Quantum key distribution beyond the repeaterless secret key capacity

Mariella Minder

Department of Engineering
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Trinity College August 2020

I would like to dedicate this thesis to my parents and grandparents...

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Mariella Minder
August 2020

Acknowledgements

I would like to begin by thanking my academic supervisor, Seb Savory, and my industrial group leader, Andrew Shields, for giving me the opportunity to conduct high impact research at the University of Cambridge and Toshiba CRL. Thank you Seb for the insightful advice and your willingness to always protect your students.

I cannot express how grateful I am to all the researchers at Toshiba for their continuous support and pleasant spirit. I am especially thankful to my supervisor and mentor, Marco Lucamarini. Thank you for using so much of your time to teach me, for always prioritising knowledge and for believing in me enough to hand me your most beloved project. To Zhiliang Yuan, I am thankful for setting the example of an excellent experimentalist and for his willingness to jump in the lab and help whenever I was in distress. I will be privileged if I become half the scientist you are.

In my years at Toshiba I have been surrounded by kind people who made our work place feel like home. Special mentions go to Mirko Pittaluga, my lab partner in crime; George Roberts for teaching me probably everything I know about the lab; Andrea Barbiero for being the best cubicle mate, friend and dance partner anyone could ever ask for. Innocenzo, Matthew, Ziheng, Jonathan, Christiana, Bruno and Jamie for sharing with me all the PhD ups and downs and filling my postgraduate life with unforgettable memories and experiences. Finally, Amos Martinez, for all the funny moments and his major networking skills.

I was only able to get here today because of my family. I am infinitely grateful to my mother for believing in my aptitudes, pushing me to aim higher and always prioritising my needs before hers. To my dad, thank you for the love you nested in my for the sciences when I was a kid tinkering in your lab. Στον παππού και τη γιαγιά μου, Ανδρέα και Μαρούλλα, δυό φορές γονείς μου, είμαι αιώνια ευγνώμων για την άνευ όρων αγάπη τους και τη συνεχή τους προθυμία να με στηρίξουν με ό,τι έχουν. Last but certainly not least, I have to thank my partner and my inspiration, Christos. I did all of this so you could call me Doctor.

Abstract

Quantum communications promise to provide information theoretic security in the exchange of information. However, unlike their classical counterpart, they utilise dim optical pulses whose amplification is prohibited. Consequently, their transmission rate and range is confined below a theoretical limit known as repeaterless secret key capacity. Overcoming this limit with today's technology was believed to be impossible until the recent proposal of Twin-field (TF) quantum key distribution (QKD), a scheme that uses phase-coherent optical signals and an auxiliary measuring station to distribute quantum information. Here, TF-QKD and its main variations are initially explored and compared in simulations, to assess their performance in different attributes. Such schemes are also practically implemented for the first time in two experiments. The first is a proof-of-principle implementation over significant channel losses, in excess of 90 dB. In the second, the setup is developed further and the protocol is implemented over real fibre channels exceeding 600 km in length, representing the first fibre-based secure quantum communication beyond the barriers of 600 km and 100 dB. In both cases, in the high loss/distance regime, the resulting secure key rates exceed the repeaterless secret key capacity, a result never achieved before. These achievements represent a major step in promoting quantum communications as a dependable resource in today's world.

List of Publications

Work published in journals as an outcome of the research carried out during this Ph.D.:

- **Minder, M.**, Pittaluga, M., Roberts, G. L., Lucamarini, M., Dynes, J. F., Yuan, Z. L., & Shields, A. J. (2019). *Experimental quantum key distribution beyond the repeaterless secret key capacity*. Nature Photonics, 13(5), 334-338.
- Roberts, G. L., Pittaluga, M., **Minder, M.**, Lucamarini, M., Dynes, J. F., Yuan, Z. L., & Shields, A.J. (2018). *Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution.* Optics Letters, 43(20), 5110.
- Pittaluga, M., **Minder, M.**, Lucamarini, M., Woodward, R.I., Sanzaro, M., Yuan, Z. L., & Shields, A. J. (2020). *Repeater-like experimental quantum communications over 600 km of optical fibre with two-stage phase-stabilisation* (joint first author), [Out for review in Nature Photonics]
- Woodward, R.I., Lo, Y.S., Pittaluga, M., **Minder, M.**, Paraiso, T., Lucamarini, M., Sanzaro M., Yuan, Z. L., & Shields, A. J. (2020). *Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers*, [Submitted to PRL]

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Cryptography

Currently, 2.5×10^{18} bytes of data are generated daily, with this number only increasing with time, as shown by the Data Never Sleeps project [4]. Almost at its entirety, this data, is exchanged over public channels. As a natural repercussion, the development and implementation of fast communication systems which guarantee secure exchanges is becoming an increasingly vital task.

The choice of public channels is one of practicality and comes at the cost of security. Authorised users exchanging private information over such channels run the risk of adversary third parties gaining knowledge, of all or part of the information, undetected. This is of particular concern in transactions involving authorities such as governments, hospitals, militaries and banks, where the data transmitted is highly sensitive. It therefore comes as no surprise that modern communications go hand in hand with cryptography, the science concerned with developing techniques for the authentication of authorised users and data, and for maintaining the confidentiality of information travelling through channels, as to prevent leakage of information [5].

Encryption is the main ingredient of all cryptosystems. It is the process in which a sender, Alice, uses a *key* to encode her *plaintext* message into an unintelligible form, known as *ciphertext*, before allowing it to travel through the channel. The encryption key should only be known to authorised users. In this manner, a nefarious third party, referred to as Eve,

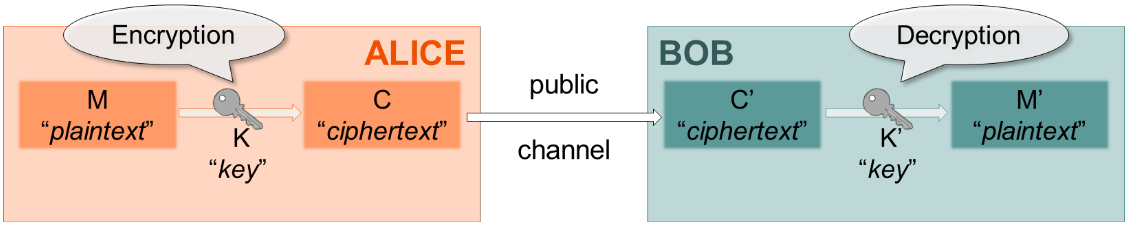

Figure 1.1 **A cryptographic process:** Alice encodes her plaintext message, M, with a key, K. She sends the resulting ciphertext, C, to Bob over a public channel. Bob will receive a ciphertext C' and will use a key K' to decrypt it into a plaintext M'.

interfering with the transmission, cannot infer the true content of the message. However, the authorised receiver, Bob, also having knowledge of the key, can decrypt the ciphertext back to its original form and read the contents of the message [5]. This process is explained schematically in figure 1.1.

Cryptosystems are susceptible to various types of attacks. Eve could directly gather plaintext or ciphertext or she could plant data to control and guide the procedure. In certain instances she can take advantage of imperfections in the physical systems responsible for encryption and decryption, known as side channels, to gain information. Security is the most vital attribute of a cryptosystem and hence it is crucial that possible attacks are minimised. This can be achieved by eliminating side channels, implementing attack countermeasures or evolving encryption protocols to increase their robustness. An ideal cryptosystem would be one whose security is unbreakable.

Algorithms used in cryptosystems belong to families of reversible transformations. These are conventionally considered as publicly available information for any cryptosystem, even though it is common for many cryptographers to keep them private nonetheless. Thus, the security of these transformations, or protocols, fully depends on the confidentiality of the enciphering key. Consequently, a protocol is only secure if Eve is unable to decrypt the ciphertext without knowing the key [5].

We can quantify the security of cryptographic protocols by classifying them in two categories: *information-theoretically secure* and *computationally secure*. The first category is compatible with Shannon's theory [6] and includes any protocol that remains secure irrespective of Eve's computational power. On the other hand, the latter, refers to any protocol that remains secure under the assumption that Eve's computational power is limited by current technology [5].

1.1.1 Conventional cryptography and the BB84 protocol

Encryption systems in conventional cryptography are divided in two categories depending on the enciphering key being either private or public [7]. Taking the simplest one, private key cryptography describes the case where the same key is used for both encryption and decryption. In the scheme found in figure 1.1, if $K = K'$, then the encryption is symmetric. In such cases, there evidently exists a need for a private and secure channel connecting the authorised users over which the key can be distributed, unless the users are to do this in person. This is known as the key exchange problem and it is intrinsic to private cryptography [8]. The Advanced Encryption Standard (AES) [9] is a significant example of this category of protocols. It is classified as computationally secure and its deciphering, for a 128-bit key, would take on average 10^{18} years [10].

The key exchange problem was solved with the discovery of public key cryptography, which gets rid of the need for a pre-shared secret key. Instead, users have a pair of keys: their own secret key, *sk*, and an associated public key, *pk*, known to Eve [10]. Public keys have to belong to the family of "trap-door one-way functions" [11]. This name derives from the complexity of calculating the inverse of such functions, when the computational power is limited by current technology. In such functions, this calculation is highly inefficient. However given some "trap-door" information, in this case the *sk* key, the inverse of the function can be swiftly calculated. Hence, for Alice to securely send a message to Bob, she will have to encrypt her message using Bob's *pk* key. Bob will in turn use his *sk* key to decrypt the original message. Thus now, in figure 1.1, $K \neq K'$. One of the currently most used public key cryptosystems is the RSA algorithm which is based on the complexity of factoring large semi-prime numbers [12].

Both the symmetric and asymmetric methods (equivalent to private and public respectively) in modern cryptography have major drawbacks. The necessary initial step for a symmetrically encrypted exchange to take place is the distribution of a secret key over a secure channel. In the real world, it is impossible to characterise any classical channel as such. The mere possibility of any channel being tampered with always exists and therefore the security of private key cryptography cannot be guaranteed [13]. On the other hand, public key cryptography uses algorithms that are only computationally secure. In the event that Eve gains a significant boost in her computational capabilities, the security of any such protocol collapses. To exploit both methods given their distinct weaknesses, they can be implemented together. Asymmetric cryptography can be used to distribute a key between Alice and Bob at the beginning of the communication. Symmetric cryptography can then be implemented to exchange a secret message. The concern of security nevertheless remains. The aforementioned trap-door one-way functions of public cryptography are only computationally secure and an evolved algorithm of increased efficiency could be devised and allow Eve to hack the secret key distribution.

An unconditionally secure encryption protocol was devised by V. A. Kotelnikov in 1941 during World War II and is known as the one-time pad (OTP). His original report remains classified to this day. In earlier work dating back to 1926, G. S. Vernam also refers to similar one-time ciphers [14]. The idea of such schemes is the use of randomly generated keys for encryption, where these keys are to be used solely once and then discarded and which are of at least equal length to the message. Randomness, length and single use of keys are three of the requirements for a cipher to be classified as unbreakable under any condition. The latter guarantees that no parts of the key will be repeated throughout the ciphertext eliminating all chances of Eve gaining information about it. These conditions must be accompanied by the previously mentioned secrecy of the key [13]. The OTP is directly comparable to symmetric key cryptography as it also aims used for message encryption rather than key distribution.

The unconditional security, information-theoretic security or "*perfect secrecy*" of the OTP was originally proved by Shannon [6] (see also ref. [15]). Assuming Eve has unlimited computational efficiency, she can apply a brute-force attack on the ciphertext, trying all possible keys and keeping every meaningful message she retrieves. As the amount of ciphertext she intercepts increases, the number of meaningful messages decreases until only one solution exists. Shannon refers to this amount of ciphertext as the unicity distance N_0 and defines it for a random cipher as:

$$N_0 = \frac{H(K)}{D} \tag{1.1}$$

where $H(K)$ is the information entropy of the key and D is the redundancy of the message's language. To obtain a unique solution in any problem, the unknowns must be less or equal to the number of equations involving them. In this case, the entropy of the key is equivalent to the number of unknowns in binary, while we can think of the multiple of the redundancy and the amount of ciphertext available to Eve as equivalent to the number of equations. Thus, for a sole solution:

$$H(K) \leq N_0 D \tag{1.2}$$

For the OTP it is trivial that $H(K) \rightarrow \infty$ and as a result $N_0 \rightarrow \infty$ [5]. Unless one possesses the secret key, and given that this key was generated via a truly random process, there is no way to perform successful cryptanalysis on the ciphertext. Consequently, the need for an unconditionally secure key distribution method remains the main hindrance in employing practical unbreakable cryptosystems.

1.1.2 Quantum cryptography and the BB84

Currently, the only information-theoretically secure solution to the key exchange problem exploits properties of quantum mechanics. This is known as quantum cryptography. It was first introduced in 1970 by S. Wiesner but was only published over a decade later [16]. This was followed by the publication of the first quantum key distribution (QKD) protocol the year after, by Charles Bennett and Gilles Brassard [17]. The unconditional security of QKD is guaranteed by the very laws of quantum mechanics. It generates truly random keys and distributes them between authenticated users over public channels, while giving these users the ability to detect the presence of Eve in the case that enough information was leaked to render the exchange insecure. It is consequently ideal for the implementation of the OTP scheme.

General principles of quantum mechanics form the foundation of QKD. These include the no-cloning theorem, the Heisenberg uncertainty principle (HUP) [18], the phenomenon known as entanglement and the non-orthogonality of quantum states. In this section emphasis if given to the first two principles, while entanglement will be explored in section 1.2.2. The no-cloning theorem was proven by Wootters and Zurek in 1982 [19]. They showed that an arbitrary unknown quantum state cannot be cloned due to the linearity of quantum mechanics and therefore the perfect, deterministic amplification of quantum states, is forbidden. The HUP principle states that it is impossible to measure, with full precision, a pair of non-commuting properties or complementary variables of a particle. Obtaining information about one variable comes at the expense of introducing an error in the measurement outcome of its pair. This principle is directly related to the no-cloning theorem since a classical measurement can be described as a repeated cloning operation.

These principles complement one another in providing information-theoretic security for QKD. Let's assume that the two classical bits, [0, 1], are to be encoded on complementary variables of particles. For this, a quantum two-state system is necessary. Such systems are known as qubits (quantum bits) and their general form is given below in Dirac notation [20]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.3}$$

where α (β) is the probability amplitude of state $|0\rangle$ ($|1\rangle$). In the BB84 proposal, polarisation states of single photons are used as qubits. The rectilinear and the diagonal bases are used, in each of which two orthogonal states represent the two bits. In the rectilinear (diagonal) basis, horizontally (diagonally) polarised photons represent bit 0, while vertically (anti-diagonally) polarised photons represent bit 1, or vice versa. Alice randomly selects the basis and bit to be encoded on single photons she will be sending to Bob. In the same way, Bob randomly selects the bases in which he will measure the received encoded photons. If Bob selects the correct basis, and considering a perfect measurement, he will deterministically obtain the bit value encoded by Alice. Since the two bases are complementary variables, the HUP applies, and if Bob chooses the wrong basis he will obtain a random result. Such instances are removed during *sifting*, a process where Alice and Bob announce, over a public classical channel, information about their encoding. In the case of the BB84 protocol, they announce the bases in which they encoded/measured the photons and only keep bits acquired when they have both used the same basis. The no-cloning theorem protects the authorised users when making such announcements. A malicious adversary, usually denoted as Eve, cannot make a copy of a photon without measuring and hence collapsing the state of the original photon. If she could, she would send the original photons over to Bob while storing her copies in a quantum memory. She would then wait until the classical announcement is finished to measure all photons in the correct bases and obtain 100% information about the bit-string shared by Alice and Bob.

Error estimation follows sifting. Authorised users must always assume Eve is attempting to gain information about their secret key exchange. Any measurement she performs on the exchanged photons will introduce errors between the sifted keys of Alice and Bob. To examine this, the users randomly select, announce and throw away a subset of the sifted bit-string. They use the error of this subset as an estimation for the overall error in the total sifted string. Every protocol has a theoretical upper limit to this error. If the measured error exceeds this value, the exchange was not secure and it is aborted. However, in a practical implementation, the system is imperfect and subject to various noise sources. Hence even at the absence of an eavesdropper the error value will always be finite. Nevertheless, during security analysis, the worst-case scenario is always considered and all errors must be attributed to Eve. It is now evident how the principles of quantum mechanics form the basis for the information-theoretic security of QKD. An example of a BB84 exchange is drawn out in table 1.1.

Alice's bases	R	D	D	D	R	D	R	R	D	R
Alice's bits	0	1	0	1	0	1	0	0	1	1
Alice's encoded state	↑	↗	↗	↖	→	↖	→	→	↖	↑
Bob's bases	D	D	D	R	D	R	D	R	R	R
Bob's raw key	0	1	0	0	1	0	0	0	0	0
Alice's sifted key	-	1	0	-	-	-	-	0	-	1
Bob's sifted key	-	1	0	-	-	-	-	0	-	0

Table 1.1 **BB84 protocol:** This is an example of a key exchange using the BB84 protocol with information encoded on the polarisation states of single photons. R: Rectilinear basis, D: Diagonal basis. Here bit 0 (1) corresponds to the vertical(horizontal) state in the R basis and to the diagonal (anti-diagonal) state in the D basis. The error in the sifted key is $\frac{1}{4}$ and is attributed to Eve.

1.2 Beyond the BB84 protocol

BB84 is the first and simplest example of a QKD protocol. Since its proposal many have followed, including methods for improving the practicality of quantum communication schemes. Although many are quite similar to the BB84, some take advantage of further quantum phenomena like entanglement, to introduce new characteristics to the schemes, or to elevate their security. Different protocols have different benefits and drawbacks, and for every implementation there is one that fits the best. Aptitudes of protocols range from reaching longer distances and achieving higher rates, to providing unconditional implementation security, resilience to noise or simplification of the hardware required.

QKD protocols belong in one of two categories: discrete variable (DV) or continuous variable (CV). As the names suggest, the first category refers to protocols where information is encoded on discrete properties of single photons, just like in the BB84. Instead, in the latter, information is encoded on continuous variables of light utilising, for example, the phase and amplitude quadratures as complementary variables. CV-QKD is particularly promising due to its similarity with current optical telecommunications, based on coherent detectors. Single-photon detectors (SPDs), vital for DV-QKD, are replaced by heterodyne or homodyne detection techniques [21]. However, due to its intrinsic intolerance to noise, the maximum transmission distance of CV-QKD is limited. The distance record for experimental CV-QKD in-fibre was for many years 100 km [22]. Recently, a demonstration successfully doubled up the distance to a record of 203 km in fibre [23]. Even so, field tests in fibre links have only managed to distribute a key over a maximum of 50 km [24].

On the other hand, even though DV-QKD has been able to successfully distribute keys over lossier channels, distance still remains one of its main drawbacks when compared to its conventional counterpart. Information must be carried by single photons whose amplification is restricted by the no-cloning theorem. Losses in the channel impose the maximum distance of DV-QKD. In conventional communications, not only is bright light used, but also signal amplifiers are a standard component of every system. These extend the maximum distance for conventional communications to be arbitrary. Nevertheless, even with these stringent restrictions, it will be shown in section 1.4.3 that DV-QKD protocols have been able to reach the realistically required distances if they were to be integrated in the conventional infrastructure and utilised commercially. This key achievement, combined with DV-QKD's comparative robustness against noise and its advanced state-of-art, render it favourable over CV-QKD for the time being.

Aforementioned distance examples refer to QKD performed over optical fibre links. Distance however can be arbitrary and depends on the nature of the quantum channel connecting the users and its characteristic loss. Fibre is made of silica and hence permits the transmission of light with minimal losses and with robustness against decoherence. Standard telecommunication single-mode fibre has an attenuation coefficient of 0.20 dB/km at 1550 nm and is widely used in current infrastructure for commercial conventional communication. Due to the detrimental effects loss has on a QKD implementation, lower loss coefficient fibres are highly desirable. Currently, the most efficient silica fibres have a loss coefficient of 0.14 dB/km [25]. Due to the recency of this development, these low-loss fibres are not generally available. Instead, the latest QKD experiments have been using what is referred to as ultra-low-loss fibre (ULL) that has a loss coefficient of 0.16 dB/km [26, 27].

The alternative to in-fibre QKD is free-space QKD. Air itself, depending on wavelength, has a much smaller loss coefficient per km than fibre. In free-space implementations, wavelengths around 800 nm are used to minimise this attenuation, but also avoid cross-contamination with other sources of light [28] . If the implementation is done over satellite, then no losses affect the beam after it exits the first 10 km of the atmosphere [29] and enters the negligible density zone or vacuum space. Although vacuum space does not incur losses per se, diffraction of the beam is an unavoidable phenomenon that causes a major issue in any free space implementation and will account for losses. Nevertheless, much longer distances can still be reached when QKD is implemented over satellite. For example, a 1200 km satellite link could have the same loss as a 250 km ultra-low loss fibre link. Nevertheless this improvement comes with a trade-off. As aforementioned, contamination is a major issue. Strong daylight increases the QKD noise to levels that are not tolerable thus forcing the vast majority of current demonstrations to be performed at night. There have been however recent developments in which, not only was free-space QKD achieved during daylight but also utilising C-band wavelengths, showing compatibility of free-space systems with underlying fibre infrastructure [30]. Finally, atmospheric turbulence is an enemy of any free-space QKD implementation, where stability is of the utmost importance, requiring development and integration of robust and accurate tracking systems.

1.2.1 Decoy states and weak coherent pulses

As mentioned in section 1.2, the biggest hurdle in QKD is tolerating high-loss in a quantum channel. The attenuation of the channel directly limits the maximum distance achievable in quantum communications while high loss can also compromise security as it can be exploited to attack a practical QKD system. Most of practical QKD systems adopt weak coherent pulses (WCPs) as a source of light. WCPs are highly attenuated laser pulses, so that the average number of photons per pulse is reduced to be less than one. They are used as a practical work-around to pure single-photon sources which, due to their high repetition rate, integrability and simplicity of use. In fact, WCPs have been proven to have a significant performance advantage over single-photon sources [31–34]. Practical examples of QKD performed with single-photon sources, show poor performance in implementations in terms of both key rates and distances [35, 36].

Laser pulses follow a Poissonian distribution and hence the probability of having n number of photons in a pulse, $P(n)$ is formulated by:

$$P(n) = \frac{\mu^n e^{-\mu}}{n!} \tag{1.4}$$

where μ is the average number of photons per pulse, known as the photon flux. With the aid of figure 1.2, the Poissonian behaviour of WCPs is visualised. It is clear that lower fluxes maximise the probability of a vacuum or single-photon state, while they minimise multi-photon probabilities.

Nevertheless, the probability of multi-photon pulses remains finite and such pulses will cause security implications when observed in a QKD exchange. Specifically, Eve can take advantage of their presence in the high-loss regime to perform an attack known as photon number splitting (PNS) [37]. We assume that Bob uses SPDs which cannot resolve the photon number of the incident pulses. Eve intercepts the quantum channel and measures the number of photons in each pulse. Whenever she detects a multi-photon pulse she stores one

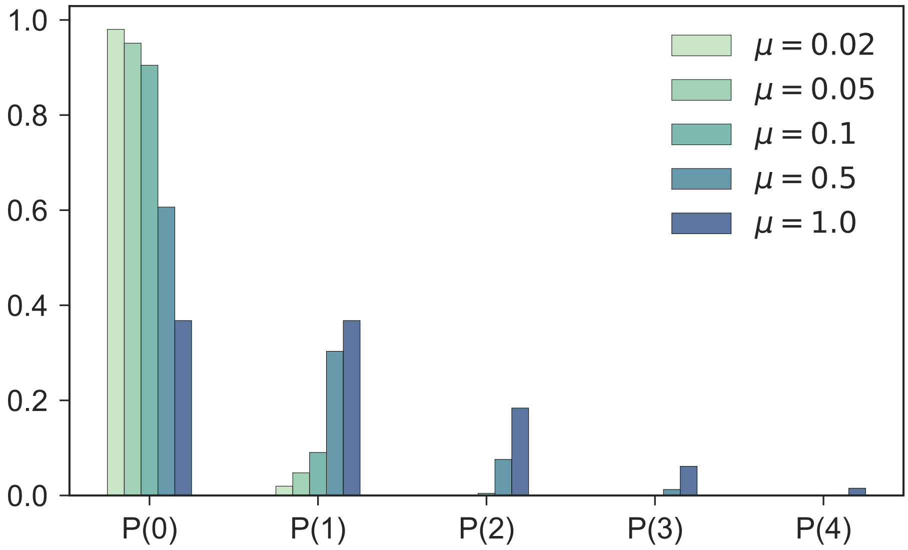

Figure 1.2 **Photon-number distribution of pulses:** Weak coherent pulses follow the Poisson distribution. Here the probabilities of 0 to 4 photons in a pulse are plotted for varying average photon number, or flux, μ.

photon and sends the rest to Bob. Single-photon pulses on the other hand, are always blocked. Therefore, if Eve adopts this strategy while the channel transmission is less or equal to the probability of sending a multi-photon pulse, then the attack will go undetected [38] as all losses will be attributed to the efficiency of the channel. The PNS attack dramatically reduces the maximum secure distance for the BB84 protocol implemented with non deterministic sources down to 24 km [32].

To overcome this limit, a technique known as the decoy state method was proposed [38–40], a method that is essential to guarantee the security of practical, long distance QKD. Alice sends signal WCPs or pulses from her imperfect single-photon source. She also deliberately sends decoy states which must be indistinguishable from signal states in every degree of freedom other than the photon flux. For Eve, these are impossible to distinguish from signal pulses. As a result, if Eve proceeds with the PNS attack, the yields of the signal and decoy states will become identical. If Alice and Bob announce the instances where signals and decoys were sent, they can monitor their yields and immediately detect Eve's presence [38, 39]. Consequently, the maximum loss over which a secure distribution can take place is increased. In the case of the BB84 protocol, the improvement is from few tens of km to hundreds of km [38–40], while if the choice of decoy or signal is biased, then the key rate can get a 45% boost [41]. In fact, it is shown that the decoy state method successfully improves not only the loss tolerance of the BB84 protocol, but of any DV-QKD protocol it is applied to.

Essential to the security of any protocol with coherent pulses and decoy states is phase randomisation. A weak coherent state of phase theta, $|\sqrt{\mu}e^{i\theta}\rangle$ is described by:

$$|\sqrt{\mu}e^{i\theta}\rangle = e^{-\frac{|\sqrt{\mu}e^{i\theta}|2}{2}} \sum_{n=0}^{\infty} \frac{\left(\sqrt{\mu}e^{i\theta}\right)^n}{\sqrt{n!}} |n\rangle \tag{1.5}$$

where $e^{i\theta}$ is the phase of the emitted pulse and $|n\rangle$ is the state containing n number of photons. When the phase is uniformly and randomly distributed and no information about it is available to an eavesdropper, then he observes a source emitting:

$$\rho(\mu) = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n| \tag{1.6}$$

and hence the source is indistinguishable from a mixed photon number Poisson emitter [39]. This entails that Eve cannot distinguish between a phase-randomised source of WCPs and an emission of photon number states. We can then adopt the description of photon number states and use it to study the robustness of the QKD protocol to the PNS attack.

1.2.2 Entanglement based schemes

In 1991, seven years after the publication of the BB84 protocol, Arthur Ekert used the Einstein-Podolsky-Rosen (EPR) *gedanken experiment* [42] as the basis for a new QKD protocol, now known as the E91 [43]. With the proposal of the E91 a new family of QKD protocols emerged, known as entanglement-based QKD. Entanglement is a phenomenon of quantum mechanics which describes instant correlations that can arise between particles separated by arbitrary distances. If such correlations are in place for a group of particles in a superposition state, then measuring one of them will cause the wavefunction collapse of every particle in that ensemble. The results of the collapse are not random but are in fact directly correlated to the result obtained from the initial measurement. In this manner, information is distributed to particles with an arbitrary space separation. The fundamental difference between the E91 and previous protocols is the exploitation of these quantum correlations for the distillation of the key.

The scheme is explained in its simplest form in figure 1.3. An entangled-pair of photons is produced and distributed to Alice and Bob so that each end up with one entangled

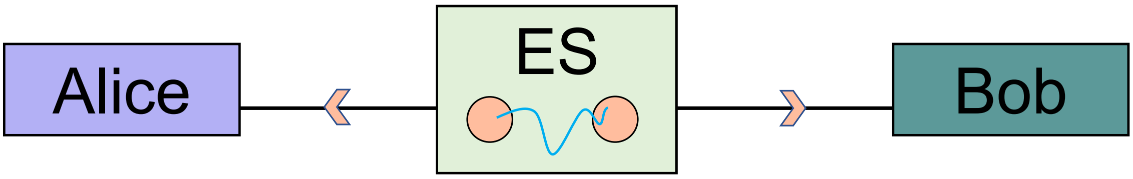

Figure 1.3 **Entanglement based QKD:** An entangled photon pair source (ES) distributes entangled pairs to Alice and Bob. They will independently and randomly choose a basis in which to measure the received photon. With classical announcements they will form a key from the values that have occurred from matching basis choices.

photon. They will each measure these photons in their basis of independent random choice, repeating the process many times. This will be followed by the sifting of the bases through announcements over classical channels. Thus, due to the classical announcements, although entanglement effects are instant, the speed of the key distribution is still limited by the speed of light. Since the source of entangled photons can be outside the stations of the authorised users, Alice and Bob need to test whether the received particles were, in point of fact, entangled. For this, they must test whether the John Clauser, Michael Horne, Abner Shimony, and Richard Holt (CHSH) inequality [44] is violated. This is a generalised version of a practical test for Bell's inequality [45] that is only violated when the examined particles are entangled. A Bell test involves observing coincidence counts in the detectors of Alice and Bob after the photons pass through polarising beam splitters. Depending on which pair of detectors the coincidence counts are observed on, the initial superposition state of entanglement can be deduced out of four possible *Bell states* [46]. Hence the type of correlation between the user's measurements is also deduced. The state-of-art of such protocols will be outlined in 1.4.2.

1.2.3 Measurement-device-independent QKD

With an increased interest in experimental QKD, it became obvious that the development of technologies for entanglement generation, distribution and successful teleportation was much too challenging and not yet feasible. As a result, BB84-type protocols were, and still are, favoured since they can be implemented with current technology. Research also focused on uncovering the weak-points of practical QKD which make it deviate from information-theoretic security. Hacking attempts on systems revealed loop-holes that could be exploited and specific strategies were developed that could render a practical system fully susceptible to an eavesdropper. It is clearly seen that most attacks take advantage of imperfections in the detectors [47, 48] and hence the Achilles' heel of a QKD system is its measurement station [49, 50].

Security issues related to detector attacks were solved in the proposal of a practical entanglement-based protocol known as Measurement-Device-Independent (MDI)-QKD [51], see also [52]. MDI-QKD was published in 2012, over a decade after Ekert proposed the E91, by Lo, Curty and Qi. As the name suggest, the security of the key in an MDI-QKD scheme is fully independent of the measurement device, including the detector. In this protocol, as shown in figure 1.4, the established Alice-Bob scheme is replaced by a three node architecture, in which Alice and Bob communicate through a third untrusted node, Charlie. Alice and Bob will both choose random bases and bits to encode on single photons or WCPs. In MDI-QKD demonstrations, polarisation encoding has been preferred in the past years [53–55] with a few experiments using time-bin encoding instead [56]. The decoy-state method must still be implemented and hence, following bit encoding, the two users randomly select the intensity of each pulse [57]. As shown in figure 1.4, they will both send the prepared pulses to travel through quantum channels that connect each of them to Charlie.

MDI is not an entanglement based protocol in the traditional sense as it poses no requirement for an entangled particle source or entanglement distribution. Entanglement is created during the protocol rather than distributed to the authorised users. To generate entanglement between the photons of Alice and Bob, Charlie will interfere the incoming photons on a beam splitter, the outcome of which is governed by the Hong-Ou-Mandel rule [58]. Let's assume the encoding was performed in polarisation. If the particles that interfered at Charlie's beam splitter were of identical polarisation then, following the Hong-Ou-Mandel rule, both photons will exit the beam splitter on the same output [58]. Following interference, a Bell test is necessary to determine the entangled state that was generated. For this, just like in the entanglement based QKD schemes, two polarising beam splitters and four detectors are ideally required. For practicality and cost-efficiency, Bell test setups are normally reduced to two detectors. The coincidence counts will be measured by Charlie who, given a reduced setup, can distinguish two out of four possible Bell states. He publicly announces the instances in which he observed coincidence counts and which detectors clicked. This is the only information Charlie can obtain. Similarly to standard entanglement-based QKD, Alice and Bob announce their basis choices and knowing their own encoding they can deduce the other's to distil a key.

Charlie would have to know the users' preparations to extract the bit value of each successful event. If he decides to cheat by performing a measurement different than the one required by MDI-QKD, he will be detected in the error estimation process, as his random

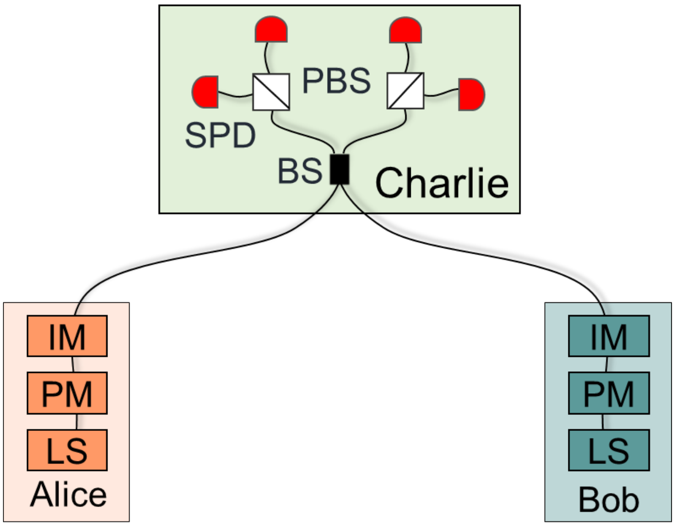

Figure 1.4 **MDI-QKD setup:** MDI-QKD uses a three node architecture where Alice and Bob are both transmitters while only Charlie is a receiver. The transmitters are equipped with a laser source (LS) to produce weak coherent pulses which they will encode, in this example, in polarisation using a polarisation modulator (PM). The decoy-state method will be employed via an intensity modulator (IM). Prepared pulses from each user are sent to travel through quantum channels to interfere at a beam splitter (BS) in Charlie's station. Due to the Hong-Ou-Mandel effect and the polarising beam splitters (PBSs) following the BSs, coincidence counts on the detectors (SPDs) will help Alice and Bob distill a key.

Bell state announcements will produce errors in the key strings. In this way, MDI-QKD is fully independent of the measurement station, which can be completely surrendered to an untrusted party. The weak point of MDI-QKD lies in the use of coincidence counts. These are rare events since losses in the system and low efficiencies in the detectors radically decrease the probability of both photons being detected by Charlie. Hence useful events are notably scarce.

1.3 Beyond the repeaterless secret key capacity

1.3.1 Repeaterless secret key capacity

As mentioned previously, the no-cloning theorem is vital for the security of quantum communications but it is also its biggest limitation. The lack of amplifying stations in QKD implies that the maximum distance over which a secret key can be distributed in such systems

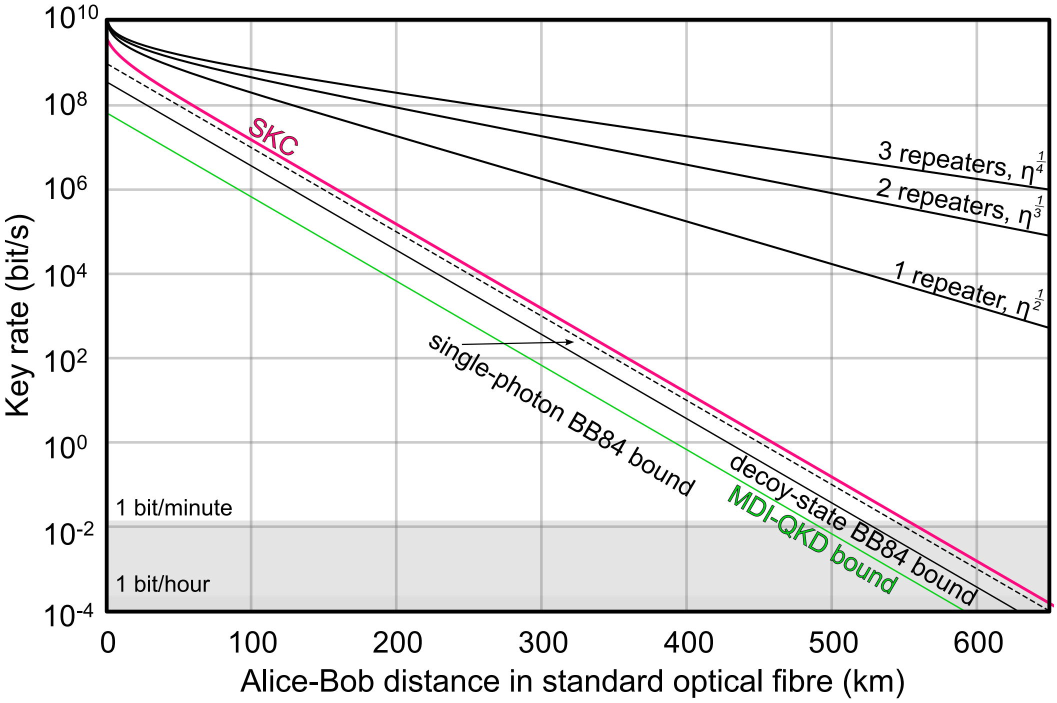

Figure 1.5 **Repeaterless secret key capacity:** The repeaterless secret key capacity is the absolute rate-distance bound for point-to-point QKD, represented here by the pink line. Assuming ideal conditions this bound is also plotted for the BB84 (black thin line), the decoy-state BB84 (black dotted line) and the MDI-QKD (green line) protocols. The lower black line surpassing the SKC$_0$ is the bound for a system with one repeater, while further lines above show the scalability for an increasing number of repeaters (see section 1.4.2). In the plotted curves, fibre channels of attenuation coefficient $\alpha = 0.2$ dB/km are considered.

is always limited by the attenuation of the channel. In other words, in any point-to-point QKD protocol the key rate is at best proportional to the channel transmission. If we imagine an Alice-Bob link, in the ideal case where every photon received by Bob is used for key generation, then we get the maximum possible key rate per distance and the total maximum distance attainable by point-to-point QKD. This limit is known as the repeaterless secret key capacity (SKC$_0$) or as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound, due to it being defined in [59]. By denoting η the transmissivity of the quantum channel, the SKC$_0$ is given by [59]:

$$R_{SKC_0} = -log_2(1-\eta) \tag{1.7}$$

This bound is represented in figure 1.5 by the pink line after taking $\eta = 10^{-\frac{\alpha L}{10}}$, with α the loss coefficient and L the length of the fibre connecting Alice and Bob. At long distances, SKC$_0$ can be approximated by 1.44η.

Apart from losses in the quantum channel, and as mentioned in section 1.1.2, not all received photons will be used to generate a key. In figure 1.5, bounds for several protocols are plotted. For the single-photon BB84 protocol the bound decreases, as the maximum key rate follows:

$$R_{BB84} = \eta \tag{1.8}$$

For the case of the decoy-state BB84 the maximum key rate is further decreased as R_{BB84} need to be divided by Euler's number as:

$$R_{dec,BB84} = \frac{\eta}{e} \tag{1.9}$$

The bound for the MDI-QKD scheme is even more pessimistic. Although utilising a three node architecture, this protocol cannot double the distance and outperform the PLOB, but rather performs worse than the rest. This is a direct result of using the Bell test and hence requiring coincidence counts for the distillation of the key, significantly decreasing the maximum key rate at every point. Hence, for MDI-QKD the key rate is given by:

$$R_{MDI-QKD} = \frac{\eta}{2e^2} \tag{1.10}$$

It is usually true that more secure protocols have tighter bounds.

1.3.2 Repeaters

A necessary condition to benchmark a quantum repeater is that it outperforms the SKC_0 [60]. A quantum repeater conventionally refers to a specific quantum technology which was thought to be the only way to achieve repetition in a quantum system and beat the PLOB. This quantum repeater was first proposed by Dür et al. in ref. [61]. It is a complex technology requiring both entanglement purification [62–64], teleportation [65] and a quantum memory to successfully *repeat*.

A scheme of a QKD system with multiple repeaters is shown in figure 1.6. The long quantum channel is cut into segments, L_i by introducing repeater stations. The repeaters are actually considered part of the channel, since they are untrusted nodes. The term untrusted node refers to any station where a secret key is not distilled even if a malicious adversary has full control of the station [66]. The target is to start with a quantum correlation between Alice and the first repeater station and transfer this to each consecutive segment until Alice and Bob end up sharing this same correlation. Each receiver increases the maximum distance allowed between two nodes. The scaling behaviour of repeaters is visualised in figure 1.5, where the transmissivity of a system with n repeaters, η_n scales with respect to the SKC$_0$, η_{SKC_0} as:

$$\eta_n = \eta_{SKC_0}^{\frac{1}{n+1}} \tag{1.11}$$

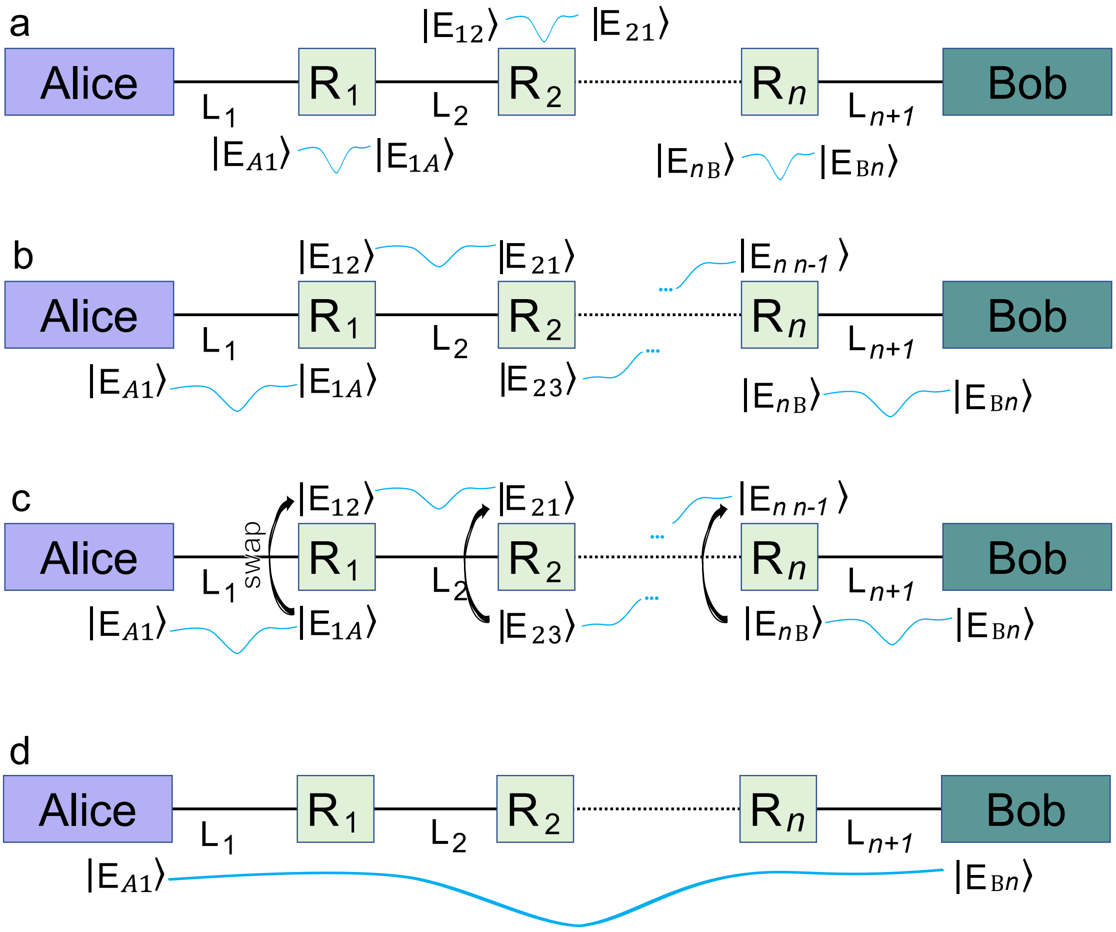

Figure 1.6 **QKD with repeaters:** A long QKD channel is divided in segments, L_i, by n repeater stations, R_i, where n in the same as the one stated in equation 1.11. Entanglement is created between consecutive stations which is swapped with the ultimate target of creating entanglement between $|E_{A1}\rangle$ and $|E_{Bn}\rangle$.

The technology of a traditional repeater is summarised here. As aforementioned the end goal is for Alice and Bob to share an entangled state when they are so far apart that channel losses will not allow this to be achieved directly. Looking at figure 1.6, every channel segment of length L_i has to be small enough for an entangled photon pair to be directly shared by the adjacent nodes. Entangled pairs can be generated with techniques such as spontaneous parametric down-conversion [67, 68], at each repeater station, R_i (see figure 1.6.a). One qubit from each pair is distributed to an adjacent station. For example, in figure 1.6.a, R_1 creates an entangled qubit pair $(|E_{A1}\rangle, |E_{1A}\rangle)$ and directly sends one of the qubits, $|E_{A1}\rangle$, to Alice, while keeping the second qubit, $|E_{1A}\rangle$ (figure 1.6.b). This is repeated several times and similarly at all repeater stations. Entanglement purification is performed on the sample of generated and distributed qubits, a process which aims to achieve pure Bell states in a smaller subset and thus undo degradation of the entanglement due to noisy channels. All stations are also equipped with a quantum memory [69], in which they store the entangled qubits until they have established a shared pure entangled pair with all adjacent stations. At this point, repeater stations can consecutively perform a Bell test on their two qubits, (e.g. R_1 on $|E_{1A}\rangle$ and $|E_{12}\rangle$) to achieve what is known as entanglement swapping [70–72]. Swapping transfers the entanglement of $|E_{1A}\rangle$ with $|E_{A1}\rangle$ to $|E_{12}\rangle$ (figure 1.6.c). As a result, Alice and R_2 are now entangled, through $|E_{1A}\rangle$ and $|E_{12}\rangle$, without ever interacting directly. If this process is repeated with all adjacent nodes up to Bob, then Alice and Bob will end up with a shared entangled pair $(|E_{1A}\rangle, |E_{Bn}\rangle)$ (figure 1.6.d). The total loss of all segments L_i would not have allowed any photons to be directly distributed between Alice and Bob and no quantum communication could have ever taken place using direct transmission. Using the repeater scheme, the final entangled pairs will be used for QKD between Alice and Bob.

The process described has intrinsic difficulties in its implementation. It is comprised of a series of complex processes which not only are difficult to perform individually, but if put together, the probability of all of them succeeding is quite low. Further development into quantum memories, entanglement purification and swapping is required, to make quantum repeaters a viable component of a quantum network. Further details on the current state-of-art of repeaters and the technologies they entail can be found in 1.4.2.

1.3.3 Twin-field QKD

The first, and currently only, protocol implementable with current technology that is able to surpass the PLOB rate-loss limit was proposed by Lucamarini et al. in 2018 [1]. This protocol is known as Twin-Field (TF) QKD and it is a measurement device independent protocol. Due to its ability to overcome the repeaterless bound, it is also known as *efficient* MDI-QKD. However this efficiency comes at the cost of a challenging experimental implementation. In fact, the idea of TF-QKD is very clean and the only worry that remained after its proposal was whether this protocol was truly feasible.

TF-QKD can essentially be seen as a phase-encoded BB84 protocol adapted to work for an MDI-QKD, three-node, architecture. In figure 1.7 the proposed setup from ref. [1] is

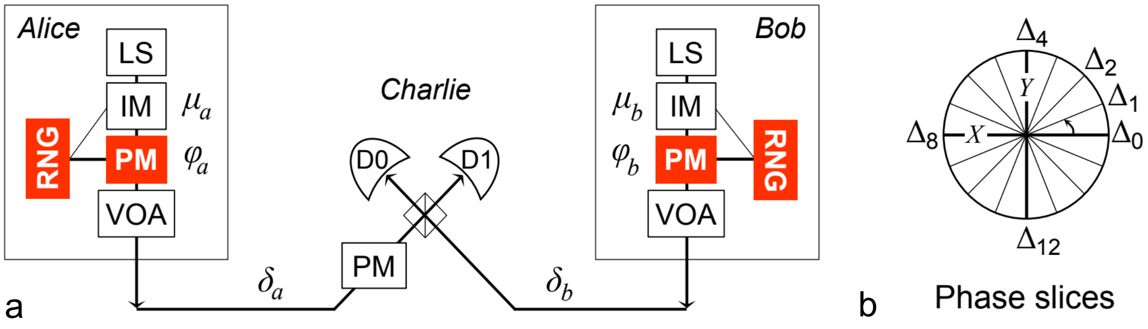

Figure 1.7 **TF-QKD scheme:** These are figures reproduced from ref. [1]. **a.** Schematic of the proposed TF-QKD setup. Laser sources, LS, produce WCPs. These are modulated in intensity, IM, for decoy state implementation and encoded in phase, PM. Phase randomisation is performed using random number generators (RNGs) and finally the flux is attenuated to the correct level through variable optical attenuators (VOAs) . The relative drift of the two channels, δ_α, δ_b, is corrected by Charlie using a PM placed in his station. He then performs a first order interference measurement of the incoming photons. **b.** The phase circle is discretised into M number of slices Δ, here 16.

shown. The first obvious difference with both MDI-QKD and QKD spotted looking at the setup is the active phase randomisation. Alice and Bob own laser sources capable of creating WCPs as per usual. Intrinsic phase randomisation of the sources is not desirable in TF-QKD. Active randomisation of known values must take place instead. For this, not only is a random number generator (RNG) necessary but moreover, the two users must begin locked to the same phase, such that the pulses from a corresponding cycle always begin with equal phase to one another.

Each WCP generated is phase randomised with any value ρ_γ in the $[0, 2\pi)$ interval, using the phase modulator attached to the RNG. In this manner, the two users have full knowledge of their phase randomisation value choice, $\rho_{\gamma_{a,b}}$. The phase modulator will also be used to encode a bit value of random choice, $\rho_{\beta_{a,b}}$, to the pulses. The original proposal suggests the use of two bases for bit encoding: $\mathbb{X}$ (0, π) and $\mathbb{Y}$ ($\frac{\pi}{2}, \frac{3\pi}{2}$). The total encoded phase of each user is hence $\phi_{a,b} = \rho_{\gamma_{a,b}} + \rho_{\beta_{a,b}}$. An intensity modulator is also used to employ the decoy state technique.

The prepared pulses are sent through long quantum channels, that in total can exceed 500 km of fibre. Upon arrival at Charlie's station, they interfere at a beam splitter just like in the MDI-QKD protocol. However here, a Bell state measurement will not follow since TF-QKD does not require entanglement. Instead, since it resembles a BB84 protocol, a first order, single-photon interference is sufficient. First order interference refers to a constructive-destructive measurement, thus Charlie must simply announce which of the two

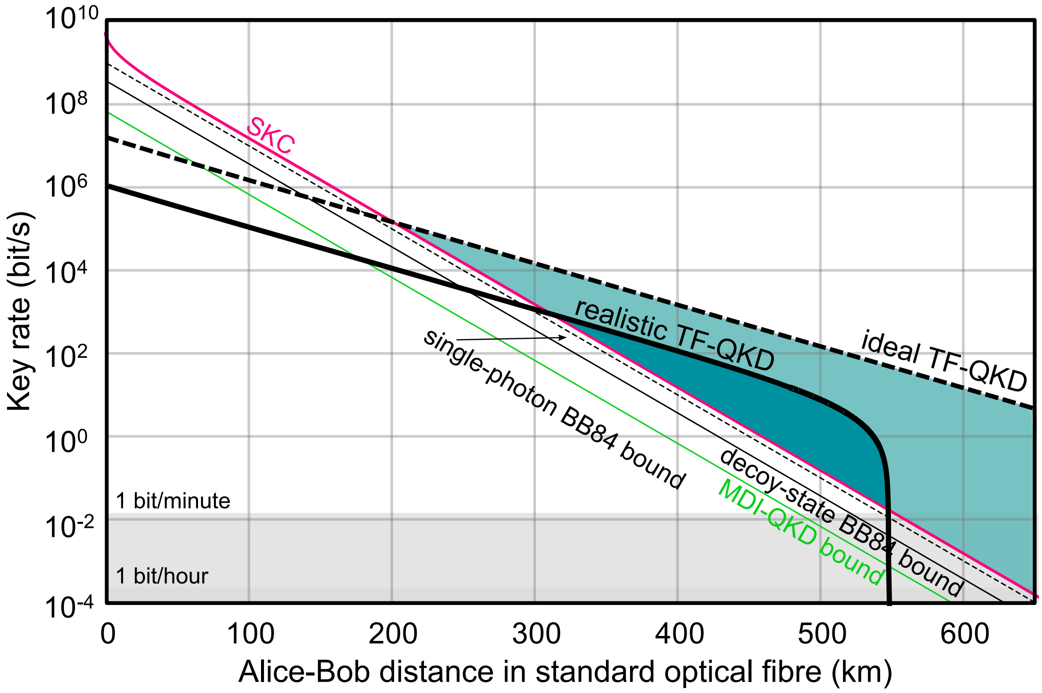

Figure 1.8 **TF-QKD vs the repeaterless secret key capacity:** Lines are added for the ideal parameter TF-QKD (thick black dashed line), and the realistic parameter TF-QKD (thick black line). TF-QKD shows the same square root dependence of key rate on channel loss as a system with a single repeater. It is able to overcome the SKC_0 for distances over 320 km of standard fibre to show a new potential record region for repeater-less QKD.

detectors, connected to the beam splitter, clicked. For example, the constructive detector only clicks when the phase difference between the interfering pulses is 0, while the destructive detector, when the difference is π.

Sifting is similar to the rest of the protocols, with the sole difference that one more piece of information must be revealed for the raw key to be formed. Alice and Bob must announce some information about the phase randomisation of each prepared pulse, so that basis choice announcements can be used to extract a bit value. Since possible randomisation values are infinite they will not announce the exact value but rather a phase-slice it belonged it. This means the phase-circle of infinite values is discretised to an optimal number of slices as shown in figure 1.7.b. Only interfered pulses randomised with values in the same slice will then be used. Alice and Bob then continue to announce their basis choices so that they can each deduce, in the matching basis and phase randomisation instances, the bit value encoded by one another, by combining Charlie's announcement and their own bit encoding choice. Intensities are sifted as per usual.

Overcoming the rate-distance limit

TF-QKD's efficiency is boosted due to the exploitation of single clicks on either of the two detectors to distill a bit. Instead, in section 1.2.3 we discussed that in MDI-QKD it is mandatory to observe coincidence counts in two detectors to determine the bit value. As a consequence, the three node architecture of conventional MDI-QKD does not actually allow the doubling the maximum distance of the quantum channel, unless the protocol is memory assisted [73]. TF-QKD is the only implementable protocol able to achieve this and beat the performance of point-to-point QKD to overcome the repeaterless secret key capacity.

In figure 1.8, two new simulation lines are added, demonstrating the performance of TF-QKD in an ideal-case scenario (thick black dashed line), and considering realistic parameters (thick black line). In the first (latter) case, the efficiency considered is 100% (30%), dark counts are set to 0 (3) Hz and the optical misalignment error is set to 0% (3%). The first thing to notice is how the gradient of the rate-loss bound for TF-QKD is identical to the gradient of the single-repeater bound. The rate is proportional to the square root of the channel transmittance as opposed to all other protocols where the rate is proportional to the channel transmittance. At short distances TF-QKD performs worse than BB84, MDI-QKD and the SKC_0. This is due to the phase-circle discretisation and slice-matching requirement during sifting, which causes a $\frac{1}{M}$ scaling, where M is the number of slices after discretisation. Nevertheless, this is small compared to the exponential loss and at medium to long distances, TF-QKD shows a clear advantage over all other protocols. In both the ideal and realistic case scenario, this protocol is able to overcome the PLOB bound at long distances without using quantum memories or other complex, non-available technologies. Its efficiency is fully attributed to the single-photon interference of the three-node architecture.

Main experimental challenge

TF-QKD was characterised as an *efficient* MDI-QKD protocol. It predicted a quantum system with a repeater-like behaviour, implementable with current technology. Nevertheless, there are significant experimental challenges that need to be surpassed for successful, distance breaking TF-QKD to take place.

The most significant challenge is overcoming phase noise induced in the channels. In TF-QKD, phase encoding and randomisation takes place in the transmitter stations. The prepared pulses travel down long quantum channels to arrive at the receiver, where a first order interferometric measurement will take place. However, when pulses travel down long fibres, they are exposed to environmental fluctuations which modify the optical path of the channels and hence the pulses' phase. Local thermal changes or vibrations can cause tiny changes in the optical paths of the quantum channels, whether these are free space or fibre. Given that the wavelength of light used for QKD is also quite small, usually at 1550 nm, the optical path changes are relatively significant. Since the two quantum channels are independent, these perturbations are different for Alice and Bob and hence all information about the initial relative phase of their pulses is lost. When long fibres are used, the induced phase error accumulates and can cause a total drift exceeding 10 rad/ms at 500 km. As a result, Charlie's measurement outcome is random and the two users are not be able to distil a secret key. Consequently, for TF-QKD to be successfully implemented, it is mandatory that the pulses, after travelling down long quantum channels, can still interfere in their encoded phase state.

This is a challenge new to practical QKD. The BB84 protocol is encoded and measured in phase, however, it only requires a point-to-point link and relative phase measurements are not performed. MDI-QKD, on the other hand, does have a three node architecture but uses a second order interferometric measurement (Hong-Ou-Mandel) which is not crucially affected by phase noise. The combination of the three node architecture with the first order interference measurement in TF-QKD is what gives rise to this new experimental challenge.

Further experimental difficulties include distributing a common phase reference, achieving indistinguishability in remote sources, maintaining indistinguishability at interference and accurately implementing active phase randomisation. These will be explained in depth in chapter 4 where the channel phase noise problem will also be discussed in further detail.

1.4 State of the art QKD

This section will describe the current state-of-art of DV-QKD systems and of the components required for successful implementations. Many novel technologies are fundamental to practical QKD, technologies that are not necessarily useful for conventional communications. Consequently, development of such technology has only started at most 25 years ago. It is therefore important to look at the current progress and success of QKD given its novelty.

1.4.1 Single-photon detectors

Since DV-QKD is based on the use of single photons for the encoding of information, single-photon detectors (SPDs) are a vital part of any DV-QKD system. These are detectors sensitive enough to measure individual incident photons, rather than bulk light as needed in conventional optical communications and most other current applications.

The performance of an SPD can be quantified with the following factors. Sensitivity is represented by the *efficiency* factor, η, of an SPD, which is one of the most important parameters to be optimised in their development. Efficiency is given by the ratio of detected photons over the total number of photons incident on the detector. Not only are QKD users sending out single photons, but if they are employing a WCP protocol then most pulses will be vacuums. It is crucial that an SPD is therefore efficient enough, so that sufficient information is exchanged within a viable amount of time. The second characteristic is related to noise and is known as the *dark count rate*. This is the rate of detections measured by the device when no light is incident. These can arise from various sources depending on the nature of the detector, such as background light that was not fully filtered, photons generated by thermal excitation in the fibre parts of the detector or due to side-effects of the detection method (e.g. avalanche generation). Countermeasures to such phenomena are cooling of the detectors to extremely low temperatures near absolute zero or using filters to make sure that light of different wavelength than the one expected is absorbed before entering the detection region. For protocols like TF-QKD, where the channel losses can be extremely high, keeping a low dark count rate is crucial as it becomes the dominant source of error. Dark count probability and detection efficiency are usually a trade-off. Increasing the efficiency of an SPD will also increase the dark count rate. Hence, in every implementation, the importance of efficiency versus noise must be quantified and the parameters of the SPD optimised accordingly. *Timing jitter* is yet another significant performance characteristic. It is the time uncertainty when a detection is made and it is usually denoted in pico-seconds. QKD is optimally performed in the GHz regime and requires time-tagged events. Thus, this parameter should be minimised. Finally, independent of the specific SPD technology, all devices require a finite recovery time after a detection is observed. This is known as the *dead-time* between detection events and it is one on the main factors limiting the maximum effective rate of QKD systems.

In current QKD implementations, two types of SPDs are in use: single-photon avalanche photodiodes (SPADs) and superconducting nanowire single-photon detectors (SNSPDs).

Record performance demonstrations are summarised in table 1.2, while their underlying technology is briefly outlined in the following two subsections.

Single-photon avalanche photodiodes

A SPAD, just like a standard avalanche photodiode (APD), operates based on the photoelectric effect. The photodiode is made of semiconducting materials creating a PN or PIN junction on which a reverse bias is applied. Incident photons are absorbed creating electron-hole pairs while the reverse bias, if strong enough, can generate a multiplication region, where a single photon is able to trigger an avalanche effect. APDs have two operating regimes, the linear and the Geiger mode, which arise depending on the bias voltage applied to the diode. In the linear regime, the bias is kept below the breakdown voltage and the output signal of the APD is proportional to the intensity of the incident light. Therefore, single photons are not detected, as the generated charge is insufficient for detection. In the Geiger regime however, self-sustained avalanches of charge carriers occur, amplifying the electrical output of the device to macroscopic levels and hence making it sensitive to single-photons. Avalanches can be passively quenched, but due to high detection rate demands, SPADs used for QKD are mostly actively quenched by gating their operation with an AC bias voltage driven above and below the breakdown voltage [74]. Alternatively, active quenching can also be achieved through a circuit which reduces the SPAD's bias voltage for a certain amount of time upon detection of an avalanche [75].

SPADs are the only single-photon detectors useful for QKD that can currently perform well in room temperature and don't necessarily require cryogenics. Consequently, they are significantly cheaper to use while they can be, and have been, miniaturised and implemented within devices. However, SPADs overall keep a lower detection efficiency than SNSPDs and a higher dark count rate. Telecom wavelength, high-repetition SPADs ordinarily have an efficiency of $20-30\%$ [76]. The avalanche effect is a direct contributor of extra dark counts. As not all avalanches are quenched fully, carriers get trapped and create erroneous detection events with their random release. This is also the main limitation on the maximum operation frequency of SPADs.

Self-differencing circuits were developed to combat noise in such devices and increase the limit on the gating frequency to the GHz regime [77]. The aforementioned circuits cancel capacitive noise by dividing the electrical output of the SPAD and delaying one part by one gate. Recombination of the two parts takes place, where capacitive noise is cancelled and an avalanche, easy to discriminate, is produced.

Detector type	η	Dark counts	Timing jitter	Dead-time	Temp.
	(%)	(Hz)	(ps)	(ns)	(K)
SNSPD [81]	**93**	1	150	40	1
SNSPD [82]	0.04	**0.001**	-	-	0.4
SNSPD [83]	0.01	-	**4.3**	-	0.9
SNSPD, on-chip 2D [80]	67	**0.0001**	29	**0.48**	1.6
SPAD [84]	45	94000	60	2	**293**
SPAD [84]	10	480	60	2	**243**

Table 1.2 **SPD state-of-art:** Summary of important SPD demonstrations in the 1550 nm wavelength band. Values of the detection efficiency η, dark count rate, timing jitter, dead-time and driving temperature are given. Numbers in bold indicate the record breaking quantity in each implementation.

Superconducting nanowire single-photon detectors

SNSPDs were first proposed in 2001 in refs. [78, 79] They are comprised of micrometer long nanowires arranged so that a pixel is formed. Zero resistance is maintained across the nanowire by cooling it below the superconducting critical temperature. An applied bias voltage keeps the temperature close to the superconductivity critical point. Hence, photons incident on the nanowire will locally break superconductivity, increasing the local resistance and sending the bias current to an amplifier, so that counts can be recorded. The time needed to re-cool nanowires, so the dead-time, is in the order of picoseconds, rendering them appropriate for fast QKD implementations.

The average efficiencies of SNSPDs are double those of SPADs and their dark count rates many orders of magnitude lower. Therefore, SNSPDs are highly beneficial for QKD and consequently are usually favoured. Nevertheless, the requirement for cooling them down to near absolute zero temperatures means they cannot function without cryogenics. These poses two significant obstacles. Firstly, SNSPDs are much more expensive to buy and operate, hence they cannot yet be commercialised on a large scale. On top of that, although SNSPDs have been implemented on-chip in combination with optical circuitry [80], cryogenics are bulky components which, for the time being, stand far from being miniaturised.

1.4.2 Entanglement and repeaters

Entanglement generation, distribution and purification are undoubtedly challenging processes and hence, entanglement based protocols, at the moment, lack the impressive results acquired by standard QKD. The main impeding factor in such experiments is the low entangled pair production rate achievable given that sources, such as those based on spontaneous parametric downconversion (SPDC), are not sufficiently bright and usually have significant losses[85]. Nevertheless there have been successful demonstrations of entanglement distribution and teleportation, both in fibre and in free-space channels, including satellite links. In free-space and excluding satellite systems, teleportation has been performed over a record distance of 97 km in a one-link configuration enabled by entanglement distribution over 102 km over a two-link configuration [86]. In-fibre experiments have also successfully distributed entanglement over 96 km using a submarine link connecting Malta to Sicily [87]. Satellite quantum communications have seen major research interest over the past years. Entanglement distribution has been demonstrated between two Earth locations separated by 1200 km, utilising a low-Earth orbit satellite [88]. In terms of entanglement-based QKD the key rates are quite limited, following the rarity of coincidence counts. Extending the aforementioned satellite experiment to include a QKD protocol, the average rate achieved was 3.5 bps, as the channel length was ranging from 530 km to 1000 km [89]. In ref.[85], for an in-fibre system with 5 dB channel loss (equivalent to 25 km of standard optical fibre), only 0.1 bps of key rate were achieved.

Moving on to repeaters, there's the extra experimental challenge of implementing a quantum memory, on top of performing the previously discussed distribution, entanglement and teleportation processes. Recently, major progress has been made in the field of quantum memories where an MDI-QKD-like system was enhanced by the use of a solid-state memory based on a diamond nano-photonic cavity, of storing time around 0.2 ms [73]. Although it is not clear as to whether this experiment was able to surpass the SKC_0, the clear enhancement of the protocol and the low losses of their system suggest that this technique could soon provide a full fledged quantum repeater demonstration. Preceding this implementation, coincidence count enhancement of a factor 30 was shown in an entanglement based MDI-QKD experiment, without however showing an enhancement of the protocol's output [90]. In terms of pure coherence time for telecom wavelength compatible quantum memories, the current record is set at 1.3 s, found in ref. [91].

1.4.3 Key rates and distances

The past year has seen significant leaps in terms of channel distances reached and losses tolerated in experimental in-fibre QKD. This is for no reason other than the proposal of readily implementable TF-QKD protocol, which has prompted groups to research it experimentally. The latest TF-QKD experiments were able to obtain positive key rates in channels longer than 500 km. To lead the road to such distances there are a few significant steps that were to be taken. Firstly, the protocol was implemented over channel losses up to 90 dB but without long fibre channels, in the first part of the work presented in this thesis and found in ref. [92]. This was achieved with a 2 GHz clocked system of 22 Hz dark counts in the SNSPDs. The key rate at maximum loss was 45 bps. This temporarily held the record for the maximum loss tolerated in any QKD implementation, to be surpassed a year later by the following two experiments. In ref. [93], the distance of the quantum channel was extended to 502 km in a further proof-of-principle TF-QKD demonstration. Classical communication servo-fibres were kept shorter, while the system was working at 312.5 MHz, with less than 50% duty cycle, to reach 0.118 bps. Finally, the latest implementation has reached 509 km [94], where all fibre channels utilised were of the same length, showing a complete implementation and giving the record for the longest channel in an in-fibre QKD experiment. This system used a low clock rate of 1.85 MHz with extremely low dark count rate at 3.5 Hz for a secret key rate output of 0.011 bps at maximum distance. Both of these experiments used a post-processing scheme to avoid errors from the phase-drift of the channels and therefore kept low repetition rates, explaining the acquired low key rates.

The current record for standard QKD in-fibre was set in ref. [26] in 2018, by reaching 421 km with 6.5 bps output and by implementing a one-decoy state protocol [95]. Nevertheless, this was achieved using SNSPDs with extremely low dark count rate at 0.1 Hz and with a fast 2.5 GHz clock. For systems using APDs instead, the record distance for QKD is 240 km [96] with the detectors performing at 10 Hz dark counts but with a low efficiency of 10%. All aforementioned distances refer to ultra-low loss fibres with loss coefficients between 0.165-0.185 dB/km. MDI-QKD's record is currently 404 km [97]. However, given the rarity of coincidence counts the implementations are inefficient, with this particular one achieving $3.2x10^{-4}$ bps within an acquisition period of three months, while working at 75 MHz repetition rate with 30 Hz dark counts. The advantage of TF-QKD over MDI-QKD is hence quite clear.

Finally, it is important to refer to the experiment by Yuan et al. in 2018, which holds the record for the highest key rate ever extracted from a QKD system, at 10 Mbps. This

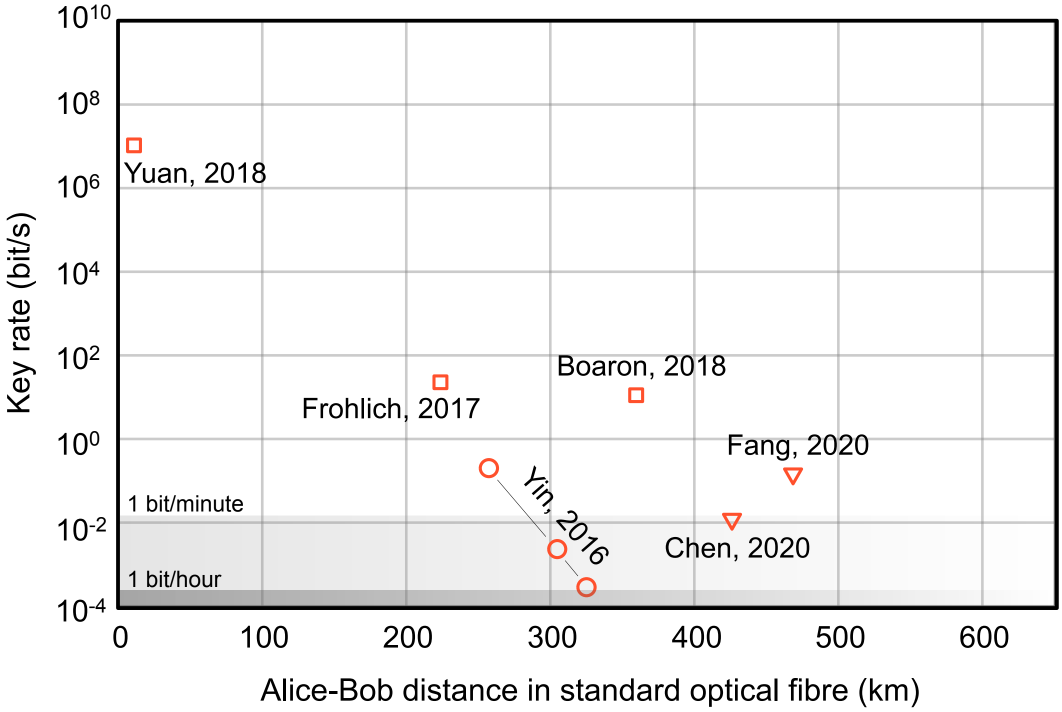

Figure 1.9 **QKD state-of-art:** The key rates versus distance of major QKD experiments discussed in this section. Squares represent experiments implementing standard QKD, circles represent MDI-QKD implementations while triangles represent TF-QKD experiments.

was achieved by developing in-house electronics able to count and tag single photons at high rates. These electronics perform all post-processing such as sifting and error correction, enabling the system to be highly efficient. In figure 1.9, all the aforementioned real fibre experiments are plotted in a key rate versus distance plot, normalised to standard fibre of loss coefficient 0.20 dB/km for homogeneity. From the figure it is easy to notice that TF-QKD is clearly pushing the limits of long distance QKD.

Since QKD is achievable over long distances, quantum communication networks are also being extensively researched for good reason. The target is to connect multiple users in short links but to also interconnect cities and metropolitan networks. Several quantum networks are already in place and used in several countries [98–100]. In the United Kingdom, the first metro network node was established between the University of Cambridge and the Science Park, over which QKD has been performed along classical communication traffic [101]. The Cambridge network is expected to be connected with Bristol soon, to form the longest deployed quantum channel in the UK. In the Bristol metro network, there exists an eight-node sub section where simultaneous exchange between all configurations of the eight users is possible [102]. The Bristol network is also home to an interconnection of four users communicating through a novel wavelength-entanglement based scheme [103].

The future of commercial QKD, like most communication technologies, lies in integrated photonics. Bulk setups are translated into chip configurations where all components, like phase modulators and lasers, are integrated within the lithographic chip [104]. Various protocols have already been implemented on chip, like BB84 [105], differential phase shift QKD [106] and MDI-QKD [107, 54]. Such chips would be integrated within cell phone devices, computers and credit cards. Consequently, hand-held on-chip QKD has been a recurring research theme, with the first examples found in ref. [108] and ref. [109]. In such demonstrations, reference-frame independent QKD is favoured, since these systems will be subject to rotations. For now, docking stations are necessary for their successful implementation.

Satellite QKD has also seen major advances in the last three years with the first successful demonstrations taking place. Satellites have been launched to be used specifically for QKD but have also been exploited to test fundamental theories on quantum mechanics [110]. In 2017 two major milestones were achieved by J. W. Pan's group. The Micius satellite launched in 2015 was successfully used in the first QKD demonstration over satellite, achieving a 1 kbps distribution at a distance of 1200 km [29]. This was accompanied by the entanglement distribution experiment mentioned in the previous section [88]. China had expressed plans to establish the first quantum satellite constellation for intercontinental QKD. The first intercontinental QKD was achieved with the same satellite in 2018, where locations in France and China were able to perform a conference call with keys distributed by Micius [111], a landmark achievement for QKD.

1.5 Research motivation

The TF-QKD protocol is a novel proposal which promises to break theoretical limits using solely current technology. The motivation behind the work described in this thesis was to develop theoretical and experimental tools to successfully implement the TF-QKD protocol and its variants. The aims was to show the first experimental demonstration of the protocol and to beat the performance of point-to-point QKD, to surpass the repeaterless secret key capacity. This would show the first system to behave similarly to a single-repeater QKD system, and therefore the first one to effectively *repeat*.

Since TF-QKD gives us the opportunity to readily achieve successful QKD in channels longer than 500 km, new distance and loss records are desirable. A direct objective was therefore to develop a system not solely able to beat theoretical limits, but one that would break these physical records. Such a system should escape the proof-of-principle regime and assimilate a real-life implementation as closely as possible.

1.6 Novel contributions

The work in this thesis presents the development of a set of tools required for a TF-QKD experimental demonstration. These tools led to the first realisation of the TF-QKD protocol and to the first demonstration of a system that outperforms the repeaterless secret key capacity. They were also used to break the distance and loss record for in-fibre QKD.
The author has made the following novel contributions:

- Explored all major representatives of Twin-field type protocols by developing simulations fitted to a general channel model. These were used to perform a direct comparison of the protocols' attributes, reviewing for the first time different TF-QKD variants.

- Developed the setup and software required for implementing the TF-QKD protocol and two of its variants. Utilised the setup to carry out the first ever experimental demonstration of TF type protocols, in a proof-of-principle implementation, where optical attenuators were used to simulate long fibre channels. For this, the author developed and brought together several experimental techniques such as optical injection locking and phase stabilisation, in a fast system with a 2 GHz clock and with all the necessary modulations.

- Optimised simulations and experimental parameters and performed relevant security analyses on experimental data to extract and fit positive key rates up to a total channel loss of 90 dB, for a conditionally secure protocol, and up to 84 dB for unconditionally secure variants. These losses, at the time of publication of the results, had set the channel loss record for QKD. The key rate results surpassed the repeaterless secret key capacity, to show the first system with a repeating behaviour.

- Co-developed and implemented a novel dual-band phase stabilisation scheme, able to accurately correct phase-drift in quantum channels longer than 600 km. Previous phase stabilisation methods for quantum channels were limited to 8 km long interferometers [112], before the proposal of TF-QKD and to 300 km [113] after. The stabilisation scheme is not only useful for implementing TF-QKD in real channels but is a technique important for other sought after quantum technologies, such as repeaters.

- Designed and built a multi-protocol system able to implement TF-QKD in quantum channels up to 600 km in length, reaching a new record distance for in-fibre QKD. The system, working at a 1 GHz repetition rate, included polarisation feedback and stabilisation of phase and intensity drifts, to successfully extract keys using the SNS-TF-QKD protocol, with and without two-way classical communication (TWCC), and the CAL-TF-QKD protocol. A complex encoding and sifting program was developed such that all necessary modulations for all protocols were performed on-line.
- Performed the full implementation of the TWCC post-processing method for the first time as well as the asymptotic and finite-size analysis of the acquired data. Previous TF-QKD demonstrations had been limited to sole estimations of the effect of TWCC, due to the difficulty of extracting and processing single counts. Here, the author developed efficient software which extracted real bit strings during the protocol and then post-processed them to extend the maximum distance achievable with the SNS-TF-QKD protocol, allowing us to reach the 600 km mark. Processing the experimental data obtained with all three protocols, key rates above the repeaterless secret key capacity were extracted. At the longest distance of 605 km, and a loss of 104.8 dB, 0.969 bps were extracted using the asymptotic case while at 555 km, 2.468 bps are obtained when including finite-size effects.

The author of this thesis acknowledges the contribution of other researchers in achieving the presented results. M. Pittaluga supported all experimental work with significant contributions in the development of the optical phase-locked loop, the refinement of the slow phase feedback and the encoding of the QKD patterns in the 600 km experiment. G.L. Roberts supervised the work on optical-injection locking. M. Sanzaro developed the FPGA for the fast phase feedback. M. Lucamarini supervised theoretical and experimental work, and Z. Yuan supervised all experimental work. Finally, the author acknowledges useful discussions with S.J. Savory and A.J. Shields.

1.7 Thesis organisation

This thesis is devoted to the exploration and practical implementation of Twin-field type protocols. Chapter 1 is a general introduction to quantum cryptography and QKD, beginning from its conventional communication counterpart. The different TF-QKD variants of interest are explored in chapter 2, which provides an overview of the theoretical tools required to simulate and predict the measurable quantities obtained in the security analyses of experimental data. All expressions are fitted to a defined practical channel model. The chapter also includes a brief comparison of various aspects of the protocols. Chapter 3 is the implementation chapter, describing the two major experiments performed during this Ph.D. and their results. These are: the first ever proof-of-principle demonstration of TF-QKD, and the currently longest distance QKD implementation reaching 605 km in-fibre. This chapter focuses on protocol implementation, while specific experimental methods developed and utilised in the aforementioned demonstrations are described in-depth in chapter 4. Chapter 5 is devoted to improvements and alternative ideas for the TF-QKD setup which would be interesting to be researched in the future. Finally, the contents of the thesis are summarised in chapter 6, where all obtained results are collected and compared to the literature at the time of submission.

Chapter 2

Theoretical tools for twin-field type QKD protocols

2.1 Introduction

The publication of the original proposal of the TF-QKD protocol in 2018 [1] was a breakthrough in quantum communications. One of the main drawbacks of conventional QKD protocols is, as discussed previously, the distance limitation. To establish a quantum communication protocol over long distances, such as inter-city channels or channels connecting different countries, quantum repeaters are required. Their development is still in its early stages, as shown in section 1.4.2, since the complexity of the technologies required for their realisation is a critical hindrance. Instead, the classical counterpart of QKD can easily distribute keys over long distances.

If quantum communications are to be integrated in current infrastructure, the distance limitation has to be overcome. TF-QKD promised exactly that, by extending the maximum distance of secure quantum communications by hundreds of kilometres. In the scientific community of quantum information this was a major advancement and following the publication of the first proposal many variations have been explored [2] [114] [115] [3]. These are variants of the TF-QKD protocol aiming to improve specific properties of the original proposal, such as ease of implementation and security. In the work described in this thesis, three different versions of TF-QKD have been implemented [1] [3] [2]. To do so, their security analysis had to be reproduced in simulations, as to guide the correct and optimal way of extracting keys in each experiment. This chapter serves as an introduction to these protocols and their security analyses. The protocols are compared in terms of their benefits and drawbacks, not solely in terms of performance, but also of their experimental difficulties.

2.2 Security analysis and channel model

The security analysis of a QKD protocol aims to determine the amount of privacy amplification that the authorised users have to do to extract secure keys from their exchange. It determines how much of the distribution was secure, if any, and hence how many secure bits can be extracted from a particular implementation. The analysis depends on the security definition, as well as on the assumptions made on the devices employed by the users and on the eavesdropper. Typically, the fewer the assumptions, the lower the resulting secure key rate. The final secure key rate of a QKD protocol comprises quantities that can be directly observed in an experiment and quantities that can only be estimated from theory, based on the measured quantities. This chapter will focus on the measurable quantities demanded by each TF-QKD protocol variant and their final key rate equations.

Although key rate formulas can differ significantly from protocol to protocol, there are certain quantities that are always present. There are three terms that should be familiarised as they are always encountered: yield, gain and quantum-bit error rate (QBER). Without loss of generality, let's define these for a point-to point QKD scheme where Alice is the transmitter and Bob the receiver. The yield is of interest for different intensity preparations or bit preparations. If we are interested in the yield of the state with intensity μ it will be denoted as Y_{μ}. Y_{μ} is the conditional probability of Bob making a detection of a μ state, given that Alice has prepared a photon in the μ state. The gain, Q_{μ} is similar to the yield. However this time, it is the absolute probability of Bob making a detection of the μ state irrespective of the state prepared by Alice. At last, the QBER quantity in a protocol, is the ratio between the detected errors and the detection events, and can be directly observed during an implementation. The meaning of an error is defined in every protocol and will be discussed explicitly for each variation.

An important point is that when quantifying the security of a protocol, the target is to always aim for the worst case scenario. Hence, when we refer to key rate formulas, we always refer to the formula that will extract a pessimistic value of the key rate, given the experimental implementation and protocol used. This is the lower bound of a secure key rate formula and hence maximises the security of the extracted key.

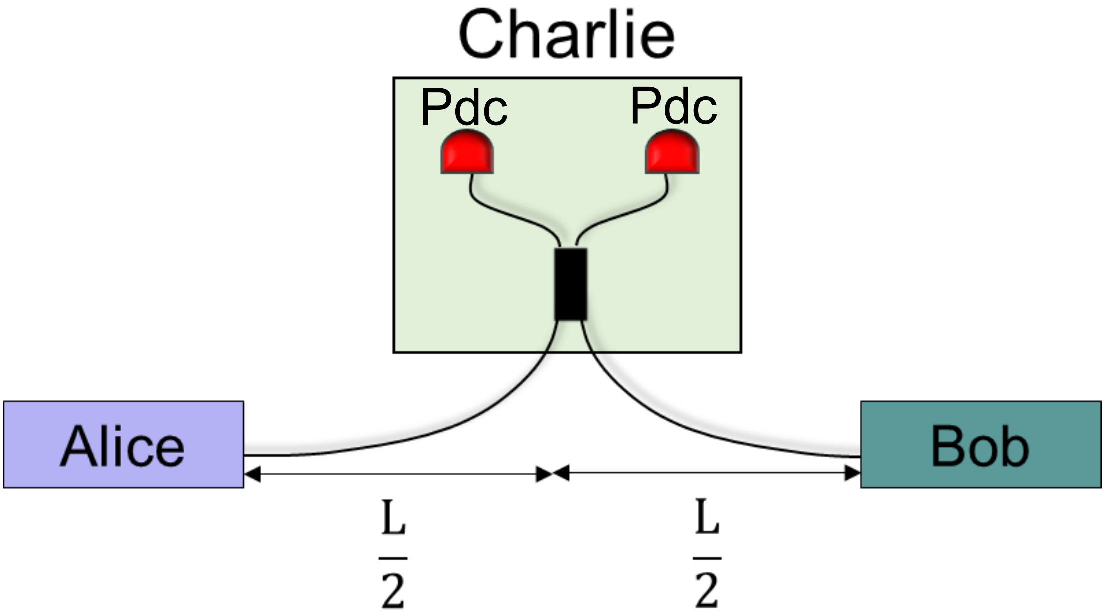

Figure 2.1 **Channel model:** This figure depicts the channel model used in the formulation of the security analyses in this thesis. While the total length, L, of the quantum channel includes both segments from Alice to Charlie and Bob to Charlie, these will be modelled separately. Hence, each fibre channel and detector can be treated independently and then combined to extract the total final key rate.

There are major differences between ideal theoretical models and experimental implementations. The most significant is the fact that in an ideal case scenario, Alice and Bob are exchanging infinite amount of photons. Therefore, there are infinite exchanges of each and all different pieces of information that are relevant to the security analysis. In an infinite dataset there are no statistical fluctuations and the measured values coincide with the true value of the quantity under measurement. This is called the "*asymptotic scenario*" and typically leads to optimistic secret key rates. However, in any real experiment, the experimental dataset is finite and measurements are prone to statistical fluctuations. The measured values fall in a fiducial interval that depends on the overall length of the measurement. Because of the above-mentioned worst-case approach to security, this "*finite-size scenario*" often leads to a significant reduction of the QKD protocol's secure key rate.

A protocol's security analysis depends solely on the measured quantities and the theory's assumptions. However, to build the simulations which will describe these quantities and hence the protocol's performance, a specific channel model is required. In simulations we assume that Eve is not present in the communication but instead that the channel is noisy or lossy. This description on the transmission of the quantum channel will be used to formulate the expressions that can extract the measured quantities such as the gain and the yield. These are then put together according to the protocol's theory to simulate a key rate, given the channel model. Experimental points extracted from the experiments described in this thesis are drawn from the security analysis, while curves that are used to fit the experimental points are drawn from simulations based on the channel model. If the channel model fails, the simulation fails as well, however the experimental point does not. Thus, simulations are improved to match the observed points.

Here, a channel model is defined to be used in all different variations to be explored, even if the original proposal suggests a different version. This is done to maintain homogeneity and continuousness in the thesis and for ease of use. Figure 2.1 shows the structure of the TF-QKD channels of total length L. It is convenient to consider each side, Alice - Charlie and Bob - Charlie, independently to be able to take account of differences in parameters of specific elements such as detectors and channel fibre. To achieve this, the $\frac{L}{2}$ segments are considered separately along with one of the two detectors. The transmittance, η, of half the channel should then be modelled and considered. Equation 2.1 below, formulates this function as:

$$\eta_A = \eta_{det_A} \eta_{Charlie_A} \eta_{AC} \tag{2.1}$$

where η_A is the transmittance on Alice's side. $\eta_{det_A}, \eta_{Charlie_A}$ are the efficiencies of the detector and Charlie's components on Alice's side and η_{AC} is the transmittance of the channel connecting Alice to Charlie. The latter is given below:

$$\eta_{AC} = 10^{\frac{-\alpha \frac{L}{2}}{10}} \tag{2.2}$$

Here, L is the total distance of the two quantum channels, so the distance between Alice and Bob and α is the fibre's average loss coefficient. L was halved since the protocols described in this thesis refer strictly to symmetric channels, where the channel Alice-Charlie has the same length as the channel Bob-Charlie. The same equations, with the subscripts A replaced by B, give the transmittance on Bob's side. Given that two detectors are used in the experiment and each side is considered separately, the final total key rate would be the sum of the ones extracted on each detector.

2.3 The TF-QKD proposal

2.3.1 Protocol and key rate formula

The method for carrying out the protocol of the original proposal of TF-QKD [1] was briefly introduced in chapter 1. Here, a thorough recap is included for completion of the chapter.

- Two authorised and independent users, Alice and Bob, prepare weak coherent pulses which they encode with a global phase randomisation value, $\rho_{A,B}$.
- They each randomly choose a basis, $\alpha_{A,B}$, from the set $\{\mathbb{X},\mathbb{Y}\}$. Whenever the $\mathbb{X}$ basis is chosen by a user he must also phase encode a random bit value, $b_{A,B}$, from the set $\{0,\pi\}$. Instead, in the case of the $\mathbb{Y}$ basis, he must choose the bit to be represented by encoding a value from the set $\{\frac{\pi}{2},\frac{3\pi}{2}\}$.
- Following phase encoding, the two users will also encode a random intensity, μ, on their pulses from a set of three possible states: $\{u,v,w\}$.
- Alice and Bob will now send their fully modulated weak coherent pulses down long independent quantum channels to arrive at Charlie's station.
- Charlie will interfere the incoming pulses on a beam splitter, to observe the resulting first order interference and publicly announce the outcome. The latter refers to which of the two detectors connected to the outputs of the beam splitter clicks, D_0 or D_π.
- After Charlie's announcements, Alice and Bob will announce over a public channel their basis and intensity choices. They will also need to announce the phase slice, Δ, in which the encoded global phase values belonged in for every instance. The latter is achieved by discretising the phase circle into M number of slices.
- To form the raw bit key, Alice and Bob will only keep bit values for the detection events where they have chosen the same global phase slice, intensity and basis.

The key rate formula describing the above protocol is given by:

$$R=\frac{1}{M}\{Q_1^L[1-h(e_1^U)]-f_{EC}Q_{u_Au_b}h(E_{u_Au_b})\} \tag{2.3}$$

where M is the number of phase slices used, Q_1^L is the lower bound of the single-photon gain, e_1^U is the upper bound for the single-photon error rate, f_{EC} is the error correction coefficient and $Q_{u_A u_b}, E_{u_A u_b}$ are the directly observed gain and error quantities of signal pulses. TF-QKD has two important groups of successful events. Successful *signal* events are the instances when Charlie has announced a detection while both Alice and Bob have prepared a state of intensity u with matching $\rho_{A,B}$ and $\alpha_{A,B}$ choices. Successful *decoy* events refer to detection events where Alice and Bob have used matching $\rho_{A,B}$ and $\alpha_{A,B}$ choices and a matching intensity, either v or w. These two groups, signals and decoys, are treated differently in post-processing. Signal events are used to distil a key and therefore are always kept secret. On the other hand, decoy events are used to test the security of the channel against Eve. Hence, all the elements of this group, including the bit values, are publicly revealed on the public channel.

An immediate difference observed between the key rate formula as expressed in equation 2.3 and equivalent formulas for other protocols like the BB84, is the $\frac{1}{M}$ scaling coefficient. The entire security of the TF-QKD proposal is based on the phase encoding, phase randomisation and slicing of the phase circle into M number of slices. Whenever the two pulses prepared by Alice and Bob have interfered at Charlie with different global phase randomisation values the entire information of their initial bit encoding is lost and a random detector clicks. Correct results are more probable when the phase randomisation values used by the two users are the same or different by π. However, if detection events are to be kept solely when these two conditions are satisfied, we would need infinite number of preparations. This is a result of the infinite possible values that can be used in the phase randomisation step. The probability of Alice and Bob making the same choice is negligible and therefore no key can be distilled between the two users. To avoid this and make the protocol practical, the errors should be minimised while the key rate should be finite. To achieve this, the phase circle is divided into M number of slices of width Δ. The two conditions are then relaxed by using slice width intervals, so that the tolerated phase difference becomes $\pm\Delta$ and $\pi \pm \Delta$. This means that only $\frac{2}{M}$ of the number of pulses created in the signal intensity will be useful. In the original proposal, as well as in equation 2.3, the scaling coefficient omits this factor two, since the π difference condition was not considered. However this is a straight-forward improvement to the protocol. Therefore, from here onwards, the phrase "matching phase-slice" refers to either of the two relaxed conditions being satisfied in the preparations of Alice and Bob.

2.3.2 Simulations of measurable quantities

$Q_{u_A u_B}$ and $E_{u_A u_B}$ are the two measurable quantities shown in the key rate formula of this protocol. These are the gain and error of the pulse pairs where both Alice and Bob have encoded the signal intensity u and they have used matching phase slices and bases.

An important point to be discussed is the definition of an error, $E_{\mu_A \mu_B}$, in this particular protocol. Information is encoded in phase and the first order interference is observed on single photon detectors connected to the two outputs of the interference beam splitter. Thus, given that the users have prepared the same intensity state $\mu_A \mu_B$, a click should be observed on detector D_0 when Alice and Bob have encoded the same total phase on their pulses. A click on detector D_π is expected when the two users have encoded values different by π. As a result, a wrong click is defined as the event where a detection is observed on D_0 when the encoded phase difference was π and when the D_π detector clicks while the encoded difference was 0. Contributing factors to the error in this particular protocol are the dark counts, the intrinsic error resulting from the finite width of the slices used, e_Δ, and any base optical error due to imperfect field generation sources or relative phase misalignment at interference, e_{mis}. Dark counts and base optical error can be directly quantified experimentally. e_Δ however will be calculated using the number of slices [1] as shown in the equation below.

$$e_\Delta = \frac{M}{2\pi} \int_0^{\frac{2\pi}{M}} sin^2\left(\frac{\theta}{2}\right) d\theta \tag{2.4}$$

Excluding dark counts and assuming stabilised channels, the total error probability at every point would hence be:

$$e_{opt} = e_{mis} + e_\Delta - e_{mis} e_\Delta \tag{2.5}$$

where e_{mis} includes errors due to the finite indistinguishability of the sources, but also due to the leftover phase error $\frac{\sigma_\phi}{2\pi}$ resulting from an imperfect stabilisation with standard deviation σ_ϕ. Dark counts deteriorate the error and hence as the loss (or distance) in the channel increases, the error should also increase accordingly. Given that a dark count is random and hence has 50% probability of giving a correct outcome, the distance dependent total QBER can be formulated as:

$$E_{\mu_A \mu_B}(L) = e_{opt} + \frac{P_{dc}}{2Q_{\mu_A \mu_B}(L)} \tag{2.6}$$

The optical error, e_{opt}, and the dark count probability per detector, P_{dc}, are independent of distance L, while the gain of the $\mu_A \mu_B$ state, $Q_{\mu_A \mu_B}(L)$, decreases with increasing channel losses.

Since the asymptotic case of the TF-QKD security analysis is considered in ref. [1] and this work, the physical meaning of the quantities gain and yield is identical. This is because the asymptotic case scenario assumes an infinite number of pulses and therefore the probability of sending a specific basis and state will always be equal to 1. Specifically, the yield of the $\mathbb{Z}$-basis state μ_A, μ_B is the probability of Charlie detecting a click, given that Alice and Bob have prepared photons of flux μ_A, μ_B, as shown in the formula below:

$$Y_{\mu_A \mu_B} = P(Z)^2 P(\mu)^2 \left(1 - e^{-\eta(\mu_A+\mu_B)} + P_{dc}\right) \tag{2.7}$$

where $P(Z), P(\mu)$ are the probabilities of a preparation in the $\mathbb{Z}$ basis and the μ state respectively. Since all state preparation probabilities are equal to 1, then $P(Z), P(\mu) = 1$, making the yield a non-conditional detection probability and equating it to the gain:

$$Y_{\mu_A \mu_B} = 1 - e^{-\eta(\mu_A+\mu_B)} + P_{dc} \tag{2.8a}$$

$$\Rightarrow Y_{\mu_A \mu_B} = Q_{\mu_A \mu_B} \tag{2.8b}$$

The exponential term in gain and yield formulas such as the above, arises from the Poisson distributed nature of weak coherent pulses. The fact that this exponential term is negative causes the QBER, $E_{\mu_A \mu_B}(L)$, to increase exponentially with loss.

The gain and error of the $u_A u_B$ state are quantities that must be measured in the experiment, as they are explicitly stated in the key rate formula, equation 2.3. Further experimental observables are hidden within the decoy analysis required to estimate the quantities of Q_1^L and e_1^U related to single-photon pulses. We focus the discussion on modeling the measurable quantities required, without using explicit formulas for the estimations. For the TF-QKD protocol as described here, we notice that all pulse preparations in Alice and Bob, independent of flux, are treated equivalently in terms of phase encoding. Therefore $Q_{\mu_A \mu_B}, E_{\mu_A \mu_B}$ can be measured not only for $u_A u_B$ but also for $u_A u_B$, $v_A v_B$ and $w_A w_B$. Since they have the same physical form, they can also be modelled with the same equations previously described. In fact, these quantities complete the information required to distill keys and assess security in the TF-QKD protocol.

2.3.3 Parameter optimisation

An important part of translating theory to experiment is to explore parameter behaviour in the particular practical case and optimise synchronously for performance and experimental ease.

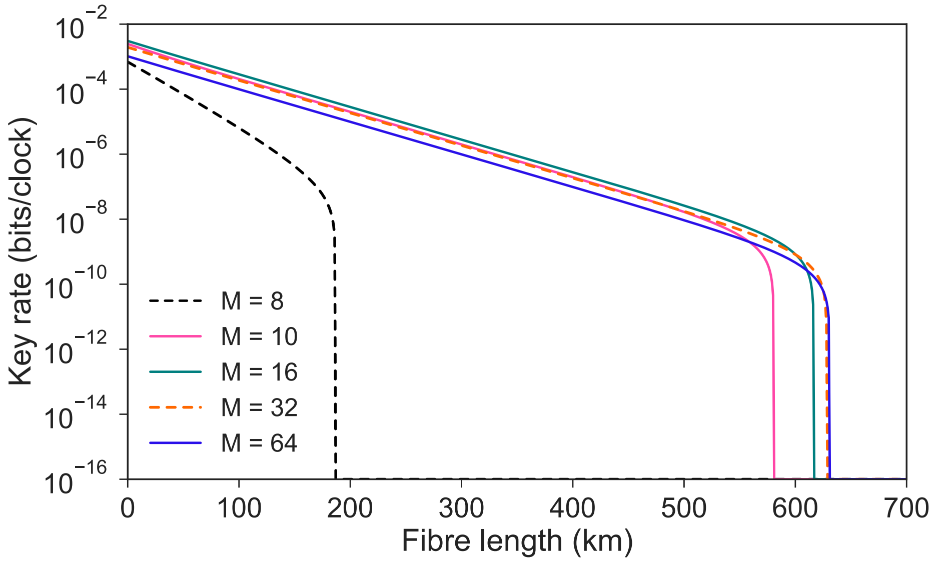

Figure 2.2 **Optimisation - Phase slices:** The number of slices used in TF-QKD is varied from 8 to 64 and the resulting optimised key rate vs fibre length ($\alpha = 0.20\ dB/km$) is plotted. The best value for M seems to be 16, where the key rate and maximum distance trade-off seems optimal.

One of the easiest parameters to optimise is the number of slices that will be used during the sifting stage. Optimising the number of slices counterbalances the effect of the scaling coefficient of the key rate formula with the increase in the overall optical error, e_{opt}, since slice width increase will directly increase e_{Δ}. In the graph plotted in figure 2.2, the key rate versus distance of the TF-QKD protocol is plotted for different number of slices. It is observed that the number of slices must be at least 8 for a positive key rate to be obtained. Below that, the e_{Δ} factor is too large and as a consequence the overall QBER is also too large to extract any key. It is also clear that the greatest effect in maximum distance increase is shown for 16 slices. After that, for double or quadruple the number of slices, we reach the overall limit which is not significantly better. In terms of key rate, it is shown that the maximum value is also achieved in the case of 16 slices. For a larger amount of slices, the effect of the scaling coefficient on key rate decrease seems larger than the effect of QBER decrease, resulting in an overall decrease of the key rate. Consequently, in a general experimental implementation, 16 number of slices seems ideal.

The parameters that must always be optimised before a practical implementation is carried out, are the fluxes of the different states. While the vacuum state, w, invariably needs to stay as low as possible to maximise a key rate formula, the fluxes u, v need to be optimised for every situation. For ease of implementation of this protocol, we decide to keep the ratio

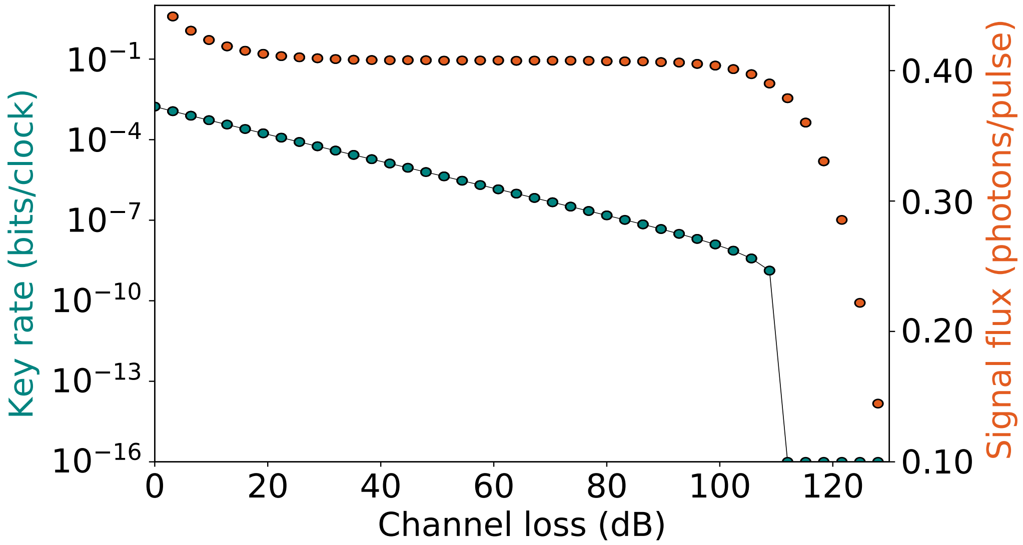

Figure 2.3 **Optimisation - TF-QKD:** The key rate formula as stated in equation 2.3 is optimised in terms signal flux u only. The decoy flux is kept 10 dB lower than the signal for ease of implementation, since it does not affect the performance significantly.

between the v and the u flux at 10 dB. This particular value is chosen empirically. Firstly, it is easy to achieve it with a single Lithium Niobate intensity modulator, the optoelectronic device used in fibre-optic QKD systems. Moreover, this choice is supported by the simulations, where it is observed that a deviation from 10 dB does not provide a significant benefit to the key rate. More details about such devices will be found in the experimental chapters. To find the ideal values of the u, v fluxes, we perform a constrained optimisation by linear approximation (COBYLA). Keeping the 10 dB extinction rate between u and v, we show the optimisation of the u value in figure 2.3. The laboratory parameters used in the optimisation and in plotting the resulting key rates, are shown in table 2.1. For parameters which describe the instruments used in the lab, such as dark counts or efficiency, the values observed in the laboratory at the time were used. From the graph it seems that $u_A + u_B = 0.4$ is a good choice for the overall range of losses. We hence use this value, along with $v_A + v_B = 0.04$, and the previously attained $M = 16$ to plot the optimised key rate in bits per clock versus channel loss. It is observed that the protocol would allow us to extract a positive key rate over 100 dB losses in the quantum channels, given the employed parameters. For standard fibre with loss coefficient 0.20 dB/km this would be equal to over 500 km. For ultra-low-loss fibre of loss coefficient 0.16 dB/km this extends to 625 km.

η_{det}	0.43
$\eta_{Charlie}$	0.70
P_{dc}	$22x10^{-9}$
e_{mis}	0.025
M	16
w	10^{-8}

Table 2.1 **Parameters in optimisations:** Parameters used in all optimisations present in this chapter. η_{det}, detector efficiency; $\eta_{Charlie}$, Charlie's module efficiency; P_{dc}, probability of dark counts; e_{mis}, misalignment error; M, number of phase slices; w, vacuum flux.

2.4 TF-QKD without phase post-selection

In the previous section it was discussed how TF-QKD in its original proposal requires the phase circle to be discretised. Therefore, the described key rate formula included a scaling coefficient which reduced the key rate as the number of slices decreased. Due to this inverse proportionality of slice number and key rate the number of slices should ideally be kept as small as possible. Furthermore, to sample and represent all the slices well, more preparations are needed with more slices. As a result the pattern length and acquisition time for a large number of slices could be unfeasible in practice. The minimum number of slices is also limited, this time by the intrinsic error the slice width causes and adds to the overall optical error. If very few slices are implemented then the error will be high enough to cause the secret key rate to fall to zero. And even though the number of slices was previously optimised given all these facts, its effect will always be present, when the original proposal is implemented.

The scaling coefficient was perceived as a weakness of TF-QKD and for this reason, soon after the first proposal, a variation of the TF-QKD protocol where phase post-selection is omitted was proposed. Three different groups independently worked on the same idea for simplifying the protocol. They have published three similar security analyses based on the same idea and these can be found in ref. [115], ref. [2] and ref. [114]. In this work we will be focusing on the analysis published by Curty, Azuma and Lo [2].

For convenience we will refer to this protocol as the CAL-TF-QKD protocol. The security analysis for CAL-TF-QKD benefits this TF-QKD compared to the original proposal. Firstly, the absence of phase post-selection undoubtedly simplifies its experimental implementation. There is no longer need for extensive post-processing during sifting. And since pulses are not thrown away due to unmatched phase randomisation, less time is required to acquire enough detection events contributing to the distillation of the key. In addition, although it is an information theoretic-secure protocol unlike the original proposal, it still maintains well the rate-loss advantage of TF-QKD due to the absence of the $\frac{1}{M}$ scaling coefficient in the key rate formula. Security will be discussed further in section 2.7.

2.4.1 Protocol, key rate formula and simulations of measurable quantities

The scheme of CAL-TF-QKD [2] is significantly similar to that found in the original proposal by Lucamarini et al [1]. There is however one major difference in the first step of the protocol and in the sifting. Let's change the basis convention to $\mathbb{X}, \mathbb{Z}$ to go in-line with the particular publication. The protocol steps are as follows:

- Alice and Bob independently and randomly choose a basis from the set $\{\mathbb{X}, \mathbb{Z}\}$, with probabilities $P(X)$ and $P(Z)$.
- If the $\mathbb{X}$-basis is chosen, the user will also chose a random bit value, $b_{A,B}$, at random. In the case of $b_{A,B} = 0$ the coherent state $|\alpha\rangle$ is prepared through a phase modulation of 0 rad. Instead, for $b_{A,B} = 1$, the state $|-\alpha\rangle$ is prepared through a phase modulation of π rad. Both of these states are prepared with intensity s.
- If the $\mathbb{Z}$-basis is selected, the user prepares a phase randomised weak coherent pulse, with a global randomisation value, $\rho_{A,B}$ and a random intensity from the set $\{u, v, w\}$.
- The prepared pulses are sent by Alice and Bob down long quantum channels to arrive at Charlie.
- Charlie interferes the incoming pulses on a beam splitter and announces which detector has clicked.
- The two authorised users publicly announce their basis and intensity choices for every detection event. They keep bits extracted solely from the instances where they have both chosen the same basis.

Here we refer to the $\mathbb{X}$-basis as the *code* basis while the $\mathbb{Z}$-basis is the *test* basis. The bit string extracted from code preparations will be used to distil the key, while the bit string from the test preparations will be used to carry out the security analysis.

Compared to TF-QKD, the CAL-TF-QKD protocol is simplified, as it does not demand for a global random phase to be applied on pulses of the code basis. Phase randomisation is only mandatory for extracting security parameters in the decoy basis. Given that the information is entirely encoded in phase, removing the randomisation from the code basis also removes the necessity for phase post-selection during sifting. Announcement of the phase-slice is no longer required, even for the decoy pulses, as all required information for the developed security analysis can be extracted from their random interference. The only requirement that remains, present in all decoy state implementations, is fair and high quality phase randomisation. If this is not fulfilled the decoy states do not enhance the security of the protocol at high losses.

Given the alterations in the scheme, the old security analysis no longer applies and a new one was proposed. The CAL-TF-QKD key rate formula as described in ref. [2] is shown in equation 2.9 below:

$$R_{CAL} = Q_X^{s_A s_B}\left[1 - h(e_{1Z}) - f_{EC} h\left(E_X^{s_A s_B}\right)\right] \tag{2.9}$$

where $Q_X^{s_A s_B}$ is the gain of the code basis, $h(e_{1Z})$ is the minimum entropy of the single-photon phase error rate e_{1Z}, f_{EC} is the error correction coefficient and $h(E_X^{s_A s_B})$ is the minimum entropy of the QBER of the code basis, $E_X^{s_A s_B}$. s is the flux of the code basis states. The authors of the proposal refer to an alternative channel model in their security analysis. They do not separate the system into the two segments. Instead, they treat the entire fibre channel L as one, but still look at independent detection events by square rooting the new transmittance formula to account for the beam splitter in Charlie. Additionally, their quantities are formulated by equations derived following a quantum mechanical approach, which is not as intuitive as the expressions in our channel model. For this and for homogeneity, their channel model was translated to fit the channel model as described in this chapter.

There are two groups of detection events useful in CAL-TF-QKD. Detector 0 clicking with no clicks in detector 1, $D_0\bar{D_1}$, and detector 1 clicking with no clicks in detector 0, $\bar{D_0}D_1$. For each of this cases the proposal separates the four possible preparations by Alice and Bob. Hence, the gain is split into eight separate cases which were formulated based on the transmittance given in equation 2.1. They are given below in equations 2.10, with the total gain per detection event group given at last.

$$Q^{|\alpha,\alpha\rangle}_{D_0\bar{D}_1} = 1 - e^{-\eta\frac{s_A+s_B}{2}(1-cos\theta)} + P_{dc}; Q^{|-\alpha,-\alpha\rangle}_{D_0\bar{D}_1} = Q^{|\alpha,\alpha\rangle}_{D_0\bar{D}_1} \tag{2.10a}$$

$$Q^{|\alpha,-\alpha\rangle}_{D_0\bar{D}_1} = 1 - e^{-\eta\frac{s_A+s_B}{2}(1+cos\theta)} + P_{dc}; Q^{|-\alpha,\alpha\rangle}_{D_0\bar{D}_1} = Q^{|\alpha,-\alpha\rangle}_{D_0\bar{D}_1} \tag{2.10b}$$

$$Q^{|\alpha,\alpha\rangle}_{\bar{D}_0D_1} = 1 - e^{-\eta\frac{s_A+s_B}{2}(1+cos\theta)} + P_{dc}; Q^{|-\alpha,-\alpha\rangle}_{\bar{D}_0D_1} = Q^{|\alpha,\alpha\rangle}_{\bar{D}_0D_1} \tag{2.10c}$$

$$Q^{|\alpha,-\alpha\rangle}_{\bar{D}_0D_1} = 1 - e^{-\eta\frac{s_A+s_B}{2}(1-cos\theta)} + P_{dc}; Q^{|-\alpha,\alpha\rangle}_{\bar{D}_0D_1} = Q^{|\alpha,-\alpha\rangle}_{\bar{D}_0D_1} \tag{2.10d}$$

$$\Rightarrow Q_{D_0\bar{D}_1} = \frac{1}{4}\left(Q^{|\alpha,\alpha\rangle}_{D_0\bar{D}_1} + Q^{|-\alpha,-\alpha\rangle}_{D_0\bar{D}_1} + Q^{|\alpha,-\alpha\rangle}_{D_0\bar{D}_1} + Q^{|-\alpha,\alpha\rangle}_{D_0\bar{D}_1}\right) \tag{2.10e}$$

$$\Rightarrow Q_{\bar{D}_0D_1} = \frac{1}{4}\left(Q^{|\alpha,\alpha\rangle}_{\bar{D}_0D_1} + Q^{|-\alpha,-\alpha\rangle}_{\bar{D}_0D_1} + Q^{|\alpha,-\alpha\rangle}_{\bar{D}_0D_1} + Q^{|-\alpha,\alpha\rangle}_{\bar{D}_0D_1}\right) \tag{2.10f}$$

The base optical error between Alice and Bob, e_{opt}, was translated into an angle θ through equations 2.11:

$$\theta_A = sin^{-1}(\sqrt{e_{opt}}) \tag{2.11a}$$

$$\theta_B = -sin^{-1}(\sqrt{e_{opt}}) \tag{2.11b}$$

$$\Rightarrow \theta_{BA} = \theta_B - \theta_A = \theta \tag{2.11c}$$

From the gains it follows that the $\mathbb{X}$-basis error will be given by:

$$E_{D_0\bar{D}_1} = \frac{Q^{|\alpha,\alpha\rangle}_{D_0\bar{D}_1} + Q^{|-\alpha,-\alpha\rangle}_{D_0\bar{D}_1}}{4Q_{D_0\bar{D}_1}} \tag{2.12a}$$

$$E_{\bar{D}_0D_1} = \frac{Q^{|\alpha,-\alpha\rangle}_{\bar{D}_0D_1} + Q^{|-\alpha,\alpha\rangle}_{\bar{D}_0D_1}}{4Q_{\bar{D}_0D_1}} \tag{2.12b}$$

$$\Rightarrow E_X^{s_As_B} = \frac{E_{D_0\bar{D}_1} + E_{\bar{D}_0D_1}}{2} \tag{2.12c}$$

which finalises the quantity modesls in the X basis analysis.

Moving to the decoy state analysis, there are two methods that can be implemented. The first is the numerical method and it is used in the aforementioned proposal found in ref. [2]. The second is the analytical method and was published later on in 2019 in ref. [116]. In this thesis, the analytical version was used. Further details about the derivations are beyond the scope of the chapter and will not be disclosed. As mentioned in the protocol description, decoy pulses are phase randomised but will not be post-selected based on phase slice. Thus, there is no way of extracting an optical error from them. Instead, the formula for e_{1Z} utilises the gains of all different combinations of fluxes to estimate the upper and lower limits of

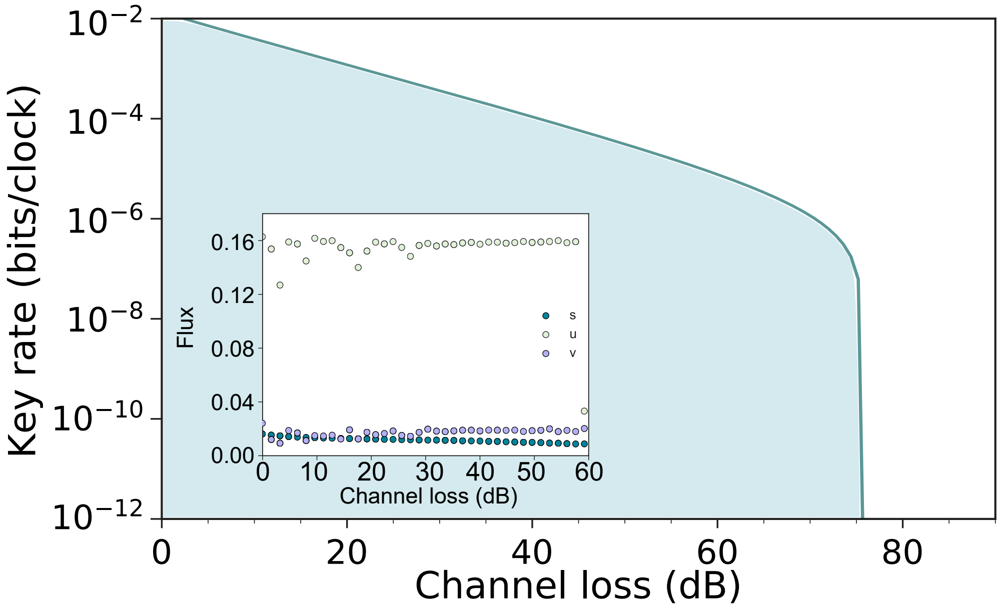

Figure 2.4 **Optimisation - CAL-TF-QKD:** The CAL-TF-QKD performance with optimised signal flux, s, first decoy flux, u, and second decoy flux, v. The inset graph shows the evolution of these parameters. It is noticeable that s and v tend to similar values and hence the same flux could be used for both.

n-photon yields up to Y_{20}, Y_{02} and uses those to extract an error. Consequently, while only the $s_A s_B$ state error has to be monitored, all combinations of states from the set $\{u, v, w\}$ have to be monitored in terms of gain for a complete analysis. These are modelled using the 0th order modified Bessel function of the first kind, $I_0(x)$:

$$Q^{\mu_A,\mu_B}_{D_0\bar{D}_1} = 1 - e^{-\eta \frac{\mu_A+\mu_B}{2}} I_0(\eta \mu_A \mu_B cos\theta) + Pdc = Q^{\mu_A,\mu_B}_{D_0\bar{D}_1} \tag{2.13}$$

2.4.2 Optimisation

One interesting fact about this protocol is the behavior of the optimal values for the state intensities. The protocol was suggested to be used with four different intensities including the vacuum. Through performing a COBYLA optimisation for the four intensity states (inset of figure 2.4) it is discovered that the signal state is not the strongest of the fluxes in the ideal case. Its flux actually is similar to the flux required for the second intensity state v. For ease of implementation, in the experiments to follow, we will always create a total of three intensities including the vacuum. Thus, in this case, the value of the signal flux, s, will be used for v as well, e.g. $s, u, v = s, w$, like the optimisation suggests. The optimised result of the key rate versus channel loss for the CAL-TF-QKD protocol with three intensities is plotted in the main part of figure 2.4. The same parameters used for the simulation of the TF-QKD protocol in the previous section (table 2.1) were used for this optimisation and the resulting key rate vs. distance plot. From the graph it is deduced that the CAL-TF-QKD protocol, with three intensity states and the experimental parameters observed in the lab, is able to distil a secure key up to a total channel loss of 76 dB. This is equivalent to 380 km of standard fibre and 475 km of ultra-low-loss fibre.

2.5 Send, not-send TF-QKD

The most counter-intuitive of the TF-QKD variations would be the *send, not-send* (SNS) TF-QKD porotocol [3]. While the rest of the variants focus on following the original proposals phase encoding to distil keys, the SNS changes the code basis to an intensity encoded basis. As the name suggests, bits are encoded by sending or not sending a pulse, which is equal to preparing a pulse of signal flux or a vacuum pulse. This not only benefits the practical feasibility of the protocol but it also has some interesting effects on the QBER. These effects make it highly tolerant to misalignment error and they can be taken advantage of to push the protocol to extreme distances, as will be discussed in section 2.6.

2.5.1 Protocol and key rate formula

The protocol, as proposed in ref. [3], asks for the following procedure:

- Alice and Bob each independently and randomly choose one of two bases from $\{\mathbb{Z},\mathbb{X}\}$. If they have chosen the $\mathbb{Z}$-basis then they must prepare a weak coherent pulse of flux u with probability ε, or prepare a vacuum pulse with probability $(1-\varepsilon)$.
  In the case of choosing the X-basis, they must prepare a weak coherent pulse with a global random phase $\rho_{A,B}$. The intensity of each $\mathbb{X}$-basis pulse is chosen at random from the set of $\{u,v,w\}$.
- Alice and Bob send their prepared pulses down long quantum channels to arrive at Charlie's station
- Charlie performs a first order interference measurement using a beam splitter with one detector connected to each of its outputs. He publicly announces all detection events and which detector clicked in each instance.

Preparation		Outcome
Alice	Bob	$b_A b_B$
s	s	10
s	n	11
n	s	00
n	n	01

Table 2.2 **SNS-TF-QKD key distillation combinations:** Summary of all possible successful detection event outcomes in the Z basis. The first two columns show the preparations of Alice and Bob, where s stands for sending a pulse with probability ε and n stands for not sending anything with probability $(1-\varepsilon)$. For each case the resulting distilled bits by Alice and Bob are shown in the final column. It is apparent that correct outcomes occur only one of the two users has prepared and sent a pulse.

- Alice and Bob announce their basis choices. For the instances where they have chosen the $\mathbb{Z}$-basis, no further announcements are necessary. Instead, for pulses prepared in the $\mathbb{X}$-basis, they must also announce the intensity as well as the phase slice, from the predetermined M number of slices, in which their global randomisation phase choice falls in.
- They will form a key bit-string from all instances where they have both chosen the $\mathbb{Z}$-basis and Charlie announced a detection. They will also keep all detection events where they have both made preparations in the $\mathbb{X}$-basis. However, the decoy bit string will be extracted from detection events where they have both prepared the $\mathbb{X}$-basis with identical intensities and matching global phase randomisation slices.

The $\mathbb{Z}$-basis forms the code basis for key distillation while the $\mathbb{X}$-basis is the test basis for security assessment. Table 2.2 shows the outcome of every possible combination of $\mathbb{Z}$-basis preparations made by Alice and Bob. When Charlie announces a detection, Alice (Bob) will add a bit 1 (0) to the key whenever she (he) has chosen to send a pulse. Otherwise, a bit 0 (1) is added to the key. It is consequently the case that, all instances where both or none have chosen to sent a pulse will generate errors in the bit-string key. Correct bits are extracted whenever only one user has chosen to sent a pulse. Thus, the error is no longer dependent on phase mismatch errors and is instead fully attributed to the ε parameter. In a perfect system with zero dark counts, the probability of errors in the key is fixed and independent of the channel. More specifically, in the next section (2.5.2), the QBER acquired in a perfect system will be proven to be equal to ε, a therefore vital parameter to optimise.

The key rate formula of SNS-TF-QKD, just like its procedure, is very much separated in two parts. It is given in equation 2.14 below [117].

$$R = Q_1^L \left[1 - h(e_1^U)\right] - f_{EC} Q_Z h(E_Z) \tag{2.14}$$

The first part from the left-hand side is completely extracted from decoy states and all the errors related to it will not affect the code basis at all. Q_1^L is the lower bound of the single-photon gain and e_1^U is the upper bound of the single-photon phase error rate. The second part of the equation uses information extracted entirely from the code basis and essentially depends solely on the parameter ε.

2.5.2 Simulations of measurable quantities

The channel model used in the SNS protocol is identical to that used in the TF-QKD protocol in section 2.3. A minor difference that will be considered is the fact that the vacuum state will not be dismissed as easily. Due to the sending probability, ε, in the $\mathbb{Z}$-basis being small, a lot of the preparations will be just vacuums. Starting from the yield of any state $\mu_A \mu_B$, the equation remains the same and is shown below:

$$Y_{\mu_A \mu_B} = 1 - e^{-\eta(\mu_A + \mu_B)} + P_{dc} \tag{2.15}$$

Yields are independent of specific state preparation as they are essentially normalised gains and hence the equation is unchanged with no reference to the new parameter ε. In this protocol, the possible state combinations are the set comprised of both $\mathbb{XX}, \mathbb{ZZ}$ as well as $\mathbb{ZX}, \mathbb{XZ}$ pairs. Nevertheless, taking advantage of mixed basis combinations only improves the key rate in the case of the finite-size analysis. Since solely the asymptotic analysis is considered here, we will just keep the reduced set of pure basis combinations. In contrast to the yields, the gain of the $\mathbb{Z}$-basis in the SNS protocol is strongly dependent on the sending probability, ε. From table 2.2, summarising all the possible combinations of the code basis, we can extract the formula required to formulate the gain, equation 2.16, and the error, equation 2.17, expected in the $\mathbb{Z}$-basis.

$$Q_Z = \varepsilon(1-\varepsilon)Y_{sn} + (1-\varepsilon)\varepsilon Y_{ns} + \varepsilon^2 Y_{ss} + (1-\varepsilon)^2 Y_{nn} \tag{2.16}$$

$$E_Z = \frac{\varepsilon^2 Y_{ss} + (1-\varepsilon)^2 Y_{nn}}{Q_Z} \tag{2.17}$$

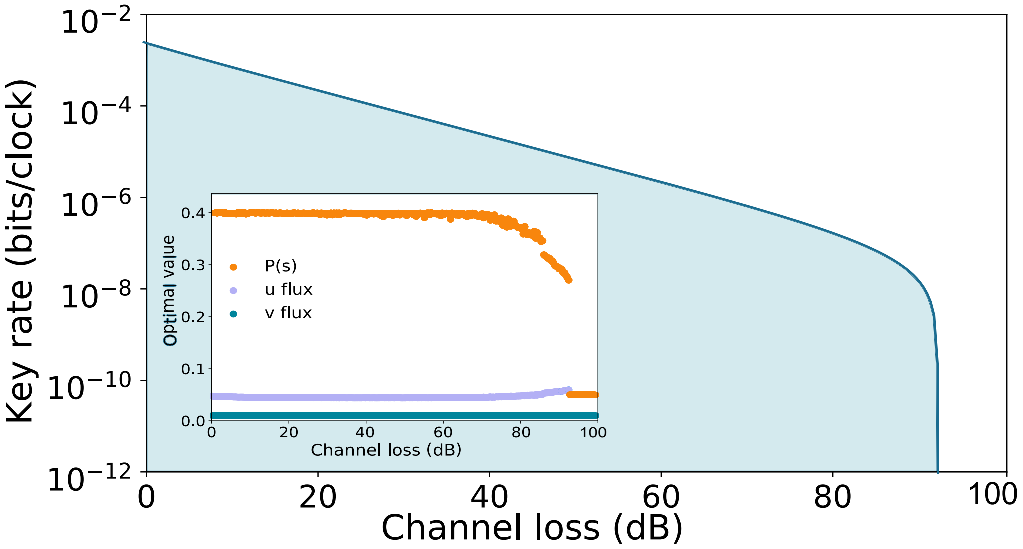

Figure 2.5 **Optimisation - SNS-TF-QKD:** Plot of the optimised key rate versus channel loss for the SNS-TF-QKD protocol. The optimisation takes into account the probability of sending, P(s), the signal flux and first decoy flux, u, and the flux of the second decoy, v. The evolution of these parameters is shown by the inset graph.

Assuming zero dark counts and perfect state preparation: $Y_{nn} = w = 0$ and $Y_{ss} = 2Y_{ns} = 2Y_{sn}$ Hence:

$$E_Z \approx \frac{\varepsilon^2 2Y_{sn}}{2\varepsilon(1-\varepsilon)Y_{sn} + \varepsilon^2 2Y_{sn}} \tag{2.18a}$$

$$\Rightarrow E_Z \approx \varepsilon \tag{2.18b}$$

It is therefore deduced that the base QBER in the SNS-TF-QKD protocol will be approximately equal to the sending probability ε and, in a realistic system, will increase as dark counts become more significant with increasing channel loss.

The $\mathbb{X}$-basis of the SNS protocol will be treated similarly to the TF-QKD protocol. Formulas for the estimation of Q_1^L and e_1^U require the yields of all decoy state combinations. In the case that the state is a combination of mixed intensities, all detection events are retained and their yields are required. The optical error E_X is extracted from matching intensity states, whose yields are also needed. E_X, in this case, is an outcome of the phase misalignment of pulses with a randomisation slice different by 0 or π radians, or the normalised extinction ratio between the two groups. Therefore E_X is given by:

$$E_X^{\mu_A\mu_B} = \frac{1}{2} + \frac{P_{dc}}{2Y_X^{\mu_A\mu_B}}\left(e^{-\eta(\mu_A+\mu_B)(1-e_{opt})} - e^{-\eta(\mu_A+\mu_B)e_{opt}}\right) \tag{2.19}$$

where $Y_X^{\mu_A\mu_B}$ is the yield of the $\mu_A\mu_B$ state in the $\mathbb{X}$-basis, described by equation 2.15. Consequently, the quantity Q_1^L will be deduced from all mixed intensity decoy events, while e_1^U solely from matched intensities.

2.5.3 Optimisation

Optimisation of the performance of the protocol for varying channel loss depends on the three state fluxes as well as the sending probability ε. Therefore, a global optimisation with COBYLA is performed on the four parameters. The ideal values of the four quantities are shown on the inset of figure 2.5, with the resulting key rate plotted for channel losses up to 100 dB. Keeping the experimental parameters the same, the SNS-TF-QKD protocol allows us to extract a key for a channel of 92 dB maximum loss. In standard fibre this is equivalent to 460 km while if ultra-low-loss fibre is used 575 km can be reached.

2.6 Sending, not-sending TF-QKD with two-way classical communication

In the previous section, the behaviour of the errors in the SNS-TF-QKD protocol was described. Errors in the key distillation basis are fully independent on any phase misalignment error, which instead only contributes to the single-photon phase error rate, extracted from the decoy basis. Due to this effect, the author of the first SNS protocol has been able to combine his proposal with a classical post-processing error-correction technique know as two-way classical communication (TWCC) [118]. The classical techniques significantly increases the signal-to-noise ratio of the code basis at high losses. As a result, a great improvement in the maximum distance achievable with the SNS-TF-QKD protocol is observed. A difference between this protocol and the rest is that, to truly implement it, it is mandatory to extract real bit-strings from the QKD experiment, due to the bit-wise operations.

2.6.1 Protocol and key rate formula

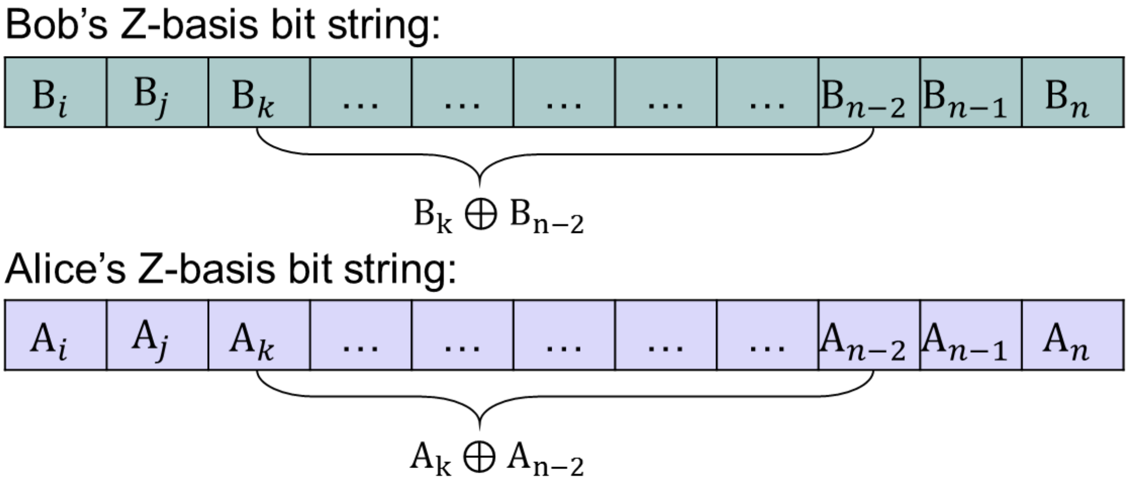

Figure 2.6 **Two-way classical communication post-processing:** In two-way classical communication, the two users must randomly pair up bits distilled in the key generation basis. They will use a modulo addition operation on the pairs and only keep the first bit of every pair whose modulo addition produces the same result in both Alice and Bob.

TWCC is a post-processing technique applied on Alice and Bob's Z-basis bit strings extracted from an implementation of the SNS-TF-QKD protocol. The method can be described in the steps below and with the aid of figure 2.6. These steps must be implemented after completing the sifting stage in the implementation of the standard SNS-TF-QKD protocol:

- Bob randomly pairs up the bits in his $\mathbb{Z}$-basis string of length n and performs the bit-wise modulo addition operation on each pari, e.g. $B_k \oplus B_{n-2}$ from figure 2.6.
- He announces the positions of the bits he has paired, e.g. $(k, n-2)$, and the result of the modulo operation.
- Alice pairs up her bits according to the positions announced by Bob and performs the bit-wise modulo addition operation on her pairs, e.g. $A_k \oplus A_{n-2}$.
- Alice announces the positions of the pairs for which her modulo operation result matched Bob's.
- As a result, the two users reduce their initial bit string to one of length n_t, comprised solely of the first bit from each successful pair, discarding all other bits.

This process will reduce the errors observed in the key distillation basis, while at the same time, the gain of the $\mathbb{Z}$-basis will also be reduced. Nevertheless, the overall signal-to-noise ratio is improved, which allows for enhanced tolerance to dark counts at long distances. They key rate formula of the SNS-TF-QKD with TWCC protocol is given by:

$$R = \frac{1}{N_{tot}} \left\{ \tilde{n_1} \left[1 - h(\tilde{e_1}^U)\right] - f_{EC} \left[n_{t_1} h(E_{t_1}) + n_{t_2} h(E_{t_2}) + n_{t_3} h(E_{t_3})\right] \right\} \tag{2.20}$$

where N_{tot} is the total number of preparations by Alice and Bob, $\tilde{n_1}, \tilde{e_1}$ are the single-photon gain and single-photon phase error after TWCC and n_{t_i}, E_{t_i} are the gains and errors of three groups that occur during the bit pairing in TWCC. These groups will be introduced in the next section.

2.6.2 Simulations of measurable quantities

During the TWCC pairing process, three different pairing groups will be formed. The first class, t_1, contains all pairs with odd-parity. The second class, t_2, contains the even-parity pairs where both bits are 0 and the final class, t_3, contains the even-parity pairs with both bits equal to 1. Thus, the final gains and errors that can be measured from the TWCC bit-string, are extracted from three different sets of bits, formed by separating them based on which of the aforementioned classes they belong in.

To simulate the quantities required in the key rate formula, one must consider all preparations of Alice and Bob which would contribute to bits in every class. It is easy to then see that the three classes are comprised of the following preparation combinations:

$$\{VD, DV, C1C0, C0C1\} \in t_1 \tag{2.21a}$$

$$\{DD, C0C0\} \in t_2 \tag{2.21b}$$

$$\{VV, C1C1\} \in t_3 \tag{2.21c}$$

where V, nobody sent; D, both sent; C1C0, Alice sent Bob didn't; C0C1, Bob sent Alice didn't. The total number of bits obtained from each preparation combination, n_{k_A,k_B}, can be found as follows:

$$n_{k_1,k_2} = \frac{N_{tot} Q_Z}{2} \frac{N_{tot} Q_{k_1}}{N_{tot} Q_Z} \frac{N_{tot} Q_{k_2}}{N_{tot} Q_Z} \tag{2.22}$$

where k_1, k_2 are the preparations the first and second bit respectively, N_{tot} is the total number of state preparations by Alice and Bob, Q_Z is the gain of the Z-basis as found in equation 2.16 and $Q_{k_{1,2}}$ is the gain of the particular preparation within the $\mathbb{Z}$-basis. Consequently the total bits in each of the three groups are given by:

$$n_{t_1} = n_{VD} + n_{DV} + n_{C1C0} + n_{C0C1} \tag{2.23a}$$

$$n_{t_2} = n_{DD} + n_{C0C0} \tag{2.23b}$$

$$n_{t_3} = n_{VV} + n_{C1C1} \tag{2.23c}$$

We can also deduce which preparation pairs will produce errors in the final TWCC string. Combining a bit occurring from the case where both didn't send with a bit from a preparation where both sent (DV, VD pairs) is guaranteed to generate an error between the strings of Alice and Bob. This combination will produce a 10 (01) bit-pair for one user and a 01 (10) bit-pair for the other. As a result, the parity calculation of Alice and Bob will agree and they each will keep the first bit in their pair. Since the bit positions are swapped between the two users, the key-bit resulting from the TWCC process on this combination will be different in Alice and Bob. For the same reasons, the DD and VV pairs also contribute to errors. Thus, the errors in the final string are given by:

$$E_{t_1} = \frac{n_{VD} + n_{DV}}{n_{t_1}} \tag{2.24a}$$

$$E_{t_2} = \frac{n_{DD}}{n_{t_2}} \tag{2.24b}$$

$$E_{t_3} = \frac{n_{VV}}{n_{t_3}} \tag{2.24c}$$

Since this process is only applied on the code basis, the decoy basis does not require extra quantity exploration. Consequently, to implement the decoy analysis in the TWCC method, it is enough to have the initial and the final string lengths and combine them with the single-photon phase error rate already extracted from the SNS-TF-QKD $\mathbb{X}$-basis analysis.

2.6.3 Optimisation

The optimal parameters found for the SNS-TF-QKD protocol in section 2.5, are not expected to be ideal in the case of the TWCC enhancement. When employing the TWCC technique, at least 50% of the bits will be lost. The ideal case expects only 25% of the initial SNS string to remain in the final key. It is hence anticipated that the sending probability (or flux) would increase, to make up for a fraction of the losses of the method. Performing a COBYLA optimisation with the new security analysis that includes the TWCC effects, this is

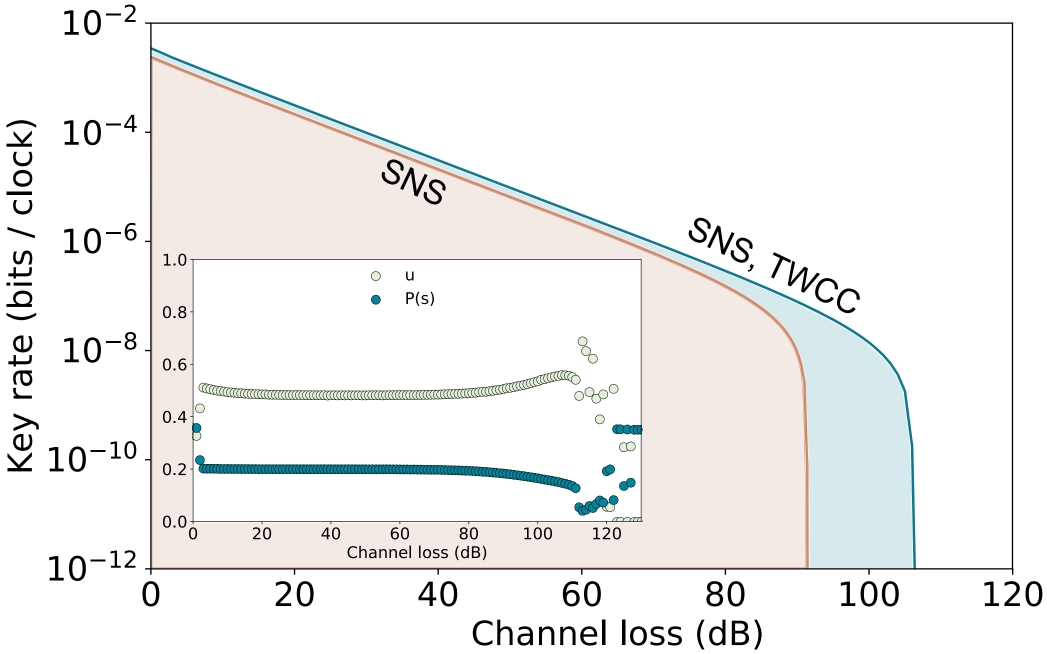

Figure 2.7 **Optimisation - SNS-TF-QKD with TWCC:**

confirmed. As with the SNS-TF-QKD analysis, we consider a three intensity implementation with $\{u, v, w\}$ where u is used for both the signal and the first decoy state. Once again, the second decoy, v, is constrained to 10% of the signal flux. The inset of figure 2.7 shows the results of the optimisation for the signal flux, u, and the sending probability $P(s) = \varepsilon$. The latter has increased from around 5% found in the standard SNS protocol, to around 20% for the TWCC protocol at almost every loss value. This increase aims to counterbalance the significant losses affecting the bit-string after TWCC is applied.

Impressively, the maximum channel loss that can now be tolerated by the SNS protocol is extended to 107 dB. The advantage of TWCC over the standard SNS protocol is shown by the blue fill in figure 2.7. Not only is the maximum loss tolerated dramatically extended, but moreover, the secret key rate at lower losses has increased by a factor 1.5. These benefits can be explained looking closely at the effect of TWCC. The method forces the elimination of all bit pairs containing one error while it guarantees that bit pairs with no errors will remain. Hence, while the majority of the bit-string of each user will be discarded, the new, shorter strings will be of remarkably reduced QBER. As a result, the overall signal-to-noise ratio is improved. The direct comparison of the SNS protocol, with and without TWCC, as shown in figure 2.7 proves exactly that. This makes the SNS-TF-QKD with TWCC protocol by far the most loss tolerant of the proposals and the best performing at high loss.

2.7 Comparison of variations

It is of high importance to understand how the four aforementioned protocols compare. There are three aspects we need to take into account when comparing the different variants: security, performance and practicality. The first two parameters are of interest to both the theoreticians proposing protocols and to the experimentalists looking to implement them. Ease of implementation is key for practicality and can ultimately be the prohibiting factor for experiments. Nevertheless, all three are to be taken into account to assess the suitability of variations in different situations.

The easiest parameter for comparison is the security, as due to its importance, it is always examined in protocol proposals. Information theoretic security is typically studied by casting a protocol into entanglement based QKD (section 1.2.2). The latter provides the simplest description of an information theoretically secure protocol, hence why it is used. If a protocol can be proven to be secure in this description, then it is directly derived that its original form is also secure. For a protocol where security is proven only for a certain set of attacks, this set must be defined. The original TF-QKD proposal in its initial publication was proven secure but only against such a set of attacks. This limitation was lifted in a following publication, ref. [119], where the security against general attacks was proven, at the expense of performance. Protocols with improved performance were then explored, like the CAL-TF-QKD and SNS-TF-QKD. The CAL-TF-QKD [2] and its similar variants [115, 114] are secure against general attacks, thus representing a stronger version, security-wise, of the original protocol. Finally, all SNS variations described previously [3, 117, 118] have been proven to be secure against general attacks as well.

In terms of pure performance, let's first compare the behaviour of the optimal key rates vs. channel loss, for all four variants plotted in figure 2.8. Again, all protocols here are simulated using the experimental parameters found in table 2.1 and the same channel model. The reference for comparison is the original TF-QKD proposal drawn by the light blue, dashed line. A dashed line is used to represent this protocol, firstly to separate and note it as the original proposal and secondly as to note that its comparison with the other variants should not be direct. From the set of all plotted variants, TF-QKD is the only one whose security proof assumes some restrictions on Eve's action. Hence, while it visibly performs better in terms of loss tolerance extracting a positive secure key rate up to 116 dB of loss, it does not provide equal security.

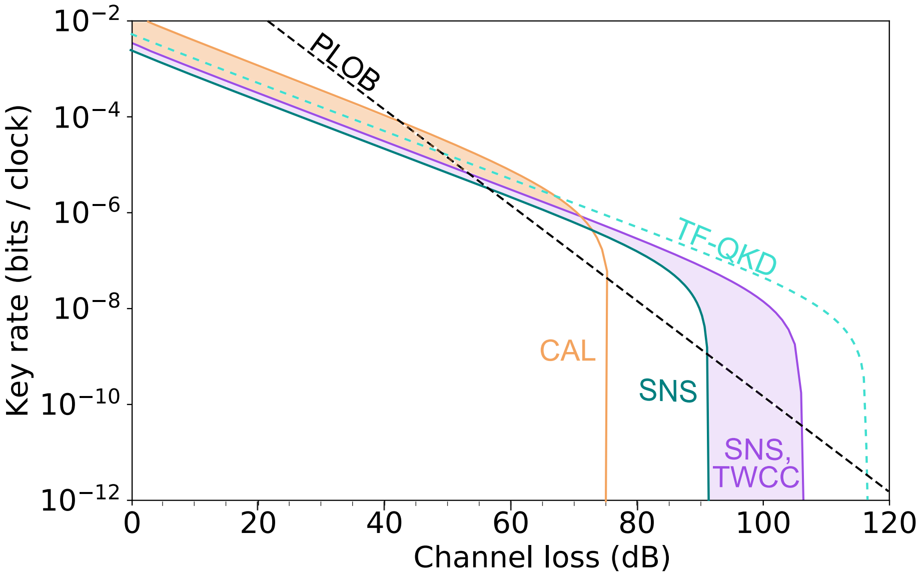

Figure 2.8 **Key rate vs. loss comparison of all protocols:** A plot comparing the performance of all protocols with reference to the original TF-QKD protocol. While SNS-TF-QKD with TWCC clearly outperforms other protocols in terms of maximum loss, CAL-TF-QKD offers significantly higher key rates at low losses.

In terms of key rate at short distances, the CAL-TF-QKD protocol performs the best with a key rate at 0 dB around 9 and 6 orders of magnitude higher than the SNS protocol with and without TWCC respectively, and 4 orders of magnitude higher than the original TF-QKD protocol. Although all four variants beat the SKC bound at high loss, CAL-TF-QKD is able to do it at the lowest loss, which is 40 dB for the chosen parameters, 10 dB less than the original proposal. SNS variants are able to surpass the SKC at higher losses than both the CAL-TF-QKD and the TF-QKD protocols. The TWCC variant overcomes the SKC at around 55 dB, while it's standard counterpart from 57 dB.

Nevertheless, while the SNS-TF-QKD extracts slightly lower key rates, its advantage in highly lossy channels is significantly stronger than the key rate penalty. Regarding loss tolerance, the TWCC methods seems to boost significantly the maximum distance achievable when implementing the SNS protocol, from 92 dB to 108 dB. This is only 8 dB less than the original but provides information-theoretic security. Instead, the CAL-TF-QKD variant fails to extract a key once the channel loss exceeds 75 dB.

Another figure of merit for the performance of the protocols, is their tolerance to phase misalignment error. In figure 2.9 the maximum key rate achieved at 100 km by each protocol as a function of phase misalignment error is plotted. For this, it is assumed that the

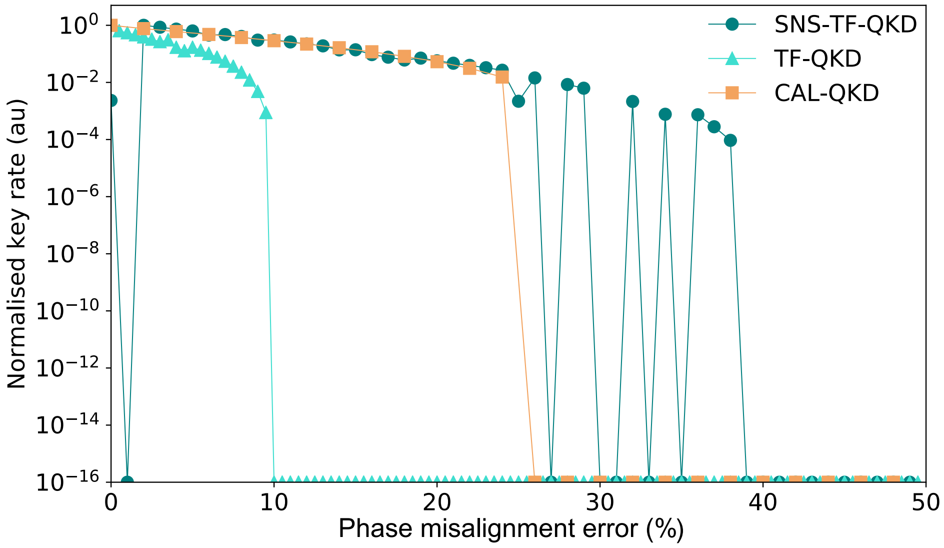

Figure 2.9 **Phase misalignment error tolerance:** The key rate output of the three protocols is optimised at 100 km for increasing phase misalignment error, defined as $\frac{\sigma_\phi}{2\pi}$, with σ_ϕ the standard deviation of the phase. Normalisation of the key rate is performed to aid visualisation while dark count probability is set to zero to avoid any effects on the total QBER.

phase misalignment error is entirely attributed to an imperfect stabilisation of the phase and therefore it is defined as $\frac{\sigma_\phi}{2\pi}$. Dark count probability is set to zero, such that the only source of error is the phase misalignment error while the key rate extracted is normalised to ease visualisation.

SNS-TF-QKD is also known as "TF-QKD with large misalignment error", something that is evident in the plot. With SNS-TF-QKD, a positive key rate can be extracted for up to 38% misalignment error. This is expected, as the particular protocol replaces phase encoding in the key distillation basis with intensity encoding. Hence, phase error does not directly affect the generation of a key, but has an less pronounced, indirect effect on the single-photon phase error estimation of the decoy basis. To achieve positive key rates at high misalignment error,it was observed that the probability of sending a pulse, ε must decrease significantly. This makes the optimisation process difficult at high misalignment error, causing the drops to zero key rate, as can be seen in figure 2.9. These are therefore not a physical phenomenon, but rather a simulation problem which could be removed by repeating the optimisation process until it succeeds for every error value, although this would be time consuming.

CAL-TF-QKD also seems robust to phase misalignment. As shown in the figure, it can tolerate a maximum of 26% error before falling to negative key rate. For this protocol, the robustness is attributed to the phase post-selection necessitated only in the decoy basis and to an efficient security analysis.

Finally, TF-QKD, as originally proposed, seems to be the protocol most susceptible to phase misalignment. It can tolerate a maximum of 10% phase error before falling to negative key rate. It is clear from the figure that the three protocols show different levels of phase misalignment tolerance. Therefore, depending on the conditions of a practical implementation, such as phase noise level, a different variant might be suitable.

At last, the difficulty of implementing each variant should be discussed. Any experimental implementation of TF-QKD is challenging, given the strict requirements set by the phase encoding. Phase drift in 500 km long fibres can be in the order of 20 rad/ms [1] and hence accurate correction may be unachievable. The fact that the SNS protocol is highly tolerant to errors in phase alignment slightly relaxes the requirements on the phase which could be advantageous in an experiment. Additionally, the intensity encoding in the $\mathbb{Z}$-basis is straightforward to implement. Nevertheless, the SNS has a small probability of sending a pulse in the $\mathbb{Z}$-basis which, in the finite-size case, could degrade the quality of a phase stabilisation scheme, increasing the single-photon phase error and eventually making the protocol unfeasible. It also still requires post-selection in the $\mathbb{X}$-basis, a procedure that necessitates longer acquisition times and a big amount of post-processing. Post-processing software can be quite complicated and can be slow in sifting the key.

The CAL-TF-QKD protocol removes the requirement for phase post-selection and is hence simpler to implement. Nevertheless the low ideal flux of the signal could have the same effect as the low sending probability in SNS. Since this protocol is not tolerant to phase noise, this could make its implementation, although simpler in principle, more difficult in practice.

The difficulty in implementing the original TF-QKD protocol lies in the post-selection of all pulses. While the requirements in terms of phase stability are midway between the SNS and the CAL protocols, the fact that most pulses will be thrown away, in both the key distillation basis and the security assessment basis, means that it would require a longer acquisition time and more post-processing.

Finally, the TWCC enhancement to the SNS variation is only a post-processing technique with crucial advantages. If the SNS protocol is to be implemented, the TWCC technique could be a straightforward extension to it. This nevertheless depends on the nature of the experiment. If it is a fully proof-of-principle demonstration, then the TWCC quantities could be estimated without extracting real bits. On the other hand, if the technique is to be truly implemented, then bit-strings must be extracted. Doing this is a difficult process, as average quantities of gains are no longer useful and all counts must be treated individually. Extracting and analysing single counts is a timely and complex procedure, hence why the majority of QKD demonstrations do not involve the acquisition of bit-strings. Nevertheless, if QKD is to escape the academic scope and be commercially available, it will become necessary to extract real bit-string keys.

Chapter 3

Practical TF-QKD beyond the repeaterless secret key capacity

The first section of this chapter will describe the first ever practical implementation of TF-QKD. This demonstration does not incorporate the use of long fibres but instead simulates their losses with optical attenuators. Three different TF-QKD variants will be implemented experimentally in a proof-of-principle demonstration. A side-experiment will also be described to support the validity of these findings and quality of the setup. The work described here was first to achieve two important milestones for quantum communications. As aforementioned, it successfully carried out the TF-QKD protocol and two of its variants for the first time and proved its feasibility in practice. Moreover, and quite significantly, it is the first system to show a repeater-like behaviour. The gain of the system shows the same trend you would expect from a quantum communications system including one repeater. Its overall performance clearly beats point-to-point QKD, with key rates high above the theoretical rate-loss limit. This work has therefore been characterised as the first experimental realisation of an *effective* quantum repeater in ref. [60].

In the second section, the setup is developed further to handle a realistic situation where up to 605 km of real fibre comprise the quantum channels. This implementation not only broke the record for the longest successful demonstration of TF-QKD in fibre but also it was the first to show a multi-protocol setup and an active phase stabilisation successful with long fibres. Able to perform any TF-QKD variant, this setup exploits the protocol's full potential. This is demonstrated through the implementation of both the SNS-TF-QKD and the CAL-TF-QKD protocols, representing two major categories of TF-type protocols. The multi-protocol potential is attributed to the novel dual-band phase stabilisation technique developed, described in detail in section 4.5. A further novelty demonstrated in this experiment is the extraction of real key bit-strings from a TF-QKD protocol, for the first time. This allows the true implementation of the TWCC post-processing technique to enhance the SNS-TF-QKD protocol, rather than simply estimating its effect. In this case, the analysis is extended to the finite-size scenario to obtain realistic values rather than overestimated, ideal key rates.

The aim of this chapter is to provide a thorough explanation of the protocol implementations and their results while specific experimental techniques are focused on and described in detail in chapter 4.

3.1 Proof of principle demonstration

In the realisation of TF-QKD as described in the following work, a generalised protocol is considered that can be modified to encompass various TF-QKD protocols based on coherent states. These are the protocols described in chapter 2. In general, to validate the three protocols (TF-QKD, CAL-TF-QKD and SNS-TF-QKD) and overcome the SKC_0 bound, Alice and Bob should use two optically independent 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 reference as to allow the users reconcile their phase values. We represent Alice's states as $|\sqrt{\mu_\alpha}e^{i\phi_\alpha}\rangle$, where μ_α is the intensity and $\phi_\alpha \in [0, 2\pi)$ is the phase. Bob prepares similar states with the subscript α replaced by b. The phases $\phi_{\alpha,b}$ include both the bit information and the random values needed in coherent-state TF-QKD. The optical pulses emitted by the users should interfere with high visibility in the intermediate station after having travelled through a pair of highly lossy channels. High loss is needed to overcome the SKC_0. The optical phase should remain stable in time, which is challenging when the channel loss reduces the amount of detected counts.

3.1.1 Setup

The features described in the introduction above, were implemented using the experimental setup shown in figure 3.1. Each user is endowed with a continuous-wave (CW) laser source (LS). Alice's LS acts as the phase reference. Its light is split in two at a first beam splitter (BS). One part is sent to Bob through a service fibre, depicted in orange, and it is used to lock Bob's LS via a heterodyne optical phase-locked loop (OPLL). Please refer to section 4.1.2 for an introduction to OPLLs and to section 4.3 for further details about the

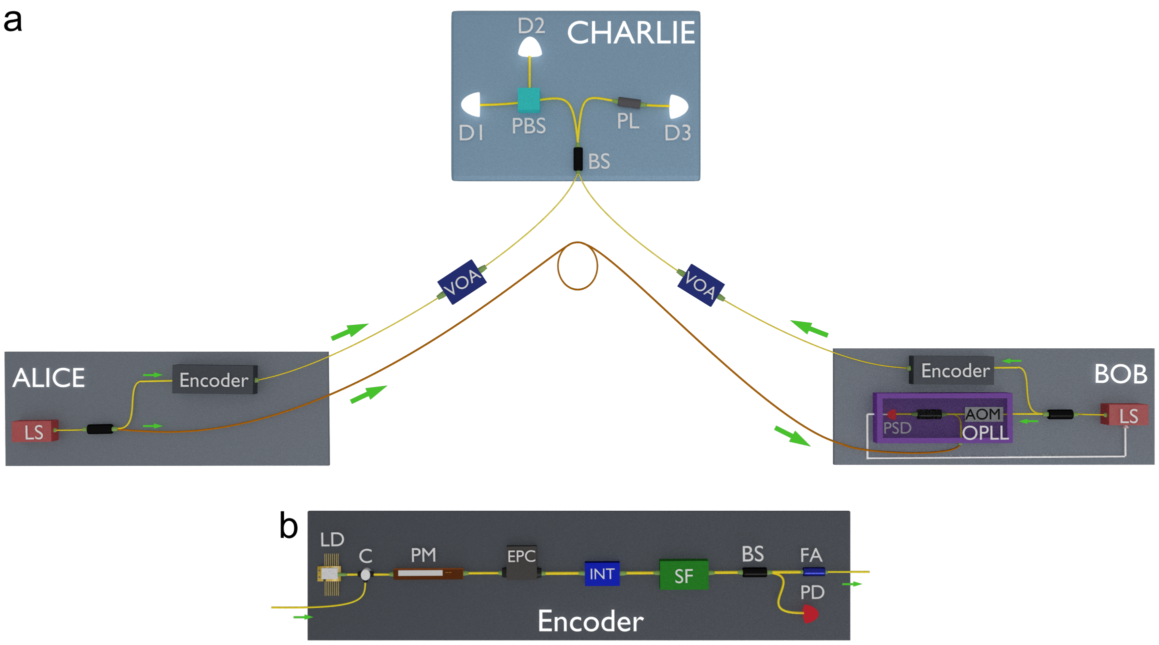

Figure 3.1 **Proof-of-principle experiment setup. a:** Alice and Bob generate light fields from their local laser sources (LSs) and send them to beam splitters. One output goes to the Encoders while the other is used to lock the LSs through a service fibre, depicted in orange, in an optical phase-locked loop (OPLL), comprised of an acousto-optic modulator (AOM) and a phase-sensitive diode (PSD). **b:** In the Encoder, the CW light seeds a gain-switched laser diode (LD) that carves it into pulses. These are either rapidly modulated or finely controlled in phase by the phase modulators (PMs). After crossing the electrically driven polarisation controller (EPC) and the intensity controller (INT), part of the pulses is directed to the power detector (PD) for intensity monitoring and the other part travels through the quantum channel towards Charlie's beam splitter (BS). Here, the pulses interfere and the outcome is registered by the SNSPDs D1, D2 and D3. Variable optical attenuators (VOAs) add losses to the quantum channel. C, circulator; SF, spectral filter; FA, fixed attenuator; PL, polariser; PBS, polarising beam splitter.

OPLL developed and utilised here. Through the OPLL, Bob's laser is locked to Alice's with a phase error less than 5 deg, which includes the potential phase fluctuation in the service fibre. An attacker could modify the reference light while it travels to Bob, but that would not affect the security of the scheme. Any modification would translate into a different value for the phase difference between the two users, which is equivalent to Eve introducing phase noise on the main quantum channels connecting the two users to Charlie. Ref. [120] includes a similar argument applied to standard QKD. Nevertheless, this is not a claim about the robustness of Alice's and Bob's modules to side-channel attacks, which requires more scrutiny, similarly to the ongoing for the MDI-QKD modules.

The fraction of each user's light not involved in the phase-locking mechanism is directed to the Encoder, depicted in figure 3.1b. Here, it enters the cavity of a slave laser diode (LD) which is gain-switched to produce a pulse train at 2 GHz. This ensures that each pulse inherits the phase of the injected light which is locked to the reference. This technique is known as optical injection locking (OIL). Alice's and Bob's LDs emit pulses as narrow as 70 ps at 1548.92 nm, with high extinction ratio and constant intensity, due to the strength of optical injection being 1400 times weaker than the electrical injection. This value is obtained by dividing the number of electron-hole pairs generated by electrical injection over the number of carriers generated by optical injection, using the respective values of bias current and optical power. It is assumed that both injection sources have similar carrier injection efficiency. Further experimental methods and details about the OIL technique can be found in section 4.2.

After the LD, the optical pulses pass through an in-line phase modulator (PM), which applies fast modulation from an RF sinal to encode the phase values required by the specific TF-QKD protocol, and a slow correction from a DC signal to compensate the phase noise on the paths linking to Charlie. After setting the optical pulses' polarisation and intensity, the pulses pass through 15 GHz filters that clean their spectral mode, thus ensuring high visibility interference between twin-fields. A BS in each encoder sends part of the pulses to a power detector (PD) for monitoring the intensity while the other part is sent to the quantum channel. Variable optical attenuators (VOAs) in the quantum channels vary the losses.

Alice's and Bob's optical fields interfere in Charlie's BS and are eventually detected by superconducting nanowire single-photon detectors (SNSPDs, Single Quantum EOS 410 CS) cooled at 3.2 K, featuring 22 Hz dark count rate and 44% detection efficiency at the time when the experiment was performed. Detector D1 is associated with a 100 ps resolution time-tagger and is used to extract the raw key rate. The fact that a single detector is used for QKD reduces the key and gain by 50% which must be taken into account when assessing Charlie's efficiency. D2 monitors the optical field leakage into the non-intended polarisation, which is minimised by Alice and Bob through their polarisation controllers. D3 is sampled by a photon counter at a minimum interval of 10 ms to stabilise the overall phase. The phase stabilisation method used in this experiment is described in section 4.4.

3.1.2 Phase stabilisation and time-multiplexing

The phase stabilisation system as described later in section 4.4 was used during the implementations of the protocols. To do so, the QKD system had to be combined with the stabilisation control using correlated or the same light fields.

Time-multiplexing reference and signal pulses

The feedback requires unmodulated pulses to interfere at Charlie. Their fringes are used as inputs to the feedback to calculate the error signal and correct the drift. However, pulses used for TF-QKD must be encoded in phase, in one or both bases depending on the protocol, in a BB84 format. Consequently, if signal and reference light fields have to travel down the same channel then they must be multiplexed and separable.

The approach employed in this experiment was time-multiplexing. This is the most-straight forward way to reach the target of stabilising the quantum light using the reference, when the drift is slow but the loss is high. There were two ways of time-multiplexing reference and signal pulses. The first will be referred to as the *interleaved* mode, which as the name suggests, requires that every QKD signal pulse is interleaved with a fully unmodulated reference pulse. The second will be referred to as *burst* mode. Here, signal and reference pulses are separated in large time segments. For example, the pattern could be encoded as 200 signal pulses followed by 200 references and repeated. In both modes the duty cycle remains 50% which means that the effective clock rate of the QKD system is halved and will now be 1 GHz.

Phase modulation was tested in both modes, with satisfying results. The resulting performance can be seen in the time-tagged shot of the output of the SNSPDs, in figure 3.2.a. Reference pulses denoted as R interfere with $\frac{\pi}{2}$ phase difference as this is the locking value set by the phase stabilisation mechanism. Once the reference pulses are locked, QKD pulses are also stabilised in phase and the interference from pulses with no phase difference and pulses with phase difference π can be clearly distinguished. The QBER, directly measured from the extinction ratio of the signal pulses, is smaller than 1%, and the modulation mode does not seem to affect this result.

Nevertheless, following further investigation, the interleaved mode was decided to be most suitable for this application. This decision relates to the sustainability of the setup for a future advanced demonstration. The drift measured for the current setup, figure 3.1, never exceeded the order of 10 rad/s. It is tested and shown in section 4.4, that if the flux of the pulses is set to the average value required by the protocols, the stabilisation can work successfully up to 90 dB of channel loss. Beyond that point, an intensity contrast between signals and references must be introduced as to provide sufficient reference light photons to perform the stabilisation. In this case, interleaving the pulses could cause an issue. Generating strong intensity contrast between consecutive pulses at high repetition rates creates an effect known as inter-symbol interference. During time-tagging, the strong pulses contaminate nearby dim pulses with stray photons, decreasing the signal to noise ratio of the QKD encoded pulses. Nevertheless, the limit for the protocols tested here is around 100 dB, hence only a small contrast of 10 dB would be needed which should not be prohibitive. The same does not apply to burst mode. Although this mode localises inter-symbol interference to the boundary regions, contaminating a minimum number of pulses, a new problem arises which negatively impacts the system at all losses. Lithium Niobate intensity modulators, discussed in section 4.4, perform better at high repetition rates, in the GHz regime.

In the burst mode, assuming the previous example of 200-200 signal-reference pulses, the intensity modulator is driven at 5 MHz. The effect of low repetition rates on such modulators is shown in figure 3.2.b, where a 30 dB contrast is created between signal and reference pulses. Noise in the long electrical signals and drift within the time of one pulse created strong perturbations in the intensity levels of the signal and reference sections. Strong reference overshoots are also shown at the boundaries, deteriorating the performance of the stabilisation due to the fluctuation of the reference intensity within one burst mode cycle.

The DC drift between the reference-quantum sections was also monitored over 60 minutes and the findings plotted in figure 3.2.c further discourage the use of this mode. Within one hour, 20 dB of intensity contrast is lost. The rapid DC drift is attributed bad calibration of the intensity modulator. The ideal DC bias of an intensity modulator is found by minimising the light output by the modulator. When the power output is minimum, the intensity contrast of the levels generated by a digitally modulated modulator is maximum. At this point, the modulator is working on the maximum and minimum points of its sinusoidal response and hence small DC drifts will negligibly vary the contrast. Stability is therefore maintained for longer, usually requiring recalibration only once every four hours. When using a burst modulation, the inhomogeneous intensity distribution within pattern cycles does not allow for optimal calibration of the modulators and large intensity changes are observed quickly.

With the burst mode intensity configuration and a BB84 pattern phase modulated on the QKD section of pulses, a low QBER could not be obtained, deeming the method inappropriate for this experiment. Consequently, interleaved mode was decided as the only viable solution.

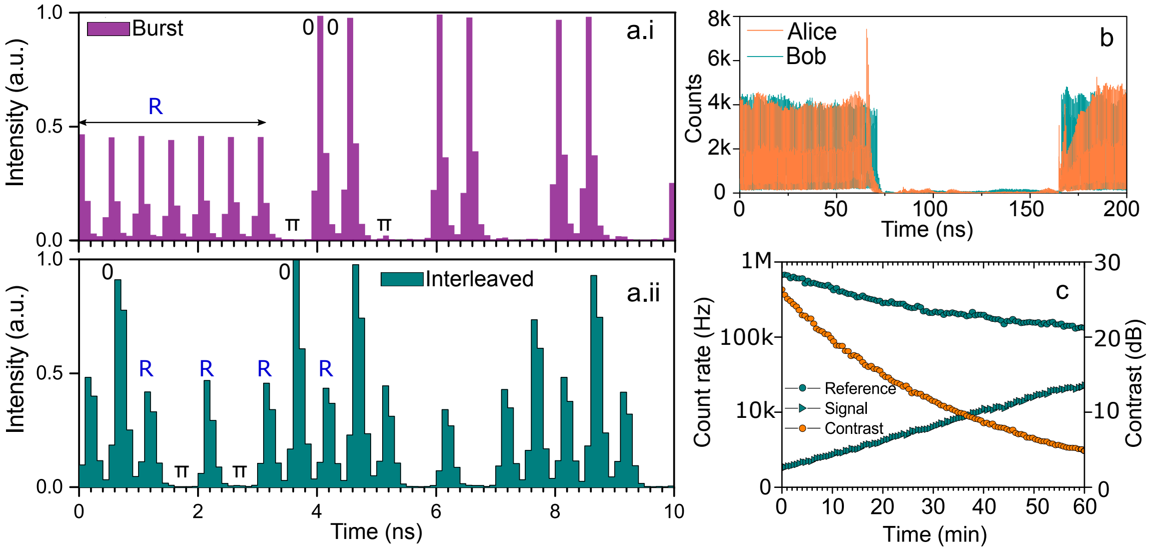

Figure 3.2 **Time-multiplexing: a,** Averaged time tagged results of the interference when the time-multiplexing is performed in burst (**a.i**) and interleaved mode (**a.ii**). TF-QKD information is encoded in a BB84 style where pulses can have a difference of π or 0. QBER is comparable in both modes. **b,** Burst mode intensity modulation result. Strong noise dominates the modulation as the devices are driven to much lower frequencies than they are meant to. **c,** Burst mode intensity modulation is highly susceptible to DC drifts where the contrast generated between signal and reference pulses diminishes by over 20 dB in one hour.

This decision is supported in a later experiment where this mode was used in a system exposed to much higher drift rates, see section 3.2, with the intensity contrast requirement alternatively handled.

Phase stabilisation and QKD

It is interesting to see the performance of the phase stabilisation when it is combined with the interleaved time-multiplexing technique. As a measure of the quality of the stabilisation we take the normalised standard deviation of the count rate incident on a single-photon detector. The count rate is monitored for the duration of the protocols, while the system is stabilised, for multiple attenuation values up to 90 dB The normalisation is achieved by dividing the standard deviation with the average count rate for every sample. To visualise the overall performance, four factors must be indicated in every measurement: the loss of the quantum channel, the normalised standard deviation, the average count rate incident on the detector and the repetition time of the feedback. All these are shown in figure 3.3.a. The mean photon number and normalised standard deviation are plotted on the vertical axes, versus the channel loss on the horizontal axis. The repetition time of the feedback is represented by the colour of each point, according to the heat map on the top of the graph. The minimum value used for this variable was 10 ms while the maximum was 110 ms. It is clear from the plot that as the count rate decreases, and hence the integration time increases, the stabilisation degrades. The normalised standard deviation is over 5 times larger at 90 dB channel loss than it is at 20 dB. Since feedback counts decrease exponentially with the Alice-Bob channel loss, L, as $10^{-\frac{L}{20}}$, the noise in the count rate becomes increasingly noticeable. This introduces an estimation error in the phase drift but nevertheless still allows for an approximate phase correction, even at high loss. This error is on average: $\Delta\theta_e = \frac{2}{\sqrt{C}}$, where C are the feedback counts. Such degradation was expected given that no intensity contrast was created between reference and signal pulses.

Nevertheless, looking at figure 3.3.b, the QBER extracted from the visibility of 0 and π phase difference pulses remains reasonable. At 90 dB this was 2.65%, only 0.36% larger than the QBER at 20 dB. Such values are sufficiently low for the successful implementation of TF-QKD, subject to all other error contributions being kept low. Looking at the QBER expression for TF-QKD in chapter 2 (equation 2.6), two contributions are observed: the total optical base error (which includes the base optical error and the phase misalignment error intrinsic to the protocol) and the dark count error. Hence, the total optical error remains constant while dark counts become more significant as the losses increase. As a result, the total QBER also increases.

The two contributions are simulated and plotted in figure 3.3.b alongside the experimental points measured, for increasing channel loss. The base error is shown by the straight black line, while the dark count contribution is drawn with a dashed line. To match the experimental data to the theoretical model for the QBER, a new contribution had to be introduced. This contribution is the stabilisation error, which was modelled based on the observed experimental results. For this, it was assumed that the phase estimation error of the phase stabilisation feedback causes a persistent phase misalignment proportional to $\Delta\theta_e$, with a coefficient as the only fitting parameter used in the entire model. The updated QBER model, given by the sum of the three aforementioned errors fits the data well as can be seen by the thick line in figure 3.3.b, proving the model's success.

3.1.3 Phase randomisation

During the implementation of the different TF-QKD protocols, phase randomisation was actively performed using the PM in each user's encoder. A pseudo-random pattern containing

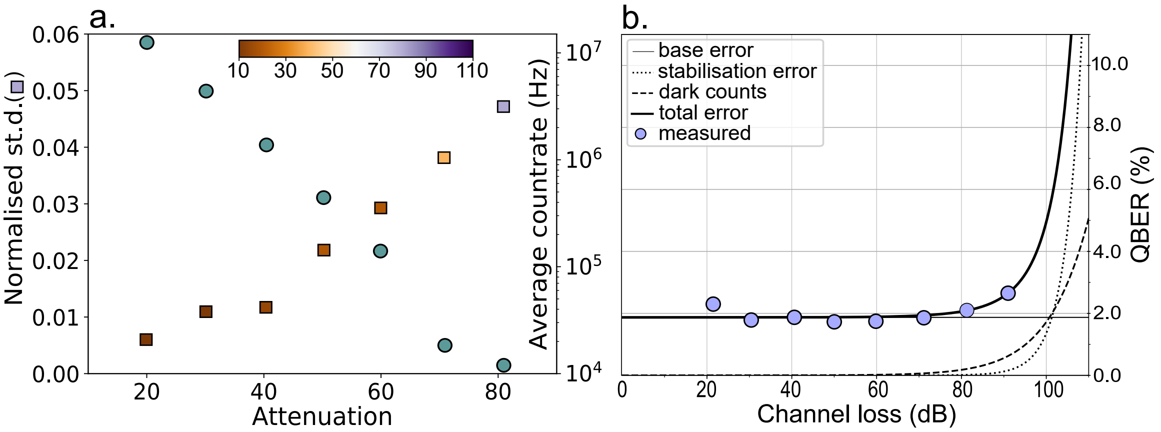

Figure 3.3 **QBER and phase correction:** During the TF-QKD experiment, the phase feedback is on and the intensity of the signal light as well as the QBER are monitored. **a.** On the left y-axis the normalised standard deviation (squares) of the count rate of the stabilised signal is plotted versus the varying attenuation of the experiment. The right y-axis shows the average value of the count rate (circles) as a function of attenuation. The heat map of the squares represents the repetition rate of the phase correction, which increases with increasing attenuation as to gather enough photons for successful control. **b.** The QBER measure for every attenuation is plotted along three simulation curves which represent the various contributions required to model it.

2^{10} symbols having 2^5 modulation levels was encoded through the PMs driven by high-speed 12 GSa/s digital-to-analogue converters (DACs) with 8-bit amplitude resolution.The number of phases chosen is sufficiently close to a phase randomisation with infinite random phases. Using this technique the free-drifting visibility obtained was 96.4%.

To additionally demonstrate a full phase randomisation, a parallel experiment was performed using a continuous phase randomisation from a gain-switched master laser. To achieve this the setup was required to be altered. The OPLL was fully removed and the phase locking was fully performed through OIL instead. Each user was endowed with a laser diode, switched periodically to produce an optical pulse train at a clock rate of 2 GHz. Due to the consequent full depletion of the diodes' cavities, injecting them with light from a master guarantees that the pulses will inherit its phase. This was exploited by injecting the diodes with a third laser diode, the master, also gain-switched at 2 GHz. Alice and Bob emitted 70 ps pulses at 1548.9 nm with the same phase, randomly and uniformly selected in every clock cycle. Active phase randomisation was therefore no longer needed and the phase modulator was solely used to encode the four BB84 values, useful for all three protocols. The rest of the setup remains the same. Using the altered setup, a continuous passive phase randomisation was achieved. Since this was still a proof-of-principle demonstration, matching the global randomisation values in each clock cycle was a valid approach. In a real-world implementation the resulting phase from the OIL would need to be measured with local interference and announced at the end of the protocol.

From this setup a free drifting visibility of 97.5% was obtained, 1.1% higher than in the main experiment. This difference is attributed to the absence of errors from the OPLL and the active phase randomisation. This result shows that the overall visibility is not affected by the absolute number of encoded phases. It is in fact higher with more phases than fewer. Instead, the visibility is much more affected by the components used to implement the phase randomisation. Nevertheless, the base optical error of the system remains in all cases smaller than 1.8% and there is no in-principle limitation to increasing the number of encoded phases. Further experimental methods of continuous phase randomisation can be found in the OIL section 4.2.

3.1.4 Results

A main advantage of TF-QKD is the scaling property of the secret key rate with the square root of the channel transmission, $\eta^{\frac{1}{2}}$. This would be impossible without correspondingly having this same scaling in the detection rate. This essential feature was verified directly and the result is summarised in figure 3.4. 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. The data for double path transmission, on the other hand, was taken with both arms open. It is apparent from figure 3.4 that the single-path gain (triangular markers on dotted line) scales linearly with the loss, $1-\eta$, whereas the double-path gain (square markers on dashed line) scales with the square root. At any given gain, the double-path TF-QKD can tolerate twice the loss the single-path QKD can. In the same figure, the experimental QBERs of TF-QKD are also reported. These are composed of three main contributions: quantum state preparation, detector dark counts and phase feedback. The last two terms significantly affect the overall QBER of the setup only at losses higher than 70 dB.

In figure 3.5 the secure key rates versus the channel loss are plotted for the protocols analysed. The simulations used refer to the ones developed in chapter 2 for the three protocols. Hence all analyses are in the asymptotic case. These results are independent of the specific security analysis adopted to extract a key rate and can hence be used as a reference to test the performance of any TF-QKD-like protocol. Additionally, two more lines are shown for the SKC_0. The *realistic* (*ideal*) SKC_0 accounts for the point-to-point QKD

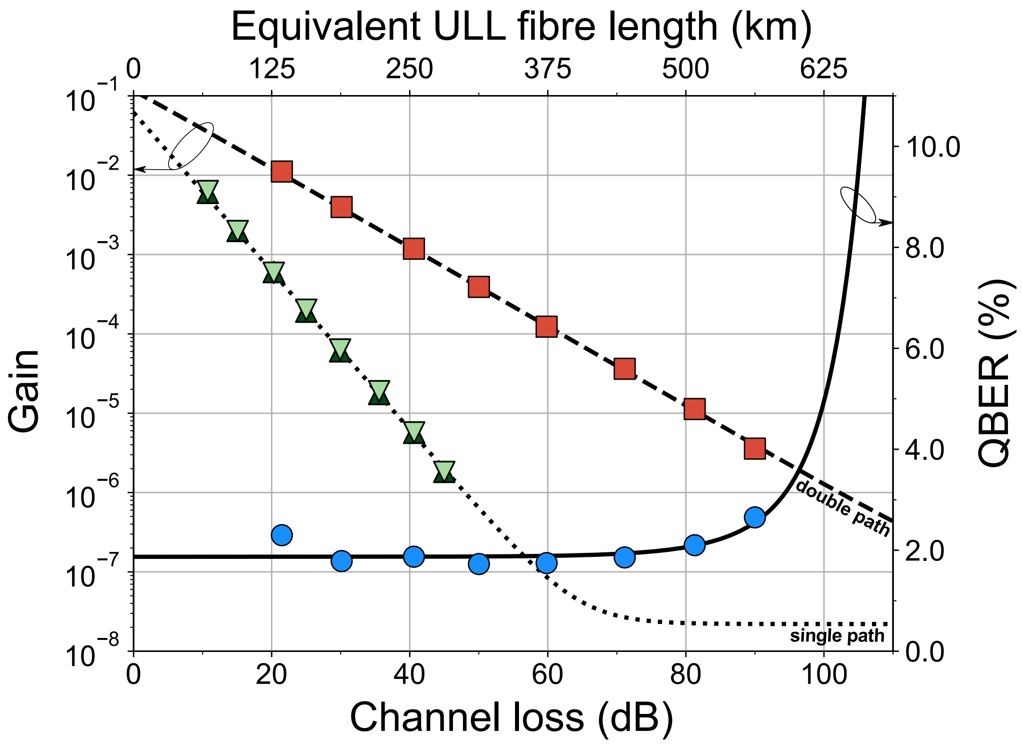

Figure 3.4 **Gain and QBER:** Gain and QBER are plotted against the channel loss. The equivalent fibre length on the top axis pertains to an ultra-low-loss fibre of coefficient 0.16 dB/km. The scaling laws for a QKD-like single-path system and the TF-QKD double-path system are apparent. The triangular (square) points are the single-path (double-path) experimental detection rates recorded. Circle points are the double-path experimental QBERs.

between Alice and Bob with a total detection efficiency of Bob's module equal to $\eta_B = 25\%$ ($\eta_B = 100\%$). The former is a reasonable bound, as it considers that the receiving modules in the developed TF-QKD setup and in the corresponding QKD setup have exactly the same detection efficiency. The latter, on the contrary, is an upper bound to what is theoretically achievable, as it compares the realistic Charlie's module with a Bob's module that features unitary detection efficiency. The expression for this was given previously in equation 1.7. All the data presented in this figure is available in section A.1.

The lighter (darker) pink shaded area indicates the region where the secret key rate of the TF-QKD protocol in [1] (the on in [3]) surpasses the realistic SKC_0. This region extends from about 50 dB to 83 dB, limited only by the detectors' dark counts. In this range, the developed TF-QKD setup provides higher secret key rate than a QKD setup with the same components. This is remarkable in light of the fact that TF-QKD provides higher security assurance than QKD, as it protects against attacks directed at the detection devices. Even

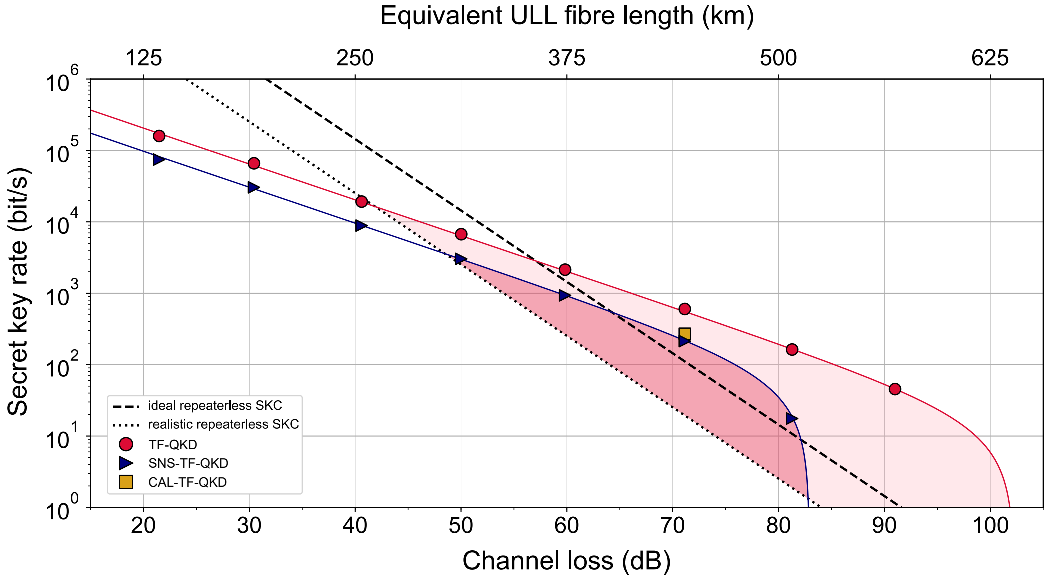

Figure 3.5 **Proof of principle TF-QKD key rates:** Secret key rates are plotted against the channel loss in the lower horizontal axis, and the corresponding ULL fibre distance in the upper horizontal axis. Markers show the experimental data acquired while solid lines the results of the simulations. The ideal and realistic SKC cases are plotted with the dashed and dotted lines respectively. Red markes show the results for the TF-QKD protocol, blue markers the one from the SNS-TF-QKD protocol and the orange marker shows the result obtained from the CAL-TF-QKD protocol. The TF-QKD supremacy region is shaded in pink. Parameters used in the simulations are summarised in table 3.1

more interestingly, there are experimental points that fall beyond the ideal repeaterless SKC. At 71.1 dB, for instance, the secure key rates of the protocols in refs. [3, 2] are 213.0 bps and 270.7 bps respectively. That is 1.90 times and 2.42 times larger than the corresponding ideal repeaterless SKC (112.0 bps). It is worth mentioning that all the reported secret key rates are conservative since they include the penalty due to an imperfect error correction ($f_{EC} = 1.15$).

The maximum channel loss over which phase could be successfully stabilised in this experiment and hence a secret key rate could be obtained is 90.8 dB (rightmost red circle in figure 3.5). This is equivalent to 454 km and 567 km of standard and ULL fibre (0.16 dB/km) single-mode optical fibre respectively, connecting the users. It is interesting to compare these results with the record distances at the time of their publication. The QKD record distance was 421.1 km in ULL fibre, with a key rate of 0.25 bps over a total loss of 71.9 dB [26]. For a similar channel loss, with a clock rate 60% slower and with two orders of magnitude higher dark count rate, this system with any of the protocols implemented is able to obtain key rates three orders of magnitude higher. The longest MDI-QKD demonstration was 404 km in ULL fibre [97]. With a clock rate of 75 MHz, over a channel loss of 64.64 dB this provided a

η_{det}	0.45
$\eta_{Charlie}$	0.5×0.7
P_{dc}	22×10^{-9}
e_{mis}	0.02
M	16
w	10^{-6}

Table 3.1 **Parameters in proof-of-principle experiment:** η_{det}, detector efficiency; $\eta_{Charlie}$, Charlie's module efficiency; P_{dc}, probability of dark counts; e_{mis}, misalignment error; M, number of phase slices; w, vacuum flux. The 0.5 term in $\eta_{Charlie}$ accounts for the beam splitter, since only one detector was used.

key rate of 3.2×10^{-4} bps, six order of magnitude smaller than the key rates obtained here at 71.1 dB. Although the results of this work have been achieved in the asymptotic regime and do not include finite-size effects or long-haul fibres as the referenced experiments, the improvement they enable is substantial.

3.2 TF-QKD over 600 km of fibre

The successful proof-of-principle experiment described in the previous section paved the way for a full implementation, where the channel attenuators were replaced with real long fibres reaching up to 605 km.

Just as in the previous experiment, the new setup was also based on an active stabilisation system, however this time utilising two wavelengths and hence referred to as dual-band stabilisation. The benefit of active stabilisation is that all successful detections at Charlie can be used for secret key distillation or error estimation as the mechanism guarantees that the incoming pulses will always interfere at Charlie with an acceptable phase error. Moreover, the dual-band nature of the developed feedback allows the use of reference light that is many orders of magnitude brighter than signal light. Since the two bands occupy different wavelength channels, contamination of signal light from bright reference light is avoided.

In this section a description of the long distance experiment will be provided, with emphasis to the protocol methods rather than the specific techniques. CAL-TF-QKD, SNS-TF-QKD and SNS-TF-QKD with TWCC were implemented to achieve optimal results at short distances (CAL-TF-QKD) as well as a new record distance for quantum communications with an impressively high key rate (SNS-TF-QKD with TWCC). Finite-size analysis is included up to a fibre channel distance of 555 km and real bit-string keys are distilled.

3.2.1 Setup

The setup developed to enable the implementation of TF-type protocols over long fibres was based on a novel dual-band stabilisation which will be described in detail 4.5. In this section emphasis will be given to the QKD components and the system overall, without in depth explanations of the phase stabilisation scheme.

An important target for this experiment was to develop a setup in which Alice, Bob and Charlie are fully independent. This is a crucial requirement when performing a realistic experiment. Although the long fibre channels connecting Alice, Bob and Charlie are spooled so that all three users are placed on the same optics table, we aim for a setup that could be directly transferred to the field where the users would occupy distant locations. This requires that all optics and electronics are independent but synced and that no computers or controller boards are shared.

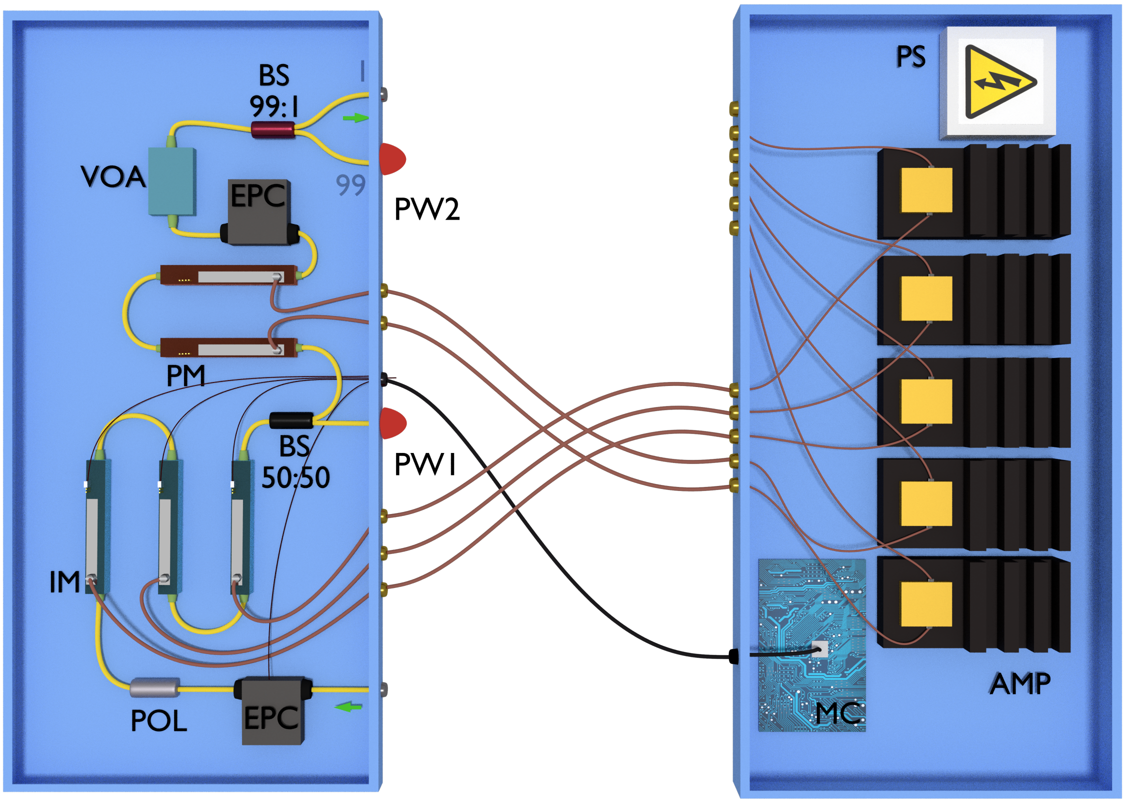

Figure 3.6 **Encoder boxes:** Detailed representation of the optical components inside the users' encoding boxes, as well as the supplementary box containing all the electronics. EPC: Electrical polarisation controller, POL: Polariser, IM: Intensity modulator, BS 50:50: Beam splitter, PW: Power meter, PM: Phase modulator, VOA: Variable optical attenuator, BS 99:1: Beam splitter. MC: Microcontroller board, AMP: Electrical amplifier, PS: Power supply.

As with the previous experiment, all components required for the encoding of the protocol and its calibration are enclosed in a box at each user's station. The boxes are referred to as encoders and are identical in both stations. The contents of the encoders are depicted in figure 3.6. Each encoder box is divided in two subsections. One smaller box for all the optics and opto-electronics and a second box isolating all the purely electrical components. This is done so that any heat dissipated from electrical components is not allowed to compromise the stability of the encoder's optics.

In the optics encoder box, CW light enters the box to be aligned in polarisation with the axis of the subsequent modulators. This was achieved by combining an EPC and a polariser. Next, the light encounters three IMs. The first is used to carve 1 GHz pulses of 250 ps width at intensity u. The two subsequent IMs will create an extra intensity level, v, and enhance the vacuum intensity, w. Contrast between intensity levels is reconfigurable as it is controlled by the applied AC bias. For calibration, a 50:50 BS right after the IMs has one output connected to a power meter channel. Adjusting the DC bias and observing the intensity registered by the power meter allows optimal calibration of the IMs. Specifically, as mentioned in the previous section, the contrast between two intensities created by an IM is maximum when its power output is minimum.

The second output of the BS leads the light to a series of two PMs. Two separate PMs are used so that the amplitude of the RF signal driving them is reduced compared to using a single PM. This achieves linearity between the driving signal and the resulting phase modulation. At each station, a 12 Gsample/s waveform generator drives the PMs through 8-bit DACs, to achieve a total of 512 different phase values. The duty cycle of the phase modulation is kept at 50%, so that half of the quantum pulses are unmodulated to be used as phase references in the stabilisation scheme. Therefore, even-numbered pulses are "quantum signals", modulated in intensity and phase according to the requirements of the different TF-QKD protocols to be implemented. Odd-numbered pulses do not receive any further modulation after being carved and are used to track the phase drift of the quantum signals. They are referred to as "quantum reference". The time-multiplexing of quantum signals and references is identical to the one described in section 3.1.2.

A second EPC after the PMs is used for polarisation control of the QKD light as it drifts in the long fibre channels that follow the user stations. This control system is explained in section 4.5.3 and is performed with the help of a classical announcement from Charlie's station. It aims to continuously align the quantum signals to the preferred optical axis at Charlie.

Following the EPC, a VOA, a 99:1 BS and a second power meter channel form a flux calibration control. The major output of the BS is monitored by the power meter. Given the ratio of the BS, and the power measured locally, the flux of the quantum signal sent to the quantum channel can be calculated. This is also a continuously applied adjustment that keeps the average output flux stable and to the level required by the protocol being carried out.

A simplified version of the total setup is shown in figure 3.7. Simplifications include the reduction of all polarisation control components and dedicated SNSPD, as these will be described in section 4.5.3. Fibre channels are also reduced to a simple configuration. The figure aims to explain how all the developed techniques are put together for a successful TF-QKD experiment.

Alice acts as the master in both the OPLL and the dual-band phase correction. Alice's first CW laser source (LQ), emitting light at $\lambda_Q = 1548.51$ *nm* with a 50 kHz linewidth,

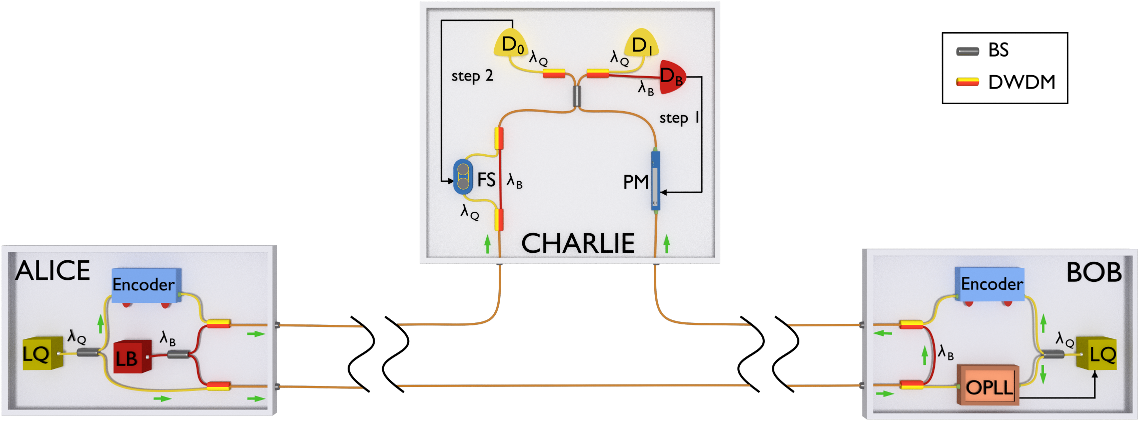

Figure 3.7 **Long distance experiment setup:** Alice and Bob generate λ_Q light (yellow fibres) using local CW lasers LQ. A set of intensity and phase modulators inside each user's Encoder allow them to run different TF-QKD protocols. A second laser (LB) generates the bright reference signal λ_B (red fibres) used for fast phase stabilisation. A service fibre (lower one in the figure) distributes the λ_Q and λ_B wavelengths. After locking the LQ lasers through an OPLL, the users multiplex the wavelengths in the quantum channel (upper fibres in the figure) and send them to Charlie. At Charlie, a beam splitter (BS) combines Alice's and Bob's signals, while the dual band phase stabilisation realised by a phase modulator (PM) and a fibre stretcher (FS) removes the phase noise introduced by the quantum channel. SNSPDs D0 and D1 record the interference output for λ_Q, while DB records the one for λ_B.

is used to carry the quantum signal as well as the OPLL reference. Her second CW laser (LB), emits light at $\lambda_B = 1550.12\ nm$ with a linewidth of 150 kHz, and will be used as the bright phase correction reference light. λ_B light in the reference channel will be many orders of magnitude stronger in intensity than λ_Q, to allow fast phase tracking and correction. Nevertheless, the bright light flux is set so that attenuation of the fibres will also bring it to single photon level so keep the SPDs from saturating.

Both of these sources are followed by BSs that direct one of their outputs to a dense wavelength division multiplexer (DWDM). The two wavelengths are combined before exiting Alice's station to travel to Bob. The complementary output of the BS following the LQ source, sends the light to pass through the QKD encoder box. When this light is prepared for the protocol, it exits the encoder to be wavelength multiplexed with the second output of the BS following the LB source. This DWDM injects the light in the quantum channel to travel to the receiver, Charlie.

Bob holds only one laser (LQ), also emitting light at the signal wavelength λ_Q, whose output is divided by another BS. Light entering Bob's station from Alice is immediately de-multiplexed through a DWDM so that λ_Q and λ_B can follow different paths. Just like the

Fibre length (km)	Alice's loss (dB)	Bob's loss (dB)
76.641	13.25	13.30
184.351	31.39	32.20
260.866	44.70	45.39
277.461	47.73	48.46
302.585	52.38	53.13

Table 3.2 **Fibre channel distances and losses:** The first column states the length of fibre for one channel from Alice (Bob) to Charlie as the two channels were equalised in length. Losses were not exactly equalised and are given in the two rightmost columns for the two segments independently.

experiment in section 3.1, he uses an AOM to shift half his λ_Q light and interfere it with the received λ_Q light, to observe the beating node and activate the OPLL feedback. The rest of the light is sent to his own encoder to undergo the necessary QKD modulations and calibrations. As a result, Bob's quantum signal remains locked in phase with Alice's. The de-multiplexed λ_B arrives at Bob solely to be multiplexed with the λ_Q light output by the encoder. The multiplexed fields are then sent to travel down the quantum channel to arrive at Charlie.

Contrary to the proof-of-principle experiment, the quantum channels here are comprised of many ULL fibre spools combined together. For the longest distance tested, around 50 km of standard loss fibre was also used. The loss coefficient for the ULL spools averaged at $\alpha = 0.17$ dB/km which includes splices and connectors. In total, 22 ULL spools and 2 standard fibres spools were used plus some extra fibre to equalise the lengths of the two channels. This is a crucial step as significant differences in the lengths of the two fibre channels would have detrimental effects on the stability of the system. As will be discussed in chapter 4, the interfering fields need to have their frequencies locked. The equation governing this locking has a contributing term dedicated to differences in the optical path. With two channels of different lengths, we can never get rid of that contribution. The precision with which the fibre lengths need to match is debatable.

Although the length difference was matched to be less than 10 cm in all cases, the losses could not be matched exactly. The combined losses at all distances are reported in table 3.2. The lossier spools were assigned to Bob. This was an attempt to ameliorate the loss balance as Charlie's station had higher losses on Alice's side. In case of asymmetries in the photon fluxes received by Charlie from either input, compensation was applied through changing the attenuation in Bob's transmitter. Insertion losses for Charlie's station are given in table 3.3. It is important to note that for simulations, the lowest transmission figure was used to characterise the losses at the receiver.

Arriving at the receiver, the two light fields are each subjected to a different stage of the dual-band phase correction system. Bob's light faces the first step, which utilises a PM to reduce the phase drift rate by at least three orders of magnitude. On the other side, Alice's light will face the second step of the correction. This step has a slightly more complex setup with two DWDM's de-multiplexing and the re-multiplexing the incoming light. In the described structure, the arm through which light λ_Q will travel through contains a fibre stretcher (FS). This is a device that can extend and reduce the length of the fibre passing through it as to shift the travelling light's phase. It hence has the same effect as a PM but with much lower losses. This is also the reason why Bob's insertion loss at Charlie is smaller. Step 2 of the phase correction aims to fully stabilise the quantum signal.

Once the relative phase drift between Alice's and Bob's light fields has been fully suppressed, these will interfere at Charlie's BS. DWDM's follow both outputs of the BS to isolate the λ_Q light so that it is incident on two SNSPDs (Single Quantum EOS 410 CS cooled at 2.9 K), D_0 and D_1. Both of these detectors are connected to time-taggers to enable QKD on the quantum signals, while one of them is also connected to a counter, as in the proof-of-principle experiment. The counter is used for the implementation of step 2 of the phase correction scheme. Quantum references in λ_Q are utilised in this step. One BS output sends to a third detector, D_B, the isolated λ_B light. This detector is solely used for the successful implementation of step 1 of the phase correction.

Details about the dark counts of detectors D_0, D_1 used for QKD are given in table 3.3. Two different values are stated as opposed to the previous experiment. The first value refers to the standard dark count rate measured on the detectors with no fibre attached to them. The second value refers to the dark count rate observed on the two detectors when the fibre is attached but only λ_B light travels through the fibres. Hence, this is a realistic value occurring due to light contamination in the λ_Q wavelength mainly from λ_B scattering.

3.2.2 Protocol encoding

As aforementioned, two different TF-QKD protocols were implemented: the CAL-TF-QKD and the SNS-TF-QKD protocol. The specific protocols were chosen to represent the two main categories of TF-type protocols. The first category, in which the CAL-TF-QKD protocol belongs in, refers to protocols that do not require phase post-selection because the code

Charlie’s system transmission (from Alice)	50.77%
Charlie’s system transmission (from Bob)	62.86%
Efficiency SNSPD D0	77%
Efficiency SNSPD D1	73%
SNSPD dark count rate (calibration)	10 Hz
SNSPD dark count rate (experiment)	14 Hz
Signal clock rate	500 MHz

Table 3.3 **Setup parameters:** Important parameters in the characterisation of the setup. These are crucial for exact system simulation.

basis in encoded such that the phase matching condition is always met. The SNS-TF-QKD protocol belongs in the second category which encompasses all protocols requiring phase post-selection, such as the originally proposed TF-QKD protocol.

Independent of the protocol being carried out, the encoding patterns utilised were 25040 pulses long. Similarly to the previous experiment the QKD duty cycle is kept at 50%, since signal pulses were interleaved by phase unmodulated reference pulses. As described in section 3.2.1, two independent but time-synchronised pattern generators executed the patterns by applying an AC bias to the phase and intensity modulators of the encoder modules. The pattern size remained constant through different protocols and measurements since in all cases the same number of phase values (512) and intensity levels (3) were implemented. Nevertheless, depending on the protocols, the encoding parameters changed. As explained in chapter 2, optimising different protocols yields different results. Moreover, key rate optimisation at various distances may also vary the required encoding parameters. In the measurements that will be presented in section 3.2.3, for the asymptotic and finite-size versions of the SNS-TF-QKD with TWCC, the same pattern was encoded at all distances except for 604.8 km.

Patterns encoded in this experiment were created following *fair sampling*. Tables 3.4 and 3.5 include the preparation probabilities of the bases and states demanded by the CAL-TF-QKD and the SNS-TF-QKD protocols. Using these values the probabilities of different pulse combinations can be calculated. For example, and referring to the SNS, when Alice and Bob both prepare a "send" state we will end up with an "ss" pulse at Charlie. It is important that these states appear with the correct frequency in the pattern. Since the latter is not infinitely long we aim to avoid artefacts in the data from imperfect pulse combination probabilities. Using the extracted combined probabilities, a 12520 pulse pair list is created and then randomly shuffled. As a result the pattern, although random, is forced to respect the matching probabilities to agree with the protocol simulations.

Asymptotic CAL-TF-QKD, 368.7 km	
Fluxes (photons/pulse)	
s	0.015
u	0.1
v	0.015
w	0.0002
Probabilities	
P(Z)	50.0%
P(X)	50.0%
P(u)	33.3%
P(v)	33.3%
P(w)	33.3%
Secret key rate = 852.7 bps	

Table 3.4 **Asymptotic CAL-TF-QKD encoding details:** The parameters used to perform this protocol in the asymptotic regime. s, u, v, w are the photon fluxes encoded on the signal and the three decoy states respectively. P(N) gives the probability of preparing a pulse in the N basis while P(n), the probability of preparing a pulse in the intensity state n. The secret key rate is also given in bps.

All information about fluxes and probabilities is included in table 3.4 for the CAL-TF-QKD protocol. As described in previous chapters this protocol uses the $\mathbb{X}$-basis for key distillation while the $\mathbb{Z}$-basis is solely used for decoy state analysis. $\mathbb{X}$-basis pulses can only take two values to represent the two bits, encoded in phase by 0 and π. The intensity, s, of these signal pulses is set to be equal to the intensity of the v decoy state. This follows the result of optimisation procedures summarised in 2.4.2. Since this is a phase-matching protocol, $\mathbb{X}$-basis pulses are not phase randomised, while $\mathbb{Z}$-basis pulses are all phase randomised. Given that the CAL-TF-QKD protocol was only run in the asymptotic regime, while the probability of preparing an $\mathbb{X}$-basis pulses was experimentally set to 50%, it was then treated as 99.99% in the analysis.

The SNS-TF-QKD protocol parameters are summarised, for the different configurations carried out, in table 3.5. Here the $\mathbb{Z}$-basis is the key distillation basis and it is of the sending, not-sending form. The $\mathbb{X}$-basis is used for decoy state analysis. All pulses in both bases are required to be phase randomised for the security of the protocol to hold. This protocol was performed both in the asymptotic and finite-size regime with different parameters. Again, in the asymptotic case, the key rate estimation was executed by normalising the probability of using the code basis, $\mathbb{Z}$, from 50% to 99.9%.

	SNS - asymptotic	SNS, TWCC - asymptotic		SNS, TWCC - finite size
Fibre length (km)	368.7	all	605	all
Fluxes (photons/pulse)				
s	0.35	0.35	0.38	0.40
u	0.35	0.35	0.38	0.40
v	0.035	0.0105	0.0107	0.075
w	0.0002	0.0002	0.00023	0.0002
Probabilities				
P(Z)	50%	50%		60%
P(s)	5.8%	13%		7.5%
P(X)	50%	50%		40%
P(u)	33.3%	33.3%		20%
P(v)	33.3%	33.3%		60%
P(w)	33.3%	33.3%		20%

Table 3.5 **SNS-TF-QKD encoding details:** The parameters used for carrying this protocol at specific fibre lengths are given. The fluxes s, u, v, w refer to the signal state and the three decoy states respectively. P(N) gives the probability of preparing a pulse in the N basis while P(n), the probability of preparing a pulse in the intensity state n. The secret key rate is also given in bps.

3.2.3 Results

The different protocols are performed by varying the operational regimes and optimised the parameters for each test. In the asymptotic regime, the CAL-TF-QKD and the SNS-TF-QKD protocols are performed. SNS-TF-QKD with TWCC is performed in both the asymptotic and finite-size case scnenarios. The reason for this is because SNS-TF-QKD with TWCC is the protocol that performs the best in terms of distance and hence the acquired key rates should be practically relevant. From the finite-size data, real bits of the raw key are extracted. The latter process is outlined in detail in section 3.2.4. Detailed experimental results are given in the appendix, section A.2.

The acquired results for the secret key rate versus distance are shown in figure 3.8. For the case of the TWCC, in both the asymptotic and finite-size regimes, simulation curves accompany the experimental data. The asymptotic simulation is based on the equations of section 2.6. A thorough description of the finite-size analysis is beyond the scope of this thesis and is therefore not included. Nevertheless, it is based on using the asymptotic case analysis combined with statistical fluctuation expressions to extract a more realistic quantity. For the purposes of quantifying the significance of these results presented here, the plot also includes a line representing the secret key capacity for a system of 100% efficiency

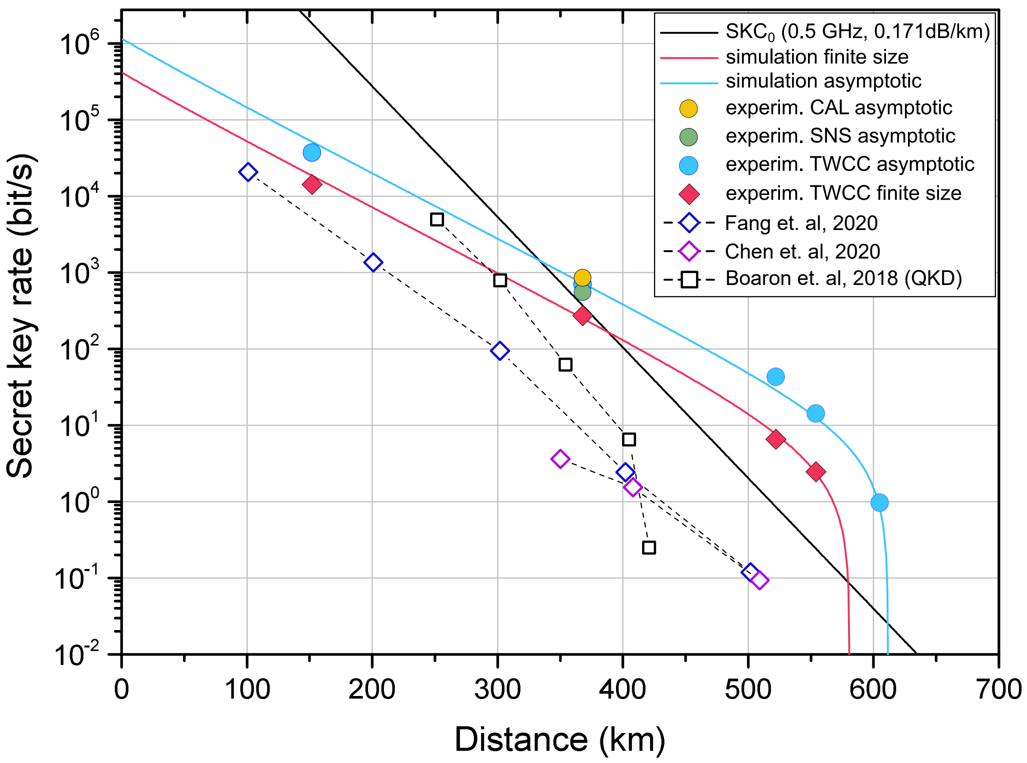

Figure 3.8 **Secret key rates at long distances:** A graph of the secret key rates versus the ULL fibre channel distance for the four different cases tested in this work. The experimental results (filled markers) for the SNS-TF-QKD with TWCC protocol are accompanied by the relevant simulations in the finite-size (red line) and asymptotic (light blue line) regimes. Previous record results from other groups are plotted on the same graph for comparison (empty markers). For the same reason, the secret key capacity (SKC_0) for a 100% efficient system is also plotted (black line).

(SKC_0). This is the strictest bound as it assumes ideal equipment for Alice and Bob. Just as in the previous experiment, surpassing this bound indicates that the setup under examination is showing a repeater-like behaviour. Additionally, state-of-the-art secure key rates from previous long distance implementations of both TF-QKD and QKD are depicted.

The reason for including the CAL-TF-QKD protocol was to show the ability of the system to perform different types of protocols and hence output optimal key rates even at small distances. The SNS-TF-QKD protocol without TWCC was performed for completeness. Hence, these were both only tested at the single distance of 368.7 km (62.8 dB loss) and were solely analysed in the asymptotic regime. Their performance is represented respectively by the yellow and green markers on the plot. A secret key rate of 857.2 bps is obtained for the CAL-TF-QKD protocol. This is a value 2.39 times larger than the SKC_0. For the

SNS-TF-QKD protocol at the same distance, a value of 549.2 bps was acquired, 1.54 times larger than the SKC_0.

For longer distances to be attainable the use of TWCC as a post-processing method to the SNS-TF-QKD protocol was mandatory. For this protocol measurements are taken at 5 distances in the case of the asymptotic analysis and at 4 distances for the finite-size analysis. These distances ranged in loss from 26.5 dB to 104.8 dB and their specific lengths were 153.3, 368.7, 522.0, 555.2 and 605.2 km. The finite-size analysis (red markers) reaches 555.2 km, where with only 2 hours of continuous measurement, a secret key rate of 2.468 bps, 10 times larger than the SKC_0, was obtained. At the longest distance of 605.2 km, where the losses reached 104.8 dB, the secret key rate obtained using an asymptotic analysis was 0.969 bps, 30 times larger than the SKC_0.

With this experiment, for the first time, secure quantum communication has been established beyond 600 km and the 100 dB loss barrier. Comparison between these results and the previous state-of-art-experiments, a distance increase of tens of kilometres and over one hundred kilometres has been shown compared to TF-QKD [93, 94] and QKD [26] respectively. Regarding key rate, the results described here are 2 orders of magnitude higher at the furthest distance previously achieved. Another significant milestone reached was the real distillation of a quantum key for the first time in practical TF-QKD. Previous TF-QKD experiments did not include the extraction of a real key but solely the estimation of the secure key rate from average quantities. More details about the key generation process are found in the following section.

3.2.4 Generating real bits strings

One of the novelties of the 600 km experiment was the generation of real keys. Keys are strings of bits which can only be extracted via manipulating and processing each detector click individually, according to the current protocol. Although such keys have been previously extracted from the implementation of other protocols, all the TF-QKD experiments performed so far, as well as the vast majority of long-distance QKD experiments, have only provided an in-principle estimation of the key rate without a real extraction of the bits that form a cryptographic key after suitable post-processing. In fact, it is uncommon for research papers to include such keys. Quantities such as QBER, gain and key rate are usually extracted through histograms of counts rather than the actual, single count bit-strings. The reason behind this is the complexity and time consumption of the post-processing required to carry

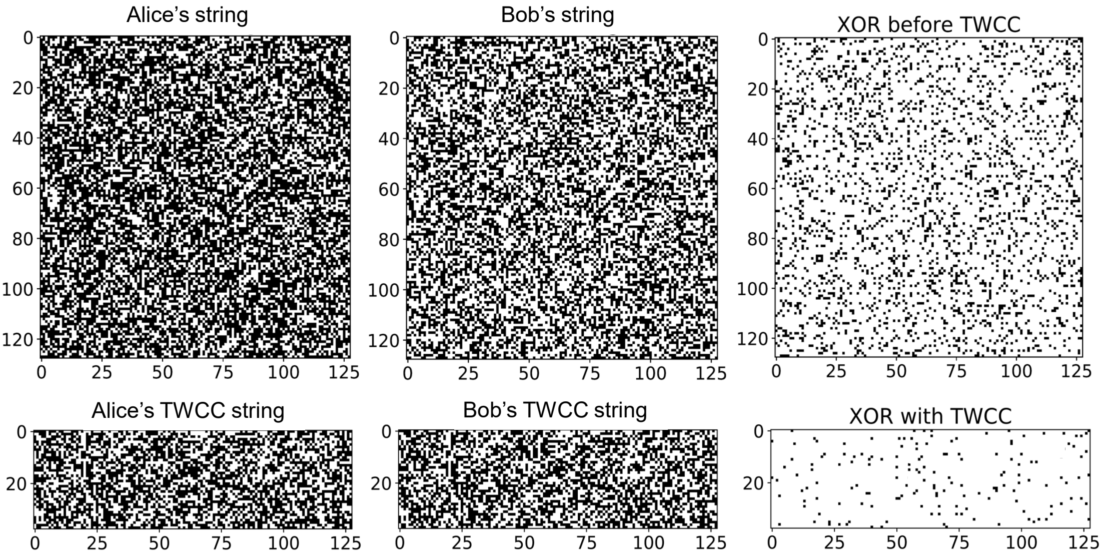

Figure 3.9 **Binary maps of the extracted bit strings:** Samples of the bits extracted from the experiment performed at 522 km before (top panels) and after (bottom panels) TWCC is applied. *Top* - The first two squares on the left (128 x 128 pixels) are a sample of the users' raw strings before TWCC is applied, with white (black) pixels associated with the bit value 0 (1). The third square on the right is obtained by modulo-2 addition (XOR) of the first two. The black dots in this square represent the errors in the strings. *Bottom* - Refined keys after TWCC has been applied. The strings shrink by 70% into rectangles with 128 x 38 pixels. Reduction in key size is accompanied by a substantial reduction in the key errors, as is apparent from the rightmost rectangle.

out the task of forming bit-strings. Especially at a clock rate as high as 1 GHz, real-time manipulation of individual signals recorded at the detectors is a challenging task.

Extracting keys from a protocol is essential to show the practicality of a system. QKD is not solely a research interest but it is a commercial demand, a technology which will soon be part of the standard communication infrastructure. It is hence essential that a quantum communications system is able to extract real keys, independent of the protocol being carried out. Nevertheless, for TF-QKD this is even more vital due to the TWCC post-processing method beneficial to SNS-TF-QKD. The particular protocol promises the longest distances achievable without the use of repeaters and owes this to TWCC. For the true implementation of the latter, bitwise operations are required. Hence, while the theory offers expressions to estimate the benefits of TWCC [118], it is important that systems are able to also carry out the method.

The main difficulty in achieving individual time-tagged event processing is to extract the information from the time-tagging device and generate a program able to read the raw clicks and process them for every round of measurements independently. A time-tagger has three time parameters: bin-width, range and sweeps. The bin-width is the minimum time resolution of the tagger, in our case 100 ps, while the range is the number of bins in one measurement. The range needs to be large enough to register at least one full encoded pattern of pulses sent by Alice and Bob. In the case of this experiment and for the SNS protocol, given that three intensity states were used and 512 different phase values could be encoded, the range used to make sure a fair sample of all combinations was registered was 261000 bins, equal to 13050 QKD pulses and 13050 unmodulated reference pulses. Finally, the number of sweeps is equal to the number of measurements averaged on a single histogram which is then used to extract the necessary average quantities. For optimal performance in the time-tagging device, the sweep number needs to lie within the range of 0.1 M - 1 M. These are all taken as one measurement with the advantage that the dead-time between sweeps (single shot measurements) is much smaller than the dead-time between repetitions of sets of sweeps (set of measurements). This is exactly because sweeps are all averaged together and therefore single count information is lost within the created histograms as the device measures single counts but only reads them congregated at the end of the total sweeps.

Although time-taggers are not created to instantly read-out individual clicks, they are able to output list (.lst) files with all the time-tagged information. These were the files utilised to form the bit-strings in this experiment. Python code was created to perform an algorithm similar to what the time-tagging device is programmed to do with the exception of averaging the counts together. Hence, for every sweep number, the clicking bins could be attained, sifted and post-processed to form the final key bit-strings. A gate window of 500 ps was chosen to extract valid clicks from each pulse, which covered the entire 250 ps pulse width and accounted for any jitter or inter-symbol interference. Clicks belonging to the reference pulses were discarded.

Specifically, to sift Charlie's announcements (detected counts), clicks in the $\mathbb{Z}$-basis from both detectors were isolated and concatenated (clicks in the $\mathbb{X}$-basis need not be processed individually for decoy state error estimation). They were then used by Alice and Bob to separately generate their own initial key string. For every photon click recorded in the $\mathbb{Z}$-basis, Alice (Bob) registers a bit 1 (0) if she (he) had sent a weak-coherent pulse within the time slot and a bit 0 (1) if she (he) had chosen not to send anything. As a result, they obtain matching bits in the cases where only one user has prepared and sent a pulse and opposite bits if both have sent. Bits acquired from the latter case, or from dark counts, contribute to the QBER in the key generation basis. A sample of the initial sifted keys for Alice and Bob are shown in the first two squares in the top row of figure 3.9, in the form of binary maps comprised of 128x128 pixels, for the finite-size measurement taken at 522 km. Zeros and ones are represented by white and black pixels respectively. The white-bias of Alice and black bias of Bob are expected and attributed to the send-send clicks that have the highest occurrence probability and during which Alice will always obtain a 1 while Bob will obtain a 0.

Initial keys were post-processed according to the TWCC method to reduce their initial QBER of 16% and allow successful QKD at such long distances. During this process, Bob's bits are randomly paired up and their parity calculated. The pair positions and resulting parity must be publicly announced so that the procedure can be repeated by Alice who will also announce her results. The initial keys are then further sifted to include only the first bit of pairs whose parity matched in both users. For instance, given the SNS encoding in the key generation basis, pairs encoded as "send, not-send" (sn) by Alice in a randomly selected pair will provide a matching parity if paired with bits encoded as "not-send, send" (ns) by Bob, whereas will provide unmatched parity if paired with bits encoded as "send, send" (ss) by Bob. Although TWCC reduces the length of the secret key, it also significantly reduces the QBER so that the overall signal-to-noise ratio is increased. The effect of the process on the 522 km data is shown in the first two rectangles in the bottom row of figure 3.9. The binary map is reduced in dimension by 70% to represent the equivalent reduction in the entire bit strings due to TWCC. The white/black bias is also visibly reduced. To better depict the QBER reduction, the binary maps are bitwise XORed before and after TWCC in the rightmost boxes of figure 3.9. Matching and opposite bits are represented by white and black pixels respectively. In this case, the QBER is reduced by over a factor 4.5, from 16% to 3.5%, thus allowing us to extract a secret key at distances up to 605 km.

3.3 Summary

In this chapter, experimental implementations of TF-QKD variants and their results were described. The first ever TF-QKD demonstration, described in section 3.1, was performed by limiting the quantum fibre channel lengths to around 100 m, while simulating the loss of longer distances using variable optical attenuators. This restricted the phase drift rate to the order of 1-10 rad/s and hence allowed a proof-of-principle experiment to be carried out by utilising a slow phase correction feedback. Due to the limited drift rate, this feedback utilised reference pulses time-multiplexed with signal pulses, while no intensity contrast between references and signals was required. In this experiment, three different TF-QKD variants were implemented: TF-QKD [1], CAL-TF-QKD [2] and SNS-TF-QKD [3]. In all three cases, the repeaterless secret key capacity was surpassed, obtaining key rates up to a loss of 90.8 dB, for a protocol secure against a set of attacks, and up to 81.2 dB for an information-theoretic secure protocol. These results set the loss record at the time, beating previous implementations of both QKD and MDI-QKD while the key rates obtained at medium to high loss were also the best ever practically achieved in quantum communications.

The second section of this chapter, 3.2, describes the utilisation of an upgraded setup to perform TF-QKD in fibre quantum channels up to 605 km in length. System upgrades include a dual-band phase stabilisation system able to correct the fast phase drift observed in long fibres, live and continuous polarisation control and flux calibration feedbacks, and the full independence of the stations of Alice, Bob and Charlie. Furthermore, all necessary intensity and phase modulations were now performed on-line in long pseudo-random patterns, assimilating a real-life implementation. Once again, multiple TF-QKD protocols are implemented to represent all the variant categories and hence prove the multi-protocol nature of the developed setup. For this, the CAL-TF-QKD [2] and SNS-TF-QKD with [113] and without [3] TWCC protocols were carried out. The absolute SKC_0 was overcome at several distances, proving that the system behaves similarly to a quantum repeater even when long fibres comprise the channels. The secure key rate vs distance results beat any previous QKD, MDI-QKD and TF-QKD records with the asymptotic scenario reaching 605 km and the finite-size scenario 555 km. Both aforementioned distances surpass the previous distance record of 509 km [94]. An impressive maximum loss of around 105 dB was reached. From this experiment, real bit-string keys were extracted for the first time in the implementation of a TF-QKD protocol. This allowed, also for the first time, a true implementation of the TWCC post-processing method rather than a sole estimation. Even if TWCC is not to be utilised in an experiment, developing the software and hardware required for extracting keys is a significant milestone in the road towards realistic and dependable TF-QKD. With these results, TF-QKD is greatly advanced beyond its limits, substantially increasing the practical rate and range of secure quantum communications.

Chapter 4

Experimental methods for TF-QKD

4.1 Introduction

In chapter 3, two implementations of TF-QKD were described: a proof-of-principle examination with short fibres but over high loss and a full implementation over 605 km of fibre. As discussed briefly in chapter 1, for the successful experimental implementation of the TF-QKD protocol, high quality first-order interference of two distinct lasers is required. This is achieved by developing and utilising indistinguishable sources. Any imperfections at the pulse generation and encoding staging or perturbations affecting the pulses during flight-time, deteriorate the interference visibility. For TF-QKD, we define visibility as the contrast between constructive and destructive interference fringes observed at Charlie, and resulting from the combination of Alice's and Bob's pulses at the beam splitter. This is given by equation 4.1, where n_{con}, n_{des} refer to the counts observed on the constructive and destructive detector respectively. The two detectors are assumed to be of equal efficiency:

$$V = \frac{n_{con} - n_{des}}{n_{con} + n_{des}} \tag{4.1}$$

Poor visibility is detrimental to the QBER of the protocol since the two quantities are directly correlated:

$$QBER = \frac{1-V}{2} \tag{4.2}$$

Hence, to minimise the QBER, visibility has to be maximised. To achieve the latter it is necessary to accurately calibrate and control several involved degrees of freedom. To sum up, the ultimate global target when implementing TF-QKD is to develop a setup where the indistinguishability between Alice's and Bob's sources is maximised and retained at interference in Charlie's station.

The degrees of freedom ultimately contributing to the QBER are outlined here:

- **Phase:** Information is encoded in phase and recovered through a first-order interference measurement. It is therefore mandatory that a common phase reference is distributed between the two users and that phase is preserved from transmitter to receiver.
- **Wavelength:** The two sources must have identical frequency spectrum. Any detuning increases source distinguishability and additionally enhances the total relative phase noise acquired by the pulses as they travel down the quantum channels.
- **Polarisation:** Pulses from the two transmitters must interfere at Charlie with identical polarisation states.
- **Intensity:** As one of the most critical properties able to highly degrade visibility, signal intensity must be continuously optimised and accurately corrected.

Firstly, since information is encoded in phase and the measurement is first-order interferometric, it is vital that Alice and Bob share a common phase reference. Secondly, all phase information must be preserved from transmitter to receiver. Wavelength is equally important as any detuning will increase distinguishability and additionally add to the total relative phase drift rate during the fields' travel down the quantum channels. Finally, polarisation and intensity also need be identical.

Control of some of these parameters is significantly challenging, with TF-QKD being the first quantum protocol to pose certain of these stringent requirements. In fact, the main concern after its publication was whether the protocol was practically feasible. In this chapter, the experimental techniques developed to achieve control and optimisation of these degrees of freedom will be described in detail. Due to the novelty of these challenges, several of these techniques are areas of quantum communication engineering that have not been extensively researched or researched at all. Moreover, some of the techniques, while commonly used in classical communications, had however not been previously integrated into quantum systems.

The following section describes the theory and previous state-of-art of the mechanisms developed in this work. It also analyses the experimental research, development, testing and results for every technique. Precise control of all the aforementioned degrees of freedom is achieved and provides the foundation for performing the first TF-QKD experiments as they were described in the previous chapter.

4.1.1 Phase drift in long fibres

The biggest challenge in any TF-QKD experimental demonstration is undoubtedly to achieve control of the phase, so that the information encoded at the transmitters is maintained or recovered at the point of interference. Let's assume Alice and Bob prepare pulses of phase ϕ and $\phi + \pi$ respectively. Interference at Charlie's 50/50 beam splitter should then produce an outcome with photons directed to the destructive detector. However the pulses will travel through long quantum channels, in this specific case fibre channels, before interfering. Alice and Bob can be separated by more than 500 km so each quantum channel will be over 250 km long.

Environmental fluctuations will directly influence the fibre and hence how the light is transformed in each channel. Vibrations and thermal fluctuations are unavoidable even in controlled environments like a lab, nevermind in the field. Tiny changes in temperature are enough to cause changes in the fibre lengths comparable to the wavelength of infrared (IR) light. Accumulating over 250 km, the tiny changes become extremely significant. As a result, they will introduce random phase errors $\Delta\phi_A$, $\Delta\phi_B$ in the two channels and the pulses will interfere with a phase difference $\pi + \Delta\phi_A + \Delta\phi_B = \delta$. The encoded phase information has been fully scrambled and either of the two detectors can observe a click without any correlation to Alice's and Bob's encoded phases. For a system free drifting in phase, the QBER is 50% and no mutual information can be established between the two users.

While the stabilisation of long interferometers with dim light, as is the TF-QKD setup, is needless in classical communications, it is vital for long-distance QKD. This is due to the difficulties associated with implementing repeaters in quantum links, even in the current state-of-the-art [121]. In fact, interferometric phase noise in quantum systems is studied mainly for the development of quantum repeaters. In ref. [122] such a study has shown that phase noise in a fibre-optic MZI has the nature of a random walk and hence shows a Gaussian distribution. It was also quantified that a 25 nm mismatch in the length of the two fibre arms causes 0.1 rad of phase shift, given light at 1550 nm.

In ref. [1], the phase drift rate of a 500 km long interferometer was measured to be as high as 18 rad/ms. For TF-QKD, a phase error of 0.3 rad is the maximum accepted value for a realistic phase discretisation choice of 16 slices. As a result, for successful TF-QKD over the rate-distance limit, it is required to develop a phase-correction system of high accuracy working at repetition rates around 50 kHz. This is a particularly demanding task to perform over a quantum interferometer. The use of dim light means that the photons available for sampling in each repetition cycle of a phase stabilisation feedback will be minimised. As a result, the accuracy of the correction is decrease. The integration time of the system could potentially be increased to provide a bigger photon sample. Nevertheless, since the repetition rate of the feedback must be sufficiently faster than the phase drift rate, it is highly likely that the accuracy of the system cannot be significantly improved in this manner.

Attempts to stabilise interferometers have been previously demonstrated. In ref. [123], the basis for phase stabilisation quantum systems was set using a Michelson interferometer with 6 km fibre arms. The feedback utilised wavelength-division multiplexing so that bright phase reference light would travel alongside the quantum light. The interference of the reference was monitored continuously and was used to activate a fibre-stretcher which corrected the phase. In following demonstrations, the idea of multiplexing wavelengths was conserved and stabilisation was demonstrated in a 1 km MZI [124], and in an 8 km MZI with combined active polarisation-drift compensation for highly stable visibility [112].

State-of-the-art phase stabilisation for quantum networks is described in ref. [125], where the fibre is stabilised by submerging it into a temperature controlled sink of water. In terms of classical communications, an impressive stabilisation system over 146 km has been demonstrated at telecom wavelengths. For this, digital phase-locked loops were implemented, where the compensation observes beats and acts on the RF signal [126]. Nevertheless, none of the previous demonstrations have shown successful phase stabilisation with sufficient visibility for demanding protocols like TF-QKD, for interferometers long enough to exceed QKD record distances and while operating at the single-photon level.

4.1.2 Optically phase-locked loops

As mentioned in section 1.3.3, correcting the phase drift of long channels is only meaningful if the two transmitters begin on a common phase. If they encode phase information on pulses with different initial phases, then the interference at Charlie will be random, even if no phase drift affects the fibre channels. Moreover, two independent laser sources are doomed to observe random drifts in their central frequency, a phenomenon known as wavelength detuning. This detuning, contributes to the total phase drift induced in the interferometric setup. Therefore, for TF-QKD to be implemented, a common phase reference between the two sources must be established and continuously distributed.

Wavelength and path differences (phase drift as described in section 4.1.1) are the two contributors to the phase noise accumulated in the quantum channel, see equation 4.3 [1].

$$\delta = \frac{2\pi}{c}(\Delta\nu L + \nu\Delta L) \tag{4.3}$$

δ is the total accumulated phase, c is the speed of light in fibre, ν is the frequency of the light and L is the fibre length. $\Delta\nu$ and ΔL represent the detuning and optical path variation respectively. Consequently, the aim of an OPLL is to suppress the $\Delta\nu$ contribution, while the aim of a phase stabilisation system is to supress the ΔL term.

To distribute a phase reference between two users, a method known as an optically phase-locked loop (OPLL) can be employed. OPLLs are a commonly used tool in classical communications [127–130]. They are control systems used to keep two or more lasers locked in phase, where slave lasers follow the exact behaviour of the master. OPLLs do not suppress the inherent phase drift in the sources but rather synchronise every source in the loop such that the relative phase drift between them is negligible. Since this technique has not been used in quantum communications before, there is no prior state-of-the-art to be described. The working principle of OPLLs will be explored instead.

The main ingredient to an OPLL is optical homodyne or heterodyne detection, a technique used in many different types of communication systems [131, 132]. These detection methods are essentially a tool for extracting phase or frequency information out of a system, through an intensity measurement of interference. In this work we are interested in heterodyne OPLLs and hence we will focus solely on that. The advantage of heterodyne over homodyne detection for our application is outlined in section 4.3.

Optical heterodyne detection requires that two optical signals of slightly different central frequency interfere and the resulting electronic signal is measured. For example, a laser source of frequency f and a second laser source, also known as the local oscillator, of frequency $f + \delta f$ are the inputs to a fibre-optic coupler. The output is connected to a photodiode. Since the difference between the frequencies of the two sources, δf, is quite small and within the bandwidth of the photodiode, the electrical signal output will be the *beating* of the two sources. Due to the slight frequency mismatch, the beating signal of two independent sources oscillates, as the interference drifts from destructive to constructive. Hence, from the intensity of this signal we can infer the phase information and the photodiode can be seen as a phase-sensitive diode. Electronic processing of the beating node can follow, depending on the purpose of the heterodyne detection. Since it is a technique based on first-order optical interference, the same rules for high visibility apply. The two interfering lasers must be indistinguishable in all degrees of freedom (excluding frequency where the offset generation is required) while they should also be spatially coherent before interference.

For the particular application of developing an OPLL based on heterodyne detection, electronic post-processing of the beating signal of the two lasers to be locked is required. The master laser is equivalent to the signal of frequency f mentioned in the above paragraph. The local oscillator however is not equal to the slave laser. In this case both lasers need to be of frequency f, as the aim is to lock two sources of the same central frequency. To implement heterodyne detection, the slave laser light must be shifted after emission and before interference by an amount δf.

In fibre-optics this can be achieved using an acousto-optic modulator (AOM). An AOM shifts the frequency of light passing through it by using the interaction of light with acoustic waves. Acoustic waves in a crystal cause an oscillation of high and low refractive index regions. Light passing through the crystal will scatter and diffract on the boundaries of refractive index changes. However, as the acoustic waves travel through the crystal, the boundaries move creating a Doppler effect. As a result, the frequency of the diffracted light is shifted. The shift is equal to the frequency of the sound waves [133]. Consequently, if the AOM is set to δf then the slave laser light can be shifted to $f + \delta f$ as required by heterodyne detection. A local oscillator is used to drive the AOM at the required repetition rate.

The frequency-shifted light interferes with the master laser light on a coupler and the beating signal is observed via the photodiode. To achieve phase-locking, the photocurrent of the photodiode is mixed with the electrical signal of the local oscillator, the same signal used to drive the AOM. An electronic control loop uses the output of the mixing to extract the phase difference between the master laser and the slave laser. It then sends a command to the slave laser to shift its frequency by the amount required for the two lasers to behave identically. As a result, the slave laser's frequency will follow the perturbations of the master which acts as the phase reference.

4.1.3 Optical injection locking

Optical injection locking (OIL) is based on the phenomenon where two oscillators can acquire identical frequency when coupled. This was initially observed by Huygens, who noticed pendulums would oscillate uniformly if hung on the same rod and hypothesised this was due to the vibrations travelling inside the rod [134]. OIL in a TF-QKD implementation could be potentnially useful in performing the following tasks:

- Suppress all **spectral detuning** between the two interfering laser sources [135–138], similarly to an OPLL.

- Create high **spectral indistinguishability** and reduce noise to optimise interference visibility [139].

- Passively perform continuous **phase randomisation** [139, 140].

A laser cavity is an oscillator, where photons are generated by the recombination of charge carriers when the driving voltage exceeds the lasing threshold [141]. In OIL, the majority of the charge carriers in the cavity of a first laser, known as the slave, are electrically excited while the electrical bias is kept below lasing threshold. A second laser, known as the master, is biased as per usual above the lasing threshold and injects its generated photons into the cavity of the slave. As a result, stimulated emission in the slave is initiated by the injected seed photons of the master and sharp spectral peaks are generated [137]. This is known as a frequency comb, where the spacing between consecutive peaks is equal to the repetition frequency of the slave laser. Thus, if two lasers are locked via OIL, they gain highly indistinguishable spectral profiles with negligible wavelength detuning. Moreover, since OIL suppresses spontaneous emission that occurs in laser cavities, it is also shown to reduce timing jitter [142, 139, 140]. All of these benefits contribute to higher visibility in the interference of the locked lasers.

With regards to phase manipulation and randomisation, OIL may be used with a gain-switched or continuous-wave (CW) master laser. Gain-switching occurs when short pulses, in the ps regime, are created in semiconductor lasers by applying a short but strong electrical gate. Laser dynamics are described by coupled rate-equations, which correlate the phase of the emitted light when lasing, to the carrier and photon densities in the cavity [143, 144]. As soon as the electrical gate is applied, the carrier density in the active region of the laser increases. Lasing starts once the carrier density passes the threshold and stimulated emission begins. Stimulated emission, however, causes carriers to deplete faster than they are pumped via the electrical gate, thus decreasing the carrier density and photon generation rapidly. Nevertheless, if the gate still applies, the increase-decrease of the carriers undergoes damping in every cycle. When the gate ceases to exist the carriers can only deplete and the laser stops lasing, until the next gate where the process is repeated. The phase is randomised as the laser is driven above and below threshold, subject to the cavity being fully depleted between gates. Due to increased frequency chirp at the beginning of electrical gates, optimal randomness is found towards the end of the gates, once the carrier population exchange process dampens out.

If a gain-switched laser is used as a seed, then the resulting pulses emitted by the slave laser will inherit the random phase of the master. This is a passive phase randomisation technique that is being implemented in protocols to remove side channels occurring from keeping the phase constant [139, 140]. For example, as mentioned in section 1.2.1, the decoy state technique is successful only if each pulse is phase randomised.

The phase inheritance feature of OIL can additionally be used actively to replace phase modulators in QKD experiments. A master laser works at half the frequency of the slave. By controlling the electrical signal of the master and adding an extra, small step modulation during a gate, the phase difference of the two slave laser pulses seeded in that window can be set arbitrarily [142, 145], while maintaining the effect of jitter reduction. Contrary, if the master is CW and the electrical bias is kept constant and above the lasing threshold the phase will not be randomised and master and slave will be locked to a constant phase.

4.2 Optical injection locking for indistinguishable, phase-randomised sources

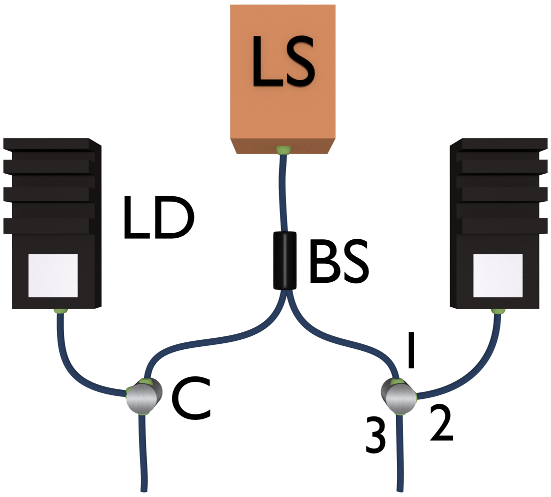

Figure 4.1 **Optical injection locking scheme:** The light from a single laser source (LS) is split in half by a 50:50 beam splitter (BS) and distributed to two separate stations. Both stations are equipped with circulators via which the injection lights enters through port 1 to be directed to the cavity of a pulsed slave laser diode (LD), after exiting port 2. Optical injection locking is enabled and the LDs begin to lase in pulsed mode. This light is directed by the circulator from port 2 to port 3 to exit the station.

As mentioned multiple times in this thesis, for TF-QKD, phase-locking and phase randomisation of highly indistinguishable sources are required. In this section synchronous OIL of two laser diodes is performed, using both a CW and a gain-switched master laser as to satisfy these requirements. Separate lasers are locked in phase, high spectral indistinguishability is achieved and successful phase randomisation is demonstrated, all through the OIL technique.

4.2.1 Two lasers injection-locked by a single master

TF-QKD in its simplest form can be seen as a big interferometer. The most straightforward way to lock Alice and Bob to a common reference is to let them share a single master laser. This will not only lock their phases to a common reference but it will also benefit their spectral indistinguishability.

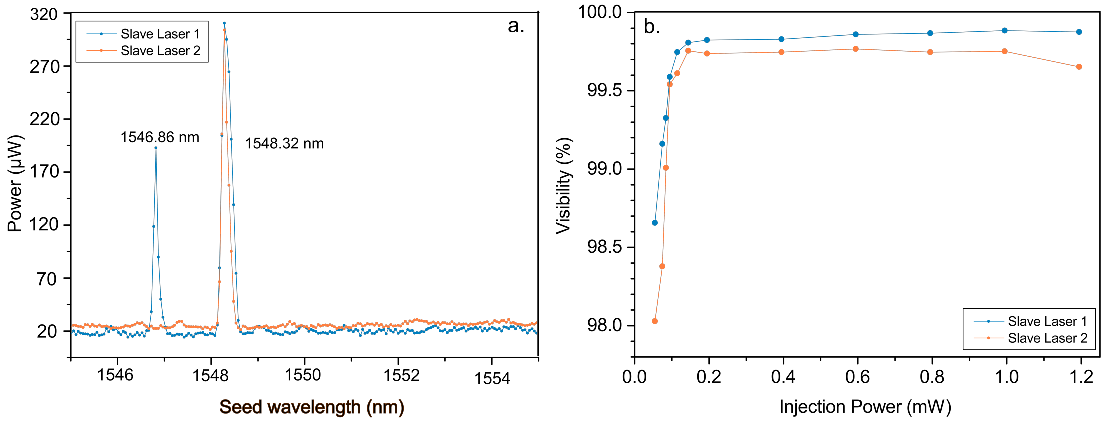

Figure 4.2 **Optical injection locking investigation: a.** The wavelengths of the two injected slave lasers are scanned while their power output is monitored. The OIL resonances are clearly seen at 1548.32 nm for both lasers. Laser 1 has a weaker side mode at 1546.86 nm, which however can be removed with spectral filters. **b.** Using an AMZI integrated on a PLC, consecutive slave laser pulses interfere. From the fringes, the visibility is extracted, as a measure of coherence. As the seeding power increases, the visibilities of the slave lasers improve before reaching a plateau at 0.2 mW. Both lasers successfully reach a visibility higher than 99.7%.

The setup for OIL is shown in figure 4.1. A narrow-linewidth master laser source (LS), CW or pulsed, is set up and tuned to the desired wavelength of around 1550 nm. The linewidth of this source is around 50 kHz. Two distributed feedback (DFB) laser diodes (LD) are tuned to a similar wavelength through their DC voltage and TEC control. The slaves are required to generate pulses and hence they are gain-switched by a 2 GHz electrical signal created by a pulse generator, where the duty cycle of the signal is 25%. Gain-switching at this frequency depletes the electromagnetic field in the laser cavity, and thus ensures that each pulse will either have a random phase or inherit one from an injected optical field. For OIL to take place, the laser diodes are biased below the lasing threshold as to output light of around 20 μW when no light is injected into their cavities.

Circulators are used to connect master and slaves and enable OIL. Light from the master laser is split in half by a beam splitter (BS). Each half enters a circulator (C) throught port 1. The circulators direct the light from port 1 to port 2m to enter the cavity of a slave laser diode. Commonly, laser diodes have isolators at their outputs to avoid back-reflections. Slave laser diodes must lack this feature, otherwise light from the master will not be able to enter the slave. Instead, the master requires the isolator, to output higher quality light.

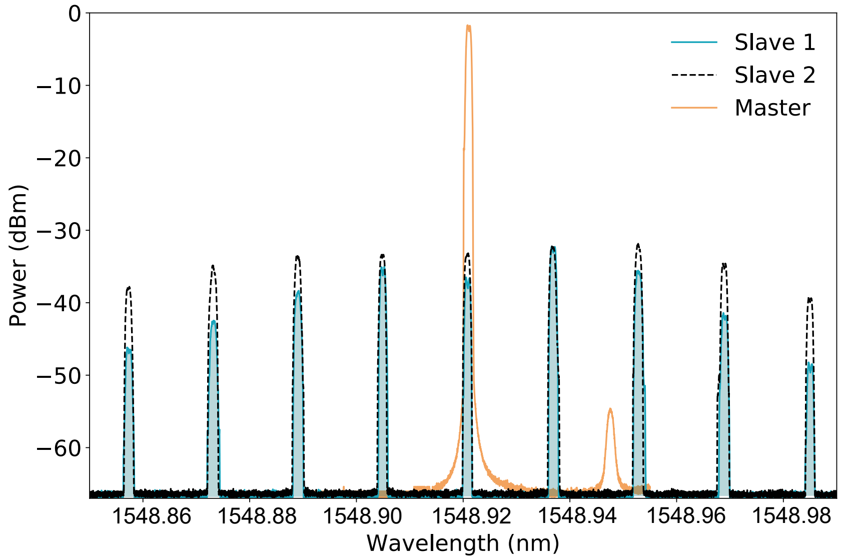

Figure 4.3 **OIL wavelength spectra:** The spectra of the two slave lasers and their master are shown. As expected, a frequency comb with a 2 GHz separation is generated in the slaves' outputs, with well aligned peaks between the two. The central peaks of the combs also align with the narrow peak of the master laser. The latter shows a side band on the right-hand side of its central peak, which however is clearly not the peak causing OIL in the slaves.

Stimulated emission begins in the cavity and the temperature is varied to ensure the wavelength of master and slave are matched. The indicator of matching wavelengths is the power output of the slaves. Once wavelength detuning is minimised, slaves generate maximum power output at around $300\mu W$. This optimisation is shown in figure 4.2a, where the power output of the both laser diodes is monitored during a wavelength scan. Resonances at the central wavelength of the master laser, 1548.32 nm, are observed in both diodes during this measurement. A side mode at 1546.86 nm is also shown for slave laser 1, which however will be removed with spectral filters. This will be done to avoid contamination and therefore visibility degradation.

It is enough that the master laser injects μW into each slave. Nevertheless, there seems to be a correlation between injection power and coherence of the slaver laser's emitted light. In figure 4.2.b, the coherence of the slave lasers is inspected versus a varying injection power. Coherence is measured through the visibility of interference fringes when the slave laser interferes with itself [146]. For this measurement, an asymmetric MZI (AMZI) on a planar lightwave circuit (PLC) silica waveguide was used. The PLC has a non-tunable delay of 500 ps between the two arms which matches well the 2 GHz repetition rate of the system, making consecutive pulses interfere. Its benefit over a fibre optic AMZI is its high phase stability and robustness against temperature changes, due to its shorter optical paths and active temperature-stabilisation system. Consequently, polarisation and phase do not drift during the light's travel through the waveguide. It is apparent from the figure that as the power increases, the coherence of both injected lasers improves until it plateaus to a visibility of 99.8%, at the optimal injection power of 200 μW. Using this measurement the injection power was optimised. This is of great importance since unoptimised coherence of the lasers will negatively affect the visibility in a TF-QKD experiment and hence will increase the QBER and decrease or fully demolish the secret key rate.

With OIL, the indistinguishability of the spectra of the two slave lasers increases dramatically. The central peaks of the frequency combs of the slave lasers overlapped perfectly with each other and with the spectral peak of the master laser. However, the outer peaks did not seem to match well since the envelopes which enclosed the frequency combs were not identical. To correct this, tunable spectral filters were added after port 3 of the circulators on each side. The insertion losses of the filters were measured at around 7 dB and 9 dB but are depended on the set bandwidth. The latter was optimised based on monitoring how the visibility of the interference of the two lasers changed, while also monitoring the shapes of the two spectra on an optical spectrum analyser (OSA) of pm resolution. The optimised values were found to be 30 GHz and 20 GHz and the final spectra of the injection locked lasers, as well as the CW master, are shown in figure 4.3. In the time domain, with the use of these filters, the pulses broadened from about 67 ps to 75 ps, a width which was still sufficiently narrow, given the of 2 GHz clock rate.

4.2.2 Phase randomisation

In the experiment described in section 4.2.1, the master laser was driven in CW mode. The PLC was used to interfere consecutive pulses to determine the coherence of the injected lasers and hence the quality of the OIL. As mentioned in section 4.1.3, in OIL, not only is the spectrum of the master inherited by the slave but also its phase. Therefore the slave pulses are constant in phase, following the constant phase of their CW master.

In the case of a pulsed master laser, the phase of each emitted pulse should be randomised as it is driven above and below lasing threshold. To achieve this, we replace the CW master laser with a third DFB laser diode. This diode includes an isolator at its output, removing back reflections and thus improving its quality. It is also driven at 2 GHz by a pulse generator

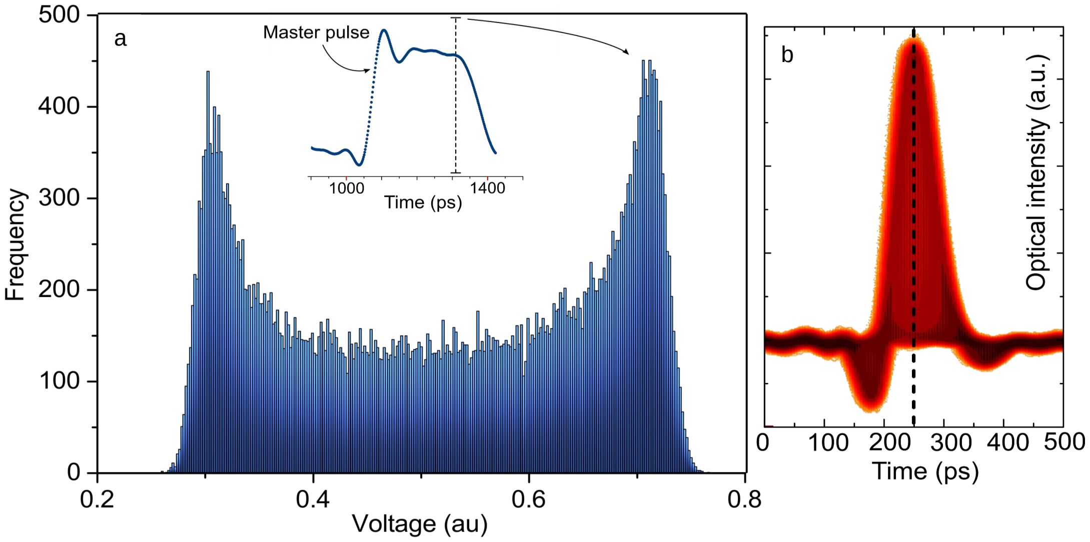

Figure 4.4 **Phase randomisation via OIL: a.** The inset figure shows the time-tagged optical intensity of a gain-switched DFB master laser pulse. In the main figure, the histogram of the optical intensity of a gain-switched DFB master laser pulse is represented by the dashed line in the inset figure. The characteristic U shape confirms the continuous phase-randomisation of the pulse. **b.** Colour coded density plot of a slave laser's intensity after a 500 ps AMZI, when injected by a *gain-switched* master laser, confirming the random phase is inherited after injection.

and tuned to around 1548 nm. The main difference in the way the master laser diode is driven, compared to the slave lasers, is the length of the electrical gate and the DC bias level. While slave laser pulses should be short, to avoid cross contamination in the final interference, master laser pulses used in OIL should be long. Moreover, the DC bias needs to be strong enough, such that the lasing threshold is exceeded in each applied electric gate, to cause stimulated emission in the master.

An optical pulse emitted by the gate-switched master laser is shown in the inset of figure 4.4.a. At the start of the electrical signal it shows an overshoot, followed by a ringing, before finally settling into a flatter intensity region resembling the electrical signal and lasting until the gate is switched off. The observed characteristics are in line with the laser dynamics, as explained in section 4.1.3. It is expected that the phase randomisation of the master's optical pulse is best towards its end, where the carrier population inversion process has dampened. Therefore, the master pulse was generated to be 350 ps long, to allow time for the relaxation of this process and provide a segment where phase randomisation is optimal.

Interfering the master laser pulses using the PLC integrated AMZI, we quantify their phase randomisation. The output of the PLC is connected to a fast photodiode, whose electrical signal is read by a real-time oscilloscope of 40 GSa/s. Creating a histogram of the registered interfering pulses, by choosing a tiny cross section in the flat region of the pulse, we observe the characteristic U-shape expected from the interference of coherent signals with random mutual phases.

The occurrence of the U-shape in the histogram of interference intensities can be easily explained. When interfering light the most common outcomes are destructive and constructive interference. This is due to the fact that interference intensity has a sinusoidal dependence on the relative phase of the interfering fields. As this phase randomly acquires any value from the interval $(0, 2\pi]$ in a flat distribution, the corresponding interference intensity distribution peaks at its constructive and destructive values. If a perfect system is under inspection the constructive and destructive peaks should be sharp and of equal height.

In the measurement presented here the two peaks in the U-shape differ slightly in height and width. Starting form the left-hand side, the first peak (destructive interference) is shorter and spread wider while the second (constructive interference) pulse is slightly taller and slimmer. These deviations from the optimal case are to be expected in a practical system. Higher intensities are more defined and well-measured. Instead, as we get closer to the minimum sensitivity of the photodiode, the measurement jitter increases and so does the background noise intrinsic to the device. Consequently, lower intensities are registered with a bigger standard deviation, slightly widening and shortening the destructive peak of the histogram. These experimental imperfections are accounted for, in the simulation used to fit the histogram. The two parameters used to implement the imperfections are fit empirically. Agreement between the theoretical curve and the experimental histogram, confirms the randomness of the phase of the master's pulses.

Two synchronisation requirements result from the above observation:

- OIL should be time-aligned such that the flat part of the master pulse seeds the slave lasers.
- Same cycle pulses from the two slave lasers must be incident on the interference beam splitter at the same time.

To fulfil these requirements, time calibration is required. The delays of the electrical signals pulsing the slaves are fine-tuned, while observing their first order interference as to maximise their visibility. Next, while keeping these delays constant, the delay of the gain-switched master laser is coarsely-varied. This is done while observing the coherence of a slave laser using the PLC interference. This time, the light fed to the PLC is the output of port three of the circulator, so the OIL generated light from a slave laser. Plotting the heat map, or colour coded density, from the interference of one slave laser we confirm the phase randomisation was inherited from the master, figure 4.4.b. An analogous measurement on the second slave laser gives similar results.

4.2.3 Results

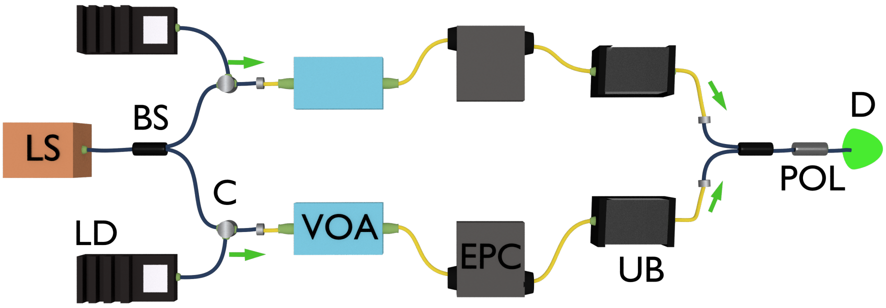

Figure 4.5 **Optical injection locking test setup:** A simple interferometer was built to test the indistinguishability of two sources locked via OIL. A single master laser source (LS) split in half by a beam splitter (BS), injects two slave laser diodes (LDs) by using circulators (C). Variable optical attenuators (VOAs) are used to equalise intensity in the two interferometric arms, while a combination of electrically driven polarisation controllers (EPCs) and a polariser (POL) after the interfering BS form a polarisation control system. Fibre U-benches (UB) allow individual arm isolation. SNSPD D is used for interference-fringe detection.

To confirm that OIL has induced high spectral indistinguishability between the two sources and suppressed phase drifts in the central frequency, an interferometric measurement is performed. To ensure that other degrees of freedom will not impair interference visibility, the setup is upgraded to minimise noise through the control of polarisation and intensity. The upgraded setup as shown in figure 4.5. Polarisation control is achieved through the addition of a polariser (POL) preceding the interference detector (D) and electrically driven polarisation controllers (EPCs) in each arm. Since the polariser only allows one polarisation axis to pass through, we use it in conjunction with the EPCs to maximise the power incident on the power meter. To isolate light of each arm and perform the optimisation independently, fibre U-benches in each arm are utilised. Finally, for intensity optimisation, variable optical

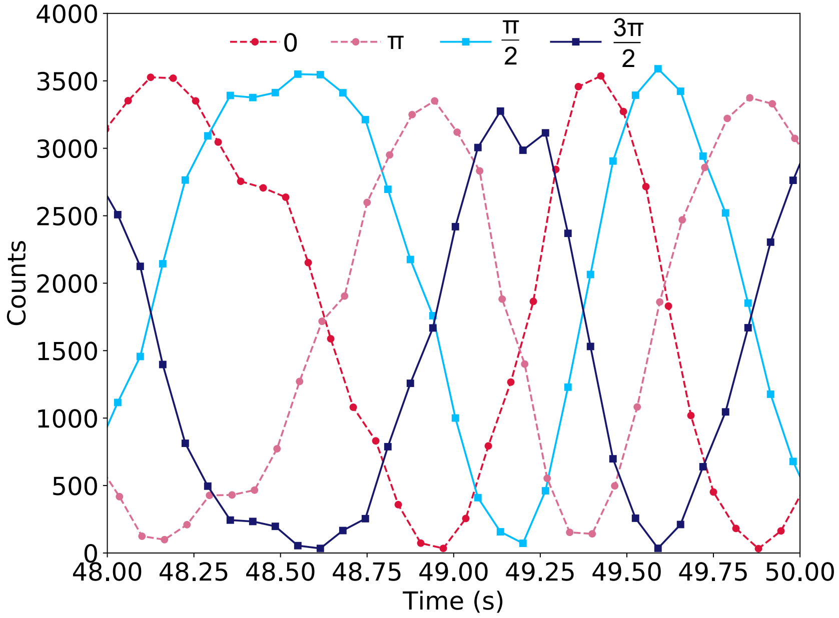

Figure 4.6 **Interference fringes of optically injection-locked sources:** Two sources generate pulses through OIL from a common master. These are encoded with the four BB84 phase states, optimised in polarisation and intensity and sent to interfere at a beam splitter. The plot shows the resulting interference fringes as a function of time, by grouping and monitoring pulses from the same phase state independently.

attenuators (VOAs) are now also part of the interferometric arms. The intensity is calibrated acting on the VOAs and utilising the U-benches, until equal intensities from the two arms are observed on the detector.

In the final measurement, optimised pulse pairs of the same clock cycle emitted by the two injection-locked lasers interfere through the new MZI setup. The maximum acquired first-order interference visibility reached 98.7%, confirming the phase and spectral coordination as well as the indistinguishability of the sources in all degrees of freedom. In a QKD experiment, this value would translate to 0.65% QBER, a highly robust result. The maximum value is taken since the interference visibility showed a slow drift due to changes in the relative lengths of the two arms in the interferometer of figure 4.5. Even with around 40m of optical fibre, environmental fluctuations caused a relative phase-drift in our setup of 1-10 rad/s. Hence, it was deduced that for high visibility to be maintained, OIL should be combined with a phase feedback control acting every 10-100 ms.

The phase drifting interference fringes of the injection-locked lasers can be observed in figure 4.6. Four different sets of data are plotted on the graph. This was done as a preliminary test to the QKD encoding quality potential of the setup. Using a simple in-line phase modulator on one arm, connected to an arbitrary waveform generator, the four BB84 states $0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}$ were encoded in a repeated pattern. A time-tagger connected to the detector was used to select and monitor the drift of each encoded state independently. As can be seen, all encoded states are free drifting in phase at around 6 rad/s but their maximum visibility is high, exceeding 98%. Optimised orthogonality between states of the same basis is also observed.

4.3 Phase locking of distant lasers sources through an optically phase-locked loop

In the previous section phase-locking of two lasers to a common source was successfully demonstrated via OIL. While the latter technique provides significant benefits to the system, the concern with using it to perform TF-QKD revolves around implementation security. There is a significant lack of research into the fundamentals of OIL for QKD and potential side-channels have not been investigated. For example, in the case of utilising OIL for distributing a common phase reference to Alice and Bob, even if the incoming light at the users' stations was to be monitored by detectors, Eve could tamper with the wavelength to move some of the light out of the spectral response of these detectors. This poses a security risk, which renders OIL unsuitable for an implementation where the injected light is to be deployed in a public channel, such as the one needed to phase-lock distant lasers. For this reason we have instead developed an OPLL based on heterodyne detection, to replace OIL in phase-locking the lasers. OIL was otherwise exploited in the proof-of-principle demonstration described in section 3.1, both directly, and in a supporting experiment. The security advantage of the OPLL versus the OIL method will be explained in the following sections. It is important to note that an OPLL had never been employed in a QKD system before even though it is a technique commonly encountered in classical communication systems.

4.3.1 Setup

For the development of the OPLL, optical and electronic components were combined in one loop. In figure 4.7, the schematic incorporating all constituents is presented. Alice and Bob each possess a tunable narrow-linewidth CW semiconductor laser of 50 GHz linewidth set at

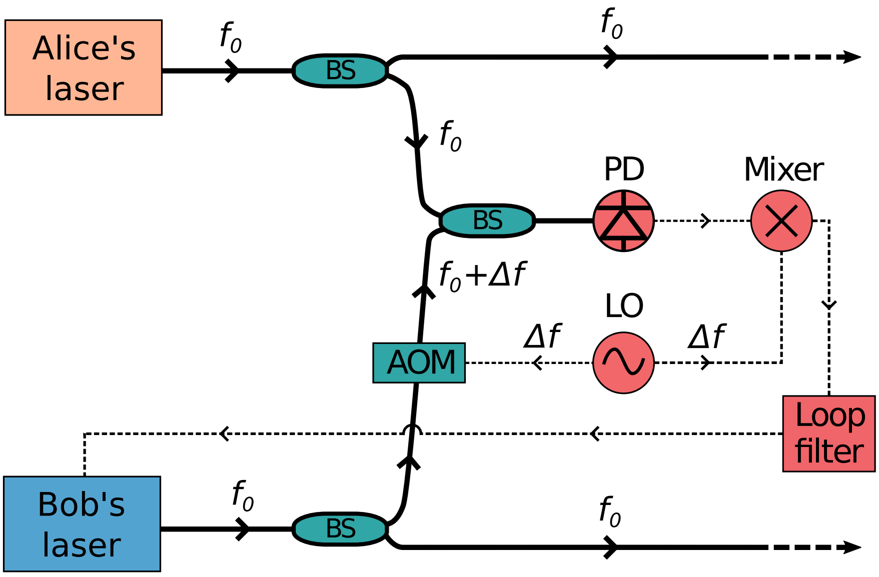

Figure 4.7 **Phase-locking scheme:** A diagram of the OPLL developed for locking distant laser sources. Electronics (cables) are shown in red (dotted black lines) while optics (fibres) in green (solid black lines). BS, 50:50 beam splitter; PD, photodiode; Mixer, electronic mixer used as a phase detector; LO, electronic local oscillator; f_0, reference frequency; Δf, frequency offset (80 MHz) provided by the LO.

the C-band wavelength. They both want to use half of this light to phase-lock their lasers to each other, while keeping the rest to be utilised for QKD purposes. Thus, they use a beam splitter to send half their light to the experiment and half to the OPLL. In this section, only the light used for phase-locking is of interest and hence all following mentions refer to this.

Alice's laser source will act as the master, rendering Bob's laser as the slave. She sends her light of frequency f_0 down a duty fibre to Bob's station while Bob uses an acousto-optic modulator (AOM) to shift his frequency, f_0, by a small amount Δf. In our experiment, the AOM upconverts Bob's frequency by 80 MHz with respect to a local oscillator. The upconverted light interferes with the master's light on a coupler (BS). Due to their frequency offset, the interference between the lasers will produce a beating signal, which in turn is registered by a photodiode. After detection, the electrical signal of the beating is directly compared to the local oscillator used in the upconversion, by mixing of the two electrical signals. Hence, the photodiode acts as a phase-sensitive detector mapping the registered intensity to the phase difference between Alice's and Bob's light. The loop filter is responsible for acquiring this signal, calculating the feedback required to minimise the difference and sending the appropriate feedback signal to shift Bob's laser. As a result, while the frequency of Alice's light naturally drifts, Bob's laser is forced to follow these fluctuations and the two sources successfully phase-lock.

4.3.2 Results

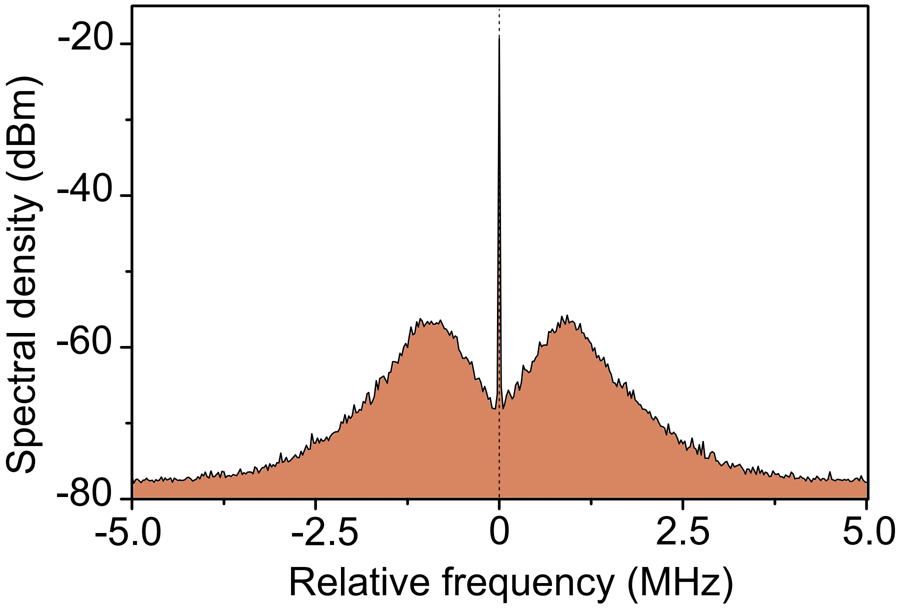

Figure 4.8 **Phase-locking results:** The RF output of the phase-sensitive photodiode is presented, as recorded by a spectrum analyser while the phase-locking mechanism was on. An 80 MHz offset is applied to the graph horizontal axis. The measurement shows a 40 dB extinction ratio, signifying a residual phase error of $\sigma_\phi^2 = 7.53 \times 10^{-3} rad^2$.

To characterise the **performance** of the phase locking, the RF output of the photodiode was recorded on an electrical spectrum analyser. This measurement, shown in figure 4.8, was taken while the locking-loop between the two laser sources was active. The relative frequency between the two sources in MHz is shown on the horizontal axis, with the spectral density in dBm on the vertical axis. The 80 MHz AOM induced offset is also applied to the horizontal axis. The frequency difference of the sources is centred around zero, with the strong peak of 40 dB extinction ratio used to extract a residual phase error of $\sigma_\phi^2 = 7.53 \times 10^{-3} rad^2$. Assuming 16 phase slices are used when carrying out the TF-QKD protocol, the maximum tolerated phase error is 0.3 rad. Consequently, the OPLL gives us plenty of space for other sources of phase error to be introduced without catastrophic results on the secure key rate.

One of the reasons why the phase-locking was successful to such a high degree was the use of the heterodyne detection technique. A homodyne OPLL could have been employed as in ref. [113]. However, in that case, the beat note recorded by the photodiode would be close to its DC and further from the frequency of the local oscillator. The heterodyne loop had the opposite effect. Consequently, we were able to filter out the low-frequeny noise and make the locking mechanism more robust against intensity fluctuations. The phase-locking mechanism was occasionally disrupted only due to specific types of vibrations. For example, if the source of the vibration was a metal-on-metal clash on the optics table, then high frequency noise would affect the AOM and break the OPLL. Nevertheless, re-locking the sources was easy and the only required steps were relocating the correct beating peak on the spectrum analyser and resetting the control loop.

The **security** benefits of using the OPLL instead of OIL to perform phase-locking are outlined below:

- The master laser light is prepared locally by Alice, so it is inaccessible to Eve, whereas previously Eve controlled the master laser.
- In the OIL setup, the light from the master was injected directly into the cavity of the users' slave lasers. Hence, Eve could potentially influence the light entering the cavity. On the contrary, with the OPLL in place, the light from Alice's master laser, that could possibly be attacked by Eve, only interferes on a beam splitter with the light beam prepared locally by Bob and Eve's light never reaches Bob's laser cavity.
- The OPLL allows us to lock both users to a constant phase and then perform active phase randomisation locally in Alice's and Bob's modules using modulators. Since phase randomisation is essential for the security of the protocol this step was a vital improvement.
- OIL can still be used in conjunction to the OPLL. The remaining light emitted by Bob's locked laser, can be sent to the cavity of a gain-switched DFB laser, as to exploit OIL to perform pulse carving for QKD. This allows further decoupling of the QKD pulses and the OPLL.

4.4 Phase control of a short quantum interferometer

The most crucial obstacle to overcome before successfully performing TF-QKD, is the stabilisation of the light fields in terms of phase drift induced in the channels. Fibre, whether standard single-mode or polarisation maintaining, is highly susceptible to its environment, especially with regards phase. It is expected that, even a 50 m long interferometer will drift at around 10 rad/s while a long interferometer of 500 km will drift 1000 times more rapidly [1]. In this section, a short quantum interferometer is built and a feedback system is developed to correct the phase drift with high accuracy. This will serve as the basis to extend the correction to realistic distances for a real-life long distance TF-QKD system.

4.4.1 Setup

Referring back to the setup in figure 4.5, the interferometer depicted was about 40 m long. Interference fringes for this setup were recorded as the light was free drifting in the fibre, see figure 4.6. Quantifying this drift we obtain a value in the order of a few radians per second. Specifically, depending on lab conditions, the drift varied from 5-10 rads/s. To compensate for this drift and maintain sufficiently low phase-error between the two interfering lasers a phase-correction feedback must act every 10-100ms.

For the realisation of the phase-correction mechanism, our device of choice was a Lithium Niobate ($LiNbO_3$) electro-optic in-line phase modulator. This type of modulator can be biased by a DC and an AC voltage simultaneously. An applied electric field changes the refractive index of the $LiNbO_3$ crystal. As a result, the change in refractive index of the crystal alters the speed of light as it travels through the crystal. This phenomenon is used to control the optical phase of the light as it passes through the device. The RF input, where AC current can be applied, is used to create fast changes in phase up to GHz clock rates and hence individual pulses can be manipulated, for example to achieve bit encoding or phase randomisation. The DC input is used to create slower and continuous changes in the phase and consequently it is ideal for a phase-correction feedback.

The phase modulator is added to one of the two interferometric arms. In a TF-QKD experiment, this is assumed to belong to the detection station. For the purposes of the experiment described in this section there is no need to act on the RF input of the phase modulator, as no QKD encoding will take place. The modulator will be controlled solely through a varying DC voltage. A 12-bit digital to analogue converter (DAC) is connected

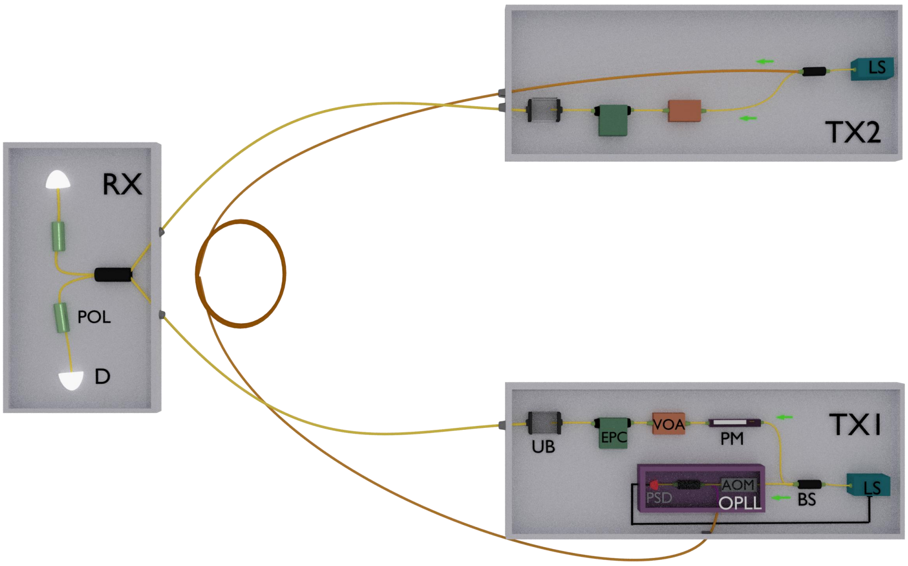

Figure 4.9 **Setup with slow phase stabilisation:** The setup is phase-stabilised via an added phase-modulator in TX1, using the light travelling down the yellow fibres. The phase-locking (OPLL) co-exists and takes place in an extra duty fibre (orange fibre). The components are similar to the setup described in 4.3 with the receiver (RX) now utilising both beam splitter (BS) outputs. LS, laser source; AOM, acousto-optic modulator; PSD, phase-sensitive diode; VOA, variable optical attenuator; EPC, electronic polarisation controller; UB, fibre U-bench; POL, polariser; D, detector.

to the phase modulator to translate the digital commands, given by the developed feedback algorithm, to a DC voltage. The feedback is decided subject to the optical power incident on a power meter recording the interference fringes. In section 1.3.3, it was stressed that TF-QKD is an MDI-QKD protocol. Thus, Charlie being in complete control of the phase control mechanism poses no risk to the security of TF-QKD.

In the case where the light is attenuated to a flux smaller than 1 photon/pulse, as required by a QKD system, the power meter is replaced by a superconducting nanowire single-photon detector (SNSPD) and counts are used instead. The full setup is depicted in figure 4.9, where the light used for phase stabilisation travels down the yellow quantum channel fibres while phase-locking is synchronously taking place using light travelling down the orange duty fibre.

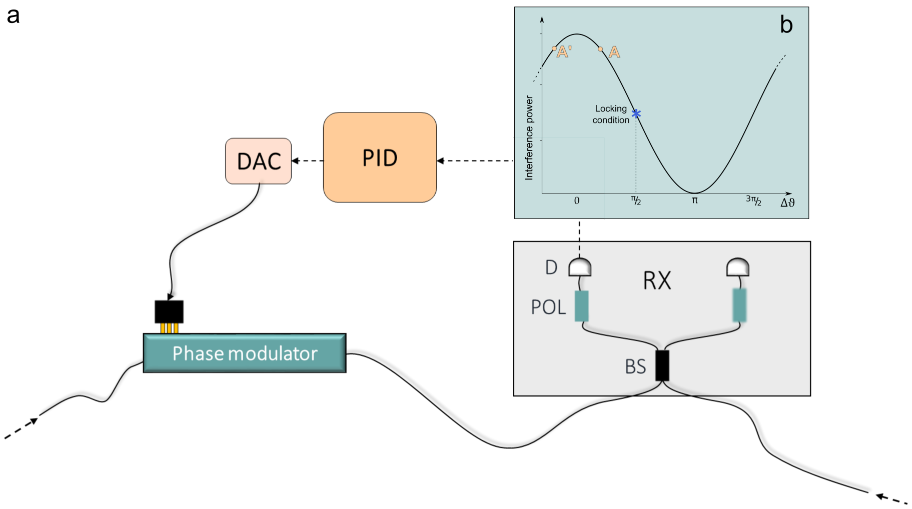

Figure 4.10 **Control loop for slow phase drift correction:** The intensity of the interference fringes is monitored through detector D and must be locked at the $\frac{\pi}{2}$ target point, as shown in **b**. The error signal is extracted from the difference of the instantaneous intensity from the target intensity. It is then processed by a PID algorithm which, using a DAC, sends the correction signal as a voltage to the DC input of the phase modulator to stabilise the phase of the interfering fields.

4.4.2 Basic control routine

To understand the idea behind the phase-correction routine developed, it is helpful to first consider a simple interference curve. Looking at figure 4.10.b if two light fields interfere in an MZI configuration, such as the one shown in figure 4.9, then the intensity of the interference fringes has a sinusoidal relationship to the phase difference between the two fields at the time interference. Such a relationship entails that the interference intensity is most stable when the constructive or destructive conditions hold. Contrary to that, at the multiples of $\frac{\pi}{2}$ phase difference, the intensity is almost linearly dependent to the phase fluctuations between the two fields. Therefore, if the target is precise and quick control of the phase drift, then working in the linear part of the sinusoidal is optimal. We shall then intent to provide a feedback to the phase modulator that will keep the output intensity locked to the quadrature point ($\frac{\pi}{2}$).

A crucial piece of information required to develop the aforementioned feedback system is the relationship between the voltage applied to the DC pins of the phase modulator and the induced optical phase change. A linear trend is expected as the refractive index of $LiNbO_3$ changes linearly with the applied electrical field. This was confirmed by characterising this relationship in three different phase modulators, in a short and well-isolated MZI setup. It was confirmed that linear regression fits the behaviour of all modulators. Nevertheless, the voltage required to cause a 2π shift in optical phase, $V_{2\pi}$, differs in each modulator. This was measured in the range of 20-24 V, setting the requirement for the feedback DAC to be followed by an amplifier to allow a total voltage output range of -12 V to +12 V.

Correction algorithm

The feedback algorithm is comprised of three steps. The first is the **initialisation stage**, responsible for gathering all information necessary for the feedback to proceed correctly. To achieve this, the DAC outputs a few cycles of a linear voltage variation, to scan across the horizontal axis of figure 4.10.b. During the scan, the power of one of the interference beam splitter outputs is monitored. The target is to determine the maximum and minimum interference intensities, I_0, I_π, so the value at the constructive and destructive points respectively.

I_0 and I_π depend not only on the individual intensities of the fields, but also on their total indistinguishability. If the light fields are distinguishable, optimum constructive interference will not be achieved, constructive intensity will be finite and as a result the visibility will be less than 1. In fact, in a realistic experiment, the visibility will never be equal to 1. This causes an offset in the y-axis of the intensity sinusoid shown in figure 4.10.b. The aforementioned curve is defined through the following equation:

$$I = \frac{I_0 - I_\pi}{2}(cos\phi + 1) + I_\pi \tag{4.4}$$

where ϕ is the phase difference of the fields at interference. We will be inputting the two quantities, I_0, I_π, extracted from the initialisation stage into equation 4.4, to calculate the phase difference of the fields for every recorded intensity.

As soon as the initialisation cycles finish and the I_0, I_π quantities have been well defined, the **feedback calculation stage** begins. The algorithm has already used equation 4.4 to calculate what the intensity at the quadrature point, $I_{\frac{\pi}{2}}$, should be. It hence proceeds by ending the linear cycling and measuring the intensity of the interference fringe when no DC voltage is applied, I. Inputting I, I_0, I_π into the same equation, outputs the current phase difference, $\phi = \frac{\pi}{2} + \delta\phi$, between the interfering fields.

The phase modulator needs to push the light passing through it by $-\delta\phi$ to establish the quadrature condition. Using the $V_{2\pi}$ value, as characterised for the modulator in use, phase is translated into voltage and the command is sent to the DAC. One vital detail of the feedback algorithm is that it always commands a push to the right hand side of the interference curve. In figure 4.10.b the points marked as A and A' would be indistinguishable in a power measurement. However to avoid pushing in the wrong direction and confusing the feedback we require that it always pushes in the same direction. Given that the feedback is applied quickly enough, the light shouldn't have enough time to drift to a point such as A' and the feedback successfully runs continuously.

In the final step, the **correction stage**, the DAC applies the necessary voltage to the phase modulator. Stages 2 and 3 are repeated until the feedback is turned off while stage 1 can be re-activated in case the feedback performs poorly or fails.

The repetition rate of the feedback is limited by the integration time set to acquiring the power measurement. When using the power meter, the minimum integration period is around 0.08 s while with the counter we can go down to 10 ms. The speed-up in the single-photon scenario is significant since lower fluxes require longer acquisition times for decent sampling. If not enough counts are collected during integration, then the standard deviation in the phase-error estimation increases and the feedback cannot perform with sufficient accuracy.

The control routine was further upgraded to enable the user to fine tune the feedback depending on the situation. The calculation of the error-correction signal, as described in the previous paragraphs, relied on a proportional control loop. In such loops, only the scaling factor in front of the error-correction signal can be varied, to force the correction to provide a smaller or bigger fraction of it. A proportional-differential-integral (PID) control loop was developed as an alternative method of calculating the error-correction signal. Depending on the amount of fibre in the setup or the lab conditions at the time of the experiment, the PID allowed us to further smooth-out the effect of the phase feedback, mainly by acting on the proportional and integral terms. The differential term did not offer any observable benefit to the quality of the correction.

4.4.3 Results

For the developed phase correction feedback to be deemed successful, it should satisfy the condition below:

- Its action should minimise the phase error between the two transmitters to at least one quarter of 0.3 rads (0.075 rads). This should be achieved while the flux sent by the transmitters is in the single-photon regime and lossy quantum channels connect the transmitters to the receiver. An SPD-counter combination must be used for intensity monitoring.

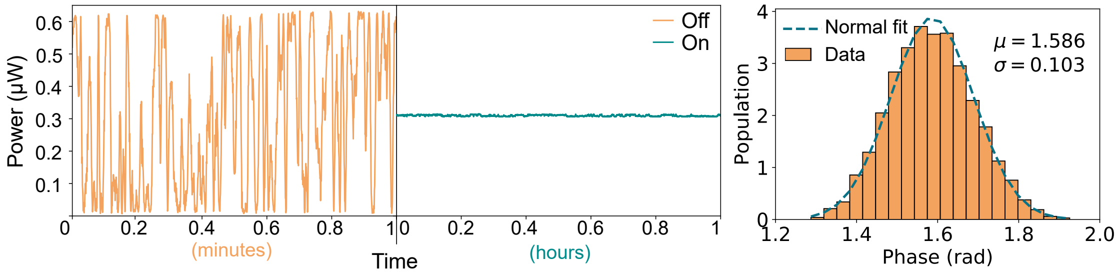

Figure 4.11 **Slow phase drift correction in the classical regime: a.** The initial phase drift of a 30 m long interferometer with bright light travelling through it is recorded to be in the order of 3 rad/s, see left-hand side plot. The correction feedback is turned on and the phase fluctuations are suppressed to the order of 1% of the mean power, see right-hand side plot. **b.** The histogram of the phase difference between the interfering light fields of Alice and Bob is centred near the $\frac{\pi}{2}$ condition with $\sigma = 0.103$ rad.

Bright light regime

Of course testing of the feedback was first performed with bright classical light, low-loss channels and a power meter as the detector, see figure 4.9. The interferometer was small and hence a polarisation optimisation routine utilising the power meter, polariser and electronic polarisation controller was only required twice per day. With the OPLL in place, the phase-feedback was isolated as the only source of leftover phase-error.

The feedback was initially turned off to observe the drift to be corrected. This is shown on the left-hand side plot of figure 4.11.a. Interference fringes show a visibility of 98% and take the form of a random walk sinusoid, as expected. Here, the drift is measured to be around 3 rad/s. The feedback was turned on with a repetition rate of 12.5 Hz and the PID optimised the control parameters. Monitoring of the stable interference intensity took place for an hour and is plotted on the right-hand side of figure 4.11.a.

Looking at the statistics of the correction, the residual fluctuations are 1% of the average stabilised power. Transforming power into phase-error and plotting the histogram we obtain a normal distribution, see figure 4.11.b. The full width at half maximum (FWHM) of the curve equals the leftover phase error and is equal to $\sigma = 0.103$.

Sent flux, Alice	0.2 photons/pulse
Sent flux, Bob	0.2 photons/pulse
Channel loss	90 dB
Detector efficiency	0.4
RX station transmissivity	0.5 x 0.7
Dark count rate	22 Hz
Clock rate	2 GHz
Wavelength	1550 nm

Table 4.1 **Experimental parameters:** These were used as a worst-case scenario to estimate the rate of photons available in a high-loss TF-QKD experiment with a short interferometer.

Quantum regime

The ultimate target for the short interferometer was to demonstrate TF-QKD over high losses but short fibres. As a result, the feedback loop must be able to stabilise slow phase-drift when however the incident light on the detector is dim. To test the efficacy of the feedback in the worst-case scenario, we set the parameters as they would be in a final experiment and monitored the performance of the phase control.

The estimation of the count rate incident on the detector involved in the stabilisation, assuming channels of 90 dB total loss, was 1800 Hz. All parameters used in the estimation are shown in table 4.1. It is assumed that the users would each be sending 0.2 photons/pulse. This flux would be subjected to a loss of 45 dB and the losses of the receiver station. To the latter contribute the finite efficiency of the SNSPDs, the dark count rate as well as insertion losses of the station's optical components. For the estimation of the count rate, the initial flux was converted to power, by taking into account the clock rate. We calculated the effect of the losses and transformed the received power to a measured count rate using $P = \frac{hc}{\lambda}t^{-1}$, where P, power; h, Planck's constant; c, speed of light in fibre; λ, wavelength; t^{-1}, count rate.

We replaced the power meter with an SNSPD and set the attenuation in the two channels such that around 900 Hz were incident on the detector, D. Fine tuning of the attenuation was achieved by adding one VOA into each interferometric arm preceding the 50:50 beam splitter. The other SNSPD was used for polarisation optimisation by acting on the EPCs to maximise the received counts. The PID values were re-optimised and the feedback was turned on for 50 minutes during which the count rate registered by the detector was monitored. During those 50 minutes, the total number of counts registered was near 10^6. It is important to note that the integration time of the counter required for the feedback to work with such a small

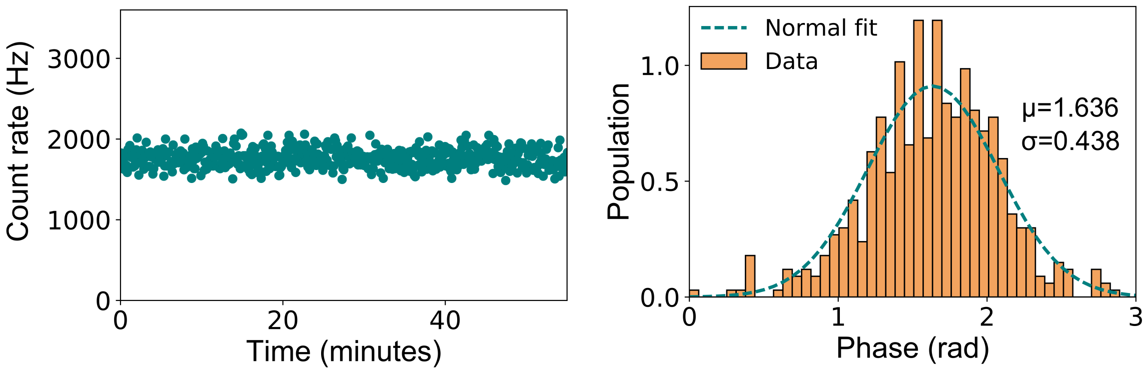

Figure 4.12 **Slow phase correction in the quantum regime:** The plot on the left-hand side shown the counts, after interference, incident on the detector while the system is stabilised. Here, the flux is in the correct level to simulate a TF-QKD system with 500 km of ULL fibre in the quantum channels. The above result is analysed in terms of remaining phase error, right-hand side plot, where the normal curve yields a standard deviation of 0.438 rad.

sample of photons incident on the detector was 100 ms. Hence the maximum repetition rate was 10 Hz.

The results are shown in figure 4.12. On the left-hand side plot of this figure, the monitored stabilised counts are plotted to show the long-term stability of the setup. On the right-hand side, this data was translated into phase difference between the two arms and their histogram was plotted and fitted to a normal distribution. The fitting confirms that the average phase difference between the interfering light fields is close to the quadrature point, as the mean value calculated is $\mu = 1.636$ rad. The FHWM of the normal curve gives a standard deviation value of $\sigma = 0.438$ rad. Compared to the results obtained when bright light was used, there is a clear degradation of the stabilisation. The standard deviation is four times higher than the standard deviation measured in the bright-light testing, while the entire distribution seems a lot more disorderly. With an integration time one order of magnitude longer than the previous case and a smaller sample of photons, this was an unavoidable result.

The equations below, 4.5, were used to estimate the phase-stabilisation leftover error contribution to the QBER, if TF-QKD was to be performed using the system

$$\begin{aligned} \delta\phi &= \frac{\sigma}{2} \\ \Rightarrow I_0' &= \frac{I_0 - I_\pi}{2}(cos(0) - \delta\phi + 1) + I_\pi \\ \Rightarrow I_\pi' &= \frac{I_0 - I_\pi}{2}(cos(\pi) - \delta\phi + 1) + I_\pi \end{aligned} \tag{4.5}$$

We arrive to the value starting from the standard deviation of the normal distribution fitted on the data, $\sigma = 0.438$ rad. We use half σ as the remaining phase error $\delta\phi$ and use this to estimate the constructive and destructive intensities in the case of stabilisation (I'_0, I'_π), using the equivalent values obtained from the free phase drift of the system (I_0, I_π). We use the latter values to estimate the minimum QBER, if the system was to be perfectly stabilised, as in equation 4.2. Similarly the new values I'_0, I'_π give a pessimistic estimate on the QBER value for a system with the stabilisation as described above. The difference between the two QBER values was found to be 0.85% which is equivalent to the contribution of the phase-stabilisation leftover error to the total QBER. This value seems satisfactory since other sources of error could be minimised to less than 2% giving an overall QBER of 2.85%. According to the simulations presented in chapter 2, this error is low enough to give a key rate in a quantum channel of 90 dB loss.

4.5 Dual-band phase stabilisation in the MHz regime

This section describes a complex dual-band stabilisation system developed to correct phase drifts in long quantum interferometers. It is based on dense wavelength division multiplexing (DWDM), a technique in which monochromatic light of slightly different wavelength can travel along the same fibre with low cross-talk. This was combined with fast and slow electronics to successfully recover the phase after a maximum of 605 km of fibre. The slow phase correction feedback described in the previous section, formed the foundation for this MHz control.

4.5.1 Wavelength multiplexing

In this novel feedback, two different wavelengths were utilised. The idea was to isolate *reference* light used for fast phase-correction from *signal* light used to actualise QKD, even if they are both travelling down the same fibre. Ultimately, the target was to achieve strong isolation, without cross-talk, between DWDM channels so that the reference light is allowed to be of much stronger intensity. This permits the application of a fast feedback able to correct extreme drifts, as the reference light fed to the loop can be sufficiently bright.

Assuming we are able to correct the rapid phase drift by observing the strong reference light, then we can synchronously correct most of the phase-drift in the signal. However, the wavelength mismatch between the two channels means that the light with the shorter

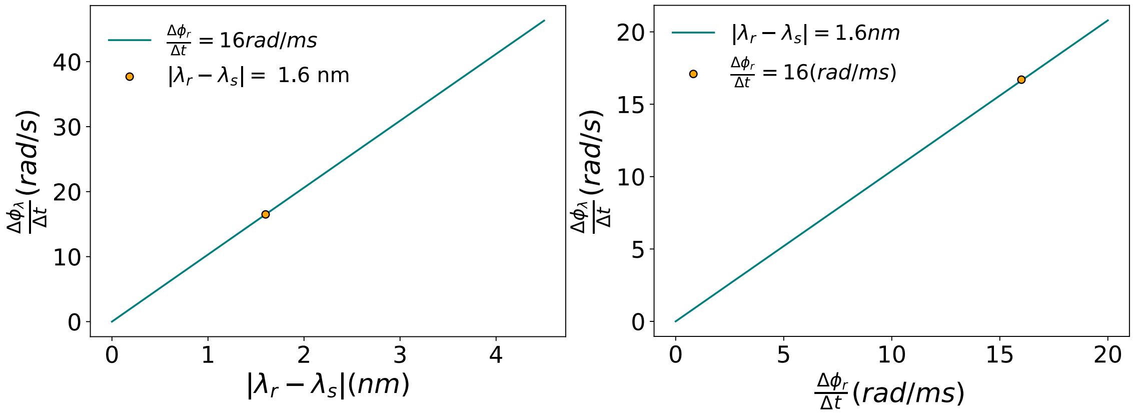

Figure 4.13 **Wavelength multiplexing simulations:** Different wavelengths drift at different rates. Hence, after correcting the fast phase drift of the reference light, $\frac{\Delta\phi_r}{\Delta t}$, a leftover slow drift is expected, $\frac{\Delta\phi_s}{\Delta t}$. **a.** The leftover drift rate is plotted against the wavelength difference between reference and signal, $|\lambda_r - \lambda_s|$ for $\frac{\Delta\phi_r}{\Delta t} = 16\frac{rad}{ms}$. **b.** Here, $|\lambda_r - \lambda_s|$ is fixed to 1.6 nm (2 DWDM channels) and the leftover drift rate is plotted against a varying fast drift instead.

wavelength will have completed more oscillations than the other. Consequently, during their travel, the two wavelengths will slowly drift in phase relative to one another. As a result, after correcting the fast drift induced by the optical paths in both wavelengths, the signal light will still show a leftover slow drift.

To quantify this effect we use equation 4.6 below:

$$\frac{\Delta\phi_s}{\Delta t} = \frac{\Delta\phi_r}{\Delta t}(1 - \frac{\lambda_r}{\lambda_s}) \tag{4.6}$$

where $\frac{\Delta\phi_s}{\Delta t}$ is the leftover drift rate of the signal due to the wavelength difference, $\frac{\Delta\phi_r}{\Delta t}$ is the phase drift rate corrected through the reference light and λ_r, λ_s are the wavelengths of the reference and signal respectively. The derivation of this equation makes use of the expression $\frac{\Delta\phi_k}{\Delta t} = \frac{2\pi n}{\lambda_k}\frac{\Delta L_k}{\Delta t}$ with $k \in \{s, r\}$. Equation 4.5.1, directly correlates the leftover drift of the signal to the wavelength separation of the two channels and the corrected fast phase drift rate of the reference. The behaviour of the leftover drift was simulated as a function of varying wavelength spacing and corrected phase-drift as shown in figure 4.13.

To choose the appropriate DWDM channels, several factors were considered. Firstly, for the particular application, the leftover phase drift rate of the signal must be comparable to the one encountered in the short interferometer experiment (1-10 rad/s). Hence, from the simulations it is extracted that a DWDM spacing larger than 2.5 nm would be inappropriate.

The next considered factor was the isolation between neighbouring channels in a DWDM system which is around 25 dB. However, non-linear effects, such as Raman scattering, are unavoidable and increase exponentially in frequency with the power of the light travelling through. Given that a drift rate three orders of magnitude faster than the short interferometer experiment is expected, the reference light utilised here would also need to be at least three orders of magnitude stronger. Consequently, the chosen channels should have at least 2 channels spacing between them.

Finally, the in-fibre components used in the QKD setups are optimised to work in the C-band. Hence, the QKD light wavelength should be kept as close to 1550 nm as possible to avoid increased insertion losses from various opto-electronic elements. Taking all the requirements into considerations, ITU DWDM channels 34 (1550.12 nm) and 36 (1548.51 nm) were chosen to accommodate signal and reference respectively. Please refer to section 4.5.4 for details about the performance of the chosen channels.

4.5.2 Correction scheme

The architecture required for the dual-band phase correction technique is shown in figure 4.14. A minimum of three laser sources is required. Two will be used as *signal* sources and eventually will be the sources used in QKD for Alice and Bob. The third laser is tuned to a slightly different wavelength to be used as the *reference* and could be located within Alice's or Bob's stations or at a separate node. Light emitted by the reference source is split in half by a 50:50 coupler. Each signal source is combined with one output of the coupler in a dense wavelength division multiplexer (DWDM). Following multiplexing, the two light fields of different wavelength travel side by side in long fibres without mixing.

The first step in the dual-band protocol is the *coarse* phase correction. This is performed on the top arm of the interferometer shown in the diagram and utilises the reference light only. The interference beam splitter, after the long fibre channels, follows another DWDM, which de-multiplexes the two wavelengths. The reference light is detected by SPD0 and the electrical signal of the detector is fed to an FPGA through an RF input. The on-board counter of the FPGA counts the events detected by SPD0 during a certain integration time and passes the result to its motherboard. A correction routine synthesised on the FPGA takes the countrate as input and outputs a correction signal. After passing through the on-board DAC, this is transformed into an RF output which will act on the DC port of the phase modulator in the top arm of the interferometer, to correct the drift similarly to section 4.4.2. Both channels will be affected as they are travelling side by side inside the modulator. Since

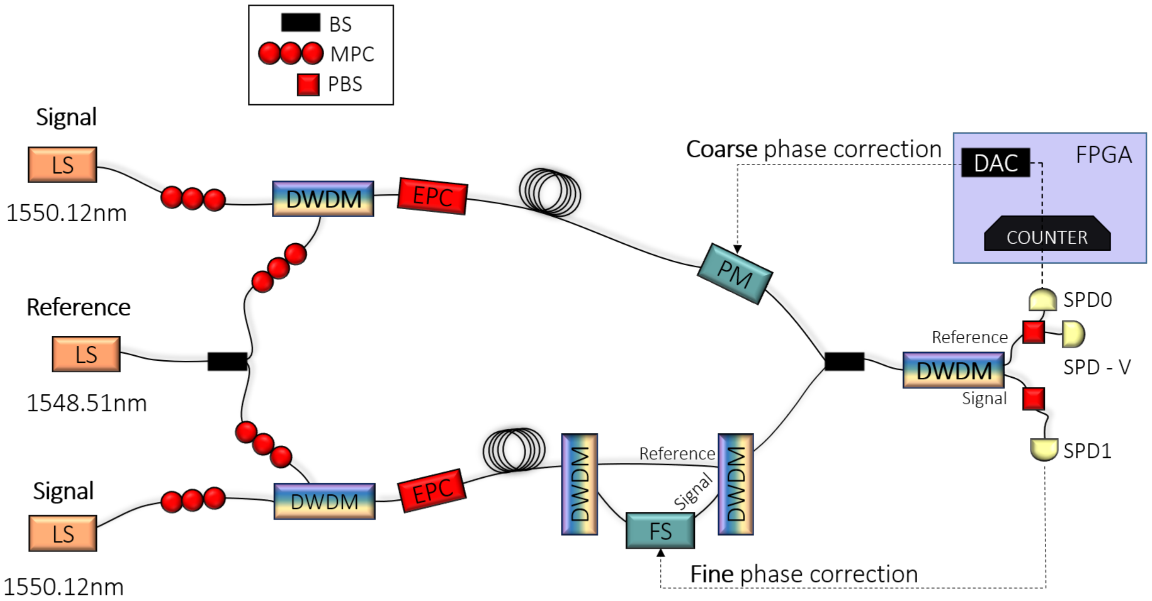

Figure 4.14 **Dual-band fast phase correction scheme:** The diagram explains the basic architecture needed in the setup to implement the dual-band fast phase correction. Coarse and fine phase correction work synchronously, each one at a slightly different wavelength. The first utilises a phase modulator (PM) while the latter a fibre stretcher (FS). Components in red are used for polarisation control. LS, laser source; BS, beam splitter; MPC, manual polarisation controller; DWDM, dense wavelength division multiplexer; EPC, electrically driven polarisation controller; PBS, polarising beam splitter; SPD, single photon detector; DAC, digital to analogue converter; FPGA, field programmable gate array.

FPGAs have fast internal clocks capable of hundreads of MHz the maximum drift the coarse feedback can correct is realistically only limited by the intensity of the reference light. As discussed in previous sections, in every integration period there should be enough photons to form a reliable sample otherwise the correction may not be sufficiently accurate or fail entirely. With successful completion of the first step, the reference channel should be fully stabilised in phase. The channel of interest however remains that of the signal. There, the drift should now be reduced to a slow drift whose origin is almost entirely the effect of the difference in wavelengths described in section 4.5.1.

We refer to the second phase of the dual-band correction as *fine* correction, since its purpose is to suppress the leftover drift in the signal after step one. The de-multiplexed signal light after interference will be used to achieve this. This light is incident on SPD1 which has an integrated photon counter. The minimum integration time of the SPD counter is much larger than that of the on-board counter. Note that the signal channel will also be used to carry the quantum states as encoded by Alice and Bob, hence its brightness is attenuated to the single-photon level. However these two characteristics should not pose a limitation on the control system since the first step has already diminished the drift to a manageable level similar to the drift encountered in section 4.4. Once again, through a control loop the count rate is used to calculate a correction signal.

The main difference on how the correction is applied in the second step, is that now we want the correction to act on the signal channel only. For this, an extra station is added right before interference, in the bottom arm of the MZI. As the multiplexed channels enter this station via a single fibre, they are subjected to a DWDM which separates the two wavelengths. The signal channel output of the DWDM is followed by a fibre stretcher. The output of the latter is combined with the reference channel arm of the DWDM in a second DWDM which re-multiplexes the two wavelengths in a single fibre, before sending them to interfere with the light incoming from the top arm. This station enables the variation of the phase of the signal channel independently by acting on the fibre stretcher. A fibre stretcher is an optoelectronic device which uses piezoelectric actuators to induce tiny changes in the lengths of the fibre. Consequently, the phase of light travelling through it can be modified by changing its DC bias. In this configuration, the correction signal calculated in step-two (fine correction) is directed to the fibre stretcher DC input. As a result, the leftover slow drift of the signal channel can be correct, without affecting the reference. All in all, the dual-band control enables us to fully suppress the phase fluctuations in the signal channel which can therefore be used to stably carry all QKD information.

4.5.3 Setup

An important ingredient for the realisation of the scheme described in the previous section was the FPGA. The board had an internal clock of 200 MHz and an integrated DAC of 16-bit resolution and 50 MHz sampling rate. A custom mezzanine card was added with 4 comparators for transforming the output signal of the SNSPDs into FPGA compatible digital inputs. The output of the integrated DAC was quite limited in range, less than 1 V, so an amplifying circuit was added through the mezzanine card. The combination of the DAC and the amplifying circuit provided an output DC range of $\pm 13\ V$. The counter's repetition rate was limited by the internal clock of the board. Hence, the maximum repetition rate of the control system, given the aforementioned components, was much higher than the requirement the phase drift rate at 600 km is expected to pose. The FPGA output was connected to a $LiNbO_3$ phase modulator with a 2π voltage of around $22\ V$ to match the DAC output range. The maximum bandwidth of the modulator is in the MHz regime, since the DC port was utilised. A greater bandwidth is allowed via its RF port but high RF voltage would produce heat due to the 50 Ohm impedance matching, destroying the device. Nevertheless, the DC bandwidth was sufficient for our application.

For the fine phase correction the same DAC as in section 4.4 was used. The output of this DAC was connected to the DC input of a fibre stretcher with a mechanical time constant of 100 Hz. The maximum stretching length of the fibre stretcher is 19 μm. For light at around 1550 nm, this device covers a 24π range. As required, the fibre stretcher was isolated to act solely on the signal wavelength through the following mini MZI: DWDM - fibre stretcher (signal arm), fibre (reference arm)- DWDM. A dedicated SNSPD channel on Charlie's station monitored the signal interference fringes through the slow counter. The error signal was calculated in a developed LabView PID algorithm and sent to the DAC.

Polarisation control

It was necessary for polarisation control to be continuously applied, as the long fibres in the quantum channels caused significant drifts within minutes. Components in figure 4.14 shown in red, comprise the elements used to control the polarisation. Polarisation states are observed with the help of a polarising beam splitter (PBS) at Charlie. The PBS directs horizontally polarised reference light to the SNSPD used for phase stabilisation (SNSPD0), while vertically polarised light is sent to a second SNSPD (SNSPD - V) for polarisation control.

Since reference and signal are travelling together, if initiated in the same polarisation state, they should follow the same drift. To achieve this, before the two wavelengths are initially combined via DWDMs, manual polarisation controllers (MPCs) are in place to align all light fields to the horizontal polarisation. These required optimisation around once a day, as the amount of fibre before them was quite short. For the rest of the setup, including the long channels, the drift rate of polarisation is in the order of minutes. Hence, while the drift is measured, at the receiver station, the correction can still be applied at the transmitters.

The counts are monitored at SNSPD-V through a slow counter with an integration time of 100 ms. Once they fall below a pre-determined threshold, a gravity search algorithm is automatically initiated to re-align the fields. On each arm, a custom-microcontroller board with multiple DC outputs changes the bias voltage of electrically driven polarisation controllers (EPCs) in three different rotation directions separately. The algorithm corrects all rotations independently, until the improvement in polarisation plateaus. This is done for the

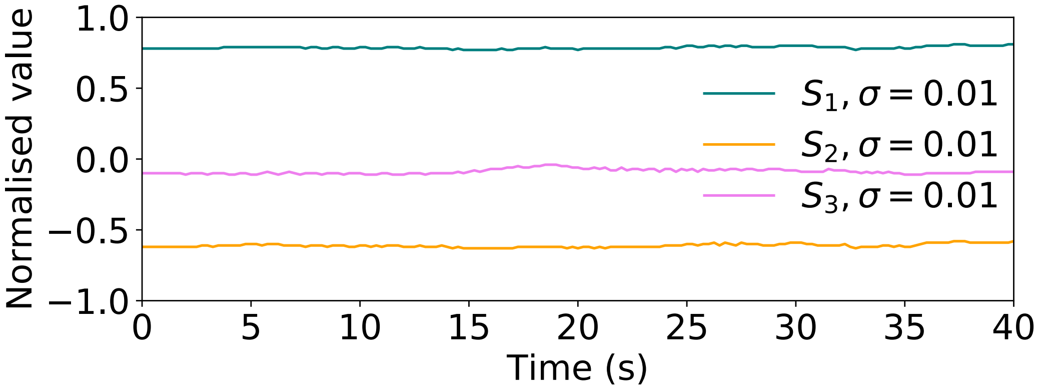

Figure 4.15 **Fibre stretcher polarisation test** The possible effects of the fibre stretcher phase correction on polarisation were investigated via the use of a polarimeter. While the fibre stretcher DC bias was randomly varied, the three Stokes parameters were monitored. The small standard deviation in all three parameters signifies the suitability of the fibre stretcher for the experiment.

two transmitters sequentially, with the polarisation successfully realigned once the process is finalised.

While polarisation control should be effective on natural drifts in the fibre, faster drifts due to the phase compensation scheme may not be successfully corrected. The hazard with the phase compensation scheme is the fibre stretcher, which due to its mechanical nature could potentially have detrimental effects on the polarisation and hence the QBER. To examine any polarisation changes due to the fibre stretcher's action, a polarimeter was used. The three Stokes parameters, S_1, S_2, S_3 of the light passing through the fibre stretcher were monitored over 40 seconds, meanwhile the bias voltage of the fibre stretcher was varied randomly through its entire range. The overall measurement time was kept short so that environmentally caused drifts would not affect it. The voltage step duration was set to 250 ms, as to match the measurement integration time. The result was promising as no sudden changes in the polarisation occurred and no patterns could be seen in the measurement outcome, signifying that the fibre stretcher phase action was not coupled to a polarisation shift. The standard deviation, σ of all three normalised Stokes values was 0.01, which includes mostly smooth effects from external parameters rather than rapid changes related to the feedback. These results are summarised in figure 4.15.

4.5.4 Results

The success of the setup can be determined by its effect on the phase drift rate and thus how low a QBER it can maintain. As previously described, the fast phase drift compensation scheme is separated in two steps. In the first, the aim is to reduce the phase drift **rate** of the signal light to less than 10 rad/s, while in the second the phase **error** should be suppressed. Of course, further degrees of freedom could play a crucial role as well. For example, the polarisation control previously described should be active throughout the operation of the system, since a decrease in the polarisation contrast of the light fields will also degrade the base QBER over time. This also applied to other parameters such as intensity. If these conditions are fulfilled, a low QBER should be maintainable for long periods of time, even in fibre channels longer than 500 km.

To test the effectiveness of the setup, three measurements are required. The first would be a measurement of the free drifting signal interference fringes. Given that the drift rate expected from a system with quantum channels longer than 300 km should be at least 4 rad/ms on average [1], fast sampling rate is required to track the fringes. The second measurement monitors the interference fringes of the signal, while step 1 of the stabilisation is turned on. This is expected to show fringes drifting at at least 3 orders of magnitude less than in the first measurement and thus longer integration times are appropriate. Finally, the last measurement should be an interference test with both step 1 and step 2 turned on. The expected outcome is a fully stabilised system, where the phase error between the two transmitters should be close to 0 rad.

The reference channel is not necessary to be monitored as only its intensity could affect the QBER. However, to set up a successful PID it is useful to monitor the suppressed amplitude of the intensity (phase) jumps once step 1 is turned on. It is important to note here that the stabilisation scheme is not expected to eliminate the phase drift rate in either of the two wavelengths. Instead, it is only expected to reduce the relative phase error of the signals to around 0 rad. A natural outcome of using a PID system is a rapid oscillation of the corrected phase around the locking point. Although such oscillations can be violent and hence have a large instantaneous phase drift rate, they should at the same time be very small in amplitude. Consequently, these vibrations should have negligible effect on the QBER while the phase drift rate that characterises them could be even faster than the one observed in the free drifting system, depending on the speed of the electronics.

The length over which the measurements listed above were taken was 605 km, corresponding to the maximum channel distance. The reference flux was set to 400 photons/pulse

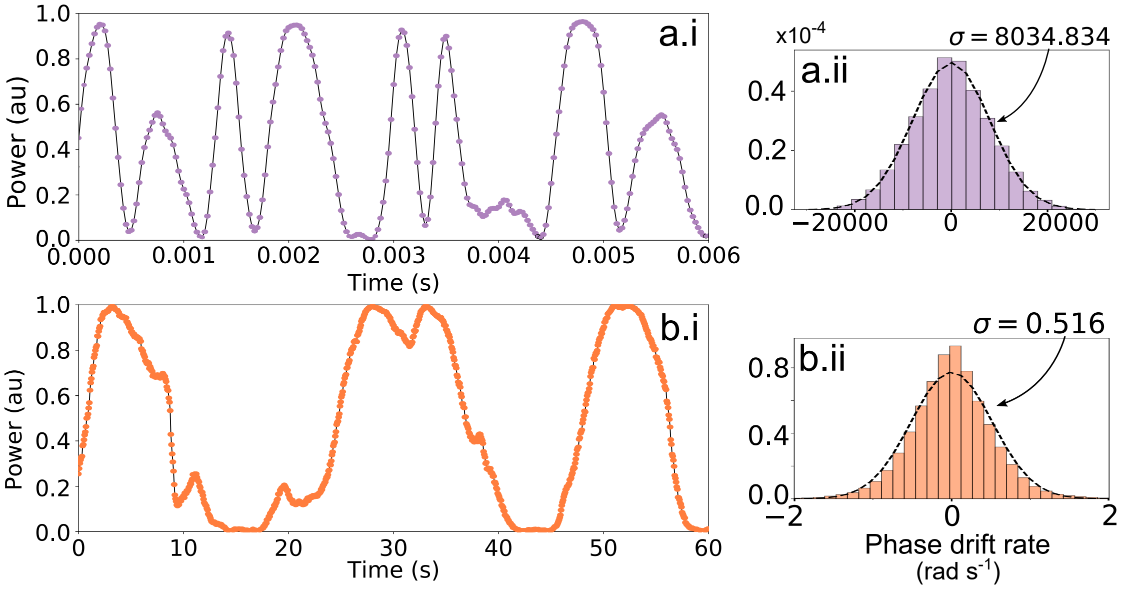

Figure 4.16 **Signal phase drift rate in 602 km channels: a.** The interference fringes of the free drifting system (**a.i**) and the extracted drift rate histogram fitted with a normal distribution (**a.ii** are showing an average drift rate of $8000 rads^{-2}$. **b.** The measurement is repeated with step 1 of the stabilisation turned on (**b.i**), and the standard deviation of the histogram is reduced by 16000 times (**b.ii**) to an average drift of $0.5 rads^{-1}$.

and the quantum flux to a sufficiently large value to allow detection by a power meter and produce easily visible fringes. The repetition rate of the FPGA was set to 200 kHz. Starting from the first measurement, the free drift interference fringes were monitored with $25\mu\ s$ integration time by using a power meter in fast-logging mode. These fringes are plotted with normalised intensity in figure 4.16.a.i, for a time range of only 6 *ms* for better visibility.

On the right hand side, in figure 4.16.a.ii, the phase drift rate histogram of the interference fringes is shown, fitted to a normal distribution. To translate the intensity versus time measurement to phase drift rate, the intensity was changed to phase via equation 4.4 and then, the derivative with respect to time of each two consecutive phase points was calculated. Since drift is random it should have an equal weighting of values in either direction, explaining why the Gaussian is centred at around 0 $rad\ s^{-1}$. The width of the fitted curve, σ gives the average drift rate, which in this case is 8000 $rad\ s^{-1}$, while the range of the curve shows that the maximum drift rate observed is around 20000 $rad\ s^{-1}$.

The second measurement, where step 1 of the phase correction was applied (FPGA only), is depicted in figure 4.16.b.i, over a time range of 60 *s*, 10000 times longer than the free drift plot. This measurement was taken both with 25 μs and with 60 *ms* integration time. It

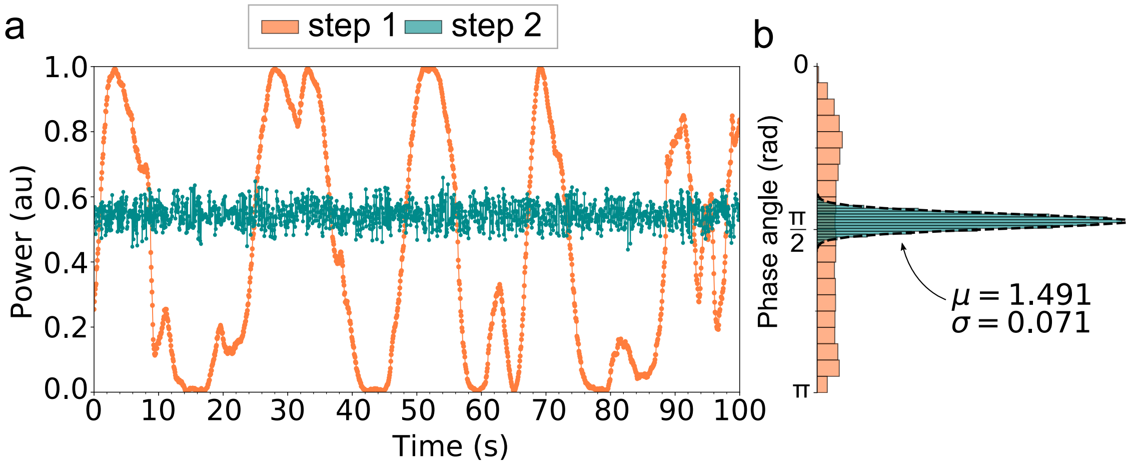

Figure 4.17 **Phase stabilised light in 602 km channels: a.** The interference fringes with step 2 of the stabilisation turned off (orange) are compared to the interference intensity of the fully stabilised signal channel (teal). The stability is demonstrated over 60 s. **b.** Intensity is translated into phase for both cases. The phase distribution of the semi-stabilised light (orange histogram) is flat, typical of a random interference. Instead, with the compensation fully in action, the stabilised lights can be fitted to a narrow Gaussian (teal histogram) with $\sigma = 0.07$ *rad* and centred near the $\frac{\pi}{2}$ locking condition.

was previously explained how the phase drift rate, after step 1 of the compensation may not decrease. This was indeed the case with our PID feedback. However, this rate was not the representative rate for the system since the induced drift from the locking did not negatively affect our QBER. This assumption will be discussed in the following paragraphs. Here, the 60 *ms* integration time measurement is shown, which hides the induced, small but rapid variations in the phase and shows solely the slow but significant leftover drift, a result of the wavelength difference between signal and reference.

With the introduction of step 1 of the correction, the range of the drift was reduced by three orders of magnitude, while the average drift rate by 16000 times to 0.5 $rad\ s^{-1}$. It was estimated in section 4.5.1 that the reduction would have been 1000 times rather than 16000 times. This can be explained by the fact that the integration time in the free drift measurement was 2400 times shorter than the step 1 measurement. The above two measurements confirm that step 1 of the stabilisation successfully decreases the rapid drift to a rate even slower than the one shown in section 4.4. Consequently, the slow stabilisation scheme implemented through step 2 should comfortably fully stabilise the channels so that their relative phase error is around 0 rad.

For the final measurement, with both step 1 and step 2 of the compensation synchronously acting on the light fields, the phase angle at interference becomes of interest. The fibre stretcher feedback was turned on with a repetition rate of 10-20 Hz. This measurement was taken with an integration time of 60 ms, to be directly comparable to the measurement taken with the semi-stabilised light. The results are summarised in figure 4.17. In figure 4.17.a, the interference fringes of the semi-stabilised system (orange) are fully suppressed and the lights is stabilised around the $\frac{\pi}{2}$ intensity locking condition (teal).

The phase angle histograms of both cases are plotted and compared in figure 4.17.b. As expected, the orange points give a flat distribution of phase with a slightly raised edge at 0 *rad* probably due to dark counts. Instead, the stabilised system shows a thin Gaussian centred around $\frac{\pi}{2}$ *rad* which was the pre-set value. The reason for the slight deviation is the fact that the locking point was manually adjusted as to provide the highest interference visibility and hence the lowest QBER. The standard deviation of the fitted Gaussian to the teal histogram is 0.07 *rad*. This value is less than half of the one obtained in the stabilisation of the short quantum interferometer in section 4.4.3. While the plotted measurement was taken at brighter signal light than what would actually be used in a TF-QKD implementation, it was repeated with SNSPDs at a flux of 0.2 photons/pulse, producing similar results. The improvement in the result is attributed to more accurate optimisation of the slow feedback parameters while it was also assisted by the fact that the leftover slow drift was usually 2 to 4 times slower than the drift we observed in the short interferometer experiment.

The main advantage that the new system has over the short interferometer feedback developed initially, is its ability to allow a strong intensity contrast between reference and signal channels. The DWDM technique gives access to a large photon sample in the first fast compensation step, which acts to reduce the phase drift to a rate that can be comfortably corrected with dim light by the second slow feedback. DWDM also ensures that contamination of the signal by the reference light does not occur up to an intensity contrast of around 40 dB. Moreover, active intensity modulation gives us the ability to modulate the reference pulses to the flux of the highest intensity state required by each protocol. Instead, in earlier experiments, the proof-of-principle approach of taking decoy and signal fluxes in separate measurements through a VOA rather than an intensity modulator, limited the reference flux to the value of the state measured in each round. In the case that the photon sample of the time-multiplexed reference pulses in the signal wavelength was not enough to produce decent results, the intensity modulators could be exploited further, to add an extra contrast between quantum reference pulses and quantum signal pulses.

4.6 Summary

This chapter provided background introduction as well as experimental details and results for the methods developed and used in the experiments described in chapter 3. The two experiments required the generation of indistinguishable WCPs from two distant sources, phase locked to a common reference and actively phase randomised. The proof-of-principle TF-QKD demonstration required the phase stabilisation of a short interferometer where the drift observed in the particular degree of freedom was in the radians per second regime. Instead, the realistic experiment performed over 605 km of fibre required fast phase correction of the quantum interferometer in the MHz regime.

To fulfil the requisites of the experiments, several techniques were developed. Firstly, the OIL technique was implemented to achieve strong spectral indistinguishability of the laser sources of two distinct users. OIL generated matching frequency combs and reduced the frequency chirp of the injected DFB lasers improving their individual visibilities to over 99.7%. Interference of the two slave lasers injected by the same master achieved 97.5% visibility, implying a small optical error of 1.25%. As a passive spectral control, it cancelled out any phase drift effects resulting from wavelength detuning. OIL was also used to show continuous phase randomisation as the slave lasers inherited in each cycle the random phase of their pulsed master.

Phase control was first devised for the proof-of-principle experiment to suppress slow drift using dim light. Feedback signals were sent to the DC bias of a phase modulator, after observing the interference fringes of the two lasers with the target of locking the intensity to a $\frac{\pi}{2}$ difference between the interfering pulses. The maximum attenuation over which this feedback was shown to be successful was 90 dB, where the leftover phase error distribution showed a satisfactory standard deviation of 0.4 rad from the target quadrature position.

The slow phase control scheme was used as the basis to develop a MHz repetition rate dual-band phase correction feedback. Such correction was achieved by wavelength multiplexing dim signal light with bright reference light. The interference of the bright light was used to suppress the initial rad/ms phase drift rate of the signal by three orders of magnitude. Leftover drift due to the 1.6 *nm* wavelength separation of the two light fields was corrected with the slow phase correction scheme described in the previous paragraph. This dual-band stabilisation achieved stable interference over 605 km of fibre, with the leftover error distribution showing a standard deviation of 0.07 rad. An impressive result as such could prove useful not solely for the implementation of TF-QKD but also for integration within repeaters, where stability should be maintained over long fibres.

Chapter 5

Future work

The work described in this thesis showed the path for the evolution of TF-QKD from theory to realisation. Although the developed setup has successfully demonstrated the feasibility of TF-QKD for quantum channels up to 600 km long, further work remains, to increase practicality and prove the protocol's potential in the real world. Experimental TF-QKD is an extremely novel area of research, thus, more fundamental research into an effective but simplified and agile setup is still required for further significant leaps to be made.

An obvious improvement to the setup described in this work would be the increase of the length of the OPLL duty fibre. If this system was to be deployed in a real network, the duty fibre would need to match the 600 km length of the quantum channel. There are significant problems arising from the implementation this step. If the duty fibre length surpasses the coherence length of the phase reference laser, the OPLL could potentially fail. A potential solution that could be examined is the insertion of an additional fibre spool, equal in length to the duty fibre connecting Alice and Bob, inside Alice's station. The target would be to achieve equal decoherence between the OPLL/QKD light arriving at Bob and the QKD light at Alice.

Although this technique is the most straightforward approach and should be looked into for research purposes, having such a long fibre inside the transmitter station would be inefficient and an unlikely approach for a deployable setup. It could also require expensive equipment such as an Erbium-doped fiber link amplifier. An alternative would be a time-frequency distribution system such as the one used in the 509 km TF-QKD paper [94]. Nevertheless, such systems are cost-inefficient and critically increase the complexity of the setup. It is hence improbable that real-life QKD networks will be based on such technologies in the near future.

The optimal solution would be the elimination of the need for a complex phase-locking system requiring an extra service fibre. Further research should therefore be focused on investigating and developing a locking mechanism based on side-band modulation. The main laser used for QKD would be rapidly modulated in phase to generate a side-band well separated from the central frequency. If the DWDM technique is employed, then the side-band can be kept at a much higher intensity than the quantum signal as they both travel down the same fibre. The bright light would then be used to phase-lock the laser sources of the two users, completely eliminating the requirement for a service fibre. Occupying a total of three DWDM channels, signal, phase reference and phase correction light fields will all travel side by side in the main quantum channels connecting Alice, Bob and Charlie.

While the work described in this thesis under development, the TF-QKD demonstrations in ref. [94, 93] showed an alternative approach to phase correction. The phase is tracked with the help of bright pulses so that QKD pulses are post-selected depending on their random phase. This reconciliation method can only be implemented with the SNS-TF-QKD and the PM-TF-QKD protocols. Although unable to implement other variants, it is an interesting solution to the fast phase-drift problem. Nevertheless, a major issue in their setup is the strong backwards re-Rayleigh scattering of the bright pulses which pollutes with noise the signal. This was the in fact limiting factor (in addition to dark counts) in the maximum distance achievable with their setup.

To avoid contamination of the signals while still utilising the practical phase reconciliation technique, a hybrid of the setup developed in this work and the setup in ref. [94] could be developed. Wavelength multiplexing would be used to keep the phase tracking reference pulses many orders of magnitude stronger than the signal, without however increasing the noise in the latter. The hybrid setup should allow the users to communicate at record distances, by eliminating the limiting factor of the post-selection approach. Additionally, the setup as described in this thesis, would be significantly simplified, not requiring active phase correction mechanisms.

Some of the simplest setups developed for QKD are based on direct light modulation by acting on the electrical bias of the laser sources set up in an OIL configuration. This was briefly mentioned in section 4.1.3. TF-QKD requires the following modulations: intensity modulation for the generation of decoy states, global active phase randomisation and bit encoding in phase. It is hence compelling to research whether the TF-QKD setup could be simplified by removing the phase and intensity modulators and use the OIL direct modulation approach instead. OIL with a pulsed master guarantees a random phase inherited by the slave which would fulfil the phase randomisation requirement. Especially in the case of the CAL-TF-QKD protocol, which does not require that the randomisation value is known, such an approach could be ideal. Intensity modulation can also take place directly in the pulse generation stage in a similar manner. As a result, most modulators will be removed, requiring less DC and AC generators and a smaller setup. If TF-QKD is to be commercialised in the future, direct modulation is definitely a tempting technique to be integrated within the setup.

One crucial and novel strength of the long-distance experiment described in section 3.2 was its multi-protocol potential. This characteristic could be further developed to improve the performance of the setup at shorter distances. While TF-QKD performs much better than any other practical protocol at long distances, it is evident, from the theoretical limit graphs in chapter 1, that the same does not apply to short distances. A real-life network will need to cover both long and short distances with optimal performance. An MDI-QKD setup has the same architecture as TF-QKD but evidently performs better at distances shorter than 200 km. Therefore, an agile setup able to switch between TF-QKD and MDI-QKD, depending on the channel losses, would be ideal and should be explored. MDI-QKD is usually done with polarisation encoding, however time-bin encoding is becoming increasingly popular. Time-bin and phase encoding are similar as they both represent information through the delay of optical pulses. Time-bin MDI-QKD and TF-QKD could potentially form a practical combination that requires no additional components.

The above improvements and alternative ways of carrying out TF-QKD can help exploit its full potential and diminish its experimental complexity so that it becomes a protocol, not only favoured by theorists, but also by experimentalists. The benefits of TF-QKD in terms of distance and key rate are highly desirable in commercial QKD. If the above improvements are successful it could render it as the universal protocol, guaranteeing optimal results while maintaining practicality.

Chapter 6

Conclusions

QKD has provided the answer for information-theoretic secure communications. Alice and Bob can use single photons or highly attenuated laser sources to encode and transfer information. A third party attempting to gain any knowledge of the information is guaranteed to cause a disturbance in the system detectable by the authorised users.

Nevertheless, due to the use of single photons or dim pulses, QKD is limited by channel losses. This limitation had set a theoretical bound, known as the SKC_0, that practical QKD protocols could not surpass, therefore decreasing the suitability of quantum communications for real-life applications, such as inter-city fibre networks. Successful implementations of point-to-point QKD have shown secure key exchanges over fibre links as long as 421 km, reaching close to the SKC_0, but only due to the use of extremely powerful single-photon detectors.

Protocols able to surpass the SKC_0 require complex quantum processes such as storing of quantum states and entanglement distribution, purification and swapping. For this reason, such protocols are not yet implementable and must await the successful advancement of these technologies. However, a recent protocol proposal, namely TF-QKD, promised to outperform the SKC_0 bound using only readily available technology. TF-QKD not only predicted readily achievable distances longer than 500 km but additionally guaranteed measurement device independent security. The protocol requires the phase-stable single-photon interference of distinct indistinguishable laser sources in a long interferometric setup. Hence, although it does not pose the need for future technologies, its practical realisation is highly challenging. Alice and Bob must produce indistinguishable pulses, locked to a common phase reference although separated by huge distances, and Charlie must extract accurate phase information after the pulses have travelled hundreds of kilometres in fibre, undergoing a drift in the order of tens of radians per millisecond.

Since the initial proposal, many TF-type variants have been published, each one aiming to benefit the protocol in different aspects. As a result, three main categories of variants have occurred. The first one includes variants very similar to the original TF-QKD, which require phase encoding and randomisation of all pulses, as well as phase reconciliation during sifting. The second class, includes protocols that pose no need for phase reconciliation since signal pulses are not phase randomised, such as the CAL-TF-QKD. Finally, the third category includes protocols where signal encoding is performed in intensity rather than phase, such as the SNS-TF-QKD. In this work, the security analysis of the three aforementioned protocols was developed on a common channel model to ease direct comparison and multi-protocol implementations.

It was indeed confirmed that the three variants excel in different conditions. TF-QKD in its original form, although a strong competitor in terms of loss tolerance and key rate, is only secure against collective attacks. Its implementation, with the requirement of phase randomisation and reconciliation of all pulses, is challenging. For the same reason and if the analysis was to be performed in the finite-size case with the optimal phase discretisation value of 16 slices, the acquisition time would be quite long. Given that the security is conditional, the TF-QKD protocol should solely be implemented to prove the feasibility of the protocol. It covers the most experimentally difficult case and hence its successful implementation encompasses the guaranteed potential of implementing the rest of them. Nevertheless, its implementation should be supported by information-theoretic secure protocols which will be useful in real-life applications.

Both the CAL-TF-QKD and the SNS-TF-QKD protocols are information-theoretically secure. Additionally, the CAL-TF-QKD protocol significantly eases practical implementations by removing the requirement for phase post-selection in the key distillation basis. It is also highly resilient to phase misalignment error, achieving positive secret key rates, at 100 km, for a misalignment error up to 26%. Due to the fact that no phase post-selection is required to distil a key, this protocol can surpass the SKC_0 at the lowest loss. Nevertheless, these benefits come at the cost of limited maximum loss, decreased by around 40 dB compared to TF-QKD.

The SNS-TF-QKD protocol has been shown to be the most tolerant to phase error (up to 38%) and is hence ideal for noisy systems. Since the encoding of the signals is performed in intensity, realistically it is expected to be less noisy in the key distillation basis than an equivalent system encoded in phase. No interference is required for a correct click in the key distillation basis, instead, solely a well performing intensity modulator is needed. SNS-TF-QKD is able to tolerate around 25 dB less loss in the quantum channels than the original proposal, given the specific parameters used in simulations and experiments in this work. However, this can be significantly increased if the protocol is combined with the TWCC post-processing technique. The latter adds an extra 15 dB to the maximum tolerated loss, making this protocol the clear winner in the long distance race of the unconditionally secure TF-type protocols.

The analyses were used to deduce a generalised protocol which if applied can encompass all variants with only slight changes. This protocol defines a proof-of-principle approach with the target of experimentally proving the feasibility of TF-QKD for the first time and its claim of outperforming the SKC_0. In this first experiment, distinct laser sources in each transmitter were locked together through an OPLL, in which Alice acts as a master. OIL was utilised at the sources, to carve short pico-second pulses with 2 GHz repetition rate, and decouple the light used for QKD from the light used for phase-locking. A separate servo fibre carried the latter. Phase randomisation was performed on all pulses through a phase modulator producing 2^5 different modulation levels. On top of the phase randomisation, phase encoding of four states was performed, $\left[0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\right]$. Decoy states were implemented in a proof-of-principle manner, in different runs, using variable optical attenuators. Channels were kept short in length, to minimise the phase drift rate, however their losses were varied as to simulate channels longer than 500 km.

A slow phase correction feedback was necessary, as phase drifted in the order of ten radians per second. The scheme developed to achieve accurate stabilisation of the phase was based on intensity monitoring of the single-photon interference fringes at Charlie. An SNSPD channel connected to a slow counter of minimum integration time of 10 ms, fed the monitored count rate to a PID control. An error signal was extracted, which aimed to lock the measured count rate to the $\frac{\pi}{2}$ interference intensity. This was then translated to a DC voltage and applied to the phase modulator at Bob's station. To achieve synchronous QKD and phase correction, phase encoded signal pulses were time-multiplexed with fully unmodulated reference pulses, with a duty cycle of 50%. The feedback was continuous and achieved accurate and prolonged locking of the sources at the single-photon level. With 90.8 dB losses in the quantum channels, an average QBER of 2.65% was obtained throughout the measurements.

The proof-of-principle demonstration showed the first quantum system able to achieve repeating behaviour and clearly proved that the gain of a TF-type system scales as the square

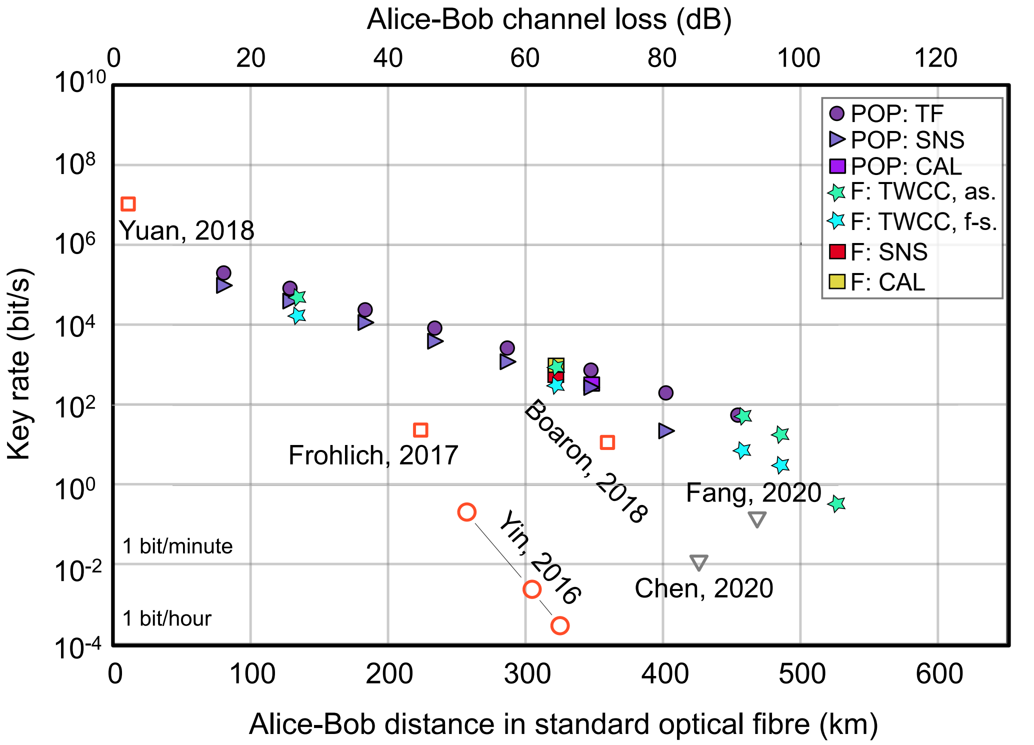

Figure 6.1 **Comparison of this work and current literature:** Secret key rate versus distance in standard optical fibre results obtained in this experiment and in previous state-of-art implementations. POP labelled points refer to the proof-of-principle results of section 3.1. F labelled points refer to the experiment of section 3.2, performed over real fibre channels. Empty markers represent previous record results obtained in QKD and TF-QKD.

root of the channel transmission, doubling up the maximum achievable distanc,e compared to an equivalent QKD system. In terms of key rate versus distance, the system was able to overcome the SKC_0 using all three different TF variants. The first points over the SKC_0 were acquired at 50 dB with the supremacy maintained up to 82 dB with SNS-TF-QKD and 90 dB with TF-QKD, when the respective key rates fall to zero. The overall maximum loss over which a positive key rate was obtained is equivalent to 567 km of ULL fibre. At the time of publication, this result exceeded the maximum losses previously shown in a QKD system by almost 20 dB, while using SNSPDs with dark counts two orders of magnitude higher. Comparing similar losses in the two experiments, the acquired key rate is three orders of magnitude higher.

The experiment was further developed into a more realistic version, where real long fibres comprised the quantum channels. As a result, the drift observed was increased by three orders of magnitude, to exceed 10 rad/ms at long distances. This demonstration targets not only to accurately stabilise such drifts in the quantum channel and achieve record distances but also to show an agile setup able to implement any TF variant previously explored and hence exploit the protocol's full potential. It was previously noted that the original TF-QKD proposal does not efficiently offer information-theoretic security, hence only the SNS-TF-QKD and CAL-TF-QKD protocols were implemented, while only the SNS-TF-QKD enhanced with TWCC was able to beat the current distance record of 509 km.

This setup included several improvements over the prototype. Long patterns were implemented to fairly sample decoy states and phase randomisation values which were both performed on-line in independent pseudorandom patterns for Alice and Bob. The OPLL was maintained but the phase stabilisation scheme was replaced by a novel dual-band phase control utilising wavelength multiplexing. Alice and Bob multiplex bright reference light with the signal light used for QKD, resulting in the two fields experiencing the same drifts on their trip to Charlie. For step one, Charlie isolates the bright fringes of the reference to generate a MHz correction signal through an FPGA, acting on a phase modulator and correcting both wavelengths. The reference is fully stabilised, while the signal drift is reduced by three orders of magnitude. Residue drift is slow and caused by the wavelength difference of the two fields. Nevertheless, it is corrected in step two by implementing the same stabilisation used in the prototype experiment, but acting on a fibre stretcher with isolated signal light passing through.

Using the above setup and the SNS-TWCC method, new record distances were reached, of 555 km in the asymptotic case and 605 km in the finite-size case. Real bits were extracted from TF-QKD for the first time, allowing the first true TWCC implementation rather than its estimation. To show the setup's multi-protocol potential, the CAL-TF-QKD protocol was implemented at 368 km. Figure 6.1 shows the results of the advanced setup in turquoise and blue stars for the SNS-TF-QKD with TWCC protocol in the asymptotic and finite-size regime respectively. On the same figure, the new results for SNS-TF-QKD without TWCC and for the CAL-TF-QKD protocol in the asymptotic regime are shown in red and yellow squares respectively.

All results obtained in this work are summarised in figure 6.1. The proof-of-principle results are shown in purple along previous record implementations (orange) and implementations occurring after their publication (gray). The key rates obtained from the advanced experiment are the latest record results in QKD, hence all depicted state-of-art results are data obtained before this experiment was performed. The advantage achieved in this work, in both distance (or attenuation) and key rate is evident.

The work in this thesis paved the way for an implementable TF-QKD system. Further work should focus on simplification of this setup. Servo fibres utilised throughout the experiment would ideally be fully eliminated by investigating an OPLL based on side-band modulation. In specific implementations where SNS-TF-QKD is ideal, it would additionally be beneficial to merge the DWDM scheme developed here with a phase-tracking method for post-selection rather than correction, as in [94]. Further simplifications that would decrease the size of the setup would be a direct intensity modulation for decoy states using OIL, while if the CAL-TF-QKD protocol is to be implemented, this solution could also apply to phase randomisation. Finally, given that TF-QKD performs worse than other protocols at short distances, an agile setup able to also accommodate protocols, such as time-bin MDI-QKD, should be developed.

With the above improvements on the setup, the system would be ideal for implementation in a quantum network with long channels, such as the one connecting Bristol to Cambridge and Cambridge to London. The latter channel could be extended using the fibre distributed along the channel between the UK and France to show the longest overseas in-fibre QKD. This would validate the claim that TF-QKD could be a practical and universal protocol for long distance quantum communications.

Bibliography

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

[2] M. Curty, K. Azuma, and H. K. Lo, “Simple security proof of twin-field type quantum key distribution protocol,” *npj Quantum Information*, vol. 5, pp. 1–6, dec 2019.

[3] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, “Twin-field quantum key distribution with large misalignment error,” *Phys. Rev. A*, vol. 98, p. 062323, Dec 2018.

[4] B. Marr, “How much data do we create every day? the mind-blowing stats everyone should read,” 2019.

[5] W. Diffie and M. E. Hellman, “Privacy and authentication: An introduction to cryptography,” *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397–427, 1979.

[6] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[7] J.-S. Coron, “What is cryptography?,” *IEEE Security & Privacy Magazine*, vol. 4, no. 1, pp. 70–73, 2006.

[8] H. Delfs and H. Knebl, *Symmetric-Key Cryptography*, pp. 11–48. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015.

[9] J. Daor, J. Daemen, and V. Rijmen, “Aes proposal: rijndael,” 10 1999.

[10] P. Mahajan and A. Sachdeva, “A study of encryption algorithms aes, des and rsa for security,” *Global Journal of Computer Science and Technology*, 2013.

[11] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[12] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[13] S. N. Molotkov, “Quantum cryptography and v a kotel’nikov’s one-time key and sampling theorems,” *Physics-uspekhi - PHYS-USP*, vol. 49, pp. 750–761, 07 2006.

[14] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, Jan 1926.

[15] M. Hellman, “An extension of the shannon theory approach to cryptography,” *IEEE Transactions on Information Theory*, vol. 23, pp. 289–294, May 1977.

[16] S. W., “Conjugate coding,” *SIGACT News*, vol. 15, pp. 78–88, Jan. 1983.

[17] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, p. 8, 1984.

[18] W. Heisenberg, “Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik,” *Zeitschrift für Physik*, vol. 43, pp. 172–198, Mar 1927.

[19] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, pp. 802–803, 1982.

[20] P. A. M. Dirac, “A new notation for quantum mechanics,” *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35, no. 3, p. 416–418, 1939.

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

[22] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Scientific Reports*, vol. 6, p. 19201, Jan 2016.

[23] Y.-C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, “Long-distance continuous-variable quantum key distribution over 202.81 km fiber,” 2020.

[24] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, “Continuous-variable QKD over 50 km commercial fiber,” *Quantum Science and Technology*, vol. 4, p. 035006, may 2019.

[25] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, “The first 0.14-db/km loss optical fiber and its impact on submarine transmission,” *J. Lightwave Technol.*, vol. 36, pp. 44–49, Jan 2018.

[26] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, “Secure quantum key distribution over 421 km of optical fiber,” *Phys. Rev. Lett.*, vol. 121, p. 190502, Nov 2018.

[27] D. Stucki, N. Walenta, F. Vannel, R. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250km of ultra low loss fibres," *New Journal of Physics*, vol. 11, Apr 2009.

[28] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[29] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[30] S. K. Liao, H. L. Yong, C. Liu, G. L. Shentu, D. D. Li, J. Lin, H. Dai, S. Q. Zhao, B. Li, J. Y. Guan, W. Chen, Y. H. Gong, Y. Li, Z. H. Lin, G. S. Pan, J. S. Pelc, M. M. Fejer, W. Z. Zhang, W. Y. Liu, J. Yin, J. G. Ren, X. B. Wang, Q. Zhang, C. Z. Peng, and J. W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics*, vol. 11, pp. 509–513, aug 2017.

[31] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000.

[32] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000.

[33] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, pp. 44–44, jul 2002.

[34] D. Gottesman, H. . Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pp. 136–, June 2004.

[35] T. Heindel, C. A. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter, M. Kamp, S. Reitzenstein, S. Höfling, P. Michler, H. Weinfurter, and A. Forchel, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New Journal of Physics*, vol. 14, p. 083001, aug 2012.

[36] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120km using ultrahigh purity single-photon source and superconducting single-photon detectors," *Scientific Reports*, vol. 5, pp. 1–7, sep 2015.

[37] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, Mar 1995.

[38] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug 2003.

[39] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, p. 230504, Jun 2005.

[40] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, p. 012326, Jul 2005.

[41] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, “Decoy-state quantum key distribution with biased basis choice,” *Scientific Reports*, vol. 3, 2013.

[42] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Phys. Rev.*, vol. 47, pp. 777–780, May 1935.

[43] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[44] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

[45] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[46] W. Tittel and G. Weihs, “Photonic entanglement for fundamental tests and quantum communication,” 2001.

[47] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photonics*, vol. 4, pp. 686–689, oct 2010.

[48] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, “After-gate attack on a quantum cryptosystem,” *New Journal of Physics*, vol. 13, p. 013043, jan 2011.

[49] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[50] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *npj Quantum Information*, vol. 2, no. 1, p. 16025, 2016.

[51] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[52] S. L. Braunstein and S. Pirandola, “Side-channel-free quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, p. 130502, Mar 2012.

[53] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers,” *Nature Photonics*, vol. 10, no. 5, pp. 312–315, 2016.

[54] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, “High-speed measurement-device-independent quantum key distribution with integrated silicon photonics,” 2019.

[55] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," *Optica*, vol. 7, pp. 238–242, Mar 2020.

[56] G.-Z. Tang, S.-H. Sun, H. Chen, C.-Y. Li, and L.-M. Liang, "Time-bin phase-encoding measurement-device-independent quantum key distribution with four single-photon detectors," *Chinese Physics Letters*, vol. 33, p. 120301, dec 2016.

[57] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A*, vol. 93, p. 042324, Apr 2016.

[58] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, Nov 1987.

[59] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, 2017.

[60] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," 2019.

[61] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Phys. Rev. A*, vol. 59, pp. 169–181, Jan 1999.

[62] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, pp. 722–725, Jan 1996.

[63] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, pp. 2818–2821, Sep 1996.

[64] S. Bose, V. Vedral, and P. L. Knight, "Purification via entanglement swapping and conserved entanglement," *Phys. Rev. A*, vol. 60, pp. 194–197, Jul 1999.

[65] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.

[66] S. N. Molotkov and I. V. Sinilshchikov, "Quantum key distribution through untrusted nodes: exact solution for single-photon states," *Laser Physics Letters*, vol. 16, p. 105205, sep 2019.

[67] D. N. Klyshko, A. N. Penin, and B. F. Polkovnikov, "Parametric Luminescence and Light Scattering by Polaritons," *Soviet Journal of Experimental and Theoretical Physics Letters*, vol. 11, p. 5, Jan. 1970.

[68] D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," *Phys. Rev. Lett.*, vol. 25, pp. 84–87, Jul 1970.

[69] N. Ohlsson, S. Kröll, and S. A. Moiseev, "Delayed single-photon self-interference — A double slit experiment in the time domain," in *Coherence and Quantum Optics VIII*, pp. 383–384, Springer US, 2003.

[70] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, pp. 3891–3894, May 1998.

[71] X.-s. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, "Experimental delayed-choice entanglement swapping," *Nature Physics*, vol. 8, no. 6, pp. 479–484, 2012.

[72] Q.-C. Sun, Y.-F. Jiang, Y.-L. Mao, L.-X. You, W. Zhang, W.-J. Zhang, X. Jiang, T.-Y. Chen, H. Li, Y.-D. Huang, X.-F. Chen, Z. Wang, J. Fan, Q. Zhang, and J.-W. Pan, "Entanglement swapping over 100&#x2009;&#x2009;km optical fiber with independent entangled photon-pair sources," *Optica*, vol. 4, pp. 1214–1218, Oct 2017.

[73] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, no. 7801, pp. 60–64, 2020.

[74] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Appl. Opt.*, vol. 35, pp. 1956–1976, Apr 1996.

[75] G. Ribordy, N. Gisin, O. Guinnard, D. Stuck, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial ingaas/inp avalanche photodiodes: Current performance," *Journal of Modern Optics*, vol. 51, no. 9-10, pp. 1381–1398, 2004.

[76] Z. Yuan, A. Sharpe, J. Dynes, A. Dixon, and A. Shields, "Multi-gigahertz operation of photon counting ingaas avalanche photodiodes," *Applied Physics Letters*, vol. 96, no. 7, 2012.

[77] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," *Applied Physics Letters*, vol. 91, no. 4, p. 041114, 2007.

[78] A. D. Semenov, G. N. Gol'tsman, and A. A. Korneev, "Quantum detection by current carrying superconducting film," *Physica C: Superconductivity*, vol. 351, no. 4, pp. 349 – 356, 2001.

[79] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," *Applied Physics Letters*, vol. 79, no. 6, pp. 705–707, 2001.

[80] J. Münzberg, A. Vetter, F. Beutel, W. Hartmann, S. Ferrari, W. H. P. Pernice, and C. Rockstuhl, "Superconducting nanowire single-photon detector implemented in a 2d photonic crystal cavity," *Optica*, vol. 5, pp. 658–665, May 2018.

[81] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, no. 3, pp. 210–214, 2013.

[82] H. Shibata, K. Fukao, N. Kirigane, S. Karimoto, and H. Yamamoto, "Snspd with ultimate low system dark count rate using various cold filters," *IEEE Transactions on Applied Superconductivity*, vol. 27, pp. 1–4, June 2017.

[83] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, Di Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, S. W. Nam, A. G. Kozorezov, M. D. Shaw, and K. K. Berggren, "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector," *Nature Photonics*, 2020.

[84] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," *Applied Physics Letters*, vol. 104, no. 2, p. 021101, 2014.

[85] H. Chen, Z.-Y. Zhou, A. J. J. Zangana, Z.-Q. Yin, J. Wu, Y.-G. Han, S. Wang, H.-W. Li, D.-Y. He, S. K. Tawfeeq, B.-S. Shi, G.-C. Guo, W. Chen, and Z.-F. Han, "Experimental demonstration on the deterministic quantum key distribution based on entangled photons," *Scientific Reports*, vol. 6, no. 1, p. 20962, 2016.

[86] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, no. 7410, pp. 185–188, 2012.

[87] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, "Entanglement distribution over a 96-km-long submarine optical fiber," *Proceedings of the National Academy of Sciences*, vol. 116, no. 14, pp. 6684–6688, 2019.

[88] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[89] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.*, vol. 119, p. 200501, Nov 2017.

[90] F. Kaneda, F. Xu, J. Chapman, and P. G. Kwiat, “Quantum-memory-assisted multi-photon generation for efficient quantum information processing,” *Optica*, vol. 4, pp. 1034–1037, Sep 2017.

[91] M. Rančić, M. P. Hedges, R. L. Ahlefeldt, and M. J. Sellars, “Coherence time of over a second in a telecom-compatible quantum memory storage material,” *Nature Physics*, vol. 14, no. 1, pp. 50–54, 2018.

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

[93] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, “Implementation of quantum key distribution surpassing the linear rate-transmittance bound,” *Nature Photonics*, 2020.

[94] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, “Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,” *Phys. Rev. Lett.*, vol. 124, p. 070501, Feb 2020.

[95] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, “Finite-key analysis for the 1-decoy state qkd protocol,” *Applied Physics Letters*, vol. 112, no. 17, p. 171104, 2018.

[96] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, “Long-distance quantum key distribution secure against coherent attacks,” *Optica*, vol. 4, pp. 163–167, Jan 2017.

[97] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, p. 190501, Nov 2016.

[98] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in vienna,” *New Journal of Physics*, vol. 11, p. 075001, jul 2009.

[99] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu,

T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, pp. 10387–10409, May 2011.

[100] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, p. 123001, dec 2011.

[101] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, p. 101, 2019.

[102] S. Koduru Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, Ž. Samec, L. Kling, A. Qiu, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted-node-free eight-user metropolitan quantum communication network," *arXiv e-prints*, p. arXiv:1907.08229, July 2019.

[103] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," *Nature*, vol. 564, no. 7735, pp. 225–228, 2018.

[104] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Communications*, vol. 8, no. 1, p. 13984, 2017.

[105] W. Geng, C. Zhang, Y. Zheng, J. He, C. Zhou, and Y. Kong, "Stable quantum key distribution using a silicon photonic transceiver," *Opt. Express*, vol. 27, pp. 29045–29054, Sep 2019.

[106] T. K. Paraïso, I. de Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," *npj Quantum Information*, vol. 5, no. 1, p. 42, 2019.

[107] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," 2019.

[108] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, and D. Bitauld, "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Express*, vol. 25, pp. 6784–6795, Mar 2017.

[109] G. Mélen, P. Freiwang, J. Luhn, T. Vogl, M. Rau, W. Rosenfeld, and H. Weinfurter, "Handheld quantum key distribution," in *Conference on Lasers and Electro-Optics*, p. FTu3G.1, Optical Society of America, 2018.

[110] P. Xu, Y. Ma, J.-G. Ren, H.-L. Yong, T. C. Ralph, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, X. Han, H.-N. Wu, W.-Y. Wang, F.-Z. Li, M. Yang, F.-L. Lin, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, Y. Chen, J. Fan, C.-Z. Peng, and J.-W. Pan, "Satellite testing of a gravitationally induced quantum decoherence model," *Science*, vol. 366, no. 6461, pp. 132–135, 2019.

[111] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018.

[112] G. B. Xavier, T. R. Da Silva, G. P. Temporão, and J. P. Von Der Weid, "Polarisation drift compensation in 8 km-long mach-zehnder fibre-optical interferometer for quantum communication," *Electronics Letters*, vol. 47, pp. 608 –609, May 2011.

[113] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, p. 021046, Jun 2019.

[114] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," *Phys. Rev. Applied*, vol. 11, p. 034053, Mar 2019.

[115] J. Lin and N. Lütkenhaus, "Simple security analysis of phase-matching measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 98, p. 042332, Oct 2018.

[116] F. Grasselli and M. Curty, "Practical decoy-state method for twin-field quantum key distribution," *New Journal of Physics*, vol. 21, jul 2019.

[117] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, "Sending-or-not-sending twin-field quantum key distribution in practice," *Scientific reports*, vol. 9, no. 1, p. 3080, 2019.

[118] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, "Improved results for sending-or-not-sending twin-field quantun key distribution: breaking the absolute limit of repeaterless key rate," 2019.

[119] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," 2018.

[120] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," *Phys. Rev. Lett.*, vol. 93, p. 120501, Sep 2004.

[121] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, "Limitations on quantum key repeaters," *Nature Communications*, vol. 6, no. 1, p. 6908, 2015.

[122] J. c. v. Minář, H. de Riedmatten, C. Simon, H. Zbinden, and N. Gisin, "Phase-noise measurements in long-fiber interferometers for quantum-repeater applications," *Phys. Rev. A*, vol. 77, p. 052325, May 2008.

[123] S.-B. Cho and T.-G. Noh, "Stabilization of a long-armed fiber-optic single-photon interferometer," *Opt. Express*, vol. 17, pp. 19027–19032, Oct 2009.

[124] G. B. Xavier and J. P. von der Weid, "Stable single-photon interference in a 1 km fiber-optic mach–zehnder interferometer with continuous phase adjustment," *Opt. Lett.*, vol. 36, pp. 1764–1766, May 2011.

[125] M. E. Grein, M. L. Stevens, N. D. Hardy, and P. B. Dixon, "Stabilization of long, deployed optical fiber links for quantum networks," in *Conference on Lasers and Electro-Optics*, p. FTu4F.6, Optical Society of America, 2017.

[126] O. Terra, G. Grosche, K. Predehl, R. Holzwarth, T. Legero, U. Sterr, B. Lipphardt, and H. Schnatz, "Phase-coherent comparison of two optical frequency standards over 146 km using a telecommunication fiber link," *Applied Physics B*, vol. 97, no. 3, p. 541, 2009.

[127] V. Ferrero and S. Camatel, "Optical phase locking techniques: an overview and a novel method based on single side sub-carrier modulation," *Opt. Express*, vol. 16, pp. 818–828, Jan 2008.

[128] K. Balakier, L. Ponnampalam, M. J. Fice, C. C. Renaud, and A. J. Seeds, "Integrated semiconductor laser optical phase lock loops," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 24, pp. 1–12, Jan 2018.

[129] S. Naresh, W. Liang, and A. Yariv, "Coherence cloning using semiconductor laser optical phase-lock loops," *Quantum Electronics, IEEE Journal of*, vol. 45, pp. 755 – 761, 08 2009.

[130] 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," *J. Lightwave Technol.*, vol. 17, p. 328, Feb 1999.

[131] J. M. Kahn, "1 gbit/s psk homodyne transmission system using phase-locked semiconductor lasers," *IEEE Photonics Technology Letters*, vol. 1, pp. 340–342, Oct 1989.

[132] A. C. Bordonalli, B. Cai, A. J. Seeds, and P. J. Williams, "Generation of microwave signals by active mode locking in a gain bandwidth restricted laser structure," *IEEE Photonics Technology Letters*, vol. 8, pp. 151–153, Jan 1996.

[133] I. C. Chang, "Acoustooptic devices and applications," in *Handbook of Optics: devices, measurements and properties* (M. Bass, ed.), vol. 2, ch. 12, pp. 12.1 – 12.54, New York, USA: McGraw-Hill, 2 ed., Apr 1993.

[134] M. Bennett, M. F. Schatz, H. Rockwood, and K. Wiesenfeld, "Huygens's clocks," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 458, no. 2019, pp. 563–579, 2002.

[135] R. H. Pantell, "The laser oscillator with an external signal," *Proceedings of the IEEE*, vol. 53, no. 5, pp. 474–477, 1965.

[136] H. L. Stover and W. H. Steier, "Locking of laser oscillators by light injection," *Applied Physics Letters*, vol. 8, no. 4, pp. 91–93, 1966.

[137] C. L. Tang and H. Statz, "Phase–locking of laser oscillators by injected signal," *Journal of Applied Physics*, vol. 38, no. 1, pp. 323–324, 1967.

[138] C. J. Buczek, R. J. Freiberg, and M. L. Skolnick, "Laser injection locking," *Proceedings of the IEEE*, vol. 61, no. 10, pp. 1411–1431, 1973.

[139] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," *Optics express*, vol. 24, no. 16, pp. 17849–17859, 2016.

[140] T. K. Paraïso, I. de Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," *npj Quantum Information*, vol. 5, no. 1, p. 145, 2019.

[141] R. H. Kingston, *Optical sources, detectors, and systems: Fundamentals and applications / Robert H. Kingston.* Optics and photonics series, San Diego and London: Academic Press, 1995.

[142] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, "Directly phase-modulated light source," *Physical Review X*, vol. 6, no. 3, p. 325, 2016.

[143] J. C. Cartledge and R. C. Srinivasan, "Extraction of dfb laser rate equation parameters for system simulation purposes," *Physical Review A*, vol. 15, no. 5, pp. 852–860, 1997.

[144] I. Fatadin, D. Ives, and M. Wicks, "Numerical simulation of intensity and phase noise from extracted parameters for cw dfb lasers," *IEEE Journal of Quantum Electronics*, vol. 42, no. 9, pp. 934–941, 2006.

[145] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, "A direct ghz-clocked phase and intensity modulated transmitter applied to quantum key distribution," *Quantum Science and Technology*, vol. 3, no. 4, p. 045010, 2018.

[146] T. Biswas, M. Garcia Diaz, and A. Winter, "Interferometric visibility and coherence," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 473, p. 20170170, jul 2017.

Appendix A

Detailed data

A.1 Results of section 3.1

Phase randomised		
Flux	Gain (1 detector) ($\times 10^{-6}$)	
uu	1.71	
vv	18.2	
ww	0.026	
uv	8.77	
uw	0.913	
vw	8.74	
Encoded		
Flux	Gain ($\times 10^{-6}$)	QBER %
uu	1.79	2.65

Table A.1 **CAL-TF-QKD data:** Measured quantities for the protocol in ref. [2]. At 71.1 dB channel loss it provides a SKR of 270.7 bit/s, which is 2.42 times above the ideal SKC$_0$ bound at the same attenuation (112.0 bit/s). The flux set by each user was $u_a = u_b = 0.02$ photons per pulse for the signal states and $v_a = v_b = 0.2$ photons per pulse for the decoy states. The total vacuum was set to $w = 10^{-5}$.

Alice → Charlie		Bob → Charlie		Alice & Bob → Charlie			Secret key rate		
Attenuation	Gain	Attenuation	Gain	Attenuation	Gain	QBER	ref. [1]	ref. [3]	SKC$_0$
(dB)	($\times 10^{-6}$)	(dB)	($\times 10^{-6}$)	(dB)	($\times 10^{-6}$)	%		($\times 10^3$) bit/sec	
10.7	3000.8	10.8	3149.9	21.5	5562.8	2.29	159	74.5	10,250
	1154.4		1228.7		2172.4	2.20			
15.3	993.4	15.2	985.8	30.5	1984.0	1.79	66.1	30.4	1,286
	382.2		388.3		765.7	1.96			
20.4	301.1	20.3	293.8	40.7	592.1	1.87	19.2	8.86	122.8
	117.2		117.0		233.4	1.99			
25.1	95.4	25.0	100.4	50.1	195.6	1.73	6.71	3.03	14.10
	37.2		39.3		76.2	1.83			
30.0	30.2	29.9	63.4	61.7	61.6	1.75	2.14	0.933	1.476
	12.1		12.0		24.6	1.71			
35.6	8.74	35.5	9.44	71.1	18.2	1.86	0.602	0.213	0.112
	3.48		3.72		7.19	1.97			
40.6	2.84	40.6	2.86	81.2	5.65	2.10	0.163	0.0176	0.011
	1.14		1.20		2.32	2.40			
45.4	0.91	45.4	0.91	90.8	1.79	2.65	0.045	-	0.001
	0.353		0.368		0.72	3.57			

Table A.2 **TF-QKD and SNS-TF-QKD data:** Numerical data for the main experiment using the OPLL, with the TF-QKD protocols in refs. [1, 3]. 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 D1 in Fig. 1a when only Alice, only Bob or 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 was $u_a = u_b = 0.2$ photons per pulse for the signal states and $v_a = v_b = 0.08$ photons per pulse for the decoy states. The total vacuum is set to $w = 10^{-5}$.

A.2 Results of section 3.2

The experimental results obtained for the different variations of the SNS-TF-QKD protocol are presented below. Table A.3 shows the results for SNS-TF-QKD in the asymptotic regime. The SNS-TF-QKD protocol with TWCC results are presented in tables A.4 and A.5 for the asymptotic and finite-size regime respectively. Channel distances as well as the total number of signal pulses sent, N0, are shown in all tables. Errors from all the possible bases and intensities are also shown along with the extracted secret key rate (SKR) for every tested distance. For comparison, the relative secret key capacity (SKC_0) is also given. In the tables, the number of pulses sent for every pulse-pair combination is not explicitly stated but can be directly calculated by multiplying the probabilities given in tables 3.4 and 3.5 by N0. Nevertheless, the detections of every pulse-pair combination are given in the format $B_A B_B s_A s_B$, where B_A (B_B) denotes the basis chosen by Alice (Bob) and s_A (s_B) the state prepared by Alice (Bob). TWCC relevant quantities are also listed where appropriate.

Table A.3 **SNS-TF-QKD data in the asymptotic regime:** Experimental results for 368.7 km fibre channels.

SNS-TF-QKD, asymptotic	
Fibre length (km)	368.702
Number of slices (M)	16
Total pulses sent (N0)	2.066 x 10^{11}
E_Z	6.59%
$E_{X_{uu}}$	3.29%
$E_{X_{vv}}$	3.87%
e_1^X	4.15%
SKR (bits/signal)	1.098 x 10^{-6}
SKR (bits/second)	5.492 x 10^{2}
SKC_0 (bits/signal)	7.151 x 10^{-7}
SKR over SKC_0 ratio	1.54
Detections	
D_0	4887891
D_1	4624363
ZZss	39403
ZZsn	314309
ZZns	304872
ZZnn	4264
ZXsu	217790

ZXsv	121824
ZXsw	112334
ZXnu	1729304
ZXnv	173107
ZXnw	1634
XZus	217780
XZun	1786996
XZvs	117638
XZvn	155240
XZws	113964
XZwn	1486
XXuu	1240351
XXuv	685682
XXuw	643480
XXvu	668424
XXvv	115296
XXvw	55695
XXwu	628786
XXwv	62043
XXww	552
XXuu matching (D0)	79037
XXuu matching (D1)	74844
XXuu matching (D0)	76474
XXuu matching (D1)	72352
ZZ errors	43667
ZZ correct	619181

Table A.4 **SNS-TF-QKD with TWCC data in the asymptotic regime:** Experimental results for channels up to 605.17 km in length.

SNS-TF-QKD with TWCC, asymptotic					
Fibre length (km)	153.282	368.702	521.982	555.172	605.17
Number of slices (M)	16	16	16	16	16
Total pulses sent (N0)	5.296×10^{10}	1.527×10^{11}	5.208×10^{11}	2.554×10^{11}	1.002×10^{12}
Raw key, odd pairs	3.522×10^{6}	2.277×10^{5}	3.968×10^{4}	9.565×10^{3}	1.369×10^{4}
Raw key, even pairs, 00	1.938×10^{6}	1.228×10^{5}	2.162×10^{4}	5.174×10^{3}	7.411×10^{2}
Raw key, even pairs, 11	1.74×10^{6}	$6\ 1.15 \times 10^{5}$	1.963×10^{4}	4.725×10^{3}	6.575×10^{3}
Raw key, error pairs	1.591×10^{5}	1.039×10^{4}	2.096×10^{3}	5.532×10^{2}	1.029×10^{3}
E_Z before TWCC	13.1%	13.1%	14.0%	14.6%	16.4%

E_Z after TWCC	2.21%	2.23%	2.59%	2.84%	3.72%
$E_{X_{uu}}$	2.8%	3.21%	3.86%	3.68%	3.5%
$E_{X_{vv}}$	5.53%	6.32%	4.78%	8.33%	13.6%
e_1^X	5.68%	6.4%	3.71%	6.08%	2.31%
SKR (bits/signal)	7.441 x 10^{-5}	1.412 x 10^{-6}	8.557 x 10^{-8}	2.838 x 10^{-8}	1.937 x 10^{-9}
SKR (bits/second)	3.721 x 10^{4}	7.059 x 10^{2}	4.278 x 10^{1}	1419 x 10^{1}	9.685 x 10^{-1}
SKC$_0$ (bits/signal)	3.456 x 10^{-3}	7.151 x 10^{-7}	1.711 x 10^{-9}	4.632 x 10^{-10}	6.511 x 10^{-11}
SKR over SKC$_0$ ratio	0.0215	1.97	50.0	61.3	29.7
Detections					
D_0	69221704	4524664	795437	193156	278746
D_1	66051719	4241991	745698	181085	263766
ZZss	2423210	156953	27876	6727	9620
ZZsn	8146041	521082	91891	22168	32219
ZZns	8052039	526583	91497	22122	31538
ZZnn	11389	1380	2024	848	2907
ZXsu	6196623	403188	70879	17076	24785
ZXsv	3217021	205870	36367	8629	12876
ZXsw	3107274	198690	35299	8610	12320
ZXnu	20581340	1349062	235655	57121	81690
ZXnv	604012	37884	7635	1915	3125
ZXnw	4212	518	747	289	1085
XZus	6202770	403207	70119	17168	24722
XZun	20928197	1340008	236339	57217	82636
XZvs	3181382	208453	36111	8811	12607
XZvn	628269	41662	7104	1879	3037
XZws	3078177	202140	35286	8426	12396
XZwn	4250	534	765	281	1102
XXuu	15759404	1022280	179333	43000	61766
XXuv	8202418	526279	92761	22151	32573
XXuw	7977865	511560	89706	21900	31585
XXvu	8127297	531576	92456	22577	31672
XXvv	480868	30579	5527	1427	1904
XXvw	247965	16325	2809	799	1182
XXwu	7874039	516027	89699	22269	31572
XXwv	235716	14614	2968	718	1170
XXww	1645	201	282	113	423
XXuu matching (D0)	990284	64565	11389	2746	3939
XXuu matching (D1)	930327	59658	10558	2581	3712

XXuu matching (D0)	961135	62388	10921	2653	3789
XXuu matching (D1)	905683	57844	10179	2478	3594
ZZ errors	2434599	158333	29900	7575	12527
ZZ correct	16198080	1047665	183388	44290	63757

Table A.5 **SNS-TF-QKD with TWCC data in the finite-size regime:** Experimental results for channels up to 555.172 km in length.

SNS-TF-QKD with TWCC, finite-size				
Fibre length (km)	153.282	368.702	521.982	555.172
Number of slices (M)	16	16	16	16
Total pulses sent (N0)	6 x 10^{11}	2.435 x 10^{12}	3.07 x 10^{12}	3.536 x 10^{12}
Raw key, odd pairs	4.164 x 10^{7}	3.564x 10^{6}	2.333 x 10^{5}	1.336 x 10^{5}
Raw key, even pairs, 00	2.135 x 10^{7}	1.838 x 10^{6}	1.198 x 10^{5}	6.922 x 10^{4}
Raw key, even pairs, 11	2.077 x 10^{7}	1.768 x 10^{6}	1.152 x 10^{5}	6.501 x 10^{4}
Raw key, error pairs	5.738 x 10^{5}	4.938 x 10^{4}	4.542 x 10^{3}	3.103 x 10^{3}
E_Z before TWCC	7.67%	7.69%	9.01%	9.77%
E_Z after TWCC	0.685%	0.689%	0.97%	1.16%
$E_{X_{uu}}$	2.69%	2.88%	2.87%	3.47%
$E_{X_{vv}}$	3.56%	3.81%	5.31%	5.09%
e_1^X	4.16%	4.47%	6.04%	5.59%
Secure bits generated	1.707 x 10^{7}	1.329 x 10^{6}	4.046 x 10^{4}	1.745 x 10^{4}
SKR (bits/signal)	2.846 x 10^{-5}	5.459 x 10^{-7}	1.318 x 10^{-8}	4.937 x 10^{-9}
SKR (bits/second)	1.423 x 10^{4}	2.729 x 10^{2}	6.59	2.468
SKC_0 (bits/signal)				
SKR over SKC_0 ratio	0.00823	0.763	7.7	10.7
Detections				
D_0	623261177	54266217	3616047	2071809
D_1	601407532	50532067	3317070	1945930
ZZss	14322977	1229675	80689	46061
ZZsn	90153430	7739935	511622	296484
ZZns	90035335	7685653	507468	290238
ZZnn	642059	54944	20176	17462
ZXsu	25714805	2199489	144929	82891
ZXsv	46330397	3956642	262219	150458
ZXsw	12870272	1107377	72977	42765
ZXnu	159718589	13637478	898693	517464
ZXnv	90956994	7710475	507227	297300
ZXnw	93804	7989	2973	2550

XZus	25704406	2209257	146032	85067
XZun	159575781	13695784	906734	526484
XZvs	46091214	3944702	259209	149050
XZvn	89990485	7718247	507676	294097
XZws	12982067	1109205	73179	42204
XZwn	92445	7776	2977	2516
XXuu	44724005	3838050	252841	145782
XXuv	82278922	7047247	466076	270776
XXuw	22992576	1978960	131444	75985
XXvu	82116355	7042214	463506	268561
XXvv	78177798	6684280	437657	252988
XXvw	13010771	1116305	73487	42281
XXwu	22952199	1964545	129678	75082
XXwv	13127709	1110997	73238	42795
XXww	13314	1058	410	398
XXuu matching (D0)	2880087	250202	16753	9609
XXuu matching (D1)	2822546	239368	15656	9148
XXuu matching (D0)	2805790	243186	16263	9260
XXuu matching (D1)	2743311	232285	15215	8846
ZZ errors	14965036	1284619	100865	63523
ZZ correct	180188765	15425588	1019090	586722