Preface

Almost Too Much Awesome

I love quantum computing so much, I don't know where to start. I'm tongue-tied. I'm delirious. I can't contain my joy. I'm doing backflips off dumpsters. I'm riding shopping carts down stairs. I'm swinging by vines over rivers of lava. As in a song lyric I liked in high school, "I'm so bloated up happy I could throw things around me." ("Heavenly Pop Hit" by The Chills.)

In high school, I had a book called *The Secret Guide to Computers*. It taught BASIC programming. The book opened a misty passageway to a world of almost mystical union with silicon circuitry. It was an initiation to a fellowship of advanced nerds. Because if you're going to be a nerd, you might as well be an advanced one. Well, I've got news for you, advanced nerds. It's time to take a quantum leap.

Quantum information science, the broader discipline that contains quantum computing, stands at a grand conjunction of computer science, digital electronics, engineering, quantum mechanics, linear algebra, number theory, and even philosophy. It's a bustling crossroads of all my favorite nerdy pursuits. It's almost too much awesome.

Yes, even philosophy is relevant to quantum information science, as we will see in the chapter about the 2022 Nobel Prize in Physics. As we continue to expand the frontiers of knowledge, the rigorous mysteries of quantum physics remain stubbornly unsolved. I wonder if this is a salutary check on human hubris, a reminder of our place in a world we never made. Physics achieves the goal of medieval alchemy and astrology, to illuminate the invisible forces that govern the destinies of all things. But something always scurries away from the light, and our thirst for complete understanding is forever unquenched.

Philosophical questions aside, quantum technology is advancing all the time, and the potential uses for quantum computers are exciting and fun to explore. Quantum computing is a new and growing field that students hunger to learn about, and instructors who are new to the field are desperate for

books they can understand. (I speak from experience as an instructor who is new to the field.) I had to carefully study a dozen quantum computing books before I understood any of them. New instructors, as well as autodidactic hobbyists, need a large pool of resources. I hope I'm contributing to this pool.

I'm keeping the math as simple as I possibly can, and I'm avoiding matrices entirely, until the completely optional final two chapters. You do need to know some precalculus (algebra and occasional trigonometry). On the other hand, you don't need to know any quantum physics at all. I hope that our leap to the farthest Shor, over the howling abyss of quantum phase estimation, is not too daunting. Please don't feel bad if you have to skim some sections, or chew over them slowly like cud. It's also okay to skip some passages out of sheer boredom. Not every sentence can be a thrill, and the parts you skip are always there if you ever want to go back to them.

So without any further ado, onward to the awesome.

Chapter 1

Forging the Quantum Key

There are a lot of reasons to keep data secret, accessible only to intended viewers. Examples include credit card numbers intended only for a seller, medical information intended only for health care providers, military intelligence intended only for allies, proprietary industrial processes intended only for collaborators, and photos from a meeting of the Nude Headstand Enthusiasts Club intended only for fellow club members (you *said* the site was password protected, Steve).

One way to keep data secure is to seal it in a bank vault, or in a safe wrapped with padlocked chains buried in a cobra-infested island in a sea swarming with sharks. The trouble with this kind of security is that data often needs to be shared. So we need a convenient way to share data remotely with intended recipients, and only with intended recipients.

All electronic data, whether text, images, videos, or anything else, is stored as combinations of 0's and 1's. 0 and 1 represent two different voltages in electronic circuits. The two voltages could be 0 volts and 1 volt, but that's not the only choice. The two voltages could be 0 volts and 5 volts; we simply use 1 to represent 5 volts. The two voltages could be –4 volts and 3.5 volts; we arbitrarily pick one of these to call 0, and the other to call 1. The point is that we can analyze the 0's and 1's in data without paying any attention to the physical details of how they're stored.

In fact, 0's and 1's can represent more than just voltages. The 0's and 1's in bar codes and QR codes are black and white stripes or squares. The 0's and 1's in CDs and DVDs are different thicknesses of a layer of plastic. As long as there are two, and only two, distinct physical conditions, we have 0's and 1's, and we can do classical computation.

Our electronic devices know how to convert 0's and 1's to videos, images, sounds, text, and so on. The details of this conversion are not our focus. We wish only to securely transmit 0's and 1's from a sender to a recipient, over a perilous distance fraught with eavesdroppers. In fact, we assume that eavesdroppers will be greedily poring over our data transmissions, combing through our 0's and 1's for valuable secrets.

So we have little choice, then, but to encrypt our data. We transmute our sequence of 0's and 1's into meaningless gibberish, a cipher, which only the intended recipient can decipher. There are many ways of achieving this. Near the end of our journey, we will meet the RSA cryptosystem, which is vulnerable to the quantum attack of Shor's algorithm. For now, we will consider a simpler cryptosystem: the private, or secret, key.

It's convenient to give names to the sender and receiver of data. The traditional names are Alice and Bob. But I think Alice and Bob deserve a vacation. So as Alice and Bob settle into their cozy rooms overlooking waves booming against a rocky shore silvered by moonlight, let's meet our new heroes, Odysseus and Penelope. Odysseus is rightly regarded as the most cunning of warriors. Less well known is that his wife Penelope is the most cunning of quantum engineers.

A 0 or 1 is called a *bit*. For each bit of the message that Penelope wants to send to Odysseus, she needs a secret *key* bit. The message bit is combined with the key bit to form an encrypted bit, according to these rules:

0 combined with 0 is 0.
0 combined with 1 is 1.
1 combined with 1 is 0.

In other words, if the message bit and the key bit are the same, the encrypted bit is 0. If the message bit and the key bit are different, the key bit is 1. There's a mathematical symbol, $\oplus$, called "exclusive OR," that represents these rules:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1 \text{ (also, } 1 \oplus 0 = 1)$$
$$1 \oplus 1 = 0$$

Let's represent the message bit by M, the key bit by K, and the encrypted bit by E. So $E = M \oplus K$. Penelope sends encrypted bit E to Odysseus. How can Odysseus recover the message bit M? Odysseus knows the key bit K; this is the secret information known only to Odysseus and Penelope. To recover the message bit M, all Odysseus has to do is combine the encrypted bit E with the key bit K according to the same rule: $E \oplus K$. Since $E = M \oplus K$, Odysseus is really computing $E \oplus K = M \oplus K \oplus K$. Now, K is either 0 or 1. Since $0 \oplus 0 = 0$ and $1 \oplus 1 = 0$,

$$K \oplus K = 0, \tag{1.1}$$

whether K is 0 or 1. So Odysseus computes $M \oplus K \oplus K = M \oplus 0$. Because M is either 0 or 1, and because $0 \oplus 0 = 0$ and $1 \oplus 0 = 1$,

$$M \oplus 0 = M. \tag{1.2}$$

So Odysseus recovers the message bit, but only because he knows the key bit. A potential eavesdropper like Hector doesn't know the key bit and cannot compute the message bit even if he glimpses the encrypted bit.

Let's take an example. Suppose Penelope wants to send Odysseus the message 0010. Before Odysseus began his voyage, with masts creaking and 10-foot waves slapping the hull, he and Penelope agreed to use the secret key 1011. Penelope combines each bit of the message with the corresponding bit of the secret key to obtain the cipher, as shown in Table 1.1. The first encrypted bit is $0 \oplus 1 = 1$, the second is $0 \oplus 0 = 0$, the third is $1 \oplus 1 = 0$, and the fourth is $0 \oplus 1 = 1$. So the cipher is 1001, which Penelope sends to Odysseus. Hector spies on this message but can't make heads or tails of it because he doesn't know the secret key.

Now, Odysseus receives the cipher 1001, and he combines each of its bits with the corresponding bit of the secret key, 1011, as shown in Table 1.2. The first bit becomes $1 \oplus 1 = 0$, the second bit becomes $0 \oplus 0 = 0$, the third bit becomes $0 \oplus 1 = 1$, and the fourth bit becomes $1 \oplus 1 = 0$. Thus, Odysseus has restored the (lurid and poignant) message, 0010.

So far, there's nothing quantum about this. Suppose, however, that Penelope and Odysseus decide they need to periodically change their secret key to keep Hector from guessing it. How can Penelope and Odysseus establish a secret key remotely? This is where Penelope's quantum genius comes in.

Three thousand years ahead of her time, Penelope has perfected a single-atom version of an experiment that normally requires a beam of atoms. (The real experiment, with a beam of atoms, is called the Stern-Gerlach experiment.) Penelope launches silver atoms through a magnetic field and observes that each atom is deflected toward either the magnet's north pole or south pole; no atom passes straight through. If the magnetic field is vertical, each atom is deflected either UP or DOWN. If the magnetic field is horizontal, each atom is deflected either RIGHT or LEFT.

Table 1.1

	Message Bit	Key Bit	Encrypted Bit
First Bit	0	1	$0 \oplus 1 = 1$
Second Bit	0	0	$0 \oplus 0 = 0$
Third Bit	1	1	$1 \oplus 1 = 0$
Fourth Bit	0	1	$0 \oplus 1 = 1$

Table 1.2

	Encrypted Bit	Key Bit	Message Bit
First Bit	1	1	$1 \oplus 1 = 0$
Second Bit	0	0	$0 \oplus 0 = 0$
Third Bit	0	1	$0 \oplus 1 = 1$
Fourth Bit	1	1	$1 \oplus 1 = 0$

Penelope observes that if an atom is deflected UP and then immediately enters another vertical magnetic field, it will again be deflected UP:

atom → [vertical magnetic field] → deflected UP
→ [vertical magnetic field] → deflected UP

We could send the atom through a hundred vertical magnetic fields in a row, and it would get deflected UP every time. The atom apparently has an enduring property that determines its behavior in vertical magnetic fields.

Similarly, an atom deflected DOWN is again deflected DOWN when it immediately enters another vertical magnetic field. If an atom is deflected RIGHT in a horizontal magnetic field, it is again deflected RIGHT in another horizontal magnetic field; the same rule applies to an atom deflected LEFT.

Penelope further observes that if an atom is deflected UP, and then enters a horizontal magnetic field, it is equally likely to be deflected RIGHT or LEFT. If the atom then enters a vertical magnetic field, it is no longer certain to go UP; it is equally likely to go DOWN:

atom → [vertical magnetic field] → deflected UP → [horizontal magnetic field]
→ deflected LEFT or RIGHT → [vertical magnetic field]
→ deflected UP or DOWN

The horizontal magnetic field apparently erased the atom's vertical-field property: The atom lost its reliable UP-ness and has become just as likely to deflect DOWN.

Similarly, an atom initially deflected DOWN is equally likely to be deflected RIGHT or LEFT in a horizontal magnetic field, after which it is equally likely to go UP and DOWN in a vertical magnetic field. An atom initially deflected either RIGHT or LEFT is equally likely to be deflected UP or DOWN in a vertical magnetic field, after which it is equally likely to go either direction in a horizontal field, regardless of its initial deflection.

This is 100% of the quantum physics we need to understand quantum key distribution. To summarize, a silver atom deflected in a magnetic field will be deflected the same way if it subsequently enters a magnetic field in the same direction—if it hasn't been in any other magnetic fields. If the atom enters a magnetic field perpendicular to the field it initially passed through, it has a 50% chance of going either way, and if it later enters a magnetic field in the same direction as the original field it traversed, it has a 50% chance of going either way.

In effect, when a silver atom passes through a magnetic field, it is endowed with one bit of information about how it behaves in that field: UP or DOWN in a vertical field, and RIGHT or LEFT in a horizontal field. But when the atom passes through a field perpendicular to the original field, the original information is erased and replaced with information about how the atom behaves in the new field.

So, Penelope's plan is this. She will represent a 0 by a silver atom initially deflected either UP or RIGHT. She will represent a 1 by a silver atom initially deflected either DOWN or LEFT. She launches the selected atom to Odysseus, across the azure tides of sea-roiling Poseidon. Odysseus randomly sets his magnetic field either vertical or horizontal, and he observes the deflection of the atom.

For example, suppose Penelope wants to transmit a 1 by sending Odysseus a DOWN atom. Suppose Odysseus chooses to set his magnetic field vertical. Then, he will observe the atom deflected DOWN. He knows that Penelope uses DOWN to represent 1, so he guesses that Penelope wanted to transmit a 1.

However, if Odysseus instead chooses a horizontal magnetic field for this atom, it equally likely deflects RIGHT or LEFT. If it deflects RIGHT, Odysseus guesses incorrectly that Penelope wanted to transmit a 0.

Suppose that the choices and results for the first four atoms are as shown in Table 1.3. After Odysseus measures all the atoms, he and Penelope reveal the directions of their magnetic fields in all cases. They don't need to encode this announcement; eavesdroppers can do no harm now. Odysseus discards his guesses whenever he chose a different magnetic field direction than Penelope. So in the example in Table 1.3, he discards his guesses for the second and fourth atoms. He knows that his guesses for the first and third atoms were correct, so he and Penelope have now established two bits of their secret key: 11. They repeat with as many atoms as necessary to generate a sufficiently long key.

Now, how do the laws of quantum physics guarantee that their key is secure? In other words, how can they be *certain* that no eavesdropper copied the data as it traveled from Penelope to Odysseus? If Hector tries to intercept the silver atom, he has to choose whether to set his magnetic field horizontal or vertical, just as Odysseus does. He observes the atom and passes it on to Odysseus, but his attempt at espionage is thwarted by quantum physics. Let's see how.

Table 1.3

	First atom	Second atom	Third atom	Fourth atom
Penelope's bit	1	1	1	0
Penelope's magnetic field	vertical	horizontal	horizontal	vertical
Penelope's atom	DOWN	LEFT	LEFT	UP
Odysseus's magnetic field	vertical	vertical	horizontal	horizontal
Odysseus's observation	DOWN	UP	LEFT	RIGHT
Odysseus's guess	1	0	1	0

Consider this sequence of choices and outcomes:

Penelope's bit	1
Penelope's magnetic field	vertical
Penelope's atom	DOWN
Hector's magnetic field	horizontal
Hector's observation	RIGHT
Odysseus's magnetic field	vertical
Odysseus's observation	UP
Odysseus's guess	0

Penelope chooses a vertical magnetic field, and Hector chooses a horizontal magnetic field. The silver atom is equally likely to deflect RIGHT or LEFT in Hector's magnetic field. Odysseus has chosen the same magnetic field as Penelope, but the silver atom, having been deflected RIGHT, is equally likely to deflect UP and DOWN. If it deflects UP, Odysseus's guess, 0, differs from Penelope's bit, even though they chose the same magnetic field direction.

To detect Hector's meddling, Penelope and Odysseus sacrifice some of their key bits by revealing them to each other (and unavoidably to any eavesdropper monitoring their communication). If their key bits disagree, when they chose the same magnetic field direction, they must conclude that an eavesdropper meddled with their attempt to generate a secret key. So they have to abandon this attempt at a secret key, and maybe try again later.

Penelope and Odysseus have to compare a sufficiently large number of key bits, perhaps 10, to have a high probability of detecting an eavesdropper. This is because the eavesdropper corrupts only 25% of the key bits. Half of the time, the eavesdropper chooses the same magnetic field direction as Penelope. In this case, the eavesdropper observes the silver atom without changing it and passes it unaltered on to Odysseus. The other half of the time, the eavesdropper chooses a different magnetic field direction than Penelope. This effectively erases the information about deflection in the direction of Penelope's magnetic field. So when Odysseus sets his magnetic field in the same direction as Penelope's, he's only 50% likely to re-create Penelope's original deflection. In summary: Half of the time, Hector chooses a different magnetic field direction than Penelope, and when this occurs, the key bit is corrupted half of the time. Half of one half is 25%, the rate of key bit corruption.

If Penelope and Odysseus compare a subset of their key bits and find that they all agree, they conclude that no eavesdropper was present, and all their *other* key bits remain secret and secure. (They have to discard the bits they reveal because an eavesdropper could be eavesdropping on this communication, even if no eavesdropper intercepted the silver atoms.) This is a successful instance of quantum key distribution. Quantum key distribution can't stop eavesdroppers from eavesdropping, but it reveals the presence of an eavesdropper if there is one.

Now, let's rewrite UP, DOWN, RIGHT, and LEFT in the language of quantum computing. Let's use the symbol $|0\rangle$ to represent a silver atom deflected UP. This symbol, $|0\rangle$, is called a *ket*, which is the second syllable of brac*ket*. $|0\rangle$ is often pronounced "ket zero." We'll use $|1\rangle$ to represent an atom deflected DOWN. $|0\rangle$ and $|1\rangle$ are two possible states of a quantum bit, or *qubit*.

Remember that classical bits, 0 and 1, can represent two voltages in a circuit, or black and white stripes in a bar code, or different thicknesses of a plastic layer in CDs and DVDs. Similarly, a qubit can be constructed of many different physical systems. A silver atom is only one possibility, and not a very feasible one; not all quantum engineers are as cunning as Penelope. A qubit can be made of a photon, such that $|0\rangle$ and $|1\rangle$ represent two different polarization directions. In IBM's quantum processors that we'll use throughout this book, $|0\rangle$ and $|1\rangle$ represent two different states of a superconducting circuit. In fact, we'd rather *not* specify how our qubits are constructed: We want to establish rules and algorithms that work for *any* qubits, however they are made.

I once asked Matthias Steffen, IBM's chief quantum architect, how to think about the $|0\rangle$ and $|1\rangle$ states of a superconducting circuit. He told me that he'd given up on visualizing it. So let's follow the lead of IBM's chief quantum architect. We will establish rules that allow us to predict the results when qubits are measured. But we will not stumble far along the rocky path of wondering what qubits are doing when we're not measuring them.

Whereas a classical bit is either 0 or 1, a qubit can be in some combination of $|0\rangle$ and $|1\rangle$, written $\alpha|0\rangle + \beta|1\rangle$. α and β are called *probability amplitudes*, and they are related to the probabilities of different measurements. Now, there are different ways of measuring qubits, analogous to the different magnetic field directions for the silver atoms. If we do a measurement that results in either $|0\rangle$ and $|1\rangle$, this is called a measurement in the *computational basis*. (The computational basis is sometimes called the z basis by association with the vertical, or z, direction.) The probability of measuring $|0\rangle$ is $|\alpha|^2$, and the probability of measuring $|1\rangle$ is $|\beta|^2$. The total probability of measuring *something* is 1, which means

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.3}$$

This condition is called *normalization*. If α and β are real numbers, then $|\alpha|^2 = \alpha^2$ and $|\beta|^2 = \beta^2$. However, α and β are allowed to be complex numbers. In this case, $|\alpha|^2 = \alpha\alpha^*$, where α^* is the complex conjugate of α. We will work exclusively with real numbers for most of our journey.

We assigned UP $= |0\rangle$ and DOWN $= |1\rangle$. What about RIGHT and LEFT? Atoms deflected RIGHT and LEFT are equally likely to subsequently deflect UP or DOWN in a vertical magnetic field. This means α^2 and β^2 should both be 1/2. We'll choose $\text{RIGHT} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

and $\text{LEFT} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$. When we write $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, the probability amplitude of $|0\rangle$ is $\frac{1}{\sqrt{2}}$, and the probability amplitude of $|1\rangle$ is $-\frac{1}{\sqrt{2}}$.

It's convenient to define

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{1.4a}$$

and

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{1.4b}$$

In the language of qubits, we can now say that deflection in a horizontal magnetic field is a case of a measurement that yields either $|+\rangle$ or $|-\rangle$. This is called a measurement in the x basis by association with the horizontal, or x, direction.

We can combine Eqs. (1.4a) and (1.4b) to write $|0\rangle$ and $|1\rangle$ in terms of $|+\rangle$ and $|-\rangle$. The ket symbols can be manipulated exactly like algebraic symbols such as x and y. We can add Eqs. (1.4a) and (1.4b) together, to find $|+\rangle + |-\rangle = \frac{2}{\sqrt{2}}|0\rangle$. Solving for $|0\rangle$, we obtain

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right), \tag{1.5a}$$

using $\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{\sqrt{2}}\right) = \frac{2}{2\sqrt{2}} = \frac{1}{\sqrt{2}}$. Similarly, subtracting Eq. (1.4b) from Eq. (1.4a) yields $|+\rangle - |-\rangle = \frac{2}{\sqrt{2}}|1\rangle$. Solving for $|1\rangle$,

$$|1\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right). \tag{1.5b}$$

Whereas Eq. (1.4) gives probability amplitudes of $|0\rangle$ and $|1\rangle$, Eq. (1.5) gives probability amplitudes of $|+\rangle$ and $|-\rangle$: probability amplitudes for measurements in the x basis. Remembering to square probability amplitudes to find probabilities, we see that a qubit in state $|0\rangle$ or $|1\rangle$ is equally likely to be found in $|+\rangle$ or $|-\rangle$ when measured in the x basis. This is a generalization of the fact that a silver atom deflected UP or DOWN is equally likely to deflect RIGHT or LEFT when entering a horizontal magnetic field.

When a qubit is measured, the state *becomes* whatever was measured. For example, if a qubit, initially in state $|1\rangle$, is measured in the x basis, it is equally likely to *become* $|+\rangle$ or $|-\rangle$. Effectively, its original state is erased and replaced by the new one. This is a generalization of the rule we saw for the silver atoms: If an atom is initially deflected UP or DOWN, and then traverses

a horizontal magnetic field, it will deflect RIGHT or LEFT without retaining any information about whether it had been deflected UP or DOWN. This is sometimes called the *collapse* of the state due to measurement.

Actually, this effect of measurement is not significant in most of the later chapters. Measurements will occur only at the end of our quantum circuits. And we will almost always measure in the computational basis, so the result of measuring a qubit will be either $|0\rangle$ or $|1\rangle$. In fact, the result of the measurement will be recorded as a classical bit, 0 or 1. All we have to remember going forward is that if a qubit in state $\alpha|0\rangle + \beta|1\rangle$ is measured, then the probability of measuring 0 is $|\alpha|^2$, and the probability of measuring 1 is $|\beta|^2$.

To review, let's repeat our example with Penelope, Hector, and Odysseus, but now using ket notation:

Penelope's bit	1
Penelope's basis	computational, also called z (measurement yields $|0\rangle$ or $|1\rangle$)
Penelope's atom	$|1\rangle$
Hector's basis	x (measurement yields $|+\rangle$ or $|-\rangle$)
Hector's measurement	$|+\rangle$
Odysseus's basis	computational, also called z (measurement yields $|0\rangle$ or $|1\rangle$)
Odysseus's measurement	$|0\rangle$
Odysseus's guess	0

Penelope's initial state is $|1\rangle$, which equals $|1\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right)$, given by Eq. (1.5b). Hector measures this qubit in the x basis, so the result will be $|+\rangle$ or $|-\rangle$. The probability amplitude of $|+\rangle$ is $\frac{1}{\sqrt{2}}$, and the probability amplitude of $|-\rangle$ is $-\frac{1}{\sqrt{2}}$. We square these amplitudes to determine probabilities, and we find that the probability of measuring $|+\rangle$ is 1/2, and so is the probability of measuring $|-\rangle$. Hector's measurement happens to yield $|+\rangle$.

Next, Odysseus measures this qubit in the computational basis, so we have to write $|+\rangle$ in terms of computational basis states: $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$, as given in Eq. (1.4a). The probability amplitude is $\frac{1}{\sqrt{2}}$ for both $|0\rangle$ and $|1\rangle$, so $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ is the probability of obtaining either result. Odysseus happens to find $|0\rangle$, which is different from the state that Penelope sent him. If they share these facts with each other, they will know that Hector has meddled with their qubit.