

Nitrogen vacancies (NV) are essentially impurities in a diamond lattice where a single carbon atom is replaced by a nitrogen atom with a vacancy next to it. A representation of an NV center is shown in Figure 2.

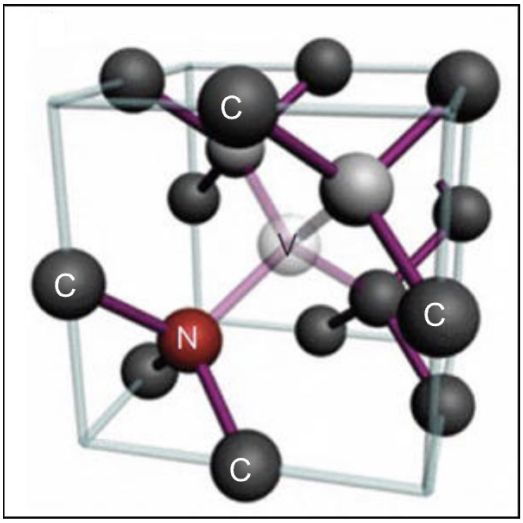


Figure 2. The black spheres represent the carbon atoms that contain the NV center, which is represented by the red sphere with the "N", and the transparent sphere with the "V" represents the vacancy. Readapted from the Growth of Diamond Thin Film and Creation of NV Centers [4].

Because of the vacancy in the NV center, an electron occupies the vacancy in a similar way to how electrons are shared in a covalent bond. A mental model used by physicists is to understand the NV center as a molecule, with the second atom being a missing atom instead of one that is actually there. The nitrogen atom has seven electrons, of which six are paired (three pairs of up-down spins) and one is

left unpaired (Figure 3).

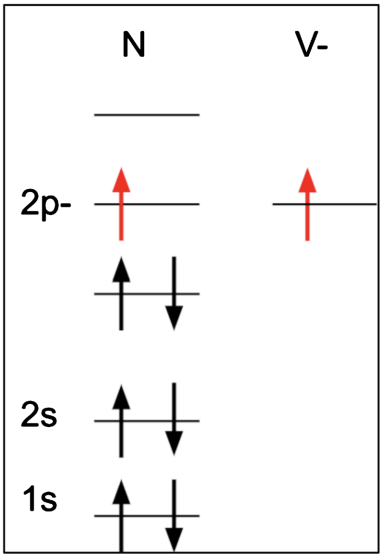


Figure 3. A representation of the electron configuration of the NV center. The arrows to the left represent the electrons in the nitrogen atom, and the arrows to the right represent the electrons in the vacancy. The 2 red arrows represent the unpaired electrons.

The vacancy, when negatively charged, will host an extra electron, taken from the neighboring carbons. Therefore, the NV center will host two unpaired valence electrons (See Figure 3), leaving four possible states of the NV center based on the spins of those unpaired electrons: $|++\rangle$, $|--\rangle$, $|+-\rangle$, $|-+\rangle$. However, the electron pairs in the $|+-\rangle$ and $|-+\rangle$ states are indistinguishable, so in practice there are only three states. As mentioned before, each electron has spin $\frac{1}{2}$ leading to $|++\rangle = |+1\rangle$, $|--\rangle = |-1\rangle$, $|+-\rangle = |0\rangle$, with the +1, −1, and 0 representing the net magnetic moment of the NV center (also known as the magnetic quantum number). It is this magnetic moment that makes these states of the NV center sensitive to magnetic fields, analogous to the sensitivity of compass needles to Earth's magnetic field mentioned earlier.

When there is no magnetic field and in the hypothetical absence of the surrounding atoms, the three states are degenerate, meaning that all three states have the same energy level. Because the NV center is surrounded by carbon atoms, the energy levels are split, with $m = 0$ becoming the ground state and $m = \pm 1$ becoming the excited states as shown in Figure 4.

This occurs due to the lack of symmetry in the carbon lattice [6]. However, the $m = -1$ and $m = +1$ still remain degenerate in the absence of a magnetic field. The introduction of a magnetic field leads to a further splitting of the $m = \pm 1$ into the $m = +1$ and $m = -1$ energy levels, known as the Zeeman effect. Additionally, the amount of separation between these energy levels is dependent on the strength of the magnetic field. More specifically, the energy level of the $|-1\rangle$ decreases and the $|+1\rangle$ increases in energy level as the magnetic field strength in-

creases. The energy difference E between $|-1\rangle$ and the $|+1\rangle$ is also directly proportional to the strength of the magnetic field (see also Figure 4):

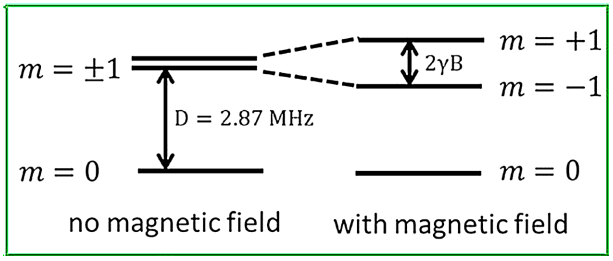


Figure 4. The energy difference in Hz between $m=-1$ and $m=+1$ is equal to $2\gamma B$, where B is the magnetic field strength and $\gamma = \frac{g\mu_B}{h}$ [5].

$$E = 2g\mu_B B, \tag{6}$$

where μ_B is the bohr magneton, a fundamental constant of nature, g is the Lande g-factor, and B is the strength of the magnetic field.

To induce a transition of the quantum state from state $|0\rangle$ to one of the higher-energy states of $|-1\rangle$ or $|+1\rangle$, we irradiate the NV center with electromagnetic waves at a frequency of around 2.88 GHz (microwave) when there is no external magnetic field. The need for a specific frequency is due to quantum mechanical energy conservation, in other words the energy carried by the light has to match the energy difference between the energy levels of the quantum system. This property is known as resonance. After driving the system at resonance, an important question to answer is whether or not a system is in state $|0\rangle$, $|-1\rangle$, or $|+1\rangle$. This is where a concept called Rabi oscillation comes in handy. It is known that when light of the correct frequency is directed towards a quantum system, it will cause the quantum state to oscillate between the lower and higher energy levels. One cycle of these oscillations is known as a Rabi cycle, which is crucial to both quantum computing and sensing. We use our understanding of Rabi oscillations by timing the drive and "stopping" the system at a particular point in the oscillation, effectively controlling which state the quantum system is in.

The first step in measuring a magnetic field using an NV center is to excite some of the NV centers from $|0\rangle$ to $|+1\rangle$ or $|-1\rangle$ by irradiating the system with microwaves. The next step is to quantify the energy gap between $|+1\rangle$ or $|-1\rangle$, caused by the Zeeman splitting, which is directly proportional to the magnetic field. To do this, we use a phenomenon known as photoluminescence, whereby a system illuminated with visible light will radiate back light of lower frequency. Photoluminescence can be detected in NV centers. If the light is not resonant with the transition from $|0\rangle$ to $|1\rangle$, then it will stay in $|0\rangle$ and thus give the highest photoluminescence. If the light is resonant with the transition, it will oscillate between $|0\rangle$ and $|-1\rangle$ and thus we will see a decrease in photoluminescence, otherwise known as a "dip" in the frequency. This is known as optically detected magnetic resonance (ODMR). The same thing happens with the $|0\rangle$ and $|+1\rangle$ tran-

sition. The magnetic field pushes the $|+1\rangle$ and $|-1\rangle$ states symmetrically apart. The two states have a difference of frequency,

$$\Delta f = f_{+1} - f_{-1}.$$

We can use Equation (6) to determine Δf, since $E = h\Delta f$. Therefore,

$$h\Delta f = 2g\mu_B B$$

$$\Delta f = 2\frac{g\mu_B}{h}B,$$

$$\text{or} \quad \Delta f = 2\gamma B,$$

where $\gamma = \frac{g\mu_B}{h}$, which is called the gyromagnetic ratio of the NV.

This is only one of the many types of quantum sensors that are being discovered and studied as a result of the second quantum revolution, but what makes NV centers so special is their ability to be leveraged at standard temperature and pressure, something that most qubits used in quantum sensors or computers cannot do. As a result they have greater practical use as magnetic field sensors since there is no need to use complex setups including cryogenic cooling and other bulky sample environments.

4. Quantum Computing

In a classical computer, a bit can only be in two possible states: 0 and 1. In a quantum computer, a qubit has a probability of being in both states as a result of superposition, Equation (1). To understand how useful this is, consider n qubits. The combined quantum state of these qubits is the superposition of every possible string of length, n. For example, consider $n = 3$. Equation (1) becomes

$$|\Psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle.$$

That is a superposition of all 8 possible classical bit strings of length 3. This is very useful because a quantum computer can hold all 2^n possible classical states in superposition at once. The problem arises when we take a measurement of the quantum system. Only one of the possible combinations is revealed and all others are lost. Quantum algorithms are therefore designed in order to get the correct solution to constructively interfere and for incorrect solutions to destructively interfere. This is due to the wave-particle duality of qubits, allowing for wavelike behaviors such as interference. This wavelike behavior is leveraged in Grover's amplitude-amplification algorithm. It provides a systematic way of increasing the amplitude of the correct solution, equivalently increasing its probability. The algorithm applies a sequence of quantum operations that act on the state driving it towards the correct solution [7].

As classical computers have classical logic gates, quantum computers have their own quantum logic gates, whose operations can be represented on the Bloch sphere. We will only cover the most basic quantum gates in this review. For a more

comprehensive treatise on quantum gates, see [8].

Each quantum gate can be thought of as performing a rotation of the vector on the Bloch sphere. For example, the Pauli X gate rotates the vector on the Bloch sphere 180 degrees around the X axis of the Bloch sphere, and similarly for the Pauli Y and Z gates (See Figure 5).

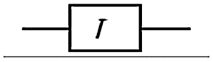
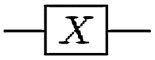
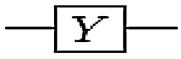
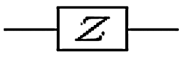
No.	Name of gate	Circuit symbol	Matrix equivalency	Qubit conversion When Applied
1	Pauli I gate		$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\|0\rangle \to I \to \|0\rangle$ $\|1\rangle \to I \to \|1\rangle$ $\alpha\|0\rangle+\beta\|1\rangle \to I \to \alpha\|0\rangle+\beta\|1\rangle$
2	Pauli X gate		$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|0\rangle \to X \to \|1\rangle$ $\|1\rangle \to X \to \|0\rangle$ $\alpha\|0\rangle+\beta\|1\rangle \to X \to \alpha\|1\rangle+\beta\|0\rangle$
3	Pauli Y gate		$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\|0\rangle \to Y \to i\|1\rangle$ $\|1\rangle \to Y \to -i\|0\rangle$ $\alpha\|0\rangle+\beta\|1\rangle \to Y \to \alpha i\|1\rangle - i\beta\|0\rangle$
4	Pauli Z Gate		$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|0\rangle \to Z \to \|0\rangle$ $\|1\rangle \to Z \to -\|1\rangle$ $\alpha\|0\rangle+\beta\|1\rangle \to Z \to \alpha\|0\rangle-\beta\|1\rangle$

Figure 5. Quantum gates [8]. Each gate has a circuit symbol just as classical gates do. The matrix equivalency column shows the matrix used to multiply a vector representing a quantum state such as $(0,1)$ in order to rotate it on the Block sphere. The final column explains what happens to the probability amplitudes attached to each basis state in the superposition state. For example, the Pauli I gate effectively does nothing to each basis state in the superposition state. The Pauli X gate swaps the probability amplitudes attached to each basis state.

The Pauli X gate can be thought of as the quantum analogue of the classical NOT gate, since it flips the state of the qubit, but the Pauli Y and Z gates do not have simple classical analogs.

In the introduction to the paper, "faulty" qubits were mentioned as being one of the challenges of quantum computing. However, researchers have developed quantum-error-correction (QEC) schemes to overcome such challenges [9]. The idea behind these schemes is to allow imperfect qubits to exist, but combine groups of them and treat them like one perfect qubit. The imperfect qubits are called "physical" qubits since they exist at the hardware level inside the quantum computer. These qubits are "noisy," meaning they are unreliable since quantum systems are so sensitive as discussed in the Quantum Sensing section of this paper. The perfect qubits are called "logical" qubits, which are the higher-level units of information we build out of the physical qubits. The information that each logical qubit contains is spread out into many physical qubits. Once that happens, the computer looks at each qubit for indirect indicators of error so as not to measure the qubits directly which would collapse the state. These kinds of measurements are called, "syndrome measurements," because the computer is looking at the "symptoms," so to speak, of the error "syndrome." An example of an error could be a qubit flipping states from $|1\rangle$ to $|0\rangle$ or vice versa. Whatever error the computer notices, it fixes.

The most commonly used algorithm for public key cryptography today is Rivest-Shamir-Adleman (RSA). The way it works is as follows: consider Alice and Bob. They need to communicate a secure message, but it's too difficult to meet up and exchange the key required to decrypt the cipher text, so they do the following: Alice and Bob each think of two very large prime numbers and multiply them together. The two prime numbers are the private key that is used to decrypt the message. The product is the public key that is used to encrypt the message. When one person wants to send the other person a message, they take the public key of the other person, encrypt their message and send it. Without knowing the two prime factors, an attacker cannot decrypt the message. Shor's algorithm threatens this security however.

To understand Shor's algorithm, we must review some basics on modular arithmetic. First we review the mod operator:

$$a \bmod n = \text{remainder when } a \text{ is divided by } n.$$

Two integers a and b are relatively prime when they share no common factors other than 1. If a and b are relatively prime positive integers, there will always be a smallest number r such that a^r leaves a remainder of 1 when divided by b. For example, suppose

$$a = 7,\ b = 15$$

Since 7 and 15 share no common factors, they are relatively prime, and we can find the smallest integer r such that

$$7^r \bmod 15 = 1.$$

In this case, $r = 4$ since

$$7^4 = 2401 \quad 2401 \bmod 15 = 1$$

Once that r is found, we can find infinitely many such powers that yield a remainder of 1 when dividing by b. Those powers are repeated every r steps. In our example, since $r = 4$, we will have a remainder of 1 every 4^{th} power of 7:

$$7^4 \bmod 15 = 1 \quad 7^8 \bmod 15 = 1 \quad 7^{12} \bmod 15 = 1 \vdots$$

In other words, for any positive integers k and n, the numbers a^k and a^{k+nr} leave the same remainder when divided by b. In mathematics, this is known as periodic behavior. The purpose of Shor's algorithm is to find this number r in a computationally efficient manner through the use of a quantum computer, which can then be used to factor a large number.

The full Shor's algorithm used in factoring a large number (denoted N) is as follows:

1) Pick a number k smaller than N that most likely is relatively prime to N.

2) Find the smallest number r such that k^r leaves a remainder of 1 when divided by N. It is at this step that quantum computation makes this algorithm much more efficient than classical computation.

3) If r is odd, go back to step 1. If r is even, go to step 4.

4) Because k^r leaves a remainder of 1 when divided by N, k^r-1 leaves a remainder of 0. We then factor k^r-1 into $\left(k^{\frac{r}{2}}-1\right)\left(k^{\frac{r}{2}}+1\right)$.

5) If $k^{\frac{r}{2}}+1$ or $k^{\frac{r}{2}}-1$ leaves a remainder of 0 when divided by N, then go back to step 1. This is because assuming that N is the product of two primes, which is most common in RSA cryptography, we want both $k^{\frac{r}{2}}+1$ and $k^{\frac{r}{2}}-1$ to each have only 1 of the factors of N.

6) Calculate the greatest common denominator between N and $k^{\frac{r}{1}}-1$, and our result is a prime factor of N. Readapted from [10].

Because RSA relies on the computational difficulty of factoring large numbers, even with classical algorithms, Shor's algorithm poses a serious threat to cybersecurity. Thankfully, the number of qubits required to break RSA using Shor's algorithm is well beyond the amount of qubits we can currently achieve in a quantum computer, but innovations in quantum technology mean that all of our current cybersecurity architecture that uses RSA may be at future risk.

Because of this, governments and researchers are thinking ahead and coming up with encryption strategies that are valid even in a "post-quantum" world. In the US, this research is led by the National Institute of Standards and Technology (NIST). The leading cryptographic encryption systems being developed come from a family of such systems called the Cryptographic Suite for Algebraic Lattices (CRYSTALS). An algebraic lattice is a grid of points that follow a consistent and repeating pattern. One may come up with a problem involving a lattice with the goal of finding something out about the lattice such as finding the shortest non-zero vector or which two points are the closest to each other. In particular, there are "hard" problems, in which no efficient algorithm is known to solve such a problem. There are two CRYSTALS-based encryption systems of note, currently: CRYSTALS-Kyber and CRYSTALS-Dilithium. The CRYSTALS-Kyber encryption was selected by NIST as the first standardized post-quantum key-establishment method [11]. NIST selected Dilithium as its primary post-quantum digital-signature standard.

5. Outlook

This relatively short review gave a simplified overview with some specific examples of how emerging quantum technologies work. The second quantum revolution will bring about profound changes that will impact the world forever, from the average person to the world leader, everyone will be affected one way or another. As demonstrated with the invention of Shor's algorithm, quantum computers pose a threat to the encryption schemes that both civilians and militaries rely on for privacy, secrecy, and to ensure authenticity between virtual transactions. The main outstanding challenge is how to create a quantum computer with enough qubits to be practical. It is estimated that to break modern RSA encryption schemes, it would require at least a couple thousand perfect qubits. Because the qubits in

current quantum computers are not perfect, they will likely require more to account for errors.

The field of quantum sensing is similarly rife with excitement and innovations. NV centers are very powerful and sensitive magnetometers (among other things) but are not the only type of quantum sensor that is being explored. Other types of defects, like Silicon-vacancy centers also in diamond, or defects in different materials, such as hexagonal Boron Nitride centers are potential alternatives to NV centers regarding quantum magnetometry [12].

Even more exotic developments are taking place at the frontier of quantum technology. For example, atom interferometry shows promise for use in highly sensitive gravitometers. Researchers have also investigated the use of entanglement in quantum key distribution, leveraging the fundamental laws of physics to create a theoretically unbreakable form of encryption. These new technologies hold great potential for the future of science.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Bansimba, G.R. and Babindamana, R.F. (2025) Integer Factorization: Another Perspective. arXiv: 2507.07055.

[2] Shor, P.W. (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, **26**, 1484-1509. https://doi.org/10.1137/s0097539795293172

[3] Scholbach, J. (2006) Bloch Sphere Illustration. https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg

[4] Ma, Y.P., Chen, J.B. and Wang, C.H. (2022) Growth of Diamond Thin Film and Creation of NV Centers. In: David, G., Ed., *Applications and Use of Diamond*, IntechOpen.

[5] Crawford, S.E., Shugayev, R.A., Paudel, H.P., Lu, P., Syamlal, M., Ohodnicki, P.R., *et al.* (2021) Quantum Sensing for Energy Applications: Review and Perspective. *Advanced Quantum Technologies*, **4**, Article ID: 2100049. https://doi.org/10.1002/qute.202100049

[6] Doherty, M.W., Manson, N.B., Delaney, P., Jelezko, F., Wrachtrup, J. and Hollenberg, L.C.L. (2013) The Nitrogen-Vacancy Colour Centre in Diamond. *Physics Reports*, **528**, 1-45. https://doi.org/10.1016/j.physrep.2013.02.001

[7] Grover, L.K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing—STOC'*96, Philadelphia, 22-24 May 1996, 212-219. https://doi.org/10.1145/237814.237866

[8] Dejen, A. and Ridwan, M. (2022) A Review of Quantum Computing. *International Journal of Mathematical Sciences and Computing*, **8**, 49-59. https://doi.org/10.5815/ijmsc.2022.04.05

[9] Brady, A.J., Eickbusch, A., Singh, S., Wu, J. and Zhuang, Q. (2024) Advances in Bosonic Quantum Error Correction with Gottesman-Kitaev-Preskill Codes: Theory, Engineering and Applications. *Progress in Quantum Electronics*, **93**, Article ID: 100496. https://doi.org/10.1016/j.pquantelec.2023.100496

[10] Ekert, A. and Jozsa, R. (1996) Quantum Computation and Shor's Factoring Algorithm. *Reviews of Modern Physics*, **68**, 733-753. https://doi.org/10.1103/revmodphys.68.733

[11] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Miller, C., *et al.* (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Technical Report NIST IR 8240, National Institute of Standards and Technology.

[12] Fang, H., Wang, X., Marie, X. and Sun, H. (2024) Quantum Sensing with Optically Accessible Spin Defects in Van Der Waals Layered Materials. *Light*: *Science & Applications*, **13**, Article No. 303. https://doi.org/10.1038/s41377-024-01630-y