

# Understanding Quantum Cryptography Through the BB84 Protocol

Siddhant Khera

The Shri Ram School Aravali



Signature of Examiner

# Contents

<b>1</b>	<b>Abstract</b>	<b>3</b>
<b>2</b>	<b>What is Superposition?</b>	<b>4</b>
2.1	Superposition in Classical Physics . . . . .	4
2.2	Quantum Superposition . . . . .	5
<b>3</b>	<b>What are Qubits?</b>	<b>6</b>
3.1	Dirac Bracket Notation . . . . .	6
<b>4</b>	<b>Understanding the Properties of Quantum Superposition</b>	<b>7</b>
4.1	Colour and Hardness Boxes . . . . .	7
4.2	Property 1 . . . . .	9
4.3	Property 2 . . . . .	10
4.4	Property 3 . . . . .	11
<b>5</b>	<b>Breaking the Abstraction: Stern Gerlach Apparatus</b>	<b>12</b>
5.1	Experiment 1: Property 1 . . . . .	14
5.2	Experiment 2: Property 2 . . . . .	14
5.3	Experiment 3: Property 3 . . . . .	15
<b>6</b>	<b>BB84 Protocol</b>	<b>16</b>
6.1	Quantum Part . . . . .	16
6.1.1	Example . . . . .	17
<b>7</b>	<b>Post Processing</b>	<b>17</b>
7.1	Detecting an Eavesdropper . . . . .	18
<b>8</b>	<b>Bibliography</b>	<b>19</b>

# 1 Abstract

Ronald Rivest, one of the inventors of the ubiquitous RSA algorithm and many symmetric encryption in the Handbook of Theoretical Computer Science defined cryptography as “practice and study of techniques for secure communication in the presence of adversarial behavior.” Cryptography has been used throughout history from Caesar Ciphers in Rome to the Vigenere Cipher in Renaissance Italy and the Enigma machine during World War 2. When Alan Turing created the Turing Machine, he fundamentally broke encryption.

In 1976, Martin Hellman and Whitfield Diffie devised a new encryption scheme called ‘public-key encryption’. It revolutionised the field of cryptography and is still being used today. The problem with encryption before this was that the people communicating had to share a ‘key’ to decrypt the messages. If the key being shared was intercepted by an adversarial entity then their entire encryption was pointless.

Public Key cryptography involves 2 keys. One that is shared to the public and the other which is private. The public key is shared while only the recipient has access to the private key. The message is encrypted using the public key while only the private key can decode it. Without the private key, it would take over a few generations for even the most advanced super computers to decrypt it. This encryption model utilizes the fact that it is extremely hard to factor large prime numbers.

The same way Alan Turing and Computers broke pre-modern encryption only to make it more secure than ever. Quantum Computers are here to revolutionise modern encryption. In 1994, a mathematician, Peter Shor created an algorithm for quantum computers that could theoretically break even the most complex encryption algorithms in less than a day. Currently quantum computers aren’t advanced enough to implement this algorithm but if they could, it would mean the death of modern encryption as we know it.

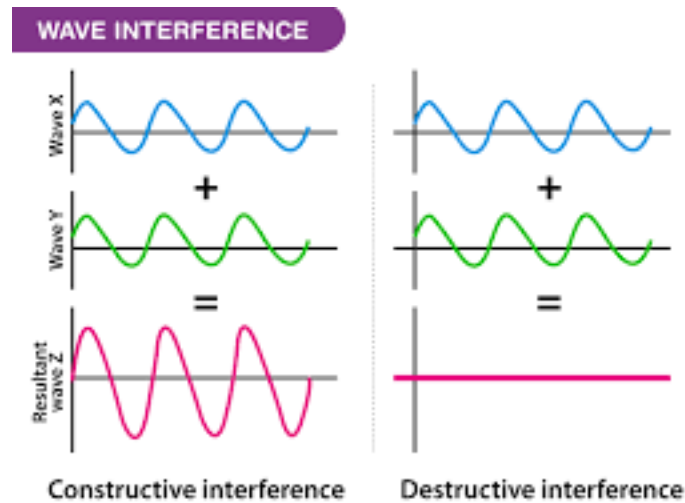
Luckily Quantum Cryptography can solve this problem. We will study BB84 the first Quantum Cryptography protocol created by Charles Bennett and Gilles Brassard in 1984. BB84 solves the problem of sharing secret keys, making encryption methods while using the BB84 protocol virtually impossible to decrypt.

Cryptographic Literature uses 3 people to demonstrate the encryption methods. Alice (A) is receiver, Bob (B) is sender and Eve (E) is eavesdropper.

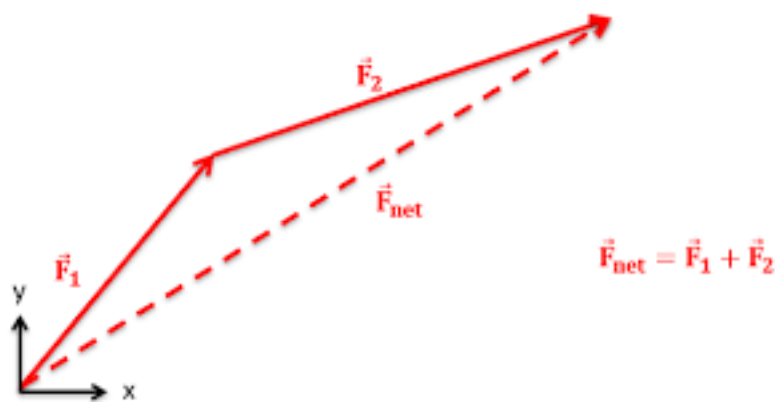
## 2 What is Superposition?

### 2.1 Superposition in Classical Physics

In classical physics, superposition refers to describe when two physical quantities are added to make another third physical quantity which is entirely different from both the original quantities. Superposition is a property for all linear systems such as Waves, Force, Momentum etc. An example of classical superposition properties would be destructive and constructive interference shows by waves.



The Vector addition of Forces is also a classical superposition property.



## 2.2 Quantum Superposition

Certain Small Objects such as electrons and photons possess features of both waves and also that of particles, these objects are said to be quantised. As we have learned in ISC, these objects that have show phenomena associated with both linearity and particles are said to possess wave particle duality. Quantum superposition is a phenomena present in systems have show wave-particle duality and other non classical effects.

We first need to understand what quantisation is. We would expect that a cricket ball could take any arbitrary value of Kinetic Energy from  $0 \rightarrow \infty$ . This is in fact not true, according to quantum mechanics, the energy of a cricket ball is quantised and it can only take up certain values and nothing in between. A specific example of this is when energies can have only integral values  $E = 1, 2, 3, 4 \dots$  and nothing in between. The gaps in these are too small to be measured on the macroscopic level therefore we ignore them while learning classical mechanics.

To understand quantum superposition we will use abstraction and look at coins. A coin thrown in the air has a 50/50 probability of landing as either heads or tails. While the coin is in the air, what state is it in? Is it heads or tails? The “state” refers to a particular way to describe a system. In this instance, while the coin is in the air, it is neither heads nor tails. It exists as a combination of heads and tails, called a superposition. The moment we measure it, it collapses from a state of superposition and takes the value of either heads or tails. Quantum Systems are special because they exist in a superposition of these states (Often multiple states). The outcome of the measurement is to quantify some definitive state with a given probability. After the measurement, the state collapses and it becomes a definite non-superposition state and it stays that way.



### 3 What are Qubits?

In classical computing, information is represented in the form of bits which take the value of either 0 or 1. All the information on a computer can be encoded as a mix of 1s and 0s.

Qubits or Quantum Bits are special because they exist in a superposition of both 0 and 1. Qubits are in a superposition of 2 different states, they collapse when measured into either a 0 or 1.

#### 3.1 Dirac Bracket Notation

In order to work with qubits, we first have to learn how to represent them. There are many ways to mathematically represent Quantum Mechanical States but the easiest way is by using DIRAC or ‘Bra-Ket’ notation. The ‘Bra-Ket’ notation encloses the right half on an angled bracket called “ket”. A Qubit,  $|\psi\rangle$  can be represented as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The Qubit  $|\psi\rangle$  is in a superposition of both  $|0\rangle$  and  $|1\rangle$ .

$\alpha$  and  $\beta$  represent the amplitudes of the states. They are usually complex numbers, but to understand them, we can take them as real. Amplitudes allow us to mathematically represent all the possible superpositions.

Amplitudes are very important because they tell the probability of finding the particle in a particular state. The probability of measuring  $|0\rangle$  is  $|\alpha|^2$  while the probability of measuring  $|1\rangle$  is  $|\beta|^2$ . Since the probability of observing all the states must add up to 1, the amplitudes must obey this formula.

$$|\alpha|^2 + |\beta|^2 = 1$$

This formula is called the “Normalisation Rule”.

For example, if we take a coin with 50/50 chance of getting heads or tails, then we can represent it as a quantum system as.

$$|coin\rangle = \frac{1}{\sqrt{2}}(|Heads\rangle + |Tails\rangle)$$

The probability of getting either heads or tails is  $|\beta|^2 = (\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$

## 4 Understanding the Properties of Quantum Superposition

Normally, one would have to explain certain quantum phenomena and then proceed to use them to explain the properties of quantum superpositions. This would serve to confuse most people and make it harder for them to gain intuition about this subject.

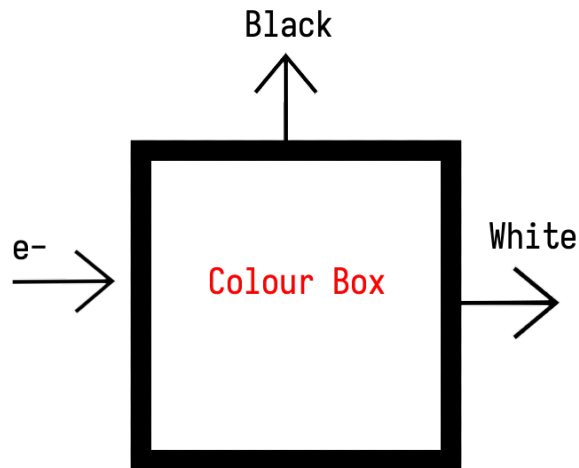
For this reason, I am going to use 2 properties of electrons, **Colour** and **Hardness**. These properties don't exist but to avoid distracting you by preconcieved notions we are going to use abstraction and assign electrons ambiguous, quantum properties of colour and hardness.

Let us say that every electron exists as either Black or White. There are no electrons of another colours. As for their hardness, electrons are either Hard or Soft. These are both binary properties, it is either this or that. It cannot be anything else.

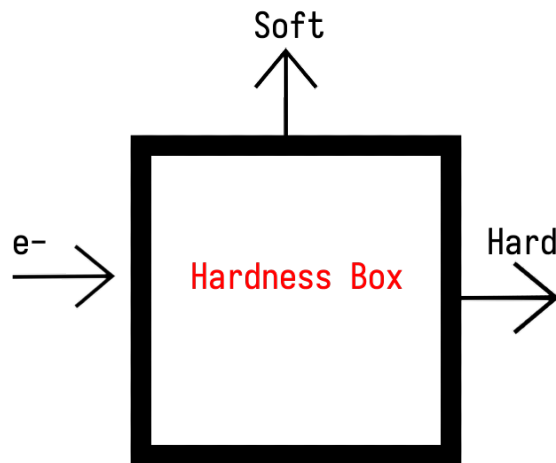
### 4.1 Colour and Hardness Boxes

It is possible to build a device to measure if an electron is Black or White or if it is Hard or Soft. Since Colour and Hardness aren't real properties of electrons, this box is a black box where we don't need to know its inner working to experiment with it.

The Colour Box distinguishes between White and Black electrons by changing their directions, the White electrons come out of one side of the box and Black electrons come out of the other side of the box.



The same way the Hardness Box distinguishes between Soft and Hard electrons. Hard electrons come out of one side and Soft electrons out of the other.



First let's give the electrons the property of being completely random. The electrons exist in a superposition of Hard and Soft or Black and White. Let these properties have similar probabilities. (A random electron has a 50/50 chance of being either White or Black, and it has a 50/50 chance of being Hard or Soft)

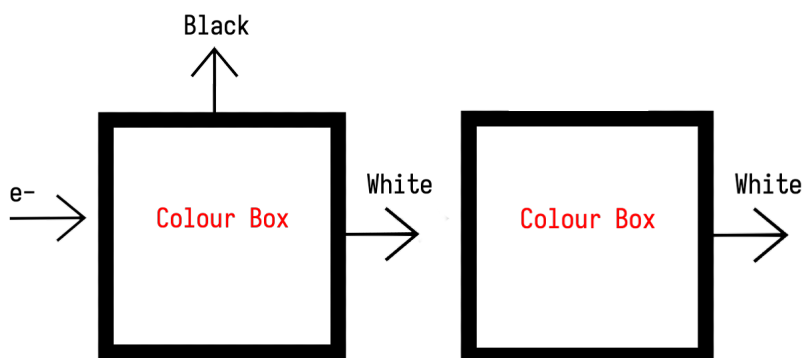
$$\therefore |electron\rangle = \frac{1}{\sqrt{2}}|Soft\rangle + \frac{1}{\sqrt{2}}|Hard\rangle$$

$$\text{Likewise, } |electron\rangle = \frac{1}{\sqrt{2}}|White\rangle + \frac{1}{\sqrt{2}}|Black\rangle$$



## 4.2 Property 1

The first property is that once an electron is measured, as a colour or hardness, it remains that colour of hardness. For example if he take an electron and pass it through the Colour Box. If it is White, we will pass it through another colour box. This electron will have collapsed from it's super position and will always come out as White. Only 50% of the electrons reach the second box, but we are disregarding the Black electrons that do not.



This is True for all scenarios and all Quantum Properties. If through all the electrons that come out as Black into another colour box, they will remain Black. The same thing will apply for Hard and Soft electrons with the Hardness Box.

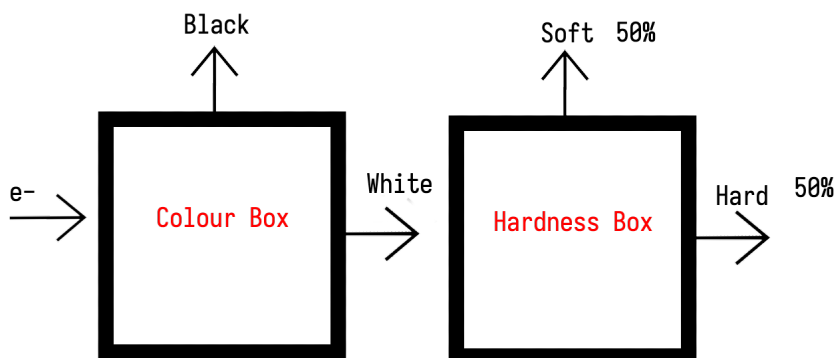
At this point, your intuition might be working against you. You may fallaciously be thinking that the electron is already Black or White, before we measure it it isn't in superposition of both Black and White. We simply don't know whether it is Black or White. Unfortunately, this is **absolutely wrong**.

We know this is wrong because if we take 2 exactly identical electrons and pass it through a Colour Box, they might collapse to either Black or White. When it is in superposition, it is as if is a coin flipping in the air. The coin flipping is neither Heads or Tails, the same can be said about these Quantum Properties in a superposition. The other properties we are going to look at will confirm this fact.

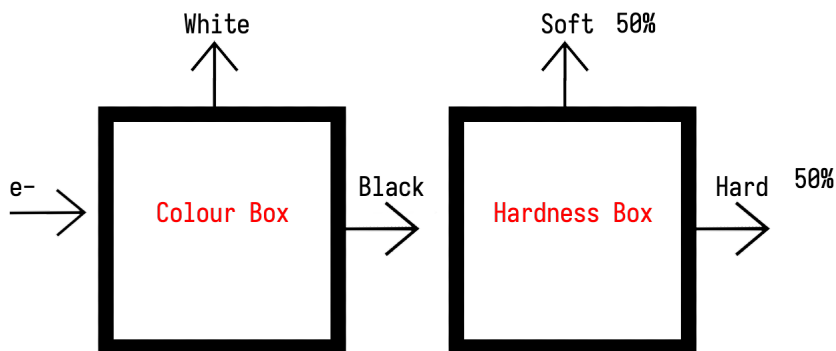
### 4.3 Property 2

Quantum Property of Colour has no bearing or correlation with the Quantum Property of Hardness. If we take a White or Black electron and pass it through a hardness box, it will come out as Hard half the time and Soft the other half.

We can confirm that the property of Colour is not related to the Property of Hardness.



We are disregarding the Black electrons in this instance



We are disregarding the White electrons in this instance

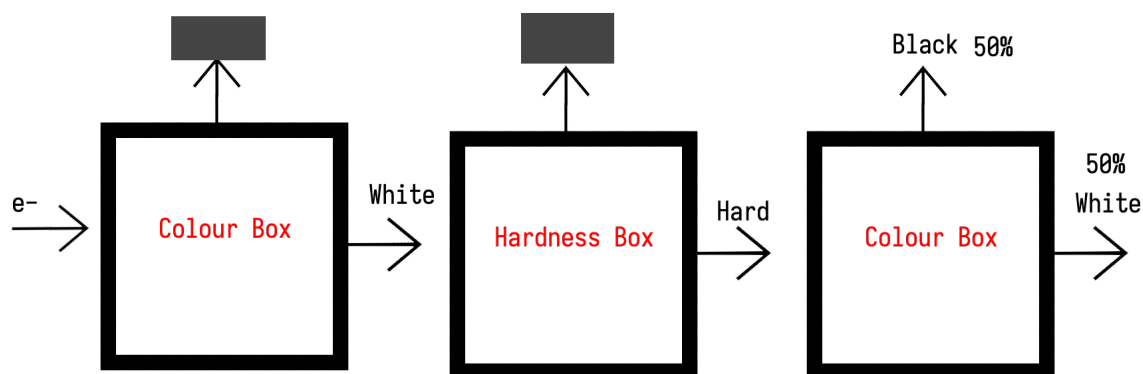
This property can also be seen the other way around. If we take a Hard or Soft electron and put it through a coloured box, it has an equal chance of being both Black or White.

## 4.4 Property 3

This Property is the one that forms the basis for the BB84 protocol and what somewhat proves the existence of a superposition. There are many other experiments and properties that give a more concrete proof of superposition but they involve mirrors and reflections, something that will complicate this topic too much.

As we know in from Property 1, once an electron has collapsed from Superposition into a given state, it stays in that state. The second Property tells us that one quantum property is not related to another. What will happen if we take a Colour Box and send only the White electrons to a Hardness Box and then after measuring the electrons as either hard or soft, we send them back to another Colour box.

Intuitively, we may think that since the superposition has collapsed, we should get back a White electron, but this is not the case. We get Black and White electrons with an equal frequency.



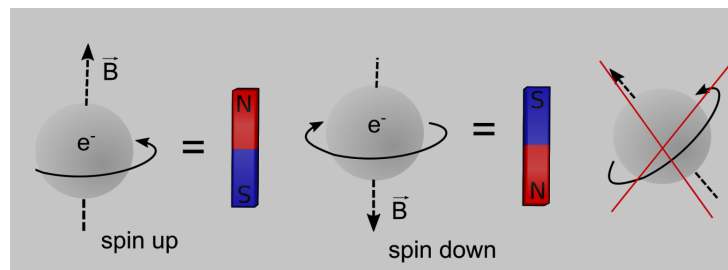
We are initially disregarding the Black electrons and then the Soft ones.

There are many more properties of objects in quantum superpositions, but they since they are not needed to understand the BB84 protocol, they will not be covered.

## 5 Breaking the Abstraction: Stern Gerlach Apparatus

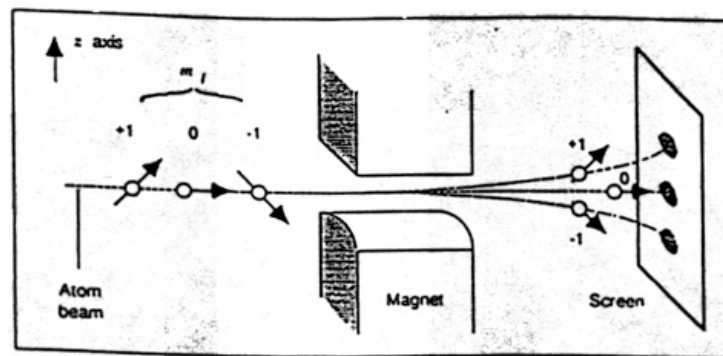
The properties of Colour and Hardness do not actually exist in electrons, but have been used to make this topic more approachable. We will continue to use this abstraction while explaining the BB84 protocol but we will also learn about their actual counterparts, the quantum phenomena of spin.

Electrons possess a binary property of spin. We can visualise electrons as rotating around their own axis. We know that moving charges create a magnetic field according to the right hand rule. Thus spinning electrons behave a little like magnets.



The Stern-Gerlach experiment used this to demonstrate that the spatial orientation of angular momentum is quantised. The Stern-Gerlach Apparatus or SGA shot silver atoms through an inhomogeneous magnetic field and the electrons were deflected based on their spin and hit a photoelectric screen. We can use this deflection from the angular momentum to measure an electron's spin state.

The experiments that were conducted reflect the properties that we just discussed in the previous section.



Classically, horizontally oriented bar magnets in a vertical magnetic field would land at the centre of the screen, but since spin can only be measured as up or down, they cannot possibly land at the centre. They will either land on the top or bottom with a 50% probability.

Therefore a Horizontal Spin can be represented as

$$\begin{aligned} |\leftarrow\rangle &= \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle \\ |\rightarrow\rangle &= \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle \end{aligned}$$

This is non-classical because you cannot add and subtract vertical magnetic field vectors to get a horizontal magnetic vector.

For the spin of an electron, we represent it based on horizontal and vertical lines using the x and z axis.

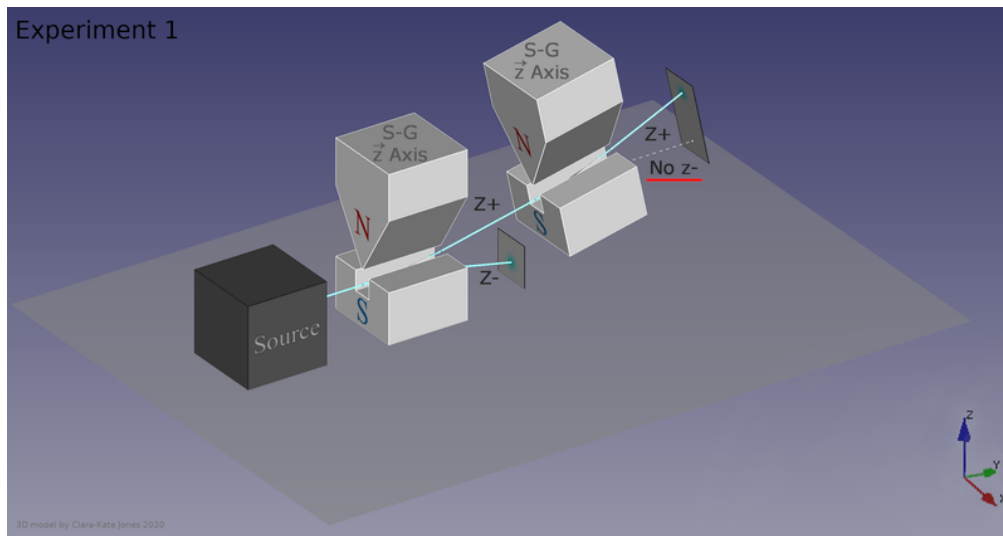
$$\begin{aligned} | + z \rangle &= \frac{1}{\sqrt{2}}| + x \rangle + \frac{1}{\sqrt{2}}| - x \rangle \\ | - z \rangle &= \frac{1}{\sqrt{2}}| + x \rangle - \frac{1}{\sqrt{2}}| - x \rangle \end{aligned}$$

Using simple algebra, we can also rearrange and get the formulas.

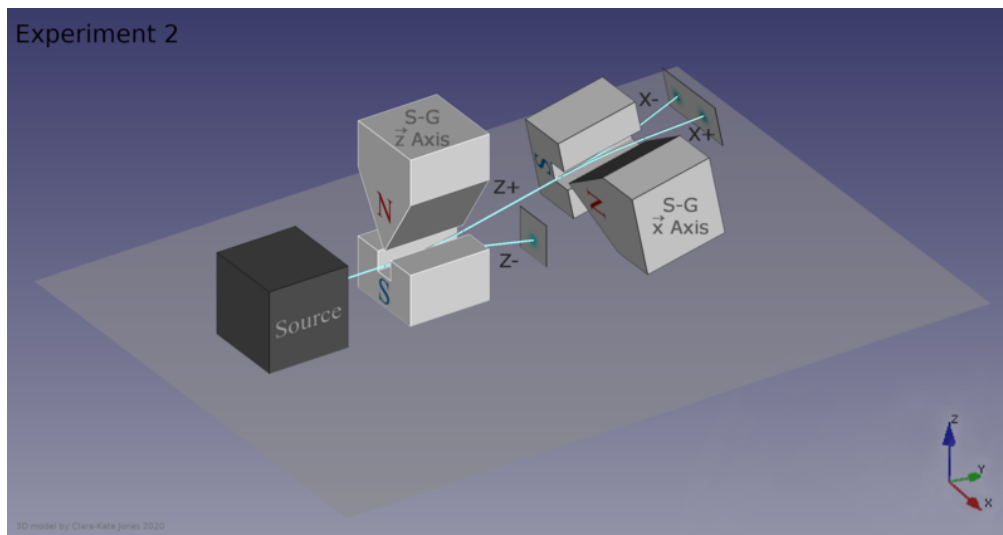
$$\begin{aligned} | + x \rangle &= \frac{1}{\sqrt{2}}| + z \rangle + \frac{1}{\sqrt{2}}| - z \rangle \\ | - x \rangle &= \frac{1}{\sqrt{2}}| + z \rangle - \frac{1}{\sqrt{2}}| - z \rangle \end{aligned}$$

The Stern-Gerlach experiments demonstrated the properties discussed in the previous section. Placing the Stern-Gerlach Apparatus vertically gives us the vertical spin, while placing it horizontally gives us the horizontal spin.

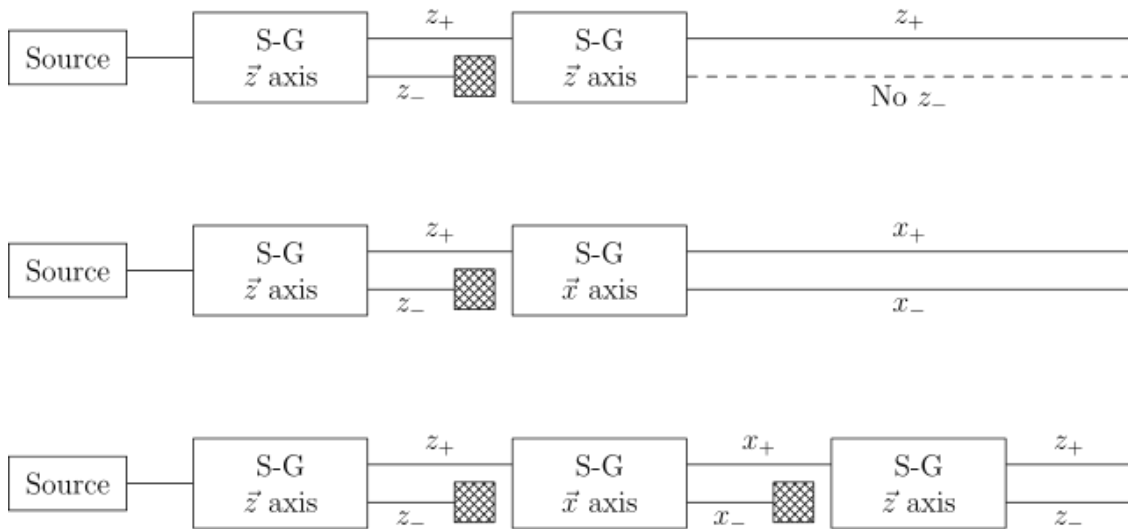
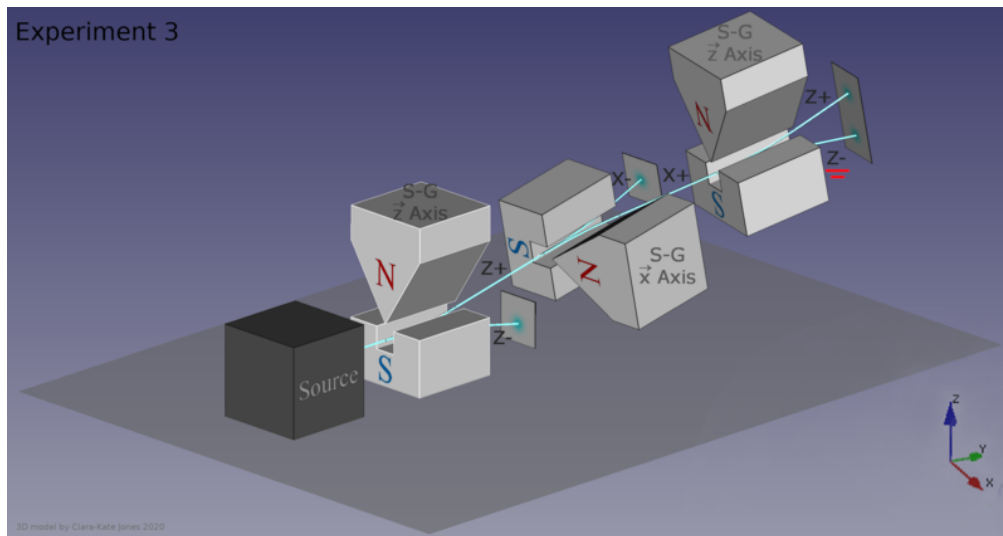
## 5.1 Experiment 1: Property 1



## 5.2 Experiment 2: Property 2



### 5.3 Experiment 3: Property 3



## 6 BB84 Protocol

We will use Colour and Hardness as the Quantum Properties to explain this protocol. Let Colour represent vertical spin and Hardness represent horizontal spin. Therefore the Colour Box is the vertical SGA while the Horizontal Box is the horizontal SGA.

We can pair the BB84 with the Vernam Cipher (One Time Pad) encryption where we use a separate key of either a 0 or 1 with each bit in the code and add it with modular arithmetic. There is a bit in the key for every single bit in the message to be shared, modular arithmetic would mean a 0 in the message and 1 in the key would become 1 and a 1 in the message and 0 in the key would also become a 1. Whereas, two 1s or two 0s would become 0s. The Vernam Cipher is a mathematically perfect cipher. BB48 along with the Vernam Cipher is a theoretically invincible method of cryptography.

Property	Black	White	Hard	Soft
Bit Value	0	1	0	1

### 6.1 Quantum Part

1. Alice randomly chooses either the Colour or the Hardness metric.
2. Alice sends an electron in superposition in the chosen metric, measures the property and records the corresponding bit value.
3. Alice sends the electron to Bob.
4. Bob randomly chooses either the Colour or Hardness metric.
5. Bob measures the spin of the electron and records its corresponding bit value.
6. Repeat

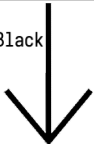


### 6.1.1 Example

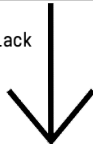
Alice's Metric	Colour	Colour	Hardness	Colour	Hardness
Value Measured	Black	Black	Soft	White	Soft
Bit Value	0	0	1	1	1

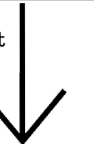
Black




Black




Soft



White



Soft



Bob's Metric	Colour	Hardness	Hardness	Colour	Colour
Value Measured	Black	Hard	Soft	White	Black
Bit Value	0	1	1	1	0

## 7 Post Processing

1. Alice and Bob publicly share which metric they used for each bit measurement, without revealing the actual bits they measures.
2. They discard all the bits measured in different metrics. The bits remaining are kept as the key. As long as Eve (the Eavesdropper) wasn't present, they should have the same keys.
3. Alice and Bob publicly compare a subset of the bits, say 150 out of 1000. If all 150 are the same then it is statistically extremely unlikely that there is an eavesdropper. The remaing 850 becomes the shared key.

In the given example, after processing (ingoring the dropped keys during verification), the secret key should be 011.

## 7.1 Detecting an Eavesdropper

Due to the unique properties of Quantum Computers, we can detect any eavesdropper if present. There is only one way for Eve to figure out the bit being communicated between Alice and Bob, through her own Colour or Hardness Box, before it gets to Bob. Since the metric is not shared during the transmission, Eve must randomly choose a metric.

If Alice and Bob used a different metric during that transmission, the discard of those bits and it does not matter which metric Eve uses.

If Eve chooses the same metric as Alice, she can measure the bit correctly and also not alter the collapsed state. Neither Alice or Bob would be able to detect Eve.

If Eve chooses a different metric but Alice and Bob choose the same metric, then Eve alters the electron and puts it in a state of superposition. There is a possibility that the electron would collapse into a different state than which Alice had sent it in, on Bob's Box.

If Alice and Bob have a different bit value despite using the same metric, they can know that they have an Eavesdropper in between them.

There is a  $\frac{1}{8}$  that Eve will reset the electron back in a state of superposition and Bob will receive a different value than what Alice sent. If we use 10 bits for verification, there is a 26.4% chance that Eve won't get caught. If we use 20 bits for verification, then there is a 7% chance that Eve won't get caught. If we use 100 bits for verification, then there is a 0.00016% of Eve not being caught.

## 8 Bibliography

- MIT OpenCourseWare 6.453, Fall 2016, Quantum Optical Communication
- MIT OpenCourseWare 8.04, Spring 2013, Quantum Physics I
- MIT OpenCourseWare 8.370.3x Quantum Information Science I, Part 3
- TUDelft OpenCourseWare 6.4.1 The BB84 protocol
- Quantum cryptography: Public key distribution and coin tossing <https://arxiv.org/abs/2003.0655>
- Quantum Computing as a High School Module <https://arxiv.org/abs/1905.00282>
- <https://byjus.com/physics/constructive-interference/>
- Wikipedia Stern Gerlach Experiment
- Coursera Understanding Modern Physics II: Quantum Mechanics and Atoms  
<https://www.coursera.org/learn/understanding-modern-physics-2-quantum-mechanics-and-atoms>
- Wikipedia: Superposition Principal
- <http://mechanicsmap.psu.edu/>
- Wikipedia: Quantum Superposition
- <https://www.istockphoto.com/vector/flipping-a-coin-illustration-gm1124512915-295237245>
- Wikipedia: Cryptography