

(BB84 protocol)
 Quantum Computer Scientist
 Computer Scientist

$$|+\rangle = \{ |\rightarrow\rangle, |\uparrow\rangle \} \quad \left. \right\} \text{ Computational Basis}$$

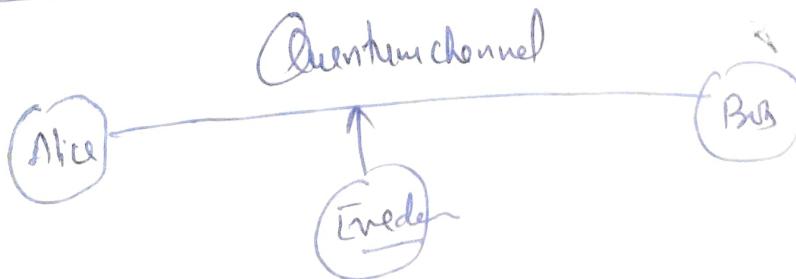
$$|X\rangle = \{ |\rightarrow\rangle, |\nwarrow\rangle \} \quad \left. \right\} \text{ Hadamard Basis}$$

$$|\uparrow\rangle \text{ w.r.t. to } X \text{ will be } \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$$

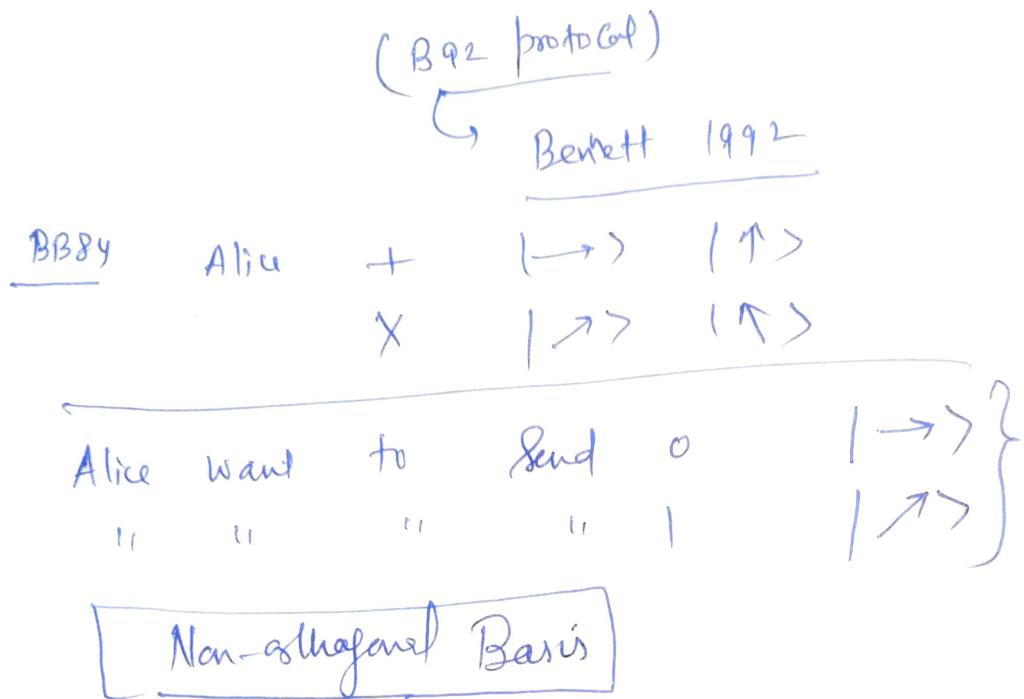
$\stackrel{\text{neat trick}}{=}$

$$\frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|+\rangle \right] = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$\begin{aligned} |\langle \rightarrow | \rightarrow \rangle|^2 &= \frac{1}{2} \\ |\langle \rightarrow | \uparrow \rangle|^2 &= \frac{1}{2} \\ |\langle \rightarrow | \rightarrow \rangle|^2 &= 1 \end{aligned} \quad \left. \right\}$$



$(4n + \delta)$ bits



Step-2 Bob receives the publics. Bob tosses the coin 4 times & decide the basis in + or X for measurement.

$$+ \rightarrow | \rightarrow \rangle$$

$$\rightarrow | \uparrow \rangle$$

Alice	Bob	Bob
$ \rightarrow \rangle$	$ \rightarrow \rangle$	$ \rightarrow \rangle$
$ \uparrow \rangle$	$ \uparrow \rangle$	$ \rightarrow \rangle$

so. chance

Alice	Bob	Bob Observation		
			\rightarrow \rangle	\uparrow \rangle
$ \rightarrow \rangle$	H	$ \rightarrow \rangle$ uncertain	$ \rightarrow \rangle$	$ \rightarrow \rangle$ Reject Not possible
$ \uparrow \rangle$	H	$ \uparrow \rangle$	$ \uparrow \rangle$	$ \uparrow \rangle$ Certain Case
$ \rightarrow \rangle$	H	$\rightarrow \rangle$ ^{Get Measured}	$ \rightarrow \rangle$	$ \rightarrow \rangle$ Bob found Alice sent 1
$ \uparrow \rangle$	H	$\uparrow \rangle$ ^{Not Possible}	$ \uparrow \rangle$	$ \uparrow \rangle$ Alice sent 1

Cryptography

*We dance round in a ring and suppose,
But the Secret sits in the middle and knows.
Robert Frost, *The Secret Sits* (1942)*

In this chapter we explore the merging of quantum computation and classical cryptography. This is a new and exciting field of pure and applied research known as **quantum cryptography**.

We begin with the basics of classical cryptography in Section 9.1. Section 9.2 demonstrates a quantum cryptographic protocol that uses two different bases. We improve on this in Section 9.3, where a protocol with one basis is employed. Section 9.4 shows how to use entanglement to secretly send a message. We conclude with Section 9.5, in which teleportation is demonstrated.

9.1 CLASSICAL CRYPTOGRAPHY

Before delving into quantum cryptography, we need to familiarize ourselves with the core ideas of classical cryptography. A good place to start is the following definition.

Definition 9.1.1 *Cryptography is the art of concealing messages.*

Indeed, this is precisely what the etymology reveals: “Cryptography” is a compound of two Greek words, *crypton*¹ and *graphein*, which mean, respectively, hidden and writing.

Turning an ordinary message into an indecipherable one is called **encryption**. The opposite action, i.e., restoring the original message, is **decryption**. The original message is generally referred to as the **plaintext**, and the encrypted message is the **ciphertext**. A method for encryption is often referred to as an **encryption protocol**.

¹ Now you know where the Kryptonite got its name. It is rare to find and hence is “hidden.” It usually stays concealed unless Lex Luthor gets hold of it!

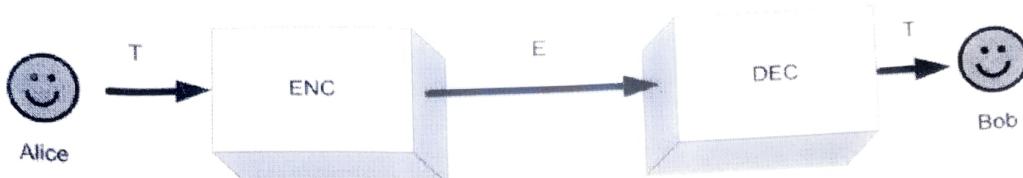


Figure 9.1. A basic communication scheme.

The history of cryptography is a very long one. As soon as people started sending messages to each other that were not intended for the public, the need for privacy arose. At the very moment encryption ideas and techniques were devised by some smart individual, another one, just as smart set out to break them. Thus, **cryptology** was born.

To present encryption and decryption methods, we need to set the scene. First, we need two characters – the **sender** of messages and the **receiver**. In the standard cryptology literature, these two are named Alice and Bob. Alice wants to send a message to Bob, say, a string of plaintext T . We assume that Alice and Bob are physically separated and that they can communicate with each other over some kind of **insecure channel**.²

Alice uses an encryption algorithm – let's call it ENC – that turns T into some encrypted text E . We can think of ENC as some computable function, taking T and an additional parameter K_E , known as the **encryption key**, as inputs. ENC computes the encrypted message E , which is transmitted to Bob.

$$ENC(T, K_E) = E. \quad (9.1)$$

Bob receives E (assuming there is no noise involved) and applies a decryption algorithm, DEC , to the encrypted message to reconstruct T . DEC requires a **decryption key** K_D as input.

$$DEC(E, K_D) = T. \quad (9.2)$$

The entire scheme is shown in Figure 9.1.

Summing up, $ENC(-, K_E)$ and $DEC(-, K_D)$ are a pair of computable functions such that for every message T , the following equation holds:

$$DEC(ENC(T, K_E), K_D) = T. \quad (9.3)$$

What does this equation tell us? It states that as long as we use the right keys, we can always retrieve the original message intact without any loss of information.

Exercise 9.1.1 Does Equation (9.3) imply that $ENC(-, K_E)$ and $DEC(-, K_D)$ are a pair of bijective functions that are inverse to each other? ■

Let us now examine a concrete example of an encryption protocol, a method known as the **Caesar's protocol**.³ Arrange the letters of the English alphabet on a

² Why insecure? First of all, if the channel were foolproof beyond any reasonable doubt, we would have no story. Why bother with cryptography if no one else can spy on the message? Second, in the context of secure message transmission, *every* channel must be assumed insecure unless proven safe.

³ Julius Caesar apparently used an encryption technique like this one to communicate with his generals during his military campaigns. See Suetonius' *Life of Julius Caesar*, Paragraph 56.

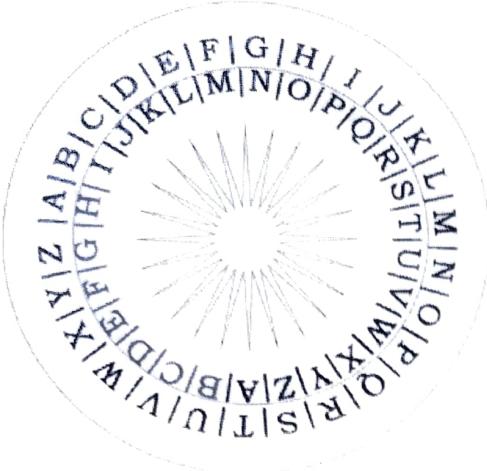


Figure 9.2. A children's encryption toy.

circle, so that the order is

$$\dots, A, B, C, \dots, X, Y, Z, A, B, \dots \quad (9.4)$$

Let $ENC = DEC = \text{shift}(-, -)$, where $\text{shift}(T, n) = T'$, the string obtained from T by shifting each character n steps clockwise if n is positive, or counterclockwise if it is negative (for instance, $\text{shift}(\text{"MOM," } 3) = \text{"PRP"}$). Children actually make a helpful toy for this encryption protocol as depicted in Figure 9.2. This toy consists of two concentric circles with the alphabet written clockwise on each circle. The circles can be turned until the desired letters are matched up. With this encryption protocol, the decryption key is just the encryption key with the sign changed: $K_D = -K_E$.

Exercise 9.1.2 Decipher the following message “JNTGMNF VKRIMHZKTIAR BL YNG.” (Hint: Use Figure 9.2.) ■

Programming Drill 9.1.1 Implement the encryption and decryption of text with the Caesar’s protocol. Using ASCII makes this particularly easy.

To make our story a bit more exciting, we need a third character, Eve, the **eavesdropper**, who can intercept the encrypted message and try to decode it. As previously noted, Alice is using an insecure channel (such as a public telephone wire) to transmit messages to Bob. Eve can thus tap into the channel and eavesdrop on its content. The protocol we have just presented is quite primitive and would not stand Eve’s scrutiny for too long.

Imagine that you are Eve and that by tapping into the insecure channel you can save fairly long encrypted messages from Alice. How would you discover the encryption mechanism? If you were Eve, you might have a hunch about the weak side of the simple-minded protocol we have just introduced. The weakness lies in the fact that the original message and the encrypted one are *highly correlated*. By calculating simple statistics on the encrypted text, Eve may easily find her way back to the original text. Aside from her malicious purposes, Eve works exactly like an archeologist decoding an ancient unknown language.

To counter Eve’s insight, Alice and Bob change their protocol. Their ideal strategy is to create an encrypted message E that bears no statistical correlation with the

original message T . How can this be accomplished? Here is a surprisingly simple answer: a straightforward protocol known as the **One-Time-Pad protocol** or **Vernam cipher**.

As we are computer scientists, for the rest of this chapter, we shall refer to T as a binary string of length n . Alice tosses a coin n times and generates a sequence of random bits that she uses as her random key K . Assuming Alice and Bob both share K , they can exchange messages by means of the following protocol:

Step 1. Alice calculates $E = T \oplus K$, where \oplus stands for the bitwise XOR operation.⁴

Step 2. Alice sends E along a public insecure channel.

Step 3. Bob retrieves E and calculates T from $T = E \oplus K$.

In this notation that we have introduced,

$$K_E = K_D = K, \quad (9.5)$$

$$ENC(T, K) = DEC(T, K) = T \oplus K, \quad (9.6)$$

and

$$\begin{aligned} DEC(ENC(T, K), K) &= DEC(T \oplus K, K) \\ &= (T \oplus K) \oplus K = T \oplus (K \oplus K) = T. \end{aligned} \quad (9.7)$$

Example 9.1.1 The following table shows an example of an implementation of the One-Time-Pad protocol:

One-Time-Pad Protocol						
Original message T	0	1	1	0	1	1
Encryption key K	\oplus	1	1	1	0	1
Encrypted message E	1	0	0	0	0	1
Public channel	↓	↓	↓	↓	↓	↓
Received message E	1	0	0	0	0	1
Decryption key K	\oplus	1	1	1	0	1
Decrypted message T	0	1	1	0	1	1

⁴ A quick reminder on XOR: it is simply bitwise addition modulo two. $01001101 \oplus 11110001 = 10111100$

Exercise 9.1.3 Find a friend and flip a coin to get an encryption key K . Then use K to send a message. See if it works. ■

Programming Drill 9.1.2 Implement the One-Time-Pad protocol.

Exercise 9.1.4 Suppose Alice generates only one pad key K , and uses it to encrypt two messages T_1 and T_2 (we are assuming they have exactly the same length). Show that by intercepting E_1 and E_2 , Eve can get $T_1 \oplus T_2$ and hence is closer to the original text. ■

There are a couple of issues with the One-Time-Pad protocol:

1. As Exercise 9.1.4 shows, the generation of a new key K is required each time a new message is sent. If the same key is used twice, the text can be discovered through statistical analysis, and hence the name “One-Time-Pad.”
2. The protocol is secure only insofar as the key K is not intercepted by Eve (remember, Alice and Bob must share the same pad in order to communicate). We see in the next section that quantum computing comes to the rescue for this crucial issue.

So far, we have assumed that the pair of keys K_E and K_D are kept secret. In fact, only one key was needed because knowledge of the first key implies knowledge of the second and vice versa.⁵ A cryptographic protocol where the two keys are computable from one another, thus requiring that both keys be kept secret, is said to be **private key**.

There is yet another game in town: in the 1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman introduced one of the first examples of public-key cryptography, now simply known as **RSA** (Rivest, Shamir, and Adleman, 1978). In public-key protocols, the knowledge of one key does not enable us to calculate the second one. To be precise, the requirement is that the computation of the second key from the first should be hard.⁶

Now, suppose that Bob has computed such a pair of keys K_E and K_D . Furthermore, suppose that brute force trial and error to find K_D given K_E is totally infeasible by Eve or anyone else (for instance, there could be an endless list of candidate keys). Bob's course of action is as follows: he places the encryption key K_E in some public domain, where *anyone* can get it. He can safely advertise his protocol, i.e., the knowledge of $ENC(-, -)$ and $DEC(-, -)$. At the same time, he guards the decryption key for himself. When Alice wants to send a message to Bob, she simply uses K_E on her message. Even if Eve intercepts the encrypted text, she cannot retrieve K_D 's decryption key, and so the message is safe. This scheme is shown in Figure 9.3.

Let us rephrase the foregoing: once Bob has his magic pair of keys, he finds himself with two computable functions

$$F_E(-) = ENC(-, K_E) \tag{9.9}$$

$$F_D(-) = DEC(-, K_D) \tag{9.10}$$

⁵ In Caesar's protocol, the decryption key is just the encryption key with changed sign, whereas in the One-Time-Pad protocol, the two keys are exactly the same.

⁶ By “hard,” we mean that the number of computational steps to get from the first key to the second key is more than polynomial in the length of the first key.

Exercise 9.1.5 Suppose Alice and Bob communicate using some kind of public-key protocol. Alice has a pair of keys (one public, one private), and so does Bob. Devise a way in which Alice and Bob can communicate simultaneously while authenticating their messages. (Hint: Think of encoding one message “inside” another.) ■

9.2 QUANTUM KEY EXCHANGE I: THE BB84 PROTOCOL

While discussing the One-Time-Pad protocol, we pointed out that the problem of securely transmitting the key is a serious one. During the 1980s, two authors came up with a clever idea that exploits quantum mechanics. This idea formed the basis of the first **quantum key exchange (QKE)** protocol.

Before presenting QKE in some detail, let us first see if we can guess which features of the quantum world are appealing to cryptographers. In the classical case, Eve is somewhere along the insecure channel listening for some bits of information. What can she do?

1. She can make copies of arbitrary portions of the encrypted bit stream and store them somewhere to be used for later analysis and investigations.
2. Eve can listen without affecting the bitstream, i.e., her eavesdropping does not leave traces.

Now, assume that Alice sends qubits, rather than bits, over some channel.⁹

- 1'. Eve cannot make perfect copies of the qubit stream: the no-cloning theorem discussed in Section 5.4 prevents this from happening.
- 2'. The very act of measuring the qubit stream alters it.

At first sight, the points raised above seem like limitations, but from the point of view of Alice and Bob, they actually turn out to be great opportunities. How? For one thing, the no-cloning theorem hampers Eve’s ability to use past messages to conduct her analysis. Even more important, each time she measures the qubit stream, she disturbs it, allowing Alice and Bob to detect her presence along the channel.

The first quantum key exchange protocol was introduced by Charles Bennett and Gilles Brassard in 1984, and hence the name **BB84**. This section describes this important protocol.

Alice’s goal is to send Bob a key via a quantum channel. Just as in the One-Time-Pad protocol, her key is a sequence of random (classical) bits obtained, perhaps, by tossing a coin. Alice will send a qubit each time she generates a new bit of her key. But which qubit should she send?

In this protocol, Alice will employ two different orthogonal bases shown in Figure 9.4:

$$+ = \{|-\rangle, |\uparrow\rangle\} = \{[1, 0]^T, [0, 1]^T\} \quad (9.11)$$

⁹ This chapter is not concerned with hardware implementation of quantum cryptography. That topic is tackled in Chapter 11. For the time being, suffice it to note that any two-dimensional quantum system (like spin or photon polarization) could be employed for transmission.

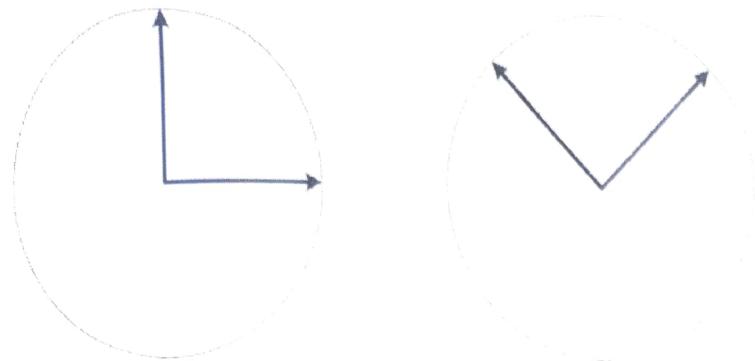


Figure 9.4. Two bases used for BB84.

and

$$X = \{| \nwarrow \rangle, | \nearrow \rangle\} = \left\{ \frac{1}{\sqrt{2}}[-1, 1]^T, \frac{1}{\sqrt{2}}[1, 1]^T \right\}. \quad (9.12)$$

We shall refer to the first basis as the “plus” basis and the second as the “times” basis. Essentially, they are two alternative vocabularies that Alice and Bob will use to communicate.

In these vocabularies, the states $|0\rangle$ and $|1\rangle$ shall be described by the following table:

State / Basis	+	X	
$ 0\rangle$	$ \rightarrow \rangle$	$ \nearrow \rangle$	
$ 1\rangle$	$ \uparrow \rangle$	$ \nwarrow \rangle$	

(9.13)

For example, in the + basis, a $| \rightarrow \rangle$ will correspond to a $|0\rangle$. If Alice wants to work in the X basis and wants to convey a $|1\rangle$, she will send a $| \nwarrow \rangle$. Similarly, if Alice sends a $| \uparrow \rangle$ and Bob measures a $| \uparrow \rangle$ in the + basis, he should record a $|1\rangle$.

This is fine for basic states, but what about superpositions? If Bob measures photons using the + basis, he will only see photons as $| \rightarrow \rangle$ or $| \uparrow \rangle$. What if Alice sends a $| \nearrow \rangle$ and Bob measures it in the + basis? Then it will be in a superposition of states

$$| \nearrow \rangle = \frac{1}{\sqrt{2}}| \uparrow \rangle + \frac{1}{\sqrt{2}}| \rightarrow \rangle. \quad (9.14)$$

In other words, after measurement, there is a 50–50 chance of Bob’s recording a $|0\rangle$ or a $|1\rangle$. Again, Alice could use the X basis, intending to send a $|0\rangle$, and Bob has a 50–50 chance of recording a $|1\rangle$ and a 50–50 chance of recording a $|0\rangle$. In all, there are four possible superpositions:

- $| \nwarrow \rangle$ with respect to + will be $\frac{1}{\sqrt{2}}| \uparrow \rangle - \frac{1}{\sqrt{2}}| \rightarrow \rangle$.
- $| \nearrow \rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}| \uparrow \rangle + \frac{1}{\sqrt{2}}| \rightarrow \rangle$.
- $| \uparrow \rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}| \nearrow \rangle + \frac{1}{\sqrt{2}}| \nwarrow \rangle$.
- $| \rightarrow \rangle$ with respect to X, will be $\frac{1}{\sqrt{2}}| \nearrow \rangle - \frac{1}{\sqrt{2}}| \nwarrow \rangle$.

$$\begin{aligned} P = |1\rangle &= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) = |0\rangle \\ &+ \frac{1}{\sqrt{2}} \left(\left(\frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle) \right) \right) \end{aligned}$$

Basis Reconciliation

Exercise 9.2.1 Work out what $| \leftarrow \rangle$, $| \downarrow \rangle$, $| \swarrow \rangle$, and $| \searrow \rangle$ would be in terms of the two bases.

Armed with this vocabulary and the inherent indeterminacy of the two bases, Alice and Bob are ready to start communicating. Here are the steps of the protocol:

Step 1. Alice flips a coin n times to determine which classical bits to send. She then flips the coin another n times to determine in which of the two bases to send those bits. She then sends the bits in their appropriate basis.

For example, if n is 12, we might have something like this:

Step 1: Alice sends n random bits in random bases

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

(9.15)

Step 2. As the sequence of qubits reaches Bob, he does not know which basis Alice used to send them, so to determine the basis by which to measure them he also tosses a coin n times. He then goes on to measure the qubit in those random bases.

In our example, we might have something like this:

Step 2: Bob receives n random bits in random measurements

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob's bits	0	1	1	1	1	0	1	0	1	0	1	0

(9.16)

Here is the catch: for about half of the time, Bob's basis will be the same as Alice's, in which case his result after measuring the qubit will be identical to Alice's original bit. The other half of the time, though, Bob's basis will differ from Alice's. In that case, the result of Bob's measurement will agree with Alice's original bit about 50% of the time.

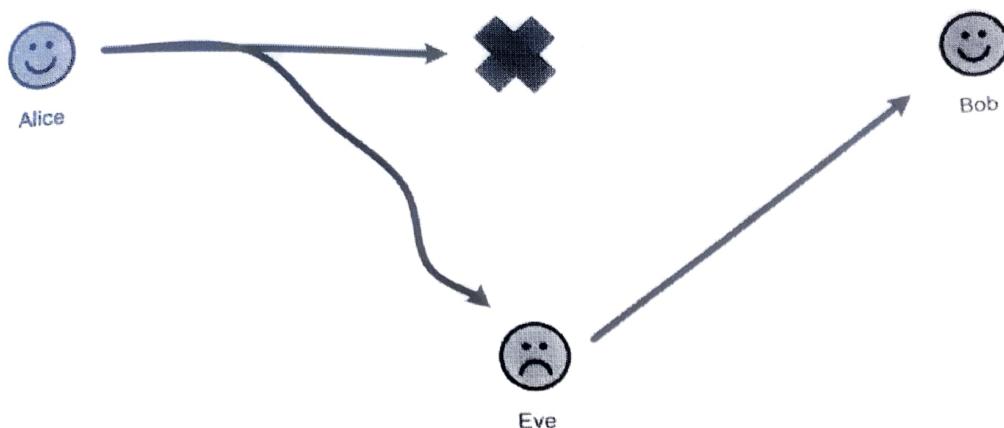


Figure 9.5. Eve “cutting” the quantum wire and transmitting her own message.

Programming Drill 9.2.1 Write functions that mimic Alice, Bob, and their interactions. **Alice** should generate two random bit strings of the same length. Call one **BitSent** and the other **SendingBasis**.

Bob will be a function that generates a random bit string of the same length called **ReceivingBasis**.

All three of these bit strings should be sent to an “all-knowing” function named **Knuth**. This function must look at all three and create a fourth bit string named **BitReceived**. This is defined by the following instruction:

$$\text{BitReceived}[i] = \begin{cases} \text{BitSent}[i], & \text{if } \text{SendingBasis}[i] = \text{ReceivingBasis}[i], \\ \text{random}\{0, 1\}, & \text{otherwise.} \end{cases} \quad (9.17)$$

This $\text{random}\{0, 1\}$ is the classical analog of a qubit collapsing to a bit. **Knuth** must furthermore evaluate the percentage of bits that **Bob** receives accurately.

Let us continue with the protocol: If evil Eve is eavesdropping, she must be reading the information that Alice transmits and sending that information onward to Bob, as shown in Figure 9.5.

Eve also does not know in which basis Alice sent each qubit, so she must act like Bob. She will also toss a coin each time. If Eve’s basis is identical to Alice’s, her measure will be accurate and she will, in turn, send accurate information on to Bob. If, on the other hand, her basis is different from Alice’s, her bit will be in agreement with Alice’s only 50% of the time. However, here’s the rub: the qubit has now collapsed to one of the two elements of Eve’s basis. Because of the no-cloning theorem, Eve does not have the luxury of making a copy of the original qubit and then sending it on (after her probe), so she just sends the qubit after her observation. Now

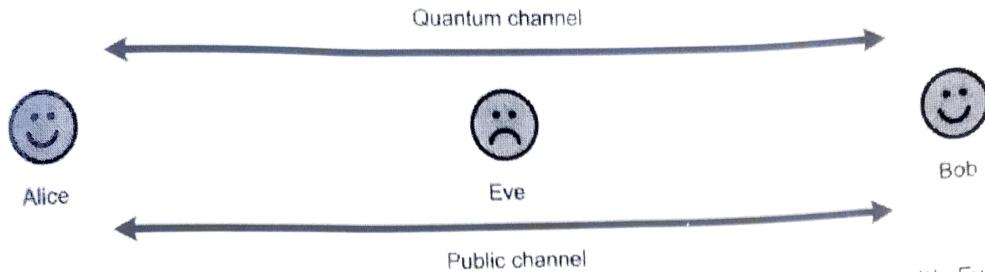


Figure 9.6. Alice and Bob communicating on quantum and public channels, with Eve eavesdropping.

Bob will receive it in the wrong basis. What are his chances of getting the same bit Alice has? Answer: His chances are 50–50.¹⁰

Therefore if Eve intercepts and measures each qubit sent, she will negatively affect Bob's chances of agreement with Alice.

Exercise 9.2.2 Give an estimate of how frequently Bob's bit will agree with Alice's if Eve is constantly eavesdropping. ■

By computing some simple statistics, a potential intrusion by Eve would be detected. This suggests how to complete BB84. Let us examine the details.

After Bob has finished decoding the qubit stream, he has in his hands a bit stream of length n . Bob and Alice will discuss which of the n bits were sent and received in the same basis. They can do this on a public channel, such as a telephone line. Figure 9.6 is helpful.

Step 3. Bob and Alice publicly compare which basis they used chose at each step. For instance, he can tell her X, +, X, X, Alice replies by telling him when he was right, and when he was not. Each time they disagreed, Alice and Bob scratch out the corresponding bit. Proceeding this way until the end, they are each left with a subsequence of bits that were sent and received in the same basis. If Eve was not listening to the quantum channel, this subsequence should be exactly identical. On average, this subsequence is of length $\frac{n}{2}$.

Step 3: Alice and Bob publicly compare bases used

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	+	+	X	+	+	+	X	+	X	X	X	+
Public channel	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔
Bob's random bases	X	+	X	X	+	X	+	+	X	X	X	+
Which agree?	✓	✓		✓				✓	✓	✓	✓	✓
Shared secret keys	1	1		1				0	1	0	1	0

(9.18)

¹⁰ Eve does, in fact, have other options. For example, she can “listen in” with a third basis. However, such considerations would take us too far afield.

Programming Drill 9.2.2 Continuing with the last programming drill, write a function named **Knuth2** that accepts all three-bit strings and creates a bit string (of possibly shorter length) called **AgreedBits**, which is a substring of both **BitSent** and **BitReceived**.

But what if Eve was eavesdropping? Alice and Bob would also like to engage in some intrusion detection. They want to know if Eve (or anyone else) was listening in. They do this by comparing some of the bits of the subsequence.

Step 4. Bob randomly chooses half of the $\frac{n}{2}$ bits and publicly compares them with Alice. If they disagree by more than a tiny percentage (that could be attributed to noise), they know that Eve was listening in and then sending what she received. In that case, they scratch the whole sequence and try something else. If the exposed sequence is mostly similar, it means that either Eve has great guessing ability (improbable) or Eve was not listening in. In that case, they simply scratch out the revealed test subsequence and what remains is the unrevealed secret private key.

Step 4: Alice and Bob publicly compare half of the remaining bits

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Shared secret keys	1	1		1			0	1	0	1	1	0
Randomly chosen to compare			✓					✓	✓			✓
Public channel				⇒				⇒	⇒			⇒
Shared secret keys	1	1		1			0	1	0	1	0	
Which agree?				✓				✓	✓			✓
Unrevealed secret keys:				1			1		0		1	

In this protocol, Step 3 has eliminated half of the original qubits sent. So if we begin with n qubits, only $\frac{n}{2}$ qubits will be available after Step 3. Furthermore, Alice and Bob publicly display half of the resulting qubits in Step 4. This leaves us with $\frac{n}{4}$ of the original qubits. Do not be disturbed about this, as Alice can make her qubit stream as large as she needs. Hence, if Alice is interested in sending an m bit key, she simply starts with a $4m$ qubit stream.

9.3 QUANTUM KEY EXCHANGE II: THE B92 PROTOCOL

In the previous section, we introduced the first quantum key exchange protocol. Alice had two distinct orthogonal bases at her disposal. It turns out that the use of two different bases is redundant, provided one employs a slightly slicker means of measuring. This simplification results in another quantum key distribution protocol, known as **B92**. **B** stands for its inventor, Charles Bennett, and 1992 is the year it was published.

The main idea in B92 is that Alice uses only one *nonorthogonal* basis. Let us work out the protocol with the following example:

$$\{| \rightarrow \rangle, | \nearrow \rangle\} = \left\{ [1, 0]^T, \frac{1}{\sqrt{2}}[1, 1]^T \right\}. \quad (9.19)$$

Exercise 9.3.1 Verify that these two vectors are, in fact, not orthogonal. ■

Before going into detail, we need to pause and reflect a little. We know that all observables have an orthogonal basis of eigenvectors. This means that if we consider a nonorthogonal basis, there is no observable whose basis of eigenvectors is the one we have chosen. In turn, this means that there is no single experiment whose resulting states are precisely the members of our basis. Stated differently, no single experiment can be set up for the specific purpose of discriminating unambiguously between the nonorthogonal states of the basis.

Alice takes $| \rightarrow \rangle$ to be 0 and $| \nearrow \rangle$ to be 1. Using this language, we can begin the protocol.

Step 1. Alice flips a coin n times and transmits to Bob the n random bits in the appropriate polarization with a quantum channel.

Here is an example.

Step 1: Alice sends n random bits in the \angle basis												
Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's qubits	\rightarrow	\rightarrow	\nearrow	\rightarrow	\nearrow	\rightarrow	\nearrow	\rightarrow	\nearrow	\nearrow	\nearrow	\rightarrow
Quantum channel	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow	\Downarrow

(9.20)

Step 2. For each of the n qubits, Bob measures the received qubits in either the $+$ basis or the X basis. He flips a coin to determine which basis to use.

There are several possible scenarios that can occur:

- If Bob uses the $+$ basis and observes a $| \uparrow \rangle$, then he knows that Alice must have sent a $| \nearrow \rangle = | 1 \rangle$ because if Alice had sent a $| \rightarrow \rangle$, Bob would have received a $| \rightarrow \rangle$.
- If Bob uses the $+$ basis and observes a $| \rightarrow \rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $| \rightarrow \rangle$ but she could also have sent a $| \nearrow \rangle$ that collapsed to a $| \rightarrow \rangle$. Because Bob is in doubt, he will omit this bit.
- If Bob uses the X basis and observes a $| \nwarrow \rangle$, then he knows that Alice must have sent a $| \rightarrow \rangle = | 0 \rangle$ because if Alice had sent a $| \nearrow \rangle$, Bob would have received a $| \nearrow \rangle$.
- If Bob uses the X basis and observes a $| \nearrow \rangle$, then it is not clear to him which qubit Alice sent. She could have sent a $| \nearrow \rangle$ but she could also have sent a $| \rightarrow \rangle$ that collapsed to a $| \nearrow \rangle$. Because Bob is in doubt, he will omit this bit.

Continuing the example, we have the following:

Step 2: Bob receives n random bits in a random basis

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Bob's random bases	X	+	X	X	+	X	+	+	X	+	X	+
Bob's observations	↖	→	↗	↖	↑	↖	→	→	↗	↑	↗	→
Bob's bits	0	?	?	0	1	0	?	?	?	1	?	?

(9.21)

There are two possible bases that Bob could have used to measure. For each basis, there are two types of results. For half of those four results, the bit sent is certain. For the other half, there is uncertainty. Bob must omit the uncertain ones and keep the others hidden. He must inform Alice of this.

Step 3. Bob publicly tells Alice which bits were uncertain and they both omit them.

At this point, Alice and Bob know which bits are secret, so they may use those. But there is one more step if they want to detect whether or not Eve was listening in. They can, as in Step 4 of BB84, sacrifice half their hidden bits and publicly compare them. If they do not agree for a significant number, then they know that evil Eve has been doing her wicked deeds and the entire bit string should be ignored.

Programming Drill 9.3.1 Write three functions that mimic Alice, Bob, and their interactions. Use functions named **Alice92**, **Bob92**, and **Knuth92**. They should create bit strings that perform the B92 protocol.

9.4 QUANTUM KEY EXCHANGE III: THE EPR PROTOCOL

In 1991, Artur K. Ekert proposed a completely different type of quantum distribution protocol based on entanglement (Ekert, 1991). We shall present a simplified version of the protocol and then point to the original version.

We remind the reader that it is possible to place two qubits in the following entangled state¹¹:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (9.22)$$

¹¹ In the real world, the entangled pairs will probably be in a state

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}}. \quad (9.23)$$

as explained on page 136 of Chapter 4. When one is measured, they will both collapse to opposite values. We shall deal with the slightly easier version given in Equation (9.22). It will become apparent that if we use Equation (9.23), then Alice and Bob will have inverted bit strings. But if we use the simplified one given in Equation (9.22), they will share the exact same bit string.