TECHNISCHE UNIVERSITÄT WIEN

Dissertation

Novel Schemes for QKD

Ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der Naturwissenschaften unter der Leitung von

Univ.-Doz. Dipl.-Ing. Dr. Martin Suda

E141

Atominstitut der Österreichischen Universitäten

eingereicht an der Technischen Universität Wien

Fakultät für Physik

von

Mag. rer. nat. Florian Hipp

Martikelnummer: 0309072

Meiselstraße 14, 1150 Wien

Wien am, 31. 08. 2016

Kurzfassung der Dissertation

Neue Ansätze zur Quanten-Schlüssel Verteilung

Quanten Kryptographie oder genauer gesagt Quanten-Schlüssel Verteilung (Quantum Key Distribution - QKD) ist die erste Anwendung der Quantentheorie die kurz davor steht den Sprung vom Experiment zur industriellen Verwertung zu schaffen. Ermöglicht wurde diese Erfolgsgeschichte durch zahllose theoretische und experimentelle Arbeiten innerhalb der letzten 30 Jahre. Thema dieser Arbeit sind experimentelle Fortschritte der jüngsten Zeit, QKD Protokolle und Attacken auf QKD sowie eine mögliche Integration dieser quantenbasierten Technologie in die "klassische Welt". Die größte Herausforderung bei dieser Zusammenführung ist in drei Bereichen zu finden, nämlich die unzureichende technische Ausgereiftheit der verwendeten Hardware, die das Gebiet des "quanten Hackens" hervorgebracht hat, QKD über lange Distanzen (100km und mehr) und die Integration von QKD in bereits verlegte Backbone und Access Netzwerke. Zwar werden alle drei Gebiete in dieser Arbeit behandelt, neue Erkenntnisse werden zu den beiden letzteren erörtert, da das Ausnutzen von technischen Fehlern in Hardware im Prinzip nicht mehr als ein Wettlauf zwischen Hackern und Hersteller ist, der im Prinzip schon durch hardwareunabhängige QKD Modelle gelöst wurde.

Als möglicher Ansatz zum Überbrücken großer Distanzen mit QKD Technologie bietet sich die satellitenbasierte Kommunikation zwischen entfernten Punkten auf der Erde an. Zu diesem Zweck stellt diese Arbeit zwei Generationen von Lithiumniobat Wellenleitern vor, die auf spontaner parametrischer Downconversion (SPDC) und Quasi Phasen Anpassung (QPS) zur Erzeugung verschränkter Photonenpaare basiert. Das Ziel ist die Entwicklung einer autonomen, komplett integrierten Quelle polarisationsverschränkter Photonen im C-Band. Verglichen mit anderen Quellen ist in diesem Fall der Herstellungsprozess des Wellenleiters sowie dessen Integration in fasergebundene Optik bei einem eingeschränkten Formfaktor ($< 0.5m^2$) eine zusätzliche Herausforderung. In einem nicht fasergebundenen Aufbau wurde für die erste Generation von Wellenleiter eine 'Visibility' von über 91% und eine 'spectrale Brightness' von 10^6 $\frac{\text{Paare}}{s \cdot nm \cdot W}$ gemessen. Bei der zweiten Generation von Wellenleitern, komplett fasergebunden, wurde hingegen nur 75% 'Visibility' and $4 \cdot 10^3$ $\frac{\text{Paare}}{s \cdot nm \cdot W}$ 'spectrale Brightness' erreicht. Dieser wesentlich schlechtere Wert kommt von hohen Verlusten beim Übergang von Kristall auf Faser und rührt vom Anbringen der Faser auf den Wellenleiter her.

Das zweite große Thema dieser Arbeit ist die mögliche Integration von QKD in bereits bestehende Netzwerkinfrastruktur und der damit einhergehende Einfluss starker klassischer Datensignale auf die sehr schwachen Quantensignale. Trotz erarbeiteter Konzepte die es erlauben die klassischen Kanäle zu überbrücken und den Quantenkanal von diesen

zu trennen, müssen Beeinträchtigungen durch nichtlineare Prozesse, überwiegend Ramanstreuung, berücksichtigt werden, gerade wenn alle Kanäle über dieselbe Faser laufen, wie es in der sogenannten Single-Feeder Methode üblich ist. Sensible Raman Messungen bis zur Energie von Einzelphotonen, durchgeführt an einem 20 Kanal DWDM Netzwerk, zeigen, dass sogar über 200nm weg von den klassischen Daten Kanälen ca. 10^6 $\frac{\text{photons}}{s \cdot nm}$ erzeugt werden. Unsere Simulationen und experimentellen Daten ergaben weiterhin, dass ein Quantenkanal durchaus in passive optische Netzwerke integrierbar ist, wenn ausreichend spektraler Abstand sowie passende Wellenlängen und zeitliche Filter verwendet werden, die es erlauben die einzelnen Photonen vom Hintergrund zu trennen. Diese Resultate wurden mit einer Quelle polarisationsverschränkter Photonen gemessen, bestehend aus einem ppKTP Kristall in Sagnac Konfiguration, der Photonenpaare bei 589nm und im O-Band bei 1310nm erzeugt. Damit ist es gelungen eine full-duplex Punkt zu Punkt Verbindung über 13.2km aufzubauen bei der sowohl klassische Signale als auch Quantensignale über dieselbe Faser geschickt werden.

Die Erkenntnisse die in dieser Arbeit präsentiert werden zeigen die Möglichkeiten aber auch die Grenzen von QKD sowohl für die Übertragung über weite Strecken durch satellitenbasierte Systeme als auch für die Integration in optische Netzwerke. Diese Arbeit wird mithelfen Standards für mögliche zukünftige Entwicklungen im Bereich QKD zu setzen.

Abgesehen von dieser Arbeit wurden die Ergebnisse im Journal Optics Express (2015), den SPIE Proceedings (2016) und der CLEO Europe Konferenz (2015) sowie anderen kleineren Konferenzen vorgestellt.

Abstract

Quantum cryptography or quantum key distribution (QKD) in particular is the first application of quantum theory that is about to accomplish the leap from laboratory to industry. This story of success was enabled by plenty of theoretical and experimental research over the past 30 years. In this work current state of the art experiments, protocols and threats of QKD are discussed and a potential integration of this quantum technology into the classical world is presented. The main challenges of this merge can be summarized by three issues, namely impurities of technical devices, which enable the possibility of quantum hacking, long haul QKD between two distant parties (>100km) and an integration of quantum channels into existing backbone and access networks. Although all three problems are discussed in this thesis, new insights are given to the latter two, since the impurity of devices seems to be more of an arms race between manufacturer and hackers and is, at least theoretically, solved by device independent QKD schemes.

A possible solution for long haul encryption using QKD is a satellite based communication between two remote earth-bound parties. For this purpose two generations of Lithium-Niobate waveguide crystal sources are presented that generate entangled photon pairs using spontaneous parametric down conversion (SPDC) and Quasi Phase Matching (QPM). The goal is the development of an autonomous, fully integrated source that emits polarization entangled photon pairs in the C-Band. Compared to other sources, the challenge in this case is the fabrication process of the crystal itself as well as the integration in fiber optics with a suitable small footprint for space application ($< 0.5m^2$). In a free space setup visibilities over 91% and a spectral brightness of 10^6 $\frac{\text{pairs}}{s \cdot nm \cdot W}$ have been measured for the first generation waveguide source. However, for the fully integrated version of the second waveguide only 75% visibility and $4 \cdot 10^3$ $\frac{\text{pairs}}{s \cdot nm \cdot W}$ spectral brightness could be achieved due to high losses originating in the fiber bonding process. In the second topic of the thesis a possible integration of QKD into existing optical network infrastructure and the corresponding influence of the strong classical signal on the quantum signal is discussed. Despite elaborated concepts to bypass and separate the strong classical channels from the quantum signal, nonlinear impairments mainly caused by Raman scattering have to be considered, especially in a single feeder scheme, where all signals share the same fiber. Raman measurements of a 20 Channel DWDM signal down to single photon energy levels show that even 200nm away from the classical signals $\approx 10^6$ $\frac{\text{photons}}{s \cdot nm}$ are present. Furthermore, simulations and measurements show that an integration of a quantum channel in passive optical networks is possible with a reasonable spectral distance as well as suitable filtering in the optical and temporal domain to recover the single photons from the noisy background. The results have been gained

using a polarization entangled QKD source with ppKTP crystal in Sagnac configuration with photon pairs emitted at 586nm and in the O-Band at around 1310nm. Finally we were able to establish an encrypted full duplex communication with quantum and classical post-processing channel sharing a single 13.2km fiber for usage in the telecom network.

The insights gained in this work demonstrate possibilities and limitations of QKD in satellite based free space long haul transmissions as well as network integration and will help to set standards for possible future QKD applications.

Apart from this work the results have been published in Optical Express (2015), SPIE proceedings (2016) and CLEO Europe (2015) among other smaller conference contributions.

Declaration

I, Florian Hipp, hereby declare that this thesis titled, 'Novel Schemes for QKD' and the work presented in it are my own. All contributions to it that are not done by myself, are, to my best knowledge, marked as such and whenever possible stated with the respective source. The main results that have been gathered during my work at the Austrian Institute of Technology (AIT) and my PhD studies at the Technical University Vienna (TU Wien), are, apart from stated publications, exclusively presented in this thesis for the purpose of acquiring the academic doctor degree of technical physics ('Doktor der Naturwissenschaften technische Physik') at the TU Wien.

Florian Hipp
31. 08. 2016

Acknowledgements

This page is dedicated to all people that helped me accomplish this work and all the experiences that have gone along with it. First of all I want to express my gratitude to my supervisor, Martin Suda, who supported me with his kindness, his wonderful sense of humor and of course his knowledge and curiosity about various fields of physics. Furthermore I want to thank my colleagues and supervisors from AIT, in particular Andreas Poppe and Hannes Hübel as well as Martina Miková, Michael (Mike) Hentschel and Bernhard Schrenk, who helped a former theorist to find his way around the lab.
Another VIP for this work I want to thank is Slavisa Aleksic, who introduced me to the world of classical networks and telecommunications and contributed a great part to the success of this thesis.
Last but not least I want to thank my family and friends for their constant support and interest in my work as well as my girlfriend Conny for all the wonderful years and the years to come with our gorgeous yet anonymous girl.

Contents

List of Figures

Abbreviations

10G-EPON	**10** **G**bit/s **E**thernet **P**assive **O**ptical **N**etwork
AES	**A**dvanced **E**ncryption **S**tandard
AIT	**A**ustrian **I**nstitute of **T**echnology
APD	**A**valanche **P**hoto **D**iode
ASE	**A**mplified **S**pontaneous **E**mission
ATM	**A**synchronous **T**ransfer **M**ode
ATOF	**A**cousto-optic **T**unable **F**iltering
ATT	**Att**enuation
AWG	**A**rrayed **W**aveguide **G**rating
BB84	Type of QKD protocol established 19**84**; after **B**ennett, **B**rassard
BB92	Type of QKD protocol established 19**92** by Eckart; after **B**ennett, **B**rassard
BBO	β-**B**arium **B**orate
BER	**B**it **E**rror **R**ate
BS	**B**eam **S**plitter
BW	**B**irefringent **W**edges
CAN	**C**ampus **A**rea **N**etwork
CBC	**C**ipher **B**lock **C**haining
CFB	**C**ipher **F**eed**b**ack (CFB)
CHSH	**C**lauser, **H**orne, **S**himony, **H**olt
CO	**C**entral **O**ffice
COW	Type of QKD protocol, **C**oherent **O**ne **W**ay
CPE	**C**ustomer **P**remises **E**quipment
CRHF	**C**ollision **R**esistant **H**ash **F**unctions
CV	**C**ontinuous **V**arible
CWDM	**C**ourse **W**avelength **D**ivision **M**ultiplexing
DES	**D**ata **E**ncryption **S**tandard

DFG	**D**ifference **F**requency **G**eneration
DG	**D**elay **G**enerator
DM	**D**ichroic **M**irror
DNSSEC	**D**omain **N**ame **S**ystem **S**ecurity **E**xtensions
DPS	Type of QKD protocl, **D**ifferential **P**hase **S**hift
DS	**D**own **S**tream
DV	**D**iscrete **V**ariable
DWDM	**D**ense **W**avelength **D**ivision **M**ultiplexing
ECB	**E**lectronic **C**ode **B**ook
ECC	**E**lliptic **C**urve **C**ryptography
ECDF	**E**lliptic **C**urve **D**iffe-Hellman
ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
EDFA	**E**rbium **D**oped **F**iber **A**mplifier
EPON	**E**thernet **P**assive **O**ptical **N**etwork
EPR	**E**instein **P**odolski **R**osen, synonymous for entanglement
FBG	**F**iber **B**ragg **G**rating
FWDM	**F**ar **W**ave **D**ivision **M**ultiplexing
FWHM	**F**ull **W**idth **H**alf **M**aximum
GMPLS	**G**eneral **Multi P**rotocol **L**abel **S**witching
GPON	**G**igabit **P**assive **O**ptical **N**etwork
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**lobal **S**ystem for **M**obile Communications
GUI	**G**raphical **U**ser **I**nterface
IEEE	**I**nstitut of **E**lectrical and **E**lectronics **E**ngineers
InGaAS	**I**ndium **G**allium **A**rsenide
IPSec	**I**nternet **P**rotocol **Sec**urity
ITU-T	**I**nternational **T**elecommunication **U**nion, -**T** denotes the standardization unit
KDP	**K**alium**d**ihydrogen**p**hosphat
KTP	**K**alium**t**itanyl**p**hosphat
LAN	**L**ocal **A**rea **N**etwork
LFSR	**L**inear **F**edback **S**ift **R**egister
LOCC	**L**ocal **O**peration and **C**lassical **C**ommunication
LWPF	**L**ow **W**ater **P**eak **F**iber

MAC	**M**essage **A**uthentication **C**ode
MAN	**M**etropolitan **A**rea **N**etwork
MDC	**M**odifcation **D**etection **C**odes
NTC	**N**egative **T**emperature **C**ontroller
OADM	**O**ptical **A**dd **D**rop **M**ultiplexer
OBPF	**O**ptical **B**and **P**ass **F**ilter
OFB	**O**utput **F**eed**b**ack
OLT	**O**ptical **L**ine **T**ermination
ONU	**O**ptical **N**etwork **U**nit
OSA	**O**ptical **S**pectrum **A**nalyser
OSC	**O**ptical **S**upervisory **C**hannel
OTP	**O**ne **T**ime **P**ad
OWHF	**O**ne **W**ay **H**ash **F**unctions
OXC	**O**ptical **C**ross **C**onnect
PBS	**P**olarizing **B**eam **S**plitter
PC	**P**olarization **C**ontrol
PDH	**P**lesiochronous **D**igital **H**ierarchy
PM	**P**hase **M**atching
P&M QKD	**P**repare and **M**easure QKD
PMT	**P**hoton **M**ulitplier **T**ube
PON	**P**assive **O**ptical **N**etwork
ppXXX	**P**eriodically **p**oled XXX, (e.g. ppKTP)
PtC	**P**oint **t**o **C**urb
PtMP	**P**oint **t**o **M**ulti **P**oint
PtP	**P**oint **t**o **P**oint
QBER	**Q**uantum **B**it **E**rror **R**ate
QE	**Q**uantum **E**fficiency
QKD	**Q**ist **K**ey **D**istribution
QPM	**Q**uasi **P**hase **M**atching
RGC	**R**aman **G**ain **C**urve
RSA	Encryption algorithm, named after **R**ivest,**S**hamir, **A**dleman
Rx	**R**eceiver
SARG04	Type of QKD protocol established 20**04**; after **S**carani, **A**cin, **R**ibordy, **G**isin

SDH	**S**ynchronous **D**igital **H**ierarchy
SFG	**S**um **F**requency **G**eneration
SFP	**S**mall **F**orm-factor **P**luggable
SHA	**S**ecure **H**ash **A**lgorithm
SHG	**S**econd **H**armonic **G**eneration
SNR	**S**ignal to **N**oise **R**atio
SOA	**S**emiconductor **O**ptical **A**mplifier
SONET	**S**ynchronous **O**ptical **Net**work
SPAD	**S**ingle **P**hoton **A**valanche **D**etector
SPDC	**S**pontaneous **P**arametric **D**own **C**onversion
SSH	**S**ecure **Sh**ell
SSMF	**S**tandard **S**ingle **M**ode **F**iber
STM	**S**ynchronous **T**ransport **M**odule
SW	**Sw**itch
TDC	**T**ime to **D**igit **C**onverter
TDM	**T**ime **D**ivision **M**ultiplexing
TE	**T**ransversal **E**lectric
TM	**T**ransversal **M**agnetic
TM	**T**richroic **M**irror
TMN	**T**elecommunication **M**anagement **N**etwork
TLS	**T**ransport **L**ayer **S**ecurity
TTM	**T**ime **T**agging **M**odule
Tx	**T**ransmitter
UDP	**U**ser **D**atagram **P**rotocol
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
US	**U**p **S**tream
WDM	**W**avelength **D**ivision **M**ultiplexing
WEP	**W**ired **E**quivalent **P**rivacy
WG	**W**ave **G**enerator
WPA	**W**i-Fi **P**rotected **A**ccess
XG-PON	**10-G**igabit-capable **P**assive **O**ptical **N**etwork

Chapter 1

Introduction

1.1 Why Cryptography and why "Quantum"?

The usual way to start a thesis is to give a short motivation about the topics discussed in upcoming chapters. For work that is located rather in the field of fundamental research with no direct application these lines boil down to the curiosity of a deeper insight into nature, rooted in a primary human instinct. The irony of introducing cryptography lies in the fact that it is mainly motivated by successfully hiding information. This goal is usually achieved by scrambling a message in such a way that its meaning can only be reassembled by the rightful receiver of the message, but none else. However, this presumptive contradiction is resolved by looking closer into the pillars of today's society. Yet it is not so much the most obvious applications in the military or economical sector that benefit most from a secure communication as the individual citizen itself. The development towards an information society, where everything and everyone will be permanently connected and accessible, the demand for a secure communication is higher than ever. It is obvious that basic human rights and ethical values, such as the "inviolability of human dignity", can only be protected when personal information and communication can be kept private.

Cryptography or Quantum Cryptography in particular comes as an interdisciplinary field with plenty of contributions from physical, mathematical and information theoretical perspectives.

Although classic cryptographic concepts and ciphers go far back in the history of mankind, all ciphers generated by mathematical methods could so far be broken. From the well known Caesar cipher (80 B.C.), that shifts the letters of the alphabet, to the Vigenère cipher (1553), which uses a key word together with an alphabet, to more recent cryptography, such as the Enigma machine used by the Germans during the second World War, these, and numerous other examples, shared the same fate. While some basic

ideas of these ancient approaches can be extracted for modern cryptography, a lot of existing concepts had to be discarded when logical electric gates and modern electronics enabled algorithms to systematically search a cipher-text for its underlying mathematical concept and eventually break the cryptographic method. Crypto-analysis today is mostly based on frequency analysis of the cipher text. Due to the sheer speed of CPUs and FPGAs combined with a smart algorithm to search for patterns within the cipher, encryption, as it is used in most higher layer protocols today, such as IPSec, SSH or TLS, is nothing more than the hope for the attacker to have limited time and processing speed. The bottom line for classic cryptography is, that no unconditionally security can be guaranteed as long as encryption is based on mathematical problems that are hard to reverse.

Quantum cryptography however can be seen as an update to modern existing cryptography. The peculiar properties of quantum particles, such as the no cloning theorem, that forbids to create an unknown state twice, as well as the random behavior when measuring in a non-eigenstate, are able to succeed where classic cryptography is condemned to fail. The laws of quantum physics imply, that no attack on a quantum cryptographic method remains unnoticed, when the decisions of the sender and receiver are assumed to be freely eligible. A quantum key distribution (QKD) protocol is able to react directly to an attackers knowledge about the key and hence generate a cipher that is proved to be unconditional secure [1]. This means, in more lofty words, that as long as the decisions of humans (in this case sender and receiver) are assumed to be non-deterministic and depend on free will, QKD can be expected to be secure.

1.2 Outline of the Thesis

This dissertation should give insights into whether and how it is possible to integrate QKD into existing communication infrastructure, such as optical networks and free space satellite links. The next two chapters are building the theoretical framework for the experimental work. They will help to understand and interpret the data acquired from the experiments described in the consecutive chapters.

On the next page a short overview about the topics of the upcoming chapter is given.

[1] The definition of unconditional security will be discussed in chapter 2.2. It excludes for example the infinitesimal small probability to guess the plain text correctly. Also Denial of Service (DoS) and information leakage due to side-channels, such as unknown device impurities, are not considered

Chapter 2 - *"Information Theory And Classic Cryptography"*
The following chapter will give an introduction into commonly used concepts of cryptography as it is applied today. Basic axioms, authentication and finally the creation of a cipher using DES, AES, RSA, etc., will be explained. Special focus lies on the comparison of asymmetric and symmetric cryptography, and the classical concept of key exchange between two remote parties.

Chapter 3 - *"Quantum Key Distribution - And Its Various Forms"*
The third chapter presents a selection of different QKD concepts. It discusses the prepare and measure, the entanglement as well as the continuous variable (CV) scheme. Security proofs, attacks and countermeasures are discussed with respect to recent developments and works in the field.

Chapter 4 - *"Satellite Based QKD"*
The fourth chapter introduces a satellite-based QKD scheme to enable key exchange for secure long distance communication. The fundamental topic of this chapter is the source that distributes the quantum signal to the two communicating parties. A promising candidate is a $LiNbO_3$ waveguide source that uses spontaneous parametric down conversion (SPDC) to create entangled photon pairs. Two types of sources with different waveguides are investigated with respect to their brightness, visibility and pair rate to determine a possible candidate.

Chapter 5 - *"Passive Optical Networks"*
Chapter five gives additional information about passive optical networks in general. More precisely metropolitan backbone networks, i.e. networks for heavy traffic use in a wider deployed area, as well as access networks that connect the user to the latter kind are discussed with regard to a potential integration of QKD into such infrastructures.

Chapter 6 - *"QKD In Passive Optical Networks"*
In this chapter the demands and limits of a coexistence scheme, i.e. the usage of a quantum channel and classical data signals on a shared fiber, are discussed by simulations and experiments on a 20 channel dense wavelength division multiplexed (DWDM) ring network. Impairment evaluations for different fiber lengths are presented originating from different classical channel combinations in the C-Band up to 50THz. Based on this results, a spectral window for the quantum channel is selected and an entanglement based source for QKD is assembled with respect to this result. Further measurements with appropriate filtering are presented that evaluate the performance of the source for different network scenarios and wavelengths. Finally, a full duplex encryption is presented with quantum channel and post processing data sharing the same fiber.

Chapter 7 - *"Summary & Discussion"*
The final chapter will summarize and discuss the gained results. Based on this, perspectives and limitations are pointed out and possible experiments for further research are proposed and discussed.

Chapter 2

Information Theory And Classic Cryptography

2.1 Information Theory

The way on how information is passed varied and changed during the past years. While historically information is usually bequeathed in written, oral or drawn messages, things changed in the 19th and 20th century when first telegraph- and landlines were deployed. The channel through which information is passed can be of various forms. In 1948 Claude E. Shannon explained in his paper how information can be quantified and how the capacity of a channel can be calculated independently from the used medium and the meaning of the message for the receiver [20]. By introducing the *entropy function*

$$H(p_i) = -\sum_{i=1}^{n} p_i \cdot log_n(p_i), \tag{2.1}$$

that satisfies all required criteria of a measure, the maximum of H is determined as the unit of information. The p_i denotes the probability that a certain symbol, labeled i, is received from a channel. The symbol itself can be chosen from an arbitrary alphabet that comprises n elements. In the most common case, where $n = 2$, the alphabet comprises the elements "0" and "1" and the unit of information is called *bit*. Furthermore $H(p_i)$ is written as $h(p_i)$ and called *binary entropy function*.
This definition can be understood as a measure of uncertainty about the next symbol. A bit of information is hence transmitted when no a priori information about the next transmitted symbol can be gained from the previously sent symbol or any other source, i.e. the received symbol is completely random.
Another important definition derived from information theory is the *mutual information* $I(X : Y)$ of two discrete random variables X and Y. Using the conditional

entropy $H(X|Y) = -\sum_{i,j} p(i,j) \cdot log_n(p(i|j))$ (a logical extension of equation 1.1 together with the conditional probability $p(i|j)$) with i and j being from the sample space of X and Y, respectively, as well as the entropy of the joint events, $H(X,Y) = -\sum_{i,j} p(i,j) \cdot log_n(p(i,j))$ the mutual information can be written as

$$I(X:Y) = H(X) - H(X|Y) \tag{2.2}$$

$$= H(X) + H(Y) - H(X,Y). \tag{2.3}$$

This quantity can be understood as the uncertainty about a random Variable X, while the random variable Y is completely known. It yields zero when X and Y are uncorrelated and increases when the knowledge of Y gives information about the statistical behavior of X. This definition will be especially useful in chapter 3, when the security of the various QKD protocols are investigated in more detail. Since such a quantity is of great importance to determine the security of a cipher, either by estimating the knowledge of an attacker, when a fraction of the cypher is revealed, or by comparing the sent and received messages in the presence of errors due to a noise channel, it is a crucial part of several security proofs.
Furthermore the mutual information allows to characterize the channel that is used for transferring information. With respect to the mutual information the *channel capacity* C can be defined as

$$C = \frac{1}{\tau} \cdot \max\big(I(X:Y)\big). \tag{2.4}$$

The random variable X is hereby assigned to the symbols used at the input of the channel, while Y represents the random variable for the symbols at the output. The time τ donates the time in which the message was sent. The capacity of a channel can be understood as a maximal transmission rate of information, hence its unit is $[bits/s]$. For an ideal channel the random variables X and Y are exactly the same, however, the advantage of treating input and output differently lies in the potential to model noise within the channel. X and Y hereby differ by a probabilistic quantity that refers to the fact that in the presence of noise (or an attack) a symbol might have been changed or entirely dropped during the transmission. By compensating noise with a redundant transmission of symbols, i.e. error correction, it is possible to compensate these occurring errors. The channel capacity allows to determine a maximal possible throughput limit of a given channel also in the presence of noise. This is often referred to as the *Shannon limit*.

2.2 Cryptography

The term *cryptography*, as it is understood today, is the attempt to provide security for information, as defined in the previous chapter. As vague this statement is, as wide the field of cryptography ranges. In order to give an overview, the so called *information security objectives* are defined that can be understood as the building blocks of cryptography. The security of information is provided when all these objectives are met, which is, however, only a theoretical goal, impossible to reach in practice. The four main objectives of cryptography [1] are given by

- ***Confidentiality (Privacy)***: The information should only be accessible to those who are authorized to see it.
- ***Data Integrity***: Any unauthorized change of information should be impossible or traceable.
- ***Authentication***: The origin or source of an information or message should be unambiguously allocatable. Hereby the identity of the entity corresponding to the respective message or information should be assignable.
- ***Non-Repudiation***: A previous commitment or action should be impossible to deny or to erase.

However, providing these objectives is not always enough to guarantee a reasonable transmission of information. Given a situation where it is not only important to have a secure but a sufficiently fast channel to transmit all information in time, a transmission as secure as possible but as fast as necessary has to be chosen. Hence the evaluation of the respective cryptographic solution strongly depends on the respective situation. The following criteria, as stated for example in [1], attempt to compare properties of different cryptographic solutions.

1. Functionality & methods of operation

The methods on how the above objectives are provided are called *cryptographic primitives*. In order to achieve security the eligible primitive has to be determined with respect to its performance in the given circumstances. In addition to this a primitive behaves differently according to its inputs and use in a combination with other primitives. Hence the mode of operation has to be contemplated carefully. An incomplete collection of primitives is given in Figure 2.1.

2. Performance

[1] The list of information security objectives can be extended by other issues, such as access control, witnessing or time-stamping. However these are irrelevant for the upcoming chapters and beyond the scope of this thesis

Depending on the need of the user the respective primitive has to meet required criteria.

3. Implementation

A fast and modular implementation into existing infrastructure is desirable. This means that the primitives can be realized using common CPU, FPGA or ASICS hardware and the corresponding software tools.

4. Level of security

In order to determine the level of security and hence compare two methods, it is common to elaborate a lower bound on the work necessary to break the respective objective. This is usually called an (optimal) *attack*. An attack can be *passive*, where the adversary is monitoring the data sent through the channel, or *active*, when data is altered, deleted or added. While a passive attack is only able to target the confidentiality objective an active attack can compromise all four objectives. These attacks can further be divided, depending on the power of the adversary [2]. Based on such assumptions security models can be developed. According to Shannon [21] each of those models can be can be assigned to one of the following two classes.

Theoretical security

Theoretical security, sometimes also called information-theoretical or unconditional security, denotes the highest possible security. Although the eavesdropper is in this case granted with unlimited computational power and resources, no information can be gained from a cipher text and no other security objectives can be corrupted without being noticed, neither in the case of a passive attack nor an active attack. An example of unconditional security is given by the *One-Time-Pad* encryption, which will be discussed in chapter 2.3.1.

Practical Security

The practical or sometimes called computational security analyzes the potential vulnerability of a security model and compares it to the feasibility of an adversary with limited powers to exploit these known flaws. The most common approach is to consult the field of complexity theory. Hereby the respective cryptographic scheme is assigned to a certain *complexity class* with respect to the effort of breaking it. It is assumed that the attacker can break the scheme by applying an (optimal) algorithm, i.e. a well defined (computational) procedure that takes a variable as input and provides, after a certain number of steps (commonly bit operations), a respective output. According to the steps of operations a running time can be assigned to each algorithm. Since, however, the running time is connected to a respective step-speed, complexity classes are referred to certain intrinsic constraints that determine the running time of an algorithm [3]. The most important complexity classes in cryptography are **P** and **NP**. **P** denotes hereby

[2] Examples for attacking confidentiality are cipher-/plaintext only or chosen cipher-/plaintext attacks and variations of those.

[3] Typically the properties of the Turing machine are used as a reference.

all possible decision problems that an algorithm can solve in polynomial time, whereas **NP** refers to the set of decision problems for which a "Yes" answer can be verified by an algorithm in polynomial time [4]. A simple example for an NP problem is the test whether a number n comprises a certain factor a, i.e. $n = a \cdot b$. If n comprises a an algorithm can verify it in polynomial time. The security of a certain cryptographic scheme can hereby often linked to an optimal attack, that uses an algorithm of a certain complexity class. Practical security is sometimes subdivided into provable security, which means, that it can be shown that the security scheme requires the attacker to solve a supposedly difficult (usually number-theoretic) problem. Examples of provable security schemes are RSA or elliptic curve cryptography schemes that boil down to integer factorization and the solution of a discrete logarithm. Chapter 2.3.2.2 will discuss these concepts in more detail.

The cryptographic primitives that are used to ensure the four objectives are *Ciphers*, constructed with the help of a *key* to make the message unreadable for anyone without it, *Signatures* and *Message Authentication Codes (MAC)* or *Hash functions*, validating the authorship and integrity of a message as well as the correct identity of the entity. These primitives can either be realized using so called *symmetric-* or *asymmetric-* (or *public-*) key cryptography, as states in Figure 2.1. In the next chapters a short introduction into each scheme will be given.

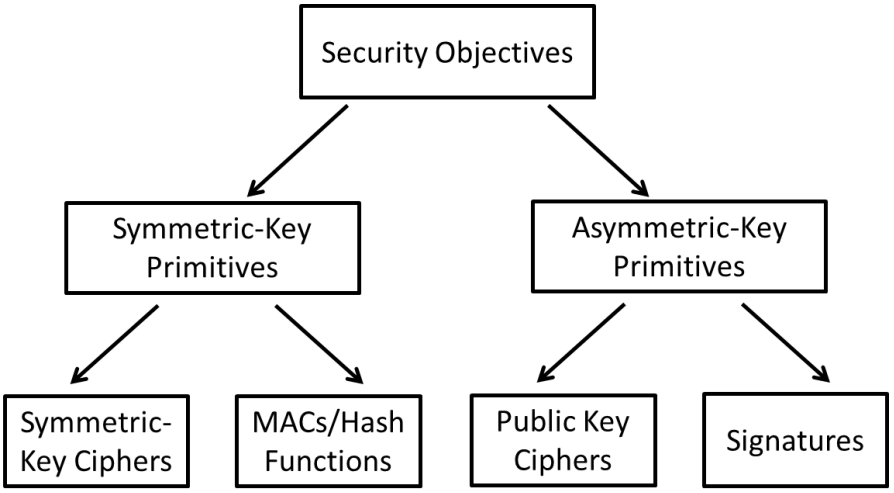

FIGURE 2.1: Overview of Cryptographic Primitives to meet the four security objectives

[4] This definition corresponds to the set of all decision problem that are solvable in polynomial time when the deterministic constraint is released, as for example given by a non-deterministic Turing machine

2.3 Public-Key vs. Private-Key Cryptography

2.3.1 Symmetric Cryptography

Symmetric cryptography schemes are the oldest and straightforward way to authenticate messages and its corresponding authors as well as create ciphers to keep communication private. The crucial point of this scheme is a random key k from a key space K, usually shared by two parties called Alice and Bob. This key can, on the one hand be used for authentication by employing signatures, MACs or hash functions, on the other hand it allows, together with an encryption and decryption function E and D, to turn a plain text message m from the message space M in to a cipher c from the cipher space C, by

$$E(m,k) = c \quad \text{and} \quad D(c,k) = m, \tag{2.5}$$

respectively. For all k $\in K$ and m $\in M$, $D(k, E(k,m)) = m$ holds. This scheme grants theoretical security, as defined previously, when the key is assumed to be known only to the legitimate parties and key and message space are independent. This means that for each k $\in K$ and m $\in M$ the information about the key must not increase when the eavesdropper learns the corresponding message to a given cipher, $H(k|m) = H(k)$, with H denoting the uncertainty as defined in the equation 2.1. This means further that $H(k) \geq H(m)$ and therefore that $|H| \geq |M|$.
An example of such a theoretical symmetric encryption is the Vernam cipher, first mentioned in 1926 by Gilbert Vernam, which is better known as the one-time-pad encryption. When using the two letter alphabet $\{0,1\}$ each symbol of the message m is hereby transferred into a symbol of the cipher c by applying the XOR operation on the message bit and a random key bit. The key needs to be as long as the message itself and can only be used once in order to fulfill the above criteria of a information secure encryption.
However, there is an intrinsic assumption to the one time pad when it comes to prove the theoretical security of this encryption: In order to get perfect security, a shared random key only known to Alice and Bob has to be present. The distribution of this key is the bottleneck of this scheme, since an authenticated and secure channel is needed. But when such a channel is available, why not use it to transmit the private message in the first place? Due to this fact the one-time-pad encryption was not considered to meet the performance and functionality constraints stated in the previous chapter and discarded as a classical concept. It turns out that exactly this key distribution problem can be solved by quantum mechanics. This fact is elaborated in detail in section 3.
In order to find classical methods that are feasible with current technology, the constraint of true randomness of the key was reduced to concepts that required a shorter

random key, a so called *random seed*, for generating a cipher as well as its corresponding authentication. Nowadays two processes are distinguished concerning this matter, namely *stream* and *block ciphers*. These are able to turn a random seed into a pseudo random string of arbitrary length. A short introduction and examples of those are given in the following.

2.3.1.1 Symmetric Key Ciphers

Stream cipher

The stream cipher intends to generate a pseudo random number (PRN) bit for each plain text bit and encrypt the whole message with this random string of bits, the key. The random seed itself, that is shared by Alice and Bob, can be gained from various sources, like radioactive material, noise variations from an acoustic source or dark counts from single photon detectors or similar. Depending on the input parameters, stream ciphers are said to be synchronous if the generated pseudo random key stream does not depend on the message or the cipher. For a given initial state σ_0, a next step function f, a key stream function g and an output function h, the synchronous stream cipher can be specified by

$$\sigma_{i+1} = f(\sigma_i, k), \quad z_i = g(\sigma_i, k), \quad c_i = h(z_i, m_i), \tag{2.6}$$

whereas σ_i is the i-th state of process, the z_i denotes i-th element of the key stream and c_i of cipher text stream, respectively. In order to generate the same key stream, Alice and Bob need to share the same initial state and key seed k and must furthermore to be synchronized to perform all steps equally. Therefore such types of stream ciphers are said to be *synchronous stream ciphers*.

Contrary to synchronous stream ciphers *self-synchronizing stream ciphers* can be constructed that depend not only on the key k, but on the cipher itself and hence on the message. The respective relations are given by

$$\sigma_{i+1} = f(c_{i-t}, c_{i-t+1}, ..., c_{i-1}), \quad z_i = g(\sigma_i, k), \quad c_i = h(z_i, m_i). \tag{2.7}$$

The process starts with an initial state $\sigma_0 = (c_{-t}, c_{-t+1}, ..., c_{-1})$. Both, synchronous and self-synchronizing streams have advantages with respect to error correction, attack strategies for an adversary and statistical distribution of cipher text bits. A more detailed discussion can be found in [1].

A popular choice of practical realization of such stream ciphers are *linear feedback shift*

registers (LFSR) due to their easy implementation in hardware and a good approximation to a real random string [5].

A LFSR comprises L stages $(0, ..., L-1)$ each capable of storing a bit, accepting one input or giving one output. During each time step, registered by an internal clock, the following operations are performed:

(i) The content of stage 0 is returned as part of the output sequence.

(ii) The content of state i is moved to stage $i-1$ for $1 \leq i \leq L-1$.

(iii) The new content of state L-1 is called the feedback bit s_j, received by adding the previous contents of a fixed subset of stages.

Figure 2.2 as found in [1] shows the graph of a LSFR with length L. The $\oplus$ denotes hereby the XOR addition.

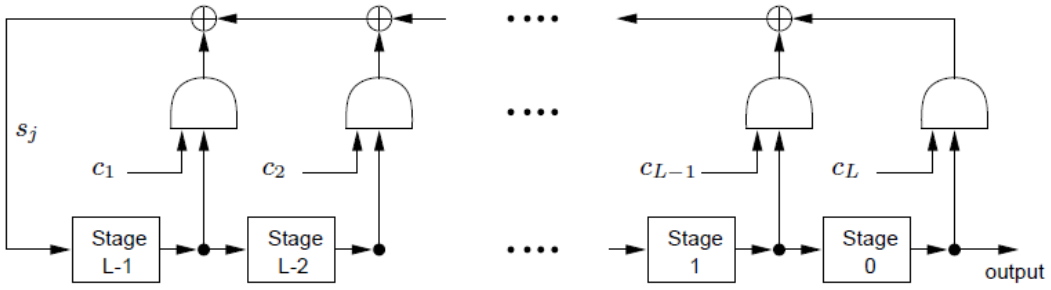

FIGURE 2.2: Schematics of a Linear Feedback Shift Register (LFSR) of Length L, taken from [1]

An example of stream ciphers using LSFR is the A5/1 key stream generator as it was used in GSM networks in Europe and USA for cellphones providing security for voice calls and text messages. Although the algorithm developed in 1987 was first kept secret [6] its functionality eventually leaked in 1994. As shown in Figure 2.3 it comprises three LSFR of lengths 19 (X-register), 21(Y-register) and 23 (Z-register). Each box of these three registers is filled according to an addition rule with a 64bit key seed such that the initial states of the registers are defined. When the majority of bits coincides with the 8-th box of the X register (10-th box of the Y- and Z-register) the bits are shifted (steped) one box to the left, filling the remaining first register with a respective XOR addition of entries as shown in Figure 2.3 below. key stream bit is extracted by XOR combination of the outer left entries of the three registers. Today the A5/1 as well as the weaker version A5/2 algorithm are considered insecure. An improved version, A5/3

[5] The quality of a PRN G(s), gained from a truly random seed s, is given by the *Advantage*, a measured defined by $Adv(A, G(s)) = |P(A(G(s))) = 1 - p(A(R) = 1)|$, with P being the usual probability measure. A denote hereby a statistical test that returns a number in the interval $[0, 1]$ where 1 is considered random, i.e. for a random sequence R, $A(R) = 1$.

[6] The approach to provide "security by obscurity" violates Kerckhoff's principles, a list of rules stated by Auguste Kerckhoff to standardize modern cryptography. He claimed that it is easier to establish a secret key than keeping the method of encryption private.

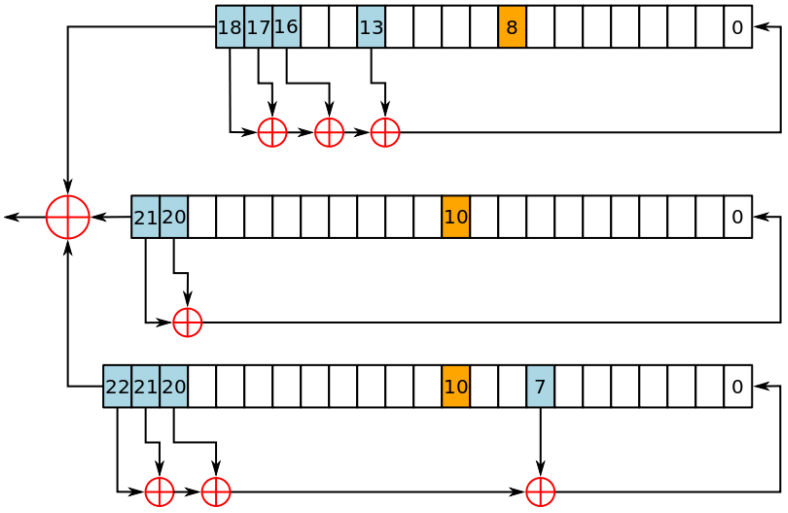

FIGURE 2.3: R5/1 stream cipher random number generator with three LSFR

also known as KASUMI, was deveoloped in 2000 and used in UMTS, GSM and GPRS. However apart from other, rather inefficient attacks, in 2010 a successful attack on this Block Cipher was presented [22].

Another prominent example is the RC4 stream cipher, originally used by software applications like Transport Layer Security (TLS) and Secure Socket Layer to establish secure communication or Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) to protect wireless networks. Although RC4 allows a random key seed of up to 256bits together with a 24 bit initialization vector (publicly known) to initialize the start of the LSFR, it can be shown that the key is extractable by a related key attack, where the algorithm is observed by an attacker with different initialization keys producing different ciphers that are connected through the process itself. Using simple algebra the key seed can be extracted as shown in [23]. At the time of writing symmetric cryptography in the form of stream ciphers is rarely used in state of the art cryptography, at least not as an exclusive way to provide secure communication.

Other methods such as Data Encryption Standard (DES), Triple DES or Advanced Encryption Standard (AES) are at the moment the most popular algorithms for PNG generation. They belong to the class of Block ciphers.

Block cipher

A block cipher stream is, in the most general case, defined as a function E that maps n-bit plain text blocks to n-bit cipher text blocks, i.e. $E : V_n \times K \to V_n$, with V_n being the set of all text blocks of length n. In order to get a unique decryption a bijective mapping has to be assumed, as defined in equation 2.5. Hence in contrast to the stream cipher this is not a bit-wise process. The functions E can usually be subdivided into rounds where the Block cipher employs either permutation (P-Box) or substitution (S-Box) operations, that permute blocks of the plain text message or respectively substitute

it according to a certain rule usually specified by the random key seed k. With respect to their mode of operation Block ciphers can be divided into four groups.

Electronic code book (ECB) mode

In the ECB mode the message is divided into parts $x_1, ..., x_t$ consisting of n bits each and combined with the encryption function E, comprising the key k, as shown on the left side of Figure 2.4. Since each plain text block x_i is uniquely assigned to a cipher text block c_i, the principle of a code book is imitated, hence the name. The decryption is done by inverting this process using the inverse function E^{-1}. A drawback of this scheme is that equal plain text blocks result in equal cipher blocks.

Cipher block chaining (CBC) mode

In this mode the encryption function E takes, in addition to the key and message block x_j, the output of the previously encoded message block x_{j-1}, the cipher block c_{j-1} as an input. Hence the disadvantage of the ECB mode is solved by iteration of the cipher text. This mode however requires an initialization vector (IV) before starting the first round as depicted in the right hand side of Figure 2.4. CBC has been used for example in an outdated version of the authentication protocol Kerberos.

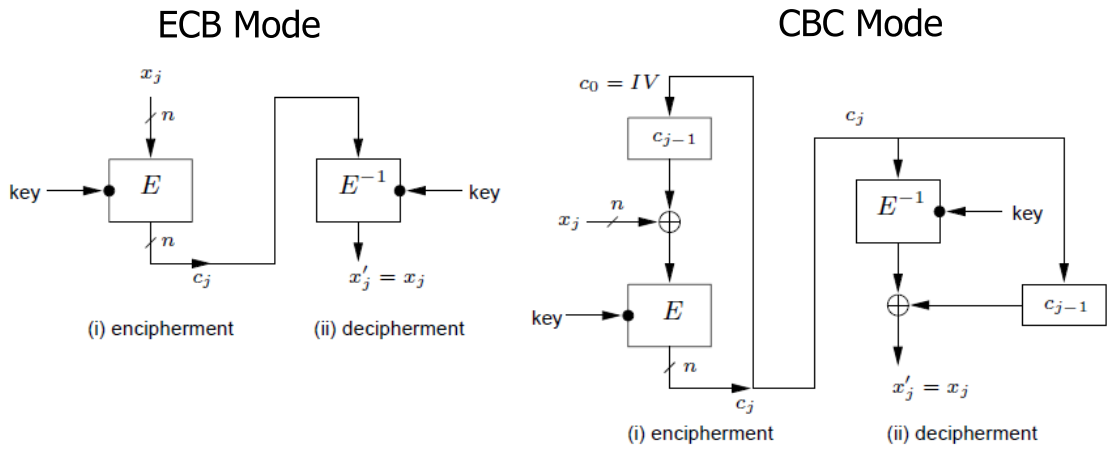

FIGURE 2.4: Left: Schematics of Electronic Code Book Block (ECB) cipher mode. Right: Cipher Block Chaining (CBC) Block cipher mode. Source [1]

Cipher feedback (CFB) & Output feedback (OFB) mode

CFB and OFB mode are both used to simulate a synchronous and self synchronizing stream ciphers, respectively, that allow to transmit part of the plain text message without any delay. In CFB mode the (i-1)-th cipher C_{i-1} is reused in addition to the plain text block P_i to generate the i-th cipher, i.e. $C_i = E_k(C_i) \oplus P_i$.

The OFB mode, on the other hand, produces an output O_i that is independent from plain and cipher text and feed-backed in the encryption function E_k by $O_i = E_k(O_{i-1})$. The cipher of the i-th block is then given by $C_i = P_i \oplus O_i$. The advantage of OFB lies

in the fact that any bit error of the cipher text is at the same position in plain text which allows an easy application of error correction codes. Both modes, CFB and OFB, evidently need an initialization vector for the first block.

As previously mentioned, the most used block ciphers are DES, T-DES and AES. DES, the oldest of the three was first introduced in 1976 by the American National Bureau of Standards (NBS), today called NIST. The DES Block cipher was based on the so called Lucifer Cipher invented in 1971 by IBM and used the so called Feistel cipher, named after his inventor Horst Feistel. The Feistel Cipher is divides into rounds that either apply P- or S-Box operation. It therefore splits the plain text into a left and right part, L_i and R_i, and applies on the left part a (not necessarily invertible) round function F with a dedicated round key k_i that is a part of the initial random seed k. For DES the round function F consists of bit expansion until a 48bit block is received, a mixing process (XOR) of this block with the k_i and finally a S-Box and P-Box operation. After this function F has been applied to the left part, the round ends by interchanging the right and left part of the split message, i.e. $L_{i+1} = R_i$ and $R_{i+1} = F(L_{i+1}, k_i)$. The entire process finishes after 16 of such rounds. Since in the early '90 the insecurity of DES with a 56bit key seed could be shown by several attacks, the key size was doubled and the procedure was repetitively applied up to three times, hereby named Triple-DES. Applications of Triple-DES are for example electronic payment systems as well as Microsoft Outlook or Microsoft One Note.
In 1997 NIST released an official call for a DES/T-DES successor. In 2000 AES (Advanced Encryption Standard) was released. AES offers operation modes with key lengths up to 256bit acting on block lengths of 128bits in 10-14 rounds, depending on the key lengths. It comprises a substitution layer, that uses a lookup table derived from the Galois Field $GF(2^8)$ with nonlinear properties, a permutation layer that shifts and interchanges parts of the message that is arranged as already mentioned in blocks of 128 bits, and a key addition layer, that adds a part of the random seed at each round. Although some attacks to this algorithm are known [24], they are computationally infeasible. However possible side channels attacks have been presented that use the significance of the caching time of the protocol or the compression tables to gain information about the key seed [25].

2.3.1.2 Message Authentication Codes and Hash Functions

The previous chapter established the basic techniques of symmetric cryptography by approximating the one-time-pad encryption with a stream cipher or creating a cipher by permutation and substitution of the plain text message, similar to a code-book.

Since these methods are only protecting the confidentiality (privacy) of a message and the adversary is assumed to be passive, active (man in the middle) attacks, such as masquerading or message modification, have to be treated in a different manner. For this purpose Message Authentication Codes (MACs) are introduced to generate a unique tag associated with the respective message. It has to be noted, that stream and block cipher schemes are still a crucial part of MACs, since sender as well as verifier need to share a random secret key k. In [1] a MAC algorithm is defined as a family of functions h_k that are parametrized by a secret key k and provide an *easy computable* and *computation resistant* value $h_k(x)$ of n bit length when an input x (the message) of arbitrary but finite bit length is given. Computation resistance means that once a message x, or a set of messages x_i, and their corresponding MAC values $h_k(x_i)$ are known, it is infeasible to compute the hash value $h_k(y)$ for any other message y. When Alice sends in addition to her message the corresponding MAC value $h_k(x)$, Bob can calculate the MAC itself and approve it if he knows which key, k, has been used. The bottleneck of message authentication is the set of hash functions h_k.

Hash functions

Hash functions are divided into keyed and un-keyed versions. While un-keyed versions are mainly used for Modification Detection Codes (MDCs), that allow to ensure data integrity, the purpose of keyed versions is message and user authentication (MACs). Furthermore due to the properties of a cryptographic hash function two types are distinguished. *One Way Hash Functions* (OWHF), that are hard to invert when a result is given and *Collision Resistant Hash Functions* (CRHF), that show a low probability that two inputs are mapped on the same output. Since constructions of CRHF functions are not as straight forward, it is referred to [1]. However a simple example of an OWHF can be given by $f(x) = x^2 - 1 \bmod n$ with n being the product of two primes p and q with unknown factorization, $n = p \cdot q$. Another easy construction of an OWHF is received when a Block cipher algorithm $E_k(x)$ is given, as defined in the previous chapter. Setting $h(x) = E_k(x) \oplus x$ derives a OWHF. When regarding the function $h(x)$ as a function of the key k, $h(x, k)$, a keyed hashed function is given.

In order to give an unique authentication a secret (key) that is only known to the respective party has to be considered [7]. Hence the latter construction $h(x, k)$ can be used for calculating a MAC value. The first approach for MAC algorithms was in fact taken directly from the Cipher Block Chaining (CBC) method which creates a randomized cipher text employing a secret key and an initialization vector. When the length of such a Block cipher is reduced it fulfills the eligible properties of a hash value.

Another approach to generate keyed hashed function and hence generate a MAC is the

[7] Authentication can be assumed as the exchange of information that is only known to the dialog partners or uniquely connected to the respective person. Characteristics in voice and speech of can for example serve to authenticate two people on the phone.

use of a cryptographic hash function together with a secret key. The cryptographic hash function needs to be easily calculable, efficiently compressible and combine the properties of a OWHF and CRHF.
The so called *Merkle-Damgård construction* is hereby a useful theorem to construct a keyed hash function with these desired properties. It states that if a suitable padding scheme is used the hash function is collision resistant when the underlying compression function c is collision resistant. Since in this construction the hash function's input size is fixed, it might be that the message has to be extended by a certain amount of bits. This process, called padding, has, according to this theorem, to be chosen in such a way that the lengths of the message is considered within the padding. Afterwards the message is divided into equal parts x_i. Starting with x_1 and an initialization key k an output $c(x_1, k) = c_1$ is created that is iteratively fed into the compression function $c(x_2, c_1) = c_2$. This process is repeated until the entire message is processed and the final hash value is received. Sometimes a finalization function is applied to adjust the output size or that are increase its the randomness of the bits. Applications like Message Digest 5 (MD5) or SHA1 and SHA2 (Secure Hash Algorithm) make use of this construction.

2.3.2 Asymmetric Cryptography

Asymmetric or often called *Public Cryptography* evolved due to the need of an easy key exchange between two remote parties. Since symmetric encryption assumes that at least a common secret key seed is held be Alice and Bob, this premise is connected with intrinsic logistic problems and in some cases just not grantable. Asymmetric cryptography does not discard the concepts of symmetric cryptography but uses other, rather mathematical techniques to generate a secret key between Alice and Bob. Once the key is created, the concepts are similar when it comes to encryption and authentication. An advantage that is offered by asymmetric cryptography is the ability to connect a message with an individual signature that allows to comply with the non repudiation security objective, defined at the beginning of this section 2.2. In the following the most common methods of asymmetric cryptography are introduced.

2.3.2.1 Authentication and Signatures

The basic concept of asymmetric cryptography is to give Alice and Bob a key pair comprising a *public key* and a *private key*. As the names imply the public key is known to everyone, whereas the private key is only known to the respective person. Hence in the case of Alice and Bob four keys are part of the game, Alice's private and public key, $k_{A,pr.}$ and $k_{A,pu.}$ and the respective keys on Bob's side, $k_{B,pr.}$ and $k_{B,pu.}$. Since

$k_{A,pu.}$ and $k_{B,pu.}$ can be freely accessed, everyone can create ciphers using public keys and an encryption function E, e.g. $c = E(k_{A,pu.}, m)$. However, due to the construction of the key pairs, only the holder of the private key is able to decrypt these messages, e.g. $m = D(k_{A,pr.}, c)$. This offers an easy encryption scheme, though does obviously not guarantee authentication.

Signature

When the keys are used in different order, a digital signature can be created, that not only authenticates the origin of the message but offers non repudiation in addition. Once a message is signed with the private key, the origin and transmission of the message is proved. If, for instance, Alice wanted to sign the message (or the cipher) she sends to Bob, she would not only transmit the message but creates a tag comprising her private key and the respective message, $E(k_{A,pr.}, m)$ [8]. Bob (or in principle anyone else) on the other side can verify the that the message was truly send from Alice by confirming that $D(k_{A,pu}, E(k_{A,pr.}, m))$ corresponds to the message m. In order to make this authentication scheme reliable it requires an entity that ensures that the available public keys are unique and correspond to the respective holder.

Authentication

In order to proof the authenticity of a party a so called challenge is sent. If, for example, Bob wanted to ensure Alice identity he sends her an arbitrary message $m_{Challenge}$, encrypted with her public key $E(k_{A,pu.}, m_{Challenge})$. Since only Alice posses her private key, she can decrypt it, $D(k_{A,pr.}, m_{Challenge})$, and send $m_{Challenge}$ back as a confirmation of her identity [9]. The problem that arises due to the free access of the public key is that with each authentication the cipher text of the challenge message is publicly known. Which eventually compromises the secrecy of the private keys. A way to minimize this risk is that once the authentication is established a different key is used for encryption and data integrity. In the next chapter the most common methods of asymmetric cryptography are presented. They show ways to create such a public/private key pair as well as exchange or renew keys.

2.3.2.2 Asymmetric Key Ciphers

Once an authenticated channel is provided, asymmetric cryptography uses the two private and public key pairs of Alice and Bob to provide them with a computational secure

[8] Usually neither the message nor the cipher is signed directly but a hash of one of the two is used to create a signature.

[9] In order to avoid an attack, where an adversary somehow found $m_{Challenge}$ and hence pretends to be Alice by sending it back to Bob, the challenge message is usually never sent as plain text. Hence Alice does not respond with $m_{Challenge}$, but with $E(k_{A,pr.}, m_{Challenge})$. In this manner the private key has to be used twice.

shared key. Alice and Bob make hereby use of mathematical problems that are generally known to have no explicit solution. An attacker in this case has to work out an presumable infeasible effort to extract the created key. The most used algorithms for creating asymmetric ciphers are the Diffie-Hellman key exchange, worked out in 1976 by Whitefield Diffie and Martin Hellman [26] as well as RSA, named after Ron Rivest, Adi Shamir, and Leonard Adleman, published in 1978 [27]. While the first relies on the problem of inverting the discrete logarithm the latter uses the approach that the factorization of large numbers together with inversion of the equation $c = m^e \pmod{n}$ is practically unsolvable.

Diffie-Hellman Key Exchange

In order to gain a secret shared key the cyclic group that comprises all elements that are *relative prime* (also called *co-prime*) to a given prime number p, $\mathbb{Z}_p^*$, is considered. Any value $A \in \mathbb{Z}_p^*$ is now connected to a certain value a when a generator g is defined as the base of the discrete logarithm, $A = g^a \bmod p$. Given for example the group $\mathbb{Z}_3^*$ with $g = 2$, the discrete logarithm of 2 would be 3, as $2^3 = 2 \bmod 3$.

When Alice and Bob have agreed on a common cyclic group, i.e. the respective prime number p, as well as a generator g (both publicly known), they both choose a random secret number (a and b) and calculate the corresponding discrete logarithms, $A = g^a \bmod p$ and $B = g^b \bmod p$. When the values A and B are exchanged a common key is given by $K = A^b \bmod p$ and $K = B^a \bmod p$, since the values of the discrete logarithm are commutative. However, without the knowledge of both exponents the recovery of K from with the publicly known values g, p, A and B is mathematically hard.

This algorithm is obviously vulnerable to man-in-the-middle attacks, as no authentication is assumed. A possible way to solve this problem is to include asymmetric cryptography and make use of authenticated public keys. Alice for instance can hereby choose to use Bob's authenticated public key $k_{B,pu}$ as $B = g^b \bmod p$. Together with her counterpart $A = g^a \bmod p$ consisting of her randomly chosen number a she is able to prepare a key only familiar to Bob, since only he holds the corresponding private key.

Another approach is to encrypt the process with a long term key that is unknown to the adversary. However, this reduces the Diffie-Hellman Key Exchange to a forward security scheme that assumes that the first key exchange was at least as computational secure as the discrete logarithm problem itself. Security can hereby be preserved (forward security) to use this key exchange to establishing temporary session keys.

RSA

The RSA encryption algorithm is at the time of writing the most used way to encrypt and decrypt messages via an insecure channel. It is used by several security protocols on the transport or application layer. The algorithm itself starts with the creation of a public/private key pair. Note that this is done independently form Alice and Bob. The

particular steps are stated in the following

- Two large (e.g. 256 bit) distinct prime numbers p and q are secretly chosen.
- The product $n = p \cdot q$ is calculated and all coprime numbers of n are determined using Euler's totient function $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+p-1)$. While $\varphi(n)$ must be kept private, n is publicly known.
- A single co-prime number $e \in \mathbb{Z}^*_{\varphi(n)}$, i.e. $1 < e < \varphi(n)$ is chosen. The number e is publicly announced and denotes the public key.
- The equation $e \cdot d = 1 \mod \varphi(n)$ is solved for d. This is the multiplicative inverse of $e \cdot \mod \varphi(n)$ and denotes the private key, that evidently kept secret.

Based on the numbers n and e (public key) a trapdoor function E can be constructed by $y = E(x, e) = x^e \mod n$ whose inversion $E^{-1} = D$ can only be calculated when d (secret key) is known, i.e. $D(y, d) = y^d \mod n = x^{e \cdot d} \mod n$ [10]. When using E as well as the public key e and n for creating a cipher text c out of a given message m, i.e. $c = E(m, e) = m^e \mod n$, the corresponding plain text can be reconstructed by the private key d as $m = D(c, d) = m^{e \cdot d} \mod n$. The drawback of this construction is the collision resistance of the encryption function E, since everyone can use the public key a message m' can be found such that $c = c'$. Similar to the authentication in chapter 2.3.1.2. a hash value together with an appropriate padding to process the messages in equally sized block lengths can solve this problem. Hereby a random number x is generated and encrypted with the public key, $y = x^e \mod n$. A Hash function k corresponding to x is calculated, i.e. $k = H(x)$, and used to encrypt the message m, $c = E(k, m)$. By transmitting c and y sufficient information is given to decrypt the cipher using the private key d. First the random value x is determined by $x = y^d \mod n$, then the corresponding hash value, $H(x) = k$, and finally the message $m = D(k, m)$.
Similarly RSA can be used for creation of a digital signature. When calculating the hash value of a message $h = H(m)$ it can be uniquely bound to the private key by the tag $h' = d^d \mod n$.

Elliptic Curve Cryptography (ECC)

In recent years the development of faster computers and algorithms partially compromised the security of RSA and Diffie-Hellman key exchange. As a response to this the key size was increased to restore a sufficient level of computational security. Considering Moore's law this is only a temporary solution. Therefore another scheme, called Elliptic Curve Cryptography (ECC), became popular in more and more application, such as

[10] The proof that D is the inverse of E can easily be shown by using Euler's theorem, $x^{\varphi(n)} = 1 \mod n$. Since $x^{e \cdot d} \mod n = x^{k \cdot \varphi(n)+1} \mod n = x^{k \cdot \varphi(n)} \cdot x \mod n = (x^{\varphi(n)})^k \cdot x \mod n = 1^k \cdot x \mod n = x$, the inversion is shown. The original paper uses an equivalent proof based on Fermat's little theorem.

passports, electronic cash cards, internet protocols, such as TLS, SSH or DNSSEC, or operation systems and game consoles, at least as an additional security to RSA. The security of ECC is mainly based on the fact that instead of the set of numbers relative prime to n, $\mathbb{Z}_n^*$, the discrete logarithm problem is taken to elements of a field [11] defined by an elliptic curve. This curve itself is hereby given in a two dimensional equation

$$y^2 = x^3 + ax + b, \tag{2.8}$$

with x and y being elements of this field. In order to avoid singularities the coefficients a and b must fulfill $4a^3 + 27b^2 \neq 0$. A possible shape of an elliptic curve as well as the graphical addition operation between two elements of field over an elliptic curve, P and Q, is shown in Figure 2.5. The point P and Q are connected and the third intersection is mirrored at the x axis to get the result $R = P + Q$. If no intersection can be found the "∞" element is the obtained result

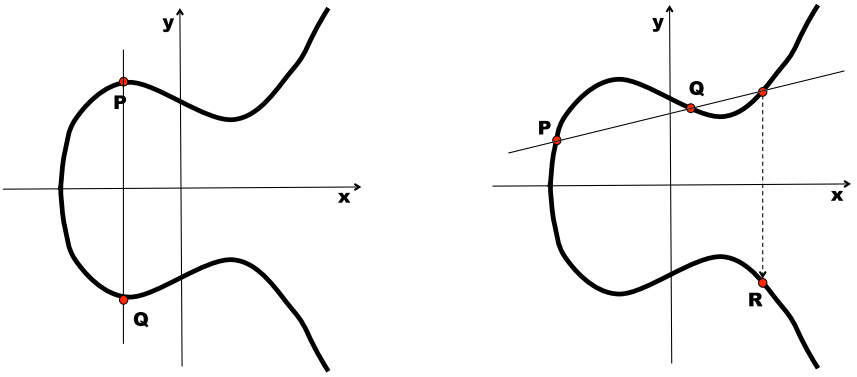

FIGURE 2.5: Graphical representation of the addition operation, $P + Q = R$, over the field of an elliptic curve. The left picture shows the case when no intersection point of the elliptic curve is given by the line spanned from two points P and Q. In this case the result is defined as infinity, ∞. On the right side the case of a third intersection point R is shown.

A point P(x,y) is element of the finite field over an elliptic curve when equation $y^2 = x^3 + ax + b \bmod n$ holds for x and y. The practical fields that are used for cryptography are the set $\mathbb{F}_p$ that denotes the set $\{0, 1, \cdots, p-1\}$ and its corresponding operations mod p, with a large prime number p. These fields over an elliptic curve are called *prime curves*. Since for hardware application binary fields are faster and easier to implement, $\mathbb{F}_{2^m}$, with $m \in \mathbb{N}$ is another important type. They are called *binary curves*. Each so defined set hence comprises the points of the given field that fulfill the elliptic curve equation and for completeness, the "∞" element.

Elliptic curve cryptography can be used for encryption, i.e. key distribution, and signatures (elliptic curve digital signature algorithm, ECDSA). The key distribution scheme

[11] A field is given when each element of a ring (a group with two operations) has a multiplicative inverse.

is similar to the Diffie-Hellman key exchange and therefore called *elliptic curve Diffie-Hellman* (ECDH). A field over an elliptic curve is hereby defined, i.e. a prime curve, $E(\mathbb{F}_p)$ with the parameters a and b that determines Equation 2.8. The values a,b and p are publicly known. A simple example, taken from [28], shows how this scheme is applied. We assume here the parameters $a = 11$, $b = 19$ and $p = 167$, and a point $P(2, 7)$ that solves the corresponding equation $y^2 = x^3 + 11x + 19 \bmod 167$ The algorithm for ECDH goes as follows.

- Alice chooses a random multiplier $n_A = 15$ and applies it to P, $Q_A = n_A \cdot P = (102, 88)$. The new point Q_A is send to Bob
- Bob does the same thing, e.g. $n_B = 22$, and finds a point $Q_B = n_B \cdot P = (9, 43)$. Q_B is given to Alice
- Each of them multiply the received point with their respective multiplier n_A and n_B and both share the same key $Q_{AB} = (131, 140)$.

The security of this scheme lies in the fact, that solving for an unknown multiplier k that connects two given points of the field $E(\mathbb{F}_p)$, i.e. P and $Q \in E(\mathbb{F}_p)$, is a hard mathematical problem, $Q = k \cdot P$. Since this problem is considered harder than the discrete logarithm or the factorization problem, the key lengths in the ECC scheme can be significantly reduced [12].

The presented methods of symmetric key cryptography are able to fulfill the first three security objectives, defined at the beginning of chapter 2.2. Confidentiality is guaranteed by creating a pseudo random key using stream or block ciphers, that imitate the OTP encryption. Data integrity as well as message authentication is achieved using MACs that are calculated with CBC of block ciphers or keyed and un-keyed cryptographic hash functions, respectively. The crucial point is that a pre-shared secret key needs to be assumed for secure symmetric communication. The fourth point, non repudiation, however, needs digital signatures to uniquely bind a given message to a sender and confirm its transmission. Unfortunately symmetric cryptography is not able to fulfill this security objective. Asymmetric cryptography, though, can provide this by the use of digital signatures. In addition to this it offers a more convenient and easier way to implement key exchange and management without the logistic effort needed in asymmetric cryptography. However, this comes with the price of a lower security and slower processing times. A possible compromise is hybrid cryptography that combines the two approaches. Since although symmetric cryptography is not mathematical secure, as the one-time-pad is only simulated with a pseudo-random key, its security, given the state

[12] The security levels of a 160 (224, 256, 384, 512) bit key in ECCis is supposed to provide the same security as a 1024 (2048, 3072, 7680, 15360) bit key used in RSA or Diffie-Hellman key exchange

of the art concepts, is still considered higher than offered by asymmetric cryptography. However, when taking into account possible design flaws, that allow to exploit back-doors and side-channels to reduce the size of the key space or allow an faster search algorithm for the key, it immediately recalls that both techniques suffer from an inherent weakness. Although a mathematical problem has not been generally solved, an individual case as used when a cipher is created may not grant the desired security. New algorithms are waiting when the quantum computer will reach maturity, making the factorization problem, as used in RSA, solvable in polynomial time by applying Shor's algorithm. The future of classic cryptography as it was used over the past years is uncertain. New ways, such as lattice based cryptography or hash based signatures, are possible candidates to replace existing schemes. The intrinsic mathematical weakness still remains within these these concepts.

Another approach, first developed in the early '80s, is to replace mathematics with quantum physics, and use its peculiar properties. A simple algorithm is able to generate a shared key between two parties, when an authenticated classical channel is assumed. This allows to solve key distribution problem of symmetric cryptography can in principle grant a mathematical secure encryption, when equal key and message size are assumed. The basic idea of quantum key distribution as well as the different approaches and the underlying security aspects with respect to certain attack strategies are discusses in the next section.

Chapter 3

Quantum Key Distribution - And Its Various Forms

3.1 The Big Bang of QKD - The BB84 Protocol

The field of Quantum Cryptography started with an an idea by two men, Charles H. Benett and Giles Brassard in 1984, and is therefore better known as the BB84 protocol [29]. Although most readers are probably familiar with this scheme, this beautiful and simple idea will shortly be presented to serve as an introduction for other types of protocols.

The aim of the protocol is to grow a common identical key between two remote parties, Alice and Bob, that is only known to them and none else. This final key can in theory be made arbitrary large to serve as a one time pad for encryption.

The protocol starts with the sender, Alice, who has access to two channels. An untrusted, but authenticated classical channel and a quantum channel, each connected to Bob. An eavesdropper, Eve, is granted the power to attack, i.e. listen, measure and alter (also combinations of those) the signals sent on both channels, but she cannot manipulate Alice's and Bobs decision, which signal she transmits or which measurement he performs, respectively.

1. Alice is given the choice of randomly picking a photon in either a horizontal ($0°$) - $|H\rangle$, vertical ($90°$) - $|V\rangle$, diagonal ($+45°$) - $|+\rangle$ or anti-diagonal ($-45°$) - $|-\rangle$ polarization [1]. The first two and the latter two are each orthogonal and hence form a basis in the H/V-system and $+/-$-system. Alice and Bob agree on a way to code the polarization into bits, w.l.o.g. the states $|H\rangle$ and $|+\rangle$ correspond to 0, the others to 1.

[1] The original protocol uses polarized photons. Any other observable of a quantum system can be chosen just as well.

2. The photon is sent via the Quantum channel. Eve can perform an intersect-resend attack (I&R) on which she measures the photon and sends another photon with the measured polarization to Bob. However on average half of the photons have a changed polarization, since the outcome of an $|H\rangle$- or $|V\rangle$-polarized photon is completely random when measured in the $+/-$-basis and vice versa.

3. Bob performs his measurement on the received photon. His outcome depends, exactly as in Eve's case, on the choice of his measurement basis. On average 50% of the time his measurement outcome will coincide with the state that Alice prepared or, if there has been an attack, with the state Eve sent to him.

These three steps are repeated until a sufficient amount of data is collected by Alice and Bob. This ends the measurement stage, and the post-processing stage begins. In these steps the received measurement results will be turned into a secure identical key for Alice and Bob.

1. First, the classical channel is used to compare the measurement bases that Alice and Bob have been used for each photon. When the basis does not coincide, each of them discards the result of this measurement otherwise it is kept. This process is usually called *sifting*. However, since this information is also accessible to Eve, who can extract from this knowledge in which cases she has sent the right states to Bob, she knows on average each fourth measurement result Alice and Bob share [2].

2. Alice and Bob sacrifice a part of the key to determine how much errors occured during the measurement stage. This step is usually called *error estimation*. Since it is similar to the bit error rate, BER, in classical theory, the result in this case is commonly called *QBER*, Qubit error rate. In this stage it can be determined, whether an eavesdropper was present during the measurement stage [3]. For instance, an intercept-resend attack will cause an average error of 25% on each of the measurement in which Alice and Bob performed her measurement in the same basis [4]. If there were no errors and the measurement results correlated perfectly, the key could be used as a secure one-time-pad. Otherwise the protocol was not successful and secure communication is not possible.

Figure 3.1 summarizes the process of the quantum stage, from Alice's preparation to Bob's measurement, as well as the sifting process that leads to the raw key extraction.

[2] This knowledge comes from the fact that on average 25% of Eve's attacks are successful: Her chance of choosing the right basis is 50% and the same holds for Bobs choice

[3] The errors due to device imperfection have to be taken into account as well.

[4] This value is due to the 50% chance of Bob to receive the same results as Alice, even if Eve prepared it in the wrong basis

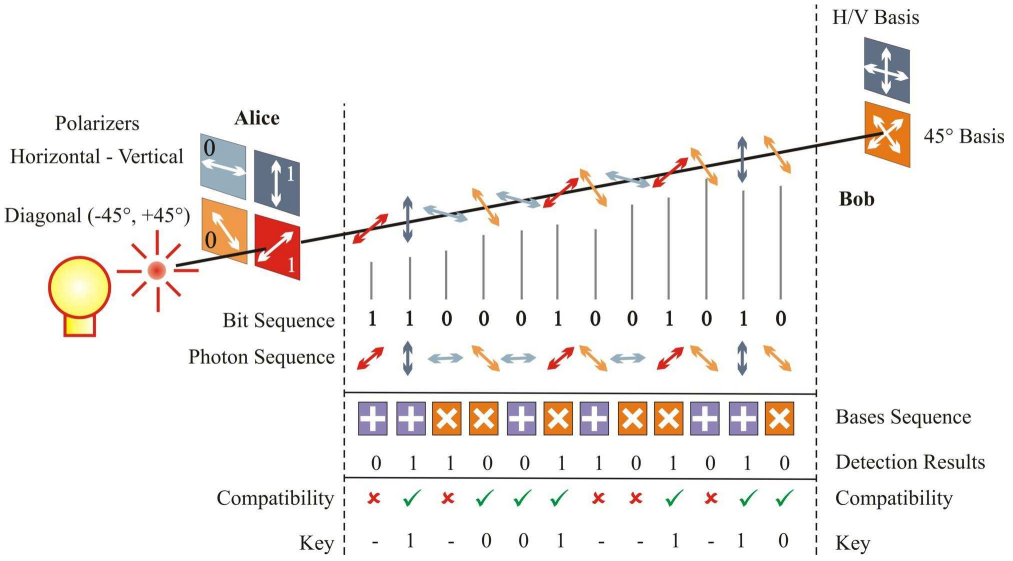

FIGURE 3.1: Schematics of the BB84 Protocol.
Source: [2]

The security of this protocol lies in the fact that it is not possible for Eve to prepare the same state that Alice sent to her, because of the no cloning theorem, that forbids to copy an unknown quantum state. Since her measurement relays on pure chance she will introduce errors that can be noticed by Alice and Bob.
From a theoretical point of view intersect-resend-attacks and variations of it [5] are the only attack strategies that have to be considered by Alice and Bob. Other approaches that Eve can perform to extract information about the key are based on device imperfections and stated in more detail in 3.2.1.4. A relatively new strategy to deal with this fact is called device independent QKD, which tries to shift the reliability of the devices to a concept in which the received qubits are tested before they are measured. In a sense the error estimation is here done before the actual measurement.

3.2 Categorizing QKD Protocols

In the subsequent years various protocols evolved that offered either new ideas to previous work or proposed a new way of distributing or creating quantum states. Since so far no rigorous advantage of one protocol over others has been emerged, the special case of each application has to be considered. Mutually dependent properties of a QKD protocol, such as key rate and security (in terms of errors that occur during the transmission) or distance and device properties have to be contemplated carefully, especially when it comes to experimental or even commercial use. Today's QKD schemes are usually

[5] E.g. Collective attacks as stated in can be considered as a variation of an I&R attack, in which Eve uses entanglement on ancilla states. In chapter 3.2.1.4 attack strategies for the simple I&R approach are discussed in more detail.

either distinguished with respect to their source that emits the quantum states or with respect to the measurement process after the quantum channel. The latter approach divides QKD schemes in *discrete variable QKD* protocols, where the eigenvalues of the observables have discrete values, and *continuous variable QKD* protocols, in which the measurement outcome is received from a continuous set of eigenvalues. When considering the different sources of quantum states, discrete variable QKD can further be subdivided into Prepare & Measure (using the uncertainty principle) and entanglement based protocols. Recent work that reveals the vulnerability of sources, detectors or the quantum channel to possible attacks, e.g. [30], [31] or [32] such that total or partial information about the key can be extracted, opened the new field of *quantum hacking* evolved. As a reaction to this threat counter measures were proposed that should prevent the hardware from tampering or close the leakage of information through side channels. However knowing that this can not be the ultimate solution, since more and more device impurities were uncovered by the quantum hacking community, *device independent QKD* schemes were proposed that detach the security of a protocol from its hardware by constantly assuring the integrity of the sent quantum states.
Before going into a more detailed overview about the different QKD schemes in the subsequent chapters a general overview about the generation of the key is given. Regardless of the type of protocol the following steps are necessary constraints for each QKD system.

1. *Quantum Stage*
   In this step the quantum channel between Alice and Bob is used to perform measurements. The source of the quantum based transmission as well as the form of the channel can differ according to the respective protocol.

2. *Sifting*
   In this stage the measurements are compared using the classical data channel. After this step, a *raw key* is shared by Alice and Bob, that contains errors due to technical imperfection and/or eavesdropping.

3. *Error Estimation*
   Part of the raw key is taken to compare the correlation of the bits. At this step the information leakage to Eve (QBER) has to be calculated, whereas imperfection from technical devices or channel errors have to be treated as a possible attack and counted in Eve's favor. If the error does not exceed a certain threshold the rest of the key can be used for further processing.

4. *Error Correction / Information Reconciliation*
   Since the remaining raw key still contains errors, Alice and Bob use classical communication to generate a perfect matching key. Two techniques of error correction

are defined depending on whether the sender of the quantum states performs this procedure or the receiver. The first case is referred to *direct reconciliation* the latter *reverse reconciliation.*

5. *Privacy Amplification*
   In this final step the secure key is gained from the corrected raw key by applying certain hash functions, that shorten the key but reduce Eve's possible remaining knowledge about it to an arbitrary small percentage. Depending on the error estimation, the rounds of hash functions are chosen until the desired mathematical security is given.

3.2.1 Discrete Variable QKD

3.2.1.1 Measuring discrete Variables

All protocols that are targeting an experimental realization using discrete observables to encode a classical bit, propose single photon counters as measurement devices. The most widely distributed devices to detect single photons are avalanche photo diodes (APD), avalanche single photon detectors (SPAD) or photomultiplier tubes (PMT), all based on the concept of the photoelectric effect, where electrons are released from the valance band by a photon with appropriate energy or wavelength. PMTs utilize cascaded evacuated electrodes that, when the first one is initially triggered by an incoming photon, increase the number of electrons after each electrode until a measurable current is received. APD and SPAD, use layered p and n doped materials to create a n-p junction when a photon hits the sensitive region of the semiconductor. The difference between APD and SPAD is found in the circuit and the operation point of the semiconductor and hence in the sensitivity of the device. While an APD is operated just below the breakdown voltage of the semiconductor the resulting photo current rises linear with the absorbed photons while for the SPAD, which is operated just above the breakdown voltage (commonly called Geiger-mode) the received avalanche grows exponentially from a single photon and is in the range of a few mA. In order to quickly restore the voltage of an APD or SPAD back to the operating level, once an avalanche has been triggered, a high resistance is needed to lower the voltage in the circuit. The time duration of this process, usually called quenching, determines the dead time of the detector. During this time the detector is blind to any other incoming photons. However, if the voltage is restored too fast, trapped electrons within the semiconductor, originating from the previous event, may cause another avalanche resulting in a false count. This effect, known as after-pulsing, can be mitigated by waiting until all electrons are discharged, i.e. applying an appropriate dead time. Three different types of circuits are typically

used in most QKD systems for single photon detection [33–35]:

Passive Quenching

The resistor is connected in series with the APD circuit, causing an immediate decrease of the voltage once an avalanche has been triggered.

Active Quenching

As soon as the rising edge of the photo current is detected the semiconductor is lowered below the breakdown voltage. Active Quenching demands for a more complicated circuit but results in a lower dead time and hence in a higher count rate.

Gated mode

In the gated mode operation the detector is only sensitive to incoming photons within certain time intervals (in the range of ns). This application is especially useful when source and photon arrival times are determined. In this case the detector opens only when a photon is expected.

Since APD and SPAD demand a suitable semiconductor, the materials have to be optimized for the respective wavelengths. While Indium Gallium Arsenide (InGaAS) detectors show the best results for photons in the telecom spectrum, around $1550nm$, with a quantum efficiency around 20%, Silicon (Si) detectors for lower wavelengths, around $400nm$, provide up to 4 times more efficient detection. When considering the relevant properties for QKD systems with respect to a measurement device, a low dark dark count rate, d [counts/s], a high quantum efficency, μ[%], a high duty cycle or low dead time, d_0, as well as a low after-pulsing probability, η [%], and timing jitter is desired. The concept of PMT can hereby not compete with state of the art APDs or SPADs in terms of duty cycle, which is one of the major factors for a high key rate.

Another issue is the tradeoff between feasibility and performance of a device. Although dark counts and quantum efficiency can be optimized by operating in cryogenic temperatures, the maintenance and commercial aspect of QKD has to be considered [6]. Therefore most detectors use a rather simple Peltier cooling circuit and accept the slightly worse specifications with regard to convenience. Similar to the photon detection the source of a QKD system has to be contemplated accordingly. The following chapters introduce the most common discrete variable protocols and its respective sources.

3.2.1.2 Prepare & Measure (P&M) QKD

Since the presented BB84-protocol is the prototype of a prepare and measure protocol, it is the oldest known version of QKD. It is a very popular scheme especially by commercial companies or telecommunication vendors due to its simplicity and flexibility concerning

[6] For experimental purposes superconducting nanowire single photon detectors (SNSPD) are a very promising approach that however demand temperature lower than 10K [36]. The principle of operation is a superconducting wire that, when hit by a single photon, gets a positive resistance which results in an measurable voltage. An overview about this topic is given for example in [37]

the preparation of polarized attenuated laser pulses, see e.g. [38], [39]. All P&M schemes relay on the no cloning theorem and a random generation of quantum states. Therefore a source of qubits [7], needed for Alice to prepare quantum states as well as a source of randomness is mandatory for Alice and Bob for state preparation and measurement basis choices, respectively.

Two State Protocol, B92

Six years after the BB84 protocol has been published, Bennett realized that, in order to get an identical raw key string, it was sufficient for Alice to send only two instead of four non-orthogonal states, $|u_0\rangle$ and $|u_1\rangle$, with $\langle u_0|u_1\rangle \neq 0$. This is commonly referred to as the B92 protocol [41]. By randomly applying the projectors $P_0 = 1 - |u_1\rangle\langle u_1|$ and $P_1 = 1 - |u_0\rangle\langle u_0|$ Bob either annihilates the send state or gets a positive measurement value, $1 - |\langle u_0|u_1\rangle| > 0$ from his measurement. Again, by announcing which state was sent, a correlated raw key can be sifted from the measurement results and the protocol is thereafter identical to the BB84 case. In his paper Bennett proposed an experimental realization using a Mach-Zehnder-interferometer that randomly introduces a phase shift (i.e. a 0° or 180° phase shifted state is applied) in one arm and a time delay (Δt) in the other. Alice first sends a weak state that gets randomly phase shifted in one arm and delayed in the other. After Δt a bright reference pulse with no phase coding is sent through the same fiber. Bob who uses an identical Mach-Zehnder-interferometer applies accordingly a random phase shift on the weak pulse in one arm of his interferometer and a time delay on the other. The bright laser pulse is only delayed by Bob, no phase coding is applied. At the output of Bob's interferometer the delayed (from Alice's interferometer) and phase shifted (from Bob's interferometer) as well as the phase shifted (Alice) and delayed (Bob) weak pulse interfere constructively or destructively, depending on the random phase choice. A constructive interference will result in a detector count and hence in raw key bit. The bright reference pulse is supposed to detect a possible eavesdropper who would introduce an intensity decrease, if part of the light was split.

Six State Protocol

The six state protocol is a logical generalization of the classical BB84 that uses six instead of four preparation states. When considering qubits as spin $\frac{1}{2}$ particles described by the group of $SU(2)$, the respective generators of this group are given by the three Pauli matrices $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, with $SU(2) = \left\{ e^{-\frac{i}{2}\vec{\alpha}\cdot\vec{\sigma}}, \alpha \in \mathbb{R}^3 \right\}$.. While in four states QKD only two of them (usually $\sigma_x = |+\rangle\langle+| - |-\rangle\langle-|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$) are used, the six state protocol adds the third eigenstates $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$ of the generator

[7] There exist protocols that apply quantum states with more degrees of freedom. Since this is beyond the scope of this thesis, it is for example referred to [40] for further information.

(usually $\sigma_y = |\Phi^+\rangle\langle\Phi^+| - |\Phi^-\rangle\langle\Phi^-|$). Alice and Bob hence choose randomly to prepare one of these three different states and measure them after passing the quantum channel, respectively. This protocol shows not only a higher vulnerability to eavesdropping, as further discussed in chapter 3.2.1.4, but also its practical implementation is rather complicated compared to the four state case. While for example horizontal/vertical as well as diagonal/anti-diagonal polarization uniquely correspond to σ_x and σ_z and are easily prepared using $\frac{\lambda}{2}$ wave-plates, circular polarization on the other hand, corresponding to σ_z, needs an additional $\frac{\lambda}{4}$ wave-plate. This fact becomes reasonable when considering the Bloch sphere. While for two bases, i.e. four states, only one plane of the sphere is used, a third basis demands a third degree of freedom, mathematically represented by the complex eigenstates of σ_y. When researching the origin of this protocol, two sources are dominant. On the one hand it is often referred to a talk, given by N. Gisin during a Quantum Computation workshop in Torino, on the other hand security proofs and eavesdropping strategies are found in [42, 43]

The First Experiment

The first experimental setup of the BB84 protocol that reported a successful key exchange over a distance of $30cm$, was published in 1992 by Benett, Bessette et al. [3]. This proof of principles experiment comprised a pulsed green LED as an incoherent light source, that was recollimated by a $25\mu m$ pinhole and an appropriate focal lens. An interference filter was used for filtering to an average photon number $\mu = 0.1$ [photon/puls] and cutting out the optimal wavelengths for the photomultiplier to have the highest efficiency. With two electro-optical polarisers, Pockel cells, the respective horizontal-vertical and left-and right-circular states were prepared by changing the voltage. The quantum channel was a 32cm air gap between the laser source (Alice) and the measurement apparatus (Bob). The measurements were performed using another Pockel cell in order to measure in the circular basis, as for the horizontal/vertical basis a prism was used that splits light in the appropriate polarization before sending it into a photomultiplier tube. With the adequate timing adjustment between laser pulses, detector dead time and Pockel cell voltage, 2000 correlated bits could be collected by Alice and Bob after the sifting phase, with an average error of $3,95\%$. Figure 3.2 shows the setup as it is found in the original work [3]

Coherent vs Fock states

Although P&M protocols used pure single photon Fock states and qubits, i.e. $|1\rangle$ and $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, to proof unconditional security, such as the presented BB84 protocol in the previous chapter, most experiments applied pulsed or continuous wave (cw)

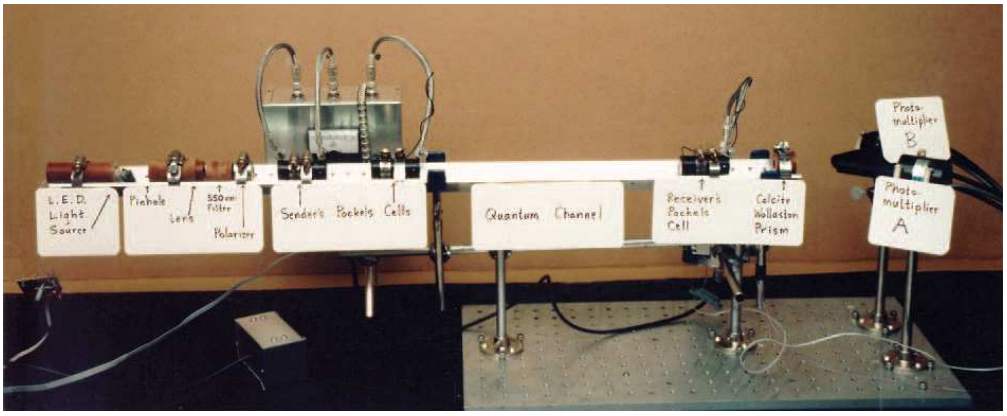

FIGURE 3.2: First experimental setup of QKD system. The BB84 Protocol is used to generate a key between Alice and Bob, who are separated by an air gap of 30cm. Taken from [3].

attenuated laser sources that emit coherent states, i.e.

$$|\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{3.1}$$

with an average photon number $\mu = |\alpha|^2$ below one. The parameter α is the eigenvalue of the annihilation operator $\hat{a}$, i.e. in general a complex number. However since coherent states comprise an infinite sum over all possible number states, not only vacuum or single photon states, such as $|0\rangle$ and $|1\rangle$, respectively, but arbitrary photon numbers states, $|n\rangle$ are produced according to the Poissonian distribution, $|\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!} e^{-|\mu|^2}$. As a consequence, the photon number splitting (PNS) attack, [44], exposes this experimental flaw by allowing the attacker to steal a single photon with all information without leaving a statistical mark. But this experimentally convenient and simple way of employing coherent states could be eventually approved by slightly modifying the BB84 protocol. The result are two proposed alternatives, the so called *SARG04* protocol [4] as well as the *decoy state protocol* [45], both shortly stated in the following.

SARG04

This protocol was proposed in 2004 as a response to the PNS attack. Unlike in the BB84 case the two bases that Alice can use for encoding comprise two non-orthogonal states, i.e. $A = \{|0_a\rangle, |1_a\rangle\}$ and $B = \{|0_b\rangle, |1_b\rangle\}$, respectively, with $\langle 0_i|1_i\rangle = \chi > 0$, and $i \in \{a, b\}$. The left projection of the Poincaré sphere depicted in Figure 3.3 shows this initial setup. In order to discriminate whether a state was sent from set A or B Bob uses the following "filter" operator $F_A = \frac{1}{\sqrt{1-\chi}}(|+x\rangle \langle 1_a^{\perp}| + |-x\rangle \langle 0_a^{\perp}|)$, with $|0_a^{\perp}\rangle$ and $|1_a^{\perp}\rangle$ being orthogonal to $|0_a\rangle$ and $|1_a\rangle$. The respective operator F_B is defined for the set B, again with a projection on either the x, y or z. After Bob has randomly applied one of the filter operators to the received state, he eventually performs a random measurement in σ_x to either receive $+1$ or -1 corresponding to $|0_a\rangle$ or $|1_a\rangle$, respectively, as shown on

the right hand side of Figure 3.3.

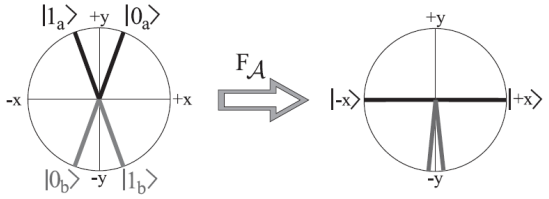

FIGURE 3.3: The left side shows the four states on the projected Poincaré sphere that Alice can choose from. In the right picture the operator F_A has been applied to the four states. They can be discriminated by a measurement of σ_x providing the correlation between the measured results and the preparation state. Source [4]

The same holds for a measurement of F_B followed by the spin measurement in the respective axis.

Due to this additional measurement it is possible to perform the sifting process without Alice explicitly revealing her prepared basis. As a simple example to illustrate the sifting, the four prepared states are assumed in the x and z direction of the Poincaré sphere, after F_A or F_B has been applied. Hence Alice knows that Bob either measures $|\pm x\rangle$ and $|\pm z\rangle$ with the respective spin operators σ_x and σ_z. Instead of revealing her basis of preparation she announces a pair of states that are not in the same basis, generally written as $A_{\omega,\omega'} = \{|\omega x\rangle, |\omega' z\rangle\}$ with $\omega, \omega' \in \{+,-\}$. Bob is able to discriminate the state Alice has sent in 25% of all cases. Assuming now that Alice has sent $|+x\rangle$ and additionally announces $A_{+,+}$. Bob can guess the state $|+x\rangle$ when he chooses to measure in the z basis σ_z, which happens half the time, and receives the outcome $\sigma_z |+x\rangle = -1$, which happens again half the time. Hence this protocol uses on average only $\frac{1}{4}$ (instead of $\frac{1}{2}$ for the BB84) of the measurement. This however can be compensated by doubling the average photon number from $\mu = 0.1$ to $\mu = 0.2$ photons per pulse. The fact that due to the use of non-orthogonal states the measurement results may be inconclusive although the basis has been chosen correctly, results in a non-deterministic information for Eve even if she can extract the same state sent to Bob from a multi-photon coherent pulse. For more information about limits, constraints as well as the rigorous proof of this protocol it is referred to [4, 46]

Decoy state protocol

The decoy state protocol has first been introduced by W.Y Hwang in 2003 [45]. He proposed that Alice uses two kind of coherent sources, a signal source that emits pulses with an average photon number $\mu < 1$ and a decoy source with a higher mean photon number $\mu' > \mu$. The crucial point of this protocol is that Alice randomly sends pulses from one of these sources, but Eve can not distinguish which of them was used. During the measurement process Bob assigns the relative frequencies of his n detected pulses, to the respective source, giving him y_n and y'_n, respectively. This allows to calculate

the yield Y of the quantum channel for the respective source, $Y_s = \sum_{n=1}^{\infty} P_n(\mu) y_n$ for the signal and $Y_d = \sum_{n=1}^{\infty} P_n(\mu') y'_n$ for the decoy source, with $P_n(\mu)$ and $P_n(\mu')$ being the probability of the source to emit an n number photon state given μ or μ' [8]. An inequality of these two quantities can be derived from these measurements, $Y_s > \frac{P_2(\mu)}{P_2(\mu')} Y_d$. As long as this relation holds an attack can be excluded. Although Eve would gain full information about the sent bit by splitting a multi-photon pulses, she will hereby violate this bound by altering the channel yield of signal and decoy state differently. Further work for making this protocol more suitable to practical QKD systems as well as further information about the decoy state protocol can for example be found in [47–49].

3.2.1.3 Entanglement-based (EB) QKD

The E91 Protocol

The first idea to employ entanglement to create a common secret secret key was introduced in the E91 protocol, derived by Arthur Eckert in '91 [50]. Eckert proposed to use the four Bell states, $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$, emitted by a source located in between Alice and Bob. Due to perfect (anti)-correlation of the states when measured in the same basis as well as the randomness of the eigenvalue inherent in the outcome of the projected observables, a common secret key can be grown [9]. In his original work Eckert proposed to measure the polarization of spin-$\frac{1}{2}$ particles in three different bases, namely $\Phi_1^a = 0°$, $\Phi_2^a = 90°$, $\Phi_3^a = 45°$ for Alice and $\Phi_1^b = 0°$, $\Phi_2^a = -45°$, $\Phi_3^a = 45°$ with the corresponding unit vectors $\vec{a}_i$ and $\vec{b}_j$, respectively, with $i, j \in \{1, 2, 3\}$, that represent the direction of polarization orthogonal to the direction of propagation. When considering photons, i.e. spin-1 particles, the polarization angles are given by half the stated angles. In the next step Alice and Bob randomly and independently measure the polarization of the incoming particles in the available bases. By defining the expectation value or *correlation coefficient* $E(\vec{a}_j, \vec{b}_j) := P_{+\,+}(\vec{a}_j, \vec{b}_j) + P_{-\,-}(\vec{a}_j, \vec{b}_j) - P_{+\,-}(\vec{a}_j, \vec{b}_j) - P_{-\,+}(\vec{a}_j, \vec{b}_j)$, with $P_{\pm\,\pm}(\vec{a}_j, \vec{b}_j)$ denoting the probability of measuring ± 1 with $\vec{a}_i$ and ± 1 with $\vec{b}_j$, a quantity similar to the CHSH inequality, [51], can be derived, $S = E(\vec{a}_1, \vec{b}_1) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_3, \vec{b}_1) + E(\vec{a}_3, \vec{b}_3)$. When a measurement is performed an explicit value of E can be calculated: $E(\vec{a}_i, \vec{b}_j) = -\vec{a}_i \cdot \vec{b}_j = -|\vec{a}| \cdot \left|\vec{b}\right| \cdot \cos(\phi) = -\cos\phi$, with ϕ being the angle between two bases $\Phi_i^a - \Phi_j^b$. In the special case when the same axis is chosen E yields -1, indicating a perfect anti-correlation. Furthermore S can be calculated for non-local quantum states to be $2\sqrt{2}$. This can be practically verified when Alice and Bob use the

[8] It has to be noted that the probability for a coherent source with mean photon number μ to emit a state with n photons is calculated from Eq. 3.1, whereas the probability of Bob detecting an n photon state using a detector with quantum efficiency ν is given by $P_s = \nu\mu e^{-\mu}$ for a single photon state and $P_s = \sum_{n=2}^{\infty}(1-(1-\nu)^n)\frac{\mu^n}{n!}e^{-\mu}$ for a pulse comprising more than one photon. Therefore the yield can be still be high, or even 1, although some photons are lost.

[9] The anti-correlation is given when the Bell states $|\Psi\rangle^{\pm} = |HV\rangle \pm |VH\rangle$ are emitted by the source. Correlation otherwise.

measurements where the orientations of the basis do not coincide. This gives them the possibility to check for the quality of the source, the properties of the quantum channel or the presence of an eavesdropping attack without loosing potential key bits. The remaining measurement results in which the bases coincide are correlated can be used as the raw key.

Although it is in principle possible to create entangled states using any available observable with at least two degrees of freedom of a quantum state, the most common ones are time, energy, momenta or polarization entangled states. The variety of these type of protocols lies in the source and hence in the measurement of entanglement. Before going further into detail on how polarization entangled states can be efficiently generated, which is a crucial topic in further chapters of this thesis, two other quite popular approaches of entanglement based protocol are shortly presented.

The so called coherent one way (COW) and differential phase shift (DPS) protocol use time-energy and time-bin entanglement, respectively. In the strict sense these two types of protocols, both proposed by experimental groups, are a hybrid of discrete and continuous variable QKD, since the information transferred via the quantum channel, is encoded in a sequence of coherent states, while not the single state itself but the difference between the previous and subsequent state are measured. These values lie in a continuous outcome space. In this theses they are included in the discrete variable section, since the sent quantum states are still given in discrete values.

Differential Phase Shift (DPS)

The DPS protocol was first suggested in 2002 by Inoue et al. [5], where the experimental setup of Bennetts work in the $B92$ protocol [41] (presented in the previous chapter 3.2.1.2) has served as the basic idea. They realized that a protocol that exploits the phase interference of a Mach Zender interferometer is possible without the strong reference pulse that was proposed in the B92 protocol due to a precise scaling extracted from the time between two subsequent signals. Alice prepares hereby a string of single photon pulses, each modulated with a phase shift of either 0 or π and a time difference T. Bob measures this sequence with an interferometer that introduces the same time difference of T between both arms. The interferometer splits the i-th signal sent by Alice into the fast and delayed pulse that interferes hereby with the $(i-1)$-th as well as with the $(i+1)$-th signal of the previous and the subsequent pulse. The consecutive detection is modified in a way that the possible phase differences of π and 0 are detected by two separate detectors that determine a bit value of the raw key, depending on the respective click. When Bob forwards the information to Alice at which time a photon was detected using the classical channel, she immediately knows which detector has measured the photon, since she prepared the phase information, and hence an equal bit can be established. The original setup as it was proposed in [5] is shown in Figure 3.4.

The preparation of the pulse train, denoted by a, b and c, is in this case realized by a cascade of beamsplitters and switches [10].

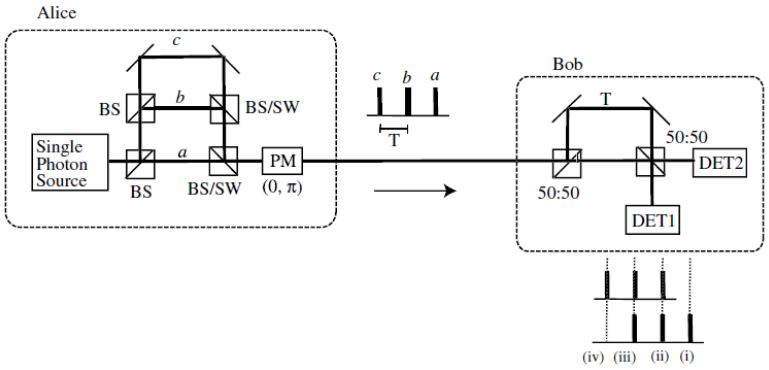

FIGURE 3.4: Setup of the DPS protocol, employing Beam splitters (BS) and switches (SW) as well as the Polarization modulation (PM) at Alice's side. The randomly phase shifted pulse train with time difference T is measured by an interferometer at Bobs side. Four different time slots, (i)-(iv), for three signals are possible. Detector 2 responds to phase differences of $\pm\pi$ and Detector 1 to 0. Picture taken from [5].

Coherent One Way (COW)

The COW protocol uses a similar approach in the sense that it demands a strict time synchronization between the sent quantum signals and the measured data. However in this protocol the bits are encoded in the sequence of two consecutive pulses. An empty pulse followed by a pulse with the photon number μ denotes "1" and vice versa "0", i.e. $|0\rangle_A := \left|\sqrt{\mu}e^{i(2k-1)\phi}\right\rangle_{2k-1}|0\rangle_{2k}$ and $|1\rangle_A := |0\rangle_{2k-1}\left|\sqrt{\mu}e^{i(2k)\phi}\right\rangle_{2k}$. Alice can realize this source using a pulsed laser followed by a variable attenuator. Bobs measurement is hereby divided into two parts, a data line that comprises one detector D_B and a monitoring line that consists of an interferometer with a phase shift ϕ in the long arm and two detectors D_{M1} and D_{M2} at the respective outputs. Fig. 3.5 illustrates this setup. The two lines are connected by an imbalanced beam splitter with ratio t_B. The overlap

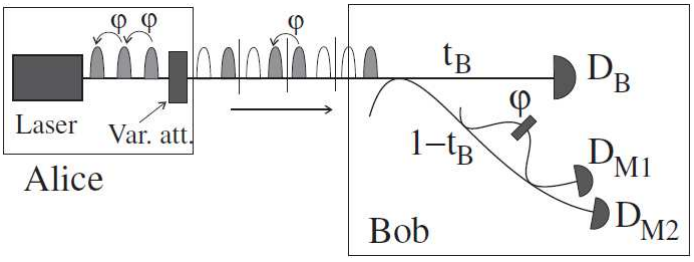

FIGURE 3.5: Setup of Coherent One Way (COW) QKD system with phase differences φ between adjacent signals. The eligible exits of the Mach-Zender Interferometer allow for a constructive or destructive superposition, noted by the respective detector M1 or M2. The splitter in front of the interferometer, with splitting ratio t_B allows an additional heralding of the pulse train. Picture taken from [6].

[10]The authors use the nomenclature "switch" for a beamsplitter that does not have a transmitted beam but two reflected (left and right) beams.

between the two bits is given by $|\langle 0|1\rangle|$ and hence the probability p for an unambiguous detection for a bit with detector D_B is $p = 1 - |\langle 0|1\rangle|^2$. With the monitoring Alice and Bob are able to detect a possible attack. When considering the pulses of two photons with α_j being the amplitude of the j-th pulse and respectively for α_{j+1}, then the probability to detect a photon at either D_{M1} or D_{M2} is calculated from $|D_{M1}\rangle = \left|i\frac{\alpha_j+\alpha_{j+1}}{2}\right\rangle$ and $|D_{M2}\rangle = \left|\frac{-\alpha_j+\alpha_{j+1}}{2}\right\rangle$, respectively. The amplitude square is $|\alpha_j|^2 = 0$ for vacuum or $|\alpha_j|^2 = \mu \cdot t \cdot t_B$ for pulses with average photon number μ and an attenuation factor of t. The phase Φ is chosen w.l.o.g. to be zero. When therefore either the j-th or the $j+1$-th pulse is empty, the probabilities for a detector click are $|D_{M1}|^2 = |D_{M2}|^2 = \frac{1}{2}\mu t(1-t_B)$. When both pulses contain μ photons $|D_{M1}|^2 = \mu t(1-t_B)$ and $|D_{M1}|^2 = 0$. Considering the arrivals times $2k$ and $2k+1$ of a sequence of two non empty photon pulses, a count on detector D_{M2} at time $2k+1$ can only occur when the interference hase changed due to an altered phase coherence. This serves as an indication for an adversary. If, however, an eavesdropper was able determine photons present in between two consecutive bit sequences the respective phase in each bit would not be disturbed and Eve gains full information about the bit when Bob announces the time stamp of the measured bit for Alice. In order to prevent this problem a decoy state was added that is sent randomly within the pulses. This state comprises again two pulses that carry an average photon number of μ each. Therefore Eve does not gain any information about the key since in this case a bit can not be determined by a measurement in between a bit sequence. This protocol was first introduced in 2004 by Gisin et. al [6].

DPS and COW are rather untypical protocols for entanglement based QKD, since the states do not directly show the typical entangled state. However since the security is here based on a sequence of states where each pulse has to be regarded with respect to previous and subsequent pulse, the information encoded in its parts is smaller than the information of the entire sequence, which is the information theoretical approach for EB QKD to describe entanglement. In the next sub-chapter a more obvious approach is presented in the form of polarization entangled photon pairs.

Polarization Entanglement

Since sources that emit polarization entangled states (or EPR, Einstein-Podolski-Rosen, states) for QKD are mostly photonic crystal sources, other possible approaches are shortly mentioned in 4.1 but omitted in more detail as they are beyond the scope of this thesis. Photonic crystals use spontaneous parametric down conversion (SPDC) to split a pump photon into two photons of shorter wavelength with opposite or equal polarization (usually called signal and idler state), e.g. $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm e^{i\varphi}|VV\rangle)$ and $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm e^{i\varphi}|VH\rangle)$. The goal is now to adapt the phase φ to gain one of the four maximally entangled Bell states. Since the measurement of such polarization

entangled states is easily performed using polarizers in front of an SPAD, it is one of the most used schemes for QKD as well as for other application, such as proving the non-locality of quantum mechanics via CHSH inequality or providing a single photon state source that can easily be heralded by measuring one photon immediately after creation knowing that the other was created. Since the SPDC is a fundamental concept of this thesis, the theory behind it will be introduced in more detail.

Spontaneous Parametric Down Conversion (SPDC) Sources

The experimental basics of SPDC using a birefringent (non linear) isotropic waveguide crystal, that carries no further external electromagnetic fields except for the incoming light, is rather simple and quickly explained. The geometric properties of the crystal lattice allows the light to propagate along two paths, one with refractive index n_O and another with n_E, an ordinary and an extraordinary path. The difference of both refractive indices $\Delta n = |n_O - n_E|$ donates the quantity of birefringence of a material. The incoming light, commonly referred to as "the pump", is hereby separated with respect to energy and momentum conservation,

$$\omega_{Pump} = \omega_{Signal} + \omega_{Idler} \quad \text{and} \quad \vec{k}_{Pump} = \vec{k}_{Signal} + \vec{k}_{Idler}. \tag{3.2}$$

The second equation is also known as phase matching and will become of great importance for the SPDC process.

Depending on whether signal and idler have equal or different polarization, the SPDC process is called Type I or Type II, respectively. As the name implies this process is spontaneous and random, hence the splitting of a pump photon can not be controlled by external parameters. Here a major drawback of this method is rooted, since, depending on the respective crystal, the conversion efficiency (also called brightness) is in the order of 10^{-12} per incoming photon. The most used crystal types are $\beta-$Barium Borate (BaB_2O_4), also known as BBO, KDP (KH_2PO_4), KTP ($KTiOPO_4$), Lithium Niobate ($LiNbO_3$) or Gallium Arsenide ($GaAS$). The crystal structure of these materials share a common property that is explained in more detail in the course of the following theoretical description.

When it comes to a correct mathematical formalism, SPDC has to be regarded in a larger context. It is part of a three wave mixing processes (parametric interaction), triggered by second order polarization of the electromagnetic fields with frequencies ω_1, ω_2 and ω_3 in a nonlinear medium. The origin of three wave mixing is found in the electrical displacement of an electric field $\vec{E}(\vec{r},t)$, given by $\vec{D}(\vec{r},t) = \epsilon_0\vec{E}(\vec{r},t) + \vec{P}(\vec{r},t)$, with ϵ_0 being the vacuum permittivity. The polarization vector $\vec{P}$ is hereby composed by the respective orders of the electric susceptibility χ that for its part depends on the orders of the electric field (more precisely from the eligible frequencies of the orders of

the electric field),

$$\chi(\vec{E}) = \chi^{(1)} + \chi_j^{(2)} E^j + \chi_{jk}^{(3)} E^j E^k + \cdots , \tag{3.3}$$

noted in Einstein notation for upper and lower indices. The components of the polarization vector, defined by $\vec{P} = \epsilon_0 \cdot \chi \cdot \vec{E}$, are hence given by

$$P_i = \epsilon_0 \big(\underbrace{\chi^{(1)} E_i}_{\text{linear Polarization, } \vec{P}_L} + \underbrace{\chi_{ijk}^{(2)} E^j E^k + \chi_{ijkl}^{(3)} E^j E^k E^l + \cdots}_{\text{nonlinear Polarization, } \vec{P}_{NL}} \big). \tag{3.4}$$

The entries of the tensor $\chi_{ijk}^{(2)}$ are essential for second order nonlinear effects comprising three waves. Only crystal structures that have no inversion symmetry, i.e. these crystals that can not be mapped onto itself by a point reflection, are possible candidates for second order effects [11]. The resulting field within a nonlinear media is hence described by the wave equation together with a perturbation term, namely the nonlinear part of the polarization $\vec{P}_{NL}$

$$\vec{\nabla}^2 \vec{E} - \frac{\epsilon_0}{c_0^2} \frac{\partial^2 \vec{E}}{\partial t^2} = \mu_0 \frac{\partial^2 \vec{P}_{NL}}{\partial t^2}, \tag{3.5}$$

with c_0 being the speed of light in medium and μ_0 being the permeability constant of free space. This fundamental equation is valid for all three wave mixing processes.
In order to give a short derivation of the interacting waves, two monochromatic fields with frequencies (ω_1, ω_2), given by $E(\vec{r},t) = \frac{1}{2}\big[\vec{E}(\vec{r},\omega_1)e^{i\omega_1 t} + \vec{E}(\vec{r},\omega_2)e^{i\omega_2 t} + c.c.\big]$, are inserted into the second order polarization of Eq. (3.3), $P^{(2)}(\vec{r},t) = \epsilon_0 \chi^{(2)} \vec{E}(\vec{r},t)\vec{E}(\vec{r},t)$. The contributions of all terms, written in index notation, are given by

$$\begin{aligned} P_i^{(2)}(\vec{r},t) = & \underbrace{\frac{1}{2}\big[P_i(\vec{r},2\omega_1)e^{i2\omega_1 t} + cc.\big]}_{\text{Second harmonic generation of } \omega_1} \\ & + \underbrace{\frac{1}{2}\big[P_i(\vec{r},2\omega_2)e^{i2\omega_2 t} + cc.\big]}_{\text{Second harmonic generation of } \omega_2} \\ & + \underbrace{\frac{1}{2}\big[P_i(\vec{r},\omega_1+\omega_2)e^{i(\omega_1+\omega_2)t} + cc.\big]}_{\text{Sum frequency generation of } \omega_1 \text{and } \omega_2} \\ & + \underbrace{\frac{1}{2}\big[P_i(\vec{r},\omega_1-\omega_2)e^{i(\omega_1-\omega_2)t} + cc.\big]}_{\text{Difference frequency generation of } \omega_1 \text{and } \omega_2} \\ & + \underbrace{\frac{1}{2}\big[P_i(\vec{r},0) + cc.\big]}_{\text{Constant field}}, \end{aligned} \tag{3.6}$$

[11] This can easily be seen by applying point symmetry $f(x) = -f(-x)$ to the second order term of the polarization: $P_i^{(2)}(-\vec{E}) = \epsilon_0 \chi_{ijk}^{(2)} E^j E^k = -P_i^{(2)}(\vec{E})$. This only holds for $\chi^{(2)} = 0$.

with

$$P_i(\vec{r}, \cdot \pm \cdot) = \frac{1}{2}\epsilon_0 \chi^{(2)}_{ijk} E^j(\vec{r}, \cdot) E^k(\vec{r}, \cdot). \tag{3.7}$$

The intensity of the fields generated in the course of this process can be easily derived from the conservation of momentum when regarding the photon flux of the respective field I_{ω_i},

$$\frac{dI_{\omega_3}}{\omega_3 dz} = -\frac{dI_{\omega_1}}{\omega_1 dz} = -\frac{dI_{\omega_2}}{\omega_2 dz}. \tag{3.8}$$

These equations are known as the MANLEY-ROWE relations that are valid when all fields propagate into the same direction. A more precise evaluation with respect to the different contribution is discussed in the following lines. The constant field is hereby ignored since this effect is dispensable for three wave mixing.

Sum frequency generation (SFG) and Second harmonic generation (SHG)
As the name implies SFG occurs when the frequencies of two waves ω_1 and ω_2 interact to create a field with the sum of the single frequencies $\omega_3 = \omega_1 + \omega_2$. SHG can be seen as a special case of SFG that occurs despite the lack of a second and third field. The second wave ω_2 coincides in this case with the first wave $\omega_1 = \omega_2 = \omega$ in a self-interaction process. This results in a frequency doubling of the generated third field $\omega_3 = 2\omega$. The intensity of the SFG and SHG field, respectively, can be derived by exchanging the second order perturbation of the nonlinear polarization, given by Eq. (3.6), with the right hand side of the wave equation Eq. 3.5. This means fields of $O(E^3)$ are neglected. The relation between the energy flux I, i.e. its intensity, is given by $I = \frac{n|\vec{E}|^2}{2Z_0}$, with the vacuum impedance $Z_0 = \frac{\mu_0}{\epsilon_0} \approx 377\Omega$ and the refractive index n. When solving Eq.(3.5) in the case of SHG (using the slow envelope approximation), with frequency ω, and assuming that the pump wave only propagates along the crystal of length l [12] with intensity I_ω, the intensity of the second order term $I_{2\omega}$ is calculated to be

$$I_{2\omega} = I_\omega^2 \frac{\omega_0 Z_0 l^2}{2c_0^2 n_{2\omega} n_\omega^2} \sum_{i=1,2} \left| \chi^{(2)}_{ijk} e_j e_k \right|^2 \left[\frac{\sin(\Delta k l/2)}{\Delta k l/2} \right]^2. \tag{3.9}$$

Hereby n_ω and $n_{2\omega}$ denote the refractive indices of the respective waves and $\Delta k := k_{2\omega} - 2k_\omega$ is defined as the deviation from the phase matching condition, expressed with the notation $k_{2\omega} = \frac{2\omega n_{2\omega}}{c_0}$, with $c_0 = \frac{1}{\sqrt{\mu_0 \epsilon_0}}$. This result holds assuming that pump as well as generated second order waves propagate in one direction, without any dependencies on the other two spatial coordinates. A similar equation is received when the more general case of SFG is assumed, where an additional dependence from the intensity of second

[12] l denotes, to be precise, the interaction lengths of the two waves inside the crystal which is in the first order approximation given by the crystal length.

wave and its refractive index has to be considered. When the intensity of the second order term $I_{2\omega}$ with respect to the crystal length l, as well as the phase deviation Δk, as shown in Figure 3.6, is considered, it becomes clear that due to the periodic behavior only a certain interaction length and a small deviation from the phase matched case results in a high second order wave.

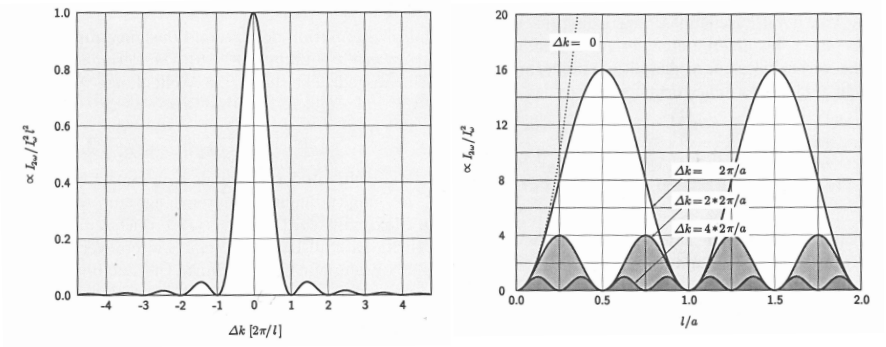

FIGURE 3.6: Left: Intensity of the Second Harmonic wave $I_{2\omega}$ in dependence of the phase deviation Δk. Right: Intensity of the Second Harmonic wave $I_{2\omega}$ in dependence of the Interaction length l for different phase deviations. Pictures taken from [7].

Difference frequency generation (DFG) and SPDC

In analogy to SFG and SHG, DFG is the result of the interaction of two frequencies ω_1 and ω_2, that, however, generate a field of lower frequency with respect to the frequency ω_1, $\omega_3 = \omega_1 - \omega_2$. As previously mentioned the notation for the involved fields are in this cased pump (P), signal (S) and idler wave (I), $\omega_S = \omega_P - \omega_I$. Just like SFG and SHG, SPDC is a special case of DFG where again only one field, the pump, needs to be present. In order to create a signal field it is enough to assume the idler wave originating from quantum vacuum fluctuations. These "idler" fluctuations are boosted to a measurable level by amplifying the frequency of the wave within an appropriate cavity. The three wave mixing process in the crystal is triggered in the presence of the pump wave. The intensity for this as well as for the DFG is derived similarly to SFG and SHG but depends in this case on the intensity of the respective field at the beginning of the interaction length l. The equation for signal and idler are explicitly given by

$$I_{\omega_S}(l) = I_{\omega_S}(0)\Big[\cosh(\chi \frac{\omega_S \omega_I}{n_{\omega_S} n_{\omega_I} n_{\omega_P}} \frac{Z_0 I_{\omega_P}}{2c_0^2} \cdot\ l)\Big]^2 \tag{3.10}$$

$$I_{\omega_I}(l) = I_{\omega_S}(0)\Big[\sinh(\underbrace{\chi \frac{\omega_S \omega_I}{n_{\omega_S} n_{\omega_I} n_{\omega_P}} \frac{Z_0 I_{\omega_P}}{2c_0^2}}_{\kappa'} \cdot\ l)\Big]^2 \tag{3.11}$$

For a positive gain of signal and idler wave it is necessary for the phase displacement Δk to fulfill the inequality $|\Delta k| < 2\,|\kappa'|$. Further reading about this topic as well as a more detailed description of the respective derivations can be found in various textbooks and works, e.g. [7] or [52].

Phase Matching (PM) and Quasi Phase Matching (QPM)

Before closing the section of polarization entanglement, some additional background about the phase matching condition has to be given in order to entirely understand the experimental work presented in the upcoming chapters. There are two possible ways to achieve a suitable phase matching.

The first exploits the angle dependence of the refractive index of the extraordinary wave. Considering a unidirectional crystal with a single crystal axis. The refractive index of the extraordinary wave depends hereby on the constant refractive indices for the two path, n_O and n_E, as well as on the angle between the wave vector of the pump beam and the crystal axis Θ,

$$\frac{1}{\tilde{n}_E(\Theta)} = \frac{\cos^2(\Theta)}{n_O^2} + \frac{\sin^2(\Theta)}{n_E^2}. \tag{3.12}$$

With the phase matching constraint $\Delta\kappa = k_P - k_S - k_I = 0$, with $k_\cdot = \frac{\omega_\cdot \tilde{n}_\cdot}{c_0}$, as well as the refractive indices n_O and n_E, given by the Sellmeier equations of the respective material, the angle of this equation can be uniquely determined. In practice this angle can only be achieved when it is exactly 90°, as otherwise the wave vectors of different polarized fields diverge in birefringent crystals.

The other, rather popular approach, is called QPM. The interaction length, or coherence length l_c, given by $l_c = \frac{2\pi}{\Delta k}$ donates the maximal gain of intensity, given by Eq. 3.10 and 3.11, respectively. The periodic behavior of these equations stems from the second order nonlinearity $\chi^{(2)}$ and hence from the crystal structure itself. However when this structure is inverted periodically according the coherence length l_c a continual rise of the intensity can be realized. This structural flip is achieved by applying short electrical fields on respective regions along the crystal. This periodically poled structure within the waveguide reduces furthermore the divergence of differently polarized waves. The drawback of this technique are high demands in the manufacturing process and hence high costs. Figure 3.7 shows a comparison of intensity for the perfect, the QPM and the case of no phase matching.

However, when using SPDC for creating polarization entangled photons it has to be noted that the received state is not a pure Bell state but a mixture of all possible higher order states, similar to the P&M scheme where coherent states are chosen over Fock states. Since higher order fields have been neglected during this calculation, as well as a completely classical approach to SPDC was presented, the stated results do not reflect this fact. In more detail the states received after a nonlinear crystal can be approximated by

$$|\Psi\rangle \approx \sqrt{p(0)}\,|0\rangle + \sqrt{p(1)}\,|\Psi_2\rangle + \sqrt{p(2)}\,|\Psi_4\rangle + \cdots \tag{3.13}$$

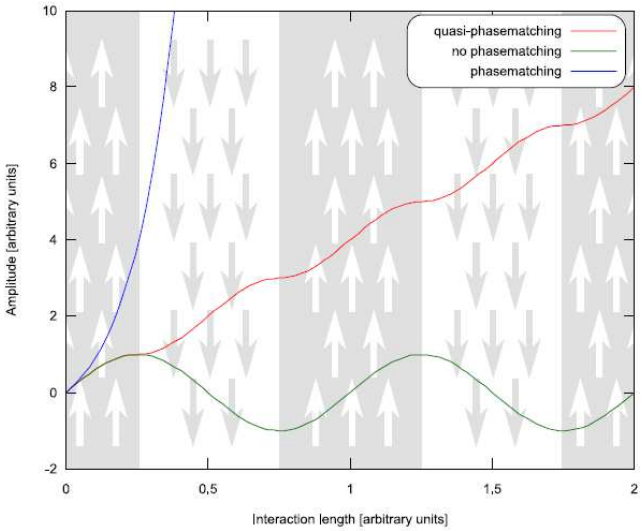

FIGURE 3.7: The three curves show the behavior of perfect phase matching (blue), quasi phase matching (red) with alternating poling periods and no phase matching (green).

with $p(i)$ being the probability with respect to the average photon number, e.g. $p(1) = \mu$ and $p(2) = \frac{3}{4}\mu^2$. $|\Psi_2\rangle$ is the respective Bell state, depending on type I or type II SPDC and $|\Psi_4\rangle = \frac{1}{\sqrt{3}}\big(\,|02\rangle\,|02\rangle + |20\rangle\,|20\rangle + |11\rangle\,|11\rangle\,\big)$ being a higher order state received from four wave mixing of the third order χ^3 susceptibility. In analogy to the P&M case this has to be taken into account as a possible source of information for an adversary to gain information. The security proofs are hereby able to estimate this leak of information and annihilate it by using respective post processing.

This concludes the short overview about discrete variable QKD protocols and the experimental implementations. The chapters 4.2.2.2 and 4.2.2.3 show more concrete results and applications of the discussed topics. Before proceeding with continuous variable QKD an overview about possible attack strategies of an eavesdropper and the corresponding theoretical concepts for a secure key creation considering these threats are addressed. A convenient conclusion for this matter is that each P&M protocol can be treated as an EB protocol which makes a security proof applicable on both concepts. This can be shown by introducing a binary string S_n [13] and its corresponding quantum state $|\Psi(S_n)\rangle$ that Alice wants to transmit in a P&M way. The entangled state $|\Phi^n_{AB}\rangle_{AB} = \frac{1}{d_n}\sum_{S_n} |S_n\rangle_A \otimes |\Psi(S_n)\rangle_B$ can be defined, with d_n being the cardinality of the set of all S_n. When Alice chooses the sequence S_n she sends the corresponding state $|\Psi(S_n)\rangle_B$ to Bob. This shows that the first two concepts, P&M and EB QKD, can be treated equally from a mathematical point of view [14].

[13] S_n, chosen by Alice, can be seen as a "pre-key" that does not need to satisfy any criteria since each bit is randomly changed by Bobs measurement anyway. All possible combination of S_n form a basis in the key space.

[14] Mathematical equality means in this case, that one security proof of one can be applied to both.

3.2.1.4 Eavesdropping and Security of discrete QKD Schemes

In this section possible eavesdropping strategies as well as bounds for secure key rates with respect to the presented protocols are discussed following the work of [35], [53] and [54]. Generally speaking eavesdropping attempts can be classified by three different types, namely *individual (incoherent) attacks*, *collective attacks* and *coherent (joint) attacks*. The three classes differ in the threat an eavesdropper poses to the protocol. In the first two types Eve is bound by current or possible future technology, whereas the latter type limits an attacker only by the laws of quantum mechanics. Before discussing respective types in more detail an example of an individual attack, the intersect/resend attack, is examined in the following lines as a motivation.

Simple Intersect/Resend-attack

Since the publication of BB84 the intersect-resent attack is one of the most studied attack strategies in QKD. In this few lines we give Eve the power to measure an intercepted photon in whatever basis she likes, while device imperfections of Eve as well as of Alice and Bob are not considered. As already previously mentioned in 3.1, Eve can gain a maximal knowledge of $\frac{1}{4}$ of the key using the same bases as Bob, with the cost of being exposed due to statistical errors. The Shannon entropy that corresponds to that probability is calculated by Eq. 2.1 to be 0.81. This means that Eve gets an information of $1 - 0.81 = 0.19$ bits per photon measured. In the experimental setup these knowledge is erased using privacy amplification [15]. A hash function can be used to reduce the transmitted, but partially known, bit string to a shorter but secure string. However, in order to guarantee mathematical security of the final key, the information Eve can extract during the quantum phase has to be considered more carefully. Apparently the best strategy for Eve is a measurement in a basis that lies between the two preparation bases of Alice. This basis is commonly known as the *Breidbart* basis. This can easily be shown when we assume that Eve can choose her measurement basis, in the following called $|\Psi\rangle$, freely on the Bloch sphere. Hence the most general form is given by

$$|\Psi\rangle = \sin(\theta/2)e^{\frac{-i\Phi}{2}} |H\rangle + \cos(\theta/2)e^{\frac{i\Phi}{2}} |V\rangle \,, \tag{3.14}$$

with θ being the polar and Φ being the Azimuth angel of the sphere, respectively. The horizontal state $|H\rangle$ can w.l.o.g. chosen to be at the north-pole of the sphere. Since we assume that Alice uses only two different bases to encode her bits, only one plane of the sphere has to be considered, meaning that $\Phi = 0$. We assume further that Alice will encode "0" with either $|H\rangle$ or $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. The probability that Eve gets the

[15] Before privacy amplification, error correction is applied in order to gain a common, error free key.

right result is therefore given by

$$p(\theta) = \frac{1}{2}\Big\{ |\langle\Psi|H\rangle|^2 + |\langle\Psi|+\rangle|^2 \Big\} \tag{3.15}$$

$$= \frac{1}{2}\Big\{ \sin^2(\theta/2) + \frac{1}{2} + \sin(\theta/2)\cos(\theta/2)\Big\} \tag{3.16}$$

When maximizing this by $p'(\theta) = 0$, the constraint for θ is given by $\sin(\theta) + \cos(\theta) = 0$ and hence $\theta = \pi/4 = 45°$, right between the two bases on the Bloch sphere. By calculating the probabilities $|\langle\Psi|H\rangle|^2$ and $|\langle\Psi|+\rangle|^2$ the corresponding Shannon entropy is about 0.6 which gives an average information gain of 0.4 bits per photon for Eve. Compared with the standard basis this is even more than twice the information. However, other than in the standard basis, this value denotes an average knowledge about Eve's received bits. On the other hand it can further be shown that also the errors that Eve introduces are uniformly distributed.
Eve can therefore choose to measure in the same basis as used for preparation by Alice, giving her a deterministic result for $\frac{1}{4}$ of the bits, as it is discussed before. Or she can choose the intermediate basis that gives her on average more information about the sent bits. Furthermore when Eve uses the intermediate basis it becomes harder for Alice and Bob to detect her since also the introduced errors are not detected at each wrong measurement of Eve but uniformly distributed. The next part of this section shows a more detailed overview about individual as well as collective attacks and gives the respective bounds derived to guarantee unconditional security in the presence of an eavesdropper.

Individual and Collective Attacks

In individual as well as collective attacks Eve performs the same action on each qubit sent from Alice. Other than the collective, the individual attack follows a chronological order and hence determines that Eve's measurement is done right when she interacts with the sent qubit. Whereas a collective attack allows her to interact with the Alice state ρ_A without directly measuring it, $\rho_{AE} = \rho_A \otimes \rho_E$ and ρ_{ABE}, respectively, when Bobs measurement is taken into account. Eve is hereby able to store her ancilla ρ_E (e.g. in a quantum memory) and postpone its measurement until sifting, error correction or privacy amplification has been performed or even after a cypher text of the respective key is available. The two approaches obviously lead to two different bounds on the mutual information achievable for Eve. For individual attacks the secret key rate that is extractable for Alice and Bob in presence of an eavesdropper is given by

$$r = I(A:B) - \min(I_{EA}, I_{EB}), \tag{3.17}$$

with $I_{EA} = \max_{Eve} I(E:A)$ and $I_{EB} = \max_{Eve} I(E:B)$ denoting the maximal information that Eve can extract from the raw key of Alice and Bob, respectively. For collective attacks the bound, that is known as the *Holevo bound* which donates the

maximum information about a quantum system [55], reads

$$I_{AE} = \max_{Eve} \{S(\rho_E) - \sum_a p(a) S(\rho_{E|a})\}, \tag{3.18}$$

with S being the van Neumann Entropy $S(\rho) = -\mathrm{Tr}(\rho ln(\rho))$, a being a symbol of the alphabet, $\rho_{E|a}$ the state of Eve's ancilla on the attacked state and $\rho_E = \sum_a p(a)\rho_{E|a}$ the remaining state held by Eve after Bobs measurement (partial trace). Considering the BB84 and the six state protocol, as introduces in section 3.2.1.2, this bound can be easily calculated when the protocols are treated in the entanglement based scheme, which is, as previously mentioned, mathematically equivalent to P&M protocols [56]. When assuming a source that prepares Bell states (e.g. $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$), the results of Alice and Bob measurements are perfectly correlated whenever they use the same basis $\sigma_x \otimes \sigma_x$, $\sigma_y \otimes \sigma_y$ or $\sigma_z \otimes \sigma_z$, with the first subsystem belonging to Alice and the second to Bob [16]. Due to local unitary operation and classical communication (LOCC) the joint state of Alice and Bob can always be expressed in a Bell diagonal form, $\rho_{AB} = \lambda_1 |\Phi^+\rangle\langle\Phi^+| + \lambda_2 |\Phi^-\rangle\langle\Phi^-| + \lambda_3 |\Psi^+\rangle\langle\Psi^+| + \lambda_4 |\Psi^-\rangle\langle\Psi^-|$, with $\sum_{i=1}^4 \lambda_i = 1$. Depending on the chosen common bases, the QBER, i.e. the uncorrelated measurement results are in this case given by,

$$\epsilon_z = \lambda_3 + \lambda_4, \epsilon_x = \lambda_2 + \lambda_4 \text{ and } \epsilon_y = \lambda_2 + \lambda_3. \tag{3.19}$$

The Holevo bound, as defined in equation 3.18, is hereby

$$I_E = S(\rho_E) - \frac{1}{2} S(\rho_{E|0}) - \frac{1}{2} S(\rho_{E|1}), \tag{3.20}$$

with $\rho_{E|i}$ being Eves state when Alice prepared the bit $i \in \{0, 1\}$, which is equally distributed, indicated by the factor $\frac{1}{2}$. Since the distilled state $\rho_E = \rho_{AB}$ and ρ_{AB} depends only on the parameters λ_i, in the following referred to as $\bar{\lambda} := \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$, $S(\rho_E)$, is equal to the Shannon Entropy function of those values (see Eq. 2.1), $H(\bar{\lambda})$. In order to determine the state $\rho_{E|i}$ of Eq. 3.20, with $i \in \{0, 1\}$, Alice and Bob states $|\Phi_k\rangle$ as well as Eve's respective ancilla state $|e_k\rangle$ has to be considered $|\Psi\rangle_{ABE} = \sum_k \sqrt{\lambda_k} |\Phi_k\rangle_{AB} \otimes |e_k\rangle$, with $\langle e_k | e_j \rangle = \delta_{kj}$. After tracing out Bobs subsystem and Alice measurement in either basis one receives $S(\rho_{E|0}) = S(\rho_{E|1}) = h(\epsilon_z)$, with h being the binary entropy function. The Holevo bound hence reduces to

$$I_E(\bar{\lambda}) = H(\bar{\lambda}) - h(\epsilon_z). \tag{3.21}$$

Bound for the Six state Protocol

Due to the preparation in three different bases as well as the constraint that all λ_i add

[16] For $\sigma_y \otimes \sigma_y$ the result is anti-correlated such that Bob has to multiply the result by -1.

up to unity, all quantities can directly be derived, i.e. $\epsilon_x = \epsilon_y = \epsilon_z = Q$, with Q being the QBER, the corresponding bound on Eve knowledge I_E and the secret key rate reads

$$I_E(Q) = Q + (1-Q)h\Big(\frac{1-3Q/2}{1-Q}\Big) \tag{3.22}$$

$$r(Q) = 1 - h(Q) - I_E(Q). \tag{3.23}$$

The maximum tolerable QBER for this protocol, that means $r(Q) = 0$, is calculated to be $12,61\%$

Bound for the BB84 Protocol

Other than in the six state protocol, two bases are used and hence only two constraints are given. The respective entropy given by the entries $\bar{\lambda}$ of ρ_{AB} is $H(\bar{\lambda}) = h(\epsilon_z) + (1-\epsilon_z)h(u) + \epsilon_z h(v)$ and the corresponding information of Eve $I_E(\bar{\lambda}) = (1-\epsilon_z)h(u) + \epsilon_z h(v)$. The equations contain the remaining unknown values that are parametrized by the variables u and v, with $u, v \in \{0,1\}$. Maximizing this equation with respect to the constraint $(1-\epsilon_z)u + \epsilon_z v = \epsilon_x$ that is derived from Eq. 3.19 gives $u = v = \epsilon_x$. For secret key rate and Eve's knowledge about the final key [17] the following equations hold for $\epsilon_x = \epsilon_z = Q$

$$I_E(\bar{\epsilon}) = h(Q) \tag{3.24}$$

$$r(Q) = 1 - h(Q) - I_E(Q). \tag{3.25}$$

For Q=11% the key rate $r(Q)$ vanishes in this case and is hence an upper bound for a secure key exchange [18].

Bound for the BB92 Protocol

Since in this case only two non orthogonal states states $|u_0\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|u_1\rangle = \alpha|0\rangle - \beta|1\rangle$ are prepared the Bell diagonal form of ρ_{AB} loses its symmetry. Another approach, stated in [56], gives a bound that depends on the noise δ introduced by a channel. A depolarizing quantum channel is usually described by completely positive trace preserving map that adds a certain fraction of noise to a given state, $\rho \to F \cdot \rho + \left(\frac{1-F}{2}\right) \cdot \mathbb{1}$, with F being the fidelity. Substituting F with δ the equation is given by $\rho \to (1-2\delta)\cdot\rho + \delta\mathbb{1}$. The secure key rate $r(\delta)$ is positive for $\delta < 0.0278$ which corresponds to a QBER Q of about 2δ.

The shortly sketched estimations about Eve's information and the secure key rates are just one possible example among plenty of techniques to proof unconditional security for

[17] One way post-processing, no pre-processing and optimal error correction is assumed.

[18] While the equations for the six state protocol are valid for a depolarizing channel, these results apply for more specific constraints. For more information it is referred to [56].

the introduced attacks. Considering now the most general approach, the coherent attack, Eve is basically able to treat the sequence of qubits sent by Alice as one quantum state. She is allowed to interact with this state according to quantum mechanics by unitary operations and applying ancilla states of arbitrary dimensions that are measured at an optional time. The basic approaches to such security proofs as well as to the previously mentioned cases are tightly discussed in the following pages.

Distillation of Entanglement

The presence of an entangled state between Alice and Bob ρ_{AB} is a sufficient criterion on which a security proof can be based on. The equation that denote Eves information and limits the QBER rate, as the ones derived on the previous pages, are an example of such a proof methodology. Depending on the noise, added either by the quantum channel or the respective hardware, bounds can be derived that determine the "amount" of post processing, especially privacy amplification, to erase an eavesdroppers remaining information. Theoretically as long as some amount of entanglement [19] is present between Alice and Bob unitary operations and LOCC can be applied locally by Alice and Bobs who can hereby restore sufficient fidelity to share an entangled state even in the presence of noise.

Universal Composability

The crucial point of this approach is to describe cryptographic protocols as part of a larger system that comprises several parts. The security of the whole system must not be compromised when information leaks in one of the subsystems. When for instance part of the secure key is given to the adversary, no information about the remaining key can be extracted from it. Starting from this concept the estimation of an eavesdroppers possible knowledge about a system and hence its security can be bounded by the distance of a perfectly secure, ideal system given an appropriate measure. In order to give a mathematical sound proof, the concept of a random, *two universal function* (variable) F has to be defined. The map F from $X \to Y$ is called two universal iff $Pr[F(x) = F(x')] \leq \frac{1}{|Y|}$, whereas $x, x' \in X$, with X and Y being random variables. Furthermore the mentioned distance measure, called *variational distance* in the classical case, between two probability distributions P and Q (mapping into the same range Y) is defined by $\delta(P,Q) := \frac{1}{2}\sum_{x\in X} |P(X) - Q(X)|$. This definition can be expanded to quantum states by taking a random variable S (denoting the secret key), a random state ρ and $\epsilon \geq 0$. S is said to be ϵ-secure iff $d(S,\rho) \leq \epsilon$. Here the distance between a random variable X and a random state ρ is taken, which is defined by $d(X,\rho) = \delta([\{X\} \otimes \rho], [\{U\}] \otimes [\rho])$, with U as a random variable with the same range as X, $\{X\} := |X\rangle\langle X|$ being the random variable X mapped onto a suitable Hilbertspace H with its dimension corresponding to

[19] At least for two qubit state an entanglement measure is given by the van Neumann entropy $S(\rho) = -\mathrm{Tr}(\rho ln(\rho))$.

the range of X. More precisely, when a probability space (Ω, P) is given, there exists a function from $\Omega \to S(H)$ with $S(H)$ being the set of all density operators on this Hilbertspace. This gives a probability distribution from a classical random variable to a the set density operators. Hence the previously used notation $[\rho]$ can be defined as $[\rho] := \sum_{\omega\in\Omega} = P(\omega)\rho(\omega)$, with $P(\omega)$ being the probability that an arbitrary $\omega \in \Omega$ is mapped to the state $\rho(\omega)$ and hence straightforward $[\{X\} \otimes \rho]$. The derived bound for this approach given a random variable Z with range z, a random state ρ and F being a two universal function, independent of ρ and Z, with domain z and range $S = \{0,1\}^s$ is proved to be

$$d(F(z)|F(z) \otimes \rho) \leq \frac{1}{2} 2^{-\frac{1}{2}(S_2([\{Z\}\otimes\rho]) - S_0([\rho]) - s)}, \tag{3.26}$$

with $S_\alpha(\rho)$ being the *Rényi entropy* of order α of ρ, $S_\alpha(\rho) := \frac{1}{1-\alpha} log_2\big(tr(\rho^\alpha)\big)$. For an exact proof it is referred to [57].

Twisted state

Asking about a necessary and sufficient condition for a secure key exchange the authors of [58] found an answer by introducing certain states, called *private states*. These are constructed in two subsystems of both parties, i.e. AA' for Alice and BB' for Bob, by $\gamma_{ABA'B'} = U \sum_{i=1}^{2^m} |ii\rangle \langle ii|_{AB} \otimes \rho_{A'B'} U^\dagger$, for m qubits acting on subsystem AB and with $\rho_{A'B'}$ being an arbitrary state in an auxiliary subsystem $A'B'$. The unitary operation U in the state is given by $U = \sum_{i,j}^{2^m} |ij\rangle \langle ij|_{AB} \otimes U_{ij}^{A'B'}$ and called *twist operation*. It turns out that a secure key exchange is possible whenever such private states can be distilled from Alice and Bob using LOCC operation. Furthermore it has been shown that even from a bound entangled state [20] a private state can be distilled. This implies that states that are used for a secure key exchange demand a more general approach than entanglement.

Apart from these well known approaches two other ideas that are rather neglected by the major community are shortly presented in the following. A security proof in [59] states that when two conjugate observables σ_x and σ_z are given, the ability to grow a common secure key in the basis σ_z corresponds to a common preparation of an eigenstate in the σ_z basis using additional sub-channels A', B', similar to the twisted state approach. Another interesting attempt to prove the unconditional security of a common key is to imply causality constraints imposed by the no-signaling theorem. It states that the exchange of information between parties that hold a shared entangled state is limited when a subsystem is measured. This preserves the space-like nature of the outcome of quantum observables with respect special relativity. Hence Eve's knowledge about the

[20] A state is called bound entangled when entanglement is used to create it but no pure entangled state can be distilled from it.

measurement outcome of her subsystem is bounded. A more precise description can be found in [60].

3.2.2 Continuous Variable (CV) QKD

Unlike in discrete variable QKD, where the measurement outcomes are limited to a countable finite set, as introduced in the previous chapters, CV QKD uses observables whose eigenvalues are elements of a continuous set, and are hence described by a continuous infinite Hilbert space. Around 15 years ago the first protocols employing weak coherent or squeezed signals were proposed. Their preparation and measurement was not using single quantum objects and single photon detectors as in discrete variable QKD but classic PIN detectors as commonly designed for telecom networks and pulses in the mW-range. Yet these pulses were sufficiently weak to obey quantum statistics and therefore offering the advantages of a secure key generation. Other than discrete variable protocols the security is hereby based on the uncertainty principle between the two non commuting quadrature operators $\hat{x}$ and $\hat{p}$ of the quantized electromagnetic field in the Volume V,

$$\vec{E} = \sum_j \sqrt{\frac{\hbar\omega_j}{2\epsilon_0 V}} \cdot \vec{e}_j \left(\hat{x}_j \cos(\vec{k}_j\vec{x} - \omega_j t) + \hat{p}_j^\dagger \sin(\vec{k}_j\vec{x} - \omega_j t) \right),$$

with $\vec{e}_j$ and $\vec{k}_j$ being the polarization and propagation vector, $\hat{x}_j = 2^{-1/2}(\hat{a}_j + \hat{a}_j^\dagger)$, $\hat{p}_j = 2^{-1/2} i(\hat{a}_j - \hat{a}_j^\dagger)$ and $\hat{a}_j^\dagger$, $\hat{a}_j$ being creation and annihilation operator of mode j. The operators obey the Bosonic commutation relations of two different modes of a state, k and l, $\left[\hat{a}_k, \hat{a}_l^\dagger\right] = \delta_{kl}$, $[\hat{a}_k, \hat{a}_l] = 0$ and $\left[\hat{a}_k^\dagger, \hat{a}_l^\dagger\right] = 0$. Early protocols [61] proposed to prepare a vacuum state that was first squeezed in $\hat{x}$ or $\hat{p}$ direction of the phase space and then afterwards displaced from the origin. An experimentally easier approach was found by using the so called *Gaussian States* as a source for QKD, as introduced in the following section. The well known and already in discrete QKD employed Coherent states are a subclass of such states. The reason why CV QKD is presented in this theses, although no direct result is connected with it, is the fact that, at the moment of writing, it is seen as one of the most promising candidates for the coexistence scheme, i.e. a possible integration of QKD into classical networks as for example described in [62]. Since CV-QKD is just on the edge of a classical signal it shows a high compatibility with hardware used in classical communication, such as PIN photodiodes instead of SPADs. A more elaborated discussion about a possible integration of QKD into networks is presented in chapter 6.

3.2.2.1 Gaussian States & Measurement

Phase space representation

Since the creation of squeezed states is an experimentally challenging task, another more convenient source was introduced by a protocol that proposed the use of Gaussian modulated coherent states [63]. As the name implies these states follow a Gaussian behavior when regarded by a quasi probability function in the phase space of $\hat{x}$ and $\hat{p}$. Since the mathematical description of Gaussian states with the usual quantum mechanical notation turns out to be rather complex due to continuous infinite operators, an alternative description with the so called *Symplectic group structure* in an $\mathbb{R}^{2N}$-dimensional vector space with the Symplectic form $\mathbf{\Omega} = \oplus_{k=1}^{N}\omega_k = \begin{pmatrix} \omega_1 & 0 & 0 & \cdots & 0 \\ 0 & \omega_2 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & 0 & \omega_{N-1} & 0 \\ 0 & \cdots & 0 & 0 & \omega_N \end{pmatrix}$, with $\omega_k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, written as $\Gamma = (\mathbb{R}^{2N}, \mathbf{\Omega})$ is favored. Elements of the space Γ, such as the vector representing a Bosonic 2N-mode quantum state that comprises the pairwise sorted annihilation and creation operators, $\boldsymbol{R} = (\hat{x}_1, \hat{p}_1, \cdots, \hat{x}_N, \hat{p}_N)^T$, are in the following denoted by bold letters. This notation allows to summarize the 2N commutation relations of the quadrature operators by $[\boldsymbol{R}_i, \boldsymbol{R}_j] = \mathbf{\Omega}_{ij}$, with $i,j \in \{1, 2, ..., 2N\}$. The classical notation of a (2N-dimensional) state in the Hilbertspace $\mathbb{H} = \otimes_{k=1}^{2N}\mathbb{H}_k$ that comprises all statistical information is given by the density operator ρ. The representation in phase space replaces ρ by the so called *s-ordered characteristic function* $\chi_\rho^s(\boldsymbol{\xi}) = Tr[\rho\hat{D}(\boldsymbol{\xi})]e^{s\|\boldsymbol{\xi}\|^2/2}$, with $\hat{D}(\boldsymbol{\xi}) := e^{i\boldsymbol{R}^T\mathbf{\Omega}\boldsymbol{\xi}}$ and $\boldsymbol{\xi} \in \Gamma$ with $\|\cdot\|$ being the Euclidean norm on Γ. For $s = 0$ [21], the Fourier transform of the characteristic function gives the distribution for the eigenvectors $\boldsymbol{r}$ of $\boldsymbol{R}$ (that form a basis in $\mathbb{R}^{2N}$ and Γ, respectively) with the so called normalized *Wigner function*

$$W(\boldsymbol{r}) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\boldsymbol{\xi}}{(2\Pi)^{2N}} e^{-\boldsymbol{r}^T\mathbf{\Omega}\boldsymbol{\xi}}\chi_\rho^0(\boldsymbol{\xi}). \tag{3.27}$$

The first and the second statistical moments of this distribution are hereby sufficient to give a precise definition of Gaussian states in the phase space and due to the presented homomorphism also in Hilbert space. Figure 3.8 represents the most important Gaussian states in the Phase space diagram.

The first moment corresponding to a state $\rho \in \mathbb{H}^{2N}$ is given by the so called *displacement*

[21] The ordering, s, of the characteristic function denotes the sequence of creation and annihilation operators and leads to different quasi-distribution functions. The symmetrical ordering, here given by $s = 0$ refers to the Wigner distribution, whereas $s = -1$ and $s = 1$ lead to the Husimi Q-function and P-representation, respectively.

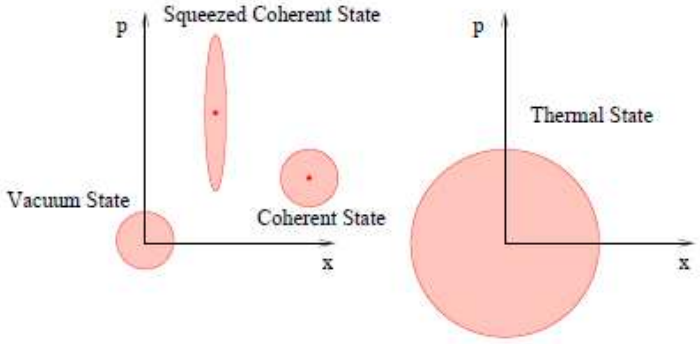

FIGURE 3.8: Different Gaussian States represented in the phase space diagram. An arbitrary coherent state shows the statistical behavior of a displaced vacuum state. A squeezed state is gained by applying the squeezing operator onto a coherent state. When measuring the amplitudes x or p a Gaussian distribution with displaced origin and squeezed variance is observed. The phase space on the right shows the statics of a thermal state. Source: [8]

vector $\boldsymbol{d}$, defined as $\boldsymbol{d}_j = \langle \boldsymbol{R}_j \rangle_\rho = Tr(\boldsymbol{R}_j \rho)$. The second moment is called the *covariance matrix* $\boldsymbol{\sigma}$, given by $\boldsymbol{\sigma}_{ij} = \langle \boldsymbol{R}_i \boldsymbol{R}_j + \boldsymbol{R}_j \boldsymbol{R}_i \rangle_\rho - 2 \langle \boldsymbol{R}_i \rangle_\rho \langle \boldsymbol{R}_j \rangle_\rho$. When the first moment is regarded as the mean value of ρ, the second moment quantifies the corresponding variance and is bounded by the uncertainty relation $\boldsymbol{\sigma} + i\boldsymbol{\Omega} \geq 0$. For the Gaussian state $|0\rangle$, the vacuum state, $\boldsymbol{d} = \boldsymbol{0}$ and the covariance matrix $\boldsymbol{\sigma}(\hat{x}) = \boldsymbol{\sigma}(\hat{p}) = \boldsymbol{\sigma} = \mathbb{1}$ has minimal variance. This is usually referred to as the *vacuum noise* or *quantum shot noise*. Another important example is the single mode coherent state $|\alpha\rangle_k$, whose moments read $\boldsymbol{d} = \sqrt{2}\big(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)\big)^T$ and $\boldsymbol{\sigma} = \mathbb{1}$.

Written in terms of a statistical multi-variate Gaussian function [22], that satisfies a Gaussian distribution, a sound mathematical definition of a Gaussian state is hence obtained by the previously introduced characteristic function $\chi(\rho)$ in dependence of these statistical moments,

$$\chi_\rho(\boldsymbol{\xi}) = e^{\frac{1}{4}\boldsymbol{\xi}^T \boldsymbol{\Omega}\boldsymbol{\sigma}\boldsymbol{\Omega}^T \boldsymbol{\xi} - i(\boldsymbol{\Omega}\boldsymbol{d})^T \boldsymbol{\xi}} \tag{3.28}$$

and its corresponding Wigner function

$$W_\rho(\boldsymbol{X}) = \frac{1}{\pi^N} \frac{1}{\sqrt{\det(\boldsymbol{\sigma})}} e^{-(\boldsymbol{X}-\boldsymbol{d})^T \boldsymbol{\sigma}^{-1} (\boldsymbol{X}-\boldsymbol{d})}, \tag{3.29}$$

with $\boldsymbol{\xi}$ and $\boldsymbol{X}$ being vectors in $\mathbb{R}^{2N}$.

Gaussian Unitaries

In order to characterize special Gaussian states that are used as sources for QKD, a

[22] A multi-variate Gaussian function is of the form $f(\vec{x}) = C \cdot exp(-\frac{1}{2}\vec{x}^T \mathbf{A} \vec{x} + \vec{b}^T \vec{x})$, with $\vec{x}$, $\vec{b} \in \mathbb{R}^{2N}$ and $\mathbf{A}$ being an $2N \times 2N$ positive definite matrix.

certain class of operators, called *Gaussian Unitaries* $\boldsymbol{S}$, have to be considered. They represent maps that preserve the Gaussian statistic of a Gaussian state. It can be shown (see e.g. [64]) that this condition coincides with $\boldsymbol{S\Omega S}^T = \boldsymbol{\Omega}$, $\boldsymbol{S}$ is hereby called Symplectic. In analogy to the homomorphism $\mathbb{H} \to \Gamma$ of $\rho \to (\chi_\rho, W_\rho)$ an unitary operator U can be mapped to the phase space by a corresponding Gaussian unitary $\boldsymbol{S}$ and a translation operator $\boldsymbol{\delta}$ acting on the first and second moment of the distribution, i.e. $\boldsymbol{d} \to \boldsymbol{Sd} + \boldsymbol{\delta}$ and $\boldsymbol{\sigma} \to \boldsymbol{S\sigma S}^T$. When such an operator can be expressed in matrix form, a diagonal form just like in normal Hilbertspace can always be achieved with corresponding eigenvalues $1 \leq \nu_k < \infty$. Similar to the Hilbertspace notation, pure and mixed states can be distinguished in this notation. The respective description in Hilbert and Phase space is compared and summarized in Table 1, taken from [65].

Property	**Hilbert Space**	**Phase Space** Γ
Dimension	∞	2N
Structure	$\otimes$	$\oplus$
state description	ρ	$\boldsymbol{d}, \boldsymbol{\omega}$
constraint	$\rho \geq 0$	$\boldsymbol{\sigma} + i\boldsymbol{\Omega} \geq 0$
Unitary operator	$U^\dagger U = 1,\ \rho \to U\rho U^\dagger$	$\boldsymbol{S\Omega S^T} = \boldsymbol{\Omega},\ \boldsymbol{d} \to \boldsymbol{S} \cdot \boldsymbol{d},$ $\boldsymbol{\sigma} \to \boldsymbol{S\sigma S^T}$

TABLE 3.1: Comparison between Hilbert space and phase space for N-mode Gaussian states.

The most important Gaussian unitaries for QKD are phase rotations and beamsplitter transformations as well as the *squeezing operator*, $\hat{S}(s, \varphi)$, and the *displacement operator*, $\hat{D}(\alpha)$. The latter is defined (on the Hilberspace) by $\hat{D} = e^{(\alpha\hat{a}^\dagger - \alpha^*\hat{a})}$ and its effect on the Fock vacuum state, $\hat{D}\,|0\rangle = |\alpha\rangle$, with $|\alpha\rangle$ being a coherent state as defined in Eq. (3.1) and with $\alpha \in \mathbb{C}$ being the eigenvalue of the annihilation operator with respect to the eigenvector $|\alpha\rangle$, $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$. The application of the squeezing operator, defined as $\hat{S}(r) = \exp\left[\frac{1}{2}\left(r(\hat{a}^\dagger)^2 - r^*\hat{a}^2\right)\right]$, with $r = s \cdot e^{i\varphi}$ denoting the squeezing degree by $s \in \mathbb{R}^+$ and φ being the squeezing phase, results in an elliptical distribution as well as a rotation of a previously circular distributed coherent state in the phase space. A Gaussian state, $|\Phi\rangle$, usable for CV QKD comprises a displacement as well as a squeezing operation, $|\Phi\rangle\,(\alpha, r)_{\text{Gaussian}} = \hat{D}(\alpha)\hat{S}(r)\,|0\rangle$.

Figure 3.9 denotes its visualization in the phase space [23].

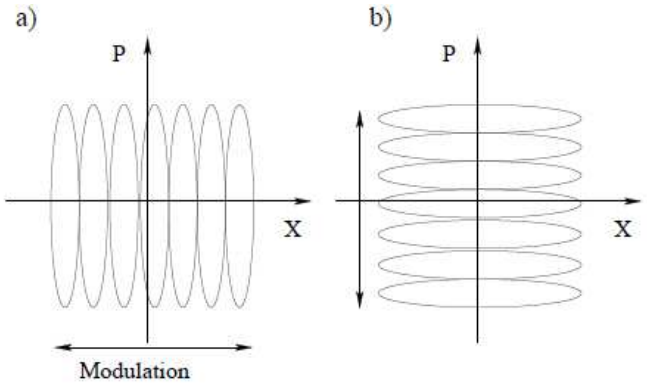

FIGURE 3.9: The two plots show squeezing and displacement operators applied in x and p direction of the phase space. Source: [8]

For more detailed and broad introduction into Gaussian states it is referred to [65] or [64].

Heterodyne Measurement

In order to measure the quadratures of a prepared state the so called balanced homodyne detection technique is used. Before explaining these scheme in more details the more general measurement technique of heterodyne detection is shortly introduced. The setup of heterodyne detection comprises a beam splitter that combines an incoming signal wave (S) with a reference wave, the so called local oscillator (LO), and two PIN detectors that measure the intensity at the respective exits. Assuming the simple classically approach that the two waves before and after the beam splitter are given by $\begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} t_1 & r_2 \\ r_1 & t_2 \end{pmatrix} \cdot \begin{pmatrix} E_{S,in} \\ E_{LO,in} \end{pmatrix}$, with $E_i = E_i e^{i(\omega_i t + \phi_i)}$. Furthermore the respective intensities $I = |E|^2$ at the two outputs are calculated to be

$$I_{Out1} = t_1^2 E_S^2 + r_2^2 E_{LO}^2 + 2 r_2 t_1 \, |E_S| \, |E_{LO}| \cos\big((\omega_S - \omega_{LO})t + (\phi_S - \phi_{LO})\big) \tag{3.30}$$

$$I_{Out2} = r_1^2 E_S^2 + t_2^2 E_{LO}^2 - 2 r_1 t_2 \, |E_S| \, |E_{LO}| \cos\big((\omega_S - \omega_{LO})t + (\phi_S - \phi_{LO})\big), \tag{3.31}$$

considering the phase shift of the beam splitter (π) by applying the minus sign at r_1 and assuming that the amplitudes E_i are real. A photo diode placed at either output of the beam splitter allows a measurement of the enhanced signal amplitude E_S and, more importantly, of the phase ϕ_S with respect to the phase of the local oscillator ϕ_{LO} [24]. The intensity at both outputs varies in time with the difference frequency $\omega_D = (\omega_S - \omega_{LO})$.

[23] According to their statistical behavior in the quadrature basis coherent states can be seen as a special sup-group of Gaussian states and are due to the easy preparation the first choice of an experimental realization.

[24] The first two constant terms of Eq. 3.30 and 3.31 are hereby neglected

Depending on this frequency, the measurement is said to be *heterodyne* ($\omega_D \neq 0$) or *homodyne* ($\omega_D = 0$).

Homodyne Measurement

In the case of homodyne detection the signal is, at least theoretically, time independent. The difference of the two intensities $I_{Out1} - I_{Out2}$ can be derived when each output of the beam splitter is measured. In this case a further increased signal amplitude from both cross-terms as well as an accurate signal phase can be determined and a reconstruction of the input signal with an even higher signal to noise ratio is achieved. Heterodyne and homodyne measurements are often depict in *shot-noise* units, which indicates the maximal possible accuracy of the measurement. The shot-noise is received by using vacuum instead of the local oscillator signal on the second input of the beam splitter. The intensity difference corresponds in this case to intrinsic fluctuations of the input signal.

The measurement used for CV-QKD employs a beam splitter that distributes incoming light equally, i.e. $t_1 = t_2 = r_2 = \frac{1}{\sqrt{2}}$ and $r_1 = -\frac{1}{\sqrt{2}}$. This is called *balanced homodyne* detection and allows a direct measurement of either quadrature operator $\hat{X}_1$ or $\hat{X}_2$. A heuristic explanation can be extracted from the fact that the measured intensity difference corresponds to the difference of the number operators $\Delta\hat{n} = \hat{n_1} - \hat{n_2}$ of the states. The measured intensity reflects the distribution of this difference, i.e. $W(\Delta\hat{n})$, with W being the Wigner distribution function in phase space. The resulting statistic can be shown to coincide with the distribution of an operator that is equal to the quadrature operator (up to a constant). The complete mathematical proof can for example be found in [66]. An easier way to show this without employing quantum statistics, is to calculate the difference of the two outcomes after the $50:50$ beam splitter. When $\hat{a}_S$ and $\hat{a}_{LO}$ ($\hat{a}_S^\dagger$ and $\hat{a}_{LO}^\dagger$) denote the annihilation (creation) operators of the two inputs and $\hat{b}_1, \hat{b}_2$ ($\hat{b}_1^\dagger, \hat{b}_2^\dagger$) the two modes at the outputs, the respective transformation at the beam splitter is given by

$$\begin{pmatrix} \hat{b}_1 \\ \hat{b}_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \hat{a}_S \\ \hat{a}_{LO} \end{pmatrix}. \tag{3.32}$$

The intensity difference measured by homodyne detection is hence proportional to the difference of the respective number operators, $\hat{n}_1 := \hat{b}_1^\dagger \hat{b}_1$ and $\hat{n}_2 := \hat{b}_2^\dagger \hat{b}_2$, i.e. $\Delta\hat{n} = \hat{n}_1 - \hat{n}_2$. Using the relations in Eq. 3.31, the difference $\Delta\hat{n}$ in terms of input signals can be expressed as $\Delta\hat{n} = \hat{a}_S^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_S$. Assuming now a semi-classic approach with the strong local oscillator signal given by $\hat{a}_{LO} \to |a_{LO}|\, e^{i\Delta\varphi}$, with $\Delta\varphi$, the difference-intensity operator reads

$$\Delta\hat{n} = |a_{LO}|\, e^{i\Delta\varphi}(\hat{a}_S^\dagger + e^{-2i\Delta\varphi}\hat{a}_S). \tag{3.33}$$

For $\Delta\varphi = 0$ and $\Delta\varphi = \frac{\pi}{2}$ $\Delta\hat{n} \propto \hat{X}_1$ and $\Delta\hat{n} \propto \hat{X}_2$, respectively. Hence a direct measurement of the quadrature operators is given.

3.2.2.2 Protocols, Post-Processing and Attacks

Similar to discrete variable QKD, various types of protocols evolved that differ either in the preparation or the measurement of the states. The usage of coherent or squeezed states as well as heterodyne or homodyne detection characterizes most of them already during the quantum stage. In addition to this the post processing of CV-QKD schemes is an ongoing issue in current protocols. Two possible ways, called *direct* and *reverse reconciliation*, are distinguished. While in direct reconciliation Bob announces his results to Alice, who continues with sifting and error estimation, reverse reconciliation swaps the role of Alice and Bob, i.e. Alice announces her prepared states and Bob proceeds with the post processing stage. With respect to these approaches a rough classification of CV-QKD protocols can be given.

Squeezed-state protocols

The first squeezed state protocol was introduced in 2001 by [61] and employed Gaussian states that were randomly squeezed and displaced from the origin of phase space by a real value number a. In order to realize this Alice extracts this number a randomly from a Gaussian distribution of variance V_a and mean 0. Similarly the squeezing of the quadrature is randomized by applying a phase shift $\varphi = u\frac{\Pi}{2}$ on the state with a randomly chosen $u \in \{0, 1\}$. Subsequent averaging of the output states over a Gaussian distribution conserves the attributes of a thermal state with equal variance V for $u = 0$ and $u = 1$ in order to close a possible information leakage to Eve. Bob can now either use homodyne or heterodyne measurement to receive a value correlated to Alice's shift a. Direct as well as reverse reconciliation versions of squeezed state protocols exist.

Coherent state protocol

This protocol, first proposed in [63], uses the experimentally easiest way to create Gaussian states, namely coherent states. Alice extracts two real random variables a_x and a_p from a Gaussian distribution with mean value 0 and variance V_a. The pair (a_x, a_p) is subsequently encoded into a coherent state by shifting it to the respective position in the phase space (see e.g. the coherent state in Figure 3.8). After the state is sent over the quantum channel, Bob randomly picks either the $\hat{x}$ or $\hat{p}$ quadratures for homodyne detection, ending with a result b. This process is repeated until a sufficient amount of data is collected. The obtained results b are hence correlated with (a_x, a_p). Via direct reconciliation Bob reveals his measurement choices ($\hat{x}$ or $\hat{p}$) to Alice who, with respect to this information, either keeps a_x or a_p and eventually ends up with a string matching Bobs results b.

No-switching Protocol

This protocol was proposed two years after the coherent state protocol, in 2004 [67]. It adopted the state preparation process of the previous protocol, however saw that one of two created variables a_x or a_p is eventually discarded. By replacing homodyne with heterodyne detection, Bob is able to measure both quadratures at the same time, however, with the penalty of a higher variance. Still the authors showed that with appropriate post processing two matching and secure key strings, (a_x, a_p) and (b_x, b_p), can be extracted and hence a higher key rate. The switching of Bob between the two quadrature is not required in this scheme.

Entanglement based description of CV-protocols

Similar to the discrete variables the mathematical description of the introduced protocols can be united by an entanglement scheme, where Alice holds an EPR state $|V\rangle_{A',A}$ with variance V. During the quantum stage she sends one mode A to Bob, while measuring the other A' with respect to both quadratures using homodyne detection with the vacuum state as the local oscillator and the beamsplitter transmitivity τ_A. In the process of this measurement Bob's mode A is projected onto a Gaussian state with the first moment $\boldsymbol{d} = (\gamma_x x_A, \gamma_p p_A)$ and the covariance matrix $\boldsymbol{\sigma} = \mathrm{diag}(q^{-1}, q)$, with $q = \frac{(1-\tau_A)V+1}{V+1-\tau_A)}$, $\gamma_x = \frac{\sqrt{\tau_A(V^2-1)}}{\tau_A V+1-\tau_A}$ and $\gamma_p = \frac{\sqrt{(1-\tau_T)(V^2-1)}}{(1-\tau_A)V+\tau_A}$. Depending on τ_A, Bob receives a coherent or squeezed Gaussian state and applies in the same manner on his side either a homodyne or heterodyne (again with the vacuum state as local oscillator) detection. The postprocessing stage is equal to the previous protocols.

Postselection Protocol

This type of protocol, first suggested by [68], finds a way to overcome the 3dB loss limit. Since direct reconciliation is not able to generate a secure key when more than 50% of the data is assumed to be accredited to Eve, reverse reconciliation as well as the here introduced postselection protocol are able to achieve higher noise tolerance and hence longer distance. The quantum stage is equal to the coherent state protocol. After Bob announced his measured quadrature (here homodyne detection is assumed) Alice publicly gives her absolute values of her prepared quadrature $|a_x|$ and $|a_p|$, respectively. According to these results Bob can now estimate the mutual information between Alice and him, $I(A:B)$, as well as Alice and Eve $I(A:E)$, and deduces, depending on the parameters of the transmitted coherent states, possible values for which $I(A:B) > I(A:E)$ and the resulting key rate is positive. According to these calculation certain states are discarded or kept. This type of protocol has shown to be possible in combination with the no-switching protocol yielding higher key rates.

Discrete modulation protocols

Unlike the previously introduced protocols, in the discrete modulation scheme Alice does

not select an amplitude a from a Gaussian distribution but randomly chooses the respective state from a given discrete set. In [69], for example, a two and four state modulation protocol is introduced. The distribution of the states in phase space is shown in Figure 3.8. Similar to the previous protocol the choice of homodyne or heterodyne detection as well as direct or reverse reconciliation allows different variations of this protocol.

3.2.2.3 Security Proofs & Key Rates

Security Proofs and Attacks

Since CV-QKD protocols are not a major topic of this thesis, this section will only give a quick overview about the concept of the mathematical proof of security and refer to the respective papers for further readings. As stated in section 3.2.1.4, an attack can be divided into an individual, collective or coherent scenario depending on the eavesdropper's possibilities. Since the concepts of security proofs presented in this previous chapter can in general not be simply transferred to an infinity Hilbert space, only the concept of universal composability and the related definition of ϵ-security (also defined in 3.2.1.4) has been successfully transferred to the continuous regime [70]. As this first attempt of proofing unconditional security for CV-QKD succeeded only for individual and collective attacks, another issue arose due to the false assumption that the number of exchanged signals between Alice and Bob are infinite. As it turned out the so called *finite size* analysis has to be applied to adapt security proofs and key rates to the fact that only a finite number of signals is exchanged during the quantum stage. At the time of writing promising efforts in expanding security proofs to the most general case, namely a coherent Gaussian state protocol with heterodyne detection and reverse reconciliation under the aspect of a general, coherent attacks with finite size analysis have been made in [71], [72] or [73].

Key Rate

The secure key rate r (or achievable range) is, equally to equation 3.17 in the discrete variable case, given by $r = \varphi\big(I(A:B) - I(X:E)\big)$, with $I(X:E)$ being the Holevo bound comprising X which represents either A(lice) or B(ob) depending on direct or reverse reconciliation. The factor φ denotes the no switching ($\varphi = 1$) or homodyne detection case ($\varphi = 1/2$). By respecting finite size keys with a total number of N exchanged signals and a correction term $\Delta(n)$, depending on the n signals that are used to establish a key, as well as a further deduction $D(n)$ due to collective instead of coherent attacks, a more realistic key rate can be defined as

$$r = \frac{\varphi n}{N}\big\{\beta I(A:B) - S_{\epsilon PE}(X:E) - \Delta(n) - D(n)\big\}. \tag{3.34}$$

Additionally a reconciliation factor β between Alice and Bob's mutual information $I(A:B)$ is introduced. A more detailed deduction of this equation is found in [74]. In order to give a more concrete example the key rate of a fully Gaussian protocols as introduced in the previous section is investigated more closely considering a collective attack. In this scheme a lossy quantum channel with transmission factor τ as well as the excess noise $\eta := \frac{2\bar{n}(1-\tau)}{\tau}$, with thermal number $\bar{n}$, is considered. The excess noise denotes the ratio of noise from Bob to Alice. Considering here only the terms of Eq. 3.17 the mutual information between Alice and Bob $I(A:B)$ is here given by

$$I(A:B) = \varphi \log\Big[\frac{V+\eta}{\eta+\lambda V^{-1}}\Big]. \tag{3.35}$$

The associated covariance matrix for the state shared by Alice and Bob reads hereby $\boldsymbol{\sigma}_{AB} = \begin{pmatrix} x\mathbb{1} & z\boldsymbol{Z} \\ z\boldsymbol{Z} & y\mathbb{1} \end{pmatrix}$, with $\boldsymbol{Z} = \mathrm{diag}(1,-1) \in \mathbb{R}^2$ $x = V$, $y = \tau(V+\eta)$ and $z = \sqrt{\tau(V^2-1)}$ given the state's thermal variance V. Using these values obtained from this matrix as well as $\lambda = V$ for coherent or $\lambda = 1$ for squeezed states together with Eq. 3.35 the mutual information is derived.

The calculation of the Holevo information shared between Alice/Bob and Eve $S(X:E) = S(E) - S(E|X)$ is, however, not as straightforward. Eve's van Neumann entropy equals the purfied shared state between Alice and Bob, hence $S(E) = S(AB)$. With $S(AB)$ being the entropy of the Symplectic eigenvalues ν_k of $\boldsymbol{\sigma}_{AB}$, $S(\nu(\boldsymbol{\sigma}_{AB}))$ [25]. The mutual information between Eve and Alice/Bob, $S(E|X)$ is derived in the same way but with the partially measured covariance matrix $\boldsymbol{\sigma}_{E|X}$. In order to define such a partial measurement it has to be noted that the covariance matrix of each two mode Gaussian state can be written in the form $\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B} \end{pmatrix}$ with $\boldsymbol{A}$, $\boldsymbol{B}$ and $\boldsymbol{C}$ being $2x2$ real valued matrices, fulfilling $\boldsymbol{A} = \boldsymbol{A}^T$ and $\boldsymbol{B} = \boldsymbol{B}^T$. The remaining matrix in subsystem A after partial measurement of subsystem B is given by

$$\boldsymbol{\sigma}_{AB|B} = \boldsymbol{A} - \boldsymbol{C} B_{11}^{-1} \boldsymbol{\Pi} \boldsymbol{C}^T, \tag{3.36}$$

with B_{11} being the first element of matrix $\boldsymbol{B}$ and $\boldsymbol{\Pi} = \mathrm{diag}(1,0)$. In this special case $\boldsymbol{\sigma}_{E|X} = \boldsymbol{\sigma}_{AB|X} = x\mathbb{1} - yz^2\boldsymbol{Z}^2$.

Security Proofs and Attacks

Some promising experiments have been carried out during the last 10 years, found e.g. in [75], [76] or [77]. The most prominent and recent example was published 2013 in Nature Photonics [78]. Since a more detailed review of the experimental realizations is beyond

[25] The von Neumann entropy $S(\rho)$ can be decomposed using the Symplectic eigenvalues ν_k of a state ρ by $S(\rho) = \sum_{k=1}^{N} g(\nu_k)$ with $g(\nu) = \frac{\nu+1}{2}\log(\frac{\nu+1}{2}) - (\frac{\nu-1}{2})\log(\frac{\nu-1}{2})$

the scope of this document, the reader is invited to follow the respective citations for more information on this matter.

Chapter 4

Satellite Based QKD

4.1 Single Photon Sources

Satellite Based QKD is a promising approach to expand the range of QKD towards a secure long haul key exchange. Therefore it is considered to primarily serve as a secure earth to satellite and earth to earth link, respectively. The transmitted signal has to be chosen according to the atmospheric composition and its influence on electromagnetic radiation. The graph in Figure 4.1 shows the opacity of the atmosphere with respect to wavelength radiation. The common wavelength region for QKD, i.e. for single photon creation, lies between 400nm and 1600nm. The bottom inset of Figure 4.1 shows a more detailed transmittance in this region.

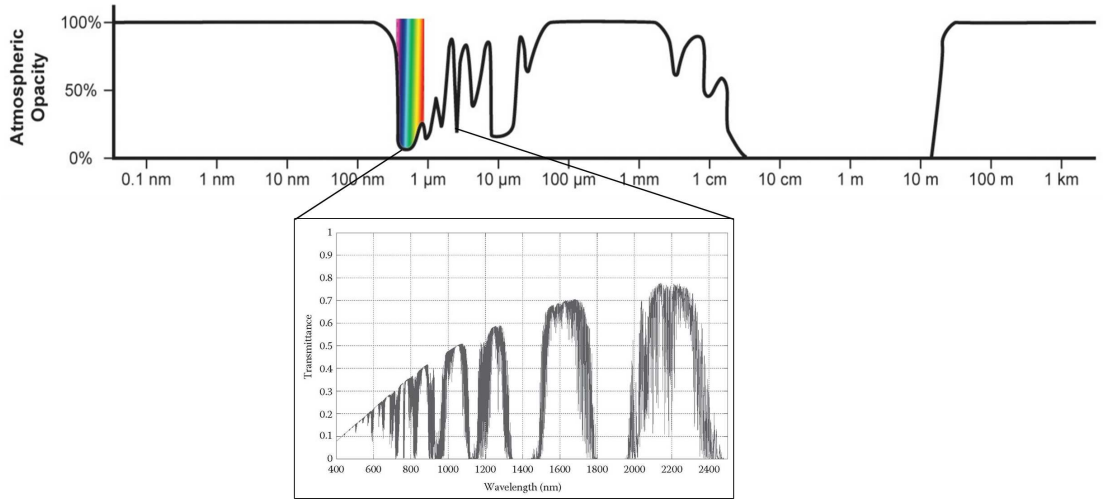

FIGURE 4.1: Atmospheric Opacity. Inset taken from [9]

Although the atmospheric conditions favor visible wavelengths, C-Band signals are a considerable alternative due to their compatibility with telecommunication standards.

Apart from the wavelength selection, a suitable single photon source for space applications has to be chosen. The decision process is evaluated in more detail in [10] and summerized in the following. The graphic of Figure 4.2 denotes an overview of current single photon creation techniques that are able to emit light in this (and also other) wavelength regions. It is divided into spontaneous and deterministic generation, whereas so far the only known deterministic sources are quantum dots, a technology that is, at the moment of writing, not mature for remote long haul transmissions.

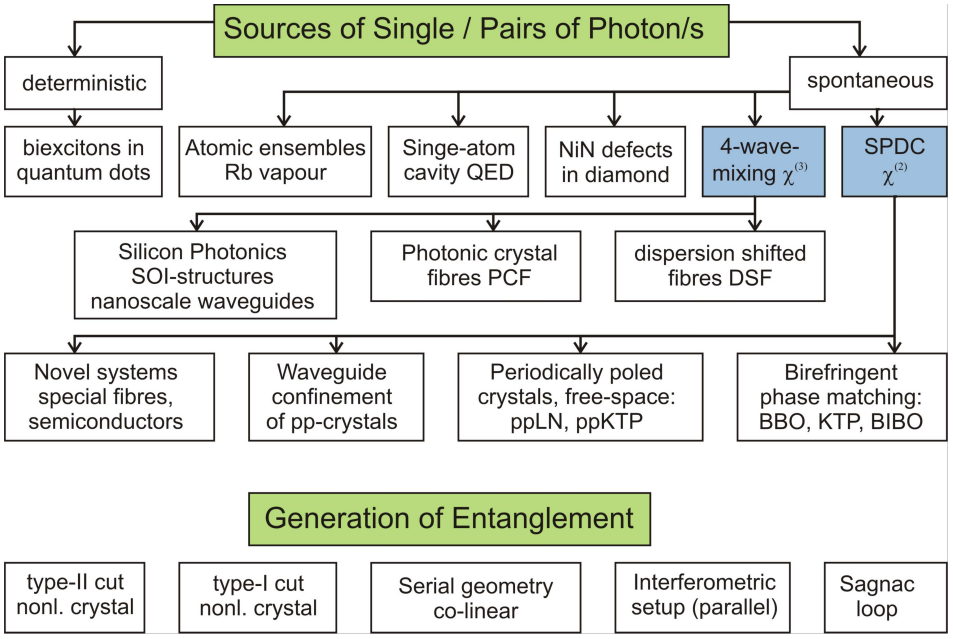

FIGURE 4.2: Techniques for single photon creation. Source: [10].

The blue colored boxes in Figure 4.2, i.e. four wave mixing and SPDC, denote all optical approaches that are mostly used for QKD, especially for entanglement based systems due to their simplicity. As already mentioned briefly in section 3.2.1.3, where the mathematical background of SPDC was introduced, different types and geometries are possible in this case, as it is shown in more detail in the five different boxes for generating entanglement in the lower part of Figure 4.2. Since four wave mixing processes in fibers or waveguides are promising, but not yet well established methodes, their performance in photon pair rates as well as quality of entanglement is so far not comparable to birefringent SPDC crystal sources. These, on the other hand, can be further divided into bulk setups employing either BBO, KTP or BIBO crystals, that fulfill the eligible phase matching (PM) condition due to length and temperature. Another more recent approach of waveguide based SPDC utilizes periodical poling to achieve quasi phase matching (QPM). Here periodically poled Lithium Niobate (ppLN) or Titanyl Phosphate (ppKTP) are well established candidates. Although KTP is the most used material and therefore a well known technology when it comes to generating entanglement with high

rates and high visibility, it lacks the possibility of smooth integration into existing optics and its miniaturization is limited due to its development for free space setups. Therefore a waveguide based LN single photon pair source offers more stability and flexibility for space applications due to its integrated design on chip. The generation rates of single counts for LN sources are even higher compared to bulk setups, see e.g. [79] (type I) or [80] (type II) , whereas these publications show that the challenging part of these setups is to accomplish a similar quality of entanglement, i.e. convert the single to coincidences and eventually in a high visibility. The problem is on the one hand the high losses within the waveguide on the other hand the broad spectral bandwidth of the generated pairs. As LN is already a well known material for electro- and acusto-optical devices in the field of classical telecommunication, its maturity in terms of fabrication also favors such a waveguide over a KTP based source. In the following the fabrication procedure as well as the theoretical properties of such a LN based entangled photon pair source are stated. All theoretical models and fabrication techniques of such an LN source that are presented in the upcoming chapter have been adopted from the University Paderborn and are taken from [11], an unpublished deliverable. Similar published versions can be found e.g. in [79], [81] or [82] and other sources.

4.1.1 Two Generations of entanglement base Ti:$LNbO_3$ waveguide sources

The Manufacturing Process

The first step towards an integrated entanglement source is the fabrication of a low loss waveguide structure that supports all polarization modes, i.e. TE and TM, equally. In our case a Titanium indiffused waveguide structure was fabricated by the university Paderborn with an expected loss budged below 0.1dB per cm. However, it has to be noted that ordinary and extraordinary polarized beams have slightly different behavior. It can be calculated by Fick's Law, used with the parameters introduced in the following, that the refractive index of the extraordinary waveguide depends linearly on the indiffused Titanium concentration while the refractive index of the ordinary beam shows stronger nonlinear dependance. This affects also the dispersion of the respective modes. This theory has been confirmed in experimental setups, as it is shown in Figure 4.3. These two pictures shown below are calculated intensity distribution for TE and TM mode, respectively, while the corresponding experimental results are shown below.

The fabrication steps of the waveguide itself are depict in Figure 4.4. A layer of approximately 100nm of Titanium is applied on a 0.5mm LN substrate that is reduced to a 7μ m stripe using a layer of photolack. The substrates are applied using e-beam evaporation or sputtering techniques while the removal is done by contact photolitography in the case of photolack or otherwise by etching and organic solvents. The final indiffusion

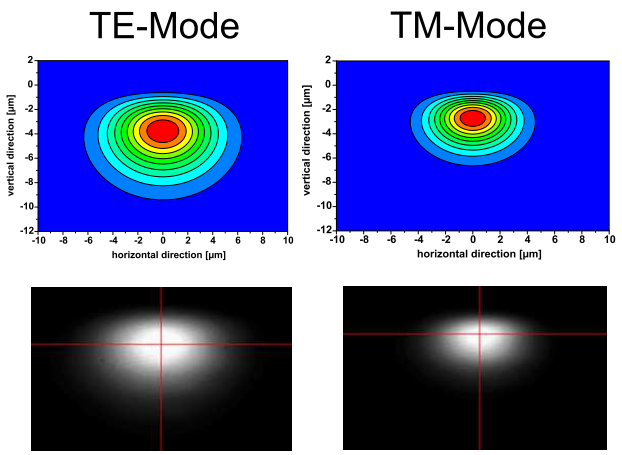

FIGURE 4.3: TE and TM mode of the Ti:LN waveguide. The differences are due to slightly different behavior of the refractive index for ordinary and extraordinary beam. Source: [11].

of the Titanium to form the optical waveguides is achieved by heating the sample to $1090°C$ degree for 9 hours.

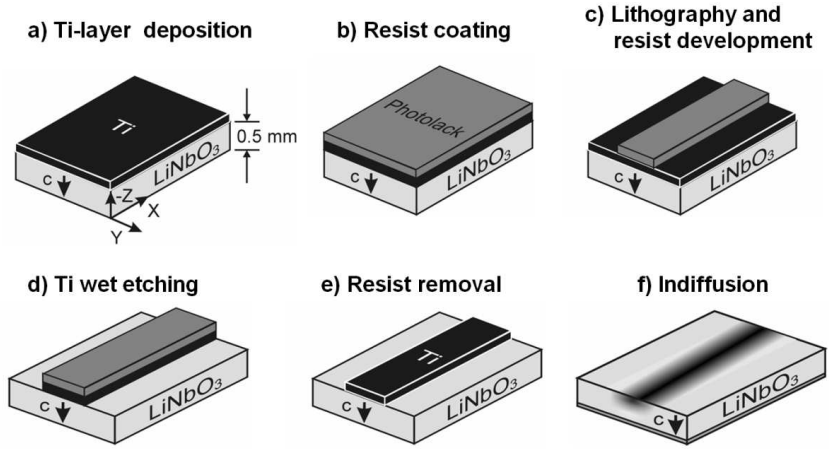

FIGURE 4.4: Steps for fabrication of Titanium indiffused Lithium Niobate waveguide structure. Source: [11].

Quasi Phase Matching and Entanglement

In order to create polarization entangled states at a high rate the phase matching condition has to be fulfilled. Since this source employs quasi phase matching, a periodic poling pattern Λ_1 is used to receive a high rate of orthogonally polarized photon pairs at two different wavelengths λ_s and λ_i. A second poling pattern Λ_2 is used to create a second photon pair according to its respective phase matching curve. This concept is shown in Figure 4.7, while schematics of the corresponding QPM curves are shown in Figure 4.5. This picture shows furthermore that at a certain pump wavelength (here about 775nm) signal and idler wavelengths of each QPM curve coincide. This means

that for a polarized signal photon of wavelength λ_1 generated by the first QPM curve at Λ_1 (blue curve in 4.5) an orthogonally polarized idler photon of the same wavelength λ_1 is created by Λ_2 (red curve). the same holds for the idler photon of the first QPM curve Λ_1 and the corresponding signal photon of Λ_2. These two photon pairs, indicated by the green dots in Figure 4.5, yield the maximally entangled Bell state $|\Psi^+\rangle$ up to a relative phase φ, originating from the difference in the refractive indices for TE and TM modes, $\Psi^+ = \frac{1}{\sqrt{2}}\big(|H\rangle_{\lambda_1}|V\rangle_{\lambda_2} + e^{i\varphi}|V\rangle_{\lambda_1}|H\rangle_{\lambda_2}\big)$. For the experimentally received state, best written as $\Psi^+_{\text{real}} = \frac{1}{\sqrt{M}}\big(\alpha|H\rangle_{\lambda_1}|V\rangle_{\lambda_2} + \beta e^{i\varphi}|V\rangle_{\lambda_1}|H\rangle_{\lambda_2}\big)$ with false pair generations already neglected, attenuation parameters α, β as well as the normalization value M are determined by the individual properties of the respective waveguide. Due to material properties the operation point, i.e. the pumping wavelength and hence the signal and idler wavelength, can be tuned by several 10th of nm by adjusting the temperature of the waveguide, as it is the case for all crystal sources.

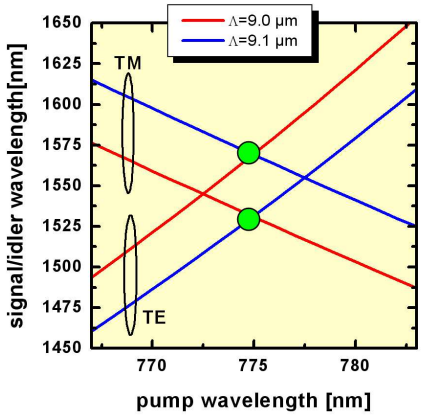

FIGURE 4.5: Two QPM curves for different pump, signal and idler wavelength. Source: [11].

In the course of this project two ways of implementing the two poling pattern Λ_1 and Λ_2 were tested. The first prototype was a single waveguide, in a cascade or interlaced structure, separating the photon pairs afters the crystal, while in the second prototype all components were integrated. The pump light was hereby split into two separated periodically poled waveguides and accordingly recombined afterwards, making additional components hereafter obsolete. These two methods discriminate the two generation of entangled photon sources that have been used. They are depict in Figures 4.6 (1st generation waveguide source) and 4.9 (2nd generation waveguide source), respectively.

The first generation comprises a polarization maintaining fiber for the diagonally polarized pump beam, a waveguide with 2 poling periods over 50mm, that are either sequential, or interlaced with 10, 100 or 500 domains per segments, as it is shown in Figure 4.7. The result of the second harmonic signal of SPDC for such interlaced structures is shown in Figure 4.8. It can be observed that the satellite peaks are pushed away from

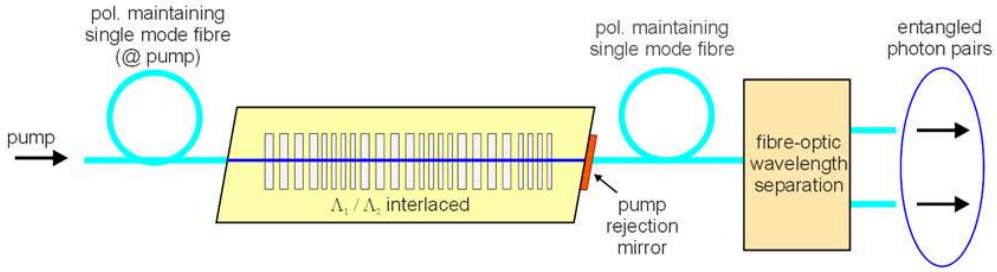

FIGURE 4.6: Design of the 1st generation entangled photon waveguide with interlaced poling periods. Source: [11].

the SH-peaks when the periods per segment are sufficiently decreased. In addition an anti-reflective mirror at the end of the waveguide is used to prevent the pump light from entering the PM fiber that is used to carry signal and idler photons. Afterwards the photon pairs are spectrally separated by a wavelength division multiplexer and distributed to Alice and Bob for measurement.

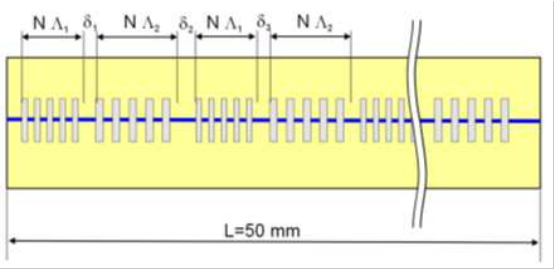

FIGURE 4.7: Schematics of the interlaced structure of the poling period with N being either 10, 100 or 500 domains per segment. Source: [11].

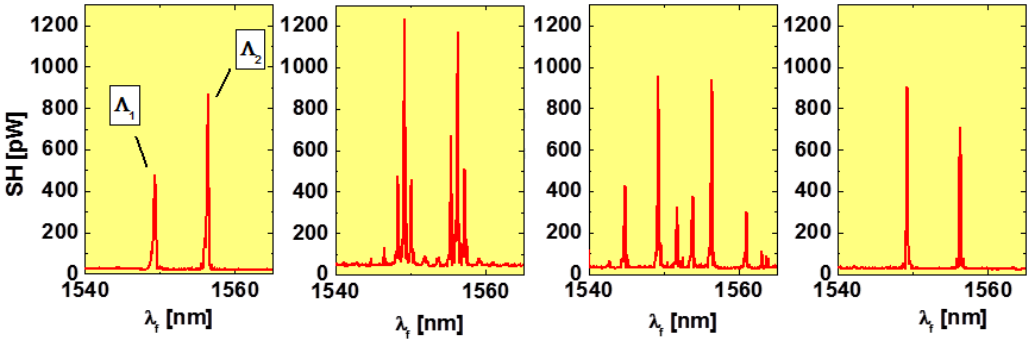

FIGURE 4.8: Measured power of second harmonic signal for decreasing number of periods per section N. On the left the sequential case is shown (N=3000), the next picture show the results for N=500, N=100 and N=10 domains per segment. Source: [11].

The second generation waveguide source, as it is depict in Figure 4.9, or in more detail in Figure 4.10, contains a Y-junction to route the pump beam into two separated waveguide with the two respective poling periods, one on each waveguide. A photon pair is generated in each of the waveguides and afterwards separated by a directional zero-gap

polarization coupler in such a way that TE and TM mode waves are guided in the cross or the bar waveguide according to their propagation constants.

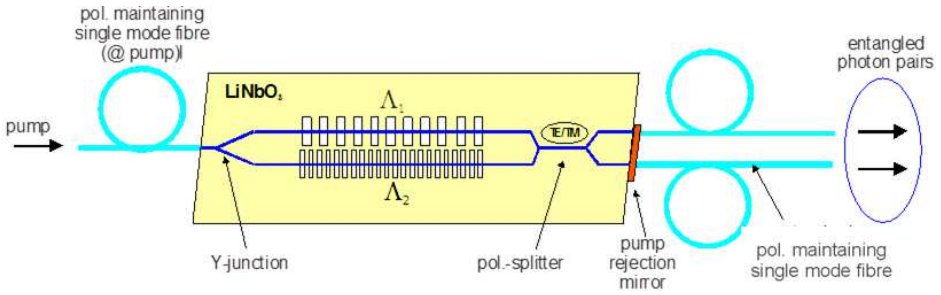

FIGURE 4.9: Design of the 2nd generation entangled photon waveguide source. Source: [11].

The length and opening angle of this coupler are designed in such a way that only the two eigenmodes, TE and TM, can propagate through the coupler. Their separation is achieved by introducing a phase shift induced by the design parameters that yield either an even or odd multiple of π of the eigenmodes, which correspond to the respective exits of the coupler. The theoretical background is described in more details in [83]. The precise specifications of the 2nd generation waveguide are shown in the picture below.

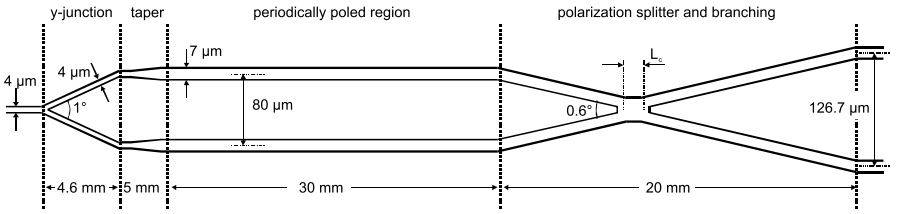

FIGURE 4.10: Specification of the 2nd generation entangled waveguide source. Source: [11].

Although the desired goal for a QKD space application is a fully integrated waveguide source with all optical components on a scalable chip, as it is proposed in the 2nd generation waveguide, the manufacturing process of the waveguide itself as well as the beam splitter and the TE/TM coupler of the 2nd generation waveguide are still a challenging task. Therefore the waver samples that have been produced and will be investigated in this project comprise not only one but 25 groups of waveguides, with 3 waveguides within each group. The waveguides of such a sample have different length and width as well as different poling periods Λ_i and domains per segment N_i. However, not all of them are periodically poled. A schematic overview of the sample is shown in 4.11. The colored regions are the periodically poled waveguide, while in front of them taper and in the second generation Y-junction can be observed. After thorough evaluation of each waveguide the most promising candidate will be pigtailed, i.e. permanently bonded with optical fiber, to receive an integrated optical device. The evaluation criteria are the shape of the spectral mode, internal loss as well as symmetrical power of signal and

idler in the SPDC and SFG processes. In the next chapter these methods are presented in detail. Table 4.1 concludes this chapter by shortly summarizing the specifications of the two waveguide samples in terms of poling periods, length and width and domains per segment.

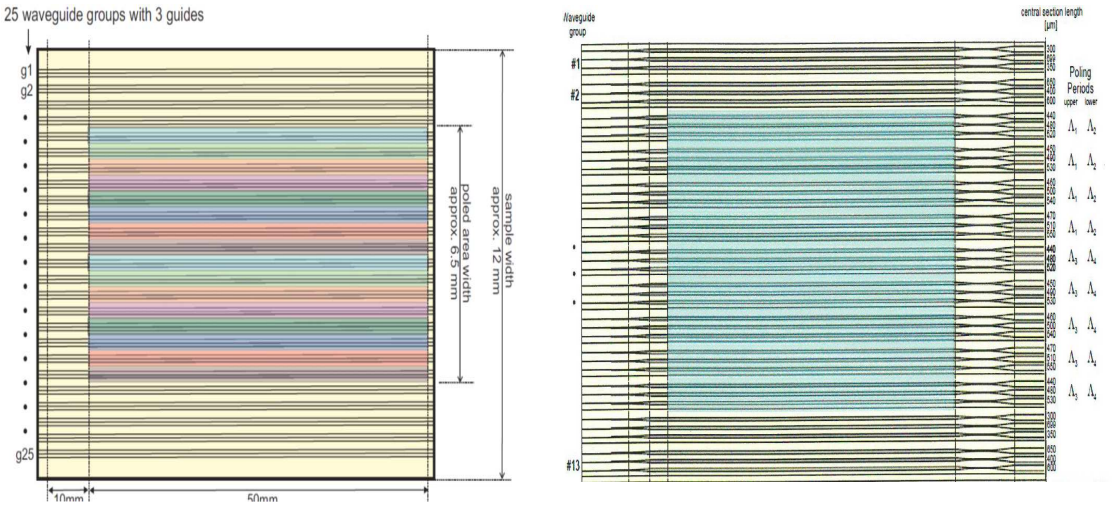

FIGURE 4.11: Schematics of the waveguide groups and poling periods on the samples of 1st (left) and 2nd (right) Generation Sources. Source: [11].

	1st Generation Source	**2nd Generation Source**
Groups	25	13
Poled section	$49mm$	$30mm$
Poling Periods Λ_i	$\Lambda_1 = 9.07\mu m$, $\Lambda_2 = 9.14\mu m$ $\Lambda_3 = 9.30\mu m$, $\Lambda_4 = 9.37\mu m$ $\Lambda_1 = 9.02\mu m$, $\Lambda_2 = 9.09\mu m$ $\Lambda_3 = 9.35\mu m$, $\Lambda_4 = 9.41\mu m$	$\Lambda_1 = 9.07\mu m$, $\Lambda_2 = 9.14\mu m$ $\Lambda_3 = 9.30\mu m$, $\Lambda_4 = 9.37\mu m$ $\Lambda_1 = 9.02\mu m$, $\Lambda_2 = 9.09\mu m$ $\Lambda_3 = 9.35\mu m$, $\Lambda_4 = 9.41\mu m$
Number of domains per segment	N_1 = sequential (3000), $N_2 = 500$, $N_3 = 100$, $N_4 = 10$	—

TABLE 4.1: Specifications of the waveguide samples under investigation.

4.2 Measurement and Evaluation

4.2.1 SFG Measurement of 1st Generation Waveguide

After several approaches to find a suitable setup that allows a precise and fast way to scan through all waveguides of a sample crystal, the setup shown in Figures 4.12 and 4.13 turned out to fit best. While the waveguide sample itself is placed sideways on a 3D mounting with micrometer precision surrounded by an aluminum cage that allows the metal around the crystal to be heated to temperatures up to 200° Celsius. In order to reach these high temperature a custom build device with a $10k\Omega$ negative temperature controller (NTC) thermistor and ThorLabs ITC510 laser diode controller has been used to give sufficient power to the Peltier heater. Due to this combination of an unknown NTC and an independent power source a precise value of the temperature in degree Celsius could not be given. Hence all temperatures are given in $k\Omega$ with respect to the used components. The mounting of the crystal is shown in the graphic and the photos below.

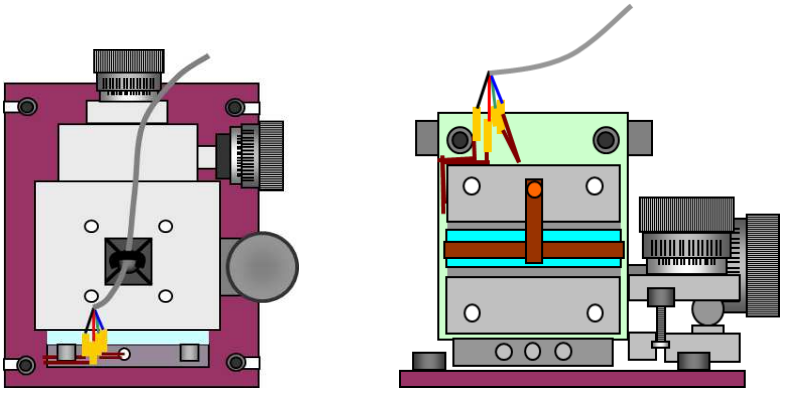

FIGURE 4.12: The Waveguide is clamped to an aluminum case with an attached Peltier element for temperature tuning. This construction is attached to a 3D mount. Source: [12].

The first stage was to align the coupling lenses in front of the crystal to precisely hit the taper section before entering the waveguide, as it is shown in Figure 4.14. The outgoing beam was again recollimated and fiber-coupled. The focal lengths are 11 mm before and 15.3 mm after the crystal. In the best case a 775nm with attached polarization control was able to transmit 23% of the input power through the waveguide.

Once the optimal position of the lenses has been found, the waveguide properties are further determined by SFG, which allows to reconstruct the optimal point of operation for SPDC, with respect to pump wavelength and crystal temperature. As a first step the crystal has been investigated for 70°C, 150°C and 150°C. A diagram of the setup is shown in Figure 4.15.

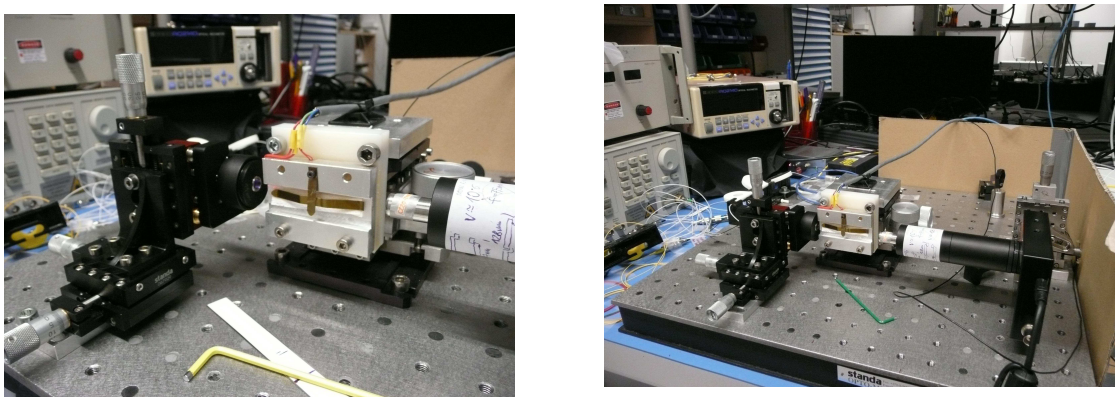

FIGURE 4.13: Photo of the free space setup for investigating the waveguide of the provided sample. The crystal is placed on a 3D-micrometer stage while the incoupled after a recollimation lens and observed by a CCD camera. Source: [12].

FIGURE 4.14: Setup to determine the Coupling efficiency of the waveguides. Source: [12].

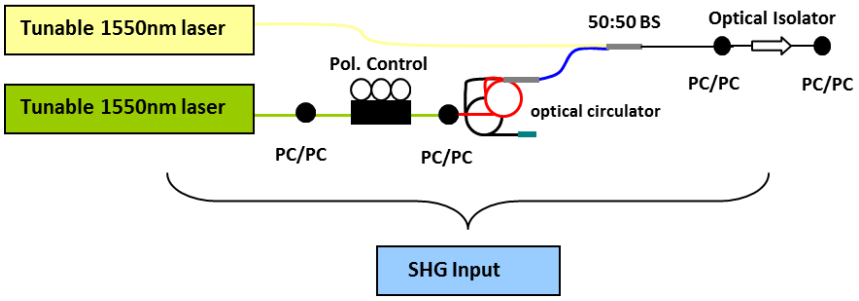

FIGURE 4.15: Setup to determine the Coupling efficiency of the waveguides. Source: [12].

The third waveguide of each group is used as a representation of the group quality, since the width of $7\mu m$ should provide the most modes and hence the lowest loss. Following the theory of DGF, as stated in chapter 3.2.1.3, two wavelengths are pumped into the crystal to create a third. As we expect signal and idler wavelength to be in the C-Band, two tunable lasers, λ_1 one from 1537nm - 1553nm, the other, λ_2, from 1520nm-1590nm are used to scan for the respective pump wavelength. While λ_1 was fixed, λ_2 was swept within the stated range. A silicon SPDC, sensitive to light in the near infrared was used to collect the created photons. When looking at the two QPM curves of Figure 4.5, we see that in the most general case [1] six different wavelengths in the near infrared are created as it is displayed on the left side in Figure 4.16. Since the two QPM curves (red and green) are in a cross position at most two pump wavelengths exist where λ_1 and λ_2 fulfill the QPM condition, i.e. one with $\lambda_2 > \lambda_1$, where λ_1 is in TM-mode and λ_2 in

[1] The most general case means here that λ_1 is not located at any crossing points of the QPM curves.

TE-mode (left of the cross point of TE and TM curve), and the other with $\lambda_2 < \lambda_1$ with opposite modes (right of the cross point of TE and TM curve). However two exceptions arise when one of the wavelengths λ_1 or λ_2 is located in the crossing points of the QPM curves.

Given that λ_i is located in the crossing point of the same poling period (green-green or red-red), two wavelengths coincide and only four pump wavelengths are generated.

On the other hand, when λ_i is chosen to be in one of the two crossing points of two different poling periods (green-red or red-green), two wavelengths coincide and only five pump wavelengths are created. This situation is shown on the right picture of Figure 4.16.

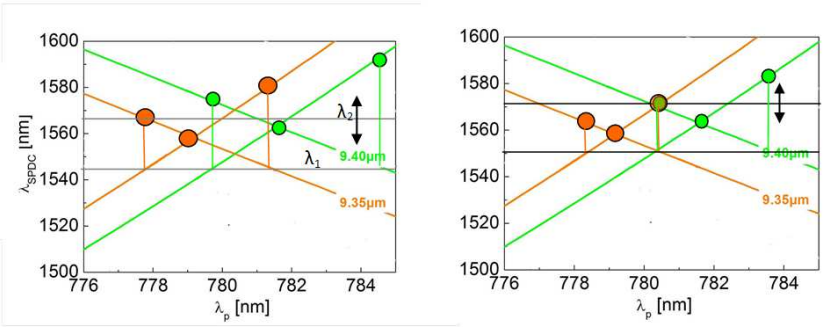

FIGURE 4.16: Left: Six different wavelengths are created due to SFG when λ_1 is fixed at a position away from the cross points and $\lambda 2$ is sweeped. Right: When λ_1 is located at the cross point only five different wavelength are created since two peaks coincide. Source: [13].

The latter case corresponds exactly to the optimal operation point of SPDC that will eventually be used to create entangled photon pairs and therefore gives the accurate pumping wavelength. The results of this SFG measurement is summarized in Figures 4.17 for 150°C and 4.18 for 30°C. The 'fixed' wavelength λ_1 moved in 2nm steps while λ_2 is swept in 0.1nm steps. In Figure 4.17 the two expected wavelength at the crossing points of the QPM curves occur each time at a tuning wavelength of λ_2=1557.5nm and 1564nm (x-axis of the Figure 4.16) independent of the fixed wavelength λ_1 (y-axis). These values are taken from the waveguide of group 14 with poling periods $\Lambda_1 = 9.30\mu$ m and $\Lambda_2 = 9.37\mu$ m

The measurement has been repeated for 30°C for the third waveguide of group 13 with poling periods $\Lambda_1 = 9.02\mu$m and $\Lambda_2 = 9.09\mu$m and again the crossing points occur around the wavelengths λ_2=1550nm and 1557nm independent of λ_1, as it is shown in 4.18. However two weaker wavelengths at around 1535nm and 1542nm are measured with the same behavior. Due to the symmetric spacing of these wavelength these are assumed to be higher order effects of the SFG and of no interest for our measurement.

The results are converted using $\frac{1}{\lambda_1} + \frac{1}{\lambda_2} = \frac{1}{\lambda_{Pump}}$ and plotted in Figure 4.19. Here the

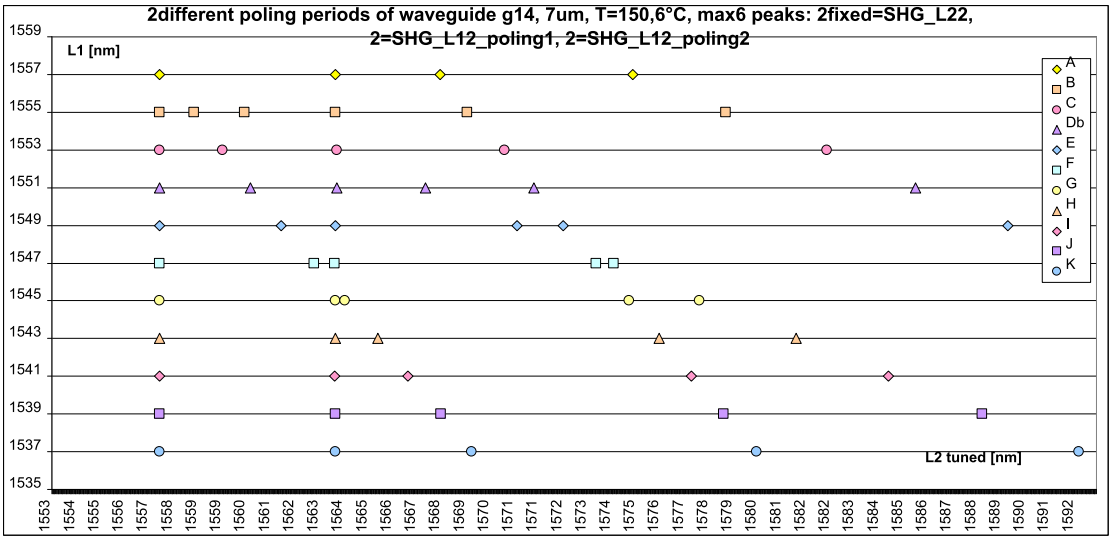

FIGURE 4.17: SFG Scan with a fixed and a tunable wavelength for waveguide group 13. Source: [12].

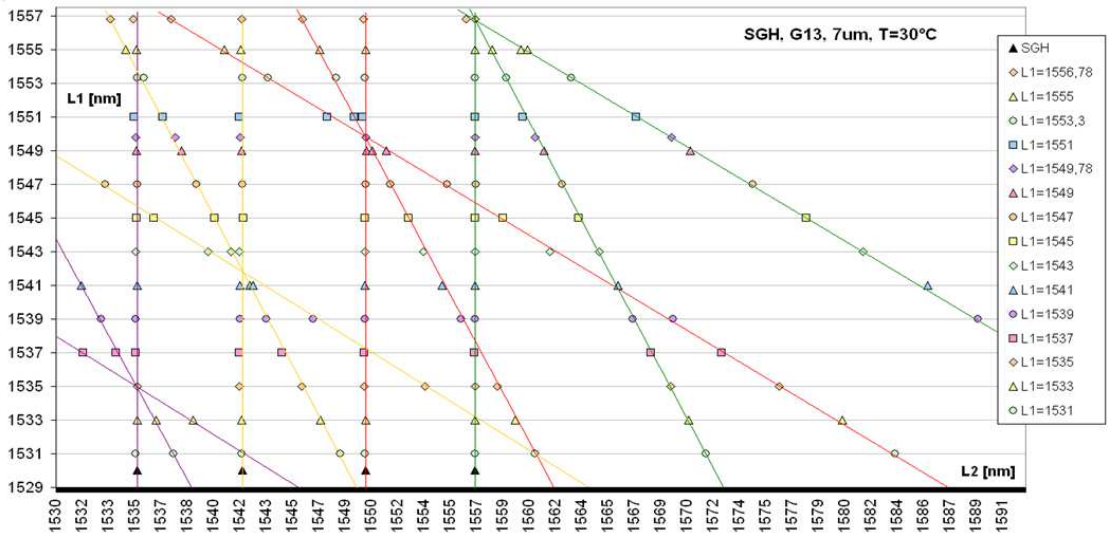

FIGURE 4.18: SFG Scan with a fixed and a tunable wavelength for waveguide group 12. Source: [12].

theoretically predicted QPM curves are experimentally confirmed for the just presented poling waveguides. The red and green curve corresponds to $\Lambda_1 = 9.02\mu$ m and $\Lambda_2 = 9.09\mu$ m, respectively of group 13, while yellow and purple represent the curve of $\Lambda_1 = 9.30\mu$ m and $\Lambda_2 = 9.37\mu$ m, respectively.

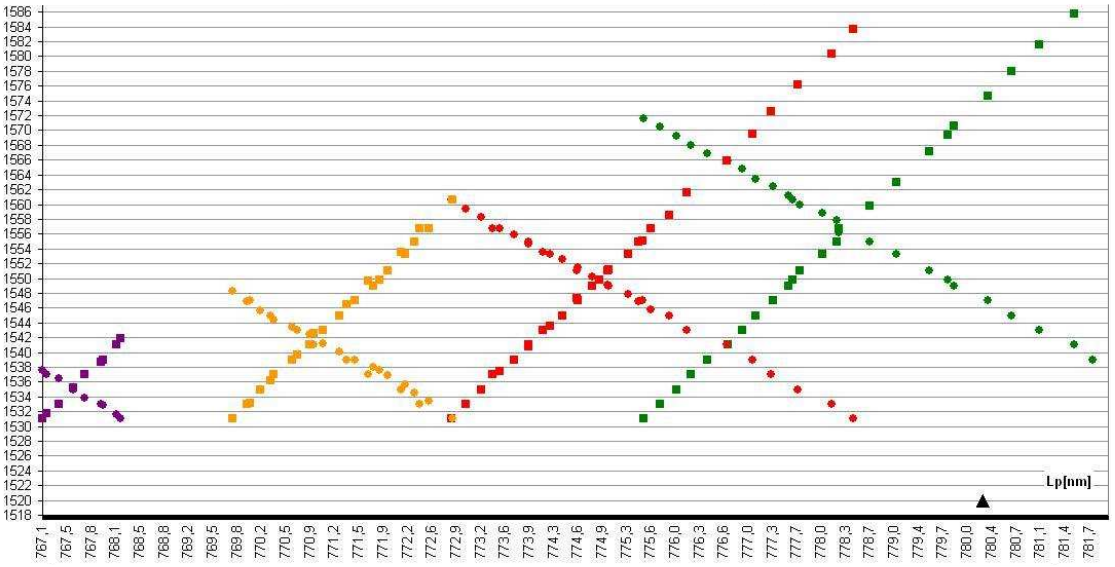

FIGURE 4.19: Experimental reconstruction of the QPM curves for waveguide groups 12 and 13. Source: [12].

4.2.2 SPDC Measurement of the 1st generation Waveguide

4.2.2.1 Correcting the temporal Walk-off of the Photon Pairs

Following the theory of SPDC a photon propagating within a waveguide with a non-vanishing second order non-linearity term $X^{(2)}$, a birefringent media, decays into signal and idler photon with matching wavelengths and opposite polarizations. Hence the created photons propagate along a fast and a slow axis, with refractive index n_{fast} and n_{slow} respectively. When following this thought two photons are created at a certain point of the crystal and suffer a certain walk-off, i.e. a time difference, depending on the propagated length. Figure 4.20 illustrates this fact for the case that the photons are created in the first poling period Λ_1. Between each poling segment a phase shift compensator denoted by its lengths δ is supposed to correct the phase mismatch of the QPM curve that is introduced when the two poling periods are interlaced, since the wavenumbers of the poling periods for QPM are not equal. However an additional time shift is introduced by this section, that is included in the time difference $\|t_2 - t_1\|$ as shown in the illustration.

In the other case, namely the creation of the photons in the second poling period Λ_2 results in the same delay time, however, the time delay of signal and idler are reversed. Therefore, in the most general case the possible walk-off times are illustrated in Figure 4.21.

According to this simple model the minimal and maximal delay times can be calculated when the refractive index of fast and slow axis is known. The Sellmeier equation for

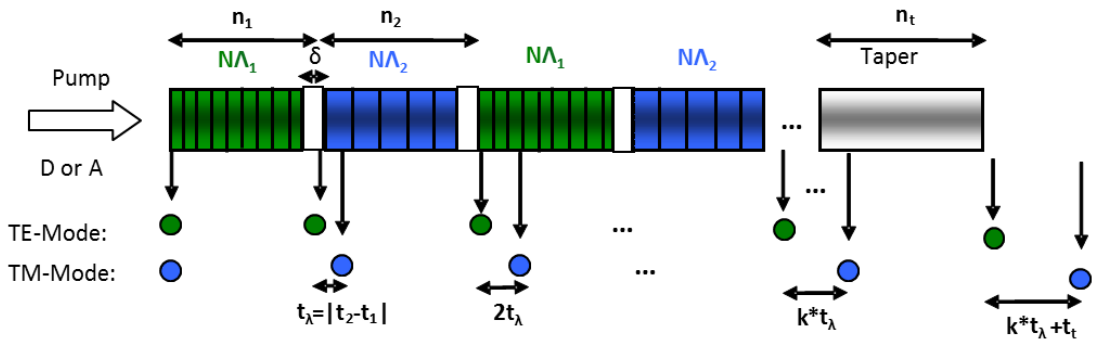

FIGURE 4.20: Temporal walk-off of the two photon pairs generated by SPDC. Source: [12].

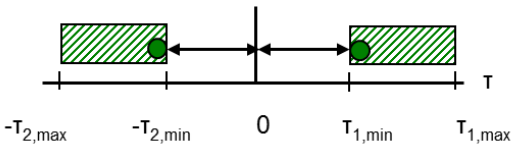

FIGURE 4.21: Possible Delays of TE (or TM) photon with respect to its photon pair. Source: [12].

$LiNbO_3$ can serve as a first approximation. They denote the refractive index, n, in dependence of wavelength λ and temperature T,

$$n(\lambda, T) = \sqrt{a_1 + \frac{a_2 + b_1 F}{\lambda^2 - (a_3 + b_2 F)^2} + b_3 F - a_4 \lambda^4}, \text{with } F = (T - 24.5)(T + T_0) \quad (4.1)$$

The constants a_i, b_i and T_0 depend on the respective substrate. The group refractive index of the two modes, $n_{g,TM}$ and $n_{g,TE}$ can now be calculated and used in the following equation to determine the maximal delay time τ_{max}

$$\tau_{max} = \frac{L_{WG}}{V_{g,TM}} - \frac{L_{WG}}{V_{g,TE}} = L_{WG}\left(\frac{n_{g,TM}}{c} - \frac{n_{g,TE}}{c}\right) = L_{WG}\Delta n_g, \text{with } n_g = n - \lambda\frac{\partial n}{\partial \lambda} \quad (4.2)$$

with L_{WG} being the interaction length and $V_{g,TM/TE}$ being the group velocity of the photon in TE and TM mode.

Using the signal and idler wavelengths λ_1=1536.72nm and λ_2=1563.6nm measured in the SFG measurement of the previous chapter as well as a temperature of 70°C and an interaction length of 49mm the maximal time delays for λ_1 and λ_2 yield τ_{max,λ_1}=13.1895ps and τ_{max,λ_2}=13.1895ps giving an average delay time of 6.59ps.

In practice this time compensation is done by a Babinet-Soleil birefringent crystal, i.e. two birefringent wedges that allow to adjust the interaction length of the photons with the material by displacing one against the other. Hereby the time compensation can be precisely tuned. Another way is the application of polarization maintaining (PM) fiber,

that is precisely cut in length to compensate for the temporal walk-off. The Babinet-Soleil and PM fiber are displayed in Figure 4.22. The delay time applied on the faster photon is in this case given by $\tau_{delay} = \tau_P L = \frac{\lambda^2}{\Delta\lambda c}$, where $\Delta\lambda$ is the fringe width that occurs by interference between slow and fast axis signals and τ_P is called polarization mode dispersion, given by $\tau_P = \frac{B}{c}$, with B being the birefringence, i.e. $n_{fast} - n_{slow}$. Here the common beat length L_B for panda PM fiber, 3mm, is used to calculate the birefringence $B = \frac{\lambda}{L_B}$ and together with the previous equation a PM fiber length of 3.8m is calculated compensate the temporal walk-off in our case.

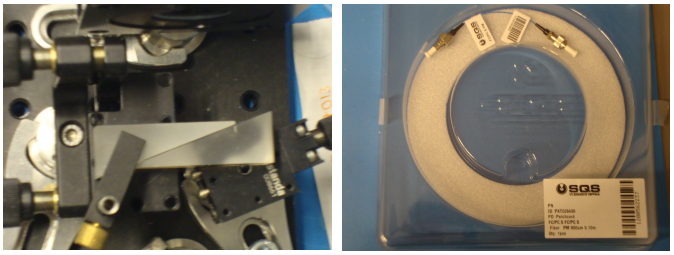

FIGURE 4.22: Left: Babinet-Soleil Crystal Wedges Right: PM Panda Fiber. Source: [12].

4.2.2.2 SPDC and Coincidence Measurements

With the preparation of the SFG measurement and the compensation of the temporal walk-off the waveguide source can finally be used to create signal and idler photons and eventually entangled photon pairs. Two setups are possible approaches for this matter and displayed in 4.23 and 4.24. They comprise a tunable pump laser, a bat ear polarization control and focus lens in front of the crystal to focus with diagonal polarization in the taper section. As shown in the previous chapter the crystal is attached to a heater to tune the wavelength according to the waveguides poling period and point of operation. After the crystal, the pump is suppressed by an optical isolator while signal and idler are spectraly separated by a common CWDM filter and detected by two gated single photon detectors. The coinciding photon pairs arriving at the detectors are in this setup detected by applying a common trigger to both detectors.

A second possible option is to use a free-running, or independently triggered detector that forwards a trigger pulse to the second detector each time a photon arrives. This is shown in Figure 4.24. An optical delay line is needed to compensate the time span of the electrical trigger pulse. The measurements showed that with this setup an order of magnitude in coincidence counts per seconds is gained. In both cases a time tagging module (TTM) with a temporal resolution of about 50ps is used to attach a time stamp to each detection event and send it via Ethernet port to a coincidence software for processing. Two received event are hereby matched to its corresponding click on the

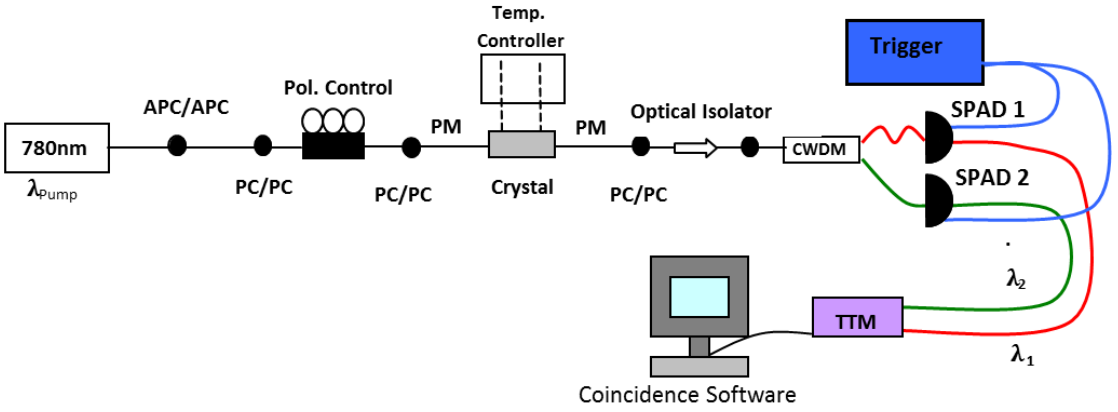

FIGURE 4.23: First experimental setup for SPDC measurement. Source: [12].

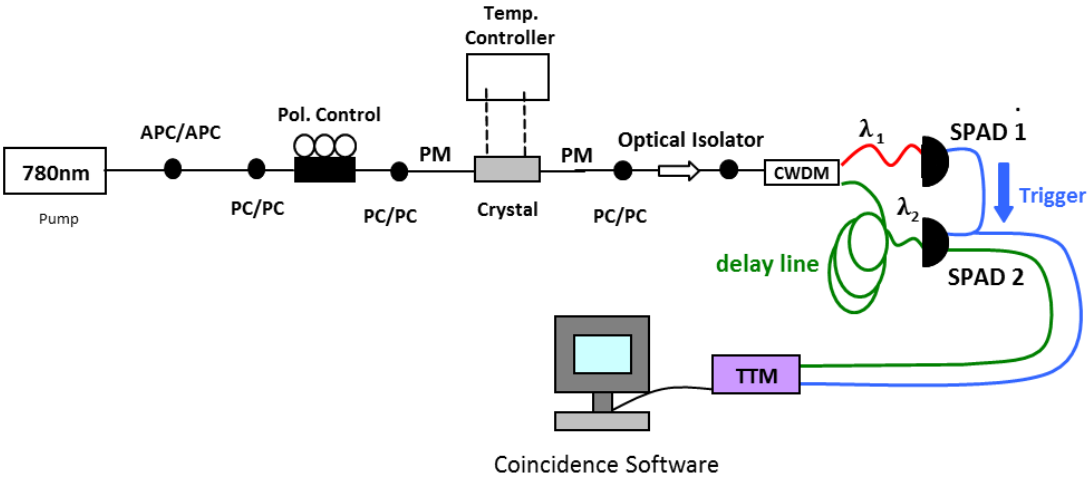

FIGURE 4.24: Second experimental setup for SPDC measurement. Source: [12].

other detector when they coincide within a certain time frame. They are counted as coincidence event. The highest coincidence rate has been achieved with a custom build free running AIT-detector with a dead time of 1μs a quantum efficiency of 7% and triggered IDQuantique detector IDQ201 with In the following measurements the idQ201 detectors were used with a dead time of 10μs as well as a opening window of 20ns with a quantum efficiency of 15%. All waveguides have been scanned and evaluated with these setup. Figure 4.25 shows an extraction how the coincidence counts are compared.

4.2.2.3 Entanglement Measurement

In order to demonstrate the capability of the titanium indiffused $LiNbO_3$ to produce entangled photon pairs a detection in two non orthogonal bases has to be prepared. In this case a free space setup was prepared that allows to adjust linear and circular polarization on signal and idler beam independently with a cascade of half- and quarter

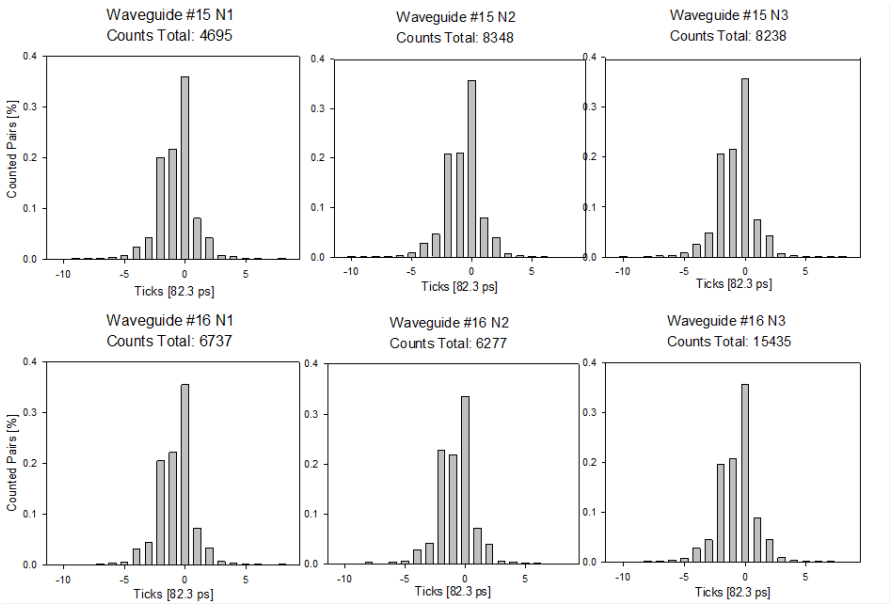

FIGURE 4.25: SPDC coincidence histrograms from waveguide groups 13 and 14. Source: [12].

waveplate (HWP and QWP) in order to restore the drifts induced by SSMF or CWDM. Using an analyzer setup comprising a HWP and a rotatable polarizer the four combinations of H,V,+,- for signal and idler beam as well as H,V,+,- for the measurement basis can be adjusted. The coupling efficiency of this setup could be measured to be around 80% - 85% due to an accurate alignment of coupling lenses. The setup in detail is shown in Figure 4.26.

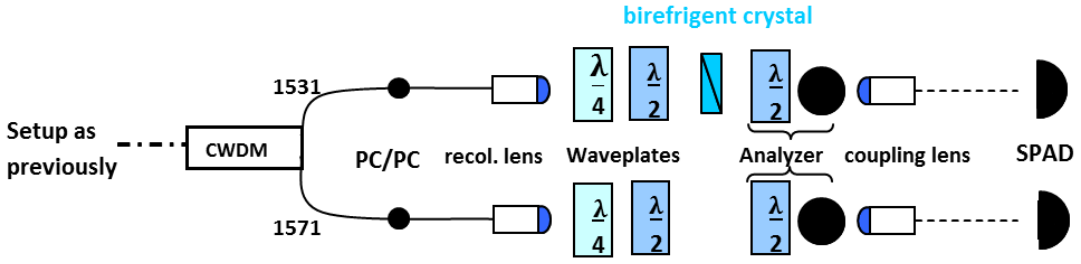

FIGURE 4.26: BB84 setup for entanglement measurement. Source: [12] and [13].

The first attempt to measure entanglement is displayed in the histograms of Figures 4.27 and 4.28 as well as in Table 4.2. As one can see the visibility in the H-V basis is rather good (95.5%). However the "quantum" basis D-A reveals that no correlated photon pairs are found here (5% visibility).

After the sample has been pigtailed with an appropriate PM fiber, the result of the measured coincidences improved as it is shown in Table 4.4. The coincidences have been averaged over 1 minute. Unfortunately we were not able to further improve the visibility

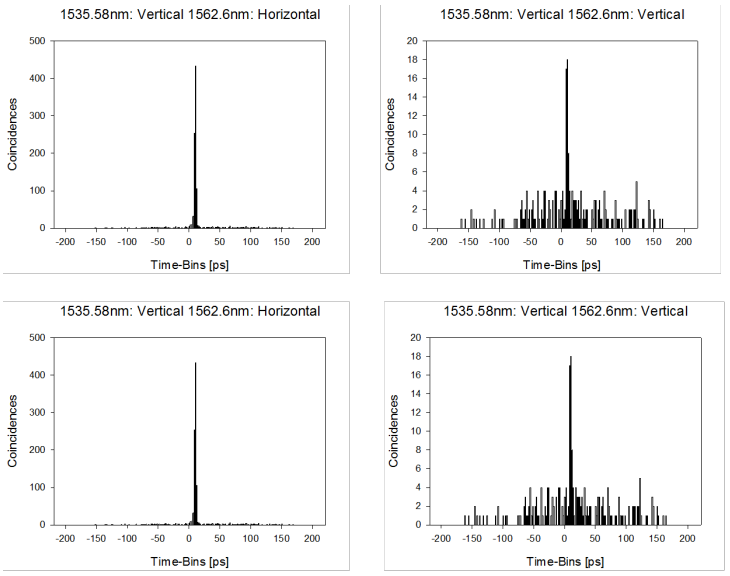

FIGURE 4.27: Results for the H-V Basis. Source: [13]

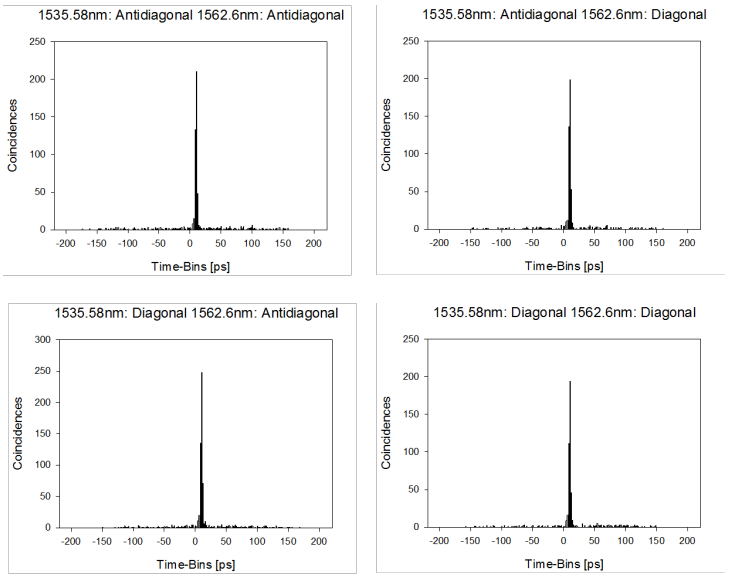

FIGURE 4.28: Results for the D-A Basis. Source: [13]

Basis	**H**	**V**	Basis	+	-
H	7	433	+	194	199
V	661	18	-	248	210

TABLE 4.2: Measured Coincidences in the respective bases without any walk-off compensation. Source: [13].

since the exact length of the PM fiber and hence the related temporal compensation could not be realized experimentally for the given sample. The dependence of the visibility from the PM fiber length as well as from the relative phase is displayed in Figure 4.29.

However when we follow the work of [14] we see the full potential of the waveguide when the spectral and temporal compensation as well as the wavelength and temperature

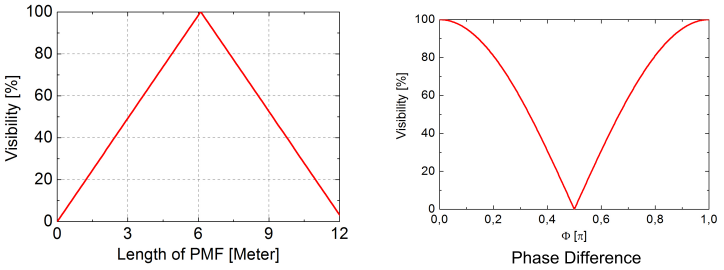

FIGURE 4.29: Left: Visibility over PM fiber length. Right: Visibility over Phase difference. Source: [14].

Basis	**H**	**V**	Basis	+	-
H	4.61	119.53	+	41.62	83.01
V	135.27	5.43	-	90.93	52.2

TABLE 4.3: Measured Coincidences in the respective bases with partial walk-off compensation. Source: [13].

drift are corrected in best way possible. The experimental setup in this case differs slightly from the our setup and is shown in 4.30. The coincidence counts are hereby collected by a common trigger signal between AOM, i.e. a pulsed laser source, and two gated detectors controlled by a delay generator (DG) and time to digit converter (TDC). Before entering the detector a Fiber Bragg Grating (FBG) is employed to filter for the precise wavelength of signal and idler, respectively.

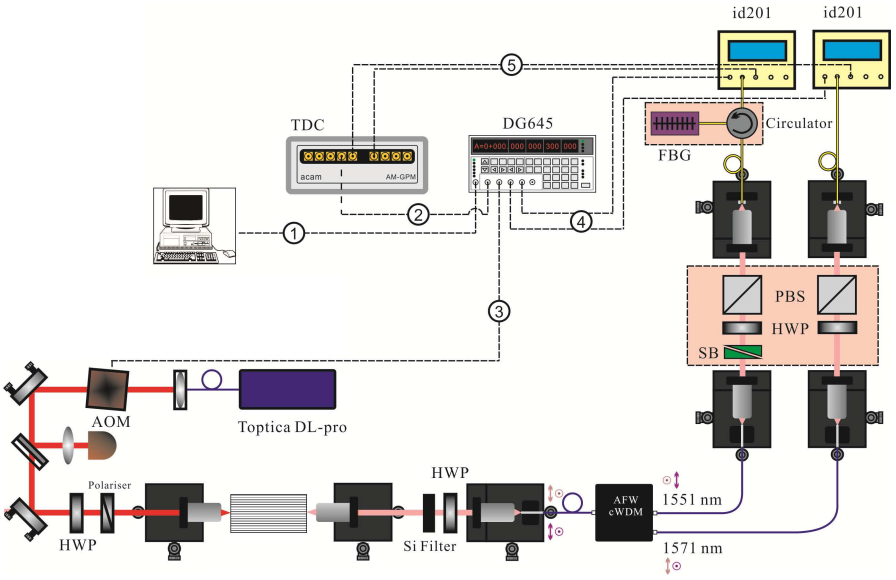

FIGURE 4.30: Setup for optimal results.Taken from [14]

With this setup a visibility of 89.7% for the H/V basis and 92.5% for the +/- basis could be reached [14]. Compared to bulk crystal free space optics this might seem as a rather poor result, since those entanglement sources reach visibilities close to 99% [84]. Also the nonlocality of the created photon pair has been shown in a Bell measurement. The

measured value of 2.57 clearly exceeds the classical expectation of 2 but is still away from the optimal $2\sqrt{2}$. The reason for these values not being state of the art is clearly due to to slight spectral and temporal mismatches of the setup. However, it has to be noted that despite these values the properties of this source for space application is one of the best options. It is a fully integrated, maintenance free EPR source with high brightness, narrow linewidth at telecom wavelength.

Basis	**H**	**V**	Basis	+	-
H	4.61	119.53	+	41.62	83.01
V	135.27	5.43	-	90.93	52.2

TABLE 4.4: Measured Coincidences in the respective bases with partial walk-off compensation. Source: [13].

4.2.3 Characterization of the 2nd Generation Waveguide Source

As stated chapter 4.1.1. the second generation waveguide applies an integrated TE/TM splitter that obsoletes the CWDM spectral filtering and is supposed to produce entangled photon pairs right from the crystal. Two pigtailed PM fibers correct the temporal walk-off and send the eligible photons to Alice and Bob, respectively.
How compact the entire setup can be packed is shown in 4.31. The right picture shows the waveguide sample in its housing with heater wiring. On the left picture, the entire setup is displayed with pump laser, polarizer, heater, power supply and waveguide. The whole source is fully integrated and reduced to less than $0.5m^2$, suitable for any space application.

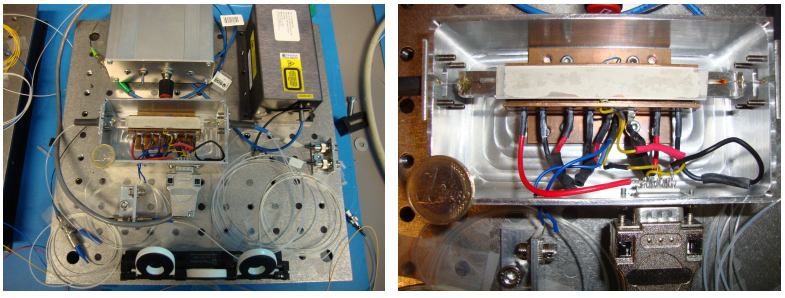

FIGURE 4.31: Left: 2nd generation waveguide with housing and heater wirering. Right: Closely packet setup with pump laser, polarization control, heater and electronics for 2nd generation waveguide. Source: [13].

Similar to the 1st generation multiple waveguide groups with different poling periods are fabricated on a $LiNbO_3$ waver sample with operating temperatures at around 30°C and up to $150° - 200°$C. However for SFG as well as SHG the two waveguides have to be pumped individually. Hence both waveguides, spatially separated by about 0.1mm, have to be accessed simultaneously. A glass ferrule is used that holds two fibers in exact

this spacing. Furthermore a polarizer on each input is needed to enter each waveguide with diagonal polarization. The entire setup was build by the university Paderborn and is shown in Figure 4.32.

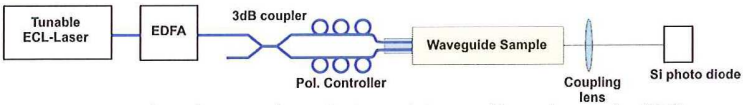

FIGURE 4.32: Setup for SHG for 2nd generation waveguide. Source: [13].

The same approach as for the 1st generation waveguide, namely scanning the different waveguides for its efficiency (i.e. ratio of input power to to received output on both exits) and applying SHG is also used in this case. For this sample waveguide group 6, subsection 2, with a poling period of $\Lambda_1 = 9.07\mu$ m and $\Lambda_1 = 9.07\mu$ m showed a input-output ratio of 4% at a temperature of T=10kΩ and was chosen for pigtailing. The measured SHG counts are shown in Figure 4.33. Signal and idler correspond hereby to 1556.8nm and 1564nm. It can be seen that the attached fiber causes a significant reduction in both cases, but for 1564nm signal an even 3 times lower signal is received as for the lower wavelength.

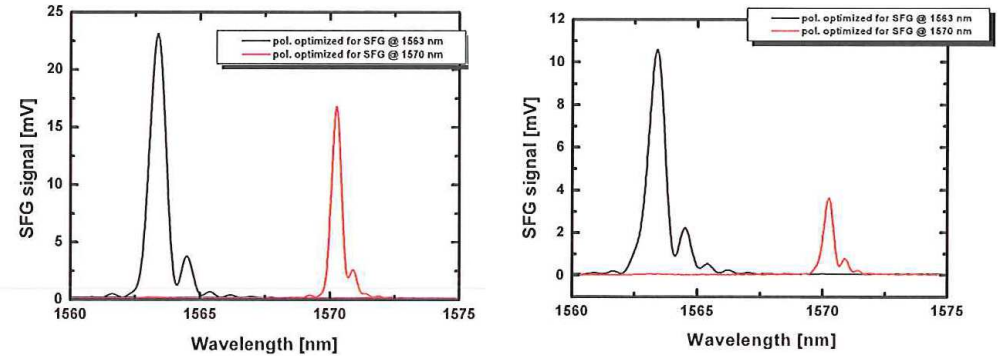

FIGURE 4.33: Left: SHG signal with free space setup. Right: SHG signal after pigtail. Both signal have been separately optimized in polarization. Source: [13].

The pigtailed sample was further investigated in the AIT lab. Similar to the 1st generation, SFG was used to find the optimal operation point. Unlike in the 1st generation case, the optimal polarization of one waveguide denies a high SFG count of the other and vice versa. Hence the most general case of 6 peaks does not entirely comply for the 2nd generation waveguide since in some cases the polarization offset is not sufficient to create a measurable signal peak. The measurement on the left in Figure 4.34 shows that the two largest peaks do not coincide and hence the spectral overlap would allow to distinguish the photons in the SPDC case and no entangled pair would be produced. On the right picture this mismatch is corrected by shifting temperature and fixed signal / idler wavelength to the correct value. In this case a temperature of T=5.524kΩ, with

the two corresponding signal and idler wavelengths of λ_S=1544.96nm and λ_S=1576.3nm was measured. The pump wavelength yields in this case $\lambda_P = 779.13nm$.

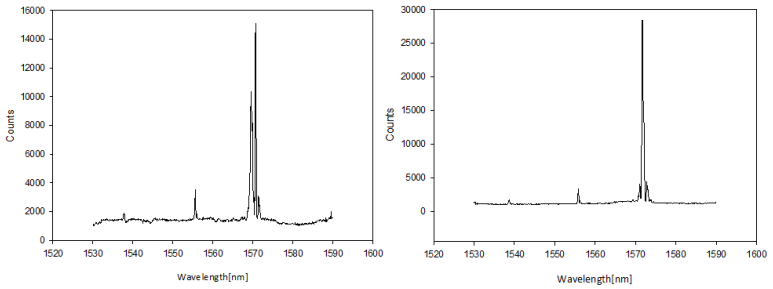

FIGURE 4.34: SFG of the 2nd generation waveguide. Left: Slight offset of the created photon pairs. Right: the created photon pairs overlap perfectly. Source: [13].

The SPCD and hence the entanglement measurement was performed in the same manner as in the first generation case, except for an additional Babinet-Soleil compensator in one branch that was used to correct the phase mismatch of the photon pairs. The two SPAD detectors have been commonly triggered with a 1MHz signal, a gate width of 20ns and a dead time of 2μs at a quantum efficiency of 15%. The measured counts are stated in Table 4.5. They yield a visibility of 91.1% for the H/V basis and 59.3% for the +/-. The assumption for the rather low value in the +/- base is on the one hand an incorrect time compensation on the other the imbalance of the two waveguides that is already apparent in SHG measurement in Figure 4.33.

Basis	**H**	**V**	Basis	+	-
H	5	185	+	21	86
V	51	6	-	90	24

TABLE 4.5: Measured Coincidences in the respective bases with partial walk-off compensation for 2nd generation Waveguide. Source: [13].

Considering the duty cycle of the detectors, 1:50, a total spectral brightness calculated from the measured counts N is given by $B = \frac{N}{\Delta\lambda\tau P_{Pump}}$ of 4.3 $\cdot 10^3 \frac{\text{Counts}}{nm \cdot mW \cdot s}$ is received. Hereby the linewidth of signal and idler $\Delta\lambda$ was assumed to be 1.2nm. Further $\tau = 1s$ and P_{Pump} = 1mW.

4.2.4 Requirements in a Space Environment

Apart from an optimal performance of an entanglement source in a lab environment some consideration has to be given on the different environments the source will be exposed in a potential space application. The basic robustness against vibrations as it is common in a space launch should be provided due to the integrated nature of the

source. Also large temperature changes, ranging from -25°C to 85°C in a stationary orbit have to be balanced by suitable cooling and heating to operate the source at constant parameters. In the next lines a short survey about the conditions in Vacuum as well as electromagnetic and ionizing radiation is given.

Vaccum

The operation of the EPR source in vacuum should not affect the optical part and performance. However, it has to be noted that due to the pressure reduction from $1 \cdot 10^4$ Pa to $3 \cdot 10^{15}$ Pa working temperatures of laser and crystal have to be adapted. Furthermore the European Space Agency (ESA) reported during the project Atmospheric LAser Doppler INstrument (ALADIN) that optical coating deposited on fibers or other waveguides dissolves in low pressure environment. This has to be considered since anti-reflective and high-reflective coating, respectively, are attached to the crystal.

Electro-magnetic radiation

The effect of electro-magnetic or more precisely gamma radiation on optical and optoelectronic parts has been discussed, apart from other publications, discussed in [85]. The results show that the refractive index of a standard single mode fiber depends on its temperature, the optical signal wavelength and additionally the irradiation fluency of γ rays. An increase of thermal and gamma irradiation results in an increase of pulse rise time of a pulsed signal and eventually a decrease of transmission power of the signal. The presented results are received from experiments on communication transmissions fiber links of 10km. Yet, even a slight change in the refractive index of the EPR crystal source can determine the performance of the SPDC process or shift temporal or phase compensation in birefringent components. Similar results, see [86], have been reported for Ti:$LiNbO_3$ waveguides fabricated by proton exchange (PE) as well as annealed proton exchange (APE). The waveguides have been exposed to a total irradiation of 10Mrad and a dosage of 800krad/h. The measured power loss inside the waveguide is in the order of about 0.1dB/cm, whereas the APE has been reported to have lower loss compared to the PE. The measurements have been performed using 633nm, 1530nm and 1550nm.

Ionizing radiation

An interesting effect of ionizing radation, i.e. electrons in this case, has been published in [87], where accelerated electrons have been focused on a Z cut Ti:$LiNbO_3$ waveguide with pigtailed polarization maintaining fibers. A total electron energy of 15MeV was applied. Due to photon electron scattering a mode switching between TE and TM polarized photons has been observed as well as a decrease in power.

Although the presented impairments might induce some more steps into the development of an EPR source for space applications the technology and know-how of an fully integrated QKD space system is here. As the results of the second generation waveguide show, the integration of more complex optical parts in $LiNbO_3$ is demanding and requires several attempts until a suitable benchmark is reached. Nevertheless with suitable funding and effort a promising project could not only show that QKD via space is possible but also give fundamental insight on entanglement over large distances and hence a step towards a possible integration of quantum mechanics and general relativity.

Chapter 5

Photonic Networks

In order to accomplish the step from fully integrated EPR sources for space application to QKD in telecom networks, a quick and understanding outline about photonic networks in general is given in the following sections. The *Open System Interconnection* (*OSI*) model, shortly summerized in Table 5.1, serves as an orientation for the hierarchic structure of the upcoming subjects.

Layer	**Description**	**Unit**	**Protocols**
Application	Data input and output via programs using an user interface	Data	HTTP, FTP, SSH
Presentation	Data is transformed, compressed or encrypted/decrypted for further processing in upper or lower levels	Data	ASCI II, JPEG, MP3
Session	Communication management between remote computers within a network	Data	RPC, PAP
Transport	Establishing the transmission of data using (de-)segmentation, error correction or multiplexing	Segment	UDP, TCP
Network	Routing and secure transmission of packets between multiple network nodes is managed	Packet	IPv4/IPv6, IPSec
Data Link	Comprises Media Access Control (MAC) for device management and Logical Link Control (LLC) for synchronization and error correction	Bit/Frame	PPP, IEEE802.2, L2TP
Physical	Network topology, transmission modes and physical properties of the respective network devices	Bit	DSL, USB

Table 5.1: OSI-Model

While cryptographic application for authentication and encryption, as described in chapter 2, are exclusively embedded in higher layers, such as the network (IPSec) and upper

layers (SSH), the hardware infrastructure is the crucial point for Quantum Cryptography. Hence before going into greater detail about a potential integration of QKD into photonic networks, it is necessary to understand the components, protocols and standards of the two bottom layers that are provided by existing networks. The next chapter presents a selection of important electro-optical and all optical devices from this layer and their respective function within the network.

5.1 Introduction into Optical Networks and its Components

The main purpose of a network is the reasonable fast and error free transmission of bits between several network nodes. The first step towards this goal is a suitable network topology. The easiest way is a *bus-network*, this means a cascade of network nodes with a single link to the left and right neighbor. Another possibility is a closed bus, in other words a *ring topology*. These approaches however suffer a failure of the entire network once a single node or link is corrupted. A *star topology* reduces this risk to a single node located in the middle of this network, whereas networks with *mesh topologies*, i.e. the interconnection of multiple rings, the thread of failure is reduced even further by connecting each node to at least two others. These and further examples of basic topologies are sketches in Figure 5.1.

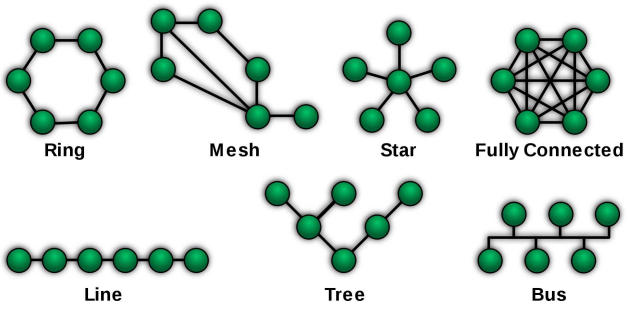

FIGURE 5.1: Different types of network topolgies

It is obvious that the more complex the network becomes, the more cost and maintenance is needed to operate it. The more optical fibers have to be deployed the more complex the routing and timing administration becomes. The decision, which topology is best suited for the respective users depends on the one hand on the amount of transmitted data and the given geographic situation and the hereby related costs for deployment.

5.1.1 First Generation Networks

The first setup of such topologies was done with copper wire for establishing a wide deployment of landline telephone networks. However, shortly after the digitalization of analogue signals (mostly telephone signals) using Pulse Code Modulation (PCM) the demand for a faster transmission and a higher capacity lead to the first multiplexing standard called *Plesiochronous Digital Hierarchy* (PDH), standardized by the ITU-T in the late 1970s. The first generation of photon networks used light exclusively for the transmission of data, whereas routing and processing was done by eligible electronics. PDH is a time multiplexed technique that binds a certain amount of channels, separated by certain time difference, to build a frame. This frame is thereby collectively send at fixed bit rates (2048kbit/s in Europa and 1544kbit/s in north America and Japan). The reference time between the channels may differ by a certain amount, hence 'plesiochronous'.
However, since this techniques suffered from fundamental problems [1] another multiplexing standard was introduced in 1985, that relied on complete synchronized signals, though was capable of processing frames from PDH. This standard was first developed in the U.S. under the name SDH, *Synchronous Digital Hierarchy*, and is known in Europe and Japan as SONET, *Synchronous Optical NETwork*. It comprises in either case regenerators (for synchronizing, reshaping and regenerating attenuated and dispersion shifted signals), terminal multiplexers (for combining PDH and SONET/SDH signals), Add-Drop multiplexers (for extracting or adding lower bit rate PDH or SONET/SDH signals in higher bit rate signals) and digital cross connects (for mapping signals from various frame lengths into each other). In order to control these elements a software based telecommunication management network (TMN) extracts the information embedded in the respective header and pointer section of the signal, located at fixed positions in the so called Synchronous Transport Module (STM) frame. On top of these two transport modes, the so called *Asynchronous Transfer Mode* (ATM) has been developed (2nd layer of the OSI model) in order to provide independence from bit rates and network delays with the help of fixed sized frames, called cells.
Although a relatively large amount of transmissions is still done electronically on already existing copper wires, the upgrade to optical transmission via glass fiber is rapid and clearly offers advantages in speed, bandwidth as well maintenance and running costs at least for all optical networks. The main components that enable this progress are presented in the following:

- *Optical fibres*

[1] The main problem, due to a bit interleaved structure, was, that the channels within a frame could not be accessed unless the entire frame was read out.

Optical fibers are standardized according to their core diameter as well as their change in refractive index between core and cladding. The simple schematics of an optical fiber is shown in Figure 5.2, with the SiO_2 core, doped with GeO_2, and the pure silica cladding.

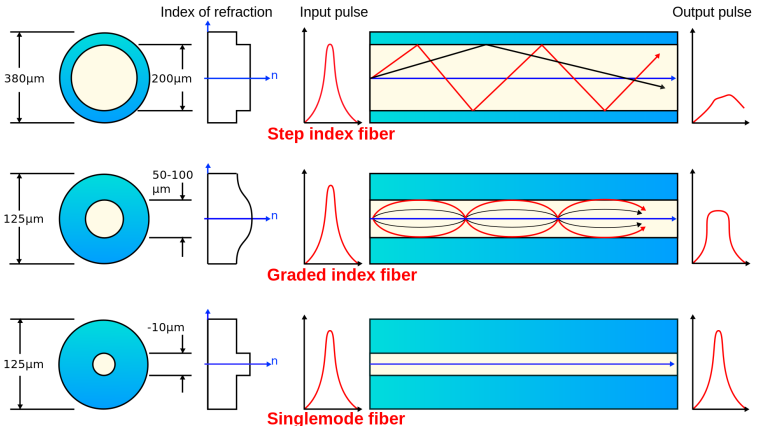

FIGURE 5.2: Schmatics of multimode step index fiber (top), graded index fiber (middle) and step index single mode fiber (bottom). Source: Mrzeon, CC BY-SA 3.0

Apart from several other types, the most common fibers standardized for optical networks are multi- and single-mode step- and graded-index fibers. While multimode fibers have an core diameter of 62.5 or 50 $\cdot 10^{-6}$ μm, and hence support the propagation of many optical modes, single mode fibers are supposed to support only few modes due to a core diameter of 6-9 μm. The step index fiber has an abrupt change between the refractive index of core and cladding while the graded-index fiber offers a smooth transition in the refractive index change and hence reduces mode dispersion. Due to a low production cost and high range the single mode step index fiber defined by the standard ITU-T G.652 A/B is the preferred fiber in most networks, known as the standard single mode fiber (SSMF). When the attenuation curve, i.e. the loss of this fiber in dependence of the wavelength, as shown in the curve of Figure 5.3, is considered, a high attenuation at around 1400nm is noticed, the so called water-peak.

In order to enable wavelengths in this window for long range optical networking a low water peak fiber (LWPF) has been developed standardized according to ITU-T G.652 C/D. Due to this specifications the preferred wavelengths for optical signals lies in the infrared range of 1550nm, commonly referred to as the *third window* (blue curve in Figure A.3), the *long wavelength band* or *C-Band*. Other possible wavelengths are in the *first window*, around 850nm (red), or the *second window* or *O-Band*, in the range of 1310nm (green). The most common telecom bands, the C- and O-band have a attenuation of about $0.2\frac{dB}{km}$ and $0.5\frac{dB}{km}$, respectively.

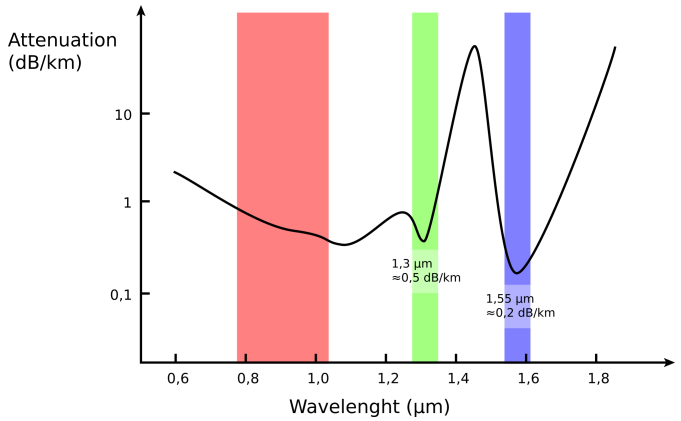

FIGURE 5.3: Attenuation in optical fiber over length. Picture taken from Sassospicco CC BY-SA 3.0.

- *Optical switching*

  Several optical switching techniques are known, depending on their respective principle of operation. They are closely related to the methods of optical filtering. In order to give a short overview the most common switches are shortly summerized in the following.

  - *Electro-optical switches* control the light pass by electrodes that enable a changing the photo refractive index in the respective waveguides when voltage is applied.
  - *Micro-electro-mechanical switches (MEMS)* employ an array of electro-mechanical controlled mirrors that are able to distribute incoming light to various output ports in a 2- or 3-dimensional regime.
  - *SOA based switches* exploit the fact that a semi-conductor can either be used to enhance or lower the incoming signal, depending whether population inversion is achieved or not.
  - *Interferometric switches* use thermo- or electro-optic Mach-Zehnder or Sagnac-loop configuration with a controllable relative phase difference. The output signal is controlled by the thermally or electronically induced phase that results in extinction of the signal in the respective interferometer output. The inclusion of a SOA and a control signal, that, if necessary, enables the gain of the amplifiers, leads to an all optical switching, where no electrical or thermal control is needed.

  How the routing and switching between notes is managed, e.g. burst or packet switching, is supervised in the network and session layer. The next chapter gives a closer insight into such higher layer functions.

- *Amplifiers*
  Amplifiers are a fundamental module for long range communication. Amplifiers mostly comprise semiconducting material, such as Erbium or Silica, that is triggered by an arriving signal and a pump laser that depletes the free electrons in the material which leads to an amplification of the incoming signal. Erbium-doped fiber amplifier (*EDFA*) as well as Semiconducter optical Amplifiers (*SOA*) are the most prominent examples of all optical amplifiers.
  However, in some cases, a simple amplification in power is not enough to grant a error free long haul communication. So called 3R repeaters are used not only to re-amplify but also to re-shape and re-time the signal and its intrinsic clock. This, however, is only realizable in an electro-optical device. Amplifiers are characterized according to their position in the network. *Inline amplifiers* are used as signal repeaters in long distance transmission, while *pre- and booster-amplifiers* are used to enhance the signal before detection and after modulation, respectively. It has to be taken into account, especially for weak signals, that amplifiers usually add noise to the existing signal as a result from amplified spontaneous emission (ASE). This will be discussed in more details in section 6, when it comes to an integration of QKD into networks with such respective amplifiers.

- *Optical Filter, Isolator & Switching Techniques*
  Optical filters are used to select as well as discard certain wavelengths. With slight changes these switches or filters can be used as isolators that allow the optical signal to propagate forward but not backwards. The most commonly applied techniques are *Fabry-Perot* filtering, that utilizes a mirrored cavity with a certain spacing to either enhance or destruct certain wavelengths, phase selective *diffraction gratings*, fiber *Bragg gratings*, that create a selective cavity by a periodically changing the refractive index within the waveguide, or arrayed waveguide gratings (AWG). An AWG comprises two star coupler. The first splits the incoming signal into an array of rectangular or square waveguides, each with a fixed length difference. This results in an phase difference at the second star coupler. This phase difference causes all input wavelengths to interfere differently depending on their respective wavelength. Hence on the second star coupler the different wavelengths are coupled into the eligible output port with respect to a certain center wavelength that remains unchanged in accordance with the length difference of the waveguides.
  Another technique, usable for switching or filtering, is called acousto-optic tunable filtering (ATOF). Unpolarized light is hereby splitted into two arms of orthogonal polarization. Acoustic waves, resonant to a certain wavelength, are superimposed

with both arms causing a polarization change that prevents extinction at the output splitter.

A final remark is made on Mach-Zehnder-Interfermeter based filters, that allow to select periodical passbands. A cascade of several MZ-filters can be used to specifically select a single wavelength. This techniques are used for wavelength division multiplexing (WDM) and add-drop multiplexing.

Today the most common network standard is optical Ethernet which refers to the bottom two layers of the OSI model, the physical and the data link layer. Each device is connected to this network with a 48bit MAC address and communicates with the transport unit frame, standardized in the Gigabit Ethernet specification (IEEE 802.3). The bandwidth ranges from 100-1000 Mbits/s depending on the transmission medium. The Ethernet network is distinguished according to its deployment range into Local Area Networks (LAN), Campus Area Networks (CAN), Metropolitan Area Networks (MAN) or Wide Area networks (WAN).

Depending on the amount of traffic a network is carrying the geometry of the network is planed accordingly. High data rates are routed through certain high populated ares as cities and the main connection notes between cities. These networks are referred to as *backbone network* that are able to transmit, rout, add or drop big amounts of data. Furthermore they are connected to smaller branches that allow to access these backbone networks, hence called *access networks*. Different scenarios for such access networks are possible and displayed in Figure 5.4. Here a point to point (PtP), point to curb (PtC) with cascaded multiplexer and point to multipoint (PtMP) connection with passive splitter is shown, each connected to the central office of the telecom provider that is connected to the backbone network.

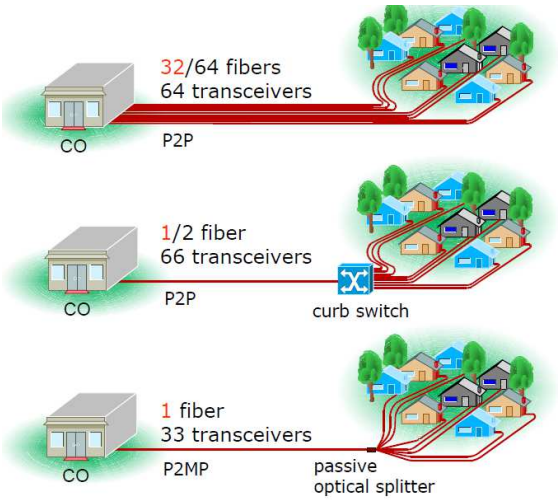

FIGURE 5.4: Possible Access network schemes. Source: [15].

Average access networks comprise between 32 and 64 users. While in metropolitan networks the transmission medium comprises almost exclusively optical fiber technologies, the access network still uses copper wire infrastructure available in most building for due to economical aspects. However, nowadays the movement towards all optical passive optical networks (PON) is clearly seen, especially in this last mile sector. In this case the data signal are shared between the CO, in technical terms called *optical line termination* (OLT), and the users, called *optical network units* (ONU), without any electrical devices. This reduces cost while increasing transmission speed. Most deployed PON networks can either be assigned to an Ethernet or an ATM based type.
In the first case, the Ethernet PON (EPON) standards are defined by IEEE 802.3. It uses an 8b/10b line coding [2] and operates at standard Ethernet speed. The corresponding properties and operation modes can be found in [88].
The ATM based PON is standardized according to the Full Service Access Network (FSAN), a group consisting of the most important telecom providers, test labs and equipment suppliers, in ITU G.983. It uses ATM as its layer 2 protocol. Further developments of ATM-based PONs lead to ATM PON (APON), broadband PON (BPON) and Gigabit PON (GPON) networks. The respective standards can for example be found in [89]

5.1.2 Second Generation Networks

Second generation networks evolved from the growing maturity of all optical components that are able to perform network services, such as routing and switching as introduced in the previous chapter, without any help from the electrical devices. The main part of this new generation of network is the ability to transmit high bandwidth on a single fiber using wavelength division multiplexing (WDM), i.e. the transmission of multiple spectrally separated user channels on the same optical fiber, performed in optical line terminals (OLT). Furthermore optical add drop multiplexers (OADM) allow to merge and divert single data channels into the data stream by individually selecting the respective wavelength. The routing and switching in this second generation networks is done by optical cross connects (OXC) that allow to connect different ports to rout data to its destination encoded in the respective header of the frame.
The use of these all optical components brought a new "optical layer" into the existing network technology. On this layer all optical packet and label switching is applied to handle requests from users with different protocols types and technologies (e.g. ATM

[2] The 8b/10b encoding scheme uses 10bits to transfer 8bits of information. This method allows to keep a long term DC balance due to the restricted numbers of "0"(negative current) and "1" (positive) allowed in a ten bit block. The number of "0"s and "1"s differs hereby only by maximally one. An excess of positive or negative current (disparity) is adjusted by the upcoming 10bit code block. In addition to this a clock recovery for the receiver is possible.

or SDH). This resulted in the commonly used general multi-protocol label switching (GMPLS) or multi-protocol lambda switching (MPLambdaS) protocols for resource discovery, state information dissemination as well as path selection and management.

5.2 Integration of QKD in Optical Networks

QKD experiments have shown that a secure key exchange is possible in free space, covering a range of about 144km at optimal weather conditions [90]. Furthermore with dedicated optical fiber a distance of 260km was reported in [91]. It has to be mentioned that in this case a specially customized low loss fiber is used. Although these results are economically unfeasible, the "average experiments" show that QKD is a technology ready for networks in the metropolitan range for distances up to 50km. In order to smoothly integrate QKD into existing infrastructure it has to be evaluated for which devices the necessity to bypass is given and where an integration is possible. The upcoming considerations have also been published in [16] and [17]. Figure 5.5 shows the schematics of backbone metro-network (a) with various adjacent access networks attached and a point to point QKD link between two users of the access networks. In the central node of the backbone network a QKD system can be operated while in the others trusted QKD nodes have to be applied to refresh the signal before routing it into the respective access network. In this left picture the QKD link is depict with fibers dedicated exclusively for single photons which allows a flawless operation of the key generation though by a very high cost. The schematics of (b) (c) and (d) in Figure 5.5 offer a different solution. In the first inset (b) the situation of an access network is shown. From the QKD node, the equivalent to the OLT, the single quantum signals use the same fibers as the classical signals. Due to the high loss the quantum signal bypasses the AWG in this case before it gets measured in the QKD receiver. The same scheme can be applied within the backbone network, as shown in insets (c) and (d). Here critical equipment, such as amplifiers and network nodes (that contain amplifiers, switches and AWG) have to bypassed while existing optical fibers can be shared with classical signals.

Considerations on how an integration of QKD in metro access networks could look like are given on the basis of three examples, shown in Figure 5.6. The first network (a) depicts a point to point connection of an 1 or 10G Ethernet with a dedicated fiber for each user, the second setup (b) shows an EPON, GPON or XG-PON/10G-EPON network with multiple multiplexed QKD signals and classic signals sharing the same fiber for the first 15km but splitting the into individual fibers for the last mile. This would represent a fiber to the curb approach, as seen in the previous chapter. In the last setup (c) a WDM PON and a WDM-TDM PON, respectively, is displayed. It is similar

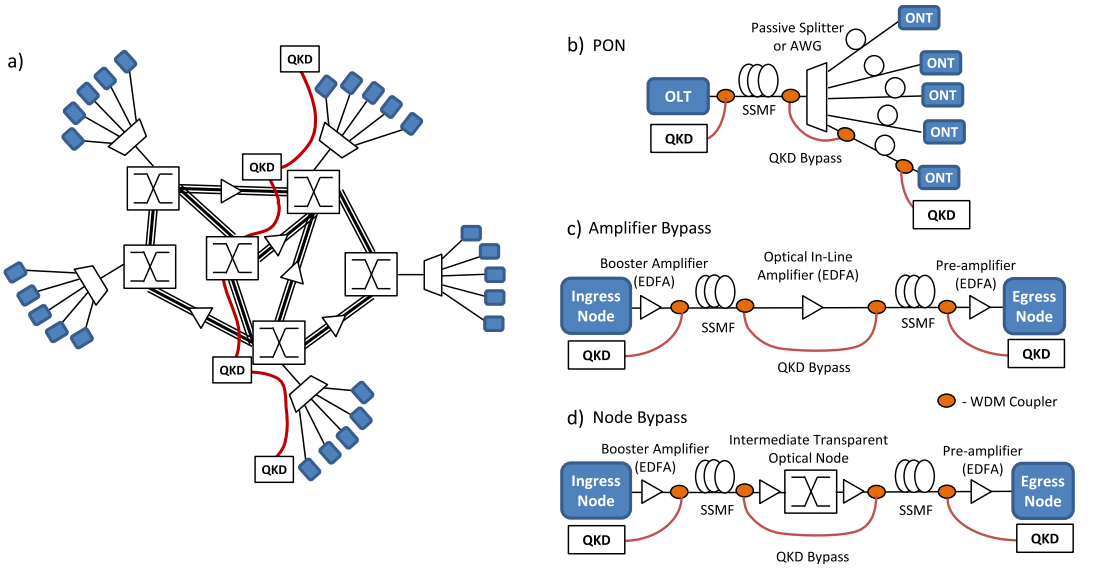

FIGURE 5.5: Schematics of possible integration scenario of QKD into PON networks. Source [16].

to the topology in (b) but with additional splitters for time and wavelength multiplexing.

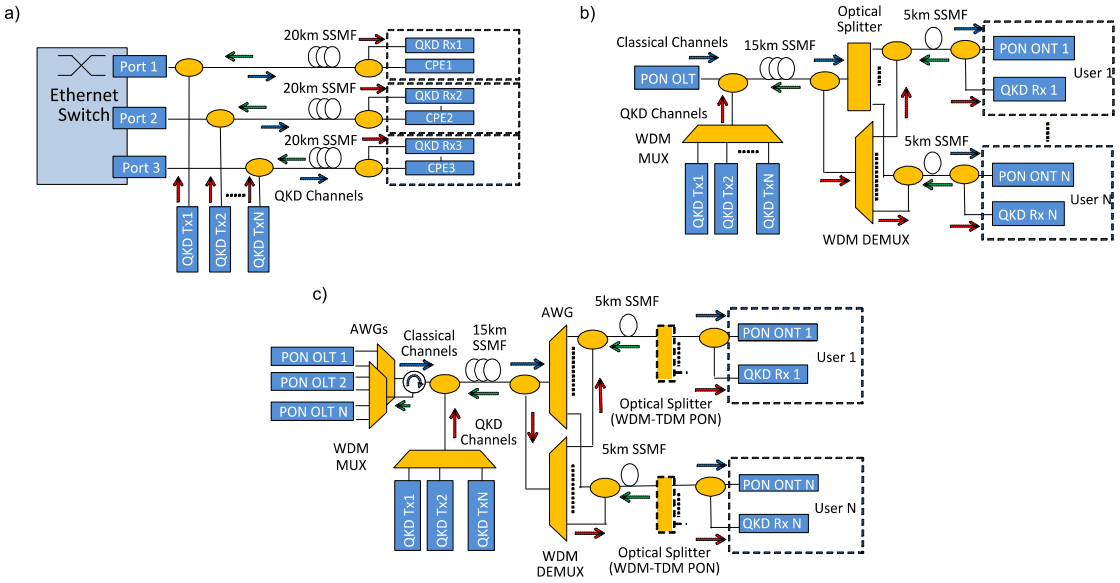

FIGURE 5.6: Schematics of possible integration scenario of QKD into PON networks. Source: [17].

When looking at the wavelength distribution of the respective access network standards it becomes apparent that most of the C-, L- and M-band is occupied by classical channels. In some older standards, like 1G EPON, also parts of the O-Band is occupied by upstream (US) data signals. The situation is summarized by the left side of Figure 5.7. It has to be noted that point to point networks as well as EPON and GPON still use the O-Band, mainly for US data. Furthermore the right hand side of Figure 5.7 indicates

the noise originating either from the signals depict on the left side, i.e. from single C or O-Band channels, an optical supervisory channel (OSC) at 1510nm or a 40 Channel DWDM data channel all within a power range of -8dBm - 1dBm in a 20km SSMF [3]. In this Figure six windows are distinguished that are an available option for the quantum channel. However it becomes apparent that the generated noise photons exceed or equal the acceptable noise level (here 600.000 Photons/s· nm, indicated by the dashed red line) in most cases. Only in the case of WDM and TDM PON with channels exclusively in the C-Band the first four windows show a promising low background.

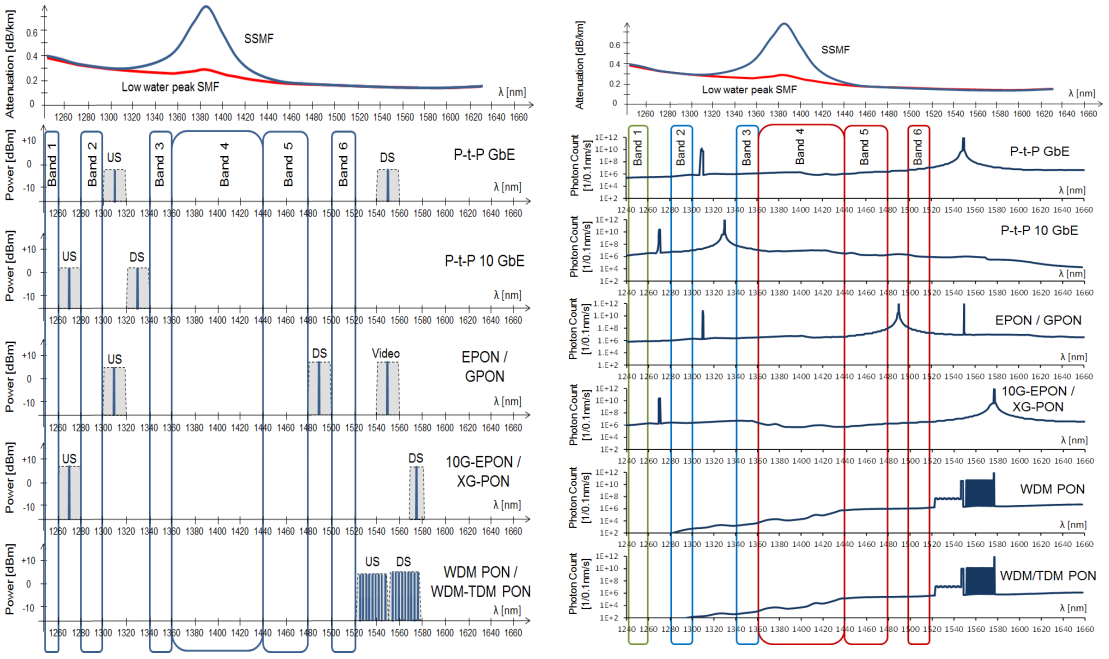

FIGURE 5.7: Left: Wavelength placement for most commonly used network standards. Right: Simulated noise spectrum for most commonly used network standards. Source: [17].

In order to get a first reference on how much the quantum bit error QBER and the key rates are affected by scattering effects of classical data channels, simulations with the respective setups of Figure 5.6 and 5.7 in the VPI software have been prepared. The key rate is received following the work of [92]. The raw key rate R_{raw} and the respective sifted key rate R_{raw} is given by

$$R_{\text{raw}} = (p_\mu + 2p_{\text{dc}} + p_{\text{AP}} + p_{\text{ram}} + p_{\text{ct}}) \cdot f_{\text{rep}} \cdot \mu_{\text{duty}} \cdot \mu_{\text{dead}} \tag{5.1}$$

$$R_{\text{sift}} = \frac{1}{2}(\beta p_\mu + 2p_{\text{dc}} + p_{\text{AP}} + p_{\text{ram}} + p_{\text{ct}}) \cdot f_{\text{rep}} \cdot \mu_{\text{duty}} \cdot \mu_{\text{dead}} \tag{5.2}$$

The rates in this case are calculated by looking at a single gating window of the detector and taking within this time frame the probabilities of p_μ, being a product of average

[3] The noise is caused by Raman scattering and will be investigated in more detail in section 5.2.1 and 6.1.1

photon number μ, fiber transmission t, detector efficiency η and internal loss at Bobs detector t_B. Futhermore p_{dc} denotes the probability of a measured dark count, p_{AP} the probability of an measured after pulse photon, p_{ram} the probability of a detected Raman photon and finally p_{dc}, the probability of a detected crosstalk photon. These added probabilities are then multiplied with f_{rep}, the pulse repetition frequency, μ_{duty}, the efficiency due to the detection duty cycle as well as the μ_{dead}, the detection efficiency due to dead time. For the sifted key rate R_{sift} a parameter β distinguishes the protocol types BB84, where $\beta_{BB84} = 1$ and SARG, where $\beta_{\text{SARG}} = \frac{2-V}{2}$, with V denoting the respective visibility. For the sifted key rate the mutual information between Alice and Bob $I(A:B)$ and Alice and Eve $I(A:E)$ has to be taken into account:

$$R_{\text{sec}} = R_{\text{sift}}(I(A:B) - I(A:E)) \tag{5.3}$$

The mutual information $I(A:B)$ and $I(A:E)$, respectively, is hereby defined per bit, while the latter has to distinguished between BB84 and SARG. It yields

$$I(A:B) = 1 - \nu_{ec} H \tag{5.4}$$

$$I(A:E)_{BB84} = \frac{1 - \frac{\mu}{2t}(1 - H(P)) + \frac{\mu}{2t}}{1 - \frac{2p_{dc}}{\mu t \eta}}, \text{with } P = \frac{1}{2} + \sqrt{D(1-D}} \text{ and } D = \frac{1-V}{2 - \frac{\mu}{t}} \tag{5.5}$$

$$I(A:E)_{SARG} = I_{pns}(1) + \frac{1}{12}\frac{\mu^2}{2}e^{-\mu}(1 - I_{pns}(1)), \text{with } I_{pns}(k) = 1 - H(\frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{1}{2^k}}), \tag{5.6}$$

where H(p) is the binary entropy, as defined in 2.1, ν_{ec} being the percentage lost error correction (in the case of Shannon limit $\nu_{ec} = 1$). Furthermore the QBER is given by $QBER = \frac{\text{false counts}}{\text{right + false counts}}$. This means in more detail

$$QBER = \frac{1}{2} \cdot \frac{p_\mu(1-V) + 2p_{\text{dc}} + p_{\text{AP}} + p_{\text{ram}} + p_{ct}}{\beta p_\mu + 2p_{\text{dc}} + p_{\text{AP}} + p_{\text{ram}} + p_{ct}} \tag{5.7}$$

The values received from the simulation results, shown in Figure 5.7, are inserted in the above formula for QBER and secure key rate and displayed in Figure 5.8. It shows key rates over wavelength in an access networks with a 20km fiber link. For reference, the Shannon limit is displayed as a red dashed line to indicate the maximal QBER and key rate. The graphic shows that for EPON/GPON as well as for 10G-EPON/XG-PON both with classic signals in the O-Band the high QBER does not yield a secure key. Only in the case of WDM-PON and PtP GbE, respectively, a secure key rate can be extracted for wavelength between 1280nm - 1360nm and 1320nm - 1360nm, respectively. Other wavelength at around 1400nm are only possible in LWPF. Furthermore the simulations show the improvement of the SARG protocol (green line) over the classic BB84 (blue

line) in terms of key rate and QBER, especially in the WDM PON. When we consider

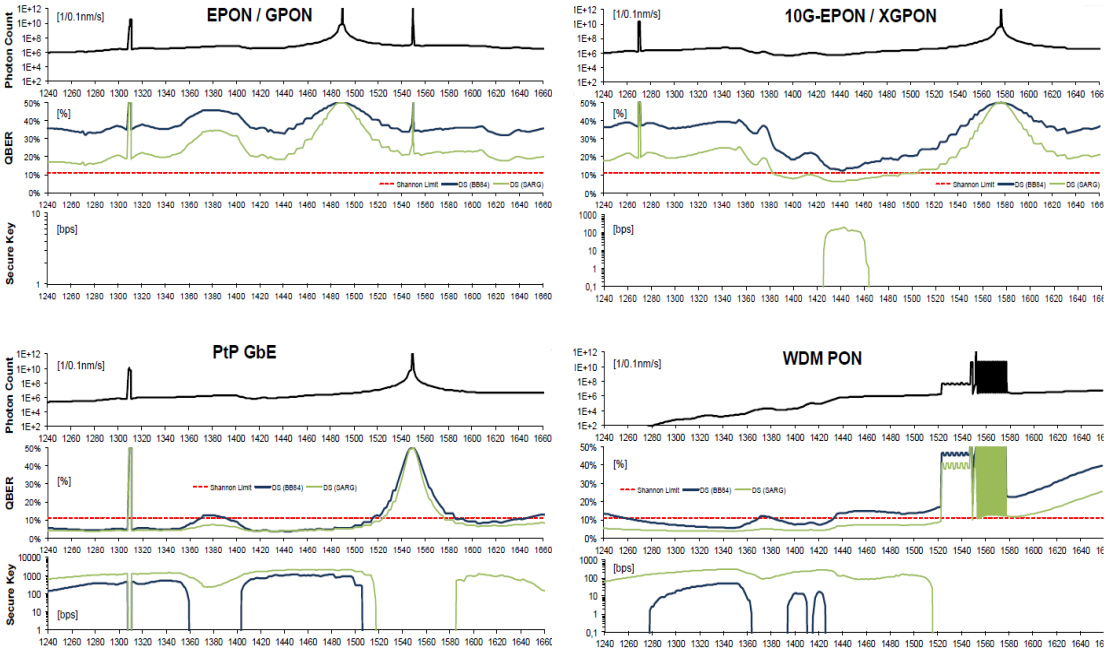

FIGURE 5.8: Simulations of QBER and key rates for different PON access networks for 20km SSMF. Source: [16].

the situation in a metro, backbone network with more data channels in the C-Band as well as the amplifier and node bypass scenario as shown in (c) and (d) of Figure 5.5 the simulations show that only for distances lower than 30km a secure key rate can be expected. For a point to point DWDM network with 40 data channels the noise and key rate for various inputs can be seen in the first row of a), b) and c) in Figure 5.9. Only wavelength below 1360nm show a acceptable noise and lead to a secure key. Similar results are given for amplifier (second row of a),b) and c)) and node bypass (third row of a), b) and c)).

When summarizing the results of the simulations it becomes obvious that the quantum channel is occupied by noise photons arising nonlinear effects, such as Raman, Brillouin, Four-Wave-mixing, etc. that produce noise photons in a vast spectral range around its origin. Since networks standards are mitigating more and more into C-, L- and - Band it might seem like a natural move to locate the quantum channel in the O-Band where the simulations showed some promising results. It has to be noted that a higher attenuation lowers the SNR ratio of the quantum channel in this wavelength and might therefore compromise the advantage gained through the large spectral distance. However, in this work an allocation of the quantum channel in the wavelength range around 1310nm is still preferred due to the fact that attenuation is a more acceptable obstacle than high amounts of scattered photons. Furthermore it has to be noted that critical optical equipment, such as network nodes, amplifiers of any kind and AWGs, have to be bypassed.

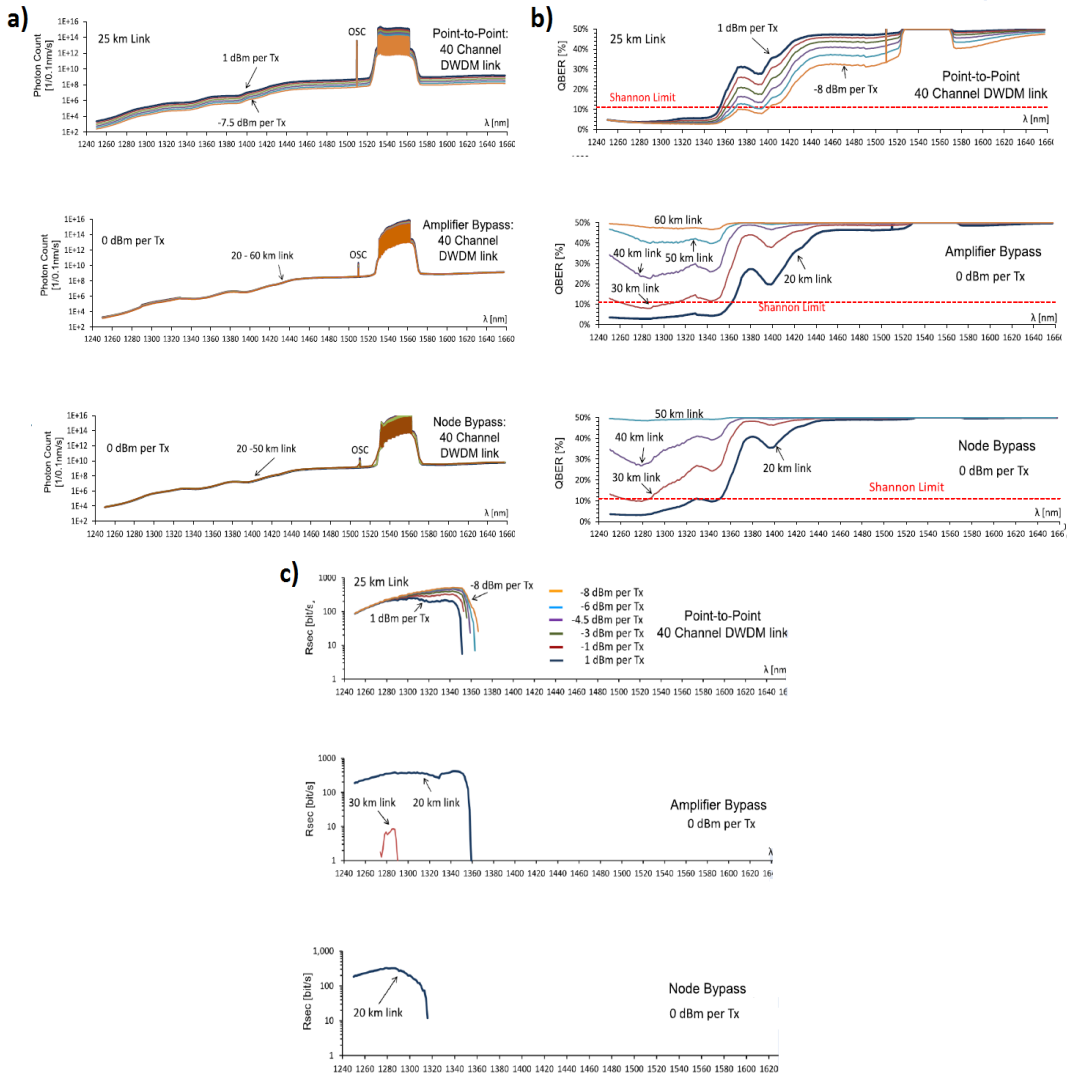

FIGURE 5.9: Simulations of noise (a) QBER (b) and key rates (c) for metro networks, node bypass and amplifier bypass with various fiber length. Source: [16].

Additional coupling loss has to be added in this case. Simulations on this matter are discussed in 6.1.1.4.

5.2.1 Impairments due to nonlinear Effects

This chapter gives a quick introduction to nonlinear effects in optical fibers. It will address the most important impairments for the quantum channel and discuss the presumable threats.

Scattering processes can be divided into elastic and inelastic types. While in elastic scattering the entire energy is transferred from one object to the other, inelastic scattering allows energy to be leaked into the environment. For fiber optic scattering this

discriminates the wavelengths of the scattered photons. This means that for elastic scattering the wavelength of the scattered photon is equal to the pump photon, while in the inelastic case scattered photons can have a large wavelength bandwidth. The three main scattering types are compared in Table 5.2 with respect to their origin, i.e. where an incoming photon is scattered, direction/orientation of the scattered photon as well as possible countermeasures applied in the classical and quantum domain to avoid impairments from the scattered photons.

Name	**Raman**	**Rayleigh**	**Brillouin**
Origin	Optical phonons	Dipole interaction with small objects (w.r.t. wavelength)	Acoustic phonons
Scattering type	Inelastic	Elastic	Inelastic
Orientation of scattered photons with respect to pump	No Orientation	Co- and counter-propagating	Co- and counter-propagating
Countermeasure for channels	Isolators, Amplify data channels	Isolator	Isolators
Countermeasure for quantum channel	Narrow time and wavelength filtering	Restricts a certain wavelength	Restricts certain wavelengths, wavelength filtering

TABLE 5.2: Comparison of the scattering types in optical fiber

The three scattering types have its origin in thermal material fluctuations that cause the SiO_2 of the optical fiber to expand and compress and the refractive index to oscillate. On the molecular level this results in two vibrational modes of the lattice structure of SiO_2, that comprises two atoms with different masses. When Si and O atoms oscillate in phase it is referred to as an *acoustic phonon*, while when the two atoms oscillate out of phase, an *optical phonon* is given [93]. As for Rayleigh scattering the incoming photon is absorbed and a scattered photon with the same wavelength is emitted it can be seen as a simple interaction with the atom or the molecule itself. While in the Brillouin scattering process, the incoming photon either absorbs an acoustic phonon, resulting in a shorter wavelength scattered photon (Stokes case), or creates an acoustic phonon, resulting in the emission of a longer wavelength photon (Anti-Stokes case). Hence two scattering regions can be defined around the central Rayleigh line.

Raman scattering on the other hand is the interaction of incoming photons with optical phonons. The classical theory of induced electric dipole moment in matter, P, by an incoming electric field $E = E_0 \cdot cos(2\pi\omega t)$ with the vibrational mode ω_1 of the material

and its polarizability $\alpha = \alpha_0 + (\frac{\partial \alpha}{\partial x})x$ is given by $P = \alpha \cdot E$. The polarizability α comprises hereby the vibrational mode of the molecule at frequency ω_1, $x = x_{\omega_1} cos(2\pi\omega_1 t)$. Simplifying and applying trigonometric rules yields

$$P = \underbrace{\alpha_0 \cdot E_0 \cdot cos(2\pi\omega t)}_{\text{Rayleigh scattering}} + \frac{1}{2}(\frac{\partial \alpha}{\partial x})x_0 E_0 \Big(\underbrace{cos(2\pi(\omega + \omega_1)t)}_{\text{Anti-Stokes Raman Scattering}} + \underbrace{cos(2\pi(\omega - \omega_1)t)}_{\text{Stokes Raman Scattering}} \Big). \tag{5.8}$$

The first part yields a wave with frequency equal to the incoming field, hence an elastic scattering, while higher order give the Stokes and Anti-Stokes terms of the Raman process. Figure 5.10 depicts the theory of Raman and Rayleigh scattering in a simple way. Molecules are either in the ground or an excited vibrational state. By absorbing incoming photons higher vibrational states are induced in the materials that either fall back to the first vibrational state causing a lower energy photon (Stokes scattering) to emit or are further excited to an even higher vibrational state and return to the ground state while emitting a higher energy photon (Anti-Stokes scattering)

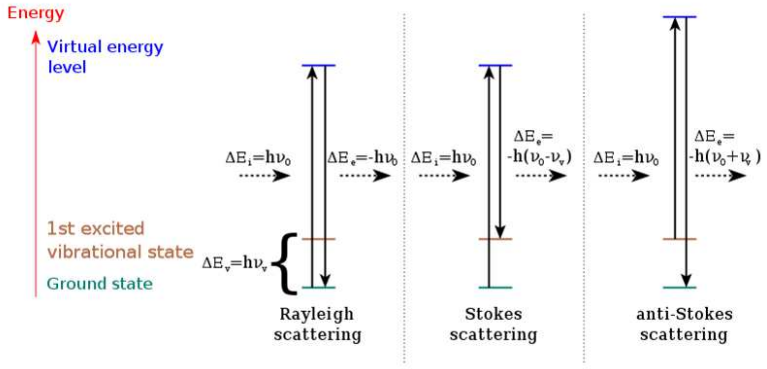

FIGURE 5.10: Simple theory of Raman scattering. Source: Slashme, CC BY-SA 3.0

A more precise quantum mechanical model of Raman scattering has been developed to exactly predict how excited vibrational states are thermally populated. This approach, however, goes beyond the scope of this work. For more details it is referred to [94] and various available scripts, e.g. [95]. It can be deduced from this theoretical approach that Raman scattering is about $10^{-3} - 10^{-4}$ less intense than the Rayleigh photons and also of lower intensity than Brillouin scattering. However due to its long spectral tails Raman scattering emits photons in wavelengths tens of THz away from its origin.
Other nonlinear effects, such as 4-wave-mixing or Kerr effect are third order effects that are neglected in this work, since their intensity is several orders of magnitude lower than the introduced scattering processes.
In the next chapter the simulations are tested by experimental setups that measure the

noise emitted by classical signals and hence the impairments an integrated QKD will face.

Chapter 6

QKD in passive Optical Networks

In this chapter the potential integration of an entanglement based QKD system into previously introduced network infrastructure will be discusses, based on recent work in the field as well as impairment measurement on a 20-channel Metro network. In order to bring QKD from a laboratory setup to a commercial application two possible approaches seem to be reasonable roadmaps. The first approach involves the usage of additional fiber, dedicated exclusively for QKD signals, so called *dark fiber*. This however is associated with high additional costs in fiber deployment and maintenance and might in some cases result in an entire restructuring of access networks and last mile infrastructure, since copper wiring has to be entirely replaced by optical fiber. Following this approach it is likely that QKD will be reduced to a few dedicated links but will not be able to become the standard technology for private communication. Similar to the approach to distribute keys via satellite it will be limited to few users.
In order to enable a broad market it is crucial for QKD to adapt to the existing telecommunication infrastructure and become a technology that is cheap and easily accessible for a wide range of users. The first steps towards such an integration is done by investigating the impairments of the quantum channel when using it alongside with classical signals. This chapter determines the major obstacles, the goals and the current limitations of such an approach. The results have also been published in [18] and [96] and presented at CLEO Europe in 2015 and SPIE Photonics Europe in 2016 as well as at QCrypt, international conference on Quantum Cryptography, in 2013 and 2014, see Appendices B and C.

6.1 The Coexistence Scheme

As most QKD scenarios so far involve a two party scenario the obvious approach is to establish a point to point link between Alice and Bob. Further networks topologies on

quantum level are so far only designed for research purposes and far from becoming a deployable technology, since they either involve routing of photons, i.e. swapping entanglement with the help of repeaters, or multi-partite entanglement between several photons. Both technologies are not yet mature at the time of writing. The key rates and distances that can be achieved when a dedicated quantum channel is used compared to a coexisting approach is illustrated by Figures 6.1 and 6.2. Both Figures summarize promising results published in recent years and show a significant drop in key rate and distance, respectively, when the quantum channel is shared with classical channels.

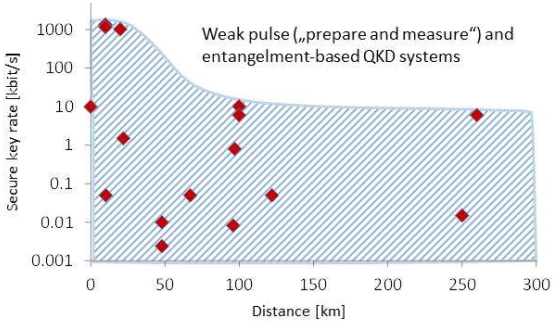

FIGURE 6.1: Key rate over distance of experimental QKD systems using weak coherent pulses or entanglement with dedicated dark fiber. Source: [17].

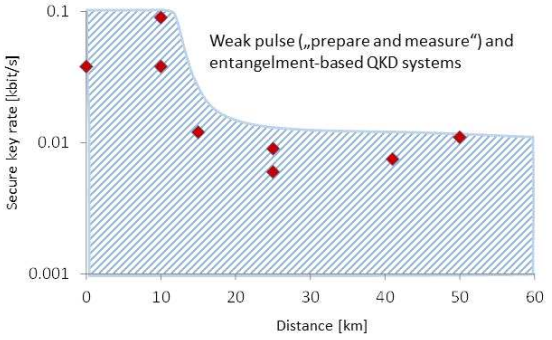

FIGURE 6.2: Key rate over distance of experimental QKD systems using weak coherent pulses or entanglement in coexistence experiments. Source: [17].

Coexistence schemes can be divided into time- and wavelength-multiplexed techniques. The first case however reduces the key rates of the classical channels as well as the quantum channel but allows on the other hand further distances, since the impairments are lower as in the wavelength-multiplexed case. The chosen type of multiplexing depends mainly on the practical application of the network, whether high bandwidth or high key rates are needed. Since so far all results from coexistence experiments partially recorded in the upper graph are drawn from setups where classical channels have been attenuated or shut off to increase the eligible key rates, no real answer can be given which technique is best suited in a given situation. Therefore this work focuses on exactly this question by evaluating noise and impairments on the quantum channel originating from various combinations and power levels of classical network signals. The main part will deal with

the wavelength division multiplexing of quantum and classical signals, but also results on time division multiplexing will be given and discussed. The gathered results and considerations on this matter can also be found in [17] and [18].

When contemplating the infrastructure of a backbone network with its respective branch, the access network for users, a favored way of integrating the quantum channel is to add only parts that are needed unconditionally. Figure 6.3 shows how such a minimal integration could look like. This means in the specific case that a DWDM node has either be completely bypassed or at least its booster amplifier. The same holds for inline- and pre-amplifiers that quantum signals can not survive.

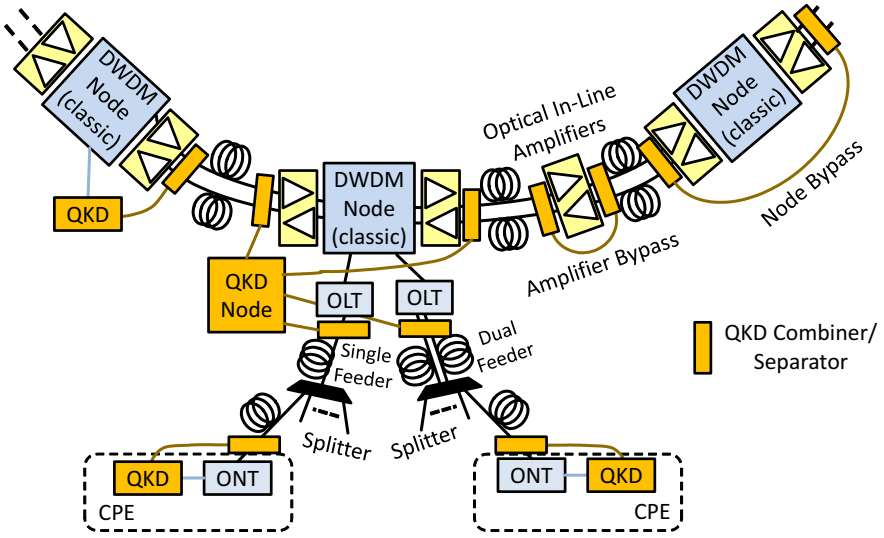

FIGURE 6.3: Schematics of a coexistance Scheme for backbone and access network. Source [18].

This circumvention is realized by a separator - combiner unit that allows to divide and merge the quantum from the classical channels, as shown in Figure 6.4.

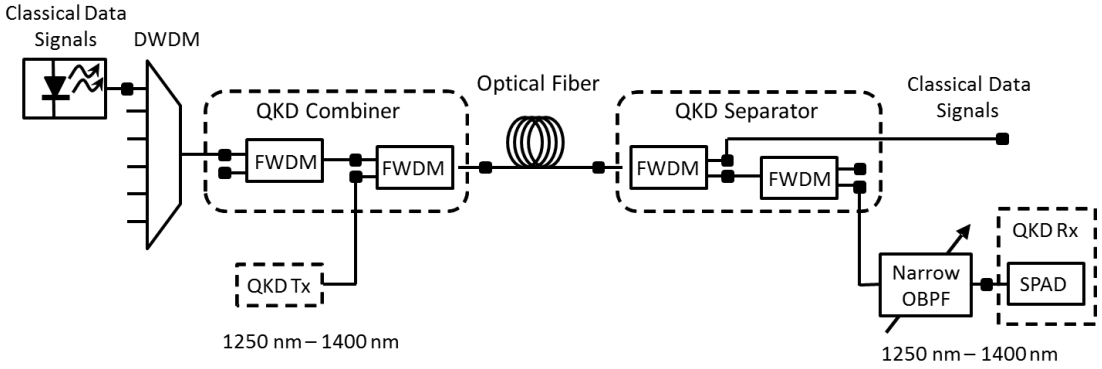

FIGURE 6.4: Combining and Separating quantum and classical channels for bypassing critical telecommunication equipment. Source: [18].

First measurements showed that a cascade of two Far-Wave-Division-Multiplexing (FWDM) filters are needed to cleanse the quantum channel before classical and quantum signals

are launched into the fiber as well as afterwards when separating them again. The attenuation curves of such FWDM filters are displayed in Figure 6.5. The first two FWDM are used to clean laser sidebands and scattering effects arising from those, while the two FWDM after the fiber are needed to suppress the Raman photons created within fiber. This filter can be seen as a high- or lowpass filter depending on the used exits. When assuming that the classical signals are mainly located in the C-band, the O-band is a promising candidate for the quantum channel. A majority of nonlinear effects in fiber are avoided in this wavelength range.

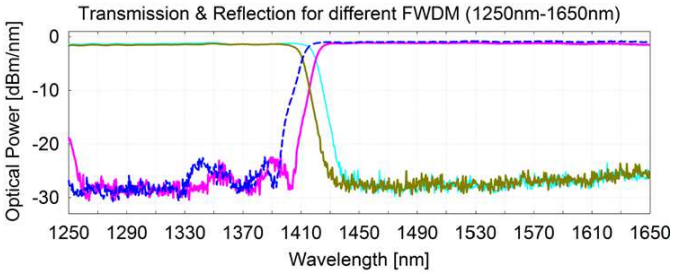

FIGURE 6.5: Attenuation curves of the used FWDM filters

Although quantum and classical channels are separated 200nm huge detrimental impairments could still be observed on the SPAD. Since photons in this spectral range can only be caused by Raman scattering and nothing else, see Table 5.2 in chapter 5, other types of impairments can be neglected. In order to determine how strong these effects are for the respective wavelengths a combination of OSA and SPAD measurements have been taken to analyse the scattered photons down to the single photon level. The DWDM in the top left of Figure 6.4 is hereby used to combine different classic signals. Regarding the theory of Raman scattering, the interaction length, i.e. the length of optical fibers, should influence the number of scattered photons. Furthermore the Anti-Stokes photons are expected to be created in fewer numbers compared to the Stokes photons, since they are statistically more unlikely. In the next chapter these assumptions are experimentally tested.

6.1.1 Raman Scattering - The Showstopper for Coexistence?

6.1.1.1 Raman Scattering of a single Source

A rough estimation on how much noise can be accepted by a QKD system the work of Aleksic et al. [16] gives a first approach with a simple calculation. A weak laser source of a repetition rate of 10MHz with an average photon number of 0.1 per pulse is considered. Assuming further a single mode fiber of about 50km length (15dB attenuation), the SPAD is expected to receive slightly over 30000 photons. With a 10MHz gating

and an opening window of 5ns, 50ms effective opening time is given within a second. If we assume an tolerable QBER of about 10-11% (depending on the eligible protocol the QBER varies between 10 and 20%) as for common prepare and measure protocols 3000 noise photons can be tolerated during detector opening time. This yields about 600000 noise photons (for 1550nm this is about -101dBm).

In order to get a reference on how strong the Raman photons can be expected, a single classical signal at 1550.12nm, a common DWDM wavelength channel, is launched into fibers of 14 and 17 km length. A tunable cw laser (New Focus) with variable power output was used for this purpose. The sidebands of the laser have been suppressed by a DWDM filter. The measured input power in front of the fiber was measured to be 3.8dBm. For different fiber lengths the results shown in Figure 6.6 have been received. Each Raman curve is actually composed by two curves. For lower wavelengths (about 1250-1400nm) the OSA is not sensitive enough to detect the scattered photons. Hence in this case the filtered output of this device was connected to SPAD. For higher wavelength the spectral power of the Raman photons could be directly measured with the OSA. The measurement setup is the same as already displayed in 6.4. It has to be noted that the two curves, measured by OSA and SPAD can only be smoothly connected when the loss of all optical components is subtracted in such a way that the two scales coincide. For this purpose a broadband white light source has been used to characterize the transmission of all components. The internal loss of the OSA has been determined by comparison with an external power meter and is subtracted for each measurement. Furthermore the quantum efficiency (QE) of the SPAD [1] has to be determined with respect to the scanned wavelength. The results of these measurements as well as the attenuation curves of the used fibers [2] can be found in Appendix A. These measurements determine the power originating from photons that are scattering in the same direction as the pump laser, the forward direction.
The next goal was to see if any advantage could arise, when the quantum channel is sent backwards through the fiber, i.e. counter-propagating with respect to the pump laser. The used setups are in this case similar to Figure 6.4. Figure 6.7 shows the slightly altered setup for weak signals, recorded with the SPAD, in the left picture. The right hand side includes a circulator, applied for measurement with the OSA at higher intensities. The results for different fiber lengths are shown in Figure 6.8.

It is interesting to see that for longer fibers, e.g. 12.8km and 14.3km fiber length the SPAD and OSA curves have a mismatch of about 3dB which has been confirmed by

[1] All measurements have been performed with a free running IDQ 220 single photon detector with quantum efficiency set to 5%

[2] In the experiments standart single mode fibers (SSMF) (ITU-T G652-B) and low-water-peak fibers (LWPF) (ITU-T G652-B) of different age and length have been applied.

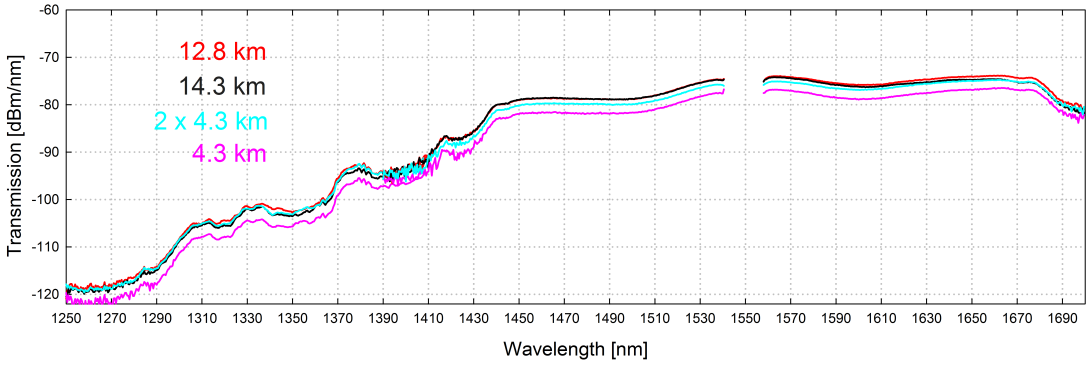

FIGURE 6.6: Measured power of forwards Raman scattering for various wavelengths originating from 1550.12nm pump with 3.8dBm. The gap at 1550nm is due to the filtering of the classical signal.

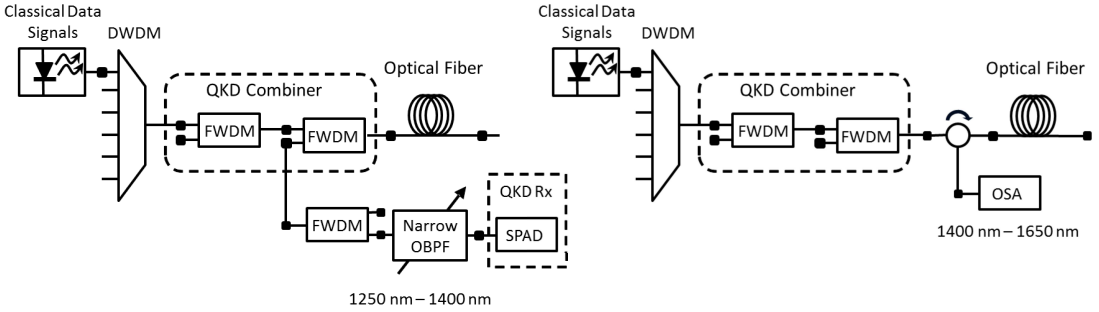

FIGURE 6.7: Left: Setup for low intensity measurement with SPAD at 1250nm to 1400nm. Right: Setup with circulator for measurement with OSA at 1400nm to 1650nm.

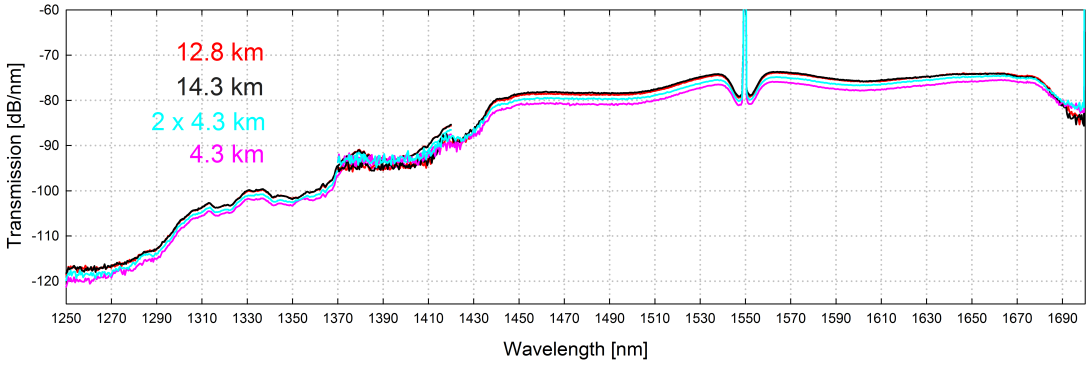

FIGURE 6.8: Measured power of backwards Raman scattering for various wavelengths originating from 1550.12nm pump with 3.8dBm

further measurements. Since this effect does decrease for shorter fibers and almost vanishes in case of 4km, it might be due to the higher attenuation of long fibers.
When comparing forwards and backwards direction of the Raman curves, i.e. Figures 6.6 and 6.8, no significant advantages of either scheme can be found. Hence a counter-propagating scheme of quantum and classical channels does not improve the integration. Furthermore the assumption, stated in the previous chapter that Anti-Stokes scattered

Raman photons are assumed to give a higher contribution due to statistical reasons that this process is more probably compared to Stokes scattered photons, has not been observed in these measurements. Therefore these measurements confirm on the one hand that an allocation of the quantum channel in the O-Band is the preferable choice on the other hand that co- and counter propagating schemes can for our purpose be treated equally.

6.1.1.2 Theoretical Model of the Raman Gain Curves

The simulation tool *VPITransmissionMaker* [97] was used to simulate the measured Raman curves. A GUI with given optical elements and measurement devices can be used to compose any network or measurement scenario. The software already comprises a the respective functions to measure Raman photons originating from scattering in optical fiber. However the default functions had to be adjusted to match the measured results. In order to created a new Raman gain profile the intermediate-broadening model as introduced in [98] is used. The Raman gain coefficient that depends on the pump power f_P and the frequency of the scattered photon with respect to the pump frequency δf, is hereby the crucial function that yields the strength of the scattered signal, RGC(f_P, Δf). The commonly used Raman gain curve is displayed in Figure 6.9 as the gray dashed curve, originally measured and published in [99]. It shows the Raman gain in $\frac{1}{W \cdot km}$ units over the frequency offset in THz. Originally this curve has been recorded with a 1500nm pump signal up to a frequency offset of 35THz. For modeling such a

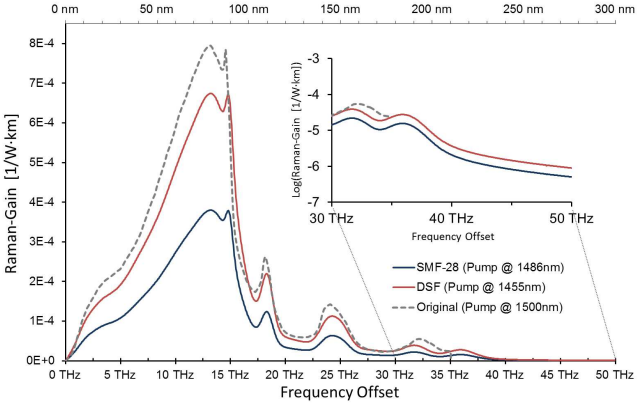

FIGURE 6.9: Raman gain curves for different pump wavelengths and fibers and parameters. Source [18].

curve with multiple peaks, that correspond to different vibrational modes a convolution of Lorentzian and Gaussian functions is needed. This time dependent [3] function is called Raman response function $h_R(t)$. When applying a Fourier transform on this response function the Raman model is shifted from time to frequency space and called Raman gain

[3] Also models with instant time response $\delta(t)$ exist.

function, $s(\omega)$. In this model, called the intermediate-broadening model, 13 vibrational modes are simulated with the response function. Following [98], it is given by

$$h_R(t) = \sum_{i=1}^{13} \frac{A_i'}{\omega_{\nu,i}} exp(-\gamma_i t) exp(-\Gamma_i^2 t^2/4) \sin(\omega_{\nu,i}) \Theta(t) \tag{6.1}$$

and hence the fourier transform, the gain function, yields

$$s_\omega(t) = \sum_{i=1}^{13} \frac{A_i'}{2\omega_{\nu,i}} \int_0^\infty exp(-\gamma_i t) exp(-\Gamma_i^2 t^2/4) \Big\{ \cos[(\omega_{\nu,i} - \omega)t] - \cos[(\omega_{\nu,i} + \omega)t] \Big\} dt. \tag{6.2}$$

The sum runs hereby over i vibrational modes with amplitudes A_i', frequencies $\omega_{\nu,i}$ and Laurentzian and Gaussian linewidth γ_i and Γ_i. Theta, Θ, in (6.1) denotes the theta-function, with 1 for $t \geq 0$ and 0 otherwise. When adapting these parameters correctly the measured Raman curves can be simulated with acceptable accuracy, as shown in Figure 6.10. The corresponding gain curves are shown in 6.9 (blue and red curve). In the linearly scaled inset the region of interest is shown, i.e. about 200nm away from the pump.

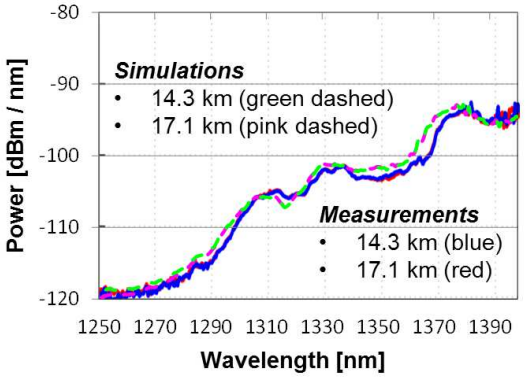

FIGURE 6.10: Raman gain curves for different pump wavelengths and fibers and parameters. Source [18].

6.1.1.3 Raman Measurement on a 20 Channel DWDM Network

The measurement so far revealed that even a single channel causes about -100dBm Raman photons in the O-Band which is, assuming that the rough noise estimation of 600k photons, made at the beginning of this chapter is true, already at the limit of impairments that the quantum channel can accept. However it has to be noted that the power in these measurement is denoted by $\frac{nm}{s}$. Given a sub-nm filter as well as a gated detector with a short opening time (here it is supposed that the arrival time of the photon pair is known), the measured power may be reduces adequately.

The next step is to determine how much more impairments a quantum channel is facing in the presence of a real DWDM network on the same fiber. For this purpose a 20 Channel DWDM backbone ring network has been prepared. A Lucent Wave Star OLS400G was configured for this purpose. By tapping of 99% of the signal and feeding 1% back into the respective node we were able to keep supervisory channel and EDFA running at each node and use the signal for Raman measurements. Figure 6.11 shows the setup of the network. The received signal comprises a residual pump signal at 1470nm (used for the EDFA in the network nodes), a supervisory channel (OSC) at 1510nm and the DWDM data channels [4] from 1530nm to 1579nm. The signals can be seen in Figures 6.12 and 6.13, labeled a, b and c, respectively.

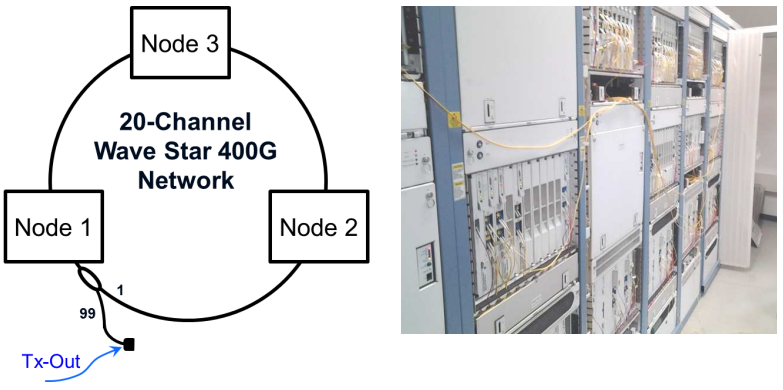

FIGURE 6.11: Left: Schematics of the DWDM ring Network. Right: Photo of the Network nodes

As previously the input signal is launched into the Combiner/Separator setup, shown in 6.4, again measured with SPAD and OSA and post-processed to fit the same scale. Various fibers with different lengths and age have also been used in this case. Figures 6.12 and 6.13, evaluate the Raman counts when the signal is launched alongside (forward) and in opposite direction (backward) with respect to the quantum signal the quantum signal.

Similar to the previous results no real advantage can be seen in either direction. Furthermore it is remarkable that compared to the single input evaluated in the latter chapter the Raman counts did not increase much. As a reference an one million threshold is indicated by the dashed gray curve.
In order to determine which signal causes the major part of scattered photons, four input signals are separately measured and compared. They are displayed in 6.14 and labeled I-IV.

The first signal (I) comprises the entire signal as it was used in Figure 6.12 and 6.13, the second signal (II) only the OSC (a CWDM is used to to suppress all other signals), the third (III) contains OSC and data channel (a FWDM with 1490nm edge is applied)

[4]The data channels are randomly modulated with a NRZ amplitude modulation.

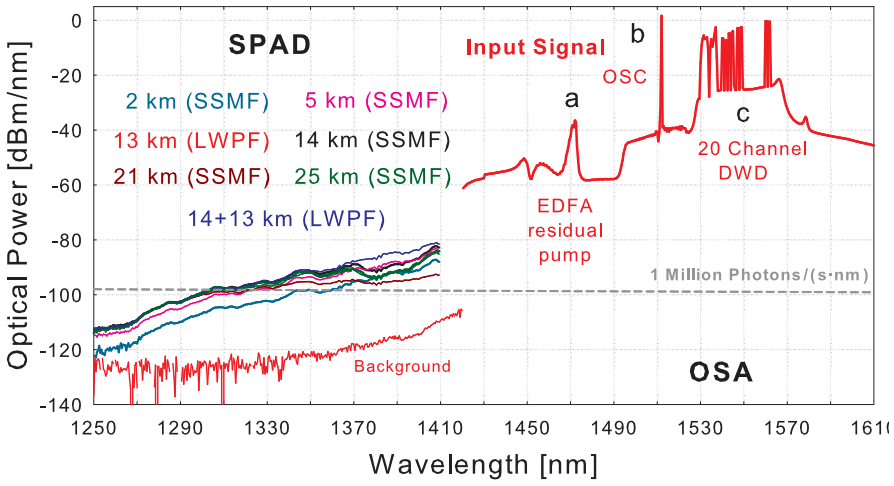

FIGURE 6.12: Forward Raman curves originating from residual pump, OSC and data channels for different fiber length

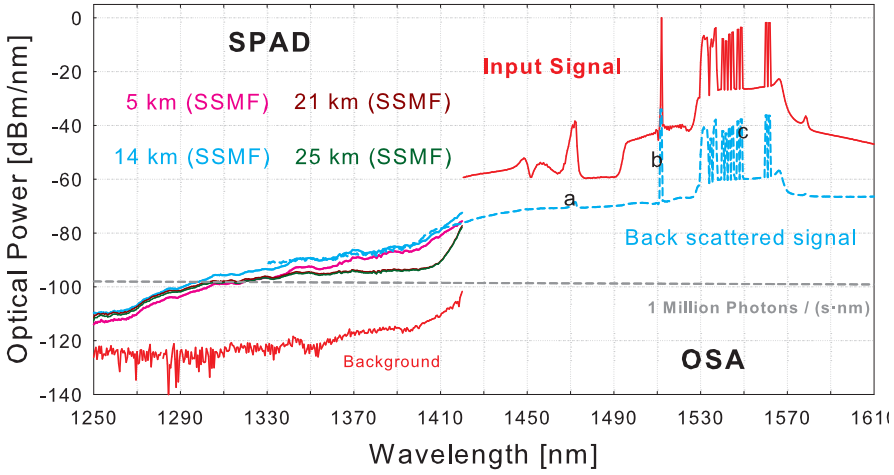

FIGURE 6.13: Backward Raman curves originating from from residual pump, OSC and data channels for different fiber length.

and the fourth signal (IV) provides OSC and and residual pump signal.

Figure 6.15 shows the contribution of the respective signals in a 14km SSMF. It is obvious that the weak residual pump signal gives not much contribution to the entire Raman curve when the red and black curve is compared. It is a little surprising to see that the contribution of the data channels strongly depends on the wavelength, since by comparing green and the black curve certain spectral regions are equal or almost equal (e.g. around 1290nm or 1340nm) while for other wavelength the data channels give an increase in scattered photon power of over $5\frac{dB}{nm}$ (e.g. at around 1320nm). When considering the theoretical background of Raman scattering it might be the case that higher energy pump photons of certain wavelengths correspond to certain resonances in Stokes and anti-Stokes scattering event due to quantized energy of the vibrational modes in SiO_2. This effect becomes even more dominant when we suppress the OSC

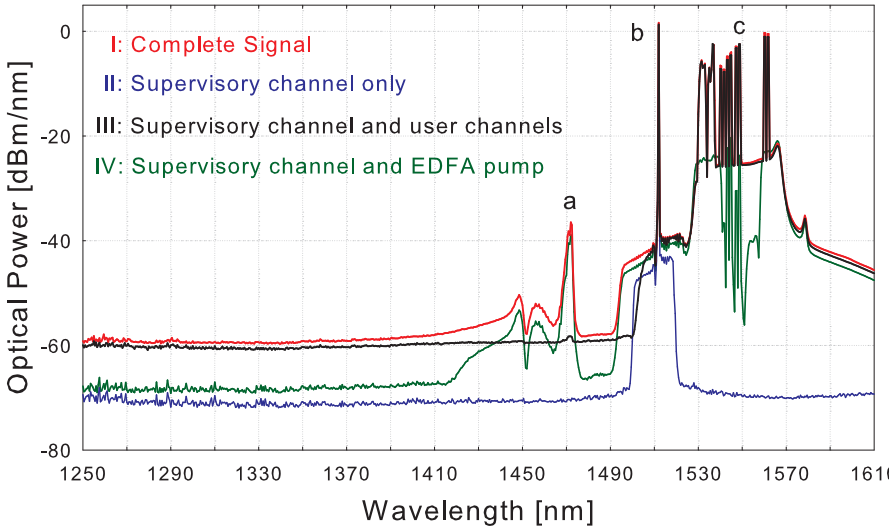

FIGURE 6.14: Four different signal for Raman curve measurements

and residual EDFA pump signal [5] and look at the Raman photons originating from the data channels only, as it can be observed in the brown curve of Figure 6.16. Here it even looks like OSC and data channel have an inverted behavior in the wavelength characteristics of the scattered Raman photons (brown and blue curve). The power of the impairments differs here up to $10\frac{\text{dB}}{nm}$. It might therefore be reasonable to arrange the classical channels at certain wavelengths or move the quantum channel away from certain resonant wavelength, respectively, to avoid a few dB of scattered photons.

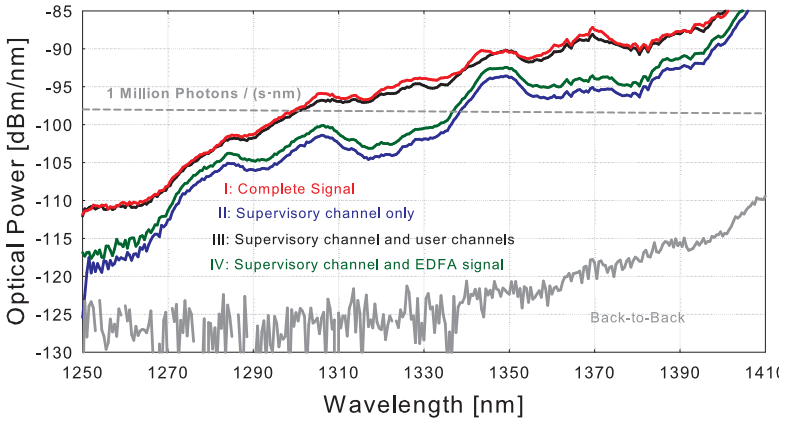

FIGURE 6.15: Raman curves originating from Inputs I-IV

[5] This is done by applying an FWDM with an edge at 1510nm that attenuates the power of the OSC by 35dB and the residual EDFA pump to lower than -90dBm

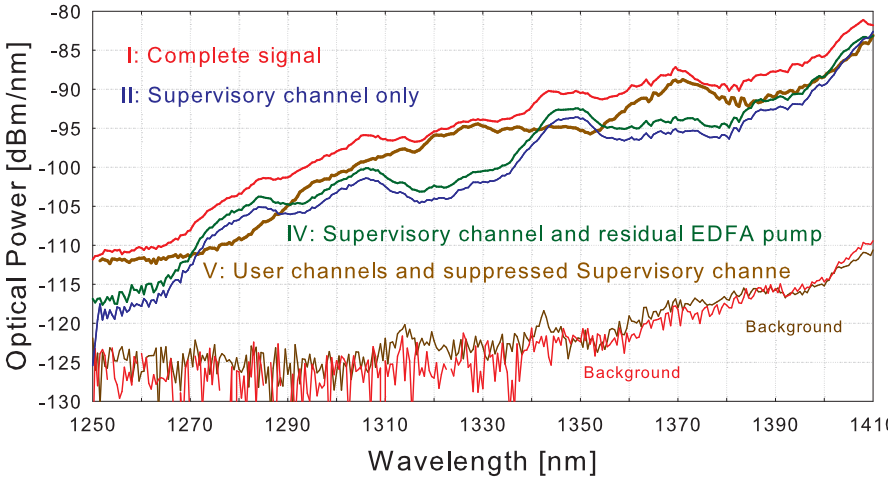

FIGURE 6.16: Raman curves originating from Inputs I, III, IV and the data channels only (brown curve)

6.1.1.4 Simulations of Node and Amplifier Bypass

Similar to chapter 5.2 simulations have been performed using the input signal of the 20 Channel DWDM network, as displayed for example in 6.14, 6.12 and 6.13 as the red line, the complete signal. The setups under consideration in this section are the node and amplifier bypass that have already been introduced in Figure 5.6 in (c) and (d), but are in more detail shown in 6.17

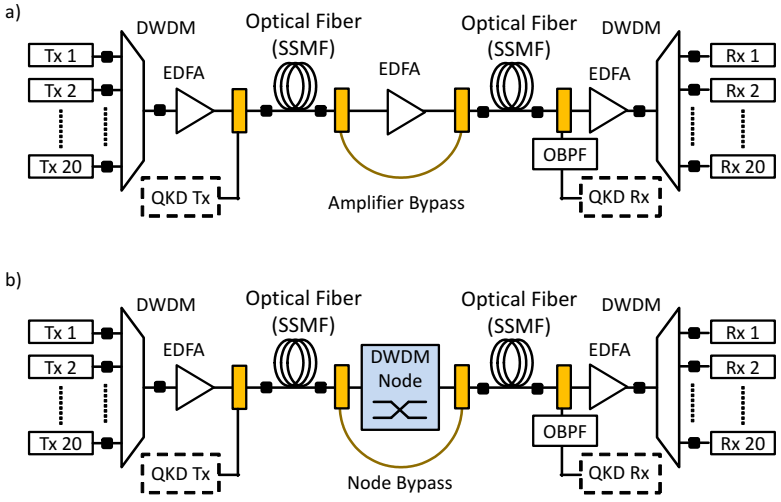

FIGURE 6.17: Schematics of amplifier (top) and node (bottom) bypass. Source [18].

Assuming a QKD integration into backbone networks with amplifiers and network nodes, additional loss has to be taken into account by establishing QKD bypass links for such critical infrastructure. The simulation results, shown in Figures 6.19 reveal that noise levels caused by an amplifier bypass is in general about 5dB higher as for a node bypass. Furthermore, a big difference is observed for 2x2.5km and fiber lengths of 2x5, 2x10km

and 2x 15km. The latter three do not differ much in their noise generation whereas in the short fiber a clear benefit is observed. In order to make the results comparable the previous results, the Raman noise of a 14km fiber with a single data channel is added to the plot as a red line. All shown in Figure 6.18.

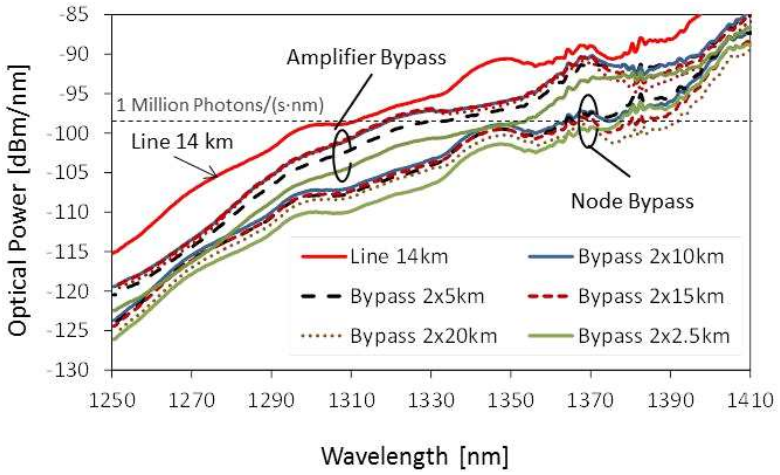

FIGURE 6.18: Simulated Raman impairments curves for amplifier and node bypass for different fiber lengths. Source [18].

Furthermore the attenuation of the bypass setup has been evaluated and is displayed in 6.19

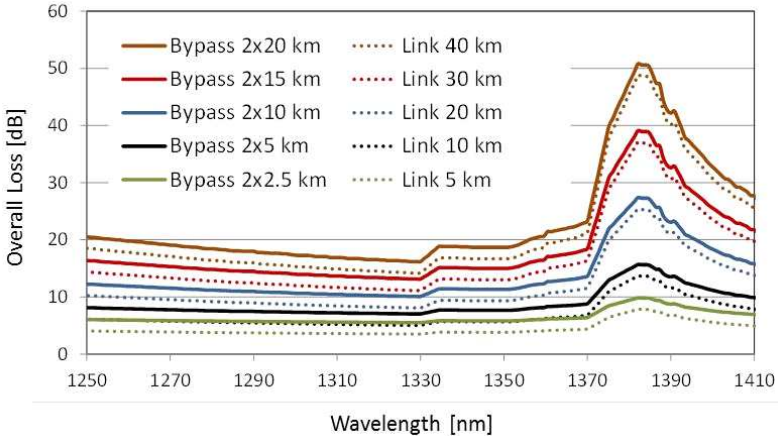

FIGURE 6.19: Attenuation for different bypass lengths with respect to wavelength. Source [18].

6.1.1.5 Discussion of the Results

The Raman noise measurements show in a deflating way how strong the influence of Raman scattering is even over several hundreds of nm away from the originating pump wavelength(s). When a single pump source is compared to multiple sources as it is the

case in the latter two chapters it also becomes apparent that the noise does not increase linearly with the number of sources. However, the input power of the respective source does strongly influences the number of created photons. This is the reason why several groups publish results with attenuated classical channels, see e.g. [100] or [92], to achieve higher key rates and distances. There is also no benefit to send data and classical channels in opposite directions through the fiber. We see, however, that shorter fibers (5km and less), show significantly fewer Raman photons, while impairments were measured strongest in 14km SSMF and LWPF, since here the interaction length is long enough and the fiber attenuation does not decrease the power as it is the case for longer fibers (20km and over). Although Raman impairment photons decrease significantly in the O-Band, when classical channels are present in the L-,C- and M-Band, for lower wavelength it has to be considered that also the number of photon from the QKD source are lost at such long fibers and hence no advantage is gained in this case.
On the positive side for a potential integration of QKD in optical networks, is the fact that filtering for the right photons in the wavelength and the time domain could reduce the high noise background. Very narrow wavelength filter below 100GHz may halve the impairments to an acceptable level. Another significant reduction can be achieved when reducing the detector opening time to the ns range, which would reduce the noise by 90dB, but lower the over all opening time and hence the key rate. In addition to this, the arrival time of the respective photons has to be known very precisely, i.e. in cm range of the optical fiber. In the upcoming chapter another time filtering approach is used made possible when applying the E92 protocol that uses entangled photon pairs for QKD. By tagging each photon with its respective arrival time a correlation peak can be found when post-processing the measured photons. Only matching pairs are kept and hence distinguished from noise photons.
In the upcoming chapters an entangled photon source in Sagnac configuration is introduced and characterized and afterwards integrated into a classical PON network with point to point data channels to measure its performance in the presence of Raman noise.

6.2 The QKD system - From the Source to the Key

6.2.1 Entangled Photon Source

In order to generate entangled photon pairs for a coexistance scheme some mandatory properties have to be fulfilled. Most importantly signal and pump have to be tailored in such a way that the idler fullfils a wavelength of 1310nm, well suited for the O-Band. As for the pump laser a well known cw 405nm is used, energy conservation dictates a signal wavelength of about 586nm. The diagonal polarized pump light is hereby guided

into the loop configuration, as shown on the left side of Figure 6.20 and focused into a periodically poled Potassium Titanyl Phosphate (KTP) crystal with a poling period of $\Lambda = 3.875$ μm. A polarizing beam splitter (PBS) in front of the loop splits the incoming diagonally polarized light into the left and right arm vertically and horizontally polarized, respectively. In order to trigger the type 0 down conversion in the KTP with horizontally polarized light a Fresnel-Rhomb is applied in the left arm in 45° configuration to change the angle between p and s polarization in such a way that after four total reflection within the Rhomb the vertical polarized light is changed to horizontally polarized. Since $\frac{\lambda}{2}$ waveplates can only be used to rotate a single wavelength, a Fresnel Rhomb is applied here suited for multiple wavelengths spectrally apart from each other. The right arm comprises the same Fresnel-Rhomb but in 0° configuration. Here linear polarized light enters and the angle between p and s polarization remains unchanged and the same polarization exits the Rhomb. The reason for applying this crystal is to compensate for the induced phase shift from the other crystal in the left arm due to its refractive index. Although the change in angle between p and s polarization of the incident beam depends on the respective wavelength and is therefore not entirely equal for signal, idler and pump wavelength, since the refractive index of the Rhomb depends on the wavelength. However, the difference from perfect linear polarization is acceptably small. In a similar matter the birefringent walkoff between the polarizations in the PBS is compensated by a piece of Calcite whose optical axis is rotated by 90° with respect to the splitter. A trichroic mirror (TM) is used in front of the loop to reflect signal and idler and let the pump signal pass. Afterwards a dichroic mirror (DM) is used to route signal and idler through their respective bandpass filters (F) and eventually couple them into optical fiber with suitable lenses (C). The emerging signal and idler photons are in the maximally entangled bipartite Bell state $|\Phi\rangle = |H_{586nm}\rangle\,|H_{1310nm}\rangle + e^{i\varphi}\,|V_{586nm}\rangle\,|V_{1310nm}\rangle$. In order to set $e^{i\varphi} = 1$, to receive the $|\Phi\rangle^+$ state birefringent wedges (BW) in front the loop are applied to control the phase of the pump laser. The schematics in 6.20 does not show that due to the elliptically shaped pump laser two cylinder lenses have been used to reshape the focus spot of the pump beam into a circular shape. Furthermore a polarization control and an isolator is used after the pump laser to avoid back reflected light into the laser cavity.

6.2.1.1 Entanglement Measurement and Visibility

The BB84 module

The created entangled photon pairs are eventually coupled into optical fibers and sent to the two parties, Alice and Bob, for further processing. Since 586nm, w.l.o.g. named Alice, is not suited for telecom purposes the photons would suffer a high attenuation in SSMF. Hence, they are sent, after a few meters of fiber with polarization control into the

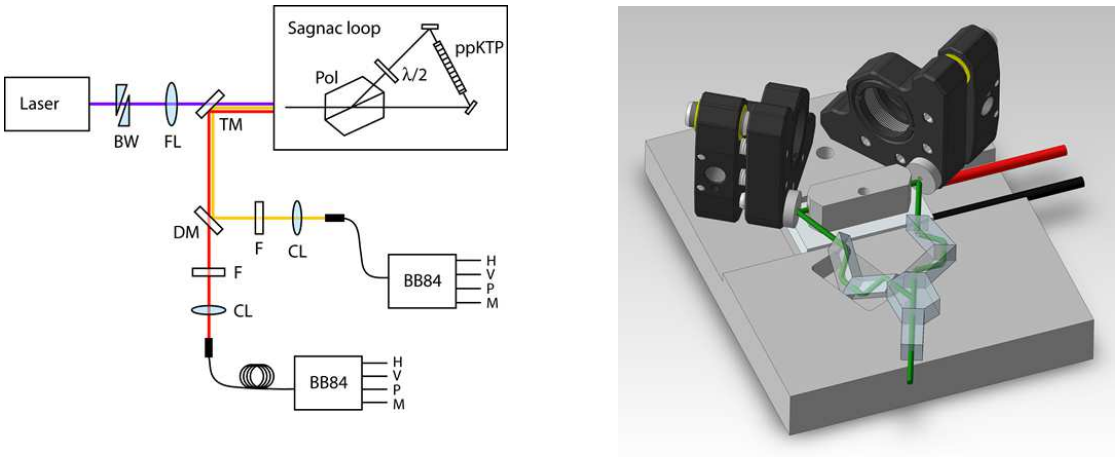

FIGURE 6.20: Left: Schematics of a Sagnac Loop for EPR pair generation. Right: The design of the loop itself with Calcite, Fresnel-Rhombs, PBS and the embedded KTP crystal. Source: AIT.

so called *BB84 module* that comprises freespace optics to measure the photons randomly in two non orthogonal bases, i.e. here H/V and +45/-45. Figure 6.21 shows the design and schematics of this module. The incoming photons are split into two paths and either measured in the H/V basis by a PBS or guided through a $\frac{\lambda}{2}$ and $\frac{\lambda}{4}$ (not shown in 6.21) waveplate that rotates the incoming photon by the +45° to be measured in the +/- basis. As it turned out the $\frac{\lambda}{4}$ is needed to compensate the elliptic polarizations caused by the beam splitter.

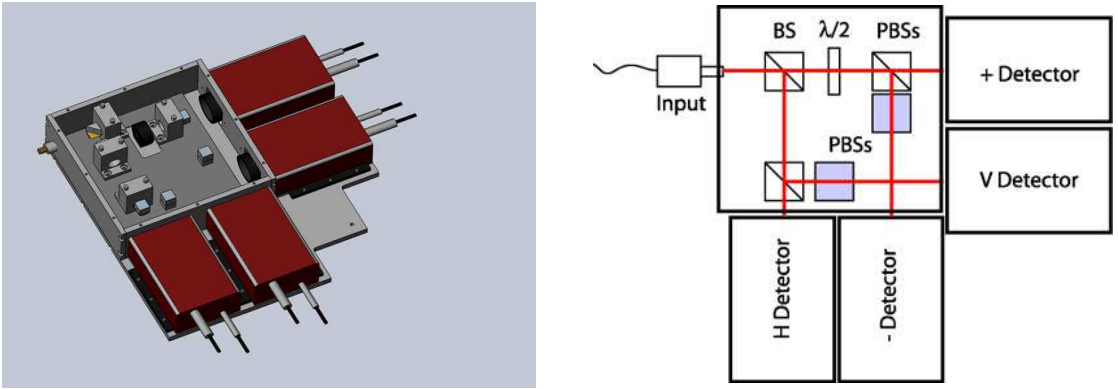

FIGURE 6.21: Left: CAD model of BB84 module with the four detectors. Right: Schematics of BB84 measurement optics. Source: AIT.

On Alice's side it was planned to use Silicon detectors manufactured by AIT itself during this project. Unfortunately the timing jitter of these detectors was to high such that the eligible photon pairs could not be unambiguously discriminated from noise by the post-processing. For further measurements a Perkin-Elmer Silicon SPDC measurement unit is used that comprises four slots suited for H/V and +/- measurement. It was therefore necessary to couple the photons again into a multimode fiber after the BB84 module is passed.

Time encoded measurement at Bob's

On Bob's side the same BB84 module is used. In this case, however, standard telecom equipment can be used such that all parts can be realized in optical SSMF. Again a polarization control is connected after coupling the photons into the fiber. Hereafter a fiber BS guides the photons into the two measurement bases. Similar to the Alice case an additional polarization control (PC) is applied in the +/- base to correct the polarization rotation due to the optical components. Since Bob in this scenario is considered to be the receiver of classical data and quantum channel it is therefore economically reasonable to lower the equipment cost by lowering the number of critical devices. Since InGaAs SPDC for infrared wavelengths are expensive and have to be operated at low temperatures of about -50°, the approach has been chosen to measure the two bases H/V and +/- by time-encoding the incoming photons. A fiber bound PBS with different fiber lengths at each exit separates H and V as well as + and - measurements by a timing constant τ. The distinction of the bases itself is given in the same way, namely by adding additional fiber and hence devide them temporally with 2τ. With this approach all four measured photons, guided in four SSMF are merged to a single multimode fiber that is connected to a single free running SPAD detector, a IDQ220. The setup of the BB84 as well as the schematics of the time encoded measurements are shown in Figure 6.22.

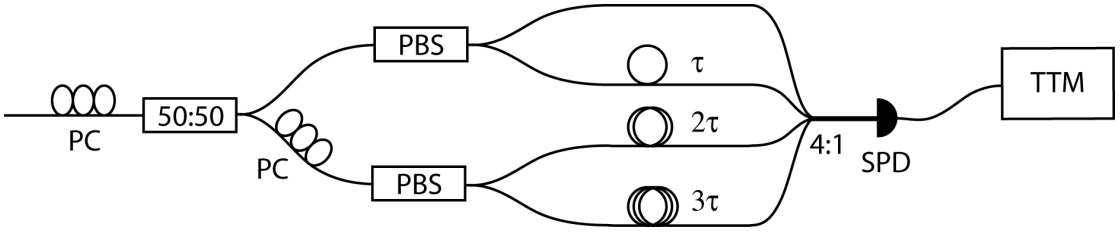

FIGURE 6.22: Schematics of BB84 measurement with the time multiplexed encoding for a single SPDC.

All detector counts from Alice as well as from Bob are collected by a time tagging module (TTM) that provides a maximal resolution of several tens of picoseconds. The TTM software is able to display a histogram of delay time slots of the incoming photons. Whenever two photons arrive in the same time slot a photon pair is counted. Figure 6.23 shows an entanglement measurement with the respective histogram. In the left pictures the HH and VV correlation is shown while in the right picture the ++ and – coincidences are maximized using polarizers after the dichroic mirrors in the source. Unfortunately the expected quality, i.e. a visibility of over 95%, of the source could not be reached. The reason for this still remains unclear, but it is assumed that due to positioning the birefringent wedges not in or close to the focus point of the pump laser the correct phase could not be applied. The visibility of the diagonal basis only being 85,38%, while in the horizontal/vertical base a value of 96,68% could be obtained, would support this assumption. An average visibility of 91,12% is hence the benchmark

of the source. These values have been measured with a free running IDQ 220 at Bob side with quantum efficiency set to 15% and four PerkinElmer detectors with an estimated quantum efficiency of 45%. False coincidences and dark counts have been considered.

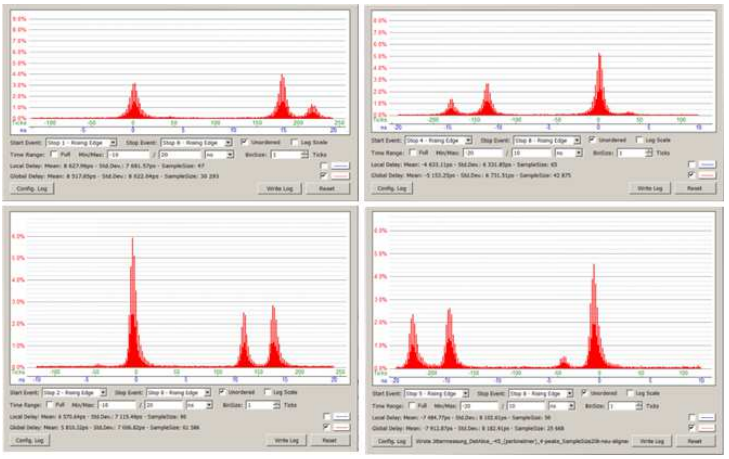

FIGURE 6.23: Corellation Histogram of matching photon pairs with time encoded Bob detector

In order to generate keys, the arrival times of each photon from each of the four branches has to be known precisely. Furthermore the time multiplexed signal has to be matched with the signal from the respective detector at Alice's side (H,V,+ and -). The signal received from Bobs detector on one channel has to be multiplied into four signals (one for each signal on Alice side) and then shifted with the individual delay times to receive the matching correlations of the pairs that have been measured in the same basis. This time is given by the fiber length between source and Bob as well as the fixed time delays of Bobs BB84 module (τ - 3τ) and has therefore be adjusted individually to each fiber length [6]. Since this stated benchmark of the source could not further improved, the next step was the integration of the source in an actual telecom network situation. It has to be noted at this point that due to the rather low visibility the QBER is expected to be quite high. More mature entanglement sources reach visibilities in the range of 98% or 99%, as seen e.g. in [101] and will hence result in better key rates and longer distances. However, it has to be mentioned that this is not the goal of this work. The target here is to give an insight whether and how an integration of QKD in PON networks is in principle possible and determine the best approach by given the change of QBER due to impairments in the quantum channel. In the next section a quick insight in the post processing of the applied software is given.

[6] It would be possible to automate this length adjustment in software by searching for correlation peak. For all measurements in this work the time delay has been adjusted manually for each fiber length.

6.2.2 Basic Overview of the QKD Software

Before the results are presented a quick introduction into the QKD postprocessing software is given in the following lines. A more detailed introduction can for example be found in [19], which this work is based on. The so called QKD stack is divided into 4 blocks, the *sifting stage*, *error detection /correction*, *privacy amplification* and *authentication*, depict by the blue boxes on the right hand side (b) in Figure 6.24. The received raw key, i.e. the time stamps of the respective detector clicks pass through all four stages until an information theoretical secure key is received. The left side of

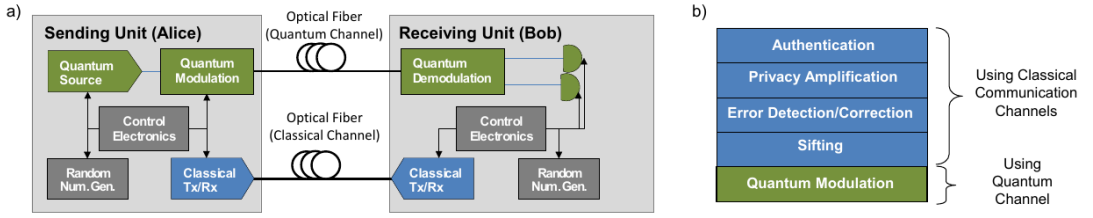

FIGURE 6.24: Left: Schematics of a QKD system in general. Green boxes denote the quantum channel, blue classical communication. Right: Processing stages from the raw key (green box: Quantum Modulation) to secure key after privacy amplification

Figure 6.24 displays the QKD scheme in general with color coded blocks, referring to the quantum sector (green), the electronic processing (gray) and the classic optical transmission (blue). The interface between the quantum channel and electronics is usually a recording device with a fast precise clock in the ps range that forwards each event of the detector to the postprocessing software together with its precise timing information.

Sifting

The comparison of times between Alice and Bob allows to match correlated events. This is called sifting. For this work a Time Tagging module (TTM) of the Austrian Institute of Technology (AIT) has been used to record detector events and forward them via UDP packets to the eligible software connected by an Ethernet port. The software compares the time tagged events and evaluates from their correlation a raw key bit string. It has to be noted that synchronized clocks between Alice and Bob are crucial in this matter. Entanglement based systems offer the advantage of a high amount of correlated photon pairs that can easily be detected when delay times in the optical and electronic regime are precisely added to the time stamp of the TTM module. Since this time correction is applied before the sifting stage, it is referred to as pre-sifting and either realized manually or automatized in software. In the latter case the filtering for the correlation peak is used to precisely lock Alice and Bobs system clocks to each other.

Error estimation and reconciliation

When a raw key is established, bit flips and remaining false detector clicks originating from noise or eavesdropping have to be located in the raw key strings and eliminated

by error correction. In order to exclude information leakage through a side channel that could feed an eavesdropper with information about the key, an expected error rate, p, is calculated from a small part of the raw key that is compared by Alice and Bob publicly. Since errors in the raw key might emerge from a certain pattern due to repeating technical flaws the raw key string is usually scrambled and permuted equally before comparison. If the estimated error rate exceeds the acceptable error rate of the respective protocol, as discussed in chapter 3, the raw key is discarded, since no unconditional secure key can be produced. This process is known as error estimation. An advancement of this process where bits from the respective bases are estimated separately helps to avoid attacks with biased basis choice, as addressed in section 3.2.1.4.
After error estimation has been passed the remaining varying bits between Alice's and Bob's key strings, k_a and k_b, have to be corrected [7]. Relaying on the previously estimated error rate, p, n·p bits are statistically wrong, with n = $|k_a|$, and $|k_a|$ being the length of the key. The amount of information that has to be exchanged between Alice and Bob in order to correct those errors is given by

$$H(A|B) = n \cdot h(p), \tag{6.3}$$

with $h(p)$ being the Shannon entropy H(X) with random variable X, that obeys a Bernoulli trail with probability p. This means each bit has a certain probability for being an error while the other n-1 are correct. The Shannon entropy of this value is the needed information exchange to correct a single bit. Based on this approach, a minimal bound for exchanged information can be deduced. A so called reconciliation protocol R^p has now the task to correct errors on both key strings, k_a and k_b and produce an identical string S, while giving Eve a certain amount of information Q, that, however, is not sufficient to reconstruct the string S. Hence a protocol R^p is called *optimal* if $\forall\epsilon \geq 0$, R^p is ϵ-robust [8] and

$$lim_{n\to\infty}\frac{I_E(S|Q)}{n \cdot h(p)} = 1, \tag{6.4}$$

given a binary symmetric channel [9]. Since optimal protocols turned out to be unpractical, see e.g. [102], the efficiency of a reconciliation protocol has been defined. Given an n bit input string and an corresponding polynomial time span $t(n)$ a protocol is called *efficient* if the expected running time $\bar{T}^{R^p(n)}$ is shorter than $t(n)$, $\bar{T}^{R^p(n)} \leq t(n)$. Furthermore a reconciliation protocol is ideal if it is optimal and efficient. A more relaxed version is given in the case of an *almost ideal* protocol R^p_ξ that is (1) ϵ-robust, (2)

[7] This is usually written as $dist(k_a, k_b)$ and called the Hamming distance, the number of bits on which both keys differ.

[8] R^p is called ϵ-robust if the probability for the protocol to fail is at most ϵ, when revealing Q and the goal is the identical string S

[9] If R^p is only ϵ-robust the more general case of $lim_{n\to\infty}\frac{I_E(S|Q)}{n\cdot h(p)} \leq 1$ is given.

$lim_{n\to\infty}\frac{I_E(S|Q)}{n\cdot h(p)} \leq 1+\xi$ and (3) efficient. For error correction in QKD the common way is an almost ideal reconciliation protocol called *CASCADE*, first introduced in [102]. The basic principle is shown in Figure 6.25. The technique applied here is called *BINARY* and consists of three steps, explained in the following.

- Alice sends Bob the *parity bit* of the first half of the key string. The parity bit holds the information whether an even or odd number of '1's is given in the corresponding bit string
- Bob compares the parity of his first half of the key string with the received one.
- This is continued until a single bit remains and is hereby revealed.

The revealed bit has normally be discarded, since it gives information to Eve. However, in an improved version of CASCADE the bit is kept for further runs and different partitions of the bit string to find errors that remained unnoticed in the first run.

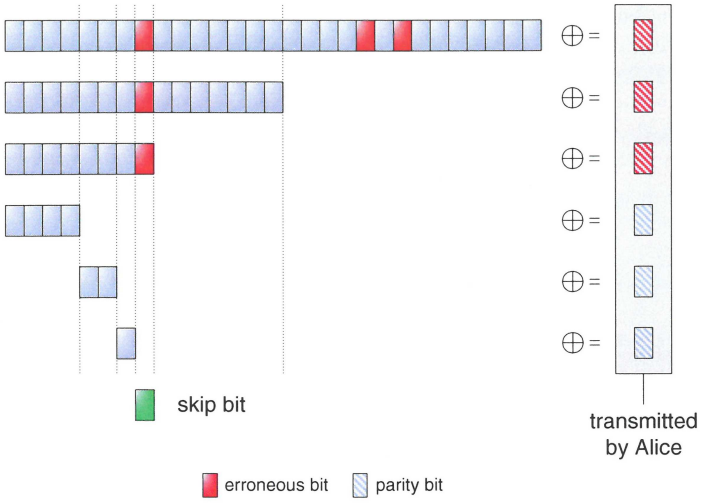

FIGURE 6.25: Operation principle of CASCADE and BINARY, respectively. Source: [19].

Confirmation

In the confirmation step error correction is concluded and the received keys have to be verified for their equality. In this case, a man in the middle attack by Eve is a considerable threat. Hence an authenticated channel between Alice and Bob is mandatory. When the authentication is executed with the corrected common key using *Wegman-Carter authentication*, the confirmation of the error correction is obtained as a byproduct in the same step. Wegman-Carter authentication is based on so called ϵ-*almost universal*$_2$ hashing, which is defined similar to the hash functions used in classic cryptography, introduced in 2.3.1.2.. A set of hash function H is hereby called ϵ-almost universal$_2$,

if $\frac{\delta_H(x,y)}{|H|} \leq \epsilon$, whereas $\frac{\delta_H(x,y)}{|H|}$ denotes the probability of a function $h \in H$ to give the same output for two elements, x and y ($x \neq y$), of a finite set A. $\delta_H(x,y)$ is given by $\delta_H(x,y) = \sum_{h \in H} \delta_h(x,y)$, the accumulated value of coinciding hash results for all functions $h \in H$ with $\delta_h(x,y) = 1$, when $h(x) = h(y)$ and 0 otherwise. An even stronger condition is implied by ϵ-*almost strongly universal*$_2$ (ϵ ASU$_2$) hash functions. The set of functions H, with $H : A \to B$ fulfills

- $\forall x_1 \in A, y_1 \in B$, with $|B| \geq |H|, |\{h \in H : h(x_1) = y_1\}| = \frac{|H|}{|B|}$
  This states the probability of any $x \in A$ to be mapped to a certain $y \in B$ is $\frac{1}{|B|}$.
- $\forall x_1, x_2 \in A$, with $x_1 \neq x_2$ and $\forall y_1, y_2 \in B$, $|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}| \leq \epsilon \frac{|H|}{|B|}$. This means that when a certain tag is known, $h(x_1) = y_1$, the probability of a second element x_2 being referred to a certain hash value $h(x_2) = y_2$ is smaller or equal $\frac{1}{\epsilon}$.

A message m, sent by Alice to Bob who both hold the same key k, is now authenticated in the following way. Alice and Bob previously agreed on an ordered set H of ϵ ASU$_2$ hash functions. The key k has the length $log_2(|H|)$ and denotes which hash function is used to create the corresponding tag $t = h_k(m)$ to the message m. Bob confirms the tag by recalculating since he holds the key k and the corresponding hash function h_k and the received message m. Due to the previous definition an adversary has a $\frac{1}{T}$ chance to guess the right tag, with T being the set of all possible tags. Furthermore a replaced message m' yields the same tag with a probability of at most ϵ when the message m is known due to the part of the definition. In order to keep ϵ small the set H has to be large. This results in a large key, as $log_2(|H|)$ is in the order of the message length for large sets $|H|$. This problem has been solved by Wegman-Carter authentication, which showed that a suitable segmentation of the message with multiple rounds of hash functions, results in an acceptable scaling [103]. The post processing software used in this work is based on this authentication process. When Alice authenticates her message in this manner with her corrected key Bob receives a tag. If Bob receives the same tag with his key, both keys are identical and the message is authenticated.

Privacy Amplification

This final steps aims to minimize Eve's information gained on the previous steps by applying a function g: $\{0,1\}^n \to \{0,1\}^r$ that shortens the key from n bits to r bits. The question is, how short should the key be chosen, i.e. what's the maximal secure value of r. In addition to the revealed parts of the key, all leaked information on the quantum channel is added to Eve's amount of information. An information theoretical approach summarizes all this in a random Variable V, that is correlated to a random variable

W, the bit string held by Alice and Bob. Assuming further that the information that each party gained from the quantum channel is given by X for Alice, Y for Bob and Z for Eve, the Shannon entropy after sifting, denoted by the random variable C, of the previously introduced W changes to $H(W|XC) = 0$ (Alice), and $H(W|YC)$ (Bob) $< H(W|ZC)$ (Eve). Here we assume that Bobs information is higher than Eve's but not equal to Alice's. Only after the confirmation step, D the uncertainty of Bob can be considered $H(W|YCD) \approx 0$. Summarizing the steps ZCD in Eve's case to V the actual privacy amplification can be applied by shortening the common key W with the function g, $K = g(W)$. When Eve is assumed to know t bits of the initial key W the uncertainty of the key K with length r should be r, i.e. $H(K|GV) \approx r$. It can be shown, [104], that the length r of the secure key corresponds to Eve's information $I(K : GV)$ by $r = n - t - s$, with s giving a bound to Eve's information by $I(K : GV) \leq \frac{2^{-s}}{ln(2)}$.

6.3 Results from the integrated QKD System

The basic experimental setup for the integrated QKD system is given in Figure 6.26. The setup is divided into four parts, two quantum parts and two telecom parts: $\text{QKD}_{\text{Alice}}$, Tx_{Alice} and QKD_{Bob}, Rx_{Bob}. In this scenario Alice can be regarded as the trusted node in the backbone network operated by the telecom provider, while Bob is a single user receiving his data through the access network [10]. All telecom parts are displayed in red, while commonly used parts are shown in brown and QKD gear is colored blue (1310nm) and purple (590nm). Electronics and opto-electronics is shown black. In the transmitting red part, Tx_{Alice}, a variable attenuation is used to scale the data channels in power. The well known cascade of FWDM that has already been used for the Raman noise measurements clears all remaining signals from the O-Band. An additional FWDM (brown) is used to merge the data channels and the emitted 1310nm photons in the same fiber and separates them again with another FWDM in opposite configuration. In order to suppress noise photons two additional FWDMs as well as a CWDM are used before connecting the BB84 unit at Bob's QKD receiver. It has to be noted that both parties, Alice and Bob, use the same TTM and PC, which is, of course not a secure way for key distribution, in fact no key distribution at all. The goal of this setup, however, is to determine the results of the QKD system in the presence of classical channels, not give a secure transmission. An example of a secure coexistance setup will be given in chapter 6.3.5.

In order to interpret the results correctly, a back to back measurement, i.e. a direct connection of Alice and Bob without optical fiber and data channels, sets a reference

[10] The influence of noise originating in an access network is discussed in chapter 6.3.4.

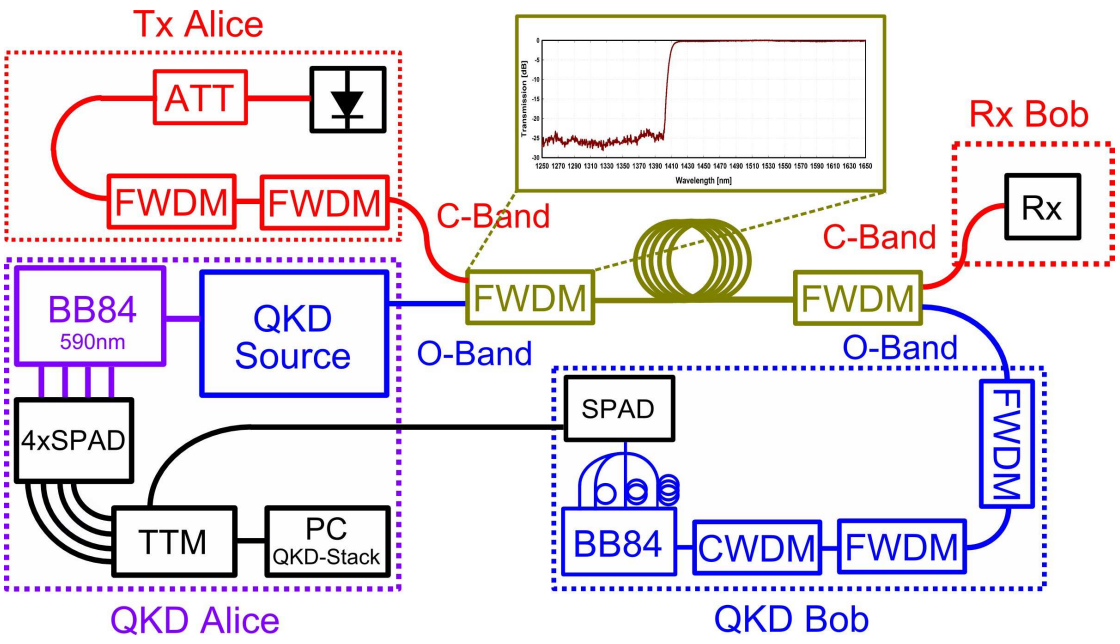

FIGURE 6.26: Integrated QKD system with local measurement at Alice and transmitted photon pairs together with classical data channels using a common optical fiber.

value to the upcoming results. The source operates hereby with a QBER of 5.6% and a raw key rate of about 3000 bits/s. After privacy amplification a secure key rate of 220 bits/s is transmitted.

6.3.1 Single classical Channel

Similar to the Raman noise measurements the first superposition of the quantum channel is done with a single DWDM channel at 1550.12nm. As for those measurements a wavelength and power tunable cw laser is used. Figures 6.27, 6.28 and 6.29 show the results for 4.3, 2x4.3km and 15.3km LWPF. In each case the output power after the FWDM is measured, i.e. the receiver unit Rx on Bobs side. Since most PIN detectors are responsive to at least -20dBm, this value is taken as the minimal threshold. The left pictures show the increase of QBER as the power is increase, the right pictures indicate the respective raise of noise photons. The dashed red line can be taken as a reference QBER when no classical data channel is present.

The measurements show that for longer fibers, i.e. here 8.6km and 15km the noise photons increase faster when the channel power is increased, whereas for 4.3km an almost linear growth is observed. It was measured that at a certain power level the noise photon count change their increase from this linear to an exponential behavior. This becomes even more apparent when the change in QBER is displayed over the output power of the three cases in Figure 6.30. For the 4.4km case, this threshold is at higher powers while for the long fibers cases it is already noticed at -16dBm (for 15.3km) and

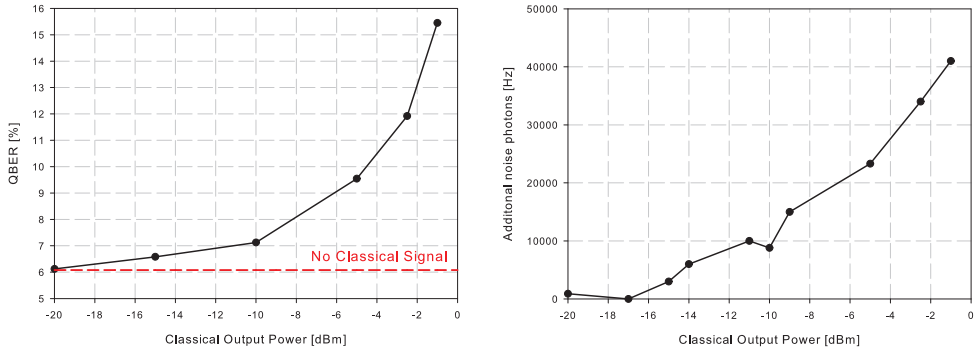

FIGURE 6.27: Left: QBER over data channel power for 4.3km LWPF. Right: Noise photons on Bob detector over data channel power for 4.3km

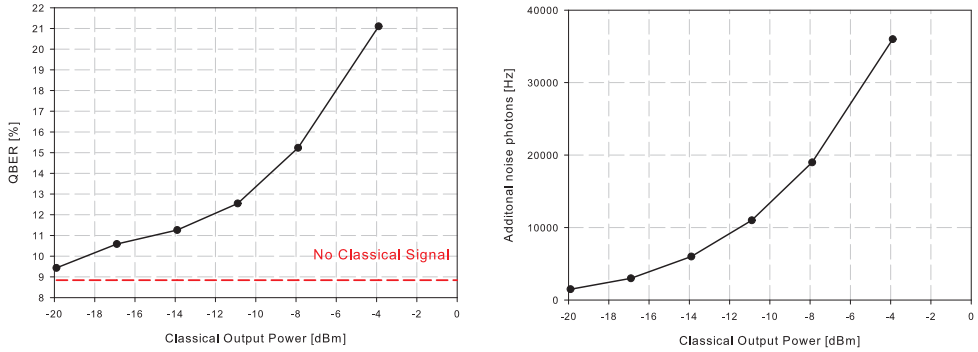

FIGURE 6.28: Left: QBER over data channel power for 2x4.3km LWPF. Right: Noise photons on Bob detector over data channel power for 2x4.3km

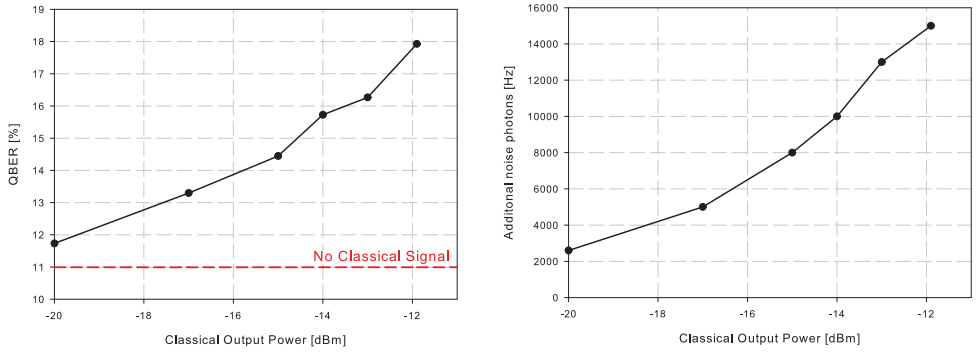

FIGURE 6.29: Left: QBER over data channel power for 15.3km LWPF. Right: Noise photons on Bob detector over data channel power for 15.3km

-14dBm (for 2x4.3km). At -20dBm, the minimal classical data power, a significant effect is only seen for 15.3km, while for the two shorter fibers only a very small increase in QBER is seen. This can be explained by the higher signal to noise ratio (SNR) in longer fibers. Here a single noise photons causes more damage since the correct photons are already hard to discriminate from the background.

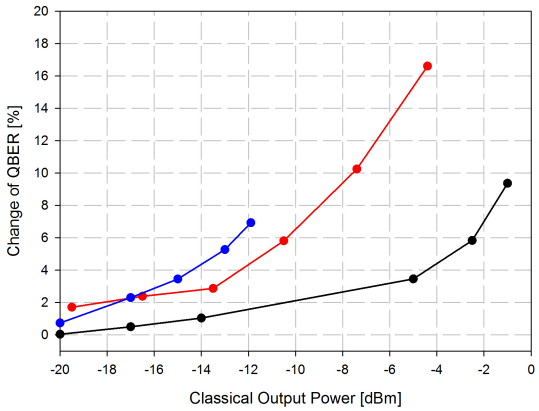

FIGURE 6.30: Change of QBER over data channel power for 4.3 (blue), 2x 4.3 (red) and 15.3km (black) optical fiber with a single data channel.

6.3.2 Six classical Channels

In this section the number of classical channels is increased to six. Standard Small Form-factor Pluggable (SFP) laser modules with transceivers in the CWDM grid, i.e. 1470nm - 1590nm are used. Unfortunately, at the time of measuring no 1490nm SFP module was available, so only six in the eligible wavelengths, 1470nm, 1510nm, 1530nm, 1550nm, 1570nm and 1590nm are combined and merged with the quantum channel. As before the power level is increased starting with -20dBm. It has to be mentioned that this power corresponds to six combined channels. In this case, when demultiplexing the respective wavelengths, a single wavelength channel might not be detected, since some modules require a -20dBm threshold. Though it is reasonable to test how the QKD system reacts to closer wavelength. The results are again displayed for the fiber length 4.3km, 2x4.3km and 15.3 km in Figure 6.31, 6.32 and 6.33 again with the red dashed lines being the QBER with no data channels present.

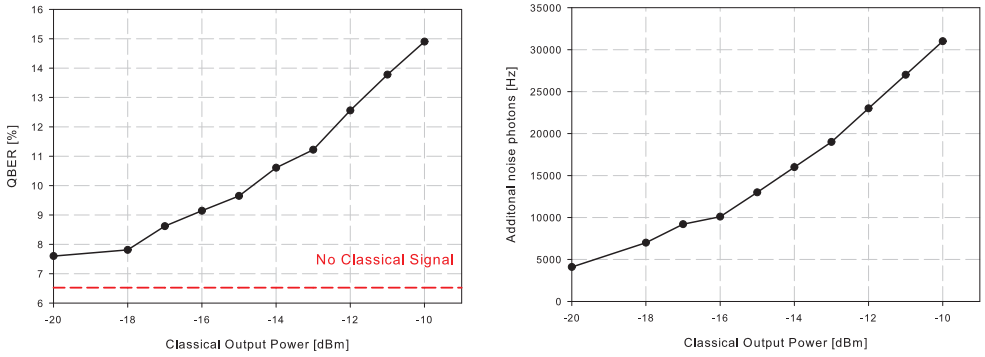

FIGURE 6.31: Left: QBER over six data channels power for 4.3km LWPF. Right: Noise photons on Bob detector over six data channels power for 4.3km

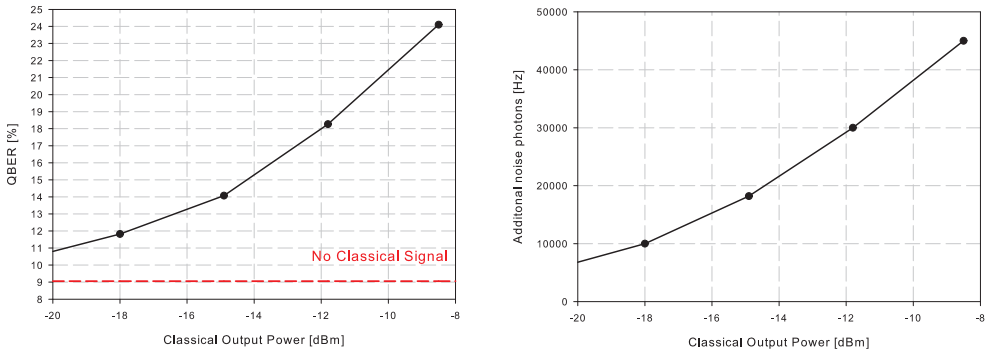

FIGURE 6.32: Left: QBER over six data channels power for 2x4.3km LWPF. Right: Noise photons on Bob detector over six data channels power for 2x4.3km

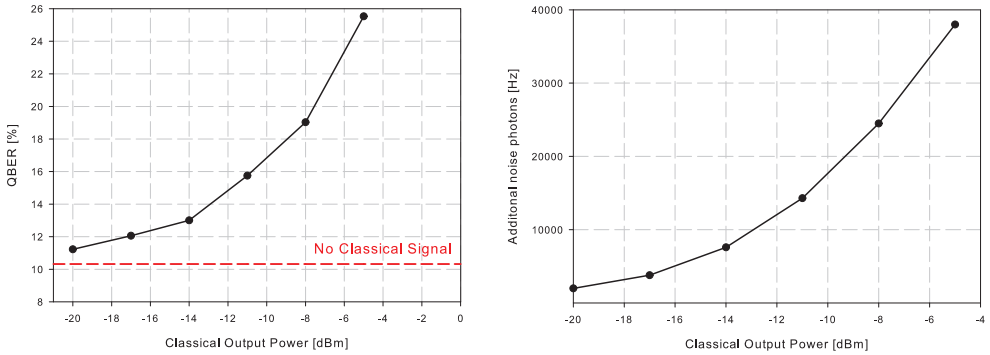

FIGURE 6.33: Left: QBER over six data channels power for 15.3km LWPF. Right: Noise photons on Bob detector over six data channels power for 15.3km

Again as before the change of QBER is displayed in 6.34. The results show in this case that already -20dBm have a detrimental effect on the quantum channel and by increasing the power further the noise photons and hence the QBER increases exponentially, as it is nicely seen on the blue curve for 4.3km in Figure 6.34. For lower powers a linear increase as in the previous measurement is observed. As it turns out the spectral proximity of

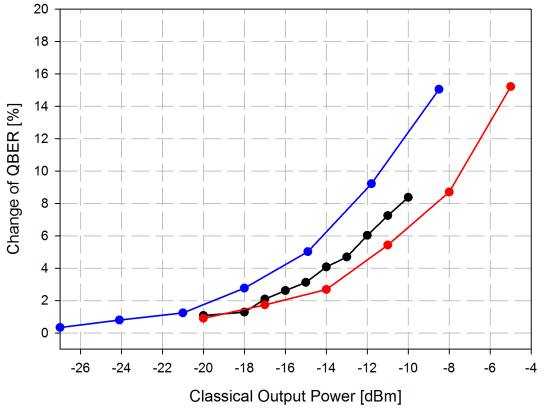

FIGURE 6.34: Change of QBER over data channel power for 4.3 (blue), 2x 4.3 (red) and 15.3km (black) optical fiber with 6 SFP modules as classical data signals.

the data channels to the quantum channel is an important, if not the important factor in this integration scenario. This is shown in the next chapter when the influence of each CWDM channels on the quantum channel is determined in more detail.

6.3.3 Different Channel Combinations

The measurements in this section will assign the change of QBER and noise photons to the respective wavelength of the CWDM grid. Hence each channel is measured individually with equal input power. The results displayed in Figure 6.35 show the reason for the drastically increasing QBER in the previous measurement. Not only the input power but also the spectral proximity of quantum and data channel increases exponentially when a certain threshold is reached. In the case of this setup it is located at around 1490nm, as shown in 6.35.

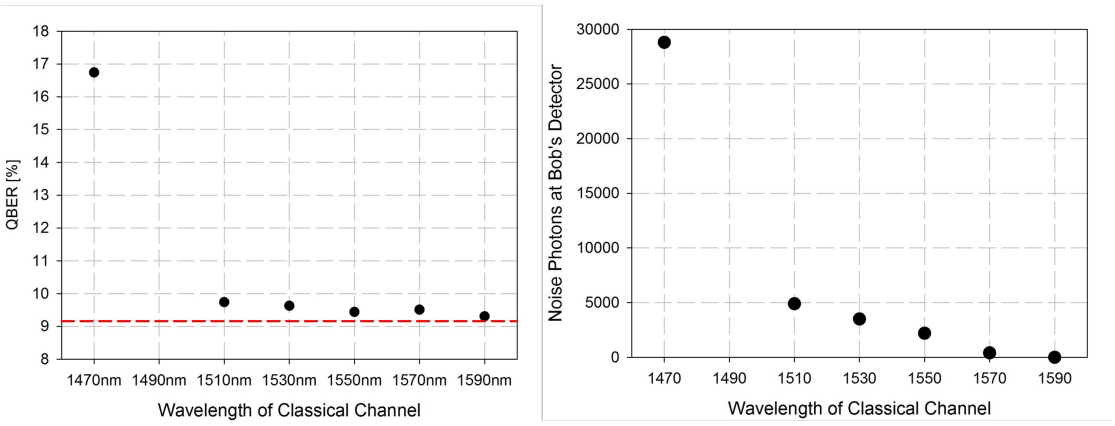

FIGURE 6.35: QBER over data channel from 1470nm-1590nm in 2x4.3km fiber

The next Figure 6.36 connects this result to the previous measurement with six data channels. Here the output power is kept constant at -19dBm. Starting from the left the black and green dots represent the six combined channels.The black dots show what happens when channels that are spectrally closer to the quantum channel (1470nm, 1510nm, ...) are unplugged, one by one, until the threshold with no data channels is reached (red dashed line). This is the case when 1570nm and 1590nm are the only two channels. The spectral distance to the quantum channel is so large that no impairments are present in this case. However, when removing the channels the other way round, starting with the higher wavelength (1590nm, 1570nm, ...) the portion of the spectrally close wavelengths gets more influence resulting in an exponential raise of QBER. Starting from these insights, the next chapters are dealing with the previously addressed methods of tight specral filtering and time multiplexing to further decrease scattering photons and their influence on the quantum channel.

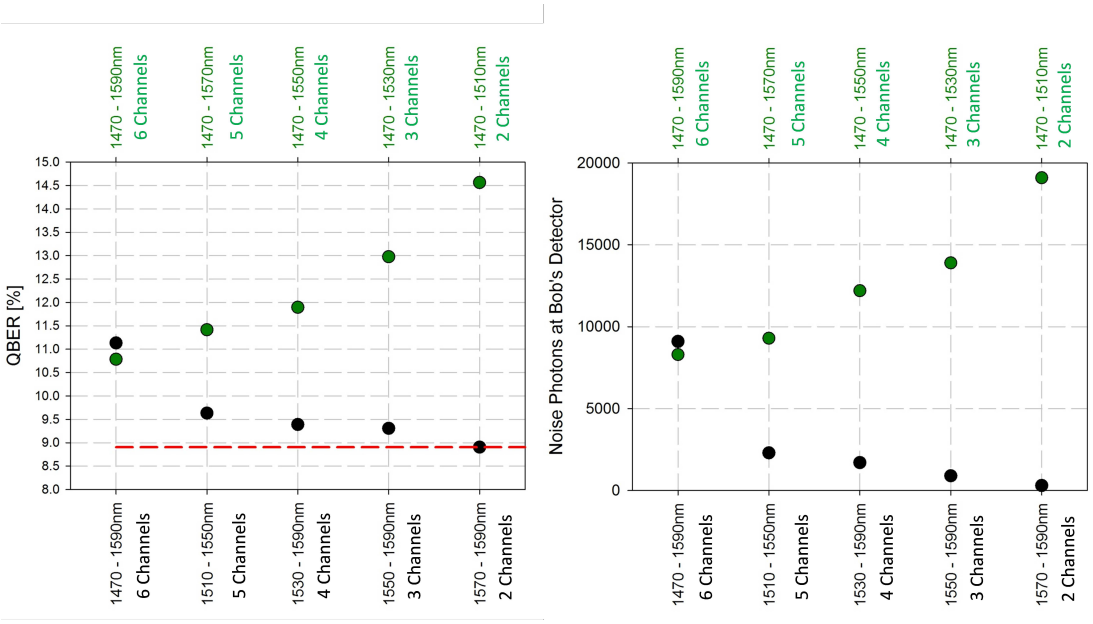

FIGURE 6.36: QBER over constant power with decreasing number of channels from starting with spectrally close channels (black dots) and starting with spectrally far channels (green dots) from in 2x4.3km fiber

6.3.4 Filtering and Time Multiplexing

Filtering

The first approach to further improve the robustness of the QKD system with respect to scattering photons is to apply a narrow filtering that closes the window for unwanted wavelengths. Regarding the used setup in Figure 6.26 a CWDM with a broad window of ±10nm around the center wavelength of 1310nm is used. By cascading another narrow filter with a FWHM bandwidth of about 1.22nm that shows the same attenuation curve as the CWDM filter at around 1300nm a very narrow filtering at around 1302nm, as it is shown in loss curve of Figure 6.37, is provided. The introduced loss of about 4dB should be acceptable considering the advantages in spectral density. At first it was unclear whether the photons of the QKD source could be shifted by almost 10nm to fit the spectral window of the filter. The temperature control of the source, that was switched off for all previous measurements had to be used to cool the crystal. By adjusting the heater with the help of a tunable filter the photon wavelength could be changed to match the filter characteristics, however, since the NTC coefficent is not known, the applied voltage of the Peltier heater could not been converted into degrees. By introducing this additional degree of freedom not only the polarization and phase had to be stabilized before each measurement but also the temperature had be kept constant throughout a measurement cycle. When temperature, phase, polarization and optical alignment was correctly adjusted a huge improvement in terms of noise resistance could be observed when the narrow DWDM is used to filter the entangled photon pairs. For the case of a

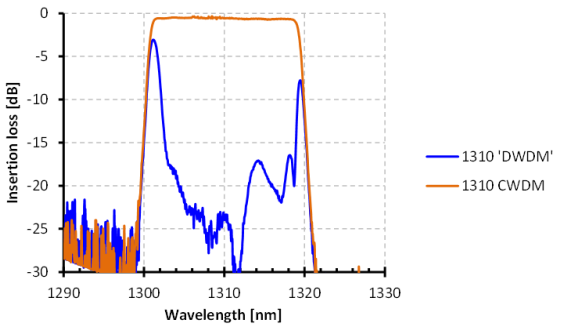

FIGURE 6.37: Cascade of CWDM (brown) and DWDM (blue) filter for narrow spectral filtering of the QKD photons.

single data channel at 1550.12nm it is displayed in 6.38. The graphs show that although the initial QBER with no data channel is higher than in the CWDM case (red and blue dashed lines) the QBER rises significantly slower when the data power is increased. This is reflected by the additional noise photons that are collected by Bobs detector, shown for the CWDM and DWDM case in the right picture.

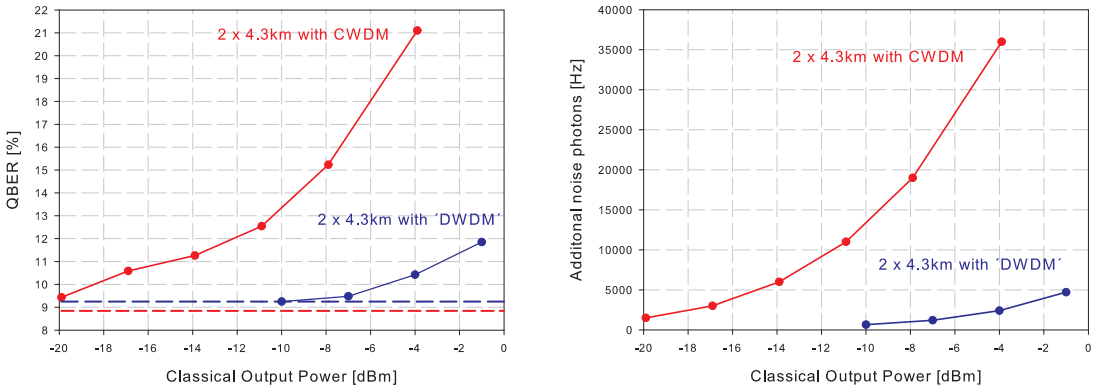

FIGURE 6.38: Left: QBER over data channel power for a single signal over 2 x 4.3km LWPF filtered with CWDM (red) and with DWDM(blue). Right: Noise photons over data channel power for a single signal over 2 x 4.3km LWPF filtered with CWDM (red) and with DWDM(blue).

The benefit of the DWDM filter becomes even more apparent when SFP laser modules are applied that are closer to the quantum channel. As seen in the previous chapter it was not possible to reduce the number of CWDM channel when the power was kept constant in such a way that only the channels close to the quantum channel remained, see Figure 6.36. The same measurement has been repeated with DWDM filter and is shown in Figure 6.39 (blue dots) with respect to the previous results with the CWDM filter (red dots). The filter allows to operate each SFP module, even 1470nm alone (which previously caused an increase in QBER of about 7%) with no effect on the quantum channel. The power, as before, has been kept constant at -19.1 dBm. The 2 and 3 channel results (blue dots) show a slight drift of temperature and polarization, which

was corrected in the last case where only 1470nm is operated. Here no loss in QBER could be measured. This result is reflected when looking at the additional noise photons. In the case of 1470nm almost 30000 noise photons can be suppressed by narrow filtering.

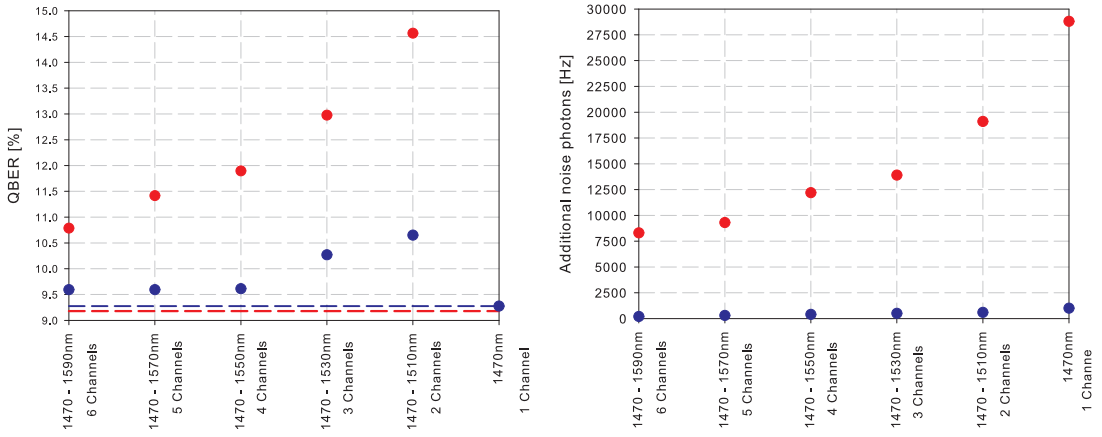

FIGURE 6.39: Left: QBER over number of SFP modules with constant power filtered with CWDM (red) and with DWDM (blue) over 2 x 4.3km LWPF. Right: Noise photons over number of SFP modules with constant power filtered with CWDM (red) and with DWDM (blue) over 2 x 4.3km LWPF filtered with CWDM (red) and with DWDM(blue).

In order to test the limit of such a narrow filter the next step is to increase the power of multiple multiplexed SPF modules in such a way that each classical wavelength can be detected without an EDFA, i.e. the power for each wavelength is $\geq$ -20dBm. This means that for two modules at least -17 dBm, for three modules -15.2 dBm, and so forth up to -12.2dBm for 6 modules have to be applied. Starting from 1470nm (-20dBm) the results are shown in Figure 6.40. The QBER increases in this case by about 1%. It is likely that the rise in QBER for 6 modules (last blue dot) is due to temperature or polarization drift, since the noise photons do not increase much in this case. It is therefore safe to say that 6 classical CWDM channel can be sent alongside with the quantum channel when they are slightly attenuated. In this case no further amplification is needed in front of the PIN diodes.

Finally we increase the number of channels to 40 and use a DWDM signal alongside with the quantum channel. The signal ranges from about 1575nm to 1600nm and is displayed in Figure 6.41. The power of the signal before entering the fiber is about 3.2dBm, after the fiber, the output power is about -1dBm. Due to the narrow filter and the large spectral separation to the quantum channel only 400 additional impairment photons have been detected and a QBER of 7.57% was reached. Hence the quantum channel was not influenced by the classical data channels.

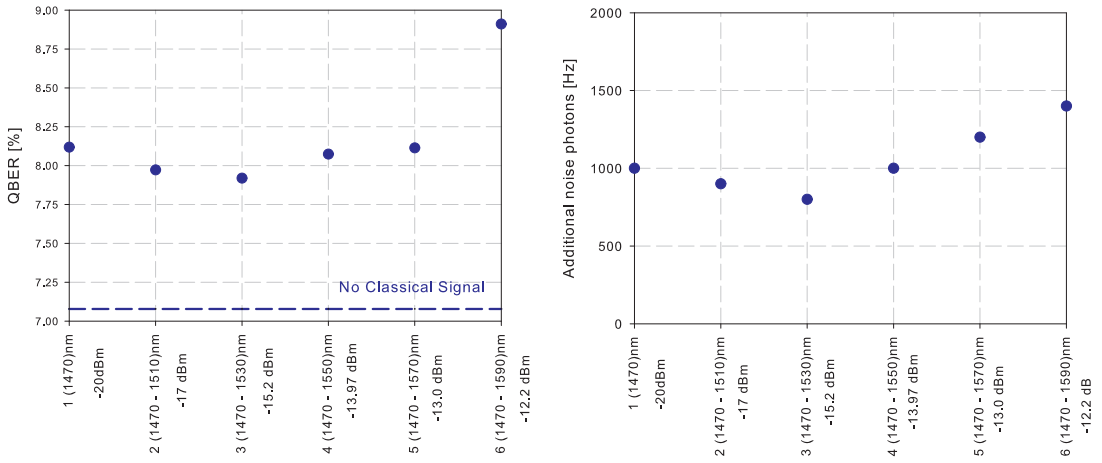

FIGURE 6.40: Left: QBER over number of SFP modules with constant power filtered with CWDM (red) and with DWDM (blue) over 2 x 4.3km LWPF. Right: Noise photons over number of SFP modules with constant power filtered with CWDM (red) and with DWDM (blue) over 2 x 4.3km LWPF filtered with CWDM (red) and with DWDM(blue).

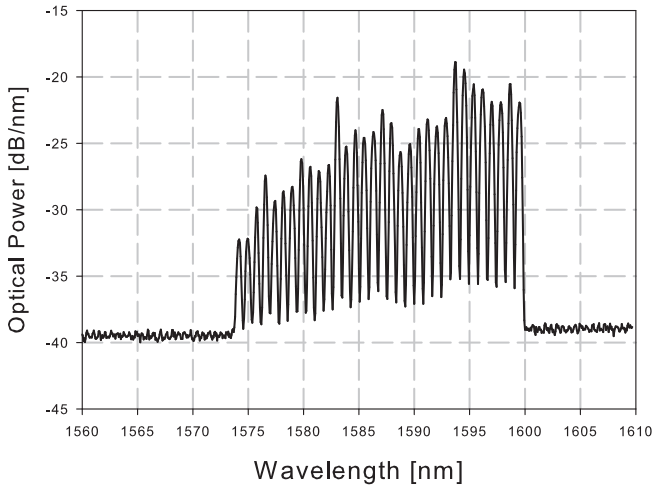

FIGURE 6.41: Attenuated DWDM input signal

Summerizing the results so far it can be observed that a narrow filter slightly reduces the initial QBER due to a higher attenuation but strongly improves the robustness of the QKD system to Raman noise photons. It was possible to operate classical channels up to 1470nm with a power level that allows a reception on PIN diodes without any additional amplification.

Time Multiplexing

The next results presented in the following pages will tackle the question whether an additional improvement can be achieved by time multiplexing classical and quantum channel. Since this scenario is especially interesting for multi-user access networks the experimental setup of 6.26 was changed to emulate the situation in such a scenario. The

first type of setup is shown in Figure 6.43. Here the user, Bob, sends upstream data with a 1290 SFP module while receiving single photons from the QKD system. Alice controls the timing window for her detector and the SFP module with a wave generator (WG). A rectangular waveform was applied at all four Alice detectors with an opening duty cycle of 90%. Another rectangular waveform with 30% duty cycle was used to control the SFP module. By aligning both waveforms correctly the detector is closed when the classic data is sent and opens when no data signal is present. The left and right picture of Figure 6.42 show how the time multiplexed signals look like. The green data channels from the SFP module are hereby located in the time window when the SPAD is closed.

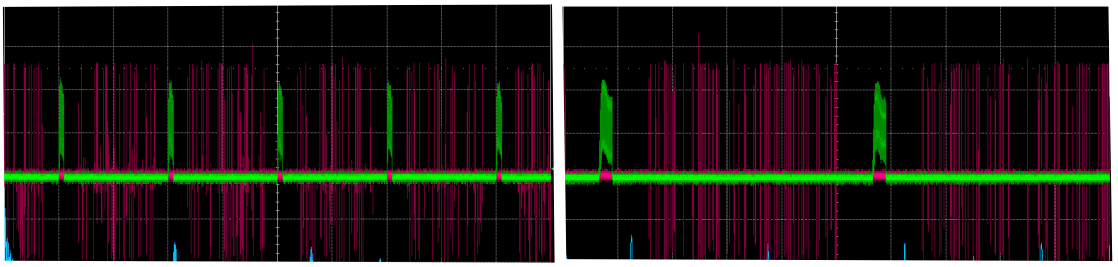

FIGURE 6.42: Two gated signals displayed on the oscilloscope with low (left) and high (right) time resolution. The red curve indicates the signal from the SPAD while in between the SFP signal is displayed in green

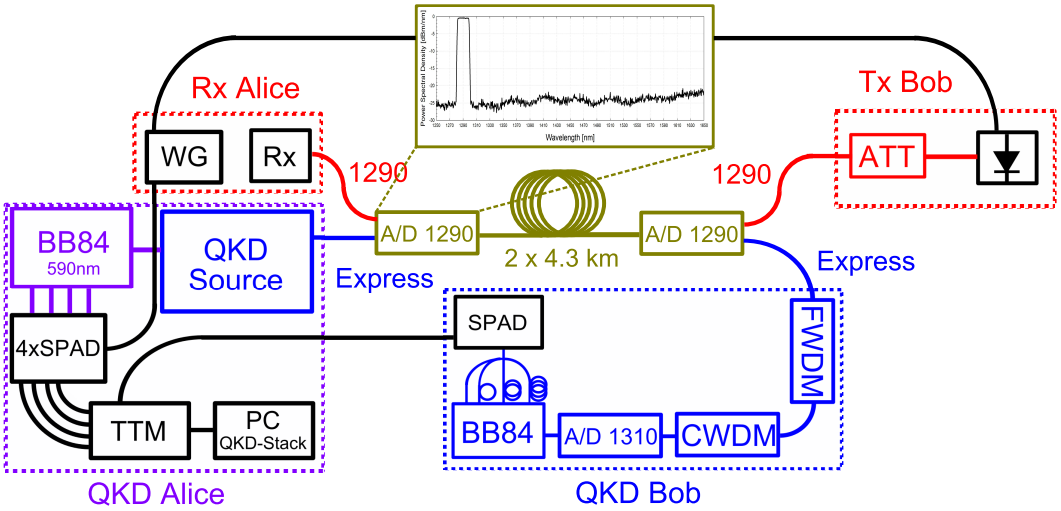

FIGURE 6.43: Schematics of a time-multiplexed coexistence scheme. Bobs transmitter and Alice detector are correlated by a waveform generator (WG). The classic signal is activated when the detection window is closed and vice versa.

The second setup that was assembled for time multiplexed measurements is displayed in Figure 6.44. The difference in this case is an additional 3x3 splitter applied after the fiber to simulate an N user network. At one fiber Bob is connected as the QKD and classical data user, on a second fiber the remaining N users are connected. Their classical upstream data is simulated with a laser diode with an optional attenuator. Bob is hereby separated from the splitter by a last mile fiber of about 100m length.

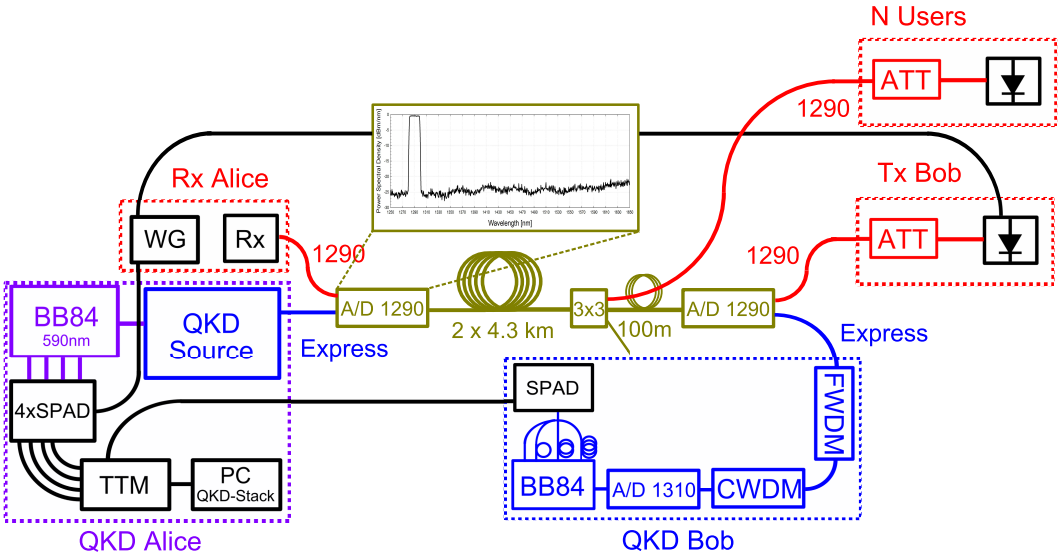

FIGURE 6.44: The same schematics as in 6.43 but with an additional 3x3 splitter and 100m last mile optical fiber to simulate the coexistence scheme in an Metro-Access fiber.

Based on these two setups four different scenarios can be tested. The first two follow the setup of 6.43 for 4.3km and 2 x 4.3km fiber. The other two correspond to setup 6.44, one without additional users, the others with N-users active while operating the quantum channel. The results for the respective setups are summarized in the following Table 6.1 and compared to the case when no data signals are operated.

QBER	**4.3km**	**2 x 4.3km**	**4.3 km & 3x3 Splitter & 100m**	**4.3 km & 3x3 Splitter & 100m & N channels**
Detector ungated SFP ungated	49.0%	48.6%	38.7%	38.7%
Detector gated SFP ungated	11.2%	–	–	–
Detector ungated SFP gated	–	11.9%	–	11.2%
Detector gated SFP gated	8.1%	8.8%	8.4%	8.4%
No data signals, quantum only	7.5%	8.2%	8.1%	8.1%

TABLE 6.1: QBER for time multiplexing in Access networks

The results show that when no gating is applied at the SFP module Bobs detector is overflown with noise photons (approximately 80000 photons/s) and hence a QBER of about 40-50% is received in each case. However, just by gating Alice Detector the noise photons that are still present at Bobs detector are temporally filtered by post-processing, since only time tags of the detector opening time are considered when sifting

in the respective bases. This reduces in the case of 4.3km the QBER by over 35%. Similar results are expected in the other cases but no measurements have been taken here. The same reduction of QBER is given when the SFP modules are gated and Alice detectors are operated normally. Here the same effect and hence the same magnitude of QBER reduction is received as seen in the 2 x 4.3km case. In this operation mode also the noise photons at Bobs detector are reduced. A further 3% QBER is gained when Alice detectors as well as SFP modules are gated. The measured QBERs show that in this case the QKD system is operated close the optimal case, i.e. when no data channels are present. Furthermore it is interesting to see that an N user upstream or downstream[11] in the C-Band, here 1550.12nm has no effect on the quantum channel. It has to be noted that here the N user upstream is operated in the C-Band. When they operate as usual in the O-Band around 1290nm or 1310nm with a power of about -3dBm, Bobs detector is saturated and hence the QBER close to 50%. If it was possible to assign each of the upstream signals of the n users as well as Bobs upstream and quantum channel mutually disjunct time windows, the QKD can be assumed to operate properly. However this approach does not scale well, since reduced time windows result in unacceptable low data rates.
The time multiplexed approach is therefore a useful alternative for a few user access network that operates their upstream channels in the O-Band. Since upstream are usually lower than downstream rates it is possible to operate quantum channel and data channels in the same wavelength band when detector and data channels can be time multiplexed. It has to be noted further that gating the detector at Alice is not the best approach, since Bobs detector deals with high noise photons. Unfortunately in the setup it was not able to gate Bobs SPDC, since no designated interface is given. Nevertheless it is obvious that when Bobs detector is gated, similar or even better results can be expected. In the optimal case the detection windows of both detectors, Alice and Bobs, can be aligned according to the data channels to avoid most impairments.

6.3.5 Encrypted Link System

In this chapter a final experimental setup is introduced that simulates an autonomous point to point link between Alice and Bob. It operates the QKD channel and the corresponding classical data channel for sifting, error correction and privacy amplification over a single 2x4.3km and 13.2km optical fiber. Figure 6.45 depicts the entire setup. For easier measurement readout only a single TTM is used. The UDP packets from this TTM are sent to a PC with the QKD-stack software for Alice and Bob and recorded for evaluation. Furthermore the incoming UDP packets are copied and forwarded to Alice's

[11] As the previous Raman measurements showed, the orientation of the classical signal has no influence on the generated noise photons.

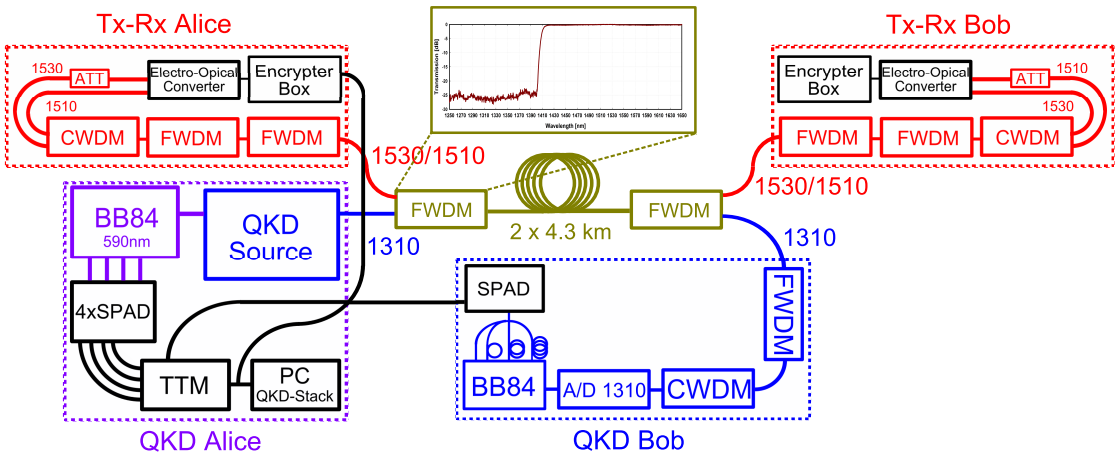

FIGURE 6.45: Experimental setup for a autonomous point to point QKD system with shared fiber for classical and quantum channel.

encryption box that runs the QKD stack as well. The time tags from Alice's detector are processed on Alice encryption box while the time tags from Bobs detector are converted in optical signals transmitted over the optical fiber and eventually received by Bob for further processing with his QKD stack. For turning this setup into a secure link, two individual TTMs for Alice and Bob had to be used that are connected to the respective encryption box. The classical signal from Alice to Bob is sent via Ethernet to an electro-optic converter with embedded SFP transceiver. Alice operates a 1530nm and Bob a 1510nm SFP module. A variable attenuator is used at each party before the data signal is combined with a CWDM filter to observe the impairments with respect to the signal strength. The result of this measurement is shown Table 6.2. The additionally measured noise photons at Bobs detector are hereby denoted in brackets. When comparing the results of the first column (where Bobs classical receiving unit gets a power of -29dBm) to the second set of measurements in the second column (where Bob receives a power of -19.1dBm) it is observed that the first measurements suffered from a slightly misaligned QKD source. Nevertheless the results from the second column show that a key exchange is possible while sufficiently strong classical powers are sent alongside with the single photons. No amplification in the classical domain in front of the detectors is needed. The SFP receivers that are used for this experiments are operational down to -30dBm, hence whenever the QBER was below 10% a key could be extracted (the theoretical threshold of 11% applies only when post processing is excluded).

The experiment has been repeated with a 13.2km fiber. The respective results are shown in Table 6.3. In this case the QKD source was suitable aligned such that for combinations of -20dBm and -10dBm attenuation a secure key could be generated.

For the sake of completeness the specifications of the S.P.I.E. encryption box hardware comprises a Q87 mainboard with 6 GbEthernet on board, an Intel Celeron processor, 2·

Rx_{Alice} \ Rx_{Bob}	**-29.6 dBm**	**-19.1 dBm**
-29 dBm	8.4% (0 Hz)	–
-19.4 dBm	9.2% (500 Hz)	8.1% (1100 Hz)
-14 dBm	11.1% (1800 Hz)	9.6% (2000 Hz)
-10 dBm	–	11.2% (5000 Hz)

TABLE 6.2: QBER for different attenuation for 2x4.3km optical fiber

Rx_{Alice} \ Rx_{Bob}	**-20 dBm**	**-15 dBm**	**-10 dBm**	**-5 dBm**
-20 dBm	9.3% (0 Hz)	9.3% (200 Hz)	9.7% (1000 Hz)	10.8% (2900 Hz)
-10 dBm	9.57% (2000 Hz)	10.6% (2200 Hz)	10.7% (2500 Hz)	–

TABLE 6.3: QBER for different attenuation for 13.2km optical fiber

2 GByte 240pin un-buffered DDR3 DIMM and a 4 GB CFEX SSD. The housing of the boxes is shown in Figure 6.46.

FIGURE 6.46: Photo of the two encryption boxes

This scenario shows that a QKD link with little hardware is implementable in classic telecom equipment and useable alongside with classic signals. The QKD link can be operated with little or acceptable impairments that result in a lower key rate or distance. Since the purpose of this project was the evaluation of different scenarios how a possible QKD integration could look like and how it is affected by strong data signals, the received

key rates of our system are not mentioned here. It has to be clear that even state of the art QKD system can not deliver key rates that are able to produce one-time pads for each sent data packet. However, even a small amount of secure key material can be used for symmetric cryptography and is still offers a higher amount of security compared to standard encryption methods, as discussed in chapter 2. A more detailed outlook and summary about these measurement results as well as the integrated entanglement source for space application is given in the next and final chapter.

Chapter 7

Summary and Discussion

In this thesis a rough overview about existing classical cryptographic methods, such as RSA or AES, as well as the unconditionally secure key exchange with the help of QKD have been presented. Starting with the first theoretical concept, the BB84, various flavors of protocols for discrete and continuous variables emerged. A survey of these protocols has been presented and the respective ideas of their security proofs have been outlined. Some of these protocols are designed to achieve better key rates by improving post processing or use a more efficient way to get closer to the Shannon limit by exploiting other degrees of freedom, others target to minimize possible side channels and hardware dependency. So far, no type of protocol is preferred over the others, since no essential advantage can be gained from a certain scenario. This, however, could be a significant factor why QKD still lacks the commercial success. Once a standardized system and protocol has been chosen, it might be easier for start up companies to commit to a certain system and hardware that will optimize costs as well as performance. So far QKD systems are mainly bound to experimental setups.

Another obstacle that QKD is facing, apart from its standardization, is its limited flexibility and high complexity to become an economic feasible alternative for classic standard cryptography. It is even doubtful whether a realization of a quantum computer and hence Shors algorithm, which would compromise most of current cryptography protocols, could really trigger the the breakthrough of QKD to a mass technology applicable for private and business users. Other alternatives, such as lattice cryptography, that relay on other hard mathematical problem, are considered promising candidates in the case of such a “cryoptocalypse”. The only realistic way that QKD will enter a broad commercial market is by making the technology easy, cheap and compatible with nowadays technologies.

The results that have been acquired in the course of the projects of the last years and presented in this thesis, namely the space source for satellite communication and the

demonstration of an entanglement based coexistance scheme of QKD in passive optical networks, contribute to accomplish this final step for QKD. The results from the fully integrated entanglement source show that great potential lays in integrated optics in general and in quantum optics in particular. Still the production cost and the integrated elements can not be compared with standard equipment in terms of performance and attenuation but the results show that by continuous improvement in the manufacturing process, the creation of entangled photon pairs on a chip with high visibility and brightness will result in key rates that allow long haul encryption. This will enable experiments for QKD in a range of over 30000km and, in addition to this technical aspect, give insights into the gravitational influence on quantum theory on a fundamental level. For this purpose two periodically poled $LiNbO_3$ crystals have been manufactured and tested for its optimal performance. The combination of two poling periods to reach quasi phase matching that allowes SPDC to generated two indistinguishable photon pairs with wavelengths λ_{Signal} and λ_{Idler} such that the Bell state $\Psi^+ = \frac{1}{\sqrt{2}}\big(|H\rangle_{\lambda_{\text{Signal}}}|V\rangle_{\lambda_{\text{Idler}}} + |V\rangle_{\lambda_{\text{Signal}}}|H\rangle_{\lambda_{\text{Idler}}}\big)$ is created. The most important results of this two sources are summarized in Table 7.1 and the waveguide crystal as well as the compact setup is shown in Figure 7.1.

	1st Generation	**2nd Generation**
Wavelength of the entangled photon pairs	1535.3nm/1562.7nm 1536.72nm/1563.6nm	1546.9nm/1573.1nm
crystal temperature	$\approx 159.6°C$	$5.524k\Omega$
Pump power	$\approx$ 6mW (cw)	$\approx$ 1mW (cw)
Optical bandwith of signal and idler	1.2nm	1.2nm
Coincidance Rate	$1.34 \cdot 10^6 \ \frac{\text{pairs}}{s}$	$5.2 \cdot 10^4 \ \frac{\text{pairs}}{s}$
Visibility	91.5%	75.2%
Spectral Brightness	$1 \cdot 10^6 \ \frac{\text{pairs}}{s \cdot nm \cdot W}$	$4 \cdot 10^3 \ \frac{\text{pairs}}{s \cdot nm \cdot W}$

TABLE 7.1: Summary of specifactions for 1st and 2nd generation entanglement waveguide sources

Although satellite based QKD is a promising candidate to enable long distance encryption, it suffers from a poor scalability and is hence restricted to a limited number of users. The second part of this work connects at this point and determines where an potential integration of QKD into existing network infrastructure is possible. Critical equipment, such as AWG and amplifiers, has to be bypassed with a respective loss

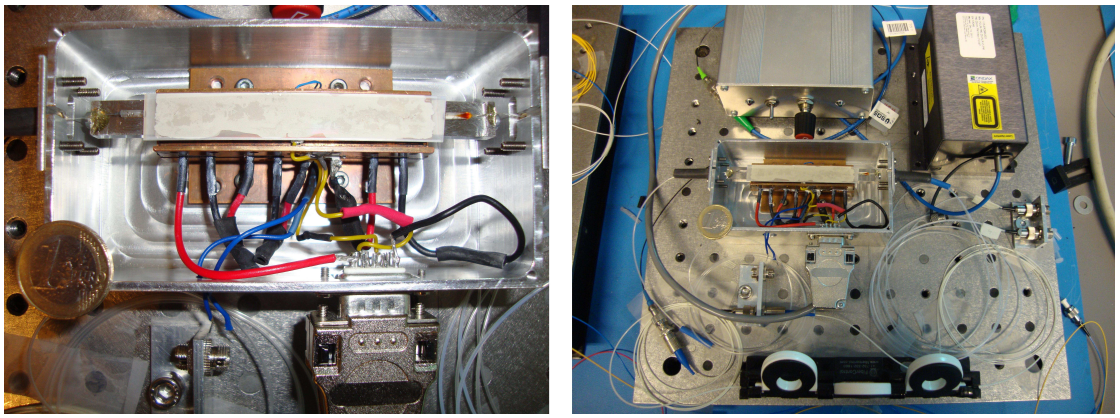

FIGURE 7.1: Left: 2nd Generation Crystal with heater connection in housing. Right: Entire setup for entanglement pair generation with pump laser (top right) heater control (top center) waveguide crystal (middle) and polarization control (bottom).

budged. Furthermore Raman impairment simulations and measurements have been presented, that showed the spectral influence of strong classical signals on potential telecom bands where a quantum channel may transmit. The simulations could be matched to the experimental results by adapting the Raman gain curve. The results revealed that apart from tight wavelength and time filtering a spectral distance of about 200nm from the classical signals shows an acceptable but still considerable amount of scattering photons. The measurements have been performed with standard, of the shelf telecom equipment and filters and a combination of classic power meters as well as single photon diodes. Based on these results it was decided to allocate the quantum channel in the O-Band. A free space entanglement source with a ppKTP crystal in Sagnac configuration has been build with a wavelength combination of 1310nm and 586nm to match the required benchmark. The experimental setup of the source is shown in Figure 7.2 where the left hand side depicts the entire setup with measurement modules from Alice and Bob. The measurements are hereby performed in two mutually unbiased bases. In the case of Alice, the 586nm brunch, a free space setup with four silicon detectors forwards the measurement to a TTM module, whereas in Bobs case a fiber bound version of this setup has been build to collect the 1310nm photons a single InGaAs SPAD with time-encoded measurement bases. The two detection setups are shown in more detail in Figure 7.3. This setup was subsequently used in combination with strong classical signals. Various filtering methods in the time and wavelength domain have been applied in order to improve the robustness of the entire system against Raman noise. The results showed that even an attenuated 40 channel DWDM signal with appropriate filtering could be operated without significant impairment on the QKD system. Further experiments showed that the spectral proximity of the classical channels closer than 150nm-100nm causes a problem to QKD due to the high background noise. A 200GHz filtering allowed a closer proximity of quantum and classical channels, however, only up to certain power levels.

It can be concluded from these measurements that a quantum channel in the same band as a classical channel is so far not a possible scenario, when the standard power levels are assumed. However, further measurements showed that such a scenario is possible when quantum and classical channels are time multiplexed.

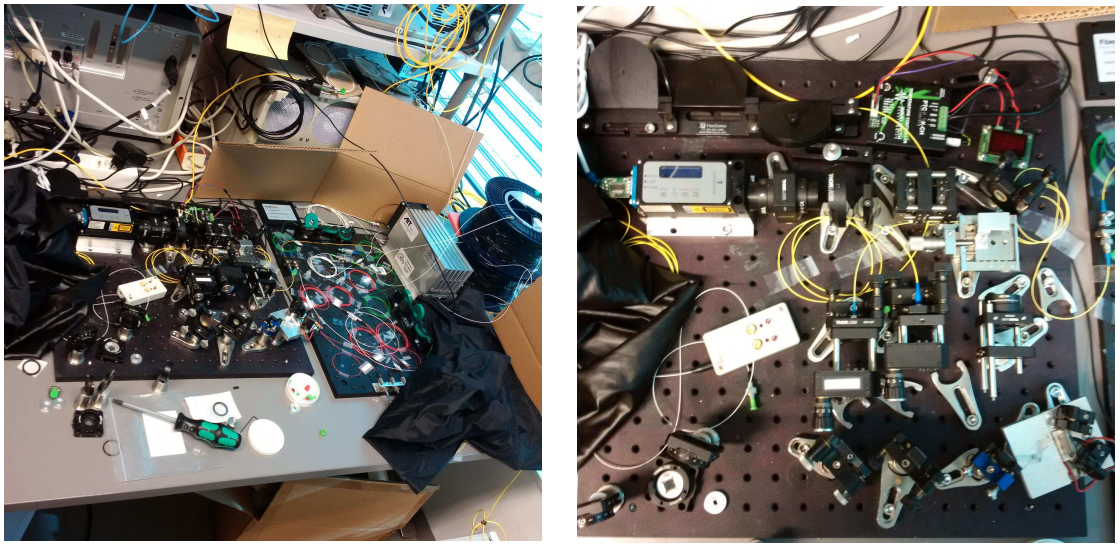

FIGURE 7.2: Left: Entire setup with measurement modules from Alice (left) and Bob (right) and entanglement source (middle). Right: Entanglement source in detail with pump laser (top left), optics (cylinder lenses, mirror, $\frac{\lambda}{2}$ waveplate, phase compensator,), Sagnac loop (bottom right) and dichroic mirrors for selecting the entangled photons from SPDC.

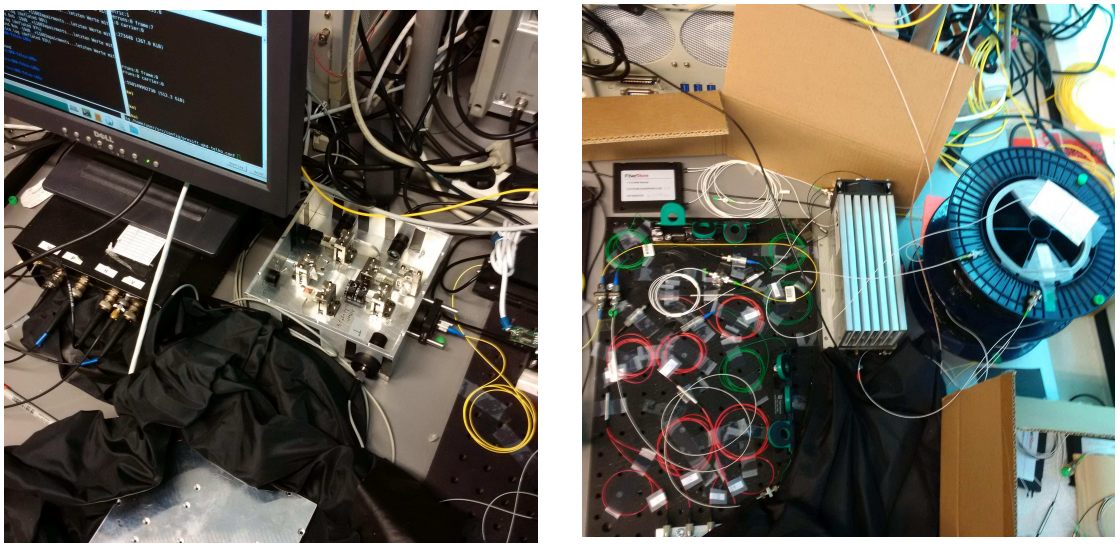

FIGURE 7.3: Left: Free space setup for Alice measurements in H/V and 45/-45 basis. Right: Fiber bound setup for Bobs measurement in H/V and 45/-45 basis.

As a final measurement the preparation of encryption box hardware together with QKD post-processing allowed to run quantum and classical channel full duplex communication on a single fiber over 13.2km.

The results of this project show that an integration of QKD in classical networks is

possible, given certain constraint on both parties. On the one hand the wavelength allocation of classical signal has to be done carefully with respect to the spectral region of the quantum channel. Furthermore the power levels of data channels have to be adapted and, if necessary, amplified before the measurement with the PIN detectors [1]. The major drawback of QKD that has also been observed in the presented results is the limitation of single photons to travel long distances. The received results have been gained for ranges up to 15km, which is an acceptable result for access, but a limiting factor for metropolitan networks. The mitigation of QKD into the O-band comes with an even higher attenuation and will increase this intrinsic weakness. A star topology with an trusted center note could hereby evade this problem and distribute the key between two users, until the maturity of entanglement swapping for trusted repeater technology. The usage of trusted nodes, however, contradicts the unconditional security propagated by QKD. It is therefore still an open and exciting question whether QKD will be a side note in applied cryptography in commercial telecommunications or it will eventually reach its big breakthrough and hence be the first application of quantum mechanics.

[1] Since the sensitivity of PIN detectors varies between -20dBm to -30dBm and mainly short range networks tend to be run passive, it can be assumed that the lower input powers are also in favor of modern networks.

Appendix A

Fiber Attenuation, quantum Efficiency and internal OSA Loss

Internal OSA loss

In order to determine the internal loss of the OSA that is added when a signal passes through the optical grating and exits through the pre-selection output, the spectral power recorded by the OSA is compared to the measured power of a powermeter. The powermeter is hereby connected with a short ($\approx$ 1m) multimode fiber to the pre-selection output. The difference for 1250nm-1420nm is recorded and shown in Figure A.1. It is unclear if the received values are valid for all input powers. The curve was recorded for low input power at around -90dBm since this have been the relevant powers at which OSA and SPAD have been operated for the Raman measurements presented in chapter 6.1.1.

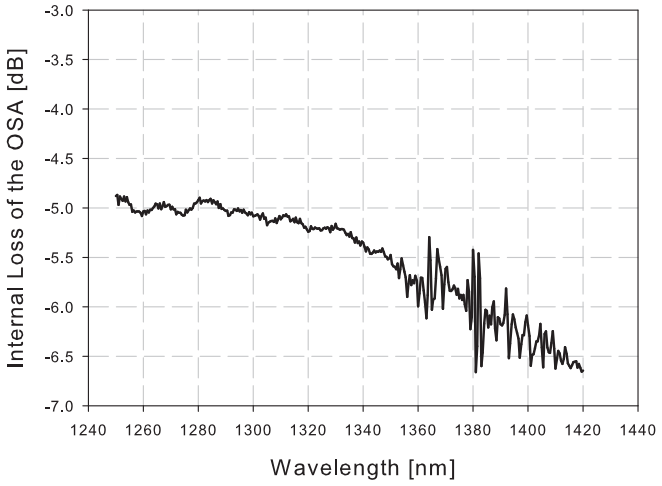

FIGURE A.1: Attenuation curve for internal OSA loss over wavelength, when operated with the monochromator output.

Correction of the Quantum Efficiency

The Raman measurements shown in this work present the scattered photons down to a power level of about -130dBm and up to about -70dBm. The measured curves have been recorded using a SPAD for low and an OSA for high power levels. A single consistent curve is only received when the two scales match perfectly. The internal OSA loss was not sufficient to achieve this goal. Although the IDQ220 freerunning SPAD was specified with a Quantum efficiency of 5%, it was obvious after excluding all other possible sources of loss that for a continuous Raman curve the QE has to measured precisely and in dependence of the respective wavelength. A broad white light source with stable power of -66dBm was used to measure the correct QE. Before launching it into the OSA it was attenuated by -30dB. The total output power at the monochromator output of the OSA was below -95dBm when the internal loss of the OSA is added. Using a simple model of the freerunning detector with R denoting its count rate, D the dark counts, T_d the dead time and QE the quantum efficiency, the total number of photons arriving at the detector can be estimated by

$$N = \frac{R - D}{(1 - R \cdot T_d)QE}. \tag{A.1}$$

Contemplating the energy $E = \frac{hc}{\lambda}$ of a photon, the total power hence given by $\frac{R-D}{(1-R\cdot T_d)QE} \cdot \frac{hc}{\lambda}$. Assuming now that the total energy arriving at the detector, and therefore, N is known, the Quantum efficiency over wavelength can be received by comparing the measured counts with the expected, since $T_d = 2.5 \cdot 10^{-6}$ and $D = 350Hz$ are known values. The result is displayed in Figure A.2 and turned out to be sufficient to match the SPAD and OSA scale [1].

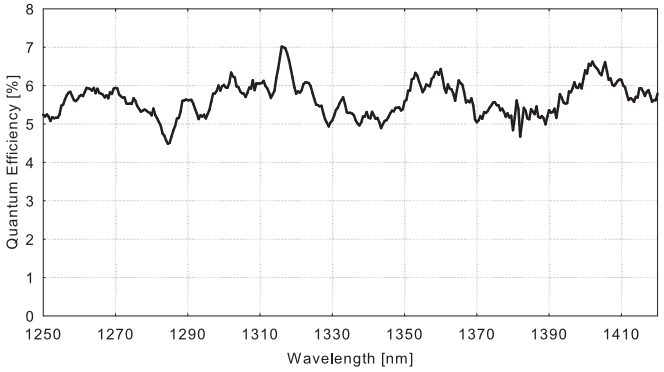

FIGURE A.2: Corrected quantum efficiency over wavelength for the IDQ201 freerunning SPAD operated at 5% QE.

Fiber attenuation curves

Finally the fiber attenuation curves for all investigated fibers in section 6.1.1. are shown

[1] In addition to loss and QE correction the linear scale of the SPAD counts, i.e. the photon energie X in $[W]$ have to be converted to the logarithmic scale, Y in $[dBm]$ by $X[dBm] = 10 \cdot log(\frac{Y[W]}{10^{-3}[W]})$.

in Figure A.3. It is noticed that different characteristics of the waterpeak are observed. This is due to the wide range of different fiber lengths and ages that have been used throughout the Raman noise experiments. The attenuation curves have been measured using a broad white light source, averaged over a few minutes.

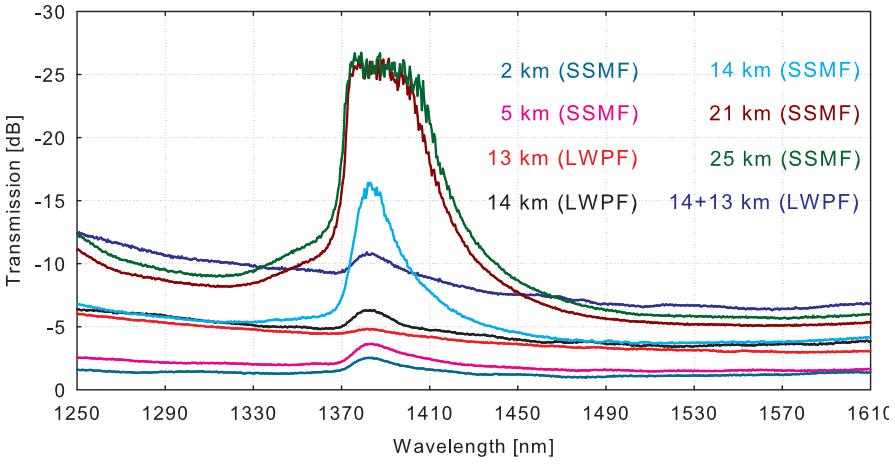

FIGURE A.3: Attenuation Curves for investigated Fibers for the Raman scattering measurements presented in chapter 6.1.1.

Appendix B

Optics Express Journal Paper

Perspectives and limitations of QKD integration in metropolitan area networks

Slavisa Aleksic,[1] * **Florian Hipp,**[2] **Dominic Winkler,**[1] **Andreas Poppe,**[2] **Bernhard Schrenk,**[2] **and Gerald Franzl**[1]

[1] *Vienna University of Technology, Institute of Telecommunications, Favoritenstr. 9-11/E389, Vienna, Austria*
[2] *Digital Safety & Security Department, Optical Quantum Technology, AIT Austrian Institute of Technology GmbH, Donau-City-Strae 1, 1220 Vienna, Austria*
* *slavisa.aleksic@tuwien.ac.at.*

Abstract: Quantum key distribution (QKD) systems have already reached a reasonable level of maturity. However, a smooth integration and a wide adoption of commercial QKD systems in metropolitan area networks has still remained challenging because of technical and economical obstacles. Mainly the need for dedicated fibers and the strong dependence of the secret key rate on both loss budget and background noise in the quantum channel hinder a practical, flexible and robust implementation of QKD in current and next-generation optical metro networks.
In this paper, we discuss these obstacles and present approaches to share existing fiber infrastructures among quantum and classical channels. Particularly, a proposal for a smooth integration of QKD in optical metro networks, which implies removing spurious background photons caused by optical transmitters, amplifiers and nonlinear effects in fibers, is presented and discussed. We determine and characterize impairments on quantum channels caused by many classical telecom channels at practically used power levels coexisting within the same fiber. Extensive experimental results are presented and indicate that a practical integration of QKD in conventional optical metro networks is possible.

OCIS codes: (060.4510) Optical communications; (060.5565) Quantum communications; (270.5568) Quantum cryptography.

References and links

1. C. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," IEEE Intern. Conf. on Comp. Syst. and Sign. Process., Bangalore, IEEE, 1291–1293 (1984).
2. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics **4**(10), 686–689 (2010).
3. D. Winkler, "Practical Integration of a Quantum Channel for QKD in commercial WDM systems," M.Sc. Thesis, Vienna University of Technology, pages 95 (2013).
4. P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibr," New Journal of Physics, **12**(6), 063027 (2010).
5. K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A.W. Sharpe, Z. L. Yuan, R.V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Applied Physics Letters **104** 051123 (2014).

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

6. K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," Physical Review X, **2**, 041010 (2012).
7. B. Froehlich, J. F. Dynes, M. Lucamarini, A.W. Sharpe, Z. L. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69–72 (2013).
8. I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New Journal of Physics **13**, 063039 (2011).
9. L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimatal multiplexing of quantum key distribution with classical optical communication," Applied Phisics Letters **106** 081108 (2015).
10. T E Chapuran, P Toliver, N A Peters, J Jackel, M S Goodman, R J Runser, S R McNown, N Dallmann, R J Hughes, K P McCabe, J E Nordholt, C G Peterson, K T Tyagi, L. Mercer, and H. Dardy, "Optical networking for QKD and quantum communications," New Journal of Physics **13**, 105001 (2009).
11. A. Poppe, B. Schrenk, F. Hipp, M. Peev, S. Aleksic, G. Franzl, A. Ciurana, and V. Martin, "Integration of Quantum Key Distribution in Metropolitan Area Networks," 2014 OSA Optics & Photonics Research in Optical Sciences Congress, Quantum Information and Measurement, Berlin, Germany, 1–3 (2014).
12. S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, "Quantum Key Distribution over Optical Access Networks," 18th European Conference on Networks and Optical Communications (NOC 2013), pp. 11–18 (2013).
13. R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, N. Nweke, S. R. McNown, R. J. Hughes, D. Rosenberg, C. G. Peterson, K. P. McCabe, J. E. Nordholt, K. Tyagi, P. A. Hiskett, and N. Dallmann, "Progress toward quantum communications networks: opportunities and challenges," Proc. SPIE 6476, Optoelectronic Integrated Circuits IX, **6476**, 6476OI (2007).
14. P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electronics Letters, **33**(3), 188–190 (1996).
15. S. Aleksic, D. Winkler, A. Poppe, G. Franzl, B. Schrenk and F. Hipp,Distribution of quantum keys in optical transparent networks: issues and challenges," 15th International Conference on Transparent Optical Networks (ICTON 2013), Cartagena, Spain, We.B1.3 (2013).
16. T. F. da Silva, G. B. Xavier, G. P. Temperão, and J. P. von der Weid, "Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems," Journal of Lightwave Technology, **32** (13), 2332–2339 (2014).
17. S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Impairment Evaluation toward QKD Integration in a Conventional 20-Channel Metro Network," Optical Fiber Communication Conference (OFC 2015), Los Angeles, California, USA, W4F.2 (2015).
18. S. Aleksic, D. Winkler, F. Hipp, A. Poppe, G. Franzl, and B. Schrenk, "Towards a Smooth Integration of Quantum Key Distribution in Metro Networks," 16th International Conference on Transparent Optical Networks (ICTON 2014), Graz, paper Tu.B1.1 (2014).
19. VPI Systems, *VPItransmissionMaker Optical Systems*. [Online]. Available: http://www.vpiphotonics.com/
20. D. Hollenbeck and C. D. Cantrell, "Multiple-vibrational-mode model for fiber-optic raman gain spectrum and response function," JOSA B, **19**(12), 2886–2892, (2002).
21. N. R. Newbury, "Pump-wavelength dependence of Raman gain in single-mode fibers," Journal of Lightwave Technology, **21**(12), 3364–3373 (2003).
22. R. H. Stolen, "Issues in Raman gain measurements," Tech. Dig. Symp. Optical Fiber Measurements, NIST Special Publication 953 (National Institute of Standards and Technology), Gaithersburg, MD, 139–142 (2000).

1. Introduction

Although the idea to utilize the quantum nature of optical phenomena to encrypt transmitted data is not substantially new, it was already introduced in the early 1980's [1], practical QKD systems that can be smoothly and economically integrated in conventional optical networks are still not available. Current commercially available QKD systems generally presume dedicated point-to-point fiber links connecting the two network terminals that create a common and secret key. For simplicity and in accordance with network security literature, the two terminals are called Alice and Bob. In a QKD system, quantum bits (*qubits*) are exchanged between Alice and Bob, which yields the encryption key used to secure their communication [1]. Photons received by Bob that are not originating from Alice, detected as not being in accordance to the known statistical data, indicate a potential intruder. However, if the number of noise photons exceeds a certain level, Bob is unable to detect the qubits sent by Alice, making the secure key distillation impossible. Thus, the main reason for using dark fibers to transmit qubits between Bob and

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

Alice is to avoid high levels of noise in the quantum channel by preventing any interaction between strong classical telecommunication channels and weak quantum channels.

On the other hand, dedicated fibers are a major drawback for an economical implementation because of the high costs of installing or leasing extra dark fibers. Additionally, QKD systems commonly require a complex on-site calibration of detectors and modulators, which are reported to be vulnerable to certain attacks [2]. Even for a system using dedicated dark fibers, achievable secret key rates are rather low (below 1 Mb/s) for distances of several tens of kilometers and above. Figure 1 presents achieved secret key rates versus link length as reported in recent experimental demonstrations and summarized in [3].

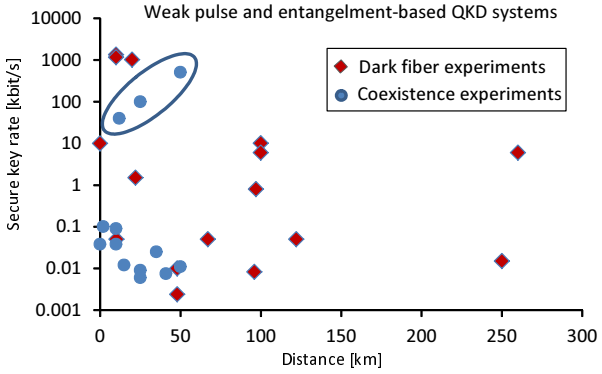

Fig. 1. QKD experiments using weak pulse and entanglement-based QKD systems.

A first step to make QKD systems more economical is to find a way to transmit weak QKD signals together with strong conventional optical signals over the same optical fiber. Such an option, referred to as *coexistence scheme*, has attracted particular interest in recent years. Several studies show that the coexistence scheme is in principle possible [4–15], but the introduced impairments strongly limit the performance of the QKD system. As can be seen from Fig. 1, the achievable secret key rate using the coexistence scheme is mostly below 1 kb/s for QKD systems based on either the weak pulse or entanglement methods, as detailed in [3]. The reported experimental results known to the authors consider systems with limited launch powers, reduced network reach and/or sparse spectral occupancy (a few active wavelength channels only). However, these restrictions on the system parameters are hardly achievable with common WDM metro network designs, in which several tens of wavelength channels and much higher power levels are used. Recently, secret key rates similar to those reported using dedicated fibers have been achieved for the coexistence scheme by optimizing the system parameters [5] (see the encircled points in Fig. 1). Key rates in the order of hundreds of kbit/s over 25 km have been demonstrated in coexistence with several classical signals at typical power levels (about 0 dBm). Moreover, the impact of Raman scattered noise from up to 14 classical channels with -10.5 dBm each has recently been studied [16]. It has been shown that an increase of the number of coexisting classical channels to more than six can severely limit both secret key rate and distance of a QKD system working at 1546.12 nm. Although a lot of effort has been put recently into investigation of the coexistence scheme, an overall characterization of possibilities and limitations upon the integration of QKD systems in conventional networks, considering typical and worst case conditions, is to the best knowledge of the current authors missing.

In this paper, we address perspectives and limitations of a smooth QKD integration in conventional metropolitan area networks and aim to find a wavelength range that best suits to allocate quantum channels. For this purpose, we analyze the impairments on quantum channels that result from many strong classical signals. The paper is structured as follows. In section 2,

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

we briefly outline integration options and challenges, before we examine the most dominant problem, being Raman scattering. Section 3 presents the approaches used to model and characterize Raman scattering. Section 5 introduces an experimental set-up for evaluating the QKD integration, which is based on a legacy 20-channel DWDM system. The combined experimental and simulation approach leads to the performance estimates presented in section 6. Finally, Section 7 summarizes and concludes the paper.

2. Integration of quantum key distribution in metropolitan area networks

The limited reach of weak quantum signals binds its distribution to a rather small range. To become scalable, means to cascade QKD encrypted links and to integrate QKD into conventional telecommunication networks need to be defined [18]. The scheme for a smooth integration of QKD in the metropolitan area is sketched in Fig. 2. It envisages the integration of QKD assuming the coexistence scheme, where quantum channels, the key distillation channel and all classical communication channels are transmitted over the same fiber, hop-by-hop multiplexed/demultiplexed using a so called QKD combiner/separator to sensibly add/drop/bypass the weak quantum channels.

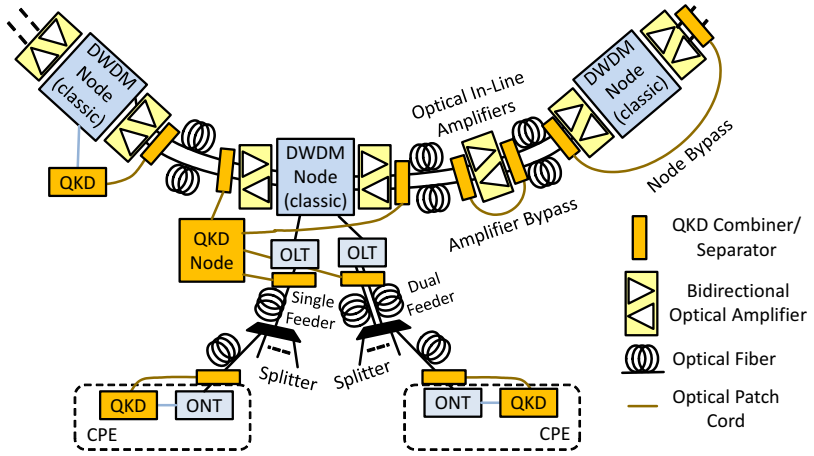

Fig. 2. Deployment of QKD in metropolitan area networks using a smooth integration in the co-existence scheme (CPE: Customer Premises Equipment, ONT: Optical Network Terminal, OLT: Optical Line Terminal).

2.1. Beyond QKD point-to-point links

To extend QKD from static point-to-point key-exchange among terminals to an end-to-end approach based on switched quantum channels, various optical components are needed: optical filters (muxes/demuxes), splitters and optically transparent switches, e.g., based on micro-electro-mechanical systems (MEMS). These components need to be specifically selected to support the weak quantum signals residing in potentially uncommon wavelength regions. Similar to the QKD combiner/separator units required to realize the co-existence approach, these are necessary to realize the transparent QKD overlay nodes.

The influence of such additional components on the quantum channel needs to be considered in the QKD overlay design because these determine the quantum signals reach, which in turn limits the span of the transparent sections and thus the QKD overlay's reach. Thus, any QKD network needs to be designed in its whole, including all signal degrading components along all

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

QKD paths. To share quantum channels along multiple terminal pairs, a feasible technique to multiplex/demultiplex the quantum signals is additionally required.

Topologies to be considered include point-to-point and point-to-multipoint, representing typical access topologies, as well as ring and meshed topologies, representing common metro topologies. Only put together these reveal the true topology necessary to interconnect distributed QKD terminals such that QKD enabled metropolitan area network results.

2.2. Challenges of the coexistence approach

Realizing the coexistence approach raises two specific challenges. First, quantum signals cannot pass amplifiers. These have to be bypassed using QKD combiner/separator units. Actually, if the degradation caused by any classical data network component is more than what a bypass causes, bypassing the component shall be foreseen in order to maximize the achievable secret key rate. Second, QKD systems are extremely sensitive to losses and noise. Strong conventional signals may constitute severe impairments on the weak quantum signals [6], as identified and analyzed in [11, 12, 15, 17, 18].

The 3rd transmission window around 1.5 μm (C-band), widely used for long-range communications due to the low attenuation down to 0.2 dB/km, is also very attractive for QKD systems. However, coexisting classical signals within the same band cause serious impairments [15, 18]. There have been several successful experiments demonstrating the use of the C band for QKD [5], but also showing limitations regarding the acceptable power levels and number of channels [16].

The band around 1.3 μm (O-band) shows higher attenuation of about 0.3 dB/km and is traditionally used for local area and access networks and thus today likely occupied by strong signals. Recent trends in optical access networks indicate that in order to achieve high data rates above 10 Gbit/s and due to the wide availability and maturity of the DWDM technology for the C-band, this technology will increasingly be used also in the access area within a few years' time (e.g. in NG-PON2, radio front/backhaul). Carefully taking into account all those advantages and disadvantages we decide to allocate the quantum channels in the 1.3 μm region (O-band) under assumption that conventional channels will reside in the C-band. As a consequence, the influence of numerous nonlinear effects such as four-wave mixing, Brillouin and Rayleigh scattering can be avoided by allocating the quantum channel spectrally far away from classical data channels. However, Raman scattering still represents a source of bothersome noise photons in the quantum channel, even if the spectral separation between the quantum and classical channels is 200 nm and more, as here assumed.

3. Modeling of Raman scattering

Scattering effects in the fiber medium poses one of the major sources of the noise in QKD channels. The scattering related to acoustic vibrations (Brillouin scattering) can be mostly neglected because of its low bandwidth (1-10 GHz), so Brillouin scattering does not have a considerable influence on QKD channels positioned spectrally far away from classical channels. In contrast, Raman scattering, where optical phonons are involved, introduces large spectral shifts with a large offset from the incident (pump) wavelength. In case of Stokes scattering, part of the photons energy is absorbed by the fiber resulting in the generation of scattered waves at lower frequencies. On the other hand, the resulting excited phonon energy is transferred to a photon at a higher frequency, i.e., a lower wavelength, in an anti-Stokes process. The anti-Stokes scattering is less effective as it requires the pre-existence of vibrational modes, which makes the wavelengths below the wavelength of data channels more preferable for QKD. While this difference is not significant for fibers at room temperature, an allocation of QKD channels below the wavelength of crosstalk-inducing data channels, e.g. in the O-band, offers additional

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

benefits such as using the standard telecom components for the O-band and enjoying a large spectral separation from the C-band wavelengths.

For optical fibers, the Raman gain is usually defined by the Raman gain coefficient, $RGC(f_p,\Delta f)$ [m/W]. This gain relates the power of the pump, f_p, and the scattering strength (offset by Δf) and can be experimentally measured. For modeling purposes, the Raman gain can be characterized by the Raman gain factor, $g(f_p,\Delta f)$ $[\frac{1}{Wm}]$, which is the Raman gain coefficient divided by the effective core area of the fiber, A_{eff} $[m^2]$. Raman gain profiles containing the chosen pump frequency, f_p, and the measured Raman gain factor across a frequency offset range, Δf, can be used in simulations in order to roughly evaluate the noise magnitude in the quantum channel. This profile is independent of fiber dimensions such as A_{eff} and can be re-scaled on-the-fly according to chosen pump wavelengths and signal powers.

A fiber model based on a solution of the full Schrödinger equations as implemented in the commercial simulation tool *VPITransmissionMaker* [19] is used for simulation studies. The Raman gain profiles are adapted to fit our measurements. The original maximum offset parameter has been extended from 35 THz to more than 50 THz and a new Raman gain profile generated by implementing the intermediate-broadening model [20] and using data obtained by measurements. The intermediate-broadening model provides a simple analytic expression which fits the shape of the Raman gain spectrum and the Raman response function of silica fibers. The approach utilizes a convolution of Lorentzian and Gaussian functions that represent multiple vibrational modes. For example, the sharp peak in the Raman spectrum of silica fibers at around 400 cm^{-1} offset corresponds to the bending of an Si-O-Si dihedral angle. At this offset each Lorentzian peak can be seen as a physical representation of a different equilibrium value of the dihedral angle [20]. The expression for the Raman response functions is

$$h_R(t) = \sum_{i=1}^{13} \frac{A_i^{'}}{\omega_{\upsilon,i}} exp(-\gamma_i t) exp(-\Gamma_i^2 t^2/4) sin(\omega_{\upsilon,i})\theta(t) \tag{1}$$

and the Raman gain function (i.e., the Fourier transform of the Raman response functions) is given by

$$s(\omega) = \sum_{l=1}^{13} \frac{A_i^{'}}{2\omega_{\upsilon,i}} \int_0^{\infty} exp(-\gamma_i t)\, exp(-\Gamma_i^2 t^2/4)\{cos[(\omega_{\upsilon,i}-\omega)t] - cos[(\omega_{\upsilon,i}+\omega)t]\}\,\mathrm{d}t, \tag{2}$$

where $A_i^{'}$ is the amplitude of the i^{th} vibrational mode, $\omega_{\upsilon,i}$ is the center vibrational frequency for mode i, γ_i and Γ_i are Lorentzian and Gaussian mode linewidths, respectively. $\theta(t)$ represents the unit step function, being one for $t \geq 0$ and zero otherwise. Note that we use here, similar to the approach presented in [20], thirteen Gaussians with various widths and amplitudes that are centered at various frequency offsets, where each Gaussian corresponds to a different vibrational mode in fused silica.

The envelope curve generated from Eq. 2 is only proportional to the Raman gain spectrum and needs to be normalized. The peak of the envelope curve has to be chosen as reference point and the scaling performed according to the peak amplitude of the SMF-28 NIST reference curve [21,22] and other empirical data. The resulting Raman gain spectrum is depicted in Fig. 3. We performed measurements to verify our simulation model. Both simulation and measurement are shown in the inset of Fig. 4.

4. Simplified model of a QKD system

The selection of an appropriate wavelength for a QKD link as discussed in Section 2.2 is based on assumptions regarding its resistance against uncorrelated noise photons. Highly optimized

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

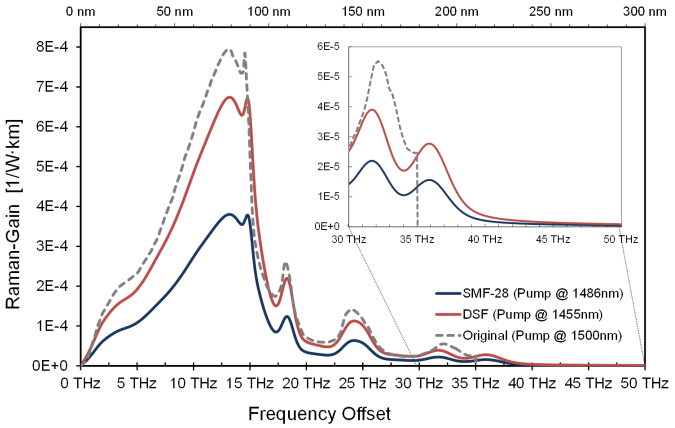

Fig. 3. Raman gain profile as used in simulations.

systems [6] with narrow-band attenuated laser emission and accurate filtering in wavelength and time can extract the photons carrying modulated qubit information much better than typical university research systems designed for operation at dark fibers. In the case these research systems are embedded in telecom equipment, they will suffer from background noise generated by telecom communication carriers. This work indicates the level of expected background photons to select the right wavelength regime for the quantum channel. With the following simplified model of a QKD system we introduce an indicative acceptance rate of 1 million noise photons per second and nanometer for a reliable operation [15].

For Alice we assume a weak laser pulse system operated at a pulse repetition rate of 10 MHz (limited by the detector opening frequency) and a typical number of photons/pulse of $\mu = 1/10$. The quantum channel is ideal, but suffers from transmission losses. We assume here a transmission loss of 13 dB. At the receiver, Bob can expect the arrival of approximately 50,000 photons per second. InGaAs SPADs are gated with 10 MHz in accordance to the expected photon rate with a time window of 1ns, so photons are detected only during a time period of 10 ms within a second. For the sake of simplicity, we do not consider here the effect of the detector dead time. Assuming the use of the BB84 protocol, every in-band noise photon reaching the detectors within this 1% of time in which detection is possible has the chance of 50% to cause an error event. To the end, overall 100,000 background photons per second would generate an additional quantum bit-error rate (QBER) of 1%. A filtering in wavelength by commercial 25 GHz-DWDM grid filters would reduce the noise photon flux and allow $\approx 10^6$ photons/(s·nm) to cause an additional QBER in the order of few percent. We will use this value in the following diagrams as a guide to the eye.

5. Combined QKD and metro networks

To enable a reliable exchange of qubits in presence of strong classical signals an accurate consideration of the impairments caused by Raman scattering and an effective noise filtering in the O-band are essential. We first concentrate on defining and analyzing the method for combining and separating QKD and classical signals by spectral filtering. A cascade of two band multiplexers/demultiplexers (far wavelength-division multiplexers - FWDMs) is used as shown in Fig. 4, because with a single typical band filter sufficient band rejection cannot be achieved. Additionally, a narrow-band filter (0.1 nm) is needed in front of the QKD receiver to further reduce the noise level. The experimental setup depicted in Fig. 4 is applied to experimentally analyze the combining/separating of quantum and classical channels and also to evaluate the

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

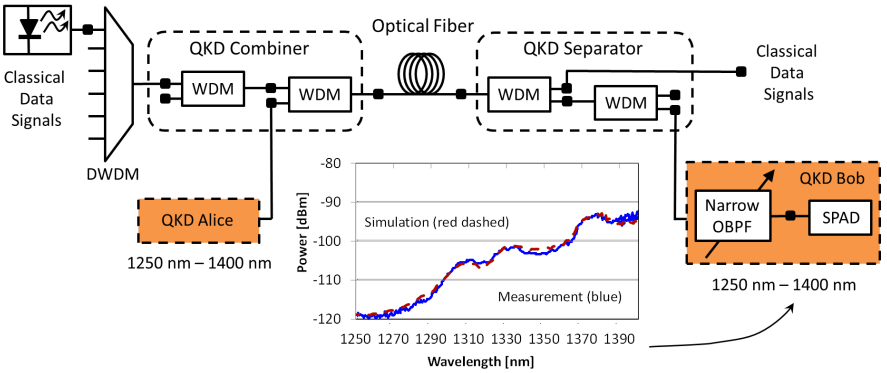

Fig. 4. Experimental and simulation setup for analyzing the influence of forward Raman scattering on integrated QKD systems in metropolitan area networks. Inset measurement and simulation results for 14 km of standard single mode fiber (SSMF) and the wavelength range from 1250 nm to 1400 nm. The resolution bandwidth was 0.1 nm in both cases (measurement and simulation). FWDM: Far Wavelength Division Multiplexer.

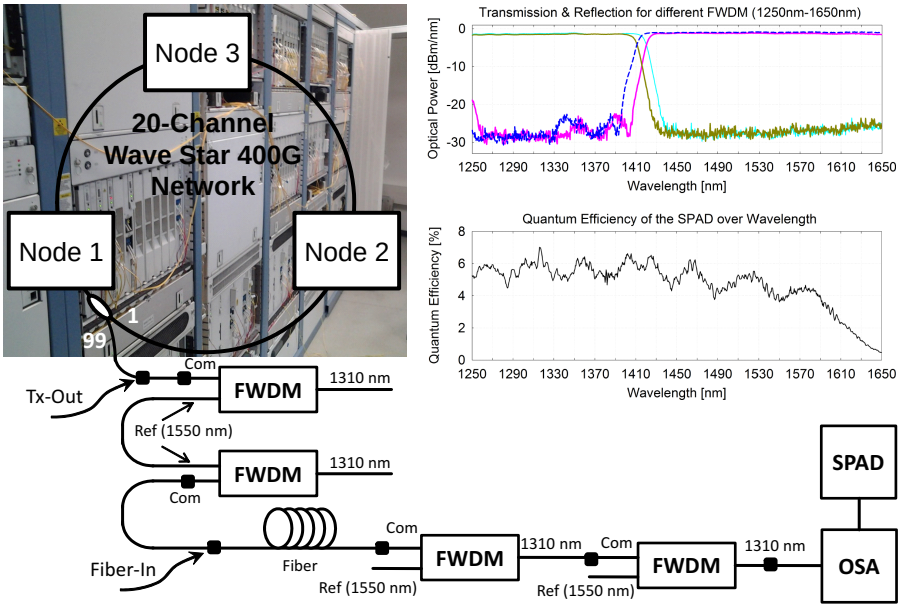

Fig. 5. Experimental setup for characterization of QKD integration in metropolitan area networks. Inset measured transmission and reflection curves for different FWDM components used to combine/separate quantum and classical channels as well as measured quantum efficiency of the single photon avalanche photodiode (SPAD) used to count noise photons below 1410 nm.

influence of Raman scattering. Because noise levels below -90 dBm can hardly be measured with conventional optical spectrum analyzers (OSA), we count the noise photons using a single-photon avalanche photo diode (SPAD). A narrow coherent 1550.12 nm continuous-wave (CW) laser source with 3.5 dBm optical output power is used as Raman pump. The measured forward Raman scattering in a 14 km long standard single mode fiber (SSMF) is shown inset in Fig. 4 together with the simulation result (dashed lines). At 1250 nm the noise level is as low as -120 dBm and increases toward longer wavelengths. Above 1360 nm and 1400 nm the optical

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

noise power rises above -100 dBm and -95 dBm, respectively, which already prohibits reliable exchange of qubits in these spectral regions. Experimental and simulation results fit very well over the wavelength range of interest, i.e., between 1250 nm and 1400 nm.

6. Characterization of QKD integration

We analyze the performance of QKD integration in the metropolitan area by applying a combined experimental and simulation approach. First, we configured a 3-node commercial DWDM system (Lucent Wave Star OLS400G) to provide 20 DWDM channels (classical data channels). A generic picture of the configured ring network containing 3 nodes is shown in Fig. 5. The 20-channel DWDM signal generated in node 1 and amplified by a booster erbium-doped fiber amplifier (EDFA) is tapped off using a 99/1 optical coupler. Cascaded 1310/1550 far wavelength-division multiplexers (FWDMs) are used for combining and separating quantum channels with classical data channels and to further suppress the background noise in the O-band to a tolerable level. Measured transmission and reflection curves for FWDM components and quantum efficiency of the SPAD are shown inset. Note that the SPAD is used to count noise photons within the O-band, while the spectrum above 1410 nm is measured using an OSA.

6.1. QKD link

In order to reflect the variety of installed fiber types, we choose standard (ITU-T G652-B) and low-water-peak single mode fibers (G652.D) of different age and length. Additionally, to address the influence of connectors and splices, we consider a 27 km long fiber made of two pieces (14 km and 13 km) that are connected with each other by connectors. The fibers are characterized by a white light source to obtain the attenuation curve. The measurement results are presented in Fig. 6.

We performed measurements on the fibers characterized in Fig. 6 using the setup shown in Fig. 5. As can be seen from Fig. 7, the noise within the O-band is mainly caused by the forward Raman scattering. A noise level below 1 million photons/(s·nm) has been obtained up to 1310 nm, for all fiber types and lengths considered. The difference in noise levels between the considered fibers lies within a range of 10 dB. This emphasizes the need for characterization of the installed fibers prior to considering QKD integration. Coexisting strong signals within the C-band, i.e., the 20-channel DWDM signal, the optical supervisory channel (OSC) at 1510 nm and the residual power of the filtered EDFA pump at about 1480 nm, cause a reduction of the useable wavelength range for about 60 nm when comparing to the single channel measurement shown in Fig. 4.

Since scattered signals propagate in both forward (together with data signals) and backward (in opposite to data signals) directions, we also have to consider the backward Raman. In systems where either telecom or quantum signals are transmitted bidirectionally, which can be the case in some access networks, the backward Raman scattering becomes important. In order to measure the effect of backward Raman scattering, we slightly modify the experimental setup presented in Fig. 5 by connecting the fiber input to the common (Com) output of the third FWDM device (see Fig. 8). Thus, the DWDM signal enters the fiber through the Com port, while the backward scattered (as well as reflected) photons pass through the reflective (Ref) port to be further filtered by the fourth FWDM and counted by SPAD and OSA.

The noise spectrum measured using the setup depicted in Fig. 8 is shown in Fig. 9. The obtained available wavelength range is similar to that obtained for the forward scattering. However, the difference in noise levels for long and short fibers is lower. Moreover, the effect of Raman backward scattering is strongest for the 14 km long fiber, which is an expected outcome. This is due to a higher attenuation in longer fibers, which effects both pump signal and

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

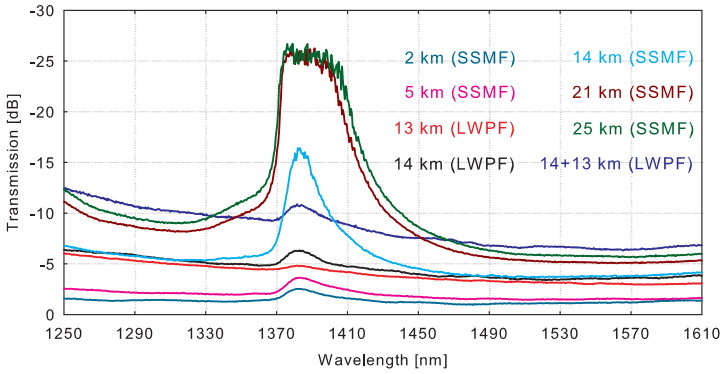

Fig. 6. Characterization of fiber attenuation for different fiber types and lengths obtained using a white light source. Low-water-peak fibers (LWPF) and standard single mode fibers (SSMF) in one piece or made from two pieces (14 km + 13 km) are chosen to reflect the variety of installed fibers.

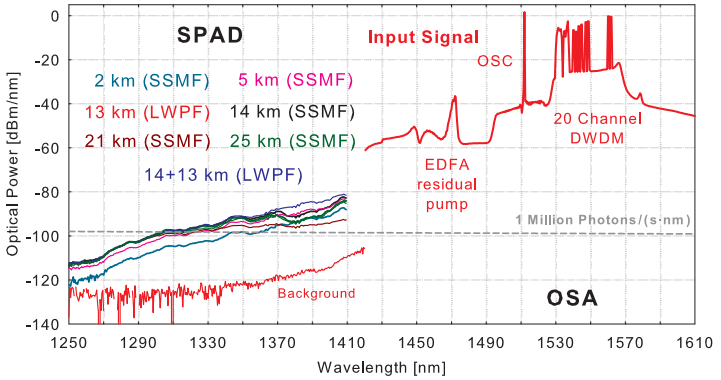

Fig. 7. Forward Raman scattering: noise power level within the O-band caused by the strong classical signals in the C-band of a conventional DWDM system in operation. Results are shown for different fiber types and lengths. Also background noise of the signal before transmission is shown (red line).

scattered photons. Since the pump power decays exponentially with fiber length, the major contribution of noise is saturated at a certain fiber length and gets reduced by exceeding this threshold.

In order to estimate the contributions of the data channels, the optical supervisory channel (OSC) and the residual EDFA pump to the noise in the O-band, we carried out measurements with OSC only, with OSC and EDFA pump and with OSC and data channels without EDFA pump. The input signals used to characterize the main cause of the noise are obtained by using appropriate filters to split up the signal generated by node 1 into signals I to IV presented in Fig. 10.

The corresponding results for cases I to IV and a fiber length of 14 km are shown in Fig. 11. The blue curve represents the measured photon noise level in the O-band when the DWDM signal and the residual EDFA pump are removed (case II). Here, the background noise noise is only due to the OSC signal. Even though OSC is only a single channel, it has a significant influence on the noise generated in the O-band since it is allocated at least 20 nm closer to the quantum channel than the data channels. To obtain the green curve representing case IV, we filter out the DWDM signal. Here, an increase of the photon noise by about 2 dB in comparison

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

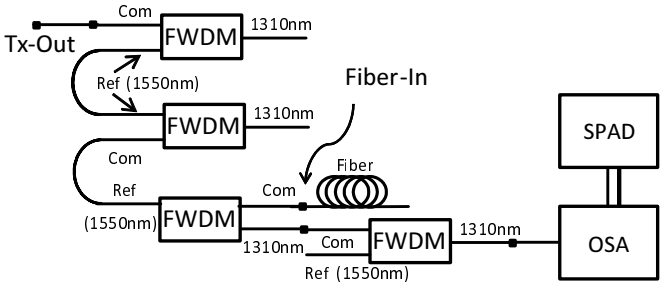

Fig. 8. Setup for measuring the noise level caused by backward Raman scattering.

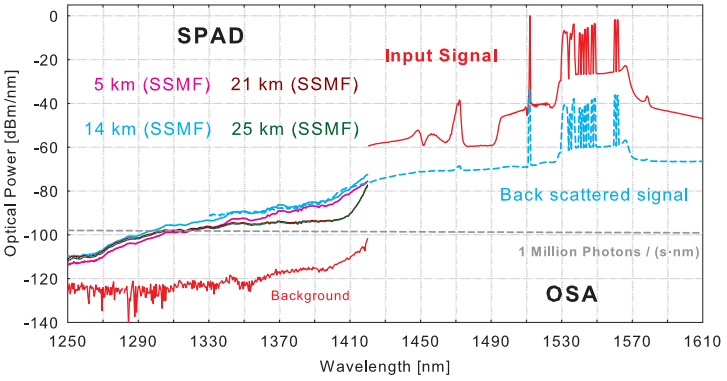

Fig. 9. Backward Raman scattering: noise power level within the O-band caused by the strong classical signals in the C-band of a conventional DWDM system in operation. Results are shown for different fiber types and lengths. Also background noise of the signal before transmission is shown (red line).

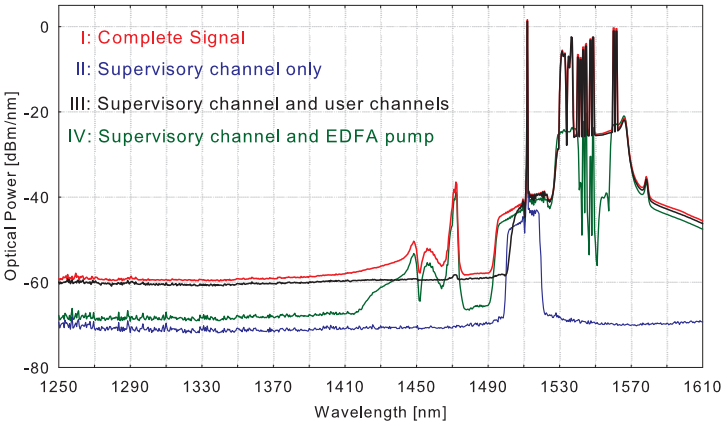

Fig. 10. Fiber input signals for characterizing the main cause of the Raman-generated noise in the O-band measured by an OSA.

to case II has been observed, which is mainly due to the EDFA's amplified spontaneous emission (ASE) noise. Finally, we filter out the residual EDFA pump only in order to assess its influence. The corresponding noise spectrum is shown by the black curve (case III), which is almost identical to the red curve (case I - entire signal) for the forward and lies slightly below it for the backward scattering. This result indicates that the influence of the residual EDFA pump

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

signal can be neglected. Even though it is spectrally closer to the O-Band than the OSC, its low power (about -40 dBm) does not suffice to generate many scattered photons in the O-band. The 20-channel DWDM signal contributes by up to 5 dB to the photon noise. This significant contribution varies with wavelength, the number of classical channels and their power levels.

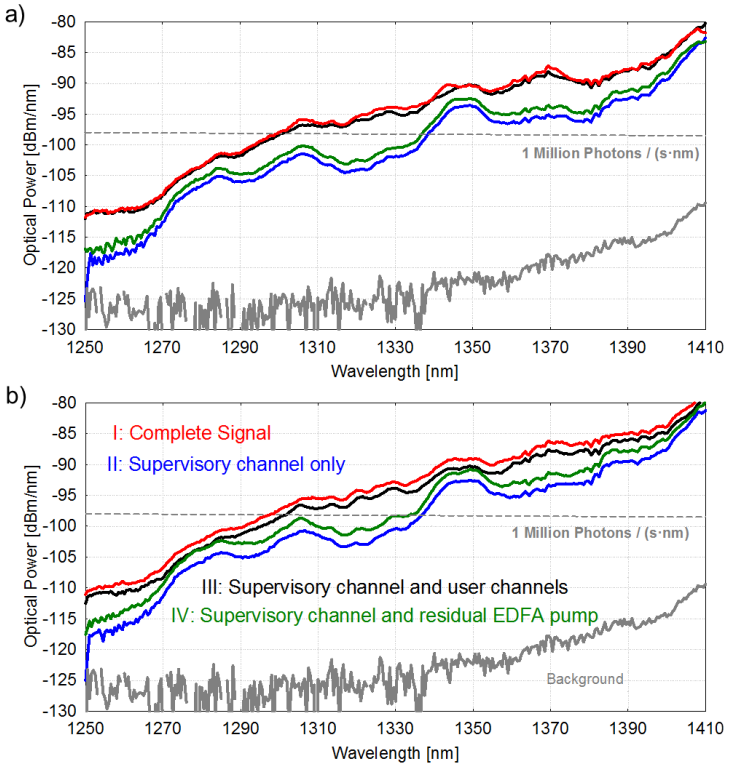

Fig. 11. Contributions of signals I, II, III and IV (see Fig. 10) to the noise in the O-band a) for forward and b) backward scattering. Also background noise of the signal (back-to-back) before transmission is shown (grey line).

6.2. Add/Drop filters for implementing QKD combiners/separators

The presented experimental results are obtained using FWDM filters that separate incoming and outgoing wavelengths above and below about 1420 nm, as it is shown in the inset of Fig. 5. By introducing FWDM filters with a separation at 1510 nm a fifth input signal can be generated, which comprises the DWDM classical data signals only, while the supervisory channel and EDFA residual pump are suppressed. In analogy to the setup shown in Fig. 4, two cascaded 1510 nm-FWDM filters are inserted before the fiber input. The supervisory channels' power is hereby attenuated by about 35 dB and the residual EDFA pump is completely suppressed. The input is displayed by the dashed brown line in Fig. 12.

In order to separate the outgoing C- and O-band signals after the fiber, two FWDMs are once again needed. As it turns out a cascade of 1520 nm FWDM filters is not sufficient to suppress the background noise below -100 dBm and is therefore unsuitable to distinguish the originated impairments at such low energy levels. We therefore employ the well tried 1410 nm FWDMs after the fiber for our experimental setup. The Raman curve resulting from this combination of 1510 nm filters before and 1420 nm FWDMs after the investigated 14 km fibre is shown by the brown line in Fig. 12 (Input V). The comparison with the results obtained using the

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

inputs II and III (Fig. 10), where the supervisory channel is fully present, is shown in Fig. 13. As indicated by the black arrows, the generated noise spectra shows an inverted behavior for certain wavelengths depending on whether the OSC is fully present or not. This behavior can be explained as follows. Depending on the wavelength and the strength of classical signals certain modes seem to become more or less dominant, which causes a wavelength dependence of the Raman counts with respect to input signal wavelengths. This is particularly interesting for the wavelength window between 1310 nm to 1350 nm. Here, the absence of the data signals causes a drop in counts of almost 10 dB.

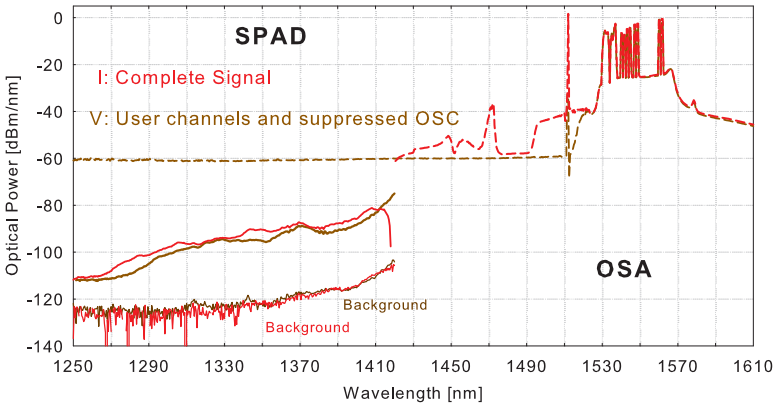

Fig. 12. Raman counts obtained for 14 km SSMF using 1510 nm and 1410 nm FWDM.

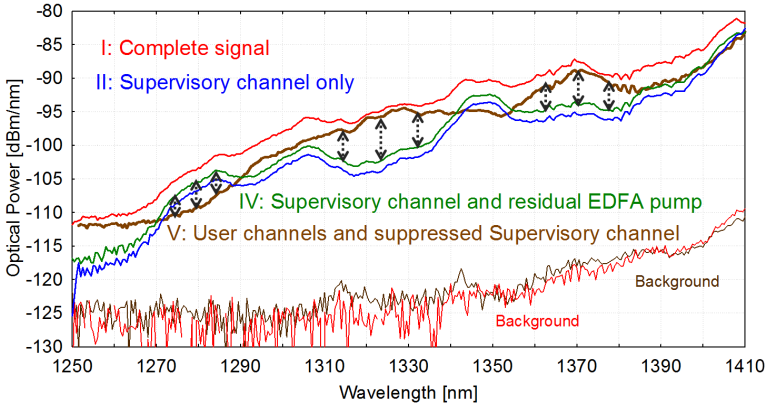

Fig. 13. Raman scattering caused by signals with optical supervisory channel (OSC) (II and III) show a different behavior from the signal with suppressed OSC.

6.3. QKD bypass

As already mentioned in Section 2, a smooth integration of QKD able to provide an end-to-end data encryption in the metropolitan area presumes implementing methods for multiplexing and switching of quantum channels as well as an efficient bypass of some conventional network elements. Since weak quantum signals cannot pass opaque network nodes and amplifiers without being destroyed, those elements have to be bypassed. An efficient bypass of amplifiers and network nodes can be realized using two QKD combiners/separators and a short piece of fiber to directly connect them, thereby providing a low-attenuation bypass for quantum channels,

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

while data channels are being processed as usual. The simulation setup we use to analyze the influence of the amplifier and node bypass is is shown in Fig. 14 a) and Fig. 14 b), respectively. Similar to the experimental setup shown in Fig. 5, we generate a 20-channel DWDM signal together with an OSC signal at 1510 nm. The signal generated in the simulator and launched into the fiber perfectly mimics the measured signal shown in Fig. 10 - case I (complete signal). We set all the simulation parameters such as fiber characteristics, background noise spectrum and power/bandwidth of all signals according to the measured data.

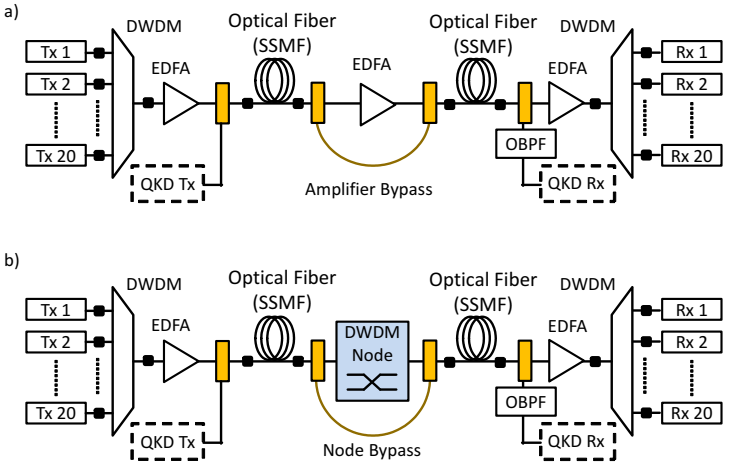

Fig. 14. Simulation setup for characterizing a) amplifier bypass and b) node bypass. Note that the bypassed node is assumed to be opaque, i.e., the incoming DWDM signal is terminated at the input and a new one generated at the output. EDFA: Erbium-Doped Fiber Amplifier.

The simulation results for amplifier and node bypass are presented in Fig. 15. For comparison purposes, we also show the spectrum of the 14-km point-to-point link (red curve in Fig. 15). It is evident that the additional filtering needed for bypass causes a reduction of the noise in the O-band, also through suppressing the noise generated within the C-band in the first fiber span, which has a positive impact on the Raman noise being generated within the O-band in the second span. Especially the bypass of an opaque node, as depicted in Fig. 14 b), benefits from a noise reduction of more than 10 dB in comparison to the line without bypass because the signal from the first span is terminated in the node and a new, low-noise one generated. As regards fiber length, the minimum noise level is obtained, as expected, for 2×2.5 km, while for 2×10 km, the generated noise is highest. This is in agreement with the experimental results reported in Figs. 7 and 9 because similar reasoning regarding attenuation of Raman noise in longer fibers also holds here.

As already mentioned, weak quantum signals are not only affected by noise photons, but also are significantly impaired by attenuation. The two QKD combiners/separators required for QKD bypass introduce about 1 dB of attenuation each, which causes about 2 dB additional loss in the bypass configuration. However, for typical distances in the metropolitan area, the attenuation of optical fibers contributes considerably more to the overall loss than the QKD combiners/separators. For example, attenuation introduced by 40 km of SSMF is about 12 dB for the O-band, which is six times higher than the insertion loss of a QKD combiner/separator. On the other hand, the impact of the increased loss of QKD bypass is compensated by the reduced noise level (see Fig. 15).

#232520 - $15.00 USD Received 15 Jan 2015; revised 23 Mar 2015; accepted 24 Mar 2015; published 14 Apr 2015

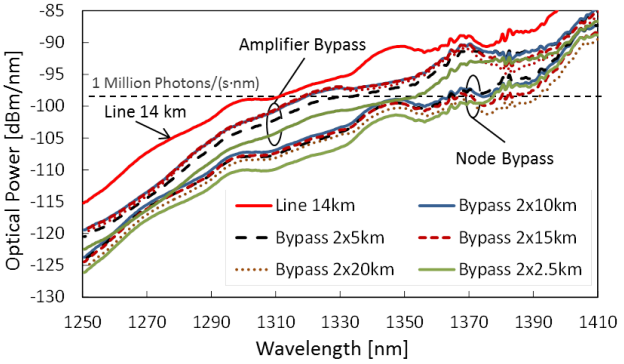

Fig. 15. Simulation results for amplifier and node bypass.

6.4. Discussion

As the presented measurements show, an integration of QKD systems into existing metro and access networks boils down to the question whether a QKD scheme can be found that withstands the high noise levels almost entirely caused by Raman scattering originating from the multiplexed strong classical data channels. Although an elaborated positioning of classical channels and quantum channels may reduce noise to a tolerable level for the quantum channel, key rate and user scaling still remain challenging issues. Possible approaches to tackle these problems are filtering in the time and the wavelength domain. The latter can be achieved with standard equipment used in telecommunication networks, as shown in the presented approach that propose the allocation of quantum channels in the O-band. For wavelengths shorter than 1310 nm the noise can be reduced to acceptable levels. This approach allows bypassing active network components such as optical nodes and amplifiers as well as potential multiplexing and switching of quantum signals towards QKD networks. However, without appropriate time filtering the photons of interest are hard to separate from noise. Recently developed detectors with gating times in the sub-ns range are able to reduce noise by about 10 dB [6], making it likely to detect a photon sent by Alice, when exact timing information is available.

7. Conclusions

In this paper, we proposed and investigated an approach for reliable exchange of quantum keys over existing fiber infrastructures in coexistence with many classical (conventional) data channels operated at usual power levels. In particular, we analyzed the influence of Raman scattering caused by a commercial 20-channel DWDM system on quantum channels allocated in the O-band (around 1.3 μm). The presented measurements show that an elaborated positioning of classical and quantum channels and filtering in the time and wavelength domains can reduce the noise to a tolerable level for a QKD system. The positioning of quantum channels in the O-band simplifies the bypassing of active network equipment such as network nodes and amplifiers as well as multiplexing and switching of quantum signals toward QKD networks. This approach enables the use of standard equipment to realize a smooth integration of quantum key distribution (QKD) systems in deployed metropolitan area networks.

Acknowledgment

This work has been supported in part by the project ”QKD-Telco: Practical Quantum Key Distribution over Telecom Infrastructures” (contract No. 835926), within the FIT-IT programme funded by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT) in coordination with the Austrian Research Promotion Agency (FFG).

Appendix C

SPIE Proceedings

Demonstration of a coexistence scheme between polarization-entangled QKD and classical data channels

Florian Hipp[*a,b], Michael Hentschel[a], Slavisa Aleksic[b], Andreas Poppe[a] and Hannes Hübel[a]
[a]Safety & Security Department, AIT Austrian Institute of Technology GmbH, Donau-City-Strasse 1,1220 Vienna, Austria; [b]Institute of Telecommunications, Vienna University of Technology, Favoritenstrasse 9/388, 1040 Vienna, Austria

ABSTRACT

Incorporating single photon links used for quantum communication applications like quantum key distribution is a challenging task. Direct contamination from the strong classical signal and induced Raman scattering easily obscures the weak quantum signal. Generating entangled photons in the O-band might allow the coexistence of classical and quantum signals. We present results demonstrating the feasibility of transmitting entangled photons and strong classical communication signals over the same fiber.

Keywords: Quantum cryptography, entanglement, wavelength division multiplexing, coexistence scheme

1. INTRODUCTION

Quantum key distribution (QKD) promises a high level of communication privacy and security through utilizing quantum physical properties of optical signals. Distributing quantum mechanically secured keys over optical fiber networks will substantially enhance the security of digital communication. Current QKD systems however require a dedicated point-to-point fiber between sender (Alice) and receiver (Bob) to act solely as the quantum channel. This need arises because additional signals, in particular classical telecommunication signals, on the same fiber lead to high levels of noise and in most cases the weak quantum signal cannot be recovered afterwards. The high cost of a dark fiber which is exclusively used for the quantum data transfer is likely to prohibit a large scale roll-out of QKD over metropolitan area networks (MAN) and passive optical networks (PON). It is therefore essential for the further grow of QKD in telecommunication networks that the quantum signal and classical data is transmitted over the same fiber. Integrating a quantum signal and classical channel on the same fiber, also referred to as a *coexistence scheme*, has recently been demonstrated in a number of QKD implementations[1-5].

These implementations have all been based on classical laser pulses to transmit the quantum state. In contrast to the weak laser pulse approaches it is also possible to exploit the entanglement of two photons[6]. Spontaneous parametric down-conversion (SPDC) in non-linear crystals can be used to generate such pairs of photons that can be distributed to Alice and Bob. Non-classical correlations measured at Alice and Bob are then used to establish a secure key.

The main problem for entangled photons produced by SPDC is the relative low rate and a rather wide spectral bandwidth of a few nanometers. This technique to generate quantum signals suffers therefore disproportionate from the high background in the optical fiber caused by the strong classical signal and has therefore not yet been implemented in a coexistence scheme. Studies[7-9] into the origin and spectral distribution of noise photons created by Raman scattering have shown that, while impossible to inject the quantum signal close to the classical signal, it would be possible to operate the quantum channel in the O-band region of the telecommunication window while maintaining a strong classical data signal in the C-band as shown in Figure 1. Entangled photons have the added benefit that they are not only usable for QKD but are also essential for other quantum communication primitives, like quantum teleportation[10], device independent QKD[11] and blind quantum computing[12]. The demonstration of coexistence of classical signals and entangled photons is therefore a key requirement for future quantum networks.

*florian.hipp.fl@ait.ac.at; ait.ac.at

Quantum Optics, edited by Jürgen Stuhler, Andrew J. Shields, Proc. of SPIE Vol. 9900
99000P · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2230222

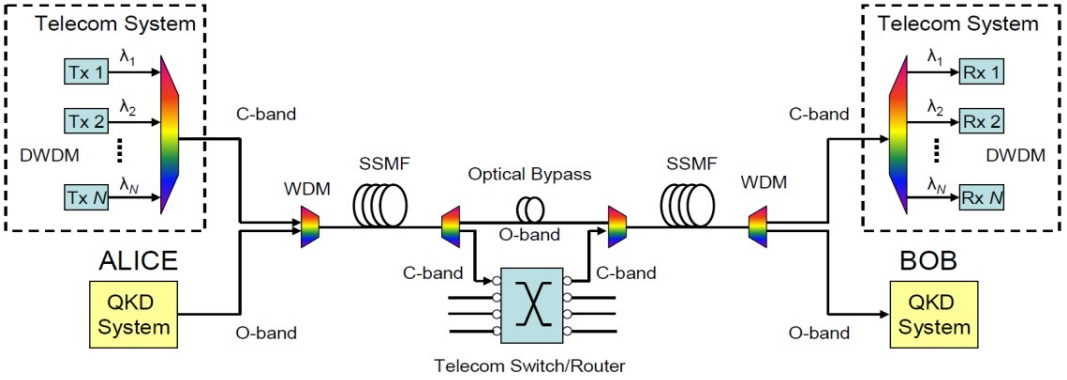

Figure 1. Coexistence scheme of a classical telecommunication link in the C-band with a multiplexed quantum channel in the O-band. The QKD system transmits entangled photons over the quantum channel.

We report here the demonstration of a coexistence scheme using polarization-entangled photons as the quantum signal in the O-band. In section 2 we present the source of entangled photons detailing the conversion process to arrive at a wavelength of around 1310nm for one of the photons from the entangled pair. This photon is sent via the optical fiber to Bob, whereas the remaining photon of the produced pair is detected locally at Alice. The influence of Raman scattering is presented in section 3. The additional noise was measured in a variety of settings, e.g. by changing the number of classical channels and the overall power and length of fiber. Filtering techniques are discussed to reduce the background photons such that a key generation is possible.

2. DESCRIPTION OF ENTANGLEMENT BASED QKD SYSTEM

2.1 Source of polarization entangled photon pairs

In entanglement based QKD, two communication parties negotiate a secret key by means of quantum effects. In order to provide the communication parties with strong non-classical correlations, they are supplied with entangled photons. These photons are generated in pairs from a source based on SPDC. Here, a nonlinear crystal mediates the decay of pump photons into two daughter photons (historically called signal and idler) fulfilling conservation of energy and momentum. Regarding the former, the wavelengths involved obey the equation $1/\lambda_p = 1/\lambda_s + 1/\lambda_i$. In order to fulfill the latter, phase matching must be ensured. This can be achieved by exploiting the birefringent properties of the crystal or by means of quasi-phase matching, where a structure of periodic poling is imposed on the crystal. This technique can be tailored to ensure a collinear emission of all photons and for maximum conversion efficiency.

In our setup we make use of a periodically poled Potassium Titanyl Phosphate (KTP) crystal with a poling period of $\Lambda = 3.875\mu m$ embedded in a Sagnac interferometer[13]. Figure 2 shows the setup of the complete source. The pump laser is a 405nm single frequency laser with an elliptical beam profile, which needs to be reshaped by means of cylindrical lenses and is focused with a spherical lens to a spot size of 40µm. The polarization is set to diagonal and the phase can be adjusted with a pair of birefringent wedges. Inside the Sagnac loop the two polarization components (horizontal and vertical) are split with a polarizer and sent into the loop with counter-propagating directions. The vertical polarization (clockwise) is flipped to horizontal with a half wave retarder set to 45°. As, to our knowledge, half-wave-plates operating at three arbitrary wavelengths are not readily available, we employ the phase shift of total internal reflection in Fresnel-rhombs to obtain the desired wave retardation. The actual implementation can be seen on the right of Figure 2. In order to provide a complete indistinguishability of the two round trip modes, we placed an identical wave retarder at the according position in the other arm, only set to zero degree. Moreover, a piece of Calcite is placed before the interferometer with its optical axis rotated by 90° with respect to the polarizer, in order to exactly compensate the birefringent effect of the latter. The respective pump beams are then steered by two silver mirrors into the nonlinear crystal where the type-0 down-conversion takes place. Thus, signal and idler photons are generated with $\lambda_s = 586nm$ and $\lambda_i = 1310nm$, respectively. Again, the counter-clockwise mode gets flipped in polarization and is superimposed on the clockwise mode at the polarizer, thus creating the entangled state $|\phi^+\rangle = |H_{586}\rangle\,|H_{1310}\rangle + |V_{586}\rangle\,|V_{1310}\rangle$. The photons are

then separated from the pump beam with a specially designed trichroic mirror and further split into signal and idler with a dichroic mirror. Finally the photons are bandpass filtered and coupled into the optical fibers. The signal photons are analyzed locally in a BB84 module (in the polarizations horizontal, vertical, +45° and -45°) using standard Si-APDs, while the idler photons are transmitted over several kilometers of standard telecom fiber before detection.

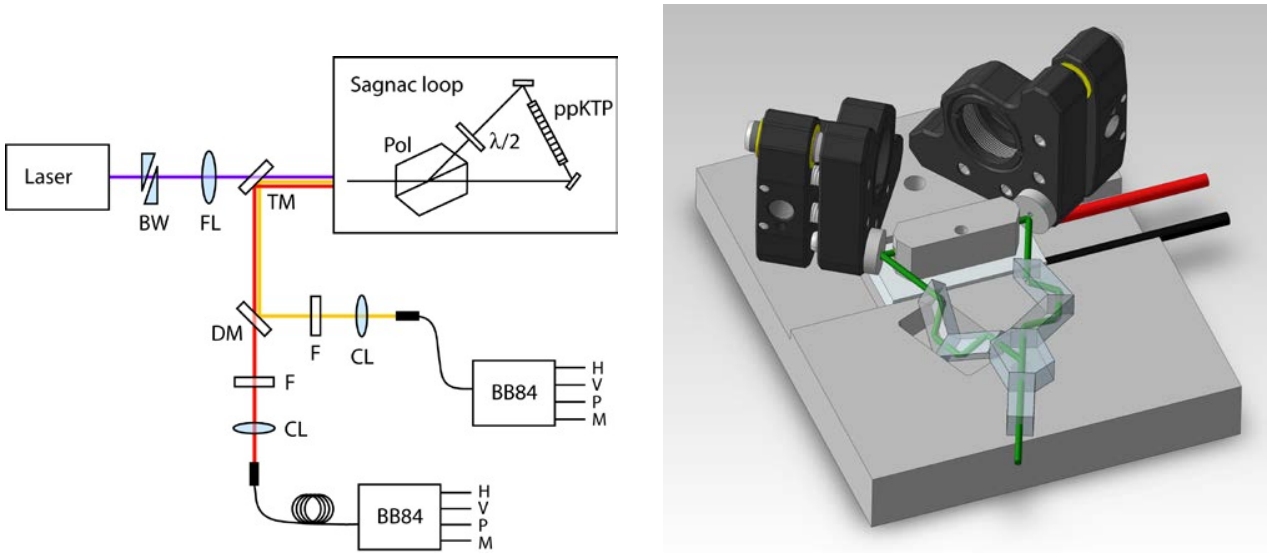

Figure 2. Left: Schematic of the entangled source with birefringent wedges BW, focusing lens FL, trichroic mirror TM, Glan-Thomson polarizer, half wave retarder, KTP crystal, dichroic mirror DM, filters F and coupling lenses CL. Right: A three dimensional model of the Sagnac loop showing the mechanical details and beam paths.

2.2 Time multiplexed detection scheme

The idler photon at 1310nm is measured using a single InGaAs-APD. In the usual setup four such detectors are needed to measure all four polarization states. However the cost of Bob's detection apparatus can be substantially reduced by implementing a technique patented by AIT, as shown in Figure 3. Here, a normal fiber based BB84 module is set up, consisting of a 50:50 beam splitter and two polarizing beam splitters. Then, the four output fibers are extended by different delay fibers and combined with a 4:1 single-mode to multi-mode coupler, which is connected to only one single photon detector. By observing the time-of-arrival of the photons one obtains four correlation peaks, each of which can be attributed to its respective measured polarization.

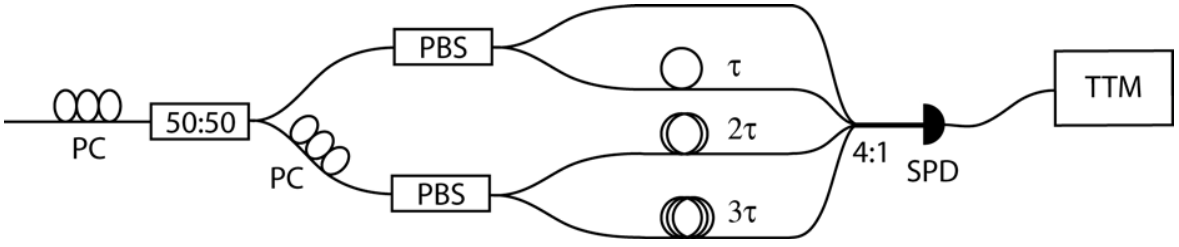

Figure 3. Time multiplexed BB84 detection module with polarization controllers PC, 50:50 beam splitter, polarizing beam splitters PBS, delay fibers, 4:1 single-mode to multi-mode coupler, single photon detector SPD and time tagging module TTM.

3. NOISE MEASUREMENTS AND RESULTS

In order to determine the robustness of our QKD system regarding strong classical channels that are located mainly in the C-Band a suitable filtering has to be applied to reduce the emerging Raman radiation to an acceptable level.

The QKD system itself comprises the Sagnac source and two non-orthogonal polarization measurement devices at Alice and Bob (here called BB84). Since in our scenario the source is located at Alice, she measures her entangled photon (586nm) right away, while the other photon (1310nm) is multiplexed with the classical signal and sent through 4.3km, 8.6km and 15km of SSMF. The schematics of the entire setup, including the classical channel are shown in Figure 4.

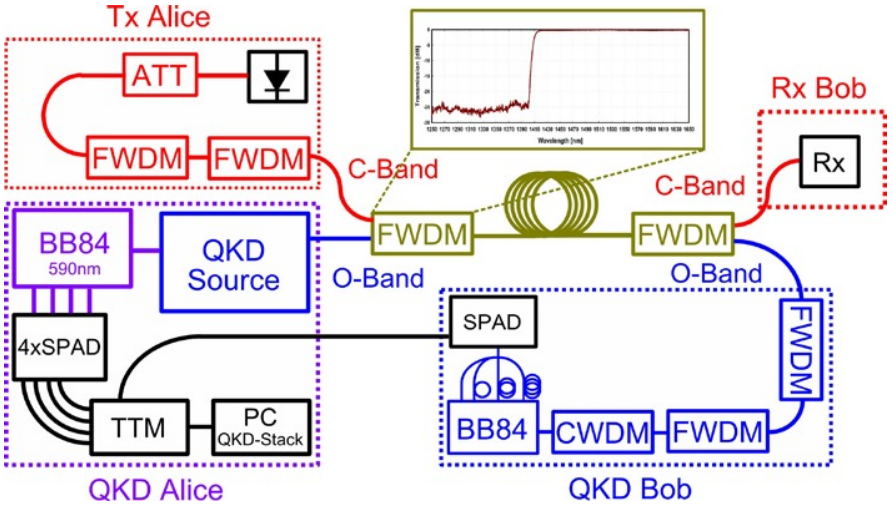

Figure 4. Schematics of the experimental setup for multiplexing quantum and classical signal. The quantum channel is located in the O-band while classical data is transmitted mostly in C-band (also S- and L-band).

Figure 4 shows that a cascade of Far-Wave-Division Multiplexing (FWDM) filters acting as long and short pass filters are needed to separate the C- from the O-Band. Their transmission curve is displayed in the inset of Figure 4. Two of them are used as Add/Drop filters to combine and separate both signals before and after the fiber. Despite this strong filtering an additional CWDM is needed to reduce the impairments originating from the Raman scattering of the classical channels within the fiber.

While the photon pairs on Alice's side are measured with 4 different detectors, one for each polarization, Bob applies only one single photon detector. The information about the polarization of the photon is hereby encoded in the different arrival times. It is therefore mandatory to tag the precise arrival times of each photon at each detector. The Time Tagging Module (TTM), that operates with a timing resolution of 82ps, is able provide a sufficiently fast processing time. In order to assign all photons arriving at Alice to their entangled partners at Bob's side the precise time delay between the two has to be known. This time filtering is achieved by searching for the four correlation peaks arising from the H-H, V-V, 45-45 and -45 - -45 polarization entangled photons. Once this time information is known to the QKD-stack software (pre-sift), the sifting process itself can start to sort for the eligible polarizations. After error correction and privacy amplification a valid, information theoretical secure key is created.

When measured locally, i.e. without a long fiber between Alice and Bob and without multiplexed classical signal, the source produces a raw key rate of around 3000 bit/s with an error rate (QBER) 5.6%. Using a fully operational QKD post-processing stack a secure key with a rate of 220 bit/s can be extracted with this setup. The low overall rate and rather high QBER is attributed to a faulty wedge (BW), which produces spatial beam distortions and phase distortions. Nevertheless the performance of the setup alone can be seen as a benchmark against which the influence of Raman scattering is evaluated. The overall QBER at which key generation is no longer possible lies around 11%.

The upcoming measurements and results are all based on the above setup. They are structured as follows:

1. In section 3.1 we show how a single classical channel at a wavelength of 1550.12nm (DWDM-Grid) is multiplexed with the quantum signal. Various power levels are investigated until the power of the transmitted signal drops below -20dBm, the threshold of a standard PIN-diode receiver. The noise photons as well as QBER are monitored for three different fiber lengths (4.3km, 8.6km and 15.2km).
2. In section 3.1 we increased the number of classical channels to 6, using SFP-Modules of the CWDM grid, 1470nm, 1510nm, 1530nm, 1550nm, 1570nm and 1590nm. The signals are merged to the same fiber using a CWDM and attenuated until the -20dBm threshold is reached. Again noise photons as well as QBER are evaluated for the three fiber lengths.
3. Finally, in section 3.3 we show how the QBER and hence the key rate depends on the wavelengths of the classical channel. Each wavelength of the CWDM grid is hereby multiplexed with the quantum channel. Furthermore starting with 6 attenuated classical channels, lower wavelength signals are successively removed starting from 1470nm until 2 channels remain. This process is compared to successively removing higher wavelengths starting from 1590nm.

3.1 Single Classical Channel

For the first measurement a cw-tunable laser source at 1550.12nm was used to simulate the classical channel. Since the laser shows long spectral sidebands a DWDM filter was applied to receive a narrow signal. A variable attenuator was furthermore used to control the power of the laser in addition to the lasers internal variable power setting. The left graph of Figure 5 shows the obvious behaviour of the QBER when the classical output power is increased. The dashed red line shows the performance of the QKD-system without any classical signal present. The right graph of Figure 5 shows that already for -20dB output power an additional photon count of about 5000 is observed at Bob's detector, hence the raise of QBER.

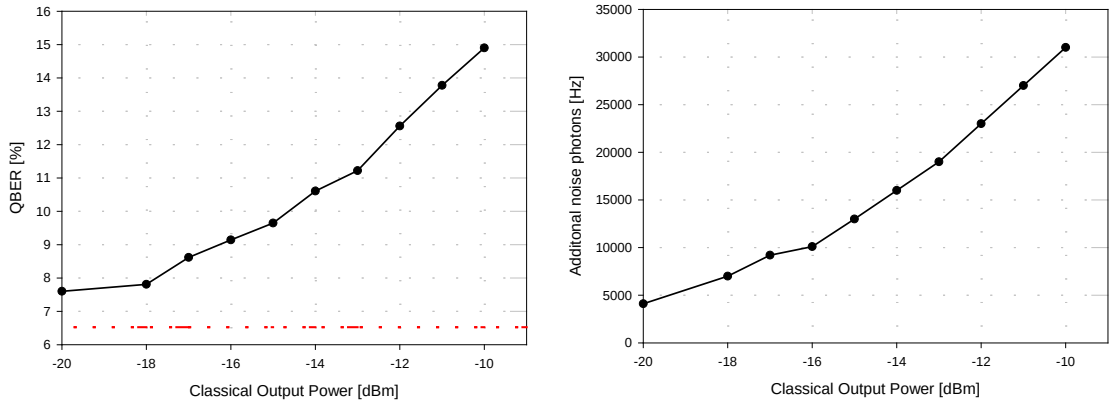

Figure 5. Left: QBER over classical output power of a single channel for 4.3km. The dashed red line indicates QBER with no classic signal present. Right: Noise photons over output power of a single classical channel for 4.3km.

The same measurement has been repeated for 8.6km and a 15.3km fiber, see Figures 6 and 7. In the 8.6km case it is surprising that at a power level of -20dBm almost no influence of the classical channel on the quantum channel can be observed. This becomes even more apparent when we look at the additional noise that is detected at Bob's side. Up to -17dBm only a small number of additional noise photons is detected. It is observed that higher fiber attenuation leads to a higher initial QBER on the quantum channel due to a lower signal to noise ratio. The same applies to the classical channel and to keep the output power constant a higher launch power is required raising the QBER even more due to the increased Raman scattering. The latter effect can be better seen in Figure 8, where only the relative increase of the QBER is plotted, i.e. the base QBER with no classical signal present was substracted. The black curve indicates the measurement with a 4.3km fiber, the red curve 8.6km and the blue curve 15.3km.

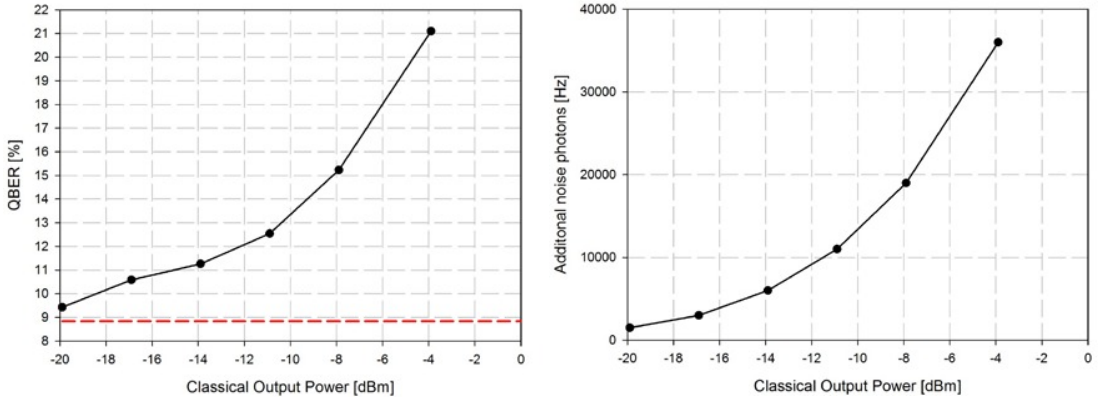

Figure 6. Left: QBER over classical output power of a classical channel for 8.6km. The dashed red line indicates the QBER with no classic signal present. Right: Noise photons over output power of a classical channel for 8.6km.

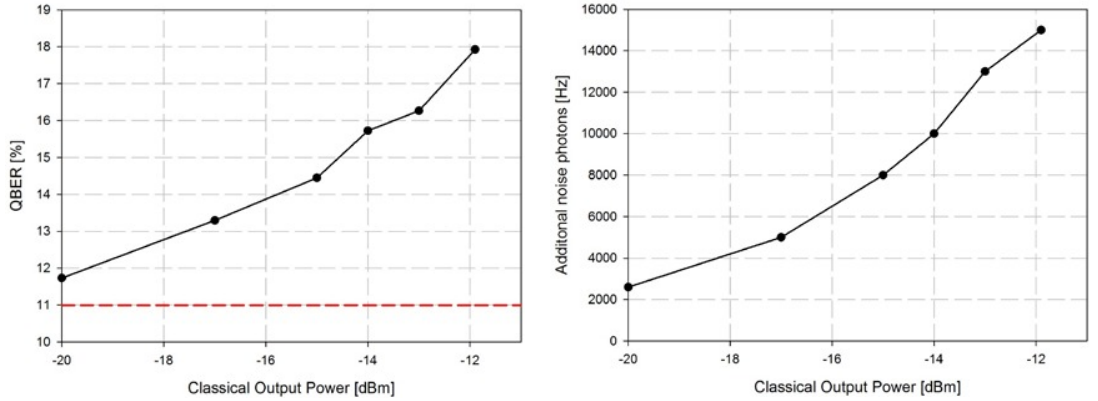

Figure 7. Left: QBER over classical output power of a classical channel for 15.3km. The dashed red line indicates the QBER with no classic signal present. Right: Noise photons over output power for of a classical channel 15.3km.

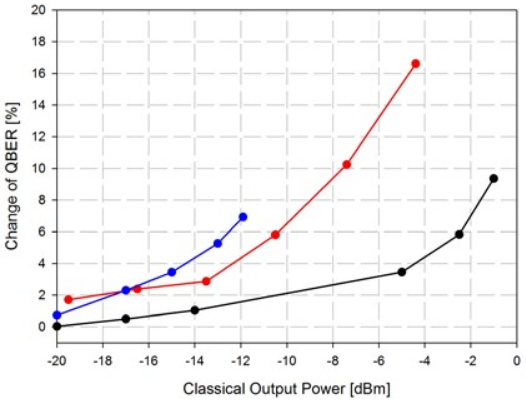

Figure 8. Change of QBER with increasing output power of a single classical channel for 4.3km (black curve) 8.6km (red curve) and 15.3km (blue curve).

3.2 Six Classical Channels

The following measurements show how the quantum channel is affected by standard telecom equipment. We used random data signals from 6 Small Form-factor Pluggable (SFP) modules operating at 1470nm, 1510nm, 1530nm, 1550nm, 1570nm and 1590nm. The six channels are combined and again attenuated before merged with the quantum signal and sent through the fiber. The same effects as for the single channel apply also in this case. Due to the high starting QBER a successful key distribution could only be achieved over 4.3km and 8.6km for attenuated classical signals. The results for 4.3km, 8.6km and 15.3 km fiber lenghts for different output powers are shown in Figures 9 – 11.

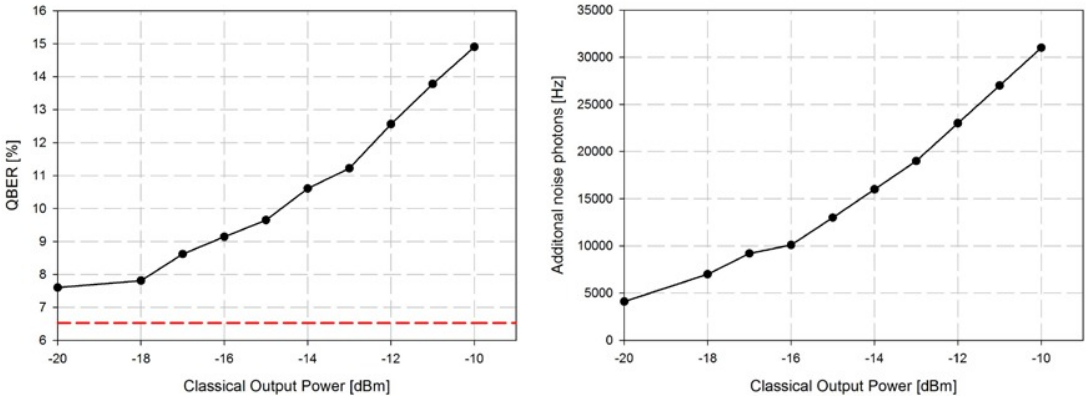

Figure 9. Left: QBER over classical output power from 6 classical channels for 4.3km. The dashed red line indicates the QBER with no classic signal present. Right: Noise photons over output power from 6 channels for 4.3km.

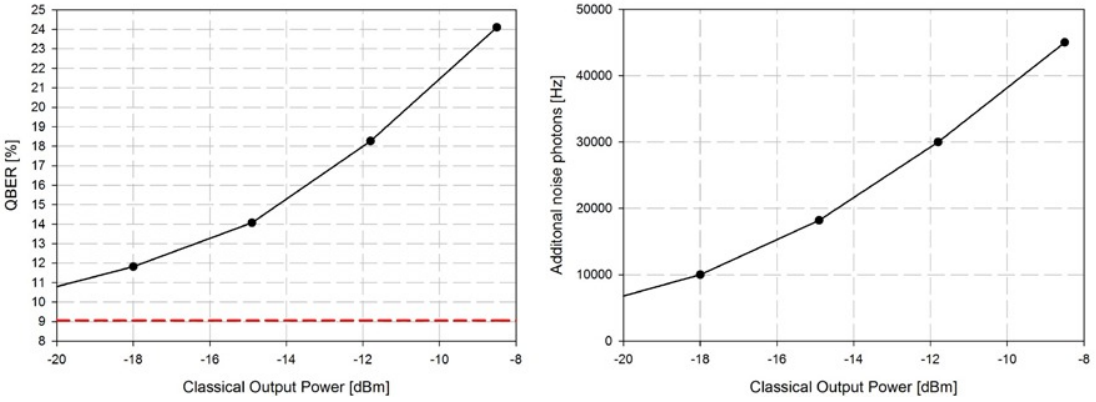

Figure 10. Left: QBER over classical output power from 6 classical channels for 8.6km. The dashed red line indicates the QBER with no classic signal present. Right: Noise photons over output power from 6 channels for 8.6km.

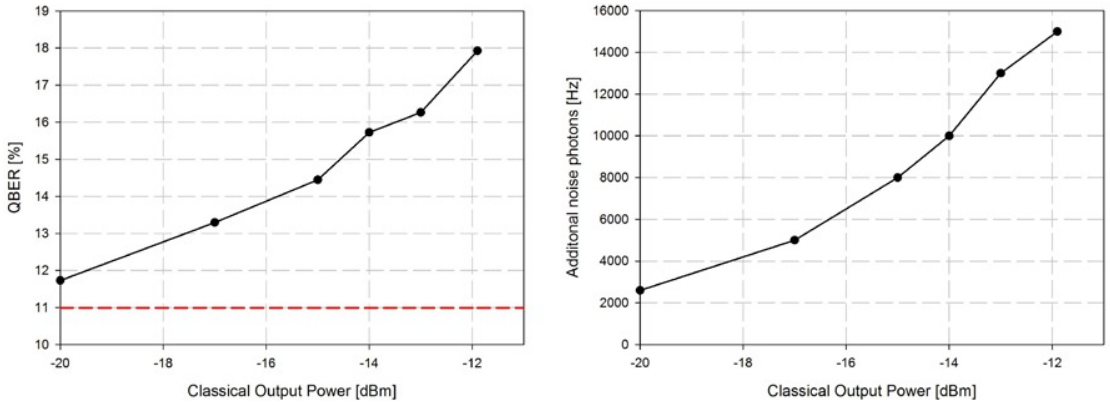

Figure 11. Left: QBER over classical output power from 6 classical channels for 15.3 km. The dashed red line indicates the QBER with no classic signal present. Right: Noise photons over output power from 6 channels for 15.3km.

As before, we normalize the results from the source to make the results applicable for other discrete variable sources with similar detector specification by regarding only the change of QBER. The combined results are shown in Figure 12.

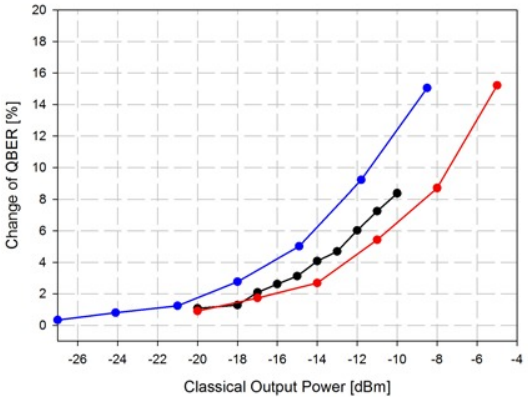

Figure 12. Change of QBER with increasing output power for 4.3km (black curve) 8.6km (red curve) and 15.3km (blue curve).

Since the total output power has to be split between the 6 classical channels, the lowest power setting to guarantee the function of all 6 classical links is around -12.5dBm. Comparing the curves on Figure 12 it is apparent that the QBER at this power setting is still low enough for all investigated fiber lengths to yield a secure key.

3.3 Wavelength dependence of the QBER

The goal of the last measurements is to determine the influence of the spectral proximity of the classical channels to the quantum channel. For this purpose each CWDM signal has been measured individually at constant output power (-19dBm) with the respective change in QBER. All measurements are performed for 8.6km fiber length. The result is shown in Figure 13.

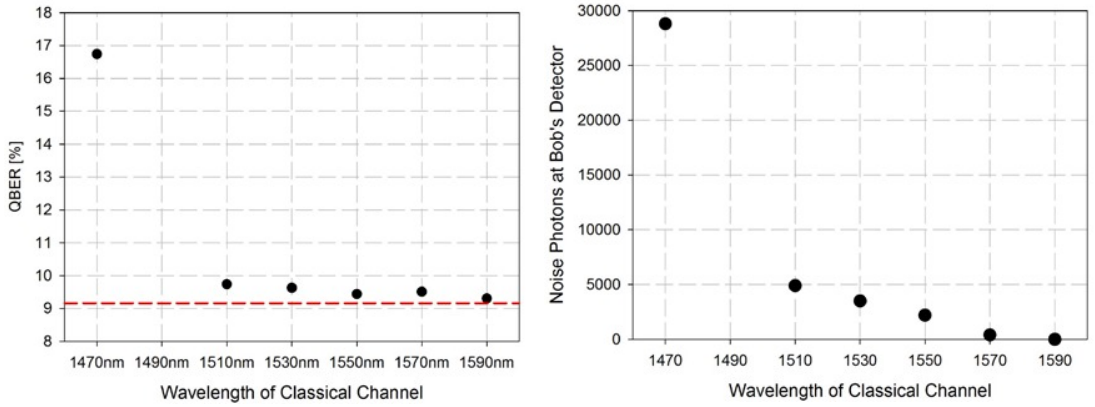

Figure 13. Left: QBER for each individual SFP-Module with respective wavelength over 8.6km. Right: Noise over individual SFP-module for 8.6km.

The results show that the proximity of 1470nm to the quantum channel at 1310nm causes a detrimental increase in QBER as well as in additional noise photons.

The situation becomes more apparent when different channel combinations are investigated. The scenario of a quantum channel multiplexed with 6 classical channels has been introduced above. When we reduce the channels that are spectrally further away from the quantum channel while keeping the total output power constant, the impairments and hence the QBER immediately rise due to a higher proportion of spectrally closer signals (green dots in Figure 14). In contrast, when the reduction of channels starts with the channels lying spectrally closest to the quantum signal, the more intuitive behaviour of a reduction of QBER is observed, see black dots in Figure 14.

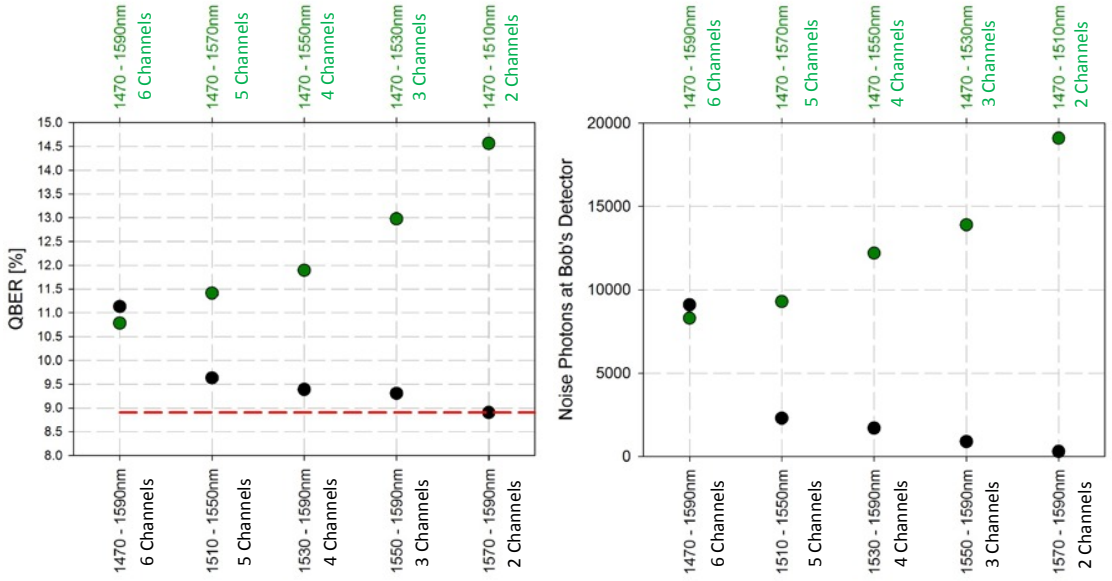

Figure 14. QBER (left) and noise (right) over channel number. The classical channels that are spectrally closer to the quantum channel are removed first (black dots). The channels that are spectrally further away from the quantum channel are removed first (green dots).

4. CONCLUSION

Our results demonstrate that it is indeed possible to multiplex classical data channels in the C-band and a quantum channel in the O-band for entangled photons with little influence on the quantum signal. We showed that a single telecommunication link can easily operate over a 15km long fiber while only adding 2 % to the QBER. In the case of multiple classical channels we could show that up to 6 channels can be transmitted over the full length of 15 km. If more channels are added, tighter spectral filter will become necessary. We could also show that the exact location of the classical channels in the ITU grid is important and spectrally closer channels lead to much higher noise figures. The results here demonstrate the feasibility for future quantum networks imbedded in the existing telecom infrastructure.

ACKNOWLEDGMENTS

This work was supported in part by the project “QKD-Telco: Practical Quantum Key Distribution over Telecom Infrastructures” (contract No. 835926), within the FIT-IT programme funded by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT) in coordination with the Austrian Research Agency (FFG).

REFERENCES

[1] P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," Electronics Letters, 33, 3, 188--190 (1996).
[2] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fiber," New Journal of Physics, 12,6, 063027 (2010).
[3] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A.W. Sharpe, Z. L. Yuan, R.V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Applied Physics Letters, 104 051123 (2014).
[4] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimatal multiplexing of quantum key distribution with classical optical communication," Applied Physics Letters, 106, 081108 (2015).
[5] R. Kumar, H. Qin, R. Alleaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," New J. Phys. 17, 043027 (2015)
[6] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell’s theorem, " Phys. Rev. Lett. 68, 557 (1992).
[7] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks", Optics Express, Vol. 23, Issue 8, pp. 10359-10373 (2015).
[8] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, "Quantum Key Distribution over Optical Access Networks," 18th European Conference on Networks and Optical Communications (NOC 2013), pp. 11--18 (2013).
[9] A. Poppe, B. Schrenk, F. Hipp, M. Peev, S. Aleksic, G. Franzl, A. Ciurana, and V. Martin, "Integration of Quantum Key Distribution in Metropolitan Area Networks," 2014 OSA Optics & Photonics Research in Optical Sciences Congress, Quantum Information and Measurement, Berlin, Germany, 1--3 (2014).
[10] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation, " Nature 390, 575-579 (1997).
[11] F. Xu, B. Qi, Z. Liao, H.-K. Lo, "Long distance measurement-device-independent quantum key distribution with entangled photon sources, " Appl. Phys. Lett. 103, 061101 (2013)
[12] S. Barz, E. Kashefi, A. Broadbent, J.F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of Blind Quantum Computing," Science, 335, 303 (2012).
[13] M. Hentschel, H. Hübel, A. Poppe, and A. Zeilinger, "Three-color Sagnac source of polarization-entangled photon pairs," Opt. Express 17, 23153-23159 (2009).

Appendix D

Curriculum Vitae

PERSONAL INFORMATION

Name: Florian Peter Hipp

Nationality: German

Date of birth: 19.10.1982

Birth place: Kempten (Allgäu, Germany)

Languages: German (mother tongue), English (fluent), French (basics)

PRIMARY AND SECONDARY SCHOOL

1992 - 2002	Carl-von-Linde Gymnasium Kempten (Abitur in spring 2002)
1989 - 1992	Volksschule Sulzberg

UNIVERSITY

2012 - 2016	PhD Student of Technical Physics at the technical university Vienna (TU Wien)
2008 - 2010	Diploma student at the institute of theoretical Physics at the University Vienna (Graduation with honors in February 2011)
2004 - 2009	Studies of Mathematics at the university Vienna
2003 - 2007	Continuation of studies of Physics at the university Vienna
2002 - 2003	Studies of Physics at the university Augsburg

JOBS/WORKINGS (recent)

2011-2016	Researcher at the Austrian Institute of Technology (AIT) (Safety & Security Department, Optical Quantum Technology) with focus on Optics, Photonics, Networktechnology and Quantum Cryptography
2015-2016	Project Assistant for the TU Wien at the Institute of Telecommunications

CONFERENCES/SEMINARS/WORKSHOPS (recent)

2015	SPIE Photonics Europe (Belgium), Talk: *'Demonstration of a coexistence scheme between polarization-entangled QKD and classical data channels'*
2014	AIT PhD Seminar and Workshop (Austria), Talk: *'Quantum Cryptography'*
Since 2013	QCrypt - International Conference on Quantum Cryptography (Canada/France), Posters on *'QKD Integration in Optical Networks'* and *' Integrated entangled photon source'*
Since 2011	CLEO/Europe-EQEC - European Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference (Germany), Talk: *'Quantum Key Distribution in Optical Networks: Does Raman scattering spoil things for Integration?'*
2011	Summerschool at University Waterloo (Canada)
2008-2009	Non-local-Seminar: Vienna (Austria) and Bratislava (Slovakia), Talk: *'A simplex of bound entangled multipartite qubit states'*

PUBLICATIONS

2016	*Demonstration of a coexistence scheme between polarization-entangled QKD and classical data channels*, Proc. SPIE 9900, Quantum Optics, 99000P
2015	*Perspectives and limitations of QKD integration in metropolitan area networks*, Optics express 23.8: 10359-10373
2013	*Quantum interference of photons in simple networks*, Quantum information processing, 12.5: 1915-1945
2012	*Heisenbergs uncertainty relation and Bell inequalities in high energy physics*, Foundations of Physics, 42(6), 778-802.
2010	*Geometry of Qudits*, University Vienna, Diploma Thesis
2008	*Simplex of bound entangled multipartite qubit states*, Physical Review A, 78(4), 042327

Bibliography

[1] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[2] http://www.swissquantum.idquantique.com/IMG/jpg/bb84.jpg.

[3] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[4] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[5] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase-shift quantum key distribution. In *Photonics Asia 2002*, pages 32–39. International Society for Optics and Photonics, 2002.

[6] Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, and Valerio Scarani. Towards practical and fast quantum cryptography. *arXiv preprint quant-ph/0411022*, 2004.

[7] Georg A Reider. *Photonik: eine Einführung in die Grundlagen*. Springer-Verlag, 2012.

[8] Raúl García-Patrón Sánchez and Nicolas Cerf. Quantum information with optical continuous variables: from bell tests to key distribution. 2007.

[9] Abdulsalam Ghalib Alkholidi and Khaleel Saeed Altowij. Free space optical communications—theory and practices. *Contemporary Issues in Wireless Communications*, DOI: 10.5772/58884, 2014. http://www.intechopen.com/books/contemporary-issues-in-wireless-communications/free-space-optical-communications-theory-and-practices.

[10] Florian Hipp, Michael Hentschel, Momchil Peev, Andreas Poppe, Harald Hermann, Wolfgang Sohler, John Rarity, Thomas Scheidl, and Rupert Ursin. Summary report. *ESA Deliverable, unpublished*, 2013.

[11] Harald Herrmann, Abu Thomas, Wolfgang Sohler, Momchil Peev, and Michael Hentschel. Design of the entangled photon pair sources. *ESA Deliverable, unpublished*, 2011.

[12] Florian Hipp, Andreas Poppe, and Michael Hentschel. Developement and testing of the entangled photon breadboard. *ESA Deliverable, unpublished*, 2013.

[13] Michael Hentschel, Momchil Peev, Florian Hipp, and Andreas Poppe. Test results of the entangled photon source. *ESA Deliverable, unpublished*, 2013.

[14] Xu Yang. Implementation of a waveguide based source of polarization entanglement. *Master Thesis, Universtität Paderborn, Applied Physics/Integrated Quantum Optics Group*, 2012, unpublished.

[15] http://www.ieee802.org/3/efm/public/jul01/tutorial/pesavento_1_0701.pdf, .

[16] S Aleksic, D Winkler, A Poppe, G Franzl, B Schrenk, and F Hipp. Distribution of quantum keys in optical transparent networks: issues and challenges,". In *15th International Conference on Transparent Optical Networks (ICTON 2013), Cartagena, Spain, We. B*, volume 1, page 3, 2013.

[17] Slavisa Aleksic, Dominic Winkler, Gerald Franzl, Andreas Poppe, Bernhard Schrenk, and Florian Hipp. Quantum key distribution over optical access networks. In *Network and Optical Communications (NOC), 2013 18th European Conference on and Optical Cabling and Infrastructure (OC&i), 2013 8th Conference on*, pages 11–18. IEEE, 2013.

[18] Slavisa Aleksic, Florian Hipp, Dominic Winkler, Andreas Poppe, Bernhard Schrenk, and Gerald Franzl. Perspectives and limitations of qkd integration in metropolitan area networks. *Optics express*, 23(8):10359–10373, 2015.

[19] Christian Kollmitzer and Mario Pivk (Editors). *Applied quantum cryptography*, volume 797. Springer, 2010.

[20] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[21] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[22] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony. Cryptology ePrint Archive, Report 2010/013, 2010. http://eprint.iacr.org/.

[23] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of rc4. In *Selected areas in cryptography*, pages 1–24. Springer, 2001.

[24] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full aes-192 and aes-256. Cryptology ePrint Archive, Report 2009/317, 2009. http://eprint.iacr.org/.

[25] Daniel J Bernstein. Cache-timing attacks on aes, 2005.

[26] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

[27] Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120–126, 1978.

[28] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, 2011.

[29] Charles H Bennett, Gilles Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175(0), 1984.

[30] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[31] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):168–177, 2015.

[32] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Source attack of decoy-state quantum key distribution using phase information. *Physical Review A*, 88(2):022308, 2013.

[33] Robert GW Brown, Kevin D Ridley, and John G Rarity. Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching. *Applied Optics*, 25(22):4122–4126, 1986.

[34] Robert GW Brown, Robin Jones, John G Rarity, and Kevin D Ridley. Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching. *Applied Optics*, 26(12):2383–2389, 1987.

[35] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[36] Alex D Semenov, Gregory N Gol'tsman, and Alexander A Korneev. Quantum detection by current carrying superconducting film. *Physica C: Superconductivity*, 351(4):349–356, 2001.

[37] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor science and technology*, 25(6):063001, 2012.

[38] IDQuantique. http://www.idquantique.com/.

[39] Magiqtech. http://www.magiqtech.com/.

[40] Simon Gröblacher, Thomas Jennewein, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8(5):75, 2006.

[41] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[42] H Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6): 4238, 1999.

[43] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.

[44] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.

[45] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[46] Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3):032301, 2005.

[47] Xiongfeng Ma. Security of quantum key distribution with realistic devices. *arXiv preprint quant-ph/0503057*, 2005.

[48] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[49] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[50] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[51] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15): 880, 1969.

[52] Frits Zernike and John E Midwinter. *Applied nonlinear optics*. Courier Corporation, 2006.

[53] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[54] Hoi-Kwong Lo and Yi Zhao. Quantum cryptography. In *Computational Complexity*, pages 2453–2477. Springer, 2012.

[55] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[56] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, 2005.

[57] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer, 2005.

[58] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical review letters*, 94(16):160502, 2005.

[59] Masato Koashi. Complementarity, distillable secret key, and distillable entanglement. *arXiv preprint arXiv:0704.3661*, 2007.

[60] Llus Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett. Unconditional security of key distribution from causality constraints. *arXiv preprint quant-ph/0606049*, 108, 2006.

[61] Nicolas J Cerf, Marc Levy, and Gilles Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63(5):052311, 2001.

[62] Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable qkd with intense dwdm classical channels. *arXiv preprint arXiv:1412.1403*, 2014.

[63] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5):057902, 2002.

[64] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[65] Gerardo Adesso, Sammy Ragy, and Antony R Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Systems & Information Dynamics*, 21(01n02), 2014.

[66] Wolfgang P Schleich. *Quantum optics in phase space*. John Wiley & Sons, 2011.

[67] Christian Weedbrook, Andrew M Lance, Warwick P Bowen, Thomas Symul, Timothy C Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical review letters*, 93(17):170504, 2004.

[68] Ch Silberhorn, Timothy C Ralph, Norbert Lütkenhaus, and Gerd Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Physical review letters*, 89(16):167901, 2002.

[69] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical review letters*, 102(18):180504, 2009.

[70] Renato Renner and J Ignacio Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical review letters*, 102(11):110504, 2009.

[71] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J Cerf. Security of continuous-variable quantum key distribution against general attacks. *Physical review letters*, 110(3):030502, 2013.

[72] Fabian Furrer, Torsten Franz, Mario Berta, Anthony Leverrier, Volkher B Scholz, Marco Tomamichel, and Reinhard F Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical review letters*, 109(10):100502, 2012.

[73] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, 2014.

[74] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6): 062343, 2010.

[75] Thomas Symul, Daniel J Alton, Syed M Assad, Andrew M Lance, Christian Weedbrook, Timothy C Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. *Physical Review A*, 76(3):030303, 2007.

[76] Jérôme Lodewyck, Thierry Debuisschert, Raul Garcia-Patron, Rosa Tualle-Brouri, Nicolas J Cerf, and Philippe Grangier. Experimental implementation of non-gaussian attacks on a continuous-variable quantum-key-distribution system. *Physical review letters*, 98(3):030503, 2007.

[77] Yong Shen, Hongxin Zou, Liang Tian, Pingxing Chen, and Jianmin Yuan. Experimental study on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 82(2):022317, 2010.

[78] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

[79] Anthony Martin, Valentina Cristofori, Pierre Aboussouan, Harrald Herrmann, Wolfgang Sohler, Daniel Barry Ostrowsky, Olivier Alibart, and Sébastien Tanzilli. Integrated optical source of polarization entangled photons at 1310 nm. *Optics express*, 17(2):1033–1041, 2009.

[80] S Tanzilli, W Tittel, H De Riedmatten, H Zbinden, P Baldi, M DeMicheli, Da B Ostrowsky, and N Gisin. Ppln waveguide for quantum communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2): 155–160, 2002.

[81] Anthony Martin, Amandine Issautier, Harald Herrmann, Wolfgang Sohler, Daniel Barry Ostrowsky, Olivier Alibart, and Sébastien Tanzilli. A polarization entangled photon-pair source based on a type-ii ppln waveguide emitting at a telecom wavelength. *New Journal of Physics*, 12(10):103005, 2010.

[82] Harald Herrmann, Xu Yang, Abu Thomas, Andreas Poppe, Wolfgang Sohler, and Christine Silberhorn. Post-selection free, integrated optical source of non-degenerate, polarization entangled photon pairs. *Optics express*, 21(23):27981–27991, 2013.

[83] L Bersiner, U Hempelmann, and E Strake. Numerical analysis of passive integrated-optical polarization splitters: comparison of finite-element method and beam-propagation method results. *JOSA B*, 8(2):422–433, 1991.

[84] Natalia Bruno, E Zambrini Cruzeiro, Anthony Martin, and RT Thew. Simple, pulsed, polarization entangled photon pair source. *Optics Communications*, 327: 3–6, 2014.

[85] Ahmed Nabih Zaki Rashed. Harmful effects of gamma irradiation on optical fiber communication system links under thermal environment effects. *International Journal of Computer, Electronics & Electrical Engineering (IJCEEE)*, 2(1):4–13, 2012.

[86] Cheng-Chih Lai, Chin-Yu Chang, Yuan-Yaw Wei, and Way-Seen Wang. Study of gamma-irradiation damage in linbo 3 waveguides. *IEEE Photonics Technology Letters*, 19(13):1002–1004, 2007.

[87] Richard J Padden, Edward W Taylor, Anthony D Sanchez, JN Berry, SP Chapman, Steve A DeWalt, and Ka K Wong. Litao3 and linbo3: Ti responses to ionizing radiation. In *Orlando'91, Orlando, FL*, pages 148–159. International Society for Optics and Photonics, 1991.

[88] http://www.ieee802.org/3/av/public/2007_11/3av_0711_effenberger_1.pdf, .

[89] G ITU. 984.1: Gigabit-capable passive optical networks (gpon): General characteristics. *ITU-T, March*, 2008.

[90] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[91] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2 ghz clock quantum key distribution over 260 km of standard telecom fiber. *Optics letters*, 37(6):1008–1010, 2012.

[92] Patrick Eraerds, Nino Walenta, Matthieu Legre, Nicolas Gisin, and Hugo Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, 2010.

[93] Sunil Pratap Singh, Ramgopal Gangwar, and Nar Singh. Nonlinear scattering effects in optical fibers. *Progress In Electromagnetics Research*, 74:379–405, 2007.

[94] Peter E Powers. *Fundamentals of nonlinear optics*. CRC Press, 2011.

[95] Eric Olaf Potma and Shaul Mukamel. 1. theory of coherent raman scattering. *Coherent Raman Scattering Microscopy*, page 1, 2012.

[96] Florian Hipp, Michael Hentschel, Slavisa Aleksic, Andreas Poppe, and Hannes Huebel. Demonstration of a coexistence scheme between polarization-entangled qkd and classical data channels. In *SPIE Photonics Europe*, pages 99000P–99000P. International Society for Optics and Photonics, 2016.

[97] http://www.vpiphotonics.com.

[98] Dawn Hollenbeck and Cyrus D Cantrell. Multiple-vibrational-mode model for fiber-optic raman gain spectrum and response function. *JOSA B*, 19(12):2886–2892, 2002.

[99] RH Stolen. Issues in raman gain measurements. In *Tech. Dig. Symp. Optical Fiber Measurements, NIST Special Publication*, volume 953, pages 139–142, 2000.

[100] KA Patel, JF Dynes, M Lucamarini, I Choi, AW Sharpe, ZL Yuan, RV Penty, and AJ Shields. Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks. *Applied Physics Letters*, 104(5):051123, 2014.

[101] Michael Hentschel, Hannes Hübel, Andreas Poppe, and Anton Zeilinger. Three-color sagnac source of polarization-entangled photon pairs. *Optics express*, 17(25): 23153–23159, 2009.

[102] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, 1993.

[103] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3): 265–279, 1981.

[104] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6): 1915–1923, 1995.