

Activity

BB84: QUANTUM COINS

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



Institute for
Quantum
Computing



**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 hands-on activity, we'll simulate the BB84 quantum key distribution protocol using coins and boxes. 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.

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

Five coins
Two boxes labelled "HV" and " $\pm 45^\circ$ "
Alice, Bob, and Eve worksheets
Groups of at least four students each



Activity

BB84: Quantum Coins

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.

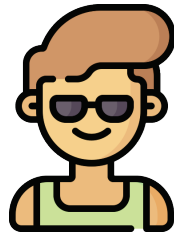
First, split your group into four teams:



Alice

Sends qubits

Starts with
three coins
and two boxes



Bob

Measures qubits

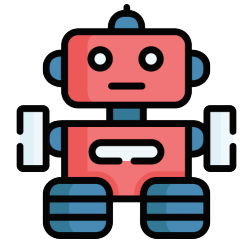
Starts with
one coin



Eve

Interrupts qubits

Starts with
one coin



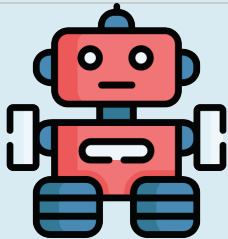
Moderator

Enforces quantum
mechanics



Eve

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.




Moderator

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 $\pm 45^\circ$.

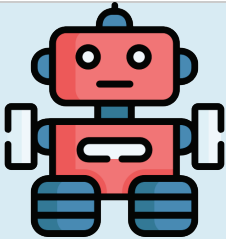
Alice then encodes her bit in the appropriate box gently with the first coin, and randomly shakes the second coin in other box.

Toss	Bit	Basis	HV box	$\pm 45^\circ$ box
H, H	0	HV	Place coin heads-up	Place coin inside and shake to randomize
H, T	0	$\pm 45^\circ$	Place coin inside and shake to randomize	Place coin heads-up
T, H	1	HV	Place coin tails-up	Place coin inside and shake to randomize
T, T	1	$\pm 45^\circ$	Place coin inside and shake to randomize	Place coin tails-up

Write down your bit and basis on your worksheet.

Both boxes together represent a single photon. Each box individually represents a different possible measurement that could be made by Bob or Eve.

Shaking the box that is **not** used by Alice mimics the quantum uncertainty principle – since Alice knows exactly what the result is in one box / measurement, the result of the other must be completely random.




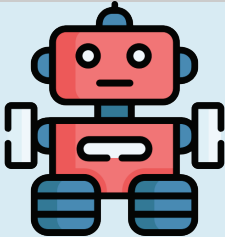
Moderator

Take both boxes **gently** to Eve, making sure that neither Eve nor Bob sees which box Alice shook up.


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



 <p>Eve</p>	<p>Eve chooses to open one box or neither box. If they wish, they may use their coin to help make their decisions random.</p> <p>If Eve opens a box, write down the bit you see (heads = 0, tails = 1) and which box you opened.</p> <p>If Eve choose to not open a box, pretend to so Alice and Bob remain suspicious, and write down an “X” to indicate a missed bit.</p>
---	--

 <p>Moderator</p>	<p>If Eve opened a box, shake the box that Eve did not open to randomize it.</p> <p>If Eve did nothing, do not shake either box.</p> <p>Take both boxes gently to Bob, giving him the open to look in one box of his choosing. Do not let Bob look in the second box!</p>
---	--

The moderator is playing the role of quantum mechanics in this simulation. By shaking the box, they’re simulating the disturbance caused by Eve’s measurement!

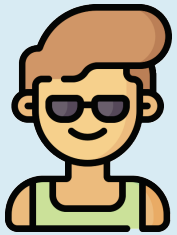
 <p>Bob</p>	<p>Bob flips a coin to choose which basis to measure in. If heads, open the HV box. If tails, open the $\pm 45^\circ$ box.</p> <p>Write down the bit value and which box you chose on the worksheet.</p>
--	--

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 (open both boxes) at the same time?
2. Eve was allowed to freely choose which box/basis to measure in, but Alice and Bob had to choose randomly. What could Eve have done if they knew which basis/box Alice and Bob would choose?

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

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)

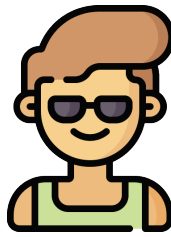
	Communication		Post-processing
	Raw key		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

	Communication		Post-processing
	Raw key		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
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		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
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		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
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		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
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		Keep bit?
	Bit (0, 1)	Basis (H/V, $\pm 45^\circ$)	
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: _____