DIPLOMA THESIS

Practical Integration of a Quantum Channel for QKD in commercial WDM systems

Simulation and Setup of a Quantum Channel

Submitted at the Faculty of Electrical Engineering and Information Technology,
Vienna University of Technology
in partial fulfillment of the requirements for the degree of
Diplom-Ingenieur (equals Master of Sciences)

under supervision of

Em.O.Univ.Prof. Dipl.-Ing. Dr.techn. Harmen R. Van As
Dipl.-Ing. Dr.techn. Slavisa Aleksic

by

Dominic Winkler, BSc.
Matr.Nr. 0426151
Gerasdorfer Strasse 61/30/5, 1210 Wien

Date ______________________________

Kurzfassung

Das große Problem des initialen Schlüsseltausches bei symmetrischen Verschlüsselungsverfahren kann mit Hilfe der quantenmechanischen Theorie gelöst werden. Quantum Key Distribution (QKD) ist die praktische Anwendung von Quantenmechanik, um den Schlüsseltausch über einen unsicheren Kanal zu ermöglichen. Wenn man die zu übertragenden Schlüsseldaten quantenmechanisch kodiert, ist es physikalisch (nicht nur ressourcen-bedingt) unmöglich, den Kanal unerkannt abzuhören.

In transparenten optischen Glasfasernetzen wird das optische Signal am gesamten Übertragungsweg nie zu einem elektrischen Signal konvertiert, wodurch eine hohe Flexibilität hinsichtlich Datenformaten und Übertragungsraten erreicht wird. Im Prinzip werden transparente Glasfasernetze für rein optische Ende-zu-Ende Verbindungen verwendet, sie sind aber auch für die Übertragung von Quantensignalen verwendbar. Quantensignale sind sehr anfällig für Dämpfung und Rauschen, was besonders bei den kaskadierten passiven und aktiven Komponenten von typischen Netztopologien zum Tragen kommt.

Diese Arbeit analysiert verschiedene Möglichkeiten um Quantum Key Distribution (QKD) in transparente optische Netze, die auf dem Wellenlängenmultiplex-Verfahren basieren, zu integrieren. Es wird untersucht wie sich klassische Signale auf das Rauschverhalten des Kanals auswirken, um potentielle Frequenzbereiche für den Quantenkanal bestimmen zu können. Dazu wurden Simulationen von realistischen optischen Netzwerken in *VPItransmissionMaker* aufgebaut. Verbindungsstrecken in städtischen Netzen wurden für Längen zwischen 20 und 60 km untersucht wobei 40 WDM Kanäle aktiviert waren und zwischengeschaltete optische Verstärker (EDFA) und Schaltknoten (OXC) vom Quantenkanal überbrückt wurden. Des weiteren wurden die optischen Zugangsnetztechnologien EPON, GPON, 10GPON, XGPON, PtP-GbE, PtP-10GbE, WDM-PON und WDM/TDM-PON auf Kompatibilität mit QKD-Systemen untersucht.

Das Ergebnis der Simulationen war das komplette Rauschspektrum an potentiellen QKD Endpunkten im Netzwerk. Um genauere Aussagen für ein kommerziell erhältliches QKD System zu erhalten, waren einige Nachbearbeitungsschritte der Rauschdaten notwendig. Quantitative Schätzungen der Quanten Bitfehlerwahrscheinlichkeit (QBER) und der endgültigen Schlüsselrate wurden anhand von analytischen Modellen für das BB84 und das SARG Protokoll errechnet. Der Betrieb eines QKD Systems für Glasfaserlängen über Strecken mit 40 konventionellen Kommunikationskanälen und bis 30 km Glasfaserlängen ist möglich unter der Bedingung, dass der Quantenkanal im O-Band liegt, aktive Komponenten wie z.B. EDFA und OXC überbrückt werden und die konventionellen Kanäle im C-band liegen.

Abstract

The problem of distributing keys for encryption and decryption of sensitive data can be solved on the physical layer by means of quantum physics. Quantum key distribution (QKD) is the application of quantum theory to facilitate secure key transmission over an insecure channel. By performing key data transmission in the quantum regime, the possibility of eavesdropping information or man-in-the-middle attacks are made impossible based on physical properties rather than mathematical or computational complexity.

Transparent optical networks are capable of providing a flexible and dynamic data transport via transparency regarding both data rate and format of transmitted signals, which is achieved by implementing data transmission and forwarding in the optical domain. While supporting all-optical end-to-end paths, transparent optical networks are in principle suitable to integrate end-to-end quantum cryptography. However, quantum signals are extremely sensitive to loss and noise, which is a particular issue because of the cascaded passive and active components along signal paths, common with transparent optical networks.

This thesis analyzes different options for integrating quantum key distribution (QKD) in wavelength-division multiplexed (WDM) transparent optical networks where QKD signals are transmitted along with conventional WDM signals. Realistic simulations were implemented in *VPItransmissionMaker* with the goal to find applicable wavelength bands for the uninterrupted operation of a quantum channel. Metropolitan area network links with typical lengths of 20 km to 60 km and 40 WDM channels were simulated in scenarios with a direct point-to-point connection, using an intermediate amplifier (EDFA) and an intermediate optical switch node (OXC). Additionally, passive optical access networks (PONs) were examined considering standard options such as EPON, GPON, 10GPON, XGPON, PtP-GbE, PtP-10GbE, WDM-PON and WDM/TDM-PON.

Finally, the background noise spectra at QKD receiver sites are presented. This data was further post-processed using analytical models of a well-known commercially available QKD system to estimate the quantum bit error rate (QBER) and final secure key rate (Rsec) for BB84 and SARG protocols across all wavelengths. The main conclusion is that QKD operation may be possible for fiber lengths up to 30 km, if the quantum channel is allocated in the O-Band, active nodes such as EDFA and OXC are bypassed and conventional data channels are restricted to the C-band.

Acknowledgements

I consider myself very lucky that I got the chance to be part of a joint project of Vienna University of Technology (TU Wien) and Austria Research Institue (AIT) to examine the feasibility of integrating quantum key distribution in commercially available optical network.

First, I want to thank Slavisa Aleksic for his support and teamwork over the last year, which resulted in the publication of two scientific papers [AWP+13b, AWP+13a] and the thesis in hand. I enjoyed the friendly work climate and the freedom he has given me time-wise to finish all required tasks. Also I want to thank the researchers from AIT, especially Andreas Poppe, for interesting talks and skilled feedback.

Further, I want to thank Harmen R. Van As for allowing me to be one of his last few graduation students. His lectures were filled with insights into latest technologies but still grounding on the fundamental basics.

Finally, I want to thank my family for their patience and understanding while I was busy working for the project, writing the thesis and being a part-time employee. Especially the support of my wife and the amazing hours with my son helped me to bring everything to an end.

Table of Contents

Abbreviations

AMZI	Asymmetric Mach-Zehnder Interferometers
APD	Avalanche Photo Diodes
ASE	Amplified spontaneous emission
AWG	arrayed waveguide grating
BB84	Bennet/Bassard 1984
BDF	Boolean dataflow domain
BER	Bit error rate
CO	central office
COW	Coherence One-Way
CV	Continuous-Variables
DDF	Dynamic dataflow domain
DPS	Differential phase-shift
DPSK	Differential phase-shift keying
DSF	Dispersion shifted Fibers
DWDM	Dense Wavelength Devision Multiplexing
E91	Ekert 1991
EDFA	Erbium doped fiber amplifier
EPR	Einstein, Podolsky and Rosen
FTTH	Fiber-to-the-home
FWM	Four-wave mixing
GMCS	Gaussian modulated coherent state
HOF	Higher-order functions
ITS	information theoretically secure
LDPC	Low Density Parity Check
LO	Local oscillator
OLT	Optical line terminal
ONU	Optical network unit
OSA	optical spectrum analyzer
OTP	One-time pad
OXC	Optical Cross Connect
PDA	Photonic Design Automation
PDL	Polarization Dependent Loss
PMD	Polarization mode dispersion
PNS	Photon-number splitting attack
PON	Passive Optical Network
PPLN	Periodically poled Lithium Niobate
QBER	Quantum bit error rate
QE	Quantum efficiency
QKD	Quantum key distribution
SARG	Scarani/Acin/Ribordy/Gisin

SDF	Synchronous dataflow domain
SMF	Single-Mode Fibers
SPDC	Spontaneous parametric down-conversion
SPD	Single photon detector
SPM	Self Phase modulation
SSMF	Standard Single-Mode Fibers
SSPD	Superconducting single photon detectors
Rsec	Secure key rate
Rx	Receiver
Tx	Transmitter
TDM	Time devision multiplexing
WDM	Wavelength Devision Multiplexing
XOR	Exclusive OR
XPM	Cross Phase modulation

1 Introduction

A secure and reliable data transmission is of major importance in todays communication networks. Cryptography has been developed to meet these requirements and keep confidential information secure. Nowadays most sensitive information like financial transactions, medical records, credit card data or some ones social life events is exchanged over public insecure channels. In order to secure such data from being eavesdropped, mathematically engineered encryption schemes – such as Public-Key Cryptography – are applied. The privacy of the data is based on the computational complexity of deciphering the message without having the decryption key.

The problem is that this computational complexity can be circumvented if the encryption method contains a backdoor or implementation flaws. Recent media reports state implications of United States National Security Agency (NSA) in eavesdropping enormous amount of personal data by breaking the transport layer security (TLS) encryption of internet traffic. This was made possible by exploiting an intentionally implemented backdoor of TLS encryption which was part of secret agreements between security companies and the NSA.

Information theoretically secure encryption requires the distribution of symmetric keys over the same insecure channel. This problem can be solved on the physical layer by means of quantum physics. Quantum key distribution (QKD) is the application of quantum theory to facilitate secure key transmission over an insecure channel. By performing the key exchange in the quantum regime, the possibility of eavesdropping information or man-in-the-middle attacks are made impossible based on physical properties rather than mathematical or computational complexity.

1.1 Cryptography

The digital age in cryptography was introduced in the course of World War II as computers were initially deployed for cryptanalysis. Modern cryptography uses digital signal processing and mathematical theory to facilitate the exchange of secret messages over an insecure communication channel. Basically a message is encrypted at the transmitter (usually called *Alice*), transmitted over an insecure channel and decrypted at the receiver (usually called *Bob*). The encryption/decryption mechanism varies between modern cryptosystems and can be divided in *symmetric-key algorithms* and *public-key algorithms*.

1.1.1 Symmetric-Key Cryptography

For a long time symmetric-key cryptography was the only known encryption scheme. At Alice, the message to be sent is encrypted by a transformation with a shared secret key. The same key is used by Bob to decrypt the received message. Typically message digits are represented as bit values which are combined with key bits via a reversible binary operation (for example XOR).

In the case of *stream ciphers* this transformation is done bit-wise and requires a key length which is equal to the message length. Stream ciphers using such a key can be regarded an implementation of the one-time pad (OTP) algorithm also called *Vernam cipher*. The OTP encryption was proved to be information theoretically secure (ITS) by Claude E. Shannon. Assuming a perfectly random key bit stream (i.e. with no repetitions) the ciphertext does not contain any references to the plain message. In practical realisations the keystream is generated by digital shift registers which are initialized with a short secret key acting as random seed. The consequence of using a shorter key is an only pseudo-random keystream which renders the ITS property ineffective and opens the possibility for cryptanalysis.

Block ciphers operate on equally sized blocks of message digits. The message is padded to multiples of the block size before each block is encrypted using a symmetric key. As with stream ciphers, the decryption algorithm at Bob is the inverse operation of the encryption at Alice using the same key. The encryption algorithm has to be designed such that identical plaintext blocks do not generate the same ciphertext. Well known examples are DES, AES (Rijndael), Blowfish, 3DES and RC4. Block ciphers requires less implementation effort than stream ciphers but are vulnerable to cryptanalysis if secret keys are repeatedly used.

1.1.2 Public-Key Cryptography

Apparently, the biggest problem with symmetric keys is that both communication nodes need to exchange the key in advance (*Key distribution problem*). In 1976, Whitfield Diffie and Martin Hellman introduced the revolutionary idea of *public-key algorithms*. Here two different keys are asymmetrically used for encryption and decryption. Alice encrypts the message with Bobs publicly announced public-key but only Bobs private-key is able to decrypt the ciphertext generated by Alice. Public-key and private-key share a mathematical relation but it is *infeasible* to calculate the private-key given the public-key. In the case of RSA algorithm this infeasibility is created by exploiting the computational difficulty of factoring large integers. Here, the product of two large prime numbers and an additional value constitute Bobs public key. Only Bob knows the prime numbers and uses them to calculates a corresponding private-key. Public-key encryption relies on the hardness of the factoring problem to which no known algorithm can provide a solution in polynomial time on conventional computers. Thus, the information will no longer be relevant by the time an eavesdropper could complete decryption of the ciphertext.

However, it is important to bear in mind that the security of public-key encryption has not been proven (see Fig. 1.1) to be an information theoretically secure encryption scheme such as OTP and could be broken [1]. Considering unconventional computers - like a quantum computer - Shors algorithm [2] proves that the problem could be solved in polynomial time. Recent scientific advances in quantum computing enabled an experimental demonstration of Shors algorithm. Even though quantum computers seem futuristic, one should never underestimate the technological capabilities of a potential eavesdropper (usually referred to as *Eve*).

	Security based on
Encryption	
Symmetrical block or stream cipher (key shorter than message)	Assumption
Public key cryptography	Assumption
One time pad	Information theory
Key distribution	
Secure channel	Assumption
Public key cryptography	Assumption
QKD	(Quantum) information theory
Message authentication	
Public key cryptography	Assumption
MAC	Assumption
Universal-2 hash functions	Information theory

Figure 1.1: Security foundation of cryptographic primitives from [3]

1.2 Quantum Cryptography

The key distribution problem of the one-time pad (OTP) encryption scheme - or any other key distribution - can be resolved by means of quantum mechanics [1, 4]. Among all the research fields of quantum information science *Quantum cryptography* has probably made the most progress both from the theoretical and experimental perspective and matured to an applied science. Quantum key distribution (QKD) makes use of the quantum mechanics theory to facilitate secure transmission of keys over an insecure channel that may be accessible to an eavesdropper, Eve. The secrecy of encryption keys is the foundation of all cryptosystems security using symmetric keys. By performing key data transmission in the quantum regime, the possibility of eavesdropping information or man-in-the-middle attacks are made impossible based on physical properties rather than mathematical or computational complexity.

1.2.1 Qubits and Quantum States

In classical systems the keys are encoded as bits with the value 0 or 1. In the quantum regime information is encoded in a two-state quantum system called *qubits*. The state of a qubit may also be exactly 0 or 1 but also - in contrast to the classical bit - the superposition of both states is possible. In general all two-state quantum systems can represent a qubit but the most common applications use the polarisation or phase of photons. Other representations are for example the electronic spin of electrons or the nuclear spin of nucleus [5]. In this work a quantum state is mathematically described using the *bra-ket notation* introduced by Paul Dirac but there also exist other notations.

In bra-ket notation a vector $\mathbf{A}$ is written as $|A\rangle$ (*ket-A*) and the inner product (dot product) of two vectors $\mathbf{A}$ and $\mathbf{B}$ is written as $\langle A|B\rangle$. A qubit can be represented as the linear combination of eigenbases (i.e. polarisations, phase, spin directions, . . .),

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \Bigg| \quad |\alpha|^2 + |\beta|^2 = 1.$$

, where α and β are complex possibility amplitudes. In case of photon polarisation the eigenbases $|0\rangle$ and $|1\rangle$ can be mapped to the orthogonal polarisation states 0° and 90°. If a qubit is evaluated by a measurement the possibility of outcome $|0\rangle$ is $|\alpha|^2$ and the possibility of $|1\rangle$ is $|\beta|^2$. α and β are constrained by $|\alpha|^2 + |\beta|^2 = 1$ because the total probability of any outcome has to be 1. The two-dimensional state space of a pure qubit can be regarded as the surface of a sphere (Bloch sphere).

Some physical operations can be performed on qubits. On the one hand a quantum logic gate operating on one or more qubits can be regarded a unitary transformation preserving the inner product (i.e. a rotation in the bloch sphere). On the other hand the act of measurement collapses the qubit (i.e. the wave function) to one of the eigenvectors of the eigenbasis (eg. $|0\rangle$ or $|1\rangle$). This is called the *wave function collapse* and causes all subsequent measurements to yield the same result. This phenomenon of quantum mechanics is exploited by the category of "Prepare and Measure" Quantum Key Distribution protocols to detect eavesdropping.

1.2.2 Quantum Entanglement

Another important difference to a classical bit is that qubits can exhibit *quantum entanglement*. A qubit is in the state of quantum entanglement if it cannot be fully described without considering the another qubit [6, 7]. That is, it cannot be described in the form $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. In order to get entangled, two particles representing qubits have to interact physically and then become separated by an arbitrary distance. Spontaneous parametric down-conversion (SPDC) in nonlinear crystals [8] can be utilized to generate a pair of photons entangled in polarisation (Fig. 1.2). Alternatively a fibre coupler can be used to mix and confine photons or quantum dots are trapping electrons until decay occurs. After this process a measurement taken on one photon of the pair entails the exactly correlated result on the other photon. The wave function collapse for the second photon happens instantaneously and is independent of the distance between the photons (hence also referred to as "Spooky action at a distance" by Einstein).

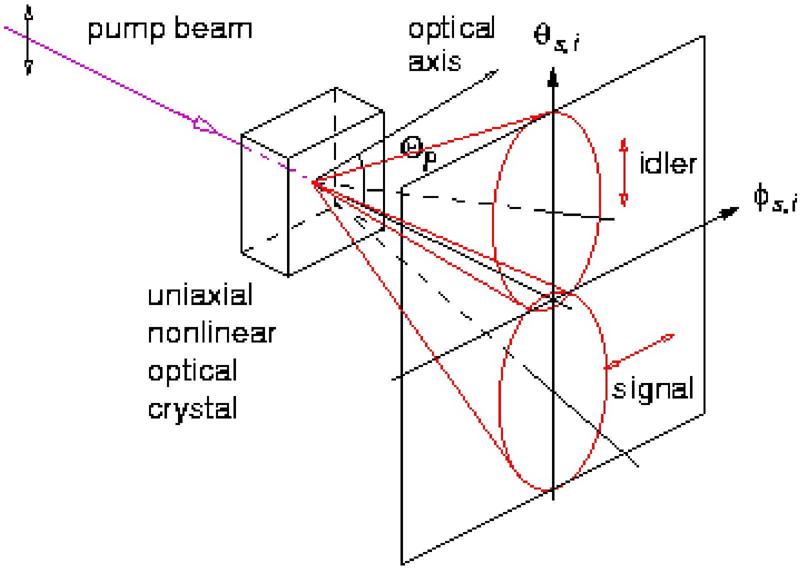


Figure 1.2: Generation of entangled photons in a non-linear crystal

Mathematically an entangled state can be described as inseparable tensor product of two hilbert spaces. An example for an entangled quantum state is

$$\frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\Big)\text{(Bell state)}.$$

Entanglement is a non-local property which is fully in accordance with the Heisenberg uncertainty principle but does not adhere to the principle of locality (i.e. information cannot travel faster than the speed of light). The phenomenon was initially discussed 1935 in a well-known paper by Einstein, Podolsky and Rosen (EPR). They presented a thought experiment (the EPR paradox) in which one of two spin-entangled electrons is measured and fixes the measurement of the other. Considering the concept of *local realism* their conclusion was that the quantum mechanics theory is incomplete because of the instantaneous wave-function collapse of both electrons. To resolve this paradox, EPR proposed the theory of *local hidden variables* which explains the non-deterministic behaviour of quantum mechanics to hidden but well-defined properties of particles.

In 1964, John Bell calculated the upper bound for correlation measurements of entangled particle pairs (ERP-pairs) if local realism is presumed – that is physical effects have a finite propagation speed and particles have deterministic properties. He summarized his results in the so-called Bell inequalities which are experimentally detectable. Bells theorem shows that quantum mechanical predictions violate these inequalities and contradict with theories based on the local realism assumptions (e.g. hidden variable theory). The Bell inequalities can be experimentally evaluated and thus be used to test for the strong quantum mechanical correlations caused by quantum entanglement. This effect is exploited by the category of "Entanglement based" QKD protocols.

1.2.3 "No-go" theorems

In quantum mechanics there are several "no-go" theorems which describe situations that are physically impossible. The *no-teleportation* theorem states that a quantum state (a qubit) cannot be fully determined via a single measurement. Due to the probabilistic nature of quantum mechanics a qubit cannot be prepared to yield the exact same measurement result as the qubit before. This is only possible if the respective qubits exhibit quantum entanglement (see 1.2.2). The *no-communication* theorem proves that even if quantum entanglement is considered, superluminar information exchange (faster than the speed of light) is impossible and thus the principle of special relativity is preserved. The *no-cloning* theorem and as a consequence the *no-broadcast* theorem shows that a quantum state cannot be copied [9]. An important implication of the no-cloning theorem is that classical error-correction cannot be used. More importantly it prevents a potential attacker to eavesdrop information without being detected by Alice or Bob.

2 Quantum key distribution systems

Quantum key distribution (QKD) systems use single photons as physical representation of qubits (two-level quantum systems). In the 1970s the initial idea of using the uncertainty printicple of quantum mechanical for cryptography was expressed in a manuscript by Stephan Wiesner and later published in [10]. First practical protocols and experimental setups were completed in the 1990s [4, 11, 12, 13, 14, 15]. The transmission media can be either free-space or optical fiber. In this work fiber based QKD-systems are primary considered. The high availability of optical fiber communication networks implies an economic opportunity for adopting QKD on a widespread scale.

2.1 Generic QKD System

Any quantum-encrypted communication systems comprise a sending unit (Alice) and a receiving unit (Bob) (see Fig. 2.1). The public classical channel is necessary for communication between different layers of the QKD protocol stack (see Fig. 2.2) and need to be authenticated. Thus an eavesdropper can monitor but not alter or suppress the classical signals. Furthermore, depending on the QKD system a co-existing time-stable classical channel for synchronization may be needed. QKD systems can be distinguished by various details of their implementation (see 2.2).

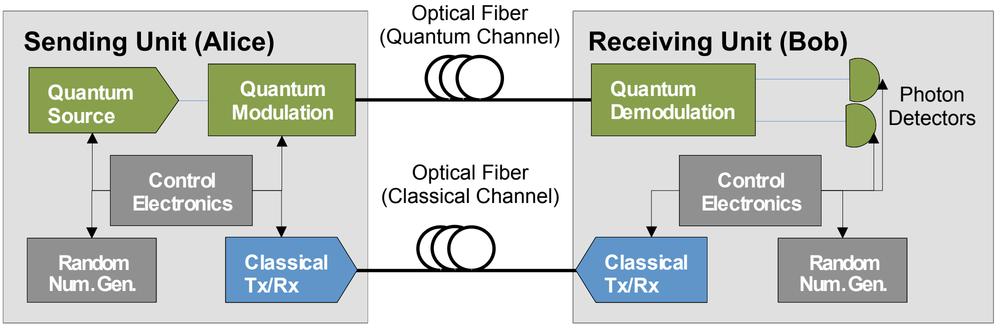


Figure 2.1: Generic QKD system

The main difference to classical communication systems resides in the properties of the exchanged optical signals, particularly the extremely low signal power of single photons and the methods used to establish a reliable exchange of secret keys. There exists an extreme mismatch in signal intensities between classical and quantum channels, as a quantum signal typically contains approximately 0.5 photons per pulse (i.e. per qubit) when implementing decoy protocols with weak laser pulses (see 2.2.1), while a data-laser pulse may contain 10^6 photons or more for a Gigabit/sec transmission. One can imagine that problems arise if a single optical fiber is used for both quantum and classical communication (see 2.3).

The foundation of any QKD system is the quantum channel. It carries photons that are encoded with quantum information (e.g. qubits) and eventually measured in one of at least two unbiased, non-orthogonal bases. As mentioned before, quantum mechanics and mathematical statistics dictate that an eavesdropper cannot gain full information without prior knowledge about the encoding bases (see. 1.2.3). Any attempt to eavesdrop, i.e. to measure the transmitted photon collapses the quantum state to a certain result. The attacker will be noticed either by the absence or the incorrect state (only guessing is possible) of the transmitted photon. The eavesdropper thus leaves its mark in the form of an increased quantum bit error rate (QBER) among Alice and Bob, if the best possible attack is assumed and all photons are successfully attacked. A low QBER indicates that the quantum information sufficiently protected by physical laws against eavesdropping. In that case, a secret key can be extracted with confidence by executing a QKD protocol stack. Fig. 2.2 shows the different layers which any QKD protocol consists of. The layers are briefly described in the next paragraphs together with specific protocol implementations.

2.1.1 QKD Protocol Stack

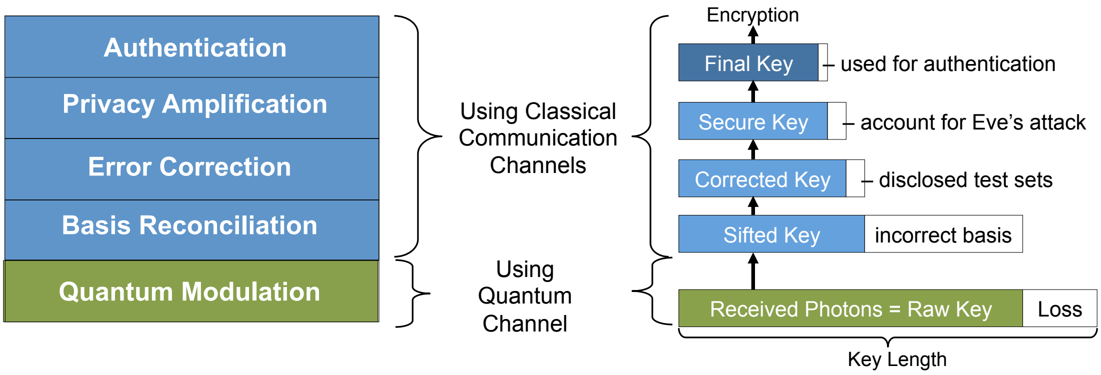


Figure 2.2: Protocol stack of a QKD system [7, 16]

2.1.1.1 Quantum modulation

QKD protocols either belong to the family of “prepare and measure” or are “entanglement based” protocols. In the former case (e.g. BB84, B92, SARG) Alice prepares a photon by measuring it in a certain basis and then transmits it to Bob together with the information gained. In the latter case (E91, BBM92) Alice and Bob both receive entangled photons and perform measurements on an individual basis. However the quantum channel is only used to transmit qubit photons unidirectional for both types of protocols. After photon detection at Bob the quantum information has been converted to classical bits and is forwarded as so-called *raw key* to the higher layers of the QKD protocol stack. Any further communication between Alice and Bob is done over the insecure but authenticated public channel (bidirectional).

2.1.1.2 Sifting Phase

During sifting phase (also called basis reconciliation) Alice and Bob start a discussion about the photon detection events using the classical channel. The public channel is only used to exchange information about the measurement bases not the detection results themselves. Bob discards all transmitted keys for which he has not detected any photon due to absorption or limited quantum efficiency (QE) of the detector. Further he discards all detected photons which Alice measured with a different basis. The remaining key material is called *sifted key.*

2.1.1.3 Error Correction

Next an error detection/correction phase is executed where Alice and Bob have to sacrifice some of the sifted key bits to certify it's coincidence. Wrong measurements due to intrinsic detector or channel noise and potential quantum attacks may cause erroneous disparity in the key material. All errors will be contributed to eavesdropping attacks and are expressed by the qubit error rate (QBER) with is the QKD equivalent of the bit error rate (BER) of classical signals. QBER is always $> 0\%$ even if no eavasdropper is listening and only channel noise and component loss is present. Classical error correction protocols - such as CASCADE [17] or LDPC (Low Density Parity Check) [18] - can be used to correct these inherently wrong bits and produce the *corrected key.* CASCADE uses parity bits to locate the errors but consumes about 20% more key bits [7] than predicted by Shannon's coding theorem [19]. There is a theoretical upper limit to QBER ($QBER_{shannon} \leq 13\%$, $QBER_{CASCADE} \leq 11\%$) at which the QKD protocol can not extract secure keys anymore.

2.1.1.4 Privacy Amplification

Finally, the key length is reduced according to the evaluated QBER level in order to decrease the potential information an eavesdropper (Eve) could have gained. In order to reduce Eve's total amount of key information, the technique of privacy amplification [20] is applied. Here the key is shortened by a QBER-dependent fraction using hash functions (e.g. a Tplitz matrix approach). The key length has to be reduced by at least the number of bits exchanged during the error correction phase to account for any information leakage to Eve. Some schemes pre-estimate the contributions to QBER of the system components themselves and only consider the remaining QBER magnitude for privacy amplification. After key shortening the eavesdropper is left with a Shannon information of only one bit of the entire key if the best possible attack is assumed. The remaining key bits represent the *secret key* and can be securely used to exchange sensitive data utilizing classical data encryption methods.

2.1.1.5 Authentication

In order to prevent a man-in-the-middle attack some sort of authentication needs to be established on top. For example in BB84 a small pre-shared key has to be known a-priori to Alice and Bob. After privacy amplification both share the exact same secure key bits. Blocks of these bits are hashed with the pre-shared key to generate an authentication tag which is subsequently exchanged and compared. Since the *final key* is grown from a small pre-shared the BB84 protocol is referred to as *Quantum Key Growing protocol.*

2.1.1.6 Encryption

The QKD protocol stack outputs secure key material which is consequently used by the application layer to perform encryption/decryption of plaintext messages. The initial idea of using the information-theoretical secure one-time pad (OTP) encryption would require a final key rate that is equal to the data rate. As the next sections show, the key rate of existing QKD schemes - both experimental and commercially available - is still far below the data-channel rates of 1 to 100 Gbit/s. However in scenarios with small QBER values it is feasible to protect a low data rate by using OTP encryption. If QBER increases - due to eavesdropping or channel noise - the key bits could be used in classical symmetric encryption schemes (block or stream ciphers, e.g. AES) to protect high data rate links without the problem of initial key distribution. Even the security of asymmetric cryptography can be enhanced by mixing in some OTP encrypted bits. With this approach QKD operation can still be maintained even in situations with extremely high QBER and a small amount of usable key bits (e.g. Denial-of-Service attacks, see [21]).

2.2 QKD Schemes

The recent research literature presents a variety of QKD schemes that can be distinguished by the type of quantum encoding (phase or polarization of photons) and consequently the used photon detectors and sources. In this work the photon source is used to characterize the systems as suggested by [22]. Depending on the signal source certain QKD protocols can be applied [23] which are introduced in the following sections. Fig. 2.3 outlines the hierarchical relations between the described QKD schemes.

2.2.1 Weak Laser Pulse QKD

In Weak Laser Pulse schemes the quantum information is encoded on quantum signals with a resolution of only one photon corresponding to a pulse energy of $1.28 \times 10^{-19} J$ at 1550 μm. Each signal with two or more photons is a security risk, because a second photon may carry the same quantum information and could subsequently be eavesdropped by an adversary without being noticed. Since the technology to generate single photons on demand with quantum dots is not mature enough, most QKD schemes use weak laser pulse sources. The laser pulse is attenuated by approximately 70 dB to the level of 1 photon/pulse in average.

The usage of polarisation encoding is difficult because of birefringence of optical fibers. Phase modulation with Asymmetric Mach-Zehnder Interferometers (AMZI) can be used to realize a fast weak laser pulse scheme with the disadvantage of on-going phase-stabilization [24]. Further, the first commercially available Mach-Zehnder implementation called *plug&play* scheme from the Swiss company idQuantique [25] can be used to phase-encode quantum bits. Here, the signal is generated and attenuated at Bobs site, subsequently sent to Alice where the qubits are measured (hence prepared) and reflected by a Faraday mirror to compensate for polarization and phase fluctuations along the quantum channel. Another option to avoid phase-stabilization techniques is to encode quantum information in the phase difference between pulses (DPS protocol, see 2.2.1.6).

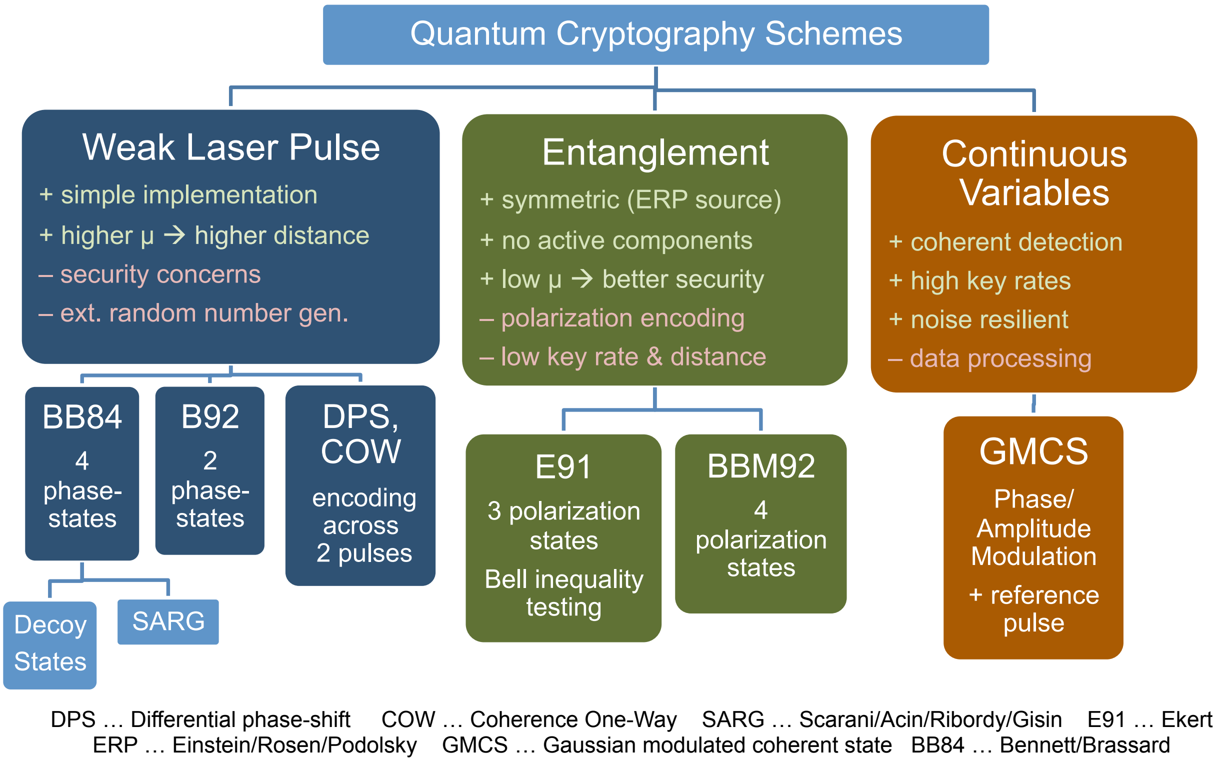


Figure 2.3: Overview of Quantum Key Distribution schemes

2.2.1.1 BB84 [11]

In 1984 Charles Bennett and Gilles Brassard presented the first protocol for quantum key distribution which is now referred to as BB84. It is the most widely used QKD protocol and foundation for some derivations. Here Alice and Bob choose one of two non-orthogonal polarisation bases (0°/90° or 45°/135°). When Bob measures the qubits he uses the wrong basis half of the time resulting in a key length reduction of 50% after comparing his bases with Alice (sifting). The security of BB84 is rooted in the random basis selection by Alice and Bob together with the no-cloning theorem of single photons. According to quantum mechanics Eve cannot fully measure incoming photons in both bases which would allow her to select the corresponding measurement result after the measurement bases is revealed by Alice in the sifting process.

2.2.1.2 B92 [26]

The B92 Protocol is a simplified version of BB84 in the form of reduced set polarisation states. While a qubit in BB84 can have one of four non-orthogonal polarisation states, B92 uses just two non-orthogonal polarisation states. Additionally Bob only transmits the positions of the bases he keeps, rendering the protocol simpler and faster to operate.

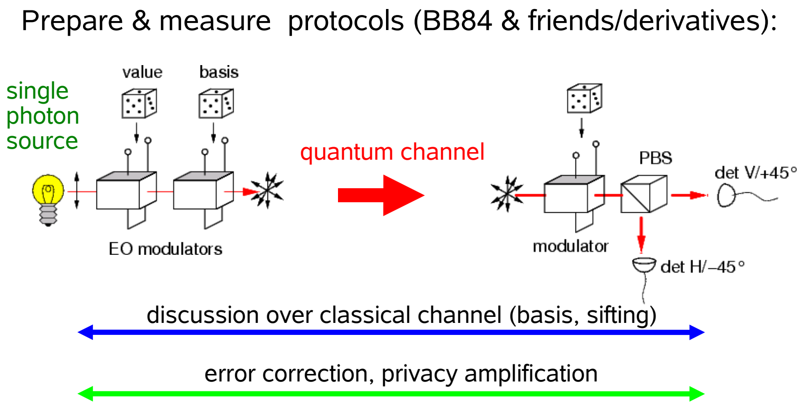

Prepare & measure protocols (BB84 & friends/derivatives):
single photon source
value
basis
EO modulators
quantum channel
PBS
det V/+45°
modulator
det H/–45°
discussion over classical channel (basis, sifting)
error correction, privacy amplification

Figure 2.4: Measure and Prepare (BB84) scheme

2.2.1.3 Security Concerns

The basic *intercept and resend* attack of Eve describes an attack on a photon originating from a perfect single photon source. The attack is incoherent as each signal photon is attacked independently. Eve measures the photon in a random basis and re-sends a new photon she had prepared corresponding to her measurement result. Since this is the basic eavesdropping scenario all QKD protocols are able to detect this attack in the error correction phase. The subsequent step of privacy amplification reduces Eve's gained knowledge to almost zero. So-called *man-in-the-middle* attacks can not be prevented by quantum mechanics as Eve can always cut the fiber and appear to be Bob or Alice respectively. This class of attacks can be ruled out by applying unconditionally secure authentication schemes as mentioned in 2.1.1.5.

On the theoretical side, proof of the unconditional security of the BB84 and the B92 protocols were found [20]. However in real QKD systems assumptions such as a perfect single photon source or ideal detectors are problematic. According to Poisson statistics, there still exist quite many pulses consisting of more than one photon, which open the possibility for *photon-number splitting* (PNS) attacks [20, 27]. In PNS attacks, Eve counts the number of photons and for pulses with more than one photon she keeps one in her quantum memory and forwards the others on a lossless channel. During basis reconciliation the measurement bases are revealed on the public channel and she can measure the stored photon in the corresponding basis to read the entire sifted key. PNS also belongs to the class of incoherent attacks. Protocol extensions – such as SARG and Decoy States – are suggested to make PNS ineffective.

A completely different but technically feasible approach is to exploit implementation imperfections of the QKD system and not to attack the QKD protocol itself. On the one hand, *side-channel attacks* take advantage of any leaked information such as detector efficiency mismatch or not totally random number generators [7]. On the other hand, the even more aggressive attacks called *quantum hacking* try to take complete control the detectors, for example by overloading them with strong light pulses. Their counter measures have been discussed intensively in the scientific community. The defense strategies comprise different approaches, from avoiding specific electronic components to monitoring the intensity of the light. These type of attacks need to be considered in any practical QKD system implementation by careful selection of components.

2.2.1.4 SARG [28]

The SARG protocol uses BB84 in it's four-bases version but introduces changes in the sifting phase. With SARG, Alice does not reveal her measurement basis but a choice of two possible qubit states (e.g. qubit was either 0° or 135°). So if Bob's measurement in the 0°/90° basis yields the result 90° he knows for sure that the qubit state was 135°. This scenario happens only 25% of the time, thus the sifted key rate is reduced with respect to BB84. However, even if Eve fully measured the photons (e.g. by a photon-number-splitting attack - see) she is left with two equally possible qubit states and can not deterministically gain any information about the sifted key. The inefficiency of PNS attacks allows the QKD system to utilize stronger laser pulses (higher mean photon number per pulse) as compared to BB84.

2.2.1.5 Decoy State Protocol [29]

The usage of decoy states was first proposed by Hwang in 2003 as another strategy to overcome PNS attacks on BB84 [29]. Here a qubit is prepared in either one of the four BB84 polarisation states (signal states) or as an introduced decoy states. Decoy states are not encoding any key information but are only used to detect PNS attacks. Decoy and signal states differ only in their photon number distributions thus Eve's measurements can not distinguish between them as both appear to be multi-photon pulses. A real world implementation that is working with existing QKD systems was presented in [30]. By applying decoy states in QKD protocols, a higher average photon number per pulse can be used without worrying about PNS attacks. As with SARG a longer transmission distance can be archived.

2.2.1.6 DPS State Protocol [31]

Another method to overcome PNS attacks on BB84 is the Differential phase-shift (DPS) protocol. Here Alice emits a sequential pulse train and randomly prepares the relative phase of each pulse in the train as $+\frac{\pi}{2}$ or $-\frac{\pi}{2}$. At Bob the sequential pulses interfere after a 1-bit delay Mach-Zehnder interferometer with its' outputs connected to two single photon detectors, respectively. Depending on which detectors fires, the receiver can conclude whether the phase is $+\frac{\pi}{2}$ or $-\frac{\pi}{2}$. Bob records the phase result and the detection time instance and reports the time instance information to Alice, which allows her to figure out the value of the relative phase.

2.2.1.7 Coherence One-Way Protocol (COW) [32]

In [33] a totally new coherence one-way protocol (COW) is suggested which adopts encoding schemes from classical physical layer protocols. COW is a so-called distributed-phase-reference protocol and its security relies on the coherence between successive non-empty pulses. As in DPS protocol a pulse train is emitted by Alice consisting of full and empty pulses and Bob's detectors temporally distinguishes between them. The key bit value is defined by the position of the non-empty pulse: first = 0 and second = 1. In order to facilitate a subsequent coherence check, Alice prepares all pulses with a common phase reference. Bob randomly selects a fraction of pulses not used as raw key but to measure the coherence between adjacent qubits by an interferometer. COW is resilient to PNS attacks because an eavesdropper may not individually act on qubits by either removing one photon out of pulses with multiple photons, or by blocking pulses with only 1 photon, without disturbing the system and being detected. Additionally decoy sequences are used as a counter measure against coherent attacks on two pulses across the bit separation.

2.2.2 Entanglement-based QKD

In contrast to the weak laser pulse approaches it is also possible to exploit entanglement of two photons (an ERP-pair). In order to get entangled, Spontaneous parametric down-conversion (SPDC) in non-linear crystals can be used to generate such photon pairs that can be distributed to Alice and Bob respectively. Initially no information is encoded by the photon generation process. The qubit is encoded after Alice measures her photon along one polarization axis and initiates a wave-function-collapse which fixes the polarization of Bob's photon. Two different approaches can be used to measure the correlation. The rather impracticable Ekert scheme (E91) uses on-going tests based on Bell's inequality to detect eavesdropping. Today, most entanglement based QKD schemes implement an adaptation of the conventional BB84 protocol called BBM92. Entanglement-based QKD schemes are more resilient to quantum-hacking attacks because they can be implemented with passive components only. Alice's random choice of the key bit values happens in the pair generation process, while the basis selection can be passively randomized by interposition of a beam splitter. However, since entanglement-based cryptography requires a correlated detection of two photons, the raw (unsifted) bit rate is limited by the squared detection probability of a single photon detector [34].

2.2.2.1 E91 [13]

Different from the protocols described so far, the E91 protocol is not based on the no-cloning theorem but on quantum entanglement. In 1991, Artur Ekert introduced the idea of supplying each Alice and Bob with one photon of an ERP-pair having correlated polarizations. For each photon they perform a measurement along a randomly chosen basis from two different sets of non-orthogonal polarisation directions (ϕ_{Alice}=$\{0,\frac{\pi}{4},\frac{\pi}{2}\}$, ϕ_{Bob}=$\{\frac{\pi}{4},\frac{\pi}{2},\frac{3\pi}{4}\}$) yielding randomized but strongly correlated results. The protocol then utilizes a fraction of the raw key to check for Bell inequality violations. If the Bell inequality is not violated then eavesdropping must have destroyed the entanglement correlation and corresponding key bits are discarded during basis reconciliation. The benefits of E91 compared to BB84 are that there is no need for external random number generators or any other active components which can be compromised by Eve's attacks (also termed *quantum hacking*). However, Ekert has not proven the protocol's resilience against the replacement of the ERP-source with a fake source designed to show ERP-characteristics while leaking information to Eve (also termed *source substitution*).

2.2.2.2 BBM92 [35]

One year after Ekert proposed E91, the authors of BB84 included the possibility to utilize entangled photon sources in their original scheme. The adapted protocol – called BBM92 – is simpler than E91 because it avoids the impractical Bell inequality check but assumes independent random measurements of Alice and Bob on the polarisation bases 0°/90° or 45°/135° (see Fig. **??**). As before the basis choice is random but in cases where Alice and Bob used the same basis they get perfectly correlated results. The implementation of BBM92 can also be achieved by exclusive use of passive components and was proved to be resilient against fake ERP-source replacements.

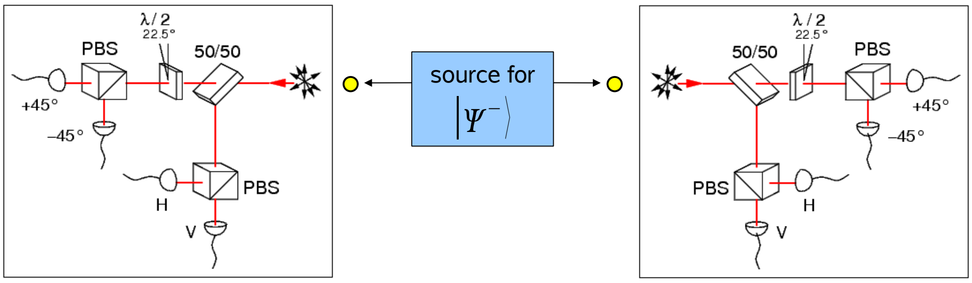


Figure 2.5: Entanglement Based scheme (BBM92)

2.2.3 Continuous-Variable QKD

Instead of using the phase or polarization of single photons to encode qubits, Continuous-Variable (CV) QKD protocols use coherent detection of strong optical pulses [36, 37]. For example the Gaussian modulated coherent state (GMCS) QKD protocol uses the two quadratures (phase and amplitude) of a coherent state as conjugate variables [38]. Alice modulates the phase and amplitude of the signal pulse according to two Gaussian distributions with mean at zero and variance of $V_A N_0$ (with $N_0 \leq \Delta x \Delta p$ being the quantum noise variance of the Heisenberg relation). Additionally an orthogonally polarized intense phase reference called local oscillator (LO) is time-multiplexed onto the channel. At Bob the LO pulse is phase modulated by either 0° or 90° to select the quadrature to measure. After a delay line at Bob the LO pulse interferes with the weak signal pulse. The detector accepts only photons in the same spatiotemporal and polarization mode as the LO, while noise photons in different modes will be suppressed effectively. Thus this scheme is very resilient to noise photons which can be beneficial for a co-existence WDM architecture (see 2.3). Furthermore the GMCS QKD has the potential of providing high secure key rate, especially at relatively short distances. A comprehensive overview about the signal encoding and detection implementations can be found in [22].

2.2.4 Single photon detectors (SPD)

All of the previously mentioned schemes need to include single photon detectors. Given a certain type of photon source, these detectors are the most critical part regarding QKD system performance. Hence, a lot of research effort is undertaken to improve timing accuracy, detection rate and noise figures of single photon detectors. Some characterizing features of photon detectors are the detector dark count rate (ns^{-1}), quantum efficiency QE (%), after-pulse probability (%) and the gate length (ns) in case of gated operation. The quantum efficiency is the probability that an incoming photon is detected while the after-pulse probability determines the rate of erronous detection events subsequent to real photon arrivals.

2.2.4.1 Avalanche Photo Diodes (APD)

Avalanche Photo Diodes are most widely used in various QKD experiments because of their detection capabilities across telecom fiber wavelengths (O-Band/C-Band) and can be realized in InGaAs or InP. In an APD a photon excites a small carrier which grows into a macroscopic current output via the carrier avalanche multiplication. However, some carriers remain trapped in the APD until they spontaneously trigger additional avalanche Problems. This problem is referred to as *after-pulsing* and can be mitigated by restricting photon detection to a finite time-window (known as gated mode) but has a negative effect on achievable raw key rates. Quantum efficiency (QE) and dark count rate of APDs is 10% and $10^{-5} \ldots 10^{-6} nm^{-1}$, respectively. In [39] the concept of a **self-differencing** InGaAs APD has helped the research group to achieve very high secure key rates of 1.02 Mbit/s. Here the APD was cooled to $-30 \circ C$ and a self-differencing circuit was included to remove the periodic capacitive response before detection by the discrimination electronics. This permits ultrashort detector dead time which allows minimum photon detection intervals of 2ns.

2.2.4.2 Superconducting single photon detectors (SSPD)

Superconducting single photon detectors exhibit a very low dark count ($\approx 10^{-9} nm^{-1}$) and high timing accuracy but need to be cooled to few kelvin. The drawback of SSPD is the low quantum efficiency of 1%. Since SSPDs are almost free of after-pulsing they can be operated in free-running mode (no gating windows) which result in higher key rates.

2.2.4.3 Frequency up-conversion SPDs

Some implementations try to overcome the drawbacks of using photon detectors for telecom frequencies (such as APD) by up-converting the signal frequency. A non-linear effect in Periodically poled Lithium Niobate (PPLN) waveguides called sum frequency generation (SFG) allows to convert C-Band photons to a visible photon at around 600nm with 99% efficency [40]. The higher signal frequency facilitates the usage of Silicon APDs which exhibit higher QE of 8% and dark count rate of $10^{-6} nm^{-1}$. As this kind of SPD can be operated on 10 GHz systems it is best candidate for high bit rate QKD. However, problems related to timing jutter arise for high count rates.

2.2.5 Dark Fiber Experiments

In Tab. 2.1 on the following page a summary of available QKD experimental results is presented. The columns describe various parameters used for the results such as the fiber length (Len), the final secure rate (R_{sec}), the average photon number emitted by the source (μ), the encoding scheme and its implementation (Encoding), the pulse rate of the source (f_{rep}), the QKD channel wavelength and generation method (Source), the type of photon detectors uses (Detector) and the synchronisation technique (Sync). Additionally references to the corresponding papers and their publishing date is given.

$Len[km]$	R_{sec} $[s^{-1}]$	μ	Encoding	f_{rep}	Source	Detector	Sync	Status	Year
10.2	50	0.5	BB84 phase-modulation (AMZI)	3.5-5MHz	1550nm weak	gated InGaAs APD QE 10-18	TDM	Experimental	2005 [34]
0.01	10 000	0.1	BB84 phase-modulation (AMZI)	3.5-5MHz	1550nm weak	gated InGaAs APD QE 10-18	TDM	Experimental	2005 [34]
–	–	–	BB84 polarization-entangled (SPDC)	3.5-5MHz	1550nm ERP	gated InGaAs APD QE 15-20	TDM	Experimental	2005 [34]
48	10	0.63	B92 phase-modulation (AMZI)	100kHz	1310nm weak	gated InGaAs APD QE 11, DC 5×10^{-6}	WDM 1550nm	Experimental	2000 [41]
48	2.4	0.39	B92 phase-modulation (AMZI)	100kHz	1310nm weak	gated InGaAs APD QE 11, DC 5×10^{-6}	WDM 1550nm	Experimental	2000 [41]
22	1 510	0.2	BB84 phase-difference (send-and-return FM)	5MHz	1550nm weak	gated InGaAs APD DC 10^{-5}	TDM	Commercial	2002 [25]
67	50	0.2	BB84 phase-difference (send-and-return FM)	5MHz	1550nm weak	gated InGaAs APD DC 10^{-5}	TDM	Commercial	2002 [25]
96	8.2	0.2	BB84 phase-difference (send-and-return FM)	5MHz	1550nm weak	gated InGaAs APD DC 10^{-5}	TDM	Commercial	2002 [25]
122	50	0.1	BB84 phase-modulation (optimized AMZI)	2MHz	1550nm weak	gated InGaAs APD QE 12, DC 10^{-7}, $-100°C$	WDM 1310nm	Experimental	2004 [24]
97	800	0.4	BB84 phase-modulation (AMZI + DCF)	625MHz	1550nm weak+decoy	SSPDs QE 1.6, DC 10^{-7}	WDM 1570nm	Long-time	2008 [42]
20	1 020 000	0.55	BB84 phase-modulation (AMZI)	1GHz	1550nm weak+decoy	SD InGaAs APD QE 10, DC 6.8×10^{-6}	separate	Experimental	2008 [39]
100	10 100	0.55	BB84 phase-modulation (AMZI)	1GHz	1550nm weak+decoy	SD InGaAs APD QE 10, DC 6.8×10^{-6}	separate	Experimental	2008 [39]
10	1 340 000	0.2	DPS phase-difference (AMZI)	2GHz	1550nm weak+decoy	PPLN frequency up-conversion SPDs QE 25, DC 8.4×10^{-6}	separate	Experimental	2009 [40]
100	6 000	0.5	COW phase modulation (AMZI)	625MHz	1550nm weak+decoy	SSPDs QE 2.65, DC 5×10^{-9}	separate	Long-time	2009 [43]
250	15	0.5	COW phase modulation (AMZI + ULL)	625MHz	1550nm weak+decoy	SSPDs QE 2.65, DC 5×10^{-9}	separate	Long-time	2009 [43]
10	1 160 000	0.2	DPS phase modulation (Faraday-Michelson interferometer)	2GHz	1550nm weak	SSPDs QE 3, DC 10^{-9}, 1.7 K	separate	Experimental	2012 [44]
260	6 000	0.2	DPS phase modulation (Faraday-Michelson interferometer)	2GHz	1550nm weak	SSPDs QE 3, DC 10^{-9}, 1.7 K	separate	Experimental	2012 [44]

Table 2.1: Experimental results of QKD systems using dark fibers.

2.3 Integration of QKD systems in transparent optical networks

The QKD schemes described in Table 2.1 were realized using dedicated dark fibers for the quantum channel. If no data signals are present on quantum channel fiber, secure key rate exceeding 1 Mb/s and a transmission distance of over 250 km has been achieved [44]. However, prohibitive lease costs and limited availability of dark fibers hinder the widespread application of such QKD systems. Theoretical and experimental investigations concerning the co-existing of quantum and conventional channels have shown that when using the current QKD technology, limiting the number of WDM channels (e.g. to four channels) and reducing the signal power far below the standardized levels, a reach up to 50 km is achievable. This is too short for long-haul links, but suitable for implementing QKD in the metropolitan area. An overview about recently reported experiments using co-existence schemes are presented in the end of this section (Tab. 2.2).

2.3.1 Impairments

Strong conventional signals in optical access networks are causing nonlinear effects in optical fibers. These effects can constitute severe problems for the weak quantum signals and need to be addressed individually and in combination. Additionally, imperfections of optical components also contribute to an increase in signal loss. Several studies have shown that coexistence architectures are in principle possible [45, 46, 47], but impairments are strongly limiting the performance of QKD systems. The optical noise power in a quantum band should not exceed -138 dBm or 16 attowatts (corresponding to 1.24×10^{-7} photons per nanosecond in the 1550 nm band) to not severely impact the performance of a QKD system with a dark count probability of 10^{-7} [46]. Conventional network designs do not care about such low levels of noise and need to be investigated. In order to find wavelength regions in which QKD operation is feasible, all effects causing background noise photons need to be characterized and understood [46, 47, 48**?**].

2.3.1.1 Attenuation

Since all QKD systems are extremely sensitive to losses and noise, the effects that mainly influence the transmission of the weak QKD signals determine if sharing the same fiber is possible or not. Depending on the fiber type used for transmission, an attenuation curve describes the wavelength dependent attenuation of optical signals being transmitted along the fiber. ITU-T G.652-compatible Standard Single-Mode Fibers (SSMF) exhibit a broad water peak around 1383 nm, making this wavelength range impractical for efficient transmission. The “conventional” band about 1.5 m (*C-band*) is most widely used for modern long-range optical communications due to the low attenuation down to 0.2 dB/km. The low attenuation makes this band also attractive for QKD systems, but the co-existing classical signals within the same band likely cause serious impairments. The “original” band around 1.3 m (O-band) has a higher attenuation of about 0.3 dB/km. It is often used for short- and middle-range transmission and may be appropriate for accommodating a quantum channel in some cases because of the large spectral separation to signals in the typically highly occupied C-band.

2.3.1.2 Rayleigh scattering

In schemes with bidirectional communication within the same fiber (like access networks or two-way QKD systems), problems with Rayleigh scattering may occur. Rayleigh scattering is caused by fiber refractive index inhomogeneities [49] and generates noise photons at the same wavelength as the incident signal thus referred to as elastic scattering effect. Some of the generated photons are captured in a fiber's spatial mode and propagate in the backward direction. Spectral filtering can not be applied to decouple these photons as their frequency equals the signal frequency. Furthermore, Rayleigh scattering can occur anywhere in the fiber, which hinders the effective suppression by temporal filtering with gated photon detectors. The prominent two-way QKD system developed by the swiss company *idQuantique* [25] mitigates phase and polarisation drifts in the fiber by employing a faraday mirror reflector (*send-and-return* scheme). As a negative side effect their system suffers from Rayleigh scattering due to this bidirectional approach. In their system Bob sends trains of pulses and Alice's station incorporates a storage line of corresponding length to delay the response. They managed to suppress the elastic scattering, but at the same time decreasing the achievable key rate due to the introduced delay time.

2.3.1.3 Brillouin scattering and Spontaneous Raman scattering

Scattering effects in fibers pose one of the major sources for signal degradation in QKD channels. Inelastic photon scattering causes frequency shifts of incident photons. The frequency shifts caused by acoustic vibrations (Brillouin scattering) has a low bandwidth (1-10 GHz) but to be considered if the quantum channel is being placed in between of neighboring channels in the 100 GHz ITU-T grid. In contrast, Raman scattering, where optical phonons (i.e. incoherent movements of atoms in a lattice) are involved, introduces large spectral shifts with a maximum offset of 13 THz from the incident (pump) wavelength. Here the optical fiber itself acts as active gain medium. The co-existing wavelength channels can be interpreted as pump sources of an optical amplifier integrated into the fiber.

Two types of photon wavelength generation processes take place. In case of *Stokes scattering*, part of the photon energy is absorbed by the fiber resulting in the generation of scattered waves at lower frequencies. When a photon scatters off an exited phonon, energy is transferred to the photon in an *anti-Stokes scattering* process generating a wave of higher frequency. The anti-Stokes scattering is less effective than Stokes scattering as it requires the pre-existence of vibrational modes. As a consequence the QKD wavelength should preferably be chosen below the wavelength of co-existing data channels in order to minimize Raman scattering effects. The effect of Raman scattering depends on the fiber length and increases until a distance of 17 km [50]. Above a length of 17 km, fiber attenuation outweighs Raman scattering powers and decreases the overall background noise contribution.

2.3.1.4 Amplified Spontaneous Emission

Optical amplifiers are necessary in some metropolitan area networks and also more frequently in wide area networks to increase bit-error-free transmission distances. Doped fiber amplifiers, Semiconductor optical amplifier or Raman amplifiers allow amplification in transparent optical networks without the need to cross-convert optical to electrical signals. Erbium Doped Fiber amplifiers (EDFA) provide a gain across the 1550 nm region (C-Band) and can be efficiently pumped with a laser at a wavelength of 980 nm or 1480 nm. The pump signal excites erbium ions to their higher-energy state which consequently transfer power to incoming signal photons when descending back to ground state. The noise generated by doped fiber amplifiers originates from spontaneous decaying erbium ions which emit incoherent omnidirectional photons. Some photons can be guided in the fiber and are further amplified when interacting with other exited erbium ions. This effect is called Amplified Spontaneous Emission and exhibits the same spectral characteristics as the gain itself.

2.3.1.5 Four-wave mixing

Finally, when dealing with multiple signals at different wavelengths or frequencies $f1, f2, ..fn$, as in the case of WDM transmission systems, the effect of four-wave mixing has to be considered as well. Here, no energy is transferred to or from the optical fiber, but the scattering of incident photons produces another photon at a different wavelength. The efficiency of four-wave mixing depends on the coherence of the incident photons and commonly decreases quickly due to the chromatic dispersion. Thus, the quantum channel should not be placed at frequencies corresponding to $f_{ijk} = f_i + f_j - f_k$, where $i, j \neq k$.

2.3.2 Co-existence Experiments

Theoretical and experimental investigations concerning the co-existing of quantum and conventional channels have shown that when using the current QKD technology, limiting the number of WDM channels (e.g. to four channels) and reducing the signal power far below the standardized levels, a reach up to 50-90 km is achievable [51]. In Table 2.2 an overview of published co-existence QKD experiments is given. Among the most important aspects when incorporating QKD systems into classical optical networks is the filtering architecture. Spectral and temporal filtering can be applied in order to suppress in-band noise photons reaching into the quantum channel.

km	R_{sec}	QBER	Data Channels	Quantum Channel	Filtering	Detector	Year
28	–	4%	1ch 1591nm 1.2Gbit/s, -29.1dBm	1300nm BB84, 1Mhz, $\mu = .2$	CWDM Mux/Demux EX = 50dB	InGaAs APD QE 0.4%	1997 [52]
10	38	%	1ch 1550nm, 2dBm 100kHz sync pulses	1300nm B92, 100kHz, $\mu = .36$	CWDM Couplers EX = ?	InGaAs APD, 2.5ns gating QE 11%	2003 [53]
0.01	38	%	1ch 1550nm, 2dBm 100kHz sync pulses	1300nm B92, 100kHz, $\mu = .36$	CWDM Couplers + MEMS EX = 110dB, IL = 6dB	InGaAs APD, 2.5ns gating QE 11%	2003 [54]
10	90	4.3%	4ch+OSC 155x+1510nm 2dBm	1310nm B92, 100kHz, $\mu = .5$	1310/1550 Couplers + NBF EX = ?, IL = 2.2dB	InGaAs APD, 2.5ns gating QE 11%	2004 [55]
50	–	4.8%	1ch 1552.5nm -8dBm	1549.3nm BB84	DWDM Couplers EX = ?	QKD system MagiQ Model OPN 7505	2006 [47]
25	9	4.6%	4ch+OSC 155x+1510nm 0dBm, 1x10Gbps + 3x2.5Gbps	1310nm B92, 100kHz, $\mu = .5$	1310/1550 Couplers + 1.5nm NBF EX = 27dB, IL = 2.2dB	InGaAs APD, 2.5ns gating QE 20%, DC 1.4×10^{-4}	2006 [50, 56]
15	12	5.8%	4ch 155x -25dBm, 4x10Gbps	1310nm B92, 100kHz, $\mu = .5$	1310/1550 Couplers + 1.5nm NBF EX = 120dB, IL = 1.3dB	InGaAs APD, 2.5ns gating QE 20%, DC 1.4×10^{-4}	2007 [46]
25	6	5.8%	2ch 1552.5/1550.9nm -8dBm per ch	1549.32nm BB84, 10MHz, $\mu = .5$	5Ghz NBF + 140GHz ROADM + 15Ghz NBF EX = 28dB/45dB	InGaAs APD	2009 [57]
25	90	4.6%	4ch+OSC 155x+1510nm 2dBm per ch	1310nm B92, 100kHz, $\mu = .5$	1310/1550 Couplers + 1.5nm NBF EX = 27dB, IL = 2.2dB	InGaAs APD, 1ns gating DC 1.4×10^{-4}	2009 [58]
41	7.5	6.4%	4ch 155x nm 2x1Gb/s encrypted data, 2xPublic, -22dBm per ch	1549.32nm BB84, 5MHz, $\mu = t$	DWDM Couplers + 45pm NBF EX = 82dB+12dB, IL = 1.95dB+2dB	InGaAs APD, 1.5ns gating QE 7%, DC 5×10^{-6}	2010 [18]
50	11	5.4%	4ch 155x nm 2x1Gb/s encrypted data, 2xPublic, -22dBm per ch	1549.32nm SARG, 5MHz, $\mu = 2\sqrt{t}$	DWDM Couplers + 45pm NBF EX = 82dB+12dB, IL = 1.95dB+2dB	InGaAs APD, 1.5ns gating QE 7%, DC 5×10^{-6}	2010 [18]
10	0	$> 13\%$	1ch 1554.94nm Public, 0dBm	1559.79nm BB84, 5MHz, $\mu = .5$	100GHz DWDM Couplers EX = 80dB, IL = 3dB	InGaAs APD, 1ns gating QE 3.8%, DC 5×10^{-6}	2010 [38]
10	> 0	$< 13\%$	38ch C-Band 0dBm	1559.79nm GMCS CV QKD, 1MHz	100GHz DWDM Couplers EX = 80dB, IL = 3dB	100MHz homodyne detector 1ns gating	2010 [38]
90	7600	%	3ch 1571/1591/1611nm 1xSync -47.6dBm, 2xData -18.5dBm	1551nm BB84, 1GHz, $\mu = .5$, DSF, polCtrl	CWDM Couplers + 0.56nm NBF EX = CWDM + 15dB + 9.4dB (temporal), IL = 2dB+0.6dB	InGaAs SD-APD 100ps gating, $T_{dead} < 2$ns, QE 20%, DC 1.4×10^{-4}	2012 [51]

Table 2.2: Experimental results of QKD systems in a co-existence scheme. (EX . . . extinction ratio, IL . . . insertion loss, QE . . . quantum efficiency, DSF . . . Dispersion Shifted Fiber, DC . . . Dark Counts per ns, NBF . . . Narrow Bandpass Filter, polCtrl . . . Polarisation Controller)

3 Optical Networks Technologies

In general, data networks can be grouped according to the geographical area they cover, i.e. the transmission distance. In general networks are categorized as either *long-haul*, *metropolitan area (metro)* or *access* area network. In Fig. 3.1 a generic overview is given which outlines the hierarchical relations between these different types of network technologies.

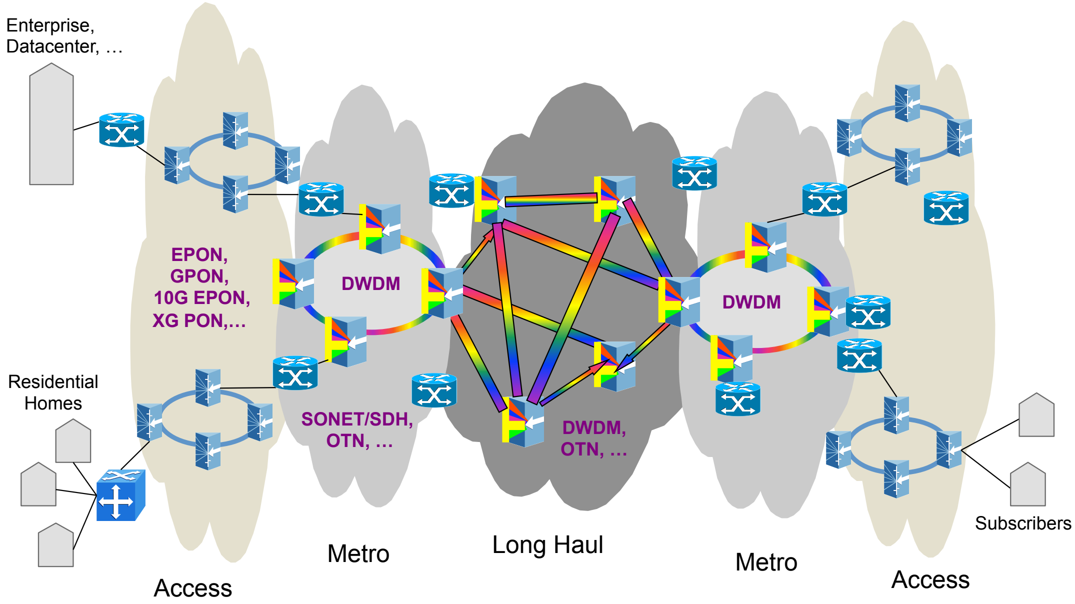


Figure 3.1: Generic structure of today's network technologies

Internet service providers (ISPs) are operating access networks through which subscribers (e.g. residential homes or enterprises) can connect to the Internet. Typically, the reach of access area networks is a few kilometers up to around 20 kilometers depending on the access technology. The physical connection can be either traditional copper cables (e.g. telephone network), wireless radio transmission (e.g. WiMax) or optical fibers. Since quantum key distribution rely on photons as information carriers, this section describes only optical access networks in greater detail.

Metropolitan area networks are usually located in an urban area or region. Their geographical reach can extend from tens to hundreds of kilometers which are consistent with the maximum reach of recent QKD experiments (see section 2). In the following section different variants of metropolitan area networks are explained regarding data format, data rates, wavelength plans, multiplexing and signal modulation.

The long-haul network is also referred to as core network or wide area network. It represents the global communication network and connects different metropolitan area networks. Both long-haul and metropolitan area networks have either a meshed, a ring topology or a combination. Long-haul connections are exclusively made of optical fiber links in contrast to access networks which can also comprise copper cables. The advantages of optical fibers are the low attenuation (long reach), low noise, no electromagnetic interference (EMI) and a very large bandwidth.

3.1 Metropolitan Area Networks

First generation photonic networks use optical technology only for transmission of signals between nodes. Only a single wavelength is used for transmission and functions such as switching, processing, monitoring and routing have to be realised in electronics. Hence, all nodes of first generation optical networks need to convert optical signals to electronic signals prior to further processing. The processing power of electronics limits the maximum achievable transmission rates to currently 40 Gbit/s in commercially available first generation network systems. In order to overcome these limitations, functionality needs to be move towards the optical domain. By integrating optical switches, gates and add-drop multiplexers networks become faster and more *transparent*. Since optical components do not require a clock signal they can process all kinds of signals independent of data format and data rate.

Section 3.1.1 introduces the architecture and data format of SDH as it constitutes the most important multiplexing method for long-haul and metropolitan networks. Subsequently, the technical evolution of using multiple wavelengths for signal transmission is explained in section 3.1.2. Finally, the optical transport network (OTN) is presented in section 3.1.3 as an architecture of a transparent optical network.

3.1.1 Synchronous Digital Hierarchy (SDH/SONET)

The Synchronous Digital Hierarchy (SDH) is a multiplexing method for transferring multiple digital bit streams over optical fibers. It was initially developed by the European Telecommunications Standards Institute (ETSI) to replace the Plesiochronous Digital Hierarchy (PDH) as a synchronized network for circuit-oriented communication. PDH was the result of the growing need for more multiplexing stages to transport large quantities of data and voice calls. Decentralized clocks posed a major problem to PDH and limited scaling of networks. SDH solves this problem by using atomic clocks as a time reference for the entire network. This decreases the buffering requirements between elements of the network.

SDH is not a communication protocol but a transmission protocol, because it allows the simultaneous transmission of various data formats within a single framing protocol. It allows to multiplex channels from 64 kbit/s (as the PCM encoded voice calls of PDH) to the primary rates of 1 544 kbit/s and 2 048 kbit/s. The base frame is defined in ITU-T Recommendation G.707 as *STM-1* (synchronous transport module level 1) and has a bit rate of 155 Mbit/s. The frame format of a STM-1 frame (Fig. 3.2) can be seen as a byte matrix of 9 rows and 270 columns and is transmitted row by row. The first 9 bytes in each row make up the frame header (overhead) which is split

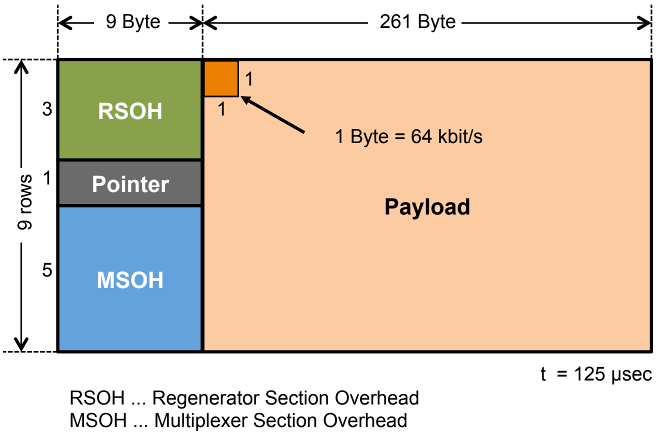


Figure 3.2: STM-1 frame format

into pointer, multiplexing section overhead (MSOH) and regenerator section overhead (RSOH). A transmission of a complete STM-1 frame takes exactly 125 μs which means each byte of the payload represents a 64 kbit/s channel.

In order to transmit multiple tributary signals (PDH or ATM) in the STM-1 payload, a process called mapping is needed. During mapping tributary signals are packaged into containers together with a path overhead - forming a virtual container (VC). The path overhead designates the type of container (i.e. the type of tributary signal) and monitors the link quality. Subsequently, virtual containers are filled into STM-1 frames and the pointer in the STM-1 header can be used to directly access these containers when needed.

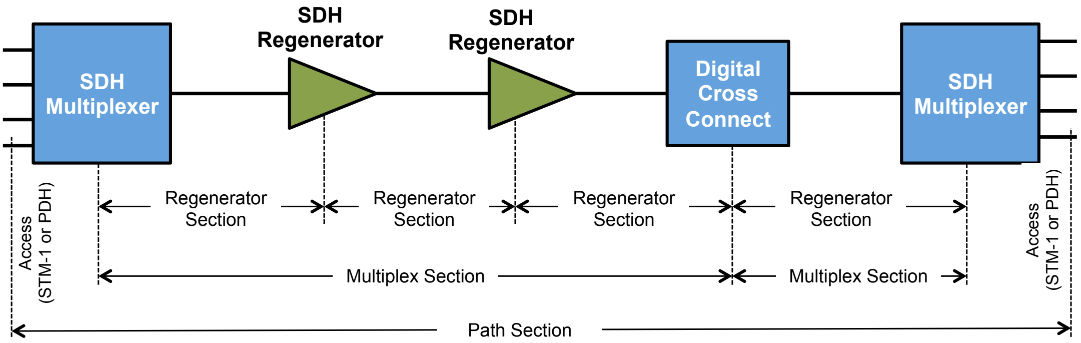


Figure 3.3: Generic overview of SDH devices and sections

SDH networks typically comprise regenerators, multiplexers, add/drop multiplexers (ADM) and digital cross connects (DXC) as depicted in Fig. 3.3. These components operate at different layers of the SDH network. The lowest layer is the physical layer (path connection) at which signals are filled into STM-N frames via terminal multiplexers. These frames are transmitted between add/drop multiplexers and digital cross connects within so-called *multiplexer sections*. At the multiplexing layer certain overhead bytes are used for network managements and monitoring. The virtual containers (VC) are directly accessible to ADMs and DXCs and can be easily extracted. A multiplexer section can be further split into *regenerator sections* by intermediate SDH regenerators. RSOH header bytes are reserved for monitoring signal quality across regenerators. All network components of SDH are using optical technology only for transmission whereas data processing in SDH nodes is done electronically. Hence SDH is an example for a first generation photonic network.

SONET is the American equivalent of SDH and was defined by Telcordia and American National Standards Institute (ANSI) in 1985. SDH and SONET are using the same protocol neutral multiplexing method and frame structure. However, the usable data rates, frame sizes and terminology are different. The base bit rate of SONET is 51.84 Mbit/s and is designated as STS-1 (synchronous transport signal) or OC-1 (optical carrier) if transmitted over an optical fiber. The defined SONET levels increase by multiples of three (OC-3, OC-9, OC-12, . . .) and match the plesiochronous bit rates of PDH. Some bit rates have an equivalent in SDH and can be used as transition between SONET and SDH (see Tab. 3.1). Matching the frame structures of SDH and SONET is quite simple as it was considered in the specification of SDH and only requires the adjustment of certain overhead bytes.

SONET Optical Carrier level	SONET frame format	SDH frame format	Payload bandwidth $[kbit/s]$	Line rate $[kbit/s]$
OC-1	STS-1	STM-0	50 112	51 840
OC-3	STS-3	STM-1	150 336	155 520
OC-12	STS-12	STM-4	601 344	622 080
OC-24	STS-24	–	1 202 688	1 244 160
OC-48	STS-48	STM-16	2 405 376	2 488 320
OC-192	STS-192	STM-64	9 621 504	9 953 280
OC-768	STS-768	STM-256	38 486 016	39 813 120

Table 3.1: Frame formats and data rates for SDH and SONET

3.1.2 Wavelength-Division Multiplexing (WDM)

Wavelength-Division Multiplexing (WDM) was the next step towards second generation photonic networks. It describes the mechanism of combining multiple optical carriers of different wavelengths onto a single fiber. In the first experiments in 1978 only two wavelengths were multiplexed but today commercially available WDM systems can handle up to 160 wavelengths. The term wavelength-division multiplexing is used when speaking of optical signals, while frequency-division multiplexing describes the same technical method for radio signals.

In a WDM network dedicated lasers need to emit a constant wavelength for each channel. A multiplexer combines these channels and a wideband optical amplifier (e.g. erbium doped fiber amplifier) is used to increase the power level of the channels before fiber transmission. At the receiver node optical filters are utilized to split the spectrum according to the wavelength grid spacing. This is necessary because optical receivers (i.e. photo diodes) are typically wideband devices in contrast to lasers diodes. Filtering can be realized by Fabry-Perot interferometers in the form of thin-film-coated optical glass – so called *elatons*. Because the wavelength channels are completely isolated, an independent data format and bit rate can be used for each channel. In WDM networks bi-directional communication can be facilitated either by using a different wavelength on the same fiber or a separate fiber for the backwards direction. The spacing and number of wavelength channels of a WDM system is categorized by Coarse WDM (CWDM) and Dense WDM (DWDM) standards (see Figure 3.4).

Course WDM (CWDM) was defined in 2003 as ITU-T recommendation G.694.2 [59] and specifies a channel spacing of 20 nm between 1271 and 1611 nm. Before this standard was introduced

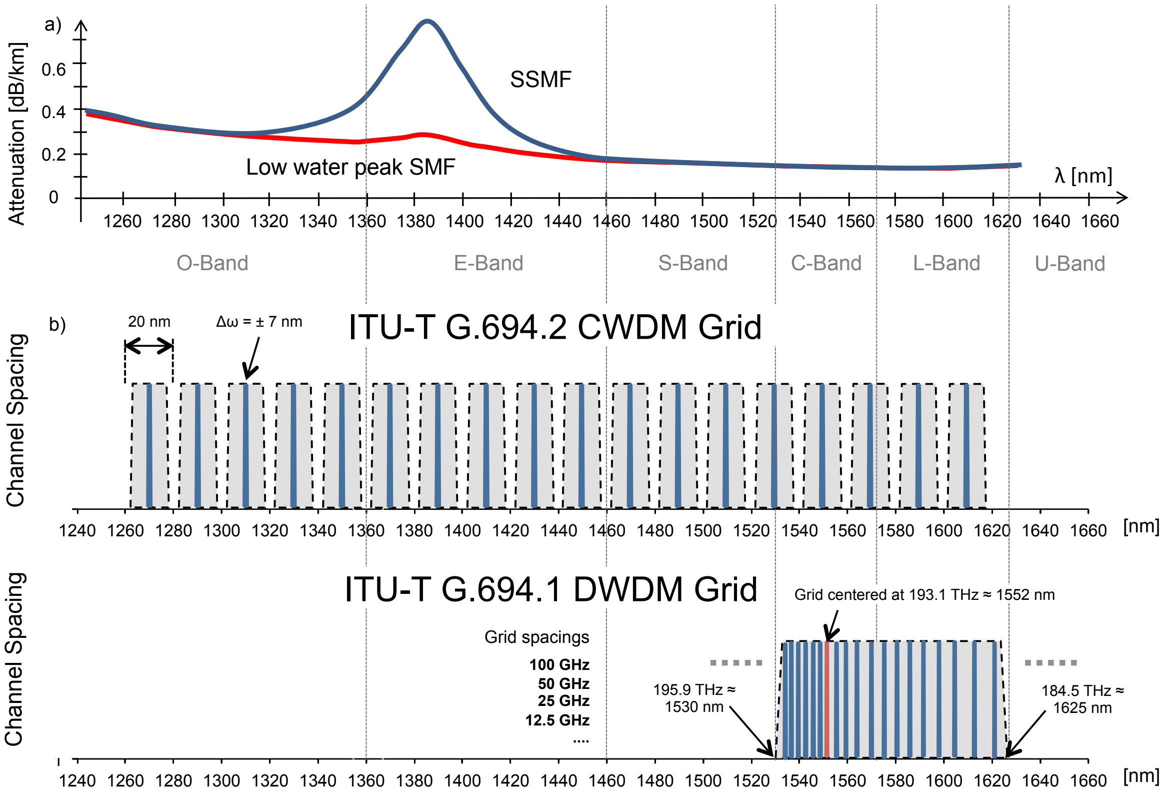


Figure 3.4: a) Attenuation of SMF-28 and low waterpeak fibers, b) wavelength grid for CWDM, c) wavelength grid for DWDM

the term CWDM was used for multiplexing channels from the O-band and the C-band. The channel spacing of 20 nm permits the use of uncooled laser sources and inexpensive optical filters. The maximum allowed center wavelength variance is ±7 nm which implies a guard band of 12 nm between adjacent channels. Due to a higher attenuation of standard single mode fibers (e.g. SMF-28) some CWDM channels falling in the region 1270 – 1470 nm are unusable. The attenuation peak is reduced to a bare minimum when newer *low waterpeak fibers*) are used. First generation optical networks use CWDM for the transport between nodes. The problem with CWDM is that no existing optical amplifiers cover the entire spectral reach of all CWDM channels. Hence, the CWDM channels need to be terminated at any intermediate nodes (see SONET regenerators in Fig. 3.3) and converted to electrical signals before being retransmitted to the next node.

The specification of Dense WDM (DWDM) [60] fixes the center of the wavelength grid to the reference frequency of 193.1 THz (i.e. the center of the C-Band). On each side of this center frequency optical carriers can be multiplexed with a spectral spacing of 100 GHz, 50 GHz, 25 GHz or even 12.5 GHz. The tight grid spacing demands for temperature-stabilized laser sources and narrow optical filters. In order to avoid the need for O/E/O converters the C-Band and S-Band is used. Erbium doped fiber amplifiers (EDFAs) enable optical amplification of all wavelengths channels in the C-Band without terminating the lightpath. An active gain medium is pumped with an external pump laser which in turn amplifies incident light by transferring energy from exited erbium ions. Raman amplification can be applied for channels in the S-Band.

With the evolution of second generation photonic networks more functionality is moved into WDM networks. The exclusive use of wavelength multiplexing for data transport between nodes is enhanced with the possibility to optically extract and add channels of different wavelength or switch channels to other fibers. These functions are implemented in the optical domain by components such as optical add-drop-multiplexers (OADM), optical cross-connects (OXC), wavelength converters, tunable filters, splitters and combiners. These advances in WDM networks pave the way for a fast transmission network which is independent of data format, modulation and bit-rate.

An architectural framework for management and monitoring of such second generation photonic networks is introduced in the next section.

3.1.3 Optical Transport Network (OTN)

ITU-T G.872 specifies the Optical Transport Network (OTN) architecture to transport client signals in the optical domain. OTN defines logical interfaces of optical network elements to facilitate transport, multiplexing, switching, management, supervision and survivability of optical channels. OTN natively supports the transport of client signal formats SDH/SONET, Internet Protocol (IP), Frame Relay, Fiber Channel (FC), Gigabit Ethernet (GbE), ATM and many more. End-to-End transparency for client signals is maintained in terms of data format (bit-transparency), timing and delay. ITU-T G.709 defines a digital frame format called *digital wrapper* to carry all kinds of client signals including overhead information for OTN functions.

In contrast to SDH, the frame format of OTN remains the same regardless of the data rate. As the data rate increases the frame period reduces, prohibiting the use of SONET/SDH switch fabrics which assume constant frame periods. The switching scalability of OTN is a main feature compared to a pure wavelength multiplexing approach. Services of certain bit rates can be multiplexed in a digital wrapper regardless of the line rate. Thus, OTN enables all-optical networking by combining the idea of multiplexing various tributary signals into containers (SDH) with wavelength multiplexing techniques (WDM). Additionally, OTN adds a stronger forward error correction (FEC) compared to SDH. The Reed-Solomon 16 byte-interleaved FEC scheme has been proved to be effective in systems limited by optical signal-to-noise ratio (OSNR) and dispersion. The FEC uses 4×256 byte of check information per frame which can result in up to 6.2 dB improvement is OSNR.

3.2 Access Networks

The term *access network* is specified by ITU-T G.902 as the set of entities which together enable the provisioning of telecommunication services between a service node interface (SNI) and each of the associated user-network interfaces (UNI) [61]. Here, we consider both Point-to-Point (P-t-P) and Point-to-Multipoint (P-t-MP) optical access options and analyze their suitability for integrating quantum key distribution.

Optical access networks are generally named Fiber-To-The-x (FTTx). The different options for FTTx differ basically in how near to the subscriber the fiber reaches (Fig. 3.5), but also in the multiplexing technique applied and the wavelength bands used to carry the up- and downstream signals. Typical cases are: the Fiber-To-The-Home (FTTH), which means that the optical signals reach the end subscribers equipment situated in the subscribers home. Other examples are Fiber-To-The-Building (FTTB), Fiber-To-The-Curb (FTTC) and Fiber-To-The-Node (FTTN), where the final section into the subscribers home is realized by copper or radio.

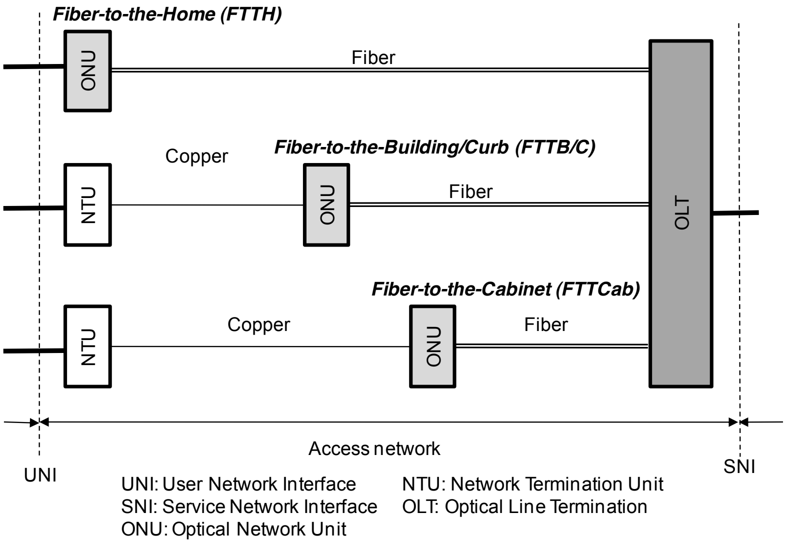

Fiber-to-the-Home (FTTH)
ONU
Fiber
NTU
Copper
Fiber-to-the-Building/Curb (FTTB/C)
ONU
Fiber
OLT
Fiber-to-the-Cabinet (FTTCab)
NTU
Copper
ONU
Fiber
Access network
UNI
SNI
UNI: User Network Interface
SNI: Service Network Interface
ONU: Optical Network Unit
NTU: Network Termination Unit
OLT: Optical Line Termination

Figure 3.5: Different types of Fiber-To-The-x (FTTx) architectures (taken from [62])

In the case of FTTH a direct optical connection exists between the provider's central office (CO) and the subscriber. In access network descriptions the term optical line terminal (OLT) represents the connection endpoint at the CO, whereas the optical network unit (ONU) describes the module at the subscriber's home. Downstream (DS, from OLT to ONU) and upstream (US, from ONU to OLT) signals can be transmitted over the same fiber or over two separate fibers. The usual network topology is either of ring or tree type or a combination of those two.

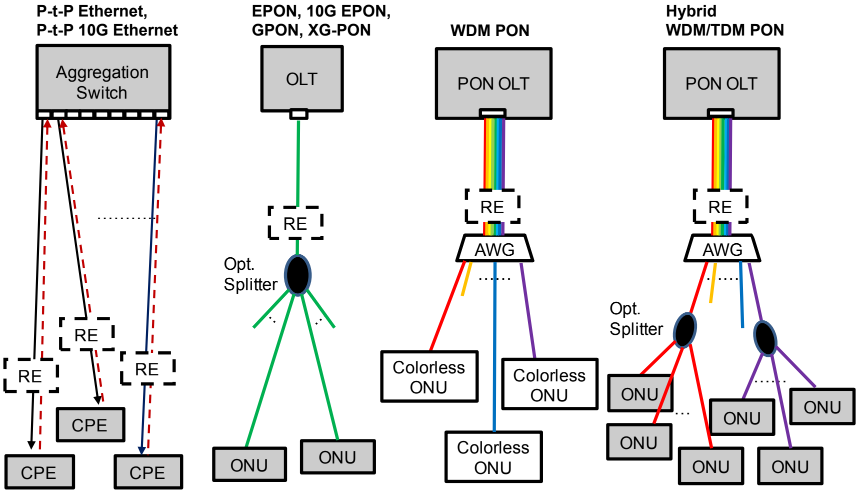


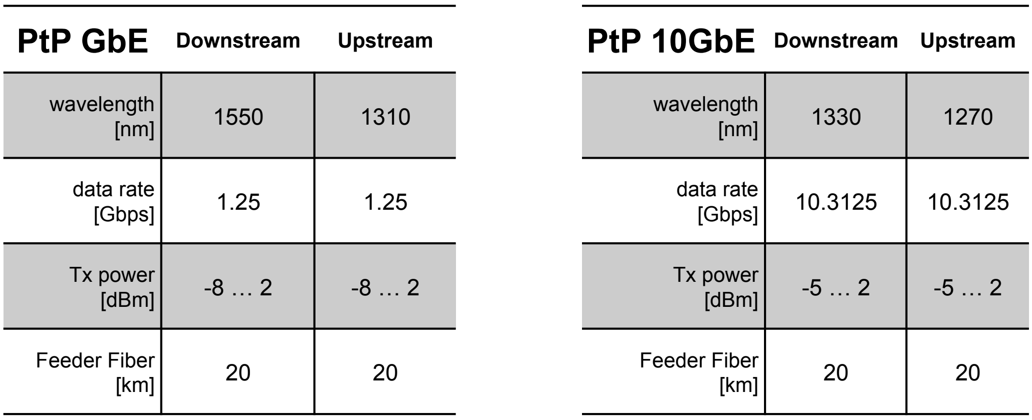
Figure 3.6: Schematic overview of passive potical networks (PONs) (taken from [63]). CPE: Customer Premises Equipment, AWG: Arrayed waveguide grating, OLT: Optical Line Terminal, ONU: Optical network unit, RE: optional range extender (i.e. optical amplifier)

In Fig. 3.6 generic structures of the considered access networks are depicted. The option on the left shows a Point-to-Point (P-t-P) passive optical network which uses a dedicated fiber for each end-user interconnection. The other options have a tree like topology with an intermediate component (remote node) which acts as the root of a subsequent optical distribution network (ODN). These access networks are commonly referred to as Point-to-Multipoint (P-t-MP) passive optical networks and can be distinguished by the multiplexing technique, the wavelength plan and the implementation of remote node (e.g. optical splitter, AWG, . . .).

3.2.1 Point-to-Point access networks

The most trivial way to deploy optical fibers in local access networks is to use point-to-point (P-t-P) topology. In P-t-P networks a dedicated fiber interconnects each end-user with the central office (CO). This fiber can be utilized for both upstream and downstream channel in order to provide bi-directional communication. Two different wavelengths are assigned to upstream and downstream respectively providing a so-called *diplex* transmission scheme. In contrast, *duplex* transmission describes the setup where only a single wavelength is used for both directions. With P-t-P networks the link capacity can be completely consumed by the end-user which is not possible in P-t-MP networks. Additionally, a fiber connection can be individually upgraded without affecting other users.

IEEE 802.3ah *Ethernet in the first mile (EFM)* [64] specifies the use of Ethernet frames as communication protocol between OLT and ONU. The aim of EFM was to avoid the non-native transport of Ethernet frames in Asynchronous Transfer Mode (ATM) cells. It defines new Ethernet physical layer (PHY) interfaces for transmitting Ethernet frames over dedicated long wavelength optical fibers (i.e. P-t-P GbE) as well as P-t-MP passive optical networks (i.e. EPON). 100BASE-LX10 and 100BASE-BX10 provide P-t-P 100 Mbit/s Ethernet links up to 10 km via two fibers (LX10) or a single fiber (BX10). Similarly, 1000BASE-BX10 and 1000BASE-BX10 provide P-t-P 1000 Mbit/s Ethernet links up to 10 km over two/one fiber(s). Here, the PHY interface 1000BASE-BX10 is considered which specifies the wavelengths for upstream and downstream and the allowed range of transmission powers for each direction shown in Fig. 3.7. Further, the symmetric 10 Gbit/s Ethernet interface 10GBASE-PR is examined, which is downwards compatible to 1000BASE-BX10.



PtP GbE	Downstream	Upstream
wavelength [nm]	1550	1310
data rate [Gbps]	1.25	1.25
Tx power [dBm]	-8 … 2	-8 … 2
Feeder Fiber [km]	20	20

(a)

PtP 10GbE	Downstream	Upstream
wavelength [nm]	1330	1270
data rate [Gbps]	10.3125	10.3125
Tx power [dBm]	-5 … 2	-5 … 2
Feeder Fiber [km]	20	20

(b)

Figure 3.7: Specification for a) PtP 1G Ethernet (1000BASE-BX10) and b) PtP 10G Ethernet (10GBASE-PR)

Point-to-point (P-t-P) access networks can potentially accommodate a quantum channel since only upstream and downstream channels of a single user occupy the fiber. Hence, the overall power spectrum is low and non-linear effects may not cause significant background noise in bands outside of US and DS wavelengths. In figure 3.8 an option for integration of a quantum channel is depicted for *P-t-P Gigabit Ethernet* and *P-t-P 10Gigabit Ethernet*. The suggestion envisions one QKD transmitter for each fiber. The quantum channels are wavelength multiplexed with the corresponding downstream signals from the OLT. Multiplexing can be done with inexpensive CWDM waveband couplers given a sufficient wavelength spacing between quantum and downstream channel.

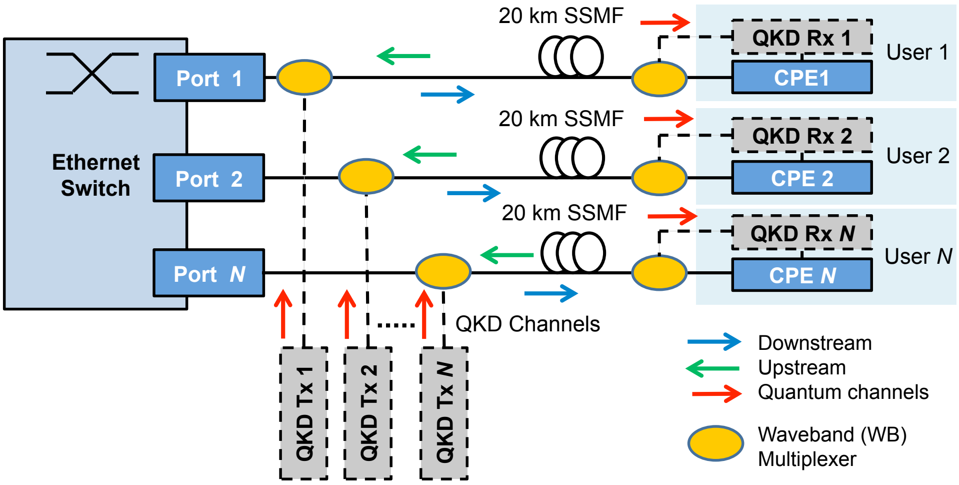


Figure 3.8: QKD Integration in PtP Active Optical Ethernet (1G Ethernet and 10G Ethernet)

3.2.2 Point-to-Multipoint access networks

P-t-P passive optical networks require a significant outside plant fiber deployment which is in most cases cost prohibitive. Therefore the trend is to multiplex individual subscriber channels onto a common feeder fiber which connects the OLT with the *remote node* placed close to the subscribers homes. This scenario is referred to as Point-to-Multipoint (P-t-MP) and entails a broadcast of all subscriber channels from the OLT. When a common feeder fiber is used to distribute downstream channels to subscribers some kind of multiplexing needs to be applied.

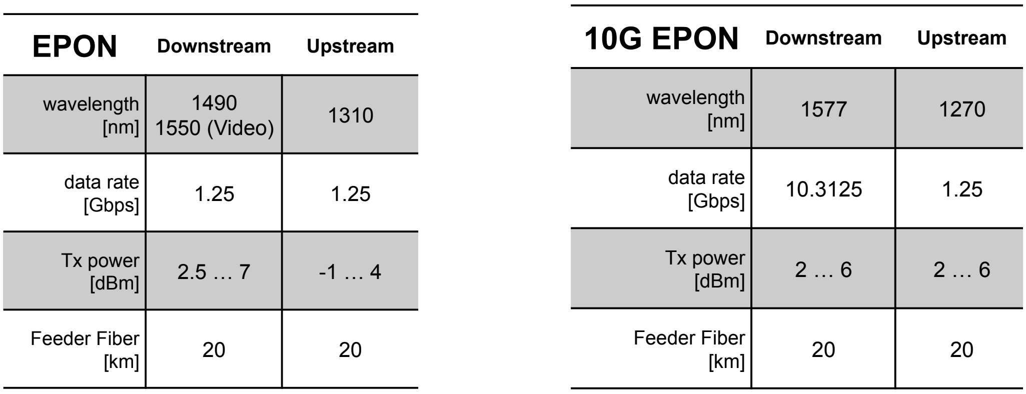
When a higher transmission distance is required a range extender (i.e. optical amplifier) can be added in the remote node. Such extended reach passive optical networks (ER-PONs) with high optical loss budget typically follow the approach of dedicating a dual-feeder to avoid impairments caused by the strong downstream signals and affecting the weak upstream signal, while laying out the drop segment of the optical distribution network using a single-feeder design in order to preserve a simple and low-cost optical network terminal (OLT) with single fiber pigtail. The fiber between remote node and ONU is called *drop fiber* and is typically much shorter than the fiber between OLT and remote node (*feeder fiber*).

The individual downstream and upstream channels of P-t-MP access networks need to be multiplexed on the feeder fiber. PONs implement the technique of time-division multiple access (TDMA) or wavelength-division multiple access (WDMA). Also a hybrid version of TDMA/WDMA is suggested in a following subsection. In any case the optical distribution network (ODN) including fiber plant and remote node is a passive structure, hence the name *passive optical network (PON)*.

3.2.2.1 Time-division multiplexed passive optical networks

In a time-division multiple access scheme a single wavelength is used for downstream and upstream channel respectively. The remote node contains a passive optical splitter which splits the power of the downstream channel by a certain ratio (*splitting ratio*). Typical splitting ratios are 1:16 or 1:32 which represents a distribution among 16 or 32 ONUs. Higher splitting ratios result in higher insertion loss and require highly sensitive receivers and low-loss optical components. The received downstream signal is the same across all ONUs but a distinct identifier is assigned to each ONU. All frames include an ONU identifier to uniquely determine the target ONU. The upstream direction can be seen as a many-to-one connection where the upstream channels of all ONUs are combined by the optical splitter back onto the feeder fiber. Each ONU has an individual timeslot within it is allowed to burst upstream traffic.

The data signals can be encoded and multiplexed in various ways. Equally to P-t-P Gigabit Ethernet, 1G EPON and 10G EPON are using Ethernet frames. IEEE 802.3ah and IEEE 802.3av define wavelength allocation, data format and data rates of 1G EPON and 10G EPON. The specification of the Ethernet physical layer (PHY) for P-t-MP differs in major parts from the P-t-P PHY, due to the additional *multipoint media access control* layer. The line coding of 1G EPON utilizes a 8B/10B code as forward error correction whereas 10G EPON specifies the mandatory use of a 64B/66B coding scheme. Figure 3.9 summarizes the wavelengths, maximum transmission powers and reaches for both 1G EPON [64] and 10G EPON [65].



EPON	Downstream	Upstream
wavelength [nm]	1490 1550 (Video)	1310
data rate [Gbps]	1.25	1.25
Tx power [dBm]	2.5 … 7	-1 … 4
Feeder Fiber [km]	20	20

(a)

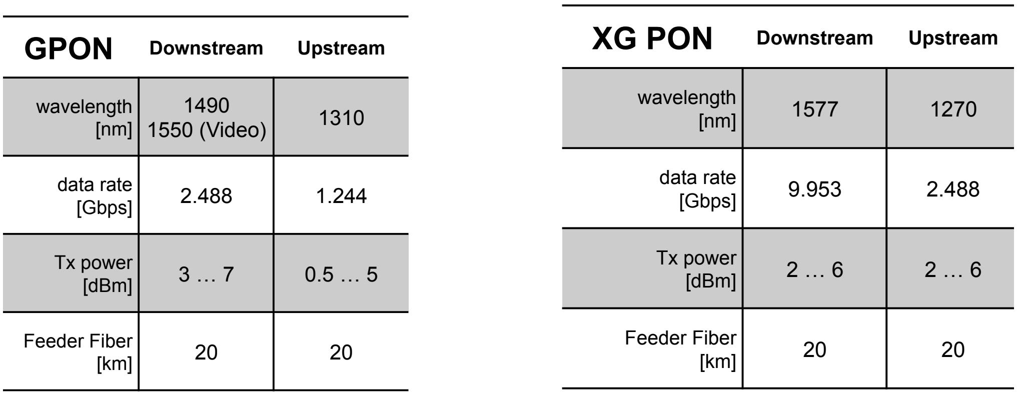
10G EPON	Downstream	Upstream
wavelength [nm]	1577	1270
data rate [Gbps]	10.3125	1.25
Tx power [dBm]	2 … 6	2 … 6
Feeder Fiber [km]	20	20

(b)

Figure 3.9: Specification for a) 1G EPON and b) 10G EPON

Another frame structure is used by GPON which is defined by ITU-T G.984. The possible data rates are fixed to multiples of 8 kbit/s with a maximum achievable data rate of 1244.16 Mbit/s for upstream and 2488.32 Mbit/s for downstream. The multiplexing mechanism of GPON is facilitated by *GPON encapsulation method (GEM)*. An identifier scheme similar to EPON is used to tag frames for a specific ONU. GPON standardizes a power-leveling mechanism which allows the OLT to control the received upstream channel powers. The ONUs are dynamically instructed to level their transmitter power according to their path loss to the OLT. The allowed transmitter powers, wavelength assignments and data rates for GPON [66] and XG PON [61] is outlined in Figure 3.10.

Figure 3.11 depicts an option for integrating a quantum channel in TDMA PONs of the types EPON, GPON, 10G-EPON and XG-PON. Depending on the applied splitting ratio, a number of



GPON	Downstream	Upstream
wavelength [nm]	1490 1550 (Video)	1310
data rate [Gbps]	2.488	1.244
Tx power [dBm]	3 … 7	0.5 … 5
Feeder Fiber [km]	20	20

(a)

XG PON	Downstream	Upstream
wavelength [nm]	1577	1270
data rate [Gbps]	9.953	2.488
Tx power [dBm]	2 … 6	2 … 6
Feeder Fiber [km]	20	20

(b)

Figure 3.10: Specification for a) GPON and b) XG PON

distinct QKD channels are wavelength multiplexed using a DWDM multiplexer. Subsequently a CWDM waveband coupler is used to combine the QKD wavelengths with the downstream direction. The high transmission loss introduced by the optical splitter would severely impair quantum signals thus the splitter needs to be bypassed. A wavelength coupler extracts the QKD wavelengths before a DWDM demultiplexer extracts the individual quantum channels for each ONU. For each drop fiber the output of the optical splitter is recombined with a single quantum channel. Finally, the quantum signal is obtained by a CWDM waveband coupler at the ONU.

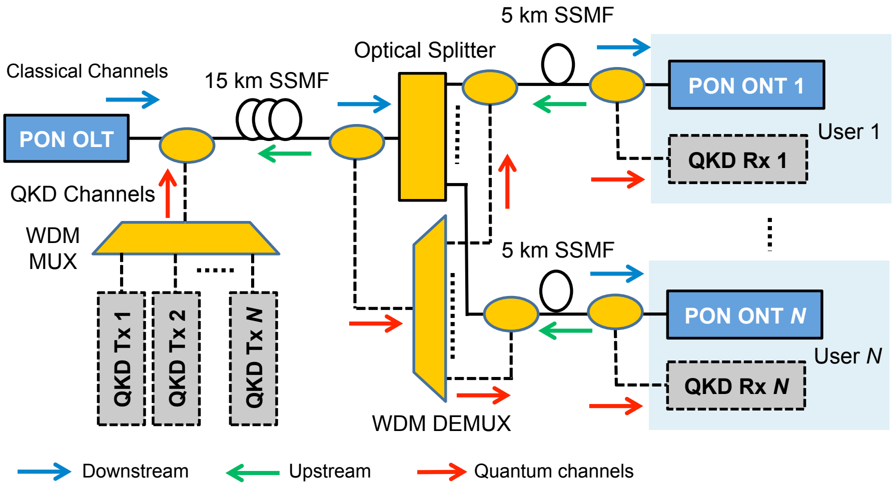
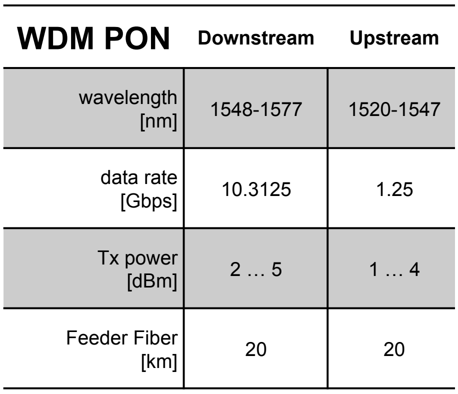


Figure 3.11: QKD Integration in EPON, GPON, 10G-EPON and XG-PON

3.2.2.2 Wavelength-division multiplexed passive optical networks

The usage of wavelength-division multiplexing in PONs allows to distribute the available fiber bandwidth more efficiently. Since WDM PON and WDM/TDM PON are not standardized yet, we assume for these two options the use of arrayed waveguide gratings (AWGs) operational in the C-band as available today. The confinement to the C-band facilitates the use of standard DWDM certified transceiver technology and EDFAs for all-optical amplification. For the envisioned WDM PON option the downstream and upstream encompass 32 channels each with a spacing of 100

GHz. The upstream wavelengths are assigned between 1520-1547 nm, while the downstream is between 1548-1577 (see Fig. 3.12).



WDM PON	Downstream	Upstream
wavelength [nm]	1548-1577	1520-1547
data rate [Gbps]	10.3125	1.25
Tx power [dBm]	2 … 5	1 … 4
Feeder Fiber [km]	20	20

Figure 3.12: Specification for WDM PONs and hybrid WDM/TDM PONs

Hybrid wavelength-division multiplexing and time-division multiplexing (WDM/TDM) PON is envisioned as wavelength-stacked 10 Gbps TDM-PON for the second phase of the next-generation PON evolution (NG-PON2). The transmitter powers and wavelength allocations remain the same as for WDM PON (see Fig. 3.12).

The integration of a QKD system into WDM PONs (Fig. 3.13) has the exact same structure as in TDM PONs. Quantum channels can not be multiplexed by time because of the critical synchronisation and after pulsing effects of single photon detectors. Therefore, the DWDM multiplexed quantum channels of the TDM PON scenario is also valid for WDM PONs. The arrayed waveguide grating (AWG) needs to be bypassed because of the high path loss compared to a DWDM demultiplexer. CWDM waveband couplers can still be used to extract and combine classical and quantum signals.

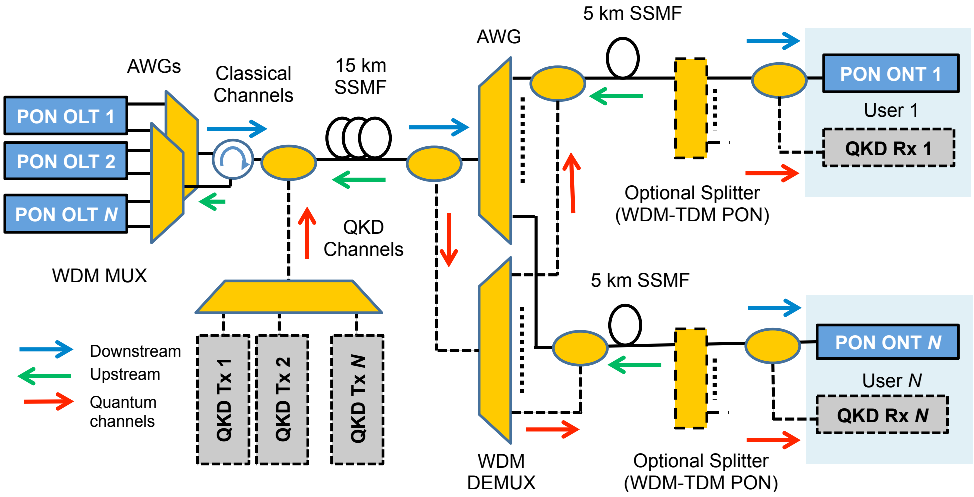


Figure 3.13: QKD Integration in WDM PON and WDM-TDM PON

3.2.3 Waveband allocation of FTTH solutions

For QKD integration in optical access networks it would be desirable that all envisioned scenarios utilize the same QKD wavelength assignment. Fig. 3.14 summarizes the wavelength plans of all FTTH options and additionally shows the attenuation curve of standard single-mode fiber. The marked wavelength regions (Band 1 - Band 6) are not used for classical communications and can thus be potentially used for QKD. Note that Band 4 can only be considered when using the low water peak fiber. The simulations of background noise in section 5 will reveal which bands are applicable for the considered FTTH options.

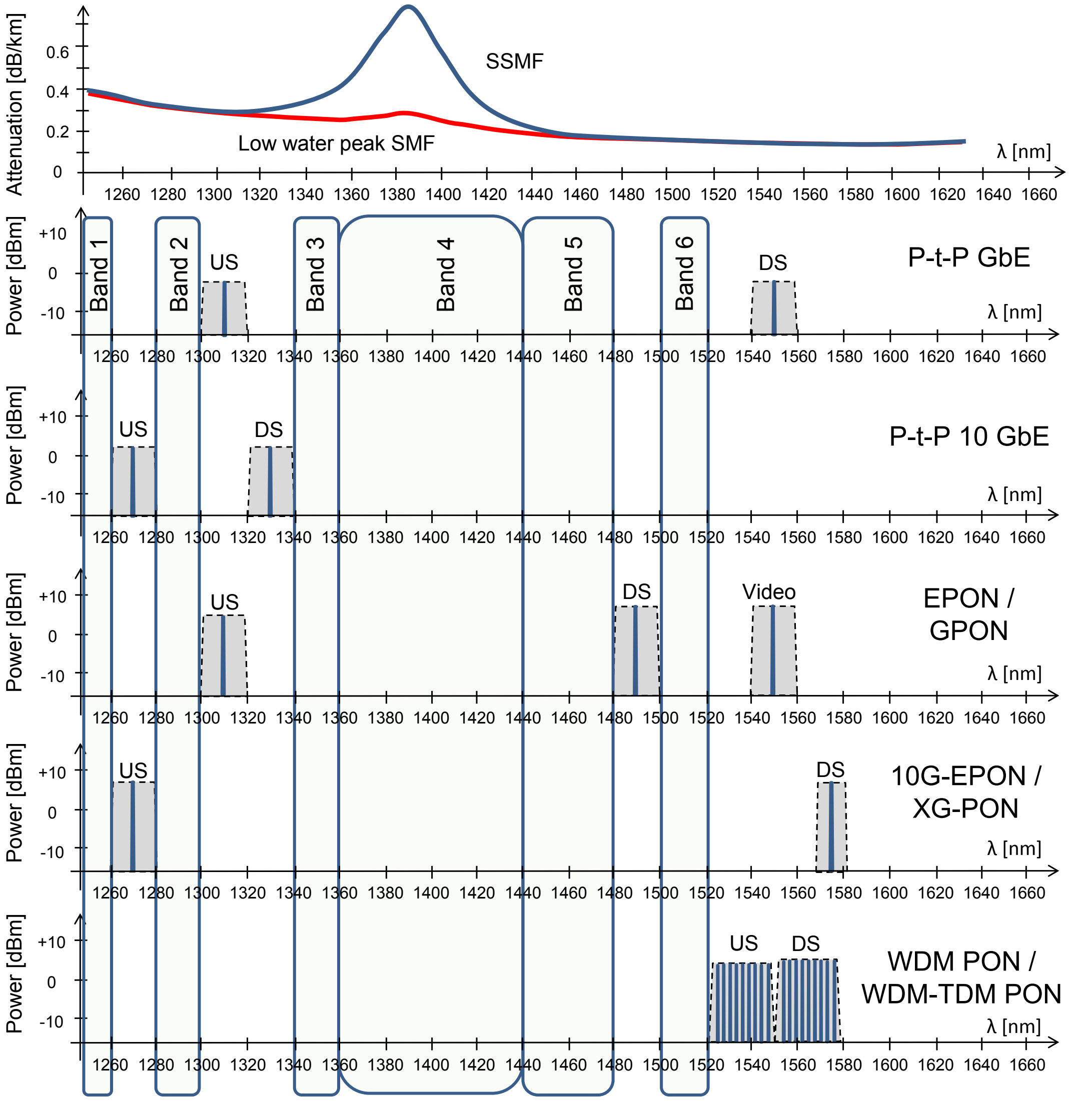


Figure 3.14: Attenuation of optical fiber and wavelength plan for the considered optical access options.

4 Simulation Setup

The authors of recent experiments that consider QKD co-existence with background traffic in commercial WDM networks are tweaking system parameters such as launch power and channel count in order to achieve successful key distribution. This work investigates the compatibility of QKD to optically transparent metro and access networks as depicted in Fig. 4.1a that are operated according to **typical standards**. The following remarks assume typical distances (20 km to 60 km), signal power levels (-8 dBm to 1 dBm) and channel count (40 channels) in metro and access networks. The maximal span length of 60 km is too short for long-haul links, but suitable for implementing QKD in metropolitan area networks.

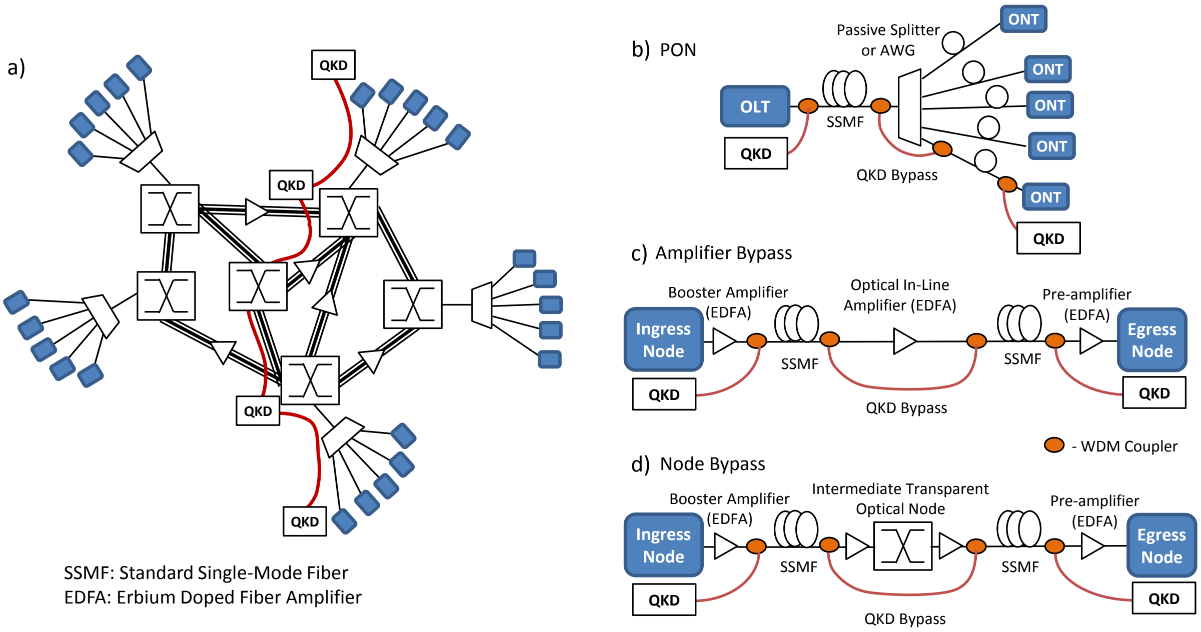


Figure 4.1: Integration of QKD in transparent optical networks: a) generic representation of a QKD path in metro-access networks, b) QKD in passive optical access networks (PON), and QKD bypass for c) an in-line amplifier and d) a transparent node

The quantum information is encoded on quantum signals with a resolution of only one photon corresponding to pulse energy of 1.28×10^{-19} J at 1550 nm. When these weak quantum signals traverse optical fibers, amplifiers and switches both, active and passive components within an optically transparent node contribute to an increase in either background noise or attenuation, which can severely impair the quantum signal.

4.1 Simulation Software

In order to analyse the impact of non-linear effects (such as amplified spontaneous emission (ASE) noise, attenuation, crosstalk and scattering effects) on the quantum channel, simulations of realistic network configurations were completed using the numerical simulation program *VPItransmissionMaker^{TM} 8.5* [67]. A library of ready-to-use models for optical components was utilized to layout the network topologies depicted in Fig. 4.1.

VPItransmissionMaker is a "Photonic Design Automation" (PDA) software package that can be used to engineer complex photonic networks and products. Just as "Electronic Design Automation" tools in the semiconductor and electronics industry, this tool captures design rules and strategies electronically in order to streamline processes from RD to technical sales and marketing. Furthermore next-generation technology can be evaluated within existing system designs before being commercially available. Realistic simulations of optical fibers and transport network designs can be conducted by importing physical parameters of vendor components.

In the next sections practical aspects of working with *VPItransmissionMaker* are discussed in general as well as the consequences for the examined systems.

4.1.1 Signal Representations

As PDA tools support design tools for various scopes – such as photonic devices, components, systems and networks – the programs offers different signal representations for different levels of abstraction. In *VPItransmissionMaker* signals are represented by samples. Data exchange between various simulation modules can occur on a sample-by-sample basis or by sending blocks of samples. Additionally the parameterized mode can be used to model the most important signal characteristics approximately.

Sample Mode

When components are spaced very closely and the delay between the modules is much shorter than a block length, sample mode should be used. Samples are exchanged individually between modules allowing to simulate the full dynamics of a system. Accurate results in the time and frequency domain can be achieved for scenarios where modules must communicate rapidly in order to fully simulate their joint behavior. The sample mode representation is important for simulation of complex photonic devices and circuits such as regenerators, wavelength converters, stabilized and tunable lasers, and systems with feedback. The drawback of sample mode is the high computational effort which results in long simulation times. For the simulation of WDM systems and high bandwidth links this mode is unusable, hence it was avoided during the simulations.

Parameterized Signals

In contrast to sample mode signals, Parameterized Signals (PS) can be utilized to describe signals based on incomplete information about the channel. The representation keeps track of signal parameters such as the central frequency, the average signal power, the polarization state, accumulated dispersion, accumulated differential group delay, accumulated self-phase modulation, total length of fibers the signal has passed, accumulated timing jitter information, and an average pulse shape. However, the waveform of the pulse stream can not be retained for this signal type. The advantages of parameterized signals are the high simulation speed and the scalability of complex simulations with many carrier frequencies – such as WDM systems.

Block Mode

The block mode representation combines the power of both sample mode and parameterized signals by using the duality between representations in the time and frequency domain. In order to select the most efficient model in every case, *VPItransmissionMaker* exchanges the signal characteristics in blocks of samples according to a long time window. Different representations can be used within these blocks.

Most generally the entire signal can be simulated at once in a *Single Frequency Band (SFB)*. Since the bandwidth of a signal can be very large (especially in WDM applications with Raman noise) this approach is very memory and time intensive. On could split the spectrum of the signal into *Multiple Frequency Bands (MFB)* switch to the. While this approach lowers the stress on hardware resources, effects such as four-wave mixing between the individual frequency bands can not be modelled any more. This mode was used for simulating the **classical data channels**.

Distortions and Noise Bins

An elegant way to simulate large optical systems with wide frequency bandwidths is to store the signal in a *parameterized mode* while capturing the magnitude of non-linear effects in separate representations. Parasitic signals created by four-wave mixing (FWM), Rayleigh and Brillouin scattering are represented as *Distortions* which have the same data-structure as parameterized signals. *Noise Bins* are used to characterize the noise power density of the signal. In a simulation the user has to specify spectral attributes of the noise bins such as bandwidth of each noise bin and the aggregate bandwidth in which noise power density shall be calculated. A large aggregate bandwidth and narrow noise bins increase the calculation time for the simulation.

The properties of the *block mode* make it an obvious choice for the simulation of the **classical data channels** in the examined access and metro technologies. The multiplexed wavelengths of certain access networks are far apart, hence the simulations have to be done across a wide spectral range including both the O-band and the C-band. The **noise bins** provide a convenient way to calculate the background noise spectrum in order to find potential frequency ranges for the quantum channel. For the simulations to be examined the noise bins were configured with a resolution bandwidth of 100 Ghz and the spectral range from 1240 nm to 1660 nm.

4.1.2 Modeling Domains

In *VPItransmissionMaker* simulations can be designed to abstract the problem by a certain degree according to the modeling domain. A modeling domain stands for some kind of simplified assumption. This simplification can either concern the periodicity of signals or the propagation direction.

Aperiodic vs. Periodic Signals

In periodic simulations all signals are expected to be periodic in nature, thus the signal power outside the specified simulation bandwidth is zero. When applying time delays signal parts that are shifted outside of the current simulation time window are being discarded. Memory can be added to the system by running aperiodic simulations where delayed signal parts are stored in memory for insertion in the next time window. Aperiodic simulations can handle both sampled and block mode signals, whereas periodic simulations only accept block mode signals. For the QKD simulations only periodic signals were assumed as any data channel has a constant bit rate.

Unidirectional vs. Bidirectional Propagation

Certain physical effects within optical fibers and other components are known to be bidirectional in nature – e.g. Rayleigh scattering, ASE from EDFA pumping, etc. Simulations of complex components – such as erbium doped fiber amplifiers (EDFA) – or critical non-linearity's in fiber links – such as Rayleigh scattering – prompt for models that consider both propagation directions. In the examined access technologies both upstream and downstream channels use the same optical fiber. These simulations require a bidirectional model of an optical fiber whereas the metropolitan area scenarios (node by-pass, node switching, . . .) are modeled as unidirectional simulations.

4.1.3 Scheduler

The simulation scheduler determines the order by which modules are executed ("fired"). In *VPItransmissionMaker* the scheduler is based on `Ptolemy`. The execution order of the scheduler depends on the operation mode ("simulation domain"). In VPI these domains are the synchronous dataflow domain (SDF), Boolean dataflow domain (BDF), dynamic dataflow domain (DDF) and a domain of so-called higher-order functions (HOF).

Synchronous dataflow domain

In SDF simulations the execution order is statically determined during the start-up phase, thus completely predictable at compile time. All modules are fired periodically by this execution order. When a module is fired, a fixed amount of accumulated signal particles (i.e. samples or blocks) at the input ports is consumed by the module which in turn produces a fixed amount of outgoing signal particles at the output ports. The fact that the firing pattern is determined statically means that data-dependent flow of control between modules is not allowed. This would require the scheduler to operate in the Dynamic dataflow (DDF) or the Boolean dataflow (BDF) domain.

Dynamic dataflow domain

In DDF simulations the scheduler makes no attempt to construct a schedule at compile-time but fires modules one by one as soon as there is enough data to consume. Hence, DDF modules must specify how much data is required at each execution. Since DDF is a superset of the synchronous dataflow (SDF) all SDF modules are runnable in DDF simulations.

Boolean dataflow domain

The Boolean dataflow (BDF) domain combines the strengths of both SDF and DDF. The BDF scheduler tries to construct a compile time schedule by applying a clustering algorithm to the graph. The clusters can take the form of traditional control structures such as `if-then-else` and `do-while`. Within any cluster a static schedule as in SDF will be applied while the DDF approach is used in between clusters. The resulting schedule is *as static as possible* and the ideal choice for the simulations examined.

Higher-order functions

In general a function of higher-order takes another function as argument and returns either a function or a value. In *VPItransmissionMaker* higher-order function (HOF) modules implement such special behaviour. As an example the `Map` modules takes two arguments, a function and a list, and applies this function to each element of the list. The implemented QKD simulations use modules such as `LaserArray, WDM_MUX` in order to define repeating parts of the schematic, for example an array of transmission laser modules with the exact same parameters except for the emission wavelength. The usage of HOF modules simplifies complex schematics by avoiding copy-past error of redundant parts and their parameter values. The input and output ports of HOF modules are usually buses which represent a bundle of optical or electrical signal wires. The concept of buses also helps to keep schematics neatly arranged.

4.2 Modelled Effects

In a co-existence architecture classical data channels are wavelength multiplexed with a quantum channel on the same fiber. These channels introduce background noise in the entire transmission spectrum of the fiber caused by several effects. These fiber-based non-linear effects were analyzed both quantitative and qualitative in order to identify the potential impact on QKD operations.

4.2.1 Attenuation Model

For attenuation calculations a data file (`Attenuation.dat`, bundled with VPI) was used to account for wavelength dependent attenuation of a standard single-mode fiber (SMF-28). This file contains the attenuation values in $\frac{dB}{km}$ for wavelength $1004.3nm$ to $1701.7nm$ in increments of $\approx 1nm$. Around 1510nm the attenuation is 0.19dB/km (Fig 4.2). As attenuation affects the entire spectrum it will harm any QKD system regardless of the QKD wavelength. However the quantum channel has to be placed with care due to higher attenuation outside of standard optical transmission windows. For example the water peak in silica fiber generates high attenuation vales in the range of 1360 nm . . . 1390 nm.

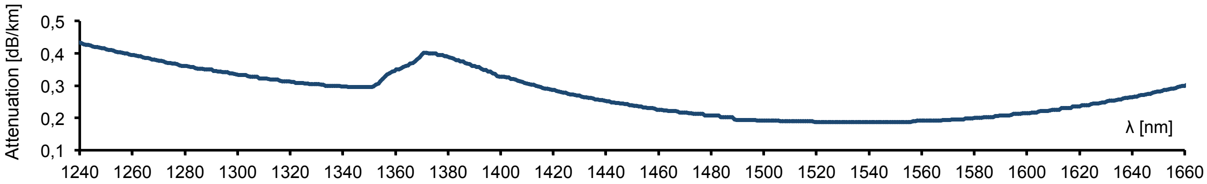
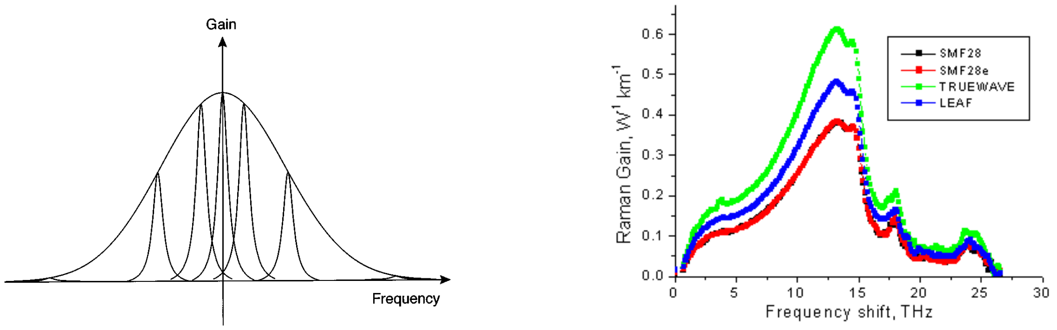


Figure 4.2: Fiber attenuation $[\frac{dB}{km}]$ for standard single-mode fiber (SMF-28) that came bundled with *VPItransmissionMaker*

4.2.2 Raman Scattering

For optical fibers, the Raman gain is usually defined by the Raman gain coefficient $RGC(f_p, \Delta f)$ $[\frac{m}{W}]$. This gain relates the power of the pump f_p and the scattering strength (offset by Δf) and can be experimentally measured [67]. In *VPItransmissionMaker* the Raman gain of an optical fiber is 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 A_{eff} $[m^2]$ of the fiber. Specific Raman gain profiles can be loaded into a fiber model by pointing to an external space-separated data file which contains the applied pump frequency f_p and the measured Raman gain factor across a frequency offset range



(a) **(b)**

Figure 4.3: (a) Example for a convolution of Lorentzians with Gaussians from [68] — (b) SMF-28 NIST reference curve bundled with *VPItransmissionMaker* .

Δf. This data file is independent of fiber dimensions such as A_{eff} and gets re-scaled on-the-fly according to the applied pump wavelength (e.g. WDM channels) and power in the simulation.

The VPI software comes bundled with pre-calculated Raman Gain data files for limited frequency offsets. However, the maximum specified offset of 35 THz was too less for the purpose of this work, thus a new Raman Gain data file had to be calculated. The data points of an extended range envelope curve were calculated in *MatLab* by implementing the intermediate-broadening model from [68]. The authors provide a simple analytic expression which perfectly fits the shape of Raman gain spectrum and Raman response function of silica fibers. Their approach utilizes a convolution of Lorentzians with Gaussians representing multiple vibrational modes (Fig. 4.2(a)). For example, the sharp peak in the Raman spectrum of silica fibers at around $400cm^{-1}$ offset corresponds to the bending of an Si-O-Si dihedral angle. At this offset each Lorentzian peak can be seen as physical representation of a different equilibrium value of the dihedral angle [68]. The expression for the Raman response functions is,

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

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

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

where A_i' is the amplitude of the ith vibrational mode, $\omega_{v,i}$ is the center vibrational frequency for mode i, γ_i and Γ_i are the Lorentzian and Gaussian linewidth for mode i respectively, and $\theta(t)$ is the unit step function with the value 1 for $t \geq 0$ and 0 otherwise. The paper proposes a convolution of 13 modes to match the Raman gain profile and accordingly provides 13 numerical values for A_i', $\omega_{v,i}$, γ_i and Γ_i.

The envelop curve generated from Eq. $s(\omega)$ is only proportional to the Raman gain spectrum and needs to be normalized. The peak of the envelop curve was chosen as reference point and the amplitude was set according to the peak amplitude of the SMF-28 NIST reference curve bundled with *VPItransmissionMaker* (Fig. 4.2(b), $3.5 \times 10^{-4} \frac{1}{Wm}$ at $440cm^{-1}$ at a pump wavelength of 1486nm) and other empirical data from [69]. The data-file with resulting Raman gain spectrum is depicted in Fig.4.4. Test simulations were implemented to match the experimentation setups from papers [55, 58] in order to verify the applicability of the Raman data-file. Only SMF was evaluated during the final simulations.

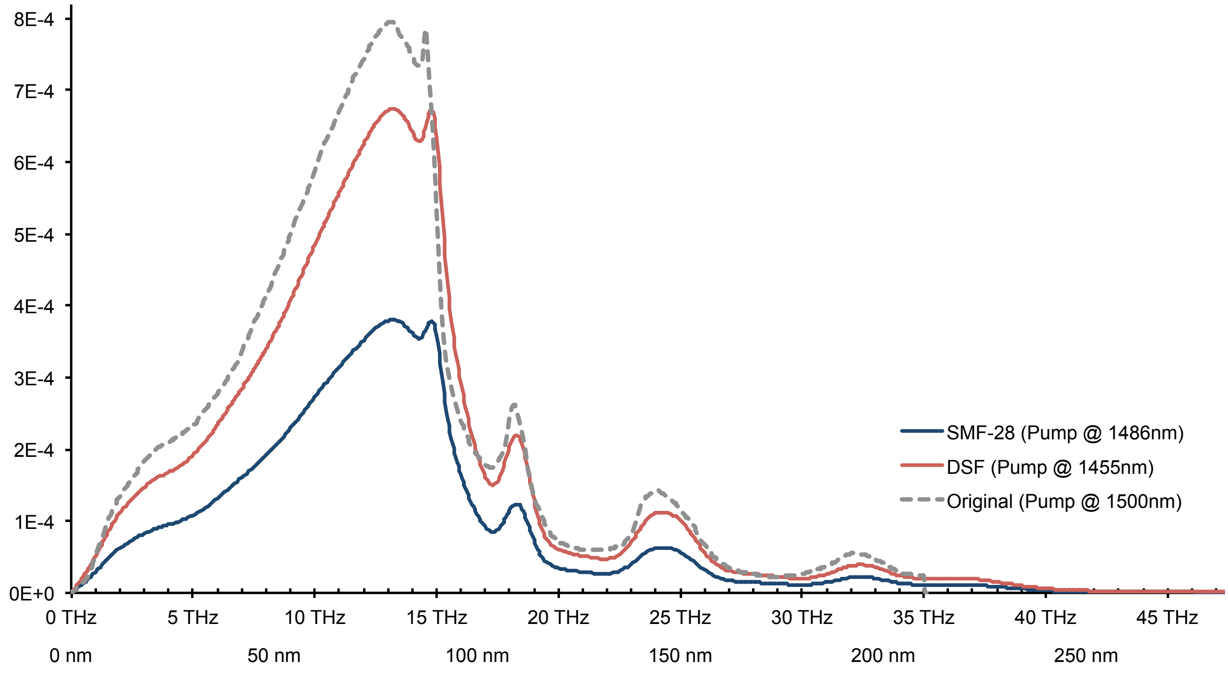


Figure 4.4: Raman gain factor [$\frac{1}{Wm}$] for standard single-mode fiber (SMF-28) and dispersion shifted fiber (DSF). The dotted line is the packaged data file that comes with *VPItransmissionMaker* .

4.2.3 Brillouin and Rayleigh scattering

Both Brillouin scattering and Rayleigh scattering are considered in scenarios with bi-directional communication where noise generated in backward direction matters. The module `UniversalFiberFwd` lacks the ability to simulate these effects, hence it was only used for the uni-directional simulations. Brillouin scattering occurs only above a high power threshold, therefore only WDM carrier frequencies contribute to the effect. However the Self-Brillouin-Scattering (SBS) frequency shift of 11 GHz does not affects adjacent a WDM grid of 50 or 100 GHz. Rayleigh scattering introduces backscattered noise photons of the same frequency as the incident light (no frequency shift). In *VPItransmissionMaker* these noise powers are calculated separately to the signal powers and represented as *distortions*. Just as noise bins store noise powers due to Raman scattering and amplified spontaneous emission (ASE), distortions hold the information about Brillouin and Rayleigh scattering effects. Converters were used to convert distortions to noise bins in order to obtain a consistent representation of the background noise.

4.2.4 Self-/Cross-Phase Modulation and Four-wave Mixing

Self- and Cross-Phase modulation are caused by the intensity dependent refractive index of optical fibers. When the optical signal varies in intensity over time, a phase shift is induced on itself (SPM).

When a co-propagation optical signal induces this phase shift the effect is called Cross-Phase Modulation (XPM). The consequence of SPM and XPM is a broader signal spectrum which in turn results in additional broadening due to chromatic dispersion. Four-wave Mixing happens also due to intensity dependent changes of the refractive index. Similar to Brillouin and Rayleigh scattering, distortion signals represent the additionally generated wavelengths. These were also cross-converted to noise bins prior to background noise measurements.

4.3 Modules and Galaxies

The simulation setup in *VPItransmissionMaker* is essentially a graph of connected modules. A module implements the analytical model for a specific electrical or optical component. Modules need to be connected through `wires` which can be seen as edges of a connected graph. These wires are data-flow channels between the input and output ports of successive modules and have no physical equivalent. A wire has only a single property which describes the scheduler `delay` a signal experiences when passing the fiber. Typically a delay is needed for simulating rings and feedback loops to avoid dead-lock. Other transmission effects that change signal properties have to be modelled in dedicated modules (such as the optical fiber modules `UniversalFiber` and `UniversalFiberFwd`).

The basis for numeric results of non-linear effects in *VPItransmissionMaker* are mathematical models and empirical data files. The mathematical models describe effects analytically and can be parametrized to account for different materials and physical properties (such as the linewidth of imperfect laser diodes). Some other models utilize experimentally measured data and re-scale it to characterize the effect for the actual problem (e.g. the wavelength dependence of Raman scattering and attenuation). The following sections explain how the simulations were setup and which components and parameters (values, data files) were used.

4.3.1 Wiring

The wiring of modules need to obey certain rules. All unused input ports must be terminated by `Null Source` modules, as well as all unused output ports must be terminated by `Ground` modules. In more difficult simulation graphs the direction of data signals through the modules can not be uniquely determined by the scheduler. A `Fork` module or a `BusCreate` module has to be used to provide additional hints. As mentioned before multiple wires can be combined into buses to make wiring easier, especially when connecting modules with many ports (e.g. a WDM-multiplexer with one port per wavelength). In addition to buses the schematic can be further simplified by grouping functional blocks of modules together in a `Galaxy`. Galaxies are stored in external files and can be included by multiple simulations. Within a Galaxy certain module properties can be exposed to the user for easy configuration of complex structures. In the subsequent experimental setups, various galaxies were defined and will be discussed separately in the following sections.

4.3.2 Universal Fiber

The most important module for simulation QKD co-existence schemes is the optical fiber. Fortunately *VPItransmissionMaker* has a very good model for optical fibers called `UniversalFiber`. This module can be configured with many attributes to match realistic optical fibers. Among those attributes are the `Length`, `Temperature`, `CoreArea` as well as parameters which define the magnitude of specific non-linear effects. Parameters such as the characteristic `Raman gain spectrum`, `Attenuation`, `Dispersion` can be found in the literature for many different fiber types [70]. The non-linear effects discussed in section 2.3.1 were considered in the module (see 4.2). In table 4.1 the parameters are listed which were applied to the UniversalFiber modules for all simulations.

Parameter name	Type	Value	Dimension
`Attenuation`	file	`Attenuation.dat (see A.5)`	$^{dB}/_{m}$
`Dispersion`	value	`16e-6`	$^{s}/_{m^2}$
`DispersionSlope`	value	`0.08e3`	$^{s}/_{m^3}$
`RamanGain`	file	`RamanGain-SMF28-NIST.prn (see A.6)`	$^{1}/_{Wm}$
`RamanAdjustmentFactors`	value	`0.5`	–
`RamanFraction`	value	`0.17`	–
`SBSBandwidth`	value	`100e6`	Hz
`SBSStokesShift`	value	`11e9`	Hz
`SBSGain`	value	`4.6e-11`	$^{m}/_{W}$
`FWMThreshold`	value	`-30.0`	dBm
`SBSThresholdFactor`	value	`10`	–
`Temperature`	value	`300`	K
`NonLinearIndex`	value	`2.6e-20`	$^{m^2}/_{W}$
`CoreArea`	value	`72.8e-12`	m^2
`RayleighBackscatterCoefficient`	value	`-80.0`	dB
`NoiseBinResolution`	value	`100e9`	Hz
`NoiseBinStart`	value	`1200e-9`	m
`NoiseBinEnd`	value	`1660e-9`	m

Table 4.1: Parameters of the `UniversalFiber` module used in both Metropolitan and Access Network QKD simulations.

The fiber module is provided in two variants, one for bidirectional optical communication (`UniversalFiber`) and the other for unidirectional (`UniversalFiberFwd`). The uni-directional model is a subset of the full bi-directional model and does not model non-linear effects generating noise in the backward direction, such as Rayleigh scattering and Brillouin scattering. For the QKD simulations in metropolitan area networks the unidirectional module was used, while the bidirectional module was used in passive optical access network simulations to account for upstream and downstream directions. As mentioned before the numerical configuration was to calculate noise bins between 1200 nm and 1660 nm with a resolution of 100 GHz. Subsequent figures are using the more common 12.5 GHz scale with corresponds to a bandwidth of 0.1 nm.

4.3.3 WDM Couplers

For any bypass scenario the WDM coupler is the most important factor when it comes to separating both QKD and classical channels. An insertion loss of 0.5 dB and an isolation of 16 dB was used according to commercially available products. Two band-pass filters were used with center frequencies at 1310 nm + 1550 nm and a bandwidth of 40 nm (Fig. 4.5).

4.3.4 Erbium doped fiber amplifier (EDFA)

Many of the components used in the schematics were taken from the VPI library. However, in the case of metropolitan area networks a realistic model for an erbium doped fiber amplifier (EDFA)

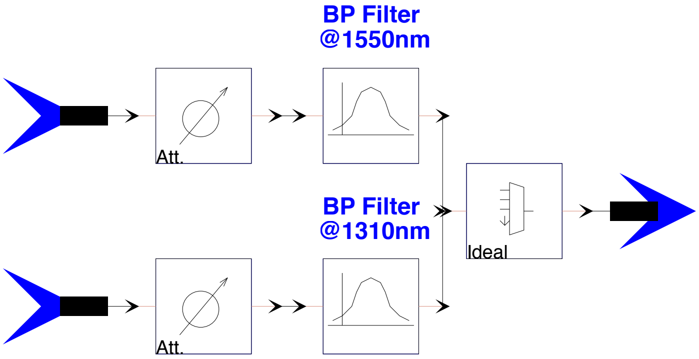


Figure 4.5: Internal structure of the WDM Coupler galaxy

was needed. Fortunately an amplifier demonstration schematic of an inline two-stage EDFA for C-Band is bundled with *VPItransmissionMaker* . This schematic was transformed into a galaxy with configurable parameters for the laser power and doped fiber length of each stage. Fig. 4.6 shows the internal structure and Tab. 4.2 lists the parameters of the EDFA galaxy.

Parameter name	Type	Value	Dimension
`1st Stage Laser Power`	value	`80e-3`	W
`1st Doped Fiber Length`	value	`8`	m
`2nd Stage Laser Power`	value	`25e-3`	W
`2nd Doped Fiber Length`	value	`35`	m

Table 4.2: Parameters of the EDFA galaxy

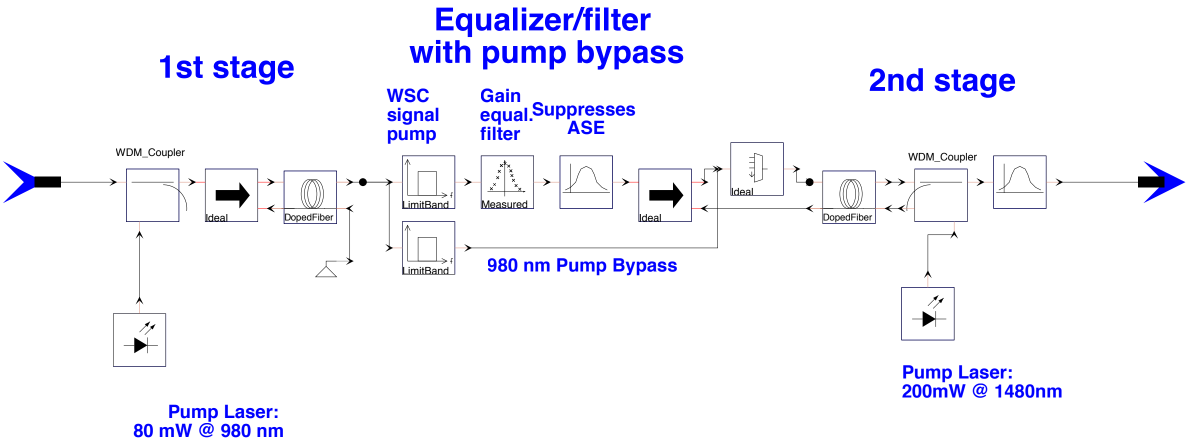


Figure 4.6: Internal structure of the EDFA galaxy

In order to limit the maximum gain a `PowerLimiter` configured to 0 dBm per WDM channel was used after all EDFA galaxies. This was necessary because otherwise the output power would have been unrealistically high due to the short fiber spans (10 - 30 km). However the characteristic gain profile of an EDFA was still visible after the power limiter modules due to limiting the total aggregated power and not just clipping the peaks. Hence the ASE profile of realistic EDFA modules was present and contributed to background noise power.

4.3.5 Optical Cross Connect (OXC)

A model of an optical cross connect (OXC) was used for the simulation of the QKD channel bypass of a transparent optical switch node. The shortest four of the 40 WDM wavelengths are de-multiplexed and passed through two 4x4 switches (which were set to pass-through). Then four frequency converters (which implement a pump laser source) change the frequencies as follows: $1 \rightarrow 4 \ldots 2 \rightarrow 3 \ldots 3 \rightarrow 2 \ldots 4 \rightarrow 1$. Finally the four switched wavelengths are combined with the remaining 36 bypassed wavelengths (Fig. 4.7).

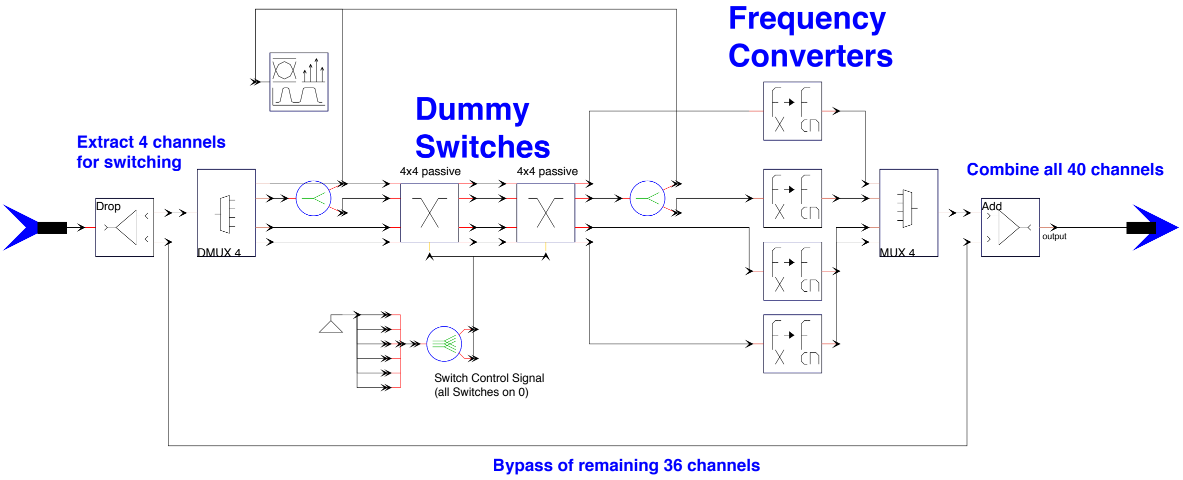

Frequency Converters
Dummy Switches
Extract 4 channels for switching
4x4 passive
4x4 passive
Combine all 40 channels
Drop
DMUX 4
MUX 4
Add
output
Switch Control Signal (all Switches on 0)
Bypass of remaining 36 channels

Figure 4.7: Internal structure of the OXC galaxy

According to [53] the usage of Optical Switches effects the quantum channel mainly because of insertion loss and crosstalk, as well as minimal polarization-dependent dispersion and loss (PMD, PDL). Since the objective of the simulations was to calculate the scalar background noise without any QKD signal present, polarization related impacts were not considered (Tab. 4.3).

Parameter name	Type	Value	Dimension
`InsertionLoss`	value	`0.5`	dB
`CrossTalk`	value	`30`	dB
`PhaseShift`	value	`0`	–
`Bandwidth`	value	`25e9`	Hz

Table 4.3: Parameters of the OXC galaxy

4.4 Schematics

The results presented here consider scenarios for implementing QKD in optically transparent metro and access networks. Both network technologies can be combined to form a fully integrated QKD transport network. In this integrated solution envisions that the central offices (CO) of access network providers are connected to the metropolitan QKD network and represent trusted QKD nodes which terminate QKD links of the core network [46]. Consequently new QKD channels are generated at the CO for quantum key distribution with subscribers. In the following, we assume typical distances (20 km to 60 km), signal power levels (-8 dBm to 1 dBm) and channel count (maximum 40 channels) for metro and access networks.

4.4.1 Metro

First, QKD transmission over core network links was investigated in three different scenarios. Metropolitan area networks commonly make use of the ITU-T grid within the C-band. Optionally, an optical supervisory channel (OSC) can be placed around 1510 nm. Scenario 1 (Fig. 4.8) consisted of a straight connection between a 40 channel DWDM transmitter and a DWDM receiver. The optical fiber span which interconnected the transmitting and receiving node was fixed to a length of 25 km. This length was chosen to match typical metropolitan area network link lengths where no intermediate amplification takes place. Additionally the effect of Raman scattering (see 2.3.1) is greatest around 20 - 25 km. A sweep was performed to change the laser power between 1 dBm and -8 dBm per channel. The module `UniversalFiberFwd` was used to model the optical fiber (see 4.3.2).

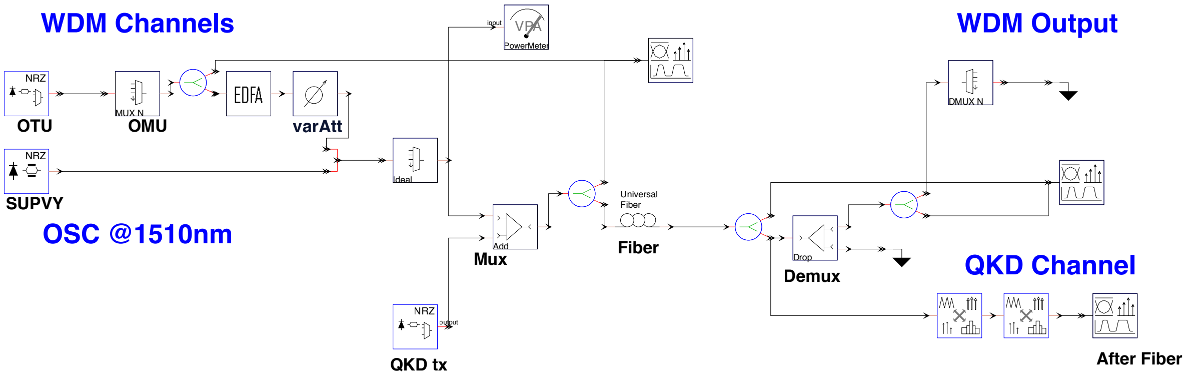


Figure 4.8: Metropolitan network link without intermediate node

In scenario 2 (Fig. 4.9) the laser power was fixed to 0 dBm per channel. The straight fiber span was replaced with two fibers and an intermediate erbium doped fiber amplifier (EDFA) (see 4.3.4). The lengths of the fibers were changed between 10 km and 30 km resulting in a total fiber length of 20 km . . . 60 km. As mentioned before the power output of the EDFA was post-equalized to 0 dBm per channel in order to avoid unrealistically high transmission powers which would entail strong non-linear effects. For classical channels no amplification would be required for 10 - 30 km fiber spans but the aim was to reproduce the characteristic ASE profile of EDFAs and their impact on background noise. The quantum channel bypassed the EDFA galaxy by frequency selective filtering (see 4.3.3).

For scenario 3 (Fig. 4.10) an optical cross-connect (OXC) was inserted after the EDFA. The combination of EDFA and OXC shall represent an optically switched node in a transparent network. As in scenario 2 the optical node was bypassed with WDM couplers. The frequency

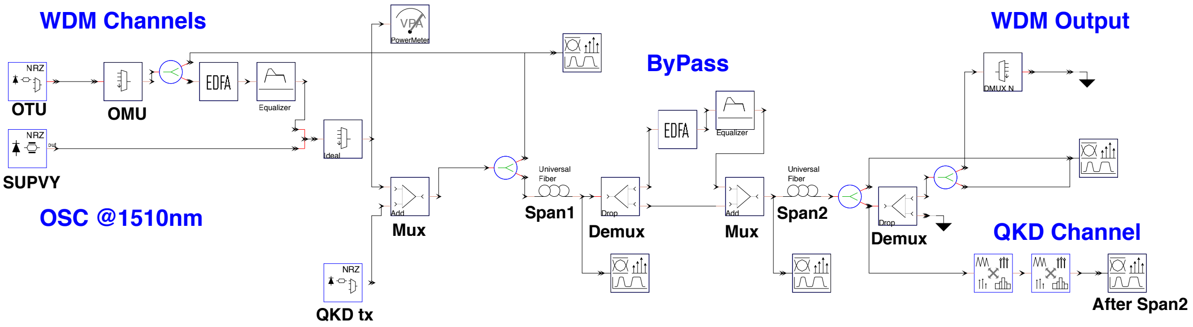


Figure 4.9: Metropolitan network link with inline EDFA bypass

conversion performed by the OXC introduces further background noise and channel crosstalk (see4.3.5). A sweep changed the length of fiber links from 10 to 30 km.

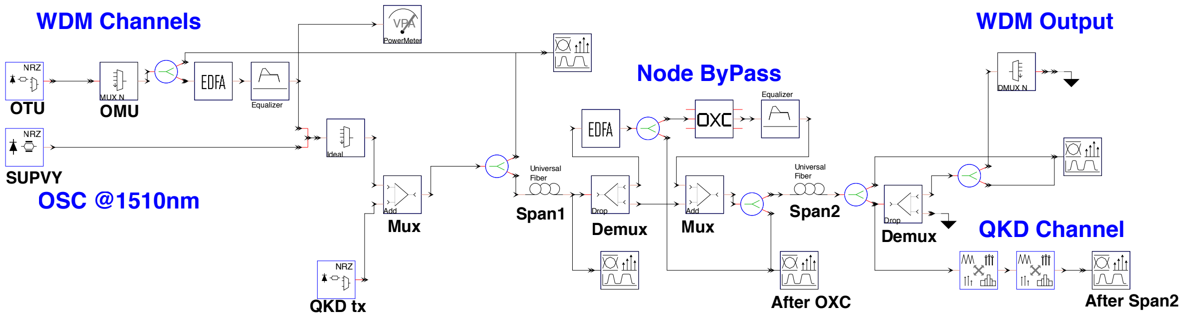


Figure 4.10: Metropolitan Network Link with switched node EDFA bypass

4.4.2 PON

The second type of scenarios examined passive optical access networks (PONs) to facilitate QKD transport to the subscribers of fiber-to-the-home (FTTH) topologies. Standardized wavelength plans were applied for the following technologies: *EPON, GPON, 10GPON, XGPON, PtP-GbE, PtP-10GbE, WDM-PON and WDM/TDM-PON*. For each technology the maximum specified transmission power (tx Power) was used to simulate the worst case scenarios for QKD operation. Since the PONs are inherently bidirectional the module `UniversalFiber` was used to account for backscattering effects. Background noise spectra were measured both for uplink and downlink at the optical line terminal (OLT) and the optical network unit (ONU) respectively.

EPON, GPON, 10GPON and XGPON schematics were essentially identical except for the configuration of upstream and downstream wavelengths and powers (Fig. 4.11). For EPON and GPON an additional downstream video channel at 1550 nm is specified in the standards and was also considered in the simulation setups. A single feeder fiber was used to accommodate both upstream and downstream as well as the quantum channels. The feeder fiber length was fixed to 15 km and connects the optical line terminal (OLT) at the central office (CO) with a passive

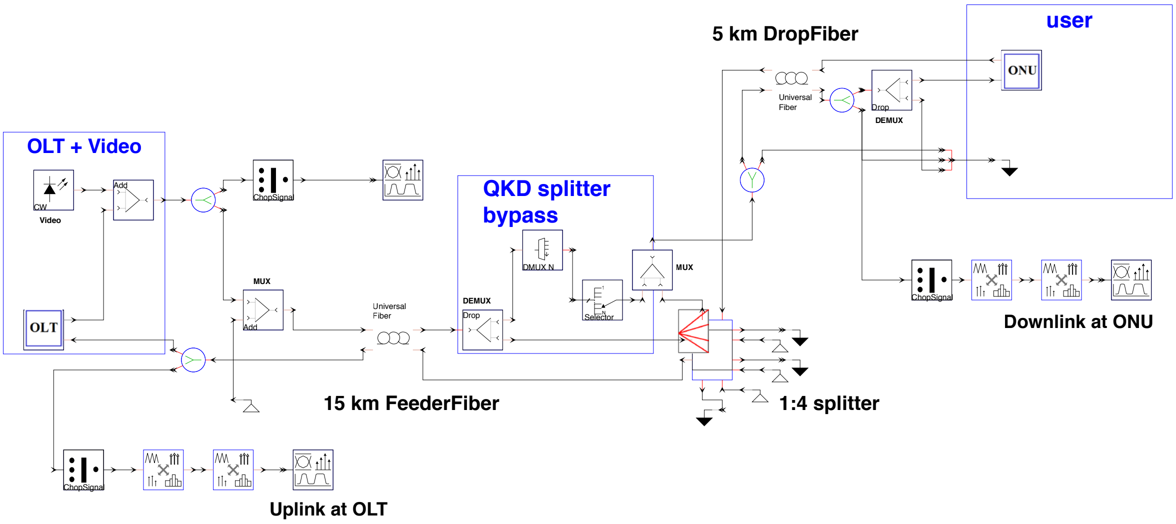


Figure 4.11: Access network configuration for EPON, GPON, 10GPON and XGPON (video channel at OLT only for EPON, GPON active)

optical splitter. The splitter duplicates the downstream across four drop fibers of 5 km length. For QKD an array of 4 channels is envisaged, one for each drop fiber. The quantum channels bypass the splitter via a WDM coupler and are sent through a de-multiplexer. For each drop fiber the corresponding QKD channel is picked and re-multiplexed to the signals on that fiber. From the signals point of view, the 1:4 splitting ratio introduces an insertion loss of $10log^{10}(4) = 6.02dB$ prior to each drop fiber. The drop fibers are terminated at optical network units (ONU) which are typically placed in the subscribers homes. For the sake of simplicity only one ONU and drop fiber was simulated. The upstream channel was generated at the ONU according to the standards.

The simulation of PtP-GbE and PtP-10GbE configurations required no splitter just a single fiber span of 20 km connecting OLT and ONU (Fig. 4.12). Both downlink and uplink spectra were measured.

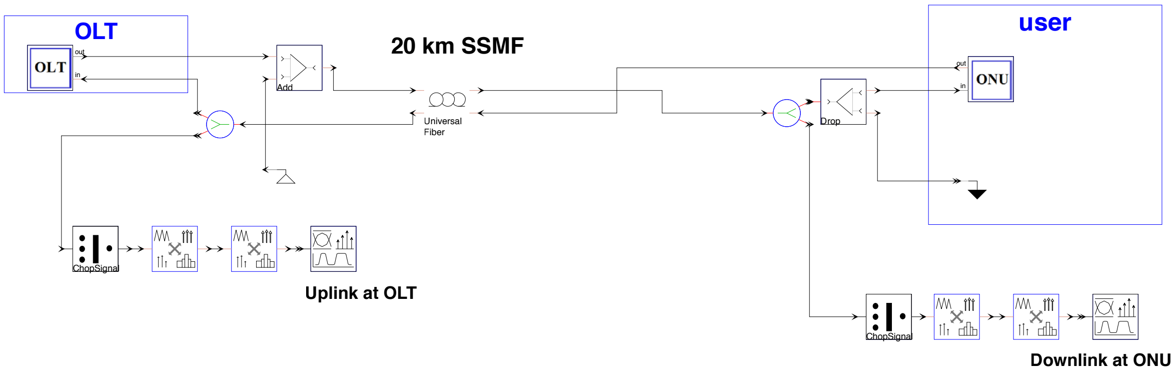


Figure 4.12: Access network configuration for PtP-GbE and PtP-10GbE

For WDM-PON and WDM/TDM-PON another schematic was produced which is similar to

EPON/GPON. A 15 km feeder fiber connects the OLT with an arrayed waveguide grating (AWG) which in turn connects to the ONUs through 5 km drop fibers (Fig. 4.13). In this technology the OLT does not only transmit one downstream wavelength but 32 wavelengths spaced by 100 GHz. The lasers at ONUs are also tuned to emit 32 different wavelengths for the upstream direction. Only one ONU was simulated whose upstream channel was ignored. In order to simulate all 32 upstream channels on the feeder fiber, an artificial laser array was used. This modification ensures a realistic channel allocation even for the upstream direction. The only inaccuracy comes from the lack of background noise generated by Raman scattering in the short drop fiber. But since Raman scattering in 5 km fibers is minimal the simplification imposes no major errors on the noise measurements.

In order to account for the time-division multiplexing of downstream channels in WDM/TDM-PONs, another 1:4 splitting factor was applied to the signal powers. The QKD channels on the drop fiber must be terminated or bypassed prior to the passive optical splitter because quantum signals are incompatible to splitting.

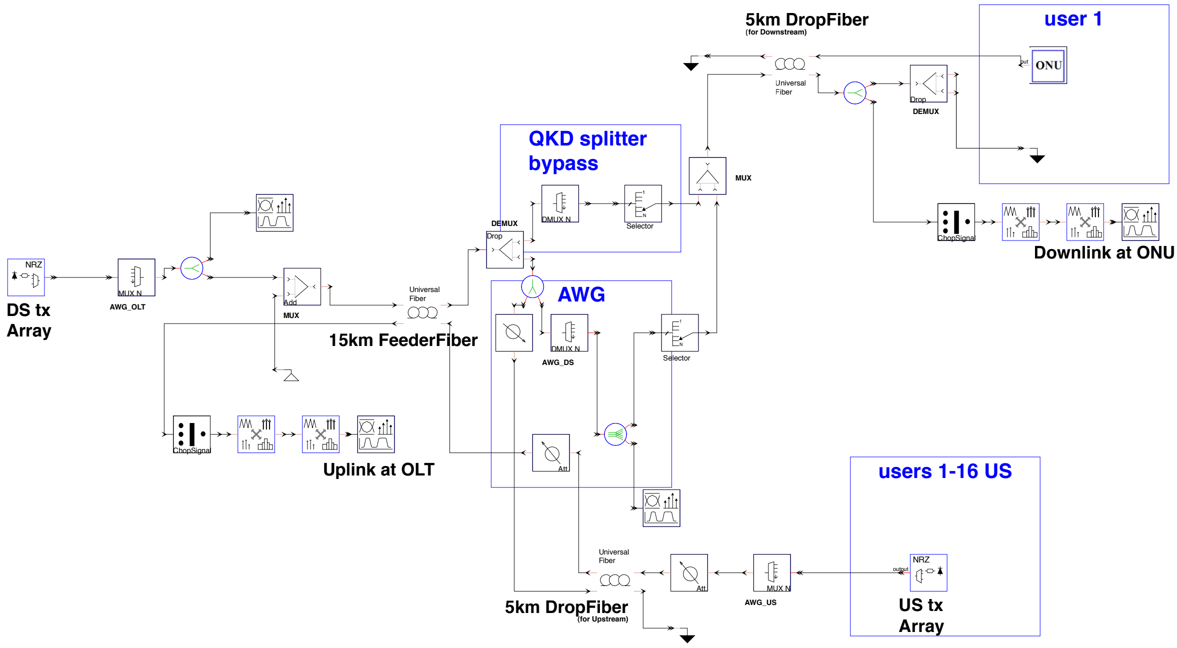


Figure 4.13: Access network configuration for WDM-PON and WDM/TDM-PON

5 Results and Discussion

The result of the numeric simulations was the optical spectrum consisting of signal and noise powers. The spectrum is influenced by fiber attenuation, component losses, non-linear effects, ASE, laser noise, etc. The various signal representation (sampled, parameterized signals, distortions, etc. – see 4.1.1) returned by *VPItransmissionMaker* were converted to noise bins which characterize the noise level in dBm per wavelength interval. The property called `NoiseResolution` is used by modules that generate noise and it configures the granularity of the calculated noise bins. Independent from the noise bin spacing (here set to 100 GHz), the program can act as an optical spectrum analyzer (OSA) which has its own frequency resolution. The OSA resolution was set to 0.1 nm equaling 12.5 GHz at 1550 nm. As a consequence the depicted noise levels can only be achieved if a narrow bandwidth filter of 0.1 nm is placed in front of all QKD detectors. Before presenting the background noise spectra, the chosen figures of merit are explained.

5.1 Figures of merit

The program returned the optical power spectrum in the range of 1200 nm to 1660 nm. The dimension of the power spectrum was returned in *dBm*. For reasons of better understanding, some post-processing was applied to the values returned from *VPItransmissionMaker* . All following conversions and calculations were implemented in *Microsoft Excel* processing the raw comma-separated data-files containing lines of:

```
LowerFrequency (nm); UpperFrequency (nm); Power (dBm).
```

5.1.1 Photon flux

In most papers about QKD systems and quantum channel performance the background noise is characterized as photon flux. Hence, the dBm power values needed to be converted to *photons per second*. The following formula was used where P_W is the noise power in W, P_{dBm} is the noise power in dBm, ν is the frequency in Hz, ω is the wavelength in nm, h is the Planck constant and c is the speed of light.

$$\Phi_{photons} = \frac{P_W}{h\,\nu} \;\Bigg|\; P_W = 0,001 \times 10^{\frac{P_{dBm}}{10}} \;,\; \nu = \frac{c}{\omega * 10^{-9}}$$

5.1.2 Quantum Key Distribution System

In this work the analytical model from [45] is used to characterize a QKD system. The authors presented analytic formulae for the Quantum Bit error rate (QBER) and the final secure key rate (Rsec). Additionally the paper suggests specific parameter values to plug in for the well-known plug-and-play QKD scheme by idQuantique (see 2.2.1) which is commercially available. Here the same system is chosen to calculate QBER and Rsec values. Of course many papers propose more sophisticated QKD systems which may or may not perform better in high noise power environment but those systems are still experimental and this work examined the most practical integration of QKD. Table 5.1 outlines the parameters values used to model the detector performance of the weak-pulse QKD scheme by idQuantique.

Parameter name	Symbol	Value	Dimension
Quantum Efficency	η	0.07	–
Gate Length	t_{gate}	1.50E-09	sec
Pulse Rate	f_{rep}	5.00E+06	Hz
Detector Number	n_{det}	2	–
Dark Count Probability	P_{dc}	5.00E-06	$^1/_{ns}$
After Pulse Probability	P_{AP}	0.008	–
Detector Losses	L_{det}	2.65	dB
Path Losses	L_{path}	from scenario	dB
Dead Time	t_{dead}	1.00E-05	sec
Mean Photon Number per pulse	μ	auto	–
Duty Line (p-n-p system)	L_s	0	m
Error Correction factor	η_{ec}	1.2	–
Visibility	V	0.98	–

Table 5.1: QKD system parameters used for background noise post-processing

5.1.3 Quantum bit error rate (QBER)

The figure of merit for a quantum channel depends both on transmission losses and the background noise level caused by nonlinear effect from classical channels propagating in the same fiber. The quantum bit error rate (QBER) combines these properties by defining a ratio between the number of false photon detections and total number of detected photons:

$$QBER = \frac{false}{right + false} = \frac{1}{2}\frac{p_\mu(1-V) + n_{det}\, p_{dc} + p_{AP} + p_{ram} + p_{ct}}{\beta p_\mu + n_{det} p_{dc} + p_{AP} + p_{ram} + p_{ct}}.$$

False photon detections can occur due to detector dark counts (p_{dc}), after pulsing (p_{AP}), Raman noise photons (p_{ram}) and crosstalk (p_{ct}). Raman noise and crosstalk probabilities are derived from the noise spectrum ($\Phi_{photons}$) returned by the simulations:

$$p_{ram} + p_{ct} = \Phi_{photons}\, \eta\, t_{gate}.$$

Dark count probability depends on the detectors used:

$$p_{dc} = P_{dc}\, t_{gate}\, 10^9.$$

The possibility that a detected photon causes after pulsing is fixed to 0.8 %:

$$p_{AP} = P_{ap}\,(p_\mu + n_{det}\,p_{dc} + p_{AP} + p_{ram} + p_{ct}).$$

In order to reduce the after pulsing to this value a detector dead time (t_{dead}) is applied after each detection. This is expressed by the parameter

$$\eta_{dead} = (1 + t_{dead}\,f_{rep}(p_\mu + n_{det}p_{dc} + p_{AP} + p_{ram} + p_{ct}))^{-1}.$$

The parameter η_{duty} shall represent the reduced efficiency of the QKD system by using a storage line to minimize Rayleigh backscattering. Here this effect is not considered and η_{duty} is set to 1.

Choosing the optimal mean photon number per pulse (μ) is not trivial. On the one hand there have to be enough photons to withstand path loss, but on the other hand too many photons facilitate photon number splitting (PNS) attacks. Here the optimal value for BB84 is defined to be $\mu_{BB84} = 10^{L_{path}/-10}$ with L_{path} being the path transmission of the quantum channel in dB. SARG applies a different sifting algorithm which renders PNS attacks ineffective. This allows QKD systems to use a higher mean photon number of $\mu_{SARG} = 2\,\sqrt{10^{L_{path}/-10}}$. Finally the probability of detecting a real pulse photon is

$$p_\mu = \mu^2\,\eta\,10^{-L_{det}/10}.$$

5.1.4 Final secure key rate (Rsec)

To further characterize the performance of a QKD system the final secure key rate (Rsec) can be estimated. Therefore the full QKD stack (Fig. 2.2) including the sifting protocol needs to be modeled. Fortunately [45] provides expressions that model the QKD stack of BB84 and SARG. The basis for privacy amplification is the sifted key rate:

$$R_{sifted} = \frac{1}{2}(\beta\,p_\mu + n_{det}\,p_{dc} + p_{AP} + p_{ram} + p_{ct})\,f_{rep}\,\eta_{duty}\,\eta_{dead}.$$

The β parameter accounts for the protocol differences between BB84 and SARG ($\beta_{BB84} = 1$, $\beta_{SARG} = \frac{2-V}{2}$) . All other parameters used to calculate R_{sifted} were explained for QBER (see 5.1.3). The final secure key rate can be expressed as the difference of the mutual information per bit between Alice and Bob (I_{AB}), and between Alice and a potential eavesdropper (I_{AE}):

$$R_{rec} = R_{sifted}(I_{AB} - I_{AE}).$$

The mutual information per bit between Alice and Bob is:

$$I_{AB} = 1 - \eta_{ec}\,H(QBER)$$

with $H(p)$ being the binary entropy function $H(p) = -p\,log_2(p) - (1-p)\,log_2(1-p)$. The maximum QBER allowed to extract a secure key is referred to as *Shannon Limit* and is about 11 %. This limit is theoretical and cannot be reached with real protocols due to suboptimal error correction and additional bits lost for authentication. Here the error correction algorithm

CASCADE is assumed to need 20 % more bits then given by the Shannon Limit ($\eta_{ec} = 1.2$). Due to this factor the charts show secret key rates when QBER decreases below ≈ 8.6 %.

The mutual information per bit between Alice and a potential eavesdropper (Eve) depends on the sifting protocol used. For BB84 the following formula applies:

$$I_{AE,BB84} = \frac{\left(1 - \frac{\mu}{2t}\right)\left(1 - H(P)\right) + \frac{\mu}{2t}}{1 + \frac{2p_{dc}}{\mu t \eta}}.$$

When SARG is used then less bits are revealed during the sifting process decreasing Eves information per bit to:

$$I_{AE,SARG} = I_{PNS}(1) + \frac{1}{12}\frac{\mu^2}{t}e^{-\mu}\left(1 - I_{PNS}(1)\right) \;\Big|\; I_{PNS}(k) = 1 - H(\frac{1}{2} + \frac{1}{2}\sqrt{1 - {}^{1}\!/_{2^k}}).$$

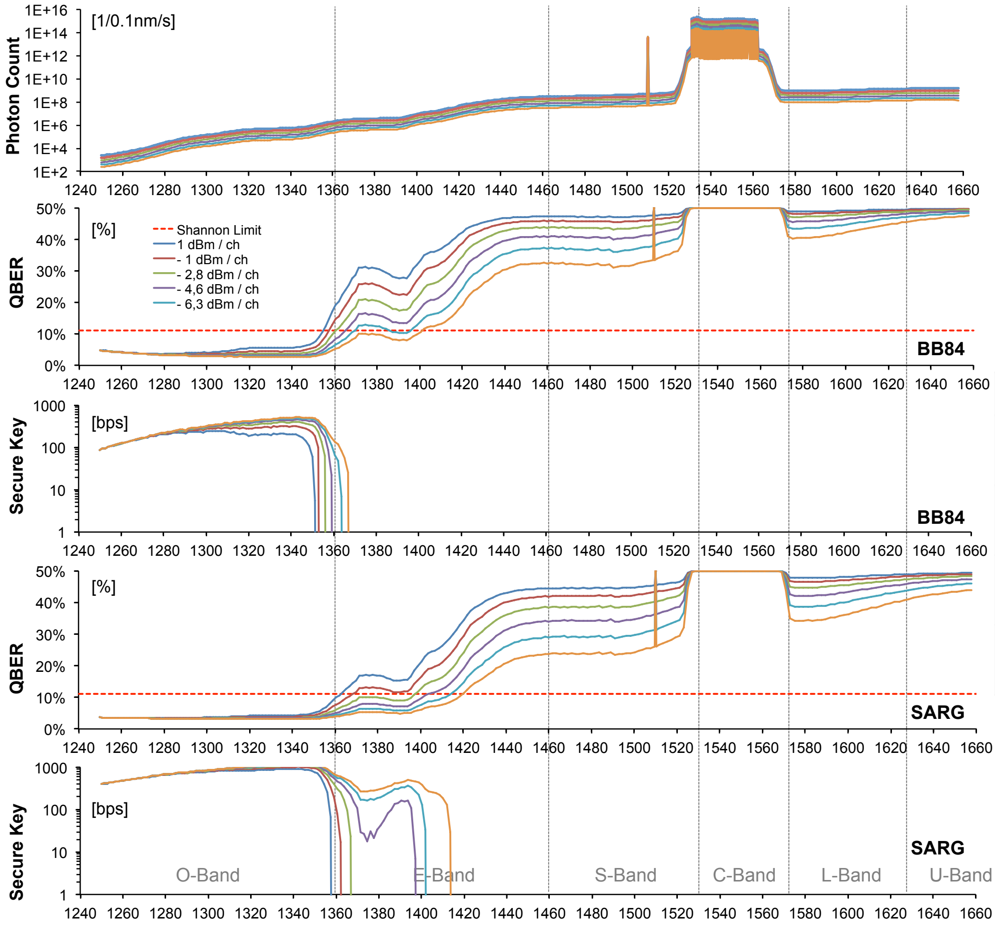
In both cases the path linear transmission is given by $t = 10^{L_{path}/-10}$. I_{PNS} expresses potential information gain of Eve when executing PNS attacks.

5.2 Metro

Both attenuation and accumulated background noise depend on the chosen wavelength and are influenced by system parameters such as the fiber length, power levels of transmitters, wavelength plan and network architecture. Therefore typical system parameters were used for standardized network architectures (see 4.4) to determine noise levels, QBER and achievable key rates. Most WDM related system parameters were derived from the *WaveStar OLS 400G* demonstration network from *Lucent Technologies*, which is installed in the laboratories of the Institute of Telecommunications at Vienna University of Technology.

In order to allow a reliable exchange of quantum keys, the number of background photons should be in the order of or preferably below 10^5 (< 600.000 photons). For 40-channel point-to-point DWDM metro networks with 100 GHz spacing between 191.9 THz and 195.9 THz, the background photon count remains below 600.000 per second within the whole O-band for launch powers up to 1 dBm per channel (see Fig. 5.1). A similar noise spectrum with 10^4 to 10^6 background photons per second within the O-band has been obtained for optically transparent paths with bypassed in-line amplifiers (Fig. 5.2) and optical nodes (Fig. 5.3).

In addition to the background noise, the path loss and the QKD scheme and protocol applied influence the achievable QBER and, thereby, the achievable secret key rate (Rsec) of the QKD system. To illustrate the effect of combined impairments, QBER and Rsec were estimated for the exemplary QKD system explained in 5.1.2. As sifting protocols both BB84 and SARG were assumed (see 5.1.4. The figures shows that for a point-to-point 20 km DWDM link, the QBER remains below 5 % in the whole O-band, promising achievable secret key rates of several hundreds of bit/s. The higher mean photon number of SARG allows to place a quantum channel in the E-band (waterpeak). Bypassing amplifiers or nodes the Rsec reduces to a maximum of 10 bit/s (BB84) or 100 bit/s (SARG) for 30 km long transparent optical paths. For wavelengths above 1360 nm and paths longer than 30 km the QBER increases above the Shannon limit (11 %) in any bypassing case.

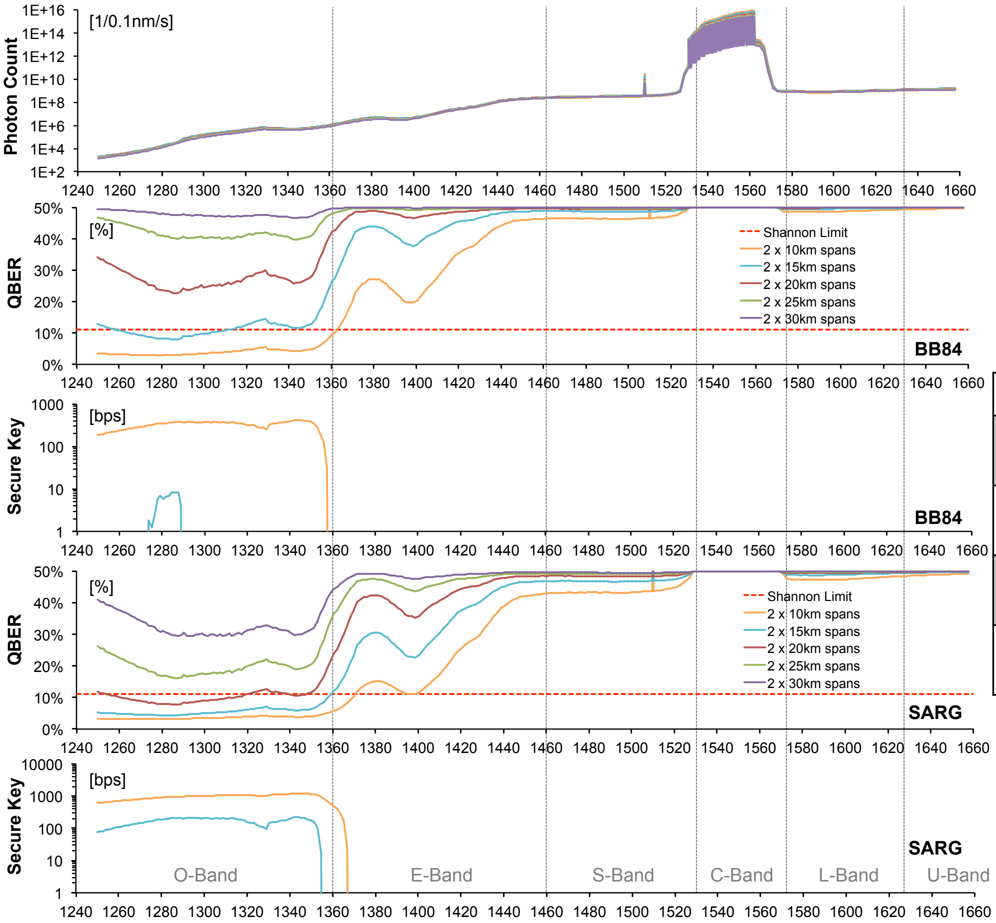


Direct Link MAN

40 DWDM ch. @ 100 GHz	
wavelength [nm]	1530-1562 1510 [OSC]
data rate [Gbps]	2.5
Tx power [dBm]	- 7,5 … 1
Fiber Length [km]	25

Figure 5.1: Direct Link — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for uni-directional link – Standard wavelengths with specified powers and fiber lengths were used (right box).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.

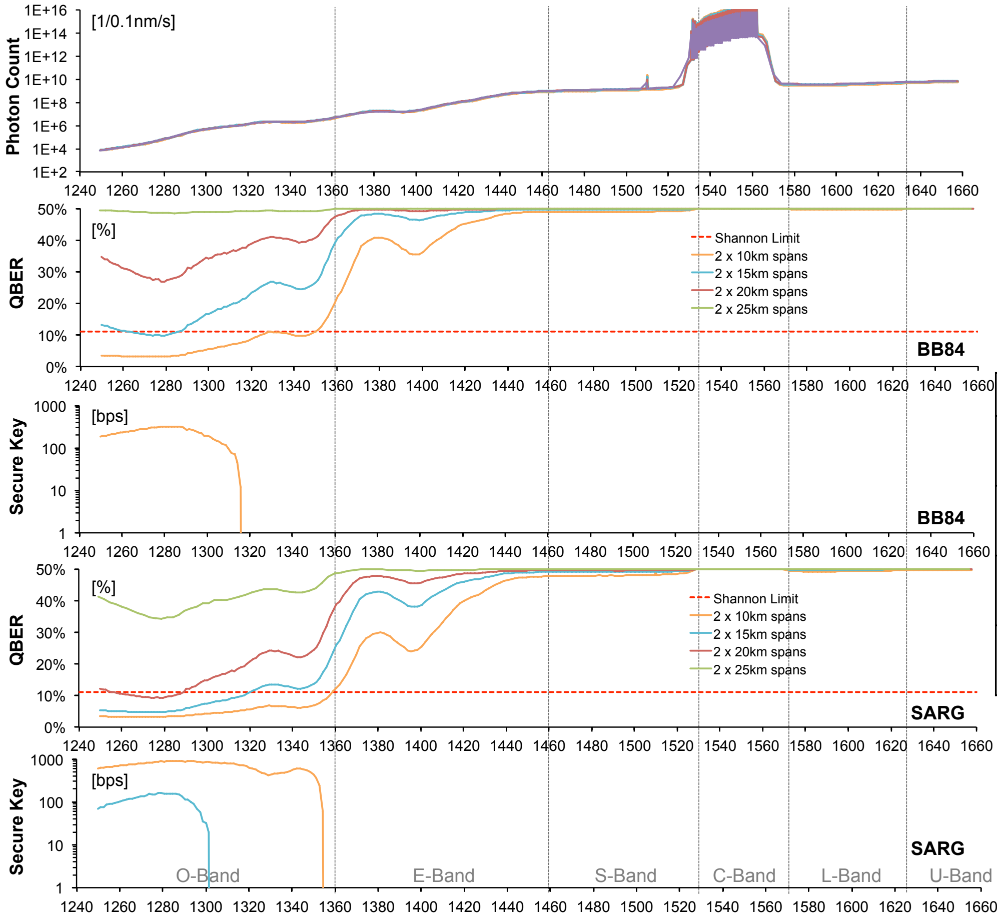


EDFA Bypass MAN

40 DWDM ch. @ 100 GHz	
wavelength [nm]	1530-1562 1510 [OSC]
data rate [Gbps]	2.5
Tx power [dBm]	0
Fiber Length [km]	20 … 60

Figure 5.2: EDFA Bypass — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for uni-directional link – Standard wavelengths with specified powers and fiber lengths were used (right box).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



Node Bypass MAN

40 DWDM ch. @ 100 GHz	
wavelength [nm]	1530-1562 1510 [OSC]
data rate [Gbps]	2.5
Tx power [dBm]	0
Fiber Length [km]	20 … 50

Figure 5.3: Node Bypass — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for uni-directional link – Standard wavelengths with specified powers and fiber lengths were used (right box).

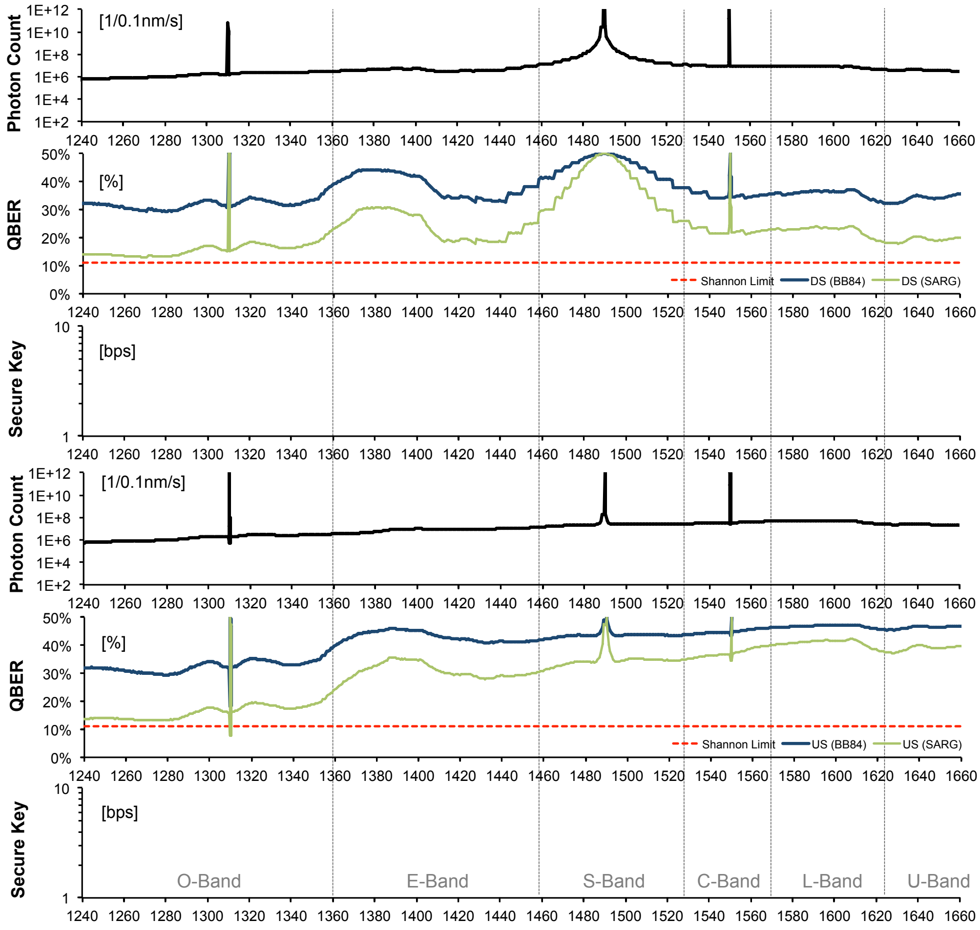
QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.

5.3 PON

Figures 5.4 – 5.11 present the background noise spectra obtained by numerical simulations in terms of photon numbers per second and 12.5 GHz resolution bandwidth. In the case of BB84 it is evident from the figures that the background noise in 1 Gbit/s and 10 Gbit/s PONs such as EPON (Fig. 5.4), GPON (Fig. 5.5), 10G-EPON (Fig. 5.6) and XG-PON (Fig. 5.7) is above 10^5 across the entire considered wavelength range for both upstream and downstream. This is mainly due to the fact that these standards specify spectrally widely separated upstream and downstream channels. However, when applying the SARG protocol a key rate of 100 bit/s can be extracted for a quantum channel placed around 1440 nm in 10G-EPON and XG-PON.

In contrast, for PONs employing wavelength-division multiplexing (WDM PON and WDM/TDM PON, Fig. 5.10 and 5.11) all upstream and downstream channels can be accommodated within the C-band such that background noise in the O-band remains below 10^5. The QBER and Rsec values indicate that for WDM and WDM/TDM PONs, a QBER $< 11\%$ and secret key rates in the order of tens of bit/s are achievable within a portion of the O-band. With BB84 only downstream QKD operation is possible while SARG also faciliates a quantum upstream channel placed inside the O-band.

As with point-to-point PONs different QKD wavelength allocations need to be applied for PtP GbE and PtP 10GbE. In PtP GbE (Fig. 5.8) the wavelengths of upstream and downstream channel are widely separated so a quantum channel can be placed almost anywhere in between with both BB84 and SARG. Just the wavelengths near the classical channels need to be avoided. In PtP 10GbE (Fig. 5.9) upstream and downstream channels are both located in the O-Band, which limits QKD operation to wavelengths greater than 1450 nm. The low attenuation of single mode fibers can be employed to advantage for the quantum channel. In both PtP scenarios secret key rates of 1000 bit/s can be achieved.



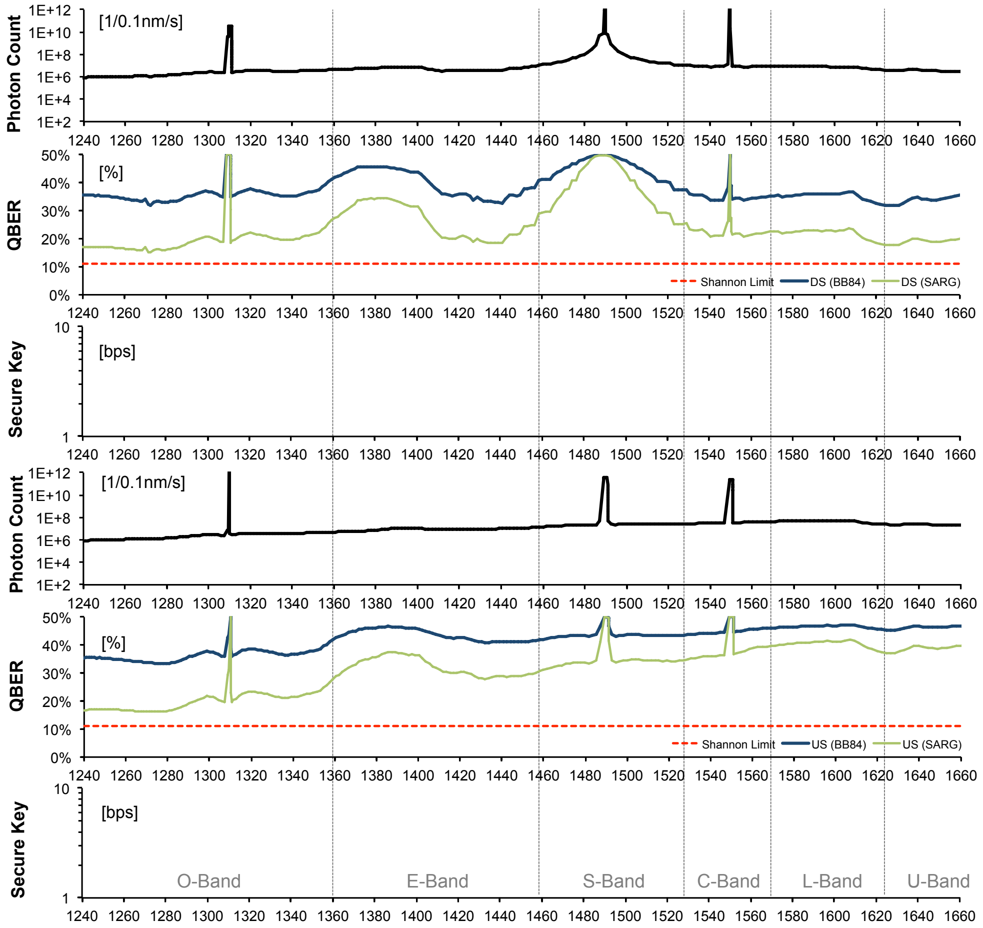
Downstream	EPON
wavelength [nm]	1490 1550 (Video)
data rate [Gbps]	1.25
Tx power [dBm]	2.5 … **7**
Feeder Fiber [km]	20

EPON

Upstream	EPON
wavelength [nm]	1310
data rate [Gbps]	1.25
Tx power [dBm]	-1 … **4**
Feeder Fiber [km]	20

Figure 5.4: EPON — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



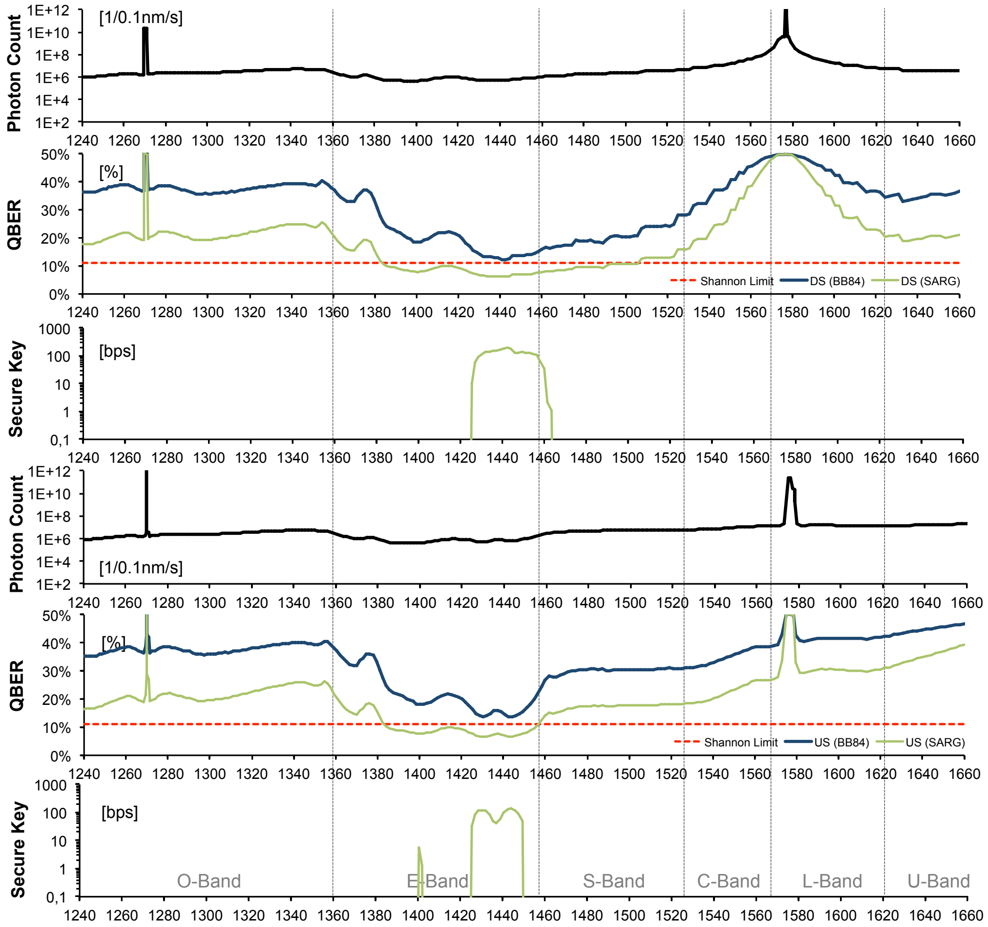
Downstream	GPON
wavelength [nm]	1490 1550 (Video)
data rate [Gbps]	2.488
Tx power [dBm]	3 … 7
Feeder Fiber [km]	20

GPON

Upstream	GPON
wavelength [nm]	1310
data rate [Gbps]	1.244
Tx power [dBm]	0.5 … 5
Feeder Fiber [km]	20

Figure 5.5: **GPON** — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



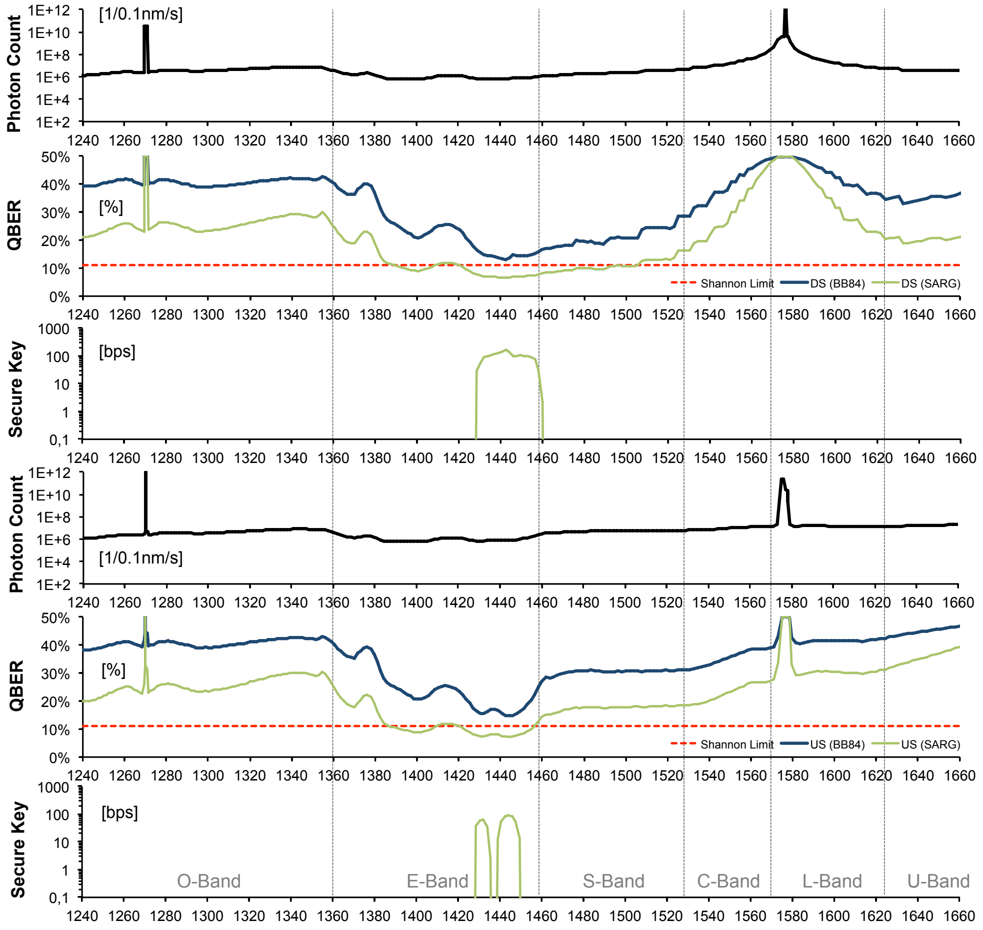
Downstream	10G EPON
wavelength [nm]	1577
data rate [Gbps]	10.3125
Tx power [dBm]	2 … <u>6</u>
Feeder Fiber [km]	20

10G EPON

Upstream	10G EPON
wavelength [nm]	1270
data rate [Gbps]	1.25
Tx power [dBm]	2 … <u>6</u>
Feeder Fiber [km]	20

Figure 5.6: 10G EPON — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



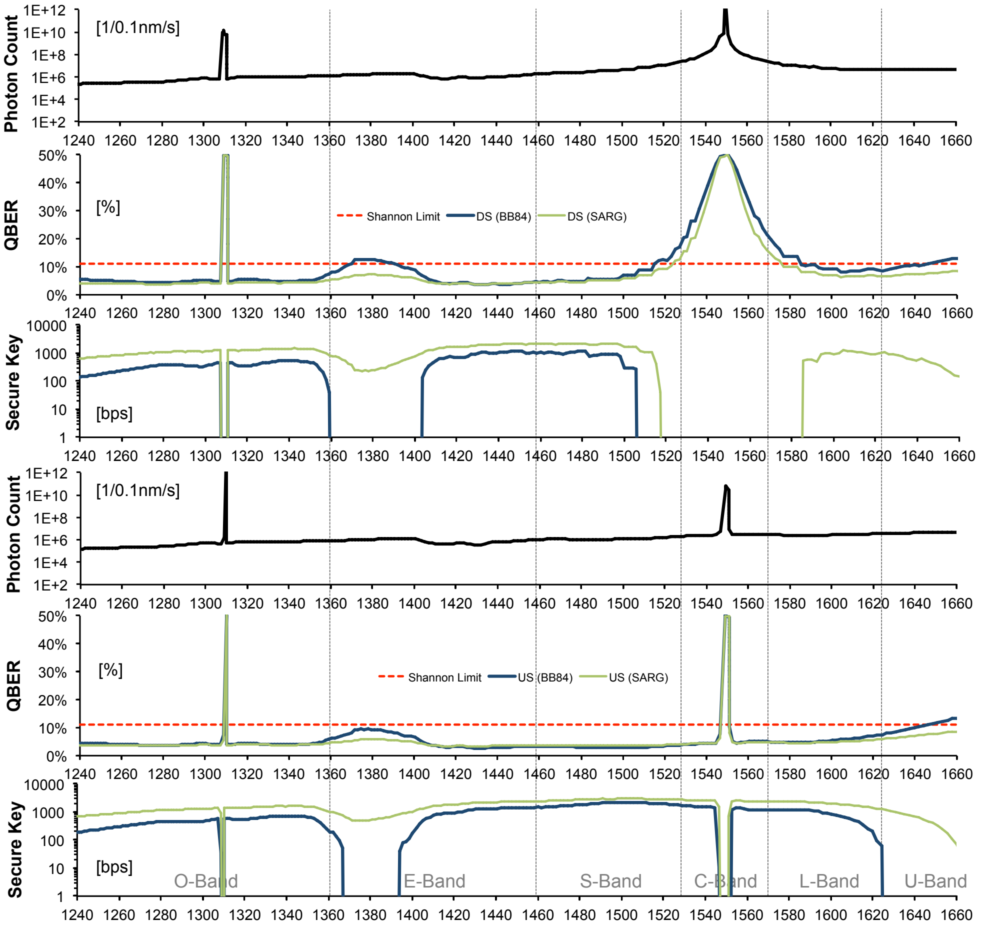
Downstream	XG PON
wavelength [nm]	1577
data rate [Gbps]	9.953
Tx power [dBm]	2 … 6
Feeder Fiber [km]	20

XG PON

Upstream	XG PON
wavelength [nm]	1270
data rate [Gbps]	2.488
Tx power [dBm]	2 … 6
Feeder Fiber [km]	20

Figure 5.7: XG PON — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



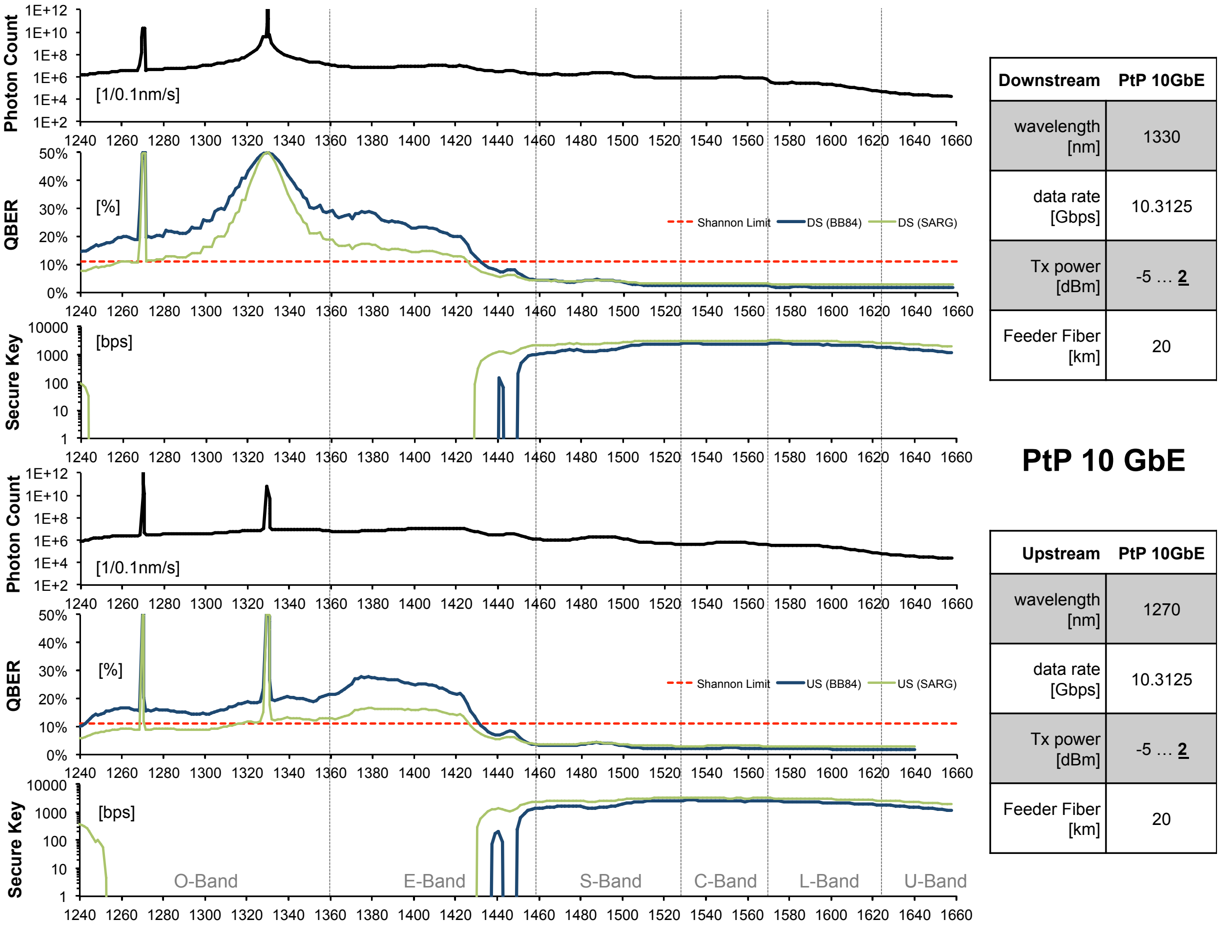
Downstream	PtP GbE
wavelength [nm]	1550
data rate [Gbps]	1.25
Tx power [dBm]	-8 … **2**
Feeder Fiber [km]	20

PtP GbE

Upstream	PtP GbE
wavelength [nm]	1310
data rate [Gbps]	1.25
Tx power [dBm]	-8 … **2**
Feeder Fiber [km]	20

Figure 5.8: PtP GbE — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.

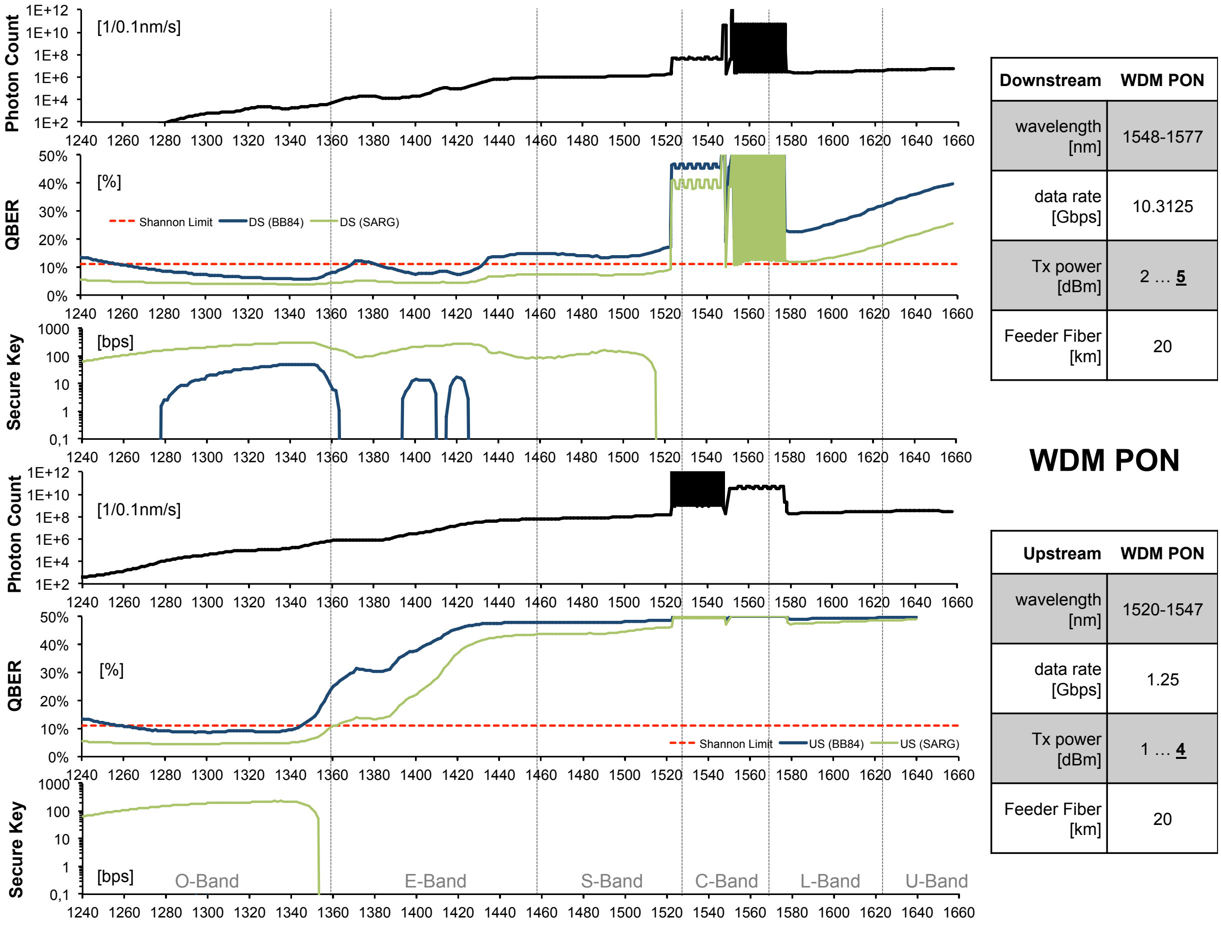


Downstream	PtP 10GbE
wavelength [nm]	1330
data rate [Gbps]	10.3125
Tx power [dBm]	-5 … **2**
Feeder Fiber [km]	20

Upstream	PtP 10GbE
wavelength [nm]	1270
data rate [Gbps]	10.3125
Tx power [dBm]	-5 … **2**
Feeder Fiber [km]	20

Figure 5.9: PtP 10GbE — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.

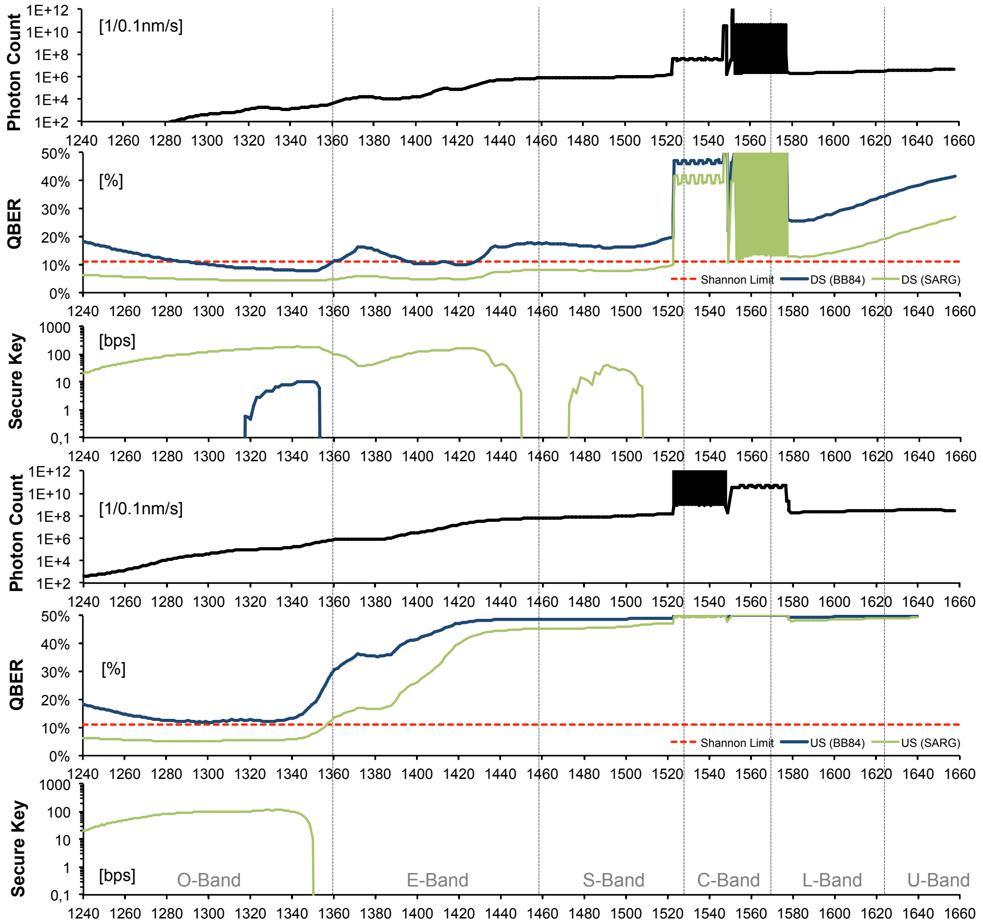


Downstream	WDM PON
wavelength [nm]	1548-1577
data rate [Gbps]	10.3125
Tx power [dBm]	2 … **5**
Feeder Fiber [km]	20

Upstream	WDM PON
wavelength [nm]	1520-1547
data rate [Gbps]	1.25
Tx power [dBm]	1 … **4**
Feeder Fiber [km]	20

Figure 5.10: WDM PON — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.



Downstream	WDM TDM
wavelength [nm]	1548-1577
data rate [Gbps]	10.3125
Tx power [dBm]	2 … 5
Feeder Fiber [km]	20

WDM/TDM PON

Upstream	WDM TDM
wavelength [nm]	1520-1547
data rate [Gbps]	1.25
Tx power [dBm]	1 … 4
Feeder Fiber [km]	20

Figure 5.11: WDM/TDM PON — Background noise, quantum bit error rate (QBER), final secure key rate (Rsec) over wavelength (λ) for downstream (upper figures) and upstream direction (lower figures) – Standard wavelengths (right boxes) with maximal specified powers were used (underlined).

QBER and Rsec are calculated with system parameters of the weak-pulse send-and-return scheme from idQuantique [25, 45] using the QKD protocols BB84 [11] and SARG [28]. Background noise is plotted per 12.5 GHz bandwidth, hence a QKD systems has to employ a narrow bandwidth filter of 0.1 nm to obtain this rejection.

6 Conclusion and Outlook

Although the idea to utilize the quantum optical properties for the encryption of data transmitted over optical links is about 30 years old, the implementation of quantum cryptography has not yet reached acceptance by users, also caused by the current need of a dark fiber for each quantum key distribution (QKD) system. The integration in conventional optical networks presumes a robust and economical embodiment of QKD systems.

This work examined perspectives, limitations and challenges for implementing QKD systems in transparent optical networks. The entire wavelength region between 1240 nm and 1660 nm was considered, in order to cover all the important telecommunication bands. The author evaluated the expected impairments caused by co-existing data channels and network subsystems in accordance to conventional standards. Even following the selection of the preferred wavelength for QKD systems (according to the outcome of our simulations) the QKD performance is limited by optical excess losses and noise accumulation along the lightpath. Optical components and network nodes heavily affect the QKD channel and need to be bypassed at the cost of additional coupling losses.

In particular, for QKD channels placed within the preferred O-band the author observed low-enough background noise levels for a reliable quantum key exchange in WDM PON, WDM/TDM PON and 40-channel DWDM metro networks. A forbiddingly high background noise level across the entire considered spectrum was observed for EPON and GPON. 10G-EPON and XG-PON, which can only be combined with a QKD system using the SARG protocol. Acceptable QBER and sufficient secret bit rates seem possible if conventional data channels are restricted to the C-band and the QKD channel is allocated in the O-band, at least for transparent optical paths not exceeding 20 to 30 km of standard single-mode fibers, provided that optical amplifiers, splitters and any intermediate active nodes are bypassed. Additionally, narrow-band optical filters in the sub-0.1 nm range have to be used in front of QKD receivers to efficiently suppress background noise.

The simulation results also proved that the QKD performance can be substantially increased by employing more sophisticated QKD schemes – just as the SARG protocol. The use of more noise resilient protocols like COW, DSP or Continuous-Variable protocols can potentially increase achievable fiber lengths and key rates. The simulations of this work constitute the worst case scenario for the background noise every QKD system has to deal with if seamlessly integrated in standard telecom networks.

The results of background noise, QBER and Rsec assuming the BB84 sifting protocol were published in proceedings to the NOC 2013 [AWP+13b] and ICTON 2013 [AWP+13a] conferences.

References

[1] Y. Zhao, “Quantum cryptography in real-life applications: Assumptions and security,” Ph.D. dissertation, University of Toronto, 2009.

[2] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM journal on computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[3] T. Länger and G. Lenhart, “Standardization of quantum key distribution and the etsi standardization initiative isg-qkd,” *New Journal of Physics*, vol. 11, no. 5, p. 055051, 2009.

[4] P. D. Townsend, “Secure key distribution system based on quantum cryptography,” *Electronics Letters*, vol. 30, no. 10, pp. 809–811, 1994.

[5] J. J. Morton, A. M. Tyryshkin, R. M. Brown, S. Shankar, B. W. Lovett, A. Ardavan, T. Schenkel, E. E. Haller, J. W. Ager, and S. Lyon, “Solid-state quantum memory using the 31p nuclear spin,” *Nature*, vol. 455, no. 7216, pp. 1085–1088, 2008.

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Reviews of Modern Physics*, vol. 81, no. 2, p. 865, 2009.

[7] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lornser, E. Querasser, T. Matyus, H. Hbel, and A. Zeilinger, “A fully automated quantum cryptography system based on entanglement for optical fibre networks,” in *New Journal of Physics*, vol. 11, 2009.

[8] J. S. Pelc, L. Ma, C. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, and M. Fejer, “Long-wavelength-pumped upconversion single-photon detector at 1550 nm: performance and noise analysis,” *Optics Express*, vol. 19, no. 22, pp. 21 445–21 456, 2011.

[9] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[10] S. Wiesner, “Conjugate coding,” *Sigact News*, vol. 15-1, pp. 78–88, 1983.

[11] C. H. Bennett, G. Brassard *et al.*, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, no. 0. Bangalore, India, 1984.

[12] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[13] A. K. Ekert, “Quantum cryptography based on bells theorem,” *Physical review letters*, vol. 67, no. 6, pp. 661–663, 1991.

[14] P. Townsend, J. Rarity, and P. Tapster, “Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel,” *Electronics Letters*, vol. 29, no. 14, pp. 1291–1293, 1993.

[15] H. Zbinden, J. Gautier, N. Gisin, B. Huttner, A. Muller *et al.*, “Interferometry with faraday mirrors for quantum cryptography,” *Electronics Letters*, vol. 33, no. 7, pp. 586–588, 1997.

[16] S. Wijesekera, S. Palit, and B. Balachandran, “Software development for B92 quantum key distribution communication protocol,” in *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on.* IEEE, 2007, pp. 274–278.

[17] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *advances in CryptologyEUROCRYPT93.* Springer, 1994, pp. 410–423.

[18] D. E. M. S. D. Lancho, J. Martinez and V. Martin, "Qkd in standard optical telecommunication networks," *Lect. Notes Inst. Comput. Sci., Soc. Inf. Tele- com. Eng.*, vol. 36, pp. 142–149, 2010.

[19] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, p. 379423 and 623656, 1984.

[20] N. Lütkenhaus and S. M. Barnett, "Security against eavesdropping in quantum cryptography," in *Quantum Communication, Computing, and Measurement.* Springer, 1997, pp. 89–98.

[21] P. Schartner and S. Rass, "Quantum key distribution and denial-of-service: Using strengthened classical cryptography as a fallback option," in *Computer Symposium (ICS), 2010 International.* IEEE, 2010, pp. 131–136.

[22] ETSI, "Quantum key distribution (qkd); components and internal interfaces," ETSI Industry Specification (ISG) Group Quantum Key Distribution, Tech. Rep., 2010.

[23] M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocols: A survey," *International Journal of Universal Computer Sciences*, vol. 1, no. 2, pp. 59–67, 2010.

[24] A. J. Shields, C. Gobby, and Z. L. Yuan, "Quantum key distribution over 122 km of standard telecom fiber," in *Applied Physics Letters*, vol. 84, 2004.

[25] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics*, vol. 4, pp. 41–1, 2002.

[26] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[27] A. Niederberger, V. Scarani, and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the bennett-brassard 1984 protocol for quantum cryptography," *Physical Review A*, vol. 71, no. 4, p. 042316, 2005.

[28] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, no. 5, p. 057901, 2004.

[29] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[30] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical review letters*, vol. 94, no. 23, p. 230503, 2005.

[31] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase-shift quantum key distribution," in *Photonics Asia 2002.* International Society for Optics and Photonics, 2002, pp. 32–39.

[32] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, pp. 194 108–194 108, 2005.

[33] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," in *arXiv preprint quant-ph/0411022*, 2004.

[34] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," in *Defense and Security.* International Society for Optics and Photonics, 2005, pp. 138–149.

[35] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bells theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[36] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[37] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, “Field test of a continuous-variable quantum key distribution prototype,” *New Journal of Physics*, vol. 11, no. 4, p. 045023, 2009.

[38] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, “Feasibility of quantum key distribution through a dense wavelength division multiplexing network,” *New Journal of Physics*, vol. 12, no. 10, p. 103042, 2010.

[39] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, “Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate,” *Optics Express*, vol. 16, no. 23, pp. 18 790–18 979, 2008.

[40] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga *et al.*, “Megabits secure key rate quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, p. 045010, 2009.

[41] R. J. Hughes, G. L. Morgan, and C. G. Peterson, “Quantum key distribution over a 48 km optical fibre network,” *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 533–547, 2000.

[42] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-i. Yoshino, S. Miki, B. Baek, Z. Wang *et al.*, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” *Optics Express*, vol. 16, no. 15, pp. 11 354–11 360, 2008.

[43] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” *New Journal of Physics*, vol. 11, no. 7, p. 075003, 2009.

[44] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, “2 ghz clock quantum key distribution over 260 km of standard telecom fiber,” *Optics Letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[45] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 gbps data encryption over a single fibre,” *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[46] 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 *et al.*, “Progress toward quantum communications networks: opportunities and challenges,” *Optoelectronic Integrated Circuits IX*, vol. 6476, p. 6476OI, 2007.

[47] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, “In-band quantum key distribution (qkd) on fiber populated by high-speed classical data channels,” in *Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference. OFC 2006.* IEEE, 2006, pp. 3–pp.

[48] H. Rohde, S. Smolorz, A. Poppe, and H. Huebel, “Quantum key distribution integrated into commercial wdm systems,” in *Optical Fiber Communication Conference.* Optical Society of America, 2008.

[49] D. Subacius, A. Zavriyev, and A. Trifonov, “Backscattering limitation for fiber-optic quantum key distribution systems,” *Applied Physics Letters*, vol. 86, no. 1, pp. 011 103–011 103, 2005.

[50] R. J. Runser, T. E. Chapuran, P. Toliver, M. S. Goodman, J. Jackel, N.Nweke, S. R. McNown, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Demonstration of 1.3 pm quantum key distribution (qkd) compatibility with 1.5 pm metropolitan wdm," in *Optical Society of America*, 2006.

[51] K. Patel, J. Dynes, I. Choi, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, no. 4, p. 041010, 2012.

[52] P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," in *Electronics Letters*, vol. 33, no. 3, 1996.

[53] P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, J. E. Nordholt *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *Photonics Technology Letters, IEEE*, vol. 15, no. 11, pp. 1669–1671, 2003.

[54] M. Goodman, P. Toliver, R. Runser, T. Chapuran, J. Jackel, R. Hughes, C. Peterson, K. McCabe, J. Nordholt, K. Tyagi *et al.*, "Quantum cryptography for optical networks: A systems perspective," in *Lasers and Electro-Optics Society, 2003. LEOS 2003. The 16th Annual Meeting of the IEEE*, vol. 2. IEEE, 2003, pp. 1040–1041.

[55] P. Toliver, R. Runser, T. Chapuran, S. McNown, M. Goodman, J. Jackel, R. Hughes, C. Peterson, K. McCabe, J. Nordholt *et al.*, "Impact of spontaneous anti-stokes raman scattering on qkd+ dwdm networking," in *Lasers and Electro-Optics Society, 2004. LEOS 2004. The 17th Annual Meeting of the IEEE*, vol. 2. IEEE, 2004, pp. 491–492.

[56] N. I. Nweke, R. J. Runser, S. R. McNown, J. B. Khurgin, T. E. Chapuran, P. Toliver, M. S. Goodman, J. Jackel, R. J. Hughes, C. G. Peterson *et al.*, "Edfa bypass and filtering architecture enabling qkd+ wdm coexistence on mid-span amplified links," in *Conference on Lasers and Electro-Optics*. Optical Society of America, 2006.

[57] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments," *New Journal of Physics*, vol. 11, no. 4, p. 045012, 2009.

[58] T. Chapuran, P. Toliver, N. Peters, J. Jackel, M. Goodman, R. Runser, S. McNown, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics*, vol. 11, no. 10, p. 105001, 2009.

[59] ITU-T G.694.2. (2003) Spectral grids for WDM applications: CWDM wavelength grid. ITU Telecommunication Standardization Sector. [Online]. Available: http://www.itu.int/rec/T-REC-G.694.2/en

[60] ITU-T G.694.1. (2012) Spectral grids for WDM applications: DWDM frequency grid. ITU Telecommunication Standardization Sector. [Online]. Available: http://www.itu.int/rec/T-REC-G.694.1/en

[61] ITU-T G.987. (2012) 10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms. ITU Telecommunication Standardization Sector.

[62] ITU-T G.983.1. (2005, January) Broadband optical access systems based on passive optical networks (pon). ITU Telecommunication Standardization Sector.

[63] A. Lovric, “Power efficiency of state-of-the-art and advanced wired access networks,” in *Diploma Thesis*, 2010, p. 65.

[64] IEEE 802.3ah. (2008) Ethernet in the First Mile Standard. [Online]. Available: http://www.ieee802.org/3/efm/

[65] IEEE 802.3av. 10G-EPON (Ethernet Passive Optical Network) Task Force. [Online]. Available: http://www.ieee802.org/3/av/

[66] ITU-T G.984.1. (2008) Gigabit-capable passive optical networks (GPON): General characteristics. ITU Telecommunication Standardization Sector. [Online]. Available: http://www.itu.int/rec/T-REC-G.984.1/en

[67] VPI Systems, VPItransmissionMaker Optical Systems. [Online]. Available: http://www.vpiphotonics.com/

[68] D. Hollenbeck and C. D. Cantrell, “Multiple-vibrational-mode model for fiber-optic raman gain spectrum and response function,” *JOSA B*, vol. 19, no. 12, pp. 2886–2892, 2002.

[69] G. S. Felinskyi, “Spectroscopic multiple-vibrational-modeling of raman gain for fra design,” in *Laser and Fiber-Optical Networks Modeling, 2005. Proceedings of LFNM 2005. 7th International Conference on.* IEEE, 2005, pp. 262–265.

[70] Y. Kang, “Calculations and measurements of raman gain coefficients of different fiber types,” Ph.D. dissertation, Citeseer, 2002.

[71] S. Aleksic and A. Lovric, “Energy consumption and environmental implications of wired access networks,” in *American Journal of Engineering and Applied Sciences*, 2012, pp. 531 – 539.

[72] S. Bhattacharya and K. Pradeep Kumar, “Decoy-pulse protocol for frequency-coded quantum key distribution,” in *Communications (NCC), 2012 National Conference on.* IEEE, 2012, pp. 1–4.

[73] J. Capmany and C. R. Fernández-Pousa, “Optimum design for bb84 quantum key distribution in tree-type passive optical networks,” *JOSA B*, vol. 27, no. 6, pp. A146–A151, 2010.

[74] M. Cen, “Study on supervision of wavelength division multiplexing passive optical network systems,” Ph.D. dissertation, KTH, 2011.

[75] F. Chen-Xu, J. Rong-Zhen, and Z. Wen-Han, “Performance of differential-phase-shift keying protocol applying 1310 nm up-conversion single-photon detector,” *Chinese Physics Letters*, vol. 25, no. 9, p. 3135, 2008.

[76] I. Choi, R. J. Young, and P. D. Townsend, “Quantum information to the home,” *New Journal of Physics*, vol. 13, no. 6, p. 063039, 2011.

[77] I. P. Choi and P. D. Townsend, “Quantum key distribution on a 10Gb/s WDM-PON,” in *Optical Fiber Communication Conference.* Optical Society of America, 2010.

[78] ETSI, “Quantum key distribution (qkd); use cases,” ETSI Industry Specification (ISG) Group Quantum Key Distribution, Tech. Rep., 2010.

[79] D. Harkins and D. Carrel, “The internet key exchange (IKE),” Internet Engineering Task Force, RFC 2409, Nov. 1998. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2409.txt

[80] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. H. Hadfield *et al.*, “Entanglement-based bbm92 qkd experiment

using superconducting single photon detectors," in *Quantum Electronics and Laser Science Conference*. Optical Society of America, 2008.

[81] H. Kawahara, A. Medhipour, and K. Inoue, "Effect of spontaneous raman scattering on quantum channel wavelength-multiplexed with classical channel," *Optics Communications*, vol. 284, no. 2, pp. 691–696, 2011.

[82] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *Journal of lightwave technology*, vol. 23, no. 1, p. 268, 2005.

[83] C. Liang, K. F. Lee, J. Chen, and P. Kumar, "Distribution of fiber-generated polarization entangled photon-pairs over 100 km of standard fiber in oc-192 wdm environment," in *Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference. OFC 2006.* IEEE, 2006, pp. 1–3.

[84] Q. Lin, F. Yaman, and G. P. Agrawal, "Photon-pair generation in optical fibers through four-wave mixing: Role of raman scattering and pump polarization," *Physical Review A*, vol. 75, no. 2, p. 023803, 2007.

[85] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, "Experimental quantum key distribution based on a bell test," *Physical Review A*, vol. 78, no. 2, p. 20301, 2008.

[86] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005.

[87] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[88] M. Maier, "Wdm passive optical networks and beyond: The road ahead," in *J. Opt. Commun. Netw.*, vol. 1, no. 4, 2009, pp. C1–C16.

[89] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, "Faraday-michelson system for quantum cryptography," *Optics Letters*, vol. 30, no. 19, pp. 2632–2634, 2005.

[90] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. G. Muñoz, and J. Capmany, "Simultaneous transmission of 20x2 wdm/scm-qkd and 4 bidirectional classical channels over a pon," *Optics Express*, vol. 20, no. 15, pp. 16 358–16 365, 2012.

[91] S.-G. Mun, J.-H. Moon, H.-K. Lee, J.-Y. Kim, and C.-H. Lee, "A wdm-pon with a 40 gb/s (32 x 1.25 gb/s) capacity based on wavelength-locked fabry-perot laser diodes," *Opt. Express*, vol. 16, no. 15, pp. 11 361–11 368, 2008.

[92] N. R. Newbury, "Pump-wavelength dependence of raman gain in single-mode optical fibers," *Journal of lightwave technology*, vol. 21, no. 12, p. 3364, 2003.

[93] J. Oh, C. Antonelli, and M. Brodsky, "Coincidence rates for photon pairs in wdm environment," *Journal of Lightwave Technology*, vol. 29, no. 3, pp. 324–329, 2011.

[94] P. Ossieur, C.Antony, A. M. C. andA.Naughton, H.-G. Krimmel, Y. Chang, C. Ford, A. Borghesani, D. G. Moodie, A. Poustie, R.Wyatt, B. Harmon, I. Lealman, G. Maxwell, D. Rogers, D. W. Smith, D. Nesset, R. P. Davey, and P. D. Townsend, "A 135-km 8192-split carrier distributed dwdm-tdma pon with 2 32 10 gb/s capacity," in *J. Lightw. Technol.*, vol. 29, no. 4, February 2011, pp. 463–474.

[95] M. Peev, C. Pacher, R. Allaume, and A. Zeilinger, "The secoqc quantum key distribution network in vienna," in *New Journal of Physics*, vol. 11, 2011.

[96] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter *et al.*, "Practical quantum key distribution with polarization entangled photons," *Optics Express*, vol. 12, no. 16, pp. 3865–3871, 2004.

[97] M. Razavi, "Multiple-access quantum key distribution networks," *Communications, IEEE Transactions on*, vol. 60, no. 10, pp. 3071–3079, 2012.

[98] P. L. K. Reddy, B. R. B. Reddy, and S. R. Krishna, "Multi-user quantum key distribution using wavelength division multiplexing," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 4, no. 6, p. 43, 2012.

[99] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[100] B. Schrenk, J. Lazaro, D. Klonidis, F. Bonada, F. Saliou, V. Polo, E. Lopez, Q. Le, P. Chanclou, L. Costa, A. Teixeira, S. Chatzi, I. Tomkos, G. T. Beleffi, D. Leino, R. Soila, S. Spirou, G. de Valicourt, R. Brenot, C. Kazmierski, and J. Prat, "Demonstration of a remotely dual-pumped long-reach PON for flexible deployment," in *IEEE/OSA J. Lightwave Technol.*, vol. 30, April 2012, pp. 953–961.

[101] K. V. Shrikhande, I. M. White, D.-r. Wonglumsom, S. M. Gemelos, M. S. Rogge, Y. Fukashiro, M. Avenarius, and L. G. Kazovsky, "Hornet: A packet-over-wdm multiple access metropolitan area ring network," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 10, pp. 2004–2016, 2000.

[102] N. A. Silva, . J. Almeida, and A. N. Pinto, "Interference in a quantum channel due to classical four-wave mixing in optical fibers," *Quantum Electronics, IEEE Journal of*, vol. 48, no. 4, pp. 472–479, 2012.

[103] X. Tank, L. Ma, A. Mink, T. Chang, H. Xu, O. Slattery, A. Nakassis, B. Hershman, D. Su, and R. F. Boisvert, "High-speed quantum key distribution systems for optical fiber networks in campus and metro areas," DTIC Document, Tech. Rep., 2008.

[104] G. Xavier and J. Von der Weid, "Limitations for transmission of photonic qubits in optical fibres carrying telecom traffic," *Electronics letters*, vol. 46, no. 15, pp. 1071–1072, 2010.

[105] S. Yao, S. B. Yoo, B. Mukherjee, and S. Dixit, "All-optical packet switching for metropolitan area networks: opportunities and challenges," *Communications Magazine, IEEE*, vol. 39, no. 3, pp. 142–148, 2001.

[106] Y. Zhao, M. Roetteler, L. Xu, and T. Wang, "Design of synchronous plug & play QKD-WDM-PON for efficient quantum communications," in *CLEO: Science and Innovations*. Optical Society of America, 2011.

Publications

[AWP$^+$13a] S. Aleksic, D. Winkler, A. Poppe, B. Schrenk, and F. Hipp. Distribution of quantum keys in optically transparent networks: Perspectives, limitations and challenges. In *ICTON 2013*, Cartagena, Spain, June 2013.

[AWP$^+$13b] Slavisa Aleksic, Dominic Winkler, Andreas Poppe, Bernhard Schrenk, and Florian Hipp. Quantum key distribution over optical access networks. In *NOC/OC&I 2013*, Graz, Austria, July 2013.

A Annex

A.1 Simulation Parameters

A.1.1 Universal Fiber

Parameter name	Type	Value	Dimension
`Attenuation`	file	`Attenuation.dat (see A.5)`	$^{dB}/_{m}$
`Dispersion`	value	`16e-6`	$^{s}/_{m^2}$
`DispersionSlope`	value	`0.08e3`	$^{s}/_{m^3}$
`RamanGain`	file	`RamanGain-SMF28-NIST.prn (see A.6)`	$^{1}/_{Wm}$
`RamanAdjustmentFactors`	value	`0.5`	–
`RamanFraction`	value	`0.17`	–
`SBSBandwidth`	value	`100e6`	Hz
`SBSStokesShift`	value	`11e9`	Hz
`SBSGain`	value	`4.6e-11`	$^{m}/_{W}$
`FWMThreshold`	value	`-30.0`	dBm
`SBSThresholdFactor`	value	`10`	–
`Temperature`	value	`300`	K
`NonLinearIndex`	value	`2.6e-20`	$^{m^2}/_{W}$
`CoreArea`	value	`72.8e-12`	m^2
`RayleighBackscatterCoefficient`	value	`-80.0`	dB
`NoiseBinResolution`	value	`100e9`	Hz
`NoiseBinStart`	value	`1200e-9`	m
`NoiseBinEnd`	value	`1660e-9`	m

Table A.1: Parameters of the `UniversalFiber` module

A.1.2 EDFA

Parameter name	Type	Value	Dimension
`1st Stage Laser Power`	value	`80e-3`	W
`1st Doped Fiber Length`	value	`8`	m
`2nd Stage Laser Power`	value	`25e-3`	W
`2nd Doped Fiber Length`	value	`35`	m

Table A.2: Parameters of the EDFA galaxy

A.1.3 OXC

Parameter name	Type	Value	Dimension
InsertionLoss	value	0.5	dB
CrossTalk	value	30	dB
PhaseShift	value	0	–
Bandwidth	value	25e9	Hz

Table A.3: Parameters of the OXC galaxy

A.1.4 QKD System

Parameter name	Symbol	Value	Dimension
Quantum Efficency	η	0.07	–
Gate Length	t_{gate}	1.50E-09	sec
Pulse Rate	f_{rep}	5.00E+06	Hz
Detector Number	n_{det}	2	–
Dark Count Probability	P_{dc}	5.00E-06	$^1/_{ns}$
After Pulse Probability	P_{AP}	0.008	–
Detector Losses	L_{det}	2.65	dB
Path Losses	L_{path}	from scenario	dB
Dead Time	t_{dead}	1.00E-05	sec
Mean Photon Number per pulse	μ	auto	–
Duty Line (p-n-p system)	L_s	0	m
Error Correction factor	η_{ec}	1.2	–
Visibility	V	0.98	–

Table A.4: QKD system parameters used for background noise post-processing

A.2 Simulation Data Files

A.2.1 Attenuation.dat

Table A.5: Attenuation of SMF-28 optical fiber

Wavelength $[nm]$	Attenuation $[\frac{dB}{km}]$
1004.3	1.081
1005.2	1.079
1006.1	1.079
1006.9	1.074
1007.8	1.070
1008.7	1.070
1009.6	1.068
1010.4	1.065
1011.3	1.061
1012.2	1.056
1013	1.054
1013.9	1.050
1014.8	1.045
1015.6	1.036
1016.5	1.032
1017.4	1.029
1018.2	1.027
1019.1	1.023
1020	1.018
1020.8	1.016
1021.7	1.014
1022.6	1.009
1023.4	1.005
1024.3	1.005
1025.2	1.000
1026.1	0.995
1026.9	0.993
1027.8	0.991
1028.7	0.986
1029.5	0.984
1030.4	0.982
1031.3	0.977
1032.1	0.973
1033	0.973
1033.9	0.968
1034.7	0.964
1035.6	0.964
1036.5	0.962
1037.3	0.957
1038.2	0.955
1039.1	0.953
1040	0.948
1040.8	0.948
1041.7	0.941
1042.6	0.939
1043.4	0.937
1044.3	0.932
1045.2	0.930
1046	0.928
1046.9	0.923
1047.8	0.921
1048.6	0.919
1049.5	0.914
1050.4	0.914
1051.2	0.910
1052.1	0.907
1053	0.905
1053.8	0.901
1054.7	0.898
1055.6	0.896
1056.5	0.892
1057.3	0.892
1058.2	0.887
1059.1	0.885
1059.9	0.883
1060.8	0.878
1061.7	0.878
1062.5	0.874
1063.4	0.871
1064.3	0.869
1065.1	0.865
1066	0.865
1066.9	0.860
1067.7	0.858
1068.6	0.856
1069.5	0.851
1070.3	0.851
1071.2	0.847
1072.1	0.847
1073	0.842
1073.8	0.840
1074.7	0.837
1075.6	0.833
1076.4	0.833
1077.3	0.828
1078.2	0.828
1079	0.824
1079.9	0.819
1080.8	0.819

Wavelength $[nm]$	Attenuation $[\frac{dB}{km}]$
1081.6	0.815
1082.5	0.815
1083.4	0.810
1084.2	0.810
1085.1	0.806
1086	0.804
1086.8	0.801
1087.7	0.797
1088.6	0.797
1089.5	0.792
1090.3	0.792
1091.2	0.788
1092.1	0.788
1092.9	0.783
1093.8	0.781
1094.7	0.781
1095.5	0.779
1096.4	0.779
1097.3	0.770
1098.1	0.770
1099	0.770
1099.9	0.765
1100.7	0.765
1101.6	0.761
1102.5	0.758
1103.3	0.754
1104.2	0.752
1105.1	0.747
1106	0.747
1106.8	0.743
1107.7	0.743
1108.6	0.738
1109.4	0.738
1110.3	0.734
1111.2	0.734
1112	0.729
1112.9	0.729
1113.8	0.725
1114.6	0.725
1115.5	0.720
1116.4	0.720
1117.2	0.716
1118.1	0.713
1119	0.711
1119.9	0.709
1120.7	0.707
1121.6	0.704
1122.5	0.702
1123.3	0.700
1124.2	0.698
1125.1	0.695
1125.9	0.693
1126.8	0.691
1127.7	0.688
1128.5	0.686
1129.4	0.684
1130.3	0.682
1131.1	0.679
1132	0.677
1132.9	0.675
1133.7	0.673
1134.6	0.670
1135.5	0.668
1136.4	0.666
1137.2	0.664
1138.1	0.661
1139	0.659
1139.8	0.657
1140.7	0.655
1141.6	0.652
1142.4	0.650
1143.3	0.648
1144.2	0.646
1145	0.643
1145.9	0.641
1146.8	0.639
1147.6	0.637
1148.5	0.634
1149.4	0.632
1150.2	0.630
1151.1	0.628
1152	0.625
1152.9	0.623
1153.7	0.621
1154.6	0.621
1155.5	0.619
1156.3	0.616
1157.2	0.614
1158.1	0.612
1158.9	0.609

Wavelength	Attenuation
$[nm]$	$[\frac{dB}{km}]$
1159.8	0.607
1160.7	0.605
1161.5	0.603
1162.4	0.600
1163.3	0.598
1164.1	0.596
1165	0.594
1165.9	0.591
1166.7	0.589
1167.6	0.587
1168.5	0.587
1169.4	0.585
1170.2	0.582
1171.1	0.580
1172	0.578
1172.8	0.576
1173.7	0.573
1174.6	0.571
1175.4	0.569
1176.3	0.569
1177.2	0.564
1178	0.564
1178.9	0.560
1179.8	0.560
1180.6	0.558
1181.5	0.555
1182.4	0.553
1183.3	0.551
1184.1	0.551
1185	0.546
1185.9	0.546
1186.7	0.542
1187.6	0.542
1188.5	0.537
1189.3	0.537
1190.2	0.537
1191.1	0.533
1191.9	0.530
1192.8	0.528
1193.7	0.526
1194.5	0.524
1195.4	0.524
1196.3	0.521
1197.1	0.521
1198	0.519
1198.9	0.517
1199.8	0.515
1200.6	0.515
1201.5	0.515
1202.4	0.512
1203.2	0.510
1204.1	0.506
1205	0.503
1205.8	0.501
1206.7	0.501
1207.6	0.497
1208.4	0.497
1209.3	0.492
1210.2	0.492
1211	0.492
1211.9	0.488
1212.8	0.488
1213.6	0.483
1214.5	0.483
1215.4	0.481
1216.3	0.479
1217.1	0.479
1218	0.474
1218.9	0.474
1219.7	0.472
1220.6	0.470
1221.5	0.470
1222.3	0.465
1223.2	0.465
1224.1	0.463
1224.9	0.460
1225.8	0.460
1226.7	0.458
1227.5	0.456
1228.4	0.456
1229.3	0.451
1230.1	0.451
1231	0.449
1231.9	0.447
1232.8	0.447
1233.6	0.445
1234.5	0.442
1235.4	0.440
1236.2	0.438
1237.1	0.438

Wavelength [nm]	Attenuation [$\frac{dB}{km}$]
1238	0.436
1238.8	0.433
1239.7	0.433
1240.6	0.431
1241.4	0.429
1242.3	0.427
1243.2	0.427
1244	0.424
1244.9	0.422
1245.8	0.420
1246.7	0.420
1247.5	0.418
1248.4	0.415
1249.3	0.415
1250.1	0.413
1251	0.411
1251.9	0.411
1252.7	0.409
1253.6	0.406
1254.5	0.404
1255.3	0.404
1256.2	0.402
1257.1	0.400
1257.9	0.400
1258.8	0.397
1259.7	0.395
1260.5	0.395
1261.4	0.393
1262.3	0.391
1263.2	0.391
1264	0.388
1264.9	0.386
1265.8	0.386
1266.6	0.384
1267.5	0.381
1268.4	0.381
1269.2	0.379
1270.1	0.377
1271	0.377
1271.8	0.375
1272.7	0.372
1273.6	0.370
1274.4	0.370
1275.3	0.368
1276.2	0.368
1277	0.366
1277.9	0.363
1278.8	0.361
1279.7	0.361
1280.5	0.361
1281.4	0.359
1282.3	0.357
1283.1	0.357
1284	0.354
1284.9	0.352
1285.7	0.352
1286.6	0.352
1287.5	0.350
1288.3	0.350
1289.2	0.350
1290.1	0.350
1290.9	0.345
1291.8	0.345
1292.7	0.343
1293.5	0.343
1294.4	0.341
1295.3	0.341
1296.2	0.341
1297	0.339
1297.9	0.339
1298.8	0.336
1299.6	0.334
1300.5	0.332
1301.4	0.332
1302.2	0.332
1303.1	0.332
1304	0.330
1304.8	0.327
1305.7	0.327
1306.6	0.327
1307.4	0.327
1308.3	0.323
1309.2	0.323
1310	0.323
1310.9	0.323
1311.8	0.321
1312.7	0.318
1313.5	0.318
1314.4	0.318
1315.3	0.318

Wavelength [nm]	Attenuation [$\frac{dB}{km}$]
1316.1	0.316
1317	0.314
1317.9	0.314
1318.7	0.314
1319.6	0.314
1320.5	0.312
1321.3	0.312
1322.2	0.309
1323.1	0.309
1323.9	0.309
1324.8	0.309
1325.7	0.307
1326.6	0.307
1327.4	0.305
1328.3	0.305
1329.2	0.305
1330	0.305
1330.9	0.305
1331.8	0.302
1332.6	0.302
1333.5	0.300
1334.4	0.300
1335.2	0.300
1336.1	0.300
1337	0.300
1337.8	0.300
1338.7	0.300
1339.6	0.298
1340.4	0.298
1341.3	0.298
1342.2	0.296
1343.1	0.296
1343.9	0.296
1344.8	0.296
1345.7	0.296
1346.5	0.296
1347.4	0.296
1348.3	0.296
1349.1	0.296
1350	0.296
1350.9	0.296
1351.7	0.298
1352.6	0.302
1353.5	0.307
1354.3	0.314
1355.2	0.321
1356.1	0.330
1356.9	0.334
1357.8	0.339
1358.7	0.343
1359.6	0.345
1360.4	0.350
1361.3	0.350
1362.2	0.354
1363	0.357
1363.9	0.361
1364.8	0.363
1365.6	0.368
1366.5	0.370
1367.4	0.375
1368.2	0.381
1369.1	0.388
1370	0.397
1370.8	0.402
1371.7	0.402
1372.6	0.400
1373.4	0.400
1374.3	0.400
1375.2	0.400
1376.1	0.395
1376.9	0.395
1377.8	0.395
1378.7	0.391
1379.5	0.391
1380.4	0.388
1381.3	0.386
1382.1	0.384
1383	0.379
1383.9	0.379
1384.7	0.375
1385.6	0.375
1386.5	0.370
1387.3	0.368
1388.2	0.366
1389.1	0.361
1390	0.361
1390.8	0.357
1391.7	0.357
1392.6	0.352
1393.4	0.348

Wavelength [nm]	Attenuation [$\frac{dB}{km}$]
1394.3	0.348
1395.2	0.343
1396	0.343
1396.9	0.339
1397.8	0.336
1398.6	0.330
1399.5	0.327
1400.4	0.327
1401.2	0.327
1402.1	0.325
1403	0.325
1403.8	0.321
1404.7	0.321
1405.6	0.318
1406.5	0.316
1407.3	0.314
1408.2	0.312
1409.1	0.309
1409.9	0.307
1410.8	0.305
1411.7	0.302
1412.5	0.302
1413.4	0.300
1414.3	0.298
1415.1	0.296
1416	0.293
1416.9	0.291
1417.7	0.291
1418.6	0.289
1419.5	0.287
1420.3	0.287
1421.2	0.284
1422.1	0.282
1423	0.280
1423.8	0.278
1424.7	0.278
1425.6	0.275
1426.4	0.273
1427.3	0.273
1428.2	0.271
1429	0.269
1429.9	0.269
1430.8	0.266
1431.6	0.264
1432.5	0.264
1433.4	0.262
1434.2	0.262
1435.1	0.260
1436	0.257
1436.8	0.257
1437.7	0.255
1438.6	0.255
1439.5	0.253
1440.3	0.251
1441.2	0.251
1442.1	0.248
1442.9	0.248
1443.8	0.246
1444.7	0.246
1445.5	0.244
1446.4	0.244
1447.3	0.242
1448.1	0.242
1449	0.239
1449.9	0.239
1450.7	0.237
1451.6	0.237
1452.5	0.235
1453.3	0.235
1454.2	0.233
1455.1	0.233
1456	0.230
1456.8	0.230
1457.7	0.230
1458.6	0.228
1459.4	0.226
1460.3	0.226
1461.2	0.226
1462	0.223
1462.9	0.223
1463.8	0.221
1464.6	0.221
1465.5	0.221
1466.4	0.221
1467.2	0.219
1468.1	0.217
1469	0.217
1469.9	0.217
1470.7	0.217
1471.6	0.214

Wavelength $[nm]$	Attenuation $[\frac{dB}{km}]$
1472.5	0.214
1473.3	0.212
1474.2	0.212
1475.1	0.212
1475.9	0.212
1476.8	0.212
1477.7	0.208
1478.5	0.208
1479.4	0.208
1480.3	0.208
1481.1	0.208
1482	0.208
1482.9	0.208
1483.7	0.203
1484.6	0.203
1485.5	0.203
1486.4	0.203
1487.2	0.203
1488.1	0.203
1489	0.196
1489.8	0.194
1490.7	0.194
1491.6	0.194
1492.4	0.194
1493.3	0.194
1494.2	0.194
1495	0.194
1495.9	0.194
1496.8	0.194
1497.6	0.192
1498.5	0.192
1499.4	0.192
1500.2	0.192
1501.1	0.192
1502	0.192
1502.9	0.192
1503.7	0.192
1504.6	0.192
1505.5	0.192
1506.3	0.190
1507.2	0.190
1508.1	0.190
1508.9	0.190
1509.8	0.190
1510.7	0.190
1511.5	0.190
1512.4	0.190
1513.3	0.190
1514.1	0.190
1515	0.190
1515.9	0.190
1516.7	0.190
1517.6	0.190
1518.5	0.190
1519.4	0.187
1520.2	0.187
1521.1	0.187
1522	0.187
1522.8	0.187
1523.7	0.187
1524.6	0.187
1525.4	0.187
1526.3	0.187
1527.2	0.187
1528	0.187
1528.9	0.187
1529.8	0.187
1530.6	0.187
1531.5	0.187
1532.4	0.187
1533.3	0.187
1534.1	0.187
1535	0.187
1535.9	0.187
1536.7	0.187
1537.6	0.187
1538.5	0.187
1539.3	0.187
1540.2	0.187
1541.1	0.187
1541.9	0.187
1542.8	0.187
1543.7	0.187
1544.5	0.187
1545.4	0.187
1546.3	0.187
1547.1	0.187
1548	0.187
1548.9	0.187
1549.8	0.187

Wavelength $[nm]$	Attenuation $[\frac{dB}{km}]$
1550.6	0.187
1551.5	0.187
1552.4	0.187
1553.2	0.187
1554.1	0.187
1555	0.187
1555.8	0.187
1556.7	0.190
1557.6	0.190
1558.4	0.192
1559.3	0.192
1560.2	0.192
1561	0.192
1561.9	0.192
1562.8	0.192
1563.6	0.192
1564.5	0.192
1565.4	0.192
1566.3	0.192
1567.1	0.192
1568	0.194
1568.9	0.194
1569.7	0.194
1570.6	0.194
1571.5	0.196
1572.3	0.196
1573.2	0.196
1574.1	0.196
1574.9	0.196
1575.8	0.196
1576.7	0.199
1577.5	0.199
1578.4	0.199
1579.3	0.199
1580.1	0.201
1581	0.201
1581.9	0.201
1582.8	0.201
1583.6	0.203
1584.5	0.203
1585.4	0.203
1586.2	0.203
1587.1	0.203
1588	0.205
1588.8	0.205
1589.7	0.208
1590.6	0.208
1591.4	0.208
1592.3	0.208
1593.2	0.208
1594	0.210
1594.9	0.212
1595.8	0.212
1596.7	0.212
1597.5	0.212
1598.4	0.214
1599.3	0.214
1600.1	0.214
1601	0.214
1601.9	0.217
1602.7	0.217
1603.6	0.217
1604.5	0.219
1605.3	0.221
1606.2	0.221
1607.1	0.221
1607.9	0.221
1608.8	0.223
1609.7	0.226
1610.5	0.226
1611.4	0.226
1612.3	0.226
1613.2	0.230
1614	0.230
1614.9	0.230
1615.8	0.230
1616.6	0.230
1617.5	0.235
1618.4	0.235
1619.2	0.235
1620.1	0.235
1621	0.239
1621.8	0.239
1622.7	0.239
1623.6	0.239
1624.4	0.242
1625.3	0.244
1626.2	0.244
1627	0.244
1627.9	0.246

Wavelength $[nm]$	Attenuation $[\frac{dB}{km}]$
1628.8	0.248
1629.7	0.248
1630.5	0.251
1631.4	0.253
1632.3	0.253
1633.1	0.253
1634	0.255
1634.9	0.257
1635.7	0.257
1636.6	0.260
1637.5	0.262
1638.3	0.262
1639.2	0.264
1640.1	0.264
1640.9	0.266
1641.8	0.266
1642.7	0.269
1643.5	0.271
1644.4	0.271
1645.3	0.273
1646.2	0.275
1647	0.275
1647.9	0.278
1648.8	0.280
1649.6	0.282
1650.5	0.282
1651.4	0.284
1652.2	0.287
1653.1	0.287
1654	0.289
1654.8	0.291
1655.7	0.291
1656.6	0.293
1657.4	0.296
1658.3	0.298
1659.2	0.300
1660	0.300
1660.9	0.302
1661.8	0.305
1662.7	0.307
1663.5	0.309
1664.4	0.309
1665.3	0.314
1666.1	0.314
1667	0.316
1667.9	0.318
1668.7	0.318
1669.6	0.323
1670.5	0.323
1671.3	0.327
1672.2	0.327
1673.1	0.332
1673.9	0.332
1674.8	0.336
1675.7	0.336
1676.6	0.341
1677.4	0.341
1678.3	0.345
1679.2	0.345
1680	0.350
1680.9	0.350
1681.8	0.354
1682.6	0.354
1683.5	0.359
1684.4	0.359
1685.2	0.363
1686.1	0.363
1687	0.368
1687.8	0.368
1688.7	0.372
1689.6	0.375
1690.4	0.377
1691.3	0.379
1692.2	0.381
1693.1	0.386
1693.9	0.386
1694.8	0.391
1695.7	0.393
1696.5	0.395
1697.4	0.400
1698.3	0.400
1699.1	0.404
1700	0.404
1700.9	0.406
1701.7	0.409

A.2.2 `RamanGain-SMF28-NIST.prn`

Table A.6: Raman Gain in SMF-28 fibers with a pump wavelength of 1486 nm

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
0.00E+00	0.000E+00
5.00E+10	1.224E-06
1.00E+11	2.451E-06
1.50E+11	3.687E-06
2.00E+11	4.935E-06
2.50E+11	6.199E-06
3.00E+11	7.483E-06
3.50E+11	8.790E-06
4.00E+11	1.012E-05
4.50E+11	1.149E-05
5.00E+11	1.289E-05
5.50E+11	1.432E-05
6.00E+11	1.579E-05
6.50E+11	1.730E-05
7.00E+11	1.885E-05
7.50E+11	2.044E-05
8.00E+11	2.207E-05
8.50E+11	2.374E-05
9.00E+11	2.545E-05
9.50E+11	2.719E-05
1.00E+12	2.897E-05
1.05E+12	3.077E-05
1.10E+12	3.259E-05
1.15E+12	3.444E-05
1.20E+12	3.629E-05
1.25E+12	3.815E-05
1.30E+12	4.000E-05
1.35E+12	4.185E-05
1.40E+12	4.368E-05
1.45E+12	4.548E-05
1.50E+12	4.726E-05
1.55E+12	4.901E-05
1.60E+12	5.071E-05
1.65E+12	5.237E-05
1.70E+12	5.399E-05
1.75E+12	5.556E-05
1.80E+12	5.707E-05
1.85E+12	5.853E-05
1.90E+12	5.995E-05
1.95E+12	6.131E-05
2.00E+12	6.262E-05
2.05E+12	6.389E-05
2.10E+12	6.512E-05
2.15E+12	6.631E-05
2.20E+12	6.746E-05
2.25E+12	6.858E-05
2.30E+12	6.967E-05
2.35E+12	7.073E-05
2.40E+12	7.177E-05
2.45E+12	7.279E-05
2.50E+12	7.379E-05
2.55E+12	7.477E-05
2.60E+12	7.574E-05
2.65E+12	7.668E-05
2.70E+12	7.761E-05
2.75E+12	7.853E-05
2.80E+12	7.942E-05
2.85E+12	8.030E-05
2.90E+12	8.116E-05
2.95E+12	8.200E-05
3.00E+12	8.282E-05
3.05E+12	8.362E-05
3.10E+12	8.439E-05
3.15E+12	8.514E-05
3.20E+12	8.587E-05
3.25E+12	8.657E-05
3.30E+12	8.725E-05
3.35E+12	8.791E-05
3.40E+12	8.854E-05
3.45E+12	8.915E-05
3.50E+12	8.974E-05
3.55E+12	9.031E-05
3.60E+12	9.086E-05
3.65E+12	9.140E-05
3.70E+12	9.192E-05
3.75E+12	9.243E-05
3.80E+12	9.293E-05
3.85E+12	9.342E-05
3.90E+12	9.390E-05
3.95E+12	9.439E-05
4.00E+12	9.488E-05
4.05E+12	9.536E-05
4.10E+12	9.586E-05
4.15E+12	9.636E-05
4.20E+12	9.687E-05
4.25E+12	9.740E-05
4.30E+12	9.794E-05
4.35E+12	9.850E-05
4.40E+12	9.908E-05
4.45E+12	9.968E-05
4.50E+12	1.003E-04
4.55E+12	1.010E-04

Frequency Offset $[Hz]$	Raman Gain $[\frac{1}{mW}]$
4.60E+12	1.016E-04
4.65E+12	1.023E-04
4.70E+12	1.031E-04
4.75E+12	1.038E-04
4.80E+12	1.046E-04
4.85E+12	1.054E-04
4.90E+12	1.063E-04
4.95E+12	1.072E-04
5.00E+12	1.081E-04
5.05E+12	1.090E-04
5.10E+12	1.100E-04
5.15E+12	1.110E-04
5.20E+12	1.121E-04
5.25E+12	1.131E-04
5.30E+12	1.142E-04
5.35E+12	1.154E-04
5.40E+12	1.165E-04
5.45E+12	1.177E-04
5.50E+12	1.189E-04
5.55E+12	1.201E-04
5.60E+12	1.213E-04
5.65E+12	1.226E-04
5.70E+12	1.239E-04
5.75E+12	1.252E-04
5.80E+12	1.265E-04
5.85E+12	1.279E-04
5.90E+12	1.292E-04
5.95E+12	1.306E-04
6.00E+12	1.319E-04
6.05E+12	1.333E-04
6.10E+12	1.347E-04
6.15E+12	1.361E-04
6.20E+12	1.375E-04
6.25E+12	1.389E-04
6.30E+12	1.404E-04
6.35E+12	1.418E-04
6.40E+12	1.432E-04
6.45E+12	1.446E-04
6.50E+12	1.461E-04
6.55E+12	1.475E-04
6.60E+12	1.490E-04
6.65E+12	1.504E-04
6.70E+12	1.518E-04
6.75E+12	1.533E-04
6.80E+12	1.547E-04
6.85E+12	1.562E-04
6.90E+12	1.576E-04
6.95E+12	1.591E-04
7.00E+12	1.605E-04
7.05E+12	1.620E-04
7.10E+12	1.635E-04
7.15E+12	1.649E-04
7.20E+12	1.664E-04
7.25E+12	1.679E-04
7.30E+12	1.694E-04
7.35E+12	1.709E-04
7.40E+12	1.724E-04
7.45E+12	1.739E-04
7.50E+12	1.754E-04
7.55E+12	1.770E-04
7.60E+12	1.785E-04
7.65E+12	1.801E-04
7.70E+12	1.817E-04
7.75E+12	1.832E-04
7.80E+12	1.849E-04
7.85E+12	1.865E-04
7.90E+12	1.881E-04
7.95E+12	1.898E-04
8.00E+12	1.915E-04
8.05E+12	1.932E-04
8.10E+12	1.949E-04
8.15E+12	1.966E-04
8.20E+12	1.984E-04
8.25E+12	2.002E-04
8.30E+12	2.020E-04
8.35E+12	2.038E-04
8.40E+12	2.057E-04
8.45E+12	2.076E-04
8.50E+12	2.095E-04
8.55E+12	2.114E-04
8.60E+12	2.133E-04
8.65E+12	2.153E-04
8.70E+12	2.173E-04
8.75E+12	2.193E-04
8.80E+12	2.213E-04
8.85E+12	2.234E-04
8.90E+12	2.254E-04
8.95E+12	2.275E-04
9.00E+12	2.296E-04
9.05E+12	2.317E-04
9.10E+12	2.338E-04
9.15E+12	2.360E-04
9.20E+12	2.381E-04

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
9.25E+12	2.403E-04
9.30E+12	2.425E-04
9.35E+12	2.447E-04
9.40E+12	2.468E-04
9.45E+12	2.490E-04
9.50E+12	2.512E-04
9.55E+12	2.534E-04
9.60E+12	2.556E-04
9.65E+12	2.578E-04
9.70E+12	2.600E-04
9.75E+12	2.622E-04
9.80E+12	2.644E-04
9.85E+12	2.666E-04
9.90E+12	2.688E-04
9.95E+12	2.709E-04
1.00E+13	2.731E-04
1.01E+13	2.753E-04
1.01E+13	2.774E-04
1.02E+13	2.795E-04
1.02E+13	2.817E-04
1.03E+13	2.838E-04
1.03E+13	2.859E-04
1.04E+13	2.879E-04
1.04E+13	2.900E-04
1.05E+13	2.921E-04
1.05E+13	2.941E-04
1.06E+13	2.962E-04
1.06E+13	2.982E-04
1.07E+13	3.002E-04
1.07E+13	3.022E-04
1.08E+13	3.042E-04
1.08E+13	3.062E-04
1.09E+13	3.082E-04
1.09E+13	3.101E-04
1.10E+13	3.121E-04
1.10E+13	3.141E-04
1.11E+13	3.160E-04
1.11E+13	3.180E-04
1.12E+13	3.199E-04
1.12E+13	3.218E-04
1.13E+13	3.238E-04
1.13E+13	3.257E-04
1.14E+13	3.276E-04
1.14E+13	3.295E-04
1.15E+13	3.315E-04
1.15E+13	3.334E-04
1.16E+13	3.353E-04
1.16E+13	3.372E-04
1.17E+13	3.391E-04
1.17E+13	3.410E-04
1.18E+13	3.429E-04
1.18E+13	3.448E-04
1.19E+13	3.467E-04
1.19E+13	3.485E-04
1.20E+13	3.504E-04
1.20E+13	3.522E-04
1.21E+13	3.540E-04
1.21E+13	3.558E-04
1.22E+13	3.576E-04
1.22E+13	3.593E-04
1.23E+13	3.610E-04
1.23E+13	3.627E-04
1.24E+13	3.643E-04
1.24E+13	3.659E-04
1.25E+13	3.674E-04
1.25E+13	3.688E-04
1.26E+13	3.702E-04
1.26E+13	3.716E-04
1.27E+13	3.728E-04
1.27E+13	3.740E-04
1.28E+13	3.751E-04
1.28E+13	3.761E-04
1.29E+13	3.770E-04
1.29E+13	3.778E-04
1.30E+13	3.785E-04
1.30E+13	3.790E-04
1.31E+13	3.795E-04
1.31E+13	3.798E-04
1.32E+13	3.800E-04
1.32E+13	3.801E-04
1.33E+13	3.800E-04
1.33E+13	3.797E-04
1.34E+13	3.794E-04
1.34E+13	3.789E-04
1.35E+13	3.782E-04
1.35E+13	3.773E-04
1.36E+13	3.764E-04
1.36E+13	3.752E-04
1.37E+13	3.739E-04
1.37E+13	3.725E-04
1.38E+13	3.709E-04
1.38E+13	3.693E-04
1.39E+13	3.675E-04

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
1.39E+13	3.656E-04
1.40E+13	3.636E-04
1.40E+13	3.617E-04
1.41E+13	3.598E-04
1.41E+13	3.581E-04
1.42E+13	3.565E-04
1.42E+13	3.553E-04
1.43E+13	3.546E-04
1.43E+13	3.545E-04
1.44E+13	3.551E-04
1.44E+13	3.565E-04
1.45E+13	3.588E-04
1.45E+13	3.618E-04
1.46E+13	3.653E-04
1.46E+13	3.692E-04
1.47E+13	3.730E-04
1.47E+13	3.761E-04
1.48E+13	3.782E-04
1.48E+13	3.785E-04
1.49E+13	3.768E-04
1.49E+13	3.727E-04
1.50E+13	3.662E-04
1.50E+13	3.573E-04
1.51E+13	3.464E-04
1.51E+13	3.339E-04
1.52E+13	3.203E-04
1.52E+13	3.062E-04
1.53E+13	2.922E-04
1.53E+13	2.785E-04
1.54E+13	2.655E-04
1.54E+13	2.535E-04
1.55E+13	2.425E-04
1.55E+13	2.324E-04
1.56E+13	2.232E-04
1.56E+13	2.149E-04
1.57E+13	2.072E-04
1.57E+13	2.001E-04
1.58E+13	1.935E-04
1.58E+13	1.872E-04
1.59E+13	1.812E-04
1.59E+13	1.755E-04
1.60E+13	1.700E-04
1.60E+13	1.648E-04
1.61E+13	1.596E-04
1.61E+13	1.547E-04
1.62E+13	1.498E-04
1.62E+13	1.452E-04
1.63E+13	1.406E-04
1.63E+13	1.363E-04
1.64E+13	1.320E-04
1.64E+13	1.279E-04
1.65E+13	1.239E-04
1.65E+13	1.201E-04
1.66E+13	1.165E-04
1.66E+13	1.129E-04
1.67E+13	1.096E-04
1.67E+13	1.064E-04
1.68E+13	1.034E-04
1.68E+13	1.005E-04
1.69E+13	9.786E-05
1.69E+13	9.539E-05
1.70E+13	9.314E-05
1.70E+13	9.111E-05
1.71E+13	8.932E-05
1.71E+13	8.780E-05
1.72E+13	8.655E-05
1.72E+13	8.561E-05
1.73E+13	8.499E-05
1.73E+13	8.472E-05
1.74E+13	8.481E-05
1.74E+13	8.527E-05
1.75E+13	8.613E-05
1.75E+13	8.737E-05
1.76E+13	8.901E-05
1.76E+13	9.102E-05
1.77E+13	9.337E-05
1.77E+13	9.603E-05
1.78E+13	9.895E-05
1.78E+13	1.021E-04
1.79E+13	1.053E-04
1.79E+13	1.085E-04
1.80E+13	1.117E-04
1.80E+13	1.147E-04
1.81E+13	1.175E-04
1.81E+13	1.198E-04
1.82E+13	1.217E-04
1.82E+13	1.231E-04
1.83E+13	1.238E-04
1.83E+13	1.238E-04
1.84E+13	1.232E-04
1.84E+13	1.219E-04
1.85E+13	1.199E-04
1.85E+13	1.172E-04

Frequency Offset $[Hz]$	Raman Gain $[\frac{1}{mW}]$
1.86E+13	1.139E-04
1.86E+13	1.102E-04
1.87E+13	1.060E-04
1.87E+13	1.015E-04
1.88E+13	9.671E-05
1.88E+13	9.182E-05
1.89E+13	8.689E-05
1.89E+13	8.201E-05
1.90E+13	7.725E-05
1.90E+13	7.268E-05
1.91E+13	6.835E-05
1.91E+13	6.430E-05
1.92E+13	6.054E-05
1.92E+13	5.711E-05
1.93E+13	5.400E-05
1.93E+13	5.120E-05
1.94E+13	4.870E-05
1.94E+13	4.649E-05
1.95E+13	4.454E-05
1.95E+13	4.283E-05
1.96E+13	4.134E-05
1.96E+13	4.004E-05
1.97E+13	3.891E-05
1.97E+13	3.792E-05
1.98E+13	3.706E-05
1.98E+13	3.631E-05
1.99E+13	3.565E-05
1.99E+13	3.506E-05
2.00E+13	3.454E-05
2.00E+13	3.408E-05
2.01E+13	3.366E-05
2.01E+13	3.328E-05
2.02E+13	3.294E-05
2.02E+13	3.262E-05
2.03E+13	3.232E-05
2.03E+13	3.204E-05
2.04E+13	3.178E-05
2.04E+13	3.153E-05
2.05E+13	3.129E-05
2.05E+13	3.107E-05
2.06E+13	3.084E-05
2.06E+13	3.063E-05
2.07E+13	3.042E-05
2.07E+13	3.022E-05
2.08E+13	3.001E-05
2.08E+13	2.982E-05
2.09E+13	2.962E-05
2.09E+13	2.943E-05
2.10E+13	2.924E-05
2.10E+13	2.905E-05
2.11E+13	2.887E-05
2.11E+13	2.868E-05
2.12E+13	2.850E-05
2.12E+13	2.832E-05
2.13E+13	2.815E-05
2.13E+13	2.798E-05
2.14E+13	2.782E-05
2.14E+13	2.766E-05
2.15E+13	2.751E-05
2.15E+13	2.737E-05
2.16E+13	2.723E-05
2.16E+13	2.711E-05
2.17E+13	2.701E-05
2.17E+13	2.692E-05
2.18E+13	2.684E-05
2.18E+13	2.679E-05
2.19E+13	2.676E-05
2.19E+13	2.676E-05
2.20E+13	2.679E-05
2.20E+13	2.685E-05
2.21E+13	2.695E-05
2.21E+13	2.709E-05
2.22E+13	2.728E-05
2.22E+13	2.751E-05
2.23E+13	2.780E-05
2.23E+13	2.814E-05
2.24E+13	2.855E-05
2.24E+13	2.902E-05
2.25E+13	2.956E-05
2.25E+13	3.017E-05
2.26E+13	3.086E-05
2.26E+13	3.162E-05
2.27E+13	3.246E-05
2.27E+13	3.337E-05
2.28E+13	3.436E-05
2.28E+13	3.543E-05
2.29E+13	3.656E-05
2.29E+13	3.776E-05
2.30E+13	3.902E-05
2.30E+13	4.034E-05
2.31E+13	4.169E-05
2.31E+13	4.309E-05
2.32E+13	4.451E-05

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
2.32E+13	4.595E-05
2.33E+13	4.739E-05
2.33E+13	4.883E-05
2.34E+13	5.024E-05
2.34E+13	5.162E-05
2.35E+13	5.296E-05
2.35E+13	5.425E-05
2.36E+13	5.548E-05
2.36E+13	5.663E-05
2.37E+13	5.770E-05
2.37E+13	5.868E-05
2.38E+13	5.958E-05
2.38E+13	6.038E-05
2.39E+13	6.108E-05
2.39E+13	6.168E-05
2.40E+13	6.219E-05
2.40E+13	6.261E-05
2.41E+13	6.294E-05
2.41E+13	6.318E-05
2.42E+13	6.333E-05
2.42E+13	6.342E-05
2.43E+13	6.343E-05
2.43E+13	6.337E-05
2.44E+13	6.326E-05
2.44E+13	6.309E-05
2.45E+13	6.286E-05
2.45E+13	6.258E-05
2.46E+13	6.225E-05
2.46E+13	6.187E-05
2.47E+13	6.145E-05
2.47E+13	6.097E-05

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
2.48E+13	6.044E-05
2.48E+13	5.987E-05
2.49E+13	5.923E-05
2.49E+13	5.854E-05
2.50E+13	5.779E-05
2.50E+13	5.698E-05
2.51E+13	5.610E-05
2.51E+13	5.517E-05
2.52E+13	5.417E-05
2.52E+13	5.310E-05
2.53E+13	5.198E-05
2.53E+13	5.081E-05
2.54E+13	4.957E-05
2.54E+13	4.829E-05
2.55E+13	4.697E-05
2.55E+13	4.562E-05
2.56E+13	4.423E-05
2.56E+13	4.283E-05
2.57E+13	4.141E-05
2.57E+13	3.998E-05
2.58E+13	3.856E-05
2.58E+13	3.716E-05
2.59E+13	3.577E-05
2.59E+13	3.441E-05
2.60E+13	3.308E-05
2.60E+13	3.180E-05
2.61E+13	3.055E-05
2.61E+13	2.936E-05
2.62E+13	2.822E-05
2.62E+13	2.714E-05
2.63E+13	2.612E-05

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
2.63E+13	2.516E-05
2.64E+13	2.426E-05
2.64E+13	2.341E-05
2.65E+13	2.263E-05
2.65E+13	2.191E-05
2.66E+13	2.124E-05
2.66E+13	2.063E-05
2.67E+13	2.007E-05
2.67E+13	1.956E-05
2.68E+13	1.910E-05
2.68E+13	1.868E-05
2.69E+13	1.830E-05
2.69E+13	1.795E-05
2.70E+13	1.764E-05
2.70E+13	1.736E-05
2.71E+13	1.711E-05
2.71E+13	1.688E-05
2.72E+13	1.668E-05
2.72E+13	1.649E-05
2.73E+13	1.632E-05
2.73E+13	1.617E-05
2.74E+13	1.603E-05
2.74E+13	1.590E-05
2.75E+13	1.578E-05
2.75E+13	1.567E-05
2.76E+13	1.557E-05
2.76E+13	1.547E-05
2.77E+13	1.537E-05
2.77E+13	1.528E-05
2.78E+13	1.519E-05
2.78E+13	1.510E-05

Frequency Offset $[Hz]$	Raman Gain $[\frac{1}{mW}]$
2.79E+13	1.501E-05
2.79E+13	1.493E-05
2.80E+13	1.484E-05
2.80E+13	1.475E-05
2.81E+13	1.466E-05
2.81E+13	1.457E-05
2.82E+13	1.448E-05
2.82E+13	1.439E-05
2.83E+13	1.429E-05
2.83E+13	1.419E-05
2.84E+13	1.409E-05
2.84E+13	1.399E-05
2.85E+13	1.389E-05
2.85E+13	1.379E-05
2.86E+13	1.368E-05
2.86E+13	1.357E-05
2.87E+13	1.346E-05
2.87E+13	1.335E-05
2.88E+13	1.324E-05
2.88E+13	1.313E-05
2.89E+13	1.302E-05
2.89E+13	1.291E-05
2.90E+13	1.280E-05
2.90E+13	1.268E-05
2.91E+13	1.257E-05
2.91E+13	1.247E-05
2.92E+13	1.236E-05
2.92E+13	1.226E-05
2.93E+13	1.216E-05
2.93E+13	1.206E-05
2.94E+13	1.197E-05
2.94E+13	1.188E-05
2.95E+13	1.179E-05
2.95E+13	1.171E-05
2.96E+13	1.164E-05
2.96E+13	1.158E-05
2.97E+13	1.152E-05
2.97E+13	1.147E-05
2.98E+13	1.143E-05
2.98E+13	1.140E-05
2.99E+13	1.138E-05
2.99E+13	1.136E-05
3.00E+13	1.137E-05
3.00E+13	1.138E-05
3.01E+13	1.140E-05
3.01E+13	1.144E-05
3.02E+13	1.149E-05
3.02E+13	1.156E-05
3.03E+13	1.164E-05
3.03E+13	1.173E-05
3.04E+13	1.185E-05
3.04E+13	1.197E-05
3.05E+13	1.212E-05
3.05E+13	1.227E-05
3.06E+13	1.245E-05
3.06E+13	1.264E-05
3.07E+13	1.285E-05
3.07E+13	1.307E-05
3.08E+13	1.331E-05
3.08E+13	1.357E-05
3.09E+13	1.384E-05
3.09E+13	1.412E-05
3.10E+13	1.442E-05
3.10E+13	1.473E-05
3.11E+13	1.505E-05
3.11E+13	1.538E-05
3.12E+13	1.572E-05
3.12E+13	1.607E-05
3.13E+13	1.643E-05
3.13E+13	1.678E-05
3.14E+13	1.714E-05
3.14E+13	1.751E-05
3.15E+13	1.787E-05
3.15E+13	1.823E-05
3.16E+13	1.858E-05
3.16E+13	1.893E-05
3.17E+13	1.926E-05
3.17E+13	1.959E-05
3.18E+13	1.991E-05
3.18E+13	2.021E-05
3.19E+13	2.049E-05
3.19E+13	2.075E-05
3.20E+13	2.100E-05
3.20E+13	2.122E-05
3.21E+13	2.142E-05
3.21E+13	2.160E-05
3.22E+13	2.175E-05
3.22E+13	2.187E-05
3.23E+13	2.197E-05
3.23E+13	2.204E-05
3.24E+13	2.208E-05
3.24E+13	2.209E-05
3.25E+13	2.207E-05

Frequency Offset $[Hz]$	Raman Gain $[\frac{1}{mW}]$
3.25E+13	2.203E-05
3.26E+13	2.195E-05
3.26E+13	2.185E-05
3.27E+13	2.172E-05
3.27E+13	2.157E-05
3.28E+13	2.139E-05
3.28E+13	2.119E-05
3.29E+13	2.097E-05
3.29E+13	2.072E-05
3.30E+13	2.046E-05
3.30E+13	2.018E-05
3.31E+13	1.988E-05
3.31E+13	1.957E-05
3.32E+13	1.925E-05
3.32E+13	1.892E-05
3.33E+13	1.859E-05
3.33E+13	1.824E-05
3.34E+13	1.790E-05
3.34E+13	1.755E-05
3.35E+13	1.720E-05
3.35E+13	1.685E-05
3.36E+13	1.651E-05
3.36E+13	1.617E-05
3.37E+13	1.584E-05
3.37E+13	1.551E-05
3.38E+13	1.520E-05
3.38E+13	1.489E-05
3.39E+13	1.459E-05
3.39E+13	1.431E-05
3.40E+13	1.404E-05
3.40E+13	1.378E-05
3.41E+13	1.354E-05
3.41E+13	1.331E-05
3.42E+13	1.309E-05
3.42E+13	1.289E-05
3.43E+13	1.270E-05
3.43E+13	1.253E-05
3.44E+13	1.237E-05
3.44E+13	1.223E-05
3.45E+13	1.209E-05
3.45E+13	1.198E-05
3.46E+13	1.187E-05
3.46E+13	1.178E-05
3.47E+13	1.169E-05
3.47E+13	1.162E-05
3.48E+13	1.156E-05
3.48E+13	1.151E-05
3.49E+13	1.147E-05
3.49E+13	1.144E-05
3.50E+13	1.142E-05
3.50E+13	1.140E-05
3.51E+13	1.139E-05
3.51E+13	1.138E-05
3.52E+13	1.138E-05
3.52E+13	1.139E-05
3.53E+13	1.140E-05
3.53E+13	1.141E-05
3.54E+13	1.142E-05
3.54E+13	1.144E-05
3.55E+13	1.146E-05
3.55E+13	1.148E-05
3.56E+13	1.150E-05
3.56E+13	1.152E-05
3.57E+13	1.154E-05
3.57E+13	1.156E-05
3.58E+13	1.158E-05
3.58E+13	1.159E-05
3.59E+13	1.161E-05
3.59E+13	1.162E-05
3.60E+13	1.163E-05
3.60E+13	1.164E-05
3.61E+13	1.164E-05
3.61E+13	1.164E-05
3.62E+13	1.164E-05
3.62E+13	1.163E-05
3.63E+13	1.162E-05
3.63E+13	1.160E-05
3.64E+13	1.158E-05
3.64E+13	1.156E-05
3.65E+13	1.153E-05
3.65E+13	1.149E-05
3.66E+13	1.145E-05
3.66E+13	1.141E-05
3.67E+13	1.136E-05
3.67E+13	1.131E-05
3.68E+13	1.125E-05
3.68E+13	1.119E-05
3.69E+13	1.112E-05
3.69E+13	1.105E-05
3.70E+13	1.098E-05
3.70E+13	1.090E-05
3.71E+13	1.081E-05
3.71E+13	1.072E-05

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
3.72E+13	1.063E-05
3.72E+13	1.053E-05
3.73E+13	1.043E-05
3.73E+13	1.032E-05
3.74E+13	1.021E-05
3.74E+13	1.010E-05
3.75E+13	9.986E-06
3.75E+13	9.866E-06
3.76E+13	9.744E-06
3.76E+13	9.619E-06
3.77E+13	9.491E-06
3.77E+13	9.361E-06
3.78E+13	9.228E-06
3.78E+13	9.093E-06
3.79E+13	8.956E-06
3.79E+13	8.818E-06
3.80E+13	8.678E-06
3.80E+13	8.537E-06
3.81E+13	8.394E-06
3.81E+13	8.251E-06
3.82E+13	8.107E-06
3.82E+13	7.962E-06
3.83E+13	7.817E-06
3.83E+13	7.671E-06
3.84E+13	7.526E-06
3.84E+13	7.380E-06
3.85E+13	7.235E-06
3.85E+13	7.090E-06
3.86E+13	6.946E-06
3.86E+13	6.803E-06
3.87E+13	6.660E-06
3.87E+13	6.519E-06
3.88E+13	6.379E-06
3.88E+13	6.240E-06
3.89E+13	6.102E-06
3.89E+13	5.966E-06
3.90E+13	5.832E-06
3.90E+13	5.699E-06
3.91E+13	5.568E-06
3.91E+13	5.439E-06
3.92E+13	5.312E-06
3.92E+13	5.187E-06
3.93E+13	5.064E-06
3.93E+13	4.943E-06
3.94E+13	4.825E-06
3.94E+13	4.709E-06
3.95E+13	4.595E-06
3.95E+13	4.483E-06
3.96E+13	4.374E-06
3.96E+13	4.268E-06
3.97E+13	4.163E-06
3.97E+13	4.061E-06
3.98E+13	3.962E-06
3.98E+13	3.865E-06
3.99E+13	3.770E-06
3.99E+13	3.678E-06
4.00E+13	3.588E-06
4.00E+13	3.501E-06
4.01E+13	3.416E-06
4.01E+13	3.334E-06
4.02E+13	3.253E-06
4.02E+13	3.175E-06
4.03E+13	3.100E-06
4.03E+13	3.026E-06
4.04E+13	2.955E-06
4.04E+13	2.886E-06
4.05E+13	2.819E-06
4.05E+13	2.754E-06
4.06E+13	2.691E-06
4.06E+13	2.630E-06
4.07E+13	2.572E-06
4.07E+13	2.515E-06
4.08E+13	2.460E-06
4.08E+13	2.406E-06
4.09E+13	2.355E-06
4.09E+13	2.305E-06
4.10E+13	2.257E-06
4.10E+13	2.210E-06
4.11E+13	2.165E-06
4.11E+13	2.122E-06
4.12E+13	2.080E-06
4.12E+13	2.040E-06
4.13E+13	2.000E-06
4.13E+13	1.963E-06
4.14E+13	1.926E-06
4.14E+13	1.891E-06
4.15E+13	1.857E-06
4.15E+13	1.824E-06
4.16E+13	1.792E-06
4.16E+13	1.762E-06
4.17E+13	1.732E-06
4.17E+13	1.703E-06
4.18E+13	1.676E-06

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
4.18E+13	1.649E-06
4.19E+13	1.623E-06
4.19E+13	1.598E-06
4.20E+13	1.574E-06
4.20E+13	1.551E-06
4.21E+13	1.528E-06
4.21E+13	1.506E-06
4.22E+13	1.485E-06
4.22E+13	1.464E-06
4.23E+13	1.444E-06
4.23E+13	1.425E-06
4.24E+13	1.407E-06
4.24E+13	1.388E-06
4.25E+13	1.371E-06
4.25E+13	1.354E-06
4.26E+13	1.337E-06
4.26E+13	1.321E-06
4.27E+13	1.306E-06
4.27E+13	1.291E-06
4.28E+13	1.276E-06
4.28E+13	1.262E-06
4.29E+13	1.248E-06
4.29E+13	1.234E-06
4.30E+13	1.221E-06
4.30E+13	1.208E-06
4.31E+13	1.195E-06
4.31E+13	1.183E-06
4.32E+13	1.171E-06
4.32E+13	1.160E-06
4.33E+13	1.148E-06
4.33E+13	1.137E-06
4.34E+13	1.127E-06
4.34E+13	1.116E-06
4.35E+13	1.106E-06
4.35E+13	1.096E-06
4.36E+13	1.086E-06
4.36E+13	1.076E-06
4.37E+13	1.067E-06
4.37E+13	1.057E-06
4.38E+13	1.048E-06
4.38E+13	1.039E-06
4.39E+13	1.031E-06
4.39E+13	1.022E-06
4.40E+13	1.014E-06
4.40E+13	1.006E-06
4.41E+13	9.977E-07
4.41E+13	9.898E-07
4.42E+13	9.820E-07
4.42E+13	9.744E-07
4.43E+13	9.670E-07
4.43E+13	9.596E-07
4.44E+13	9.524E-07
4.44E+13	9.453E-07
4.45E+13	9.383E-07
4.45E+13	9.315E-07
4.46E+13	9.247E-07
4.46E+13	9.181E-07
4.47E+13	9.116E-07
4.47E+13	9.051E-07
4.48E+13	8.988E-07
4.48E+13	8.926E-07
4.49E+13	8.864E-07
4.49E+13	8.804E-07
4.50E+13	8.744E-07
4.50E+13	8.685E-07
4.51E+13	8.628E-07
4.51E+13	8.570E-07
4.52E+13	8.514E-07
4.52E+13	8.459E-07
4.53E+13	8.404E-07
4.53E+13	8.350E-07
4.54E+13	8.297E-07
4.54E+13	8.244E-07
4.55E+13	8.192E-07
4.55E+13	8.141E-07
4.56E+13	8.090E-07
4.56E+13	8.041E-07
4.57E+13	7.991E-07
4.57E+13	7.943E-07
4.58E+13	7.895E-07
4.58E+13	7.847E-07
4.59E+13	7.800E-07
4.59E+13	7.754E-07
4.60E+13	7.708E-07
4.60E+13	7.663E-07
4.61E+13	7.618E-07
4.61E+13	7.574E-07
4.62E+13	7.530E-07
4.62E+13	7.487E-07
4.63E+13	7.444E-07
4.63E+13	7.402E-07
4.64E+13	7.360E-07
4.64E+13	7.319E-07

Frequency Offset [Hz]	Raman Gain [$\frac{1}{mW}$]
4.65E+13	7.278E-07
4.65E+13	7.238E-07
4.66E+13	7.197E-07
4.66E+13	7.158E-07
4.67E+13	7.119E-07
4.67E+13	7.080E-07
4.68E+13	7.042E-07
4.68E+13	7.004E-07
4.69E+13	6.966E-07
4.69E+13	6.929E-07
4.70E+13	6.892E-07
4.70E+13	6.856E-07
4.71E+13	6.820E-07
4.71E+13	6.784E-07
4.72E+13	6.748E-07
4.72E+13	6.713E-07
4.73E+13	6.679E-07
4.73E+13	6.644E-07
4.74E+13	6.610E-07
4.74E+13	6.577E-07
4.75E+13	6.543E-07
4.75E+13	6.510E-07
4.76E+13	6.477E-07
4.76E+13	6.445E-07
4.77E+13	6.413E-07
4.77E+13	6.381E-07
4.78E+13	6.349E-07
4.78E+13	6.318E-07
4.79E+13	6.287E-07
4.79E+13	6.095E-07
4.80E+13	6.225E-07
4.80E+13	6.195E-07
4.81E+13	6.165E-07
4.81E+13	6.135E-07
4.82E+13	6.106E-07
4.82E+13	6.077E-07
4.83E+13	6.048E-07
4.83E+13	6.019E-07
4.84E+13	5.990E-07
4.84E+13	5.962E-07
4.85E+13	5.934E-07
4.85E+13	5.906E-07
4.86E+13	5.879E-07
4.86E+13	5.852E-07
4.87E+13	5.824E-07
4.87E+13	5.798E-07
4.88E+13	5.771E-07
4.88E+13	5.744E-07
4.89E+13	5.718E-07
4.89E+13	5.692E-07
4.90E+13	5.666E-07
4.90E+13	5.641E-07
4.91E+13	5.615E-07
4.91E+13	5.590E-07
4.92E+13	5.565E-07
4.92E+13	5.540E-07
4.93E+13	5.515E-07
4.93E+13	5.491E-07
4.94E+13	5.467E-07
4.94E+13	5.442E-07
4.95E+13	5.418E-07
4.95E+13	5.395E-07
4.96E+13	5.371E-07
4.96E+13	5.348E-07
4.97E+13	5.325E-07
4.97E+13	5.301E-07
4.98E+13	5.279E-07
4.98E+13	5.256E-07
4.99E+13	5.233E-07
4.99E+13	5.211E-07
5.00E+13	5.189E-07
5.00E+13	5.167E-07