**Middle East Technical University**
**Institute of Applied Mathematics**

# Quantum Key Distribution and Recent Advancements

**Nazlı Ceren Demir**
(Cryptography)

**Advisor: Assoc. Prof. Dr. Oğuz Yayla**

Term Project Report
February 2022

# Abstract

Secure key distribution between communicating parties is important in encryption using symmetric keys. The advance of quantum computers is expected to make some key distribution schemes obsolete. Quantum key distribution is one of the main approaches taken in order to achieve security against quantum computers. This term project examines the BB84 Protocol, which is the first quantum key distribution protocol, and the recent developments in quantum key distribution.



# Öz

Güvenli anahtar değişiminin sağlanması simetrik anahtar ile şifrelemede önemli bir konudur. Kuantum bilgisayarların geliştirilmesiyle günümüzde kullanımda olan sistemlerin güvenlik ihtiyacını karşılamayacağı değerlendirilmektedir. Bu doğrultuda öne çıkan önemli bir araştırma konusu kuantum anahtar değişimidir. Bu bitirme projesi, ilk kuantum anahtar değişimi protokolü olan BB84 Protokolünü ve kuantum anahtar paylaşımında son dönemde meydana gelen gelişmeleri ele almaktadır.

# Contents

# Chapter 1

# INTRODUCTION

Encryption has been an important part of security in message transfer for ages. The most well known early ciphers are the Cesarean Cipher and the Vernam Cipher.

In the modern day, there have two kinds of encryption.

- Symmetric key encryption
- Asymmetric key (public key) encryption

The differences, as can be derived from the names, lies in how the keys are used.

In symmetric encryption, the sender and receiver (from now on they may be called Alice and Bob) share a common key to encrypt and decrypt a message. This can be shown as:

$$E_k(M) = C, \quad D_k(C) = M$$

in which $M$ represents the message being sent, or in other words, the Plaintext, and $C$ symbolizes the encrypted text, which is known as the Ciphertext. The symbol $k$ is used for the key.

In asymmetric cryptography on the other hand, Alice and Bob have a set of two keys. One of the keys is public, the other one is private. They communicate through the use of mathematics, mostly depending on the hardness of factorization or discrete logarithm problems.

This paper deals with symmetric key cryptography. It's crucial that the keys are kept secret. Hence, an important aspect in this kind of encryption is how the common keys are shared between Alice and Bob. There are various protocols to achieve this in public networks, in which either symmetric keys or public keys are used. [1][6]

These protocols usually involve a trusted server. Another solution is quantum key distribution. The transfer of symmetric keys between two communicating parties depends on the hardness of mathematical problems. Therefore, they are only computationally secure. This means that if a better algorithm was developed to solve that problem or if an adversary had access to faster computation powers, such as quantum computers, then the cipher would be broken. Quantum Key Distribution (QKD) on the other hand, relies not on the hardness of problems, but the properties of quantum mechanics. The security of classical key sharing schemes cannot be proven, while QKD is information theoretical security.

Shor's algorithm is well known in the cryptography community and it is believed that its fast method in factoring large numbers may be used to break RSA with a quantum computer. It would take 8 hours to brake a 2048-bit RSA with a quantum computer that has 20 million qubits. Currently, Google's Sycamore computer has 53 qubits. In October 2019, Google announced that they achieved 'quantum supremacy' in which Sycamore computed a calculation in 300 seconds, which would have taken 10.000 years in a classical computer. IBM later rebuted these claims by stating that the same task could be achieved with a classical computer with more disk storage in 2.5 days. [34] It is expected to take about a decade or two to reach a level of computation to break RSA in life-time. [33]

In order to achieve security against quantum computers two approaches may be taken: to develop algorithms that are quantum-resistant or to use quantum key distribution. This report examines the latter method.

There are various protocols regarding quantum key distribution. This report will focus on the BB84 Protocol.

BB84 is the first quantum key distribution protocol, and it is still in use today. The BB84 Protocol was founded by Charles Bennett and Gilles Brassard in 1984.

The structure of the report is as follows. After the introduction, the second section will introduce the concepts of quantum mechanics and familiarise the reader with the principles of quantum mechanics that are important to understand the BB84 Protocol. It details the concepts of the superposition principle, the Heisenberg uncertainty principle, the no-cloning theorem and entanglement. The third section will detail the implementation of the BB84 protocol and elaborate on its security and real life implementation. The fourth section will summarise the recent experiments regarding QKD, focusing primarily on the trials that use the BB84 protocol. The fifth section will close with a conclusion regarding QKD.

# Chapter 2

# QUANTUM MECHANICS FOR CRYPTOGRAPHY

## 2.1 Some Preliminaries

Quantum Mechanics uses linear algebraic operations.

A set with operations addition and multiplication by a scalar $R$ is called a vector space $V$. Its elements are vectors $\vec{v}$, represented by a column

$$\vec{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_R \end{bmatrix} \tag{2.1}$$

Dirac's notation is used to show elements of a vector space. Any vector is denoted by a ket, as

$$|v\rangle = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \quad v_i \in \mathbb{C} \tag{2.2}$$

A bra on the other hand, is defined as:

$$\langle v| = (v_1^*, v_2^*, \ldots, v_n^*), \quad v_i^* \in \mathbb{C} \tag{2.3}$$

Quantum Mechanics deals with complex vector spaces.

The set of $n$ linearly independent kets $|v_i\rangle$, spanning $V$, is called the basis of $V$.

$$\mathbb{B} = \{|v_i\rangle, i = 1, ..., n\} \tag{2.4}$$

The number n is called the dimension of $V$. It might be infinite, such as the Hilbert space.

Let $V$ be a complex, finite dimensional vector space on $\mathbb{C}$. If $\hat{A}$ is a linear operator, and

$$\hat{A}|v\rangle = \lambda|v\rangle, \quad v \in V \tag{2.5}$$

then the complex number $\lambda$ is called the eigenvalue of $\hat{A}$ corresponding to the eigenket $|v\rangle$. Equation 2.5 is called the eigenvalue equation. It is a straightforward procedure to determine eigenkets and eigenvalues of $\hat{A}$, using the characteristic equation.

$$det(\hat{A} - \lambda I) = 0$$

where $\hat{A}$ is an $nxn$ matrix and $\lambda \in \mathbb{C}$.

Solutions of the characteristic equation determine eigenvalues $\lambda_i$. Eigenkets are determined using Equation 2.5. Theoretically, characteristic equation has at least one complex root.

If some of the eigenvalues repeat, then they are called degenerate.

We will mostly deal with Hermitian operators ($\hat{A} = \hat{A}^\dagger$). If an observable is Hermitian, its eigenvectors are orthonormal and they are basis vectors that span the vector space. Hermitian operators have real eigenvalues.

We will also use the expectation values for operators. The expectation value is the expected value of a measurement with their probabilities taken in to account. In order to find the average value, we first find the eigenvalues and eigenvectors of the given operator since the average value of $A$ is given by:

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \sum_j a_j |\langle\psi|\varphi_j\rangle|^2$$

in which $\varphi_j$'s are the eigenvectors and $a_i$'s are the eigenvalues of $A$.

In quantum mechanics, Pauli's spin matrices, which are three $2x2$ matrices, $\hat{\sigma_x}, \hat{\sigma_y}, \hat{\sigma_z}$, are extensively used. The matrices $\hat{\sigma_x}$ and $\hat{\sigma_z}$ will be used in the BB84 Protocol.

$$\hat{\sigma_x} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \hat{\sigma_y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \hat{\sigma_z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.6}$$

## 2.2 The Superposition Principle

Measurement of an observable $\hat{A}$ on the ket $|\psi\rangle$ (State), gives one of the eigenvalues of $\hat{A}$ and leaves the state in the eigenket corresponding to the specific eigenvalue of $\hat{A}$, i.e., the ket $|a\rangle$. So,

$$\begin{array}{cc} \text{Before} & \text{After} \\ |\psi\rangle & |a\rangle \end{array} \tag{2.7}$$

This is called the collapse of the state $|\psi\rangle$ into a definite eigenstate $|a\rangle$. In other words, measurement disturbs the system. This type of measurement is called the projective measurement.

The quantum mechanical "state" of a physical system at any instant of time may be represented by a ket $|\psi(\vec{r},t)\rangle$ or wave function, which is continuous and differentiable. To determine it, we use the Hilbert space of eigenkets of maximum number of commuting operators. The state $|\psi(\vec{r},t)\rangle$ is a complex function and does not have a physical meaning, but

$$\||\psi(\vec{r},t)\rangle\|^2 \tag{2.8}$$

has a physical meaning. It gives the probability density of finding the system at $\vec{r}$, at time $t$.[4]

Quantum mechanics is a probabilistic theory. Measurements do not always give definite results. The measurement procedure is completely different than classical mechanics. To make a quantum mechanical measurement one should prepare many identical states to be observed, then make measurements on each state, obtain eigenvalues and then calculate the probability. This is called the Born interpretation. [4]

The superposition principle states that if $|\psi\rangle$ and $|\varphi\rangle$ are two states of a quantum system, then any superposition $\alpha|\psi\rangle + \beta|\varphi\rangle$ should also be an allowed state of a quantum system, in which $|\alpha|^2 + |\beta|^2 = 1$.

Assume that we have the common eigenstates of maximum number of commuting operators. Then one can construct an orthonormal basis

$$\mathbb{B} = \{|\varphi_i, i = 1, ...\rangle\}$$

for these states, and any ket $|\psi(\vec{r},t)\rangle$ can be expressed as

$$|\psi(\vec{r},t)\rangle = \sum_i c_i |\varphi_i\rangle, \quad c_i \in \mathbb{C} \tag{2.9}$$

Notice that, 2.9 is a solution for all $c_i$. [4]

In addition, we can say:

$$\langle\psi,\psi\rangle = \||\psi\rangle\|^2 = \sum_i c_i^* \langle\varphi_i| \sum_j c_j |\varphi_j\rangle \tag{2.10}$$

$$\langle\psi,\psi\rangle = \sum_{i,j} c_i^* c_j \langle\varphi_i,\varphi_j\rangle = \sum_i c_i^* c_i = \sum_i |c_i|^2 \tag{2.11}$$

where $\langle\varphi_i,\varphi_j\rangle = \delta_{ij}$.

Thus, if the state ket $|\psi\rangle$ is normalized, i.e,

$$\langle\psi,\psi\rangle = 1 = \sum_i |c_i|^2 \tag{2.12}$$

The expansion coefficients absolute square $|c_i|^2$ is interpreted as the probability to measure the eigenvalue corresponding to the eigenket $|\varphi_i\rangle$.

Notice that the total probability is 1.

In other words, it is possible to measure any of the eigenvalues after measurement.

For a general ket:

$$c_i = \langle\varphi_i,\psi\rangle \tag{2.13}$$

We can also use another formula to compute the probability of making a certain measurement. First, we define the projection operator. The projection operator $\hat{P}_k$ is defined as the outer product of the state $|v_k\rangle$:

$$\hat{P}_k = |v_k\rangle \langle v_k| \tag{2.14}$$

The properties of the projection operator are:[4]

1. $\hat{P}_k{}^2 = \hat{P}_k$
2. $\hat{P}_k \hat{P}_j = 0$ if $k \neq j$

3. $\sum_{k=1}^{n} \hat{P}_k = I$

From these properties, projection operators are Hermitian, therefore $P_k^\dagger = P_k$.

If we have eigenstates $|\varphi_i\rangle$, then the projective measurement can be defined as:

$$\hat{P}_i = |\varphi_i\rangle \langle\varphi_i|$$

It is easy to see that since $c_i = \langle\varphi_i, \psi\rangle$, $c_i^* = \langle\psi, \varphi_i\rangle$. This means $|c_i|^2 = \langle\psi|P_i|\psi\rangle$. From the first property of the projection operators and the fact that they are Hermitian, we can write:

$$|c_i|^2 = \langle\psi|P_i|\psi\rangle = \langle\psi|P_i^2|\psi\rangle = \langle\psi|P_i^\dagger P_i|\psi\rangle \tag{2.15}$$

Therefore, we can write the probability to measure an outcome i (an eigenvalue) as:

$$p(i) = \langle\psi|P_i^\dagger P_i|\psi\rangle \tag{2.16}$$

To any self-consistently and well defined observable (position, energy, momentum) $A$, there exists a linear, Hermitian operator $\hat{A}$ acting on a Hilbert space such that the measurement of that specific observable gives one of the eigenvalues of $\hat{A}$. The main problem of quantum mechanics is to determine a Hilbert space such that it is the eigenspace of maximum number of commuting operators (matrices) used in quantum computing.[4]

Another important concept in quantum mechanics is phase. Phase can refer to different things depending on context. If we consider the state $e^{i\theta}|\psi\rangle$, this is actually equivalent to the state $|\psi\rangle$ and $e^{i\theta}$ is the global phase factor. We can show that the global factor does not change the measurement of the state. Using 2.16, we can show that for state $|\psi\rangle$, $p(i) = \langle\psi|P_i^\dagger P_i|\psi\rangle$. If we calculate the probability for the state $e^{i\theta}|\psi\rangle$, we have $p(i) = \langle\psi|e^{-i\theta}P_i^\dagger e^{i\theta}P_i|\psi\rangle$. Due to $e^{-i\theta}e^{i\theta} = 1$, the probabilities are equal. This means the measurement was not affected by the global phase factor. [2]

Another phase definition is the relative phase. Consider the states $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The amplitudes are different in this case, differing only in sign. A relative phase is defined as when the amplitudes $\alpha$ and $\beta$ can be written as $\alpha = e^{i\theta}\beta$, in which $\theta$ is a real number. The difference between relative phase and global phase is that relative phase is base-dependent, while global phase is not. This means that two states with differing relative phase cannot be accepted as physically having the same properties and they have different measurement statistics. [2] This can be used in variations of BB84 that uses entanglement.

## 2.3 The Heisenberg Uncertainty Principle

**Theorem 1.** *If two operators $\hat{A}$ and $\hat{B}$ commute, i.e., $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} = 0$, then they have a set of non-trivial common eigenstates.*

*If they do not commute, i.e $[\hat{A}, \hat{B}] = \hat{C}$, then*

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}\Big|\langle\psi|\hat{C}|\psi\rangle\Big| \tag{2.17}$$

*with respect to any state $|\psi\rangle$. Here,*

$\Delta\hat{A} \equiv$ *Standard deviation in measuring* $\hat{A}$

$\Delta\hat{B} \equiv$ *Standard deviation in measuring* $\hat{B}$

$\Delta\hat{A}$ *is defined as*

$$[\Delta\hat{A}]^2 = \langle\hat{A}^2\rangle - (\langle\hat{A}\rangle)^2 \tag{2.18}$$

The equation 2.17 is the Heisenberg inequality.

Proof: Suppose we have two Hermitian operators $\hat{A}$ and $\hat{B}$. Their expectation values are $\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle$ and $\langle\hat{B}\rangle = \langle\psi|\hat{B}|\psi\rangle$. Since both $\hat{A}$ and $\hat{B}$ are Hermitian operators, their expectation values are real numbers.

We also have two values, the commutator $[A, B]$ and the anti-commutator $\{A, B\}$ of $\hat{A}$ and $\hat{B}$ defined as $\hat{A}\hat{B} - \hat{B}\hat{A}$ and $\hat{A}\hat{B} + \hat{B}\hat{A}$ respectively.

We define $\sigma_A = \hat{A} - \hat{I}\langle\hat{A}\rangle$. This is defined such that $\langle\sigma_A^2\rangle$ is defined as the mean square deviation in statistics and $(\Delta\hat{A})^2 = \langle\sigma_A^2\rangle = \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2$. Therefore, standard deviation in measuring $\hat{A}$ is defined as $\Delta\hat{A} = \sqrt{\langle\sigma_A^2\rangle}$. [25]

Now we will introduce the Cauchy-Schwarz inequality. [25]

Let $|\Phi\rangle = |\psi\rangle + \alpha\,|\varphi\rangle$

$$\Rightarrow \langle\Phi, \Phi\rangle = (\langle\psi| + \alpha^*\,\langle\varphi|)(|\psi\rangle + \alpha\,|\varphi\rangle)$$

$$= \langle\psi, \psi\rangle + \alpha\langle\psi, \varphi\rangle + \alpha^*\langle\varphi, \psi\rangle + |\alpha|^2\langle\varphi, \varphi\rangle \geq 0$$

This inequality holds for any $\alpha$, so we can choose $\alpha = -\frac{\langle\varphi,\psi\rangle}{\langle\varphi,\varphi\rangle} \in \mathbb{C}$

$$= \langle\psi, \psi\rangle - \frac{\langle\varphi, \psi\rangle}{\langle\varphi, \varphi\rangle} + \left(-\frac{\langle\varphi, \psi\rangle}{\langle\varphi, \varphi\rangle}\right)^*\langle\varphi, \psi\rangle + \left|\frac{\langle\varphi, \psi\rangle}{\langle\varphi, \varphi\rangle}\right|^2\langle\varphi, \varphi\rangle \geq 0$$

We have $\langle\varphi,\psi\rangle^* = \langle\psi,\varphi\rangle$ and $|\langle\varphi,\psi\rangle|^2 = \langle\varphi,\psi\rangle\langle\psi,\varphi\rangle$

$$\Rightarrow \langle\psi,\psi\rangle - \frac{|\langle\varphi,\psi\rangle|^2}{\langle\varphi,\varphi\rangle} - \frac{|\langle\varphi,\psi\rangle|^2}{\langle\varphi,\varphi\rangle} + \frac{|\langle\varphi,\psi\rangle|^2}{\langle\varphi,\varphi\rangle} \geq 0$$

$$\langle\psi,\psi\rangle\langle\varphi,\varphi\rangle - |\langle\varphi,\psi\rangle|^2 \geq 0$$

$$\langle\psi,\psi\rangle\langle\varphi,\varphi\rangle \geq |\langle\varphi,\psi\rangle|^2 \tag{2.19}$$

Let's define $|\psi_A\rangle = \sigma_A|\psi\rangle$ and $|\psi_B\rangle = \sigma_B|\psi\rangle$ From (2.19) we have:

$$\langle\psi_A,\psi_A\rangle\langle\psi_B,\psi_B\rangle \geq |\langle\psi_A,\psi_B\rangle|^2 \tag{2.20}$$

$$\langle\psi_A,\psi_A\rangle = \langle\psi|\sigma_A^\dagger\sigma_A|\psi\rangle = \langle\psi|\sigma_A^2|\psi\rangle = \langle\sigma_A^2\rangle$$

$$\langle\psi_B,\psi_B\rangle = \langle\psi|\sigma_B^\dagger\sigma_B|\psi\rangle = \langle\psi|\sigma_B^2|\psi\rangle = \langle\sigma_B^2\rangle$$

$$\langle\psi_A,\psi_B\rangle = \langle\psi|\sigma_A\sigma_B|\psi\rangle = \langle\sigma_A\sigma_B\rangle$$

From (2.20) we have:

$$\langle\sigma_A^2\rangle\langle\sigma_B^2\rangle \geq \langle\sigma_A\sigma_B\rangle$$

From the definition of the commutator and the anti-commutator we have:

$$\sigma_A\sigma_B = \frac{1}{2}[\sigma_A,\sigma_B] + \frac{1}{2}\{\sigma_A,\sigma_B\} \tag{2.21}$$

$$[\sigma_A,\sigma_B] = (\hat{A} - \langle\hat{A}\rangle)(\hat{B} - \langle\hat{B}\rangle) - (\hat{B} - \langle\hat{B}\rangle)(\hat{A} - \langle\hat{A}\rangle) = \hat{A}\hat{B} - \hat{B}\hat{A} = [\hat{A},\hat{B}] \tag{2.22}$$

Next, we try to find $\langle\sigma_A\sigma_B\rangle$.

Using (2.22) in (2.21), we have:

$$\sigma_A\sigma_B = \frac{1}{2}[\hat{A},\hat{B}] + \frac{1}{2}\{\sigma_A,\sigma_B\}$$

$$\langle\sigma_A^2\rangle\langle\sigma_B^2\rangle \geq |\langle\sigma_A\sigma_B\rangle|^2 = \left|\frac{1}{2}\langle[\hat{A},\hat{B}]\rangle + \frac{1}{2}\langle\{\sigma_A,\sigma_B\}\rangle\right|^2 \tag{2.23}$$

Now we will show that

$$\left|\frac{1}{2}\langle[\hat{A},\hat{B}]\rangle + \frac{1}{2}\langle\{\sigma_A,\sigma_B\}\rangle\right|^2 = \left|\frac{1}{2}\langle[\hat{A},\hat{B}]\rangle\right|^2 + \left|\frac{1}{2}\langle\{\sigma_A,\sigma_B\}\rangle\right|^2 \tag{2.24}$$

This is due to the fact that the commutator of Hermitian operators is anti-Hermitian and hence the expectation value is an imaginary number, while the anti-commutator of Hermitian operators are Hermitian, hence the expectation value is a real number. We will show this below.

For any Hermitian $\hat{A}$ and $\hat{B}$, we have

$$[A,B]^\dagger = (\hat{A}\hat{B} - \hat{B}\hat{A})^\dagger = \hat{B}^\dagger\hat{A}^\dagger - \hat{A}^\dagger\hat{B}^\dagger = \hat{B}\hat{A} - \hat{A}\hat{B} = -[A,B] \tag{2.25}$$

$$\{A,B\}^\dagger = (\hat{A}\hat{B} + \hat{B}\hat{A})^\dagger = \hat{B}^\dagger\hat{A}^\dagger + \hat{A}^\dagger\hat{B}^\dagger = \hat{B}\hat{A} + \hat{A}\hat{B} = \{A,B\} \tag{2.26}$$

Let $\hat{A}^\dagger = -\hat{A}$, then $\langle\hat{A}\rangle^* = \langle\psi|\hat{A}|\psi\rangle^* = \langle\psi|\hat{A}^\dagger|\psi\rangle$

$$= -\langle\psi|\hat{A}|\psi\rangle = -\langle\hat{A}\rangle$$

This means from (2.25) that $\langle[A,B]\rangle^* = -\langle[A,B]\rangle$, which means it's an imaginary value.

From (2.26) $\langle\{A,B\}\rangle^* = \langle\{A,B\}\rangle$, meaning it's a real value.

Hence, as stated 2.23 can be written as:

$$\langle\sigma_A^2\rangle\langle\sigma_B^2\rangle \geq \left|\frac{1}{2}\langle[\hat{A},\hat{B}]\rangle\right|^2 + \left|\frac{1}{2}\langle\{\sigma_A,\sigma_B\}\rangle\right|^2$$

$$\langle\sigma_A^2\rangle\langle\sigma_B^2\rangle \geq \left|\frac{1}{2}\langle[\hat{A},\hat{B}]\rangle\right|^2$$

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}|\langle[A,B]\rangle|$$

This completes our proof.

Heisenberg's Uncertainty Principle tells us that simultaneous measurement of two non-commuting observables is impossible as there is a lower limit given by the principle. If one makes two projective measurements of non-commuting observables at the same time, one cannot measure both of them with certainty. This is only valid in quantum mechanics. Classical physics does not have such a restriction.

If observables commute, then they have common eigenstates with different eigenvalues. Then simultaneous measurement is possible.

The importance of the Heisenberg principle tells us that one cannot simultaneously measure a state with two non-commuting observables. We know that when a state $|\psi\rangle$ is measured, it collapses into one of the observer's eigenstates. Two non-commuting observables will have different eigenstates, while commuting observables have the same eigensates for different eigenvalues. If the state $|\psi\rangle$ is measured simultaneously by two non-commuting states $A$ and $B$, it will collapse to an eigenstate of $A$ with a probability given in 2.9. When the measurement with $B$ is performed, it collapses in to an eigenstate of $B$. When measured by $A$ again, we get different outcomes, with the given probabilities. Therefore, we can say that the measurement of a state by non-commuting observables disturbs one another.

We can give an example to this as follows. Suppose we have two observables and they have the following eigenstates: $|0\rangle$ and $|1\rangle$ for one observable ($\hat{\sigma_z}$) and $\begin{bmatrix}1\\1\end{bmatrix}$ and $\begin{bmatrix}1\\-1\end{bmatrix}$ for the other observable $\hat{\sigma_x}$. We suppose we first measure the state $|0\rangle$ with $\hat{\sigma_z}$, then $\hat{\sigma_x}$ and then $\hat{\sigma_z}$ again.

In our first measurement we get $|0\rangle$, with probability 1 as $|0\rangle$ is an eigenstate of $\hat{\sigma_z}$ and $|\langle(1,0),(1,0)\rangle|^2 = 1$.

As can be seen, the state $|0\rangle$ collapses in to one of the eigenstates of $\hat{\sigma_z}$, which is also $|0\rangle$, so we have an exact measurement.

Now, we measure this resulting state with $\hat{\sigma_x}$. Since the observable $\sigma_x$ has eigenstates $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$, the state collapses in to $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ with a probability of $\left|\langle(1,0),\frac{1}{\sqrt{2}}(1,1)\rangle\right|^2 = \frac{1}{2}$ and $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$ with a probability of $\left|\langle(1,0),\frac{1}{\sqrt{2}}(1,-1)\rangle\right|^2 = \frac{1}{2}$. Since they have equal probability, we can suppose that the resulting state was $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$. Now, we measure once more with $\hat{\sigma_z}$.

When measured by $\hat{\sigma_z}$, the state we have either collapses to $|0\rangle$ or $|1\rangle$. The probabilities of each are as follows. $\left|\langle\frac{1}{\sqrt{2}}(1,-1),(1,0)\rangle\right|^2 = \frac{1}{2}$. This means there is a $\frac{1}{2}$ probability of getting $|0\rangle$ and $\frac{1}{2}$ probability of the result being $|1\rangle$. This means the system was disturbed as in our first measurement of $|0\rangle$ with $\hat{\sigma_z}$ we had a 100% chance of the state collapsing to $|0\rangle$, while after simultaneous measurements it is only 50%.

More succinctly, the Heisenberg uncertainty principle tells us that if $\hat{A}$ and $\hat{B}$ are non-commuting observables, the accuracy of their simultaneous measurement is limited. $\Delta\hat{A}\Delta\hat{B}$ is the Heisenberg inequality. Accurate simultaneous measurement of $\hat{A}$ and $\hat{B}$ is impossible with non-commuting observables and increasing accuracy in one observable results in the diminishing accuracy of the other. This will be important in the security of the BB84 Protocol.

## 2.4 The No-Cloning Theorem

The no-cloning theorem was discovered in the early 1980s and is one of the earliest results of quantum computation and quantum information. It is one of the differences between classical and quantum information.

The no-cloning theorem tells us that it is not possible to clone a qubit in an unknown state. To be more precise, it is not possible to build a device that copies two non-orthogonal states.

We will present two proofs for no-cloning.

**Theorem 2.** *Any general superposition state of a quantum system cannot be cloned (copied) by any unitary transformation $\hat{U}$.*

*Proof: Let us assume that there is such a transformation as:[4]*

$$\hat{U}[|\varphi\rangle \otimes |0\rangle] = |\varphi\rangle \otimes |\varphi\rangle \tag{2.27}$$

*If $|\psi\rangle$ and $|\varphi\rangle$ are linearly independent,*

$$\hat{U}\,|\varphi 0\rangle = |\varphi\varphi\rangle\,, \quad \hat{U}\,|\phi 0\rangle = |\phi\phi\rangle \tag{2.28}$$

*Consider the superposition state,*

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\varphi\rangle + |\phi\rangle] \tag{2.29}$$

$$\hat{U}[|\psi 0\rangle] = \frac{1}{\sqrt{2}}[|\varphi\varphi\rangle + |\phi\phi\rangle] \tag{2.30}$$

*But,*

$$\begin{aligned}\hat{U}[|\psi 0\rangle] &= |\psi\psi\rangle \\ &= \frac{1}{\sqrt{2}}[(|\varphi\rangle + |\phi\rangle) \otimes (|\varphi\rangle + |\phi\rangle)] \\ &= \frac{1}{\sqrt{2}}[|\varphi\varphi\rangle + |\varphi\phi\rangle + |\phi\varphi\rangle + |\phi\phi\rangle]\end{aligned}$$

*Obviously, these two results are not the same.*

For the second proof we will use pure states and a unitary transformation for the cloning device.

**Theorem 3.** *Suppose there are is a machine with two slots A and B. The slot A receives the qubit to be cloned and it will be cloned in slot B. So, we can say A has the unknown state $|\psi\rangle$ and B has the qubit $|s\rangle$. Therefore, the state of the device can be shown as: [2]*

$$|\psi\rangle \otimes |s\rangle$$

*Using a unitary evolution $U$, we have:*

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{2.30}$$

*Now, we suppose this copying procedure works for two pure states $|\psi\rangle$ and $|\phi\rangle$. Then we can write:*

$$\begin{aligned}U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U(|\phi\rangle \otimes |s\rangle) &= |\phi\rangle \otimes |\phi\rangle\end{aligned}$$

*Taking the inner product of the two equations gives us the below equation since unitary operations preserve inner product and the inner product of tensor product translates to multiplication.*

$$\langle\psi|\phi\rangle \cdot 1 = (\langle\psi|\phi\rangle)^2 \tag{2.31}$$

*This gives us either* $\langle\psi|\phi\rangle = 1$ *or* $\langle\psi|\phi\rangle = 0$.

*In the first case, we have* $|\psi\rangle = |\phi\rangle$*, which makes them the same state. If* $\langle\psi|\phi\rangle = 0$ *then* $|\psi\rangle$ *and* $|\phi\rangle$ *must be orthogonal to each other.*

Therefore, although a machine can clone the states $|0\rangle$ and $|1\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ as they are pairwise orthogonal, no device can clone all of them. This will be important in the secure implementation of the BB84 protocol.

We will use pure states in quantum key distribution, hence these proofs are deemed sufficient.

## 2.5 Entanglement

Entanglement is observed in composite quantum systems. It means there are correlations between measurements performed on well separated particles. [3]

Suppose we have a bi-partite Hilbert Space

$$\mathbb{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

A basis of $\mathbb{H}$ can be construct from the basis of $\mathcal{H}_1$ and $\mathcal{H}_2$ such that

$$\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}$$

From the superposition principle, the most general way to write a state in $\mathbb{H}$ is:

$$|\psi\rangle = \sum_{i,j=0}^{l} c_{i,j} |i\rangle_1 \otimes |j\rangle_2$$

If a state is entangled, it cannot be written as the tensor product of two states.

If it is separable, it is possible to write it as

$$|\psi\rangle = |\alpha\rangle_1 \otimes |\beta\rangle_2$$

For example

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

is entangled.

The state

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

can be written as

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$$

so it is separable.

If the take the entangled state

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and give one particle to Alice and the other to Bob, Alice's measurements will affect Bob's as well. This means that even if there is a distance between the particles, Alice's measurement will have an effect on Bob's measurement.

Entanglement is not a necessarily used in the implementation of the BB84 Protocol. However, it can be used to increase the security of the protocol by overcoming weaknesses arising from hardware.

# Chapter 3

# The BB84 PROTOCOL

The BB84 Protocol was presented by Charles Bennett and Gilles Brassard in 1984. The first demonstration was conducted in 1989. [7]

## 3.1 The Implementation

This protocol makes use of two alphabets (or axis) and four quantum states. The states used are:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

The states can be shown in the Bloch sphere.

As can be seen, the states $|0\rangle$ and $|1\rangle$ are rectilinear, while the states $|+\rangle$ or $|-\rangle$ are diagonal. Although, the Bloch sphere does not show this, it can be easily shown that $|0\rangle$ and $|1\rangle$ are orthogonal with each other and the same is true between $|+\rangle$ and $|-\rangle$.

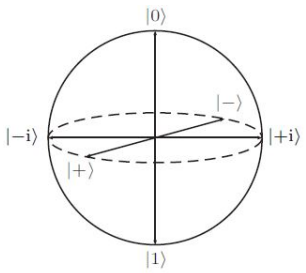


Figure 3.1: The Bloch Sphere

As can be seen, these states are not mutually orthogonal. $|0\rangle$ and $|1\rangle$ are orthogonal as $\langle \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix} \rangle = 0$. $|+\rangle$ and $|-\rangle$ are orthogonal as well, since $\langle \frac{1}{\sqrt{2}} \begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix}1\\-1\end{bmatrix} \rangle = 0$. However, if we compare the inner products of $|0\rangle$ and $|+\rangle$, we have $\frac{1}{\sqrt{2}} \neq 0$, hence they are not orthogonal. This property will be used later.

The alphabets used by the sender (Alice) and the receiver (Bob) are based on Paulis spin matrices, $\hat{\sigma_x}$ and $\hat{\sigma_z}$.

The protocol is pictured below. [5]

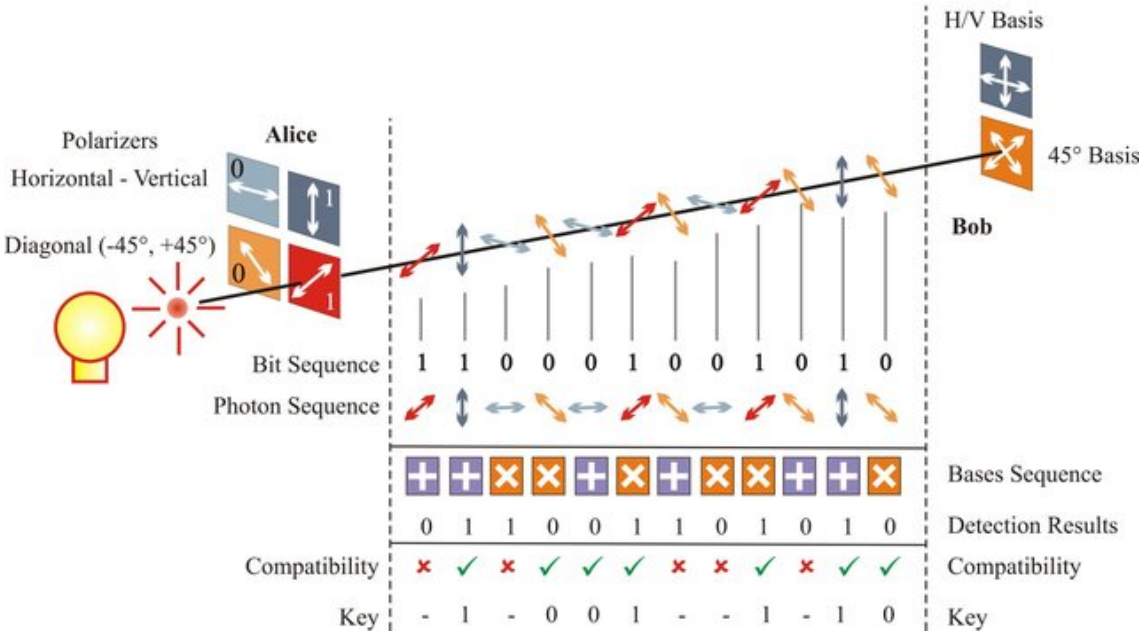


Figure 3.2: The BB84 Protocol

The steps are as follows:

1. Alice generates a random sequence of bits.

2. She encodes the bits using the $x$-alphabet ($\hat{\sigma_x}$) or the $z$-alphabet ($\hat{\sigma_z}$). For each bit, she chooses the alphabet she will use randomly.

   If she has bit 0, she obtains the state/qubit $|0\rangle$ using the $z$-alphabet and the state $|+\rangle = |0\rangle_x$ using the $x$-alphabet. When she encodes bit 1, she obtains $|1\rangle$ using the $z$-alphabet and the $x$-alphabet gives the state $|-\rangle = |1\rangle_x$.

3. Alice sends the sequence of qubits to Bob using a quantum channel. This is done through the transmission of polarized photons.

4. Bob also randomly chooses the $x$-alphabet or the $z$-alphabet in order to measure the sequence of qubits sent by Alice.

5. Neither Alice nor Bob have any information regarding the alphabet the other party has chosen for any of the bits. Therefore, by the randomness in the selection of the alphabets, it can be concurred that about half the time they will have chosen the same alphabet.

6. In the cases that Alice and Bob chose the same alphabet, Bob will be able to measure which bit was sent by Alice with a 100% certainty. In the case that they chose different alphabets, Bob only has a 50% chance of correctly finding the qubit sent by Alice.

   For instance, if Alice chooses the bit 1 and the alphabet $x$, then the qubit she sends is in the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. When Bob receives this state, if he chose the alphabet $x$, then he obtains the result 1. If he uses the $z$ alphabet, then he has a 50% chance of measuring 0 (if the state collapses to $|0\rangle$) and 50% chance of measuring 1 (if the state collapses to $|1\rangle$).

7. After Bob has completed the measurements, Alice and Bob share their alphabet through a public channel. The important aspect is that this is done after the measurement and neither Alice nor Bob share their results. They only share the alphabets they used.

   It should be noted that Bob does not know which of the results he obtained is correct until the alphabets are shared, as he does not know which measurements were 100% true.

8. After information sharing both Alice and Bob compare the sequence of alphabets and discard the qubits for which they did not use the same alphabet. It can be said that if they started with a sequence of $4n$ qubits, then they are left with approximately $2n$ qubits after this procedure.

9. For the next step they send a certain amount of the bits to each other through a public channel and try to ascertain the error rate.

10. The error rate could be high due to noise or an adversary (Eve). If the error rate is too high they discard everything and start the protocol again. If the error rate is acceptable they continue with *information reconciliation* and *privacy amplification*. The latter method reduces Eve's information about the shared key. After these procedures, the length of the key is reduced. However, for security, these are necessary steps.

## 3.2 The Security of The BB84 Protocol

The BB84 Protocol is considered information-theoretic secure with the one time pad (OTP). This means that it cannot be broken despite the supposed computational power of an adversary. However, since the OTP implementation is not efficient due to the long key size required, AES implementation is also deemed secure if used with longer keys and it has true randomness such as through the use of quantum random number generators. [32]

An important aspect regarding security is authentication. The BB84 Protocol should be used with the Wegman Carter authentication during the sharing of the bases. Unless authentication is ensured, Eve will be able to launch a man-in-the-middle attack in which she communicates both with Alice and Bob, while both Alice and Bob assume that they are talking to each other. This way Eve will be able to establish a secret key with Alice and another secret key with Bob. She will intercept their communication and act like Alice to Bob and Bob to Alice without any of them noticing. [19]

The security of the BB84 Protocol lies in quantum physics and principles already mentioned in the report. They will be detailed below.

We already know states that are measured collapse to one of the eigenstates of the observable operator. In addition, if two commuting observables are used, then they have common eigenstates. If the observables do not commute, then this is not the case.

The Paulis spin matrices that are used for the alphabet are:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3.1}$$

We check if they commute using the below formula:

$$[\hat{\sigma_x}, \hat{\sigma_z}] = \hat{\sigma_x}\hat{\sigma_z} - \hat{\sigma_z}\hat{\sigma_x}$$

$$\begin{aligned}[\hat{\sigma_x}, \hat{\sigma_z}] &= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} - \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \\ &= \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} - \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix} = \begin{bmatrix}0 & -2\\ 2 & 0\end{bmatrix} = 2\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} \neq 0\end{aligned}$$

Therefore, we can say that $\hat{\sigma_x}$ and $\hat{\sigma_z}$ do not commute. Hence, we can say that they do not share common eigenstates.

If we want to measure the Heisenberg inequality, we have:

$$\Delta\hat{\sigma_x}\Delta\hat{\sigma_z} \geq \frac{|\langle\psi|[\hat{\sigma_x}, \hat{\sigma_z}]|\psi\rangle|}{2} \tag{3.2}$$

We have as $\psi$ for states:

$$\begin{aligned}|\psi\rangle = |0\rangle &= \begin{bmatrix}1\\ 0\end{bmatrix} \\ |\psi\rangle = |1\rangle &= \begin{bmatrix}0\\ 1\end{bmatrix} \\ |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} \\ |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}\end{aligned}$$

The average value of $A$ is given by:

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \sum_j a_j|\langle\psi|\varphi_j\rangle|^2$$

in which $\varphi_j$'s are the eigenvectors and $a_i$'s are the eigenvalues of $A$.

In fact, the eigenvalue and the eigenvectors of these operators are given below:

for $\hat{\sigma_x}$:

$$\lambda_1 = 1 \Rightarrow |\lambda_1\rangle = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$\lambda_2 = -1 \Rightarrow |\lambda_2\rangle = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

If we normalize the eigenstates we get:

$$|\lambda_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0\rangle_x \tag{3.3}$$

$$|\lambda_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle_x \tag{3.4}$$

for $\hat{\sigma_z}$:

$$\lambda_1 = 1 \Rightarrow |\lambda_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$\lambda_2 = 1 \Rightarrow |\lambda_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\lambda_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{3.5}$$

$$|\lambda_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{3.6}$$

It can be seen that $\hat{\sigma_x}$ and $\hat{\sigma_z}$ do not share any eigenkets. By the Heisenberg Uncertainty Principle, it can be said that a state cannot be simultaneously measured by $\hat{\sigma_x}$ and $\hat{\sigma_z}$. Hence, when a bit is encoded as $|0\rangle_x$ or $|1\rangle_x$ and we measure the qubit with the $x$-alphabet, we get the right state for certain. Similarly, when a bit is encoded using the $z$-alphabet, the states $|0\rangle$ and $|1\rangle$ can be measured definitely. However, if we measure the state $|0\rangle_x$ with the $z$-alphabet, we have a 50% chance of measuring 0 and 50% chance of measuring 1. The same condition holds when the states and alphabets are reversed.

The Heisenberg inequality tells us that measurement disturbs the system as stated below and shown in Section 2.3. It is interesting to compute the Heisenberg inequality. If we take the right-hand side of the inequality in 3.2 and compute the average value of the commutator operator $[\hat{\sigma_x}, \hat{\sigma_z}]$ in measuring one of our states $|0\rangle$, we obtain:

$$\langle |\psi\rangle \, |[\hat{\sigma_x}, \hat{\sigma_z}]| \, |\psi\rangle\rangle = \langle |0\rangle \, |2 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} | \, |0\rangle\rangle = 0$$

This is interesting, because we found the right side of the Heisenberg inequality as 0, when we expected the standard deviation in measurements to be larger than 0. This is because the states that we measure are eigenstates of the observable operators as can be seen above. If we calculate the standard deviation in measuring $|0\rangle$ with $\hat{\sigma_z}$ ($\Delta\hat{\sigma_z}$), we obtain 0. This means the left-hand side of the inequality in 3.2 is also 0. This is the general case when measuring an eigenstate of an operator. The mathematics behind it are easy to see from the formula 2.18. Hence, the Heisenberg inequality still holds as we obtained $0 \geq 0$.

There are other issues to be considered as well. What if an adversary Eve, wanted to get in the way and measure the states before Bob? We know that measurement changes states. Hence, if Eve intercepts and measures the states before Bob she will have disturbed the qubits. This will result in too many errors in the secret key formed between Alice and Bob. As a result, Eve's interference will be exposed and Bob and Alice will abort the protocol.

Eve has a 50% chance (probability $\frac{1}{2}$) of choosing the same basis as Alice and therefore making correct measurements. When she sends all these disturbed states to Bob, she only has $2n$ of the $4n$ qubits that are measured correctly. In order for Bob to measure them correctly as well, Bob needs to choose the same alphabet as Eve for those $2n$ qubits. Bob only has $\frac{1}{2}$ probability of achieving this. Hence, in the overall communication between Alice and Bob, due to Eve's interference (assuming Eve intercepted all the $(4n)$ qubits sent by Alice), the error rate between Alice and Bob will be $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$, which is 25%. This error rate is too high and the protocol needs to be aborted.

A way Eve can be able to interfere without being noticed is to clone the states. That way, she can have multiple copies of the same state, measure one state and send the other non-interfered state to Bob. Bob would have no idea that the state has been interfered with and Eve can make multiple measurements and infer which qubit was sent.

Here, the security is provided by the No-cloning Theorem. By this theorem, it would be impossible for Eve to clone the unknown states she receives, as it is impossible to build a machine that clones non-orthogonal states as mentioned in section 2.4. Therefore, it can be

concurred that if Eve wants to eavesdrop, she has to make her presence known through noise and the high error rate will result in Alice and Bob in Step 9 to abort the protocol.

## 3.3 Implementation Issues

Quantum key distribution is advantageous in that it does not rely on the hardness of mathematical problems, but a disadvantage it has is that it is heavily reliant on hardware.

The protocol depends on the the emitting and detection of single photons. Photons are very small particles of energy and it is very difficult to send them separately. For this reason, the BB84 protocol is liable to Photon Number Splitting Attacks (PNS).

This is the most prominent weakness regarding the security of the protocol. In the PNS attack, due to the fact that more than one photon is emitted at a time, it is possible for Eve to eavesdrop and make use of the multi-photons to make her measurements without being detected by Alice or Bob. She can make her measurements on one photon and send the other to Bob as if she were able to clone the photons. In order to safely transfer photons without being subject to PNS, using decoy photons has proven itself to be a good solution. The decoy protocol was invented in 2005 independently by Lo et al. and Wang. [7]

In a decoy quantum key distribution (QKD) implementation, photons with differing intensities are sent. One set has high intensity, while another (or others) are of low intensity. The difference in intensity means that their photon number distributions are different. They are the same in all other aspects such as wavelength, timing information, etc, which makes them indistinguishable to an adversary Eve. The original photons are used for key generation, while the decoy photons are used to detect interference by an adversary. Eve only knows the number of photons that are being transmitted in a signal. The yield is the amount of photons absorbed at per unit time, and bit error rate can only depend on the number of photons and not whether a state is real or decoy. Alice and Bob know the acceptable amount for both the yield and the bit error rate. Hence, if Eve interferes, these values will be changed and Alice and Bob will be aware that their communication is under attack. [15]

Entanglement can also be used to detect PNS attacks. The original BB84 Protocol does not used entangled photons, however, the protocol can be implemented with entangled states in order to detect Eve's interference. Researchers have proposed various ways to use entanglement as a variance in the BB84 Protocol and they all rely on not the avoidance of the PNS attack, but the ability to detect it. Eve can use a measurement type called quantum non-demolition to measure the number of photons emitted in a pulse. This lets her detect when multiple photons are emitted at once, without disturbing the system. Sabottke

et al. introduce an entangled state into the system to detect Eve when she uses quantum non-demolition measurements. In this scheme, Alice and Bob use phase entangled states, which actually serve as photons and are not used for key formation. Phase and the number measurements require observables that do not commute. Hence, by performing a number measurement Eve disturbs the phase entangled states, making her presence known. [8] There are also other implementations, but they are they are too varying in method to elaborate all of them. It should also be noted that entanglement is also a factor that causes challenges regarding distance especially in optical fibers.

In the Trojan horse attack, Eve can send short pulses of light to either Alice's or Bob's device and obtain information about the qubit state by the device's polarization or phase modulator settings, from the reflection of the light. There are counter measures such as active monitoring of light, or Alice can use an optical isolator or a monitoring device. [19] [20]

Another attack is the time-shift attack. Bob has different detectors to detect the bit 0 and 1 and these detectors are only active during the detection window. This detection window is timed between Alice and Bob, depending on when they expect the photon to arrive. Eve uses a possible detection efficiency mismatch between these detectors (for instance the detector for 0 to be active, while the detector for 1 is not) for her attack. She measures the photons sent by Alice and sends new photons to Bob. [9] She is able to control the arrival time of each photon to Bob, which allows her to manipulate the probability of a certain detector to detect the photons. In this scenario Eve is able to gather information about the key. Some solutions are proposed against the weakness of single photon detectors whether in the protocol implemented or the hardware used. However, solutions regarding the time-shift attack can make the system vulnerable to other attacks. [19]

One important aspect to consider is that despite the BB84 Protocol's or QKD protocols' weaknesses in implementation, their security relies on the technological advances that the adversary has at the time of the key exchange. This is in contrast to classical key distribution in which encoded messages can be stored and decoded later. Hence, this is a point that enhances the security of the BB84 Protocol for messages that need to endure time. [19]

# Chapter 4

# RECENT STUDIES IN QUANTUM KEY DISTRIBUTION

The BB84 Protocol had been introduced in 1984, but the first trial was conducted in 1989 over a distance of 32 cm with a system clock rate of 200 Hz. The achievements have increased significantly in which the distance has exceeded 100 km and the speed has gone over 1 GHz in system clock rate. QKD is also being tested in network environments. [7] [11]

The BB84 protocol makes use of photon polarization. Hence, the quantum communication channel used can be free space or an optical fibre. A challenge QKD is facing in general is the medium which will be used in sending the photons and the distance that can be achieved. In general, fibre optic cables are used for quantum key distribution. However, when photons are sent through an optical fiber cable, there is a chance that some will be absorbed. Therefore, the longer the distance of communication, the less of a chance a photon has at arriving to its destination. This causes a reduction in the key exchange rates, making long distances of communication problematic. [11]

The key exchange rate decreases as the distance is increased to the lower number of photons reaching the destination. Another issue is that the signal-to-noise ratio decreases. The increase in distance decreases the signal detection probability, while the noise probability stays the same. This means that the error rate is increased, which results in a more costly key distillation. [11]

Amplifiers or optical repeaters are considered to increase the signal strength, however, they will not help as their use will be disturbing the system. Scientists have proven that repeaters that do not disturb the system are within the realms of possibility, however, more research

is needed for its development. [10]

Another solution is building a network from trusted nodes, in order to use QKD repeaters. There are various trials of network QKD. Quantum repeaters, which are being advanced, also present a possible solution. [11]

The above concerns make quantum key distribution over long distances a difficult ordeal. However, there are trials and experiments in lengthening the distance of QKD, using fiber lines or free space with the use of satellites. The longest distance of quantum communication has been achieved using the latter method. However, it should be noted that satellite transfer is more susceptible to noise. [10]

In previous work with decoy protons, we see that the secure key rate is 10 kbit/s for a distance of 20 km and around 10 bit/s for 100 km. Unfortunately this performance does not allow for practical use. [7]

The trial by Dixon et al. in 2008 with a decoy, funded under the FP6 Integrated Project SECOQC, exceeds 1 Mbit/s over a fiber distance of 20 km. This is a first for a fiber distance trial. At a distance of 100 km, the secure key rate is 10.1 kbit/s. This is a significant increase by an order of 2 in comparison with previous work and this key rate is deemed sufficient to allow secure encryption of broadband communication. [7]

There are experiments in which photons were sent a distance exceeding 100 km, and the BB84 Protocol was implemented, however, the distance in which a PNS attack was averted is lower than 100 km. Hickett et al. (2006) state that their experiment shows that a PNS-secure QKD could be extended into a distance exceeding 100 km using TES (transition-edge sensor) detectors with a decoy state protocol.[16]

It had been also shown before that QKD could be achieved using free space for a distance of over 100 kilometers, using the BB84 Protocol. [10] New studies have taken this distance much further.

Some free space endeavours are the satellite connections established between the ground and an aircraft flying at 290 km/h in Los Alamos and Munich. China also has shown success in satellite connection with "Micius," which demonstrated a satellite-to-ground QKD over a distance of 645 to 1200 kilometers. [14]

In 2017, using Micius key formation between China and Austria was established on multiple locations, in which a maximal distance of 7600 km was reached. An intercontinental video conference was held between the Academy of Sciences between China and Austria. Also, using AES-128, a video conference, which lasted for 75 minutes was held. [13]

Another interesting medium for quantum key distribution is the water channel. An experiment conducted by Feng et al. in 2021 demonstrates that a decoy set up underwater reaches a distance 19.2 m, and it can be increased to 237.1 m in seawater with a lower dark count single photon detector. [18]

The no-cloning theorem mentioned before prevents an adversary from copying qubits, which the BB84 Protocol partly owes its security to. However, it also prevents broadcasting the identical quantum keys to more than one receiver. Therefore, BB84 Protocol is implemented on a point-to-point (P2P) basis. Regardless, QKD can be implemented in networks as well. [19]

In a QKD network, distant users $A$ and $B$ are able to share a secret key by each user being connected to a node, $NA$ and $NB$ respectively in which these nodes are connected via a chain of intermediate nodes as can be seen in the figure below. Trusted-node quantum networks can make use of repeaters to allow for an increase in distance. [28] [11]

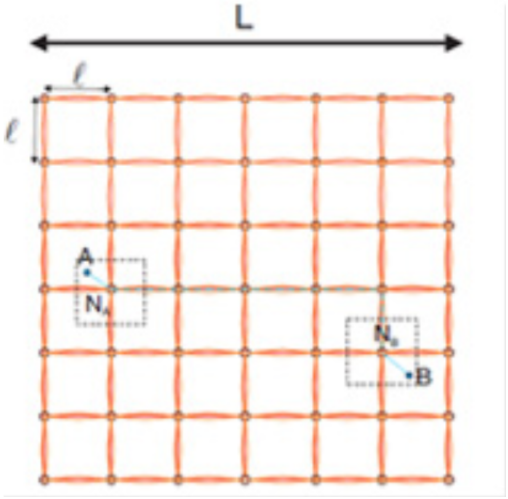


Figure 4.1: QKD Backbone Network [28]

The QKD network types can be categorized in two. In a switched QKD network a direct optical P2P QKD connection is established between any two nodes within the network. This limits the distance of the network to a regional scale. Another category is the trusted repeater QKD network. In this network type, the security of each node is essential for the transfer of information. P2P communication between nodes provides each with an identical key. This type of network is not limited by distance as there are repeaters, although a drawback is that all nodes in a communication path need to be secured. [14] Another category is full quantum-enabled networks that do not require fully trusted nodes or are not restrained by distance barriers, however the technology required is currently beyond our scope.[19]

The previously deployed, prominent QKD networks are:

1. The DARPA QKD Network
2. SECOQC QKD Network
3. Tokyo UQCC QKD Network
4. QKD Network in China
5. OpenQKD

In the DARPA QKD Network, which used 10 nodes, the researchers implemented the BB84 protocol with a pair of senders and a pair of receivers. A trusted repeated network depending on entanglement was used. It was implemented between 2002-2006 and it was the first QKD network. The maximum key rate reached was 400 bps, while the maximum distance was of 29 km between Harvard University and Boston University. [14]

The SECOQC QKD Network was formed in 2004 under the European Union funded "Framework Programme 6" project. The team comprised of 41 research and industrial partners from 11 EU countries along with Russia and Switzerland. The objective was to firmly define the practical application of QKD technologies and systematically treat the issue of QKD networks. The project was implemented between 2004-2008 and achieved a maximum key rate of 3.1 kbps over 31 km. The maximum length reached in a single link is 82 km. [14]

The Tokyo UQCC QKD Network was established two years after the SECOQQ QKD Network with participation from Japan and EU. The network consisted of parts of the National Institute of Information and Communications Technology and nodes connected to commercial optical fibers. Maximal key rate reached is 3.1 kbps, while the maximal distance of a single link is 33 km. In 2010, a secure TV conference was demonstrated using QKD. [14]

China is taking the lead in quantum key distribution and space-oriented quantum technology. The Chinese endeavours are of a national scale. The 2,000 km Beijing-Shanghai backbone QKD network, which is the longest optical fiber QKD in the world to date, commenced operation in September 2017. All the implementations so far are decoy BB84 protocols. The Beijing-Shanghai QKD network reached a maximum key rate of 250 kbps over 43 km. It deployed 32 nodes and it achieved the highest key rate over a maximum distance compared to other Chinese experiments. [14]

The OpenQKD is a project funded by the European Union under Horizon 2020. The project has 38 partners from 13 EU countries and Israel. OpenQKD can be considered as an umbrella

project with a budget of nearly 18 million Euro and a variety of work regarding QKD is underway. The project, which started in September 2019 and is planned to finish in September 2022, deploys open testbeds for quantum key distribution and is open to external stakeholders to perform trials. The project establishes the first experimental QKD testbed and 43 projects are funded under the $1^{st}$ open call. The project aims to lay the foundations for a Pan-European Quantum Network.

These endeavours include an international film festival in Berlin using QKD for film distribution, secure key distribution between governmental institutions in Greece and Austria, processing of personal medical data in CERN, recognition of composite signals in genome and protein in Portugal, interfacing satellite and terrestrial fiber connections in Italy, quantum security of crypto assets in Geneva, long term encryption to be used in clouds to encrypt only data that needs it, and securing banking institutions with QKD. [27]

Currently, in commercial endeavours with optical fibers, QKD links can be effectively applied to to roughly 100-200 km, not surpassing a hundred kbp/s. [14] [29]

The Cambridge Research Laboratory of Toshiba Europe has been able to build a quantum internet exceeding a distance of 600 km. In 2018, Toshiba had also proposed a new QKD protocol named Twin Field QKD. The said protocol has been implemented over fibres and a distance of 600 km in quantum key distribution has been reached. This technology will allow cities and countries to be connected to each other without the need of trusted nodes. It will also be possible to implement it with a Satellite QKD, making the distance covered span globally. The work was partially funded by the EU through the H2020 project, OpenQKD. [29]

There are other commercial companies working on QKD as well. These are Quintessence with their qOptica CV-QKD, MagiQ's 8505 and Q-box, AIT's EPR SYS-405 System, ID Quantique's Clavis2, SeQureNet's Cygnus and Toshiba QKD GHz system. [30] The below table provides information on recent QKD experiments using the BB84 protocol and their results regarding speed and distance. Regarding the network trials, numbers regarding the maximum key rate are used.

| QKD Trials | | | | |
|---|---|---|---|---|
| Year | Team | Method | Speed | Distance |
| 2007 | Schmitt-Manderbach et al. | Free space/Decoy | - | 144 km |
| 2008 | Dixon et al. | Decoy | 1.02 Mbps | 20 km |
| 2008 | Dixon et al. | Decoy | 10.1 kbps | 100 km |
| 2002-2006 | DARPA | Network | 400 bps | 10 km |
| 2007 | SECOQC | Network | 3.1 kbps | 33 km |
| 2009 | Tokyo | Network | 304 kbps | 45 km |
| 2010 | Liu et al. | Decoy | 15 Hz/3089s | 200 km |
| 2015 | Korzh et al. | Fiber | 3.18 bps | 307 km |
| 2017 | Beijing-Shanghai | Network | 250 kps | 43 km |
| 2016 | Liao et al. | Satellite (Micius) | 100 bps | 719 km |
| 2021 | Feng et al. | Underwater | - | 19.2 $\rightarrow$ 237.1 m |

There are already real life applications that have been performed with QKD. In 2004, a bank transfer has been made in Vienna with QKD. [10] In 2008, the first live demonstration of QKD took place, again in Vienna, in the framework of the SECOQC Demonstration and International Conference. A network was established and different company sites from SIEMENS Austria were connected. Secure telephone and video conferencing were among the services achieved. [22] In 2007, one canton (state) of Switzerland participated in the national election, in which the votes cast were transmitted to Geneva by QKD. The technology was provided by Id Quantique and the photons were transferred through a distance of 62 miles. [23] In 2013, a non-profit organisation, Battelle Memorial Institute, installed a QKD system between their main campus and their manufacturing facilities within a distance of 20 miles. The system was built by ID Quantique as well. [24]

# Chapter 5

# CONCLUSION

The BB84 Protocol has information theoretic security due to the properties of quantum mechanics when used with the OTP. The security relies on the Heisenberg's uncertainty principle and the no-cloning theorem, which show that an adversary's interference does not go undetected. The important issue here is that in using OTP, the key should be used only once. It is also deemed secure with AES, which is more efficient compared to OTP.

There are however, attacks that can be successfully performed due to hardware deficiencies. Some of these attacks are performed by an adversary that has access to encoding and decoding devices of the communicating parties. Other attacks may be harder to avoid, however, there are certain precautions that can be taken. Some of these precautions again rely on hardware, such as producing single photon sources and detectors, while others require several modifications to the implementation, such as using decoy states or entanglement. It can also be the case that modifications that resolve a threat can leave the system weak to other attacks. Research is still being developed in this area.

Other conditions that need to be in place for the security is that the parties must use authentication during the exchange of the basis to prevent a man-in-the-middle attack.

Currently, the implementation of QKD is limited due to the challenges faced in increasing the distance and the key exchange rate. There are instances of QKD being used in real life, however, we are still far from achieving a large scale QKD in an efficient manner.

Scientists have proven that it is possible to build quantum repeaters, which unlike classical repeaters, will not disturb the system while increasing the distance. However, so far this remains in theory and the technological advances are expected to be far in the future. The advancement of quantum networks will also break the distance barrier.

Overall, QKD is an expensive method and some criticise it to be too costly to have any value and real life use. As long as asymmetric algorithms continue to provide security, QKD might be seen as unnecessary and advancements may be slow. However, scientists are working on quantum computers and they are expected to be a part of our future. When quantum computers are more mainstream, public key cryptography schemes we use today will be obsolete. Although, some may see this as far in the future, it may not be such a distant future.

For the moment, increasing the key sizes might be enough as breaking them would require more quantum powers. There are two main ways to ensure that cryptography provides enough security for our everyday transactions, such as using emails and conducting bank transfers. One option is the development of quantum-resistant algorithms for key exchange. The other option is employing quantum key distribution. The latter is too costly. Perfecting quantum key distribution is a difficult ordeal. The requirements regarding hardware, along with the new satellites ans optical fibers needed pose a problem. However, there is no way to prove that a quantum-resistant algorithm will truly be secure against quantum computers. There will always be the possibility that a better computer will be able to break the algorithms. Therefore, research in many areas regarding the hardware and advancement of new QKD protocols or variants of existing protocols need to be developed in order to continue the existing level of security achieved by the use of cryptography.

# Bibliography


[1] Nigel P. Smart, 2016, *Cryptography Made Simple*, Springer International Publishing, Switzerland.

[2] M. A. Nielsen, and I. L. Chuang, 2000, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge.

[3] G. Benenti, G. Casati, G. Strini, 2004, *Principles of Quantum Computation and Information, Volume 1 - Basic Concepts*, P, World Scientific Publishing Co. Pte. Ltd.

[4] Güler, İ. Y., *Lecture Notes on Quantum Cryptography*

[5] Mavroeidis, V., Vishi, K., Zych, M. D., 2018, *The Impact of Quantum Computing on Present Cryptography*, International Journal of Advanced Computer Science and Applications 9(3).

[6] V. Mavroeidis, M. D. Zych, K. Vishi, March 2018, *The Impact of Quantum Cryptography in Present Cryptography*, International Journal of Advanced Computer Science and Applications.

[7] A. R. Dixon1, Z. L. Yuan, J. F. Dynes, A.W. Sharpe, and A. J. Shields, 2008, *Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate*, Optical Society of America.

[8] Sabottke, C. F., Richardson, C. D., Anisimov, P. M., Yurtsever, U., Lamas-Linares, A. and Dowling, J. P. 2012, *Thwarting the photon-number-splitting attack with entanglement-enhanced BB84 quantum key distribution*, New Journal of Physics 14 (2012) 043003.

[9] Qi, B., Fung C-H. B., Lo H-K., Ma, X., 2007, *Time-Shift Attack in Practical Quantum Cryptosystems*, Quantum Information and Computation, vol. 7, pp. 073-082

[10] P. Winiarczyk and W. Zabierowski, February 2011, *BB84 analysis of operation and practical considerations and implementations of quantum key distribution systems*, CADSM.

[11] ID Quantique SA, 2020 *Quantum-Safe Security White Paper: Understanding Quantum Cryptography*,

[12] Liao, S-K., Cai, W-Q, Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J-G., Liu, W-Y., Li, Y., Shen, Q., Cao, Y., Li, F-Z., Wang, F-J., Huang, Y-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N-L., Koidl, F., Wang, P., Chen, Y-A., Wang, X-B., Steindorfer, M., Kirchner, G., Lu, C-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C-Z., Wang, J-Y., Zeilinger, A., Pan, J-W., *Satellite-relayed Intercontinental Quantum Network*

[13] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan, 2018, *Satellite-relayed Intercontinental Quantum Network*, Phys. Rev. Lett. 120, 030501.

[14] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and M. Voznak, September 2020, *Quantum Key Distribution A Networking Perspective*, ACM Computing Surveys, Vol. 53, No. 5, Article 96.

[15] H. K. Lo, X. Ma and K. Chen, 2005. "Decoy state quantum key distribution," Phys. Rev. Lett. 94, 230504.

[16] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt, 2006,"Long-distance quantum key distribution in optical fibre", New Journal of Physics 8 (2006) 193.

[17] B. Korzh, C. C. Wen Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew and H. Zbinden,2015, "Provably secure and practical quantum key distribution over 307 km of optical fibre", Nature Photonics.

[18] Z. Feng, S. Li, and Z. Xu, "Experimental underwater quantum key distribution," Opt. Express 29, 8725-8736 (2021).

[19] P. Chan, I. Lucio-Martínez, X. Mo and W. Tittel, "Quantum Key Distribution", Femtosecond-Scale Optics, 2011.

[20] Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., and Leuchs, G., 2014, *Trojan-horse attacks threaten the security of practical quantum cryptography*, New Journal of Physics.

[21] Liu, Y. et al., 2010, *Decoy-state quantum key distribution with polarized photons over 200 km*, Opt. Express 18, 8587–8594.

[22] https://secoqc.network/ Accessed on 12.01.2022

[23] https://web.archive.org/web/20071209214958/http://www.technewsworld.com/story/59793.html Accessed on 12.01.2022

[24] https://web.archive.org/web/20131014104149/http://tech.fortune.cnn.com/2013/10/14/quantum-key/ Accessed on 12.01.2022

[25] https://www.youtube.com/watch?v=fsC5Mhd7YUcAccessed on 01.02.2022

[26] https://openqkd.eu/ Accessed on 12.01.2022

[27] https://cordis.europa.eu/project/id/857156 Accessed on 12.01.2022

[28] University of Waterloo Research webpage, https://uwaterloo.ca/research/waterloo-commercialization-office-watco/business-opportunities-industry/simplified-trusted-nodes-quantum-key-distribution-qkd Accessed on 06.02.2022

[29] https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/toshiba-announces-breakthrough-in-long-distance-quantum-communication Accessed on 06.02.2022

[30] https://seqre.net/seqre2014/qkd.php Accessed on 06.02.2022

[31] https://www.youtube.com/watch?v=fsC5Mhd7YUcAccessed on 06.02.2022

[32] https://www.quintessencelabs.com/quantum-safe-cyber-security/Accessed on 06.02.2022

[33] https://www.protocol.com/manuals/quantum-computing/quantum-computers-wont-break-encryption-yet Accessed on 16.02.2022

[34] https://www.pcmag.com/news/google-claims-quantum-computing-achievement-ibm-says-not-s Accessed on 16.02.2022