


QUANTUM TELEPORTATION AND QUANTUM CRYPTOGRAPHY

A Masters Thesis Report Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF SCIENCE

in
Physical Sciences

by

Piyush Sharma
(Roll No. )




to

**DEPARTMENT OF PHYSICAL SCIENCES,
INDIAN INSTITUTE OF SCIENCE EDUCATION
AND RESEARCH, KOLKATA**

May 2022

DECLARATION

I, **Piyush Sharma** (Roll No: ) , hereby declare that this report entitled “**Quantum Teleportation and Quantum Cryptography**” submitted to Indian Institute of Science Education and Research, Kolkata towards partial requirement of **Masters of Science** in **Physical Sciences** is an original work carried out by me under the supervision of Prof Joyee Ghosh and has not formed the basis for the award of any degree or diploma, in this or any other institution or university. I have sincerely tried to uphold the academic ethics and honesty. Wherever an external information or statement or result is used, it has been duly acknowledged and cited.


Kolkata - 741246

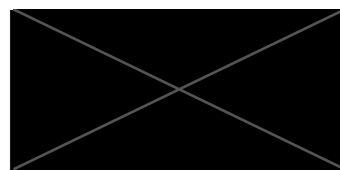


Piyush Sharma

May 2022

CERTIFICATE

This is to certify that the work contained in this project report entitled “**Quantum Teleportation and Quantum Cryptography**” submitted by **Piyush Sharma** (Roll No: ) to Indian Institute of Science Education and Research, Kolkata towards partial requirement of **Masters of Science in Physical Sciences** has been carried out by him under my supervision and that it has not been submitted elsewhere for the award of any degree.



Dr. Joyee Ghosh
Associate Professor
Department of Physics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi-110016 (India)

New Delhi - 110016

Prof Joyee Ghosh

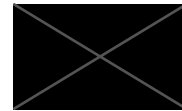
May 2022

Project Supervisor

ACKNOWLEDGEMENT

I'm highly indebted to Prof Joyee Ghosh for taking me in as her project student and for giving me the freedom to choose my project topic. I'm also grateful for the time she made for me despite her busy schedule and her valuable guidance in terms of things I could pursue for this project. This project wouldn't have been possible without the constant support of Prof Mithali Sisodia, a post-doc student of Prof Ghosh's, and her help every step of the way. Sincere thanks are also due to Prof Prasanta Panigrahi for his guidance and all his original and thought-provoking ideas.

Kolkata - 741246



Piyush Sharma

May 2022

ABSTRACT

The main aim of the project was to conduct a study of quantum teleportation and quantum cryptography. In this regard, first a literature study of teleportation was carried out. SPDC (spontaneous parametric down-conversion) is discussed next as it is a very important process in quantum optics for the generation of single photons and entangled pairs of photons and is a key ingredient in many quantum optics experiments, including those for applications in teleportation of photonic states and quantum cryptography (with photons for qubits). The report then moves on to analyzing various quantum key distribution protocols, some entanglement based and some not, before implementing different circuits for the different protocols on the IBM Quantum Computer.

Keywords: [quantum teleportation, quantum cryptography, SPDC, quantum optics, qubit, quantum key distribution, entanglement, IBM Quantum Computer]

Contents

List of Figures	viii
List of Tables	x
1 Basics	1
2 Quantum Teleportation	7
2.1 Mathematical description	8
2.2 Superdense Coding	10
3 SPDC	13
3.1 Classical picture	15
3.1.1 Nonlinear Optics regime	16
3.1.2 Phase-matching conditions	17

3.1.3	Solving the SPDC problem	18
3.2	Quantum picture	20
3.3	Type-I and Type-II phase-matching	23
4	Quantum Cryptography	25
4.1	Quantum Key Distribution Protocols	26
4.1.1	Not entanglement based	26
4.1.2	Entanglement Based	31
4.2	Implementation on the IBM QC	33
4.2.1	Six-state protocol	33
4.2.2	E91	37
4.2.3	BBM92	41
4.3	Conclusion and Discussion	44
	Bibliography	45

List of Figures

1.1	Bloch sphere representation of the various states	3
2.1	Spacetime diagrams for a) quantum teleportation and b) superdense coding. Solid lines represent classical bits, and the wavy line a qubit. Alice performs a quantum measurement, and Bob a unitary operation. Source: [3]	11
2.2	Circuits for quantum teleportation (above) and superdense coding (below) constructed in IBM Quantum Composer	12
3.1	The schematic of Bouwmeester <i>et al.</i> 's experiment [5]	14
3.2	A schematic of the output of SPDC for a type II BBO crystal. Source: Wikipedia	24
4.1	Our circuit (Eve absent)	35
4.2	Histogram plot with the experimental result for each qubit calculated	36

4.3	Circuit in the presence of Eve	36
4.4	New histogram plot and the experimental values of the qubits	37
4.5	Circuits to calculate the terms in the equation for E	38
4.6	Histogram plots for the different circuits	39
4.7	Circuit (run on ibmq_manila with 9999 shots) and histogram plot for $a_2 = b_1 = \frac{\pi}{4}$	40
4.8	Almost perfect correlation for the same measurement basis when Eve absent	42
4.9	Measurements still correlated when they all choose the X basis	42
4.10	Uncorrelated results whenever Eve chooses a different basis . .	43

List of Tables

1.1	Some of the most commonly used quantum gates	5
2.1	The scheme of superdense coding	10
4.1	An example to illustrate the BB84 protocol	28
4.2	Bob's results for his choice of different bases	30
4.3	Alice and Bob's bases for the six-state protocol	34
4.4	Alice and Bob's gates for the different bits and bases	34
4.5	Expected result for each qubit after measurement	35
4.6	Alice, Bob and Eve's bases for the BBM92 protocol	41
4.7	Measurement results uncorrelated for entangled pair 3 due to Eve	43

Chapter 1

Basics

Just like classical computers operate on and store information in classical bits, quantum computers operate on qubits. These are two-level quantum systems with, say, the kets $|0\rangle$ and $|1\rangle$ representing the two states. They may also be represented by an up state $|\uparrow\rangle$ and a down state $|\downarrow\rangle$ when, for instance, dealing with the spin states of an electron. Unlike a classical bit though, which can only take one of two values, 0 and 1, at a time, a qubit can exist in any superposition of the states $|0\rangle$ and $|1\rangle$ as shown below.

$$\begin{aligned} |\psi\rangle &= \alpha |0\rangle + \beta |1\rangle & \alpha, \beta \in \mathbb{C} \\ &= \cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle & \theta \in (0, \pi), \phi \in (0, 2\pi) \end{aligned}$$

Using the latter equation, the qubit states can be represented as vectors on the Bloch sphere with θ being the angle from the positive z -axis and

ϕ being the angle from the positive x -axis of the projection of the vector onto the x - y plane (angle of longitude). At the poles you have the states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (for $\theta = 0$) and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ (for $\theta = \pi$) that lie on the z -axis. Likewise, on the x - y plane, you have

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} && \text{for } \theta = \frac{\pi}{2}, \phi = 0 \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} && \text{for } \theta = \frac{\pi}{2}, \phi = \pi \\ |+_i\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} && \text{for } \theta = \frac{\pi}{2}, \phi = \frac{\pi}{2} \\ |-_i\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} && \text{for } \theta = \frac{\pi}{2}, \phi = \frac{3\pi}{2} \end{aligned}$$

where $|+\rangle$ and $|-\rangle$ lie on the x -axis while $|+_i\rangle$ and $|-_i\rangle$ lie on the y -axis.

The vector \vec{a} that represents $|\psi\rangle$ on the Bloch sphere (fig. 1.1) can be written in spherical coordinates as

$$\begin{aligned} \vec{a} &= (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta) \\ &= (\langle \sigma_x \rangle, \langle \sigma_y \rangle, \langle \sigma_z \rangle) \end{aligned}$$

where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are the Pauli

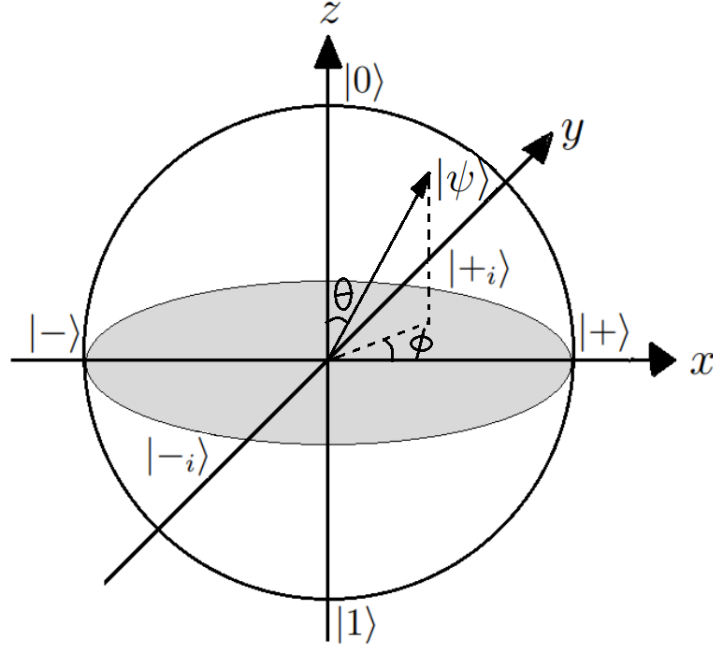


Figure 1.1: Bloch sphere representation of the various states

matrices and $\langle \sigma_x \rangle = \langle \psi | \sigma_x | \psi \rangle$ is the expectation value of σ_x and so on. It is easy to verify that $|0\rangle$ and $|1\rangle$ are eigenstates of σ_z , $|+\rangle$ and $|-\rangle$ are of σ_x , and $|+_i\rangle$ and $|-_i\rangle$ are of σ_y . In fact, σ_x , σ_y and σ_z matrices represent rotations of π in the Bloch sphere about the x , y and z -axes respectively.

A rotation of θ in the Bloch sphere about an arbitrary unit vector $\hat{n} = (n_x, n_y, n_z)$ is given by

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Thus, the rotation operators about the x , y and

z -axes are given by

$$\begin{aligned}
R_x(\theta) &= e^{-i\theta X/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} X = \begin{pmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \\
R_y(\theta) &= e^{-i\theta Y/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \\
R_z(\theta) &= e^{-i\theta Z/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z = \begin{pmatrix} e^{-\frac{\theta}{2}} & 0 \\ 0 & e^{\frac{\theta}{2}} \end{pmatrix}
\end{aligned}$$

Quantum gates, the counterpart of classical logic gates in quantum computers, perform operations on and manipulate information stored in qubits. An n -qubit gate performs a linear unitary transformation in a 2^n -dimensional Hilbert space spanned by all the possible n -qubit states and is represented by a $2^n \times 2^n$ unitary matrix. Single qubit gates, in addition, can also be thought to represent rotations in the Bloch sphere. Apart from the Pauli gates (one for each Pauli matrix), some of the most common gates are given in table 1.1. The H gate transforms $|0\rangle$ into $|+\rangle$ and $|1\rangle$ into $|-\rangle$. Applying H again gives back the original state as $H^2 = I$. The S state adds a phase of $\frac{\pi}{2}$ to the $|1\rangle$ state relative to $|0\rangle$ while the T gate adds a phase of $\frac{\pi}{4}$ and so $S = T^2$. The C -NOT (also called controlled-NOT or CX) is a two-qubit gate that performs a NOT on the target qubit whenever the control qubit is in $|1\rangle$ state but leaves it unchanged otherwise. All the single qubit gates along with the C -NOT gate form a universal set in that they can be used to implement any arbitrary unitary operation on n qubits [11].

Finally, the density matrix formulation becomes important when dealing

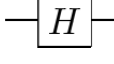
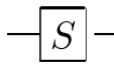
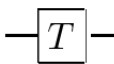

Hadamard gate		$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Phase gate		$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
T gate		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
C -NOT gate		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Table 1.1: Some of the most commonly used quantum gates

with mixed states. The density matrix ρ is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$$

to describe a quantum system whose state is not completely known but the probabilities p_i for the different pure states $|\psi_i\rangle$ are. The expectation of any observable A is calculated using the density matrix as

$$\langle A \rangle = \text{tr}(\rho A)$$

The set of matrices $\{I, \sigma_x, \sigma_y, \sigma_z\}$ forms a complete basis for real vector space of 2×2 Hermitian matrices. Since any arbitrary density matrix for a single qubit system is a 2×2 Hermitian matrix, it can be uniquely decomposed

in the form

$$\rho = \frac{1}{2}(aI + \sum_i b_i \sigma_i) = \frac{1}{2}(aI + \vec{b} \cdot \vec{\sigma})$$

where a and b_i 's are some real numbers ($i = \{x, y, z\}$) and the factor $\frac{1}{2}$ has been added in anticipation of the following result. Solving for them gives $a = 1$ and $b_i = \langle \sigma_i \rangle$. Thus, $\vec{b} = (\langle \sigma_x \rangle, \langle \sigma_y \rangle, \langle \sigma_z \rangle)$ actually represents a vector in the Bloch sphere and is called the *Bloch vector* for state ρ . Unlike before, \vec{b} doesn't need to be a unit vector ($\|\vec{b}\| = 1$ for pure states, < 1 for mixed). Writing $I = \sigma_0$, $\sigma_x = \sigma_1$, $\sigma_y = \sigma_2$ and $\sigma_z = \sigma_3$ with $i = \{0, 1, 2, 3\}$ makes the notation more compact.

$$\rho = \frac{1}{2} \sum_i \langle \sigma_i \rangle \sigma_i = \frac{1}{2} \begin{pmatrix} 1 + \langle \sigma_z \rangle & \langle \sigma_x \rangle - i \langle \sigma_y \rangle \\ \langle \sigma_x \rangle + i \langle \sigma_y \rangle & 1 - \langle \sigma_z \rangle \end{pmatrix}$$

Extrapolating to the case of two-qubit systems, you need 16 linearly independent 4×4 Hermitian matrices to decompose an arbitrary density matrix into. The choice of those 16 matrices can be taken to be the set $\{\sigma_i \otimes \sigma_j | i, j = 0, 1, 2, 3\}$ and then, by drawing inspiration from the single qubit case, we have

$$\rho = \frac{1}{4} \sum_{i,j} \langle \sigma_i \otimes \sigma_j \rangle \sigma_i \otimes \sigma_j$$

Chapter 2

Quantum Teleportation

Quantum teleportation was first described by Bennett *et al.* in 1993 [3] as a means to teleport an unknown qubit state using quantum entanglement and a classical channel to send two classical bits of information. Suppose Alice to be faced with the problem of conveying sufficient information about an unknown state of a particle she possesses to Bob so that he can make his own copy of the state. It turns out that she must know what orthonormal set the state belongs to, before making a measurement, to gain complete information and make copies. If, though, the possibilities for the state include two or more nonorthogonal states, no measurement will yield sufficient information to prepare an accurate copy. This is at the heart of the quantum no-cloning theorem: a quantum state can be swapped from one system to another but can't be copied or cloned and quantum teleportation achieves the former, remotely.

2.1 Mathematical description

Consider Alice to have a particle in an arbitrary unknown qubit state $|\psi_1\rangle = \alpha|0_1\rangle + \beta|1_1\rangle$ that she wishes to teleport to Bob. The particle is numbered 1 to differentiate it from the pair of entangled particles, numbered 2 and 3, that Alice and Bob are required to share beforehand for the purpose of teleportation. Consider the entangled pair to be in the singlet state

$$|\Psi_{23}^-\rangle = \frac{1}{\sqrt{2}}(|0_21_3\rangle - |1_20_3\rangle)$$

The full state of the system of all three particles is given by

$$\begin{aligned} |\Psi\rangle &= |\psi_1\rangle \otimes |\Psi_{23}^-\rangle \\ &= \frac{1}{\sqrt{2}}(\alpha|0_10_2\rangle|1_3\rangle - \alpha|0_11_2\rangle|0_3\rangle + \beta|1_10_2\rangle|1_3\rangle - \beta|1_11_2\rangle|0_3\rangle) \end{aligned}$$

Alice now makes a Bell-state measurement on particles 1 and 2, which projects the state of the two particles into one of the four Bell states which, apart from the singlet state, are

$$\begin{aligned} |\Psi_{12}^+\rangle &= \frac{1}{\sqrt{2}}(|0_11_2\rangle + |1_10_2\rangle) \\ |\Phi_{12}^+\rangle &= \frac{1}{\sqrt{2}}(|0_10_2\rangle + |1_11_2\rangle) \\ |\Phi_{12}^-\rangle &= \frac{1}{\sqrt{2}}(|0_10_2\rangle - |1_11_2\rangle) \end{aligned}$$

Thus, the complete state of the system before the Bell state measurement

can be written as

$$\begin{aligned}
|\Psi\rangle &= \frac{1}{2}(\alpha(|\Phi_{12}^+\rangle + |\Phi_{12}^-\rangle)|1_3\rangle - \alpha(|\Psi_{12}^+\rangle + |\Psi_{12}^-\rangle)|0_3\rangle \\
&\quad + \beta(|\Psi_{12}^+\rangle - |\Psi_{12}^-\rangle)|1_3\rangle - \beta(|\Phi_{12}^+\rangle - |\Phi_{12}^-\rangle)|0_3\rangle) \\
|\Psi\rangle &= \frac{1}{2}(|\Psi_{12}^-\rangle(-\alpha|0_3\rangle - \beta|1_3\rangle) + |\Psi_{12}^+\rangle(-\alpha|0_3\rangle + \beta|1_3\rangle) \\
&\quad + |\Phi_{12}^+\rangle(\alpha|1_3\rangle - \beta|0_3\rangle) + |\Phi_{12}^-\rangle(\alpha|1_3\rangle + \beta|0_3\rangle))
\end{aligned}$$

As is evident from the above equation, after the Bell-state measurement, as the particles 1 and 2 are projected into one of the Bell states, the state of particle 3 is projected with equal probability into one of four states, all of which are actions of simple unitary operators on the unknown quantum state $|\psi\rangle$. To compare Alice's result and the state to which Bob's particle collapses (σ_x , σ_y and σ_z are written as X , Y and Z from here on),

$$\begin{aligned}
|\Psi_{12}^-\rangle &\longrightarrow -I|\psi_3\rangle \\
|\Phi_{12}^-\rangle &\longrightarrow X|\psi_3\rangle \\
|\Phi_{12}^+\rangle &\longrightarrow -iY|\psi_3\rangle \\
|\Psi_{12}^+\rangle &\longrightarrow -Z|\psi_3\rangle
\end{aligned}$$

Alice conveys the result of her measurement to Bob through a classical channel (takes two bits) and he applies the corresponding unitary operator (X for $|\Phi^-\rangle$, Y for $|\Phi^+\rangle$ and Z for $|\Psi^+\rangle$) on his particle to obtain the state. Teleportation is incomplete without this step. With no communication from Alice, if Bob were to guess his state and apply a unitary operator, he'd leave

his particle in a maximally mixed state, containing no information about the state $|\psi\rangle$.

2.2 Superdense Coding

Superdense coding accomplishes the task of sending two classical bits using a qubit, the inverse of teleportation. It's imperative that Alice (receiver) and Bob (sender) share an entangled pair of qubits, in the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2\rangle + |1_1 1_2\rangle)$$

for example, before the process, like in the case of teleportation. Bob applies next a unitary operator on his qubit (his qubit is numbered 1 now) depending on the two-bit message he wishes to send, before sending his qubit off to Alice. Bob's operation changes the state $|\Phi^+\rangle$ into one of the four Bell states. Alice first applies a *C*-NOT operation with Bob's qubit as the control and hers as the target and then the operation $H \otimes I$ (H applied on Bob's qubit). She finally measures the two-qubit state and retrieves the message (see table 2.1).

Two-bit message	Bob applies	$ \Phi^+\rangle$ changes into	Alice finally measures
00	I	$ \Phi^+\rangle$	$ 00\rangle$
01	X	$ \Psi^+\rangle$	$ 01\rangle$
10	Z	$ \Phi^-\rangle$	$ 10\rangle$
11	Y	$ \Psi^-\rangle$	$ 11\rangle$

Table 2.1: The scheme of superdense coding

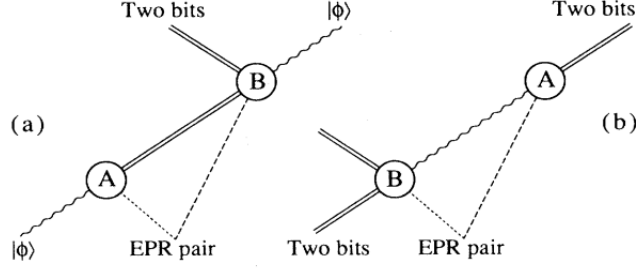


Figure 2.1: Spacetime diagrams for a) quantum teleportation and b) superdense coding. Solid lines represent classical bits, and the wavy line a qubit. Alice performs a quantum measurement, and Bob a unitary operation. Source: [3]

In the circuit for quantum teleportation in fig. 2.2, $q[0]$ is the qubit in the unknown state while $q[1]$ and $q[2]$ are prepared in the entangled state $|\Phi^+\rangle$. In this case, Alice's measurement on $q[0]$ and $q[1]$ yields one of four states, $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$. Bob applies the gates CX and CZ (controlled- Z), effectively applying I for Alice's measurement of $|00\rangle$, X for $|01\rangle$, Z for $|10\rangle$ or $Z \cdot X = iY$ for $|11\rangle$ on his qubit $q[2]$, and the state of $q[0]$ is finally teleported to $q[2]$. In the superdense-coding circuit, the two-bit message to be sent is 10 and Bob applies Z on his qubit $q[0]$. Alice applies C -NOT with $q[0]$ as control and $q[1]$ as target and H on $q[0]$, before measuring to get $|10\rangle$.

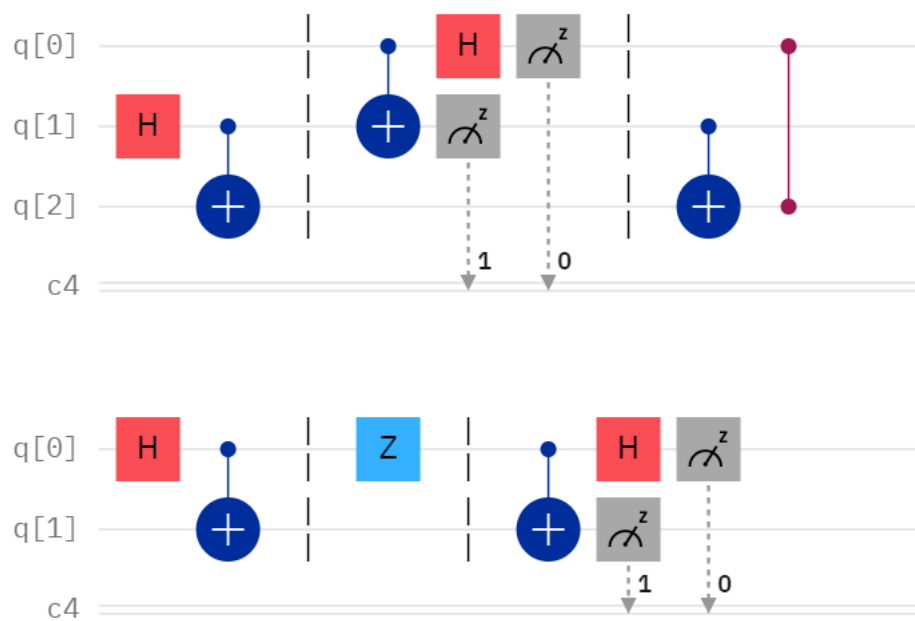


Figure 2.2: Circuits for quantum teleportation (above) and superdense coding (below) constructed in IBM Quantum Composer

Chapter 3

SPDC

Bouwmeester *et al.* were one of the first to experimentally demonstrate teleportation of photonic states in 1997 [5]. The schematic of the experiment as it appeared in the original paper is shown in fig. 3.1. A UV pulse shot at a nonlinear crystal creates the pair of entangled photons numbered 2 and 3 in the state $|\Psi^-\rangle$ through type-II SPDC (spontaneous parametric down-conversion). It is a nonlinear optical process in which a photon of higher energy spontaneously splits into two of lower energies (types of SPDC are discussed later). When the pulse reflects off the mirror and hits the crystal again, it creates another entangled pair of photons, 1 and 4. When photon 4 is detected, it serves to confirm the presence of photon 1, which is prepared in a polarization state that is to be teleported. Thus, SPDC also finds use as a heralded single-photon source in the experiment. For the Bell-state measurement, Alice makes the photons 1 and 2 indistinguishable by superposing them at a beam-splitter (BS). For the antisymmetric state $|\Psi_{12}^-\rangle$, unlike the

other Bell states, the two photons emerge one on each side ([6]) and it is thus measured by detecting coincidence at detectors $f1$ and $f2$. $|\Psi^-\rangle$ is measured only in one-fourth of the cases and the coincidence serves as the classical message informing Bob that teleportation has taken place (since measurement of $|\Psi^-\rangle$ only requires applying I on photon 3). This can be verified using a polarizing beam-splitter (PBS) which, suppose, transmits the initial polarization state of photon 1 but reflects the orthogonal polarization, in which case we look for the three-fold coincidences $d2f1f2$ together with the absence of $d1f1f2$.

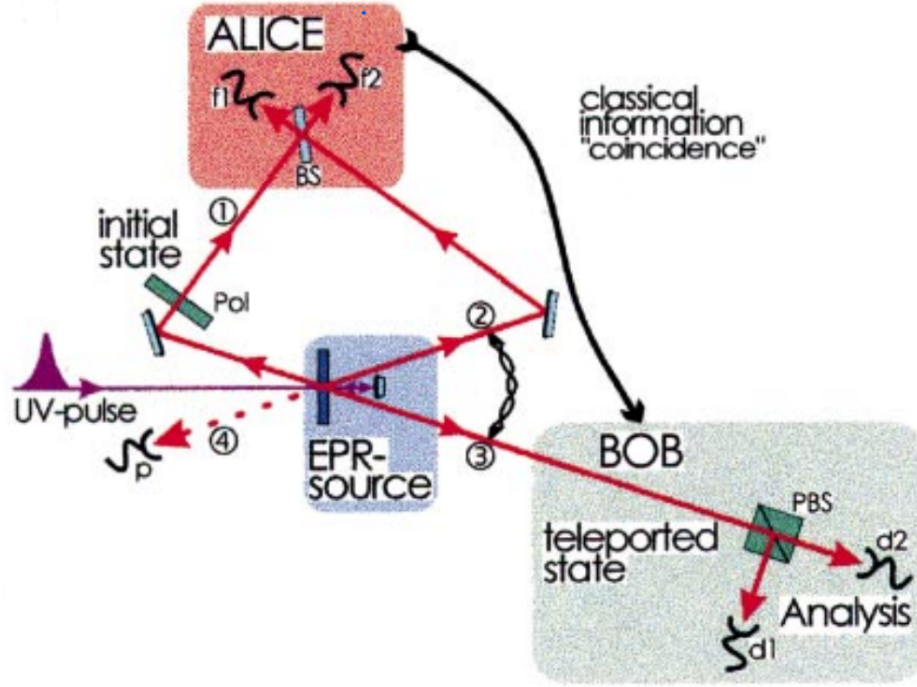


Figure 3.1: The schematic of Bouwmeester *et al.*'s experiment [5]

The above teleportation experiment motivates us to study SPDC in some

detail. In fact, SPDC is a very important process to generate single and entangled photons and finds applications, among many other quantum optics experiments, in several quantum cryptography experiments as well. I'll first approach the phenomenon from the classical perspective and show how it is not possible classically, before discussing the quantum mechanical perspective.

3.1 Classical picture

To begin with, consider an electron in a dielectric under the influence of an oscillating electric field ($E = E_0 e^{-i\omega t}$) of an incident beam of light. The Lorentz model then describes the electron motion as that of a damped driven harmonic oscillator, which, in the 1D case, satisfies the equation

$$\ddot{x} + \gamma \dot{x} + \omega_0^2 x = -\frac{q}{m} E_0 e^{-i\omega t}$$

where $-q$ is the electron charge and the other symbols have their usual meaning. Solving for x gives a complex amplitude, implying the electron motion lags behind the driving electric field in phase.

$$x = -\frac{q}{m} \frac{1}{\omega_0^2 - \omega^2 - i\omega\gamma} E_0 e^{-i\omega t}$$

For a linear isotropic material, the polarization \mathbf{P} is only dependent on the first power of \mathbf{E} and the susceptibility χ is a scalar. For our 1D case,

$P = -Nqx = \epsilon_0\chi E$ (N is number density of electrons), giving

$$P = \frac{Nq^2}{m} \frac{1}{\omega_0^2 - \omega^2 - i\omega\gamma} E, \quad \chi = \frac{Nq^2}{m\epsilon_0} \frac{1}{\omega_0^2 - \omega^2 - i\omega\gamma}$$

and giving the relative permittivity ϵ_r finally as

$$\epsilon_r = 1 + \chi = 1 + \frac{\omega_p^2}{\omega_0^2 - \omega^2 - i\omega\gamma}$$

where $\omega_p = \sqrt{\frac{Nq^2}{m\epsilon_0}}$ is the plasma frequency. The refractive index of the material is the square root of the real part of ϵ_r .

3.1.1 Nonlinear Optics regime

But the electron motion becomes anharmonic for higher incoming light energies. In such cases, \mathbf{P} is usually approximated to a Taylor series in E with susceptibilities of increasing order as coefficients.

$$\begin{aligned} \mathbf{P}(t) &= \epsilon_0(\chi^{(1)}\mathbf{E}(t) + \chi^{(2)}\mathbf{E}^2(t) + \chi^{(3)}\mathbf{E}^3(t) + \dots) \\ \frac{P_i}{\epsilon_0} &= \sum_j \chi_{ij}^{(1)} E_j + \sum_{jk} \chi_{ijk}^{(2)} E_j E_k + \sum_{jkl} \chi_{ijkl}^{(3)} E_j E_k E_l + \dots \end{aligned}$$

In general, $\chi^{(n)}$ is an $(n + 1)$ -rank tensor. In the first nonlinear term (polarization dependent on the square of the field) therefore, the second order susceptibility $\chi^{(2)}$ is a third rank tensor. This term corresponds to the phe-

nomenon of three-wave mixing. To see how, consider, for example

$$E(t) = E_1 \cos(\omega_1 t) + E_2 \cos(\omega_2 t) = \frac{1}{2}E_1 e^{-i\omega_1 t} + \frac{1}{2}E_2 e^{-i\omega_2 t} + c.c.$$

where *c.c.* stands for complex conjugate. The first nonlinear polarization term

$$P^{NL} = \epsilon_0 \chi^{(2)} E^2(t) = \frac{\epsilon_0}{4} \chi^{(2)} \left(E_1^2 e^{-2i\omega_1 t} + E_2^2 e^{-2i\omega_2 t} + 2E_1 E_2 e^{-i(\omega_1 + \omega_2)t} \right. \\ \left. + 2E_1 E_2^* e^{-i(\omega_1 - \omega_2)t} + (|E_1|^2 + |E_2|^2) + c.c. \right)$$

The different terms in the above equation represent different three-wave mixing processes. The first two terms have the incident frequencies doubled, in a process called second-harmonic generation (SHG). Then you'd see a term with the frequencies summed and another with their difference, corresponding to the processes of sum-frequency generation (SFG) and difference-frequency generation (DFG), respectively. Finally, the 0 frequency terms correspond to something called optical rectification in which a quasi-DC polarization is generated in the medium. Note that SPDC is the reverse of SFG.

3.1.2 Phase-matching conditions

As does any other physical process, SPDC conserves energy and momen-

tum. Energy conservation implies

$$\hbar\omega_3 = \hbar\omega_1 + \hbar\omega_2$$

$$\Delta\omega = \omega_3 - \omega_2 - \omega_1 = 0$$

when a photon at frequency ω_3 splits into two at frequencies ω_1 and ω_2 . For momentum conservation, we have

$$k_1 + k_2 = k_3 \quad \text{or} \quad \frac{n_3\omega_3}{c} = \frac{n_1\omega_1}{c} + \frac{n_2\omega_2}{c}$$

$$\Delta k = k_3 - k_2 - k_1 = 0$$

For most materials, $n_1(\omega_1) < n_2(\omega_2) < n_3(\omega_3)$ for $\omega_1 < \omega_2 < \omega_3$ for ‘normal’ dispersion, which makes the condition for momentum conservation impossible to satisfy. This is where birefringent crystals come into play as they have two (uniaxial) or three (biaxial) different refractive indices along different symmetry axes which can help satisfy the phase-matching condition.

3.1.3 Solving the SPDC problem

From the Maxwell’s equations, one can derive

$$\nabla^2 \mathbf{E} - \frac{n^2}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} = \frac{1}{\epsilon_0 c^2} \frac{\partial^2 \mathbf{P}^{NL}}{\partial t^2} \quad (3.1)$$

where n is the refractive index of the medium. We’ll approximate \mathbf{P}^{NL} to only be the first nonlinear polarization term.

SPDC corresponds to the process of parametric amplification in classical nonlinear optics in which a strong pump beam at frequency ω_3 is combined with a weak signal beam at ω_1 to give rise to an amplified signal at ω_1 but also to a second signal called the idler beam at ω_2 ([8]). Let's solve for the signal beam using eq. 3.1 by first considering it to be of the form

$$E_1(z, t) = A_1 e^{i(k_1 z - \omega_1 t)} + c.c. \quad (3.2)$$

Imagine the pump and idler beams generating the signal beam through difference-frequency generation ($\omega_1 = \omega_3 - \omega_2$). We ignore all the other terms but the relevant term in the expansion of $P^{NL} = \epsilon_0 \chi^{(2)}(E_3 + E_2)^2$, where

$$E_3(z, t) = A_2 e^{i(k_2 z - \omega_2 t)} + c.c.$$

$$E_2(z, t) = A_3 e^{i(k_3 z - \omega_3 t)} + c.c.$$

are respectively the pump and idler beams, for the concerned process (DFG), to have

$$P^{NL} = 2\epsilon_0 \chi_{eff}^{(2)} E_3 E_2^* + c.c. = 2\epsilon_0 \chi_{eff}^{(2)} A_3 A_2^* e^{i(k_1 z - \omega_1 t)} + c.c. \quad (3.3)$$

where we reduced the tensor $\chi^{(2)}$ to a scalar $\chi_{eff}^{(2)}$ as an approximation and also used the relations $k_3 - k_2 = k_1$ and $\omega_3 - \omega_2 = \omega_1$. Using equations 3.1, 3.2 and 3.3 together, we finally get

$$\frac{d^2 A_1}{dz^2} + 2ik_1 \frac{dA_1}{dz} = -2 \frac{\omega_1^2}{c^2} \chi_{eff}^{(2)} A_3 A_2^*$$

At last, we make the slowly varying amplitude approximation to neglect the first term compared to the second on the left-hand side of the equation to get

$$\frac{dA_1}{dz} = i \frac{\omega_1}{n_1 c} \chi_{eff}^{(2)} A_3 A_2^* \quad (3.4)$$

But we can reach a similar equation for the idler beam just as well instead of the signal beam.

$$\frac{dA_2}{dz} = i \frac{\omega_2}{n_2 c} \chi_{eff}^{(2)} A_3 A_1^* \quad (3.5)$$

Equations 3.4 and 3.5 are our final system of differential equations which lead us to the so-called Manley-Rowe relations.

$$\begin{aligned} A_2(z) &= i \sqrt{\frac{\omega_2 n_1}{\omega_1 n_2}} \frac{A_3}{|A_3|} A_1^*(0) \sinh(\alpha z) \\ A_1(z) &= A_1(0) \cosh(\alpha z) \\ \alpha &= \frac{\chi_{eff}^{(2)} |A_3|}{c} \sqrt{\frac{\omega_1 \omega_2}{n_1 n_2}} \end{aligned}$$

It is evident from these equations that if there is no initial incident signal beam ($A_1(0) = 0$), $A_1(z) = A_2(z) = 0$ and the signal and idler beams can't exist. Clearly, the classical picture fails to explain SPDC because photons do sometimes spontaneously split into two with lower energies without any initial signal or idler beam.

3.2 Quantum picture

A quantized EM field, on the other hand, can perfectly explain a photon

getting destroyed and those with lower energies springing into existence during an interaction with a nonlinear medium. To provide a description for such an event, we can infer an effective interaction Hamiltonian for SPDC to look like

$$\hat{H}_{SPDC} = i\hbar\kappa(\hat{a}_i\hat{a}_s\hat{a}_p^\dagger e^{i\Delta\vec{k}\cdot\vec{r}-i\Delta\omega t} + \hat{a}_i^\dagger\hat{a}_s^\dagger\hat{a}_p e^{-i\Delta\vec{k}\cdot\vec{r}+i\Delta\omega t})$$

where an \hat{a} is an annihilator operator and an \hat{a}^\dagger is a creation operator. The first term thus accounts for the process of SFG in which an idler and a signal photon (at frequencies ω_1 and ω_2) are destroyed and a pump photon (at ω_3) is created. And the second term represents SPDC for which a pump photon is destroyed to create an idler and a signal photon. Both processes evidently do compete and coexist. The constant κ is given by

$$\kappa = \frac{\chi_{eff}}{3\epsilon_0 V} \sqrt{\frac{\omega_1\omega_2\omega_3}{2\epsilon_0 V}}$$

Now consider the effect of the above Hamiltonian on an incoming pump beam in the state $|0_i, 0_s, N_p\rangle$ (N_p number of pump photons, 0 idler and signal photons). The Schrödinger equation implies

$$|\psi(t)\rangle = e^{\frac{1}{i\hbar} \int_0^t \hat{H}_{SPDC}(t') dt'} |0_i, 0_s, N_p\rangle$$

As κ is quite small, most of the pump beam is unperturbed by the process and the exponential Hamiltonian can be Taylor expanded up to first order

to give

$$|\psi(t)\rangle \approx C_0 |0_i, 0_s, N_p\rangle + C_1 \frac{1}{i\hbar} \int_0^t \hat{H}_{SPDC}(t') dt' |0_i, 0_s, N_p\rangle$$

where C_0 and C_1 are coefficients for the normalization of the wave function and $C_1 \approx 1 - C_0$ since $C_0 \gg C_1$. We have $\Delta\omega \approx 0$ for perfect phase-matching in energy and the integral thus becomes a Dirac function so that we can simply apply the operators \hat{a}_i^\dagger , \hat{a}_s^\dagger and \hat{a}_p on the state $|0_i, 0_s, N_p\rangle$ to find

$$|\psi(t)\rangle \approx C_0 |0_i, 0_s, N_p\rangle + \kappa C_1 e^{-\Delta\vec{k}\cdot\vec{r}} |1_i, 1_s, N_p - 1\rangle$$

The intensity I_{SPDC} is proportional to the square of the wave function. This is where the phase-matching condition in the wave vector appears. SPDC is a linear process with the pump beam intensity I_p . To see this, we need to assume that the pump field is strong enough to be considered like a totally classical field so that $\hat{a}_p \approx E_p$. As a result, I_{SPDC} will depend linearly on I_p . Also, $C_0 \gg C_1$ implies that SPDC is a highly inefficient process. For higher pump powers, more terms appear in the Taylor expansion of the exponential \hat{H} but they are proportional to increasing powers of κ so that the probability to have more and more photon pairs generated through SPDC decreases drastically. Finally, unlike in the classical case where we needed a non-zero signal beam, quantum optics explains SPDC perfectly even for the case with zero signal and idler photons initially.

3.3 Type-I and Type-II phase-matching

As already discussed, the phase-matching condition in the wave vector is impossible to satisfy except for birefringent crystals for which the refractive index depends on the direction and polarization of the incoming light. The technique of choosing the polarization of the fields and the orientations of the crystal to fulfil the phase-matching condition is called angle tuning. Crystals that possess two different refractive indices along their different symmetry axes, one along a preferred axis called the extraordinary (e) axis, and another along the other two axes called the ordinary (o) axes, are called uniaxial. Biaxial crystals possess three different refractive indices along their three symmetry axes.

Most nonlinear crystals are negative uniaxial, meaning that the refractive index along the e axis smaller than that along the o axes. For such crystals, like BBO for example, one can have two types of phase matching:

$$\begin{array}{ll}
 e \longrightarrow o + o & \text{Type-I} \\
 e \longrightarrow o + e & \text{Type-II} \\
 e \longrightarrow e + o & \text{Type-II}
 \end{array}$$

The idler and signal photons have the same polarization for type-I but orthogonal polarizations for type-II.

Fig. 3.2 shows the output cones of SPDC of the ordinary (horizontally polarized) and extraordinary (vertically polarized) beams for a type II BBO

crystal. For two photons emitted along the intersection of the two cones, all we know is if one is horizontally polarized, the other must be vertically polarized, but we can't tell which is which. Thus, they are entangled and given, in general, by the state $\frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_1 |\uparrow\rangle_2 + e^{i\phi} |\uparrow\rangle_1 |\leftrightarrow\rangle_2)$.

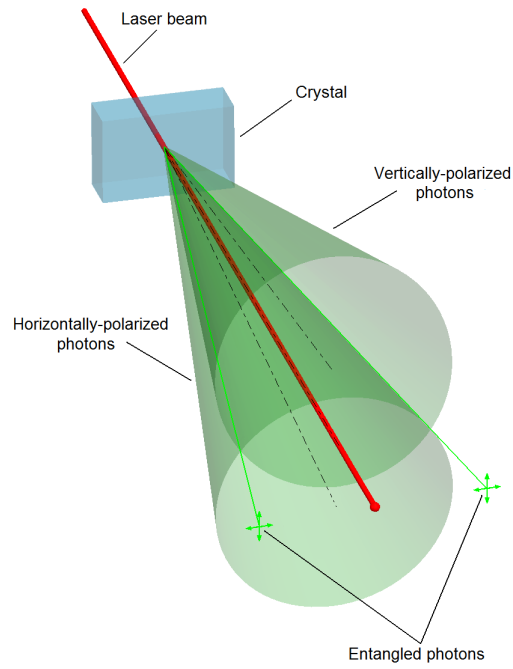


Figure 3.2: A schematic of the output of SPDC for a type II BBO crystal.
Source: Wikipedia

Chapter 4

Quantum Cryptography

The security of classical cryptographic protocols is based on the mathematical complexity of the encoding function. The RSA (Rivest–Shamir–Adleman), for example, is a public-key cryptosystem which relies on the practical difficulty of factoring a product of two large prime numbers [13]. Every RSA user has a public key and a private key. The public key is created using two large prime numbers which are kept secret. Any sender can use the intended recipient’s public key to encrypt a message but it would only take the private key, which employs actual knowledge of the prime numbers, of the recipient to decrypt it. As such, the security of the RSA, and the whole of classical cryptography, for that matter, is not provable but only dependent on the fact that the amount of computation or time required to breach the protocol is not feasible.

With quantum computers coming into the picture though, the situation

is dramatically altered. Because certain quantum algorithms have already been shown to run in polynomial time for problems that would take the best known classical algorithms super-polynomial time [14], it might not be long before large quantum computers achieve the computational capabilities to successfully breach classical protocols. This sets the stage for quantum cryptographic protocols to take over as their security is based on quantum mechanical principles of uncertainty and the no-cloning theorem, among others, and can actually be proven. In fact, the first of its kind, the BB84 protocol, was first proven secure in 1999 [10], and many others have similarly been shown to be secure since then.

In this chapter, I'll discuss a few protocols, some entanglement based and some not, for quantum key distribution (QKD) and then implement circuits for a few of them as a proof of their concept on the IBM Quantum Computer. The aim of QKD is only to produce and distribute a key securely among users who share no secret information initially. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) messages.

4.1 Quantum Key Distribution Protocols

4.1.1 Not entanglement based

BB84

BB84 was the first ever QKD protocol, developed by Bennett *et al.* in

1984 [2]. The distribution of a secure key among users is accomplished using a quantum channel to send qubits and a public classical channel susceptible to passive eavesdropping (meaning a third party may view the content in the channel but may not alter it) to communicate after.

See table 4.1 for an illustrative example of the protocol. Alice begins with a string of random bits, each of which she must encode into a qubit state. For our present example, we consider the qubits to be photons. She chooses one of two bases, say the rectangular (R) and the diagonal (D) bases, at random for each bit and encodes the bit into the corresponding polarization state of the photon. We can have other pairs of bases for the protocol but it is the most efficient to have those that are mutually unbiased, a quality attributed to two orthonormal bases $\{e_1, e_2\}$ and $\{f_1, f_2\}$ for qubit states when

$$|\langle e_i | f_j \rangle|^2 = \frac{1}{2} \quad \forall i, j \in \{1, 2\}$$

Mutually unbiased bases are so useful because the outcome is totally random when a measurement is made in a basis unbiased to that in which the state was prepared.

Alice now sends the photons that she prepared in different polarization states off to Bob. In the table we assume some are lost on the way. Bob chooses the R or the D basis at random to measure the polarization of each photon he receives and thus obtains his own string of bits. Over a public classical channel, the two next announce their bases for each photon, identify the ones for which they chose the same basis, and discard the rest of the bits (these bits of Bob's are totally random compared to Alice's). The bits for

Quantum Transmission										
Alice's random bits	0	1	1	0	0	1	0	1	0	1
Random sending bases	D	R	D	D	D	R	D	R	R	R
Photons Alice sends	\nearrow	\uparrow	\nwarrow	\nearrow	\nearrow	\uparrow	\nearrow	\uparrow	\rightarrow	\uparrow
Random receiving bases	D	D	R	R	D	R	D	D	D	R
Bits received by Bob	0	1		1	0	1	0	0		1
Public discussion										
Bob reports bases of received bits	D	D		R	D	R	D	D		R
Alice says which bases were correct	OK				OK	OK	OK			OK
Shared key if no eavesdrop	0				0	1	0			1
Bob reveals some bits at random					0		0			
Alice confirms					OK		OK			
Outcome										
Shared key	0					1				1

Table 4.1: An example to illustrate the BB84 protocol

these photons should match unless someone tampered with them on their way. Bob reveals some bits at random. When Alice confirms they do indeed match, they generate a key from the remaining bits.

The most commonly discussed strategy for attack by an eavesdropper Eve is the intercept-resend. Suppose Alice and Bob both choose the R basis for a bit. If Eve intercepts this photon and makes a measurement in the R basis before it reaches Bob, he'd measure the same value as Alice and the situation is no different than when Eve was absent. But if she measures in the D basis, he measures a random value (different than Alice's around half the time). This implies an error rate of 0.25 for when Eve is present. When finally revealing some of his bits to Alice to check for the presence of Eve, if they find that a good number (more than at least $\frac{3}{4}$ of them) match, they deduce that a sufficient number of photons were not intercepted for them to abort the protocol and start over. And because Eve gets the basis correct around half the time, her information gain is 0.5. But this is no more than

when she makes no measurement at all and is asked to guess the bits to a random string.

Six-state Protocol

The six-state protocol is exactly like the BB84 save the part that it utilizes six states or three bases to encode the qubits or to measure [7]. The choice of three mutually unbiased bases could be the rectangular, the diagonal and the circular bases in the case of photons or the X , Y and Z bases for qubits in a quantum computer. Like before, Alice and Bob keep the bits for the qubits for which they chose the same basis and discard the rest.

The advantage the six-state protocol has over the BB84 is that it increases the error rate to $\frac{1}{3}$ in case of an intercept-resend attack. The probability of Eve choosing a different basis than Alice and Bob for a qubit is now $\frac{2}{3}$ but that of Bob getting a different value than Alice due to the consequent randomization is still $\frac{1}{2}$. This makes detecting Eve easier but also the protocol more noise tolerant because a small error rate due to noise is now less likely to be confused with her presence.

B92

B92 is probably the simplest QKD protocol, proposed by Bennett in 1992 [1]. It uses just two states to distribute a key. In this protocol, Alice encodes her bits using any two non-orthogonal states but preferably from two mutually unbiased bases, like $|0\rangle$ for 0 and $|+\rangle$ for 1. Bob chooses at random the

Z (the one that $|0\rangle$ belongs to) or the X (which $|+\rangle$ belongs to) basis for measurement (see table 4.2).

Bit	Alice	Bob (Z)	Bob (X)
0	$ 0\rangle$	$ 0\rangle, Pr = 1$	$ +\rangle, Pr = 1/2$
		$ 1\rangle, Pr = 0$	$ -\rangle, Pr = 1/2$
1	$ +\rangle$	$ 0\rangle, Pr = 1/2$	$ +\rangle, Pr = 1$
		$ 1\rangle, Pr = 1/2$	$ -\rangle, Pr = 0$

Table 4.2: Bob's results for his choice of different bases

When measuring in the Z basis, obtaining the state $|1\rangle$ for bit 0 has zero probability. And so does the state $|-\rangle$ for bit 1. Bob thus notes down the bit value 1 whenever he obtains $|1\rangle$ and 0 for when he obtains $|-\rangle$ and discards measurements of all other states. He finally reveals the positions of the qubits for which he measured the states $|1\rangle$ and $|-\rangle$ over the classical channel to Alice for the key.

Eve could intercept the qubits and perform much the same job as Bob to note down her own 0s and 1s. But the positions of her bits are expected to be significantly different which would result in her gaining little information about the key. Even so, Bob would compare a random sample of his bits with Alice's to estimate the error rate and see if it is within a threshold to go ahead with generating a key.

4.1.2 Entanglement Based

E91

In 1991, Ekert, for the first time ever, exploited quantum entanglement for cryptographic purposes and proposed the ‘E91’ protocol [9]. It involves Alice and Bob sharing an entangled pair of particles in, say, the singlet state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Alice makes a measurement on her particle in one of three bases, Z , $(X + Z)/\sqrt{2}$ and X , that she chooses at random. These bases correspond to axes at angles $a_1 = 0$, $a_2 = \frac{\pi}{4}$ and $a_3 = \frac{\pi}{2}$ from the z -axis in the x - z plane. Likewise, Bob makes a measurement on his share of the pair after randomly choosing one from the $(X + Z)/\sqrt{2}$, X and $(X - Z)/\sqrt{2}$ bases, which correspond to the angles $b_1 = \frac{\pi}{4}$, $b_2 = \frac{\pi}{2}$ and $b_3 = \frac{3\pi}{4}$.

The bases are so chosen because they maximize the magnitude of the CHSH quantity E , calculated as ([12])

$$E = \langle a_1 b_1 \rangle - \langle a_1 b_3 \rangle + \langle a_3 b_1 \rangle + \langle a_3 b_3 \rangle$$

The quantities $\langle a_i b_j \rangle$ are a measure of the degree of correlation between the result of Alice’s measurement in the a_i basis and of Bob’s in the b_j basis and can be experimentally calculated as

$$\langle a_i b_j \rangle = P(|00\rangle | a_i b_j) - P(|01\rangle | a_i b_j) - P(|10\rangle | a_i b_j) + P(|11\rangle | a_i b_j)$$

where the right-hand side terms are the conditional probabilities of different kets given that Alice measured in the a_i basis, and Bob in the b_j basis. Theoretically, for a maximally entangled anti-correlated state (like the singlet state), quantum mechanics predicts that

$$\langle a_i b_j \rangle = -\mathbf{a}_i \cdot \mathbf{b}_j = -\cos(a_i - b_j)$$

so that E turns out to be

$$E = -\cos \frac{\pi}{4} + \cos \frac{3\pi}{4} - \cos \frac{\pi}{4} - \cos \frac{\pi}{4} = -2\sqrt{2}$$

$|E| > 2$ implies correlations (or anti-correlations when E is negative) stronger than any classical process would ever allow and thus the CHSH inequality $-2 \leq E \leq 2$ is violated for all entangled particles. $|E| = 2\sqrt{2}$ is the maximal violation of the inequality and represents perfect correlation (or anti-correlation), found to be the case for maximally entangled states.

Back to the protocol, Alice and Bob, after a series of measurements on a number of entangled pairs, coordinate over a public channel to measure E and if they find the inequality to not be violated, they reason that sufficient eavesdropping has taken place so as to compromise the security and authenticity of the protocol. Otherwise, they go ahead and identify the instances in which they chose the same measurement basis and utilize the fact that their resultant bits in these cases will be significantly anti-correlated to generate a key.

BBM92

The next protocol is one which employs entanglement but is very similar to the BB84 [4]. Alice and Bob share particles in a maximally entangled state, say

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and measure their particles randomly in the Z or the X basis. In the absence of Eve, their results are perfectly correlated whenever they choose the same basis. They identify over a public channel the instances in which they chose the same basis and reveal their results for a random sample of them. If they find them to be correlated (within a reasonable margin of error due to, say, noise or eavesdropping), they generate a key using their results from the rest of the cases in which they chose the same basis.

4.2 Implementation on the IBM QC

In this section, I'll discuss my implementations of different circuits of three of the several QKD protocols discussed above, the six-state protocol, the E91 and the BBM92, on the IBM Quantum Computer (IBM QC).

4.2.1 Six-state protocol

Implementation of this protocol here is identical to the way performed in [15]. Suppose Alice has a string of 8 random bits (see table 4.3) and she takes

Qubits	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7
Bits	0	1	0	0	1	0	1	1
Alice's bases	Z	Z	X	Y	X	Z	Y	X
Bob's bases	Z	Y	X	Y	Y	Z	X	Z

Table 4.3: Alice and Bob's bases for the six-state protocol

Qubits	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7
Bits	0	1	0	0	1	0	1	1
Gates for constructing the string of bits	-	X	-	-	X	-	X	X
Alice's gates to encode in different bases	-	-	H	SH	H	-	SH	H
Bob's gates to measure in different bases	-	HS^\dagger	H	HS^\dagger	HS^\dagger	-	H	

Table 4.4: Alice and Bob's gates for the different bits and bases

8 qubits, all initialized to $|0\rangle$, to encode the bits with. She first applies the X gate on all qubits for bit 1 (see table 4.4), transforming their states into $|1\rangle$. She now randomly chooses one of the X , Y and Z bases to encode each bit and subsequently, so does Bob, to measure. We assume no eavesdropping.

The gates that they use for the different bases are given in table 4.4. The Z basis doesn't require any as it is the default in the IBM QC. She uses the H gate for the X basis (transforms $|0\rangle$ into $|+\rangle$ and $|1\rangle$ into $|-\rangle$, the X basis states) and the SH gate (H applied first) for the Y basis (transforms $|0\rangle$ into $|+_i\rangle$ and $|1\rangle$ into $|-_i\rangle$, the Y basis states). To measure in a particular basis, Bob simply applies gates which are the inverse of Alice's (H for the X basis and HS^\dagger for the Y), before finally measuring in the Z basis.

The circuit is shown in fig. 4.1. It is expected that they would agree over the bits for which they chose the same basis. For the rest of them, Bob's is a random result (see table 4.5).

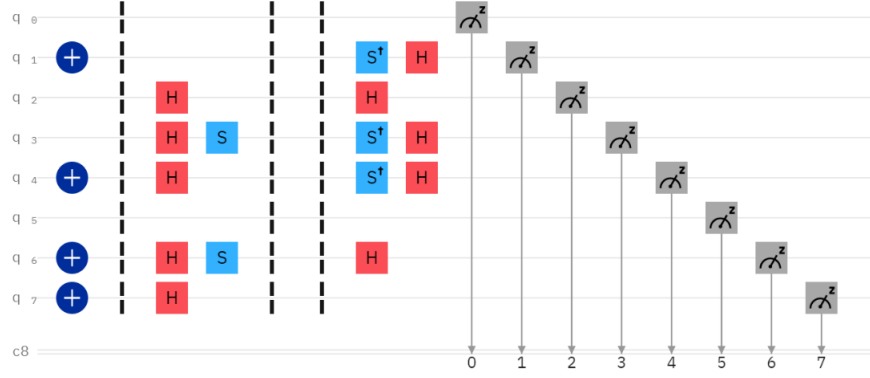


Figure 4.1: Our circuit (Eve absent)

Qubit	Expected result	Qubit	Expected result
q_0	0 (100%)	q_4	0 (50%), 1 (50%)
q_1	0 (50%), 1 (50%)	q_5	0 (100%)
q_2	0 (100%)	q_6	0 (50%), 1 (50%)
q_3	0 (100%)	q_7	0 (50%), 1 (50%)

Table 4.5: Expected result for each qubit after measurement

Running this circuit on the `ibmq_qasm_simulator` (9999 shots) gave the histogram plot in fig. 4.2. The experimental results are thus very close to the expected. The two identify the qubits q_0 , q_2 , q_3 and q_5 as those for which they both chose the same basis and go on to complete the rest of the protocol.

For the same example, consider now an eavesdropper Eve present, intercepting some of Alice's qubits to make her own measurements on them. She randomly chooses a basis for each qubit from X , Y and Z , applies the corresponding gate before measuring and the inverse after, all before Bob receives it. Suppose she intercepts the qubits q_2 , q_3 , q_5 and q_7 , measuring them in the bases X , X , Z and Y , respectively (see fig. 4.3 for the circuit).

The cases for which Alice and Bob don't choose the same basis (like q_7),

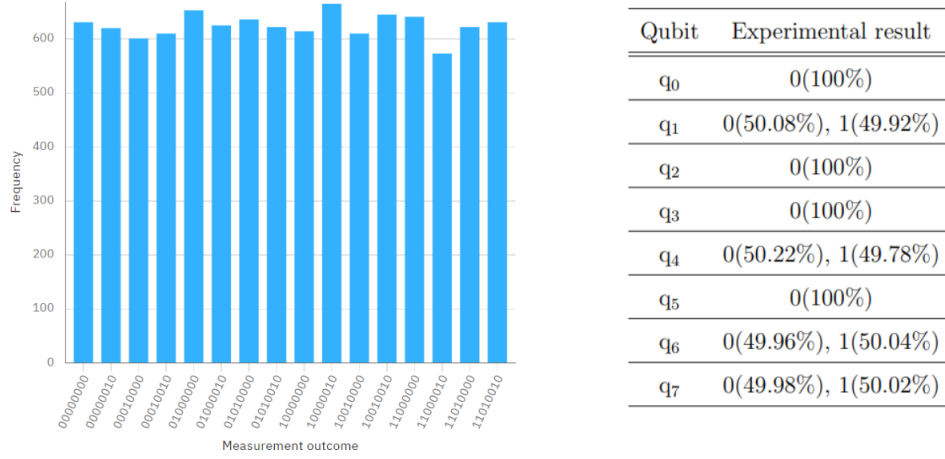


Figure 4.2: Histogram plot with the experimental result for each qubit calculated

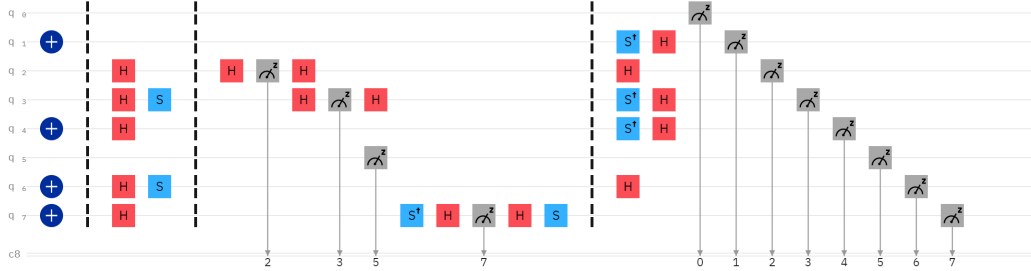


Figure 4.3: Circuit in the presence of Eve

they anyway discard so we need not consider them. We expect that whenever Eve chooses the same basis as them, she causes no error but when she doesn't, it randomizes Bob's result (the case for q_3). The histogram plot in fig. 4.4 obtained from running our new circuit on the `ibmq_qasm_simulator` (9999 shots) meets these expectations precisely. If Bob were to measure the bit 1 for q_3 (Alice's was 0) and reveal it to Alice, they could successfully establish that Eve is present.

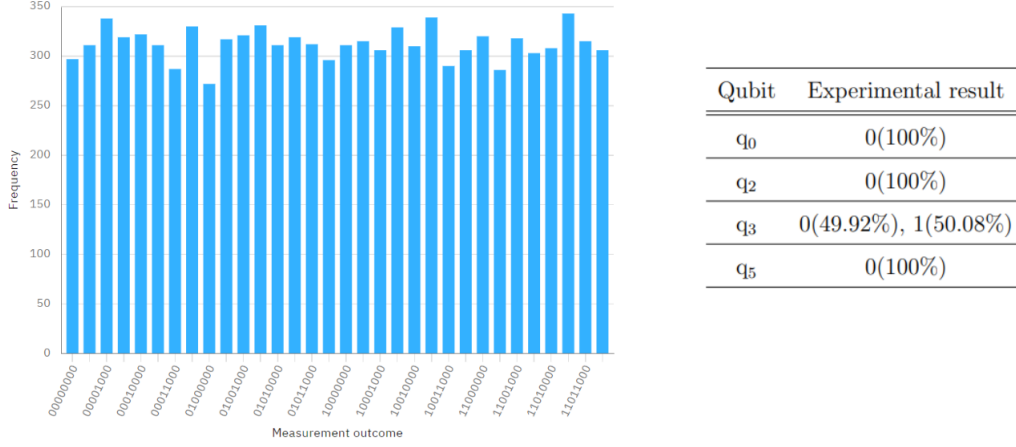
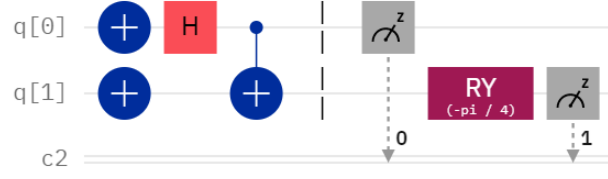


Figure 4.4: New histogram plot and the experimental values of the qubits

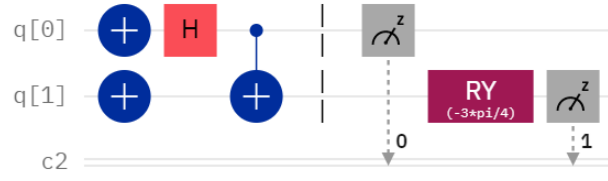
4.2.2 E91

We consider four circuits, one for measuring each term in the equation for E (see fig. 4.5). The qubits $q[0]$ and $q[1]$ are first prepared in the singlet state in each circuit, before being measured in different bases by Alice and Bob, respectively. Angle $a_1 = 0$ corresponds simply to the Z basis while $a_3 = b_2 = \frac{\pi}{2}$ corresponds to the X basis. For the basis corresponding to $a_2 = b_1 = \frac{\pi}{4}$, one needs to apply $R_y(-\frac{\pi}{4})$, a rotation in the Bloch sphere of $\frac{\pi}{4}$ about the y -axis which would rotate a state along a_1 to align with the z -axis, before the measurement in the default Z basis. For much the same reason, one applies $R_y(-\frac{3\pi}{4})$ for $b_3 = \frac{3\pi}{4}$ before measurement.

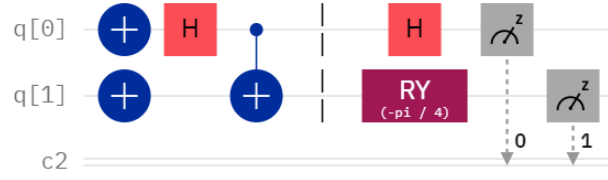
The circuits were run on ibmq_manila (9999 shots each) and the histogram plots obtained are shown in fig. 4.6. It is found from the plots that $\langle a_1 b_1 \rangle = -0.6157$, $\langle a_1 b_3 \rangle = 0.6061$, $\langle a_3 b_1 \rangle = -0.6063$ and $\langle a_3 b_3 \rangle = -0.6331$.



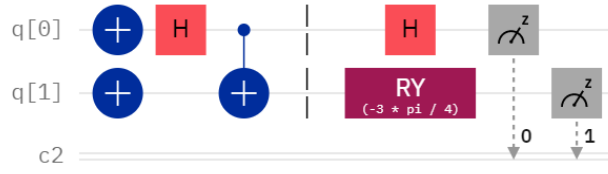
(a) Circuit I: To calculate $\langle a_1 b_1 \rangle$



(b) Circuit II: To calculate $\langle a_1 b_3 \rangle$

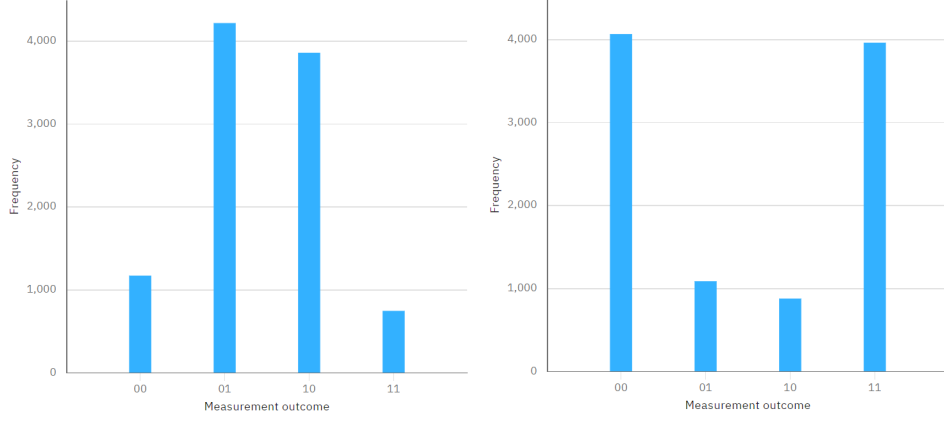


(c) Circuit III: To calculate $\langle a_3 b_1 \rangle$

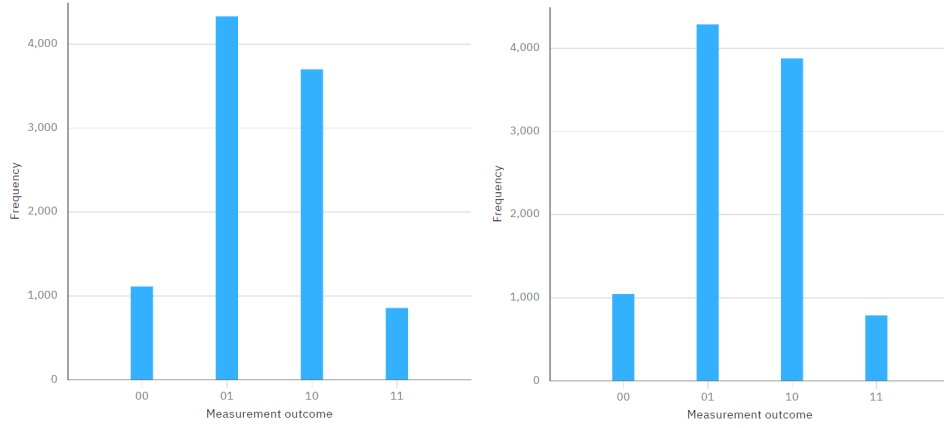


(d) Circuit IV: To calculate $\langle a_3 b_3 \rangle$

Figure 4.5: Circuits to calculate the terms in the equation for E



(a) Plot for circuit I; $\langle a_1 b_1 \rangle = -0.6157$ (b) Plot for circuit II; $\langle a_1 b_3 \rangle = 0.6061$



(c) Plot for circuit III; $\langle a_3 b_1 \rangle = -0.6063$ (d) Plot for circuit IV; $\langle a_1 b_1 \rangle = -0.6331$

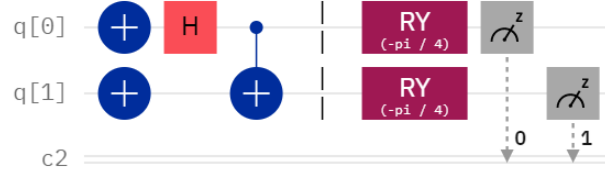
Figure 4.6: Histogram plots for the different circuits

Calculating E for these values for the terms gives

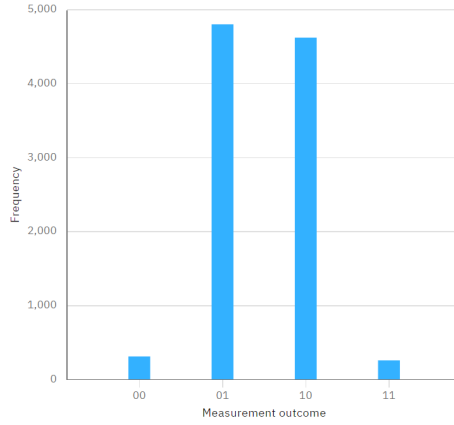
$$E = \langle a_1 b_1 \rangle - \langle a_1 b_3 \rangle + \langle a_3 b_1 \rangle + \langle a_3 b_3 \rangle = -2.4612$$

Though it is not quite close to the maximal violation of $-2\sqrt{2} = -2.8284$ that

we expect of the singlet state, our E does violate the CHSH inequality and the qubits are therefore entangled. This indicates that the eavesdropping, if at all there was, wasn't significant and the measurement results of Alice and Bob would still be significantly anti-correlated for the instances in which they chose the same basis. The histogram plot for the circuit in fig. 4.7 shows just that for $a_2 = b_1 = \frac{\pi}{4}$. The error in E in the present case is likely to be due to errors in implementation of the gates for the different circuits.



(a) Circuit for $a_2 = b_1 = \frac{\pi}{4}$



(b) Histogram plot shows $P(|01\rangle \text{ or } |10\rangle) = 0.9426$

Figure 4.7: Circuit (run on ibmq_manila with 9999 shots) and histogram plot for $a_2 = b_1 = \frac{\pi}{4}$

Entangled pairs	1	2	3	4	5	6	7	8
Alice's bits	0	1	0	0	1	0	1	1
Alice's measurement basis	Z	Z	X	Z	X	Z	X	Z
Eve's attack		Z	Z		X		X	
Bob's measurement basis	X	Z	X	X	Z	X	X	Z
A and B chose the same basis?	No	Yes	Yes	No	No	No	Yes	Yes

Table 4.6: Alice, Bob and Eve's bases for the BBM92 protocol

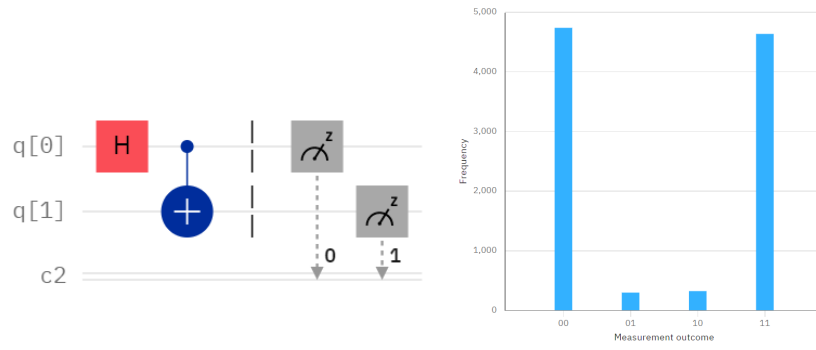
4.2.3 BBM92

Suppose Alice and Bob share 8 pairs of entangled qubits in the state

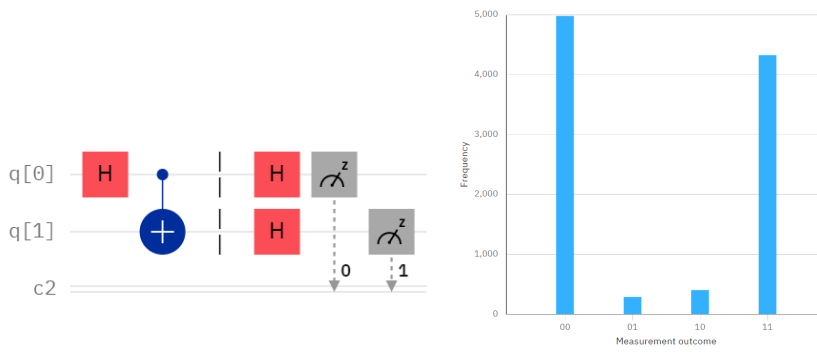
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

They randomly choose the Z or the X basis for measurement for their qubit of each entangled pair (see table 4.6) and get overwhelmingly correlated results whenever they choose the same basis for the entangled qubits that Eve doesn't intercept (see fig. 4.8). All circuits were run on ibmq_manila for 9999 shots each. The results for which Alice and Bob choose different bases, they anyway discard so we need not consider them. For those that Eve does intercept, their measurements are still correlated and she goes undetected whenever she chooses the same basis as them. (See fig. 4.9 for the case they all choose the X basis). But this isn't the case when she chooses a different basis (Alice and Bob's results become uncorrelated, see fig. 4.10).

If Eve were not present, Alice and Bob's results would have all been almost perfectly correlated for the entangled pairs 2, 3, 7 and 8. In the present scenario however, they would find the pair 3 to give uncorrelated



(a) Both measure in the Z basis



(b) Both measure in the X basis

Figure 4.8: Almost perfect correlation for the same measurement basis when Eve absent

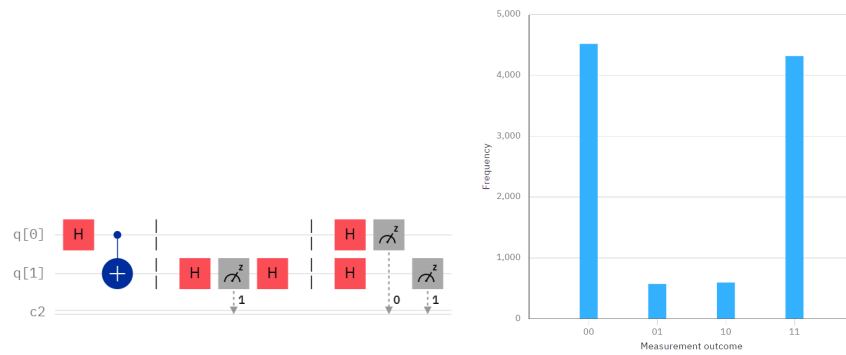
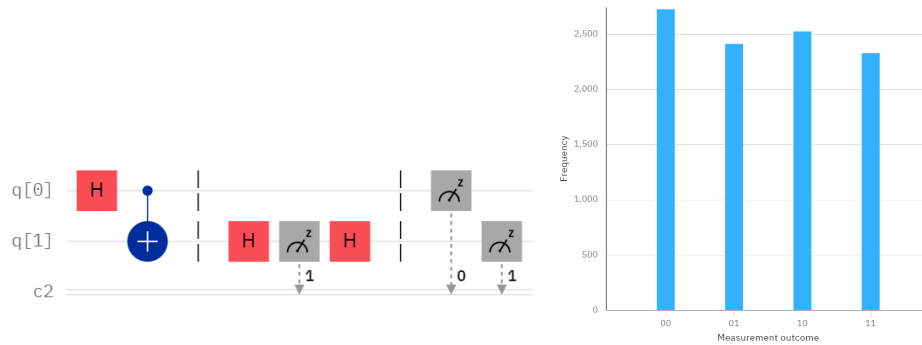
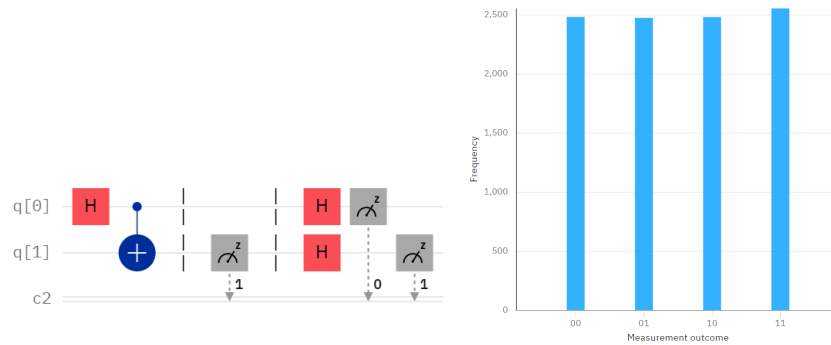


Figure 4.9: Measurements still correlated when they all choose the X basis



(a) Alice and Bob measure in the Z basis but Eve in the X



(b) Alice and Bob measure in the X basis but Eve in the Z

Figure 4.10: Uncorrelated results whenever Eve chooses a different basis

results (see table 4.7) if they were to reveal their measurements for this pair over a public channel and they could thus potentially establish the presence of Eve.

Entangled pairs	2	3	7	8
Alice and Bob's results	correlated	uncorrelated	correlated	correlated

Table 4.7: Measurement results uncorrelated for entangled pair 3 due to Eve

4.3 Conclusion and Discussion

We saw why quantum cryptography and quantum key distribution protocols are needed today more than ever. It is, no doubt, very expensive and unfeasible to actually implement these protocols at any appreciable scale at the moment. And it is still very much a challenge to produce, preserve and measure entanglement and to maintain coherence between quantum systems. But with the recent advances in quantum computation and quantum information and the continuous development of and search for more efficient and sophisticated protocols, the future of quantum cryptography looks hopeful.

We have laid out procedures for some of the most discussed and cited quantum key distribution protocols in this report and then have successfully implemented various kinds of circuits for a few of those protocols as a proof of their concept on the IBM QC.

Bibliography

- [1] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.
- [2] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 1984.
- [3] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.
- [4] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell’s theorem. *Physical review letters*, 68(5):557, 1992.
- [5] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

- [6] Samuel L Braunstein and Ady Mann. Measurement of the bell operator and quantum teleportation. *Physical Review A*, 51(3):R1727, 1995.
- [7] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.
- [8] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.
- [9] Artur K Ekert. Quantum cryptography based on bell’s theorem. *Physical Review Letters*, 67(6):661, 1991.
- [10] Hoi-Kwong Lo and Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *science*, 283(5410):2050–2056, 1999.
- [11] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2001.
- [12] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.
- [13] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

- [14] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
- [15] Aakash Warke, Bikash K Behera, and Prasanta K Panigrahi. Experimental realization of three quantum key distribution protocols. *Quantum Information Processing*, 19(11):1–15, 2020.