Answer Key

Lesson

QUANTUM CRYPTOGRAPHY

Created by the IQC Scientific Outreach team
Contact: iqc-outreach@uwaterloo.ca

Institute for Quantum Computing
University of Waterloo
200 University Avenue West
Waterloo, Ontario, Canada N2L 3G1

uwaterloo.ca/iqc

Answer Key

Outline

QUANTUM CRYPTOGRAPHY

ACTIVITY GOAL:
Understand how the superposition and measurement principles can be used to communicate securely.

LEARNING OBJECTIVES

- The no-cloning theorem.
- Cryptography and the one-time pad.
- The BB84 quantum key distribution protocol.
- Compatible vs. incompatible measurement bases.

ACTIVITY OUTLINE

We start by outlining the **no-cloning theorem** and how it relates to the **quantum uncertainty principle**.

CONCEPT:
We only get to measure a quantum state once.

We then take a detour into cryptography to outline the one-time pad cryptographic scheme, and the issue of **secret key distribution**. A potential solution to this issue is **quantum key distribution (QKD)**.

CONCEPT:
Quantum systems can carry and encode information.

We show how QKD can be used to alert users to the presence of an eavesdropper, but only if we consider encodings in multiple measurement bases.

CONCEPT:
Measuring in one basis disturbs the information in another.

PREREQUISITE KNOWLEDGE

The **polarization** of light
Superposition and measurement (the **Two Golden Rules**)

SUPPLIES REQUIRED

QKD Worksheets #1 and #2

Lesson

QUANTUM CRYPTOGRAPHY

PHOTONS, QUBITS, AND THE NO-CLONING THEOREM

A photon is an indivisible unit of light. While it is countable like a particle is, it still has many of the same wave properties as bright beams of light do. For example, a photon may have its electromagnetic field polarized along a specific direction.

We can encode information into photons using these properties. We can describe the polarization of a photon in terms of two mutually exclusive states, such as horizontal and vertical polarization. By encoding the photon as either horizontal or vertical, we can encode binary information, or **bits**, into the photons. For example, "0" could be encoded as horizontal polarization and "1" as vertical polarization.

We can also create photons that are in a superposition of polarization states, and measure them in different measurement bases. These properties allow us to encode **quantum bits**, or **qubits**, into the polarization of a photon. Just like binary bits, qubits can take one of two values, "0" or "1". But they can also exist in a superposition of those states as well!

Say that we have one qubit, and we want to make a copy of it. While we can split a classical beam of light into two beams each with half the original intensity, a photon cannot be split in two in the same way. In fact, it can be proven that if you are given a quantum system in an unknown superposition state, there is no way to copy this state without destroying the original state. This result is the **no-cloning theorem**:

The No-Cloning Theorem
It is impossible to copy an unknown quantum state.

The **uncertainty principle** implies that it is impossible to know everything about a quantum state; if we measure one property, we disturb the others.

The Uncertainty Principle
If we measure a quantum system, we disturb it.

Since we disturb the system when we measure it, and we cannot make a copy of the system, we cannot learn anything about a quantum system without disturbing it in some way.

In this activity, we'll investigate how we can use this fact to create unbreakable information security tools. Using quantum mechanics to protect information is known as **quantum cryptography**, and the protocol we'll study here is called **Quantum Key Distribution**.

CRYPTOGRAPHY: THE SCIENCE OF SECRETS

When you send private information over the internet, such as emails, your banking information, or torrid love letters, the information is **encrypted** in such a way that only the sender and the receiver can access that information, and any malicious eavesdropper is unable to decrypt that information in a reasonable amount of time.

While using the internet as a communication channel, we encrypt information with security protocols based on mathematical problems that are very hard to do in reverse. This is known as **computational cryptography.** For example, it is very easy to multiply two numbers together, and a computer can do it quickly even for very large numbers. But finding the factors of a large number is very difficult, even for a supercomputer.

The most used computational crypto-protocol is known as RSA. Attempting to break the RSA protocol would take thousands, even millions, of years for the most powerful supercomputer running the best-known algorithm. Although safe in practice, computational cryptography is vulnerable to advances in algorithms and breakthroughs in computing, such as the development of the quantum computer. In fact, we already know how to break most crypto-protocols in use today if we had a quantum computer, and none of the other computational-based protocols are proven to be secure against a quantum attack.

However, there are protocols not based on computational complexity that are known to be secure against any potential attack. The most well-known is the **one-time pad**, also known as the **Vernam Cipher.**

THE ONE-TIME PAD

In practice, information is stored, manipulated and communicated in strings of bits (series of 0's and 1's). For example, using the ASCII encoding, we write the word "hi" as:

"hi" = 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 1

In the one-time pad protocol, we assume that the sender (Alice) and the receiver (Bob) share two **completely random, but identical and secret** strings of bits that are at least as long as the message. Each string is known as the **key.** The protocol goes as follows:

1. Alice generates a cipher text by adding the key to her message bit-by-bit ("bitwise").
   She adds the first bit of the message with the first bit of the key, then adds the second bit of message with the second bit of the key, and so on.
   When adding bitwise, we skip the remainder, so: 0+0=0, 0+1=1+0=1 and 1+1=0.

2. Alice sends the cipher text to Bob.

3. Bob retrieves the original message by adding his key to the cipher text bit-by-bit.

Let’s now put that protocol into practice:

1. Suppose Alice and Bob share the 16-bit key below and Alice wants to secretly send the number “**42**” to Bob, which is “101010” in binary. Ahead of time, the shared the secret key “100111”. Fill in the table below:

	Alice		Bob	
Message	101010		001101	Cipher
Key	100111		100111	Key
Cipher	001101		101010	Message

2. Explain why Bob can retrieve the message by adding the key again.

Adding the key once scrambles the message, and adding the same key again unscrambles it. In bitwise addition, 1+1=0, so x+1+1=x+0=x for any value of x.

3. If an eavesdropper (let’s call them Eve) manages to intercept the cipher, would they be able to recover the original message?

They could only recover the message if they also have the key.

4. If the eavesdropper does not know the key, what is the probability that they successfully guess it at random? What if the key was twice or three times as long?

Each bit has two possible options, 0 or 1. For six bits, there are 2*2*2*2*2*2 = 2^6 = 64 possibilities. The probability of randomly guessing the correct key is then 1 in 64.

If they message and key were twice as long (12 bits), there would be 2^{12} = 4096 possibilities. If they were three times as long (18 bits), there would be 262,144 possibilities. This is an example of exponential growth.

5. Suppose Alice sends an encrypted five-letter word to Bob, and by chance Eve finds a key that decrypts the message to “Hello”. Can Eve know for sure that Alice was sending that word? What other possible words could Alice have sent?

Eve cannot be sure that “Hello” is the correct decryption. Because the key and the message are the same length, any five-letter word could be decrypted from the scrambled cipher text. Even if Eve tries every possible key, they will be left with multiple possible decryptions and no way to tell which message was actually intended.

6. Although unbreakable, the one-time pad is not commonly used due to impracticality. What assumption made in the protocol makes it impractical in the real world?

We assumed that Alice and Bob share the key in the first place, which must be done in such a way that Eve cannot steal it.

QUANTUM KEY DISTRIBUTION (QKD)

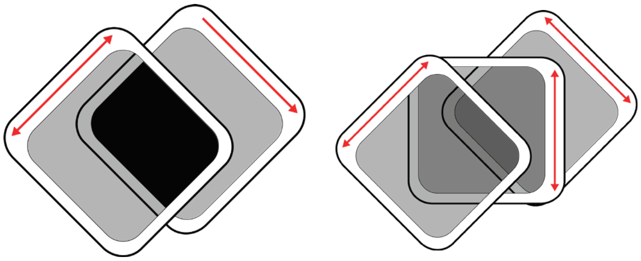
The one-time pad is a perfectly secure way for Alice and Bob to communicate a secret message. Think of the cipher like a locked safe that holds the message. An eavesdropper can intercept the safe, but without the key, they have no way of opening it to reveal the message.

As long as Alice and Bob keep their shared key perfectly secret, there is no way for an eavesdropper to learn the message. But how do Alice and Bob share the key in the first place?

> Note that sharing the **key** is different than sharing a **message**.
> The key is a completely random binary sequence, and contains no useful information itself.
> But if Alice and Bob share the same random sequence, they can use it to encrypt secret messages!

Quantum key distribution (QKD) uses quantum mechanics to solve the problem of establishing the secret key securely. Alice and Bob will exchange qubits to build a random sequence of bits in such a way that any attempts by an eavesdropper to tamper with the key exchange will be noticed.

If you completed the Two Golden Rules activity, you already know the basic physics! Recall that when we inserted a polarizer between two crossed polarizers, we were able to see through the complete set. By introducing a **measurement**, we affected the overall system. QKD uses this exact phenomenon to detect the presence of an eavesdropper.

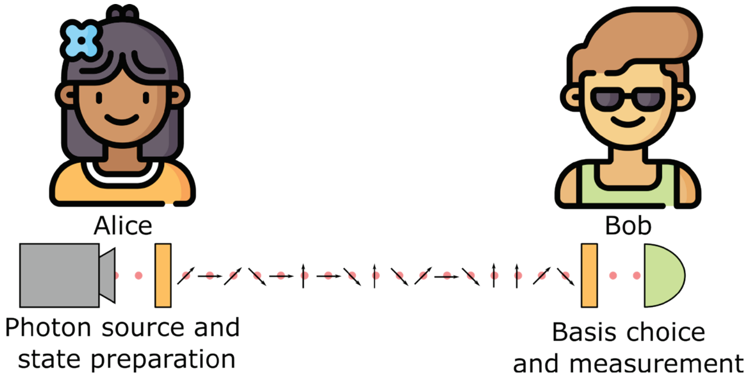


In the three-polarizer phenomenon, light can be seen through two crossed polarizers if a third is introduced in between.

The earliest QKD protocol is known as the **BB84 Protocol**, proposed in 1984 by Charles Bennett of IBM and Gilles Brassard of the Université de Montréal. In QKD, each bit of the secret key is built by having Alice send a **random** polarization-encoded qubit to Bob, who measures it.

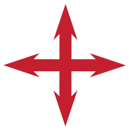
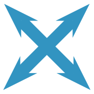
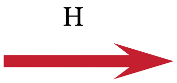
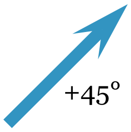
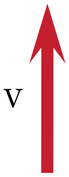
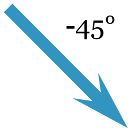
In each round of QKD, Alice will send Bob a single photon randomly chosen to be in one of four different polarization states: horizontal, vertical, +45°, or -45°. The horizontal and vertical states together form the **HV basis** and the ±45° states form the **±45° basis**.

On his side, Bob will randomly choose a **measurement** to make: either an **HV basis** measurement (distinguishing the horizontal and vertical states) or a **±45° basis** measurement (distinguishing the ±45° states).


Alice
Bob
Photon source and state preparation
Basis choice and measurement

In the BB84 QKD protocol, Alice prepares a single photon in a random polarization state and sends it to Bob, who measures it in a random basis. The orange plates represent polarization controllers.

Alice and Bob agree on the following bit-to-qubit correspondence, with two possible ways of representing each bit depending on the basis chosen.

	 HV Basis	 ±45° Basis
0		
1		

1. If Alice sends the bit "0" in the HV basis, what photon state does she need to prepare?

   In the HV basis, Alice would send a horizontal photon to send the bit "0".

2. If Bob performs a measurement in the HV basis on that photon, what state will he measure? Which bit value will he record?

   He is measuring a horizontal photon in the HV basis, so he will measure "H" and record "0".

3. If Bob instead measured in the ±45° basis, what state will he measure? What bit value?

   Measuring a horizontal photon in the ±45° basis results in a 50% chance of measuring +45°, and a 50% chance of measuring -45°. Either result is equally likely, and Bob has a 50/50 probability of recording either "0" or "1".

4. What is the condition needed for Alice and Bob to reliably agree on the bit recorded?

   Alice and Bob always agree on the bit value if they use the same basis to prepare/measure the photons. If they disagree on the basis, then their bits may or may not agree, with a 50% probability.

Below is a table showing the relationship between Alice's preparation and Bob's measurement:

State Preparation (Alice)	HV Basis Measurement Result (Bob)	±45° Basis Measurement Result (Bob)
H	H	Random
V	V	Random
+45°	Random	+45°
-45°	Random	-45°

BB84 – THE QUANTUM EXCHANGE

The BB84 QKD protocol has two parts: the quantum part where Alice and Bob exchange qubits, and a classical part where Alice and Bob process their data. The quantum exchange is accomplished step-by-step as:

Quantum exchange

1. Alice chooses at random the bit value to send to Bob.
2. Alice chooses at random the basis she'll prepare the photon state corresponding to that bit.
3. Alice prepares the photon in that specific state and sends it to Bob.
4. Before receiving the photon, Bob chooses at random which basis he'll measure the photon in.
5. Bob measures the photon in his chosen basis.
6. Bob records the bit corresponding to the photon state he just measured.
7. Repeat steps 1-6 as many times as needed.

1. Use **QKD Worksheet #1** and fill in the blanks. If you suspect Bob's result will be random, denote it using the letter "R".

2. Discuss in which cases Alice and Bob will share the same bit with 100% certainty. How could they learn whether they agree or not without revealing the bit being sent?

   Alice and Bob agree with certainty when Alice encodes her qubit in the same basis that Bob measures in. If they reveal to each other which basis they used, without revealing the exact state/bit being sent, they could filter out cases where they disagree.

3. If Alice and Bob exchanged a string of 1 million bits this way, approximately how many corresponding pairs of bits will Alice and Bob agree on the answer to?

   Statistically, they'd expect an average of 500,000 out of 1,000,000 bits to agree.

BB84 – CLASSICAL PROCESSING

When Alice and Bob don't agree on the basis, their bits have only a 50% chance of agreeing. However, whenever Alice and Bob use the same basis, they share the exact same bit value 100% of the time. In **classical post-processing**, Alice and Bob filter out the cases where they choose different bases, leaving them with a sequence of random bits that they both agree on 100% of the time.

After the quantum part, there is no need for secrecy anymore. Alice and Bob communicate on **public channels** like the internet for the rest of the protocol, meaning that an eavesdropper could listen in. The first post-processing step is called **basis reconciliation**.

Post-processing: Basis reconciliation

8. For each bit, Alice tells Bob the basis she used **without revealing the actual bit value**.
9. Bob tells Alice to keep the bit if he measured in the same basis. If he measured in a different basis, Bob discards the bit and tells Alice to do the same.

The sequence of bits left is known as the **sifted key**. While the original sequence of bits had some random elements, every bit in Alice and Bob's sifted keys should agree with each other.

1. Return to **QKD Worksheet #1** and cross out each bit where Alice and Bob used different bases. Do their remaining bits agree with each other?

Yes, the sifted keys agree with each other and have no remaining random (R) bits.

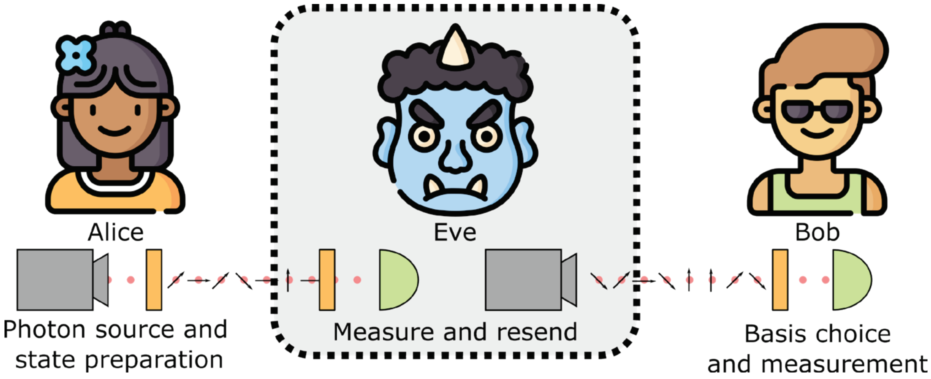
2. Why aren't Alice and Bob worried about Eve listening in on their basis reconciliation?

Because telling Eve the basis used doesn't give them any information about the bits. Alice and Bob will encrypt their information based on the bit values, not on the bases used.

WHAT ABOUT EVE?

For an eavesdropper (Eve) to learn Alice and Bob's secret key, they need to listen in to the quantum part of the exchange. When studying security, we assume that Eve is infinitely powerful, with access to unlimited computer power and the ability to tap into any communication channel. But, like the rest of the universe, Eve has to obey the laws of quantum physics.

As Alice prepares her photons one-at-a-time and at random, Eve only gets one chance to measure the photon from Alice on its way to Bob. Due to the no-cloning theorem, Eve cannot make a copy of the polarization state. Eve's only chance is to **measure** the photon and resend a new photon with the same state to Bob. But what basis should Eve measure in, and what happens if they choose the wrong one?


Alice
Eve
Bob
Photon source and state preparation
Measure and resend
Basis choice and measurement

Eve must intercept during the quantum part. Since they cannot make a copy, they must measure and resend the polarization-encoded photon.

1. Fill in **QKD Worksheet #2**, which is the same as #1 but with Eve in the middle. If you suspect Eve's result will be random, denote it with an "R".

2. Go through basis reconciliation on **QKD Worksheet #2** between Alice and Bob. Do Alice and Bob share the same sifted key?

   While there is a small chance that they do, it is unlikely given the new random elements.

3. In what circumstances does Eve introduce an error? When do they not?

   Eve introduces an error when their basis is different than Alice and Bob's.

4. How often will Eve get lucky and eavesdrop without introducing an error?

   75% of the time; 50% of the time they guess the right basis, and when the guess the wrong basis they only introduce an error with 50% probability. (0.5*0.5) = 0.25 probability that they introduce an error, and the other 75% of the time they get lucky.

5. What is the probability that Eve could eavesdrop on 10 bits and not introduce an error? 100 bits? What about on a 8,000 bit (1 kilobyte) secret key?

   $0.75^{10} \approx 5.6\%$ for 10 bits. $0.75^{100} \approx 3*10^{-13}$ for 100 bits.
   For 1kB, the probability is 0.75^{8000}, which is below calculator precision.

We just saw that, for large enough secret keys, Eve will unavoidably introduce errors in Alice and Bob's sifted key. To determine whether Eve is present or not, Alice and Bob need to take one more post-processing step:

Post-processing: Error estimation and eavesdropper detection

Alice and Bob randomly take a subset of the sifted key and compare it publicly.
For example, they could compare every third bit, or the first 100 bits.

If their shared bits are identical, Alice and Bob can be confident that no one was eavesdropping on their key exchange. They discard the bits they publicly shared, and can use the rest of the sifted key as a one-time pad for secret communication with a quantum security guarantee!

If there are errors, Alice and Bob have detected the presence of an eavesdropper, and have to discard the whole sifted key. This prevents them from exchanging secret information, but more importantly, keeps them from using an unsecure key to exchange information.

In practice, it is still possible to extract a shorter secret key if there are some errors in the key, due to a partially active eavesdropper or imperfections in the experiment. BB84 can tolerate an error rate of up to 11% and still provide Alice and Bob with a secret key.

1. Suppose Eve discovers that quantum mechanics is wrong and finds a way to clone the state of each photon. How could they use their quantum cloning machine to learn about the entire secret key without being detected?

   If Eve could make a copy of Alice's photon, they could hold on to their copy of the photon and wait until Alice and Bob announce their bases publicly before choosing the make a measurement. Alternative, Eve could make two copies and measure one in each basis, keeping only the results that agree with Alice or Bob's basis choices. Either strategy would give Eve an exact copy of the key. Thankfully for QKD, building such a device is not possible quantum mechanically.

THE IMPORTANCE OF BASES

If Alice sends a photon in the HV basis, and Bob measures in the HV basis, their results should always agree. But if Eve measures in the ±45° basis in the middle, something changes. Say Alice sent the horizontal “H” state. If Eve measures in the ±45° basis in the middle, that H-polarized photon must collapse to either +45° or -45°, randomly. Eve will send on a +45° or -45° photon to Bob, who measures it in the HV basis. But photon is now +45° or -45°; Eve’s measurement in the middle disturbed the information about the state in the HV basis.

This is the quantum uncertainty principle in action: **when we measure a photon’s state in one basis, we disturb its state in another basis.**

The HV and ±45° bases have the property that measuring the state prepared in one basis yields a completely random result (50%) in the other basis. The HV information is maximally disturbed if we measure it in the ±45° basis, and vice-versa. In this protocol, the use of two bases that are related to each other in the same way as HV and ±45° are is necessary in order to detect the presence of an eavesdropper.

We summarise Eve’s role in the two tables below. For simplicity, we greyed out the instances that don’t matter (these are results that will be thrown away in the basis reconciliation step).

If Eve and Bob measure in the same basis, Eve will not be detected (see cases 1 and 2 in table below).

	Case 1		Case 2	
State Preparation (Alice)	HV basis measurement result (Eve)	HV basis measurement result (Bob)	±45° basis measurement result (Bob)	±45° basis measurement result (Eve)
H	H	H		
V	V	V		
+45°			+45°	+45°
-45°			-45°	-45°

However, if Eve and Bob measure in different bases, Eve will randomise Bob’s result that would otherwise be definite (see cases 3 and 4 below, compare with the table without Eve in the middle).

	Case 3		Case 4	
State Preparation (Alice)	±45° basis measurement result (Eve)	HV basis measurement result (Bob)	HV basis measurement result (Bob)	±45° basis measurement result (Eve)
H	Random	Random		
V	Random	Random		
+45°			Random	Random
-45°			Random	Random

This leaves room for Eve to be detected in the error estimation step, following the basis reconciliation step.

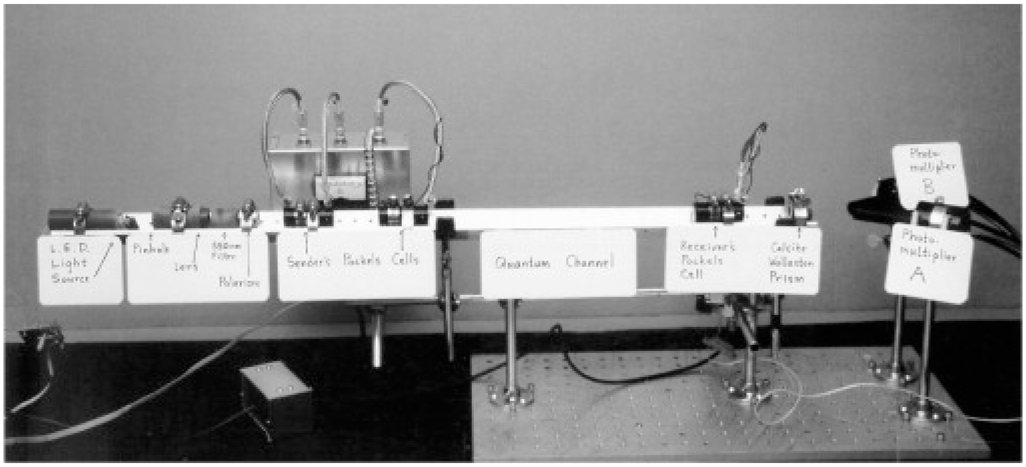
FURTHER EXPLORATIONS: REAL-WORLD QKD

In order to build QKD in the real world, we need tools to generate, transport, and measure photons one at a time. Early experiments, like the one seen at the bottom of the page, used a **weak laser beam** with an average photon number of less than one in each pulse. Nowadays, there are reliable tools based on **quantum dots** and **nonlinear optics** that can generate a single photon.

Transporting photons can be accomplished using **fibre-optic networks**, which guide light in wires made of glass and are common in the telecommunications industry. By using different wavelengths than telecommunications signals, it's possible to send single photons through fibre at the same time as bright telecom signals and separate them later on. Photons do eventually get lost in fibre though, limiting their use to distances of around 300 km. Researchers are working on testing satellite connections to link people around the world with QKD by sending photons to space, one at a time.

Photon detectors based on phenomenon like superconductivity, semiconductors, and the photoelectric effect can be used to measure the presence of an individual photon. We can encode qubits in the polarization states outlined above using polarization rotators called **wave plates** and polarization-dependent beam splitters to measure their state. There are other ways to encode information in a photon as well, including putting it in a superposition of different **times** or **colors.**

Other protocols beyond BB84 exist, sometimes providing more security through fewer assumptions. Some even take advantage of other quantum features like entanglement! The core idea behind all of them remains the same: in quantum mechanics, you can't measure something without disturbing it!



A 1992 experimental demonstration of BB84 QKD using faint polarized laser light, photomultiplier tubes, and polarization switches (Pockels cells).

Modern experiments have been performed over much greater distances, and the photons often travel through optical fibre networks.

Image: C.H. Bennett et al, Journal of Cryptology **5**, 3-28 (1992).

Answer Key

QUANTUM QUIZ

1. Alice and Bob wish to encrypt the message “QUANTUMBITS” securely using QKD. Each letter is represented by 8 bits in ASCII.
   - **a.** How many bits long is the message? How long must the secret key be to encrypt it?
     The message is 11 letters long, meaning 8*11=88 bits in ASCII.
     The secret key must be the same length, also 88 bits long.
   - **b.** On average, how many photons must Alice and Bob exchange in QKD to generate a secret key of that length? Assume they estimate their error by randomly selecting half of the bits to compare, and that they find no eavesdropper present.
     Alice and Bob will lose half of their bits due to basis reconciliation, and another half due to error estimation. Therefore, they will need to exchange approximately 88*2*2 = 352 photons to generate that key, at minimum.
   - **c.** What is the probability that the eavesdropper was present but not detected during the error estimation step?
     Alice and Bob checked for errors with 88 bits. Eve has a 75% probability per bit of not introducing an error, so the probability of not being detected in 88 bits is $(0.75)^{88} \approx 10^{-11}$, or one-in-ten-billion.

QUANTUM CONCEPTS

1. Quantum optics researchers often use devices that convert one horizontally polarized photon into two horizontally polarized photons. However, they do not violate the no-cloning theorem. How is this possible?
   The no-cloning theorem rules out devices that copy **unknown** polarization states. Devices that copy **known** polarization states are possible. An eavesdropper could not build a device that copies all four BB84 states accurately unless they knew in advance which state to expect.

2. Alice and Bob, in an effort to speed their key exchange up, decide to agree on which bases to use ahead of time by publicly announcing them. Why is this not secure?
   Since Eve only introduces an error when their basis choice doesn’t match Alice and Bob’s, it is important that Alice and Bob choose random bases during every round of QKD. Otherwise, Eve can predict which basis each photon will be sent/measured in and match their basis choice accordingly.

3. Is QKD still secure if Alice sends a small laser burst of approximately 10 photons instead of one single photon at a time? What might Eve be able to do here instead?
   QKD with multiple photons is not secure, as Eve could pick off one or two of the photons from the burst and read their state without disturbing the polarization state Bob receives.

QUANTUM LEAP: CHALLENGE QUESTION

1. Why would QKD be less secure if, instead of the HV and ±45° bases, Alice and Bob used the HV and +15° / -75° bases?
   This would be less secure as, if Eve chooses the wrong basis, she would still get some partial information. For example, if Eve measures in the HV basis but Alice sent +15° instead, there is a much larger probability of Eve measuring H than V ($\cos^2 15°$ vs. $\sin^2 15°$). If Eve learns later on that Alice sent either H or V, they can guess that Alice probably sent H rather than V.

   Compare this to the ±45° case, where if Eve later learns that Alice sent either H or V, Eve’s measurement of +45° does not give them any information about what Alice might have sent, since both H and V have the same statistics in the ±45° basis.

GLOSSARY

- The **No-Cloning Theorem** states that it is impossible to clone the information encoded in a quantum state. For example, it is impossible to create a machine that receives one photon with an unknown polarization and creates two photons with the same polarization as the first. It was first explicitly proven by Wootters and Zurek in 1982.
- The **one-time pad** or **Vernam cipher** is secure method of communication between two parties, who use a secret key to encrypt a message that can only be decrypted by someone with the same key. It is inefficient, in that the key must be as long as the message, and often impractical as the two parties must share a secret key securely in advance.
- **Bitwise addition** (also known as **XOR** or **addition-mod-two**) is a way to process two binary numbers. It can be thought of as addition, but disregarding the carryover in binary. It can also be thought of as an equality check, which returns "0" if the bits are the same and "1" if the bits are different. In bitwise addition, 0+0=0, 0+1=1, 1+0=1, and 1+1=0.
- **Alice and Bob** are the traditional names given by cryptographers to two people communicating with each other. The eavesdropper, who tries to listen in on their secrets, is usually called **Eve**.
- A **secret key** is a sequence of bits shared between Alice and Bob, which Alice uses to encrypt or "lock" a message. Only Bob, who has a copy of the key, can decrypt or "unlock" the message.
- The **cipher text** or simply **cipher** is the sequence of bits corresponding to the message after encryption with the key. The cipher text is meaningless to anyone who doesn't have the right key to decrypt it.
- **Quantum key distribution (QKD)** is a quantum technique to distribute secret keys between a distant Alice and Bob. All QKD protocols rely on the no-cloning theorem and the impossibility of measuring in two different bases at the same time.
- **BB84** is a specific QKD protocol proposed by Charles Bennett and Gilles Brassard in 1984, which uses photons encoded in and measured in one of two possible bases.
- **Basis reconciliation** is the part of BB84 where Alice and Bob publicly announce their bases, to remove any potential randomness from their shared binary sequence.

Written by Martin Laforest
Published by the **IQC Scientific Outreach team**
Contact: iqc-outreach@uwaterloo.ca

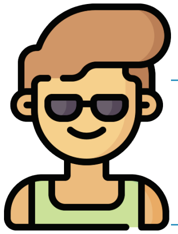
Institute for Quantum Computing
University of Waterloo
200 University Ave. W.
Waterloo, ON, Canada, N2L3G1

About IQC
The Institute for Quantum Computing (IQC) is a world-leading research centre in quantum information science and technology at the University of Waterloo. IQC's mission is to develop and advance quantum information science and technology through interdisciplinary collaboration at the highest international level. Enabled by IQC's unique infrastructure, the world's top experimentalists and theorists are making powerful new advances in fields spanning quantum computing, communications, sensors and materials. IQC's award-winning outreach opportunities foster scientific curiosity and discovery among students, teachers and the community.

uwaterloo.ca/institute-for-quantum-computing

QKD WORKSHEET #1

Alice


Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	0	1	1	1	0	0	1	0	1	0	1	0	0	1
2.	+	+	×	+	×	+	×	×	+	×	×	+	×	+
3.	→	↑	↘	↑	↗	→	↘	↗	↑	↗	↘	→	↗	↑
4.	+	×	×	+	+	+	×	+	×	×	+	+	×	×
5.	→	R	↘	↑	R	→	↘	R	R	↗	R	→	↗	R
6.	0	R	1	1	R	0	1	R	R	0	R	0	0	R

Schrödinger's Class

UNIVERSITY OF WATERLOO

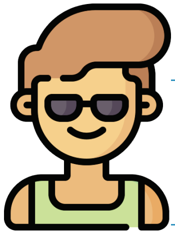
IQC Institute for Quantum Computing

Answer Key

QKD WORKSHEET #2

Alice

Eve



Bob

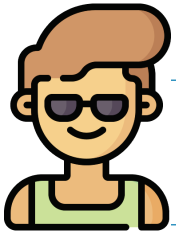
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Alice	1.	0	1	1	1	0	0	1	0	1	0	1	0	0	1
	2.	+	+	×	+	×	+	×	×	+	×	×	+	×	+
	3.	→	↑	↘	↑	↗	→	↘	↗	↑	↗	↘	→	↗	↑
Eve		×	×	+	+	×	+	+	×	+	×	×	+	+	+
		R	R	R	↑	↗	→	R	↗	↑	↗	↘	→	R	↑
Bob	4.	+	×	×	+	+	+	×	+	×	×	+	+	×	×
	5.	R	R	R	↑	R	→	R	R	R	↗	R	→	R	R
	6.	R	R	R	1	R	0	R	R	R	0	R	0	R	R

Answer Key

QKD WORKSHEET #1

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	0	1	1	1	0	0	1	0	1	0	1	0	0	1
2.	+	+	×	+	×	+	×	×	+	×	×	+	×	+
3.	→	↑	↘											
4.	+	×	×	+	+	+	×	+	×	×	+	+	×	×
5.	→	R												
6.	0	R												



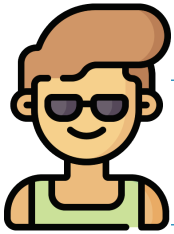
Bob

SC Schrödinger's Class

UNIVERSITY OF WATERLOO

IQC Institute for Quantum Computing

QKD WORKSHEET #2



		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Alice	1.	0	1	1	1	0	0	1	0	1	0	1	0	0	1
	2.	+	+	×	+	×	+	×	×	+	×	×	+	×	+
	3.	→	↑	↘											
Eve		×	×	+	+	×	+	+	×	+	×	×	+	+	+
		R	R												
Bob	4.	+	×	×	+	+	+	×	+	×	×	+	+	×	×
	5.	R													
	6.	R													

SC Schrödinger's Class
UNIVERSITY OF WATERLOO
IQC Institute for Quantum Computing