LAB 6

Name: Heja Bibani
Student Number: 16301173

In [3]:
```
from qiskit import QuantumCircuit, execute, Aer
from qiskit.visualization import plot_histogram
from numpy.random import randint
import numpy as np
%matplotlib inline
```

Section 1

Suppose a qubit $q_0 = |-\rangle$. It is measured under a basis with the following two ordered vectors $\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$ and $\begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$.

Task 1.1 Show that this basis is an orthogonal basis.

To show that it is an orthogonal basis we must show that:

1. All entries in B are real numbers
2. $BB^T = B^TB = I$

First all the entires in B are real numbers. Thus we need to prove number two. This basis can also be written as:

$$\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

And we can see that $B^T =$

$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

When we multiply them together we should see that it will equal the identity matrix:

$$\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \times \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} (\frac{1}{2} \times \frac{1}{2} + -\frac{\sqrt{3}}{2} \times -\frac{\sqrt{3}}{2}) & (-\frac{\sqrt{3}}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{\sqrt{3}}{2}) \\ (\frac{\sqrt{3}}{2} \times \frac{1}{2}) + (\frac{1}{2} \times -\frac{\sqrt{3}}{2}) & (\frac{\sqrt{3}}{2} \times \frac{\sqrt{3}}{2} + \frac{1}{2} \times \frac{1}{2}) \end{bmatrix}$$

This equals the identity matrix:

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus meeting the criteria for an Orthorgonal Matrix.

Task 1.2

If $q_0 = c\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} + d\begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$, then give the steps for calculating c and d manually.

Since $|-\rangle = c\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} + d\begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$

This can be re-written as:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}$$

Multiplying both ends by the transpose:

$$\begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix}$$

Therefore:

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1-\sqrt{3}}{2\sqrt{2}} \\ \frac{-\sqrt{3}-1}{2\sqrt{2}} \end{bmatrix}$$

This is the same as applying the rule:

$c = \langle\alpha|\psi\rangle$ and $c = \langle\beta|\psi\rangle$

We can see below:

$$c = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1-\sqrt{3}}{2\sqrt{2}}$$

$$d = \begin{bmatrix} -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{-\sqrt{3}-1}{2\sqrt{2}}$$

Section 2

It is known that measuring a qubit under the Horizontal basis is equivalent to applying H gate to this qubit first and then then measuring it under the Vertical basis. Please prove this fact in a Markdown cell.

Since:

$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ and $|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$

This can also be written as the following below, to find the probability we must use its transpose, that is to to calculate a and b:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

The transpose is of the following:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

The hadamard gate is of the following:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

This is a symmetric gate, thus the transpose is the same:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Thus, applying the gate to the following qubit will satisfy the requirement of making the measurement in this direction, and we can then apply the hadamard gate to simulate making a measurement with a qubit in this direction:

$|\psi\rangle = a|+\rangle + b|-\rangle$

Applying the hadamard gate:

$H(|\psi\rangle) = a \times H(|+\rangle) + b \times H(|-\rangle)$

$$H(|+\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$H(|-\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Thus, this satisfies:

$H(|\psi\rangle) = a|0\rangle + b|1\rangle$

This means, measuring a qubit in the Horizontal basis is equivalent to applying Hadamard gate and then measuring in Vertical basis.

Section 3

In the BB84 Protocol, the bits where Alice and Bob choose different bases are not considered. Let's use D to denote the set of these bits. In this task, you should use both manual calculation and Quantum Circuit simulation to show the following:

Task 3.1

If Eve doesn't eavesdrop, the probability for Alice and Bob to agree on a bit in D is 1/2.

When Alice and Bob disagree on the measurement basis the following configurations are possible:

X-H-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

X-V-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

H-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

V-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

When Alice and Bob disagree on the basis the qubit is in a quantum superposition of the following two states:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

This means that there is a 50% chance of them agreeing on the bits when they do disagree on the basis.

In [4]:
```
def encode_message(bits, bases):
    message = []
    for i in range(n):
        qc = QuantumCircuit(1,1)
        if bases[i] == 0: # Prepare qubit in Vertical Basis
            if bits[i] == 0:
                pass
            else:
                qc.x(0)
        else: # Prepare qubit in Horizontal Basis
            if bits[i] == 0:
                qc.h(0)
            else:
                qc.x(0)
                qc.h(0)
        qc.barrier()
        message.append(qc)
    return message
```

In [5]:
```
def measure_message(message, bases):
    backend = Aer.get_backend('qasm_simulator')
    measurements = []
    for q in range(n):
        if bases[q] == 0: # measuring in Vertical Basis
            message[q].measure(0,0)
        if bases[q] == 1: # measuring in Horizontal Basis
            message[q].h(0)
            message[q].measure(0,0)
        result = execute(message[q], backend, shots=1, memory=True).result()
        measured_bit = int(result.get_memory()[0])
        measurements.append(measured_bit)
    return measurements
```

In [13]:
```
def measure_message_type2(message, bases):
    backend = Aer.get_backend('qasm_simulator')
    measurements = []
    for q in range(n):
        if bases[q] == 0: # measuring in Vertical Basis
            message[q].measure(0,0)
        if bases[q] == 1: # measuring in Horizontal Basis
            message[q].h(0)
            message[q].measure(0,0)
            message[q].h(0)
        result = execute(message[q], backend, shots=1, memory=True).result()
        measured_bit = int(result.get_memory()[0])
        measurements.append(measured_bit)
    return measurements
```

In the below, we changed the remove_garbage function and appended the values where the bases disagree.

In [14]:
```
def remove_garbage(a_bases, b_bases, bits):
    good_bits = []
    for q in range(n):
        if a_bases[q] != b_bases[q]:
            # If both used the same basis, add
            # this to the list of 'good' bits
            good_bits.append(bits[q])
    return good_bits
```

In [15]:
```
def sample_bits(bits, selection):
    sample = []
    for i in selection:
        # use np.mod to make sure the
        # bit we sample is always in
        # the list range
        i = np.mod(i, len(bits))
        # pop(i) removes the element of the
        # list at index 'i'
        sample.append(bits.pop(i))
    return sample
```

In [30]:
```
np.random.seed(seed=0)
n = 10000

## Step 1
# Alice generates bits
alice_bits = randint(2, size=n)

## Step 2
# Create an array to tell us which qubits
# are encoded in which bases
alice_bases = randint(2, size=n)
message = encode_message(alice_bits, alice_bases)

## Step 3
# Decide which basis to measure in:
bob_bases = randint(2, size=n)
bob_results = measure_message(message, bob_bases)

## Step 4
alice_agreed = remove_garbage(alice_bases, bob_bases, alice_bits)
alice_key = remove_garbage(alice_bases, bob_bases, alice_bits)
bob_key = remove_garbage(alice_bases, bob_bases, bob_results)

# Step 5 Check the proportion that is correct in the bases that have disagreed.
agreed_values = 0
for i in range(len(bob_key)):
    if bob_key[i] == alice_key[i]:
        agreed_values = agreed_values + 1

print(agreed_values / len(bob_key))
```

```
0.49295207410390657
```

We have calculated the values which don't agree in the key and notice that there is a 49% chance of it being the correct. This coincides with the expected values since the qubit is in the quantum superposition. We utilized a sample size of 10000 to confirm that the number is indeed 50%.

Task 3.2

If Eve eavesdrops all bits, the probability for Alice and Bob to agree on a bit in D is still 1/2.

Alice and Bob disagree on the basis the qubit is in a quantum superposition of the following states, since Alice is using the message which has been unaltered, the values in this state will follow with the normal case where there is no one eavesdropping, thus when comparing the two keys it keeps the proportion the same:

When Alice and Bob disagree on the measurement basis the following configurations are possible:

XH-V-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

XH-H-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

XV-V-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

X-H-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

H-V-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

H-H-V $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

V-V-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

V-H-H $\rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Note: There was an issue that was found where the program was not simulating reality properly. The issue was rectified with the teacher. We noted that when two measurements are made an issue would generate where it would change the state of the qubit and collapse it. This was noted on the measurements where Eve used a hadamard gate, and because of this another hadamard gate needed to be implemented. To account for this difference we utilized a different measurement scheme for Eve. This is in the function called measure_message_type2.

This means that there is still a 50% chance of them agreeing on the bits when they do disagree on the basis.

In [23]:
```
n = 10000
# Step 1
alice_bits = randint(2, size=n)
alice_bases = randint(2, size=n)
# Step 2
message = encode_message(alice_bits, alice_bases)
# Interception!
eve_bases = randint(2, size=n)
intercepted_message = measure_message_type2(message, eve_bases)

# Step 3
bob_bases = randint(2, size=n)
bob_results = measure_message(message, bob_bases)

# Step 4
bob_key = remove_garbage(alice_bases, bob_bases, bob_results)
alice_key = remove_garbage(alice_bases, bob_bases, alice_bits)

# Step 5 Check the proportion that is correct in the bases that have disagreed.

agreed_values = 0
for i in range(len(bob_key)):
    if bob_key[i] == alice_key[i]:
        agreed_values = agreed_values + 1

print(agreed_values / len(bob_key))
```

```
0.49300628420839243
```

We see above when we calculated the average of the values which are equal and they are around 50%, the values printed is 49%. This coincides with the expected values since the qubit is in the quantum superposition. We utilized a sample size of 10000 to confirm that the number is indeed 50%.