Contact person:

Prof. Frank Setzpfandt
Friedrich-Schiller-Universität Jena
Abbe School of Photonics
Phone: +49 (0) 3641 947569,
e-mail: f.setzpfandt@uni-jena.de

Quantum Cryptography

Lab Title:	Quantum Cryptography
Group number:	5
Student name:	Ishaan Chaturvedi
Name of Teaching Assistant:	Sabine Häussler
Date of Lab:	December 4, 2025
Date of Report Submission:	December 11, 2025

Quantum Laboratory

Abbe School of Photonics, Friedrich-Schiller-Universität Jena

Contents

1 Introduction

Secure Communication has always been an important

2 Theory

In conventional cryptography, the information is shared using public keys for encryption and private keys for decryption. However, the security of these methods relies on the computational difficulty of a computer. For example, RSA method utilises the fact that it is much harder to factorise a number into its prime factors than to multiply two prime numbers together. However, with the advent of quantum computers, we have algorithms like Shor's algorithm which can efficiently factorise large numbers, thus breaking the security of RSA. So there is a need for cryptographic methods that are secure against such attacks. This is where Quantum Key Distribution (QKD) comes into play. Instead of relying on computational difficulty, QKD used the principles of quantum mechanics to ensure that the key distribution is secure. In this experiment we will discuss the BB84 protocol, which is one of the first and most well-known QKD protocols.

2.1 BB84 Quantum Key Distribution Protocol

BB84 protocol was proposed by Charles Bennett and Gilles Brassard in 1984. It utilises the properties of quantum mechanics to securely distribute a cryptographic key. Once we share a secret key, we can use it to encrypt and decrypt messages which can now be transmitted using a classical channel. In order to share a key using BB84 protocol, we will take two communicating people, conventionally called Alice and Bob, who want to share a secret key. In order to share the key with BB84 protocal they need to follow the following steps:

1. **Preparation and Transmission:** Alice randomly selects a sequence of bits Here randomness is crucial for the success of the protocol. She also randomly chooses a basis (rectilinear or diagonal) for each bit. She will then encode each randomly chosen bit in the polarisation state of the photon according to the randomly chosen basis and sends the photons to BOB.

2. **Bob's Measurement:** Upon receiving the photons, Bob randomly chooses a basis (rectilinear or diagonal) for measuring each incoming photon. He records the measurement results and store them in the form of bits. Note that the bit encoding scheme for polarisation states is the same as Alice's encoding scheme. However, since Bob is choosing his measurement basis randomly, there will be instances where his chosen basis does not match Alice's encoding basis. Thus to make sense of the bits, they will need to communicate over a classical channel.

3. **Classical communication**: Now Alice and Bob communicate over a classical channel. Bob tells Alice which basis he used for each measurement, but he will not reveal the measurement results. Alice then reveals to Bob which measurements were done in the

correct basis. They will discard all thebibliography bits where the measurement basis did not match. The remaining bits constitute the potential secret key.

4. **Error Rate Estimation and eavesdropper detection:** The purpose of the BB84 protocol is to securely share a key. To do this, Alice and Bob should be able to detect the presence of an eavesdropper (conventionally called Eve). Eve on the other hand wants to intercept the quantum states sent by Alice and measure them to gain information about the key. However, BB84 protocol utilises two important features of quantum mechanics to detect Eve's presence:

   - **No-Cloning Theorem:** It is impossible for Eve to have a complete knowledge of the quantum state being transmitted with a single measurement. In order to do so she has to make a copy machine that creates an identical copy of an arbitrary unknown quantum state. But according to no cloning theorem it is not possible to do so. Thus, Eve cannot simply copy the quantum states sent by Alice, measure them and send a copy to Bob.
   - **Measurement Disturbance:** When Eve measures the quantum states, she will project them into one of the basis states. If her chosen measurement basis does not match Alice's encoding basis, she will introduce errors in the measurement results. When Bob measures the states sent by Eve, he will get incorrect results for those bits where Eve's measurement basis did not match Alice's encoding basis. This will be the case as Alice choses a random basis for encoding and this is one of the reasons why randomness is so crucial in the BB84 protocol.

   Bob and Alice are able to detect Eve's presence because of these two features. To estimate the error rate, they will randomly select a subset of the remaining bits (the ones where Bob's measurement basis matched Alice's encoding basis) and compare them over the classical channel. If the error rate is above a certain threshold, they will conclude that Eve is present and abort the key generation process. If the error rate is below the threshold, they can conclude that the channel is secure and can use the remaining bits as the secret key. Note that we use a threshold because in practical scenarios, there can be errors due to noise in the channel, detector inefficiencies etc.

Security of Classical Channel

It is necessary for Alice and Bob to communicate over a classical channel to determine the basis matching is secure. This means that even Bob needs to ensure that he is communicating with Alice and not Eve. This can be done using authentication methods like pre-shared keys or digital signatures.

3 Experimental Realization

The experimental setup for the implementation of BB84 protocol is shown in figure 1. However, in this experiment we will not be using HWP to prepare the states as shown in the figure,

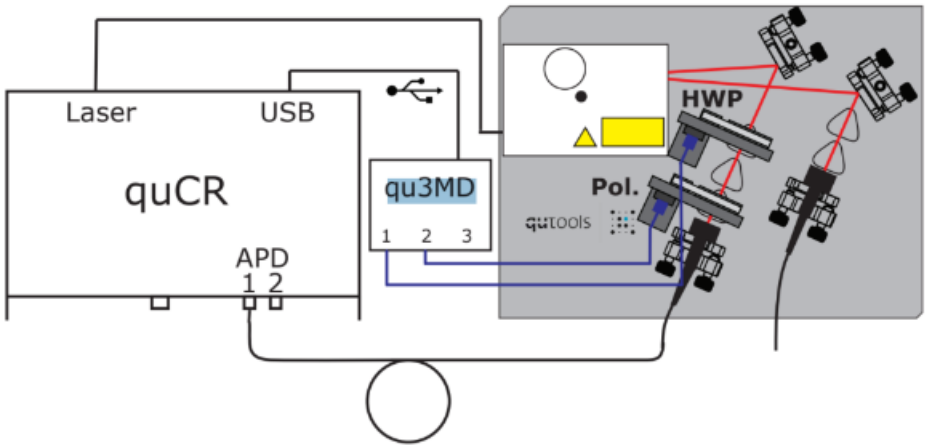

Figure 1: Schematic of the experimental setup for BB84 protocol implementation. Source:[?]

but a Polariser as our photon source is also producing circularly polarised light. This setup is an educational setup which uses quCR as a central interface for interacting with various components. The Polarisers are connected to qu3MD which controls their orientation through a motor. The single photon detectors are in the quCR which is connected to the polariser by an optical fiber. We use BBO crystal to generate a photon pair through Spontaneous Parametric Down Conversion (SPDC). One photon of the pair is discarded while the other is used for the BB84 protocol. The Pump laser is a 405 nm laser diode. This is operated in pulse wave mode to generate weak coherent pulses.

3.1 Weak coherent Pulses

In practical implementations of BB84 protocol, it is difficult to generate single photons. They are still an active area of research. So in this experiment we will be using weak coherent pulses. Since attenuating a laser pulse does not change its statistical properties, the probability of having k photon in a pulse is as follows:

$$P(k,\lambda) = \frac{\lambda^k}{k!}e^{-\lambda} \tag{1}$$

where λ is the average photon number per pulse. Now for BB84 protocol to be secure, we want to minimise the probability of having more than one photon in a pulse as this can be exploited by Eve to perform an attack with the help of a beam splitter. Thus, we want to choose the average photon number per pulse λ such that the probability of having more than one photon in a pulse is very low. However if we choose λ to be too low, the key generation rate will be very low as most pulses will not contain any photons. To see this we can calculate $\frac{P(0,\lambda)}{P(1,\lambda)}$ and $\frac{P(2,\lambda)}{P(1,\lambda)}$:

$$\frac{P(0,\lambda)}{P(1,\lambda)} = \frac{1}{\lambda} \tag{2}$$

$$\frac{P(2,\lambda)}{P(1,\lambda)} = \frac{\lambda}{2} \tag{3}$$

So we can see that as we decrease λ, the ratio of zero photon pulses to one photon pulses increases, which means that most pulses will not contain any photons. On the other hand, as we increase λ, the ratio of two photon pulses to one photon pulses increases, which means that there is a higher chance of having multiple photons in a pulse. Thus, we need to choose an optimal value of λ that balances these two factors. We can measure this effect by lowering Pulse power amplitude and Pulse width and observing the effect on Quantum Bit Error Rate (QBER) and key generation rate.

3.2 Quantum Bit error rate

In order to quantify the performance of the BB84 protocol, we use a metric called Quantum Bit Error Rate (QBER). It is defined as the ratio of the number of erroneous bits to the total number of bits in the key. Mathematically, it can be expressed as:

$$QBER = \frac{N_{error}}{N_{total}} \tag{4}$$

where N_{error} is the number of erroneous bits and N_{total} is the total number of bits in the key. A low QBER indicates that the key is secure and can be used for encryption, while a high QBER indicates that the key is not secure and should be discarded. In practical implementations of BB84 protocol, a QBER of less than 11% is considered acceptable for secure key generation.

3.3 Experiment Walkthrough

1. We set up laser in pulse mode with frequency, pulse power and pulse width
2. We begin the experiment by randomly generating a sequence of bits and basis with the software. We then start the measurement which happens automatically by the quCR software.
3. Once we have the measurement results we match the basis, we keep the bit where measurements were done in the correct basis. We then discard all the bits where the measurement basis did not match.

This is the data that we will be analysing in the next section.

4 Measurement Results and Analysis

4.1 Experimental Tasks

Statistical Analysis:

5 Conclusions

ave successfully implemented and analyzed the BB84 quantum key distribution protocol in a laboratory setting. Through the experiment, we demonstrated the fundamental principles of

quantum cryptography, including the use of quantum states for secure key exchange and the detection of potential eavesdropping via error rate estimation. The results confirm that the BB84 protocol provides a robust method for secure communication, as long as the quantum bit error rate remains below the acceptable threshold. This experimen t highlights the practical challenges in generating single photons and the importance of optimizing experimental parameters such as pulse power and width. Overall, the BB84 protocol remains a cornerstone of quantum cryptography, offering a promising approach to secure communication in the presence of quantum computational threats.

Bibliography

[1] NASA, *Speed of Sound*, Online resource.

[2] C. Nordling and J. Ostermann, *Physics Handbook for Science and Engineering*, 8th ed., Studentlitteratur, 2006.

[3] Heat Capacity Ratio for Gases, Online resource.

[4] Wikipedia, Online encyclopedia.