

# Quantum Communication Experiments with Entangled Photon Pairs

---

Peranić, Matej

Doctoral thesis / Doktorski rad

2025

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:217:160282>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-03-04**



Repository / Repozitorij:

[Repository of the Faculty of Science - University of Zagreb](#)





University of Zagreb

Faculty of Science  
Department of Physics

Matej Peranić

**Quantum Communication  
Experiments with Entangled Photon  
Pairs**

DOCTORAL THESIS

Zagreb, 2024



University of Zagreb

Faculty of Science  
Department of Physics

Matej Peranić

**Quantum Communication  
Experiments with Entangled Photon  
Pairs**

DOCTORAL THESIS

Supervisors:

dr. sc. Martin Lončarić  
Dr. Siddarth K. Joshi

Zagreb, 2024



Sveučilište u Zagrebu

Prirodoslovno-matematički fakultet  
Fizički odsjek

Matej Peranić

# **Eksperimenti kvantne komunikacije s parovima kvantno prepletenih fotona**

DOKTORSKI RAD

Mentori:

dr. sc. Martin Lončarić  
Dr. Siddarth K. Joshi

Zagreb, 2024.



Mojoj obitelji. To my family.

## About the supervisors

**Martin Lončarić** graduated in solid-state physics at the Faculty of Science of the University of Zagreb, where he received his doctorate in physics, in the field of plasmonics, in 2011. He is employed at the Ruder Bošković Institute as a Research Associate in the Laboratory for Photonics and Quantum Optics, Division of Experimental Physics. His research interests focus on photonics, quantum and nonlinear optics, quantum communication, classical optics and designing optical systems, and photodynamic processes in chemistry, biology and medicine, previously also plasmonics. He has authored 26 scientific articles in CC journals cited over 350 times. He is the co-inventor of four patents related to photodiagnosis and photodynamic therapy.

Selected publications:

- D. Ribezzo et al. “Deploying an Inter-European Quantum Network”. *Advanced Quantum Technology* 2023, 6, 2200061
- S. K. Joshi, D. Aktas, Sören Wengerowsky, M. Lončarić et al. “A trusted-node-free eight-user metropolitan quantum communication network”. *Science Advances* 2020, 6: eaba0959

**Siddarth Koduru Joshi** completed his PhD in the group of Christian Kurtsiefer in CQT, Singapore on loophole-free Bell test experiments (a way to prove the fundamental principles of quantum entanglement). He then joined the group of Rupert Ursin in IQOQI-Vienna for a post-doc, after which he joined the University of Bristol as a Senior Research Associate. After multiple rapid promotions, he started as a Lecturer of Optical Communications in 2021. His scientific research is focused on quantum optics and quantum communication, including small satellites for global scale quantum communication, long-distance fiber optic-based quantum communication for terrestrial links and multiple-user large and complex quantum networks to create the quantum internet. He also works on quantum metrology. Results of his research are published in the most renowned scientific journals like *Nature*, *Science Advances* and *Proceedings of the National Academy of Sciences*.

Selected publications:

- S. K. Joshi et al. “A trusted-node-free eight-user metropolitan quantum communication network”. *Science Advances* 2020, 6: eaba0959
- S. Wengerowsky, S. K. Joshi et al. “An entanglement-based wavelength-multiplexed quantum communication network”. *Nature* 2018, 564, 225–228

## Abstract

The development of quantum physics enabled significant progress in science and technology. For example, in the last decades, the field of quantum communication has matured to a stage where practical implementations outside the laboratory are possible. Quantum communication relies on fundamental physical laws and phenomena, such as the no-cloning theorem, Bell's inequality and quantum entanglement, and involve the use of quantum key distribution (QKD) protocols to generate a secret key for encrypting information. Although QKD protocols offer theoretically absolute security, there are numerous challenges with physical implementations. One such problem is the physical distance limitation between communicating parties due to signal losses. Unlike classical communication, quantum communication does not allow the use of amplifiers to amplify the signal since they would disturb the quantum state. Although quantum repeaters would enable long-distance communication, this technology is still not mature enough for practical implementation. On the other hand, distance limitation can be overcome by using free-space signal transmission. However, this approach requires satellites and increases both the complexity and the cost of implementation. Constructing full-mesh quantum communication networks incorporating many users also poses several challenges, such as the distribution of photons to all users to create a fully connected network or changes in a quantum state through the communication medium (optical fiber or free space). Therefore, a suitable method for compensating changes in a quantum state during transmission through the medium is required. For example, if we use photons and their polarization states for QKD, a polarization compensation method is necessary. On the other hand, it is possible to use some other physical characteristic of the system to connect multiple users, such as the wavelength of photons.

In this work, I present the results of research on a hybrid communication link and on fully connected networks. While demonstrating the approach with wavelength (de-)multiplexing to connect multiple users in a network, I will show that a hybrid link could serve as an interface between local networks in the light-polluted areas on the ground and long-distance links through free space. This presents a milestone in building interconnected networks into a quantum internet. The hybrid link was built with a type-II source of polarization-entangled photon pairs adapted for quantum commu-

nication between a user on the ground and a user in free space. To build quantum networks with four and six users, we used a type-0 source. In addition to the successfully established quantum communication with both sources, we have shown that the source of polarization-entangled photons itself can be used for the polarization compensation process without the need for an additional apparatus including an extra laser. Furthermore, we compared four methods for polarization compensation on quantum networks and realized the first compensation of a quantum state on an active network, proving that communication within the network does not have to stop during the polarization compensation process. The results of experimental research of polarization compensation in full-mesh quantum networks represent the main part of this thesis and are described in a published paper: Peranić, M., Clark, M., Wang, R. et al. A study of polarization compensation for quantum networks. EPJ Quantum Technol. 10, 30 (2023). <https://doi.org/10.1140/epjqt/s40507-023-00187-w>

Keywords: *quantum communication, quantum networks, quantum key distribution, entanglement, polarization compensation*

## Prošireni sažetak

Razvoj kvantne fizike u 20. stoljeću omogućio je značajan napredak znanosti i tehnologije. Primjerice, područje kvantnih komunikacija, koje se oslanja na temeljne fizikalne zakone i pojave kao što su "no-cloning" teorem, Bellove nejednakosti i kvantno sprezanje, doživjelo je realizaciju i izvan okvira znanstvenih laboratorija. Kvantna komunikacija se temelji na protokolima kvantne distribucije ključeva kojima se generiraju tajni ključevi za enkripciju informacija. Iako ti protokoli pružaju matematički apsolutnu sigurnost, prilikom njihove implementacije susrećemo se s nizom problema. Jedan od njih je ograničenje udaljenosti između dva korisnika zbog gubitaka prilikom korištenja optičkih kablova. Također, prisutan je i problem skaliranja komunikacije s dva na veći broj korisnika u kvantnu komunikacijsku mrežu u kojoj su svi korisnici međusobno istovremeno povezani. Za razliku od klasične komunikacije, kod kvantne komunikacije nije moguće upotrebljavati pojačala signala jer bi to podrazumijevalo izvršenje mjerenja čime bi se utjecalo na kvantno stanje fotona. Kako bi se zaobišao problem gubitaka u optičkim vlaknima, signal se može slati kroz slobodan prostor. Iako taj pristup omogućuje komunikaciju na veće udaljenosti, on zahtjeva upotrebu satelita što ga čini tehnološki zahtjevnim i skupim te dolazi do gubitaka prilikom prolaska fotona kroz atmosferu. Prilikom izgradnje kvantnih mreža također nailazimo na nekoliko problematičnih aspekata kao što je potreba za pouzdanim čvorovima (engl. *trusted nodes*) koji su potencijalna sigurnosna opasnost ili primjena aktivnih preusmjeravanja (engl. *active switching*), koja ograničavaju i funkcionalnost i povezivost. Za umrežavanje većeg broja korisnika u kvantnoj komunikaciji može se koristiti neko dodatno svojstvo, primjerice, valna duljina fotona. Bez obzira na broj korisnika te koji medij koristili za transmisiju, moramo osigurati da "signal" (kvantno stanje) nepromijenjen stigne od izvora (pošiljatelja) do primatelja. Stoga, ukoliko se za generiranje sigurnosnog ključa koriste fotoni i njihova stanja polarizacije, potrebna je prikladna metoda kompenzacije promjena stanja polarizacije tijekom fizičke transmisije kroz medij, bilo to optičko vlakno ili zrak.

U ovom radu predstavljam rezultate istraživanja na hibridnom komunikacijskom linku te na potpuno povezanim kvantnim mrežama. Hibridni link predstavlja sponu između jednog korisnika na zemlji te drugog u zraku, tj. između lokalnih mreža na zemlji i dugih linkova kroz slobodni prostor. Time čine neizostavnu poveznicu

prilikom umrežavanja kvantnih mreža u kvantni internet. Hibridni link je realiziran s izvorom polarizacijski spregnutih fotona tipa II prilagođenim za kvantnu komunikaciju između korisnika na zemlji i u zraku. S druge strane, za realizaciju kvantnih komunikacijskih mreža s četiri i šest korisnika povezanih optičkim vlaknima korišten je izvor tipa 0 širokog spektra. Osim izvora parova spregnutih fotona, u sklopu ovog rada sagrađeni su i korisnički moduli koji omogućuju potpuno pasivnu analizu polarizacije dolaznih fotona. Karakterizacija izvora tipa II polarizacijski spregnutih fotona na valnoj duljini od 810 nm pokazala je efikasnost (engl. *heralding efficiency*) od  $(24.7 \pm 0.3)\%$  te prosječnu vidljivost (engl. *entanglement visibility*) iznad 99%. Za uspostavu kvantne komunikacije između jednog korisnika na zemlji i drugog u zraku, iskoristili smo optičko vlakno kakvo se uobičajeno koristi u klasičnoj komunikaciji te dodatno vlakno za filtriranje prostornih modova viših redova prema korisniku "na zemlji", dok smo signal prema drugom korisniku slali kroz slobodan prostor (zrak). Oba korisnika su koristila izrađene module za analizu polarizacije prilagođene za valnu duljinu od 810 nm. Prije uspostave komunikacije, primijenili smo dvije metode kompenzacije polarizacije - prvu koristeći dodatnu valnu pločicu unutar samog izvora te drugu upotrebom polarizatora ispred vlakana za prikupljanje fotona. Kako bismo potvrdili uspješno uspostavljenu vezu, mjerili smo parametar pogreške, tzv. QBER (engl. *quantum bit error rate*) koji uključuje doprinos od nesavršenih detektora, izvora i ostalih hardverskih nesavršenosti, ali i eventualni doprinos koji nastaje zbog pokušaja prisluškivanja komunikacije. S obzirom na to da se različiti doprinosi ne mogu razlikovati, sve ih pripisujemo potencijalnom prisluškivaču. Iznos QBER parametra ispod 11% osigurava sigurnu kvantnu komunikacijsku vezu. Pomoću navedenih metoda kompenzacije polarizacije izmjereni QBER iznosio je  $(6.6 \pm 0.1\%)$  i  $(5.4 \pm 0.2\%)$ . Time smo dokazali da se predložene metode kompenzacije polarizacije mogu uspješno primijeniti pri uspostavi kvantne komunikacije. Za razliku od uobičajenih metoda koje koriste dodatni laser s prethodno pripremljenim stanjem polarizacije, ovim smo rezultatom dokazali da se i sam izvor parova spregnutih fotona može koristiti u procesu kompenzacije, bez potrebe za dodatnim laserom. Dok smo izvor tipa II koristili za povezivanje dvaju korisnika, izvor tipa 0 omogućuje konstrukciju kvantne mreže sa većim brojem korisnika u kojoj su svi međusobno povezani (engl. *full-mesh network*) distribuiranjem parova spregnutih fotona valnih duljina simetričnih oko centralne valne duljine. Sagrađili smo mrežu

sa šest korisnika od kojih su svi korisnici od izvora udaljeni 1.6 km, osim jednog korisnika koji je bio udaljen 5.6 km. Gubitci u optičkim vlaknima na navedenim linkovima iznosili su od 8.1 dB do 15.1 dB za najudaljenijeg korisnika. Mjerenje tajnog ključa tijekom vremena dužeg od 6 dana pokazalo je stabilnost mreže i robusnost na prekide rada mreže koji su bili nužni zbog hlađenja supravodljivih detektora te prekida koji se dogodio uslijed nepredviđenog nestanka struje. Testirali smo i dvije konfiguracije mreže u kojima su određeni korisnici povezani samo u određenom razdoblju tijekom kojeg akumuliraju tajni ključ. Rezultati pokazuju da djelomično povezane konfiguracije generiraju manju količinu ključa od potpuno povezane mreže koristeći izvor s efikasnošću iznad 10%, dok je za izvore sa niskom efikasnošću situacija obrnuta. Usporedili smo četiri metode kompenzacije polarizacije na primjeru mreže s četiri korisnika. Pokazali smo da je moguće provoditi kompenzaciju polarizacije upotrebom samog izvora parova spregnutih fotona, bez potrebe za prekidanjem rada mreže i bez korištenja dodatnog lasera. Ovaj rezultat je značajan jer pokazuje da se metoda u kojoj se prati iznos QBER-a može provoditi na aktivnoj mreži, bez zaustavljanja zbog procesa kompenzacije polarizacije, što je prva takva realizacija u svijetu. Također, u usporedbi s klasičnom metodom čija provedba u prosjeku traje 14 minuta za jedan link, ova metoda traje znatno kraće, samo 2 minute u prosjeku, što može znatno skratiti vrijeme kompenzacije kod mreža s velikim brojem korisnika. Također je važno napomenuti da je, unatoč bržoj provedbi, sigurnost mreže usporediva sa sigurnošću nakon provedbe kompenzacije klasičnom metodom. Dodatni iskorak bi se mogao postići kombinacijom motoriziranih kontrolera polarizacije s nekom od bržih metoda. Rezultati istraživanja metoda kompenzacije polarizacije na kvantnoj mreži predstavljaju glavni samostalni doprinos ovom radu te su objavljeni u radu: Peranić, M., Clark, M., Wang, R. et al. A study of polarization compensation for quantum networks. EPJ Quantum Technol. 10, 30 (2023). <https://doi.org/10.1140/epjqt/s40507-023-00187-w>

Ključne riječi: *kvantna komunikacija, kvantne mreže, kvantna distribucija ključeva, kompenzacija polarizacije*

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Historical overview of the development of communication . . . . .	1
1.2	Quantum physics in the service of communication security . . . . .	2
<b>2</b>	<b>Theoretical background</b>	<b>4</b>
2.1	Qubit . . . . .	4
2.2	Photons and polarization encoding . . . . .	5
2.3	Nonlinear optics . . . . .	7
2.3.1	Spontaneous parametric down-conversion . . . . .	8
2.3.2	Quasi-phase matching . . . . .	11
2.3.3	Second harmonic generation . . . . .	13
2.4	Quantum entanglement . . . . .	14
2.5	Sources of entangled photons . . . . .	17
2.6	Quantum key distribution . . . . .	18
2.6.1	BB84 protocol . . . . .	21
2.6.2	E91 protocol . . . . .	22
2.6.3	BBM92 protocol . . . . .	23
2.6.4	Multiple-user QKD . . . . .	24
<b>3</b>	<b>Experimental setup</b>	<b>27</b>
3.1	Sources of entangled photons . . . . .	27
3.1.1	Source of polarization-entangled photons of type 0 . . . . .	27
3.1.2	Source of polarization-entangled photons of type II . . . . .	30
3.2	Detectors . . . . .	34
3.2.1	Single-photon avalanche diodes (SPAD) . . . . .	34
3.2.2	Drawbacks - dark counts and afterpulsing . . . . .	35
3.2.3	Superconducting nanowire single-photon detector (SNSPD) . . . . .	36
3.3	Time synchronization . . . . .	39
<b>4</b>	<b>Experiments on hybrid communication link</b>	<b>42</b>
4.1	Characterization of type-II source . . . . .	42
4.2	Polarization compensation schemes . . . . .	45



<b>5</b>	<b>Experiments on full-mesh quantum networks</b>	<b>51</b>
5.1	Realization of a 6-user quantum network . . . . .	51
5.2	Long term monitoring secret key rate . . . . .	53
5.3	Full mesh vs. partial mesh . . . . .	54
5.4	Effect of additional channels . . . . .	55
5.5	Polarization compensation schemes for quantum networks . . . . .	56
5.5.1	Canonical method . . . . .	57
5.5.2	Minimization of QBER . . . . .	62
5.5.3	Advantages and drawbacks of polarization compensation methods . . . . .	63
<b>6</b>	<b>Conclusions and outlook</b>	<b>66</b>
<b>7</b>	<b>Bibliography</b>	<b>68</b>
<b>8</b>	<b>Appendix</b>	<b>79</b>
8.1	Quantization of electromagnetic field . . . . .	79
8.2	No-cloning theorem . . . . .	82
8.3	Teleportation . . . . .	83
8.4	Entanglement swapping . . . . .	84
8.5	Alignment of user modules for polarization analysis . . . . .	85
8.6	A flowchart of the algorithm for motorized polarization controllers . .	88
8.7	Distribution of channels in a six-user quantum network . . . . .	89
<b>9</b>	<b>Curriculum vitae</b>	<b>90</b>
<b>10</b>	<b>List of publications</b>	<b>91</b>
10.1	Conference papers . . . . .	91

# 1 Introduction

## 1.1 Historical overview of the development of communication

Communication has always been an integral part of human nature. Ever since prehistoric times, we have been using elements from our natural surroundings as communication tools, whether it was chalk for cave drawings or birds as carriers of messages. Today, we are doing the same thing – we are using nature and its laws to improve communication, making it faster and more secure. In the 19th century, the first telegraph signal was transmitted, soon followed by the deployment of submarine coaxial cables on the bottom of the Strait of Dover. The next important milestone was the invention of the “wireless telegraph” by Guglielmo Marconi. This radio device modified sounds or signals into radio waves, which then traveled through the air, and vice versa. In the first half of the 20th century, major advancements in communication security were accomplished, mainly due to the efforts of cryptographers in the World War I and II. With the development of satellites, we have satisfied all requirements to connect the whole world, even before the World Wide Web (WWW). The invention of optical fibers allowed for the deployment of the first transatlantic fiber-optic cable (Fig. 1) with repeaters every 40 km. One of the main advantages of fiber-optic cables is that they allow about 10 times shorter time delay in communication compared to geostationary satellites.

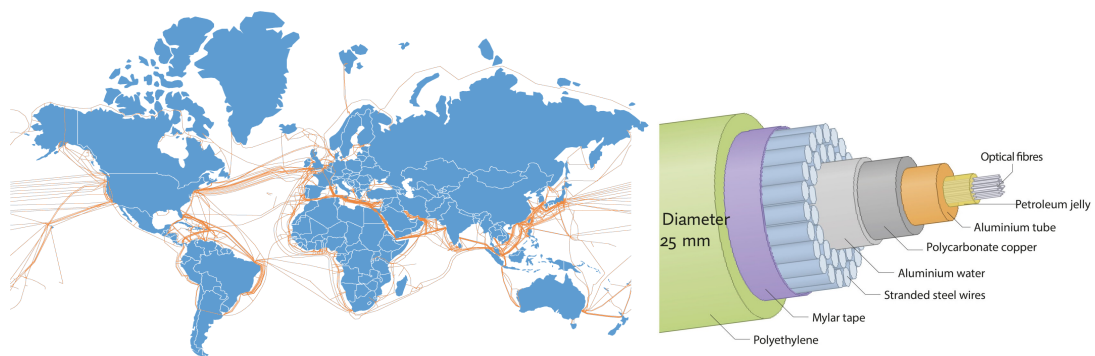


Figure 1. Left: The world’s network of fiber-optic submarine cables, Right: A cross section of a submarine communications cable, based on a patent image (1981)

More recently, new technologies like blockchain have gained a lot of attention. Instead of storing information (for example, about money transactions) in one place, a blockchain replicates that information across the network. The blocks in which transactions are stored are publicly available and accessible to anyone, making the data easily verifiable and providing anonymity. However, none of these classical communication technologies are secure from eavesdropping. The security of widely-used asymmetrical (or public-key) cryptosystems relies on mathematical problems that are “hard” for a computer to solve. This means that the time required to perform a task grows exponentially with the number of bits in the input. On the other hand, an eavesdropper can intercept communication by redirecting a copy of a signal using a beamsplitter on a fiber or by tapping the fiber. This way, communication is not interrupted, and an eavesdropper remains undetected. With enough computational power/time or by using a quantum computer, an eavesdropper can break the encryption and get the secret key.

## ***1.2 Quantum physics in the service of communication security***

Cryptography is the study of techniques for secure communication. In general, the cryptographic process involves converting ordinary information called plain-text into an unintelligible form called ciphertext through encryption. The encoded message is then sent, and the process is reversed through decryption. There are two main categories of cryptosystems: asymmetric (public-key) and symmetric (secret-key). Symmetric ciphers use a single key (random and secret sequence of symbols) for both encryption and decryption. The only provably secure cryptosystem known today is the one-time pad, which belongs to this category. Although perfectly secure, a one-time pad is not considered practical as it requires that the sender and receiver possess a common secret key. Moreover, the key must be at least as long as the message itself and can only be used once. Public-key cryptosystems rely on mathematical objects called one-way functions. With one-way functions it is easy to compute the function  $f(x)$  given the variable  $x$ , but difficult to reverse the calculation and deduce  $x$  from  $f(x)$ . A well-known example of a one-way function is factorization of large integers. However, it has not yet been possible to prove whether factoring is “difficult” or not. In addition, in 1994, Peter Shor discovered a polynomial algorithm (Shor’s algo-

rithm) that allows fast factorization of integers with a quantum computer [1], which presents a threat to security based on public-key cryptosystems. However, quantum physics could also provide a solution for unconditionally secure communication.

During the 19th and 20th centuries, new discoveries in physics led to the emergence of new opportunities. We could say that, even though quite unexpectedly, by publishing their famous EPR paper [2] in 1935, Einstein, Podolsky and Rosen started the development of a new field – quantum cryptography. They argued that the description of physical reality provided by quantum mechanics was incomplete and instead proposed the theory of hidden variables, which would consist of quantum theory extended with some yet unknown variables. Thirty years later, Bell derived inequalities for a correlation function that are necessarily satisfied by any local realist theories, but that can be violated by quantum mechanics [3]. If we assume that the same quantum channel is used to test Bell’s inequality and measure the correlation between observables used for generating a secret key for encryption and decryption, we can connect it with the communication process. For error-free channels, a maximal violation of Bell’s inequality is achievable, whereas if there is some perturbation (due to either an imperfect channel or an eavesdropper), quantum correlation is reduced. Clauser and Freedman experimentally confirmed the violation of Bell’s inequality in 1972, for which a Nobel prize was awarded in 2022 [4]. These results form the basis for security analysis of quantum key distribution (QKD) protocols that rely purely on the laws of quantum physics. The first QKD protocol was developed by Bennet and Brassard in 1984 and is known as BB84 [5]. It can be realized with single photons where the sender (usually called Alice) prepares a quantum state and sends it to the receiver (usually called Bob). In the ideal case (without losses, disturbances leading to changes in quantum state, or an eavesdropper), Bob measures this state and extracts the secret key. Protocols of this type are known as “prepare-and-measure” protocols. On the other hand, in 1991 Ekert proposed a QKD protocol that uses entangled states (E91 protocol). In this case, one photon from an entangled photon pair is sent to Alice and the other one to Bob. Any attempt of an eavesdropper (Eve) would destroy correlations between entangled photons and Eve would be detected. Therefore, QKD offers unconditional and mathematically perfect security that no amount of analysis can break. Details about QKD protocols can be found in Chapter 2.6.

## 2 Theoretical background

### 2.1 Qubit

In classical communication and information theory, we use a bit as a unit of information, represented as either 0 or 1 in the binary number system. On the other hand, quantum computing and communication use a quantum bit, or a qubit, which is the quantum version of the classical bit. It is physically realized with a two-state quantum-mechanical system. In addition to existing in states  $|0\rangle$  and  $|1\rangle$  states (written in a Dirac notation), a qubit can also exist in a superposition of both states simultaneously. This property plays an important role in quantum computing because qubits can hold an exponential number of states, i.e.  $N$  qubits are comparable to  $2^N$  bits. This means that computations can be performed faster. A single qubit can be described as a linear combination of two orthonormal basis states that span the two-dimensional linear vector space, also known as the Hilbert space:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.1)$$

where  $\alpha$  and  $\beta$  are complex probability amplitudes. In quantum mechanics, probability amplitudes are directly related to probabilities with which outcomes of measurements occur. The probability of outcome  $|0\rangle$  with value "0" is  $|\alpha|^2$  and the probability of outcome  $|1\rangle$  with value "1" is  $|\beta|^2$ , where  $|\alpha|^2 + |\beta|^2 = 1$  needs to be fulfilled. Now, the equation 2.1 can be re-written as:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \quad (2.2)$$

With equation 2.2. we can visualize quantum states of a qubit with a sphere of a radius 1, also known as a Bloch sphere (Fig. 2). Pure qubit states are represented by points on the surface of the sphere, while mixed states are represented by points inside of the Bloch sphere. For the physical realization of a qubit, we can use any two-level physical system. In this work, we will focus on the photons and their polarization states.

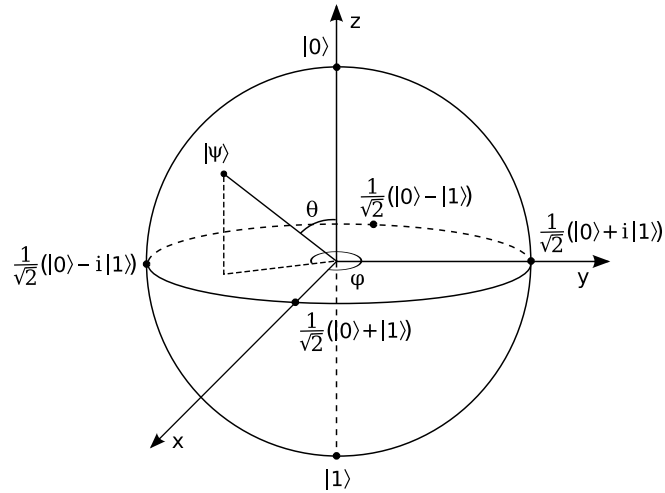


Figure 2. Bloch sphere

## 2.2 Photons and polarization encoding

A photon is an elementary particle that serves as an elementary excitation (a quantum) of an electromagnetic field. The experiments on the black-body radiation and the photoelectric effect by Planck [6, 7], Einstein [8], Compton [9] and others in the early 20th century led to the adoption of the name "photon" after it was proposed by Lewis in 1926 [10]. These experiments motivated the development of a quantum theory and the quantization of the electromagnetic field (Appendix A) which was performed for the first time in 1927 by Dirac [11]. Photons are the natural choice for quantum-communication applications since they are easy to produce, they interact weakly with their environment, they can be transmitted through an already existing classical communication infrastructure and they are detected with single photon detectors. Besides quantum cryptography, single photons are also used for a wide range of applications, including quantum computing [12], generation of truly random numbers [13, 14], remote sensing [15] or spectroscopy [16].

In quantum cryptography, to generate the secret key between two parties that want to communicate securely, we must use some degree of freedom of the photon like polarization, momentum, energy, etc. We differentiate two possibilities - discrete and continuous variables. The most preferable degree of freedom among discrete variables is polarization since it can be easily manipulated and controlled with linear optical elements (Fig. 3). The logical 0 and 1 can be represented by horizontal and vertical polarization. The diagonal and antidiagonal polarization and the left

and right circular polarization correspond to the remaining bases  $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$  and  $\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ . The time of the arrival can also be used as a physical realization of a qubit. Photons are sent through an interferometer with a short and a long arm. This creates a superposition between two different time-bins. One of the continuous variable possibilities is to use phase encoding where 0 and 1 are represented by the relative phase difference between arms of an interferometer. However, path differences cannot change and the coherence length of photons cannot be shorter than the path mismatch.

In addition to linear optical experimental components that are used to control the path (mirrors), beam radius (lenses) or polarization (waveplates), non-linear optical processes play an important role in quantum communication.

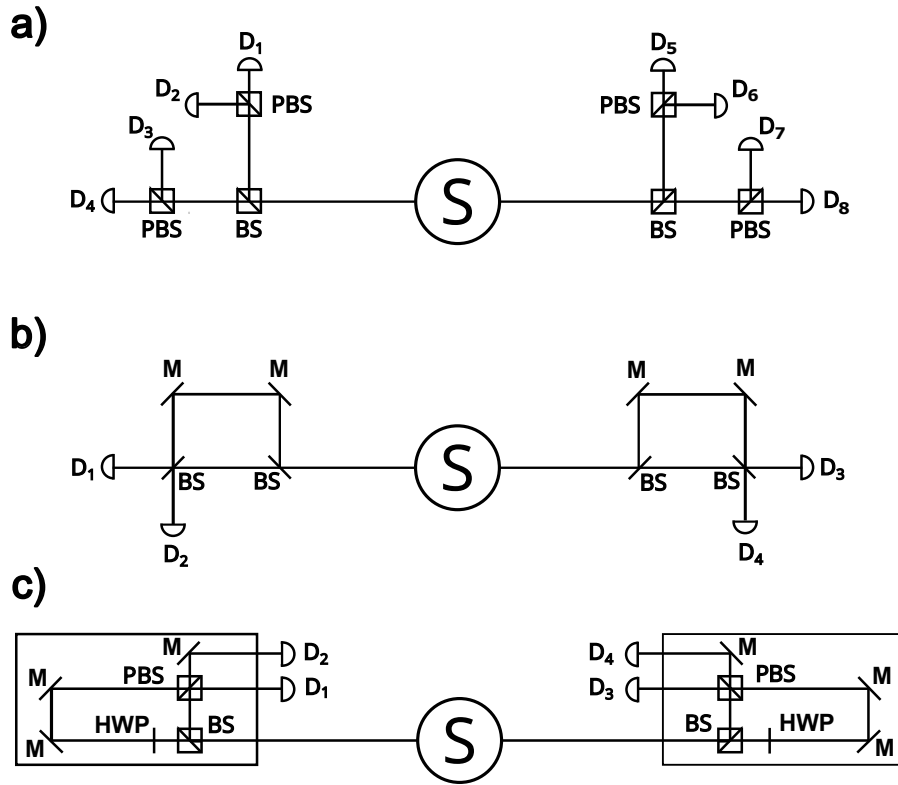


Figure 3. a) Sketch of a traditional experimental setup for polarization analysis requiring four detectors per user, b) Sketch of an experimental setup using time-bin entanglement, c) Sketch of an experimental setup for polarization analysis used in this work requiring only two detectors per user. The source of polarization entangled photons is denoted with "S", beam splitter with "BS", polarization beam splitter with "PBS", half-wave plate with "HWP" and mirror with "M". The outputs of user modules are connected to single photon detectors denoted with "D".

### 2.3 Nonlinear optics

From classical electromagnetism, it is well known that when an external electric field is applied to a dielectric material, it causes the displacement of the bound charges. For a volume element  $\Delta V$  which carries a dipole element  $\Delta \mathbf{p}$  we define the polarization density  $\mathbf{P}$  as:

$$\mathbf{P} = \frac{\Delta \mathbf{p}}{\Delta V} \quad (2.3)$$

The material in which the polarization density  $\mathbf{P}$  responds non-linearly to the electric field  $\mathbf{E}$  is called non-linear medium. The dielectric polarization  $\mathbf{P}$  of a media with non-linear susceptibility  $\chi$ , subject to an electric field  $\mathbf{E}$ , can be written as an expansion in powers of the applied field:

$$\mathbf{P} = \epsilon_0(\chi^{(1)}\mathbf{E} + \chi^{(2)}\mathbf{E}^2 + \chi^{(3)}\mathbf{E}^3 + \dots) \quad (2.4)$$

where  $\epsilon_0$  is vacuum permittivity and  $\chi^{(k)}$  is the  $k^{th}$  order susceptibility tensor of rank  $k+1$ .

The first term describes the linear optical effects such as reflection and absorption and is always present. For strong electric fields (values of atomic electric fields, typically  $10^8$  V/m) we can neglect terms higher than the second one and write  $\mathbf{P}_i^{(2)}$  in the explicit form:

$$\mathbf{P}_i^{(2)} = \epsilon_0 \sum_{j,k=1}^3 \chi_{ijk}^{(2)} \mathbf{E}_j \mathbf{E}_k \quad (2.5)$$

Furthermore, we can re-write the previous equation in the so-called Voigt notation, which is useful for comparing different types of non-linear processes:

$$\begin{pmatrix} P_1^{(2)} \\ P_2^{(2)} \\ P_3^{(2)} \end{pmatrix} = \epsilon_0 \begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \end{pmatrix} \begin{pmatrix} E_1^{(2)} \\ E_2^{(2)} \\ E_3^{(2)} \\ 2E_2E_3 \\ 2E_1E_3 \\ 2E_1E_2 \end{pmatrix} \quad (2.6)$$



A second-order nonlinearity is only present in the media that do not show inversion symmetry, usually crystals. For most non-linear media,  $\chi^{(2)}$  is only significant for one particular optical process. Even when it is significant for multiple processes, achieving conservation of momentum simultaneously is more difficult, but it can have useful applications such as the generation of a third-harmonic without the need for a high third-order nonlinearity. Some of the non-linear processes are:

- Second-harmonic generation (SHG)
- Third-harmonic generation (THG)
- Sum-frequency generation (SFG)
- Difference-frequency generation (DFG)
- Optical parametric oscillation (OPO)
- Spontaneous parametric down-conversion (SPDC)

In this work, I will focus on the process of the spontaneous parametric down-conversion that is used for the creation of entangled photon pairs and on a second-harmonic generation that is used in the process of source alignment.

### **2.3.1 Spontaneous parametric down-conversion**

Spontaneous parametric down-conversion (SPDC) is an optical process that occurs in non-linear crystals. This represents the specific case of a three-wave mixing process where the two lower energy fields are initially vacuum modes. In the SPDC process, one photon of higher energy (pump photon) converts into a pair of photons (signal photon and idler photon) of lower energy, in accordance with the law of conservation of energy and the law of conservation of momentum (Fig 4.).

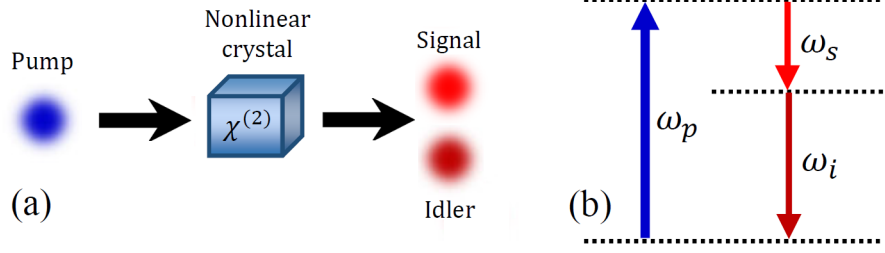


Figure 4. (a) Generation of photon pairs in the SPDC process. A pump photon of frequency  $\omega_p$  decays to two photons of frequencies  $\omega_s$  and  $\omega_i$ , known as the signal and idler photon, respectively. (b) Illustration of energy conservation in the SPDC process. Taken from [17]

Momentum conservation is related to phase matching and can be achieved despite chromatic dispersion (changes in index of refraction with polarization) by using birefringent nonlinear materials. The choice of the crystal and its periodic poling allows us to choose the wavelength of the down-converted photons as well as their bandwidth, which can vary from a few nanometers up to a few tens of nanometers. The process can be described as follows:

We can write the initial state as  $|\phi_0\rangle = |\alpha\rangle_p |0\rangle_s |0\rangle_i$ , where  $p$ ,  $s$  and  $i$  represent the pump, signal and idler photon, respectively. In the interaction picture, total Hamiltonian can be written as:

$$\hat{H} = \hat{H}_0 + \hat{H}' \quad (2.7)$$

where  $\hat{H}_0 = \sum_k \hbar\omega_k (\hat{a}_k^\dagger \hat{a}_k + 1/2)$ . Since  $\hat{H}_0$  is of a first-order in the creation and annihilation operators, it cannot be responsible for the creation of photon pairs. Therefore, we can focus on a nonlinear Hamiltonian:

$$\hat{H}' = -\epsilon_0/3 \int d^3r \chi^{(2)} \hat{E}_s^{(-)} \hat{E}_i^{(-)} \hat{E}_p^{(+)} \quad (2.8)$$

The nonlinear Hamiltonian is actually a sum over eight distinct terms whose various combinations correspond to different nonlinear processes. Only processes that conserve energy contribute significantly to the probability amplitude of down-conversion.

The second-order non-linearity required for parametric down conversion occurs in different inorganic crystals, such as KDP (potassium dihydrogen phosphate,  $\text{KH}_2\text{PO}_4$ ), BBO (beta-barium borate,  $\beta\text{-BaB}_2\text{O}_4$ ), LN (lithium niobate,  $\text{LiNbO}_3$ ) or KTP (potassium titanyl phosphate,  $\text{KTiOPO}_4$ ). Different materials have different strengths of  $\chi^{(2)}$  non-linearity and are suitable for use in different ranges of wavelengths, depending on the phase-matching conditions. Table 1. shows characteristic data for certain crystals that are used in nonlinear processes.

Table 1. Examples of crystals used in the SPDC process with their characteristics.

Potassium titanyl phosphate (KTP) was used in the type-II source and lithium niobate (LN) was used in the type-0 source (in bold) [18].

Crystal	Chemical formula	Transparency range [nm]	Spectral range of phase matching [nm]	Damage threshold [ $\text{GW}/\text{cm}^2$ ]
<b>KTP - potassium titanyl phosphate</b>	<b><math>\text{KTiOPO}_4</math></b>	<b>350-4500</b>	<b>800-2500</b>	<b>1.0</b>
<b>LN - lithium niobate</b>	<b><math>\text{LiNbO}_3</math></b>	<b>350-5200</b>	<b>1300-1600</b>	<b>4.0</b>
ADP - ammonium dihydrogen phosphate	$\text{NH}_4\text{H}_2\text{PO}_4$	220-2000	500-1100	0.5
KDP - potassium dihydrogen phosphate	$\text{K}_2\text{H}_2\text{PO}_4$	200-2500	517-1500	8.4
BBO - beta-barium borate	$\beta\text{-BaB}_2\text{O}_4$	197-3500	410-1500	9.9

The poor efficiency of the SPDC process can be calculated from the single-mode pair generation rate  $R$  for type-II degenerate SPDC where the created signal and idler photons have mutually orthogonal linear polarization:

$$R = \frac{1}{\pi \epsilon_0 c^2} \frac{n_{g1} n_{g2}}{n_1^2 n_2^2 n_p} \frac{(d_{eff})^2 \omega_p^2}{\Delta n_g} \left| \frac{\sigma_p^2}{\sigma_1^2 + 2\sigma_p^2} \right|^2 \frac{P}{\sigma_p^2} L_z \quad (2.9)$$

where  $n_{g1}$  ( $n_{g2}$ ) is the group index at the signal (idler) frequency,  $\omega_p$  is the frequency of a monochromatic pump beam,  $\Delta n_g$  is the group index mismatch for the signal and idler photons at their central frequencies,  $d_{eff} = \chi_{eff}^{(2)}/2$  is the more common convention for effective nonlinear susceptibility and  $P$  is power (mean intensity of the beam times its effective area). The generation rate, for typical values, gives about  $10^6$  pairs per second for a pump power of 1 mW. In other words, in a time window of 1 ns, the probability of finding a second pair after having already detected one is about 0.1%. A more detailed discussion about generation rates can be found in the Introduction to absolute brightness and SPDC tutorial [19].

### 2.3.2 Quasi-phase matching

The phase-matching condition is a relation among the wavevectors of the interacting waves in the nonlinear process. It determines the spatial and spectral distribution of the down-converted photons. This means that if signal and idler photons generated in different regions of the nonlinear crystal interfere constructively along the propagation direction, we will have an efficient SPDC process. Depending on the polarization of the generated photons, the phase-matching and the corresponding crystals can be classified into different types: a type 0 (where mutually parallel linear polarization of the signal and idler photons are parallel with the linear polarization of the pump beam, type I (where the signal and idler photons have mutually parallel polarization perpendicular to the linear polarization of the pump beam), and type II (where the signal and idler photons have mutually orthogonal linear polarization) (Table 2). Equation 2.14 in the next sub-chapter shows that the state depends on the  $\text{sinc}(x)$  function. For the coherence length  $L_c = 2\pi/\Delta k$ , destructive interference occurs. On the other hand, with the careful manipulation of the sign of the crystal nonlinearity, it is possible to achieve high intensity of created photons through so-called quasi-phase matching.

Table 2. Effective non-linearity coefficients for all polarisation configurations and three kinds of periodically poled crystals. The crystals in bold are used in this work.

Taken from [20]

SPDC Type		Effective non-linear coefficient $d_{eff}$ [pmV <sup>-1</sup> ]		
		<b>ppKTP</b>	<b>ppLN</b>	ppLT
0	$o \rightarrow o + o$	0	$d^{22} \sim 1.5$	$d^{22} \sim 0.9$
	$e \rightarrow e + e$	$d^{33} \sim 9.4$	<b><math>d^{33} \sim 14.5</math></b>	$d^{33} \sim 7.6$
I	$o \rightarrow e + e$	0	0	0
	$e \rightarrow o + o$	$d^{24} \sim 2.4$	$d^{31} \sim 2.8$	$d^{31} \sim 0.3$
II	$o \rightarrow o + e$	<b><math>d^{32} \sim 2.4</math></b>	$d^{31} \sim 2.8$	$d^{31} \sim 0.3$
	$e \rightarrow o + e$	0	0	0

The most common technique for achieving quasi-phase matching is periodic poling. With the periodic poling, domains with alternate orientations of nonlinearity occur. It is usually achieved by applying large electric fields with an alternating sign to the crystal during the crystal growth phase. The created domains in the crystal are regularly spaced, with periods in a multiple of the desired wavelength of operation. As a result of periodic poling, we can use longer crystals, which enables greater interaction length and results in a higher number of created photons for a given pump power. Also, crystals can be produced in a way that the emission of the signal and idler is colinear with the pump beam in contrast to the emission into two intersecting cones. Although the ideal poling period would result in  $\Delta k = 0$ , achieving shorter poling periods is more challenging. Furthermore,  $\Delta k$  is a function of the frequency and the refractive index, which is a function of the frequency and the temperature which makes it difficult to produce short poling periods. On the other hand, phase mismatch  $\Delta k$  can be used to calculate the intensity distribution of the output beam generated in the nonlinear process (Fig. 5, b).

For collinear propagation of the signal and idler photons in the source of polarization-entangled photons of type-II we use KTP that has three nonzero second-order tensor coefficients  $d_{ijk}$  (Subchapter 2.3) [21], allowing for type-0, type-I, and type-II quasi-phase-matched SPDC. Furthermore, it is a great choice due to its large nonlinearity, high transparency for pump wavelengths of around 405 nm, and its low susceptibility to photo-refractive damage.

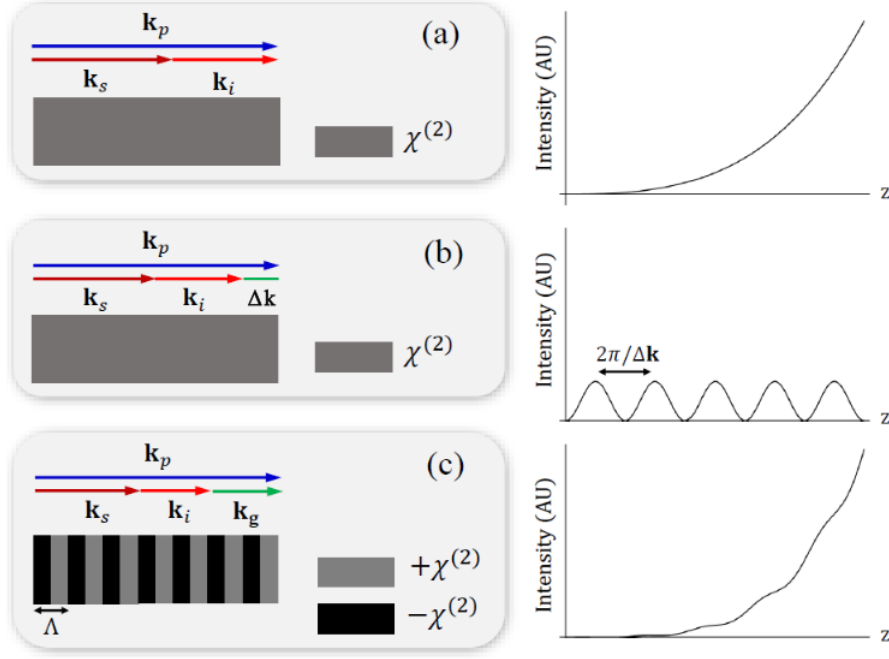


Figure 5. Comparison of ideal phase matching (a), non-phase matching (b) and quasi-phase matching (c). Adapted from [17]

### 2.3.3 Second harmonic generation

Second harmonic generation (or frequency doubling, SHG) is a nonlinear process in which a pump wave generates another wave with twice the energy (equivalently, twice the frequency and half the wavelength) in the nonlinear medium. In most cases, due to phase matching conditions, a second harmonic wave is generated in the form of a beam propagating in the same or a similar direction as a pump beam, together with the residual pump beam. In terms of this work, SHG can be useful in the process of alignment of the entangled photon source (Subchapter 3.1.1). To use it for both SHG and SPDC, the crystal needs to be specially manufactured. Some crystals that can be used for SHG conversion are BiBO ( $\text{BiB}_3\text{O}_6$ ), BBO ( $\beta\text{-BaB}_2\text{O}_4$ ), or periodically-poled crystals, like PPLN (lithium niobate).

## 2.4 Quantum entanglement

The evolution of a quantum state created in the SPDC process can be written as

$$|\phi\rangle = e^{\frac{-i\hat{H}'t}{\hbar}} |\phi_0\rangle = |\phi_0\rangle + \frac{i\epsilon_0}{\hbar} \int_0^t dt' \int d^3r \chi^{(2)} \hat{E}_s^{(-)} \hat{E}_i^{(-)} \hat{E}_p^{(+)} |\phi_0\rangle + O(2) \quad (2.10)$$

The probability of a single pair emission is obtained by assuming the weak-pump regime which allows us to keep only the first-order of the series expansion:

$$|\phi\rangle \propto \int_0^t dt' \sum_{k_p k_s k_i} \int d^3r \chi^{(2)}(\mathbf{r}) \hat{a}_{k_s}^\dagger \hat{a}_{k_i}^\dagger \hat{a}_{k_p} e^{i(\mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i) \cdot \mathbf{r}} e^{-i(\omega_p - \omega_s - \omega_i)t'} |\phi_0\rangle \quad (2.11)$$

For high pump intensities neglected higher-order terms correspond to the multi-pair emissions and must be considered. For the rectangular shaped crystal with dimensions  $L_x, L_y, L_z$ , we get:

$$|\phi\rangle \propto \frac{t\chi^{(2)}L_xL_yL_z}{16} \sum_{k_p k_s k_i} \text{sinc}[\Delta\omega t/2] \text{sinc}[\Delta k_x L_x/2] \text{sinc}[\Delta k_z L_z/2] \hat{a}_{k_s}^\dagger \hat{a}_{k_i}^\dagger \hat{a}_{k_p} \quad (2.12)$$

where  $\Delta\omega = (\omega_p - \omega_i - \omega_s)$ ,  $\Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i$  and  $\text{sinc}(x) = \sin(x)/x$ . Function  $\text{sinc}(x)$  includes wavevectors of pump, signal and idler photons inside of the crystal and determines the condition for phase matching inside of the crystal:

$$\frac{n_p(\omega_p)}{c} \cdot \omega_p - \frac{n_s(\omega_s)}{c} \cdot \omega_s - \frac{n_i(\omega_i)}{c} \cdot \omega_i = 0 \quad (2.13)$$

Finally, with the assumptions of propagation in  $\hat{z}$  and of wide crystal ( $L_x, L_y \gg L_z$ ), we get:

$$|\phi\rangle \propto \sum_{k_s k_i} \delta(\Delta\omega) \delta(\Delta k_x) \delta(\Delta k_y) \text{sinc}[\Delta k_z L_z/2] \hat{a}_{k_s}^\dagger \hat{a}_{k_i}^\dagger |\phi_0\rangle \quad (2.14)$$

Since  $\text{sinc}[\Delta k_z L_z/2] \hat{a}_{k_s}^\dagger \hat{a}_{k_i}^\dagger$  cannot be factorized, we say that the signal and idler photons are entangled. In contrast to the biphoton state, two-particle entangled state cannot be described as a state consisting of two separate states:

$$|\psi\rangle_{ab} \neq |\psi\rangle_a \otimes |\psi\rangle_b \quad (2.15)$$

Maximally entangled quantum states of two qubits are called Bell's states. They form a maximally entangled basis of the four-dimensional Hilbert space for two qubits:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) \quad (2.16)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \quad (2.17)$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \quad (2.18)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle) \quad (2.19)$$

These states are called "maximally entangled" since correlation measurement for these states can reach an upper limit to quantum mechanical correlations between distant events of  $2\sqrt{2}$ , known as a Tsirelson bound (Fig. 6) [22].

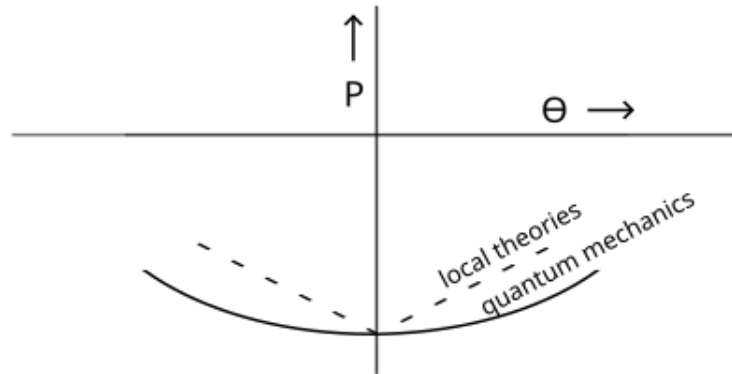


Figure 6. Behavior of correlation  $P$  near  $\Theta = 0$  and  $P = -1$  where  $\Theta$  is the angle between unit vectors representing the direction of filters in the EPR experiment. The circular region of quantum mechanics correlations is found outside Bell's straight lines, violating his inequalities. Quantum mechanics and Bell's inequalities meet at the corners. The Tsirelson bound represents maximal violation of Bell's inequality (curved line). Adapted from [3].



Quantum entanglement is another property of quantum physics far from an everyday experience. As shown in equation 2.9, two (or more) particles exist in a shared state, regardless of how far apart they are. The consequence of entanglement is that one can make a measurement of a property of one particle and immediately know the result of an equivalent measurement on the other particle, i.e. two particles behave as one system even when they are separated. In the context of quantum communications, the true power of quantum entanglement relies on the inherent randomness that can be used in communication protocols (see Subchapter 2.6.3).

The Nobel prize in 2022 was awarded to Alain Aspect, John Clauser and Anton Zeilinger “for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science” [23]. John Clauser and Stuart Freedman measured the first experimental violation of Bell’s inequality in the so-called CHSH form [24, 4], while Alain Aspect measured the first experimental violation of Bell’s inequality without the locality loophole [25, 26, 27]. Unlike classical communication, quantum communication does not allow the use of classical repeaters due to the no-cloning theorem (Appendix 8.2). The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state (or of a quantum cryptographic key in the case of quantum cryptography). However, it is possible to use quantum teleportation (Appendix 8.3) and entanglement swapping (Appendix 8.4) to create quantum repeaters that can extend the distance of a quantum communication link. Anton Zeilinger et al. [28] were the first ones to experimentally demonstrate quantum teleportation - the transfer of an unknown quantum state from one particle to another. The importance of quantum teleportation lies in the fact that this is the only way to transfer quantum information from one particle to another without losses.

## 2.5 Sources of entangled photons

High-quality single-photon sources are a long-time wish in the scientific community. However, it is difficult to achieve the emission of single photons on demand, with a high repetition rate, a 100% probability of emitting a single photon and in the desired direction. Some technologies, like quantum dots [29, 30] and nitrogen vacancies in diamonds [31], truly emit a single photon with a narrow bandwidth, but in a random direction. On the other hand, non-linear waveguides can achieve high brightness values [32], but experience low couplings to the single-mode fibers. A compromise solution that is widely used, especially in the field of quantum communication, is attenuated pulsed lasers. This approach was implemented by Bennet et al. in the first demonstration of quantum cryptography [33]. Their setup consisted of a light-emitting diode which produced faint light pulses over a distance of 30 cm in the air. Pulses were prepared in polarization states and attenuated with filters so that the average number of photons was below 1. The key part was to ensure that the polarization did not change before the photons reached the communicating parties. However, since they produce a coherent state in each pulse, the statistical photon distribution of attenuated pulsed lasers is Poissonian with variance  $\Delta n = \langle n \rangle$ . This shows that attenuated pulsed lasers are not truly single-photon sources since most pulses won't contain any photons and a small number of pulses will contain more than one photon. This results in a relative decrease in the number of detected photons since the detectors must be active all the time, even when the pulses are empty. Therefore, the number of dark counts increases and the ratio of detected photons to dark counts decreases.

As described in Subchapter 2.2.1, in the nonlinear interactions of light and dielectric materials it is possible to create single photons, but also entangled photon pairs. The first experimental realization of polarization-entangled photon pairs based on parametric down-conversion was done by Kwiat et al. in 1995 [34]. Their type-II high-intensity source of polarization-entangled photon pairs was creating signal and idler photons that were emitted in two intersecting cones. At the intersection points of cones, an entangled state occurred.

On the other hand, different types of sources have been developed to achieve co-linear emission. If we focus only on the sources based on SPDC, one possibility is to use a Mach-Zender interferometer. One crystal can be used in each arm of the inter-

ferometer to produce a superposition in path and polarization. Also, it is possible to build a folded Mach-Zender interferometer where entangled photons are generated by bidirectional pumping of a single crystal. A disadvantage of this approach is that two different interferometers need to be stabilized. Therefore, common-path interferometers have been developed to improve stability. This scheme consists of only one Sagnac interferometer to create polarization entanglement in which the crystal is pumped bidirectionally so both pump and downconverted photons follow the same path. This is the reason why all optical elements in the Sagnac loop need to work both for pump and signal and idler wavelengths. Besides the stability of the interferometer against vibration, the Sagnac interferometer offers control of the absolute difference in the length of the arms over the Mach-Zender approach. Realizations of two sources of polarization-entangled photon pairs of different SPDC types based on a Sagnac interferometer are described in Subchapter 3.1.

## ***2.6 Quantum key distribution***

In Subchapters 2.1 and 2.2 I have described how physical systems like photons and their degrees of freedom can be used to encode information. This process itself doesn't mean much, but it can be used in quantum cryptography for the creation and distribution of a secret key (Fig. 7) [35]. As mentioned in the introduction, the only proven way to be safe from eavesdropping is to use a secret cryptographic key once. Quantum key distribution enables the distribution of this secret key between Alice and Bob in a secure way based on the laws of quantum physics. For example, the fact that measurement of a quantum system perturbs the system means that an eavesdropper Eve cannot intercept the quantum key that Alice sends to Bob without disturbing the state of a quantum system (for example, photons). Let's imagine that Alice sends photons in a specific quantum state to Bob. If Bob receives photons with unperturbed states, it means that there was no measurement between Alice and Bob (under the assumption of an ideal channel without losses and perturbations) and that information is preserved (the ways in which Bob can check if the state is preserved are described in the following subchapters). In other words, if Eve makes a measurement, she will reveal her presence. Therefore, if there is no perturbation, there was no measurement conducted between the users and no eavesdropping occurred.

However, if Alice and Bob find that Eve is present, they can easily discard it since the key itself does not carry the information but is used only to encode the information to be sent. Now, imagine that in the previous example Eve tries to intercept photons halfway between Alice and Bob, make a measurement, copy the state into a new photon and resend it to Bob. In this way, she could circumvent the restriction given by the fact that her measurement would disturb the state. However, this is not possible due to the no-cloning theorem. Note that these examples assume that Alice and Bob are sure that they are communicating with each other. However, Eve can pretend that she is one of the participants (Alice or Bob). To avoid it, Alice and Bob need to perform authentication before QKD starts. One way of doing that is to pre-share a short secret key that can serve as an authenticator. This can get complicated in the case of a network with a large number of users. However, as shown by Solomons et al. [36], it is possible to use partially trusted nodes in the network for a limited period of time in the process of authentication of new users which simplifies the process.

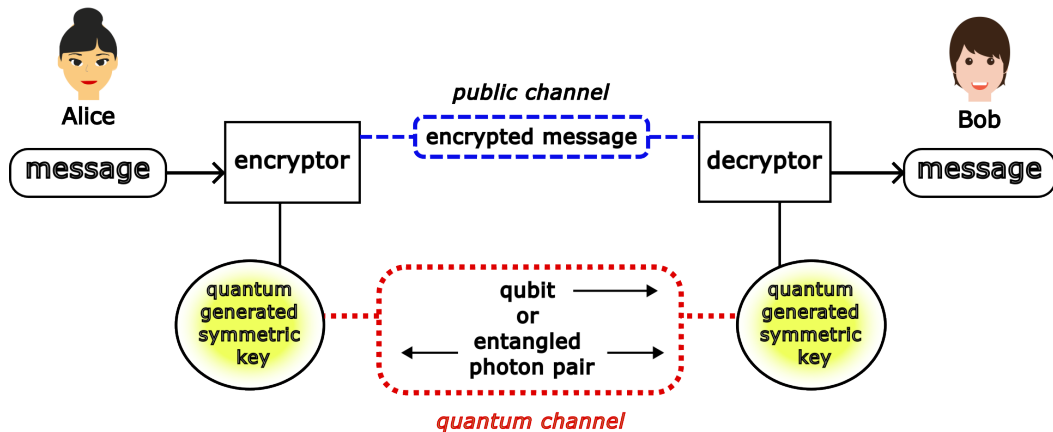


Figure 7. A schematic diagram of a quantum communication process

The first out-of-lab demonstration of QKD was done using installed telecom fiber under Lake Geneva with photons at 1300 nm which enabled the creation of a key over a distance of 23 km [37]. Two years earlier, a similar experiment was conducted using an optical fiber coil over a distance of 1100 meters with photons at 800 nm [38]. Polarization encoding was used in both experiments, and it was noticed that the error rate would suddenly increase after a couple of minutes. This was the first indication that polarization-encoded schemes in fibers require compensation methods to ensure that the polarization basis system is identical at the source and the receiver.

No matter whether classical or quantum, in-fiber or free-space, the main parts of communication systems are source, communication channel and a detector. As described in the previous subchapter, photons are a natural choice for a physical system that is used for encoding. Two main categories of photon sources are used – single photon sources (or due to practicality weak coherent light sources) and sources of entangled photon pairs. Another part of the setup that can also be considered as a part of the source is an encoder. An encoder is used to encode the bit of information to the physical carrier. When talking about photons, waveplates and polarizers can be used to prepare polarization states in the process of polarization encoding. On the other hand, Mach-Zender interferometers can be used to generate phase shifts in the implementation of phase encoding. For the communication channel, optical fibers and free space can be used. While the birefringence of the optical fibers can perturb the polarization states of photons, atmospheric absorption can cause losses in free-space communication. Also, it is important to choose the appropriate wavelength according to the communication channel used in order to minimize losses. Similar to the encoder and the source, a decoder can be considered a part of the detection system. It is used to decode information that has been sent from the source and encoded with the encoder. When using polarization encoding, an encoder can be a beamsplitter, and for phase encoding, another interferometer can be implemented. The detectors also have to be chosen according to the wavelength of the photons that are used. The most common ones are avalanche photodiodes and superconducting detectors. More details about the detectors can be found in Chapter 3.3.

The most important aspect of QKD is its security. In the ideal case, any aforementioned part of the experimental setup wouldn't introduce any errors. In reality, neither of them is perfect. However, it is not possible to distinguish between errors introduced by imperfections of the experimental setup and errors introduced by an eavesdropper. Therefore, all detected errors are attributed to Eve. Since we have concluded that errors are inevitable and that it is impossible to know when Eve is really present, the question is whether it is possible to establish a secret key at all. Steps that help Alice and Bob produce the secret key are error correction and privacy amplification. Privacy amplification allows two parties to get a secret key even if an eavesdropper has partial information. Users can start the experiment and measure the amount of errors, which is called the quantum bit error rate (QBER).

QBER can be defined as the ratio of wrong bits to the total number of bits received. Shor and Preskill [39] have shown that it is possible to extract a secret key for a QBER with a value no greater than approximately 11%. There are different contributions to the QBER - the first one is photons that end up in the wrong detector due to imperfect optical elements (for example, the extinction ratio of the PBS) or due to a change of state during transmission in the communication channel. The other one is due to detectors and their imperfections (dark counts, afterpulsing). This contribution increases with distance since the dark-count rate remains constant while the bit rate goes down. Finally, there is also a contribution from the imperfect photon sources. In the following subchapters, I will describe the most common protocols and explore the possibilities for multiple-user QKD.

### **2.6.1 BB84 protocol**

The first proposed protocol for QKD is the so-called BB84 which was presented by Charles Bennett and Gilles Brassard in 1984 [5]. The protocol can use any two-level quantum system to encode qubits, but here I will explain it using photon polarization. We note that for this protocol both classical and quantum channels are required. In the first step, Alice prepares and sends a random sequence of four states in two complementary bases (HV and DA) through the quantum channel. For (true) randomness, Alice can use a (quantum) random number generator. These states can be associated with binary 0 and binary 1. The non-orthogonality ensures that an eavesdropper Eve cannot clone or measure the prepared states with perfect fidelity (due to the no-cloning theorem). Next, Bob independently and randomly selects either the HV or DA base to analyze the polarization of the photons he receives. The so-called raw key that Bob now has, contains on average a 25% error rate. This error rate is too high for standard correction schemes so, when the quantum communication is over, Bob publicly announces his measurement basis through the classical channel. Now, Alice reveals if the basis in which she sent each qubit is the same as the basis measured by Bob. Notice that neither of them reveals the results of measurements, only the basis that was used for the preparation or a measurement. After they exchange the information about the basis, they discard all the events corresponding to different bases used. The raw key is now shortened by about 50% and is called the sifted key. If there is an eavesdropper Eve who listens to a public channel, she doesn't

get any information about the measurement results. The only way for Eve to find out the value of the bit sent is to intercept it and make a measurement of it. However, Bob would notice the missing bit, warn Alice about it and they would discard that bit. The next thing that Eve could do is to make an interception of a photon, read the polarization state, and prepare a new photon to send to Bob. However, Eve doesn't know if the sending basis was HV or DA, so half of the photons she sends would be in the wrong basis, which would be noticed in the basis reconciliation step. Another step that Alice and Bob can take to eliminate possible eavesdroppers is to take only a small part of a sifted key to get the secret key. In this way, they sacrifice the length of the key for security. This type of protocol, in which one user prepares a quantum state by encoding a discrete random variable is known as a "prepare-and-measure" protocol. The source used in the BB84 protocol are weak photon pulses (Subchapter 2.5) located at one of the users.

### **2.6.2 E91 protocol**

Unlike the BB84 protocol where a quantum channel transmits weak photon pulses from a sender to a receiver, in the E91 protocol a quantum channel transmits entangled photons from a single source in the middle to two receivers. Entanglement ensures that only after the measurement one can get some information, as opposed to the BB84 protocol where state is initially prepared and sent toward another user. The protocol was proposed by Ekert in 1991 [40]. If the source produces two qubits in the same state chosen randomly, sends them to Alice and Bob and announces the basis afterward, it is equivalent to BB84. But, if the two qubits are produced in the maximally entangled, so-called EPR state (or Bell state), when Alice and Bob use the same basis, their results are identical, providing them with a common key. Protocols that use entangled states are different from "prepare-and-measure" protocols. The security of the E91 protocol relies on the completeness of quantum mechanics, a property discussed by Einstein, Podolsky and Rosen in their gedanken\* experiment from 1935 [2]. Alice and Bob can use a third basis which gives the probability that they might choose the same basis of  $2/9$ . These bases are chosen following a special form of Bell's inequality, the so-called CHSH test (Clauser, Horne, Shimony and Holt test) to check the security of the established connection [24]. In contrast to BB84, where Bob can have empty pulses due to imperfections of the detection system, in an

E91 protocol such a problem is avoided. Furthermore, with the entanglement-based protocols random number generators can be avoided. Since the E91 protocol makes use of the nonlocal feature of entanglement, Eve's interference in the communication process can be seen as inducing additional elements of physical reality which would affect the nonlocality of quantum mechanics.

### 2.6.3 BBM92 protocol

Following Ekert's proposal, next year Bennet et al. proposed a simpler scheme based on an entanglement called BBM92 [41]. The protocol follows the steps of BB84, but Alice and Bob randomly select one conjugate basis (experimental realization can be done with a beamsplitter) to make independent measurements (Fig. 8). The probability of generating a sifted key is higher than with the E91 protocol and is equal to 1/2. Therefore, the BBM92 protocol is a common choice in experimental realizations of quantum networks (Table 3).

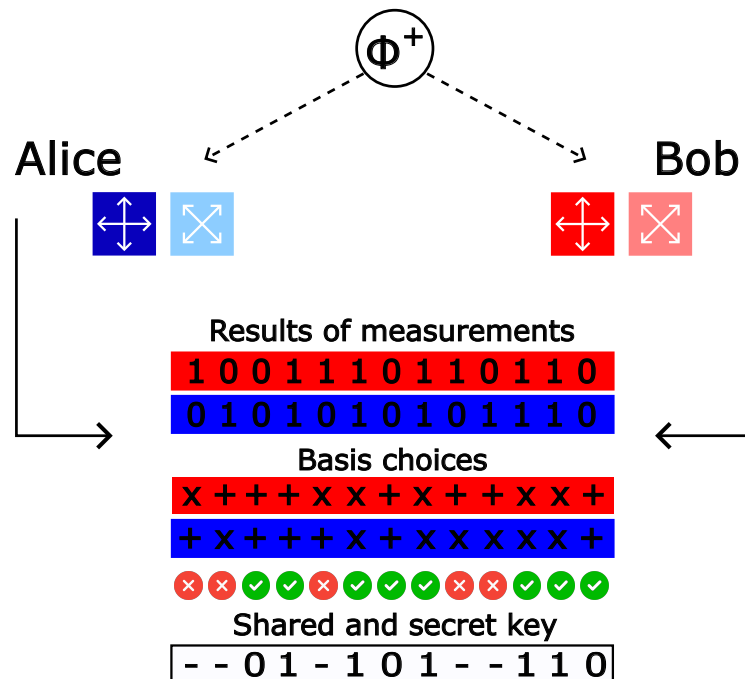


Figure 8. A scheme of a BBM92 protocol. The source of polarization entangled photon pairs is denoted as  $\phi^+$ . Alice and Bob make measurements and keep results secret, while publicly announcing their choice of basis. In that way, no information about the measurement results is public. They keep only the results of measurements made in the same basis and generate a secret key out of it.



Table 3. Examples of BBM92-based quantum networks

Reference	Platform	Spectrum bandwidth (nm)	Basis	Number of users	SKR (bps)
Wengerowsky et al. [42]	Fiber-coupled	60	Polarization	4	/*
Joshi et al. [43]	Fiber-coupled	60	Polarization	8	0.5-51.8
Fitzke et al. [44]	Fiber-coupled	75	Time-bin	4	6.3/29

\*only measured coincidence counts

#### 2.6.4 Multiple-user QKD

As we have seen in the previous subchapter, quantum communication protocols have first been developed for two users connected by a link. However, in real-life applications, we have to be able to connect multiple users. Scaling communication from two to more users into a quantum network can be done in a couple of different ways:

- **Trusted node networks** -we can imagine a situation where Alice communicates with Bob via an intermediate user or node. For example, if Alice and Bob are too far apart from each other to allow a direct link due to losses in the communication channel (Fig. 9). An intermediate node needs to be trusted by Alice and Bob since it can measure the quantum state (thereby converting it into classical information), then create a new quantum state and send it to the right user. Additional users can join the network with access to the intermediate node. However, this type of network implies that all users in the network have to be trusted which can be both hard and undesirable to achieve. Also, if the trusted node is under attack, the adversary can get all the keys stored within that node and therefore messages sent through that node would be jeopardized. This can be avoided by shutting the node down in a certain

time interval after detecting the attack [45] but it causes network downtime. Some examples of trusted node networks are the SECOQC network in Vienna [46], the SwissQuantum network in the Geneva metropolitan area [47], the Tokyo network [48] and 46-node quantum metropolitan area network in China [49].

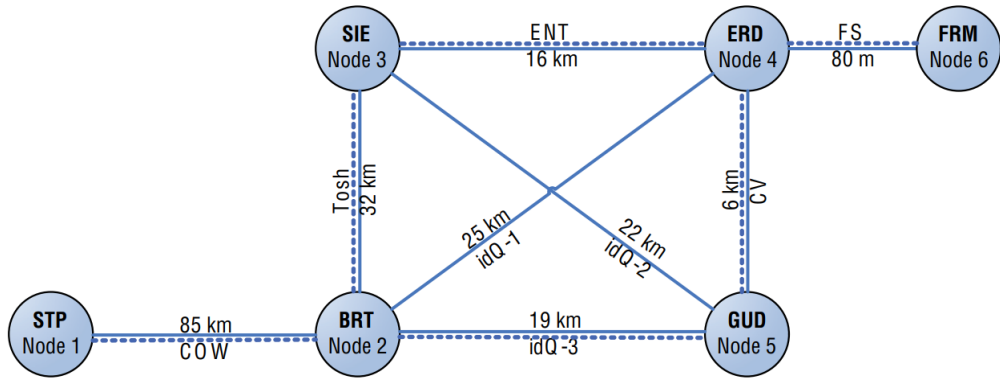


Figure 9. Topology of the SECOQC QKD network based on trusted nodes [46].

- Actively switched - Actively switched or access networks are networks in which the most expensive resource - the single photon detector, is shared among the users [50, 51] (Fig. 10). The limitation on the number of users  $N$  connected to the network is imposed only with the number of input ports on the optical switch (or with the  $1 \times N$  beamsplitter). However, if the shared resource is under attack, the security of the whole network is under question. Also, access networks require an authentication process for each new connection which takes more time. Examples of this type of network are the DARPA network in the USA [52] and the network in Hefei (China) [53].

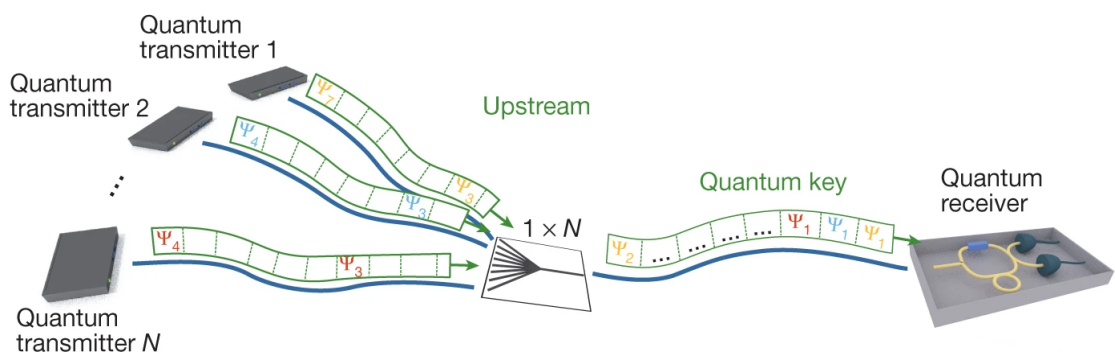


Figure 10. Topology of a point-to-multipoint quantum access network [50].

- Fully connected networks - simultaneous communication between all users in a network demands a direct connection between them. This can be achieved with multi-partite states that are shared among the users [54]. However, difficulties in their experimental realization make them impractical to use. Another approach, that will be described in this work (Subchapter 5.1), is to use entangled photon pairs and polarization degree of freedom (Fig. 11, physical layer) for protocol encoding and their wavelength distribution for distribution among the users (Fig. 11, quantum correlations layer).

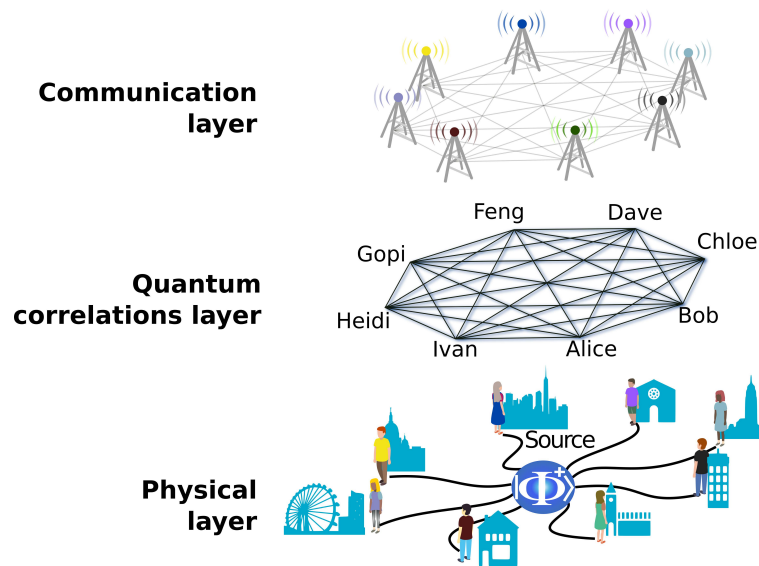


Figure 11. Three conceptual layers of a fully connected quantum network. The bottom layer represents the physical hardware, including the source of polarization entangled photon pairs, optical components for routing and polarization control, as well as detection stations (detectors and polarization analysis modules). The quantum correlations layer represents distribution of entangled photon pairs among users in the network. In the communication layer measurement results are processed to implement QKD and other protocols [36].

## 3 Experimental setup

### 3.1 Sources of entangled photons

In general, sources of polarization-entangled photons consist of the pump part, Sagnac interferometer and collection part. The pump part is used to select the polarization of the pump (polarization beamsplitter - PBS and a half-wave plate) and to direct the pump beam toward the Sagnac interferometer. The pump beam is separated on the polarization beamsplitter depending on the polarization - horizontal polarization is transmitted and vertical polarization is reflected. Down-converted photons are created in the Sagnac interferometer in both directions and re-combined on the PBS towards collection fibers.

#### 3.1.1 Source of polarization-entangled photons of type 0

To connect multiple users in a fully connected network (full-mesh) we can use a broadband source of polarization entangled photon pairs [42]. In this case, polarization of photons is used for the process of encoding and their wavelength for distribution between users. The source of polarization-entangled photons of type 0 was built by Marcus Clark and Matej Peranić under the supervision of Dr. Siddarth Joshi at the University of Bristol. The scheme of this source is presented in Fig. 12. The source produces polarization-entangled photon pairs that are distributed in the network with the Dense Wavelength Division Multiplexer (DWDM).

The spectrum of the source is presented in Fig. 13. Photon pairs that are distributed among the users are symmetrical around the central wavelength (1550.12 nm) that corresponds to the ITU channel 34, according to the ITU-T G.694.1 recommendation. The pairs were further separated into 30 ITU channels spaced around the ITU channel 34 (Appendix 8.3). For this central wavelength the loss in optical fibres is minimal and therefore it is also commonly used in classical communications.

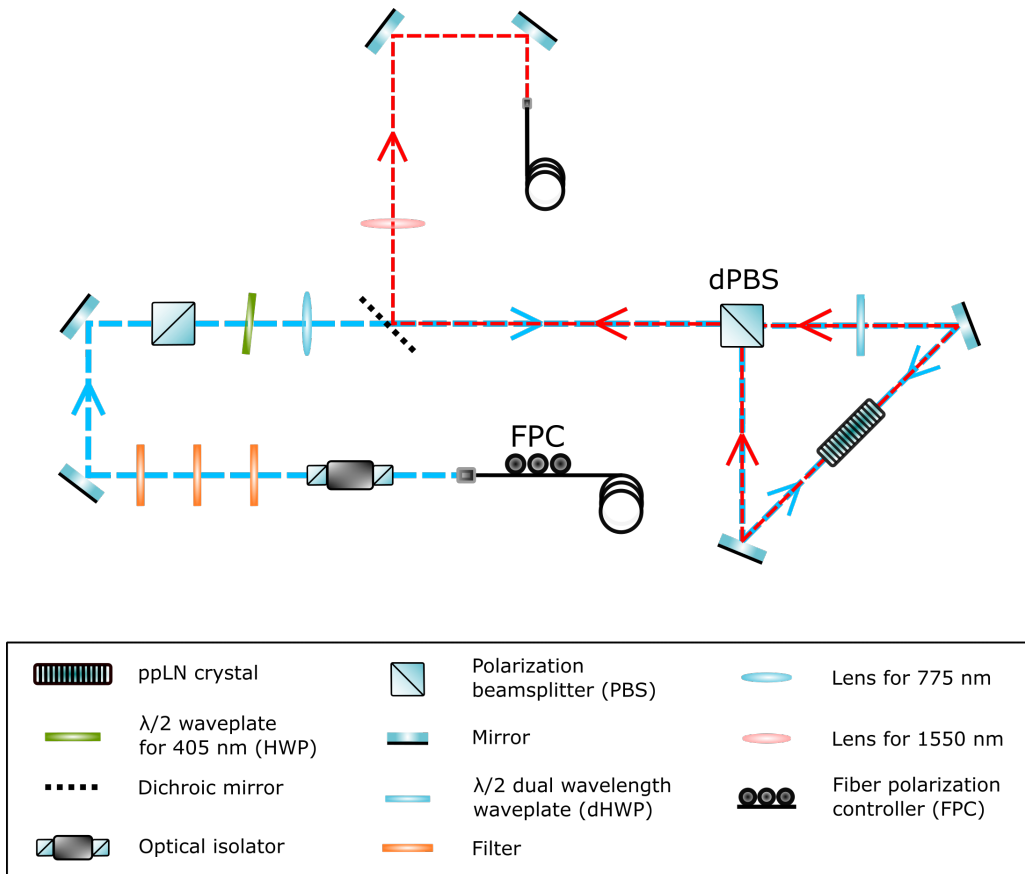


Figure 12. Experimental setup for generation of polarization-entangled photons of type 0.

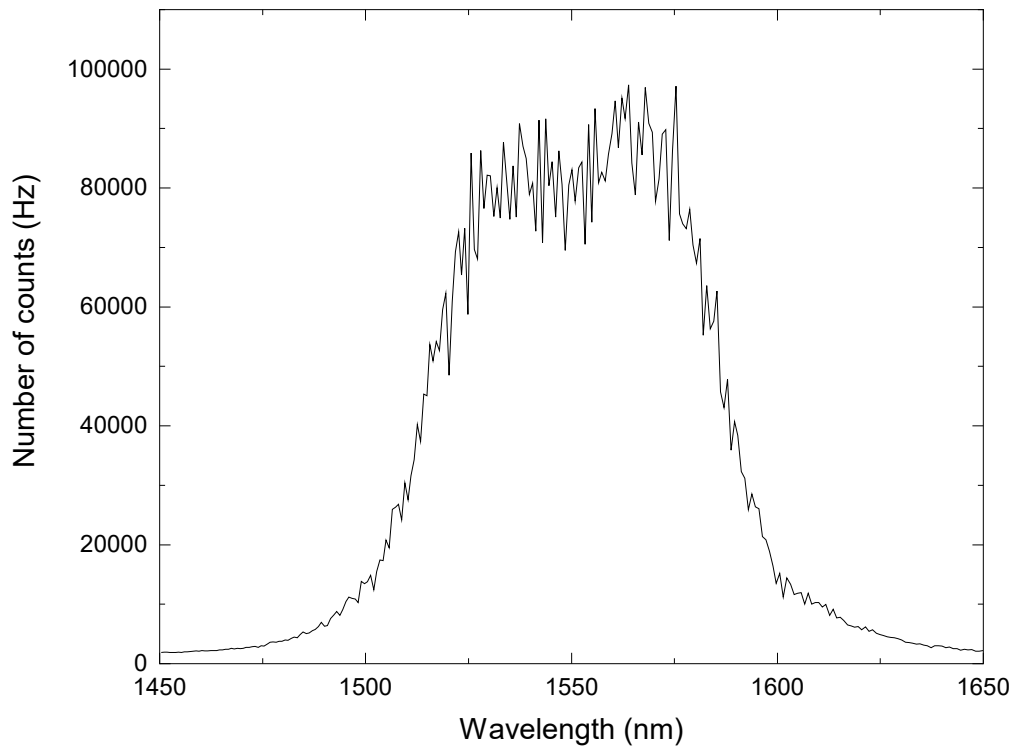


Figure 13. The experimentally measured spectrum of the type-0 source.

The source is based on a Sagnac interferometer in which 5-cm-long magnesium oxide doped periodically poled lithium niobate (MgO:ppLN) bulk crystal with a polling period of  $19.2 \mu\text{m}$  can be found. A long crystal with collinear outputs results in a higher spectral brightness and more efficient pair collection while a polling period ensures quasi-phase matching. A pump laser at  $775.06 \text{ nm}$  pumps crystal to produce signal and idler photons at  $1550 \text{ nm}$  of the same polarization as the pump (type 0). Due to the Sagnac configuration, the crystal is pumped bidirectionally with vertically polarized photons. In one arm of the interferometer dual-wavelength half-waveplate (dHWP) can be found to rotate the polarization of horizontally polarized pump photons that are transmitted on the dual-wavelength polarization beamsplitter dPBS. Also, this dHWP rotates the polarization of signal and idler photons created in the SPDC process (looking counter-clockwise) to ensure the creation of the wanted Bell state. Combining clockwise and counter-clockwise contributions in a Sagnac interferometer at the polarization beamsplitter, a maximally entangled state  $|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |H\rangle_2 + |V\rangle_1 |V\rangle_2)$  is created. In the following lines, I'll describe the alignment procedure.

The first step is to adjust the height of the pump beam without the crystal inside of the interferometer and direct the beam toward the interferometer. This can be done with the first two mirrors after the optical isolator. Once the pump beam is in plane with the optical table, we can get an overlap of the pump beam in the Sagnac loop, using two mirrors in the loop. When we get an overlap from the clockwise and the counter-clockwise direction of the pump beam inside of the loop, we can try to get the beam at  $1550 \text{ nm}$  from the output coupler into the Sagnac loop. Having both the  $775 \text{ nm}$  and  $1550 \text{ nm}$  beams inside of the loop, we can get the overlap between them. To check the overlap of the beams, we look at the interference patterns (Fig. 14). Now, we insert the crystal in the loop. The crystal is put inside the oven and positioned on the kinematic mount. We move the position controls on the kinematic mount to restore the interference pattern. When the interference pattern occurs, we start with the second-harmonic generation to get photons at  $775 \text{ nm}$  which can be coupled backwards to the input fiber.

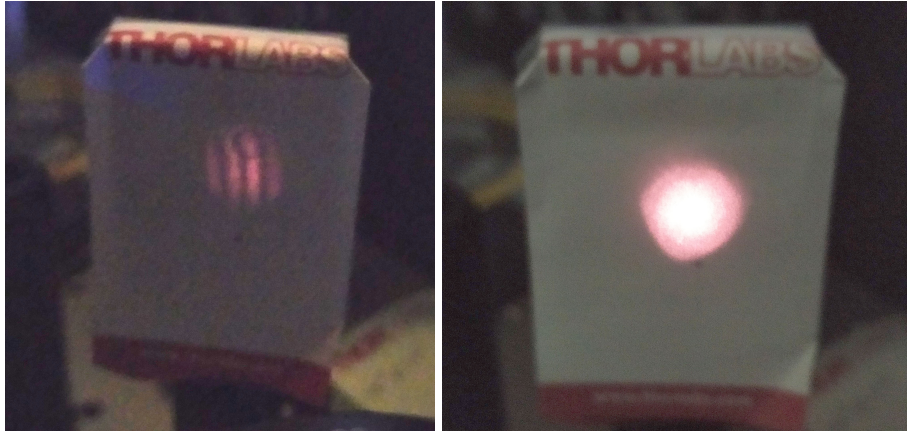


Figure 14. Left: An example of a non-optimal interference pattern, Right: With adjusting optical elements in the source, a non-optimal interference pattern is removed

### 3.1.2 Source of polarization-entangled photons of type II

In the type-II source we used a 1 cm-long temperature stabilized periodically poled potassium titanyl phosphate (ppKTP) bulk crystal with a polling period of  $9.825 \mu\text{m}$ . The ideal heating temperature optimizes the SPDC process for the creation of photons with degenerate wavelengths. The crystal is being pumped from both sides with horizontal polarization due to a dual-wavelength half-wave plate in the reflected arm of the interferometer that changes the polarization from vertical to horizontal. The alignment of the procedure of the source follows: The first step is to align the height of the beam in the whole setup. We accomplished this by using only mirrors (without any additional optical elements in the setup). At this point, the pump beam is at the planned height of the crystal, i.e. parallel to the optical table all the way. The same procedure was repeated with the auxiliary laser at 810 nm through one of the collection fibers that were later connected to the detectors. The other fiber was connected to the power meter. By adjusting the mirrors, we managed to maximize the power detected on the power meter. The next step is to simultaneously align the laser beams at 405 nm and 810 nm for spatial overlap. After the alignment, we introduced new elements in the setup - dpBS and the crystal in the interferometer, waveplates and filters. To create entangled photons of degenerated wavelengths we have to heat the crystal at the optimal temperature for the SPDC.

Before taking any further steps, we measured a number of coincidences depending on the temperature of the crystal. The optimal temperature found for our crystal is

80.1°C. Further alignments were done by tilting the dPBS in the interferometer and adjusting the position and height of the crystal. When the process of the alignment was finished, we connected the collecting optical fibers (black color in Fig. 15) to the detectors and started the measurement of detecting entangled photon pairs.

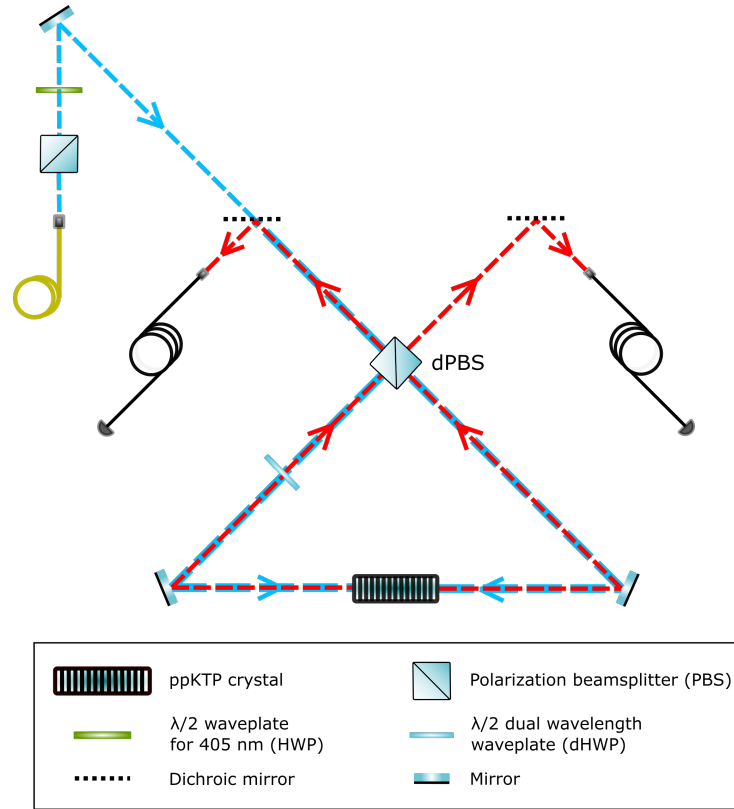


Figure 15. Experimental setup for the generation of polarization-entangled photons of type II

One point of view of the setup characteristics is how individual optical elements affect polarization. After polarization-maintaining fiber, the laser beam goes through the first dPBS which causes only the horizontal component to transmit toward the Sagnac interferometer. This dPBS is used to have complete control over polarization. This horizontal-oriented beam is rotated on the HWP to a diagonal state. This way, when reaching the main dPBS in the Sagnac, the beam is separated on the horizontal component that is transmitted and the vertical that is reflected. Also, the rotation of the HWP influences the power ratio in the two arms in the interferometer. A dichroic mirror has no any influence on the pump beam. In order to easily follow the changes of polarization inside of the interferometer, let's first take a look at the changes in the clockwise direction and then in the counter-clockwise direction (look from the top);



- The horizontal component of the beam is travelling to the dPBS where it is transmitted. After reflection from the mirror, it comes to the ppKTP crystal where the SPDC process takes place. In this process, a horizontal signal and vertical idler are created. Their polarizations are changed on the dHWP at 45° from the vertical axis in the Sagnac, after which they are separated on the dPBS. The horizontal idler is transmitted toward the first user, and the vertical signal toward the second one. Long pass filters in front of the collecting fibers are ensuring that there is no collection of the pump photons, but only of those on 810 nm (Fig. 15).
- On the other hand, the vertical component is being reflected on the dPBS and rotated to horizontal polarization on the dHWP for SPDC to take place. After the SPDC process, the signal and idler are separated on the dPBS toward two users.

Since both clockwise and counter-clockwise processes are happening simultaneously, after combining signals and idlers created in the SPDC on dPBS, we get a maximally entangled Bell state:

$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2) \quad (3.1)$$

To ensure that we are getting beam waist in the place of the crystal we used a lens of a focal length of 750 nm. The measured diameter of the pump beam in the place of the crystal is  $2r_x = 462 \mu\text{m}$ ,  $2r_y = 445.5 \mu\text{m}$ .

The beam was analyzed with the Kymera 328i spectrograph by Andor. First, a spectrograph was calibrated in the Hg-Ne excitation part of the spectrum with the calibration lamp. After the calibration, we measured the spectrum of the pump beam. The expected value (according to specifications) was 405 nm, while the result of our measurement was 404.9 nm.

We used different types of optical filters and mirrors in the setup. In front of the collecting fiber, we used two types of filters – band pass and long pass filters. Narrow band-pass filters are used to transmit only signal and idler photons on 810 nm and reflect any possible photon from the pump beam. In the case of their transmittance, they could damage the detectors. The measured transmittance of the narrow band-pass filter on 810 nm was higher than 90% (Fig. 16).

On the other hand, long-pass filters reflect lower wavelengths while ensuring the transmittance on 810 nm above 90%. Besides filters, we used a dichroic mirror that transmits the pump beam at 405 nm but reflects signal and idler photons at 810 nm (Fig. 17). The dichroic mirror is rotated on  $45^\circ$  from the vertical axis and used as a mirror for the signal and idler. All the transmittance measurements were made with the Perkin Elmer Lambda 35 spectrophotometer in the Division of Materials Chemistry of the Ruđer Bošković Institute in Zagreb.

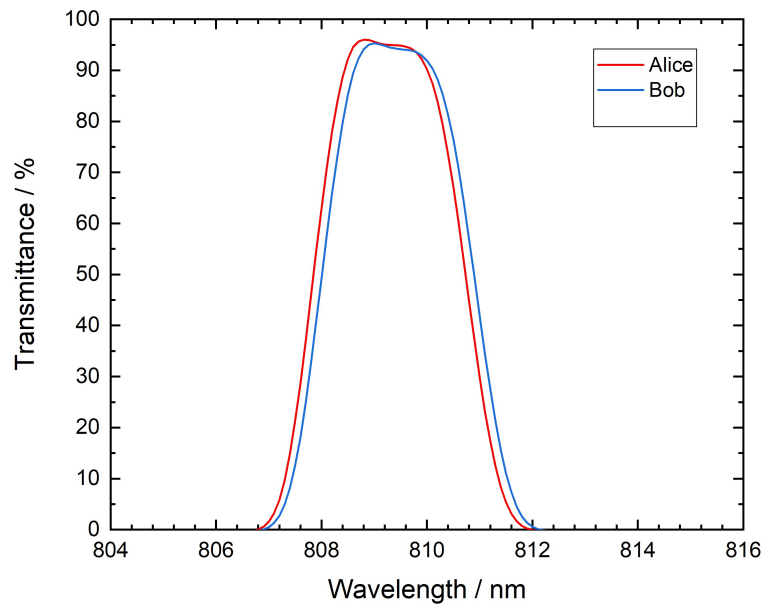


Figure 16. Measured transmittance of a narrow band pass filters

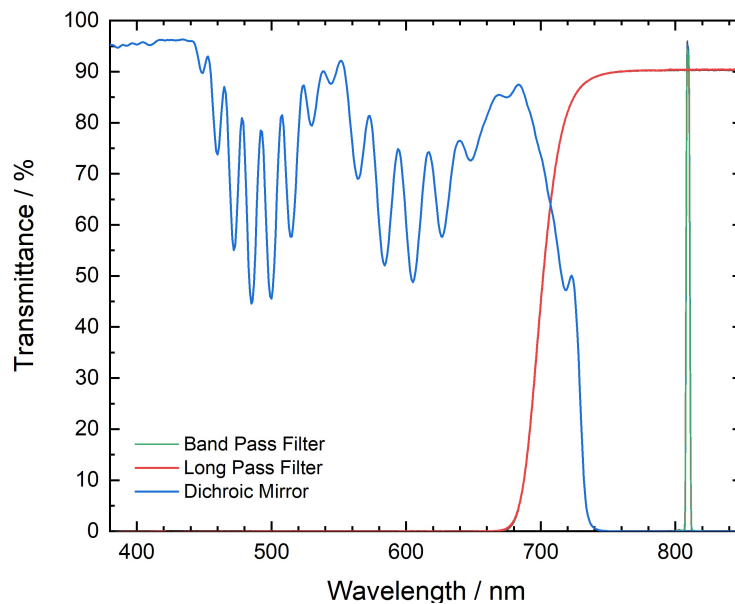


Figure 17. Measured transmittance of a narrow band-pass filter, long-pass filter and dichroic mirror

## **3.2 Detectors**

The first devices used to detect single photons were photomultiplier tubes, which combined a photoelectric cell with an electron multiplier. Although studies of the photoelectric effect - the mechanism that is behind the transformation of the kinetic energy of photons into electric energy - started in the 19th century, its full potential was not realized until Albert Einstein applied quantum theory to demonstrate that the current produced in the photoelectric cells depends on the intensity of light. Besides the conversion of a photon into an electrical signal, it is necessary to ensure that each generated electrical signal is detected with high efficiency. Additional electronics are also required to return the detector to a state that allows the detection of another photon as quickly as possible. This principle is still used today with modern solid-state detectors. We can imagine an ideal single-photon detector: all incident photons on the detector are successfully detected, the rate of detector output pulses in the absence of any incident photons is zero (dark counts), there are no afterpulses following detection, the time needed for recovery after detection in which new detection is not possible is zero, timing jitter is zero, and a detector is possible to resolve the number of detected photons. However, it is impossible to achieve all these characteristics with a single device. Therefore, it is important to carefully choose the appropriate detector to meet the demands of each measurement.

### **3.2.1 Single-photon avalanche diodes (SPAD)**

In the mid-20th century, solid-state optical single photon detection made significant progress. The development of silicon-based single-photon avalanche diodes (Si SPAD) allowed for photon counting with higher efficiency and less noise than analog semiconductor detectors in the visible range of the spectrum. However, detecting photons with lower energies, which correspond to higher wavelengths, is more challenging. Therefore, SPADs biased above breakdown are used below 900 nm, which have a detection efficiency of about 50% and a low noise rate of around 100 Hz. For optical fiber communications, one of the "telecom windows" is typically used. The first window at 800-900 nm was originally used, but due to high propagation losses, it is suitable only for short-distance transmission. The second window around 1.3  $\mu\text{m}$ , which has lower losses and weak chromatic dispersion, was originally used

for long-haul transmission. Nowadays, the third window around  $1.5 \mu\text{m}$  is widely used, offering the lowest losses of silica fibers and erbium-doped fiber amplifiers with very high performance. In the second telecom window, germanium avalanche photodiodes (Ge APD) can be used, but their performance is not as good as that of Si APD's, and they require liquid nitrogen cooling. In the third telecom window, indium gallium arsenide avalanche photodiodes (InGaAs APD) exhibit sufficient detection efficiency.

The SPAD operates by absorbing photons in the active layer, creating an electron-hole pair, and separating the carriers through voltage applied across the semiconductor lattice. The probability of triggering an avalanche current depends on whether the photogenerated electron-hole pair will be collected by the high electric field and whether the carrier reaching the depletion region will trigger an avalanche. In this sense, detection efficiency is defined as the probability that an incoming photon on the active area of the detector triggers an avalanche current that can be detected by the electronics. Usually, SPADs work in the so-called Geiger mode, where a bias voltage is above the diode's breakdown voltage. When a carrier is generated by an incoming photon, an avalanche starts until it saturates at a current typically limited by an external circuit. The saturated avalanche current flows until the bias voltage  $V$  is dropped below the breakdown voltage. The current rise time is usually less than 1ns. This process, known as quenching, is the main cause of dead time because the detector cannot respond to incoming photons until the bias voltage is restored. Geiger-mode SPADs can have detection efficiencies of up to 85% (for Si SPADs in the visible), but dark-count rates and timing jitter are higher compared to the best photomultiplier tubes. There are different schemes focused on reducing dead time, which can range from tens of nanoseconds to  $10 \mu\text{s}$ , or its effect. Some techniques result in very low-time jitter detectors, usually involving thinner absorption regions.

### **3.2.2 Drawbacks - dark counts and afterpulsing**

In the ideal case, detectors would be triggered only by the absorbed signal photon. However, this is not the only event that can start an avalanche current in SPADs. Events that start an avalanche current without the absorption of a signal photon are called dark counts, and the average number of dark pulses per unit time is usually referred to as the dark count rate. To minimize errors in quantum applications, a

long period of time between dark counts is essential. The dark count rate is affected by various factors, such as the volume of the detector, the material used and the fabrication process. Contamination that could result in dark counts may occur during wafer handling, ion implantation, or high-temperature heat treatment.

Another factor that can affect the efficiency of detectors is afterpulsing, which is caused by a train of pulses following the detection of a single photon. This phenomenon occurs due to trapped carriers during an avalanche event and their subsequent release. To minimize afterpulsing, the trapping can be reduced by quenching the avalanche current. Passive quenching can be achieved using a resistor that is small compared to the diode's resistance when no avalanche is present and large compared to the diode's residual resistance during the avalanche process. The typical range of resistance values during an avalanche is 1 M $\Omega$  to 100 k $\Omega$ . When the avalanche current flows through the bias resistor, it causes a voltage drop, which stops the avalanche process. Once the voltage rises again, the detector is ready to absorb a new photon. However, passive quenching has some limitations, as it restricts the maximum count rate. Therefore, active quenching, which involves controlling the reverse bias voltage based on the rise of an avalanche pulse, is a better option. This approach offers several advantages, such as fast switching from Geiger to quenched mode and reduced dead time.

### **3.2.3 Superconducting nanowire single-photon detector (SNSPD)**

Limitations of photomultiplier tubes and SPADs, like narrow wavelength range and limited efficiencies, have been a motivation for the development of the superconducting nanowire single-photon detector (SNSPD). It was first developed in 2001 but the first fully operational prototype was demonstrated in 2005 [55, 56]. The SNSPD consists of a thin ( $\approx 5$  nm) and narrow ( $\approx 100$  nm) superconducting material shaped into a meandering nanowire with a standard length of hundreds of micrometers (Fig. 18).

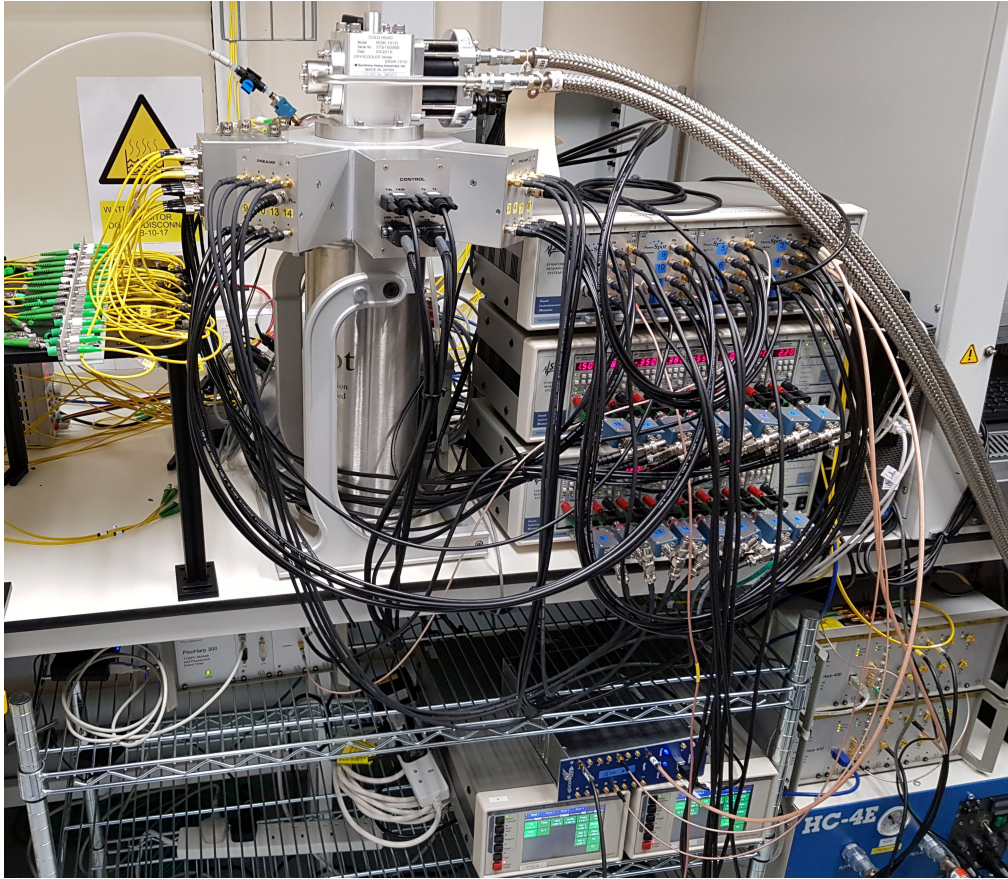


Figure 18. Superconducting nanowire single-photon detectors from Photon Spot used at the University of Bristol

The top characteristics SNSPDs have today are photon detection efficiency beyond 90%, a dark count rate lower than 0.01 counts/s and timing jitter below 50 ps [57, 58]. The nanowire is cooled below its superconducting critical temperature and biased with a constant current that is just below the critical current of the superconductor. Low noise amplifiers and counting electronics are used to detect single-photon events and register corresponding voltage pulses.

An SNSPD detection mechanism can be divided into five steps (Fig. 19):

1. Absorption of photon
2. Creation of a small resistive hotspot (a localized non-superconducting region with finite electrical resistance)
3. High current density enlarges the hotspot
4. Formation of a normal-conducting part of the strip (as the consequence of the increase of local current density around the hotspot)
5. Recovery of the superconducting state
6. Return of the bias current through the nanowire to its initial value

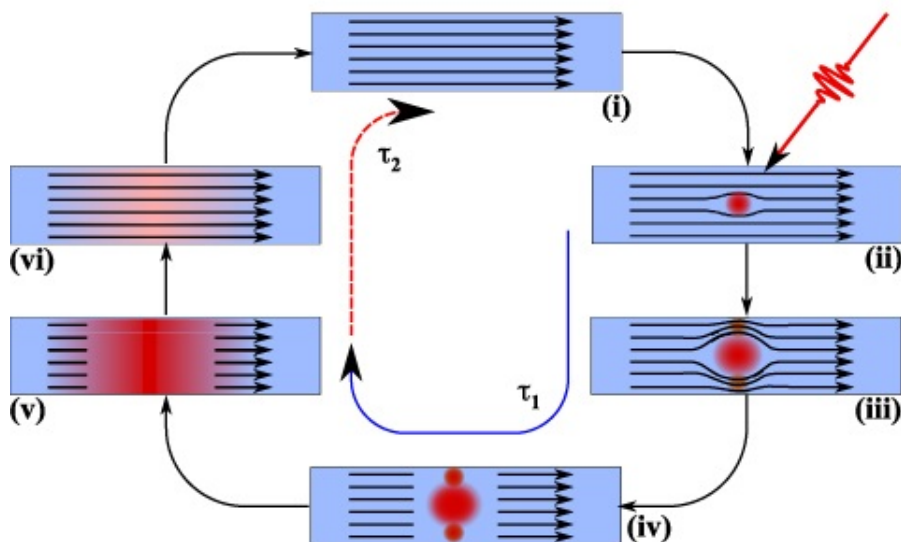


Figure 19. Operation principle of superconducting nanowire single-photon detectors. Adapted from [59]

Although these detectors do not suffer from afterpulses, they can stay in the normal state as a result of self-heating. If this happens, reset is needed by reducing the current flow. Another drawback is that they require cooling in the range of 4 K or less to keep them in the superconducting state.

### 3.3 Time synchronization

In the previous chapter, we described the work principle of different types of detectors. Their main purpose can be described in simplified terms as the detection of optical signals and their transformation into electrical signals. To make use of optical signals, we need a way to “read” the information they are carrying. This information can be encoded into a quantum state of photons but also at the time of their arrival at the detectors. For example, if we imagine a situation where two parties, Alice and Bob, want to communicate, they both need to receive a signal. But how do they know that the signal they are receiving is not just noise or, if there are more parties in the network, a signal from another user? For this purpose, we use time taggers (TT) that assign a time tag to the signal they receive (Fig. 20). If Alice and Bob use entangled photons to establish a secret key, they know that they have been produced simultaneously. Time taggers divide a time scale into bins and when they receive a signal from an entangled photon pair, they allocate a time bin to each event. Since events are rare, time taggers can compare time bins and find coincidence events between users.

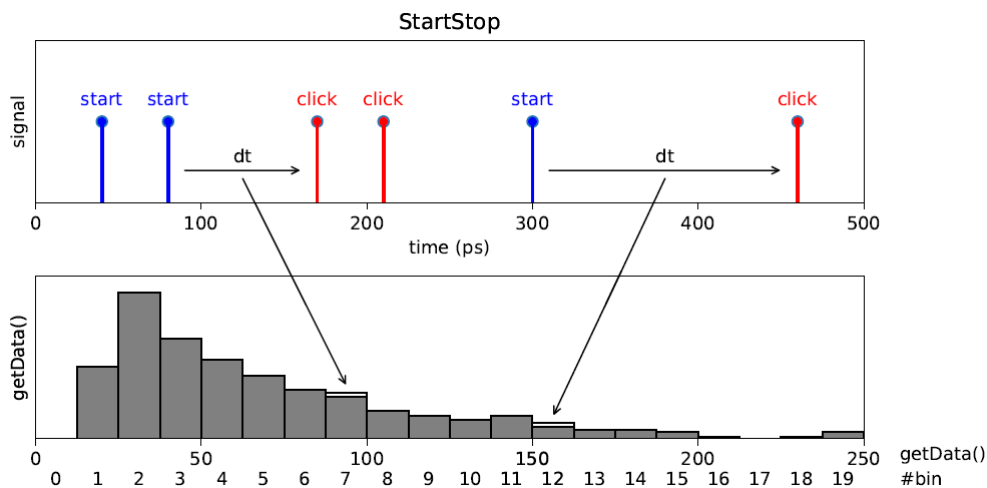


Figure 20. The operation principle of histogram measurement in a time tagger. The time tagger waits for clicks on the start channel, and for each start click, it measures the time difference between the start clicks and all subsequent clicks on the click channel and stores them in a histogram. The histogram range and resolution are specified by the number of bins and the bin width specified in ps. Adapted from Swabian instruments Time Tagger manual.



But what if Alice and Bob are far apart from each other and cannot be connected to the same device? One commercial solution can be a Synchronizer – a device that can connect multiple time taggers and provide a mutual internal clock so that they behave as a single device. However, the Synchronizer is more convenient to use for extending the number of users (input ports) rather than for solving the problem of distance between users since it requires a connection to the TTs with a coaxial cable. Therefore, a different approach is necessary. Since Alice and Bob have to be connected with an optical fiber for a QKD, we can send a train of optical pulses to users and lock their TTs to the same frequency. To achieve that, we need to transform an electrical signal from the signal generator to an optical signal, send it through the fiber, and transform it back again to an electrical signal to connect it with the time tagger. In this case, finding coincidence events needs to be done in the after-processing.

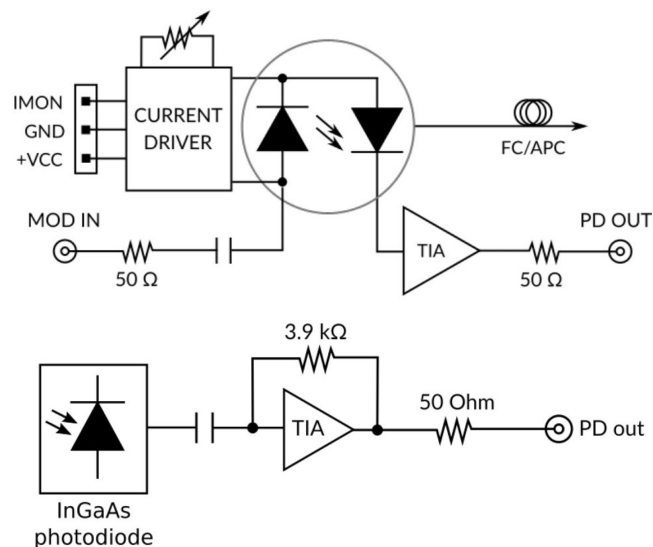


Figure 21. Above: Functional diagram of a laser diode used in time synchronization experiments, Below: Functional diagram of a photodetector used in time synchronization experiments. Adapted from Koheron manuals. As specified in the datasheet, the Time Tagger Ultra (Swabian instrument) should be able to receive an external reference signal between 10 MHz and 500 MHz in the CLK IN input and lock its internal clock to it. If properly connected, REF IN LED should light up green. To test it, we connected the signal generator (Rigol Technologies) with 1 m of coaxial cable directly to the TT and sent a 10 MHz square-wave signal. The REF IN LED turned green confirming that the TT is locked to the external reference signal. The next step was to modulate an optical signal from a laser on 1550 nm (Fig. 21, above) with a signal generator, send

it through an optical fiber, detect it with a photodetector (Fig. 21, below) and connect the photodetector to the TT with a coaxial cable. We conducted this experiment with both a one-meter optical fiber and a 10 km spool of optical fiber (SMF-28). In both cases, we managed to lock the time tagger with an external 10 MHz signal. However, even when using single-mode fiber we can suppose that after a long distance there can be a small drift in the frequency of the signal:  $f = 10 \text{ MHz} + \delta f$ . This could lead to the locking of TTs clock on different frequencies than wanted or it could stop us from locking it at all. Since we cannot access the clock directly, we have measured  $\delta f$  for which TT still shows a green light on the REF IN LED. To do this, we have connected a signal generator to the CLK input. Starting from 10 MHz, we progressively reduced and increased the frequency until the REF IN LED turned red. In this way, we measured that the acceptance range is  $\pm 2.2 \text{ kHz}$  from 10 MHz. Finally, if the reference signal wants to be sent through the same optical fiber as a quantum signal, we cannot use amplifiers. Amplifiers imply measurement, which would disturb the quantum state. Therefore, it is important to know after which distance the signal will be too weak to be detected by the TT as a reference signal. Since we had no fiber spools of various lengths available, we simulated losses by reducing the current that goes through the laser diode. In the power range of the diode that we used, the output power turned out to be linear with the current with the proportionality factor of  $0.11 \frac{\text{mW}}{\text{mA}}$  and with the threshold current  $I_{TH} = 6 \text{ mA}$ . On the other hand, relation  $P_{out} = P_{in} \cdot 10^{-\alpha \cdot d}$  connects power after an optical fiber ( $P_{out}$ ) of a length  $d$  with a linear absorption  $\alpha$ , and input power to the fiber ( $P_{in}$ ). Therefore, we can start from a maximum laser power of 5.5 mW, reduce the current through the laser diode and using the previous two relations (with the absorption of 0.28 dB/km for the SMF-28 fibre) find the distance for which TT stops locking to an external signal. By progressively decreasing the laser diode current and looking at the voltage output for modulation we were able to find the minimum current through the laser diode for which the REF IN LED still lighted up green. This gives us a minimal current/power of 7.25 mA on which the TTs clock can be locked, which corresponds to a maximum distance of 59 km. These results show that time synchronization between distant users is possible with the use of a train of optical pulses. Further research should consider the simultaneous propagation of the synchronization signal and QKD signal through the same fibre.

## 4 Experiments on hybrid communication link

In this chapter I will describe the experiments I performed at the Ruder Bošković Institute under the supervision of dr. sc. Martin Lončarić. This includes building the source of entangled photon pairs and its characterization, envisioning and designing polarization compensation experiments, building polarization analysis modules and data analysis.

### 4.1 Characterization of type-II source

In Subchapter 3.1, we described the elements and alignment procedure of sources of polarization-entangled photon pairs. To evaluate the performance of a source, we measured entanglement visibility, brightness (detected pairs/s/mW of pump power per nm) and heralding efficiency.

- Entanglement visibility

Entanglement visibility can be defined as:

$$V = \frac{N_{max} - N_{min}}{N_{max} + N_{min}} \quad (4.1)$$

where  $N_{max}$  is a maximal number of coincidences, and  $N_{min}$  a minimal number of coincidences. The Bell state that our source produces is invariant to basis transformation:

$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2) = \frac{1}{\sqrt{2}}(|D\rangle_1 |A\rangle_2 - |A\rangle_1 |D\rangle_2) \quad (4.2)$$

which means that we are expecting that the number of coincidences  $N(\alpha, \beta)$  has the following behavior:  $N(\alpha, \beta) = V \cdot \sin^2(\alpha - \beta)$ , i.e. we expect a minimal number of coincidences for  $\alpha = \beta$  or  $\alpha = \beta + 180^\circ$  where  $\alpha$  and  $\beta$  are rotation angles of polarizers from a vertical axis. In the ideal case, without any noise,  $N_{min}$  would be zero, and visibility would be exactly 1.

A visibility can be thought of as a measure of quantum entanglement quality. To measure it experimentally, we used two polarizers, one in front of each collecting fiber that is connected to the detectors. The procedure involves keeping polarizer A on a fixed angle  $\alpha$ , while the second one B is rotated in steps of  $10^\circ$  from  $0^\circ$  to  $360^\circ$ .

For each step of polarizer B, we measured the number of coincidences. We made 10 measurements for 10 s for each angle combination. The results of the visibility measurements are shown in Table 4 and in Figure 22 together with an appropriate fit with the  $\sin^2$  function.

Table 4. Entanglement visibility results for measurements in H/V and D/A bases

Analyzer angle (Alice)	Entanglement visibility
H	$(99.5 \pm 0.4)\%$
D	$(99.7 \pm 0.4)\%$
V	$(99.0 \pm 0.5)\%$
A	$(98.9 \pm 0.4)\%$

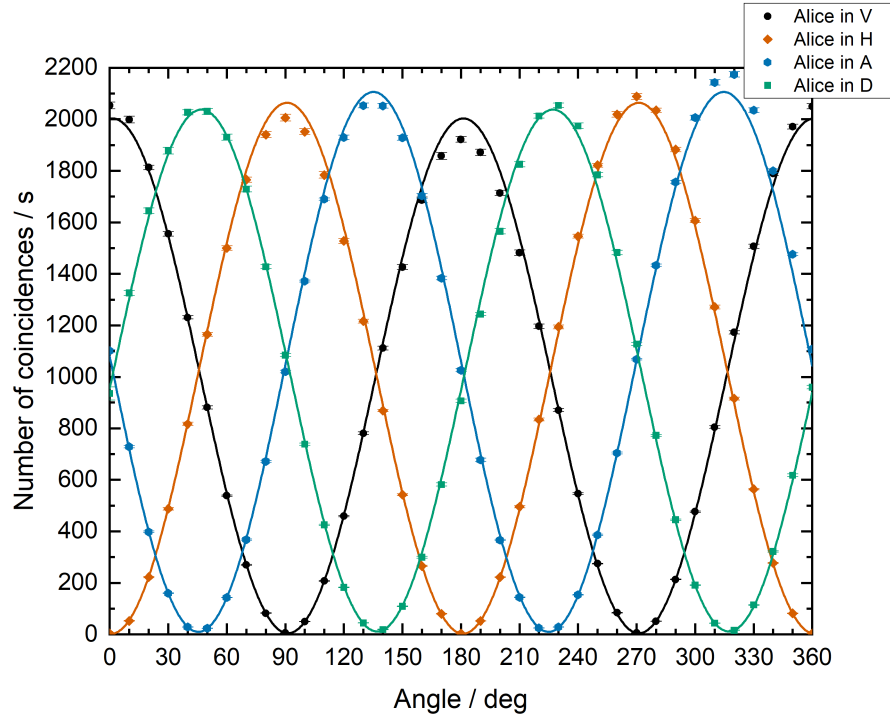


Figure 22. Measured quantum interference fringes to obtain visibility

- Brightness

Brightness is defined as the number of coincidences produced in one second for unit pump power:

$$B = \frac{N_c}{P_{laser}} \quad (4.3)$$

where  $N_c$  is the number of coincidences, and  $P_{laser}$  pump power.

The intrinsic brightness of a source depends on the nonlinear coefficient of the material (2.6) which determines the probability that the pump photon will be converted to a photon-pair. While the observed brightness is highly dependent on the configuration of the setup, the crystal used for SPDC, heralding efficiency and other system parameters such as detector efficiency, the generated brightness can be calculated once the system losses are taken into account. To measure brightness, we have prepared the pump beam in a horizontal polarization. Measurement of a coincidence number and a pump power gives us a result for the brightness of our source:

$$B = (888,5 \pm 9,2)(\text{mWs})^{-1}$$

- Heralding efficiency

Heralding efficiency ( $\eta$ ) is the probability that one photon from an entangled pair will be detected together with the other photon in another detector. In simple terms, heralding is a ratio of the number of coincidences and single detections (signal/idler counts) - for detector 1:  $\eta_1 = N_C/N_{S_2}$ , detector 2:  $\eta_2 = N_C/N_{S_1}$ , which gives us total heralding:  $\eta = \frac{N_C}{\sqrt{N_{S_1}N_{S_2}}}$ , where  $N_{S_1}$  and  $N_{S_2}$  are detections of singles in each of the detectors.

Heralding needs to be distinguished from the efficiency of entangled pairs creation that tells us the probability of conversion from one pump photon. Although the higher ratio  $N_C : N_{S_i}$  is preferable and it could be achieved with the higher pump power, we have to take saturation of detectors and higher number of accidentals into account as a limitation. The experimental result for heralding efficiency for type-II source is:

$$\eta = (24,7 \pm 0,3)\%$$

Brightness and heralding efficiency can be further improved by making the source more compact, by adjusting beam waist of a pump beam on place of the crystal and using tailored-made optical elements depending on whether the source will be used for free-space or in-fiber communication [60, 61].

## 4.2 Polarization compensation schemes

As already described, QKD provides mathematically absolute security of communication between two (or more users). However, in practice, its effectiveness can be limited due to changes in the quantum state caused by various factors such as dispersion effects within optical fibers or the atmosphere, routing geometry, or external conditions like temperature changes. To ensure that the state sent from the source reaches the users exactly as intended, a process called polarization compensation is used. Typically, this process involves using additional hardware to send classical light with a predefined polarization state through the system, while polarization controllers are used to correct any disturbances in the polarization state at the output. However, this method can cause a high level of noise on the single photon level of quantum signals or QKD needs to stop while the polarization compensation process is ongoing. Therefore, it would be preferable to use single photons in the polarization compensation process instead.

If the distance between users is larger than a few hundred kilometers, it is common to use free-space links with satellites instead of fibers [62]. Free-space communication is conducted on wavelengths around 810 nm that have low attenuation in the atmosphere [63]. However, free-space links require dark skies [64, 65] and using 810 nm results in the comparable bit rate as operation at 1310 nm or 1550 nm [63] in classical fiber-based telecom systems for short distances of up to about 5 km. Therefore, the potential use of an 810 nm signal is to connect light-polluted urban areas with satellites (Fig. 23). We can send a signal from the source that is located outside of the light-polluted area to one user located inside of it and another to the satellite.

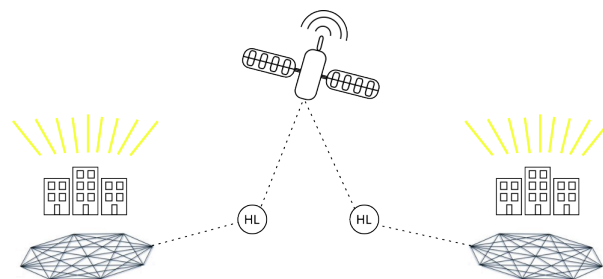


Figure 23. A schematic of a connection between two light polluted areas. These areas (e.g. cities) can be connected with a satellite via hybrid link (HL) described in this work. In this way, it is possible to establish long-distance communication with low losses.

Furthermore, another advantage of this approach is that the mixing of photons at 810 nm and 1550 nm inside the fiber is negligible (Fig. 24) [66]. This makes it a good option for real-life scenarios, such as a ground station outside of a light-polluted area with the source of entangled photons connecting the satellite with another ground station inside the light-polluted area. This situation requires uplink through free space and ground link through telecom fiber. Although the losses that arise due to atmospheric properties as turbulence and diffraction are generally lower for downlinks [66], the advantages of uplinks include avoiding the potentially complex process of locating a photon source in space, robustness from attacks against the receiver [67] and a lower photon detection rate which results in a smaller amount of data that needs to be stored [68].

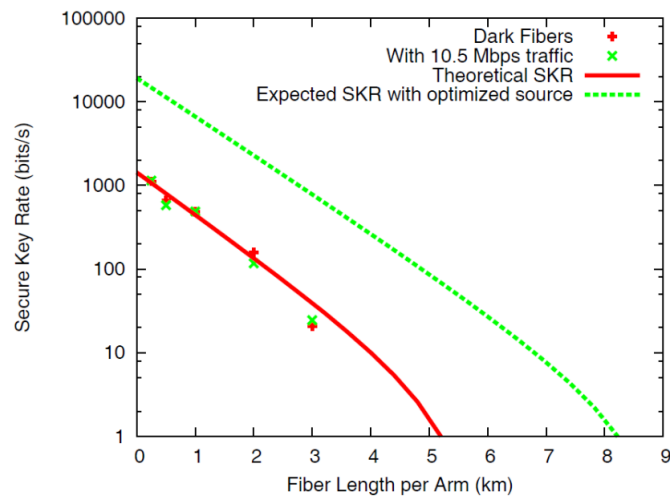


Figure 24. The secret key rate for varying lengths of fiber carrying a quantum signal at 810 nm with no telecom signals introduced (dark fibers) or with telecom signals (on 1550 nm) carrying 10.5 Mbps of traffic. Adapted from [66].

We tested polarization compensation schemes using a type-II polarization entangled photon source, as previously described. The photon source was modified to model the previously described scenario where one user is on the ground, while the other user is connected through free space (Fig. 25). However, due to technical limitations, we conducted the experiment in laboratory conditions with a 1-meter-long free-space link. For a field test, the transmitter side would need to be equipped with an emitter's output telescope (pair of lenses with an appropriate focal length) and a receiver station on the satellite would need to have adequate optical setup for detection (telescope) and analysis (PAM). Additional requirement would be a beacon signal for tracking purposes [69].

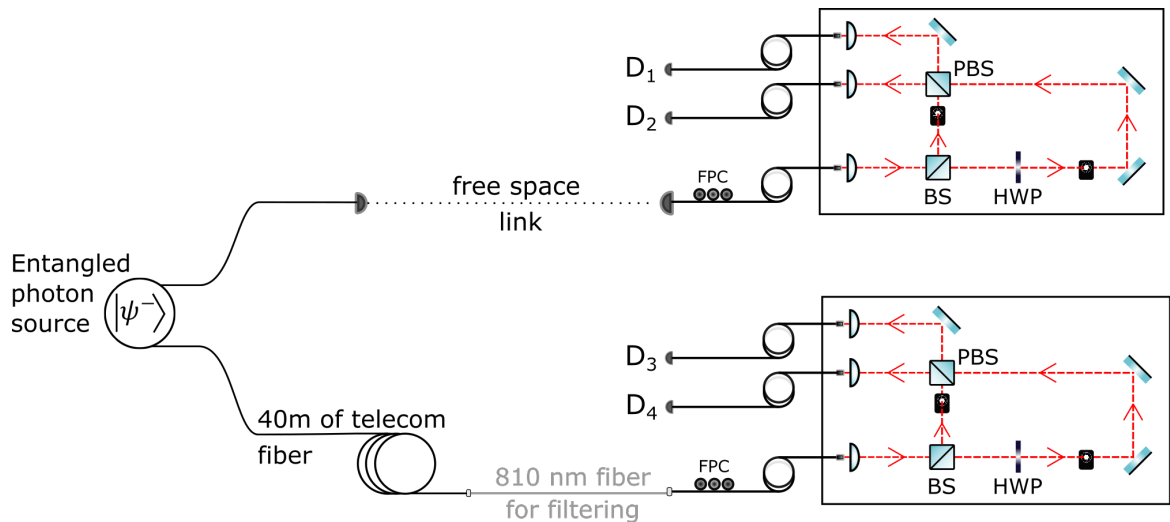


Figure 25. Experimental setup modified for the scenario with one user connected through fibre and the other user connected through free space.

A telecom fiber used in one arm of the setup caused several challenges: first of all, attenuation of about 2 dB/km is expected for 810 nm in telecom fibers. Second, since the distances from the source to the detectors in the two arms are different, a delay of the signal from one arm occurs. Finally, since standard telecom fibers are multimode for 810 nm, higher-order spatial modes will appear. The first effect will limit a communication distance, while the second effect does not present a problem since we can adjust the delay on the time tagging device (Swabian Time Tagger Ultra). Also, the higher-order spatial modes can be neutralized using an additional 810 nm single-mode fiber as a spatial filter that removes around 98% of higher-order modes [70]. The experimental setup consisted of the source of the entangled photons, passive polarization analysis module (PAM) and single photon avalanche detectors with dark counts of 227 counts per second (cps) and 552 cps at the first user and 1978 cps and 748 cps at the second user. Detectors were connected to the inputs of a time-tagging device and further to the computer for analysis.

The idea behind the first scheme is to use an additional dual-wavelength half-wave plate (dHWP) inside the Sagnac interferometer. By rotating it  $45^\circ$  from the vertical axis in the optical path in the interferometer we cancel out the effect of the first dHWP. This results in pumping the crystal only from one side. The output of the Sagnac interferometer are now photon pairs with perpendicular polarizations coming from one side to the PBS. Here, the photons from the pair are separated toward different users. Upon entering PAM, a photon can be randomly directed through the



short or long path. For polarization compensation, we track the number of photons detected in one of the detectors connected to the outputs of PAM. A polarization beamsplitter in Sagnac ensures that photons of horizontal polarization are directed toward one user and photons of vertical polarization toward another user. Knowing that the photons of horizontal polarization have been sent to PAM, we can close the short path on PAM with a mechanical shutter and compensate disturbance in polarization using a manual fiber polarisation controller. A way to achieve this is by observing the same number of counts on both detectors at one user since HWP in a long path will rotate horizontal state into a diagonal state. On the other hand, by closing the long path and opening a short path, we can minimize the number of photons coming to the first detector ( $D_1$  in Fig. 25). The same procedure can be done for the other user and photons of vertical polarization (minimizing the number of detections in the second detector  $D_2$  when the short path is opened). After the process of compensation, the additional dHWP was removed from the optical path in Sagnac and all paths on PAMs were opened. Because of the design of the PAM, users obtain three peaks in their temporal cross-correlation histogram  $g(2)$  between each detector (Fig. 26).

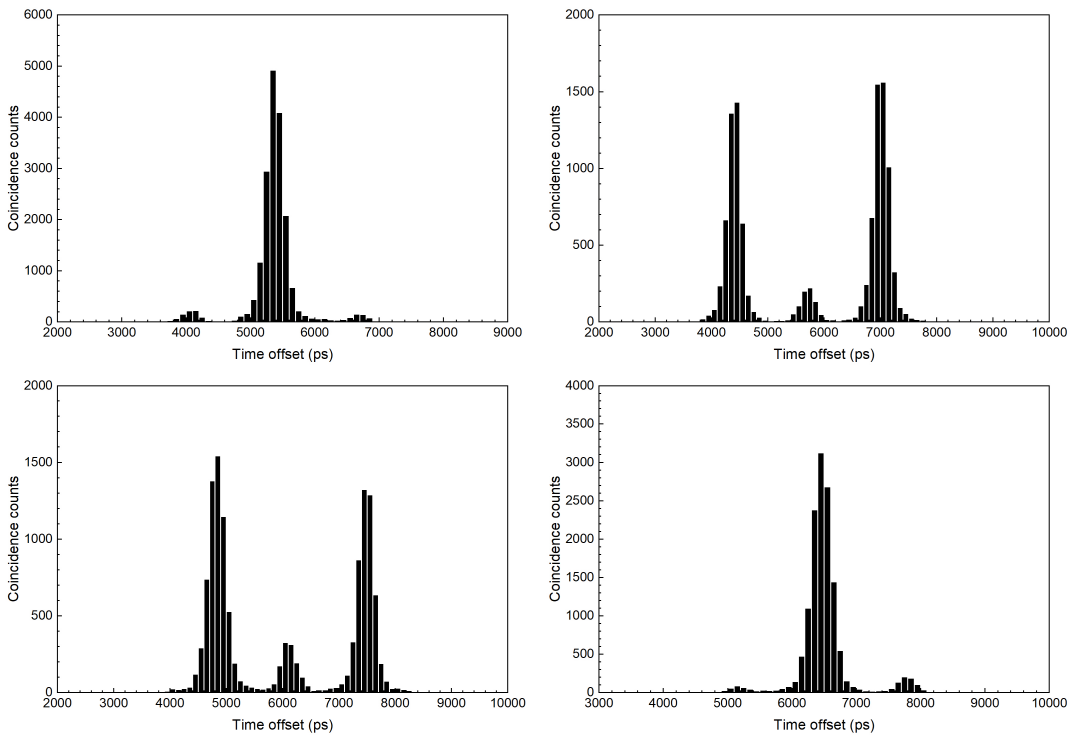


Figure 26. Temporal cross-correlation histograms. Histograms are obtained after the process of polarization compensation with an additional HWP

In this way, we can only get the information if the measurement basis choice was the same for both users. By looking at the  $g(2)$  histogram we observe the central peak that corresponds to measurements where both users chose the same measurement basis, while the side peaks correspond to choosing different basis (upper left and lower right in Fig. 26). The difference between central and side peaks corresponds to the length difference of short and long path on PAM. To ensure a positive secret key rate for entangled-based QKD protocols, a QBER under 11% is necessary [63]. The QBER can be estimated by dividing the sum of counts in the smaller central peaks (undesired anti-correlated measurement, upper right and lower left in Fig. 26) by the sum of counts in all central peaks:

$$\text{QBER} = \frac{N_{C_2} + N_{C_3}}{N_{C_1} + N_{C_2} + N_{C_3} + N_{C_4}} \quad (4.4)$$

On the other hand, following analysis in [71, 72], we can define secret key rate as:

$$R = 1 - H_2(\delta) - H_2(\delta_p) \quad (4.5)$$

where  $H_2(x)$  is Shannon entropy function

$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ . Function  $H_2(\delta)$  represents the fraction of the key sacrificed in the process of error correction and  $H_2(\delta_p)$  represents the fraction of the key sacrificed in the process of privacy amplification. Here, variables  $\delta$  and  $\delta_p$  reflect the QBER of quantum channel. We can write a more general form of the secret key rate as:

$$R = 1 - f \cdot H(\text{QBER}) - H(\text{QBER}) \quad (4.6)$$

where  $f$  stands for the efficiency of the error correction algorithm ( $f \geq 1$ ).

In our experiment, the measured QBER was  $(6.6 \pm 0.1)\%$  and the average variance of a key rate during 24 hours was under 5% from the mean value. Despite these results, we note that due to the design of PAM (Fig. 25), where the main element for the polarization analysis is PBS, one can get the same result (the same number of counts on both detectors) with both (anti)diagonal states and circular states. Therefore, it is necessary to check the result back in the HV base. This makes this scheme more time consuming and less efficient.

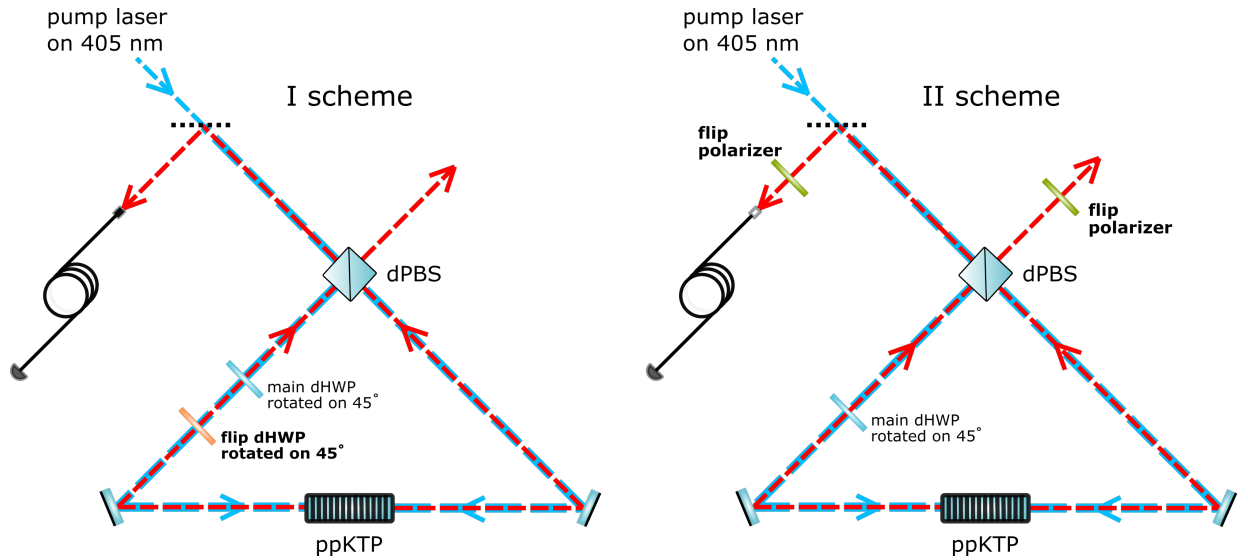


Figure 27. Two schemes for polarization compensation with type-II source

The second scheme utilizes polarizers mounted on rotators after dichroic mirrors (Fig. 27, right). When rotated on  $0^\circ/90^\circ$ , polarizers transmit only photons of vertical/horizontal polarization. The compensation has been done in the same way as previously described using manual fiber polarization controllers and PAMs. The advantages of this approach are the selection of photons of specific polarization outside of the Sagnac interferometer and the unambiguous choice of polarization. The former ensures that there is no influence on the process of creating entangled photon pairs while the latter eliminates the need for checking in both bases. Using this scheme we observed a QBER of  $(5.4 \pm 0.2)\%$ .

Based on the presented results, we showed that using the source itself in the polarization compensation process we can satisfy the security limitation for the QBER value. This approach ultimately reduces the overall cost and experimental complexity over traditional methods with an auxiliary laser. By optimizing pump power, reducing detector jitter and implementing optical elements with better extinction ratios on polarization analysis modules, we can achieve even lower QBER values.

## 5 Experiments on full-mesh quantum networks

In this chapter I will describe experiments done at the University of Bristol (UoB) under the supervision of Dr. Siddarth Joshi and dr. sc. Martin Lončarić. The source of polarization entangled photons was built by me and PhD student Marcus Clark. The quantum networks were built by me and Marcus Clark with the assistance of Post-doc Obada Alia, Dr. Sima Rahmani and Dr. Rui Wang from the High-Performance Networks Group (HPN) of UoB. The part of the experimental work with different network topologies and with the effect of additional channels was envisioned and supervised by Dr. Rui Wang from the High Performance Networks Group (HPN) of UoB. The results of experiments with compensation schemes on quantum networks were published in a paper: Peranić, M., Clark, M., Wang, R. et al. A study of polarization compensation for quantum networks. EPJ Quantum Technol. 10, 30 (2023). <https://doi.org/10.1140/epjqt/s40507-023-00187-w>.

### 5.1 Realization of a 6-user quantum network

So far, we have presented results with only two users in the process of quantum communication. However, in real life we would like to connect multiple users in the network. Another step further, connecting multiple quantum nodes with a continuous quantum channel together would create Quantum Internet (or QInternet, Fig. 28) [73]. For Quantum Internet to be fully functional, additional requirements need to be fulfilled, like the implementation of advanced network protocols supported by active switching that would allow traffic management. Also, the problem of appropriate network topologies and protocols for optimal distribution of secret keys and authentication of new users needs to be addressed [74]. To achieve this ambitious goal, first we have to find a way to support a large number of users in the network. The approach with trusted nodes has security vulnerabilities, so different alternatives have already been implemented, like wavelength multiplexing [75, 42, 43], wavelength-selective switch [76] and multiplexing combined with beamsplitters [77]. With these approaches, a large number of users has already been connected, albeit without any possibility for traffic management. Furthermore, fibers are an expensive element in the network infrastructure, so it is necessary to analyze the coexistence of a quantum signal with a classical signal through the same fiber [78].

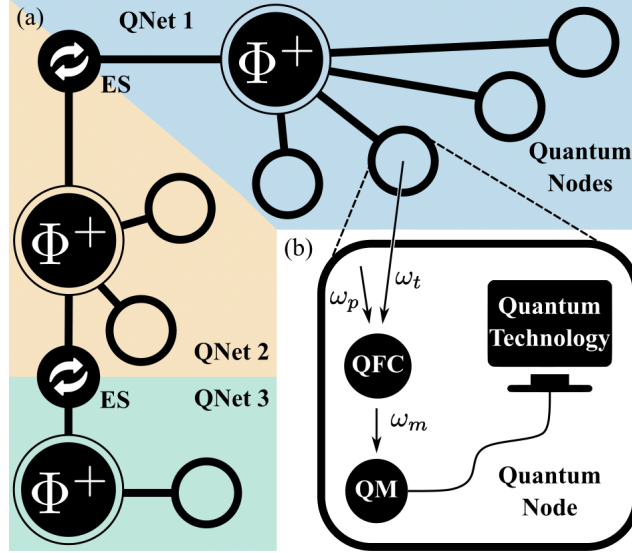


Figure 28. Schematic of Quantum Internet. a) Different colours are representing different Quantum Networks (QNet) interconnected through entanglement swapping (ES, see Appendix). b) The process of Quantum Frequency Confersion (QFC) into a Quantum Memory (QM), to connect Quantum Technology with entanglement from the QNets. Here  $\omega_p$  is the pump photon,  $\omega_t$  is the entanglement transporting photon, and  $\omega_m$  is the QM native photon [79].

As shown in Table 3, networks with four and eight users based on the BBM92 protocol have already been implemented [42, 43, 44, 80]. However, these networks are limited in network management and lack the possibility of controlling secret key rates between pairs of users. Here, we present results on a 6-user full-mesh network based on polarization encoding and wavelength multiplexing in combination with an optical switch that enables fast switching between users. This allows us to explore different topologies of the network and distribution of additional channels to particular users. The network was built through collaboration between the Ruđer Bošković Institute and the University of Bristol (UoB) as a part of the UK national quantum technology’s Quantum Communication Hub project. The main parts of the setup are the previously described source of polarization-entangled photon pairs of type-0 with the heralding efficiency of 11%, a wavelength de-multiplexer (DEMUX) that divides the broadband entangled photon spectrum into  $30 \times 100$  GHz ITU channels, an optical fibre switch (OFS) that controls the dynamicity and a multiplexer (MUX) that combines the entangled photons into a single fibre. Lastly, each user has a polarization analysis user module described in Subchapter 3.2.1 that is connected to the SNSPD and further to the time tagging device. Together the DEMUX, OFS and MUX

allow reconfiguration of the network into any arbitrary topology with dynamicity in time and wavelength. The distance between all users is 1.6 km (with a typical loss of around 11 dB), except Dave, who is connected with a metropolitan link of 5.6 km (with a loss of around 15 dB, Table 5).

Table 5. The distance and loss between users in the network and the source of entangled photon pairs. The loss includes contributions from DWDMs, optical fibre switch, fibre transmission, user modules and detectors

User	Distance (km)	Loss (dB)
Alice	1.6	8.9-10
Bob	1.6	8.1-11.1
Chloe	1.6	10.6-13
Dave	5.6	14.1-15.1
Faye	1.6	10.6-11.9
Gopi	1.6	11-11.9

## 5.2 Long term monitoring secret key rate

To test the stability of our network described in Table 5, we measured a secret key rate (SKR) for 157.3 hours. The results are presented in Fig. 29 for all 15 links. Each data point presents the average SKR over ten minutes. At  $T_1$  we performed polarization neutralization, while at  $T_2$  and  $T_3$  the operation of the network was interrupted due to cycling of SNSPDs. Also, the network was shutdown for more than 24 hours while collecting data due to power loss. However, this interruption did not affect the stability of the network. In Fig. 29 we present the monitoring of SKR in our quantum network for 7 days (Fig. 29, a) and continuous SKR over 20 hours (Fig. 29, b).

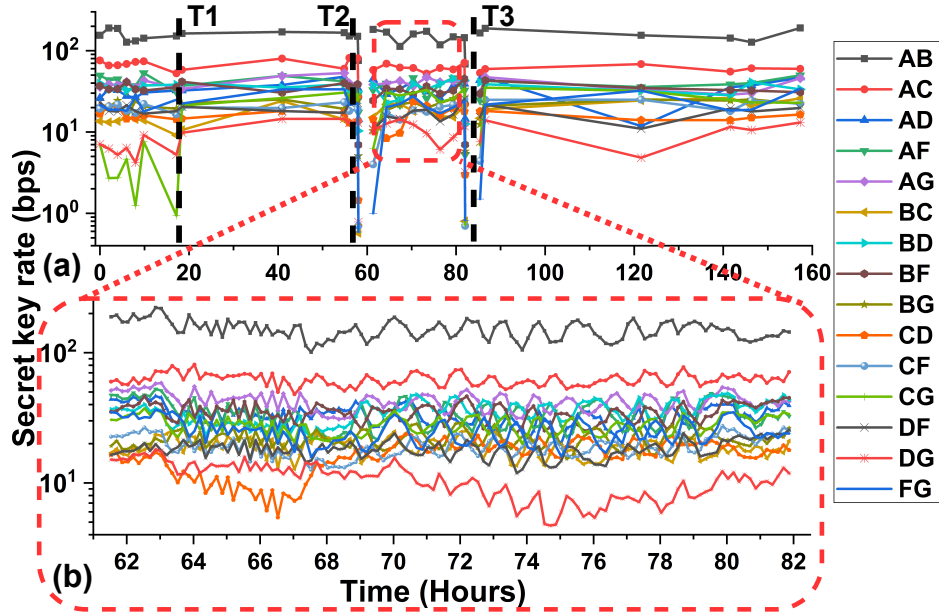


Figure 29. Long-term monitoring of a secret key rate in a full-mesh six-user network. a) Monitoring a secret key rate for 7 days, b) Monitoring a secret key rate for 20h [81].

### 5.3 Full mesh vs. partial mesh

While Fig. 29 shows the key rate for long periods of active network, it is also possible to accumulate key between a pair of users and use it in a period when the link is not active. In this case, users put a certain level of trust in the accumulated key. To compare the performance with a full-mesh network, we tested two partial mesh configurations (Fig. 30, b) and c)) that combine in a full mesh quantum network with six users (Fig. 30, a)). These partial mesh networks were actively switched after 20 minutes and compared with a full mesh network that had been running for 40 minutes.

As presented in Fig. 30, d), full mesh configuration generates more keys in the entire network than two partial mesh cases when the source laser pump power is between 0.40 mW and 1.80 mW. However, an increase in pump power results in a larger number of accidentals, which leads to higher QBER and lower SKR. This effect is best seen when comparing the total SKR for a full mesh configuration for 1.44 mW and 1.80 mW. On the other hand, for partial mesh configurations, this effect is less visible since each user receives only 2 or 3 DWDM channels compared to 5 channels for a full-mesh configuration. This result shows that it is possible to further enhance

the performance of partial mesh networks with the pump power. Interestingly, previous research of a full mesh vs. partial mesh performance with the source with 3% heralding efficiency showed that partial mesh schemes outperform the full mesh scheme by generating a higher amount of keys [81, 82]. This contradiction can be explained by the fact that with a low heralding efficiency source, most photons that detectors detect are accidentals which leads to higher QBER.

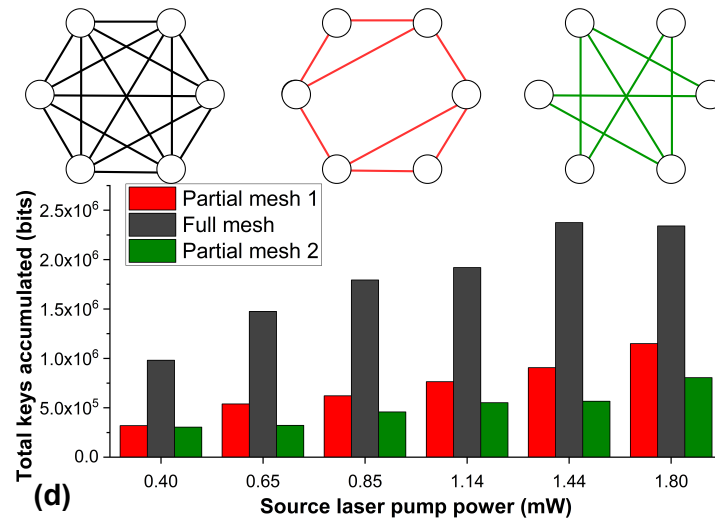


Figure 30. Comparison of accumulated secret key (d) for two partial mesh network configurations (b, c) and a full-mesh configuration (a). Adapted from [81]

#### 5.4 Effect of additional channels

One could think that adding new entangled photon pairs to the same pair of users would be a good idea for increasing the secret key rate, just like in classical communications. However, in quantum communication that is not the case. An increase in the number of entangled wavelengths the user is receiving increases the accidental count rate due to the multiplexing of more quantum channels onto a single detector. As shown in Fig. 31, for the same pump power, the AB link can achieve a higher key rate with a lower number of wavelength pairs. However, this problem could be overcome by using a pulsed laser with a pulse width smaller than the detector jitter. In the pulse scheme, users would need to have gated detectors that would be open only for each pulse. For the scheme to work, the opening of the gate should be adjusted according to the time delay between users (Fig. 26).



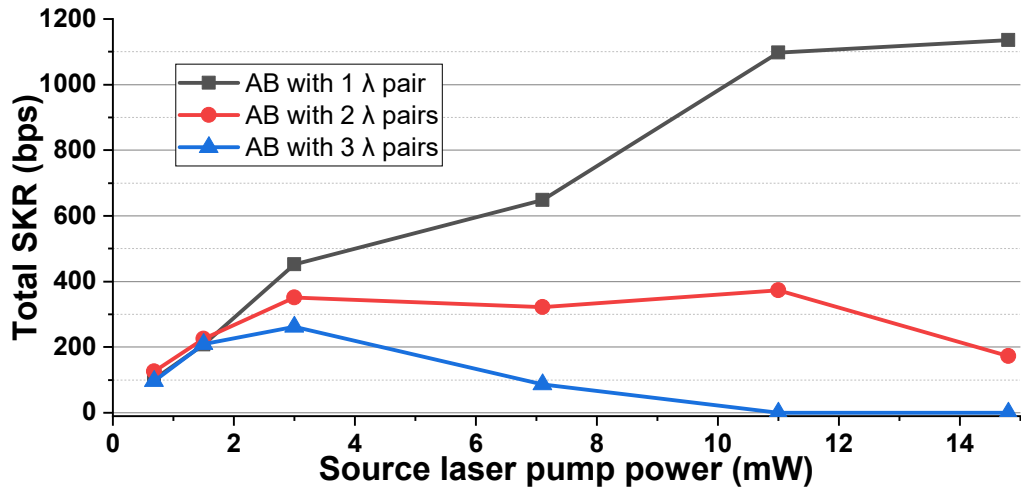


Figure 31. Comparison of secret key rates (SKR) for a link between two users with 1, 2 and 3 shared photon pairs for different pump powers. Adapted from [81]

### 5.5 Polarization compensation schemes for quantum networks

The same as with two users, any polarization encoding scheme used in the quantum network suffers from the birefringence of the optical fibres and will not work without some kind of polarization compensation procedure. Although the methods presented in Subchapter 4.2 could also be used in the quantum network scenario, they require additional optical elements that would need to be customized for a broad spectrum of a specific source and are not unambiguous. Therefore, we propose four different realizations of polarization compensation schemes for quantum networks with different types of reference signals. We assess their performances (based on the type of reference signals, complexity, effort, level of disruption to network operations and performance) in the quantum network with a polarization-entangled photon pair source and wavelength division multiplexing technique (Fig. 32). Traditional (canonical) methods that use classical light with predefined polarization cause a high level of noise on the single photon level of quantum signals or require a downtime of the network. Also, scaling these methods on quantum networks with a large number of users would require hundreds of polarization controllers, i.e. methods that are easy to implement with two-user links may not be scalable for large and interconnected quantum networks.

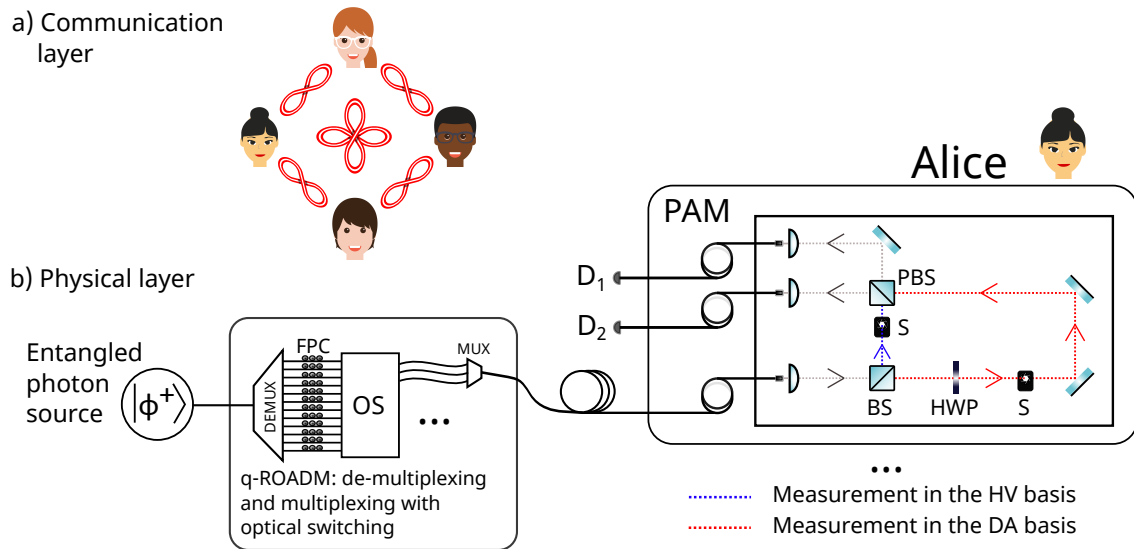


Figure 32. a) Communication layer of the four-user full-mesh network. Every pair of users shares a bipartite entangled state as represented by each individual infinity symbol. b) The physical layer of the network consists of a polarization-entangled photon source, q-ROADM (consisting of fibre polarization controllers (FPC), optical switch (OS), de-multiplexer DEMUX and multiplexer MUX) and polarization analysis module (PAM). Each user has a PAM consisting of a beamsplitter (BS), polarization beamsplitter (PBS), half waveplate (HWP), shutters (S), and mirrors. Single-photon detectors are depicted as  $D_1$  and  $D_2$ . Solid lines depict optical fibres and dashed lines free-space path of photons [83].

### 5.5.1 Canonical method

Despite the aforementioned drawbacks, the first method we examine is the canonical method to establish a basis for comparing different methods. The canonical method implies sending an auxiliary laser light with predefined polarization states through the same optical fibre that will later carry the quantum signal to the users. In our network, since different users are connected to the source with different wavelengths, we also have to keep track of which wavelength of classical light we are sending toward which user in the compensation process. Therefore, we use a tunable laser as a source. Furthermore, with the variable optical attenuator (VOA) we can control the laser power and adjust it to a level that the same single photon detectors can be used both for polarization compensation and QKD. This significantly reduces the time that would otherwise be needed to switch from single-photon detectors to photodiodes for signal measurement at the output.

In a setup for a predefined photon polarization state, horizontally polarized photons from a classical laser travel to the first beamsplitter where they are randomly reflected or transmitted (Fig. 30). Reflected photons that are traveling through the short path of the setup end up in the horizontal linear state (H state), while the transmitted photons end up in the state of diagonal linear polarization (D state) due to rotation on HWP. This setup (Fig. 33) is similar to the one on the polarization analysis user module (PAM) (Fig. 25). By closing a corresponding pair of shutters on an auxiliary setup and on a PAM, we choose to send photons of either H or D polarization states to the users. As they travel through optical fibers, photons experience perturbations that cause the polarization state of the photons to randomize upon entering the PAM before polarization compensation is implemented.

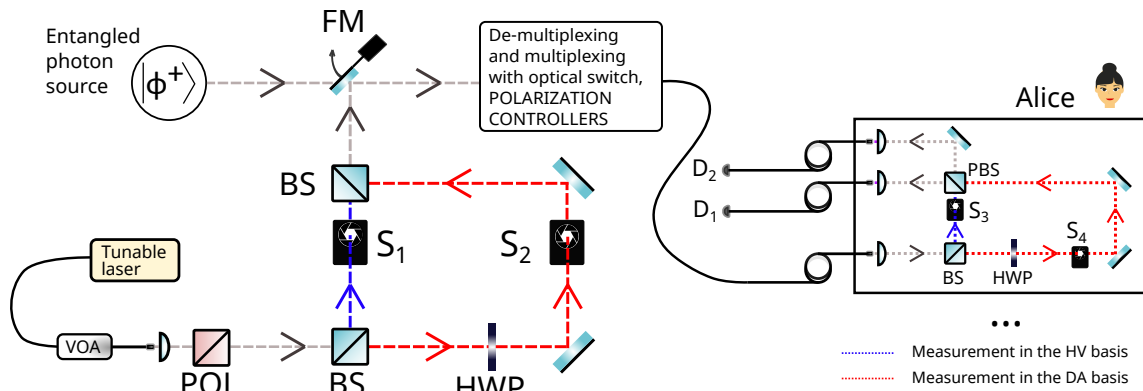


Figure 33. Setup for polarization compensation using predefined photon polarization states [83].

The power of a tunable laser that is entering the setup is controlled with the variable optical attenuator (VOA). The polarization of the photons entering the setup is defined using the polarizer (POL), in our case the Wollaston prism. The flip mirror (FM) is used to switch between the signal from the setup for polarization compensation and the signal from the source of polarization-entangled photon pairs. Mechanical shutters are depicted as  $S_1$ ,  $S_2$ ,  $S_3$  and  $S_4$ , beamsplitters as BS, polarization beamsplitter as PBS, half waveplates as HWP and single-photon detectors as  $D_1$  and  $D_2$ . Solid lines describe optical fibres and dashed lines describe the free-space path of photons.

- **Realization with manual polarization controllers**

As described in the previous subchapter, the polarization compensation process requires sending photons of one of two polarization states (H or D in our setup) and measuring the polarization state received at the PAM. Then, the measurement is performed at the detector corresponding to the orthogonal state in the same basis (we send H and measure in V or send D and measure in A) since it is easier to recognize a minimum of counts rather than a maximum. In order to ensure that the measurement basis always corresponds to the well-defined polarization state that was sent, we use optical shutters in the transmitter setup and at the receiver (PAMs). The shutters are only needed for the polarization compensation steps and both are left open (closed) on the receivers (transmitter) during the QKD protocol. Compensation in one basis is done using manual polarization controllers and is over when the minimum value is observed with the corresponding detector. After compensation in one basis, we send the other polarization state and compensate in this basis. It is necessary to iteratively alternate between both transmitted polarization states until we find a common position of the fibre polarization compensation paddles that results in the lowest values for the V detector (when we send H) and the A detector (when we send D). This iterative procedure is inevitable since photons with predefined polarization in both bases are traveling through the same fiber and are being compensated with the same controller. Even though this method can provide high polarization visibilities and fine adjustments in both bases, it disrupts the operation of the network and is time-consuming. The results of measurements on our network based on the sample of 206 compensations show that it takes 14 min on average per link, with the average entanglement visibility of  $(98.17 \pm 0.04)\%$ .

- **Realization with motorized polarization controllers**

Manual polarization controllers are widely used for polarization compensation but they suffer from limitations induced by human factors. On the other hand, motorized polarization controllers (MPC) offer reproducibility and are easy to use [63, 84]. Therefore, we have implemented twelve MPCs instead of manual polarization controllers in our network (Fig. 34). The algorithm controls MPCs and maximizes entanglement visibility above the wanted threshold (see Appendix 8.6). This approach is very natural in the sense that it follows steps that one would take to compensate polarization using manual polarization controllers. Besides threshold visibility values in each base and the global visibility threshold, the user can define the initial angle and the step size that depends on the value of visibility. It is natural to take larger steps when being far off the optimum value and to refine steps closer to the visibility threshold. The process starts by rotating all three paddles on the MPC and finding the one with the highest impact on the visibility value in one basis. This paddle is then positioned to maximize visibility. If the visibility value reaches the predetermined threshold value in that basis, that paddle is excluded from the next steps. If that condition is not satisfied, the algorithm finds the second paddle with the highest impact. With further rotations of these two paddles, we can get visibility above the threshold value. The polarization compensation process using motorized controllers and the described algorithm results in similar visibility (above 98%) as manual compensation, but this result is achieved faster (8 minutes).

In our experiment, all MPCs start from the same position and move  $10^\circ$ . The threshold values that the algorithm tries to achieve are 95% visibility for the HV base, 98% visibility for the DA basis and 95% for global visibility. If the global visibility is larger than the global threshold visibility, the algorithm stops even though the visibility in one basis might be lower than the threshold value in that basis. The algorithm will run up to four times in each basis before it reduces the threshold value (in that basis) that is trying to achieve for 0.2%. Also, it will try to switch to another basis up to 10 times before it stops if the global threshold is not achieved. Since we have found that other methods are even faster, for further research we recommend combining the best of both worlds - reproducibility and automation of algorithm with MPCs with the possibility of avoiding the disruption of the network (see Subchapter 5.5.3).

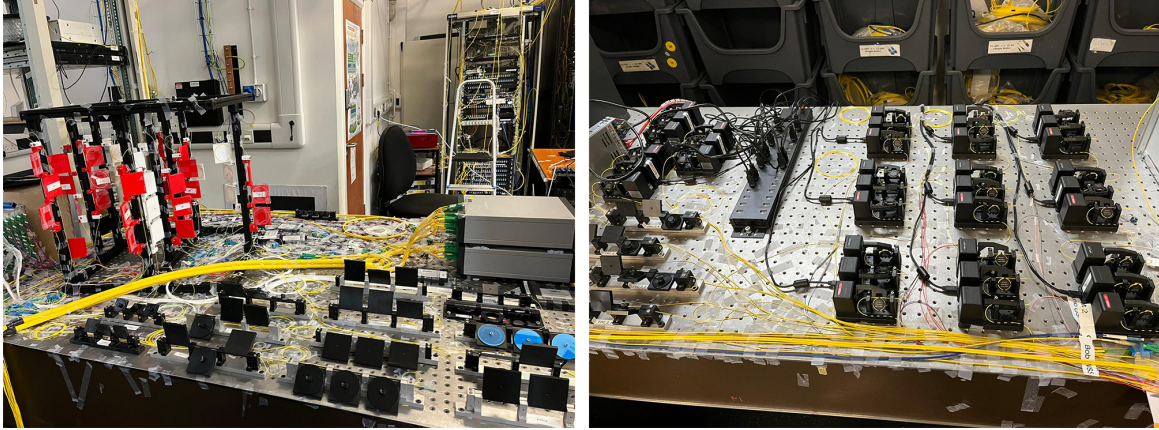


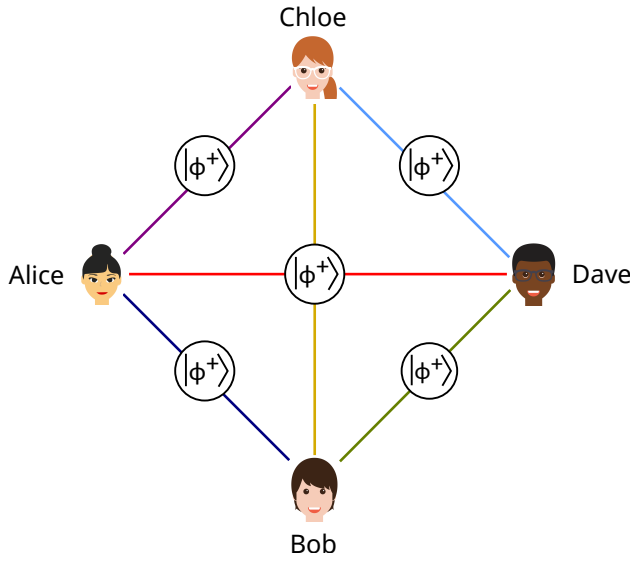
Figure 34. Left: Photography of a part of the experimental setup with manual polarization controllers, Right: Photography of a part of the experimental setup with motorized polarization controllers

- **Realization with simultaneous polarization compensation in both polarization bases - "blinking scheme"**

A major drawback of the previously described realizations is that they require iterative steps in the polarization compensation process. This can be time-consuming since the iterative procedure does not necessarily converge. However, if we find a way to send and receive polarization states from both bases (i.e. H state from HV basis, and D state from DA basis, alternately) for a short time, it could be possible to compensate both bases simultaneously. The aforementioned shutters in an auxiliary setup and on the users' PAMs can be controlled with software to open and close at will. Therefore, we can program them to "blink" - open and close with high frequency. In our experiment, both pairs of shutters were working in a blinking mode with an integration time of 0.3 s per basis. Although faster blinking would give a better average, we noticed that it leads to the mixing of different bases due to imperfect shutter synchronization. Experimentally, we noticed this effect by achieving lower maximum polarization visibility compared to the realization with manual controllers. "Blinking scheme" also requires downtime of the network, but it is much faster than the manual realization. Compensation done on 24 links shows an average polarization visibility value of  $(97.6 \pm 0.2)\%$  in 6 minutes per link on average. Using shutters in a blinking mode, the network's downtime is reduced by more than half with a similar level of performance compared with the previously described manual realization.

### 5.5.2 Minimization of QBER

Recent experiments with two users have shown that QBER can also be used in the polarization compensation process [67, 85, 86]. For entanglement-based QKD protocols, QBER below 11% is required to ensure a positive secret key rate. Unlike the previous method where we measured entanglement visibility as a measure of how well we compensated disturbances in a polarization state, here we look directly at QBER during the process of key exchange and minimize it for links between users and not for each individual fiber connecting users to the source. This corresponds to the situation depicted on the left side of Fig. 35 where effectively each pair of users shares their own source of polarization-entangled photon pairs on a specific wavelength. For this method to work, it is crucial to first find delays between users. This can be done by looking at  $g(2)$  histograms and the delays between central peaks (Fig. 26). After finding the delay between a pair of users, QBER is calculated from a temporal cross-correlation histogram. While monitoring its live value, QBER is minimized using manual controllers. However, we note that it is impossible to have continuous monitoring of compensation since the signal cannot be used for compensation and key generation simultaneously. The polarization compensation was done on 13 links that show an average QBER of  $(3.4 \pm 0.4)\%$  in 2 min on average per link. Unlike previously described realizations, it is significant that the minimization of QBER can be conducted while the network is active. Another advantage is that each new user needs to compensate only the fibres that are connecting him/her to the source, leaving the rest of the network intact.



	Bob	Chloe	Dave
Alice	CH 33 CH 35	CH 32 CH 36	CH 31 CH 37
Bob		CH 30 CH 38	CH 29 CH 39
Chloe			CH 40 CH 28

Figure 35. QBER minimization scheme effectively corresponds to having a source that produces entangled photon pairs at wavelengths corresponding to ITU channels shown in the table between each pair of users. The colors in the table represent different photon pairs that are distributed among the users, while channel numbers correspond to wavelengths symmetrically distributed around the central wavelength of 1550.12 nm (corresponding to channel 34). Taken from [83].

### 5.5.3 Advantages and drawbacks of polarization compensation methods

As described in the previous subchapters, we have successfully applied different realizations of polarization compensation methods on a four-user full-mesh quantum network. However, we note that some of them have certain advantages and/or drawbacks that we discuss in this subchapter.

The advantages that QBER minimization method shows could be a real game-changer when it comes to scaling quantum networks to a high number of users. All methods except QBER minimization require  $2k$  FPCs for  $k$  links. Since every  $n$ -th new user in a full-mesh network based on multiplexing needs to establish  $2(n - 1)$  new links, it is important to use an appropriate method to avoid the unnecessarily large number of links and FPCs (Fig. 36).



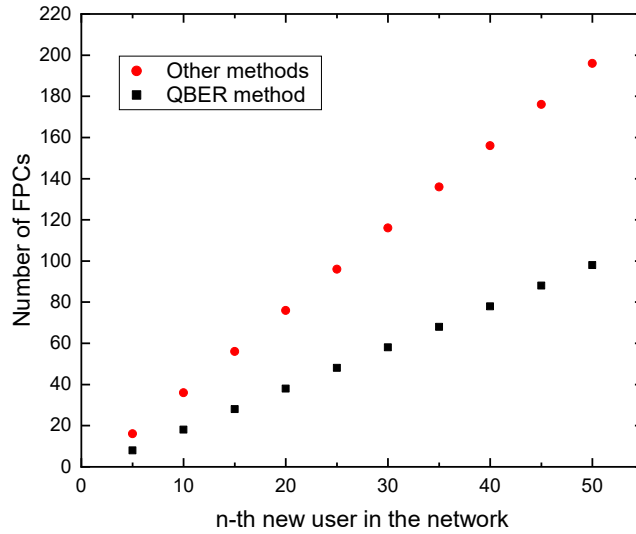














Figure 36. Number of additional FPCs needed for polarization compensation when adding the n-th user

Despite the advantages of the QBER-based method, we note that it requires a high-fidelity state from the entangled photon pair source, as well as a high coincidence rate. If the fidelity of the state needs to be adjusted, it is necessary to have at least two users sharing one link whose fibres have previously been compensated by some other method. If the coincidence rate is low, the process will be slower since it will take more time to obtain a useful QBER value.

As presented in Table 6, there is no real difference in polarization visibility after the compensation process between manual fibre polarization compensation and motorized polarization controllers. The main differences are the time needed for the process to be completed and the contribution to QBER due to compensation. In this case, motorized controllers perform better since they have fast-moving paddles and high threshold values for polarization visibilities to achieve. The main limitations when working with motorized controllers are rotation speed and the readout time of the detector counts. Further work could explore possibilities of implementation of machine learning algorithms in the QBER method or combining motorized controllers with the QBER method. This could further reduce the time required for the polarization compensation process and automate it. Also, different technical realizations of the presented methods could be analyzed (faster electronics, different shutter realization). Table 6 presents a summary of the evaluated polarization compensation methods with the measurement results.

Table 6. Summary of polarization compensation methods. Taken from [83].

Method	Canonical with an auxiliary laser			Minimization of QBER
Realization	Manual fibre polarization controllers	Motorized polarization controllers	„Blinking scheme“ using mechanical shutters	Compensation done on one fibre connecting pair of users
FPCs needed for $k$ links	$2k$	$2k$	$2k$	$k$
Does <b>not</b> disrupt the <b>whole</b> network				
Calibration signal <b>not</b> needed				
Active change of bases <b>not</b> needed				
$\bar{t}$ (per link)	~ 14 min	~ 8 min	~ 6 min	~ 2 min
Polarization visibility after compensation	$(98.17 \pm 0.04)\%$	$(98.4 \pm 0.2)\%$	$(97.6 \pm 0.2)\%$	not applicable
Entanglement fidelity	93.3% (estimated*)	93.5% (estimated*)	92.7% (estimated*)	$(93.2 \pm 0.8)\%$ (measured)
Calculated contribution to QBER due to polarization compensation	$(0.91 \pm 0.02)\%$	$(0.77 \pm 0.03)\%$	$(1.18 \pm 0.08)\%$	0.05% (estimated*)
Measured QBER	ranging from 2.7% to 4.0%**	not measured	not measured	$(3.4 \pm 0.4)\%$

\* Estimated including 3.35% (average of measured QBERs during calibration measurements) net QBER contribution (i.e. 93.3% entanglement fidelity contribution) from entangled photon pair source, user modules, timing jitter, detectors and polarization compensation

\*\* The actual experimentally measured value depends on the properties of the network link and thus there is a nearly uniform spread of QBER values between the extremes quoted

## 6 Conclusions and outlook

In this work I presented the results of my research on quantum communication with two types of polarization-entangled photon sources. We have demonstrated that the type-II source can be used for an interface between free-space and in-fiber quantum communication, while a broadband type-0 source can be used to connect multiple users in full-mesh quantum networks. We have addressed some of the challenges that arise with the implementation of QKD between two users and multiple users connected in a network. These challenges include polarization drift, which limits the key rate, security threats posed by trusted nodes, and limitations on the dynamics of the network for wavelength-multiplexed based networks. We have experimentally demonstrated solutions to these problems on quantum networks with four and six users (with one metropolitan link). This includes successful demonstration of dynamic scenarios of adding and removing users in the network with six users. These steps are crucial in the development and management of interconnected quantum networks. Our network shows a long-term stability of key rates up to 7 days. They are resilient to interruptions during the operation caused by the cycling of SNSPDs or power losses. Based on our findings, we can use the source in the process of polarization compensation, which ultimately reduces the overall cost and experimental complexity. By optimizing pump power, reducing detector jitter, and implementing better optical elements on polarization analysis modules, we can achieve even lower QBER values. These improvements could have a significant impact on the efficiency and success of future experiments. To the best of our knowledge, the method of polarization compensation with minimization of quantum bit error rate (QBER) is the first realization of polarization compensation on an active quantum network. This is an important breakthrough as it allows central network management to maintain a key rate above the wanted threshold value without disrupting communication between users. In addition, this method does not require an auxiliary classical laser, it is easily scalable to a large number of users and the compensation can be done in just a couple of minutes. We have also implemented other methods, demonstrating a simple algorithm for motorized polarization controllers and the usage of mechanical shutters that eliminate manual steps of changing the emitted and measured states in the “blinking scheme”. Future work could focus on the automation of motorized

polarization controllers and their implementation in the QBER method. Quantum Internet will require interconnectivity of networks different in terms of the number of users, technology used and performances. It will be inevitable to develop quantum repeaters based on entanglement swapping and quantum teleportation (Appendix). We believe that the results presented in this thesis will pave the way for more secure and reliable methods of communication with the development of complex interconnected quantum networks.

## 7 Bibliography

- [1] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.
- [2] Albert Einstein, Boris Podolsky, and Nathan Rosen. “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review* 47 (1935), pp. 777–780. URL: <https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777>.
- [3] J. S. Bell. “On the Einstein Podolsky Rosen paradox”. *Physics Physique Fizika* 1 (1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: <https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195>.
- [4] Stuart J. Freedman and John F. Clauser. “Experimental Test of Local Hidden-Variable Theories”. *Phys. Rev. Lett.* 28 (1972), pp. 938–941. DOI: 10.1103/PhysRevLett.28.938. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.28.938>.
- [5] C.H. Bennet and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. *Proceedings of the International Conference on Computers, Systems & Signal Processing* 1 (1984), pp. 175–179. DOI: 10.48550/arXiv.2003.06557.
- [6] Max Planck. “Vorlesungen über die Theorie der Wärmestrahlung” (1906).
- [7] Max Planck. “Ueber das Gesetz der Energieverteilung im Normalspectrum”. *Annalen der Physik* 309.3 (1901), pp. 553–563. DOI: <https://doi.org/10.1002/andp.19013090310>. eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/andp.19013090310>. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19013090310>.
- [8] Albert Einstein. “Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt”. *Annalen der Physik* 17 (1905), p. 132.
- [9] Arthur H. Compton. “A Quantum Theory of the Scattering of X-rays by Light Elements”. *Phys. Rev.* 21 (1923), pp. 483–502. DOI: 10.1103/PhysRev.21.483. URL: <https://link.aps.org/doi/10.1103/PhysRev.21.483>.

- [10] Lewis N. Gilbert. “The Conservation of Photons”. *Nature* 118 (1926), pp. 874–875.
- [11] Dirac Paul. “The quantum theory of the emission and absorption of radiation”. *Proceedings of the Royal Society A* 114 (1927), pp. 243–265. DOI: 10.1098/rspa.1927.0039.
- [12] Andrew Steane. “Quantum computing”. *Reports on Progress in Physics* 61.2 (1998), p. 117. DOI: 10.1088/0034-4885/61/2/002. URL: <https://dx.doi.org/10.1088/0034-4885/61/2/002>.
- [13] J.G. Rarity, P.C.M. Owens, and P.R. Tapster. “Quantum Random-number Generation and Key Sharing”. *Journal of Modern Optics* 41.12 (1994), pp. 2435–2444. DOI: 10.1080/09500349414552281. eprint: <https://doi.org/10.1080/09500349414552281>. URL: <https://doi.org/10.1080/09500349414552281>.
- [14] André Stefanov et al. “Optical quantum random number generator”. *Journal of Modern Optics* 47.4 (2000), pp. 595–598. DOI: 10.1080/09500340008233380. eprint: <https://doi.org/10.1080/09500340008233380>. URL: <https://doi.org/10.1080/09500340008233380>.
- [15] T. J. McIlrath et al. “Two-photon lidar technique for remote sensing of atomic oxygen”. *Appl. Opt.* 18.3 (1979), pp. 316–319. DOI: 10.1364/AO.18.000316. URL: <https://opg.optica.org/ao/abstract.cfm?URI=ao-18-3-316>.
- [16] I. Rech et al. “Photon-timing detector module for single-molecule spectroscopy with 60-ps resolution”. *IEEE Journal of Selected Topics in Quantum Electronics* 10.4 (2004), pp. 788–795. DOI: 10.1109/JSTQE.2004.833975.
- [17] Ali Anwar et al. “Entangled photon-pair sources based on three-wave mixing in bulk crystals”. *Review of Scientific Instruments* 92.4 (2021), p. 041101. ISSN: 0034-6748. DOI: 10.1063/5.0023103. URL: <https://doi.org/10.1063/5.0023103>.
- [18] Wolfgang Demtröder. “Laser spectroscopy” (2003), p. 987. DOI: 10.1007/978-3-662-05155-9.
- [19] James Schneeloch et al. “Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion”. *Journal of Optics* 21.4

- (2019), p. 043501. DOI: 10.1088/2040-8986/ab05a8. URL: <https://dx.doi.org/10.1088/2040-8986/ab05a8>.
- [20] F Laudenbach et al. “Modelling parametric down-conversion yielding spectrally pure photon pairs”. *Opt. Express* 24 (2016), pp. 2712–2727. DOI: 10.1103/PhysRevA.71.050302. URL: <https://link.aps.org/doi/10.1103/PhysRevA.71.050302>.
- [21] A. Deepthy M. N. Satyanarayan and H. L. Bhat. “Potassium Titanyl Phosphate and Its Isomorphs: Growth, Properties, and Applications”. *Critical Reviews in Solid State and Materials Sciences* 24.2 (1999), pp. 103–191. DOI: 10.1080/10408439991329189.
- [22] BS Cirelson. “Quantum generalizations of Bell’s inequality”. *Letters in Mathematical Physics* 4 (1980). DOI: 10.1007/BF00417500. URL: <https://doi.org/10.1007/BF00417500>.
- [23] *The nobel prize in physics 2022*. URL: <https://www.nobelprize.org/prizes/physics/2022/press-release/>.
- [24] John F. Clauser et al. “Proposed Experiment to Test Local Hidden-Variable Theories”. *Phys. Rev. Lett.* 23 (1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>.
- [25] Alain Aspect, Philippe Grangier, and Gérard Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities”. *Phys. Rev. Lett.* 49 (1982), pp. 91–94. DOI: 10.1103/PhysRevLett.49.91. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.49.91>.
- [26] Alain Aspect, Jean Dalibard, and Gérard Roger. “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers”. *Phys. Rev. Lett.* 49 (1982), pp. 1804–1807. DOI: 10.1103/PhysRevLett.49.1804. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.49.1804>.
- [27] Alain Aspect. “Proposed experiment to test the nonseparability of quantum mechanics”. *Phys. Rev. D* 14 (1976), pp. 1944–1951. DOI: 10.1103/PhysRevD.14.1944. URL: <https://link.aps.org/doi/10.1103/PhysRevD.14.1944>.

- [28] Dik Bouwmeester et al. “Experimental quantum teleportation”. 390 (6660 1997), pp. 575–579. DOI: 10.1038/37539. URL: <https://doi.org/10.1038/37539>.
- [29] D. Gammon et al. “Fine Structure Splitting in the Optical Spectra of Single GaAs Quantum Dots”. *Phys. Rev. Lett.* 76 (1996), pp. 3005–3008. DOI: 10.1103/PhysRevLett.76.3005. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.76.3005>.
- [30] Charles Santori et al. “Triggered Single Photons from a Quantum Dot”. *Phys. Rev. Lett.* 86 (2001), pp. 1502–1505. DOI: 10.1103/PhysRevLett.86.1502. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.86.1502>.
- [31] A. Gruber et al. “Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers”. *Science* 276.5321 (1997), pp. 2012–2014. DOI: 10.1126/science.276.5321.2012. eprint: <https://www.science.org/doi/pdf/10.1126/science.276.5321.2012>. URL: <https://www.science.org/doi/abs/10.1126/science.276.5321.2012>.
- [32] Tian Zhong et al. “High-quality fiber-optic polarization entanglement distribution at 1.3 $\mu$ m telecom wavelength”. *Opt. Lett.* 35.9 (2010), pp. 1392–1394. DOI: 10.1364/OL.35.001392. URL: <http://opg.optica.org/ol/abstract.cfm?URI=ol-35-9-1392>.
- [33] Charles H. Bennett et al. “Experimental quantum cryptography”. *Journal of Cryptology* 5 (1992). DOI: 10.1007/BF00191318. URL: <https://doi.org/10.1007/BF00191318>.
- [34] Paul G. Kwiat et al. “New High-Intensity Source of Polarization-Entangled Photon Pairs”. *Physical Review Letters* 75.24 (1995), pp. 4337–4341. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.75.4337. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.75.4337>.
- [35] Andrej Dujella and Marcel Maretić. *Kriptografija*. Element, 2007, p. 270. ISBN: 978-953-197-565-0.
- [36] Naomi R. Solomons et al. “Scalable Authentication and Optimal Flooding in a Quantum Network”. *PRX Quantum* 3 (2022), p. 020311. DOI: 10.1103/



PRXQuantum.3.020311. URL: <https://link.aps.org/doi/10.1103/PRXQuantum.3.020311>.

- [37] A Muller, H Zbinden, and N Gisin. “Quantum cryptography over 23 km in installed under-lake telecom fibre”. *Europhysics Letters (EPL)* 33.5 (1996), pp. 335–340. DOI: 10.1209/epl/i1996-00343-4. URL: <https://doi.org/10.1209/epl/i1996-00343-4>.
- [38] A Muller, J Breguet, and N Gisin. “Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km”. *Europhysics Letters (EPL)* 23.6 (1993), pp. 383–388. DOI: 10.1209/0295-5075/23/6/001. URL: <https://doi.org/10.1209/0295-5075/23/6/001>.
- [39] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. *Phys. Rev. Lett.* 85 (2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.85.441>.
- [40] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. *Phys. Rev. Lett.* 67 (1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>.
- [41] Charles H. Bennett, Gilles Brassard, and N. David Mermin. “Quantum cryptography without Bell’s theorem”. *Physical Review Letters* 68.5 (1992), pp. 557–559. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.68.557. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.68.557>.
- [42] Sören Wengerowsky et al. “An entanglement-based wavelength-multiplexed quantum communication network”. *Nature* 564.7735 (2018), pp. 225–228. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/s41586-018-0766-y. URL: <http://www.nature.com/articles/s41586-018-0766-y>.
- [43] Siddarth Koduru Joshi et al. “A trusted-node-free eight-user metropolitan quantum communication network”. *Science Advances* 6.36 (2020). arXiv: 1907.08229, eaba0959. ISSN: 2375-2548. DOI: 10.1126/sciadv.aba0959. URL: <http://arxiv.org/abs/1907.08229>.

- [44] Erik Fitzke et al. “Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding”. *PRX Quantum* 3 (2022), p. 020341. DOI: 10.1103/PRXQuantum.3.020341. URL: <https://link.aps.org/doi/10.1103/PRXQuantum.3.020341>.
- [45] Peter Schartner and Stefan Rass. “How to overcome the ‘Trusted Node Model’ in Quantum Cryptography” (2009), pp. 259–262. DOI: 10.1109/CSE.2009.171.
- [46] M Peev et al. “The SECOQC quantum key distribution network in Vienna”. *New Journal of Physics* 11.7 (2009), p. 075001. DOI: 10.1088/1367-2630/11/7/075001. URL: <https://doi.org/10.1088/1367-2630/11/7/075001>.
- [47] D Stucki et al. “Long-term performance of the SwissQuantum quantum key distribution network in a field environment”. *New Journal of Physics* 13.12 (2011), p. 123001. DOI: 10.1088/1367-2630/13/12/123001. URL: <https://doi.org/10.1088/1367-2630/13/12/123001>.
- [48] M. Sasaki, Fujiwara M., and Ishizuka H. et al. “Field test of quantum key distribution in the Tokyo QKD Network”. *Opt. Express* 19.11 (2011), pp. 10387–10409. DOI: 10.1364/OE.19.010387. URL: <http://opg.optica.org/oe/abstract.cfm?URI=oe-19-11-10387>.
- [49] TY Chen, X Jiang, and SB et al Tang. “Implementation of a 46-node quantum metropolitan area network”. *NPJ Quantum Inf* 7 (2021). DOI: 10.1038/s41534-021-00474-3.
- [50] Bernd Fröhlich et al. “A quantum access network”. *Nature* 501 (2013), pp. 69–72. DOI: 10.1038/nature12493.
- [51] Yan-Lin Tang et al. “Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network”. *Phys. Rev. X* 6 (2016), p. 011024. DOI: 10.1103/PhysRevX.6.011024. URL: <https://link.aps.org/doi/10.1103/PhysRevX.6.011024>.
- [52] C Elliott. “The DARPA Quantum Network”. *Quantum Communications and Cryptography*. Ed. by Alexander Sergienko. Vol. 20052673. Series Title: Optical Science and Engineering. CRC Press, 2006, pp. 83–102.

- [53] Teng-Yun Chen et al. “Metropolitan all-pass and inter-city quantum communication network”. *Opt. Express* 18.26 (2010), pp. 27217–27225. DOI: 10.1364/OE.18.027217. URL: <http://opg.optica.org/oe/abstract.cfm?URI=oe-18-26-27217>.
- [54] Matej Pivoluska, Marcus Huber, and Mehul Malik. “Layered quantum key distribution”. *Phys. Rev. A* 97 (2018), p. 032312. DOI: 10.1103/PhysRevA.97.032312. URL: <https://link.aps.org/doi/10.1103/PhysRevA.97.032312>.
- [55] G. N. Gol’tsman et al. “Picosecond superconducting single-photon optical detector”. *Applied Physics Letters* 79.6 (2001), pp. 705–707. DOI: 10.1063/1.1388868. eprint: <https://doi.org/10.1063/1.1388868>. URL: <https://doi.org/10.1063/1.1388868>.
- [56] Alex D. Semenov, Gregory N. Gol’tsman, and Alexander A. Korneev. “Quantum detection by current carrying superconducting film”. *Physica C: Superconductivity* 351.4 (2001), pp. 349–356. ISSN: 0921-4534. DOI: [https://doi.org/10.1016/S0921-4534\(00\)01637-3](https://doi.org/10.1016/S0921-4534(00)01637-3). URL: <https://www.sciencedirect.com/science/article/pii/S0921453400016373>.
- [57] Iman Esmaeil Zadeh et al. “Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution”. *APL Photonics* 2.11 (2017), p. 111301. DOI: 10.1063/1.5000001. URL: <https://doi.org/10.1063/1.5000001>.
- [58] E. E. Wollman et al. “UV superconducting nanowire single-photon detectors with high efficiency, low noise, and 4 K operating temperature”. *Opt. Express* 25.22 (2017), pp. 26792–26801. DOI: 10.1364/OE.25.026792. URL: <https://opg.optica.org/oe/abstract.cfm?URI=oe-25-22-26792>.
- [59] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. “Superconducting nanowire single-photon detectors: physics and applications”. *Superconductor Science and Technology* 25.6 (2012), p. 063001. ISSN: 0953-2048, 1361-6668. DOI: 10.1088/0953-2048/25/6/063001. URL: <https://iopscience.iop.org/article/10.1088/0953-2048/25/6/063001>.
- [60] Alexander Ling, Antia Lamas-Linares, and Christian Kurtsiefer. “Absolute emission rates of spontaneous parametric down-conversion into single transverse

- Gaussian modes”. *Phys. Rev. A* 77 (4 2008), p. 043834. DOI: 10.1103/PhysRevA.77.043834. URL: <https://link.aps.org/doi/10.1103/PhysRevA.77.043834>.
- [61] Sang Min Lee et al. “Polarization-entangled photon-pair source obtained via type-II non-collinear SPDC process with PPKTP crystal”. *Opt. Express* 24.3 (2016), pp. 2941–2953. DOI: 10.1364/OE.24.002941. URL: <https://opg.optica.org/oe/abstract.cfm?URI=oe-24-3-2941>.
- [62] Zhen-Sheng Yuan et al. “Entangled photons and quantum communication”. *Physics Reports* 497.1 (2010), pp. 1–40. ISSN: 03701573. DOI: 10.1016/j.physrep.2010.07.004. URL: <https://linkinghub.elsevier.com/retrieve/pii/S0370157310001833>.
- [63] Nicolas Gisin et al. “Quantum cryptography”. *Reviews of Modern Physics* 74.1 (2002), pp. 145–195. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.74.145. URL: <https://link.aps.org/doi/10.1103/RevModPhys.74.145>.
- [64] Juan Yin et al. “Entanglement-based secure quantum cryptography over 1,120 kilometres”. *Nature* 582.7813 (2020), pp. 501–505. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/s41586-020-2401-y. URL: <http://www.nature.com/articles/s41586-020-2401-y>.
- [65] Sören Wengerowsky et al. “Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre”. *npj Quantum Information* 6.1 (2020). arXiv: 1907.04864, p. 5. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0238-8. URL: <http://arxiv.org/abs/1907.04864>.
- [66] Catherine Holloway et al. “Quantum entanglement distribution with 810 nm photons through active telecommunication fibers”. *Optics Express* 19.21 (2011). arXiv: 1109.2519, p. 20597. ISSN: 1094-4087. DOI: 10.1364/OE.19.020597. URL: <http://arxiv.org/abs/1109.2519>.
- [67] Yicheng Shi et al. “Fibre polarization state compensation in entanglement-based quantum key distribution”. *Optics Express* 29.23 (2021). arXiv: 2107.07654, p. 37075. ISSN: 1094-4087. DOI: 10.1364/OE.437896. URL: <http://arxiv.org/abs/2107.07654>.

- [68] Taehyun Kim, Marco Fiorentino, and Franco N. C. Wong. “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”. *Physical Review A* 73.1 (2006). arXiv: quant-ph/0509219, p. 012316. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.73.012316. URL: <http://arxiv.org/abs/quant-ph/0509219>.
- [69] Murat Uysal, ed. *Optical Wireless Communications - An Emerging Technology*. Springer Cham, 2016. ISBN: 978-3-319-30200-3. DOI: 10.1007/978-3-319-30201-0\_27. URL: <https://link.springer.com/book/10.1007/978-3-319-30201-0>.
- [70] Evan Meyer-Scott et al. “Quantum entanglement distribution with 810 nm photons through telecom fibers”. *Applied Physics Letters* 97.3 (2010). arXiv: 1007.4495, p. 031117. ISSN: 0003-6951, 1077-3118. DOI: 10.1063/1.3460920. URL: <http://arxiv.org/abs/1007.4495>.
- [71] Daniel Gottesman et al. “Security of quantum key distribution with imperfect devices”. *Quant.Inf.Comput.* 5 (2004), pp. 325–360. DOI: 10.48550/arXiv.quant-ph/0212066.
- [72] G. Bebrov. “On the (relation between) efficiency and secret key rate of QKD”. *Scientific Reports* 14 (2024). DOI: 10.1038/s41598-024-54246-y.
- [73] Gösta Fürnkranz. *The Quantum Internet*. en. Cham: Springer Cham, 2020. ISBN: 978-3-030-42664-4. DOI: 10.1007/978-3-030-42664-4. URL: <https://link.springer.com/book/10.1007/978-3-030-42664-4>.
- [74] Masahide Sasaki. “Quantum networks: where should we be heading?” *Quantum Science and Technology* 2.2 (2017), p. 020501. DOI: 10.1088/2058-9565/aa6994. URL: <https://dx.doi.org/10.1088/2058-9565/aa6994>.
- [75] Gilles Brassard et al. “Entanglement and Wavelength Division Multiplexing for Quantum Cryptography Networks”. *AIP Conference Proceedings* 734.1 (2004), pp. 323–326. ISSN: 0094-243X. DOI: 10.1063/1.1834445. eprint: [https://pubs.aip.org/aip/acp/article-pdf/734/1/323/12204693/323\1\\\_online.pdf](https://pubs.aip.org/aip/acp/article-pdf/734/1/323/12204693/323\1\_online.pdf). URL: <https://doi.org/10.1063/1.1834445>.

- [76] Muneer Alshowkan et al. “Reconfigurable Quantum Local Area Network Over Deployed Fiber”. *PRX Quantum* 2 (2021), p. 040304. DOI: 10.1103/PRXQuantum.2.040304. URL: <https://link.aps.org/doi/10.1103/PRXQuantum.2.040304>.
- [77] WJ Munro et al. “From quantum multiplexing to high-performance quantum networking”. *Nature Photon* 4 (2010), pp. 792–796. DOI: 10.1038/nphoton.2010.213.
- [78] Obada Alia et al. “DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre”. *J. Lightwave Technol.* 40.16 (2022), pp. 5522–5529. URL: <https://opg.optica.org/jlt/abstract.cfm?URI=jlt-40-16-5522>.
- [79] M.J. Clark et al. “Polarisation Based Entanglement Distribution Quantum Networking”. *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*. 2023, pp. 271–274. DOI: 10.23919/MIPRO57284.2023.10159792.
- [80] Wenjun Wen et al. “Realizing an Entanglement-Based Multiuser Quantum Network with Integrated Photonics”. *Phys. Rev. Applied* 18 (2022), p. 024059. DOI: 10.1103/PhysRevApplied.18.024059. URL: <https://link.aps.org/doi/10.1103/PhysRevApplied.18.024059>.
- [81] Rui Wang et al. “A Dynamic Multi-Protocol Entanglement Distribution Quantum Network”. *Optical Fiber Communications Conference and Exhibition (OFC)* (2022), pp. 1–3.
- [82] Rui Wang et al. “Optimum Switching Scenario Analysis in a Dynamic Entanglement Network”. *Optical Fiber Communication Conference and Exposition* (2023).
- [83] Matej Peranić et al. “A study of polarization compensation for quantum networks”. *EPJ Quantum Technologies* 10 (2023). DOI: 10.1140/epjqt/s40507-023-00187-w.
- [84] C. Gobby, Z. L. Yuan, and A. J. Shields. “Quantum key distribution over 122 km of standard telecom fiber”. *Applied Physics Letters* 84.19 (2004), pp. 3762–3764. ISSN: 0003-6951, 1077-3118. DOI: 10.1063/1.1738173. URL: <http://aip.scitation.org/doi/10.1063/1.1738173>.

- [85] Yu-Yang Ding et al. “Polarization basis tracking scheme for quantum key distribution with revealed sifted key bits”. *Optics Letters* 42.6 (2017). arXiv: 1608.00366, p. 1023. ISSN: 0146-9592, 1539-4794. DOI: 10.1364/OL.42.001023. URL: <http://arxiv.org/abs/1608.00366>.
- [86] Sebastian Philipp Neumann et al. “Continuous entanglement distribution over a transnational 248 km fibre link”. *Nature Communications* 13.6134 (2022). ISSN: 2041-1723. DOI: 10.1038/s41467-022-33919-0. URL: <https://www.nature.com/articles/s41467-022-33919-0#citeas>.
- [87] H de Riedmatten et al. “Long-distance entanglement swapping with photons from separated sources”. *Phys. Rev. A* 71 (2005), p. 050302. DOI: 10.1103/PhysRevA.71.050302. URL: <https://link.aps.org/doi/10.1103/PhysRevA.71.050302>.

## 8 Appendix

### 8.1 Quantization of electromagnetic field

The electromagnetic field consists of two time-dependent vector fields, an electric field  $\mathbf{E}(\mathbf{r},t)$  and a magnetic field  $\mathbf{B}(\mathbf{r},t)$ . The most convenient way to make quantization of the EM field is to start from the classical Maxwell's equations in free space and in the absence of sources:

$$\nabla \cdot \mathbf{E} = 0 \quad (8.1)$$

$$\nabla \cdot \mathbf{B} = 0 \quad (8.2)$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \quad (8.3)$$

$$\nabla \times \mathbf{B} = \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t} \quad (8.4)$$

where  $\mu_0$  is magnetic permeability and  $\epsilon_0$  is electric permittivity.

Both the electric and magnetic field can be calculated from the vector potential  $\mathbf{A}$  and the scalar potential  $U$  thanks to the relations:

$$\mathbf{E} = -\nabla U - \frac{\partial \mathbf{A}}{\partial t} \quad (8.5)$$

$$\mathbf{B} = \nabla \times \mathbf{A} \quad (8.6)$$

Considering equations 8.5 and 8.6 we can notice that equations 8.2 and 8.3 are automatically satisfied, whereas equations 8.1 and 8.4 become:

$$\nabla \cdot \left( -\nabla U - \frac{\partial \mathbf{A}}{\partial t} \right) = 0 \quad (8.7)$$

$$\nabla \times (\nabla \times \mathbf{A}) = \mu_0 \epsilon_0 \frac{\partial}{\partial t} \left( -\nabla U - \frac{\partial \mathbf{A}}{\partial t} \right) \quad (8.8)$$



Since different scalar and vector potentials can lead to the same fields, we have to add an extra constraint. In this case where there are no sources, and since scalar potential is a function of the spatial charge distribution, we can choose:

$$U = 0 \quad (8.9)$$

On the other hand, for vector potential we can use the so-called Coulomb gauge:

$$\nabla \cdot \mathbf{A} = 0 \quad (8.10)$$

Then, equation 8.5 becomes:

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t} \quad (8.11)$$

which satisfies equation 8.1. On the other hand, equation 8.8 becomes:

$$\left( \nabla^2 - \frac{1}{c^2} \frac{\partial^2}{\partial t^2} \right) \mathbf{A} = 0 \quad (8.12)$$

where

$$c = \frac{1}{\sqrt{\epsilon_0 \mu_0}} \quad (8.13)$$

is the vacuum speed of light. Equation 8.12 shows us that the vector potential  $\mathbf{A}$  satisfies the classical wave equation. Spatial and temporal part of the vector potential can be separated where vector spatial modes are defined as:

$$\nabla^2 \mathbf{u}_{k,\alpha}(\mathbf{r}) = -k^2 \mathbf{u}_{k,\alpha}(\mathbf{r}) \quad (8.14)$$

and  $\mathbf{k}$  is a wave propagation vector while  $\alpha = 1, 2$  are indexes describing polarization. Vector potential can be written as:

$$\mathbf{A}(\mathbf{r}, t) = \sum_{k,\alpha} q_{k,\alpha}(t) \mathbf{u}_{k,\alpha}(\mathbf{r}) \quad (8.15)$$

where  $q_{k,\alpha}$  are time depending amplitudes. Then equation 8.12 becomes:

$$\ddot{q}_{k,\alpha} = -\omega_k^2 q_{k,\alpha} \quad (8.16)$$

This result shows that each mode of the EM field can be considered as harmonic oscillator. The Hamiltonian for each mode is:

$$H_{k,\alpha} = \frac{1}{2}m\omega^2 q_{k,\alpha}^2 + \frac{1}{2m}p_{k,\alpha}^2 \quad (8.17)$$

In order to accomplish the quantization of the electromagnetic field, it is required to replace complex numbers  $q_{k,\alpha}$  and  $p_{k,\alpha}$  with operators  $\hat{q}_{k,\alpha}$  and  $\hat{p}_{k,\alpha}$ . Those operators have to satisfy commutation relation  $[\hat{q}_{k,\alpha}, \hat{p}_{k,\alpha}] = i\hbar$ . Also, we can use creation ( $\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle$ ) and annihilation ( $\hat{a} |n\rangle = \sqrt{n} |n-1\rangle$ ) operators introduced in the second quantization formalism to write the final form of vector potential:

$$\hat{\mathbf{A}}(\mathbf{r}, t) = \sum_{k,\alpha} \sqrt{\frac{\hbar}{2\omega_k \epsilon_0}} (\hat{a}_{k,\alpha} \mathbf{u}_{k,\alpha}(\mathbf{r}) e^{-i\omega_k t} + \hat{a}_{k,\alpha}^\dagger \mathbf{u}_{k,\alpha}^*(\mathbf{r}) e^{i\omega_k t}) \quad (8.18)$$

The electric and magnetic field can be calculated using equations (8.11) and (8.6) respectively:

$$\hat{\mathbf{E}}(\mathbf{r}, t) = i \sum_{k,\alpha} \sqrt{\frac{\hbar\omega_k}{2\epsilon_0}} (\hat{a}_{k,\alpha} \mathbf{u}_{k,\alpha}(\mathbf{r}) e^{-i\omega_k t} - \hat{a}_{k,\alpha}^\dagger \mathbf{u}_{k,\alpha}^*(\mathbf{r}) e^{i\omega_k t}) \quad (8.19)$$

$$\hat{\mathbf{B}}(\mathbf{r}, t) = i \sum_{k,\alpha} \sqrt{\frac{\hbar k}{2c l^3 \epsilon_0}} (\hat{a}_{k,\alpha} e^{i(\mathbf{k}\cdot\mathbf{r} - \omega_k t)} - \hat{a}_{k,\alpha}^\dagger e^{i(\mathbf{k}\cdot\mathbf{r} - \omega_k t)}) \mathbf{k} \times \mathbf{e}_\alpha \quad (8.20)$$

The Hamiltonian can be calculated from the classical expression of the energy for the electromagnetic field in a resonator:

$$H = \frac{1}{2} \int d^3r \left( \epsilon_0 \mathbf{E}^2 + \frac{1}{\mu_0} \mathbf{B}^2 \right) \quad (8.21)$$

which gives us:

$$\hat{H} = \sum_{k,\alpha} \hbar\omega_k \left( \hat{a}_{k,\alpha}^\dagger \hat{a}_{k,\alpha} + \frac{1}{2} \right) \quad (8.22)$$

## 8.2 No-cloning theorem

The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state while maintaining the original state by unitary transformation.

To prove that, suppose that there is a unitary cloning operator  $\hat{U}$  that acts on two arbitrary states  $|\psi_1\rangle$  and  $|\psi_2\rangle$  in the following way:

$$\hat{U} |\psi_1\rangle \otimes |\phi\rangle = |\psi_1\rangle \otimes |\psi_1\rangle$$

and

$$\hat{U} |\psi_2\rangle \otimes |\phi\rangle = |\psi_2\rangle \otimes |\psi_2\rangle.$$

For the unknown quantum state  $|\psi\rangle = \alpha |\psi_1\rangle + \beta |\psi_2\rangle$ , we get:

$$\hat{U} |\psi\rangle \otimes |\phi\rangle = \alpha |\psi_1\rangle \otimes |\psi_1\rangle + \beta |\psi_2\rangle \otimes |\psi_2\rangle.$$

On the other hand, we can write:

$$|\psi\rangle \otimes |\psi\rangle = (\alpha |\psi_1\rangle + \beta |\psi_2\rangle) \otimes (\alpha |\psi_1\rangle + \beta |\psi_2\rangle).$$

Since these two results are different, we can conclude that the cloning operator  $\hat{U}$  does not exist.

### 8.3 Teleportation

Although it is impossible to clone the unknown quantum state, it is possible to transcribe an arbitrary quantum state from one position to another as long as the original copy is destroyed. This process is called a teleportation. To demonstrate the idea behind the teleportation protocols, we use a two-level system with four Bell states. Bell states are orthogonal and span the full Hilbert space for two two-level systems:

$$|\phi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2)$$

$$|\psi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 \pm |V\rangle_1 |H\rangle_2).$$

To teleport the unknown state between two parties (Alice and Bob), they have to share one Bell pair, for example,  $|\phi^-\rangle$ . The total state of Alice and Bob is:

$$|\Psi\rangle_{123} = |\chi\rangle_1 \otimes |\phi^-\rangle_{23}$$

where  $|\chi\rangle_1$  represents an unknown state, Alice possesses the states 1 and 2, Bob possesses state 3, while 2 and 3 form the shared Bell state. We can expand the combined state in the following way:

$$|\Psi\rangle_{123} = \frac{1}{2} [ |\phi^+\rangle_{12} \otimes V_3 |\chi\rangle_3 + |\phi^-\rangle_{12} \otimes V_4 |\chi\rangle_3 + |\psi^+\rangle_{12} \otimes V_2 |\chi\rangle_3 + |\psi^-\rangle_{12} \otimes V_1 |\chi\rangle_3 ]$$

where the operators  $V_i$  have the property that  $V_i^2 = 1$ .

Now, Alice performs a joint measurement on the states 1 and 2, and projects them into one of the Bell states, for example into  $|\phi^-\rangle_{12}$ . The total state now becomes  $|\phi^-\rangle_{12} \otimes V_4 |\chi\rangle_3$ . Alice can send a classical two-bit message to Bob that he should apply  $V_4$  on his state to recover  $|\chi\rangle_3$ . Note that a classical channel is inevitable for the process of teleportation.

## 8.4 Entanglement swapping

Entanglement swapping enables the entanglement of two photons that were produced from two different sources and never previously interacted. Imagine that one source emits photons 1 and 2 in a Bell state, and another source emits the photons 3 and 4 in another Bell state. One photon from each pair is received by Alice and Bob, and on the other two photons Bell state measurement is made (Fig. 33). The original state can be written as:

$$|\Psi\rangle_{1234} = |\phi\rangle_{12}^+ \otimes |\phi\rangle_{34}^+$$

which can be rewritten as a superposition of Bell state products:

$$|\Psi\rangle_{1234} = \frac{1}{2}(|\psi^+\rangle_{14} \otimes |\psi^+\rangle_{23} + |\psi^-\rangle_{14} \otimes |\psi^-\rangle_{23} + |\phi^+\rangle_{14} \otimes |\phi^+\rangle_{23} + |\phi^-\rangle_{14} \otimes |\phi^-\rangle_{23}).$$

In the next step, a joint measurement can be made projecting on one of the four Bell states of 2 and 3. Projection can be chosen to be on a particular Bell state, just like in the teleportation protocol, for example,  $|\psi^-\rangle_{23}$ . Finally, we get the initial state  $|\Psi\rangle_{1234}$  now to become  $|\psi^-\rangle_{14} \otimes |\psi^-\rangle_{23}$ . Although they have never been in contact, photons 1 and 4 are now entangled and Alice and Bob share a Bell pair. In the experiment, a beamsplitter can be used to make the Bell state measurement. Entanglement swapping is the basis for quantum repeaters which can be used to extend the distance of quantum communication.

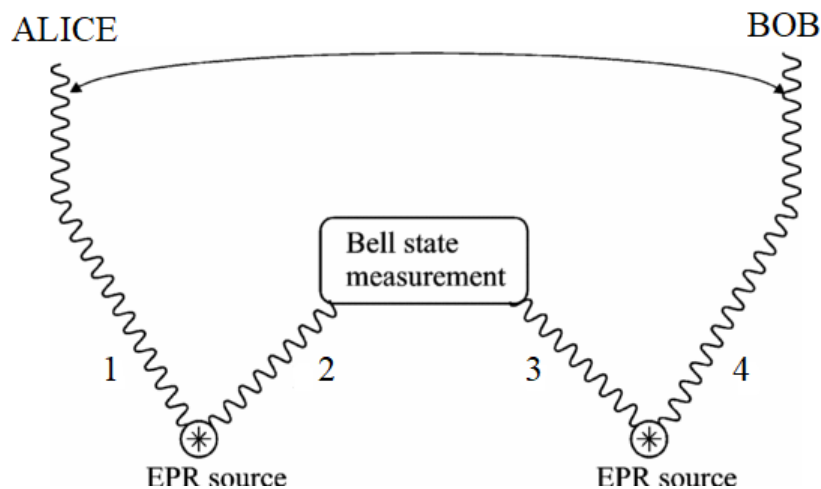


Figure 33. Entanglement swapping. Adapted from [87]

## 8.5 Alignment of user modules for polarization analysis

Upon entering the polarization analysis module (PAM), incoming photons can be randomly directed by a beamsplitter along the short path or along the long path (Fig. 34). Photons going through the short path are measured in the horizontal/vertical polarization (HV) basis and photons going through the long path are rotated  $45^\circ$  from the vertical axis with an achromatic half-wave plate and measured in the diagonal/anti-diagonal polarization (DA) basis. The difference between the short and long paths results in different time bins in polarization analysis. One major advantage of using PAM is that only two detectors per user are needed for full analysis. We used single photon avalanche detectors with dark counts of 227 counts/s and 552 counts/s for the first user and 1978 counts/s and 748 counts/s for the second user. Detectors are connected to the inputs of the time tagging device and further to the computer for analysis.

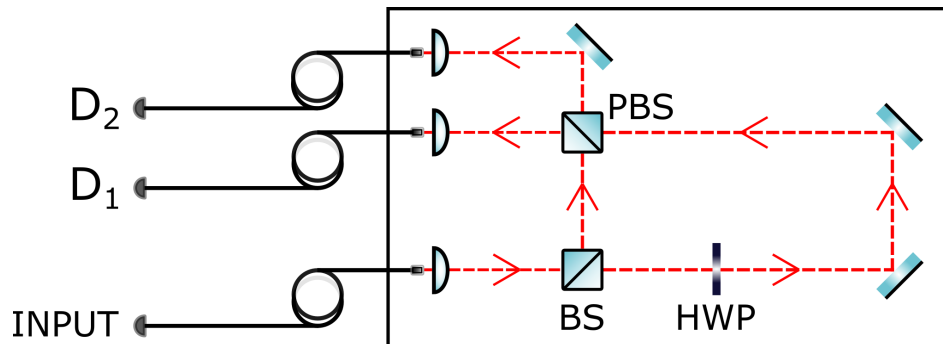


Figure 34. Scheme of the polarization analysis module consisting of the beamsplitter (BS), half-wave plate (HWP), mirrors and polarization beamsplitter (PBS). Fibers going to detectors are depicted as  $D_1$  and  $D_2$ .

Steps for alignment:

1. We connected the laser to the input fiber without any optical elements on the user module (beamsplitters, HWP or mirrors). The height and the direction of the beam were aligned using a pinhole and auxiliary tools. The same procedure was done for all three collimators/couplers (Fig. 35). In this way, we ensured that the collimators/couplers are well aligned and we did not touch them in the following steps.

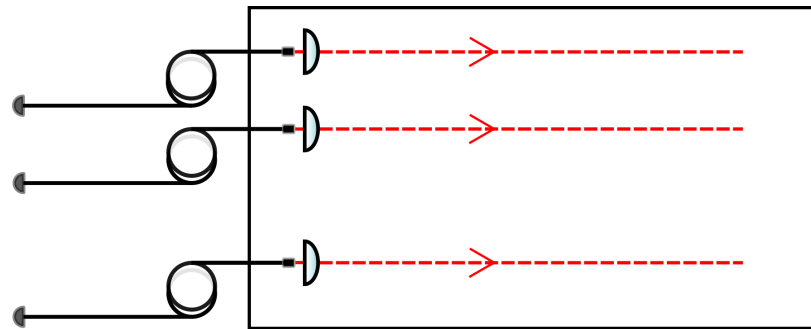


Figure 35. In the first step of the alignment procedure, we adjusted the height and the direction of the beams.

2. After aligning the straight lines, we mounted the beamsplitter and polarization beamsplitter in the short arm. Using BS and PBS as mirrors we got an overlap of the beams in front of the input and D1 and between BS and PBS, which ensures that the beam from the input will shoot directly into D1 following the short path (Fig. 36). After this step, we did not touch BS and PBS until the final step.

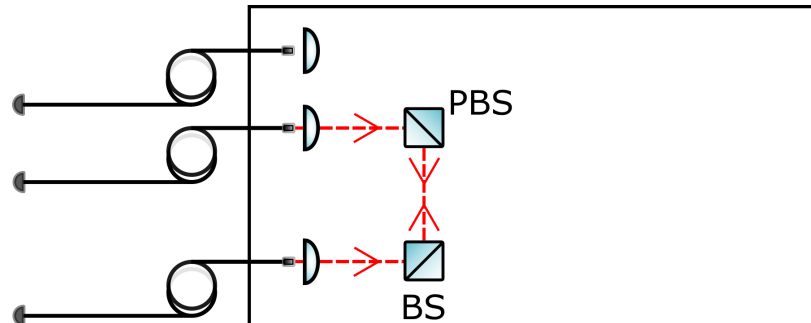


Figure 36. In the second step of the alignment procedure, we inserted BS and PBS and adjusted their positions and heights

3. In the third step we added two mirrors in the long path. An overlap of the beams in front of the input and D1 and between the mirrors ensures that the beam that is following the long path will shoot into D1 (Fig. 37).

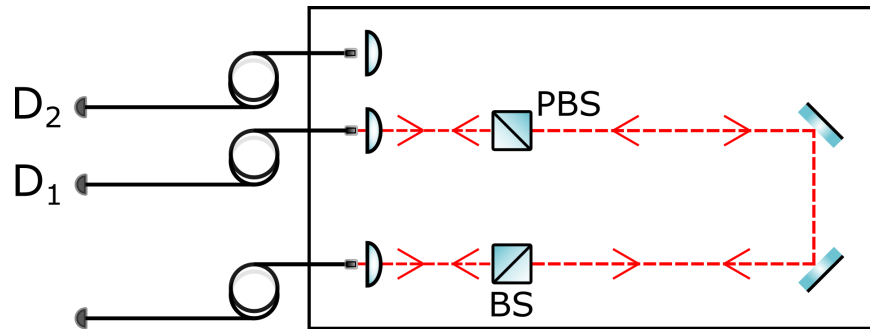


Figure 37. In the third step of the alignment procedure, we inserted two mirrors in the long path and adjusted their positions and heights

4. In the next step we added the last mirror. Its tip/tilt position can be determined by looking at an overlap in front of  $D_2$  one arm at a time (Fig. 38). With all other components aligned, we expected to see a signal on  $D_2$ . If needed, small adjustments on other elements could increase coupling efficiency on  $D_2$ .

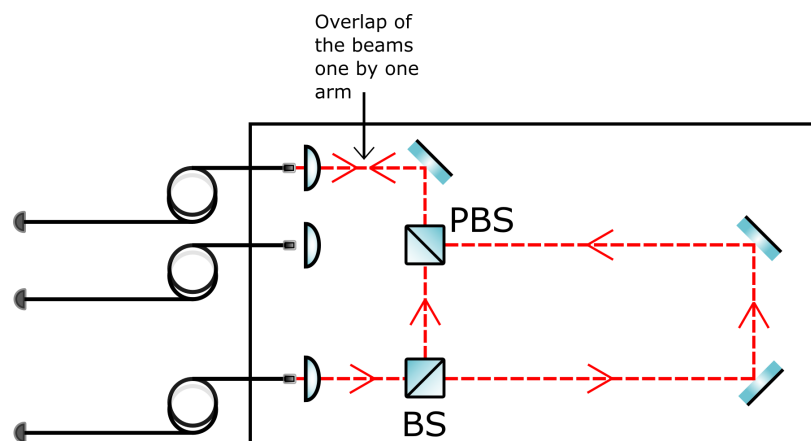


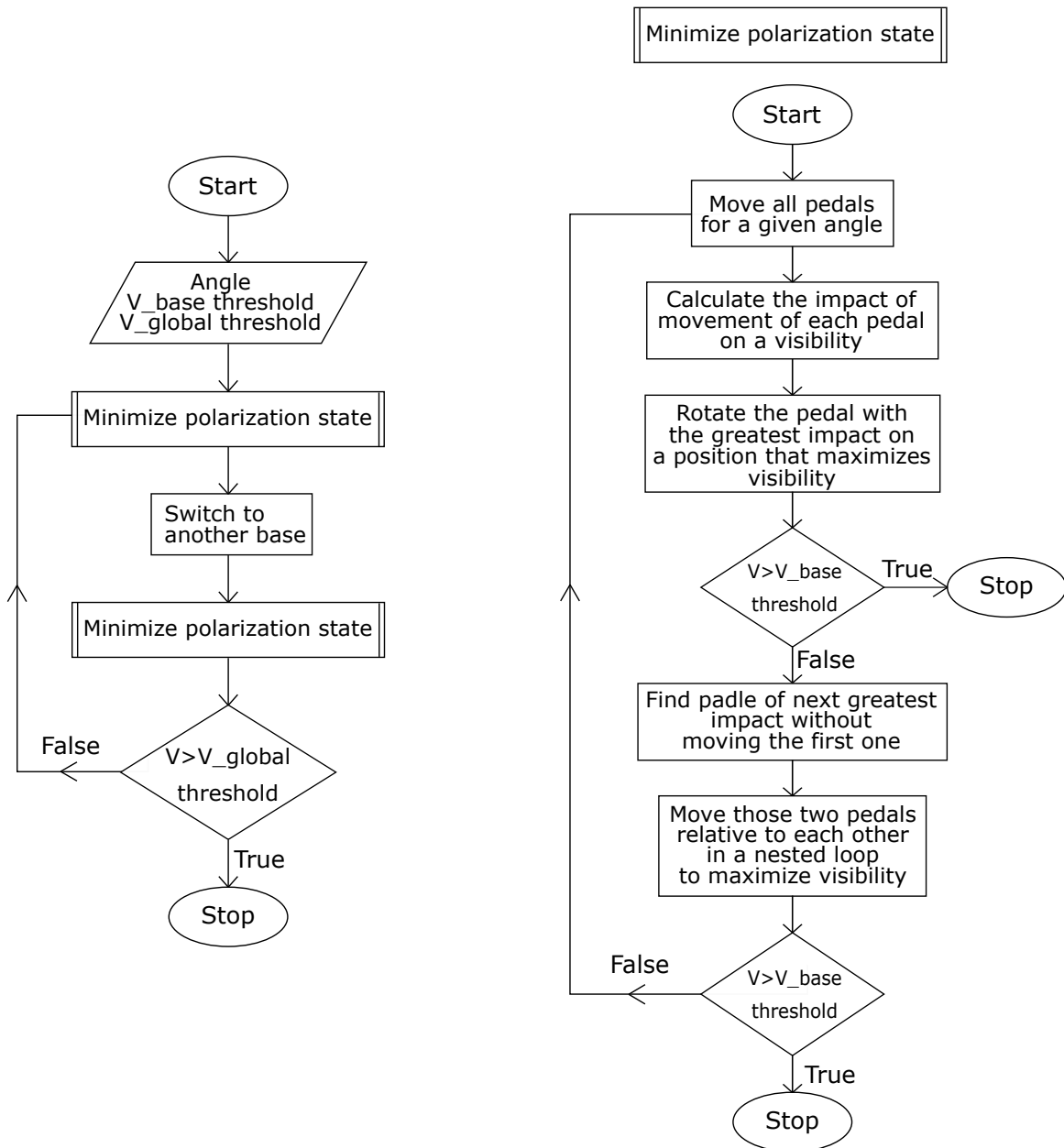
Figure 38. In the final step of the alignment procedure, we inserted a mirror in front of the second coupler and adjusted its position and height

5. After achieving the wanted coupling efficiency, the HWP is mounted in the long path.

Due to imperfections of the optical elements (typical values of reflectance and transmittance of beamsplitters are around 47%, the transmission of a parallel component on polarization beamsplitter is typically around 90%) or mechanical mismatch of the beam (rotation of HWP or lens inside of collimator/coupler) it is impossible to achieve perfect coupling. Couplings of 60-70% were achieved after the described procedure of alignment.



## 8.6 A flowchart of the algorithm for motorized polarization controllers



## 8.7 Distribution of channels in a six-user quantum network

Table 7. Distribution of ITU channels used in a six-user network

ITU channel	Wavelength (nm)	Frequency (THz)
19	1562.23	191.9
20	1561.42	192.0
21	1560.61	192.1
22	1559.79	192.2
23	1558.98	192.3
24	1558.17	192.4
25	1557.36	192.5
26	1556.55	192.6
27	1555.75	192.7
28	1554.94	192.8
29	1554.13	192.9
30	1553.33	193.0
31	1552.52	193.1
32	1551.72	193.2
33	1550.92	193.3
<b>34</b>	<b>1550.12</b>	<b>193.4</b>
35	1549.32	193.5
36	1548.51	193.6
37	1547.72	193.7
38	1546.92	193.8
39	1546.12	193.9
40	1545.32	194.0
41	1544.53	194.1
42	1543.73	194.2
43	1542.94	194.3
44	1542.14	194.4
45	1541.35	194.5
46	1540.56	194.6
47	1539.77	194.7
48	1538.98	194.8
49	1538.19	194.9

## 9 Curriculum vitae

Matej Peranić was born on July 4th, 1992 in Zagreb (Croatia). After finishing elementary and general-course high school in Velika Gorica, he started studying physics at the Faculty of Science in Zagreb. He graduated in 2018 on the topic "The source of polarization-entangled pairs of photons and testing Bell's inequality". In 2019 he started working as a research assistant at the Laboratory for Photonics and Quantum Optics at the Ruđer Bošković Institute in Zagreb. The same year he started his doctoral study at the Faculty of Science in Zagreb, module Atomic, molecular and optical physics. During his doctoral study, he participated at the Optics2019 conference in Yerevan, Armenia where he was awarded for the best student talk. Also, he was awarded for the best poster at the Symposium of doctoral students of the Faculty of Science in Zagreb in 2020. At the MIPRO conference in 2021, he held an invited talk on the topic "Quantum communication with entangled photon pairs". In 2022, he was awarded a scholarship from the British Scholarship Trust and spent three months on a study visit at the University of Bristol where he worked on the development of quantum networks. He is the first author of the paper "A study of polarization compensation for quantum networks" published in 2023 in the EPJ Quantum Technologies.

## 10 List of publications

1. Matej Peranić et al. "A study of polarization compensation for quantum networks". *EPJ Quantum Technologies* 10 (2023). DOI: 10.1140/epjqt/s40507-023-00187-w.

### 10.1 Conference papers

1. Marcus Clark et al. "Polarisation Based Entanglement Distribution Quantum Networking". *46th MIPRO ICT and Electronics Convention (MIPRO)* (2023). DOI: 10.23919/MIPRO57284.2023.10159792
2. Rui Wang et al. "Optimum Switching Scenario Analysis in a Dynamic Entanglement Network". *Optical Fiber Communications Conference and Exhibition (OFC)* (2023). DOI: 10.23919/OFC49934.2023.10117294
3. Marcus Clark et al. "Entanglement distribution quantum networking within deployed telecommunications fibre-optic infrastructure". *Quantum Technology: Driving Commercialisation of an Enabling Science III* (2023). DOI: 10.1117/12.2645095
4. Rui Wang et al. "Field trial of a dynamically switched quantum network supporting co-existence of entanglement, prepare-and-measure QKD and classical channels". *49th European Conference on Optical Communications* (2023). DOI: 10.1049/icp.2023.2666
5. Matej Peranić et al. "Quantum communication experiments with entangled photon pairs". *45th Jubilee International Convention on Information, Communication and Electronic Technology* (2022). DOI: 10.23919/MIPRO55190.2022.9803653
6. Rui Wang et al. "A Dynamic Multi-Protocol Entanglement Distribution Quantum Network". *Optical Fiber Communication Conference* (2022). DOI: 10.1364/OFC.2022.Th3D.3
7. Marcus Clark et al. "Towards a Fully Connected Many-User Entanglement Distribution Quantum Network Within Deployed Telecommunications Fibre-Optic Infrastructure". *CLEO: QELS Fundamental Science* (2022). DOI: 10.1364/CLEO-QELS.2022.FF4A.6

## **Acknowledgments**

The research leading to this thesis has received funding from the Croatian Ministry of Science, Education and Youth, MSE grant No. KK.01.1.1.01.0001, United Kingdom Research and Innovation's (UKRI) Engineering and Physical Science Research Council (EPSRC) Quantum Communications Hub (Grant Nos. EP/M013472/1, EP/T001011/1), British Scholarship Trust, Agency for Mobility and EU Programmes, and Croatian Science Foundation, HRZZ grant No. IPS-2020-1-2616.