

Qiskit Hackathon@World of QUANTUM

# QUANTUM KEY DISTRIBUTION (QKD): Lecture Plan

**One-Zero Group:** Arthur M. Faria, Vladlen Galetsky, André Lohde,  
Raúl Santos, Daniela Trienes

April 27, 2022

# Introduction

The lecture consists of four parts. The first part is a short presentation, which will approximately last 10 minutes and that gives the theoretical background on the subject of quantum key distribution. A short demonstration of the BB84 protocol using a self-made website follows, taking approximately 5 minutes. The third part, which will take 30 to 40 minutes, will be the exercises, realised via Jupyter notebook. At the end, the teacher will ask a few questions, taking 5 minutes.

The target audience will be undergraduate students with a basic knowledge of quantum mechanics and a few previous sessions covering simple quantum gates and Qiskit.

## 1 Presentation

### Slide 1 - Quantum Key Distribution

The lecturer introduces the topic: quantum key distribution.

### Slide 2 - What's the matter?

The teacher motivates the problem with a headline from a scientific article, saying that programmable superconducting processors lead to quantum supremacy, mentioning google as an example and an illustration of the configuration of an IBM 127-Qubit Quantum Processor. Furthermore, it is emphasized that advances in quantum computing may bring risks concerning private security, referring directly to the RSA algorithm, which will not be explained in more detail on this slide.

### Slide 3 - Why does it influence our current RSA protocols?

The teacher explains and distinguishes, why quantum computation is such a hazard for RSA protocols compared to other symmetric keys which are mostly resistant to the quantum computation attacks (AES-256). Using the well-known Shor algorithm in quantum computation, one can quickly identify the prime numbers of integers which define the key. There are also other classical cryptography approaches that are easily breakable such as the Diffie-Hellman and Elliptic curve cryptography that could both be mentioned in the class.

### Slide 4 - Quantum Key Distributions

The teacher differentiates between discrete and continuous variables, which are measured, naming a photon count as a discrete and an electric field as a continuous variable.

The teacher explains that a handful of protocols exist, that are based on discrete variables and points to the bubbles on the left side of the slide. They point out, that the 4-State BB84 protocol, which is marked red, is the one which will be described further.

Then they briefly mention continuous variable protocols, without going too much into detail. They explain how the quantum states are encoded into different quadratures of the electric field and what type of variables (coherent, squeezed) and methods (Gaussian, discrete) are used for that end.

## **Slide 5 - The BB84 protocol**

The teacher describes the steps for implementing the BB84 using the description and the picture on the slides.

## **Slide 6 - Example for BB84**

The teacher uses the example on the slide to illustrate the process. They need to explain, that Alice wants to send a key to Bob, which she encodes randomly with a basis containing four different polarizer types. Bob decodes that encoded key with another random basis, which does not fully match with Alice's basis. Afterwards they exchange their basis via a public channel.

Then the teacher switches to the next slide.

## **Slide 7 - Quantum bit error rate (QBER) and sifted key rate**

By comparing their bases with each other, Alice and Bob create a sifted key by only using those key components, where both Alice's and Bob's bases match.

The remaining errors contribute to the quantum bit error rate (QBER) and can either be produced by noise or an eavesdropper.

## **Slide 8 - Distillation and privacy amplification**

The teacher presents the slide. The contents are self-explanatory.

## **Slide 9 - Any more questions**

The lecturer asks if there are any questions concerning the theoretical basics and answers those questions.



**BB84 Sim**

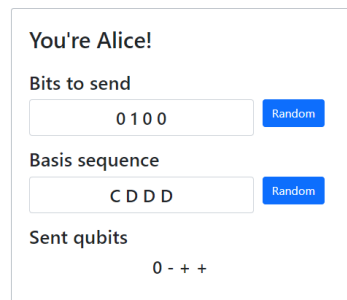
Your Code  
4537

---

Insert friend code

1583

(a) Entry page for the students, where they may share their code with a colleague, or input one



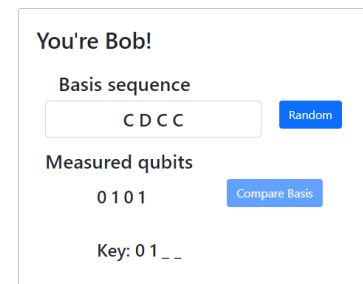
**You're Alice!**

Bits to send  
0 1 0 0 Random

Basis sequence  
C D D D Random

Sent qubits  
0 - + +

(b) Site for the Alice role of the BB84 protocol



**You're Bob!**

Basis sequence  
C D C C Random

Measured qubits  
0 1 0 1 Compare Basis

Key: 0 1 \_ \_

(c) Site for the Bob role of the BB84 protocol

## 2 Website demonstration

A link from the lecturer is granted to the students, where they will be able to access a website. There, they will be shown an entry page. Each student is given a code, which they can share with a colleague of choice. They form pairs, and one of the students inputs the code from their colleague. Afterwards, they are redirected to a different page each, and attributed the roles of 'Alice' and 'Bob'.

Alice starts by choosing 4 bits of information to send, as well as 4 basis to put the qubits in. C stands for Canonical, which represents the basis  $\{|0\rangle, |1\rangle\}$  and D stands for Diagonal, representing the basis  $\{|+\rangle, |-\rangle\}$ . Meanwhile, Bob also chooses basis, randomly, to measure the qubits in. After both students have made their choices, they will be shown the shared key. They can make the experiment multiple times, and estimate the natural qubit error rate of the BB84 protocol.

## 3 Jupyter notebook

The lecturer will show a Jupyter notebook, where they guide the students through, introducing the exercises, while giving them the necessary time to solve the problems by themselves. At the end of each exercise they then discuss possible solutions to the problems, and difficulties that the students may have had.

The additional test exercises are given as a homework.

## 4 Summary

The teacher will ask a few questions to the students depending on the time left. This way, they can get a glimpse on what was learned by the students. Possible questions can be:

- So what have you learned today?
- Do you remember, why quantum computation can be a risk on classical computation approaches?
- In BB84: Why can Alice and Bob use randomly different bases to communicate with each other? What do they use these bases for?
- Can someone explain the intrinsic relation between noise and detection capability of Eve?
- (More challenging question:) Anybody has any suggestion on how we could quantify the maximal available information for Eve to steal?
- (More challenging question:) If you add decoy states to your protocol, how would you expect your system to behave?

## Test exercises

The additional test exercises are given with the jupyter notebook and are covering decoy states. Briefly mentioning them in the outlook does not hurt, but the students should be able to solve the problem with the understanding they have of BB84 from the notebook and the information given in the exercise.

Solving the test exercise should take less than 30 minutes.