Experimental Multiuser Secure Quantum Communications

Jan Bogdanski

Department of Physics

Stockholm University

Thesis for the degree of Doctor of Philosophy in Physics
Department of Physics
Stockholm University
Sweden

ISBN 978-91-7155-846-6

Printed by Universitetsservice US AB, Stockholm

Abstract

We are currently experiencing a rapid development of quantum information, a new branch of science, being an interdisciplinary of quantum physics, information theory, telecommunications, computer science, and many others. This new science branch was born in the middle of the eighties, developed rapidly during the nineties, and in the current decade has brought a technological breakthrough in creating secure quantum key distribution (QKD), quantum secret sharing, and exciting promises in diverse technological fields. Recent QKD experiments have achieved high rate QKD at 200 km distance in optical fiber. Significant QKD results have also been achieved in free-space.

Due to the rapid broadband access deployment in many industrialized countries and the standing increasing transmission security treats, the natural development awaiting quantum communications, being a part of quantum information, is its migration into commercial switched telecom networks. Such a migration concerns both multiuser quantum key distribution and multiparty quantum secret sharing that have been the main goal of my PhD studies. They are also the main concern of the thesis.

Our research efforts in multiuser QKD has led to a development of the five-user setup for transmissions over switched fiber networks in a star and in a tree configuration. We have achieved longer secure quantum information distances and implemented more nodes than other multi-user QKD experiments. The measurements have shown feasibility of multiuser QKD over switched fiber networks, using standard fiber telecom components.

Since circular architecture networks are important parts of both intranets and the Internet, Sagnac QKD has also been a subject of our research efforts. The published experiments in this area have been very few and results were not encouraging, mainly due to the single mode fiber (SMF) birefringence. Our research has led to a development of a computer controlled birefringence compensation in Sagnac that open the door to both classical and quantum Sagnac applications. On the quantum secret sharing side, we have achieved the first quantum secret sharing experiment over telecom fiber in a five-party implementation using the "plug & play" setup and in a four-party implementation using Sagnac configuration. The setup measurements have shown feasibility and scalability of multiparty quantum communication over commercial telecom fiber networks.

Contents

List of accompanying papers

Paper I **Experimental quantum secret sharing using telecommunication fiber**
J. Bogdanski, N. Rafiei, and M. Bourennane
Phys. Rev. A **78** 062307 (2008)

Paper II **Multiuser quantum key distribution over telecom fiber networks**
J. Bogdanski, N. Rafiei, and M. Bourennane
Opt. Commun. **282** 258 (2009)

Paper III **Sagnac quantum key distribution over telecom fiber networks**
J. Bogdanski, J. Ahrens, and M. Bourennane
Opt. Commun. **282** 1231 (2009).

Paper IV **Sagnac secret sharing over telecom fiber networks**
J. Bogdanski, J. Ahrens, and M. Bourennane
Opt. Express **17** 1055 (2009).

Paper V **Single mode fiber birefringence compensation in Sagnac and "plug & play" interferometric setups**
J. Bogdanski, J. Ahrens, and M. Bourennane
Opt. Express **17** 4485 (2009).

Related paper not included

Paper 1 **Five-user QKD over switched fiber networks**
J. Bogdanski, N. Rafiei, and M. Bourennane
in *SPIE Proceedings* **7092** 70920K (2008)

Paper 2 **Five-user QKD over switched fiber networks**
J. Bogdanski, J. Ahrens, and M. Bourennane
in *SPIE Proceedings* **7236** 72360M (2009)

Paper 3 **Birefringence compensation in Sagnac and its quantum communication applications**
J. Bogdanski, J. Ahrens, and M. Bourennane
in *SPIE Proceedings*, accepted by SPIE, Quantum Communications and Quantum Imaging conference in San Diego, August 6, 2009 (2009)

Preface

We are currently experiencing a rapid development of quantum information, a new branch of science, being an interdisciplinary of quantum physics, information theory, telecommunications, computer science, and many others. This new science branch was born in the middle of the eighties, developed rapidly during the nineties, and in the current decade has brought a technological breakthrough in creating secure quantum key distribution (QKD), quantum secret sharing, and exciting promises in diverse technological fields. Recent QKD experiments have achieved high rate QKD at 200 km distance in optical fiber. Significant QKD results have also been achieved in free-space. Furthermore, there are already three start-up companies working on QKD in fiber and a number of major companies have active quantum cryptography programs.

QKD was first proposed in the 1970s by Stephen Wiesner, but was first published in 1983. In 1984 Charles H. Bennett and Gilles Brassard made a great contribution to Wiesner's idea by proposing their BB84 protocol with polarization-encoding. Basically, QKD utilizes quantum mechanics' principles stating that an unknown quantum state cannot be duplicated (the no-cloning theorem), nor measured without disturbance (for instance, polarization measurement of a photon cannot be carried out simultaneously in the vertical-horizontal and in the diagonal-antidiagonal basis). After the BB84 protocol's proposal, a large number of experimental demonstrations of QKD between two parties have been carried out with different encoding and at different wavelength, both in free space and optical fibers.

Since any commercial QKD system needs to target standard birefringent single mode fiber (SMF) networks in the second or third telecom windows (1310 nm or 1550 nm), it would be difficult and impractical to use the previously mentioned polarization encoding. Therefore, many attempts have been made to replace it with phase encoding, which is an attractive solution due

to availability of the COTS (commercial off the shelf) telecom components.

Another important quantum information application is quantum secret sharing. Classical secret sharing builds on splitting a secret message, using mathematical algorithms, and the distribution of the resulting pieces to two or more legitimate users by classical communication, in the way that a single person is not able to reconstruct it. However, all ways of classical communication currently used are susceptible to eavesdropping attacks. As the usage of quantum resources can lead to unconditionally secure communications, a protocol implementing quantum secret sharing has been developed in 1999. The protocol provides information splitting and eavesdropping protection. However, the implementation is in practice non-scalable since it used multiphoton polarization entangled states that are difficult to generate and transmit. Furthermore, the use of polarization encoding is impractical for applications over commercial birefringent SMF networks. A new protocol solving the above mentioned problems was proposed in 2005. The protocol requires only a single qubit for quantum information transmission, which has allowed its practical experimental realization and scalability. This protocol has been implemented in our quantum secret sharing experiments.

Due to the rapid broadband access deployment in many industrialized countries and the standing increasing transmission security treats, the natural development awaiting quantum communications, being a part of quantum information, is its migration into commercial switched telecom networks. Such a migration concerns both multiuser quantum key distribution and multiparty quantum secret sharing that have been the main goal of my PhD studies. They are also the main concern of the thesis.

Our research efforts has led to a development of the five-user quantum QKD over switched fiber networks in a star and in a tree configuration, using the BB84-protocol with phase encoding. In order to compensate for the SMF birefringence, we have developed a polarization insensitive phase modulator circuitry, being a key element of our setups. We have achieved longer secure quantum information distances and implemented more nodes than other multi-user QKD experiments. The measurements have shown feasibility of multiuser QKD over switched fiber networks, using standard fiber telecom components. Since circular architecture networks are important parts of both intranets and the Internet, Sagnac QKD has also been a subject of our research efforts. The published experiments in this area have been very few and results were not encouraging, mainly due to the SMF birefringence. Our research has led to a development of a computer controlled birefringence compensation in Sagnac that open the door to both classical and quantum Sagnac applications.

On the quantum secret sharing side, we have achieved the first quantum secret sharing experiment over telecom fiber in five-party implementation using the "plug & play" setup and in four-party implementation using Sagnac configuration. The setup measurements have shown feasibility and scalability of secure multiparty secret sharing over commercial telecom fiber networks.

Our QKD and quantum secret sharing experiments have resulted in five journal papers and three SPIE Quantum Information conference publications.

My contributions to the accompanying papers

As recommended, I am below including my own, of course, personal and subjective, opinion about my contribution to the accompanying papers. This has not been an easy task for me since the experiments presented in the papers have been carried out by various project teams, which I am also acknowledging in the next section.

Paper I: Experimental quantum secret sharing using telecommunication fiber

J. Bogdanski, N. Rafiei, and M. Bourennane

We report the first quantum secret sharing experiment in telecom fiber in five-party implementation. The quantum secret sharing experiment has been based on a single qubit protocol, which has opened the door to practical secret sharing implementation over fiber channels and in free-space. The previous quantum secret sharing proposals were based on multiparticle entangled states, difficult in the practical implementation and not scalable. The secret sharing protocol has been implemented in an interferometric fiber optics setup with phase encoding and demonstrated for three, four, and five parties. The experimental setup measurements have shown feasibility and scalability of secure multiparty quantum communication over commercial telecom fiber networks.

Since the experiment was started in a new-built fiber lab, it requested purchase of not only the components needed for its realization but also a lab infrastructure and all necessary instruments. I was the major contributor to all these tasks as well as to both the optical and electronic system design. Particularly, I designed a polarization insensitive phase modulator being the key component of the demonstrator and for other experiments. On the software side, I developed a LabView program for the system control. Furthermore, I was the major contributor in developing the demonstrator's measurement methodology and calibrating the measurement instruments. In the beginning of the project, the measurements were carried out together with the first coauthor, who in the final phase completed the measurements

on his own. The paper was written by me, with a very helpful feedback from the coauthors.

Paper II: Multiuser quantum key distribution over telecom fiber networks

J. Bogdanski, N. Rafiei, and M. Bourennane

We report five-user quantum key distribution (QKD) over switched fiber networks in both star and tree configurations, using the BB84-protocol with phase encoding. Both setups implement polarization insensitive phase modulators, necessary for birefringent single mode fiber (SMF) networks. In both configurations we have achieved transmission distances between 25 km and 50 km with quantum bit error rates between 1.24% and 5.56% for the mean photon number $\mu = 0.1$. The measurements have showed feasibility of multiuser QKD over switched fiber networks, using standard fiber telecom components.

The idea of the experiment was mine. I also provided a proper electrical interface and optical connectorization as well as was the major contributor in developing the demonstrator's measurement methodology. In the beginning of the project, the measurements were carried out together with the first coauthor, who in the final phase completed the measurements on his own. The paper was written by me, with a very helpful feedback from the coauthors.

Paper III: Sagnac quantum key distribution over telecom fiber networks

J. Bogdanski, J. Ahrens, and M. Bourennane

We present a new concept for compensation of single mode fiber (SMF) birefringence effects in a Sagnac quantum key distribution (QKD) setup, based on a polarization control system and a polarization insensitive phase modulator. Our experimental data show stable (in regards to birefringence drift) QKD over 1550 nm SMF telecom networks in Sagnac configuration, using the BB84-protocol with phase encoding. The achieved total Sagnac transmission loop distances were between 100 km and 150 km with quantum bit error rates (QBER) between 5.84% and 9.79% for the mean photon number $\mu = 0.1$. The distances were much longer and rates much higher than in any other published Sagnac QKD experiments. We also show an example of our one-decoy state protocol implementations (for the 45 km distance between Alice and Bob, corresponding to the 130 km total Sagnac loop length), providing an unconditional QKD security. The measurement results have showed feasibility of QKD over telecom fiber networks in Sagnac configuration, using standard fiber telecom components.

The idea of the experiment and birefringence compensation was mine, but the discussions with first the coauthor and his feedback were of a significant value. The measurements were made jointly with the coauthor. The paper was written by me, with a very helpful feedback from the coauthors.

Paper IV: Sagnac secret sharing over telecom fiber networks

J. Bogdanski, J. Ahrens, and M. Bourennane

We report the first Sagnac quantum secret sharing (in three- and four-party implementations) over 1550 nm single mode fiber (SMF) networks, using a single qubit protocol with phase encoding. Our secret sharing experiment has been based on a single qubit protocol, which has opened the door to practical secret sharing implementation over fiber telecom channels and in free-space. The previous quantum secret sharing proposals were based on multiparticle entangled states, difficult in the practical implementation and not scalable. Our experimental data in the three-party implementation show stable (in regards to birefringence drift) quantum secret sharing transmissions at the total Sagnac transmission loop distances of $55-75$ km with the quantum bit error rates (QBER) of $2.3-2.4\%$ for the mean photon number $\mu = 0.1$ and $1.7-2.1\%$ for $\mu = 0.3$. In the four-party case we have achieved quantum secret sharing transmissions at the total Sagnac transmission loop distances of $45-55$ km with the quantum bit error rates (QBER) of $3.0-3.7\%$ for the mean photon number $\mu = 0.1$ and $1.8-3.0\%$ for $\mu = 0.3$. The stability of quantum transmission has been achieved thanks to our new concept for compensation of SMF birefringence effects in Sagnac, based on a polarization control system and a polarization insensitive phase modulator. The measurement results have showed feasibility of quantum secret sharing over telecom fiber networks in Sagnac configuration, using standard fiber telecom components.

The idea of the birefringence compensation was mine, but the discussions with the first coauthor and his feedback were of a significant value. The measurements were made jointly with the coauthor. The paper was written by me, with a very helpful feedback from the coauthors.

Paper V: Single mode fiber birefringence compensation in Sagnac and "plug & play" interferometric setups

J. Bogdanski, J. Ahrens, and M. Bourennane

Single mode fiber (SMF) birefringence effects have been a limiting factor for a variety of Sagnac applications over longer distance SMF links. In this report, we present a new concept of the SMF birefringence compensation in a Sagnac interferometric setup, based on a novel polarization control system. For the destructive interference, our control system guarantees a perfect compensation of both the SMF birefringence and imperfect propagation times matching of the setup's components. For the stabilization of the constructive interference, we have applied a fiber stretcher and a simple proportional−integral−derivative (PID) controller. The enclosed experimental data of the setup's visibility confirm validity of our polarization control system. We have also showed that the SMF birefringence model used in a "plug & play" interferometric setup, widely cited in the papers on quantum key distribution, cannot be applied in SMF Sagnac interferometric setup. However, the SMF birefringence model based on the Kapron equivalence well describes SMF Sagnac.

The idea of the birefringence compensation was mine. I also developed the birefringence model published in the article. However, the discussions with the first coauthor and his feedback were of a significant value. The paper was written by me, with a very helpful feedback from the coauthors.

Acknowledgements

Writing this part of the thesis has been a difficult task for me since it touches relationships with many people I have been working with or interconnected during last four very challenging years at Fysikum. The main question here is how to avoid standard clichés, be fair, and sincere while acknowledging people, to whom I was professionally close, during my PhD studies.

I owe my deepest gratitude to my supervisor Mohamed Bourennane, who gave me the opportunity to study at Fysikum and who always strongly believed that I would successfully complete my studies. This happened despite the clear age difference, professionally and socially not easily accepted in Sweden, between me and the rest of PhD students not only at our department, but most likely worldwide, at least in the field of quantum information. On the top of the age issue, another one, namely that I had had a long academic break after the Master Degree in Electronic Engineering by mainly occupying administrative and industrial managerial positions, has never discouraged him. His belief in my research potential (that he has often expressed to me) and his trust that my deep interest in quantum information (being the main driving force for my decision of exploring quantum physics as a PhD student), were the best possible encouragements I could get.

There is another person here at Fysikum whom I owe a lot and who deserves a very special acknowledgement. Without Hoshang Heydari, I would never complete my studies. During tough times, he always encouraged me in a very special way, his own one, which helped to overcome various problems and crises.

Before acknowledging the team members, I worked with; I should also acknowledge Piotr Badziag for both his scientific comments concerning the secret sharing and Sagnac demonstrators as well as for his patient listening to my worries, at the times when I felt down.

I have also benefited a lot from working with the three, acknowledged below, Master Thesis students. Without them, the studies would take a significantly longer time. Alma Imanovic, the first student, came to only a partly equipped fiber lab. She contributed a lot to testing different semiconductor lasers and other instruments. She also helped in setting up our first quantum secret sharing demonstrator; in building and testing diverse interface cards; and generally, in establishing a working lab. Nima Rafiei, the second student, was a great contributor to the final optical and electronic solutions for the secret sharing and multiuser QKD demonstrators. Our, sometimes vibrant, discussions were very helpful not only concerning the optical and electronic hardware, but also led to a deeper understanding

of the secret sharing protocol and work on the future overlays to the protocol. He also carried out parts of the measurements on both demonstrators. Our work led to two published papers and one SPIE Quantum Information conference publication. Johan Ahrens, the third student, contributed to Sagnac QKD and Sagnac quantum secret sharing demonstrators. Our work on the demonstrators was very demanding since we entered an almost unexplored (for quantum communications) network topology that required a lot of both theory and experimental work. Discussions with Johan on birefringence generally, and Sagnac birefringence particularly, were enormously helpful in creating a new birefringence model for Sagnac. Johan has also contributed a lot to setting up two Sagnac demonstrators (one for QKD and the other one for secret sharing); to LabView programming; and to the measurements. Furthermore, he contributed significantly with his comments and his proofreading to both the thesis and the articles that we published. Our work led to three published papers and one SPIE Quantum Information conference publication. I also would like to acknowledge Magnus Rådmark for the helpful discussions concerning secret sharing demonstrator and Elias Amselem for the same in regards to both Sagnac demonstrators.

All other current members of our group i.e. the PhD students Hatim Azzouz and Christian Kothe; Master Thesis students Per Nilsson and Hoon Jang; as well as the former members should also be acknowledged, especially for creating a friendly and research encouraging environment in the group.

Finally, there are many people that have contributed to the nice atmosphere in our corridor and I would like to extend my thanks to them.

The acknowledgment list would be not completed without emphasizing the great project funding contribution of the Swedish Defense Materiel Administration (FMV) that kept me employed until the end of last year. Here, a special acknowledgment deserves my first FMV's supervisor Janne Wallin, who provided priceless instrument and component contributions into the establishment of our lab and the demonstrators as well as temporary employed to all the three, previously mentioned Master Thesis students, working with me. Also Christer Thorsson, my second FMV's supervisor, should be acknowledged for temporary employing the students and for many other contributions to my PhD.

Sammanfattning på svenska

Vi befinner oss numera i en mycket snabb utvecklingsfas av kvantinformation, en ny interdisciplinär vetenskapsgren som länkar ihop kvantfysik, informationsteori, telekommunikation, datorvetenskap och flera andra vetenskapsgrenar. Den nya vetenskapsgrenen föddes i mitten av åttiotalet, utvecklades snabbt under nittiotalet, och har, under detta decennium, åstadkommit stora teknologiska genombrott i form av säker kvantnyckelöverföring, kvantsekretessdelning, och spännande utvecklingsmöjligheter inom flera teknologiska fält. Nyliga experiment inom kvantnyckelöverföring har åstadkommit en höghastighetsöverföring av kvantnyckel i fiber på 200 km avstånd. Även i "free-space" har signifikanta resultat uppnåtts.

Med anledning av en snabb utveckling av bredbandstjänster i de flesta industriländerna och tilltagande säkerhetsrisker är den naturliga utvecklingsmöjligheten för kvantkommunikation (som är en gren av kvantinformation) dess migration till de kommersiella telekomnäten. En sådan migration förväntas omfatta både multianvändarkvantnyckelöverföring och kvantsekretessdelning vilka har varit huvudmål för mina doktorandstudier och som den här avhandlingen fokuserar på.

Vår forskning inom multianvändarkvantnyckelöverföring har resulterat i utveckling av en demonstrator för fem användare i switchade stjärn- och trädnätverk. Vi har åstadkommit längre distanser för säker kvantnyckelöverföring och använt fler noder än tidigare multianvändarexperiment. Våra mätningar har visat att multianvändarkvantnyckelöverföring är genomförbar i switchade fibernät.

Eftersom ringnätverk utgör en viktig del av både intranät och Internet väckte multianvändarkvantnyckelöverföring i Sagnac vårt forskningsintresse. Vi hade noterat att det fanns väldigt få publikationer inom detta område. De publicerade resultaten var inte speciellt uppmuntrande, huvudsakligen på grund av problem orsakade av dubbelbrytning i singelmodfiber. Vårt forskningsarbete har lett till utveckling av en datorstyrd kompenseringskrets för dubbelbrytningen i Sagnac som öppnar möjligheter för nya tillämpningar, såväl klassiska som inom kvantinformation.

Inom kvantsekretessdelning har vi genomfört det första experimentet i telekom fiber: för fem användare med "plug & play" nätverk och fyra användare i Sagnac nätverk. Mätningarna har visat att kvantsekretessdelning är genomförbar över kommersiella telekom fibernät.

Part I:
Background

Chapter 1

Introduction to quantum information

1.1 Qubit

1.1.1 Qubit versus bit

A bit is the basic unit of classical information. More explicitly, a bit is defined as the unit of Shannon information entropy of a discrete random variable X with the n possible values $\{x_1, x_2, ..., x_{n-1}, x_n\}$

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i), \tag{1.1}$$

where $p(x_i)$ denotes the probability of (x_i). It should be pointed out that for other bases of the logarithm, there are different entropy units (for instance, a nat for the natural logarithm or a dit for the decimal logarithm).

Regardless of its physical realization, a bit is always understood to be either a 0 or a 1. In computer memories and generally in classical computers only these two discrete values are used for information encoding, processing, and storing. While a bit must be either 0 or 1, a qubit, the unit of quantum information, can be 0, 1, or a superposition of both.

Quantum information is described by a state vector in a two-level quantum-mechanical system, which is formally equivalent to a two-dimensional vector space over the complex numbers

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle, \tag{1.2}$$

alternatively

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}, \tag{1.3}$$

with the basis states normalized

$$|||\psi\rangle||^2 = |c_0|^2 + |c_1|^2 = 1, \tag{1.4}$$

and orthogonal

$$\langle k|n\rangle = \delta_{kn}, \tag{1.5}$$

where δ_{kn} is Kronecker delta function

$$\delta_{kn} = 0 \ for \ k \neq n,$$
$$\delta_{kn} = 1 \ for \ k = n.$$

The quantum state can be rewritten to

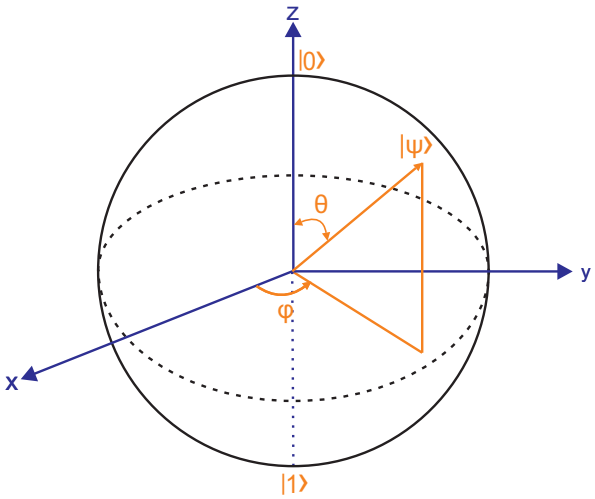

Figure 1.1: Bloch sphere

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \tag{1.6}$$

where η is the global phase (that could be omitted in less complex systems), while φ and θ are the state parameters shown on the Bloch sphere (with a

unit radius, see Fig.1.1), being a representation of the state.
It is easy to prove that the state is given by the following unit vector

$$\mathbf{R} = \begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix}, \tag{1.7}$$

on the Bloch sphere [1].
The state $|0\rangle$ lies on the sphere's north pole, while the state $|1\rangle$ on the south pole. On the sphere's equator (for $\theta = \pi/2$) lie states

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right). \tag{1.8}$$

The quantum state description on the surface of the Bloch sphere is possible only for a limited number of states. Generally, in open quantum systems the length of the Bloch vector is a variable [1]. But also for such systems, it is possible to find another illustrative description of the Bloch vector $\mathbf{R}$

$$\rho = \begin{pmatrix} c_0 c_0^* & c_0 c_1^* \\ c_1 c_0^* & c_1 c_1^* \end{pmatrix} = \frac{1}{2}\left(1 + \mathbf{R}\vec{\sigma}\right), \tag{1.9}$$

where ρ is the density matrix (also called a density operator) and $\vec{\sigma}$ is the Pauli vector given by

$$\vec{\sigma} = \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.10}$$

where σ_1, σ_2, and σ_3 are Pauli matrices.

A quantum state whose state $|\psi\rangle$ is known exactly is said to be in a pure state and its density matrix is given by

$$\rho^2 = |\psi\rangle\langle\psi|. \tag{1.11}$$

It is easy to show that

$$\rho^2 = \rho, \tag{1.12}$$

for pure states.

1.1.2 Qubit encoding

Since quantum information, generally, and its quantum communications branch (that is the subject of the thesis), particulary, use qubits as information carriers then; similarly to transforming, encoding, and storing bits in classical communications; there is a need to perform similar operations on qubits (in our case photons) in quantum communications. For instance, a qubit can be encoded in its polarization, presented, in detail, in Sec.3.6.

Qubit polarization encoding

A photon can be polarization encoded by using the polarization of its electrical field in the orthogonal bases defined by the horizontal and vertical directions

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \ |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ (see Eq.1.3);} \tag{1.13}$$

or a diagonal-antidiagonal

$$|D\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + |V\rangle \right), \ |A\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle - |V\rangle \right); \tag{1.14}$$

or a left-right circular polarization

$$|L\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle - i|V\rangle \right), \ |R\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + i|V\rangle \right). \tag{1.15}$$

Unfortunately, due to birefringence, discussed in Chap.3, polarization encoding suits not well for practical quantum communications over telecom fibers.

Qubit phase encoding

Phase encoding is much more suitable than polarization encoding for quantum communications over fiber. In phase encoding used in quantum communications, the information is encoded in the phase change of a given photon in reference to an other photon. Here, two main phase encoding schemes, based on interferometric setups, should be mentioned: the "plug & play" (widely discussed in the thesis) and differential phase modulation. Phase encoding in these schemes requires the coherence length of the photon to exceed the length difference between the different arms of the interferometers in order to guarantee high interference visibility.

Other qubit encodings

While polarization encoding has mainly been used in defining various QKD protocols (for instance, BB84, see Sec.6.1), phase encoding has been the foundation for our QKD and quantum secret sharing experiments and is, in detail, discussed in the thesis. However, the current section would be really very limited in its review of different qubit encodings if the unique features of quantum information, leading to a variety of other encodings, were not emphasized. Here, a couple of important encodings should be mentioned:

- frequency encoding that uses frequency-entangled states (generated via spontaneous parametric down-conversion) for assigning the qubit $|0\rangle$ to one of the frequency states and the qubit $|1\rangle$ to the other;
- time-bin encoding, which builds on sending a single-photon into a Mach-Zehnder interferometer with one of its two paths longer than the other (the difference in path length must be longer than the coherence length of the photon in order to distinguish the taken path);
- time-energy-entangled photon pairs, proposed by Franson in 1989 [2].

1.2 Principle of superposition

The principle of superposition is very important for understanding of various quantum mechanics phenomena and their interpretation. It says that any linear combination of two evolving quantum states that solve the Schrödinger equation is also a solution of the equation. A practical example of it is an interference of two waves propagating from the two slits in the double-slit experiment.

1.3 No-cloning theorem and indistinguishability of non-orthogonal states

The no-cloning theorem was born in 1982 when W. K. Wootters and W. H. Zurek [3] proved that the linearity of quantum mechanics forbids to clone ideally a unknown arbitrary pure quantum system. The theorem has profound implications in quantum information and quantum communications. In 1996, Barnum, Caves, Fuchs, Jozsa, and B. Schumacher [4] extended the proof into mixed states. The no-cloning theorem can be proved in a couple of different ways. Here, we use the principle of superposition (see Sec.1.2) on pure states.

Firstly, lest us define the cloning operation as

$$U_{AB}|\varphi\rangle_A|0\rangle_B = |\varphi\rangle_A|\varphi\rangle_B, \tag{1.16}$$

where A, B are two quantum systems and U_{AB} is a unitary transformation for the cloning [1].
Now, let us use the principle of superposition by considering the following state

$$|\psi\rangle_A = c_1|\varphi_1\rangle_A + c_2|\varphi_2\rangle_A. \tag{1.17}$$

After applying the cloning operation (see Eq.1.16) we are getting

$$U_{AB}|\psi\rangle_A|0\rangle_B \Rightarrow c_1|\varphi_1\rangle_A|\varphi_1\rangle_B + c_2|\varphi_2\rangle_A|\varphi_2\rangle_B \tag{1.18}$$

instead of the expected product of a proper cloning: $|\psi\rangle_A|\psi\rangle_B$. Thus, the linearity of quantum mechanics operations forbids the cloning. However, as the Eqs.1.16, 1.17, and 1.18 show, the perfect cloning is feasible on orthogonal states. But even in such a case, quantum mechanics sets a limit on the cloning by requiring a copier (a cloning machine) that is specifically built for these orthogonal states. For instance, a cloning machine built for copying in a horizontal-vertical basis of polarization states (that are orthogonal) will fail on copying in a diagonal-antidiagonal basis. This limit, set by quantum mechanics on cloning, is a foundation of QKD since it prohibits a successful eavesdropping of the quantum key. An Eavesdropper can successfully copy photons in one of the basis, by using a device designed for it, but his/her eavesdropping activity will be detected by the key distributors due to the random signal disturbance caused by the cloning machine's inability to copy photons in the other basis (see Chap.6).

Chapter 2

Basic quantum communications components

2.1 Single photon sources

2.1.1 Ideal single photon source

QKD reliability and performance depend on the photon source's quality. A single-photon generator emitting one and only one 1550 nm photon (while "on-trigged", i.e. on-demand) would be an ideal photon source for QKD.

2.1.2 Faint-pulse based single photon sources

Since an ideal single photon source is still unavailable R & D efforts are focused on designing quasi-single photon sources. For instance, a standard semiconductor laser generating coherent states can approximate single photon source. In order to do it, the laser pulses need to be strongly attenuated. The attenuated pulses follow Poisson distribution

$$P(n) = e^{-\mu}\frac{n^{\mu}}{n!}, \tag{2.1}$$

where μ is the mean photon number, which makes it possible to limit the probability that a non-empty weak pulse contains more than one photon

$$P(n>1) = \frac{1 - P(n=0) - P(n=1)}{1 - P(n=0)} \tag{2.2}$$

to an arbitrary small number. Assuming a very high attenuation giving the mean photon number $\mu = 0.1$ (also one single photon for ten laser pulses),

the probability that a non-empty pulse contains more than one photon is

$$P(n > 1) \approx \mu/2 = 0.05, \tag{2.3}$$

also a low number. This kind of pseudo single-photon source limits QKD bit rates since most of the strongly attenuated pulses are "empty".

2.2 Single photon detectors

For quantum communication applications in the 770 nm atmospheric window and in the first telecom window (820−900) nm, silicon avalanche photodiodes are widely implemented. However, for detection in the second $(1280 - 1350)$ nm and the third $(1528 - 1565)$ nm telecom windows, silicon avalanche photodiodes are not suitable, mainly because of the silicon's large band-gap that causes the material to be relatively insensitive to these light-waves. In the second telecom window, germanium avalanche photo-diodes were used by several research groups in the beginning of the last decade. Quantum efficiencies of ca 15 % were achieved by one of the groups [5]. The germanium devices require cooling to 77 K, which could be provided by liquid nitrogen. In the second part of the last decade, the germanium devices became less and less available on the commercial semiconductor market. Instead, more focus was put on InGaAs avalanche photodiodes that, in the gated mode, allow single-photon detection in both the second and the third telecom windows. In the passive-quenching mode (in which a large resistor is connected in series with the diode) the InGaAs devices are even more difficult to implement than the germanium diodes, mainly because of their high dark count ratio. In the gated-mode, the InGaAs devices perform better than the germanium diodes. Tab.2.1 summarizes performance of the avalanche photodiodes in free-space and in both telecom windows [5].

	770 nm	1310 nm	1310 nm	1550 nm
Material	Silicon	InGaAs	InGaAs	only InGaAs
Temperature [K]	253	~ 77	~ 77	~ 215
Quantum efficiency [%]	~ 70	~ 17	~ 30	~ 20

Table 2.1: Avalanche photodiode performance in free-space and in fiber at 1310 nm and 1550 nm [5].

Chapter 3

Fiber links

3.1 Introduction

During the last two decades, fiber has revolutionized the telecom and media world, especially the services requiring high-speed transmission in real time. It has replaced copper cables (twisted pair and coax), much less immune to external interferences. Its bandwidth, while using modern dense wavelength division multiplexing (DWDM) technologies seems to be almost unlimited. It neither corrodes nor requires maintenance. It also has low attenuation (in the range of 0.2 dB/km in the 1550 nm telecom window). One could continue to expand the list of its advantages over copper cables, but since here we are concerned about secure quantum communications, it should be pointed out its ability of transmitting single photons over long distances (up to 200 km), which has been explored during the last twenty years. Since multiparty QKD and secret sharing, being the subject of the thesis, uses fiber as a transmission medium, this chapter reviews some parts of its theory that are of importance for these quantum information applications.

3.2 Light propagation in fiber

A standard approach in analyzing light propagation in fiber builds on using the ray optics and Snell's law of reflection [6–9],

$$\frac{\sin\phi_{in}}{\sin\phi_T} = \frac{k_t}{k_{in}} = \frac{n_2}{n_1} = n, \tag{3.1}$$

shown in Fig.3.1, where $k_{in} = 2\pi/\lambda_{in}$ is the wavenumber of the incident ray and $k_t = 2\pi/\lambda_t$ of the transmitted ray, while n_1 and n_2 are refraction indices

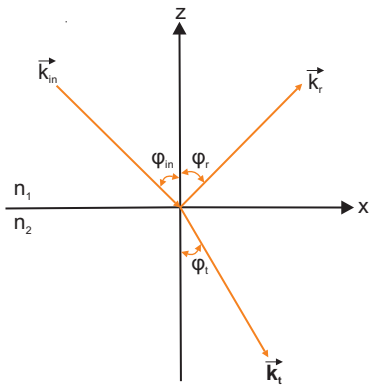

Figure 3.1: Reflection and refraction on the border between two materials with refraction indices n_1 and n_2.

for the incident ray and transmitted ray, respectively.

There are two important polarization state cases for the electromagnetic field that should be considered here: TE (Transverse Electric), shown in Fig.3.2, and TM (Transverse Magnetic), shown in Fig.3.3. In the first case,

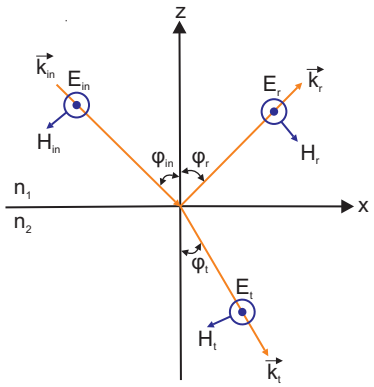

Figure 3.2: Reflection and refraction of a TE polarized light on the border between two materials with refraction indices n_1 and n_2.

i.e. the TE-mode, there are following boundary conditions for the transverse electric field and the tangential magnetic field [6–9]

$$\begin{aligned} E_{in} + E_r &= E_t, \\ -H_{in}\cos\phi + H_r\cos\phi &= -H_t\cos\phi_t, \end{aligned} \tag{3.2}$$

where $\phi = \phi_{in} = \phi_r$ since the wave vectors $\mathbf{k_{in}}$ and $\mathbf{k_t}$ propagate on the

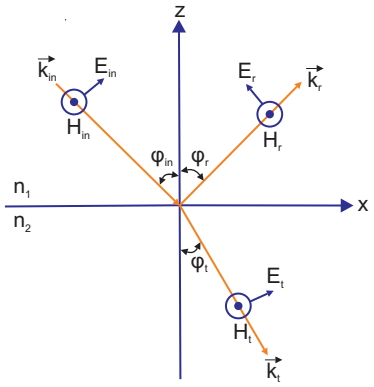

Figure 3.3: Reflection and refraction of a TM polarized light on the border between two materials with refraction indices n_1 and n_2.

same side of the border. From the Maxwell's equation, we are getting the following relationships between the electric and magnetic fields

$$H_{in} = \frac{k_{in}E_{in}}{\mu\omega},\ H_r = \frac{k_r E_r}{\mu\omega},\ H_t = \frac{k_t E_t}{\mu\omega}. \tag{3.3}$$

By substituting Eq.3.3 into Eq.3.2 we are finally getting [9]

$$-k_{in}E_{in}\cos\phi + k_r E_r \cos\phi = -k_t E_t \cos\phi_t. \tag{3.4}$$

Similarly to the TE-mode, the boundary conditions for the TM-mode are [9]

$$\begin{aligned} H_{in} + H_r &= H_t, \\ E_{in}\cos\phi - E_r\cos\phi &= E_t\cos\phi_t, \\ k_{in}E_{in} + k_r E_r &= k_t E_t. \end{aligned} \tag{3.5}$$

From Eq.3.1, Eq.3.2, Eq.3.4, and Eq.3.5 the following reflection and refraction coefficients are found for the TE an TM modes

$$\begin{aligned} R_{TE} &= \frac{E_{r_{TE}}}{E_{in_{TE}}} = \frac{\cos\phi - n\cos\phi_t}{\cos\phi + n\cos\phi_t}, \\ R_{TM} &= \frac{E_{r_{TM}}}{E_{in_{TM}}} = \frac{n\cos\phi - \cos\phi_t}{n\cos\phi + \cos\phi_t}. \end{aligned} \tag{3.6}$$

$$T_{TE} = \frac{E_{t_{TE}}}{E_{in_{TE}}} = \frac{2\cos\phi}{\cos\phi + n\cos\phi_t},$$
$$T_{TM} = \frac{E_{t_{TM}}}{E_{in_{TM}}} = \frac{2\cos\phi}{n\cos\phi + \cos\phi_t}. \tag{3.7}$$

Eq.3.6 shows that the reflection coefficients for the TE an TM modes are different. Similarly, Eq.3.7 shows that the refraction coefficients of the TE an TM modes are different. Thus, fiber is intrinsically polarization asymmetrical!

By substituting Eq.3.1 into Eq.3.6 we are getting

$$R_{TE} = \frac{\cos\phi - \sqrt{n^2 - \sin^2\phi}}{\cos\phi + \sqrt{n^2 - \sin^2\phi}},$$
$$R_{TM} = \frac{n^2\cos\phi - n\sqrt{n^2 - \sin^2\phi}}{n^2\cos\phi + \sqrt{n^2 - \sin^2\phi}}. \tag{3.8}$$

Thus, for

$$n = \sin\phi = \sin\phi_c, \tag{3.9}$$

where $\sin\phi_c$ is the critical angle, there is a total internal reflection of the light beam. In fiber, only the angles $\phi \geq \phi_c$ are of interest. For these angles, the reflection coefficients for the TE an TM modes are

$$R_{TE} = \frac{\cos\phi - i\sqrt{\sin^2\phi - n^2}}{\cos\phi + i\sqrt{\sin^2\phi - n^2}},$$
$$R_{TM} = \frac{n^2\cos\phi - in\sqrt{\sin^2\phi - n^2}}{n^2\cos\phi + i\sqrt{\sin^2\phi - n^2}}. \tag{3.10}$$

The critical angle $\sin\phi_c$ has so far been defined with respect to the orthogonal to the border between two materials of refractive indices n_1 and n_2, respectively (see Fig.3.1). In fiber, the angel is defined with respect to its axis, as it is shown in Fig.3.4. Thus, the redefined critical angle is given by

$$\sin\phi_c = \sqrt{n_{core}^2 - n_{clad}^2}. \tag{3.11}$$

The critical angle ϕ_c defines numerical aperture of the fiber

$$NA = n_0\sin\phi_c = n_0\sqrt{n_{core}^2 - n_{clad}^2}, \tag{3.12}$$

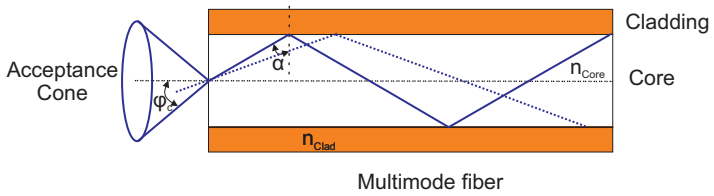

Figure 3.4: Numerical aperture of the multimode fiber. The critical angle ϕ_c shows the maximum entrance angle at which the incident beam can be coupled into the fiber. The acceptance cone shows the size of the light cone accepted by the fiber.

where n_0 is the refraction index of the incident medium. Usually, the light is incident from air and $n_0 = 1$.

The light ray approach used to analyze light propagation in fiber is simple, but does not answer more detailed questions concerning the modes that could be coupled into the fiber. Instead, the wave propagation analysis in the cylindrical coordinate system should be used in order to answer these questions. In the cylindrical coordinate system, the wave equation for the electric or magnetic field can be expressed as [9–11]

$$\left[\frac{1}{r}\frac{d}{dr}r\frac{d}{dr} - \frac{\nu^2}{r^2} + k^2n^2(r=0) - \beta^2 - \left(\frac{V}{a}\right)^2 f\left[\left(\frac{r}{a}\right)^\alpha\right]\right]\psi = \epsilon\mu\frac{\partial^2\psi}{\partial t^2}, \tag{3.13}$$

where ν is the azimuthal index number, $f[(r/a)^\alpha]$ describes the index of refraction along the fiber's radius, a is the core radius, β is the propagation constant, and V is the modal volume, called also fiber's normalized frequency, given by

$$\begin{aligned} V &= \frac{2\pi an}{\lambda}\sqrt{2\Delta}, \\ \Delta &= \frac{n_1^2 - n_2^2}{2n_1^2}. \end{aligned} \tag{3.14}$$

The number of principal modes that can propagate in the fiber depends on the number of finite solutions to Eq.3.13. For a step-index fiber, shown in Fig.3.4 the number of principal modes is approximately equal to V for large V values [9].

Fig.3.5 shows an example of the three lowest transverse electric (TE_0, TE_1, and TE_2) mode field patterns in multimode fiber [12]. In the fundamental mode, almost all light energy is concentrated near the center of the

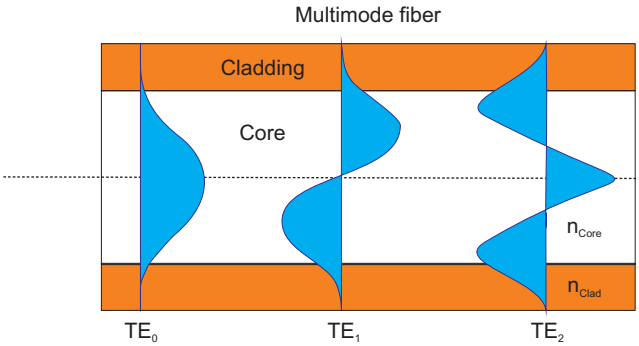

Figure 3.5: Three lowest transverse electric (TE_0, TE_1, and TE_2) mode field patterns in multimode fiber.

fiber. It is worth to notice that the higher modes are partially extending into the cladding. The refracted (out of the core into the cladding) modes are called cladding ones [12]. The cladding modes might get trapped in the cladding. If it happens, the fiber propagates two spatially separated mode groups: the core group and the cladding one, which might get coupled to one other by mode coupling (also exchange of power between the modes). Mode coupling causes power loss of the core modes. Finally, in a multimode fiber there is usually a third category of modes, called leaky ones. The leaky modes are the ones that are not totally reflected at the core-cladding boundary, but are instead refracted because of the curved nature of the boundary. The leaky modes, similarly to the cladding ones, contribute to power loss of the core modes.

3.3 Light propagation in single mode fiber

Fig.3.6 compares the older multimode fiber with the single mode (SM) fiber, widely used in telecom. The latter has a much lower diameter, compared to the first one. As it can be seen in Fig.3.4, at least a couple of modes with input angles less than the critical angle ϕ_c can be coupled into the multimode fiber. These modes would travel different path inside the fiber leading to distortion of the output signal. This is the reason for using SM fiber in the telecommunications since this fiber, with its much smaller diameter than the multimode one, couples only one mode. Fig.3.6 shows that the SM fiber has core radius approaching the light wavelength so diffraction effects should be considered, while analyzing the light propagation in the fiber. In reality, the light in the SM fiber propagates only along the fiber's axis. The cutoff modal

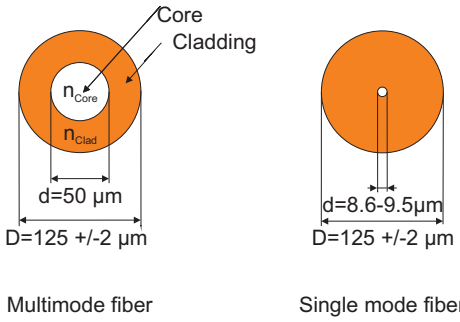

Figure 3.6: Multimode fiber profile versus the ITU-T G.652 recommendation for single mode fiber.

volume (fiber's normalized frequency) V, where only one mode is allowed to propagate in the fiber, is given by

$$V < 2.405. \tag{3.15}$$

A well designed SM fiber should have $V \preceq 2.405$ since for the low V values most of the energy of the fundamental mode propagates in the fiber's cladding, instead of in its core.

3.4 Attenuation

Fiber's attenuation A is usually defined as a unit of its length in km

$$A(dB/km) = \frac{10(\lg P_{in} - \lg P_{out})}{L}, \tag{3.16}$$

where L is the fiber's length in km, P_{in} is the power of optical signal coupled into the fiber, and P_{out} the optical output power. In Sec.3.2 two phenomena that cause optical power loss in fiber have already been mentioned: cladding and leaky modes. There are several other causes of optical power loss in fiber such as light absorption, intrinsic scattering, and bending losses which might occur if fiber bending redirects the light into the cladding [9].

Absorption leads to the optical energy exchange into heat. There are two main factors leading to light absorption in fiber: intrinsic absorption due to the basic properties of the fiber material; and extrinsic absorption caused by the fiber material impurity and structural defects, being mainly effect of an imperfect fiber draw process (such an imperfect process causes variations in the fiber diameter, which might result in the optical energy leakage from

the fiber's core into its cladding). Generally, the absorption losses are more difficult to control for fibers with a significantly increased difference between the refraction indices of the core and cladding, which leads to a increased light reflectivity on the core-cladding boundary [9, 13].

Intrinsic scattering in fiber, usually referred to as Rayleigh scattering, is mainly caused by variations of the core density (thermal fluctuations) leading to variations of the refraction index. Also concentration of dopant materials might vary along and across the fiber. These variations occur mainly during the manufacturing process. The scattering loss is given by [9]

$$\alpha = \frac{8\pi^3(n^2-1)KT\beta_{iso}}{3\lambda^4}, \tag{3.17}$$

where n is the material's index of refraction, k Boltzmann constant, T is the silica transitioning temperature (around 1770 K), β_{iso} is the isothermal compressibility, and λ the wavelength of the light. The Eq.3.17 shows that the scattering losses rapidly decrease with increasing wavelength.

Bending losses are divided, in regards to the bend radius curvature, into two categories: microbend and macrobend loss [9]. Microbends are small bends of the fiber axis caused mainly by imperfections (such as voids, particles or nonuniformities of the coating material) in the cabling material and cabling process. Also external forces can cause microbends. Macrobends might cause a severe optical power loss if the radius of curvature is less than $4-5$ cm. Such a bending causes light loss in the cladding.

Fig.3.7 shows how the fiber transmittance has been improved during last thirty years. The dashed curve shows the spectral attenuation of an early 1980's fiber, the dotted of an late 1980's fiber, and the solid of a modern optical fiber. The oldest fiber systems were using the so-called "first window" ($820-900$ nm) in which optical losses of about 3 dB/km are relatively low, but still substantial compared to the other windows. The "first window" is located between two regions of high optical losses caused mainly by moisture in the fiber and Rayleigh scattering. The "second window" ($1280-1350$ nm), also called S-band, provides much lower attenuation of about 0.5 dB/km, while the "third window" ($1528-1565$ nm), also called C-band, explored in 1977 by Nippon Telegraph and Telephone (NTT) offers the theoretically minimum optical loss for silica-based fibers of about 0.2 dB/km. The newest "forth window" ($1561-1620$ nm), also called L-band, with optical losses comparable to the 1550 nm window, was developed in the beginning of the current decade.

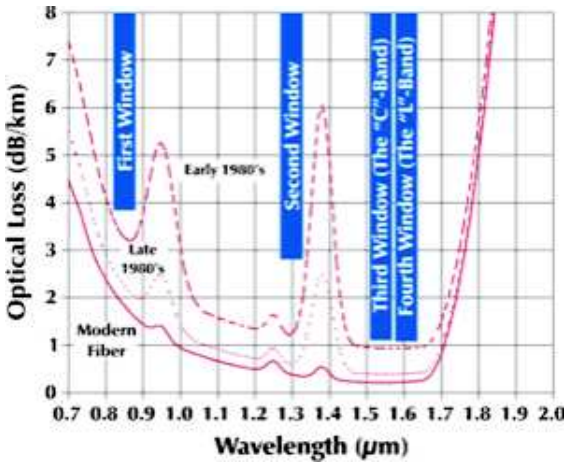

Figure 3.7: Typical spectral attenuation of Silica fiber. The dashed curve shows the spectral attenuation of an early 1980's fiber, the dotted of a late 1980's fiber, and the solid of a modern optical fiber. The figure courtesy to Fiber-Optics Info.

3.5 Dispersion

Dispersion causes the light pulse to widen out along the fiber it propagates over. The change of the wave's propagation constant for different modes is called a modal dispersion, while the change for different wavelengths is called a chromatic dispersion. Thus modal dispersion is dominant in multimode fibers and does not exist in SM fibers since the latter transmit the fundamental mode only. Since here we are mainly concerned about SM fibers let us focus on the chromatic dispersion, which usually is divided into two categories: material dispersion and wavelength dispersion [14].

The first one concerns dispersion caused by the material's dielectric constant and consequently its refractive index dependency on the light wavelength. The material dispersion can be easiest explained by taking into consideration a narrow light pulse (in the time-domain) consisting of a narrow range of wavelengths (in the frequency-domain). If the fiber's dielectric constant (and consequently its refractive index) is not flat (frequency independent in the entire frequency spectrum occupied by the pulse) then the pulse's different wavelength components exit the fiber at different times, which leads to a broadening of the pulse.

The wavelength dispersion concerns a nonlinear dependence of the propagation constant on the wavelength. Again, let us consider a narrow light

pulse (in the time-domain) consisting of a narrow range of wavelengths (in the frequency-domain). If the propagation constant shows a nonlinear dependence on frequency then, similarly to the material dispersion, the pulse's different wavelength components exit the fiber at different times, which leads to a broadening of the pulse. The wavelength dispersion can easiest be explained taking into consideration the phase propagation constant in fiber β

$$\beta = n_{eff}\beta_0, \tag{3.18}$$

where n_{eff} is the effective refractive index and

$$\beta_0 = \frac{2\pi}{\lambda_0} = \frac{\omega}{c} \tag{3.19}$$

is the light's propagation constant in vacuum.
Here, in the discussion on dispersion in fiber, we will be rather using the phase propagation constant β then the wavenumber. This approach is customary in fiber transmission's analysis, while the wavenumber refers rather to a plane wave propagation in free-space.

The effective refractive index in fiber is a function of the wavelength. As already mentioned, the wavelength dispersion occurs in the case the function is nonlinear. It should be pointed out that the effective refractive index depends not only on the wavelength but also on the light's mode in fiber. Therefore, it is also called modal index.
Also the phase and group velocities are functions of the effective refractive index and are given by

$$v_p = \frac{c}{n_{eff}}, \tag{3.20}$$

$$v_g = \frac{d\omega}{d\beta}. \tag{3.21}$$

Since

$$\beta = \frac{n_{eff}\omega}{c} \tag{3.22}$$

we are getting

$$\frac{1}{v_g} = \frac{d\beta}{d\omega} = \frac{1}{c}\left[n_{eff}(\omega) + \omega\frac{dn_{eff}}{d\omega}\right] = \frac{1}{c}\left[n_{eff}(\lambda_0) - \lambda_0\frac{dn_{eff}}{d\lambda_0}\right] = \frac{n_g}{c}, \tag{3.23}$$

where λ_0 is the wavelength in free-space and n_g is the group refractive index [15]

$$n_g = n_{eff}(\lambda_0) - \lambda_0 \frac{dn_{eff}}{d\lambda_0}. \tag{3.24}$$

The group velocity dispersion (GVD) is a second derivate of the propagation constant in fiber

$$GVD = \frac{d^2\beta}{d\omega^2}. \tag{3.25}$$

The coefficient D (known also as the chromatic dispersion coefficient) of the group velocity dispersion (GVD) is defined as the variation of travel time (per unit length of fiber) due to the wavelength variation [14]

$$D = \frac{1}{L}\frac{d\tau}{d\lambda_0}, \tag{3.26}$$

where L is the fiber's length and the travel time τ for a group of velocity propagating over the fiber's length L is given by

$$\tau = \frac{L}{v_g} = L\frac{d\beta}{d\omega}. \tag{3.27}$$

By substituting Eq.3.24 into Eq.3.27 we are getting

$$\tau(\lambda_0) = \frac{L}{v_g} = \frac{L}{c}\left(n_{eff}(\lambda_0) - \lambda_0 \frac{dn_{eff}}{d\lambda_0}\right). \tag{3.28}$$

By substituting Eq.3.28 into Eq.3.26 and calculating the derivate we are getting

$$D = \frac{1}{L}\frac{d\tau}{d\lambda_0} = -\frac{\lambda_0}{c}\frac{d^2 n_{eff}}{d\lambda_0^2}. \tag{3.29}$$

Finally, the pulse broadening $\Delta\tau_m$, often called material dispersion (due to its dependence on the material's properties, is given by [14]

$$\Delta\tau_m = \Delta\lambda_s \frac{d\tau}{d\lambda_0}, \tag{3.30}$$

where $\Delta\lambda_s$ is the spectral width of the source. By substituting Eq.3.28 into Eq.3.30 the pulse broadening $\Delta\tau_m$ becomes

$$\Delta\tau_m = \frac{d\tau}{d\lambda_0}\Delta\lambda_s = -\frac{L\lambda_0}{c}\frac{d^2 n_{eff}}{d\lambda_0^2}\Delta\lambda_s. \tag{3.31}$$

Fig.3.8 compares material dispersion for silica with dispersion of two commercial telecom fibers, the first one used in the second telecom window of 1310 nm and the second one in the third telecom window of 1550 nm (see Fig.3.7). Pure silica features zero dispersion at 1270 nm, called the zero dis-

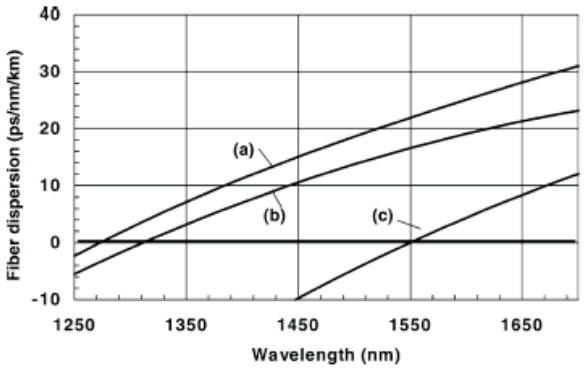

Figure 3.8: Dispersion as a function of wavelength. (a) material dispersion for silica; (b) standard single-mode fiber (SMF); (c) dispersion in dispersion shifted fiber (DSF) [16].

persion wavelength. By changing the fiber core's transverse refractive index profile, the zero dispersion wavelength can be shifted to the third telecom window of 1550 nm (see Fig.3.7). As already mentioned, SM fiber dispersion is due to the fact that the spot size of the mode is a function of the wavelength. Therefore, the ratio between the power in the core and in the cladding changes with the wavelength.

The telecom as well as quantum information systems should use wavelengths close to the fiber's zero dispersion wavelength in order to reduce the dispersive broadening of the transmitted pulses. For the telecom signals of usually much higher power than the single photon power level used in quantum information, fiber's optical nonlinearities might cause a undesirable four-wave mixing, limiting the transmission distance. In order to avoid it a special non-zero dispersion shifted fiber (NZ-DSF), providing a finite dispersion in the third telecom window was designed. Since dispersion limits both the transmission rates and secure transmission distance of the quantum information system it will be more discussed in Chap.6.

3.6 Polarization

Analysis of polarization development of single photons propagating over fiber links and of polarization of fiber components is crucial for description of multi-user QKD and multi-party secret sharing over fiber. Therefore, a significant part of the thesis has been dedicated to it.

3.6.1 The polarization ellipse

Polarization of a plan wave, propagating along z-axis and consisting of only two orthogonal electric field vectors $\mathbf{E_x}$ and $\mathbf{E_x}$

$$\begin{aligned} E_x(z,t) &= E_{0x}\cos(\omega t - kz + \delta_x), \\ E_y(z,t) &= E_{0y}\cos(\omega t - kz + \delta_y), \end{aligned} \tag{3.32}$$

where E_{0x}, E_{0y} are amplitudes and δ_x, δ_y phases of the horizontal and vertical electric fields, respectively, and $\delta = \delta_x - \delta_y$; $k = 2\pi/\lambda$ is the wave number magnitude;

is described by the polarization ellipse equation [17]

$$\frac{E_x(z,t)^2}{E_{0x}^2} + \frac{E_y(z,t)^2}{E_{0y}^2} - \frac{2E_x(z,t)E_y(z,t)}{E_{0x}E_{0y}}\cos\delta = \sin^2\delta. \tag{3.33}$$

Fig.3.9 shows the polarization ellipse, which describes a general case of the

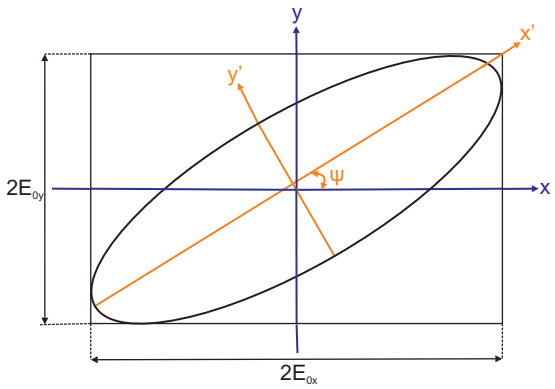

Figure 3.9: Polarization ellipse. E_{0x}, E_{0y} are amplitudes of the horizontal and vertical electric fields, respectively; x', y' rotated coordinates.

polarized light. However, in the literature on light polarization, some special

E_{0x}	E_{0y}	δ	Polarization
E_{0x}	0	0	Horizontal
0	E_{0y}	0	Vertical
E_0	E_0	0	Diagonal ($+45°$)
E_0	E_0	π	Antidiagonal ($-45°$)
E_0	E_0	$\pi/2$	Right circular
E_0	E_0	$-\pi/2$	Left circular

Table 3.1: Degenerate polarization states.

important polarization cases, called degenerative polarization states, shown in the Tab.3.1, are often cited.

The polarization ellipse equation (Eq.3.33) can easily be reexpressed as a function of the orientation angle ψ and the ellipticity angle χ

$$\begin{aligned} \tan 2\psi &= \frac{2E_{0x}E_{0y}}{E_{0x}^2 - E_{0y}^2}\cos\delta, \\ \sin 2\chi &= \frac{2E_{0x}E_{0y}}{E_{0x}^2 + E_{0y}^2}\sin\delta, \\ 0 \le \psi \le \pi,\ &-\pi/4 \le \chi \le \pi/4. \end{aligned} \tag{3.34}$$

It should be pointed out that the polarization ellipse is very helpful in visualization of degenerate states of the polarized light. For a more general polarization state, there is no easy way to determine the orientation angle ψ and ellipticity angle χ. Furthermore, the procedure of calculating the orientation angle and ellipticity angle needs to be repeated for every new optical polarizing component added to the optical setup. A Poincaré sphere approach, described in the next section, has resolved some of the above mentioned problems.

3.6.2 Polarized light representation on the Poincaré sphere

In 1892, H. Poincaré published a convenient way to represent polarized light by using a sphere of the unity radius as shown in Fig.3.10 [17]. The figure shows that any polarization can be represented by a point P on the sphere. Since the sphere has an unit radius the Cartesian coordinates are related to

the spherical ones as below

$$\begin{aligned} x &= \cos(2\chi)\cos(2\psi), \\ y &= \cos(2\chi)\sin(2\psi), \\ z &= \sin(2\chi), \end{aligned} \tag{3.35}$$

where $x^2 + y^2 + z^2 = 1$ and $0 \leq \psi < \pi, -\pi/4 < \chi < \pi/4$.

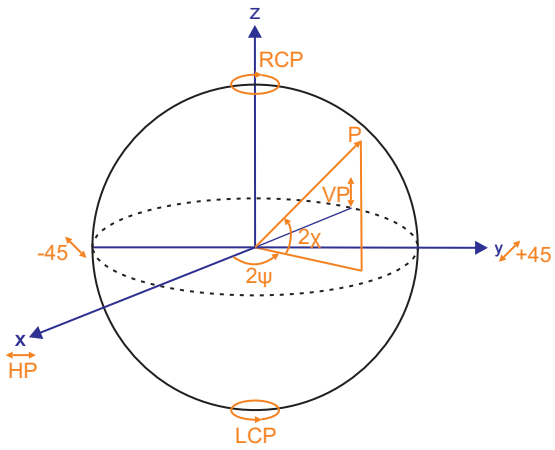

Figure 3.10: Polarized light representation on the Poincaré sphere. HP: Horizontal Polarization; VP: Vertical Polarization; RCP: Right Circular Polarization; LCP: Left Circular Polarization.

Fig.3.10 shows also the degenerate polarization states on the Poincaré sphere corresponding to the spherical coordinates $(2\psi, 2\chi)$: RCP: Right Circular Polarization for $(0, +90°)$; LCP: Left Circular Polarization $(0, -90°)$; HP: Horizontal Polarization $(0, 0)$; VP: Vertical Polarization $(+180°, 0)$; +45: Diagonal Polarization $(+90°, 0)$, and −45: Antidiagonal Polarization $(+270°, 0)$. It should be emphasized that all linear polarizations states lie on the sphere's equator, while the right and left circular polarizations are located on the north and south poles, respectively. All remaining sphere points correspond to the elliptical polarization states. Both Poincaré sphere and polarization ellipse suffer from the same problem: neither the orientation angle nor the ellipticity angle are directly measurable. The problem of determining measurables of the polarized light is discussed in the next section.

3.6.3 Stokes polarization parameters

The George Stokes parameters (published in 1852), being observables of the electromagnetic wave, provide a very useful description of the light's polarization state. In order to find the observables, the polarization ellipse equation 3.33 should be time averaged. The time average $\langle E_x(z,t)E_y(z,t)\rangle$ is defined by [17]

$$\langle E_x(z,t)E_y(z,t)\rangle = \lim_{T\to\infty}\frac{1}{T}\int_0^T E_x(z,t)E_y(z,t)dt, \tag{3.36}$$

where T is the total averaging time. Taking $z = 0$ and multiplying both sides of Eq.3.33 by $(2E_{0x}E_{0y})^2$ leads to

$$\begin{aligned} 4E_{0y}^2\langle E_x(t)^2\rangle + 4E_{0x}^2\langle E_y(t)^2\rangle - 8E_{0x}E_{0y}\langle E_x(t)\rangle\langle E_y(t)\rangle\cos\delta \\ = (2E_{0x}E_{0y}\sin\delta)^2. \end{aligned} \tag{3.37}$$

Averaging Eq.3.32 gives

$$\begin{aligned} \langle E_x(t)^2\rangle &= \frac{1}{2}E_{0x}, \\ \langle E_y(t)^2\rangle &= \frac{1}{2}E_{0y}, \\ \langle E_x(t)\rangle\langle E_x(t)\rangle &= \frac{1}{2}E_{0x}E_{0y}\cos\delta. \end{aligned} \tag{3.38}$$

By substituting Eq.3.38 into Eq.3.37 we are getting

$$4E_{0x}^2E_{0y}^2 - (2E_{0x}E_{0y}\cos\delta)^2 = (2E_{0x}E_{0y}\sin\delta)^2, \tag{3.39}$$

which by adding and subtracting the terms $E_{0x}^4 - E_{0y}^4$ leads to

$$(E_{0x}^2 + E_{0y}^2)^2 - (E_{0x}^2 - E_{0y}^2)^2 - (2E_{0x}E_{0y}\cos\delta)^2 = (2E_{0x}E_{0y}\sin\delta)^2. \tag{3.40}$$

Finally, the Stokes parameters are found by assigning them to the parentheses in the Eq.3.40

$$\begin{aligned} S_0 &= E_{0x}^2 + E_{0y}^2, \\ S_1 &= E_{0x}^2 - E_{0y}^2, \\ S_2 &= 2E_{0x}E_{0y}\cos\delta, \\ S_3 &= 2E_{0x}E_{0y}\sin\delta, \end{aligned} \tag{3.41}$$

which fulfill the following relation [17]

$$S_0^2 = S_1^2 + S_2^2 + S_3^2. \tag{3.42}$$

The parameter S_0 corresponds to the total light intensity. S_1, S_2, and S_3 correspond to difference between the intensities of the horizontal and vertical, the diagonal and antidiagonal, and the right and left circular polarizations, respectively. They can be easily measured by using a simple setup [17], shown in Fig.3.11, consisting of two polarizing elements: a wave plate providing a phase shift ϕ between the horizontal and vertical electric field components and a polarizer rotated, with the angle θ, from the x-axis. It is easy to show (by simply substituting $\theta = 0,\ \pi/4,\ \pi/2$ and $\phi = 0, \pi/2$ into the equation below) that the by the detector measured light intensity $I(\theta, \phi)$ fulfills [17]

$$I(\theta, \phi) = \frac{1}{2}(S_0 + S_1 \cos 2\theta + S_2 \sin 2\theta \cos \phi - S_3 \sin 2\theta \sin \phi). \tag{3.43}$$

By rewriting the Eq.3.43 we are getting the following relations between the

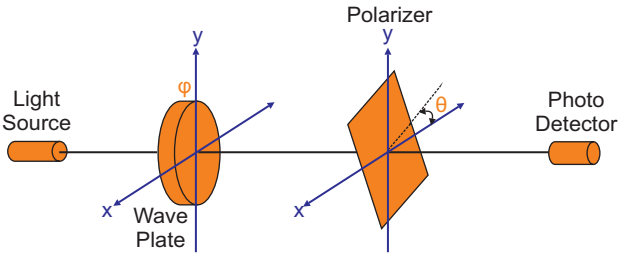

Figure 3.11: Measuring the Stokes parameters. ϕ is the phase difference between the horizontal and vertical electric field components, introduced by the wave plate. θ is the angle between the polarizer's transmission axis and the x-axis. $I(\theta, \phi)$ is the measured light intensity by the photodetector.

measured light intensity $I(\theta, \phi)$ and the Stokes parameters

$$\begin{aligned} S_0 &= E_{0x}^2 + E_{0y}^2 = I(0,0) + I(\pi/2, 0), \\ S_1 &= E_{0x}^2 - E_{0y}^2 = I(0,0) - I(\pi/2, 0), \\ S_2 &= 2E_{0x}E_{0y}\cos\delta = 2I(\pi/4, 0) - S_0, \\ S_3 &= S_0 - 2I(\pi/4, \pi/2). \end{aligned} \tag{3.44}$$

The Eq.3.44 shows that only three measurements, based on rotating the polarizer to $\theta = 0,\ \pi/4$ and $\pi/2$, are needed in order to find the Stokes

parameters S_0, S_1, and S_2. To find the parameter S_3 there is a need of introducing the phase shift $\phi = \pi/2$ (between the horizontal and vertical electric field components) with the aid of the wave plate.

3.6.4 Mueller and Jones calculus

Stokes parameters, as being observables, and their visualization on the Poincaré sphere have proved to be very useful in simple optical implementations, consisting of a single or a few optical components. In case of more complicated setups determination of the output polarization becomes a cumbersome process. To overcome these difficulties a number of different methods have been developed. The most known methods are Mueller calculus and Jones calculus. Here, we are most concerned about the last one since it has been widely used both in the thesis and in the Paper V. Therefore, the Mueller calculus will be only briefly presented.

In the Mueller calculus the optical component is represented by a 4×4 matrix M, with all elements real, while the input and output polarization states are represented by four-component Stokes vectors $\mathbf{S_{in}}$ and $\mathbf{S_{out}}$, respectively:

$$\mathbf{S_{out}} = \begin{pmatrix} m_{00} & m_{01} & m_{02} & m_{03} \\ m_{10} & m_{11} & m_{12} & m_{13} \\ m_{20} & m_{21} & m_{22} & m_{23} \\ m_{30} & m_{31} & m_{32} & m_{33} \end{pmatrix} \mathbf{S_{in}}, \tag{3.45}$$

where the Stokes vectors $\mathbf{S_{out}}$ and $\mathbf{S_{in}}$ are given by

$$\mathbf{S_{out}} = \begin{pmatrix} S_{0_{out}} \\ S_{1_{out}} \\ S_{2_{out}} \\ S_{3_{out}} \end{pmatrix} \qquad \mathbf{S_{in}} = \begin{pmatrix} S_{0_{in}} \\ S_{1_{in}} \\ S_{2_{in}} \\ S_{3_{in}} \end{pmatrix}. \tag{3.46}$$

Using only three polarization components: a polarizer, a retarder, and a rotator; any elliptical polarization state, described by the polarization ellipse equation (Eq.3.33), can be obtained. The Mueller matrix for the linear polarizer with the absorption coefficients $0 \leq p_x \leq 1$ and $0 \leq p_y \leq 1$ (0 represents here a total absorption, while 1 a total transmission) is given by [17]

$$M_{POL} = \frac{1}{2} \begin{pmatrix} p_x^2 + p_y^2 & p_x^2 - p_y^2 & 0 & 0 \\ p_x^2 - p_y^2 & p_x^2 + p_y^2 & 0 & 0 \\ 0 & 0 & 2p_x p_y & 0 \\ 0 & 0 & 0 & 2p_x p_y \end{pmatrix}. \tag{3.47}$$

The Mueller matrix for the wave plate is given by

$$M_{WP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix}, \tag{3.48}$$

where ϕ is the phase shift between the horizontal and vertical electric field. Two important cases should be mentioned here: the quarter-wave plate (QWP) for $\phi = \pi/2$

$$M_{QWP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{3.49}$$

and the half-wave plate (HWP) for $\phi = \pi$

$$M_{HWP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{3.50}$$

The QWP transforms diagonal ($+45°$) to RCP light and antidiagonal ($-45°$) to LCP light, while the HWP reverses the orientation angle ψ and ellipticity angle χ (see Sec.3.6.1).

The Mueller matrix for the rotator is given by

$$M_{ROT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos 2\theta & \sin 2\theta & 0 \\ 0 & -\sin 2\theta & \cos 2\theta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{3.51}$$

where θ is the rotation angle. It can easily be showed that rotators only rotate the polarization ellipse, characterized by the orientation angle ψ, while they do not change the ellipticity, characterized by the angle χ.

While all the Mueller's matrix elements are real, the Jones 2×2 matrix's elements are generally complex. The input and output electric fields of the polarizing component are in the Jones calculus described by 2×1 Jones vectors

$$\mathbf{E_{out}} = \begin{pmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{pmatrix} \mathbf{E_{in}}, \quad \mathbf{E_{in}} = \begin{pmatrix} E'_{0x} e^{i\delta'_x} \\ E'_{0y} e^{i\delta'_y} \end{pmatrix}, \quad \mathbf{E_{out}} = \begin{pmatrix} E''_{0x} e^{i\delta''_x} \\ E''_{0y} e^{i\delta''_y} \end{pmatrix}, \tag{3.52}$$

where $E_{0x}^{'}$, $E_{0y}^{'}$; $E_{0x}^{''}$, $E_{0y}^{''}$ are the input and output amplitudes, respectively and $\delta_x^{'}, \delta_y^{'}$; $\delta_x^{''}, \delta_y^{''}$ the input and output phases. Thus, both the vectors and matrix are smaller than the respective Mueller elements, which seems to be the Jones calculus' advantage over the Mueller one. However, the Jones calculus cannot be used for description of unpolarized or partly polarized light, while the Mueller calculus, based on Stokes parameters does not have this limitation. The Jones calculus allows also to easily find the light intensity

$$I = \begin{pmatrix} E_x^* & E_y^* \end{pmatrix} \begin{pmatrix} E_x \\ E_y \end{pmatrix}, \tag{3.53}$$

where E_x^* and E_y^* are complex conjugates of the electric field components E_x and E_y.

Tab.3.2 shows the Jones vectors for degenerative polarization states, while the Tab.3.3 shows the Jones matrices for a couple of common polarizing components.

Jones Vector	Polarization	Jones Vector	Polarization
$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	Horizontal	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	Vertical
$1/\sqrt{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	Diagonal (+45°)	$1/\sqrt{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$	Antidiagonal (−45°)
$1/\sqrt{2}\begin{pmatrix} 1 \\ i \end{pmatrix}$	Right circular	$1/\sqrt{2}\begin{pmatrix} 1 \\ -i \end{pmatrix}$	Left circular

Table 3.2: Jones vectors for degenerate polarization states.

Jones Vector	Polarization	Jones Vector	Polarization
$\begin{pmatrix} p_x & 0 \\ 0 & p_y \end{pmatrix}$ $0 \leq p_x, p_y \leq 1$	Linear polarizer	$\begin{pmatrix} e^{-i(\frac{\phi}{2})} & 0 \\ 0 & e^{i(\frac{\phi}{2})} \end{pmatrix}$ $E_{0x} = E_{0y} = 1$	Wave plate
$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$	Quarter wave plate	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Half wave plate
$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$	Rotator	$\begin{pmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix}$	Rotated horizontal polarizer

Table 3.3: Jones matrices for common polarizing components.

3.6.5 Birefringence in fiber

Two types of birefringence could be found in fibers: intrinsic and induced. The intrinsic birefringence is caused by the fiber core's inner anisotropies, shape, and stress. The induced birefringence occurs when a fiber is under influence of external forces or fields, for instance when it is twisted, bent, or pressed. Fig.3.12 shows a stress-induced birefringence. The stress causes the input's vertically polarized light to change polarization to the REP (Right Elliptical Polarization), with the horizontal component delay by the phase δ in regards to the vertical one.

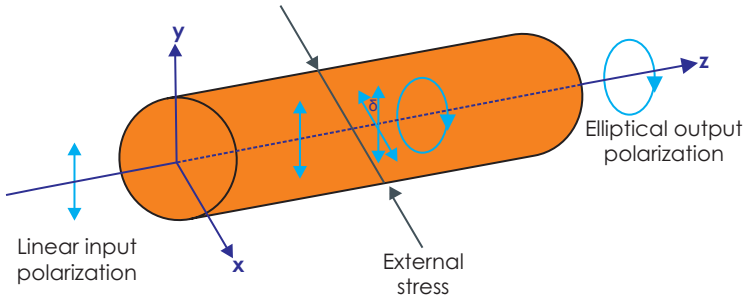

Figure 3.12: Stress-induced birefringence. The stress causes the input's vertically polarized light to change polarization to the REP (Right Elliptical Polarization), with the horizontal component delay by δ in regards to the vertical one.

3.6.6 Polarization maintaining fibers

There are a couple of different technologies for manufacturing polarization maintaining fibers. Among them, the Panda fiber produced by Fujikura Inc. shows the best polarization stability and lowest losses. The Panda fiber utilizes a rotationally asymmetrical intrinsic stress, induced by special stress rods, equally spaced along the fiber (see Fig.3.13). Due to the photoelastic effect, the intrinsic stress changes refractive indices for two orthogonal birefringent axes

$$B = \mid \Delta n \mid, \qquad (3.54)$$
$$\Delta n = n_x - n_y = c(\sigma_x - \sigma_y),$$

where B is the degree of birefringence, c is the photoelastic constant, σ_x and σ_y are the uniaxial strains applied parallel to the axis x and y, respectively [9]. In order to preserve polarization of the light propagating over the polarization maintaining fiber, the intrinsic stress should be much higher than the potential external stress in form of the fiber's bending or pressing. In reality, there will be always some "cross-talk" polarization component at the fiber's output. In order to characterize the "cross-talk", i.e. measure fiber's ability to preserve the polarization, a special parameter, called PER (polarization extinction ratio), is commonly used

$$PER = 10 \log \frac{P_x}{P_y} \text{ for } P_{in} = P_x, \qquad (3.55)$$
$$PER = 10 \log \frac{P_y}{P_x} \text{for } P_{in} = P_y,$$

where $P_{in} = P_x$, $P_{in} = P_y$ denotes the input's SOP (state of polarization).

Fig.3.14 shows a cross-section of the Panda fiber and the refractive index profile along the x-axis. Due to its high value at the fiber's core the x-component of electric field vector propagates slower than the y-component. Thus, the x-axis is called the slow and the y-axis fast.

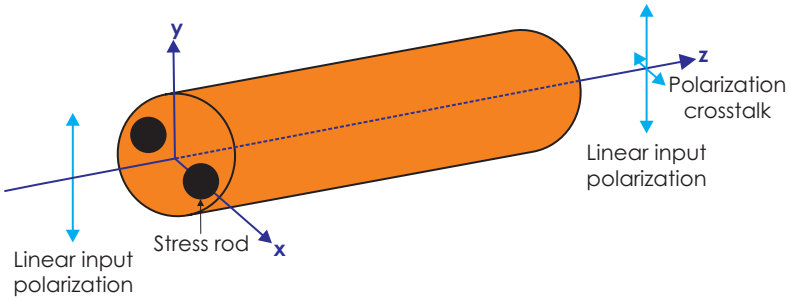

Figure 3.13: Panda fiber with a high intrinsic birefringence (much higher than externally stress-induced birefringence). The black filled circles show the stress-rods, used for inducing a high intrinsic birefringence.

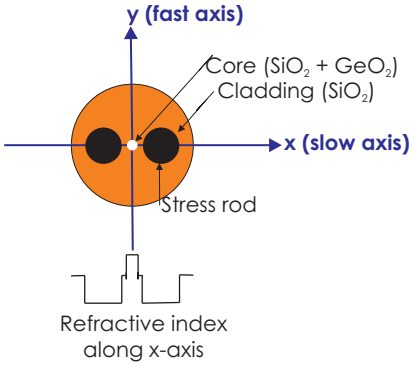

Figure 3.14: Cross-section of the Fujikura's Panda fiber. The black filled circles show the stress-rods, used for inducing a high intrinsic birefringence.

3.7 Fiber dependency on mechanical strain and temperature

Since both transmission lines, considered in the thesis, and the optocomponents used in transmitting and receiving stations are fiber-based, there is a need to consider influence of mechanical strain and temperature on fiber transmittance. In this section, these factors will be shortly described, using simple mathematical models. In detail, let us consider a fiber of the length L. A light beam with the wavelength λ, passing through a fiber with the core refractive index n of the length L, is phase delayed at the fiber's output

by [9]

$$\phi = knL = 2\pi nL/\lambda, \tag{3.56}$$

where $k = 2\pi/\lambda$ is the light's wavenumber and the typical value for the multimode fiber's core refractive index $n = 1.46$. Small variation in the phase delay is given by

$$\frac{\Delta\phi}{\phi} = 2\pi(\frac{\Delta n}{n} + \frac{\Delta L}{L} + \frac{\Delta\lambda}{\lambda}). \tag{3.57}$$

The first term describes a potential fiber birefringence influence on the propagating light (but temperature could also influence the refractive index). For instance, one of the beam could propagate slower than the other one due to the difference in the refractive index n caused by birefringence, more detailed described in Sec.3.6.5. The second term describes the fiber's environmental factors such as temperature, mechanical pressure, and strain. The last term concerns instability of the light source, including phase jitter.

3.7.1 Mechanical strain

Small phase changes in Eq.3.56 are given by

$$d\phi = kd(nL) = k(ndL + Ldn) = kL\left(n\frac{dL}{L} + dn\right), \tag{3.58}$$

where the first term, being the fiber mechanical strain, correspond to a fiber length change and the second one to a change of the refractive index n. It might be shown that the fiber's phase response $d\phi$ to the axial mechanical strain dL is given by [9]

$$d\phi = k\xi ndL, \tag{3.59}$$

where $k = 2\pi/\lambda$ is the wavenumber in vacuum, n is the refractive index of the fiber core, and ξ is the strain optic correction factor given by

$$\xi = 1 - \frac{1}{2}n^2[(1-\nu)p_{12} - \nu p_{11}], \tag{3.60}$$

where Poisson's ratio ν, being the ratio of the relative contraction strain (or transverse strain, normal to the applied load) to the relative extension strain (or axial strain) in the direction of the applied load ($\nu \approx 0.4$ for fiber), p_{11} and p_{12} elements of the strain optic tensor (Pockel's coefficients) of the fiber. Typically, $\xi \sim 0.78$ in silica glass fibers [9].

3.7.2 Temperature dependency

Eq.3.58 can be rewritten as a function of the phase change in regards to temperature

$$\frac{d\phi}{dT} = k\left(n\frac{dL}{dT} + L\frac{dn}{dT}\right) = kL\left(\frac{n}{L}\frac{dL}{dT} + \frac{dn}{dT}\right), \tag{3.61}$$

where the first term describes the thermal length change and the second one the thermal change of the refractive index. For a typical silica fiber $\frac{1}{L}\frac{dL}{dT} \sim 5 \times 10^{-7}$ K^{-1} and $\frac{dn}{dT} \sim 10^{-5}$ K^{-1} so the thermal length change can be omitted [9]. However, for a fiber with a nylon jacket of 1 mm in diameter the first term $\frac{1}{L}\frac{dL}{dT} \sim 6.5 \times 10^{-5}$ K^{-1} dominates.

Chapter 4

Classical and quantum interferometry in fiber

4.1 Introduction

The experimental work, presented in this thesis, has been performed in fiber. Thus, the thesis is dedicated to fiber physics. Therefore, also the current chapter concerns interferometry in fiber only. Since the experimental multiparty QKD and secret sharing, described in Papers I-IV, have been based on the "plug & play" and Sagnac interferometric setups, the main focus here will be put on them. Also Mach-Zehnder interferometer will be discussed in the first section of the chapter. Putting the "plug & play" setup into the section on classical interferometry might look odd, but there is really no reason for avoiding its analysis at a classical signal level.

4.2 Classical interferometry in fiber

4.2.1 Two-beam fiber interferometry

Generally, there are three conditions for high interference visibility of two light beams: their equal amplitudes, stable phase difference, and equal polarizations. Also the light source's coherence length should be considered while analyzing the interference's visibility (see Eq.4.1). The conditions will be in detail discussed in the next section, where an example of a general classical interference in the fiber Mach-Zehnder interferometer is presented.

4.2.2 Mach-Zehnder interferometer

In 1891 L. Zehnder and in 1892 L. Mach separately described what has become known as the Mach-Zehnder interferometer, which could monitor changes in refractive index, and hence density, in compressible gas flows. This over one hundred years old interferometer is still used in a variety of optical instruments. The interferometer is analyzed here since its model well describes general interferometric phenomena. Fig.4.1 shows the classical Mach-Zehnder interferometer in free-space and Fig.4.2 its fiber equivalence.

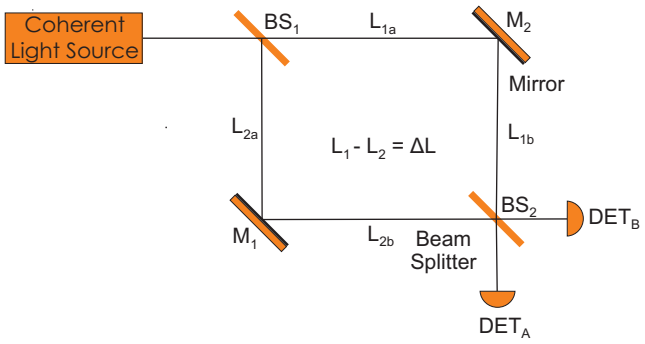

Figure 4.1: Mach-Zehnder interferometric setup in free-space.

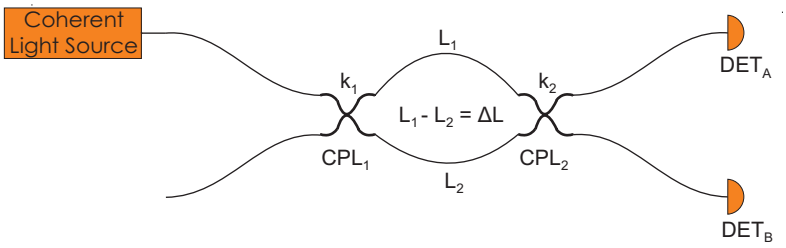

Figure 4.2: Mach-Zehnder interferometric setup in fiber.

The interferometer will be analyzed assuming no birefringence and that the differential propagation delay between the arms fulfills the condition [9, 18]

$$\tau_d \ll \tau_c, \tag{4.1}$$

where

$$\tau_c = c/\Delta f, \tag{4.2}$$

is the light source coherence time, c is the speed of light, and Δf is the spectral width of the light source.

The electric fields at the detector DET_A (see Fig.4.2) are given by

$$E_{A_1} = E_0\sqrt{\alpha_1 k_1 k_2}\cos(\omega_0 t + \phi_1) \tag{4.3}$$

for the electric field propagating over the upper arm L_1 and

$$E_{A_2} = E_0\sqrt{\alpha_2(1-k_1)(1-k_2)}\cos(\omega_0 t + \phi_2) \tag{4.4}$$

for the electric field propagating over the lower arm L_2,
where $E = E_0\cos(\omega_0 t)$ is the source electric field, k_1 and k_2 are the power coupling coefficients of the couplers, α_1 and α_2 are the optical losses in the arms L_1 and L_2, respectively. Similarly, the electric fields at the detector DET_B are given by

$$E_{B_1} = E_0\sqrt{\alpha_1 k_1(1-k_2)}\cos(\omega_0 t + \phi_1), \tag{4.5}$$

$$E_{B_2} = E_0\sqrt{\alpha_2(1-k_1)k_2}\cos(\omega_0 t + \phi_2). \tag{4.6}$$

The output intensities I_A and I_B at the detectors DET_A and DET_B are given by averaging the electric fields over a period much longer than $2\pi/\omega_0$ [9]

$$I_A = \langle E_{A_1}^2\rangle + \langle E_{A_2}^2\rangle + \langle E_{A_1}E_{A_2}\rangle, \tag{4.7}$$

$$I_B = \langle E_{B_1}^2\rangle + \langle E_{B_2}^2\rangle + \langle E_{B_1}E_{B_2}\rangle. \tag{4.8}$$

By substituting Eq.4.3, Eq.4.4, Eq.4.5, and Eq.4.6 into Eq.4.7 and Eq.4.8 we are finally getting

$$I_A = I_0[\alpha_2 k_1 k_2 + \alpha_1(1-k_1)(1-k_2) + 2\sqrt{\alpha_1\alpha_2 k_1 k_2(1-k_1)(1-k_2)}\cos\Delta\phi], \tag{4.9}$$

$$I_B = I_0[\alpha_2 k_1(1-k_2) + \alpha_1(1-k_1)k_2 + 2\sqrt{\alpha_1\alpha_2 k_1 k_2(1-k_1)(1-k_2)}\cos\Delta\phi], \tag{4.10}$$

where $\Delta\phi = \phi_1 - \phi_2$.

It is worth to notice that generally the interferometer's output signals have different visibilities

$$V_A = \frac{2\sqrt{\alpha_1\alpha_2 k_1 k_2(1-k_1)(1-k_2)}}{\alpha_2 k_1 k_2 + \alpha_1(1-k_1)(1-k_2)}, \tag{4.11}$$

$$V_B = \frac{2\sqrt{\alpha_1\alpha_2 k_1 k_2(1-k_1)(1-k_2)}}{\alpha_2 k_1(1-k_2)+\alpha_1(1-k_1)k_2}, \tag{4.12}$$

where the visibility is defined as below

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}. \tag{4.13}$$

In the case of the same optical losses ($\alpha_1 = \alpha_2 = \alpha$) in the arms L_1 and L_2 and the same power coupling coefficients ($k_1 = k_2 = k$) of the couplers the output intensities I_A and I_B at the detectors DET_A and DET_B simplifies to

$$I_A = \frac{I_0\alpha}{2}(1+\cos\Delta\phi), \tag{4.14}$$

$$I_B = \frac{I_0\alpha}{2}(1-\cos\Delta\phi). \tag{4.15}$$

Thus, both interferometer's output visibilities become equal one.

4.2.3 "Plug & play" interferometric setup

The "plug & play" interferometric setup [19] (described in Paper I, Paper II, and Paper V) has gained its popularity in the QKD applications. The setup has been described and analyzed for the single photon level laser pulses. Here, it is presented without this limitation, as a long ("extended by the SM fiber link") general classical interferometer. Fig.4.3 shows the interferometer with two phase modulators (PM_A and PM_B) at Alice's and Bob's station, respectively.

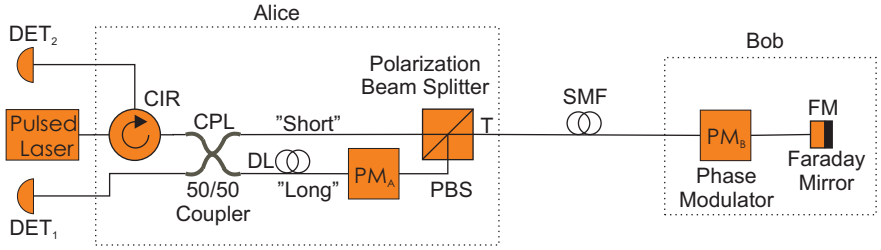

Figure 4.3: "Plug & play" interferometric setup.

In detail, a laser pulse is sent through the circulator CIR to the 50/50 coupler CPL that splits it into two pulses propagating through a short arm

and a long arm (that includes the delay line DL and the phase modulator PM_A), respectively. The phase modulator PM_A should be kept inactive during the pulse passage over the long arm. The pulses arrive to a polarization beam splitter (PBS) and leave the interferometer INT by the same PBS port (T): the long arm pulse vertically and the short one horizontally polarized. Then, the long arm and short arm pulses are transmitted over SM fiber link into Bob's station, where they are reflected at the Faraday mirror (that rotates their polarizations by 90°), and transmitted back into Alice's station. The phase modulator PM_B should modulate the long arm pulse only (it should be kept inactive during the short arm pulse's forward passage towards the Faraday mirror and backwards passage towards Alice's station). Both pulses continue their backward propagation over the SM fiber link and are directed by the PBS into the opposite arms (in regards to their forward propagation) of the interferometer INT so they arrive at the same time to the coupler CPL, where they interfere. Depending on the phase difference between the long arm pulse and the short one (that is modulated by the phase modulator PM_A on its backward way to the coupler CPL) they are detected either in the detector DET_2 (if the phase difference $\varphi = 0 \pm 2n\pi$, where n is an integer number); or in DET_1 (if $\varphi = \pi \pm 2n\pi$); or in both detectors for other φ values.

Assuming the "plug & play" system's stability in regards to birefringence and attenuation during its total (forward and backward) propagation time, it automatically provides the same propagation time for the long arm and short arm pulses since they travel the same path length. For the very same reason, the pulses arrive to the coupler CPL at the same amplitude. For a high interference visibility, there is one more condition for the pulses: the long arm pulse should arrive to the PBS horizontally and the short arm vertically polarized (they left the PBS at the opposite polarizations). Thus, the SM fiber link's birefringence should be analyzed in order to find how it influences the polarization change of the pulses.

The "plug & play" interferometer's birefringence will be analyzed here by using the Kapron equivalence [20–22] that states that polarization behavior of any unknown optical system or medium is always equivalent to the effects of the three following basic devices: a rotation of the input light axis (inclination) by an angle ϕ to yield the optical axes of the retarder, a linear retardation R, and an additional axis rotation Ω corresponding to a circular retardation, as it is shown in Eq.4.16

$$J_{sys} = R(\Omega) \cdot \begin{pmatrix} e^{-iR/2} & 0 \\ 0 & e^{iR/2} \end{pmatrix} \cdot R(\Phi), \tag{4.16}$$

where the general rotation matrix is given by

$$R(\Theta) = \begin{pmatrix} \cos\Theta & -\sin\Theta \\ \sin\Theta & \cos\Theta \end{pmatrix}. \tag{4.17}$$

By substituting Eq.4.17 into Eq.4.16 the latter one can be reexpressed as [21]

$$J_{sys} = \begin{pmatrix} P & -Q^* \\ Q & P^* \end{pmatrix}, \tag{4.18}$$

where

$$P = \cos(R/2)\cos(\Phi+\Omega) - i\sin(R/2)\cos(\Phi-\Omega), \tag{4.19}$$

$$Q = \cos(R/2)\sin(\Phi+\Omega) + i\sin(R/2)\sin(\Phi-\Omega), \tag{4.20}$$

and P^*, Q^* are complex conjugates of P and Q, respectively.

The Jones matrix for the forward (toward the Faraday Mirror) SM fiber link is given by

$$J_f = \begin{pmatrix} P & -Q^* \\ Q & P^* \end{pmatrix}. \tag{4.21}$$

The Jones matrix for the backward (back from the Faraday Mirror toward Alice's interferometer) SM fiber link is given by

$$J_b = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix}. \tag{4.22}$$

The matrix has been obtained by transposing the forward one.
The entire "plug & play" system's Jones matrix (for the forward and backward propagation) is thus given by

$$J_{sys} = J_b J_{FM} J_f, \tag{4.23}$$

where the Jones matrix for Faraday mirror is given by [23]

$$J_{FM} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \tag{4.24}$$

By substituting Eq.4.24 into Eq.4.23 we are finally getting

$$J_{sys} = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} P & -Q^* \\ Q & P^* \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \tag{4.25}$$

The Eq.4.25 shows that the Jones matrix for the entire system (forward and backward) has reduced to the Jones matrix for Faraday mirror, which has caused a full reduction of the total (forward and backward) system birefringence. This effect has first been presented in [23]. However, the birefringence matrices in [23] have been simplified by assuming $\Omega = -\phi$. This SM fiber birefringence model, widely cited in the papers dedicated to quantum key distribution, is shown in Sec.4.2.4 to be incorrect.

4.2.4 Sagnac interferometer

Principle

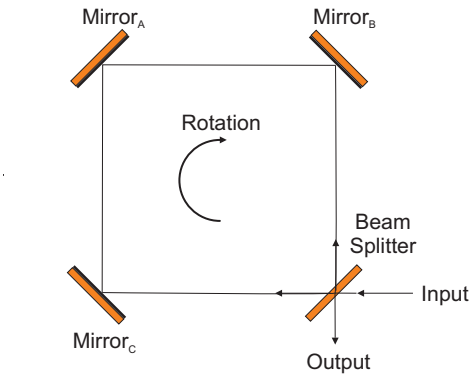

Figure 4.4: Rotating "free-space" Sagnac interferometer

The first demonstration of the "ring" interferometer [24], shown in Fig.4.4, was carried out in 1913 by the French physicist Georges Sagnac [25]. For that reason the interferometer is named Sagnac. Fig.4.4 shows that a beam of light incoming into the beam splitter's input is split into the clockwise and counterclockwise parts, propagating over the interferometer in opposite direction. If the interferometer rotates (the rotation's axis does not have to be inside the area enclosed by the clockwise and counterclockwise beams) the interference fringes will be shifted as compared to the position of them when the interferometer was idle. The shift depends on the fact that the clockwise beam has propagated over less distance (in the case of the clockwise rotation) than the counterclockwise one. The shift's value is proportional to the rotation's angular velocity.

During the light propagation time Δt over the loop, the beam splitter

moves

$$\Delta l = \Omega R \Delta t, \tag{4.26}$$

where R is the loop's radius and Ω is the rotation rate (in rad/sec). The path difference between the clockwise and counterclockwise beams is twice Δl and the phase difference $\Delta\phi$ is given by [24]

$$\Delta\phi = \frac{8\pi A\Omega}{\lambda c}, \tag{4.27}$$

where A is the area enclose by the fiber loop, λ is the light's wavelength, and c its speed in vacuum.

Fiber Sagnac interferometer

More practical in real applications are Sagnac fiber interferometers. An example of such an interferometer is shown in Fig.4.5. In order to find the phase shift in the rotating fiber interferometer let us assume that the light propagates in fiber at two different velocities [24]

$$\begin{aligned} c^{clk} &= \frac{c}{n} + \Omega R\alpha, \\ c^{cnt} &= \frac{c}{n} - \Omega R\alpha, \end{aligned} \tag{4.28}$$

where n is the effective refraction index of the fiber in the loop, and $\alpha = 1 - 1/n^2$ [24] is the relativistic drag imposed by the dielectric fiber medium. It can be shown [24] that even in this case the phase difference $\Delta\phi$, calculated as a function of the clockwise and counterclockwise beams velocities, is described by the same Eq.4.27. Sagnac fiber interferometers are mainly used in rotation sensing and gyroscopes (described, for instance, in [24, 26, 27]). In these applications, only polarization maintaining components and fibers are used so the birefringence influence on the measurement accuracy is really not any major issue. However, in remote measurement applications, requiring long fiber Sagnac loops (such as measurements of slowly varying environmental signals [24,26], distributed Sagnac sensing [26], a fiber Sagnac rotational seismometer [28, 29], a fiber Sagnac gravitational telescope [24], and Sagnac hydrophones [24]) the fiber birefringence is an important design factor. Also in the maturing quantum information area an increased interest could recently be noticed in Sagnac quantum key distribution (QKD) and Sagnac quantum secret sharing over SM fiber telecom links [30–33]. In these single photon applications, the SM fiber birefringence severely limits the secure transmission distance and also requires use of polarization insensitive phase modulators, which are commercially unavailable [5, 19, 34].

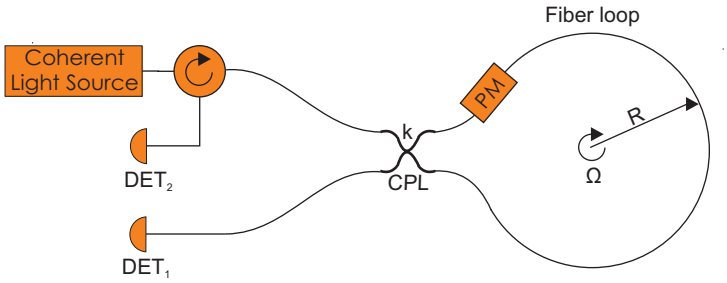

Figure 4.5: Fiber Sagnac interferometer. The circulator CIR provides bidirectional transmission for the light. The coupler CPL coupling ratio $0 \leq k \leq 1$. The phase modulator PM should be polarization insensitive unless all the components of the interferometer (including the fiber loop) are polarization maintaining.

Birefringence in single mode fiber Sagnac interferometer

Figure 4.6 shows a model of a SM fiber Sagnac interferometer with attenuation losses and with the coupler coupling ratio $k = 0.5$, assumed to be the same for the x and y part of the electric field vector, i.e. $k_x = k_y$. This coupling ratio has been chosen in order to fit into the QKD's and secret sharing's experiments described in Papers I-IV. The x-part of the electric field vector will later be called the horizontal, while the y-part the vertical component. The interferometer's birefringence will be analyzed here by using the Kapron equivalence [20–22], already discussed in Sec.4.2.3.

The Jones matrix for the fiber loop in the counterclockwise direction is the transpose of the clockwise matrix [21], which was already discussed in Sec.4.2.3.

$$J_{smf}^{clk} = \begin{pmatrix} P & -Q^* \\ Q & P^* \end{pmatrix} e^{-\alpha L}, \tag{4.29}$$

$$J_{smf}^{cnt} = (J_{smf}^{clk})^T = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} e^{-\alpha L}, \tag{4.30}$$

where α is the fiber absorption coefficient, L the length of the fiber loop,

$$P = \cos(R/2)\cos(\Phi + \Omega) - i\sin(R/2)\cos(\Phi - \Omega), \tag{4.31}$$

$$Q = \cos(R/2)\sin(\Phi + \Omega) + i\sin(R/2)\sin(\Phi - \Omega), \tag{4.32}$$

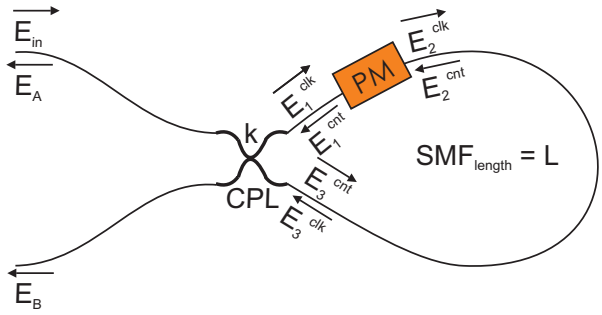

Figure 4.6: Birefringence in SM fiber Sagnac interferometer. The circulator CIR provides bidirectional transmission for the light. The coupler CPL coupling ratio $k_x = k_y = 0.5$. The phase modulator PM should be polarization insensitive unless all the components of the interferometer (except for the fiber loop) are polarization maintaining. The fiber absorption coefficient is α.

and P^*, Q^* are complex conjugates of P and Q, respectively.

The clockwise vector $\mathbf{E_1^{clk}}$ and counterclockwise one $\mathbf{E_3^{cnt}}$ are easily found by using the electric field amplitude transmission equation for a symmetrical ($k_x = k_y = 0.5$) coupler

$$\mathbf{E_1^{clk}} = \frac{\sqrt{2}}{2}\mathbf{E_{in}}, \tag{4.33}$$

$$\mathbf{E_3^{cnt}} = i\frac{\sqrt{2}}{2}\mathbf{E_{in}}, \tag{4.34}$$

where the vector $\mathbf{E_{in}}$ is given by

$$\mathbf{E_{in}} = \begin{pmatrix} E_{in_x} \\ E_{in_y} \end{pmatrix}. \tag{4.35}$$

Since the phase modulator's Jones matrices for the clockwise and the counterclockwise directions are given by

$$J_{PM}^{clk} = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \tag{4.36}$$

$$J_{PM}^{clk} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{4.37}$$

the clockwise and counterclockwise vectors $\mathbf{E_3^{clk}}$ and $\mathbf{E_2^{cnt}}$ become

$$\mathbf{E_3^{clk}} = J_{PM}^{clk} J_{smf}^{clk} \mathbf{E_1^{clk}}, \tag{4.38}$$

$$\mathbf{E_1^{cnt}} = J_{smf}^{cnt} J_{PM}^{cnt} \mathbf{E_3^{cnt}}. \tag{4.39}$$

Finally, the output vectors $\mathbf{E_A}$ and $\mathbf{E_B}$ are found by again applying the electric field amplitude transmission equation for a symmetrical ($k_x = k_y = 0.5$) coupler and substituting Eq.4.38 and Eq.4.39 into the output vector equations.

$$\mathbf{E_A} = i\frac{\sqrt{2}}{2}\mathbf{E_3^{clk}} + \frac{\sqrt{2}}{2}\mathbf{E_1^{cnt}} = i\frac{\sqrt{2}}{2} J_{smf}^{clk} J_{PM}^{clk} \mathbf{E_1^{clk}} + \frac{\sqrt{2}}{2} J_{PM}^{cnt} J_{smf}^{cnt} \mathbf{E_3^{cnt}}, \tag{4.40}$$

$$\mathbf{E_B} = \frac{\sqrt{2}}{2}\mathbf{E_3^{clk}} + i\frac{\sqrt{2}}{2}\mathbf{E_1^{cnt}} = \frac{\sqrt{2}}{2} J_{smf}^{clk} J_{PM}^{clk} \mathbf{E_1^{clk}} + i\frac{\sqrt{2}}{2} J_{PM}^{cnt} J_{smf}^{cnt} \mathbf{E_3^{cnt}}. \tag{4.41}$$

After substituting Eq.4.33 and Eq.4.34 into Eq.4.40 and Eq.4.41 we are finally getting the following electrical field vectors at the detectors $\mathrm{DET_A}$ and $\mathrm{DET_B}$

$$\mathbf{E_A} = \frac{1}{2} i (J_{smf}^{clk} J_{PM}^{clk} + J_{PM}^{cnt} J_{smf}^{cnt}) \mathbf{E_{in}}, \tag{4.42}$$

$$\mathbf{E_B} = \frac{1}{2} (J_{smf}^{clk} J_{PM}^{clk} - J_{PM}^{cnt} J_{smf}^{cnt}) \mathbf{E_{in}}. \tag{4.43}$$

In the ideal case (assuming no birefringence), the Eq.4.42 corresponds (for the modulating phase $\varphi = 0 \pm 2n\pi$, where n is an integer number) to the constructive interference, while the Eq.4.43 corresponds to the destructive one. For $\varphi = \pi \pm 2n\pi$ the vector $\mathbf{E_B}$ corresponds to the constructive interference and vector $\mathbf{E_A}$ to the destructive one. The equations Eq.4.42 and Eq.4.43 show that both constructive and destructive interference are independent of the birefringence only if the clockwise and counterclockwise birefringence (described by Eq.4.29, Eq.4.30, Eq.4.31, and Eq.4.32) are equal. However, such an assumption does not correspond to the general SM fiber birefringence.

4.3 Quantum interferometry in fiber

The experimental work, presented in this thesis, has been performed in fiber and was entirely based on an interferometric approach to quantum key distribution (QKD) and quantum secret sharing. Therefore, the current section concerns quantum interferometry (focused on QKD and quantum secret sharing) in fiber only. Here, it should be pointed out, that the interferometric approach, due to its sensitivity to birefringence, temperature, and generally environment (discussed in Sec.4.2), brings many problems into the practical realizations of QKD and quantum secret sharing. One of the alternative solutions builds on polarization encoding of photons and is presented in Sec.6.1. The solution does not require any interferometer (which is its main advantage), but, at the same time, is very sensitive to SM fiber birefringence (see Chap.3), limiting its application over SM fiber links. Therefore, it has not been explored in our experiments.

4.3.1 Quantum versus classical beam splitting

There are many ways to compare light interference phenomena in a classical and in a quantum-mechanical context. Probably one of the best way is to begin with comparing the action of a beam splitter illuminated by classical light (classical beam splitting has already been presented in Sec.4.2.1) and the same splitter's action on a single photon arriving to one of its inputs.

For a classical beam splitting, shown in Fig.4.7, we are getting the following relations between the reflected E_2 and transmitted E_3 complex electric field amplitudes and the incident complex electric field amplitude E_1

$$\begin{aligned} E_2 &= rE_1, \\ E_3 &= tE_1, \end{aligned} \tag{4.44}$$

where t is the complex transmittance coefficient, r is the complex reflectance coefficient and the splitter has been assumed to be lossless. For such a lossless beam splitter, the intensities on the input and output sides

$$|E_1|^2 = |E_2|^2 + |E_3|^2 \tag{4.45}$$

are the same.
For a symmetrical $50:50$ beam splitter, Eq.4.44 transforms to

$$\begin{aligned} E_2 &= \frac{1}{\sqrt{2}}E_1, \\ E_3 &= \frac{1}{\sqrt{2}}E_1. \end{aligned} \tag{4.46}$$

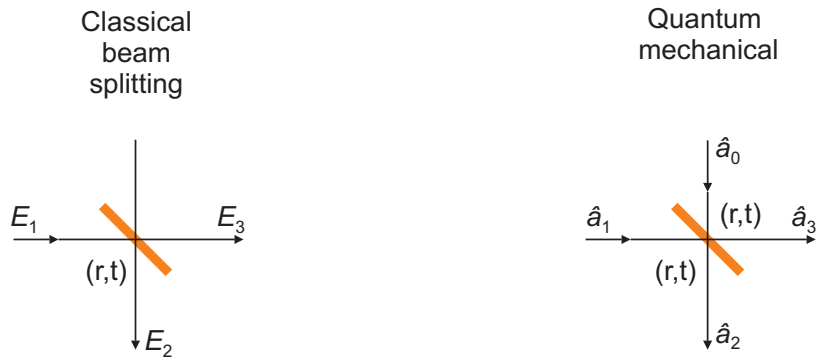

Figure 4.7: Classical versus quantum beam splitting. t is the transmittance coefficient, r the reflectance coefficient of the beam splitter. In the quantum case, it has been assumed that the r and t coefficients are the same on both sides of the splitter. E_1, E_2, and E_3 are complex electric field amplitudes, while $\hat{a}_0$, $\hat{a}_1$, $\hat{a}_2$, and $\hat{a}_3$ are annihilation operators ($\hat{a}_0$ denotes the vacuum annihilation operator). Both beams splitters are assumed lossless.

In the quantum case, the "empty port" of the beam splitter (see Fig.4.7) cannot be neglected. Instead, the vacuum annihilation operator $\hat{a}_0$, describing the vacuum state fluctuations, needs to be considered in the equations describing the beam splitter transformations for the annihilation operators [35]

$$\begin{aligned} \hat{a}_2 &= r\hat{a}_1 + t\hat{a}_0, \\ \hat{a}_3 &= t\hat{a}_1 + r\hat{a}_0. \end{aligned} \tag{4.47}$$

For a symmetrical 50 : 50 beam splitter and assuming that the reflected beam is phase delayed by $\pi/2$ (which applies to beam splitters designed with a single dielectric layers [35]), the following equations describe the transformations for the annihilation and creation operators

$$\begin{aligned} \hat{a}_2 &= \frac{1}{\sqrt{2}}(i\hat{a}_1 + \hat{a}_0) & \hat{a}_3 &= \frac{1}{\sqrt{2}}(\hat{a}_1 + i\hat{a}_0), \\ \hat{a}_0^\dagger &= \frac{1}{\sqrt{2}}(\hat{a}_2^\dagger + i\hat{a}_3^\dagger) & \hat{a}_1^\dagger &= \frac{1}{\sqrt{2}}(i\hat{a}_2^\dagger + \hat{a}_3^\dagger). \end{aligned} \tag{4.48}$$

Next section (Sec.4.3.2) compares classical and quantum interferometry. For such a comparison, the Schrödinger picture of quantum beam splitting is more illustrative. For instance, already considering a simple single photon input state $|0\rangle_0|1\rangle_1$ (with the state indices pointing to the inputs of the

beam splitter in Fig.4.7) leads to a surprising, for the classical interference approach, state transformation result derived from Eq.4.48

$$|0\rangle_0|1\rangle_1 \Longrightarrow \frac{1}{\sqrt{2}}(i\hat{a}_2^\dagger + \hat{a}_3^\dagger)|0\rangle_2|0\rangle_3 = \frac{1}{\sqrt{2}}(i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3), \qquad (4.49)$$

where $\hat{a}_2^\dagger$, $\hat{a}_3^\dagger$ are creation operators.
One cannot overestimate the significance of this counterintuitive result, which says that a single photon arriving to one of two inputs of the beam splitter is with equal probability transmitted or reflected by the device. Thus, such a setup could be used as a perfect random number generator.
Finally for this section, it should be pointed out that the state $\frac{1}{\sqrt{2}}(i|1\rangle_2|0\rangle_3 + |0\rangle_2|1\rangle_3)$ in Eq.4.49 is an entangled one since it cannot be written as a product of the individual states for the modes 2 and 3.

4.3.2 Quantum versus classical interferometry

Fig.4.8 shows two M-Z interferometers: the first one using a classical coherent light source and the other one a single photon light source. As it was shown

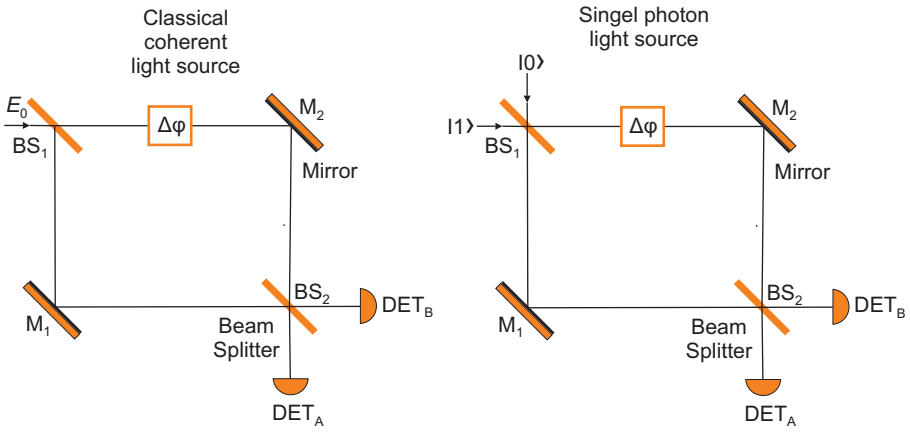

Figure 4.8: Classical versus single photon quantum interference. Both interferometers are assumed lossless. Both beam splitters are symmetrical $(50:50)$. $\Delta\phi$ is a phase delay inserted into the upper arm of the interferometer. For $\Delta\phi = 0$ there are no other phase delays caused by the interferometer components.

in Sec.4.2.2 for the classical light source, the output intensities I_A and I_B at

the detectors DET_A and DET_B are given by

$$I_A = \frac{I_0}{2}(1 + \cos\Delta\phi),$$
$$I_B = \frac{I_0}{2}(1 - \cos\Delta\phi). \tag{4.50}$$

in the case of a lossless interferometer.

In the case of a single photon light source $|0\rangle_0|1\rangle_1$ at the inputs of the M-Z interferometer, there is a need to use field operators in order to find the output states at the detectors DET_A and DET_B. As it was shown in Sec.4.3.1, the beam splitter BS_1 transforms the input state $|0\rangle_0|1\rangle_1$ into the following state

$$|0\rangle|1\rangle \Longrightarrow \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + i|1\rangle|0\rangle), \tag{4.51}$$

where the first state in the equation and in the following equations refers to the clockwise propagating light, while the second state to the counterclockwise one.

Since each arm of the interferometer is equipped with the same type of mirror, the phase delays caused by the mirrors can be omitted.
The delay element in the upper arm introduces a phase delay $\Delta\phi$ into the first component in Eq.4.51

$$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + i|1\rangle|0\rangle) \Longrightarrow \frac{1}{\sqrt{2}}(e^{i\Delta\phi}|0\rangle|1\rangle + i|1\rangle|0\rangle). \tag{4.52}$$

Similarly to the transformation in BS_1 (see Eq.4.51), the beam splitter BS_2 transforms the input state $|1\rangle|0\rangle$ into the following state

$$|1\rangle|0\rangle \Longrightarrow \frac{1}{\sqrt{2}}(i|0\rangle|1\rangle + |1\rangle|0\rangle). \tag{4.53}$$

Thus, after the second beam splitter BS_2, the following state is obtained

$$\frac{1}{\sqrt{2}}(e^{i\Delta\phi}|0\rangle|1\rangle + i|1\rangle|0\rangle) \Longrightarrow$$
$$\Longrightarrow \frac{1}{\sqrt{2}}\left[e^{i\Delta\phi}\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + i|1\rangle|0\rangle) + i\frac{1}{\sqrt{2}}(i|0\rangle|1\rangle + |1\rangle|0\rangle)\right] \Longrightarrow$$
$$\Longrightarrow \frac{1}{2}\left[(e^{i\Delta\phi} - 1)|0\rangle|1\rangle + i(e^{i\Delta\phi} + 1)|1\rangle|0\rangle)\right]. \tag{4.54}$$

Thus, the probability that the photon is detected in the detector DET_A is proportional to $|e^{i\Delta\phi}+1|^2$ and is given by

$$p_{10} = \frac{1}{2}(1+\cos\Delta\phi), \tag{4.55}$$

while the probability that the photon is detected in the detector DET_B is proportional to $|e^{i\Delta\phi}-1|^2$ and is given by

$$p_{01} = \frac{1}{2}(1-\cos\Delta\phi). \tag{4.56}$$

The right sides of Eq.4.53 and Eq.4.54 are the same as the right sides of Eq.4.50 showing the output light intensities I_A and I_B at the detectors DET_A and DET_B in the classical input light case. What differs are the left sides of the equations. While in the classical case the detector measurement function is described by the output light intensity, in the quantum case is described by the probability of detecting a given state. Thus, with the assumption that the measured components are not power level limited to quantum conditions only, classical measurements can be used for characterizing (for instance, aligning) any optical setup before switching power conditions into quantum levels.
Finally for this section, the following simplified conclusion could be made regarding the nature of classical and quantum interferometry.
In the classical case, both the light propagation in the interferometer and the detection are described by classical optics.
In the quantum case, a single photon shows its dual nature. In the interferometer it behaves as a wave, but it is measured as a particle.

4.3.3 Visibility

The classical definition of visibility has been presented in Sec.4.2.2. It is a function of the light intensity at the output detector and is given by

$$V = \frac{I_{max}-I_{min}}{I_{max}+I_{min}}, \tag{4.57}$$

where I_{max} and I_{min} are the output light intensities for the constructive and the destructive interference condition, respectively.
In the quantum case, visibility is determined by the photon detection probability (see Eq.4.55 and Eq.4.56). Thus, visibility is a function of the detector counts and is given by

$$V = \frac{n_{max}-n_{min}}{n_{max}+n_{min}}, \tag{4.58}$$

where n_{max} and n_{min} are the count numbers (measured during the same period) for the constructive and the destructive interference condition, respectively.

Chapter 5

Classical cryptography

5.1 Introduction

Cryptography is probably as old as the human civilization. However, the earliest written record on cryptography date back to the Old Testament, which parts were encrypted with atbash, a traditional Hebrew cipher [36] that builds on substituting each letter of the message by a corresponding letter from the end of the alphabet in such a way that the distance of the substituted letter from the beginning of the alphabet is the same as the distance of the replacing one from the end of the alphabet. The earliest written record on military cryptography date back to the fifth century B.C. when Greece and Persia were in a conflict of interest that soon led to a war between these countries [36]. According to Herodotus (the Greek historian), Demaratus, a Greek who lived in the Persian city of Susa, noticed in 480 B.C. a major military buildup, ordered by Xerxes, the Persian king, intending to launch a surprise attack on Greece. Demaratus decided to warn the Greeks, but the challenge was how to dispatch the warning message so it would be not intercepted by the Persian guards. In order to do it, he scrapped the wax off a pair of wooden folding tablets, wrote on the wood underneath the warning message, and finally covered the message over with wax again. The warning resulted in a military fleet buildup in Greece. On September 23, 480 B. C. the Greek fleet defeated the Persian fleet, which suffered devastating losses.

Demaratus warning message dispatch began a written history of stenography, a secret communication achieved by hiding the message existence. Stenography, however, suffers from a fundamental secrecy weakness due to the fact that once the hidden message is discovered its context is immediately

revealed!

While stenography hides the message existence, cryptography hides its context. Both methods can be combined (in order to maximize security), for instances, by creating a microdot by zooming down the message to a microsize and scrambling it at the same time [36].

Generally, cryptography can be divided into transposition and substitution [36]. Transposition builds on rearranging the order of the letters of the message. The output of the rearrangement is an anagram. For very short messages, consisting of a few words, there are not too many ways to rearrange the message so transposition is insecure. But for larger messages, transposition seems to offer a very high security. However, a random rearrangement of the letters in a large message makes it almost impossible to unscramble it not only for the enemy but also for the intended recipient. While transposition builds on rearranging the letters of the message, substitution builds on substituting each letter in the original text by a different letter in the ciphered text. Thus, the method is called a substitution cipher [36]. The first documented military use of a substitution cipher was described by Julius Caesar who replaced Roman letters with Greek ones.

A more general encryption is presented in Fig.5.1, which also shows the encryption algorithm and the conventional names (used in cryptography) of the sender, receiver, and eavesdroppers: Alice, Bob, and Eve, respectively. In Julius Caesar case, the algorithm was simply the replacement of Roman letters by Greek ones. By keeping the key and algorithm secure, the message

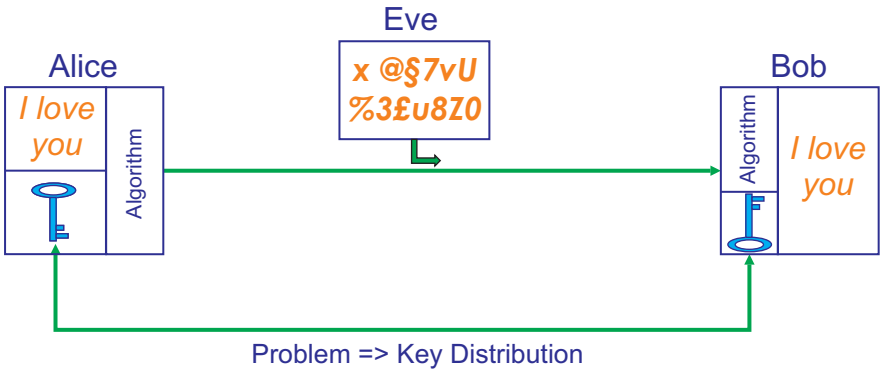

Figure 5.1: General encryption idea. The encryption algoritm together with the encryption key specifies the encryption of Alice's message. The encryption's output is a ciphertext sent to Bob.

is secure to the degree, which depends on the randomness of the encryption

key (see. Sec.5.3). Before the message is transmitted or dispatched, Alice needs to share both the key and the algorithm with Bob, which might be impractical in real applications.

5.2 Vigenère encryption

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 5.2: Vigenere square.

Vigenère, a French diplomat, born in 1523, addressed security issues of the cipher discussed in Sec.5.1, especially the randomness of the encryption key. He found that the security could be significantly increased by using not one, but 26 distinct cipher alphabets to encrypt a message. Fig.5.2 shows Vigenère square that contains 26 distinct cipher alphabets, each one

shifted to the left by one letter with respect to the former one. The main difference between Caesar and Vigenère ciphers is the fact that the first uses one alphabet for all letter of the message, while the latter one uses a dynamic encryption scheme by switching between 26 different alphabets for every letter of the message. The order of switching is determined by a keyword that Alice and Bob need to share. In order to encrypt and decrypt the message, the keyword should be written repeatedly to cover the entire length of the message. Thus, each letter of the message corresponds to a letter of the repeated keyword. The latter is chosen to select the row that begins with it. In such a way each letter will be given a dynamically selected alphabet.

The great advantage of Vigenère cipher is its immunity to the frequency analysis based on statistical frequency of using letters in a given language. Frequency analysis is a useful method to decrypt messages encrypted with one alphabet only, like a Caesar cipher. Vigenère cipher was broken first in the middle of nineteen century by Charles Babbage and independently, a decade later, by Fredrich Wilhelm Kasiski. Both used a statistical analysis of repeated patterns in a encrypted message.

5.3 Onetime-pad

Onetime-pad, shown in Fig.5.3, builds on the usage of a random encryption key, of the same length as the message, once and only once! Once the message has been deciphered, both Alice and Bob destroy the key so it can never be used again. The method guarantees an unconditional security, but requires a full randomness of the key and a handling of the key to Bob by

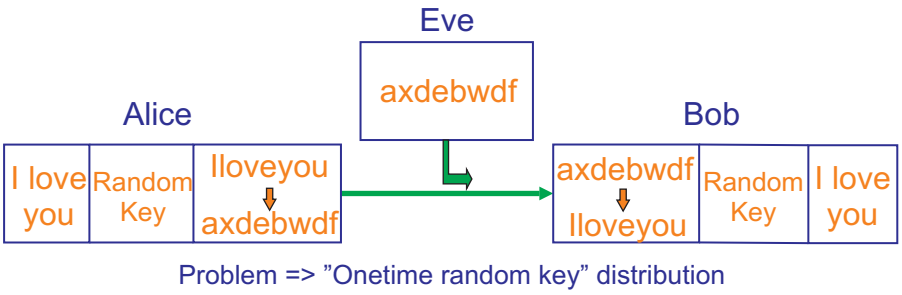

Figure 5.3: Onetime-pad cryptography. The method guarantees an unconditional security but requires a full randomness of the key and that Alice handle the key to Bob before the message is transmitted or dispatched.

Alice before the message is transmitted or dispatched. The idea of a random key and its application in the onetime-pad was introduced in 1918 by Major Joseph Mauborgne, head of cryptographic research unit of the US army [36]. However, the one-time pad is derived from the Vernam cipher, invented by Gilbert Vernam et al. [37].

5.4 Public key cryptography

Key distribution has been the main problem for cryptographers throughout history of cryptography and it seemed to be an insolvable one. Thus a new, completely different approach, was needed for solving the distribution problem. In 1973, Whitfield Diffie discovered a new, so called, asymmetric cipher, which builds on the progress achieved, by then, by computers. In asymmetric ciphering, Bob creates a pair of keys: an encryption key and a decryption key. Bob publish his encryption key (called also a public key) on a public channel, while keeping the decryption key secret. Then Alice uses the encryption key to cipher his message and sends it Bob, who decrypts it using the secret decryption key. Thus, asymmetric cipher solves the key distribution problem.

Diffie's asymmetric cipher built on the existence of so called one-way functions, which in Alice's case work in the following way: she can encrypt her message using the public key but, since she lacks the decryption key, she cannot decrypt the message.

Diffie published his asymmetric cipher idea in 1976 in a joined breakthrough paper with Martin Hellman [38]. However, it was shown later that the Diffie-Hellman key exchange protocol was vulnerable to a man-in-the-middle attack. In 1978, the team of Ronald Rivest, Adi Shamir, and Leonard Adleman published another breakthrough paper on asymmetric ciphering [39]. Thus, the public key cryptography was born.

The RSA encryption [39,40], which is widely used, builds on the one-way function, described in the following Bob's encryption procedure.
Bob:

- chooses, at random, two large prime numbers p and q of similar bit-length and calculates their product $n = p \cdot q$
- calculates the totient $\varphi(n) = (p-1)(q-1)$
- chooses an integer e such that $1 < e < \varphi$ and both e and $\varphi(n)$ are coprime numbers

- announces on a public channel e as a public key together with the modulus n
- calculates such d that fulfills the congruence relation $de \equiv 1\ mod(\varphi(n))$ and keeps it as his private key.

On the message sender site, Alice encrypts her message M by executing the following procedures.
Alice:

- uses a padding protocol [39] in order to convert the message M into an integer m such that $0 < m < n$
- computes the ciphertext $c \equiv m^e\ mod(n)$.

On the message receiver site, Bob decrypts the message c by executing the following procedures.
Bob:

- decrypts, by using the private key (d, n), the message c into the message m by computing $m \equiv c^d\ mod(n)$
- uses the same padding protocol as Alice used (they need to agree about the protocol before the key exchange) to recover the message M.

In the real applications more procedures, as described by diverse Public-Key Cryptography Standards (PKCS) provided by RSA Laboratories, are necessary.

The security of the RSA encryption is based on the exponentially increasing computing time (using classical computers) for factoring large integers. No polynomial-time factoring algorithms are know now, but it has not been proven their non-existence. For Eve, the eavesdropper, the factoring means that she would need to factor back the public key n into p and q.

Now, RSA keys are typically $1024-2048$ bits long. In 1999, it was shown that previously used 512 bits long keys were insecure. In 2008, the same was shown for 663 bits long keys. Since the factoring time increases exponentially with the key's length, $1024-2048$ bits long keys are assumed secure. However, a new, unknown now, factoring algorithm for classical computers or a future quantum computer could potentially factor in polynomial time such long and even longer keys, which makes the future of public key cryptography uncertain. While quantum computing is a huge treat to public key cryptography, quantum communications has offered a new, absolutely secure, quantum key distribution, presented in Chap.6.

Chapter 6

Quantum cryptography & secret sharing

6.1 Quantum cryptography

The idea of quantum cryptography was first proposed in the early seventies by Stephen Wiesner, but was published a decade later (in 1983). In 1984, Charles H. Bennett of IBM and Gilles Brassard of the University of Montreal made a breakthrough contribution to the Wiesner's idea by proposing their BB84 protocol. Basically, quantum cryptography utilizes some of quantum physics' counterintuitive rule: the principle of complementarity stating that an unknown quantum state cannot be duplicated due to the no-cloning theorem (proved by D. Dieks [41] and W. K. Wootters, W. H. Zurek [3]) nor measured without disturbance. For instance, polarization measurement of a photon cannot be carried out simultaneously in the horizontal-vertical basis and in the diagonal-antidiagonal basis. Thus, quantum cryptography security is based on physical law compared to classical cryptography based on complicated algorithms.

In cryptography, the conventional names of the sender, receiver, and eavesdroppers are Alice, Bob, and Eve, respectively as they are shown in Fig.6.1, presenting a polarization encoded quantum cryptography. Alice sends photons randomly polarized either horizontally, vertically, or diagonally (at +45°), or antidiagonally (at -45°), as row 1 shows. Bob randomly chooses one of his analyzer basis: horizontal-vertical or diagonal-antidiagonal (row 2) and records his measurement results (row 3). Then, with the aid of a public channel, they compare the used bases and keep all results with compatible bases (row 4). Thus, the BB84 protocol enables two people to

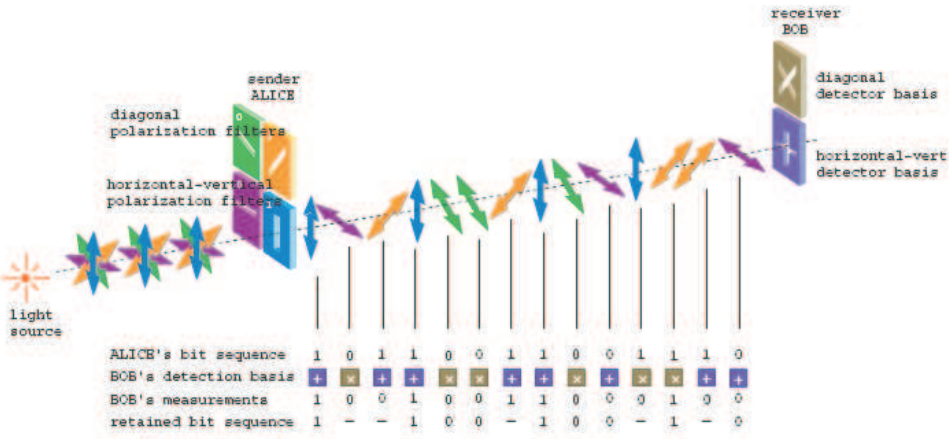

Figure 6.1: BB84 (Bennett & Brassard, 1984) quantum cryptography protocol using polarization encoding. Alice sends photons randomly polarized either horizontally, vertically, diagonally, or antidiagonally. Bob randomly chooses one of his analyzer basis (row 2) and records his result (row 3). Then they compare the used bases and keep all results with compatible basis (row 4) [42].

jointly develop a cryptographic key out of random choices that each makes independently. In the original BB84 protocol the key bits were encoded in one of the photon's quantum properties: its polarization. In the practical BB84 applications, other quantum properties (for instance, photon's phase) are more frequently used.

In detail, Alice sends to Bob a random series of qubits. She encodes her photons on a horizontal-vertical or a diagonal-antidiagonal basis. In the horizontal-vertical basis, a vertical polarization represents a 1 and a horizontal polarization represents a 0. In the diagonal-antidiagonal basis, a diagonal polarization represents a 1 and an antidiagonal polarization represents a 0. To receive Alice's qubits, Bob uses two polarization beam-splitters (one for the horizontal-vertical and the other one for the diagonal-antidiagonal basis) that allow Bob to correctly measure only photons of a specific basis. For example, in the horizontal-vertical basis Bob can correctly measure horizontally or vertically polarized photons, but not diagonally-antidiagonally polarized ones. The diagonally-antidiagonally polarized photons, encountering the horizontal-vertical beam-splitter, appear to Bob to have either a horizontal or a vertical polarization (with the equal 50% probability). The

same applies to the photons belonging to the horizontal-vertical basis at the diagonal-antidiagonal beam splitter.

Alice encodes her photons at random and Bob's choice of the basis is also random. If they use the same basis, they get the same results. If they use opposite bases, the results are random. After a series of photons has been sent, Bob announces (on a public telecommunication channel) the series of his basis choices, but does not reveal the results of his measurements. After that, Alice informs Bob (using a public channel) which of his basis choices matched hers. Then, they discard the results with no-matching bases and keep the results with matching ones. In such a way they have established a random sifted key (that is shorter than the original bit sequence sent by Alice), known only to Alice and Bob. The sifted key can be used for a secure transmission as a one-time pad, discussed in Sec.5.3. In the real applications, more steps are needed, including error correction and privacy amplification.

6.1.1 "Plug & play" QKD with phase encoding

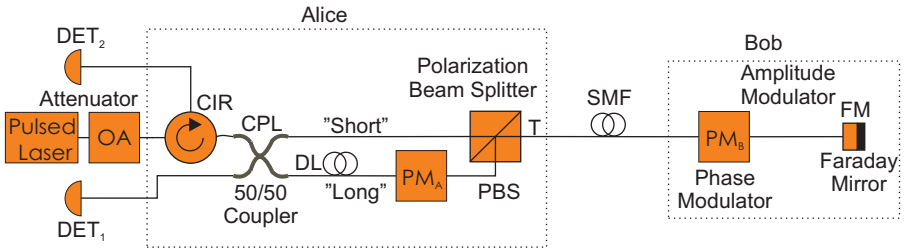

Figure 6.2: "Plug & play" QKD with phase encoding.

Since any general QKD system needs to target data transmission over standard telecom 1310/1550 nm single mode fibers (SMF), the previously mentioned polarization-encoding is impractical. The main reason for this is the significant birefringence of single mode fiber, already discussed in Sec.3.6. Therefore, many attempts have been made to apply other well established telecom modulation schemes, including a phase encoding, being an attractive solution due to availability of the COTS (commercial off the shelf) telecom phase modulators.

Fig.6.2 shows a simplified schematics of a phase-encoded "plug & play" QKD system [5, 43]. Starting from now, we change the order of the parties, traditionally associated with QKD. Now, the sender of the single photons is named Bob and the receiver is named Alice. The reason for the change is the fact that we will be discussing the "plug & play" scheme and it seems that the

order change makes the discussions more consistent for such schemes, which include quantum secret sharing and multiuser QKD, presented in Paper 1 and Paper 2.

In detail, a relatively strong 1550 nm laser pulse, at Alice's side, is attenuated in the digitally controlled optical attenuator OA (that attenuates it to such a level that the pulses leaving Bob's station will be held on a single photon level) and sent trough the circulator CIR to the 50/50 coupler CPL that splits it into two pulses propagating through a short arm and a long arm (that includes the phase modulator PM_A and the delay line DL), respectively. The pulses arrive to the polarization beam splitter (PBS) and leave Alice's side by the same T-port of the PBS. The short-arm's pulse leaves Alice horizontally polarized, while the long-arm's one vertically polarized. The pulses travel to Bob's side, are reflected on at the Faraday Mirror, attenuated and transmitted back, orthogonally polarized, compared to their initial polarization states (when they left Alice's interferometer). Both pulses continue their propagation through the opposite paths (compared to the forward propagation) of Alice's interferometer and arrive at the same time at the coupler CPL, where they interfere. After that, they are detected either

Bit	*Bob's Phase* ϕ_B	*Alice basis* ϕ_A	$Interferometer$ $\phi_A - \phi_B$	*Established bit* ϕ_E
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Table 6.1: Implementation of the BB84 protocol with phase encoding. The question marks in the table show the pulses with non-coincidental bases.

in D_1 or in D_2 (after passing through the circulator CIR). The setup's "plug & play" feature has been achieved by directing both interfering pulses to travel exactly the same path-length through both directions (i.e. forth and back) and by using the Faraday Mirror, shifting the pulses' polarization by $\pi/2$, which compensates for the SMF channel's birefringence (see Sec.4.2.3).

On Bob's side, with the aid of the phase modulator PM_B, the second pulse's phase is shifted (0, π) or ($\pi/2$, $3\pi/2$). Bob's action could be consid-

ered as a phase change in one of the two bases: the horizontal-vertical (0, π) or the diagonal-antidiagonal ($\pi/2$, $3\pi/2$). On Alice's side, the measurement basis is chosen by shifting the phase of the first (short-arm's) pulse by 0 (the horizontal-vertical basis) or by $\pi/2$ (the diagonal-antidiagonal basis) on its way back from Bob's side. The Tab.6.1.1 summarizes the implementation of the BB84 protocol with phase encoding.

6.1.2 Transmission and error rates

The raw rate in the BB84 protocol is defined as

$$Rate_{raw} = q\mu f \eta_{det} \eta_{link}, \tag{6.1}$$

where q is a setup dependent coefficient, μ is the mean photon number per pulse, f is the laser pulsing frequency, η_{det} is the photon's detection probability, and η_{link} is the transfer efficiency of the link between Bob's station and Alice's detectors. The factor $q = 0.5$ since only in 50% of all the measurement cases the measurement basis are coincidental. The quantum bit error rate (QBER) for the faint laser pulse QKD can be written as a sum of two main contributing factors

$$\begin{aligned} QBER = QBER_{opt} + QBER_{det} &= p_{opt} + p_{noise}/p_{photon} \\ &= p_{opt} + p_{noise}/\mu\eta_{det}\eta_{link}, \end{aligned} \tag{6.2}$$

where p_{opt} is the probability of a photon going to the wrong detector and p_{noise} is the probability of getting a noise-count (mainly dark counts) per the gating pulse window [5, 43].
For the phase-based QKD

$$P_{opt} = (1 - V)/2, \tag{6.3}$$

where V is the interference visibility.

6.1.3 Eavesdropping strategies

The eavesdropper Eve has a variety of strategies to listen in to the key transmission. For instance, she could intercept a photon sent by Bob. But this is not a very good strategy since Alice could simply inform Bob that she never received the photon. Neither, since copying an unknown quantum state is forbidden by no-cloning theorem [3,41], can Eve use copying photons sent by Bob to Alice as a successful eavesdropping strategy. Measuring intercepted photons is not a good strategy either since Eve has no knowledge

of the bases that Bob used to polarize photons. She can guess, but any mistake would introduce errors into Alice's measurement data, which will eventually be detected (when Alice and Bob try to establish the code by mutually exchanging information on a public channel). The errors that Eve introduces indicate for Bob and Alice a higher error rate transmission than they would otherwise have been expecting from the transmission impairment. Thus, error rate measurement is important in quantum cryptography because it allows Alice and Bob to detect eavesdropping.

Eve can also try to measure only a small fraction of the photons (which would increase the error rate only marginally) gaining a partial knowledge of the key. However, as a countermeasure, Alice and Bob may decide to use a privacy amplification protocol in order to minimize the information Eve can get. For instance, Alice chooses, at random, pairs of bits from the key and performs an exclusive-or logic operation (sum modulo 2) on them. Then, she tells Bob which bits she did the operation on, but does not share the result. Bob then carries out the same operation leading to the same result. Then, Bob and Alice replace each pair with the calculated exclusive-or value. If Eve, who has many errors in her key, tries to carry out the same operation she only increases the number of her errors.

Fortunately for Eve, a secure distribution of the key requires a single photon source. In the real QKD applications "faint pulse" sources (that only approximate a single photon source) are instead used. Thus, a big security hole is opened for Eve who can use a photon number splitting (PNS) attack to reveal the sifted key.

6.1.4 Security against individual attacks for single photon sources

So far, the quantum channel was considered to be noiseless. In the real QKD applications, there will be always some optical (for instance, a polarization misalignment) or electrical (for instance, dark counts in single photon detectors) impairments leading to the key transmission errors. Thus, Alice and Bob may need to implement an error correction (in order to correct errors in the raw key) and finally a privacy amplification to minimize the amount of information gained by Eve. After carrying out both procedures, Alice and Bob have got an almost perfectly secure key. However, the strict security proof was missing until year 1996, when Mayers [44] published his famous proof of the 11% quantum bit error rate (QBER) boundary for the BB84 single photon source QKD security. The work on the BB84 security was extended in 2000 when Shor and Preskill [45] published a simpler proof of

the border. Both these proofs assumed a one-way classical communication channel. For a two-way channel, Gottesman and Lo [46] found in 2003 that the boundary was higher (18.9%). In 2004, Lütkenhaus [47], using a different approach, provided another proof of the 11% QBER boundary for the BB84 single photon source QKD security. Additionally, he analyzed more realistic photon sources, including weak coherent pulses (faint-pulses) and down-conversation sources. Here, we will shortly review his results.

As already mentioned in Sec.6.1, in the real QKD applications two classical information procedures: error correction and privacy amplification are necessary in order to minimize the amount of information gained by Eve, the eavesdropper. Generally, in order to asses the QKD security, there is a need of comparing the amount of information gained by Eve with the error rate caused by her eavesdropping activity. In order to do it there is, among other tasks, a need for assessing the efficiency of the implemented error correction protocol.

Error Correction Protocols

Error correction can be obtained by exchanging parity bits over a public channel by using a onetime-pad. Thus, Alice and Bob need, prior to any other QKD task, to share at least short secret key for the onetime-pad public channel transmission. It is obvious that the chosen error correction protocol should at least provide the corrected code's length equal to the length of the onetime pad and consequently the length of the original parity code. As Shannon showed in 1948 [48], the minimum number of redundant bits N_{corr} that are needed to correct a key of length n is given by

$$N_{corr} = n[-e \log_2 e - (1-e) \log_2 (1-e)], \tag{6.4}$$

Error rate e	Bidirectional protocol efficiency function $f[e]$
0.01	1.16
0.05	1.16
0.10	1.22
0.15	1.35

Table 6.2: Examples of bidirectional error correction protocols performance . $f[e]$ is the ratio of actually needed redundant bits to the Shannon limit [47].

where e is the error rate in the sifted key. The probability that the errors can be corrected comes arbitrary close to unity for the large codes. In real applications, it is difficult to reach the Shannon limit while implementing unidirectional protocols (that use a one-way classical communication channel). However, bidirectional protocols (that use two-way classical communication channels [47]), shown in Tab.6.2, are much more efficient.

Privacy amplification

The process of privacy amplification should lead to such a drop of the information gathered by the Eavesdropper that the security of the key is guaranteed. An efficiency measure of the implemented privacy amplification procedure is the fraction τ_1 of bits by which the sifted key need to be shorten in order to obtain a secure key. In [47], τ_1 has been estimated to

$$\begin{aligned} \tau_1 &\leq log_2(1 + 4e - 4e^2) \quad \text{for} \quad e \leq 1/2, \\ \tau_1 &\leq 1 \quad \text{for} \quad e > 1/2. \end{aligned} \tag{6.5}$$

Gain formula for single photon sources

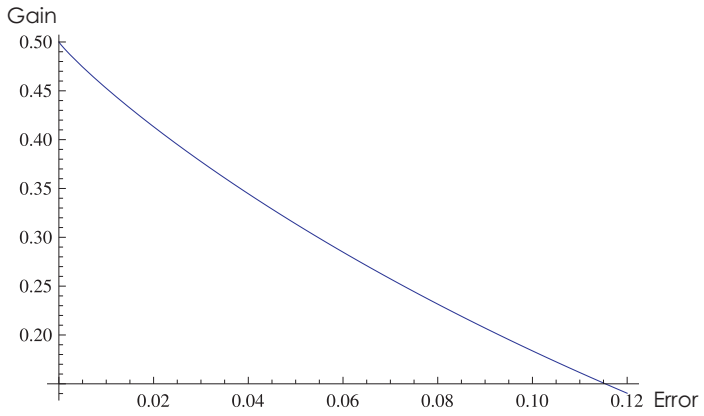

Figure 6.3: Gain of secure bits per time slot as a function of the observed error rate e for an ideal channel for single photon source and ideal error correction [47].

Error correction and privacy amplification have been summarized in the following formula, showing the gain of secure bits per time slot as a function

of the error rate e for single photon sources [47]

$$G = \frac{1}{2} p_{exp} \left\{ 1 - \tau_1 + f[e][e log_2 e + (1-e) log_2 (1-e)] \right\}, \qquad (6.6)$$

where p_{exp} is the photon's detection probability, which takes into the account the quantum channel losses and optical impairments as well as the limited quantum efficiency of the detectors (see Sec.6.1.2). The 1/2 coefficient is related to the fact that only in half of the detection cases Alice's and Bob's bases are the same. Fig.6.3 shows the gain for a lossless channel, $p_{exp} = 1$ and for the error correction on the Shannon limit i.e. for $f[e] = 1$. For such a channel the maximum error rate (for the secure key transmission) is 11%.

6.1.5 Photon number splitting attacks

Using tools, not available today, the following photon number splitting (PNS) attack could be performed by Eve, the eavesdropper [47].
Firstly, Eve could count the number of photons (in order to distinguish the single photon pulses from the multiphoton ones) by carrying out a quantum nondemolition (QND) measurement that make it possible to evade the noise arising from the measurement process. In the QND measurement of the observable $\widehat{A}$, the state of signal light remains in the same eigenstate $|a\rangle$. The basic practical approach to the QND measurement is to introduce, trough a nonlinear process, a link between the coherent light amplitude quadratures and carry out the measurement in such a way that the noise created by the measurement's action is transferred into the other quadrature [18].
Secondly, Eve blocks all the single photon pulses, stores (in a quantum memory) one photon from each multiphoton pulse and forwards the remaining photons to Bob. Since her action would influence the expected detection rate on Bob's site, Eve makes an accordant adjustment of the quantum channel attenuation.
Finally, Eve waits for the information exchange (regarding the used bases) on the public channel between Alice and Bob and measure her stored (in the quantum memory) photons. Thus, by using the PNS attack, Eve can reveal the entire sifted code without introducing any noticeable errors! This feature of the PNS attack makes it especially dangerous for prevention and detection of the eavesdropping.

Fig.6.4 shows the PNS attack's principle. The strongly attenuated (to the mean photon number μ) pulses are split by Eve in the beam splitter BS_{Eve}. The quantum channel attenuation has been adjusted by Eve to 0 (in a practical application the adjustment's value needs to be estimated by

using Eve's QND measurements) in order to compensate for a change of the expected detection rate on Bob's side.

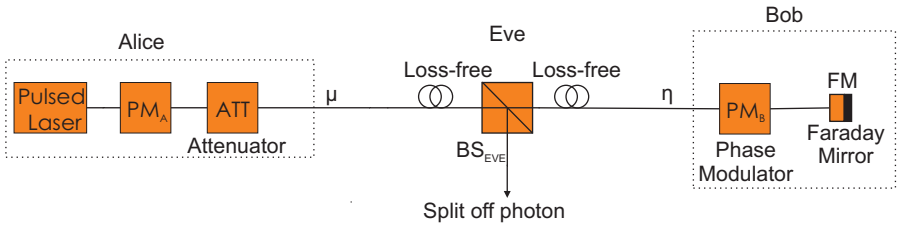

Figure 6.4: Photon number splitting attack principle. In a real PNS application the attenuation adjustment's value does not lead to a loss-free attenuation. Instead, it needs to be estimated by using Eve's QND measurements. μ is the mean photon number for pulses leaving Alice's site, while η denotes Bob's losses, including the limited quantum efficiency of his detectors.

6.1.6 Decoy states

To overcome photon-number splitting (PNS) eavesdropping attacks, decoy states are now commonly used in practical QKD realizations with weak coherent light pulses. Here, we will shortly review decoy states [49–51] and show their implementation in the "plug & play" QKD setup.

The original idea of decoy-state method and the first protocol was published by Hwang [49]. The protocol used two randomly chosen pulse intensities: signal pulses with mean-photon number $\mu = 0.3$ and decoy states with mean photon number $\nu = 1$. Thus, the decoy states have much higher probability of bearing multiphotons than the signal pulses. The pulses resent by Eve to Bob, after the QND measurement (see Sec.6.1.5), bear statistically more multiphotons than Alice's original pulse series. Thus, by randomly interleaving signal and decoy states, Eve's PNS attack can be detected by Alice and Bob. In order to do it, Alice announces (on a public channel) which pulses she sent belonged to the decoy states. If Bob's detection rate of the decoy photons is much higher than the rate of the signal pulses, the distributed key is insecure.

After Hwang's breakthrough idea, many new decoy state protocols have been developed and strict mathematical proofs of the security of the QKD implementing decoy states have been published. For instance, Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [52] published in 2004 an important contribution to the field by deriving a general lower bound on the asymp-

totic key generation rate in BB84 QKD protocol for weakly basis-dependent eavesdropping attacks. They also estimated the secure transmission rate in some special cases such as sources that emit weak coherent states with random phases, detectors with basis-dependent efficiency, and misaligned sources and detectors. GLLP also introduced a new idea of tagged qubits as a quality measure of the QKD security. The tagged qubits are the ones that correspond to the multiphoton pulses. Thus the tagging probability, assuming that all of the photons that are lost in the quantum channel were emitted as single ones, is given by

$$\Delta = \frac{p_M}{p_D}, \tag{6.7}$$

where p_M is the probability of emitting a multiphoton and p_D the probability that an emitted photon is detected. For weak-coherent laser pulses, p_M can be estimated (see. Sec.2.1.2) and p_D measured. Thus, the fraction of tagged qubits Δ is a useful parameter characterizing practical QKD implementations. Assuming that Eve can somehow (for instance, by performing a QND measurement) get basis information of tagged qubits they are considered insecure for QKD. Hence, Alice and Bob can separate the qubits into two groups: tagged and untagged ones and perform privacy amplification to the untagged qubits only [52].

In 2005, Lo, Ma, and Chen [53] combined the GLLP approach with decoy states and presented the following secure key generation rate

$$R \geq q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{6.8}$$

where $q = 1/2$ for BB84 without decoy (see Sec.6.1.2), while $q < 1/2$ with decoy implementation; μ denotes the mean-photon number for signal states; Q_μ is the gain of signal states; E_μ is the quantum bit error rate (QBER); Q_1 is the gain of single-photon states; e_1 is the error of single-photon states; $f(x) \geq 1$ is the error correction function with Shannon limit $f(x) = 1$ (see Sec.6.1.4); and $H_2(x)$ is the binary Shannon entropy function given by

$$H_2(x) = -x\ log_2(x) - (1 - x)\ log_2(1 - x). \tag{6.9}$$

The component $f(E_\mu)H_2(E_\mu)$ in Eq.6.8 corresponds to the part of the sifted key that is used during error correction process. $f(E_\mu)$ is the ratio of actually needed redundant bits to the corresponding number of the Shannon limit (see Sec.6.1.4). The gain of signal states Q_μ is defined as the probability of Bob getting a photon detection of the pulse for which Alice and Bob use the same basis, while the E_μ is defined as the probability of Bob getting a wrong

detection of the pulse for which Alice and Bob use the same basis. It should be pointed out that in the case of a finite length QKD statistical fluctuations should be analyzed [50, 51].

Optimizing the mean-photon number μ for signal states, in order to get maximum secure rate (Eq.6.8), is a quite straightforward task. For the QKD systems with high attenuation of the quantum channel ($\eta \ll 1$) and low dark counts Y_0 of the single photon detectors ($Y_0 \ll \eta$) the secure key generation rate is given by [50]

$$R \approx -\eta\mu f(e_{det})H_2(e_{det}) + \eta\mu exp(-\mu)[1 - H_2(e_{det})], \tag{6.10}$$

for μ_{opt} fulfilling

$$(1 - \mu_{opt})exp(-\mu_{opt}) = \frac{f(e_{det})H_2(e_{det})}{1 - H_2(e_{det})}, \tag{6.11}$$

where e_{det} is the probability that a photon reaches the wrong detector (see. Sec.6.1.2).

Here, it should be pointed out the following major difference between the original decoy states' idea [49] and the results of its extensive development, which is still going on: while Hwang suggested the mean-photon number for signal pulses much lower than for the decoy states ($\mu \ll \nu$) a more mathematically formal approach of Ma, Qi, Zhao, and Lo [50] and others have showed that the optimal secure key rate is obtained for the decoy states with lower intensity than the signal pulses ($0 \leq \ \nu_1 < \nu_2 <, ..., < \nu_n < \mu$).

The simplest, one-state decoy only, protocol's security has been analyzed in [50] by considering this protocol as an approximation of a more general "vacuum + decoy state" protocol (presented below) with zero vacuum states. Its performance, for transmission distances up to 80 km, was found to be close to the optimal decoy protocol (asymptotic case), with infinite number of decoy states [50]. While the optimal mean-photon number μ for signal states has been derived in Eq.6.11, the optimal choice of the decoy state mean-photon number ν depends, among other parameters, on the channel attenuation [50]. The one-decoy state protocol's simulation data, published in [50], have showed that for the fiber quantum channel lengths between 20 and 100 km the optimal decoy state mean-photon number ν varies between 0.04 and 0.13.

Another simple decoy protocol uses a "vacuum + decoy state" protocol. Its security was analyzed by Wang [54], which led to the following important finding of the upper bond for the tagging probability Δ (see Eq.6.7), being

a ratio of tagged states in the sifted key,

$$\Delta \leq \frac{\mu}{\nu - \mu}\left(\frac{\mu exp(-\mu)Q_\nu}{\nu exp(-\nu)Q_\mu} - 1\right) + \frac{\mu exp(-\mu)Y_0}{\nu Q_\mu}. \tag{6.12}$$

The Eq.6.12 parameters have already been presented in Eq.6.8. As already mentioned, only a few decoy states are needed in practical QKD implementations. Thus, the "vacuum + decoy state" protocol seems to be a good choice for most of the QKD systems. Its only drawback is a need to provide an infinite attenuation for the vacuum states, which is not an easy task in practical experiments.

Implementing decoy states in the "plug & play" QKD setup (shown in Fig.6.5) is a straightforward task. The only additional component needed for it is a fiber pigtailed acousto-optic amplitude modulator AM located at Bob's site. The AM is used for intensity modulation of the laser pulses in such a way that the signal pulses (with the average photon number μ) are interleaved with one ore more decoy states (with the average photon numbers $\nu_1, \nu_2, ..., \nu_n$). As already mentioned, by analyzing statistical characteristics of both decoy and signal states, a PNS attack can be detected [49–51], which greatly enhances security of "faint-pulse" based QKD systems.

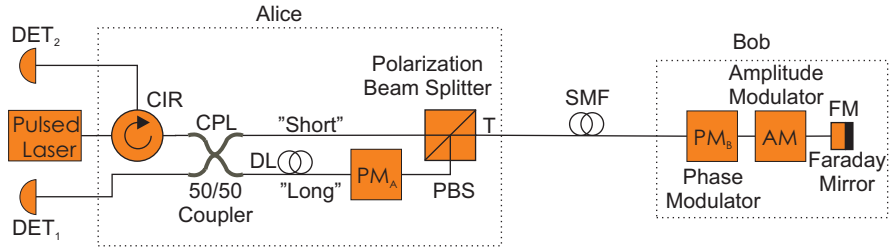

Figure 6.5: "Plug & play" setup with decoy states.

6.2 Multiuser quantum key distribution

6.2.1 Introduction

First theoretical contributions regarding applicability of multiuser QKD over telecom fiber networks were already made in the middle of the nineties when feasibility of multiuser QKD between any two users in passive optical networks (PON), using passive optical couplers, had been studied [55, 56]. In 2005, an important contribution to the field was made by Kumavor, Beal, Yelin, Donkor, and Wang who compared applicability and performance of different PON configurations [57].

PON architecture is a fiber access technology with a passive splitter between the access node and the user. The first PON, dedicated to phone services, was deployed in the US already during the early nineties. The broadband PON (BPON), asynchronous transfer mode (ATM) based, was standardized in 1998. Earlier in the current decade, two new broadband standards have been approved: Ethernet PON (EPON) in 2004 and Gigabit PON (GPON) in 2003. The PON neither needs power nor active electronic parts (for instance, amplifiers). Thus, it is suitable for quantum communications, which use single photons as the information carrier. The network's major drawback for quantum information applications is an incremental loss (in couplers) of photons reaching the receivers when the number of receiving terminals increases.

In the current section, we will shortly review both the PON and switched network configurations. More detailed information about the PON can be found in Paper II in which also switched multiuser "plug & play" QKD in a star and in a tree configuration are presented.

6.2.2 Star network topology

Fig.6.6 shows a simplified PON network in the Star configuration with only one expansion level consisting of an $1 : N$ coupler. In such a configuration the losses are quite limited, especially for the small N. However, they would increase incrementally if the network was further expanded (into one or more star configurations) by adding new couplers at the consecutive nodes. For instance, a new $1 : K$ coupler could be placed at the node R_3, one more coupler at the node of the new star network created by the $1 : K$ coupler and so on. Another disadvantage of the star topology, compared to two other network configurations (Sagnac and "plug & play"), is an incremental increase of the number of single photon detectors, which makes the topology

very expensive. The same disadvantage applies to the wavelength routed network topologies (see Sec.6.2.3).

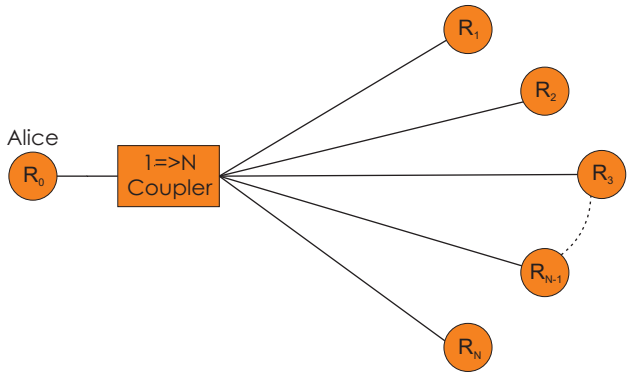

Figure 6.6: Simplified PON N+1 user Star network topology.

6.2.3 Wavelength routed network topologies

Wavelength routed network using an arrayed waveguide grating

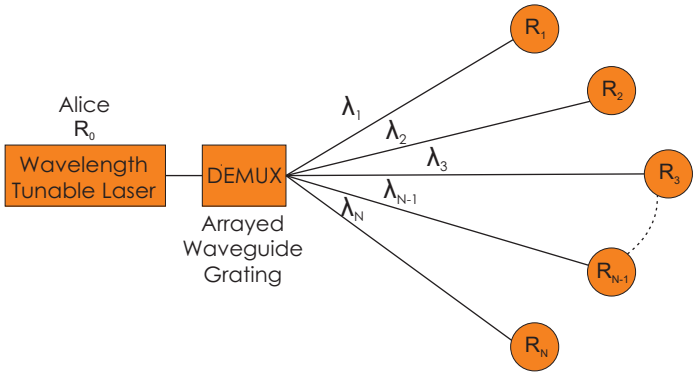

Figure 6.7: Simplified N+1 user wavelength addressed bus network topology.

Instead of using the $1 : N$ coupler for single photon routing to the QKD multiusers, the routing process could be arranged by using a wavelength routed network topology [14, 57]. Fig.6.7 shows a simplified configuration of such a network. Its key components are a wavelength tunable laser and a demultiplexer: an arrayed waveguide grating (AWG) consisting of two multiport couplers ($n \times m$ in size on the input and $m \times n$ in size on the

output), interconnected by an array of waveguides [8]. An AWG can be considered as a generalized version of the Mach-Zehnder interferometer, which is a special case of the AWG for $m = n = 2$. Its working principal can be found, for instance, in [8]. AWG can be used both as a multiplexer and demultiplexer. The latter case is shown in Fig.6.7. The big advantage of the wavelength routed network topology, compared to the star configuration, is an approximately uniform insertion loss of the AWG. Furthermore, the loss does not incrementally increases as in the star topology so, theoretically, the number of users for such a topology is limited only by the AWG's channel spacing [8, 57].

Wavelength routed network with fiber Bragg grating drops

Another wavelength routed topology is a wavelength addressed bus network shown in Fig.6.8. Instead of an arrayed waveguide grating for the signal routing to different users, it uses fiber Bragg gratings (FBG) to drop the signals of different wavelengths into the receiver nodes. The big advantage of the topology is its straightforward scalability: the network can be easily expanded by connecting in series additional gratings. It should be pointed out that the topology is very common in broadband networks.

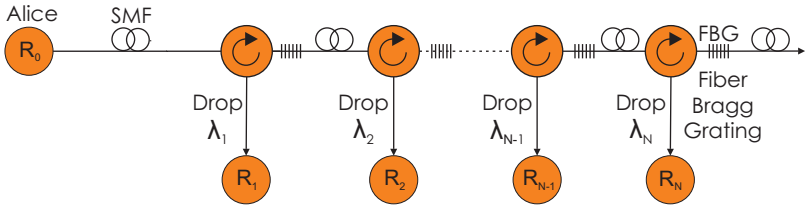

Figure 6.8: N+1 user bus based QKD with fiber Bragg grating drops.

6.2.4 Network topologies with photon detection at the single photon source site

Multiuser "plug & play" QKD

Fig.6.9 shows a simplified N-user "plug & play" QKD with phase encoding. The "plug & play" setup has already been described in Sec.6.1.1 and is also discussed in Papers I and Paper II. Its SMF birefringence compensation's feature has been proved in Sec.4.2.3.

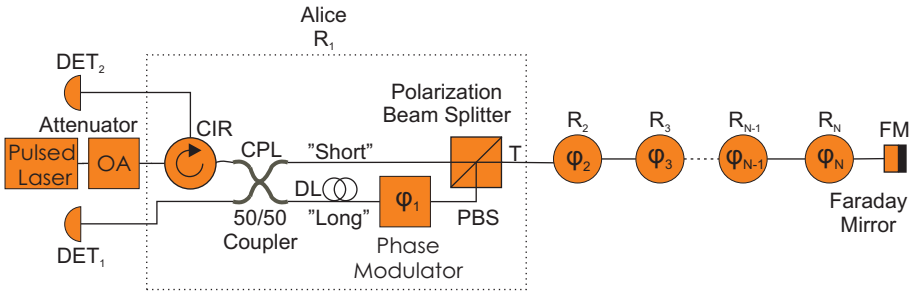

Figure 6.9: Simplified N-user "plug & play" QKD with phase encoding.

Multiuser Sagnac QKD

Fig.6.10 shows a simplified N-user Sagnac QKD with phase encoding. Sagnac interferometer has already been described in Sec.4.2.4 and is also discussed in Papers III and Paper IV. In Sec.4.2.4 its birefringence has been analyzed, while in Paper V we show how to compensate for it.

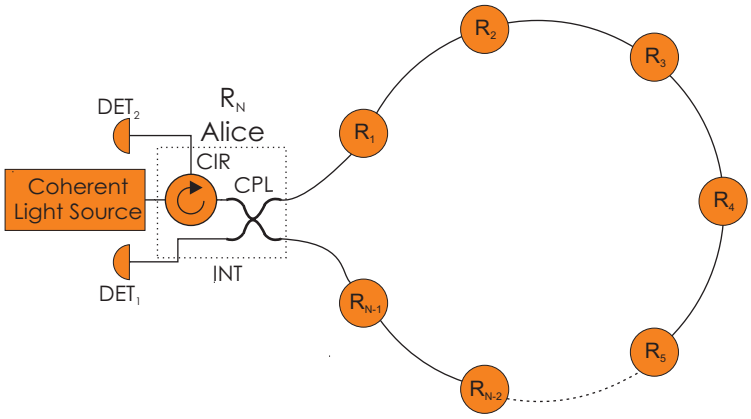

Figure 6.10: N-user Sagnac QKD.

6.2.5 Multiuser QKD experiments

In the first telecom window (at 850 nm) a PON based experiment in 2007 [58] led to transmission distances of less than 10 km for four active nodes of the total 32 nodes provided by a standard 1 x 32 telecom splitter. In the standard 1550 nm telecom window, experimental results for three quantum transmission nodes with secure quantum transmission distance in the range

of 15 km were presented in 2006 [59]. Also the Darpa quantum network in the Boston Metropolitan area showed similar results in 2002 [60].

The first Sagnac QKD experiment was carried out in 2002 at 830 nm and at transmission distances below 1 km [30]. The first Sagnac QKD experiment in the third telecom window (at 1550 nm) was carried out in 2003 [31] at the 3 km total transmission loop. The last, to the best of our knowledge, Sagnac QKD experiment in the third telecom window was performed in 2006 at the total transmission loop of 40 km [32]. Paper II and Paper III provide more information about various multiuser QKD experiments.

6.3 Quantum secret sharing

The reported work has been based on a new, innovative multiparty quantum secret sharing protocol using single qubit [61], as it is showed in Figure 1. A qubit is prepared in an initial state by the part R_1 and is sent sequentially, from R_1 to R_N, over the quantum channel, until is measured by the last part R_N. Each party modulates the photon with a randomly chosen phase

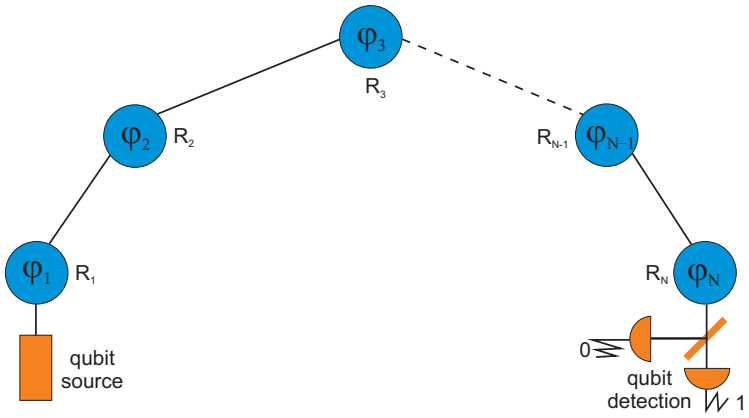

Figure 6.11: N-party single qubit secret sharing. A qubit (in our case a photon) is prepared in an initial state by the part R_1, using a single qubit source, and is sent sequentially, from R_1 to R_N, over the quantum channel, until is measured by the last part R_N. Each party modulates the photon with a randomly chosen phase $\phi_i (i = 1, ..., N-1)$ between 0, $\pi/2$, π or $3\pi/2$. The part R_N measures with phase modulation choice ϕ_N between 0 and $\pi/2$. In half of the cases the phases add up in such a way that the measurement results are deterministic, indicating a constructive or destructive interference. These cases can be used for the secret sharing.

$\phi_i(1, ..., N-1)$ equal 0, $\pi/2$, π, or $3\pi/2$. The parties R_1, R_2,..., and R_{N-1} modulating phase choices 0, $\pi/2$, π, and $3\pi/2$ can be assigned into two bases $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. The part R_N phase modulation choice ϕ_N is limited to two phases only: 0 (which belongs to the basis $\{0, \pi\}$) and $\pi/2$ (which belongs to the basis $\{\pi/2, 3\pi/2\}$). In half of the cases the phases add up in such a way that the measurement results are deterministic, indicating a constructive or destructive interference with the total correlation function given by

$$E(\phi_1, ..., \phi_N) = \cos(\phi_1 + ... + \phi_N). \tag{6.13}$$

These cases can be used for the secret sharing. After the photon has been detected, the parties in a reverse order (i.e. R_N, R_{N-1},..., R_2, R_1) announce on a public channel their basis choices, but keep their particular modulating phases secret. From the publicly shared basis information, the parties can determine which runs led to deterministic measurements. In these cases, any subset of $N-1$ parties is able to infer the modulating phase of the remaining part if all the parties of the subset collaborate and reveal among themselves their modulating phases. If the subset includes the part R_N, it must reveal the measurement result (it has already revealed its basis choices on the public channel). In such a way the goal of secret sharing has been achieved.

Chapter 7

Conclusion and future work

7.1 Our achievements

A natural development awaiting quantum communications is their migration into commercial switched telecom networks, intranets, and the Internet. Such a migration concerns both multiuser quantum key distribution and multiparty quantum secret sharing, presented in the thesis, and is an enormously challenging task due to the nature of quantum communications that use single photons as information carriers. In our research work on multiuser secure quantum communications, we have only explored a small part of the challenges awaiting, first quantum communications scientists, and later (when the necessary scientific and technological breakthroughs have been achieved) the industry.

Our multiparty quantum secret sharing experiment, presented in Paper I, was funded by the Swedish Defense Materiel Administration (FMV), which requested a working (on a "proof of principle" level) quantum secret sharing demonstrator in SM fiber, implementing (for the first time) a new, innovative multiparty quantum secret sharing protocol using single qubits (photons in our case). Since the experiment was started in a new-built fiber lab, it requested purchase of not only the components needed for its realization but also a lab infrastructure and all necessary instruments.

The optical and electronic system design of the secret sharing demonstrator proved to be a complex and time consuming task. For instance, we designed a new innovative scheme, providing polarization insensitivity for standard telecom phase modulator, being the key component of both the secret sharing demonstrator and other experiments. On the software side, we

have developed LabView FPGA (Field Programmable Gate Array) programs for the National Instrument Digital Acquisition card that was intended to control the phase modulators and detectors of the setup. Due to the project's urgency, we put the further development of the FPGA control system on hold and instead used a prereleased programmable pulse generator from Quantum Composers Inc., that solved most of the timing problems. However, the original design approach of using the FPGA based timing control is superior (in regards to the demonstrator's performance) and should be completed in the future.

Our experiment was the first quantum secret sharing in fiber. We carried it out in three, four, and five-party implementations, using the "plug & play" configuration with phase encoding. In our experiment, we achieved reasonably long distances and rates. For instance, in the three-party implementations we achieved quantum secret sharing transmission distances of 50 km, 61 km, and 66 km at the mean-photon numbers $\mu = 0.1$, $\mu = 0.2$, and $\mu = 0.3$, respectively. The achieved raw rates, below 100 Hz, could be much higher if, instead of our standard InGaAs avalanche photodiode based single photon detectors, the newly available superconducting devices were used in the experiment.

After exploring quantum secret sharing, we moved into multiparty QKD, presented in Paper II. While our former experiment was the first quantum secret sharing in fiber, multiparty QKD experiments were performed (mainly in the current decade) by a couple of labs, using passive optical networks (PON). However, only two, known to us, experiments over short distances (less than 15 km) and with only three nodes were carried out in the third telecom window (1550 nm), which is the most commonly deployed telecom network.

In our experiment, we have implemented five quantum transmission nodes in a switched star and in a tree configuration, using the "plug & play" setup with phase encoding. We implemented more nodes and achieved longer secure quantum communication distances than all other multiuser QKD experiments. The achieved stable (in many hours) measurement results confirmed feasibility of multiuser QKD over switched telecom networks.

After the two, previously mentioned, experiments were completed, our attention got focused on other network topologies than the ones explored in these experiments. It led to our decision on testing feasibility of multiuser Sagnac QKD in SM fiber due to the fact that ring network topologies are of major interest for both backbone networks and intranets. However, its

intrinsic SM fiber birefringence sensitivity had led to a very limited number of experimental trials, which were only performed over short distances and at low rates. Thus, we focused our attention on finding a way for birefringence compensation, which finally led to a novel concept for compensation of SMF birefringence effects in Sagnac, based on a polarization control system and a polarization insensitive phase modulator, that made it possible to carry out a long distance QKD at much longer secure quantum communication distances and higher rates than all other published Sagnac QKD experiments. Our birefringence's compensation opens the door to other than QKD Sagnac-based applications over SM fiber links, such as precise optical sensing, dispersion characteristics of optical fibers, acoustic and strain sensing, and generally sensing of any time varying phenomenon.

Finally for this experiment, it should be pointed out that the achieved rates could be much higher if instead of our standard InGaAs avalanche photodiode based single photon detectors the newly available superconducting devices were used in the experiment. Nevertheless, the measurement results showed that Sagnac QKD is feasible over telecom SMF networks. In order to provide an unconditional security for the key distribution we have implemented one-decoy state protocol in Sagnac QKD setup. The experiment is presented in Paper III.

After a successful execution of Sagnac QKD, our attention moved back to multiparty quantum secret sharing. We got very interested in exploring feasibility of Sagnac multiparty quantum secret sharing, despite the big challenges awaiting us due to a complicated timing for the parties' phase modulators as well as severe link attenuation, caused by the phase modulators. Nevertheless, we were able to successfully perform three and four-party quantum secret sharing at long distances and reasonably high rates. For instance, we achieved the total Sagnac transmission loop distances of $55-75$ km in the three-party and $45-55$ in the four-party configuration. The experiment, which is presented in Paper IV, was the first quantum secret sharing over fiber Sagnac.

Both previously mentioned Sagnac experiments resulted in successful outcomes which showed feasibility of Sagnac QKD and quantum secret sharing in SM fiber networks. However, we were missing a theoretical model for the birefringence compensation, which was an annoying component in the otherwise successful projects so we decided to find such a model, which was a very challenging task. In order to solve the problem, we had to question the widely accepted, by the quantum cryptography community, model of the

birefringence compensation in the "plug & play" setup. This approach and using the Kapron equivalence (described in the thesis) led to a consistent model of Sagnac birefringence and a new, more general model for the "plug & play" setup. The model is presented in Paper V, in which we also describe our previously mentioned concept of the SMF birefringence effects compensation in Sagnac. We consider the model and birefringence compensation system, described in Paper V, as one of our major contributions presented in the thesis.

7.2 Future

Our research work on multiuser secure quantum communications has been focused on transmission over fiber. Thus, even our visions concerning future development of quantum communications are limited to fiber media.

One of the key elements in the future migration of quantum communications into standard telecom networks is the establishment of industrial standards for quantum encoding and transmission protocols, quantum networking as well as for network managements. Fortunately, on July 29, 2008 the European Telecommunications Standards Institute (ETSI) founded the Industry Specification Group on Quantum Key Distribution and Quantum Technologies (QISG) that addresses standardization issues in quantum cryptography and other quantum technologies. The group's main focus is on definition of security objectives; systematization of security proofs; QKD security specification; standardization of QKD components (sources, detectors) and interfaces (including common interfaces between macroscopic components).

The first important step in the standardization efforts was last year's release by SECOQC (Secure Communication based on Quantum Cryptography), being an EU initiative in quantum information and quantum communications, of the SECOQC Quantum-Back-Bone Link-Interface (QBB-LI), an interface documentation as well as a software package, including a network node simulator and a sample quantum device. By this interface, quantum cryptographic links can be inserted into the SECOQC Quantum Back Bone secrets distribution network. The software package can also be used without actual quantum cryptographic links to simulate a SECOQC QKD network with an arbitrary number of network nodes and quantum cryptographic links. In the SECOQC QBB demonstrator, seven technologically different QKD distribution links were connected over it to the nodes of the

network. The SECOQC QKD network is organized in three layers: QKD link layer, transport layer, and network layer. Key creation and QKD are hidden in the lowest layer, i.e. in the QKD link layer.

As previously mentioned, the future migration of quantum communications into standard telecom networks needs to overcome many technological challenges in order to reduce and finally eliminate quantum communications limitations in transmission distance, rates, and availability to a common consumer. We think that one should question a feasibility of such a migration into all types of telecom switched fiber networks, intranets, and the Internet. The reason for the questioning is the fact that most of the networks practically are not passive since they include such active components as optical and electronic amplifiers; optical to analog and analog to optical signal converters; and many others active components and thus are not suitable for transmitting single photons. The only suitable network topology for quantum communications is PON (passive optical network), with all its limitations (for instance, an incremental loss when the number of nodes increases) discussed in the thesis.

In order to migrate quantum communications into other than PON network topologies one could envision quantum repeaters that, however, are probably many decades from practical realization since they require use of a complex entanglement purification [62, 63]. In order to design such a repeater a long quantum channel should be divided into shorter segments, purified separately, before they are reconnected. Connecting two segments of a channel is to build up quantum correlations across the compound channel from correlations across the individual segments which can be done by entanglement swapping or teleportation of entanglement.

Another more realistic migration method builds on a "classical trusted relaying network" [60], which uses local keys that are generated over QKD links, being a part of a larger network, and then stored in the end nodes (the trusted relays) of the link. The key distribution between distant nodes is carried out over a chain of trusted relays connected by QKD links. However, security of a practical network based on trusted relays is questionable.

Finally, it should be emphasized that a number of security issues in multiuser quantum communications still awaits strict mathematical solutions, for instance, decoy implementation in both multiuser QKD and multiparty secret sharing.

Bibliography

[1] S. Stenholm and K. A. Suominen, *Quantum approach to informatics* (Wiley-Interscience, Hoboken, New Jersey, 2005).

[2] J. D. Franson, Phys. Rev. Lett. **62**, 2205–2208 (1989).

[3] K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[6] G. Brooker, *Modern classical optics* (Oxford University Press, New York, USA, 2003).

[7] M. Mansuripur, *Classical optics and its applications* (Cambridge University Press, Cambridge, UK, 2002).

[8] R. Ramaswami and K. N. Sivarajan, *Optical networks, a practical perspective* (Morgan Kaufmann Publishers, Harcourt Inc., Bellingham, Washington, 2002).

[9] E. Udd, *Fiber optic sensors* (John Wiley & Sons, Inc., Hoboken, New Jersey, 2006).

[10] J.-P. Goure and I. Verrier, *Optical fiber devices* (Institute of Physics Publishing, Bristol and Philadelphia, USA, 2002).

[11] B. E. A. Saleh and M. C. Teich, *Fundamentals of photonics* (John Wiley & Sons, Inc., Hoboken, New Jersey, USA, 2007).

[12] C. Pask, A. Snyder, and D. J. Mitchell, JOSA **65**, 356 (1975).

[13] J. Bures, *Guided optics* (Wiley-VCH Verlag GmbH & Co, KGaA, Weinheim, Germany, 2009).

[14] S. V. Kartalopoulos, *Introduction to DWDM technology* (IEEE Press, New York, USA, 2000).

[15] K. Thyagarajan and A. Ghatak, *Fiber optic essentials* (A John Wiley & Sons, Inc., New York, USA, 2007).

[16] P. Nouchi, L. A. de Montmorillon, P. Sillard, A. Bertaina, and P. Guenot, C. R. Physique **4**, 29 (2003).

[17] E. Collett, *Field guide to polarization* (SPIE Press, San Diego, USA, 2005).

[18] H. A. Bachor and T. C. Ralph, *A guide to experiments in quantum optics* (Viley-VCH, Weinheim, 2004).

[19] A. Muller *et al.*, Appl. Phys. Lett. **70**, 793 (1997).

[20] F. P. Kapron, N. F. Borrelli, and D. B. Keck, IEEE Jour. of Quant. Electron. **QE-8**, 222 (1972).

[21] D. B. Mortimore, J. Lightwave Technol. **6**, 1217 (1988).

[22] C. Tsao, *Optical fibre waveguide analysis* (Oxford Science Publ., Oxford, 1992).

[23] M. Martinelli, Opt. Commun. **72**, 341 (1989).

[24] B. Culshaw, Electr. Lett. **17**, 1 (2006).

[25] G. Sagnac, C. R. Acad. Sci.,Paris **95**, 708 (1913).

[26] E. Udd, Sensing and instrumentation applications of the Sagnac fiber optic interferometer, in *Proceedings SPIE*, , Proc. SPIE Vol. 2341, pp. 52–59, 1994.

[27] J. Zheng, Meas. Sci. Technol. **41**, 727 (2005).

[28] L. R. Jaroszewicz, Molecular and Quantum Acoustics **22**, 133 (2001).

[29] L. R. Jaroszewicz, Fiber-optic Sagnac interferometer as real sensor of the physical quantities, in *Proceedings of the Symposium on Photonics Technologies*, , Framework program Vol. 7, pp. 99–101, 2006.

[30] T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, IEEE Photonics Tech. Lett. **14**, 576 (2002).

[31] C. Zhou, G. Wu, L. Ding, and H. Zeng, Appl. Phys. Lett. **83**, 15 (2003).

[32] B. Qi, L. L. Huang, H. K. Lo, and L. Qian, Quantum key distribution based on a Sagnac loop interferometer and polarization-insensitive phase modulators, in *IEEE International Symposium on Information Theory*, pp. 2090–2093, 2006.

[33] W. A. de Brito and R. V. Ramos, J. Mod. Opt. **55**, 1231 (2008).

[34] D. S. Bethune and W. P. Risk, New J. Phys. **4**, 42.1 (2002).

[35] C. C. Gerry and P. L. Knight, *Introductory quantum optics* (Cambridge University Press, Cambridge, UK, 2005).

[36] S. Singh, *The code book* (Anchor Books, Hoboken, New Jersey, USA, 1999).

[37] G. S. Vernam, Journal of the IEEE **55**, 109–115 (1926).

[38] W. Diffie and M. Hellman, Multi-user cryptographic techniques, in *AFIPS Proceedings*, edited by AFIPS, , Advances in Cryptology Vol. 45, pp. 109–112, 1976.

[39] R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120–126 (1978).

[40] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge,UK, 2000).

[41] D. Dieks, Physics Letters **92A**, 2305051.1 (1982).

[42] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. B **67**, 743 (1998).

[43] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zibiden, New J. Phys. **4**, 41.1 (2002).

[44] D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, in *Proceedings of Crypto '96*, Advances in Cryptology, pp. 343–357, 1996.

[45] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[46] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[47] N. Lütkenhaus, Phys. Rev. A **61**, 052304.1 (2004).

[48] C. Shannon, Bell Syst. Tech. J. **27**, 379–423, 623–656 (1948).

[49] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901.1 (2003).

[50] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326.1 (2005).

[51] X. B. Wang, Phys. Rev. A **75**, 052301.1 (2007).

[52] D. Gottesman, H.-K. Lo, Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[53] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504.1 (2005).

[54] X. B. Wang, Phys. Rev. Lett. **94**, 230503.1 (2005).

[55] P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, Elec.lett. **30**, 1875 (1994).

[56] P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, Nature **385**, 47 (1997).

[57] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, Jour. Light. Tech. **23**, 268 (2005).

[58] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, J. Quantum Electron. **43**, 130 (2007).

[59] T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, and H. Takahashi, Opt. Comm. **263**, 120 (2006).

[60] C. Elliott, Opt. Comm. **4**, 46.1 (2002).

[61] C. Schmid *et al.*, Phys. Rev. Lett. **95**, 230505.1 (2005).

[62] W. Dür, H.-J. Briegel, J. I. Cirac1, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[63] D. Collins, N. Gisin, and H. D. Riedmatten, J. Mod. Opt. **52**, 735–753 (2003).

Part II:
Scientific papers