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

Fundamentals of Quantum Optics

Lab Title:	Fundamentals of Quantum Optics
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'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:** In order to check the security of the communication channel, Alice

2.2 Quantum States and Bases

Information is encoded using four quantum states: $|0\rangle$, $|1\rangle$ in the rectilinear basis, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the diagonal basis. An eavesdropper attempting to intercept the quantum states will introduce detectable errors due to quantum mechanics principles.

3 Experimental Realization

4 Measurement Results and Analysis

5 Conclusions

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.