*Activity*

# BB84: QUANTUM COINS VIRTUAL VERSION

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**

Copyright © 2021 University of Waterloo

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

SC Schrödinger's Class

*Outline*

# BB84: QUANTUM COINS

**ACTIVITY GOAL:**
Simulate the quantum key distribution protocol through role-playing.

## LEARNING OBJECTIVES

- Measurement disturbance.
- Cryptography and the one-time pad.
- The BB84 quantum key distribution protocol.

## ACTIVITY OUTLINE

In this **virtual** activity, we'll simulate the BB84 quantum key distribution protocol using coins and chat windows. Groups of four (at minimum) will take on the roles of Alice, Bob, Eve, and quantum nature itself.

Alice will encode information in one basis, which they will then send to Bob. Eve gets an opportunity to measure the system, which may disturb Alice's encoding. Bob then measures the bit. Alice and Bob post-process their data to either generate a secret key or detect the presence of an eavesdropper.

They must communicate indirectly through a moderator who enforces quantum mechanics at every step.

**CONCEPT**:
If an eavesdropper measures a quantum system, they will disturb the quantum state and can be detected.

## PREREQUISITE KNOWLEDGE

The **quantum cryptography** lesson

## SUPPLIES REQUIRED

One coin per person
Alice, Bob, Eve, and Moderator worksheets
Groups of at four students each
Private and public chat features

*Activity*

# BB84: QUANTUM COINS (VIRTUAL)

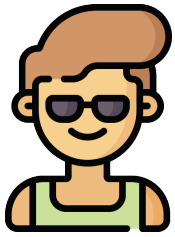
## THE SET-UP

In this activity, you're going to demonstrate the basic ideas of the BB84 protocol for Quantum Key Distribution (QKD). Acting as Alice and Bob, you'll attempt to establish a secret key and test for the presence of an eavesdropper.

First, split your group into four. The overall group should have a **public channel**, where every member can see the communication. Alice, Bob, and Eve should also all have a **private channel** for communicating with the moderator.

**Alice**

Sends qubits

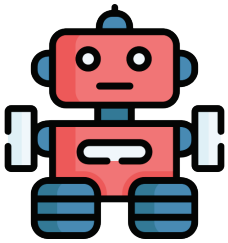


**Bob**

Measures qubits

**Eve**

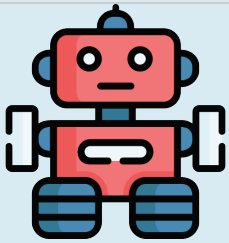
Interrupts qubits



**Moderator**

Enforces quantum mechanics

**Eve**



**Moderator**

First, Eve must choose a strategy. Will they look at every bit, every other bit, or none at all? Your teacher may provide you with a strategy, or you may choose your own.

Eve should secretly tell the moderator their strategy so that they can communicate quietly about Eve's decisions during the key exchange.

## THE PROTOCOL

To build the secret key, Alice, Bob, Eve, and moderator should repeat the following steps, filling out their tables as they go. Alice, Eve, and Bob should try to complete their tasks quietly, so that the others don't overhear their bits and basis choices.

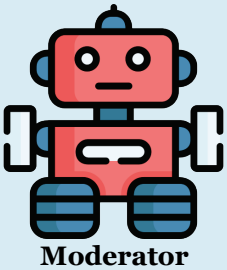
**Alice**

Alice tosses her first coin, which tells her which bit to encode in her qubit.
If it lands heads, encode "0". If it lands tails, encode "1".

Alice's second coin tells her which **basis** to encode her qubit in.
If it lands heads, encode in HV. If it lands tails, encode in ±45°.

| Toss | Bit | Basis | State |
|---|---|---|---|
| H, H | 0 | HV | H |
| H, T | 0 | ±45° | +45° |
| T, H | 1 | HV | V |
| T, T | 1 | ±45° | -45° |

Write down your bit and basis on your worksheet, and tell the **moderator** your state (both the bit and the basis).



**Moderator**

Depending on the information that Alice provides, mark your worksheet as below.

| Bit | Basis | HV box | ±45° box |
|---|---|---|---|
| 0 | HV | 0 | X |
| 0 | ±45° | X | 0 |
| 1 | HV | 1 | X |
| 1 | ±45° | X | 0 |

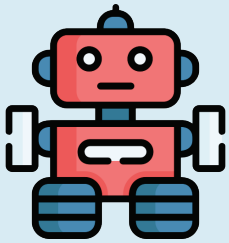
Next, give Eve the option to measure in one (and only one!) of the bases.

**Eve**

Eve chooses to make a measurement or not.

If Eve makes a measurement, they must tell the **moderator** which basis they measure in.

If Eve choose to not make a measurement, pretend to so Alice and Bob remain suspicious by messaging the **moderator** that they aren't looking.



**Moderator**

If Eve **made a measurement in the same basis as Alice**, tell Eve Alice's bit value and copy the information from Alice's column under Eve's. For example, if Alice prepared the state "H" and Eve measured in the HV basis:

| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | 0 | >> | |
| 45° | X | >> | X | >> | |

If Eve **made a measurement in a different basis than Alice**, flip a coin and tell Eve the random bit value. In the Eve column, write that bit value in their chosen basis and put an "X" in the other basis, overwriting Alice's bit. For example, if Alice prepared the state "H" and Eve measured in the ±45° basis:

| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | X | >> | |
| 45° | X | >> | 0 or 1 | >> | |

In the above case, the choice of "0" or "1" depends on the moderator's coin flip (0 if heads, 1 if tails).

If Eve **did not make a measurement**, write the same values under Eve as under Alice and tell Eve nothing.

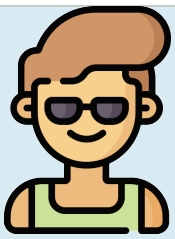
| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | 0 | >> | |
| 45° | X | >> | X | >> | |

**Eve**

If you made a measurement, write down the basis chosen and the bit the moderator tells you on your worksheet.

The moderator is playing the role of quantum mechanics in this simulation. By randomizing the bit when Eve measures in the wrong basis, they're simulating the disturbance caused by Eve's measurement!

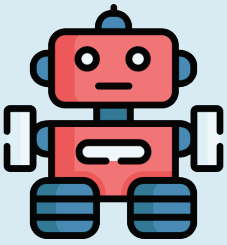
Next is Bob's turn to make a measurement.



**Bob**

Bob flips a coin to choose which **basis** to measure in.
If heads, measure in the HV basis. If tails, measure in the ±45° basis.

Write down the bit value and which box you chose on the worksheet.



**Moderator**

If Bob **made a measurement in the same basis as Eve** (or Alice if Eve made no measurement), tell Bob the bit in Eve's column and copy the information into Bob's column in your worksheet. For example, if everyone has used the HV basis, the sheet may look as below:

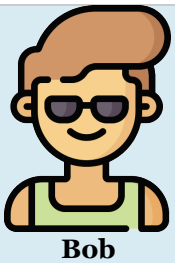
| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | 0 | >> | 0 |
| 45° | X | >> | X | >> | X |

If Bob **made a measurement in a different basis than Eve** (or Alice if Eve made no measurement), flip a coin and tell Bob the random bit value. In the Bob column, write that bit value in their chosen basis and put an "X" in the other basis, overwriting Alice's bit. For example, if Alice prepared the state "H" and Eve measured in the HV basis, but Bob measured in the ±45° basis:

| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | 0 | >> | X |
| 45° | X | >> | X | >> | 0 or 1 |

In the below example, Alice and Bob both used the HV basis, but Eve measured in the ±45° basis:

| | Alice | | Eve | | Bob |
|---|---|---|---|---|---|
| HV | 0 | >> | X | >> | 0 or 1 |
| 45° | X | >> | 0 or 1 | >> | X |



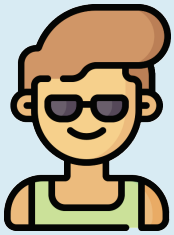
**Bob**

Write down the bit value and which basis you chose on the worksheet.

**Repeat** up to fifty times to build a secret key!

## POST-PROCESSING

**Alice**



**Bob**

**Basis reconciliation**

Once all "photons" have been exchanged, Alice announces loudly the basis she used for each step, being careful not to reveal the bit.

For each basis announced, Bob will say "keep" if he measured in the same basis, and "discard" if he measured in a different basis.

Alice, Bob, and Eve will keep the bits they measured if Alice and Bob's measurements agree, and cross out the bits where Alice and Bob disagreed.

The bits that remain are the sifted key! Alice and Bob should write it out separately.

**Error estimation and eavesdropper detection**

Alice and Bob publicly compare one third of the bits from their sifted key, chosen at random (for example, every third bit).

If all of these bits are the same, they can conclude that the eavesdropper was not listening in. They discard the bits they compared publicly and use the rest as their **secret key** to encrypt a message (try sending a binary number perhaps).

If those bits have errors, they can conclude that Eve was listening in! Their secret key isn't so secret after all.

## QUANTUM CONCEPTS

1. In quantum mechanics, why can't we measure in two bases at the same time?
2. Eve was allowed to freely choose which basis to measure in, but Alice and Bob had to choose randomly. What could Eve have done if they knew which basis Alice and Bob would choose?

Written by Martin Laforest and John Donohue
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

Copyright © 2021 University of Waterloo

**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

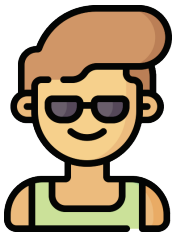
# Worksheet (Alice)

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 26 | | | |
| 27 | | | |
| 28 | | | |
| 29 | | | |
| 30 | | | |
| 31 | | | |
| 32 | | | |
| 33 | | | |
| 34 | | | |
| 35 | | | |
| 36 | | | |
| 37 | | | |
| 38 | | | |
| 39 | | | |
| 40 | | | |
| 41 | | | |
| 42 | | | |
| 43 | | | |
| 44 | | | |
| 45 | | | |
| 46 | | | |
| 47 | | | |
| 48 | | | |
| 49 | | | |
| 50 | | | |

**Sifted Key:** _____

**Secret Key:** _____



# Worksheet (Bob)

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 26 | | | |
| 27 | | | |
| 28 | | | |
| 29 | | | |
| 30 | | | |
| 31 | | | |
| 32 | | | |
| 33 | | | |
| 34 | | | |
| 35 | | | |
| 36 | | | |
| 37 | | | |
| 38 | | | |
| 39 | | | |
| 40 | | | |
| 41 | | | |
| 42 | | | |
| 43 | | | |
| 44 | | | |
| 45 | | | |
| 46 | | | |
| 47 | | | |
| 48 | | | |
| 49 | | | |
| 50 | | | |

**Sifted Key:** _____

**Secret Key:** _____

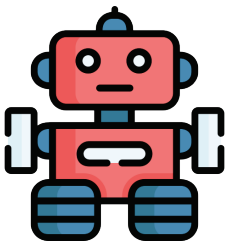
# Worksheet (Eve)

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |

| | Communication | | Post-processing |
|---|---|---|---|
| | Raw key | | |
| | Bit (0, 1) | Basis (H/V, ±45°) | Keep bit? |
| 26 | | | |
| 27 | | | |
| 28 | | | |
| 29 | | | |
| 30 | | | |
| 31 | | | |
| 32 | | | |
| 33 | | | |
| 34 | | | |
| 35 | | | |
| 36 | | | |
| 37 | | | |
| 38 | | | |
| 39 | | | |
| 40 | | | |
| 41 | | | |
| 42 | | | |
| 43 | | | |
| 44 | | | |
| 45 | | | |
| 46 | | | |
| 47 | | | |
| 48 | | | |
| 49 | | | |
| 50 | | | |

**Sifted Key:** _____

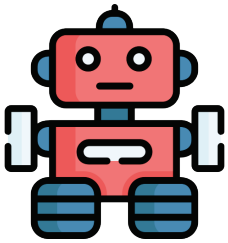
**Secret Key:** _____



# Worksheet (Moderator p. 1)

| | | Alice | | Eve | | Bob |
|---|---|---|---|---|---|---|
| 1 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 2 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 3 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 4 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 5 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 6 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 7 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 8 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 9 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 10 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 11 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 12 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 13 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |

| | | Alice | | Eve | | Bob |
|---|---|---|---|---|---|---|
| 14 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 15 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 16 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 17 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 18 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 19 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 20 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 21 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 22 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 23 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 24 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 25 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |



## Worksheet (Moderator p. 2)

| | | Alice | | Eve | | Bob |
|---|---|---|---|---|---|---|
| 26 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 27 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 28 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 29 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 30 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 31 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 32 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 33 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 34 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 35 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 36 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 37 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 38 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |

| | | Alice | | Eve | | Bob |
|---|---|---|---|---|---|---|
| 39 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 40 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 41 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 42 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 43 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 44 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 45 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 46 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 47 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 48 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 49 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |
| 50 | HV | | >> | | >> | |
| | 45° | | >> | | >> | |