BB84

dljustice

January 28, 2026

1 Introduction

1.1 Definition

BB84 is the first Quantum Cryptography Protocol developed in 1984 by Charles Bennett and Gilles Brassard. It utilizes quantum superposition and the no-cloning theorem to distribute cryptography keys.

1.2 Basis

For this worksheet we will need to distinguish between measuring the quantum state $|\psi\rangle$ in the Bit-basis ($|0\rangle, |1\rangle$) and the Sign basis ($|+\rangle, |-\rangle$). Note: Bit and Sign basis are often call the Z and X basis of measurement.

$$\begin{array}{lll} \text{Bit-Basis} & |0\rangle = \uparrow & |1\rangle = \downarrow \\ \text{Sign-Basis} & |0\rangle = \leftarrow & |1\rangle = \rightarrow \end{array}$$

1.3 Measuring

Measuring a quantum state results in a classical value (0, 1) and a quantum state ($\uparrow, \downarrow, \leftarrow, \rightarrow$). When measuring the quantum state we must measure with respect to a Basis. Measuring the state in the same Basis it was prepared in will return the intended value and the same quantum state. Measuring the state in a different basis from which it was prepared will return a value at random. With a 50/50 probability either the value 0 or 1 will be returned and the quantum state will be altered to match the measured basis.

1.3.1 Example

State Preparation: We prepare the state $|0\rangle$ in the Sign-basis. The state is represented as $\leftarrow$.

Sign-Basis Measurement: We measure the $\leftarrow$ state in the Sign-basis. The output value is 0 and the resulting quantum state is $\leftarrow$.
Bit Basis Measurement: We measure the $\leftarrow$ state in the Bit-basis. The output value is 0 or 1 with a 50% probability and the resulting quantum state is $\uparrow$ or $\downarrow$ correspondingly.

1.4 Imagination

We are attempting to recreate a quantum protocol in a classical world. This is not possible, but with some imagination we can make it happen! Remember, anytime you are dealing with ARROWS you are dealing with quantum states which cannot be perfectly known as a human. So when you translate from VALUES to ARROWS, you are going from classical to quantum states. When you go from ARROWS to VALUES, that is a quantum to classical interface.

2 ALICE Himitsu

1. Randomly choose the SIGN (X) or BIT (Z) basis 8 times (Before speaking to BOB!) These BASIS will be used to prepare the quantum string.

BASIS

X	Z	X	X						

2. Randomly Choose 0 or 1 eight (8) times

VALUES

0	1	0	1						

3. Prepare the Quantum String by translating the bits into ARROW notation. Remember, this is now the quantum realm and a person would not be able to "see" the ARROW.

ARROWS

$\leftarrow$	$\downarrow$	$\leftarrow$	$\rightarrow$						

4. Tell BOB your ARROWS in order.

   NOTE: At this point you no longer have access to the quantum states. To represent this you can blackout the ARROWS above.

5. Wait for BOB to tell you the order of the BASIS in which he measured your states

BOB's BASIS

Z	Z	Z	X						

6. Cross out the columns for where BOB's BASIS do not match your own
7. Tell BOB which columns to cross out
8. Your Sift Key is the non-crossed out VALUES

SIFT KEY

9. Compare your Sift Key With BOB's Sift Key

3 BOB Ryoukai

1. Randomly Choose the SIGN (X) or BIT (Z) basis 8 times (Before speaking to ALICE!) These BASIS will be used to observe ALICE's quantum string.

BASIS

Z	Z	Z	X						

2. Listen to ALICE's stream of ARROW states and record them. Remember, these are quantum states and a person would not be able to "see" the ARROW.

ARROWS

←	↓	←	→						

3. Measure the Quantum States and record their VALUES. To do this, compare the ARROWS to your BASIS choices:

   - If your BASIS is the same as the ARROW's, record them the VALUE as a 0 or 1 respectively
   - If your BASIS is NOT the same as the ARROW's, flip a coin and record the state as 0 or 1 based on the coin

VALUES

1	1	0	1						

   NOTE: At this point the quantum states have been altered by your measurements. To represent this you can blackout the ARROWS above.

4. Tell ALICE the order of the BASIS you chose in step 1
5. Wait for ALICE to tell you which columns to cross out
6. Your Sift Key is the non-crossed out VALUES

SIFT KEY

7. Compare your Sift Key With ALICE's Sift Key

4 EVE Dropper

Hello EVE.
This entire protocol was created with you in mind. Take that as you will. Your task here will be to intercept ALICE and BOB's communications and attempt to get the correct SIFT KEY **WITHOUT** being caught.

1. Randomly Choose the SIGN (X) or BIT (Z) basis 8 times (Before speaking to ALICE!) These BASIS will be used to prepare the quantum string.

BASIS

2. Pretend to be BOB and intercept ALICE's stream of ARROW states.

ALICE's ARROWS

3. Measure the Quantum States and record their VALUES and new ARROW states. To do this, compare the ARROWS to your BASIS choices:

   - If your BASIS is the same as the ARROW's, record the VALUE as a 0 or 1 respectively
   - If your BASIS is NOT the same as the ARROW's, flip a coin and record the state as 0 or 1 based on the coin

VALUES

   - If your BASIS is the same as ALICE's ARROW, record EVE's ARROW to be the same as ALICE's ARROW
   - If your BASIS is NOT the same as ALICE's ARROW, flip a coin and record EVE's ARROW in the BASIS that EVE measured it in based on the coin flip

   NOTE: At this point the quantum states have been altered by your measurements. To represent this you can blackout ALICE's ARROWS.

EVE's ARROWS

4. Pretend to be ALICE and tell BOB your ARROWS in order.

   NOTE: At this point you no longer have access to the quantum states. To represent this you can blackout EVE's ARROWS.

5. Pretend to be ALICE and wait for BOB to tell you the order of the BASIS in which he measured your states.

BOB's BASIS

6. Pretend to be BOB and send her a set of BASIS. Send her either your BASIS from step 1 or BOB's BASIS from step 5.
7. Pretend to be BOB and wait for ALICE to tell you which columns to cross out
8. Pretend to be ALICE and tell BOB which columns to cross out
9. Your Sift Key is the non-crossed out VALUES

SIFT KEY

10. Compare your Sift Key With ALICE's Sift Key