1. Introduce Quantum Cryptography
   1. BB84 protocol for communication channel
   2. Present technology and limitation of the technology
      1. Cost
      2. Showcase NUS’ idea
   3. Goal of the project
      1. Reduce cost
      2. Improve the representation of the idea
2. Solution
   1. Explain setup
      1. Picture
      2. How to detect eve
      3. Encryption
3. Solution’s hardware
   1. Using Polarizing film
      1. Capacity
   2. Lasers
      1. Reason of laser
      2. Intensity
      3. Focal Lens
      4. Reason for not using quarter wave plate
   3. OPT101
      1. Data: how it works (Intensity graph)
         1. Keep the graph at a linear
         2. PWM laser
         3. Variable voltage laser
      2. Wiring
      3. Brandwidth
      4. Ambient noise (case)
      5. LDR
   4. SG 90
      1. Issues faced
         1. Backlashed
         2. High tolerance (Need more tolerance)
      2. Why this motor
         1. Faster
      3. Able to home to step 0
      4. Fking Cheap
   5. Linear rail
      1. Modular
      2. Easier to assemble
      3. Cost $5
   6. 3D printed parts
      1. PETG
      2. Less brittle
   7. Arduino
      1. Mega, fking cheap
      2. More SRAM
4. Software
   1. Coded in C
   2. Libraries used
   3. XOR encryption
   4. How data transmitted
      1. IR protocol, NEC
      2. No. of bytes
      3. Frequency used
   5. How laser intensity is read for high and low

[] - in-text citation

() - references in the same document

A(1) - appendix reference where “A” is the specific appendix section and (1) is a part with in the section.

| Quantum Cryptography  (SUTD Version) |
| --- |
| Research done by:  Tan Da Yang,Shu Yi, Xing Yi, Hui Juan, Sean Gunawan,  Seow Sin Kiat, Ivan Feng, Christopher |

Content Page

[**Introduction**](#_gi5q7dnqoppq) **5**

[**Appendix A - BB84 Protocol**](#_vb0hpnsdxyc9) **7**

[**Solution**](#_1zqhbpeo9fps) **8**

[**Solution’s hardware**](#_2hjn2pq99dyd) **10**

# Introduction

The rapid growth in networking technology has led to an increase in demand for more secure channels of communication. Sensitive information such as credit card number, personal information need to be protected. [1] For this purpose many encryption techniques have been developed. However, an encryption scheme is only as secure as its key. Currently, the public-key-based key distribution schemes such as the Diffie–Hellman scheme [2] solve the key distribution problem by making computational assumptions such as that the discrete logarithm problem is hard. However, future development in quantum technology could render many of these public-key-based schemes insecure. [3] Thus, there is a rise in implementing quantum mechanics in cryptography. The aim of quantum cryptography is to create an encryption system that is resistant to quantum attacks. Indeed, thanks to the quantum no-cloning theorem [4], it is possible to detect eavesdropping using the laws of quantum physics. In 1984, Bennett and Brassard invented a scheme to distribute symmetric keys securely between two parties. [5] This quantum key distribution (QKD) protocol is known as the BB84 protocol. (For a more detailed explanation of the BB84 protocol, please refer to Appendix A). QKD has also intrigued the general public. There now exist several QKD demonstrations for non-experts which focus on teaching the underlying physics of QKD. [6-11] However, these kits can be very expensive. The commercially available Quantum Cryptography Analogy Demonstration Kit by ThorLab would cost $3,547.21 USD. [12] The Centre for Quantum Technologies in the National University of Singapore (NUS) has also done a hands-on quantum cryptography workshop for pre-university students. [13] Though the out-of-pocket expenses were 450 USD, the optomechanical, optical, and electronic components they borrowed from the optics lab and electronics workshop was approximately 2.5k USD. [13] Furthermore, in the aforementioned workshop, they left an exploitable loophole. They sent multiple photons with the same polarization and the eavesdropper was able to take a fraction of the photons to implement a side channel attack. However, in the original BB84, only a single photon is encoded and the workshop did not illustrate how the two parties can detect the presence of an eavesdropper. Thus, our research aims to achieve the following objectives:

1. Increase affordability of the demonstration kit
2. Remove the need for any lab grade equipments, using only commercial available parts
3. Successful shows how the BB84 protocol can detect the presence of an eavesdropper.

[1] Thambiraja, E., G. Ramesh, and Dr R. Umarani. "A survey on various most common encryption techniques." *International journal of advanced research in computer science and software engineering* 2.7 (2012).

[2] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT–22, no. 6 (1976), pp. 644–654.

[3] Lo, Hoi-Kwong, Hoi Fung Chau, and Mohammed Ardehali. "Efficient quantum key distribution scheme and a proof of its unconditional security." *Journal of Cryptology* 18.2 (2005): 133-165.

[4] D. Dieks, Communication by EPR devices, Phys. Lett. A, vol. 92 (1982), pp. 271–273

[5] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution

and coin tossing,” Theor. Comput. Sci. 560, 7–11 (2014).

[6] D. S. Lemelle, M. P. Almeida, P. H. Souto Ribeiro, and S. P. Walborn, “A

simple optical demonstration of quantum cryptography using transverse

position and momentum variables,” Am. J. Phys. 74, 542–546 (2006).

[7] A. L. P. Camargo, L. O. Pereira, W. F. Balthazar, and J. A. O. Huguenin,

“Simulation of the BB84 protocol of quantum cryptography by using an

intense laser beam,” Rev. Bras. Ensino F ıs. 39, e2305 (2017).

[8] Karl Svozil, “Staging quantum cryptography with chocolate balls,” Am. J.

Phys. 74, 800–803 (2006).

[9] A. L opez-Incera and W. D€ur, “Entangle me! A game to demonstrate the

principles of quantum mechanics,” Am. J. Phys. 87(2), 95–101 (2019).

[10] A. Kohnle and A. Rizzoli, “Interactive simulations for quantum key distribution,”

Eur. J. Phys. 38, 035403 (2017).

[11] S. DeVore and C. Singh, “Interactive learning tutorial on quantum

[12] "Quantum Cryptography Analogy Demonstration Kit", *Thorlabs.com*, 2021. [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup\_id=9869. [Accessed: 09- Jul- 2021].

[13] A. N. Utama, J. Lee, and M. A. Seidler, “A hands-on quantum cryptography workshop for pre-university students,” *American Journal of Physics*, vol. 88, no. 12, pp. 1094–1102, 2020.

# Appendix A(1) - BB84 Protocol

In this section we will give a more detailed description of the BB84 Protocol. The protocol generates a symmetric encryption key between two parties, usually called Alice and Bob and the eavesdropper is usually called Eve.

| Pre execution:  Alice and Bob need to agree on two sets of orthogonal polarisation basis.  For the purpose of the illustration, an example of the two sets of basis could be {|H>,|V>} and {|+>,|->}.  Alice and Bob also need to agree on the representation of the bit for each state vector.  For example, the state vectors |H> and |+> will represent bit 1. Whereas, the state vector |V> and |-> will represent bit 0. | |
| --- | --- |
| Alice’s part of the protocol  Alice generates a random sequence of bits where and a random sequence of where to denote the polarisation basis used. | Bob’s part of the protocol  Bob generates a random sequence where of polarised measurement basis to measure the incoming photons in sequence where  Bob then sends Alice Y through a classical channel. |
| Alice’s part of the protocol  Alice will compare the elements in X and Y and create a sequence Z where  Alice then communicates Z to Bob through a classical channel.  Alice will edit the sequence A by keeping and removing . | Bob’s part of the protocol  Bob will use Z to edit the sequence B by keeping  and removing . |
| By this step, both sequences of A and B will be identical and thus Alice and Bob would have a shared sequence of bits as their encryption key. But before using the sequence, they will need a validation process. | |
| Alice’s part of the protocol  Alice will take a fraction of the established sequence and send it to Bob through a classical channel. | Bob’s part of the protocol  Bob will compare the fraction with the same fraction of his sequence to see if it is a match. Bob will communicate whether they are matched through a classical channel. If they are matched, they would have a high confidence that there is no eavesdropper. |

The process is illustrated in Figure A(1)-1.

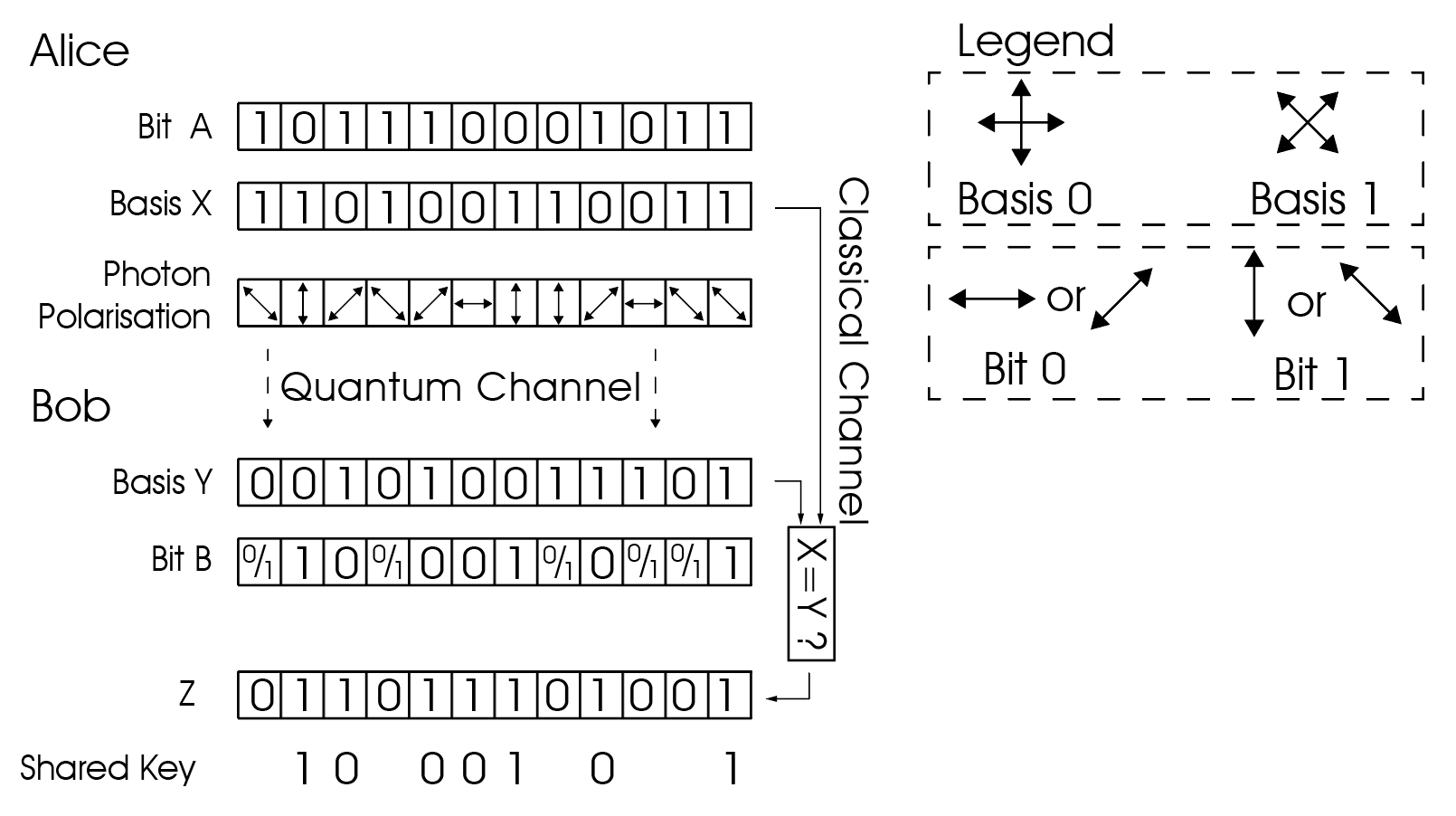


Figure A(1)-1

We will now show what happens if Eve is listening in the quantum channel.

Since you can never clone quantum information, Eve would need her own sequence of polarised measurement basis to listen to the channel. For example, if Eve measured a 0 bit using the basis 0 from the legend above, there is no way of knowing Alice’s bit. Alice could be sending |V>, |+>, |-> with equal probability for each option. Therefore, Eve would have to make a random guess with a probability of ⅓ of being correct. Let’s say Alice sends in |+> and Eve guess Alice send |V> and sends |V> to Bob and Bob used |+> to measure and get a 0 bit. When Bob communicate that he used |+> and Alice would have told Bob to keep the bit. When they chose that bit to compare and realise Bob got a 0 bit instead of 1, Alice and Bob would have a mismatched bit and be able to detect the presence of Eve, assuming there is no noise in the quantum channel.

Though someone may claim that there is a chance that Eve hides herself. We can use statistics to prove that the chance is very low. We can use the complement method to get the answer.

P(Eve hides herself in one bit)

= 1- P(Eve is discovered)

= 1-P(Eve guessed wrongly and the bit is kept and measured)

= 1-P(Eve guess wrongly)P(Eve’s bit is kept)P(Eve’s bit is measured)

= 1-(2/3)(1/2)(v/N) where v is the size of checking bits and N is the size of the total bits kept

P(Eve hides herself perfectly in n bits)

= [P(Eve hides herself in one bit) ]^n

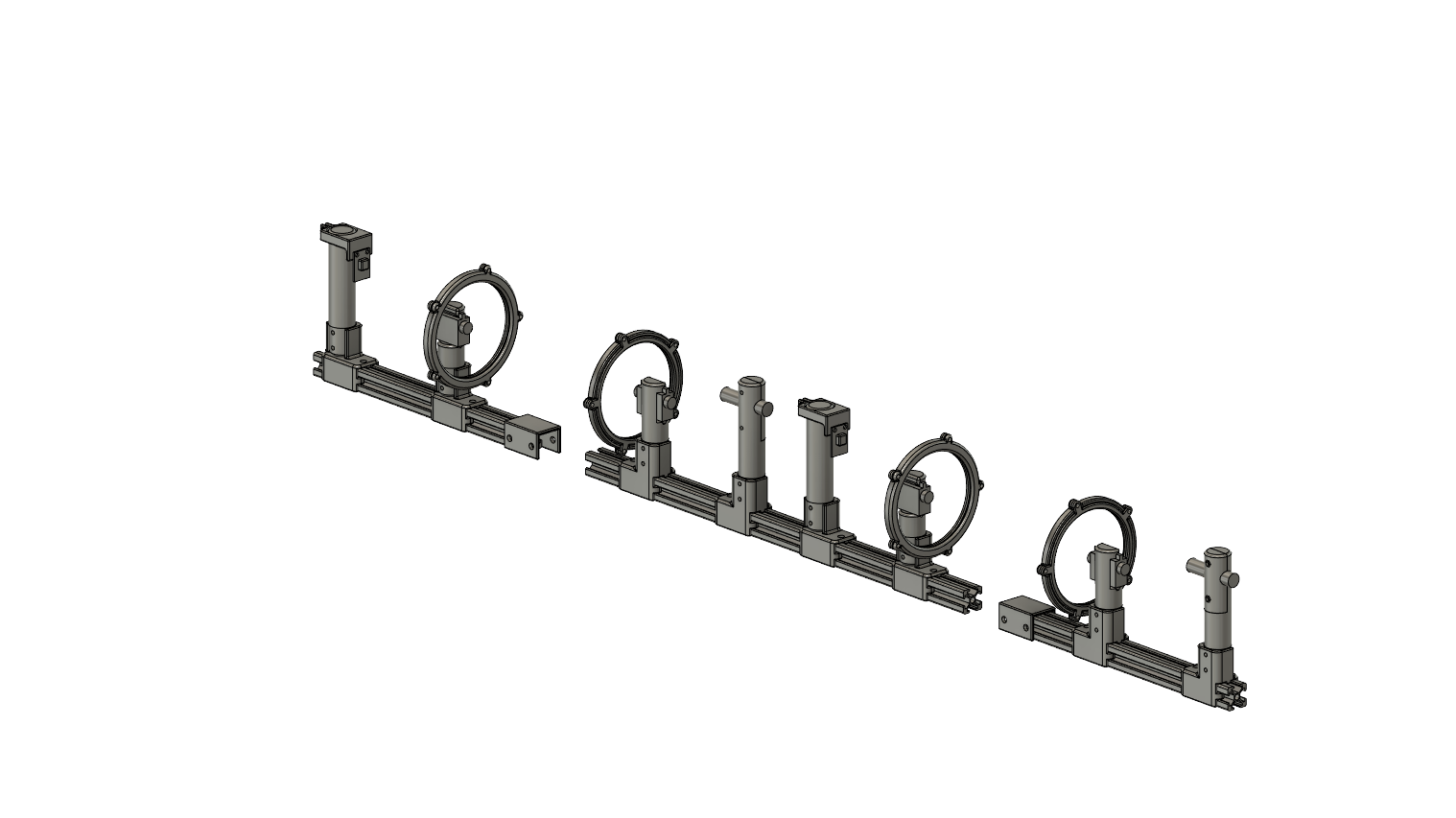
= [1-(2/3)(1/2)(v/N) ]^n

v < N <=n

The expected number of bits kept in n trials using binomial distribution is n/2. So we can simplify that in a long run, for Eve to continuously hide herself

# Solution

To keep the price of the product down, lower-cost components were utilized. The device is designed to be modular, using a 20mm x 20mm aluminum profile as the foundation. Individual sections are 3D printed and fitted onto an aluminum profile. Alice, Bob, and Eve are modulars that are self-contained and independent of one another. The solution works with or without an eavesdropper as the modules are controlled by separate microcontrollers..



Eve, an eavesdropper, is built between Alice and Bob to replicate the notion of quantum cryptography in a real-world scenario. Eve intercepts the photon Alice sends out and delivers the anticipated photon to Bob in an attempt to forecast its polarization as a single photon extinguishes when collided with an obstruction. In this scenario, Eve receives the photon sent by Alice and sends a new photon to Bob. As a result, a photon's function is replicated to simulate quantum cryptography.

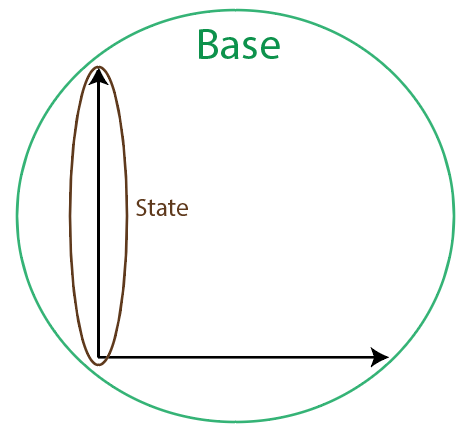
The quantum channel is used for key transmission, while the classical channel is used for the rest of the communication. Bob and Alice will never disclose the state (2) they transmit or receive in. Alice emits a photon with a random polarization, which Bob reads with a random polarization. Through the classical channel, Bob transmits Alice the base (1) of the polarisation he reads in the quantum channel. Alice compares Bob's base and advises him which bit he should accept as the secret key for their encryption. A portion of the key is utilized to compare the key's validity. If one or more bits in the comparison are found to be erroneous, the presence of Eve will be obvious.

If the system determines Eve's existence, it will flag (3) her and constantly reconstruct a new secret key until a safe key is achieved. The communication channel between Alice and Bob will be activated after a secure key is established. With the protected key, Alice and Bob will encrypt and decode communications using XOR encryption.

There are two drawbacks to the solution. If Eve is able to fully anticipate the polarisation of the photon delivered by Alice, the system will be unable to detect her existence. As a result, no safe encryption key is generated. Moreover, the solution's construction is flawed, and it can only read one side's classical channel. Eve can only read Bob or Alice’s classical transmission.

Keyword:

1. Base: Base refers to the coordinate system used. Multiple coordinate systems can be used for polarisation.
2. State: State refers to the axis of the basis.



1. Flag: Flag refers to the notice given by the system to the user when an unpredicted situation occurs.

# Solution’s hardware

The research's major objective is to reduce the cost of the solution thus understanding quantum physics and how hardware works is critical to the project's success. This section will contain the hardware comparison and its purpose.

## Components used in this prototype:

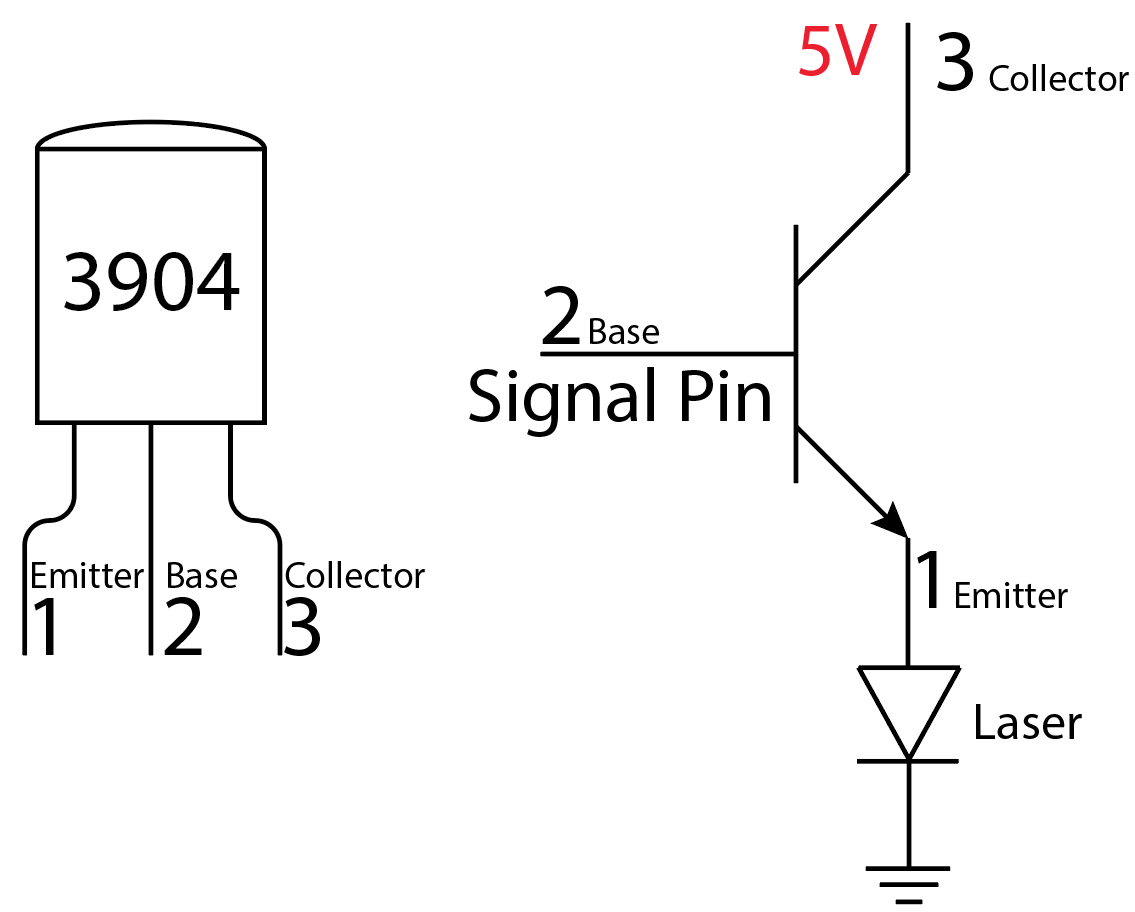
| Components | Quantity | Price (SGD)  (Last Check: 10/09/2021) |
| --- | --- | --- |
| Laser | 2 | 11.81 |
| Reflective polarising film | 4 Cut Out | 17.24 |
| OPT101 | 2 | 2.89 |
| PETG Filament | 2 Rolls | 26.9 |
| IR Transmitter | 2 | 10 |
| IR Receiver | 3 |
| SG90 Motor | 4 | 18.9 (for 10) |
| Arduino Mega | 3 | 10 |
| Batteries | 12 AA | 12.5 (for 6) |
| Wires | lots | 6 per lot |
| Dupont connector | lots | - |
| 3904 Transistor | 2 | 0.66 |
| 150nF Ceramic Capacitor | 2 | 0.79 |
| 0.1µF Electrolyte Capacitor | 2 | 0.43 |
| 100Ω Resistor | 2 | 0.15 |
| 10kΩ Resistor | 2 | 0.22 |
| Solder | - | 29.4 |
| Stripboard/ PCB/ | - | 10 |
| Total Estimate: | | ~SGD 226.48 |

## Linear polarising film

A linear polariser polarises light into a specific polarisation by blocking out or reflecting light that is not orthogonal to its orientation. Reflective polarisers, dichroic absorptive polarisers, and Birefringent polarisers are the three types of linear polarisers you may find in the market. The solution uses reflective polariser as it can be purchased easily at an affordable price. Reflection polarisers contain many strips of wires with diameter measured in nanometers. These wires reflect any light that is parallel to its orientation. However, there is a limit to how much light can be reflected. If the intensity of the light is too great, it will sever the wires in the linear polariser shown in the image below. With a polarising film, refraction within the polariser is insignificant enough to present an issue with the prototype's functionality.

|  |  |
| --- | --- |
| Image of linear polariser with severed wires | Image of linear polariser’s concept [14] |

**Wiring of laser**

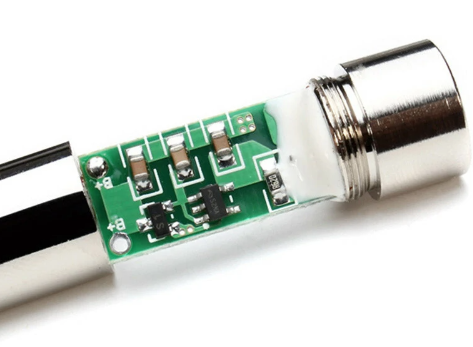


A NPN transistor is used to power the laser as an arduino’s pin is insufficient to power the laser.

## 

## Lasers

To mimic photon transmission, lasers are utilized in the solution. Laser-produced light has a higher intensity and travels longer distances. We can get a well-focused laser for much less cost than developing a collimator-based transmitter. We can adjust the strength and the focus of the laser which we bought on Aliexpress.



<https://www.aliexpress.com/item/32901545471.html?spm=a2g0s.9042311.0.0.1cf34c4dnFhmw7>

Another laser discovered on Banggood operates in the same way as the one mentioned before.

<https://sea.banggood.com/Focusable-200-250mW-650nm-Laser-Module-Red-Dot-Laser-Generator-Diode-Replacement-Mini-DIY-Engraver-p-955966.html?utm_source=googleshopping&utm_medium=cpc_organic&gmcCountry=SG&utm_content=minha&utm_campaign=minha-sg-sea-en-pc&currency=SGD&cur_warehouse=CN&createTmp=1>

## Quarter Waveplate

A quarter wave plate polarises light in a circular manner, allowing the maximum intensity of the laser to permeate through a linear polariser. We don't need a quarter wave plate to circularly polarise the transmission since the laser’s transmission is intense.

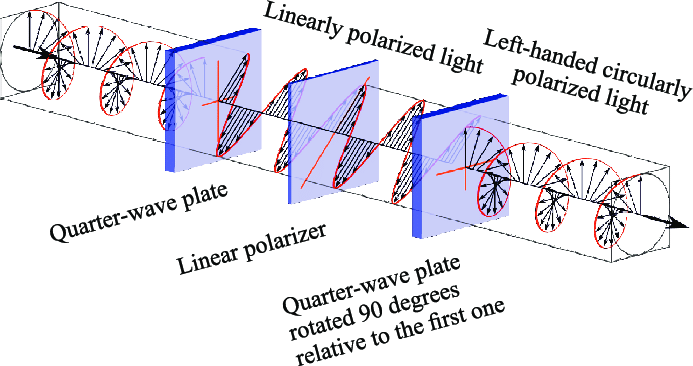


Image of a circularly polarised light passing through a linear polariser and exit from a quarter wave plate at the end

## Grey Filter

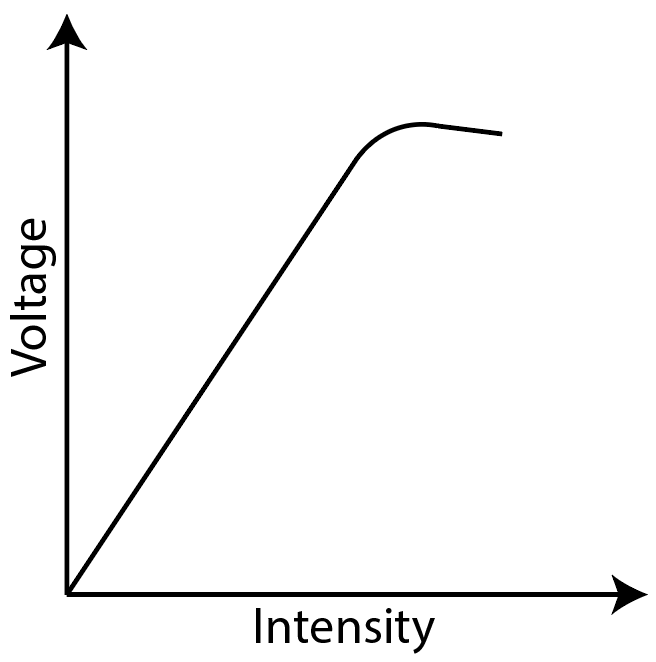
Grey filters reflect excessive light while allowing some amount of light to pass through. The filter is tested in effort to see if it can lower the laser's intensity. The grey filter on the Element14 laser filters out 70% of the 650nm light that passes through it. However, the laser's intensity is still too high for our light sensor and grey filter to detect. Furthermore, the grey filter increases the laser's focus size, making it difficult to distinguish the laser's brightness in the light sensor.

<https://sg.element14.com/visualux/2711xg1-5/filter-220x130mm-grey-neutral/dp/178186>

## OPT101

OPT101 is a photodiode that measures light intensity and can be adjusted to be more sensitive to certain light spectrums. This light sensor is superior to a light dependent sensor (LDR) because it can detect minor fluctuations in the laser's intensity. However, the increased sensitivity of the light sensor has a drawback. The OPT101 is sensitive to light from the environment. The ambient light generated by the surroundings and reflection has a significant impact on the intensity read by OPT101. Therefore, a case is created to shield the OPT101 from most of the ambient light.

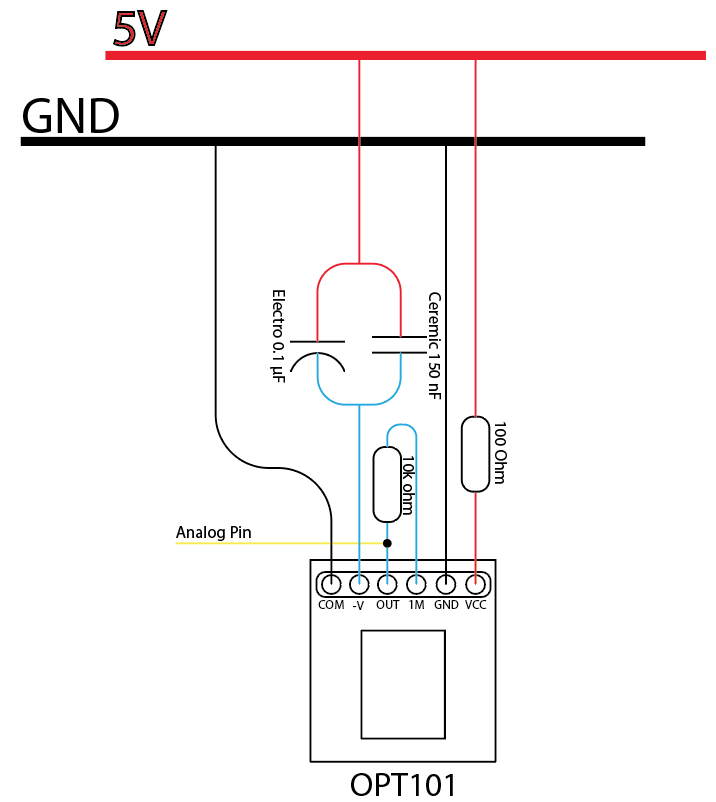
The photodiode generates voltage that are proportional to the light intensity. However, if the light intensity exceeds the sensor's collection capability, the voltage measured will decrease rather than increase. The readings are sketched out in the picture below.



Voltage - intensity graph

As intensity is measured at a high rate, utilizing pulse width modulation, PWM to control the laser's intensity will have certain drawbacks for this photodiode. The OPT101 can detect the intensity of the period when the duty cycle is low. The intensity could be computed using the average of the intensity, however this would cause the entire system to lag. Therefore, the use of PWM to control the laser is off the list.

**Wiring of OPT101**



## SG 90

The SG90 is a low-cost servo motor that rotates from 0 to 180 degrees and requires no additional driver board to operate. The SG90 was chosen for the prototype because of its low cost, fast speed, and ability to return to position 0 after a restart. The ability to return to position 0 eases the testing phase of the project, even though it is not necessary for the prototype. SG90 is sufficient to support the project as linear polarisers are light.

The SG90 motor, on the other hand, has certain flaws. Because the motor uses gears, there is backlash while spinning in the opposite direction, causing light intensity levels to vary on a specific angle. The problem is remedied by setting a wide range of tolerance levels to offset its high and low values. Due to inadequate power, the Arduino Mega frequently restarts unintentionally when the SG90 is continuously rotated. The SG90 must be powered by a separate battery pack. The motor rotates slower without an extra power source thus increasing the time required for the SG90 to reach its desired position and read the intensity level.

## 3D Printed Parts

PLA was first chosen for the project mainly for its low cost and biodegradability. Parts that serve as crimpers, on the other hand, crack over time. For example, the OPT101 and Laser holders. PETG is used instead of PLA because it is easier to print than ABS or Nylon.

## Arduino Mega

Due to its ease of acquisition, the project began with an Arduino Uno. As the application grows in size, more RAM is required to store the encrypted data. The Uno has 2KB of memory, whereas the Mega has 8KB. Data cannot be stored properly due to a lack of memory, resulting in the encryption being broken. Although there are other microcontrollers that can do the job, the Arduino Mega was chosen because of the ease with which the code can be reused and the inexpensive cost.

[14] “Beyond conventional Imaging: Sony's Polarized Sensor,” *LUCID Vision Labs*. [Online]. Available: https://thinklucid.com/tech-briefs/polarization-explained-sony-polarized-sensor/. [Accessed: 07-Sep-2021].