Quantum Key Distribution

Erin Kerciku
B.Sc Department of Computer Science
Chair of IT Security
Munich, Germany
Email: ge95huj@mytum.de

a lot unecessary specifics, too little motivation

***Abstract*—Quantum Key Distribution (QKD) uses the principles of quantum mechanics to create and exchange unbreakable keys. Photons are the information carriers between two communicating parties. To regulate the communication between two parties, protocols are needed and for multiple parties and long distances QKD networks have been developed. This field of study is developing very fast and there are hundreds of papers and studies for it. Our paper provides a comprehensive and summarized understanding of the Quantum Key Distribution and its significance in secure communication. It sums up the most important knowledge needed to enter the world of Quantum Cryptography by understanding the basics in the beginning and continuing to more complex terms. Our paper should be easily understandable by readers with low to medium knowledge in the field of maths, computer science or physics.**

***Index Terms*—Quantum Cryptography, Quantum Mechanics, QKD, photons, key distribution, protocols, QKD Network**

I. Introduction

The need for trustworthy and error-proof secure communication systems has become essential in today's increasingly interdependent society. Protecting the integrity and confidentiality of sensitive information has grown to be a major issue for people, organizations, and governments all around the world. Cryptography, the science of securing information, plays a pivotal role in creating a secure communication with the only goal to prevent unwanted access and information winning. It involves the use of mathematical algorithms to transform plain text into ciphertext, making it unreadable to third parties. Traditional cryptographic attacks, although fairly successful to some extent, face difficulties keeping up with cutting-edge technology and advanced attacks. To address these vulnerabilities, Quantum Key Distribution (QKD) has been presented as a groundbreaking and innovative solution that uses the principles of quantum mechanics to create and exchange unbreakable keys and achieve unbreakable encryption.

??

QKD employs these complex principles to allow the secure exchange of cryptographic keys between two parties. QKD utilizes the characteristics of quantum physics and quantum objects, such as photons, to construct an encryption key that is resistant to attacks, in contrast to classical cryptography, which depends on complicated algorithms and computer capacity. By going beyond the limitations of traditional cryptography and utilizing quantum phenomena like superposition and entanglement, QKD offers a high level of security. Furthermore, notable progress has also been made in real-world practical implementations of QKD systems. Researchers and engineers have successfully deployed QKD systems using technologies like fiber-optic networks and satellite-based free-space transmissions. These practical applications demonstrate the effectiveness and potential of QKD in achieving secure communication.

This paper is structured into several sections to provide a comprehensive understanding of the Quantum Key Distribution and its significance in secure communication. The Background section delves into the main concepts of the quantum mechanics. The Related Work section examines existing research and practical implementations in the field of QKD, highlighting notable protocols and advancements. Our Work section covers the core content of the paper. It begins by discussing the basics of QKD, some key terms and concepts. It is then followed by a deep-dive in the most prominent and most popular protocols, such as the BB84 Protocol. The section continues with an examination of the possible threats presented to this and other QKD protocols, while showing some of the possible solutions to these threats.

Lastly, it follows with a summary of the present state of QKD and an introduction to the QKD networks by presenting the most famous and mention-worthy networks built around the world. The paper ends by discussing the practical applications and ongoing developments in the field of Quantum Key Distribution.

The ultimate goal for this paper is to provide a middle ground between the complex principles of Quantum Key Distribution and the need for a simplified understanding of its importance in this era. This paper intends to give readers a thorough understanding of QKD's function in protecting sensitive information by dissecting the fundamental ideas of QKD, looking at its real-world application. This research also aims to present the future possibilities and breakthrough potentials of these systems in Quantum Networks.

II. Background

A. Heisenberg Uncertainty Principle

The Heisenberg uncertainty principle, formulated by the German physicist Werner Heisenberg in 1927, is a key concept in quantum mechanics that describes that the momentum and the position of a particle is impossible to be measured with

high precision at the same time [1]. Mathematically it is expressed as:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \tag{1}$$

where Δx represents the uncertainty in the measurement of the position of a particle, Δp represents the uncertainty in the measurement of the momentum of a particle, and $\hbar$ is the *reduced Planck constant* with $\hbar = h/2\pi$, which is approximately equal to $6.626 \cdot 10^{-34} \mathrm{J} \cdot \mathrm{s}$.

According to the uncertainty principle, the more accurately we try to measure the location of a particle, the less accurate the calculation of the momentum is, and vice versa. In other words, there is a trade-off between the accuracy of position and momentum measurements. The uncertainty principle derives from the concept of wave-particle duality, which states that every particle has wave-like characteristics. This means that a particle behaves both like a particle and wave at the same time. It is important to note that the uncertainty principle is not a result of limitations in experimental precision or measurement devices. Even with perfect and precise gadgets, these uncertainties would still exist. The exact value of $\Delta x \cdot \Delta p$ depends on the wave function, but with the Gaussian function it was calculated that the minimum is $\hbar/2$.

B. Hilbert Space

Hilbert spaces [2] are mathematical structures that play a fundamental role in physics and mathematics, in particular in the field of quantum mechanics, named after the German mathematician David Hilbert. A **Hilbert space** $\mathcal{H}$ is a vector space over $\mathbb{C}$ with inner product:

$$(\cdot, \cdot) : \mathcal{H} \times \mathcal{H} \to \mathbb{C} \tag{2}$$

with the norm defined as:

$$\|u\| = \sqrt{(u, u)} \tag{3}$$

satisfies the following properties: Form!

1) Linearity: $(\alpha u + \beta v, w) = \alpha(u, w) + \beta(v, w)$ because:
   a) $(u + v, w) = (u, w) + (v, w)$
   b) $(\alpha u, w) = \alpha(u, w)$
2) Complex Conjugate Symmetry: $(u, v) = \overline{(v, u)}$,
3) Positive Definite: $(u, u) = 0$ if $v = 0$, else $(u, u) \geq 0$,

In quantum mechanics, Hilbert spaces provide a mathematical framework for describing the states and dynamics of quantum systems. The state of a quantum system is represented by a vector in a Hilbert space, often denoted as a ket vector: $|x\rangle$ where x is a label. These ket vectors can be used to calculate the probabilities of different outcomes in measurements.

III. Related Work that all RW?

Information security is a relatively new field of study, but the quantum aspects of it are even newer. Quantum Key Distribution is a field which has only been studied for intensively in the last 2 decades, with the first paper about it published in 1984 by Bennet and Brassard [7]. It presents for the first time a Quantum Key Distribution protocol called BB84 and provides the basis for all the other papers and studies.

Even though not many, there have been some very noteworthy books written solely on the topic of QKD and its properties such with the top 2 books which sum up everything someone needs to know being: "Applied Quantum Cryptography" by C. Kollmitzer and M. Pivk [3] and "Quantum Key Distribution Networks" by M. Mehic , S. Rass , P. Fazio and M. Voznak [4].

Besides the books there have also been several papers, that focus on a shorter, conciser way of explaining the QKD concept or a specific detail of the QKD, which gets further explored and analyzed. Papers that are like a summary of knowledge in the field of QKD are: "A Quick Glance at Quantum Cryptography" [15], and "Quantum Key Distribution protocols: A survey" [8].

Along with these there have been some papers and studies focused on different field of the QKD. A very extensive paper in the security of the QKD Protocols is "The security of practical quantum key distribution" [5]. A great introduction and summary to all the attacks on the protocols: general and specific attacks. "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet" [20] presents a more modern approach by introducing the usage of the QKD nowadays in the so called QKD Networks and long-range communication. Other papers like [11] [12] [13] describe different aspects of the QKD protocols.

Based on the current work done in this field, the goal of this paper is to sum up the most needed and important information that currently exists on the field of Quantum Key Distribution and to provide a fully general detailed introduction to the Quantum Cryptography world and its usage for secure communication in the context of QKD Protocols and Networks.

IV. Our Work How is that better then existing RW?

A. Basic terms and Concepts

Classical information theory uses the notation of bit (short for binary digit)min its theory. A bit has only 2 possible states: 1 and 0. It can be visualized as a switch, where the "on" state represents 1 and the "off" state represents the 0. On the other hand, quantum information theory introduces the quantum representative of the bit, which is the **qubit** (quantum bit). A qubit is not limited to just the states 1 and 0, but can exist in a superposition of both basis vectors defined in the *Hilbert Space* simultaneously. For this the Dirac notation (or ket) is used: superpos ? basis vectors?

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{4}$$

with $\alpha, \beta \in \mathbb{C}$. A qubit is also a unit vector which means: intuition?

$$|\alpha|^2 + |\beta|^2 = 1 \tag{5}$$

Furthermore, the states $|0\rangle$ and $|1\rangle$ are orthogonal and orthonormal to each other, e.g.: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or $|0\rangle = \begin{pmatrix} 0.6 \\ 0.8 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} -0.8 \\ 0.6 \end{pmatrix}$

Quantum communication uses photons as information carriers such leading to the Dirac's Notation $|\psi\rangle$ to represent a light

Fig. 1. Polarization of light.

particle ψ [3]. This qubit is placed within a chosen polarization plane, such as vertical $\updownarrow$, horizontal $\leftrightarrow$, or a combination of the two (this is also called the rectilinear polarization). The qubit can then be represented as a linear combination of these polarization states. Let us denote this by:

$$|\psi\rangle = \alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle \tag{6}$$

where α and β are the probability amplitudes, in other words the probability of our measured light particle has a vertical or horizontal polarization. The other alternative polarization that can be used is called a diagonal polarization, which is a combination of the +45° polarization $|\nearrow\rangle$ (rotated by +45° with respect to $|\leftrightarrow\rangle$) and the -45° polarization $|\nwarrow\searrow\rangle$ (rotated by -45° with respect to $|\leftrightarrow\rangle$) and can be represented as:

$$|\psi\rangle = \alpha\,|\nearrow\rangle + \beta\,|\nwarrow\searrow\rangle \tag{7}$$

However, measurement/reading of a qubit is big topic in the quantum world. When either α or β is 0 then the result will surely be respectively 1 or 0. But α and β are only possibilities, which means they can take any value: $-1 \leq \alpha,\ \beta \leq 1$ Different studies and books can use the notation of $|+\rangle$ and $|-\rangle$ for $|\nearrow\rangle$ and $|\nwarrow\searrow\rangle$ respectively.CRUCIAL part missing

1) Generalized scenario of Quantum Communication: Let us analyse how 2 people, Alice and Bob, communicate with each other using light particles. As shown in Fig. 1 two polarization filters (the red squares) are used. First the Alice sends photons to Bob, the smallest particle of light and since photons are not only particles but also waves they oscillate. The oscillation happens in different directions, but when they oscillate in only one direction they are called polarized and with polarized filters we can filter photons to do this. Due to quantum mechanics it is possible to send single photons. For example Alice wants to send an up and down (vertical) oscillating photon, thus she uses a vertically polarized filter. Then the photon is directed to the second filter. If Bob is holding the filter at an angle 90° to the vertical plane such that it represents a horizontal polarization then the photon's probability of the photon passing through is 0%. If Bob uses also a vertically polarized filter as Alice then the probability of the photon passing through is 100%. However if he uses a diagonal polarizing filter then the probability is 50%. All of this happens in the quantum channel. Normally a communication in the quantum channel is followed directly by a communication in the classical channel and it needs to be kept in mind that Eve might "spy" both channels. So like for any other communication in the IT Security field we need a structured way to conduct a communication and this is called a protocol.

B. QKD Protocols

Quantum Key Distribution (QKD) protocols play a vital role in establishing secure communication channels based on the principles of quantum mechanics. These protocols can be classified into 3 main categories: discrete-variable protocols (DV-QKD), continuous-variable protocols (CV-QKD) and distributed-phase-reference protocols [5].

- **DV-QKD** - involves the use of discrete quantum states to encode information, which are represented by the polarization of single photons. The main idea is to transmit single photons over a quantum channel and measure their properties at the receivers end to establish the secret key needed for the communication. Examples of the DV-QKD include: BB84, B92, E91, SARG04.
- **CV-QKD** - utilizes continuous variables of quantum states to encode information. In CV-QKD, the quantum states are typically represented by the quadrature amplitudes of an electromagnetic field [6]. Compared to the DV-QKDs which use a single photon detector, CV-QKD protocols often involve homodyne detection (a detection method that involves a device used in signal processing that measures the quadrature amplitude). Since the amplitude value is continuous, continuous values are needed. The continuous variables are measured and used to establish a secure key.
- **Distributed Phase** - The main idea of the protocol is to encode and transmit polarization information across a quantum channel and then do measurements at the receiver's end to extract the secret key. Depending on the specific design, discrete or continuous variables can be used by these protocols.difference to DVQKD?

As BB84 is the pioneering protocol in quantum key distribution, we will further analyse various aspects of the communication involved in implementing the BB84 protocol.

C. BB84 Protocol

The BB84 protocol was invented in 1984 by Charles Benett and Gilles Brassard [7]; hence the name. This protocol utilizes the polarization properties of single photons to exchange

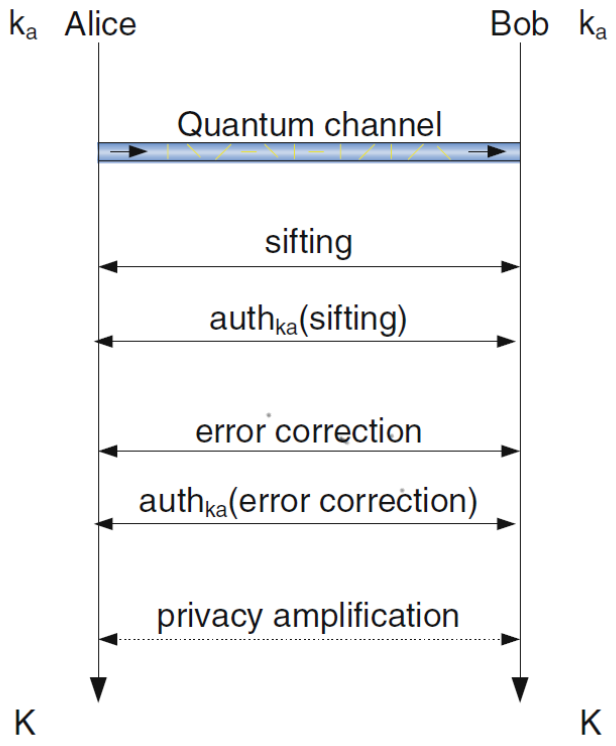

Fig. 2. BB84 protocol

information over a quantum channel. In BB84 we use the 2 bases: rectilinear (horizontal and vertical) and diagonal (+45° and -45°) as explained in (6) and (7). An simple illustration of the BB84 protocol is shown in Fig 2 [3]. k_a is the pre-shared key needed for authentication and K is the final key generated after the BB84 protocol. After the photon exchange comes: sifting (the extraction of the key), authentication of the sifting ref Quantum Bit Error Rate (QBER) estimation and correction, authentication of error correction and privacy amplification.

goal?

1) Quantum channel: The quantum channel can be very good represented by Fig. 1, where Alice is the lamp, the transmitter which sends single photons and Bob is our far right receiver, where the photon ends his journey. Alice and Bob require knowledge of the polarization state bit representation. Therefore, they agree before the communication about the representation Table I. The table is just an example, as it is up to the preference of the parties to choose what bit represents what. In our paper, we will denote the rectilinear base with 0 and the diagonal base with 1. We also denote the $|\updownarrow\rangle$ and $|\nearrow\rangle$ with the 1 bit value and the $|\leftrightarrow\rangle$ and $|\nwarrow\rangle$ with 0. Since there are four different polarization states and only 2 presentable bits, 0 and 1, so that means that there are 2 different representations for each bit and they are represented in Table I. Alice and Bob agree on the scheme before beginning their communication.

Firstly, Alice generates a random string of bases b $\in \{0,1\}^n$ to determine the basis that is going to be used and a random

TABLE I
POLARIZATION-ENCODING SCHEME

Basis	Basis representation bit	Polarization	Polarization value
$\oplus$	0	$\|\leftrightarrow\rangle$	0
		$\|\updownarrow\rangle$	1
$\otimes$	1	$\|\nearrow\rangle, \|+\rangle$	1
		$\|\nwarrow\rangle, \|-\rangle$	0

string of bits d $\in \{0,1\}^n$ to determine the choice of the polarization filter (in other words which orientation the red rectangle in Fig 1 will have), where $n > length(K)$ (K is the final key). Then for every b_i and d_i Alice sends the corresponding photon in the quantum channel [4] [8] [9]. Bob's choice for the polarization filter has a 50% chance that it is the same as Alice's. Bob creates his own string of bases b' $\in \{0,1\}^n$ and begins measuring the polarization of the received photon and creates his d' $\in \{0,1\}^n$. After both Alice and Bob have their b,d and b',d' then the next phase begins, which is *Sifting*. In a few words the next step Alice and Bob compare their bases. If $b_i \neq b'_i$, then d_i and d'_i are discarded and if they used the same bases, d_i is used for the sifted key if it the same as d'_i. Table II represents an example of a communication between Alice and Bob.

TABLE II
EXAMPLE OF COMMUNICATION ON THE QUANTUM CHANNEL

Alice's basis	$\otimes$	$\oplus$	$\otimes$	$\otimes$
Alice's polarization	$\nwarrow$	$\updownarrow$	$\nearrow$	$\nearrow$
Alice's bit	0	1	1	1
Bob's basis	$\otimes$	$\oplus$	$\oplus$	$\oplus$
Bob's measurement	$\nwarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$
Bob's measured bit	0	1	1	0
Shared secret key	0	1	1*	Error

In the first two columns Bob got lucky and chose the same basis as Alice. This means that bit that Alice sends which represents the polarization of the photon is the same as the bit that Bob reads, the same polarization. Subsequently the bit is used in the sifted key since bases and polarizations are the same. In the next 2 columns, Bob chose the rectilinear base, while Alice used the diagonal base. Alice sends the $|\nearrow\rangle$ polarized photon. Since Bob's filter can only detect $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$, he detects one of them reason not explained and then ??

2) Threats in the quantum channel: Now let us assume that there is an eavesdropper named Eve acting as a MITM (Man In The Middle). Eve uses a naive intercept-resend eavesdropping attack. Without knowing the bases Alice is using, Eve also has to choose a random base to detect the polarization. If the basis chosen correctly the polarization does not change, but if not it will change. An example of how the communication is influenced in the presence of Eve is shown in Table III.

TABLE III
EXAMPLE OF COMMUNICATION ON THE QUANTUM CHANNEL IN THE PRESENCE OF EVE

Alice's basis	⊗	⊕	⊕	⊕
Alice's polarization	↖↘	↔	↔	↕
Alice's bit	0	0	0	1
Eve's basis	⊗	⊗	⊗	⊕
Eve's polarization	↖↘	↗↙	↗↙	↕
Bob's basis	⊗	⊕	⊕	⊗
Bob's measurement	↖↘	↕	↔	↖↘
Bob's measured bit	0	1	0	0
Shared secret key	0	!!!	0*	Error

this entire section is wrong

The first column is the perfect scenario for Eve. She guessed Alice's basis correctly and Bob guessed correctly too. The same polarization that is sent by Alice is read by Eve and by Bob. the bit created goes into the sifted key and Eve's presence goes undetected. In the second column, Bob uses the same basis as Alice, which theoretically should mean that the polarization sent by Alice should be the one detected by Bob. This doesn't happen, because Eve uses the wrong basis and detects a diagonally polarized photon, ~~which is then forwarded to Bob who can detect either a vertically or horizontally polarized photon.~~ Both possibilities are shown in column 2 and 3. When Bob detects ↕, then it is the opposite of what Alice and even though they have the same basis, they got different bits, ~~which can have only one reason~~: someone is eavesdropping the conversation in the quantum channel. In the third column Bob's filter reads it right and Eve lucks out. In the third column the result just get discarded because Alice and Bob have different bases. Other reasons for the wrong detection, when the bases used are the same, can be optical misalignment, disturbance in the quantum channel or noise in the detectors.

wrong!

3) Sifting and its Authentication: Sifting is the first phase of the public channel. In this public discussion Bob and Alice share as previously mentioned which bases they used. If $b_i \neq b'_i$, then d_i and d'_i are discarded. Theoretically if the string of bases is randomly chosen Bob has to discard half of his results and notifies Alice which "i-s" did not match and Alice discards those bits too. Alice chooses afterwards a subset of the remaining bits and shares them with Bob. If Bob detects a certain amount of mismatches the results(even though same basis), something has gone wrong and the communication is aborted. Else the bits are removed and the remaining bits form the shared secret $K \in \{0,1\}^N$, also called the ***sifted key***.

Even though all of this is happening in a public channel, it is to be noted that only the bases are publicly revealed, so it isn't a problem if Eve listens. However, Eve has to be prevented from manipulating the data, therefore an authentication method comes in play. A symmetric authentication method is used in the BB84, which derives from the universal families of hash functions introduced by Wegman and Carter [10]. Since it is a symmetric authentication, a pre-shared key k_a is needed Fig. 2 This key has to be shared through a secret secure channel before the protocol starts.

4) Error Rate Estimation and Authentication: The Quantum Bit Error Rate (QBER) can be estimated by looking at the mismatches at the bit string that Alice and Bob compare with each other. The QBER value p is measured by comparing a small random subset s of the bits given from the sifted key. After the comparison a number of errors e is detected and our p is calculated by the formula:

$$p = \frac{e}{length(s)} \tag{8}$$

Both agree before on a maximum tolerance rate p_{max} regarding the bit difference. The QBER value p is ten compared with the already agree on threshold value p_{max}. If $p > p_{max}$ then this means that Eve's presence was detected or the channel has too many other interference, which regardless means that a key must not be derived by those bits. The strings are then discarded and the communication restarts. In "Applied Quantum Cryptography" book by C. Kollmitzer and M. Pivk [3] it was stated that the value of p_{max} should be 11%, because the best error correction code currently has a max toleration error rate of 12.9% [11]. If $p < p_{max}$ then Alice and Bob continue with the next step, which is error correction.

5) Error Correction: Even though $p < p_{max}$, measurement mistakes still need to be found and fixed. This process produces a "new" key, which is called a reconciled key and the process itself is called a error key reconciliation [4] [12] [13]. Detailed reconciliation methods include:

1) **Cascade** - involves dividing the raw key into blocks and performing a series of reconciliation steps. In each step, Alice and Bob compare the parity of the qubits in a block. If the parities match, the block is considered error-free and included in the final key. However, if the parities do not match, Alice and Bob engage in a binary search process to locate and correct the errors.
2) **Winnow Protocol** - uses the properties of the Hamming Code for error-correcting. It is much more faster than Cascade in practice, but it exchanges more information in the channel, therefore it is less efficient.
3) **Low Density parity Check (LDCP)** - The problem with the two above methods is that they both can only detect error in a rate of 1 bit/block, which leads to the need of frequent use of bit shuffling in the iterations. Therefore the attention was directed to higher error rate detection codes, the LDCP codes, which have a relatively low communication overhead. Even though it requires a larger computational power than the other 2, the trade-off is worth it.

6) Privacy Amplification: This is the last step of the BB84 QKD Protocol. Alice and Bob initially establish a partially correlated key (before QBER, hence partially) by comparing a subset of their measurement bases and discarding

the mismatched results. However, due to the possibility of Eve intercepting and measuring some of the qubits during the communication, there is a chance that she gained partial information about the key.

To counteract this, privacy amplification [14] [15] is performed to a shorter, secure key that has a negligible correlation with any information that Eve may possess. The basic idea behind privacy amplification is to apply a cryptographic hash function, such as the one-time pad (OTP) or a secure hash function like SHA-256, to the shared key and the random seed (Alice and Bob agree before hand on the seed). This process transforms the longer partially correlated key into a shorter key with a desired length n. The resulting output from the hash function becomes the final shared key between Alice and Bob. To make it very unlikely that Eve would know the new key, the amount by which it is would be shortened, is determined depending on how much knowledge she may have obtained about the previous key (which is known due to the calculated QBER in Eq. 8).

D. Threats

Naturally with the development of new cryptographic key distribution methods comes also the possibility of exploiting them by developing new attack strategies [3] [5]. Such attacks are:

1) **Intercept And Resend (I&R) Attack Strategies Naive Intercept and Resend** - As explained in the *Threats in the Quantum channel* section the most basic attack constructed is the naive Interception and Resend, which happens only before the sifting of the key. Eve prepares a new photon and sends it to the intended recipient, Bob. Alice's message can be in one of the 4 phases: 2 for each polarization plane. By calculation in [3] in Eve obtains 0.2 bits per bit sent by Alice. But this attack is not yet the final form of the attack.

   ??

   hier hätte der fail auffallen müssen

   Intercept and Resend in the Breidbart Basis - As mentioned we only took into consideration that Eve "spies" the channel only before sifting. But she can also obtain information during the public channel communication when they share if their bases and measurements were correct or not. In this I&R attack Eve obtains 0.4 bits per bit sent by Alice [16]. why?

   Full Intercept and Resend - This is a combination of the 2 above I&R methods which gives Eve the best probability of success. If Eve guessed the basis used by Alice correctly then she obtains 100% of the bits, but if not only 0.5 bits per bit sent.
2) **Other Attacks** These attacks have a more real-life usage, which means they exploit the imperfections of the methods, physical limitations or loopholes that can happen in real life.

   The photon number splitting attack - also known as the **PNS attack** is one of the most powerful individual attacks there exist. It exploits the low probability of realistic photon sources to generate a multi-photon pulse. This pulse has 2 or more photons of the same polarization. Eve's plan consists of blocking these pulses, grabbing one photon and sending the remaining back to Bob. After Alice and Bob exchange their measurement information in the public channel, Eve then can measure the intercepted photon using the correct measurement base [17]. why?

   Trojan Horse Attack - Mainly the victim of Eve in this case is the Alice subsystem, since it is the one sending the photons. Eve sends pre-prepared light pulses to Alice in order to obtain information about what kind of polarization filter Alice is using (reminder that the filter is the red rectangle in Fig. 1). However to detect a Trojan-horse attack effectively, Alice can incorporate a passive monitoring device within her system. This monitoring device allows Alice to detect any unauthorized access or manipulation attempts in real-time. By continuously monitoring the system's behavior, Alice can identify and respond accordingly to any suspicious activities [18].

   Faked-state attack - is a sort of an I&R attack strategy, where Eve sends pulses to Bob in a certain way to not trigger any alarms. After obtaining a result from her measurement, Eve sends a signal pulse to Bob, intentionally encoding the opposite bit value in the opposite measurement basis compared to what she detected. As a result, if Bob attempts to detect the signal pulse in a different basis than Eve, he will not register any detection. However, if Bob chooses the same measurement basis as Eve, he will either detect the same bit value as Eve or receive no detection at all. Consequently, whenever Eve measures Alice's state in the wrong basis, Bob will unknowingly measure it in the wrong basis as well, leading to the discarding of the measurement results. Conversely, if Eve chooses the correct measurement basis, Bob will also measure the state in the correct basis, maintaining the integrity of the measurement outcomes [19].

To sum up QKD protocols help the 2 parties Alice and Bob establish a secure key by exchanging quantum states and performing measurements. This secure key can then be used to encrypt and decrypt messages between Alice and Bob, ensuring confidentiality. However, all this is restricted to only a peer-to-peer communication, where Alice and Bob share the same quantum media. Can it go above these limitations?

E. Present - Quantum Networks

Quantum Key Distribution networks (QKD networks) have been developed as a revolutionary solution to secure communication, building on the foundation established by classical QKD protocols. Their aim is to create cryptographic keys between numerous participants over long distances to enable secure communication in a networked context.

To achieve this QKD networks introduce the concept of additional nodes to create links among multiple parties. These nodes are connected with quantum channels. A quantum channel links exactly only two nodes. The one-to-many behaviour

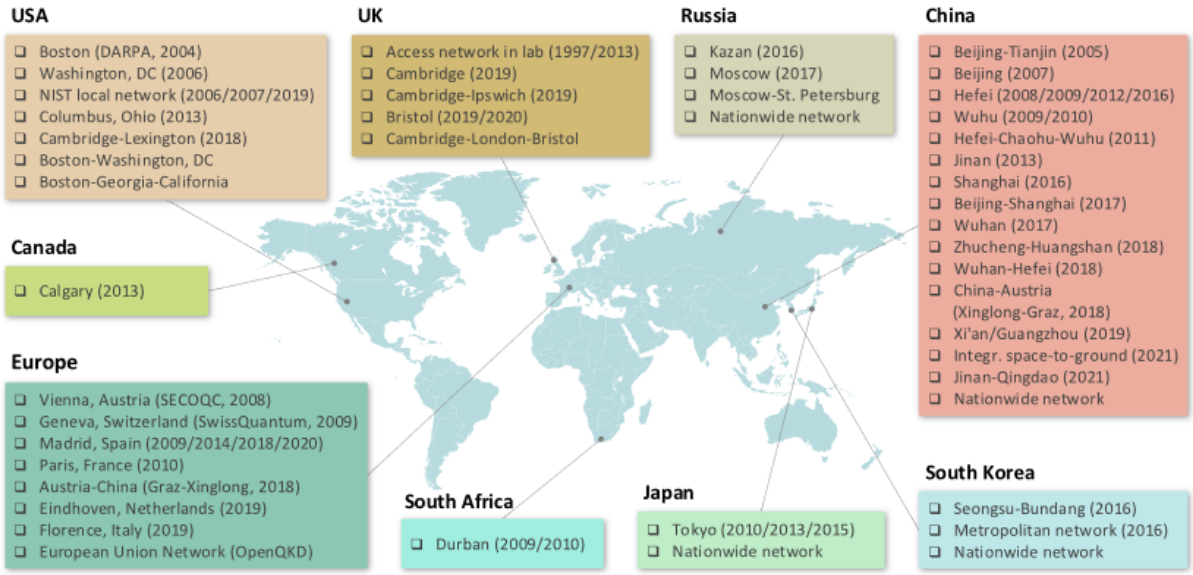

Fig. 3. Overview of the QKD networks and experiments worldwide.

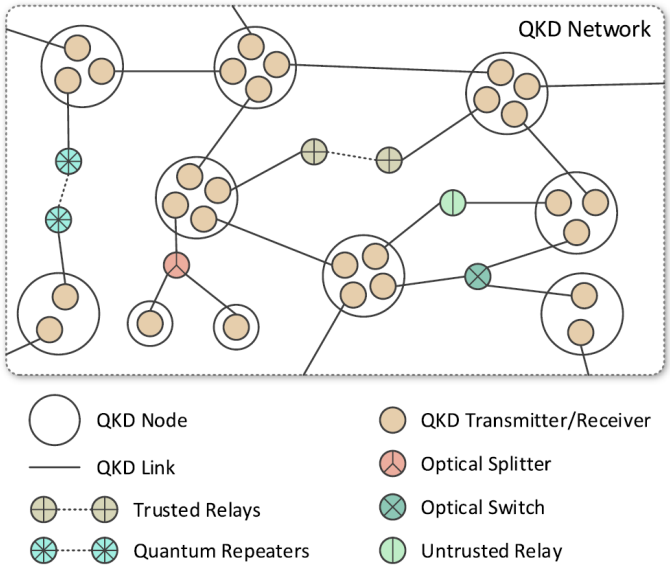

Fig. 4. Abstract illustration of a QKD Network

is created through multiple logical point-to-point connections. An abstract illustration of quantum network is represented in Fig. 4 [20], which in addition to the respective nodes has some other components such as: QKD transmitters/receivers, trusted and untrusted relays, quantum repeaters, optical switches and splitters. Quantum repeaters [21], for example, are essential for increasing the range of quantum communication across long distances. They amplify and regenerate quantum states to maintain the consistency of key distribution throughout the network. In QKD networks, quantum switches are also used to allow the routing of quantum signals between various nodes. These switches make it easier to create secure connections and allow key distribution among several network users.

Quantum Networks have been developed and experimented on around the whole world as seen in Fig. 3, where it is to be noted that China, Europe and USA are the top 3 regions mostly experimenting and further developing the new technology of Quantum Networks. Some of the first and most notable QKD networks pioneering these field of study are: *DARPA network*, *SECOQC network*, *SwissQuantum network*:

1) ***DARPA Network****:* The Defense Advanced Research projects Agency (DARPA) started building a QKD network in 2002 in Boston (also called the Boston Metropolitan Network). It had multiple "Alice and Bobs" in its structure (Alice & Bob, Anna & Boris, Ali & Baba, Alex & Barb). It became fully laboratory-operational in 2003 and in 2004 it made its real life appearance by connceting campuses in the area with a rate of 24h/day, non-stop. The DARPA Quantum Network stands as the world's pioneering quantum cryptography network and potentially the first metropolitan quantum key distribution (QKD) deployment to remain consistently operational [22].

2) ***SECOQC Network****:* Another network developed, which was introduced in 2004 was the project SECOQC (Secure Communication based on Quantum Cryptography). The goal was to provide a tool for all European citizens and institutions to face the threats of the developing modern attack strategies that would harm Europe's economy. The basis was to build long distant connection. The SECOQC Network in Vienna (also called the Vienna Metropolitan Network) was built in 2008 using telecom fiber network and was built to connect the Siemens' office buildings in Vienna, Austria. This network connected four nodes and onther station in the suburbs of Vienna, St. Pölten. The circumference of the fiber for the four nodes was $\approx 85km$. and the one that connected to St.

Pölten was $\approx 63km$. This architecture improves the DARPA network in the number of nodes and the maximum distance of key transmission. [23]

*3) **SwissQuantum Network**:* The SwissQuantum Network was installed in Geneva and it operated from 2009 to 2011. The topology of this network consists of three nodes:

- Unige (University of Geneva)
- CERN (The European Organization for Nuclear Research)
- hepia (University of Landscape, Engineering, and Architecture)

Even though this network had a relatively short lifetime, it fulfilled the 2 important prerequisites that a QKD Network should have, *reliability* and *robustness*. These two qualities were shown in a real-life environment and no longer in a laboratory. It proved that QKD can be implemented in telecommunication networks [24].

F. Application Areas and Future

Nowadays QKD Protocols and Networks are finding a popularity in increase, since many fields of life want to benefit from what they have to offer in the section of secure communication. Some real-life industries [20] that are starting to or already "exploiting" QKD features are:

- *Finance and Banking* - Very secure storage and communication of banking information such as: financial transactions, online banking, authentication. Already banks in Austria and China have started adopting QKD Networks in their architecture
- *Governments and Defense* - Protecting national secrets from unknown intruders is a goal for every country, especially for the top countries whose secrets can be exploited and used against them by their enemies. Integrity, confidentiality and authenticity is very wanted. Already QKD has been used for ballot counting in Switzerland in national elections [25]
- *Healthcare* - protecting from attacks that want to get information about the medical information of patients. That is sensitive information that can be exploited, hence why hospitals and medical centers can use QKD Networks for communicating and transmitting this sensitive information such as: patient information, past diseases, records, etc.

V. Conclusion

Quantum Key Distribution is past the up-and-rising phase and has started to be heavily studied by the top regions worldwide such as Europe, China and USA. These regions are investing extensively in QKD to enhance the security of their communication. As with BB84 from Bennett and Brassard opening the way to a new future, resources put on this field are endless.

This has lead to the emergence of many QKD protocols each using the power of Quantum Mechanics to ensure secure information transmission. Of course, with the invention of new protocols, new ways to attack them are discovered too. However, this should not be seen as a setback, rather it provides an opportunity to strengthen the protocols by implementing countermeasures and addressing these identified weaknesses.

With this paper we wanted to provide an "All You Need To Know" guide to Quantum Key Distribution not only to the ones passionate and with previous knowledge in Information Security, but also to newcomers to the field with limited knowledge of classical cryptography in general but interested and trying to read and learn something new. We covered the basics of Quantum Cryptography, delved into the foundational BB84 protocol, the first and most important one, which lays the groundwork for understanding other protocols. Additionally, we explored general attacks on QKD protocols and some of their countermeasures. In the end, we offered a concise overview of the present state of QKD development and its real-life applications.

Looking ahead, for future papers and research we would really like to dive more deeply in some other QKD protocols such as B92 or some CV-QKD protocol and also in the field of Quantum Networks, how they are built and function in detail. Our future goal is to compile a simplified representation of existing knowledge for these topics, to make understanding of complicated concepts easier for potential contributors, opening the way to further research in this field.

REFERENCES

[1] Busch, Paul, Teiko Heinonen, and Pekka Lahti. "Heisenberg's uncertainty principle.

[2] Young, Nicholas. An introduction to Hilbert space. Chapter 1.

[3] Kollmitzer, C., & Pivk, M. (2010). Applied Quantum Cryptography, vol.797. Berlin: Springer. ISBN 364-2-04829-3.

[4] Mehic, M., Rass, S., Fazio, P., Voznak, M. (2022). Fundamentals of Quantum Key Distribution, 1-24.

[5] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.

[6] Qin Liao et al 2020 New J. Phys. 22 083086

[7] Bennett, C.H., Brassard, G. (1985). An Update on Quantum Cryptography.

[8] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, Bali, Indonesia, 2018

[9] Ordavo, Ivan, and Harald Weinfurter. Free-space quantum cryptography. Diss. Diplomarbeit, Ludwig-Maximilians-Universität München, 2006.

[10] Carter, J. "Lawrence et al.," Universal Classes of Hash Functions."

[11] Smith, G., Renes, J.M., Smolin, J.A.: Better codes for BB84 with one-way post-processing (2006).

[12] Mehic, M., Niemiec, M., Siljak, H., Voznak, M. (2020). Error Reconciliation in Quantum Key Distribution Protocols.

[13] Brassard, G., Salvail, L. (1994). Secret-Key Reconciliation by Public Discussion.

[14] Bennett, Charles H., Gilles Brassards, and Jean-Marc Roberts, Privacy amplification by public discussions

[15] Lomonaco, Samuel J. "A quick glance at quantum cryptography."

[16] L. Dan, P. Chang-xing, Q. Dong-xiao, H. Bao-bin and Z. Nan, "A new attack strategy for BB84 protocol based on, Breidbart basis," 2009 Fourth International Conference on Communications and Networking in China, Xi'an, China, 2009

[17] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin and G. B. Baumgartner, "Using Modeling and Simulation to Study Photon Number Splitting Attacks,"

[18] Nitin Jain et al 2014 New J. Phys. 16 123030

[19] Vadim, Makarov., Dag, Roar, Hjelme. (2005). Faked states attack on quantum cryptosystems. Journal of Modern Optics, 52(5):691-705.

[20] Cao, Yuan, et al. "The evolution of quantum key distribution networks: On the road to the qinternet."

[21] Mehic, M., Rass, S., Fazio, P., Voznak, M. (2022). Fundamentals of Quantum Key Distribution, p. 219.

[22] Elliott, Chip, et al. "Current status of the DARPA quantum network." Quantum Information and computation III. Vol. 5815. SPIE, 2005.

[23] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," Int. J. Quantum Inf., vol. 6, no. 2, pp. 209–218, Apr. 2008.

[24] D Stucki et al 2011 New J. Phys. 13 123001

[25] "Securing Data Transfer for Elections: Ethernet Encryption with Quantum Key Distribution."