Experimental Implementation of Twin-Field Quantum Key Distribution Protocols

Mirko Pittaluga

University of Leeds

School of Electronic and Electrical Engineering

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

September, 2021

Intellectual Property Statement

The candidate confirms that the work submitted is his own, except where work which has formed part of jointly authored publications has been included. The contribution of the candidate to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others.

The work in chapters 3 and 4 of the thesis has appeared in publication as follows:

- Mariella Minder, **Mirko Pittaluga**, George L. Roberts, Marco Lucamarini, James F. Dynes, Zhiliang Yuan, and Andrew J. Shields (2019) *Experimental quantum key distribution beyond the repeaterless secret key capacity.* Nature Photonics 13 (5), pp. 334–338. (joint first author)

In this experiment, I contributed to designing, building and testing the experimental setup. I designed, developed and implemented the phase feedback system and the optical frequency regeneration setup. I also developed the code used to simulate the protocol and analyse the data. I developed the error model for the feedback QBER contribution. I was in charge of data collection. I contributed to the writing of the manuscript.

The work in chapters 3 and 6 of the thesis has appeared in publication as follows:

- **Mirko Pittaluga**, Mariella Minder, Marco Lucamarini, Mirko Sanzaro, Robert I. Woodward, Ming-Jun Li, Zhiliang Yuan, and Andrew J. Shields (2021) *600-km repeater-like quantum communications with dual-band stabilization.* Nature Photonics 15 (7), pp. 530–535.

In this experiment, I designed, built and tested the experimental setup. I developed the code used to control the experiment and analyse the data. I was in charge of data collection and analysis. I contributed to the writing of the manuscript.

The author of this thesis acknowledges the contribution of other researchers in achieving the aforementioned results. M. Minder participated in all experimental work with significant contributions in the development of the setup and the data analysis for the proof-of-principle TF-QKD experiment, the simulations of the TF-QKD protocol and its variants, and the early developments of the dual-band phase stabilisation technique. M. Lucamarini provided theoretical support and experimental supervision. Z. Yuan provided experimental support.

Other work conducted during this PhD that was not explicitly addressed in this thesis has appeared in publication as follows:

- George L. Roberts, **Mirko Pittaluga**, Mariella Minder, Marco Lucamarini, James F. Dynes, Zhiliang Yuan, and Andrew J. Shields (2018) *Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution.* Optics Letters, 43 (20) pp. 5110-5113.
- Cecilia Clivati, Alice Meda, Simone Donadello, Salvatore Virzì, Marco Genovese, Filippo Levi, Alberto Mura, **Mirko Pittaluga**, Zhiliang Yuan, Andrew J. Shields, Marco Lucamarini, Ivo Pietro Degiovanni and Davide Calonico (2022) *Coherent phase transfer for real-world twin-field quantum key distribution.* Nat Commun 13 (1), p. 157.
- Robert I. Woodward, Yuen San Lo, **Mirko Pittaluga**, Mariella Minder, Taofiq K. Paraïso, Marco Lucamarini, Zhiliang Yuan, Andrew J. Shields (2021) *Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers.* npj Quantum Inf 7 (1), p. 58.

Contents from published papers were presented at the following conferences:

- **Mirko Pittaluga**, Mariella Minder, George L. Roberts, Marco Lucamarini, James F. Dynes, Zhiliang Yuan, Andrew J. Shields. Contributed talk: *Experimental Twin-Field Quantum Key Distribu-*

tion Beyond the Repeaterless Secret Key Capacity Bound, QCrypt 2019, Montreal (Canada), 26-30 August 2019.

- **Mirko Pittaluga**, Mariella Minder, George L. Roberts, Marco Lucamarini, James F. Dynes, Zhiliang Yuan, Andrew J. Shields. Contributed talk: *Experimental Twin-Field Quantum Key Distribution Beyond the Repeaterless Secret Key Capacity Bound*, QCALL ESR Conference, Mondello - Palermo (Italy), 16-19 September 2019.
- **Mirko Pittaluga**. Contributed talk: *Dual-Band Phase Stabilisation Technique for Phase-Sensitive Quantum Communications*, QCall Final Symposium on Advances in Quantum Communications, virtual conference, 3-5 May 2021.
- **Mirko Pittaluga**. Invited talk: *Experimental Repeater-Like Quantum Communications over 600 km of Optical Fibre with Dual-Band Phase Stabilisation*, QCrypt 2021, virtual conference based in Amsterdam (Netherlands), 23-27 August 2021.
- **Mirko Pittaluga**. Contributed talk: *Experimental repeater-like quantum communications over 600 km of optical fibre with wavelength-multiplexed phase stabilisation*, Frontiers in Optics + Laser Science (FiO+LS) 2021, virtual conference based in Washington D.C. (USA), 1-4 November 2021.
- **Mirko Pittaluga**. Contributed talk: *Experimental Repeater-Like Quantum Communications Over 600 km of Optical Fibre Aided by Wavelength-Multiplexed Phase Stabilisation*, SPIE Photonics West 2022, San Francisco (California, USA), 22-27 Jan 2022.

Contents from published papers were also presented at the following workshop:

- **Mirko Pittaluga**, Piotr Rydlichowski, Domenico Vicinanza, Guy Roberts. Invited talk: *Experimental Twin-Field Quantum Key Distribution Beyond the Repeaterless Secret Key Capacity Bound*, GÉANT Infoshare Meeting, virtual meeting, 17 March 2021.
- **Mirko Pittaluga**. Invited talk: *Quantum Communications over 600 km of Optical Fibre with Dual-Band Phase Stabilisation*, CloNetS-DS workshop 2021, Bad Honnef (Germany), 13-15 September 2021.

Acknowledgements

I would like to thank Dr Andrew J. Shield, my group leader at Toshiba Europe Ltd., Prof Mohsen Razavi, my academic supervisor at Leeds University, and the institutions they represent for giving me the precious opportunity to conduct the research presented in this thesis. This was a wonderful experience that I truly enjoyed and from which I learned so much.

I acknowledge funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 'QCALL' and under the grant agreement number 857156 'OPENQKD'.

I would also like to thank sincerely QCALL and all its members, especially my fellow early-stage researchers. Being part of this network was a fantastic opportunity to grow and have fun while doing so.

A special thank goes to Dr Zhiliang Yuan and Prof Marco Lucamarini, my direct supervisors at Toshiba Cambridge Research Laboratory. Working with you has been a privilege. Almost everything presented here was enabled by your support.

I am grateful to all present and past researchers and students at Toshiba CRL for their invaluable help and companionship. I feel extremely fortunate to have had the opportunity to work and spend time with you. A special mention goes to Mariella Minder, with whom I shared many joys and sorrows of hard laboratory work.

Thank to my partner Elena, my family and friends. You are what makes life worth living.

Abstract

Quantum Key Distribution allows two distant users to establish a common secret string of bits by sending photons across a communication line, often an optical fibre. The photons, however, are scattered by the propagation medium and have only a small probability of reaching the end of the line, which limits the QKD key rate and its transmission range. A rigorous theorem limits the number of secure bits delivered by a point-to-point QKD link to 1.44η, with η being the channel transmission probability. This is known as the 'repeaterless secret key capacity', or the PLOB bound. The key question at the core of this thesis is to design and implement QKD systems that surpass the PLOB bound.

Until very recently, this task was believed to be impossible with today's technology. This changed with the introduction of the 'Twin-Field' (TF) QKD protocol, which features a key rate that scales proportionally to the square root of η and therefore offers a way to extend the current range of QKD.

This work provides a contextualisation and description of the TF-QKD protocol and its variants. The experimental challenges for its implementation are considered and followed by the development of experimental techniques, setups and analysis frameworks necessary to implement the protocol.

As a result, the first proof-of-principle demonstration of the protocol over highly attenuated channels is obtained and described. In this experiment, a secure key could be distributed in excess of 90 dB channel loss and the PLOB bound could be exceeded for the first time. The setup implemented for this experiment is currently considered the first realisation of an effective quantum repeater.

A second experiment, which exploits a novel dual-band phase stabilisation technique, is also developed. In this experiment, TF-QKD is performed over long communication channels that reached over 600 km of fibre length and 100 dB of channel loss. This experiment represents today's the longest fibre-based quantum communication system.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard 10, 130
AOM	Acousto-Optic Modulator 79
APD	Avalanche Photo-Diode 138
AWG	Arbitrary Waveform Generator 96, 98, 99, 102, 105
BB84	Bennett-Brassard 1984 ..... xvii, 7–13, 20, 21, 60, 61, 64, 86
BBM92	Bennett-Brassard-Mermin 1992 protocol 10, 12
BR	Bright Reference signal 67, 70
BS	Beam Splitter xv, 13, 25, 26, 33, 39, 41, 44, 60, 61, 69, 70, 76, 79, 81, 82, 85, 97–101, 122, 123, 141, 146
BSM	Bell State Measurement 13, 14, 21
CHSH	Clauser-Horne-Shimony-Holt 11
CW	Continuous Wave 67, 71, 81, 82, 87, 97, 116
DAC	Digital-to-Analog Converter 80, 99, 146
DC	Direct Current 57, 65, 70, 80, 99
DQ	Dim Quantum pulses 67
DR	Dim Reference pulses 67
DV	Discrete Variable 17
DWDM	Dense Wavelength Division Multiplexer/Multiplexing 69, 117, 122
E91	Ekert 91 ..... 10–12, 28
EDFA	Erbium-Doped Fibre Amplifier 19, 104, 105, 119, 120
EPC	Electronic Polarisation Controller 81, 82, 97–101, 122, 145, 146
EPR	Einstein–Podolsky–Rosen 10
FPGA	Field Programmable Gate Array 70
FS	Fibre Stretcher 69, 71, 123
FWHM	Full Width at Half Maximum 72

IM	Intensity Modulator 25, 48, 50, 97–99, 107, 145, 146
ITU	International Telecommunication Union 52, 67, 102
LD	Laser Diode 76, 77, 81, 82
LO	Local Oscillator 57, 79
MZI	Mach-Zehnder Interferometer 50, 77, 78
OIL	Optical Injection Locking . . . xvi, 31, 55, 56, 65, 76–81, 83, 93, 138, 141
OPLL	Optical Phase-Locked Loop xv, xvi, 31, 55–57, 78–83, 93, 106, 119, 120, 138, 143
OTP	One-Time-Pad 4, 5, 10, 133
PBS	Polarizing Beam Splitter 13, 100, 122
PCB	Printed Circuit Board 99, 105
PID	Proportional-Integral-Derivative . xv, 59, 60, 65, 66, 68, 70, 71
PLL	Phase-Locked Loop . . . . . xv, 56, 57
PLOB	Pirandola-Laurenza-Ottaviani-Banchi . . . . . ix, 20, 22, 134
PM	Phase Modulator . 25, 26, 48, 50, 64, 65, 68–70, 81–83, 96–101, 107, 123, 146
PNS	Photon Number Splitting 15–17
QBER	Quantum Bit Error Rate . . . . . xvi, 18, 83–87, 106–108, 120
QKD	Quantum Key Distribution . ix, xv, 5, 7, 10–12, 14–21, 23, 24, 27–33, 35–37, 44, 47, 48, 53, 56, 60, 73, 75, 79, 87, 90, 92, 112, 113, 128, 129, 133–135, 137, 138
DV-QKD	Discrete Variable QKD 47, 53
MDI-QKD	Measurement-Device Independent QKD xv, 12–14, 21, 24, 26, 27
TF-QKD	Twin-Field QKD . . . . . iv, ix, xv–xviii, 24–33, 36–40, 42–44, 47, 54, 58, 60, 62, 64, 65, 73, 75, 76, 78, 79, 81, 82, 84, 89–93, 95–97, 99–103, 106–108, 111–115, 120, 122–130, 134, 135, 137, 138, 141–143, 147
CAL	Curty-Azuma-Lo . . . . . xvii, 31, 38–40, 125, 126, 128, 143
SNS	Sending-or-Not-Sending xvii, xviii, 31, 38, 40, 42–44, 125–129, 147–152
QR	Quantum Reference 122, 125
QS	Quantum Signal 122, 125, 126
RF	Radio Frequency 57, 80, 97–99, 141, 146
RSA	Rivest-Shamir-Adleman cryptosystem 6

SKC	Secret Key Capacity. 20–22, 24–27, 31, 36, 37, 75, 91, 92, 113, 128, 129, 134, 147
SKR	Secure Key Rate.. xv, 14, 17–22, 24, 26–28, 32, 33, 35–38, 75, 83, 85, 89, 92, 95, 113, 114, 128, 129, 142, 144, 147
SNSPD	Superconducting Nanowire Single Photon Detector.... 53, 64, 68–71, 81, 100, 101, 122–124
SPAD	Single Photon Avalanche Diode 53
TEUR	Toshiba Europe Ltd..... 30
TOF	Time Of Flight..... 96
TWCC	Two-Way Classical Communication.... xvii, xviii, 43, 44, 125, 127–129, 147, 149–152
ULL	Ultra-Low-Loss..... 40, 42, 44, 92, 128
VOA	Variable Optical Attenuator 25, 48, 50, 51, 75, 81, 95, 98–100, 111, 141, 146
WCP	Weak Coherent Pulses..... xv, 15–18, 25, 39–41
WDM	Wavelength-Division Multiplexing 48, 52, 53, 67, 105

Part I

Background

Chapter 1

Introduction

1.1 Cryptography

Our time is often referred to as the "Information Age" [1]. The distinctive feature of this period compared to the previous ones is the increase in speed, diffusion and ease of accessibility of information. The start of the information revolution can be dated back to the second half of the 20st century, when two main driving factors led to its commencement. The first was the wide availability of computational power, fueled by breakthroughs in semiconductor science and advances in the miniaturization of computing devices. The second was the formalisation and development by Claude E. Shannon in 1948 [2] of Information Theory, the mathematical framework describing information processing.

Most of the information we create and exchange today is in digital form, and the rate at which we generate it is increasing exponentially. Recent studies show that starting from 1985, the amount of digital information generated worldwide on a daily basis increased by a factor of 10 every 2 years [3]. In this context of increasing importance of information generation and exchange, there are countless scenarios in which it has to be transmitted in a secret way. These confidential exchanges could be related to countries' national interests, companies strategic assets, or simply private communications between common citizens.

The science of exchanging information while keeping it private is called cryptography. Cryptography has been an active field of research for a long time. The most ancient evidence of this practice is thought to be a secret form of hieroglyphics found inside the Great Pyramid in Egypt, which are dated about 4000 years old [4]. From those times, history is replete with examples of cryptographic strategies put in

practice to transfer messages secretely. The outcome of key historical events such as battles or wars have often been decided by the effectiveness of secret communication schemes developed over time by cryptographers [5].

Modern cryptography is a complex interdisciplinary field that includes aspects of information theory, computational complexity, and finite mathematics. Tools developed by modern cryptography are ubiquitous nowadays. All of the private conversations, financial transactions, and secure data exchange we have daily over the Internet for example, are kept secret by means of these tools.

Encryption strategies are broadly divided into two families based on the type of keys used in the process: symmetric encryption (or secret key protocols) and asymmetric encryption (or public key protocols).

1.1.1 Symmetric Cryptography

In symmetric key encryption schemes, both the sender and receiver use the same secret key to encrypt and decrypt the secret message. The strength and security of this type of protocols relies on the secrecy of the shared secret key. It can be proved that once Alice and Bob share a sufficiently long secret key, a particular type of symmetric encryption scheme, the One-Time-Pad (OTP), can guarantee perfect communication security [6]. To date, the one-time pad is the only cryptosystem that can be proven unconditionally secure, and for this reason it is said to be *information-theoretic secure*.

To explain how this cryptosystem works let us consider a scenario where a user named *Alice* wants to send a confidential message to a second user named *Bob*. Before any communication takes place, Alice and Bob make sure they are the only two owners of a long and perfectly random bit string called the key, K. The first step of the OTP procedure requires Alice to encode her message in a string of bits, M. After this, Alice performs a binary addition operation between her bit string M and a portion of the key string K having the same length of M. The result of this operation will be a random string, technically called cipher text, denoted as $C = M \oplus K$.

At this point Alice sends C through a public communication channel to Bob. Even by eavesdropping the string C, any malicious adversary that does not know the secret key will not be able to retrieve the secret message. Bob retrieves the original message M by performing the same binary bit sum operation between the received string C and his copy of the secret key K: $C \oplus K = M \oplus K \oplus K = M$. A

Figure 1.1: Working principle of a symmetric encryption scheme (including the OTP). A message (M) is encoded into the cipher text (C) via a secret key (K) and is transmitted by Alice to Bob. The cipher text C travels through a public channel and is received by Bob who recovers M by decrypting C thanks to his local copy of the key K.

simple representation of the working mechanism of the OTP (and, by extension, of any symmetric key encryption scheme) is shown in fig. 1.1.

The security of the one-time pad is based on the assumptions that the key K used for the encryption is random, known only to the intended users, as long as the secret message, and that the same key cannot be used more than once. These requirements clearly introduce a practical problem: the generation and distribution of such a key. This problem is so hard that no solution to it was found in the realm of classical information theory. The only solution to this problem available today requires the use of quantum resources and is called Quantum Key Distribution (QKD), which will be discussed later.

1.1.2 Asymmetric Cryptography

In asymmetric key encryption, or public-key protocols, Alice and Bob are able to encrypt their messages without sharing a common secret key. In these protocols, Bob computes a public-private key pair, with the two keys being linked by a one-way mathematical function, i.e., a function which is easy to compute on every input, but hard to invert given the image of a random input [7]. He then publicly announces the public key, which can be used by Alice to encrypt her message into a cipher text that she makes publicly available. The cipher text can be decrypted only by Bob through his private key. The security of this type of encryption strategy relies on the computational difficulty of computing the inverse of the one-way function linking the private and public keys. These types of schemes are more convenient to implement than symmetric ones, but they cannot guarantee perfect security.

The first practical asymmetric encryption scheme was proposed in 1978 by Ronald Rivest, Ari Shamir and Leonard Adleman [8], and it is today commonly referred to as the RSA[1] Public Key Algorithm. The security of RSA is based on the practical difficulty of factoring the product of two large prime numbers (a task that is also known as the integer factorization problem). It was not long after the first asymmetric key encryption scheme was published that several other protocols, based on similar logic, were proposed. Nowadays, public key protocols are the fundamental element that allows us to establish secure and private digital communication. With the currently available technology and mathematical knowledge, eavesdropping a message encoded with common public key protocols would take a prohibitive amount of time.

This scenario could radically change with the advent of Quantum Computers [9–11]. The field of quantum computation investigates the capabilities of machines that use single quantum elements (instead of the solid state compounds used in classical computing) as building blocks for computing architectures. Theoretically, quantum computers have been shown to have the potential to outperform classical ones when addressing particular problems. For instance, by implementing Shor's algorithm [12], quantum computers may solve the integer factorization problem exponentially more efficiently than classical computers [13, 14].

Substantial progress has been made in recent years with the construction of quantum computers [15, 16] and the development of algorithms to be run with them [17, 18]. A powerful quantum computer capable of running Shor's algorithm could break current asymmetric encryption schemes in a fraction of the time required by today's computers, jeopardising the security of today's communications. The faster these developments occur, the more we should be concerned about the security of our communications. Observers in the field estimate that the quantum technology needed to break 2048-RSA is likely to become available in 20 years [19–21].

1.2 Quantum Key Distribution

Interestingly, as by taking advantage of quantum effects for computation could undermine the security of current cryptographic schemes, by exploiting the properties of quantum systems for information exchange it is possible to establish an information-theoretic secure key exchange.

This is achieved by exploiting a fundamental postulate of quantum mechanics,

[1] After the name of the three inventors of the algorithm

the fact that in the quantum regime the observation of the state of a physical system affects the state itself [22]. By looking at this statement from a slightly different angle we can get an insight of how by shifting from the classical to the quantum regime we can actually solve the key distribution problem mentioned at the end of section 1.1.1.

In classical communications, the biggest obstacle with the distribution of the keys needed to implement the one-time pad is that there is no way to tell if the transmitted keys arrived securely to the designated user without being intercepted by a malicious adversary (often referred to as *Eve*). The risk is that if during the key exchange an eavesdropper manages to get the key K, they would then be able to access the message M by decrypting the publicly available string C transmitted over the communication channel.

Let us now consider what changes when quantum signals are used to establish a common encryption key between Alice and Bob. In this scenario, Alice encodes some information into single photons and sends them to Bob over a channel (often called *quantum channel*) connecting the two users. In this case, the measurement postulate of quantum mechanics turns into a formidable resource. In fact, if Eve was eavesdropping any information about the photons sent by Alice by observing/measuring them, her action would affect the state of the photons received by Bob. This guarantees that by monitoring the state of a subset of the exchanged photons, the legitimate users can tell if any eavesdropping occurred. This ensures that when Alice and Bob certify that no significant perturbations of the exchanged photons occurred, they can also conclude that no external measurement, and hence no interception, had taken place.

The procedure of using quantum carriers to transfer the information that will be used to distill a secret key for symmetric encryption is called QKD. QKD can effectively solve the problem of distributing symmetric encryption keys, and, for this reason, it is currently the only known cryptosystem (when used together with the one-time pad) that guarantees provable information-theoretic security. The first QKD protocol was proposed in 1984 by C. H. Bennett and G. Brassard [23], and is now known as the Bennett-Brassard 1984 (BB84) protocol.

QKD has been a field of intense research for the past forty years [24–27]. Over this period of time, quantum cryptography moved from being an interesting theoretical proposal [23, 28] to be implemented experimentally [29], and, already for some time now, to be a commercially available technology.

1.2.1 The BB84 Protocol

In this section the BB84 protocol will be explained following the original Bennet's and Brassard's 1984 argument [23], using single photons as qubits (i.e., the smallest amount of information, *-bit*, encoded by a quantum carrier, *qu-*) and polarization as the degree of freedom used for the encoding.

Four quantum states which constitute two non-orthogonal bases of the photons' polarization state space are used for the encoding of the BB84 protocol. The two orthogonal vertical $|\updownarrow\rangle$ and horizontal $|\leftrightarrow\rangle$ polarizations, constitute the generating vectors of the rectilinear basis, $\boldsymbol{+}$. The two orthogonal diagonal $|\swarrow\!\!\nearrow\rangle$ and antidiagonal $|\nwarrow\!\!\searrow\rangle$ polarizations, constitute the generating vectors of the diagonal basis, $\boldsymbol{\times}$. The two bases are maximally conjugate in the sense that any pair of vectors, one from each basis, has the same overlap, e.g., $|\langle\updownarrow|\swarrow\!\!\nearrow\rangle|^2 = \frac{1}{2}$. Choosing one of the two bases is equivalent to picking a value from a binary set. The two bases are therefore conventionally mapped into the values 0 and 1:

- Rectilinear basis $\longrightarrow$ 1
- Diagonal basis $\longrightarrow$ 0

Similarly, once the basis has been set, also the selection of a basis vector can be reduced to a binary choice that can be mapped into the bit values 0 and 1.

The protocol starts with Alice choosing randomly two bits. The two bits define the quantum state that she is preparing: with the first one she will select a basis, with the second one she will select a basis vector. After having prepared the polarization of her single photon, Alice sends it to Bob over a quantum channel[1].

When Bob receives the qubit, he randomly chooses a basis to measure it in. If a conclusive measurement outcome is obtained, he retrieves a bit out of each measurement. He then communicates to Alice which basis he used for each qubit measurement, and Alice responds to inform him when he guessed correctly. Since both Alice and Bob have chosen their basis randomly and in an uncorrelated manner, Bob will have measured in the correct basis 50% of the time (provided that Alice picks her basis in an unbiased manner). At this point, they discard all the bits where they chose a different basis (a procedure called **key sifting**) and are both left with a string called the *sifted key*. If the qubits are not subjected to any perturbation in

[1] A quantum channel is simply the transmission route of quantum signals.

Alice Sent Bits	↗	↖	↔	↗	↕	↕	↗	↔
Bob Basis Choice	✣	⤫	⤫	✣	✣	⤫	⤫	✣
Bob Measured Bit	↕	↖	↗	↔	↕	↖	↗	↔
Post Sifting Results	✗	✓	✗	✗	✓	✗	✓	✓
Agreed Key	-	↖	-	-	↕	-	↗	↔

Table 1.1: Example of the BB84 protocol key exchange and sifting. ✣ corresponds to the rectilinear basis ($|\updownarrow\rangle$, $|\leftrightarrow\rangle$) and ⤫ corresponds to diagonal basis ($|\nearrow\rangle$, $|\nwarrow\rangle$).

the quantum channel, and Alice's and Bob's setups are perfect, all the bits in the two sifted keys will match perfectly.

The interesting property of this scheme is that if a malicious adversary (Eve) tries to get any information out of the transferred qubits, she will have to guess randomly a basis to measure them in at each time. Eve's measurement will modify the state of the quantum carrier, in fact, 50% of the time she will collapse the photon polarization state in a different basis from the one chosen by Bob. As a consequence of Eve's eavesdropping, 25% of the bits in Alice and Bob sifted keys will be different. Eve's activity could be then easily discovered by checking how many bits in the sifted keys are matching on average. An example of BB84 protocol sifting precess is represented in table 1.1.

In an ideal world (where error-free communication and perfect state preparation and detection are possible) the BB84 protocol would terminate here. Due to implementation imperfections however, Alice's and Bob's sifted keys will never be identical. Other operations must be carried out to ensure that at end the protocol the users share an identical and secret key. The next step of the protocol is called **error estimation**. During this phase, Alice and Bob compare a random subset of their sifted keys, and compute their bit and phase errors. The former provides an indication of much the users' keys differ from each other, the latter informs the users of how much information Eve may have about their key.

At the end of this phase, an **error correction** procedure is carried out. An error correction algorithm is applied to the two sifted keys to ensure that Alice and Bob share identical keys.

The last step of the protocol is called **privacy amplification**. During this phase, the two identical error-corrected keys possessed by Alice and Bob are manipulated

through some classical algorithms with the aim of diminishing the amount of information Eve might have on the key. At the end of this process, Alice and Bob will share a private key that they can use for secure communication. They can for instance use the obtained secret key to perform perfectly secure communication using the OTP encryption strategy. BB84 has been proven theoretically secure [30, 31].

In order to allow encryption of large datasets, QKD could also be used in combination with other symmetric encryption protocols, e.g. Advanced Encryption Standard (AES). Such ciphers, differently from OTP, are not information-theoretic secure, but no attack against them exists better than the Grover's quantum algorithm [32] which can be overcome by increasing the key size.

1.2.2 Entanglement-Based QKD

A second important class of QKD protocols are the entanglement-based ones. The first example of this type of protocols was proposed by Artur Ekert in 1991, who proposed a cryptographic scheme based on the peculiar correlations of entangled photon pairs. This intuition is so relevant for QKD that the associated protocol is commonly referred to as the Ekert 91 (E91) protocol.

Another well known entanglement-based protocol is the Bennett-Brassard-Mermin 1992 protocol (BBM92) protocol [33]. This protocol is actually more practical than E91, and most entanglement-based QKD implementations rely on it. However, in the following, we will describe only the E91, which is chosen for its historical relevance.

Unlike BB84, in E91 it is no longer the users aiming to establish a shared secret key who transmit quantum states. The transmitted quantum state is instead an Einstein–Podolsky–Rosen (EPR) pair [34] generated by an entangled photon source possibly controlled by a third untrusted party. The two photons constituting the pair are distributed to Alice and Bob who act as receivers. A simple representation of the typical E91 configuration is shown in fig. 1.2.

To explain the working principle of an entanglement-based protocol let us consider a system where the photon source produces a maximally entangled state $|\phi^+\rangle$:

$$|\phi^+\rangle = \frac{|\updownarrow,\updownarrow\rangle + |\leftrightarrow,\leftrightarrow\rangle}{\sqrt{2}}. \tag{1.1}$$

After the generation, one photon of the pair is sent to Alice and the other to Bob. The two users choose independently and randomly the basis for their measurement $\mathcal{Z}$ or $\mathcal{X}$ (graphically, $\oplus$ or $\boxtimes$) . The entanglement of $|\phi^+\rangle$ state guarantees that when the users choose to measure in the same basis, which will happen on average

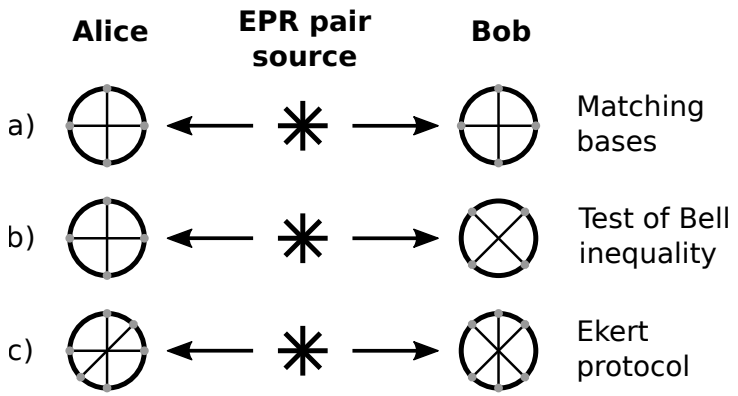

Figure 1.2: Representation of the elements required for an entanglement-based QKD protocol. **a.** When Alice and Bob choose the same measurement bases, their outcomes are related deterministically and they can use their measurement outcomes to build a secret key, similarly to the BB84 protocol instances where Bob measures in the same basis used by Alice for her preparation. **b.** The outcomes obtained when Alice and Bob measure in different bases can be used to perform a Bell test to verify that they are effectively receiving entangled states. **c.** In the E91 protocol, the results obtained when the users measure in the same basis are used for the generation of the key, while those obtained when they choose different bases are used to monitor the eavesdropping on the channel.

50% of the time, they will obtain the same measurement outcome. Therefore, in this scheme, Alice and Bob shall announce publicly their measurement bases, and when they match, use the outcome of their measurements to generate the secret key.

The security of these types of protocols is based on two properties of quantum systems: the fact that the observation of a quantum system has an impact on the state of the system itself (fundamental for the BB84 protocol as well), and the monogamy of entanglement [35]. The latter guarantees that two qubits that are maximally entangled cannot be correlated with a third party. For this reason, an important step in the execution of entanglement-based protocols is the certification of the entanglement. This is generally done through CHSH-like correlation measurements [36], which provide a practical way to test the violation of Bell inequalities [37] and thus quantify the degree of entanglement between the two photons.

From a historical point of view, these types of protocols were particularly relevant because they highlighted the relevance of entanglement for quantum cryptography. Entanglement proved to be an essential resource for other areas of quantum information, such as quantum repeaters [38, 39] (discussed later in section 1.4.2) and Device Independent (DI) QKD [40, 41].

1.2.3 Measurement Device Independent QKD

The proposals of the first QKD protocols (BB84 and E91) were soon followed by their first experimental implementations [42–45]. These experiments made apparent that despite the conceptual interest of the entanglement-based protocols (E91 and BBM92), their implementation was more challenging than prepare-and-measure (such as BB84) type of configurations. The challenges were mainly related to the construction of robust and high rate entangled photon source, and to the impact on performance and complexity of multiple detection stations. For these reasons, the experimental implementations of prepare-and-measure QKD became the most common.

As more QKD experiments were demonstrated, attention was drawn to more technical aspects of QKD. Researchers soon discovered that although most of QKD protocols can be proven to be information-theoretic secure, their practical implementation have often small deviations from the ideal model that undermine the security of the communication. These imperfections may introduce security loop-holes that can be exploited by eavesdroppers to gather full or partial information on the exchanged key [46, 47]. With time, it became apparent that the weakest components of practical QKD are the single photon detectors [48, 49].

In order to overcome this problem, a new type of protocol called Measurement-Device Independent QKD (MDI-QKD) [50, 51] was introduced in 2012. MDI-QKD exploits a more practical way to establish entanglement between the users involved in the communication, and, as the name suggests, its implementation security is completely uncorrelated to the devices used for the measurement, including the detectors. In fig. 1.3, a schematic representation of an MDI-QKD setup is shown. Similar to E91, in MDI-QKD, the communication link between Alice an Bob is configured as a three-node network. But, while in E91 the entangled photons are generated in the middle node and then distributed to the communicating users, in MDI-QKD the photons are prepared by Alice and Bob who send them to the middle node (often referred to as Charlie), where they effectively generate an entangled Bell state by means of optical interference.

In the following, we will give a simplified description of an MDI-QKD protocol where the encoding users have single photon sources and execute polarisation encoding. The protocol starts with Alice and Bob randomly and independently preparing one of four polarisation BB84 states: $|H\rangle$ and $|V\rangle$ for the $\mathcal{Z}$ basis, and $|D\rangle$ and $|A\rangle$

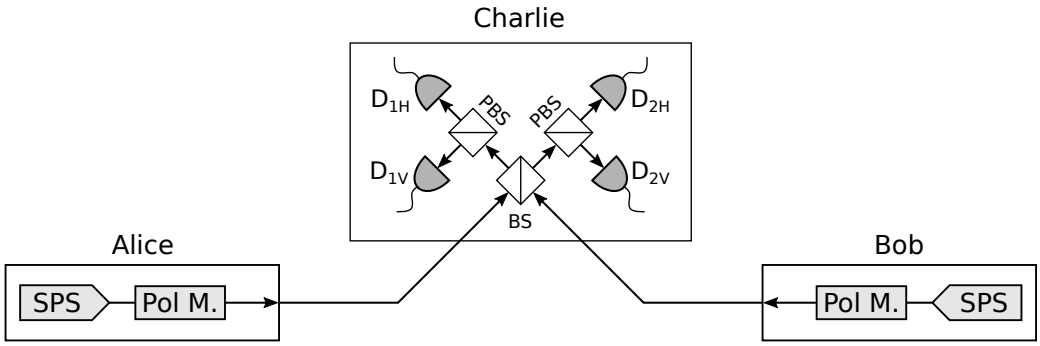

Figure 1.3: Scheme of a single-photon, polarisation based MDI-QKD setup. SPS: Single Photon Source, Pol M.: Polarisation Modulator, BS: Beam Splitter, PBS: Polarizing Beam Splitter, D_{xx}: single photon detectors.

for the $\mathcal{X}$ basis. They then send their photons to Charlie through the two quantum channels. Charlie performs a Bell State Measurement (BSM) on the quantum system generated by the interference of Alice's and Bob's photons. Entanglement between these photons is generated by their interference on a 50:50 Beam Splitter (BS) at the receiving station, whose outcome is governed by the Hong-Ou-Mandel rule [52]. Successively, Charlie measures the interference outcome with the setup represented in fig. 1.3. Here, four detectors collecting the output of the two Polarizing Beam Splitters (PBSs) are placed after the BS. A coincidence measurement between D_{1H} and D_{2V} or between D_{1V} and D_{2H} indicates the projection into the singlet state $|\psi^-\rangle = \frac{|HV\rangle - |VH\rangle}{\sqrt{2}}$, while a coincidence measurement between D_{1H} and D_{1V} or between D_{2H} and D_{2V} signals the projection into the triplet state $|\psi^+\rangle = \frac{|HV\rangle + |VH\rangle}{\sqrt{2}}$. Other detection combinations are considered unsuccessful and discarded. It is worth noting that the implementation of the BSM with linear optics allows to distinguish only 2 out of 4 Bell states. This is nevertheless sufficient for the protocol execution. When Alice and Bob prepare their states using the same basis, the measurement outcomes ($|\psi^-\rangle$ or $|\psi^+\rangle$) are strictly related to the parity of their encoded states, i.e., on whether they encoded the same or different state within the same basis. This is exploited for the key generation.

After the detection Charlie broadcasts the measurement results over a public channel. Alice and Bob then announce publicly their encoding bases, and if they match, they (and only them) can infer the state (and thus the bit) encoded by the other user. This process (which is equivalent to the key sifting in BB84) is followed by an error correction and a privacy amplification phase. The most interesting feature

of this protocol is that the BSM is used only to postselect entanglement, and can therefore be treated as a black box. This implies that the MDI-QKD removes all the detection side channels and that, more broadly, the security of the protocol would not be compromised even if Charlie was an adversary with malicious intents.

After its first introduction in 2012, experimental MDI-QKD demonstration followed shortly [53–56]. In 2014, a demonstration over 200 km of fibre was executed. A result that was improved further in 2016 when a demonstration over 400 km of fibre was achieved [57]. Another important result was achieved in 2016 when the rate of MDI-QKD was increased to 1 GHz and a Secure Key Rate (SKR) of 1 Mbit s^{-1} was demonstrated over short distances [58].

1.3 Practical QKD

In the previous sections we have introduced the main concepts of QKD, and we discussed the fundamental principles of operation of a few protocols. The descriptions of the protocols given in sections 1.2.1 to 1.2.3 were quite simplistic, in the sense that we did not really consider how the discussed systems can be implemented experimentally.

In this section we will focus on two main aspects of QKD realisation. In sections 1.3.1 and 1.3.2 we will discuss the implementation details of the photon sources in QKD. In section 1.3.3 we will explain the fundamental concepts of the *security analysis*, a set of theoretical tools that provides a recipe for what experimental data should be collected and how it should be analysed, resulting in a guaranteed Secure Key Rate (SKR) generated by a protocol.

1.3.1 Single Photon Sources and Weak Coherent Pulses

The information carriers most commonly used for quantum cryptography are photons. The main reason for this choice is the low scattering coefficient that photons have in several media, which makes them suitable for long distance transmission [24]. In all QKD protocols discussed so far (sections 1.2.1 to 1.2.3), the information was encoded on *single* photon Fock states[1]. This was done to avoid encoding the same information onto two different quantum systems, an eventuality that would invalidate the protocols hypothesis.

Desirable features for an ideal single photon source are [59]:

[1] Fock states are quantum states with a well defined number of particles.

- deterministic emission of a photon, at an arbitrary rate, upon user's request;
- that subsequent photons are indistinguishable;
- that there is a 0% probability of multi-photon emission.

To date there is no single source having all of the properties above, and all the promising candidates display deviations from these characteristics. Most of the deterministic single photon sources being investigated today exploit specific transitions of specific quantum systems such as color centres, quantum dots, single atoms, single ions, single molecules or atomic ensembles [60]. Unfortunately, all these solutions are difficult to implement experimentally, and so far have led to QKD implementations with poor performances both in terms of key rates and distance [61, 62].

For these reasons, almost all QKD implementations today rely on approximations of single photon sources via Weak Coherent Pulses (WCP), which are laser pulses with an average number of photons per pulse below one [63, 64]. Contrary to single photon sources, WCP sources can offer high repetition rate, simplicity of use, as well as ambient operating temperatures. The state of a laser generated pulse can be described within its coherence time as a coherent state $|\alpha\rangle$, with α a complex number decomposable as $\alpha = \sqrt{\mu}e^{i\theta}$, $\mu = |\alpha|^2$ the average number of photons in the pulse, and θ the phase of the optical field [65, 66]. The coherent state can be expanded in the Fock basis as:

$$|\alpha\rangle \equiv |\sqrt{\mu}e^{i\theta}\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{1.2}$$

It is possible to demonstrate (see ref. [67]) that the number of photons in a given coherent state $|\alpha\rangle$ follows a Poissonian distribution:

$$\mathcal{P}(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}. \tag{1.3}$$

Figure 1.4 shows the photon number distribution for WCPs with increasing average photon number. From a practical perspective, when using WCPs to approximate single photon sources, the value of μ is subject to a tradeoff between minimising the number of multi-photon pulses while having at the same time a sufficient number of one-photon pulses to carry the information.

The nonzero probability of multi-photon pulses in WCPs has immediate security implications. A malicious adversary (often referred to as Eve) could exploit them to perform an attack known as Photon Number Splitting (PNS) [63, 68]. In this attack,

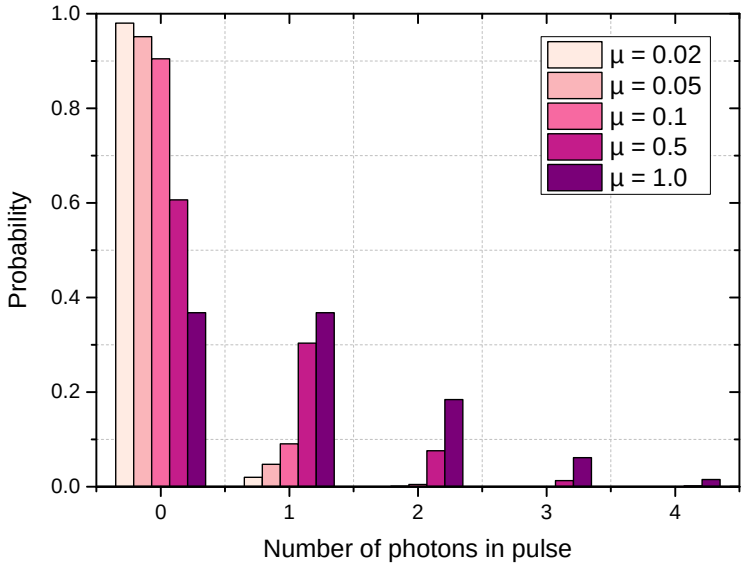

Figure 1.4: Photon number distribution in WCPs with different photon fluxes (μ).

Eve first executes a quantum nondemolition measurement to obtain information on the number of photons in the WCP sent by Alice to Bob. If she detects the presence of a single photon in the pulse she blocks it, and nothing arrives to Bob. While, if she senses more than one photon, she sends one photon to Bob and stores the remaining ones. Eve can then tap into the basis reconciliation conversation between Alice and Bob, which is executed over the public channel, and measure the photon(s) in her possession accordingly. With this strategy, Eve can get full information on the multi-photon WCPs exchanged by the communicating parties, and get full knowledge of the final key without being detected.

The implications of PNS had a severe impact on the development of QKD. On a practical level, it restricts the maximum distances of QKD executed with WCPs below 30 km [69]. On a more general level, it casted doubts on the practicality of QKD done with WCPs. Luckily, the introduction of the decoy state method, which will be the subject of the next section, provided a way to overcome this problem.

1.3.2 Decoy State Method

The decoy state method is the most common strategy employed in modern QKD to tackle the problem of multi-photon WCPs [70–72].

In this technique, an encoding user chooses from various phase randomised pulses at different intensities and sends them through the communication channel. The

pulses need to be indistinguishable apart from their different intensity. The intensities of the pulses are revealed by the encoding user (for example, Alice) only after the pulses are detected by the receiving user (for example, Bob). Only the detections that occurred from pulses with a specific photon flux, the *signal* or s photon flux, are used for the key generation. Detections that occurred when other intensities were prepared by Alice are used to monitor the transmittance of different photon-number components. With this information, the users can bound tightly the number of detections arising from single photon components.

Let us now see how this technique can neutralise the PNS attack. If Eve tries executing it now, she would change the transmittance of the pulses depending on her sensed photon-number states. Alice and Bob would then be able to detect her presence by observing different yields for different decoy states.

Without using the decoy state technique, it was found (see ref. [63]) that in order to maintain the security of the most common QKD protocols, it was necessary to reduce the average photon flux prepared by the sender proportionally with the increase of the channel loss. This dependance of the pulses intensity on the channel transmission (indicated with η) impacted the SKR scaling over distance of the protocols, which was forced to scale $\propto \eta^2$. This, on a practical level, limited the maximum operation distance of QKD to few tens of kilometres [73].

Remarkably, by adopting the decoy state technique, the SKR of the protocols could be improved to scale linearly with the channel transmission ($\propto \eta$), which increased the maximum distance achievable for QKD to a few hundreds of kilometres. In general, the decoy state method improves the performance of all Discrete Variable (DV) QKD protocols that rely on WCPs.

A requirement accompanying the implementation of the decoy state method is the phase randomisation of the optical pulses. This is needed to satisfy the assumptions of the majority of security proofs [74], which require a photon number channel, i.e., that the output state of Alice can be expressed as:

$$\rho_A = \sum_{n=0}^{\infty} P(n) \left|n\right\rangle \left\langle n\right|, \tag{1.4}$$

with only diagonal terms appearing in the density matrix ρ_A. In general, the density matrix ρ_α associated to a coherent state $\left|\alpha\right\rangle$

$$\rho_\alpha = \left|\alpha\right\rangle \left\langle\alpha\right|, \tag{1.5}$$

will include non diagonal terms. This can be fixed by phase randomising the coherent

states, in which case one obtains:

$$\frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}|\, d\theta = \rho_A = \sum_{n=0}^{\infty} P(n,\mu)\,|n\rangle\langle n|\,, \tag{1.6}$$

with now only diagonal terms appearing in ρ_A, and with $P(n,\mu)$ as in eq. (1.3). For this reason, the vast majority of modern QKD implementations feature WCPs randomisation.

1.3.3 Experimental QKD Quantities and Asymptotic and Finite Size SKR Analysis

As discussed at the end of section 1.2.1, the last step of every QKD protocol is the **privacy amplification**. The amount of privacy amplification to be executed on the error corrected sifted keys is determined by the security analysis of the protocol. The security analysis evaluates how much of the key distribution was secure, which in turn affects the number of secret bits that can be extracted from a given key exchange. It is the security analysis that provides a formal relationship between the quantities measured experimentally and the final Secure Key Rate (SKR) of a particular protocol.

The measurable experimental quantities that we often need in decoy state QKD protocols are yield, gain and Quantum Bit Error Rate (QBER), which are defined as follow:

Yield - the probability of detecting a signal at the receiver for a given transmitted state. Y_μ denotes the yield for a phase randomised input state with mean μ, and Y_n denotes the yield for the Fock state $|n\rangle$.

Gain - the probability of transmitting a certain signal and having a corresponding detection event at the receiver. Q_μ denotes the gain for a phase randomised input state with mean μ, and Q_n denotes the gain for the Fock state $|n\rangle$.

QBER - quantity associated to each prepared photon flux (μ), and often referred to as E_μ in the formulas. Amount of error detections over all the detections made during the protocol, for each specific photon flux μ. The definition of error detection is protocol-dependant.

First-approximation SKR formulas analyse these quantities under the assumption that a very large number of pulses ($n \gg 1$, ideally infinite) were exchanged during

the protocol. This assumption implies that since the considered dataset is of infinite size, the measured quantities coincide with their true values. This type of analysis is called *asymptotic scenario*, and leads to optimistic SKRs.

In reality, in practical QKD the users will exchange signals until they have built a raw key block of a certain size, say 10^6 bits, at which point they will start the post-processing. Given the finite size of the analysed blocks, the measured quantities will be affected by statistical fluctuations which will distance them from their true value. This is known as the *finite-key-size effect* [75–79]. In this case, the security analysis will have to take into account the effect of statistical fluctuations, and use the block size and the measured quantities to estimate the interval over which each specific quantity could have taken value. For the key estimation, the case leading to the worst key (and thus the best security) is chosen. For this reason, the finite size analysis often leads to a significant reduction of the protocol SKR, especially if the size of the analysed block is small.

1.4 Overcoming the Limitations of Point-To-Point QKD

A direct consequence of the postulates of quantum mechanics [80] is that it is not possible to perfectly clone an unknown quantum state, or a state drawn from a set of two (or more) nonorthogonal states [81]. This result is known as the *no-cloning* theorem. It was demonstrated and clearly stated for the first time in ref. [82] and has fundamental implications for quantum communications.

The first one, and probably the most obvious, is related to the security of QKD. The no-cloning theorem guarantees that an eavesdropper cannot make a copy on the transmitted qubit and store it for a later measurement.

The second one is related to the range of QKD. Since any transmission channel is characterised by a finite, nonzero, loss coefficient (often indicated by the symbol α), the no-cloning theorem poses a limit on the distance a quantum system can be transmitted for while maintaining a reasonable probability of detecting it. This is in contrast with the transmission of classical signals, which can be amplified (i.e., cloned) to extend their transmission range. As an example, in classical optical communication over optical fibres signals are generally amplified with Erbium-Doped Fibre Amplifiers (EDFAs).

In the following sections we will discuss in more detail the consequences of the no-cloning theorem on the maximum loss (and thus maximum transmission distance)

sustainable by quantum communications. In section 1.4.1 we introduce a formal theorem quantifying the constraints for point-to-point QKD. In section 1.4.2 we present the concept of quantum repeaters, while in section 1.4.3 and section 1.4.4 we discuss in detail measurement-based and entanglement-based quantum repeater architectures.

1.4.1 Repeaterless Secret Key Capacity Bound

One question that arises naturally when considering the transmission of quantum information over a pure-loss channel is: what is the maximum amount that can be transmitted over it? In quantum information theory terms [81], this question corresponds to evaluating the *capacity* of the quantum channel (or $\mathcal{C}_{quant}$).

At first sight, it seems reasonable to expect the quantum capacity of an uninterrupted (often referred to as point-to-point) communication channel to scale linearly with the number of carriers reaching the end of the line. A condition that can be expressed in terms of channel transmission as $\mathcal{C}_{quant}(\eta) \propto \eta$. Over recent years, the relevance of the question encouraged a precise investigation of the subject, which culminated with the results presented in [83, 84]. Ref. [84] in particular identifies the ultimate Secret Key Capacity (SKC) for point-to-point QKD communications, a limit that is often referred to as SKC_0 (where the subscript indicates the lack of intermediate relays along the communication line) or PLOB bound, from the name of the authors of ref. [84].

Reference [84] establishes that the SKC_0 of a pure loss channel is:

$$\mathcal{C}_{quant}(\eta) = R_{SKC_0}(\eta) = -\log_2(1-\eta), \tag{1.7}$$

which, for high attenuations, can be approximated to $SKC_0 \approx 1.44\eta$. This bound can only be overcome if the users at the two ends of the communication line (Alice and Bob) preshare some secret randomness or if there is a quantum repeater or relay splitting the quantum communication channel and assisting them.

Alongside the aforementioned characterisation of the maximum capacity of the quantum channel, it is also possible to assess the maximum SKRs obtainable in ideal conditions by several QKD protocols, including the ones already discussed in this thesis, which we will report below. All the following equations can be found in ref. [27].

For BB84 protocol implemented with a perfect single photon source the ideal

SKR is:

$$R^{ideal}_{BB84,\,single\,photons}(\eta) = \eta. \tag{1.8}$$

For BB84 protocol implemented with decoy states the ideal SKR is:

$$R^{ideal}_{BB84,\,decoy}(\eta) = \frac{\eta}{e}. \tag{1.9}$$

The ideal SKR for MDI-QKD implemented with decoy states is:

$$R^{ideal}_{MDI-QKD,\,decoy}(\eta) = \frac{\eta}{2e^2}. \tag{1.10}$$

By looking at eq. (1.10), it is apparent that the ideal SKR of the MDI-QKD protocol does not overcome the SKC_0 (eq. (1.7)), and that it actually performs worse than the comparable BB84 protocol (eq. (1.9)). This may seem counterintuitive considering that in MDI-QKD there is a relay between Alice and Bob splitting the length of the quantum channel. One would think that this allows MDI-QKD to overcome the limitations of point-to-point QKD. This does not happen due to the type of measurement used in the protocol to distill the secret key, which is a BSM that requires the simultaneous detections (coincidences) of two photons (one from each user) at the central node. This is the reason why MDI-QKD does not beat the SKC_0.

Figure 1.5 shows the curves associated to eqs. (1.7) to (1.10) for comparison.

1.4.2 Quantum Repeaters: Trusted and Untrusted Architectures

In this and the following sections, we will follow the reasoning presented in ref. [27] and take the perspective of quantum information theory to classify different quantum repeater architectures. It is worth mentioning that this categorisation can sometimes differ from that used in the quantum optics/devices research communities[1]. However, the information theory approach has the advantage of providing a theoretical framework to clearly separate all the different repeater architectures based on their specific characteristics.

In an information-theoretic sense, a quantum repeater is any type of middle node between Alice and Bob that helps their quantum communication by breaking down their original quantum channel in two different sub-quantum channels [27].

[1] In quantum optics/devices research communities, a quantum repeater is often referred to as a solution/system/platform that extends the transmission range of a quantum state and that should be scalable by default.

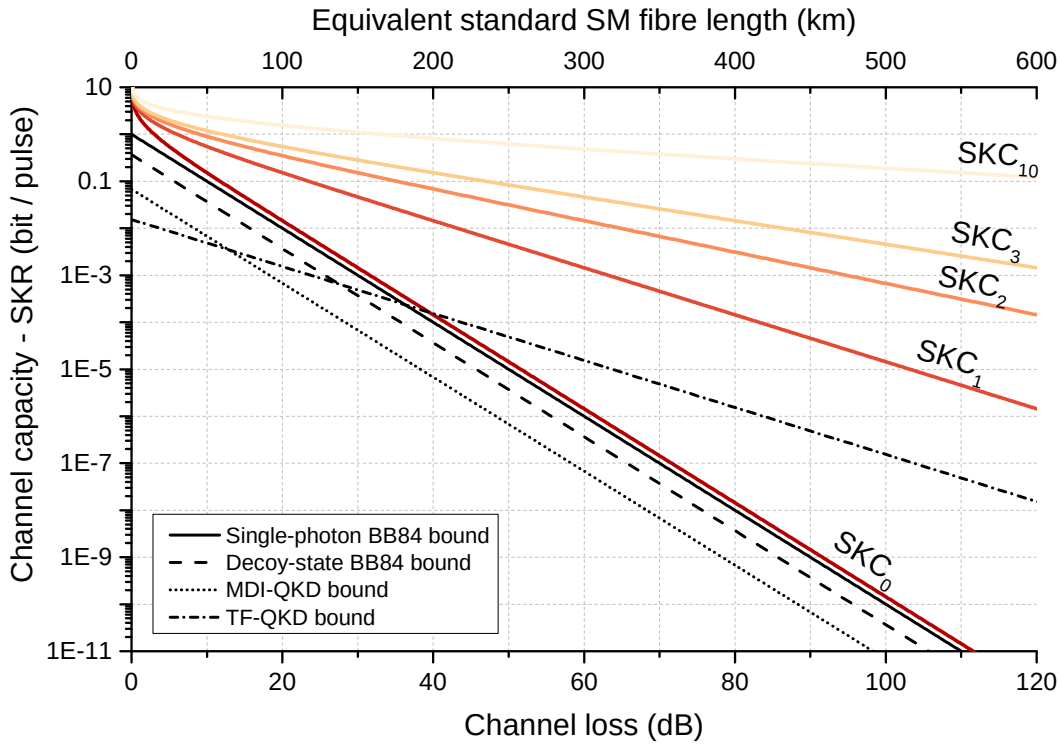

Figure 1.5: SKC_0 is the repeaterless secret key capacity, or PLOB, bound (see eq. (1.7)). SKC_n is the capacity of a quantum channel aided n equally spaced quantum repeaters (which will be discussed in section 1.4.4, eq. (1.12)). The curves follow the relation reported in eq. (1.12). In the graph are also reported the maximum, or ideal, SKR for several protocols introduced in this chapter (eqs. (1.7) to (1.10) - see legend at the bottom-left).

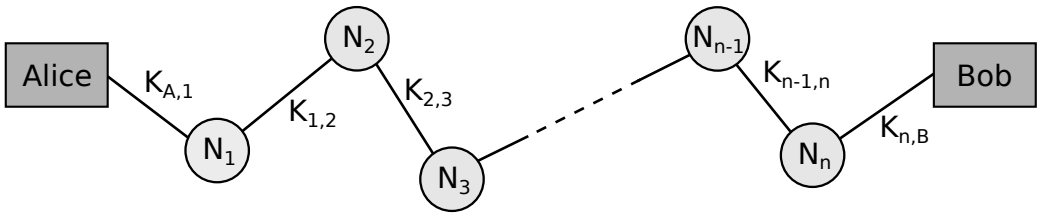

Figure 1.6: Representation of a one-dimensional trusted node QKD network. The distance between Alice and Bob is split into shorter segments by n nodes N_i. Adjacent nodes N_i and N_{i+1} establish a secret key $K_{i,i+1}$ through point-to-point QKD. In this one-dimensional network, Alice and Bob have to trust all the nodes between them because these will gain full knowledge of the secret message that they want to share.

This broad definition includes many different types of architectures, which can be categorised based on some relevant features. The first distinction that should be done is based on security arguments, and distinguishes between *trusted* and *untrusted* repeaters.

Trusted repeaters, also known as trusted nodes, are today's most commonly employed solution for situations where the distance between Alice and Bob is too large for point-to-point QKD [85, 86]. In the trusted repeater architecture, the communication is aided by inserting along the transmission line intermediate nodes that execute point-to-point QKD between them. This way the channel connecting Alice and Bob is split into shorter sections with length suitable for point-to-point QKD, see scheme in fig. 1.6. This solution solves the problem of loss of the information carriers at the cost of security. Assuming there is only a single, one-dimensional, link of trusted nodes connecting Alice and Bob, the two users will have to rely and place unconditional trust on all of the intermediate nodes. This is a hefty requirement in terms of security assumptions. A single misbehaving node along the line would compromise the security of the entire communication network and prevent Alice and Bob from sharing their message.

Untrusted repeaters, on the contrary, are devices that may be operated by an untrusted party without affecting the security of the key generation process. A protocol performed with untrusted QKD repeaters offer end-to-end security, in the sense that its security only relies on its end users. Untrusted repeaters can be further divided into two classes: *measurement-based* and *entanglement-based* quantum repeaters, which will be discussed in the following sections.

1.4.3 Measurement-Based Quantum Repeaters

In measurement-based repeater architectures, the middle node breaking up the channel between the communicating users is the measurement station and both the users aiming at establishing a common secret key act as transmitters. With its measurements, the central node gets some information about the correlation between the pulses prepared by the users. This information is non-conclusive about the bits composing the final key without some other pieces of information available only to the encoding users. Therefore, after the public announcement of the measurement result, the transmitting users are able to distill a secret key without the central node necessarily obtaining any insight about it.

We have already encountered an example of this type of architecture in the form of MDI-QKD, discussed in section 1.2.3. As already observed at the end of section 1.4.1, despite the presence of the middle node, the SKR of MDI-QKD cannot overcome the SKC_0 bound. This leads us to the introduction of another relevant characteristics of quantum repeaters, their *effectiveness*.

A quantum repeater is said to be *effective* or *active* only if it helps the users to beat the performance of any point-to-point protocol, i.e., the SKC_0 bound. In light of this, we can understand the deeper meaning of the SKC_0 bound: besides characterizing the fundamental rate-loss scaling of point-to-point QKD, it also provides the exact benchmark for testing the quality of quantum repeaters.

If aided by quantum memories [87–89], MDI-QKD could overcome the SKC_0 bound [90]. Encouraging demonstrations of memory-assisted MDI-QKD have been recently reported in refs. [91, 92]. However, as will be discussed in section 1.4.4, the development of quantum memories has not yet reached a stage where they are practical enough to be easily integrated in QKD systems. And the experiments executed so far were over limited distance. Entanglement-based quantum repeaters [93, 94], which will be discussed in section 1.4.4, are expected to allow the overcoming of the SKC_0 bound. But entanglement-based quantum repeaters are even more complex than quantum memories, and the same caveats of current technological infeasibility applies to them. For these reasons, until very recently it was thought that the implementation of an effective quantum repeater was out of reach with current technology.

This belief was shattered in 2018 with the introduction of the Twin-Field QKD (TF-QKD) protocol [95], a novel measurement-based type of quantum repeater that

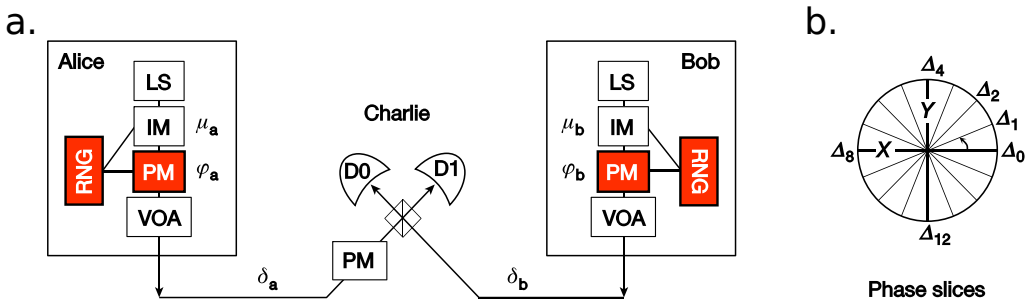

Figure 1.7: Schematics of the original TF-QKD proposal reproduced from ref. [95]. **a.** Set-up to implement TF-QKD. Alice and Bob use their light sources (LSs) to generate WCPs that are modulated to different intensities $\mu_{a,b}$ by Intensity Modulators (IMs). Phase Modulators (PMs) combined with random number generators (RNGs) encode the phase $\varphi_{a,b}$ onto the pulses. Variable Optical Attenuators (VOAs) set the average photon flux to the correct value. After travelling through the quantum channel, the pulses interfere at Charlie's BS to be then detected by the single-photon detectors D_0 and D_1. **b.** Discretisation of the phase space to identify the twin fields during the phase reconciliation stage of the protocol.

the authors proved capable of overcoming the SKC_0 bound, and that is feasible with today's technology. A description of the protocol is provided in the following subsection.

Twin-Field Quantum Key Distribution

In this section we will give a brief introduction to the Twin-Field QKD protocol [95], with the aim of highlighting its most important characteristics. Given the fundamental role this protocol has played in my research over the past years, a more detailed description and discussion of the protocol (and its variants) will be given in chapter 2.

Figure fig. 1.7.a shows a schematic representation of the Twin-Field QKD (TF-QKD) setup. In Twin-Field QKD, the encoding users, Alice and Bob (i = A or B), prepare and send to the central relay (Charlie) two phase randomised optical fields. More precisely, they generate WCPs (or dim pulses) with intensities ξ_i randomly selected between the *signal* intensity $\frac{u}{2}$, and the *decoy* intensities $\frac{v}{2}$ and $\frac{w}{2}$: $\xi_i \in \frac{\{u,v,w\}}{2}$.

For phase randomisation purposes, the users divide the interval $[0, 2\pi)$ into M equal slices Δ_k with $k = \{0, 1..., M-1\}$ (see fig. 1.7.b), they randomly select a phase $\delta_i \in [0, 2\pi)$, and record to which phase slices Δ_k^A (for Alice) and Δ_k^B (for Bob)

their values δ_A and δ_B belong. They continue their phase encoding by selecting $\alpha_i \in \{0, \pi\}$ which encodes a bit $(0, 1)$ and $\beta_i \in \{0, \pi/2\}$ which determines the basis. They finally sum all the phase components together into $\varphi_i = (\alpha_i + \beta_i + \delta_i) \oplus 2\pi$, and use a PM to encode the φ_i phase on their dim optical pulse. After the intensity and phase modulation, the users send their pulses to the central node, Charlie.

At Charlie, the optical fields interact on a BS to produce a single photon (or first-order) optical interference. The interference outcome is recorded by two single photon detectors (D_0, D_1 in fig. 1.7.a) placed at the outputs of the BS. When both or none of the detectors click the measurement is discarded. When a single detector clicks, Charlie announces publicly which one did.

In cases where the intensities, the basis, and the phase slices of the interfering pulses are matched, which of the detectors clicks depends only on the phase difference of the information bit (α_i) encoded by the users. In the matching instances where $\xi_i \in \frac{\{v,w\}}{2}$ the users reveal also α_i, and they use theirs and Charlie's announcements to perform estimation of the error rates and the decoy-state paremeters. In the matching instances where $\xi_i = \frac{u}{2}$, they can use Charlie's announcement to infer the bit encoded by the other user and use it to grow their shared secret key.

The protocol reliance on a first-order optical interference explains two things: its name and its different SKR scaling compared to MDI-QKD. The term 'twin-field' comes from the fact that the key generation depends on the interference of optical fields having electromagnetic phases that are similar enough to allow the users to comfortably predict their interference outcome.

The most important feature of TF-QKD is that it constitutes an effective measurement-based quantum repeater. A precise analysis of the protocol [27, 95] set its ideal SKR to:

$$R^{ideal}_{TF-QKD}(\eta) \simeq 0.0154\,\sqrt{\eta}, \tag{1.11}$$

which shows how, differently from all the other protocols we have seen so far, the SKR of TF-QKD scales with the square root of the channel transmission. This allows the protocol to overcome the SKC_0 ($\simeq 1.44\eta$) at high attenuations. For a channel constituted of standard optical fibre with loss coefficient of $0.2\,\mathrm{dB\,km^{-1}}$, R^{ideal}_{TF-QKD} overcomes the SKC_0 around 200 km of channel length. The factor in front of $\sqrt{\eta}$ in eq. (1.11) comes from the combined effect of several factors: the use of the decoy states and the slicing of the 2π phase range in M slices, which reduces the matching instances between the users by a factor M and introduces an intrinsic error in the protocol.

Finally, it is worth stressing again the cause for the different scaling of the SKR of TF-QKD compared to MDI-QKD. In MDI-QKD, the Bell measurement used for the key generation requires the photons prepared by both users to arrive simultaneously at the receiving station and two detectors to click simultaneously. By way of example, let us consider a symmetric three node network with overall transmission coefficient η. The two channels connecting the transmitting users (Alice and Bob) to Charlie will be characterised by transmission $\eta_A = \eta_B = \sqrt{\eta}$. The probability for Charlie to receive simultaneously the photons from both Alice *AND* Bob is: $\eta_A \cdot \eta_B = \eta$, which sets the scaling of the SKR. By contrast, in TF-QKD the measurement executed at the central node is a single photon detection that requires a single photon, either from Alice *OR* Bob to reach the relay. An event that happens with probability proportional to $\sqrt{\eta}$. From here the different SKR scaling of the two protocols follows.

It is also worth noting that, similarly to MDI-QKD, the implementation security of TF-QKD is independent of the characteristics and operation of the detectors.

1.4.4 Entanglement-Based Quantum Repeaters

In section 1.4.3 we have discussed how measurement-based quantum repeaters in the form of TF-QKD can have a SKR-to-loss scaling $\propto \sqrt{\eta}$. This provides a way to overcome the SKC_0 bound and extend the range of QKD beyond the limits of point-to-point protocols. Such improvement has very concrete consequences for fibre-based QKD implementations, allowing for the first time to establish QKD links over national or even international distances. However, the maximum range of a single TF-QKD link is still limited and it is unclear whether it is possible to devise an untrusted measurement-based quantum repeater scheme that scales to arbitrarily long distances.

For these reasons, it is interesting to look at the possible solutions to extend even further the range of quantum communications based on untrusted nodes, with the intent of allowing them to cover global distances. The most promising technology to solve this problem are *entanglement-based quantum repeaters* [96]. Quantum repeaters are strctures that overcome the limitations imposed by the no-cloning theorem by harnessing the properties of entanglement, another purely quantum phenomenon. We have already discussed how entanglement and its unique correlations can be directly exploited by QKD in section 1.2.2. Entanglement becomes a resource also for long distance quantum communications when it is used to implement *entangle-*

ment swapping and *quantum teleportation* [97–99]. These two related techniques allow entangling of two originally independent quantum systems by means of already entangled states, Bell state measurements, and classical communication.

The original scheme for entanglement-based quantum repeaters (see ref. [96]) is based on the idea of placing several nodes operating entanglement swapping (and purification [100–102]) along a communication line that would be otherwise too lossy for point-to-point communication. This way, the transmission loss problem is substituted by the entanglement distribution one. A schematic representation of this scheme is given in fig. 1.8. Here, Alice and Bob are connected by a communication line equipped with n quantum repeater stations R_i. The entanglement distribution scheme follows the steps below:

(a) Each repeater station is endowed with a quantum memory and generates a maximally entangled photon pair composed by the two elements $|E_i\rangle$ and $|E_i'\rangle$;

(b) Each node keeps one of the two elements $|E_i\rangle$ and distributes the other one $|E_i'\rangle$ to an adjacent node;

(c) Each node stores both the original and the received entangled states in their quantum memory before proceeding to the next step;

(d) When all the nodes are in possession of their original $|E_i\rangle$ and received $|E_{i+1}'\rangle$ entangled states, they execute entanglement swapping [97] between them;

(e) After swapping is executed by all nodes, Alice and Bob end up sharing an entangled photon pair which can be directly used to implement E91 QKD or to transfer any arbitrary quantum state from one user to the other via quantum teleportation [97].

The presence of n quantum repeaters in a quantum channel alters its capacity, which becomes (assuming evenly spaced nodes) [103]:

$$\mathcal{C}_{quant}(\eta, n) = -\log_2(1 - \sqrt[n+1]{\eta}). \tag{1.12}$$

The channel capacity for links aided by an increasing number of quantum repeaters is shown in fig. 1.5. It is worth noting here that since TF-QKD is an *effective* 1-node quantum repeater, it features the SKR scaling of a single node quantum repeater.

The scheme represented in fig. 1.8 can be applied to channels of arbitrary length at the cost of adding more nodes, potentially providing the final solution to the problem

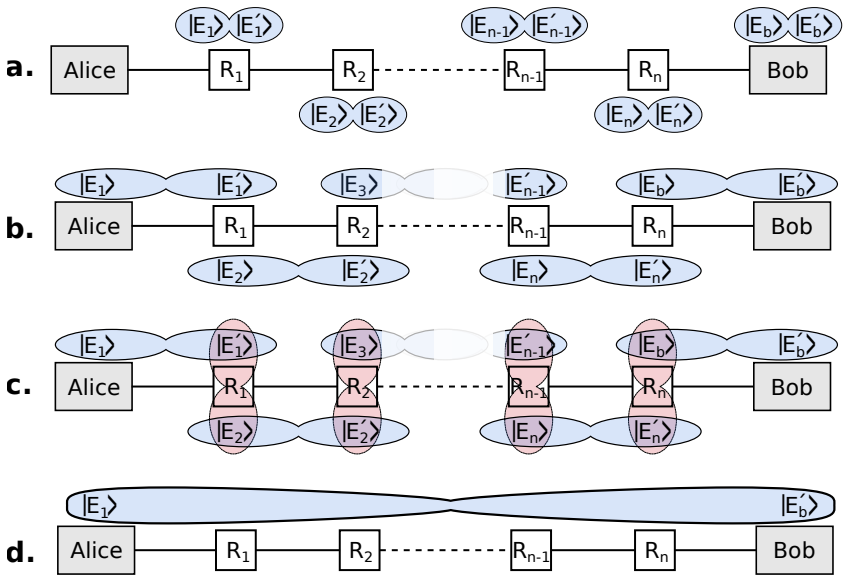

Figure 1.8: Quantum communications aided by entanglement-based quantum repeaters.

of long-distance quantum communications. Its experimental implementation though is very challenging. Although all the steps described above have been proven possible individually [104–106], they are complex processes at the edge of today's technological capabilities. When combined together, the steps described above produce a very low chance of success for the whole process. In order for entanglement-based quantum repeaters to become a viable component for quantum networks, further development of quantum memories, entanglement purification and swapping is required.

1.5 Research Motivations and Thesis Organisation

In the previous sections, we have described how quantum communications performance is affected by channel loss. Practically speaking, this limits the range of today's QKD implementations, with the longest (non-TF-QKD) fibre-based experiments reaching a maximum distance of 421 km [107] in a laboratory environment and of 130 km [108] in field deployments.

In the previous sections we have introduced the concept of quantum repeaters, and explained how these could help extending the operation range of QKD. Another way to extend the range of quantum communications is transferring the qubits via channels characterised by an attenuation coefficient lower than that of optical fibres. The most promising results in this direction have been obtained by

satellite-based QKD, which has been an area of intense research over the past twenty years [106, 109–111]. Satellite based quantum communications at the moment are focused on overcoming the limitations of point-to-point QKD by establishing ultra-long communications that exploit the geometric optical loss outside the atmosphere. Recently, landmark results have been obtained in this area, with a 1200 km satellite to ground QKD transmission demonstrated in 2017 [112], a satellite-relayed intercontinental QKD transmission in 2018 [113], and an integrated space-to-ground quantum communication network over 4600 km demonstrated in 2021 [114]. There are a few factors that prevent satellite QKD from being the definitive solution for long distance quantum communications though:

- expensive equipment and facilities needed to operate it;
- high dependence on atmospheric conditions of these links;
- intermittent nature of the links, conditioned by the limited time the satellite is in the field of view of a telescope;
- low rate of quantum information exchange that this architecture can currently support.

In light of this, research around quantum repeaters and practical ways to extend the range of quantum communications is still extremely relevant.

It is for this reason that the introduction of the TF-QKD protocol in 2018 [95] sparked considerable interest in the QKD community and a new wave of research activity [115–121]. The main motivation of this interest is related to the experimental feasibility of TF-QKD compared to that of entanglement-based repeaters, which are not yet at the stage to support stable and reliable long-distance operations.

The work described in this thesis covers the early experimental developments of the TF-QKD protocol at Toshiba Europe Ltd (TEUR) after its introduction in ref. [95]. Below is summarised the organisation of remainder of the material presented in the thesis.

- Chapter 2 describes in detail the TF-QKD protocol and its variants.
- Chapter 3 provides a background on the experimental techniques needed for the implementation of the TF-QKD protocol.

- Chapter 4 describes the first proof-of-principle TF-QKD experiment ever executed, which represents also the first implementation of an effective quantum repeater.

- Chapter 5 discusses a number of technical improvements made to the TF-QKD setup presented in chapter 4. These modifications were necessary to prepare the system to operate in more realistic scenarios.

- Chapter 6 describes a long-distance TF-QKD experiment that currently represents the longest fibre-based quantum communication ever performed.

- Finally, chapter 7 presents some final remarks on the work presented in this thesis while chapter 8 offers a perspective on future research directions that could be undertaken as a continuation of results presented here.

1.6 Novel Contributions of the Thesis

The work presented in this thesis focuses on the experimental realisation of the TF-QKD protocol. To this end, a new set of experimental techniques and methods was developed and introduced in the field of quantum communications, which resulted in the following contributions:

- First realisation of a time-multiplexed phase-stabilised QKD system and development of the setup and techniques required to implement it (reported in [122]).

- First realisation of a pair of optically-frequency-locked transmitters for quantum communications. Two techniques, Optical Injection Locking and Optical Phase-Locked Loop, have been tested and implemented for this purpose (reported in [122]).

- First successful implementation of the TF-QKD protocol and of the Curty-Azuma-Lo (CAL) and Sending-or-Not-Sending (SNS) variants. This was achieved in a proof-of-principle experiment conducted over highly attenuated optical channels (reported in [122]).

- The aforementioned proof-of-principle experiment is, to our knowledge, the first realisation of a QKD system capable of overcoming the SKC_0 bound, i.e.,

the theoretical limit restricting the key rate of point-to-point QKD (reported in [122]).

- Development of a compact and remotely controllable TF-QKD system capable of full intensity and phase encoding.
- Invention and development of the dual-band phase stabilisation technique for the phase stabilisation of long optical channels for quantum communications (reported in [123]).
- Phase-locking of two optical sources separated by 610 km of optical fibre. To our knowledge, this is the longest distance two lasers have been locked over for the purpose of quantum communications (reported in [123]).
- Phase stabilisation of a 1200 km long optical channel. To our knowledge, this is the longest (instantaneously) phase-stabilised channel ever implemented (reported in [123]).
- The aforementioned techniques were instrumental for the realisation of a second TF-QKD experiment performed over long optical fibres. This experiment generated a positive SKR over 555 km in the finite-size regime, and 605 km in the asymptotic regime. In both cases, these are the longest distances ever achieved in fibre-based QKD (reported in [123]).

Chapter 2

TF-QKD Protocol

In this chapter we will describe in more detail the TF-QKD protocol already introduced in section 1.4.3. In section 2.1 we will describe all the steps required for implementing the original protocol and provide its SKR formula. In section 2.2 we will discuss the scaling features of the protocol and provide a SKR graph for a realistic implementation of it. In section 2.3 we will detail the different variants of TF-QKD that have been proposed since its first publication in 2018. Finally, in section 2.4, we will explain the implementation challenges of TF-QKD and relate them to the specific requirements of this protocol compared to other QKD protocols.

2.1 Original TF-QKD Protocol Description and SKR Formula

Intuitively, the TF-QKD protocol (schematic reported in fig. 1.7) works as follow: Alice and Bob encode in phase and intensity on weak coherent optical pulses generated by their phase-locked lasers. The decoy state technique is still used to assess the properties of the quantum channels. The pulses are sent to Charlie through two phase stabilised channels. Once the pulses arrive at Charlie, he lets them interfere on a 50:50 BS. The two outputs of the BS are measured by two single photon detectors. Depending on which detector clicks, Charlie can infer if the prepared pulses had the same or different phase encoding. With the same information, the legitimate users can infer the bit encoded by the other user and therefore grow a shared encryption key.

Considering the central role played by the TF-QKD protocol in this thesis, below

is provided its precise implementation description as presented in ref. [95].

0. *Initial operations* – The $[0, 2\pi)$ phase interval is split into M equal slices $\Delta k = 2\pi k/M$, with $k = \{0, ..., M-1\}$. An authenticated channel is set up for the public announcements made by the legitimate users Alice and Bob.

1. *Classical stage* - The users send bright unmodulated optical pulses to the relay station, to let Charlie stabilise the communication channels and in particular minimise the phase misalignment $\delta_{ba} = \delta_b - \delta_a$.

2. *Quantum stage* – The users attenuate the optical pulses to the single-photon level and modulate their phase and intensity.

3. *Preparation* – Alice and Bob select random values for the intensities $\mu_{a,b} \in \{u/2, v/2, w/2\}$; the bit phases $\alpha_{a,b} \in \{0, \pi\}$, corresponding to bits {0, 1}, respectively; the basis phases $\beta_{a,b} \in \{0, \pi/2\}$, corresponding to bases $\{\mathcal{X}, \mathcal{Y}\}$, respectively; and the global random phases $\rho_{a,b} \in [0, 2\pi)$. They record in which phase slice Δk_a (Alice) or Δk_b (Bob) their values ρ_a and ρ_b fall into. They then prepare pulses with intensities $\mu_{a,b}$ and phases $\phi_{a,b} = (\alpha_{a,b} + \beta_{a,b} + \rho_{a,b}) \oplus 2\pi$ and send them to Charlie.

4. *Charlie's measurement and announcement* – Charlie interferes the incoming pulses and records which detector clicks. When the quantum communication is over, he publicly announces all the runs where his detector 0 (1) clicked; Alice and Bob will correspondingly set a variable χ equal to $0\,(\pi)$. All the runs where none of or both of his detectors clicked are discarded.

5. *Users's announcement and sifting* – After the previous step is complete, Alice announces the intensities μ_a, the basis phases β_a and the phase slices Δk_a and Bob announces the runs where his values match Alice's. The users discard all the mismatched runs. Then they disclose the bit values of the matched runs except those in basis $\mathcal{X}$ and intensity class u, which are kept secret.

6. *Raw key bit distillation and parameter estimation* – The users perform a coordinated random permutation of the bits. For the bits in basis $\mathcal{X}$ and intensity class u, Bob draws Alice's bit phase α_a from the relation $\chi = |\alpha_b - \alpha_a|$. The users can then distill a key bit equal to 0 (1) when $\alpha_a = 0\,(\pi)$. A raw key is formed by concatenating these bits. All the remaining bits, fully disclosed in

the previous step, are used to perform the decoy-state parameter estimation and test the channel against the presence of Eve.

7. *Post-processing* – The users run classical post-processing procedures, such as error correction and privacy amplification, to distil the final secret key from the raw key.

The Secure Key Rate formula for the protocol described above is:

$$R_{TF-QKD} = \frac{1}{M}\{\underline{Q}_1\,[1 - h(\bar{e}_1)] - f_{EC}\,Q_{u_A u_B}\,h(E_{u_A u_B})\}, \tag{2.1}$$

with:

- M the number of slices used for the phase slicing;
- $\underline{Q}_1$ the lower bound of the single-photon gain (retrieved through the *decoy state* technique, mentioned in section 1.3.2);
- $\bar{e}_1$ the upper bound for the single-photon phase-error rate;
- f_{EC} accounts for the inefficiency of error correction ($f_{EC} \geq 1$);
- $Q_{u_A u_B}$ and $E_{u_A u_B}$ are the gain and the QBER associated to the signal pulses observed in the QKD session;
- $h(x)$ is the binary entropy function, given by: $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

The slicing of the $[0, 2\pi)$ phase interval carried out during the *initial operations* is a defining feature of the protocol. This is required to allow both the reconciliation of the phases of the u pulses used to generate the secret key and the phase randomisation of the decoy pulses used to characterise the channel. For these reasons, M should satisfy two contrasting requirements. It should be large enough to allow a precise phase slicing which does not introduce too much error associated to in-slice phase misalignment. At the same time, it should be small enough to allow a sufficient number of detections to meet the matching conditions described in *users's announcement and sifting*, so to grow efficiently the secret key. The phase slicing has two immediate consequences on the SKR formula: it introduces the $\frac{1}{M}$ coefficient, and introduces an intrinsic protocol error e_Δ related to the slicing. The factor $\frac{1}{M}$ in eq. (2.1) quantifies the number of pulses satisfying the phase matching condition.

The contribution to the phase error of the slicing, e_Δ, can be calculated precisely and is equal to:

$$e_\Delta = \frac{M}{2\pi} \int_0^{\frac{2\pi}{M}} \sin^2\left(\frac{\theta}{2}\right) d\theta. \tag{2.2}$$

This error adds up to the other typical sources of error in QKD systems [124], which are related to the optical misalignment of the experimental setup (referred to as e_{mis}), and to the detectors' dark counts (e_{dc}).

2.2 TF-QKD Protocol SKR Scaling and Overcoming of the SKC_0

Technically speaking, the SKR scaling advantage of TF-QKD over other QKD protocols enters eq. (2.1) through the analytical expression of the gains Q_x. Considering a symmetric TF-QKD system (as the one represented in fig. 1.7.a) where Alice and Bob are separated by a distance L and equidistant from the central node, the probability of detecting a pulse with mean photon intensity u prepared and sent by either of the two users at the detection station is:

$$Q_{u_{a,b}} \simeq 1 - e^{\eta(L) u_{a,b}} + P_{dc}, \tag{2.3}$$

in the nominal mode of operation where no Eve is present. In eq. (2.3), P_{dc} is the detectors' dark counts probability, and $\eta(L)$ the overall channel loss defined as:

$$\eta(L) = \eta_{det}\, \eta_{Charlie}\, 10^{-\frac{\alpha L/2}{10}}, \tag{2.4}$$

with η_{det} the quantum efficiency of the detectors, $\eta_{Charlie}$ the loss of Charlie's receiver module, and α the channel average loss coefficient. The factor 2 dividing L in eq. (2.4) in the TF-QKD channel model is responsible for the square root scaling of the SKR. In standard point-to-point QKD implementations the gains Q_x scales $\propto e^{-L}$ rather than $\propto e^{-\frac{L}{2}}$.

Figure 2.1 shows the SKR associated to eq. (2.1). Importantly, in this figure, it is possible to observe that the SKR of realistic implementations of the TF-QKD protocol can overcome the SKC_0 bound.

2.3 TF-QKD Protocol Variants

After the introduction of TF-QKD in 2018 [95], several protocol variants have been proposed to address some of its initial limitations. These variants can be grouped

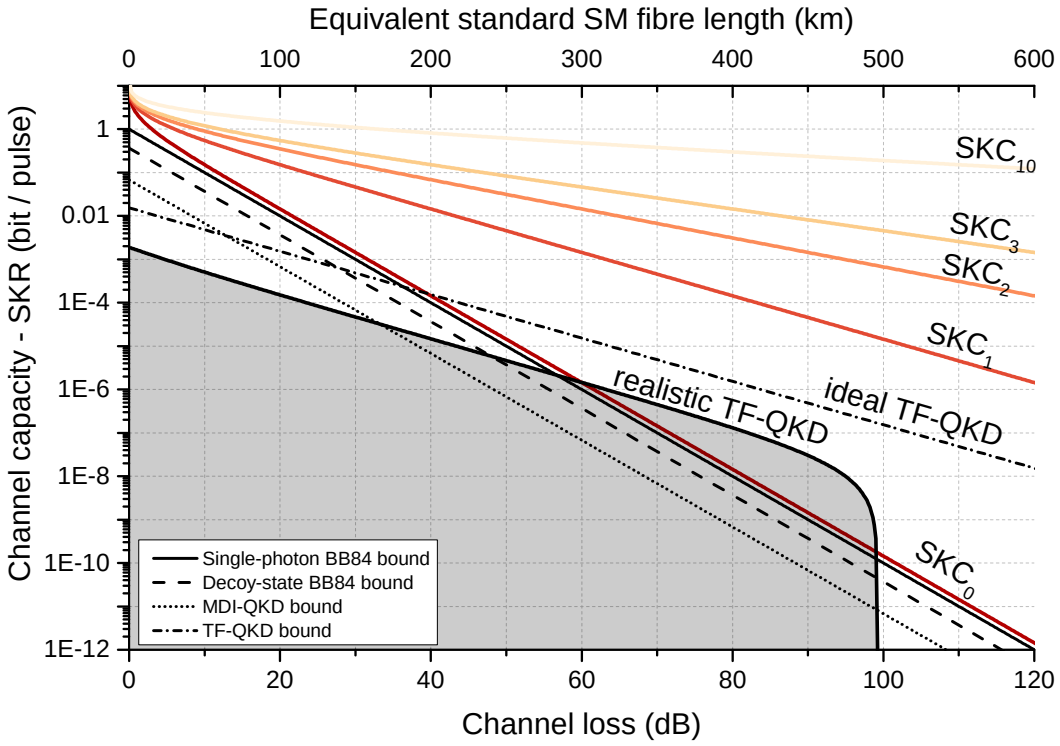

Figure 2.1: TF-QKD SKR (black continuous line) plotted alongside theoretical bounds of other QKD protocols. The "realistic TF-QKD" SKR is plotted using eq. (2.1) and the following parameters: $P_{dc} = 10$ Hz, $\eta_{det} = 30\%$, $e_{mis} = 3\%$, $u = 0.4$ ph/pulse, $v = 0.01$ ph/pulse, $w = 10^{-4}$ ph/pulse, $f_{EC} = 1.15$. From this graph it is apparent that the SKR scaling of TF-QKD is that of a single-node quantum repeater, i.e., $\propto \sqrt{\eta}$. It is also possible to observe that even considering realistic implementation parameters, the protocol is able to overcome the SKC_0 bound.

into three classes, according to the type of improvement that they introduce:

- Improvements to the original security proof of the protocol, presented in the refs. [118, 125] which introduced respectively two protocol variants called "TF-QKD*" and "Phase-Matching (PM) QKD".
- Simplification of the experimental requirements for executing the protocol, by the variant proposed in ref. [120] and called "Simple TF-QKD" or "Curty-Azuma-Lo (CAL) TF-QKD".
- Extension of the communication distance obtainable by the protocol through improvement of the signal to noise ratio of the key bits at high attenuations. This variant was proposed in ref. [121, 126, 127] and is known as "Sending-or-Not-Sending (SNS) TF-QKD".

We will not discuss in detail the properties of the TF-QKD* and PM-QKD protocols because we will not use them in the rest of this thesis. However, it is relevant to mention that the main contribution of these two variants was providing an *unconditional security proof* for TF-QKD, i.e., a security proof valid against any type of attack made to the system. The original protocol was in fact proved secure only against *collective attacks* and not *general* ones.

In sections 2.3.1 and 2.3.2 we will provide simple descriptions of the CAL and SNS TF-QKD protocols, which are relevant for our work because we experimentally implemented them alongside the originally proposed protocol.

2.3.1 Curty-Azuma-Lo (CAL) TF-QKD Protocol Variant

As described at the beginning of this chapter, on the implementation level, one of the signatures of the TF-QKD protocol is the discretisation of the 2π phase interval. This phase slicing was required to allow both the phase reconciliation of the signal pulses and the phase randomisation of the decoy pulses. By taking a different approach for their security proof, the authors of ref. [120], were able to devise a TF-QKD protocol variant characterised by *unconditional security* that also removes the requirement for phase post-selection (and therefore also for the phase slicing of the 2π phase range). A similar approach was also proposed in [117]. The removal of the phase post-selection simplifies the experimental implementation of the protocol, reducing the steps required during the sifting stage. Additionally, CAL TF-QKD offers the highest SKR at low losses among the *unconditionally secure* protocol variants.

A key characteristic of CAL TF-QKD is that it distinguishes between two types of pulses prepared by the users, the *code* pulses and the *testing* pulses. The two classes of pulses are identified by the authors by two different encoding bases. The *code* pulses belongs to the $\mathcal{X}$ basis, while the *testing* pulses belong to the $\mathcal{Z}$ basis. Below we describe the steps to implement CAL TF-QKD. In this description, for consistency with its original proposal, we will use the same basis convention used in ref. [120] and described above.

1. With probability $P(\mathcal{X})$ and $P(\mathcal{Z})$, satisfying $P(\mathcal{X}) + P(\mathcal{Z}) = 1$, Alice and Bob independently and randomly choose a basis from $\{\mathcal{X}, \mathcal{Z}\}$.

2. When $\mathcal{X}$ is selected, the users will also choose a bit $b_{a,b}$ at random. If bit 0 is chosen ($b_{a,b} = 0$), the users prepare the WCP $|\alpha\rangle$. If bit 1 is chosen ($b_{a,b} = 1$), the users prepare the WCP $|-\alpha\rangle$ (which is the state $|\alpha\rangle$, phase shifted by π). All the pulses prepared in $\mathcal{X}$ have the same intensity s.

3. When $\mathcal{Z}$ is chosen, the users prepare a WCP with random and potentially unknown phase. Pulses in $\mathcal{Z}$ can take different intensities $\{u, v, w\}$ randomly selected by the users with probabilities $P(u)$, $P(v)$ and $P(w)$, satisfying $P(u) + P(v) + P(w) = 1$.

4. The prepared pulses are sent by the users through two phase-stabilised channels, after which they meet at Charlie's detection station.

5. Once received by Charlie, the pulses interfere on a 50:50 BS. Charlie measures the interference outcome with two single photon detectors and announces the result over a public channel.

6. Alice and Bob then publicly announce the basis and the intensity used for their encoding. If they both encoded in $\mathcal{X}$, they keep their bits for key generation purposes. If they both encoded in $\mathcal{Z}$, they use the gains measured by Charlie to characterise the quantum channel. They discard other instances.

The variant implementation is simpler than the original protocol described in section 2.1.

When optimised for maximum communication distance, under the constraint of using only three pulse intensities[1] (u, v, w, and $s = v$), and assuming realistic system

[1] For experimental practicality.

imperfections, the maximum channel loss at which this variant can distill a secret key is $\approx 90\,\mathrm{dB}$. This is equivalent to 450 km of standard[1] optical fibre, and 562 km of Ultra-Low-Loss (ULL)[2] fibre.

2.3.2 Sending-or-Not-Sending (SNS) TF-QKD Protocol Variant

The SNS TF-QKD variant, introduced in ref. [121] and then further developed in refs. [126, 127], improves on the original protocol by extending its maximum communication distance and making it more resistant to phase misalignments. Similarly to the CAL variant, SNS introduces two different emission modes for the encoding users: a *code* and a *testing* mode, which are respectively associated to the bases $\mathcal{Z}$ and $\mathcal{X}$ of the protocol. Importantly, and differently from all other variants seen so far, the information in the *code* mode of SNS TF-QKD is encoded on the intensity of the emitted pulses rather than on their phase. Practically speaking, this means that Alice and Bob encode their bits by choosing whether to send or not send (and hence the protocol name) an optical pulse. Similarly to the original TF-QKD protocol, the phase slicing of the 2π phase interval is maintained for the pulses in the *testing* basis.

Below we will provide a description of the protocol and, as for the CAL variant described in section 2.3.1, we will use the same $\mathcal{X}$ and $\mathcal{Z}$ basis convention used by the authors of the protocol.

1. With probability $P(\mathcal{X})$ and $P(\mathcal{Z})$, satisfying $P(\mathcal{X}) + P(\mathcal{Z}) = 1$, Alice and Bob independently and randomly choose a basis from $\{\mathcal{X},\ \mathcal{Z}\}$. When they choose the $\mathcal{Z}$ basis, or *code* basis, they proceed to prepare a phase-randomised WCP of intensity s with probability ϵ, which is associated to a bit encoding of 1 for Alice and 0 for Bob. With probability $1-\epsilon$ they instead prepare a vacuum pulse, which is associated with a bit encoding of 0 for Alice and 1 for Bob. When the users choose the $\mathcal{X}$ basis, or *testing* basis, they prepare a WCP of known global random phase $\rho_{a,b}$, which will fall in one of the M phase slices in which the 2π phase interval has been sliced. Pulses in $\mathcal{X}$ can take different intensities $\{u, v, w\}$ randomly selected by the users with probabilities $P(u)$, $P(v)$ and $P(w)$, satisfying $P(u) + P(v) + P(w) = 1$.

2. The prepared pulses are sent by the users through two phase-stabilised channels,

[1] Standard optical fibre loss coefficient: $\alpha = 0.2\,\mathrm{dB\,km^{-1}}$

[2] Ultra-Low-Loss optical fibre loss coefficient: $\alpha = 0.16\,\mathrm{dB\,km^{-1}}$

after which they meet at Charlie's detection station.

3. Once arrived at Charlie, the pulses interfere on a 50:50 BS. Charlie measures the interference outcome with two single photon detectors and announces the result over a public channel.

4. After the detection outcomes are broadcast, Alice and Bob publicly announce their encoding bases. For cases when both Alice and Bob choose to encode in $\mathcal{Z}$, no further public announcements are required. When they both choose to encode in $\mathcal{X}$, the intensities of the pulses and the phase slices onto which $\rho_{a,b}$ fell into are also publicly announced. Detections occurred when the users choose different encoding basis are discarded.

5. The users will then grow their shared keys by using the bits associated to the instances where Charlie announced a single detection and they both encoded in $\mathcal{Z}$. Single detections occurred when both users encoded in $\mathcal{X}$ and when the WCP had the same intensities and matching phase slices, are used for characterising the security of the channel via the decoy state technique. This is the reason why $\mathcal{Z}$ is called *coding* basis, and $\mathcal{X}$ *testing* basis.

From the description above it emerges that the bit encoding scheme of this variant introduces a systematic error in the key generation process. This is clarified by table 2.1, where on the left are reported the bits associated to the users' encoding, while on the right these are compared side by side, alongside with the probability and yield of the combination. By looking at the right side, it is evident that only for cases II° and III° Alice and Bob add the same bit to their string. In cases I° and IV°, they add different bits, thus introducing the error. The expected systematic error can be calculated using the following definition of error:

$$E_{\mathcal{Z}} = \frac{Wrong\ \mathcal{Z}\ clicks}{Total\ \mathcal{Z}\ clicks}. \tag{2.5}$$

Assuming no detector dark counts, perfect state preparation, $Y_{nn} = 0$, and $Y_{ss} =$

	Users' preparations				Protocol outcome		
	Alice		Bob				
	Sending choice	Recorded bit	Sending choice	Recoded bit	Shared bits	Event probability	Gains
I°	s	1	s	0	10	$\epsilon\,\epsilon$	Y_{ss}
II°	s	1	n	1	11	$\epsilon\,(1-\epsilon)$	Y_{sn}
III°	n	0	s	0	00	$(1-\epsilon)\,\epsilon$	Y_{ns}
IV°	n	0	n	1	01	$(1-\epsilon)\,(1-\epsilon)$	Y_{nn}

Table 2.1: Summary of the possible combinations of pulses when both users encode in the $\mathcal{Z}$ basis. Alice's and Bob's sending or not-sending events are associated to opposite information bits. The "shared bits" column highlights that only for the instances when only one user decides to send a pulse (cases II° and III°), the two users have the same bit in their shared key. Detections associated to cases I° and IV° leads to an error which is intrinsic to this variant encoding strategy.

$2Y_{sn} = 2Y_{ns}$, the intrinsic error on the $\mathcal{Z}$ basis can be calculated as follows:

$$E_{\mathcal{Z}} \simeq \frac{I^\circ + IV^\circ}{I^\circ + II^\circ + III^\circ + IV^\circ} \tag{2.6}$$

$$= \frac{\epsilon^2 Y_{ss} + (1-\epsilon)^2 Y_{nn}}{\epsilon^2 Y_{ss} + \epsilon(1-\epsilon)Y_{sn} + (1-\epsilon)\epsilon Y_{ns} + (1-\epsilon)^2 Y_{nn}} \tag{2.7}$$

$$= \frac{2\epsilon^2 Y_{sn}}{2\epsilon^2 Y_{sn} + 2\epsilon(1-\epsilon)Y_{sn}} \tag{2.8}$$

$$= \epsilon. \tag{2.9}$$

Which means that the systematic error in the $\mathcal{Z}$ basis of this variant is equal to Alice's and Bob's probability of *sending* a pulse ϵ. This error will be corrected during the classical error correction stage of the protocol, and despite its presence, the SNS variant improves considerably the maximum distance achievable by the TF-QKD protocol.

When optimised for maximum communication distance, under the constraint of using only three pulse intensities (u, v, w, and $s = u$), and assuming realistic system imperfections, the maximum channel loss at which this variant can distill a secret key is $\approx 100\,\mathrm{dB}$. This is equivalent to 500 km of standard optical fibre, and 625 km of ULL fibre.

SNS TF-QKD with Two-Way Classical Communication

In the previous section we have seen that SNS TF-QKD is affected by an intrinsic error on the $\mathcal{Z}$ basis, which is independent of the phase misalignment of the channel. In this variant, the phase misalignment of the system contributes only to the single-photon phase error rate evaluated through the decoy state technique on the $\mathcal{X}$ basis.

Due to the specific encoding scheme used in the $\mathcal{Z}$ basis, the performance of the protocol can substantially benefit from a post-processing technique that uses a Two-Way Classical Communication (TWCC) approach [69, 128], as first reported in ref. [126]. TWCC can significantly reduce the intrinsic quantum bit error rate (QBER) floor in the $\mathcal{Z}$ basis, thereby extending the communication distance. The steps to implement TWCC post-processing technique on are described below:

- Let us start by considering Alice's $\{A_1, A_2, \ldots, A_i, \ldots, A_{n-1}, A_n\}$ and Bob's $\{B_1, B_2, \ldots, B_i, \ldots, B_{n-1}, B_n\}$ raw bit strings.
- In a random fashion, Bob pairs up the bits of his raw key of length n (for example A_k and A_j), and performs a bit-wise modulo addition on them (e.g., $B_j \oplus B_k$).
- Bob then announces the positions of the bits he paired (e.g., j and k) and the outcome of the bits addition.
- At this point Alice pairs up her bits copying the pairing already made by Bob, and executes the bit-wise modulo addition on the resulting pairs (e.g., $A_j \oplus A_k$).
- Alice announces publicly the pairs that gave the same addition outcome as Bob.
- Alice and Bob then discard the pairs for which they obtained different results, and they keep only the first bit of the pairs where they obtained the same result. As a consequence, they end up with a shorter string comprised of t elements.

This process reduces the length of the shared key from n to t, while also reducing considerably the differences between the users' strings. The improvement of the signal-to-noise ratio associated with this procedure is so significant that even if the size of the raw key is reduced, it improves both the length of the final key, and

the maximum achievable distance. When optimised for maximum communication distance, under the constraint of using only three pulse intensities (u, v, w, and $s = u$), and assuming realistic system imperfections, TWCC SNS improve the maximum loss for the protocol to $\approx 107\,\mathrm{dB}$. This is equivalent to 535 km of standard optical fibre, and $\simeq 670\,\mathrm{km}$ of ULL fibre.

2.4 Experimental Challenges

In this and the previous chapter we have discussed the details and the advantages associated to TF-QKD compared to other feasible QKD protocols. These advantages come with new challenges related to the practical implementation of the protocol, which add up to the usual difficulties of implementing a QKD protocol (e.g. single photon generation, single photon manipulation, and single photon detection). The challenges are associated to the type of encoding and detection used by TF-QKD, which are absolute phase encoding and single photon interference/detection. For a successful implementation of the protocol, it is necessary to control the phase evolution of twin fields that travel for hundreds of kilometers before interfering at Charlie's 50:50 BS. The relative phase difference between the two paths connecting Alice and Bob to Charlie, that can be seen as a source of error in this protocol, can be expressed as:

$$\delta_{ab} = \frac{2\pi}{s}(\Delta\nu L + \nu\Delta L), \tag{2.10}$$

with s the speed of light in fibre, ν the mean emission frequency of the lasers, $\Delta\nu$ the frequency difference between the two lasers, L the length of the fibre links and ΔL their length fluctuation. This equation highlights that two fundamental ingredients of the protocol are the distribution of a precise frequency reference to the encoding users, to keep $\Delta\nu$ small, and the precise length stabilisation of the transmission channel, to keep ΔL small.

The first task can be achieved by means of phase locking techniques between different laser sources. The second task can be achieved by developing fast phase stabilisation feedbacks capable of correcting the instantaneous phase noise introduced by hundreds of kilometers long channels, which is on the order of tens of radians per millisecond. Developing solutions to these problems has been a central part of the research presented in this thesis. In chapter 3 we will describe the solutions we considered and implemented. In chapters 4 to 6, we will describe the results obtained by applying this techniques to a TF-QKD system.

Part II

Experimental Results

Chapter 3

Experimental Methods

In this chapter we will discuss in detail the main elements and experimental techniques that will be used in the rest of this thesis to achieve our experimental goals. As discussed in section 2.4, the main ingredients required to implement the TF-QKD protocol are:

- the dissemination of an optical frequency reference over long distances;
- the ability to precisely manipulate optical fields;
- the detection of single photons;
- the reconciliation of the phase encoding between optical fields prepared by users that are far-apart from each other.

The second and third elements listed above are standard requisites for the implementation of Discrete Variable QKD (DV-QKD) protocols, and for this reason there are well established techniques to address them. These will be presented in sections 3.1 and 3.2 of this chapter.

The first and last points, on the other hand, are specific requirements of phase-coded quantum communications protocols, for which we have to develop new solutions as there are no standard techniques to address them. Our solutions will be described in sections 3.3 and 3.4.

3.1 Practical Optical Field Manipulation

A fundamental requirement for experimental QKD is the ability to manipulate with precision several degrees of freedom of the optical fields exchanged during

the key generation process. The details of the optical manipulation depend on the specific QKD protocol being implemented, but almost all protocols require control of optical phase, intensity and polarisation. Fortunately, these manipulations are not QKD-specific tasks. They are a common requirement also for classical optical communications, i.e., the information encoding techniques used to exchange information over optical fibres, the backbones of today's digital infrastructure. For this reason, it is nowadays possible to find off-the-shelf modulators that execute most of the encodings/optical manipulations needed in our experiments.

In the following subsections we will give a brief explanation of the principle of operation of the main fibre-based optical modulators that will be used throughout this thesis. In section 3.1.1 and section 3.1.2, respectively, we will describe the functioning of wideband Phase Modulators and Intensity Modulators. In section 3.1.2 we will describe also the Variable Optical Attenuators, which are slower but more precise devices for the manipulation of optical field intensity. In section 3.1.3 we will describe the physical process through which it is possible to modify the polarisation of an optical field. In section 3.1.4 we will introduce Wavelength-Division Multiplexing (WDM), a fundamental technique used in classical communications to increase the throughput of a communication channel that is increasingly becoming relevant also in QKD.

3.1.1 Phase Modulators

Phase modulators are the simplest optical modulators and are devices used to control the phase of the optical fields passing through them. There are various types of phase modulators which are classified according to the physical phenomenon used to control the phase of the target optical field. Possible examples are phase modulators based on the Pockels effect, the manipulation of liquid crystals, or the thermal or mechanical expansion of the transmission medium. In the work presented in this thesis, the most used type of modulator is the one based on the Pockels effect [129], which has been chosen over the alternatives due to the high modulation bandwidth that it can support. In the following we will provide a more detailed description of its operation.

The Pockels effect is a linear electro-optic effect characterising materials that change their optical refractive index proportionally with the intensity of an electric field applied to them. This effect arises only in materials with crystalline structures that lack inversion symmetry. The most commonly used electro-optic materials are

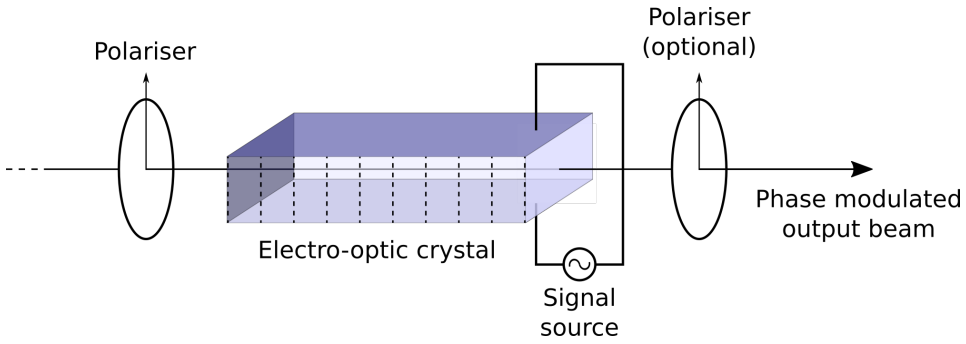

Figure 3.1: Schematic of a transverse electro-optic phase modulator. In the case shown, the input beam is polarised (by a polariser) along the direction of the electric field within the crystal. The modulation signal is applied as a voltage to electrodes at the top and bottom of the electro-optic crystal.

$LiNbO_3$ and KH_2Po_4.

Figure 3.1 outlines the working principle of a simple electro-optic phase modulator. An electro-optic material is sandwiched between two electrodes connected to a voltage generator. The electrodes are positioned so that the electromagnetic field they generate is aligned with one of the crystallographic axes of the material (from now on referred to as the crystal principal axis), the one that will experience the index of refraction change. When the voltage between the electrodes is modified, the component of the material optical index parallel to the principal axis changes proportionally. This induces an optical path variation (and thus a phase variation) on the component of the optical field travelling through the crystal that is parallel to the electric field.

Phase modulators based on the Pockels effect can be used both for slow and fast phase modulation. For slow phase modulations (up to a few GHz), the modulation process is precisely the one described in the previous paragraph, with a slowly varying DC bias applied to the electrodes. The principle of operation for high modulation bandwidth (between 20 kHz and hundreds of GHz) is slightly different, and the travelling wave approach [130] is generally employed there. In this case, the modulators are designed so that the electrical signal used to modify the optical phase travels along the electrodes surrounding the electro-optic material at the same speed of the optical signal to be modulated. When the phase velocities of the driving and modulated waves are matched efficiently, extremely high modulation bandwidth can be achieved, beyond hundred of GHz [131–133]

3.1.2 Intensity Modulators and Variable Optical Attenuators

Intensity Modulators (IM) and Variable Optical Attenuators (VOAs) are devices used to change the intensity of an optical field. While IMs are used for fast intensity manipulations, VOAs are used for slow but precise intensity control.

Similarly to PMs, there are many types of IMs and VOAs which are classified according to the physical phenomenon used to control the intensity of the target optical field. Possible examples are acousto-optic modulators, electro-optic modulators, mechanical modulators, electroabsorption modulators, or liquid crystal modulators. In the work presented in this thesis, the most used type of intensity modulators are the electro-optic modulators based on the Pockels effect (chosen again for the high modulation bandwidth that they can support) and the mechanical modulators, both of which will be described in the following.

IMs based on the Pockels effect work in a very similar fashion to the PM described in the previous section, with the difference between the modulators residing in their waveguides structures. A PM is configured as a transmission line where the phase shift is applied to the whole optical field transmitted through it. The internal structure of an IM is instead that of a Mach-Zehnder Interferometer (MZI) where the phase modulation is applied only to one of the two arms [134–136]. By tuning the phase in one arm of the MZI, it is possible to control the interference at the combining Y-junction of the IM, and thus the intensity of the optical field exiting the modulator. Similarly to PMs, also with IMs it is possible to use the travelling wave approach to achieve high modulation bandwidths, which can reach hundreds of GHz [137].

Mechanical VOAs[1] are devices that change the intensity of the transmitted light by physically blocking part of the signal passing through them. Figure 3.2 shows a possible example the principle of operation of a single mode VOA. The optical signal at the input, initially carried by an optical fibre, is collimated into a larger beam by a collimating lens. A movable blocking device is interposed between the collimating and the focusing lens to block the desired amount of signal. The unblocked part of the signal is then coupled into an optical fibre by a focusing lens. The position of the blocking device is controlled by an accurate stepper motor that allows a precise and high resolution intensity control.

[1] There is also another common class of VOAs based on micro-electro-mechanical systems. These are not described here as they are not used in the experiments presented in this thesis.

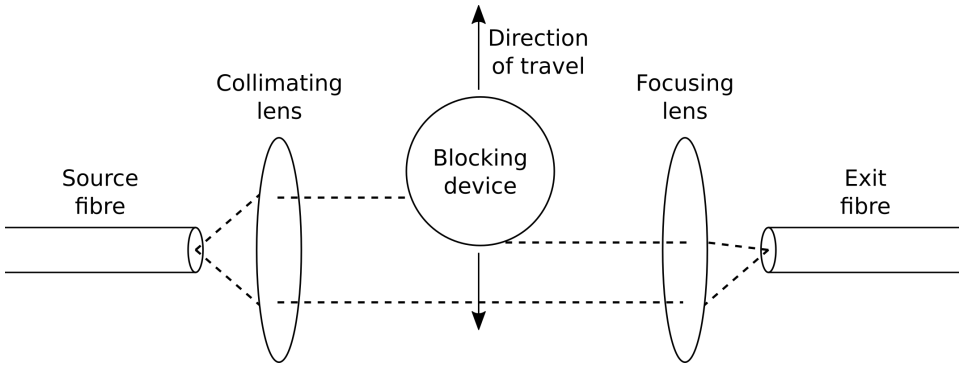

Figure 3.2: Schematic of a blocking-type VOA. Light from the source fibre is collimated into a beam along which is inserted a blocking device. The signal attenuation will depend on the position of the blocking device, which is controlled by a precision stepper motor.

3.1.3 Polarisation Controllers

Most of the applications involving optical signals for data transfer are based on protocols that use only optical phase and intensity modulation for the information encoding. But there are applications, such as integrated optics devices or interferometry-based techniques, where also the polarisation of the optical fields is a relevant property that needs to be controlled. Polarisation controllers are devices used to manipulate the polarisation of optical signals transmitted through single mode optical fibres. There are two main types of controllers: mechanical modulators, which are simple but slow (up to $\sim$100 Hz modulation bandwidth), and electro-optic modulators, which are more complex but much faster (up to $\sim$100 krad s^{-1} optical phase modulation speed [138]).

Since the polarisation rotations that we have to compensate in our experiments are relatively slow, in the experiments described in this thesis we used only the mechanical type of controllers. Their principle of operation is based on the polarisation power transfer between the two fundamental modes of the single optical fibres induced by asymmetries in the fibres. Mechanical controllers exploit this effect by gently twisting and squeezing the optical fibre carrying the signals [139]. Well designed modulators can reach any point in the Poincaré sphere by controlling the strain applied to the fibre. Three fibre squeezers are usually sufficient to reach full polarisation control, as they effectively play the role of one $^1/_2$ wave plate and two $^1/_4$ wave plates.

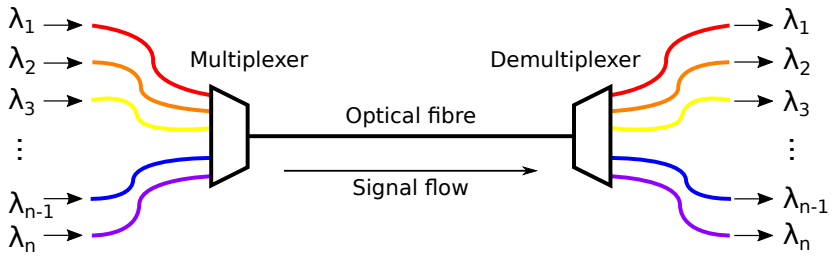

Figure 3.3: Schematic of a Wavelength Division Multiplexing communication system. λ_1, λ_2, ... , λ_n: different optical wavelengths use to encode different signals. Trapezoids: optical multiplexer and demultiplexer.

3.1.4 Wavelength Division Multiplexing

Wavelength-Division Multiplexing (WDM) [140] is a type of *frequency division multiplexing* technique consisting in the transmission of multiple signals over the same channel (generally optical fibres). This is done with the objective of increasing the channel capacity, i.e. the maximum amount of information that can be transferred over a single optical fibre, and it is a technique routinely employed in classical optical telecommunications.

In WDM, different signals are encoded at different optical wavelengths, generally by using different lasers. The signals are then combined together (a process also called *multiplexing*) through optical couplers or optical multiplexers, and sent through the same optical channel. The key feature of this system is that the signals at different wavelengths do not interfere with each other in the optical fibre[1]. At the receiver end, the different signals are separated through a process called demultiplexing.

When the number of considered wavelengths is small, the (de-)multiplexing process is done with optical spectral filters (such as thin-film interference filters or fibre Bragg gratings) that selectively transmit or reflect the different signals. When the number of considered wavelengths is large, Arrayed Waveguide Gratings are used instead. Figure 3.3 shows the scheme of a simple system employing WDM.

There are two main standards for WDM recognised by the International Telecommunication Union (ITU):

- "Coarse wavelength division multiplexing" [141], which uses a relatively small number of channels (four or eight) and a large channel spacing of 20 nm.

[1]This holds true provided that the overall intensity of the signals along the fibre is low enough to avoid nonlinear effects that would introduce detrimental crosstalk between the signals.

- "Dense wavelength division multiplexing" [141], which uses a larger number of channels (up to 160) and channel spacing equal or smaller than 100 GHz (with 100, 50, 25, 12.5 GHz as possible options). Systems with 25 and 12.5 GHz spacing can also be referred to as "Ultradense WDM".

3.2 Single Photon Detectors

Once information has been encoded in single photons, and these have travelled along the channels connecting the communicating users, it is necessary to perform single photon measurements in DV-QKD protocols. In the last thirty years single photon detectors have been continuously improved to suit the specific requirements of QKD [142, 143]. The relevant properties for a single photon detector employed in QKD are:

Efficiency - the fraction of photons registered by the detector from a given photon input;

Dark count rate - the rate of false events registered by the detector given no light input;

Recovery time - the time a detector needs to become operative after detecting one photon. This figure is directly related to the detector maximum count rate;

Afterpulsing - the probability a detected photon generates a following spontaneous, and therefore erroneous, detection.

Two types of detectors have good performances in all the figure of merits listed above: Single Photon Avalanche Diode (SPAD) and Superconducting Nanowire Single Photon Detector (SNSPD).

The basic element of SPAD is a p-n junction operated with a large reverse bias. Incident light creates electron-hole pairs in the p-n junction, and the high bias causes the charge carriers to accelerate towards the electrodes. The high acceleration gives the carriers enough energy to ionize other carriers. The number of ionized carriers increases exponentially, and by the time the carriers reach the electrodes, the generated carrier current is enough to be detected by the diode circuit [129].

A SNSPD consists of a nanowire maintained well below its superconducting critical temperature and DC biased just below its critical temperature. When a photon interacts with the nanowire by breaking Cooper pairs, it reduces the local

critical current below that of the bias current. This results in the formation of a localized non-superconducting region, or hotspot, with finite electrical resistance. This resistance is typically larger than the input impedance of the readout amplifier, and hence most of the bias current is shunted to the amplifier. This produces a measurable voltage output that is detected by the electronics [144, 145].

Devices based on superconducting nanowires show low dark count rates and high efficiencies. The main downside to these detectors is that they function at cryogenic temperatures. This requirement means they are expensive and bulky to operate.

3.3 Optical Frequency Regeneration

As discussed in detail in chapter 2, in TF-QKD the transmitting users encode their information on the absolute phase of an optical field and the correlation between the users' prepared states is retrieved through a first order optical interference. For a successful protocol execution it is therefore essential that the users execute their encodings on optical fields having the same frequency. From an experimental standpoint, this is a challenging requirement.

All laser sources are characterised by a certain amount of wandering of their emission frequency, which generates a short-term finite spectral linewidth and a long-term frequency drift [146]. These instabilities are related to many factors, such as atomic transition widths, temperature variations, mechanical vibrations and imperfections, laser driver current fluctuations, etc., and it is technically very demanding to control all of them simultaneously. For this reason, having two independent laser sources emitting at exactly the same wavelength to run the protocol is impractical.

A more practical solution to this problem is the dissemination of a common frequency reference to the transmitting users. This approach, however, introduces another issue, this time related to the protocol implementation security. Since the optical frequency used for the encoding is now distributed to the users as an external reference, there could be a problem of trust with this signal: since it comes from outside the users' secure perimeter we cannot necessarily guarantee its trustworthiness.

Given the current assumptions of the TF-QKD protocol and its variants, on a practical level this means that we cannot simply use the distributed frequency reference for the protocol encoding. We will have to decouple the signal used for the encoding from the one received as reference, while maintaining the optical frequency

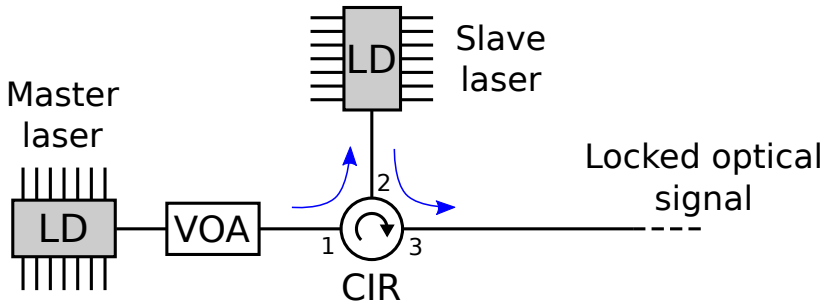

Figure 3.4: Representation of an Optical Injection Locking setup. The optical output of a laser diode (LD) which acts a master laxer is attenuated by an attenuator (VOA) and then injected by an optical circulator (CIR) into a second laser diode acting as a slave laser.

information carried by the latter. In other words, we will have to operate a frequency regeneration.

In this section we will describe the two strategies used in the rest of this thesis for executing the frequency regeneration. In section 3.3.1 we will describe the Optical Injection Locking (OIL) technique, while in section 3.3.2 we will describe the Optical Phase-Locked Loop (OPLL) technique.

3.3.1 Optical Injection Locking

Optical Injection Locking (OIL) is a is a well-established technique in optics [147–149] that allows to lock the emission frequency of a laser (commonly referred to as the "slave laser") to that of another laser (called the "master"). Optical Injection Locking (OIL) is the optical counterpart of the broader injection locking phenomenon, which indicates those situations where two oscillators with similar frequencies adopt the same frequency and phase. A notable example of injection locking in classical mechanics is the spontaneous synchronisation of pendulums, as observed by Huygens already in the 17^{th} century [150].

In OIL the oscillators are the laser cavities, and its typical experimental configuration is the one shown in fig. 3.4. Here, the light from the master laser is injected into the cavity of an isolator free slave laser. If the frequency detuning ($\Delta\nu$) between the two free-running lasers is small enough, and sufficient power is injected into the slave laser, then the slave laser will lase at the same wavelength of the master laser.

In laser physics, OIL is commonly used to amplify the optical signal of low phase and intensity noise lasers. This is done by injecting the output of the stable laser

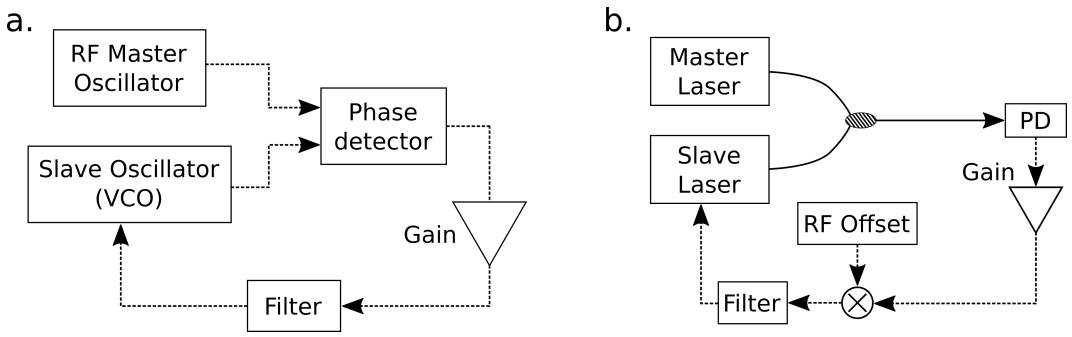

Figure 3.5: **a.** Schematic diagram of a generic Phase-Locked Loop (PLL). VCO: Voltage Controlled Oscillator. **b.** Schematic diagram of a generic heterodyne Optical Phase-Locked Loop (OPLL). PD: photodetector.

into a high power laser. High power lasers are generally characterised by higher noise figures, but when these are injected by a more stable signal, and once the injection parameters are optimised properly, OIL allows the slave laser to inherit most of the optical properties of the master laser. This effectively allows the regeneration of an input optical reference signal, which is exactly what we need for our experiments.

Over the recent years, application of the OIL technique to QKD has been extensively studied, especially in relation to improvements that it can bring to the performance and design of QKD transmitters [151–155].

3.3.2 Optical Phase-Locked Loop

Another instance of the injection locking mechanisms mentioned at the beginning of section 3.3.1 are the Phase-Locked Loops (PLL). PLLs are electronic negative-feedback control systems that control and modify the phase and frequency of a "slave" oscillator so that it closely follows the one of a reference "master" oscillator [156–158]. PLLs are fundamental components in modern electronic circuits, where they are used for clock delivery and recovery, frequency division/multiplication, noise reduction and much more. Figure 3.5.a shows the diagram of a simple and generic Phase-Locked Loop (PLL) system which includes two fundamental components: a variable frequency oscillator (generally voltage-controlled) and a phase detector connected to a feedback loop. The phase detector (generally an electronic mixer) is used to compare the phase of the master oscillator with that of the slave oscillator and provides the error signal to be fed to the voltage-controlled slave oscillator to keep it in tune with the reference.

Optical Phase-Locked Loops (OPLL) are the optical counterpart of PLLs, where the signals to be synchronised are optical ones [159–161]. Normally, in OPLL implementations, the master oscillator is a high quality laser, the slave oscillator a semiconductor laser (i.e. a current controlled oscillator) and the phase detector is a photodetector monitoring the interference of the two optical lasers. The fundamental working principle of OPLL circuits is based on obtaining some information on the phase and frequency of an optical field, which spontaneously oscillates at a frequency of hundreds of THz, too fast to be tracked by any electronic device, by mixing (interfering) it with a second optical field close in frequency. If the two optical fields, for example $E_m(t) = a_m cos\left(\omega_m t + \phi_m(t)\right)$ and $E_s(t) = a_s cos\left(\omega_s t + \phi_s(t)\right)$, are close enough in wavelength, their interference beatings become detectable by electronic devices such as photodiodes. The photocurrent of a diode recording the interference will in fact be:

$$i_{PD}(t) \propto a_m^2 + a_s^2 + 2a_m a_s cos\left[(\omega_m - \omega_s)t + (\phi_m(t) - \phi_s(t))\right]. \tag{3.1}$$

From eq. (3.1) it is apparent that the photocurrent includes a term proportional to the frequency and phase detuning between $E_m(t)$ and $E_s(t)$. This signal, once appropriately filtered, can be used to control the current of the slave laser in order to change its emission frequency and lock it to the master laser.

Figure 3.5.b shows the schematics of a typical Optical Phase-Locked Loop (OPLL) configuration. It is worth noting that in the lower part of the diagram it is shown the possibility of adding an Radio Frequency (RF) offset to the photocurrent signal recorded by the photodiode. When no RF offset is added, the OPLL is said to be in homodyne configuration. In this case the OPLL circuit will lock the master and slave lasers at exactly the same emission frequency. When an RF signal is introduced in the circuit, generally through a Local Oscillator (LO), the OPLL will force the two lasers to emit with a fixed frequency offset. The advantage of using heterodyne locking over its homodyne counterpart is mostly related to noise rejections. In an heterodyne configuration, the interference signal is at an intermediate frequency dictated by the Local Oscillator (LO), where it can be easily filtered from low frequency noise terms such as Direct Current (DC) drifts.

The main figures of merit characterising the performance of an OPLL system are:

Loop bandwidth - the largest frequency that the feedback loop can process and amplify to lock the lasers;

Hold-in range - the largest frequency offset that the slave can have with respect to the master laser without breaking the locking;

Residual phase error - the variance in the deviation of the phase of the locked laser from the ideal case where it perfectly follows the master laser.

3.4 Quantum Channel Stabilisation

As discussed in chapter 2, another fundamental requirement for TF-QKD is controlling the phase noise affecting the signals encoded by the transmitting users (Alice and Bob). This is necessary to interpret correctly the outcome of the interference between their encoded pulses. As mentioned in section 2.4, the stabilisation of the phase of the transmission channels is a difficult task, especially when the channels are hundreds of kilometers long and the introduced phase noise is on the order of tens of radians per millisecond.

In order to accomplish this, in this work, we adopt an active stabilisation approach where the phase misalignment between the users is constantly monitored and corrected to keep it locked to a predetermined value. We achieve this by implementing suitable closed-loop control systems, which are a key element of our experiments.

Given the fundamental role played by control loops in our setups, in section 3.4.1, we provide a general introduction to these systems. This will be a useful reference for sections 3.4.2 and 3.4.3, where we will describe in detail the two phase stabilisation systems employed in the experiments described in this thesis.

3.4.1 Closed-Loop Control Systems

Automatic controls are an essential tool of modern engineering and science, and are ubiquitously present in most of today's technology [162, 163]. The aim of automatic controls is maintaining a prescribed relationship between the input and the output of a given system.

One of the most common type of control systems are *feedback control systems*. These are automatic controls designed to operate a system in the presence of external, unpredictable disturbances. Their operation is generally based on the comparison between the current state of a system with its desired state, often called the *setpoint*. The difference (or distance) between the two states is the *error signal* which is used

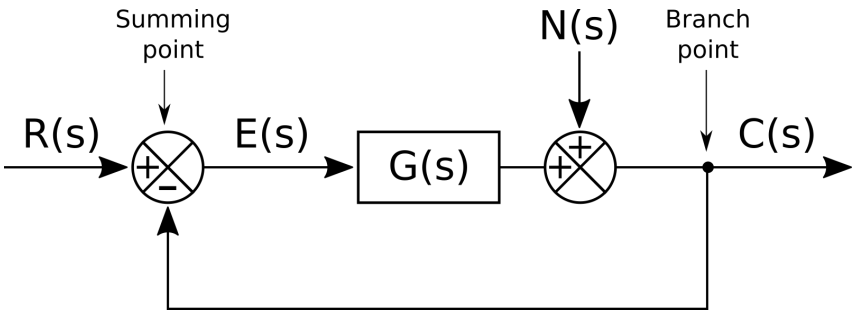

Figure 3.6: Diagram of a closed feedback loop. $R(s)$: reference input or *setpoint*, $E(s)$: error signal, $G(s)$: transfer function of the filter and actuator acting on the system to modify its state, $N(s)$: uncontrolled noise, $C(s)$: current state of the system.

by the *feedback controller* to generates a *correction signal* that is fed back to the system. The purpose of the correction signal is reducing the error signal as much as possible.

Due to the interdependence between the current status of a system and its associated error signal, feedback controlled systems are often referred to as *closed-loop control systems*. The motivation of this name becomes apparent by looking at fig. 3.6, where a simplified block diagram representation of a feedback controlled system is given. At the left of the diagram is the setpoint, which is given as reference input $R(s)$ to the feedback system. This is mixed (through a subtraction) to the current state of the system $C(s)$, from which the error signal $E(s)$ is calculated. The error signal then passes through a controller, described by its transfer function $G(s)$ [162]. The controller consists of two elements: a filter and an actuator. The filter calculates the correction signal that will be fed to the actuator. The actuator imparts the correction signal to the system, modifying its state. In the scheme, a second summing point represents the introduction of uncontrolled disturbances $N(s)$ affecting the final status of the system. The final system status is fed back as "new" current state to the initial summing block of the system so that the correction cycle can restart.

A very important aspect characterising feedback loops is the implementation of the controller ($G(s)$), which is responsible of generating the correction signal from the error signal. The most commonly employed type of controllers in feedback loops are Proportional-Integral-Derivative (PID) controllers, an example of which is shown in fig. 3.7. In this type of controllers, the error signal is used by three sub-controllers to calculate three different correction factors which are:

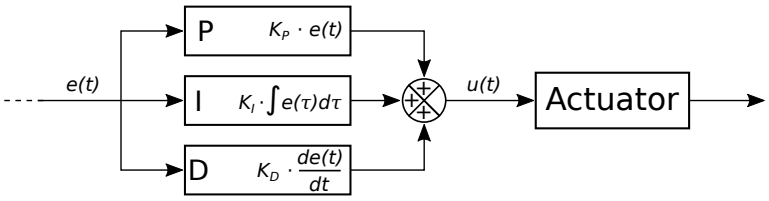

Figure 3.7: Diagram of a Proportional-Integral-Derivative (PID) controller.

- directly **proportional** to $e(t)$, by a factor K_P;
- proportional, by a factor K_I, to the **integral** over time of $e(t)$;
- proportional, by a factor K_D, to the **derivative** over time of $e(t)$.

These three factors are then summed together to generate the final correction signal $u(t)$ that will be fed to the actuator, as shown in fig. 3.7. The name PID is the acronym of the initials of the three sub-controllers stages.

3.4.2 Phase Stabilisation Through Time Multiplexing

In this section we will describe the first type of phase stabilisation strategies we develop for our experiments, which is based on the time multiplexing of some phase-unmodulated reference pulses alongside the protocol encoded pulses.

Phase Encoding

The qubit encoding, when using optical fields as information carriers such as in TF-QKD, is operated on the relative phase of the optical pulses prepared by Alice and Bob with respect to a common optical phase reference. In this scenario, the Bell state measurement carried out by Charlie resolves into a constructive/destructive interference of the optical fields prepared by the two users.

By modulating the relative phase offset of their optical fields, the users can generate an interference at Charlie's station whose outcome can be mapped into the outcome of a standard four-state BB84 measurement. It is sufficient for Alice and Bob to encode four phase offsets to their pulses in order to each have a full BB84 encoding. This approach is similar to the standard QKD phase encoding [29]. A simple schematic of a first-order optical interference is reported in fig. 3.8. The figure shows the intensity output of a 50:50 BS when two identical optical fields interfere

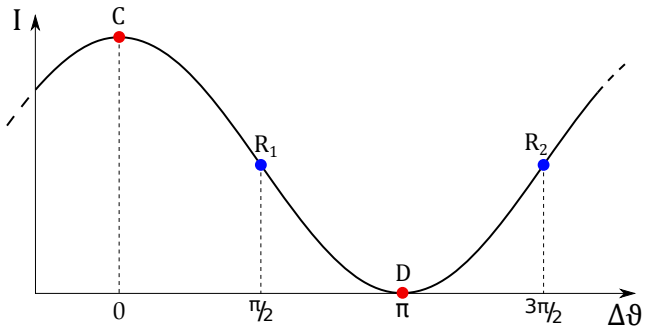

Figure 3.8: Optical intensity at one output of a 50:50 BS plotted as a function of the phase offset between the two identical optical fields that interfere with each other. Point **C** and **D** represent the positions of constructive and destructive interference respectively. Point $\mathbf{R}_1$ and $\mathbf{R}_2$ represent the interference at quadrature condition, when an equal amount of light exit the two output ports of the BS.

on it. The intensity is plotted as a function of the phase offset $\Delta\vartheta$ between the incoming fields. The function describing the normalised curve is:

$$I(\Delta\vartheta) = \frac{1}{2}(1 + \cos(\Delta\vartheta)). \tag{3.2}$$

Constructive interference between the incoming fields occurs when the phase difference between them satisfies the relation: $\Delta\vartheta = 0 + 2n\pi$, $n \in \mathbb{Z}$ (position **C** in fig. 3.8). Destructive interference occurs when $\Delta\vartheta = \pi + 2n\pi$, $n \in \mathbb{Z}$ (position **D** in fig. 3.8). While, when $\Delta\vartheta = \frac{\pi}{2} + n\pi$, $n \in \mathbb{Z}$, equal amount of light comes out of the two output ports of the 50:50 BS (positions $\mathbf{R_1}$ and $\mathbf{R_2}$ in fig. 3.8).

When at the input of the BS are optical fields that interfere to produce one single photon, the interference process can be interpreted as follows: when constructive or destructive interference take place, the generated photon will exit a well defined port of the beam splitter. When instead the phase offset is $\frac{\pi}{2} + n\pi$, $n \in \mathbb{Z}$, the photon will exit with equal probability from either of the BS output ports.

This can be mapped into the standard BB84 phase encoding as follows. By applying a phase offset of 0 or π, the users encode a bit 1 or 0 in the $\mathcal{X}$ basis respectively. When applying a phase offset of $\pi/2$ or $3\pi/2$, the users encode a bit 1 or 0 in the $\mathcal{Y}$ basis respectively. Only when Alice and Bob encode their bits in the same basis the interference outcome gives useful information for the key distillation (positions **C** and **D** in fig. 3.8 can be achieved). When the users encode their bits in different bases, the interference outcome is random, and thus it is useless for generating a secret key (only positions $\mathbf{R_1}$ and $\mathbf{R_2}$ in fig. 3.8 can be achieved).

Alice enc.	Bob phase encoding: 0	$\pi/2$	π	$3\pi/2$
0	**C**	R	**D**	R
$\pi/2$	R	**C**	R	**D**
π	**D**	R	**C**	R
$3\pi/2$	R	**D**	R	**C**

Table 3.1: Possible interference combination between the states prepared by Alice and Bob. **C**: constructive interference. **D**: destructive interference. **R**: random outcome, interference at the quadrature situation. Only the outcomes **C** and **D** are useful for the key generation.

Table 3.1 shows the outcomes of all possible combinations between the optical fields prepared by Alice and Bob. In this table, the combinations useful for building a secret key are typed with a character in bold.

Encoded Pattern

In the time-multiplexed stabilisation technique, some phase unmodulated reference pulses are interleaved to the qubit pulses for phase stabilization purposes. The phase feedback system is designed to lock the two arms of the TF-QKD system to a $\pi/2$ phase offset (more details on the phase feedback algorithm and on the motivations for choosing this locking point can be found in the next subsection). This constant phase offset affects the interference outcome of the encoded pulses by shifting cyclically (of one position to the right or left, depending which arm is shifted with respect to the other) the results reported in table 3.1. This phase shift has to be taken into account to interpret correctly the interference outcomes.

For the sake of simplicity, in this and the following sections, we will discuss in detail our first approach to the phase stabilisation used in the proof-of-principle TF-QKD experiment reported in chapter 4. In our initial approach, a periodically repeated 8-bit pattern was encoded by the transmitting users. The short repeated pattern was substituted in later experiments by longer pseudo-random patterns, but the principles of operation remained unchanged. The short pattern used to test the time multiplexed phase stabilisation is represented schematically in fig. 3.9. The two top graphs in figure represent the phase pattern of the two encoding users. Alice and Bob encode the respective phase patterns into the optical pulses through their

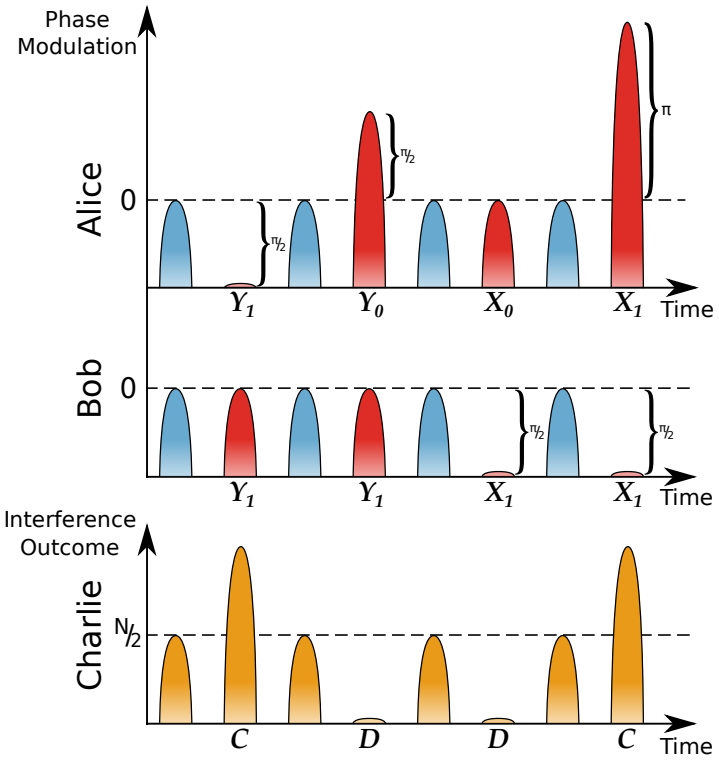

Figure 3.9: **Top two graphs:** schematic of Alice's and Bob's phase encoding schemes. The blue pulses represent the unmodulated interleaved pulses used by the feedback system for phase stabilization. The red pulses represent the quantum pulses, the ones used for qubit encoding. The feedback system keeps the reference (unmodulated) pulses locked to a $\pi/2$ phase difference. This introduces a $\pi/2$ phase shift for the encoding in the two bases between Alice and Bob. **Bottom graph:** outcome of the optical fields interference at one output of Charlie's station, when the system is stabilised at $\pi/2$ phase offset. N is the number of photons collected over time within the time windows where constructive interference is occurring. Each pulse in the bottom row is obtained by interfering Alice's and Bob's pulses represented above it. Depending on the encoded phases, the quantum pulses interfere to give constructive (C) or destructive (D) interference.

PMs.

The red pulses are the ones used for bit encoding. From the figure it is possible to see that in her pattern, Alice encodes all the four BB84 states, while Bob encodes only two of them in his. This was done in order to simplify the setup preparation, and it does not affect TF-QKD protocol realization. Both constructive and destructive optical field interference in both bases are still obtained.

The blue pulses in the two top graphs represent the reference pulses. These are interleaved with the quantum signals and, as visible from the figure, and they are not modulated.

The bottom graph in fig. 3.9 represents the interference outcome integrated over time of the patterns shown in the two rows above. N is the number of photons collected over time within the time windows where constructive interference is occurring. Since the feedback system keeps the two communication channels to a fixed $\pi/2$ phase offset, the unmodulated pulses interfere to give a $N/2$ outcome. When destructive interference occurs, the number of detected photons is approximately zero.

Feedback System

The feedback system is designed to lock the phase difference between the two quantum channels to $\pi/2$. This is the most efficient solution as it exploits the linear part of the interference response function. Information about the instantaneous interference condition is retrieved from the same SNSPD used for key distillation. Detection signals are collected by an electronic counter with a fixed averaging time and then processed by the feedback algorithm.

Given the encoding scheme used in the experiment (described in the previous section), the dependence of the number of photons recorded by the detector on the phase difference between the two quantum channels is described by the function:

$$N_{out}(N_{floor}, \Delta\theta) = N_{floor} + \left(\frac{3N_{floor} - N_{floor}}{2}\right)(1 + \cos\Delta\theta). \tag{3.3}$$

A graphical representation of the function is shown in the fig. 3.10. As shown in figure, the detected number of photons follow a typical $\frac{1+\cos\Delta\theta}{2}$ interference pattern, offset by a constant number of counts N_{floor}. This happens because, independently of the phase difference between the two arms, the phase encoded pulses (or quantum pulses) always interfere to give a constant amount of counts. The interference of the unmodulated reference pulses, on the other hand, follows a typical sinusoidal behaviour. The overall interference is given by the sum of these two contributions.

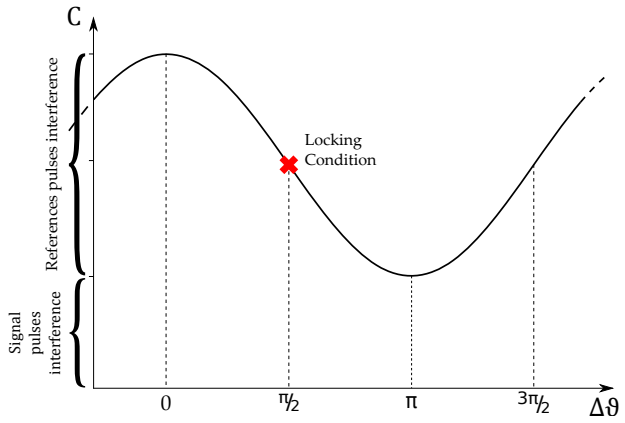

Figure 3.10: Schematic of the number of counts recorded by the detector used for phase stabilization as function of the phase offset between the two quantum channels. A red cross marks the $\pi/2$ phase locking condition.

By looking at the overall interference outcome it is then possible to understand when the phase difference between the two quantum channels is $\pi/2$. The phase stabilization is executed through a PID feedback system that keeps the detected number of counts locked to the value associated to the $\pi/2$ phase offset condition. The phase offset is corrected by varying the DC bias of Alice's PM.

Feedback Characterisation

Figure 3.11 shows a characterisation of the stabilisation feedback performance. In this measurement, for the sake of simplicity, no phase encoding is applied by Alice and Bob to their pulses. The phase of the users' photons is locked through OIL with the master laser. This stabilization system is capable of locking the two quantum channels to a $\pi/2$ phase difference with a precision of 1.6×10^{-2} rad, equivalent to 0.92°. This satisfies the requirement of having a phase stabilization uncertainty that is considerably smaller than the $2\pi/16$ phase slice used in TF-QKD for phase reconciliation (for a description of the protocol refer to section 2.1).

3.4.3 Phase Stabilisation Through Wavelength Multiplexing

In this section we will describe the second type of phase stabilisation strategy we develop for our experiments, which is based on the wavelength multiplexing of some phase-unmodulated reference pulses alongside the protocol encoded pulses. This strategy, which requires a 2-stage stabilisation system, is also called the *dual-band*

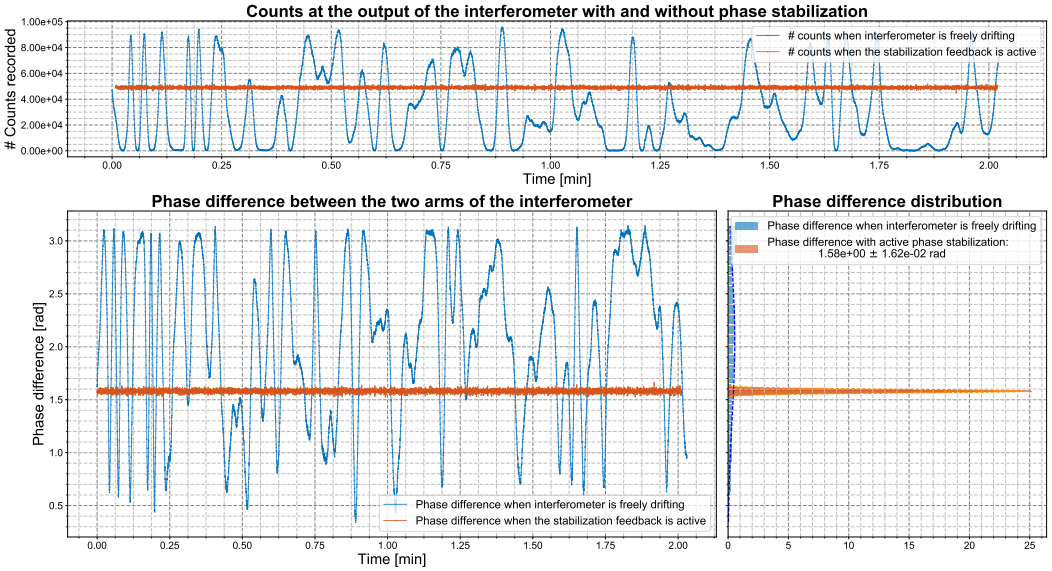

Figure 3.11: **Top:** number of counts recorded by one of the detectors associated to the interference of single photon pulses sent by the users. In blue are the data recorded when the phase difference between the two arms is drifting freely, in orange are the data when the PID loop is activated. **Bottom-left:** graph showing the differential phase difference between the two arms of the setup. These data are extracted by the top graph inverting the relation eq. (3.2). **Bottom-right:** histogram of the data shown in the bottom left graph. The stabilized signal phase standard deviation is 1.6×10^{-2} rad.

	Acronym	Wavelength	Intensity	Type of signal	Modulation	Function
Bright Reference	BR	λ_2	High	CW	None	Stage-1 phase compensation
Dim Reference	DR	λ_1	Low	Pulsed	None	Stage-2 phase compensation
Dim Quantum	DQ	λ_1	Low	Pulsed	Intensity and phase	Key generation

Table 3.2: Summary of the names, acronyms, properties and functions of the signals used in the dual-band phase stabilisation strategy.

stabilisation approach.

In the dual-band approach, each user prepares two optical signals at two different but close wavelengths (λ_1, λ_2), and sends them over the same communication channel. The interference outcome of the Continuous Wave (CW) signal at λ_2, also called the Bright Reference signal (BR), is used to detect the phase drift introduced by the long fibre channel. This stabilisation is executed by a fast feedback loop constituting the stage-1 of the 2-stage stabilisation system. The other wavelength, λ_1, is used for the protocol encoding. This wavelength carries two type of pulses: some phase unmodulated pulses, called Dim Reference pulses (DR), and some phase and intensity modulated pulses used for the protocol encoding, called Dim Quantum pulses (DQ). Table 3.2 provides a summary of the different signals used in the dual-band stabilisation technique introduced in this section.

Since the signals for the channel stabilisation and for the protocol encoding are located at two different wavelengths, and thanks to the very high filtering contrast achievable with WDM, there is almost no limit on the intensity contrast that one can generate between reference and signal pulses. The brightness of the BR signals can be set to whatever level is needed to stabilise the phase of the communication channel. Given the proximity in wavelength of λ_1 and λ_2, once the communication channel is stabilised for λ_2, it will be approximately stabilised also for λ_1. Assuming unidirectional phase drift, the stage-1 stabilisation (acting on λ_2) will reduce the phase drift over λ_1 by a factor of $\lambda_1/(\lambda_1 - \lambda_2)$, corresponding to approximately 3 orders of magnitude, when the two wavelengths are a few ITU channels [164] far apart.

The remaining slow phase drift over the λ_1 wavelength can be stabilised by a second slow feedback system that uses the interference outcome of the DR pulses to assess the residual phase offset between the DQ ones. The remaining (slow) phase drift on λ_1 is related to two factors: the fact that λ_1 and λ_2 travel separately in certain sections of the setup (necessary for the protocol encoding over λ_1 at the transmitting stations), and the fact that the fast feedback introduces a phase drift

over λ_1 when the length difference between the two channels varies over time. The former component of the slow phase drift can be seen as the phase noise picked up by an asymmetric Mach-Zehnder interferometer having the dimensions of those sections of the setup where the two wavelengths travel separately. The latter component can be explained as a consequence of the finite modulations range of the PM, and of the phase locking of the fast feedback over λ_2, rather than λ_1.

The PM operating in the stage-1 feedback actively compensates the fast phase drift. However, its finite adjustment range is incapable of compensating at entirety the phase drift caused by fibre length variation. It must rely on multiple (M) resets in order to maintain the λ_2 phase difference to $\phi = 2\pi M + \phi_t$, where ϕ_t is the target phase. Due to $\lambda_2 - \lambda_1$ wavelength difference, this compensation will introduce a residual phase drift ($\Delta\phi$) over λ_1 equal to:

$$\Delta\phi = 2\pi M \left(\frac{\lambda_2 - \lambda_1}{\lambda_1} \right). \tag{3.4}$$

The residual drift introduced by the λ_2-stabilisation over λ_1 is estimated to be $\frac{\phi}{\Delta\phi} = \frac{\lambda_1}{\lambda_2 - \lambda_1} \approx 1000$ times smaller than the original fibre phase drift, assuming unidirectional fibre length drift. In reality, the fibre length drift direction is random. With cancellation of positive and negative 2π resets, we obtain experimentally a higher reduction factor of ~ 6800 (as will be discussed in details in the "2-Stage Feedback System Characterisation" section).

Figure 3.13.b shows the stabilisation mechanism that correct the residual phase drift on λ_1. This stabilisation feedback is the same as what we developed for the proof-of-principle experiment discussed in section 3.4.2. The error signal for it is provided by the overall interference of quantum signals and dim reference. The quantum signals are interleaved with the dim reference pulses, which are unmodulated and have the same intensity as the brightest decoy pulse (u). The presence of dim reference pulses guarantees that the averaged output of the interference is directly related to the residual phase offset in λ_1. This is retrieved by integrating the single photons detected by SNSPD D_1 over 50 ms or 100 ms, depending on the distance. The difference between this value and a set value provides the error signal for a PID controller implemented with a micro-controller operating at the frequency of 20 Hz or 10 Hz, depending on the distance. The micro-controller corrects the phase offset by modulating a fibre stretcher acting on the quantum signal coming from Alice. Differently from the stabilisation in λ_2, the one in λ_1 acts solely on the quantum signals and can therefore correct its residual phase drift.

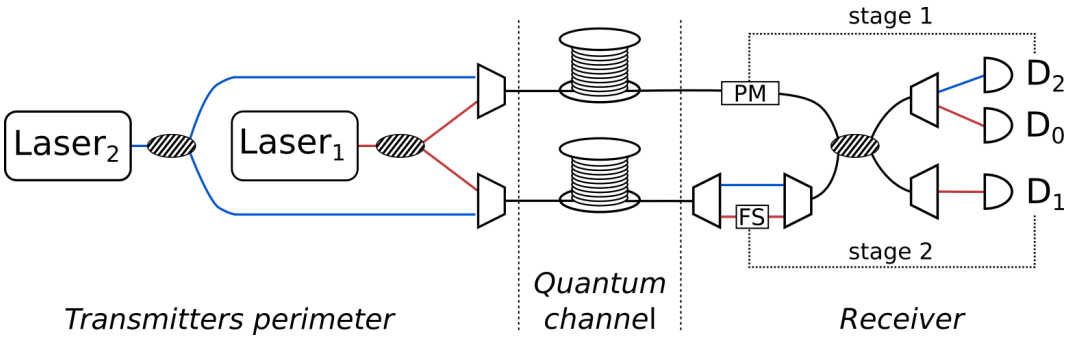

Figure 3.12: Schematic of the setup used to test the dual-band phase stabilisation system. Laser_1 and Laser_2: narrow bandwidth lasers used to emit λ_1 and λ_2 frequencies respectively. Striped ovals: BSs, trapezoids: Dense Wavelength Division Multiplexer/Demultiplexer (DWDMs), the spools represent the long optical fibre spools used for this test, semicircles: SNSPDs, PM: phase modulator, Fibre Stretcher (FS): fibre stretcher.

Due to the different expansion/contraction rates of the channels connecting Charlie to the two users, during the protocol execution we had to compensate for the change in length of the quantum channels. We did that by appropriately delaying the pattern encoding of one user with respect to the other, aiming at obtaining always optimal time alignment of the users' pulses at Charlie's BS. The intervals between these alignment adjustments depended on the stability of the environmental conditions in the lab, and varied from once every 4 minutes, up to once every 30 minutes. From the highest adjustments frequency, we estimated an upper limit on the length difference drift between the two sides of the communication channel (in our air-conditioned temperature stabilised lab) of $\sim 3\,\text{mm}\,\text{min}^{-1}$ over 600 km of fibre.

2-Stage Feedback Implementation Details

In order to prove the effectiveness of the dual-band phase stabilisation system, we built the testing setup shown in fig. 3.12. In this setup, two lasers (Laser_1 and Laser_2) generate the two different wavelengths needed for coarse (stage-1) and fine (stage-2) phase corrections. The two wavelengths are set to λ_1=1550.12 nm and λ_2=1548.51 nm. The output of each laser is split in two. Each half is multiplexed together with a part of the signal from the other laser. The combined signals are then sent through two fibre spools, each 277.46 km long. After the fibre spools, which constitute the communication channel being tested, the two signals are recombined at the receiver station. Here, two modulators (a PM and a FS) constitute the actuators of the stage-1 and stage-2 of the feedback system. The signals coming

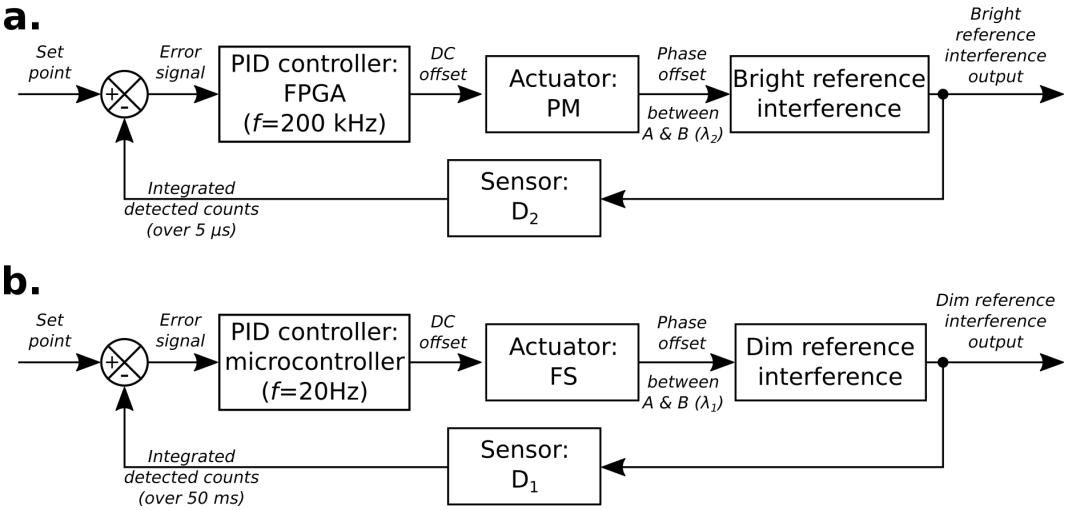

Figure 3.13: Block diagrams of the phase-stabilisation system. **a.** Stage-1 compensation. **b.** Stage-2 compensation.

from the two different paths interfere on a 50:50 BS, and a series of SNSPDs record the interference outcomes. In fig. 3.12, whenever the signal at different frequencies are separated, the fibres are marked with a different color (red for λ_1 and blue for λ_2).

A detailed block diagram representations of the two-stage phase stabilisation system is given in fig. 3.13. The top diagram (fig. 3.13a) shows the stage-1 of the compensation feedback. It features a closed loop cycle that locks the interference between the λ_2 signals to a given intensity level. This, in turn, locks the phase offset between the BR signals to a fixed value. Their interference is monitored by the SNSPD D_2. Single photons detected by D_2 are integrated over a period of 5 µs. The difference between the integrated number of counts and a set value constitutes the error signal of a PID controller implemented with a Field Programmable Gate Array (FPGA) clocked at 200 kHz. By tuning the DC offset of the PM placed on the upper arm of the interferometer in fig. 3.12, the FPGA controls the interference between the bright references. It is important to notice here that the phase shift applied by the PM affects both the wavelengths λ_1 and λ_2. The stage-1 feedback fully stabilises the bright reference light, while it only partially stabilises the signal at λ_1. As explained in the previous section, the remaining phase drift over λ_1 is related to the ratio $(\lambda_1 - \lambda_2)/\lambda_1$.

Figure 3.13b refers to the stage-2 of the compensation system. This second closed loop aims at correcting the residual phase drift on λ_1. The error signal for it

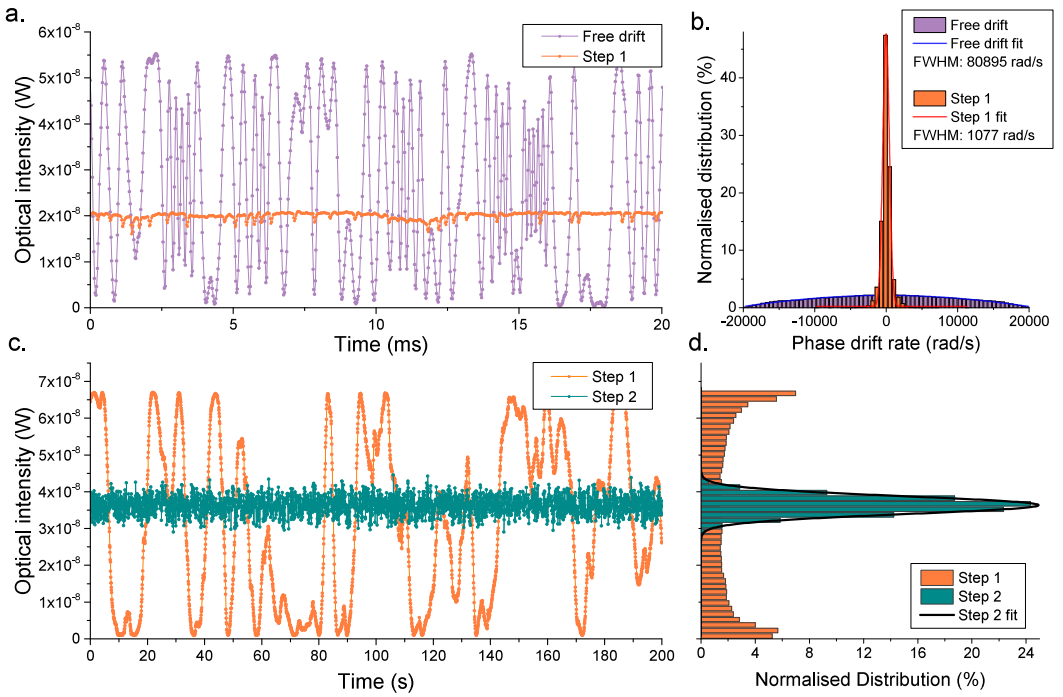

Figure 3.14: The data shown in this figure was obtained with the setup shown in fig. 3.12. All these measurements have been done with a power meter for easier comparison. **a.** Comparison between free drifting (purple) and step-1 stabilised (orange) data. Acquisition time for this measurement was 25 µs. **b.** Histogram of the phase drift rate for the data presented in panel (a). **c.** Comparison between step-1 (orange) and step-2 (teal) stabilised data. **d.** Optical intensity distribution for the data shown in (c).

is provided by the overall interference outcome of the signals at λ_1. For the purpose of the test showed in fig. 3.12, this is constituted by the CW light produced by Laser$_1$. The residual phase offset is retrieved by integrating the single photons detected by SNSPD D_1 over 50 ms. The difference between this value and a set value provides the error signal for a PID controller implemented with a micro-controller operating at the frequency of 20 Hz. The micro-controller corrects the phase offset by modulating a FS acting on the dim signal passing through the bottom arm of the interferometer in fig. 3.12. Differently from stage-1, stage-2 acts solely on the λ_1 signal and can therefore can correct the residual phase drift on this wavelength.

2-Stage Feedback System Characterisation

Figure 3.14 shows the results of the tests executed on the setup in fig. 3.12. In our tests we looked at the interference outcome for λ_1, over a 555 km long quantum

channel, at different stages of the stabilisation process.

The purple dots in fig. 3.14a represent the interference when no phase stabilisation is applied. Over this distance, the phase drift is so rapid (in the order of $10 \times 10^4\,\mathrm{rad\,s^{-1}}$) that it is possible to discern the interference fringes only after zooming into the millisecond time scale. The orange dots in fig. 3.14a represent the interference when stage-1 of the stabilisation system is activated. Stage-1 stabilisation system reduces drastically the phase drift rate for λ_1 interference. The effectiveness of this stabilisation is quantifiable by the reduction in the phase drift rate, as shown in fig. 3.14b. When step-1 feedback is enabled, the FWHM of the drift rate (for the data shown in fig. 3.14a) decreases from $81\,900\,\mathrm{rad\,s^{-1}}$ to around $1100\,\mathrm{rad\,s^{-1}}$. The phase drift reduction is even more significant if we compare the phase drift measured in the µs time scale for the free drifting interference, with the one measured in the ms time scale for the step-1 stabilised interference (i.e. using the orange data shown in fig. 3.14c). By looking at a longer time frame for the step-1 stabilised data, we average out the small phase jumps occurring at the µs level (visible in fig. 3.14a). This gives a more meaningful measure of the phase drift reduction achieved by the fast feedback. In this case, the standard deviation of the phase drift reduces from $34\,400\,\mathrm{rad\,s^{-1}}$ to $0.52\,\mathrm{rad\,s^{-1}}$, i.e. a phase drift reduction of a factor ~ 66000. The reduction ratio is ~ 60 times better than the estimated factor 1000 due to the self-cancellation of rapid opposite drifts.

After activating step-1 of the stabilisation system, a residual slow phase drift is still present for λ_1. In fig. 3.14c it is possible to follow the evolution of constructive or destructive interference over a time scale of tens of seconds. Figure 3.14d shows the optical intensity distribution associated to the data shown in panel (c). Here, the step-1 stabilised data (orange) present the typical 2-peaks intensity distribution associated with samples having a uniformly distributed phase over the $[0, 2\pi)$ interval.

The residual slow phase drift can be readily compensated by step-2 of the stabilisation system, which acts exclusively on the λ_1 signals. Step-2 activation leads to a stable interference output (teal dots in fig. 3.14c) lockable to any arbitrary value. In fig. 3.14c and (d) the interference is locked at $\pi/2$. The locking error is calculated to be $0.07\,\mathrm{rad}$, sufficient for low QBER operation.

3.5 Discussion

At the beginning of this chapter, in sections 3.1 and 3.2, we gave an overview of the main experimental methods and components commonly used in QKD experiments. This discussion was followed by a more detailed description and characterisation of the techniques we developed to succeed in the implementation of the TF-QKD protocol. These are related to the phase locking of two space separated laser sources (in section 3.3), and to the stabilisation of the phase of the quantum channel (section 3.4). Both these techniques were probably introduced to the field of quantum communications through our work.

In chapter 6, and section 6.2.1 in particular, a comparison will be made between the two phase stabilisation techniques introduced in this chapter in the context of long-distance quantum communications.

All the methods described in this chapter have been fundamental to obtain the results presented in chapters 4 to 6.

Chapter 4

Proof of Principle TF-QKD Experiment

The introduction of the TF-QKD protocol in 2018 [95] by researchers at Toshiba Europe Ltd. (see chapter 2) sparked considerable interest in the QKD research community. Enthusiasm about the new possibilities enabled by the protocol was accompanied by skepticism about its experimental feasibility. For this reason, assessing the experimental viability of the protocol and demonstrating its advantages over other QKD protocols was a crucial step.

This chapter describes the first experimental realisation of TF-QKD, executed over significant channel losses (up to 90 dB) using VOAs. In the high loss regime, the obtained SKR exceeds the repeaterless Secret Key Capacity (SKC_0) bound, providing the first experimental evidence that the repeaterless rate-loss limit can be overcome with present-day technology. The results of this research[1] were published in [122].

4.1 Experimental Setup

For this experiment, we consider a generalised TF-QKD protocol that can be modified to encompass a few of its variants [95, 117, 118, 120, 121, 125]. All these variants

[1] This experiment was executed in close collaboration with Mariella Minder. Together we designed, built and tested the experimental setup. I personally designed, developed and implemented the phase feedback system and the optical frequency regeneration setup. I also developed the code used to simulate the protocol and analyse the data and the error model for the feedback QBER contribution. I collected the vast majority of the data presented in this chapter and its appendix.

have the same essential experimental requirements, which are outlined below.

Alice and Bob should use two separate lasers to prepare coherent states in a given phase and polarisation state, with various intensities. The two lasers should be phase-locked to a common optical reference to allow the process of phase reconciliation between the users' pulses at the end of the protocol. We represent Alice's states as $|\sqrt{\mu_a}e^{i\varphi_a}\rangle$, where μ_a is the pulse intensity and $\varphi_a \in [0, 2\pi)$ is its phase. Bob prepares similar states with the subscript a replaced by b. The phases $\varphi_{a,b}$ include both the bit information and the random values needed in coherent-state TF-QKD. Experimental techniques that could be used to accomplish the phase referencing between the users' pulses have been discussed in section 3.3. In sections 4.1.1 and 4.1.2 we will describe how these techniques have been adapted for this experiment, providing their experimental characterisation.

The prepared optical pulses should interfere with high visibility at Charlie's BS after travelling through the quantum channel separating the users. The interference visibility should remain stable over the time, a challenging task when the channel loss significantly reduces the number of photons arriving at the receiver station. Possible strategies to address the channel stabilisation have already been discussed in section 3.4, and only the one based on time-multiplexing (presented in section 3.4.2) will be employed in this experiment. In section 4.2 we will describe the results obtained with it.

Finally, the users should detect the pulses, reconcile the random phases and reconstruct the key bits. The encoding pattern used to achieve this is the one already presented in section 3.4.2.

4.1.1 Optical Injection Locking Characterisation

The first approach to phase randomisation and dissemination tested in this experiment consisted of a combination of Laser Diodes (LDs), gain switching and OIL. The gain switching technique is used to generate optical fields with random phase [165]. OIL is used to synchronise the phase between the two users and was discussed in section 3.3.1.

Figure 4.1 shows how these techniques can be combined together to meet the requirements of TF-QKD. In this setup, a master LD is periodically gain-switched at a frequency of 2 GHz, producing a train of optical pulses with the same clock rate. The chosen gain switching frequency is low enough to guarantee the depletion of the electromagnetic field in the LD cavity, and thus ensures that each generated pulse

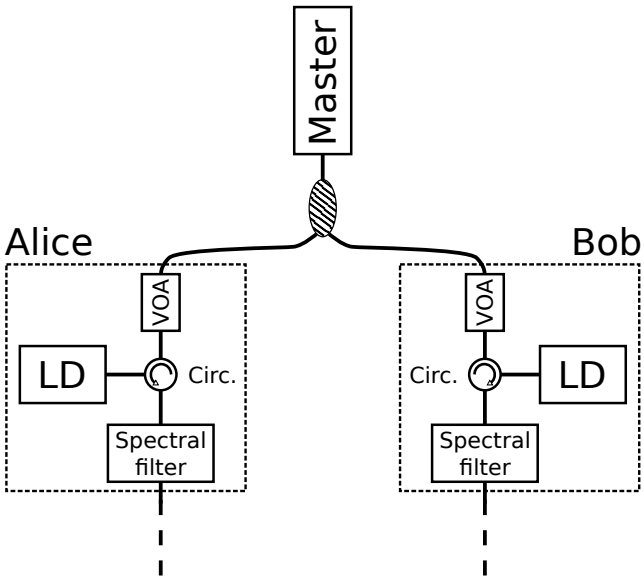

Figure 4.1: Alice's and Bob's LDs are optically injected by a gain-switched master LD through a circulator. This way, the master laser distribute the phase reference to the users' lasers, which will produce phase referenced randomised optical pulses.

has a random phase due to sampling vacuum fluctuations [165, 166].

Each user is also endowed with another LD that is gain-switched at 2 GHz. Differently from the master laser, the users' LDs are injected with the light produced by the master laser (OIL technique [167]). Every cycle, Alice's and Bob's lasers emit a 70 ps pulse at 1548.92 nm with the same random phase, uniformly selected from the $[0,2\pi)$ phase interval. Additional 15 GHz spectral filters are used to clean the spectral modes of the emitted pulses [167], thus ensuring high visibility first-order interference between the twin-fields.

In fig. 4.2 we test the effective randomness of the pulses generated with this setup. We do this by interfering, for each user separately, pulses of adjacent clock cycles using a 500 ps asymmetric MZI. This interference produces the standard double peak histogram expected from phase-randomised laser pulses [165]. We then confirm the phase coordination by interfering pulse pairs emitted by the users' lasers at the same clock cycle and obtain a first-order optical interference with 98.7% visibility for both users.

In order to test the phase coordination of the pulses prepared by the two users, we also test the first-order optical interference visibility between pulses prepared by them. In this case, the measured interference visibility is 97.5%.

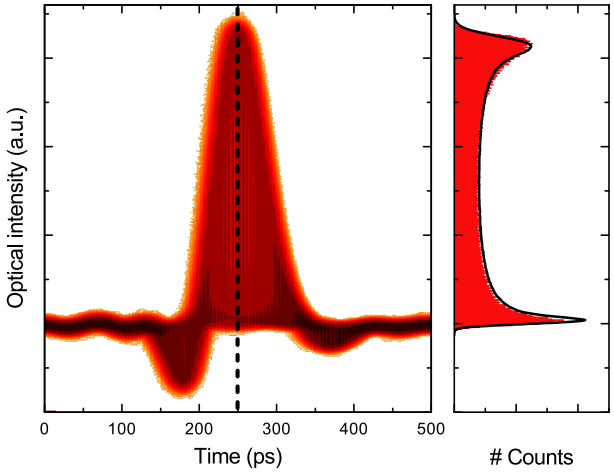

Figure 4.2: **Left:** colour coded density plot of Alice's slave laser intensity after a 500 ps asymmetric Mach-Zehnder Interferometer (MZI). **Right:** histogram of the optical intensity, recorded along the dashed line in the left figure. Also shown is the simulation line that accounts for experimental imperfections (solid black line). The agreement between the experimental results and simulation indicates that the pulses have random phase [154]. An analogous measurement on Bob's slave laser gives similar results.

Although OIL proved to be an effective way to execute frequency cloning between the two users, there is one aspect of this technique that could have undesirable consequences for TF-QKD. These are related to the fact that in OIL the users expose their lasers' cavity to the seeding light coming from an external master laser. This configuration, without additional assumptions on the trustworthiness of the agent controlling the mater laser and on the security of the optical channels used for frequency distribution, could introduce side channels in the setup that could compromise the security of the protocol implementation. Since no study has been conducted yet to investigate these possible security concerns for OIL, in this experiment we tested also a second approach to frequency cloning based on OPLL, which removes the concerns about a side channel. This will be the argument of the next section.

4.1.2 Optical Phase-Locked Loop Characterisation

The second approach tested in this experiment for phase synchronisation and randomisation used the OPLL technique and active phase randomisation (discussed in section 3.3.2).

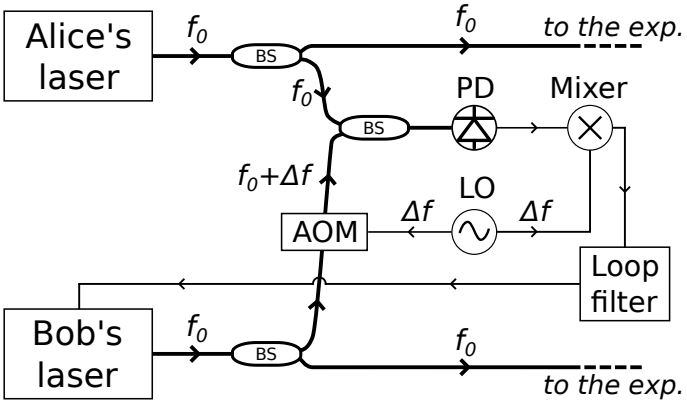

Figure 4.3: Alice's and Bob's lasers are locked with each other through a heterodyne optical phase-locked loop. In this configuration, when the lasers are locked, they emit the same optical frequency, with Bob's laser following Alice's free-running fluctuations. BS, 50:50 optical coupler; PD, photodiode; Mixer, electronic mixer used as phase detector; LO, local oscillator (80 MHz); f_0, reference frequency; Δf, frequency offset (80 MHz) provided by the LO.

The advantage of OPLL over OIL in TF-QKD emerges from the fact that in the former no one except for the legitimate laser owner has access to the laser cavity. In a scheme using OPLL for frequency cloning, the only way an attacker could influence Alice's and Bob's output is by modifying the reference light received by the users. However, this would not compromise the security of the protocol. Any such modification would reflect into a shifted $\varphi_{a,b}$ value encoded by Alice and Bob, which is equivalent to introducing phase noise on the main channels going from the users to Charlie (see also [168] for a similar argument applied to QKD).

Figure 4.3 shows the diagram of the heterodyne OPLL implemented in this experiment for cloning Alice's laser frequency to Bob's laser. Since in this experiment Alice's and Bob's lasers are required to have the same frequency, the standard heterodyne OPLL scheme has been modified to include a frequency shift of the slave laser. The frequency shifting is executed by an Acousto-Optic Modulator (AOM) acting on Bob's laser just before its interference with the signal coming from Alice. The AOM is driven by the same local oscillator used as reference for the OPLL. In this setup the LO provides a constant 80 MHz sinusoidal signal.

For this experiment, heterodyne OPLL has been chosen over its homodyne analogue for one main reason: this type of locking ensures that the beat note recorded from the photodetector is at an intermediate frequency, close to the one of the local

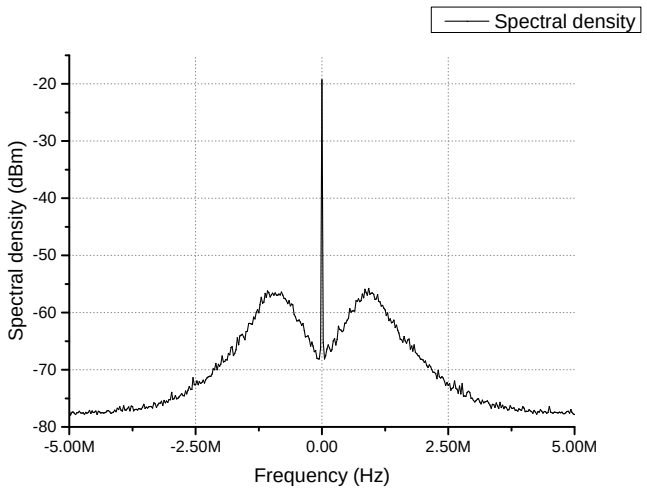

Figure 4.4: RF output of the photodiode as recorded by a spectrum analyser when the two lasers are phase-locked. An 80 MHz offset is applied to the graph horizontal axis. The measurements shows a -40 dB extinction ratio leading to a residual phase error of less than 5°.

oscillator. This has two advantages: it allows a straightforward electronic filtering of the low-frequency noise sources, such as DC fluctuations, and it makes the frequency locking more robust against the lasers intensity fluctuations, making the frequency cloning more efficient.

The performance of the implemented OPLL setup has been tested by looking at the residual phase noise associated with the frequency cloning. The results of this test are shown in fig. 4.4. The measured residual phase noise is $\sigma_\varphi^2 = 7.5 \cdot 10^{-3}$ rad^2, equivalent to a phase error between the users' lasers of 5.0°.

When OPLL is used for frequency cloning between the two users' lasers, phase randomisation of the pulses is obtained by actively encoding a random phase value onto them through two phase modulators driven by a Digital-to-Analog Converter (DAC) with 8-bit amplitude resolution.

A measurement of the first-order optical interference visibility between the pulses prepared by the two users through OPLL and active phase randomisation yields 96.4%. This is 1.1% lower than the interference visibility obtained when OIL and passive phase stabilisation through gain switching are used. We attribute this difference to phase errors introduced by the OPLL and the active phase randomization.

4.1.3 Complete Experimental Setup

Figure 4.5 shows the full setup used for the experiment. Here we show a version of the setup using the OPLL for frequency distribution and active phase randomisation through PMs. An almost identical version of it using OIL for frequency cloning and laser gain-switching for phase randomisation has also been tested.

In this setup each user is endowed with a CW laser source (LS). Alice's LS acts as a reference. Its output is split in two by a first BS. One part is sent to Bob through a service fibre, and is used to lock Bob's LS via a heterodyned OPLL (described in section 4.1.2).

The fraction of each user's light not involved in the phase locking mechanism is directed to the Encoder, depicted in fig. 4.5b. Here light enters the cavity of a slave LD that is periodically gain-switched to produce a pulse train at 2 GHz. This ensures that each pulse will inherit the phase of the injected optical field, which is locked to the reference light. Moreover, Alice's and Bob's LDs will emit pulses as narrow as 70 ps at 1548.92 nm, with a high extinction ratio and constant intensity. After the LD, the optical pulses pass through an in-line PM which applies fast modulation of the phase values required by the specific TF-QKD protocol, including the values of the key bits, the random global phase and the reference phases necessary to control the phase noise on the paths linking to Charlie. 15 GHz spectral filters clean the spectral modes of the emitted pulses. The intensity of the optical pulses is set by the intensity controller (INT) and the power detector (PD), while the polarisation is controlled with the EPC. After the encoding, the pulses are sent to a VOA that varies the loss of the channel connecting each user to Charlie.

The pattern used in the experiment is 2^{10}-bit-long, and is periodically repeated over time. As explained in section 3.4.2, half of the pattern consists of phase unmodulated pulses, which are needed for the phase stabilisation of the setup. The remaining half consists of phase modulated pulses where the phase information required for the key generation is added to one of the 2^5 equally spaced phase values randomly taken within the $[0, 2\pi)$ interval. The number of phases used is sufficient to closely approach a phase randomisation with infinite random phases [169].

At Charlie's BS, Alice and Bob's optical fields meet and produce an outcome that is detected by SNSPDs featuring dark count rate 22 Hz and approximate efficiency 43%.

Detector D_2 is used to detect optical field leakage into the non-intended polarisa-

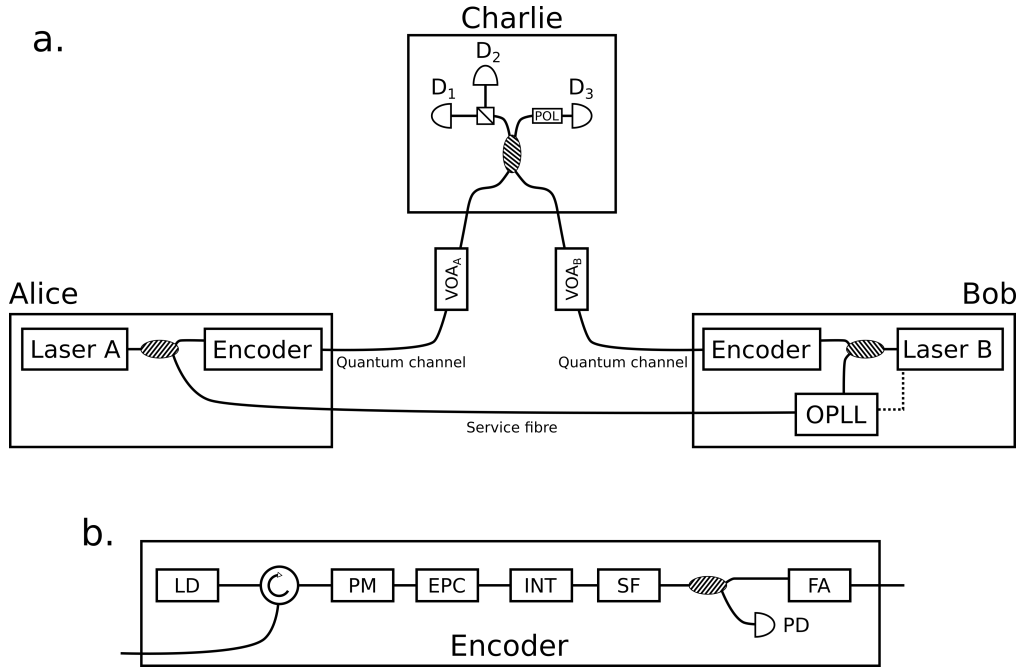

Figure 4.5: **a.** Alice and Bob generate light beams from their local CW laser sources and send them onto a pair of beam splitters. One pair of output beams go to the Encoders and is used to perform TF-QKD encoding. The other pair is used to lock the users' lasers through a service fibre and the heterodyne OPLL (described in section 4.1.2). The pulses produced within the Encoders travel through the quantum channel to interfere on Charlie's BS. The outcome of the interference is registered by detectors D_1, D_2 and D_3. **b.** In the encoder modules, the continuous-wave light prepared locally by Alice's and Bob's laser sources seeds a gain-switched LD that carves it into pulses. The optical pulses are either rapidly modulated or finely controlled in phase by a PM. After crossing the Electronic Polarisation Controller (EPC) and the intensity controller (INT), part of the pulses is directed to the power detector (PD) for monitoring the intensity, and the other part travels through the quantum channel towards Charlie's BS. SF, spectral filter; FA, fixed attenuator; POL, polariser; D_n, single photon detectors.

tion, and minimises it using Alice and Bob's polarisation controllers to prevent such leakage and maintain the same polarisation for both twin-fields.

Detector D_1 is associated with a 100 ps resolution time tagger and is used to generate the raw cryptographic key. These detections are grouped in post-processing according to the phase values encoded onto the interfering pulses. By analysing the statistics of the different phase combination groups, the experimental gain and the QBER of the system are retrieved.

D_3's signal is sampled at an interval of 10 ms by a photon counter to provide feedback to stabilise a common reference phase between Alice and Bob. This is achieved through DC modulation of one of the two users' PM. This is equivalent (for small-sized systems) to having an extra PM in Charlie's station, as proposed in the original TF-QKD paper [95].

The ambient temperature fluctuations cause the interference between the users to drift over time. Even with only ≈40 m of optical fibre in the setup, the environmental fluctuations cause a relative phase drift in our setup of $0.7\,\mathrm{rad\,s^{-1}}$. This requires the feedback control (described in section 3.4.2) to correct the phase at least every 100 ms to avoid detrimental effects on the QBER.

4.2 Results

In this section we will present the experimental results obtained with the setup described in section 4.1.3, where the frequency locking between the two transmitting users is achieved through OPLL.

Before executing this experiment, we ran another experiment that used OIL for frequency distribution between the users. We will refer to the first experiment as the "support experiment", in contrast to the "final experiment" discussed in the rest of this chapter. The reason why we repeated the experiment by substituting OIL with OPLL is related to the security concerns for OIL mentioned at the end of section 4.1.1. Although no further mention to the "support experiment" will be made in the remainder of this chapter, the detailed experimental results obtained in that experimental configuration are reported in appendix A.1, to offer a comparison to the "final" results.

The rest of this section is divided in three parts: we will first discuss the results regarding the QBER and its stabilisation (section 4.2.1), then the gain obtained experimentally at various channel attenuations (section 4.2.2), and finally the SKR

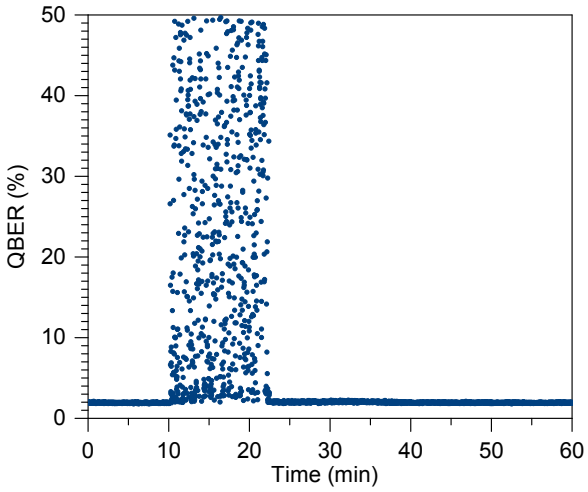

Figure 4.6: While monitoring the QBER during the a TF-QKD session, the phase feedback system is turned OFF for a period of ∼12 minutes, letting the relative phase between the optical fields drift freely. When the feedback system is ON, the QBER is well stabilized to its minimum.

extracted from the experiment (section 4.2.3).

4.2.1 QBER

Phase Stabilization and QBER

With a 50% duty cycle of reference and signal pulses, the phase stabilization feedback was running continuously during the TF-QKD protocol execution. The effectiveness of the control system is shown in fig. 4.6. In this measurement, taken with 30.1 dB of loss in the quantum channel, the feedback was ON for approximately the first 10 minutes. During this period, the measured QBER in the $\mathcal{X}$ and $\mathcal{Y}$ bases is kept at an average value of 2%. After 10 minutes, the feedback was switched OFF for ∼12 minutes. During this period, the QBER fluctuates between its minimum and 50%. In this graph the QBER never exceeds the 50% threshold due to its bit-flip symmetry. Whenever its value overcomes 50%, we plot its complementary 1-QBER instead. Little after 22 minutes, the feedback is switched ON again and the QBER fluctuations are suppressed again for the next 40 minutes.

Feedback contribute to the QBER

In this experiment the maximum channel attenuation at which it is possible to obtain a positive SKR is limited by the feedback system used for the phase stabilization. To work properly, the feedback system needs to detect a number of photons that is representative of the interference process occurring at the BS. An increase in the channel attenuation entails a reduction of the detected sample size, and, consequently, an increase of significance in the statistical fluctuations of the detected number of photons. The stabilization feedback will interpret these statistical fluctuations as a phase offset between the two arms of the interferometer, and will thus erroneously correct the phase difference between the two arms to a position that is different from the ideal $\pi/2$ locking position. At a low counts, the effectiveness of the stabilization system will therefore be reduced. This will introduce an additional error to the detection process.

In order to take this aspect into account, the effect of the feedback instability on the QBER increase has to be modelled. Under the assumption of dealing with small errors the experimental QBER can be divided into three independent factors:

$$E_{exp} = E_{opt} + E_{DC} + E_{Fb}. \tag{4.1}$$

The first two terms, E_{opt} and E_{DC}, correspond, respectively, to the optical QBER and to the QBER due to the detectors' dark counts. More details about this standard QBER decomposition can be found in previous work [124]. E_{Fb} is the contribution to the QBER given by the feedback instability. We linked it to the channel attenuation through a mathematical model that takes into account the physics of the feedback system.

E_{Fb} modelling can be divided into the three steps described below. The first step consists in estimating the count fluctuations at the detector used to obtain the input signal of the feedback. The expected number of counts arriving at the detector, assuming a certain transmitted photon flux (μ), channel length (L), Charlie's apparatus transmissivity (η_{Ch}) and detector efficiency (η_{det}), is:

$$N_{det}(L) \propto \mu e^{-\frac{\alpha\, L/2}{10}}\, \eta_{Ch}\, \eta_{det}. \tag{4.2}$$

N_{det} will also depend on the integration time set on the counter used in the feedback system (this is the reason why we used the proportionality relation in eq. (4.2)). By assuming that the number of counts (N_{det}) recorded by the feedback system

follows a Poissonian distribution, we can estimate that the standard deviation of such quantity is proportional to $\sqrt{N_{det}}$.

The second step consists in evaluating the consequences of a fluctuation of the detected number of counts, on the phase correction given by the feedback system. From the model of the feedback system given in section 3.4.2, we can calculate the phase deviation associated to a Poissonian photon number fluctuation. Around the $\pi/2$ locking condition the evaluated fluctuation is:

$$\Delta\theta(N_{det}) = -\arccos\left(\sqrt{\frac{2}{a \cdot N_{det}}}\right) + \frac{\pi}{2}. \tag{4.3}$$

In eq. (4.3), a is a factor that incorporates the averaging time of the counter used for the feedback.

In the third step we link the interference phase offset to the decrease in visibility associated with it, and from there, we evaluate the QBER associated to the feedback instability. From standard optical interference calculations, it follows that the visibility of the interference between two incoming optical fields with a respective phase offset of $\Delta\theta$ is:

$$Vis(\Delta\theta) = \frac{4\cos(\Delta\theta)}{3 + \cos(2\Delta\theta)}. \tag{4.4}$$

Inserting this information into the standard relation between the visibility and QBER for BB84 encoding

$$E_{Fb}(Vis) = \frac{1 - Vis}{2}, \tag{4.5}$$

we prepared all the relations to obtain E_{Fb}.

Inserting eq. (4.2) into eq. (4.3), and the result in eq. (4.4) and then in eq. (4.5), we obtain the relation that bounds the QBER introduced by the feedback system instability to the channel attenuation. In order to obtain some flexibility on the final E_{Fb} function, we can insert two tunable parameters a and b in eq. (4.3): $\Delta\theta(N_{det}) = -\arccos\left(\sqrt{\frac{1+b}{a \cdot N_{det}}}\right) + \frac{\pi}{2}$. The parameters a and b are directly connected to two aspects of the feedback system: a represent the mean value of the averaging time set on the counter used for the feedback, and b is a weighting factor of the number of photons constituting the count floor (given by the pulses used for quantum states encoding) compared to the counts related to the reference pulses. In order for these two parameters to match with the feedback system characteristics, the two values must be approximately: $a \approx 1$ and $b \approx 15 \times 10^6$.

Figure 4.7 shows how this model fit to the experimental data. In the graph, the three contributors to the QBER (E_{opt}, E_{DC}, E_{Fb}) are plotted alongside the overall

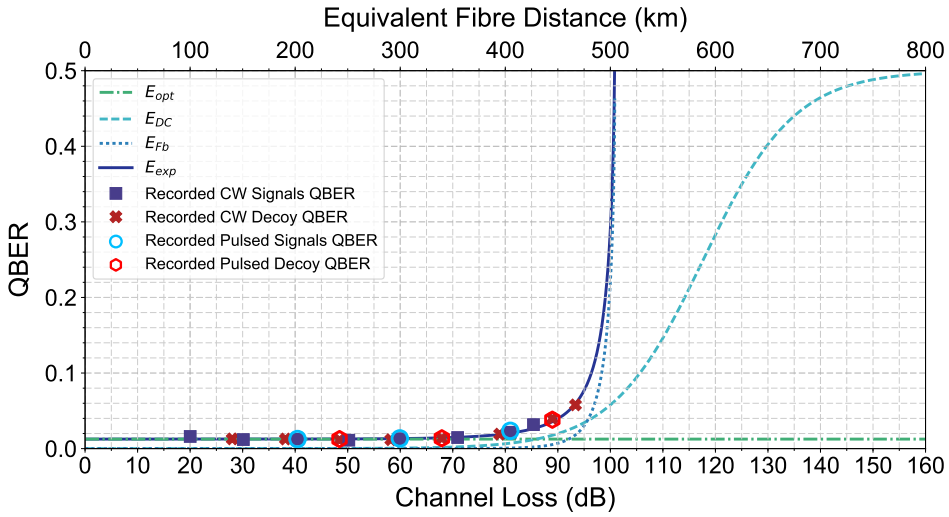

Figure 4.7: Signal and decoy states (of intensity v) QBER plotted in line (as if all the state were sent with a Signal photon flux) alongside the curves used to simulate the QBER trend. The equivalent fibre distance at the top of the graph is calculated assuming a standard single mode fibre with an attenuation of $0.2\,\mathrm{dB\,km^{-1}}$.

E_{exp} function and the experimental data (more presented in the next section). The graph shows the results obtained when seeding the Slave lasers both with a CW and a pulsed master laser. The solid line shows the trend of the overall E_{exp} model. The curve follows nicely the trend of the experimentally recorded data. The dotted and dashed lines show E_{opt}, E_{DC}, E_{Fb} contributions. E_{opt} represent the optical QBER, it is constant over the channel attenuation, and in this configuration is equal to 1.3%. Its value has been retrieved experimentally by fitting the QBER value recorded below 70 dB by a constant factor. E_{DC} is the QBER due to the dark counts at the detector used for the phase feedback. The curve is described by the standard QKD model, with a Dark Counts rate of 55 Hz. E_{Fb} is the QBER associated to the feedback instability. From the graph it is evident that this is the factor that affects the most the overall QBER at high channel attenuations. In order to obtain the precise E_{Fb} expression, we fitted the experimental data with the E_{exp} model given in section 4.2.1. From the fit we obtained a=1.05 and b=10.8×10^6, close to the expected values, considering their physical meaning. In this graph, the equivalent fibre distance values on the top x-axis are obtained considering a quantum channel consisting of standard optical fibre with a $0.2\,\mathrm{dB\,km^{-1}}$ loss coefficient.

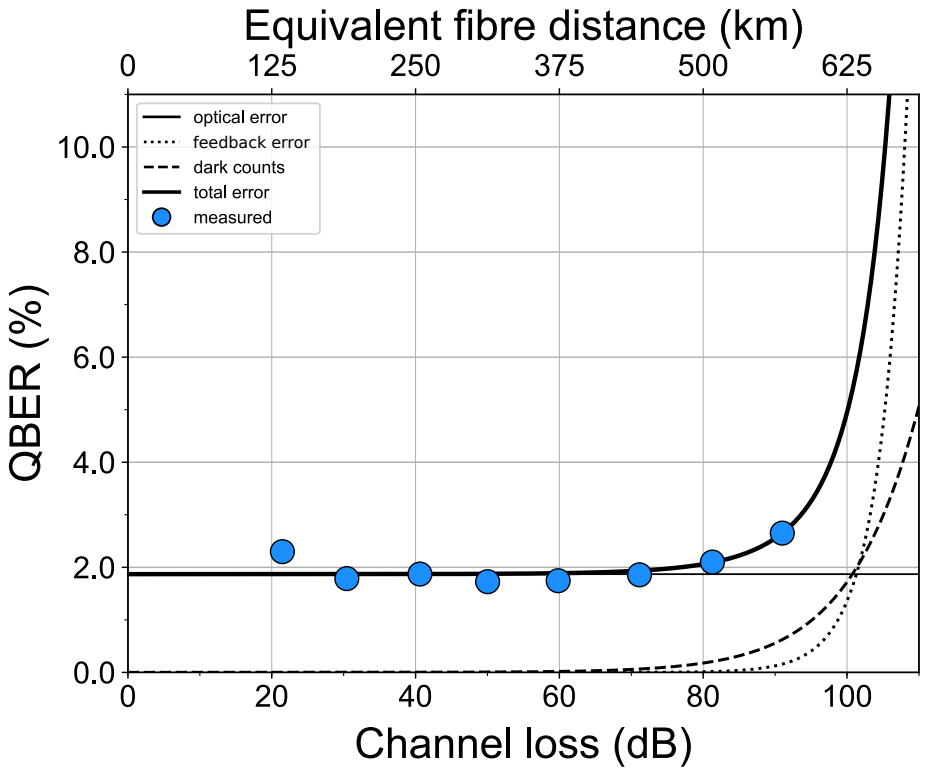

Figure 4.8: QBER retrieved experimentally (symbols) alongside their theoretical simulation (solid line). Also plotted are QBER contributions from the optical error (thin solid line), the detector dark count (dashed line) and the feedback error (dotted line). Raw data of the points presented in this figure is reported in table A.2 in appendix A. The equivalent fibre distance at the top of the graph is calculated assuming a ultra-low-loss single mode fibre with an attenuation of $0.16\,\mathrm{dB\,km^{-1}}$.

Experimental QBER

Experimentally, the QBER in each basis is defined as the number of clicks recorded when destructive interference should take place, over the total number of clicks received by the detectors in both the constructive and destructive time windows.

Figure 4.8 shows the experimental QBER (blue markers) recorded at different channel attenuations with the setup in fig. 4.5. Alongside the experimental QBER, in fig. 4.8 are also reported the simulations of the different QBER contributions in this setup. The optical misalignment of the system, which gives a constant QBER contribution for different channel attenuations, is represented with a thin solid line. The QBER associated with the detectors' dark counts (dashed line) is observable from

60 dB onwards. The feedback error affects mainly the last point, at approximately 90 dB attenuation, but limits acquisitions at higher attenuations. The sum of the three contributions to the QBER (thick solid line) fits well the experimental data.

The acquisition parameters had to be modified for the different measurements. Up to 70 dB, the integration time of the counter used in the feedback is kept to 20 ms, allowing for a feedback correction rate of 50 Hz. As the attenuation of the quantum channel was increased, the integration time had also to be increased to allow the feedback system collecting enough photons to assess the phase difference of the interfering fields. The maximum integration time used at the highest attenuation was 90 ms.

4.2.2 Gain

Experimentally, the gain is defined as the detection probability of a certain pulse type, per encoding gate. As discussed in section 2.2, the main advantage of TF-QKD over single-photon based QKD schemes is the scaling of its SKR with the square-root of the channel transmission, $\eta^{1/2}$. This would be impossible without correspondingly having the square-root scaling of the detection rate. We verified this essential feature of TF-QKD directly and summarised the result in fig. 4.9. Here, the recorded experimental data is plotted alongside the simulation of the expected gain.

The data corresponding to a direct-link quantum transmission was taken by shutting off one arm of the experimental setup, thus allowing a single user at a time to signal to Charlie's station. The data for double-path transmission, on the other hand, was taken with both arms open, while letting interfering at Charlie's station the pulses prepared by Alice and Bob. As is apparent from the figure, the single-path detection rate (triangular points on the dotted line) scales linearly with the loss, $1 - \eta$, whereas the double-path detection rate (square points on the dashed line) scales with the square-root. Limitedly to the detection rate, this entails that at any given rate, the double-path TF-QKD can tolerate twice the loss that direct-link QKD can.

Raw data of the points presented in fig. 4.9 is reported in table A.2 in appendix A.

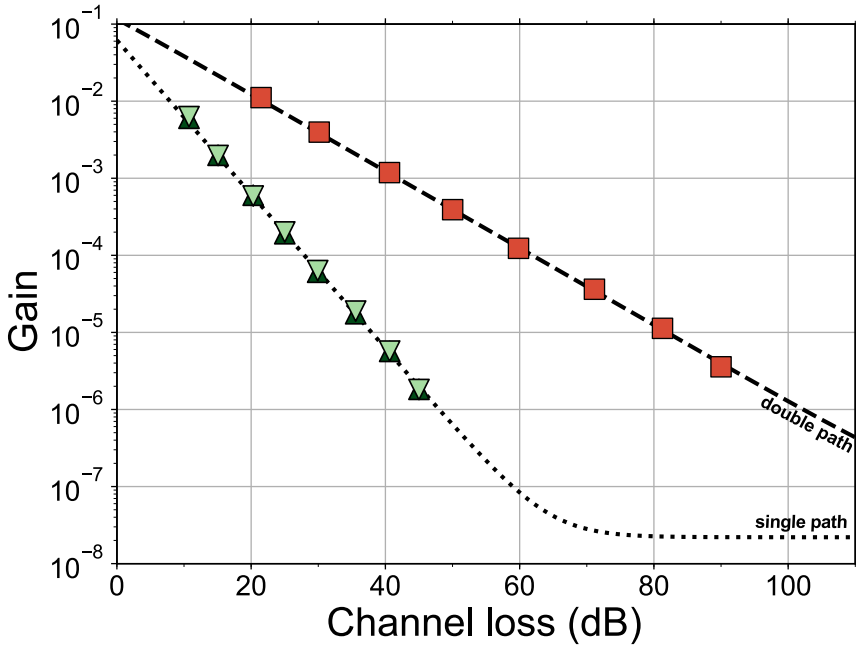

Figure 4.9: Gain plotted against the channel loss $(1-\eta)$. The different scaling laws of the gain for a QKD-like single-path quantum transmission and for a TF-QKD-like double-path quantum transmission are apparent. The upward and downward triangular (square) points on the dotted (dashed) line are the single-path (double-path) experimental detection rate recorded for different channel loss. All the experimental data agrees well with the theoretical curves.

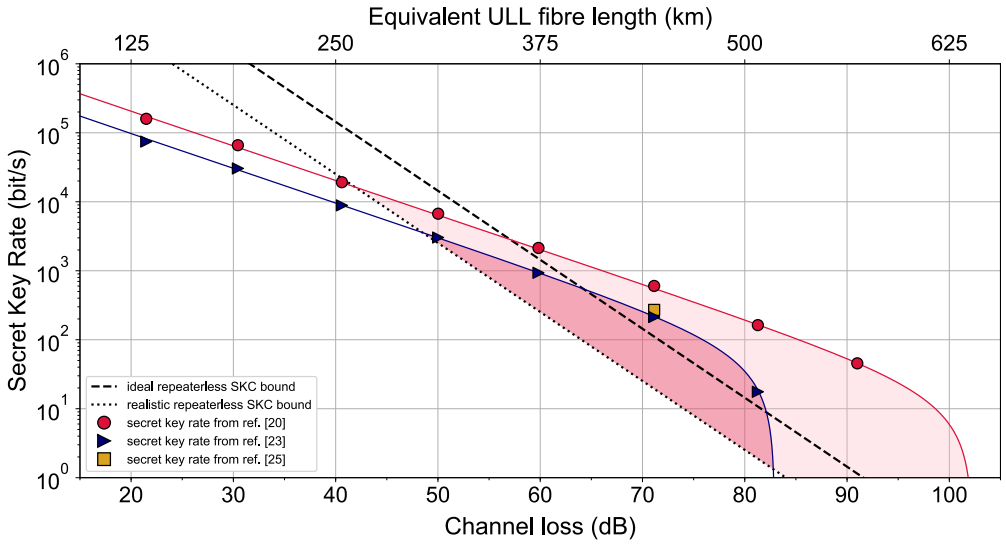

Figure 4.10: All the key rates are plotted against the channel loss (lower x-axis) and the corresponding ULL fibre distance (upper x-axis). The markers show the acquired experimental data. The realistic repeaterless bound SKC_0 [84] (dotted line) and the ideal one (dashed line) are plotted along with the key rates of the original TF-QKD protocol [95] (thin red line) and of the 'send-not send' one [121] (thin blue line). The TF-QKD supremacy region is shaded in pink. The simulations assume 1 GHz effective clock rate. The other parameters are: α =0.16 dB km^{-1}, ULL fibre attenuation; $\eta_C = 30\%$, total transmission of Charlie's module, resulting from $\eta_{det} = 43\%$ and $\eta_{\mathrm{coupling}} = 70\%$; $P_{dc} = 22$ Hz, dark count rate; $u = 0.4$, $v = 0.16$, $w = 0$, total (i.e. Alice + Bob) signal, decoy and vacuum flux, respectively. Charlie is assumed to be at equal distance from Alice and Bob.

4.2.3 Secret Key Rate

The experimental results presented in the previous two sections are independent of the specific security analysis adopted to extract a key rate. Hence they can be used as a reference to test the performance of different TF-QKD-like protocols. Here we analyze the data for three TF-QKD protocols, two [95, 121] over the whole loss range and one [120] at a specific loss of 70 dB. The first protocol is the original TF-QKD [95], which was proven secure under restrictive assumptions on the eavesdropper. The second and the third are the variants proposed by Wang *et al.* [121] and Curty *et al.* [120], respectively, which have been proved to be unconditionally secure. We have implemented these protocols using only 3 pulse intensities, rather than infinite, which is more practical.

In fig. 4.10 we plot the projected secret key rates versus channel loss for the

protocols analysed. We also plot two lines for the repeaterless secret key capacity. The *realistic* (*ideal*) SKC_0 accounts for a point-to-point QKD between Alice and Bob with a total detection efficiency of Bob's module equal to $\eta_B = 30.8\%$ ($\eta_B = 100\%$). The former is a reasonable bound, as it considers that Bob in the corresponding QKD setup that determines the SKC_0 bound has the same total detection efficiency as Charlie in our TF-QKD setup. The latter, on the contrary, is an upper bound to what is technologically feasible, as it compares our realistic Charlie's module with a lossless Bob having 100% detection efficiency.

The lighter (darker) pink shaded area is the TF-QKD supremacy region where the secret key rate of the protocol in [95] (the one in [121]) surpasses the realistic SKC_0. It is clear from the graph that starting from about 50 dB all the experimental points surpass the realistic SKC_0 bound and fall into the pink shaded region. From 60 dB onward, the points overcome also the ideal SKC_0 bound. This is the first time that such a fundamental limit has been overcome experimentally.

When we consider the protocol proposed by Curty *et al.* [120] we obtain a SKR of $271\,\mathrm{bit\,s^{-1}}$ at 71.1 dB with 1 GHz clock rate, which is 2.42 times above the ideal SKC_0 at the same attenuation ($112\,\mathrm{bit\,s^{-1}}$). It is worth mentioning that all the reported SKRs are quite conservative as they include the penalty due to an imperfect error correction ($f_{EC} = 1.15$).

The maximum channel loss at which we were able to stabilise the phase and obtain a key rate is 90.8 dB. This is equivalent to 454 km and 567 km of standard ($0.2\,\mathrm{dB\,km^{-1}}$) and ULL ($0.16\,\mathrm{dB\,km^{-1}}$) single-mode optical fibre, respectively, separating Alice and Bob. The SKR we extract from this point is $1.1\,\mathrm{bit\,s^{-1}}$ for the original TF-QKD.

The detailed parameters and rates for all tested protocols in the final experiment are given in appendix A.2.

4.3 Discussion

With this experiment we overcame for the first time rate-loss limit of direct-link quantum communications [84]. For this reason, recent literature (see [27]) considered it the first experimental realisation of an *effective quantum repeater*.

The other merit of this experiment is that it introduced a new set of experimental techniques in QKD to address the specific requirements of the TF-QKD protocol. These techniques are related to the phase locking of distant laser sources, for which

OIL and OPLL were employed, and to the phase referencing of the signals travelling through the quantum channel, for which a time-multiplexed phase stabilisation strategy was developed.

This proof-of-concept experiment showed that TF-QKD can greatly enhance the range and rate of quantum communications using currently available technology. In the next chapters (chapters 5 and 6) we will see how the experimental setup developed for this experiment can be improved to obtain similar results in more realistic operation scenarios.

Chapter 5

TF-QKD Setup Improvements

In this chapter we will discuss the improvements[1] made to the experiment presented in chapter 4. That setup, despite having all the fundamental features needed for testing TF-QKD, was characterised by numerous design simplifications which made it ideal for a preliminary investigation of the protocol but unsuitable for functioning in more realistic scenarios. Below are listed the aspects limiting the flexibility of the setup shown in fig. 4.5.

Physical proximity of the encoding equipment - In the proof of principle experiment, the equipment used by the encoding users (Alice and Bob) was not physically separated, and it actually was all anchored to the same $(60 \times 60)\,\mathrm{cm}^2$ optical breadboard.

Lack of fast intensity modulation by the users - In the proof of principle experiment, the intensity modulation necessary to encode the decoy states of the protocol was executed with VOAs. These devices are characterised by a limited modulation bandwidth, which extends only to the kHz region, and are therefore unsuitable to individually modulate pulses with a repetition rate in the GHz region. The use of VOAs for intensity modulation is the reason why for each SKR point shown in fig. 4.10 we had to take several measurements, one for each combination of the decoy states intensities sent by the users.

Control of all the modulators by a single signal generator - All the electronically driven elements in the encoder boxes (shown in fig. 4.5b) of both users

[1] The new experimental designs and their implementation discussed in this chapter were made by me. Colleagues and supervisors contributed with fruitful discussions and with the development of bespoke electronics.

were driven by a singular computer and a singular Arbitrary Waveform Generator (AWG). In a realistic scenario, each user must be equipped with its own computer and AWG, and the users' controlling units need to be synchronised remotely.

Length of the service channel - In order to reduce the phase drift introduced by it and simplify the experimental implementation, only a short ∼10 m long service fibre separated the two transmitters (Alice and Bob).

Length of the quantum channel - In order to reduce the phase drift introduced by it and simplify the experimental implementation, only a short ∼20 m long quantum channel separated the two transmitters (Alice and Bob) from the interfering station (Charlie), for a total length of the quantum channel of ∼40 m.

Optical phase drift stabilised with a PM in the transmitters - The feedback loop stabilising the phase of the TF-QKD setup used a PM in one of the encoder boxes as actuator. This solution is not suitable for the stabilisation of long communication channels where the timescale of the spontaneous phase drift introduced by the optical fibres is much smaller than the Time Of Flight (TOF) of the pulses travelling from the transmitters to the receiver.

Speed of the electronics driving the feedback loop - The maximum speed of the micro-controller driving the phase feedback loop was 1 kHz. A much faster correction speed is required to compensate the fast phase drift introduced by long optical fibres.

Lack of intensity contrast between reference and encoded pulses - The lack of an intensity contrast between the reference pulses used for channel stabilisation and the pulses used for encoding the protocol limited both the maximum speed of the phase correction feedback and the maximum channel attenuation the system could withstand.

In order to enhance the performance of our system and prepare it for future experiments, all the aforementioned aspects were addressed and improved. In this chapter we will describe the details of the upgraded experimental setup.

5.1 Design of Improved Transmitters for TF-QKD

Looking at the list at the beginning of this chapter, the most apparent limitation of the proof-of-principle setup is probably the proximity and interdependence of the users' equipment. A redesign and rearrangement of the transmitting units and of their components was necessary to enable the physical separation of the users.

Figure 5.1 shows a diagram of the upgraded transmitter modules. Two identical implementations of the diagram were realised, one for each transmitting station involved in the TF-QKD protocol. Most of the components in fig. 5.1 are inside gray areas. These areas represent two separate telecom rack boxes inside which the components have been arranged and fixed. Mounting all the components inside rack boxes increases the portability of the equipment and simplifies its deployment.

Inside the "Encoder" box, at the top of fig. 5.1, are placed all the components involved in the manipulation of the optical signal. The purpose of this box is modulating some incoming CW light with the aim of implementing the protocol. In the diagram, the CW light enters the encoder box from the left, while the fully modulated optical signals leaves the box from the right. The optical elements encountered by the light inside the box are in order:

- One EPC followed by a polariser (POL) which are used to polarise and maximise the coupling of the incoming CW light along the optical axes of the other modulators inside the box.

- Three IMs arranged in cascade which are driven by digital RF signals and are used to modulate the intensity of the incoming CW light. The three IMs are used to carve optical pulses out of the CW light and to set three different intensity levels for the pulses (u, v, w decoy states). The intensity ratios between the different intensity levels can be adjusted by the amplitude of the RF signals driving the IMs. Three daisy chained IMs are used instead of a single IM to increase the stability and precision of the intensity modulation.

- One 50:50 BS is used to split the light in two. Half of it will receive additional modulation, while the other half is sent to a power meter for monitoring purposes.

- Two PMs are then used to encode the phase of the optical pulses. Two daisy chained PMs are used instead of a single one to reduce the amplitudes of the driving RF signals. By limiting the modulation range for each PM to $[-\frac{\pi}{2}, \frac{\pi}{2})$,

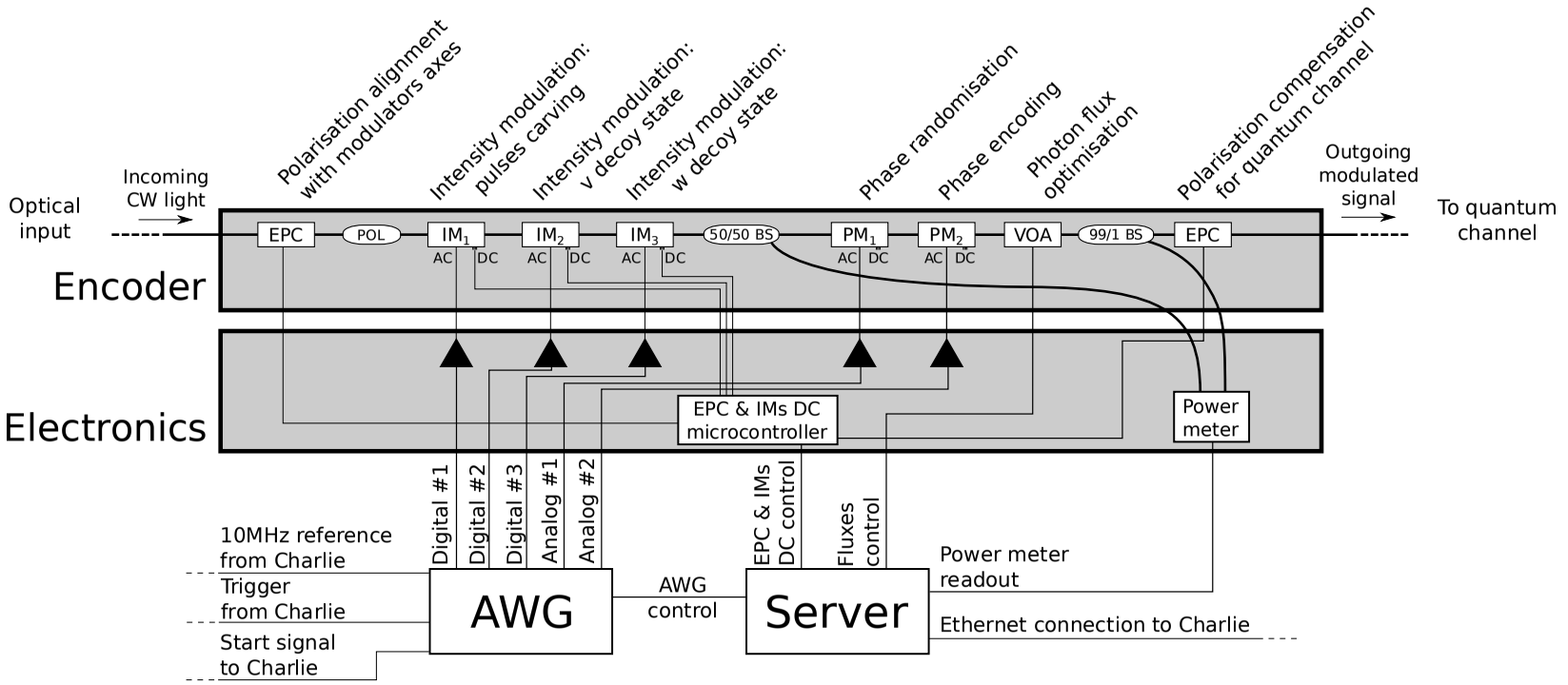

Figure 5.1: Schematic of the compact transmitting modules. The gray area at the top of the figure represents the 'Encoder' box, a telecom rack box which includes all the modulators needed to encode the protocol. The gray area at the bottom represents the 'Electronics' box, a rack box which includes most of the electronics providing the driving signals for the modulators in the encoder. The AWG and the Server at the bottom are used to generate the RF patterns needed for the encoding and control all the equipment in the transmitter. EPC: Electronic Polarisation Controller, POL: Polariser, IM: Intensity Modulator, BS: Beam Splitter, PM: Phase Modulator, black triangles: RF amplifiers, VOA: Variable Optical Attenuator, AWG: Arbitrary Waveform Generator.

we ensure to work in the linear regime of the PMs driving electronics, while still achieving a phase modulation that covers the whole $[0, 2\pi)$ range. Each PM is driven by a 8-bit DAC, and with two cascaded ones we are able to encode 512 different phase values over the 2π phase range.

- The PMs are followed by a VOA and a 99:1 BS. The strong output of the BS is sent to the second port of a monitoring power meter. The VOA and the power meter are used to set and monitor the photon flux at the output of the Encoder box. The photon flux is constantly adjusted to the correct value through an automatic control loop that set the VOA so as to have the desired optical output.

- The final component in the Encoder box is an EPC which is used to control the polarisation of the encoded pulses as they enter the quantum channel.

Inside the 'Electronics' box in fig. 5.1 are placed the electronic elements needed to drive the modulators in the encoder box. The five black triangles in this box represent high bandwidth RF amplifiers, which are needed to drive the PMs and the IMs with the right electrical signal. The white board in the middle of the electronics box represents a custom-built Printed Circuit Board (PCB) that provides the DC signals to drive the two EPCs and to set the appropriate DC offset to the IMs in the encoder box. Finally, the last element in the encoder box is a power meter, used to monitor the optical signal modulated by the encoder box.

The final elements constituting the transmitters, and represented at the bottom of fig. 5.1, are one AWG and a server. The former is characterised by a $12\,\mathrm{GSa\,s^{-1}}$ sampling rate and is used to generate all the RF patterns driving the fast optical modulators inside the encoder. The AWGs in the two transmitter units (Alice's and Bob's ones) are synchronised to each other through a common 10 MHz reference, and a triggering signal, provided by the central node (Charlie), initiates pattern generation. The server is used to monitor and control the functioning of all the electronic elements composing the modulators.

5.2 Design of the Improved Receiver for TF-QKD

The other part of the proof-of-principle TF-QKD setup (fig. 4.5) that needed improvement to allow operation with long quantum channels was the receiver module. The two main features that needed to be added to the system are: an effective way to

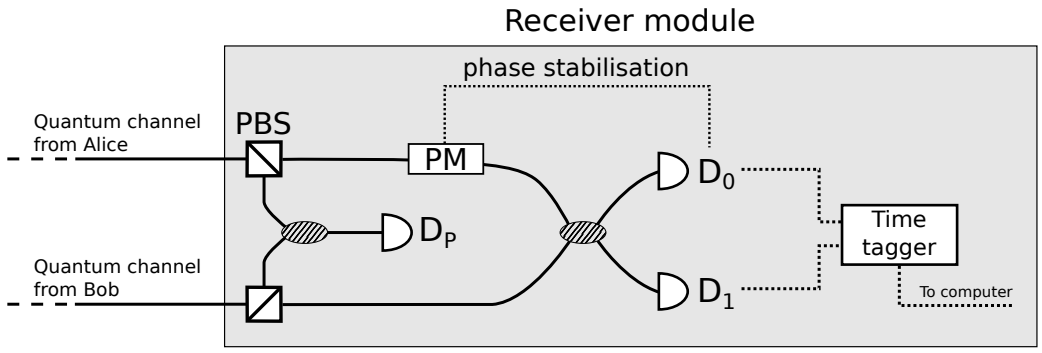

Figure 5.2: Diagram of the improved receiver module for TF-QKD. Signals from the transmitter units (Alice and Bob) enter the receiver module from the left after travelling through the quantum channel. Two PBSs together with a SNSPD (D_P in figure) are used to detect the photons with vertical polarisation entering the receiver module. The horizontally polarised light interfere at the second BS, and the interference outcome is recorded by two SNSPDs and a time tagger. A PM in the upper arm of the transmitter is used to implement a phase feedback loop that removes the phase noise introduced by the long quantum channels.

provide the phase stabilisation directly at the interfering station and a way to monitor (and correct) the polarisation rotations occurring along the quantum channel. In the proof-of-principle experiment, the use of VOAs for simulating of the channel losses made these features non essential. In a system with a quantum channel made of short fibres, correcting the phase noise with one of the PMs at the transmitter is equivalent to correcting it at the receiver station. This, as argued at the beginning of this chapter, is no longer true for a system with long quantum channels. Similarly, a system with short fibres for the quantum channels is not subject to significant polarisation rotations over time. In that case the polarisation could be optimised at the beginning of the experiment and would remain stable throughout it. Again, this is no longer true for quantum channels made up of long fibres.

Figure 5.2 shows the diagram of the receiver module developed for the improved TF-QKD setup. In the diagram, the light coming from the transmitting users (Alice and Bob) enters the receiver module from the left after having travelled through the quantum channels. Once entered the module, these signals encounter two PBSs which send the horizontal and vertical polarisation components of light down two different paths. The two vertical components are combined together through a BS whose output is monitored by D_P, a SNSPD. The readouts of D_P are used together with the last two EPCs in the users' transmitter modules (fig. 5.1) to implement an

automatic polarisation control loop. The control loop is implemented in the following way: Charlie broadcasts the counts received at D_P over a public channel, and the users take turns in changing their EPCs settings with the aim of minimising the detections at D_P. This guarantees that the majority of the light coming from the users is horizontally polarised when the interference takes place at the second BS in the receiver module.

The phase stabilisation feedback is implemented at the receiver station by inserting a PM in one of the input ports of the interfering BS (upper arm in fig. 5.2). The logic of the phase feedback is the same as described in section 3.4.2 with the only difference that with long communication channels the phase stabilisation will have to be performed at much higher speeds to compensate for the faster phase noise introduced by the long fibres. Effectively improving the speed of the phase stabilisation feedback will be the main focus of chapter 6, and we will delay this discussion until then. For the time being, for the benefit of the discussion in the next section, we only mention that our solution to achieve fast phase stabilisation involves the use of two different optical wavelengths.

After the interfering BS the last elements in the receiver module are two SNSPDs (D_0 and D_1) and a time tagger. These are used to detect and record the outcome of the interference between the signals sent by the two users.

5.3 Synchronisation and Communication Scheme for a Three Node Quantum Network

After the construction of the transmitter and receiver modules, the last missing element for building a fully operational TF-QKD setup is the creation of a synchronisation and communication scheme between the three modules constituting the setup. With this purpose in mind, we designed and developed the communication scheme summarised in fig. 5.3. The first thing to notice here is that the communication network has a centralised structure, with Charlie's module placed in the middle and in direct communication with the transmitting users, while Alice and Bob are not in direct communication with each others. The second thing to notice is that all the communications between the modules occurs through two optical fibres dubbed 'classical fibre' and 'quantum fibre', and that each fibre carries a collection of signals. This is possible thanks to the wavelength-division multiplexing of different optical carriers into the same fibre (see section 3.1.4 or refs. [171, 172]).

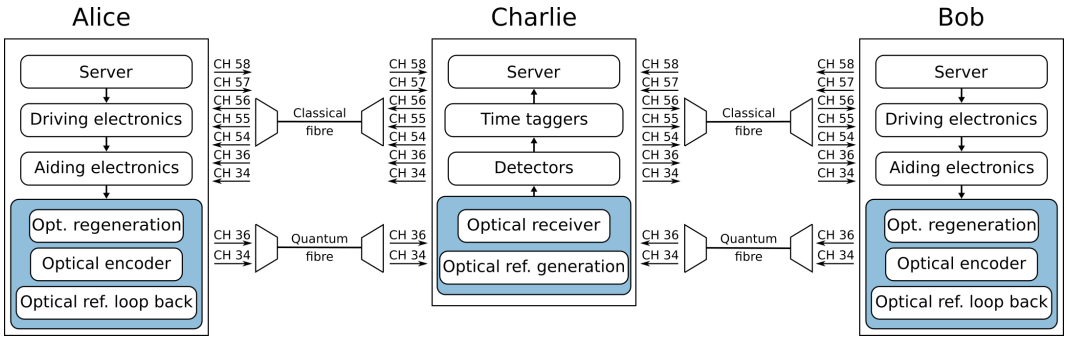

Figure 5.3: Schematic of the network layout for the three nodes TF-QKD network. The network has a centralised topology with Charlie in the middle and Alice and Bob not connected with each others. The sub-elements inside each node (Alice, Bob and Charlie) are grouped into electronic components (white background) and optical components (light blue background). Adjacent nodes are connected with two fibres: a 'classical fibre' which is used for setting up a classical communication channel, synchronisation purposes, and optical frequency distribution, and a 'quantum fibre' used for the exchange of optical signals needed for the protocol execution. The labels on top of the small arrows indicating signals distribution are the ITU channel [170] used for the transmission of the signal. Trapezoid shapes: Dense Wavelength division Multiplexers/Demultiplexers.

The three network nodes in fig. 5.3 contains different sub elements some of which we have already encountered in this chapter. Starting from the transmitter nodes (Alice and Bob), the sub elements with a white background (server, driving electronics and aiding electronics) are the ones shown at the bottom of fig. 5.1: server, AWG and encoder box. The elements with a light blue background in the transmitter nodes are those related to the encoding of the signal used for the protocol execution. Among these, the only one that we have already encountered is the 'optical encoder', that is encoder box in fig. 5.1. The remaining two sub elements, 'opt. regeneration' and 'Optical ref. loop back' will be introduced in chapter 6.

Also the sub-elements inside Charlie's node are divided into two groups. The electronic components are in a white background, and are used to monitor the interference outcome ('detectors' and 'time taggers') and control the coordinate the protocol execution ('server'). The optical components are the ones with a light blue background and consist of an 'optical receiver' (the module presented in section 5.2), and of an 'optical ref. generation' unit, which will be introduced in 6.

Figure 5.3 shows what signals are transmitted through the classical and quantum fibres and their direction of travel. The different signals are labelled by their ITU

Signals transmitted through the quantum fibre			
ITU channel	**Wavelength (nm)**	**Purpose**	**Signal direction**
CH 33	1550.92	—	—
CH 34	1550.12	Reference signal	Uplink
CH 35	1549.32	—	—
CH 36	1548.51	Quantum signal	Uplink
CH 37	1547.72	—	—

Table 5.1: Summary of the properties and purpose of the optical signals transmitted on the quantum fibre.

grid [170] transmission channel.

Quantum Fibre

The quantum fibre carries only two signals travelling unidirectionally from the transmitters to the receiver modules. From now on this configuration will be referred to as the uplink configuration. The properties of these signal alongside their purpose is summarised in table 5.1. These two signals are the ones used for the execution of the TF-QKD protocol. The 'quantum signal' (in table 5.1) is the one carrying the protocol encoded optical pulses. The 'reference signal' is a signal instrumental for the phase stabilisation process that will be described in chapter 6.

Classical Fibre

The classical fibre carries signals travelling both from the transmitters to the receiver (uplink configuration) and from the receiver to the transmitters (downlink configuration). Table 5.2 offers a breakdown of all the signals transmitted through the classical fibre, with a summary of the properties and purpose of each of them. The first two signals in table 5.2 are at the same wavelengths of those sent through the quantum fibre, but in this case they are transmitted in downlink configuration. The idea here is that these signals are generated at the central node, distributed to the transmitters, where they are modulated accordingly to the TF-QKD protocol, and then relayed back to the central node where they interfere.

The purpose of the other signals is explained below:

CH 54 - trigger signal sent from Charlie to Alice and Bob to initiate the transmission

Signals transmitted through the classical fibre			
ITU channel	**Wavelength (nm)**	**Purpose**	**Signal direction**
CH 33	1550.92	—	—
CH 34	1550.12	Reference signal	Downlink
CH 35	1549.32	—	—
CH 36	1548.51	Quantum signal	Downlink
CH 37	1547.72	—	—
—	—	—	—
CH 53	1535.04	—	—
CH 54	1534.25	Trigger	Downlink
CH 55	1533.47	10 MHz ref	Downlink
CH 56	1532.68	Ethernet down-link	Downlink
CH 57	1531.90	Pseudo-random pattern	Uplink
CH 58	1531.12	Ethernet up-link	Uplink
CH 59	1530.33	—	—

Table 5.2: Summary of the properties and purpose of the optical signals transmitted on the classical fibre.

of the encoded pulses.

CH 55 - 10 MHz reference signal transferred from the central node to the transmitting node to establish a common clock among the electronic instruments composing the setup.

CH 56 & 58 - down and uplink components of an optical ethernet connection used to establish a common local network among the three nodes. The local network allow classical communication among the nodes via TCP/IP protocol.

CH 57 - pseudorandom pattern sent from transmitters to the receiver to aid Charlie in establishing a common timebase among the three nodes.

Figure 5.4 shows a more detailed representation of the routing of the signals over the classical fibre. The figure illustrates in greater detail the multiplexing and demultiplexing strategy adopted to transmit the signals and indicates the position of the EDFAs in the setup to amplify the optical signals.

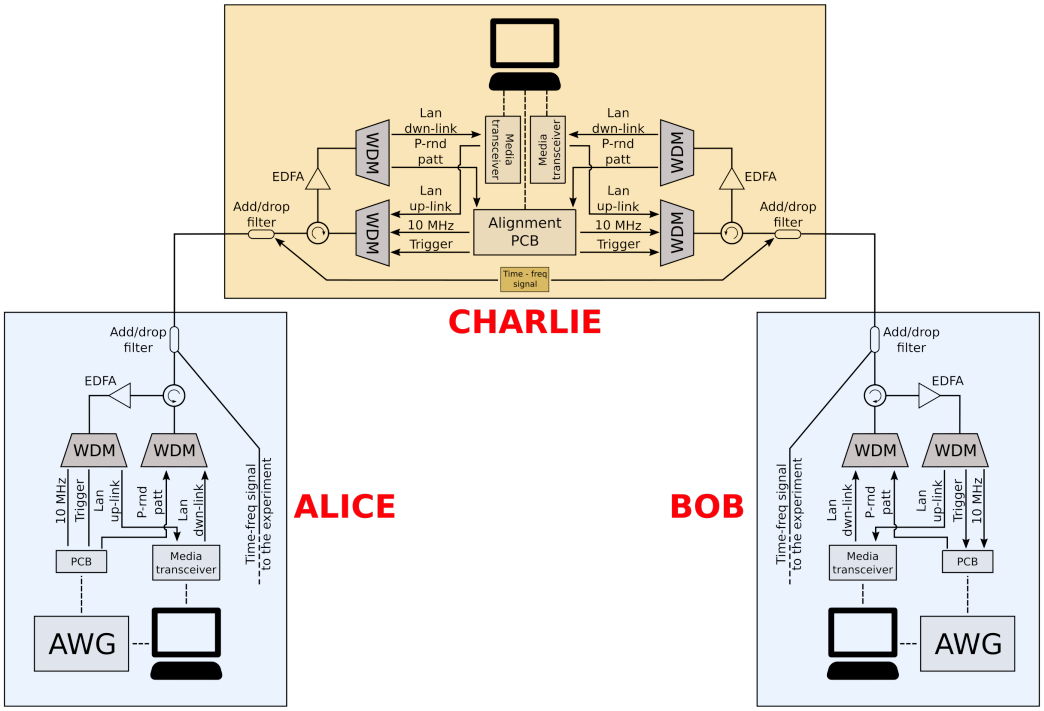

Figure 5.4: Routing of signals on the classical fibre. The only fibre represented in figure is the quantum fibre. WDM: Wavelength-Division Multiplexer, EDFA: Erbium-Doped Fibre Amplifier, PCB: Printed Circuit Board, AWG: Arbitrary Waveform Generator.

	Percentage in pattern	Photon flux (ph/pulse)
u	33.3%	0.35
v	33.3%	0.035
w	33.3%	0.0002

Table 5.3: Parameters of the pattern used for testing the new transmitter and receiver modules.

5.4 Testing of Improved Setup Over Short Distance

The first thing we did after building the transmitter and receiver modules (as described in sections 5.1 and 5.2) and setting up the communication channels (as described in section 5.3) was to test them in a simplified operational scenario. The main aspects under test were the quality of the encoding of the new modules and our ability to control them effectively. For this purpose, we used the new modules to implement a TF-QKD system similar the one shown in fig. 4.5, with the only difference that in this case a single laser was used to seed both the encoder boxes (i.e., no OPLL for seed regeneration).

For this test we prepared a 25 040 pulse long pseudo-random pattern for both Alice and Bob, composed in equal parts by pulses with three different intensities (u, v, w). The pattern composition and the photon fluxes used are summarised in table 5.3. We then introduced 15 dB of optical attenuation on the channel connecting each transmitter to the receiver, and we let interfere the patterns prepared by the users. After stabilising the phase of the system with the same strategy described in section 3.4.2, we recorded the interference of the pulses and we monitored the stability of the intensity modulation of the system and its QBER.

Figure 5.5 shows a characterisation of the intensity modulation with the new transmitters. In this figure, each point represents the measurement of the v/u pulses intensity ratio averaged over 500 000 consecutive patterns for both Alice and Bob recorded by both the D_0 and D_1 detectors. All points in the graph cluster around 0.1, which is the expected ratio between the v and u photon fluxes encoded as per table 5.3. The other element emerging form fig. 5.5 is that the intensity modulation provided by the encoders is stable over time.

Figure 5.6 shows the QBER for the u and v pulses obtained with the new transmitters and receiver. The QBER is calculated in post-processing by analysing

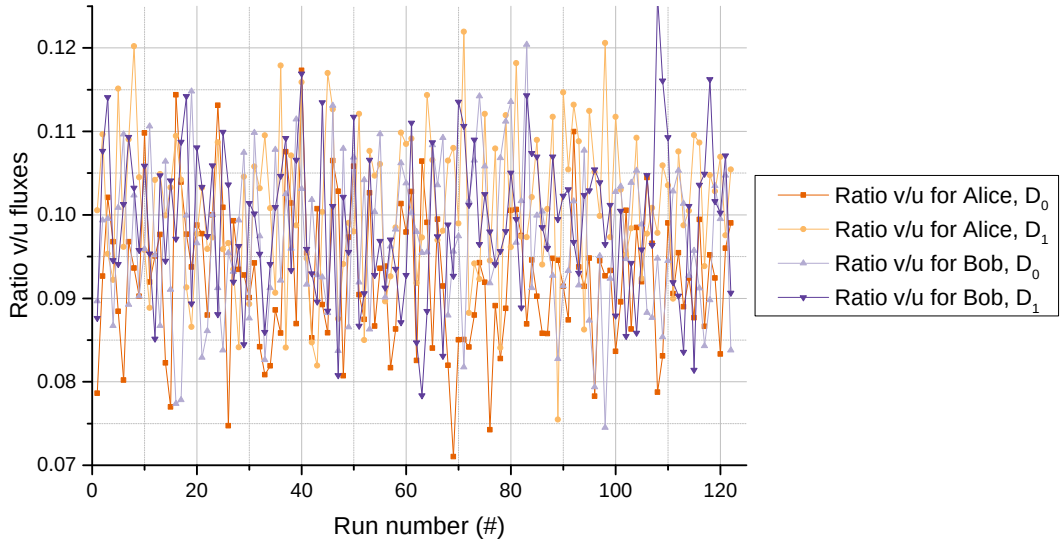

Figure 5.5: Intensity ratio between the v and u pulses generated with the new encoders. Each point in the graph (run) represents the average of the quantity of interest over 500 000 consecutive 25 040 pulses long pseudo-random patterns.

the interference outcome of only the pulses having the same intensity and satisfying a phase matching condition (that the phases of the interfering pulses differ at most by $1/16$ of 2π). The average QBER for the u pulses for both D_0 and D_1 is 1.5%, which is the baseline optical misalignment (as defined in section 4.2.1) of the new system. This is a good result that, despite the higher complexity of the new setup featuring three IMs and one PM more and using a pseudo-random pattern with different pulse intensities, improves over the results obtained with the proof-of-principle setup. The average QBER for the v pulses for D_0 (D_1) is 2.9% (3.0%). These values are higher than those for the u pulses due to the greater contribution played in this measurement by the dark counts of the detectors. Both QBERs (for u and v pulses) are stable over time.

5.5 Discussion

In this chapter we described in detail the improvements made to the TF-QKD setup that we started building for the proof-of-principle experiments described in chapter 4. With the upgrades made to the transmitter and receiver modules, we developed a system capable of addressing the technical challenges introduced by long communication channels (fast phase noise, synchronisation of the modules and

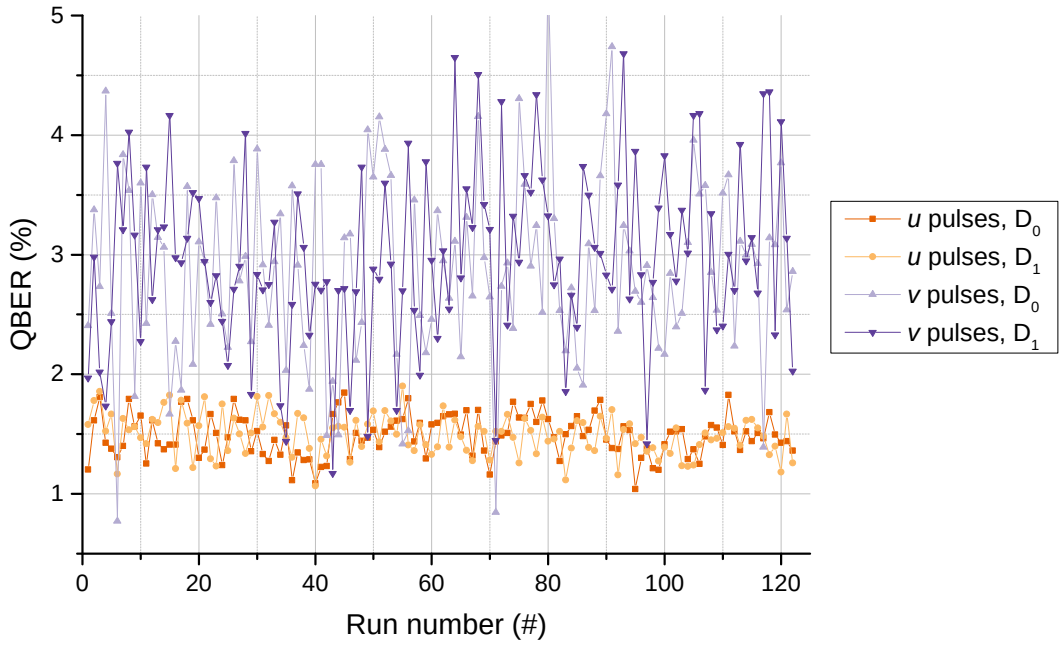

Figure 5.6: QBER of the u and v pulses recorded by detectors D_0 and D_1 with a TF-QKD setup with short optical fibres for quantum channel and featuring the new transmitter (section 5.1) and receiver (section 5.2) modules. Each point in the graph (run) represents the average of the quantity of interest over 500 000 consecutive 25 040 pulses long pseudo-random patterns.

optical frequencies distribution).

Preliminary tests with the new setup confirmed its flexibility and low-error operation. The improvements described in this chapter have been instrumental to obtain the results described in the next, and final, experimental chapter.

Chapter 6

TF-QKD over 600 km of Optical Fibre

6.1 Experiment Motivation

With the proof-of-principle experiment presented in chapter 4 we realised the first implementation of the TF-QKD protocol, demonstrating its in-principle feasibility and repeater-like behaviour. In that experiment the transmission losses associated with the quantum channel were simulated through VOAs, and the frequency dissemination between the two users was realised only over a short distance (tens of meters). These two solutions simplified considerably the experimental implementation of the protocol, by leaving to a later moment the complex task of dealing with the rapid phase noise introduced by a long quantum channel, and the one of distributing a frequency reference over long distances.

To demonstrate the feasibility of the protocol in a real world scenario, we need to address also these two remaining issues. This chapter will describe the development of a TF-QKD system capable of distributing secret encryption keys over long fibre spools. The results presented in this chapter[1] have been published in [123].

[1] This experiment was executed in collaboration with Mariella Minder. I designed, built and tested the experimental setup. I developed the code used to control the experiment and analyse the data. I collected and analysed all the data presented in this chapter and its appendix.

6.2 Experimental Setup

Before presenting the full system used for this experiment, we will analyse separately our solutions for the stabilisation of a long communication channel (section 6.2.1), and for the frequency dissemination over long distances (section 6.2.2). In section 6.2.3 we will describe the final setup used for the experiment.

6.2.1 Dual-Band Phase Stabilisation

As explained in chapter 2, for a successful execution of TF-QKD it is necessary to know the optical phase relationship between all (or some of[1]) the pulses interfering at the measurement station. Experimentally, the phase of an optical field is a delicate physical property. In section 2.4, we reported a phase noise measurement executed on a 550 km symmetric three-node optical fibre link. Over that distance, the spontaneous phase drift took values between $-20 \times 10^3\,\mathrm{rad\,s^{-1}}$ to $20 \times 10^3\,\mathrm{rad\,s^{-1}}$. Since the main advantages of TF-QKD over other QKD protocols emerge at long distances, rapidly evolving phase noise is an unavoidable technical challenge to solve in real-world implementations of the protocol.

So far, three different approaches have been tested [122, 173–178] to phase reference the interfering pulses after these travelled through long optical channels:

1. **Adopting an experimental layout that removes the phase noise:** in this approach the experimental layout is specifically designed to reduce the phase noise introduced by the communication channel to a negligible level.

2. **Passive phase stabilisation:** in this approach the phase misalignment between the two users is continuously monitored at the central node, and it is taken into account during the postprocessing phase of the protocol.

3. **Active phase stabilisation:** in this approach the phase misalignment between the two users is constantly corrected, by locking it, for example, to a fixed value.

Solution #1, adopted in refs. [173, 174], works for TF-QKD setups where the encoding users are placed along the loop of a Sagnac interferometer [179]. The specific layout required by this approach reduces the possible use-cases to very specific network configurations, and so far the solution has been proved effective only

[1] Depending on the protocol variant

over short distances (max. 17 km [173]). At the moment it is still unknown whether this approach could work over long distances.

Solution #2 was adopted in [175–177]. Since this approach does not require components executing the active phase stabilisation, the associated experimental setups are slightly simpler than the ones adopting the solution #3. A more sophisticated post-processing than in #3 is needed though, as in this approach it is necessary to estimate the relative phase difference between the interfering pulses at every instant. This information is generally retrieved by analysing the interference of some bright reference pulses travelling alongside the encoded pulses. Once the instantaneous phase difference is determined, the detected encoded pulses are divided into groups where the users' phase difference is roughly the same. Each group is then analysed separately, taking into account the specific phase offset.

Solution #3, adopted by us in a simplified scenario (see chapter 4 and [122]), and by [178] in a more realistic scenario (with the communication channel consisting of long fibre spools), works by locking the global phase offset between the two users to a constant value over time. In this case, the post processing is relatively simple, since it is not necessary to track over time the evolution of the phase difference between Alice and Bob. Systems using this solution require fast closed-loop cycles capable of cancelling the fast phase drift introduced by long communication channels.

Through approaches #2 and #3, remarkable results have been achieved in recently published works. In [122] we have been the first reporting the overcoming of the SKC_0 bound. In [178] the authors overcame for the first time the relative SKC_0 bound over a communication channel constituted of long optical fibres. While the implementations presented in [176, 177], represent the longest QKD communications over optical fibres to date, reaching 502 km and 509 km respectively.

Independently of the specific solution adopted (#2 or #3), in all the long distance TF-QKD experiments cited so far [175–178], the information about the users' phase offset was retrieved from the interference of some reference pulses sent together with the encoded pulses. These reference pulses are brighter than the protocol encoded pulses and they are all time multiplexed over the same optical wavelength. Given that for an effective phase correction a minimum receiving power needs to be guaranteed at the measurement node, the longer the fibres used during the experiment, the brighter the reference pulses have to be. The requirement for an high intensity contrast between the reference and the encoded pulses, ultimately limits the maximum distance and SKR achievable with this strategy. Time multiplexing

alone in fact:

- Inevitably introduces a source of noise for the encoded signal in the form of double Rayleigh scattering, which fundamentally limits the maximum distance achievable with this approach (see [177]).
- Requires the intensity contrast over the same wavelength to increase with the communication distance. Generating such contrast is practically challenging, especially because the intensity of the dim pulses needs to be set precisely.
- Reduces the clock rate of the encoded pulses, thus reducing the achievable SKR.
- Requires the allocation of some time to the recovery of Charlie's detectors, after these have received the bright reference pulses, which again reduces the achievable SKR.

All these factors combined together inhibit the performance of the TF-QKD protocol, preventing the realisation of its full potential.

To overcome these problems, we devised a novel dual-band phase stabilisation strategy that allows the generation of a strong intensity contrast between reference and encoded signals, while preventing at the same time the contamination of the latter. The dual-band stabilisation technique was introduced and discussed in detail in section 3.4.3.

6.2.2 Frequency Distribution over Long Distance

The second challenging aspect related to the TF-QKD implementation is the distribution of the optical frequency reference to the users executing the protocol encoding. In an ideal scenario, we could think of providing the users with two identical laser sources, with stable and ultra-narrow emission linewidth. This would be enough to allow the protocol execution. Practically though, ultra-narrow lasers are very expensive and all laser sources are characterised by a certain amount of frequency drifting. Optical frequency dissemination is in fact a major area of research on its own [180–182].

To solve this issue, one could equip each encoding node of a TF-QKD network with a stable optical reference (to resemble a network such as in [183]). This approach would require one or more ultra-stable optical references [184], a mechanism

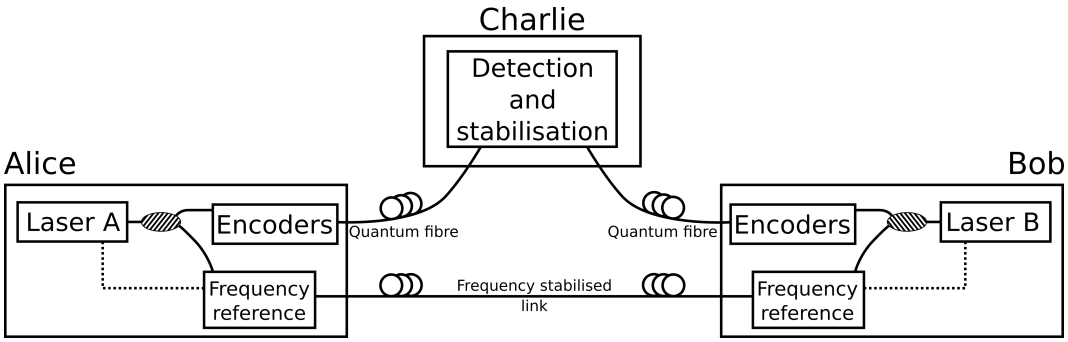

Figure 6.1: Schematic of a TF-QKD setup employing frequency references and frequency stabilised link for frequency dissemination.

to lock the laser sources to it [185, 186], phase stabilised links for the frequency dissemination [187, 188], and optical repeaters. This is the approach taken for the TF-QKD implementation presented in ref. [177]. In this work the authors built a full-fledged frequency dissemination network between Alice and Bob, having the structure presented in fig. 6.1. This solution lead to excellent results (TF-QKD over 509 km of optical fibre), but its experimental realisation is rather complex and difficult to replicate. It is hard to imagine that this approach could be widely adopted for practical TF-QKD implementations.

One of the aims of our work was to propose a simpler and more replicable solution to the frequency dissemination problem. The main idea behind our approach is that for TF-QKD to work, it is not necessary that the emission frequency of the laser sources is constant over time. The actual requirement for TF-QKD is that the users' encoded pulses that interfere at Charlie were encoded over optical fields of the same frequency. In other words, the emission frequency of the users' laser sources can vary over time, but it should be identical when they encode the pulses that are going to interfere.

Based on this observation, we developed a simpler frequency dissemination system suitable for TF-QKD, and compatible with the 2-stage stabilisation technique. In our scheme, the reference frequency(-ies) is generated in one node of the communication network, and then it is disseminated to the encoding users through a service fibre. The fact that during the frequency dissemination the classical (λ_B) and quantum (λ_Q) frequencies are distributed together, guarantees that the step-1 stabilisation of the dual-band stabilisation system (see section 3.4.3) will compensate also for the noise introduced by the dissemination fibres.

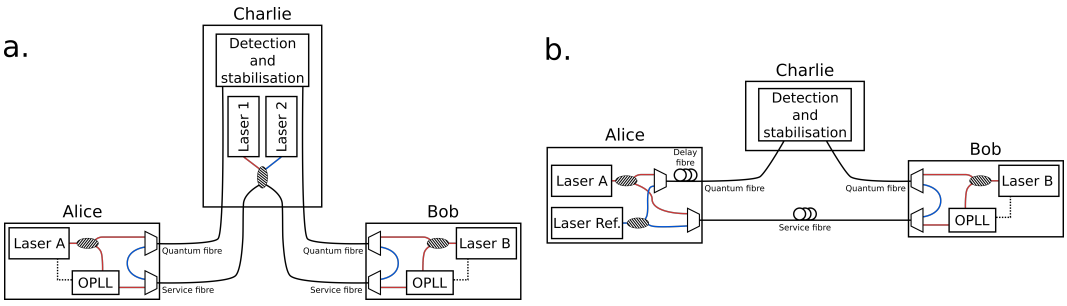

Figure 6.2: Red (blue) lines represent the fibres where λ_Q (λ_B) wavelength travels alone. Black lines represent the fibres where the λ_Q and λ_B travel together. **a.** Symmetric frequency dissemination technique employing two standard lasers and service fibres. Laser 1 (Laser 2) emits CW light at λ_Q (λ_B). When the classical and quantum signals reaches the users, the first will be looped back, while the second will be used to regenerate a local version of the quantum signal. **b.** Folded version of **a.** where the lasers sources are located in Alice's perimeter together with a delay fibre which is needed to satisfy eq. (6.1) by matching the fibres length difference with the coherence length of the lasers. Laser A (Laser Ref.) emits CW light at λ_Q (λ_B).

The dissemination should take into account the finite coherence length of the employed laser source. For this reason, the length mismatch of the service fibres should satisfy the following relation:

$$\Delta L_{Serv.} \lesssim \frac{1}{10} L_{coh}, \tag{6.1}$$

where $\Delta L_{Serv.}$ is the length mismatch of the fibres used for frequency distribution, and L_{coh} is the coherence length of the laser source. Two representations of this frequency dissemination strategy are given in fig. 6.2. Panel **a** of fig. 6.2 shows the symmetric version of this approach, where the frequencies are distributed from the central node (Charlie) to the users executing the protocol encoding (Alice and Bob). Panel **b** shows an asymmetric version of the same distribution strategy where the frequencies are distributed from Alice to Bob. This configuration can be seen as a folded version of the schematic in panel **a**.

In our experiments we tested both the frequency disseminations layouts. We started by testing the configuration fig. 6.2**.b** with a 50 km long servo fibre. We then implemented the configuration in fig. 6.2**.a** for the final experiment a with 600 km long servo fibre.

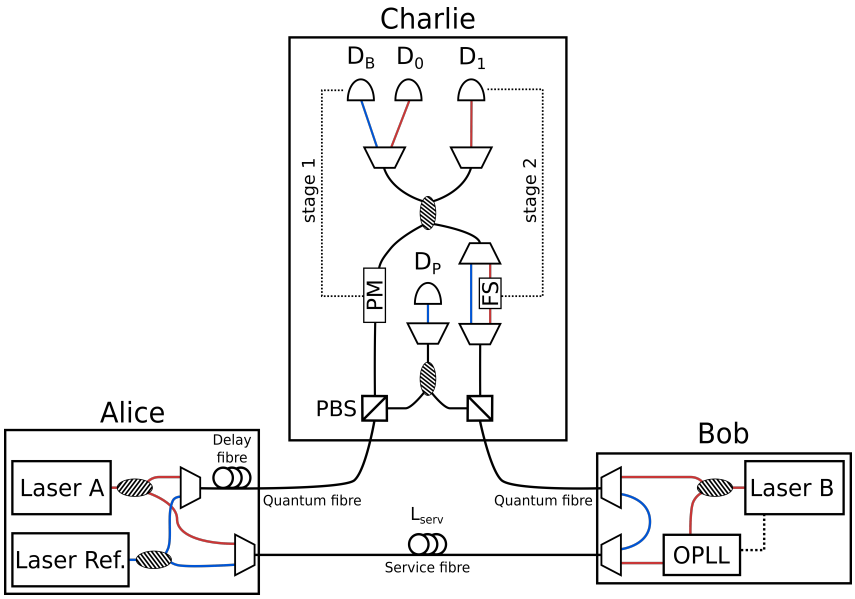

Figure 6.3: Setup used to test the frequency dissemination strategy with an asymmetric layout. In the asymmetric configuration, the primary laser sources are located in Alice and distributed to Bob through a service fibre connecting the two transmitting users. In this test the *Quantum fibre* is only a few meters long, while the *Service* and *Delay Fibre* are both $\sim$ 50 km long.

Frequency Dissemination Test - Asymmetric Layout

In this section we discuss the preliminary characterisation of our frequency dissemination strategies. We started by testing the one for the asymmetric layout in fig. 6.2**.b** with the setup shown in fig. 6.3. Here, *Laser Ref* and *Laser A* are placed in Alice and are used to generate the frequency λ_B=1548.51 nm and λ_Q=1550.12 nm respectively. Their output is split in two. Half of the generated signals are multiplexed via a Dense Wavelength Division Multiplexer/Multiplexing (DWDM) and sent to Bob through a service fibre of length L_{serv}. The second half of *Laser Ref* and *Laser A* outputs are used to generate Alice's own signals. For the purpose of this test, no modulation is applied to any of them.

In order to satisfy the condition presented in eq. (6.1), a *Delay fibre* with roughly the same length of L_{serv} is placed inside Alice and is used to delay her optical signals. In this test, L_{serv} = 50 km. We choose this distance to prove that by appropriately delaying the optical signals it is possible to disseminate the optical frequencies at distances much longer than the coherence length of the lasers used in the experiment. *Laser Ref* and *Laser A* have an optical linewidth of $\Delta\nu$ =150 kHz and $\Delta\nu$ =50 kHz

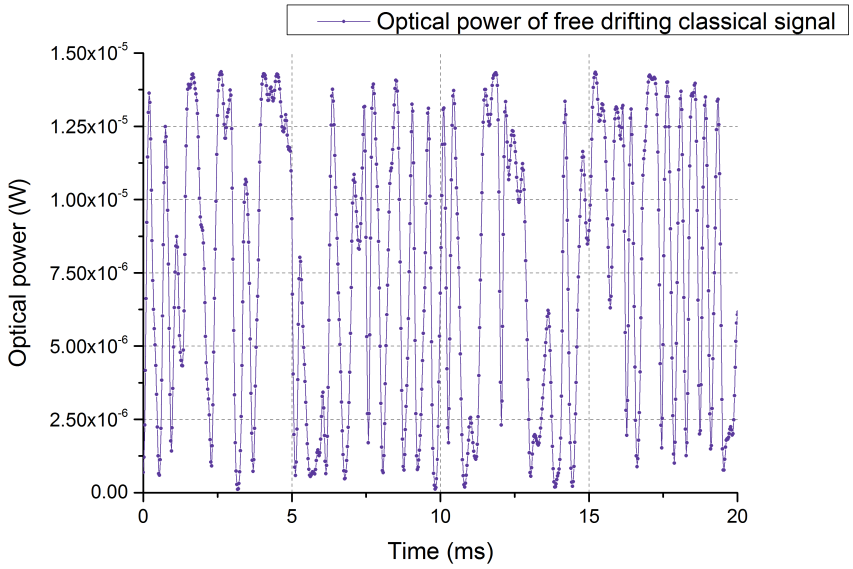

Figure 6.4: Free drifting optical interference of Alice's and Bob's λ_B signals measured with the setup in fig. 6.3. The optical interference visibility in this measurement amounts to 99.85 %. This measurement was acquired with a power meter with 25 µs integration time.

respectively. Without the delay fibre the physical separation between Alice and Bob would be limited to a couple of hundreds of meters, the order of magnitude of the coherence length of *Laser Ref.*

After the generation, the multiplexing, and the delay of her signals, Alice sends them to Charlie. Bob treats differently the λ_B and λ_Q signals received from the service fibre. After de-multiplexing them, he locks his own laser source *Laser B* to the λ_Q wavelength received from Alice. He then multiplexes the locally generated λ_Q signal to the λ_B signal received by Alice, and sends them to Charlie.

In this test, the encoding users are separated from Charlie only by short quantum channel, constituted by a fibre that is just tens of metres long. This allows us to test only the frequency transfer and regeneration, without having to consider effects associated to a long quantum channel. We tested our setup by first measuring the visibility of the free drifting optical interference between the λ_B signals sent by the two users to the central node. The measurement outcome is shown in fig. 6.4. The recorded visibility amounts to 99.85 %, which proves that the presence of the delay fibre in Alice allows to achieve a very good coherence between the λ_B signals.

We then tested the interference visibility between the λ_Q signals after activating the stage-1 of the dual-band stabilisation system (see section 3.4.3). The outcome of

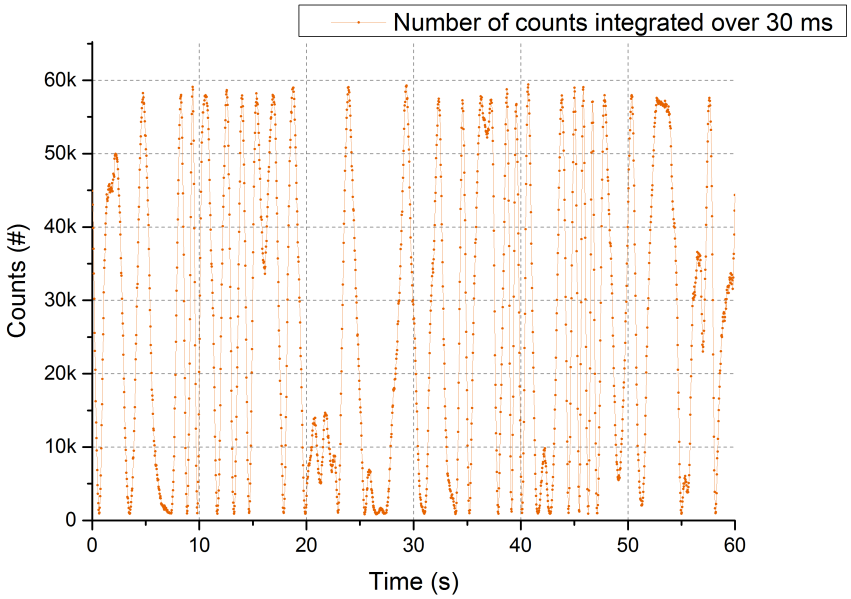

Figure 6.5: Optical interference of Alice's and Bob's quantum signals (λ_Q) measured with the setup in fig. 6.3. In this measurement, the stage-1 of the dual-band stabilisation system was activated so that only the residual phase drift on λ_Q was recorded. The optical interference visibility in this measurement amounts to 99.8 %.

this measurement is shown in fig. 6.5. From the graph it is possible to appreciate its effectiveness. The interference fringes now fluctuate on a time scale that is about 4 orders of magnitude smaller than the measurement reported in fig. 6.4. The recorded interference visibility in this case is 99.8 %. This measurement proves that also over λ_Q the frequency dissemination works correctly and that the frequency regeneration in Bob through an OPLL does not lead to a significant degradation of the quality of the optical interference .

Frequency Dissemination Test - Symmetric Layout

We also characterised the performance of the frequency dissemination executed with a symmetric layout by recording the visibility of the optical interference obtained with the setup shown in fig. 6.6. The main difference with the results presented in the previous section is that for this final test we used a more complex setup, which included two OPLL stations for frequency regeneration (one per transmitting user), long service and quantum fibres (each one of them 600 km long), and several EDFAs along the service channel for the amplification of the distributed optical signals. These results are shown in fig. 6.7. The data is presented in a similar manner to the

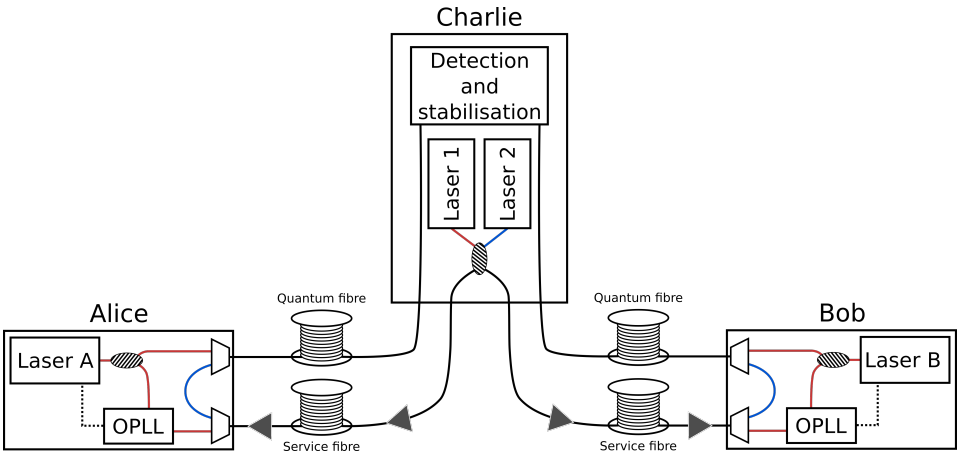

Figure 6.6: Setup to test frequency dissemination strategy with a symmetric layout. In the symmetric configuration the primary laser sources (*Laser 1* and *Laser 2*) are located at the central node (Charlie) and distributed to the transmitting nodes (Alice and Bob) through two servo fibres. This experiment uses long fibres (represented by the fibre spools in figure) between the users. Each channel is 300 km long for a total distance between Alice and Charlie of 600 km. The triangles inserted in the *service fibres* represents EDFAs.

one reported in fig. 3.12 in section 3.4.3.

The optical interference visibility for the fully stabilised λ_Q signal is 96.2 %. This high visibility value is a good starting condition for the protocol encoding which should allow TF-QKD operation with low QBER. It is also a confirmation that the two solutions adopted for frequency dissemination and phase stabilisation (the dual-band stabilisation technique) works well together and can stand phase drifts introduced by extremely long optical channels (∼1200 km in this test), optical regeneration through OPLLs and optical amplification along the service fibre through the EDFAs.

6.2.3 Complete Experimental Setups

The complete experimental setups used for the final experiment are shown in figs. 6.8 and 6.9. They are composed of three modules: two for the transmitting users which are assumed to be trusted and one for Charlie which can be considered untrusted. The users send the encoded optical pulses to Charlie via the quantum channel, which is made of Corning SMF-28 ULL fibre spools. The spools are spliced into different sets, enabling experiments over 5 different communication distances, ranging from 153.2 km to 605.2 km. The average loss coefficient of the fibre channel, including

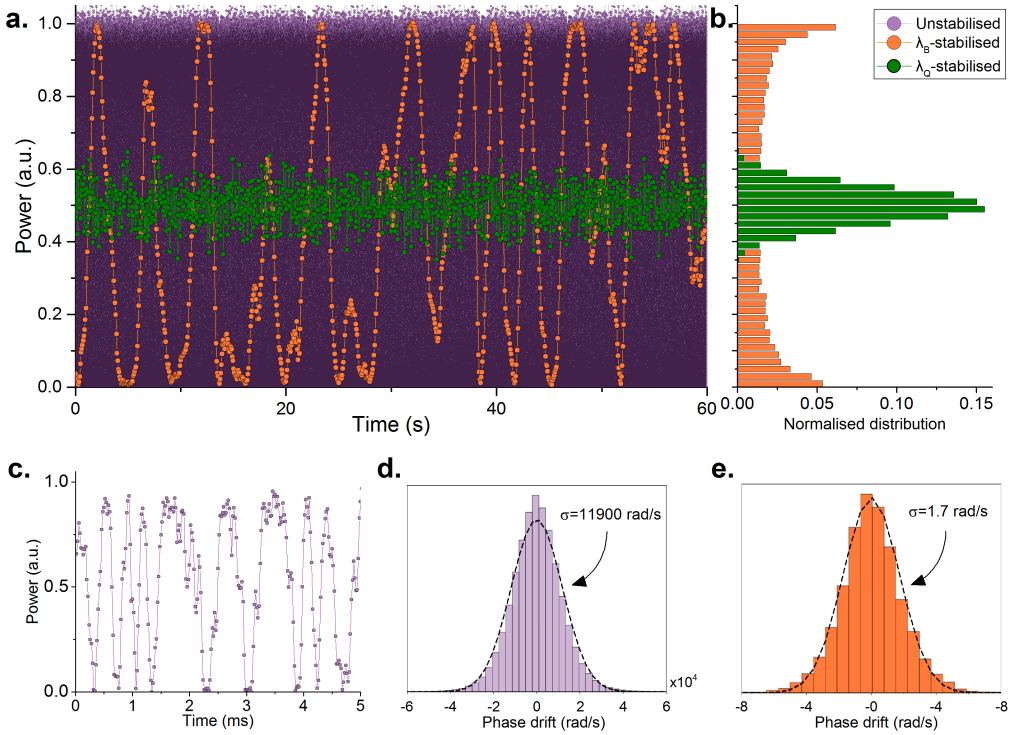

Figure 6.7: Data in this figure shows the interference of λ_Q light at different stabilisation stages. Data was acquired over 605 km quantum and 611 km servo fibres, with the configuration shown in fig. 6.6. The colour code is: purple for free drift, orange for λ_B-stabilised data and green for λ_Q-stabilised data. **a**, Comparison between the free drifting and stabilised data. Due to the different time scales of the fluctuations at the different stages, integration times were 20 µs for free drifting data and 60 ms for the stabilised data. An interference visibility measurement over the free drifting (λ_B-stabilised) data yields 98.2% (96.2%). **b**, Histograms of the intensities of the stabilised data in (a). The λ_B-stabilised data show the typical double peak distribution that characterises data set with uniform phase distribution. λ_Q-stabilised data take a gaussian a distribution with mean μ=1.56 rad and σ=0.10 rad. **c**, Same data set as in (a) but over a ms time scale, to appreciate the intensity fluctuations of the free drifting data. **d**, Histogram of the free drifting phase drift. The standard deviation is 11 900 rad s^{-1}. **e**, Histogram of the λ_B-stabilised phase drift. The standard deviation is 1.7 rad s^{-1}, i.e., about 6800 times smaller than in sub-figure (d).

splices and connectors, is 0.171 dB km^{-1}. For detailed information on the fibres used for the quantum channel refer to appendix B.1. The only difference between the setups shown in figs. 6.8 and 6.9 is the frequency dissemination strategy used in the two experiments. The former uses an asymmetric frequency dissemination layout and the two transmitting users are separated by 50 km of fibre, while the latter uses a symmetric frequency dissemination strategy and the users are separated by 600 km of fibre.

A description of the components inside the Encoder boxes was already given in section 5.1. In these experiment we operate them at 1 GHz repetition rate, and they are used to carve the λ_Q input signal into a train of 250 ps pulses with three possible intensity levels (u, v, w). The even-numbered pulses are further modulated in intensity and phase, according to the requirements of the specific TF-QKD protocol implemented. These pulses constitute the 'quantum signals' (Quantum Signal (QS)) introduced in section 3.4.3, and summarised in table 3.2. The odd-numbered pulses do not receive any further modulation and are used to track the phase drift of the quantum signals. These are the 'quantum reference' (Quantum Reference (QR)) from table 3.2. In this experiment the QR pulses have the same intensity of the brightest decoy pulses (u) encoded on the QS.

All pulses are attenuated to the single-photon level before entering the quantum channel. For a detailed description of the modulation executed by the encoder boxes, refer to appendix B.2.

After executing the encoding over the λ_Q wavelength, each user combines it with their λ_B signal. The users provide independent pre-compensation for polarisation rotations occurring along the quantum channel for both λ_Q and λ_B, so that all photons arrive with identical polarisation at Charlie's 50:50 BS.

The first components inside Charlie's setup are the ones needed for the polarisation optimisation. These consists of two PBSs, a BS and a SNSPD (S_P). To compensate for the polarisation rotation introduced by the quantum channels, the users tune their EPCs to minimise the counts recorded at S_P (as described in section 5.2). The following elements encountered by the users' signals are the components needed for stage-1 and stage-2 phase stabilisation (see section 3.4.3). After this, interference occur on a 50:50 BS. The interference output of the BS are separated by DWDM filters before detection by three SNSPDs: D_0 and D_1 for λ_Q photons and D_B for λ_B photons.

Table 6.1 reports a detailed characterisation of the experimental setup. This

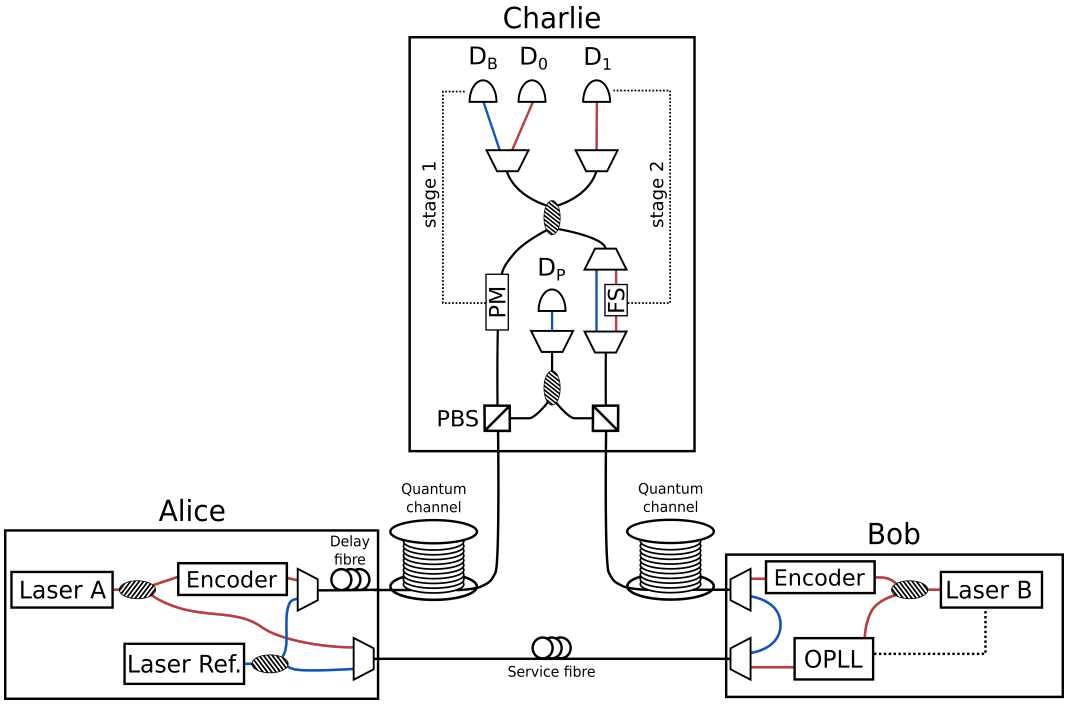

Figure 6.8: Alice and Bob generate λ_Q (red fibres in the schematic) using their local continuous-wave laser sources. A set of intensity and phase modulators inside each user's Encoder allow them to run different TF-QKD protocols. A second laser in Alice (Laser Ref.) generates the bright reference signal λ_B (blue fibres) used for fast phase correction. A service fibre of length L distributes Alice's λ_Q and λ_B signals to Bob. After locking his local laser to the λ_Q received by Alice through an OPLL, Bob multiplexes together the modulated quantum pulses with the received λ_B, and sends them to Charlie. After multiplexing her λ_Q and λ_B together, Alice delays them with a fibre spool of length L, and sends them to Charlie. At Charlie, a BS combines Alice's and Bob's signals, while the two-stage phase stabilisation system (step-1 using a PM and step-2 a FS as actuators) removes the phase noise introduced by the quantum channel. SNSPDs D_0 and D_1 record the interference output for λ_Q, while D_B records the one for λ_B.

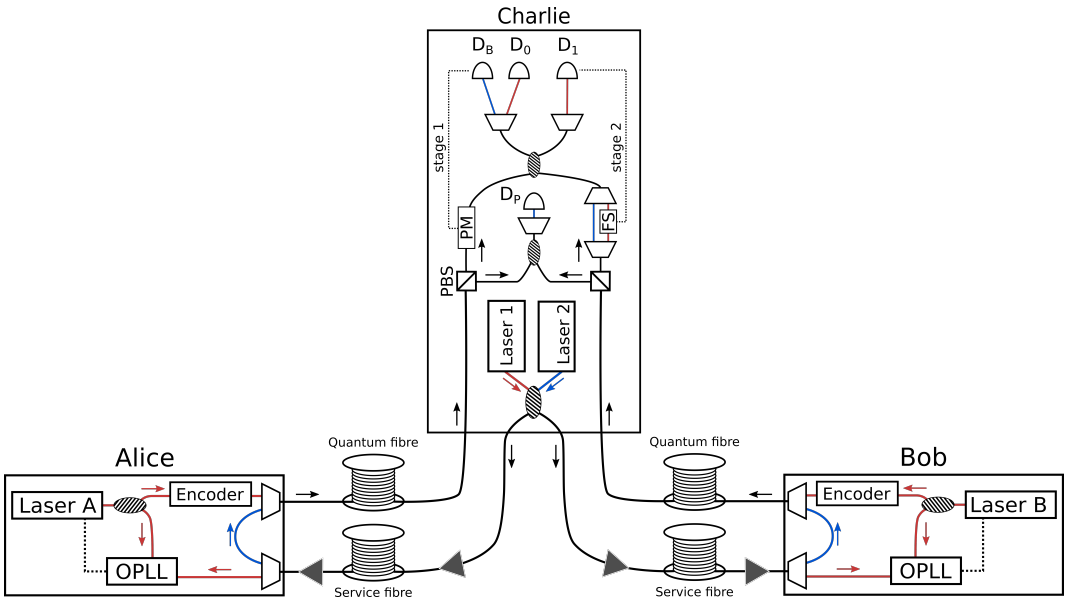

Figure 6.9: Setup identical to the one shown in fig. 6.8 with exception for the symmetric frequency dissemination strategy which was described in section 6.2.2.

table highlights an asymmetry between the users' insertion losses at Charlie. The asymmetry is related to the two different types of modulators acting on the incoming signals. A phase modulator is lossier than a fibre stretcher (which is almost lossless), and therefore Charlie's system transmission for Alice is lower than for Bob. In the protocol simulations, we used the lowest transmission figure to characterise the losses at the receiver. We exploited Bob's higher transmission coefficient to compensate for a small asymmetry in the quantum channels losses.

In table 6.1 we present two different dark counts figures. The first is derived from the SNSPDs (Single Quantum EOS 410 CS cooled at 2.9 K) characterisation, executed with no connected fibre. The second is extracted from the experimental data during protocol execution. We associate the increase in dark counts in the second case to environmental contaminations and to the scattering occurring in the fibres.

The presented setup is versatile as it is capable of implementing all of the kinds of TF-QKD variants proposed so far, including the phase-matching ones [119, 120, 189], which cannot be efficiently run with previously proposed passive phase compensation methods.

Charlie's system transmission (from Alice)	50.8%
Charlie's system transmission (from Bob)	62.9%
Efficiency SNSPD D_0	77%
Efficiency SNSPD D_1	73%
SNSPD dark counts (calibration)	10 Hz
SNSPD dark counts (experiment)	14 Hz
Clock rate for quantum signal	500 MHz

Table 6.1: Experimental parameters of the setup.

6.3 Protocols and Patterns

We perform four experiments with different TF-QKD protocols, varying the operational regimes and optimising the parameters in each case. Firstly, we perform the CAL [120] and SNS [121] protocols in the asymptotic regime. Then we implement SNS with the TWCC method [126], both in the asymptotic and in the finite-size regimes [190, 191]. More details about the implemented protocols can be found in section 2.3. In all protocols, we consider a symmetric situation, with identical photon fluxes for the users Alice and Bob. This is the real situation in the experiment, where fibre lengths and losses between the users and Charlie are nearly identical (see table B.1).

For all the measurements we used a 25040 pulses long pattern. Half of the pulses were used for the protocol encoding (QS), the other half were used as quantum references (QR). The pattern encoding was executed by two time-synchronised waveform generators, which controlled the phase and intensity modulators in the Encoders. For every protocol, the pattern properties have been chosen with the aim of maximising the communication distance. With the exception of the point at 604.8 km, the two versions of the TWCC SNS protocol (asymptotic and finite size) used the same pattern over the different tested distances.

The way we encode the patterns is by fair sampling. Using the pattern properties shown in table 6.2 and 6.3, for each protocol we calculate the probabilities of the different users' pulses combinations. At this point, we generate a 12520-element-long list of pulses pairs reflecting the matching probabilities. This list is then randomly shuffled, resulting in two patterns with a random pulse distribution that respects the matching probabilities expected by the protocol simulations.

Table 6.2 summarises the photon fluxes and the pattern probabilities used for

	CAL asympt.
Fibre length (km)	368.7
s (ph/pulse)	0.015
u (ph/pulse)	0.1
v (ph/pulse)	0.015
w (ph/pulse)	0.0002
P_Z (code basis)	50.0%
P_X (test basis)	50.0%
P_u	33.3%
P_v	33.3%
P_w	33.3%

Table 6.2: Secret key rate and parameters used for the implementation of the CAL TF-QKD protocol [120] in the asymptotic scenario. s is the photon flux used for signal pulses, while u, v, w are the photon fluxes used for the decoy states. P_Z is the users' probability of sending a pulse in the code basis. P_X is the users' probability of sending a pulse in the test basis, P_u, P_v, P_w are the probabilities of sending the u, v, w decoy pulses respectively.

the CAL TF-QKD protocol. In this protocol the $\mathcal{X}$ basis is the one used for coding, while the $\mathcal{Z}$ is used for testing (decoy states). Pulses in the $\mathcal{X}$ basis can only take two phase values: either $+\pi/2$ or $-\pi/2$. Their intensity is set to be equal to the one of the v decoy pulses. Pulses in the $\mathcal{Z}$ basis on the contrary are all phase randomised. Since this protocol has been run only in the asymptotic regime, for the purpose of the key rate estimation, calculations have been carried out by normalising P_X from the original 50% to 99.9%.

Table 6.3 summarises the parameters for the different configurations of the SNS TF-QKD protocol we tested. In the SNS protocol, the $\mathcal{Z}$ basis is the one used for the key generation (sending-or-not-sending), while the $\mathcal{X}$ basis is used for testing the quantum channel (decoy states). In this protocol, all the encoded pulses (QS) are phase randomised. Also for SNS, in the asymptotic case the key rate estimation was executed by normalising the probability of using the coding basis P_Z form 50% to 99.9%.

	SNS asympt.	TWCC SNS asympt.		SNS finite size
Fibre length (km)	368.7	all except 605	605	all
s (ph/pulse)	0.35	0.35	0.38	0.4
u (ph/pulse)	0.35	0.35	0.38	0.4
v (ph/pulse)	0.035	0.0105	0.01065	0.075
w (ph/pulse)	0.0002	0.0002	0.00023	0.0002
P_Z (code basis)	50.0%	50.0%		60.0%
P_s	5.8%	13.0%		7.5%
P_X (test basis)	50.0%	50.0%		40.0%
P_u	33.3%	33.3%		20.0%
P_v	33.3%	33.3%		60.0%
P_w	33.3%	33.3%		20.0%

Table 6.3: Parameters of the patterns used for the implementation of the SNS TF-QKD protocol [121] in different experimental scenarios (with or without TWCC [126, 190], in the asymptotic or finite-size regimes). s is the photon flux used for signal pulses, while u, v, w are the photon fluxes used for the decoy states. P_Z is the users' probability of choosing to encode a pulse in the code basis, P_s is the probability of actually sending a signal when the Z basis is chosen. P_X is the users' probability of encoding a pulse in the test basis, P_u, P_v, P_w are the probabilities of sending the u, v, w decoy pulses respectively.

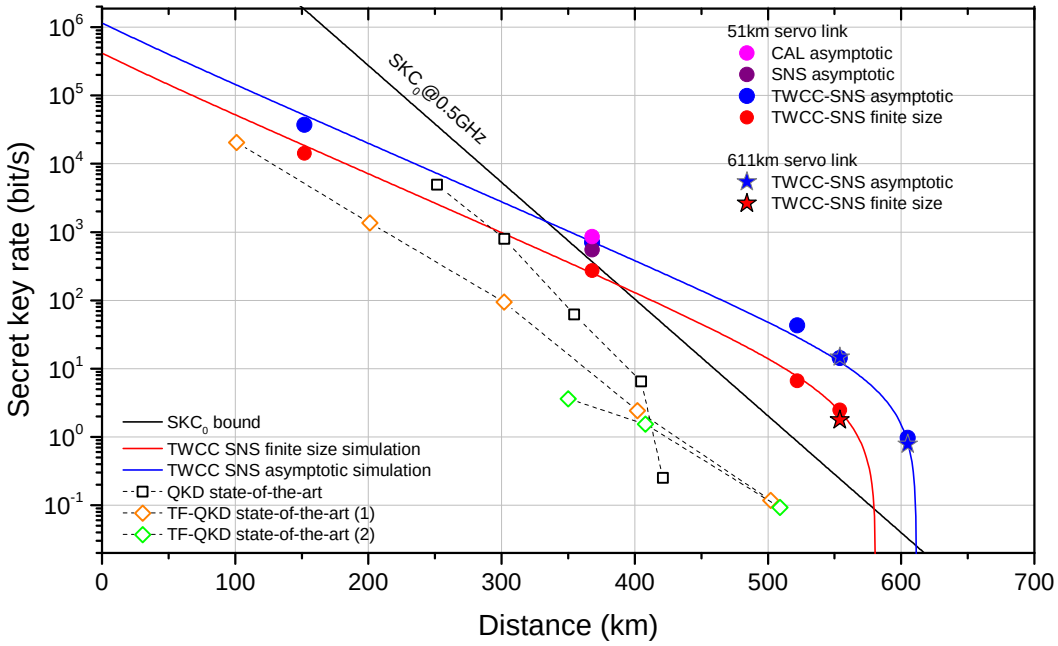

Figure 6.10: Secret key rates are plotted against the quantum channel length. This is constituted by ULL fibres of 0.171 dB km^{-1} loss. The SKC$_0$ bound for unitary detection efficiency (black line) is plotted along the simulations for the TWCC SNS TF-QKD protocol in the asymptotic and finite size regimes (blue and red curves respectively). Filled markers show the experimental results we obtained for the different protocols whereas unfilled markers are the state of the art results in term of SKR over long distance for fibre-based TF-QKD ((1):[176], (2):[177]) (diamonds) and QKD [107] (squares).

6.4 Results

In fig. 6.10 we report our results in terms of SKR versus distance obtained with both setups in figs. 6.8 and 6.9. Alongside the extracted SKRs we plot the simulation curves and the state-of-the-art SKRs for long-distance TF-QKD [176, 177] and QKD [107] over optical fibres. In the same graph we also plot the absolute SKC$_0$, which assumes ideal equipment for Alice and Bob and hence is the most difficult bound to overcome. Surpassing this limit proves the repeater-like behaviour of our setup. The complete experimental results are reported in appendix B.3.

The CAL and SNS protocols have been implemented on a 368.7 km-long optical fibre (62.8 dB loss) and analysed in the asymptotic scenario (pink and violet full circles in fig. 6.10, respectively). For CAL, we obtain an SKR of 853 bit s^{-1}, 2.39 times larger than SKC$_0$. For SNS, the SKR is 550 bit s^{-1}, 1.54 times larger than SKC$_0$.

In order to reach longer distances, we resort to TWCC SNS. We take measurements at 153.3, 368.7, 522.0, 555.2 and 605.2 km, i.e. from 26.5 dB to 104.8 dB loss, and we extract positive SKRs both in the asymptotic and in the finite-size regimes (blue and red points in fig. 6.10, respectively). Stars (circles) represent results obtained through the symmetric (asymmetric) setup with a 611 km (51 km) servo fibre. Despite periodic optical amplifications, the longer servo link introduces only a marginal reduction of the secret key rate. At a 555 km quantum channel and a 611 km servo link, with less than 2 h of continuous measurement, we are able to extract a finite-size SKR of 1.78 bit s^{-1}, a value 7.68 times higher than the absolute SKC_0. Extending the quantum channel to 605.2 km, with a loss budget of 104.8 dB, we achieve an asymptotic SKR of 0.78 bit s^{-1}, which is 24 times higher than the SKC_0.

To further appreciate the progress entailed by our new technique, we compare our results with the experimental points setting the current record distances for fibre-based QKD (421 km [107]) and TF-QKD (502 km [176], 509 km [177]).

6.5 Discussion

Distance-wise, there is an increase of tens of (more than a hundred) kilometres over the previous TF-QKD (QKD) state-of-the-art. The main element enabling the distance improvement over previous TF-QKD implementations is the dual-band stabilisation technique, which leads to negligible contamination of the encoded signal by the bright reference. In previous experiments, the bright stabilisation signal was emitted at the same wavelength as the encoded signal, thus causing an intense double Rayleigh backscattering that ultimately limited the maximum communication distance. In our case, on the other hand, even at the longest distance the noise introduced by the stabilisation signal was below the detectors' dark counts.

The dual-band stabilisation technique leads also to an even more pronounced enhancement of the SKR, with an improvement of 2 orders of magnitude at 500 km, the furthest distance achieved by previous state-of-the-art. This is possible because we could keep the clock rate of the encoded signals at the high value of 500 MHz at all distances. In previous experiments, where the stabilisation signal was time-multiplexed, the protocol clock rate had to be reduced considerably to accommodate for reference signals, and to leave some recovery time at the detectors (after these received the bright intensity reference pulses).

We have shown that dual-band phase stabilisation can dramatically reduce the phase fluctuations on optical fibre by almost four orders of magnitude. This has allowed us to overcome the fundamental noise limitation of long distance TF-QKD and increase its secret key rate from the current millibit per second range to the bit per second range for the longest fibre length. We notice here that $1\,\mathrm{bit\,s^{-1}}$ key generation rate is sufficient to enable fast key refresh of symmetric cryptographic protocols, such as the AES, several times per hour. Our setup tolerates a maximum loss beyond 100 dB allowing quantum communication over 600 km of fibre. We believe these techniques will have more general application in quantum communications, for example enabling DLCZ-type quantum repeaters [93], longer-baseline telescopes [192], quantum fingerprinting [193–195] over longer distances or a phase-based architecture for the quantum internet [38].

Part III

Final Remarks

Chapter 7

Conclusions

As discussed in chapter 1, QKD combined with One-Time-Pad encryption is currently the only information-theoretic secure method to protect the communication between two distant users (that do not already share a long encryption key) from eavesdropping by an unauthorised party. For this reason, QKD is a valuable resource for the exchange of highly confidential information between distant parties. The forward secrecy enabled by QKD is particularly appealing today due to the recent advances in the development of quantum computers ([15, 16]) which have the potential to compromise the foundations of the current public key encryption infrastructure. It can be argued, see [196], that for critical data requiring long-term secrecy it is already necessary to switch to post-quantum (and ideally QKD-based) cryptography. An encrypted message exchanged today could in fact be recorded by an adversary who in the future could decrypt it once the technology needed to do so will be available.

Over the past 30 years, QKD has developed from an interesting theoretical idea [23], to a theory backing a successful series of proof-of-principle experiments (that initially could exchange a secret key just over $\approx 30\,\mathrm{cm}$ [42]), and finally to a relatively mature technology that can be used over hundreds of kilometers of fibre [107], or even thousands of kilometers via satellite links [112]. Still, the limited distance at which this technology can be operated is one of its main constraints, which prevents its wide adoption and possibly further developments. This limitation is related to the unavoidable loss of the encoded quantum carriers along the communications channel.

Over the recent years, considerable efforts have been made to solve this problem. Most notably, the development of new theoretical tools for the security analysis of the

channel (the decoy state technique [70–72]), improvements to the specifications of the equipment used to establish QKD links (such as in ref. [107]), and the development of satellite based QKD [112–114]. However, none of these attempts succeeded in overcoming the intrinsic limitations of point-to-point quantum communications, a limit formally embodied by the repeaterless secret key capacity (SKC_0), or PLOB bound [84].

In order to overcome this limit (without using trusted nodes), it is necessary to implement an *effective* quantum repeater[1], a task that until very recently was believed to be out of reach with current technology. This belief was refuted in 2018 by the introduction of the TF-QKD protocol, which conjectured that by encoding information on the phase of optical fields that are then transmitted over a channel preserving their optical coherence, it would be possible to overcome the SKC_0 bound, and therefore reach unprecedented communication distance. However, despite its potential advantages, the experimental requirements of the TF-QKD protocol are so demanding that its proposal was accompanied by doubts on its experimental practicality and feasibility.

In our work, we provided the first experimental demonstration of the TF-QKD protocol, which was reported in chapter 4. To achieve this, we introduced new experimental techniques related to optical frequency regeneration and optical phase stabilisation to the field of quantum communications. These techniques were described in chapter 3. As result of our work, we realised the first quantum communications system overcoming the SKC_0, and therefore provided the first implementation of an *effective* quantum repeater [27]. Incidentally, we also note that in this experiment we were able to extract a positive key rate over a 90 dB loss link, which was about 20 dB larger than any previous quantum communications experiment at the time of our tests.

As a continuation of our first experiment, we then improved the experimental setup we developed for it. This was done to prepare a TF-QKD system capable of exchanging secret keys over long distances (and not just high channel attenuations) and capable of full pattern encoding. A discussion of the new design and its performance presented in chapter 5.

The final investigation presented in this thesis (chapter 6) was related to the realisation of the longest fibre-based quantum communications to date. To achieve this, we developed a new dual-band phase stabilisation system, described in chapter 3,

[1] A definition introduced by quantum information theory and discussed in section 1.4.3.

and applied to the system presented in chapter 5. The dual-band stabilisation system was instrumental in overcoming the limitations of the time-multiplexed phase stabilisation systems developed in previous long-distance TF-QKD experiments ([176, 177]). It allowed us to extend the maximum distance of fibre-based QKD by ≈100 km, to reach ≈605 km.

Chapter 8

Future Work

In this thesis we reported on the early developments of the TF-QKD protocol. From the theoretical point of view, we have discussed the characteristics of the original protocol (in chapter 1), and of its variants (in chapter 2). From the experimental point of view, we reported its first experimental proof-of-concept implementation (in chapter 4 and published in ref. [122]), and also the current longest fibre-based quantum communication which was obtained by implementing it (in chapter 6 and published in ref. [123]).

Our last experimental results, together with those of other research groups working on the implementation of the protocol [176, 177], highlighted the advantages that TF-QKD can offer to high-loss/long-distance quantum communications. However, there are still numerous aspects related to the protocol that require further study and development. These could be grouped in two broad categories: improving current TF-QKD systems, mainly in terms of their performance and practicality, and investigating what is beyond TF-QKD for quantum communications.

Current TF-QKD systems could be improved by a reduction in complexity. So far, for example, all the encoders used to implement the protocol are rather complex and feature several identical modulators arranged in line to execute a precise modulation. It would be interesting to evaluate whether this is a stringent requirement for the implementation of the protocol, or an excess of precautions of the early implementations. One could also investigate if direct phase and intensity modulation techniques applied to the laser diodes (which have already been proved effective for other QKD protocols [153–155]) could be successfully employed in TF-QKD systems. In general, all the improvements that reduce the amount of equipment and complexity of the setup (also at the receiver station), could simplify its deployment

in real-world scenarios.

The realisation of field trial experiments (as the ones recently reported in refs. [197, 198]) is another important direction of development for this technology. From our perspective, a first step would be testing the compatibility and performance of the dual-band stabilisation technique with field deployed fibres. Also it would be interesting to study if this stabilisation technique has some advantages (beyond the extension of the communication distance) over the time-multiplexed stabilisation in the context of real fibre networks.

To increase the practicality of TF-QKD, one could also investigate the feasibility of integrating its setup onto photonic circuits. Photonic circuits are an emerging and promising platform for optical communications in general and quantum communications in particular [199–202]. With their small size and scalable mass production aptitude, they could help reduce costs and accelerate QKD adoption.

Another interesting direction of study would be a detailed analysis of the security aspects of the protocol implementation. For example, it would be relevant to assess the security implications of different frequency regeneration techniques for TF-QKD, such as the possible side channel opened by OIL or OPLL. The result of this study would have a direct impact on the practicality of TF-QKD setups, as OIL is easier to implement than OPLL.

From a more practical standpoint, it would be useful to study precisely how TF-QKD fits in the landscape of other QKD protocols when considering realistic operating environments and use cases. This study could investigate the performance of the protocol when performed with standard Avalanche Photo-Diode (APD) detectors or in a configuration where the protocol is multiplexed with other signals over the communication channel. It would also be interesting to consider whether setup configurations using a single fibre instead of a pair of them are possible. The goal of these studies would be to identify the specific scenarios in which TF-QKD can offer unique advantages over other protocols. The challenges of implementing a field trial test will most likely be associated with controlling of the phase noise introduced by the environment, reducing the size and complexity of the setup and implementing a fully automated control system.

Beyond the TF-QKD protocol, it would be interesting to evaluate if there are other applications (within quantum communications and beyond) that could benefit from the dual-band stabilisation system developed here. This research could fit into the recent developments of the concept of the quantum Internet [38, 203–205] and

of large time-frequency dissemination networks [183].

Appendix A

Details of the "Proof of Principle TF-QKD Experiment"

In this appendix are reported additional information on the protocols encoding and the detailed experimental results for the proof of principle TF-QKD experiment discussed in chapter 4.

A.1 Detailed Results of the Support Experiment

In table A.1 are reported the results obtained in the support experiment where the users' lasers are phase locked together through OIL with the configuration described in section 4.1.1, for the protocols described in [95, 178]. Data for each channel attenuation is retrieved in a different measurement session. Each measurement session is divided in two parts: system preparation and data acquisition.

During the preparation stage, each user (Alice and Bob) adjust their emitted photon flux (μ_a or μ_b) to the desired level. The channels attenuation (between Alice-Charlie and Bob-Charlie) is then adjusted to the desired level through the VOAs inserted on the quantum channels (in a configuration similar to the one presented in fig. 4.5a). The results obtained at the end of the preparation stage are reported in the first two columns of table A.1. The precise photon fluxes used in the experiment are reported in caption of table A.1.

During the measurement session, Alice's and Bob's pulses are allowed to interfere. The arrival time of the pulses at Charlie's BS is first synchronized via a precise equalisation (within a few ps) of the users' pulses optical paths, and then is optimised by finely adjusting the timing of the users' laser diodes driving RF signals. After the

synchronisation of the pulses at the beginning of the experiment, the setup remains stable throughout. At this stage, after the activation of the phase stabilization system (as described in section 3.4.3), the users' interference could be recorded.

For every channel attenuation, two measurements are carried out: one with pulses having "signal" photon flux (u_a and u_b, data with white background in table A.1), and one with pulses having "decoy" photon flux (v_a and v_b, data with grey background in table A.1).

The gain and QBER obtained experimentally from the interference (third column in table A.1) are then used to calculate the SKR of the tested protocols for different channel attenuations (results shown in the last column of table A.1).

Alice → Charlie		Bob → Charlie		Alice & Bob → Charlie			Secret key rate	
Attenuation (dB)	Gain ($\times 10^{-6}$)	Attenuation (dB)	Gain ($\times 10^{-6}$)	Attenuation (dB)	Gain ($\times 10^{-6}$)	QBER %	TF-QKD ($\times 10^3$)	SNS bit/second
10.7	6000	10.8	6300	21.5	11100	2.3	319	149
	2310		2460		4340	2.2		
15.3	1990	15.2	1970	30.4	3970	1.8	132	60.8
	764		777		1530	2.0		
20.4	602	20.3	588	40.6	1180	1.9	38.4	17.8
	235		234		467	2.0		
25.1	191	25.0	201	50.0	391	1.7	13.4	6.13
	74.5		78.6		152	1.8		
30.0	60.4	29.9	63.4	59.8	123	1.8	4.27	1.93
	24.2		24.0		49.2	1.7		
35.6	17.5	35.5	18.9	71.1	36.3	1.9	1.19	0.49
	6.97		7.45		14.4	2.0		
40.6	5.67	40.6	5.72	81.3	11.3	2.1	0.33	0.09
	2.28		2.40		4.64	2.4		
45.0	1.83	44.9	1.81	90.0	3.58	2.7	0.08	-
	0.71		0.74		1.43	3.6		

Table A.1: Numerical results associated to the support experiment for the proof of principle TF-QKD demonstration for the protocols in [95, 178]. The white (grey) rows in the first, second and third column report the values for the signal gains Q_{u_a}, Q_{u_b}, Q_u (decoy gains Q_{v_a}, Q_{v_b}, Q_v), respectively, registered by detectors D_1 and D_3 in fig. 4.5 when only Alice, only Bob, both users send pulses to the intermediate node. When no user send pulses, the measured gain from the two detectors is $Q_0 = 51.8 \times 10^{-9}$. The flux set by each user is $u_a = u_b = 0.2$ photons per pulse for the signal states and $v_a = v_b = 0.08$ photons per pulse for the decoy states. The vacuum is set to $w = 1 \times 10^{-5}$.

A.2 Detailed Results of the Final Experiment

In tables A.2 and A.3 are reported the results obtained in the main experiment where three different protocols ([95, 120, 178]) were tested. In this case, the users' lasers are phase locked together through OPLL, with the configuration described in section 4.1.2.

The data in table A.2 is acquired with a procedure identical to the one described in the previous section for data in table A.1. For this reason, data in table A.2 is organised as described in appendix A.1 for table A.1. Differently from the support experiment, in the main experiment only the counts recorded by detector D_1 are used for the key generation.

The data in table A.3 refers to the data acquisition executed at 71.1 dB for the CAL TF-QKD protocol variant proposed in [120].

Alice → Charlie		Bob → Charlie		Alice & Bob → Charlie			Secret key rate		
Attenuation (dB)	Gain ($\times 10^{-6}$)	Attenuation (dB)	Gain ($\times 10^{-6}$)	Attenuation (dB)	Gain ($\times 10^{-6}$)	QBER %	TF-QKD ($\times 10^3$) bit/s	SNS	SKC_0
10.7	3000	10.8	3150	21.5	5560	2.3	159	74.5	10200
	1550		1230		2170	2.2			
15.3	993	15.2	986	30.5	1980	1.8	66.1	30.4	1290
	382		388		765	2.0			
20.4	301	20.3	294	40.7	592	1.9	19.2	8.86	123
	117		117		233	2.0			
25.1	95.4	25.0	100	50.1	196	1.7	6.71	3.03	14.1
	37.2		39.3		76.2	1.8			
30.0	30.2	29.9	63.4	61.7	61.6	1.8	2.14	0.93	1.48
	12.1		12.0		24.6	1.7			
35.6	8.74	35.5	9.44	71.1	18.2	1.9	0.602	0.21	0.112
	3.48		3.72		7.19	2.0			
40.6	2.84	40.6	2.86	81.2	5.65	2.1	0.163	0.018	0.011
	1.14		1.20		2.32	2.4			
45.4	0.91	45.4	0.91	90.8	1.79	2.7	0.045	-	0.001
	0.35		0.37		0.72	3.6			

Table A.2: Numerical results of the main experiment with the TF-QKD protocols in [95, 178]. The white (grey) rows in the first, second and third column report the values for the signal gains Q_{u_a}, Q_{u_b}, Q_u (decoy gains Q_{v_a}, Q_{v_b}, Q_v), respectively, registered by detector D_1 in fig. 4.5 when only Alice, only Bob, both users send pulses to the intermediate node. When no user sends out pulses, the measured gain is $Q_0 = 25.9 \times 10^{-9}$. The flux set by each user is $u_a = u_b = 0.2$ photons per pulse for the signal states and $v_a = v_b = 0.08$ photons per pulse for the decoy states. The vacuum is set to $w = 1 \times 10^{-5}$.

A. DETAILS OF THE "PROOF OF PRINCIPLE TF-QKD EXPERIMENT"

Phase randomised	
Flux	Gain (1 detector) ($\times 10^{-6}$)
uu	1.7
vv	18
ww	0.03
uv	8.8
uw	0.91
vw	8.7

Encoded		
Flux	Gain ($\times 10^{-6}$)	QBER %
uu	1.8	2.7

Table A.3: Measured quantities for the protocol in Ref. [120]. At 71.1 dB channel loss it provides a SKR of 270 bit s^{-1}, which is 2.4 times above the ideal SKC_0 bound at the same attenuation (112 bit s^{-1}). The fluxes set by each user are $u_a = u_b = 0.02$ photons per pulse for the signal states and $v_a = v_b = 0.2$ photons per pulse for the decoy states. The total vacuum is set to w=1×10^{-5}.

Appendix B

Details of the "TF-QKD over 600 km of Optical Fibre" Experiment

In this appendix are reported some detailed characterisation and results associated with the experiment discussed in chapter 6.

B.1 Optical Fibre Characterisation

In table B.1 we report the combined losses of the fibre spools used at the different distances. At all distances, we have assigned the lossier spools to Bob. The additional channel losses on Bob's side were compensated by his higher transmission coefficient at Charlie's module. During the experiment, when there was an asymmetry between the users' photon rate received by Charlie, we compensated for it by increasing the attenuation of Bob's transmitter.

B.2 Detailed Description of the Encoding Strategy

In this section we describe how the transmitter boxes presented in section 5.1 are used to execute the encoding of the experiment presented in chapter 6.

The EPC and the polariser placed at the entrance of the transmitter boxes are used to align the polarisation of the incoming CW light with the optical axes of the subsequent modulators. The following components in the encoders are three IMs,

B. DETAILS OF THE "TF-QKD OVER 600 KM OF OPTICAL FIBRE" EXPERIMENT

	Losses (dB)	
Fibre length (km)	Alice	Bob
76.64	13.2	13.3
184.35	31.4	32.2
260.86	44.7	45.4
277.46	47.7	48.5
302.58	52.4	53.1

Table B.1: Combined losses of the fibre spools used at different distances.

used to carve 250 ps long pulses at a 1 GHz rate, with three possible intensity levels (u, v, w). The intensity ratios between the different intensity levels can be adjusted by the RF signals amplitude driving the IMs. In order to initialise the IMs settings, and monitor possible intensity fluctuations due to DC drifts, the IMs are followed by a 50:50 BS which sends half of its output to a monitoring port of a power meter.

The other BS output continues through two PMs which are used to set the phase of the optical pulses. In this system, we cascade two PMs instead of using just one to reduce the amplitudes of their driving RF signals. Limiting each PM to have a modulation range of $[-\pi/2, \pi/2]$, we achieve a phase modulation that covers the whole $[0, 2\pi)$ range and that is linear with its driving signal amplitude. Each PM is driven by a 8-bit DAC.

All the modulators are driven by a 12 GSa s^{-1} waveform generator, programmed to encode a 25040-pulse long pseudo-random pattern. For more information on this refer to the section 6.3.

The PMs are followed by an EPC, a VOA, and a 99:1 BS. The EPC is used to control the polarisation of the λ_Q photons after transmission through the channel. Each user has a continuous polarisation optimisation routine that aligns the quantum signals to polarise along the preferred optical axis at Charlie.

The VOA sets the flux of the quantum signal before injection into the quantum channel, through a flux calibration control loop that continuously adjusts the VOA so as to have a stable optical output, monitored at the strong output of the BS.

B.3 Detailed Experimental Results

In tables B.2 to B.6 are reported the detailed experimental results for the different SNS-type protocols tested during the experiment presented in chapter 6. The first three tables show the results obtained with a 50 km long service fibre between Alice and Bob (setup shown in fig. 6.8). Table B.2 reports the results for the asymptotic SNS protocol (without TWCC). Table B.3 summarises the results for the TWCC SNS TF-QKD protocol in the asymptotic scenario, while the results obtained in the finite size regime are reported in table B.3.

The last two tables (B.5 and B.6) show the results obtained with a 610 km long service fibre separating Alice and Bob (setup shown in fig. 6.9). Table B.5 summarises the results for the TWCC SNS TF-QKD protocol in the asymptotic scenario, while table B.6 summarises the results obtained in the finite size regime.

For each measurement are reported the length of the quantum channel, the length of the service channel, and the number of protocol encoded pulses that were sent (N_0). Also reported are the errors in the different bases and for different pulse intensities, and the calculated SKR obtained at that distance (alongside the relative SKC_0 bound). For all the protocols, the exact number of pulses sent in each pulses pair configuration can be calculated by multiplying N_0 by the respective pulses combinations probabilities deducible from tables 6.2 and 6.3. The number of pulses detected in these configurations are reported in the tables below, labelled in the format $B_1B_2t_1t_2$, where B_1 and t_1 (B_2 and t_2) are the basis and the type of pulse sent by Alice (Bob). When TWCC is employed, quantities relative to the key post-processing are listed.

B. DETAILS OF THE "TF-QKD OVER 600 KM OF OPTICAL FIBRE" EXPERIMENT

Quantum link length (km)	368.702
Servo link length (km)	51.220
N_0	$2.066 \cdot 10^{11}$
Phase mismatch acceptance	22.5°
Z error rate	6.59%
Xuu error rate	3.29%
Xvv error rate	3.87%
Phase error rate	4.15%
SKR SNS (no TWCC) asympt norm (bit/signal)	$1.098 \cdot 10^{-6}$
SKR SNS (no TWCC) asympt norm (bit/s)	$5.492 \cdot 10^{2}$
Ratio SKR over SKC_0	1.54
SKC_0 (bit/signal)	$7.151 \cdot 10^{-7}$
SKC_0 (bit/s)	$3.576 \cdot 10^{2}$
Total Detected D_0	4887891
Total Detected D_1	4624363
Detected ZZss	39403
Detected ZZsn	314309
Detected ZZns	304872
Detected ZZnn	4264
Detected ZXsu	217790
Detected ZXsv	121824
Detected ZXsw	112334
Detected ZXnu	1729304
Detected ZXnv	173107
Detected ZXnw	1634
Detected XZus	217780
Detected XZun	1786996
Detected XZvs	117638
Detected XZvn	155240
Detected XZws	113964
Detected XZwn	1486
Detected XXuu	1240351
Detected XXuv	685682
Detected XXuw	643480
Detected XXvu	668424
Detected XXvv	115296
Detected XXvw	55695
Detected XXwu	628786
Detected XXwv	62043
Detected XXww	552
Detected XXuu matching (D_0)	79037
Detected XXuu matching (D_1)	74844
Correct XXuu matching (D_0)	76474
Correct XXuu matching (D_1)	72352
Detected ZZ errors	43667
Detected ZZ correct	619181

Table B.2: Asymptotic SNS: experimental results obtained with a 51 km long servo link and a 368.7 km long quantum channel.

Quantum link length (km)	153.282	368.702	521.982	555.172	605.17
Servo link length (km)	51.220	51.220	51.220	51.220	51.220
N_0	$5.296 \cdot 10^{10}$	$1.527 \cdot 10^{11}$	$5.208 \cdot 10^{11}$	$2.554 \cdot 10^{11}$	$1.002 \cdot 10^{12}$
Phase mismatch acceptance	22.5°	22.5°	22.5°	22.5°	22.5°
Z error rate (before)	13.1%	13.1%	14.%	14.6%	16.4%
Odd pairs in raw keys	$3.522 \cdot 10^{6}$	$2.277 \cdot 10^{5}$	$3.968 \cdot 10^{4}$	$9.565 \cdot 10^{3}$	$1.369 \cdot 10^{4}$
Even pairs 00 in raw keys	$1.938 \cdot 10^{6}$	$1.228 \cdot 10^{5}$	$2.162 \cdot 10^{4}$	$5.174 \cdot 10^{3}$	$7.411 \cdot 10^{3}$
Even pairs 11 in raw keys	$1.74 \cdot 10^{6}$	$1.15 \cdot 10^{5}$	$1.963 \cdot 10^{4}$	$4.725 \cdot 10^{3}$	$6.575 \cdot 10^{3}$
Error pairs in raw keys	$1.591 \cdot 10^{5}$	$1.039 \cdot 10^{4}$	$2.096 \cdot 10^{3}$	$5.532 \cdot 10^{2}$	$1.029 \cdot 10^{3}$
Z error rate (after)	2.21%	2.23%	2.59%	2.84%	3.72%
Xuu error rate	2.8%	3.21%	3.86%	3.68%	3.5%
Xvv error rate	5.53%	6.32%	4.78%	8.33%	13.6%
Phase error rate	5.68%	6.4%	3.71%	6.08%	2.31%
n_1 (before TWCC)	$1.159 \cdot 10^{7}$	$7.49 \cdot 10^{5}$	$1.254 \cdot 10^{5}$	$3.284 \cdot 10^{4}$	$3.733 \cdot 10^{4}$
n_1 (after TWCC)	$3.605 \cdot 10^{6}$	$2.326 \cdot 10^{5}$	$3.685 \cdot 10^{4}$	$1.04 \cdot 10^{4}$	$9.136 \cdot 10^{3}$
${e_1}^{\mathrm{ph}}$ (before TWCC)	5.68%	6.4%	3.71%	6.08%	2.31%
${e_1}^{\mathrm{ph}}$ (after TWCC - asympt)	10.7%	12.%	7.15%	11.4%	4.52%
SKR TWCC asympt norm (bit/signal)	$7.441 \cdot 10^{-5}$	$1.412 \cdot 10^{-6}$	$8.557 \cdot 10^{-8}$	$2.838 \cdot 10^{-8}$	$1.937 \cdot 10^{-9}$
SKR TWCC asympt norm (bit/s)	$3.721 \cdot 10^{4}$	$7.059 \cdot 10^{2}$	$4.278 \cdot 10^{1}$	$1.419 \cdot 10^{1}$	$9.685 \cdot 10^{-1}$
Ratio SKR over SKC_0	0.0215	1.97	50.	61.3	29.7
SKC_0 (bit/signal)	$3.456 \cdot 10^{-3}$	$7.151 \cdot 10^{-7}$	$1.711 \cdot 10^{-9}$	$4.632 \cdot 10^{-10}$	$6.511 \cdot 10^{-11}$
SKC_0 (bit/s)	$1.728 \cdot 10^{6}$	$3.576 \cdot 10^{2}$	$8.556 \cdot 10^{-1}$	$2.316 \cdot 10^{-1}$	$3.256 \cdot 10^{-2}$
Total Detected D_0	69221704	4524664	795437	193156	278746
Total Detected D_1	66051719	4241991	745698	181085	263766
Detected ZZss	2423210	156953	27876	6727	9620
Detected ZZsn	8146041	521082	91891	22168	32219
Detected ZZns	8052039	526583	91497	22122	31538
Detected ZZnn	11389	1380	2024	848	2907
Detected ZXsu	6196623	403188	70879	17076	24785
Detected ZXsv	3217021	205870	36367	8629	12876
Detected ZXsw	3107274	198690	35299	8610	12320
Detected ZXnu	20581340	1349062	235655	57121	81690
Detected ZXnv	604012	37884	7635	1915	3125
Detected ZXnw	4212	518	747	289	1085
Detected XZus	6202770	403207	70119	17168	24722
Detected XZun	20928197	1340008	236339	57217	82636
Detected XZvs	3181382	208453	36111	8811	12607
Detected XZvn	628269	41662	7104	1879	3037
Detected XZws	3078177	202140	35286	8426	12396
Detected XZwn	4250	534	765	281	1102
Detected XXuu	15759404	1022280	179333	43000	61766
Detected XXuv	8202418	526279	92761	22151	32573
Detected XXuw	7977865	511560	89706	21900	31585
Detected XXvu	8127297	531576	92456	22577	31672
Detected XXvv	480868	30579	5527	1427	1904
Detected XXvw	247965	16325	2809	799	1182
Detected XXwu	7874039	516027	89699	22269	31572
Detected XXwv	235716	14614	2968	718	1170
Detected XXww	1645	201	282	113	423
Detected XXuu matching (D_0)	990284	64565	11389	2746	3939
Detected XXuu matching (D_1)	930327	59658	10558	2581	3712
Correct XXuu matching (D_0)	961135	62388	10921	2653	3789
Correct XXuu matching (D_1)	905683	57844	10179	2478	3594
Detected ZZ errors	2434599	158333	29900	7575	12527
Detected ZZ correct	16198080	1047665	183388	44290	63757

Table B.3: Asymptotic TWCC SNS: experimental results obtained with a 51 km long servo link at various quantum channel lengths.

B. DETAILS OF THE "TF-QKD OVER 600 KM OF OPTICAL FIBRE" EXPERIMENT

Quantum link length (km)	153.282	368.702	521.982	555.172
Servo link length (km)	51.220	51.220	51.220	51.220
N_0	$6. \cdot 10^{11}$	$2.435 \cdot 10^{12}$	$3.07 \cdot 10^{12}$	$3.536 \cdot 10^{12}$
Phase mismatch acceptance	22.5°	22.5°	22.5°	22.5°
Z error rate (before)	7.67%	7.69%	9.01%	9.77%
Odd pairs in raw keys	$4.164 \cdot 10^{7}$	$3.564 \cdot 10^{6}$	$2.333 \cdot 10^{5}$	$1.336 \cdot 10^{5}$
Even pairs 00 in raw keys	$2.135 \cdot 10^{7}$	$1.838 \cdot 10^{6}$	$1.198 \cdot 10^{5}$	$6.922 \cdot 10^{4}$
Even pairs 11 in raw keys	$2.077 \cdot 10^{7}$	$1.768 \cdot 10^{6}$	$1.152 \cdot 10^{5}$	$6.501 \cdot 10^{4}$
Error pairs in raw keys	$5.738 \cdot 10^{5}$	$4.938 \cdot 10^{4}$	$4.542 \cdot 10^{3}$	$3.103 \cdot 10^{3}$
Z error rate (after)	0.685%	0.689%	0.97%	1.16%
Xuu error rate	2.69%	2.88%	2.87%	3.47%
Xvv error rate	3.56%	3.81%	5.31%	5.09%
Phase error rate	4.16%	4.47%	6.04%	5.59%
n_1 (before TWCC)	$1.185 \cdot 10^{8}$	$1.003 \cdot 10^{7}$	$6.4 \cdot 10^{5}$	$3.652 \cdot 10^{5}$
n_1 (after TWCC)	$3.596 \cdot 10^{7}$	$3.013 \cdot 10^{6}$	$1.828 \cdot 10^{5}$	$1.026 \cdot 10^{5}$
${e_1}^{\mathrm{ph}}$ (before TWCC)	4.23%	4.71%	7.48%	7.65%
${e_1}^{\mathrm{ph}}$ (after TWCC)	8.09%	8.98%	13.8%	14.1%
Number of secret bits generated (bits)	$1.707 \cdot 10^{7}$	$1.329 \cdot 10^{6}$	$4.046 \cdot 10^{4}$	$1.745 \cdot 10^{4}$
SKR (bit/signal)	$2.846 \cdot 10^{-5}$	$5.459 \cdot 10^{-7}$	$1.318 \cdot 10^{-8}$	$4.937 \cdot 10^{-9}$
SKR (bit/s)	$1.423 \cdot 10^{4}$	$2.729 \cdot 10^{2}$	6.59	2.468
Ratio SKR over SKC_0	0.00823	0.763	7.7	10.7
SKC_0 (bit/signal)	$3.456 \cdot 10^{-3}$	$7.151 \cdot 10^{-7}$	$1.711 \cdot 10^{-9}$	$4.632 \cdot 10^{-10}$
SKC_0 (bit/s)	$1.728 \cdot 10^{6}$	$3.576 \cdot 10^{2}$	$8.556 \cdot 10^{-1}$	$2.316 \cdot 10^{-1}$
Total Detected D_0	623261177	54266217	3616047	2071809
Total Detected D_1	601407532	50532067	3317070	1945930
Detected ZZss	14322977	1229675	80689	46061
Detected ZZsn	90153430	7739935	511622	296484
Detected ZZns	90035335	7685653	507468	290238
Detected ZZnn	642059	54944	20176	17462
Detected ZXsu	25714805	2199489	144929	82891
Detected ZXsv	46330397	3956642	262219	150458
Detected ZXsw	12870272	1107377	72977	42765
Detected ZXnu	159718589	13637478	898693	517464
Detected ZXnv	90956994	7710475	507227	297300
Detected ZXnw	93804	7989	2973	2550
Detected XZus	25704406	2209257	146032	85067
Detected XZun	159575781	13695784	906734	526484
Detected XZvs	46091214	3944702	259209	149050
Detected XZvn	89990485	7718247	507676	294097
Detected XZws	12982067	1109205	73179	42204
Detected XZwn	92445	7776	2977	2516
Detected XXuu	44724005	3838050	252841	145782
Detected XXuv	82278922	7047247	466076	270776
Detected XXuw	22992576	1978960	131444	75985
Detected XXvu	82116355	7042214	463506	268561
Detected XXvv	78177798	6684280	437657	252988
Detected XXvw	13010771	1116305	73487	42281
Detected XXwu	22952199	1964545	129678	75082
Detected XXwv	13127709	1110997	73238	42795
Detected XXww	13314	1058	410	398
Detected XXuu matching (D_0)	2880087	250202	16753	9609
Detected XXuu matching (D_1)	2822546	239368	15656	9148
Correct XXuu matching (D_0)	2805790	243186	16263	9260
Correct XXuu matching (D_1)	2743311	232285	15215	8846
Detected ZZ errors	14965036	1284619	100865	63523
Detected ZZ correct	180188765	15425588	1019090	586722

Table B.4: Finite-size TWCC SNS: experimental results obtained with a 51 km long servo link at various quantum channel lengths.

Quantum link length (km)	555.172	605.170
Servo link length (km)	611.448	611.448
N_0	$8.038 \cdot 10^{11}$	$1.353 \cdot 10^{12}$
Phase mismatch acceptance	22.5°	22.5°
Z error rate (before)	14.1%	16.3%
Odd pairs in raw keys	$2.622 \cdot 10^4$	$1.631 \cdot 10^4$
Even pairs 00 in raw keys	$1.445 \cdot 10^4$	$8.530 \cdot 10^3$
Even pairs 11 in raw keys	$1.272 \cdot 10^4$	$8.134 \cdot 10^3$
Error pairs in raw keys	$1.412 \cdot 10^3$	$1.205 \cdot 10^3$
Z error rate (after)	2.64%	3.65%
Xuu error rate	4.99%	5.41%
Xvv error rate	9.68%	13.%
Phase error rate	5.12%	5.94%
n_1 (before TWCC)	$8.615 \cdot 10^4$	$5.346 \cdot 10^4$
n_1 (after TWCC)	$2.631 \cdot 10^4$	$1.5756 \cdot 10^4$
$e_1{}^{\text{ph}}$ (before TWCC)	5.12%	5.94%
$e_1{}^{\text{ph}}$ (after TWCC - asympt)	9.71%	11.2%
SKR TWCC asympt norm (bit/signal)	$2.936 \cdot 10^{-8}$	$1.555 \cdot 10^{-9}$
SKR TWCC asympt norm (bit/s)	$1.468 \cdot 10^1$	$7.778 \cdot 10^{-1}$
Ratio SKR over SKC_0	63.4	24.0
SKC_0 (bit/signal)	$4.632 \cdot 10^{-10}$	$6.468 \cdot 10^{-11}$
SKC_0 (bit/s)	$2.316 \cdot 10^{-1}$	$3.234 \cdot 10^{-2}$
Total Detected D_0	494716	312237
Total Detected D_1	523903	329627
Detected ZZss	18133	11390
Detected ZZsn	61210	37648
Detected ZZns	59884	38261
Detected ZZnn	1822	3392
Detected ZXsu	46849	28773
Detected ZXsv	24278	14942
Detected ZXsw	23458	14489
Detected ZXnu	153672	96970
Detected ZXnv	4919	4045
Detected ZXnw	685	1319
Detected XZus	46598	28882
Detected XZun	157244	96571
Detected XZvs	23398	14948
Detected XZvn	4967	4004
Detected XZws	22942	14598
Detected XZwn	686	1371
Detected XXuu	118175	73243
Detected XXuv	62210	38161
Detected XXuw	60417	36867
Detected XXvu	60505	38517
Detected XXvv	3671	2582
Detected XXvw	2015	1588
Detected XXwu	58686	37257
Detected XXwv	1940	1548
Detected XXww	255	498
Detected XXuu matching (D_0)	6963	4178
Detected XXuu matching (D_1)	7452	4358
Correct XXuu matching (D_0)	6624	3974
Correct XXuu matching (D_1)	7071	4100
Detected ZZ errors	19955	14782
Detected ZZ correct	121094	75909

Table B.5: Asymptotic TWCC SNS: experimental results obtained with a 611 km long servo link at various quantum channel lengths.

B. DETAILS OF THE "TF-QKD OVER 600 KM OF OPTICAL FIBRE" EXPERIMENT

Quantum link length (km)	555.172
Servo link length (km)	611.448
N_0	$3.121 \cdot 10^{12}$
Phase mismatch acceptance	22.5°
Z error rate (before)	9.98%
Odd pairs in raw keys	$9.163 \cdot 10^{4}$
Even pairs 00 in raw keys	$4.608 \cdot 10^{4}$
Even pairs 11 in raw keys	$4.594 \cdot 10^{4}$
Error pairs in raw keys	$2.234 \cdot 10^{3}$
Z error rate (after)	1.22%
Xuu error rate	5.12%
Xvv error rate	5.49%
Phase error rate	5.73%
n_1 (before TWCC)	$2.597 \cdot 10^{5}$
n_1 (after TWCC)	$7.530 \cdot 10^{4}$
$e_1{}^{\mathrm{ph}}$ (before TWCC)	8.32%
$e_1{}^{\mathrm{ph}}$ (after TWCC)	15.2%
Number of secret bits generated (bits)	$1.109 \cdot 10^{4}$
SKR (bit/signal)	$3.555 \cdot 10^{-9}$
SKR (bit/s)	1.777
Ratio SKR over SKC_0	7.675
SKC_0 (bit/signal)	$4.632 \cdot 10^{-10}$
SKC_0 (bit/s)	$2.316 \cdot 10^{-1}$
Total Detected D_0	1330784
Total Detected D_1	1429497
Detected ZZss	31819
Detected ZZsn	200662
Detected ZZns	202447
Detected ZZnn	12911
Detected ZXsu	57243
Detected ZXsv	103341
Detected ZXsw	28818
Detected ZXnu	357386
Detected ZXnv	209380
Detected ZXnw	1823
Detected XZus	57723
Detected XZun	354724
Detected XZvs	102785
Detected XZvn	203294
Detected XZws	29110
Detected XZwn	1825
Detected XXuu	99664
Detected XXuv	183501
Detected XXuw	51213
Detected XXvu	183158
Detected XXvv	175638
Detected XXvw	29287
Detected XXwu	51513
Detected XXwv	30769
Detected XXww	247
Detected XXuu matching (D_0)	5842
Detected XXuu matching (D_1)	6417
Correct XXuu matching (D_0)	5529
Correct XXuu matching (D_1)	6102
Detected ZZ errors	44730
Detected ZZ correct	403109

Table B.6: Finite-size TWCC SNS obtained with a 555.2 km long quantum channel and 611 km of servo fibre.

Bibliography

[1] M. Castells. *The information age, volumes 1-3: Economy, society and culture.* 1999.

[2] C. E. Shannon. 'A mathematical theory of communication'. *The Bell System Technical Journal* 27.3 (1948), pp. 379–423.

[3] P. B. Brandtzæg. *Big Data, for better or worse: 90% of world's data generated over last two years.* 11/06/2018.

[4] M. Willett. 'Cryptography old and new'. *Computers & Security* 1.2 (1982), pp. 177–186.

[5] S. Singh. *The code book: The evolution of secrecy from Mary, Queen of Scots, to quantum cryptography.* Doubleday, 1999.

[6] C. E. Shannon. 'Communication theory of secrecy systems'. *The Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[7] O. Goldreich. *Foundations of cryptography.* Cambridge: Cambridge University Press, 2001.

[8] R. L. Rivest, A. Shamir and L. Adleman. 'A Method for Obtaining Digital Signatures and Public-key Cryptosystems'. *Commun. ACM* 21.2 (1978), pp. 120–126.

[9] M. A. Nielsen and I. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2000.

[10] S. Aaronson. *Quantum computing since Democritus.* Cambridge: Cambridge University Press, 2013.

[11] J. D. Hidary. *Quantum Computing: An Applied Approach.* Cham: Springer International Publishing, 2019.

[12] P. W. Shor. 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer'. *SIAM review* 41.2 (1999), pp. 303–332.

[13] D. Castelvecchi. 'Quantum-computing pioneer warns of complacency over Internet security'. *Nature* 587.7833 (2020), p. 189.

[14] D. Castelvecchi. 'The race to save the Internet from quantum hackers'. *Nature* 602.7896 (2022), pp. 198–201.

[15] F. Arute et al. 'Quantum supremacy using a programmable superconducting processor'. *Nature* 574.7779 (2019), pp. 505–510.

[16] H.-S. Zhong et al. 'Quantum computational advantage using photons'. *Science* 370.6523 (2020), pp. 1460–1463.

[17] V. Gheorghiu and M. Mosca. *Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes*. 2019.

[18] C. Gidney and M. Ekerå. 'How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits'. *Quantum* 5 (2021), p. 433.

[19] A. Baumhof. *Breaking RSA Encryption – an Update on the State-of-the-Art*. Ed. by Quintessence Labs.

[20] A. Herman. *Q-Day Is Coming Sooner Than We Think*. Ed. by Forbes.

[21] S. Shankland. *Quantum computers could crack today's encrypted messages. That's a problem: We'll likely see the top picks for safer, post-quantum encryption technology early in 2022.* Ed. by CNet.

[22] C. Cohen-Tannoudji, B. Diu and F. Laloë. *Quantum mechanics*. Second edition. Weinheim, Germany: Wiley-VCH, 2020.

[23] C. H. Bennett and G. Brassard. 'Quantum cryptography: Public key distribution and coin tossing: Public key distribution and coin tossing'. *Theoretical Computer Science* 560 (2014), pp. 7–11.

[24] N. Gisin et al. 'Quantum cryptography'. *Reviews of Modern Physics* 74.1 (2002), pp. 145–195.

[25] V. Scarani et al. 'The security of practical quantum key distribution'. *Reviews of Modern Physics* 81.3 (2009), pp. 1301–1350.

[26] F. Xu et al. 'Secure quantum key distribution with realistic devices'. *Reviews of Modern Physics* 92.2 (2020), p. 131.

[27] S. Pirandola et al. 'Advances in quantum cryptography'. *Advances in Optics and Photonics* 12.4 (2020), p. 1012.

[28] Ekert. 'Quantum cryptography based on Bell's theorem'. *Physical review letters* 67.6 (1991), pp. 661–663.

[29] C. H. Bennett. 'Quantum cryptography using any two nonorthogonal states'. *Phys. Rev. Lett.* 68.21 (1992), pp. 3121–3124.

[30] D. Mayers. 'Unconditional Security in Quantum Cryptography'. *J. ACM* 48.3 (2001), pp. 351–406.

[31] P. W. Shor and J. Preskill. 'Simple proof of security of the BB84 quantum key distribution protocol'. *Physical review letters* 85.2 (2000), pp. 441–444.

[32] L. K. Grover. 'A fast quantum mechanical algorithm for database search'. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Ed. by G. L. Miller. New York, New York, USA: ACM Press, 1996, pp. 212–219.

[33] Bennett, Brassard and Mermin. 'Quantum cryptography without Bell's theorem'. *Physical review letters* 68.5 (1992), pp. 557–559.

[34] A. Einstein, B. Podolsky and N. Rosen. 'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?' *Physical Review* 47.10 (1935), pp. 777–780.

[35] M. Pawłowski. 'Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations'. *Physical Review A* 82.3 (2010).

[36] J. F. Clauser et al. 'Proposed Experiment to Test Local Hidden-Variable Theories'. *Physical Review Letters* 23.15 (1969), pp. 880–884.

[37] J. S. Bell. 'On the Einstein Podolsky Rosen paradox'. *Physics (Physics Physique Fizika)* 1.3 (1964), pp. 195–200.

[38] H. J. Kimble. 'The quantum internet'. *Nature* 453.7198 (2008), pp. 1023–1030.

[39] N. Sangouard et al. 'Quantum repeaters based on atomic ensembles and linear optics'. *Reviews of Modern Physics* 83.1 (2011), pp. 33–80.

[40] D. Mayers and A. Yao. 'Quantum cryptography with imperfect apparatus'. In: *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*. IEEE Comput. Soc, 8-11/11/1998, pp. 503–509.

[41] U. Vazirani and T. Vidick. 'Fully device independent quantum key distribution'. *Commun. ACM* 62.4 (2019), p. 133.

[42] C. H. Bennett et al. 'Experimental quantum cryptography'. *Journal of Cryptology* 5.1 (1992), pp. 3–28.

[43] A. Muller, J. Breguet and N. Gisin. 'Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km'. *EPL (Europhysics Letters)* 23.6 (1993), p. 383.

[44] P. D. Townsend. 'Secure key distribution system based on quantum cryptography'. *Measurement Science and Technology* 30.10 (1994), pp. 809–811.

[45] P. D. Townsend. 'Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing'. *Electronics Letters* 33.3 (1997), p. 188.

[46] L. Lydersen et al. 'Hacking commercial quantum cryptography systems by tailored bright illumination'. *Nature Photonics* 4.10 (2010), pp. 686–689.

[47] C. Wiechers et al. 'After-gate attack on a quantum cryptosystem'. *New Journal of Physics* 13.1 (2011), p. 013043.

[48] H.-K. Lo, M. Curty and K. Tamaki. 'Secure quantum key distribution'. *Nature Photonics* 8.8 (2014), pp. 595–604.

[49] E. Diamanti et al. 'Practical challenges in quantum key distribution'. *npj Quantum Information* 2.1 (2016), p. 167.

[50] H.-K. Lo, M. Curty and B. Qi. 'Supplemental Information for "Measurement-device-independent quantum key distribution"'. *Physical review letters* 108.13 (2012).

[51] S. L. Braunstein and S. Pirandola. 'Side-channel-free quantum key distribution'. *Physical review letters* 108.13 (2012), p. 130502.

[52] Hong, Ou and Mandel. 'Measurement of subpicosecond time intervals between two photons by interference'. *Physical review letters* 59.18 (1987), pp. 2044–2046.

[53] A. Rubenok et al. 'Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks'. *Physical review letters* 111.13 (2013), p. 130501.

[54] Y. Liu et al. 'Experimental measurement-device-independent quantum key distribution'. *Physical review letters* 111.13 (2013), p. 130502.

[55] T. Ferreira da Silva et al. 'Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits'. *Physical Review A* 88.5 (2013), p. 325.

[56] Z. Tang et al. 'Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution'. *Physical review letters* 112.19 (2014), p. 190503.

[57] H.-L. Yin et al. 'Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber'. *Physical review letters* 117.19 (2016), p. 190501.

[58] L. C. Comandar et al. 'Quantum key distribution without detector vulnerabilities using optically seeded lasers'. *Nature Photonics* 10.5 (2016), pp. 312–315.

[59] B. Lounis and M. Orrit. 'Single-photon sources'. *New Journal of Physics* 68.5 (2005), pp. 1129–1179.

[60] M. D. Eisaman et al. 'Invited review article: Single-photon sources and detectors'. *The Review of scientific instruments* 82.7 (2011), p. 071101.

[61] T. Heindel et al. 'Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range'. *New Journal of Physics* 14.8 (2012), p. 083001.

[62] K. Takemoto et al. 'Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors'. *Scientific reports* 5 (2015), p. 14383.

[63] N. Lütkenhaus. 'Security against individual attacks for realistic quantum key distribution'. *Physical Review A* 61.5 (2000), p. 78.

[64] N. Lütkenhaus and M. Jahma. 'Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack'. *Optics Letters* 4 (2002), p. 44.

[65] R. J. Glauber. 'The Quantum Theory of Optical Coherence'. *Physical Review* 130.6 (1963), pp. 2529–2539.

[66] L. Salasnich. *Quantum physics of light and matter: A Modern Introduction to Photons, Atoms and Many-Body Systems*. New York: Springer, 2014.

[67] M. Fox. *Quantum optics: An introduction*. Vol. 15. Oxford master series in physics. Oxford and New York: Oxford university press, 2006.

[68] Brassard et al. 'Limitations on practical quantum cryptography'. *Physical review letters* 85.6 (2000), pp. 1330–1333.

[69] D. Gottesman and Lo Hoi-Kwong. 'Proof of security of quantum key distribution with two-way classical communications'. *IEEE Transactions on Information Theory* 49.2 (2003), pp. 457–475.

[70] W.-Y. Hwang. 'Quantum Key Distribution with High Loss: Toward Global Secure Communication'. *Physical review letters* 91.5 (2003), p. 057901.

[71] H.-K. Lo, X. Ma and K. Chen. 'Decoy state quantum key distribution'. *Physical review letters* 94.23 (2005), p. 230504.

[72] X.-B. Wang. 'Beating the photon-number-splitting attack in practical quantum cryptography'. *Physical review letters* 94.23 (2005), p. 230503.

[73] C. Gobby, Z. L. Yuan and A. J. Shields. 'Unconditionally secure quantum key distribution over 50 km of standard telecom fibre'. *New Journal of Physics* 40.25 (2004), p. 1603.

[74] D. Gottesman et al. 'Security of quantum key distribution with imperfect devices'. In: *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*. IEEE, 2004, p. 135.

[75] H. Inamori, N. Lütkenhaus and D. Mayers. 'Unconditional security of practical quantum key distribution'. *The European Physical Journal D* 41.3 (2007), pp. 599–627.

[76] V. Scarani and R. Renner. 'Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing'. *Physical Review Letters* 100.20 (2008), p. 200501.

[77] R. Y. Q. Cai and V. Scarani. 'Finite-key analysis for practical implementations of quantum key distribution'. *New Journal of Physics* 11.4 (2009), p. 045024.

[78] M. Tomamichel et al. 'Tight finite-key analysis for quantum cryptography'. *Nature Communications* 3 (2012), p. 634.

[79] S. Kawakami, T. Sasaki and M. Koashi. 'Finite-key analysis for quantum key distribution with weak coherent pulses based on Bernoulli sampling'. *Physical Review A* 96.1 (2017), p. 325.

[80] D. Bruss et al. 'Approximate quantum cloning and the impossibility of superluminal information transfer'. *Physical Review A* 62.6 (2000), p. 293.

[81] D. Bruß and G. Leuchs. *Quantum Information*. Wiley, 2016.

[82] W. K. Wootters and W. H. Zurek. 'A single quantum cannot be cloned'. *Nature* 299.5886 (1982), pp. 802–803.

[83] M. Takeoka, S. Guha and M. M. Wilde. 'Fundamental rate-loss tradeoff for optical quantum key distribution'. *Nature Communications* 5 (2014), p. 5235.

[84] S. Pirandola et al. 'Fundamental limits of repeaterless quantum communications'. *Nature Communications* 8 (2017), p. 15043.

[85] M. Peev et al. 'The SECOQC quantum key distribution network in Vienna'. *New Journal of Physics* 11.7 (2009), p. 075001.

[86] M. Sasaki et al. 'Field test of quantum key distribution in the Tokyo QKD Network'. *Optics express* 19.11 (2011), pp. 10387–10409.

[87] A. I. Lvovsky, B. C. Sanders and W. Tittel. 'Optical quantum memory'. *Nature Photonics* 3.12 (2009), pp. 706–714.

[88] C. Simon et al. 'Quantum memories'. *The European Physical Journal D* 58.1 (2010), pp. 1–22.

[89] K. Heshami et al. 'Quantum memories: emerging applications and recent advances'. *Journal of Modern Optics* 63.20 (2016), pp. 2005–2028.

[90] C. Panayi et al. 'Memory-assisted measurement-device-independent quantum key distribution'. *New Journal of Physics* 16.4 (2014), p. 043005.

[91] M. K. Bhaskar et al. 'Experimental demonstration of memory-enhanced quantum communication'. *Nature* 580.7801 (2020), pp. 60–64.

[92] S. Langenfeld et al. 'Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution'. *Physical review letters* 126.23 (2021), p. 230506.

[93] L. M. Duan et al. 'Long-distance quantum communication with atomic ensembles and linear optics'. *Nature* 414.6862 (2001), pp. 413–418.

[94] W. J. Munro et al. 'Inside Quantum Repeaters'. *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 78–90.

[95] M. Lucamarini et al. 'Overcoming the rate-distance limit of quantum key distribution without quantum repeaters'. *Nature* 557.7705 (2018), pp. 400–403.

[96] H.-J. Briegel et al. 'Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication: The Role of Imperfect Local Operations in Quantum Communication'. *Physical review letters* 81.26 (1998), pp. 5932–5935.

[97] Bennett et al. 'Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels'. *Physical review letters* 70.13 (1993), pp. 1895–1899.

[98] D. Boschi et al. 'Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels'. *Physical review letters* 80.6 (1998), pp. 1121–1125.

[99] D. Bouwmeester et al. 'Experimental quantum teleportation'. *Nature* 390.6660 (1997), pp. 575–579.

[100] Bennett et al. 'Concentrating partial entanglement by local operations'. *Physical Review A* 53.4 (1996), pp. 2046–2052.

[101] Bennett et al. 'Purification of noisy entanglement and faithful teleportation via noisy channels'. *Physical review letters* 76.5 (1996), pp. 722–725.

[102] Bennett et al. 'Mixed-state entanglement and quantum error correction'. *Physical Review A* 54.5 (1996), pp. 3824–3851.

[103] S. Pirandola. 'End-to-end capacities of a quantum communication network'. *Communications Physics* 2.1 (2019), p. 1023.

[104] J. Yin et al. 'Quantum teleportation and entanglement distribution over 100-kilometre free-space channels'. *Nature* 488.7410 (2012), pp. 185–188.

[105] S. Wengerowsky et al. 'Entanglement distribution over a 96-km-long submarine optical fiber'. *Proceedings of the National Academy of Sciences of the United States of America* 116.14 (2019), pp. 6684–6688.

[106] J. Yin et al. 'Satellite-based entanglement distribution over 1200 kilometers'. *Science (New York, N.Y.)* 356.6343 (2017), pp. 1140–1144.

[107] A. Boaron et al. 'Secure Quantum Key Distribution over 421 km of Optical Fiber'. *Physical review letters* 121.19 (2018), p. 190502.

[108] A. Wonfor et al. 'Quantum networks in the UK'. In: *Metro and Data Center Optical Networks and Short-Reach Links IV*. Ed. by M. Glick, A. K. Srivastava and Y. Akasaka. SPIE, 6/03/2021 - 12/03/2021, p. 4.

[109] G. Vallone et al. 'Interference at the Single Photon Level Along Satellite-Ground Channels'. *Physical review letters* 116.25 (2016), p. 253601.

[110] D. Dequal et al. 'Experimental single-photon exchange along a space link of 7000 km'. *Physical Review A* 93.1 (2016), p. 195.

[111] R. Bedington, J. M. Arrazola and A. Ling. 'Progress in satellite quantum key distribution'. *npj Quantum Information* 3.1 (2017), p. 175.

[112] S.-K. Liao et al. 'Satellite-to-ground quantum key distribution'. *Nature* 549.7670 (2017), pp. 43–47.

[113] S.-K. Liao et al. 'Satellite-Relayed Intercontinental Quantum Network'. *Physical review letters* 120.3 (2018), p. 030501.

[114] Y.-A. Chen et al. 'An integrated space-to-ground quantum communication network over 4,600 kilometres'. *Nature* 589.7841 (2021), pp. 214–219.

[115] H.-L. Yin and Y. Fu. 'Measurement-Device-Independent Twin-Field Quantum Key Distribution'. *Scientific reports* 9.1 (2019), p. 3045.

[116] K. Maeda, T. Sasaki and M. Koashi. 'Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit'. *Nature communications* 10.1 (2019), p. 3140.

[117] C. Cui et al. 'Twin-Field Quantum Key Distribution without Phase Postselection'. *Physical Review Applied* 11.3 (2019), p. 325.

[118] X. Ma, P. Zeng and H. Zhou. 'Phase-Matching Quantum Key Distribution'. *Physical Review X* 8.3 (2018), p. 325.

[119] J. Lin and N. Lütkenhaus. 'Simple security analysis of phase-matching measurement-device-independent quantum key distribution'. *Physical Review A* 98.4 (2018).

[120] M. Curty, K. Azuma and H.-K. Lo. 'Simple security proof of twin-field type quantum key distribution protocol'. *npj Quantum Information* 5.1 (2019), p. 64.

[121] X.-B. Wang, Z.-W. Yu and X.-L. Hu. 'Twin-field quantum key distribution with large misalignment error'. *Physical Review A* 98.6 (2018).

[122] M. Minder et al. 'Experimental quantum key distribution beyond the repeaterless secret key capacity'. *Nature Photonics* 13.5 (2019), pp. 334–338.

[123] M. Pittaluga et al. '600-km repeater-like quantum communications with dual-band stabilization'. *Nature Photonics* 15.7 (2021), pp. 530–535.

[124] K. A. Patel et al. 'Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber'. *Physical Review X* 2.4 (2012).

[125] K. Tamaki et al. *Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound*.

[126] H. Xu et al. 'Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate'. *Physical Review A* 101.4 (2020).

[127] C. Jiang et al. 'Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects'. *New Journal of Physics* 22.5 (2020), p. 053048.

[128] H. F. Chau. 'Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate'. *Physical Review A* 66.6 (2002), p. 802.

[129] B. E. A. Saleh and M. C. Teich. *Fundamentals of photonics*. Vol. 22. Wiley New York, 1991.

[130] G. White and G. M. Chin. 'Travelling wave electro-optic modulators'. *Optics Communications* 5.5 (1972), pp. 374–379.

[131] J. Nees, S. Williamson and G. Mourou. '100 GHz traveling–wave electro–optic phase modulator'. *IEEE Transactions on Microwave Theory and Techniques* 54.20 (1989), pp. 1962–1964.

[132] Y.-q. Lu, M. Xiao and G. J. Salamo. 'Wide-bandwidth high-frequency electro-optic modulator based on periodically poled LiNbO3'. *Applied Physics Letters* 78.8 (2001), pp. 1035–1037.

[133] C. Wang et al. 'Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages'. *Nature* 562.7725 (2018), pp. 101–104.

[134] E. L. Wooten et al. 'A review of lithium niobate modulators for fiber-optic communications systems'. *IEEE Journal of Selected Topics in Quantum Electronics* 6.1 (2000), pp. 69–82.

[135] W. Pascher et al. 'Modelling and design of a travelling-wave electro-optic modulator on InP'. *Optical and Quantum Electronics* 35.4/5 (2003), pp. 453–464.

[136] S. L. Chuang. *Physics of Photonic Devices*. 2nd ed. Wiley Publishing, 2009.

[137] M. He et al. 'High-performance hybrid silicon and lithium niobate Mach–Zehnder modulators for 100 Gbit s−1 and beyond'. *Nature Photonics* 13.5 (2019), pp. 359–364.

[138] B. Koch et al. '20 krad/s endless optical polarisation and phase control'. *Electronics Letters* 49.7 (2013), pp. 483–485.

[139] R. Ulrich and A. Simon. 'Polarization optics of twisted single-mode fibers'. *Applied optics* 18.13 (1979), pp. 2241–2251.

[140] C. A. Brackett. 'Dense wavelength division multiplexing networks: principles and applications'. *IEEE Journal on Selected Areas in Communications* 8.6 (1990), pp. 948–964.

[141] Tsbmail. *G.694.1 : Spectral grids for WDM applications: DWDM frequency grid*. 2021-06-26.

[142] R. H. Hadfield. 'Single-photon detectors for optical quantum information applications'. *Nature Photonics* 3.12 (2009), pp. 696–705.

[143] Z. Yuan et al. 'High speed single photon detection in the near infrared'. *Applied Physics Letters* 91.4 (2007), p. 041114.

[144] G. N. Gol'tsman et al. 'Picosecond superconducting single-photon optical detector'. *Applied Physics Letters* 79.6 (2001), pp. 705–707.

[145] C. M. Natarajan, M. G. Tanner and R. H. Hadfield. 'Superconducting nanowire single-photon detectors: Physics and applications'. *Superconductor Science and Technology* 25.6 (2012), p. 063001.

[146] A. E. Siegman. *Lasers / Anthony E. Siegman*. University Science Books Mill Valley, Calif, 1986.

[147] R. Lang. 'Injection locking properties of a semiconductor laser'. *IEEE Journal of Quantum Electronics* 18.6 (1982), pp. 976–983.

[148] E. K. Lau, L. J. Wong and M. C. Wu. 'Enhanced Modulation Characteristics of Optical Injection-Locked Lasers: A Tutorial'. *IEEE Journal of Selected Topics in Quantum Electronics* 15.3 (2009), pp. 618–633.

[149] Z. Liu and R. Slavik. 'Optical Injection Locking: From Principle to Applications'. *Journal of Lightwave Technology* 38.1 (2020), pp. 43–59.

[150] M. Bennett et al. 'Huygens's clocks'. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 458.2019 (2002), pp. 563–579.

[151] Z. Yuan et al. 'Directly Phase-Modulated Light Source'. *Physical Review X* 6.3 (2016), p. 325.

[152] G. L. Roberts et al. 'Experimental measurement-device-independent quantum digital signatures'. *Nature communications* 8.1 (2017), p. 1098.

[153] G. L. Roberts et al. 'Modulator-Free Coherent-One-Way Quantum Key Distribution'. *Laser & Photonics Reviews* 11.4 (2017), p. 1700067.

[154] G. L. Roberts et al. 'Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution'. *Applied Physics Letters* 111.26 (2017), p. 261106.

[155] G. L. Roberts et al. 'A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution'. *New Journal of Physics* 3.4 (2018), p. 045010.

[156] P. Horowitz and W. Hill. *The art of electronics*. 2nd ed. Cambridge England and New York: Cambridge University Press, 1989.

[157] D. R. Stephens. *Phase-Locked Loops for Wireless Communications: Digital and Analog Implementation*. Boston, MA and s.l.: Springer US, 1998.

[158] R. E. Best. *Phase-locked loops: design, simulation, and applications*. McGraw-Hill Education, 2007.

[159] A. C. Bordonalli, C. Walton and A. J. Seeds. 'High-performance phase locking of wide linewidth semiconductor lasers by combined use of optical injection locking and optical phase-lock loop'. *Journal of Lightwave Technology* 17.2 (1999), pp. 328–342.

[160] N. Satyan. 'Optoelectronic control of the phase and frequency of semiconductor lasers'. PhD thesis. California Institute of Technology, 2011.

[161] K. Balakier et al. 'Integrated Semiconductor Laser Optical Phase Lock Loops'. *IEEE Journal of Selected Topics in Quantum Electronics* 24.1 (2018), pp. 1–12.

[162] K. Ogata. *Modern control engineering*. 5th ed. Prentice-Hall electrical engineering series. Instrumentation and controls series. Boston: Prentice-Hall, 2010.

[163] B. C. Kuo and M. F. Golnaraghi. *Automatic control systems*. 8th ed. / Benjamin C. Kuo, Farid Golnaraghi. Hoboken and Chichester?: Wiley, 2003.

[164] International Telecommunication Union. *G.694.1 : Spectral grids for WDM applications: DWDM frequency grid*. 2020-10-02.

[165] Z. Yuan et al. 'Robust random number generation using steady-state emission of gain-switched laser diodes'. *Applied Physics Letters* 104.26 (2014), p. 261112.

[166] M. Jofre et al. 'True random numbers from amplified quantum vacuum'. *Optics express* 19.21 (2011), pp. 20665–20672.

[167] L. C. Comandar et al. 'Near perfect mode overlap between independently seeded, gain-switched lasers'. *Optics express* 24.16 (2016), pp. 17849–17859.

[168] M. Koashi. 'Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse'. *Physical review letters* 93.12 (2004), p. 120501.

[169] Z. Cao et al. 'Discrete-phase-randomized coherent state source and its application in quantum key distribution'. *New Journal of Physics* 17.5 (2015), p. 053014.

[170] 'ITU-T/FSAN PON Protocols: 4'. In: *Broadband Access*. John Wiley & Sons, Ltd, 2014, pp. 77–114.

[171] J. A. Buck. *Fundamentals of Optical Fibers*. Wiley Series in Pure and Applied Optics. Wiley, 2004.

[172] J. M. Senior. *Optical Fiber Communications: Principles and Practice*. Prentice Hall Internacional series in optoelectronics. Financial Times/Prentice Hall, 2009.

[173] X. Zhong et al. 'Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution'. *Phys. Rev. Lett.* 123.10 (2019), p. 100506.

[174] X. Zhong et al. *Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses*.

[175] Y. Liu et al. 'Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending'. *Physical Review Letters* 123.10 (2019).

[176] X.-T. Fang et al. 'Implementation of quantum key distribution surpassing the linear rate-transmittance bound'. *Nature Photonics* 14.7 (2020), pp. 422–425.

[177] J.-P. Chen et al. 'Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km'. *Phys. Rev. Lett.* 124.7 (2020), p. 070501.

[178] S. Wang et al. 'Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System'. *Physical Review X* 9.2 (2019).

[179] B. Culshaw. 'The optical fibre Sagnac interferometer: an overview of its principles and applications'. *Measurement Science and Technology* 17.1 (2006), R1–R16.

[180] D. Calonico et al. 'High-accuracy coherent optical frequency transfer over a doubled 642-km fiber link'. *Applied Physics B* 117.3 (2014), pp. 979–986.

[181] K. Predehl et al. 'A 920-kilometer optical fiber link for frequency metrology at the 19th decimal place'. *Science (New York, N.Y.)* 336.6080 (2012), pp. 441–444.

[182] S. M. Foreman et al. 'Remote transfer of ultrastable frequency references via fiber networks'. *The Review of scientific instruments* 78.2 (2007), p. 021101.

[183] F. Riehle. 'Optical clock networks'. *Nature Photonics* 11.1 (2017), pp. 25–31.

[184] F. Bondu et al. 'Ultrahigh-spectral-purity laser for the VIRGO experiment'. *Optics Letters* 21.8 (1996), pp. 582–584.

[185] R. W. P. Drever et al. 'Laser phase and frequency stabilization using an optical resonator'. *Applied Physics B* 31.2 (1983), pp. 97–105.

[186] E. D. Black. 'An introduction to Pound–Drever–Hall laser frequency stabilization'. *American Journal of Physics* 69.1 (2001), pp. 79–87.

[187] C. E. Calosso et al. 'Frequency transfer via a two-way optical phase comparison on a multiplexed fiber network'. *Optics Letters* 39.5 (2014), pp. 1177–1180.

[188] C. E. Calosso et al. 'Doppler-stabilized fiber link with 6 dB noise improvement below the classical limit'. *Optics Letters* 40.2 (2015), pp. 131–134.

[189] G. C. Lorenzo et al. *Tight finite-key security for twin-field quantum key distribution.*

[190] C. Jiang et al. 'Unconditional Security of Sending or Not Sending Twin-Field Quantum Key Distribution with Finite Pulses'. *Physical Review Applied* 12.2 (2019), p. 024061.

[191] Z.-W. Yu et al. 'Sending-or-not-sending twin-field quantum key distribution in practice'. *Scientific reports* 9.1 (2019), p. 3080.

[192] D. Gottesman, T. Jennewein and S. Croke. 'Longer-baseline telescopes using quantum repeaters'. *Physical review letters* 109.7 (2012), p. 070503.

[193] J. M. Arrazola and N. Lütkenhaus. 'Quantum fingerprinting with coherent states and a constant mean number of photons'. *Physical Review A* 89.6 (2014), p. 062305.

[194] F. Xu et al. 'Experimental quantum fingerprinting with weak coherent pulses'. *Nature communications* 6 (2015), p. 8735.

[195] X. Zhong et al. *Efficient experimental quantum fingerprinting with wavelength division multiplexing.*

[196] R. Sagar. 'Mosca's Inequality And Its Effect On Quantum Cryptography -AIM'. *Analytics India Magazine* (1/02/2019).

[197] H. Liu et al. 'Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km'. *Physical Review Letters* 126.25 (2021).

[198] J.-P. Chen et al. 'Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas'. *Nature Photonics* 299 (2021), p. 1476.

[199] P. Sibson et al. 'Chip-based quantum key distribution'. *Nature communications* 8 (2017), p. 13984.

[200] D. Bunandar et al. 'Metropolitan Quantum Key Distribution with Silicon Photonics'. *Physical Review X* 8.2 (2018).

[201] T. K. Paraïso et al. 'A modulator-free quantum key distribution transmitter chip'. *npj Quantum Information* 5.1 (2019), p. 145.

[202] I. de Marco et al. 'Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter'. *Optica* 8.6 (2021), p. 911.

[203] S. Pirandola and S. L. Braunstein. 'Physics: Unite to build a quantum Internet'. *Nature* 532.7598 (2016), pp. 169–171.

[204] S. Wehner, D. Elkouss and R. Hanson. 'Quantum internet: A vision for the road ahead'. *Science (New York, N.Y.)* 362.6412 (2018).

[205] M. Pompili et al. 'Realization of a multinode quantum network of remote solid-state qubits'. *Science (New York, N.Y.)* 372.6539 (2021), pp. 259–264.

style=numeric-comp