## 115C Quantum Mechanics

# BB84 Protocol and Quantum Key Distribution

**Emma Allen**
**June 2024**

## Contents

# 1 Introduction

Encryption can be traced back to ancient civilisations, with records dating back to 1900 BC in ancient Egypt [1]. Throughout the centuries, encryption techniques have evolved in response to the need for secure communication, with significant advancements occurring during the digital age. The creation of the internet heralded a new era of encryption, with the development of the first encryption protocols, such as the Data Encryption Standard (DES) and RSA. Since then, numerous protocols have been invented and deployed across various domains, underpinning the security of digital communication.

The security of conventional encryption protocols relies on the assumption that current computing systems lack the computational power or time required to break the encryption keys. This assumption faces a significant challenge with the emergence of quantum computing. For example, RSA, a widely used protocol, is based on the assumption that factoring large integers is computationally impossible. However, Shor's algorithm, a quantum algorithm, is capable of factoring an integer N with polynomial time complexity [2], rendering RSA vulnerable to attacks by quantum computers. Although current quantum computers are not nearly large enough to break RSA, in the future it is highly likely they will be, increasing the necessity for quantum safe communication methods.

There are multiple pieces to quantum safe communication, This document will give an overview of what necessitates secure communication and the roll Quantum Key Distribution (QKD) will play, with a focus on the BB84 Protocol. Throughout the document, Alice, Bob and Eve are used as characters to illustrate the different roles in secure communication. Alice represents the sender of a message, Bob the intended recipient, and Eve an eavesdropper.

# 2 Background

## 2.1 Quantum Mechanics Principles:

**No-Cloning Theorem:**
This theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state [3]. I will not explain a full proof here, however it is relativity simple using proof by contradiction, references to the full proof are included in the further reading.

This theorem has significant consequences throughout quantum computing; for QKD, there are two main ramifications. Firstly an Eve cannot intercept communication between Alice and Bob and perfectly copy the quantum states without altering the states in some manner before they reach Bob. Hence any attempt to intercept the message can be measured by Bob and Alice. Secondly the theorem prevents the use of certain classical error correction techniques on quantum states such as backup copies of a state in the middle of a computation is impossible. This means alternative techniques must be used error correction.

## 2.2 Classical Secure Communication Fundamentals

Classically, secure communication typically adheres to a fundamental formula comprising three essential steps:

- Authentication
- Key generation and distribution for encryption
- Data encryption and decryption

In the authentication phase, Alice and Bob establish their identities to each other, Popular ways of doing this include public key encryption or pre-shared secrets.

Key generation is the process of creating cryptographic keys that are used to encrypt and decrypt data during communication. There are two main types of key encryption: Firstly asymmetric key encryption where a pair of keys is generated; a public key and private key. The public key is shared openly, while the private key is kept secret. In this scenario, Alice would have both keys and Bob would only have the public key which he would use to encrypt his message and send to Alice who can decrypt it with the private key.

Secondly is symmetric key encryption which involves a single secret key is shared between the sender and receiver for both encryption and decryption. In order for communication to be secure the key must be created and distributed to both parties such that no eavesdropper can access it.

In the classical case, the key is always made separately then can be distributed through various methods. Many of these methods rely on algorithms such as RSA key exchange. Recall that RSA relies on the computational difficulty of factoring large numbers and as quantum computing develops this will be breakable. This is where QKD can be used, instead of relying on the computational difficulty of certain mathematical functions, QKD utilises quantum mechanics principles to provide security, furthermore, some QKD protocols will generate and distribute the key at the same time; One example of this is BB84 which will be explained in due course.

Once this key is generated and distributed to Alice and Bob. They can begin the final phase; data encryption and decryption. Effectively they can have a secure conversation. Alice can encrypt her information, send it to Bob through a public channel who then decrypts the information with the shared key, hence they are able to have a secure conversation without eavesdropping as only they have the key to decrypt the message.

## 2.3 Quantum Key Distribution

At a high level, QKD is an umbrella term for secure communication protocols that allow parties to generate and distribute a shared secret key. Once generated and distributed this key can be used to encrypt and decrypt messages. It is not used to transmit any message data, it is solely used to generate and distribute the key.

After QKD generates and distributes the key, this key is utilised alongside any encryption algorithm for encrypting and decrypting messages. These encrypted messages are then transmitted through public classical communication channels. One example of such an encryption algorithm is the classical one-time pad.[3]. At a high level this algorithm is where each plaintext character is combined with a unique key character only once to produce a ciphertext character. It is proven to be unbreakable provided the key remains secret, QKD can keep the key secret. In comparison to classical key distribution, which are fundamentally insecure because in classical physics there is nothing preventing Eve, from copying the key during its transit from Alice to Bob. For more information see further reading.

In order to generate a shared key, information is encoded in quantum states or qubits, QKD can be split into two main categories depending on which quantum mechanics property it exploits [**types˙of˙qkd**]:

*1. Prepare and Measure Protocols:*
In quantum mechanics, by taking a measurement you break the wavefunction, which cannot be replicated. This property can be exploited to detect any eavesdropping and calculate the amount of information that has been intercepted.

*2. Entanglement Based Protocols:*
Two (or more) quantum states can become entangled, therefore they can be described by a combined quantum state. One consequence is that measurement on one quantum state effects the other one. Hence if an entangled pair is shared between Alice and Bob, and Eve takes a measurement on either quantum state she will alter the overall system, revealing her presence and the amount of information she gained.

Both of these categories can be split further into discrete variable, continuous variable and distributed phase reference coding. In this discussion, our focus will be a discrete variable protocol, called BB84. At a high level, BB84 distributes a shared secret key between Alice and Bob, which is subsequently employed for symmetric encryption. This key is derived from the outcomes of measurements performed on quantum states transmitted from Alice to Bob.

The BB84 protocol was developed in 1984 by Charles Bennett and Gilles Brassard. Fundamentally, each bit of information of the key is encoded into the polarisation state of an individual photon. By the No-Cloning theorem, the polarised state of a single photon cannot be cloned or measured without disruption. Hence in order to intercept a message, Eve must make a measurement which risks disturbing a particular quantum state, or qubit, if she guesses wrong. Alice and Bob can then use information reconciliation and privacy amplification techniques to determine whether their message has been intercepted, based on the Quantum Bit Error Rate (QBER).

# 3 BB84 Protocol Explanation

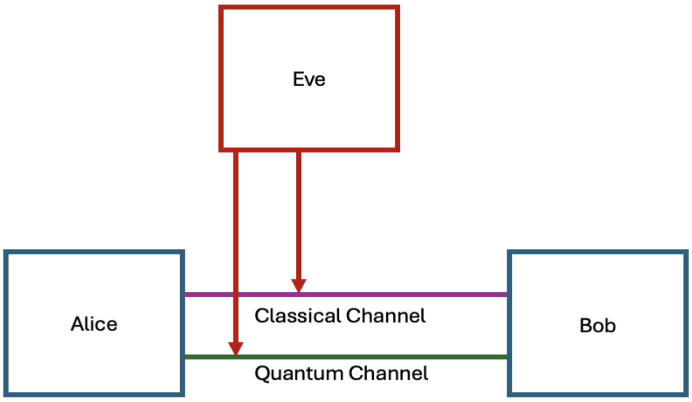

Figure 1: Figure Showing the Classical and Quantum Channels

First, we assume that Alice and Bob can communicate over a classical public channel and can send qubits over a quantum channel, see figure 1. Eve also has access to these channels and aims to acquire information without detection, however for simplicity we shall assume the channel is noiseless and there is no eavesdropping at the moment. For quantum transmissions, we use the following four qubit states [3]

$$|\psi_{00}\rangle = |0\rangle\,, \tag{1}$$

$$|\psi_{10}\rangle = |1\rangle\,, \tag{2}$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3}$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{4}$$

These states make up two orthogonal bases, $\mathcal{B}_0 = \{|\psi_{00}\rangle\,, |\psi_{10}\rangle\}$ and $\mathcal{B}_1 = \{|\psi_{01}\rangle\,, |\psi_{11}\rangle\}$. These are the Pauli Z eigenbasis and Pauli X eigenbasis. These bases are mutually unbiased. Bases are said to be mutually unbiased a system is prepared in an eigenstate of ones of the bases, then all outcomes of the measurement with respect to the other basis are predicted to occur with an equal probability. See in further reading for more information.

**Step One**

Alice generates two uniformly random binary strings $x = x_1, x_2, x_3, \ldots, x_m$ and $y = y_1, y_2, y_3, \ldots, y_m$

such that $x_i$ and $y_i \in \{0, 1\}$. Where $x_i$ represents the bit value of information and $y_i$ is her choice of quantum encoding for that bit of information. Alice prepares $m$ qubits in the states:

$$|\psi_{x_1 y_1}\rangle \, |\psi_{x_2 y_2}\rangle \dots |\psi_{x_m y_m}\rangle \, , \tag{5}$$

and sends these $m$ qubits to Bob.

**Step Two**
Bob receives the $m$ qubits, As we assume noiseless and no eavesdropping, the qubits will be in the state that Alice sent, in reality this would not always be the case.

Bob chooses a uniformly random bit string $y' = y_1, y_2, \dots, y_m$ and measures each received qubit in the basis $y'$ to get the string $x'$. The basis $y'$ is Bob's guess at Alice's choice of encoding basis ($y$) and $x'$ is essentially his guess at the information Alice is sending ($x$). Hence, we can see that if Bob guessed correctly, $y'_i = y_i$, then he knows Alice's message. However, if $y'_i \neq y_i$ then $x'_i$ is completely uncorrelated with $x_i$, as this basis is mutually unbiased, Bob's guess is either right or wrong, there is no in-between.

**Step Three**
Alice and Bob publicly reveal and compare their strings $y$ and $y'$ and their choice of basis. Note here they do not reveal the strings $x$ and $x'$ and Recall that $x$ is the message which Alice wants to send securely and $y$ is the encoding scheme. They discard all bits $x_i$ and $x'_i$ for which $y \neq y'_i$. This leaves a shorter string we shall denote $\tilde{x}$ and $\tilde{x'}$ (in this case they are equal, but that will not always be the case) of expected length $m/2$. As Bob has a probability of $1/2$ to guess the correct basis for each bit. This is under the assumption of no noise and eavesdropping, these bit strings provide a shared secret key as desired. This bit string is called the sifted key.

**Example**
To illustrate this process, consider an example where Alice randomly chooses a basis, either rectilinear or diagonal, see 2, to polarise a photon hence encoding each information bit. For each bit, she transmits a photon with the corresponding polarisation through a public channel. Bob receives these photons and measures the polarisation of each photon using his own randomly chosen basis. If Bob's basis matches Alice's, he will measure the same polarisation and can correctly determine the bit Alice intended to send. Alice and Bob then compare their bases publicly and discard all bits where their bases did not match. Assuming no noise or eavesdropping, the remaining bits form their sifted key.

This process is shown in the Table 1.

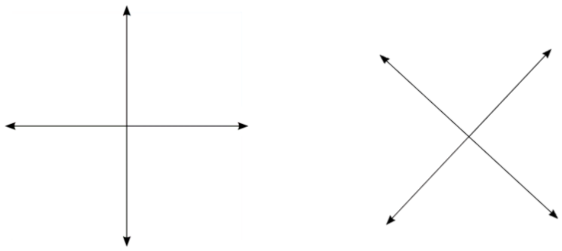

Figure 2: Rectilinear and Diagonal Basis

In practice, there will always be an amount of noise through transmission, and there is always a possibility of eavesdropping. These issues are dealt with through information reconciliation and privacy amplification. These techniques ensure that even if Eve has intercepted some of the key information, it is impossible for her to reconstruct the entire key.

| | | | | | | |
|---|---|---|---|---|---|---|
| Alice's Information Bit (x) | 1 | 1 | 1 | 0 | 0 | 1 |
| Alice's Basis (y) | × | × | + | + | × | + |
| Alice's Polarisation | ← | ↓ | ↓ | ← | ↑ | → |
| Bob's Basis (y') | + | × | × | + | × | × |
| Bob's Polarisation Measurement | ↓ | ↓ | → | ← | ↑ | ← |
| Bob's Measurement Result (x') | 0 | 1 | 0 | 0 | 0 | 0 |
| Sifted Key ($\tilde{x}$, $\widetilde{x'}$) | | 1 | | 0 | 0 | |

Table 1: Sifted Key Example

# 4 Dealing with Noise and Eavesdroppers

**Quantum Bit Error Rate (QBER):**
The QBER is defined as the ratio of incorrect bits to the total number of bits in the sifted key [3]. Mathematically, if $\tilde{x}'$ represents Bob's version of the sifted key and $\tilde{x}$ represents Alice's version, the QBER is the proportion of bits where $\tilde{x}' \neq \tilde{x}$. In the absence of errors, the QBER would be 0. These errors could be due to numerous factors such as eavesdropping, noise or equipment imperfections. There is no way to tell what caused the error therefore a certain level of QBER is expected and acceptable. The QBER can be improved through information reconciliation and privacy amplification techniques, but if it still exceeds a predefined threshold, it suggests compromised security and the key may need to be discarded. On its own QBER does not prevent attacks however it is an effective indicator of whether an attack has occurred, thus allowing the party to decide what protective measures are necessary.

In practise this is found by Alice and Bob comparing a random sample of their sifted key publicly and calculating the proportion which are the same. All announced bits are then discarded to create the new sifted key. It is assumed the remaining bits have about the same proportion of error as those checked.

**Information Reconciliation:**
The primary objective of information reconciliation is to ensure that Alice and Bob end up with a reliable shared secret key despite errors, noise and eavesdroppers. The QBER gives us a measure of errors during transmission then information reconciliation is the process used to correct errors in the shared key after transmission.

After determining the error rate through QBER (or an alternative method), information reconciliation utilises classical methods only. Example methods include the cascade method and turbo codes. See further reading for more information.

**Privacy Amplification:**
Privacy Amplification techniques aim to enhance the security of the shared key by reducing the amount of information that Eve can gain about the key. Thus these techniques ensure that even if Eve has intercepted some of the key information, it is impossible for her to reconstruct the original key.

There exists both quantum and classical privacy amplification techniques however classical techniques are more common due to their well-established security guarantees, practicality and efficiency. Furthermore it has been shown that the privacy amplification techniques of classical information theory can be shown to provide security against any possible eavesdropping strategy that's consistent with the laws of physics. One common technique is hashing, again see further reading for more information.

# 5 Potential Attacks

Although there are several methods of attach which Eve could utilise, we will focus on one, the intercept-resend attack [3]. At a high level, Eve has to intercept each transmitted qubit separately, measures it in some chosen basis to acquire some information, then sends it onto Bob in the post-measurement state.

To explain this attack we assume Alice and Bob are doing exactly the same measurements as in the previous example with the same rectilinear or diagonal basis. Furthermore we assume that the quantum channel is noiseless. Eve will intercept each qubit and take a measurement in the Breidbart Basis [4]. The Breidbart Basis is constructed by Eve using measuring apparatus at an angle of $\frac{\pi}{8}$ with respect to the encoding bases. This means that the Breidbart basis is halfway between the basis that Alice and Bob use, i.e. there is overlap with the $|+\rangle$ and $|-\rangle$ states

$$|\alpha_0\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle\,, \tag{6}$$

$$|\alpha_1\rangle = -\sin\left(\frac{\pi}{8}\right)|0\rangle + \cos\left(\frac{\pi}{8}\right)|1\rangle\,. \tag{7}$$

The overlap squared of $|\alpha_0\rangle$ with the two states $|0\rangle$ and $|+\rangle$ which were used to encode bit value 0 are equal. Mathematically, we can write this as $|\langle\alpha_0|0\rangle|^2 = |\langle\alpha_0|+\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$, and similarly for $|\alpha_1\rangle$ with $|1\rangle$ and $|-\rangle$. If any other basis is chosen, one of these four overlaps will be smaller, hence the $|\alpha_i\rangle$'s provide the best approximation to the two non-orthogonal states that were originally used to encode each bit value; and Eve will learn each bit of $\tilde{x}$ with probability $\cos^2\left(\frac{\pi}{8}\right) \approx 0.85$.

After intercepting each transmitted qubit individually, Eve measures it in a chosen basis, potentially acquiring information, before forwarding it to Bob in its post-measurement state. Subsequently, we calculate the Quantum Bit Error Rate (QBER) in the strings $\tilde{x}$ and $\widetilde{x'}$ resulting from Eve's intervention.

Bob treats each state as having an equal probability of $\frac{1}{4}$ (as he does not know what Alice will choose). The probability of Bob obtaining a specific measurement outcome given that he received a qubit in the state $|\alpha_0\rangle$ is denoted by $\mathbb{P}(B_{\text{gets}}|1\rangle \text{ — } |\alpha_0\rangle)$. Now we compute the QBER [3]

$$\begin{aligned}
&\mathbb{P}(x' \neq x) = \mathbb{P}(B_{\text{gets}}|1\rangle \text{ — } A_{\text{sent}}|0\rangle) \\
&= \mathbb{P}(E_{\text{gets}}|\alpha_0\rangle \text{ — } |0\rangle) \cdot \mathbb{P}(B_{\text{gets}}|1\rangle \text{ — } |\alpha_0\rangle) + \mathbb{P}(E_{\text{gets}}|\alpha_1\rangle \text{ — } |0\rangle) \cdot \mathbb{P}(B_{\text{gets}}|1\rangle \text{ — } |\alpha_1\rangle) \\
&= |\langle\alpha_0|0\rangle|^2|\langle 1|\alpha_0\rangle|^2 + |\langle\alpha_1|0\rangle|^2|\langle 1|\alpha_1\rangle|^2 \\
&= \cos^2\frac{\pi}{8}\sin^2\frac{\pi}{8} + \sin^2\frac{\pi}{8}\cos^2\frac{\pi}{8} \\
&= \frac{1}{4}.
\end{aligned}$$

Hence the eavesdropping with result in a disturbance amounting to a theoretical bit error rate of $\frac{1}{4}$. Once Alice and Bob have finished their key generation, they can calculate the actual QBER to see whether Eve was present or there was noise. Then they can perform information reconciliation and privacy amplification to correct some errors and limit the amount of information that Eve could gain. Throughout this process Eve is endeavouring to gain information without significantly raising the QBER, she can do this by choosing the Breidbart Basis, performing measurements and resending qubits accurately.

To illustrate this idea further, table 2 demonstrates what would happen in our previous example had there been noise and Eve were present.

| | | | | | | |
|---|---|---|---|---|---|---|
| Alice’s Information Bit (x) | 1 | 1 | 1 | 0 | 0 | 1 |
| Alice’s Basis (y) | × | × | + | + | × | + |
| Alice’s Polarisation | ← | ↓ | ↓ | ← | ↑ | → |
| Eve’s Measuring Basis | × | + | × | + | × | × |
| Eve’s Polarisation Measurement | ← | ← | → | ← | ↑ | ↓ |
| Bob’s Basis Guess (y’) | + | × | × | + | × | × |
| Bob’s Polarisation Measurement | ↓ | ↓ | → | ← | ↑ | ← |
| Bob’s Measurement Result (x’) | 0 | 1 | 0 | 0 | 0 | 0 |
| Public Discussion / Noise | Noise | No Noise | No Noise | No Noise | No Noise | No Noise |
| Sifted Key | 1 | 1 | | 0 | 0 | |
| Errors | Error | No Error | | No Error | No Error | |
| Final Sifted Key ($\tilde{x}$, $\tilde{x'}$) | | 1 | | 0 | 0 | |

Table 2: Sifted Key example with eavesdropping and noise.

In Table 2 column two demonstrates that noise in the channel leads to an error that the information bit is included in the sifted key. Through information reconciliation this error can be found and removed.

# 6 Conclusions and Future Developments

To summarise the BB84 protocol is a discrete variable QKD method that encodes information into the polarisation of the state of a photon. The key is distributed through Bob completing a series of measurements and sharing his results. This is achieved with some QBER, that can be calculated. By the no-cloning theorem, it is impossible for Eve to take a measurement without altering the quantum state, therefore any eavesdropping will be reflected in the QBER. Alice and Bob can limit the error rate and information gained by Eve through classical information reconciliation and privacy amplification.

Despite its robust framework, persistent challenges such as noise and potential security breaches persist. Techniques like privacy amplification and information reconciliation are effective mitigation techniques; however, they cannot fully solve these issues. Further challenges arise in BB84’s implementation as it requires precise alignment and synchronisation between sender and receiver for the transmission and measurement of individual qubits, posing practical hurdles.

Future developments are likely to explore alternative protocols to address these shortcomings. Promising alternatives include Continuous Variable Quantum Key Distribution (CV-QKD)[5]. This protocol has fewer alignment issues as it utilises continuous variables. Furthermore it has the potential for higher key rates compared to BB84, particularly over longer distances, thus enhancing operational efficiency. Currently, QKD is theoretically feasible, and there have been multiple successful trials; however, widespread use is still some time away. In a recent success story, researchers at The Technical University of Denmark successfully distributed a quantum-secure key using CV-QKD over a distance of 100km ($\sim$ 60 miles) [5], roughly equivalent to the distance between Oxford and London.

In the broader context of quantum networks, it is highly highly unlikely that they will fully replace their classical counterparts. Instead, they are expected to complement classical computers, as there are specific tasks at which quantum networks excel, such as networks between quantum computers and secure communications, particularly in government and military applications, where QKD will play a critical role.

Ultimately, as quantum computing advances, the vulnerabilities of classical encryption methods become increasingly apparent. Quantum cryptography, as exemplified by protocols like BB84, presents a promising foundational solution to the security challenges posed by the advent of quantum computing.

# References

[1] J. Schneider. *A Brief History of Cryptography: Sending Secret Messages Throughout Time.* Jan. 2024. URL: https://www.ibm.com/blog/cryptography-history/.

[2] S. Madane. *Shor's Algorithm.* Sept. 2023. URL: https://medium.com/@sanchit.madane.2003/shors-algorithm-bf431cac2f24.

[3] R. Jozsa. *Quantum Information and Computation.* Lecture notes for Part IIC, Lent Term 2019. DAMTP, University of Cambridge. Jan. 2019.

[4] T. Nakassis et al. "Has Quantum Cryptography Been Proven Secure". In: *Proceedings of SPIE - The International Society for Optical Engineering* 6244 (June 2006). DOI: 10.1117/12.665086.

[5] A. A. E. Hajomer et al. "Long-distance Continuous Variable Quantum Key Distribution Over 100-km Fiber With Local Local Oscillator". In: *Science Advances* 10.1 (2024), eadi9474. DOI: 10.1126/sciadv.adi9474. eprint: https://www.science.org/doi/pdf/10.1126/sciadv.adi9474. URL: https://www.science.org/doi/abs/10.1126/sciadv.adi9474.

[6] M. Mafu and F. Petruccione. "Derivation of the Quantum Bit-Error-Rate for BB84 Protocol Based on the Phase-Covariant Cloning Machine". In: *Proceedings of the 56th Annual Conference of the South African Institute of Physics.* South African Institute of Physics. 2011. URL: https://events.saip.org.za/event/14/papers/1070/files/606-JPCSLaTeXGuidelines.pdf.

[8] D. Bacon. *CSE 599d - Quantum Computing The No-Cloning Theorem, Classical Teleportation and Quantum Teleportation, Superdense Coding.* Department of Computer Science & Engineering, University of Washington. 2024.

# Further Reading

[7] YouTube. *No-Cloning Theorem Proof by Contradiction.* Accessed on 30th May 2024. 2022. URL: https://www.youtube.com/watch?v=R-en60rDT8s.

[9] Crypto Museum. *One-time pad.* https://web.archive.org/web/20140314175211/http://www.cryptomuseum.com/crypto/otp.htm. 2014.

[10] S. Yoon and J. Heo. "Efficient Information Reconciliation with Turbo Codes over the Quantum Channel". In: *International Conference on ICT Convergence* (Oct. 2013). DOI: 10.1109/ICTC.2013.6675563.

[11] B. Rijsman. *A Cascade Information Reconciliation Tutorial.* Jan. 2020. URL: https://cascade-python.readthedocs.io/en/latest/protocol.html.

[12] G. van Assche. "Privacy amplification using hash functions". In: *Quantum Cryptography and Secret-Key Distillation.* Cambridge University Press, 2006, pp. 101–112.

[13] GeeksforGeeks. *Quantum Key Distribution (QKD).* URL: https://www.geeksforgeeks.org/quantum-key-distribution-qkd/# (visited on 03/11/2024).