BB84: Build and Compare a Sifted Key

Student quick-start guide

In this activity, Alice prepares quantum states, Bob measures them, and Eve may intercept them. The goal is to create a shared sequence of bits and observe whether the quantum channel was disturbed.

1. USE ONE SET OF NAMES

Basis	Raw bit 0	Raw bit 1	State names	Classroom tokens
Z basis (computational / bit)	0	1	$\|0\rangle$ and $\|1\rangle$	↑ and ↓
X basis (Hadamard)	0	1	$\|+\rangle$ and $\|-\rangle$	← and →

The arrows are classroom symbols for the four possible states. In a real protocol, nobody can simply look at an unknown quantum state and read its arrow.

2. APPLY THE MEASUREMENT RULE

SAME BASIS

The outcome is certain. Bob records the bit Alice encoded.

DIFFERENT BASIS

The outcome is random. Flip a coin: heads = 0, tails = 1.

3. RUN THE PROTOCOL IN THIS ORDER

1. **Prepare** — Alice privately chooses 8 bases and 8 bits, then encodes 8 state tokens.
2. **Transmit** — Alice sends only the state tokens. With Eve: Alice → Eve → Bob.
3. **Measure** — Bob privately chooses 8 bases and records 8 outcomes.
4. **Sift** — Alice and Bob publicly reveal bases. Keep rounds where their bases match.
5. **Compare** — For this demonstration, reveal and compare every bit from the kept rounds.
6. **Observe** — Mark each kept round MATCH or MISMATCH. Any mismatch shows disturbance.

CLASSROOM DEMONSTRATION

Because this activity compares every sifted bit, it does not produce a secret key. Real BB84 reveals only a random sample and keeps the unrevealed bits secret.

Alice Worksheet

Keep private until each step says to reveal

ROLE: ALICE - sender

You prepare the states

1 Privately choose one basis for each round. Write Z or X.

Round	1	2	3	4	5	6	7	8
Alice basis								

2 Privately choose one raw bit for each round. Write 0 or 1.

Round	1	2	3	4	5	6	7	8
Alice bit								

3 Encode each basis-bit pair using the reference below. Record the resulting state token.

Z + 0	Z + 1	X + 0	X + 1
↑	↓	←	→

Round	1	2	3	4	5	6	7	8
State token								

4 Transmit only the 8 state tokens, in order. Do not reveal your bases or bits yet.

5 After Bob has measured all 8 states, publicly reveal your bases. Record Bob's bases below.

Round	1	2	3	4	5	6	7	8
Bob basis								

6 On the Classroom Comparison Sheet, mark KEEP only where your basis matches Bob's basis.

CLASSROOM COMPARISON

Read your bits from every KEEP round and compare them with Bob's outcomes. Write your sifted key here first: My sifted key: _____

Bob Worksheet

Keep private until each step says to reveal

ROLE: BOB - receiver

You choose how to measure

1 Before receiving any states, privately choose one measurement basis per round. Write Z or X.

Round	1	2	3	4	5	6	7	8
Bob basis								

2 Receive each state token from Alice - or from Eve, if Eve is playing. Record the token exactly as received.

Round	1	2	3	4	5	6	7	8
Received state								

3 Measure each state using your chosen basis. Use the rule below and record one outcome bit per round.

Received token	Matching basis	Outcome
↑ or ↓	Z	↑ = 0; ↓ = 1
← or →	X	← = 0; → = 1
Any token	Different basis	Flip a coin: heads = 0; tails = 1

Round	1	2	3	4	5	6	7	8
Bob outcome								

4 After all measurements are complete, publicly reveal your bases. Do not reveal outcomes yet.

5 Use the Classroom Comparison Sheet to sift the results and compare every kept bit.

WHY WRONG-BASE OUTCOMES ARE RANDOM

Measuring an X-basis state in Z, or a Z-basis state in X, gives 0 or 1 with equal probability. The measurement also changes the state to match the basis used.

My sifted key: _____

Eve Worksheet

Use only for the intercept-resend round

ROLE: EVE - interceptor

You intercept the quantum channel

1 Before Alice transmits, privately choose one measurement basis per round. Write Z or X.

Round	1	2	3	4	5	6	7	8
Eve basis								

2 Intercept Alice's 8 state tokens. Record each token; do not let Bob hear Alice directly.

Round	1	2	3	4	5	6	7	8
Alice token								

3 Measure each token using your chosen basis. Same-basis outcomes are certain; different-basis outcomes require a coin flip.

Round	1	2	3	4	5	6	7	8
Eve outcome								

4 Prepare a replacement state from your basis and your outcome. Use the encoding map, then send the new token to Bob.

Eve basis + outcome	Z + 0	Z + 1	X + 0	X + 1
Replacement token	↑	↓	←	→

Round	1	2	3	4	5	6	7	8
Token to Bob								

5 Listen to the public basis comparison. Do not speak or alter it. Circle rounds in which you happened to use Alice's basis.

EVE'S LIMIT

You cannot copy an unknown state and keep the original. Measuring in the wrong basis can change what Bob later receives - the disturbance Alice and Bob are testing for.

Compare the Sifted Key

Alice and Bob complete this together

First compare bases and mark KEEP or DROP. Then reveal and compare the bits from every KEEP round.

Round	1	2	3	4	5	6	7	8
Alice basis								
Bob basis								
KEEP or DROP								
Alice bit (KEEP only)								
Bob outcome (KEEP only)								
MATCH or MISMATCH								

HOW TO FINISH

1. Sift: Write KEEP where Alice and Bob used the same basis. Write DROP everywhere else.
2. Reveal: For every KEEP round, Alice reads her bit and Bob reads his outcome. Record both.
3. Compare: Mark each KEEP round MATCH or MISMATCH.
4. Interpret: Any mismatch shows that the transmission was disturbed by noise or possible eavesdropping.

RESULT

Kept rounds compared: _____ Matches: _____ Mismatches: _____

Disturbance observed? YES / NO (This demonstration leaves no secret key.)

Instructor Guide

Suggested timing: 20-25 minutes

LEARNING TARGETS

Students should be able to explain why basis agreement is required, why wrong-basis measurement is random, how intercept-resend introduces errors, and why bits revealed during comparison cannot remain secret.

RECOMMENDED CLASSROOM FLOW

Time	Activity	Instructor cue
2 min	Assign Alice and Bob; optionally Eve	Give each role only its own worksheet.
5 min	Run 1: no Eve	Alice sends directly to Bob. Their sifted bits should match.
3 min	Sift and compare	Compare every kept bit for this classroom demonstration.
5 min	Run 2: with Eve	Alice sends to Eve; Eve measures and resends to Bob.
3 min	Sift and compare again	Compare the observed error rate with Run 1.
5 min	Debrief	Connect the coin flips to incompatible quantum bases.

WHAT STUDENTS SHOULD OBSERVE

Without Eve, every sifted bit should match. With intercept-resend, Eve chooses the wrong basis about half the time; when Alice and Bob later keep a round, that disturbance produces a Bob-Alice mismatch about half of those disturbed rounds. Therefore, the idealized error rate among sifted bits is about 25% under a full intercept-resend attack.

SMALL-SAMPLE WARNING

Eight rounds make a fast demonstration, not a reliable statistical test. A run can show no detected mismatch by chance. Pool results across groups or repeat with 16-32 rounds.

DEBRIEF QUESTIONS

1. Why can Alice and Bob reveal their bases without revealing their bit values?
2. Where exactly does Eve introduce disturbance?
3. Why is this classroom sifted key no longer secret, and what does real BB84 reveal instead?
4. What real-world effects besides Eve could cause mismatches?
5. What additional classical-channel property does BB84 require? (Authentication.)