Establishing a Quantum Key Distribution (QKD) Channel using a continuous photon source

Ashesh Kumar Gupta
Indian Institute of Technology, Gandhinagar

Ayaz Khan
Indian Institute of Technology, Gandhinagar

Ayush Jain
Indian Institute of Technology, Gandhinagar

(Dated: April 15, 2024)

The main challenges we will find in the literature today are the factors limiting the communication rates of quantum cryptography systems by single photon are mainly related to the choice of the encoding method. In order to overcome partially these drawbacks, it is advantageous to use continuous quantum states as an alternative to standard encodings based on quantum qubits. For solving this problem, we design and develop a continuous model for quantum key distribution based on the polarization state of photons. The model works with a limited number of allowed polarization states and the characteristics of the laser to enable a larger number of possible states. We also consider the impact of external noise on the model and demonstrate that it produces results consistent with the BB84 protocol for quantum key distribution. Our findings suggest that polarization-based classical models have the potential to provide a viable alternative to traditional quantum key distribution protocols based on entangled states, offering cost efficiency and scalability without compromising on security.

I. INTRODUCTION

If you encrypt a secret message with a random key that is as long as the message itself, your cipher will not be crackable. This is called the One-Time-Pad encryption. But, of course, your communication partner must have the same key, and you cannot use the same key twice. So how do you distribute a secret key between two parties without meeting in person? Quantum cryptography, or better, quantum key distribution has the solution: Use quantum information!

Quantum key distribution (QKD) has emerged as a promising approach for secure communication, enabling two parties to establish a secret key that can be used to encrypt and decrypt messages and also to detect any third-party listener. However, implementing QKD protocols requires expensive and delicate hardware, making it challenging to scale up the technology to large-scale communication networks. As an alternative to QKD, we present a classical model for quantum key distribution that uses continuous monochromatic polarized pulses to establish keys and the characteristics of the laser to achieve a larger number of possible states. Our study investigates the impact of external noise on the performance of the model, demonstrating that it produces results consistent with the well-established BB84 protocol for QKD[1]. Our findings provide new insights into the potential of polarization-based classical models for achieving efficient and scalable quantum key distribution while maintaining the high level of security required for secure communication networks. In this project, we describe the model in detail, present our results, and discuss their implications for the future development of key distribution.

In principle, using a continuous source produces photons which are not correlated with each other in the system and may lead to compromising the security of the protocol. So, why should be this useful if we can't guarantee the safety of the message or key produced using this method? Turns out we can!

By the end of this paper, we will be able to send information and produce a "Quantum Key" by using the standard continuous laser source available in your everyday labs.

II. EXPERIMENT

The main idea behind the original BB84 protocol was to encode every bit of the secret key into the polarization state of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be 'fragile' and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarization state. This will lead to errors, and again the eavesdropper will reveal herself. Alice sends single photons randomly polarized horizontally or verti-

cally (straight base), or +45° or -45° (diagonal base). In our setup, we use weak coherent pulses with adjustable average photon numbers and a half-waveplate to switch between . Bob, on the other hand, uses a polarizer also set randomly to these angles and tries to detect the single photons.

But instead of using single photons and utilizing the inherent quantumness of quantum particles, we would be describing a classical analogue of the experiment. We are using the intensity modulation as a method of encoding our information and producing the key for communication.

Here we, instead of just playing with the polarization of the photons, we are playing with the intensity of the source. The information is encoded in the intensity or the amplitude of the EM wave, which is modulated to determine the presence of a third party.

A. Design

The schematic diagram of our experimental setup is presented in Fig.(1). It consists of a quantum transmitter (Alice) and a quantum receiver (Bob) connected over free space based quantum channel and a classical channel for them to communicate necessary information which does not effect the security of the protocol. The quantum communication link between Alice(Ashesh) and Bob(Ayaz) has been established, operating over 2 meter of free space optical path.

The experimental setup consists of three parts:

Ashesh: The sender part consists of a laser source and a polarizer which encodes the information. The laser intensity is reduced to almost half at this stage. The polarizer is rotated using a servo motor, which receives it's instructions from an Arduino, rotating the polarizer randomly.

Ayaz: The receiver part and most complicated portion of the setup. Here the photodiode is used to measure the intensity of light. As the current generated by this photodiode is very small and can't be used as an input to the microprocessor, we designed a circuit which measures the charging time of a 1μF capacitor and thus the intensity of the light incident on the photodiode.

Ayush(Eve): The eavesdropper is present all the time. But when we don't want him to affect the data, we sync the polarized axis same as that of Ashesh's. When we want to study it's presence, we simply make him random as well, and look that the intensity difference in the two cases, thus identifying the presence of Eve.

Circuit Design: To measure the intensity of the polarized pulsed laser charging time of a capacitor is measured and the charging current in controlled by the intensity of light falling into the photodiode, if no light is falling into it current through the photodiode is zero and increases proportionally with the increasing light intensity falling into the photodiode. This current is utilized to charge a capacitor from 0v to 5v and charging time is measured using a microcontroller (Arduino).

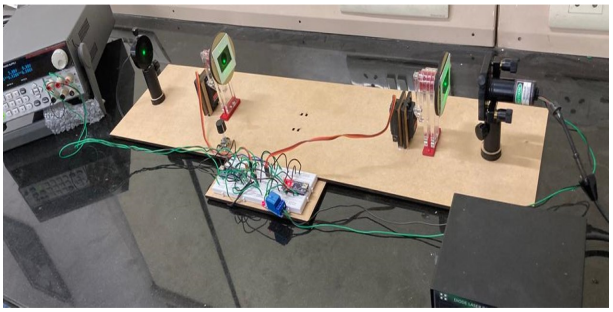

FIG. 1: The Experimental Set-Up

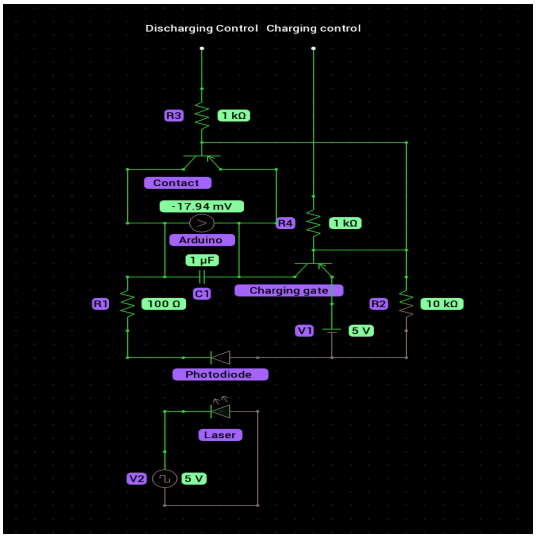

FIG. 2: Circuit Diagram for Detector

B. Method

The system consists of two main units first is the sender, which sends a continuous light pulse in one of the polarization states at a time, and the second is a receiver, which measures the polarization state in any of the possible states at a time. The larger the number of possible states larger will be the probability that a third person's guess of the polarization state is wrong. We use elliptically polarised green laser source in our experiment. For convention, we'll call the senders state as S0, S1, S2, and the measured state at the receiver end R0, R1, R2. In our experiment, we refer 0, 40, and 90 degrees as 0, 1, and 2.

At the sender's and receiver's side the states are generated by a rotating polarizer and detected by an analyzer. Both are controlled by servo motor.

To measure the intensity of the polarized pulsed laser, sereval methods were thought off. At the beginning, methods like an Om-amp bases Transimpedence Cir-

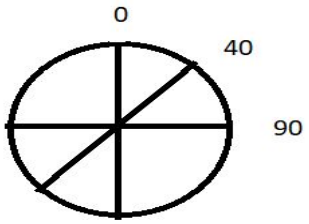

FIG. 3: Experimental Base

cuit(TIA) was made, but it failed to capture the difference and amplify the current required to serve the Arduino circuit(See A1). Finally, the charging time of a capacitor is measured and the charging current in controlled by the intensity of light falling into the photodiode was used to measure the intensity. If no light is falling into it current through the photodiode is zero and increases proportionally with the increasing light intensity falling into the photodiode. This current is utilized to charge a capacitor from 0V to 5V and charging time is measured using a microcontroller (Arduino).

We used the green laser available in the lab with high intensity and low beam cross-section. We found that either we should increase the beam diameter in add a filter to reduce the intensity of laser but the beam diameter of the laser we are using can't be changed so we decided to keep the center of the beam slightly away from the pinhole of photodiode and this worked.

III. EXPERIMENTAL DATA

The data obtained from the experiment is divided into two parts. First the Arduino, stores reference data, which will be important for data analysis. The reference act as the base which we compare, to identify the base of senders.

A. Results Without Ayush

```
##Reference_Data
Time0= 95
Time30= 177
Time90= 1001
Time0= 373
Time30= 236
Time90= 415
Time0= 415
Time30= 177
Time90= 39

SATES
S11  161
S10  93
S11  228
S01  403
S11  84
S10  456
S01  1001
S10  343
S01  39
S11  212
S01  437
S11  86
S10  97
over
```

1. *Analysis*

Comparing each state with the reference data, we receive,

Ashesh's Bases	0	1	0	2	0	1	2	1	1	0	2	1
Ayaz's Bases	1	0	0	1	0	2	2	0	2	0	1	1
Matching	x	x	✓	x	✓	x	✓	x	x	✓	x	✓

Table 1: Experimental Data

From the data above, we can see that the indices(starting from 0) of their bases 2,4,6,9,11 are matching. Therefore, after Ashesh confirms these matching indices from the data of Ayaz's bases, which he receives from him via a classical channel, he informs Ayaz about the key.

For example, he tells Ayaz that the intensity corresponds to the indices [2,4] representing 'A' and [6,9] representing 'B' and so on.

Now, the information is encoded by the key formed in this way.

B. Results with Ayush

Then, Ayush is added to the system. The intensity dropped due to adding another polarizer calibrated in the final measurement.

```
##Reference_Data
Time0= 53
Time30= 95
Time90= 1001
Time0= 177
Time30= 119
Time90= 241
Time0= 256
Time30= 111
Time90= 23
```

```
SATES
S11  99
S10  61
S11  107
S01  197
S11  41
S10  299
S01  1002
S10  192
S01  20
S11  126
S01  198
S11  42
S10  60
over
```

1. *Analysis*

Comparing each state with the reference data, we receive,

Ashesh's Bases	0	1	0	2	0	1	2	1	1	0	2	1
Ayaz's Bases	1	0	0	1	0	2	2	0	2	0	1	1
Matching	x	x	✓	x	x	x	✓	x	x	✓	x	x

Table 2: Experimental Data

As in Table: 2, after adding Ayush, we can see that even when the bases of both Ashesh and Ayaz are the same, the intensity that we measured is much less than expected. Hence, we can conclude that there is third-party eavesdropping.

IV. DISCUSSIONS

We have successfully establish a communication channel which was ever to identify the presence of the eavesdropper and thus securing the channel. One of the major issue in this method is that we can only use certain angles of the polarization as intensity measured is depend on the difference in angle between the polarization axis. Thus, for example, 45° cannot be used as we won't be able to differentiate the states. As we were getting data that says around a large range at 0 degrees, the intensity of light falling into the photodiode is the same up to 30 degrees. As , $I = I_0 \cos^2\theta$ and

$$\frac{dI}{d\theta} = -2I_0 \cos\theta \sin\theta$$

suggests, we thought this was because there is small change in intensity at zero degree and large change at 45 degrees, but soon we realized that as light intensity increases current through the capacitor increases, but up to a certain value, after that no matter how large is the intensity the photodiode allows that fixed max current to pass through it and hence a fixed charging time of the capacitor.

At first, we used a circularly polarized laser and decided to use three polarization states 0, 45, and 90 degrees from vertical but we realized that our detector would not be able to distinguish if the arriving pulse is polarized in 0 states and receiver measured in 45 or the arriving state is in 90 and the receiver measured in 45. Then we set the middle state to 30 degrees, the same problem arrived it couldn't be able to distinguish between arriving state 30 and the measured state at the receiver's end 90, and arriving state 90 and the measured state 30 at the receiver's end. To overcome this problem, we used an elliptically polarized laser and kept its major axis vertical.

Also, the probability of catching Ayush in just few of such measurements is very less. It may well happen that we won't be able to catch Ayush as though random, his and Ashesh's bases are same. But this chances decreases drastically with the same of observations made. Also, there were situations where difference in angle between all three were such, Ayush was undetected, but chances of that decreases with number of observations(See A2).

V. ACKNOWLEDGEMENTS

We want to show our gratitude to Prof. Chandan K Mishra for supporting us every step of the way. Also no one can ignore the immense contributions of Raju Beerasant, without whom this experiment was not possible. We also want to thank the TAs assigned for their timely discussions.

VI. REFERENCES

1. https://doi.org/10.48550/arXiv.2003.06557
2. `https://en.wikipedia.org/wiki/Transimpedance_amplifier`

VII. APPENDIX

A. A1

A transimpedance amplifier (TIA)[2] is a current to voltage converter, almost exclusively implemented with one or more operational amplifiers. Current to voltage converters are used with sensors that have a current response that is more linear than the voltage response.

This is the case with photodiodes where it is not uncommon for the current response to have better than 1% nonlinearity over a wide range of light input. The transimpedance amplifier presents a low impedance to the photodiode and isolates it from the output voltage of the operational amplifier. In its simplest form a transimpedance amplifier has just a large valued feedback resistor, R_f. The gain of the amplifier is set by this resistor and because the amplifier is in an inverting configuration, has a value of $-R_f$.

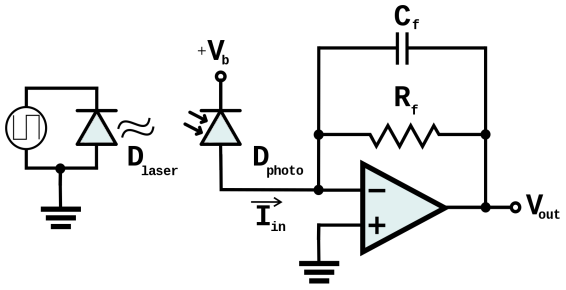

FIG. 4: TIA Circuit

Now, using this circuit, we were unable to acquire the required amount of the amplification. Therefore, we used the capacitor model to find the intensity falling on the photodiode.

B. A2

Using a bit of information, or one pulse of laser beam, we noticed that Ayush might get lucky. The chances that he will choose the same basis as Ashesh and thus goes unnoticed is

$$P = \frac{1}{3}$$

.
But just by using this seven times, the probability goes as,

$$P(\texttt{Ayush getting undetected}) = \frac{1}{3^7} = 0.00045$$

Conversely, probability of catching an eavesdropper is 99.9995%.