# Cryptography Apocalypse

# Cryptography Apocalypse

## Preparing for the Day When Quantum Computing Breaks Today's Crypto

Roger A. Grimes

WILEY

**Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto**

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
www.wiley.com



Published simultaneously in Canada

ISBN: 978-1-119-61819-5
ISBN: 978-1-119-61821-8 (ebk)
ISBN: 978-1-119-61822-5 (ebk)

Manufactured in the United States of America



**Library of Congress Control Number:** 2019946679

# Contents

# Contents

# Introduction

In the late 1990s the world was consumed by a coming computer problem known as Y2K, which stood for the Year 2000. The difficulty was that most of the world's devices, computers, and programs to that point in time recorded dates using only the last two digits of the year. From a programmatic level, they couldn't tell the difference between 1850, 1950, and 2050.

When 1999 turned into 2000, many of those computers and programs would not have been able to correctly process any calculation involving two-digit dates in the new century. There had been many known failures by programs and devices that were already using dates in the future (such as scheduling and warranty programs). Symptoms of failed devices and programs ranged from visible errors to errors that happened but were not readily visible (which can be extremely dangerous) to complete device and program shutdowns.

The problem was that although we knew that a sizable percentage of devices and programs were impacted, no one knew which untested things were fine and didn't need to be updated and which had to be updated or replaced before January 1, 2000. There was a two- to three-year rush to find out what was broken and what was fine. As with many slow-moving potential catastrophes, most of the world did little to nothing to prepare until the last few months. The last-minute global rush created a bit of a worldwide panic about what would happen as clocks moved into the new century. There was even a fantastically bad 1999 disaster movie (`www.imdb.com/title/tt0215370`) that had planes dropping out of the sky along with other worldwide cataclysmic mayhem.

In the end, when Y2K rolled around, it was a bit of a dud if you wanted real life to be like the movies. There were issues, but for the most part the world continued as usual. There were devices and programs that failed to handle the newer dates appropriately, but most major systems worked correctly. There were no falling planes, fires, or burst dams. For many people who were expecting disaster outcomes, it was a bit of a letdown—so much so that, over time the term Y2K evolved to become a unofficial synonym for overly hyped events involving premature panic with little resulting damage.

What most people today don't realize is that Y2K was anticlimactic precisely because we had years of preparation and warning. Most major systems were checked for Y2K issues and replaced or updated as needed. Had the world not become aware of it and not done anything, Y2K would have certainly been far, far worse (albeit, I'm still not sure planes would be falling out of the sky). Y2K wasn't a premature panic dud. It was the foreseeable outcome from years of preparation, demonstrating the success of what humanity can do when faced with a looming digital problem.

## The Coming Quantum Day of Reckoning

Most of the world doesn't know it yet, but we are in another even more momentous, looming Y2K moment, except this one is likely already causing serious problems and damage. Worse, we can't stop all the damage even if we begin preparing now. There are organizations sustaining harm today that will not be able to program their way out. Nation-states and corporate adversaries are likely already taking advantage of the problem.

Quantum computers will likely soon break traditional public key cryptography, including the ciphers protecting most of the world's digital secrets. These soon-to-be-broken protocols and components include HTTPS, TLS, SSH, PKI, digital certificates, RSA, DH, ECC, most Wi-Fi networks, most VPNs, smartcards, HSMs, most cryptocurrencies, and most multifactor authentication devices that rely on public key crypto. If the list just included HTTPS and TLS, it would cover most of the Internet. On the day that quantum computing breaks traditional public crypto, every captured secret protected by those protocols and mechanisms will be readable.

Even more important, anyone capturing and storing those (currently protected) secrets will be able to go back after the quantum crypto break and reveal them. How many secrets do you have or does your organization have that you want revealed to anyone within a few years? That's the new Y2K problem we are dealing with today.

There are many workable solutions you can implement today, although some are beyond the average company's means or, if implemented prematurely, can cause significant performance and operational disruption. Preparing for the coming quantum break requires education, critical choices, and planning. Individuals and organizations who clearly understand what is ahead can take the right steps now to be as prepared as possible. They can stop the unwarranted eavesdropping today and start to move their managed assets to a more quantum-resistant environment. This book has that knowledge and gives you the plan to help minimize your organization's risk from the coming quantum crypto break. If enough organizations prepare now, we can make the quantum break as inconsequential as the Y2K problem.

## Who This Book Is For

This book is primarily aimed at anyone who is in charge of managing their organization's computer security and, in particular, computer cryptography. These are the people who will likely be in charge and leading the way for their post-quantum migration project. It is also for managers and other leaders who understand the importance of good cryptography and its impact on their organization. Last, anyone with a passing interest in quantum mechanics, quantum computers, and quantum cryptography will find many new facts to make this book a worthwhile read.

## What Is Covered in This Book?

*Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto* contains nine chapters separated into two parts.

Part I, "Quantum Computing Primer," is a basic primer on quantum mechanics, computing, and how it can break today's cryptographic protection.

**Chapter 1, "Introduction to Quantum Mechanics"**

If you didn't understand quantum mechanics the first time you read about it, don't worry—quantum mechanics has vexed the most brilliant minds our planet has ever had for over a century. We mere mortals can be forgiven for not immediately grasping the central concepts. Chapter 1 explains the properties most important to our understanding of how it impacts our digital world. If I do my job right, you'll understand it better than 99 percent of everyone else in the computer world.

**Chapter 2, "Introduction to Quantum Computers"**

Quantum computers use quantum properties to provide capabilities, logic, and arithmetic outcomes that are simply not possible with traditional binary computers. Chapter 2 covers the different types of quantum computers, the various quantum properties they support, and where they are likely headed in the next decade as we become surrounded by them.

**Chapter 3, "How Can Quantum Computing Break Today's Cryptography?"**

The most common question asked when a person is told that quantum computers will likely break traditional public key cryptography is how. Chapter 3 tells why traditional binary computers can't easily break most public key crypto and how quantum computers likely will. It covers what quantum computers are likely to break and what is resistant to quantum computing power.

**Chapter 4, "When Will the Quantum Crypto Break Happen?"**

After explaining how quantum computers will likely break traditional public key crypto, the second most often asked question is when it will happen. Although no one (publicly) knows, it is likely to be sooner than later. Chapter 4 discusses the different possible timings and their possibilities.

**Chapter 5, "What Will a Post-Quantum World Look Like?"**

Like the invention of the Internet, there will be a world before and a world after quantum supremacy. Quantum will solve problems that have plagued us for centuries and will give us new problems that will vex us in the future. Chapter 5 will describe that post-quantum world and how it will impact you.

Part II, "Preparing for the Quantum Break," will help you and your organization most efficiently prepare for the coming quantum supremacy.

**Chapter 6, "Quantum-Resistant Cryptography"**

Chapter 6 covers over two dozen quantum-resistant ciphers and schemes, which the National Institute of Standards and Technology (NIST) is considering in the second round of its post-quantum

gets mentally fatigued. I'm not alone. It's being gracious to simply say that at first glance quantum mechanics is counterintuitive and seemingly unnatural. It often beggars belief. It goes against many things we've been previously taught about how our world and the universe works. One plus one does not always equal two. It goes against much of what we can readily see, touch, and feel, even though all of reality is possible due to it.

Even though the top minds of our civilization have repeatedly proven the existence of quantum mechanics beyond a shadow of a doubt, what it entails sounds so strange to the average person that it often remains unbelievable and magical. Understanding the implications of quantum mechanics for the first time means questioning what reality even means.

A not uncommon first-time response from laypeople first exposed to quantum theory is to suppose that all believers must be under some sort of science fiction, mass delusion because what they are saying cannot possibly be true. Or as a friend once said to me after I did an obviously poor job of explaining it to her, "You can believe whatever you want to believe, but that's a bunch of bull!" except she didn't say the word *bull*.

Even Albert Einstein, who helped discover and participate in some of its most important underlying principles, didn't completely believe many of its other fundamental tenets. He spent decades trying to understand it and he understood it better than most. It was his strong understanding of its implications which caused him problems. He even created experiments to prove or disprove it. He just couldn't logically believe or explain its many strange properties and "spooky at a distance" outcomes. After decades of waiting for experiments to catch up with his propositions, he just moved on to other subjects of study. Apparently, his head tired of thinking about it. So lesser minds can be excused.

With that said, I wrote this quantum primer chapter in a way that I wish it had been explained to me when I first started studying it. It is my hope that this chapter can help shorten the learning curve.

## Quantum Is Counterintuitive

Even though quantum mechanics underlies all of reality, it doesn't readily appear in a way that laypeople can easily discern in their everyday life. As examples, a single-colored dog can't both be white and black at the same time, a white dog stuck in a room doesn't suddenly become a black dog when it exits, and a dog can't split into two dogs in front of your very eyes and then merge together again. But at the atomic and subatomic levels, the peculiarities of quantum mechanics are equivalently strange.

What are the quantum properties I keep saying are so strange? Here are some examples:

- A single quantum particle can be in two places and be two distinctly different things at once.
- A single quantum particle can split in two and then later appear to run into or interfere with itself and recombine or cancel itself out.
- In a truly empty space with absolutely nothing (that scientists are aware of), quantum particles can just appear "out of thin air" and then vanish.

- A quantum particle will seem to behave one way when not being measured and another when being measured, as if nature absolutely cares about the action of measurement. It will seemingly even change its path or behavior back in time if you decide to measure it after it went through its original path.
- Two quantum particles can be "entangled" in such a way that when you change one, the other also instantly changes in the same way, every time, no matter how far apart they are, even across the universe.
- A quantum state is always all possible states (called a *superposition of states*), but the single, eventual resulting state can't be predicted with certainty.
- Every possible answer will be the answer at some point, although those answers may each be in their own separate universe. There may be a different universe for each possible combination of answer choices (called *multiverses*) at the atomic level.
- *Star Trek*–like teleportation is possible.

Here's the example I love to share with people to explain exactly how strange quantum mechanics can be. When we look up into the night sky and see stars, the light from those stars has traveled millions of miles and taken many years to reach your eye. The closest stars to Earth (besides our own Sun) are 4.2 light-years away. That means that it took at least 4.2 years or longer for the light from any star that you are looking at in the moment to reach your eye. That star isn't where you think you "see it," but where the star was when the light left it many years ago. This is a great astronomic fact to share on a romantic night or with kids and friends.

Quantum mechanics says that the path that any individual particle of light (known as a *photon*) travels from the star is changed simply because you decided to look up and see it at that particular moment. The path it started was adjusted, before you looked at it, because you looked at it. And if you decided to hesitate a millisecond before you looked up or not look up at all, the photon from that star would have taken a different overall path. If your friend looked up before you and saw that same photon instead, the path the photon took from the star would be different than what it took if you looked at it. And the path appears to change back in time based upon what happened now. Seems impossible, but events very similar to this story have been witnessed and repeated over and over. We don't know what is going on or how, but we know it is occurring. We don't even know enough to know if we are describing the event correctly, only that what our meager minds appear to be seeing can be described as a historic change based on a current event. Welcome to the world of quantum mechanics!

## Quantum Mechanics Is Real

The "strange" properties of quantum particles can be hard to believe. But except for the multi-universe proclamations, not only have these quantum properties and outcomes been tested and proved, but they are among the most tested and accepted scientific theories in the world. They are continuously

being tested and challenged. All experiments that have been conducted to disprove the basic, accepted theories of quantum mechanics have failed. Many of the failures, including those by Einstein, only succeeded in proving quantum theory even more. Most of the Nobel Prizes in physics from the last 75 years have been awarded to scientists who improved our understanding of quantum mechanics. There has been a renewed focus on quantum mechanics the last few decades and our understanding is improving each year.

Although the facts listed in the previous section may appear unbelievable on first reading, the genuineness of quantum physics appears to us throughout our larger reality, including how the Sun gives life to our planet, the red hot glow of any superheated material, digital cameras, fiber-optic cables, lasers, computer chips, and even the majority of the Internet (storage and transmission media). The very likely reality is that every bit of our reality is based on quantum mechanics.

Quantum mechanics is giving us very powerful computers that were previously unthinkable. Quantum computers and devices are going to change our world in many incredible ways that we can and can't fathom now, just like the Internet, USB memory storage keys, and iPods did for the current generation. Critical quantum inventions will significantly change our lives for the better, and the most important ones are coming soon.

Interestingly, although much of quantum theory has been confirmed by repeated observations, experiments, and math, scientists still don't know why many quantum properties are the way they are or why particular results occur. Theoretical physicists often take guesses about why a quantum-something is the way it is. You'll hear these guesses talked about as *interpretations* or *views*, such as the *Copenhagen interpretation* or the *Many Worlds view* (covered in the "Observer Effect" section later in this chapter). There are well over a dozen interpretations, each trying to explain some part of quantum mechanics, without really knowing if their interpretation is the accurate one.

What's important to understand is that regardless of the guess of why or how some quantum action or result occurs, the action or result does occur, always occurs in an expected way, and is experimentally and mathematically proven regardless of the interpretation. There has never been a serious quantum prediction not backed up by well-formed experimentation. We may not always know why quantum behavior is, well, quantum-acting, but we know it is real. It may seem like magic, but it is real, even if we can't explain it or "see it" in a conventional sense.

This bothers some nonscientists. Asking someone to believe in something they can't see or feel and that is supercounterintuitive to everything they've previously been taught is asking a lot. It's not like how they previously learned to appreciate science. For example, they may not understand the physics and math behind gravity, but they can "see it" and its outcome every time they throw a ball, trip and fall, see a proverbial apple fall from a tree, or watch the Moon circle Earth. They may not understand the math, but they understand how and why gravity works . . . well, most of us, that is. Many people ask, how can we believe anything science says really exists without knowing how or why it occurred? How can we believe in something we can't readily see with our own eyes, especially something so incredible and counterintuitive sounding?

What skeptics usually don't know is that much, if not most, of the advancement in science for the last century—especially in physics and especially, especially in quantum physics—has almost always first been proven by experiments and/or math without understanding why or how. Many times, scientists have only the vaguest of theories to support what little they can tangentially observe and prove with math. This is where the term *theoretical physicist* comes from. They are often starting from the barest of real evidence and haphazard an intelligent supporting theory to explain what they are observing. If they (or someone else) can provide a math equation that consistently describes what they are observing, then most scientists will rely on the math as conclusive proof of the behavior. It doesn't take a picture of something to be believed by a physicist.

The math is even more important than a picture or direct whole observation to a physicist. Someone once said, "The only absolute truth in the world is math." What they meant is that anything else besides a well-supported math equation is subject to personal biases and interpretations. Either the math works consistently or it doesn't. Either it supports something or it doesn't. It isn't subject to the opinion of the observer. If a scientist sees some previously unexplained phenomenon and can consistently support its interactions with a math formula and if every experiment and outcome is accurately described by the math, then the scientific fact is considered proven. The math is the proof. Direct, conclusive, confirmative observation isn't necessarily needed.

The conclusive observable event that most nonscientists think of as proof often comes many decades, or even centuries, later. Usually by then the involved scientists and their successors had long believed and treated the earlier theory supported by mathematical proof as a trusted fact. In their mind, the final uncontestable, physical proof is considered an almost unneeded formality.

Many past scientific postulations, both very small and very large, including the discovery of atoms, electrons, and black holes, were first discovered by scientists creating theories and math around previously unexplained observed phenomena. In the previous examples of the black hole and newly discovered solar system planets, observers had noticed subtle deviations in orbiting bodies and light that they knew could be explained only by previously unknown third-party effects. Black holes were theorized beginning in 1784 (by John Mitchell), and mathematically supported by Einstein's theory of general relativity in 1915. Further related observations over the next half century supported the math and existence of black holes, even if we couldn't "see" them. From the 1970s on, scientists considered the reality of black holes as a given. The first picture and what many nonscientists would think of as the first "real proof" of black holes didn't occur until April 2019 (`https://phys.org/news/2019-04-scientists-unveil-picture-black-hole.html`).

The history of quantum mechanics follows a similar path. It involves hundreds of brilliant physicists observing behaviors on very small objects that they could not otherwise explain using traditional (i.e., classical) physics. They then began exploring the new, strange phenomena even more, figuring out math equations that appeared to support what they were seeing. They made guesses as to why and how something was happening and then created experiments to prove or disprove their guess. Over time, additional experiments and observation created the known facts of quantum

mechanics. Some brilliant minds, like Einstein's, were proven wrong on certain facts, and previously obscure physicists had their careers made (and won Nobel Prizes) proving others. All in all, the contributions of hundreds of individual scientists and their skepticism has created the field of quantum mechanics as we know it today, strange and unexplainable as it may be at times.

## The Basic Properties of Quantum Mechanics

In this section, I will cover popular properties of quantum mechanics, such as the photoelectric effect, wave-particle duality, probabilities, the uncertainty principle, spin states, tunneling, superposition, the observer effect, and quantum entanglement.

**NOTE** So, what is the *quantum* in quantum physics? When physicists use the term *quantum* or *quanta* (from the Latin root *quantus*, which means the amount or how much), they are stating that whatever they are describing is the smallest possible unit of something (e.g., light or energy) and cannot be divided into smaller units. And any mathematical calculation involving a quanta cannot further subdivide the quanta into anything less than a whole number.

*Quantum mechanics* or *quantum physics* consists of the properties of and actions of quantum particles and interactions. It is also what the field of study involving quantum properties and particles is called. Everyone pretty much uses these words interchangeably.

Although our entire reality is made up of quantum particles and actions, quantum mechanics happens at the very microscopic level on very, very small elemental objects, such as photons, quarks, electrons, and atoms. If an elemental object displays quantum properties, it's known as a *quantum particle*. The smallest known particles usually display quantum properties. Quantum properties may occur on larger objects, on what is known as the *macroscopic level*, but science has not yet advanced to understand if it does or doesn't consistently, and if it does, how it does it. Understanding how the actions of very small objects transition and impact larger things is the ultimate goal of the much-sought-after, so-called unifying *Theory of Everything*.

**NOTE** The macroscopic level includes any object larger than the microscopic level of atomic and subatomic particles but is often interpreted as beginning with objects that can be detected by the naked human eye. Most scientists agree that the human eye can detect an object that is the width of a human hair (or 0.4mm), or about 100,000 atoms of an element.

### Photons and Quantum Mechanics

You will often read about photons (originally called *energy quanta* by Einstein) being used in quantum mechanics experiments. A *photon* is the smallest possible divisible unit of light and is

number of complete up-and-down wave oscillations in a particular time period determines its *frequency*.

Particles and waves are guided by very different physical properties, or so scientists thought. Particles function more like rocks or baseballs. They don't easily "bend" around objects. They strike with momentum and force. Their collision trajectories and resulting glancing bounces can be predetermined and calculated ahead of time. You can more easily see each discrete unit making up the large mass of particles, like seeing the individual rocks that make up a rock pile. A particle hitting a wall impacts it like a bug hitting a windshield. Waves have the opposite properties.

In the mid-1800s it was "settled science," after much theory and experimentation, that light and the photons that make it up traveled as waves. But starting in the early 1900s, when photons and other electromagnetic particles were observed and used in a greater number of subatomic experiments, different scientists started to notice that photons and other particles behaved as both a wave and a particle (i.e., *wave-particle duality*). At the time, this was considered scientifically blasphemous. Einstein, in particular, persisted with this new view and won his only Nobel Prize in physics for demonstrating that light also acted as a particle. Einstein wrote of his discovery:

> *It seems as though we must use sometimes the one theory and sometimes the other, while at times we may use either. We are faced with a new kind of difficulty. We have two contradictory pictures of reality; separately neither of them fully explains the phenomena of light, but together they do.*

One of the best ways to think of wave-particle duality is to imagine you have a rubber ball, which when behaving like a particle bounces all around, hitting other objects and bouncing back and forth, depending on its trajectory and what it bounces into. Then imagine that it falls into a lake and disappears (below the surface). Its energy is immediately transformed into waves and the resulting ripples. Then imagine that the wave ripples hit a dock post sitting in the water, and at that instant, a rubber ball reappears on a dock and the waves disappear. That's wave-particle duality. Depending on the situation, sometimes a photon is acting like a wave and sometimes like a particle. Thanks to Dominic Walliman for that excellent allegory.

### *It's a Particle*

Scientists demonstrated wave-particle duality by using a simple experiment using a high-intensity (laser) light, a background, and an intervening blocking material with one or two cut slits in it. They shot photons, one a time, into the slit(s) of the blocking material and then checked to see where they landed on the background.

When one slit was used and the photon was fired, the photon went through the slit and landed somewhat directly on the background behind. When multiple photons were shot, one at a time, each landed fairly near each other, somewhat mimicking the shape of the slit. Picture a marksman firing a bullet from a rifle through the same slit. If the rifle was in the exact same position each time, you

could expect the bullet to land almost in the same place, with minor adjustments due to the rifleman's expertise, the gun's ability to accurately fire a bullet, the bullet's individual characteristics, and any other intervening factors. If the gun was shot from a bunch of different angles, the bullets could land in a more scattershot pattern. This is what happened when multiple photons were shot, one at a time. The photons were demonstrating characteristics of a particle.

### *Interfering Waves*

Something surprising happened when they added a second nearby slit in the intervening blocking material. When they fired a single photon, it still landed on the background behind the slits, with the footprint of a single particle (i.e., like a bullet hole), but no longer directly behind the slots. Instead, as they shot more and more photons (one at a time), they seemed to land in areas not directly behind the slits. There were areas of distinct preferences, with clusters of areas with lots of aggregated landings interweaved with areas where the photons did not land much at all. It created banding—alternating areas of light and dark vertical bands (as represented by Figure 1.2).

The scientists immediately realized that what they were seeing was a result of the photons, shot one at a time, traveling as a wave (and landing as a particle). The bands are caused because when the photon, traveling as a wave, hits both slits, it creates two resulting waves, one on the other side of each slit, with each part of the original single wave going through the slit it interacted with. On the other side, the two resulting waves interfered with each other, creating the bands. But when the photon landed, it landed with the footprint of a particle (as represented by this Wikipedia video: `https://upload.wikimedia.org/wikipedia/commons/e/e4/Wave-particle_duality.ogv`). It was a remarkable finding.

The banding is created by the waves interacting with each other. If one light wave is at top of its crest and it meets another light wave at the top of its crest at the same moment, it will create the largest possible combined, synchronized, light wave possible, which makes the brightest light. It also

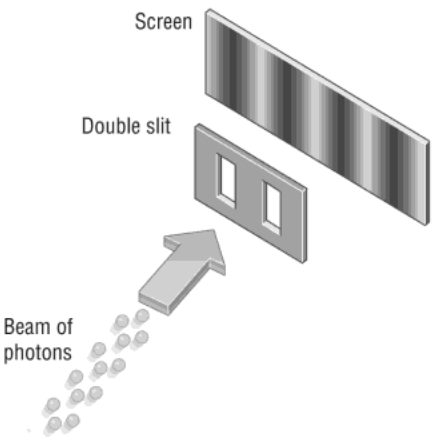


**Figure 1.2:** Wave-particle x duality experiment using light source and two slits
David Young and Shane Stadler, Figure 29-1 from *Cutnell & Johnson Physics, 11th Edition*; Wiley, 2018

means at their combined troughs, it creates the darkest extremes as well. Any other combination, other than two of the highest peaks (or lowest troughs) perfectly synchronizing up, will cause a smaller combined wave with less bright and dark outcomes.

Early on when this was being discovered, scientists simply couldn't believe the claims, math, or results. It took decades for light to be believed by most of science as acting as both a particle and a wave at the same time. Now we know without a doubt that all subatomic particles, which make up all matter, act with wave-particle duality. This finding strengthened scientists' resolve to more fully explore quantum mechanics and try to more fully "hook it" to the rest of our larger world. Today, anyone can perform a simple experiment to see that wave-particle duality of light.

### *Your Double-Slit Experiment*

It's kind of cool to be able to re-create one of the early wave-particle duality experiments to see quantumness working in front of you. You can duplicate this experiment using a laser pointer, tinfoil, and a solid background such as a wall. Use a strong, solid-color (not white light) laser pointer. The stronger, the better. White light is all the colors of light and it makes the experiment harder to see because the individual colors that make up white light have different frequencies. Place the tinfoil against a cutting board surface and cut two equal-length vertical slits about 1 inch long as close together as possible (we are talking millimeters apart). Then in a darkened room shine the laser light in between the two slits from a foot or more away with the tinfoil a foot or more away from the background surface. You may have to experiment with the distances away that the laser pointer, intervening material, and wall are from each other, but if done correctly you will see the banding. It probably won't be as stark as you see in serious physics experiments with better lab equipment, but you'll get the banding.

The particle nature of light is proven in the same experiment, although we can't readily see this without special detection equipment, because each individual fired photon will be detected as a single particle right at the slits or upon landing on the background. When photon detectors are used, they confirm that each photon goes through a slit and lands as a particle. But when all the fired photons are measured over many, many experiments, the effect is that of light and dark interleaved bands, again reaffirming the wave properties of light. This one experiment proves that light (like all quantum particles and molecules) has wave-particle duality.

**NOTE** If you want to see real-life examples of this experiment, just go to YouTube and search for **wave double slit experiment** or something like that. You will usually find dozens of videos showing the experiment. One great, animated example is `https://www.youtube.com/watch?v=fwXQjRBLwsQ`.

### *Detection Strangeness*

Now things get really strange. When scientists place photon detectors at one or both slits to see which slit the photon actually travels through, the photon acts as a particle and all wave-like behavior goes immediately away. Let me say that again. Before the detectors are put in front of or back of the two

slits, the photons act like waves. And after the detectors are placed and turned on, for reasons we cannot yet fully explain, the photons immediately begin acting like particles, as if there were only one slit. It's as if the particles, themselves, see the act of detection and change their behavior. Scientists have even done experiments where they don't turn on the detectors until after the photons have gone through a slit and when they turn on the detectors the photons appear to act as particles (when they should have gone through the slits as waves). It is as if the photon has retroactively adjusted its initial behavior in the past based upon the initiation of a future detection. We cannot say this (i.e., changing the past) is really happening or for that matter what time, the past, or reality really is. No one knows what is happening or how. Only that the behavior change happens anytime a detector is used, and we are having a hard time understanding what is going on. This known as part of the observer effect, which is covered in more detail below and is the explanation behind the star light path change story that started this chapter.

## Probability Principle

Understanding of how electrons orbit around a nucleus led to better understanding of how our world works, especially at the quantum level. For example, as schoolchildren, we probably all learned that each atomic element is made up of electrons, protons, and neutrons. Every *atom* (the smallest unit of ordinary matter) is made up of a *nucleus* (which is made up of positively charged *protons*) and (no charge) *neutrons*, surrounded by negatively charged electrons. The electrons "orbit" the nucleus because of electromagnetic attraction. In elementary school, most of us learned that electrons circle the nucleus in orbital bands known as *shells*.

In elementary school, likely for simplistic reasons, these electron orbital shells were shown as perfect circles or maybe ovals, often conjuring up perfect planetary-like orbits, but at the atomic level (see Figure 1.3).

But quantum physics has shown us that electrons don't orbit in perfect circles or even ovals. Those perfect circle electron shells are a figment of somebody's early imagination, and today are used solely to demonstrate electron shells in an uncomplicated pattern. But that's not the way nature really works. Instead, electrons orbit the nucleus in more complex patterns dictated by quantum mechanics and the involved energy (Figure 1.4 shows a two-dimensional representative example for electron orbits around a nucleus at a particular energy level). These areas of probable orbit are known as *atomic orbits* or *electron clouds*. The probable part is very important in quantum mechanics and will be explained in more detail in the next section.

Complicating matters a bit, no one can guess ahead of time where a particular electron may be orbiting at any one time, only the *probability* of it to be in certain (predicted) atomic orbital areas. No math equation exists that can say with any certainty that any electron will be exactly in spot A at any time. The best quantum mechanics can say is that an electron has a particular percentage of likelihood of being in spot A when you try to measure it. And if you take that measurement many times, that electron will be in spot A the number of times indicated by its probability percentage.

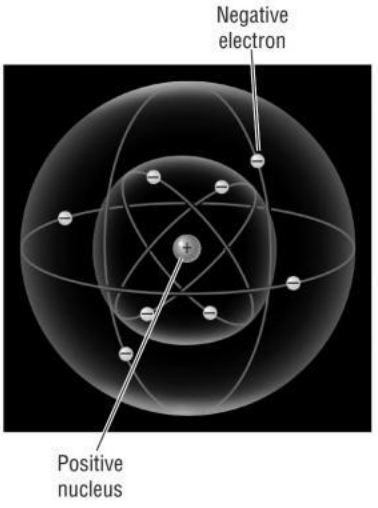


**Figure 1.3:** Atom nucleus surrounded by overly simplified electron shell orbits
David Young and Shane Stadler, Figure 30-1 from *Cutnell & Johnson Physics, 11th Edition*; Wiley, 2018

The probability principle applies to any property of a quantum particle, not just electrons. Not only can't a particular property state or position be guessed ahead of time, but the state or position when measured is absolutely random within the larger confines of the probability predictions during any single measurement. And this randomness of a specific answer or state isn't accidental; it's fundamental and inherent to quantum mechanics.

This is a key difference between quantum mechanics and traditional, classical physics in that the exact state or position of a quantum object or property cannot be precisely predicted ahead of time. In classical physics, A + B = C, and will always equal C. Not only that, but if I know A and C, I can

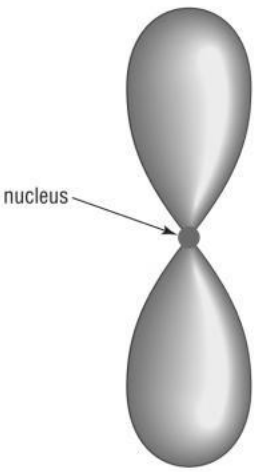


**Figure 1.4:** Two-dimensional atomic orbit for an electron orbiting a nucleus

or momentum about a quantum particle at the same time, and as you attempt to more precisely measure one quantity, the other side of the dependent pair becomes less accurate.

Let's use another macroscopic allegory, that of trying to measure the speed of a car. In the macroscopic, classical world, a car's speed is simply a measurement of its distance traveled in a particular time period. If the car traveled 100 kilometers in exactly 1 hour, you would say it averaged 100km/hr. But in the quantum world, when looking at quantum properties of very small particles, both the time and distance variables are not fixed at all. They are changing across a range of probabilities, and any single measurement can result in a different answer out of those ranges. That makes measurement tougher out of the starting gate.

Although with our speeding car example, there is a very similar allegory. If at any time along the car's path you took a measurement, the car could be going faster and slower than 100km/hr. It's really highly unlikely that any complex self-powered object would be traveling at exactly the same speed at all moments. For a car you would have to factor in wind resistance, surface condition changes, temperature changes, and the hundreds of factors within the engine itself that determine how much power and torque it is generating at any one time to get the speed at which it was traveling at any one second. Although, if the car was ultimately measured at traveling 100km/hr over the whole course, it probably traveled exactly 100km/hr more of the time than any other speed.

This is representative of the probability principle. At any point along the course if someone had held a radar gun, the car could have been going any number of speeds, but odds are that a car finally measured as having traveled 100 kilometers in exactly 1 hour was going 100km/hr at more points along the course than any other (although there is always a chance it was going exactly 98km/hour for half the course and exactly 101km/hr for the other half, but less likely).

The uncertainty principle says that as you go to more accurately measure the time involved in the speed, the less accurately the distance can be measured at the same time, and there is no way to fix it. In the quantum world there is no such thing as highly accurate speed. As a concept, it does not exist. It's a law of nature. To continue our speeding car allegory, suppose our judges wanted to be superaccurate, and to do so they decided to get the world's best flash photography to take a picture of the car just as it crossed the finish line of the measuring contest. In order to get the exact instant the car crossed the line, the shutter of the camera would have to open and close extremely fast. At that exact microsecond, the car would be "frozen" in time. In the picture of the exact instant it crossed the line, the car would not appear to be moving at all. The finish line camera can capture the exact moment the car crosses the line, but in that exact instant the car would not be moving (or moving very much). The camera, trying to get the exact moment when the timing was over, would have to remove the speed out of the measurement. And if you had another camera that was measuring the true speed of the car, it would not be able to accurately capture the exact moment when the car crossed the line.

To complicate matters, what is the line? Any line at a macro level looks like a straight line. But magnify any painted or drawn line and its individual, tiny undulations come out under magnification.

To be the most accurate you would have to snap a picture or click the stopwatch exactly as the car crossed the first atom of the painted line. And your eye and the camera's eye would have to click exactly when the car crossed that first atom, knowing that we can't even see when the car actually crossed the first atom of the line until a photo, at that instant, comes back to our retina or camera lens. And those processes depend on photons and the speed of light.

By the time the first recording photon made it back, the car would actually be past the actual first atom for those measurements to be made. And we know the first atom is made up subatomic particles—electrons, protons, and neutrons. To be the most accurate, you would have to stop the stopwatch or trigger the camera when the car met the first electron in the outer electron shell orbit, and according to quantum theory we don't know where that first electron will be and at any single measure it can be anywhere, and may not be where its highest-probability location would be. Ultimately you can't make a truly accurate speed calculation because the very attributes you need to get the most accuracy (i.e., the electron) is moving and the whole particle is moving as a wave along a wave function of outputs. As you try to get more and more accurate, you realize that you simply can't get a truly accurate measure of anything, much less conjugate pairs whose very definition depends on the other. Everything is moving at all times (even a rock is made up of moving electrons), everything is both a particle and a wave, everything behaves differently when measured versus not measured, every answer during a particular measurement is random, and it may not even be the "right" (highest-probability) answer. And with conjugate pairs, the accurate measurement of one value depends on the other, which by definition must get less precisely measured. In our example, the concept of kilometers/hour (i.e., position and momentum) doesn't really exist down at the quantum level. It just doesn't. That's the uncertainty principle.

You have to understand that the uncertainty in the measurement pairs isn't due to a lack of measuring equipment capabilities. Many people when first hearing about the uncertainty principle think it has to do with problems with the measuring apparatus not being accurate enough. They think it has to do with a flaw in the measuring devices. It doesn't. We could have the most accurate measuring equipment that could very accurately (to our human senses) measure time and distance, and it wouldn't matter. It's not the measurement that is imprecise; it's due to the (quantum) laws of nature that govern how accurately we can measure any quantum state that relies on two dependent conjugate variables. As we measure one side of the dependent pair more accurately, it simply isn't possible to measure the other side of the equation as precisely. In fact, it's a guaranteed inverse relationship.

**NOTE** The probability and uncertainty principles should not be misconstrued to mean that quantum mechanics and quantum properties cannot be mathematically accurate. The exact opposite is true. The math and outcomes from quantum mechanics are incredibly accurate, and with a proven confidence level unsurpassed by most other sciences. The uncertainty principle should also not be confused with the observer effect, which is discussed below.

## Spin States and Charges

There are 12 *fundamental* (also known as an *elemental*) quantum particles that make up all matter in the universe. Fundamental particles, as best we know, can't be broken down to into smaller, whole particles. Be prepared if you haven't been introduced to them before. Some of these particles have some strange-sounding names. The fundamental quantum particles are electron, *muon*, *tau*, *electron neutrino*, *muon neutrino*, *tau neutrino* (all part of the *lepton* family), and *up*, *down*, *top*, *bottom*, *charm*, *strange* (the last six are part of the *quark* family).

These fundamental quantum particles make up all other subatomic particles. For example, every proton is made up of two up quarks and one down quark. A neutron is made up of two down quarks and one up quark. The electron, as an elementary particle, is not made up of anything. It's an electron, with no further subatomic particles to add up or break it down into. But electrons, protons, and neutrons make up atoms, atoms make up elements and molecules, and so on.

**NOTE** We can never be sure that we have discovered every elementary particle, or even that the existing leptons and quarks are elemental, although current science is very adamant that they are the lowest-common-denominator particles. But in history we previously said that about cells, atoms, and protons. So, who knows what we will discover as we try to finish the grand jigsaw puzzle that is our reality?

Each elemental quantum particle has a mass, charge, and a spin. Everyone understands what mass is, so let's quickly discuss the other two. A *charge* is the amount of current as compared to an electron. For example, an up quark has two-thirds of an electron charge and a down quark has a negative one-third of an electron charge. Because a proton has two up quarks and one down quark, this means the proton has a 3/3 (2/3 + 2/3 – 1/3) charge of an electron, or exactly equal to one electron. In most stable atoms, the number of protons in the nucleus equals the number of orbiting electrons for this reason.

Elemental particles also have a *spin*, which relates inversely to the number of revolutions a particle must make to return to its original orientation. All elemental particles have a spin of one-half, which means they must rotate twice to return to their starting orientation. Why am I teaching you about quantum charges and spins? Because the answers that quantum computers give us are often a result of charges and spins. As covered in Chapter 2, "Introduction to Quantum Computers," different quantum properties and states are used to provide answers in different types of quantum computers.

## Quantum Tunneling

*Quantum tunneling* is an unexplained ability for quantum particles to pass through barriers, which classical physics said could not happen. The common macroscopic similar example is a ball sitting at the bottom of a hill or wall. Suppose a person is trying to throw the ball over the wall, but they do not physically have enough strength to get the ball over the wall. They try again and again with

no success. Classical physics, looking at the person's arm and body strength, says the person will never be able to do it. But then, for reasons that cannot be explained, the thrown ball sometimes ends up on the other side of the wall. Some theories say that the ball unexplainably just rises over the wall. Others say that the wall lowers for that one throw or that the ball is allowed through the wall without leaving an entry or exit point.

We don't yet know how it works or exactly when a subatomic particle will have success using it versus all the previous unsuccessful tries, but it does exist and is the basis for all known life. Tunneling is how our Sun generates heat and light using *thermonuclear fusion*. Tunneling is how a radioactivity element decays. Tunneling is the basis for photosynthesis, which supports most plant life on Earth, which then supports human life. Quantum tunneling is also involved in some types of quantum computing.

## Superposition

*Superposition* is a quantum property that says a particle can exist in all possible states, until the state is finally observed and measured to give a single answer. For example, let's say that a particular math problem that you don't know the answer to can possibly be answer A or B. Superposition says that while the answer is in its quantum state before being observed or measured, it is both A and B at the same time. It's not A *or* B. It's both.

This is because, as discussed above, at any particular measurement of a quantum property, the measured property can be any possible answer. And the actual measured answer from any single measurement can randomly be any of those possible answers. In the classical world, everything is what it is. An A is an A. A B is a B. A single letter can't randomly be A sometimes and B sometimes. But in the quantum world that is exactly what happens.

Perhaps you've heard of Erwin Schrödinger's famous quantum cat conundrum. Schrödinger created a (thought experiment only) scenario where a cat was placed in a closed box with a capped bottle of deadly poison, a radioactive element, and a Geiger counter. The radioactive element could decay or not decay. Radioactive decay is a quantum event, and the moment when any particular atom of the element decides to decay is a random event. If the Geiger counter detects radiation (from radioactive decay), the Geiger counter would trigger the shattering of the bottle containing the poison, which would kill the cat.

Schrödinger created this thought experiment, which is an example of a quantum superposition process leading to an observable, macroscopic event, to demonstrate how weird superposition would be if expanded to the macroscopic level. Schrödinger was trying to show how absurd quantum mechanics, as described in his day, was. He didn't make the thought experiment to back up quantum mechanics. He did it to show how absurd it was, and to say that we didn't really understand what was going on. If he were alive today he would probably chuckle that his purposefully absurd thought experiment is actually the most commonly used enduring example of how quantum mechanics truly works, because that was not what he was going for.

Prior to opening the box and observing the cat, the superposition principle states that the radioactive element has both decayed and not decayed. The cat is both alive and dead. In the classical physics (or real) world, the cat at any particular point in time would be either alive *or* dead—one or the other at a particular point in time. What quantum physics has proven, at the quantum level, is that the cat (by extension of the radioactive decay) is both alive and dead at the same time, before being observed by opening the box—and not in some half-state where the cat is somewhat poisoned but not completely dead or fully healthy. No, it means it's both 100 percent healthy and 100 percent dead at the same time. What seems nonsensical at the macroscopic level is the absolute reality at the quantum level.

If you're going to understand quantum mechanics and quantum computers, you have to understand the concept of superposition. You have to break how you otherwise see and understand the world, because at the quantum level, the world does not act like you think it would. It took me a long time to understand the ramifications of Schrödinger's thought experiment. I figured the cat was alive or dead, and when we opened the box, it was one or the other and had been since some previous point in time. That's not what superposition says. Superposition, which has been proven over and over again, says the cat is both alive and dead, in both states, until finally observed and measured. Once the cat's "state" is measured, the cat is either permanently alive or dead, and from that point forward, this will be the measured result for that observation. This reckoning has flummoxed the greatest scientific minds who ever existed and still does. Yet experiment after experiment supports superposition as a reality at the quantum level.

Quantum mechanics and, by extension, quantum computers are instantaneously generating all possible answers all at once, and until the answer is observed and measured, the "correct" answer is all possible answers. Once we observe or measure the answer, only one answer becomes our permanent reality.

To complicate matters, as discussed earlier, no one can predict what the final observed answer will be. No one can say, "Surely, the cat is dead!" or "Surely, the cat is alive!" and always be correct—only that the cat is both alive and dead before being measured, and that the cat will be alive *or* dead when measured, but only within a particular probability of likely outcomes, and the specific outcome when measured is random among the possible choices. If someone's guess is right, it is only because they were lucky (or played the probabilities).

If this is confusing or hurting your head, we haven't even gotten to the weirdest parts yet. Hold on.

## Observer Effect

In the quantum world, merely observing a quantum system changes it, although quantum physicists don't know or agree why. Like all of the quantum properties discussed in this chapter, decades of experimentation have shown that this property is real and accurate. Scientists aren't wondering if is true, only why or how it is true. For example, in every double-slit experiment, when scientists place a photon detector to measure which of the two slits a photon goes through, the photon always behaves only as a particle (and the resulting wave bands do not occur). If they turn off the detector,

when you're trying to get at the truth of something in an experiment, less is usually more. Having to figure out something that is a result from the interactions of billions of particles just muddies the waters.

So in experiments where entanglement is desired, scientists will work hard to isolate the experimental environment to prevent any unwanted entanglement and create their own entanglements on much smaller scales. Experimental entanglement can be done a bunch of different ways, although one of the most common methods is to take a single photon of higher energy and split it into two photons of lower energy. There are several other common entanglement methods, but they are too technically complex to describe than is fitting for this book.

So far experimental, the entanglement must involve two very nearby quantum particles. Scientists up to now have not been able to entangle two particles that are far away from each other, although the distance is lengthening all the time. But once entangled, these two particles can be moved very, very far away from each other and still keep their entanglement bonding. Although as distance increases, the chances of entangled particles interacting with other entangled particles increases, making it hard to impossible for the scientists to measure what they wanted from the original, intended entanglement.

Irish physicist John S. Bell strengthened the theory of quantum entanglement in a series of uncontestable experiments whose description he published in 1987 in his seminal white paper titled "Speakable and unspeakable in quantum mechanics" (`https://web.archive.org/web/20150412044550/http://philosophyfaculty.ucsd.edu/faculty/wuthrich/GSSPP09/Files/BellJohnS1981Speakable_BertlmannsSocks.pdf`). Bell ruled out "hidden local variables," which Einstein had postulated were another possible, more likely, explanation for entanglement. Bell proved there were no hidden local variables, which significantly strengthened entanglement theory and all of quantum physics.

Since then, his experiments have been repeated with the same success each time and on different quantum particles. Spooky entanglement has been demonstrated in photons, electrons, neutrinos, and even larger molecules such as "buckyballs." Quantum entanglement has even been demonstrated in macroscopic objects, like diamonds (`https://news.yahoo.com/two-diamonds-linked-strange-quantum-entanglement-190805281.html`). Not that quantum physicists need pictures to believe or prove anything, but in July 2019, scientists were able to capture the first picture of entangled particles (`https://phys.org/news/2019-07-scientists-unveil-first-ever-image-quantum.html`), which thrilled scientific and nonscientific minds alike.

## Decoherence

The last quantum property we will discuss in this chapter is *decoherence*. It is extremely important in quantum physics and computing. It is something we both want and want to avoid (until the right time). When a quantum particle or system is in an easy-to-see set of quantum states we say that it is cohered or in *coherence*. We can easily see the results of its quantumness, which is operating along a

wave function with all the probable answers. Without extreme environment isolation, any quantum particle or system will begin to interact and entangle with other quantum particles. In fact, billions and billions of interactions within microseconds. This happens in even what we might think is a empty void. For example, when scientists create an artificial vacuum inside a box with no light or other intentional quantum particles in it, the apparatus used to create the vacuum will leach into the void. It's unavoidable. Again, without extreme conditions, this happens very often and very fast. With the best of conditions it still happens. It cannot be stopped from happening.

Each unwanted interaction causes entanglement, and now scientists trying to follow one or a few particles or properties must begin dealing with results that are from a more complex, multiparticle amalgam that they usually did not desire. Their original particle(s) are there but can easily be lost among a sea of other entangled particles, and in any case, they cannot easily figure out the impact or result of the original particle(s) they were watching and wanting to measure.

Imagine you wanted to follow a single drop of water and it dropped into an ocean. Or you wanted to follow a single photon out on a beach on a sunny day. The drop of water would still be in the ocean, but now immediately dispersed among trillions and trillions of other drops. You could possibly still follow the original drop, but it would be hard. You could possibly keep track of your original photon on the beach, but not only is it lost among a trillion other photons, but it is interacting with the other photons and other particles, both micro and macro (e.g., dust, air, wind). For all practical purposes, after just a few interactions, it would be difficult for any single particle to be tracked and to figure out what all the other entanglements caused or didn't cause.

Because of this, for quantum experiments and inside quantum computers and other devices, the internal structures must be highly isolated from the outside world. Quantum scientists want to prevent as much unwanted entanglement from happening as is humanly possible. Barren surfaces using a single stable element, cold temperatures, and shielding against the outside world are all commonly used. But when the scientists or machinery lose their ability to track the original particle(s) or their property/properties and figure out the originally desired outcome (which will always eventually happen no matter what), the quantum particle or system is considered decohered or in decoherence. It's important to note that the quantumness of the particle or system didn't change into something else. It didn't become nonquantum/classical. It just became too difficult for our meager minds and equipment to track and understand in a meaningful way.

Sometimes we need decoherence. In quantum information science, when we want to get a quantum answer we can write down and call a result, we have to measure it, and measuring it entangles and changes it. Whatever the measurement device is, it's also made up of quantum particles and properties and must interact with the particle or property being measured. Even if the measurement only involves light, light is made up of photons, and in order for the photon to capture the result and report it back, it must "hit" the particle and bounce back. Now that photon is entangled with the thing it measured. So, measurement alone will decohere a quantum system. It didn't suddenly change the quantum state into something not quantum, it just starts to immediately add measurement complexity.

But to record a quantum result of a particular experiment or computation, we must measure it. So, we want to measure it when and where the decoherence is controlled and minimized until our measurement apparatus is the thing decohering it. We need to measure and decohere it so we can get a final measurement and answer. We don't want the answer to be A sometimes and B sometimes. We need a permanent outcome value to record. Can you imagine if every time we needed an answer, we could just say "it's a range of all possible answers across a probability spectrum" and leave it at that? We couldn't just say the car is going 100km/hr. We'd have to say, well, it's going a speed somewhere between 0 and 200 km/hr (or whatever the maximum possible speed is) and here are the probabilities. It would be a nuts way of describing the world especially when everyone understands that a car recorded as going 100 km/hr was likely not going 100 km/hr at all times. In order for us to record answers we pretty much just want the most probable "right" answer, and not some spectrum of answers along a mathematical wave function. So, we want to intentionally decohere the system at only the time of needed measurement. We want to avoid decohering the system before the measurement, and once we have the measurement we need, it can decohere further all it likes. Although scientists would also like, and are trying, to get multiple measurements done without decohering a system. One of the biggest struggles, if not *the* biggest challenge, in quantum information sciences is to protect a system from premature decoherence until final measurement is needed.

There are many other central quantum mechanics properties, principles, and theories, such as contextuality, that we could cover, but what we have already discussed is a great base for discussing how quantum computers work in Chapter 2.

## Quantum Examples in Our World Today

Although quantum mechanics mostly happens at a subatomic level, none of our reality could be possible except for its very real existence and impact at our real-life level. Quantum mechanics makes the Sun shine, is the reason all matter holds together, and is the basis for most of the things we see at the macroscopic level. When you look at a stove burner glowing red hot, that's only possible because of quantum effects. Quantum mechanics is responsible for our computer microprocessors, transistors, resistors, and all integrated circuits. Disk storage and network communications are only possible because of quantum mechanics. Your Wi-Fi connection works only because of quantum properties. Here are other macroscopic realities that are only possible directly due to quantum mechanics:

- Fiber-optic cables
- Lasers
- Superconductivity
- Superfluid liquids
- Atomic clocks
- Magnetic resonance imaging (MRI)
- And don't forget the whole reason for this book, quantum computers and quantum cryptography