

Experimental Development of a Polarisation-Entanglement System for Application in Real-World Quantum Communications

Karolina Petra Schatz

Doctor of Philosophy

University of York

Physics, Engineering and Technology

March 2026

Abstract

Quantum Key Distribution (QKD) is an emerging technology that enables secure data encryption by basing key generation on the transmission of quantum states rather than computational complexity, thereby anchoring security in the laws of physics and offering resilience against quantum computing attacks. Current research efforts focus on transitioning QKD from laboratory-based demonstrations to real-world deployment, thereby establishing it as a practical communication technology. Quantum entanglement plays a central role in QKD by enabling robust security assurance and providing a path towards scalable quantum networks.

This thesis presents a polarisation-entanglement system designed for operation in practical research scenarios, comprising state preparation from a commercial source, transmission, reception and data analysis. The system's capabilities are demonstrated through measurement of polarisation correlation visibility, violation of CHSH-type inequalities, and quantum state tomography, culminating in the generation of the first discrete-variable secret key generated within the Experimental Quantum Communication Group at the University of York.

Using the developed system, the integration of quantum communication into existing information infrastructure is experimentally investigated in two distinct scenarios. First, the coexistence of quantum and classical signals in the shared optical fibre is explored in the context of a White Rabbit time-distribution system, recovering entanglement visibilities above 96% over co-propagation distances of up to 1 km. Second, the transmission of photon pairs from the entanglement source is demonstrated over a 224 km deployed submarine fibre link, connecting the UK and Ireland used for classical data traffic. Together, these efforts provide a versatile, robust research tool for future experimental studies of polarisation-based QKD and demonstrate the viability of integrating quantum communication into existing optical infrastructure, paving the way for practical QKD systems.

Author's Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for a degree or other qualification at this University or elsewhere. All sources are acknowledged as references.

The work presented in Chapter 5 is based on the publication: K. P. Schatz, B. Amies-King, S. Albosh, R. Kumar, M. Lucamarini, "Practical single-fibre network-oriented quantum key distribution from a compact source of entangled photons in presence of White Rabbit time synchronisation," Proc. SPIE 12335, Quantum Technology: Driving Commercialisation of an Enabling Science III, 123350F (11 January 2023); <https://doi.org/10.1117/12.2647691> [1]. The experimental design, implementation, and analysis were carried out primarily by the author of this thesis, with the co-authors providing supervision, guidance, and feedback on the research and manuscript.

The work presented in Chapter 6 includes results published in: Amies-King, B.; Schatz, K.P.; Duan, H.; Biswas, A.; Bailey, J.; Felvinti, A.; Winward, J.; Dixon, M.; Minder, M.; Kumar, R.; et al. Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link. Entropy 2023, 25, 1572. <https://doi.org/10.3390/e25121572> [2]. The experimental design, implementation, and analysis presented in this thesis were carried out primarily by the author, with contributions from the co-authors including supervision, experimental assistance during the field trial, and feedback on the research and manuscript. The only exception is the characterisation of the Rockabill-link time-dependent polarisation stability, which was performed primarily by Mr Haofan Duan, with assistance from the author.

Acknowledgments

I would like to thank,

My family, for supporting me in chasing my dreams. I could not have done this without you, and I cherish every holiday that I can come back to see you all.

My supervisor, Professor Marco Lucamarini. Few supervisors know exactly how to support each student in just the way that they need. I consider myself very lucky to have come to York and learnt from one of the best.

My group, especially Ben Amies-King, Ry Render, Ormond Taylor, Emma Tien Hwai Medlock, Haofan Duan, Jennifer Bartlett, Panos Papanastasiou, Sophie Albosh, and Igor Konieczniak, for providing me with camaraderie and much useful collaboration. I can hardly imagine another group that feels so welcoming and supportive.

My friends, especially Caitlin Cunningham, Emma Tien Hwai Medlock, and Ormond Taylor. I do not think that I would have survived this PhD without a tea or (decaf) coffee and a jest every now and then, not to mention all the heart-to-hearts we have had over these years. Also, Alex Piasente, whose friendship brought me to the UK in the first place and gave me the courage to grow.

My teachers, especially Frau Stefanie Bertsch, who insisted I do not let any silly obstacles stop me from applying for a certain MINT programme. Not only has she been a mentor throughout my early scientific education, her tenacity in giving her students every possible opportunity to go further is what put me on my path as a scientist.

My thesis advisors and examiners, Professor Tim Spiller, Professor Sarah Thompson, and Dr Deirdre Kilbane, whose advice has been invaluable.

The Quantum Communications Hub, for funding this position, and Dr Georgia Mortzou, for always thinking of me when opportunities arose to engage in outreach, communicating, and putting up workshops.

Finally, my dearest Brendan. There are not enough words to express all the things you do for me, and even fewer to express how much you mean to me. None of this would have been possible without you.

Contents

1	Introduction	13
1.1	Quantum Cryptography	14
1.1.1	Classical Encryption	14
1.1.2	Quantum Key Distribution (QKD)	14
1.1.3	Qubit Definition & Notation	15
1.1.4	The BB84 Protocol	16
1.1.5	Entanglement in Quantum Cryptography	17
1.2	Current State of the Art and Challenges in QKD	20
1.2.1	Key Generation Rate-Distance Limitation	20
1.2.2	Security Assurance & Quantum Hacking	21
1.2.3	Real-World Deployment & Standardisation	22
1.2.4	Current Quantum Networks & Initiatives	24
1.3	Thesis Overview	26
2	Instrument Characterisation	27
2.1	Single Photon Avalanche Diodes	28
2.1.1	Photon Detection Efficiency	28
2.1.2	Dark Count Rates	30
2.1.3	Timing Jitter	31
2.1.4	Detector Gate Profile	32
2.2	Superconducting Nanowire Single Photon Detectors	34
2.3	Entangled Pair Source	35
2.3.1	Wavelength Spectrum	37
2.3.2	CAR & Heralding Efficiency	38
2.3.3	Single Photon Quality	40
2.3.4	Intensity Stability	42
2.4	Software Development	43
2.4.1	Time Tagger Analysis Code	43
2.4.2	Rotating Waveplate Controls	44
3	Developing a QKD Receiver	47
3.1	Polarisation Analyser Requirements	48
3.2	Fibre-Centric Measurement of Polarisation States	48
3.3	Polarisation State Collapse in Free Space	50
3.4	Dual Polarisation Output and Motorised Waveplates	51
3.5	Passive Basis Selection for QKD	54

3.6	Detection Output Time-Multiplexing	56
3.7	Passive Receiver Characterisation	58
3.7.1	Coupling Efficiency/Attenuation	58
3.7.2	Setup Stability	59
4	Polarisation Entanglement System for Quantum Key Distribution	61
4.1	Experimental Setup	62
4.2	Visibility of Polarisation Correlations	63
4.3	Polarisation Correlation Curves	64
4.4	CHSH-Inequalities and Bell-Violation under Restricted Polarisation Manipulation	67
4.5	Quantum State Tomography	69
4.5.1	Tomographic Method	70
4.5.2	Measurement Results	70
4.5.3	Maximum Likelihood Estimation	71
4.6	Entanglement-based QKD	74
4.6.1	Measured QBER and Secret Key fraction	74
4.6.2	Distance Scaling	76
4.6.3	Post-Processing and Distillation of a Secret Key	79
5	Entanglement Distribution in Shared Fibre Infrastructure	81
5.1	White Rabbit Time-Synchronisation and QKD	81
5.2	Quantum and Classical Coexistence – Experimental Setup	83
5.3	Entanglement Visibility Results	85
5.4	Conclusion & Future Work	87
6	Feasibility of Entanglement-Based Quantum Communications over a 224 km Undersea Optical Fibre Link	89
6.1	The UK-Ireland Feasibility Study	90
6.2	Laboratory-Based Channel Emulation	92
6.3	Dark Fibre Noise Level	93
6.4	Polarisation Stability	95
6.5	Distribution of Photon Pairs from a Source of Polarisation Entanglement . . .	95
6.6	Underwater Polarisation-Stability Study	97
6.7	Conclusions & Future Work	99
7	Conclusion & Future Work	101
A	Phase Difference in the $\Phi_{\varphi}^{+}\rangle$ Bell-State	103
B	Derivation of CHSH-Inequalities for Specific Waveplate Transformations	109

List of Tables

1.1	Basis specific notation for qubits and polarisation based single photon states .	16
2.1	SPAD models acquired for the EQC group	28
2.2	Numerical comparison of SPAD gate length at FWHM	33
2.3	Maximum relative detection efficiency difference for equivalent SPADs	33
2.4	SNSPD detection efficiency per channel	35
3.1	Visibilities of polarisation correlations in first Bell test	50
3.2	Fibre lengths and resulting time delta between different PA outputs	56
3.3	Coupling efficiencies and insertion losses for both PAs	59
4.1	PA waveplate positions to project into the three Pauli bases	63
4.2	CHSH measurement angles, theoretical Bell-state violation and measurement results for all PA HWP and QWP combinations	69
4.3	Possible PA settings for BBM92	74
6.1	Approximate CAR and coincidence peak widths observed during the laboratory emulation of the Rockabill link	92

List of Figures

1.1	Schematic representation of the BB84 protocol and the BBM92 protocol . . .	19
1.2	Schematic representation of the communication layers in a quantum secured network	23
2.1	Schematic representation of the experimental setup used to determine the SPAD detection efficiency via the substitution method	29
2.2	Measured detection efficiencies for the IDQubes, PDM-IRs, and ID220s	29
2.3	DCR against detector dead time for the IDQubes, PDM-IRs, and ID220s . . .	30
2.4	Examples of convoluted SPAD timing jitter	31
2.5	SPAD gate shape visualisation at different detection efficiencies	32
2.6	SPAD gate shape comparison of equivalent detectors at identical settings . . .	33
2.7	SNSPD dark count rate under different environmental conditions	35
2.8	Schematic representation of SPDC and associated conservations	36
2.9	Schematic representation of the EPS	36
2.10	Wavelength spectrum of the entangled pairs emitted by the EPS	37
2.11	CAR dependency on EPS emission rate	39
2.12	Coincidence rate and heralding efficiency of the EPS in relation to pump power	39
2.13	Schematic representation of the EPS's $g^{(2)}$, based on a HBT-interferometer . .	40
2.14	Second-order correlation function ($g^2(\tau)$) of the EPS	41
2.15	EPS count rate stability over a 24 hour period	42
2.16	EPS coincidence rate and thermistor voltage during warm-up	43
2.17	Schematic representation of long measurements utilising the MultiHarp and Python scripts	45
3.1	Schematic representation of the first Bell test setup	49
3.2	Correlation curves between static signal photons and idler photons rotating along the Poincaré sphere	50
3.3	Photograph of the revised PA in free space	51
3.4	PAs with motorised waveplates and two output couplers	52
3.5	Simulation of rotation effected by achromatic vs zero-order half and quarter waveplates	54
3.6	Final polarisation analyser design in schematic and image	55
3.7	Experimental setup combining two PA outputs into one fibre	56
3.8	Schematic representation of the multiplexed detection outputs and resulting fibre lengths	57
3.9	Schematic representation PAs and power losses experienced at each optical component	58

3.10	Multi-day stability measurement for PA singles count rate and coincidences . .	60
4.1	Schematic of the complete (EPS + PAs) entanglement system	62
4.2	Visibility of polarisation correlations for the EPS	63
4.3	Correlation curves for entangled photons as measured with the PAs	66
4.4	Density matrix ρ of the entangled state emitted by the EPS	72
4.5	Estimated secret key rate for the given system as a function of distance between Alice and Bob	78
4.6	First 2,624 digits of the first-ever secret key generated at the University of York via discrete-variable QKD	80
5.1	Schematics of the network-oriented entanglement-based QKD multiplexed with WR time distribution	83
5.2	EPS Polarisation correlations in dark fibre and in the presence of White Rabbit signals (2D)	86
5.3	EPS polarisation correlations in dark fibre and in the presence of White Rabbit signals (3D)	87
6.1	Geographic and schematic representation of the UK-IE field trial	91
6.2	Coincidences of photons emitted by the EPS after travelling through 200 km of laboratory based SMF per photon	93
6.3	Background noise by wavelength present in the Rockabill link	94
6.4	Long-term polarisation drift of the UK-IE channel over 14 hours	95
6.5	Coincidences of photons emitted by the EPS after travelling through the UK-IE channel	97
6.6	Relative and absolute polarisation drifts of submerged fibre spools	98
A.1	Bell state phase dependence in analytical expressions and graphical form . . .	108

Chapter 1

Introduction

Since its inception in 1935, the notion of quantum entanglement has challenged the intuition and understanding of the physics community. In his letters to Max Born, Albert Einstein famously objected to these 'spooky interactions at a distance', and the thought experiment in his joint publication with Boris Podolsky and Nathan Rosen on the matter came to be known as the EPR paradox [3].

In today's world of quantum science however, entanglement is seen in a markedly different light. Experiments evaluating Bell inequalities [4, 5, 6, 7] have ruled out local hidden-variable theories, preserving realism only by abandoning locality. The importance of this result and the consequent shift in accepted thinking are evidenced by the 2022 Nobel prize in Physics, awarded to Anton Zeilinger, Alain Aspect and John Clauser for their "experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science" [8].

Instead of a conceptual paradox and ghostly action, entanglement has become a physical resource that is harnessed in advanced technological applications. Its role in quantum computation, quantum communication and quantum sensing places it at the heart of modern quantum technology. For quantum cryptography in particular, entanglement is an invaluable tool to assure information-theoretic security and enable a future quantum internet [9]. This thesis presents the development of robust receivers for polarisation-entangled quantum communications research, implementation with a commercial single photon source to produce a cryptographic key, and two optical fibre infrastructure based experimental investigations that address practical challenges in real-world deployment.

1.1 Quantum Cryptography

1.1.1 Classical Encryption

The secure transfer of large quantities of data is a fundamental process underpinning modern society. Governments, healthcare systems, financial sectors and not least private consumers all rely on encryption methods to protect their data as it traverses the predominantly public channels that comprise the internet.

Modern classical encryption practices may be summarised by a three-stage process. First, two users authenticate and establish an initial shared secret via an asymmetric key agreement protocol over an insecure public channel. Historically, RSA [10] has been the predominant system for this initial step. In recent years, the initial key establishment has migrated to the Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) method [11] due to its forward secrecy and increased efficiency [12]. In the second step, both users derive identical session keys from their shared initial secret and use a symmetric encryption algorithm to protect their data, typically following the Advanced Encryption Standard (AES) [13]. Finally, the information is securely exchanged over the public channel. The security of these mechanisms relies on computational hardness of the underlying mathematical problems, such as integer factorisation or the elliptic-curve discrete logarithm problem. A potentially malicious attacker would not be able to reconstruct the key from the public information without impractical computational effort.

Classical encryption algorithms such as RSA, ECDHE, and AES thus provide sufficient security against attacks based on contemporary technology. However, they are severely threatened or even broken by quantum computing. In 1994, Peter Shor introduced a factorisation algorithm for quantum computation [14] that constitutes an exponential speed-up over the best-known classical algorithms. If implemented successfully, this algorithm would break the security of public-key exchanges such as RSA and ECDHE. Similarly, in 1996, Lov Grover developed an algorithm for unstructured database search [15] which quadratically reduces search-time, effectively weakening the security of symmetric ciphers such as AES and requiring longer key-lengths to maintain equivalent security. Although no quantum computer exists as of today that can perform these operations at the relevant scale, the field is steadily advancing [16]. Classical encryption is susceptible to store-now-decrypt-later attacks, which necessitate early adoption of counter-measures. According to Mosca's theorem [17], any information that remains relevant beyond the arrival of powerful quantum computers must be quantum-securely encrypted now. Consequently, transitioning to quantum-safe encryption standards is a pressing issue.

1.1.2 Quantum Key Distribution (QKD)

Quantum cryptography [18] is a class of quantum physics-based cryptographic methods, which provide protection against the threat of quantum computing. Its security is not based on the hardness of a problem, but on the physical laws dictating quantum mechanics. Assuming flawless implementation, even an all-powerful adversary would not be able to compromise

quantum cryptography's security, making messages exchanged via this method information-theoretically secure.

Quantum cryptography is ultimately rooted in the principles of quantum mechanics, namely quantum superposition and the no-cloning theorem [19]. Quantum superposition allows a quantum state to exist as a linear combination of multiple eigenstates simultaneously. Upon measurement, the system is projected onto a single eigenstate corresponding to the measurement outcome, thereby altering the original state. The no-cloning theorem establishes that it is impossible to perfectly clone an arbitrary unknown quantum state. Together, these principles imply that if a secret key is communicated using a suitable set of non-orthogonal quantum states, any attempt at intercepting and/or manipulating them unavoidably introduces a detectable disturbance to the system, thus revealing the presence of an eavesdropper. If the measured rate of disturbance exceeds a certain threshold, the exchange is aborted and the key discarded. If an identical shared secret key is obtained, information-theoretic security can be achieved by using this key as a one-time pad (OTP) to encode the desired secret message [20].

This understanding has given rise to myriad Quantum Key Distribution (QKD) protocols, a small subset of which will be discussed in the following sections. Physically, the quantum states may be implemented via a variety of quantum carriers such as electronic spin, photonic phase, and particle arrival time-bins. This work focuses on polarisation encoded photons, chosen due to the maturity and ready availability of polarisation based quantum sources - including those generating polarisation entanglement - and their relative ease of measurement. Leveraging these advantages, the QKD-system developed in this project marks the first complete QKD implementation with discrete variables (DVs) at the University of York (see Chapter 4.6).

1.1.3 Qubit Definition & Notation

The classical binary bits $\{0, 1\}$ can be directly mapped onto their quantum counterparts known as qubits. In Dirac notation, the computational basis of a qubit therefore consists of the orthogonal state vectors $\{|0\rangle, |1\rangle\}$, where

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (1.1)$$

From the computational basis, three mutually unbiased bases $\{\mathbb{Z}, \mathbb{X}, \mathbb{Y}\}$ may be defined as the eigenbases of the three Pauli matrices respectively:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (1.2)$$

The resulting eigenstates correspond to physical polarisation vectors as given in Table 1.1. Tensor products of multi-qubit vectors are written in the shorthand form $|0\rangle \otimes |0\rangle = |00\rangle$.

Note that additionally, in this work, the kets $|0\rangle, |1\rangle$ or any two-qubit combination thereof may also be used to refer to general orthogonal states in an arbitrary basis, especially in tables

Basis	Qubit Definition
Computational or Key	$ 0\rangle, 1\rangle$
Pauli $\mathbb{Z}$ (rectilinear)	$ H\rangle = 0\rangle$ $ V\rangle = 1\rangle$
Pauli $\mathbb{X}$ (diagonal)	$ +\rangle = D\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $ -\rangle = A\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$
Pauli $\mathbb{Y}$ (circular)	$ R\rangle = \frac{1}{\sqrt{2}}(0\rangle + i 1\rangle)$ $ L\rangle = \frac{1}{\sqrt{2}}(0\rangle - i 1\rangle)$

Table 1.1: Basis specific notation for qubits and polarisation based single photon states.

and figures or when referring to the obtained key bits. For example, if a measurement was performed in all three Pauli bases, the resulting table may possess a column labelled ' $|00\rangle$ ' to signify the results for $|HH\rangle$, $|++\rangle$, and $|RR\rangle$, whereas ' $|11\rangle$ ' denotes $|VV\rangle$, $|--\rangle$, and $|LL\rangle$.

1.1.4 The BB84 Protocol

The first QKD protocol was introduced in 1984 by Charles Bennett and Gilles Brassard, commonly referred to as BB84 [21]. In this protocol, the sender (Alice) encodes random secret key bits onto the polarisation states of single photons. The encoding basis is chosen randomly for each photon from two non-orthogonal options, typically the $\mathbb{Z}$ and $\mathbb{X}$ bases. Accordingly, a $|0\rangle$ qubits may be transmitted by a $|H\rangle$ or $|+\rangle$ state, and a $|1\rangle$ qubit by $|V\rangle$ or $|-\rangle$ (see Table 1.1). Alice then sends her states to the receiver (Bob), who independently and randomly chooses a measurement basis from the same set $\{\mathbb{Z}, \mathbb{X}\}$ and extracts key bits from his results. After a sufficiently large number of states has been exchanged, they both announce their preparation/measurement bases publicly (a step known as basis reconciliation) and discard all instances in which their choices do not coincide (key sifting). The remaining shared bits now form a theoretically identical secret key, without at any point revealing the actual key values.

Any intermediate polarisation measurement by a malicious eavesdropper (Eve) necessarily takes place before the announcement of Alice's and Bob's basis choices. Consequently, Eve will select an incorrect basis with non-zero probability. In such cases, the state she transmits after measurement will no longer be an eigenstate of Bob's measurement basis, potentially resulting in an incorrect key bit. Alice and Bob monitor this in the form of error rate estimation: they reveal randomly chosen bits of their key, check for discrepancies, and discard the revealed bits. In modern QKD protocols, the resulting parameter is formalised as the quantum bit error rate (QBER), i.e. the proportion of errors to correlated shared bits in Alice's and Bob's final strings.

In physical implementations, experimental imperfections additionally contribute to the QBER even in the absence of an eavesdropper. These include detector noise, imperfect polarisation state preparation, multi-photon emissions, and reference frame misalignment due to decoherence in the transmission channel. To reconcile the discrepancies in the shared secret key, modern QKD protocols include error correction procedures, which will cause additional information leakage. Subsequently, Alice and Bob utilise privacy amplification schemes that compress the secret key in order to eliminate any information that may be held by Eve.

A formal security proof for BB84 was eventually supplied in 2000 by Peter Shor and John Preskill [22]. They relate the QBER to an upper bound on the secret key rate (SKR), i.e. the number of secure key bits generated per second, given by

$$R = 1 - 2h(Q). \quad (1.3)$$

Here, Q represents the QBER, and

$$h(Q) = -Q \log_2(Q) - (1 - Q) \log_2(1 - Q) \quad (1.4)$$

is the binary Shannon entropy, a quantification of the information that may be held by Eve per bit of the raw key. The factor of $2h(Q)$ accounts for both the information leakage caused by the QBER correction and the key loss during privacy amplification. This expression assumes an asymptotic key length and a perfect single photon source. In a non-idealised scenario, correction factors consequently reduce the SKR further.

Given the above assumptions, Shor and Preskill demonstrate that for $Q \geq 11\%$, secure communication is not possible as privacy amplification cannot recover a positive SKR. Below this value however, their proof establishes unconditional security against any coherent eavesdropping attacks allowed by quantum mechanics. Even an adversary with unlimited computational power and capable of the most general coherent attacks would not be able to access useful information about the key.

1.1.5 Entanglement in Quantum Cryptography

Quantum entanglement is closely related to the previously discussed quantum mechanical principle of superposition. Two or more particles (or multiple degrees of freedom on a single particle) are considered entangled when their joint quantum state cannot be written as a separable product of individual quantum vectors. Instead, the system must be described by a global state that represents a superposition of all possible joint measurement results. Consequently, simultaneous measurements on subsystems produce correlated outcomes even if the physical particles are spatially separated. Canonical examples of such states are the four maximally entangled two-qubit Bell-states, denoted $|\Psi^\pm\rangle$ and $|\Phi^\pm\rangle$. Recalling the qubit notation introduced in Section 1.1.3, the specific polarisation based Bell-state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (1.5)$$

$$= \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \quad (1.6)$$

will be of primary interest throughout this work. Importantly for QKD, quantum entanglement is subject to monogamy [23], meaning any entanglement with an additional quantum state will reduce the existing entanglement between the original pair.

Basing QKD on quantum entanglement rather than traditional prepare-and-measure protocols not only enhances security but enables various advances in quantum communications technology, such as the use of quantum repeaters and multi-user quantum networking.

Pioneering in this category is Arthur Ekert's 1991 E91 protocol [24], which distributes entangled pairs to Alice and Bob and has them choose randomly between three measurement settings each. Some of these configurations are used for key generation analogously to BB84, while others serve to evaluate the Clauser-Horne-Shimony-Holt (CHSH) inequality [25], from which the Bell parameter S is determined (see Section 4.4 for details). S is then used to monitor the security of the channel, as any eavesdropping attempt would reduce the amount of Bell-violation present. The CHSH inequality constitutes an immediate test of non-local correlations, and as such places a fundamental bound rooted in quantum mechanics on the information that an eavesdropper could have obtained, as opposed to approaches whose security relies on assumptions about the internal functioning of the devices.

Notably, Charles Bennett, Gilles Brassard, and David Mermin introduced an entanglement based variation of BB84 in 1992, BBM92 [21], which does not directly utilise Bell-inequalities. A schematic comparison between BB84 and BBM92 is shown in Figure 1.1. This scheme closely follows the structure of BB84, with the key difference that an entangled photon pair is generated by a central source and distributed to Alice and Bob, who again each perform polarisation measurements in randomly chosen bases. Bennett, Brassard and Mermin presented this scenario to show that a violation of Bell inequalities is not required to produce a secret key, and that BB84 is already fundamentally equivalent to an entanglement based formalism. This entanglement-based perspective proved instrumental, as it is the theoretical basis for Shor and Preskill's comprehensive BB84 security proof [22], which had otherwise remained elusive.

Building on Ekert's 1991 proposal, additional entanglement based QKD protocols have emerged that address critical security challenges in practical implementations. A number of eavesdropping attacks exploit experimental imperfections without raising the QBER, such as photon number splitting attacks [26], detector blinding attacks [27], or time-shift attacks [28]. Security based on Bell-violation statistics however can be assured without any assumptions on the inner working of physical devices, thus resulting in device-independent (DI) QKD. Antonio Acín *et al.* performed practical security analysis for DI-QKD against collective attacks and determined a tight bound for Eve's information in the DI scenario. In doing so, they demonstrated that security can be guaranteed even in the presence of device imperfections up to a maximum QBER value of 7.1%.

A further application for quantum entanglement in QKD takes place in the context of future quantum networking related to the inherent key rate-distance limitations to which QKD is subject. Losses in optical fibre scale exponentially with distance as $I_T = I_0 \times 10^{-\frac{\alpha L}{10}}$. Here α is the fibre attenuation coefficient (typically $\sim 0.2 \text{ dB/km}$ in standard optical fibre), I_0 is the initial intensity and L is the transmission length of fibre. As a consequence of the no-cloning theorem, intermediate amplification is not possible and lost photons cannot be

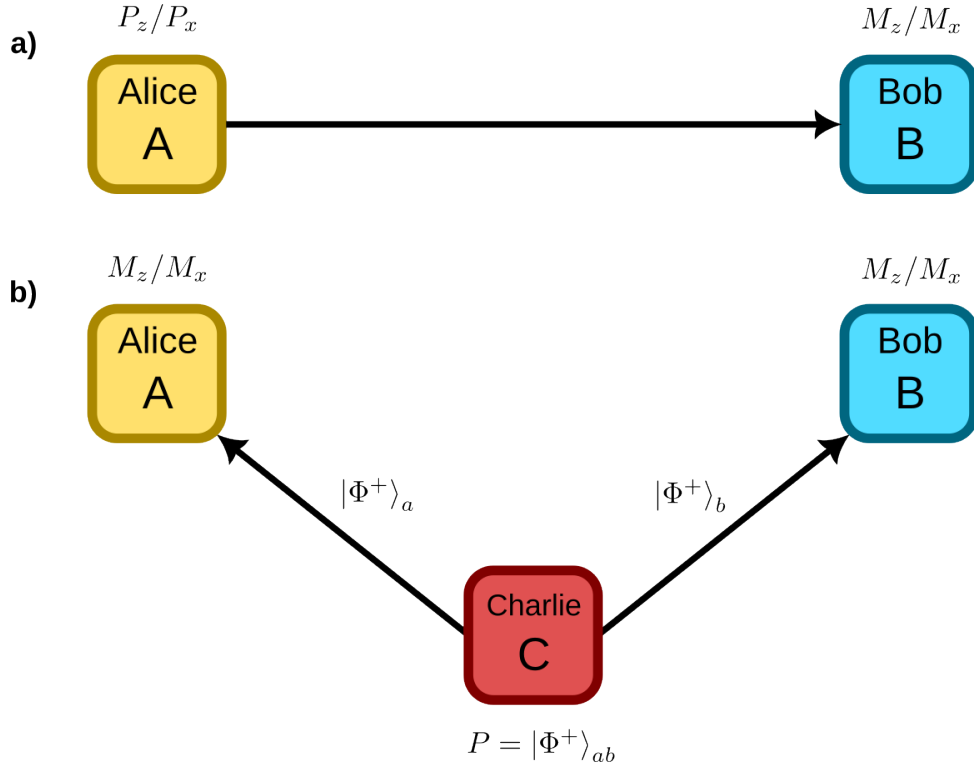


Figure 1.1: Schematic representation of a) the BB84 protocol and b) the BBM92 protocol. In BB84, Alice prepares a random state $|\psi\rangle \in \{|H\rangle, |V\rangle, |+\rangle, |-\rangle\}$, while Bob measures in a random basis $\in \{\mathbb{Z}, \mathbb{X}\}$. In BBM92, an intermediate third party Charlie prepares the entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ and sends one photon to each Alice and Bob, who then measure in a randomly chosen basis $\in \{\mathbb{Z}, \mathbb{X}\}$. The protocols are equivalent from both a security perspective and in terms of distance scaling.

replaced. Consequently, the SKR drops with distance, the QBER steadily increases due to the growing relative noise, and eventually secrecy can no longer be assured without the use of trusted nodes. The fundamental limit for repeaterless secret key capacity of QKD, SKC_0 , was presented by Pirandola, Laurenza, Ottaviani, and Banchi (PLOB) in 2017 [29]. The SKC_0 determines that a lossy channel with transmissivity η supports a maximum secret key rate $K(\eta) = -\log_2(1 - \eta)$.

Quantum repeaters are broadly defined as any device that enable QKD to surpass the repeaterless secret key capacity. The only currently known protocol exhibiting repeater-like distance behaviour is Twin-Field QKD (TF-QKD) [30], in which phase-encoded coherent states undergo single-photon interference at an intermediate station. Since transmission probabilities for weak coherent states scale as $\sqrt{\eta}$, TF-QKD can achieve a positive secret key capacity beyond the repeaterless capacity, as shown in early theoretical [31, 32, 33, 34, 35] and experimental [36, 37] works. However, TF-QKD does not constitute a scalable quantum repeater as it cannot be concatenated across multiple nodes. To reach arbitrary distances, it is necessary to create a type of quantum repeater that can be operated in series. For this purpose, Briegel, Dür, Cirac, and Zoller proposed a scheme based on repeated Bell-measurements to distribute entanglement to arbitrarily distant parties [38]. In a process known as entanglement swapping, a Bell-state measurement is performed on two photons, each belonging to a different entangled pair each. This transfers their respective entanglement to the remaining half of each pair, leav-

ing a single entangled pair that may be spatially distant. In this manner, entanglement can be distributed via an arbitrary number of intermediate nodes. A physical quantum repeater architecture has been presented as early as 2001 by Duan, Lukin, Cirac and Zoller [39], based on entangled photon states from atomic ensembles and repeated potentially noisy Bell-state measurements. However, a practical quantum repeater network using this technology requires quantum memories to store the entangled photons while waiting for successful entanglement swapping at other nodes, which is still an unresolved challenge in the current technological landscape [40, 41].

Lastly, several works have highlighted the advantages of quantum entangled states for multi-user quantum network architectures. Entanglement sources based on spontaneous parametric down-conversion (SPDC) are commonly employed in QKD systems due to their relative technological maturity. These sources can feature a broad spectral bandwidth, which allows for straightforward multiplexing of multiple users and thereby facilitating scalable quantum networks [42, 43]. Furthermore, recent studies have proposed the usage of multipartite-entangled Greenberger-Horne-Zeilinger (GHZ) states to improve resource allocation and streamline transmission traffic, enabling more efficient multi-user QKD protocols [44].

1.2 Current State of the Art and Challenges in QKD

When reviewing the current state of the art in quantum communications, it is important to distinguish between laboratory-based demonstrations, practical field experiments, and sustainable technology deployed in operational settings. Naturally, new milestones are most readily achieved in the controlled environment of an optical laboratory. However, the adoption of QKD as a mature technology also relies on demonstrations of practical deployed system. The following sections will provide a concise overview of recent advancements made in quantum communications research in both the laboratory and field contexts, touch upon some of the prevalent challenges, and provide an outline of current national quantum networks. This discussion does not address the plethora of commercially available QKD systems or their associated recent economic growth, which are beyond the scope of this work.

1.2.1 Key Generation Rate-Distance Limitation

For the reasons described in Sec. 1.1.5, point-to-point QKD distance is often quoted as a benchmark for technological progress in quantum communications. Many fibre-based QKD implementations achieve success over distances of several hundred kilometres [45, 46, 47], and the current distance record for fibre-based QKD is held by Liu *et al.*, who implemented TF-QKD over 1002 km in a laboratory environment [48] and over 428 km in deployed infrastructure [49].

Entanglement-based QKD, on the other hand, has been demonstrated by Neumann *et al.* [50] over up to 248 km of deployed fibre, connecting the cities of St Pölten in Austria and Bratislava in Slovakia for 110 hours with continuous secret key generation of 1.3 bits/s. Other recent notable works include the entanglement QKD demonstration over 404 km of optical fibre

by Zhuang *et al.* [51], using an ultra-bright source and wavelength multiplexing to achieve an SKR of 440.8 bits/s at 200 km, and the laboratory based entanglement of quantum memories over 420 km kilometres reported by Luo *et al.* [52], working specifically towards a quantum repeater infrastructure.

Beyond fibre-based limits, satellite QKD can bridge significantly greater physical distances due to the different dominant loss mechanisms in free-space channels, albeit at the cost of limited transmission periods during overhead passes. Most recently, the Jinan-1 microsatellite [53] set a new distance record for trusted-relay QKD by generating shared keys between ground stations in China and South Africa separated by roughly 12,900 km. The longest entanglement distribution to date was performed using the Micius satellite [54], which distributed entangled photons to ground stations separated by 1,203 km and evidencing the violation of Bell-inequalities.

Imperfect transmission in optical fibres results in an intrinsic trade-off between SKR and the achievable transmission distance. For practical quantum networks, sufficiently high SKRs are required to support large volumes of data traffic, which remains a significant challenge. In discrete-variable systems, SKRs on the order of 10 Mbit/s over approximately 10 km can be considered baseline performance [55]. Leveraging improved electronics and advanced detectors such as multi-pixel superconducting nanowire single photon detectors, recent demonstrations have achieved rates ranging from 60-115 Mbit/s over comparable links [56, 57], representing the current state of the art for discrete-variable implementations. Continuous-variable QKD is typically more limited in terms of achievable range due its higher sensitivity to noise, but can operate at favourable key rates over metropolitan-scale deployments (up to ~ 100 km). Recent breakthroughs report SKRs of ≥ 1 Gbit/s up to 10 km distances and ~ 100 Mbit/s at 50 km [58].

1.2.2 Security Assurance & Quantum Hacking

Modern security proofs typically provide security against the most general coherent attacks allowed by quantum mechanics. Inevitably, such proofs rely on a set of assumptions about the physical devices, and experimental implementations are striving to fulfil these assumptions as closely as possible. Whenever a discrepancy between the theoretical model and the real device behaviour exists, vulnerabilities arise which may give Eve an opening to obtain information about the shared secret. A substantial body of current research revolves around discovering potential quantum hacking attacks that exploit such vulnerabilities and designing secure protocols to protect against them in realistic settings [40, 59]. This includes both the identification of specific attacks and development of transferable mitigation strategies, for example the photon number splitting attack and the decoy state method [60, 61], as well as the extension of security proofs to account for experimental imperfections and finite-size effects [62].

Many known quantum hacking attacks arise specifically from imperfections of physical devices [18]. Detector side-channel attacks are one prominent class, which exploit unintended information leakage based on implementation specific vulnerabilities. Examples include

detector efficiency mismatch, time-shift attacks, blinding attacks and backflash attacks. Similarly, quantum state preparation may be affected by imperfections, such as multi-photon emissions which can enable photon number splitting attacks. In addition, channel probing attacks such as Trojan-horse attacks leverage unwanted responses of optical components in the physical system.

One approach to mitigate physical detector vulnerabilities is measurement-device-independent (MDI) QKD [63, 64, 65], as well as the already mentioned TF-QKD [30], which shares a similar architecture to MDI-QKD. In MDI-QKD, measurement devices are treated as untrusted and thus do not need to be fully characterised, thereby removing all detector side-channels from the security model. However, the sources still have to satisfy certain trust assumptions. While MDI-QKD can achieve secure transmission distances on the order of several hundred kilometres and thus represents an important step towards practical secure QKD, it does not account for source-based quantum attacks and consequently retains some implementation vulnerabilities.

The aforementioned DI-QKD protocol provides more extensive implementation security, as it requires minimal assumptions on the internal functioning of the devices used by the communicating parties. However, experimental accomplishment of loophole-free Bell-violation is extremely challenging. Ideal DI-QKD requires high detection rates, low losses, near-unity detector efficiency, and high timing precision to retain space-like separation of the single photon detection events. These are only possible with costly specialised equipment and over short distances. Truly loophole-free DI-QKD implementations are limited to a few hundred metres of separation between Alice and Bob [66]. A recent breakthrough [67] pushed this distance towards 100 km, though without closing the locality loophole, a remarkable increase over prior-art results, which brings DI-QKD much closer to practical applications.

In the pursuit of practical QKD, certain trade-offs between security guarantees and implementation complexity are therefore unavoidable. An important ongoing research direction in the QKD community is the identification of QKD architectures that prove feasible for real-world deployment while retaining a security advantage rooted in quantum-mechanical principles. Ultimately, it is natural that QKD will be adopted into usage if it provides stronger security than classical approaches based on physical laws at a reasonable cost in terms of monetary investment and performance.

1.2.3 Real-World Deployment & Standardisation

On the path towards deployed quantum communication networks, integrating QKD systems with the current technological standard constitutes a central challenge [68] and is often considered at least as critical as the ongoing technical progress. Utilisation of the already present optical infrastructure significantly lowers the barrier towards large-scale deployment, and alignment with industry-accepted standards accelerates both adoption and accessibility of QKD technologies for global stakeholders. Consequently, a substantial amount of research is aimed specifically at reducing the technological overhead associated with incorporating quantum signals into conventional systems, developing practical implementations using off-the-shelf components and assessing deployed fibre connections for QKD operation.

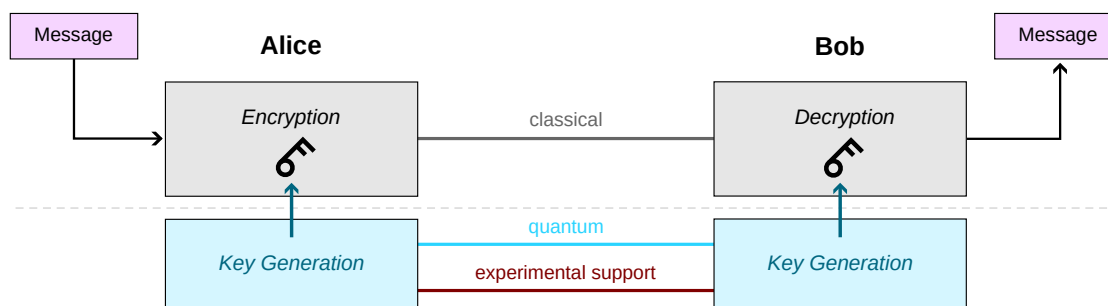


Figure 1.2: Schematic representation of the communication layers in a quantum secured network. The quantum system produces a secret key, which is handed to the classical system to perform encryption and message exchange. Current network architecture (above dashed line) is thus expanded by physical quantum hardware and two conceptual channels for the exchange of quantum states and experimental support data (below dashed line). Depending on the implementation, it may be possible to combine some or all channels in one physical channel, though this is subject of ongoing research.

Figure 1.2 shows a schematic representation of the different layers making up a quantum secured optical communications network. Presently, all communication networks consist solely of a classical layer, which exchanges both the cryptographic keys and the encrypted data traffic. QKD necessitates two additional layers. First is the quantum layer, over which the comparatively delicate quantum states are exchanged. This is often assumed to be a dedicated dark fibre, as any background light could increase the QBER and negatively impact the key generation process. Secondly, an experimental support layer is needed to facilitate the physical quantum measurements. Depending on the protocol employed, this may include high-precision time-synchronisation, channel birefringence monitoring, optical phase stabilisation or other comparable continuous referencing methods. The QKD system must also take advantage of the classical communication layer for steps such as basis-reconciliation, error correction and privacy amplification.

Despite representing these three layers as separate entities in Figure 1.2, a favourable solution for practical QKD integration into the current infrastructure is to combine all three sub-systems into a single optical fibre using wavelength division multiplexing (WDM) or other space-division approaches. By sharing the optical fibre with the classical channels, the existing optical network landscape could be fully leveraged while minimising deployment costs. This approach presents engineering challenges such as managing inter-channel noise and scattering from the high power classical communications. Several works of recent years have successfully demonstrated QKD and classical communication coexistence in a variety of system configurations [69, 70, 71], highlighting the potential of this strategy.

In parallel with practical advances, standardisation is a crucial endeavour in the acceleration of commercial adoption. A number of leading standardisation bodies are contributing to efforts toward QKD-network integration [72]: The international Telecommunication Union has issued Recommendation ITU-T Y.3810, a framework for quantum key distribution network interworking including functional models and reference models as well as configuration recommendations [73]; the European Telecommunications Standards Institute (ETSI) has formed an industry specification group that has published a white paper on implementation secur-

ity standards for QKD [74] and is currently spearheading further specifications that include protection profiles for QKD, control interfaces for software defined networks, and characterisations of QKD transmitter outputs [75]; and the International Organisation for Standardization (ISO) has published a suite of security functionality requirements and methods for QKD in the form of ISO/IEC 23837-1:2023 [76]. Together, these guidelines show a clear focus on security certification requirements, characterisation of devices, and network interfacing with classical architectures, reflecting growing interest in the interoperability of quantum communication technologies and classical communication networks.

1.2.4 Current Quantum Networks & Initiatives

Over the past decade, public sector interest in quantum communication has driven rapid growth of physical quantum communication networks and national research initiatives. The United Kingdom has established a strong standing within this evolving landscape, which provides the context for the research presented in this thesis, supported by the UK Quantum Communications Hub (QCH). The following section offers a brief introduction to the United Kingdom's current position, as well as an illustrative selection of leading global quantum networks.

The United Kingdom was one of the first European countries to initiate a national effort in quantum technologies, launching the Quantum Communications Hub [77, 77] in 2014 as part of the their National Quantum Technologies programme (NQTP) [78]. Led by the University of York, the QCH accelerated commercialisation of QKD technology, advanced foundational research in secure quantum networks, and built partnerships across the public sector, global industry, and national universities. Following the conclusion of the QCH in 2024, a successor hub was established by the NQTP. This Integrated Quantum Networks Hub (IQN Hub) [79] is directed by Heriot-Watt University under a decentralised management structure involving several of the UK's major universities. While the QCH primarily pursued development of industry-ready quantum communication technologies, the IQN Hub signifies a strategic shift towards establishing a fully integrated national quantum infrastructure. One of the QCH's core achievements is the consolidation of a national quantum network, anchored by two metropolitan quantum networks in Bristol and Cambridge and connected via an additional 410 km of fibre in the National Dark Fibre Facility. Building on this foundation, the IQN Hub is now moving from point-to-point QKD implementations and proof-of-principle demonstrations to scalable, multi-node quantum network structures that support various QKD protocols, entanglement distribution for quantum computing and sensing, and integration of free-space and satellite links.

The European quantum infrastructure has been defined by sustainable, network-driven collaborative initiatives since its early days. A seminal example is the Secure Communication based on Quantum Cryptography (SECOQC) project (2004-2008) [80], which resulted in Europe's first deployed multi-user QKD demonstration, combining various point-to-point commercial systems to form a trusted-node based QKD network in Vienna. This pioneering project, which brought together 41 academic and industrial organisations, proved instrumental for the development of a pan-European quantum networking strategy. Further early collaborations include the SwissQuantum network [81] in Geneva (2009-2011), demonstrating an

operational metropolitan network and providing valuable long-term performance data.

In the wake of these early projects, Europe has since seen the emergence of extensive quantum communication test-beds, national quantum links and inter-country connections. Examples notable for their maturity and geographical extent include the Italian Quantum Backbone [82] and the MadQCI test-bed in Spain [83], while several other countries such as Germany, the Netherlands, and Ireland recently launched programmes to deploy and integrate quantum technologies at a national scale, exemplified by initiatives such as IrelandQCI [84]. Today, these advancements are being consolidated under the European Quantum Communication Infrastructure initiative (EuroQCI), which brings together national efforts from all EU member states and the European Space Agency (ESA) to lay the foundations of a quantum internet. EuroQCI encompasses terrestrial quantum networks as well as space-based satellite links, enabling secure, multinational QKD demonstrations [85] and accelerating a comprehensive quantum infrastructure across Europe and beyond.

Globally, China is currently the most advanced actor in quantum communications. Its network comprises four metropolitan centres — Beijing, Jinan, Hefei, and Shanghai — interconnected via dozens of trusted-node relays, forming a terrestrial network exceeding 10,000 km [86]. Additionally, two optical ground stations integrate high-speed satellite-to-ground communications with the dedicated quantum satellite Micius [87], facilitating quantum-secure communication between users up to 4,600 km apart [88]. This network's reach has recently been further extended by the addition of the microsatellite Jinan-1, auxiliary to Micius, and a portable optical ground station, which together have achieved connections over distances up to 12,600 km, linking China and South Africa [53]. Beyond China, significant quantum networks exist in other non-European countries: In Japan, the Tokyo QKD Network has supported field demonstrations for over a decade [89], and an expansion to a 600 km national network linking multiple major cities is planned [90]. In the United States, despite the National Institute of Standards and Technology (NIST) electing post-quantum cryptography as the primary defence against the cryptographic threat of quantum computers, several metropolitan-scale quantum networks [91, 92, 93] remain operational. These developments indicate that quantum communication technologies are rapidly maturing worldwide, outgrowing experimental test-beds and moving to components of the contemporary communication landscape.

Evidently, the world is steadily moving towards a global quantum internet. However, while quantum communication networks are increasingly deployed and integrated over terrestrial and space-based links, one aspect of infrastructure that remains relatively unexplored are underwater fibres. Submarine links are a natural choice for numerous international connections and are widely employed in traditional communication infrastructure, yet only very limited investigations into their feasibility within a quantum technology context exist at the present date. Mainly two fibres have been reported on, the roughly 100 km long link between Sicily and Malta [94, 95], and a 224 km UK-Ireland connection [2], which is subject of Chapter 6 of this thesis. Investigating these undersea links is a crucial step towards realising a fully-connected quantum-secured infrastructure, bridging the gap between existing national networks and a global quantum internet.

1.3 Thesis Overview

The beginning of this PhD programme coincided with the starting phase of the discrete-variable experimental quantum communications group at the University of York, during the tail-end of the COVID-19 pandemic in early 2021. At this time, there was no established laboratory space, no prior research projects, and limited guidance due to the absence of postdoctoral researchers and experienced students, until the group markedly expanded and moved to a dedicated DV-optics laboratory in 2022. Expertise from colleagues working on continuous-variable QKD provided valuable support during the initial year, but regardless, the start of this PhD was mainly devoted to developing research capacity, establishing laboratory resources, and acquiring the necessary experimental skills from the ground up.

Consequently, Chapter 2 of this thesis is dedicated to characterisation and setting up of DV-specific laboratory equipment. Unless stated otherwise, all work in this thesis is performed at or around the telecom wavelength of 1550 nm for minimum losses and optimal compatibility with existing optical infrastructure. The instruments listed in this chapter were subsequently used throughout the thesis, and intimate knowledge of their functioning informed the design of the polarisation entanglement system as well as the choice of novel experimental investigations.

Chapter 3 provides a detailed account of the development of a set of polarisation analysers (PAs) capable of performing various investigative polarisation-state measurements and functioning as passive receivers for BB84 and BBM92-type quantum key distribution. The PAs were designed with special focus on experimental stability, ease of use, and flexible application in future quantum communication studies, both in the laboratory and during field deployments. In conjunction with the entangled-pair source characterised in 3, the PAs were then used to implement a complete polarisation-entanglement system for QKD applications. Chapter 4 demonstrates the PA's functionalities through a series of entanglement based measurements, including CHSH-type Bell-inequalities and quantum state tomography. Lastly, the entanglement system was employed to generate a secret key following the BBM92 protocol, representing the first complete demonstration of quantum key distribution within the DV experimental quantum communications group at the University of York.

Finally, Chapters 5 and 6 present two research projects in the context of accelerating deployment of entanglement based QKD in real-world communication infrastructure, both of which resulted in publications [2, 1]. Chapter 5 explores the coexistence of entanglement-based QKD with White-Rabbit time synchronisation, highlighting the integration of QKD into existing optical communication infrastructure as discussed in Section 1.2.3. Chapter 6 reports entanglement-related results from a field-trial assessing the suitability of a 224 km international, submarine fibre link between the UK and Ireland to support QKD, representing one of the few instances of its kind (see Section 1.2.4). While neither investigation employs the final-design PAs, prototypes were featured, and several open research questions remain as avenues for future investigations using the mature PAs developed in this work.

Chapter 2

Instrument Characterisation

This chapter reports in-depth characterisations of the key instruments that were used throughout this thesis. These include Single Photon Avalanche Detectors (SPADs), Superconducting Nanowire Single Photon Detectors (SNSPDs), a source of polarisation entangled photon pairs (EPS), and analysis methods for time taggers. Each of these instruments was acquired as part of the new Experimental Quantum Communications (EQC) laboratory at the University of York. Consequently, these characterisations not only serve to commission and validate their performance, but also establish a baseline for the experimental capabilities and limitations of the available facilities. This initial work has shaped the direction of both the research presented later in this thesis and the broader efforts of the research group.

2.1 Single Photon Avalanche Diodes

Single Photon Avalanche Detectors (SPADs) are a commonly used type of click-or-no-click detectors, often chosen for their practicality and robustness. They function based on an InGaAs semiconductor diode that is reversely biased above breakdown voltage, so that an incoming single photon triggers an electronic avalanche through the photoelectric effect. At an operating wavelength of 1550 nm, SPADs exhibit typical detection efficiencies of $\eta_{det} \leq 25\%$, while recovery times on the order of microseconds limit the maximum repetition rate to several hundred kHz. These detectors can be operated free-running mode, where they are continuously biased above breakdown, or in gated mode, with the latter periodically applying the excess bias for a short duration (the gate), reducing the detector noise probability and providing temporal selectivity. As comparatively affordable, compact devices operating at room temperature, SPADs are widely used in practical applications.

A total of six SPADs, three pairs of different models, were acquired for the EQC group (see Table 2.1). Due to SPADs' typically limited detection efficiencies, low temporal bandwidth, and high noise levels, a thorough understanding of their optimal operating parameters was required to maximise their performance across different research scenarios. Consequently, the first step was to conduct a comprehensive characterisation, investigating metrics such as detection efficiency, dark count rates, and signal to noise ratio. A selection of particularly relevant or insightful results is presented in the remainder of this section.

Model	Device ID	Operating Mode	Manufacturer
ID220	D1 D2	FR	ID-Quantique
IDQubes NIR	Q1 Q2	FR + Gated	ID-Quantique
PDM-IR	P1 P2	FR + Gated	MPD

Table 2.1: SPAD models acquired for the EQC group and their operational modes (FR = free-running).

2.1.1 Photon Detection Efficiency

The SPADs' detection efficiencies were determined using the substitution method. A stable Continuous Wave (CW) laser illuminates the SPADs through a precisely calibrated optical attenuation system. A reference power-meter, connected in parallel with the SPADs, monitors the incident optical power, enabling calculation of the detection efficiency. The experimental setup is shown in Figure 2.1. A series of measurements with varying incident power levels is taken, and the slope of the resulting count rate in the near-linear regime provides a precise estimation of the detection efficiency. The SPADs were calibrated in gated mode with varying gate lengths where possible, as this configuration exhibits a better signal to noise ratio. Figure 2.2 shows the detection efficiency calibration results.

2.1.1 PHOTON DETECTION EFFICIENCY

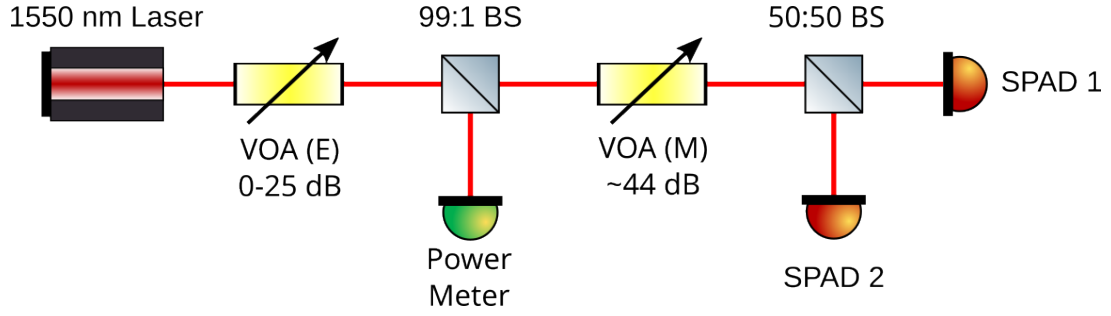


Figure 2.1: Schematic representation of the experimental setup used to determine the SPAD detection efficiency via the substitution method. CW-laser light is first attenuated via an electrical Variable Optical Attenuator (VOA (E)), whose attenuation is varied throughout the experiment. A 99:1 Beam Splitter (BS) distributes the light between a power meter and a further manual VOA (M) fixed at 44 dB attenuation, after which the SPADs under investigation are connected.

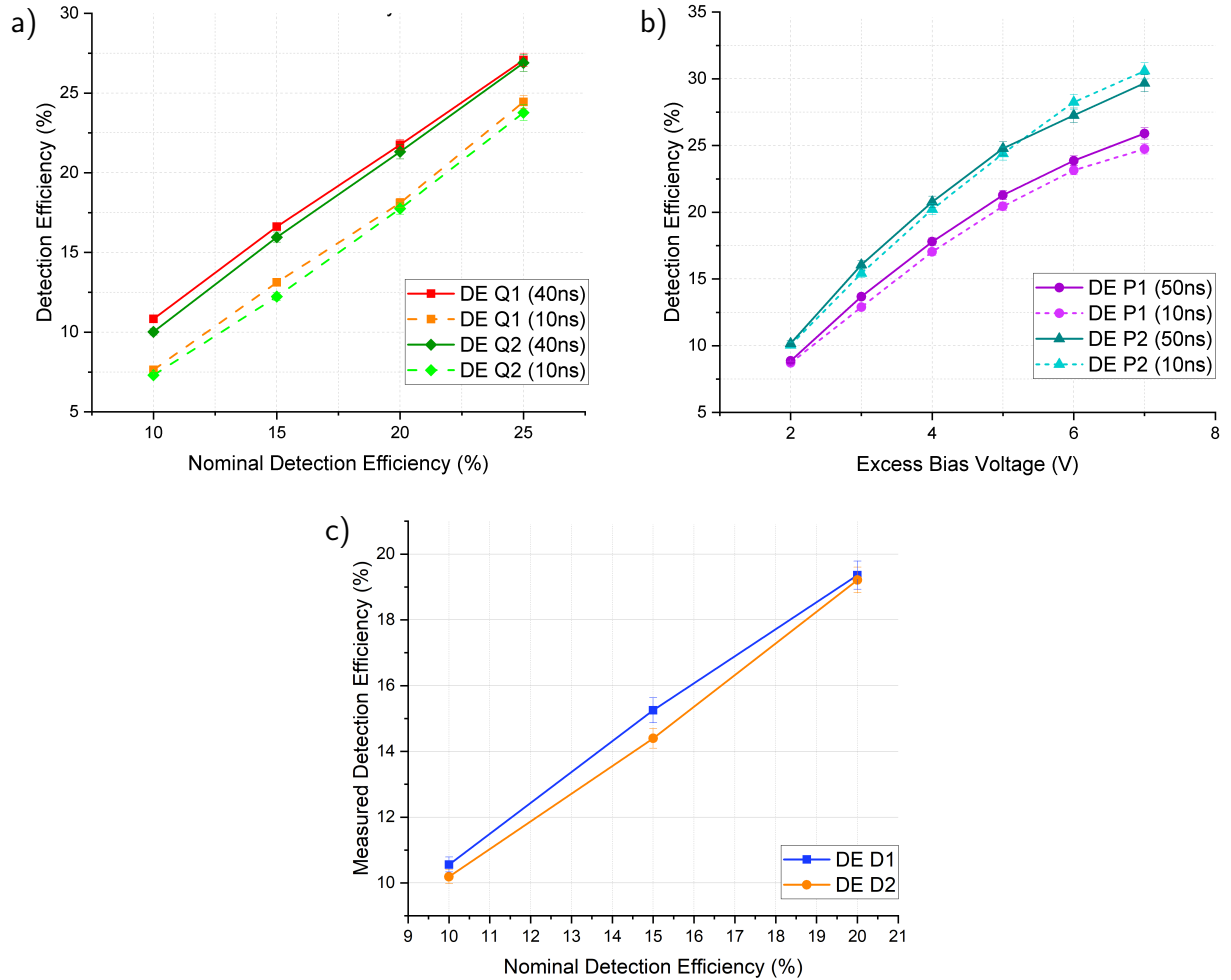


Figure 2.2: Measured detection efficiencies at various gate lengths (given in brackets) for a) the IDQubes, versus nominal detection efficiency; b) the PDM-IRs, versus excess bias voltage; c) ID220s, versus nominal detection efficiency. In each case, the variable on the x-axis corresponds to the setting available in that detector's GUI.

The PDM detectors are operated with an excess bias setting rather than a detection efficiency setting, so this graph serves as a laboratory reference to align their performance with the other detectors. Notably, the gate length appears to influence the observed detection efficiency for the IDQubes, which prompted further investigation, as detailed in Section 2.1.4.

2.1.2 Dark Count Rates

Even with perfect shielding from noise photons, SPADs exhibit an intrinsic Dark Count Rate (DCR) caused by voltage-induced spontaneous avalanche formation and afterpulsing effects. The DCR is strongly dependent on operational parameters such as excess bias, detector dead time and, in the case of gated operation, the gate repetition rate. DCR calibration should be performed before every experimental measurement to account for all relevant factors, including optical power and stray light. However, to establish a guideline for suitable operating parameters, selected DCR calibrations were conducted. Figure 2.3 shows one such calibration, investigating the DCR with detector dead time for the SPADs in free-running mode at 20% detection efficiency.

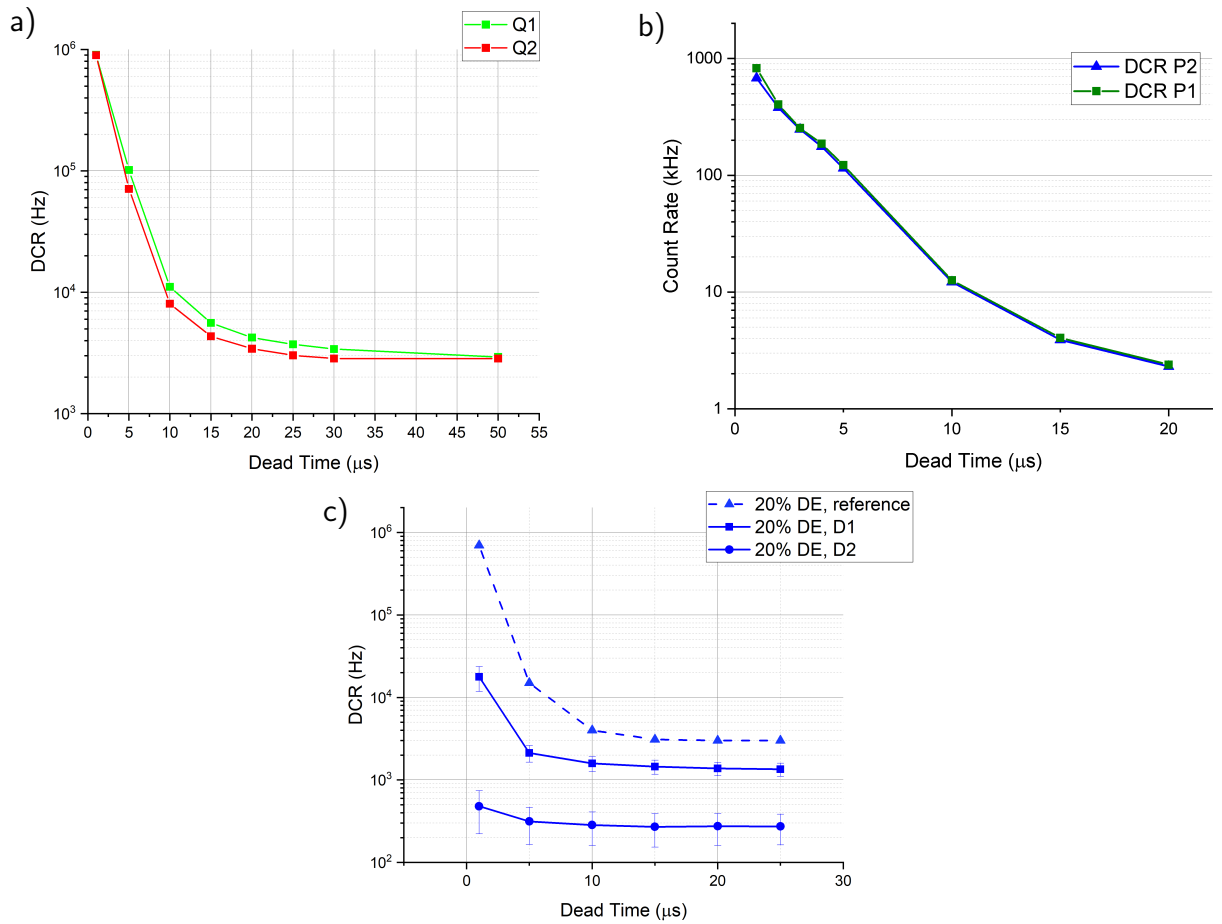


Figure 2.3: DCR against detector dead time for the a) IDQubes, b) PDMs and c) ID220s. In each case, the detector was operated in free-running mode at 20% detection efficiency.

The detector dead time setting determines the period following a detection event during which the SPAD is biased below breakdown voltage, allowing the avalanche to dissipate. The ID220 detectors, which are designed specifically for free-running operation, exhibit low DCR for dead times of $5\ \mu\text{s}$ and above, while the gating-capable detectors show escalating dark counts below $15\ \mu\text{s}$ dead time and a higher DCR baseline. Additional measurements indicate that, in gated mode, the IDQubes and PDMs offer a greatly superior signal-to-noise ratio and can operate with comparatively short dead times, depending on their gating frequency.

2.1.3 Timing Jitter

The timing resolution of SPADs typically ranges from around fifty to a few hundred picoseconds, with higher bias voltages improving the precision. When measuring coincident detections of photons with coherence times shorter than this range, as is the case for the photons from the entanglement source used throughout this thesis, the detector timing jitter becomes the limiting factor determining the width of the coincidence peak and consequently the timing window that should define a coincidence (the 'coincidence window'). As experiments involve longer channels, chromatic dispersion eventually can become the dominant contribution. Regardless, in all cases the coincidence window has to be appropriately matched to the observed temporal spread of the detected photon pairs.

A practical method to achieve this is the histogramming of the time-tagged coincidence times and fitting of a Gaussian function to the resulting peak. The parameters of this fit allow the selection of a coincidence window that captures the majority of photon pairs while keeping the inclusion of background counts to a minimum. Figure 2.4 shows two examples of this procedure. The measured convolution of instrument jitters in this detector pairing was found to be lower than the value expected from the combined typical specifications, indicating that at least one model operates above its nominal specifications.

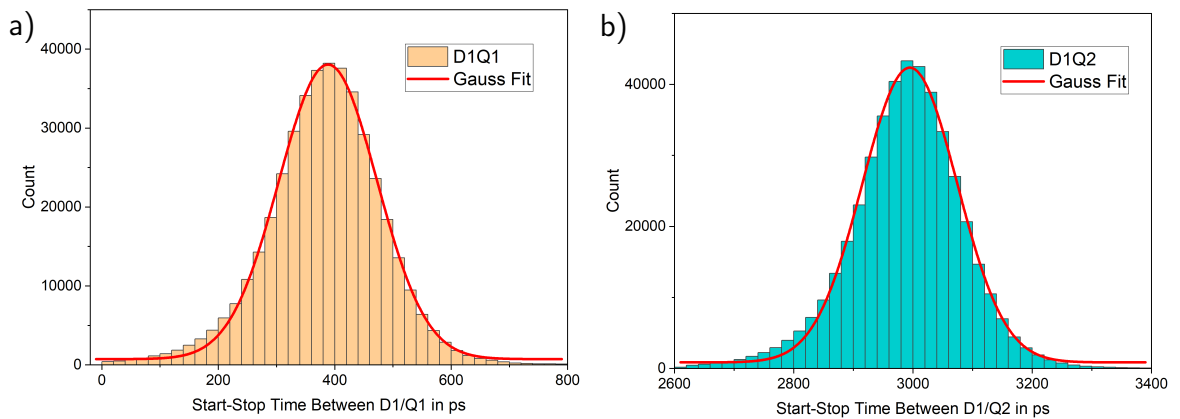
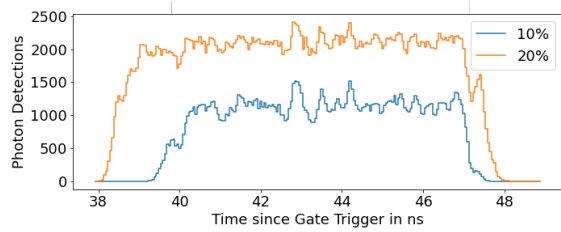


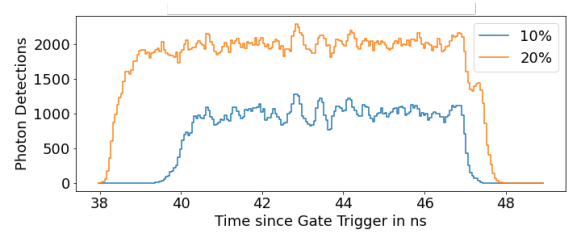
Figure 2.4: Coincidences from the EPS between a) D1 and Q1, with measured $\text{FWHM} = 198 \pm 2\ \text{ps}$, and expected combined jitter is around 300 ps; b) D1 and Q2, with measured $\text{FWHM} = 187 \pm 2\ \text{ps}$, and expected combined jitter is around 300 ps.

2.1.4 Detector Gate Profile

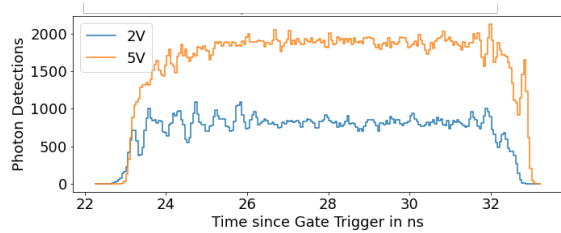
For the SPADs capable of gated operation, the detector gate shape was visualised to understand the trends in detection efficiency noted in Section 2.1.1. This is commonly achieved using a picosecond pulsed laser to probe different temporal regions of the gate. In the absence of such a source, an alternative approach is employed. By shining attenuated coherent laser light on the detector, a uniform probability distribution of incident photons across the gate is obtained. Referencing the photon arrival times to the gating frequency and histogramming the results therefore yields the relative detection sensitivity as a function of time. This creates a direct visualisation of the detector gate shape as displayed in Figure 2.5.



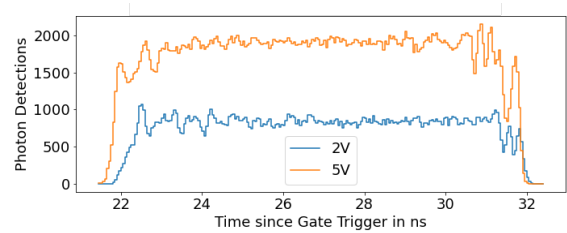
a) Q1 gate at 10% and 20% detection efficiency.



b) Q2 gate at 10% and 20% detection efficiency.



c) P1 gate at 2V and 5V detection efficiency.



d) P2 gate at 2V and 5V detection efficiency.

Figure 2.5: Time resolved photon count rates within the detection gate of each SPAD at different detection efficiencies, visualising the gate profile. All gates were set to a length of 10 ns.

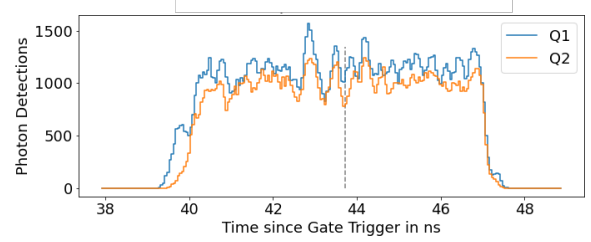
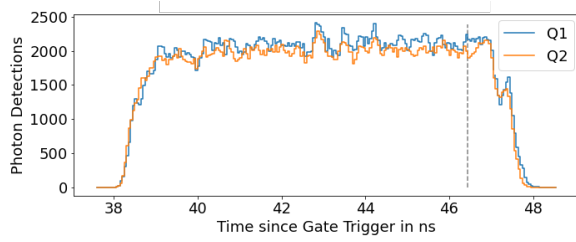
The resulting gate shapes are consistent across repeated measurements, indicating that any irregularities are likely characteristic of the underlying physical detector elements. Notable observances include a delay in reaching the target bias voltage on the IDQube detectors, particularly for low detection efficiency, which explains why the nominal detection efficiencies were consistently higher than the measured efficiencies for short (10 ns) gates (see 2.2 a)). Table 2.2 lists the FWHM of the observed detection gates, which are all nominally designed to be 10 ns.

Additionally, both detector models exhibit sections of periodically oscillating sensitivity, especially at low excess bias voltages. These peaks and troughs have implications on QKD security, as a static, non-uniform gate profile could be exploited in the form of a time-shift attack. By selectively delaying photons, Eve could increase the probability that one detector triggers over the other, thus biasing the bit selection and gaining information about the secret key. Figure 2.6 shows two gates on equivalent detectors overlapped at the optimal alignment to minimise any efficiency differences, representing the best-case scenario the receiver can create.

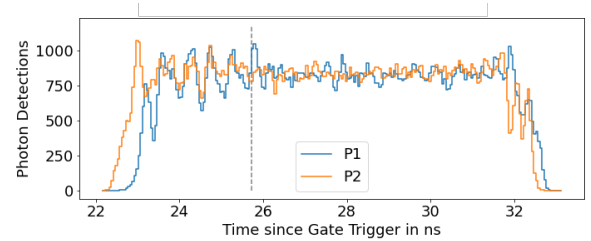
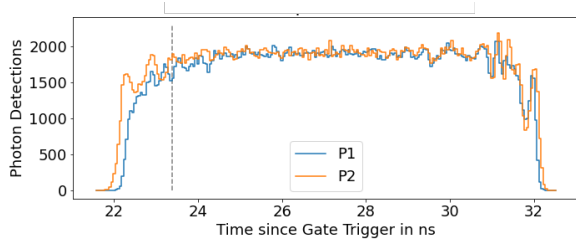
Efficiency/Bias	Gate Width FWHM (ns)			
	Q1	Q2	P1	P2
10%/2V	6.9	6.9	9.25	9.5
20%/5V	8.95	8.95	9.6	9.95

Table 2.2: Comparison of the detector gate length measured as the full gate width at half maximum. All values are given in ns and have an uncertainty of ± 50 ps.

Vertical lines indicate the points where the remaining mismatch is maximal (corresponding to the points Eve would target in her time-shift attack), while disregarding the very edges of the gates which Alice and Bob may choose to discard. Table 2.3 summarises the relative differences in efficiency at these locations. The resulting detection bias is more pronounced at smaller bias voltages, but remains non-negligible in all cases. This investigation highlights the critical importance of thorough detector characterisation for prepare-and-measure QKD implementations and, as motivated in Chapter 1.3, illustrates one of the advantages of entanglement-based device-independent QKD.



a) Gate shapes for Q1 and Q2 at 20% efficiency. b) Gate shapes for Q1 and Q2 at 10% efficiency.



c) Gate shapes for P1 and P2 at 5V excess bias. d) Gate shapes for P1 and P2 at 2V excess bias.

Figure 2.6: Time resolved photon detections within the detection gate for different detectors at identical settings, contrasting the sensitivity of equivalent detectors. Vertical lines indicate the data points where the discrepancy between two detectors is largest (excluding gate edges), despite optimised temporal overlap.

	Q1/Q2	P1/P2
10%/2V	39.5%	29.2%
20%/5V	14.1%	21.9%

Table 2.3: Differences in relative detection efficiencies at the most discrepant points after optimisation of the gate alignment for different detectors of the same model under the same conditions.

2.2 Superconducting Nanowire Single Photon Detectors

Superconducting Nanowire Single Photon Detectors (SNSPDs) are another type of click-or-no-click single photon detectors. Their operation principle is based on passing a current through a nanowire held at cryogenic temperatures, thus keeping it in a superconducting state. Absorption of a single photon locally increases the energy of the nanowire, temporarily bringing it out of superconductivity and the resulting drop in current is used to signal the detection event. Modern SNSPDs outperform SPADs in several key metrics, routinely achieving detection efficiencies $\geq 90\%$, recovery times ≤ 100 ns, DCRs ≤ 100 Hz, and are not subject to afterpulsing effects. However, in contrast to SPADs, they are considerably more expensive, sensitive to environmental conditions, and significantly larger including all the additionally required supportive hardware.

After moving into the new EQC laboratory in 2022, an SNSPD system comprising six channels was acquired, including two channels sensitive in the near-infrared (N-IR) just outside the visible spectrum (780 nm) and four in the telecom C-band (1550 nm) range. The rest of this section presents the noise behaviour and detection efficiency of the four IR channels (labelled 3-6), as they were used extensively during experiments in subsequent chapters. The installation, laboratory integration and many of the initial measurements with the SNSPDs were performed as part of this thesis work. The resulting thorough understanding of the setup process, along with familiarity with its operational challenges, were instrumental in making the UK-IE experimental campaign possible, as described in Chapter 6.

The dark count rate of SNSPDs is primarily caused by thermal photons generated within the detector itself through black body radiation. As a result, the detector DCRs are highly sensitive to both the ambient temperature and the temperature of the device itself. Figure 2.7 shows a selection of DCR values observed under varying conditions. As a general guideline, a DCR < 100 Hz across all channels was considered indicative of acceptable environmental conditions.

Unlike SPADs, SNSPDs detection efficiency is highly dependent on the incoming polarisation state. Shortly after the initial installation, a Manual Polarisation Controller (MPC) station was integrated into the SNSPD system, where the incoming signal can be aligned to best match the detector's preferred orientation. It is important to note that this alignment requires the fibre to support only a single polarisation mode.

The SNSPD detection efficiency was measured by Mr Ormond Taylor, following the same methodology outlined in Section 2.1.1 for SPAD detection efficiency measurements, and is included here as a reference for the subsequent chapters. An additional step involved using the MPC station prior to each measurement to either maximise or minimise counts, corresponding to an aligned or maximally misaligned incoming polarisation state. The resultant efficiency values are quoted in table 2.4 and show good agreement with the manufacturer's test report, as well as a high dependency on the incoming polarisation state.

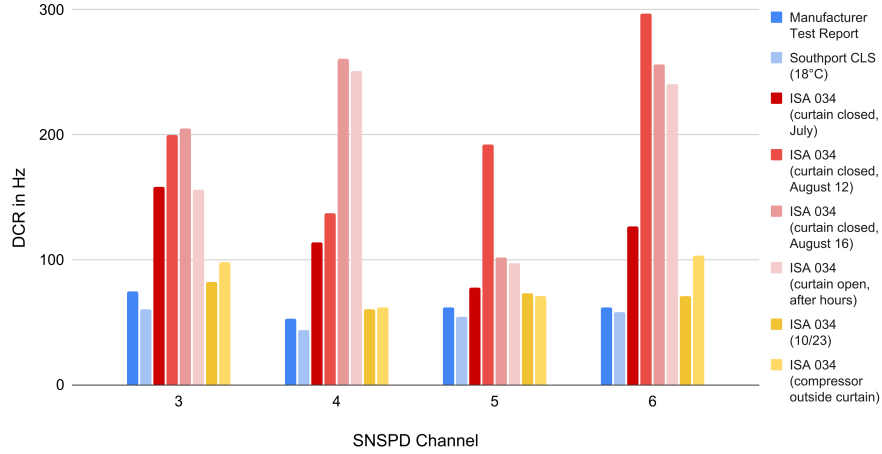


Figure 2.7: SNSPD dark count rate under different environmental conditions. The blue datasets indicate reference values from strictly controlled environments. Initially, a lack of air circulation in the EQCG laboratory caused increased dark counts in the laboratory setting due to rising temperatures around the detector. This was resolved by a reconfiguration of the experimental space and moving of the SNSPD helium compressor to a well-ventilated area.

Channel	Nominal Efficiency %	Max Efficiency %	Min Efficiency %
3	94	87 ± 3	52 ± 1
4	92	90.5 ± 0.01	62 ± 1
5	88	86.6 ± 0.8	58 ± 2
6	93	93 ± 1	48 ± 2

Table 2.4: Detection efficiency of the SNSPD C-band channels as measured by the manufacturer and within our laboratory, all in percent. Data obtained from Mr Ormond Taylor.

2.3 Entangled Pair Source

The polarisation entangled photon source employed in this thesis is based on Spontaneous Parametric Down-Conversion (SPDC). This process leverages the non-linear susceptibility $\chi^{(n)}$ of a dielectric material, which when exposed to a sufficiently strong electric field E , gives rise to an induced polarisation density P in relation to the vacuum permittivity ϵ_0 [96]:

$$P = \epsilon_0 \chi^{(1)} E + \epsilon_0 (\chi^{(2)} E^2 + \chi^{(3)} E^3 + \dots) \quad (2.1)$$

This polarisation acts as a source term in the wave equation for E , giving rise to new frequency components, and in the case of SPDC resulting in three-wave mixing driven by the second-order non-linear term including $\chi^{(2)}$. Quantisation of the involved electric fields reveals that this three-wave mixing spontaneously annihilates a pump photon and creates two lower energy photons, termed signal and idler (see Figure 2.8). Importantly, within the non-linear crystal, both energy and momentum have to be conserved for the conversion to be allowed.

SPDC is an inherently probabilistic process with a low conversion efficiency, such that pairs are produced infrequently enough to be considered well time-separated. SPDC based single

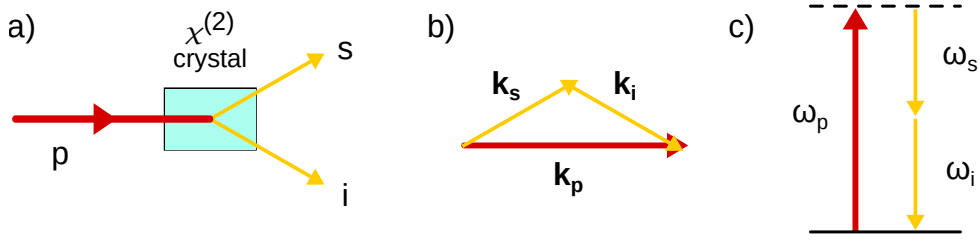


Figure 2.8: Schematic representation of a) the physical SPDC process, b) momentum $\mathbf{k}$ conservation, and c) energy ω conservation within the non-linear crystal. The subscripts denote the pump (p) beam, signal photons (s), and idler photons (i) respectively.

photon sources therefore enable a technique known as photon heralding, by which the presence of a single photon (the idler) is identified by the detection of its heralding partner (the signal). This allows for the filtering of the SPDC pairs against an unrelated background, making the heralded half of the pair into a single photon.

The entangled pair source (EPS) utilised in this work, schematically depicted in Figure 2.9, contains two 25 mm type-0 periodically poled lithium niobate (PPLN) crystals, which facilitate the down-conversion process. Periodic poling enables quasi-phase matching between the interacting fields, thereby enhancing the conversion efficiency, while the type-0 configuration specifies a shared polarisation alignment of the pump, signal, and idler photons parallel to one common crystal axis. The two crystals are arranged in an auto-balanced interferometer setup [97], resulting in the coherent superposition of orthogonally polarised SPDC-pairs to create entangled photons in the $|\Phi^+\rangle$ Bell-state (see Equation 1.5). This specific setup produces count rates on the order of 1 MHz after filtering as described in Section 2.3.1.

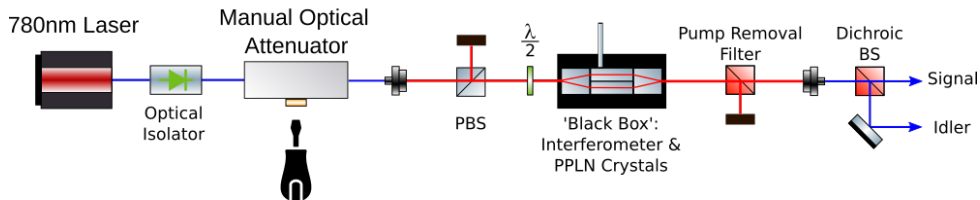


Figure 2.9: Schematic representation of the entangled pair source. Blue lines indicate fibre-based components, red lines free space sections.

This compact, commercially available entangled photon source includes several custom modifications. A manually adjustable optical attenuator can be engaged externally to vary the pump intensity. An access hatch enables adjustment of an internal Half-Wave Plate (HWP), which sets the polarisation state entering the crystals, and thereby controls the relative polarisation components that interfere. Finally, one arm of the interferometer can be occluded with a metal bar, suppressing the entangling interference and causing the source to produce classically correlated photons in the $|HH\rangle$ -state.

The following subsections present a characterisation of the source, assessing its suitability for quantum communication applications.

2.3.1 Wavelength Spectrum

The EPS operates in a wavelength-degenerate SPDC configuration, producing photon pairs symmetrically around a central wavelength determined by the crystal and poling parameters. Figure 2.10 shows the wavelength-dependent count rates measured with the SNSPD system connected after an Optical Tunable Filter (OTF). The measurement is limited by the tuning range of the optical filter and therefore does not capture the full emission spectrum. Within its range, a spectral bandwidth of approximately 60 nm can be determined.

The source is centred at approximately 1560 nm, with signal photons emerging at shorter wavelengths and idler photons at longer wavelengths. This provides a convenient way of isolating entangled pairs using optical wavelength filtering, as entangled photons will be equidistant from the central wavelength. The source itself uses the wavelength spectrum to separate the collinear signal and idler streams before coupling them into individual fibres. The design calls for a fibre-based dichroic mirror with a cut-off wavelength of 1560 nm to split signal and idler photons and send them to separate fibre outputs. However, this particular source exhibits a manufacturing defect, where the cut-off wavelength of the dichroic is mismatched with the SPDC central wavelength. Photon pairs are separated at 1565 nm, which means that any pairs with the idler between 1560 nm - 1565 nm are not separated and instead wholly sent on the signal path.

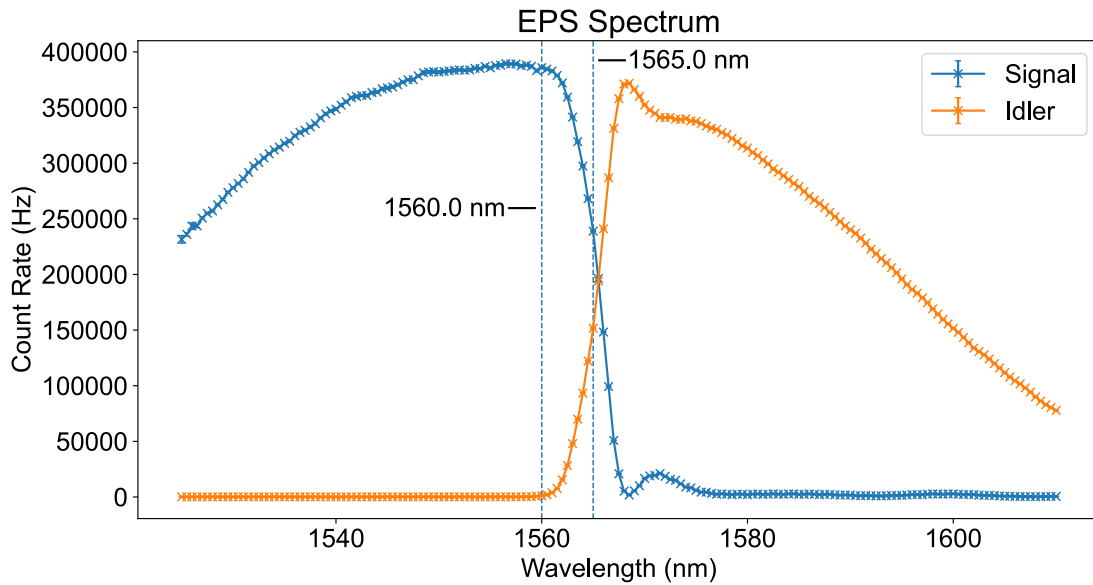


Figure 2.10: Wavelength spectrum of the entangled pairs emitted by the EPS. The mismatch between the dichroic mirror and actual central wavelength can be seen clearly.

The dichroic mismatch causes significant issues when utilising this source for QKD. A non-negligible percentage of the source brightness is immediately lost, as the unseparated photons cannot be individually measured in experiments. Furthermore, the erroneous pairs contribute to excess noise in the form of background counts on single photon detectors, and present as a multi-photon emission, degrading the results of quantum measurements such as HBT-interferometry (see Section 2.3.3).

To circumvent this issue, a practice of only using the source with narrow wavelength filtering is adopted. Generally, pair photons at 1550 nm and 1570 nm are employed, in order to take advantage of the optimisation of optical components for 1550 nm while remaining at a high pair emission rate. Multiple fixed filters at 1550 nm were used with different pass-bandwidths, dependent on the experimental requirements. The higher wavelength idler photons were isolated using the OTF, whose width and central wavelength were chosen to match those of the fixed filters. This strategy eliminates not only the erroneous SPDC photons from the source itself, but also cuts down much of the excess noise that couples into the experiment from the environment. A drawback, however, arises from the drastically reduced source brightness (most of the emitted pairs remain unused) and the increased losses, especially on the OTF path, which presents an insertion loss of 5-7 dB.

2.3.2 CAR & Heralding Efficiency

Two important characteristics when discussing a single photon pair source for QKD are the Coincidences-to-Accidentals Ratio (CAR) and the heralding efficiency. Both are a measure of the amount of genuine pair detections versus the noise present in the system. As such, both the pair and noise emission of the source as well as the noise and losses in the detection system contribute to these figures.

The CAR is defined in Equation 2.2 as the quotient between the total coincidences observed from the source emission, made up of genuine pair detections and unrelated, but coincident events, and the number of accidental coincidences based on statistically arising coincidences. Experimentally, this can be measured by applying a large time delay τ to the detection time of one detector, so only uncorrelated coincidences are recorded.

$$CAR = \frac{\text{Coincidences}}{\text{Accidentals}} \quad (2.2)$$

The CAR scales strongly with detector noise, the coincidence window, and count rates in the regime where detector block-off effects prevent the detection of all pairs. Hence, the CAR can be engineered by manipulating the source brightness and coincidence window (see Figure 2.11). Using SAPDs for the detection, exhibiting DCR values in the range of single kHz, and choosing a coincidence window of 1 ns, this source produces a CAR of several hundreds, exceeding one thousand for optimised source brightness, which is the expected standard for present-day SPDC sources. SNSPDs improve this figure so that a CAR of several hundreds is maintained at the highest pair emission rates [98].

The heralding efficiency $\eta_{(i|s)}$ (also known as Klyshko efficiency) is a measure of the conditional probability that the detection of one photon (e.g. the signal) heralds the presence of its partner photon (e.g. the idler). It is defined as in Equation 2.3 as the quotient between the observed rate of signal and idler coincidences C_{si} and the rate of signal photons alone S_s . The heralding efficiency is equal to the optical losses that the heralded photons experience multiplied by the detection efficiency, and can thus be used to estimate the total losses of an optical connection.

$$\eta_{(i|s)} = \frac{C_{si}}{S_s} \quad (2.3)$$

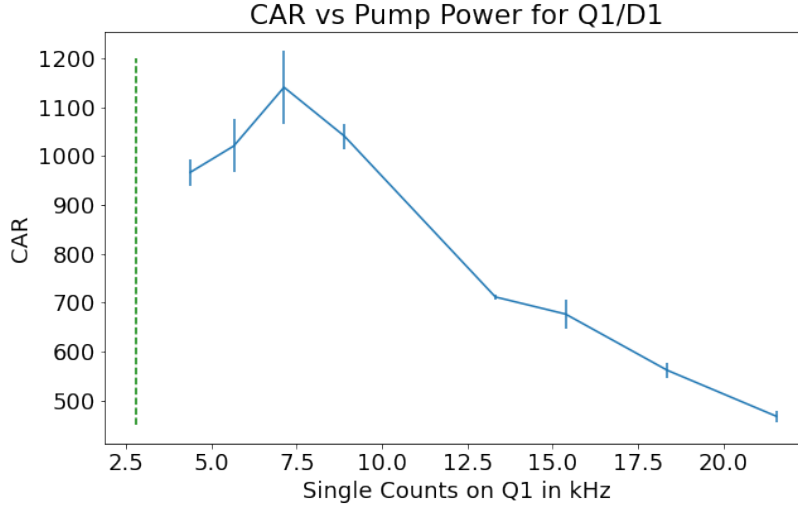


Figure 2.11: Dependency of the CAR on the source emission rate. In the lowest regime, detector dark count (green line) induced accidentals dominate the observed coincidences, thus limiting the CAR. In the higher regime, statistical accidental coincidences between emitted singles dominate as they scale faster than coincidences stemming from true pair emissions.

For the full QKD setup including the EPS, a heralding efficiency of $\sim 5\%$ is measured (see Figure 2.12), which is low for the current technological standard. This value corresponds to an attenuation of 13 dB on both outputs, since the heralding efficiency is similar when using either photon as the herald. However, known losses in the full setup can account for part of this attenuation, particularly the OTF with an estimated insertion loss of 5 dB, 50:50 beam splitters in the detection system that contribute an additional 3 dB, and coupling losses between free space and fibre. Details on these losses can be found in Section 3.7. Other factors may include low source-to-fibre coupling within the source itself, measurement of which is infeasible with the available experimental resources.

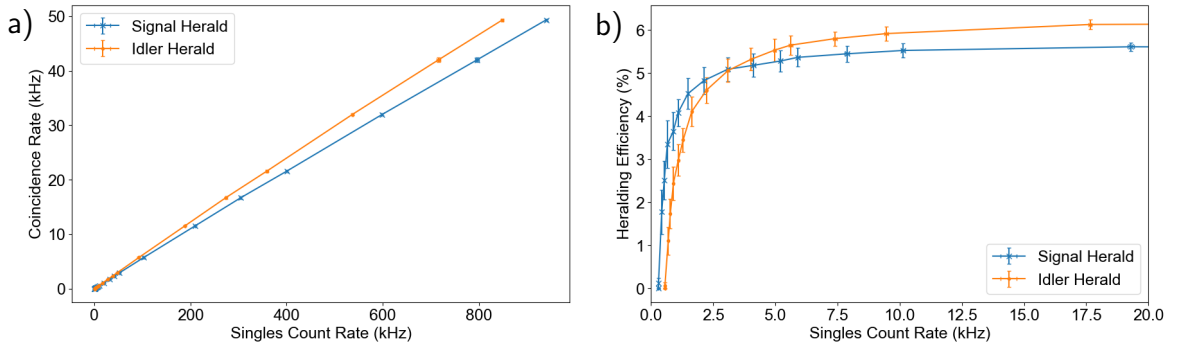


Figure 2.12: a) Coincidence rate versus single count rates with increasing pump power. The slope of this relationship determines the heralding efficiency. b) Heralding efficiency as a function of single count rate in the low pump power regime. The heralding efficiency stabilises after emerging from the noise dominated regime and reaches a value of around 5%. Legends indicate which photon was considered the herald.

2.3.3 Single Photon Quality

The EPS is characterised with respect to its single photon nature by computing the second-order correlation function of emitted pairs, denoted $g^2(\tau)$. $g^2(\tau)$ is defined as the correlations in intensity of an electric field $I(t)$ at two different times t and $t + \tau$ and is given by equation 2.4 [99].

$$g^2(\tau) = \frac{\langle I(t)I(t+\tau) \rangle}{\langle I(t) \rangle \langle I(t+\tau) \rangle} \quad (2.4)$$

At $\tau = 0$, the $g^2(0)$ becomes a measure of photon statistics. For perfectly uncorrelated light, such as photons from a coherent laser source, this equation will evaluate to exactly 1. A $g^2(0) > 1$ indicates super-Poissonian photon statistics (bunched light), whereas a value $g^2(0) < 1$ is only caused by photons with sub-Poissonian statistics (anti-bunched light). Perfect single photon sources approach $g^2(0) = 0$.

Replacing the classical intensity fields in the above equation with quantum-mechanical ladder operators leads to the $g^2(\tau)$ as a function of the heralded single photon and coincidence detection probabilities conditioned on a detection at the heralding detector:

$$g^2(\tau) = \frac{P(Q_1 Q_2 | D_1)}{P(Q_1 | D_1) P(Q_2 | D_1)} = \frac{N(Q_1 Q_2 D_1) N(D_1)}{N(Q_1 D_1) N(Q_2 D_1)} \quad (2.5)$$

Here, $P(A|B)$ refers to the probability that detector A clicks given that detector B has clicked, and $N(A)$, $N(AB)$ etc. refer to the absolute recorded number of single or coincident detections of the detector(s) in parentheses. Experimentally, the $g^2(\tau)$ was measured by setting up a heralded, three-detector version of the Hanbury-Brown-Twiss interferometer (see Figure 2.13) [100].

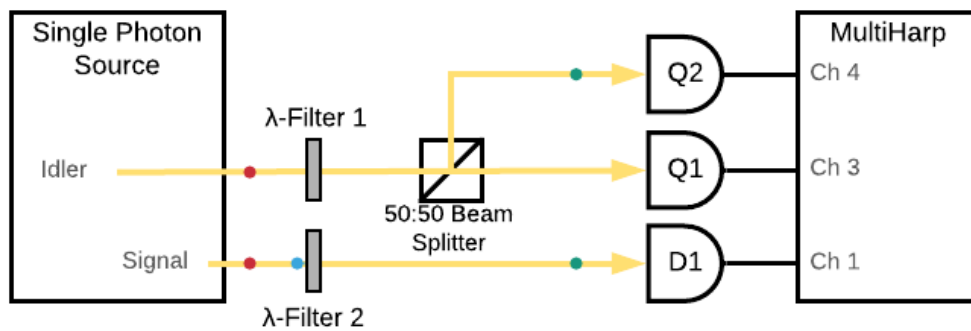


Figure 2.13: Schematic setup for the measurement of the EPS's second order correlation function, based on a heralded Hanbury Brown-Twiss interferometer. The filters select signal and idler wavelengths that correspond to entangled photons, reducing the noise due to the dichroic mismatch. Many two-fold coincidences are expected between the heralding detector D1 and each of the signal detectors Q1/2, but three-fold coincidences across all detectors are infrequent.

In this specific setup, the signal photons at D1 are used to herald the arrival of the idler photons, which can be detected by either Q1 or Q2, but not by both simultaneously. If multi-photon emissions are infrequent, triple coincidences across all three detectors at $\tau = 0$ are thus low, while twofold coincidences between the heralding and either idler detector are high. In post-processing, a varying delay is applied to the detection times received from Q1 to determine the $g^2(\tau)$ at different τ .

Using this methodology, a number of $g^2(0) \ll 1$ measurements were recorded, with the lowest achieved $g^2(0) = 0.0042 \pm 0.0009$ shown in Figure 2.14. This remarkably low value was obtained with the help of optimised detection rates, a narrow coincidence window and low source brightness, all designed to minimise the accidentals contribution.

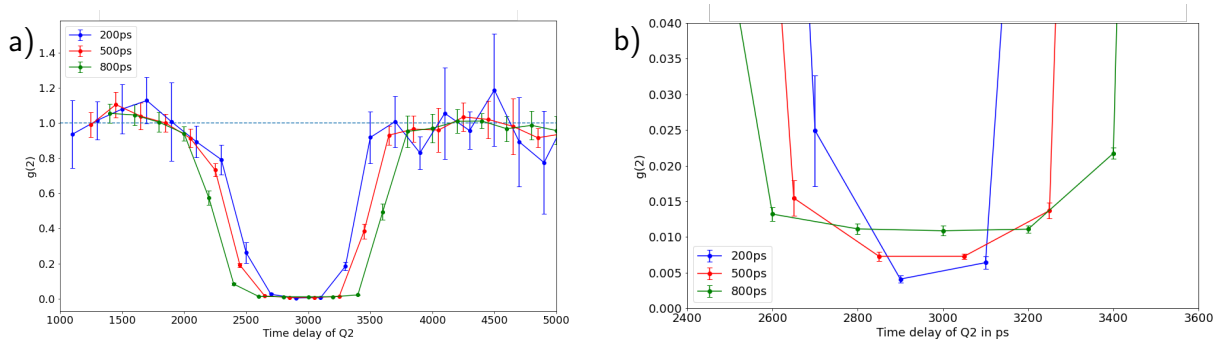


Figure 2.14: a) $g^2(\tau)$ for the EPS as measured using free-running SPADs and optimised experimental parameters with different coincidence windows applied. b) Detailed view of the $g^2(0)$, highlighting the effects of a widening coincidence window.

Experimental imperfections such as stray light, detector dark counts, and a poor heralding efficiency increase the $g^2(0)$ above the ideal value of 0 even in the absence of multi-photon emission. The g^2 elevation due to triple coincidences caused by these effects can be estimated by accounting for accidental coincidences between a two-fold coincidence and unrelated single counts on the third detector, according to Equation 2.6. As in Equation 2.5, $P(A|B)$ and $N(A)/N(AB)$ refer to the conditional probabilities and absolute counts respectively, while $R(A)$ is the detection rate in Hz and Δt is the coincidence window in seconds. Further types of accidental triple coincidences are sufficiently rare to be neglected.

$$g^{2*}(\tau) = P(Q_1|D_1)P(Q_2) + P(Q_2|D_1)P(Q_1) \quad (2.6)$$

$$= R(D_1)\Delta t \left(\frac{N(Q_1)}{N(Q_1D_1)} + \frac{N(Q_2)}{N(Q_2D_1)} \right) \quad (2.7)$$

This $g^{2*}(0)$ fully accounts for the $g^2(0)$ values found in the presented setup and thus indicates minimal multi-photon emission. It should be noted that a fair assessment of the EPS's single photon quality in a QKD context, where a high key rate is imperative, should consider the source at full brightness and with a coincidence window encompassing the entire coincidence peak. However, in the full-power QKD scenario presented in Chapter 4, the system exhibits a high entanglement fidelity, sufficiently indicating that any multi-photon contribution is still negligible.

2.3.4 Intensity Stability

Lastly, it is worth commenting on the intensity stability of the EPS as a function of time. During stable, continuous operation, the entangled pair generation rate varies slowly within $\pm 5\%$ of its average value on the scale of tens of minutes, maintaining a stable mean count rate overall (see Figure 2.15). The manufacturer's report indicates that this can be tracked back to a known residual instability in the pump laser. These fluctuations have to be accounted for when designing long, interrelated measurement series where these drifts cannot be averaged, for example by repeating a shorter cycle of measurements every few minutes.

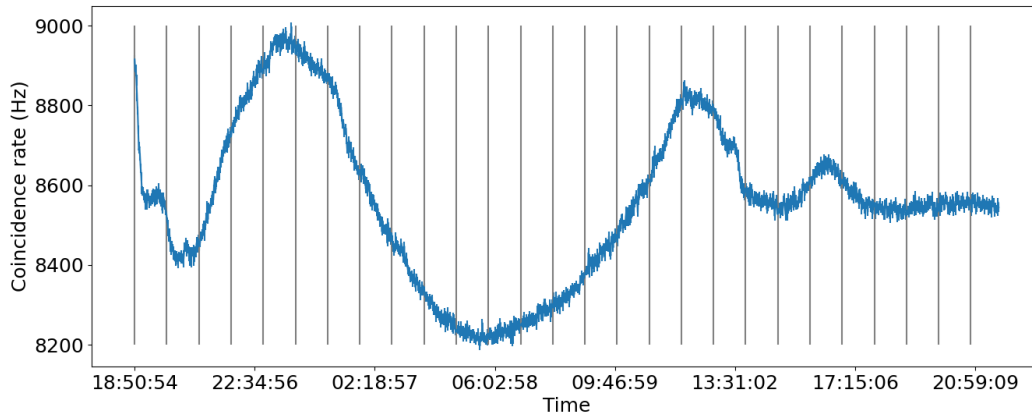


Figure 2.15: 24 hour measurement of the coincidence rate produced by the EPS under stable environmental conditions. The source had been generating entanglement for several hours prior to the measurement start.

Furthermore, during the initial 1-2 hours after turning the laser on, coincidence rates and count rates fluctuate noticeably. To investigate whether the phase-matching conditions of the crystal are the cause of this warm-up behaviour, the EPS coincidences and the resistance of a thermistor located under the interferometer are recorded simultaneously. Figure 2.16 shows that while the magnitude of the coincidence count drift is similar to what is observed in steady-state operation, the frequency of fluctuations during the first 1.5 hours is significantly higher. This coincides with the thermistor warm-up period (signified by the falling voltage across the thermistor), although the intensity fluctuations do not appear correlated to the thermistor temperature. Regardless, a 1.5 hour warm-up period for the EPS can minimise the influence of rapid intensity fluctuations on measurement results.

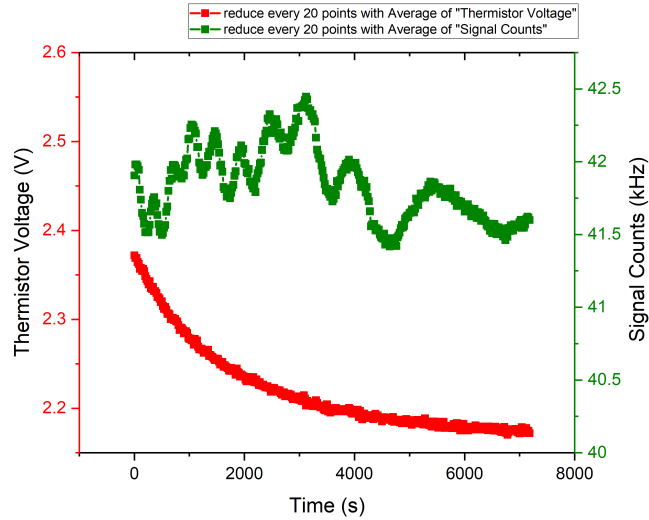


Figure 2.16: EPS coincidence rate and thermistor voltage in the period immediately following turn-on.

2.4 Software Development

2.4.1 Time Tagger Analysis Code

Time taggers are devices used to precisely timestamp photon detection events from incoming detectors against a common clock, thereby enabling time correlated analysis. Within this work, time tagging is implicitly included as part of the single-photon detection system, and is therefore not discussed separately. Two separate time taggers (distributed by different companies) are used in this thesis. Their proprietary software is not designed to record measurements with the desired parameter control, nor in a manner that is easily compatible with the laboratories other relevant instruments. Consequently, for both time taggers, an entirely new code library had to be developed to efficiently record, save, and analyse the time tags. This was done in the laboratory's most prevalent coding language, Python.

It is worth noting that almost all of the code for this thesis was developed independently and from the ground up. Recently, some effort has been made to create a common Python library termed 'Quince' that comprises all time-tagger operation and analysis code for the laboratory's three time tagger models. Quince is intended to be an exhaustive resource for the entire group, though at the time of writing, this is still a work in progress, pursued by other group members. The code used in this thesis was updated to incorporate Quince functions to be suitable for re-use in future collaborative experiments, however, all functionalities used were already present in previous versions developed entirely independently.

One challenge to this coding venture is the amount of accumulated data. Each detection event, comprising of a time tag and associated channel number, is placed in an internal buffer within the time tagger. This buffer has to be emptied efficiently to avoid loss of data, which can make it challenging to perform on-the-fly analysis. For event-rich experiments, the resulting datafiles can be large (exceeding 100 GB), even within binary format. Furthermore,

it is desirable that analysis code is independent of the physical device used in order to aid experimental flexibility. Thus the task of processing time tags is generally modularised into the following functionalities:

- Acquisition of data and saving of raw time stamps (in their innate binary format)
- Translation from binary time stamps to a universal channel/time stamp data-frame or collection of coincidences
- Evaluation of time stamps/coincidences data-frames to obtain physical values (such as count rates, coincidences, $g^2(\tau)$ etc.)

Data partitioning or preliminary sifting can be performed in the translation step to reduce file size and speed up the evaluation step, which in turn is agnostic of the device used to record the time stamps. The analysis step is thus fully device-agnostic and decoupled from the data-taking step.

During development, additional challenges were encountered with specific devices, which are outlined below:

PicoQuant 'MultiHarp 150' - This time tagger's paid-for analysis software 'QuCoa' was unsuitable to perform the required analysis. The device also offered very limited Python support at the time of purchase, and by default produced results in a proprietary file format that proved tedious to integrate with other code.

By far the most time consuming step in using this time tagger is the manual conversion of datasets from their binary format due to a quirk of the MultiHarp's time-tag incrementation that prevents efficient parallelisation. An interleaved measurement/analysis method for long measurements was adopted, where the data taking process is broken into segments and each segment is analysed while the next one is being recorded (see Figure 2.17). Additional analysis steps reduce the raw data to only the potentially relevant coincidence information, which is then saved separately. This leads to much of the analysis being performed on a massively reduced dataset, which greatly reduces computing time.

qutools 'quTAG' - On this instrument, the translation from binary to processing-ready data is straightforward, so interleaving is generally not necessary. However, the quTAG is susceptible to bugged time-stamping, requiring additional fail-safes and functionality checks. This device also offers an accessible, FPGA-based capability to immediately return coincidence information, which can easily be saved to a human-readable format. Where appropriate, this is chosen over recording the full timestamp information to obtain results in a fast and accessible manner.

2.4.2 Rotating Waveplate Controls

The final polarisation analysers developed in Chapter 3 include piezo-electrical rotational mounts for remote/automated polarisation control. The devices can be operated either manually via an interface board or in software via a USB connection and GUI. However, to utilise

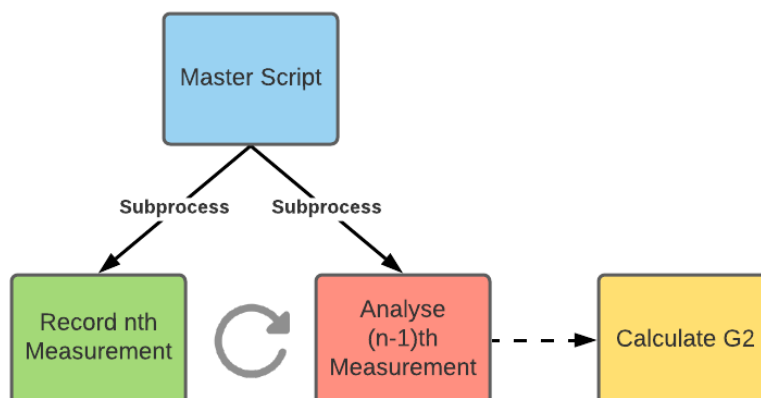


Figure 2.17: Schematic representation of how long measurements are recorded with the MultiHarp using Python scripts. A master script delegates the data acquisition and pre-analysis in segments to several subprocesses, which reduce the data to purely that of interest for analysis. Final results are extracted from the combined retained information at the end.

the waveplate mounts in scripted measurement sets, it is more convenient to bypass the GUI and control them directly through the USB connection. Commands are passed as bit strings, comprising of a 3-byte header and variable length data packages.

Deriving from the pre-existing general `ycqtinst` class (originally developed by Dr Ben-Amies King), designed for connecting with generic USB devices throughout the laboratory, all useful command-strings for the piezo mounts are wrapped in Python as part of a new 'ELL14K' instrument class. This class controls actions including connecting to a rotator at a specified port, reading the current position, rotating by a certain amount, and many more. Each waveplate is instantiated as a new object and commands are sent to the object to control/read it, so multiple rotators can easily be operated in parallel. This class integrates seamlessly into the general measurement scripts and can be expanded easily with new commands if required.

Measurements using the polarisation analysers described in Chapter 3 combine the rotating waveplate controls with detection events recorded on multiple time tagger channels, leading to a complex array of measurement variables, especially in the time-multiplexed coincidence detection scenario. Additionally, scripts for sequential measurement series produce myriad files that need to be managed efficiently. To streamline this process, a specific datafile naming convention was established and automatically implemented by measurements scripts. This convention allows the analysis files to extract relevant experimental parameters programmatically, reducing manual overhead and potential for clerical errors.

Chapter 3

Developing a QKD Receiver

The measurement of polarisation entanglement is a well-established and widely practised technique in quantum optics. A variety of different setups have been developed for this purpose in quantum communication, tailored to their specific applications. Manipulation of the polarisation states is typically achieved in free-space implementations via optical wave retarders (waveplates), Linear Polarisers (LPs), and Polarising Beam Splitters (PBSs). These components enable projection of quantum states onto the chosen measurement basis, most commonly the linear and circular bases associated with the Pauli operators (see Section 1.1.3).

This chapter details the evolution of the experimental PA setup, highlighting the motivation behind specific design choices and providing a description of the devices utilised within the experimental investigations presented in Chapters 5 & 6. Finally, the mature PAs are presented and their key physical setup metrics are assessed. This is distinct from their measurement performance, which is exhaustively demonstrated in Chapter 4.

3.1 Polarisation Analyser Requirements

For this thesis, two Polarisation Analysers (PAs) for the measurement of quantum entanglement were developed from the ground up. This system is designed to fully characterise arbitrary polarisation states and facilitate quantum communication specific research applications such as the evaluation of QKD transmitters, the investigation of transmission channels, and performance of polarisation-based QKD protocols. The setup is compatible with both prepare-and-measure schemes using single-photon polarisation states as well as entangled two-photon systems.

Several key design requirements were identified in the early stages of development, including:

- Precise and deterministic polarisation manipulation and measurement
- High extinction ratio between orthogonal states
- Low optical insertion loss
- Alignment stability and physical robustness
- Fast operation and random basis selection
- Ease of use
- Remote control and queued measurement capability

3.2 Fibre-Centric Measurement of Polarisation States

Conducting polarisation state measurements in free space provides a convenient reference frame for the definition of measurement axes — for example, the horizontal state can be defined as parallel to the optical table. Over the free-space propagation distance, the polarisation states also remain stable and any state transformations introduced by optical elements can be described deterministically. However, free-space bulk optics are susceptible to spatial misalignment, are time-consuming to set up, and incur additional coupling losses. To meet the requirement for long-term stability, the first PA model was therefore designed to minimise free-space sections and rely predominantly on fibre components.

Conversely, in optical fibre, polarisation is subject to unitary transformation induced by birefringence, which varies with temperature and mechanical stress. This birefringence can be employed for polarisation control using Manual Polarisation Controllers (MPCs). However, such control is less precise and affected by hysteresis due to the continuously changing fibre birefringence. Consequently, constant monitoring of a reference polarisation state would be required in a fully fibre-based polarisation analyser. To address this, the early PA design performs basis selection within a short free-space section, implemented using three waveplates in a miniature, pre-assembled, optical fibre bench, referred to as the U-bench. Fibre benches exhibit high alignment stability based on their solid structure, with this U-bench maintaining

3.2. FIBRE-CENTRIC MEASUREMENT OF POLARISATION STATES

a collimation/coupling efficiency of $\sim 80\%$ for both ports. They allow for different optical components to be placed in the free-space path with similar stability and in many cases without disturbing the alignment.

This prototype PA consists of the previously described U-bench for polarisation control and a fibre-coupled polarising beam splitter that performs the polarisation measurement by splitting any incoming polarisation state into orthogonal components. Figure 3.1 shows the full setup used to measure entanglement from the EPS, including the polarisation analysing elements. Within the U-bench, the photons propagate in free-space over a distance of approximately 5 cm, during which they pass through a sequence of a half-waveplate (HWP, $\frac{\lambda}{2}$ -plate) and two quarter-waveplates (QWP, $\frac{\lambda}{4}$ -plate) in the arrangement of QWP-HWP-QWP. This configuration represents the standard setup for arbitrary polarisation manipulation, as it allows full unitary control over an arbitrary polarisation state. As such, these waveplates can be used to simultaneously compensate for the birefringence of the channel and project the state into a known measurement basis aligned with the fibre-based PBS. Initial polarisation alignment is performed by setting the EPS to emit the linear $|HH\rangle$ -state, removing all waveplates from the U-bench and placing them in one-by-one to recover a linear state on the polarising beam splitter. Then, by rotation of the waveplates, deterministic measurements can be taken.

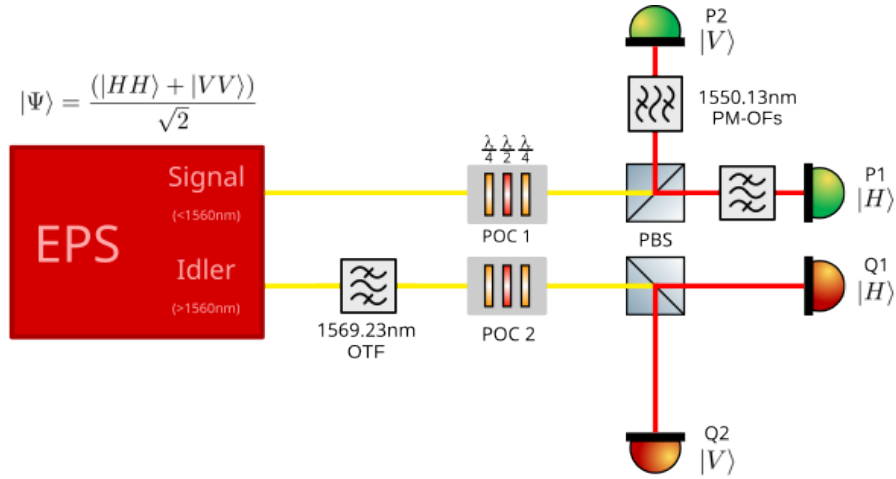


Figure 3.1: Schematic representation of the first Bell test setup. All components except the Polarisation Controller (POC) benches are fibre-based, red and yellow lines denote polarisation maintaining fibre and single mode fibre respectively. The idler photons are filtered by the OTF, selecting 1596.23 ± 0.40 nm wavelength immediately after exiting the source. Based on component availability, the matching signal photons were isolated by two polarisation maintaining optical filters (PM-OFs) after the PBS, selecting 1550.13 ± 0.50 nm.

Using this setup, first attempts at measuring polarisation entanglement were made as explained in Section 4.3. The resulting polarisation correlation curves, shown in Figure 3.2, indicate the presence of quantum entanglement based on the visibility extracted from fitted sinusoidal curves as listed in Table 3.1. Generally, an average visibility $\geq 70.7\%$ [101] in two orthogonal bases is evidence of quantum entanglement, with modern implementations routinely achieving visibilities $\geq 90\%$.

The described experimental setup is therefore capable of demonstrating polarisation entanglement. However, the visibility of observed correlations can be significantly improved. The

3.3. POLARISATION STATE COLLAPSE IN FREE SPACE

Basis	Visibility	
	$ 00\rangle / 01\rangle$	$ 11\rangle / 10\rangle$
$\mathbb{Z}$	87.3%	92.0%
$\mathbb{X}$	64.2%	84.1%
$\mathbb{Y}$	67.6%	81.6%

Table 3.1: Absolute visibilities of polarisation correlations observed based on the fitted entangled state coincidences from the EPS.

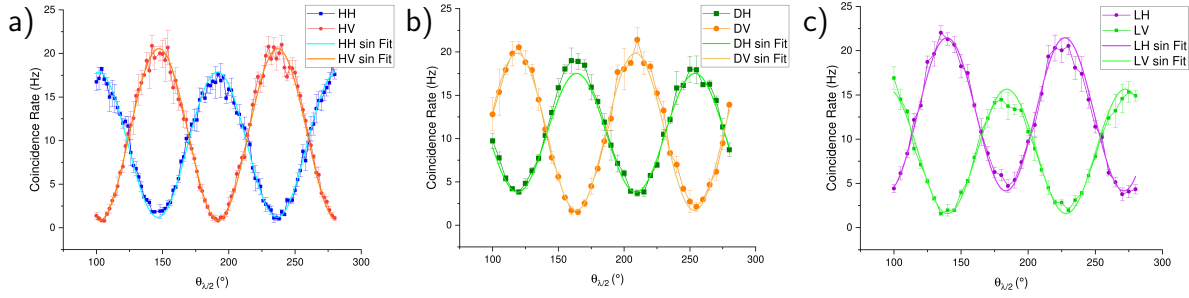


Figure 3.2: Correlation curves of coincidences between signal photons in a fixed basis and the idler photon rotating along the Poincaré sphere via rotation of the HWP by the angle $\theta_{\lambda/2}$ in $^\circ$. The legend refers to the starting polarisation states of both photons. a) Signal photon aligned to $|H\rangle$, idler photon tracing through all linear polarisation states on the Poincaré sphere equator. b) Signal photon is aligned to $|D\rangle = |+\rangle$, idler photon tracing through all linear polarisation states on the Poincaré sphere equator. c) Signal photon is aligned to $|L\rangle$, idler photon tracing through rectilinear and circular states along the Poincaré sphere sagittal plane.

most probable reason for the reduced visibility is the section of single-mode fibre connecting the U-bench coupling port to the PBS. Birefringence in this fibre introduces an unknown polarisation transformation, leading to a misalignment between the measurement reference frame and the intended rotation, even after an initial linear reference state has been aligned. As a result, precise control over the projective measurements is compromised.

3.3 Polarisation State Collapse in Free Space

To mitigate the effect of an unknown polarisation reference frame misalignment between the controlling and collapsing elements, the polarisation measurement has to be incorporated into the free-space section of the PA, thereby preserving reference frame alignment and allowing full control over the measured state.

The previously employed U-bench was too small to house free-space components for both polarisation control and measurement simultaneously. Switching to a longer fibre-bench however proved incompatible with the current collimators due to their limited collimation length. Ultimately, a new fibre-bench base plate, slightly longer than the first iteration but still within the collimation range, could be fitted with one HWP, one QWP and interchangeably either a PBS or LP. Figure 3.3 shows this PA with the two waveplates and an LP in place.

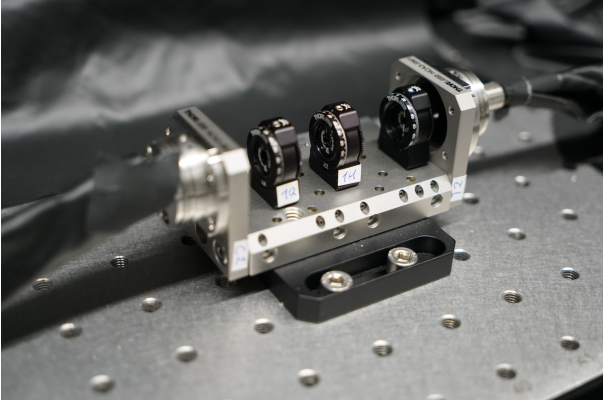


Figure 3.3: A photograph of the revised PA in free space. The U-bench contains a QWP, a HWP and a LP in series. An in-fibre MPC is used to align the incoming polarisation state with the LP before inserting the desired waveplates.

Removal of the initial QWP required that the polarisation state entering the PA is aligned to a linear state in order to maintain full control over the projection. This necessitated the inclusion of a fibre-based MPC in front of each PA, which can be used to compensate for any channel birefringence. Due to the spatial restrictions on the short fibre-bench, it was not possible to utilise the reflected output of the PBS. Consequently, measurements can only be performed for a single state at a time and its orthogonal complement must be recorded separately.

This PA setup maintained high coupling efficiencies of $\geq 70\%$ per port and measured average polarisation correlation visibilities

$\geq 93\%$ in all three Pauli-bases, demonstrating that the placement of the polarisation state collapse in free-space succeeded in significantly improving the accuracy of the induced polarisation state projection. The experiment presented in Chapter 5 uses this implementation of the PAs to successfully conduct experiments on coexistence of classical data traffic and quantum signals in optical fibre infrastructure, achieving visibilities of similar magnitude.

Despite the favourable performance of these PAs, their scalability is limited by the fact that only a single polarisation state can be measured at a time. In practice, this constraint complicates investigations that require numerous projective measurements, such as evaluations of the CHSH inequality or full quantum state tomography.

3.4 Dual Polarisation Output and Motorised Waveplates

The next iteration of the PAs incorporated several hardware upgrades. An additional output coupling port was introduced to capture the reflected beam from the PBS. This modification necessitated both a larger fibre-bench base plate as well as matching longer focal length collimators, achieving $>70\%$ simultaneous coupling efficiency. Linear polarisers were inserted after the PBS to provide a high polarisation extinction ratio of around 30 dB, while anti-reflection-coated fibres enhance the coupling efficiency. Furthermore, the achromatic waveplates placed in the fibre-bench were replaced with zero-order waveplates mounted in motorised, piezo-electronic rotational stages, enabling automated and precise control over the applied polarisation transformations. Since the piezo-mounts are not compatible with fibre-bench architecture, they were integrated into an alignment-maintaining cage system positioned at the input of the fibre-bench, with the QWP preceding the HWP. Figure 3.4 shows the resulting PA configuration.

3.4. DUAL POLARISATION OUTPUT AND MOTORISED WAVEPLATES

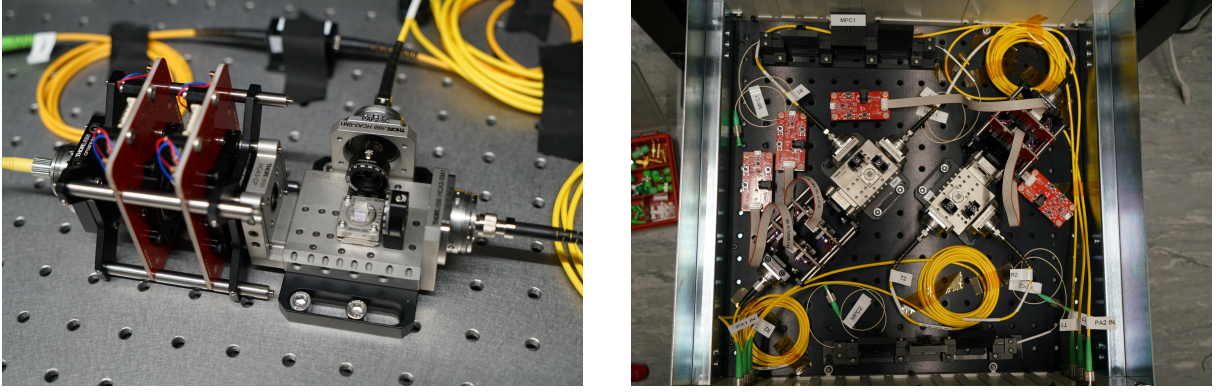


Figure 3.4: PAs with motorised waveplates and two output couplers. The cage-mounting ensures alignment stability and contains a QWP followed by a HWP for exhaustive polarisation control when starting with a linear state. The right image shows the PAs packed into a rack-mounted drawer for transport and deployment in the UK-IE field trial.

In addition to making experiments involving a large number of different measurements more convenient, simultaneous monitoring of both PBS outputs provides an additional benefit during the initial alignment of the entangled state's generation reference frame with that of the PAs. The unitary transformation applied by the transmission channel involves a free parameter that has not yet been discussed, namely the relative phase difference φ . The general form of a $|\Phi_{\varphi}^{+}\rangle$ Bell-state includes a relative phase between the orthogonal polarisation components:

$$|\Phi_{\varphi}^{+}\rangle = \frac{|HH\rangle + e^{i\varphi}|VV\rangle}{\sqrt{2}} \quad (3.1)$$

As detailed in Appendix A, this phase difference φ must be appropriately compensated to maintain the expected polarisation correlations in the $\mathbb{X}$ and $\mathbb{Y}$ bases. However, the phase difference is not visible at all in the $\mathbb{Z}$ basis, where the initial polarisation alignment is performed, nor can φ be deterministically manipulated with the given MPCs. In the absence of dedicated phase-compensation components, the correct compensation can therefore only be identified by trial and error: varying the MPCs and recovering $\mathbb{Z}$ basis alignment until the expected correlations are observed in all three bases. This process is significantly accelerated when both basis eigenstates can be monitored simultaneously, allowing the relevant minimum and maximum polarisation correlations to be observed within a single measurement. Furthermore, the use of motorised waveplates enables rapid and precise switching between different measurement bases, eliminating the need for manual adjustment and further reducing polarisation alignment time.

The rotational mounts are controlled via command strings transmitted over a USB connection to the control board. A Python wrapper class was developed (as discussed in Section 2.4.2) to integrate waveplate readout and control into the general experimental software. This modification thus enables fully automated operation and, following the initial physical polarisation alignment, entirely remote execution of a wide range of measurement sequences. For example, CHSH measurements, quantum state tomography, and long-term stability tests can be scheduled and performed without further manual intervention.

3.4. DUAL POLARISATION OUTPUT AND MOTORISED WAVEPLATES

As mentioned above, the previously employed achromatic waveplates were replaced with zero-order waveplates optimised for a wavelength of 1550 nm. Although the EPS is centred at 1560 nm and, as discussed in Section 2.3.1, the idler photons are intentionally filtered at 1570 nm, the use of zero-order waveplates nonetheless results in reduced rotational errors during polarisation manipulation.

This can be understood from the wavelength-dependence of the retardance. Achromatic waveplates exhibit a retardance that is slightly below the ideal value over a broad wavelength range, whereas the zero-order waveplates achieve the exact retardance at their design wavelength but deviate more rapidly away from it. Crucially, a wavelength offset of up to 25 nm does not introduce a retardance error exceeding the intrinsic deviation of the achromatic waveplates. Consequently, the transformation applied to the idler remains comparably accurate, while the transformation of the signal at 1550 nm is significantly improved. This behaviour was modelled based on the wavelength-dependent retardance values provided in the manufacturer's data sheets for both waveplate types, shown in Figure 3.5, and subsequently verified experimentally at 1550 nm using a laser source and polarimeter.

This version of the setup was deployed during the UK-IE field-trial, which is the subject of Chapter 6, and was intended for use in the investigation of entanglement distribution over a 224 km submarine fibre link. However, due to unexpectedly high noise levels encountered during the trial, it was ultimately not utilised for measurements. Nevertheless, the system was transported to the experimental site and installed, providing an opportunity to assess its optical alignment stability.

Remarkably, after transport over 175 km by van, the transmitted output of the PBS remained aligned with a coupling efficiency above 60% and could be restored to above 70% with minor adjustments in less than 20 minutes. The reflected PBS beam could not be evaluated, as the PBS on its fibre-bench mount cannot be reliably locked in place and was intended to be aligned on-site. This stress-test demonstrates the robustness and stability of the PAs, confirming that these key design objectives were successfully achieved.

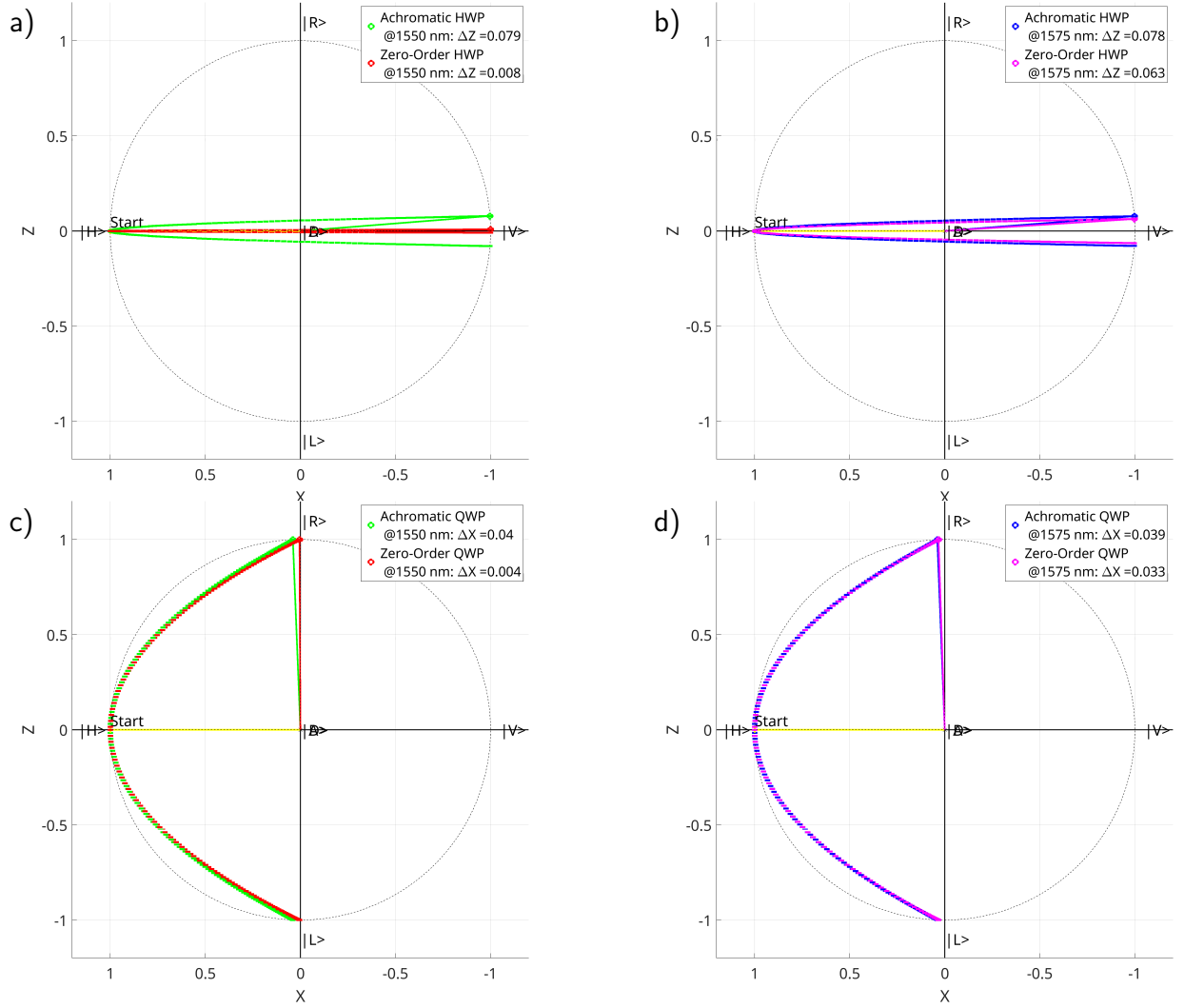


Figure 3.5: Simulation of rotation effected by achromatic vs zero-order waveplates for a) 1550 nm light through a HWP, b) 1575 nm light through a HWP, c) 1550 nm light through a QWP, and d) 1575 nm light through a QWP. Each plot includes the maximum error produced by the respective waveplate when measuring an eigenstate in the most affected basis ($\Delta X, \Delta Z$), which even at 1575 nm favours the zero-order waveplate.

3.5 Passive Basis Selection for QKD

The last major revision of the PA design involved tailoring the setup specifically for QKD applications. Although the motorised rotational mounts enable switching between measurement settings on millisecond timescales, which is sufficient for investigative measurements, QKD protocols require a randomly selected measurement basis for every individual photon. A straightforward solution to implement this employs a 50:50 polarisation-insensitive Beam Splitter (BS), with each output arm configured to measure a distinct basis. This approach is widely used (see Pirandola *et al.* [40], Section X.4) and referred to as passive basis selection, as it eliminates the need for actively switched components. Consequently, the resulting PAs function as passive QKD receivers.

In the PAs, passive basis selection was implemented by introducing a 50:50 BS cube and duplicating the waveplate–PBS–LP–fibre coupler assembly, so that there is an equivalent measurement path behind each BS output. This modification substantially increases both the complexity and physical size of the setup, as can be seen in Figure 3.6. In this configuration, a single input collimator defines the free-space input beam, which is subsequently split into four paths that each must be coupled into separate output fibres over a propagation distance approaching the collimation limit. Because the alignment of all four couplers is governed by the same collimator, optimising the simultaneous coupling efficiency is technically challenging. Special receiver fibres with a Thermally Expanded Core (TEC) were therefore employed to increase the mode field diameter of the receiving fibres, enabling simultaneous coupling into all four outputs with satisfactory efficiency. Both the basis-selecting beam splitter and the polarising beam splitters are glued in place after alignment to ensure optical stability.

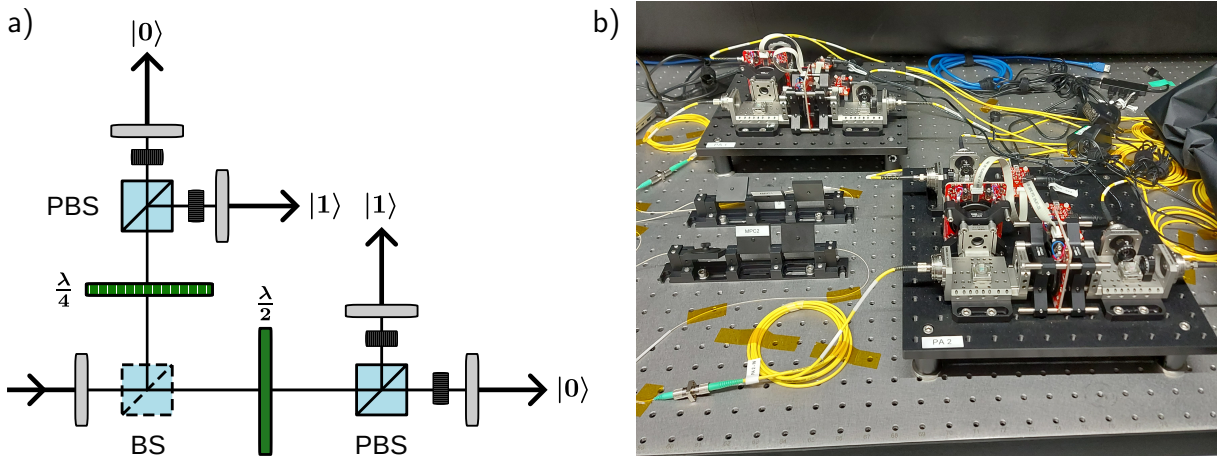


Figure 3.6: Final polarisation analyser design in a) schematic and b) image. Photons are projected into the chosen measurement basis via the HWP ($\frac{\lambda}{2}$) and QWP ($\frac{\lambda}{4}$), and polarisation measurement is performed at the two PBSs. LPs are used to enhance the polarisation extinction ratio of the PBSs. The BS performs random basis choice, so that the PAs can act as passive receivers in a QKD protocol.

The final PAs comprise three fibre benches, interconnected via cage-mounted rotators. Each PA has two arms: one for the photons transmitted through the BS, and one for those reflected. The transmitted arm contains a HWP, and the reflected arm contains a QWP. The choice of this waveplate configuration represents a compromise between polarisation control, space restrictions imposed by the maximum collimation length, and minimisation of optical losses. By employing a fibre-based MPC upstream of the PA, the input polarisation can be prepared in a linear state. In the HWP arm, this enables access to all linear polarisation projections, including measurements in the $\mathbb{Z}$ and $\mathbb{X}$ bases. In the QWP arm, measurements can be performed in the $\mathbb{Z}$ and $\mathbb{Y}$ basis, as well as in elliptical states obtained through rotation of a QWP.

This PA design enables simultaneous, continuous bit generation in any two Pauli bases for QKD protocols; determination of CHSH parameters from two waveplate settings; and full two-qubit quantum tomography using three measurement configurations (see Chapter 4 for demonstrations). It therefore balances experimental flexibility (supporting applications such as QKD demonstrations, quantum state characterisation, and transmission monitoring) and a compact, stable implementation constrained by the available collimation optics.

3.6 Detection Output Time-Multiplexing

The two PAs provide a total of eight output ports. However, only four IR-SNSPD channels are available in the EQC laboratory. Entanglement-based measurements require the simultaneous utilisation of both PAs, so the two detection outputs corresponding to each measurement basis are multiplexed into a single optical fibre using a fibre coupler. While this introduces an additional 3 dB of attenuation, it also reduces the required number of detectors to four and thus enables the employment of the high-performance SNSPDs. A photograph of this configuration is shown in Figure 3.7, and a schematic in Figure 3.8 a).

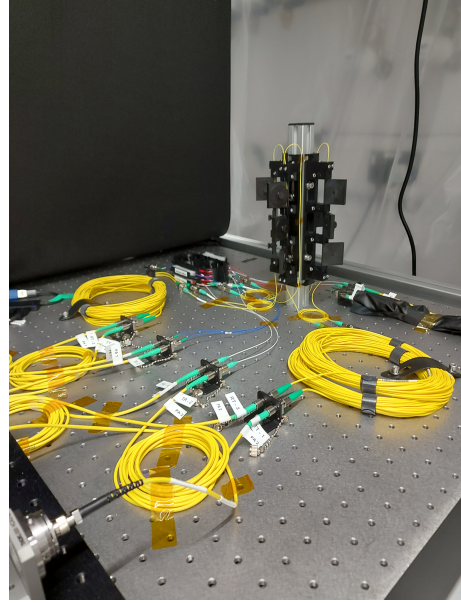


Figure 3.7: Experimental setup combining two PA outputs into one fibre and simultaneously aligning each polarisation state with the SNSPD's preferred axis. Additional fibres introduce appropriate relative delays, so that bit-values can be identified.

To distinguish events originating from different PA outputs, fibre delay lines are introduced immediately before and after the PA collimators to create characteristic time delays between the two output ports of a given PBS measurement. Since the entangled photon pairs are generated via SPDC from a CW laser, there is no external timing reference that can be used to assign absolute event times. Consequently, detections must be analysed relative to their partner photon, with the relative arrival time providing the information required to infer the measured two-photon state. Figure 3.8 b) and Table 3.2 summarise the nominal fibre delays and corresponding coincidence times for each bit combination. Real coincidence times differ by a few nanoseconds from these conceptual values due to small variations in fibre lengths, as well as the inclusion of MPCs. However, these variations are sufficiently small compared to the required time separations.

Bit Combination	Fibre Length ΔAB	Time ΔAB
$ 01\rangle$	0 m	0 ns
$ 00\rangle$	20 m	100 ns
$ 11\rangle$	25 m	125 ns
$ 10\rangle$	45 m	225 ns

Table 3.2: Fibre length and resulting time delta between different output combinations on the PAs.

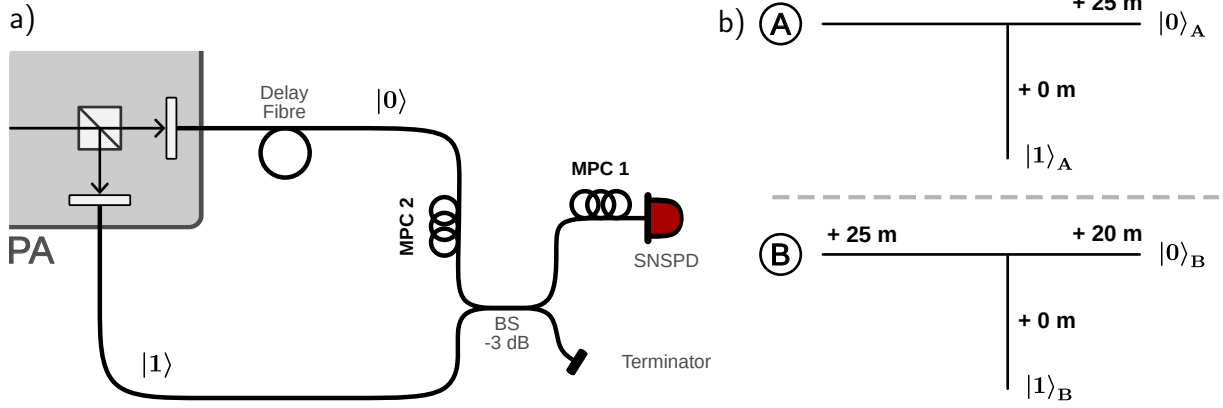


Figure 3.8: a) Schematic representation of the multiplexed detection outputs, visualising the delay fibre and SNSPD polarisation alignment via MPCs. b) Diagram indicating the delay lengths applied to each detection state. Delay fibres are added immediately before and after the PA collimators. The displayed intersection represents the polarisation measurement conducted at a PBS. Both arms on each individual PA are delayed identically.

The delay between coincidence events involving the same bit value is chosen to exceed the recovery time of the SNSPD (~ 70 ns). If this condition is not satisfied, subsequent detection events may occur during the detector dead time and therefore go unregistered. This would lead to a systematic suppression of later coincidences and a resulting bias in the measured quantum state statistics towards earlier events. In a QKD context, such a bias constitutes a potential security vulnerability, as it could theoretically be exploited by an eavesdropper to gain information about the secret key.

Additionally, the output states of each PA port are orthogonally polarised with respect to each other, which conflicts with the SNSPD system's polarisation dependent sensitivity. In order to enable the detection of both states using a single SNSPD channel with optimised detection efficiency, an additional fibre-based MPC (MPC 2 in Figure 3.8 a)) is added to the $|0\rangle$ path as shown in Figure 3.8 a). Since the SNSPD MPC station affects both incoming states, the alignment procedure must be performed sequentially. First, the $|0\rangle$ state is temporarily blocked in free-space and the SNSPD MPC (MPC 1 in Figure 3.8 a)) station is used to align the $|1\rangle$ state. Then, the $|1\rangle$ state is blocked and the additional MPC is used to optimise the $|0\rangle$ state, leaving the previously aligned state unaffected. This procedure ensures that both states are individually optimised for maximum SNSPD detection efficiency.

As discussed previously, due to the multiplexing scheme, the arrival times of both detection events at Alice and Bob must be jointly known in order to identify the measurement outcome. This introduces a complication in QKD scenarios, where this information cannot be securely exchanged without compromising the security of the key. The setup presented in Chapter 4 therefore does not constitute a fully secure QKD implementation. However, maintaining comparable experimental performance, the detection events at Alice and Bobs could be fully decoupled either by employing eight independent detectors, or by using a pulsed entangled-photon source, which would require a global timing reference for correlating measurement outcomes. It is therefore appropriate to regard the results presented in Chapter 4 as a valid experimental demonstration of QKD functionality, with limitations arising solely from the detection architecture rather than the underlying transmitter or receiver performance.

3.7 Passive Receiver Characterisation

The following sections present measurements of the coupling efficiencies of the PAs, as well as their optical and polarisation alignment stability. These results represent the physical performance of the PAs, while their functionality in polarisation measurements and their applicability to entanglement-based experiments are discussed in Chapter 4.

3.7.1 Coupling Efficiency/Attenuation

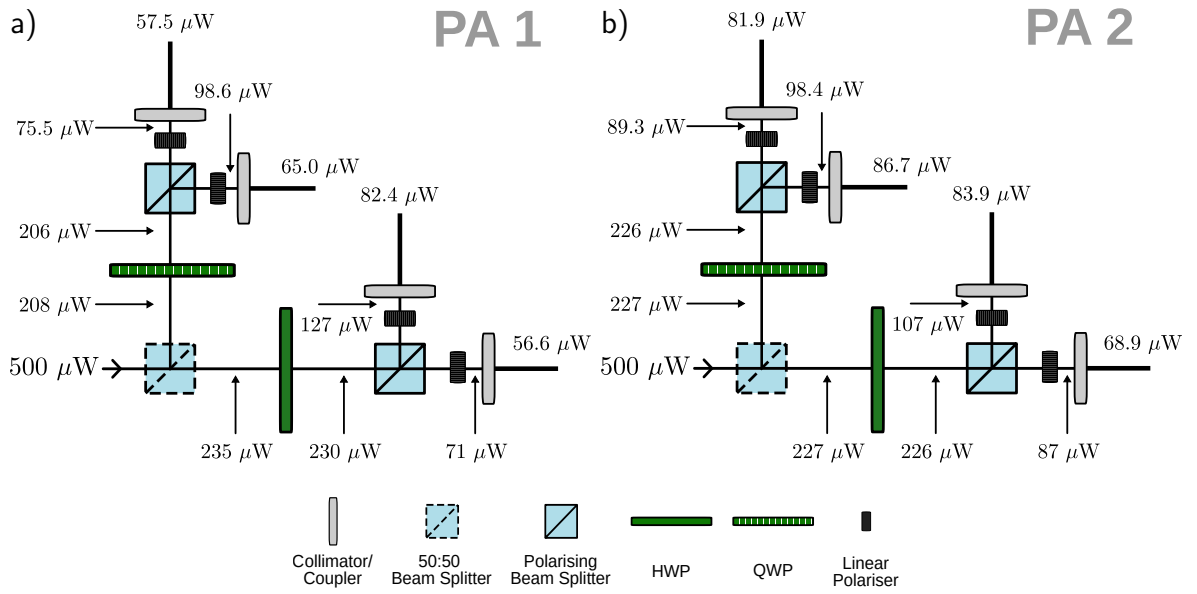


Figure 3.9: Schematic representation of the power transmitted through the PAs and losses experienced at each optical component. Due to space restrictions, measurements could not be taken between the PBSs and LPs.

Figure 3.9 shows a map of the splitting ratios and insertion losses as measured with a 1550 nm laser source and power meter. Values after the couplers correspond to the coupled power measured in fibre. For this measurement, the polarisation state of the input light was aligned with the horizontal state of the PBS's, then, the HWPs and QWPs were used to rotate the laser light to $|+\rangle$ and $|R\rangle$, so that each output is illuminated equally. Table 3.3 summarises the cumulative insertion losses for each output, excluding the 3 dB incurred by the PBS. The biggest losses are caused by the LPs, which are necessary for a high polarisation contrast, as the PBSs' reflected ($|V\rangle$) output still contains around 5% $|H\rangle$ light as per specifications. Coupling efficiencies are calculated between the power in free space immediately preceding the coupler and the output of the TEC fibre. These coupling values exhibit minor fluctuations over time, but have proven to be stable on average over several months. After three months of inactivity, all outputs exhibited coupling efficiencies above 60%, demonstrating long-term stability, therefore achieving one of the central design objectives.

PA & Coupler	Coupling Efficiency	Insertion Loss
PA1 - HWP, T	79.7 %	6.45 dB
PA1 - HWP, R	65.0 %	4.82 dB
PA1 - QWP, T	76.2 %	6.38 dB
PA1 - QWP, R	65.9 %	4.04 dB
PA2 - HWP, T	79.2 %	5.60 dB
PA2 - HWP, R	78.1 %	4.74 dB
PA2 - QWP, T	83.3 %	4.85 dB
PA2 - QWP, R	88.1 %	4.60 dB

Table 3.3: Coupling efficiencies and insertion losses for the two PAs. Insertion losses do not include the intentional 3 dB removed by the PBS. Coupling efficiencies are calculated between the power in free space immediately preceding the coupler and the output of the TEC fibre.

3.7.2 Setup Stability

Figure 3.10 illustrates the stability of the final receiver setup. Both the coupling efficiency and the polarisation alignment remain stable over timescales of several days under typical laboratory conditions. It has been observed that even after extended periods of inactivity, the system retains near-optimal optical alignment. In multiple instances, the analysers were operated without the need for realignment after several weeks, and in some cases even after months of inactivity. This level of stability makes the PAs well-suited for long-term measurements, such as quantum measurements with low coincidence rates that require data to be accumulated over several hours (see 6), as well as extended QKD demonstrations.

This chapter has presented an overview of the development of a set of PAs intended for use in quantum communication research. The final devices are shown to be robust and stable with respect to optical and polarisation alignment, while introducing minimal insertion loss and maintaining a high extinction ratio between orthogonal polarisations. They are also capable of utilising the high-performance SNSPD system despite the limited availability of IR-channels. The next step is to integrate these PAs with the EPS characterised in Chapter 2 to realise a complete entanglement system, and to perform entanglement measurements and QKD demonstrations, as will be explored in the next Chapter 4.

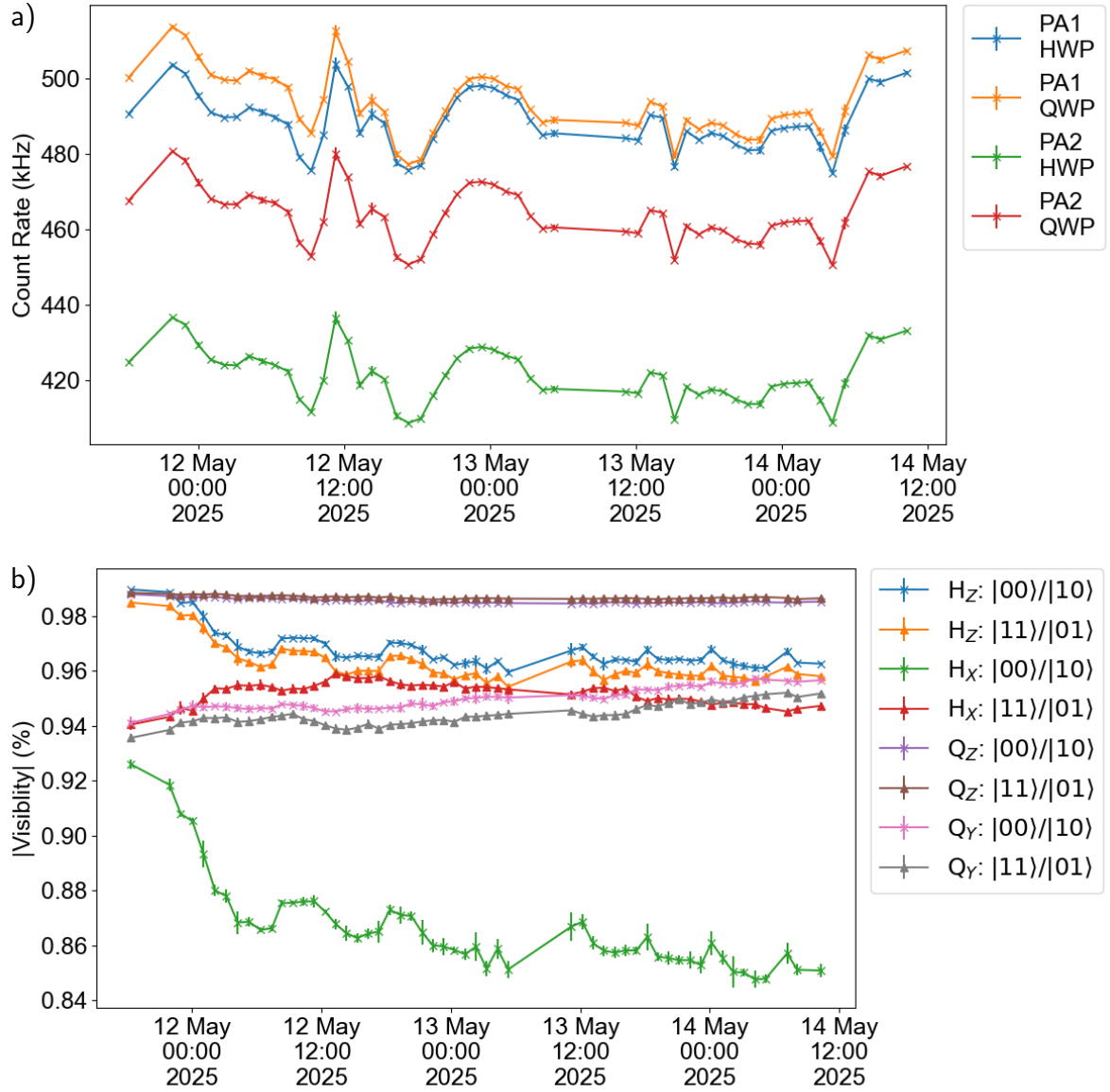


Figure 3.10: a) Count rate stability over several days as measured with the EPS and PAs. b) Stability of absolute polarisation correlation visibility over several days. Visibilities are computed for coincidences on equivalent PA arms (i.e., both HWP or both QWP paths). Apart from a small initial drift in correlated visibility of the X basis, good stability of the polarisation state is present throughout both measurements. Variations in single photon count rates are consistent with the source laser stability (see Figure 2.15).

Chapter 4

Polarisation Entanglement System for Quantum Key Distribution

This chapter combines the entanglement source characterised in Chapter 2 and polarisation analyser developed in Chapter 3 into a comprehensive polarisation entanglement system for QKD investigations. It details how the Polarisation Analysers (PAs) can be used for efficient polarisation state characterisation of a two-photon state, covering measurements of simultaneous polarisation states, assessment of an entanglement witness in the form of CHSH-type inequalities, and full-state quantum tomography. Finally, the system's QKD capabilities are demonstrated by measuring its QBER, estimating secret key fractions for BBM92 and DI-type protocols, predicting distance-scaled secret-key rates, and finally distilling a cryptographic key.

4.1 Experimental Setup

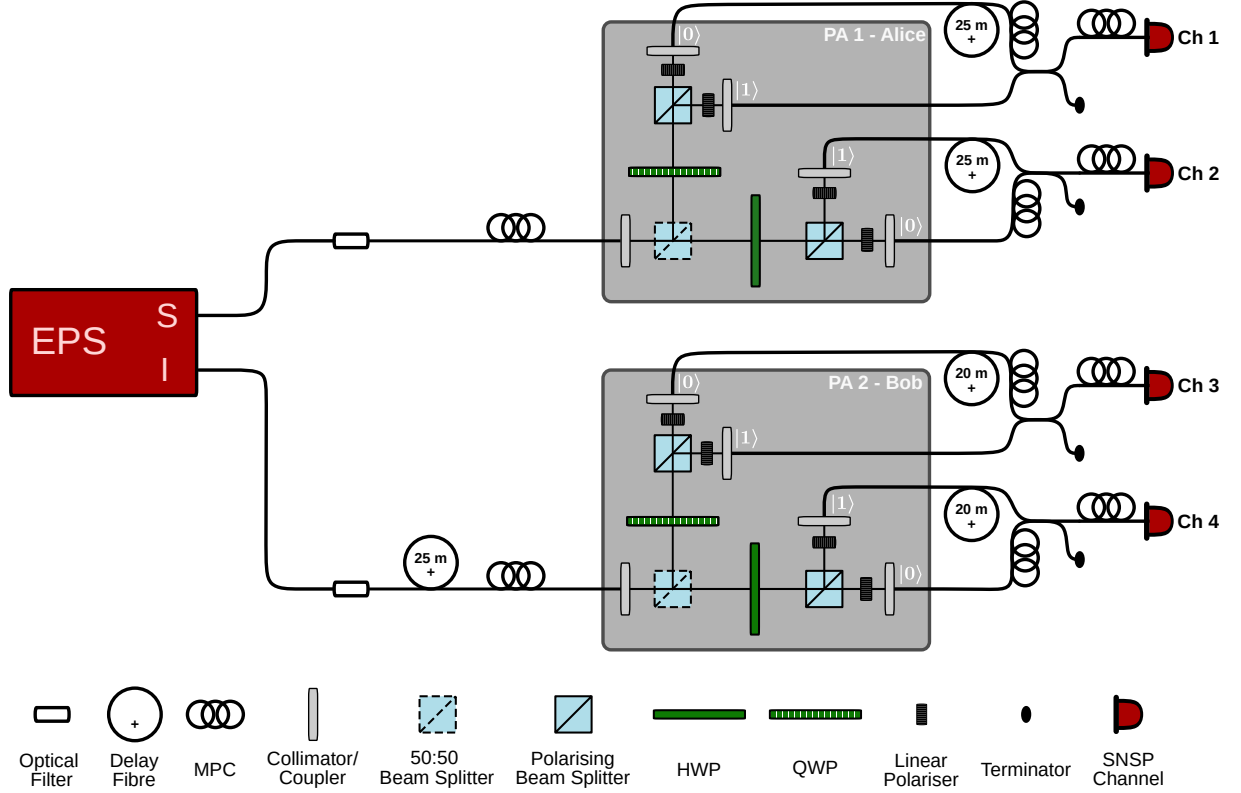


Figure 4.1: Schematic of the complete entanglement system used throughout the chapter. The optical filters are centred at 1550.1 nm for the signal photons and at 1569.3 nm for the idler photons, both with a total bandwidth of 1.39 nm. SNSPDs and a coincidence window of 150 ps were used for all measurements.

Figure 4.1 shows a schematic representation of the complete entanglement system as it was used throughout this chapter. Before all measurements in this section, the polarisation reference frame of each receiver was aligned with that of the source and transmission channel by sending a linear state through the entire setup with all waveplates in their neutral position, and varying an MPC before the receivers until the linear state was recovered. To determine the relative phase within the $|\Phi^+\rangle_\varphi$ Bell-state, an additional check on the entangled signal in the $\mathbb{X}$ - and $\mathbb{Y}$ -bases was performed and continuous adjustments to the MPCs were made until each basis showed a linear eigenstate.

Using the fully developed passive receivers, it is possible to visualise polarisation measurements in multiple bases simultaneously in real time. This means that compensation for the unknown unitary transformation applied by the intermediate channel is now much more practical than previously. The relative phase between the entangled components can be tracked while applying rotations, although some trial and error in appropriate compensation is still involved.

4.2 Visibility of Polarisation Correlations

The visibility of orthogonal polarisation correlations can easily be recorded on the PAs in all three Pauli bases by setting the waveplates to the angles θ listed in Table 4.1, with any two bases available for simultaneous measurement on one PA. Recall that the EPS produces the Bell-state $|\Phi^+\rangle = \frac{|00\rangle + e^{i\phi}|11\rangle}{\sqrt{2}}$, representable using the three orthogonal Pauli eigenstates:

$$|\Phi^+\rangle_Z = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}} \quad (4.1)$$

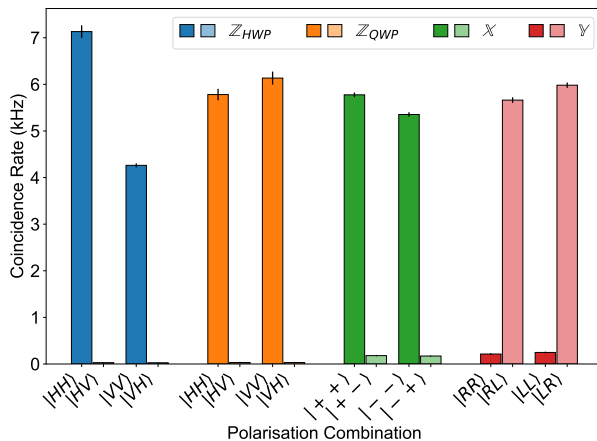
$$= |\Phi^+\rangle_X = \frac{|++\rangle + |--\rangle}{\sqrt{2}} \quad (4.2)$$

$$= |\Phi^+\rangle_Y = \frac{|RL\rangle + |LR\rangle}{\sqrt{2}} \quad (4.3)$$

Table 4.1: PA waveplate fast-axis angles θ relative to the horizontal axis of the corresponding PA PBS required to project into the three Pauli bases

HWP		QWP	
Basis	θ	Basis	θ
$\mathbb{Z}$	0°	$\mathbb{Z}$	0°
$\mathbb{X}$	22.5°	$\mathbb{Y}$	45°

Therefore, maximum correlations are expected in the $\mathbb{Z}$ and $\mathbb{X}$ bases and maximum anti-correlation in the $\mathbb{Y}$ basis (assuming appropriate phase compensation so that $\phi = 0$). Experimentally, this can be measured in two steps using the passive receivers. Both arms are capable of measuring in the $\mathbb{Z}$ -basis with the waveplates in their neutral positions; furthermore, the HWP arm can shift to the $\mathbb{X}$ -basis, and the QWP arm can shift to the $\mathbb{Y}$ basis. The exact numerical results will depend on environmental factors including background noise, detector DCR and precision of the channel compensation. Figure 4.2 gives one set of illustrative results. Generally, visibilities $>90\%$ are consistently achieved in all three bases simultaneously.



Basis	Visibility (%)	
	$ 00\rangle / 01\rangle$	$ 11\rangle / 10\rangle$
$\mathbb{Z}_{HWP}$	99.20 ± 0.11	98.78 ± 0.17
$\mathbb{Z}_{QWP}$	98.91 ± 0.10	98.99 ± 0.08
$\mathbb{X}$	93.98 ± 0.32	93.82 ± 0.23
$\mathbb{Y}$	-92.72 ± 0.47	-92.05 ± 0.40

Figure 4.2: Visibility of polarisation correlations for the EPS. Note that here, the kets in the table do not refer to computational basis qubits, but simply denote parallel or orthogonal polarisation states (hence the negative correlation in the $\mathbb{Y}$ -basis). The $\mathbb{Z}$ -basis measurement is given as measured in both the HWP and QWP arm. In practice, an average of both values may be used in any further calculations and QKD applications.

4.3 Polarisation Correlation Curves

In the discussed physical setup, the two entangled photons a and b in each pair travel separately towards the two PAs. Within the PAs, each photon randomly travels along a path where it undergoes transformation through either the HWP (H) or QWP (Q). By applying the unitary transformations $U_{H,Q}^{(a,b)}$ enacted by the waveplates respectively at angles θ_a, θ_b to the $|\Phi^+\rangle$ Bell-state, the following angle-dependent $|\Phi_{ab}^+(\theta_a, \theta_b)\rangle$ Bell-states after passing through any of the possible waveplate combinations can be determined. Consult Appendix B for a step-by-step derivation of all expressions in this section.

$$U_H^{(a)} U_H^{(b)} |\Phi_{ab}^+\rangle = \frac{1}{\sqrt{2}} [\cos 2(\theta_a - \theta_b) |0\rangle_a |0\rangle_b - \sin 2(\theta_a - \theta_b) |0\rangle_a |1\rangle_b + \sin 2(\theta_a - \theta_b) |1\rangle_a |0\rangle_b + \cos 2(\theta_a - \theta_b) |1\rangle_a |1\rangle_b] \quad (4.4)$$

$$U_Q^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle = \frac{1}{2\sqrt{2}} [\cos 2\theta_a + \cos 2\theta_b + i(1 - \cos 2(\theta_a - \theta_b)) |0\rangle_a |0\rangle_b + \sin 2\theta_a + \sin 2\theta_b + i \sin 2(\theta_a - \theta_b) |0\rangle_a |1\rangle_b + \sin 2\theta_a + \sin 2\theta_b - i \sin 2(\theta_a - \theta_b) |1\rangle_a |0\rangle_b - \cos 2\theta_a + \cos 2\theta_b - i(1 - \cos 2(\theta_a - \theta_b)) |1\rangle_a |1\rangle_b] \quad (4.5)$$

$$U_H^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle = \frac{1}{2\sqrt{2}} [[(1+i)(\cos 2\theta_a - i \cos 2(\theta_a - \theta_b))] |0\rangle_a |0\rangle_b + [(1+i)(\sin 2\theta_a - i \sin 2(\theta_a - \theta_b))] |0\rangle_a |1\rangle_b + [(1+i)(\sin 2\theta_a - i \sin 2(\theta_a - \theta_b))] |1\rangle_a |0\rangle_b + [(1+i)(-\cos 2\theta_a - i \cos 2(\theta_a - \theta_b))] |1\rangle_a |1\rangle_b] \quad (4.6)$$

$$U_Q^{(a)} U_H^{(b)} |\Phi_{ab}^+\rangle = \frac{1}{2\sqrt{2}} [[(1+i)(\cos 2\theta_b - i \cos 2(\theta_b - \theta_a))] |0\rangle_a |0\rangle_b + [(1+i)(\sin 2\theta_b - i \sin 2(\theta_b - \theta_a))] |0\rangle_a |1\rangle_b + [(1+i)(\sin 2\theta_b - i \sin 2(\theta_b - \theta_a))] |1\rangle_a |0\rangle_b + [(1+i)(-\cos 2\theta_b - i \cos 2(\theta_b - \theta_a))] |1\rangle_a |1\rangle_b] \quad (4.7)$$

From states 4.4-4.7, the probabilities $P_{ij}(\theta_a, \theta_b)$ for detecting a given polarisation combination follow from the Born Rule [102], where the subscripts $i, j \in \{0, 1\}$ denote the polarisation state each photon is found in.

$$U_H^{(a)} U_H^{(b)} |\Phi_{ab}^+\rangle : \quad P_{|00\rangle}(\theta_a, \theta_b) = P_{|11\rangle}(\theta_a, \theta_b) = \frac{1}{2} \cos^2 2(\theta_a - \theta_b) \quad (4.8)$$

$$P_{|01\rangle}(\theta_a, \theta_b) = P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{2} \sin^2 2(\theta_a - \theta_b)$$

$$U_Q^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle : \quad P_{|00\rangle}(\theta_a, \theta_b) = P_{|11\rangle}(\theta_a, \theta_b) = \frac{1}{8} [(\cos 2\theta_a + \cos 2\theta_b)^2 + 4 \sin^4(\theta_a - \theta_b)]$$

$$P_{|01\rangle}(\theta_a, \theta_b) = P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{8} [(\sin 2\theta_a + \sin 2\theta_b)^2 + \sin^2 2(\theta_a - \theta_b)] \quad (4.9)$$

$$U_H^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle : \quad P_{|00\rangle}(\theta_a, \theta_b) = P_{|11\rangle}(\theta_a, \theta_b) = \frac{1}{4} [\cos^2 2\theta_a + \cos^2 2(\theta_a - \theta_b)] \quad (4.10)$$

$$P_{|01\rangle}(\theta_a, \theta_b) = P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{4} [\sin^2 2\theta_a + \sin^2 2(\theta_a - \theta_b)]$$

$$U_Q^{(a)} U_H^{(b)} |\Phi_{ab}^+\rangle : \quad P_{|00\rangle}(\theta_a, \theta_b) = P_{|11\rangle}(\theta_a, \theta_b) = \frac{1}{4} [\cos^2 2\theta_b + \cos^2 2(\theta_b - \theta_a)] \quad (4.11)$$

$$P_{|01\rangle}(\theta_a, \theta_b) = P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{4} [\sin^2 2\theta_b + \sin^2 2(\theta_b - \theta_a)]$$

Experimental measurements using the passive receivers should follow these probability functions. Correlation curves are recorded by fixing the polarisation state on one PA at an angle θ_a , and rotating the waveplates of the other PA through a full rotation of 2π . Figure 4.3 shows the experimentally observed correlations, fitted with a function of the form predicted in Equations 4.8-4.11. The experimental data agrees well with the theoretical predictions, and any differences fall within the expected margin based on imprecise polarisation rotation (see Section 2.3.1), accidental coincidences, and imperfect initial channel polarisation compensation.

Notably, the top left plot of Figure 4.3 shows a significant difference between the absolute number of $|HH\rangle$ and $|VV\rangle$ coincidences, which is not apparent in equivalent measurements in the $\mathbb{X}$ or $\mathbb{Y}$ basis. This suggests that there is an imbalance in the number of $|HH\rangle$ and $|VV\rangle$ coincidences produced by the source as opposed to coupling issues in the measurement setup. Considering the source architecture (see Section 2.3), this is either due to an incorrectly polarised pump beam (i.e. not diagonal with respect to the interferometer, but biased towards $|VV\rangle$), or due to coupling issues specifically for the $|HH\rangle$ polarised component of the field.

4.3. POLARISATION CORRELATION CURVES

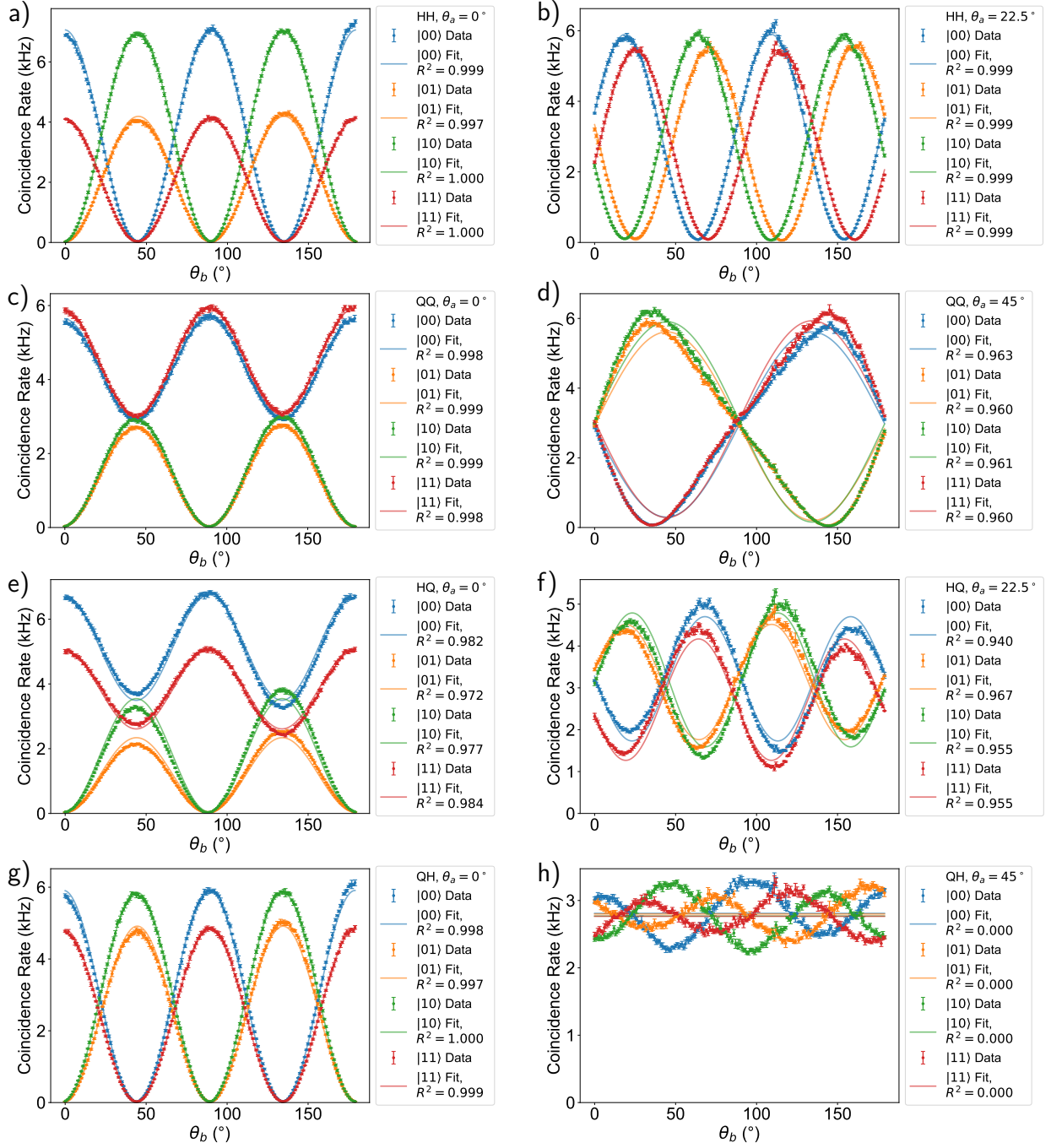


Figure 4.3: Correlation curves for EPS photons measured with the PAs, showing correlation rates changing as photon b's waveplate is rotated, with photon a's waveplate fixed. Subplots differ in waveplate (H/Q) for each photon a, b and θ_a as: a) H, H, 0° ; b) H, H, 22.5° ; c) Q, Q, 0° ; d) Q, Q, 45° ; e) H, Q, 0° ; f) H, Q, 22.5° ; g) Q, H, 0° ; h) Q, H, 45° . Data agree well with fitted theoretical expressions. Subplot h) can be considered acceptable despite low R^2 values as even small experimental imperfections are expected to degrade the fit quickly.

4.4 CHSH-Inequalities and Bell-Violation under Restricted Polarisation Manipulation

To evidence entanglement in the polarisation of emitted photon pairs, an entanglement witness is necessary. One of the most commonly employed figures for this purpose is the CHSH parameter S and its associated Bell-violation [4],[25]:

$$-2 \leq S \leq 2 \quad (4.12)$$

$$S = E(\theta_a, \theta_b) - E(\theta_a, \theta'_b) + E(\theta'_a, \theta_b) + E(\theta'_a, \theta'_b) \quad (4.13)$$

$$E(\theta_a, \theta_b) = P_{|00\rangle}(\theta_a, \theta_b) + P_{|11\rangle}(\theta_a, \theta_b) - P_{|01\rangle}(\theta_a, \theta_b) - P_{|10\rangle}(\theta_a, \theta_b) \quad (4.14)$$

In Equation 4.13, S is defined as a combination of four expectation values $E(\theta_a^{(')}, \theta_b^{(')})$, each measured at one of two waveplate angle settings per photon. Recall here that the angles $\theta_{a,b}$ refer to the waveplate fast axis angles with respect to the initially aligned vertical measurement axis, not (as often quoted) the linear polarisation state to be measured. Equation 4.14 gives $E(\theta_a, \theta_b)$ as the correlation coefficients between polarisation outcomes as defined in Section 4.3; the expectation values for the other angle combinations follow equivalently.

Quantum mechanics enables a maximally achievable Bell-violation (4.12) of $S = 2\sqrt{2}$, known as the Tsirelson bound. To measure S experimentally, many potential sets of the angles exist that maximise the violation of Bell's inequality. Most commonly, the linear polarisation states $\{\theta_a = 0^\circ, \theta_b = 22.5^\circ, \theta'_a = 45^\circ, \theta'_b = 67.5^\circ\}$ are employed, since they are straightforward to manipulate and evaluate.

In this setup, the CHSH-inequality can be evaluated using these well-known angles on the arms where a HWP is placed. The other half of each PA employs only a QWP for polarisation state manipulation and has thus limited access to the equator of the Poincaré sphere, which does not include all the necessary linear polarisation projections. Consequently, to show that both halves of the PAs are functioning as intended and that on each potential bi-photon path, the CHSH-inequality can be violated, specific expressions for the S -parameter in dependence on the angles given by each available waveplate combination are derived. These expressions enable determination of the waveplate angles for which the CHSH-violation will be maximised, and by how much the classical bound can be exceeded in each configuration.

In setup 4.1, the Bell-violation can be evidenced using two HWPs, two QWPs, or one HWP and one QWP in either allocation. Using the probabilities obtained in Eqs. 4.13 & 4.14,

4.4. CHSH-INEQUALITIES AND BELL-VIOLATION UNDER RESTRICTED POLARISATION MANIPULATION

an explicit expressions for the parameters $E_{\text{WP}_1\text{WP}_2}(\theta_a, \theta_b)$ and $S_{\text{WP}_a\text{WP}_b}$ can be obtained as a function of the angles of the two waveplates $\text{WP}_a, \text{WP}_b \in \{\text{H}, \text{Q}\}$:

$$E_{\text{HH}}(\theta_a, \theta_b) = \cos 4(\theta_a - \theta_b) \quad (4.15)$$

$$E_{\text{QQ}}(\theta_a, \theta_b) = \frac{1}{4} [1 + \cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) - 2 \cos 2(\theta_a - \theta_b) + \cos 4(\theta_a - \theta_b)] \quad (4.16)$$

$$E_{\text{HQ}}(\theta_a, \theta_b) = \frac{1}{2} [\cos 4\theta_a + \cos 4(\theta_a - \theta_b)] \quad (4.17)$$

$$E_{\text{QH}}(\theta_a, \theta_b) = \frac{1}{2} [\cos 4\theta_b + \cos 4(\theta_b - \theta_a)] \quad (4.18)$$

and subsequently

$$S_{\text{HH}} = \cos 4(\theta_a - \theta_b) - \cos 4(\theta_a - \theta'_b) + \cos 4(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta'_b) \quad (4.19)$$

$$S_{\text{QQ}} = \frac{1}{4} [2 + 2 \cos 4\theta'_a + 2 \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) - 2 \cos 2(\theta_a - \theta_b) + \cos 4(\theta_a - \theta_b) - 2 \cos 2(\theta_a + \theta'_b) + 2 \cos 2(\theta_a - \theta'_b) - \cos 4(\theta_a - \theta'_b) + 2 \cos 2(\theta'_a + \theta_b) - 2 \cos 2(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta_b) + 2 \cos 2(\theta'_a + \theta'_b) - 2 \cos 2(\theta'_a - \theta'_b) + \cos 4(\theta'_a - \theta'_b)] \quad (4.20)$$

$$S_{\text{HQ}} = \frac{1}{2} [\cos 4(\theta_a - \theta_b) - \cos 4(\theta_a - \theta'_b) + \cos 4(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta'_b) + \cos 4\theta'_a] \quad (4.21)$$

$$S_{\text{QH}} = \frac{1}{2} [\cos 4(\theta_b - \theta_a) - \cos 4(\theta_b - \theta'_a) + \cos 4(\theta'_b - \theta_a) + \cos 4(\theta'_b - \theta'_a) + \cos 4\theta'_b] \quad (4.22)$$

Finally, symbolic optimisation (in *Wolfram Mathematica*) is employed to find a set of angles $\{\theta_a, \theta'_a, \theta_b, \theta'_b\}$ for which $|S_{\text{WP}_1, \text{WP}_2}|$ is maximised in each case. For the HH case, this simply reproduces the well-known linear polarisation states utilised by Clauser, Horne, Shimony and Holt. For all other configurations, the quantum-allowed maximum violation of $S = 2\sqrt{2}$ cannot be reached due to the limited polarisation rotations accessible through the QWP. Regardless, $S > 2$ can still be achieved. Table 4.2 lists the angles for each waveplate combination and their theoretically maximal $|S|$ values.

Table 4.2 also displays the experimental results of all four CHSH-measurements recorded with the PAs. Significant Bell-violation is observed in all configurations, approaching the theoretically predicted values, and discrepancies are well within the expected range of polarisation misalignment induced errors. The last column represents the quantity $n_\Delta = \frac{S-2}{\Delta S}$, i.e. how many standard deviations above the classical limit we find the quantum state to be. This is a frequently quoted parameter to quantify the strength of the Bell-violation given experimental uncertainties. Collectively, the results show that the PAs are working as intended and that the quantum state can be investigated on all arms of the receivers.

WP Configuration	Angles θ_x	Theoretical Violation	Measured Violation	Excess $\Delta S > 2$
HH	$\theta_a = 0^\circ$	$S \leq 2\sqrt{2}$ ≈ 2.828	$S = 2.732$ ± 0.006	$n_\Delta = 130.9$
	$\theta_b = 11.25^\circ$			
	$\theta'_a = 22.5^\circ$			
	$\theta'_b = 33.75^\circ$			
QQ	$\theta_a = 22.5^\circ$	$S \leq 2.5$	$S = 2.459$ ± 0.007	$n_\Delta = 69.4$
	$\theta_b = 0^\circ$			
	$\theta'_a = 0^\circ$			
	$\theta'_b = 67.5^\circ$			
HQ	$\theta_a = 22.5^\circ$	$S \leq 1 + \sqrt{2}$ ≈ 2.414	$S = 2.384$ ± 0.008	$n_\Delta = 51.0$
	$\theta_b = 11.25^\circ$			
	$\theta'_a = 0^\circ$			
	$\theta'_b = 78.75^\circ$			
QH	$\theta_a = 78.75^\circ$	$S \leq 1 + \sqrt{2}$ ≈ 2.414	$S = 2.358$ ± 0.008	$n_\Delta = 47.5$
	$\theta_b = 0^\circ$			
	$\theta'_a = 11.25^\circ$			
	$\theta'_b = 22.5^\circ$			

Table 4.2: CHSH measurement angles, theoretical Bell-state violation and measurement results for all HWP and QWP combinations. Significant Bell-violation is observed in all configurations. For the HQ and QH, the experimental results were obtained using an equivalent set of measurement angles due to neglecting the mirrored reference frame introduced in the QWP measurement path. The resultant expectation values are equal in magnitude after appropriate reordering.

4.5 Quantum State Tomography

Quantum state tomography [103], [104] is a technique to fully characterise an unknown quantum state by reconstructing its density matrix $\hat{\rho}$ through repeated measurements of identically prepared states in an informationally complete set of bases. From $\hat{\rho}$, various figures of merit can be derived, such as the state's fidelity and concurrence in the case of a two-qubit entangled state. This manner of practical tomographic description of an arbitrary two-photon state was one of the target capabilities in the design of the polarisation analysers. As discussed previously, this is the main motivation behind the inclusion of QWPs in the setup. This section presents the specific method employed here, a set of results for the qubit-tomography of the entangled photons from the EPS, and some examples of further refinement of the raw data.

4.5.1 Tomographic Method

Quantum tomography is based on experimental measurement of the Stokes parameters [105], which for a two-qubit state are known as $S_{a,b}$; $a, b \in \{0, 1, 2, 3\}$ and construct the density matrix $\hat{\rho}$ as stated in Eq. 4.23:

$$\hat{\rho} = \frac{1}{4} \sum_{a,b=0}^3 S_{a,b} \sigma_a \otimes \sigma_b \quad (4.23)$$

Here, σ_0 is the identity operator and $\sigma_1, \sigma_2, \sigma_3$ denote the Pauli operators. Therefore, 16 independent, measured parameters are needed to fully construct the density matrix. Each Stokes parameter corresponds to the expectation value of $\sigma_a \otimes \sigma_b$, and thus is experimentally obtained by performing a local projective measurement in the eigenbases of σ_a and σ_b for photons a and b respectively. This is analogous to the $E(\theta_a, \theta_b)$ expectation values used in the CHSH-inequality:

$$S_{a,b} = P_{|00\rangle} + P_{|11\rangle} - P_{|10\rangle} - P_{|01\rangle} \quad (4.24)$$

The density matrix for the state produced by the EPS, the $|\Phi^+\rangle$ Bell-state, is given by:

$$\hat{\rho}_{|\Phi^+\rangle} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad (4.25)$$

To measure how closely an experimentally determined density matrix resembles the target expression, a number of different metrics are commonly employed. In this work, fidelity and concurrence will be used to characterise the measurement results. *Fidelity* is a measure of the overlap between two quantum states ρ_1 and ρ_2 , calculated following Uhlmann and Jozsa as [106]:

$$F(\hat{\rho}_1, \hat{\rho}_2) = \left(\text{Tr} \left\{ \sqrt{\sqrt{\hat{\rho}_1} \hat{\rho}_2 \sqrt{\hat{\rho}_1}} \right\} \right)^2 \quad (4.26)$$

The *concurrence* is a parameter that quantifies the entanglement of a given two-qubit density matrix by considering the overlap of the state with its bit-flipped version [107]. To obtain it, the matrix $\hat{R} = \hat{\rho} \hat{\Sigma} \hat{\rho}^T \hat{\Sigma}$ is assembled, where $\hat{\Sigma}$ is the 'spin-flip matrix' equal to $\sigma_y \otimes \sigma_y$. For evaluation of the concurrence, the eigenvalues of $\hat{R}$ are taken and ordered by magnitude so that $r_1 \geq r_2 \geq r_3 \geq r_4$. Then, the concurrence is defined as:

$$C_{\hat{\rho}} = \max\{0, \sqrt{r_1} - \sqrt{r_2} - \sqrt{r_3} - \sqrt{r_4}\} \quad (4.27)$$

For a product state $C_{\hat{\rho}} = 0$, whereas a maximally entangled pure state results in $C_{\hat{\rho}} = 1$.

4.5.2 Measurement Results

Leveraging the two simultaneous bases set by each PA, the full $|\Phi^+\rangle$ density matrix can be reconstructed using a minimum of three separate measurements. From a complete set of

experimental data, taken with the EPS and both PAs, the following $\hat{\rho}_{data}$ can be constructed directly:

$$\hat{\rho}_{data} = \frac{1}{2} \begin{pmatrix} 1.113 & 0.042 - 0.105i & 0.028 - 0.040i & 0.929 - 0.112i \\ 0.042 + 0.105i & 0.006 & 0.021 + 0.069i & 0.091 - 0.075i \\ 0.028 + 0.040i & 0.021 - 0.069i & 0.005 & 0.054 - 0.069i \\ 0.929 + 0.112i & 0.091 + 0.075i & 0.054 + 0.069i & 0.876 \end{pmatrix} \quad (4.28)$$

$$\Delta\hat{\rho}_{data} = \pm \frac{1}{2} \begin{pmatrix} 0.104 & 0.006 + 0.006i & 0.009 + 0.006i & 0.002 + 0.005i \\ 0.006 + 0.006i & 0.001 & 0.002 + 0.004i & 0.008 + 0.008i \\ 0.009 + 0.006i & 0.002 + 0.004i & 0.007 & 0.008 - 0.007i \\ 0.002 + 0.005i & 0.008 + 0.008i & 0.008 + 0.007i & 0.105 \end{pmatrix} \quad (4.29)$$

$\Delta\hat{\rho}_{data}$ is obtained via Monte-Carlo simulation with 100 samples based on the experimentally measured uncertainties for each coincidence probability, and the same applies to the experimental uncertainties on subsequent parameters presented in this section. Figure 4.4 a) visualises the density matrix $\hat{\rho}_{data}$.

The measured $\hat{\rho}_{data}$ matches the target state of $|\Phi^+\rangle$ very closely with a fidelity of 99.6% ($\pm 0.1\%$), and exhibits a high degree of entanglement with a concurrence of 0.952 (± 0.09). Both measures indicate a small degree of experimental imperfections and are in-line with current high-quality literature results [108, 109].

4.5.3 Maximum Likelihood Estimation

A density matrix representing a valid quantum state is defined by being hermitian, positive semi-definite and possessing a unit trace. Matrices constructed from experimental values, including the $\hat{\rho}_{data}$ given in Section 4.5.2, rarely fulfil these conditions due to measurement errors and noise. It is thus standard practice in quantum tomography to perform a Maximum Likelihood Estimation (MLE) to find the nearest physical $\hat{\rho}$ that is most likely to have produced the observed count rates. The methodology for MLE is taken from [104] and can be summarised as follows:

First, a generalised physical density matrix is constructed, in this case based on the Cholesky-decomposition starting from a parametrised lower-triangular matrix. This expression includes 16 real parameters, which will be determined via optimisation over the experimental measurement results. To do so, a negative log-likelihood function is formulated, which encapsulates how likely it is that any given set of physical parameters produced the observed coincidence counts. Lastly, the negative log-likelihood function is minimised using a standard optimisation routine. Differing from James *et al.* [104], the limited-memory Broyden-Fletcher-Goldfarb-Shanno algorithm was employed in this step, for efficient optimisation in Python.

After performing MLE, the $\hat{\rho}_{MLE}$ presented in Figure 4.4 b) was obtained. It has a slightly lower fidelity to $|\Phi^+\rangle$ at 99.4% ($\pm 0.03\%$), but a significantly higher, near-perfect

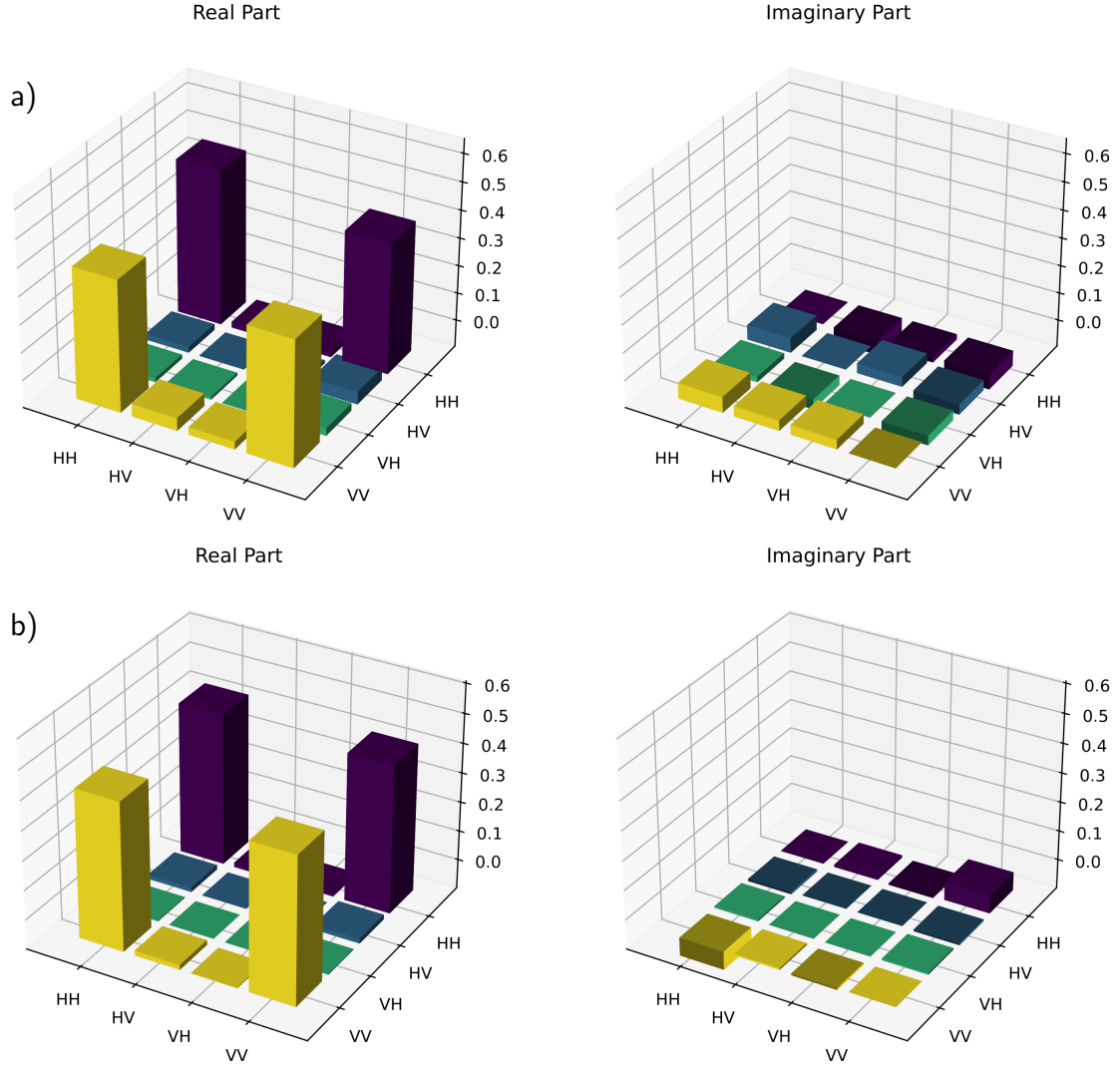


Figure 4.4: Density matrix ρ of the entangled state emitted by the EPS. In a) ρ is reconstructed directly from the measured Stokes parameters, while b) is a reconstructed physical ρ_{MLE} via maximum likelihood estimation.

concurrence of $0.996 (\pm 0.001)$. This presents an interesting insight into the sources of error present in the implementation. Essentially, by performing MLE, sources of random noise are minimised, which includes the errors introduced by detector dark counts, background photons, imprecision in waveplate positioning etc. However, systematic errors that were previously hidden by the noise floor have become more apparent, as visible when comparing the graphical representations of $\hat{\rho}_{data}$ and $\hat{\rho}_{MLE}$. The most likely physical quantum state that resulted in the given measurements differs from $|\Phi^+\rangle$ by a small, but non-negligible imaginary φ component between the $|HH\rangle$ and $|VV\rangle$ bits. Consequently, the fidelity of the real state with $|\Phi^+\rangle$ is lower than the noisy measurement initially indicated. However, the physical state produced by the EPS is most still a maximally entangled two-qubit state, only with a non-zero relative phase between the polarisation vectors. This concept has been discussed extensively in Chapter 3 and Appendix A and remains as the main challenge faced when aligning Alice and Bob to the EPS's polarisation reference frame.

Quantum tomography including MLE does not generally have direct applications to QKD, as the parameters used in the generation of a secure key cannot be based on an optimised density matrix, but need to reflect the 'worst-case scenario' in form of the actual recorded QBER. However, as exemplified here, quantum tomography is tremendously useful in the characterisation of a quantum state produced by a single photon source and the quantum channel that transmits it. In this example, a channel transformation introducing a small relative phase to the Bell-state could be identified despite the apparatus noise obscuring it in direct observation. This highlights that the inclusion of a QWP in a polarisation analyser intended for deployment-related quantum communication research is advantageous.

4.6 Entanglement-based QKD

BBM92 can be implemented with the presented system by setting the PAs to one of the configurations presented in Table 4.3. Together, the EPS and PAs allow for sustained 4-state BBM92-type QKD in any two-basis combination $\in \{\mathbb{Z}, \mathbb{X}, \mathbb{Y}\}$, or 6-state BBM92 by randomly switching between two positions to obtain results for all three bases.

Alice		Bob	
HWP	QWP	HWP	QWP
$\mathbb{Z}$	$\mathbb{Y}$	$\mathbb{Z}$	$\mathbb{Y}$
$\mathbb{X}$	$\mathbb{Z}$	$\mathbb{X}$	$\mathbb{Z}$
$\mathbb{X}$	$\mathbb{Y}$	$\mathbb{X}$	$\mathbb{Y}$

Table 4.3: Possible PA settings for BBM92.

This section reports the measured QBER and predicted secret key fraction obtained with this system, as well as a simulation of distance scaling under the given experimental parameters. Finally, the data is used to generate a secret key using a QKD post-processing provided by the research group, and the resulting final key is presented.

4.6.1 Measured QBER and Secret Key fraction

The measured QBER in each basis is found to be:

$$\begin{aligned}
 \epsilon_z &= 0.59\% \quad (\pm 0.03\%) \quad (\text{HWP}) \\
 \epsilon_z &= 0.51\% \quad (\pm 0.03\%) \quad (\text{QWP}) \\
 \epsilon_x &= 2.53\% \quad (\pm 0.10\%) \\
 \epsilon_y &= 4.62\% \quad (\pm 0.13\%)
 \end{aligned}$$

Since the $\mathbb{Z}$ and $\mathbb{X}$ bases have the lowest simultaneous QBER, the settings shown in the second row of table 4.3 are chosen for 4-state BBM92. For the 6-state protocol, the $\mathbb{Z}$ -basis may be measured on either arm of the PA depending on the current settings. Therefore, the mean QBER for both paths is used in the 6-state calculations moving forward. It is assumed that in each protocol, the $\mathbb{Z}$ -basis is used to generate the cryptographic key, while the error is estimated using the remaining bases.

The secret key rate after post-processing can be estimated based on the methodology presented in Appendix A of the Scarani *et al.* 2009 review of the security of practical QKD [59]. In the asymptotic limit of infinitely many signals, and assuming collective attacks, Eve's information on the exchanged bits is limited by the Holevo bound [110], which in this instance can be expressed as:

$$I_E(\lambda) = H(\lambda) - h(\epsilon_z) \quad (4.30)$$

Here, λ represents the eigenvalues of the Bell-diagonal state shared between Alice and Bob. The Shannon entropy $H(\lambda) = -\sum_i \lambda_i \log_2 \lambda_i$ of this eigenvalue distribution encapsulates the total uncertainty of the joint system. Subtracting from this the uncertainty associated with the observed bit-errors ϵ_z , i.e. the binary Shannon entropy obtained from the measured QBER $h(\epsilon_z) = -\epsilon_z \log_2 \epsilon_z - (1 - \epsilon_z) \log_2 (1 - \epsilon_z)$ (see Equation 1.4), yields an upper bound on the information held by Eve.

In the 6-state protocol, the two-qubit state can be fully characterised by the QBERs in all three bases, and hence the entropy $H(\lambda)$ is known. This leads to the following expression for Eve's information:

$$I_E(\epsilon) = \epsilon_z h\left(\frac{1 + (\epsilon_x - \epsilon_y)/\epsilon_z}{2}\right) + (1 - \epsilon_z) h\left(\frac{1 - (\epsilon_x + \epsilon_y + \epsilon_z)/2}{1 - \epsilon_z}\right) \quad (4.31)$$

In the 4-state protocol, an undetermined parameter remains in the description of the shared state due to the absence of measurements in one basis. The eigenvalues λ thus have to be chosen in a way that maximizes Eve's information, subject to the observed QBER, which represents the worst-case scenario. This parametrisation results in an upper bound of:

$$I_E(\epsilon) = h(\epsilon_z) \quad (4.32)$$

Assuming that Alice and Bob's key generation takes place in the $\mathbb{Z}$ -basis, their mutual information is given by:

$$H(A|B) = 1 - h(\epsilon_z) \quad (4.33)$$

Combining this with the information Eve may hold, the amount of secret key that Alice and Bob may distil per successfully exchanged bit can be expressed as the secret key fraction r :

$$r = 1 - h(\epsilon_z) - I_E(\epsilon) \quad (4.34)$$

This figure assumes perfect error correction, one-way post-processing and no key loss through pre-processing. Using Equation 4.34, a maximum tolerable QBER can be determined beyond which Eve's potential information exceeds the mutual information between Alice and Bob. For symmetric error rates, this threshold is approximately 12.6% in the 6-state protocol and 11% in the 4-state protocol.

The experimentally measured QBERs fall well below this value, so a positive Secret Key Rate (SKR) can be expected. Indeed, the following secure bits per sifted bit, i.e. the secret key fractions r , and corresponding absolute SKRs R are obtained based on the measured coincidence rates and QBER values:

$$\begin{aligned} r_4 &= 0.784 \text{ secret bits/sifted bit} \\ R_4 &= 8.673 \text{ kHz} \end{aligned} \quad (4\text{-state})$$

$$\begin{aligned} r_6 &= 0.741 \text{ secret bits/sifted bit} \\ R_6 &= 8.188 \text{ kHz} \end{aligned} \quad (6\text{-state})$$

This represents the baseline performance of the system without the involvement of any channel losses. The lower SKR of the 6-state protocol can be explained by its inclusion of the $\mathbb{Y}$ -basis, which has the highest QBER of the three. An absolute SKR of just over 8 kHz, while typical for current laboratory based implementations, may initially appear low given the pair-emission rate of the EPS of approximately 1 MHz. However, several known factors significantly reduce the coincidence rate in this apparatus. Only a small slice of the source's

emission spectrum is selected by the optical filters, necessitated by the dichroic filter mismatch (see Section 2.3.1). Furthermore, a number of high-loss components are currently required for operation, notably the tunable optical filter and the beam combiners used for time-multiplexed detection (see Section 3.6). Given these additional losses, the observed SKR is consistent with expectations.

Instead of monitoring for Eve's presence by performing error estimation in a basis orthogonal to the key generation basis, the security of the distilled key can also be based on violation of the CHSH-inequality [111]. Using the Bell parameter S_{CHSH} , the secret key fraction can be obtained via:

$$r_{\text{CHSH}} = -\log_2 \left(\frac{1}{2} + \frac{1}{2} \sqrt{2 - \frac{S_{\text{CHSH}}^2}{4}} \right) - h(e_z) \quad (4.35)$$

In Section 4.4, a Bell parameter $S = 2.73$ was found for the given system, which in combination with the ϵ_z obtained here results in a secret key fraction of $r_{\text{CHSH}} = 0.5$ and an SKR of $R_{\text{CHSH}} = 5.57$ kHz. This method represents a step towards DI-QKD, though several loopholes and trust assumptions remain in the given implementation, for example the fair sampling assumption. Nonetheless, R_{CHSH} reflects a more conservative estimate of the SKR obtained under stricter security assumptions, which account for the possibility of device imperfections and eavesdropping strategies that might not be detectable through the QBER alone.

Comparing R_6 and R_{CHSH} highlights the inherent trade-off between security assumptions and key rate. While the secrecy assurance provided by the Bell-violation offers stricter security grounded in quantum mechanical law, it results in a lower key rate, reflecting the conservative entropy assumptions required when accounting for potential device imperfections. This decrease in key rate emphasizes the challenges of achieving high security in a practical QKD system, where imperfections inevitably affect performance. As evidenced by this analysis, the design of the PAs enables them to support a broad range of research applications, offering flexibility to adjust between high throughput and high security oriented procedures, depending on the specific demands of each project.

4.6.2 Distance Scaling

Building on the zero-distance measurements, a simple loss model can be applied to the observed singles and coincidence rates to predict the SKR as a function of distance, providing an estimate of the system's effective reach.

Consider an implementation where the EPS is placed centrally between Alice and Bob, such that each photon in a pair propagates an equal distance L before arriving at their respective receivers. In this symmetric configuration, losses are modelled using the standard approximation for exponential attenuation in optical fibre:

$$\eta(L) = 10^{-\frac{\alpha L}{10}}, \quad (4.36)$$

where η is the transmission probability for one photon and $\alpha = 0.2$ dB/km is the attenuation coefficient. Essentially, the model consists of applying this transmission factor to all measured quantities, except for the detector noise.

At zero distance, the singles count rates $S_{A,B}$, detector dark count rates R_{DC} (DCR), and total coincidence rates R_{tot} per bit combination $|00\rangle, |11\rangle, |01\rangle, |10\rangle$ have been measured in each basis with a jitter-limited coincidence window of $\Delta t_{\text{jitter}} = 150$ ps. From the singles count rates, the contribution of accidental coincidences R_{acc} to the total coincidences can be estimated by assuming the statistically expected frequency of independent detection events. Subsequently, the accidentals are subtracted from the total coincidences to obtain the estimated rate of true coincidences observed due to EPS pairs R_{coinc} . Since each bit combination is treated separately but accidentals are computed based on detection channel pairs a factor of $\frac{1}{4}$ arises in front of the accidentals contribution. This accounts for equal contribution of accidentals to all four possible bit combinations.

$$R_{\text{acc}} = S_A \times S_B \times \Delta t_{\text{jitter}} \quad (4.37)$$

$$R_{\text{coinc}} = R_{\text{tot}} - \frac{R_{\text{acc}}}{4} \quad (4.38)$$

To perform realistic distance scaling, the effect of chromatic dispersion on the coincidence window has to be accounted for:

$$\Delta t_{\text{disp}} = D \times \Delta \lambda \times L \quad (4.39)$$

Here, D is the chromatic dispersion parameter, which is assumed to be close to the standard value of 17 ps/(nm · km) in SMF, and $\Delta \lambda$ is the wavelength difference between the two photons. The spectrum of the EPS is filtered to signal photons at 1550.1 nm and idler photons at 1569.3 nm with a filter pass-band of $\Delta_f = 1.391$ nm each. Since photon pairs are energetically distributed symmetrically across 1560 nm, the pairs with a larger wavelength difference will experience greater temporal separation than the pairs closer in wavelength, resulting in a broadened coincidence peak. Therefore, the coincidence window has to be increased according to:

$$\Delta t_{\text{disp}} = D \times 2\Delta_f \times L \quad (4.40)$$

$$\Delta t_{\text{coinc}} = \Delta t_{\text{jitter}} + \Delta t_{\text{disp}} \quad (4.41)$$

Using Equations 4.36 & 4.41, the count rates for single photon detections $S(L)$ and accidental coincidences $R_{\text{acc}}(L)$ therefore scale following:

$$S(L) = (S_0 - R_{DC}) \times \eta(L) + R_{DC} \quad (4.42)$$

$$R_{\text{acc}}(L) = S_A(L) \times S_B(L) \times \Delta t_{\text{coinc}}, \quad (4.43)$$

where S_0 represents the zero-distance singles rates and the DCR contribution is not affected by the transmission losses. Finally, the true coincidences are scaled based in the simultaneous transmission probability of both Alice's and Bob's photon. Total coincidence rates at distance $R_{\text{tot}}(L)$ are obtained by adding the corresponding scaled accidentals:

$$R_{\text{tot}}(L) = R_{\text{coinc}}(L) \times \eta(L)^2 + \frac{R_{\text{acc}}(L)}{4} \quad (4.44)$$

From the resulting measured coincidence rates per bit combination, the quantum bit error rates are evaluated in each basis i as a function of distance:

$$e_i = \frac{R_{|01\rangle} + R_{|10\rangle}}{R_{|00\rangle} + R_{|11\rangle} + R_{|01\rangle} + R_{|10\rangle}} \quad (4.45)$$

where $R_{|ij\rangle} = R_{\text{tot}}(L)$ using the results for each qubit combination $i, j \in \{0, 1\}$. These QBERs are then used to simulate the secret key fraction and, consequently, the SKR for both the 4-state and 6-state BBM92 protocols using Equations 4.31-4.34. Figure 4.5 plots the computed SKRs for both protocols as a function of the total distance $2 \times L$ between Alice and Bob.

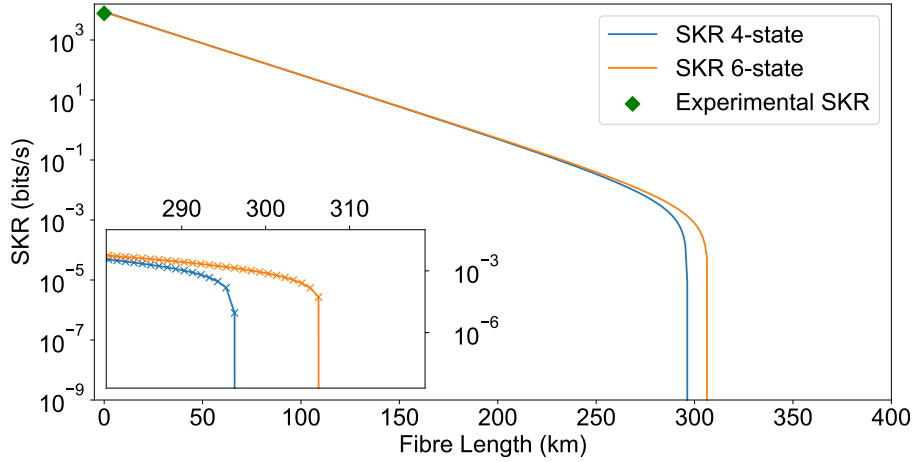


Figure 4.5: Estimated secret key rate as a function of distance between Alice and Bob based on extrapolation from the zero distance experimental SKR. The inset shows a enlarged view of the QBER-induced drop-off in the secret key rate at the maximum distance.

The SKR drops sharply at 296 km for the 4-state protocol and 307 km for the 6-state protocol, corresponding to the rise in QBER. The 6-state protocol reaches a slightly greater maximum distance due to its higher QBER threshold, making it more resilient to errors. Both distances remain well below the theoretical limit imposed by the repeaterless secret key capacity [29], and achieve promising ranges owing to the low QBER resulting from precise state measurements and low-noise SNSPDs.

The primary constraint on the maximum achievable distance can be attributed to the broadened coincidence windows predicted in 4.41. As a result of chromatic dispersion, the required coincidence windows at longer distances are significantly larger than the detector-limited window at 0 km, expanding by tens of nanoseconds over a few hundred kilometres. The resulting increase in signal-to-noise ratio constitutes a major limitation on the reach of the entanglement distribution system. Addressing this issue in future studies could enhance the system performance.

Moreover, as discussed in 4.6, the absolute key rates are reduced due to the imposed wavelength filtering. This filtering interacts directly with the chromatic dispersion, as wider filtering results in higher wavelength differences of the admitted photons. Balancing high effective source brightness and narrow chromaticity is a difficult task, which highlights the importance of further countermeasures such as dispersion compensation or a narrowed source spectrum.

Despite these challenges, the system's performance in long-distance scenarios indicates that it is well-suited for long-range studies and practical field deployments.

4.6.3 Post-Processing and Distillation of a Secret Key

Finally, the experimentally obtained coincidence events are used to distil a secret key. The data are pre-analysed to produce sifted key strings for Alice and Bob, which were then handed to a postdoctoral researcher for post-processing using a QKD software suite available within the research group.

The post-processing steps include parameter estimation, error correction using the Cascade protocol, Toeplitz hash verification, and privacy amplification, all performed in the asymptotic limit. From a 5-min sample containing approximately 3.5 million raw key bits, a secure key of 2,424,535 bits was obtained, with a security parameter of $\epsilon_{sec} = 1.00 \times 10^{-10}$. This corresponds to a secret key fraction of approximately 0.7 bits/sifted bit, and a key generation rate of roughly 8.0 kHz, which is in reasonable agreement with the 8.6 kHz presented in section 4.6.1. The discrepancy can be attributed to the fact that the theoretical prediction assumes perfect error correction, whereas in practice, Cascade incurs an additional information leakage of approximately 6,600 bits/second.

This successful secret key generation establishes a comprehensive pipeline, from the creation of the entangled quantum state to the final secure key. The polarisation entanglement system developed in this thesis, or any of its components, is now fully equipped for use in future research initiatives focused on the deployment-readiness of QKD, both in a controlled laboratory environment and in real-world field deployments. Additionally, this key generation represents the first successful demonstration of quantum key distribution within the University of York's experimental DV quantum communications group.

```
1011100010010100001010010011100101000100101001011101000110000100
1001001100011011100110001001111110010010110100100100101001010100
001101000010010101111001011111001010111110111010000011000110110
0000011110110010011110010011111000010010010111111001010001001101
0000001111110110001101111110101011000110101000001101100111111110
1000111111101010000101101000001111000101100101100101100100010000
0001100001101001111101100011000000010101010100100100100010111101
1101110110101011011010101110011110110000000111101010110011110010
0001100101011000111111001100010101001000101100101110111110001001
1110100101000000011010110101101010110010101001111000010011111100
1000011001001100110011010101001100011100111100101110001000100100
0111100100100010100111101010110010110000010011100011000010100001
0000010110000101010110000100000010110010101100000010000101010011
0000111000000110000010110000010111001111110011010000101000011001
0001011000101000100011100001100000011101110011000101101011100111
0001100010110001100110111001000001110010110000110010001010011101
1010010111001010110010010000000111000100100111011010101111001000
1000000011001111111011000001101111111100010110001000001111000001
1100010011101011001111010000011111101000100101000100010010111100
1010010111110011000101011010001011111111111110111010011110001111
0010000101001101100001110100111001111111001011010101010110001111
1000000110001000100101100111001100001100011101001110011001101011
1000000000101011111011111111011001011110101101111010001101010000
0011110000011100101001100001100101111101010001101001111001100111
1111100100010010100011101000111100101001110001011110100111111101
1000110011110101000001100101111000111101100001001101101101010000
1010101111001110100101010100000000100100010001010001001010100111
0110100011010010010101001001111010000010111001101111101111011011
0101101111011110101010011000011001001000011001000011011000111011
10101111111100101111110100011100011100000111010001100100000011001
1110001110111000010100000101011010000100110100110110000110010110
1110110110101100001010011000010110001101111000010000100010001001
1000100101010100000100000100101101000110000000011001111011110101
0010000100001011000100101011110111010010011001101100100011110110
1110001100011111100110111100101011101000011111010000100000000111
11110101001111111111010111111010101111110000110101101110010110011
10000111111110101001111111110101111110101011111100001101011011100
1011001110001101110011111010001000001100100000011010100000111000
0000110100100000110000110101101010000100110010001110000100100100
0011011011111000000110010111000111110011000001001111011101100001
0011011100100001001100111101001010011111011001101011100100000101
```

Figure 4.6: First 2,624 digits of the first-ever secret key generated at the University of York via discrete-variable QKD, leveraging the described source of entangled photons.

Chapter 5

Entanglement Distribution in Shared Fibre Infrastructure

This chapter investigates the coexistence of entangled photons with classical White Rabbit timing signals as a means to reduce the number of required physical channels in a quantum network architecture. The study uses an intermediate version of the polarisation entanglement system developed in the preceding chapters and addresses the integration of QKD into existing optical communication infrastructure.

The work presented here is based on the publication: K. P. Schatz, B. Amies-King, S. Albosh, R. Kumar, M. Lucamarini, "Practical single-fibre network-oriented quantum key distribution from a compact source of entangled photons in presence of White Rabbit time synchronisation," Proc. SPIE 12335, Quantum Technology: Driving Commercialisation of an Enabling Science III, 123350F (11 January 2023); <https://doi.org/10.1117/12.2647691> [1]. The experimental design, implementation, and analysis were carried out primarily by the author of this thesis, with the co-authors providing supervision, guidance, and feedback on the research and manuscript.

5.1 White Rabbit Time-Synchronisation and QKD

Quantum communications technologies, and QKD in particular, are increasingly progressing toward practical real-life applications, leveraging existing optical infrastructures to establish the foundations of a future quantum internet [9]. Achieving this objective requires not only compatibility between quantum and classical hardware, but may also necessitate the coexistence of quantum and classical signals within the same optical fibre [112, 113, 114, 115, 116].

One of the most fundamental features of any network, which is likely to be preserved in the development of the quantum internet, is the synchronisation of operations between its nodes. The importance of precise time-distribution in large-scale networks has been recognised by

researchers at CERN, who in 2011 introduced the White Rabbit (WR) protocol as a form of high-accuracy, low-latency time synchronisation over optical fibres [117].

WR is an optical clock distribution scheme that achieves sub-nanosecond precision over tens of kilometres in optical fibre, with a jitter of the order of picoseconds. Recent advances have further extended its capabilities, demonstrating unrepeated WR synchronisation over distances of up to 300 km [118]. As a result, WR meets the requirements of modern QKD systems, which operate at gigahertz clock rates over tens of kilometres in optical fibre [119, 120, 121], in terms of speed, precision, propagation medium, and range. Moreover, commercially available WR solutions offer off-the-shelf, plug-and-play, inexpensive devices, enhancing the practical viability of this approach.

Current QKD modules include sub-systems, sub-routines and often a separate optical channel to transmit the time information between the users, thus requiring additional hardware and software that increase complexity and cost of the modules. In the foreseeable future, optical networks will offer precise time distribution as a service. QKD suppliers could therefore leverage the network's timing capability to simplify their systems, reducing their cost but also the risk of quantum hacking based on manipulating time information [28, 122].

WR signals are launched in a power regime of 0.1–1 mW, hence they can be considered 'classical'. These signals cause broadband Raman scattering which, in turn, introduces noise to the quantum transmission and affects the overall performance of QKD. At the time that this work was conducted, prior work had shown the synchronisation of QKD systems by means of WR [123]. However, that demonstration was limited to using separate fibres for QKD and WR signals, thus leaving the question of their coexistence on the same fibre open. The purpose of this investigation is to demonstrate the distribution of single photons suitable for QKD over kilometre-scale optical fibres in the presence of bidirectional classical WR communication co-propagating within the same fibre as the QKD photons. Since the completion of this work, subsequent studies have further explored WR and quantum entanglement coexistence [124, 71], extending transmission distances and providing more comprehensive characterisation, including distance-dependent noise-profiling and detailed entanglement measurements.

This implementation emphasises practicality as it relies exclusively on cost-effective components. It uses the entanglement system developed in Chapter 3.3 as well as off-the-shelf Wavelength Division Multiplexing (WDM) components, filters and SPADs. The WR clock distribution is monitored and achieves sub-nanosecond precision. This scheme therefore allows distant users to post-select correlated detection events in a real-life QKD implementation. The large bandwidth of the emitted photons from the EPS and the network-oriented versatility of the WDMs are ideal for a network implementation with multiple users.

In this work, the correlation visibility of the distributed polarisation-entangled photons is measured and shown to remain suitable for QKD in the presence of WR signals. The measurements are performed in a network configuration that reflects existing optical networks, thereby facilitating future field deployment. These results demonstrate that the presented polarisation entanglement system can coexist with the classical signals in an optical WR network, while requiring only minimal modification to standard WDM and WR components.

of the distributed photons. The PAs used in this experiment correspond to the setup introduced in Section 3.3, i.e. a linear setup of a Half-WavePlate (HWP), a Quarter-WavePlate (QWP) and a Linear Polariser (LP). As such, polarisation state measurements are conducted individually.

The source of quantum states is the compact entangled photon source (EPS) introduced in Section 2.3. It exploits type-0 Spontaneous Parametric Down Conversion (SPDC) from a 25 mm Periodically-Poled Lithium Niobate (PPLN) crystal interferometer to generate the following maximally entangled state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|H\rangle_a |H\rangle_b + |V\rangle_a |V\rangle_b) = \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle) \quad (5.1)$$

$|H\rangle_j, |V\rangle_j$ are the eigenvectors of the $\mathbb{Z}$ matrix and a, b denote the signal and idler photons respectively. Signal and idler photons are produced symmetrically over 1560 nm, with a total bandwidth of approximately 60 nm, and separated by an internal dichroic mirror at 1565 nm. The optical spectrum of the EPS's signal and idler photons is shown in Fig 5.1 b).

The WR modules used in this study incorporate standard off-the-shelf Small Form-factor Pluggable (SFP) transceivers, operating at 1270 nm and 1330 nm with output powers of 0.562 mW and 0.793 mW respectively, suited for optical SMF links up to 10 km. The dominant scattering mechanism introducing noise into the quantum channel is spontaneous Raman scattering, which generates broadband photons that may overlap spectrally with the single-photon signals. This process occurs both in the forward (co-propagating) and backward (counter-propagating) direction of the classical signals.

In this experiment, the signal photons travel through a set of optical add-drop modules to facilitate the inclusion of additional classical WR signals on the signal photon channel. An off-the-shelf Dense Wavelength-Division Multiplexing (DWDM) module, spanning the 100 GHz ITU grid channels 35–42 (1549.32 nm–1543.73 nm), is used to filter the signal into the ITU channel 35, corresponding to 1549.32 nm. In future implementations, the DWDM module and its additional channels are intended to emulate a network of multiple users, each receiving a different wavelength channel from the source. Such QKD network architectures have been demonstrated previously [43, 42]. On the idler side, an Optical Tunable Filter (OTF) is used to select photons corresponding to a particular signal DWDM channel.

The photon polarisation is analysed in the $\mathbb{Z}$ ($\{|H\rangle, |V\rangle\}$) and $\mathbb{X}$ ($\{|D\rangle, |A\rangle\}$) bases, as required for the 4-state BB84 protocol. The setup achieves this via the Polarisation Analysers (PA in Fig. 5.1 a)), which in this representation consist of the PAs as introduced in Section 3.3 preceded by a fibre-optic Manual Polarisation Controller (MPC). The MPCs are used to compensate for any change in the polarisation state that occurs between the SPDC crystal and the analysing units. The PAs then couple the light from fibre to free-space and measurement basis selection is performed via the appropriate HWP, QWP and LP configuration.

The signal and idler photons are detected using InGaAs SPADs, specifically one free-running ID220 (D1) and one gated PDM detector (P2), chosen for their superior noise parameters. The signal detection gate of the PDM is conditioned on the detection of an idler photon by

the free-running detector, thereby implementing heralded detection to improve the signal-to-noise ratio. This approach yields measured visibilities comparable to those obtained using SNSPDs in Chapter 4 while maintaining the emphasis on practicality through the use of more cost-effective SPADs.

In the laboratory setting, the SPADs' performance can be significantly improved by using the idler photon as a trigger and gating the signal photon detection. For distant users however, this practice may not be feasible as it relies on sequential arrival of the idler photon, the signal-gating pulse, and lastly the signal photon. An alternative is to operate both SPADs in gated mode, which significantly reduces dark counts, and is particularly feasible if combined with a well-timed, pulsed photon source. This highlights the necessity of distributing a precise clock alongside the quantum signal to synchronise independent SPAD gating and enable post-selection of correlated events.

During each experiment, the WR clocks are monitored separately to ensure that they are synchronised throughout. Two experiments are performed using single-mode fibre channels in the signal and idler branches, with lengths of a few meters in the first experiment and 1 km in the second. For each configuration, the polarisation measurements are performed when the WR modules are ON and OFF to provide a direct measure of the impact of the WR signals on the quality of the distributed quantum states.

5.3 Entanglement Visibility Results

For a BBM92-type QKD protocol using distributed entangled photons, the polarisation measurements on the signal and idler photons should theoretically result in 100% correlated measurements when measured in the same basis and show only statistical (i.e. 50%) correlation when different measurement bases are chosen. The results of the polarisation measurements are shown in Figs. 5.2 a), b) and 5.2 c), d) for the short and the 1 km fibre channels respectively. The visibility between the maximum and minimum coincidence counts for each orthogonal pair of linear polarisation states is calculated, where the maximum and minimum number of coincidences occur when the signal and idler photon states are parallel and orthogonal respectively.

The visibility values for each polarisation state pair are shown in Figure 5.3 for both experimental configurations. Due to differences in the accuracy of the channel compensation, the 1 km scenario exhibits slightly higher visibilities than the short-fibre case, despite the increased loss that would ordinarily be expected to reduce visibility. Nevertheless, the visibility values for the WR-On and WR-Off conditions for a given fibre length are obtained under identical channel compensation and are therefore directly comparable.

In all scenarios, the presence of the WR signals introduces only a minor reduction in visibility of the entangled states, with the maximum decrease amounting to 2.44%. Overall, the visibility with WR-On remains above 96% in both the $\mathbb{Z}$ and $\mathbb{X}$ bases, corresponding to a Quantum Bit Error Rate (QBER) below 2%. These results demonstrate that QKD and entanglement distribution can reliably co-exist with WR-based time distribution.

5.3. ENTANGLEMENT VISIBILITY RESULTS

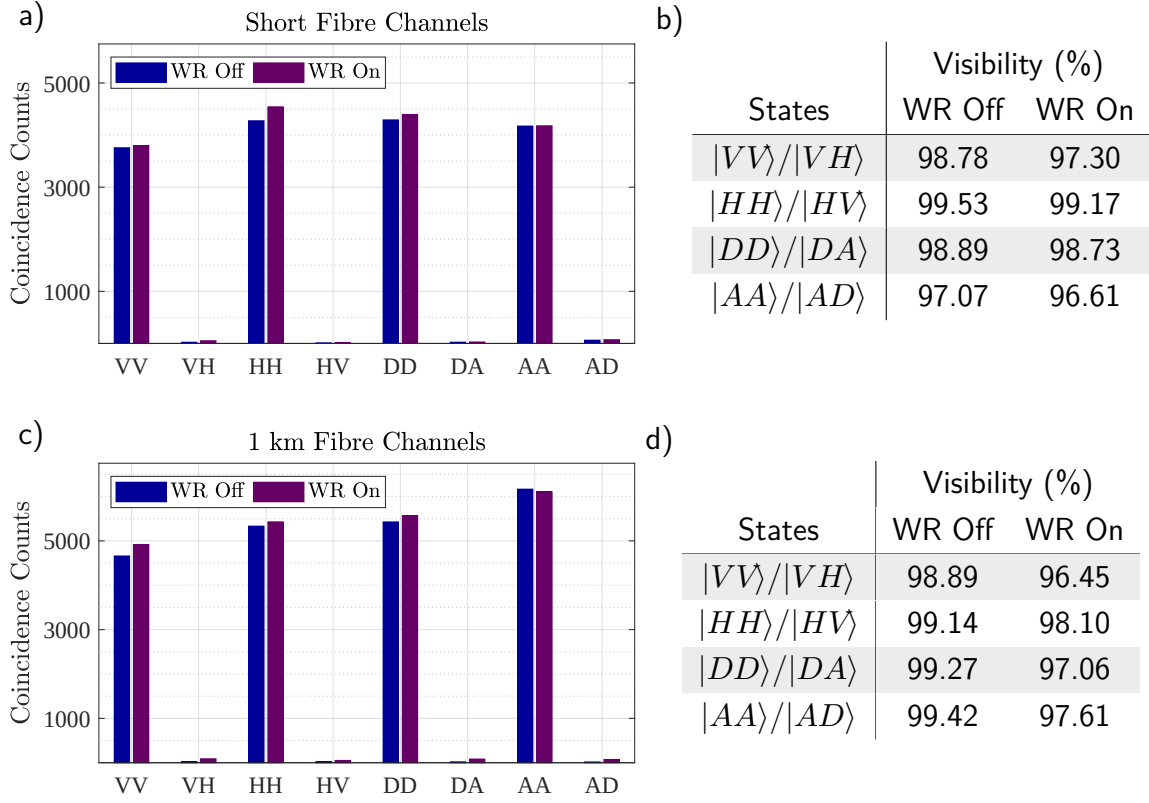


Figure 5.2: a) Coincidence counts registered over 2 minutes between the two SPADs. The single-mode fibre channels are 11 m long and measurements are taken with the WR signals ON and OFF. The settings of the PAs are detailed on the x-axis where, for example, VH indicates when the system is measuring for occurrences of $|V\rangle_a |H\rangle_b$. b) The visibility of the coincidence counts between the pairs of linear orthogonal states, calculated from the data shown in a). Figures c) and d) are equivalent to a) and b) with an extended channel length to the single-mode fibre to 1 km.

To further evaluate the quality of the distributed signals in a QKD context, an additional set of measurements was taken for the 1 km channel configuration, in which polarisation measurements were conducted for all combinations of rectilinear and diagonal states. The results for the WR-Off and WR-On conditions are shown in Figure 5.3. Simultaneous measurements in mismatched bases yield correlations of approximately 50%, as expected for the $\mathbb{Z}$ and $\mathbb{X}$ bases.

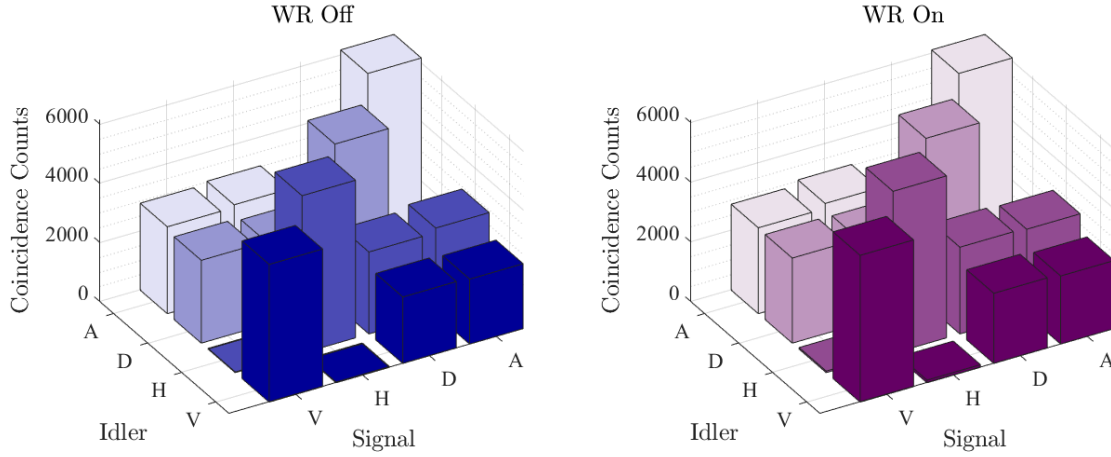


Figure 5.3: Coincidence counts registered over 2 minutes by two SPADs for the two 1 km channels with WR OFF and ON. All state combinations leveraged in BBM92 generate the expected coincidence probabilities, even in the presence of the classical WR signals.

5.4 Conclusion & Future Work

The distribution of entangled single photon polarisation states in the presence of classical White Rabbit time-synchronisation is demonstrated with high visibility over optical fibres up to 1 km. The results show that quantum key distribution can be achieved and maintained in coexistence with the classical optical signals, with only a marginal increase in the quantum bit error rate when the time synchronisation is enabled. This is realised in an experimental setup modelled on current network architectures, to which the quantum functionality is integrated through the use of simple add-drop modules.

Building on these results, several avenues for future work remain. The current setup is primarily limited by the design of the PAs, which does not permit reliable transmission channel compensation and is inefficient for increasing numbers of polarisation state measurements. Leveraging the final PA design from Chapters 3, together with the measurement routines established in Chapter 4, the scope of this coexistence study could be substantially expanded. The following suggested further experiments are achievable with already present laboratory equipment, unless stated otherwise.

The channel can be extended to explore the impact of transmission over realistic channels lengths on coexistence. In standard SMF, Raman scattering is predicted to reach a maximum approximately 20 km [115], where the interplay between scattering and channel attenuation is balanced. Consequently, measurements at or beyond this distance are critical for assessing the feasibility of WR-QKD coexistence, and longer-distance demonstrations further strengthen the case for practical implementation.

Furthermore, the current setup can be expanded to quantify entanglement via an entanglement witness, such as the CHSH inequality, and ultimately implement a full QKD protocol. To the best of the author's knowledge, existing studies on entanglement in the presence of WR signals have not yet demonstrated key generation or explicitly assessed the feasibility of quantum communication. This expansion would also encompass the synchronisation of two time taggers via WR, representing a realistic scenario with physically separated nodes, as well as the inclusion of WR in the channels in both the signal and idler channels.

Such demonstrations could be conducted over a variety of channel types, including extended SMF links in the laboratory, deployed fibre channels across the University of York campus, and hollow-core fibre channels. As indicated by the existing hardware capabilities, measurements can also be performed for different ITU channels accessible via the DWDM and OTF, or alternatively, using two wavelength-matched DWDMs if one is procured for the idler channel. This approach would simulate WR synchronisation and operation within a multi-user network akin to existing network-oriented demonstrations [43, 42].

The incorporated WR modules could also be further optimised by investigating the wavelength-dependence of the Raman scattering. Alternative SFP modules, including those operating at longer wavelengths such as 1610 nm, are available for such studies. The level of noise introduced into the quantum channel depends on both propagation direction of the classical signal, as well as their wavelength-detuning relative to the quantum signals. Determining which WR signals should co- or counter-propagate, and whether signals at lower energies than the quantum signal are advantageous, represents a potential subject for future investigations.

Chapter 6

Feasibility of Entanglement-Based Quantum Communications over a 224 km Undersea Optical Fibre Link

This chapter presents the entanglement-based investigations conducted within the framework of a field trial designed to evaluate the feasibility of quantum communications over a 224 km deployed fibre link, which is currently employed for high-speed traditional optical communications. In addition to results from the experimental campaign, the chapter also includes preliminary and follow-up laboratory-based experiments that supplement the work conducted in the field. This research plays a crucial role in advancing the readiness of QKD technology for practical deployment, representing a significant step toward integrating quantum communication systems into existing, real-world communication infrastructures.

This study builds upon the entanglement system developed in the preceding chapters. An intermediate version of the PAs, as presented in Section 3.4, was deployed for the field trial, but was ultimately not used due to adverse experimental conditions. Field trials such as this represent one of the key proposed applications for the system, which has been tailored for deployed use through the inclusion of compact and robust transmitters and receivers. Furthermore, the deployment of sensitive instruments such as the SNSPD system was made possible by intimate familiarity with the equipment and accurate assessment of operational requirements obtained through the work described in Chapter 2.

The work presented here includes results published in: Amies-King, B.; Schatz, K.P.; Duan, H.; Biswas, A.; Bailey, J.; Felvinti, A.; Winward, J.; Dixon, M.; Minder, M.; Kumar, R.; et al. Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link. *Entropy* 2023, 25, 1572. <https://doi.org/10.3390/e25121572> [2]. The experimental design, implementation, and analysis presented in this thesis were carried out primarily by the author, with contributions from the co-authors including supervision, experimental assistance during the field trial, and feedback on the research and manuscript. The only exception is the characterisation of the Rockabill-link time-dependent polarisation stability, which was performed primarily by Mr Haofan Duan, with assistance from the author.

6.1 The UK-Ireland Feasibility Study

International quantum communication links play a vital role in the establishment of a global quantum internet [9]. To date, only a limited number of cross-border QKD demonstrations have been reported, with the majority implemented either on deployed terrestrial fibre [50, 85] or via satellite-based links [125, 126, 53]. Undersea fibres, despite their widespread use in international classical information traffic, represent a largely unexplored scenario. Aside from the link investigated in this work, only one submarine optical fibre system has been systematically evaluated for QKD purposes: a 92 km (or 192 km in round-trip configuration) optical fibre under the Mediterranean Sea connecting Sicily and Malta [94, 95].

This chapter presents investigations performed on the 224 km *Rockabill* link [2], deployed by the company euNetworks between Cable Landing Stations (CLSs) in Southport (UK) and Portrane (IE). Figure 6.1 a) presents a geographic representation of the Rockabill link, illustrating its extent and relation to Dublin, Manchester and York. The channel has a total effective loss per fibre of 38.1–38.7 dB, which equates to a remarkably low average attenuation per kilometre of approximately 0.17 dB/km. This low attenuation enables classical communications between the two endpoints without the need for intermediate optical repeaters, and provides low latency to meet the requirements of existing users, such as those in the financial sector. These characteristics make the Rockabill link a natural candidate for extending quantum communication links between the United Kingdom and Ireland.

Therefore, an experimental campaign was conducted to assess the link's suitability for distributing quantum states for QKD purposes, termed the the UK-Ireland (UK-IE) field trial. A total of two equivalent pairs of dark fibre (identified as channels 39 and 40; and 59 and 60) were utilised in the submarine Rockabill link. These fibres under test were routed within a bundle comprising several active telecommunication fibres carrying high-intensity signals. The trial encompasses phase-based investigations, polarisation state dissemination for BB84, and entanglement distribution (schematically represented in Figure 6.1 b)). Together, these studies provide a comprehensive assessment of the feasibility of quantum communications via the Rockabill link. The following sections report on the noise- and polarisation-related channel characterisation in the context of QKD, the distribution and detection of entangled photon pairs over the submarine link, and supporting laboratory-based experiments. Further contributions to the field trial by the author include the preparation, relocation, and operation of experimental equipment at the CLSs, in particular the entanglement receivers and SNSPD system at the Southport CLS.

The Portrane CLS housed all transmitting equipment, including the EPS and 1550 nm coherent lasers. The receiving equipment, comprising the SNSPD system (ID281), SPADs and classical detectors, was located at the Southport CLS. Two detector channels, with respective detection efficiencies of 93.0 % and 90.5 % and dark count rates of less than 70 Hz each, were employed in the investigations detailed in this chapter.

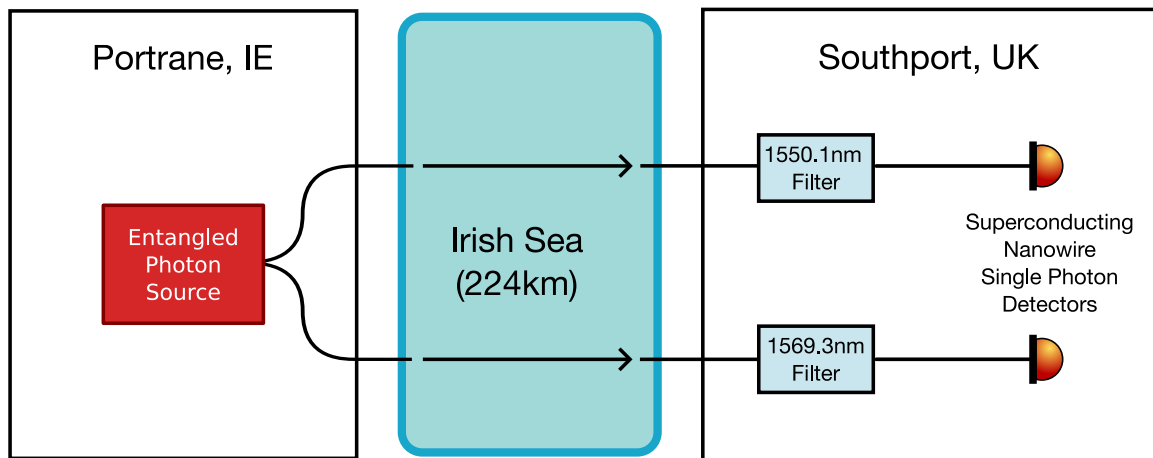
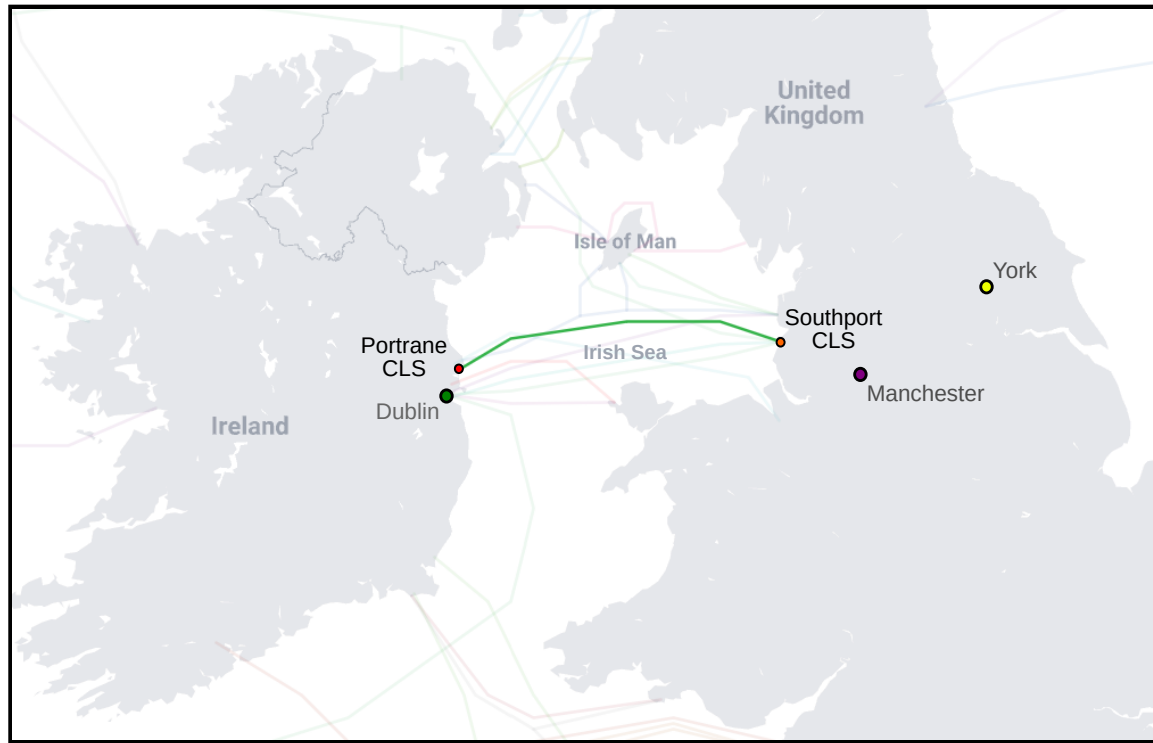


Figure 6.1: a) Geographic representation of the Rockabill link (green), Cable Landing Stations (CLS) and major nearby cities. Faintly indicated are other submarine optical fibre connections. b) Schematic experimental setup of the entanglement distribution via the UK-Ireland link. Channels 59 & 60 were employed for this investigation due to a preferable noise profile.

6.2 Laboratory-Based Channel Emulation

Prior to gaining access to the CLSs, preparatory measurements were conducted in the EQC laboratory. These tests focused on the correlated arrival times of the EPS photon pairs after different physical emulations of the Rockabill link, each progressively closer to the final field implementation. No measurement of the photons' polarisation were performed; this study instead assesses the ability to detect photon pairs after nearly 2×40 dB of attenuation. The experimental setup corresponds to Figure 6.1 b), with fixed attenuators and spools of SMF replacing the channel.

Initially, fixed attenuators were used to apply approximately 40 dB of attenuation to each photon. Using a 1 ns coincidence window and the EPS at full pump power, a Coincidence to Accidental Ratio (CAR) of 6 was observed. Subsequently, spools of Single-Mode Fibre (SMF) were added symmetrically on each arm in 50 km increments, up to a total channel length of 200 km. As mentioned above, the Rockabill link has an average attenuation coefficient of $\alpha = 0.17$ dB/km, which is lower than that of standard SMF, resulting in approximately 38 dB of attenuation over 224 km. To emulate the link on the laboratory, a combination of 0.2 dB standard SMF and 0.16 dB Ultra Low Loss (ULL) fibre spools was used, producing a total attenuation of 38 dB after 200 km.

The CAR observed after each added spool is listed in Table 6.1. With an actual channel in place and EPS pairs that are not perfectly wavelength-degenerate, the photons experience chromatic dispersion. This leads to a temporal broadening of the coincidence peak, as the photons at different wavelengths propagate at different group-velocities. This broadening can be approximated as $\Delta t_{\text{disp}} = D\Delta\lambda L$, where D is the fibre dispersion parameter, which was assumed to be comparable to the typically value for SMF of 17 ps/(nm·km) (see Section 4.6), $\Delta\lambda$ is the spectral separation of the photons, and L is the channel length.

Channel Length (km)	CAR	Coincidence Window (ns)
50	14.5	2.5
100	8.1	5.0
150	3.8*	7.5
200	4.4	12

Table 6.1: Approximate CAR and coincidence peak widths observed during the laboratory emulation of the Rockabill link, before optimisation of SNSPD voltages. All fibre spools were standard SMF, except for the second 50 km spool in each channel, which was ULL fibre. The value for 150 km was calculated using an overestimated coincidence window of 10 ns, leading to a proportionately lower CAR.

Finally, once the full 200 km channel was established, the SNSPD detection efficiencies were adjusted to optimise the signal-to-noise ratio and maximise the CAR. A final measurement with an integration time of 10 hours was performed. The resulting coincidence peak is shown in Figure 6.2, yielding a CAR of ~ 6 .

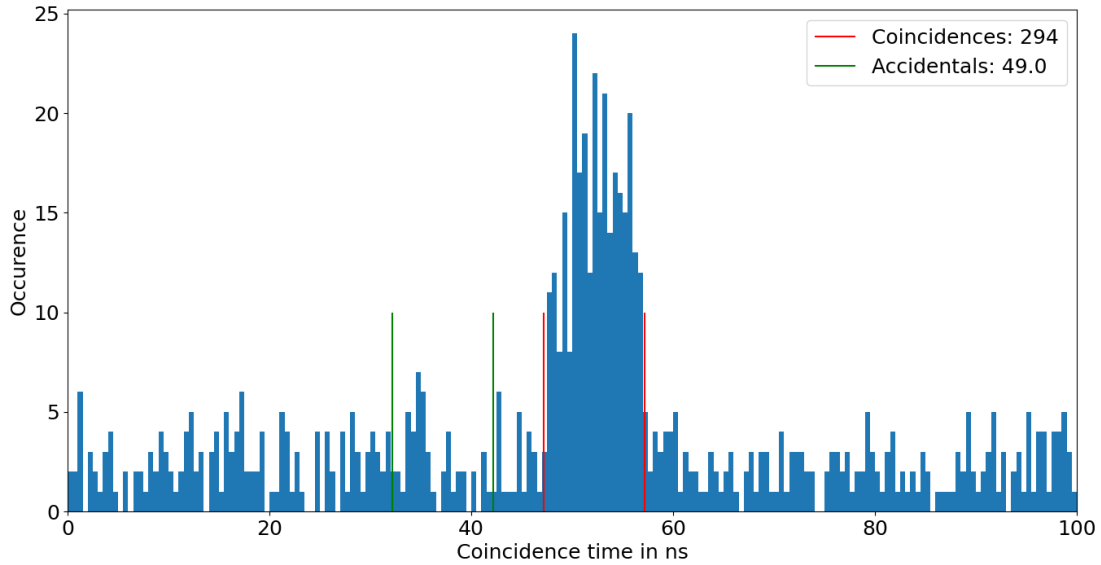


Figure 6.2: Coincidences of photons emitted by the EPS after travelling through 200 km of SMF for each the signal and idler channel over 10 hours. Coincidences are discernable above the background with a $CAR \approx 6$. Measurements taken with spools of SMF in a laboratory environment.

This value is prohibitively low for the analysis of the entangled polarisation state, as the inclusion of a PA would introduce additional losses on the order of at least 4 dB arising from insertion losses and the splitting of the beam into two polarisation eigenstates. However, the detector background noise was relatively high in the laboratory environment (around 130 Hz) due to insufficient temperature regulation, and was expected to be reduced under field conditions. Furthermore, no information was available regarding the chromatic dispersion characteristics of the deployed fibre, which may be lower than that of standard fibre given the state-of-the-art nature of the facility. Taken together, these considerations suggested that polarisation measurements could be feasible on the deployed link, although a definitive assessment could only be made during the final trial. Regardless, temporal identification of EPS pairs after transmission through the Rockabill channel was expected to remain achievable.

6.3 Dark Fibre Noise Level

Shortly after single-photon experiments commenced, it was discovered that the presence of bright, active fibres within the same bundle as the experimental fibres led to significant cross talk between channels and, consequently, an unexpectedly high noise floor. A series of tests was conducted to characterise the source of this noise and its impact on the quantum signals. During these tests, the channel inputs in Portrane were terminated, and various instruments were connected within the darkened Southport CLS to investigate the light received at that location.

Firstly, a 12 hour overnight measurement of the single-photon count rate on an individual channel fibre was collected using a SPAD. The measurement exhibits a remarkable long-term

stability of the noise amplitude, with a standard deviation of less than 0.5%. This measurement spanned both sunset and sunrise, indicating that the channel background is not affected by the time of day. Furthermore, coarse and fine sweeps of the noise wavelength spectrum were conducted using the Optical Tunable Filter (OTF) placed directly before the SNSPD at optical bandwidths of 125 and 100 GHz, respectively. The results of the coarse sweep for two selected channels are shown in Figure 6.3. The spectrum does not correspond to a typical scattering process or thermal emission; instead, it resembles a convolution of several peaks with varying amplitudes and widths. This figure also includes a reference measurement in which the fibre channel was completely disconnected from the setup, allowing the noise originating from the CLS itself to be monitored. The observed minimal count rates at the detector DCR level of 70 Hz rule out the possibility of stray light entering the exposed fibre within the CLS. Furthermore, a brief investigation using an MPC followed by a linear polariser indicated that the overall noise does not exhibit a preferred polarisation orientation, whereas individual peaks isolated with the tuneable optical filter were found to be at least partially polarised.

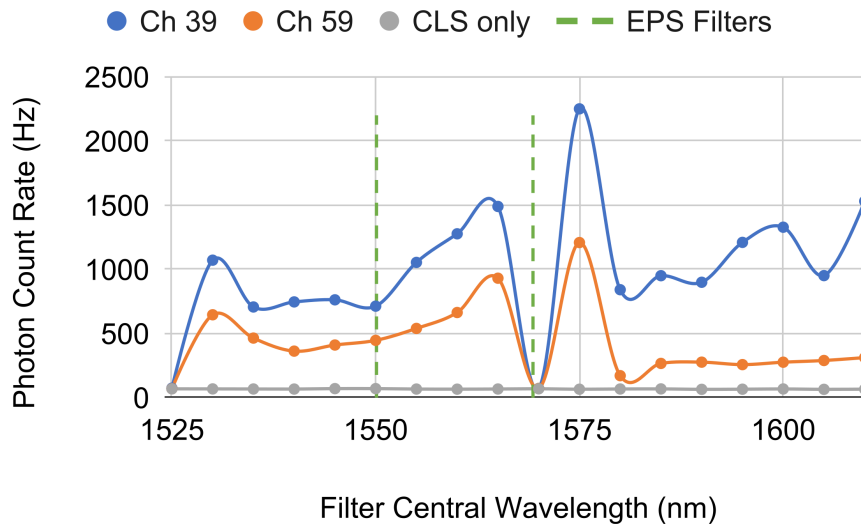


Figure 6.3: Single photon count rates as a function of wavelength as filtered with the OTF set to 1 nm width, measured for two fibres in the Rockabill link and the detection system in the Southport CLS terminated at the channel entrance.

Combining the above results, it can be concluded that the observed noise is primarily caused by stray photons from other active fibres entering the channels under test, most likely due to back-reflections of bright signals leaking into the quantum channel near the detection setup in Southport. This background noise present across all channels arriving at the CLS, although its magnitude varies considerably from channel to channel, likely due to the relative physical proximity to the most active fibres. For the two fibre pairs used in this work, noise count rates between 120 kHz to 410 kHz were recorded when the full spectrum was allowed to reach the SNSPD. The introduction of optical filters with approximately 1 nm bandwidth significantly mitigates this noise, enabling reliable measurements at the quantum level. Effective dark counts for the single-photon experiments reported here range from 90 Hz to as high as 2.2 kHz depending on the central wavelength of the employed filters.

6.4 Polarisation Stability

The long-term polarisation drift of the Rockabill link was measured by Mr. Haofan Duan over a period of nearly 14 hours, and is included here due to its relevance for the subsequent discussion on the viability of entanglement distribution. The data were obtained by sending light from a 1550 nm coherent laser through the channel and onto a Polarising Beam Splitter (PBS), with its outputs monitored using classical photodetectors. The initial polarisation state was aligned with the horizontal axis of the PBS. The resulting polarisation drift of the channel is presented in Figure 6.4.

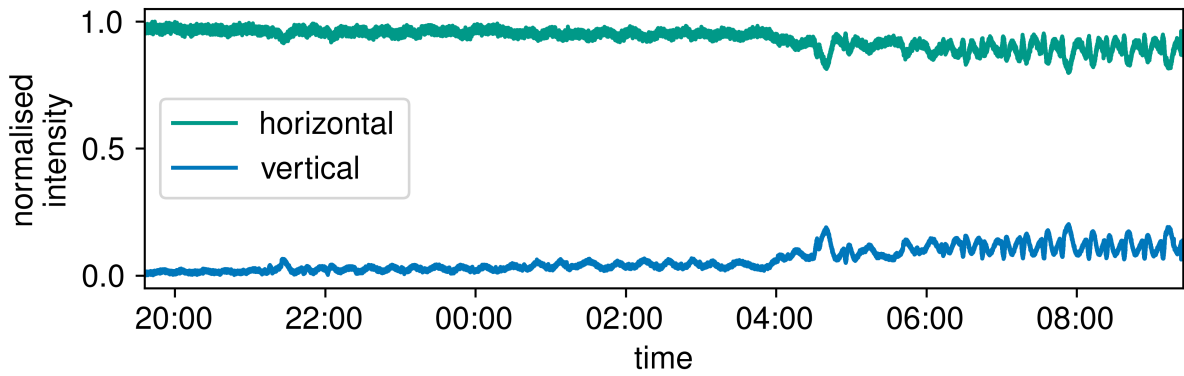


Figure 6.4: The long-term polarisation drift of the channel over 14 hours overnight.

The polarisation remains remarkably stable for approximately 9 hours, after which the observed state begins to drift significantly, possibly due to a singular disruption in one of the CLSs. Beyond this point, the data exhibit periodic drifts on a timescale of minutes, indicative of a misalignment between a static polarisation state and a polarisation-dependent component with a beat length of similar scale. This measurement was conducted between 19:35 on 5 July 2023 and 09:35 on 6 July 2023. Neither sunrise nor sunset, occurring around 05:00 and 22:00 respectively, appear to cause any noticeable changes in the polarisation or its drift rate. Overall, the channel demonstrated a remarkably stable polarisation transformation for deployed fibre, which can be attributed to the thermal and mechanical isolation effected by the Irish Sea, as well as high-quality environmental control within the CLS.

6.5 Distribution of Photon Pairs from a Source of Polarisation Entanglement

In this feasibility study, the Rockabill link's capability to distribute entangled photon pairs is explored by identifying the time-correlated arrival of photon pairs produced by the EPS. A schematic representation of the experimental setup can be seen in Figure 6.1 b). At the Portrane CLS, the EPS signal and idler outputs are coupled directly into two channel fibres (Ch 59 & Ch 60), traverse 224 km each through the deployed undersea fibre, and emerge at the Southport CLS. There, optical filters centred at 1550.1 nm and 1569.3 nm with equal pass

6.5. DISTRIBUTION OF PHOTON PAIRS FROM A SOURCE OF POLARISATION ENTANGLEMENT

bands of $\Delta = 1.39$ nm are used to isolate entangled pairs, which are subsequently detected by the SNSPD system.

The selected filtering balances time-of-flight broadening of measured photon arrival times caused by chromatic dispersion with admittance of a sufficient number of photons, particularly after the source brightness has been attenuated by 2×38 dB of optical loss. More importantly, the filtering mitigates cross-talk in the channel, as discussed in Section 6.3. This approach exploits the fact that the noise spectrum exhibits a minimum around 1570 nm, which is coincidentally already used for idler detection and simultaneously positions the signal wavelength at the conventional telecom wavelength of 1550 nm. Despite the spectral filtering, the residual channel noise remains comparable to the signal amplitude. It should be noted that the idler channel experiences approximately 5 dB of additional attenuation relative to the signal channel due to the high-insertion-loss OTF, which is reflected in the detected count rate.

Since the SNSPD efficiency is polarisation-dependent, a polarisation alignment procedure is performed to maximise the probability of detecting photon pairs. This procedure involves blocking one arm of the source interferometer to produce the non-entangled two-photon state $|\Psi\rangle = |HH\rangle$ and using MPCs to align this state with the SNSPD's preferred polarisation axis. Due to the very low absolute count rates observed at Southport, this optimisation could not be performed reliably, leading to small discrepancies between subsequent measurements. However, the data are reproducible enough to consider the detection of pairs from the EPS successful.

Using this entanglement distribution setup, two datasets were recorded, each accumulating single-photon detection events over a period of 12 hours. After transmission through the submarine channels, the single-photon count rates for each individual channel were only a few hundred Hertz above the background, yielding a signal-to-noise ratio below one for the noisier 1550.1 nm channel. Results are presented for both datasets; however, only the better aligned measurement is discussed in detail in the following.

In the better aligned measurement, the signal channel at 1550.1 nm recorded a single count rate of 2.703 kHz over a background of 2.171 kHz, whereas the much lower noise idler channel at 1569.3 nm produced a total count rate of 258 Hz over an 88 Hz background.

Figure 6.5 illustrates the difference in pair-photon arrival times for both channels relative to a common reference clock in the better-aligned dataset. A fixed offset of 113 ns is present, arising from minor channel length differences, primarily introduced by the instrumentation. The peak corresponding to the simultaneously produced photons in each pair is clearly visible. Considering the low $g^2(0) < 0.01$ and high entanglement fidelity of more than 99%, obtained in Chapters 2 and 4 respectively, this peak is expected to consist predominantly of entangled photons, with negligible contributions from multi-photon emissions.

Photon pairs can be identified within a coincidence window of 12 ns, which is consistent with the expected temporal broadening due to chromatic dispersion over 2×224 km given by the experimental channel emulation described in Section 4.6.2. Furthermore, the observed number of accidental photon coincidences agrees with the statistically expected value based on the individual count rates. The coincidence counts exceed this baseline with a CAR of 1.92

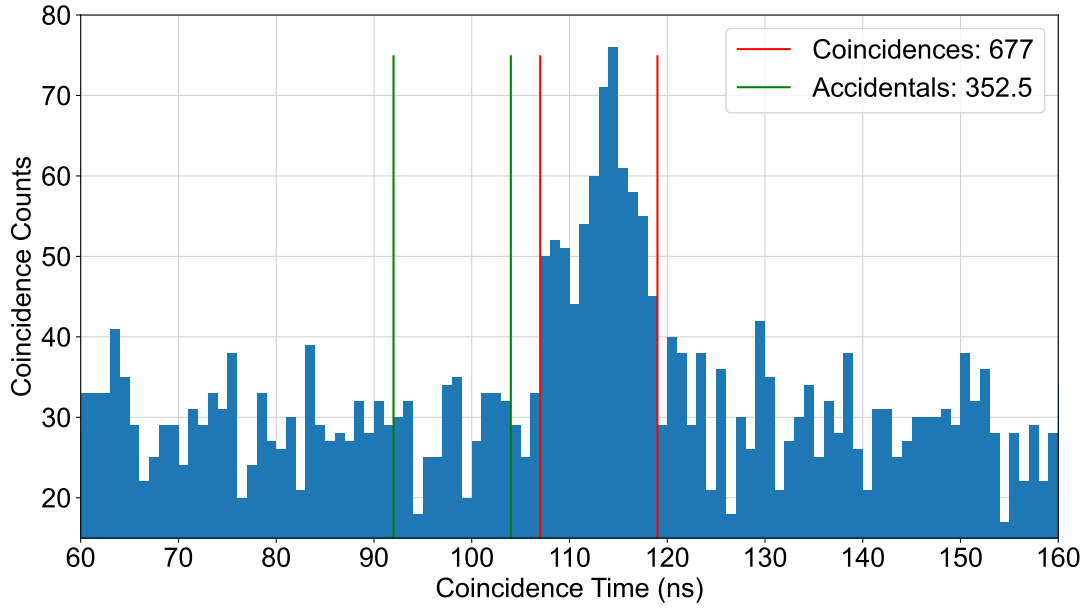


Figure 6.5: Histogram of the time delays between consecutive photon detections at the end of the two submarine channels. Pair photons from the EPS arrive with a fixed relative delay of 113 ns at a signal-to-noise ratio of 1.92, computed over the indicated red 12 ns coincidence window. The green lines represent one possible off-peak coincidence window including only accidentals.

in the better-aligned measurement and 1.80 for the other dataset. The presence of a clear peak in Figure 6.5 is encouraging and supports the feasibility of entanglement distribution over the link, especially in realistic configurations that involve only one of the two entangled photons travelling across the undersea channel. However, a more pronounced demonstration was ultimately prohibited by the restricted source brightness, the elevated noise levels described above, and the scope of the field trial.

6.6 Underwater Polarisation-Stability Study

Following the field trial, an attempt was made to replicate the exceptional stability of the undersea channel with respect to polarisation in the laboratory environment in order to facilitate further supplementary measurements of the entangled polarisation state. This stability is attributed to the isolation experienced by the fibre bundles when underwater, resulting in minimal mechanical perturbations and a highly stable thermal environment. In contrast, for fibre links of comparable length in a laboratory setting, the polarisation is typically insufficiently stable to support entanglement measurements without active polarisation stabilisation.

Within the Institute for Safe Autonomy, which houses the EQC Group, the experimental facilities of the Underwater Information Systems group (lead by Professor Paul Mitchell) provided access to a 2 m deep pool that could serve as an initial approximation of submarine conditions. An experiment was therefore conceived to investigate the stabilisation of optical fibre through submersion it in water. Although the pool was not actively temperature-stabilised, a 24-hour

6.6. UNDERWATER POLARISATION-STABILITY STUDY

monitoring period indicated that the temperature remains stable within 1°C. The pool also exhibits a small, steady current, which has the potential to influence the fibre birefringence.

Prior to the installation of the experimental setup, tests were conducted to determine whether protective measures were required to prevent damage to the optical fibre by the water. A 6.3 km test spool of standard SMF was submerged in water, initially for a short duration and subsequently for extended periods. No damage was observed after submersion for multiple days, as verified by Optical Time-Domain Reflectometry (OTDR) measurements performed before and after each trial, including a drying period. In total, the spool was submerged three times: once briefly and twice for several days. The OTDR traces were consistent across all measurements.

To monitor polarisation stability, light from a coherent 1550 nm laser source was transmitted through the 6.3 km fibre spool and recorded using a polarimeter over time periods comparable to the UK-IE experiments. These measurements were then compared with equivalent measurements performed on a laboratory table, representing unmitigated polarisation drift. Selected results are presented in Figure 6.6.

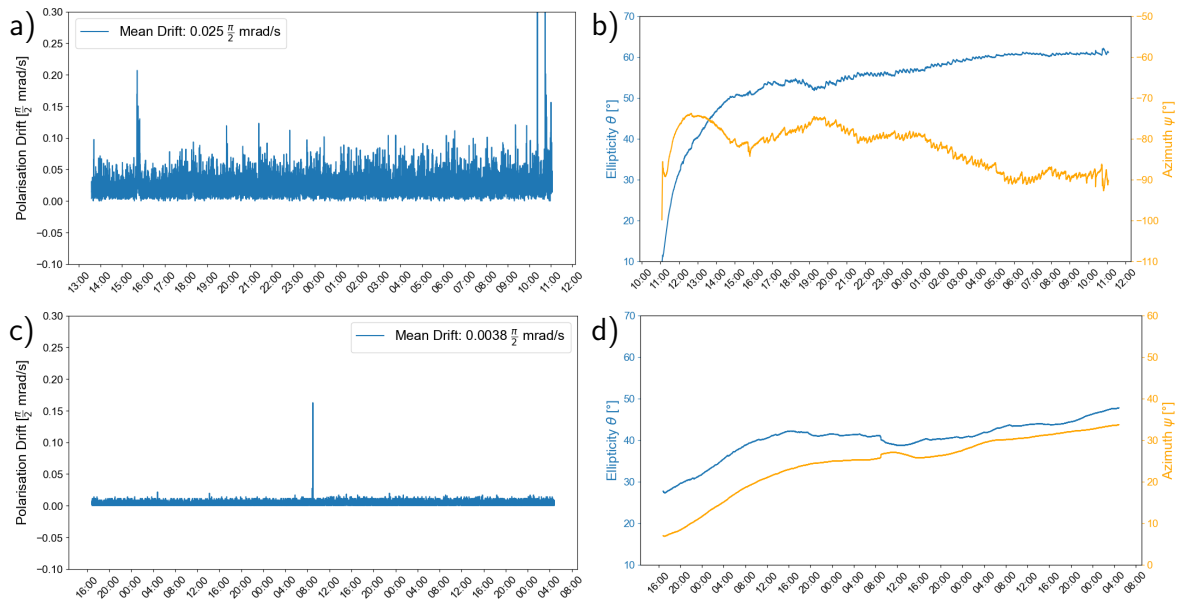


Figure 6.6: a) Relative and b) absolute polarisation drift as a function of time for a 6.3 km SMF spool in the laboratory environment. c) Relative and d) absolute polarisation drift for a 6.3 km spool submerged 1.5 m deep in the pool.

Measurements were conducted under three conditions: on a laboratory bench, just below the water surface, and at a depth of 1.5 m within the pool. Observations made on the polarisation stability were consistently present when transitioning from air to water and became more apparent with increased submersion. As shown in Figure 6.6, immersion in water effectively suppresses high-frequency polarisation drift. However, a gradual drift over longer timescales persists and may even be more pronounced than in the dry fibre.

Several factors may contribute to this behaviour. First, the pool temperature is not stabilised and therefore, given the higher thermal conductivity of water compared to air, the fibre spool is likely to more closely track ambient temperature variations. Second, the fibre was not shielded from the pool's current, which may have exerted mechanical forces on the fibre and induced a slow drift over time. Finally, is it possible that the fibre required a longer equilibration period in this environment and was simply not submerged for a sufficient duration prior to measurement.

Further experiments addressing the factors outlined above could enable the development of a stable test-bed comprising hundreds of kilometres of fibre; however, these were not pursued as they are beyond the scope of this work. Nevertheless, the present results serve to emphasise the significant advantage offered by the highly stable submarine fibre in the Rockabill link.

6.7 Conclusions & Future Work

The experiments presented in this chapter demonstrate the feasibility of entanglement distribution on a 224 km submarine optical fibre link under realistic deployment conditions. The underwater environment provides a comparatively stable transmission channel, enabling reliable quantum state distribution over long distances, and the observed photon transmission from the entanglement source is consistent with laboratory results. These findings establish submarine fibre links as a viable platform for QKD and related quantum communication protocols.

The UK-IE field trial offers a characterisation of the Rockabill link, revealing polarisation stability on the timescales of hours and providing detailed characterisation of the noise induced by neighbouring classical data channels. Entangled photon pairs were successfully transmitted over a combined propagation distance of 448 km in separate deployed fibres and identified via time-correlated detection with a signal-to-noise ratio of 1.92. This constitutes a step towards an ultra-long fibre-based entanglement distribution, which so far has been performed over maximum distances of 248 km in deployed fibre [50] and 404 km in a laboratory environment [51].

Despite these encouraging results, several limitations were identified. Performance was constrained by background photon counts from nearby classical data traffic, reduced effective source brightness due to spectral filtering, and the absence of chromatic dispersion compensation. In addition, the observed polarisation stability could not be reproduced in the laboratory, preventing further verification of polarisation entanglement.

These findings identify a number of potential improvements for future experimental campaigns. Near-term efforts should focus on increasing the signal-to-noise ratio through reducing the insertion loss induced by the optical filters, and implementing chromatic dispersion compensation, enabling broader utilisation of the source's spectrum and narrower coincidence windows. The study also highlights the importance of real-time noise characterisation to optimise filtering under varying channel conditions.

Polarisation alignment remains a key technical challenge at high attenuation. A promising approach currently under development involves a custom Micro-ElectroMechanical Systems (MEMS)-based switching system that integrates single-mode and polarisation-maintaining fibre, allowing segmented alignment using auxiliary lasers and single photon detectors. Experimental validation of this scheme is an important next step towards long-distance QKD demonstrations.

Further performance gains may be achieved through modifications to the entanglement source itself. Addressing the dichroic mirror mismatch and exploring cavity-enhanced designs to narrow the emission spectrum could significantly increase the effective brightness and extend the achievable transmission distance, as discussed in Section 4.6.2. In parallel, the development of a submerged laboratory test-bed for emulating submarine QKD conditions of great interest and currently considered for future projects, with the aim of enabling controlled, long-duration studies of mechanically isolated fibre systems.

Beyond the immediate technical developments, this work highlights the broader potential of submarine fibre infrastructure for quantum communications. The results of the full study have already motivated follow-up proposals and international collaborations aimed at extending QKD demonstrations across national boundaries. In this context, submarine links such as Rockabill could form key components of an emerging transnational quantum network, connecting metropolitan nodes and enabling secure communication over continental scales. Simultaneously, early geographical identification of suitable locations for international quantum information links informs and accelerates the necessary development of the national quantum infrastructure.

Chapter 7

Conclusion & Future Work

This thesis has addressed the challenges of transitioning entanglement-based quantum key distribution from controlled laboratory environments to practical deployments while leveraging pre-existing optical infrastructure. It presents the development and implementation of a complete entanglement distribution system, including source validation, single-photon detector characterisation, receiver design, and data analysis. Through two real-world case studies, the work identifies opportunities to integrate QKD technology into classical optical communication networks, paving the way for practical, scalable quantum communication.

As one of the first projects within the Experimental Quantum Communications Group, this work established a foundational experimental platform by deploying and characterising single-photon detectors, an entangled photon source, and time-tagging hardware and software. Building on this foundation, specialised polarisation analysers were developed to enable full quantum state characterisation and to operate as passive receivers for polarisation-based QKD protocols. Their design was driven by their use in distinct research applications, with early-stage receivers being utilised in experimental studies and subsequently reworked in response to the practical restrictions encountered in each project. Ultimately, a full entanglement system tailored to field-implementations and practical research scenarios was implemented, culminating in the first discrete-variable quantum key generation at the University of York. The system has also proven transferable beyond entanglement distribution, with the receivers having already been utilised by the wider group for the characterisation of newly developed single photon transmitters.

Within this framework, the integration of quantum communication into existing optical network infrastructure was explored in two realistic scenarios. First, the coexistence of quantum signals with classical data traffic was investigated, highlighting both the potential and optimisation requirements of shared fibre infrastructure. Second, as part of a larger field trial on a 224 km undersea fibre link between the UK and Ireland, the distribution of photon pairs from an entangled source was demonstrated. Together, these results illustrate the deployment of the developed system across progressively more realistic environments, as well as establish a clear pathway towards full QKD demonstrations in deployed fibre networks.

Several limitations remain in the presented work. Technical constraints, such as the limited availability of single-photon detectors in combination with a continuous (non-pulsed) entanglement source, introduce additional losses and prevent fully realistic and secure QKD post-processing. The lack of phase control further necessitates a non-deterministic channel compensation method, which, while comparatively successful, remains experimentally demanding. Furthermore, imperfections in the source design restrict brightness and heralding efficiency, thereby limiting achievable transmission distance. The staged development of the polarisation analysers also meant that full entanglement measurement capability and an operational QKD pipeline were only realised at a late stage and thus were not available during earlier investigations. Consequently, the final polarisation analyser design has not yet undergone the same level of physical stress-testing as its predecessors. While the presented studies demonstrate the viability of both classical and quantum coexistence and entanglement distribution over submarine fibres, they remain initial implementations and could be extended substantially, as discussed in their respective chapters.

Future work will focus on deploying the polarisation entanglement system in full-scale quantum key distribution demonstrations across both the laboratory and field environments. Although a return to the Rockabill link was not secured at the time of writing, further experimental campaigns on other submarine fibre links are currently in the proposal stage, being developed in collaboration with international partners. Additionally, the integration of White Rabbit time-distribution into the QKD pipeline represents a key step towards realistic QKD deployment, enabling demonstrations with receivers in remote locations. In parallel, the extension of this work to underwater quantum communication environments remains an important direction for future research, including the development of a pool-based channel test-bed and entanglement-distribution systems tailored for submarine operation.

In summary, this thesis demonstrates the feasibility of integrating entanglement-based quantum key distribution with existing optical networks, showcasing the current potential of quantum technology. By developing an experimental polarisation-entanglement system, a versatile research tool for practical quantum key distribution is established, enabling further advances in practical quantum key distribution research. This work therefore not only contributes to the realisation of secure, large-scale quantum communications, but also lays the foundation for future discoveries and innovations, advancing the consolidation of scalable, global quantum networks.

Appendix A

Phase Difference in the $|\Phi_\varphi^+\rangle$ Bell-State

The maximally entangled $|\Phi^+\rangle$ Bell-State may be expressed including a relative phase φ between the superposition components:

$$|\Phi_\varphi^+\rangle = \frac{|00\rangle + e^{i\varphi} |11\rangle}{\sqrt{2}} \quad (\text{A.1})$$

In the $\mathbb{Z}$ basis, measurement of the eigenstates is independent of this phase difference. However, for the $\mathbb{X}$ and $\mathbb{Y}$ basis states, the relative phase φ affects the possible measurement outcomes. Below the exact dependencies in each basis are illustrated via application of the Born-rule.

$\mathbb{Z}$ -Basis:

It is straightforward to see that the probability of observing a specific polarisation state $P_{ij}(|\Phi_\varphi^+\rangle)$, $i, j \in \{H, V\}$ amounts to:

$$\begin{aligned} P_{HH}(|\Phi_\varphi^+\rangle) &= |\langle HH|\Phi_\varphi^+\rangle|^2 \\ &= \left| \frac{\langle HH|HH\rangle + e^{i\varphi} \langle HH|VV\rangle}{\sqrt{2}} \right|^2 \\ &= \left| \frac{1}{\sqrt{2}} \right|^2 \\ &= \frac{1}{2} \end{aligned}$$

$$\begin{aligned}
P_{|HV\rangle}(|\Phi_\varphi^+\rangle) &= |\langle HV|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle HV|HH\rangle + e^{i\varphi} \langle HV|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{0}{\sqrt{2}} \right|^2 \\
&= 0
\end{aligned}$$

$$\begin{aligned}
P_{|VH\rangle}(|\Phi_\varphi^+\rangle) &= |\langle VH|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle VH|HH\rangle + e^{i\varphi} \langle VH|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{0}{\sqrt{2}} \right|^2 \\
&= 0
\end{aligned}$$

$$\begin{aligned}
P_{|VV\rangle}(|\Phi_\varphi^+\rangle) &= |\langle VV|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle VV|HH\rangle + e^{i\varphi} \langle VV|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{e^{i\varphi}}{\sqrt{2}} \right|^2 \\
&= \frac{1}{2}
\end{aligned}$$

Or in summary:

$$P_{|HH\rangle}(|\Phi_\varphi^+\rangle) = P_{|VV\rangle}(|\Phi_\varphi^+\rangle) = \frac{1}{2} \quad (\text{A.2})$$

$$P_{|HV\rangle}(|\Phi_\varphi^+\rangle) = P_{|VH\rangle}(|\Phi_\varphi^+\rangle) = 0 \quad (\text{A.3})$$

Thus measurement outcomes in the $\mathbb{Z}$ basis are independent of φ .

$\mathbb{X}$ Basis:

Given the decomposition of $\mathbb{X}$ basis states in the $\mathbb{Z}$ basis:

$$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \quad (\text{A.4})$$

$$|-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}; \quad (\text{A.5})$$

it follows that:

$$|++\rangle = \left(\frac{|H\rangle + |V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle + |V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle + |HV\rangle + |VH\rangle + |VV\rangle}{2}, \quad (\text{A.6})$$

$$|+-\rangle = \left(\frac{|H\rangle + |V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle - |V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle - |HV\rangle + |VH\rangle - |VV\rangle}{2}, \quad (\text{A.7})$$

$$|-+\rangle = \left(\frac{|H\rangle - |V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle + |V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle + |HV\rangle + |VH\rangle + |VV\rangle}{2}, \quad (\text{A.8})$$

$$|--\rangle = \left(\frac{|H\rangle - |V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle - |V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle - |HV\rangle - |VH\rangle + |VV\rangle}{2}. \quad (\text{A.9})$$

Using Equations A.6-A.9 to perform $\mathbb{X}$ basis eigenstate measurements and immediately dropping orthogonal terms, the probabilities of observing a specific polarisation state $P_{ij}(|\Phi_\varphi^+\rangle)$, $i, j \in \{+, -\}$ can be found as:

$$\begin{aligned} P_{|++\rangle}(|\Phi_\varphi^+\rangle) &= |\langle ++ | \Phi_\varphi^+ \rangle|^2 \\ &= \left| \frac{\langle HH | + \langle VV |}{2} \otimes \frac{|HH\rangle + e^{i\varphi} |VV\rangle}{\sqrt{2}} \right|^2 \\ &= \left| \frac{1 + e^{i\varphi}}{4} \right|^2 \\ &= \frac{2 + 2 \cos \varphi}{8} \\ &= \frac{1 + \cos \varphi}{4} \end{aligned}$$

$$\begin{aligned} P_{|+-\rangle}(|\Phi_\varphi^+\rangle) &= |\langle +- | \Phi_\varphi^+ \rangle|^2 \\ &= \left| \frac{\langle HH | - \langle VV |}{2} \otimes \frac{|HH\rangle + e^{i\varphi} |VV\rangle}{\sqrt{2}} \right|^2 \\ &= \left| \frac{1 - e^{i\varphi}}{4} \right|^2 \\ &= \frac{2 - 2 \cos \varphi}{8} \\ &= \frac{1 - \cos \varphi}{4} \end{aligned}$$

$$\begin{aligned} P_{|-\rangle}(|\Phi_\varphi^+\rangle) &= |\langle -+ | \Phi_\varphi^+ \rangle|^2 \\ &= \left| \frac{\langle HH | - \langle VV |}{2} \otimes \frac{|HH\rangle + e^{i\varphi} |VV\rangle}{\sqrt{2}} \right|^2 \\ &= \left| \frac{1 - e^{i\varphi}}{4} \right|^2 \\ &= \frac{2 - 2 \cos \varphi}{8} \\ &= \frac{1 - \cos \varphi}{4} \end{aligned}$$

$$\begin{aligned}
P_{|--\rangle}(|\Phi_\varphi^+\rangle) &= |\langle -- | \Phi_\varphi^+ \rangle|^2 \\
&= \left| \frac{\langle HH | + \langle VV |}{2} \otimes \frac{|HH\rangle + e^{i\varphi} |VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{1 + e^{i\varphi}}{4} \right|^2 \\
&= \frac{2 + 2 \cos \varphi}{8} \\
&= \frac{1 + \cos \varphi}{4}.
\end{aligned}$$

Or in summary:

$$P_{|++\rangle}(|\Phi_\varphi^+\rangle) = P_{|--\rangle}(|\Phi_\varphi^+\rangle) = \frac{1 + \cos \varphi}{4} \quad (\text{A.10})$$

$$P_{|+-\rangle}(|\Phi_\varphi^+\rangle) = P_{|-+\rangle}(|\Phi_\varphi^+\rangle) = \frac{1 - \cos \varphi}{4} \quad (\text{A.11})$$

Thus measurement outcomes in the $\mathbb{X}$ basis are dependent on φ .

$\mathbb{Y}$ Basis:

Given the decomposition of $\mathbb{Y}$ basis states into the $\mathbb{Z}$ basis:

$$|R\rangle = \frac{|H\rangle + i|V\rangle}{\sqrt{2}}, \quad (\text{A.12})$$

$$|L\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}}; \quad (\text{A.13})$$

it follows that:

$$|RR\rangle = \left(\frac{|H\rangle + i|V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle + i|V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle + i|HV\rangle + i|VH\rangle - |VV\rangle}{2}, \quad (\text{A.14})$$

$$|RL\rangle = \left(\frac{|H\rangle + i|V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle - i|V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle - i|HV\rangle - i|VH\rangle + |VV\rangle}{2}, \quad (\text{A.15})$$

$$|LR\rangle = \left(\frac{|H\rangle - i|V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle + i|V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle - i|HV\rangle - i|VH\rangle + |VV\rangle}{2}, \quad (\text{A.16})$$

$$|LL\rangle = \left(\frac{|H\rangle - i|V\rangle}{\sqrt{2}} \right) \left(\frac{|H\rangle - i|V\rangle}{\sqrt{2}} \right) = \frac{|HH\rangle - i|HV\rangle - i|VH\rangle - |VV\rangle}{2}. \quad (\text{A.17})$$

Using Equations A.14-A.17 to perform $\mathbb{Y}$ basis eigenstate measurements and immediately dropping orthogonal terms, the probabilities of observing a specific polarisation state

$P_{|ij\rangle}(|\Phi_\varphi^+\rangle)$, $i, j \in \{R, L\}$ can be found as:

$$\begin{aligned}
P_{|RR\rangle}(|\Phi_\varphi^+\rangle) &= |\langle RR|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle HH| - \langle VV|}{2} \otimes \frac{|HH\rangle + e^{i\varphi}|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{1 - e^{i\varphi}}{4} \right|^2 \\
&= \frac{1 - \cos \varphi}{4}
\end{aligned}$$

$$\begin{aligned}
P_{|RL\rangle}(|\Phi_\varphi^+\rangle) &= |\langle RL|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle HH| + \langle VV|}{2} \otimes \frac{|HH\rangle + e^{i\varphi}|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{1 + e^{i\varphi}}{4} \right|^2 \\
&= \frac{1 + \cos \varphi}{4}
\end{aligned}$$

$$\begin{aligned}
P_{|LR\rangle}(|\Phi_\varphi^+\rangle) &= |\langle LR|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle HH| + \langle VV|}{2} \otimes \frac{|HH\rangle + e^{i\varphi}|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{1 + e^{i\varphi}}{4} \right|^2 \\
&= \frac{1 + \cos \varphi}{4}
\end{aligned}$$

$$\begin{aligned}
P_{|LL\rangle}(|\Phi_\varphi^+\rangle) &= |\langle LL|\Phi_\varphi^+\rangle|^2 \\
&= \left| \frac{\langle HH| - \langle VV|}{2} \otimes \frac{|HH\rangle + e^{i\varphi}|VV\rangle}{\sqrt{2}} \right|^2 \\
&= \left| \frac{1 - e^{i\varphi}}{4} \right|^2 \\
&= \frac{1 - \cos \varphi}{4}.
\end{aligned}$$

Or in summary:

$$P_{|RR\rangle}(|\Phi_\varphi^+\rangle) = P_{|LL\rangle}(|\Phi_\varphi^+\rangle) = \frac{1 - \cos \varphi}{4} \quad (\text{A.18})$$

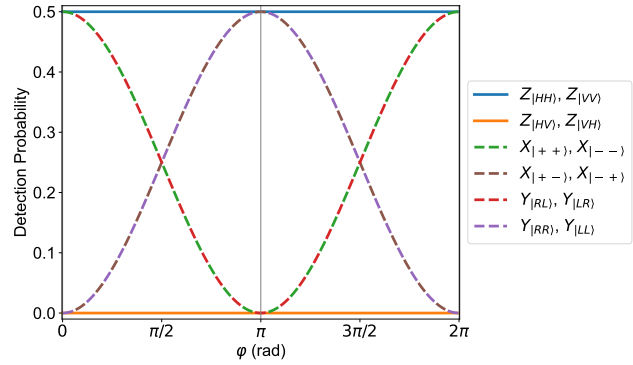
$$P_{|RL\rangle}(|\Phi_\varphi^+\rangle) = P_{|LR\rangle}(|\Phi_\varphi^+\rangle) = \frac{1 + \cos \varphi}{4} \quad (\text{A.19})$$

Thus measurement outcomes in the $\mathbb{Y}$ basis are dependent on φ .

Conclusion

Table A.1a summarises the probabilities of detecting each bit pair depending on φ . As illustrated by Figure A.1b, simultaneous maximum correlations only appear in all three Pauli bases if $\varphi = n\pi$ where n is an integer.

Basis	$P(\varphi)_{\parallel}$	$P(\varphi)_{\perp}$
$\mathbb{Z}$	$\frac{1}{2}$	0
$\mathbb{X}$	$\frac{1+\cos \varphi}{4}$	$\frac{1-\cos \varphi}{4}$
$\mathbb{Y}$	$\frac{1-\cos \varphi}{4}$	$\frac{1+\cos \varphi}{4}$



a) Analytical expressions for the $|\Phi_{\varphi}^{+}\rangle$ state's coincidence detection probabilities in all three Pauli bases.

b) Graphical representation of the Bell state's dependence on φ

Figure A.1: Bell state phase dependence in analytical expressions and graphical form.

Consequently, correlated polarisation states can only be seen in all three bases (or even in two) at specific values of the relative phase φ .

In a polarisation-based encoding implementation, the relative phase difference corresponds to a physical relative phase of the polarisation's horizontal and vertical components that could easily arise within a real setup. As the photons traverse the transmission channel, they generally acquire an uncontrolled unitary transformation due to the birefringence of optical fibre. Usually, this is compensated for by realigning a known linear state to the $\mathbb{Y}$ basis. However, since a phase shift itself can easily be unitary, this alignment may not result in a $n\pi$ phase shift and correlations may not be maximised in another orthogonal basis. Initial alignment and polarisation drift compensation thus have to take coincidences in at least two Pauli bases simultaneously.

Appendix B

Derivation of CHSH-Inequalities for Specific Waveplate Transformations

Any unitary transformation, such as from a waveplate, applied to a photonic bit represented by a Jones vector will take the form of a 4×4 matrix. Let us adopt the following generalised shorthand for a matrix U representing an arbitrary unitary transformation:

$$U = \begin{pmatrix} \textcircled{1A} & \textcircled{1B} \\ \textcircled{2A} & \textcircled{2B} \end{pmatrix}$$

Applying this matrix to the polarisation Z-basis states results in:

$$\begin{aligned} U|0\rangle &= \begin{pmatrix} \textcircled{1A} & \textcircled{1B} \\ \textcircled{2A} & \textcircled{2B} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \textcircled{1A} \\ \textcircled{1B} \end{pmatrix} = \textcircled{1A}|0\rangle + \textcircled{1B}|1\rangle \\ U|1\rangle &= \begin{pmatrix} \textcircled{1A} & \textcircled{1B} \\ \textcircled{2A} & \textcircled{2B} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \textcircled{2A} \\ \textcircled{2B} \end{pmatrix} = \textcircled{2A}|0\rangle + \textcircled{2B}|1\rangle \end{aligned}$$

Next, we consider the $|\Phi^+\rangle$ entangled Bell-state travelling along paths a and b :

$$|\Phi_{ab}^+\rangle = \frac{|0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b}{\sqrt{2}}$$

To this state, we can apply two independent unitary transformations to represent the changes that photons a and b undergo on their respective path, both represented by a generalised matrix $U_{a/b}$ as:

$$U_a = \begin{pmatrix} \textcircled{1A} & \textcircled{1B} \\ \textcircled{2A} & \textcircled{2B} \end{pmatrix} \qquad U_b = \begin{pmatrix} \textcircled{3A} & \textcircled{3B} \\ \textcircled{4A} & \textcircled{4B} \end{pmatrix}$$

Hence we can derive:

$$\begin{aligned}
U_a U_b |\Phi_{ab}^+\rangle &= \frac{1}{\sqrt{2}} [U_a |0\rangle_a U_b |0\rangle_b + U_a |1\rangle_a U_b |1\rangle_b] \\
&= \frac{1}{\sqrt{2}} \left[\left(\textcircled{1A} |0\rangle_a + \textcircled{1B} |1\rangle_a \right) \left(\textcircled{3A} |0\rangle_b + \textcircled{3B} |1\rangle_b \right) \right. \\
&\quad \left. + \left(\textcircled{2A} |0\rangle_a + \textcircled{2B} |1\rangle_a \right) \left(\textcircled{4A} |0\rangle_b + \textcircled{4B} |1\rangle_b \right) \right] \\
&= \frac{1}{\sqrt{2}} \left[\textcircled{1A} \textcircled{3A} |0\rangle_a |0\rangle_b + \textcircled{1A} \textcircled{3B} |0\rangle_a |1\rangle_b \right. \\
&\quad + \textcircled{1B} \textcircled{3A} |1\rangle_a |0\rangle_b + \textcircled{1B} \textcircled{3B} |1\rangle_a |1\rangle_b \\
&\quad + \textcircled{2A} \textcircled{4A} |0\rangle_a |0\rangle_b + \textcircled{2A} \textcircled{4B} |0\rangle_a |1\rangle_b \\
&\quad + \textcircled{2B} \textcircled{4A} |1\rangle_a |0\rangle_b + \textcircled{2B} \textcircled{4B} |1\rangle_a |1\rangle_b \left. \right] \\
&= \frac{1}{\sqrt{2}} \left[\left(\textcircled{1A} \textcircled{3A} + \textcircled{2A} \textcircled{4A} \right) |0\rangle_a |0\rangle_b \right. \\
&\quad + \left(\textcircled{1A} \textcircled{3B} + \textcircled{2A} \textcircled{4B} \right) |0\rangle_a |1\rangle_b \\
&\quad + \left(\textcircled{1B} \textcircled{3A} + \textcircled{2B} \textcircled{4A} \right) |1\rangle_a |0\rangle_b \\
&\quad \left. + \left(\textcircled{1B} \textcircled{3B} + \textcircled{2B} \textcircled{4B} \right) |1\rangle_a |1\rangle_b \right] \tag{B.1}
\end{aligned}$$

We can now use expression B.1 to obtain the final two-photon state after two independent transformations by substituting the circled terms as appropriate.

CHSH-Inequalities using two HWP, two QWP and one HWP and one QWP

The general expressions for the unitary transformations applied by a HWP (H) and QWP (Q) are:

$$U_H = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \quad U_Q = \begin{pmatrix} \cos^2 \theta + i \sin^2 \theta & (1-i) \sin \theta \cos \theta \\ (1-i) \sin \theta \cos \theta & \sin^2 \theta + i \cos^2 \theta \end{pmatrix}$$

We assume that the two photons reach the receivers in perfectly aligned polarisations states (i.e. any channel birefringence has been compensated for), so that photons a and b enter free space as eigenstates of the Pauli Z-basis. They then experience a transformation based on passing a single waveplate at some angle θ_a, θ_b , before being measured.

CHSH Inequality for two HWPs

This is the well-known configuration that is used in most practical cases. Maximum Bell-violation of $S = 2\sqrt{2}$ can be achieved for several sets of angles. To re-derive this, we apply a HWP transformation to each photon by substituting U_H into B.1:

$$\begin{aligned}
 U_H^{(a)} U_H^{(b)} |\Phi_{ab}^+\rangle &= \frac{1}{\sqrt{2}} [(\cos 2\theta_a \cos 2\theta_b + \sin 2\theta_a \sin 2\theta_b) |0\rangle_a |0\rangle_b \\
 &\quad + (\cos 2\theta_a \sin 2\theta_b - \sin 2\theta_a \cos 2\theta_b) |0\rangle_a |1\rangle_b \\
 &\quad + (\sin 2\theta_a \cos 2\theta_b - \cos 2\theta_a \sin 2\theta_b) |1\rangle_a |0\rangle_b \\
 &\quad + (\sin 2\theta_a \sin 2\theta_b + \cos 2\theta_a \cos 2\theta_b) |1\rangle_a |1\rangle_b] \\
 &= \frac{1}{\sqrt{2}} [\cos 2(\theta_a - \theta_b) |0\rangle_a |0\rangle_b \\
 &\quad - \sin 2(\theta_a - \theta_b) |0\rangle_a |1\rangle_b \\
 &\quad + \sin 2(\theta_a - \theta_b) |1\rangle_a |0\rangle_b \\
 &\quad + \cos 2(\theta_a - \theta_b) |1\rangle_a |1\rangle_b] \tag{B.2}
 \end{aligned}$$

From Equation B.2, we can obtain the probabilities of detecting each polarisation state as functions of the waveplate angles using the Born rule [102]:

$$P_{|00\rangle}(\theta_a, \theta_b) = \frac{1}{2} \cos^2 [2(\theta_a - \theta_b)] \tag{B.3}$$

$$P_{|01\rangle}(\theta_a, \theta_b) = \frac{1}{2} \sin^2 [2(\theta_a - \theta_b)] \tag{B.4}$$

$$P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{2} \sin^2 [2(\theta_a - \theta_b)] \tag{B.5}$$

$$P_{|11\rangle}(\theta_a, \theta_b) = \frac{1}{2} \cos^2 [2(\theta_a - \theta_b)] \tag{B.6}$$

where we note that $P_{|00\rangle} = P_{|11\rangle}$ and $P_{|01\rangle} = P_{|10\rangle}$. Given these probabilities, we can evaluate the CHSH-inequality 4.13, 4.14 in terms of arbitrary waveplate angles:

$$\begin{aligned}
 E(\theta_a, \theta_b) &= P_{|00\rangle}(\theta_a, \theta_b) + P_{|11\rangle}(\theta_a, \theta_b) - P_{|01\rangle}(\theta_a, \theta_b) - P_{|10\rangle}(\theta_a, \theta_b) \\
 &= \frac{1}{2} \cos^2 [2(\theta_a - \theta_b)] + \frac{1}{2} \cos^2 [2(\theta_a - \theta_b)] \\
 &\quad - \frac{1}{2} \sin^2 [2(\theta_a - \theta_b)] - \frac{1}{2} \sin^2 [2(\theta_a - \theta_b)] \\
 &= \cos^2 [2(\theta_a - \theta_b)] - \sin^2 [2(\theta_a - \theta_b)] \\
 &= \cos [4(\theta_a - \theta_b)] \tag{B.7}
 \end{aligned}$$

$$\begin{aligned}
 S &= E(\theta_a, \theta_b) - E(\theta_a, \theta'_b) + E(\theta'_a, \theta_b) + E(\theta'_a, \theta'_b) \\
 &= \cos [4(\theta_a - \theta_b)] - \cos [4(\theta_a - \theta'_b)] + \cos [4(\theta'_a - \theta_b)] + \cos [4(\theta'_a - \theta'_b)] \tag{B.8}
 \end{aligned}$$

We employ symbolic optimisation in *Mathematica* to find a set of angles $\{\theta_a, \theta'_a, \theta_b, \theta'_b\}$ for which $|S|$ is maximised. For two HWPs, this results in the following angles:

$$\begin{aligned}\theta_a &= 0 & &= 0^\circ \\ \theta_b &= \frac{\pi}{16} & &= 11.25^\circ \\ \theta'_a &= \frac{\pi}{8} & &= 22.5^\circ \\ \theta'_b &= \frac{3\pi}{16} & &= 33.75^\circ\end{aligned}$$

which produce the well-known set of linear states quoted at the beginning of the section. We can easily show that the above angles lead to a maximum Bell-violation by substituting them into our specific CHSH-inequality B:

$$\begin{aligned}S &= \cos(-4 \times 11.25^\circ) - \cos(-4 \times 33.75^\circ) + \cos(4 \times 11.25^\circ) + \cos(-4 \times 11.25^\circ) \\ &= \cos(45^\circ) - \cos(135^\circ) + \cos(45^\circ) + \cos(45^\circ) \\ &= \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \\ &= 2\sqrt{2} > 2\end{aligned}$$

CHSH-Inequality for two QWPs

Starting from Equation B.1 and the expression for a QWP transformation, we can derive:

$$U_Q^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle = \frac{1}{\sqrt{2}} \left\{ \begin{aligned} & \left[\begin{aligned} & (\cos^2 \theta_a + i \sin^2 \theta_a)(\cos^2 \theta_b + i \sin^2 \theta_b) \\ & + (1-i) \sin \theta_a \cos \theta_a (1-i) \sin \theta_b \cos \theta_b \end{aligned} \right] |0\rangle_a |0\rangle_b \\ & + \left[\begin{aligned} & (\cos^2 \theta_a + i \sin^2 \theta_a)(1-i) \sin \theta_b \cos \theta_b \\ & + (1-i) \sin \theta_a \cos \theta_a (\sin^2 \theta_b + i \cos^2 \theta_b) \end{aligned} \right] |0\rangle_a |1\rangle_b \\ & + \left[\begin{aligned} & (1-i) \sin \theta_a \cos \theta_a (\cos^2 \theta_b + i \sin^2 \theta_b) \\ & + (\sin^2 \theta_a + i \cos^2 \theta_a)(1-i) \sin \theta_b \cos \theta_b \end{aligned} \right] |1\rangle_a |0\rangle_b \\ & + \left[\begin{aligned} & (1-i) \sin \theta_a \cos \theta_a (1-i) \sin \theta_b \cos \theta_b \\ & + (\sin^2 \theta_a + i \cos^2 \theta_a)(\sin^2 \theta_b + i \cos^2 \theta_b) \end{aligned} \right] |1\rangle_a |1\rangle_b \end{aligned} \right\}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2}} \left\{ \begin{aligned} &\begin{bmatrix} \cos^2 \theta_a \cos^2 \theta_b - \sin^2 \theta_a \sin^2 \theta_b \\ + i(\cos^2 \theta_a \sin^2 \theta_b + \sin^2 \theta_a \cos^2 \theta_b) \\ - 2 \cos \theta_a \sin \theta_b \sin \theta_a \cos \theta_b \end{bmatrix} |0\rangle_a |0\rangle_b \\ &+ \begin{bmatrix} (1-i)[\cos \theta_a \sin \theta_b (\cos \theta_a \cos \theta_b + \sin \theta_a \sin \theta_b)] \\ + i \sin \theta_a \cos \theta_b (\sin \theta_a \sin \theta_b + \cos \theta_a \cos \theta_b) \end{bmatrix} |0\rangle_a |1\rangle_b \\ &+ \begin{bmatrix} (1-i)[\sin \theta_a \cos \theta_b (\cos \theta_a \cos \theta_b + \sin \theta_a \sin \theta_b)] \\ + i \cos \theta_a \sin \theta_b (\sin \theta_a \sin \theta_b + \cos \theta_a \cos \theta_b) \end{bmatrix} |1\rangle_a |0\rangle_b \\ &+ \begin{bmatrix} \sin^2 \theta_a \sin^2 \theta_b - \cos^2 \theta_a \cos^2 \theta_b \\ + i(\sin^2 \theta_a \cos^2 \theta_b + i \cos^2 \theta_a \sin^2 \theta_b) \\ - 2 \sin \theta_a \cos \theta_a \sin \theta_b \cos \theta_b \end{bmatrix} |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
&= \frac{1}{\sqrt{2}} \left\{ \begin{aligned} &\begin{bmatrix} \cos^2 \theta_a \cos^2 \theta_b - \sin^2 \theta_a \sin^2 \theta_b \\ + i(\cos \theta_a \sin \theta_b - \sin \theta_a \cos \theta_b)^2 \end{bmatrix} |0\rangle_a |0\rangle_b \\ &+ \begin{bmatrix} (1-i) \cos(\theta_a - \theta_b) \\ (\cos \theta_a \sin \theta_b + i \sin \theta_a \cos \theta_b) \end{bmatrix} |0\rangle_a |1\rangle_b \\ &+ \begin{bmatrix} (1-i) \cos(\theta_a - \theta_b) \\ (\sin \theta_a \cos \theta_b + i \cos \theta_a \sin \theta_b) \end{bmatrix} |1\rangle_a |0\rangle_b \\ &+ \begin{bmatrix} \sin^2 \theta_a \sin^2 \theta_b - \cos^2 \theta_a \cos^2 \theta_b \\ + i(\sin \theta_a \cos \theta_b - \cos \theta_a \sin \theta_b)^2 \end{bmatrix} |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
&= \frac{1}{\sqrt{2}} \left\{ \begin{aligned} &[\cos(\theta_a + \theta_b) \cos(\theta_a - \theta_b) + i \sin^2(\theta_b - \theta_a)] |0\rangle_a |0\rangle_b \\ &+ [\cos(\theta_a - \theta_b)(\sin(\theta_a + \theta_b) + i \sin(\theta_a - \theta_b))] |0\rangle_a |1\rangle_b \\ &+ [\cos(\theta_a - \theta_b)(\sin(\theta_a + \theta_b) - i \sin(\theta_a - \theta_b))] |1\rangle_a |0\rangle_b \\ &+ [-\cos(\theta_a + \theta_b) \cos(\theta_a - \theta_b) + i \sin^2(\theta_a - \theta_b)] |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
&= \frac{1}{2\sqrt{2}} \left\{ \begin{aligned} &[\cos 2\theta_a + \cos 2\theta_b + i(1 - \cos 2(\theta_a - \theta_b))] |0\rangle_a |0\rangle_b \\ &+ [\sin 2\theta_a + \sin 2\theta_b + i \sin 2(\theta_a - \theta_b)] |0\rangle_a |1\rangle_b \\ &+ [\sin 2\theta_a + \sin 2\theta_b - i \sin 2(\theta_a - \theta_b)] |1\rangle_a |0\rangle_b \\ &- [\cos 2\theta_a + \cos 2\theta_b - i(1 - \cos 2(\theta_a - \theta_b))] |1\rangle_a |1\rangle_b \end{aligned} \right\} \quad (\text{B.9})
\end{aligned}$$

From Equation B.9, we can again obtain the probabilities of detecting each polarisation state as functions of the waveplate angles:

$$\begin{aligned} P_{|00\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ [\cos 2\theta_a + \cos 2\theta_b]^2 + [1 - \cos 2(\theta_a - \theta_b)]^2 \} \\ &= \frac{1}{8} [(\cos 2\theta_a + \cos 2\theta_b)^2 + 4 \sin^4(\theta_a - \theta_b)] \end{aligned} \quad (\text{B.10})$$

$$P_{|01\rangle}(\theta_a, \theta_b) = \frac{1}{8} [(\sin 2\theta_a + \sin 2\theta_b)^2 + \sin^2 2(\theta_a - \theta_b)] \quad (\text{B.11})$$

$$P_{|10\rangle}(\theta_a, \theta_b) = \frac{1}{8} [(\sin 2\theta_a + \sin 2\theta_b)^2 + \sin^2 2(\theta_a - \theta_b)] \quad (\text{B.12})$$

$$\begin{aligned} P_{|11\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ [-(\cos 2\theta_a + \cos 2\theta_b)]^2 + [1 - \cos 2(\theta_a - \theta_b)]^2 \} \\ &= \frac{1}{8} [(\cos 2\theta_a + \cos 2\theta_b)^2 + 4 \sin^4(\theta_a - \theta_b)] \end{aligned} \quad (\text{B.13})$$

with recurring $P_{|00\rangle} = P_{|11\rangle}$ and $P_{|01\rangle} = P_{|10\rangle}$. Inserting these probabilities into the CHSH-inequality 4.13, 4.14, we can assemble an expression for the CHSH parameter S as a function of two QWP-angles:

$$\begin{aligned} E(\theta_a, \theta_b) &= P_{|00\rangle}(\theta_a, \theta_b) + P_{|11\rangle}(\theta_a, \theta_b) - P_{|01\rangle}(\theta_a, \theta_b) - P_{|10\rangle}(\theta_a, \theta_b) \\ &= \frac{1}{8} \left\{ 2[(\cos 2\theta_a + \cos 2\theta_b)^2 + 4 \sin^4(\theta_a - \theta_b)] \right. \\ &\quad \left. - 2[(\sin 2\theta_a + \sin 2\theta_b)^2 + \sin^2 2(\theta_a - \theta_b)] \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &\cos^2 2\theta_a + \cos^2 2\theta_b + 2 \cos 2\theta_a \cos 2\theta_b \\ &- \sin^2 2\theta_a - \sin^2 2\theta_b - 2 \sin 2\theta_a \sin 2\theta_b \\ &+ 4 \sin^4(\theta_a - \theta_b) - \sin^2 2(\theta_a - \theta_b) \end{aligned} \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &[\cos^2 2\theta_a - \sin^2 2\theta_a] + [\cos^2 2\theta_b - \sin^2 2\theta_b] \\ &+ 2[\cos 2\theta_a \cos 2\theta_b - \sin 2\theta_a \sin 2\theta_b] \\ &+ 4 \sin^4(\theta_a - \theta_b) - 4 \sin^2(\theta_a - \theta_b) \cos^2(\theta_a - \theta_b) \end{aligned} \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &\cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) \\ &+ 4 \sin^2(\theta_a - \theta_b) [\sin^2(\theta_a - \theta_b) - \cos^2(\theta_a - \theta_b)] \end{aligned} \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &\cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) \\ &- 4 \sin^2(\theta_a - \theta_b) \cos 2(\theta_a - \theta_b) \end{aligned} \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &\cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) \\ &- 2 \cos 2(\theta_a - \theta_b) - 2 \cos^2 2(\theta_a - \theta_b) \end{aligned} \right\} \\ &= \frac{1}{4} \left\{ \begin{aligned} &1 + \cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) \\ &- 2 \cos 2(\theta_a - \theta_b) + \cos 4(\theta_a - \theta_b) \end{aligned} \right\} \end{aligned} \quad (\text{B.14})$$

$$\begin{aligned}
S &= E(\theta_a, \theta_b) - E(\theta_a, \theta'_b) + E(\theta'_a, \theta_b) + E(\theta'_a, \theta'_b) \\
&= \frac{1}{4} [1 + \cos 4\theta_a + \cos 4\theta_b + 2 \cos 2(\theta_a + \theta_b) - 2 \cos 2(\theta_a - \theta_b) + \cos 4(\theta_a - \theta_b) \\
&\quad - 1 - \cos 4\theta_a - \cos 4\theta'_b - 2 \cos 2(\theta_a + \theta'_b) + 2 \cos 2(\theta_a - \theta'_b) - \cos 4(\theta_a - \theta'_b) \\
&\quad + 1 + \cos 4\theta'_a + \cos 4\theta_b + 2 \cos 2(\theta'_a + \theta_b) - 2 \cos 2(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta_b) \\
&\quad + 1 + \cos 4\theta'_a + \cos 4\theta'_b + 2 \cos 2(\theta'_a + \theta'_b) - 2 \cos 2(\theta'_a - \theta'_b) + \cos 4(\theta'_a - \theta'_b)] \\
&= \frac{1}{4} [2 + 2 \cos 4\theta'_a + 2 \cos 4\theta_b \\
&\quad + 2 \cos 2(\theta_a + \theta_b) - 2 \cos 2(\theta_a - \theta_b) + \cos 4(\theta_a - \theta_b) \\
&\quad - 2 \cos 2(\theta_a + \theta'_b) + 2 \cos 2(\theta_a - \theta'_b) - \cos 4(\theta_a - \theta'_b) \\
&\quad + 2 \cos 2(\theta'_a + \theta_b) - 2 \cos 2(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta_b) \\
&\quad + 2 \cos 2(\theta'_a + \theta'_b) - 2 \cos 2(\theta'_a - \theta'_b) + \cos 4(\theta'_a - \theta'_b)] \\
&= \frac{1}{2} + \frac{1}{2} \cos 4\theta'_a + \frac{1}{2} \cos 4\theta_b \tag{B.15} \\
&\quad + \frac{1}{2} \sum_{i,j} \varsigma_{ij} \cos 2(\theta_{a,i} + \theta_{b,j}) \\
&\quad - \frac{1}{2} \sum_{i,j} \varsigma_{ij} \cos 2(\theta_{a,i} - \theta_{b,j}) \\
&\quad + \frac{1}{4} \sum_{i,j} \varsigma_{ij} \cos 4(\theta_{a,i} - \theta_{b,j})
\end{aligned}$$

Where the indices $i, j \in \{0, 1\}$ map the angles as $\theta_{x,0} = \theta_x$ and $\theta_{x,1} = \theta'_x$ and ς_{ij} is defined as

$$\varsigma = \begin{pmatrix} +1 & -1 \\ +1 & +1 \end{pmatrix}.$$

Unlike with two HWP, this expression can never reach a Bell-Violation of $S = 2\sqrt{2}$. The highest achievable value is $S = 2.5$ and occurs for the following angles:

$$\begin{aligned}
\theta_a &= \frac{\pi}{8} &= 22.5^\circ \\
\theta_b &= 0 &= 0^\circ \\
\theta'_a &= 0 &= 0^\circ \\
\theta'_b &= \frac{3\pi}{8} &= 67.5^\circ
\end{aligned}$$

We now know that this configuration can only result in a lower entanglement witness, so it is not useful for QKD. Regardless, we can use this to verify the functioning of the PA.

CHSH Inequality for a HWP+QWP

Starting from Equation B.1 and the expression for a HWP and QWP transformation, we can derive the entangled polarisation state of both photons. Below, the HWP is assigned to θ_a , $|\Phi_a^+\rangle$ and the QWP is assigned to θ_b , $|\Phi_b^+\rangle$. However, due to the symmetry of the $|\Phi^+\rangle$ state, photons a and b are interchangeable in the final expression.

$$\begin{aligned}
 U_H^{(a)} U_Q^{(b)} |\Phi_{ab}^+\rangle &= \frac{1}{\sqrt{2}} \left\{ \begin{aligned} &\left[\cos 2\theta_a (\cos^2 \theta_b + i \sin^2 \theta_b) \right] |0\rangle_a |0\rangle_b \\ &+ \left[\cos 2\theta_a (1 - i) \sin \theta_b \cos \theta_b \right] |0\rangle_a |1\rangle_b \\ &+ \left[\sin 2\theta_a (\cos^2 \theta_b + i \sin^2 \theta_b) \right] |1\rangle_a |0\rangle_b \\ &+ \left[\sin 2\theta_a (1 - i) \sin \theta_b \cos \theta_b \right] |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
 &= \frac{1}{\sqrt{2}} \left\{ \begin{aligned} &\left[\frac{1}{2} \sin 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \cos 2\theta_a \left[\frac{1}{2} (1 + \cos 2\theta_b) + \frac{i}{2} (1 - \cos 2\theta_b) \right] \right] |0\rangle_a |0\rangle_b \\ &+ \left[\frac{1}{2} \cos 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \sin 2\theta_a \left[\frac{1}{2} (1 - \cos 2\theta_b) + \frac{i}{2} (1 + \cos 2\theta_b) \right] \right] |0\rangle_a |1\rangle_b \\ &+ \left[-\frac{1}{2} \cos 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \sin 2\theta_a \left[\frac{1}{2} (1 + \cos 2\theta_b) + \frac{i}{2} (1 - \cos 2\theta_b) \right] \right] |1\rangle_a |0\rangle_b \\ &+ \left[\frac{1}{2} \sin 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. - \cos 2\theta_a \left[\frac{1}{2} (1 - \cos 2\theta_b) + \frac{i}{2} (1 + \cos 2\theta_b) \right] \right] |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
 &= \frac{1}{2\sqrt{2}} \left\{ \begin{aligned} &\left[\sin 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \cos 2\theta_a [(1 + i) + (1 - i) \cos 2\theta_b] \right] |0\rangle_a |0\rangle_b \\ &+ \left[\cos 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \sin 2\theta_a [(1 + i) - (1 - i) \cos 2\theta_b] \right] |0\rangle_a |1\rangle_b \\ &+ \left[-\cos 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. + \sin 2\theta_a [(1 + i) - (1 - i) \cos 2\theta_b] \right] |1\rangle_a |0\rangle_b \\ &+ \left[\sin 2\theta_a (1 - i) \sin 2\theta_b \right. \\ &\quad \left. - \cos 2\theta_a [(1 + i) - (1 - i) \cos 2\theta_b] \right] |1\rangle_a |1\rangle_b \end{aligned} \right\}
 \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2\sqrt{2}} \left\{ \begin{aligned} &\left[\begin{array}{l} (1-i) [\cos 2\theta_a \cos 2\theta_b + \sin 2\theta_a \sin 2\theta_b] \\ + (1+i) \cos 2\theta_a \end{array} \right] |0\rangle_a |0\rangle_b \\ &+ \left[\begin{array}{l} (1-i) [\cos 2\theta_a \sin 2\theta_b - \sin 2\theta_a \cos 2\theta_b] \\ + (1+i) \sin 2\theta_a \end{array} \right] |0\rangle_a |1\rangle_b \\ &+ \left[\begin{array}{l} (1-i) [\sin 2\theta_a \cos 2\theta_b - \cos 2\theta_a \sin 2\theta_b] \\ + (1+i) \sin 2\theta_a \end{array} \right] |1\rangle_a |0\rangle_b \\ &+ \left[\begin{array}{l} (1-i) [\cos 2\theta_a \cos 2\theta_b + \sin 2\theta_a \sin 2\theta_b] \\ - (1+i) \cos 2\theta_a \end{array} \right] |1\rangle_a |1\rangle_b \end{aligned} \right\} \\
&= \frac{1}{2\sqrt{2}} \left\{ \begin{aligned} &[(1+i)(\cos 2\theta_a - i \cos 2(\theta_a - \theta_b))] |0\rangle_a |0\rangle_b \\ &+ [(1+i)(\sin 2\theta_a - i \sin 2(\theta_a - \theta_b))] |0\rangle_a |1\rangle_b \\ &+ [(1+i)(\sin 2\theta_a - i \sin 2(\theta_a - \theta_b))] |1\rangle_a |0\rangle_b \\ &+ [(1+i)(-\cos 2\theta_a - i \cos 2(\theta_a - \theta_b))] |1\rangle_a |1\rangle_b \end{aligned} \right\} \quad (\text{B.16})
\end{aligned}$$

Using Equation B.16, the probabilities for each polarisation state combination can be found to be:

$$\begin{aligned}
P_{|00\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ (1+i)(1-i) [\cos 2\theta_a - i \cos 2(\theta_a - \theta_b)] [\cos 2\theta_a + i \cos 2(\theta_a - \theta_b)] \} \\
&= \frac{1}{4} [(\cos^2 2\theta_a + \cos^2 2(\theta_a - \theta_b))] \quad (\text{B.17})
\end{aligned}$$

$$\begin{aligned}
P_{|01\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ (1+i)(1-i) [\sin 2\theta_a - i \sin 2(\theta_a - \theta_b)] [\sin 2\theta_a + i \sin 2(\theta_a - \theta_b)] \} \\
&= \frac{1}{4} [(\sin^2 2\theta_a + \sin^2 2(\theta_a - \theta_b))] \quad (\text{B.18})
\end{aligned}$$

$$\begin{aligned}
P_{|10\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ (1+i)(1-i) [\sin 2\theta_a - i \sin 2(\theta_a - \theta_b)] [\sin 2\theta_a + i \sin 2(\theta_a - \theta_b)] \} \\
&= \frac{1}{4} [(\sin^2 2\theta_a + \sin^2 2(\theta_a - \theta_b))] \quad (\text{B.19})
\end{aligned}$$

$$\begin{aligned}
P_{|11\rangle}(\theta_a, \theta_b) &= \frac{1}{8} \{ (1+i)(1-i) 2[-\cos 2\theta_a - i \cos 2(\theta_a - \theta_b)] [-\cos 2\theta_a + i \cos 2(\theta_a - \theta_b)] \} \\
&= \frac{1}{4} [(\cos^2 2\theta_a + \cos^2 2(\theta_a - \theta_b))] \quad (\text{B.20})
\end{aligned}$$

Once more, $P_{|00\rangle} = P_{|11\rangle}$ and $P_{|01\rangle} = P_{|10\rangle}$. A simple check confirms that $P_{00} + P_{01} + P_{10} + P_{11} = 1$. We obtain our final CHSH-inequality by inserting the probabilities into 4.13, 4.14, which gives us the CHSH parameter S as a function of one the angles of one HWP (θ_a) and one QWP (θ_b):

$$\begin{aligned}
E(\theta_a, \theta_b) &= P_{|00\rangle}(\theta_a, \theta_b) + P_{|11\rangle}(\theta_a, \theta_b) - P_{|01\rangle}(\theta_a, \theta_b) - P_{|10\rangle}(\theta_a, \theta_b) \\
&= \frac{1}{4} \{ 2 [\cos^2 2\theta_a + \cos^2 2(\theta_a - \theta_b)] - 2 [\sin^2 2\theta_a + \sin^2 2(\theta_a - \theta_b)] \} \\
&= \frac{1}{2} [\cos 4\theta_a + \cos 4(\theta_a - \theta_b)] \quad (\text{B.21})
\end{aligned}$$

$$\begin{aligned}
S &= E(\theta_a, \theta_b) - E(\theta_a, \theta'_b) + E(\theta'_a, \theta_b) + E(\theta'_a, \theta'_b) \\
&= \frac{1}{2} [\cos 4\theta_a + \cos 4(\theta_a - \theta_b) \\
&\quad - \cos 4\theta_a - \cos 4(\theta_a - \theta'_b) \\
&\quad + \cos 4\theta'_a + \cos 4(\theta'_a - \theta_b) \\
&\quad + \cos 4\theta'_a + \cos 4(\theta'_a - \theta'_b)] \\
&= \cos 4\theta'_a + \frac{1}{2} [\cos 4(\theta_a - \theta_b) - \cos 4(\theta_a - \theta'_b) + \cos 4(\theta'_a - \theta_b) + \cos 4(\theta'_a - \theta'_b)] \\
&\hspace{25em} \text{(B.22)}
\end{aligned}$$

This CHSH-equation also can never reach the theoretical maximum of $S = 2\sqrt{2}$. Instead, the maximum is found at $1 + \sqrt{2} = 2.414$ for the following angles:

$$\begin{aligned}
\theta_a &= \frac{\pi}{8} &= 22.5^\circ \\
\theta_b &= \frac{\pi}{16} &= 11.25^\circ \\
\theta'_a &= 0 &= 0^\circ \\
\theta'_b &= \frac{7\pi}{16} &= 78.75^\circ
\end{aligned}$$

Bibliography

- [1] K. P. Schatz, B. Amies-King, S. Albosh, R. Kumar and M. Lucamarini. 'Practical single-fibre network-oriented quantum key distribution from a compact source of entangled photons in presence of White Rabbit time synchronisation'. In: *Quantum Technology*. Proceedings of SPIE - The International Society for Optical Engineering (Jan. 2023). Ed. by Miles J. Padgett, Kai Bongs, Alessandro Fedrizzi and Alberto Politi. DOI: 10.1117/12.2647691. URL: <http://www.scopus.com/inward/record.url?scp=85152769888&partnerID=8YFLogxK> (Accessed: 16/3/2026).
- [2] Ben Amies-King et al. 'Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link'. en. In: *Entropy* 25.12 (Dec. 2023), p. 1572. ISSN: 1099-4300. DOI: 10.3390/e25121572. URL: <https://www.mdpi.com/1099-4300/25/12/1572> (Accessed: 13/3/2026).
- [3] A. Einstein, B. Podolsky and N. Rosen. 'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?' In: *Physical Review* 47.10 (May 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777. URL: <https://link.aps.org/doi/10.1103/PhysRev.47.777> (Accessed: 1/3/2026).
- [4] J. S. Bell. 'On the Einstein Podolsky Rosen paradox'. In: *Physics Physique Fizika* 1.3 (Nov. 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: <https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195> (Accessed: 2/2/2026).
- [5] Marissa Giustina et al. 'Bell violation using entangled photons without the fair-sampling assumption'. en. In: *Nature* 497.7448 (May 2013), pp. 227–230. ISSN: 1476-4687. DOI: 10.1038/nature12012. URL: <https://www.nature.com/articles/nature12012> (Accessed: 22/3/2026).
- [6] B. Hensen et al. 'Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres'. en. In: *Nature* 526.7575 (Oct. 2015), pp. 682–686. ISSN: 1476-4687. DOI: 10.1038/nature15759. URL: <https://www.nature.com/articles/nature15759> (Accessed: 22/3/2026).
- [7] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau and Harald Weinfurter. 'Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes'. In: *Physical Review Letters* 119.1 (July 2017), p. 010402. DOI: 10.1103/PhysRevLett.119.010402. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.119.010402> (Accessed: 22/3/2026).

-
- [8] Anton Zeilinger, Alain Aspect and John F. Clauser. *Nobel Prize in Physics 2022*. en-US. URL: <https://www.nobelprize.org/prizes/physics/2022/zeilinger/facts/> (Accessed: 2/3/2026).
 - [9] Stephanie Wehner, David Elkouss and Ronald Hanson. 'Quantum internet: A vision for the road ahead'. In: *Science* 362.6412 (Oct. 2018), eaam9288. DOI: 10.1126/science.aam9288. URL: <https://www.science.org/doi/10.1126/science.aam9288> (Accessed: 2/3/2026).
 - [10] R. L. Rivest, A. Shamir and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: <https://dl.acm.org/doi/10.1145/359340.359342> (Accessed: 2/3/2026).
 - [11] W. Diffie and M. Hellman. 'New directions in cryptography'. In: *IEEE Trans. Inf. Theor.* 22.6 (Sept. 2006), pp. 644–654. ISSN: 0018-9448. DOI: 10.1109/TIT.1976.1055638. URL: <https://doi.org/10.1109/TIT.1976.1055638> (Accessed: 2/3/2026).
 - [12] E. Rescorla. *RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3*. en. RFC 8446. 2018. DOI: 10.17487/RFC8446. URL: <https://dl.acm.org/doi/book/10.17487/RFC8446> (Accessed: 2/3/2026).
 - [13] ISO/IEC. *ISO/IEC 18033-3:2010 — Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*. en. URL: <https://www.iso.org/standard/54531.html> (Accessed: 2/3/2026).
 - [14] P.W. Shor. 'Algorithms for quantum computation: discrete logarithms and factoring'. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700. URL: <https://ieeexplore.ieee.org/document/365700> (Accessed: 1/3/2026).
 - [15] Lov K. Grover. 'A fast quantum mechanical algorithm for database search'. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*. STOC '96. New York, NY, USA: Association for Computing Machinery, July 1996, pp. 212–219. ISBN: 978-0-89791-785-8. DOI: 10.1145/237814.237866. URL: <https://dl.acm.org/doi/10.1145/237814.237866> (Accessed: 1/3/2026).
 - [16] John Preskill. 'Quantum Computing in the NISQ era and beyond'. en-GB. In: *Quantum* 2 (Aug. 2018), p. 79. DOI: 10.22331/q-2018-08-06-79. URL: <https://quantum-journal.org/papers/q-2018-08-06-79/> (Accessed: 2/3/2026).
 - [17] Michele Mosca. 'Cybersecurity in an Era with Quantum Computers: Will We Be Ready?' In: *IEEE Security & Privacy* 16.5 (Sept. 2018), pp. 38–41. ISSN: 1558-4046. DOI: 10.1109/MSP.2018.3761723. URL: <https://ieeexplore.ieee.org/document/8490169> (Accessed: 2/3/2026).
 - [18] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel and Hugo Zbinden. 'Quantum cryptography'. In: *Reviews of Modern Physics* 74.1 (Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145. URL: <https://link.aps.org/doi/10.1103/RevModPhys.74.145> (Accessed: 1/3/2026).
 - [19] W. K. Wootters and W. H. Zurek. 'A single quantum cannot be cloned'. en. In: *Nature* 299.5886 (Oct. 1982), pp. 802–803. ISSN: 1476-4687. DOI: 10.1038/299802a0. URL: <https://www.nature.com/articles/299802a0> (Accessed: 4/3/2026).

-
- [20] C. E. Shannon. 'Communication theory of secrecy systems'. In: *The Bell System Technical Journal* 28.4 (Oct. 1949), pp. 656–715. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1949.tb00928.x. URL: <https://ieeexplore.ieee.org/document/6769090> (Accessed: 6/3/2026).
- [21] Charles H. Bennett, Gilles Brassard and N. David Mermin. 'Quantum cryptography without Bell's theorem'. In: *Physical Review Letters* 68.5 (Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.68.557> (Accessed: 17/2/2026).
- [22] Peter W. Shor and John Preskill. 'Simple Proof of Security of the BB84 Quantum Key Distribution Protocol'. In: *Physical Review Letters* 85.2 (July 2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.85.441> (Accessed: 6/3/2026).
- [23] Masato Koashi and Andreas Winter. 'Monogamy of quantum entanglement and other correlations'. In: *Physical Review A* 69.2 (Feb. 2004), p. 022309. DOI: 10.1103/PhysRevA.69.022309. URL: <https://link.aps.org/doi/10.1103/PhysRevA.69.022309> (Accessed: 8/3/2026).
- [24] Artur K. Ekert. 'Quantum cryptography based on Bell's theorem'. In: *Physical Review Letters* 67.6 (Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661> (Accessed: 1/3/2026).
- [25] John F. Clauser, Michael A. Horne, Abner Shimony and Richard A. Holt. 'Proposed Experiment to Test Local Hidden-Variable Theories'. In: *Physical Review Letters* 23.15 (Oct. 1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880> (Accessed: 2/2/2026).
- [26] Gilles Brassard, Norbert Lütkenhaus, Tal Mor and Barry C. Sanders. 'Limitations on Practical Quantum Cryptography'. In: *Physical Review Letters* 85.6 (Aug. 2000), pp. 1330–1333. DOI: 10.1103/PhysRevLett.85.1330. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.85.1330> (Accessed: 8/3/2026).
- [27] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar and Vadim Makarov. 'Hacking commercial quantum cryptography systems by tailored bright illumination'. In: *Nature Photonics* 4.10 (Oct. 2010), pp. 686–689. ISSN: 1749-4893. DOI: 10.1038/nphoton.2010.214. URL: <https://www.nature.com/articles/nphoton.2010.214> (Accessed: 8/3/2026).
- [28] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo and Xiongfeng Ma. 'Time-shift attack in practical quantum cryptosystems'. In: *Quant. Inf. Comput.* 7.1-2 (2007). eprint: quant-ph/0512080, pp. 073–082. DOI: 10.26421/QIC7.1-2-3.
- [29] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani and Leonardo Banchi. 'Fundamental limits of repeaterless quantum communications'. In: *Nature Communications* 2017 8:1 8.1 (Apr. 2017), pp. 1–15. DOI: 10.1038/ncomms15043. URL: <https://www.nature.com/articles/ncomms15043>.

-
- [30] M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields. 'Overcoming the rate–distance limit of quantum key distribution without quantum repeaters'. en. In: *Nature* 557.7705 (May 2018), pp. 400–403. ISSN: 1476-4687. DOI: 10.1038/s41586-018-0066-6. URL: <https://www.nature.com/articles/s41586-018-0066-6> (Accessed: 9/3/2026).
 - [31] Kiyoshi Tamaki, Hoi-Kwong Lo, Wenyuan Wang and Marco Lucamarini. 'Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound'. In: (May 2018). URL: <https://arxiv.org/abs/1805.05511v3>.
 - [32] Xiang Bin Wang, Zong Wen Yu and Xiao Long Hu. 'Twin-field quantum key distribution with large misalignment error'. In: *Physical Review A* 98.6 (Dec. 2018), pp. 062323–062323. DOI: 10.1103/PHYSREVA.98.062323/FIGURES/3/MEDIUM. URL: <https://journals.aps.org/prabstract/10.1103/PhysRevA.98.062323>.
 - [33] Jie Lin and Norbert Lütkenhaus. 'Simple security analysis of phase-matching measurement-device-independent quantum key distribution'. In: *Physical Review A* 98.4 (Oct. 2018), p. 042332. DOI: 10.1103/PhysRevA.98.042332. URL: <https://link.aps.org/doi/10.1103/PhysRevA.98.042332> (Accessed: 22/3/2026).
 - [34] Marcos Curty, Koji Azuma and Hoi-Kwong Lo. 'Simple security proof of twin-field type quantum key distribution protocol'. en. In: *npj Quantum Information* 5.1 (July 2019), p. 64. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0175-6. URL: <https://www.nature.com/articles/s41534-019-0175-6> (Accessed: 9/3/2026).
 - [35] Chaohan Cui, Zhen-Qiang Yin, Rong Wang, Wei Chen, Shuang Wang, Guang-Can Guo and Zheng-Fu Han. 'Twin-Field Quantum Key Distribution without Phase Postselection'. In: *Physical Review Applied* 11.3 (Mar. 2019), p. 034053. DOI: 10.1103/PhysRevApplied.11.034053. URL: <https://link.aps.org/doi/10.1103/PhysRevApplied.11.034053> (Accessed: 22/3/2026).
 - [36] 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'. en. In: *Nature Photonics* 13.5 (May 2019), pp. 334–338. ISSN: 1749-4893. DOI: 10.1038/s41566-019-0377-7. URL: <https://www.nature.com/articles/s41566-019-0377-7> (Accessed: 22/3/2026).
 - [37] Mirko Pittaluga et al. '600-km repeater-like quantum communications with dual-band stabilization'. en. In: *Nature Photonics* 15.7 (July 2021), pp. 530–535. ISSN: 1749-4893. DOI: 10.1038/s41566-021-00811-0. URL: <https://www.nature.com/articles/s41566-021-00811-0> (Accessed: 22/3/2026).
 - [38] H.-J. Briegel, W. Dür, J. I. Cirac and P. Zoller. 'Quantum Repeater: The Role of Imperfect Local Operations in Quantum Communication'. In: *Physical Review Letters* 81.26 (Dec. 1998), pp. 5932–5935. DOI: 10.1103/PhysRevLett.81.5932. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.81.5932> (Accessed: 9/3/2026).
 - [39] L.-M. Duan, M. D. Lukin, J. I. Cirac and P. Zoller. 'Long-distance quantum communication with atomic ensembles and linear optics'. en. In: *Nature* 414.6862 (Nov. 2001), pp. 413–418. ISSN: 1476-4687. DOI: 10.1038/35106500. URL: <https://www.nature.com/articles/35106500> (Accessed: 9/3/2026).

-
- [40] S. Pirandola et al. 'Advances in quantum cryptography'. EN. In: *Advances in Optics and Photonics* 12.4 (Dec. 2020), pp. 1012–1236. ISSN: 1943-8206. DOI: 10.1364/AOP.361502. URL: <https://opg.optica.org/aop/abstract.cfm?uri=aop-12-4-1012> (Accessed: 9/3/2026).
- [41] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo and Ilan Tzitrin. 'Quantum repeaters: From quantum networks to the quantum internet'. In: *Reviews of Modern Physics* 95.4 (Dec. 2023), p. 045006. DOI: 10.1103/RevModPhys.95.045006. URL: <https://link.aps.org/doi/10.1103/RevModPhys.95.045006> (Accessed: 9/3/2026).
- [42] Siddarth Koduru Joshi et al. 'A trusted node-free eight-user metropolitan quantum communication network'. In: *Science Advances* 6.36 (Sept. 2020). DOI: 10.1126/SCIADV.ABA0959. URL: <https://www.science.org>.
- [43] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, & Rupert Ursin, Friedrich Schiller and Universitz Jena. 'An entanglement-based wavelength-multiplexed quantum communication network'. In: *Nature* (2018). DOI: 10.1038/s41586-018-0766-y. URL: <https://doi.org/10.1038/s41586-018-0766-y>.
- [44] Alexander Pickston et al. 'Conference key agreement in a quantum network'. en. In: *npj Quantum Information* 9.1 (Aug. 2023), p. 82. ISSN: 2056-6387. DOI: 10.1038/s41534-023-00750-4. URL: <https://www.nature.com/articles/s41534-023-00750-4> (Accessed: 10/3/2026).
- [45] Jiu-Peng Chen et al. 'Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km'. In: *Physical Review Letters* 124.7 (Feb. 2020), p. 070501. DOI: 10.1103/PhysRevLett.124.070501. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.124.070501> (Accessed: 9/3/2026).
- [46] Alberto Boaron et al. 'Secure Quantum Key Distribution over 421 km of Optical Fiber'. In: *Physical Review Letters* 121.19 (Nov. 2018), p. 190502. DOI: 10.1103/PhysRevLett.121.190502. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.121.190502> (Accessed: 9/3/2026).
- [47] Hua-Lei Yin et al. 'Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber'. In: *Physical Review Letters* 117.19 (Nov. 2016), p. 190501. DOI: 10.1103/PhysRevLett.117.190501. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.117.190501> (Accessed: 9/3/2026).
- [48] Yang Liu et al. 'Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance'. In: *Physical Review Letters* 130.21 (May 2023), p. 210801. DOI: 10.1103/PhysRevLett.130.210801. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.130.210801> (Accessed: 9/3/2026).
- [49] Hui Liu et al. 'Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km'. In: *Physical Review Letters* 126.25 (June 2021), p. 250502. DOI: 10.1103/PhysRevLett.126.250502. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.126.250502> (Accessed: 9/3/2026).

-
- [50] Sebastian Philipp Neumann, Alexander Buchner, Lukas Bulla, Martin Bohmann and Rupert Ursin. 'Continuous entanglement distribution over a transnational 248 km fiber link'. In: *Nature Communications* 13 (Oct. 2022), p. 6134. ISSN: 2041-1723. DOI: 10.1038/s41467-022-33919-0. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC9576737/> (Accessed: 9/3/2026).
 - [51] Shi-Chang Zhuang et al. 'Ultrabright Entanglement Based Quantum Key Distribution over a 404 km Optical Fiber'. In: *Physical Review Letters* 134.23 (June 2025), p. 230801. DOI: 10.1103/PhysRevLett.134.230801. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.134.230801> (Accessed: 9/3/2026).
 - [52] Xi-Yu Luo et al. *Entangling quantum memories over 420 km in fiber*. arXiv:2504.05660 [quant-ph]. Apr. 2025. DOI: 10.48550/arXiv.2504.05660. URL: <http://arxiv.org/abs/2504.05660> (Accessed: 9/3/2026).
 - [53] Yang Li et al. 'Microsatellite-based real-time quantum key distribution'. en. In: *Nature* 640.8057 (Apr. 2025), pp. 47–54. ISSN: 1476-4687. DOI: 10.1038/s41586-025-08739-z. URL: <https://www.nature.com/articles/s41586-025-08739-z> (Accessed: 10/3/2026).
 - [54] Juan Yin et al. 'Satellite-based entanglement distribution over 1200 kilometers'. In: *Science* 356.6343 (June 2017), pp. 1140–1144. DOI: 10.1126/science.aan3211. URL: <https://www.science.org/doi/10.1126/science.aan3211> (Accessed: 9/3/2026).
 - [55] Zhiliang Yuan et al. '10-Mb/s Quantum Key Distribution'. In: *Journal of Lightwave Technology* 36.16 (Aug. 2018), pp. 3427–3433. ISSN: 1558-2213. DOI: 10.1109/JLT.2018.2843136. URL: <https://ieeexplore.ieee.org/document/8370644> (Accessed: 10/3/2026).
 - [56] Fadri Grünenfelder et al. 'Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems'. en. In: *Nature Photonics* 17.5 (May 2023), pp. 422–426. ISSN: 1749-4893. DOI: 10.1038/s41566-023-01168-2. URL: <https://www.nature.com/articles/s41566-023-01168-2> (Accessed: 10/3/2026).
 - [57] Wei Li et al. 'High-rate quantum key distribution exceeding 110 Mb s⁻¹'. In: *Nature Photonics* 2023 17:5 17.5 (Mar. 2023), pp. 416–421. DOI: 10.1038/s41566-023-01166-4. URL: <https://www.nature.com/articles/s41566-023-01166-4>.
 - [58] Heng Wang et al. 'High-rate continuous-variable quantum key distribution over 100 km fiber with composable security'. EN. In: *Optica* 12.10 (Oct. 2025), pp. 1657–1667. ISSN: 2334-2536. DOI: 10.1364/OPTICA.566359. URL: <https://opg.optica.org/optica/abstract.cfm?uri=optica-12-10-1657> (Accessed: 10/3/2026).
 - [59] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus and Momtchil Peev. 'The security of practical quantum key distribution'. In: *Reviews of Modern Physics* 81.3 (Sept. 2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. URL: <https://link.aps.org/doi/10.1103/RevModPhys.81.1301> (Accessed: 20/1/2026).

- [60] Hoi-Kwong Lo, Xiongfeng Ma and Kai Chen. 'Decoy State Quantum Key Distribution'. In: *Physical Review Letters* 94.23 (June 2005), p. 230504. DOI: 10.1103/PhysRevLett.94.230504. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.94.230504> (Accessed: 11/3/2026).
- [61] Xiang-Bin Wang. 'Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography'. In: *Physical Review Letters* 94.23 (June 2005), p. 230503. DOI: 10.1103/PhysRevLett.94.230503. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.94.230503> (Accessed: 11/3/2026).
- [62] Cong Jiang, Xiao-Long Hu, Zong-Wen Yu and Xiang-Bin Wang. 'Side-channel security of practical quantum key distribution'. In: *Physical Review Research* 6.1 (Mar. 2024), p. 013266. DOI: 10.1103/PhysRevResearch.6.013266. URL: <https://link.aps.org/doi/10.1103/PhysRevResearch.6.013266> (Accessed: 11/3/2026).
- [63] Hoi-Kwong Lo, Marcos Curty and Bing Qi. 'Measurement-Device-Independent Quantum Key Distribution'. In: *Physical Review Letters* 108.13 (Mar. 2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.108.130503> (Accessed: 11/3/2026).
- [64] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian and Hoi-Kwong Lo. 'Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution'. In: *Physical Review Letters* 112.19 (May 2014), p. 190503. DOI: 10.1103/PhysRevLett.112.190503. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.112.190503> (Accessed: 11/3/2026).
- [65] Li-Wen Hu, Chun-Mei Zhang and Hong-Wei Li. 'Practical measurement-device-independent quantum key distribution with advantage distillation'. en. In: *Quantum Information Processing* 22.1 (Jan. 2023), p. 77. ISSN: 1573-1332. DOI: 10.1007/s11128-022-03810-4. URL: <https://doi.org/10.1007/s11128-022-03810-4> (Accessed: 11/3/2026).
- [66] Wei Zhang et al. 'A device-independent quantum key distribution system for distant users'. In: *Nature* 2022 607:7920 607.7920 (July 2022), pp. 687–691. DOI: 10.1038/s41586-022-04891-y. URL: <https://www.nature.com/articles/s41586-022-04891-y>.
- [67] Bo-Wei Lu et al. 'Device-independent quantum key distribution over 100 km with single atoms'. In: *Science* 391.6785 (Feb. 2026), pp. 592–597. DOI: 10.1126/science.aec6243. URL: <https://www.science.org/doi/10.1126/science.aec6243> (Accessed: 22/3/2026).
- [68] Erik Agrell et al. 'Roadmap on optical communications'. en. In: *Journal of Optics* 26.9 (July 2024), p. 093001. ISSN: 2040-8986. DOI: 10.1088/2040-8986/ad261f. URL: <https://doi.org/10.1088/2040-8986/ad261f> (Accessed: 9/3/2026).
- [69] Adnan A. E. Hajomer, Ivan Derkach, Vladyslav C. Usenko, Ulrik L. Andersen and Tobias Gehring. 'Coexistence of Continuous-Variable Quantum Key Distribution and Classical Data over 120 km Fiber'. In: *Physical Review Letters* 135.17 (Oct. 2025), p. 170804. DOI: 10.1103/zy2d-m3ch. URL: <https://link.aps.org/doi/10.1103/zy2d-m3ch> (Accessed: 11/3/2026).

-
- [70] Nicolás Linale, Adrià Sansa, Ignacio Lopez Grande, Lorenzo Castolvero and Valerio Pruneri. 'Coexistence of classical and polarization-encoded QKD signals over deployed fiber'. EN. In: *Optics Express* 34.5 (Mar. 2026), pp. 7566–7580. ISSN: 1094-4087. DOI: 10.1364/OE.583877. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-34-5-7566> (Accessed: 11/3/2026).
 - [71] T. Gerrits et al. 'White Rabbit-assisted quantum network node synchronization with quantum channel coexistence'. In: *2022 Conference on Lasers and Electro-Optics (CLEO)*. ISSN: 2160-8989. May 2022, pp. 1–2. URL: <https://ieeexplore.ieee.org/document/9891554> (Accessed: 11/3/2026).
 - [72] Romain Alléaume et al. 'Worldwide standardization activity for quantum key distribution'. In: *2014 IEEE Globecom Workshops (GC Wkshps)*. ISSN: 2166-0077. Dec. 2014, pp. 656–661. DOI: 10.1109/GLOCOMW.2014.7063507. URL: <https://ieeexplore.ieee.org/document/7063507> (Accessed: 12/3/2026).
 - [73] International Telecommunication Union (ITU-T). *Quantum key distribution network interworking - Framework*. Sept. 2024. URL: <https://www.itu.int/rec/T-REC-Y.3810/en> (Accessed: 12/3/2026).
 - [74] Marco Lucamarin, Andrew Shields, Romain Alléaume, Christopher Chunnillall and Zhiliang Yuan. *Implementation Security of Quantum Cryptography - Introduction, challenges, solutions*. en. Tech. rep. European Telecommunications Standards Institute.
 - [75] European Telecommunications Standards Institute. *Quantum Key Distribution (QKD) ETSI-ISG*. en-gb. URL: <https://www.etsi.org/technologies/quantum-key-distribution> (Accessed: 12/3/2026).
 - [76] International Organisation for Standardization (ISO). *Information security — Security requirements, test and evaluation methods for quantum key distribution*. Aug. 2023. (Accessed: 12/2/2026).
 - [77] Quantum Communications Hub (UK). *Quantum Communications Hub*. en. URL: <https://www.quantumcommshub.net/> (Accessed: 12/3/2026).
 - [78] UK Research and Innovation (UKRI). *UK National Quantum Technologies Programme*. en-GB. URL: <https://uknqt.ukri.org/> (Accessed: 12/3/2026).
 - [79] The UK Integrated Quantum Networks Hub. *The UK Integrated Quantum Networks Hub*. en-GB. Apr. 2025. URL: <https://iqnhub.org/welcome/> (Accessed: 12/3/2026).
 - [80] M Peev et al. 'The SECOQC quantum key distribution network in Vienna'. en. In: *New Journal of Physics* 11.7 (July 2009), p. 075001. ISSN: 1367-2630. DOI: 10.1088/1367-2630/11/7/075001. URL: <https://doi.org/10.1088/1367-2630/11/7/075001> (Accessed: 9/3/2026).
 - [81] D Stucki et al. 'Long-term performance of the SwissQuantum quantum key distribution network in a field environment'. en. In: *New Journal of Physics* 13.12 (Dec. 2011), p. 123001. ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/12/123001. URL: <https://doi.org/10.1088/1367-2630/13/12/123001> (Accessed: 13/3/2026).
 - [82] Istituto Nazionale di Ricerca Metrologica. *The Italian Quantum Backbone*. URL: <https://www.inrim.it/en/research/infrastructures/italian-quantum-backbone> (Accessed: 13/3/2026).

-
- [83] D. Lopez, J. P. Brito, A. Pastor, V. Martin, C. Sánchez, D. Rincon and V. Lopez. 'Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks'. EN. In: *Optical Fiber Communication Conference (OFC) 2021 (2021), paper Th2A.4*. Optica Publishing Group, June 2021, Th2A.4. DOI: 10.1364/OFC.2021.Th2A.4. URL: <https://opg.optica.org/abstract.cfm?uri=OFC-2021-Th2A.4> (Accessed: 13/3/2026).
 - [84] European Commission. *European Quantum Communication Infrastructure - EuroQCI / Shaping Europe's digital future*. en. URL: <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci> (Accessed: 13/3/2026).
 - [85] Domenico Ribezzo et al. 'Deploying an Inter-European Quantum Network'. en. In: *Advanced Quantum Technologies* 6.2 (2023). _eprint: <https://advanced.onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202200061>, p. 2200061. ISSN: 2511-9044. DOI: 10.1002/qute.202200061. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202200061> (Accessed: 13/3/2026).
 - [86] Hao-Ze Chen et al. 'Implementation of carrier-grade quantum communication networks over 10000 km'. en. In: *npj Quantum Information* 11.1 (Aug. 2025), p. 137. ISSN: 2056-6387. DOI: 10.1038/s41534-025-01089-8. URL: <https://www.nature.com/articles/s41534-025-01089-8> (Accessed: 22/7/2026).
 - [87] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng and Jian-Wei Pan. 'Micius quantum experiments in space'. In: *Reviews of Modern Physics* 94.3 (July 2022), p. 035001. DOI: 10.1103/RevModPhys.94.035001. URL: <https://link.aps.org/doi/10.1103/RevModPhys.94.035001> (Accessed: 13/3/2026).
 - [88] Yu-Ao Chen et al. 'An integrated space-to-ground quantum communication network over 4,600 kilometres'. en. In: *Nature* 589.7841 (Jan. 2021), pp. 214–219. ISSN: 1476-4687. DOI: 10.1038/s41586-020-03093-8. URL: <https://www.nature.com/articles/s41586-020-03093-8> (Accessed: 13/3/2026).
 - [89] M. Sasaki et al. 'Field test of quantum key distribution in the Tokyo QKD Network'. EN. In: *Optics Express* 19.11 (May 2011), pp. 10387–10409. ISSN: 1094-4087. DOI: 10.1364/OE.19.010387. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-19-11-10387> (Accessed: 9/3/2026).
 - [90] Greg Bock. *Japan to Link Major Cities with 600-km Quantum Encryption Network*. en-US. Nov. 2025. URL: <https://thequantuminsider.com/2025/11/26/japan-to-link-major-cities-with-600-km-quantum-encryption-network/> (Accessed: 13/3/2026).
 - [91] Eric Bersin et al. 'Development of a Boston-area 50-km fiber quantum network testbed'. In: (July 2023). URL: <https://arxiv.org/abs/2307.15696v1>.
 - [92] Joaquin Chung et al. 'Design and Implementation of the Illinois Express Quantum Metropolitan Area Network'. In: *IEEE Transactions on Quantum Engineering* 3 (2022), pp. 1–20. ISSN: 2689-1808. DOI: 10.1109/TQE.2022.3221029. URL: <https://ieeexplore.ieee.org/abstract/document/9946408> (Accessed: 13/3/2026).

- [93] Inder Monga, Erhan Saglamyurek, Ezra Kissel, Hartmut Haffner and Wenji Wu. 'QUANT-NET: A testbed for quantum networking research over deployed fiber'. In: *Proceedings of the 1st Workshop on Quantum Networks and Distributed Quantum Computing*. QuNet '23. New York, NY, USA: Association for Computing Machinery, Sept. 2023, pp. 31–37. ISBN: 979-8-4007-0306-5. DOI: 10.1145/3610251.3610561. URL: <https://dl.acm.org/doi/10.1145/3610251.3610561> (Accessed: 13/3/2026).
- [94] Sören Wengerowsky et al. 'Entanglement distribution over a 96-km-long submarine optical fiber'. In: *Proceedings of the National Academy of Sciences of the United States of America* 116.14 (Apr. 2019), pp. 6684–6688. DOI: 10.1073/PNAS.1818752116/ASSET/78212305-AD12-4E7F-81C3-59D155EB80A6/ASSETS/GRAPHIC/PNAS.1818752116FIG04.JPEG. URL: <https://www.pnas.org/doi/abs/10.1073/pnas.1818752116>.
- [95] Domenico Ribezzo et al. 'Quantum Key Distribution over 100 km underwater optical fiber assisted by a Fast-Gated Single-Photon Detector'. In: (Mar. 2023). URL: <https://arxiv.org/abs/2303.01449v1>.
- [96] Rodney Loudon. *The Quantum Theory of Light*. Third Edition, Third Edition. Oxford, New York: Oxford University Press, Nov. 2000. ISBN: 978-0-19-850176-3.
- [97] Rolf Horn and Thomas Jennewein. 'Auto-balancing and robust interferometer designs for polarization entangled photon sources'. In: *Optics Express* 27.12 (June 2019), pp. 17369–17369. DOI: 10.1364/oe.27.017369.
- [98] Shin Arahira, Naoto Namekata, Tadashi Kishimoto, Hiroki Yaegashi and Shuichiro Inoue. 'Generation of polarization entangled photon pairs at telecommunication wavelength using cascaded $\chi^{(2)}$ processes in a periodically poled LiNbO₃ ridge waveguide'. In: *Optics Express* 19.17 (Aug. 2011). DOI: 10.1364/OE.19.016032.
- [99] J. J. Thorn, M. S. Neel, V. W. Donato, G. S. Bergreen, R. E. Davies and M. Beck. 'Observing the quantum behavior of light in an undergraduate laboratory'. In: *American Journal of Physics* 72.9 (Sept. 2004), pp. 1210–1219. DOI: 10.1119/1.1737397.
- [100] R. Hanbury Brown and R. Q. Twiss. 'Correlation between Photons in two Coherent Beams of Light'. en. In: *Nature* 177.4497 (Jan. 1956), pp. 27–29. ISSN: 1476-4687. DOI: 10.1038/177027a0. URL: <https://www.nature.com/articles/177027a0> (Accessed: 22/3/2026).
- [101] Mark (Anthony Mark) Fox. *Quantum optics : an introduction / Mark Fox*. Oxford : Oxford University Press, 2006. ISBN: 978-0-19-856672-4.
- [102] Max Born. 'Zur Quantenmechanik der Stoßvorgänge'. de. In: *Zeitschrift für Physik* 37.12 (Dec. 1926), pp. 863–867. ISSN: 0044-3328. DOI: 10.1007/BF01397477. URL: <https://doi.org/10.1007/BF01397477> (Accessed: 11/2/2026).
- [103] J. B. Altpeter, E. R. Jeffrey and P. G. Kwiat. 'Photonic State Tomography'. en-US. In: *Advances In Atomic, Molecular, and Optical Physics*. Vol. 52. Academic Press, Jan. 2005, pp. 105–159. DOI: 10.1016/S1049-250X(05)52003-2. URL: <https://www.sciencedirect.com/science/chapter/bookseries/abs/pii/S1049250X05520032> (Accessed: 25/2/2026).

-
- [104] Daniel F. V. James, Paul G. Kwiat, William J. Munro and Andrew G. White. 'Measurement of qubits'. In: *Physical Review A* 64.5 (Oct. 2001), p. 052312. DOI: 10.1103/PhysRevA.64.052312. URL: <https://link.aps.org/doi/10.1103/PhysRevA.64.052312> (Accessed: 25/2/2026).
 - [105] 'On the Composition and Resolution of Streams of Polarized Light from different Sources'. In: *Mathematical and Physical Papers*. Ed. by George Gabriel Stokes. Vol. 3. Cambridge Library Collection - Mathematics. Cambridge: Cambridge University Press, 2009, pp. 233–258. ISBN: 978-1-108-00264-6. DOI: 10.1017/CB09780511702266.010. URL: <https://www.cambridge.org/core/books/mathematical-and-physical-papers/on-the-composition-and-resolution-of-streams-of-polarized-light-from-different-sources/A021426E1F3E9BD366E8E1F967FB E3CE> (Accessed: 25/2/2026).
 - [106] Richard Jozsa. 'Fidelity for Mixed Quantum States'. In: *Journal of Modern Optics* 41.12 (Dec. 1994). _eprint: <https://doi.org/10.1080/09500349414552171>, pp. 2315–2323. ISSN: 0950-0340. DOI: 10.1080/09500349414552171. URL: <https://doi.org/10.1080/09500349414552171> (Accessed: 16/3/2026).
 - [107] William K. Wootters. 'Entanglement of Formation of an Arbitrary State of Two Qubits'. In: *Physical Review Letters* 80.10 (Mar. 1998), pp. 2245–2248. DOI: 10.1103/PhysRevLett.80.2245. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.80.2245> (Accessed: 16/3/2026).
 - [108] Kyungdeuk Park, Jungmo Lee, Dong-Gil Im, Dongkyu Kim and Yong Sup Ihn. 'Ultrabright Fiber-Coupled Polarization-Entangled Photon Source with Spectral Brightness Surpassing 2.0 MHz mW−1 nm−1'. en. In: *Advanced Photonics Research* 6.10 (2025), p. 2500024. ISSN: 2699-9293. DOI: 10.1002/adpr.202500024. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/adpr.202500024> (Accessed: 17/8/2026).
 - [109] Ilhwan Kim, Yosep Kim, Yong-Su Kim, Kwang Jo Lee and Hyang-Tag Lim. 'Robust and bright polarization-entangled photon sources exploiting non-critical phase matching without periodic poling'. EN. In: *Optics Express* 33.11 (June 2025), pp. 22087–22103. ISSN: 1094-4087. DOI: 10.1364/OE.542612. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-33-11-22087> (Accessed: 17/8/2026).
 - [110] A. S Holevo. 'Statistical decision theory for quantum systems'. In: *Journal of Multivariate Analysis* 3.4 (Dec. 1973), pp. 337–394. ISSN: 0047-259X. DOI: 10.1016/0047-259X(73)90028-6. URL: <https://www.sciencedirect.com/science/article/pii/0047259X73900286> (Accessed: 18/3/2026).
 - [111] Lluís Masanes, Stefano Pironio and Antonio Acín. 'Secure device-independent quantum key distribution with causally independent measurement devices'. en. In: *Nature Communications* 2.1 (Mar. 2011), p. 238. ISSN: 2041-1723. DOI: 10.1038/ncomms1244. URL: <https://www.nature.com/articles/ncomms1244> (Accessed: 6/3/2026).
 - [112] T E Chapuran et al. 'Optical networking for quantum key distribution and quantum communications'. en. In: *New Journal of Physics* 11.10 (Oct. 2009), p. 105001. ISSN: 1367-2630. DOI: 10.1088/1367-2630/11/10/105001. URL: <https://doi.org/10.1088/1367-2630/11/10/105001> (Accessed: 26/3/2026).

- [113] Iris Choi, Robert J Young and Paul D Townsend. 'Quantum information to the home'. en. In: *New Journal of Physics* 13.6 (June 2011), p. 063039. ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/6/063039. URL: <https://doi.org/10.1088/1367-2630/13/6/063039> (Accessed: 26/3/2026).
- [114] P Eraerds, N Walenta, M Legré, N Gisin and H Zbinden. 'Quantum key distribution and 1 Gbps data encryption over a single fibre'. In: *New Journal of Physics* 12.6 (June 2010), pp. 63027–63027. DOI: 10.1088/1367-2630/12/6/063027. URL: <https://dx.doi.org/10.1088/1367-2630/12/6/063027>.
- [115] K. A. Patel et al. 'Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber'. In: *Physical Review X* 2.4 (Nov. 2012), p. 041010. DOI: 10.1103/PhysRevX.2.041010. URL: <https://link.aps.org/doi/10.1103/PhysRevX.2.041010> (Accessed: 26/3/2026).
- [116] Weiwen Kong et al. 'Enhanced Coexistence of Quantum Key Distribution and Classical Communication over Hollow-Core and Multi-Core Fibers'. en. In: *Entropy* 26.7 (July 2024), p. 601. ISSN: 1099-4300. DOI: 10.3390/e26070601. URL: <https://www.mdpi.com/1099-4300/26/7/601> (Accessed: 26/3/2026).
- [117] Maciej Lipiński, Tomasz Włostowski, Javier Serrano and Pablo Alvarez. 'White rabbit: A PTP application for robust sub-nanosecond synchronization'. In: *IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication, ISPCS* (2011), pp. 25–30. ISSN: 9781612848921. DOI: 10.1109/ISPCS.2011.6070148.
- [118] Ben Amies-King and Marco Lucamarini. *Unrepeated White Rabbit Time Synchronisation over a 300 km Optical Fibre Link*. arXiv:2511.23254 [quant-ph]. Nov. 2025. DOI: 10.48550/arXiv.2511.23254. URL: <http://arxiv.org/abs/2511.23254> (Accessed: 26/3/2026).
- [119] Hiroki Takesue, Toshimori Honjo, Kiyoshi Tamaki and Yasuhiro Tokura. 'Differential phase shift quantum key distribution'. In: *2008 First ITU-T Kaleidoscope Academic Conference - Innovations in NGN: Future Network and Services*. May 2008, pp. 229–236. DOI: 10.1109/KINGN.2008.4542270. URL: <https://ieeexplore.ieee.org/document/4542270> (Accessed: 26/3/2026).
- [120] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe and A. J. Shields. 'Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate'. EN. In: *Optics Express* 16.23 (Nov. 2008), pp. 18790–18797. ISSN: 1094-4087. DOI: 10.1364/OE.16.018790. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-16-23-18790> (Accessed: 26/3/2026).
- [121] M. Lucamarini et al. 'Efficient decoy-state quantum key distribution with quantified security'. EN. In: *Optics Express* 21.21 (Oct. 2013), pp. 24550–24565. ISSN: 1094-4087. DOI: 10.1364/OE.21.024550. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-21-21-24550> (Accessed: 26/3/2026).
- [122] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen and Hoi-Kwong Lo. 'Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems'. In: *Physical Review A* 78.4 (Oct. 2008), p. 042333. DOI: 10.1103/PhysRevA.78.042333. URL: <https://link.aps.org/doi/10.1103/PhysRevA.78.042333> (Accessed: 26/3/2026).

- [123] Muneer Alshowkan et al. 'Advanced architectures for high-performance quantum networking'. In: *Journal of Optical Communications and Networking*, Vol. 14, Issue 6, pp. 493-499 14.6 (June 2022), pp. 493–499. DOI: 10.1364/JOCN.450201. URL: <https://opg.optica.org/viewmedia.cfm?uri=jocn-14-6-493&seq=0&html=true>.
- [124] Ivan Burenkov et al. 'Synchronization and Coexistence in Quantum networks'. en. In: *NIST* 31.7 (Mar. 2023). Last Modified: 2023-05-26T15:05-04:00. URL: <https://www.nist.gov/publications/synchronization-and-coexistence-quantum-networks> (Accessed: 26/3/2026).
- [125] Sheng-Kai Liao et al. 'Satellite-Relayed Intercontinental Quantum Network'. In: *Physical Review Letters* 120.3 (Jan. 2018), p. 030501. DOI: 10.1103/PhysRevLett.120.030501. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.120.030501> (Accessed: 27/3/2026).
- [126] Aleksandr Khmelev et al. 'Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis'. EN. In: *Optics Express* 32.7 (Mar. 2024), pp. 11964–11978. ISSN: 1094-4087. DOI: 10.1364/OE.511772. URL: <https://opg.optica.org/oe/abstract.cfm?uri=oe-32-7-11964> (Accessed: 27/3/2026).