Summary

You begin by introducing the general concept of Hilbert spaces and explain them with an example. You go on to give us an introduction to wave physics and explain the concept of polarization.

Afterward, you dive into QKD. You propose different categories of protocols and eventually introduce BB84. You explain step-by-step how communication works using the protocol, what weaknesses there are (attacks, errors), and how they can be mitigated. One way to counteract random errors are error-correction mechanisms (Hamming Code, LDCP, etc.). You then explain attack vectors against QKD and show their effects on the protocol's security. Ultimately, you give us a less technical overview of where QKD stands, its impact, and its use cases in IT infrastructure.

Strengths

The paper gives a good overview of an important topic in IT security.

It provides an adequate level of understanding: It explains issues in good detail without becoming too overly complicated.

You propose different solutions to challenges (e.g., error correction, threats, etc.) and discuss their strengths and weaknesses, providing a critical point of view.

The figures used were great additions helping me understand your written text.

Weaknesses

In my opinion, the biggest weakness is the structure of the paper. I also had occasional problems understanding what you were trying to say. Some sentences seemed a little incoherent. I have marked a few instances in the paper.

Also, while the Introduction to quantum computing basics was much appreciated, some of the knowledge was not used afterward.

Overall, I would also enjoy seeing a broader context of the usage of QKD. How quickly do we need it (especially concerning post-quantum crypto)? How much has this technology already matured? How scalable is it? Do you see it as a solution for a few exceptional use cases, or will it be more widely deployed?

Paper Structure - Introduction

You are doing a few different things at the same time here:

1. Introduce the topic to the reader (Paragraphs 1 and 2)
2. Describe the contents of your paper (Paragraph 3)
3. State the goal of your paper (Last paragraph)

The middle one feels like you are writing out a table of contents. I suggest incorporating that one into the Related Work section instead. Describe what work is out there, its gaps, what your paper does, and how it fills them.

Depending on the context, the last one might fit into that category quite nicely as well.

Paper Structure - Background

Hilbert spaces left me somewhat irritated as there was no example to go with them. The examples came in the next chapter instead. Both somewhat belong to Background, in my opinion. If that's too much, you might consider putting them into their own chapter:

- XYZ: Quantum Computation Basics

- XYZ-A: Hilbert Spaces
- XYZ-B: Calculating with Qubits
- XYZ-C: Qubits in Quantum Communication Basically, covering II-B and IV-A from your paper.

Paper Structure - My Work

I would split that into individual chapters. Not sure what "My Work" is. I guess thats *your work*. Optimally, I should have alredy figured that one from previous chapters.

Order of Knowledge

In IV-C-2, you write about a "naive intercept-resend eavesdropping attack" but only explain it later. As a reader, having to navigate through the paper instead of being able to read it from top to bottom is irritating.

Comments

I've marked up your paper with a few thoughts - you'll find it attached below. If you can, please open it in Adobe Acrobat. Some other PDF viewers, like Chrome, can mess with the layout and make the comments hard to follow.

Contact

I really hope my feedback was helpful.

If you think I missed the mark somewhere, don't hesitate to let me know.

If you've got any questions, feel free to drop me an email at fl.nolte@tum.de. I'm here to help.

Quantum Key Distribution

Name Surname
B.Sc Department of Computer Science
Chair of IT Security
Munich, Germany
Email: max.musterman@mytum.de

Name of our University is missing + I don't think there is a separate department for B.Sc.
We are part of CIT

***Abstract*—to be written... Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Enim tortor at auctor urna nunc id. Sociis natoque penatibus et magnis. Pretium nibh ipsum consequat nisl vel pretium lectus quam id. Viverra nibh cras pulvinar mattis nunc sed blandit. Turpis egestas pretium aenean pharetra magna. Odio aenean sed adipiscing diam donec adipiscing tristique risus nec. Dictum at tempor commodo ullamcorper a lacus. Congue mauris rhoncus aenean vel elit scelerisque mauris. Adipiscing enim eu turpis egestas. Maecenas accumsan lacus vel facilisis. Enim ut tellus elementum sagittis vitae et. Mauris in aliquam sem fringilla ut morbi tincidunt augue interdum. Facilisi morbi tempus iaculis urna.**

***Index Terms*—some terms here x, y ,z**

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 some main concepts of the quantum mechanics and its theorems and mathematics. The related work section examines existing research and practical implementations in the field of QKD, highlighting notable protocols and advancements. The subsequent section, labeled "My Work," 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 protocol such as the BB84 Protocol. The section continues with an examination of the possible threats presented to this and other QKD protocols, followed with a summary of the present state of QKD, discussing its practical applications and ongoing developments. It further delves into the future prospects of QKD, considering... (TODO). The discussion section critically analyzes the findings presented in the "My Work" section, comparing and contrasting them with existing research and highlighting their significance. Finally, the conclusion section analyzes and presents the role this paper plays in contrast to the overall papers written about this topic, summarizes the key insights from the paper, highlights the importance of QKD in secure communication and possibilities future research to be done.

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. 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 $6.626 \cdot 10^{-34}\text{J} \cdot \text{s}$.

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 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:

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

TODO...

This is an odd title. You already clarified what "your work" is (what the goal of your paper is). As the reader, I'd expect the title to match the section's content.

IV. My Work

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(link) of both basis vectors defined in the *Hilbert Space* simultaneously. For this the Dirac notation (or ket) is used:

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

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

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

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 particle ψ. 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 $|\swarrow\!\nearrow\rangle$ (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:

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

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: $-1 \leq \alpha, \beta \leq 1$ For the rest of the paper let us use $|+\rangle$ and $|-\rangle$ for $|\swarrow\!\nearrow\rangle$ and $|\nwarrow\!\searrow\rangle$ respectively.

1) Generalized scenario of Quantum Communication: Let us analyse how 2 people, Alice and Bob, communicate with each other using light particles. As show in Fig. 1 two polarization filters (the red squares) are used. First the Alice sends photons to Bob, the smallest part 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

I think that what you are trying to describe is that when light passes through a polfilter, the emerging light will be polarized in the direction of the filter

That figure could be much smaller and with transparent/white background

Fig. 1. Polarization of light.

~~the help of~~ quantum mechanics it is possible to send single photons. For example Alice wants to send an up and down 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 vertical or horizontal polarization then the photon's probability of the photon passing through is 100% or 0% respectively. However if he uses a diagonal polarizing filter then the probability is 50% (some general thing about Eve here).

This is quite a jump. We were talking about pol filters (physics) and now protocols (comp sci)? All within one chapter?

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.

- **DV-QKD** - involves the use of discrete quantum states to encode information, which are represented by the polarization or phase 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, such as the amplitude and phase of coherent states or squeezed states.(Link: Advances in quantum crypto) The continuous variables are measured and used to establish a secure key. Compared to the DV-QKD 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 combines a reference signal with an incoming signal to extract information about the amplitude and phase of the signal.) techniques to measure the continuous variables.
- **Distributed Phase** - The main idea of the protocol is to encode and transmit phase information across a quantum and then do phase measurements at the receiver's end to extract the secret key. Depending on the specific design, discrete or continuous variables can be used these protocols.

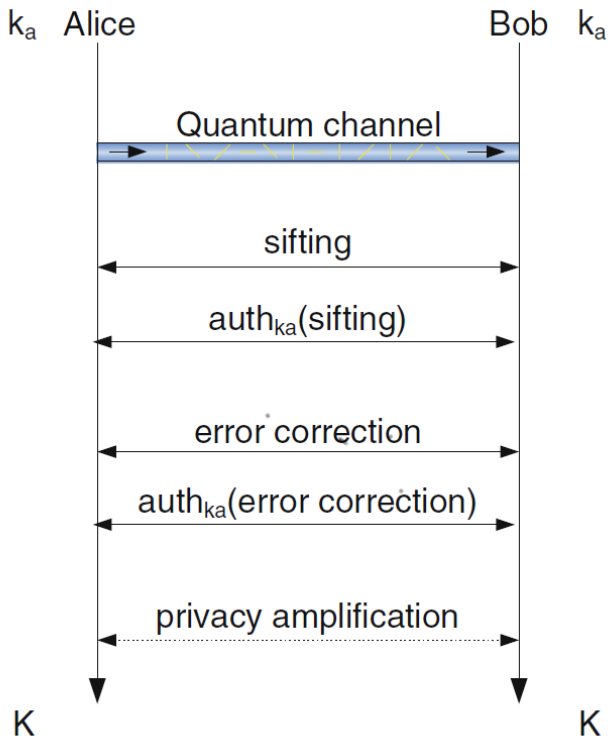

Fig. 2. BB84 protocol

As BB84 being 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, hence ~~why~~ the name. This protocol utilizes the polarization properties of single photons to exchange 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). A~~n~~ simple illustration of the BB84 protocol is shown in Fig 2. k_a is the pre-shared key needed or authentication and K is the final key generated after the BB84 protocol. After the photon exchange comes: sifting (the extraction of the key)~~ref.~~ authentication of the sifting ~~ref~~

Quantum Bit Error Rate (QBER) estimation and correction, authentication of error correction and privacy amplification.

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. The horizontal-vertical base is represented for example by 0 and the diagonal base by 1. 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 ~~first~~ before beginning their communication.

TABLE I
POLARIZATION-ENCODING SCHEME

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

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 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 $n > length(K)$ (Fig 2). Then for every d_i and b_j Alice sends the corresponding photon to the quantum channel. 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*.

2) Threats in the quantum channel: Let us assume that there is an eavesdropper named Eve acting as a MITM (Man In The Middle). Eve uses the naive intercept-resend (reference subsection below) 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. For example Alice sends a $\leftrightarrow$ (bit value 1). Eve guessed the wrong basis and detects a $|-45\rangle$ (bit value 0). Now even though Bob uses the rectilinear polarization basis, the correct one which Alice also used, he detects a $\updownarrow$ (bit value 0). Alter when Alice and Bob check their bases and detect same bases different results a relative significant amount of times then they know they are being eavesdropped. Other reasons for the wrong detection can be optical misalignment, disturbance in the quantum channel or noise in the detectors even though both used the same bases.

3) Sifting and its Authentication: Sifting is the first phase of the public channel. In this public discussion Bob and Alice share 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, 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. 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 in the sifted key. After the comparison a number of error e happens 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 paper (link) it was stated that the value of p_{max} should be 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. 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.(link)
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. (For more information link link link)
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.

For more in-depth information about the different methods of error key reconciliation and their characteristics (link link link)

6) Privacy Amplification: Alice and Bob initially establish a partially correlated key (before QBER, hence why 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 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). Some Überleitung...

D. Threats

Naturally with the development of new cryptographic key distribution methods comes also the possibility of exploiting them by developing new attack strategies. 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 (link) Eve obtains 0.2 bits per bit sent by Alice. But this attack is not yet in its final form.
   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.
   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.
   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.
   Faked-state attack - is an 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.

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?

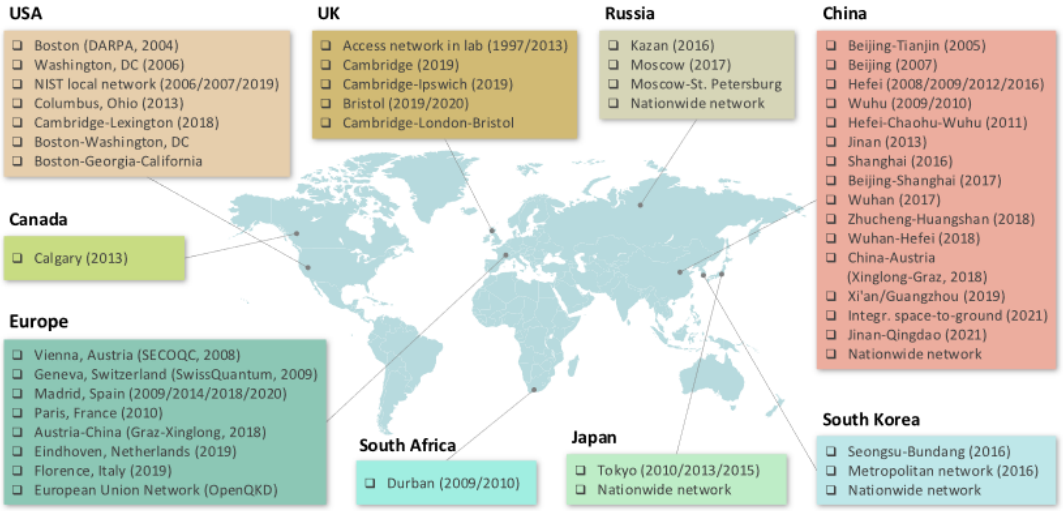

Fig. 3. Overview of the QKD networks and experiments worldwide.

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.

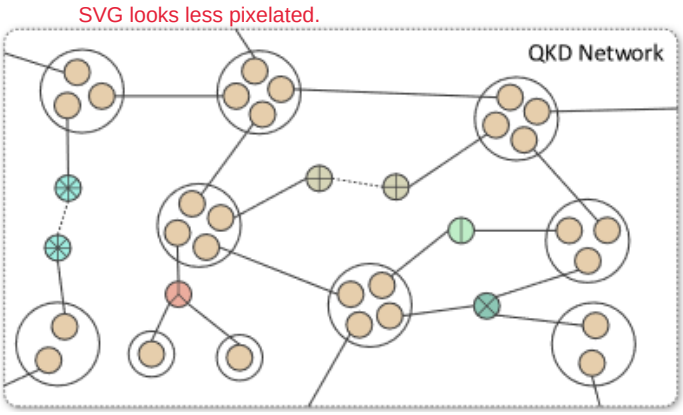

Fig. 4. Abstract illustration of a QKD Network

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 is created through multiple logical point-to-point connections. A abstract illustration of quantum network is represented in Fig. 4, which except the respective nodes has some other component such as: QKD transmitters/receivers, trusted and untrusted relays, quantum repeaters, optical switches and splitters(for more information link). Quantum repeaters, 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. Some of the first and most notable QKD networks pioneering these field of study are: *DARPA network*, *SECOQC network*, *SwissQuantum network*, *Tokyo network*:

1) DARPA Network: The Defense Advanced Research projects Agency (DARPA) started building a QKD network in 2002 which 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.

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 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.

3) SwissQuantum Network: TODO

4) Tokyo Network: TODO

F. Future and Challenges

TODO (1 page)

V. Conclusion

TODO (1 page)

References

[1] TODO not only the marked ones with (link) many more...