Author:
Alia, Obada

Title:
Advanced quantum communications for next-generation secure optical networks

Advanced Quantum Communications for Next-Generation Secure Optical Networks

By

Obada Alia

Department of Electrical and Electronic Engineering
University of Bristol

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Engineering.

March 20, 2023

Word count: 41480

Abstract

New quantum technologies are set to radically change many fields, including computation, sensing and communication. However, the question of building a large-scale quantum computer is a matter of when not if. These computers exploit quantum mechanics to solve hard and complicated mathematical problems which are unsolvable using conventional classical computers. These mathematical problems are the base of our public-key cryptography algorithms, which are used in our daily lives and critical infrastructure and will be broken using a quantum computer.

Quantum key distribution (QKD) enables the exchange of theoretically secure symmetrical random keys based on the fundamentals of quantum mechanics. QKD relies on the exchange of single photons between two distant parties in an end-to-end configuration, making it extremely difficult to integrate with the current classical infrastructure. In this thesis, we will explore the feasibility of integrating QKD technologies into the existing classical infrastructure.

We first demonstrate commercial QKD systems as a part of a deployed fibre network in the city of Bristol. The network includes a software-defined networking controller and allows the coexistence of classical and quantum channels in a single fibre to ensure compatibility with current and future infrastructure. The network also enables dynamic switching for the QKD systems overcoming end-to-end configuration and reducing implementation costs. In addition, we develop several coexistence schemes in advanced mediums, including multicore fibre, hollow core fibre, and free space, to provide a comprehensive view of different coexistence techniques and their implementation in different use cases.

Finally, we move towards entanglement-based quantum networks, which are considered the backbone of future quantum communication applications. We implement an advanced architecture to provide a flexible and on-demand allocation of entanglement across different users and allows dynamic networking for multiple quantum protocols in the network. We also integrate the hollow core fibre into the network to enable the coexistence of quantum and classical channels in a single fibre.

"And you mankind have not been given of knowledge except a little."
[Holy Quran, 17:85]

Dedication

To my parents, family & friends

Acknowledgements

First and foremost, I would like to thank Almighty Allah; all my achievements are due to Him.

I would like to extend my sincere gratitude to my supervisor Dr. George T. Kanellos for his guidance throughout the past four years. I learned from his way of research, questioning every little nuance of the work at hand, leading to exceptional and quality work. Indeed, the research skills I have learned from him will help throughout my life. I would like to also thank my second supervisor Prof. Reza Nejabati for his valuable comments and insights. I am grateful to them for providing an opportunity to carry out research at the High Performance Networks (HPN) group.

I would like to thank my friends and colleagues Dr. Emilio Hugues-Salas and Dr. Rodrigo Stange Tessinari for providing the best company someone could ask for during my research. I will never forget the nice BBQs we had and I am sure you will never forget my great and not annoying singing in the lab.

I thank Dr. Abubakar Siddique Muqaddas, Dr. Ekin Arabul, Dr. Sima Bahrani, Dr. Romerson D Oliveira, and Dr. Rui Wang for supporting me during my time at HPN group. Thanks to the Greek freaks Dr. Antonis Vafeas, Dr. Stavros Typos and Dr. Constantinos Vrontos. I also thank Dr. Siddarth K Joshi and Marcus Clark for being patient with me and explaining how does entanglement work and the physics behind it a million times.

I express my gratitude to my great parents for their constant support and motivation thought my life and my PhD. They are truly the best parents anyone can ask for. A special thank you to my brothers for always assuring me that everything will be alright and that I can make it.

I also express my gratitude to my family in Syria who were supportive all the time and made this journey much easier with their prayers.

To my amazing friends Mohammad, Anas, Musab, Omran, Khaled, and Yasin. You made this journey fun and it was so much easier with your support. Thank you for everything.

To my beautiful niece Bana, thank you for bringing the joy to our family and out life. I cannot wait to meet and hug you.

To my beautiful fiancé Marah, thank you for your understanding, constant support and for always being here when I needed you. I could not have done it without you.

To all my teachers, friends and everyone who made this possible, thank you.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: .... DATE: ....

Table of Contents

List of Acronyms and Abbreviations

AES	Advanced encryption standard
AR-HCF	Antiresonant hollow core fibre
ASE	Amplified spontaneous emission
APD	Avalanche photodiode
AWG	Arrayed waveguide grating
BB84	Bennett-Brassard 1984
BER	Bit error rate
BS	Beam splitter
BPF	Band pass filter
BRW	Bragg reflection waveguides
BVT	Bandwidth-variable transponder
CHSH	Clauser, Horne, Shimony and Holt
COW	Coherent-one-way
CV-QKD	Continuous-variable QKD
CPL	Coupler
CW	Continuous wave
DC	Data centre
DES	Data encryption standard
DeMUX	Demultiplexer
DM	Dichroic mirror

D-NANF	Double nested antiresonant nodeless fibre
DH	Diffie-Hellman
DI-QKD	Device-independent QKD
DPR-QKD	Distributed-phase-reference QKD
DPS	Differential-phase-shift
DV-QKD	Discrete-variable QKD
DWDM	Dense wavelength-division multiplexing
E91	Ekert 1991
EDC	Entanglement distribution circuit
EDFA	Erbium-doped fibre amplifier
ECDH	Elliptic Curve Diffie-Hellman
EHC	Enforced hill-climbing
EPR	Einstein, Podolsky, and Rosen
EPS	Entanglement photon source
ETSI	European Telecommunication Standards Institute
FF	Fast-forward
FM	Faraday mirrors
FoV	Field of view
FPC	Fibre polarisation controller
FPGA	Field-programmable gate array
FWM	Four-wave mixing
FWHM	Full width half maximum
FWF	Fibre-Wireless-Fibre
GCD	Greatest common divisor
GCHQ	The Government Communiations Headquarters

HCF	Hollow core fibre
HC-NANF	Hollow Core Nested Antiresonant Nodeless Fibre
HCPBGF	Hollow Core Photonic Band Gap fibre
HPN	High performance networks
HWP	Half wave plates
IM	Intensity modulator
InP	Indium phosphide
ISO	Isolator
KMS	Key management system
LCoS	Liquid crystal on silicon
MCF	Multi-core fibre
MDI QKD	Measurement device independent QKD
MEMS	Microelectromechanical system
MgO	Magnesium-Oxide
MMI	Multimode interference
MitM	Man-in-the-middle
MUX	Multiplexer
MZI	Mach-Zehnder interferometer
NCSC	National Cyber Security Centre
NDFF	National Dark Fibre Facility
NIST	The National Institute of Standards and Technology
NSA	National Security Agency
NSQI	Nanoscience & Quantum Information
NPL	The National Physical Laboratories
OA	Optical attenuator

OFS	Optical fibre switch
OSA	Optical spectrum analyser
OSNR	Optical signal-to-noise ration
OTP	One-time pad
OXC	Optical cross-connect
PAM	polarisation analysis module
PBS	Polarising beam splitter
PDDL	Planning domain definition language
PM	Polarization maintaining
PNS	Photon number splitting
PPLN	Periodical Poled Lithium Niobate
PRNG	Pseudo-random number generator
PQC	Post-quantum cryptography
QBER	Quantum Bit Error Rate
OBRF	Optical band pass/rejection filter
QMAN	Quantum metropolitan area networks
QKD	Quantum key distribution
Qubit	Quantum bit
QWP	Quarter wave plates
QRNG	Quantum random number generator
q-ROADM	Quantum reconfigurable optical add-drop multiplexer
QSFP+	Quad small form-factor pluggable
RSA	Rivest-Shamir-Adleman
SD-FEC	Soft-decision forward error correction
SDM	Space division multiplexing

SDN	Software-defined networking
SEM	Scanning electron micrograph
SIAT	Secure initial authentication transfer
SNMP	Simple Network Management Protocol
SFP	Small form-factor pluggable
SFP+	Enhanced small form-factor pluggable
SKR	Secret key rate
SMF	Single mode fibre
SNSPD	Superconducting nanowire single-photon detector
SPAD	Single-photon avalanche diode
SPD	Single-photon detector
SPDC	Spontaneous parametric down conversion
SpRS	Spontaneous Raman scattering
TBPF	Tunable bandpass filter
TCP	Transmission Control Protocol
TFF	Thin film filter
TLS	Transport layer security
TREL	Toshiba Research Europe Ltd
TRNG	True random number generator
UKQN	UK quantum network
VM	Virtual machine
VOA	Variable optical attenuator
WCP	Weak coherent pulse
WCS	Weak coherent state
WDM	Wavelength-division multiplexing

WSS	Wavelength selective switch
XOR	Exclusive OR
XT	Crosstalk

List of Publications

Journal Papers:

1. O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dynamic dv-qkd networking in trusted-node-free software-defined optical networks," *Journal of Lightwave Technology*, vol. 40, no. 17, pp. 5816–5824, 2022

2. O. Alia, R. S. Tessinari, S. Bahrani, T. D. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, D. Richardson, F. Poletti, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dv-qkd coexistence with 1.6 tbps classical channels over hollow core fibre," *Journal of Lightwave Technology*, vol. 40, no. 16, pp. 5522–5529, 2022

3. A. Schreier, O. Alia, R. Wang, S. Bahrani, R. Singh, G. Faulkner, G. T. Kanellos, R. Nejabati, D. Simeonidou, J. Rarity, and D. O'Brien, "Coexistence of quantum and 1.6 tbit/s classical data over fibre-wireless-fibre terminals," *Journal of Lightwave Technology*, 2022 (Submitted to JLT).

4. M. Peranić, M. Clark, R. Wang, S. Bahrani, O. Alia, S. Wengerowsky, A. Radman, M. Lončarić, M. Stipčević, J. Rarity, *et al.*, "Polarization compensation methods for quantum communication networks," *arXiv preprint arXiv:2208.13584*, 2022 (Submitted to EPJ Quantum Technology).

5. E. Hugues-Salas, O. Alia, R. Wang, K. Rajkumar, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "11.2 tb/s classical channel coexistence with dv-qkd over a 7-core multicore fiber," *Journal of Lightwave Technology*, vol. 38, no. 18, pp. 5064–5070, 2020

Conference Papers:

1. R. Wang, M. Clark, S. K. Joshi, S. Bahrani, O. Alia, M. Peranić, M. Lončarić, M. Stipčević, *et al.*, "Optimum switching scenario analysis in a dynamic entanglement network," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2023 (Submitted to OFC 2023).

2. M. Minder, S. Albosh, O. Alia, R. Slavik, F. Poletti, G. T. Kanellos, R. Kumar, and M. Lucamarini, "Characterisation of a nested antiresonant nodeless hollow core fibre for phase-

based quantum key distribution protocols," in *SPIE PhotoneX*, SPIE, 2022 (Submitted to SPIE PhotoneX 2022).

3. O. Alia, A. Schreier, R. Wang, S. Bahrani, R. Singh, G. Faulkner, J. Rarity, D. O'Brien, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dv-qkd coexistence with 1.6 terabit/s classical channels in free space using fiber-wireless-fiber terminals," in *2022 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2022

4. R. Wang, O. Alia, M. Clark, S. Bahrani, S. K. Joshi, D. Aktas, G. T. Kanellos, M. Peranić, M. Lončarić, M. Stipčević, *et al.*, "A dynamic multi-protocol entanglement distribution quantum network," in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2022

5. O. Alia, R. S. Tessinari, S. Bahrani, J. Sagar, T. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, *et al.*, "Coexistence analysis of classical channels with dv-qkd over hollow core nested antiresonant nodeless fibre (hc-nanf)," in *Quantum Computing, Communication, and Simulation II*, p. PC1201519, SPIE, 2022

6. M. Clark, O. Alia, R. Wang, S. Bahrani, D. Aktas, G. Kanellos, M. Loncaric, Ž. Samec, M. Peranić, A. Radman, *et al.*, "Towards a fully connected many-user entanglement distribution quantum network within deployed telecommunications fibre-optic infrastructure," in *CLEO: QELS_Fundamental Science*, pp. FF4A–6, Optica Publishing Group, 2022

7. F. Honz, F. Prawits, O. Alia, H. Sakr, T. Bradley, C. Zhang, R. Slavík, F. Poletti, G. T. Kanellos, R. Nejabati, P. Walther, D. Simeonidou, *et al.*, "Demonstration of 17 $\lambda \times 10$ gb/s c-band classical / dv-qkd co-existence over hollow-core fiber link," in *2022 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2022

8. F. Prawits, F. Honz, O. Alia, H. Sakr, T. Bradley, C. Zhang, R. Slavík, F. Poletti, G. T. Kanellos, R. Nejabati, P. Walther, and D. Simeonidou, "Dv-qkd over bidirectional fiber link in-band co-existence with 25 classical 10 gb/s channels," in *Int. Conf. on Quantum Cryptography (QCrypt)*, pp. 1–3, 2022

9. E. Arabul, R. D. Oliveira, R. Wang, O. Alia, G. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of high-speed self-reconfiguration and key slicing for 100 gbps multi-user programmable hardware encryptor," in *2022 European Conference on Optical Communications (ECOC)*, Institute of Electrical and Electronics Engineers (IEEE), 2022

10. A. Ntanos, N. K. Lyras, S. Anwar, O. Alia, D. Zavitsanos, G. Giannoulis, A. D. Panagopoulos, G. Kanellos, and H. Avramopoulos, "Large-scale leo satellite constellation to ground qkd links: Feasibility analysis," in *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pp. 288–295, IEEE, 2022

11. E. Arabul, R. S. Tessinari, O. Alia, R. Oliveira, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "100 gb/s dynamically programmable sdn-enabled hardware encryptor for optical networks," *Journal of Optical Communications and Networking*, vol. 14, no. 1, pp. A50–A60, 2022

12. O. Alia, R. S. Tessinari, T. D. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, D. Richardson, F. Poletti, *et al.*, "1.6 tbps classical channel coexistence with dv-qkd over hollow core nested antiresonant nodeless fibre (hc-nanf)," in *2021 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2021

13. O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Wavelength resources management and switching of active entanglement distribution circuits in optical networks," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021

14. M. J. Clark, O. Alia, R. S. Tessinari, R. Wang, D. Aktas, G. T. Kanellos, J. G. Rarity, R. Nejabati, D. E. Simeonidou, and S. K. Joshi, "Towards a quantum network within deployed telecommunications fibre-optic infrastructure," in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, vol. 11881, p. 118810D, SPIE, 2021

15. R. S. Tessinari, O. Alia, S. K. Joshi, D. Aktas, M. Clark, E. Hugues-Salas, G. T. Kanellos, J. Rarity, R. Nejabati, and D. Simeonidou, "Towards co-existence of 100 gbps classical channel within a wdm quantum entanglement network," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021

16. R. S. Tessinari, E. Arabul, O. Alia, A. S. Muqaddas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Demonstration of a dynamic qkd network control using a qkd-aware sdn application over a programmable hardware encryptor," in *Optical Fiber Communication Conference*, pp. M2B–3, Optical Society of America, 2021

17. E. Arabul, R. S. Tessinari, O. Alia, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of programmable 100 gb/s sdn-enabled encryptors/decryptors for qkd networks," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021

18. G. Kanellos, O. Alia, E. Hugues-Salas, R. S. Tessinari, R. Wang, R. Nejabati, and D. Simeonidou, "Dynamic optical interconnects for quantum secure distributed nodes and quantum processing," in *2020 IEEE Photonics Conference (IPC)*, pp. 1–2, IEEE, 2020

19. R. S. Tessinari, A. Bravalheri, E. Hugues-Salas, R. Collins, D. Aktas, R. S. Guimaraes, O. Alia, J. Rarity, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Field trial of dynamic dv-qkd networking in the sdn-controlled fully-meshed optical metro network of the bristol

city 5guk test network," in *45th European Conference on Optical Communication (ECOC 2019)*, pp. 1–4, 2019

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Foreword

Quantum computers are a disruptive innovation that will change the scope of modern technology. Given the money, effort and scale of investment and research in quantum technologies, and the fact that small-scale quantum computers are currently available, it is a matter of time before having large-scale quantum computers [25].

Quantum computers promise benefits in multiple applications, such as financial and pharmaceutical simulation and green technology development [25–28]. However, quantum computers are considered a threat to other applications, such as classical cryptography. With a large-scale quantum computer forthcoming, the current public encryption algorithms are considered obsolete [29]; hence new quantum-resistant technologies are required to provide secure communication and protect against future quantum algorithms.

Quantum Key Distribution (QKD) is an example of a quantum-resistant technology [30, 31]. QKD utilises quantum mechanics to generate information-theoretic keys that are used to encrypt and decrypt critical information using classical symmetric-key algorithms such as One Time pad. QKD has seen rapid progress from initial demonstrations to commercial systems and is considered an essential element in many cryptography applications [32]. However, for QKD systems to be adapted, they must have the ability to easily integrate and coexist with the current classical telecommunications infrastructure and be compatible with next-generation architecture designs.

In this thesis, we contribute to integrating QKD technologies in the next-generation secure optical networks. Mainly, we focus on developing a dynamic QKD architecture and implementing multiple coexistence schemes in single mode fibre and advanced mediums, such as multicore fibre and hollow core fibre. We also apply the dynamicity concept and coexistence schemes into quantum entanglement networks which are essential for the broader adaptation of quantum technology and efficient resource sharing across the networks.

1.2 Thesis Outline

This thesis is structured as follows:

- **Chapter 2** presents the background on different methods of modern cryptography (symmetric and asymmetric), quantum information processing, and quantum computing. We then cover quantum state sources, detectors and different QKD protocols and schemes.

- **Chapter 3** highlights the advances in metropolitan and long-haul QKD networks, including the UK QKD network. The main focus of this chapter is the Bristol QKD network. From the Bristol QKD network, we highlight its network architecture, the experimental testbed in the deployed city network, with a detailed discussion of the results.

- **Chapter 4** explores the state-of-the-art quantum and classical coexistence in optical fibre networks. First, we provide a detailed description of the position and spacing between quantum and classical channels and their effect on the quantum channel performance based on numerical calculations of nonlinear effects. After that, we provide a detailed description of the equipment that are detrimental to QKD and the necessary equipment for coexistence. We introduce the Bristol QKD network focusing on the coexistence testbed. Finally, we discuss results from different scenarios, i.e. varying powers and spacing of classical channels.

- **Chapter 5** describes the coexistence experiments in advanced mediums, such as multicore fibre, hollow core fibre, and free-space enabled by fibre-wireless-fibre terminals. We provide a detailed description of the experimental testbed, medium characterisation and coexistence scenario for each experiment, followed by a comprehensive experimental results section. Finally, we end the section by discussing the improvements across the experiments.

- **Chapter 6** introduces resource allocation methods in entanglement networks. The concept of quantum entanglement is explored in two different experiments. The first experiment is a dynamic multi-protocol entanglement distribution network enabled by a q-ROADM. The second experiment is the coexistence of classical and entanglement-based quantum channels fostered by HCF. In detail, we explain the entanglement source, quantum network connections, q-ROADM, and detection modules. Finally, we discuss the results of each experiment.

- **Chapter 7** concludes this thesis with suggestions for future work

Chapter 2

Background

Declaration of Work

Parts of this chapter have been previously written in the literature review submitted in the taught year of the CDT program. Some of the text has been reused in the chapter where appropriate, as it was written by me.

We present the general background which is required to understand the content of this thesis, as well as the motivation behind it. We first introduce cryptography and explain two types: symmetric-key cryptography and public-key cryptography. We then outline the basic principles of quantum information processing and briefly discuss quantum computing. After that, we describe QKD in detail, including quantum state sources and detectors, QKD protocols and schemes, and the challenges of implementing QKD in optical networks. Finally, we end this chapter by presenting remarks on the 2022 Nobel prize in physics and the 2023 Breakthrough Prize in fundamental physics.

2.1 Cryptography

Cryptography is the practice of providing secure communication in the presence of an adversary using different techniques and protocols. It dates back to the ancient Egyptians [33] and has been used since in many applications. In this section, we discuss different protocols and algorithms of classical cryptography, and provide a brief description of post-quantum cryptography.

2.1.1 Symmetric-Key Cryptography

Symmetric-key algorithms are the simplest type of encryption and the first algorithms used for cryptography. In symmetric-key algorithms, Alice and Bob share a key to encrypt and decrypt the information. Historically, the keys have been shared in person; therefore, any parties involved in transferring the key can decrypt the message. However, with technological advancement, keys can be shared using other security mechanisms. The most basic ciphers are monoalphabetic ciphers, where simple permutations to the original message are applied to produce the encrypted message. A historical example of monoalphabetic ciphers is the Caesar cipher. In Caesar cipher, each letter in the alphabet is assigned a value, e.g. "A"=0, "B"=1, etc. and each number is shifted by a specific number (key) which is agreed by Alice and Bob to procure the encrypted text. If the key value is 3, A becomes D, B becomes E, and so on.

2.1.1.1 One-time Pad

A well-known example symmetric-key algorithm is one-time pad (OTP). OTP is a polyalphabetic cipher where the key length equals the message, and each message is encrypted using a different and unique key. Although it was invented in 1882 [34], it became widely popular in the 20th century when the method to combine the message and key via an exclusive-OR (XOR) operation (Truth table is shown in Table 2.1) was patented [35]. Alice encrypts the message (m) with a random key (k) to produce the ciphertext (c) using the following operation:

$$c = m \oplus k \tag{2.1}$$

Bob can then decrypt the message and retrieve the message (m) using a similar operation:

$$m = c \oplus k \tag{2.2}$$

Suppose k is only used once and is generated randomly. In that case, OTP is proven secure against an adversary with unlimited computing power [36], which is referred to as information-theoretic secure. However, OTP is impractical and has limited applications because the key's length must equal the message's length.

Table 2.1: Truth table for the XOR (⊕) function

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

2.1.1.2 Block Ciphers

The most widely used symmetric algorithms are block ciphers [37], where the message is considered as a block instead of considering it as individual letters. In block ciphers, the message is divided into smaller blocks depending on the cipher, which are then passed through a deterministic algorithm that encrypts the message using a short key. The length of the key also depends on the used cipher. Moreover, encryption and decryption can be implemented using matrix multiplication due to the data being encoded in vectors. Two of the well-known examples are the data encryption standard (DES) [38], which was the standard until 2011 and the advanced encryption standard (AES) [39], which is still the standard today.

2.1.2 Public-Key Cryptography

The main challenge of symmetric-key algorithms is distributing the keys between Alice and Bob. The easy solution is for them to meet in person and exchange the keys before their secret communication. However, this is impractical in real-life scenarios. Public-key cryptography algorithms were developed mainly to exchange the secret key between Alice and Bob over a secure communication channel. Public-key cryptography is based on mathematically hard problems where Alice and Bob act asymmetrically.

These algorithms employ trapdoors, which are functions that are easy to compute one way, but highly challenging in reverse. A straightforward and naive example of such problems is the multiplications of two large prime numbers. For example, it is easy to multiply 6379 and 6961 = 44404219. However, it is harder to find the multiplier (6379) and the multiplicand (6961) given the product 44404219. Alice and Bob have a key pair consisting of a public key and a private key. Those keys are generated using cryptographic algorithms based on a one-way function. To keep the security of the algorithms, the private key must stay private, whereas the public key is openly shared without compromising the security of the algorithms.

This section will introduce the most used public-key algorithms, Diffie-Hellman algorithm [40] and Rivest-Shamir-Adleman algorithm [41]. Although these algorithms can be used to exchange messages, they are mostly used to distribute keys, which are then used to encrypt and decrypt data using symmetric-key algorithm such as AES.

2.1.2.1 Diffie-Hellman Algorithm

Diffie-Hellman (DH) algorithm was the first public-key protocol to securely share keys over a public channel. The protocol was proposed by Whitfield Diffie and Martin Hellman in 1967 [40], and it was the earliest publicly known algorithm that invented the idea of using public and private keys. However, it was revealed that a demonstration of such a protocol was first implemented by researchers at the Government Communications Headquarters (GCHQ) [42, 43].

The secuity of DH algorithm is based on the hardness of the discrete logarithm problem. The problem to find a key (k) given a prime number (p), and integers a and b where $1 < a < p$, such that

$$k = log_a(b) \tag{2.3}$$

$$a^k = b \ (mod\ p) \tag{2.4}$$

As mentioned before, no publicly known classical algorithm can solve the discreet logarithm problem efficiently. However, a quantum algorithm presented in 1994 by Peter Shor can solve the discreet logarithm problem in polynomial time [29]. Moreover, the DH algorithm is usually used for key exchange between Alice and Bob for symmetric-key encryption. The protocol of the DH algorithm is presented below and is simplified as paint colours in Figure 2.1.

Diffie-Hellman Key Exchange Protocol

1. Both Alice and Bob publicly agree on a large prime number p (common colour in Figure 2.1), and a base a.

2. Both Alice and Bob secret choose two secret integers d_A and d_B (secret colours in Figure 2.1).

3. Alice shares her public key $q_A = a^{d_A}$ with Bob (orange paint in Figure 2.1), and Bob shares his public key $q_B = a^{d_B}$ with Alice (blue paint in Figure 2.1).

4. Alice then computes $k = q_B = a^{d_A \times d_B}$ (adding the blue and red paints in Figure 2.1) and Bob computes $k = q_A^{d_B} = a^{d_A \times d_B}$ (adding the orange and aqua paints in Figure 2.1).

5. Alice and Bob now share a secret key (common secret i.e. brown paint in Figure 2.1).

p, a, q_A and q_B are publicly known and are available to an eavesdropper (Eve). However, since Eve does not have the ability to solve the discrete logarithm, she cannot compute d_A or d_B, and therefore, she cannot compute the secret key k.

2.1.2.2 Rivest-Shamir-Adleman Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm was publicly released two years after DH algorithm [41]. Similar to the DH algorithm, it was discovered that it was also known by researchers at the GCHQ [45]. The RSA algorithm security is based on the "factorising problem", which relies on the difficulties of factoring the product of two extremely large prime numbers (1024 bit to 2048 bit long). The protocol of the RSA algorithm is presented below:

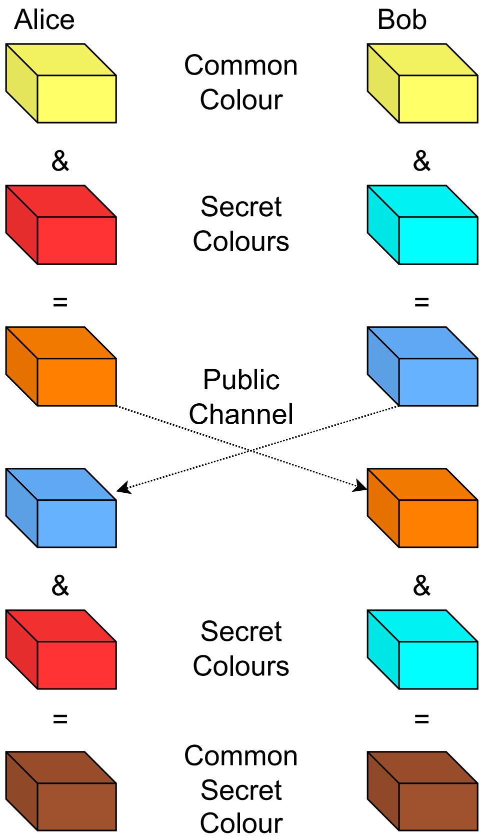


Figure 2.1: Illustration of Diffie-Hellman key exchange with colours. Figure reproduced from [44].

Rivest-Shamir-Adleman Key Exchange Protocol

1. Alice first chooses two large prime number p and q which are kept a secret and are distinct from one another.

2. Alice computes $n = p \times \ q$ which is released as part of the public key.

3. She then computes θ such that $\theta = (p - 1)\ (q - 1)$.

4. After that, Alice chooses an integer e, such that $1 < e < \theta$ and $\gcd(e, \theta) = 1$. e is also released to the public.

5. She also computes d, where $de \equiv 1 mod(\theta)$. d is kept a secret and is defined as the private key .

Rivest-Shamir-Adleman Encryption

To encrypt the messages, Bob obtains Alice's public key n, which he can use to send a message M to Alice.

1. He first turns his (un-padded) message M into a (padded) plaintext integer m, such that $0 \leq m < n$.
2. Bob then encrypts the message and produce the ciphertext $c \equiv m^e (mod\ n)$.

Rivest-Shamir-Adleman Decryption

To retrieve the message, Alice needs to decrypt the ciphertext c to produce the plaintext m and convert it back to its original from M.

1. Alice recovers the plaintext by using her private key d and computing $m \equiv c^d (mod\ n)$.
2. Given m, Alice can now recover the message M, by reversing the padding scheme applied by Bob.

RSA is being widely used for many applications, however, as mentioned before it is not secured against quantum computers [29]. Furthermore, intruding the random bits to the message M using padding is crucial to reserve the security of the RSA algorithm [46].

2.1.3 Authentication

We have described both symmetric-key and public-key (asymmetric) algorithms, and we highlighted that if Alice and Bob meet in person (which is not realistic for most applications), symmetric-key algorithms can be used. We also introduced the public-key algorithms as a way for Alice and Bob to exchange secret keys without meeting each other. However, how can we be sure that Alice is communicating with Bob and not with an adversary, Eve. In other words, how can Bob be sure that he is using Alice's public key to encrypt his messages and not Eve's. Without being sure, Alice and Bob are an easy target for a man-in-the-middle (MitM) attack [47].

Assuming Eve is aware of the communication protocol between Alice and Bob, she can appear to Alice as Bob and Bob as Alice. For instance, let's assume Alice wants to communicate with Bob and asks for his public key. If Eve can intercept Bob's public key, a MitM attack can begin. Eve can take complete control of the communication by providing her public key to Alice and using Bob's public key to transfer the message to him. Therefore, when Alice wants to communicate with Bob, she encrypts the message using Eve's public key and sends the encrypted message to Eve. Eve can decrypt the message using her private key and have the plaintext. Eve can encrypt the message using Bob's public key to send the same message to Bob. This way, Bob will decrypt the message using his private key without knowing that Eve has already intercepted it. Eve can also alter the message and send it to Bob if she wants. To prevent a MitM attack, Alice and Bob need to authenticate the communication.

To verify that the message came from the other person, Alice and Bob must use an authentication protocol. In such protocols, an authentication tag could be sent with their messages to make sure it has not been intercepted by Eve. Authentication is usually achieved by using a pre-shared key for the first communication between Alice and Bob (which is the case for current QKD systems). Authentication remains one of the main concerns for QKD today, and in their white paper, the National Cyber Security Centre (NCSC) highlights this and advises using quantum-safe cryptographic (post-quantum) mechanisms for authentication [48].

2.1.4 Post-Quantum Cryptography

Since the current public-key cryptography is considered obsolete using Shor's algorithm [29], an alternative is needed to secure against quantum computers and algorithms. Post-quantum cryptography (PQC) [49–51] has been suggested as an alternative to public-key cryptography on the premise that it will remain secure against advances in quantum computing architectures. PQC algorithms use classical computers, and their security is based on different problems. Similar to QKD, PQC fall under the umbrella of quantum-safe cryptography. PQC algorithms include Lattice, Code based and Hash cryptography along with Isogeny, Multivariate, and Symmetric key algorithms [52].

The National Institute of Standards and Technology (NIST) began a competition in 2016 to develop PQC standards [53, 54]. The primary motivation of this competition is to standardise new quantum-safe public-key encryption and digital signature algorithms. In 2017 [55], NIST received 82 submissions, from which 69 were accepted to move to the second round [56]. In 2019, 26 were advanced to round two [57], and in 2020 only seven (plus another eight alternates) were advanced to round three [58]. From the third round, one of the most popular algorithms, Rainbow, was completely broken using an off-the-shelf laptop [59], three were weakened [60], and NIST announced only four to be standardised [29]. However, three of these four algorithms are used for digital signatures, and only one is used for public-key encryption.

Given that only 4 out of the 82 submissions are being standardised, and three are for digital signatures, a lot of research is required to learn the process of turning hard mathematical problems into public-key algorithms. However, the landscape of cryptography is changing rapidly, and in the meantime, PQC is the one solution for standard and cheap quantum-safe cryptography. Another solution is increasing the key length of the commonly used public key algorithms such as RSA.

2.2 Quantum Information Processing

Quantum information processing utilises the principle of quantum mechanics, such as the superposition principle, quantum entanglement and quantum interference, to provide secure protocols for communication and key distribution. In this section, We focus on the most important principles used to develop QKD systems.

2.2.1 Quantum Mechanics Principles

The basic principles of quantum mechanics such as Heisenberg Uncertainty Principle and no-cloning theorem are exploited in quantum cryptographic systems to achieve information-theoretic security. Heisenberg Uncertainty Principle and no-cloning theorem are briefly discussed in the section.

1. **Heisenberg Uncertainty Principle**
   The first basic principle is Heisenberg uncertainty principle, which states that in a quantum system with a pair of conjugate properties, only one can be known for certain. Initially, Heisenberg indicated that any measurement of the position or the momentum of a particle would disturb the conjugate property and therefore the whole system [61]. Consequently, it is impossible to ascertain observe both properties simultaneously. Quantum cryptography implements Heisenberg uncertainty principle to detect an eavesdropper. For instance, in a system where polarized photons are exchanged through a quantum channel, any attempt of observing the photon's polarization will disturb the system; hence detecting the existence of an eavesdropper [62]. These principles are applied in many QKD protocols.

2. **No-cloning Theorem**
   Another principle that enhances the security of any quantum system and instinctively supports Heisenberg uncertainty principle is the no-cloning theorem, which proves that it is impossible to copy an unknown quantum state [63]. Without the no-cloning theorem, multiple copies of a specific quantum state can be produced which allows for measuring the different properties of each copy. Therefore, both conjugate properties of a particle could be measured simultaneously which distributes the quantum state.

2.2.2 Quantum Bits

A quantum bit (qubit) is the most fundamental unit of quantum information and it is the quantum equivalent of a classical bit. It represents a two-state quantum-mechanical system, for example, electron spin (up or down) or photon polarization (horizontal or vertical) [64, 65]. A qubit is the analogue of a classical bit and can exist in a quantum superposition, which means it can be both 0 and 1 simultaneously as shown in Equation (2.5). The state of a qubit can be written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \quad , \quad \phi = \gamma\,|0\rangle + \delta\,|1\rangle = \begin{bmatrix}\gamma\\ \delta\end{bmatrix} \tag{2.5}$$

Where α and β are complex number and $|\alpha|^2$, $|\beta|^2$ are the probabilities of finding the qubit in the state $|0\rangle$, $|1\rangle$ respectively. Furthermore, $|\alpha|^2 + |\beta|^2 = 1$. Therefore, the qubit must be found in one of these two states. In other words, we could choose to represent the states $|0\rangle$ and $|1\rangle$ as the following:

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad , \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.6}$$

Furthermore, two classical bits can be represented in any of the four states, 00, 01, 10 and 11. Similar to a single qubit, two qubits can have different weights for all four states at the same time. We can represent two qubits as the following:

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \tag{2.7}$$

Similar to a single qubit, α, β, γ and δ are complex number and $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. For instance if $\alpha = \gamma = \frac{1}{\sqrt{2}}$ and $\beta = \delta = 0$, we have an equal probability of 50% of finding $|00\rangle$ and $|11\rangle$ and no chance of finding the other two states $|01\rangle$ and $|10\rangle$, which gives us the following Bell state:

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.8}$$

2.2.3 Measurements

A measurement of the qubit forces the system into a single term of the superposition. Taking the famous Schrödinger cat as an example, until the measurement (opening the box) takes a place, the cat is both dead and alive. For instance in our basic example where $|\psi\rangle = |0\rangle$, the system is 100% in the zero state if the measurement is performed along the Z axis. For $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, the system is in superposition. However, once Alice observes the system and determines the state (e.g. 0), this result will force the entire system to a state where the qubit has been zero all along. Measurement is an extremely complicated topic and is out of the scope of this thesis. For further information, the reader can check [66] and the famous Preskill's lecture notes [67, 68].

2.2.4 Encoding

Qubits ($|0\rangle$ and $|1\rangle$) are encoded in multiple ways, such as nuclear spins, electron spins, photons polarisation, phase, and path. In quantum communication applications, quantum information is sent between two distant parties, Alice and Bob. Since light is the fundamental way to transmit data in the current communication networks, most of the quantum applications choose to encode the qubits using photons due to their compatibility with the existing network infrastructure i.e. fibre links. In this section, we will discuss different ways to encode qubits which are shown as shown in Figure 2.2.

Polarisation

Polarisation is the most common way that is used in entanglement-based quantum networks and free space applications. We can encode the qubit as $|0\rangle$ as $|H\rangle$ and the qubit $|1\rangle$ as $|V\rangle$ as shown in Figure 2.2 a). By manipulating the phase and amplitude of these states, we can access the entire Bloch sphere. This manipulation is performed using half-wave plates (HWP) and quarter-wave plates (QWP). For applications in entanglement-based quantum networks, fibre polarisation controllers are usually used to control the polarisation and to maximise the visibility of the quantum states.

Path

Path encoding is usually used in integrated circuits due to their phase stability. Two separate waveguides provide two different paths, where qubits are encoded with the relative phase and intensities between the different paths. For instance, if the photon goes through the top path, it is encoded as $|0\rangle$. Whereas, if it goes through the bottom path, it is encoded as $|1\rangle$ as shown in Figure 2.2 b). To manipulate the states, phase modulators and beam splitters can be used.

Phase

Phase encoding is implemented on most of the commercially available QKD systems, including the ID Quantique Clavis^2 system which is used in the experiments in Chapter 3, Chapter 4 , and Chapter 5. In this approach, the states are encoded in the phase difference between two pulses. The states can be manipulated using phase modulators. This approach is explained in detail while discussing the ID Quantique Clavis^2 operation in Section 3.3.2.

Time-bin

The time-bin allows us to encode the states based on the time of arrival as shown in Figure 2.2 c). This approach is implemented in the ID Quantique Clavis^3 system, which is described in detail in Section 5.2.1 and is used in two experiments in Chapter 5. To summarise, the states are encode in an early and late time-bins. If the detection occurs in the early time-bin (early time-bin is filled and the late time-bin is empty), it is encoded as $|0\rangle$, top part of Figure 2.2 c). However, if the detection occurs in the late time-bin (the early time-bin is empty and the late time-bin is filled), it is encoded as $|1\rangle$, bottom part of Figure 2.2 c). Phase and time-bin encoding are most common in fibre optics applications due to the instability of path and polarisation encoding in such applications.

2.3 Quantum Computing

Quantum computers differ from classical computers due to their capabilities of storing and manipulating quantum states. In principle, quantum computers perform massive computations, allowing us to observe all 2^n possible states simultaneously in a single operation. Such fast and massive calculations introduce the possibility of breaking the RSA and DH key exchange encryption algorithms currently used to encrypt critical information on the internet [70]. Although quantum computers represent all possible states at once, the challenge is to extract valuable information after being read using dedicated hardware devices. Therefore, quantum

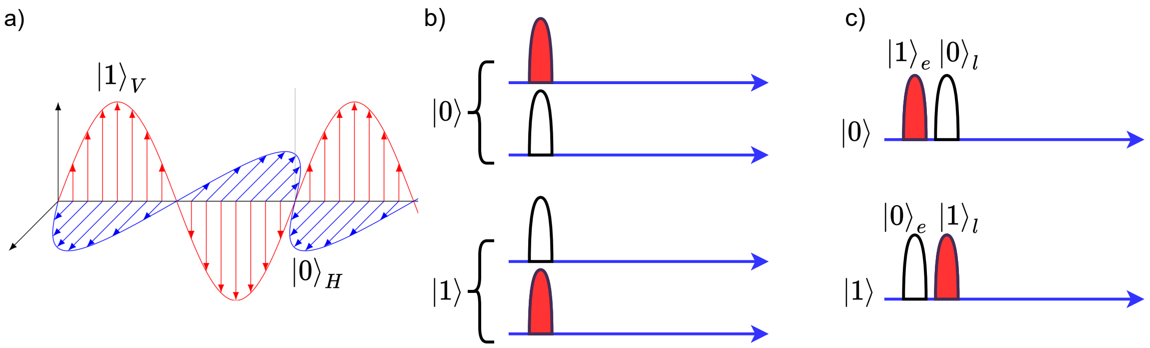


Figure 2.2: Different photon encoding methods using: a) The orthogonal polarisation H and V of light. b) the path of photons (spatial encoding). c) The early e and late l time-bins of the photons. Figure reproduced from [69].

algorithms are used to increase the likelihood of the desirable states until the system reaches a threshold, indicating a faster processing time than classical computers [71]. Several algorithms have been developed in quantum chemistry calculations [72, 73], machine learning [74], linear algebra [75] and vector space problems [76].

2.4 Quantum Key Distribution

Quantum key distribution (QKD) enables the exchange of theoretically secure information, symmetrical keys with the unique ability to detect the presence of eavesdropping third parties [32]. As mentioned, QKD is considered quantum-safe because the keys are generated by exploiting quantum mechanics rather than computationally complex functions used in public-key cryptography protocols. In QKD, whenever the distribution of symmetric keys is undertaken by transmitting photons between Alice and Bob, and eavesdropping occurs over the quantum channel, Eve's measurement will generate higher error rates allowing Alice and Bob to be able to verify the secrecy of the key and detect the intrusion. Eve will also be prevented from learning the secret key since any attempt to gain information about the photons will irreversibly change them.

2.4.1 Quantum State Sources

1. Single photon source: Although single photon sources have been improved significantly during the last decade, devices that generate a single photon are far from reality. Conventional laser sources do not have the ability to produce a photon number state (i.e. a state containing a specific number of photons) [77]. However for most QKD systems, weakly attenuated laser pulses are used to generate weak coherent states which are very easy to implement and simple to handle. In these states, the average number of photons is less

than 0.2 photons per pulse. Moreover, a decoy state is usually implemented to prevent a number of attacks including a photon-number splitting attack. The ID Quantique Clavis[2] and Clavis[3] systems use weak optical coherent pulses.

2. EPR source: By using nonlinear optical processes, such as spontaneous parametric down-conversion (SPDC) [78], an entangled pair of photons can be generated by converting a single photon with high energy into a pair of low-energy photons (a signal and an idler) using a nonlinear crystal as shown in Figure 2.3. According to the law of conservation of energy and momentum, the generated photons are entangled in spectral and spatial domains. Due to the changes in frequency caused by the refractive index of the crystal, a phase match is required to achieve energy and momentum conservation. Other methods such as four-wave mixing in optical fibre [79], are also used to generate an entangled pair of photons.

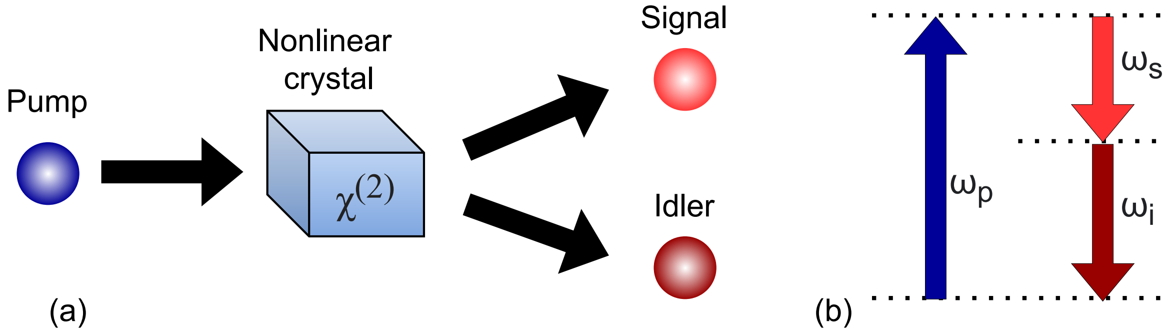


Figure 2.3: (a) Generation of photon pairs in the SPDC process. A pump photon of frequency ω_p decays to two photons of frequencies ω_s and ω_i , known as signal and idler, respectively. (b) Illustration of energy conservation in the SPDC process. Figure reproduced from [80].

2.4.2 Quantum State Detection

Two technologies of QKD detection are presented below:

1. Single photon detectors (SPDs): As mentioned above SPD are implemented in DV-QKD systems. SPDs usually are used in highly nonlinear regions, i.e. when detecting a photon an eclectic pulse is generated. These types of detectors are called "threshold detectors" because they distinguish between a vacuum state and the detection of a photon, however, they do not have the ability to quantify the number of photons [81, 82]. The following four parameters are used to evaluate the performance of SPD.

    - Detection efficiency which is the probability of recording the incoming photons correctly.

- Dark counts which is the registration process when no photon hits the detector. Dark counts probability contributes to the QBER of any QKD system.
- Deadtime which is the rest period after receiving a photon. The SPD will not register incoming photons during this period.
- Time jitter which is the time-domain fluctuation of the electric pulses generated by the SPD.

Two types of SPDs are briefly discussed below:

a) Avalanche photodiodes SPD (APDs-SPD): It is a highly sensitive semiconductor which converts the lights (photons) to electricity by exploiting the photoelectric effects. APDs have been implemented as SPDs in many QKD systems [83–85]. In APDs, the applied voltage exceeds the breakdown voltage in the Geiger mode, where an avalanche current is triggered by absorbing a single photon. Silicon APDs are used in free space QKD systems, while InGaAs APDs are used for QKD system which operates at telecommunication wavelength. APDs have high efficiency (60%) in the visible spectrum, while InGaAs/InP APDs have 25% efficiency in the C-band with a low dark count rate with 50 Hz, a deadtime as low as 2 μs and 150 ps timing resolution [86].

b) Superconducting nanowire single-photon detectors (SNSPDs): SNSPDs are being used for most quantum experiments due to their extremely high efficiency (>90%) and low time jitter of $\approx$ 10 ps [81]. They also have an extremely low dark count rate with 1 Hz [87]. Such properties make SNSPDs very attractive for applications where high efficiency is needed. However, SNSPDs require extreme cooling to sub-0 K temperatures. They are also extremely expensive and require more servicing than APDs.

2. Optical homodyne detectors: Homodyne protocols are mainly used in CV-QKD and current classical coherent communication systems. This type of detector is very sensitive to electric noise and thus necessitates that a strong local oscillator limiting the shot noise is used to decode the transmitted information [88]. The local oscillator also produces interference to strengthen the weak signal during the detection. Therefore, homodyne detectors have much higher efficiency compared to SPDs. On the contrary, homodyne detectors require stabilization of the relative phase between the oscillator and the signal. An attenuator is applied to the local oscillator since its signal power is significantly higher than the quantum signal to provide a symmetric detection on the receiver side.

2.4.3 Quantum Random Number Generator (QRNG)

QRNGs are essential devices in any cryptographic system. In prepare and measure-based protocols, a high randomness is required to choose the encoding bases by Alice and the decoding bases by Bob, therefore, a QRNG is required for both the transmitter and the receiver [89]. Pseudo-random number generators (PRNGs) are based on algorithms using mathematical formulae or pre-calculated tables. Whereas, true random number generators (TRNGs) are based on the environment or a physical phenomenon such as unstable oscillations. PRNGs and TRNGs are not applicable for QKD systems due to their deterministic properties [90, 91]. Figure 2.4 shows the basic principle of QRNG which is designed at a single photon level. After the pulsed laser emits photon pulses to a 3 dB beam splitter (50/50 BS), the photons are split into one of two SPDs (D0 and D1). If the photon is detected by D0 or D1 a bit 0 or 1 is registered accordingly.

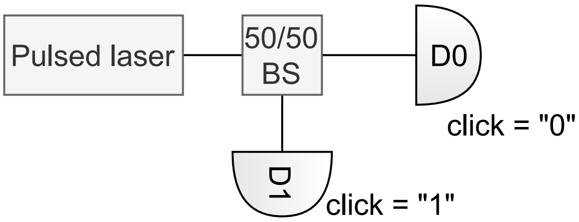


Figure 2.4: Concept for a QRNG.

2.4.4 Entanglement

Two states are entangled when an operation on the first state affects the other and vice versa. Furthermore, the probabilities of two entangled states are not independent. Einstein, Podolsky, and Rosen (EPR) studied entangled states in 1935 [92] and the three scientists argued that quantum mechanics must be incomplete and it includes hidden variables, however, Niels Bohr disagreed with them. John Bell suggested that the "non-local nature" could be tested statistically by repeating an experiment on entanglement pairs for a large number of times [93]. The results could be then analysed to check for hidden variables. Bell characterised local and non-local actions and formulated them into an inequality, which is known as Bell's inequality [93]. If the inequality holds, hidden variable theory along with classical probability is enough to describe the results. However, if the inequality is violated, only non-local variables can explain the results. There are four entangled two qubits states that are used in quantum cryptography, which are known as the Bell states:

$$|\Phi^{+}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.9}$$

$$|\Phi^{-}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.10}$$

$$|\Psi^{+}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.11}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.12}$$

As shown in the previous equations, a Bell pair has two qubits which are entangled and their state is not independent. Therefore, once we measure and know the results for the first measurement, we can predict with certainty the second measurement. In the case when we have the state $|\Phi^+\rangle$ Bell pair, we have 50% probability of finding either $|00\rangle$ or $|11\rangle$, and no chance of finding different states. However, in $|\Psi^+\rangle$ the qubits are anti-correlated. Therefore, if Alice measures a zero, Bob will measure a one and vice-versa.

John Bell formulated his inequality in 1964 [93], and following that multiple experimental demonstrations have been performed and demonstrated the violation of the inequality [94–97].

2.4.5 Protocols

QKD protocols are divided into three main categories, discrete-variable QKD (DV-QKD), distributed-phase-reference QKD (DPR-QKD), and continuous-variable QKD (CV-QKD). In this section, a brief discussion of all three protocols is presented with a comparison in terms of performance and limitations.

Table 2.2: DV-QKD vs CV-QKD

	DV-QKD	CV-QKD
Quantum State	Polarization, phase, or timebin of a single photon	Quadrature components of quantized electromagnetic field
Source	Single-photon source	Coherent-state or squeezed-states source
Detector	Single-photon detector	Homodyne or heterodyne detector
Distance limitation	Performance of single-photon detectors	Efficiency of post-processing techniques

2.4.6 Discrete-Variable Quantum Key Distribution

DV-QKD protocols are divided into prepare and measure based protocols and entanglement based protocols. In these protocol, week coherent pulses or an entangled photon source are used to generate single photon pulses, where Alice prepares and encodes the information of the transmitted pulses using the polarization, phase or time of arrival of the photons. Subsequently, Bob measures the state by employing single photon detectors (SPDs) to detect the photons and he decodes the information using random bases. These bases are then shared with Alice for the detection process. After the raw key exchange, classical post-processing is requited for every DV-QKD protocol [98].

2.4.6.1 BB84 Protocol

BB84 is the first QKD protocol which Bennett and Brassard introduced in 19841, and it is classified as a prepare-and-measure-based protocol [30]. BB84 protocol has been proved

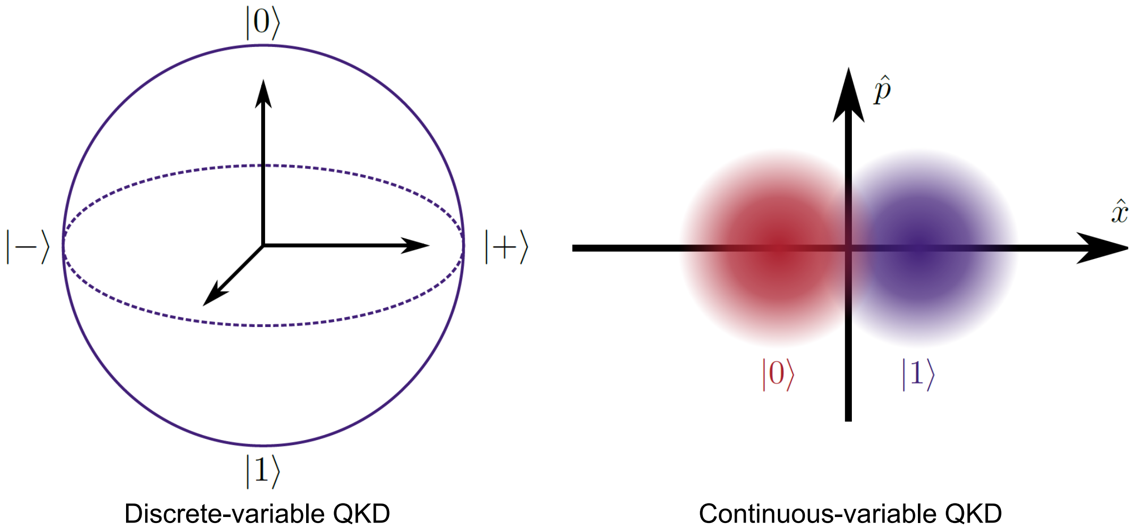


Figure 2.5: States used to encode information for DV-QKD and CV-QKD. Figure from [69].

theoretically to provide unconditionally security [99]. BB84 uses quantum polarisation to share the secret key information between Alice and Bob through a quantum channel. The single photon is polarised in one of four states either rectilinear or diagonal basis as shown in Figure 2.6. A horizontal/0° polarization of photon or a diagonal/45° polarization represent a bit value of 0, while a vertical/90° polarization or a diagonal/135° (−45°) polarization represent a bit value of 1 [32]. The bases $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$ represent the logical qubits $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ respectively from Figure 2.5. Mathematically the BB84 states are:

$$|H\rangle = |0\rangle \quad , |V\rangle = |1\rangle \quad , |D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \quad , \quad |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \tag{2.13}$$

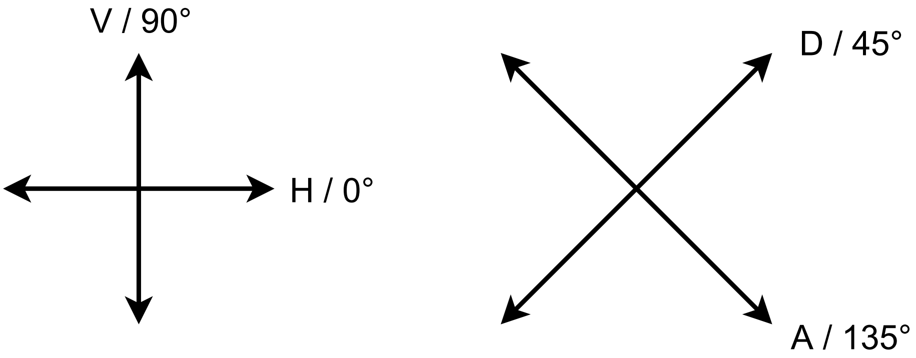
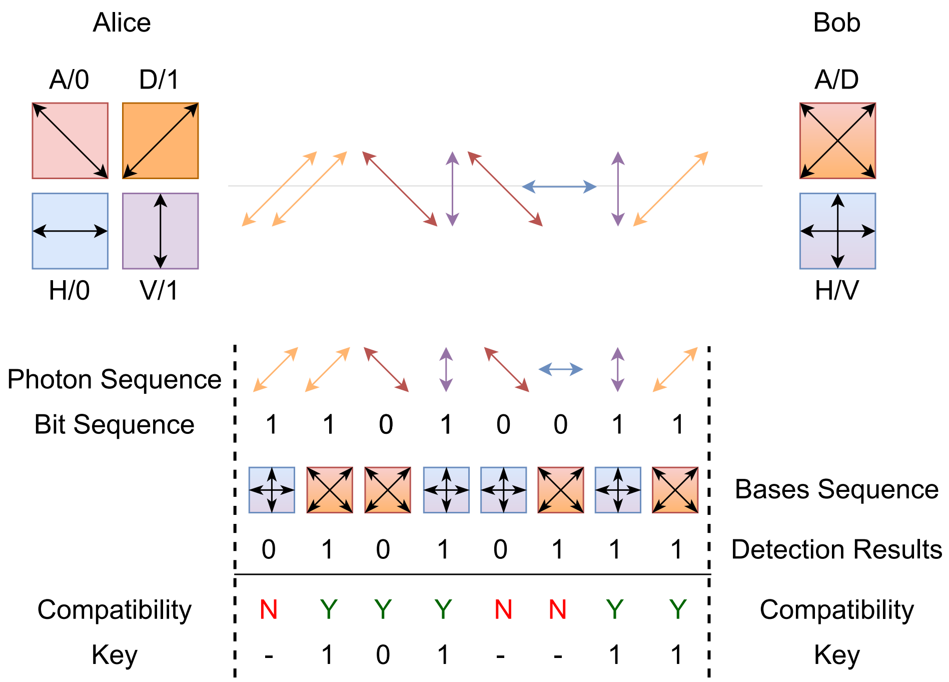


Figure 2.6: The four polarisation states, $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$.

In BB84, Alice chooses a random state out of the four BB84 states to transmit through the quantum channel and before receiving the photon, Bob randomly decides whether to use rectilinear basis (H/V) or diagonal (A/D) bases as shown in Figure 2.7.



Bit Sequence	1	1	0	1	0	0	1	1	
	0	1	0	1	0	1	1	1	Detection Results
Compatibility	N	Y	Y	Y	N	N	Y	Y	Compatibility
Key	-	1	0	1	-	-	1	1	Key

Figure 2.7: Illustration of BB84 Protocol. Figure reproduced from [30].

After selecting a bases, Bob communicates through the authenticated classical channel with Alice its bases choice and Alice shares the whether the right bases was used. They both discard all events where different bases were chosen resulting in a sifted key. Using some of the bits in the sifted key, they compare some bits randomly to check for eavesdropping. Based on the results, Alice and Bob will either abort to the protocol or move to the final step of the process, privacy amplification. In this step, Alice and Bob sacrifice bits of their secret key to further reduce Eve's knowledge and satisfy security requirements.

2.4.6.2 E91 Protocol

In 1991, Ekret proposed a new QKD protocol where the secret key is shared using quantum entanglement principles [31]. E91 protocol uses a single photon source that emits pairs of entangled photons, that are shared between Alice and Bob. E91 protocol utilises the correlation between entangled states and realises that the measurement of two entangled photon must be correlated (as explained in Section 2.2). Furthermore, Alice and Bob can use Bell's test and the Clauser, Horne, Shimony and Holt (CHSH) inequality to proofs Bell's theorem [100] and to test for the existence of Eve [93]. The presence of an eavesdropper is detected using Bell's inequality test which should not hold for the entangled particles. However, if the particles are entangled the inequality does hold, this indicates the existence of an eavesdropper. The E91 protocol works as follows. Alice generated an entangled state (e.g. any of the four Bell states in Equation (2.9)) using an EPR source. She then keeps one qubit and send the other one to Bob. After that, they both independently choose a random CHSH angle [100] to measure their qubit (similar to the measurement bases by Bob in BB84 protocol). After transmitting and measuring sufficient number of entangled states, they announce their measurement bases. After that, a random set from the measurement results is chosen to calculate the CHSH inequality and verify whether the state was entangled. If the Bell inequality is violated, the reminder of the events should be correlated. In the final step, Alice and Bob preform error correction and privacy amplification.

2.4.6.3 BBM92 protocol

In 1992 shortly after Ekert proposed the E91 protocol, Bennett, Brassard, and Mermin presented BBM92 protocol [99]. BBM92 protocol uses an entanglement photon source similar to the E91 protocol, however, entanglement is shared between Alice and Bob without having to show a violation of the Bell Inequality. The raw key exchange mechanism and the post-processing of the BBM92 are identical to those in the BB84 protocol. We use the BBM92 protocol in all the entanglement-based experiments in Chapter 6.

2.4.7 Diffierential-Phase-Reference Protocol

Diffierential-Phase-Reference (DPR) protocols were developed to overcome security issues of QKD systems when using realistic equipment. In DPR protocols, Alice typically uses weak coherent states which are prone to photon number splitting (PNS) attacks and it encodes photon using their time-bins or relative phases. DRP protocols include coherent one-way protocol (COW) [101] which is implemented by the ID Quantique Clavis[3] and Diffierential-phase-shift (DPS) [102].

2.4.7.1 Coherent one-way Protocol (COW)

In COW protocol [101], quantum states are encoded in time function and the pulses are generated from a continuous wave (CW) laser. As shown from Figure 2.8, the coherent pulses are generated using a laser which are then passed to an intensity modulator. After that, the pulses are encoded in a sequence of two pulses using time slots which are separated by a period T. The time slots are divided into either 0 pulses which contain no light (empty pulse) or μ pulses where the mean number of photos is $\mu < 1$ (non-empty pulse). In COW protocol, $|0\rangle$ is detected when we have μ-0 pulses, $|1\rangle$ is detected when we have 0-μ pulses, and decoy state detected when we have μ-μ pulses. The time of arrival of the received pulses is then registered using the detector D_{bit} for the data line and the detector D_{mon} for the monitoring line. Moreover, the raw key bits are extracted from t_b time slots to check the coherence of the data. On the other hand, the D_{mon} detector is used to check the security of the system using the decoy sequence. Finally, the interferometer detects the existence of an eavesdropper to estimate the information obtained by Eve. This protocol is easy to implement and robust to PNS due to the employment of a decoy sequence. It also offers a reduced visibility attacks and provides a better data rate than previous protocols. The COW protocol is implemented by the ID Quantique Clavis[3] system which is discussed in details in Chapter 5.

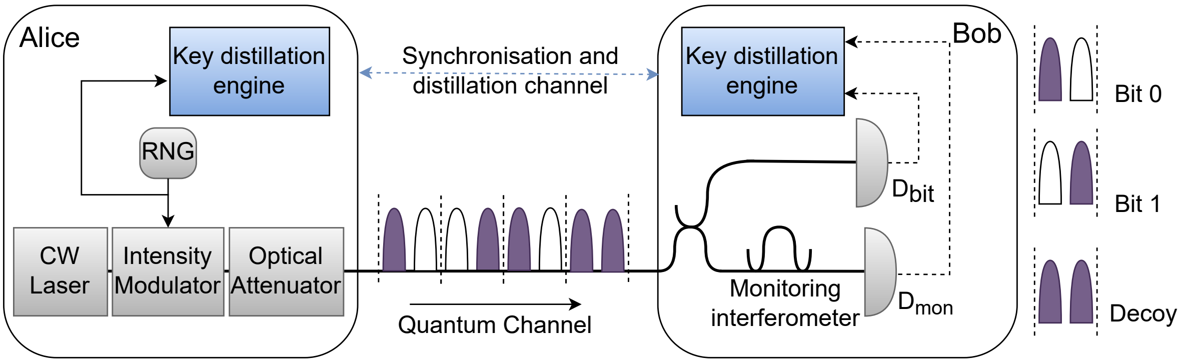


Figure 2.8: Illustration of COW protocol principle. Figure reproduced from [101].

2.4.8 Continuous-Variable Quantum Key Distribution

CV-QKD has gained a lot of interest lately because it uses off-the-shelf telecommunication equipment [103]. In a CV-QKD system, the information in encoded in either a Gaussian states [104], or squeezed states [105]. Moreover, single photon detectors are not needed, Bob instead uses commercial photodiodes to perform the measurement using homodyne or heterodyne detection. Similar to the basic principles of a prepare and measure protocol, Alice randomly encodes the information from a set of overlapping Gaussian states (Gaussian modulation) or by randomly choosing two quadrature (squeezed states). The states are then sent to Bob via a quantum channel, and Bob measures the state by switching between the two quadrature (homodyne), or by measure in the two quadratures using two detectors (heterodyne). Both Alice and Bob then use the classical channel to compare bases (quadratures) and perform parameter estimation using some of the matching bases, and finally they perform privacy amplification. A detailed comparison between DV-QKD and CV-QKD is presented in [106–108].

2.4.9 Challenges

There are multiple challenges that are limiting the adoption of QKD solutions in the current classical infrastructure. We are going to focus on three challenges and propose solutions for each challenge.

1. Cost: The cost of a commercial QKD system is currently in the \$100,000s. For the cost to be cheaper mass-manufacturability is needed, and therefore, more vendors of this technology.
2. Static nature (point-to-point): The other issue of the current commercial QKD systems is that they are point-to-point systems. Therefore, if an end-user needs to secure multiple nodes, they need a pair of QKD device for each link. This approach increases the overall cost of the network and does not utilise resource allocation. The first solution is to add a layer of dynamicity to the network by deploying an optical switch and a controller. This approach is discussed in detail in the next chapter (Chapter 3). Another solution is by implementing an entanglement-based QKD network, since a single entanglement source is used to distribute the entangled states to all the users, hence reducing the resources. However, the key rate in such network is still low and cannot be used for practical applications. This approach is discussed in details in Chapter 6.
3. Sensitivity and tolerance to noise: Finally, coexisting quantum and classical channel is an extremely difficult task due to the high power of the classical channels (orders of magnitudes higher than the quantum channel). The coexistence of quantum and classical channel in a single medium is essential for the wider deployment of QKD schemes and has been studied extensively. In Chapter 4 and Chapter 5, we discuss different coexistence techniques and mediums in detail.

2.5 Summary

In this chapter we introduced, 1) the different classical cryptography techniques which are currently used, 2) basic quantum theory and principles, 3) a brief distribution about quantum computing, 4) quantum key distribution which is the main topic of this thesis, 5) the challenges of implementing QKD and the proposed solutions. In the QKD section, we went thorough quantum state sources and detection, quantum random number generators, and the different QKD protocols.

The advances in quantum information theory allowed the existence of new quantum technologies such as quantum computer and QKD systems. Although quantum computer is considered a threat to public-key cryptography, QKD systems are considered one of the solution since they provide information-theoretic security.

2.6 Remarks

While writing this thesis, the 2022 Nobel prize in physics was awarded to Alain Aspect, John F. Clauser, and Anton Zeilinger for their work on quantum entanglement. More specifically, “For experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science”. Furthermore, Peter Shor, David Deutsch, Charles Bennett, and Gilles Brassard have won the 2023 Breakthrough Prize in fundamental physics for their contribution to the quantum information field. Their results and contribution to this field have paved the way for new quantum technology, and allowed new students and researchers like myself to dive into this amazing field. It is indeed great news for everyone in the quantum community.

CHAPTER 3

DYNAMIC QUANTUM COMMUNICATIONS IN OPTICAL NETWORKS

Declaration of Work

This chapter is based on [1, 21, 24]. I developed the final testbed physical layer design in collaboration with Emilio Hugues-Salas, while the SDN controller was developed by Rodrigo Stange Tessinari.
I built and characterised the testbed, measured the ID Quantique Clavis^2 QBER and SKR, processed the data except for the SDN controller part.
All of this work was done under the supervision of George Kanellos and Reza Nejabati.
Since I am the lead author of [1], parts of the article have been reused in the chapter where appropriate.

Quantum communication networks are evolving from relayed point-to-point quantum communication links to multi-user quantum networks with partial or full connectivity [106, 109]. Although the current quantum networks are mainly implementing QKD protocols which is the most mature quantum communication application [32], the future of quantum communication networks are needed to provide a worldwide connectivity via complex networks with a seamless interconnection between multiple nodes to enable applications beyond QKD such as blind and distributed quantum computing [110]. For such networks to reach their maximum capabilities, they should have the ability to integrate with the current classical telecommunications infrastructure, and be compatible with next-generation designs and architectures.

To this end, we have demonstrate a four-node trusted-node-free metro network configuration with dynamic DV-QKD networking capabilities across four optical network nodes. The network allows the dynamic deployment of any QKD link between two nodes of the network, while a QKD-aware centralised software-defined networking (SDN) controller is utilised to provide dynamicity in switching and rerouting.

We start this chapter by reviewing the different implementations in the popular QKD networks, such as optical switching, trusted relays, and untrusted relays. Followed by a brief description of the major metropolitan and long-haul QKD networks before highlighting the general architecture of QKD networks. After that, we introduce the UK quantum network and present the concept of the software-defined network before providing a detailed description of the Bristol dynamic QKD network. For the Bristol QKD network, we start by discussing the overall network architecture, followed by a description of the main components, such as the ID Quantique Clavis^2 QKD system [32] and the Polatis optical switch [111]. We then discuss the experimental system setup for the dynamic QKD network, followed by a discussion on the SDN control plane implementation. Finally, we present the results of the data and control plane and conclude the chapter by providing an evaluative summary of the main findings.

3.1 Advances in Quantum Key Distribution Networks

As shown in Figure 3.1, the implementation of QKD networks is growing rapidly, evolving from experimental lab-based testbeds to field trails in deployed optical fibres around the world. With such immense growth, a new novel implementation appears to facilitate the QKD networks for different scenarios. Here, we provide an overview of the different implementations and highlight the progress of metropolitan and long-haul QKD networks, concluding with a brief description of the general architecture of a QKD network.

3.1.1 Quantum Key Distribution Network Implementation Options

Based on the use case, the end-user application and specific node functionality, QKD network implementations usually fit within three categories; Optical switching, trusted relay-based and untrusted relay-based. Table 3.1 highlights the difference between the three options in terms of achievable distance, scalability, applicability, security, maturity, and field trial. Since quantum repeaters have not yet been demonstrated in a field trial, we opted to exclude them from the comparison.

1. *Optical Switching Based QKD Networks (Dynamic QKD Networks)*: Dynamic quantum network solutions are one option to overcome the established practice of relayed point-to-point quantum links and allow efficient resource sharing across the networks. Dynamic QKD would rely on the need for deployment of low-loss switching and routing elements for the quantum channel, allowing the quantum channel to be transmitted through multiple hops configuration without any interaction with trusted nodes. However, due to the extra loss from the optical switches, the performance of the quantum channel would degrade.

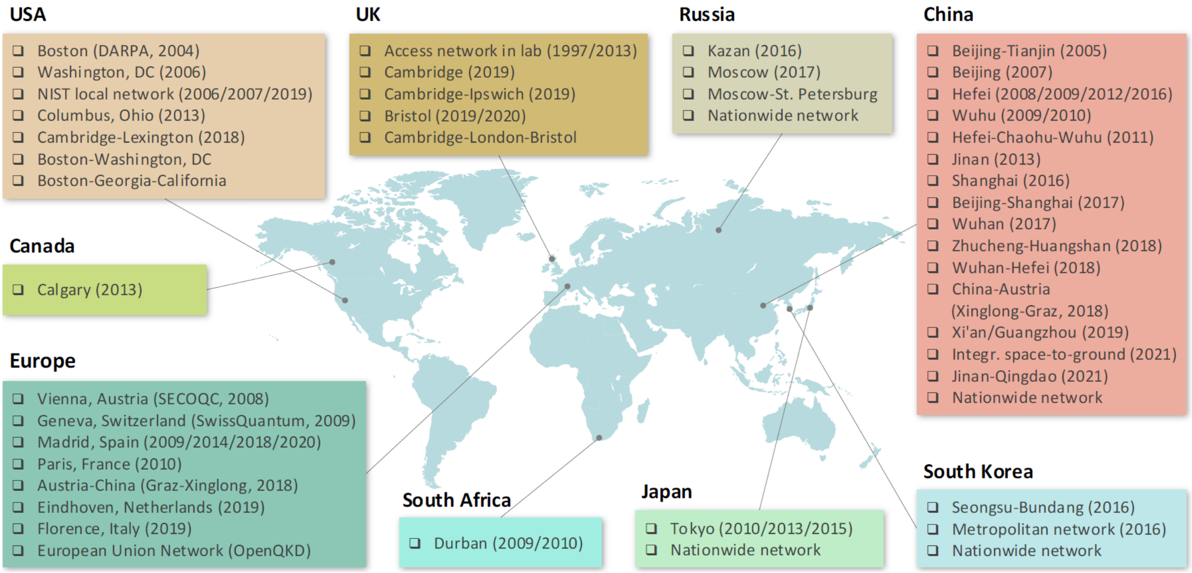


FIGURE 3.1. Overview of QKD network testbeds and field trials around the world [112].

Table 3.1: Comparison of different QKD network implementation options

	Optical switching	Trusted relay-based	Untrusted relay-based
Security	High	High	High
Distance	Relatively short	Arbitrary	Relatively long
Maturity	High	High	Relatively low
Field trial	Available	Available	Available
Scalability	Relatively low	High	Relatively low
Applicability	Limited	Wide	Limited

The concept leads to a trade-off between QKD performance in terms of SKR and increased network functionality with improved capabilities to maximise resource usage optimisation. However, this may be particularly appealing for optical networks in dense metropolitan regions of big cities, with the presence of a large number of nodes likes with short fibre length (<10km) [113]. This approach is used in the Bristol dynamic QKD network.

2. *Trusted Relay Based QKD Networks*: Commonly referred to as a trusted-node QKD network. A trusted node is an intermediate node between two QKD links containing a QKD device from each link that performs a relayed function between the two QKD links to establish an end-to-end QKD connection. In the absence of quantum repeaters, these nodes are used to extend the reach of the QKD system and to enable the distribution of secure keys between the endpoints. Having a pair of QKD devices allows the quantum-generated keys to be extracted and XORed with the keys of the QKD system in the next node. In that

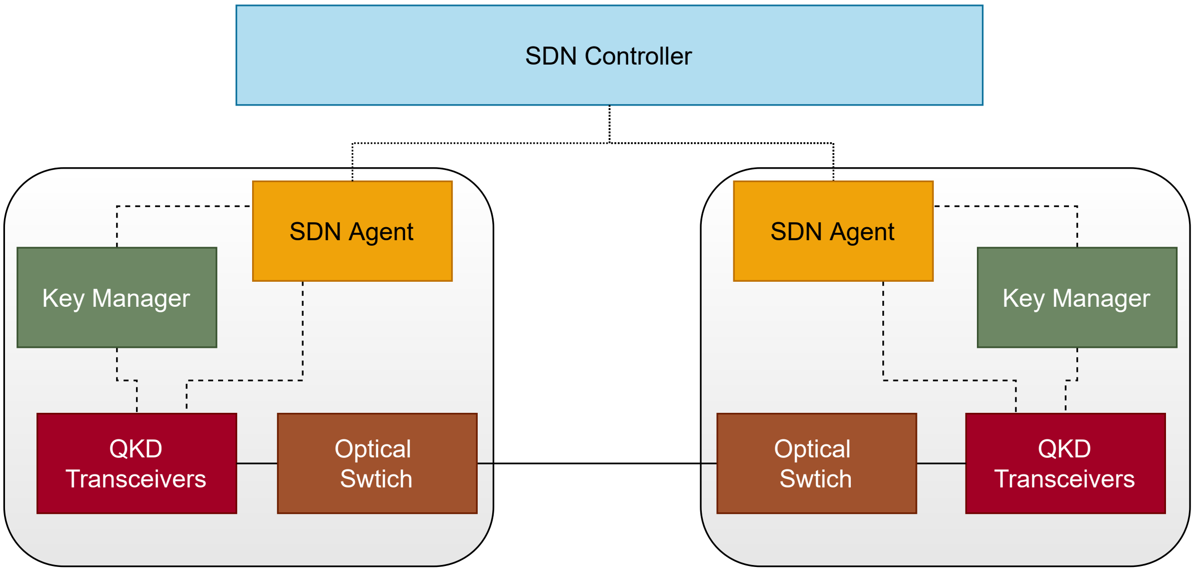


Figure 3.2: Illustration of optical switching based QKD networks.

sense, trusted nodes consume a sender (Alice) and a receiver (Bob) hardware at each intermediate node. Although trusted nodes add to the cost of the network in some cases where a link between every node is required, they are crucial to enabling long-distance end-to-end QKD operation. Furthermore, since all the nodes in the network, including intermediate trusted nodes, are assumed to be safe from eavesdropping, any access to a trusted node causes a potential security risk and relinquishes the strong security offered by quantum cryptography [114]. Therefore, a trusted-node-free network that relies on optical switches does not only reduce the cost, significantly relaxing the use of two QKD devices, but also does not stress the security requirements. However, it limits the transmission distance.

3. *Untrusted Relay Based QKD Networks*: In this scheme, the QKD networks employ more secure QKD protocols such as measurement device independent (MDI) [115] and entanglement-based protocols [31]. Such protocols allow the untrusted entity (Eve) to control the untrusted relay, removing all security threats at the measurement side, which is usually a third node (Charlie) in these protocols. Furthermore, such schemes would increase the transmission distance to increase to 100s km, which is the case using twin-field QKD [116–119]. However, since such networks allow using a single untrusted node only, the distance is limited compared to trusted-node QKD networks. Therefore, such networks are suitable for a limited range of QKD applications.

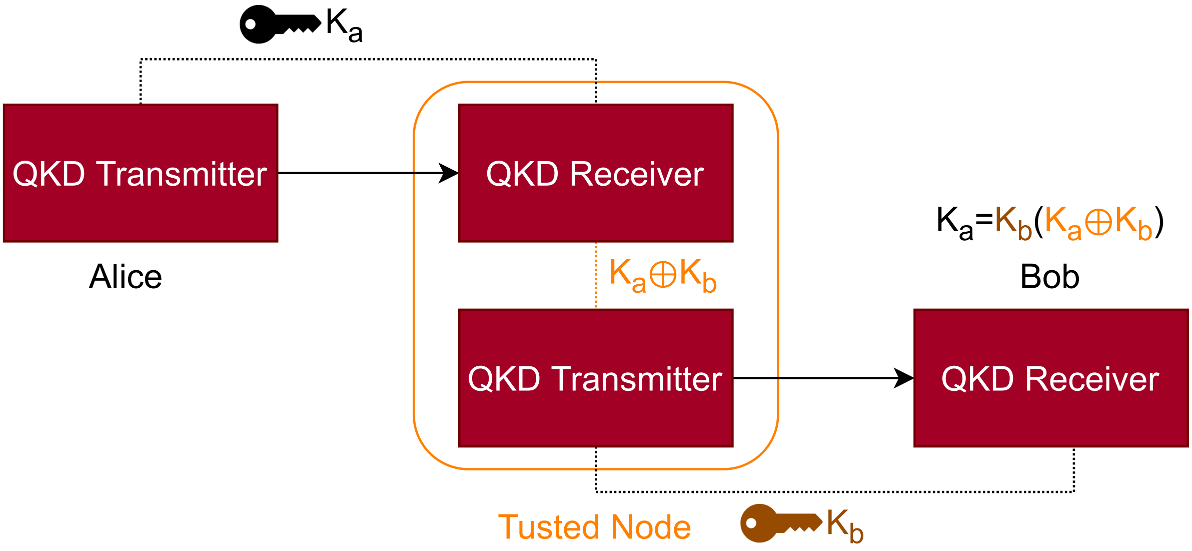


Figure 3.3: Illustration of trusted relay-based QKD networks.

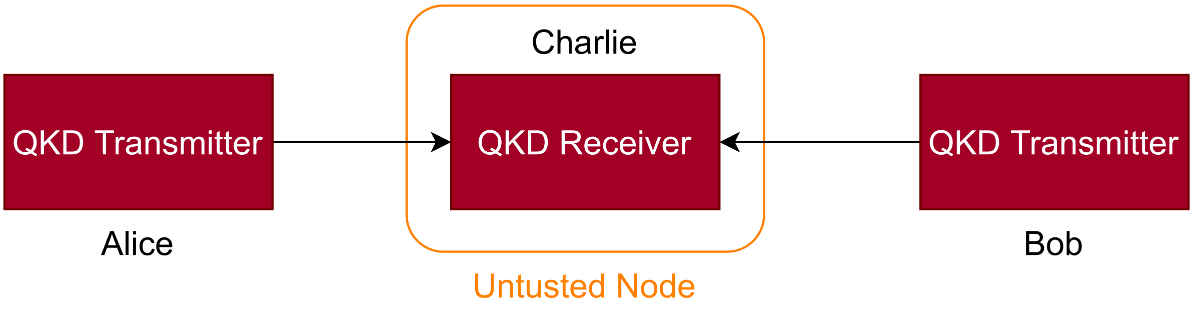


Figure 3.4: Illustration of untrusted relay based QKD networks.

3.1.2 State-of-the-Art Metropolitan Quantum Key Distribution Networks

Table 3.2 summarises the main features of the major metropolitan QKD networks chronologically. A brief description of selected deployed QKD networks is shown below.

1. *Boston Metropolitan Network*: The DARPA QKD network was the first demonstration of a QKD network in 2004. The DARPA QKD network implements the BB84 protocol and consists of 10 nodes where trusted nodes are used to extend the distance [120, 121].

2. *Vienna Metropolitan Network (the SECOQC QKD network)*: This network aimed to implement practical applications of the QKD technologies while considering the DARPA QKD network's initial results. The network infrastructure is based on point-to-point links between 6 nodes using a trusted node topology as shown in Figure 3.5. The network is the first to implement different QKD technologies, including an ID Quantique DV-QKD system,

which implements the BB84 (decoy state) and SARG04 protocols, an entanglement-based QKD system which implements the BBM92 protocol, a free-space QKD system that implemented the BB84 protocol, a COW system, a CV-QKD system and finally a weak coherent pulse (WCP) decoy state system [122–125].

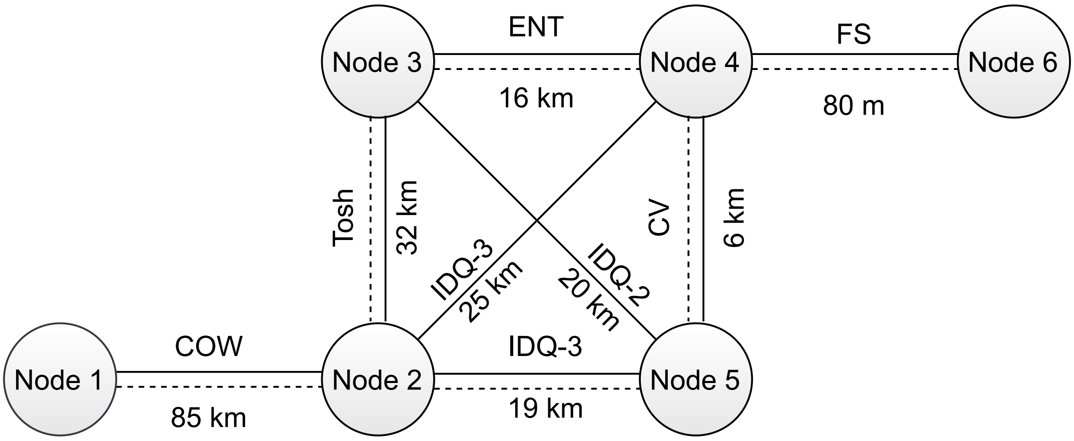


Figure 3.5: Connection scheme of the SECOQC QKD network. Solid lines represent quantum connections, while dotted lines represent classic communications connections. Figure reproduced from [122].

3. *Tokyo Metropolitan Network*: The Tokyo UQCC QKD network reaches two critical milestones: i) a record-high SKR of 304 Kbps and ii) a QKD link record of 90 km. The Tokyo QKD network is similar to the SECOQC in terms of infrastructure and is based on point-to-point links between 6 nodes using a trusted node topology as shown in Figure 3.6. However, the significant difference between the networks is the implementation of a Key Management System (KMS) for centralised management in the Tokyo QKD network. In addition, the network also uses different QKD technologies, such as an ID Quantique DV-QKD, which implements the SARG04 protocols, an entanglement-based QKD system which implements the BBM92 protocol and a DPS-QKD system [126, 127].

4. *Madrid Metropolitan Network*: Madrid quantum network consists of 11 nodes deployed in the city of Madrid. The network was used for a field trial demonstration of a dynamic software-defined CV-QKD quantum network using commercial optical switches [128, 129]. In this network, the classical and quantum channel coexisted in the same fibre (the coexistence is discussed in detail in Chapter 4 and Chapter 5).

5. *Cambridge Metropolitan Network*: The Cambridge Quantum metro network consists of three nodes acting as trusted nodes forming in a ring topology. In this network, the coexistence between quantum channels implementing a BB84 protocol with two decoy

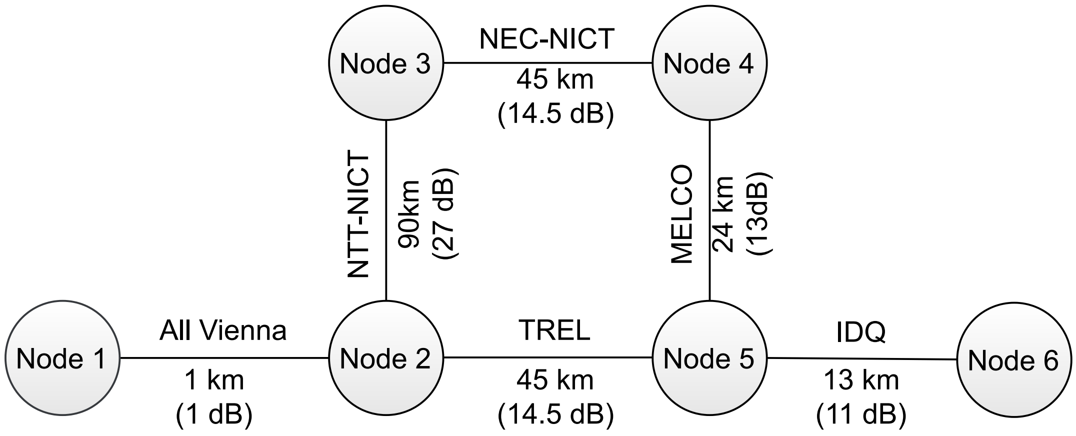


Figure 3.6: Topology of the Tokyo UQCC QKD network. Figure reproduced from [127].

states and 2 x 100 G classical channels was deployed using dense wavelength-division multiplexing (DWDM) techniques [130].

Table 3.2: QKD networks

Metropolitan	Optical	Trusted	Number	Longest Link		Max SKR	QKD	Year	Reference
Area	Switching	Relay	of Nodes	Length (km)	Loss (dB)	(kbps)	Type		
Boston	✓	✓	10	29.8	16.6	10	DV	2004	[121, 131]
Beijing	✓	✗	4	42.6	16.4	NA	DV	2007	[132]
Vienna	✗	✓	6	85	20.4	17	DV/CV	2008	[124, 125]
Hefei	✗	✓	3	20	5.6	1.6	DV	2008	[132]
Geneva	✗	✓	3	17.1	5.3	2.4	DV	2009	[133]
Durban	✓	✓	4	27	NA	0.89	DV	2009	[134]
Wuhu	✓	✓	7	10	6.23	2.53	DV	2009	[135]
Hefei	✓	✓	5	60	17	4.5	DV	2009	[136]
Madrid	✓	✗	3	NA	NA	NA	DV	2009	[137]
Wuhu	✓	✗	5	NA	14.77	4.91	DV	2010	[138]
Tokyo	✗	✓	6	90	27	304	DV	2010	[126]
Columbus	✗	✓	4	NA	NA	NA	DV	2013	[139, 140]
Jinan	✓	✓	56	NA	NA	NA	DV	2013	[114]
Madrid	✓	✗	3	16	5.12	NA	DV	2014	[141]
Hefei	✓	✗	4	55	17.3	0.038	DV	2016	[142]
Shanghai	✗	✗	4	19.92	15.1	10	CV	2016	[143]
Kazan	✗	✓	4	12.4	6.8	19.6	DV	2016	[144]
South Korea	✗	✗	5	107	NA	NA	DV	2016	[145, 146]
Moscow	✗	✓	3	30	13	0.1	DV	2017	[147]
Madrid	✗	✓	3	26.4	11	70	CV	2018	[129]
Cambridge	✗	✓	3	10.6	3.9	258	DV	2019	[130]
Madrid	✓	✓	11	55	12	NA	CV	2020	[148]
Bristol	✗	✗	8	16.9	29	83.9	DV	2020	[149]
Hefei	✓	✓	46	18	NA	60.5	DV	2021	[150]
Bristol	✓	✗	**4**	**6.8**	**9.14**	**2.6**	**DV**	**2022**	**[1, 24]**

TIMELINE 1: *A history of quantum networks throughout the world*

June 2004	DARPA Quantum Network | Cambridge, Massachusetts
March 2007	CNC Beijing | Beijing, China
October 2008	SECOQC | Vienna to St Polten, Austria
October 2008	Hefei Metro-Quantum Network | Hefei, China
February 2009	QuantumCity | Durban, South Africa
March 2009	SwissQuantum | Geneva, Switzerland to CERN, France
May 2009	Quantum Cryptography Network for Gov. Admin. | Wuhu, China
October 2009	Madrid Quantum Network | Madrid, Spain
March 2010	Tokyo QKD Network | Tokyo, Japan
December 2013	Battelle Commercial Network | Columbus to Dublin, Ohio
October 2013	Jinan Metro-Quantum Network | Jinan, China
February 2016	SK Telecom Metro Network | Seoul to Seong-nam,South Korea
February 2016	KREONET | Daejeon, South Korea
May 2016	Shanghai Quantum Network | Shanghai, China
June 2016	Moscow Quantum Network | Moscow, Russia
June 2016	SK Telecom Long-Term Network | Sejong to Daejeon, South Korea
Auguest 2016	Kazan Quantum Network | Kazan, Russia
November 2019	Cambridge Quantum Network | Cambridge, UK
November 2021	Hefei Quantum Network | Hefei, China
November 2022	Bristol Quantum Network | Bristol, UK

3.1.3 State-of-the-Art Long-Haul Quantum Key Distribution Networks

Long-haul QKD networks have been implemented across the globe, reaching a distance of 2,000 km for fibre-based networks and 7,600 km using satellite technology. Such distances were possible by utilising trusted nodes, and they tend to rely on the backbone/core network. The basic features of selected long-haul QKD networks are shown in Table 3.3 and a brief description of selected deployed QKD networks is shown below.

1. *Beijing-Shanghai Network*: It is a backbone network with a total length of 2,000 km. The network is based on trusted nodes, connecting four major Chinese QKD metropolitan networks in Beijing, Jinan, Hefei, and Shanghai. It took three years, from 2013 to 2016, to be completed.

2. *China-Austria Network*: This is the first intercontinental QKD network that connects Asia and Europe using the Micius satellite as the trusted node [151]. The Micius satellite connects the ground station in Graz, Austria and that in Xinglong, China with a total distance of 7,600 km.

3. *Cambridge-Ipswich Network*: This is the longest backbone QKD network in the UK which is composed of five nodes (3 trusted nodes) with a total length of 121 km. The network utilises commercial QKD equipment (ID Quantique Clavis^3 system [152], which will be discussed in detail in Chapter 5). This network also enables the coexistence of quantum and classical channels in the same deployed fibre.

4. *China's Integrated Space-to-Ground Network*: This network consists of a long-distance fibre backbone network, two satellite–ground links, and four quantum metropolitan area networks (QMANs) in Beijing, Jinan, Heifei and Shanghai, acting as the access points (Beijing-Shanghai Network). The network's backbone is the first national quantum backbone covering over 2000 km between Beijing and Shanghai using 32 trusted nodes. The backbone network implements a decoy state BB84 protocol with 135 QKD links over 43 km. Although the four QMANs explore different network topologies, they all implement a decoy state BB84 protocol in a trusted node infrastructure. The fibre-based network covered 2000 km, which consists of 716 QKD links serving 155 users. In addition, the high-speed satellite-to-ground QKD achieves a maximum SKR of 47.8 kbps while covering a distance of 2600 km. Therefore, integrating the free-space and fibre-based QKD link results in an overall network distance of 4600 km enabling all users to communicate via trusted nodes [135, 138, 153, 154].

Table 3.3: Long-haul QKD networks

Long-haul Network	Trusted Relay	Number of Nodes	Link Span	QKD Type	Year	Highlights	Reference
Beijing-Shanghai	✓	32	2,000	DV	2017	Longest fibre-based network	[155]
Wuhan-Hefei	✓	11	609	DV	2018	Real-world applications	[109]
China-Austria	✓	5	7,600	DV	2018	Intercontinental QKD network	[156]
Cambridge-Ipswich	✓	4	121	DV	2019	Coexistence enabled	[157]
China	✓	NA	4,600	DV	2021	Space to ground QKD	[153]
Jinan-Qingdao	✗	3	511	DV	2021	TF-QKD field deployment	[158]

3.1.4 General Architecture of Quantum Key Distribution Networks

A QKD network consists of more than a physical layer. As shown in the previous sections, QKD networks are currently being implemented in classical networks with preliminary applications in securing infrastructures. Similar to classical networks, several layered architectures have been proposed for QKD networks depending on their application, such as three layers [124–126, 133, 159–164], four layers [165–170], and five layers [153], with the three-layer architecture being the most implemented.

Given the diversity of the QKD networks architecture and that the three-layered architecture model is the most implemented, this section will focus on the three-layered architecture model. Figure 3.7 illustrates this architecture consisting of 1) the infrastructure layer; 2) the control and management layer; 3) the application layer.

1. *The infrastructure layer (physical layer)*: This layer includes the various physical QKD devices, which are secured in a secure location known as the QKD node. The QKD nodes are connected by a QKD link (quantum channels) to generate symmetric keys. The QKD parameters, such as SKR and QBER, are generated by the QKD devices and stored in the QKD node and sent to the QKD network manager for management purposes.

2. *The control and management layer*: This is the second layer (middle) in Figure 3.7; it consists of a QKD network controller which is connected to the physical layer by a control interface (e.g. OpenFlow) and a QKD network manager which is connected to the physical layer by a management interface (e.g. Simple Network Management Protocol (SNMP)). From its name, the QKD network controller controls the network by activating, de-activating, and calibrating the QKD nodes. The SDN controller can be realised as a QKD network controller. Whereas the QKD network manager monitors the critical parameters, such as the SKR, and link parameters, e.g. loss and length, to determine the status of the QKD nodes.

3. *The application layer*: This layer is constituted by the cryptographic applications run by the end-users. It is connected to the physical layer via an application interface and to the control and management layer via the same management interface.

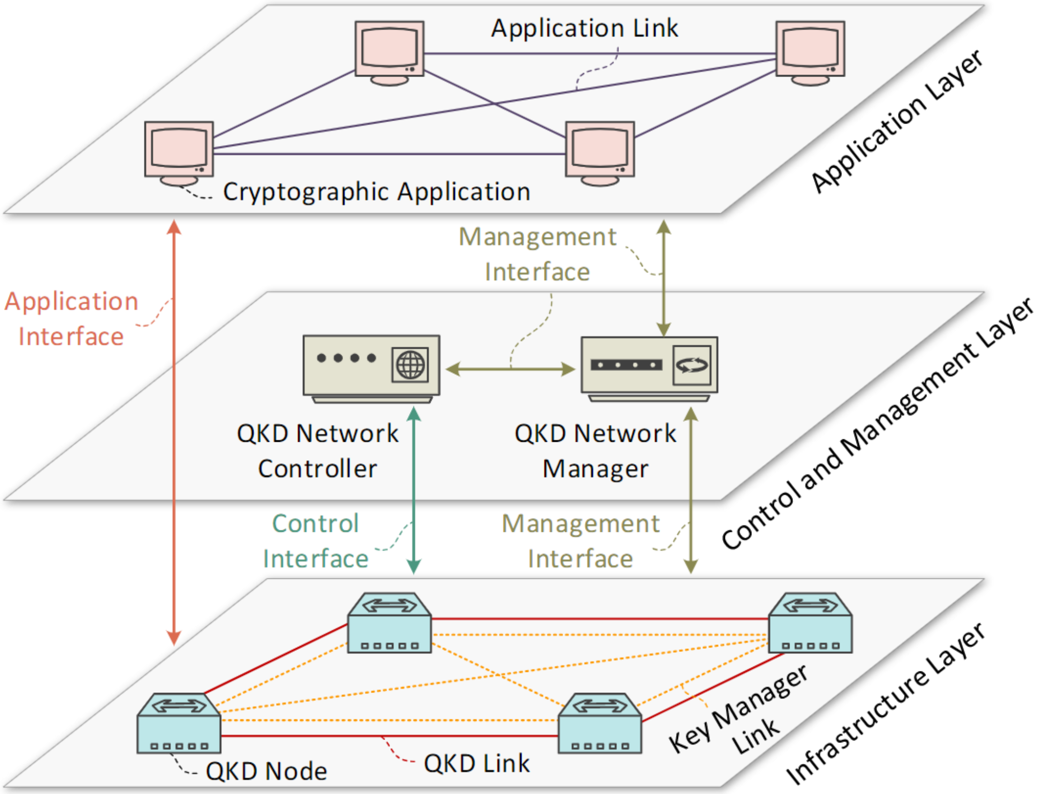


FIGURE 3.7. General architecture of QKD networks. Figure from [112].

3.2 The UK Quantum Network

The Bristol QKD network is part of the UK quantum network (UKQN), which is a mix of metro-scale QKD networks and long-distance fibre links, which are part of the UK National Dark Fibre Facility (NDFF). The network is used to provide a quantum national infrastructure testbed comparable to national classical communications infrastructure to test and validate new quantum communication devices and demonstrate proof of concept quantum communication experiments. The physical layer is a collaboration between the University of Bristol, University of Cambridge, University of York, Toshiba Research Europe Ltd (TREL) and BT Group. Figure 3.8 illustrates the physical topology of the UKQN [171], which consists of four distinct parts:

1. Cambridge metropolitan QKD network (discussed in Section 3.1.2)
2. Cambridge-Ipswich QKD network (discussed in Section 3.1.3)
3. Long-distance links between Cambridge and Bristol via London
4. **Bristol metropolitan QKD network**

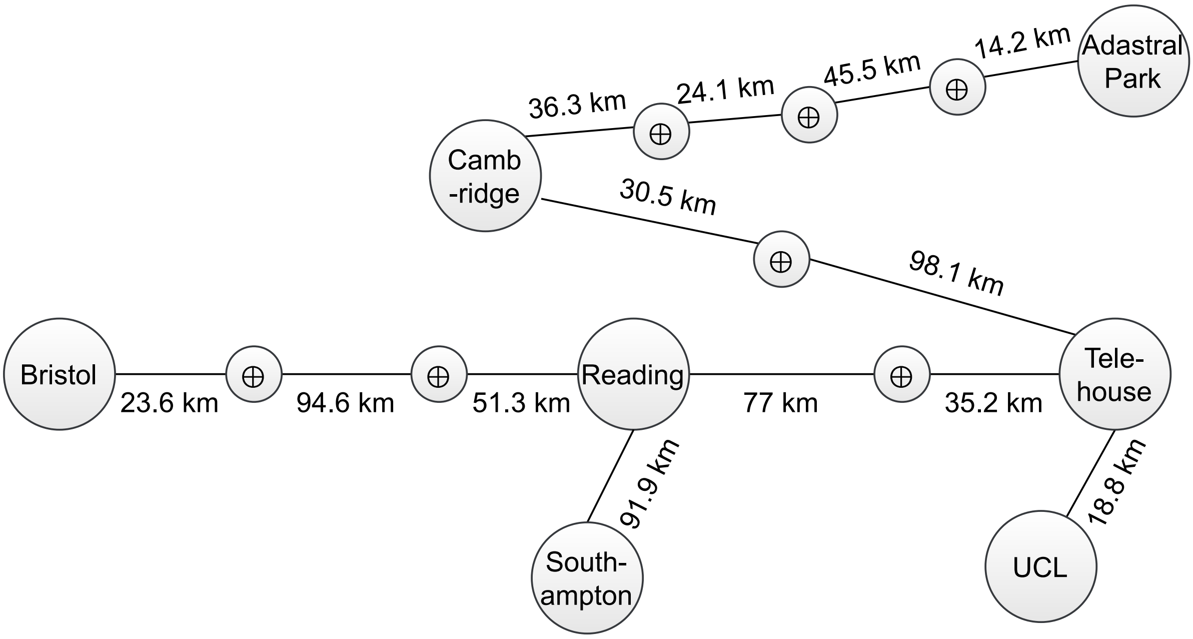


FIGURE 3.8. Physical topology of the UK quantum network.

3.3 Bristol Dynamic Quantum Optical Network

The Bristol quantum network comprises four optical network nodes across Bristol city, including the 5G access point in Millennium Square (WTC) and in One Cathedral Square (1CS) as well as the University of Bristol campus nodes of HPN Group and the centre for Nanoscience and Quantum Information (NSQI), as depicted in Figure 3.9.

As shown in Figure 3.10, each node has a QKD device, an Alice or a Bob, and an optical cross-connect (OXC) switch. The nodes are connected through the metro optical network in a meshed topology with dynamic optical switching capabilities (which is discussed in detail in this chapter). In case of a link failure or a DOS attacked, a link switch will occur which requires an additional one-hop to re-establish the link in such networks. Furthermore, the dynamicity of such network optimise the resource allocation for the QKD devices (this is discussed in details in Section 3.3.1). The network also support the coexistence of quantum and classical channels, by using a classical data channel (100 & 200 Gbps, SEP+, C-band interface) which is associated with each link and provides the system with the coexistence capability of classical and quantum channels over the same fibre. The coexistence is discussed in detail in the next chapter (Chapter 4). In this section, we first discuss the network architecture. We then introduce the ID Quantique Clavis^2 QKD system and the Polatis optical switch which are the two main components to build the dynamic Bristol quantum network, followed by a brief description of software-defined networks.

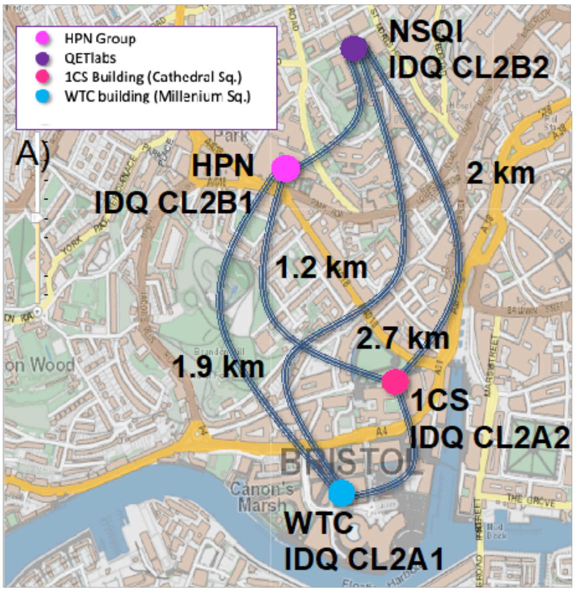


FIGURE 3.9. Map of the Bristol dynamic QKD network.

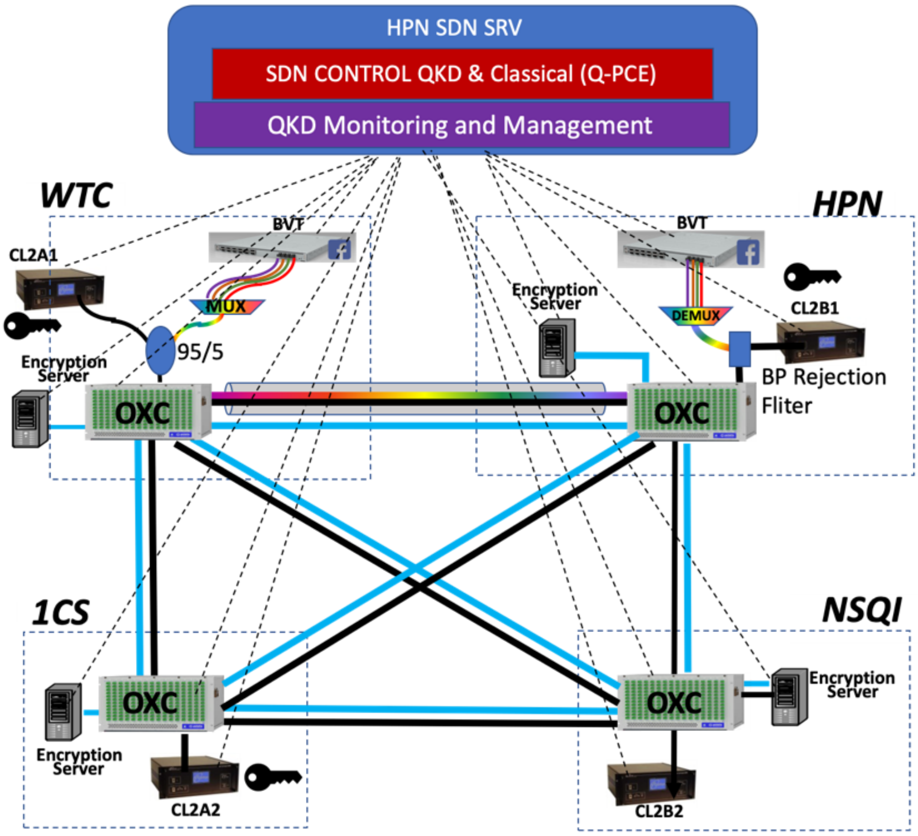


Figure 3.10: Block diagram of the Bristol dynamic QKD network.

3.3.1 Network Architecture

This section describes the overall network architecture concept used in the Bristol dynamic QKD network. Full-mesh connectivity of a network with N nodes requires a minimum of $N(N-1)/2$ links. Therefore, as shown in Figure 3.11 I) to implement a direct QKD connection between any two nodes and avoid the relayed function of trusted node configuration, six pairs of QKD devices are required to cover all possible six links L1-L6. Of course, using only four pairs of QKD devices as shown in Figure 3.11 II) the six links could be covered by realising relayed nodes (trusted nodes) at the expense of using two QKD pairs to establish some links without a direct connection (e.g. node N2 to node N3 employs QKD pairs $A_4 - B_4$ and $A_1 - B_1$ and node N1 to node N4 using $A_1 - B_1$ and $A_2 - B_2$). If a direct link is not required between each node, three pairs are enough to cover a four-node trusted-relay network. Starting with an Alice at N1, Alice and Bob at N2, Alice and a Bob at N4 and a Bob at N3. The connections between the nodes will be as follows: $A_1 - B_2$, $A_2 - B_4$, and $A_4 - B_3$. Figure 3.11 III) shows a 4 nodes implementation of our dynamic full-mesh QKD network where each node has an Alice (A), a Bob (B) and an optical switch (S). In this case, the Alice and Bob devices employed in the nodes are not dedicated to a specific Alice or Bob on any other node as the switch allows to physically connect the output of any Alice to the input of any Bob of the network. In this way, any node can establish a direct QKD link with any other node without using a trusted node due to the ability to switch the optical cross-connect port to the required destination port. The main advantage of the proposed switched QKD configuration is that the number of QKD pairs required scales linearly with the number of nodes (N QKD pairs for N nodes) for offering direct QKD links between any two nodes of the network, as opposed to $N(N-1)/2$ scaling without switches. In this experiment although the network has a full-mesh physical connectivity, only four QKD devices were used (two Alice devices and two Bob devices) and each node had either an Alice or a Bob depending on the configuration resulting in mesh QKD topology. Figure 3.11 IV) and Figure 3.11 V) show the two dynamic QKD configurations that were used in this experiment that when combined the cover all 6 links of the network. The testbed is discussed in details in Section 3.4.

3.3.2 The ID Quantique Clavis^2 Quantum Key Distribution System

The ID Quantique Clavis^2 is a QKD system developed to serve as a versatile research tool for quantum cryptography research [32], and it is a simplified version of the Cerberis QKD system [172] which is mainly used for enterprise, government, and telecommunication production environments. The Clavis^2 QKD system is considered as a “plug & play” QKD system, which uses a patented auto-compensating optical schematic capable of automatically compensating for polarisation mode dispersion providing outstanding stability and high interface contrast. Furthermore, it consists of two stations (Alice & Bob), and it implements a phase-encoded SARG04 protocol [173] where the key information is encoded in the phase of two consecutive photon pulses generated in a Mach-Zehnder interferometer. The SARG04 protocol implements

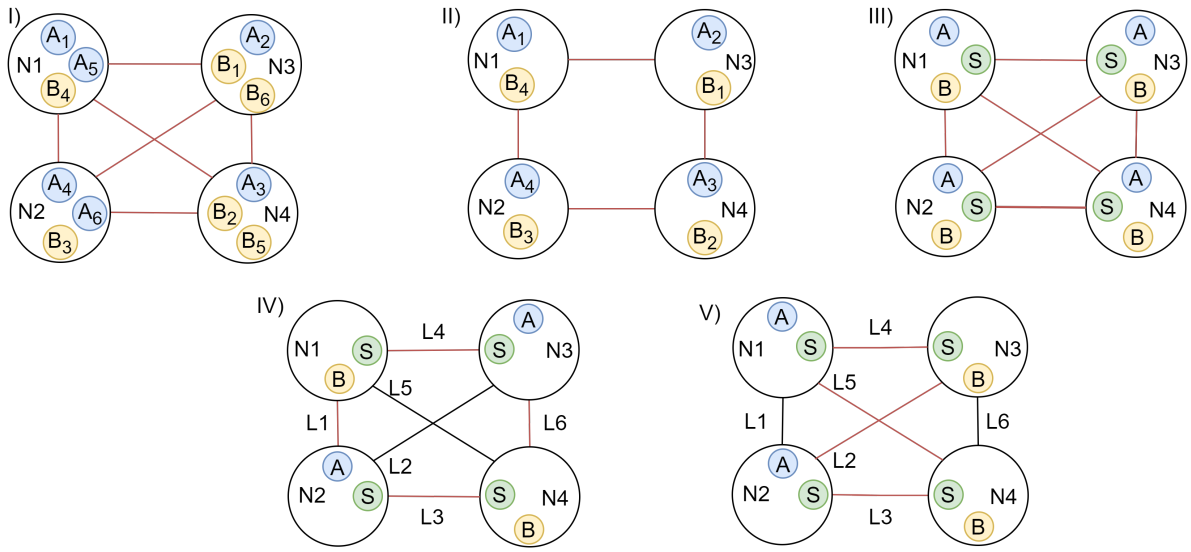


FIGURE 3.11. QKD network topologies. I) 6 QKD pairs trusted-node-free static configuration, II) 4 QKD pairs trusted-node static configuration, III) 4 QKD pairs trusted-node-free dynamic full-mesh configuration, IV) Trusted-node-free dynamic mesh configuration one, V) Trusted-node-free dynamic mesh configuration two. A: Alice, B: Bob, S: Optical Switch, Red line: Fibre with QKD communication, Black lines: Fibre without QKD communication.

an identical approach to the BB84 protocol. Furthermore, when the end-to-end optical loss is ≤ 3, the ID Quantique Clavis^2 falls back on the BB84 protocol since the SARG04 is not proven to be secure in this region.

Optical schematic for the ID Quantique Clavis^2 and General Theory of Operation Figure 3.12 shows a simplified version of the optical system schematics for both Alice and Bob. A laser pulse in the C-band (1551.7 nm) is emitted by Bob's laser and travels through the second port of the circulated into an unbalanced interferometer. Each pulse is split into two halves at the 50/50 beam splitter (BS), where the first half goes through the short arm (early) and the second half through the long arm (late). The polarisation of the pulse travelling through the long arm (late) is rotated by ($\frac{\pi}{2}$), resulting in both pulses existing from the same port at the polarising beam splitter (PBS). The pulses then travel to Alice, where they get reflected by a Faraday mirror resulting in two orthogonal polarised pulses, which are encoded and attenuated to the single photon level. To implement the phase-encoded BB84 protocol, Alice encodes the qubits only when the pulses are reflected. Alice applies a phase shift of 0, π or $\frac{\pi}{2}$, $\frac{3\pi}{2}$ only on the second pulse (late). Due to the combined effects of the PBS and the Faraday mirror, the reflected pulses go through the opposite arm of the interferometer, i.e. the early pulse that went through the short arm from Bob to Alice goes through the long arm when reflected and vice-versa. Bob then applies a phase shift of 0 or $\frac{\pi}{2}$ one the reflected pulse that goes through the long arm as the measurement basis. Since both pulses took different paths when reflected, they arrive at the BS at the same time where they interfere. If Alice encodes the photon using $\theta{=}0$ or $\theta{=}\pi$ and Bob measures in the 0, π basis (matching basis), detector 1 or detector 2 will click, respectively. Similarly, if Alice transmits $\theta{=}\frac{\pi}{2}$ or $\theta{=}\frac{3\pi}{2}$ and Bob measures in the $\frac{\pi}{2}$, $\frac{3\pi}{2}$ basis (matching basis), detector 1 or detector 2 will click, respectively. However, if the encoding of Alice differs from the measurement bases of Bob, i.e. Alice encodes using $\theta{=}0$ or $\theta{=}\pi$ and Bob measures in the $\frac{\pi}{2}$, $\frac{3\pi}{2}$ basis, there is an equal chance that detector 1 or detector 2 will click and the measurement outcome is discarded in the post-processing stages.

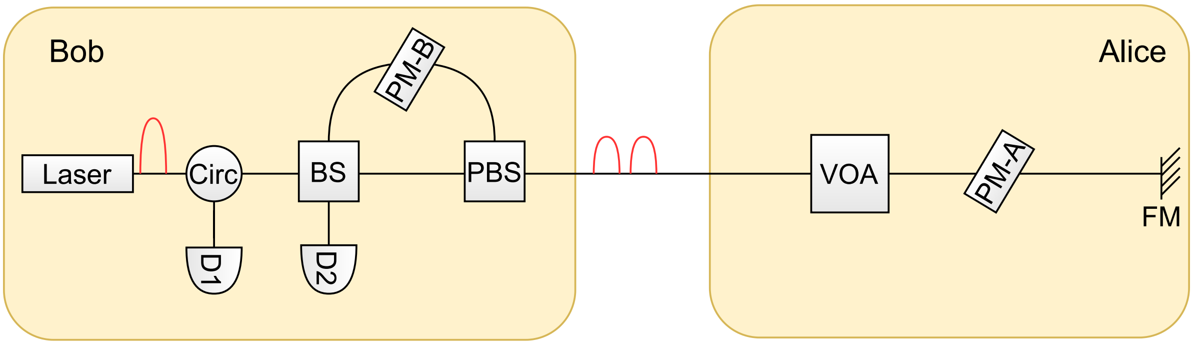


FIGURE 3.12. Optical schematic for the ID Quantique Clavis[2]. Circ: circulator, D1, D2: detectors 1 and 2, BS: Beam splitter, PBS: Polarisation beam splitter, VOA: Variable optical attenuator, FM: Faraday mirror, PM-A, PM-B: Phase modulators for Alice and Bob, respectively. Based on [32].

Optical system of QKDS-Alice station

As mentioned before in the simplified version, the optical system of the Alice station is mainly used to encode the qubits. In this section, a detailed description of the Alice station is presented. As illustrated in Figure 3.13, the intense incoming light pulses are split by a 10/90 beam splitter (BS). The bright light (corresponding to 90% output port) is directed into three classical detectors where one detector is used to serve as a time reference for the phase modulator (Synchro), and two are used to secure the system (Alarm and CW). It is also essential to notice that the light is further attenuated using a variable optical attenuator VOA2 to prevent the saturation of the classical detectors.

1. *Classical Det Synchro*: It is an APD which detects the incoming optical pulses and generates an electrical signal fed into the electronics system. The electronics delay the signals with respect to the delay line in the quantum emitter part of the Alice station and use it as a time reference to enable the phase modulation of the second reflected pulse (late). The

APD is followed by a threshold discriminator that activates at a very low threshold to indicate the timing of the late pulse.

2. *Classical Det Alarm*: It is a PIN photodiode which monitors the pulsed optical signals entering the Alice station, followed by a threshold discriminator. When the power of the pulsed optical signals entering the Alice station is above a certain threshold defined for the detector, an alarm is triggered to protect the system.

3. *Classical Det CW*: It is also a PIN photodiode followed by an analogue to digital converter used to detect the existence of a CW light in the Alice station. It is also used to measure the loss of the quantum channel between Alice and Bob. In combination with the Classical Det Alarm, both detectors are responsible for monitoring the incoming energy into the Alice station to prevent Eve from injecting light into the system (Trojan horse attack) to measure the phase applied by Alice.

The weaker light (corresponding to the 10% output port) is fed into the quantum emitter arm (dashed box in Figure 3.13). The quantum emitter consists of a variable optical attenuator (VOA1), a 200 GHz ITU standard optical bandpass fibre filter, a 12.5 km optical SMF spool (delay Line), a phase modulator and a Faraday mirror operating at 1550 nm. VOA1 attenuates the highly intense reflected light into a single photon level. The VOA1 is followed by a 200 GHz bandpass filter to filter the incoming light and contain out-of-band noise, followed by a 12.5 km SMF delay Line. After that, the pulses pass through a phase modulator to encode a bit value by modulating the second pulse of each pair of the reflected pulses, and finally, a Faraday mirror to reflect the pulses and returns them orthogonally polarized to compensate for the polarisation mode dispersion in the quantum channel fibre on a round-trip (Bob to Alice and Alice back to Bob).

Optical system of QKDS-Bob station

As mentioned before in the simplified version, the optical system of the Bob station is mainly used for three purposes, to generate the intense pulses, to apply the measurement bases on the reflected pulse that travels through the long arm, and to detect the reflected photons using two SPADs. This section highlights that all the fibres in the interferometer are polarisation maintaining (PM) fibres used to reduce polarisation effects in the Bob station, as shown in Figure 3.14.

Raw Key Distribution: General Principle of Operation

SUMMARY: Hardware protocol adhered to by the ID Quantique Clavis^2 QKD system

1. Preparation of Strong Laser pulse train:

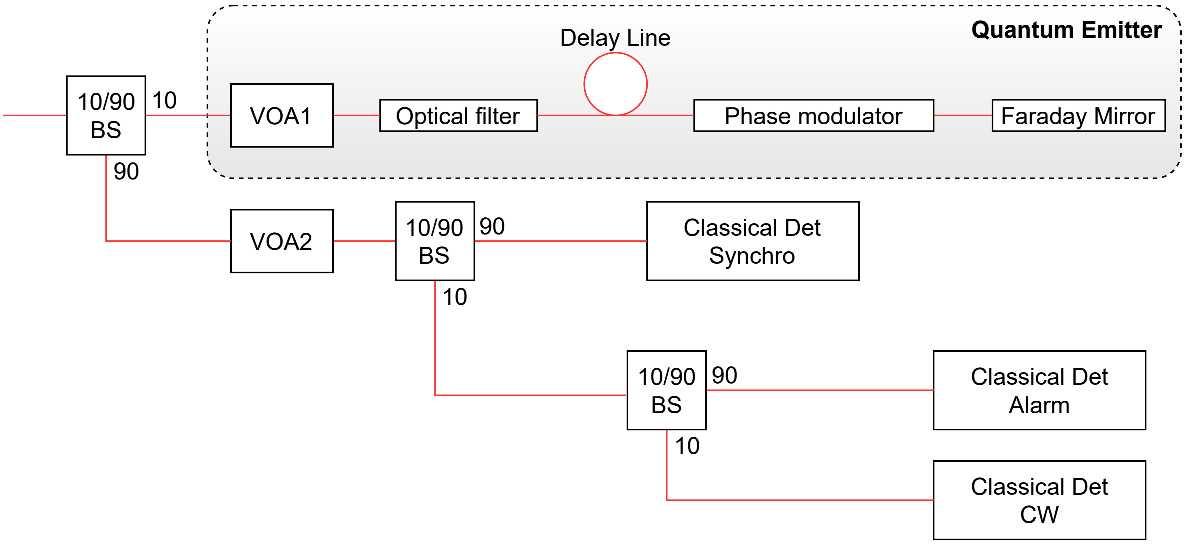


FIGURE 3.13. Optical schematic of QKDS-Alice station.

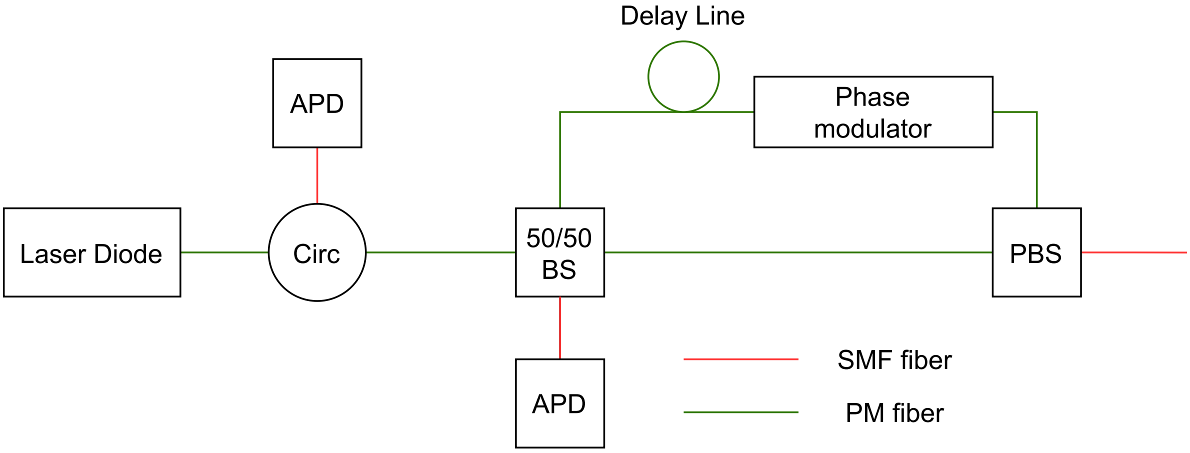


FIGURE 3.14. Optical schematic of QKDS-Bob station.

a) Bob generates a 5 MHz train of laser pulses (period of 200 ns) and produces a laser start signal.

b) Each pulse is split into two halves using the 50:50 BS.

c) The polarisation of the half-pulse (late) through the long arm in rotated by ($\frac{\pi}{2}$).

d) Both early and late pulses exist the PBS through the same port due to the polarisation rotation of the late pulse in the long arm and head towards Alice.

2. Preparation State of Alice Sync:

Alice's clock is synchronized with the incoming laser pulses using the Syncro classical detector which produce a clock sync signal.

3. State Preparation on Weak Coherent Pulses:

   a) The train of pulses is attenuated using VOA1.

   b) The polarisation of both pulses is rotated by ($\frac{\pi}{2}$) by a Faraday mirror.

   c) Alice PM: The second reflected (late) pulse of each pair is randomly modulated using one of the four states (0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$) .

   d) The train of pulses is further attenuated using a VOA1 into a set of weak coherent pulses before leaving the Alice station.

4. State Measurement:
   The first reflected coherent pulse (early) travels through the long arm of the interferometer at Bob's station where a random phase is applied (0, $\frac{\pi}{2}$) for each pulse.

5. State Bob detection:

   a) Detector 1 and Detector 2 gates activate the single photon detectors when the weak encoded coherent pulses are reflect. The detector's gates are activated with respect to the variables delay (2× time of flight from Bob to Alice's FM).

   b) After the end of the frame period, the next frame is sent.

3.3.3 The Huber+Suhner Polatis Optical Switch

The Polatis optical switch [111] is an SDN-enabled all-optical circuit switch with a density of up to 384 × 384 ports that supports all optical communication wavelength bands (Table 3.4) transmission. Additionally, it enables bi-directional transmission with optical power signal monitoring and variable optical attenuation at each port.

Table 3.4: Optical communications wavelength bands

Band	Wavelength Range (nm)
O (Original)	1260-1360
E (Extended)	1360-1460
S (Short)	1460-1530
C (Conventional)	1530-1565
L (Long)	1565-1625
U (Ultra-long)	1625-1675

It is based on a direct beam steering technology (Directlight [174]) which is achieved by having optical collimators on each side supported by compact piezoelectric actuators to point the light across a 3D-space region - any input to any output - with minimal loss. The alignment is held in position and maintained using feedback from the position sensors at each input/output. The internal structure of a 16 × 16 Polatis optical switch is shown in Figure 3.15.

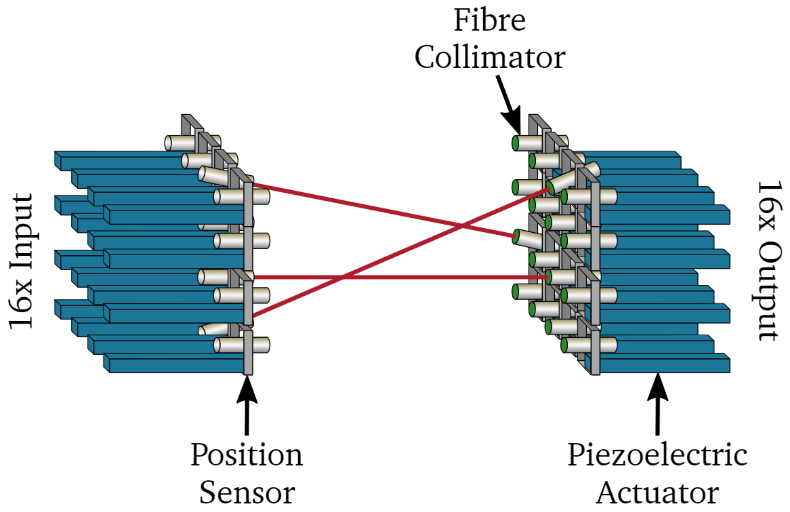


FIGURE 3.15. The internal structure of a Polatis optical switch. Each input port connects to a fibre collimator, and a piezoelectric actuator aligns this with the collimator corresponding to the desired output. Figure from [175].

Direct beam steering technology provides ultra-low loss (< 1 dB) and lower noise crosstalk compared to traditional 3D microelectromechanical system (MEMS) switches [176]. Furthermore, the Polatis optical switches is more robust, compact and cheaper compared to 3D MEMS switches. However, they are less scalable and slower than 3D MEMS switches [177]. A comparison between direct beam steering and 3D MEMS switches is shown in Table 3.5.

Table 3.5: Comparison between 3D MEMS switches and direct beam steering switches

	3D MEMS Switches	Direct Beam Steering
Price	Expensive	Cheap
Crosstalk	Higher (<-40 dB)	Lower (<-55 dB)
Scalability	Higher (1296 × 1296 [178])	Lower (384 × 384 ports [111])
Physical size	Bigger	Smaller
Insertion Loss	Higher (2-4 dB)	Lower (1 dB)
Switching speed	Faster (<10m sec)	Slower (>10m sec)

3.3.4 Software-Defined Networks

Similar to classical communication, enabling techniques, such as SDN and resource allocation, are being implemented to solve QKD networking issues. As shown in Figure 3.16, an SDN node usually consists of a QKD transceiver, a key manager and an SDN agent. The SDN controller is a centralised entity that sends the control information to an SDN agent to enable flexible and programmable configuration of the entire network. Therefore, since the SDN controller contains all the vital information of the QKD network, it can solve complex networking scenarios whilst maintaining a global perspective on the network. Hence, an SDN-enabled QKD network is a flexible and programmable QKD network run by an SDN controller, which configures the network control and management layer to optimise the QKD network performance.

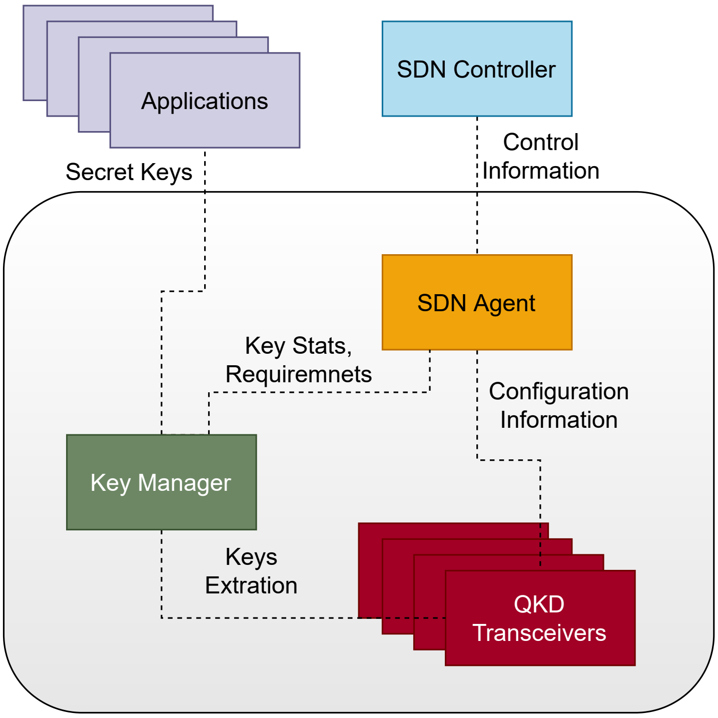


FIGURE 3.16. Abstraction model of an SDN-enabled QKD node.

As shown in Figure 3.17, devices and nodes are usually centred around an optical switch, making them easier to configure, simpler to deploy, and more efficient, providing the ability to achieve full topological reconfigurability.

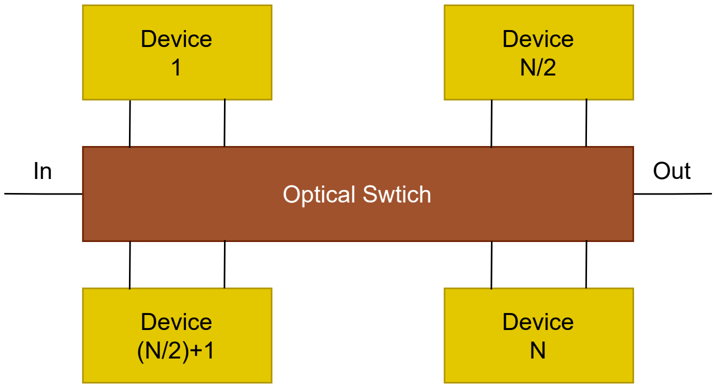


FIGURE 3.17. The internal structure of a single node in a software-defined network.

3.4 Experimental System Testbed

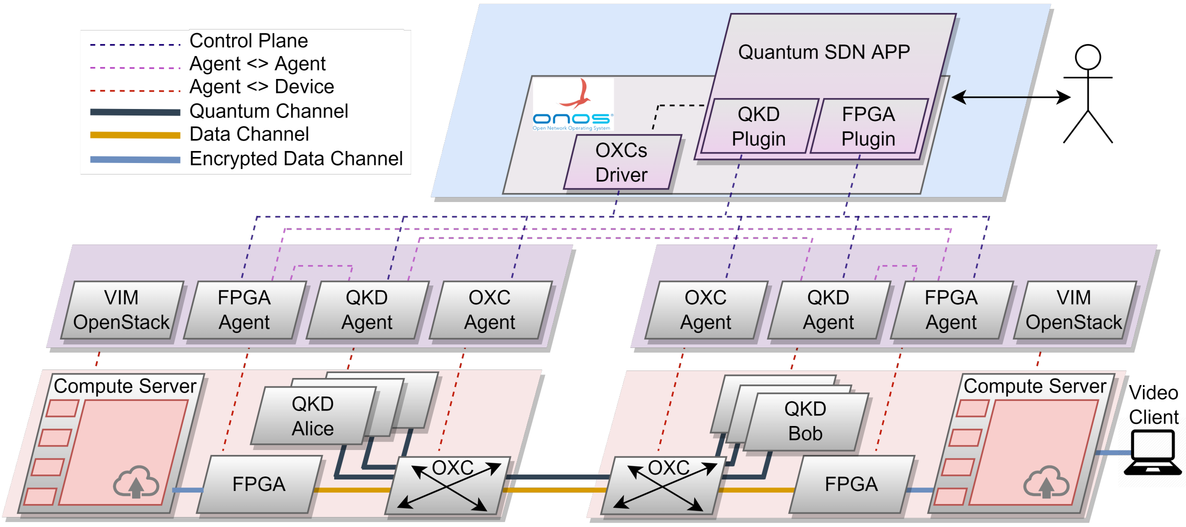


Figure 3.18: Experiment Testbed. Red link: Fibre with QKD communication, Black link: Fibre without QKD communication.

The original testbed for this experiment was designed to enable two functionality; 1) a dynamic QKD operation, 2) the coexistence of quantum and classical channels in a QKD network. However, since this chapter mainly focuses on dynamic QKD, we have decided to use a simplified testbed setup Figure 3.18. A detailed testbed is included in Chapter 4 which focuses on the coexistence of quantum and classical channels.

As shown in Figure 3.18, the network is divided into three layers; the data layer, agent layer, and control layer. In a top-down approach, the control layer contains the SDN controller and the required connectivity to the data plane equipment via the agent layer whereas the data plane represents the optical fibre infrastructure, optical equipment and QKD-related devices. The SDN controller is responsible for the computation, creation, and management of the complete path that traverses optical and SDN switches between the nodes. The SDN controller is individually controlling the switches, QKD terminals, and encryption/application server in each node to create secure channels through the agent layer. The SDN controller utilises a quantum aware path computation mechanism, that calculates the best path for QKD and classical channel including power and losses, for minimal effect on the quantum channel. The SDN controller is also responsible for the establishment and management of paths that traverses between the nodes, including both classical and quantum channels and requires an L2 network to communicate with the data plane devices as demonstrated in [21].

To be able to perform the aforementioned tasks, the controller requires some essential components, such as databases to store network data (e.g. routing and connection tables), driver modules needed to control multiple different vendor devices, communication modules that understand different protocols (e.g. gRPC and Netconf), and finally intelligent algorithms that could use both heuristics or machine learning to optimise the usage of the network resources. The computational units host the software needed to communicate and control the equipment, including the Key Management System (KMS). The KMS is an entity that manages keys in a network in cooperation with one or more other KMS. When new cryptographic keys are generated by a QKD device, the keys are securely stored in a database (also called as key store) managed by the KMS. Such key stores provide a "key buffer" within the network, effectively decoupling the key generation process from the key consumption applications, allowing greater tolerance to bursts of key usage as also to temporary unavailability of the key-generation devices. Additionally, the KMS is responsible for monitoring and recording the usage and generation of keys, thus providing valuable statistics that can be used by the SDN controller. In the next section we describe the implementation of this architecture, as we describe the experimental setup.

Each device has a companion agent that facilitates the communication with the SDN Controller. For instance, the QKD Agent (CQP Toolkit [179]) interfaces with QKD devices, stores the generated keys and can be controlled via gRPC; the OXC Agent applies the received flows from the SDN controller; and the FPGA Agent pushes keys and loads encryption algorithms. Moreover, there is a public communication channel between some of the agents to its peers, mainly for key synchronisation purposes.

Next, on the data plane, each node is composed of several components, including but not restricted to, optical switches, QKD equipment, data encryptors, and computational servers.

3.4.1 Data Plane

This testbed is used to demonstrate the dynamic QKD-networking using multiple QKD pairs. Each node is equipped with optical switch (Polatis), a QKD device (Clavis^2), an encryption unit, data servers and a secure server. The testbed was designed to provide flexibility enabled by the

SDN Controller. In these nodes, the encryption server will interface to the ID Quantique Clavis[2] unit for the QKD protocol and an optical output of 100 Gbps data rate [16, 21] will transport the encrypted data towards the optical link via the Polatis switch. The FPGA encryptors/decryptors are SDN-enabled programmable encryptors/decryptors that provide on-demand encryption algorithms from an encryption library consisting of AES-256, AES-192, AES-128, Camellia-256, XOR, and no-encryption configurations [16, 21, 22].

3.4.2 Control Plane

Each node has several components that need to be monitored and controlled by the SDN controller. To provide connectivity between the SDN controller and all the controllable devices in our deployed network we devised a supporting management network. One particular component is the Secure Server, that connects to L2 switches and other Secure Servers (using 10 Gbps small form-factor pluggables (SPFs)), thus accounting for the control plane logical and electrical connections described in Figure 3.18.

The Secure Servers also host the Key Manager System (KMS) that doubles down as a key database and as an agent to manage and control the QKD devices. The KMS software of choice was the CQP Toolkit, developed in-house [179]. Additionally, the Secure Servers also hosts the OXC agent and the encryption unit agent.

The SDN controller is responsible for the establishment and management of the complete path that traverses the optical SDN switches between the nodes. It can handle paths for the quantum channel, classical channels, and coexisting QKD and Classical channels. Additionally to the switches, the QKD terminals and the encryption units are also controlled.

In the current controller state, the routes are calculated offline using the network information and then uploaded to the controller. This network information includes the OXC ports, link connections and losses, and available routes. Therefore, the path assignment consists of selecting the most suited route available for the incoming request (e.g. fibres with smaller losses for a quantum channel). Quantum channels can be established between any two matching devices (i.e. one Alice and one Bob) as per the user's request.

The controller monitors the SKR and QBER in real-time and fetches these parameters from the QKD agent (CQP Toolkit) using gRPC whenever the parameters are updated (every two minutes). Furthermore, when a new QKD connection is established the configurations table is automatically updated based on the available links. Although the switches configuration occurs instantly, establishing a new QKD link requires 10-15mins to authenticate the QKD devices and generate keys.

Figure 3.19 summarises the flow when a new request arrives to the SDN controller. The start connection request identifies a source site and a destination site and retrieves all the information pertaining to that particular pair from the routing table. This information includes the cross connections (e.g. OXC's input and output ports) needed to fulfil the path between sites. The SDN controller utilises the information to install the flow rules in the OXC. After the OXC devices are configured, the controller issues the start QKD message towards to the KMS agents, triggering the start of the key generation process. Thereafter, the monitoring of the Quantum Bit Error Rate (QBER) starts, raising an event within the controller in case there is a deviation the QBER values. If the QBER is below a QBER threshold (6% by default), it is deemed as acceptable and the encryption unit is set to initiate the encryption software, creating an encrypted tunnel between the endpoints. However, if at any moment the QBER monitored is above the threshold, the current quantum channel quality is noted as unsatisfactory and therefore the controller proceeds to fetch the next available route in the routing table connection and the aforementioned process starts again.

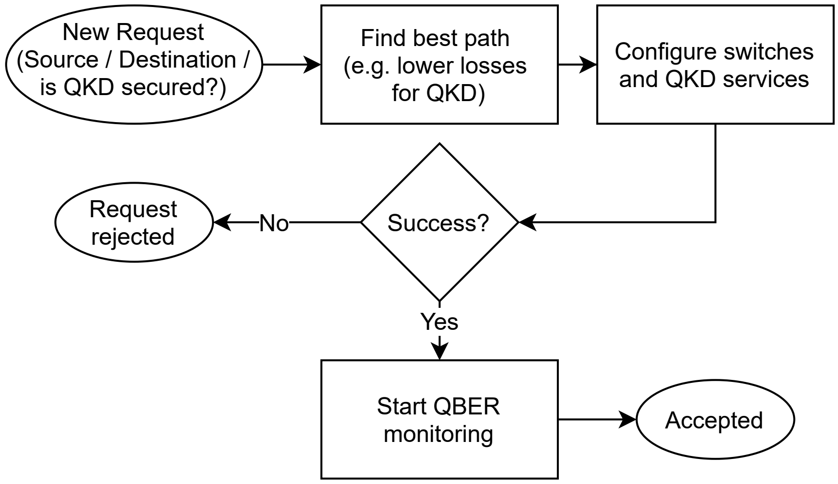

New Request (Source / Destination / is QKD secured?)
Find best path (e.g. lower losses for QKD)
Configure switches and QKD services
Success?
No
Request rejected
Yes
Start QBER monitoring
Accepted

Figure 3.19: New request flowchart. In addition to classical resource allocation, the SDN controller also considers QKD-impacting characteristics, such as link losses, and optimise the allocation to provide a better QKD experience when a QKD-secured connection is requested.

Once the whole system is running, the quantum keys are generated by the ID Quantique Clavis^2 and stored on databases managed by the KMS system. In addition to the KMS, CQPToolkit software suite also encompasses an interface to control the ID Quantique Clavis^2 devices and an encryption application. This controlling interface allows the SDN controller to start/stop ID Quantique Clavis^2 devices and subsequently to request statistics to monitor the quantum channel parameters. All communication between CQPToolkit and the SDN controller is done using gRPC as communication protocol. As encryption application, CQPToolkit suite ships with the QTunnelServer software which implements one solution to the problem of sending encrypted data from one site to another. It creates an encrypted tunnel thus allowing secured data transfer by using AES-256 encryption.

3.5 Results

Table 3.6 shows the main parameters of both configurations of the dynamic QKD network of Figure 3.11 IV and V. The parameters of the optical fibre links are described, such as fibre lengths and end-to-end power losses. Also, Table 3.6 depicts the number of cross-connections per link required for dynamically switching to the quantum channel requested. The quantum parameters of QBER and SKR are represented in this table. In addition, the combination of links for multihop scenarios is included to show the performance of the dynamic QKD network without coexistence. As observed, the link L1 with the lowest power budget (5.19 dB) excluding back-to-back configuration achieves the lowest QBER of 1.31% and the highest SKR of 1762.06 bps. However, since L6 has the highest power budget of 9.61 dB and two cross connections, results show the highest QBER of 3.65% and the lowest SKR of 360.08 bps, being near the power budget limit of the QKD system used. L5 and L6 are field deployed fibres that were purposely chosen to reach the power budget limit of the QKD system. In Table 3.6 A_2-B_1 means the direct connection from Alice in Node 2 to Bob in node 1 whereas L1 + L2 is the connection from Bob in node 1 to Alice in node 3 via the switch in node 2 as shown in Figure 3.11 IV.

Table 3.6: Dynamic QKD network parameters

Link	Fibre Length (km)	End-to-End Power Budget(dB)	# OXC	QBER (%)	SKR (bps)
Back-to-Back	0	4.99	1	1.02	2575.69
L1 (A_2-B_1)	0.5	5.19	2	1.31	1762.06
L2 (A_2-B_3)	1	5.70	2	1.43	1414.15
L3 (A_2-B_4)	5.8	6.90	2	1.70	1078.03
L4 (A_3-B_1)	4.7	7.00	2	1.91	895.54
L5 (A_1-B_4)	1.625	9.22	2	3.03	418.74
L6 (A_3-B_4)	1.625	9.61	2	3.65	360.08
L1 + L2	1.5	7.44	3	2.01	819.22
L1 + L3	6.3	8.60	3	2.70	533.97
L1 + L4	5.2	8.79	3	2.73	542.26
L2 + L3	6.8	9.14	3	3.03	430.56
L2 + L4	5.7	9.42	3	3.05	417.94

The network comprises four nodes interconnected via single-mode fibre (SMF) links resulting in a full-Mesh classical network due to physical fibre connecting all four nodes simultaneously. Figure 3.20 shows the physical connections for all the links in Table 3.6, which are constructed from Figure 3.11 IV and V. Each node has an Alice (A), a Bob (B) and an optical switch (S), and all the scenarios were tested to see the impact of the optical switch on the quantum channel performance. Figure 3.20 also highlights the advantage of using an optical switch, where each node can communicate with other nodes using multiple configuration. For instance, if A_1 needs to communication with B_4, a direct link (L5) could be established. However, in a scenario where

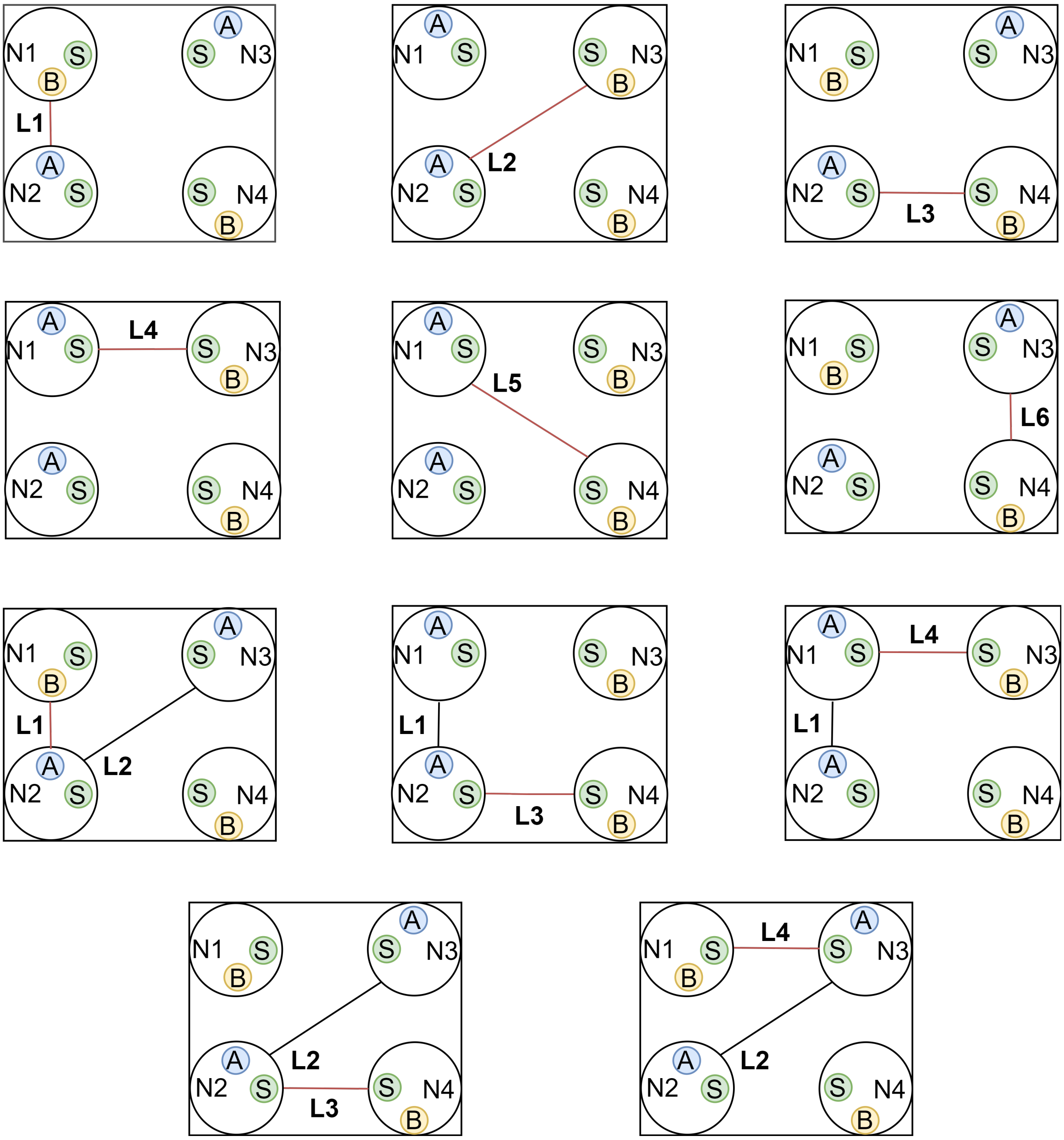


FIGURE 3.20. QKD network topologies. A: Alice, B: Bob, S: Optical Switch, Red line: Fibre with QKD communication, Black lines: Fibre without QKD communication.

L5 is down, A_1 can communicate with B_4 via the optical switch at Node 2 using L1 + L3 while avoiding trusted nodes. The ability to link two nodes using multiple configuration is useful in case of link failure or Denial of Service (DoS) attack [180]. Using the optical switch provides an additional path in such mesh topologies, making it easier and faster to re-establish the broken link. Furthermore, due to direct link connections and relativity small distance (≈ 10 km) between nodes in dense urban metropolitan networks, dynamic QKD optimises the expensive QKD equipment by adding an optical switch to each nodes, overcoming the point-to-point restriction of the QKD connections. It also increases the resilience of the QKD network in case of physical attacks on the fibres and provides faster and easier restoration of the QKD link, hence enchaining the link recovery and physical security of the network.

3.6 Summary

We have demonstrated a trusted-node-free dynamic QKD networking implementation over a testbed that spanned across four optical nodes interconnected in mesh topology with short links between nodes emulating the case of a dense metropolitan region. The network allows the dynamic deployment of any QKD link between two nodes of the network, while a QKD-aware centralised SDN controller is utilised to provide dynamicity in switching and rerouting. To test all possible links, we used two QKD systems in two different configurations. The link with the lowest optical loss (5.19 dB) achieved SKR of 1762 bps and a QBER of 1.31%. Whereas, the link with highest optical loss (9.42 dB) achieved SKR of 417 bps and a QBER of 9.42%.

Chapter 4

Coexistence of Quantum and Classical Channels in Optical Networks

Declaration of Work

This chapter is based on [1, 2]. In [1], I developed the final testbed physical layer design in collaboration with Emilio Hugues-Salas.
In [2], I developed the testbed, carried out the experiments that investigate the impact of classical channel position.
I built and characterised the testbed, measured the Clavis^2 QBER and SKR, measured the Voyager BER, and processed the data for both experiments. [1, 2]
All of this work was done under the supervision of George Kanellos and Reza Nejabati.
Since I am the lead author of [1, 2], parts of the articles have been reused in the chapter where appropriate.

One of the main goals of quantum communication is to provide worldwide connectivity via complex networks – similar to the current internet – with ultimate security based on the laws of physics rather than computational complexity. Quantum networks are moving towards interconnecting seamlessly multiple nodes and enabling applications beyond QKD, such as blind and distributed quantum computing.

Coexisting quantum and classical channels in a single medium would be beneficial for the integration of quantum technologies with the current optical infrastructure and aids applications such as QKD and blind and distributed quantum computing to reach their maximum capabilities.

To this end, we have demonstrated a four-node trusted-node-free metro network configuration with the coexistence of quantum and classical channels over deployed fibre links. We tested different scenarios, including varying the number, power and position of the classical channels and investigated their effects on the quantum channel performance in terms of SKR and QBER.

We start this chapter by reviewing the different physical impairments sources in a DWDM-QKD system, such as channel crosstalk noise, Raman scattering, and four-wave mixing (FWM). Followed by an investigation of the impact of the classical channel's spacing and position on the quantum channel. After that, we introduce the equipment needed in a DWDM-QKD system, followed by a detailed description of the equipment detrimental to QKD and necessary for the coexistence. Next, we provide a brief overview of the state-of-the-art coexistence system in the lab and field and introduce the Bristol QKD network. We then discuss the experimental system testbed for the Bristol QKD network, followed by a detailed discussion on coexistence results and scenarios. Finally, we present multiple use cases of coexistence in real-life demonstrations and conclude the chapter by providing an evaluative summary of the main findings.

4.1 Physical Impairments Sources in a DWDM-QKD System

Even though it is becoming easier to build quantum networks using classical infrastructures as shown in the previous chapter Chapter 3, classical networks are not free from physical impairments at the quantum channel power levels (a single photon level = -159 dBm). This is because, if the crosstalk noise in a classical system is 40 dB or more below the classical channel power, the classical infrastructure can operate properly [181]. Therefore, classical communication systems do not compensate for physical impairments at a power level lower than 40 dB from the classical channel power. However, since the optical power of a classical channel is orders of magnitude higher than the power of a quantum channel and the difference between the power of a classical communication channel and a quantum channel is usually $>$ 100 dB, such physical impairments are a complication that needs to be addressed when coexisting quantum and classical channel in the same fibre. These physical impairments are generated from the optical nonlinear effects from classical channels [182]. Due to the physical impairments and insufficient isolation between the quantum and classical channels, unwanted noise photons are generated in the optical bandpass of the QKD receiver; hence increasing the error rate. The increase in the error rate degrades the quantum channel performance, and therefore, limits the range and key generation rates of QKD system. In this section, we discuss three physical impairments sources: 1) Channel crosstalk noise, 2) Raman scattering and 3) Four-wave mixing.

4.1.1 Channel Crosstalk Noise

As stated above, insufficient isolation between the classical and quantum channels could cause a noise leakage into the quantum channel; this noise is called channel crosstalk noise [183]. To suppress the channel crosstalk noise, enough isolation (typically $>$ 110 dB [184]) is required to reduce the channel crosstalk noise level below the dark count contribution. This isolation is achieved by using multiple stages of filtering and could be achieved using off-the-shelf DWDM components. It can also be achieved by using different telecommunication bands for the quantum and classical channels. In this case, the nonlinear effect impact on the quantum channel becomes weaker, and therefore, it is easier to provide the required isolation. In all of our experiments, we used multiple stages of filtering, including an ultra-sharp filter (with edge slopes of up to 800 dB/nm and 60 dB of isolation), which are discussed further in Section 4.3.

4.1.2 Raman Scattering

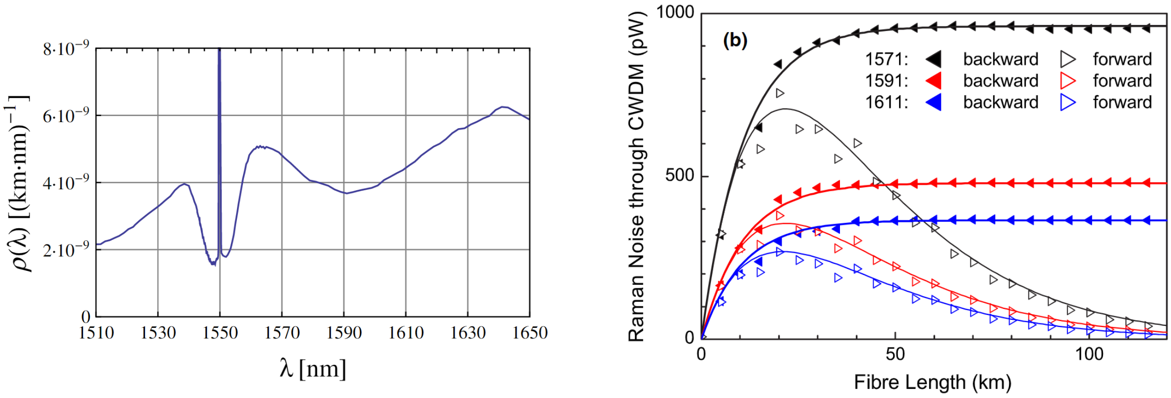
Raman scattering arises from an inelastic interaction of a pump light with vibrational modes (optical phonons) in a fibre. The scattered noise photons get excited or de-excited and generated at a wavelength higher than the pump wavelength (Stokes) and lower than the pump wavelength (anti-Stokes) [184, 185]. Raman scattered photons can cover the entire C-band [186], with the maximum intensity at around 13 THz, which is equivalent to 100 nm at 1550 nm as shown in Figure 4.1 (a). Moreover, the minimum intensity is usually at around 200 GHz, which is equivalent to 1.6 nm at 1550 nm. Whether the classical light is co-propagating or counter-propagating with respect to the quantum signal, a broad spectrum is generated with an overall optical spectrum of over 200 nm [187].

Since in all our experiments, the quantum and classical channels are co-propagating in the fibre, we only consider the forward Raman scattering noise. The power of the forward Raman scattering noise generated by the classical channels λ_i at the quantum channel wavelength λ_j within a bandwidth of $\Delta\lambda$ is given by [184, 185, 188]:

$$I_R = I_c L e^{-\alpha L} \rho(\lambda_i, \lambda_j) \Delta\lambda, \tag{4.1}$$

Where $\rho(\lambda_i, \lambda_j)$ and $\Delta\lambda$ represent Raman cross section and the bandwidth of the quantum receiver, respectively. L, α, and I_c denote fibre length, fibre attenuation coefficient, and the coexistence power, respectively.

Furthermore, forward and backward Raman scattering exhibits completely different behaviour at a higher fibre length in both the C and L-band [189]. As shown in Figure 4.1 (b), the power of forward Raman scattering peaks at a distance of around 22 km, whereas, that of backward Raman scattering does not decrease with distance. Therefore, a higher fibre distance would lead to a reduction of Raman noise in the case of forward scatter, while in the case of backward scatter, a higher fibre attenuation would not affect the Raman noise, but rather it reaches saturation asymptotically.



(a) (b)

Figure 4.1: (a) Measured Raman cross-section of a pump laser wavelength centred at 1550 nm in an SSMF. Figure from [185]. (b) Measured (symbols) and calculated (solid lines) forward (▷) and backward (◀) Raman noise power into the quantum receiver. Figure from [189].

4.1.3 Four-wave Mixing

FWM is a nonlinear effect that arises when two or more pump fields interact with the $\chi^{(3)}$ nonlinearity of optical fibre [190]. Three optical signals with frequencies f_i, f_j, and f_k (i,j ≠ k) are transmitted in an optical fibre. Due to the third-order nonlinearity, a new frequency f_{ijk} is generated.

$$f_{ijk} = f_i + f_j - f_k \tag{4.2}$$

The peak power of this new signal I_{FWM} is obtained by [185, 191]:

$$I_{\text{FWM}} = \frac{\eta D^2 \gamma^2 {I_c}^3 e^{-\alpha L}}{9\alpha^2}(1-e^{-\alpha})^2, \tag{2}$$

where D is the degeneracy factor, which is equal to 3 for $f_i \neq f_j \neq f_k$. The parameters γ denotes fibre nonlinearity, and η is obtained by:

$$\eta = \frac{\alpha^2}{\alpha^2 + \Delta\beta^2}\left(1 + \frac{4e^{-\alpha L}\sin^2(\Delta\beta L/2)}{\left(1-e^{-\alpha L}\right)^2}\right), \tag{3}$$

where $\Delta\beta$ is the phase matching factor.

The FWM noise product might fall into the optical band of the quantum channel filter as an in-band noise, and, therefore, cannot be filtered (Figure 4.2 illustrates the additional frequencies generated through FWM). To prevent this from happening, we can increase the channel spacing which would eliminate the FWM noise completely [192]. We can also use unequally spaced channels in order to minimize the noise effects on the quantum channel [193, 194].

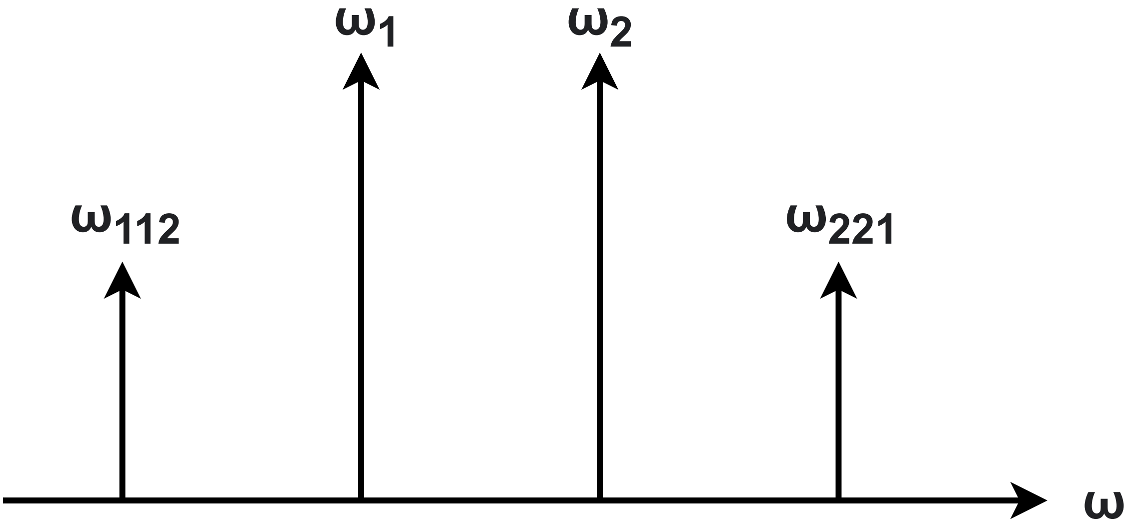


Figure 4.2: Additional frequencies generated through FWM.

4.2 The Impact of Channel Spacing and Position

For the classical channels, we consider a classical band of 8 channels and 50 GHz spacing between each channel, coexisting with a fixed quantum channel (193.70 THz 1547.72 nm) in SMF. These parameters are chosen based on the capabilities of our testbed. In [195–197], optimal wavelength assignment in DWDM-QKD systems has been investigated. Our calculation is based on the fact that the classical channels are located in the C-band and the quantum channel is at ITU channel 37 (193.70 THz 1547.72 nm). Furthermore, it is assumed that the quantum channel is in the anti-stokes region of the Raman spectrum of the classical channels. We denote the coexistence power by I_c. Considering both Raman scattering and FWM, we numerically calculate the best and worst locations of a classical band with respect to its impact on the performance of the quantum channel in terms of SKR and QBER.

Figure 4.3 shows the best and worst cases for the spacing between the classical band and the quantum channel for different values of I_c. For low values of I_c, Raman scattering is the dominant source of noise. Therefore, the optimum location of the classical band is at the dip of the Raman spectrum which is near the quantum channel (1.6 nm spacing), whereas the worst case is at the peak of the Raman spectrum (8 nm spacing). As I_c increases, both Raman noise and FWM crosstalk increase as well. For adjacent channels (1.6 nm), FWM crosstalk increases much faster and becomes more dominant at higher coexistence power ≈ -5 dBm. However, for non-adjacent channels (8 nm), Raman scattering is the only source of crosstalk that impacts the quantum channel performance due to the large spacing (8 nm) between the quantum and classical channels. As shown in Figure 4.3 inset, the FWM impact is minimal for non-adjacent

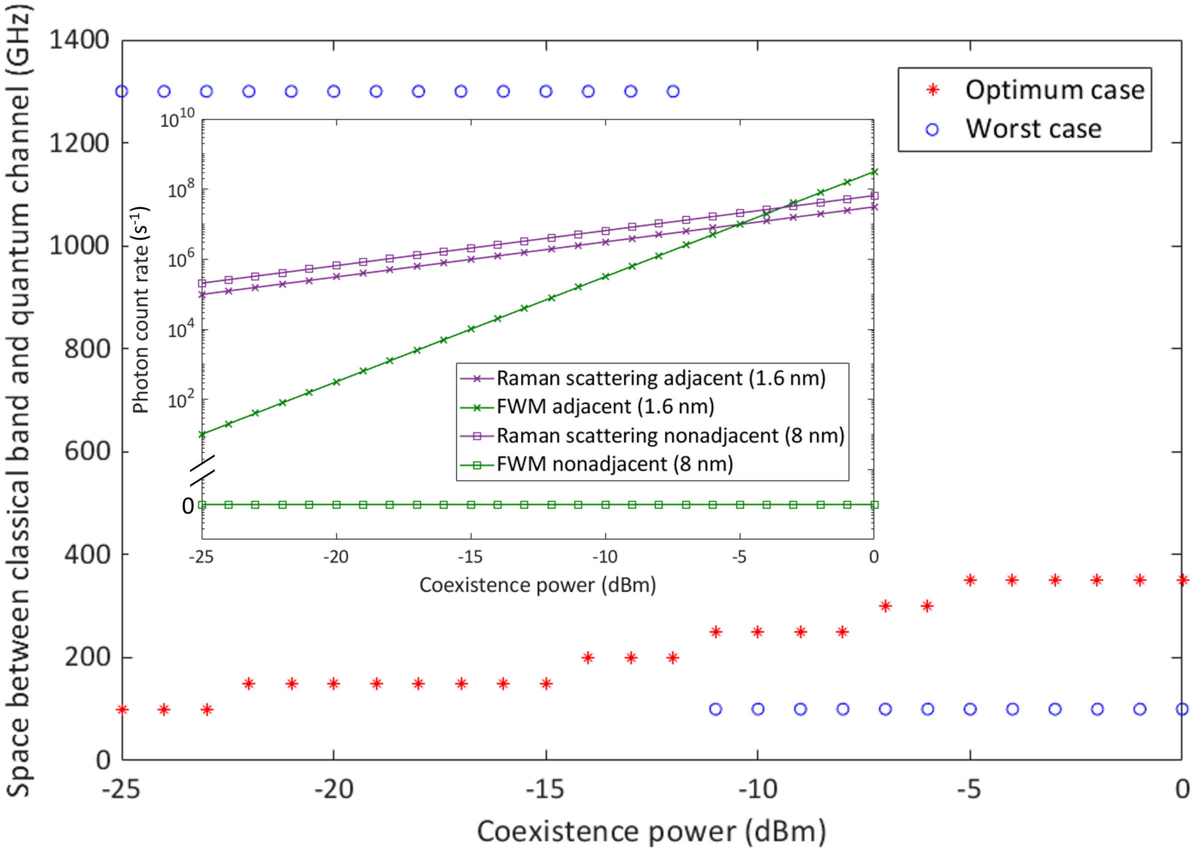


Figure 4.3: Best and worst case scenarios for the classical band spacing, considering different values for the coexistence power in the SMF. The photon count rate at the quantum channel wavelength due to Raman scattering and FWM noise of adjacent (*) and nonadjacent (□) classical channel bands are also shown in the figure. Done using Matlab.

channel, and with a spacing of 8 nm, the FWM noise is practically eliminated. Figure 4.3 inset also shows the photon count rate generated at the quantum channel wavelength (193.70 THz 1547.72 nm) due to the Raman noise and FWM noise at two different spacing between the quantum and classical channels: 1.6 nm (*) and 8 nm (□). The following parameters were considered to calculate the photon count rate: Quantum detector efficiency= 20%, fibre length= 2 km, bandwidth of quantum channel band-pass filter= 100 GHz, and γ= 14×10^{-4} based on [198].

4.3 Equipment in a DWDM-QKD System

A DWDM-QKD system is a system where the quantum channel is multiplexed with classical channels through DWDM devices. As shown in Figure 4.4 any DWDM-QKD system usually contains four main parts:

1. QKD system (transmitter & receiver)
2. Classical optical communication system (transmitter & receiver)
3. WDM optical devices (multiplexer & de-multiplexer)
4. Transmission medium (SMF, MCF, HCF, free space)

In this thesis, we used two QKD system, Clavis^2 and Clavis^3 from ID Quantique. We introduced the Clavis^2 QKD system in Section 3.3.2, whilst the Clavis^3 QKD system is introduced in Chapter 5. For the classical optical communication, we used optical packet DWDM platforms that are used with bandwidth-variable transponders (BVTs) which is introduced in the next section.

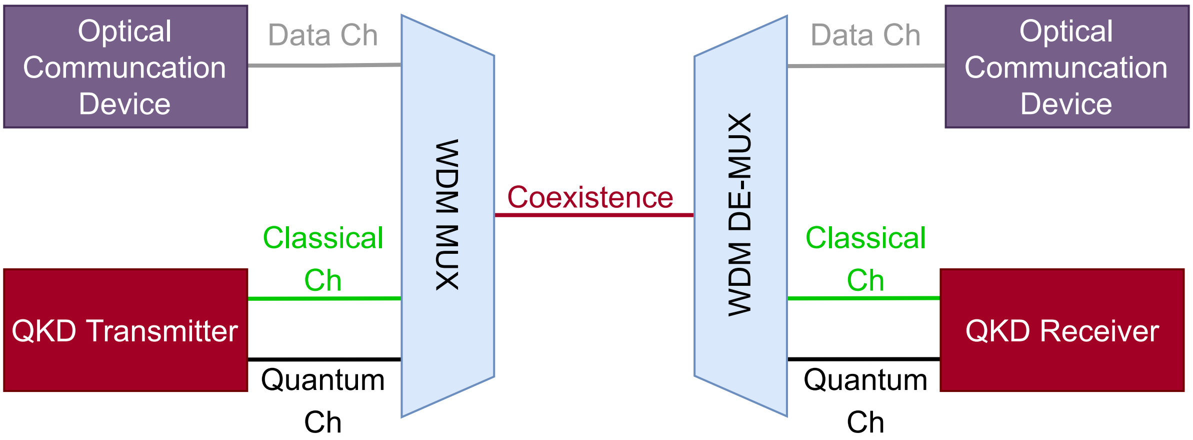


Figure 4.4: Illustration of general coexistence scheme.

4.3.1 Equipment that is Detrimental to Quantum Key Distribution

In the previous chapter, we highlighted the ease of integrating the Polatis optical switch into a quantum network. Unfortunately, not all devices can be integrated without affecting the QKD system performance. Here, we consider two optical devices that have negative effects in a quantum network.

4.3.1.1 SFP+ and QSFP+ Transceivers (Facebook Voyager)

In all of our experiments, the classical optical channels were established using enhanced small form-factor pluggable (SFP+) and enhanced quad small form-factor pluggable (QSFP+) fibre transceivers. We used two Facebook Voyager Optical systems, which are an open packet DWDM system used with bandwidth-variable transponders (BVTs) [199]. Each of these units includes four BVT ports reconfigurable to coherent 100 Gbps (PM-QPSK), 150 Gbps (8-QAM) or 200

Gbps (16-QAM) and each port can be tuned to any of the 100 wavelengths in the C-band included in the ITU-T grid with 50GHz offset. Adaptable soft-decision forward error correction (SD-FEC) is also available in the transponders to enable maximum transmission capacity with minimum errors. The Voyager is able to transmit a classical signal configured for 200 Gbps per wavelength capacity using 16-QAM modulation over a 180 km maximum transmission distance for a point-to-point link.

4.3.1.2 Erbium-Doped Fibre Amplifiers

Erbium-doped fibre amplifiers (EDFAs) are devices that amplify classical optical signals, which work on the principles of stimulating the emission of photons. At the core of an EDFA is a conventional silica fibre doped with Erbium. When the Erbium is excited with light at a suitable wavelength, it decays to a ground state after being in an intermediate state, hence amplifying classical signals by emitting light in the C-band. No-cloning theorem (discussed in Chapter 2) shows that EDFAs are incompatible with QKD. Furthermore, as shown in Figure 4.5 the amplified Spontaneous Emission (ASE) noise generated by EDFAs requires filters with over 60 dB of isolation to push the signal down to the level of weak coherent pulses. Innovative techniques which are used in the Cambridge-Ipswich network [157] include separating the quantum and classical signals before amplifying the classical signal to minimise the crosstalk from the amplified spontaneous emission (ASE) noise before combining the signals again. Other techniques are operating the quantum and classical channels at different bands (examples are shown in Section 4.4) or sending the classical and quantum signals in different fibres (no coexistence).

4.3.2 Equipment that is Necessary for Coexistence

To enable the coexistence of quantum and classical channels, components are required to filter, multiplex, and separate the quantum and classical channels.

4.3.2.1 Filters

As discussed in Section 4.1, an isolation of >110 dB is required to reduce the channel crosstalk noise level below the dark count contribution and filter out-of-band noise. Therefore, filtering the quantum and classical channels is crucial in a DWDM-QKD system. The choice of filters is limited for quantum channels due to the limited loss budget compared to the classical channels, where amplification is possible. Furthermore, the quantum channel is usually fixed to a single wavelength, in contrast with the classical channels, which are tunable to different wavelengths based on the application.

1. Quantum channel filters: We usually use a low loss (≈ 0.8 dB) passive DWDM band-pass filter centred at the quantum channel wavelength (1551.7 nm for the Clavis[2] and

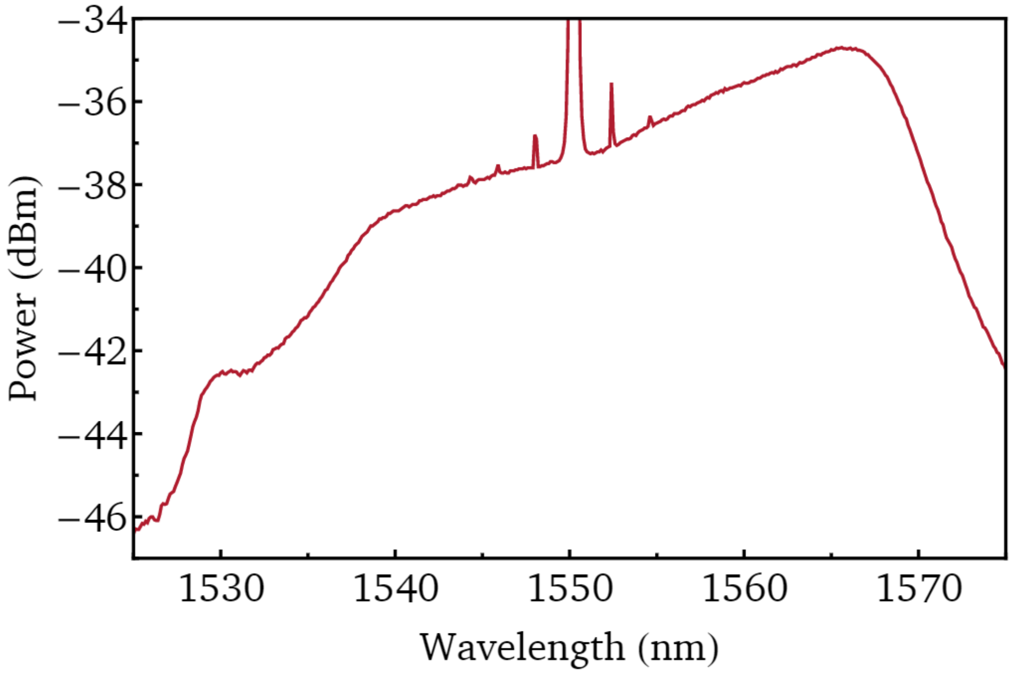


Figure 4.5: Noise profile for an erbium-doped fibre amplifier, acting ona 1550 nm signal. Figure from [175].

1547.72 nm for the Clavis[3]) with an optical bandwidth of 0.8 nm (100 GHz). Such filters provide ≥ 25 dB and ≥ 35 dB of isolation for adjacent and non-adjacent channels, respectively. Figure 4.6 illustrates a simplified version of the operating mechanism of a passive DWDM filter. When transmitting two different channels at 1551.72 nm and 1553.33 nm through the common port of a DWDM filter centred at 1551.72 nm, the 1551.72 nm channel goes through the pass port, whereas, the 1553.33 nm channels gets reflected and goes through the reflect port. Therefore, these filters are not only used to filter the quantum channel, but also to separate the quantum and classical channels at the quantum receiver node.

2. Classical channel filters: Since the classical channels can be amplified, tuned and added based on the application, a tunable bandpass filter with adjustable bandwidth and high isolation is usually used. These filters can be used to filter quantum channels, however due to their high loss (> 5 dB), passive DWDM bandpass filters are preferred. In our experiments, we used two types of filters for the classical channels, as shown below.

   a) Yenista Tunable Filter [200]: is a tunable bandpass filter (TBPF) with a flat-top and sharp filter edges (up to 800 dB/nm) with a high isolation (out-of-band suppression) of 60 dB. The full width at half maximum (FWHM) bandwidth ranges from 32 pm (4 GHz) up to 5 nm (625 GHz). The Yenista filter has an insertion loss of 6 dB,

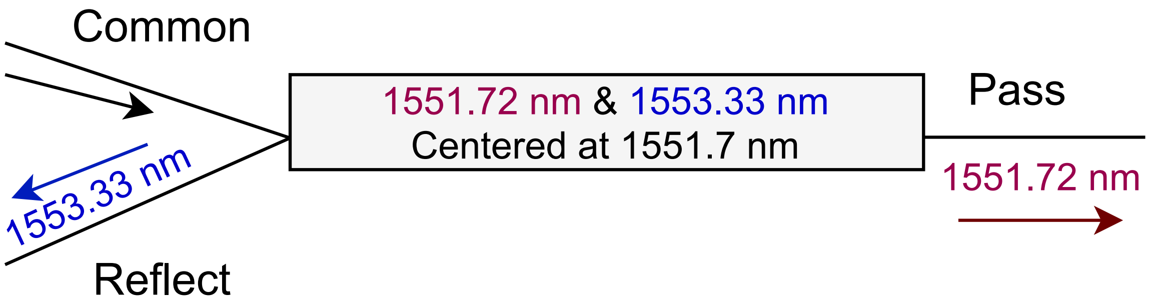


Figure 4.6: Illustration of a DWDM filter operation.

and an excellent wavelength coverage with over a 200 nm range, covering the S, C and L telecommunication bands. The shape of the filter profile is shown in pink in Figure 5.11.

b) WaveShaper [201]: is a reconfigurable optical processor that is based on Liquid Crystal on Silicon (LCoS) technology [202]. As shown in Figure 4.7, the input signal is reflected by a cylindrical mirror to a conventional grating, where it gets dispersed. The dispersed optical signal is then reflected by the same mirror to the LCoS optical processor. The LCoS optical processor consists of a matrix of reflective liquid crystal elements, which are controlled by varying the voltage of each element. By controlling the voltage, individual phase shifts are added to the reflected signals, therefore, allowing beam steering of signals hitting the LCoS processor. Each wavelength is switched and filtered independently without interfering with other wavelengths due to the wavelength separation on the LCoS chip. Such structure allows the WaveShaper to be used as a wavelength-selective switch (WSS), a bandpass filter, and a (de-)multiplexer. It is configured by software commands and has 20 bi-directional optical ports which can be used in any combination. Each port can be used as a bandpass filter covering the entire C-band with a tunable bandwidth ranging from 10 GHz (0.08 nm) to 5.36 THz (42.7 nm). The WaveShaper has an insertion loss of 5 dB.

In our experiments, the WaveShaper is usually used as a multiplexer to combine multiple classical channels and a filter to filter each classical channel individually before combining them into the output port. It is followed by the Yenista filter which filters the out-of-band noise for the combined classical channels. Further details are shown in Section 4.5 and Chapter 5. We also the WaveShaper to multiplex the quantum channels in Chapter 6's experiments.

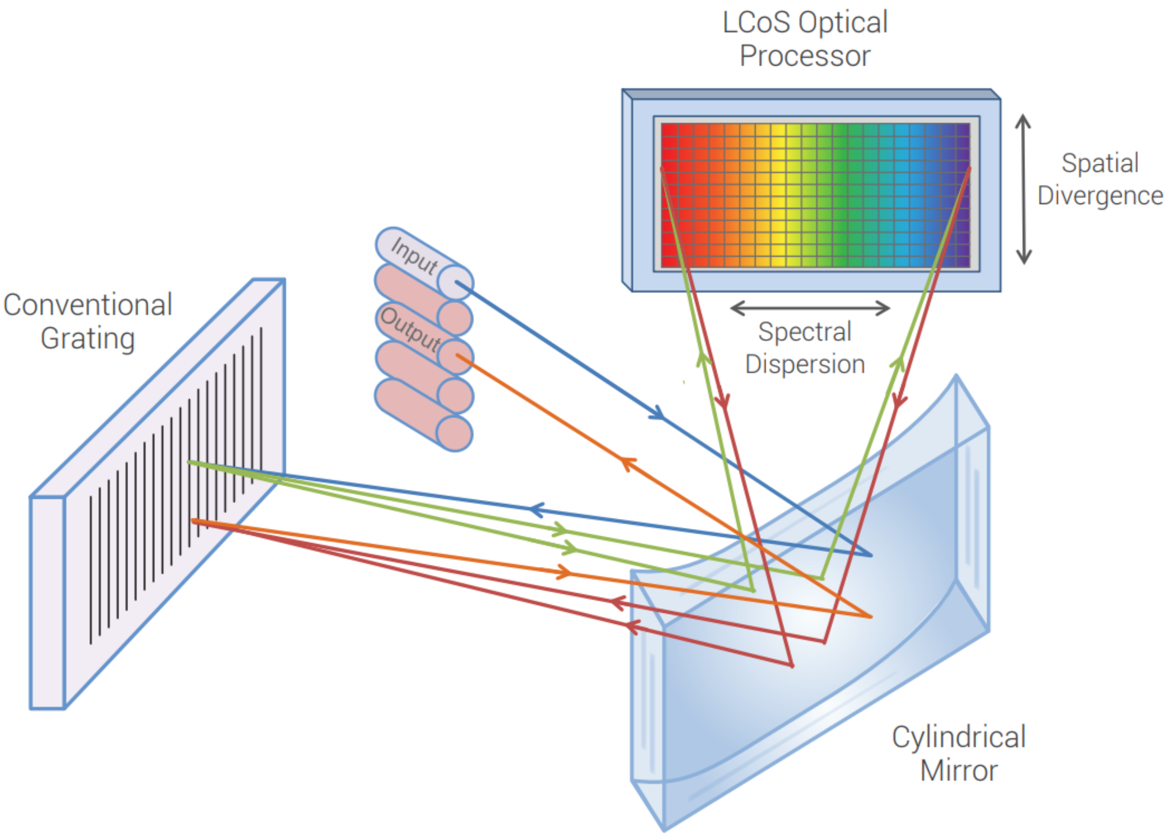


Figure 4.7: The internal structure of a WaveShaper programmable optical processor [175].

4.3.2.2 (De-)Multiplexers

Coexistence is not possible without components to multiplex (combine) the quantum and classical channels into a single medium and to de-multiplex (separate) the quantum and classical channels into their distinct receivers. Furthermore, when coexisting with more than one classical channel - which is always the case in our experiment - a multiplexer is required to combine the classical channels into a single output port to be multiplexed with the quantum channel. A de-multiplexer is also required to separate the classical channels into multiple ports for detection. If the device is wavelength-agnostic such as couplers/splitters, it can be used as a multiplexers/de-multiplexers. The following components have been used in our experiments to combine and separate quantum and classical channels:

1. Couplers/Splitters: a 95/5 coupler has been utilised in our experiment to combine the quantum and classical channels as shown in Section 4.5. The 95% port was used for the quantum channel due to the low loss ≈ 0.7 dB, whereas, the 5% port was used for the classical channel. As mentioned before, the advantage of using a coupler to coexist the quantum and classical channels is its wavelength-agnostic propriety which makes

it possible to combine any wavelength for both the quantum and classical channels. Furthermore, a 1x8 coupler/splitter was used in Section 5.1.1 to combine/separate eight classical channels to facilitate the coexistence/detection of the channels.

2. DWDM filters: As shown in Figure 4.6, a DWDM filter can be used as a de-multiplexers since it filters the quantum channel wavelength while reflecting all other wavelengths (classical channel wavelengths), therefore, it separates the quantum from the classical channels. However, it can also be used as a multiplexer (coexistence stage) by transmitting the quantum channel through the pass port and the classical channel through the reflect port, resulting in both the quantum and classical channels to be transmitted via the common port. The main advantage of using a DWDM filters is the low loss from both the pass and the reflect port ≈ 0.5 dB for both, compared to the 13 dB of loss for the 5% port of the 95/5 coupler. However, since it is wavelength specific, we can only coexist the quantum channel that is centred at the wavelength of the pass port.

3. WSS: As mentioned before, the WaveShaper can be used as a WSS, a (de-)multiplexer, and a filter due to its reconfigurability, with a fixed 5 dB of loss per port. Since in most of our experiments, we used eight classical channels (limited due to the output ports of the voyager BVT) and the loss of a 1x8 coupler is 12 dB per port, a WSS is the superior choice to use in terms of loss. Furthermore, the coupler provides no additional filtering, whereas, the WSS provides over 30 dB of isolation which is crucial to reach the 110 dB required to eliminate the crosstalk noise. Therefore in most of our experiments, we used the WSS to multiplex and combine the classical channel into a single output. We also used the WSS as a multiplexer for our quantum channels in our dynamic entanglement network in Chapter 6, since each user required more than one quantum channel to have a full-mesh connected quantum entanglement network.

4.4 State-of-the-Art Quantum and Classical Channels Coexistence

As stated before, integrating quantum technologies with the current classical infrastructure requires both technologies to coexist in one medium. In this chapter, we highlight the state-of-art coexistence experiments both in the lab and in the field. Table 4.1 summarises the main features of the lab-based coexistence experiments. The first coexistence experiment which provided a blueprint and was used as a reference for future experiments, was reported more than 25 years ago in 1997 [187]. It was then followed by a variety of theoretical analysis and system experiments both in lab and field using WDM techniques for the coexistence of quantum and classical channels [183–187, 189, 203–222]. As shown in Table 4.1, the coexistence of quantum and classical channels where they are both in the same optical wavelength bands (C-band) or in different optical wavelength bands (O-band for the quantum and C-band for the classical) has been extensively studied and demonstrated. Coexisting the quantum and classical channels in the C-band has many advantages, such as lower fibre loss in the C-band compared to the O-band and better compatibility with the current fibre infrastructure. However, the nonlinear effects such as Raman scattering and channel crosstalk noise become more dominant; hence a lower total coexistence power is achievable. In contrast, when coexisting the quantum and classical channels in different bands - by choosing the O-band for the quantum channel and the C-band for the classical channels - sufficient isolation can be ensured to eliminate physical impairments sources from the system.

Table 4.1: Summary of system experiments for the coexistence of quantum and classical channels using WDM technology

Quantum wavelength band	Classical wavelength band	Number of classical channels	Classical channel launch power (dBm)	Multiplexed data bandwidth (Gbps)	Achievable distance (km)	Max SKR (bps)	QKD Type	Year	Reference
O-band	C-band	1	Tunable	1.2	28	NA	DV	1997	[187]
O-band	C-band	4	Tunable	NA	10	100	DV	2004	[203]
O-band	C-band	1	6	NA	10	70	DV	2005	[204]
O-band	C-band	4	Tunable	17.5	25	9	DV	2005	[205]
O-band	C-band	4	-21	40	15	8	DV	2006	[206]
C-band	C-band	4	-2	10	50	NA	DV	2006	[183]
O-band	C-band	4	Tunable	NA	10	100	DV	2009	[207]
C-band	C-band	2	-5	NA	25	6	DV	2009	[184]
C-band	C-band	4	Tunable	1	50	11	DV	2010	[185]
C-band	L-band	3	Tunable	1.25	90	7,600	DV	2012	[189]
C-band	C-band	2	Tunable	20	70	52,000	DV	2014	[186]
C-band	C-band	1	-3	NA	75	490	CV	2015	[208]
C-band	L-band	3	Tunable	1.25	25	1,000,000	CV	2015	[209]
C-band	C- and O-band	2	-5	0.1	45	4,000	DV	2015	[210]
C-band	C-band	2	Tunable	200	101	10,000	DV	2016	[211]
O-band	C-band	32	10	7168	80	1,000	DV	2017	[212]
C-band	C-band	1	-5	100	150	1,000	DV	2017	[213]
C-band	C-band	20	18	560	5	NA	CV	2017	[214]
C-band	C-band	7	4	87.5	10	50,000	CV	2018	[215]
C-band	C-band	18	14	3500	10	75,000	CV	2018	[216]
C-band	C-band	10	3	100	20	90,000	CV	2018	[217]
C-band	C-band	100	12.9	18300	10	28,900	CV	2019	[218]
S-band	C-band	56	13.6	5600	25	NA	CV	2019	[219]
C-band	C-band	5	-14	50	40	NA	DV	2019	[220]
C-band	C-band	1	6	NA	13	300,000	CV	2020	[221]
C-band	C-band	11	15.6	NA	13.2	12,000,000	CV	2020	[222]

Several field trials around the world investigated the coexistence of quantum, and classical channel over deployed fibre [1, 129, 130, 143, 157, 223–225]. Table 4.2 summarises the main features of the field-trails coexistence experiments. In [223], the quantum channels in the C-band is transmitted with a clock signal in the L-band over 97 km of deployed SMF. In [225] coexistence of quantum and classical channels in the C-band is demonstrated in co- and counter-propagation configuration over 66 km of deployed fibre. Furthermore, [130], and [129] are the Cambridge quantum network and Madrid quantum network, which were discussed in Section 3.1.2. Cambridge-Ipswich Network [157] was discussed in Section 3.1.3, and finally [1] is the Bristol QKD network which is discussed in the next chapter.

Table 4.2: Summary of field trials for the coexistence of quantum and classical channels using WDM technology

Quantum wavelength band	Classical wavelength band	Number of classical channels	Classical channel launch power (dBm)	Multiplexed data bandwidth (Gbps)	Achievable distance (km)	Max SKR (kbps)	QKD Type	Year	Reference
C-band	L-band	1	-33	NA	97	0.820	DV	2008	[223]
C-band	C-band	4	-10	40	26	160	DV	2014	[224]
C-band	L-band	3	Tunable	1	2.08	10	CV	2016	[143]
O-band	C-band	20	21	3,600	66	5.1	DV	2018	[225]
C-band	C-band	2	Tunable	200	10.6	2580	DV	2019	[130]
C-band	C-band	17	NA	NA	3.9	70	CV	2019	[129]
O-band	C-band	5	Tunable	500	14.2	1.95	DV	2019	[157]
C-band	**C-band**	**4**	**Tunable**	**400**	**5.8**	**1.28**	**DV**	**2022**	**[1]**

4.5 Bristol QKD network Experimental System Testbed

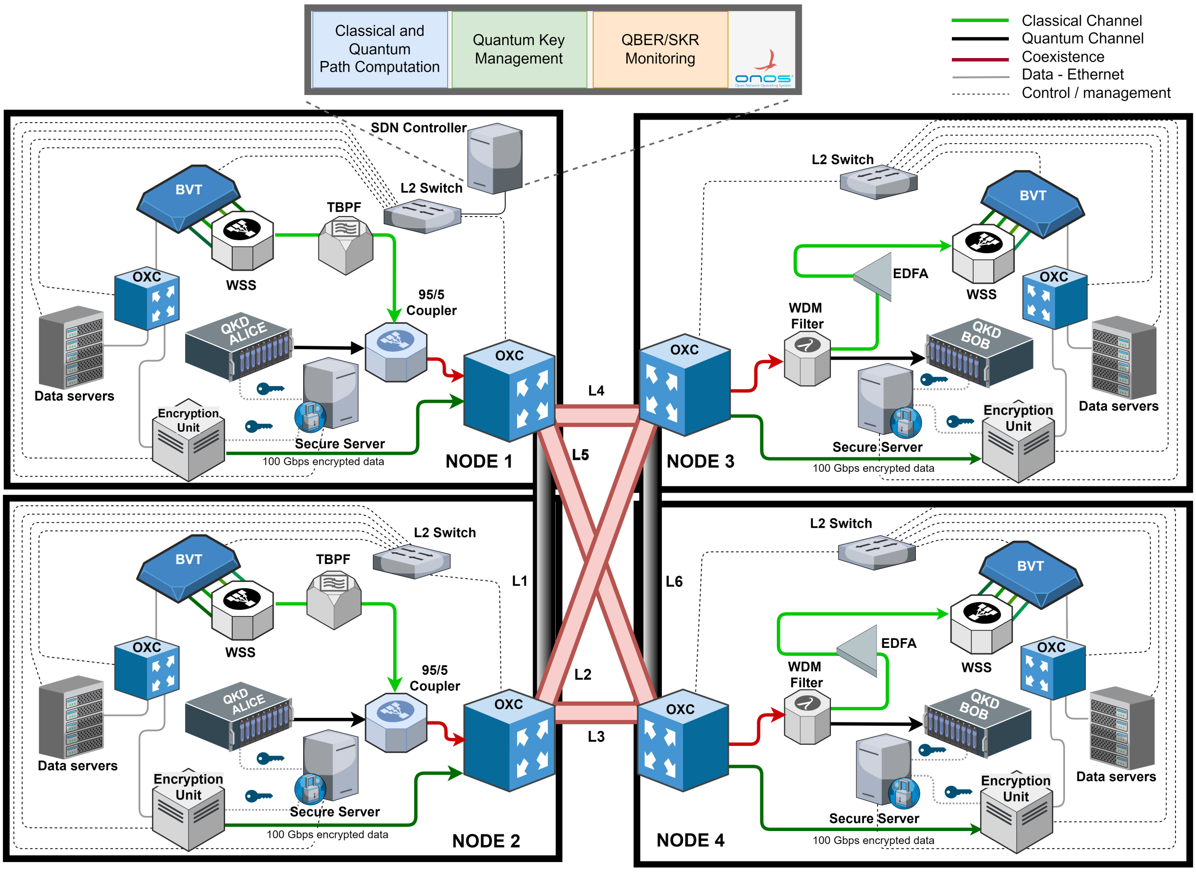


Figure 4.8: Trusted-node-free Dynamic QKD Network configuration two testbed. Red link: Fibre with QKD communication, Black link: Fibre without QKD communication.

Figure 4.8 shows a details testbed setup of Figure 3.11 V. This testbed is used to demonstrate the dynamic QKD-networking and coexistence capability using two QKD pairs and an optical classical system. The network comprises four nodes interconnected via SMF links resulting in a full-Mesh classical network due to physical fibre connecting all four nodes simultaneously. Each node is equipped with an optical cross-connects (OXC) Polatis switch, a bandwidth variable transponder (BVT), a QKD device, an encryption unit, data servers and a secure server. It is possible to transmit classical data using the BVT, coexisting or not with the quantum channel, while it is also possible to transmit encrypted data. This section describes the testbed in detail.

The BVT includes four ports at 100 Gbps (25 Gbaud) data rate, each with PM-QPSK modulation format. Each of the ports can be tuned to any of the 100 wavelengths in the C-band included in the ITU-T grid with 50 GHz offset. The QKD unit used is a commercially available ID Quantique Clavis^2 DV-QKD [32] system with an auto-compensating interferometric setup and quantum random number generators (QRNGs) to create secret keys. These Clavis^2 systems support fully automated sifting for the BB84 protocols and key distillation. The last piece of equipment included in each node is a software encryption unit Dell PowerEdge server, responsible for the software encryption and used to secure the user data transmission with AES-256 encryption.

As shown in Figure 4.8 in Node 1 and Node 2, the four coherent output ports of the BVT are coupled using a WSS, for a total throughput of 400 Gbps and an isolation of 30 dB per channel. The WSS combined output is connected to the input port of a tunable bandpass filter (TBPF1) with 60 dB of isolation and extremely sharp filter edges. A controllable OXC switch is used to enable classical data channels and QKD signal routing and switching functionality. The filtering stages and the OXC devices form a quantum reconfigurable optical add-drop multiplexer (q-ROADM). The q-ROADM provides low loss switching capability for the quantum channel that has a 10 dB limited power budget. It also allows the dynamic reconfiguration of a hybrid QKD-classical network by allowing the arbitrary multiplexing of classical wavelengths and quantum channels at any port (or any degree) of the q-ROADM [226]. The outputs of the classical and quantum channels are coupled via a 95/5 ratio and insertion loss of 13 dB for the 5% port used to enable low power loss in the quantum channel. The second port of this 95/5 coupler is used to exchange the encoded photons of the DV-QKD Alice unit considering a power loss of less than 0.5 dB for the 95% port. The output of the 95/5 coupler is connected to the OXC and the coexisting quantum and classical channels are injected into the optical link via the suitable cross-connection. The OXC used is a SDN-enabled optical fibre switch with typical optical losses per cross-connection of 1 dB (Polatis switch). In these nodes, the encryption server will interface to the ID Quantique Clavis^2 unit for the QKD protocol and an optical output of 100 Gbps data rate [16, 21] will transport the encrypted data towards the optical link via the OXC. In Node 3 and Node 4, the OXC will cross-connect the incoming coexisting signal to an optical bandpass filter with 0.8 dB of loss for the bandpass port, before connecting to the ID Quantique Clavis^2 Bob unit. The pass port of the filter has an optical bandwidth of 100 GHz centred at the 1551.7 nm wavelength of the QKD units. For the rejection port, the quantum channel is blocked and the combined classical signals are optically amplified by an erbium-doped fibre amplifier (EDFA) to boost the optical power to an acceptable level for detection. The output of the EDFA feeds a 1 × 4, 6 dB splitter and its four different optical ports are each connected to a coherent receiver of the BVT. Finally, in these nodes, the decryption server will extract the data received after processing the key. Table 4.3 summarises the main parameters of the implemented fully-meshed QKD dynamic network.

Table 4.3: Parameters for dynamic QKD networking testbed

Parameters	Value
Classical Channels	
Number of Channels	4
Classical Channel Wavelengths	1550.52 nm, 1550.12 nm, 1549.72 nm, 1549.32 nm
Classical Channel Frequencies	193.35 THz, 193.40 THz, 193.45 THz, 193.50 THz
Grid Spacing	50 GHz
Modulation Format	PM-QPSK
Optical Signal-to-Noise Ration (OSNR)	20 dB
Capacity per Channel	100 Gbps
Total Capacity	400 Gbps
Pre-FEC Level	15%
Detector sensitivity*	-35 dBm
Quantum Channel	
DV-QKD Wavelength	1551.7 nm (C-band)
DV-QKD Frequency	193.20 THz
QKD Protocol	BB84
Maximum Distance	50 km @10 dB loss
EDFA	
Noise Figure	5 dB
Operation Mode	Continuous optical power
Encryption/Decryption	
Encryption technique	AES-256
Encryption data rate	10 Gbps
Optical bandpass/Rejection Filter (OBRF)	
Insertion loss bandpass port	0.5 dB
Center wavelength bandpass port	1551.7 nm
Bandwidth bandpass port	100 GHz

**Corresponding to PM-QPSK Modulation @100 Gbps and back-to-back*

4.6 Results

Table 4.4 shows the main parameters of both configurations of the dynamic QKD network of Figure 3.11 IV and V. The parameters of the optical fibre links are described, such as fibre lengths and end-to-end power losses. Also, Table 4.4 depicts the number of cross-connections per link required for dynamically switching to the quantum channel requested. The quantum parameters, such as QBER and SKR are represented in this table. In addition, the combination of links for multi-hop scenarios is included to show the performance of the dynamic QKD network without coexistence.

Table 4.4: Dynamic QKD network results and parameters without coexistence

Link	fibre Length (km)	End-to-End Power Budget(dB)	# OXC	QBER (%)	SKR (bps)
Back-to-Back	0	4.99	1	1.02	2575.69
L1 (A_2-B_1)	0.5	5.19	2	1.31	1762.06
L2 (A_2-B_3)	1	5.70	2	1.43	1414.15
L3 (A_2-B_4)	5.8	6.90	2	1.70	1078.03
L4 (A_3-B_1)	4.7	7.00	2	1.91	895.54
L5 (A_1-B_4)	1.625	9.22	2	3.03	418.74
L6 (A_3-B_4)	1.625	9.61	2	3.65	360.08
L1 + L2	1.5	7.44	3	2.01	819.22
L1 + L3	6.3	8.60	3	2.70	533.97
L1 + L4	5.2	8.79	3	2.73	542.26
L2 + L3	6.8	9.14	3	3.03	430.56
L2 + L4	5.7	9.42	3	3.05	417.94

4.6.1 Results of the Fully-Meshed Dynamic Network with Coexistence

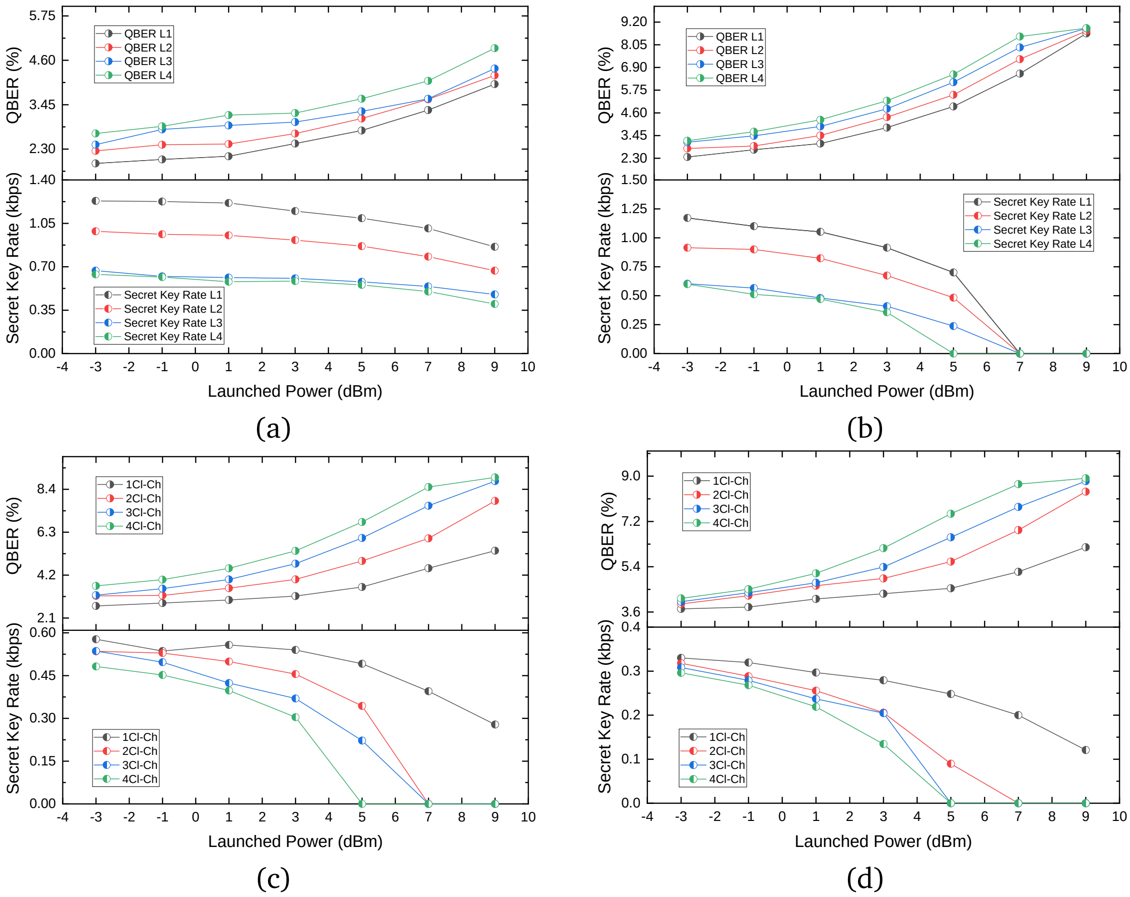
To investigate the effect of Raman noise over the quantum channel, the testbed of Figure 4.8 is used considering links L1, L2, L3 and L4 and one classical channel centred at the frequency of 193.35 THz with 150 GHz spacing from the quantum channel. Figure 4.9 (a) shows the measured SKR and QBER of the quantum channel at different launched optical power levels of the classical channel. As observed, when the launching power is more than 1 dBm, the QBER and SKR deteriorate due to the noise leakage into the 100 GHz bandwidth of the internal filter of the Bob DV-QKD unit. Moreover, the close QBER values achieved by the QKD system over all the links reflect the small variation of optical attenuation of 2 dB for each link. In addition, at the BVT highest possible launch power of 9 dB, the lowest SKR achieved is 400 bps with continuous key generation for link L4. As shown in 4.4, L3 is longer than L4 and therefore, the Raman noise should deteriorate the QKD performance for L3 more than L4 due to the longer fibre. However, as shown in Figure 4.9 (a) the SKR is identical for both L3 and L4. This is due to the short fibre length (<6km) of both links, the low coexistence power and the almost equivalent end-to-end power budget for both links.

Figure 4.9 (b) shows the impact of coexisting four classical channels (193.35 THz, 193.40 THz, 193.45 THz and 193.50 THz) over the quantum channel (193.20 THz). As observed from Figure 4.9 (b), the quantum channel deteriorates faster compared to Figure 4.9 (a) due to the higher launch power and the combination of Raman noise and other nonlinearities. Considering the two frequencies 193.35 THz and 193.50 THz as f_1 and f_2 respectively, one product of the FWM would be $f_3 = 2f_1 - f_2 = 193.20\ THz$ which is the quantum channel frequency which degrade the performance of the quantum channel due to the additional noise from such phenomena. Therefore, more noise leakage into the Bob DV-QKD unit occurs due to higher aggregated launch power (16 dBm when transmitting four classical channels at 9 dBm), and higher Raman noise. It also observed that at a launch power of 7 dB per channel, the QBER values exceed the threshold of 6% causing the SKR to be zero bps.

Figure 4.9 (c) and Figure 4.9 (d) show the SKR and QBER over the combined links of L1+L2 and L1+L3. In both figures, increasing the number of classical channels is presented to reflect the impact of incremental channels over the quantum channel. As observed, similar trends of QBER and SKR deterioration appear for both cases of links due to the optical power budgets in the vicinity of 8 dB. Also, it is clear in both links that by adding a classical channel, the total aggregated power is increased and the Raman noise effect is proportional to the power added, worsening the quantum channel performance. It can also be observed that the QBER values exceed the threshold of 6% causing the SKR to be zero bps at a launch power of 5 dB per channel which is different compared to Figure 4.9 (b). This is due the additional losses of links L1+L2 and L1+L3 and the additional cross-connection in the optical switch as shown in Table 4.4.

4.6.2 Coexistence over Bristol City 5GUK Testbed

To further explore the coexistence of quantum and classical channels, two links of the Bristol City 5GUK testbed were used [24]. One link connects the site HPN to the WTC node, with a fibre length of 1.9 km total optical fibre attenuation of 4.68 dB. The other link interconnects the sites NSQI to the node WTC passing through the node HPN (2 hops) with a fibre length of 2.7 km total optical fibre attenuation of 5 dB. Figure 4.10 (a) shows the QBER and SKR for the link HPN-WTC. A quantum channel is coexisted with 6 PM-QPSK 100 Gbps classical channels with 50 GHz spectrum space difference between them (from 193.5 THz to 193.75 THz). To evaluate the performance of the coexistence over these channels, the bandwidth of the tunable optical bandpass filter of Section 5.2.2 is tunned to gradually allow noise proliferation into the quantum channel. As observed, when the filter bandwidth is in the range of 500 GHz to 725 GHz, the SKR obtained is constant and higher than 890 bps and the QBER is lower than 2.8%. However, for filter bandwidths higher than 750 GHz, the noise leakage over the quantum



(a)

(b)

(c)

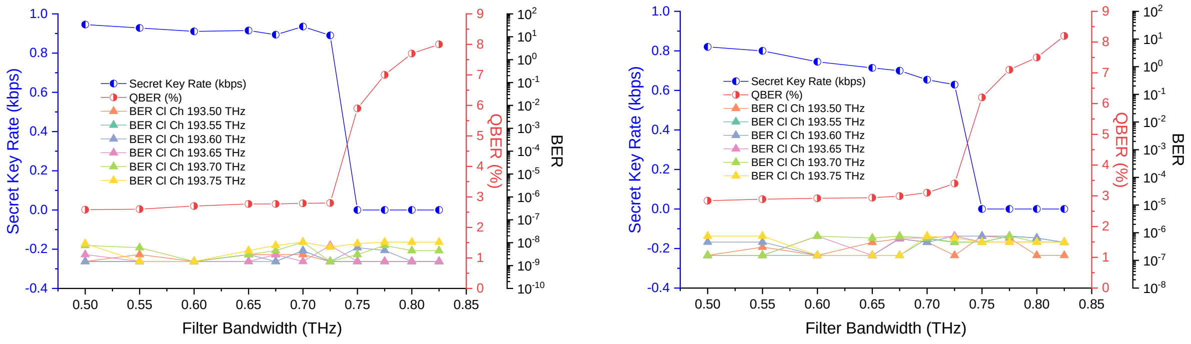
(d)

Figure 4.9: (a) Coexistence with one classical channel (F_c193.35 THz) for four different links. (b) Coexistence with four classical channels for four different links. (c) Coexistence with four classical channels for link L1+L2 (d) Coexistence with four classical channels for link L1+L3.

channel will impede the key generation due to high QBER values of more than 6% causing the SKR to plummet to zero bps. For the classical channels, the BER measured was 3.5×10^{-9} average for the channels selected. Figure 4.10 (b) shows the QBER and SKR curve with respect to the filter bandwidth for the link NSQI-WTC. Compared to the link HPN-WTC (Figure 4.10 (a)), the SKR is lower. This is due to the additional cross-connection for the extra hop in the link which increases the power budget of the link.

Experiment Highlights

Although the coexistence of quantum and classical channels has been explored before in lab and in field demonstrations as shown in Table 4.1 and Table 4.2, all the demonstrations were for a static point-to-point fibre link. In this experiment, we took the coexistence demonstrations a step further by overcoming the static point-to-point link and offering the option of switching both the quantum and classical channel in a deployed dynamic QKD network. The extra dynamicity is realised in terms of extra loss of the optical switch (>1 dB) which is used in each node and



(a) (b)

Figure 4.10: (a) Coexistence of quantum channel and six classical channels in a 1.9 km field-deployed fibre (HPC-WTC) (b) Coexistence of quantum channel and six classical channels in a 2.7 km field-deployed fibre (NSQI-WTC).

had a low penalty on the SKR generated by the QKD systems.

4.7 Use-cases

The deployment of a quantum-secure network is being adopted in real-life applications worldwide for industrial, commercial and government applications [227, 228].

4.7.1 First Industrial Deployment of a Quantum Network in the UK

BT and Toshiba announced the first industrial deployment of a quantum network in the UK between the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS). The demonstration was deployed using a standard Openreach optical fibre link between the two sites with a total length of 6 km coexisting both the quantum and classical channels. Toshiba QKD systems [229] are used to distribute the single encoded photons between the two sites, while being coexisted with the classical data in the Openreach optical fibre. Therefore, eliminating the cost of dedicated infrastructure for key distribution. Although the deployment range is only 6 km, Toshiba QKD system enables the transmission of single encoded photons over 120 km making it a great candidate across major metropolitan environments. This demonstration shows the maturity of QKD and coexistence technologies, which are used to provide information-security to valuable data while being implanted using the current classical infrastructure.

4.7.2 First Commercial Deployment of a Quantum Network in the UK

BT and Toshiba also demonstrated the first commercial deployment of quantum-secured communication services for EY [230]. The quantum link secured two EY sites one in Canary Wharf, and one near London Bridge.

4.7.3 First Government Deployment of a Quantum Network in the World

In 2020, ID Quantique and South Korea (SK) Broadband announced a 2000 km quantum-secured network in South Korea part of the government-run project "Digital New Deal" coexisting both the quantum and classical channels. QKD is used to secure communication networks of 48 government organizations across the country, including the Ministry of Economy and Finance, the Ministry of Education, the Ministry of Employment and Labor and some local governments [231]. In 2021, the quantum-secured network was expanded and seven more institutions from the public and private sectors were added to the network [232]. The public sector institutions are Korea Hydro & Nuclear Power Co., Daejeon Waterworks Headquarters, and Gwangju Institute of Health and Environment. In the private sector, QKD will be use to protect the world's best hydrogen car design technology centre at Pyeonghwa Holdings, and the first cloud-based medical system at Korea University's K-Bio Center. Keimyung University Dongsan Hospital is also using QKD to secure personal information. QKD will also be installed on the "Super-connected Intelligent Research and Development Network" which is run by the Korea National Information Society Agency (NIA). So far SK Broadband Consortium spent over 50M USD on this project [232]. This along with the government institutions that are deployed QKD shows the magnitude and importance of this technology to secure the communication network against the threat of quantum computers [228].

4.8 Summary

The best and worst spectral positions of classical channels were determined via numerical calculation of the impact of the nonlinear effects such as Raman scattering and four-wave mixing on the quantum channel performance. Furthermore, the coexistence in the Bristol dynamic QKD network was discussed. For the coexistence of a single classical channel with a launch power of -3 dBm over the longest link (L3) with 5.8km, a QBER of 2.3% and an SKR of 980 bps was demonstrated with a minimum average pre-FEC BER of 1.28×10^{-8} for the error-free classical channels. Investigations also prove that when coexisting four classical channels with 150 GHz spacing from the quantum channel, a minimum launch power of 7 dB per channel is required to deteriorate the key generation process with an SKR of zero bps. Moreover, this work also demonstrated the coexistence of a quantum channel and six classical channels through a field-deployed fibre in the 5GUK Test Network. The key generation process is maintained when the bandwidth of the optical bandpass filter which is centred at 193.625 THz and is lower than 750 GHz. When the filter bandwidths is tunned to higher than 750 GHz, the noise leakage over the quantum channel will impede the key generation due to a high QBER of more than 6%, causing the SKR to plummet to zero bps.

CHAPTER 5

Coexistence of Quantum and Classical Channels in Advanced Mediums

Declaration of Work

This chapter includes four experiments and each experiment has been published in either a conference proceeding, a journal article or both.

For the MCF experiment [5], Emilio Hugues-Salas and I developed the final testbed, carried out the experiments, analysed the results, and wrote the journal article.

For the first HCF experiment i.e. transmission over 2 km HCF [2, 10, 17], I developed the testbed, carried out the experiments, analysed the results, and led the conference paper and journal article.

For the second HCF experiment i.e. transmission over 7.7 km HCF [12, 13], I came up with the idea, and developed the initial testbed. I carried out the characterisation of the testbed with Florian Prawits. Due to the lack of time, the experiment was then continued by Florian Prawits and Florian Honz.

For the free space experiment [8], I developed the optical testbed and led the conference paper. In collaboration with Dr. Andy Schreier, we carried out the experiments, and submitted an extended journal article. The terminals are made by the University of Oxford.

All of this work was done under the supervision of George Kanellos and Reza Nejabati.

Since I am a co-author of the original text in [2, 5, 8, 10, 12, 13, 17], parts of the papers have been reused in the chapter where appropriate.

While the cost of manufacturing individual QKD systems is declining continuously through the utilization of increasingly available off-the-shelf components, one obstacle preventing the wide-scale roll-out of this technology is the limitations imposed by the required infrastructure. Extending the usage of QKD from mere point-to-point links into a real network of users is cost-prohibitive due to dedicated dark fibre links typically needed for these systems, as integrating QKD with classical channels remains a challenge [233]. To further evaluate the coexistence of quantum and classical channels and the visibility to integrate quantum and classical technologies, we investigated three different transmission mediums, a multicore fibre (MCF), hollow core fibre (HCF), and free space enabled by fibre-wireless-fibre (FWF) terminals. Although such mediums are not commonly used in the current infrastructure, they provide attractive properties for both quantum and classical telecommunication applications and are recently getting adopted for different use cases [234–245].

To this end, we have demonstrated the coexistence of quantum and classical channels over MCF, HCF and free space. For all three mediums, we tested different scenarios, including varying the number, power and position of the classical channels and investigated their effects on the quantum channel performance in terms of SKR and QBER. This chapter is divided into four sections; each section corresponds to an experiment in a different transmission medium. The mediums are a 1 km 7-core MCF, a 2 km HCF, a 7.7 km HCF and finally, a 2.5 m free-space link. We start each section by providing background, motivation and a summary of the findings. After that, we discuss the experimental testbed for each experiment in detail, followed by the results obtained from different scenarios. We then present the outcome/summary for each experiment. Finally, we conclude the chapter by discussing the improvement across the experiment.

5.1 DV-QKD Coexistence with 11.2 Tbps Classical Channel over a 7-Core Multicore fibre

With current bandwidth demands exceeding the available spectrum capacity of single-mode optical fibre (SMF), multicore fibres (MCF) have been introduced as speciality fibres to address future bandwidth needs by exploiting the space division multiplexing (SDM) dimension [246]. Numerous MCF technologies and fibre profiles have been brought into perspective, aiming to improve MCF characteristics such as the number of cores, crosstalk (XT) and coupling into the fibre. As a consequence of this research on MCFs over the last decade [247–249], initial MCF-based SDM deployments and field trials are being undertaken in different parts of the world, such as the testbeds in Japan and Italy [250–252]. In addition, since the manufacturing costs of these specialized fibres and their cost of deployment in long-reach communications are prohibitive and their main benefit is the reduction in physical space requirements, MCF primary field of application is considered to be the intra-data centre (DC) links to decrease the density of current optical fibre bundles interconnecting the thousands of processing nodes

[253]. . However, in future data centres, 94% of the total workloads and compute instances will be processed in the cloud as opposed to only 6% for the traditional data centres [254]. In these emerging cloud data centres, workloads and compute instances are migrated across servers, inside and between data centres, for optimum data center workload balance and maximum support to end-user applications. In this migration, cloud virtualization is the critical factor, and dynamic deployment of workloads is enabled by moving virtual machine (VM) images between physical machines through the data centre. However, this migration of virtual resources is vulnerable to attacks whenever VMs are in transit and between secured perimeters, and attackers can exploit the network vulnerability to gain unauthorized access to the VMs [255].

To provide security in these cloud data centers, different protocols are used to protect the data whenever communication is required between servers and applications. A typical protocol widely used is the transport layer security (TLS) protocol to protect and authenticate communications across the Internet. However, TLS relies in part on asymmetric cryptography algorithms, such as RSA and Elliptic Curve Diffie-Hellman (ECDH), which are vulnerable to quantum computing attacks [256]. Therefore, to overcome this security weakness, improvements to this TLS and other protocols are required to prevent eavesdropping and tampering. One effective method that will ensure security within cloud data centres and that can be integrated with encryption protocols is quantum key distribution (QKD). Since QKD enables the distribution of symmetric keys, the integration of TLS with QKD has been suggested in several communications [257–259] and standards [260].

As explained in the previous chapter, since DV-QKD schemes rely on the exchange of single or few photons to transfer the quantum information, severe restrictions on the acceptable noise levels are imposed, and overall optical insertion losses limit the operation of the DV-QKD link, rendering the deployment of quantum with classical optical communication channels very difficult. Therefore, a viable coexisting scheme is needed to guarantee large-scale deployment of DV-QKD technologies parallel to classical optical telecommunications. Based on this coexistence requirement and the inherent advantages of MCFs, we reported the preliminary results to optimize the transmission capacity of the classical optical channels in the peripheral cores of an MCF while sustaining the viability of a single quantum channel in the central core [261, 262].

Several coexisting schemes that allow quantum channels and classical channels in the same optical medium have been proposed, mainly relying on the principles of wavelength division multiplexing (WDM) discussed in the previous chapters. Another approach for achieving efficient coexistence levels lies with the use of SDM. In this case, multicore fibres offer enhanced channel isolation between cores and can, in principle, allow the unconditional coexistence of QC and CC. For instance, in [263] the coexistence of QC and CC was demonstrated over a 7-core CF with 2 × 10 Gbps CCs and 0 dBm of launching power. In [264] the coexistence of QCs and CCs is presented in which the CCs were emulated by a continuous-wave (CW) and launching powers of +12 dBm. In [265], 6 x 112 Gbps PAM signals were used as CCs and single-photon detection was used to verify the feasibility of the coexistence of QCs and CCs. In this direction, MCFs have also been exploited to optimize the SKR of the QC by initiating the concept of high-dimensional quantum cryptography, and in [266] a spatial-multiplexed key rate of 105.7 Mbps was demonstrated, coexisting with 37 × 10 Gbps classical channels. All these advances illustrate the suitability of QKD over multicore fibres for intra- and potentially inter-data centre deployments, in which short MCF links can be promoted to support intense traffic and quantum secure communications between compute nodes in data centres. MCF has recently gained a lot of popularity and was used in CV-QKD and high dimensions qubit experiments [234, 237, 265, 267–270].

In this section, we generalize our approach and evaluate the system architecture with an additional QKD channel for increased coexistence levels of two quantum channels and classical channels over the same 7-Core MCF. We achieved the coexistence of a quantum channel and a world record 11.2 Tbps classical channels in MCF. First, we present the experimental system testbed. After that, we present our results which are divided into four part i) MCF static XT Characterization, ii) spectrum of the quantum and classical channels over a single core (central core), iii) channel spacing impact on the quantum channel performance, and iv) characterization of the MCF for bidirectional coexistence. Finally, we conclude our findings.

5.1.1 Experimental System Testbed

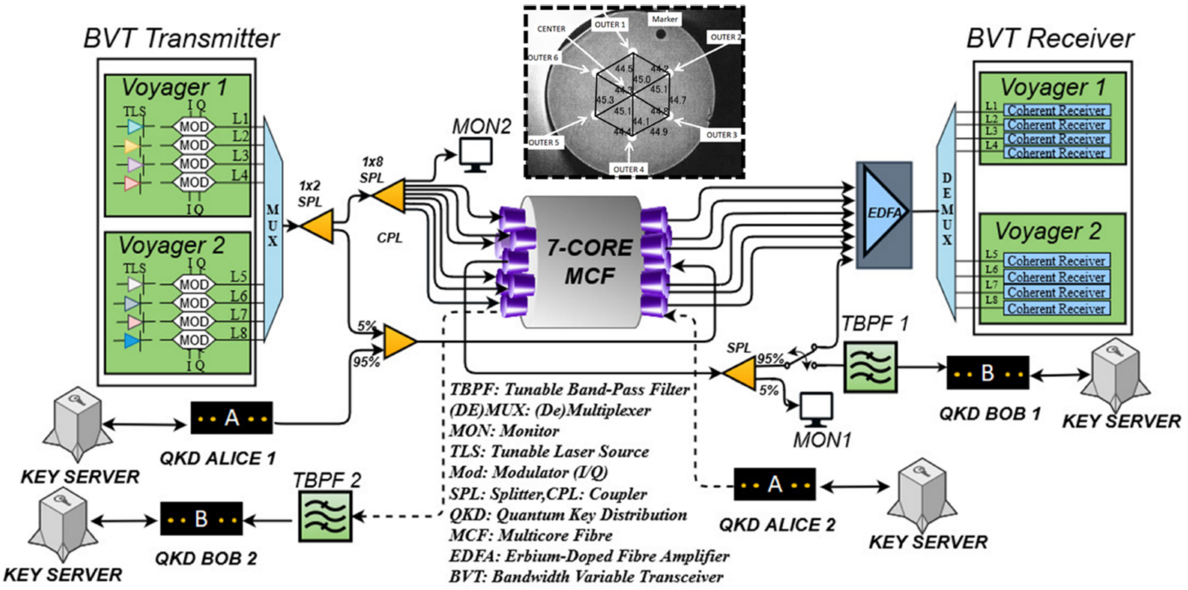


Figure 5.1: Experimental testbed for the coexistence of 11.2 Tbps classical channels and QKD channels over a 7-core multicore fibre. Inset: Cross-sectional Diagram MCF.

Figure 5.1 shows the experimental system setup used to demonstrate the coexistence of classical channels with QKD channels over a 1 km-long 7-Core MCF (as inset figure, Figure 5.1

also illustrates the cross-sectional diagram of the MCF used, fabricated by Mitsubishi). For the classical channels, two optical packet DWDM platforms are used with bandwidth-variable transponders (BVTs). Each of these units include four BVT ports reconfigurable to coherent 100 Gbps (PM-QPSK), 150 Gbps (8-QAM) or 200 Gbps (16-QAM) and each port can be tuned to any of the 100 wavelengths in the C-band included in the ITU-T grid with 50 GHz offset. Adaptable soft-decision forward error correction (SD-FEC) is also available in the transponders to enable maximum transmission capacity with minimum errors. In this experiment, all the ports where configured with 16-QAM modulation for a maximum of 200 Gbps per channel and the SD-FEC considered was 25%. For the quantum channels, we used the ID Quantique Clavis^2 [32] QKD systems.

As shown in Figure 5.1, the eight coherent output ports of the two BVTs are multiplexed using a wavelength selective switch (WSS) with 5 dB of insertion loss for a total throughput of 1.6 Tbps and its combined output feeds the input port of a 3 dB splitter which divides equally the multiplexed signal into two optical paths. One path is directed to a 10 dB-loss, 1x8 splitter, which further splits the multiplexed signal into eight different paths and six of them are directly connected to 6 cores of the MCF. The second path is coupled to the quantum channel via a coupler with 95/5 ratio and an insertion loss of 13 dB for the 5% port used to enable low power loss in the quantum channel. The second port of this 95/5 coupler is used to exchange the encoded photons of the discrete-variable DV-QKD Alice unit considering a power loss of<0.5 dBfor the 95% port. The output of this 95/5 coupler is then injected into the center core of the 7-Core MCF which has an average core pitch of 44.7 μm and a loss of 0.2 dB/km per core. In the MCF, these quantum and classical signals counter-propagate with the injected classical msignals from the other cores, as shown in Figure 5.1, for a combined data rate of 11.2 Tbps for the classical channels. After the coexistence within the MCF, the output of the center core feeds a 3.4 dB-loss, 2 nm 3 dB-bandwidth tunable-band pass filter (TBPF) tuned to the 1551.7 nm wavelength of the QKD unit. After the TBPF, the DV-QKD Bob unit undertakes the single-photon detection and processing of the encoded photon allowing the completion of the BB84 protocol of the DV-QKD systems. The output of the center core of the MCF is also directed to an optical amplification stage to set the classical signals to the suitable detectable power levels before demultiplexing via a 5 dB-loss WSS. This last WSS connects to the receiving ports of the BVT equipment for coherent reception and the outputs of the remaining outer cores of the MCFs are also connected to the amplification stage before demultiplexing and coherent detection of the classical channels. In this testbed, the total end-to-end (Alice to Bob) quantum channel loss is 6.74 dB. A summary of main parameters of the testbed is shown in Table I.

In addition, as part of this testbed, a second QKD channel was integrated to demonstrate the coexistence of not only several classical channels but also two quantum channels over the MCF. Figure 5.1 shows a second QKD Alice and Bob units interconnected via an outer core of the MCF and a TBPF. A key server is used per each QKD unit to undertake the quantum protocol and to retrieve the keys generated by the quantum channels. These key servers use as classical channel a standard ethernet connection to undertake the post-processing required to transform the photons exchanged via QKD into secure keys.

5.1.2 Results

5.1.2.1 MCF Characterization

Figure 5.2 shows the static XT characterization of the 1km-long 7-core MCF. In here, the measured XT is the difference of the injected optical power of a continuous wave (CW) on a selected core from the observed output power of another core. Co- and counter-propagation is measured by observing the output power at the input or output ports of the MCF. To characterize this type of crosstalk, the central core (core 4) was assigned with the QKD channel and the outer cores with the classical channels representing the worst-case scenario. This configuration allows an equal impact of the classical channels over the QKD channel enabling a suitable evaluation of the feasibility of QKD and classical signals simultaneously over a MCF [211, 265]. As observed in Figure 5.2(a), core 4 (central core) is the most affected with a range of XT levels from -51 dB to -44 dB for the case of co-propagation (dashed square, Figure 5.2(a)) and for the case of counter-propagation, the XT levels of core 4 vary from -66 dBm to -60 dBm (dashed ellipse, Figure 5.2(a)), being evident that the effect of XT due to counter-propagation is lower compared to the one due to co-propagation, as described in [264, 271].

Figure 5.2b shows the measured co- to counter- propagation XT difference (Co-CouXT) per core of the MCF. As observed, in the selected core 4, an additional average tolerance of 16.5 dB to XT is measured whenever counter-propagation of optical signals is used (dashed circle, Figure 5.2(b)). Therefore, for this experiment, counter-propagation of quantum to classical signals was selected, with the quantum channel in the central core (core4) since XT isolation determined the performance of the entire system for coexistence.

5.1.2.2 Quantum and Classical Channel Coexistence Over a Single Core of the MCF

Figure 5.3 shows the spectrum of the 8 x 200 Gbps classical channels coexisting with the quantum channel over the central core of the MCF, obtained by using a tap coupler in the quantum channel (Figure 5.1). As a reference, Figure 5.3 illustrates the optical filter profile used to filter out the Raman noise generated by the classical channels in the quantum channel. Figure 5.3 also shows the transmitted classical signals after passing through an adjacent core of the MCF before demultiplexing and coherent detection in the receiver (Figure 5.1).

5.1.2.3 Channel Spacing for Coexistence Over a Single Core

To further investigate the effect of the classical channels over the quantum channel over the same core, Figure 5.4 illustrates the performance of the coexisting channels by decreasing

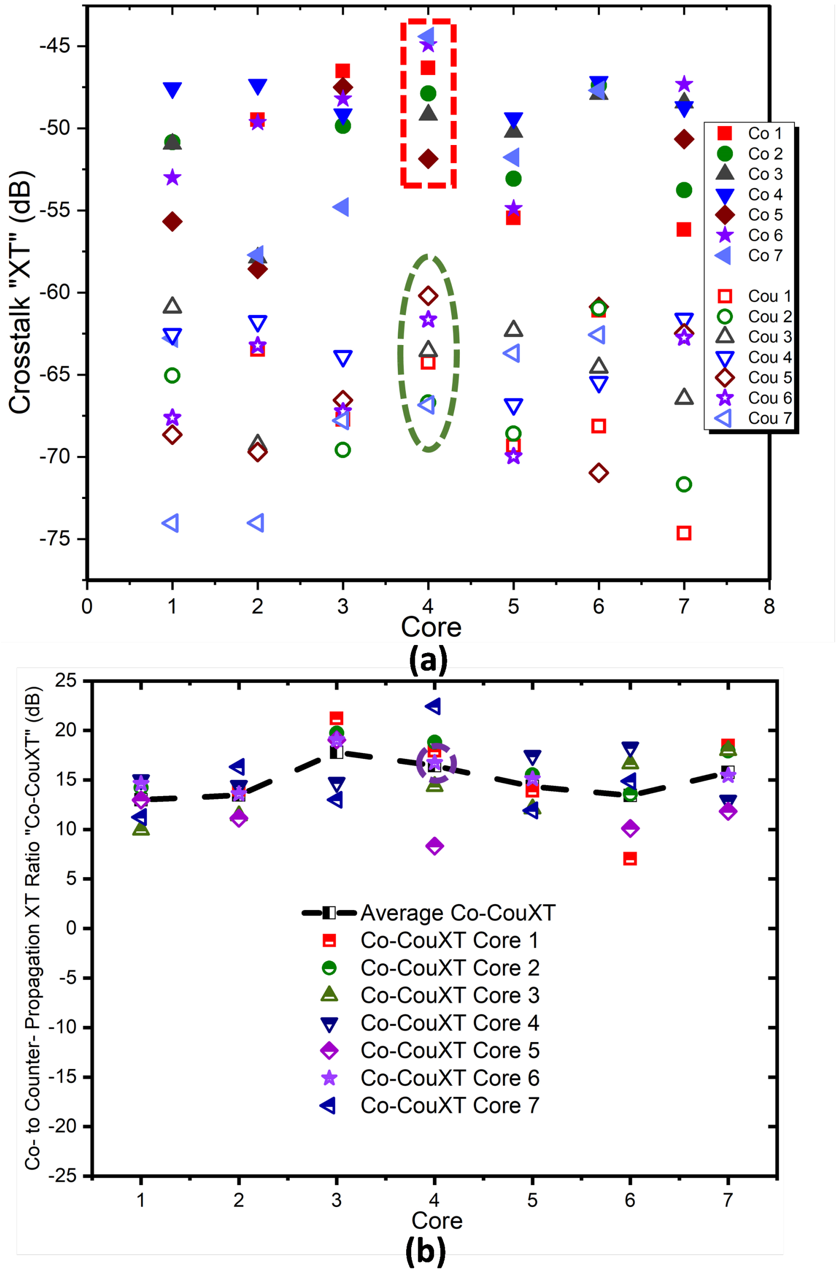


Figure 5.2: (a)Crosstalk characterization of the used MCF for co-propagation (Co) and counter-propagation (Cou) of optical signals. (b) XT difference per core of the co-propagation to the counter-propagation of optical signals in the 7-core MCF used.

the spectral spacing between them. A minimum spacing of 17 nm between non-contiguous channels (Figure 5.3) was observed with a measured QBER of 5.7% and a secret key rate of 100 bps, for the quantum channel, and an average BER of 1.8×10^{-3} for the classical channels being considerably lower than the SD-FEC limit enabled by the BVT (Figure 5.4). Beyond this

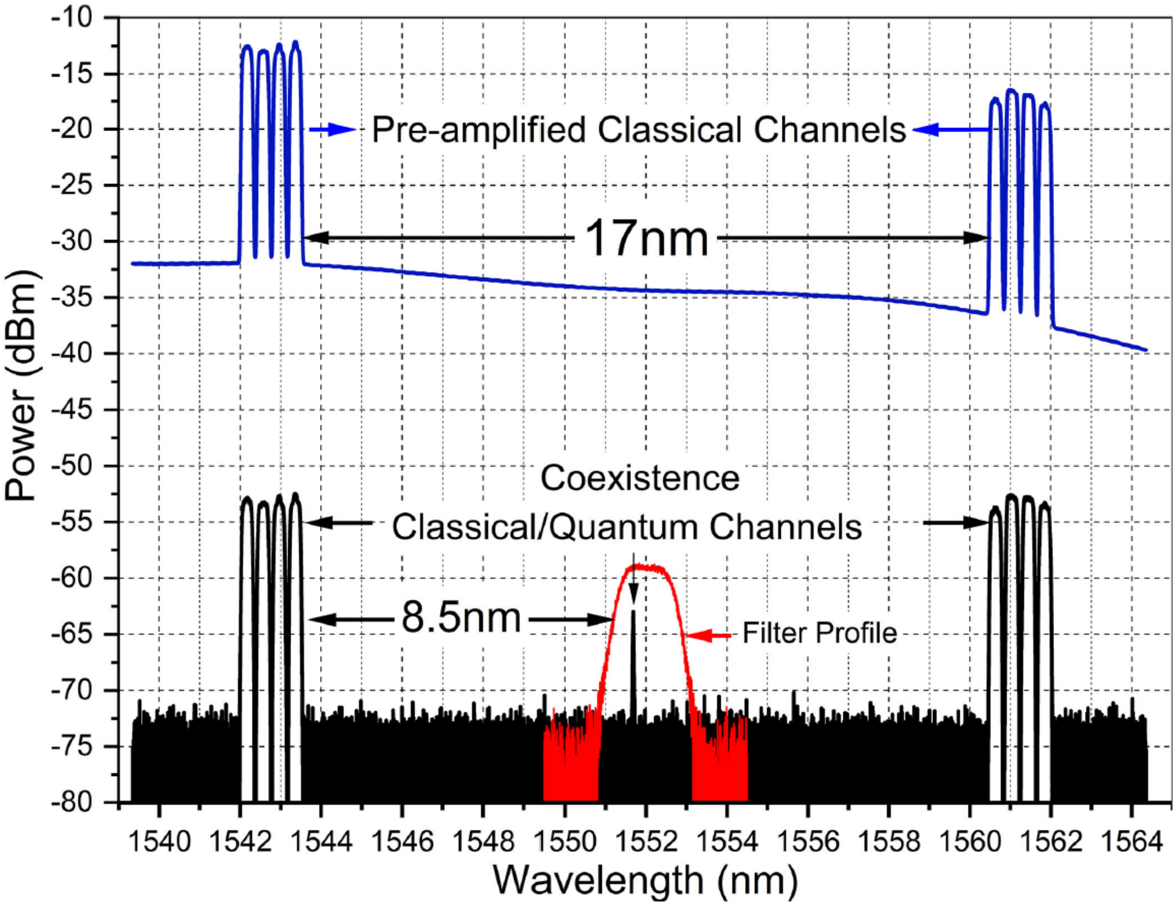


Figure 5.3: Spectrum of the combined transmission over a single core of quantum and classical channels.

minimum spacing, the QKD system stops generating keys. The transmission over the other cores with 1.6 Tbps per core was undertaken in parallel with the DV-QKD channel without the performance of these channels being affected, since the XT of the MCF enabled the coexistence with a total of 11.2 Tbps. To enable this high capacity coexistence, counter- propagation of quantum and classical channels was used, as shown in Figure 5.1, to allow additional XT tolerance shown in Figure 5.2.

5.1.2.4 Performance Evaluation of the Coexistence of a DV-QKD Channel and 11.2 Tbps Classical Channels Over a 7-Core Multicore fibre

While transmitting 1.6 Tbps through each outer core of the MCF and the central core, Figure 5.5 shows the resulting curve of the SKR, QBER and BER vs launch power for the transmission of eight 16-QAM-modulated optical channels and a DV-QKD channel over the central core of the MCF. For this Figure 5.5, the power levels of individual channels were increased from the BVT interfaces to increase the launched power. As observed, the QBER increases and the

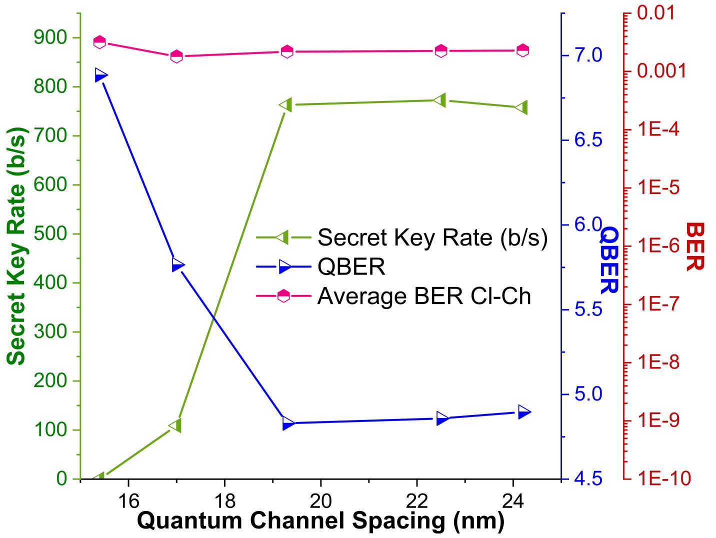


Figure 5.4: SKR, QBER and BER vs channel spacing between the quantum and classical channels of the MCF central core. (Total capacity for CCs is 11.2 Tbps).

SKR decreases when the launched optical power into the MCF is increased up to a maximum power of -9.5 dBm. Beyond this limit, the system stops generating keys due to excessive Raman noise leakage over the quantum channel. This launched power into the MCF was improved by removing the CCs from the central core to a launched power of +5 dBm, however, the coexistence capacity was reduced to 9.6 Tbps. Table II shows a summary for the different launched powers and central core configurations.

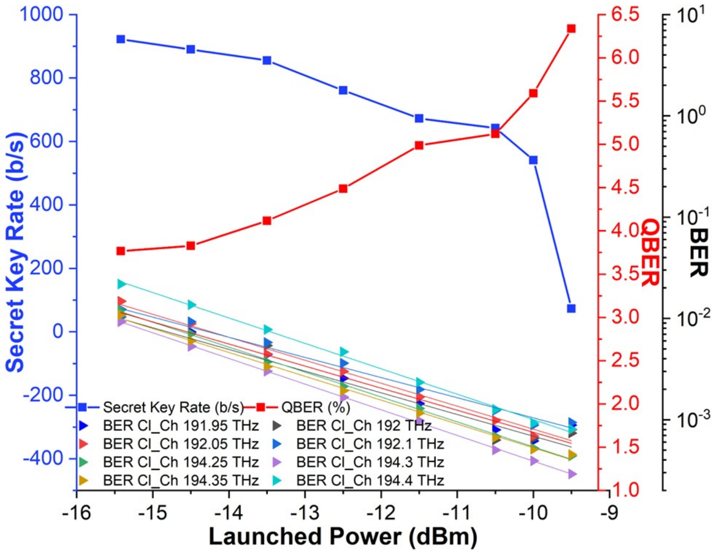


Figure 5.5: SKR, QBER and BER versus launched optical power of the central core of the 7-core multicore fibre. (Total capacity of CCs is 11.2 Tbps).

To explore the impact of the coexistence from adjacent cores of the MCF, Figure 5.6. shows the performance of the quantum and classical channels after adding channels incrementally at different outer cores. To clearly notice this effect, the TBPF before the QKD Bob unit is not used. However, CCs are not used in the central core since the Raman noise generated will not be tolerable by the QC. Therefore, the total capacity in the MCF will be 9.6 Tbps for the CCs.As observed in Figure 5.6, for the first two added cores, the quantum channel QBER and SKR are kept within the limits of 3.5% and 2220 bps, respectively. Beyond three added cores, the performance degrades to 5% (QBER) and 1520 bps (SKR). However, the same performance is kept when adding classical signals for the total six additional cores. To further investigate the coexistence over the MCF, a second DV-QKD system (BB84, ID Quantique Clavis^2) was integrated in the testbed of section II (Figure 5.1), adding a quantum channel in an adjacent core of the MCF. QKD1 coexist in the same core with the classical channels meanwhile the quantum channel of QKD2 is configured without classical channels.

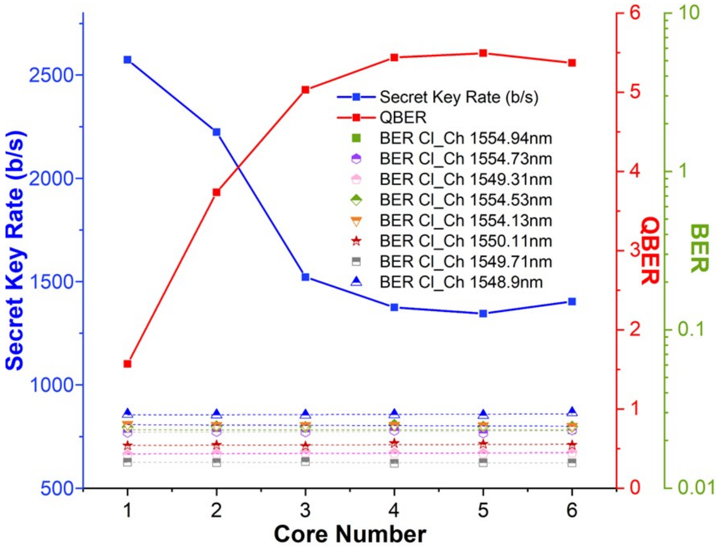


Figure 5.6: SKR, QBER and BER vs combined number of cores with classical channels. Total capacity is 9.6 Tbps (No added CCs in central core).

Figure 5.7 shows the QBER and BER vs launch power into the MCF. In this case, the QBER of the QKD 1 is maintained relatively constant, with an average of 1.7%. The QKD 2 system is affected by the adjacent cores with classical signal power and a QBER change from 2.6% to 5% is observed when the launch power into the MCF is increased from -22 dBm to -9 dBm. As observed in Figure 5.7, the classical channels improve by increasing the transmitted power obtaining an average BER of 9.5 × 10^{-5} at a launched power of -9.5 dBm. The performance of the classical channels was measured by selecting the output of an adjacent core and receiving the signals in the BVT after demultiplexing. More importantly, the system operation is demonstrated over a dynamic range of 10 dB of launched power into the MCF, with keys being generated from both quantum systems and simultaneous transmission of classical channels. It is important to mention in here that for longer lengths of MCFs, the effect of the Raman noise is more evident and should be considered while designing inter-data centres architectures with interconnection distances of tens of kilometres [218]. However, it has been demonstrated that Raman noise is also evident even at short optical fibre lengths [272].

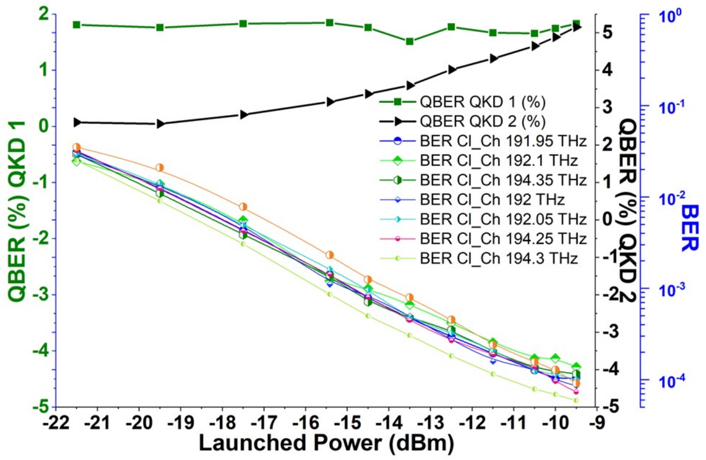


Figure 5.7: Performance evaluation of the coexistence of two DV-QKD Channels and 9.6 Tbps Classical Channels over a 7-core MCF.

5.1.3 Summary

The coexistence of a DV-QKD channel and 56 × 200 Gbps classical channels was successfully demonstrated over a 1 km long multicore fibre for a record-high coexistence transmission of 11.2 Tb/s. For the coexistence over the central core of the MCF, a minimum QBER of 3.7% and a maximum SKR of 920 bps was demonstrated for the DV-QKD simultaneously with a minimum average pre-FEC BER of 1.28 x 10^{-2} for the classical channels. Investigations also prove that a minimum channel spacing of 17 nm is required in between quantum and classical channels and that the incremental addition of classical signals at different cores will degrade the quantum channel for a maximum QBER (SKR) of 5.3% (1400 b/s). Moreover, this work also demonstrated two quantum channels successfully operating over the same MCF maintaining simultaneous generation of keys for an optical power range of 10 dB. This work shows that DV-QKD can effectively coexist with carrier-grade equipment over MCF for maximum capacity and continuous key generation, being suitable for secure intra-data centre applications.

5.2 DV-QKD coexistence with 1.6 Tbps Classical Channel over a 2 km Hollow Core Nested Antiresonant Nodeless Fibre (HC-NANF)

In this chapter, we consider a radical solution to facilitate the coexistence of quantum and classical channels by adopting HC-NANF as a transmission fibre technology, in which nonlinear effects are simply not present. Hollow core fibre (HCF) was first realised in 1999 [273] and has seen many iterations since. From its name, the main features are a hollow core where light propagates along the length of the fibre, a cladding (microstructure) which surrounds the hollow core and confines the light to the core and prevents leakage around the core, and finally, similar to SMF a solid jacket to provide mechanical strength [274]. Due to its hollow core, light propagates ≈ 30% in HCF compared to SMF, achieving low latency, low nonlinearity, and low dispersion. Such properties make HCF attractive for different classical and quantum communications applications. However, for HCF technology to be used for such applications, its loss must compete with the loss of SMF (>0.2 dB/km).

To describe the development of the HCF over the last 20 years, we are doing to describe the unique microstructure surrounding the core:

1. Hollow Core Photonic Band Gap fibre (HCPBGF): in this fibre a period lattices were used to create a bandgap. HCPBGFs were first demonstrated in 1999 [273], and achieved the lowest loss of 1.7 dB/km in 2004 [275]. Although this design achieved a low loss, the transmission window was limited to only 10s of nm. The transmission window has been expanded successfully [276], however, the loss did not improve.

2. Kagome fibre: it was firstly reported in 2002 [277], Kagome fibre covers a broader transmission window comparing to HCPBGF. In such fibres, the membranes around the core were designed to have specific thickness, and therefore, the confinement of the light was provided by anti-resonant effects and inhibited coupling.

3. Tubular fibre: in this fibre, the microstructure around the core was simply a single ring of membranes [278]. Tubular fibres provide a very wide transmission windows [279], however, the losses were too high comapred to SMF.

Antiresonant Hollow Core Fibres (AR-HCF) are optical fibres where light is guided in a hollow core via anti-resonance effects within the glass membranes surrounding the core [280]. AR-HCF surpass the performance of glass core fibres as they have ultra-low optical mode overlap with the glass (and hence reduced optical nonlinearity and Rayleigh scattering), a lower latency, a very low chromatic dispersion, an unprecedented polarisation purity and ultra-low back scattering [281–283]. Significant improvement in optical performance of HCFs were made possible by inducing new features such as negative curvature core surround [284], then by fibre topologies with a single layer of non-touching tubes [285], and finally by the addition of small nested tubes - a design known as hollow core Nested Antiresonant Nodeless Fibre (HC-NANFs) [286]. HC-NANFs provide a solution for coexistence scheme as they do not only provide several attractive advantages compared to glass core fibres, such as reduced optical nonlinearity and ultra-lower latency, but also have the ability to reach a total loss value lower than that of conventional solid single-mode fibres [286]. These desirable qualities enable the transmission of classical channels at high optical powers while coexisting with quantum channels over the same medium [2]. The losses of HC-NANF have improved immensely from 1.3 dB/km [287] (used in this experiment), to 0.28 dB/km [288] and recently to 0.22 dB/km [289]. Finally, another design where an additional nested tube was added to each set of nested elements of a NANF called Double Nested Antiresonant Nodeless fibre (D-NANF) was reported in [290]. D-NANF achieved a loss of 0.174 dB/km comparable to that of SMF in the C-band and 0.22 dB/km which is better from the fundamental loss of SMF in the O-band.

In this section, we demonstrate the coexistence of a 16 dB power budget commercial DV-QKD system (Clavis^3 [152]) and 8 x 200 Gbps 16-QAM carrier-grade classical optical channels at an extremely high total coexistence power of 0 dBm over a 2 km HC-NANF, revealing minimal effects on the quantum channel performance. We then compare the QKD performance in terms of SKR and QBER for both the best and worst wavelength location for coexisting an 8-channels classical band with a fixed quantum channel in HC-NANF and SMF. The section is organised as follows: we first introduce the ID Quantique Clavis^3 [152] system followed by the the experimental system setup in Section 5.2.2. After that in Section 5.2.3, we present the results and is divided into three parts, optical spectrum for quantum/classical coexistence , quantum system characterisation, and coexistence analysis based on the quantum channel performance. Finally, we conclude the section by discussing the experiment outcome in Section 5.2.4.

5.2.1 The ID Quantique Clavis^3 Quantum Key Distribution System

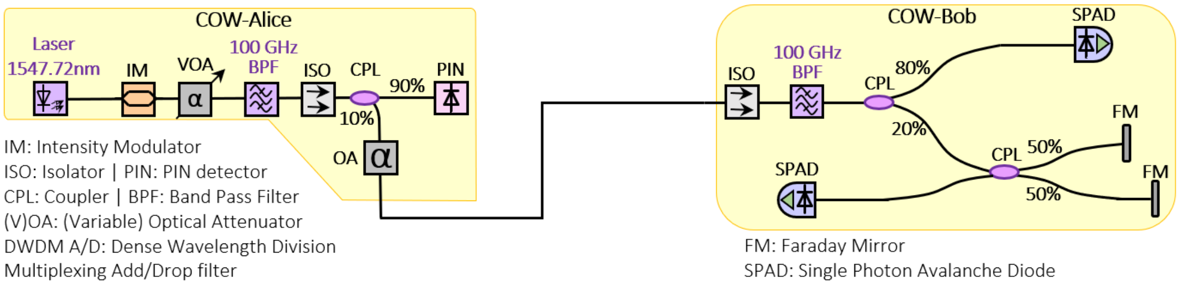

COW-Alice
Laser
1547.72nm
IM
VOA
100 GHz
BPF
ISO
CPL
90%
PIN
10%
OA
α
α
IM: Intensity Modulator
ISO: Isolator | PIN: PIN detector
CPL: Coupler | BPF: Band Pass Filter
(V)OA: (Variable) Optical Attenuator
DWDM A/D: Dense Wavelength Division
Multiplexing Add/Drop filter
COW-Bob
SPAD
ISO
100 GHz
BPF
CPL
80%
20%
FM
CPL
50%
50%
SPAD
FM
FM: Faraday Mirror
SPAD: Single Photon Avalanche Diode

Figure 5.8: Optical schematic for the ID Quantique Calvis^3 system [152].

At this point of my PhD journey, we bought the new ID Quantique Clavis^3 QKD system. Figure 5.8 shows a schematic overview of the ID Quantique Clavis^3 QKD system. The transmitter

(Alice) uses a continuous wave (CW) laser at a fixed wavelength (1547.72 nm), providing time-positioned weak coherent optical pulses with the aid of the intensity modulator (IM). The weak pulses are attenuated to the appropriated mean photon number value in multiple steps. The variable attenuator (VOA) is set based on the measured power at the output of the PIN monitoring detector at the 90% arm of the 90/10 coupler (CPL). The 10% output is connected to a fixed optical attenuator (OA) that attenuates the light signal to the required intensity level. The 100 GHz band pass filter (BPF) and the optical isolator (ISO) are included to protect the transmitter from back reflections and to prevent Trojan horse attacks [291].

The receiver (Bob) consists of two branches, the computational basis analyzer branch and the branch checking the phase relation. The branches are separated by a 80/20 coupler as shown in Figure 5.8. The computational basis analyzer is connected to the 80% arm and utilises a single-photon detector only. The second branch fed from the 20% output of the coupler, deploys an unbalanced Michelson interferometer with Faraday mirrors (FM) to compensate for any polarization variations. This compensation is crucial to maintain matching polarization modes of the two interferometer beams, which recombine in the 50/50 coupler. A single-photon detector is connected to the free output of the interferometer to check the phase relation between consecutive pulses. The optical isolator and 100 GHz band pass filter are deployed to limit the background noise effects on the detector and to prevent Trojan horse attacks.

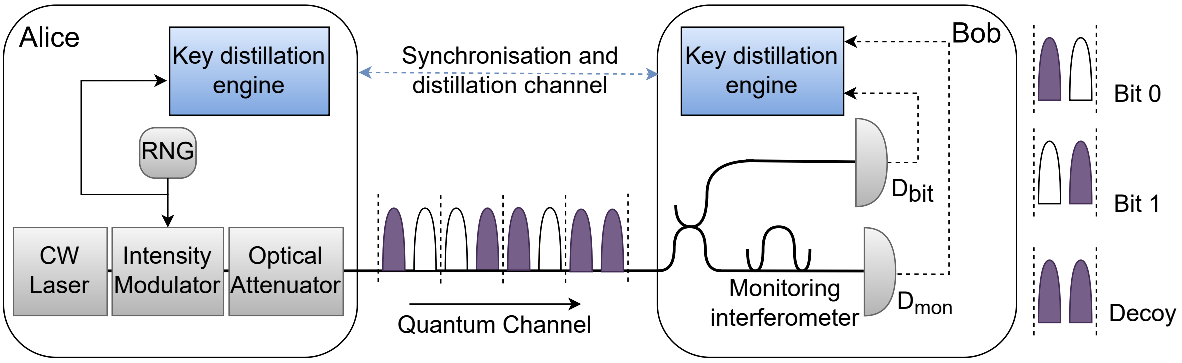


Figure 5.9: Illustration of COW protocol principle.

As shown in Figure 5.9, the COW protocol utilises weak optical coherent pulses and interferometers for detection. As the system is based on time-bin encoding of qubits and the coherent pulses are propagating in the same spatial mode and separated by a given time, the bases are measured by determining the time of the detection. If the detection occurs in the early time-bin, the qubit value is considered as $|0\rangle$ state, whereas if the qubit occurs in the late time-bin, it is considered a $|1\rangle$ state. One of the two qubit basis (the computational basis) is used to generate the raw keys and the other is used to estimate the security level of the exchanged qubits in the first basis. The security of the COW protocol is analysed by checking the coherence between two consecutive pulses using the interferometer at the receiver (Bob) station. Therefore, the transmitter (Alice) is required to generate the same phase relation between any two consecutive pulses. To further enhance the security of the COW protocol, a decoy-state - consisting of an early and a late optical pulse with the same energy level - is emitted from time to time. The phase between one of the pulses of the decoy state and the consecutive pulses must be identical to the phase between pulses of the computational basis to detect an eavesdropper. Finally, the decoy state and second basis analysis are used to estimate the security level of the raw key rate which is generated by the computational basis [101, 292].

5.2.2 Experimental System Testbed

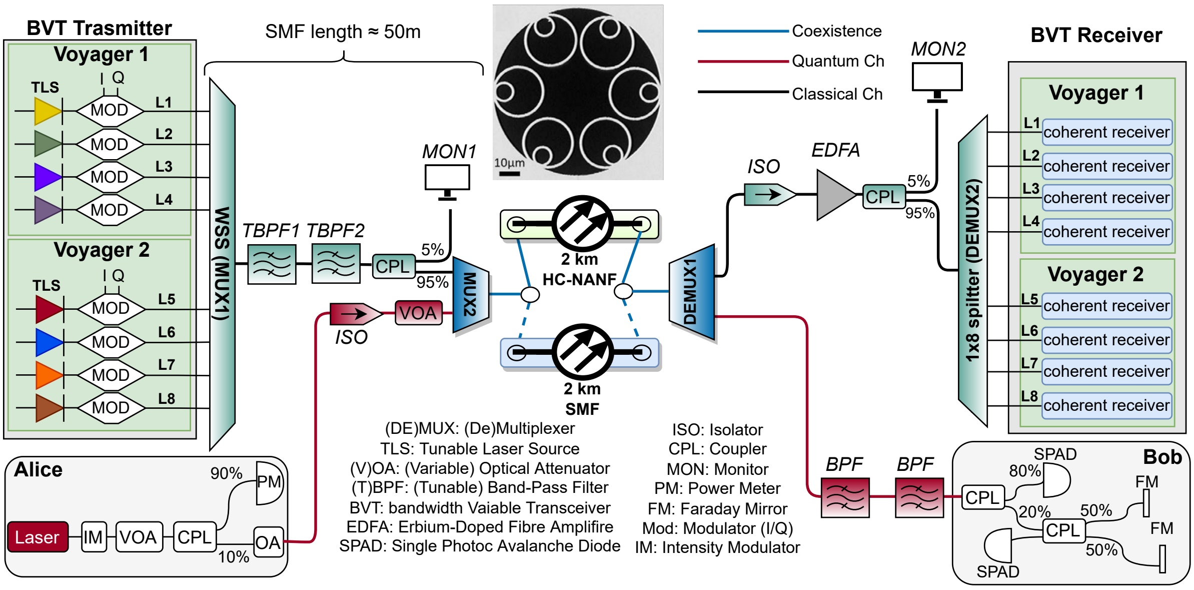


Figure 5.10: Experimental testbed for the coexistence of 1.6 Tbps classical channels and DV-QKD channel over 2 km HC-NANF and SMF. Inset: scanning electron micrograph (SEM) of the HC-NANF cross section.

Figure 5.10 shows the experimental system setup used to demonstrate the coexistence of eight classical channels with a DV-QKD channel over a 2 km-long HC-NANF and SMF (as inset figure, Figure 5.10 also illustrates the cross-sectional diagram of the HC-NANF used [287]). The testbed facilitates the experimental evaluation of the nonlinear effects on the performance of the quantum channel created by the presence of classical channels spectrally close to the quantum channel using both HC-NANF and SMF. For the classical channels, two optical packet DWDM platforms are used with bandwidth-variable transponders (BVTs) [199]. Since the HC-NANF has ultra-low optical nonlinearity, it allows the transmission of classical channels at extremely high power (over 0 dBm) with minimal effect on the quantum channel. Therefore for the HC-NANF since we are using high total coexistence power, all the ports were configured with the 16-QAM modulation for a maximum capacity of 200 Gbps per channel resulting in 1.6 Tbps

of transmission overall and the SD-FEC considered was 15% with a detector sensitivity of -26 dBm. As for the SMF, due to the nonlinear effects in this type of fibre the coexistence power was reduced compared to the HC-NANF case, and a substantially higher detector sensitivity is required to receive an error-free classical signal. Therefore, for the SMF a PM-QPSK modulation was used for a maximum capacity of 100 Gbps per channel resulting in 800 Gbs of transmission overall and the SD-FEC considered was 25% with a detector sensitivity of -35 dBm.
For the quantum channel, ID Quantique DV-QKD systems are used (Clavis^3 QKD Platform [152]). These systems are implemented to run with the COW protocol [292]. The aim of the COW protocol is to make the implementation of a QKD system as simple as possible using only two single photon detectors and to allow a significant increase (two-fold) in the final secret key rate. Moreover, in the Clavis3 system, Alice and Bob encode bits with quantum state carried by single photons (qubits) using time-bin encoding method by creating a pair of coherent pulses propagating in the same spatial mode and separated by a given time. The first pulse is called the early pulse and the second one is called the late pulse. Hence, the measurement method to analyse this basis is simply to measure the time of detection of the optical pulse. If one detection occurs in the early time-bin, the qubit value is a $|0\rangle$ state, whereas if it occurs in the late time-bin, the qubit is a $|1\rangle$ state.

As shown in Figure 5.10, the eight coherent output ports of the two BVTs are multiplexed using a wavelength selective switch (WSS) shown as MUX1 with 5 dB of insertion loss for a total throughput of 1.6 Tbps. The WSS is used as a multiplexer and a band pass filter to couple the classical channels into a single fibre and provide a 30 dB isolation. The WSS combined output is connected to the input port of a tunable band pass filter (TBPF1) with 60 dB of isolation and extremely sharp filter edges followed by a Gaussian shape tunable band pass filter (TBPF2) with 30 dB of isolation to further suppress the noise generated by the classical channels. The classical channels are then coupled to the quantum channel through a WDM multiplexer (DWDM add drop filter) MUX2 in a co-propagation coexisting configuration and travels through a 2 km of HC-NANF or SMF. After the coexistence within the selected fibre, the output is connected into a WDM demultiplexer tuned to 1547.72 nm (DEMUX1) that passes the quantum channel while rejecting all other channels (classical channels). After the WDM demultiplexer, the quantum signal is passed through a double stage filtering using two fixed WDM band pass filters centred at the quantum channel wavelength (1547.72 nm) to eliminate any noise generated by the classical channels. The output of the second filter is connected to the DV-QKD Bob unit, which undertakes the single-photon detection and processing of the encoded photons allowing the completion of the COW protocol of the DV-QKD systems. The output of the reflection port of the WDM demultiplexer is directed to an optical isolator with an insertion loss of 1 dB to prevent the tunable laser used by the BVT Rx as a local oscillator from returning to the Bob-QKD unit and interfering with the QKD measurements. It also prevents the Amplified Spontaneous Emission (ASE) noise generated by the Erbium-Doped Fibre Amplifier (EDFA) which is used

Table 5.1: Parameters for HC-NANF coexistence testbed

Parameters	Value
Classical Channels	
Number of Channels	8
Classical Channel Frequencies scenario 1	193.50 THz, 193.45 THz, 193.40 THz, 193.35 THz, 193.30 THz, 193.25 THz, 193.20 THz, 193.15 THz
Classical Channel Frequencies scenario 2	192.70 THz, 192.65 THz, 192.60 THz, 192.55 THz, 192.50 THz, 192.45 THz, 192.40 THz, 192.35 THz
Grid Spacing	50 GHz
Modulation Format	16-QAM
Optical Signal-to-Noise Ratio (OSNR)	20 dB
Transmission rate per channel	200 Gbps
Total transmission rate	1.6 Tbps
Pre-FEC Level	15%
Detector sensitivity*	-26 dBm
Quantum Channel	
DV-QKD Wavelength	1547.72 nm
DV-QKD Frequency	193.70 THz
QKD Protocol	COW
Maximum Loss	16 dB
Optical Band Pass/Rejection Filter (OBRF)	
Insertion loss band pass port	0.5 dB
Center wavelength band pass port	1547.72 nm
Bandwidth band pass port	100 GHz

**Corresponding to 16-QAM Modulation @200 Gbps and back-to-back.*

to set the classical signals to suitable detectable power levels before demultiplexing via a 1x8 splitter. Furthermore, an optical isolator is used after the Alice-QKD unit to prevent the noise generated from the classical channels from returning to the Alice-QKD unit and interfering with the quantum signal. After the optical isolator at the Alice side, a variable optical attenuator (VOA) is used to adjust the losses of the quantum channel to the minimum operational level of 10 dB to optimise the functionality of the Clavis3 QKD system and to prevent over-saturating the single photon detector in the Bob-QKD unit. It also allows us to obtain a direct comparison of the quantum/classical coexistence between the SMF and HC-NANF in terms of losses. In this testbed, the total end-to-end (Alice to Bob) quantum channel loss is 10.5 dB. A summary of the main parameters of the testbed is shown in Table 5.1.

5.2.3 Results

5.2.3.1 Optical Spectrum of Quantum and Classical Channels

Figure 5.11 shows the spectrum of 8 × 200 Gbps classical channels coexisting with a quantum channel obtained by using a tap coupler as shown in Figure 5.10 *MON1 & MON2* for the best and worst case scenarios. Figure 5.11 also demonstrates the optical filters profile (pink) of the tunable band pass filters *(TBPF1 & TBPF2)* used to filter out the noise generated by the classical channel. It also shows the optical filter profile of the band pass filter *(BPF)* used before the Bob-QKD unit (red) to suppress the nonlinear effects from passing to the QKD detectors. The filter profiles were generated by using the output of an EDFA as a noise source. Furthermore, the spectrum of the eight classical channels after the filtering (black) MON1 and the amplification stage (blue) MON2 is shown before demultiplexing and coherent detection at the BVT receiver.

5.2.3.2 Co-propagation of Quantum and Classical Channel Coexistence without Fibre - System Characterisation

To investigate the performance of the filtering stages in our system, we implemented the best-case scenario (1.6 nm spacing) using the same coexistence scheme in Figure 5.10 without using fibres; hence removing the nonlinear effects caused by the 2 km HC-NANF/SMF and the 2 m SMF pigtails of the HC-NANF from the system. Since no fibres are used, the degradation in the quantum channel performance is mainly due to the nonlinear effects generated in the ≈ 50 m of SMF between the BVT Tx and MUX2 in Figure 5.10 causing photon leakage to the Bob-QKD unit from filtering deficiencies. As shown in Figure 5.12, the average SKR stays within the expected range between 2100-2300 bps for a total coexistence power of -12 dBm which is higher than the maximum total coexistence power of -24 dBm used in SMF verifying that the degradation in the SMF fibre as shown in Figure 5.13 (b) and Figure 5.14 (b)is mostly due to nonlinear effects i.e. Raman scattering from the 2 km SMF. This comparison is to demonstrate the effectiveness of the filtering stages in preventing photon leakage to the Bob QKD-unit for the power levels which were used in SMF. Moreover, the 1,2,4 and 8 channels symbols shown in Figure 5.12, correspond to the number of channels and their aggregated power. For example, 2 channels at -9 dBm correspond to a power of -12 dBm per channel, 4 channels at -9 dBm correspond to a power of -15 dBm per channel, and finally 8 channels at -9 dBm correspond to a power of -18 dBm per channel.

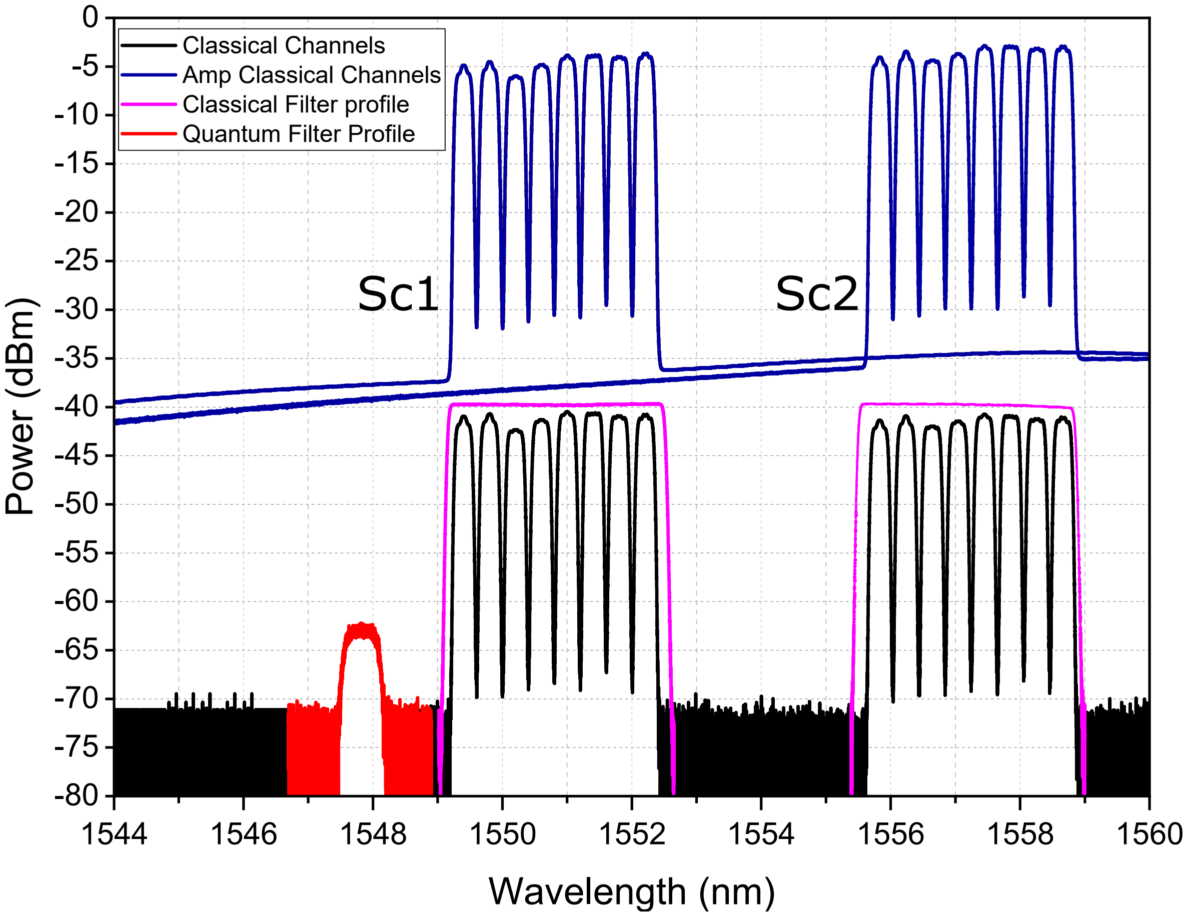


Figure 5.11: Spectrum of the combined transmission of quantum and classical channels with optical filter profiles of both scenarios.

5.2.3.3 Co-propagation of Quantum and Classical Channel Coexistence over HC-NANF and SMF with different Coexistence Power and Channels Spacing

Figure 5.13 and Figure 5.14 show the experimental evaluation of SKR and QBER of the quantum channel with different spectral spacing between the classical and quantum channels based on the calculation in Section Section 4.2. For a spacing of 1.6 nm (200 GHz) in SMF (the best case scenarios for SMF considering both Raman scattering and FWM), Figure 5.13 (b) and Figure 5.13 (d) show that the SKR value drops from ≈ 2300 bps to ≈ 600 bps while the QBER values increase from ≈ 3% to ≈ 4.2% when coexisting 8 classical channels at a total coexistence power of -24 dBm. This significant 73% drop in the SKR and 40% rise in the QBER is due to high optical nonlinearity in SMF, such as Raman scattering and FWM, causing a high noise leakage to the Bob-QKD unit and affecting the QKD performance.

Using the same spacing of 1.6 nm in HC-NANF, Figure 5.13 (a) and Figure 5.13 (c) show that, the SKR ≈ 2300 bps and QBER ≈ 2.5% values without the presence of any classical

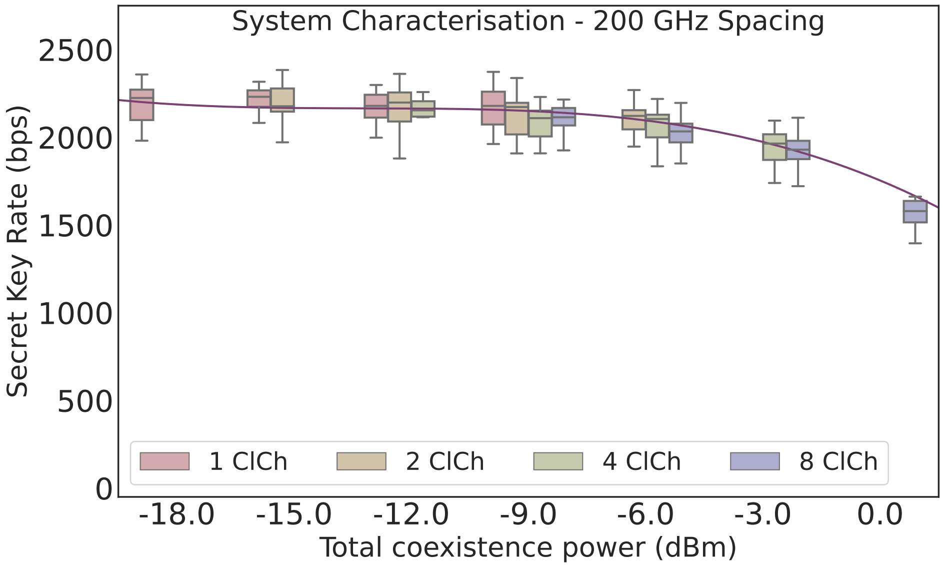


Figure 5.12: Average SKR versus total coexistence power without fibre - system characterisation at 200 GHz spacing.

channel (no coexistence) are similar to the values when coexisting 8 classical channels at a total coexistence power of 0 dBm. This is due to the ultra-low optical nonlinearity in HC-NANF. Moreover, the QKD performance of Figure 5.13 (a) is in good agreement with Figure 5.12 at -7 dBm coexistence power which matches the loss of the HC-NANF.

For a spacing of 8 nm (1 THz) in SMF (the worst case scenarios for SMF considering Raman scattering and FWM) and using the same coexistence power of -24 dBm, the SKR drops to zero as the QBER exceeds the operational threshold of 5.2% of the QKD as shown in Figure 5.14 (b) and Figure 5.14 (d). This is because the 8 nm spacing between the quantum and classical channels resulted in the peak of the Raman scattering spectrum to be located within the bandwidth of the BPF filter used to filter the quantum channel; hence the system stops generating keys due to excessive noise leakage over the quantum channel.

With the same spacing of 8 nm and coexistence power of 0 dBm in HC-NANF, Figure 5.14 (a) and Figure 5.14 (c) show that, the SKR drops from ≈ 2300 bps to ≈ 2050 bps while the QBER values increase from ≈ 2.2% to ≈ 3.1% using HC-NANF. This 10% drop in the SKR and 40% rise in the QBER is only due to the excessive Raman scattering noise generated in the ≈ 50 m SMF between the BVT Tx and MUX2 in Figure 5.10 and the 2 m SMF pigtails caused by placing the quantum channel in the Raman spectrum peak.

In both scenarios, the back-to-back losses of the quantum channel is similar when using both SMF and HC-NANF (10.5 dB) and the highest coexistence power (0 dBm) in the HC-NANF is 250 times higher than the highest coexistence power (-24 dBm) in SMF. Even though the

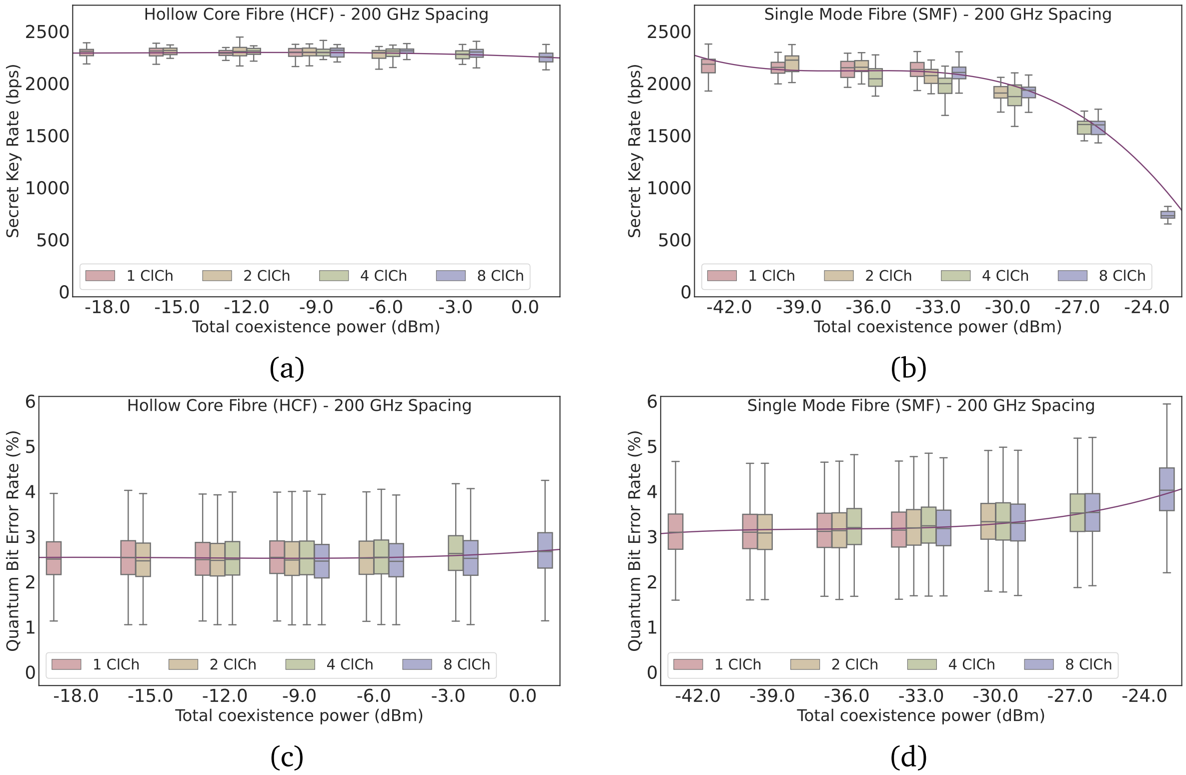
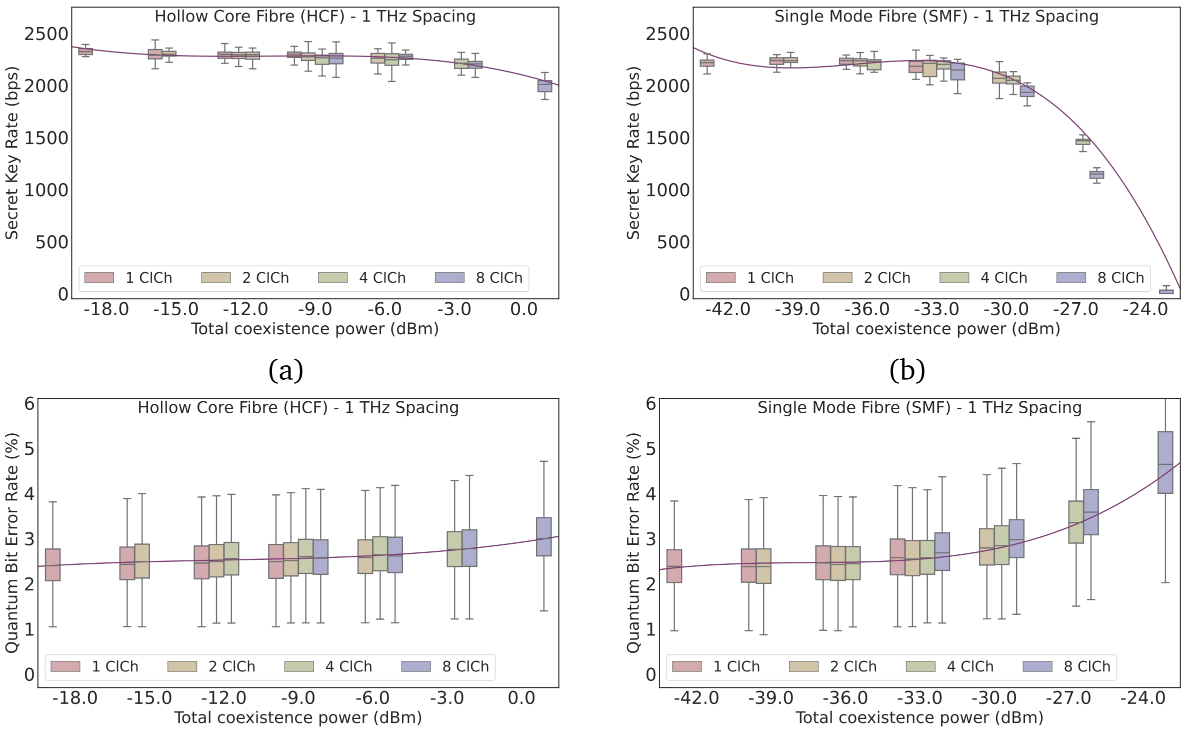


Figure 5.13: a) Average SKR versus total coexistence power using HC-NANF. b) Average SKR versus total coexistence power using SMF. c) Average QBER versus total coexistence power using HC-NANF. d) Average QBER versus total coexistence power using SMF. 200 GHz spacing between quantum and classical channels. The solid lines in the figures are trend-line fit.

coexistence power is much higher is HC-NANF, the ultra-low nonlinear effects due to its hollow core preserve or have a slight effect on the SKR and QBER of the quantum channel. This proves the suitability of HC-NANF as an excellent transmission medium for high power coexistence of quantum and classical channels.

5.2.4 Summary

The coexistence of a DV-QKD channel and 8 × 200 Gbps 16-QAM classical channels was successfully demonstrated over a 2-km long Hollow Core Nested Antiresonant Nodeless Fibre for a record-high coexistence transmission of 1.6 Tbps. In the best case scenario with 1.6 nm spacing between the quantum and classical channels (200 GHz) at -24 dBm total coexistence power in SMF, the SKR dropped by 73%, whereas, at 0 dBm total coexistence power in HC-NANF (250 times higher than the power used in SMF), the SKR was preserved. In the worst case scenario 8 nm spacing between the quantum and classical channels (1 THz - Raman spectrum peak at the quantum channel wavelength) and using the same powers, the SKR dropped to 0 bps in SMF meaning no keys were generated, whereas in HC-NANF the SKR dropped only



(a) (b)

(c) (d)

Figure 5.14: a) Average SKR versus total coexistence power using HC-NANF. b) Average SKR versus total coexistence power using SMF. c) Average QBER versus total coexistence power using HC-NANF. d) Average QBER versus total coexistence power using SMF. 1 THz spacing between quantum and classical channels. The solid lines in the figures are trend-line fit.

by 10% due to the Raman scattering generated from the ≈ 50 m SMF in the testbed before the coexistence point (MUX2) and the 2 m SMF pigtails of the HC-NANF. This significant difference in the QKD performance proves the advantage of using HC-NANF to provide a seamless coexistence of quantum and classical channels for future quantum networks with a minimal effect on the quantum channel performance regardless of the number and power of the classical channels. The HC-NANF also provides higher transmission speed (50% faster) and low latency compared to SMF. For this reason, a 7 km HC-NANF was deployed to connect an Interxion data centre and The London Stock Exchange [293]. It also provides thermal and phase stability, making it suitable for long-distance transmission using protocols such as twin-field QKD [7]. However, in the meantime, HCF is expensive to manufacture and install and could be used as a viable solution for specific use cases only.

5.3 Bidirectional coexistence of DV-QKD and 25 C+L Band Classical Channels over 7.7 km HC-NANF

Using a 7.7 km HC-NANF, we implemented a bidirectional coexistence link with 25 classical channels with an aggregated power of 12 dBm, 12 times more than the power presented in the previous experiment in Section 5.2. An overview of the state of the art investigations into the coexistence of QKD and classical links Figure 5.15 reveals that the best approaches to coexist quantum channels and high power classical channels is by using CV-QKD (■) systems [217] or using two different bands (C and O band) for the classical and quantum channels (○). However, CV-QKD is not suited for secure key generation over large distances and the higher O-band fibre losses likewise limit achievable distances as discussed in the previous section. Our previous findings [2] suggest a third option, employing a hollow-core fibre (HCF). In this experiment, we demonstrate the coexistence operation of a custom built DV-QKD system (C+L-band) for the QKD and the Sync channels, implementing the COW protocol, together with 25 classical data channels (C+L-band), of which one is counter-propagating to the QKD signal, over a single metro-scale HCF link. The reduced Raman scattering of HCF compared to SMF allows to push the coexistence limit as high as 12 dBm aggregated power while imposing no restriction on the spectral layout of quantum and classical carriers. This corresponds to a 9 dB improvement in coexisting classical power while at the same time increasing the number of co-propagating channels by a factor of 2.5 for similar in-band DV systems Figure 5.15.

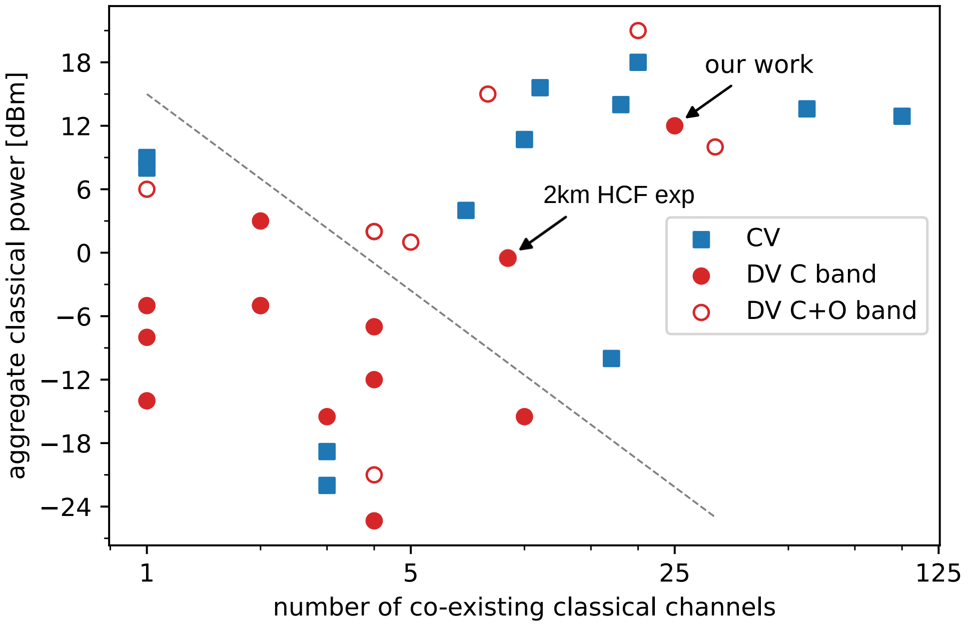


Figure 5.15: State of the art of coexistence experiments.

5.3.1 Quantum Channel Allocation and Robustness to Raman Noise

Ax explained before, When coexisting classical and quantum channels over the same fibre, in-band Raman noise is inevitable. Figure 5.16 evidences the broadband nature of spontaneous Raman scattering (SpRS) for a standard single-mode fibre (SMF) and HCF conducted with a classical and single-photon (*hν*) OSA. Measurements for a 1550-nm pump channel at 10 dBm show that its SpRS tails reach till the O-band, where the noise contribution eventually falls below 105 photons/s/100pm (Λ), a value that makes it compatible with QKD [212, 225]. To overcome this impairment in the C+L bands, this experiment builds on initial findings of the previous experiment [2]. We used a 7.7 km long HCF sample with SMF28 pigtails, described in detail in [294]. As reported in Figure 5.16, the SpRS of the HCF decreases by ≈35 dB with respect to the SMF. This allows us to explore a wide region of low Raman noise in the C-band, a band that had been predominantly used with a limited number of artificially attenuated classical channels located very close to the DV quantum channel [213] (■ in Figure 5.15) to ensure a small spectral detuning with a weak Raman noise contribution (Δ). Although this region was explored in the previous experiment with an 8 nm spacing, in this experiment we have 25 classical channels in both the C and L bands.

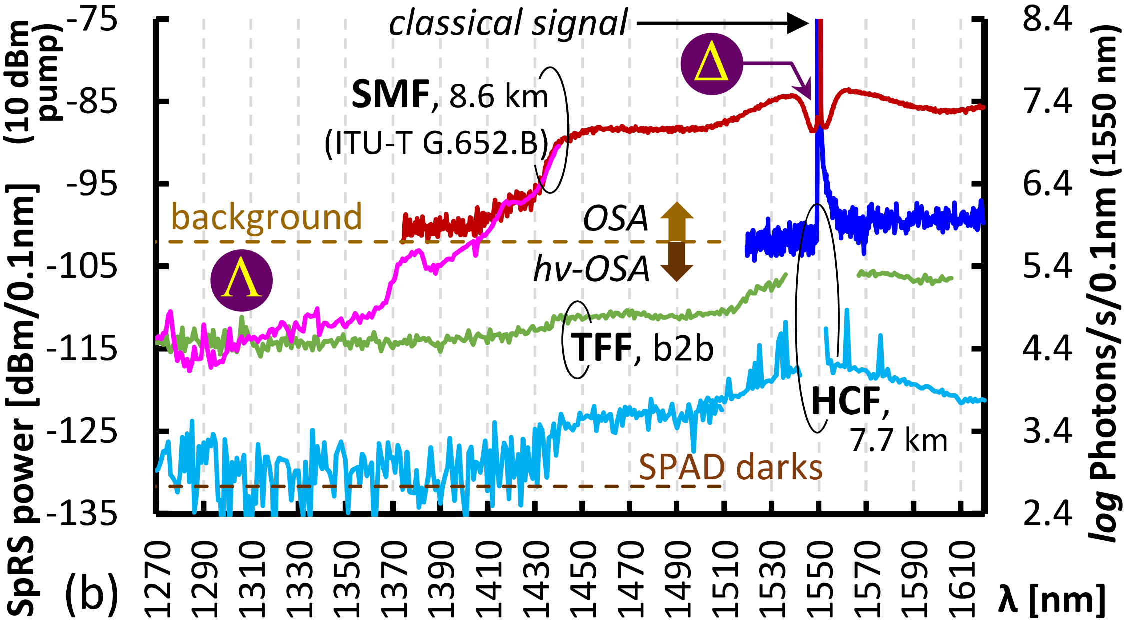


Figure 5.16: Spontaneous Raman scattering spectra of SMF and HCF.

5.3.2 Experimental System Testbed

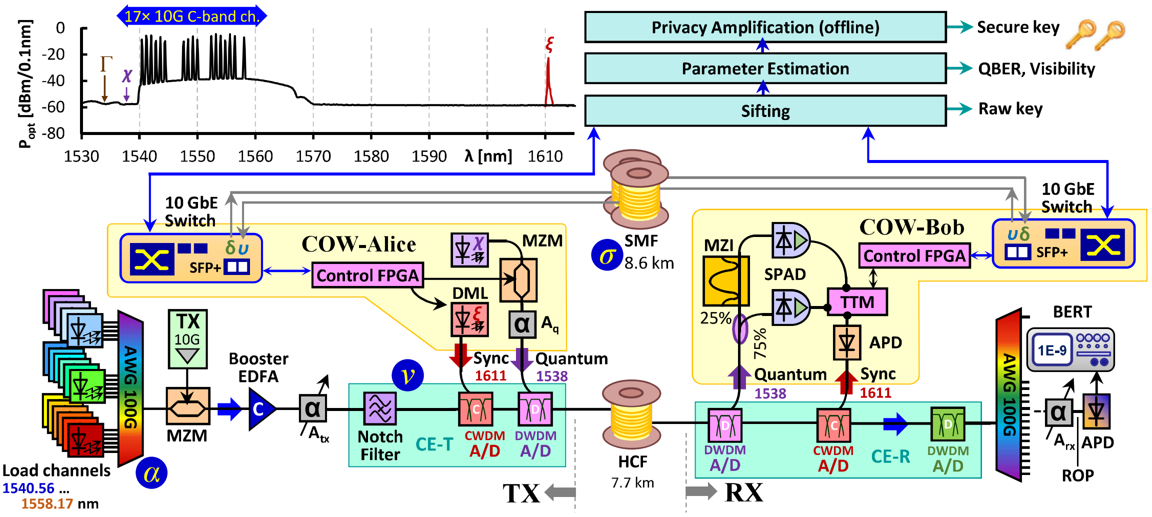


Figure 5.17: Experimental setup for joint, bidirectional classical/quantum C+L band transmission. The spectral inset presents the transmitted spectrum.

Figure 5.17 presents the experimental setup. The QKD engine implements the coherent one-way (COW) protocol [101] with the QKD channel (C-band: 1538 nm (χ)) multiplexed with a classical synchronization channel (L-band: 1611 nm (ξ)) and SFP+ modules in down- (δ, 1554.94 nm) and uplink (υ, 1552.52 nm) direction for bi-directional classical communication of the QKD transmitter and receiver. Alice's FPGA, addressable via Transmission Control Protocol (TCP) using 10 GbE switch from her control PC, streams the buffered modulation data in a burst fashion, divided into frames of configurable length and duty cycle. Each frame is accompanied by a classical sync pulse, acting as a local time reference for the coherent train that has been attenuated to the quantum level. The QKD receiver employs two free-running SPADs (10% efficiency, dark count rate of 620 Hz) to determine either the time of arrival (75% branch) or the phase between consecutive pulses (25% branch). The raw key can then be forwarded to the respective post-processing software modules, running as separate services, on the PCs, in order to finally arrive at a secure key. All communication between the two parties is optically routed through the 7.7 km@HCF (8.8 dB loss) with SMF pigtails.

The link load consists of 25 intensity-modulated channels in the C- and L-band (see inset in Figure 5.17), carrying 10 Gbps PRBS data and being boosted by a tandem of 20-dBm C/L-band EDFAs. Coexistence with QKD necessitates spectral conditioning for the classical signal spectrum. This includes (i) filtering of the ASE tails of laser line, accomplished through the arrayed waveguide grating (AWG, α) used to multiplex the optical sources (or through a band pass filter in case of the 10GbE uplink, β) and (ii) suppression of the ASE of the EDFA through a notch filter with a rejection of >95 dB (Figure 5.18, υ), cleaning out the quantum channel at 1538 nm. An attenuator A_{tx} was used to control the launch power of the classical channels to investigate the coexistence limits. The quantum signal and the corresponding frame sync at 1611 nm are lastly multiplexed to the classical signal compound using a CWDM and a DWDM passive filters. This ensures minimal multiplexing losses of 0.76 dB for the fragile quantum signal (Figure 5.18, χ), while the notching and express feed-through of the classical channels at the transmitter-side Coexistence element (CE-T) amount to 6.3 dB (ι). It shall be stressed that the notch at the quantum channel χ is not visible in Figure 5.17 due to additional scattering arising at the OSA grating (Γ). At the receiving end of the link, a Coexistence element (CE-R) first drops the quantum and QKD sync channels using a similar CWDM and a DWDM passive filters before realizing the directional split for the classical channels (Figure 5.18). The downlink has been demultiplexed and received by an APD receiver in order to prove the quality of signal reception through BER measurements (A_{rx}) as a function of the received optical power (ROP).

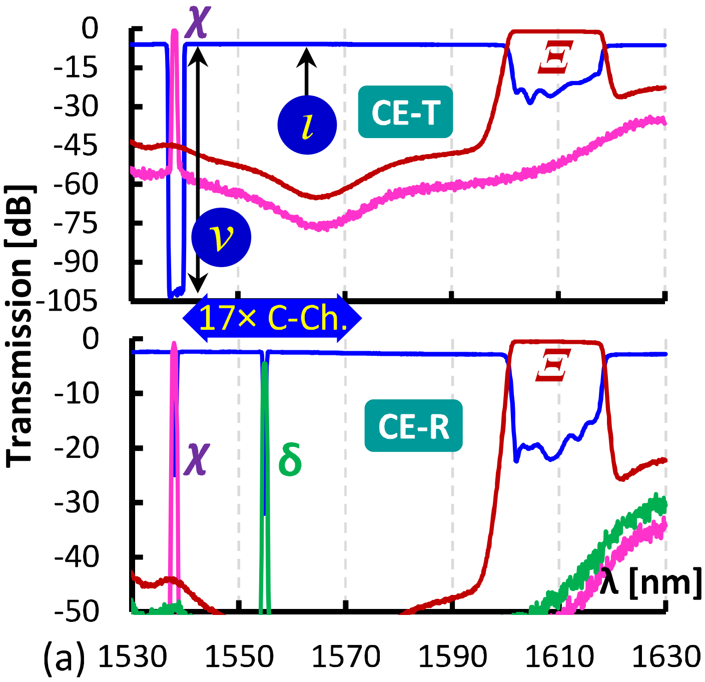


Figure 5.18: Coexistence elements at transmitter and receiver with notch (υ) for the quantum channel (χ) and add/drop for QKD sync (Ξ).

5.3.3 Results

5.3.3.1 Secure-key rate under presence of 17 classical channels (Only C-Band)

As shown in Figure 5.19, the SKR has been evaluated as a function of the aggregated classical power and channel count at the C-band only. As shown in the previous experiment, the

SKR depends on the spectral layout of the classical channels in SMF because the Raman scattering profile varies with respect to their position. However due to the low and flat Raman scattering profile of the HCF in Figure 5.16, the SKR performance is primarily determined by the aggregated classical power making the SKR widely independent of the spectral layout. As shown in Figure 5.19, a SKR of 65 bps can still be obtained for 17 classical channels aggregating 11 dBm (ψ) spanning over 17.6 nm of the C-band fibre spectrum. This proves the robustness of DV-QKD in combination with the HCF. We noticed a low background noise even for a back-to-back configuration without HCF, which was eventually identified to originate from scattering at SMF-pigtailed thin-film filters (TFF) employed at the CE-T element ((TFF) in Figure 5.16). This imposes an upper bound for the compatible launch power. The SKR expands to 1.2 kbps (κ) for a weaker launch power of 8 dBm (half the used power to obtain 65 bps), leading to a QBER of 1.2%. Using only the closest six C-band classical channels with a weaker classical signal launch of -1 dBm, we achieved a SKR 3.1 kbps (τ), and a low QBER of 0.67%. The drop in SKR from 1.5 to 2 kbps without classical channels (ε in Figure 5.19) is due to contamination the quantum channel from the elevated ASE background under no-load conditions for the booster EDFA.

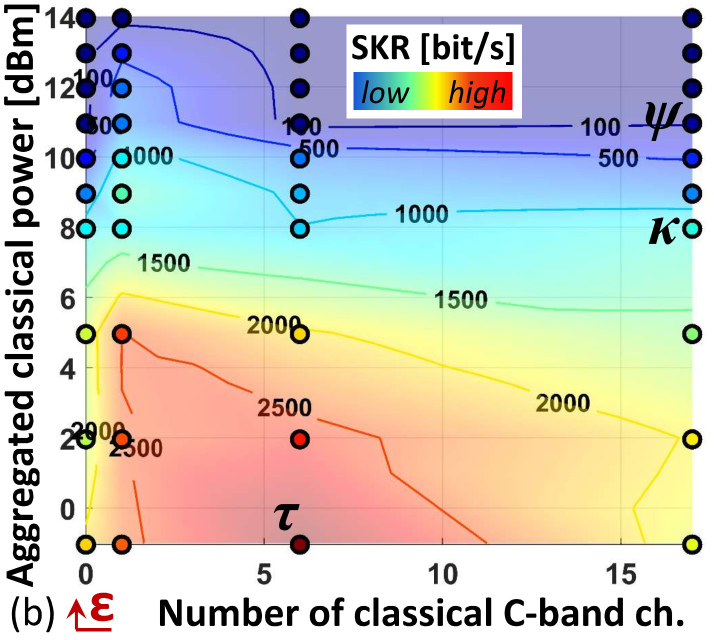
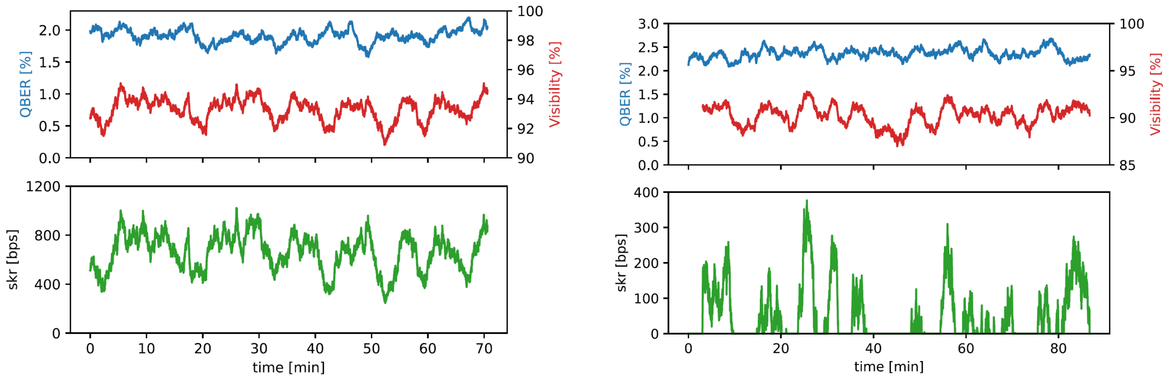


Figure 5.19: SKR under presence of 17 classical channels.

5.3.3.2 Secure-key rate under presence of 25 classical channels (C+L Band)

Figure 5.20 a) and Figure 5.20 b) showcase the long-term performance of the QKD engine for 9 and 12 dBm aggregated power of the coexisting classical channels respectively. The setup was tested for various combinations between the number and aggregated power classical channels. When all classical channels are used the coexistence limit was found around 12 dBm, at which point the QKD engine cannot guarantee continuous distillation of secure key any longer. However, the achieved SKR is still on the order of 100 bps, which would be enough to secure the classical link capacity of 25×10 Gbps, considering the NIST recommendation for AES key renewal mentioned above. A lower classical launch power of 9 dBm allows for continuous operation with a stable QBER and visibility of 1.91% and 93.3% , respectively, resulting in an average SKR of 660 bps. The still relatively high QBER at these operational conditions is mainly caused by the back scattering of the uplink into the receiver QKD receiver, via the interface given by the HCF/SMF pigtail. Routing the SFPs via a dedicated separate fibre, showcases the intrinsically low QBER of the QKD engine (0.67% at 9 dBm aggregated classical power). Finally, we acquired the BER performance of the classical channels.



(a)

(b)

Figure 5.20: a) Long term performance of QKD engine at 9 dBm power of classical channels, b)Coexistence limit of QKD engine at 12 dBm power of classical channels

Figure 5.21, showing a sensitivity better than -23.6 dBm at a BER of 10^{-10} and a spread of 2.5 dB between best and worst channel. All eye diagrams were clearly open.

5.3.4 Summary

We have demonstrated for the first time a secure-key generation at a 1538-nm quantum channel, integrating synchronization and key distillation in co-propagation with a C+L band DWDM feed from 1540.56 to 1598.89 nm. We obtained a SKR of 330 bps for an aggregated classical power of 12 dBm. This corresponds to a massive 31 dB increase in terms of classical power × optical bandwidth product compared to earlier DV-QKD works and enables its integration in high capacity, long-range metro-core links. The mitigation of Raman scattering in SMF spans, as accomplished using a novel HCF, now points to the need for upgrading fibre-optic components as well: We found thin-film add/drop multiplexers combining quantum and 90 dB stronger classical signals to prevent further scaling in terms of higher SKR and stronger classical launch,

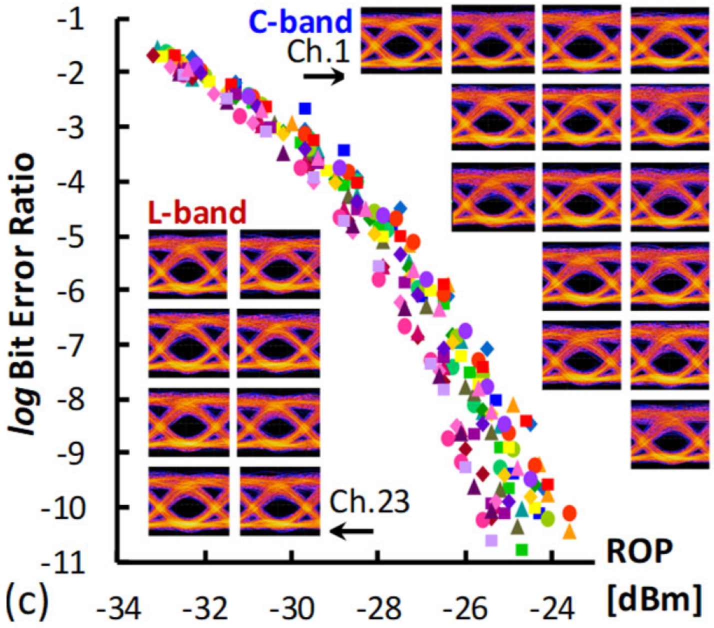


Figure 5.21: BER and eye diagrams for all PRBS channels.

unless WDM components with hollow-core layout become available. Together with sub-DWDM filtering at the quantum channel, we expect classical levels beyond 20 dBm to be compatible.

5.4 Coexistence of Quantum and Classical Channels over Free Space via Fibre-Wireless-Fibre Terminal

QKD in free-space applications has been demonstrated with indoor handheld devices [239, 240] and outdoor drones [295, 296]. Recently, the first lab demonstration of a 2 m free-space transmission of the COW protocol was published [297]. The QKD system operates in the visible spectrum (852 nm) with a fixed channel loss of 16 dB over a transmission distance of 2 m. Free-space QKD systems are typically used over long distances i.e. ground station to satellite, but the increasing demand for secure in-building connectivity makes short-range free-space QKD attractive. Such short-range links can be achieved by using Fibre-Wireless-Fibre (FWF) terminals [241–245] combined with fibre-based QKD systems. Ultra-high data-rate classical links have been achieved using FWF techniques, and the addition of a QKD channel might offer ultra-high rate data communications with the additional security that QKD brings. In this case the impairments are different from all-fibre based systems. Free-space has no nonlinearity at the power levels used, but impairments due to ambient light being detected must be considered [298]. In addition effects due to turbulence need to be assessed [297]. There has been some modelling to suggest that this FWF approach can support indoor QKD systems on their own [299] and in coexistence with classical communication channels [300]. However, experimental data are lacking and experimental characterisation is required.

This section is organised as follows: Section 5.4.1 describes the design and typical performance of the compact FWF terminals. Section 5.4.2 explains the experimental testbed. Experimental results on the coexistence of QKD and classical communication channels are detailed in Section 5.4.3. Finally, conclusions and use cases are presented in Section 5.4.3.

5.4.1 FWF Terminals

The challenge for any FWF systems is maintaining link alignment with high tolerance. For a system that uses single-mode fibre with typical commercial collimators the beam divergence/acceptance angles are ≈ 0.05 degrees, so any system must maintain alignment to these type of tolerance. Systems that use beacon based tracking [151, 301–304] and tracking that uses the communications signal [241, 242, 305] have been demonstrated. In this section a simplified version of such beacon signals will be used to drive the compact FWF terminals [244].

Figure 5.22 shows a schematic of the FWF terminals as described in [244]. Light from single-mode fibre (SMF) is fed into the terminals and collimated (Col1 & Col2) before being actively steered using fast steering mirrors (M1 & M2). These dual-axis steering mirrors allow for beam steering with up to ± 50° optical deflection per axis and a steering resolution of less than 5 μrad. The tracking system controlling M1 & M2 uses IR Tags operating at 800 nm and 890 nm as well as a set of cameras. The IR-Tags provide localisation beacons, represented by red and blue lines in Figure 5.22, respectively. Dichroic beam splitters (DF1 & DF2) separate

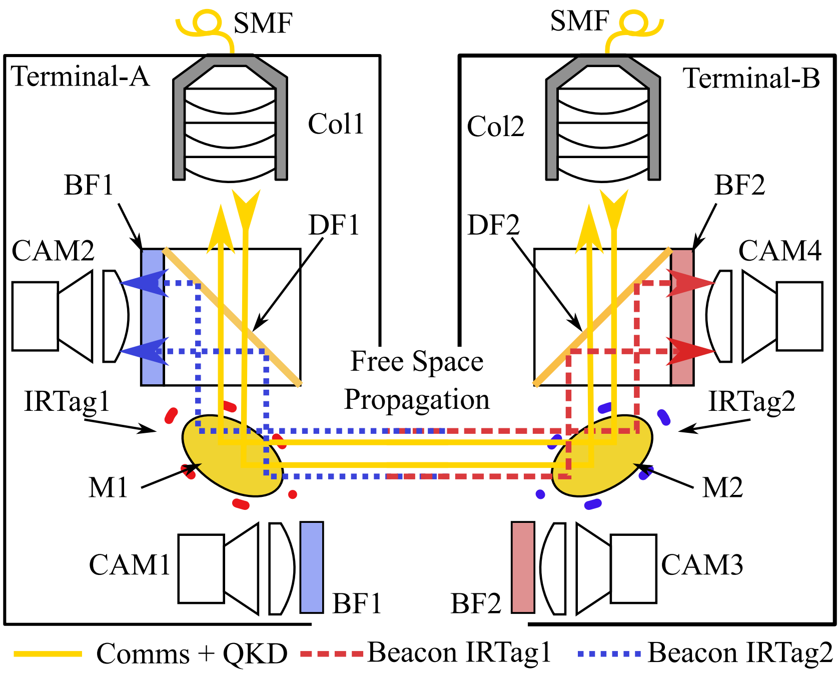


Figure 5.22: Schematic of the FWF terminals.

the localisation beacon light from the combined communication channels. Cameras CAM1 & CAM3 were set up with a wide field of view (FoV) which allows for locating the other terminal, while the cameras (CAM2 & CAM4) have a narrow FoV allowing for high precision tracking. Optical band pass filters (BF1 & BF2) in front of each camera reject ambient light to enable reliable localisation and tracking of the terminals. The latency of the tracking system supports communications between nomadic operations [244].

The tracking performance of the FWF terminal system was characterised, and shown to achieve a tracking resolution of 0.021° horizontally and 0.014° vertically all within a tracking latency of 216 ms. In operation the FWF system supported WDM channels transmitting data at ≥ 1 Tbps transmission rates for nomadic operation [245]. Wavelengths across the O and C band can be transmitted simultaneously [306].

There are two main contributors to the overall insertion loss of the FWF terminal system: (i) geometric loss L_{geo} and (ii) coupling loss induced by angular misalignment L_{ϕ}. The geometric loss scales with distance between the terminals as the collection area of the optical receiver remains constant whereas the divergence of the transmitted beam causes the illuminated area to grow with distance. The geometric loss can be expressed in dB by Eq. (5.1) [307].

$$L_{geo} = -10 \log \left[\frac{4\omega_T^2 \omega_R^2}{\frac{\lambda^2 Z_0^2}{\pi^2 n^2} + (\omega_T^2 + \omega_R^2)^2} \right] \tag{5.1}$$

where n represents the refractive medium between the two collimators ($n = 1$ is assumed in all calculations presented in this section), λ the wavelength of light in vacuum, Z_0 is the distance between the two collimators and ω_R and ω_T are the Gaussian beam radii of the receiver collimator and transmitter collimator, respectively.

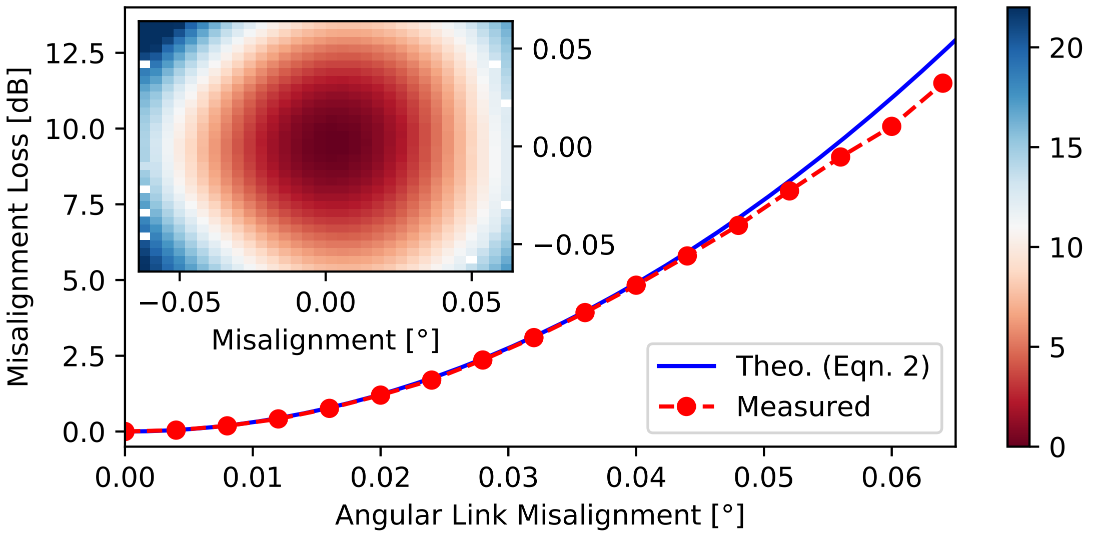


Figure 5.23: Average of measured misalignment losses gathered from the inset and a theoretically estimated loss based on Eqn. (5.2). The inset shows the measured misalignment loss as a function of horizontal and vertical steering angles.

Angular misalignment causes coupling losses due to the limited area in which light is guided in fibres as well as due to the limited acceptance angle of fibres. The angular misalignment loss in dB is given in Eqn. (5.2) [307]

$$L_\phi = \frac{20}{\ln 10} \frac{\left(\frac{n\pi\omega_R}{\lambda}\right)^2 \left[\left(\frac{\lambda Z_0}{\pi n \omega_T^2}\right)^2 + \left(\frac{\omega_R}{\omega_T}\right)^2 + 1\right]}{\left(\frac{\lambda Z_0}{\pi n \omega_T^2}\right)^2 + \left[\left(\frac{\omega_R}{\omega_T}\right)^2 + 1\right]^2} \sin^2\phi, \tag{5.2}$$

where ϕ the angular misalignment between the optical axis of transmitter and receiver collimator. Figure 5.23 shows the measured and theoretical misalignment loss for the FWF terminals with a 2.5 m wireless link. The measurement data were obtained by intentionally steering the receiving terminal off-axis and averaging over both axes with the same angular misalignment relative to the aligned position. Figure 5.23 illustrates good agreement between the theoretical estimation and the measured data.

5.4.2 Experimental System Testbed

Figure 5.24 illustrates the experimental system setup used to demonstrate the coexistence of eight classical channels with a DV-QKD channel over a 2.5 m free space enabled by a FWF terminal system. For the classical channels, two optical DWDM platforms are used with

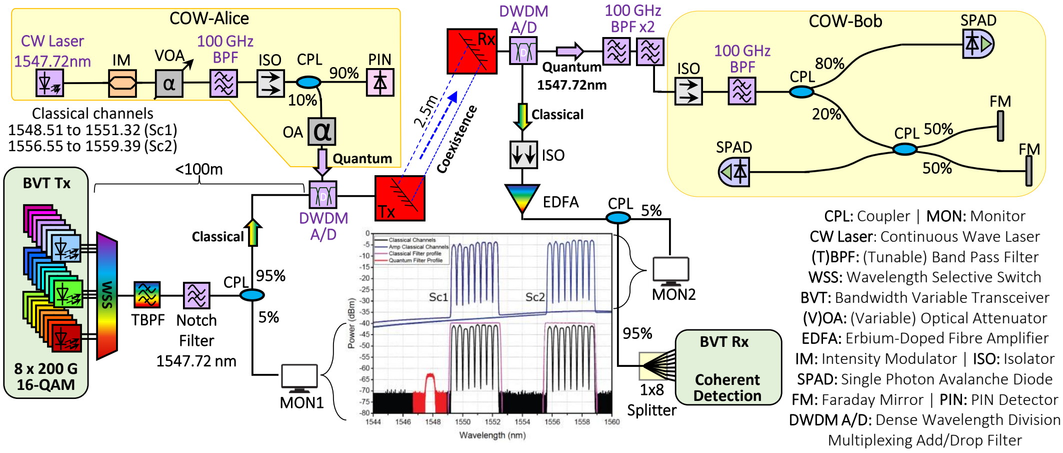


Figure 5.24: Experimental testbed. Inset: Spectrum of the combined transmission of quantum and classical channels with optical filter profiles of both scenarios.

bandwidth-variable transponders (BVTs) [199]. Each of these units include four BVT ports and each port can be tuned to any wavelength in the C-band according to the ITU-T 50 GHz grid. All 8 ports of the BVT were configured with a 16-QAM modulation for a transmission rate of 200 Gbps per channel resulting in 1.6 Tbps of transmission overall. Soft-decision forward error correction (SD-FEC) allowed a 15% error with a detector sensitivity of -23 dBm. Finally, all the ports were configured to match a total power of 0 dBm at the output of the FWF Tx terminal to meet eye safety regulations [308].

As shown in Figure 5.24, the eight coherent output ports of the BVT are multiplexed using a wavelength selective switch (WSS) which includes a band pass filter (BPF) with 30 dB of isolation. Subsequently, the wavelength accumulated signal is filtered. First, by a tuneable band pass filter (TBPF) with a flat-top and sharp filter edges (pink profile in the lower trace of the inset Figure 5.24) with a high isolation of 60 dB. Second, a notch filter was deployed to further suppress the noise level at the quantum channel wavelength (1547.72 nm). The filtered signal can be monitored in-situ via a 95/5 coupler (black channels in the inset Figure 5.24). The 95% output port of the coupler feeds into a DWDM add/drop (A/D) filter combining the quantum and classical channels which are subsequently fed into the FWF Tx terminal. After a 2.5 m free-space transmission another DWDM add/drop filter is deployed passing the quantum channel through a double stage filtering using two fixed WDM band pass filters (red profile in the lower trace inset Figure 5.24) to eliminate any noise generated by the classical channels and supress ambient light. The output of the filter pack is connected to the Bob-QKD unit. The classical channels are reflected at the DWDM A/D filter and are guided to an optical isolator. The isolator prevents the local oscillator used by the BVT Rx from entering the Bob-QKD unit and therefore interfering with the QKD measurements. Furthermore, the isolator suppresses amplified spontaneous emission (ASE) noise generated by the Erbium-doped fibre amplifier

Table 5.2: Parameters for free-space coexistence testbed

Parameters	Value
Classical Channels	
Number of Channels	8
Classical Channel Frequencies Scenario 1 (Sc1)	193.60 THz, 193.55 THz, 193.50 THz, 193.45 THz, 193.40 THz, 193.35 THz, 193.30 THz, 193.25 THz
Classical Channel Frequencies Scenario 2 (Sc2)	192.60 THz, 192.55 THz, 192.50 THz, 192.45 THz, 192.40 THz, 192.35 THz, 192.30 THz, 192.25 THz
Grid Spacing	50 GHz
Modulation Format	16-QAM
Optical Signal-to-Noise Ratio (OSNR)	30 dB
Transmission rate per Channel	200 Gbps
Total transmission rate	1.6 Tbps
Pre-FEC Level	15%
Detector sensitivity*	-23 dBm
Quantum Channel	
DV-QKD Wavelength	1547.72 nm
DV-QKD Frequency	193.70 THz
QKD Protocol	COW
Maximum Distance	80 km @ 16 dB loss
Optical Band Pass/Rejection Filter (OBRF)	
Insertion loss band pass port	0.5 dB
Center wavelength band pass port	1547.72 nm
Bandwidth band pass port	100 GHz (0.8 nm)

**Corresponding to 16-QAM Modulation @200 Gbps (BER 10^{-3}).*

(EDFA) boosting the classical signals to suitable detection levels. A 95/5 coupler is used to monitor the amplified classical channel profile (blue channels in the inset Figure 5.24). The 95% output port is connected to a 1x8 splitter separating the eight classical channels for coherent detection. A summary of main parameters of the testbed is shown in Table 5.2.

5.4.3 Results

5.4.3.1 QKD Via FWF Terminals

All following experiments in this section were conducted within a 200 lx lab environment resulting in ambient light induced count rates of minimum 1.9 kcps to a maximum of 2.3 kcps with a standard deviation of 100 Hz when using a free running ID Quantique ID210 detector (settings: 5% efficiency, 25 μs dead time and 10 s integration time). This measurement result shows that there is no significant difference to the thermal noise of the detector and counts induced by ambient light. Hence, the spatial filtering of the receiving terminal and the spectral filtering in place allow for a QKD transmission in a 200 lx lab environment free of any significant penalty to ambient light.

The IR Tags of the FWF terminals also have potential to induce additional counts degrading the QKD performance. Figure 5.25a) shows the secret key rate (SKR) and the corresponding qubit error rate (QBER) of two hour test runs with and without the IR Tags for an aligned link with fixed mirror positions. Neither the secret key rate nor the qubit error rate has shown any significant sensitivity to the emission of the IR Tags. Photons emitted by the IR Tags (800 nm and 890 nm, respectively) are expected to couple into the fibre path, however, the limited field of view of the fibre and the reduced photon detection efficiencies at those wavelengths minimise the induced counts to a negligible level. Therefore, the tracking system of the FWF terminals has a minimal impact on the QKD performance.

Free-space systems inherently rely on the alignment of Alice and Bob. As shown in Figure 5.23 and Eqn. (5.2), controlling the angular link misalignment is key to provide a stable QKD link as minor changes can cause significant changes in insertion loss. Figure 5.25b)-d) illustrate on QKD performance key parameter when deliberately steering the receiving FWF terminal off-axis. It can be seen that the SKR and the qubit visibility decrease with increasing off-axis angles, whereas the QBER remains almost constant. Those results indicate that the angular link misalignment causes increased insertion loss as well as affecting the qubit visibility. An angular misalignment of 0.042° (insertion loss equivalent of 4.9dB according to Figure 5.23) exceeded the systems margin preventing the ID Quantique Clavis[3] system from generating secret keys. A link budget design addressing the fibre optical components as well as the distance and misalignment of the terminals is crucial for a seamless operation. Thus, the links in all experiments were manually optimised for minimum losses to handle the margins. In an practical environment, the accuracy of the tracking system used in the FWF terminals (≈ 0.02° [244]) needs to be improved for the given distance of 2.5 m. However, the losses can be traded between losses induced by the fibre optical components, the link distance and the maximum angular misalignment / required tracking accuracy.

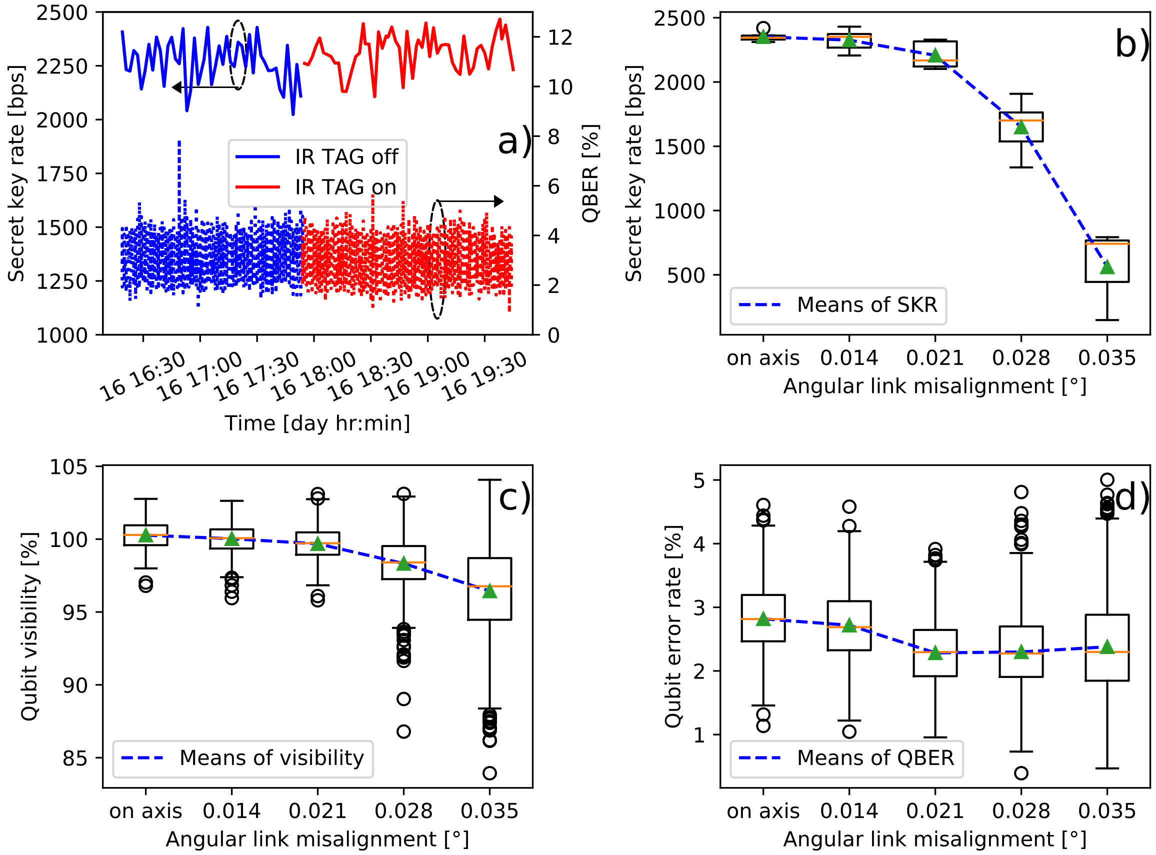


Figure 5.25: Characterising the QKD performance . a) Influence of the IR Tag used for localisation and tracking. b)-d) Secret key rate, visibility and quantum error rate plotted against the angular link misalignment of the terminals at a distance of 2.5 m.

5.4.3.2 Coexistence Of QKD And Classical Communication Channels via FWF Terminals

Due to the orders of magnitude difference in power between the QKD and the classical channels, Raman scattering caused by the classical channel degrades the QKD performance. Raman scattering is a non-linear optical effect and therefore has got a spectral response. In fibre optics both Stokes peaks of the Raman scattering can be found ≈ 1.1 THz around a 1550 nm communication channel [309]. Next to the spectral spacing, the launch power of the classical communication channels determine the amount Raman scattering [211]. Hence, two scenarios have been chosen to investigate the influence of channel spacing as shown in Figure 5.24 and Table 5.2. A spectral spacing of 100 GHz (0.8 nm, labeled ”Sc1“) means the quantum channel is placed in a Raman spectrum dip, whereas a spacing of 1.1 THz (8.8 nm, labeled ”Sc2“) means the quantum channel is placed at the Stokes peak causing additional crosstalk within the BPF filter bandwidth. Figure 5.26 a) and b) illustrate the long term stability of the pointing mirrors for both scenarios for at least 12 hours and with 7 dBm launch power per BVT channel.

None of the classical communication channels was impaired at any time of observation. The measurement results for the QKD link clearly indicate the presence of Raman noise causing a reduction in secret key rate. The origin of the Raman scattering can be found in the <100 m fibre - connecting the BVT and WSS from another lab with the experimental setup. Figure 5.26 c) shows a set of measurements of the experimental testbed with the FWF terminals replaced by a 6 dB fixed attenuator. It can be seen that the launch power of the classical channels as well as the spectral spacing affect to the QKD channel impair the secret key rate. Furthermore, the measurement results for 7dBm launch power co-align with the results presented in Figure 5.26 a) and b) proving the FWF terminals to be transparent for photons either associated with QKD, Raman noise or classical communication.

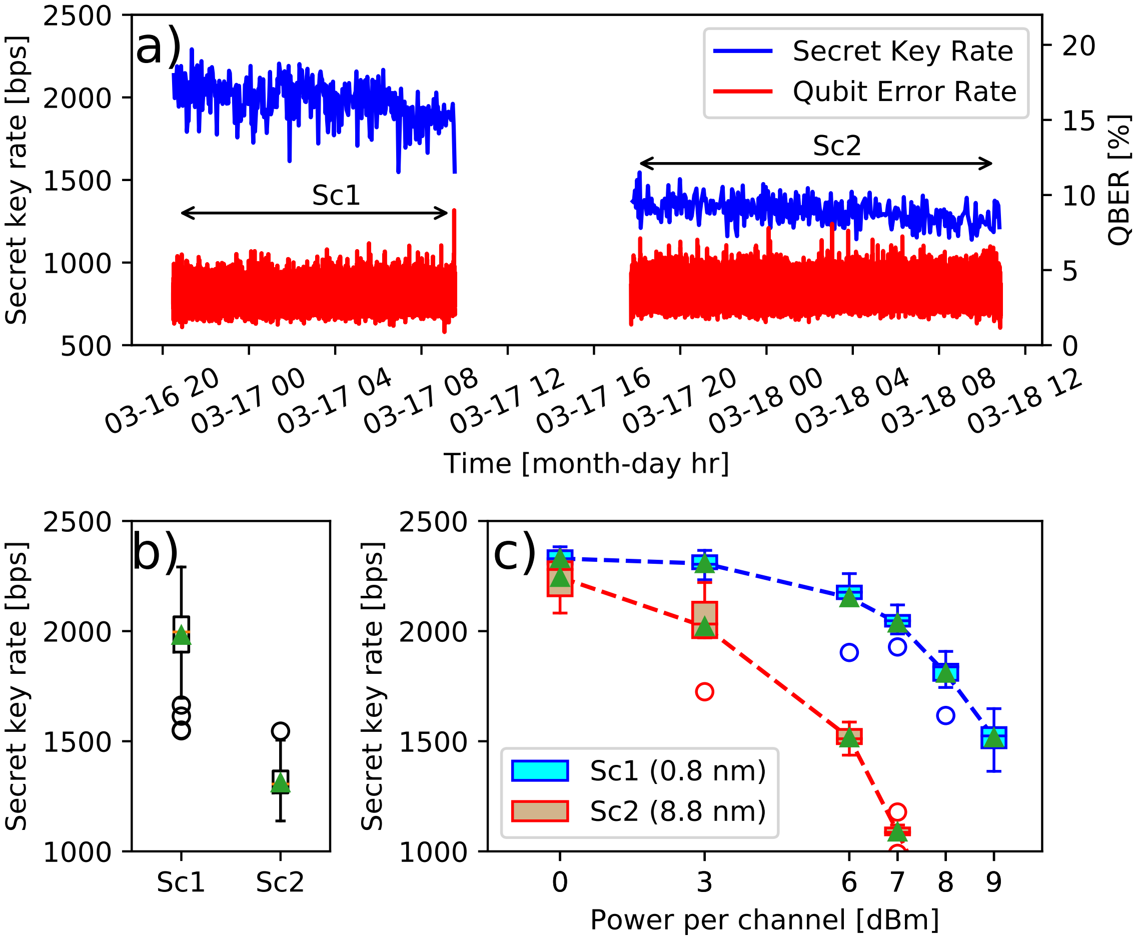


Figure 5.26: Long term measurements of the QKD link operating in coexistence with 1.6 Tbps classical comms link in two different scenarios of spectral spacing. a) Data sets of the night from 16-03 to 17-03 with 100 GHz spectral spacing (Sc1) and from 17-03 to 18-03 with 1100 GHz spectral spacing (Sc2). b) Statistical representation of a). c) Secret key rate vs launch power per channel with the FWF terminals replaced with a 6 dB attenuator.

Finally, the robustness of the coexisting free-space link was tested against angular link misalignment in the presence of Raman noise (Sc2). The receiver terminal was deliberately steered off-axis by 0.021° as this steering angle has demonstrated a minimum impact on the QKD performance as shown in Figure 5.25. That value of angular link misalignment did not impair the performance of any of the classical communication channels. The QKD measurement results are summaries in Figure 5.27. It can be seen that the secret key rate increased significantly compared to the on axis steering position. Furthermore, the qubit error rate is reduced in its mean value and the number of outliers representing high error rates are significantly reduced. The same observation can be taken from the qubit visibility: Even though the mean value is slightly reduced, the number of outliers representing lower qubit visibility is significantly reduced. The main contributor of this behaviour is the change in insertion loss. The QKD channel tolerates the additional loss as demonstrated earlier. However, the Raman noise - and therefore the noise induced qubit error counts - decrease accordingly. The combination of those two circumstances lead to an increased secret key rate at the given link misalignment. Further investigations could pin point a sweet spot for future experiments and help developing optimised tracking systems.

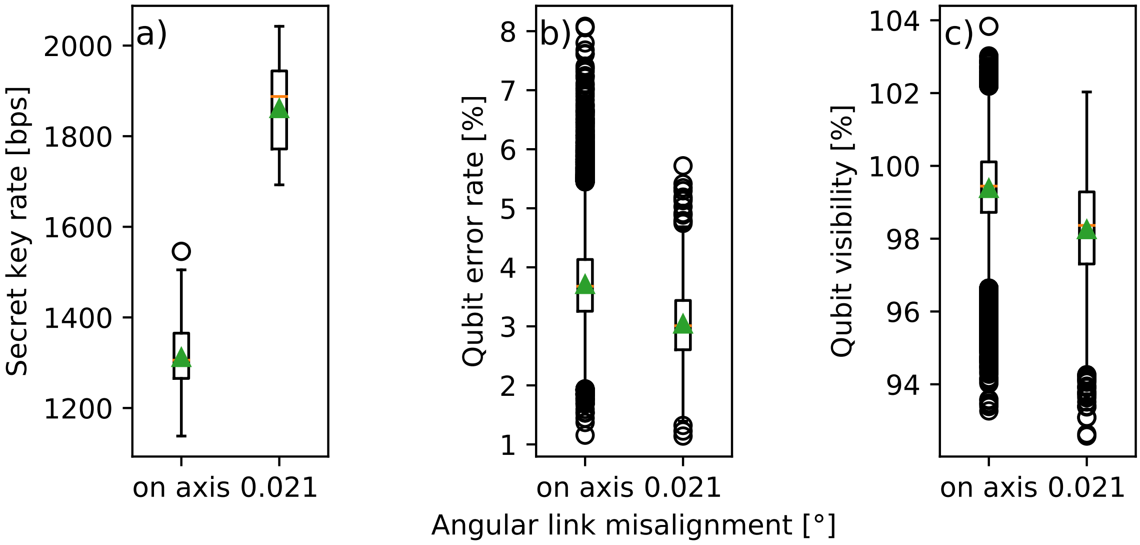


Figure 5.27: Comparison between on axis steering and slightly off-axis steering in Sc2. All three key parameters of a QKD link are displayed.

5.4.4 Summary

This experiment presents the first demonstration of the transmission of a COW-based DV-QKD channel coexisting with classical channels in free-space. The FWF terminal system presented allows for indoor QKD transmissions in a 200 lx environment free of performance penalties and for thorough investigation of the QKD performance. Pointing accuracy is key to maintain a free-space optical quantum link. However, the required pointing accuracy depends on the link budget provided by the QKD system, the insertion loss of the fibre-optical components and the distance covered between the terminals. Compared to previous Tbps FWF links over 2.5 m distance [244], the tracking accuracy needed for the QKD channel had to be refined by a factor of 10 due to tighter margins. The coexistence of quantum and 1.6 Tbps classical data in free-space has been demonstrated highlighting the crucial role of curating the combined signal. Raman scattering generated in fibre optics impairs the QKD performance in free-space. This behaviour has got implications towards the integration of the FWF terminals in PON architectures. However, the deliberate introduction of additional losses by angular misalignment demonstrated the potential to optimise the QKD performance in the presence of Raman noise. The tracking accuracy of the FWF terminal system will be further improved for automated operation with QKD links. When sufficiently accurate the FWF terminals could find applications in the fields of home access networks as part of an all-optical network and connecting quantum computers.

5.5 Improvements across Experiments

Since the QKD systems and the classical optical communication are "plug & play", the improvements across the experiments were mainly within the experimental testbeds and the transmission mediums. For the MCF experiment [262], and the first implementation of the coexistence in SMF [24], optical couplers were used for two reasons at the transmitter side. First, to combine the classical channels into one output and to enable the coexistence of quantum and classical channels. Depending on the number of the classical channels, we used a 1x4 or 1x8 optical coupler. In this case, the coupler did not provide any filtering. It only combined the classical channels into a single output. Therefore, further filtering was required to isolate the quantum and classical channels, increasing the loss for the quantum channel. Moreover, we used a 95/5 coupler to combine the quantum and classical channels into a single output. The 95% output is used for the quantum channel, and the 5% output is used for the classical channels. There are two issues with using a coupler in this case: 1) the high loss of 13 dB in the 5% arm applied to the classical channel and the reflected classical signal in the 95% arm, which affected the quantum transmitter.

We improved dramatically for the next experiment, mainly the first HCF experiment (2 km) [2].We removed the couplers from the testbed and replaced them with two components. First, we used a WSS to combine the classical channels, providing less loss and extra isolation. We removed the 95/5 coupler using a passive off-the-shelf DWDM filter centred at the quantum channel wavelength. We used the pass port for the quantum channel, and the reflect port for the combined classical channels. We also added an isolator to prevent any reflected classical noise from entering the QKD transmitter. Another addition is the double-stage filtering using two DWDM filters centred at the quantum channel wavelength at the QKD receiver side. Finally, we added an optical isolator before the EDFA to prevent the ASE noise from the EDFA from affecting the measurements.

For the second HCF experiment (7.7 km) [12] and the free-space experiment [8], we implemented a notch filter. The notch filter is a DWDM filter centred at the quantum channel wavelength. However, in this case, instead of using it to filter the quantum channel at the QKD receiver, we connected the reflect port of the filter to the classical channels combined output, hence providing us with extra isolation by suppressing the noise level at the quantum channel wavelength. Furthermore, adding the notch filter before the coexistence stage allowed us to push down the noise level at the quantum channel and reduce the in-band noise.

These improvements allowed us to push the coexistence power to the limit while maintaining a relatively low noise level at the QKD receiver. Therefore, generating a high SKR while retaining a low QBER.

CHAPTER 6

Dynamic Entanglement Distribution in Optical Networks

Declaration of Work

This chapter is mainly based on [9, 18, 20].
In [18], I came up with the concept, wrote the code, carried out the experiments, preformed results analysis, and wrote the conference paper.
In [20], I designed and built the testbed. Rodrigo Stange Tessinari and I characterised the testbed, performed the result analysis and wrote the conference paper except for noise level calculation which was written by Marcus Clark.
In [9], Rui Wang, Sima Bahrani, and I designed and built the testbed. We characterised the testbed and collected the results with Marcus Clark and Sima Bahrani. The result analysis were mainly done by Rui Wang and Marcus Clark. We all wrote the conference paper. Siddarth K Joshi provided supervision and was our helpline when needed.
All of this work was done under the supervision of George Kanellos and Reza Nejabati, and some of this work was done under the supervision of Siddarth K Joshi and John Rarity.
The entanglement source and user modules for all the experiment were maintained and aligned by Siddarth K Joshi and Marcus Clark. They have done a lot to help us with all the entanglement experiments, and without their help, this work would have not been possible.
Since I am a co-author of the original text in [9, 18, 20], some of the text have been reused in the chapter where appropriate.

To tackle the scalability issue posed by standard bipartite quantum protocols like QKD protocols, the quantum network infrastructure needs to be dynamic, scalable and sizeable to support growing demand of quantum services, as stated in the previous chapters. This is a particularly ideal case to incorporate entanglement-based networks, which empowers the distribution of entanglement resources across different nodes to enable advanced quantum applications, including but not limited to cryptographic algorithms.

We start this chapter by introducing a model for resource allocation in an entanglement network. Followed by an implementation of a dynamic entanglement distribution quantum network. We begin by discussing the experimental testbed and a brief description of each component. We then discuss the overall network architecture and the dynamicity enabled by the q-ROADM. After that, we present the results of different use cases and provide a summary of the experiment. Next, we evaluate the feasibility of the coexistence of quantum and classical channels in deployed optical networks. We then use the obtained results to demonstrate the coexistence of quantum and classical channels in HCF.

6.1 Wavelength Resources Management of Entanglement Distribution in Optical Networks

In order for the entanglement distribution technology to efficiently scale in sizes capable to address the needs for future quantum applications, networking principles, architectures and algorithms need to be developed to eventually enable flexible allocation of the valuable entanglement resources in an optimal way across the network. In this section, we discuss the development of a new active entanglement distribution architecture that can be photonic integrated with the entanglement source and allows flexible allocation of source bandwidth (entangled wavelength pairs) across multiple users to accommodate the service requirements such as QBER and SKR of on-fly scenarios. We provide a formalized form of the wavelength-pairs assignment problem using the Planning Domain Definition Language (PDDL) which could be used by different intelligent algorithms (planners) to be solved. Finally, we present an intelligent allocation of entangled wavelength pairs using the Fast-Forward (FF) planner and use this to optimize the switching architecture of the entanglement distribution circuit (EDC) to minimize the overall losses and the required switching elements of the entanglement distribution circuit.

6.1.1 Active Entanglement Distribution Circuit Architecture

An active entanglement distribution circuit is shown in Figure 6.1. It is designed to provide on-demand quantum connectivity for an N nodes network considering the time-bin EPR source [310] of Figure 6.1, where a type-II SPDC emitted by a Bragg reflection waveguides (BRW) creates spectrally broadband photon pairs in orthogonal polarization. Considering low loss integrable WDM de-multiplexers [311], the broadband EPR source can generate N pairs of entangled wavelengths and the spectrum of the signal and idler entangled wavelengths are shown in Figure 6.1, such that pairs λ1 and λ4’ are entangled, λ2 and λ3’ is entangled etc. When the wavelengths of the respective pairs are sent in two different nodes, e.g. λ1 in Alice and λ4’ to Dave, a virtual quantum link is established between Alice and Dave. The active entanglement distribution circuit aims at providing a fully connected graph (full-mesh connectivity) between all nodes by suitably redirecting the entangled wavelength pairs to the respective nodes to set up the desired virtual quantum links. For example, in Figure 6.1, λ4 λ3’ and λ2 λ4’ are redirected by changing the configuration of the single SDN-controlled 2x2 switch from the bar to the cross-state between node B and node D to create the new entangled links AD and BC (diagonal), hence provide full-mesh connectivity for the 4-Nodes network. To create graphs where each node has two virtual links (2-connected graph), pairs of entangled wavelengths need to be combined together through a 2x1 MUX or 2x2 multimode interference (MMI) coupler and then be distributed to the different nodes through 2x2 switches (Figure 6.1). Low-loss MMI are considered as multiplexers since they are more broadband and significantly smaller than AWGs in size [312]. A low-loss 2x2 thermo-optic switch [313] is considered to provide the necessary network reconfigurations for full-mesh connectivity (N)(N-1)/2 links. The goal is to calculate wavelength assignments for the entangled pairs using the PDDL model presented in section 3 to minimize the transitions required for covering the full-mesh connectivity so that the number of switches can be optimized in terms of overall losses using a switching algorithm.

6.1.2 Wavelength Pair Assignment Using PDDL with Switching Algorithm

To address the wavelength-pairs allocation problem for the aforementioned entanglement distribution circuit, we have modelled the problem of resources allocation for quantum entanglement distribution systems using PDDL [314]. PDDL is a standard encoding language for classical planning tasks. It provides a formal description of wavelength-pairs allocation in the form of a model which can be used by various planners. Our PDDL model is used by the FF planner [315], which is a forward chaining heuristic state space planner that relaxes the main task P into a simpler task P+ to obtain a heuristic estimate of the solution. The FF planner uses an enforced form of hill-climbing (EHC) technique which combines systematic and local search. The local search of EHC is based on the hill-climbing algorithm; however, to find a sequence of actions leading to a heuristically better successor it uses a breadth-first search algorithm forwards from the global optimum [315]. The planner also uses pruning techniques to select sets of promising successors to each search node and to remove branches where some goal has been achieved too early. Both techniques are obtained by the heuristic search to find a solution quickly and efficiently.

After applying priorities to each virtual link and considering the pre-calculated SKR for the virtual different links as planning metrics, the FF planner finds a plan where the overall network performance is optimized, i.e., the highest SKR is assigned to the highest priority link if possible.

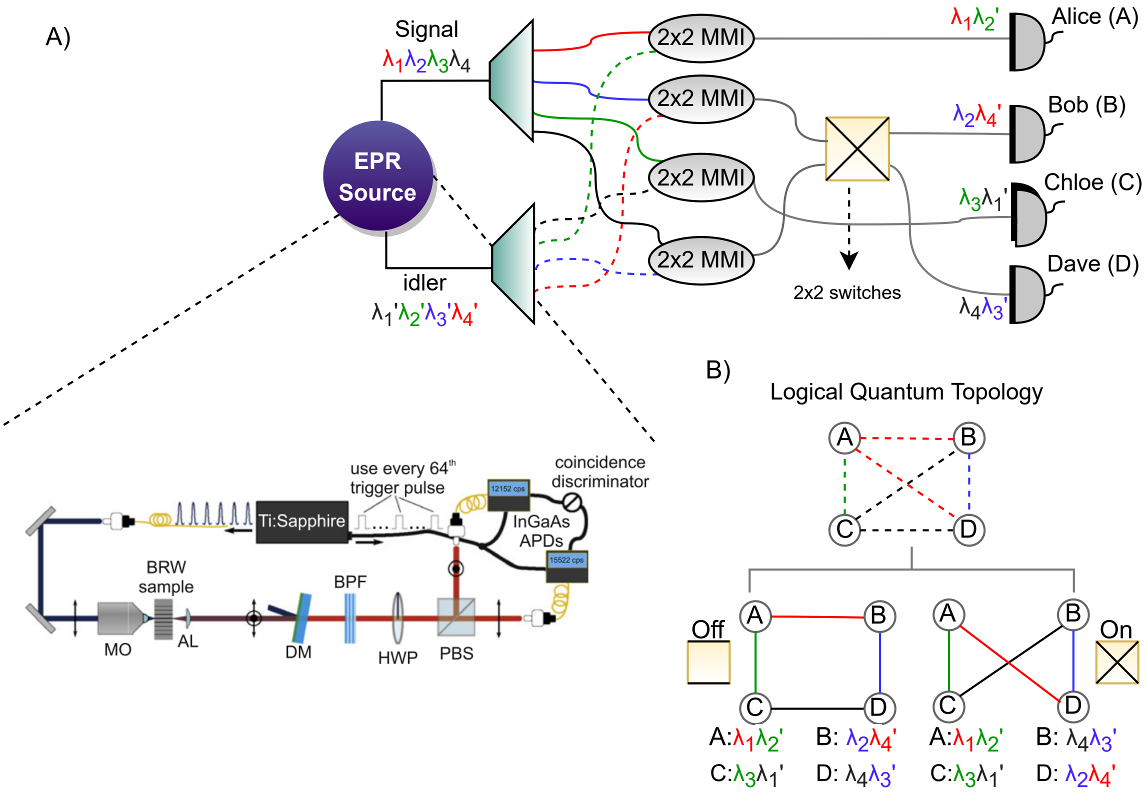


Figure 6.1: A) Active EDC architecture. B) 4-Nodes quantum network topology.

By using a formalized definition of the problem, other pre-calculated parameters such as QBER, pump power, link losses or the length of the link could be chosen as planning metrics depending on the scenario.

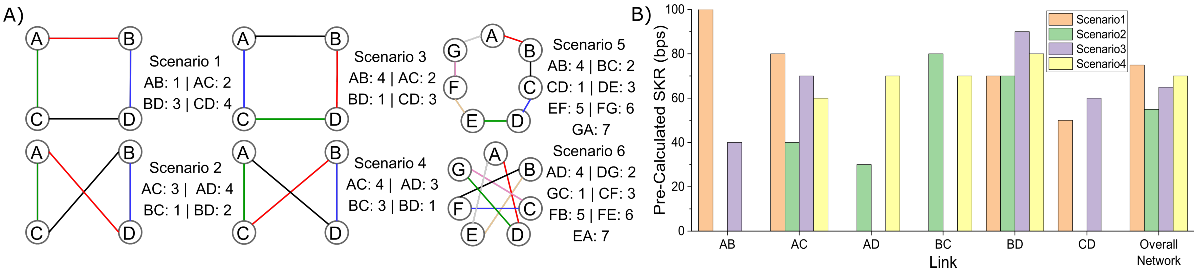


Figure 6.2: A) Different scenarios of wavelengths assignment optimization for 4 and 8 nodes for different link priorities. B) Pre-calculated SKR for different scenarios for 4-nodes network.

Figure 6.2 shows six different scenarios of resource allocation optimization, four for 4-Nodes networks and two for 7-Nodes Networks. In Figure 6.2 scenario 1, the link A-B has priority 1 which is the highest priority. As observed from Figure 6.2 scenario1 (orange), link A-B was assigned the highest value of the pre-calculated SKR of 100 bps, whereas link C-D with priority

4 was assigned the lowest value of the pre-calculated SKR of 50 bps. If the links priority changes even if the topology stays the same as shown in scenarios 1 and 3, the same wavelength pairs yield different SKR due to different paths and user's detectors. Therefore, the planner will adjust wavelength assignments to optimize the overall network performance according to the new priorities and the pre-calculated SKR. Moreover, scenarios 2 and 4 highlights the fact that, the same wavelength pair may also yield different SKR in the same link (BD) in two different scenarios, this is due to the changes in the assigned wavelength in other nodes of the network. Scenarios 5 and 6 shows the same process for a 7-nodes network. To evaluate the complexity of the wavelength assignment problem, we investigated the number of states evaluated by the FF planner and the running-time to reach an optimized solution.

Table 6.1: Number of states, switches, circuit losses and drop in SKR.

Nodes	4	7	9
Number of States w/out Resource Optimization	48	232	487
Number of States w/ Resource Optimization	123	50,877	6,056,993
Overall Switches	1	4	6
Cascaded Switches	1	2	3
Overall Losses (dB)	1.45	1.95	2.45
% Upper Bound SKR [106]	100%	80%	70%

As shown in Table 6.1, in the case of 4 nodes, to reach an optimized solution the FF planner evaluated 123 states in a negligible time and 48 states to reach a non-optimized solution, whereas in a 9-nodes network, the planner evaluated 6M states in 455sec to reach an optimized solution and 487 states in 0.01sec to reach a non-optimized solution. The five orders of magnitude in difference shows the complexity of the problem for higher number of nodes while searching for an optimized solution.

Figure 6.3 shows the flowchart of the switching algorithm used to optimize the number of switches required to transform between two on-fly scenarios after distributing the N wavelength pair from the entanglement photon source (EPS) using the PDDL wavelength assignment model. The algorithm observes the links of two scenarios, for instance scenarios 1 and 2 (Figure 6.2) and compares the distributed entangled wavelength-pairs in each node. If a link has the same entangled wavelength-pairs in both scenarios i.e., link AC (green) and link BD (blue), the algorithm ignores it. However, if there are new links, the algorithm goes through a list of available switches and execute the optimized switching in a form of 2X2 switches that transform scenario 1 to scenario 2. In this way, we minimize the number of overall switches and cascaded switches for different nodes for two on-fly scenarios. Table 1 highlights the overall circuit (Demux+MMI+switches) losses, by increasing the number nodes and thus the number cascaded switches, revealing a marginal insertion loss increase of 1 dB would reflect a tolerable

30% drop of the fundamental theoretical upper bound of SKR for QKD protocol [106].

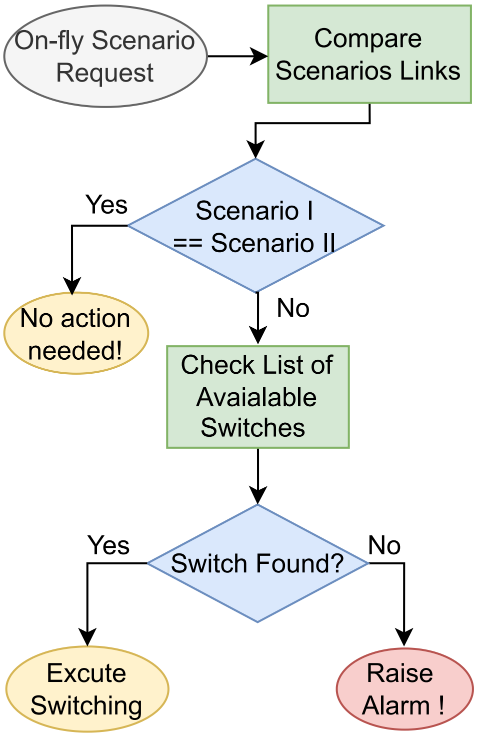


Figure 6.3: Workflow of the switching algorithm.

6.1.3 Summary

We have modeled the entangled wavelength-pairs allocation problem into a formalized form using PDDL and demonstrated an optimization technique using the FF planner which is fed to a switching algorithm to minimize the number of switching requirements to the proposed active entanglement distribution circuit in optical networks.

6.2 A Dynamic Multi-Protocol Entanglement Distribution Quantum Network

To this end, a star shaped quantum network topology has naturally been proposed by employing an entangled photon source to distribute energy-match photon pairs between users. The deployment of fully functional entanglement-based quantum networks has been demonstrated with passive distribution architecture [149, 316–320] and in an active way [321–326]. Especially, polarisation-entangled source was deployed to support a fixed topology of a 4-user quantum network [317]. This concept has been pushed further in [149] for an 8-user entanglement-based quantum communication network with adoption of dense wavelength-division multiplexing

(DWDM) and beam splitters (BS) at the cost of quantum link performance due to their losses. The concept of using beam splitters in entanglement distribution to interconnect large number of users has been demonstrated recently in [319]. Furthermore, entanglement-based quantum secure direct communication were presented in [320] for 15 users. The quantum communication networks with passive entanglement distribution architecture offers fixed topology and relatively high loss, prohibiting any active network management and configuration for dynamic quantum applications and services.

The active optical switching [324–326] were implemented to offer dynamic allocation of entanglement in the quantum networks. More recently, the employment of wavelength selective switch (WSS) for active entanglement distribution has been demonstrated in [321] with adaptive bandwidth management. In [323], a similar concept has been presented with AlGaAs chip entanglement source of up to 4 users in lab environment with various fibre length configurations. However, neither the active switching nor employment of WSS approaches offers large-scale quantum network with medium to long distance which limit the performance of the quantum networks.

6.2.1 Experimental System Testbed

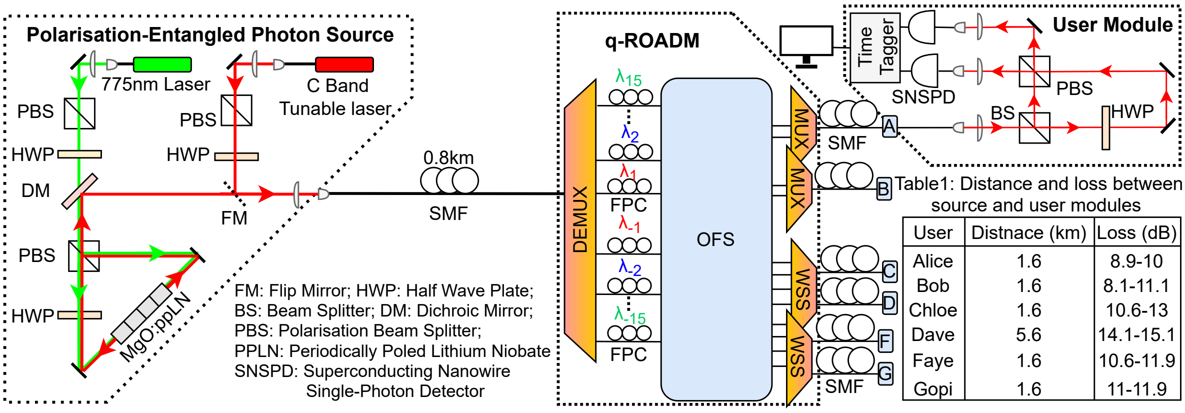

Polarisation-Entangled Photon Source
775nm Laser
C Band
Tunable laser
PBS
HWP
DM
PBS
HWP
PBS
HWP
FM
MgO:ppLN
0.8km
SMF
FM: Flip Mirror; HWP: Half Wave Plate;
BS: Beam Splitter; DM: Dichroic Mirror;
PBS: Polarisation Beam Splitter;
PPLN: Periodically Poled Lithium Niobate
SNSPD: Superconducting Nanowire
Single-Photon Detector
q-ROADM
DEMUX
λ15
λ2
λ1
FPC
λ-1
λ-2
λ-15
FPC
OFS
MUX
MUX
WSS
WSS
SMF
SMF
A
B
C
D
F
G
Time Tagger
SNSPD
User Module
PBS
BS
HWP

Table1: Distance and loss between source and user modules

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

Figure 6.4: Experimental testbed diagram consisting of a broadband polarisation-entangled photon source connecting to 6 users through campus and metropolitan fibre links via a q-ROADM.

The schematic of the experiment is illustrated in Figure 6.4, consisting mainly three parts: 1) a broadband entangled photon source to provide bipartite entanglement, 2) a q-ROADM to enable flexible and on-demand entanglement distribution, and 3) users equipped with measurement modules to perform entanglement correlation. The entangled photon source is located within the Centre for Nanoscience & Quantum Information (NSQI) building, connecting to the q-ROADM at High Performance Networks Group lab in Merchants Venturers Building via 0.8 km campus fibre. The q-ROADM supports arbitrary shapes of entanglement distribution, which can establish quantum links between any users combination. In this experiment, the q-ROADM connects to the user modules deployed at NSQI either via 0.8 km campus links directly or via 4 km (2 km one way) loop-back metropolitan fibre links between HPN lab and Watershed then back to NSQI with overall 4.8 km fibre in place.

6.2.1.1 Entanglement Source

At the entanglement source, a continuous wave laser operating at 775.12 nm (shown as green) emits light passing through a polarisation beam splitter (PBS) and a half-wave plate (HWP), where the light is set to diagonally polarised $|D\rangle$ or anti-diagonally polarised $|A\rangle$. The D/A polarised light transmits through a dichroic mirror (DM) and a PBS, where ideally 50% light propagates clockwise inside the Sagnac loop, defined as of vertically (V) polarisation and 50% of light propagates anti-clockwise, defined as horizontally (H) polarisation. A HWP inside the Sagnac loop is rotated at 45° to convert V light to H light and vice versa. The light propagating along both directions are focused into the centre of a type-0 Magnesium-Oxide-Doped Periodical Poled Lithium Niobate (MgO: PPLN) crystal. In clockwise, 775 nm vertically polarised photon splits into a vertically polarised photon pair (a signal and idler photon) via type-0 Spontaneous Parametric Down Conversion (SPDC), which are converted to horizontally polarised photon pairs by the HWP. In anti-clockwise, the horizontally polarised 775 nm photon is rotated to vertically polarised photon, which is then down converted to vertically polarised signal and idler photon pairs. The PBS then combines the signal and idler photon pair from both directions back to the DM, which reflects them to a flip mirror, isolating from 775 nm pumping light. This allows the implementation of polarisation-entangled photon pairs which centres at 1550.12 nm, in a bell state of $|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$.

6.2.1.2 Quantum Network Connection

The fibre polarisation neutralisation procedure is needed for different quantum communication links as the polarisation of photons changes randomly along the fibre. This is to ensure the polarisation state at the users to be identical to the state at the output of the entanglement source. To perform efficient neutralisation for large number of quantum links, an C-band tunable laser is deployed and is attenuated at quantum level. A Wollaston Prism at the output of C-band laser will provide horizontally polarised light, in which can be further converted to vertically polarised light by rotating the HWP. The entanglement source is able to select between sending entangled-photons to perform quantum communication and sending predefined vertically/horizontally polarised C-band light to perform fibre neutralisation via the motorised FM. Both entangled-photon pairs and the C-band light are alligned and coupled into a single mode fibre, which connects a q-ROADM at HPN lab via 0.8 km campus fibre between NSQI and HPN lab. The q-ROADM allows arbitrary entanglement distribution to form different correlation graphs, where its architecture will be discussed in detail in the following subsection.

6.2.1.3 User Modules

The user modules in this experiment, as shown in figure 6.4, consist of a polarisation analysis module (PAM) and two superconducting nanowire single-photon detectors (SNSPDs). The fibre-based input of PAM propagates to a BS via a collimator, which enables passively selection of measurement basis with a short and a long optical path. A PBS performs HV basis measurement for the short path. In the long path a HWP rotates the polarisation by a 45° for effective polarisation correlation measurement in DA basis using the same Detectors. In the experiment, the user modules are aligned between 52.8% - 76.1% coupling efficiency for two paths. The two output of the PAM are directed to guide photons into fibre towards two SNSPDs by two couplers. With 6 users in this experiment, there are 12 SNSPDs which are further connected to a time tagger (Swabian Time Tagger Ultra). It is worth noting that lower quantum bit error rate (QBER) quantum links can be achieved when each user is equipped with 2 PBS and 4 SNSPDs to perform HV basis and DA basis measurement separately. However, the proposed PAM design is more hardware efficient to implement large-scale quantum communication networks by reduce the number of single photon detectors by half.

6.2.1.4 q-ROADM

The architecture of the q-ROADM is also illustrated in Figure 6.4, where a demultiplexer (DEMUX) divides the spectrum of the broadband entangled photon source into 30 slices according to ITU-T 100 GHz DWDM standard. The central wavelength λ_0 of DEMUX is ITU-T channel 34 with wavelength of 1550.12 nm, which approximates to the centre of the broadband entanglement spectrum. We denote the rest wavelength as $\lambda_{\pm i}$ or $\pm i$, where i is an integer in the range of $[-15, 15]$. The non-degenerate SPDC process gives entangled photon pairs, where the wavelengths are equally spaced and can be abstracted in the form of wavelength pairs $[\lambda_i, \lambda_{-i}]$.

Each 100 GHz channel is connected to a fibre polarisation controller (FPC) to maintain the polarisation state identical at the users compared to the output at the entanglement source. The FPCs are then connected to an 192×192 optical fibre switch (OFS), in which any cross-connection can be programmed. The wavelength selective switch (WSS) and multiplexer (MUX) multiplex different wavelength channels into a single fibre link connected to the users. MUX being a passive device with relatively low insertion loss, poses more constraint on wavelength channels which can be distributed to the users compared to the programmable WSS. MUX supporting more DWDM channels can provide higher flexibility for entanglement distribution, however, requiring more OFS output ports. In this experiment, we use two 1×16 MUXs connecting to Alice (A) and Bob (B) respectively, to ensure certain flexibility of wavelength channels distribution without occupying too many OFS ports. Although WSS has a higher insertion loss (~5dB) compared to MUX (1.3 - 2.7 dB), its programmable capability decides its input and output port are wavelength agnostic, which requires fewer number of connection ports at OFS. We use two

4 × 16 WSSs (Finisar WaveShaper 16000S) in this experiment, one associated to Chole (C) and David (D) and the other one supports Faye (F) and Grant (G). At each WSS, 16 ingress ports connected to the OFS and 2 out of 4 egress serving as client ports connecting two users. The WSSs will be configured to combined the channels from OFS to the designated users.

Apart from DEMUX, MUX and WSS, a few extra FPCs and BSs are connected to the OFS directly. By switching (via OFS) wavelength λ_i to a BS, photons randomly pass through either of two output ports, allowing a single wavelength distributed to two users simultaneously. For example, the OFS for wavelength −8 is configured as $DEMUX_{-8} \rightarrow BS_{in} \rightarrow BS_{out_1} \rightarrow MUX_{Alice}$ and $DEMUX_{-8} \rightarrow BS_{in} \rightarrow BS_{out_2} \rightarrow FPC_{in} \rightarrow FPC_{out} \rightarrow MUX_{Bob}$. in the following order ($BS_{out_1} \Rightarrow FPC \Rightarrow user$), The FPC at output of DEMUX channel -8 is to neutralise the fibre to Alice and the extra FPC that provisioned is to neutralise the fibre to Bob. The subscription 0.5 of channel -8 in the table presents the beam splitting ratio, corresponding to the 3 dB BS adopted. In summary, the q-ROADM offers highly flexible entanglement distribution feature, allowing to serve on-demand quantum link requests. The architecture is also scalable to support additional users, which can be connected to the q-ROADM providing enough ports available.

6.2.2 Experimental Scenarios and Results

In this system we use QKD to demonstrate the ability of such a network to distribute entanglement. By showing the generation of a quantum secure key we show that entanglement has been shared without having to show a violation of the Bell Inequality.

With successful entanglement distribution via q-ROADM, the users of each quantum link exchange the time tagging information with their communication partner to perform BBM92 protocol. Each user utilises its own time tags and information from others to perform temporal correlation. The temporal cross-correlation diagram ($g^{(2)}$) of Alice-Bob link is shown in Figure 6.5. The blue and red curve represent the $g^{(2)}$ correlation of $D_{A1} - D_{B1}$ and $D_{A2} - D_{B2}$, whereD_{Xi} denotes detector i at the user X, $i \in \{1,2\}, X \in \{A, B, ...\}$. The orange and green curve show the temporal correlation between $D_{A1} - D_{B2}$ and $D_{A2} - D_{B1}$ respectively. The central peak of four curves correspond to the measurement using the same basis. Two side peaks represent the measurement performed in either with *long path - short path* or in *short path - long path* at the user modules, in which short (long) path presents measurement in HV (DA).

Given a coincidence window, coincidences (raw keys) between detector pairs can be expressed as:

$$C_{total} = C_{D_{A1}-D_{B1}} + C_{D_{A2}-D_{B1}} + C_{D_{A1}-D_{B2}} + C_{D_{A2}-D_{B2}} \tag{6.1}$$

where C_{total} is the total number of coincidence counts within the coincidence window, $C_{A_{Di}-B_{Dj}}$ represents the coincidence between detector i of user 1 (Alice) and detector j of user 2 (Bob) separately, $i, j \in \{1,2\}$. Further, the QBER of a link can be calculated as the ratio of accidental

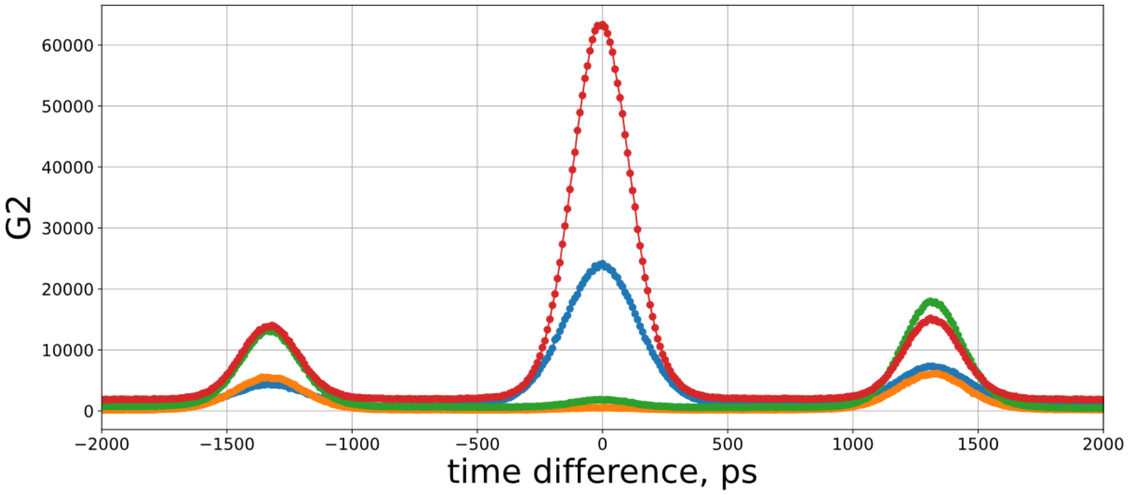


Figure 6.5: Temporal correlation histogram between Alice and Bob for the 6-user full-mesh network.

counts over the total coincidence counts, which is calculated as:

$$QBER_{A-B} = \frac{C_{D_{A2}-D_{B1}} + C_{D_{A1}-D_{B2}}}{C_{total}} \tag{6.2}$$

Thus, the amount of sifted key N_{sifted} is obtained by assigning 0 and 1 to the coincidence counts of $C_{D_{A1}-D_{B1}}$ and $C_{D_{A2}-D_{B2}}$. Then users can extract the final secret key after key distillation, including error reconciliation and privacy amplification. As a result, the total amount of secret key is given as:

$$N_{key} \geq N_{sifted}[1 - fH_2(QBER) - H_2(QBER)] \tag{6.3}$$

where the $H_2(p) = -p * log_2^p - (1-p) * log_2^{1-p}$ is the function of Shannon entropy, f is the term accounting for the error correction efficiency.

Case 1: 6-user full mesh: Figure 6.6 shows SKR stability of all 15 links over 560 minutes. The variation of the key rates of different quantum links are due almost entirely to the losses for each wavelength. The loss is a complete system loss; including the q-ROADM, fibre transmission, user modules and detectors. It is worth noting that the SKR does not only depend on the loss of q-ROADM and fibre but also relates to the detection efficiency of SNSPDs, alignment condition of polarisation analysis module and the accidental rate (noise) at each user. Through 560 minutes of monitoring data as depicted in Figure 6.6, the proposed experimental testbed is able to support stable quantum links over a long period of time.

Case 2: Effect of additional channels: Unlike in classical optical networks where additional channels between two nodes improve the capacity of the link, distributing more than one entangled wavelength pair to the same user pairs will not improve the SKR. We study this

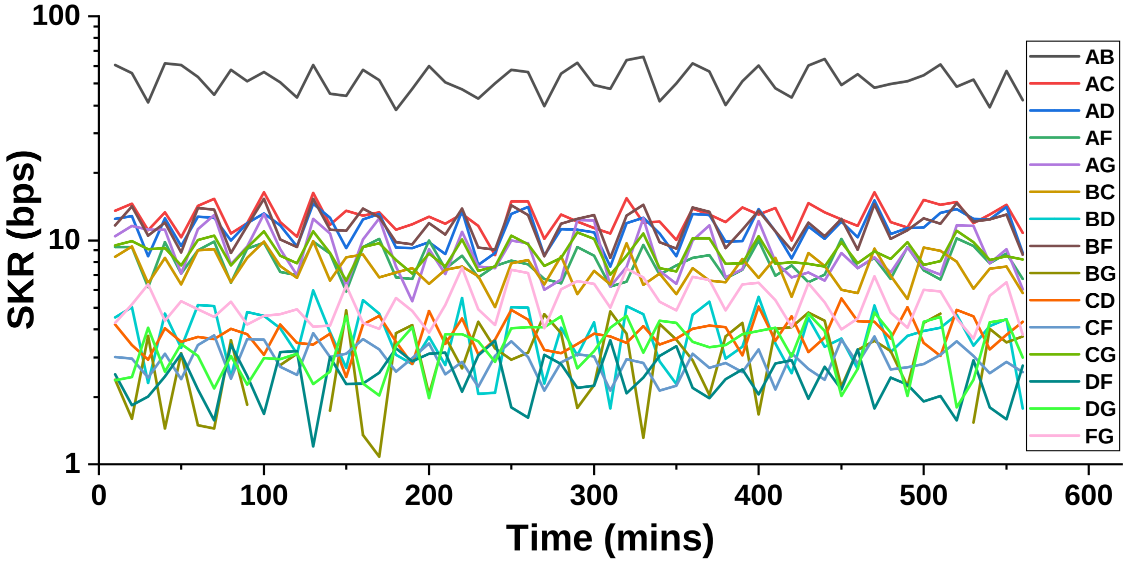


Figure 6.6: 560 minutes monitoring SKR for 6-user full mesh network configuration.

phenomenon by distributing 1, 2 and 3 pairs of entangled wavelengths between Alice and Bob. The results in Figure 6.7 depict the total SKR with 1, 2, and 3 pairs of wavelengths assigned to the AB link. In each case, the source (775 nm laser) pump power was adjusted to demonstrate its effect on the network performance. Provisioning more entangled wavelengths for one link increase the accidental rate (noise) and coincidence rate (signal) at the same time. Extra accidentals cancel out the benefit of additional coincidence posed by additional wavelengths. E.g. with 3 pairs of entangled wavelengths, the optimum source laser pump power $\approx$ 3 mW but for a single wavelength pair the optimum power is 14.8 mW. From Figure 6.7, AB link is able to achieve a maximum SKR of 1136 bps with one pair of entangled wavelength compared to SKR of 352 bps and 262 bps for two and three wavelength pairs respectively.

Case 3: Dynamic topologies: A QKD network relies on accumulated keys and does not necessarily need uninterrupted connectivity. Compared to classical networking to support ongoing Internet traffic, full-mesh quantum networks for QKD are not required constantly when enough keys can be accumulated between users. Hence, we investigate the performance of dynamically switching the quantum network between two partial-mesh schemes and compare their performance with the full-mesh scheme, as illustrated in Figure 6.8. The two partial-mesh schemes complement each other to form a time-shared full mesh network. Figure 6.8 shows the cumulative keys generated in a 6-user full-mesh setting for 40 minutes vs in 2 partial-mesh settings for 20 minutes each to obtain the cumulative secure keys over a period of 40 mins for each scenario. Data is shown with a fixed source pump power to illustrate the utility of such dynamic topologies. As shown in Figure 6.8, most links in the time-multiplexed partial-mesh

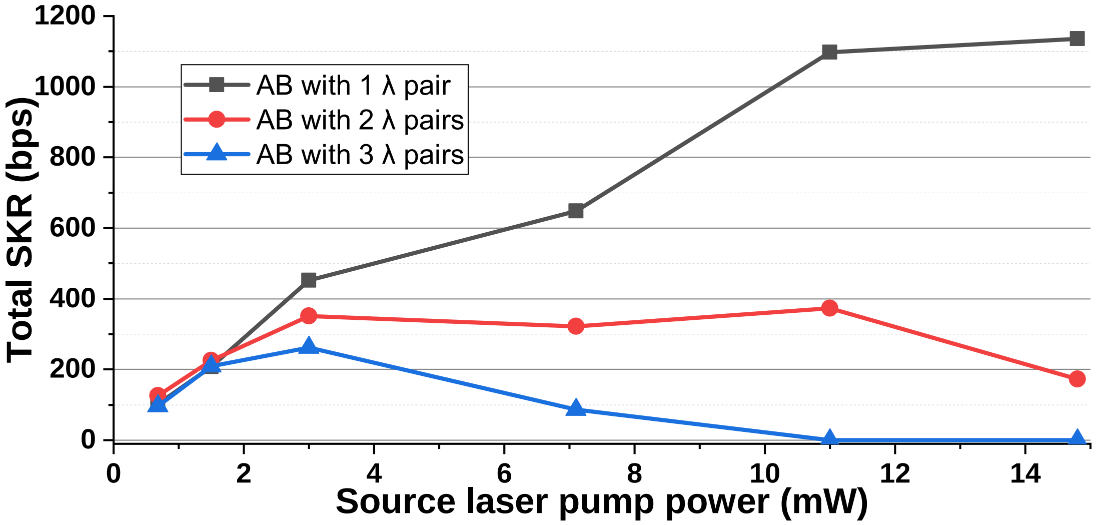


Figure 6.7: Total SKR of Alice-Bob link assigned with 1, 2, and 3 entangled wavelength pairs vs source laser pump power.

schemes outperform the same link under full-mesh condition apart from AB, AG and FG. This is because only 2-3 signal/idler wavelengths are assigned to each user compared to 5 wavelengths for the full-mesh case. Further improvements are possible by optimising the pump power of the source.

Case 4: Multiple protocols: A major limitation of quantum communication is the need for a pre-shared authentication key between any two end-users. There is no known information theoretically secure way of doing this. Thus adding a user into a large quantum network is impractical if pre-shared keys must first be exchanged with all users. Here we implement the Secure Initial Authentication Transfer (SIAT) protocol [327] to add user A to a 5-user network. Further, we demonstrate how our network dynamicity can be used to create a series of different topologies to significantly improve the time taken to run this protocol. Besides the dynamic configuration of an entanglement-based quantum network, q-ROADM supports adding new users into the quantum network via its '*plug and play*' capability. We examine this feature by adding a new user, Alice, into a 5 user full-mesh quantum network and authenticating new quantum links between Alice with other users via the SIAT protocol, where cost-effective pre-shared keys are not available. SIAT protocol first requires the new user to have a pre-shared authentication key with just one of the existing users (say B) in the network, as illustrated in the coloured (blue) solid line in Figure 6.9. The user with the pre-shared key acts as a temporary trusted node to authenticate a new link to another user (say C). In step 1 of SIAT, A and C exchange keys with B as a trusted node. In step 2 A and C use this key as the initial authentication and exchange entanglement until they have enough new keys to ensure that B no longer needs to be trusted. Step 1&2 are repeated for every user. However, in Step 1, all available

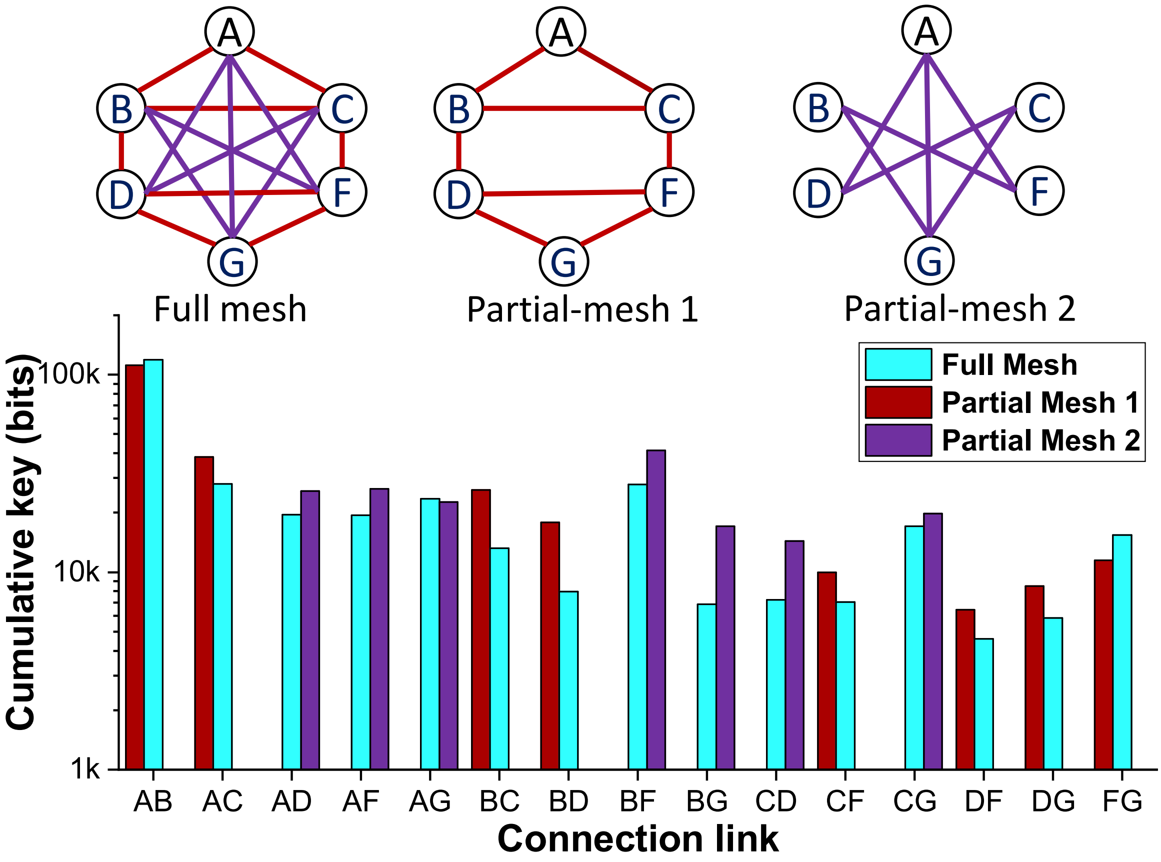


Figure 6.8: Performance comparison between full-mesh topology against time-shared full-mesh (2 partial-mesh) network topologies over 40 mins.

non-overlapping paths are used according to the flooding protocol [327]. This decreases the probability of failure for the SIAT protocol even if B now becomes malicious. Using our dynamic network, we can implement SIAT using only the desired networks topologies at each point in time. This corresponds to the fastest execution of the SIAT protocol. Further, we evaluate two SIAT strategies (results in Figure 6.9): S1) best link first (blue); Bob to be the initial trusted node having a pre-shared key with Alice, with link authentication order of AC→AD→AF→AG; S2) worst link first (red), Gopi to be the initial trusted node, with authentication order of AF→AD→AC→AB. The time required for each step of flooding SIAT protocol of two strategies is shown in Figure 6.9. Our results show that S2 is clearly a faster strategy overall.

6.2.3 Summary

A 6-user entanglement-based quantum communication network architecture. A type-0 SPDC broadband polarisation entangled photon source is connected to a q-ROADM via 0.8 km campus fibre between HPN and NSQI, which allows scalable, dynamic and arbitrary entanglement

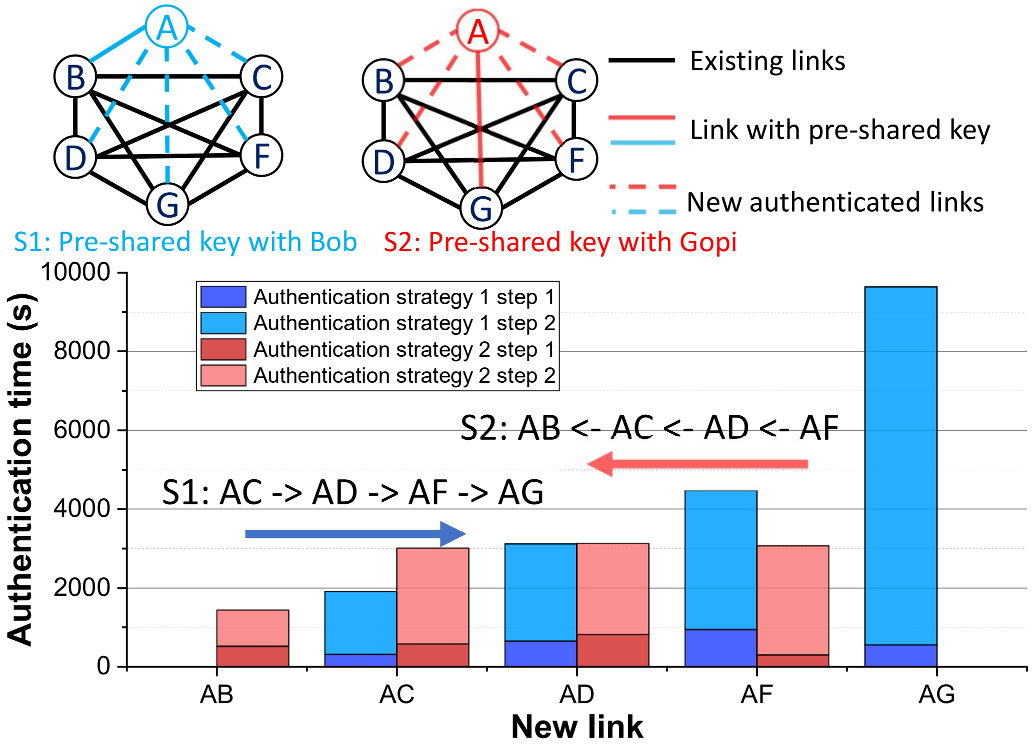


Figure 6.9: Authentication time for implementing SIAT protocols with two strategies by adding a new user Alice into a 5-user full mesh network.

distribution over many users. The 6 user modules in this experiment were deployed at NSQI, which connects to the q-ROADM via University of Bristol campus link between NSQI and HPN lab (user A, B,C,F,G) and Bristol metropolitan fibre link looping back from Watershed (user D). At each user, there is a polarisation analysis module, two SNSPDs, a time tagger and a computer to exchange the classical information of measurement outcome with other users. The input photons of PAM randomly travels along either long path or the short path. The short path measures photons in HV basis while the long path containing a HWP to performs measurement in DA basis. Our q-ROADM allows us to test different dynamic strategies for various quantum protocols, not just QKD. We show how the flooding and SIAT protocols effectively authenticate a new user to establish new QKD links. This extensive and systematic test of WDM entanglement networks is a crucial first step towards understanding the scalability and performance of such networks as well as creating advanced and intelligent network control and monitoring software.

6.3 Towards Coexistence of Classical Channels Within a Quantum Entanglement Network

We have discussed the coexistence of quantum and classical channels in quantum networks in Chapter 4 and chapter 5. However, the experiments in these chapters did not use entanglement for the QKD. For entanglement distribution, such coexistence demonstrations have so far been limited for two users and in laboratory conditions [328] while significantly affecting the performance of the quantum entangled link. In the present communication, we first obtain an analytical expression to calculate the degradation of the Secret Key Rate (SKR) of the multi-wavelength quantum entangled link at the presence of classical communication channel. Following we experimentally assess the additional noise in terms of photon counts over a 0.8 km long deployed optical fibre that is part of our previously deployed 8-user quantum network testbed together with the collected data for the average secret key rates and photon counting statistics for the quantum entangled Bob-Feng link [149], to prove that co-existence of all 30 quantum entangled channels can be achieved with a minimum penalty of < 3.8% in the SKR while sustaining an error-free 100 Gbps classical channel in the C-band.

6.3.1 Quantum Entangled Channels Noise Level Tolerance Calculation

When considering QKD as an application of quantum channels, all errors are assumed to provide the eavesdropper (Eve) with information about the key. As long as the quantum bit error rate (QBER) remains below 11%, it remains possible to extract a key with information theoretically perfect security [329]..

A bright classical signal in the same optical fibre as the quantum signal(s) can, primarily due to Raman scattering, cause an increase in noise counts ($D \times Ch$, with D increased noise counts in each of the Ch wavelength channels) seen by the quantum detectors. The corresponding increase in the QBER is given by

$$QBER = \frac{\tau_c \times (S_a + (D \times Ch)) \times S_B}{P} - \frac{\tau_c \times S_a \times S_B}{P} \tag{6.4}$$

where τ_c is the coincidence window, S_a is the photon count rate seen at user a, P is the total coincidence rate seen between the users. Further, the secure key rate is directly proportional $\left[H\left(0.5 + \sqrt{QBER \times (1 - QBER)}\right) - H(QBER)\right]$, where $H(\varepsilon)$ is the Shannon Entropy of ε. Adding classical channels to the same fibre as the quantum states has no effect on QKD other than this increased QBER and decreased key rate. Thus by measuring the noise caused by the classical transmission we can evaluate the feasibility of classical quantum coexistence.

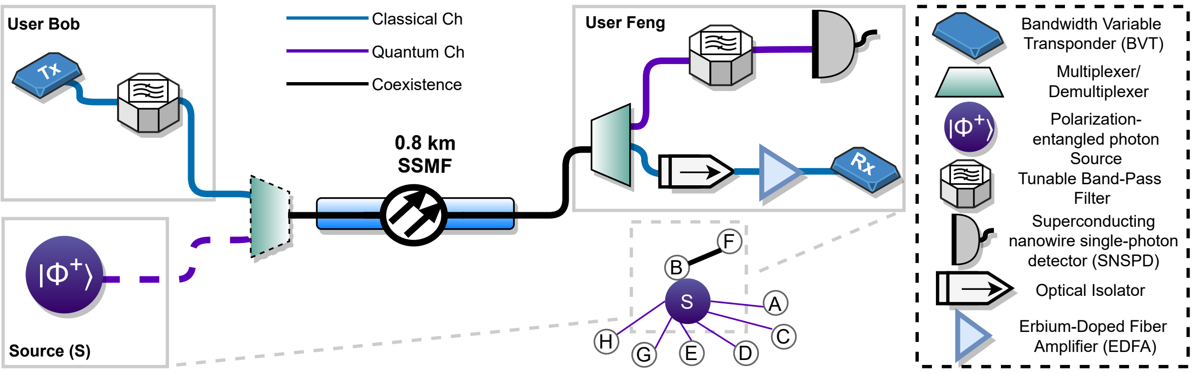

User Bob
Tx
Classical Ch
Quantum Ch
Coexistence
0.8 km
SSMF
User Feng
Rx
|Φ⁺⟩
Source (S)
F
B
S
A
C
H
G
E
D
Bandwidth Variable Transponder (BVT)
Multiplexer/ Demultiplexer
Polarization-entangled photon Source
Tunable Band-Pass Filter
Superconducting nanowire single-photon detector (SNSPD)
Optical Isolator
Erbium-Doped Fiber Amplifier (EDFA)

Figure 6.10: Experimental testbed.

6.3.2 Experimental System Testbed

To experimentally evaluate the excess noise created by the presence of a classical channel spectrally close to the quantum entangled channels, we added the classical equipment to the existing 8-user quantum network testbed presented in [149]. A bandwidth variable transponder (BVT) was deployed in nodes B and F (Bob and Feng, respectively), further enabling 0:8 km of co-existence. Figure 6.10 shows the testbed. Since Raman phenomena is the major source of noise contribution in our system, our theoretical analysis shows that anti-stokes shorter wavelengths close to the quantum channel are preferable. Given that, the quantum testbed employs thirty 100 GHz entanglement-based quantum channels ranging from ITU-T CH19, i.e. F_c = 191.9 THz to ITU-T CH49, i.e. F_c = 194.9 THz (excluding CH34, i.e. F_c = 193.4 THz because no entanglement is produced at this channel by the quantum source used in our testbed.), we decided to apply the classical channels on the lower edge of the spectrum, i.e. ITU-T CH17, i.e. F_c =191:7 THz, and CH18, i.e. F_c =191.8 THz (one at a time). In both cases, the classical channel provides a 100Gb/s 25 Gbaud PM-QPSK signal with a SD-FEC of 25% to enable a error-free transmission. A tuneable band-pass filter (TBPF) with ≈ 5 dB of insertion loss was used to suppress the noise from the BVT Tx on the quantum channels. We used a fixed WDM filter with a low insertion loss of 0.8 dB (represented by the multiplexer in Figure 6.10) in which the quantum and classical channels are passed through the rejection and passing ports respectively resulting in co-existence in the common port.

After the multiplexer, the the classical data channel travels through 0.8 km of field-deployed SMF to a similar WDM filter (represented by the demultiplexer in Figure 6.1 that passes the classical channel while rejecting all other channels towards the Superconducting nanowire single-photon detector (SNSPD). This WDM filter provides a ≈10 dB of isolation from the excess noise of the classical channel to the rejection port. The classical channel is then connected to an optical isolator with insertion loss of ≈3 dB to prevent the tunable laser used by the BVT Rx as a local oscillator from travelling back to the SNSPD and altering the measurements. It also prevents the Amplified spontaneous emission (ASE) noise generated by the Erbium-doped fibre amplifier (EDFA) which is used to amplify the classical signal. Finally, the channels rejected on the WDM filter including the quantum channels, are sent towards a TBPF with sharp filter edges and then is received by the user's detector. This 100 GHz bandwidth TBPF provides ≈60 dB of isolation to the quantum channel from the excess noise generated by the classical channel, and was used to tune the rejected channels to the required wavelength of the quantum channel to measure the excess noise using the SNSPD. The SNSPD detection efficiencies ranging from ≈70 to 90%, a jitter of between ≈60 and 80 ps (including the measurement device), and dark counts of ≈1 kHz.

6.3.3 Results

Figure 6.11 shows the experimental evaluation of excessive photon counts in the presence of a classical channel. Specifically, Figure 6.11 a) presents the excess noise due to classical channel CH17 (191.7 THz) for launching power varying from -29 to -26 dBm. The excess noise is expressed in photon counts per second, and as detailed in Section 6.3.1 impacts negatively on the Quantum Bit Error Rate of the link, thus decreasing the SKR obtained.

The line at the 20000 counts represent our maximum threshold for what we consider an acceptable impact hit in the SKR value for the link which is a reduction of 7.2% of the total value. It can be seen that 23 out of the total 30 quantum channels are within our acceptable threshold at a launch power of -26 dBm and 28 out of 30 at a launch power of -28 dBm, hence, revealing that co-existence is feasible with most of the entangled wavelength pairs produced by our source. Table 1. shows the Bit Error Rate for the classical channel 17, confirming that error-free classical data channel is also obtained for any launching power up to -28 dBm, with a Bit error rate (BER) of 0.01 due to the aid of FEC.

Raman intensity simulations shown in Figure 6.11 b) reveal that the peak of the scattering noise, highlighted within the appropriate range in both a) and b), is only affecting a limited number of the quantum entangled channels. It is also evident that the intensity of the anti-stokes (right side of Figure 6.11 b) of the Raman noise is lower than the stokes (left side), hence supporting the choice of classical channels at the lower edge of the entangled source. Finally, it reveals that there is a region close to the classical channel with a dip to the scattering noise effect, further facilitating co-existence. In our case, according to the photon counts measurement Ch19 - Ch24 are the best candidates for co-existence next to channel 17, exhibiting less than 1000 counts. Figure 6.11 c) repeats the previous experiment tuning the BVT Tx to CH18, for two power levels (-29 and -26 dBm), revealing that the noise peak is also shifted one channel to the right, thus confirming that the peak noise is a product of Raman phenomena.

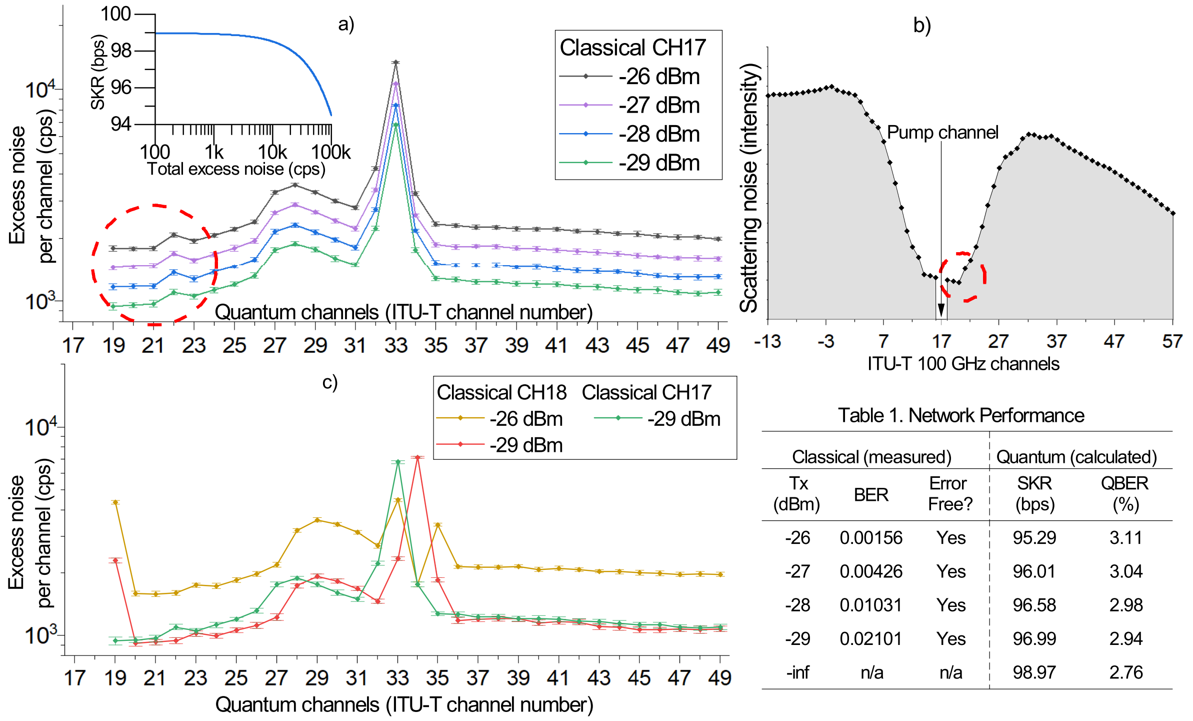


Table 1. Network Performance

Classical (measured)			Quantum (calculated)	
Tx (dBm)	BER	Error Free?	SKR (bps)	QBER (%)
-26	0.00156	Yes	95.29	3.11
-27	0.00426	Yes	96.01	3.04
-28	0.01031	Yes	96.58	2.98
-29	0.02101	Yes	96.99	2.94
-inf	n/a	n/a	98.97	2.76

Figure 6.11: a) Excess noise due to classical CH17 on different quantum channels. b) Stokes and anti-stokes of the Raman intensity centred on CH17. c) Excess noise due to classical CH17 and CH18 on different quantum channels.

Using data from our quantum network testbed [149] we collected the average secret key rates and photon counting statistics for the Bob-Feng link over 18.4 hours. When this data is combined with the excessive photon count measurements of Figure 6.11 a) and fed into the analytical expression obtained in Section 6.3.1 we obtain the impact of excessive noise from the classical channel to the secret key rate of the WDM entangled links. With a classical launch power of -26 dBm, we predict QBER will increase by 0.35% and the SKR with co-existence will be 95.3 bits per second – a decrease of <3.8%. At this point we should note that we consider the cumulative effect of the noise photon counts generated across the all 30 channels of the spectrum of the WDM entangled links. To keep the system preforming securely, the QBER should be kept close to 0.05 and the SKR must stay around 90% the original value. This would allow some 2000 extra dark counts per channel to be sent to the users.

6.3.4 Summary

We demonstrated a viability study of quantum-classical coexistence on a 0.8 km deployed SMF part of our previously deployed 8-user quantum network testbed and proved in the form of excess noise measurements that co-existence is feasible on 30 channels on the C-band with a classical channel launching at -26 dBm at F_c = 191.7 THz. This analysis will be used to determine the position of the classical and quantum channels for the coexistence experiment over HCF.

6.4 Coexistence of Entanglement-based Quantum Channel and Classical Channels Enabled by HC-NANF

So far, the coexistence of entanglement-based quantum and classical data channels has been experimentally demonstrated only between two users, Alice and Bob [328, 330]. In [328], the quantum and classical channels excited in the C-band and transmitted over 20 km of SMF in the laboratory. For the classical channels, a tunable laser was used per user at a coexistence power of -27 dBm. The achieved visibility was 76.58% which is insufficient to perform secure key exchange and QKD. Additionally, in [330], different telecommunications bands were used for the classical channel (C-band) and quantum channels (O-band). The quantum channels were transmitted over a 45.6 km deployed fibre while coexisting with a classical channel at 7 dBm launch power. The achieved visibility was 77% in the HV basis and 74% in the DA basis averaging 75.5% which is also insufficient to perform secure key exchange and QKD. In this section, we present the coexistence of four classical channels and four quantum channels over 11.1 km HCF. Due to the high visibility of > 95%, we established a secure key exchange and performed QKD in a 4-user full mesh network. The location of the classical channels is determined based on the analysis in Section 6.3. As demonstrated in Section 6.3 the smaller the wavelength separation between the quantum and the classical channels, the better. Therefore, the classical channels are assigned ITU-T channels 14, 15, 16, and 17, whereas Alice's quantum channels were assigned ITU-T channels 19, 20, and 20. In this configuration, the quantum channels are placed at the Raman spectrum dip, limiting the nonlinear effects.

6.4.1 Experimental System Testbed

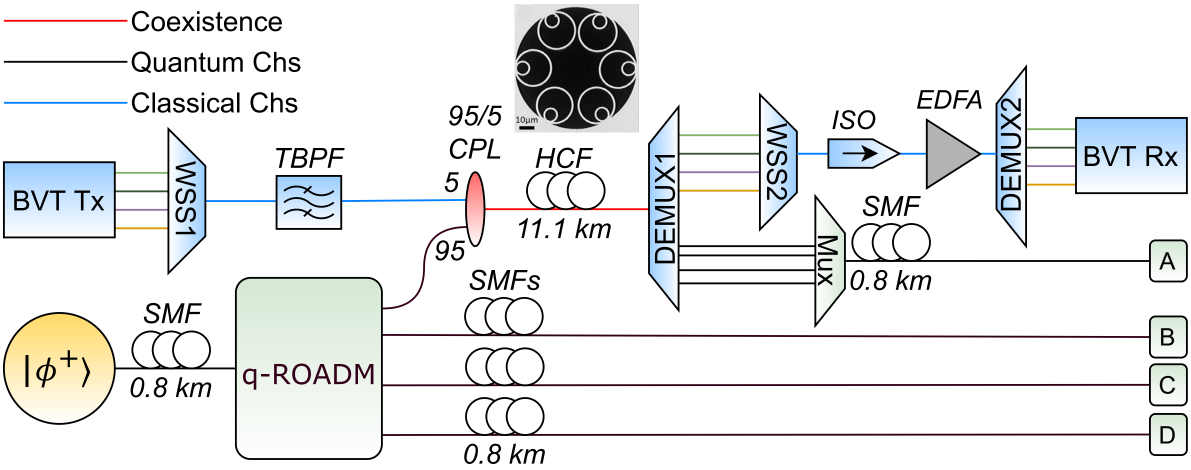


Figure 6.12: Experimental testbed enabling the coexistence of entanglement-based quantum channels and four classical channels.

Figure 6.12 shows a simplified version of the experimental system setup used to demonstrate the coexistence of 4 × 200 Gbps 16-QAM classical channels and four quantum channels over 11.1 km-long HC-NANF. For the classical channels, an optical packet DWDM platform is used with a bandwidth-variable transponder (BVT) similar to the one used in previous experiments. The four coherent output ports are multiplexed using a WSS and further filtered using a tunable band pass filter (TBPF) with 60 dB of isolation. The quantum channels are generated using the same entanglement source in Figure 6.4 and are distributed using the q-ROADM. As explained before, the q-ROADM demultiplex the broadband source into 30 × 100 GHz spacing DWDM channels denoted as λ_i,($i \in [-15, 15]$), where photons in λ_i are correlated to photons in λ_{-i}. An FPC controls the polarisation of each output and allows fibre neutralisation. The FPCs are followed by an optical switch to direct each wavelength to the appropriate port. Finally, DWDM MUXs and WSSs are used to multiplex the quantum channels to the same user. Since we have four users in this experiment, Alice, Bob, Chloe, and Dave, 12 entangled wavelengths (6 pairs) are required to have a full mesh network, a pair per link. Each user is connected to the user module shown in Figure 6.4.

The four quantum wavelengths of Bob, Chloe, and Dave are directly connected from the output of the q-ROADM to the PAM via 0.8 km SMF. However, the four quantum wavelengths of Alice are connected to a 95/5 coupler with the four classical channels. The 95/5 coupler is used as the coexistence stage to combine the quantum and classical channels into a single output. The 5% port is used for the quantum channels to minimise the loss of quantum channels, and the 95% port is used for the classical channels. Although a DWDM filter would have been better to use as the coexistence stage, it is not possible since the four classical channels are combined into a single port, and so are the quantum channels. Alice's four quantum channels and the four classical channels are transmitted through an 11.1 km HCF in a coexistence configuration. The 11.1 km HCF has a total loss of 14.46 dB. DEMUX1 separates the four classical channels from Alice's quantum channels. After the separation, the four classical channels are combined using WSS2, followed by an optical isolator (ISO) and an amplifier. We combine the classical channels to use a single EDFA before separating them for coherent detection at BVT Rx using a 1x4 splitter. The quantum channels are combined using a passive DWDM multiplier before being transmitted over 0.8 km of SMF to the PAM.

6.4.2 Results

shows the SKR vs the source (775 nm laser) pump power in mW. The pump power is adjusted to demonstrate its effect on the network performance and to find the best power in the case of a 3-user network. Increasing the pump power will increase the entangled wavelengths. However, it will simultaneously increase the accidental (noise) and coincidence rates (signal). Therefore for each case, there is a pump power to increase the SKR while keeping the noise at a minimum level. For the case of a 3-user network, we used a pump power of 1.02 mW as shown in Figure 6.13.

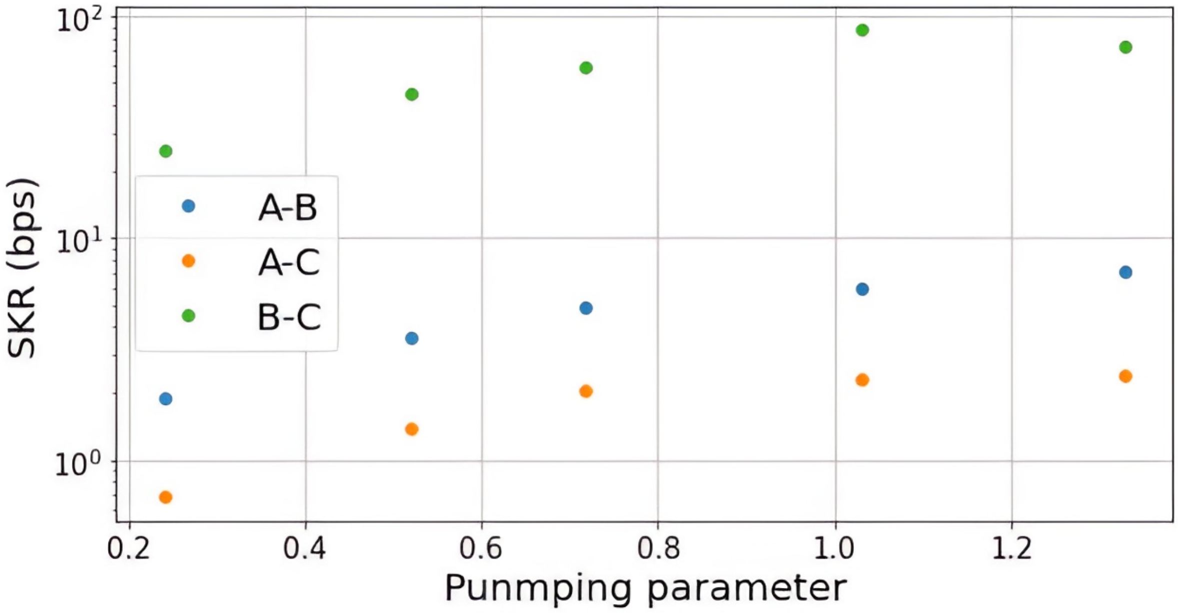


Figure 6.13: SKR vs pump power for 3-user network.

Figure 6.14 shows the SKR stability of 3 links, A-B (blue), A-C (orange), and B-C (green), over 120 minutes. As shown in Figure 6.12, Alice's wavelengths go through the coupler, HCF, demux, and mux, increasing the loss. Therefore, A-B and A-C have a higher loss than B-C, hence a lower SKR. Furthermore, in the q-ROADM, a WSS is used to combine Chloe's wavelengths compared to a passive DWDM for Bob's, and since the WSS has more loss (5 dB) than the passive DWDM (2 dB), the SKR of A-C (2 bps)is lower than the SKR of A-B (7 bps). To summarise, the variation of the key rates of different quantum links is entirely due to the extra losses for each wavelength, with link B-C having the highest SKR at 80 bps.

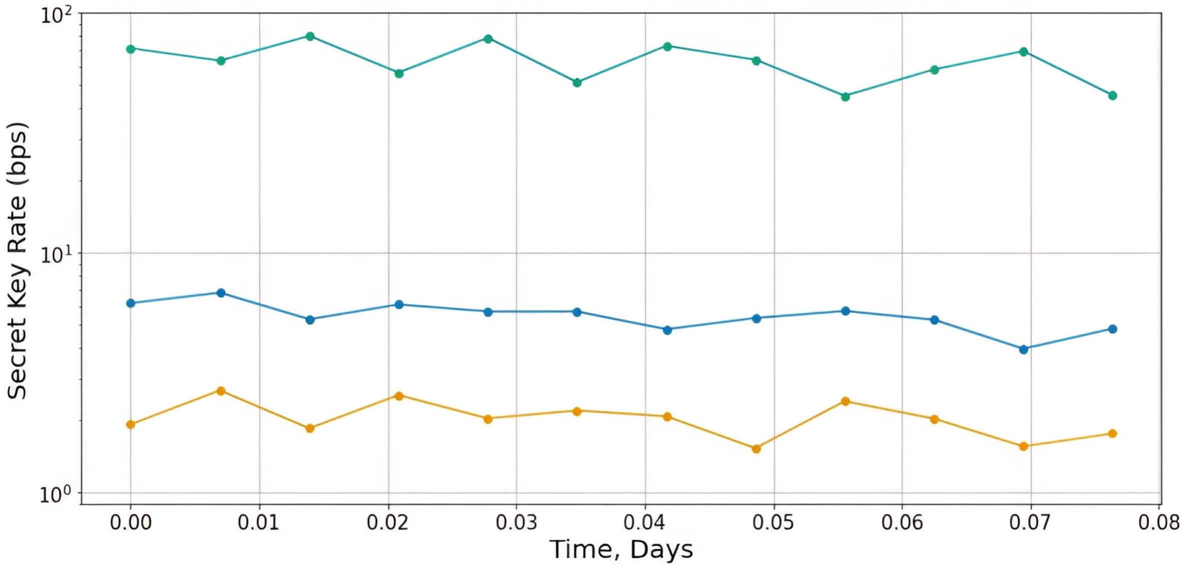
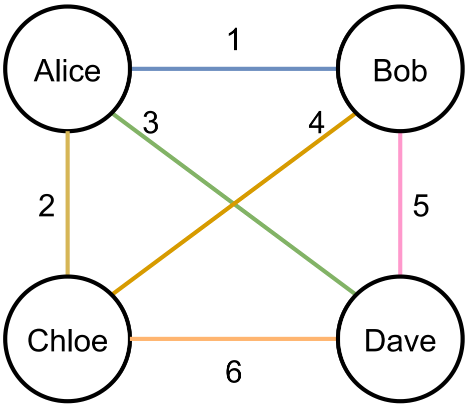


Figure 6.14: Two hours SKR monitoring for 3-user network.

After testing the network for 3-user, we added a fourth user Dave. Figure 6.15 shows the network topology and the wavelength assignment for a full mesh 4-user network. A full mesh 4-user network has 6 links, requiring 12 wavelengths (6 pairs). Since we are using a type-0 entanglement source, λ_i are correlated to photons in λ_{-i}, therefore we used λ_1 to λ_6 and λ_{-1} to λ_{-6}.



Alice	Bob	Chloe	Dave
1	-1	-2	-3
2	4	-4	-5
3	5	6	-6

Figure 6.15: Wavelength assignment for a full mesh 4-user quantum communication network.

Figure 6.16 shows the SKR over 10 mins of data for a full-mesh 4-user network. Due to the higher loss of Alice's link, its SKR is the lowest. Moreover, the SKR of the links A-B, A-C and B-C are lower than the 3-user network (Figure 6.14). This is because, as shown in Figure 6.7 distributing more than one entangled wavelength pair to the same user pairs will not improve the SKR. By adding the user Dave, we are allocating an additional pair per node, decreasing the SKR per link.

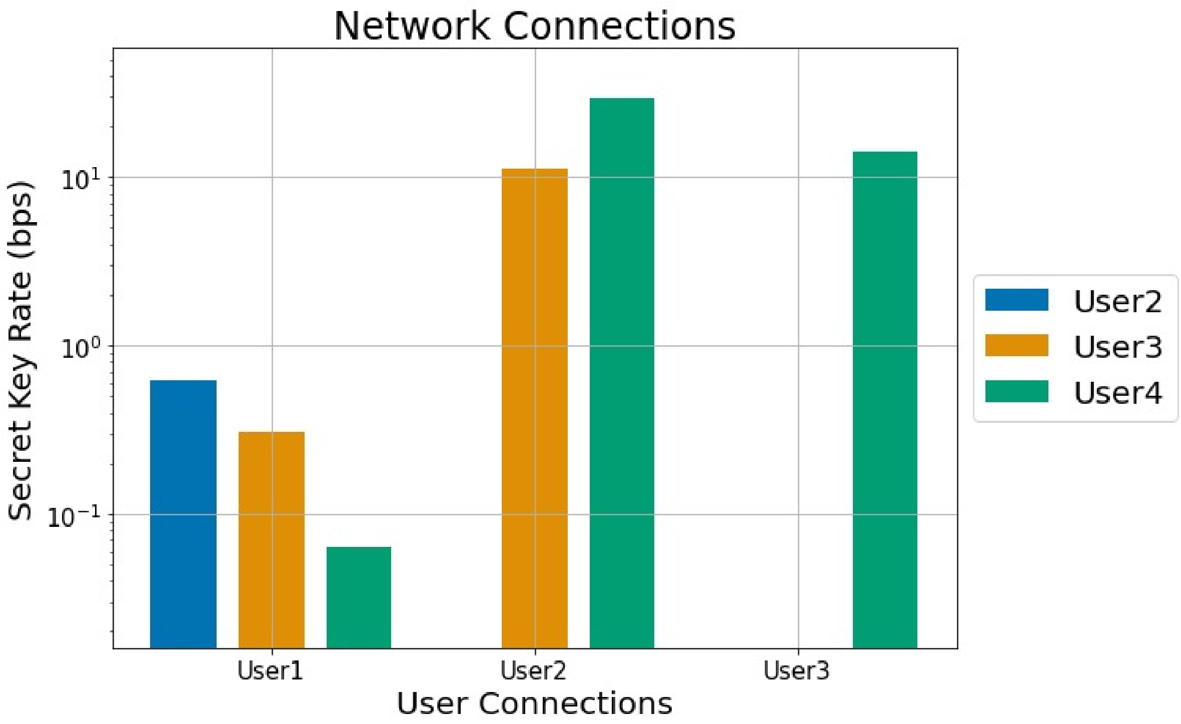


Figure 6.16: Short term SKR analysis for 4-user full mesh network. User1: Alice, user2: Bob, user3: Chloe, user4: Dave.

All the previous results are obtained without the presence of the classical channels. Figure 6.17 shows the SKR stability of all six links over 55 hours while coexisting with four classical channels at a coexistence power of -3 dBm. As shown in Figure 6.17, the SKR is not affected with the coexistence (On), or without the coexistence (Off) of classical and quantum channels throughout the 55 hours. Moreover, we used the highest possible coexistence power at -3 dBm which was limited due to equipment availability. The SKR was preserved during the coexistence due to the ultra-low nonlinear effects in the HCF which are described in detail in the previous chapter, Section 5.2. Furthermore, during the 55-hour period, the SKR was stable which illustrates the polarisation stability of the HCF.

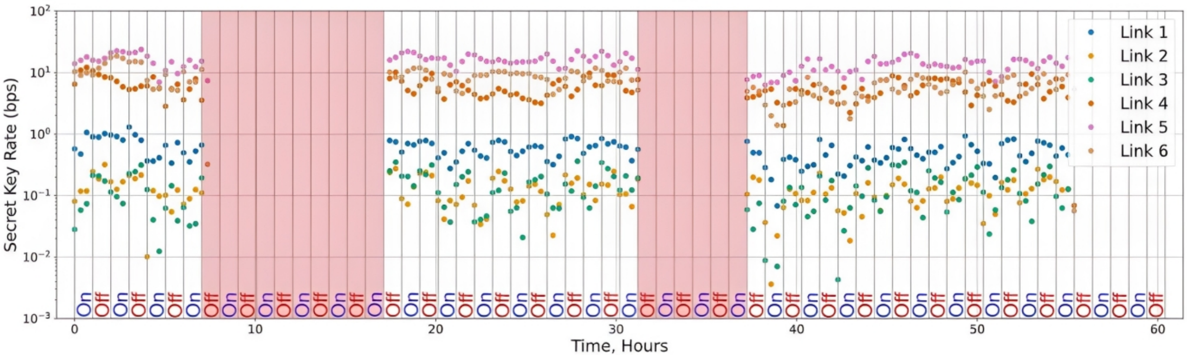


Figure 6.17: Long term (55 hours) SKR monitoring for 4-user full mesh network while coexisting with four classical channels at -3 dBm coexisting power. On: with classical channels (coexistence), off: without classical channels (no coexistence), red space: the detectors were off for cooling.

6.4.3 Summary

The coexistence of four entanglement-based quantum channels and 4 × 200 Gbps 16-QAM classical channels was successfully demonstrated over an 11.1 km long HCF in a 3 and 4-user quantum network. The classical and quantum channels operated in the C-band with a separation of 1.6 nm. The SKR was preserved while coexisting with the classical channels over 55 hours

Chapter 7

Conclusion

This thesis has advanced the application of commercial QKD systems for quantum-secured key exchange in optical networks. We introduced the concept of dynamic QKD networking and demonstrated the concept in deployed fibre links in the city of Bristol. The trusted-node-free network consists of four nodes and uses a software-defined networking controller to provide dynamicity in switching and rerouting. We used commercial QKD devices which employ the BB84 protocol and tested all possible link combinations. As a result, we achieved a SKR of 1762 pbs and a QBER of 1.31% for the link with the lowest optical loss (5.19 dB) and a SKR of 417 pbs and a QBER of 9.42% for the link with highest optical loss (9.42 dB). Furthermore, the additional optical switch at each node did not affect the QKD operation and was realised as a further optical loss. Such dynamicity provides resource optimisation and faster and easier restoration of the QKD link in case of a physical attack.

We further integrated components to the network, such as multiplexers, filters, and demultiplexers, to demonstrate the coexistence of quantum and classical channels over deployed fibre in a dynamic QKD network. By numerical calculation of nonlinear effects, we first determined the best and worst spectral location of the classical channels in terms of their impact on the quantum channel performance. After that, we employed coexistence schemes over all possible link combinations and highlighted the relevant results. For example, when coexisting the quantum channel with one classical channel, we achieved a SKR of 689 pbs and a QBER of 2.35% for the longest link (5.8 km). For the shortest link (0.5 km), we achieved a SKR of 1233 pbs and a QBER of 1.6%. We also coexisted the quantum channel with a different number of classical channels using multi-hop configurations. When using two or more classical channels at a high launch power (7 dBm), the QBER values exceed the threshold of 6%, causing the SKR to be zero bps for all link combinations. This massive drop in the SKR is due to the noise leakage into the Bob DV-QKD from Raman scattering and other nonlinear effects.

Since the coexistence of quantum and classical channels is crucial for the field deployment and broader adoption of QKD technologies, we explored the coexistence in advanced mediums to provide a comprehensive view of different coexistence techniques. The mediums include a 1 km 7-core multicore fibre, a 2 km and 7.7 km hollow core fibres, and a 2.5 m of free space enabled by a fibre-wireless-fibre terminal. For each medium, we tested different scenarios by varying the classical channel launch power, the spectral spacing between quantum and classical channels, and the filtering stages.
For the MCF fibre, we demonstrated the coexistence of 56 16-QAM carrier-grade classical optical channels with a record-high coexistence transmission of 11.2 Tbps. We achieved a QBER of 3.7% and a SKR of 920 bps when launching the QKD channel over the central core. We also tested the coexistence of two QKD systems with 56 classical channels, where one QKD system (QKD1) is configured without classical channels in the central core. Meanwhile, the other QKD system (QKD2) coexists in the same core as the classical channels. When the classical launch power is increased from -22 dBm to -9 dBm, the QBER of the QKD1 is affected by the adjacent cores with classical signal power and its QBER change from 2.6% to 5%. However, the QBER of QKD2 is maintained relatively constant, with an average of 1.7%. Both QKD channels operated successfully over the same MCF, supporting the simultaneous generation of secure keys.
For the HCF fibre, we demonstrated the coexistence in two different experiments. In the first experiments, we demonstrated the coexistence of a quantum channel and 8 16-QAM carrier-grade classical optical channels with a transmission capacity of 1.8 Tbps over a 2 km HCF. Two different sceptical spacing between the quantum and classical channels were tested based on the numerical calculation of nonlinear effects. With a classical coexistence power of 0 dBm, the SKR was preserved in the HCF in the best-case scenario (1.6 nm spacing) and dropped by 10% in the worst-case scenario (8 nm spacing). Using the same spacing and a classical coexistence power of -24 dBm (250 times lower than the power used in HCF). For SMF, the SKR dropped by 73% in the best-case scenario (1.6 nm spacing) and dropped to zero pbs in the worst-case scenario (8 nm spacing). This significant difference in the QKD performance proves the advantage of using HCF in quantum applications. In the second experiment, we demonstrated the coexistence of a quantum channel and 25 10 Gb/s C+L band classical channels over 7.7 km HCF.
We also presented a bidirectional coexistence when including 10GbE key distillation channels. We obtained SKR on the order of 100 bps for an aggregated classical power of 12 dBm of 25 classical channels. For the free-space experiment, we implemented FWF terminals to enable the transmission of a quantum channel and 8 16-QAM carrier-grade classical optical channels over 2.5 m of free space. Similar to the first HCF experiment, we tested two different sceptical spacing and found identical results where the QKD operated better with 1.6 nm spacing compared to 8.8 nm spacing. At a spectral spacing of 0.8 nm, the mean SKR drops by 13% from ≈ 2300 bps to 2000 bps. For the spacing of 8.8 nm, the mean SKR drops by 45% from ≈ 2300 bps to

1250 bps. We also tested the SKR by increasing the link misalignment in the terminals. The SKR decreases abruptly with increasing angular link misalignment and reaches zero bps when the angular link misalignment is bigger than 0.025°. This behaviour is mainly due to the additional fibre coupling losses induced by angular misalignment.

We explored the dynamicity concepts and demonstrated a coexistence scheme using HCF in entanglement-based networks. We first implement an advanced architecture in a multi-protocol 6-user network using q-ROADM to provide flexibility in resource assignment and on-demand allocating of entanglement resources for different network topologies. We demonstrated SKR stability for all 15 links across 9 hours of operation with the highest SKR of 60 bps. We also tested the effect of adding quantum channels to a user and experimentally demonstrated that, unlike classical optical networks, additional quantum channels reduce the SKR from 1136 bps (1 pair) to 262 bps (3 pairs) due to higher increase in the accidental rate compared to the coincidence rate. We finally demonstrated the coexistence of four quantum channels and four classical channels over 11.1 km HCF in a 4-user quantum network. We demonstrated SKR stability for all six links across 55 hours of operation with the highest SKR of 10 bps. Additionally, the SKR stayed contestant during the 55 hours operation with and without the coexistence with the classical channels. These results further show the suitability of using HCF across different quantum technologies.

7.1 Future Work

This thesis highlights the importance of enabling the dynamicity and the coexistence in quantum networks. There are several possibilities where the research studies could be taken onto further steps:

1. Showcase the dynamicity concept in bigger networks with multiple nodes and longer fibre links. Such networks will also require the implementation of a central SDN architecture to control the QKD SDN controller in each node providing a single integrated quantum network.

2. Deploying a coexistence simulation tool for different coexistence mediums in optical networks using the experimental coexistence data. The simulation tool will include a QKD system model, a classical system model, and a coexistence medium model, which can be modified based on the experimental implementation.

3. Further test the implementation of HCF in phase-based protocols like Twin-Field QKD. Preliminary results indicate a slight but visible improvement in the phase noise level exhibited by HC-NANF compared to SMF. This result is promising for the future deployment of HCF in the field and their exploitation for high-fidelity long-distance quantum communications.

4. Implement the coexistence schemes for more QKD protocols and integrate them with cheaper and commercial optical equipment.

Bibliography

[1] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dynamic dv-qkd networking in trusted-node-free software-defined optical networks," *Journal of Lightwave Technology*, vol. 40, no. 17, pp. 5816–5824, 2022.

[2] O. Alia, R. S. Tessinari, S. Bahrani, T. D. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, D. Richardson, F. Poletti, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dv-qkd coexistence with 1.6 tbps classical channels over hollow core fibre," *Journal of Lightwave Technology*, vol. 40, no. 16, pp. 5522–5529, 2022.

[3] A. Schreier, O. Alia, R. Wang, S. Bahrani, R. Singh, G. Faulkner, G. T. Kanellos, R. Nejabati, D. Simeonidou, J. Rarity, and D. O'Brien, "Coexistence of quantum and 1.6 tbit/s classical data over fibre-wireless-fibre terminals," *Journal of Lightwave Technology*, 2022.

[4] M. Peranić, M. Clark, R. Wang, S. Bahrani, O. Alia, S. Wengerowsky, A. Radman, M. Lončarić, M. Stipčević, J. Rarity, *et al.*, "Polarization compensation methods for quantum communication networks," *arXiv preprint arXiv:2208.13584*, 2022.

[5] E. Hugues-Salas, O. Alia, R. Wang, K. Rajkumar, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "11.2 tb/s classical channel coexistence with dv-qkd over a 7-core multicore fiber," *Journal of Lightwave Technology*, vol. 38, no. 18, pp. 5064–5070, 2020.

[6] R. Wang, M. Clark, S. K. Joshi, S. Bahrani, O. Alia, M. Peranić, M. Lončarić, M. Stipčević, *et al.*, "Optimum switching scenario analysis in a dynamic entanglement network," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2023.

[7] M. Minder, S. Albosh, O. Alia, R. Slavik, F. Poletti, G. T. Kanellos, R. Kumar, and M. Lucamarini, "Characterisation of a nested antiresonant nodeless hollow core fibre for phase-based quantum key distribution protocols," in *SPIE PhotoneX*, SPIE, 2022.

[8] O. Alia, A. Schreier, R. Wang, S. Bahrani, R. Singh, G. Faulkner, J. Rarity, D. O'Brien, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Dv-qkd coexistence with 1.6 terabit/s classical channels in free space using fiber-wireless-fiber terminals," in *2022 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2022.

[9] R. Wang, O. Alia, M. Clark, S. Bahrani, S. K. Joshi, D. Aktas, G. T. Kanellos, M. Peranić, M. Lončarić, M. Stipčević, *et al.*, "A dynamic multi-protocol entanglement distribution quantum network," in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2022.

[10] O. Alia, R. S. Tessinari, S. Bahrani, J. Sagar, T. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, *et al.*, "Coexistence analysis of classical channels with dv-qkd over hollow core nested antiresonant nodeless fibre (hc-nanf)," in *Quantum Computing, Communication, and Simulation II*, p. PC1201519, SPIE, 2022.

[11] M. Clark, O. Alia, R. Wang, S. Bahrani, D. Aktas, G. Kanellos, M. Loncaric, Ž. Samec, M. Peranić, A. Radman, *et al.*, "Towards a fully connected many-user entanglement distribution quantum network within deployed telecommunications fibre-optic infrastructure," in *CLEO: QELS_Fundamental Science*, pp. FF4A–6, Optica Publishing Group, 2022.

[12] F. Honz, F. Prawits, O. Alia, H. Sakr, T. Bradley, C. Zhang, R. Slavík, F. Poletti, G. T. Kanellos, R. Nejabati, P. Walther, D. Simeonidou, *et al.*, "Demonstration of 17 λ × 10 gb/s c-band classical / dv-qkd co-existence over hollow-core fiber link," in *2022 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2022.

[13] F. Prawits, F. Honz, O. Alia, H. Sakr, T. Bradley, C. Zhang, R. Slavík, F. Poletti, G. T. Kanellos, R. Nejabati, P. Walther, and D. Simeonidou, "Dv-qkd over bidirectional fiber link in-band co-existence with 25 classical 10 gb/s channels," in *Int. Conf. on Quantum Cryptography (QCrypt)*, pp. 1–3, 2022.

[14] E. Arabul, R. D. Oliveira, R. Wang, O. Alia, G. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of high-speed self-reconfiguration and key slicing for 100 gbps multi-user programmable hardware encryptor," in *2022 European Conference on Optical Communications (ECOC)*, Institute of Electrical and Electronics Engineers (IEEE), 2022.

[15] A. Ntanos, N. K. Lyras, S. Anwar, O. Alia, D. Zavitsanos, G. Giannoulis, A. D. Panagopoulos, G. Kanellos, and H. Avramopoulos, "Large-scale leo satellite constellation to ground qkd links: Feasibility analysis," in *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pp. 288–295, IEEE, 2022.

[16] E. Arabul, R. S. Tessinari, O. Alia, R. Oliveira, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "100 gb/s dynamically programmable sdn-enabled hardware encryptor for optical networks," *Journal of Optical Communications and Networking*, vol. 14, no. 1, pp. A50–A60, 2022.

[17] O. Alia, R. S. Tessinari, T. D. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, D. Richardson, F. Poletti, *et al.*, "1.6 tbps classical channel coexistence with dv-qkd over hollow core nested antiresonant nodeless fibre (hc-nanf)," in *2021 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2021.

[18] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Wavelength resources management and switching of active entanglement distribution circuits in optical networks," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021.

[19] M. J. Clark, O. Alia, R. S. Tessinari, R. Wang, D. Aktas, G. T. Kanellos, J. G. Rarity, R. Nejabati, D. E. Simeonidou, and S. K. Joshi, "Towards a quantum network within deployed telecommunications fibre-optic infrastructure," in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, vol. 11881, p. 118810D, SPIE, 2021.

[20] R. S. Tessinari, O. Alia, S. K. Joshi, D. Aktas, M. Clark, E. Hugues-Salas, G. T. Kanellos, J. Rarity, R. Nejabati, and D. Simeonidou, "Towards co-existence of 100 gbps classical channel within a wdm quantum entanglement network," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021.

[21] R. S. Tessinari, E. Arabul, O. Alia, A. S. Muqaddas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Demonstration of a dynamic qkd network control using a qkd-aware sdn application over a programmable hardware encryptor," in *Optical Fiber Communication Conference*, pp. M2B–3, Optical Society of America, 2021.

[22] E. Arabul, R. S. Tessinari, O. Alia, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of programmable 100 gb/s sdn-enabled encryptors/decryptors for qkd networks," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2021.

[23] G. Kanellos, O. Alia, E. Hugues-Salas, R. S. Tessinari, R. Wang, R. Nejabati, and D. Simeonidou, "Dynamic optical interconnects for quantum secure distributed nodes and quantum processing," in *2020 IEEE Photonics Conference (IPC)*, pp. 1–2, IEEE, 2020.

[24] R. S. Tessinari, A. Bravalheri, E. Hugues-Salas, R. Collins, D. Aktas, R. S. Guimaraes, O. Alia, J. Rarity, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Field trial of dynamic dv-qkd networking in the sdn-controlled fully-meshed optical metro network of the bristol city 5guk test network," in *45th European Conference on Optical Communication (ECOC 2019)*, pp. 1–4, 2019.

[25] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[26] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[27] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, “Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets,” *Nature*, vol. 549, no. 7671, pp. 242–246, 2017.

[28] R. Orús, S. Mugel, and E. Lizaso, “Quantum computing for finance: Overview and prospects,” *Reviews in Physics*, vol. 4, p. 100028, 2019.

[29] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[30] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *arXiv preprint arXiv:2003.06557*, 2020.

[31] A. K. Ekert, “Quantum cryptography and bell’s theorem,” in *Quantum Measurements in Optics*, pp. 413–418, Springer, 1992.

[32] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[33] S. Singh, “The code book,” vol. 7, Doubleday New York, 1999.

[34] F. Miller, “Telegraphic code to insure privacy and secrecy in the transmission of telegrams,” CM Cornwell, 1882.

[35] G. S. Vernam, “Secret signaling system,” 1919. United States Patent 1,310,719.

[36] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[37] N. T. Courtois and J. Pieprzyk, “Cryptanalysis of block ciphers with overdefined systems of equations,” in *International conference on the theory and application of cryptology and information security*, pp. 267–287, Springer, 2002.

[38] W. Diffie and M. Hellman, “Special feature exhaustive cryptanalysis of the nbs data encryption standard,” *Computer*, vol. 10, no. 6, pp. 74–84, 1977.

[39] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, “Advanced encryption standard (aes),” 2001-11-26 2001.

[40] W. Diffie and M. E. Hellman, “New directions in cryptography,” in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 365–390, 2022.

[41] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[42] J. H. Ellis, “The possibility of secure non-secret digital encryption,” *UK Communications Electronics Security Group*, vol. 8, 1970.

[43] M. J. Williamson, “Non–secret encryption using a finite field,” tech. rep., Technical report, CESG, 1974.

[44] S. I. Batool and H. M. Waseem, “A novel image encryption scheme based on arnold scrambling and lucas series,” *Multimedia tools and applications*, vol. 78, no. 19, pp. 27611–27637, 2019.

[45] C. C. Cocks, “A note on non-secret encryption,” *CESG Memo*, 1973.

[46] S. Goldwasser and S. Micali, “Probabilistic encryption & how to play mental poker keeping secret all partial information,” in *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pp. 365–377, 1982.

[47] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[48] National Cyber Security Centre (NCSC), “Quantum security technologies.” `https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies/`, 2020. "Accessed on 04.10.2022".

[49] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography*, pp. 1–14, Springer, 2009.

[50] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[51] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, “Report on post-quantum cryptography,” vol. 12, US Department of Commerce, National Institute of Standards and Technology . . . , 2016.

[52] S. A. Käppler and B. Schneider, “Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms,” *Proceedings of the Society*, vol. 84, pp. 61–71, 2022.

[53] B. Schneier, “Nist’s post-quantum cryptography standards competition,” *IEEE Security & Privacy*, vol. 20, no. 5, pp. 107–108, 2022.

[54] NIST, “Announcing request for nominations for public-key post-quantum cryptographic algorithms.” `https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms/`, Dec. 2016. "Accessed on 15.08.2022".

[55] NIST, “Post-quantum cryptography - round 1 submissions.” `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Round-1-Submissions`, Jan. 2016. "Accessed on 15.08.2022".

[56] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and Y.-K. Liu, “Status report on the first round of the nist post-quantum cryptography standardization process,” 2019-01-31 00:01:00 2019.

[57] NIST, “Post-quantum cryptography - round 2 submissions.” `https://https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions`, 2019. "Accessed on 15.08.2022".

[58] NIST, “Post-quantum cryptography - round 3 submissions.” `https://https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`, 2020. "Accessed on 15.08.2022".

[59] W. Beullens, “Improved cryptanalysis of uov and rainbow,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 348–373, Springer, 2021.

[60] The Center of Encryption and Information Security – MATZOV, “Report on the security of lwe: Improved dual lattice attack.” `https://marketing.idquantique.com/acton/attachment/11868/f-0587a79f-5592-47fe-9bdf-a3f3e7f7d802/1/-/-/-/-/Report%20on%20the%20Security%20of%20LWE.pdf`, 2022. "Accessed on 15.08.2022".

[61] P. Busch, T. Heinonen, and P. Lahti, “Heisenberg’s uncertainty principle,” *Physics Reports*, vol. 452, no. 6, pp. 155–176, 2007.

[62] J. Oppenheim and S. Wehner, “The uncertainty principle determines the nonlocality of quantum mechanics,” *Science*, vol. 330, no. 6007, pp. 1072–1074, 2010.

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

[64] R. Van Meter, “Quantum background,” in *Quantum Networking*, ch. 2, pp. 23–54, John Wiley & Sons, Ltd, 2014.

[65] J. R. Friedman, V. Patel, W. Chen, S. K. Tolpygo, and J. E. Lukens, “Quantum superposition of distinct macroscopic states,” *Nature*, vol. 406, no. 6791, pp. 43–46, 2000.

[66] O. Alter and Y. Yamamoto, “Quantum measurement of a single system,” 2002.

[67] J. Preskill, “Lecture notes for physics 229: Quantum information and computation,” *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.

[68] J. Preskill, “Lecture notes for physics 219: Quantum computation,” *Caltech Lecture Notes*, p. 7, 1999.

[69] H. Semenenko, “Advances in chip-based quantum key distribution,” PhD thesis, University of Bristol. 2020.

[70] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, “Factorization of a 768-bit rsa modulus,” in *Advances in Cryptology – CRYPTO 2010* (T. Rabin, ed.), (Berlin, Heidelberg), pp. 333–350, Springer Berlin Heidelberg, 2010.

[71] D. Bacon and W. van Dam, “Recent progress in quantum algorithms,” *Commun. ACM*, vol. 53, pp. 84–93, Feb. 2010.

[72] K. L. Brown, W. J. Munro, and V. M. Kendon, “Using quantum computers for quantum simulation,” *Entropy*, vol. 12, no. 11, pp. 2268–2307, 2010.

[73] I. Buluta and F. Nori, “Quantum simulators,” *Science*, vol. 326, no. 5949, pp. 108–111, 2009.

[74] S. Lloyd, M. Mohseni, and P. Rebentrost, “Quantum algorithms for supervised and unsupervised machine learning,” 2013.

[75] A. W. Harrow, A. Hassidim, and S. Lloyd, “Quantum algorithm for linear systems of equations,” *Phys. Rev. Lett.*, vol. 103, p. 150502, Oct 2009.

[76] O. Regev, “Quantum computation and lattice problems,” in *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS ’02, (Washington, DC, USA), pp. 520–529, IEEE Computer Society, 2002.

[77] J. Kim, S. Somani, and Y. Yamamoto, “Single-photon detection with visible-light photon counter,” in *Nonclassical Light from Semiconductor Lasers and LEDs*, pp. 179–205, Springer, 2001.

[78] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," *Physical Review A*, vol. 60, no. 2, p. R773, 1999.

[79] M. Fiorentino, P. L. Voss, J. E. Sharping, and P. Kumar, "All-fiber photon-pair source for quantum communications," *IEEE Photonics Technology Letters*, vol. 14, no. 7, pp. 983–985, 2002.

[80] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, "Entangled photon-pair sources based on three-wave mixing in bulk crystals," *Review of Scientific Instruments*, vol. 92, no. 4, p. 041101, 2021.

[81] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature photonics*, vol. 3, no. 12, p. 696, 2009.

[82] A. I. Lvovsky, H. Hansen, T. Aichele, O. Benson, J. Mlynek, and S. Schiller, "Quantum state reconstruction of the single-photon fock state," *Physical Review Letters*, vol. 87, no. 5, p. 050402, 2001.

[83] Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, "Practical gigahertz quantum key distribution based on avalanche photodiodes," *New Journal of Physics*, vol. 11, no. 4, p. 045019, 2009.

[84] G.-J. Fan-Yuan, J. Teng, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, "Optimizing single-photon avalanche photodiodes for dynamic quantum key distribution networks," *Physical Review Applied*, vol. 13, no. 5, p. 054027, 2020.

[85] Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz quantum key distribution with ingaas avalanche photodiodes," *Applied Physics Letters*, vol. 92, no. 20, p. 201104, 2008.

[86] IDQuantiqueSA, "Id230 infrared single-photon detector." `https://www.idquantique.com/quantum-sensing/products/id230//`, 2022. "Accessed on 15.08.2022".

[87] E. E. Wollman, V. B. Verma, A. D. Beyer, R. M. Briggs, B. Korzh, J. P. Allmaras, F. Marsili, A. E. Lita, R. Mirin, S. Nam, *et al.*, "Uv superconducting nanowire single-photon detectors with high efficiency, low noise, and 4 k operating temperature," *Optics express*, vol. 25, no. 22, pp. 26792–26801, 2017.

[88] H. P. Yuen and V. W. Chan, "Noise in homodyne and heterodyne detection," *Optics letters*, vol. 8, no. 3, pp. 177–179, 1983.

[89] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, p. 16021, 2016.

[90] I. Vasyltsov, E. Hambardzumyan, Y.-S. Kim, and B. Karpinskyy, “Fast digital trng based on metastable ring oscillator,” in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 164–180, Springer, 2008.

[91] M. Bakiri, C. Guyeux, J.-F. Couchot, L. Marangio, and S. Galatolo, “A hardware and secure pseudorandom generator for constrained devices,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3754–3765, 2018.

[92] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Physical review*, vol. 47, no. 10, p. 777, 1935.

[93] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[94] A. Aspect, “Bell’s inequality test: more ideal than ever,” *Nature*, vol. 398, no. 6724, pp. 189–190, 1999.

[95] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell’s inequalities,” *Physical review letters*, vol. 49, no. 2, p. 91, 1982.

[96] A. Aspect, P. Grangier, and G. Roger, “Experimental tests of realistic local theories via bell’s theorem,” *Physical review letters*, vol. 47, no. 7, p. 460, 1981.

[97] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of bell’s inequalities using time-varying analyzers,” *Physical review letters*, vol. 49, no. 25, p. 1804, 1982.

[98] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[99] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” *Physical review letters*, vol. 68, no. 5, p. 557, 1992.

[100] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[101] 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, p. 194108, 2005.

[102] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” *Physical review letters*, vol. 89, no. 3, p. 037902, 2002.

[103] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, “Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations,” *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.

[104] T. C. Ralph, “Continuous variable quantum cryptography,” *Physical Review A*, vol. 61, no. 1, p. 010303, 1999.

[105] M. Hillery, “Quantum cryptography with squeezed states,” *Physical Review A*, vol. 61, no. 2, p. 022309, 2000.

[106] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, “Advances in quantum cryptography,” *Advances in optics and photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[107] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[108] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, “Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2018.

[109] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, *et al.*, “Quantum key distribution: a networking perspective,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[110] R. Van Meter and S. J. Devitt, “The path to scalable distributed quantum computing,” *Computer*, vol. 49, no. 9, pp. 31–42, 2016.

[111] HUBER SUHNER, “Series 7000 - 384x384 port software-defined optical circuit switch.” `https://www.polatis.com/series-7000-384x384-port-software-controlled-optical-circuit-switch-\sdn-enabled.asp`, 2022. "Accessed on 15.08.2022".

[112] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, “The evolution of quantum key distribution networks: On the road to the qinternet,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[113] A. K. Majumdar, “Chapter 2 - basics of worldwide broadband wireless access independent of terrestrial limitations,” in *Optical Wireless Communications for Broadband Global Internet Connectivity* (A. K. Majumdar, ed.), pp. 5–38, Elsevier, 2019.

[114] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Large scale quantum key distribution: challenges and solutions,” *Optics express*, vol. 26, no. 18, pp. 24260–24273, 2018.

[115] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[116] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[117] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. J. Shields, “Experimental quantum key distribution beyond the repeaterless secret key capacity,” *Nature Photonics*, vol. 13, no. 5, pp. 334–338, 2019.

[118] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, “600-km repeater-like quantum communications with dual-band stabilization,” *Nature Photonics*, vol. 15, no. 7, pp. 530–535, 2021.

[119] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, *et al.*, “Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,” *Physical review letters*, vol. 124, no. 7, p. 070501, 2020.

[120] C. Elliott, D. Pearson, and G. Troxel, “Quantum cryptography in practice,” in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 227–238, 2003.

[121] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, “Current status of the darpa quantum network,” in *Quantum Information and computation III*, vol. 5815, pp. 138–149, SPIE, 2005.

[122] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, “The secoqc quantum key distribution network in vienna,” *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[123] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, *et al.*, “Secoqc white paper on quantum key distribution and cryptography (2007),” *arXiv preprint quant-ph/0701168*, 2007.

[124] A. Poppe, M. Peev, and O. Maurhart, “Outline of the secoqc quantum-key-distribution network in vienna,” *International Journal of Quantum Information*, vol. 6, no. 02, pp. 209–218, 2008.

[125] M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future european quantum key distribution network," *Security and Communication Networks*, vol. 1, no. 1, pp. 57–74, 2008.

[126] 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. 10387–10409, 2011.

[127] M. Sasaki, M. Fujiwra, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, *et al.*, "Tokyo qkd network and the evolution to secure photonic network," in *CLEO: Science and Innovations*, p. JTuC1, Optical Society of America, 2011.

[128] V. Martin, A. Aguado, P. Salas, A. Sanz, J. Brito, D. R. Lopez, V. López, A. Pastor, J. Folgueira, H. Brunner, *et al.*, "The madrid quantum network: a quantum-classical integrated infrastructure," in *Photonic Networks and Devices*, pp. QtW3E–5, Optical Society of America, 2019.

[129] A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martin, "The engineering of software-defined quantum key distribution networks," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 20–26, 2019.

[130] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, *et al.*, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, 2019.

[131] C. Elliott, "Building the quantum network," *New Journal of Physics*, vol. 4, no. 1, p. 46, 2002.

[132] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, *et al.*, "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[133] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[134] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *JOSA B*, vol. 27, no. 6, pp. A185–A188, 2010.

[135] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, *et al.*, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, vol. 54, no. 17, pp. 2991–2997, 2009.

[136] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Optics express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[137] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "Qkd in standard optical telecommunications networks," in *International Conference on Quantum Comunication and Quantum Networking*, pp. 142–149, Springer, 2009.

[138] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, *et al.*, "Field test of wavelength-saving quantum key distribution network," *Optics letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[139] A. Morrow, D. Hayford, and M. Legré, "Battelle qkd test bed," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pp. 162–166, IEEE, 2012.

[140] N. Walenta, D. Caselunghe, S. Chuard, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legré, T. McCandlish, *et al.*, "Towards a north american qkd backbone with certifiable security," *Proc. Qcrypt*, pp. 1–3, 2015.

[141] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, "Quantum metropolitan optical network based on wavelength division multiplexing," *Optics express*, vol. 22, no. 2, pp. 1576–1593, 2014.

[142] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Physical Review X*, vol. 6, no. 1, p. 011024, 2016.

[143] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," *Optics letters*, vol. 41, no. 15, pp. 3511–3514, 2016.

[144] O. Bannik, V. Chistyakov, L. Gilyazov, K. Melnik, A. Vasiliev, N. Arslanov, A. Gaidash, A. Kozubov, V. Egorov, S. Kozlov, *et al.*, "Multinode subcarrier wave quantum communication network," in *Proc. 7th Int. Conf. Quantum Crypt.*, pp. 1–2, 2017.

[145] T. Kim and S. Kwak, "Development of quantum technologies at sk telecom.," *AAPPS Bulletin*, vol. 26, no. 6, 2016.

[146] T. Kim, "Status of qkd system deployment and ion trap development at sk telecom," in *Proc. Relativistic Quantum Inf. North*, 2017.

[147] E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. Trushechkin, *et al.*, "Demonstration

of a quantum key distribution network in urban fibre-optic communication lines," *Quantum Electronics*, vol. 47, no. 9, p. 798, 2017.

[148] A. Aguado, V. López, J. P. Brito, A. Pastor, D. R. López, and V. Martin, "Enabling quantum key distribution networks via software-defined networking," in *2020 International Conference on Optical Network Design and Modeling (ONDM)*, pp. 1–5, IEEE, 2020.

[149] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, *et al.*, "A trusted node–free eight-user metropolitan quantum communication network," *Science advances*, vol. 6, no. 36, p. eaba0959, 2020.

[150] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, *et al.*, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information*, vol. 7, no. 1, pp. 1–6, 2021.

[151] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[152] IDQuantiqueSA, "Clavis3 qkd platform." `https://www.idquantique.com/quantum-safe-security/products/clavis3-qkd-platform-rd/`, May 2022. "Accessed on 15.08.2022".

[153] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[154] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Optics express*, vol. 22, no. 18, pp. 21739–21756, 2014.

[155] Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, "Quantum information research in china," *Quantum Science and Technology*, vol. 4, no. 4, p. 040503, 2019.

[156] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, "Satellite-relayed intercontinental quantum network," *Physical review letters*, vol. 120, no. 3, p. 030501, 2018.

[157] A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, and A. Lord, "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5× 100g dwdm transmission system," in *45th European Conference on Optical Communication (ECOC 2019)*, pp. 1–4, IET, 2019.

[158] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, no. 8, pp. 570–575, 2021.

[159] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, *et al.*, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Optics Express*, vol. 20, no. 13, pp. 14030–14041, 2012.

[160] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," *arXiv preprint arXiv:1305.0305*, 2013.

[161] A. Aguado, V. Martin, D. Lopez, M. Peev, J. Martinez-Mateo, J. Rosales, F. de la Iglesia, M. Gomez, E. Hugues-Salas, A. Lord, *et al.*, "Quantum-aware software defined networks," in *Int. Conf. on Quantum Cryptography (QCrypt)*, 2016.

[162] Y. Cao, Y. Zhao, R. Lin, X. Yu, J. Zhang, and J. Chen, "Multi-tenant secret-key assignment over quantum key distribution networks," *Optics Express*, vol. 27, no. 3, pp. 2544–2561, 2019.

[163] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Sdqaas: Software defined networking for quantum key distribution as a service," *Optics Express*, vol. 27, no. 5, pp. 6892–6909, 2019.

[164] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *JOSA B*, vol. 36, no. 3, pp. B31–B40, 2019.

[165] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, no. 6, pp. 1591–1601, 2009.

[166] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (kod) for software-defined optical networks secured by quantum key distribution (qkd)," *Optics express*, vol. 25, no. 22, pp. 26453–26467, 2017.

[167] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *Journal of Optical Communications and Networking*, vol. 9, no. 11, pp. 995–1004, 2017.

[168] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, *et al.*, "Quantum key distribution network for multiple applications," *Quantum Science and Technology*, vol. 2, no. 3, p. 034003, 2017.

[169] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, “Resource allocation in optical networks secured by quantum key distribution,” *IEEE Communications Magazine*, vol. 56, no. 8, pp. 130–137, 2018.

[170] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, “Kaas: Key as a service over quantum key distribution integrated optical networks,” *IEEE Communications Magazine*, vol. 57, no. 5, pp. 152–159, 2019.

[171] P. Knight and I. Walmsley, “Uk national quantum technology programme,” *Quantum Science and Technology*, vol. 4, no. 4, p. 040502, 2019.

[172] IDQuantiqueSA, “Id quantique cerberis3 qkd system.” `https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system`, 2022. "Accessed on 15.08.2022".

[173] 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.

[174] HUBER SUHNER, “Polatis technology - directlight beam-steering all-optical switch.” `https://www.polatis.com/polatis-all-optical-switch-technology-lowest-loss-highest-performance\-directlight-beam-steering.asp`, 2022. "Accessed on 15.08.2022".

[175] A. Price, “Pragmatic quantum cryptography in next-generation photonic networks,” PhD thesis, University of Bristol. 2019.

[176] T. Truex, A. A. Bent, and N. W. Hagood, “Beam steering optical switch fabric utilizing piezoelectric actuation technology,” in *Proc. NFOEC*, Citeseer, 2003.

[177] T. Gerard, “Optical switching for scalable data centre networks,” PhD thesis, UCL (University College London). 2021.

[178] R. Ryf, J. Kim, J. Hickey, A. Gnauck, D. Carr, F. Pardo, C. Bolle, R. Frahm, N. Basavanhally, C. Yoh, *et al.*, “1296-port mems transparent optical crossconnect with 2.07 petabit/s switch capacity,” in *OFC 2001. Optical Fiber Communication Conference and Exhibit. Technical Digest Postconference Edition (IEEE Cat. 01CH37171)*, pp. PD28–PD28, IEEE, 2001.

[179] R. Collins and D. Aktas, “Qcomms qkd software toolkit,” *Journal of Open Source Software*, vol. 4, no. 38, p. 1119, 2019.

[180] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, “Monitoring and physical-layer attack mitigation in sdn-controlled quantum key

distribution networks," *Journal of Optical Communications and Networking*, vol. 11, no. 2, pp. A209–A218, 2019.

[181] G. P. Agrawal, "Multichannel systems," in *Fiber-optic communication systems*, pp. 223–294, John Wiley & Sons, 2012.

[182] A. R. Chraplyvy, "Limitations on lightwave communications imposed by optical-fiber nonlinearities," *Journal of Lightwave Technology*, vol. 8, no. 10, pp. 1548–1557, 1990.

[183] 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*, p. OTuJ7, Optica Publishing Group, 2006.

[184] 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.

[185] P. Eraerds, N. Walenta, M. Legré, 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.

[186] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, 2 2014.

[187] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[188] I. Mandelbaum and M. Bolshtyansky, "Raman amplifier model in single-mode optical fiber," *IEEE Photonics Technology Letters*, vol. 15, no. 12, pp. 1704–1706, 2003.

[189] 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.

[190] G. P. Agrawal, "Nonlinear fiber optics," in *Nonlinear Science at the Dawn of the 21st Century*, pp. 195–211, Springer, 2000.

[191] F. Forghieri, R. Tkach, and A. Chraplyvy, "Fiber nonlinearities and their impact on transmission systems," *Optical Fiber Telecommunications IIIA*, vol. 1, 1997.

[192] M. F. Uddin, A. N. Doulah, A. Hossain, M. Z. Alam, and M. N. Islam, “Reduction of four wave mixing effect in an optical wdm system by controlling channel spacing and chromatic dispersion,” *J. Optical Engineering*, vol. 42, no. 9, pp. 2761–2767, 2003.

[193] T. Numai and O. Kubota, “Analysis of repeated unequally spaced channels for fdm lightwave systems,” *Journal of Lightwave Technology*, vol. 18, no. 5, p. 656, 2000.

[194] F. Forghieri, R. W. Tkach, A. R. Chraplyvy, and D. Marcuse, “Reduction of four-wave mixing crosstalk in wdm systems using unequally spaced channels,” *IEEE Photonics Technology Letters*, vol. 6, no. 6, pp. 754–756, 1994.

[195] S. Bahrani, M. Razavi, and J. A. Salehi, “Wavelength assignment in hybrid quantum-classical networks,” *Scientific reports*, vol. 8, no. 1, pp. 1–13, 2018.

[196] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, and D. Simeonidou, “Field-trial of machine learning-assisted quantum key distribution (qkd) networking with sdn,” in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, IEEE, 2018.

[197] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, “Resource optimization in quantum access networks,” in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 7988–7992, IEEE, 2019.

[198] Corning, “Corning smf-28 optical fiber product information.” PI1036, Available: `http://www.photonics.byu.edu/FiberOpticConnectors.parts/images/smf28.pdf`, 2022. "Accessed on 15.08.2022".

[199] Facebook Engineering, “An open approach for switching, routing, and transport.” `https://engineering.fb.com/2016/11/01/connectivity/an-open-approach-for-switching-routing-and-transport/`, 2016. "Accessed on 15.08.2022".

[200] EXFO, “Xtm-50 - tunable filter with adjustable bandwidth.” `https://www.exfo.com/en/products/lab-manufacturing-testing/tunable-filters/xtm-50/`, 2022. "Accessed on 21.08.2022".

[201] II-VI, “Waveshaper® 16000a reconfigurable optical processor.” `https://ii-vi.com/product/waveshaper-16000a-reconfigurable-optical-processor/`, 2022. "Accessed on 21.08.2022".

[202] D. Vettese, “Liquid crystal on silicon,” *Nature Photonics*, vol. 4, no. 11, pp. 752–754, 2010.

[203] 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 *The 17th Annual Meeting of the IEEELasers and Electro-Optics Society, 2004. LEOS 2004.*, vol. 2, pp. 491–492, IEEE, 2004.

[204] N. Nweke, P. Toliver, R. Runser, S. McNown, J. Khurgin, T. Chapuran, M. Goodman, R. Hughes, C. Peterson, K. McCabe, *et al.*, "Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels," *Applied Physics Letters*, vol. 87, no. 17, p. 174103, 2005.

[205] R. J. Runser, T. Chapuran, P. Toliver, M. Goodman, J. Jackel, N. Nweke, S. McNown, R. Hughes, C. Peterson, K. McCabe, *et al.*, "Demonstration of 1.3 μm quantum key distribution (qkd) compatibility with 1.5 μm metropolitan wavelength division multiplexed (wdm) systems," in *Optical Fiber Communication Conference*, p. OWI2, Optica Publishing Group, 2005.

[206] N. Nweke, R. Runser, S. McNown, J. Khurgin, T. Chapuran, P. Toliver, M. Goodman, J. Jackel, R. Hughes, C. Peterson, *et al.*, "Edfa bypass and filtering architecture enabling qkd+ wdm coexistence on mid-span amplified links," in *Conference on Lasers and Electro-Optics*, p. CWQ7, Optical Society of America, 2006.

[207] 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.

[208] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable qkd with intense dwdm classical channels," *New Journal of Physics*, vol. 17, no. 4, p. 043027, 2015.

[209] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 mbps secure key rate," *Optics express*, vol. 23, no. 13, pp. 17511–17519, 2015.

[210] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, p. 081108, 2015.

[211] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, *et al.*, "Ultra-high bandwidth quantum secured data transmission," *Scientific reports*, vol. 6, no. 1, pp. 1–6, 2016.

[212] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, *et al.*, "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," *Physical Review A*, vol. 95, no. 1, p. 012301, 2017.

[213] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, 2017.

[214] F. Karinou, L. Comandar, H. Brunner, D. Hillerkuss, F. Fung, S. Bettelli, S. Mikroulis, D. Wang, Q. Yi, M. Kuschnerov, *et al.*, "Experimental evaluation of the impairments on a qkd system in a 20-channel wdm co-existence scheme," in *2017 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pp. 145–146, IEEE, 2017.

[215] T. A. Eriksson, T. Hirano, M. Ono, M. Fujiwara, R. Namiki, K.-i. Yoshino, A. Tajima, M. Takeoka, and M. Sasaki, "Coexistence of continuous variable quantum key distribution and 7× 12.5 gbit/s classical channels," in *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pp. 71–72, IEEE, 2018.

[216] T. A. Eriksson, T. Hirano, G. Rademacher, B. J. Puttnam, R. S. Luis, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, *et al.*, "Joint propagation of continuous variable quantum key distribution and 18×24.5 gbaud pm-16qam channels," in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, IEEE, 2018.

[217] F. Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, *et al.*, "Toward the integration of cv quantum key distribution in deployed optical networks," *IEEE Photonics Technology Letters*, vol. 30, no. 7, pp. 650–653, 2018.

[218] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels," *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[219] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, "Experimental investigation of heterodyne quantum key distribution in the s-band embedded in a commercial dwdm system," in *Optical Fiber Communication Conference*, pp. Th1J–3, Optical Society of America, 2019.

[220] R. Valivarthi, P. Umesh, C. John, K. A. Owen, V. B. Verma, S. W. Nam, D. Oblak, Q. Zhou, and W. Tittel, "Measurement-device-independent quantum key distribution coexisting with classical communication," *Quantum Science and Technology*, vol. 4, no. 4, p. 045002, 2019.

[221] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Optics express*, vol. 28, no. 10, pp. 14547–14559, 2020.

[222] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "Spectrally-shaped continuous-variable qkd operating at 500 mhz over an optical pipe lit by 11 dwdm channels," in *Optical Fiber Communication Conference*, pp. T3D–4, Optica Publishing Group, 2020.

[223] 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. 11354–11360, 2008.

[224] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, *et al.*, "Field trial of a quantum secured 10 gb/s dwdm transmission system over a single installed fiber," *Optics express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[225] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, pp. 6010–6020, Mar 2018.

[226] R. Wang, R. S. Tessinari, E. Hugues-Salas, A. Bravalheri, N. Uniyal, A. S. Muqaddas, R. S. Guimaraes, T. Diallo, S. Moazzeni, Q. Wang, *et al.*, "End-to-end quantum secured inter-domain 5g service orchestration over dynamically switched flex-grid optical networks enabled by a q-roadm," *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 139–149, 2019.

[227] O. Amer, V. Garg, and W. O. Krawec, "An introduction to practical quantum key distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30–55, 2021.

[228] M. Travagnin and A. Lewis, "Quantum key distribution in-field implementations: technology assessment of qkd deployments," *EUR 29865 EN, Publications Office of the European Union, Luxembourg*, vol. 1, 2019.

[229] BT Newsroom, "Bt and toshiba install uk's first quantum-secure industrial network between key uk smart production facilities." `https://newsroom.bt.com/bt-and-toshiba-install-uks-first-quantum-secure-industrial-network-between-key-uk-smart-production-facilities//`, Oct. 2022. "Accessed on 15.08.2022".

[230] A. Banks, "Bt and toshiba launch first commercial trial of quantum secured communication services – ey becomes first commercial customer." `https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services/`, Apr. 2022.

[231] C. Simondi, “Id quantique and sk broadband selected for the construction of the first nation-wide qkd network in korea.” https://www.idquantique.com/id-quantique-and-sk-broadband-selected-for-the-construction-of-the-first-nation-wide-qkd-network-in-korea/, Nov. 2020.

[232] C. Simondi, “Idq & sk broadband expand use of qkd to protect critical data in south korea.” https://www.idquantique.com/id-quantique-and-sk-broadband-expand-the-use-of-quantum-key-distribution-to-protect-critical-information-in-south-korea/, May 2021.

[233] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, “Perspectives and limitations of qkd integration in metropolitan area networks,” *Optics express*, vol. 23, no. 8, pp. 10359–10373, 2015.

[234] S. Sarmiento, S. Etcheverry, J. Aldama, I. Lopez, L. T. Vidarte, G. B. Xavier, D. Nolan, M. Li, D. Loeber, V. Pruneri, *et al.*, “Continuous-variable quantum key distribution over a 15 km multi-core fiber,” *New Journal of Physics*, 2022.

[235] J. GENG, G.-J. FAN-YUAN, K.-J. LI, M. TANG, S. WANG, D.-Y. HE, W. CHEN, Z.-Q. YIN, G.-C. GUO, and Z.-F. HAN, “Integration in c-band between quantum key distribution and classical channel of 25 dbm launch power over multicore fiber media,” 2022.

[236] D. Bacco, M. Zahidy, N. Biagi, D. Cozzolino, Y. Liu, Y. Ding, T. Morioka, C. Antonelli, A. Mecozzi, A. Zavatta, *et al.*, “Quantum communications with space encoding technique,” in *Optical Fiber Communication Conference*, pp. M1E–6, Optica Publishing Group, 2022.

[237] D. Bacco, D. Cozzolino, N. Biagi, A. Zavatta, and L. K. Oxenløwe, “Quantum-communication using multicore fibers,” in *2021 European Conference on Optical Communication (ECOC)*, pp. 1–4, IEEE, 2021.

[238] A. Lord, “The future of optical transport: Architectures and technologies from an operator perspective,” in *Optical Fiber Communication Conference*, pp. W4F–1, Optica Publishing Group, 2022.

[239] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, “Design and evaluation of a handheld quantum key distribution sender module,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 131–137, 2014.

[240] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, and D. O`Brien, “Handheld free space quantum key distribution with dynamic motion compensation,” *Optics Express*, vol. 25, no. 6, pp. 6784–6795, 2017.

[241] A. Gomez, K. Shi, C. Quintana, M. Sato, G. Faulkner, B. C. Thomsen, and D. O'Brien, "Beyond 100-gb/s indoor wide field-of-view optical wireless communications," *IEEE Photonics Technology Letters*, vol. 27, no. 4, pp. 367–370, 2014.

[242] C. Oh, E. Tangdiongga, and A. Koonen, "Steerable pencil beams for multi-gbps indoor optical wireless communication," *Optics letters*, vol. 39, no. 18, pp. 5427–5430, 2014.

[243] T. Koonen, F. Gomez-Agis, F. Huijskens, K. A. Mekonnen, Z. Cao, and E. Tangdiongga, "High-capacity optical wireless communication using two-dimensional ir beam steering," *Journal of Lightwave Technology*, vol. 36, no. 19, pp. 4486–4493, 2018.

[244] R. Singh, F. Feng, Y. Hong, G. Faulkner, R. Deshmukh, G. Vercasson, O. Bouchet, P. Petropoulos, and D. O'Brien, "Design and Characterisation of Terabit/s Capable Compact Localisation and Beam-Steering Terminals for Fiber-Wireless-Fiber Links," *Journal of Lightwave Technology*, vol. 38, no. 24, pp. 6817–6826, 2020.

[245] Y. Hong, F. Feng, K. R. Bottrill, N. Taengnoi, R. Singh, G. Faulkner, D. C. O'Brien, and P. Petropoulos, "Demonstration of 1Tbit/s WDM OWC with wavelength-transparent beam tracking-and-steering capability," *Optics Express*, vol. 29, no. 21, pp. 33694–33702, 2021.

[246] D. J. Richardson, J. M. Fini, and L. E. Nelson, "Space-division multiplexing in optical fibres," *Nature photonics*, vol. 7, no. 5, pp. 354–362, 2013.

[247] K. Nakajima, T. Matsui, T. Sakamoto, S. Nozoe, and Y. Goto, "Progress on sdm fiber research in japan," in *Optical Fiber Communication Conference*, pp. M1E–1, Optica Publishing Group, 2019.

[248] G. M. Saridis, D. Alexandropoulos, G. Zervas, and D. Simeonidou, "Survey and evaluation of space division multiplexing: From technologies to optical networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2136–2156, 2015.

[249] P. J. Winzer, D. T. Neilson, and A. R. Chraplyvy, "Fiber-optic transmission and networking: the previous 20 and the next 20 years," *Optics express*, vol. 26, no. 18, pp. 24190–24239, 2018.

[250] T. Tsuritani, D. Soma, Y. Wakayama, Y. Miyagawa, M. Takahashi, I. Morita, K. Maeda, K. Kawasaki, T. Matsuura, M. Tsukamoto, *et al.*, "Field test of installed high-density optical fiber cable with multi-core fibers toward practical deployment," in *2019 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2019.

[251] T. Hayashi, T. Nagashima, T. Nakanishi, T. Morishima, R. Kawawada, A. Mecozzi, and C. Antonelli, "Field-deployed multi-core fiber testbed," in *2019 24th OptoElectron-*

ics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC), pp. 1–3, IEEE, 2019.

[252] R. Ryf, A. Marotta, M. Mazur, N. K. Fontaine, H. Chen, T. Hayashi, T. Nagashima, T. Nakanishi, T. Morishima, F. Graziosi, *et al.*, "Transmission over randomly-coupled 4-core fiber in field-deployed multi-core fiber cable," in *2020 European Conference on Optical Communications (ECOC)*, pp. 1–4, IEEE, 2020.

[253] L. Zhang, J. Chen, E. Agrell, R. Lin, and L. Wosinska, "Enabling technologies for optical data center networks: Spatial division multiplexing," *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 18–30, 2020.

[254] R. Ding, X. Li, X. Liu, and J. Xu, "A cost-effective time-constrained multi-workflow scheduling strategy in fog computing," in *International Conference on Service-Oriented Computing*, pp. 194–207, Springer, 2018.

[255] D. Bastos, "Cloud for iot—a survey of technologies and security features of public cloud iot solutions," in *Living in the Internet of Things (IoT 2019)*, pp. 1–6, IET, 2019.

[256] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *arXiv preprint arXiv:1804.00200*, 2018.

[257] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid conventional and quantum security for software defined and virtualized networks," *Journal of Optical Communications and Networking*, vol. 9, no. 10, pp. 819–825, 2017.

[258] M. Elboukhari, M. Azizi, and A. Azizi, "Improving tls security by quantum cryptography," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 2, no. 3, pp. 87–100, 2010.

[259] A. Mink, S. Frankel, and R. Perlner, "Quantum key distribution (qkd) and commodity security protocols: Introduction and integration," *arXiv preprint arXiv:1004.0605*, 2010.

[260] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, *et al.*, "Using quantum key distribution for cryptographic purposes: a survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[261] E. Hugues-Salas, R. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Co-existence of 9.6 tb/s classical channels and a quantum key distribution (qkd) channel over a 7-core multicore optical fibre," in *2018 IEEE British and Irish Conference on Optics and Photonics (BICOP)*, pp. 1–4, IEEE, 2018.

[262] E. Hugues-Salas, Q. Wang, R. Wang, K. Rajkumar, G. T. Kanellos, R. Nejabati, and D. Simeonidou, “Coexistence of 11.2 tb/s carrier-grade classical channels and a dv-qkd channel over a 7-core multicore fibre,” in *45th European Conference on Optical Communication (ECOC 2019)*, pp. 1–4, 2019.

[263] J. Dynes, S. Kindness, S.-B. Tam, A. Plews, A. Sharpe, M. Lucamarini, B. Fröhlich, Z. Yuan, R. Penty, and A. Shields, “Quantum key distribution over multicore fiber,” *Optics express*, vol. 24, no. 8, pp. 8081–8087, 2016.

[264] C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y. Ji, “Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber,” *Optics express*, vol. 27, no. 4, pp. 5125–5135, 2019.

[265] R. Lin, A. Udalcovs, O. Ozolins, X. Pang, L. Gan, L. Shen, M. Tang, S. Fu, S. Popov, C. Yang, W. Tong, D. Liu, T. F. da Silva, G. B. Xavier, and J. Chen, “Telecom compatibility validation of quantum key distribution co-existing with 112 gbps/λ core data transmission in non-trench and trench-assistant multicore fibers,” in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, 2018.

[266] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, *et al.*, “Boosting the secret key rate in a shared quantum and classical fibre communication system,” *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[267] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenløwe, “Path-encoded high-dimensional quantum communication over a 2-km multicore fiber,” *npj Quantum Information*, vol. 7, no. 1, pp. 1–6, 2021.

[268] M. Ureña, I. Gasulla, F. J. Fraile, and J. Capmany, “Modeling optical fiber space division multiplexed quantum key distribution systems,” *Optics express*, vol. 27, no. 5, pp. 7047–7063, 2019.

[269] W. Kong, Y. Sun, C. Cai, and Y. Ji, “Impact of classical modulation signals on quantum key distribution over multicore fiber,” *Journal of Lightwave Technology*, vol. 39, no. 13, pp. 4341–4350, 2021.

[270] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, “High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits,” *npj Quantum Information*, vol. 3, no. 1, pp. 1–7, 2017.

[271] F. Ye and T. Morioka, “Interleaved core assignment for bidirectional transmission in multicore fibers,” in *39th European Conference and Exhibition on Optical Communication (ECOC 2013)*, pp. 1–3, IET, 2013.

[272] D. Zavitsanos, G. Giannoulis, A. Raptakis, C. Papapanos, F. Setaki, E. Theodoropoulou, G. Lyberopoulos, C. Kouloumentas, and H. Avramopoulos, "Coexistence of discrete-variable qkd with wdm classical signals in the c-band for fiber access environments," in *2019 21st International Conference on Transparent Optical Networks (ICTON)*, pp. 1–5, IEEE, 2019.

[273] R. Cregan, B. Mangan, J. Knight, T. Birks, P. S. J. Russell, P. Roberts, and D. Allan, "Single-mode photonic band gap guidance of light in air," *science*, vol. 285, no. 5433, pp. 1537–1539, 1999.

[274] G. T. Jasion, T. D. Bradley, K. Harrington, H. Sakr, Y. Chen, E. N. Fokoua, I. A. Davidson, A. Taranta, J. R. Hayes, D. J. Richardson, *et al.*, "Recent breakthroughs in hollow core fiber technology," in *Optical Fiber Communication Conference*, pp. M5E–2, Optical Society of America, 2021.

[275] B. Mangan, L. Farr, A. Langford, P. J. Roberts, D. P. Williams, F. Couny, M. Lawman, M. Mason, S. Coupland, R. Flea, *et al.*, "Low loss (1.7 db/km) hollow core photonic bandgap fiber," in *Optical Fiber Communication Conference*, p. PD24, Optical Society of America, 2004.

[276] N. Wheeler, M. G. Pappa, T. Bradley, Y. Chen, W. Brooks, J. Storey, M. Foster, D. Richardson, and M. Petrovich, "Spontaneous raman scattering in hollow core photonic crystal fibres," in *2017 IEEE SENSORS*, pp. 1–3, IEEE, 2017.

[277] F. Benabid, J. C. Knight, G. Antonopoulos, and P. S. J. Russell, "Stimulated raman scattering in hydrogen-filled hollow-core photonic crystal fiber," *Science*, vol. 298, no. 5592, pp. 399–402, 2002.

[278] F. Yu and J. C. Knight, "Negative curvature hollow-core optical fiber," *IEEE J. Sel. Top. Quantum Electron*, vol. 22, no. 2, pp. 146–155, 2016.

[279] J. R. Hayes, S. R. Sandoghchi, T. D. Bradley, Z. Liu, R. Slavík, M. A. Gouveia, N. V. Wheeler, G. Jasion, Y. Chen, E. N. Fokoua, *et al.*, "Antiresonant hollow core fiber with an octave spanning bandwidth for short haul data communications," *Journal of Lightwave Technology*, vol. 35, no. 3, pp. 437–442, 2017.

[280] S.-f. Gao, Y.-y. Wang, W. Ding, D.-l. Jiang, S. Gu, X. Zhang, and P. Wang, "Hollow-core conjoined-tube negative-curvature fibre with ultralow loss," *Nature communications*, vol. 9, no. 1, pp. 1–6, 2018.

[281] H. Sakr, Y. Chen, G. T. Jasion, T. D. Bradley, J. R. Hayes, H. C. H. Mulvad, I. A. Davidson, E. Numkam Fokoua, and F. Poletti, "Hollow core optical fibres with comparable

attenuation to silica fibres between 600 and 1100 nm," *Nature communications*, vol. 11, no. 1, pp. 1–10, 2020.

[282] A. Taranta, E. Numkam Fokoua, S. Abokhamis Mousavi, J. Hayes, T. Bradley, G. Jasion, and F. Poletti, "Exceptional polarization purity in antiresonant hollow-core optical fibres," *Nature Photonics*, vol. 14, no. 8, pp. 504–510, 2020.

[283] V. Michaud-Belleau, E. N. Fokoua, T. Bradley, J. R. Hayes, Y. Chen, F. Poletti, D. J. Richardson, J. Genest, and R. Slavík, "Backscattering in antiresonant hollow-core fibers: over 40 db lower than in standard optical fibers," *Optica*, vol. 8, no. 2, pp. 216–219, 2021.

[284] Y. Wang, N. V. Wheeler, F. Couny, P. Roberts, and F. Benabid, "Low loss broadband transmission in hypocycloid-core kagome hollow-core photonic crystal fiber," *Optics letters*, vol. 36, no. 5, pp. 669–671, 2011.

[285] A. N. Kolyadin, A. F. Kosolapov, A. D. Pryamikov, A. S. Biriukov, V. G. Plotnichenko, and E. M. Dianov, "Light transmission in negative curvature hollow core fiber in extremely high material loss region," *Optics express*, vol. 21, no. 8, pp. 9514–9519, 2013.

[286] F. Poletti, "Nested antiresonant nodeless hollow core fiber," *Optics express*, vol. 22, no. 20, pp. 23807–23828, 2014.

[287] T. D. Bradley, J. R. Hayes, Y. Chen, G. T. Jasion, S. R. Sandoghchi, R. Slavík, E. N. Fokoua, S. Bawn, H. Sakr, I. A. Davidson, *et al.*, "Record low-loss 1.3 db/km data transmitting antiresonant hollow core fibre," in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, IEEE, 2018.

[288] G. T. Jasion, T. D. Bradley, K. Harrington, H. Sakr, Y. Chen, E. N. Fokoua, I. A. Davidson, A. Taranta, J. R. Hayes, D. J. Richardson, *et al.*, "Hollow core nanf with 0.28 db/km attenuation in the c and l bands," in *Optical Fiber Communication Conference*, pp. Th4B–4, Optica Publishing Group, 2020.

[289] H. Sakr, T. D. Bradley, G. T. Jasion, E. N. Fokoua, S. R. Sandoghchi, I. A. Davidson, A. Taranta, G. Guerra, W. Shere, Y. Chen, *et al.*, "Hollow core nanfs with five nested tubes and record low loss at 850, 1060, 1300 and 1625nm," in *Optical Fiber Communication Conference*, pp. F3A–4, Optica Publishing Group, 2021.

[290] G. T. Jasion, H. Sakr, J. R. Hayes, S. R. Sandoghchi, L. Hooper, E. N. Fokoua, A. Saljoghei, H. C. Mulvad, M. Alonso, A. Taranta, *et al.*, "0.174 db/km hollow core double nested antiresonant nodeless fiber (dnanf)," in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2022.

[291] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, p. 022320, 2006.

[292] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, *et al.*, "Continuous high speed coherent one-way quantum key distribution," *Optics express*, vol. 17, no. 16, pp. 13326–13334, 2009.

[293] J. Hecht, "Speeding light, mitigating loss: Hollow-core fibers step to the fore." `https://spie.org/news/photonics-focus/julyaug-2022/speeding-light-with-hollow-core-fibers`, 2022. "Accessed on 22.10.2022".

[294] A. Nespola, S. Straullu, T. D. Bradley, K. Harrington, H. Sakr, G. T. Jasion, E. N. Fokoua, Y. Jung, Y. Chen, J. R. Hayes, *et al.*, "Transmission of 61 c-band channels over record distance of hollow-core-fiber with l-band interferers," *Journal of Lightwave Technology*, vol. 39, no. 3, pp. 813–820, 2021.

[295] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, no. 5, pp. 382–386, 2013.

[296] C. Quintana, P. Sibson, G. Erry, Y. Thueux, E. Kingston, T. Ismail, G. Faulkner, J. Kennard, K. Gebremicael, C. Clark, *et al.*, "Low size, weight and power quantum key distribution system for small form unmanned aerial vehicles," in *Free-Space Laser Communications XXXI*, vol. 10910, p. 1091014, International Society for Optics and Photonics, 2019.

[297] A. T. Castillo, E. Eso, and R. Donaldson, "In-lab demonstration of coherent one-way protocol over free space with turbulence simulation," *Optics Express*, vol. 30, no. 7, pp. 11671–11683, 2022.

[298] D. Lowndes, A. Schreier, D. O'Brien, and J. Rarity, "Characterising a handheld quantum key distribution system with emulated beam steering," in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, vol. 11881, pp. 9–13, SPIE, 2021.

[299] O. Elmabrok, M. Ghalaii, and M. Razavi, "Quantum-classical access networks with embedded optical wireless links," *JOSA B*, vol. 35, no. 3, pp. 487–499, 2018.

[300] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *JOSA B*, vol. 36, no. 3, pp. B99–B108, 2019.

[301] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[302] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, *et al.*, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013.

[303] Z. Wang, R. Malaney, and B. Burnett, "Satellite-to-earth quantum key distribution via orbital angular momentum," *Physical Review Applied*, vol. 14, no. 6, p. 064031, 2020.

[304] L. Mazzarella, C. Lowe, D. Lowndes, S. K. Joshi, S. Greenland, D. McNeil, C. Mercury, M. Macdonald, J. Rarity, and D. K. L. Oi, "Quarc: quantum research cubesat—a constellation for quantum communication," *Cryptography*, vol. 4, no. 1, p. 7, 2020.

[305] R. Donaldson, D. Kundys, A. Maccarone, R. Henderson, G. S. Buller, and A. Fedrizzi, "Towards combined quantum bit detection and spatial tracking using an arrayed single-photon sensor," *Optics Express*, vol. 29, no. 6, pp. 8181–8198, 2021.

[306] R. Singh, A. Schreier, G. Faulkner, and D. O'Brien, "Fiber-wireless-fiber terminals for optical wireless communication over multiple bands," in *2020 IEEE Photonics Conference (IPC)*, pp. 1–2, IEEE, 2020.

[307] S. Yuan and N. A. Riza, "General formula for coupling-loss characterization of single-mode fiber collimators by use of gradient-index rod lenses," *Applied Optics*, vol. 38, no. 15, pp. 3214–3222, 1999.

[308] Standard, "EN 60825-1: 2014—Safety of Laser Products," *Equipment classification and requirements*, 2014.

[309] K. Rottwitt, J. Bromage, and L. Leng, "Scaling the raman gain coefficient of optical fibers," in *2002 28TH European Conference on Optical Communication*, vol. 3, pp. 1–2, IEEE, 2002.

[310] T. Günthner, B. Pressl, K. Laiho, J. Geßler, S. Höfling, M. Kamp, C. Schneider, and G. Weihs, "Broadband indistinguishability from bright parametric downconversion in a semiconductor waveguide," *Journal of Optics*, vol. 17, no. 12, p. 125201, 2015.

[311] D. Dai, Z. Wang, J. F. Bauters, M.-C. Tien, M. J. Heck, D. J. Blumenthal, and J. E. Bowers, "Low-loss si 3 n 4 arrayed-waveguide grating (de) multiplexer using nano-core optical waveguides," *Optics express*, vol. 19, no. 15, pp. 14130–14136, 2011.

[312] Á. Rosa, A. Gutiérrez, A. Brimont, A. Griol, and P. Sanchis, "High performace silicon 2x2 optical switch based on a thermo-optically tunable multimode interference coupler and efficient electrodes," *Optics express*, vol. 24, no. 1, pp. 191–198, 2016.

[313] P. Dumais, Y. Wei, M. Li, F. Zhao, X. Tu, J. Jiang, D. Celo, D. J. Goodwill, H. Fu, D. Geng, *et al.*, "2× 2 multimode interference coupler with low loss using 248 nm photolithography," in *Optical Fiber Communication Conference*, pp. W2A–19, Optica Publishing Group, 2016.

[314] D. McDermott, M. Ghallab, A. Howe, C. Knoblock, A. Ram, M. Veloso, D. Weld, and D. Wilkins, "Pddl-the planning domain definition language," 1998.

[315] J. Hoffmann and B. Nebel, "The ff planning system: Fast plan generation through heuristic search," *Journal of Artificial Intelligence Research*, vol. 14, pp. 253–302, 2001.

[316] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, 2013.

[317] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," *Nature*, vol. 564, no. 7735, pp. 225–228, 2018.

[318] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli, "Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography," *Laser & Photonics Reviews*, vol. 10, no. 3, pp. 451–457, 2016.

[319] X. Liu, J. Liu, R. Xue, H. Wang, H. Li, X. Feng, F. Liu, K. Cui, Z. Wang, L. You, *et al.*, "40-user fully connected entanglement-based quantum key distribution network without trusted node," *PhotoniX*, vol. 3, no. 1, pp. 1–15, 2022.

[320] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Science & Applications*, vol. 10, no. 1, pp. 1–8, 2021.

[321] N. B. Lingaraju, H.-H. Lu, S. Seshadri, D. E. Leaird, A. M. Weiner, and J. M. Lukens, "Adaptive bandwidth management for entanglement distribution in quantum networks," *Optica*, vol. 8, no. 3, pp. 329–332, 2021.

[322] E. Y. Zhu, C. Corbari, A. Gladyshev, P. G. Kazansky, H.-K. Lo, and L. Qian, "Toward a reconfigurable quantum network enabled by a broadband entangled source," *JOSA B*, vol. 36, no. 3, pp. B1–B6, 2019.

[323] F. Appas, F. Baboux, M. I. Amanti, A. Lemaítre, F. Boitier, E. Diamanti, and S. Ducci, "Flexible entanglement-distribution network with an algaas chip for secure communications," *npj Quantum Information*, vol. 7, no. 1, pp. 1–10, 2021.

[324] F. Laudenbach, B. Schrenk, M. Achleitner, N. Vokić, D. Milovančev, and H. Hübel, "Flexible cloud/user-centric entanglement and photon pair distribution with synthesizable

optical router," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 26, no. 3, pp. 1–9, 2020.

[325] X.-Y. Chang, D.-L. Deng, X.-X. Yuan, P.-Y. Hou, Y.-Y. Huang, and L.-M. Duan, "Experimental realization of an entanglement access network and secure multi-party computation," *Scientific Reports*, vol. 6, p. 29453, July 2016.

[326] I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Huebel, "Demonstration of active routing of entanglement in a multi-user network," *Optics express*, vol. 21, no. 23, pp. 29013–29024, 2013.

[327] N. R. Solomons, A. I. Fletcher, D. Aktas, N. Venkatachalam, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, Ž. Samec, M. Stipčević, *et al.*, "Scalable authentication and optimal flooding in a quantum network," *PRX Quantum*, vol. 3, no. 2, p. 020311, 2022.

[328] C. Yuan, H. Yu, Z. Zhang, Y. Wang, H. Li, L. You, Y. Wang, H. Song, G. Deng, and Q. Zhou, "Quantum entanglement distribution coexisting with classical fiber communication," in *Asia Communications and Photonics Conference*, pp. T2F–2, Optical Society of America, 2019.

[329] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[330] J. M. Thomas, G. S. Kanter, E. M. Eastman, K. F. Lee, and P. Kumar, "Entanglement distribution in installed fiber with coexisting classical light for quantum network applications," in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, IEEE, 2022.