2019-12

Measurement-device-independent quantum key distribution for metropolitan network

Umesh, Prathwiraj

UNIVERSITY OF CALGARY

Measurement-device-independent quantum key distribution for metropolitan network

by

Prathwiraj Umesh

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN PHYSICS AND ASTRONOMY

CALGARY, ALBERTA
DECEMBER, 2019

Abstract

Since its initial proposal in 2012, measurement-device-independent quantum key distribution (MDIQKD) has inspired rapid experimental progress as it is invulnerable to all detector side-channel attacks and ideally suitable for quantum key distribution (QKD) networks with star-topology, such as metropolitan networks. The main goal of this thesis is to develop MDIQKD systems for building a cost-effective metropolitan quantum network. Towards this end, we experimentally demonstrate the coexistence of MDIQKD with classical communication on the same fibre. This eliminates the use of dark fibre for quantum communication and minimises implementation costs by utilising the existing fibre infrastructure. Additionally, we move the quantum channel from the third telecommunication window (1530-1565 nm) to second (1260-1360 nm) to ensure MDIQKD can co-exist with classical communication rates of over 10-terabits per second. Furthermore, we enhance the performance of the MDIQKD systems by increasing the repetition rate from 20MHz to 200MHz and improve flexibility and reliability to facilitate the deployment of a metropolitan quantum network.

Acknowledgements

My masters would have been challenging without the help of many individuals. First, I can not be thankful enough to Raju Valivarthi for his guidance throughout my masters. He was a great colleague in the lab and a brother outside. I must thank Wolfgang Tittel for inviting me to be part of the team, trusting me entirely and giving me the freedom to perform the experiment the way I wanted. I have grown a lot under his tutelage in the last two years. I further thank Kim Owen and Caleb John for being lovely friends and lab mates. I appreciate all my lab members, Daniel Oblak, Marcelli Girimau, Mohsen Falamarzi, Jake Davidson, Gustavo Amaral, Thomas Lutz and Pascal, for making the lab lively place and making me feel like home. I also thank my friends in Delft Jorge Marques, Sara Marzaban and Joshua Slater for their support.

Outside the lab, I have to thank many people. I am indebted to two people for my life. First, my mother, for all the sacrifices she made and the hardest times she went through for me. Even though she never followed what I did, she always trusted me and encouraged me to do whatever I liked. My thanks will be too little for her stature. Second is my significant other, Preeti Bhat. She was with me in all my ups and downs and shared my happiness and pains. I thank her for her immense patience to make our relationship and life beautiful, and all the years she spent making me understand the value of a relationship. I further thank my father, grandmother and my family for their love. I thank my cousin, who was more than a brother, Adarsh KS, for being there for me whenever I needed his help and taking care of my family as a son while I was away from home. Many friends and mentors supported me

in my early research career. I thank Akshata, Dheeraj, Chandana, Hafsa, Surya, Ashutosh, Gaurav and all other friends in India and Urbasi Sinha for helping me to start a research career in Physics. I can not forget to thank Ajith KM, Udayshankar and Girsh BS for all their guidance in making every decision of my life. Apart from all the names mentioned above, I thank all my childhood friends and teachers for making my life pleasant.

Table of Contents

List of Figures and Illustrations

List of Tables

List of Symbols, Abbreviations and Nomenclature

Abbreviation	Definition
APD	Avalanche photodiode
ATTn	Attenuator
BS	Beam-splitter
BSM	Bell state measurement
CCS	Classical communication transceivers
CLK, clk	Clock
CWDM	Coarse wavelength division multiplexing
DAC	Digital to analog converter
DFB	Distributed feedback
DIQKD	Device independent quantum key distribution
DMM	Digital multimeter
DWDM	Dense wavelength division multiplexing
EOM	Electro-optic modulators
EVOA	Electronic variable optical attenuator
FPGA	Field programmable gate array
FWHM	Full width half maximum
FWM	Four-wave mixing
Gbps	Gigabit per second
GLLP	Gottesman, Lo, Lutkenhaus and Preskill
HOM	Hong-Ou-Mandel measurement
IM	Intensity modulator
ISO	Isolator
MAN	Metropolitan area network
MDIQKD	Measurement device independent quantum key distribution
NZ-DSF	nonzero dispersion-shifted fibre
ONT	Optical network terminal
PBS	Polarising beam-splitter
PC	Polarisation tracker
PD	Photo-detector
PM	Phase modulator
PMBS	Polarisation maintaining beam-splitter
PNS	Photon number splitting

QBER	Quantum bit error rate
QKD	Quantum key distribution
QND	Quantum non-demolition measurement
QRNG	Quantum random number generator
ROADM	reconfigurable optical adddrop multiplexer
SNSPD	Superconducting nanowire single photon detector
SPD	Single photon detector
SSMF	Single-mode fibre
Tbps	Terabit per second
VHDL	Very High Speed Integrated Circuit Hardware Description Language

Chapter 1

Introduction

1.1 Motivation for the thesis

Quantum key distribution (QKD) is the most mature technology in quantum information. QKD enables two distant users (generally known as Alice and Bob) to distil cryptographic keys based on the laws of quantum mechanics, such as the no-cloning theorem [14] and monogamy of the entanglement [15], in the presence of an Eavesdropper (commonly known as Eve) [16, 17, 18]. QKD, combined with one-time pad, an encryption technique where secret key is paired with the message, paves the way for secure communication without any assumptions about the computational capability of Eve. During the last three decades, theoretical and experimental QKD has advanced swiftly to achieve higher secret key rate [19], longer distances[20], reliability and robustness [21].

Even though QKD protocols offer information-theoretic security, real implementations of QKD do not always meet the assumptions made in the security proofs. This allows side channel attacks, also referred to as quantum hacking attacks, through which Eve may gain full information about the secret key distilled by Alice and Bob without leaving any trace. One such attack is the Blinding attack in which Eve exploits a vulnerability of single-photon detectors (SPDs) [3, 22]. In fact, the majority of side-channel attacks have targeted the

SPDs [4].

Two approaches can be pursued to overcome hacking attacks. The first approach is to devise specific countermeasures [23, 24]. However, these countermeasures may be circumvented by Eve. Furthermore, not all the possible attacks might be known at this point, and it is also possible for Eve to develop new strategies. The second approach is to implement protocols that are fundamentally secure against all side-channel attacks, such as device-independent QKD (DIQKD) [5]. Security of DIQKD is assured by a loophole-free Bell test. Even though there are demonstrations of such a test [25, 26, 27, 28], implementations of DIQKD still seem unlikely in the near future.

Noticing the fact that most of the attacks target SPDs, various groups investigated protocols that are secure against detector side-channel attacks [29, 30]. One such protocol is measurement-device-independent QKD (MDIQKD), which is based on time-reversed entanglement creation [31]. In MDIQKD, Alice and Bob both prepare qubits and send them to a central station, Charlie, who projects their joint state onto one of the maximally entangled Bell states. This ensures that Alice and Bob can establish a secret key without any assumption about the proper functioning of Charlie's devices - not even the single-photon detectors.

MDIQKD rapidly gained significant attention and triggered experimental progress. Various research groups have demonstrated the new protocol in labs and field tests [32, 33, 34, 35, 36, 37, 8, 38, 39, 40, 41]. Initial experiments were proof-of-principle demonstrations, whereas succeeding ones achieved milestones such as a communication distance of 404 km [38], a repetition rate of 1GHz [39], a 3-user MDIQKD network [37], and a sender system on a chip [41].

In addition to being invulnerable to detector-side attacks, MDIQKD is particularly well suitable for star-type networks, in which Charlie is the central station and holds all the expensive equipment. However, all previous MDIQKD demonstrations involved dark fibre (fibre which no light passing through it) for quantum communication making the creation of a network costly. When there are many users in the network, having an extra fibre per user is not an economical solution. Therefore, the investigation of coexistence of MDIQKD with classical data on the same fibre is crucial. I was a part of one such investigation, which is reported in [42]. In addition, I improved the system performance by increasing the secret key rate, flexibility and reliability. In summary, the goal of this thesis is to devise an MDI-QKD system that allows building a quantum metropolitan network.

1.2 Overview of the thesis

This thesis is organised in the following manner. In Chapter 2, I will describe some basics of quantum key distribution. Chapter 3 contains a brief description of a specific QKD protocol, "Measurement-device-independent quantum key distribution" (MDIQKD), and some related concepts such as the decoy-state method. In chapter 4, I will discuss the possibility of integrating quantum and classical communication into the same optical fibre, which would facilitate the future creation of quantum networks. Chapter 5 reports on one such investigation which was published in the journal "Quantum Science and Technology" [42]. In chapter 6, I will describe a newly devised MDIQKD that features a 10-fold increased repetition rate, enhanced flexibility and reliability, and can, according to our simulations, coexist with classical communication at rates of terabits per second. I will also detail the characterisation of the MDIQKD system, including some preliminary results. Finally, in chapter 8, I will discuss possible future improvements.

1.3 Author Contribution

I can separate my research into two parts.

The first part of my research, the demonstration of MDIQKD coexisting with classical communication (mentioned in chapter 5), was carried out by several different lab members at the University of Calgary, Canada. Wolfgang Tittel devised and supervised the experiment.

Raju Valivarthi taught me the experimental setup. Raju Valivarthi, Kim Owen, Caleb John and I performed the measurement and analysed the data with the help of Daniel Oblak and Qiang Zhou. Raju Valivarthi and I simulated the performance of the system. I also helped Wolfgang to write the manuscript of this investigation along with Daniel Oblak, Qiang Zhou, Raju Valivarthi, Kim Owen and Caleb John.

The second part of my research was carried out in the QuTech, Technical University of Delft, Netherlands. The new MDIQKD system was developed over the past year (details are mentioned in chapter 6). Wolfgang Tittel supervised the work. I discussed the specifications and the designs of the new electronic boards with Raymond Vermeulen, an Electronics Engineer at QuTech. Caleb John was part of the initial discussions and Jorge Marques joined in the end. I tested and characterised the electronic boards designed by Raymond Vermeulen. Raymond and I iterated the designing and testing for a few times in order to meet out experimental requirements. In addition, I characterised the optical components for different wavelengths and Jorge Marques performed the stability measurements. I also helped Jorge Marques to stabilise the frequencies of the lasers. I furthermore wrote the VHDL code for FPGA programming, and Jorge Marques wrote the codes that allow communication between various subsystems and the computer. Jorge and I tested our final setup, characterised the qubit states and performed the Hong-Ou-Mandel (HOM) measurements together.

Chapter 2

Background

2.1 Basic concepts

2.1.1 Qubits

The qubit is the basic unit of quantum information. It can be represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

where $|0\rangle$ and $|1\rangle$ are orthogonal quantum states with complex amplitudes α and β, and $|\alpha|^2$ and $|\beta|^2$ are the probabilities of finding the qubit in the state $|0\rangle$ and $|1\rangle$, respectively. The possibility of a qubit to exist in a superposition of quantum states is one of the main reasons that quantum information processing has remarkable advantages over its classical counterpart.

Quantum Key Distribution (QKD) is generally implemented using photonic qubits. Quantum states in these qubits are created using different modes (degrees of freedom) of a photon, namely, polarisation, temporal, spectral and spatial modes. Among these, polarisation and temporal modes are the most commonly used.

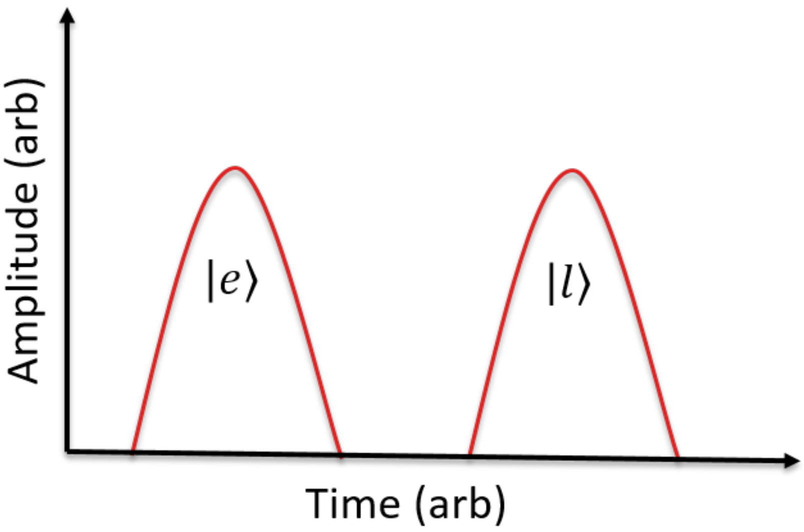


Figure 2.1: Temporal mode qubits. $|e\rangle$ and $|l\rangle$ are early and late temporal modes respectively.

2.1.2 Preparation and measurement of time-bin qubits

For all implementations in the thesis, we use temporal mode qubits (as shown in fig 2.1), also referred to as time-bin qubits, which have been shown to be well suited for fibre-based communication [43]. These qubits are typically prepared using an unbalanced Michelson or unbalanced Mach Zehender interferometer. The word "unbalanced" refers to a path-length difference that exceeds the coherence length of the photons. A photon at the output of these interferometers emerges in a superposition of having taken both short and long paths. An alternative method of preparing time-bin qubits is to use an intensity modulator and tailoring the output from a coherent cw laser into early and late temporal modes. A phase inducing element, a phase modulator, can be used to create a phase difference between early and late time-bins. Consequently, the state is written as $|\psi\rangle = \alpha|e\rangle + e^{i\phi}\beta|l\rangle$, where $|e\rangle$ and $|l\rangle$ are early and late time-bins. Time-bin qubits are measured by using an unbalanced Mach Zehender or Michelson interferometer, which is similar to that used for qubit preparation.

2.1.3 Bell states

A pure bi-partite state $|\psi_{AB}\rangle$ shared between two parties Alice (A) and Bob (B) is entangled if it cannot be expressed as a tensor product of the states of the individual parties $|\psi_A\rangle$ and $|\psi_B\rangle$, i.e ($|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$). The four maximally entangled Bell state given below are important examples for bipartite entangled states.

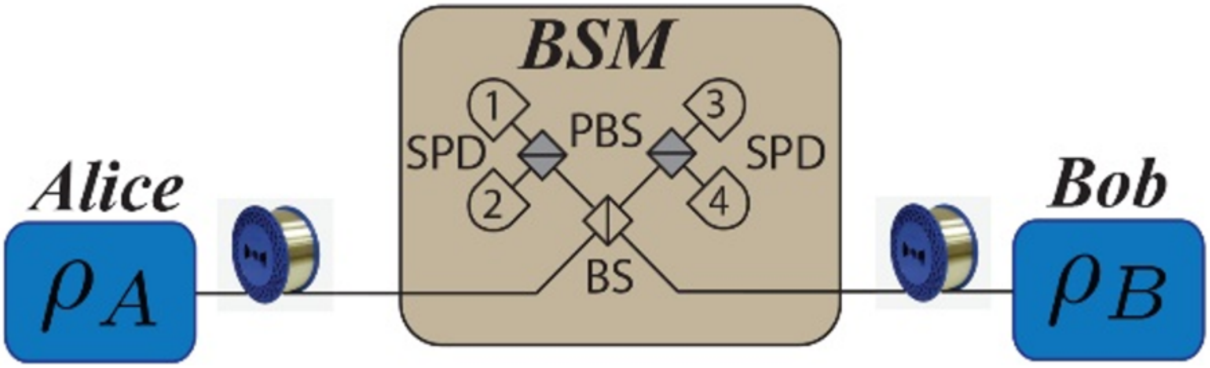
$$|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \tag{2.2}$$

$$|\psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \tag{2.3}$$

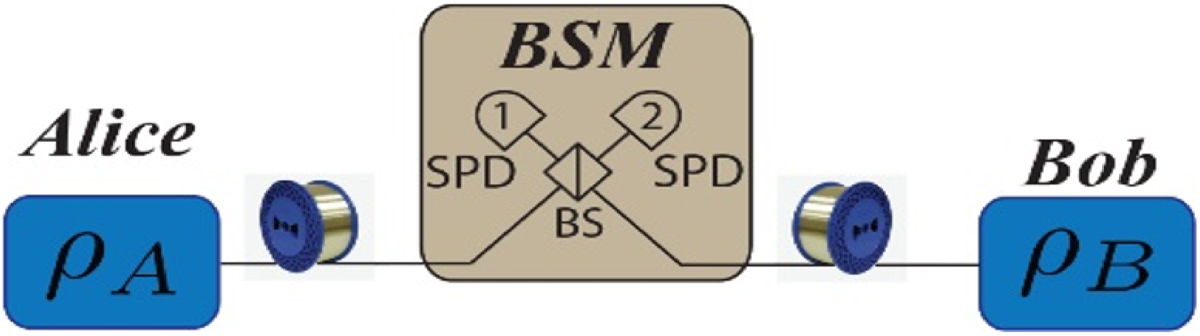
2.1.4 Bell-State Measurement

Bell state measurements are vital for quantum communication protocols such as entanglement swapping [44], quantum teleportation [45], quantum repeaters [46], some QKD protocols [29] and also in linear optics quantum computing. A BSM results in the projection of two qubits onto one of the four Bell states. For photons, BSM is generally implemented using a beam splitter followed by measurement devices that can distinguish the orthogonal modes used for qubit encoding. Common BSM setups for time-bin qubits and polarisation qubits are shown in fig 2.2.

Assuming a Bell state with one photon per input, the beam splitter transformation leads to



(a) Bell state measurement setup for polarisation qubits.



(b) Bell state measurement setup for time-bin qubits.

Figure 2.2: Experimental setups used to perform BSMs for a) polarization qubits and b) time-bin qubits. Density matrices ρ_A and ρ_B characterize the states of the photons emitted by Alice and Bob, respectively. Optical components: beam splitter (BS) and single photon detectors (SPD). The figure is reprinted with permission from [1].

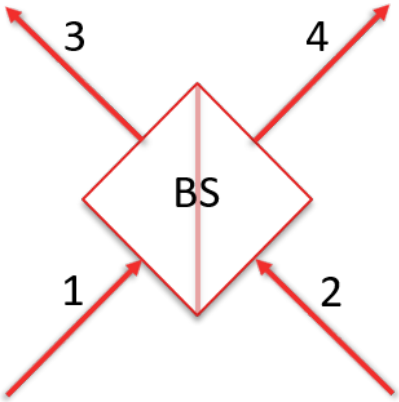


Figure 2.3: Beam splitter. 1,2 and 3,4 are input and output modes, respectively.

$$
\begin{aligned}
|\phi^{\pm}\rangle_{12} =& \frac{1}{\sqrt{2}}(|00\rangle_{12} \pm |11\rangle_{12}) \\
&\rightarrow \frac{i}{2}(|00\rangle_{33} + |00\rangle_{44} \pm |11\rangle_{33} \pm |11\rangle_{44}) \\
|\psi^{+}\rangle_{12} =& \frac{1}{\sqrt{2}}(|01\rangle_{12} \pm |10\rangle_{12}) \\
&\rightarrow \frac{i}{2}(|01\rangle_{33} + |01\rangle_{44}) \\
|\psi^{-}\rangle_{12} =& \frac{1}{\sqrt{2}}(|01\rangle_{12} - |10\rangle_{12}) \\
&\rightarrow \frac{i}{2}(|10\rangle_{34} - |01\rangle_{34})
\end{aligned}
\tag{2.4}
$$

where labels 1,2 and 3,4 are input and output spatial modes (as shown in fig 2.3), respectively. It can be noted that $|\phi^{+}\rangle$ and $|\phi^{-}\rangle$ result in coincidences of photons in states 0 and 1 in the same output of the beam splitter. Therefore $|\phi^{+}\rangle$ and $|\phi^{-}\rangle$ can not be distinguished. Also, it is evident from eq 2.4 that coincidences of photons in states 0 and 1 in the same output port of beam splitter indicate a projection onto $|\psi^{+}\rangle$, whereas coincidence of photons in states 0 and 1 in different output ports of the beam splitter results in projection onto $|\psi^{-}\rangle$. As a result, only two out of the four Bell states can be unambiguously distinguished, limiting the efficiency to 50%, which is the maximum efficiency of a BSM with linear optics and no auxiliary photons [47]. Note that the use of auxiliary photons can improve the efficiency. It is also worth emphasizing that the BSM efficiency can be increased to 100% using a CNOT gate.

2.2 Quantum Key Distribution

One of the most mature applications of quantum information is quantum key distribution (QKD). QKD allows two remote users to distribute secret keys based on the laws of quantum mechanics. Since the invention of QKD in 1984 by Bennett and Brassard [16], there have been many lab and real-world demonstrations. In the following section, I briefly discuss the original BB84 protocol.

1. **Qubits preparation, distribution and measurement:** Alice randomly prepares qubits in eigenstates of Z and X with probabilities p_Z and p_X. These eigenstates are $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$, where $|+\rangle$ and $|-\rangle$ are $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, respectively; they are sometimes referred to as BB84 states. The states $|0\rangle$ and $|+\rangle$ correspond to bit '0' and $|1\rangle$ and $|-\rangle$ correspond to bit '1'. Photons, used as qubit carriers are sent to Bob using a quantum channel such as an optical fibre or a free-space channel. Bob measures the photons randomly in the Z and X bases. After the measurement, he associates measurement results to bit values, as described above, and keeps them together with the respective basis information.

2. **Basis Reconciliation:** Alice and Bob also share an authenticated public channel for classical communication. Bob uses this channel to broadcast his measurement basis choices. Alice compares qubit preparation bases and measurement bases and directs Bob to keep only those bit values (measurement results) for which qubit preparation bases and measurement bases are the same. The left-over measurement results are used for further processing.

3. **Parameter estimation:** Ideally, at this point, Bob's bit values exactly match with what Alice prepared. However, imperfections in the preparation and measurement of the qubits, decoherence in the distribution channel, or Eve trying to gain information about the qubits can cause a mismatch. Alice and Bob, therefore, reveal some subset of their bits for parameter estimation. Please note that in most of the QKD experiments, results from the Z basis are used for key distillation and results from the X basis for parameter estimation. They estimate the number of mismatched bits and the number of matched bits. The ratio of the mismatched bits to the total number of bits is the quantum bit error rate (QBER), denoted as e^X which can be used to bound the maximum amount of information that may have leaked out during the key distribution.

4. **Classical post-processing:** Provided the QBER is below 11%, Alice and Bob use the rest of their bits to distill the secret key. Alice hashes her bit string into a tag and transmits it to Bob together with the hash, for error correction. Finally, the users perform privacy amplification through universal hashing resulting in the secret key.

The final secret key rate is given by

$$S \geq Q^Z - Q^Z h_2(E^X)) - fQ^Z h_2(E^Z) \tag{2.5}$$

where Q^Z is the probability of obtaining a detection per qubit in the Z basis (also referred to as gain), $h_2(x)$ is binary entropy function given by $h_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$, E^Z is the QBER in the Z basis, E^Z is QBER in the Z basis, E^X is the QBER in the X basis, f is the error correction efficiency. Please note that the first term in eq 2.5 is the total gain, the second term is the information gained by Eve during qubit transmission and the last term indicates information loss during the error-correction.

2.3 Side-channel attacks

Even though theoretical proofs of QKD offer complete information security, implementations may not follow all the idealistic assumptions of the proofs. Exploiting, and sometimes even causing this difference, Eve can attack the QKD systems.

2.3.1 Attacks on sources

2.3.1.1 Trojan horse attack

In many QKD systems, intensity modulators and phase modulators are employed to prepare qubits. If Eve can inject intense light into Alice's system, the effect of the modulators is also stamped on this light. She can analyse the reflected light and gain complete information about the qubits prepared by Alice. Hence Eve can obtain complete information about the key. A possible implementation of the Trojan horse attack is shown in fig 2.4.

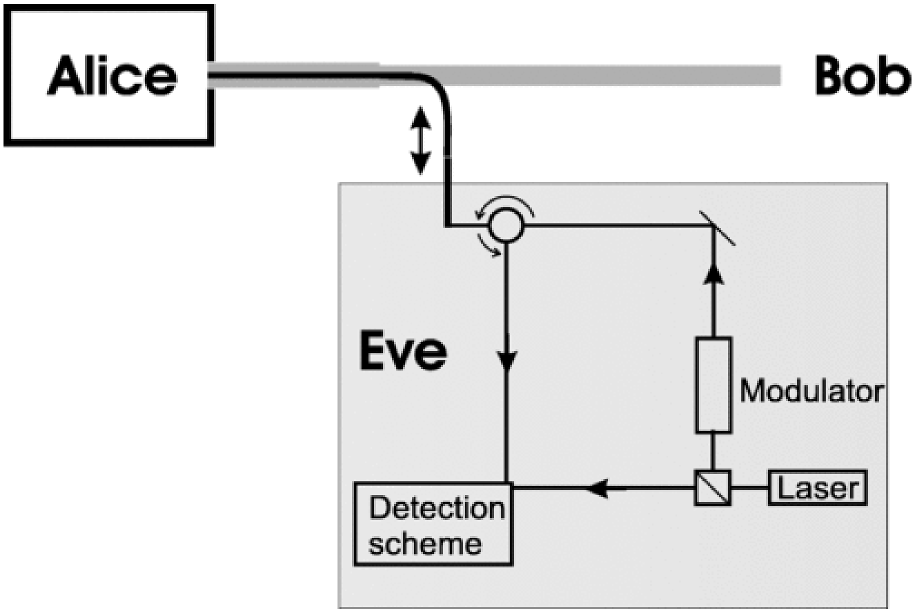


Figure 2.4: Eve occupies part of the quantum channel and tries to gain information about Alice's qubits by injecting light into her system. She compares the modulated light reflected from Alice's system with unmodulated light using a suitable detection scheme. The figure is reprinted with permission from [2].

The Trojan horse attack can be prevented by using optical filters and isolators at the exit of Alice's system. Also, incoming light to Alice's system can be monitored using photodetectors. Detailed countermeasures to prevent the Trojan horse attacks are presented in [48].

2.3.1.2 Photon number splitting (PNS) attack

In most QKD demonstrations, weak coherent pulses are used to prepare qubits instead of ideal single-photon sources. They are described by

$$|\sqrt{\mu}e^{i\theta}\rangle = e^{\frac{\mu}{2}} \sum_{n=0}^{n=\infty} \frac{(\sqrt{\mu}e^{i\theta})^n}{\sqrt{n}} |n\rangle \tag{2.6}$$

where μ is the mean photon number, θ is the phase and $|n\rangle$ is the fock state with n photons. Therefore, when preparing qubits, Alice may encode quantum information into many photons redundantly, and Eve can, in principle, use multiphoton emissions to measure the qubit state without causing the errors. To do so, Eve performs a non-demolition measurement that reveals the number of photons. Whenever a qubit is encoded into a single photon, she blocks it, and whenever it is encoded into multiple photons, she keeps one photon in a quantum memory and sends the rest to Bob. Then, she waits for the public basis reconciliation between Alice and Bob, recalls the stored photon from her quantum memory and measures it in the same basis as Bob. To compensate for the extra loss introduced by her action, she replaces the lossy link by a perfect one. Assuming the loss is sufficiently high, Eve ends up with the same key as Bob. This attack is known as the photon-number splitting attack (PNS attack). As first proposed in 2003 [49], PNS attacks can be detected using so-called decoy states. This method became rapidly popular because of the ease of implementation, which is explained in section 2.5.

2.3.2 Attacks on detectors

Even though numerous attacks against the source have been proposed, all of them can be avoided by blocking external light into Alice's system using isolators and filters. However, unlike Alice, Bob needs to allow light coming from Alice, which opens up the possibility for Eve to perform attacks on Bob's system. Several research groups proposed and demonstrated hacking attacks that targeted single-photon detectors (SPDs). Blinding and time-shift attacks are the most well-known attacks; they are discussed below:

2.3.2.1 Blinding attack

This attack has been demonstrated on commercial QKD systems, like Clavis2 from idQ and QPN 5505 from MagiQ technologies [3, 22]. Avalanche photodiodes (APDs) are widely used SPDs in QKD. APDs have two modes of operation, namely the Geiger mode and the linear mode [50]. In Geiger mode, the APD is reverse biased above the breakdown voltage to detect a single-photon. This results in a detection signal, a 'click'. In the linear mode, it is operated below the breakdown voltage such that the current created by the APD, I_{APD}, is proportional to the incident optical power, P_{opt}. If the input power is picked correctly, then the electrical output pulse may also create a 'click' after passing the usual signal conditioning electronics. However, if the signal is too small, it will not be detected. Utilising this fact and causing the detectors, by shining a strong light on them to operate in the linear mode, Eve can completely control the clicks of Bob's detectors and ends up with the same raw key as Bob without leaving any trace of her presence (see fig 2.5). More precisely, Eve measures the qubit from Alice in a random basis using a similar setup as Bob. Then, she resends the detection result to Bob using a bright pulse instead of a single-photon. She tailors the intensity of the pulse in such a way that Bob will get a click only when he chooses the same basis as her. If Bob chooses a different basis, the pulse does not result in a click. Hence, Eve establishes the same raw key as Bob and, subsequently, the secret key.

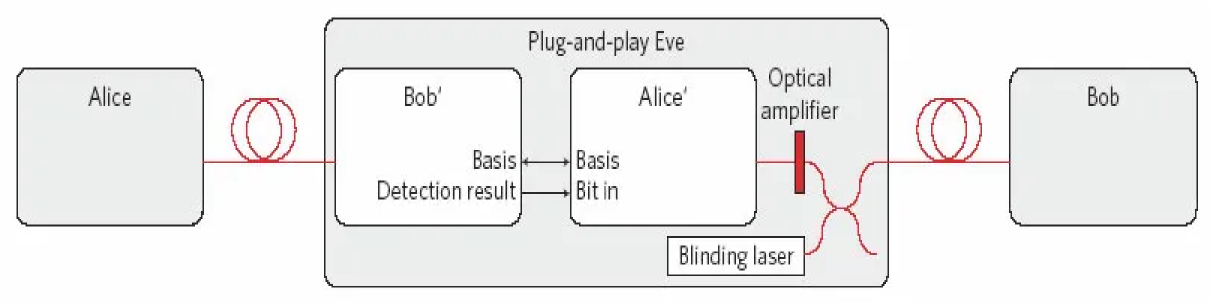


Figure 2.5: A schematic of the blinding attack using intercept-resend. The figure is reprinted with permission from [3].

The attack has been demonstrated not only for APDs but also for superconduction nanowire single-photon detectors (SNSPDs) [51].

Various countermeasures have been proposed, such as including a photodetector at the entrance of Bob's system to monitor the classical power and modifying the electrical circuits in the detector [23]. However, the effectiveness of these countermeasures is questionable [22].

2.3.2.2 Time-shift attack

In the security proofs of QKD, it is often assumed that the detectors have the same detection efficiencies. However, this assumption is questionable and opens up the possibility for eavesdropping. Indeed, a hacking attack known as the ”time-shift attack” has been proposed [52, 53] and demonstrated [4].

Eve can launch the time-shift attack as follows. Let us assume that the detectors used in the experiments have built-in calibration programs to set the activation times. As the calibrations run independently, activation times are often different, causing a mismatch in the detection efficiencies that varies as a function of time. Figure 2.6 shows the detector efficiencies of two different detectors for various time-shifts. Eve chooses two points, namely A and B (as shown in figure 2.6), where the mismatches in the detection efficiencies are large. Then, she shifts the arrival time of the qubits from Alice randomly to one of these two times using an optical variable delay line. This allows her to almost certainly predict the detector that clicked, and hence the key bit. The experimental demonstration of the time-shift attack is presented in [4]. Later, IdQuantique proposed and employed a countermeasure for the attack by randomly changing the detector efficiencies.

In summary, many side-channel attacks have been proposed and demonstrated that exploit vulnerabilities of imperfect QKD systems. One way to overcome such attacks is to implement countermeasures for each attack. However, it is still possible that Eve can come up with more sophisticated attacks in future, making the QKD systems again insecure. A better way possible is to use the QKD protocols that are inherently robust against all of the attacks. One such protocol is device-independent quantum key distribution (DIQKD), which is explained in section 2.4.1. Another protocol is measurement-device-independent quantum key distribution (MDIQKD), which is secure against all detector side-channel attacks, explained in section 2.4.2.

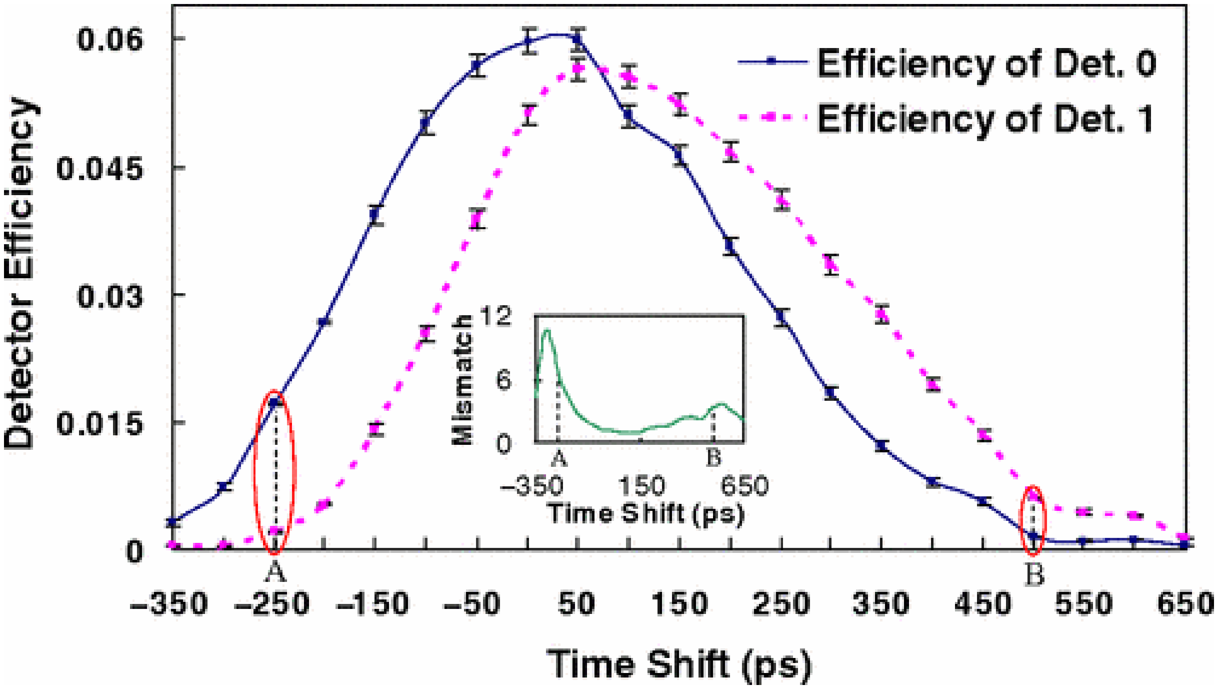


Figure 2.6: Mismatch in the detector efficiencies for various time-shifts. Blue and magenta lines represent the detection efficiencies of the detector 0 and 1, respectively. A and B are the points chosen by Eve to perform the time-shift attack. The inset shows the the mismatch in the detector efficiencies of det 0 and det 1, defined as $max[d_0/d_1, d_1/d_0]$. The figure is reprinted with permission from [4].

.

2.4 Secure protocols against side-channel attacks

2.4.1 Device-independent quantum key distribution (DIQKD)

In a practical scenario, quantum devices used in the experiment may have uncontrolled side channels or may be untrusted because Eve might have fabricated them. However, device-independent quantum key distribution (DIQKD) protocols allow Alice and Bob to distil a secret key without making assumptions about the working of the quantum devices [5, 54, 55, 56, 57]. They treat the devices as black boxes which produce classical outputs for classical inputs. The important assumptions of the DIQKD are:

- The physical locations of Alice and Bob are secure and no unwanted signals, which may be accessible to Eve, leak to the outside.

- Alice and Bob have random number generators (preferably quantum) and trusted classical devices to store and process the classical outputs produced by the quantum devices.

In DIQKD, Alice and Bob test non-local correlations between the outputs of the devices by violating a Bell inequality [57]. A brief description of a DIQKD protocol is as follows. Alice and Bob share a quantum channel consisting of a source that emits pairs of particles in an entangled state ρ_{AB}. Alice (Bob) has a device A (B) which takes classical inputs A_0, A_1 and A_2 (B_1 and B_2) and produces classical outputs $a_i \in \{+1, -1\}$ ($b_j \in \{+1, -1\}$). The raw key is extracted from $\{A_0, B_1\}$, and the QBER is defined as $Q = P(a \neq b|01)$. Alice and Bob use measurements of A_1, A_2, B_1 and B_2 to estimate the non-classical correlation using the CHSH-inequality [58] given by

$$S = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle \tag{2.7}$$

where $\langle a_i b_j \rangle$ is given by $P(a = b|ij) - P(a \neq b|ij)$ and $P(ab|ij)$ is the probability of observing the pair of outcomes a, b for inputs $A_0 = i, B_1 = j$. If the value of the CHSH-inequality $S \leq 2$ then Alice and Bob share classical correlation which makes it possible for Eve to attack the system. DIQKD is possible only if $2 < S \leq 2\sqrt{2}$, i.e. if Alice and Bob have quantum correlations between their outputs. Eve has zero correlation with Alice's and Bob's systems when $S = 2\sqrt{2}$. The secret key rate is given by

$$r \geq 1 - h(Q) - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) \tag{2.8}$$

Figure 2.7 compares the secret key rate for the entanglement-based version of BB84 with device-independent QKD. A detailed description of a DIQKD protocol is presented in [5, 54]

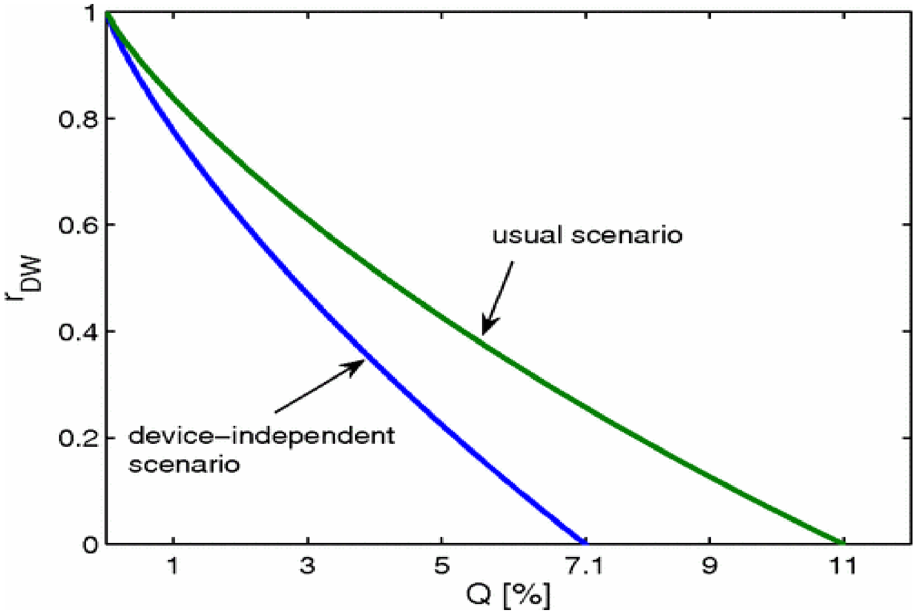


Figure 2.7: Secret key rate as a function of QBER for the entanglement-based version of BB84 and for device-independent QKD. The figure is reprinted with permission from [5].

2.4.2 Measurement-device-independent quantum key distribution (MDIQKD)

Even though loophole-free violations of Bell inequalities have been demonstrated [25, 26, 59, 60], DIQKD has not been experimentally realised. Moreover, DIQKD is still considered impractical due to low secret key rates, a shorter distance of only a few km, and the requirement for detectors with high detection efficiencies. Therefore, instead of trying to avoid all side-channel attacks, several research groups investigated protocols that prevent the most vulnerable components, i.e. SPDs, against attacks. MDIQKD is one such protocol. It closes all security loopholes of detectors.

In MDIQKD, unlike in the BB84 protocol, Alice and Bob both prepare qubits and send them to an untrusted third party, Charlie, who performs Bell state measurement (as described in section 2.1.3). It is worth noting that Charlie can be an eavesdropper controlling the entire measurement, including the SPDs. Still, he cannot gain any information about the qubits without causing errors. A detailed discussion of the protocol is presented in section 3.1.

2.5 Decoy states

First, let us look at some relevant equations and then the essence of the decoy states. A coherent state with mean photon number μ is given by equation 2.6. After phase-randomisation it becomes

$$\frac{1}{2\pi}\int_{\theta=0}^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}| d\theta = \sum_{n=0}^{n=\infty} e^{-\mu}\frac{\mu^n}{n!}|n\rangle\langle n|. \tag{2.9}$$

The gain Q_μ for the phase-randomised coherent state is given by

$$Q_\mu = \sum_{n=0}^{n=\infty} Y_n e^{-\mu}\frac{\mu^n}{n!} = 1 + Y_0 - e^{-\eta\mu} \tag{2.10}$$

where Y_0 are the detections due to dark counts and stray light, and Y_n is the yield of n photons given by

$$Y_n = 1 - (1-\eta)^n + p_{dark} \tag{2.11}$$

where η is total efficiency and given by

$$\eta = t_{ab}\eta_d \tag{2.12}$$

where t_{ab} is the transmission efficiency from Alice to Bob and η_d is the detector efficiency. Using the equations 2.10 and 2.11, Q_μ can be written as

$$Q_\mu = 1 + Y_0 - e^{-\eta\mu} \tag{2.13}$$

The quantum bit error rate (QBER) E_μ is given by

$$E_\mu Q_\mu = \sum_{n=0}^{n=\infty} e_n Y_n e^{-\mu}\frac{\mu^n}{n!} \tag{2.14}$$

where e_n is the QBER for an n-photon signal given by

$$e_n = \frac{(e_{detector}(1-(1-\eta)^n) + e_0 Y_0)}{Y_n} \tag{2.15}$$

where $e_0 = \frac{1}{2}$ is QBER for the vacuum. Using equations 2.14 and 2.15, E_μ can be written as

$$E_\mu Q_\mu = e_0 Y_0 + e_{detector}(1 - e^{-\eta\mu}) \tag{2.16}$$

Essence of the decoy states: Let us imagine that Alice randomly prepares a signal state and a decoy-state and send them over to Bob via a quantum channel. These states have the same characteristics in all the degrees of freedom. When Eve performs a QND measurement on the state sent by Alice, she gets to determine the number of photons in the state but not the mean photon number, i.e whether the state is a signal or a decoy. Hence, she can only act in the same manner on signal and decoy states, and

$$Y_n(signal) \quad = Y_n(decoy) \quad = Y_n \tag{2.17}$$

$$e_n(signal) \quad = e_n(decoy) \quad = e_n \tag{2.18}$$

Importantly, this allows Alice and Bob to distil a secret key considering the detections at Bob's corresponding to single-photon emissions from Alice, i.e. Y_1 and e_1. These parameters can be accurately estimated if Alice and Bob use an infinite number of decoy states. As it is practically impossible to do so, they can use fewer decoy states for the estimation. In [61], it is shown that the estimated parameters, Y_1 and e_1, using only two weak decoy states and a signal state, are close to the values with the infinite decoy states. Furthermore, it is also shown that one vacuum and one weak decoy-state is optimal decoy states among the two-decoy-states protocols. The single-photon yield Y_1 for the vacuum + one weak decoy-state protocol is given by

$$\underline{Y_1} \geq \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{2.19}$$

where $\underline{Y_1}$ is the lower bound for the single photon yield, μ is the mean photon number of the signal state, ν is the mean photon number of the weak decoy state, Q_μ is the gain for the signal state, Q_ν is the gain for the weak decoy state and Y_0 is the noise probability. A lower bound to the single-photon gain $\underline{Q_1}$ is thus given by

$$\begin{aligned} \underline{Q_1} &= \mu e^{-\mu} \underline{Y_1} && (2.20) \\ \underline{Q_1} &\geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) && (2.21) \end{aligned}$$

and the single-photon error rate is given by

$$\overline{e_1} \leq \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{\underline{Y_1}\nu} \tag{2.22}$$

where $\overline{e_1}$ is the upper bound for the single-photon error rate, E_ν is the QBER for signal states, e_0 is the QBER for the vacuum, Y_0 is the noise probability, $\underline{Y_1}$ is the lower bound for the single photon yield, and ν is the mean photon number of the weak decoy state. The secret key rate given by equation 2.23 can then be re-written as

$$S \geq \underline{Q_1^Z} - \underline{Q_1^Z} h_2(\overline{e_1^X})) - fQ^Z h_2(E^Z). \tag{2.23}$$

Figure 2.8 shows the comparison of the secret key rate for the BB84 protocol with and without applying decoy-state methods. It can be noted that the maximum secure distance achieved without decoy states is about 30 km, whereas it is over 140 km with decoy states [7].

Further, several research groups investigated tighter bounds for $\underline{Y_1}$ and $\overline{e_1}$, in the protocols with one, two and three-decoy states to obtain higher secret key rate [61, 62]. As well, all the earlier decoy-state analysis assumed that the secret key is distilled using an infinite number of detections at Bob also referred to as an asymptotic case. However, there is only a finite amount of resources available for Alice and Bob to distil the key. In subsequent years, the effect of the number of decoy-states on the secret key rate has been re-investigated considering finite resources [61, 63, 64, 65, 66].

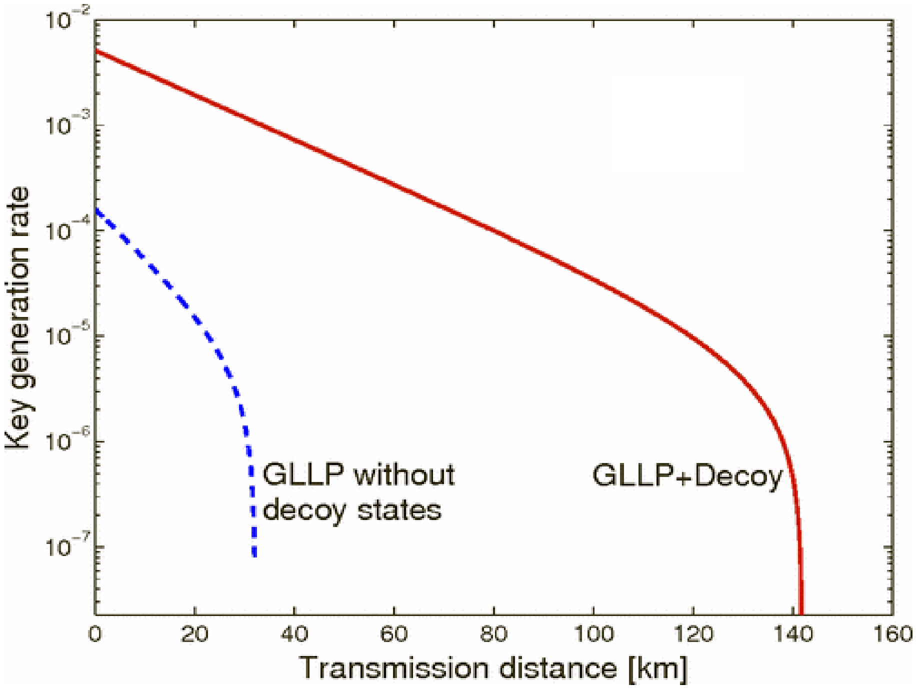


Figure 2.8: Secret key rate comparison with and without using decoy states. GLLP denotes the secret key rate for the security proof given by Gottesman, Lo, Lutkenhaus and Preskill. The figure is produced using the parameters of the experiment performed by Gobby, Yuan and Shields (GYS) [6]. The figure is reprinted with permission from [7].

Chapter 3

Measurement-Device-Independent Quantum Key Distribution (MDIQKD)

Measurement-device-independent quantum key distribution (MDIQKD) is immune to all side-channel attacks targetting the detectors. A schematic of the setup is shown in fig 3.1. In this section, I will discuss the MDIQKD protocol.

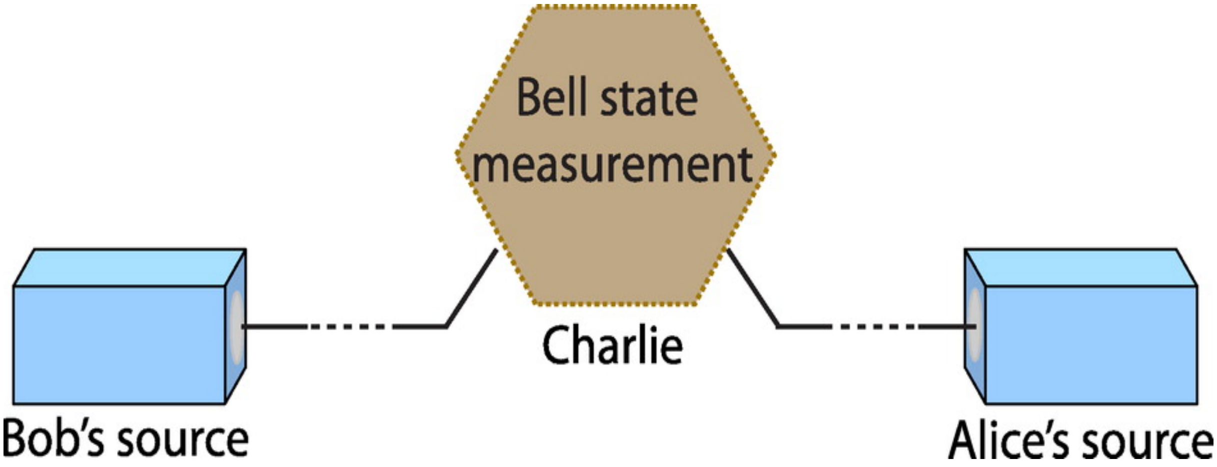


Figure 3.1: Schematic of the setup to implement the MDI-QKD protocol. The figure shows two qubit sources labelled as Bob's source and Alice's source that send qubits through a quantum channel to Charlie, an untrusted third party, who performs a BSM. The figure is reprinted with permission from [8].

3.1 Protocol

The protocol includes six steps, namely qubit preparation, distribution, measurement, sifting, parameter estimation and classical post-processing. The first three steps require quantum communication, while the rest are classical.

1. **State Preparation:** Alice (Bob) randomly prepares one of the BB84 qubit states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$ by choosing a mean photon number $q_a \in \{\mu_a, \nu_a, \omega_a\}$ ($q_b \in \{\mu_b, \nu_b, \omega_b\}$), a basis α (β) $\in$ {X, Z}, and a random bit $r \in \{0, 1\}$ with probability $P_{q_a} \in \{P_{\mu_a}, P_{\nu_a}, P_{\omega_a}\}$ ($P_{q_b} \in \{P_{\mu_b}, P_{\nu_b}, P_{\omega_b}\}$). Here, μ_a (μ_b) is a signal state and $\{\nu_a, \omega_a\}$ ($\{\nu_b, \omega_b\}$) are two decoy states. The random bit 0 (1) is encoded as $|0\rangle$ ($|1\rangle$) state in the Z basis and $|+\rangle$ ($|-\rangle$) state in the X basis.

2. **Distribution:** Alice and Bob send their qubits to Charlie, an untrusted third party, via two independent quantum channels.

3. **Measurement:** Charlie ideally performs a Bell state measurement (BSM), in which he projects the qubits from Alice and Bob onto one of the four Bell states, and announces the outcome using an authenticated public channel. Please note that it is sufficient to project only onto one Bell state and that making any other measurement does not affect the security of the protocol - only the secret key rate.

4. **Sifting:** Whenever Charlie announces a successful Bell state measurement, Alice and Bob discuss their mean photon number and basis settings using the public channel. For each Bell state k, Alice (Bob) makes sets of $Z_k^{q_a,q_b}$ and $X_k^{q_a,q_b}$. Here Z and X are the basis settings and q_a and q_b denote the used mean photon number for the Bell state measurement k. Alice and Bob repeat the protocol until $Z_k^{q_a,q_b} \geq N_k^{q_a,q_b}$ and $X_k^{q_a,q_b} \geq M_k^{q_a,q_b}$ where $N_k^{q_a,q_b}$ and $M_k^{q_a,q_b}$ is the desired block size for the secret key generation and parameter estimation. As the quantum bit error rate (QBER) in the X basis is 25% for the implementation of MDIQKD using weak coherent pulses, the

results in the X basis, $X_k^{q_a,q_b}$, are used for parameter estimation and the results in the Z basis, $Z_k^{q_a,q_b}$, are used for secret key distillation. Next, Bob flips his bits depending on the Bell state obtained to correlate his bits to those of Alice. Afterwards, Alice and Bob perform parameter estimation followed by classical post-processing.

5. **Parameter estimation:** After sifting, Alice and Bob perform parameter estimation to quantify the amount of information leaked to an eavesdropper. They reveal a subset of $Z_k^{q_a,q_b}$ to estimate the total gain for signal states in the Z basis, $Q_{Z,k}^{\mu_a,\mu_b}$, and the QBER for signal states in the Z basis, $E_{Z,k}^{\mu_a,\mu_b}$. If the QBER is more than 11%, then they abort the protocol. If not, they estimate the parameters $\underline{q}_{Z,k}^{1,1}$ and $\overline{e}_{X,k}^{1,1}$ using the decoy-state analysis where $\underline{q}_{Z,k}^{1,1}$ is the lower bound for the single-photon gain in the Z basis and $\overline{e}_{X,k}^{1,1}$ is the upper bound for the single-photon error rate in the X basis.

6. **Classical Post-processing** Alice and Bob use the rest of $Z_k^{q_a,q_b}$ for Error Correction (EC). Alice hashes her string into a tag and transmits it to Bob together with the hash, for error correction. If the two tags coincide, the users perform privacy amplification through universal hashing and draw the final key [67].

The secret key rate $R_{k(inf)}$ is given by

$$R_{k(inf)} \geq \underline{q}_{Z,k}^{1,1}(1 - h(\overline{e}_{X,k}^{1,1})) - f_{EC} Q_{Z,k}^{\mu_a,\mu_b} h(E_{Z,k}^{\mu_a,\mu_b}) \tag{3.1}$$

where $\underline{q}_{Z,k}^{1,1}$ is the lower bound for the single-photon gain in the Z basis, $h_2(x) = -x\ log_2(x) - (1-x)\ log_2(1-x)$ is the binary Shannon entropy function, $\overline{e}_{X,k}^{1,1}$ is the upper bound for the single-photon error rate in the X basis, f_{EC} is the efficiency of error correction, $Q_{Z,k}^{\mu_a,\mu_b}$ is the total gain for signal states in the Z basis, $E_{Z,k}^{\mu_a,\mu_b}$ is the QBER for signal states in the Z basis and the subscript "inf" denotes the assumption of infinitely long keys. The parameters $\underline{q}_{Z,k}^{1,1}$

and $\overline{e}_{X,k}^{1,1}$ are given by

$$\begin{aligned}\underline{q}_{Z,k}^{1,1} \geq &\frac{\mu_a\mu_b e^{-(\mu_a+\mu_b)}}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)} \\ &\times [(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)(Q_{Z,k}^{\nu_a,\nu_b}e^{(\nu_a+\nu_b)}+Q_{Z,k}^{\omega_a,\omega_b}e^{(\omega_a+\omega_b)}-Q_{Z,k}^{\nu_a,\omega_b}e^{(\nu_a+\omega_b)}-Q_{Z,k}^{\omega_a,\nu_b}e^{(\omega_a+\nu_b)}) \\ &-(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)(Q_{Z,k}^{\mu_a,\mu_b}e^{(\mu_a+\mu_b)}+Q_{Z,k}^{\omega_a,\omega_b}e^{(\omega_a+\omega_b)}-Q_{Z,k}^{\mu_a,\omega_b}e^{(\mu_a+\omega_b)}-Q_{Z,k}^{\omega_a,\mu_b}e^{(\omega_a+\mu_b)})]\end{aligned} \tag{3.2}$$

$$\begin{aligned}\overline{e}_{X,k}^{1,1} \geq &\frac{1}{(\nu_a-\omega_a)(\nu_b-\omega_b)\underline{y}_{X,k}^{1,1}} \\ &\times [e^{(\nu_a+\nu_b)}Q_{X,k}^{\nu_a,\nu_b}E_{X,k}^{\nu_a,\nu_b}+e^{(\omega_a+\omega_b)}Q_{X,k}^{\omega_a,\omega_b}E_{X,k}^{\omega_a,\omega_b}-e^{(\nu_a+\omega_b)}Q_{X,k}^{\nu_a,\omega_b}E_{X,k}^{\nu_a,\omega_b}-e^{(\omega_a+\nu_b)}Q_{X,k}^{\omega_a,\nu_b}E_{X,k}^{\omega_a,\nu_b}]\end{aligned} \tag{3.3}$$

where $\underline{y}_{X,k}^{1,1}$ is the lower bound for the single-photon yield in the X basis for Bell state k and given by

$$\begin{aligned}\underline{y}_{X,k}^{1,1} \geq &\frac{1}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)} \\ &\times [(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)(Q_{X,k}^{\nu_a,\nu_b}e^{(\nu_a+\nu_b)}+Q_{X,k}^{\omega_a,\omega_b}e^{(\omega_a+\omega_b)}-Q_{X,k}^{\nu_a,\omega_b}e^{(\nu_a+\omega_b)}-Q_{X,k}^{\omega_a,\nu_b}e^{(\omega_a+\nu_b)}) \\ &-(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)(Q_{X,k}^{\mu_a,\mu_b}e^{(\mu_a+\mu_b)}+Q_{X,k}^{\omega_a,\omega_b}e^{(\omega_a+\omega_b)}-Q_{X,k}^{\mu_a,\omega_b}e^{(\mu_a+\omega_b)}-Q_{X,k}^{\omega_a,\mu_b}e^{(\omega_a+\mu_b)})]\end{aligned} \tag{3.4}$$

If one of the decoy states from Alice (Bob), ω_a (ω_b), is a vacuum state, then ω_a (ω_b) can be set to zero in the equations 3.2 through 3.4. Please note that a similar analysis for two-decoy states has been presented in [68]. Also, $\underline{q}_{Z,k}^{1,1}$ and $\overline{e}_{X,k}^{1,1}$ have been estimated for three decoy states in [69].

Chapter 4

Integration of quantum and classical communication

4.1 Motivation

Since the first introduction of QKD in 1984 [16], there has been a great effort put towards achieving the longer distances [20], increasing the secret key rate [70] and building robust and reliable quantum communication systems [71]. These demonstrations have been conducted using dark fibers. As leasing these fibres is expensive, employing them to establish a quantum communication network is not an economical solution. Therefore, it is highly desirable to integrate quantum communication into the existing classical communication infrastructure. However, the integration of quantum and classical communication over the same fibre is challenging due to the generation of noise photons by strong classical communication, which may mask the quantum data. In the following section, I discuss the physical impairments of the integration considering classical communication within the telecommunication C-band (1530 - 1565nm wavelength).

4.2 Physical impairments

Generation of noise photons due to the interaction between light and an optical fibre is mediated by four different processes: four-wave mixing (FWM), Rayleigh scattering, Brillouin scattering and Raman scattering [12].

4.2.1 Four-wave mixing (FWM)

Four-wave-mixing (FWM) generates photons at new frequencies due to the interaction between two or more pump fields mediated by $\chi^{(3)}$, the third-order non-linear susceptibility. If there are three classical communication channels, i, j and k, with frequencies, f_i, f_j and $f_k (k \neq i, j)$ then FWM can generate a new frequency f_{ijk} that is given by,

$$f_{ijk} = f_i + f_j - f_k \tag{4.1}$$

The power P_{ijk} of the light of frequency f_{ijk} is given by,

$$P_{ijk}(L) = \frac{\eta D^2 \gamma^2 P_i P_j P_k e^{-\alpha L}}{9\alpha^2}[1 - e^{-\alpha L}]^2 \tag{4.2}$$

where P_i, P_j, P_k are powers of the frequencies f_i, f_j, f_k respectively, α is the fibre attenuation coefficient, γ is the fibre non-linearity, L is the length of the fibre, D : is the FWM degeneracy factor. D=6 for the non-degenerate case in which all three frequencies are different and D=3 for the degenerate case where there are only two frequencies. Furthermore, η is the FWM efficiency given by,

$$\eta = \frac{\alpha^2}{\alpha^2 + \beta^2}\{1 + \frac{4e^{-\alpha L} \sin^2 (\Delta\beta L/2)}{[1 - e^{-\alpha L}]^2}\}, \tag{4.3}$$

and $\Delta\beta$ is the phase matching factor given by,

$$\Delta\beta = \beta_{ijk} + \beta_k - \beta_i - \beta_j. \tag{4.4}$$

Finally, $\beta_i, \beta_j, \beta_k$ and β_{ijk} are the propagation constants of the input channels $(i, j$ and $k)$ and the resulting product (ijk). Classical communication channels within the C-band are after combined using dense wavelength division multiplexing (DWDM) systems. These channels are equally spaced with spacings of 50, 100 or 200 GHz. As a result of equal spacing, the FWM product terms fall on the same grid, i.e either on the already used DWDM channel or a neighbouring DMDM channel above or below.

In [9], the FWM noise power generated on the QKD wavelength (or QKD passband) by two adjacent DWDM channels with 0 dBm average power is investigated for various channel spacings, Δf (10 - 1000 GHz). In addition, FWM noise is analysed for two types of fibres, standard single-mode fibre (SSMF) and nonzero dispersion-shifted fibre (NZ-DSF), of different lengths (1 km and 25 km). As can be seen in fig4.1, the FWM power depends on

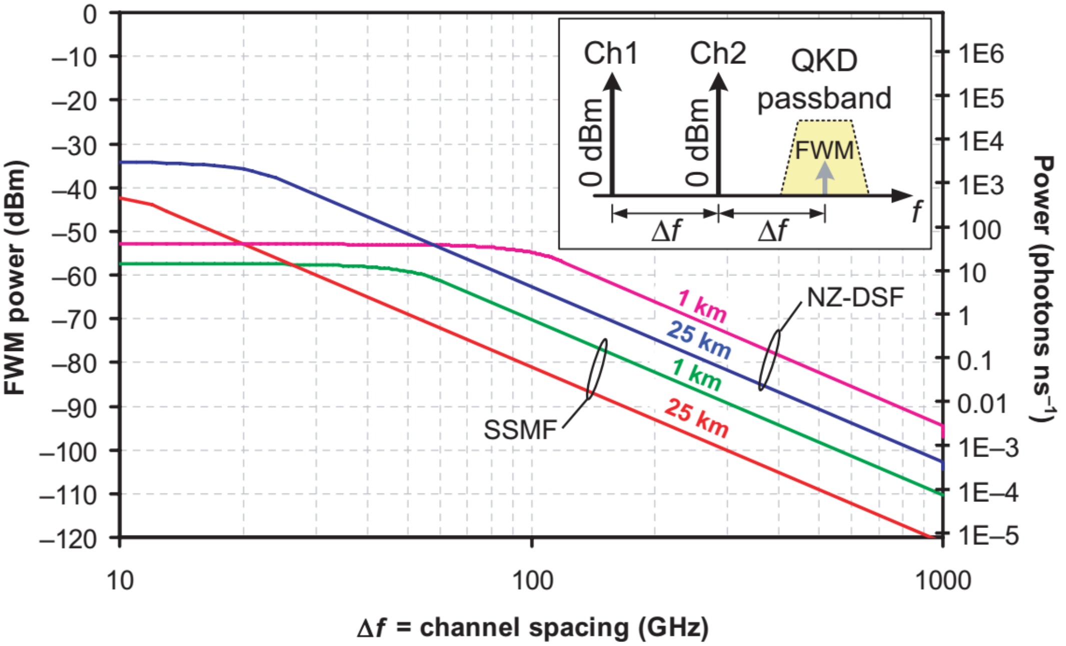


Figure 4.1: Calculation of adjacent channel FWM noise power generated by two 0 dBm cw lasers, plotted as a function of channel spacing for two different fibre types of 1 and 25 km lengths. (SSMF, standard single-mode fibre; NZ-DSF, non-zero dispersion-shifted fibre.) The figure is reprinted with permission from [9].

the length of the fibre, the type of the fibre and mainly on channel spacing. For a channel spacing of 100 GHz, 25 km fibre has less FWM power than 1 km fibre in both types of fibre. Besides, the FWM power in NZ-DSF fibre is higher compared to SSMF fibre for the same length of the fibre. Also note that the FWM power for SSMF for 100 GHz (0.8 nm) channel spacing is ~ -80 dBm. But for similar configurations and channel spacing of 1000 GHz (8 nm) the FWM power is ~ -120 dBm.

In general, photons generated by the FWM are a major source of noise in the integration of quantum and classical communication when a short length of fibre ($<$ 5 km) is used for communication, and the channel spacing among classical and quantum channels is small. Choosing a long fibre($>$25 km) and increasing the channel spacing will effectively decrease the FWM noise.

4.2.2 Rayleigh scattering & Brillouin scattering:

Rayleigh scattering is an elastic process that generates photons at the same frequency as the classical channel frequency. In contrast, Brillouin scattering leads to frequency-shifted photons up to 10 GHz from a classical channel due to acoustic phonons [72]. Also, note that the power in a classical channel can be as high as 0 dBm. Therefore, a quantum channel can not be placed at a frequency that is close ($<$ 10 GHz) to a classical channel as spectral filtering of Rayleigh and Brillouin scattered photons becomes impossible. The question of "how far" can be answered after Raman scattering is discussed, which is the bottleneck for the integration of quantum and classical communication.

4.2.3 Raman scattering

Raman scattering is an inelastic interaction between photons and phonons that generates scattered photons within a wide range of wavelengths, up to 100 nm, below (anti-Stokes scattering) and above (Stokes scattering) the classical communication wavelength [73]. In the case of Stokes-scattering, the difference energy is absorbed by phonons (vibrational modes) resulting in the generation of higher wavelengths. However, in anti-Stokes scattering, phonon energy is transferred to photons resulting in lower wavelengths. The anti-Stokes scattering is less effective than Stokes as it requires vibrational modes to be excited. Therefore, placing the quantum channel in the anti-Stokes scattering region is more favourable compared to the Stokes scattering region. Figure 4.2 shows Raman scattering when the classical channel is at ∼1550 nm.

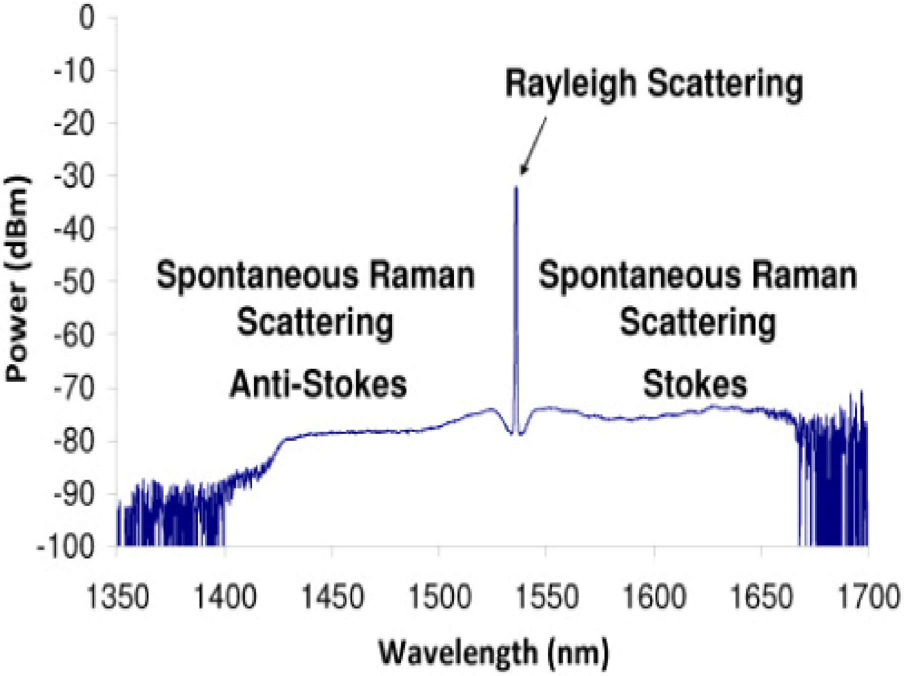


Figure 4.2: Raman and Rayleigh scattering when classical channel with power of -30 dBm is at ∼ 1550 nm.

Raman scattering analysis is assisted by the well-known Raman gain curve, as shown in fig4.3. Raman gain describes the amount of scattering from a pump of frequency f_p into a frequency interval offset by, Δf. It is generally defined by the Raman gain coefficient RGC$(f_p, \Delta f)$. Raman gain can be modelled using either analytical expressions or commercial simulation tools. The intermediate-broadening model is one of the extensively used Raman gain models [73]. It provides an analytic expression that fits the shape of the Raman gain spectrum and the Raman response function of silica fibres with good agreement. The model is based on the convolution of Lorentzian and Gaussian functions that represent multiple vibrational modes. For instance, two peaks on either side of the Raman spectrum

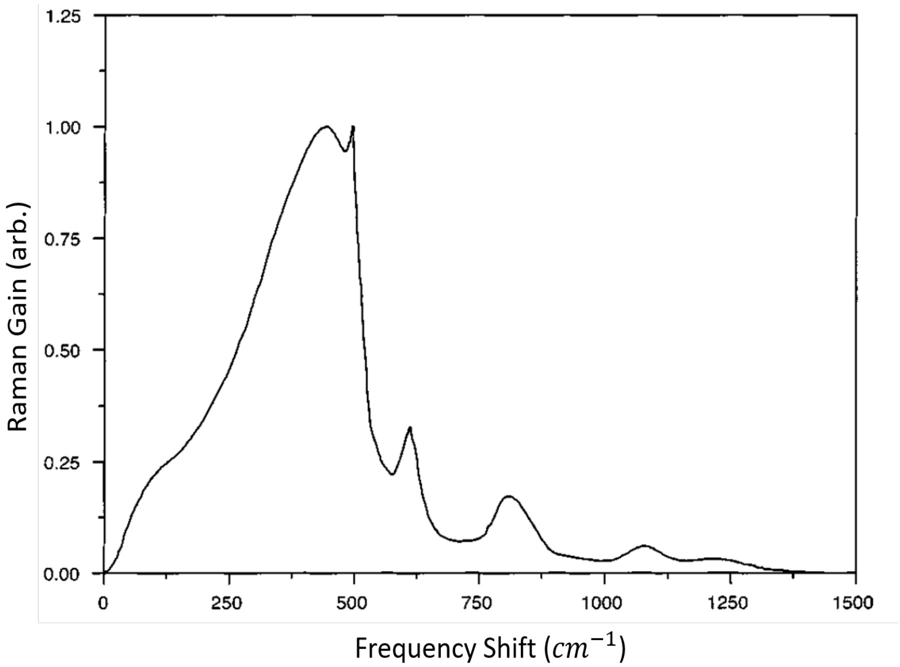


Figure 4.3: Raman gain spectrum. The figure is reprinted with permission from [10].

of silica fibres (around 400 cm^{-1}) correspond to the bending of a Si-O-Si dihedral angle. The Lorentzian peak can be visualized as a physical representation of a different equilibrium value of the dihedral angle [10]. The Raman response function is given by,

$$h_R(t) = \sum_{i=1}^{13} \frac{A_i'}{\omega_{\nu,i}} e^{-\gamma_i t} e^{-\Gamma_i^2 t^2/4} \sin(\omega_{\nu,i})\theta(t) \tag{4.5}$$

The Raman gain function is the Fourier transform of the Raman response function and is given by,

$$s(\omega) = \sum_{i=1}^{13} \frac{A_i'}{2\omega_{\nu,i}} \int_0^{\infty} e^{-\gamma_i t} e^{-\Gamma_i^2 t^2/4} \{\cos[(\omega_{\nu,i} - \omega)t] - \cos[(\omega_{\nu,i} + \omega)t]\} dt, \tag{4.6}$$

where A_i' is amplitude of the i^{th} vibrational mode, $\omega_{\nu,i}$ is the center vibrational frequency for the i^{th} mode, γ_i and Γ_i are Lorentzian and Gaussian mode linewidths, $\theta(t)$ is unit step function and $i = 1, 2, ..., 13$ represent different Gaussian functions, corresponding to different vibrational modes of the fused silica fibres as shown in figure 4.4. The widths and amplitudes of these functions are tabulated in table 4.1.

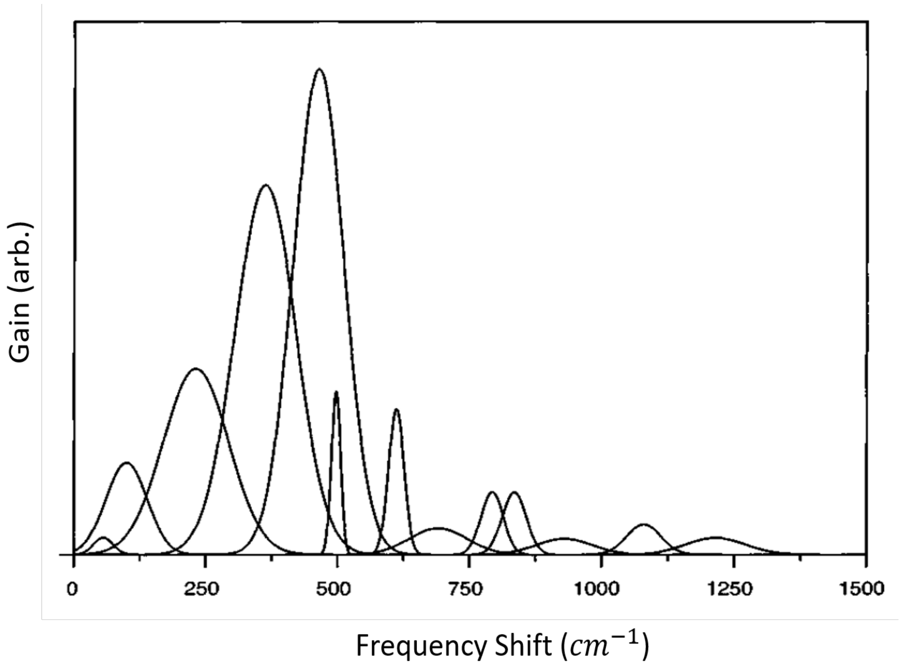


Figure 4.4: Gaussian functions used in the intermediate-broadening model of the Raman gain spectrum. The figure is reprinted with permission from [10]

.

Mode Number, i	Component Position (cm^{-1})	Peak Intensity, A_i	Gaussian FWHM(cm^{-1})	Lorentzian FWHM(cm^{-1})
1	56.25	1.00	52.10	17.37
2	100	11.40	110.42	38.81
3	231.25	36.67	175.00	58.33
4	362.50	67.67	162.50	54.17
5	463.00	74.00	135.33	45.11
6	497.00	4.50	24.50	8.17
7	611.50	6.80	41.50	13.83
8	691.67	4.60	155.00	51.67
9	793.67	4.20	59.50	19.83
10	835.50	4.50	64.30	21.43
11	930.00	2.70	150.00	50.00
12	1080.00	3.10	91.00	30.33
13	1215.00	3.00	160.00	53.33

Table 4.1: Values used in the intermediate broadening model

The amount of Raman scattering into a quantum channel depends on several parameters:

- Average launch power into a classical communication channel.

- Raman scattering coefficient: Also referred to as Raman Gain coefficient(RGC). The RGC depends on the separation between the quantum and classical communication channels and the material properties of the fibre.

- Length of the fibre.

- Relative direction of quantum and classical communication.

Classical communication generates both forward and backscattered Raman photons while propagating. The direction of classical communication relative to quantum communication decides "which"(forward or backward) scattered Raman photons end up at the detectors. The detected Raman photons act as dark counts/ stray counts. There are 3 different schemes to consider:

1. **Co-propagation**: In this instance, classical communication propagates in the same direction as quantum communication resulting in forward scattered Raman photons to end up at the detectors. A schematic of the co-propagating light in the case of MDIQKD is shown in fig 4.5.

   The amount of Raman scattering in the co-propagating case is given by,

   $$P_{co} = P_l \beta \Delta\lambda \frac{(e^{-\alpha_Q L} - e^{-\alpha_C L})}{\alpha_C - \alpha_Q} \tag{4.7}$$

   P_{CO} is the Raman scattered power. $P_{CO} = nhc/\lambda$ where n is the photon scattering rate, h is Planck's constant, c the speed of light, and λ the photon wavelength. P_l is the average launch power into the classical communication channel, β is the Raman scattering coefficient, $\Delta\lambda$ is the bandwidth of the quantum channel, α_Q and α_C are fibre attenuation coefficients for the quantum and classical communication channels, and L is the length of the fibre.

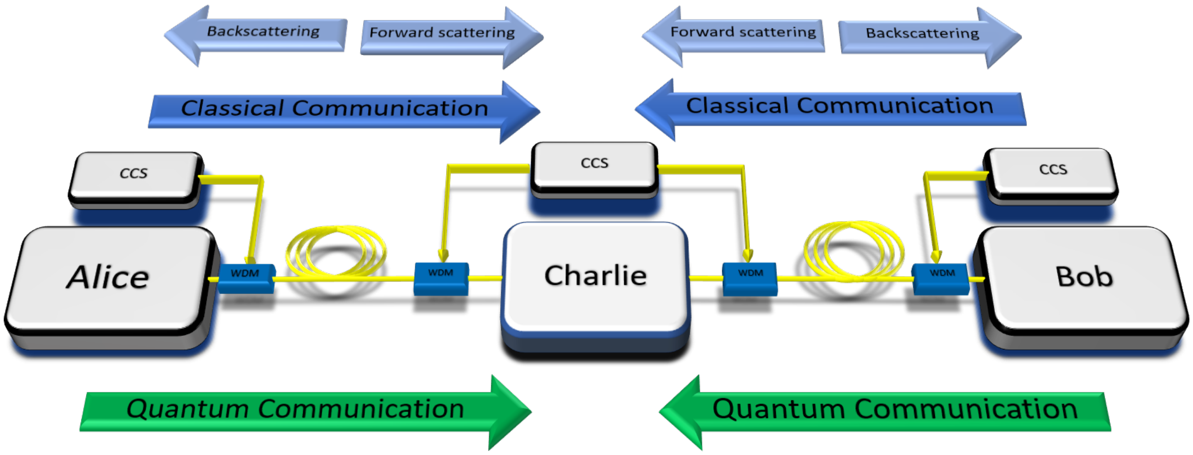


Figure 4.5: Co-propagation in the case of MDI-QKD. Alice and Bob represent quantum communication senders Charlie the measurement station. CCS: Classical communication transceivers. WDM: Wavelength division multiplexer. Note that, quantum and classical communication are in the same direction. Forward scattered photons are reaching the measurement station at Charlie.

2. **Counter-propagation**: Unlike co-propagation, counter-propagation has quantum and classical communication running in opposite directions. Therefore, back-scattered Raman photons act as noise. Fig 4.6 shows a schematic of counter-propagating in the case of MDI-QKD. The amount of Raman scattering is given by

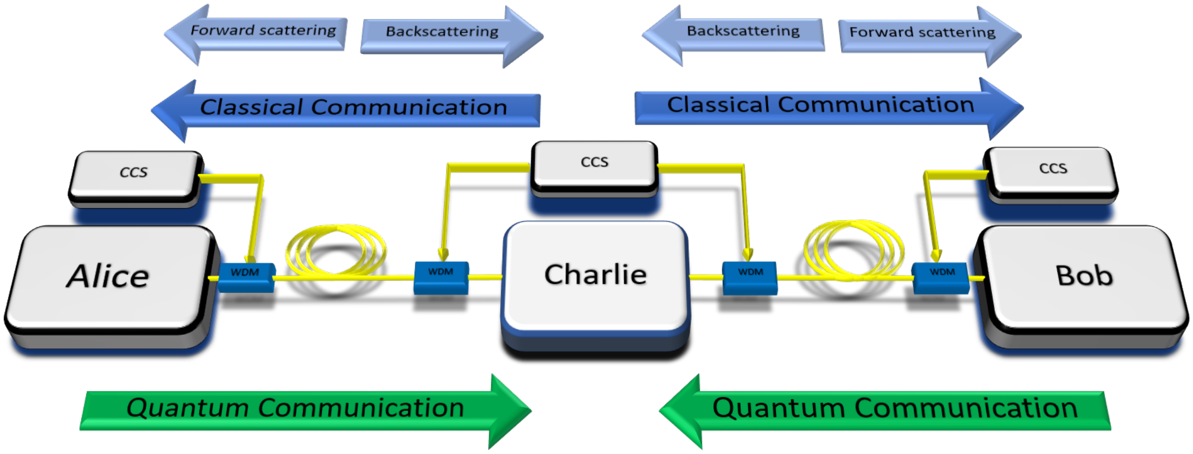


Figure 4.6: Counter-propagation in the case of MDI-QKD. Alice and Bob represent quantum communication senders and Charlie the measurement station with detectors. CCS: Classical communication transceivers. WDM: Wavelength division multiplexer. Note that, quantum and classical communication are in the opposite direction. Backscattered photons are reaching the measurement station at Charlie.

$$P_{ct} = P_l \beta \Delta\lambda \frac{(1 - e^{-(\alpha_Q + \alpha_C)L})}{\alpha_C + \alpha_Q}. \tag{4.8}$$

Here, P_{ct} is the Raman scattered power in the case of counter-propagating, $P_{ct} = nhc/\lambda$ where n is the photon scattering rate, h is Planck's constant, c the speed of light, and λ the photon wavelength. P_l is the average launch power into the classical communication channel, β is the Raman scattering coefficient, $\Delta\lambda$ is the bandwidth of the quantum channel, α_Q and α_C are fibre attenuation coefficients for the quantum and classical communication channels, and L is length of the fibre.

3. **Bi-directional**: In the case of bi-directional communication, classical communication exists in both directions, both forward scattered (co-propagation) and back-scattered (counter-propagation) Raman photons, arrive at the detectors. The total scattered power in the case of bi-directional communication is $P_{bi} = P_{CO} + P_{ct}$. A schematic in the case of MDI-QKD is shown in fig 4.7.

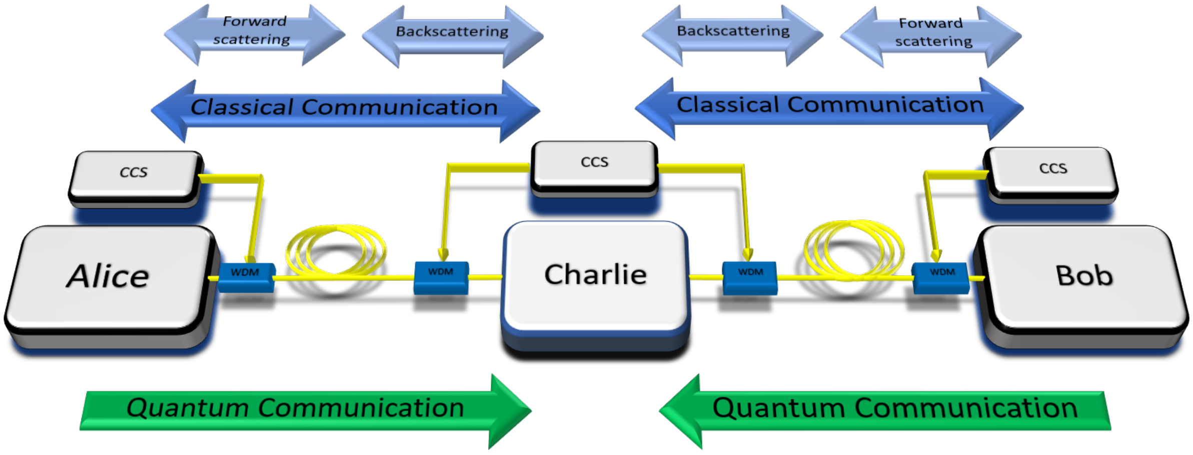


Figure 4.7: Bi-directional in the case of MDI-QKD. Alice and Bob represent quantum communication senders and Charlie the measurement station with detectors. CCS: Classical communication transceivers. WDM: Wavelength division multiplexer. Note that, quantum and classical communication are in the opposite direction. Backscattered photons are reaching the measurement station at Charlie.

Equations 4.7 and the 4.6 are plotted in figure 4.8 and distinct behaviour of forward scattering and backscattering can be seen as a function of fibre length. As fibre length increases, forward scattering increases to a maximum at approximately the distance L_{max} and decreases exponentially afterwards because of the fibre attenuation. The distance at which maximum forward scattering occurs is given by,

$$L_{max} = \begin{cases} 1/\alpha_Q & \text{if } \alpha_Q = \alpha_C \\ \frac{1}{\alpha_Q - \alpha_C} ln(\frac{\alpha_Q}{\alpha_C}) & \text{if } \alpha_Q \neq \alpha_C \end{cases} \tag{4.9}$$

However, backscattering increases until it saturates. In [13], forward and backscattered Raman noise into a QKD channel of 1550nm is studied for various classical communication channels, see in fig 4.8. It can be noted from the figure that both forward and backscattering increases with increasing fibre length, but a forward scattering reaches a maximum at around 25km 4.9. and then decreases. In contrast, backscattered Raman noise saturates as the distance increases. It is also evident from the figure that backscattering is more pronounced than forward scattering at longer fibre distances. Bi-directional communication is the worst-case scenario as it combines effects from both forward and backscattering.

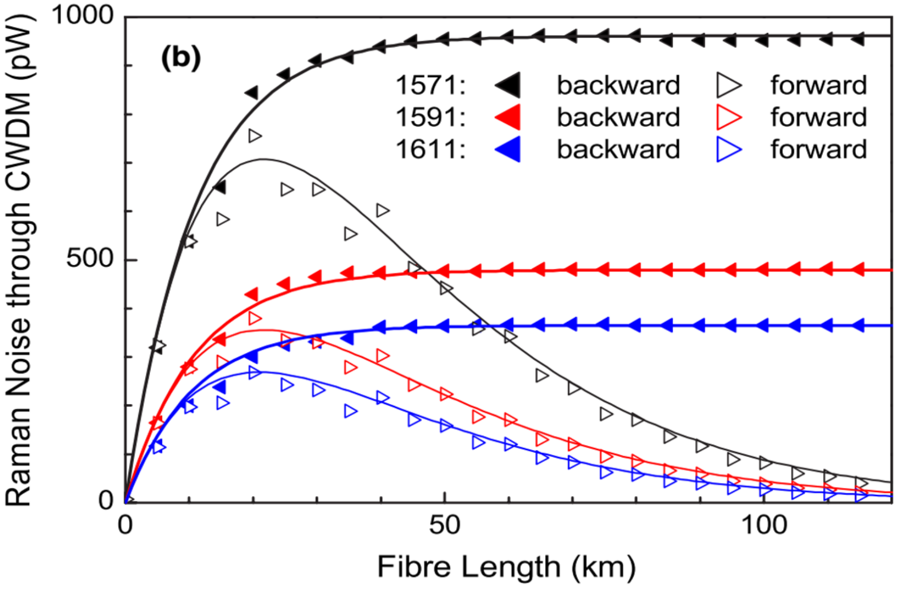


Figure 4.8: Forward and backscattered Raman noise at various wavelengths into a QKD channel at 1550 nm. The figure is reprinted with permission from [11].

4.3 Filtering noise photons

Placing the quantum channel $\sim$ 10 nm away from classical channels reduces the effect of FWM noise, Rayleigh and Brillouin scattering, but not Raman scattering. Different filtering methods are described below to diminish the amount of Raman scattering into the quantum channel.

4.3.1 Filtering of Raman photons:

Raman scattered photons can be filtered out to some extent by different filtering techniques. These are some of those filtering techniques:

- **Spectral filtering**: Spectral filtering is one of the well-known methods to block undesired photons, as shown in Figure 4.9. As mentioned earlier, the amount of Raman scattering, P_{CO} or P_{CT}, into the quantum channel is proportional to the bandwidth $\Delta\lambda$ of the quantum channel. Commercially available DWDMs (Dense wavelength division multiplexers), CWDMs (Coarse wavelength division multiplexers) and narrow-bandwidth filters (as narrow as $32pm$) can be used for spectral filtering. For instance, if the quantum channel around 1532.68 nm, a CH-56 DWDM can be used before detectors. In practice, multiple DWDMs are used in series to increase the total extinction ratio, as individual DWDMs have an extinction ratio of only $\sim$ 20 dB.

- **Temporal filtering**: This filtering method is introduced in [11] to reduce Raman scattering. In temporal filtering, successful detection events are temporally selected using the timing information of the qubit preparation. In the context of MDIQKD, Alice and Bob prepare qubits at a certain repetition rate and Charlie measures them. If Charlie has InGaAs Avalanche Photo Diodes (APDs) as detectors, he can then gate them by alternating the bias current with the same repetition rate as that of Alice's and Bob's system. Gating APDs will reduce the probability of detecting randomly arriving noise photons to a great extent and increases the probability of detecting qubits. If

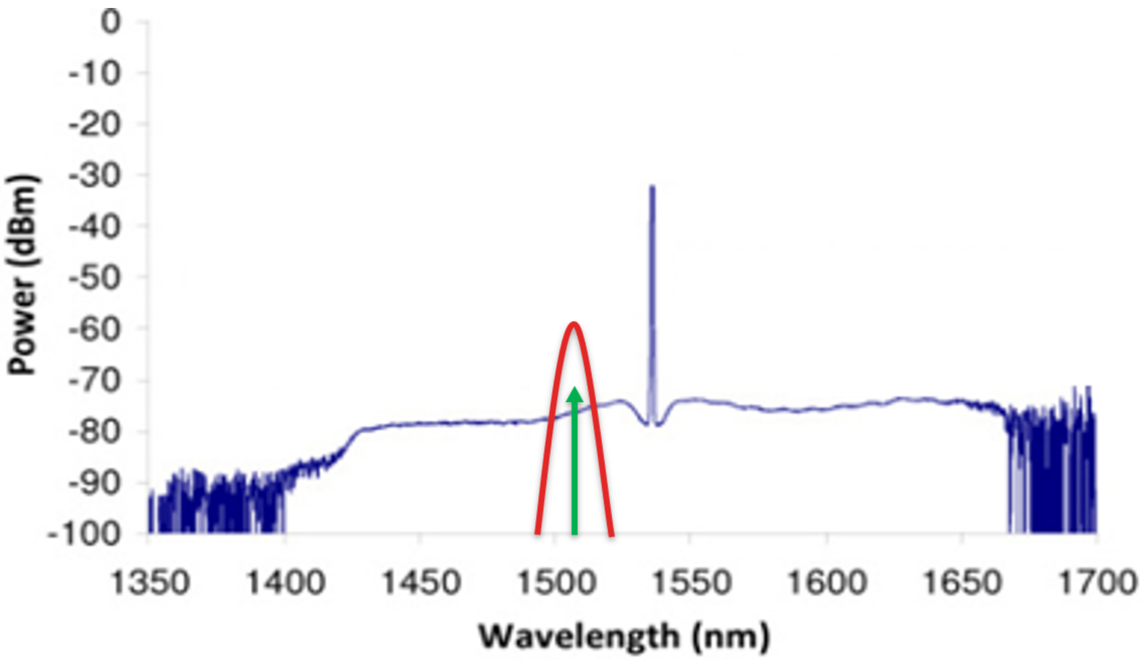


Figure 4.9: Example of spectral filtering of Raman noise. The blue line depicts the scattered light due to classical channel at 1532 nm wavelength. The green line represents the QKD wavelength. The red line represents the response function of the spectral filters, which can be a combination of DWDM/CWDM and narrow-bandwidth filters at QKD wavelength (the size of the shapes are not to the scale).

Charlie has free-running Superconducting nanowire single-photon detectors(SNSPDs) instead of APDs, he can post-select the detection events using the repetition rate by "AND" ing(logical operation) detection events with the clocking signals. In P&M QKD, all the temporal filtering techniques remain the same. But Bob will perform the filtering instead of Charlie.

- **Polarisation filtering**: This method involves placing quantum and classical communication in orthogonal polarisations. It reduces the Raman scattering by a factor of 2 and also decreases the number of pump photons (photons at classical communication wavelength) that reach the detectors. Polarisation filtering technique might not be useful while integrating quantum and real-world classical communication as this might involve modifying part of classical communication signals. For example, if the data-encoding format in the classical communication system is polarisation-based quadrature amplitude modulation, then modifying the polarisation of classical communication is not possible. Please note that this filtering method does not apply when polarisation qubits are used for quantum communication.

4.3.2 Wavelength of quantum and classical channels

As discussed in the previous section, noise photons can be reduced significantly using filtering techniques. Still, the important question of the wavelength at which to place the quantum channel with respect to classical communication channels remains open. As a guideline, the Quantum channel should be placed at a lower wavelength compared to the classical communication channels as anti-Stokes scattering is weaker than Stokes scattering. Figure 4.10 shows the different optical bands defined by the International Telecommunication Unit. Out of these bands, the C-band is currently used for classical communication while the L & U-bands are reserved for future classical communication, i.e. are not a good choice for a quantum channel. Also, Stokes-scattering from classical communication in the C-band limits, quantum communication to the L and U bands. Further, the S-band is then used for monitoring services. Residual pump photons from optical line amplifiers (EDFA amplifiers)

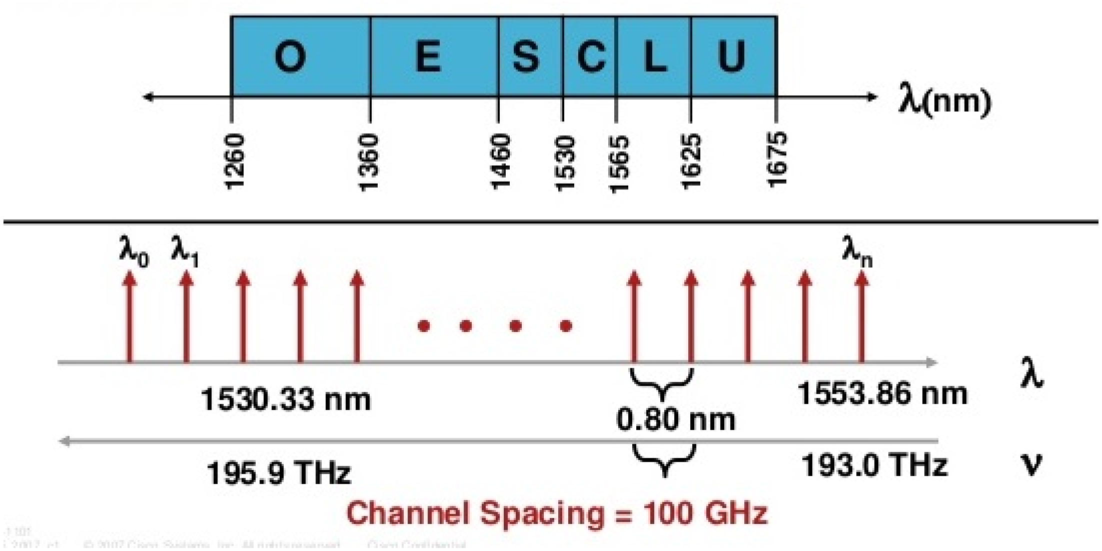


Figure 4.10: ITU optical bands.

is extended to the end of the S-band and some part of the E-band. The rest of the E-band has an OH^- absorption line in the fibre [74]. The remaining O-band is not heavily occupied and suitable for placing the quantum channel. Even though fibre attenuation in the O-band is higher ~ 0.33 dB/km compared to attenuation in the C-band ~ 0.2 dB/km, Raman scattering due to C-band communication into O-band band is negligible. Nevertheless, the reduction of secret key rate due to higher loss is more than compensated by reduced noise.

4.4 Integration of quantum communication to metropolitan network

In the previous sections, I discussed physical challenges to the integration of quantum and classical communications as well as methods to reduce the noise photons and suitable wavelengths of the quantum channel. Nonetheless, the integration of quantum communication to metropolitan area networks [12] is highly desired. Figure A.2 represents a possible way of one such integration by employing various optical components: optical splitters, wavelength multiplexers and demultiplexers, optical filters, optical switch networks etc. At customer premises (CPE), a quantum communication system, which can be a QKD system, is combined with an optical network terminal (ONT) using a QKD combiner. Amplifier bypass and DWDM bypass detour quantum communication from optical in-line amplifier and DWDM nodes respectively.

Despite successful implementations of first proposals [75, 11, 13, 76, 42], there are still a lot of open questions regarding integration:

- Classical communication networks such as metropolitan area networks (MAN) have complex topologies and only a little information is accessible in the public domain about these topologies. This limits quantum communication researchers to develop and design versatile and reconfigurable quantum communication systems.

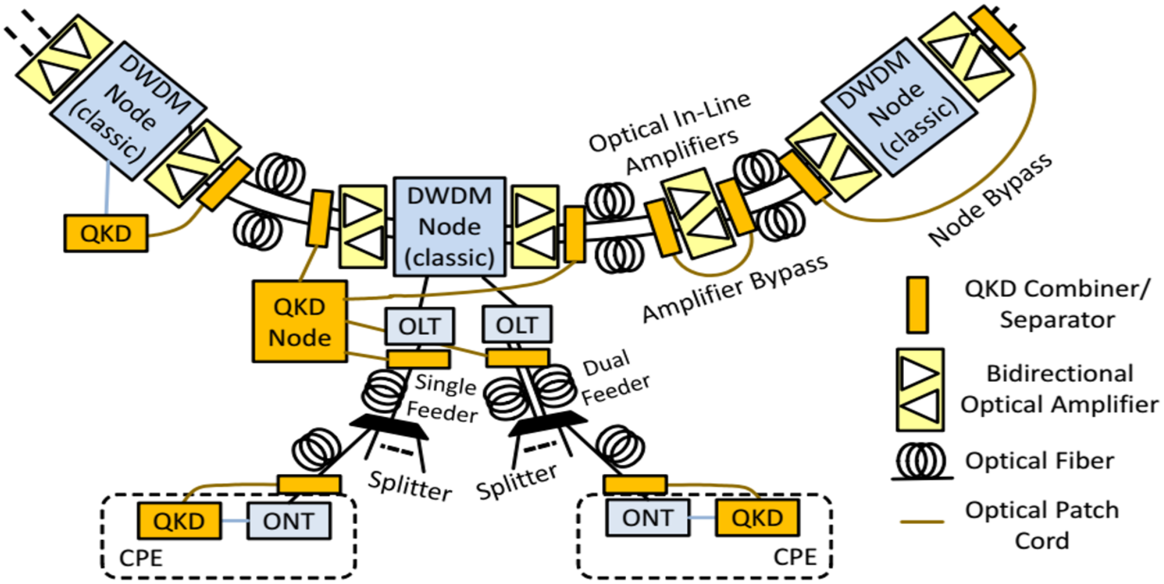


Figure 4.11: Smooth integration of QKD (quantum communication system) in metropolitan area networks. CPE: Customer premises equipment, ONT: Optical network terminal, OLT: Optical line terminal, QKD node: measurement station with switching network. The figure is reprinted with permission from [12].

- Information related to the characteristics of the optical components used in classical communication networks is not readily available in the public domain. For instance, transparency of DWDM nodes is an important piece of information to select quantum communication wavelengths. DWDM nodes were opaque to wavelengths other than DWDM wavelengths a decade ago. But, new-generation reconfigurable optical add-drop multiplexer (ROADM) nodes are mentioned as transparent to other wavelengths as well. However, more precise information is not readily available.

- If a quantum channel is placed in telecommunication bands other than the C-band then the availability of optical components, with the similar specifications as those used in classical communication networks, is not always known.

Because of the aforementioned reasons, classical communication industries and quantum communication researchers have to come together to integrate quantum and classical communication.

Chapter 5

MDIQKD coexisting with classical communication

MDIQKD is highly suitable for star-type networks, such as metropolitan networks. The investigation of MDIQKD coexisting with classical communication facilitates the economical establishment of metropolitan quantum networks. In this chapter, I report the first demonstration of MDIQKD simultaneously operating with classical communication, which is published in " Quantum Science and Technology, Volume 4, Number 4".

Author contribution: This experiment was carried out by several different lab members at the University of Calgary, Canada. Wolfgang Tittel devised and supervised the experiment. Raju Valivarthi taught me the experimental setup. Raju Valivarthi, Kim Owen, Caleb John and I performed the measurement and analysed the data with the help of Daniel Oblak and Qiang Zhou. Raju Valivarthi and I simulated the performance of the system. I also helped Wolfgang to write the manuscript of this investigation along with Daniel Oblak, Qiang Zhou, Raju Valivarthi, Kim Owen and Caleb John.

Measurement-device-independent quantum key distribution coexisting with classical communication

R. Valivarthi[1,2], P. Umesh[1,1], C. John[3], K. A. Owen[1], V. B. Verma[5], S. W. Nam[5], D. Oblak[1], Q. Zhou[1,6] and W. Tittel[1,7]

[1] Department of Physics and Astronomy, and Institute for Quantum Science and Technology, University of Calgary, Calgary, T2N 1N4, Canada

[2] The Institute of Photonic Sciences (ICFO), 08860 Casteldefels, Barcelona, Spain

[3] Department of Electrical and Computer Engineering, University of Calgary, Calgary, AB, T2N 1N4, Canada

[4] Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109, USA

[5] National Institute of Standards and Technology, Boulder, CO, 80305, USA

[6] Institute of Fundamental and Frontier Science, and School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China

[7] QuTech, and Kavli Institute of Nanoscience, Delft Technical University, Delft, The Netherlands

5.1 Abstract

The possibility for quantum and classical communication to coexist on the same fibre is important for deployment and widespread adoption of quantum key distribution (QKD) and, more generally, a future quantum internet. While coexistence has been demonstrated for different QKD implementations, a comprehensive investigation for measurement-device independent (MDI) QKD – a recently proposed QKD protocol that cannot be broken by quantum hacking that targets vulnerabilities of single-photon detectors – is still missing.

[1] Current address: QuTech, and Kavli Institute of Nanoscience, Delft Technical University, Delft, The Netherlands

Here we experimentally demonstrate that MDI-QKD can operate simultaneously with at least five 10 Gbps bidirectional classical communication channels operating at around 1550 nm wavelength and over 40 km of spooled fibre, and we project communication rates in excess of 10 THz when moving the quantum channel from the third to the second telecommunication window. The similarity of MDI-QKD with quantum repeaters suggests that classical and generalised quantum networks can co-exist on the same fibre infrastructure.

5.2 Introduction

The prospect of building a quantum internet, which promises information-theoretic secure communication [77] as well as blind or networked quantum computing [78], is generating a rapidly increasing amount of academic and corporate development efforts [79]. To minimise operating costs and hence facilitate deployment, it is important to benefit as much as possible from existing infrastructure. Starting in 1995, this has encouraged many experiments with deployed telecommunication fibre [80, 81, 82], and, since 1997, demonstrations of quantum key distribution (QKD) – the most mature application of quantum networks – together with classical data on the same fibre [75, 83, 13, 84, 85, 86, 76]. Yet, to date, comprehensive studies of the latter have been limited to so-called prepare-and-measure (P&M) QKD [77], in which one user, Alice, encodes a random string of classical bits into non-orthogonal quantum states of photons, and the other user, Bob, makes projection measurements onto a set of randomly chosen bases. Mapping measurement outcomes onto bit values leads to the so-called raw-key—two partially correlated sequences of zeros and ones (one at Alice, and one at Bob)—and, after key distillation, either to the creation of an error-free secret key, or to abortion of the key generation session.

While the security of properly implemented P&M QKD can be proven, it is threatened by quantum hacking that exploits vulnerabilities of single-photon detectors to change their functioning [87, 4, 3]. This problem can be overcome by measurement-device-independent

(MDI) QKD [29], in which Alice and Bob both send photons to a central station, Charlie, who projects their joint state onto one or more of the four maximally entangled Bell states

$$|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \tag{5.1}$$

$$|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}. \tag{5.2}$$

Here $|0\rangle$ and $|1\rangle$ denote two orthogonal quantum states, e.g. orthogonal polarisation or temporal modes. As in the case of P&M QKD (or entanglement-based QKD[77]), any eavesdropping during photon transmission will lead to errors and shortening of the secret key – possibly to zero length. However, beyond what is offered by all QKD protocols, this feature also holds in MDI-QKD if the actual measurement devices—that is the detectors—deviate from the ideal, including due to blinding or time-shift attacks by Eve.

The proposal of the MDI-QKD protocol in 2012 triggered rapid experimental progress. The first proof-of-principle demonstrations were reported only a year later [32, 33, 34], and the performance of MDI-QKD systems—including maximum distance, secret key rates, and robustness—has improved ever since [8, 38, 39, 37]. However, unlike for P&M QKD, coexistence of MDI-QKD with classical data on the same fibre has not yet been investigated in a comprehensive manner, neither experimentally nor through simulations. (But we note that spectrally multiplexed light was used in one MDI-QKD implementation to assess and compensate for polarisation transformations in the quantum channel, as well as to transmit a 1 MHz clock signal [34].)

The difficulty of combining classical and quantum communication over the same fibre lies in the generation of noise photons by the strong classical signals by means of Rayleigh, Brillouin or Raman scattering, which may mask the quantum data. Rayleigh scattering is elastic and results in additional photons at the classical communication wavelength. Assuming the quantum channel to be spectrally distinct, they can be prevented from reaching the single photon detectors using adequate spectral filters. Brillouin scattering is inelastic and leads to extra photons that are detuned by around 10 GHz from the classical signal wavelength [72]. Similar to Rayleigh scattering, Brillouin photons can be removed using spectral filters, provided the quantum and classical channels cover spectral intervals that are sufficiently far apart. Raman scattering, another inelastic process, however, generates scattered photons within a wide range of wavelengths below and above the classical communication wavelength, generally including the quantum channel. This makes spectral filtering impossible. Assuming that Rayleigh and Brillouin scattered photons can be removed, we will focus in the following only on Raman scattering.

The scattered power in case of co- and counter-propagating classical and quantum channels, P_{co} and P_{ct}, respectively, is given by [84]

$$\begin{aligned} P_{co} &= P_l \beta \Delta\lambda \frac{(e^{-\alpha_Q L} - e^{-\alpha_C L})}{\alpha_C - \alpha_Q} \qquad (5.3) \\ P_{ct} &= P_l \beta \Delta\lambda \frac{(1 - e^{-(\alpha_c + \alpha_Q)L})}{\alpha_C + \alpha_Q} \qquad (5.4) \end{aligned}$$

where L is the fibre length, P_l is the average power launched in the classical channel, β is the Raman scattering coefficient (β depends on the wavelengths of the quantum and the classical channels as well as properties of the optical fibre), $\Delta\lambda$ is the bandwidth of the quantum channel, and α_Q and α_C are the fiber attenuation coefficients for quantum and classical channels, respectively. The photon scattering rate, n, and the scattered power, P, are related by $nhc/\lambda = P$, where h is Planck's constant, c the speed of light, and λ the photon wavelength. For bidirectional communication, allowing the exchange of classical data between Alice and Bob over a single fibre, the rates for co- and counter-propagating data have to be added: $P_{bi} = P_{co} + P_{ct}$.

In this paper we experimentally demonstrate that measurement-device independent (MDI) QKD can operate simultaneously with at least five 10 Gbps bidirectional classical communication channels at around 1550 nm wavelength over 40 km of spooled fibre, and we project communication rates in excess of 10 THz when moving the quantum channel from the third to the second telecommunication window. As MDI-QKD is ideally suited for building cost-effective QKD networks with star-type topology, and can be upgraded into quantum-repeater-based networks [88], our demonstration is a first step towards a future quantum network in which secret keys, or qubits, can be distributed over arbitrarily long distances, and using which networked quantum information processing and blind quantum computing will become possible.

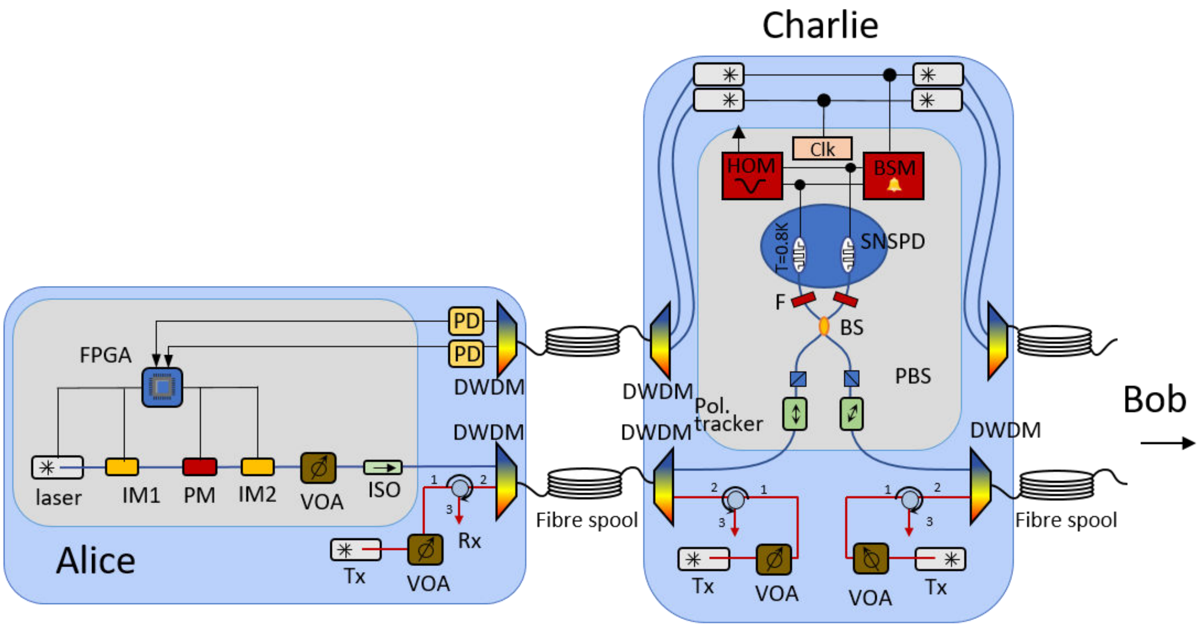


Figure 5.1: **Experimental setup.** Only one sender unit and the central receiver is shown. Intensity modulator (IM), phase modulator (PM), variable optical attenuator (VOA), optical isolator (ISO), field-programmable gate array (FPGA), dense wavelength demultiplexer (DWDM), classical transmitter (Tx), classical receiver (Rx), polarizing beam splitter (PBS), beam splitter (BS), narrow spectral filter (F), superconducting nanowire single-photon detectors (SNSPD), photo-detector (PD), Hong-Ou-Mandel dip measurement (HOM), Bell-state measurement (BSM).

5.3 Methods

Our demonstration of coexistence with classical data is based on the MDI-QKD setup depicted in figure 5.1 (see also [40]). Additional classical communication channels are prepared using four 1548 nm DFB lasers, sending continuous-wave light from Alice to Charlie, from

Charlie to Alice, from Bob to Charlie, and from Charlie to Bob. The launch power of each laser is chosen such that at the remaining power at the receiver side is an integer multiple of 2 μW – the minimum power needed for a 10 Gbps link [13]. For instance, 10 μW at the receiver side corresponds to either one 50 Gbps channel, or to five 10 Gbps channels realized using different frequencies within the ITU grid. Provided neighbouring channels are chosen, the Raman noise created by all classical channels at the quantum channel wavelength 16 nm away can be considered equal, and it does therefore not matter over how many channels classical data is distributed. Quantum and classical data are combined and split using dense wavelength division multiplexer (DWDM).

5.3.1 Raman noise

To assess the effect of Raman scattering on MDI-QKD, we first measured the noise in a narrow spectral window centred at 1532 nm—the operating wavelength of our MDI-QKD system—caused by strong light of various wavelengths propagating bi-directionally through 20 km-long standard telecommunication fibre between Alice and Charlie, and Bob and Charlie. The measurement is described in more detail in figure 5.2a.

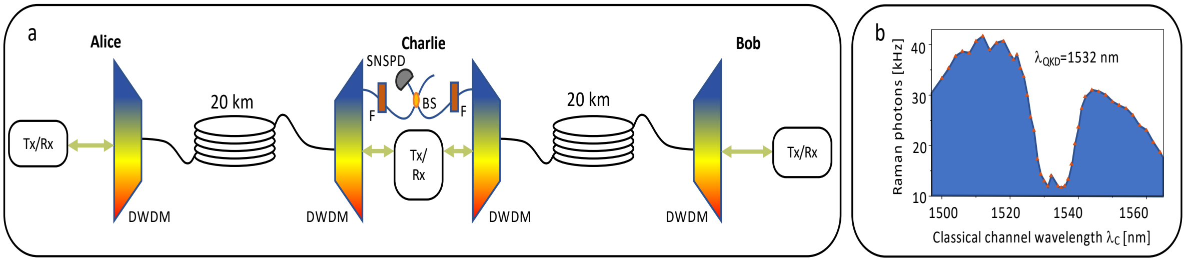


Figure 5.2: **Crosstalk. a,** Schematics of the setup used for assessing crosstalk due to Raman scattering. Classical transmitter (Tx) and receiver (Rx), dense wavelength demultiplexers (DWDM), beam splitter (BS), narrow spectral filter (F), superconducting nanowire single-photon detector (SNSPD). Classical light was injected bi-directionally into two 20 km-long fibres (Corning SMF-28 standard telecommunication fibre) connecting Alice, and Bob, to Charlie. The launch power for each classical channel, $\sim$8μW, was chosen so that each output power was 2 μW – sufficient for 10 Gbps classical communication [13]. **b,** Raman noise measured using a single-photon detector at Charlie in a 6 GHz broad spectral channel centred at λ_{QKD}=1532.68 nm wavelength for different classical channel wavelengths λ_C.

5.3.2 Experimental secret key rates

Next, we ran our QKD system over two different lengths of spooled fibre – 2 × 20 km, and 2 × 40 km. As in the case of assessing cross-talk, the quantum channels between Alice and Charlie, and Bob and Charlie, were combined with pairs of bi-directional classical data channels. To test the worst case in which Raman noise is maximized, we used 1548 nm laser light for the data channel (this choice is motivated by the result of the measurement shown in figure 5.2b), and to emulate different numbers of classical channels, we changed the power at each input in integer multiples of ~ 8 μW (~ 20 μW), corresponding to 2 μW steps in output power after 20 km (40 km) transmission. As shown in [13], 2 μW suffices to operate one 10 Gbps data channel with bit error rates $\leq 10^{-12}$, and having hence N times that power at the four receivers hence allows for N bi-directional 10 Gbps links between Alice and Bob. However, we note that the modulation scheme used to encode classical data may have an impact on the minimum power per channel, and hence on the interpretation of our results. We also remark that telecommunication operators currently do not optimize input power with respect to detector sensitivity, transmission loss and, if relevant, modulation scheme. However, this could change through software defined networking, which allows dynamic network configuration and hence optimization.

For each configuration of fibre length and number of bi-directional 10 Gbps channels, emulated using continuous-wave light with appropriately chosen power, we created sifted keys and evaluated the secret key rate according to

$$R_{\inf} \geq [Q_{11}^{Z}[1 - h_2(e_{11}^{X})] - Q_{\mu\sigma}^{Z} f h_2(e_{\mu\sigma}^{Z})]. \tag{5.5}$$

Here, Q_{11} is the gain (the probability of a projection onto a Bell state) per emitted pair of qubits; e_{11} the associated error rate; and the superscript indicates the jointly used basis (the Z basis features eigenvectors $|0\rangle$ and $|1\rangle$), and the X-basis eigenvectors $(|0\rangle \pm |1\rangle)/\sqrt{2})$. Furthermore, $h_2(x) = -x\ log_2(x) - (1-x)\ log_2(1-x)$ is the binary Shannon entropy function;

f = 1.14 is the efficiency of error correction; and the subscript “inf” denotes the assumption of infinitely long keys.

5.3.3 Simulations

We simulated secret key rates in the presence of classical communications using the code described in detail in our previous studies[89, 40]. Noise caused by Raman scattering is taken into account by increasing the detector noise according to the results shown in figure 5.2. For simulations that require Raman noise within a quantum channel centered around 1310 nm wavelength and a classical channel within the C-band, we used experimental data published elsewhere [85].

5.4 Results

5.4.1 Raman noise

The results of the measurements of the Raman noise are shown in figure 5.2b (the numerical data is listed in 5.1). The region in which $\lambda_C > \lambda_{QKD}$ corresponds to anti-Stokes scattering while the region of $\lambda_C < \lambda_{QKD}$ shows Stokes scattering. The variation of Raman photons as a function of the difference between classical and quantum channel wavelength reflects the known behavior in optical fibre [84, 73]. However, we note that in our case classical data travelled bi-directionally and that we furthermore kept the output power of the classical channel constant. This leads to a slightly different result as compared to the usual measurement in which classical data only travels uni-directionally and the input power is held at a fixed value.

Confirming previous observations [84], we find Raman noise even if the quantum and classical channels are separated by many tens’ of nanometers, and that the gain of the underpining interaction is reduced if the channel spacing is less than a few nanometers. Limiting classical channels to the extensively used C-band (extending from 1530 to 1565 nm wavelength), we furthermore see that the most cross-talk happens at a wavelength of approximately 1548 nm.

Wavelength [nm]	Noise counts [kHz]	Wavelength [nm]	Noise counts [kHz]
1500	33.33	1505	35.33
1510	40.67	1515	41.33
1520	38.00	1525	30.00
1530	13.00	1535	11.67
1540	23.67	1545	31.00
1550	28.67	1555	26.33
1560	23.00	1565	17.67

Table 5.1: Raman noise measured at Charlie in a 6 GHz wide spectral window centered at 1532 nm wavelength for different classical channel wavelengths.

5.4.2 Experimental key rates

Secret key rates in the infinite (key length) limit, together with predictions based on an independent characterisation of the complete setup (no fits) are depicted in figure 5.3 (the numerical data are listed in 5.2).

N	2 × 20 km	2 × 40 km
0	1.13E-05 ± 5.52E-06	1.72E-06 ± 6.16E-07
1	8.37E-06 ± 2.93E-06	2.66E-07 ± 5.35E-07
2	5.34E-06 ± 3.36E-06	
3	6.66E-06 ± 2.69E-06	
4	3.43E-06 ± 3.16E-06	
5	3.66E-06 ± 2.29E-06	

Table 5.2: Experimentally obtained secret key rate (R_∞) with number of co-existing 10 Gbps channels, N, for different transmission lengths of spooled fibre.

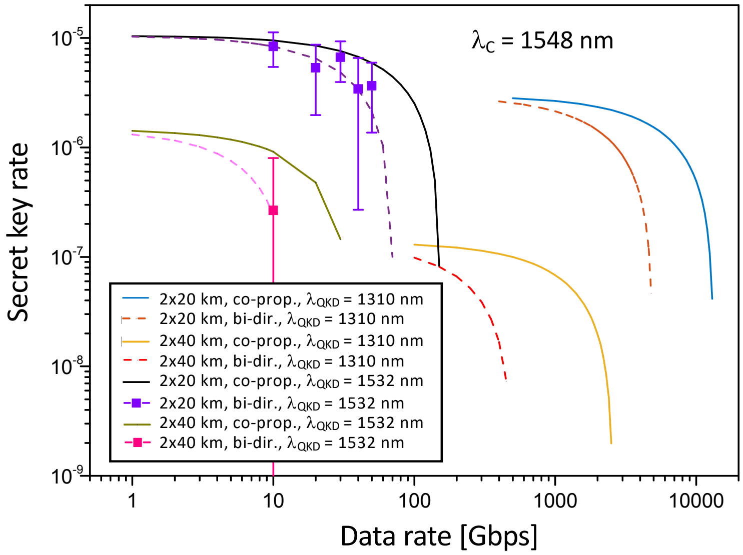


Figure 5.3: **Results.** Predicted (lines) and experimentally obtained (squared) secret key rates (per clock cycle and assuming the infinite key limit) for different fibre lengths, data rates, wavelengths of the quantum channel, and assuming bi-directional or uni-directional (co-propagating) classical communication between Alice and Bob (connected via Charlie). Classical data is assumed to be at λ_C=1548 nm wavelength. Experimental error bars indicate one standard deviation and are obtained assuming Poisson detection statistics.

5.5 Discussion

Most importantly, we find that MDI-QKD and bi-directional classical communication is possible over the same fibre. More precisely, we experimentally demonstrated positive secret key rates over a total of 40 km fibre together with the possibility for up to 50 Gbps bi-directional classical communication, and theoretically predicted positive secret key rates with up to 70 Gbps of classical data over the same fibre length. In addition, we demonstrated the possibility for QKD over a total of 80 km fibre with 10 Gbps of classical data. This is comparable to results obtained for P&M QKD, e.g. in [13] where the possibility for secure key exchange over 70 km fibre distance and coexisting with 10 Gbps of bi-directional classical communication was demonstrated. However, the quantum-classical channel spacing was only of 2.5 nm in this case, resulting in approximately three times less Raman noise as compared to the worst-case scenario of 16 nm spacing chosen in our implementation (see figure 5.2). The apparent increased resilience of MDI-QKD to Raman noise may be due to the need for detecting two photons per key bit. However, the flip-side is a reduced key rate, at least as long as single-photon detectors with quantum efficiencies significantly below unity are employed.

The classical communication rate or, alternatively, the number of classical data channels at neighbouring spectral channels can straightforwardly be increased by 50% by moving the classical data within the C-band from 1548 nm to 1565 nm wavelength, where Raman noise is reduced (see figure 5.2b). Furthermore, as shown by the simulations depicted in figure 5.3, the maximum classical data rate would increase by almost two orders of magnitude, e.g. for a total distance of 40 km from around 70 Gbps to around 5 Tbps, when shifting the QKD wavelength to 1310 nm wavelength (the classical data is assumed to be at 1548 nm wavelength, but changes within the C-band barely affect performance). In this configuration, increased photon transmission loss—normally degrading QKD performance—is more than compensated for by a reduction of Raman scattering.

Even better performance is expected when moving from bi-directional transmission of classical data to uni-directional transmission, where data co-propagates with QKD photons. In this case, most Raman photons, created in the region of highest laser power, i.e. close to Alice or Bob, would be absorbed in the fibre before arriving at Charlie's detector. As shown in figure 5.3—and still assuming a QKD wavelength of 1310 nm and classical data to be encode in the C-band—this would allow the distribution of secret keys together with classical communications over a total of 40 km at more than 10 Tbps rate. This suffices for most applications.

Obviously, our results depend on the necessary power at the receiver. For instance, increasing its value by a factor of 10 would lead to a reduction of the secure key rate to zero and by 26% if the quantum channel is at 1532 or 1310 nm wavelength, respectively. Hence, while the possibility for multiplexing of quantum and classical data will rapidly fade if encoding both channels within the same telecommunication window, using different windows—one centered at 1550 nm and one at 1310 nm—will make it very likely that both types of communication can coexist.

We note that our QKD system currently employs pairs of fibres – one fibre for clock synchronization and announcement of successful measurements at Charlie, and one for quantum communication, see Fig. 5.1. However, our results shows that quantum and classical signals can be multiplexed into the same fibre. We also point out that the calculation of the secret key rate in Eq. 5.5 assumes the limit of an infinitely long sifted key. This is in reality impossible, and an additional reduction that depends on the key length before post processing has to be taken into account [90]. For instance, with ∼0.2 kbps of sifted key, as in our current setup over 2x20 km fibre, it would take ∼ 139 hours to pass the threshold between no secret key and secret key. While feasible, this is is impractical. The time can be reduced by two orders of magnitude by increasing the clock rate from its current value of 20 MHz to a few GHz. Current bottlenecks to this solution are the maximum clock rate of the (sequentially-operated) FPGAs in the QKD senders; limited accuracy (e.g. ringing) of the signals used to drive intensity and phase modulators; and the recovery time of the superconducting nanowire single-photon detectors. They can be overcome by more advanced FPGA programming, better electronics, and the use of detector arrays[91].

5.6 Conclusion

Our investigation establishes the possibility for MDI-QKD to coexist with classical communication on the same fibre. Moreover, as MDI-QKD shares an essential feature with quantum repeater-based communication – the need for a Bell state measurement with photons that are created far apart – it also shows that classical and generalised quantum networks can co-exist on the same fibre infrastructure. We additionally note that MDI-QKD is ideally suited for building QKD networks with star-type topology in which several users are connected to the same central measurement node (Charlie). Using optical switches, it becomes then possible to connect any pair of users on demand. As users only need sender modules but no receivers (the latter will be located at the central node and be accessible to all users), this solution is both simpler and more cost-effective than the creation of a fully connected network using P&M QKD, which requires all users to have both a sender and a receiver module. Hence, our demonstration increases the commercial viability of MDI-QKD and, more generally, quantum communications will facilitate the adoption of the new quantum technology, and therefore constitutes an important step towards a world in which quantum information processing will help meeting challenges in secure data transmission, and will provide opportunities for unparalleled data processing.

Chapter 6

Implementation of high rate MDIQKD

In chapter 3, I have discussed the theory behind MDIQKD. In this chapter, I will discuss the details of the new MDIQKD system we have developed in the past year. But first, I will summarize all previous experimental demonstrations of MDIQKD, and then explore the technical requirements of MDIQKD systems.

6.1 List of demonstrations of MDIQKD

A summary of all previous experimental demonstrations of MDIQKD is tabulated in 6.1.

6.2 Previous MDIQKD systems

In this section, I will briefly discuss the challenges and limitations faced by our previous MDIQKD implementations. As summarized in the table 6.1, our previous MDIQKD systems generated time-bin qubits of 300 ps width and time-bin separation of ~2.5 ns at a rate of 20 MHz. Figure 6.1 shows a schematic diagram of the system. In order to prepare our optical states, we used phase randomized weak coherent pulses, modulated with Mach-Zehnder type

Experiment	**Encoding**	$\lambda_{quantum}$ (nm)	**Rep rate** (MHz)	**Pulsewidth** (ps)	**Equivalent Distance**(km)	**Maximum keyrate** (bps)	**Notes**
2013-Rubenok et.al[32]	Timebin	1552.9 nm	2	500	45	$3{\times}10^0$	No PR, 2×APD, RWD
2013-Liu et.al[33]	Timebin	1550.2	1	2000	50	$2{\times}10^4$	No PR, 2×SiAPD, ILD
2013-DaSilva et.al[34]	Polarisation	1546.1	1	1500	17	$1{\times}10^0$	No PR, 4×APD, RWD
2014-Tang et.al[35]	Polarisation	1542	0.5	1000	10	$1.6{\times}10^3$	PR, 2×APD, FK
2014-Tang et.al[36]	Timebin	1550	75	2500	50	$6.7{\times}10^0$	PR, 2×SSPD, FK, RWD
2015-Valivarthi et.al[8]	Timebin	1552	2 20	250 290	45 80	$3.4\ {\times}10^0$ $6.2\ {\times}10^2$	PR, 2×APD, RWD SLS, 2×SSPD, ILD
2016-Comandar et.al[39]	Polarisation	1550	1000	35	80	$1.5{\times}10^4$	PR, 4×SD-APD, PLS, ILD
2017-Valivarthi et.al[40]	Timebin	1548	20	200	80	$1{\times}10^2$	PR, 2×SSPD, ILD
Present study	Timebin	1310	200	260	NA	NA	PR, 2×SSPD, ILD

Table 6.1: List of experimental demonstrations of MDIQKD. PR: Phase Randomisation, SLS: Single Laser Source, APD: Avalanche single Photon Detector, SI-APD: Silicon Avalanche single Photon Detector, SSPD: Superconducting Single Photon Detector, SD-APD: Self differencing Avalanche single Photon Detector, FK: Finite KEy Analysis, RWD: Real World Demonstration, ILD: In-Lab Demonstration, NA: Not Applicable

intensity modulators and phase modulators. Specifically, we pulsed the laser using FPGA1 to randomise the phase between subsequent qubits. We then generated electrical signals using FPGA2 which we sent to electro-optical modulators IM1, PM and IM2. Respectively, these modulators carved temporal modes, the phase difference necessary to create the $|-\rangle$ state and created different intensities (decoy states). Then we attenuated the intensity of the laser pulse to desired mean photon number. The biggest challenge in MDIQKD is to ensure that the qubits of Alice and Bob are spectrally, temporally and spatially indistinguishable. As we used weak coherent pulses to implement qubits, the maximally possible value for indistinguishability is 50%. We had challenges in achieving this indistinguishability they are discussed in the following section.

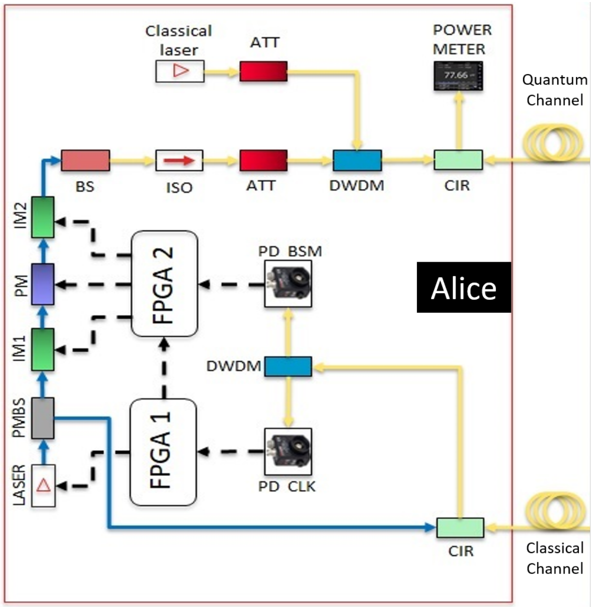


Figure 6.1: Previous Alice system. FPGA 1 & 2: Field programmable gate array 1 & 2, IM1: Intensity modulator 1, PM: Phase modulator, IM2: Intensity modulator 2, BS: 99:1 Beam splitter, ISO: Isolator: ATT: Attenuator, DWDM: Dense wavelength division multiplexer, PD BSM: Photodetector to detect optical encoded Bell state measurement result, PD CLK: Photodetector to detect optical encoded 10MHz distributed clock from Charlie and CIR: Circulator.

6.2.1 Challenges and solutions

We had three main challenges in our previous MDIQKD systems.

The first challenge was that there were discrepancies between temporal modes created at Alice and Bob. We used the electronic signals generated by FPGAs to create time-bin qubits. However, the electronic signals from the FPGAs of Alice and Bob were not identical, resulting in temporal mode mismatch. For example, the pulse width of early temporal mode from one of the FPGAs was 300 ps, and the other one was 310 ps. This difference in pulse width led to a drop in indistinguishability. In order to prevent pulse width differences, we moved away from FPGA controllers in new MDIQKD systems. More precisely, a new electronic circuit was designed to provide complete control over the width of the temporal modes.

The second challenge was to match the temporal mode separations at Alice and Bob. We utilised phase-locked loops (PLLs) in FPGA to specify the separation between early and late temporal modes. Although PLLs have the required time resolution, different FPGAs were generating different separations due to internal routing differences and stray capacitances. For instance, temporal mode separations of Alice and Bob were 2.46 ns and 2.52 ns, respectively which limited the indistinguishability. This problem can be potentially resolved with the solution to the previous problem.

The third and the main challenge in our MDIQKD systems was to achieve sufficient frequency stability of the lasers. Assuming qubits from Alice and Bob have no temporal mode mismatch and have the same temporal mode separation, the indistinguishability of these qubits further depends on the chirp and frequency difference between lasers of Alice and Bob. Specifically, the chirp can mean that a wide variety of frequencies are present within the same pulse. This results from pulsing for phase randomisation. As the repetition rate of our MDIQKD system was 20MHz, the chirp could be minimized by carving qubits near the end of the pulse, where there has been enough time for the laser to stabilize to one frequency. We still needed to minimise the frequency difference between the lasers of Alice and Bob to less than 10 MHz to achieve indistinguishability of greater than 48%, given that separation of temporal modes in our system was 2.5 ns. However, the frequency difference

between the lasers was <10 MHz for not more than 2 minutes, limiting us from performing long-term measurements. However, before choosing on a solution, we need to know how much frequency stability is required.
The qubit phase depends on the product of the temporal mode separation and frequency difference between the lasers of Alice and Bob. To achieve good indistinguishability, we can either decrease the temporal mode separation, thereby relaxing the frequency difference, or minimise the frequency difference while keeping the temporal mode separation the same. It is challenging to reduce the frequency difference between lasers to less than 10 MHz using off-the-shelf electronic components. However, decreasing the temporal mode separation is also difficult, as it usually results in the early temporal mode ringing into the late temporal mode. Consequently, we need to explore a compromise of the two options and find the optimal temporal mode separation and frequency difference.

Besides the above mentioned challenges, we also had a problem with precisely setting the mean photon numbers of decoy states. We modulated the electronic signals generated by FPGA2 on to the intensity modulator IM2 to create three different intensities corresponding to vacuum, weak-decoy and signal state. To make a vacuum state, we sent no signals to both IM1 and IM2, so no light was allowed to pass. For the signal and decoy states, we generated four electronic signals using FPGA: one signal and one weak-decoy for each of our two bases. We adjusted the voltage levels of these four electronic signals using linear potentiometers. As potentiometers are resistive in nature, temperature fluctuation resulted in fluctuations of voltage levels. In turn, this caused fluctuations in the intensities of light after IM2 and thus the mean photon numbers of Alice's and Bob's qubit states. It was not easy to then readjust these levels, because the 4 electronic signals were related to each other through an op-amp adder in a bridge network fashion. As a result, changing one of the potentiometers caused an imbalance in the bridge and altered the voltages determined by the other potentiometers. To resolve this issue, we need 4 voltages that can be adjusted independently of each other. A possible solution would be using digital-to-analog converters

(DAC) in place of potentiometers to set different voltage levels.

6.3 New MDIQKD system

While designing new MDIQKD system, we thoroughly investigated all the proposed possible solutions and resolved the problems. We designed new electronic boards to create the temporal modes, using which we can vary the temporal width from 50 ps to 2000 ps in steps of 5 ps. These boards also solved the problem of mismatch in temporal mode separations at Alice and Bob. At the same time, we increased the repetition rate of the system from 20 MHz to 200 MHz. According to our investigation described in chapter 5, we changed the wavelength of the quantum channel from 1532 nm to 1310 nm so that MDIQKD can coexist with terabits of classical communication at 1530-1565nm.

In the following section, I will discuss the functionality of our new MDIQKD system. Figure 6.2 shows the schematic diagram of the Alice setup.

6.3.1 Qubit preparation:

We use random numbers generated by a quantum random number generator (QRNG) to produce qubits. These random numbers determine temporal modes, bases and intensities which are implemented using Very high speed integrated circuit hardware description language (VHDL) and a CYCLONE-IV FPGA mounted on an evaluation board, DE0-NANO. We generate the following digital outputs from this FPGA: the laser driving signal, IMearly, IMlate, data bus to DAC1 and data bus to DAC2 (the functionalities of these signals are described below). As the digital outputs from FPGA have a large rise and fall time of ~ 2 ns, we use pulse conditioners for signal conditioning. In general, signal conditioning is a process where the characteristics of the signal, such as rise time, fall time, and so on, are modified to meet the requirements. The pulse conditioners modify the rise and fall time to ~ 200 ps from ~ 2 ns. Also, they have programmable delay generator chips using which we

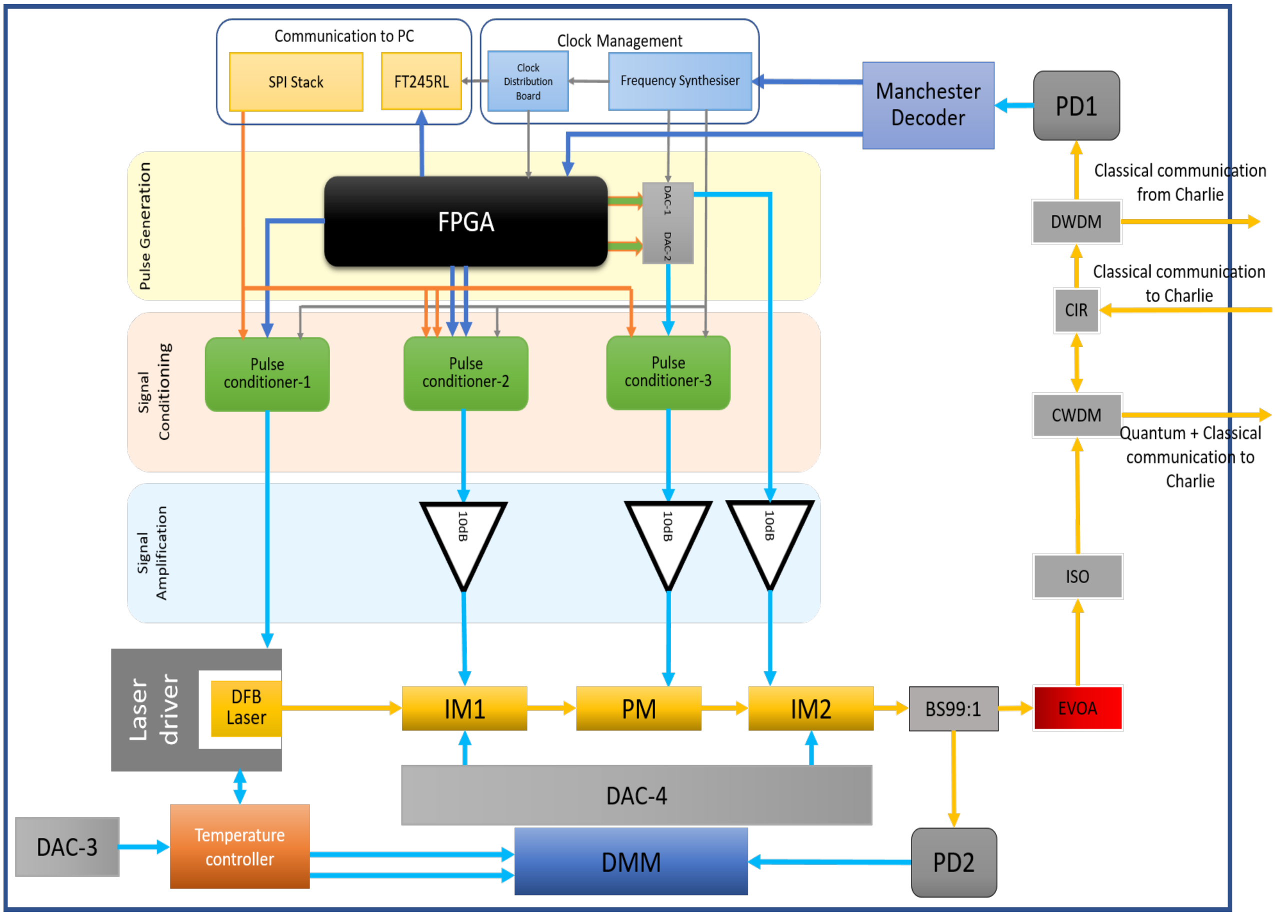


Figure 6.2: MDIQKD system of Alice/Bob. FPGA: Field programmable gate array; DAC1 & DAC2: 14-bit digital-to-analog converters; FT245RL: Integrated chip (IC) for communication; SPI Stack: stack of SPI bus used for communication with delay generator chip in pulse conditioner 1, 2 and 3; DFB laser: Distributed feedback laser; IM1 and IM2: Intensity modulators; PM: Phase modulator; BS99:1 : Beam splitter with splitting ratio of 99:1; EVOA: Electronic variable optical attenuator; ISO: Isolator; CWDM: Coarse wavelength division multiplexer; CIR: optical circulator; DWDM: Dense wavelength division multiplexer; PD1 and PD2: Photodetectors; DAC3: 18-bit digital-to-analog converter; DAC4: multichannel 14-bit digital-to-analog converter and DMM: 6.5 digits precision digital multimeter. The grey line represents 200MHz clock; the blue line represents digital signals, the magenta line represents analog signals, the green line represents data bus of width 14 bits and the orange line represents communication signals from the SPI stack.

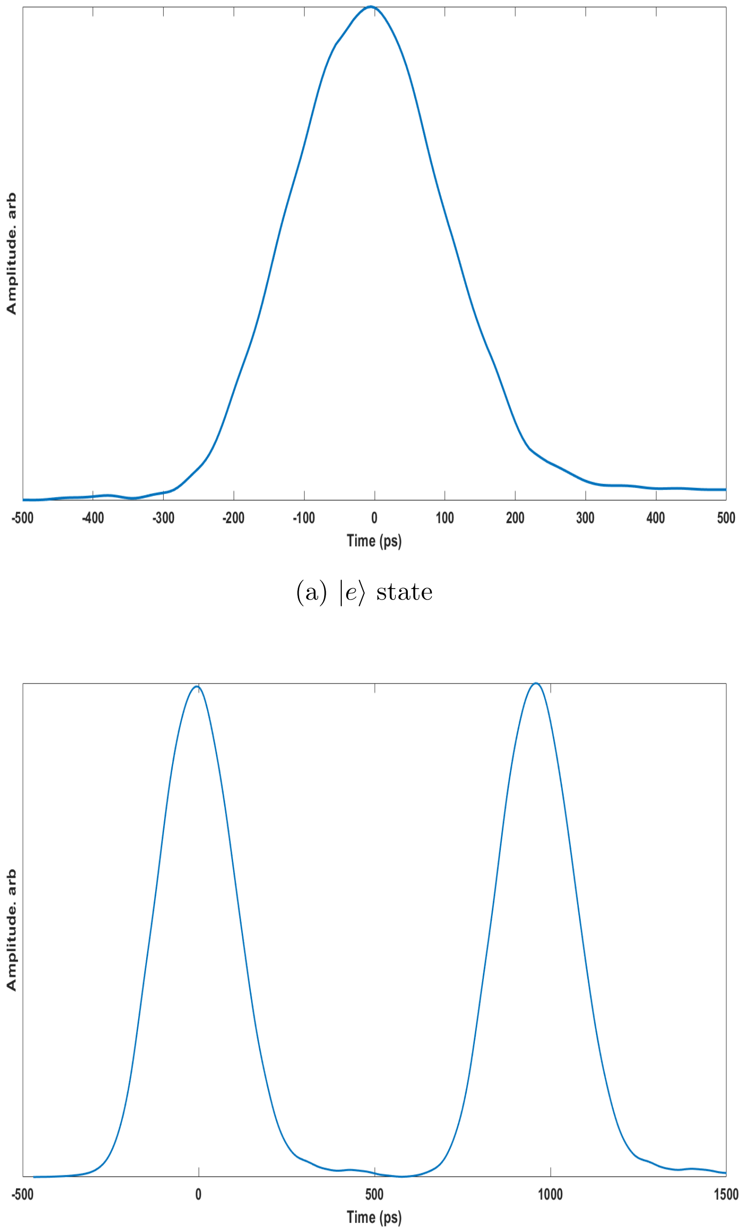
can delay the rise time and fall time in steps of 5 ps. Qubits are prepared in four steps.

First, we pulse the laser using laser driving signal from below to above threshold current in order to randomise the phase between subsequent qubits to avoid a phase remapping attack [92]. For this purpose, we generate a laser driving signal using the FPGA and pulse conditioner-1. We set the duty cycle of the laser driving signal by programming the pulse conditioner-1. Ideally, the duty cycle should be as high as possible because this decreases the laser chirp. However, we could only achieve a duty cycle of 80% due to bandwidth limitation of the laser driving board.

Second, we create temporal modes using IMearly and IMlate signals. We generate these signals from FPGA and use pulse conditioner-2 to shape the signals and combine them. We program the delay generator chips in pulse conditioner-2 to vary the pulse widths of the early and late temporal modes and the separation between them. We amplify this signal by 10 dB and modulate IM1 to carve temporal modes. Usually, we use intensity modulators with a high extinction ratio to reduce the probability of undesired photons leaking through. For instance, without a high extinction ratio of IM1, whenever we prepare the $|e\rangle$ temporal mode, we could also be leaking light into $|l\rangle$, which would reduce the probability of a correct Bell state projection, and contribute errors. Figure 6.3 shows different temporal modes after IM1.

Third, we need to phase shift the late temporal mode relative to early by 180° in order to prepare the $|-\rangle$ state. To do so, we generate 14 digital bits from the FPGA and transfer them to a 14-bit digital-to-analog converter (DAC1). DAC1 then produces an analog signal corresponding to the received 14 digital bits and connects with pulse conditioner-3. We program pulse conditioner-3 to create a pulse of 500 ps width with an appropriate delay. The delay is required to make sure that the generated pulse overlaps only on the late temporal mode and shifts the phase of the late mode by 180° relative to early. We then set the amplitude of the pulse to exactly match the pi-voltage (V_π voltage) of the phase modulator using the variable attenuator and amplifier.

In the fourth and final step, we generate another set of 14 digital bits and transfer them to another 14-bit digital-to-analog converter DAC2 to create the different intensities required for the decoy-state protocol. We amplify the analog signal from DAC2 by 10 dB and modulate IM2 to create different intensities (decoy states). In the current system, we



(a) $|e\rangle$ state

(b) $|+\rangle$ state

Figure 6.3: Temporal modes for qubits prepared in Z and X basis.

define five voltage levels: one for vacuum, two for weak decoy-states (one for the Z basis and one for the X basis) and two more for signal states (one per basis). As we are using a 14 bit DAC, we can produce 2^{13} different voltage levels and can precisely prepare different intensities. Also, we can readily change the number of decoy states if need be.

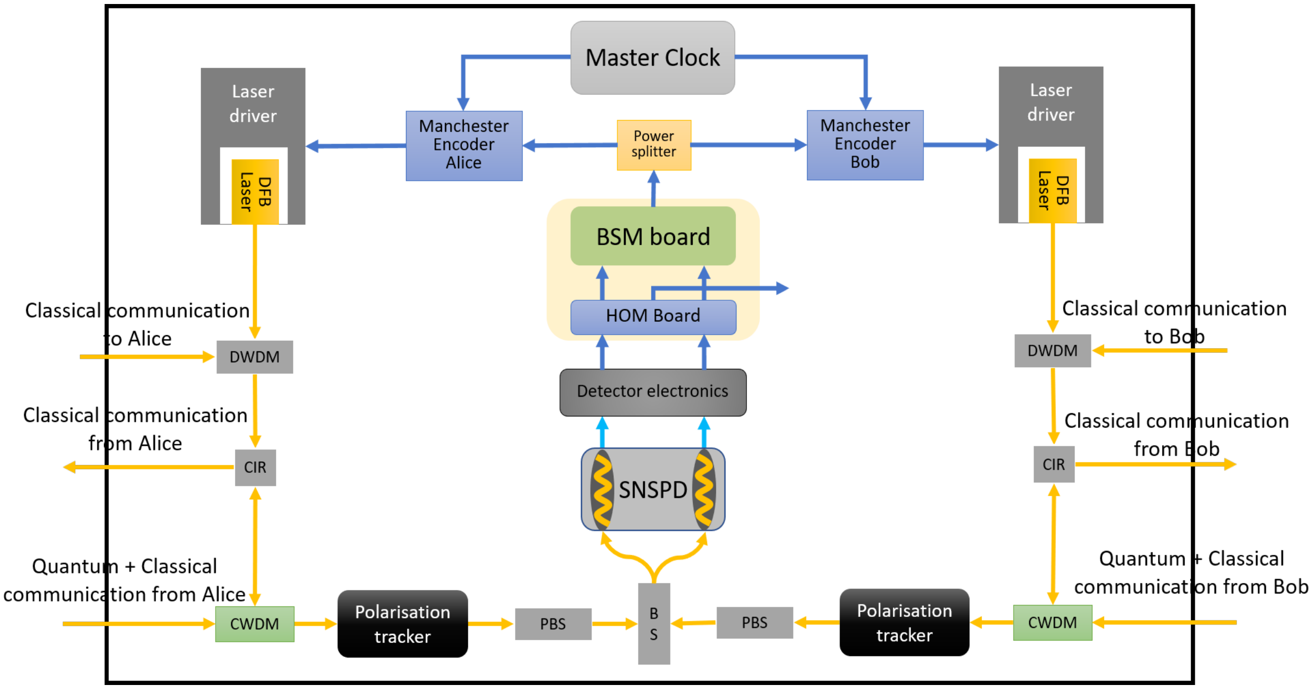


Figure 6.4: Setup of Charlie. CWDM: Coarse wavelength division Multiplexer; PBS: Polarisation beam splitter; BS: Beam splitter; SNSPDs: Superconducting nanowire single photon detectors; DWDM: Dense wavelength division multiplexer and CIR: Circulator.

All in all, we create qubits with different intensities using IM1, PM and IM2. Using a 99:1 beam splitter (BS99:1) after the EOMs and a $5GHz$ photodetector (PD1) with a multichannel digital multimeter (DMM) to monitor the high intensity output port of the BS, we enable measurement of the power and use the result in a PC based feedback loop to set the bias voltages V_{DC}, for IM1 and IM2 using digital-to-analog converter-3 (DAC3). With this feedback, we are able to carve the desired states while maintaining a total extinction ratio of 40 dB. We then attenuate the low-intensity output of the beam splitter, using an electronic variable optical attenuator (EVOA) to set the desired mean photon numbers. Due to the feedback loop, mean photon number fluctuations are minimized. Finally, we place an optical isolator at the end of the Alice's system to protect from Trojan horse attacks [2, 48]. A schematic of the Charlie's system is shown in figure 6.4.

6.3.2 Bell state measurement module

Charlie's BSM module consists of polarisation beam splitters (PBSs), a polarisation maintaining beam splitter (PMBS), superconducting nanowire single-photon detectors (SNSPDs) and electronic circuits to perform logical operations. We insert the PBSs at the input ports of the PMBS to ensure the polarisation indistinguishability. The PMBS then erases the which-way path information of Alice's and Bob's qubits, and together with the two detectors performs a Bell state measurement(BSM), which projects onto the $|\psi^{-}\rangle$ Bell state. We feed the detection signals from SNSPDs to the BSM electronic module. This module performs coincidence detections in orthogonal temporal modes, and then post selects the successful BSMs. Finally, it generates a 5 ns long pulse for each successful BSM. We split this long pulse into two electronic pulses - one for Alice, and one for Bob

6.3.3 Time tagging

In the following, I will describe the process of time tagging from the perspective of Alice. The explanation is the same for Bob because their setups are identical. Alice needs to know two critical pieces of information to do time tagging: first, she must know the total time needed for a qubit to travel from Alice to Charlie and the BSM result to travel from Charlie back to Alice; Second, she must know which states she has sent Charlie, and correctly associate them with successful BSM projections.

At the beginning of the protocol, Alice estimates the total travel time by performing an initialisation experiment with Bob. In this experiment, they decide together which qubits to send to Charlie to guarantee a successful BSM projection. Then, Alice sends that predecided qubit to Charlie and waits until the BSM result from Charlie reaches her. When she compares the time she sent the qubit (t_0) and the time she received the BSM (t_1), she can calculate the total travel ($\Delta t = t_1 - t_0$). Alice then pairs qubits with the corresponding BSMs. For each qubit she generates, she stores their classical description (bit, basis and mean photon number) in her computer's memory until the total travel time has passed. If she receives the notification of a successful BSM from Charlie, then she matches the stored information with the result for basis and decoy-state reconciliation; if she does not, then she discards the stored information. Towrads this end, Alice estimates the total travel time before each key distribution session.

6.3.4 Stabilisation and feedback modules:

We have three different stabilisation modules in our MDIQKD system.

- **Timing:** Charlie distributes a clock to Alice and Bob, which serves as a timing reference for all the devices at Alice, Bob and Charlie. But, in order to synchronize the arrival of photons from the senders at Charlie careful adjustment is required. Towards this end, we perform Hong-Ou-Mandel (HOM) interference, an indistinguishability measurement, of qubits from Alice and Bob at Charlie. This measurement utilises the same setup as that for the BSM, but detection signals are sent to the HOM measurement board, which calculates the coincidence detections corresponding to both photons arriving in early or late temporal modes. The coincidence rate is a measure of indistinguishability and is minimum when photons from Alice and Bob arrive at the PMBS precisely at the same time. A feedback signal is provided to the clock generator, which results in appropriate delays of the clock signal travelling to Alice, or Bob. Using this method, we are able to synchronise Alice and Bob with a precision of $\sim$ 20 ps.

- **Frequency stabilisation:** Frequency stabilisation was a principal concern in the previous MDIQKD system. In general, frequency stabilisation of a laser can be achieved using various techniques: controlling the temperature of the laser, Pound-Drever-Hall cavity locking [93], locking to a gas cell [94], and so on. Controlling the temperature of the laser is the simplest and most economical of all. In the current system, we use a temperature controller with an inbuilt PID for active feedback. This controller requires the target temperature and actual temperature as inputs, both in terms of voltages. The latter one is provided by inbuilt 10 kΩ thermistor of the laser and the latter one is precisely set using an 18-bit digital-to-analog converter-4 (DAC4). Figure 6.5 shows a schematic diagram of the temperature controlling electronics. In order to actually compare Alice and Bob's frequencies, they send from time to time some unmodulated light to Charlie along a separate fibre. Charlie measures the beat frequency and then provides the feedback signal to Alice and Bob, which allows them to adjust the frequencies.

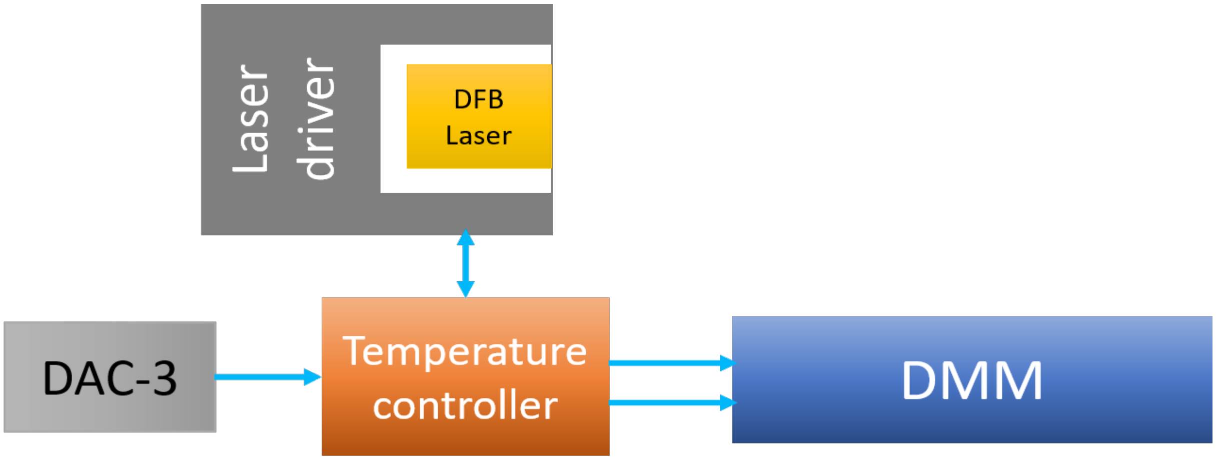


Figure 6.5: Setup for temperature control of the laser. DAC3: High precision 18-bit digital-to-analog converter and DMM: 6.5 digit precision digital multimeter.

- **Polarisation stabilisation:** The polarisation of a photon in a non-polarisation maintaining fibre is very unstable compared to any other degree of freedom. At Charlie, we insert the PBSs before the PMBS to make sure photons at the PMBS are indistinguishable in polarisation. Fluctuation in the polarisation before the PBSs then result in a decrease of the count rates in the SNSPDs. We feed this information back to the polarisation trackers, which allow maximising the count rates.

6.3.5 Classical communication

6.3.5.1 Classical communication for key distribution

In MDIQKD, the clock and the BSM result are classical communication signals distributed from Charlie to Alice and Bob. For the clock, we use a 200 MHz signal, and we use Manchester encoder modules to combine the clock and the BSM result into a single signal that is used to modulate the laser of 1548 nm wavelength. We multiplex this optical signal using a CWDM with other classical communication signals that Charlie wants to send. At Alice and Bob, we demultiplex this optical signal using similar CWDMs and DWDMs. A 5 GHz-bandwidth photodetector (PD) then converts the optical signal into an electronic signal and use the Manchester decoder module to extract the clock & the BSM results. The clock distribution board replicates the clock into multiple copies and distributes them to FPGA, DAC1, DAC2 and pulse-conditioner boards. Finally, the BSM results are fed into the FPGA for time tagging.

6.3.5.2 Coexistance of quantum and classical communication

To multiplex classical and quantum communication into the same fibre, we use different wavelengths for the two types of signals - 1532 nm and 1310 nm, respectively, and a combination of CWDMs, circulators, and DWDMs. A schematic is shown in fig 6.6.

6.4 Characterisation of the new MDIQKD system

6.4.1 Frequency stabilisation

We stabilise the frequencies of Alice's and Bob's lasers as described in section 6.3.4 using temperature control electronics. We then characterise the parameters of all components, assuming that deviations in the parameters follow Gaussian distribution. All the characterisations are discussed below.

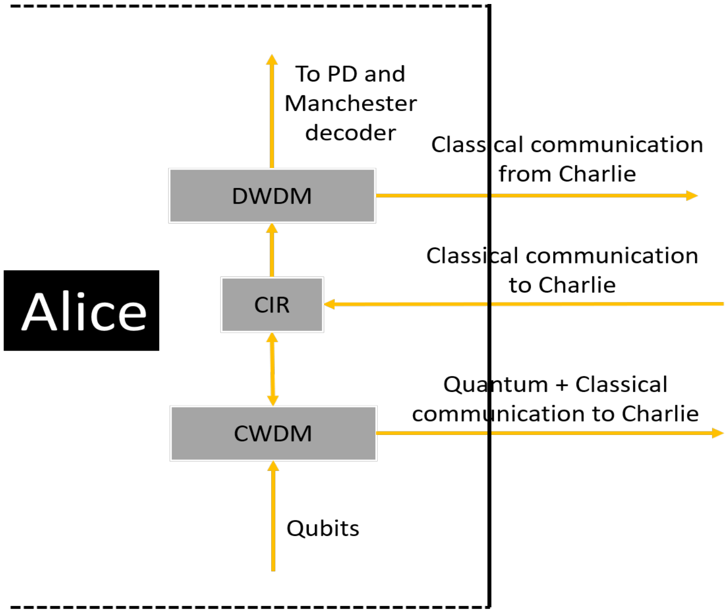

To PD and Manchester decoder
DWDM
Classical communication from Charlie
Alice
CIR
Classical communication to Charlie
CWDM
Quantum + Classical communication to Charlie
Qubits

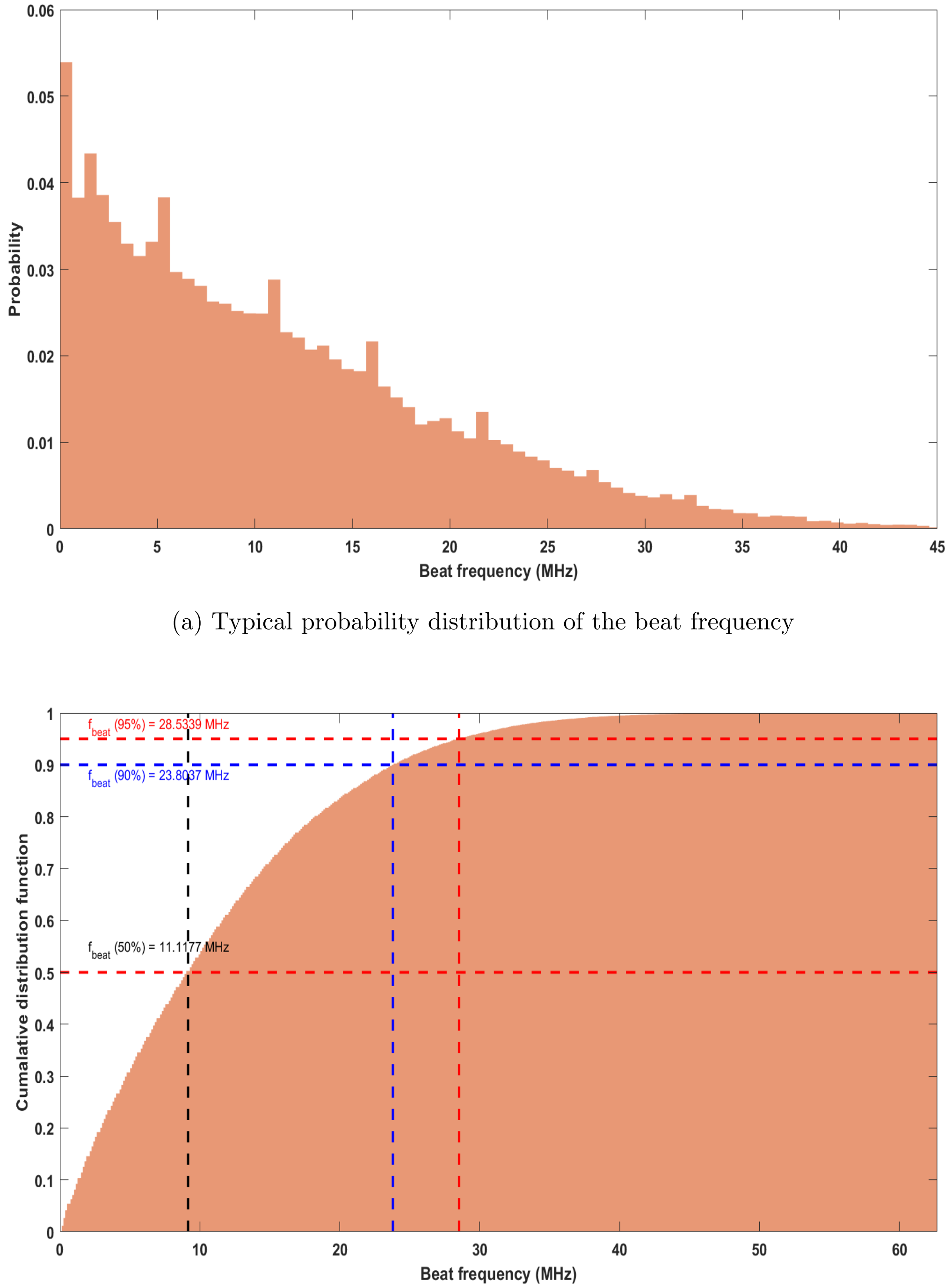
Figure 6.6: Wavelength multiplexing and demultiplexing at Alice. DWDM: Dense wavelength division multiplexer; CIR: Circulator and CWDM: Coarse wavelength division multiplexer.

Each laser features a wavelength sensitivity ($d\lambda/dT$) of 0.1 nm $/°C$. Each temperature controller has a stability of $0.0012°C$ for 1 hour, working at an off-ambient temperature. This results in a laser wavelength stability of $d\lambda = 0.0012°C\times$ 0.1 nm $/°C = 0.12pm$. At 1310 nm this corresponds to 21 MHz. With the individual lasers stabilised to 21 MHz, the beat frequency is smaller than 30 MHz with a mean <15 MHz. Typical histograms of beat frequency measurements are shown in figure 6.7. We also tested the long term stability of the beat measurement for $\sim$ 12 hours, finding that the frequency difference remained below 50 MHz.

6.4.2 Characterisation of qubits from Alice and Bob

To characterise the qubits from Alice and Bob, we describe them using the general description [89]:

$$|\psi\rangle = \frac{1}{\sqrt{1+2b^{x,z}}}(\sqrt{m^{x,z}+b^{x,z}}|0\rangle + e^{i\phi^{x,z}}\sqrt{1-m^{x,z}+b^{x,z}}|1\rangle) \tag{6.1}$$



(a) Typical probability distribution of the beat frequency

(b) Cumulative distribution function of the beat frequency

Figure 6.7: Histograms of beat frequency between lasers of Alice and Bob. The measurement is performed for the duration of 30 minutes.

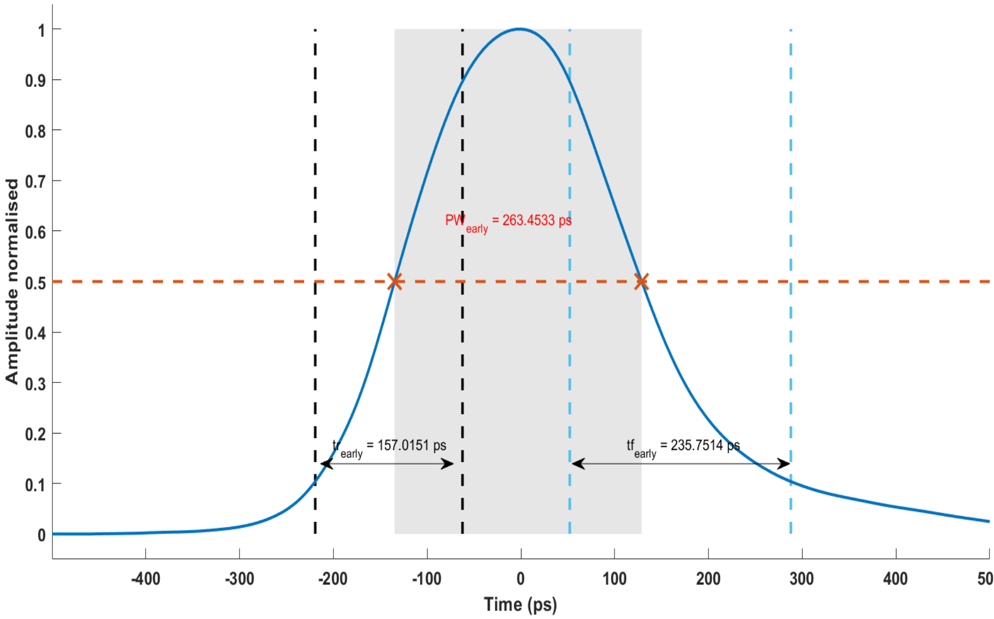
where $|0\rangle$ and $|1\rangle$ are the orthogonal qubit modes (early and late temporal modes). $|\psi\rangle$ describes any pure state and the parameters $m^{x,z}, b^{x,z}$ and $\phi^{x,z}$ allow us to characterise the experimental imperfections of the qubit states from Alice and Bob. The parameter $m^{x,z}$ describes the probabilities of creating an early or late temporal mode for qubits prepared in the Z or X basis. The parameter $b^{x,z}$ represents the background light emitted and modulated by an imperfect source. Finally, $\phi^{x,z}$ to characterise the phase part of the $|-\rangle$ state. In table 6.2, all parameters are listed with their ideal values and experimental.

Parameter	**Ideal values**	**Alice's value**	**Bob's value**
$b^{z=0} = b^{z=1}$	0	1.12×10^{-5}	1.05×10^{-5}
$b^{x=-} = b^{x=+}$	0	1.12×10^{-5}	1.05×10^{-5}
$m^{z=0}$	1	0.989	0.991
$m^{z=1}$	0	0	0
$m^{x=-} = m^{x=+}$	0.5	0.4968	0.4975
$\phi^{z=0} = \phi^{z=1} = \phi^{x=+}$	0	0	0
$\phi^{x=-}$	π	NM	NM

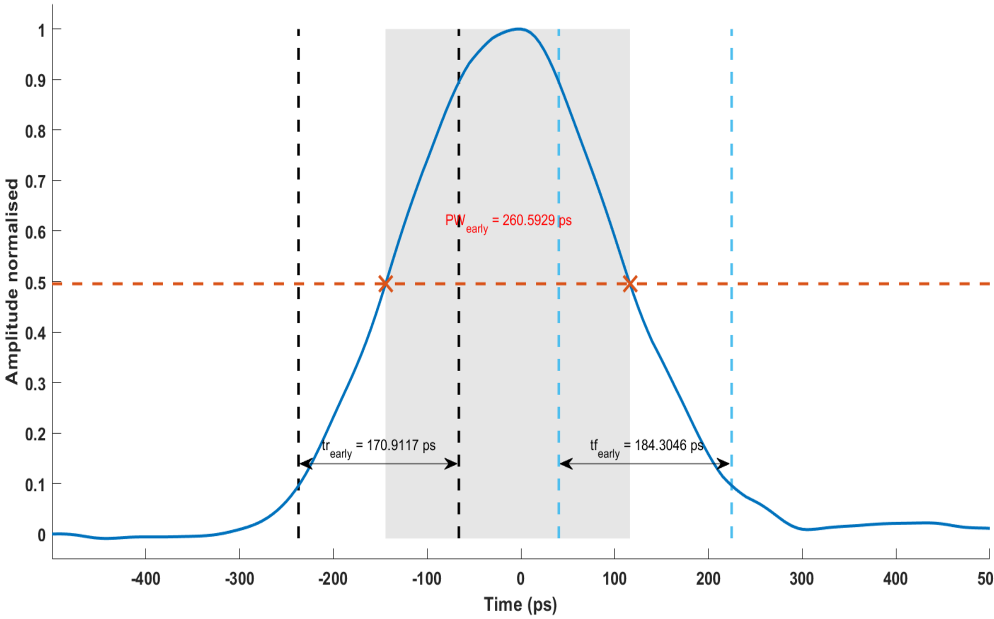
Table 6.2: Parameters of the qubit state represented by equation 6.1. NM: not measured.

Please note that equation 6.1 does not include the parameters through which other degrees of freedom can be characterised (i.e spectral, polarisation, spatial, temporal modes). We perform the beat measurement to ensure the spectral modes of Alice and Bob are sufficiently close. We use lasers followed by PBSs and confirm that we have polarisation extinction ratios of atleast 20 dB. As all the fibres used in this work are single mode fibres, we do not need to characterise the spatial modes of the qubits. However, we characterise the temporal modes separately. Figures 6.8 and 6.9 shows a comparison of the $|e\rangle$ and $|+\rangle$ states from Alice and Bob.

In table 6.3, I summarize characteristics of different temporal modes from Alice and Bob. From figure 6.8 and table 6.3, it can be noted that the $|e\rangle$ state from Alice has a longer fall time than Bob. This may be due to parasitic capacitances in Alice pulse conditioner-1 board. Also, note that $|e\rangle$ states in the Z basis and the X basis have slightly different characteristics. This might not significantly affect the indistinguishability as these variations occur in states from both Alice and Bob.

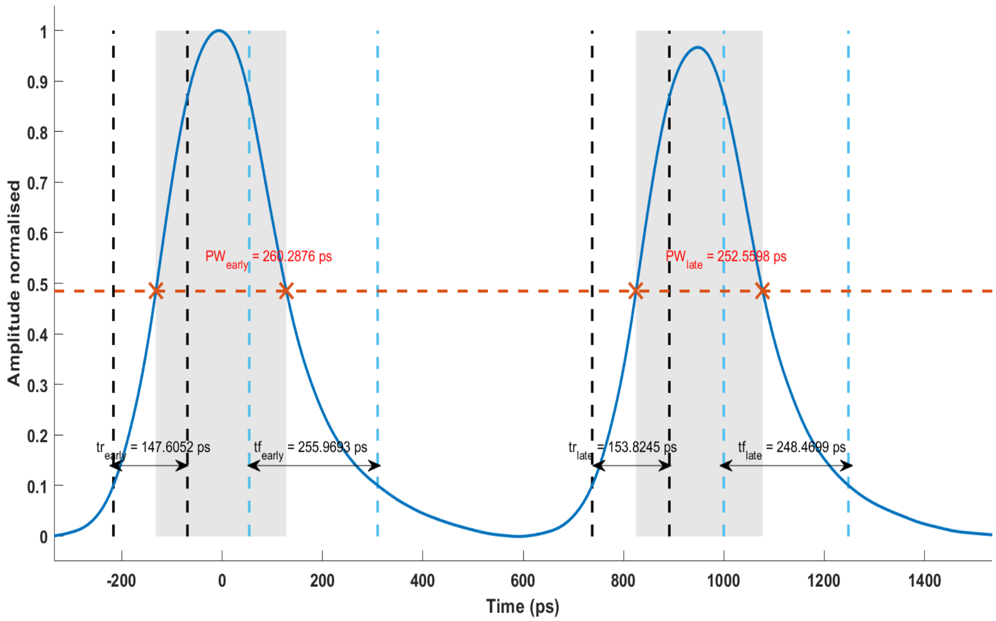


(a) $|e\rangle$ state from Alice. PW_{early}: pulsewidth of the $|e\rangle$ state; tr_{early}: risetime of the $|e\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state.

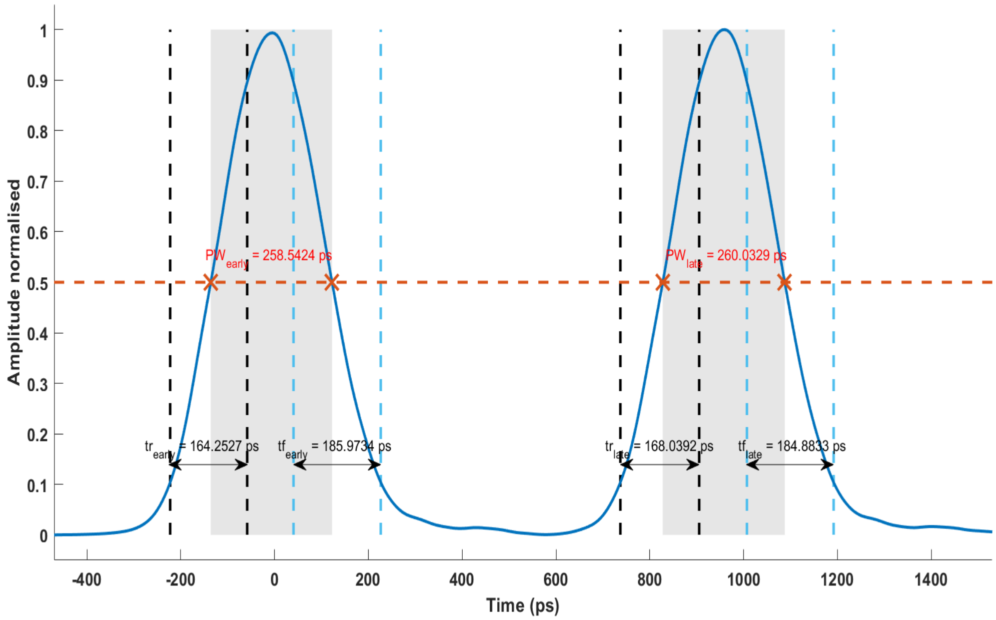


(b) $|e\rangle$ state from Bob. PW_{early}: pulsewidth of the $|e\rangle$ state; tr_{early}: risetime of the $|e\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state.

Figure 6.8: Temporal mode characterisation of $|e\rangle$ states from Alice and Bob.



(a) $|+\rangle$ state from Alice. PW_{early}: pulsewidth of the $|e\rangle$ state; PW_{late}: pulsewidth of the $|l\rangle$ state; tr_{early}: risetime of the $|e\rangle$ state; tr_{late}: risetime of the $|l\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state.



(b) $|+\rangle$ state from Bob. PW_{early}: pulsewidth of the $|e\rangle$ state; PW_{late}: pulsewidth of the $|l\rangle$ state; tr_{early}: risetime of the $|e\rangle$ state; tr_{late}: risetime of the $|l\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state; tf_{early}: falltime of the $|e\rangle$ state.

Figure 6.9: Temporal mode characterisation of $|+\rangle$ states from Alice and Bob.

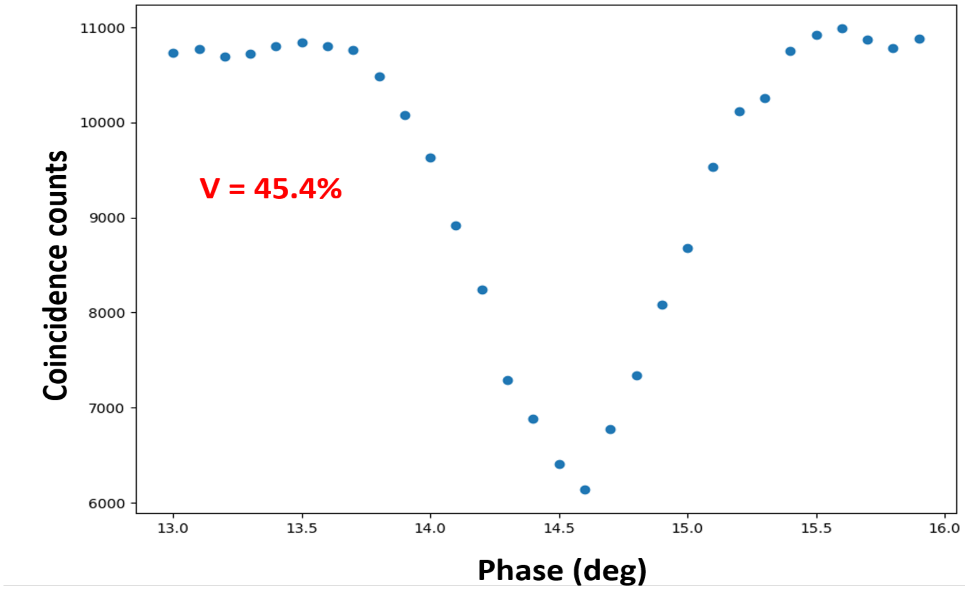
State	Parameter	Alice's value (ps)	Bob's value (ps)
$\|e\rangle$	Pulse width	263	260
	Rise time	157	170
	Fall time	235	184
$\|+\rangle$	Temporal mode separation	955	960
$\|e\rangle$ in $\|+\rangle$	Pulse width	260	258
	Rise time	147	164
	Fall time	255	185
$\|l\rangle$ in $\|+\rangle$	Pulse width	252	260
	Rise time	153	168
	Fall time	248	184

Table 6.3: Characteristics of different temporal modes from Alice and Bob.

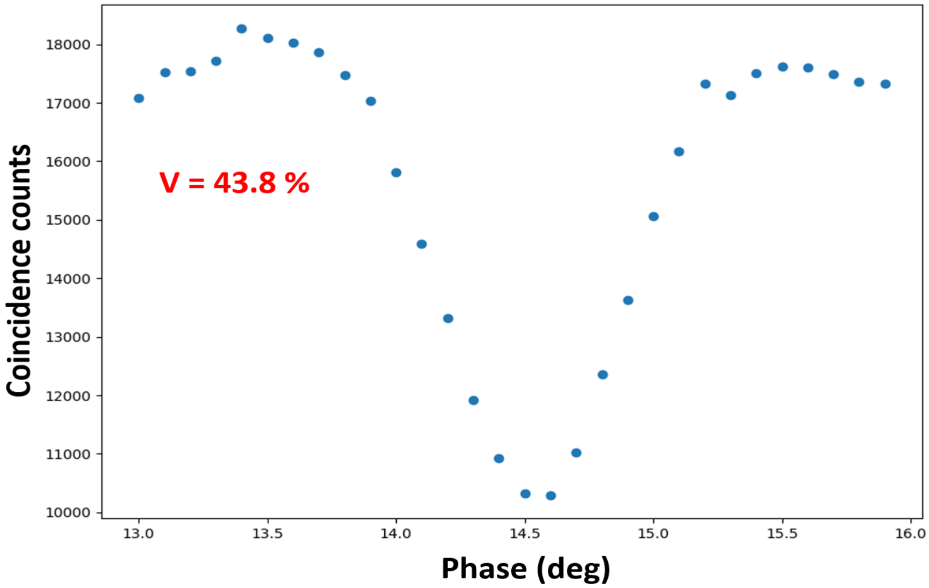
6.4.3 HOM interference measurement

After characterisation of individual qubits from Alice and Bob, we perform a HOM measurement to verify their degree of indistinguishability. In most of the QKD experiments, qubits prepared in the Z basis will have higher indistinguishability compared to X basis qubits. HOM visibility is the figure of merit for indistinguishability. We perform visibility measurement in the Z basis (X basis) by preparing $|e\rangle$ states ($|+\rangle$ state) at Alice and Bob and sending them to Charlie. At Charlie, we overlap them on the PMBS and detect them using the SNSPDs. We then investigate coincidence detections using the electronic HOM board. Before performing the HOM measurement, we make sure that we set the mean photon numbers at Alice and Bob in such a way that they are same at the PMBS. Figure 6.10 shows the visibility curve for both the Z basis and X basis. Visibility measurements in both the bases yielded values of $43\% - 45\%$ instead of 50%. As of now, we suspect that the bandwidth of the electronic HOM board is limiting us to achieve 50% visibility.

In the future, we will thoroughly investigate the reasons for the discrepancy between the expected and measured visibilities of and perform MDIQKD coexisting with hundreds of gigabits or even terabits of classical communication per second. This will help us to deploy these system in metropolitan area quantum networks.



(a) HOM measurement in the Z basis. We send $|e\rangle$ state from both Alice and Bob to measure the visibility. The number of coincidences when qubits are distinguishable is ~ 11000 and when qubits are indistinguishable it is ~ 6000. This results in a visibility of 45%.



(b) HOM measurement in the X basis. We send $|+\rangle$ states from both Alice and Bob to measure the visibility. The number of coincidences when qubits are distinguishable is ~ 17800 and when qubits are indistinguishable it is ~ 10000. This results in a visibility of 43.8%.

Figure 6.10: HOM measurements in both Z basis and X basis.

Chapter 7

Summary

The main goal of this thesis was to realise an MDIQKD system without the need for a dark channel, which will enable us to build a cost-effective metropolitan quantum network. Towards this goal, we have experimentally demonstrated MDIQKD coexisting with five 10 Gbps bi-directional classical communication channels over a 40 km fibre at around 1550 nm, which verifies that quantum networks can utilise the existing classical infrastructure and thus be implemented more economically. Taking this one step further, we investigated what would be the most suitable wavelengths for quantum communication considering classical communication networks operating in the C-band. We found that moving the quantum channel from third (1550 nm) to the second (1310 nm) telecommunication window would allow MDIQKD to work simultaneously with classical communication with rates of more than 10 terabits per second (Tbps).

In addition, we examined the shortcomings of our previously realised MDIQKD systems and devised improvements such that the system we are currently commissioning features a 200 MHz repetition rate, which is a 10-fold increased repetition rate as compared with the 20 MHz of previous systems, as well as enhanced control and improved reliability. Moreover, we now employ 1310 nm wavelength for quantum communication, we may achieve quantum communication coexisting with classical communication of Tbps rates. We fully characterised all parts of the new systems and qubits produced in different bases. Finally, we performed HOM measurements using the new system and obtained visibility values of 43% - 45% in both Z and X basis. This ensures that we can utilise these systems for the distribution of secret keys. Hence, this thesis has contributed to overall goal of developing MDIQKD systems that equip us to establish quantum metropolitan network economically.

Chapter 8

Outlook

Although we have applied our experience from past MDIQKD systems to realise a much-improved system that we should be able to readily deploy to realise a metropolitan quantum network, there remains a number of improvements. These are both of technical and more conceptual nature. On the technical side, the repetition rate of the current MDIQKD system is 200 MHz, which is comparable to other high-rate MDIQKD experiments [39, 41]. However, it needs to be increased to a few GHz so that the final secret key rate is comparable to prepare and measure QKD protocols [70]. All previous demonstrations of MDIQKD have been performed over fibre links; however, it is highly desirable to demonstrate it over a hybrid link, where one link is fibre, and another is free-space. This would enable us to combine ground-based and satellite quantum communication networks.

A more fundamental aspect relates to the use of coherent sources in MDIQKD demonstrations because of their availability and ease of operation. It is useful to investigate the possibility of using semiconductor-based single-photon sources, such as quantum dots, for MDIQKD [95]. Using the single-photon sources for MDIQKD removes the need for decoy-states and allows a significant increase in the secret key rate per pulse. However, it is worth noting that there are difficulties involved in making (even manufacturing) these sources and in particular to make them indistinguishable. As an intermediate step, one could think of using two different sources for MDIQKD, e.g. one of the sources could be a coherent source and another a quantum dot.

While an MDIQKD network involving three users has been demonstrated already [37], it is essential to realise MDIQKD network with many users. Some of the critical questions, such as simultaneous key distillation among users, should be addressed. Memory-assisted MDIQKD was proposed in 2014 [96, 97] which involves storing a photon from a sender in a quantum memory and retrieving it to take part in the Bell state measurement. Recently, it has been experimentally demonstrated in SiV centres [98]. However, the demonstration at telecommunication wavelengths is highly desired as it increases the secret key rate and extends the distance between users.

Thinking beyond MDIQKD, previous demonstrations of teleportation towards an elementary link of a quantum repeater have involved separate fibres for quantum and classical communication. An exciting investigation would be to demonstrate teleportation of a photon from an MDIQKD sender system into a quantum memory coexisting with classical communication. As MDIQKD and an elementary link of a quantum repeater share a similar architecture, this demonstration can be a step towards building a cost-effective quantum repeater.

Bibliography

[1] R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. Stern, J. A. Slater, D. Oblak, *et al.*, "Efficient bell state analyzer for time-bin qubits with fast-recovery wsi superconducting single photon detectors," *Optics express*, vol. 22, no. 20, pp. 24497–24506, 2014.

[2] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, p. 022320, 2006.

[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, p. 686, 2010.

[4] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A*, vol. 78, no. 4, p. 042333, 2008.

[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, p. 230501, 2007.

[6] C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, no. 19, pp. 3762–3764, 2004.

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

[8] R. Valivarthi *et al.*, "Measurement-device-independent quantum key distribution: from idea towards application," *Journal of Modern Optics*, vol. 62, no. 14, pp. 1141–1150, 2015.

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

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

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

[12] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of qkd integration in metropolitan area networks," *Optics express*, vol. 23, no. 8, pp. 10359–10373, 2015.

[13] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.

[14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, p. 802, 1982.

[15] M. Koashi and A. Winter, “Monogamy of quantum entanglement and other correlations,” *Physical Review A*, vol. 69, no. 2, p. 022309, 2004.

[16] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing.,” *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

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

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

[19] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, *et al.*, “10-mb/s quantum key distribution,” *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[20] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, “Secure quantum key distribution over 421 km of optical fiber,” *Physical review letters*, vol. 121, no. 19, p. 190502, 2018.

[21] A. Dixon, J. Dynes, M. Lucamarini, B. Fröhlich, A. Sharpe, A. Plews, S. Tam, Z. Yuan, Y. Tanizawa, H. Sato, *et al.*, “High speed prototype quantum key distribution system and long term field trial,” *Optics express*, vol. 23, no. 6, pp. 7583–7592, 2015.

[22] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Avoiding the blinding attack in qkd,” *Nature Photonics*, vol. 4, no. 12, p. 801, 2010.

[23] Z. Yuan, J. Dynes, and A. Shields, “Avoiding the blinding attack in qkd,” *Nature Photonics*, vol. 4, no. 12, p. 800, 2010.

[24] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, “Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum

key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 192–196, 2015.

[25] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, *et al.*, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, p. 682, 2015.

[26] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, *et al.*, "Significant-loophole-free test of bell's theorem with entangled photons," *Physical review letters*, vol. 115, no. 25, p. 250401, 2015.

[27] D. Rauch, J. Handsteiner, A. Hochrainer, J. Gallicchio, A. S. Friedman, C. Leung, B. Liu, L. Bulla, S. Ecker, F. Steinlechner, *et al.*, "Cosmic bell test using random measurement settings from high-redshift quasars," *Physical review letters*, vol. 121, no. 8, p. 080403, 2018.

[28] B. B. T. Collaboration *et al.*, "Challenging local realism with human choices.," *Nature*, vol. 557, no. 7704, p. 212, 2018.

[29] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.

[30] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130502, 2012.

[31] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Physical Review Letters*, vol. 68, no. 5, p. 557, 1992.

[32] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Physical Review Letters*, vol. 111, no. 13, p. 130501, 2013.

[33] Y. Liu *et al.*, “Experimental measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 111, no. 13, p. 130502, 2013.

[34] T. F. Da Silva, D. Vitoreti, G. Xavier, G. Do Amaral, G. Temporao, and J. Von Der Weid, “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits,” *Physical Review A*, vol. 88, no. 5, p. 052303, 2013.

[35] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, “Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution,” *Physical review letters*, vol. 112, no. 19, p. 190503, 2014.

[36] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, “Measurement-device-independent quantum key distribution over 200 km,” *Physical review letters*, vol. 113, no. 19, p. 190501, 2014.

[37] Y.-L. Tang *et al.*, “Measurement-device-independent quantum key distribution over untrustful metropolitan network,” *Physical Review X*, vol. 6, no. 1, p. 011024, 2016.

[38] H.-L. Yin *et al.*, “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Physical Review Letters*, vol. 117, no. 19, p. 190501, 2016.

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

[40] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, “A cost-effective measurement-device-independent quantum

key distribution system for quantum networks," *Quantum Science and Technology*, vol. 2, no. 4, p. 04LT01, 2017.

[41] H. Semenenko, P. Sibson, M. G. Thompson, and C. Erven, "Integrated photonic devices for measurement-device-independent quantum key distribution," in *CLEO: QELS_Fundamental Science*, pp. FM4C–4, Optical Society of America, 2019.

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

[43] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication," *Physical Review Letters*, vol. 82, no. 12, p. 2594, 1999.

[44] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""event-ready-detectors"bell experiment via entanglement swapping," *Physical Review Letters*, vol. 71, no. 26, p. 4287, 1993.

[45] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[46] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[47] J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical bell-state analyzer," *Applied Physics B*, vol. 72, no. 1, pp. 67–71, 2001.

[48] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of trojan-horse attacks on practical quantum key distribution systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 168–177, 2014.

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

[50] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," *journal of modern optics*, vol. 51, no. 9-10, pp. 1267–1288, 2004.

[51] M. G. Tanner, V. Makarov, and R. H. Hadfield, "Optimised quantum hacking of superconducting nanowire single-photon detectors," *Optics express*, vol. 22, no. 6, pp. 6734–6748, 2014.

[52] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, no. 2, p. 022313, 2006.

[53] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080*, 2005.

[54] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, no. 4, p. 045021, 2009.

[55] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Communications of the ACM*, vol. 62, no. 4, pp. 133–133, 2019.

[56] A. Ekert and R. Renner, "The ultimate physical limits of privacy," *Nature*, vol. 507, no. 7493, p. 443, 2014.

[57] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, p. 419, 2014.

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

[59] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, *et al.*, "Strong loophole-free test of local realism," *Physical review letters*, vol. 115, no. 25, p. 250402, 2015.

[60] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, "Event-ready bell test using entangled atoms simultaneously closing detection and locality loopholes," *Physical review letters*, vol. 119, no. 1, p. 010402, 2017.

[61] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[62] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Physical Review A*, vol. 72, no. 1, p. 012322, 2005.

[63] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature communications*, vol. 3, p. 634, 2012.

[64] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.

[65] T.-T. Song, S.-J. Qin, Q.-Y. Wen, Y.-K. Wang, and H.-Y. Jia, "Finite-key security analyses on passive decoy-state qkd protocols with different unstable sources," *Scientific reports*, vol. 5, p. 15276, 2015.

[66] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, "Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources," *Physical Review A*, vol. 94, no. 3, p. 032335, 2016.

[67] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography Conference*, pp. 407–425, Springer, 2005.

[68] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, "Three-intensity decoy-state method for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 88, no. 6, p. 062339, 2013.

[69] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%," *Physical Review A*, vol. 89, no. 5, p. 052325, 2014.

[70] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 ghz time-bin quantum key distribution," *Applied Physics Letters*, vol. 112, no. 17, p. 171108, 2018.

[71] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, *et al.*, "10-mb/s quantum key distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[72] A. Yeniay, J.-M. Delavaux, and J. Toulouse, "Spontaneous and stimulated brillouin scattering gain spectra in optical fibers," *Journal of lightwave technology*, vol. 20, no. 8, p. 1425, 2002.

[73] R. H. Stolen, J. P. Gordon, W. Tomlinson, and H. A. Haus, "Raman response function of silica-core fibers," *JOSA B*, vol. 6, no. 6, pp. 1159–1166, 1989.

[74] J. Zhou, K. Tajima, K. Nakajima, K. Kurokawa, C. Fukai, T. Matsui, and I. Sankawa, "Progress on low loss photonic crystal fibers," *Optical Fiber Technology*, vol. 11, no. 2, pp. 101–110, 2005.

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

[76] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[77] W. T. N. Gisin, G. Ribordy and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, p. 145, 2002.

[78] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pp. 517–526, IEEE, 2009.

[79] M. F. Riedel, D. Binosi, R. Thew, and T. Calarco, "The european quantum technologies flagship programme," *Quantum Science and Technology*, vol. 2, no. 3, p. 030501, 2017.

[80] A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding," *Nature*, vol. 378, no. 6556, p. 449, 1995.

[81] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Violation of bell inequalities by photons more than 10 km apart," *Physical Review Letters*, vol. 81, no. 17, p. 3563, 1998.

[82] R. Valivarthi, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "Quantum teleportation across a metropolitan fibre network," *Nature Photonics*, vol. 10, no. 10, p. 676, 2016.

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

[84] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. Yuan, and A. J. Shields, “Quantum secured gigabit optical access networks,” *Scientific reports*, vol. 5, p. 18121, 2015.

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

[86] T. A. Eriksson, T. Hirano, M. Ono, M. Fujiwara, R. Namiki, K.-i. Yoshino, A. Tajima, M. Takeoka, and M. Sasaki, “Coexistence of continuous variable quantum key distribution and 7×12.5 gbit/s classical channels,” *arXiv preprint arXiv:1809.01287*, 2018.

[87] A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” *Optics express*, vol. 15, no. 15, pp. 9388–9393, 2007.

[88] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[89] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, “Modeling a measurement-device-independent quantum key distribution system,” *Optics express*, vol. 22, no. 11, pp. 12716–12736, 2014.

[90] F. Xu, H. Xu, and H.-K. Lo, “Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution,” *Physical Review A*, vol. 89, no. 5, p. 052333, 2014.

[91] M. S. Allman *et al.*, “A near-infrared 64-pixel superconducting nanowire single photon detector array with integrated multiplexed readout,” *Applied Physics Letters*, vol. 106, no. 19, p. 192601, 2015.

[92] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, no. 3, p. 032314, 2007.

[93] R. Drever, J. L. Hall, F. Kowalski, J. Hough, G. Ford, A. Munley, and H. Ward, "Laser phase and frequency stabilization using an optical resonator," *Applied Physics B*, vol. 31, no. 2, pp. 97–105, 1983.

[94] S. Sudo, Y. Sakai, H. Yasaka, and T.-S. IKEGAMI, "Frequency stabilization of 1.55-μm dfb laser diode using vibrational-rotational absorption of 13 c 2 h 2 molecules," in *Optical Fiber Communication Conference*, p. THE5, Optical Society of America, 1990.

[95] Y.-H. Zhou, Z.-W. Yu, A. Li, X.-L. Hu, C. Jiang, and X.-B. Wang, "Measurement-device-independent quantum key distribution via quantum blockade," *Scientific reports*, vol. 8, no. 1, p. 4115, 2018.

[96] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 16, no. 4, p. 043005, 2014.

[97] N. L. Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," *IEEE Journal of selected topics in quantum electronics*, vol. 21, no. 3, pp. 138–147, 2014.

[98] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, *et al.*, "Experimental demonstration of memory-enhanced quantum communication," *arXiv preprint arXiv:1909.01323*, 2019.

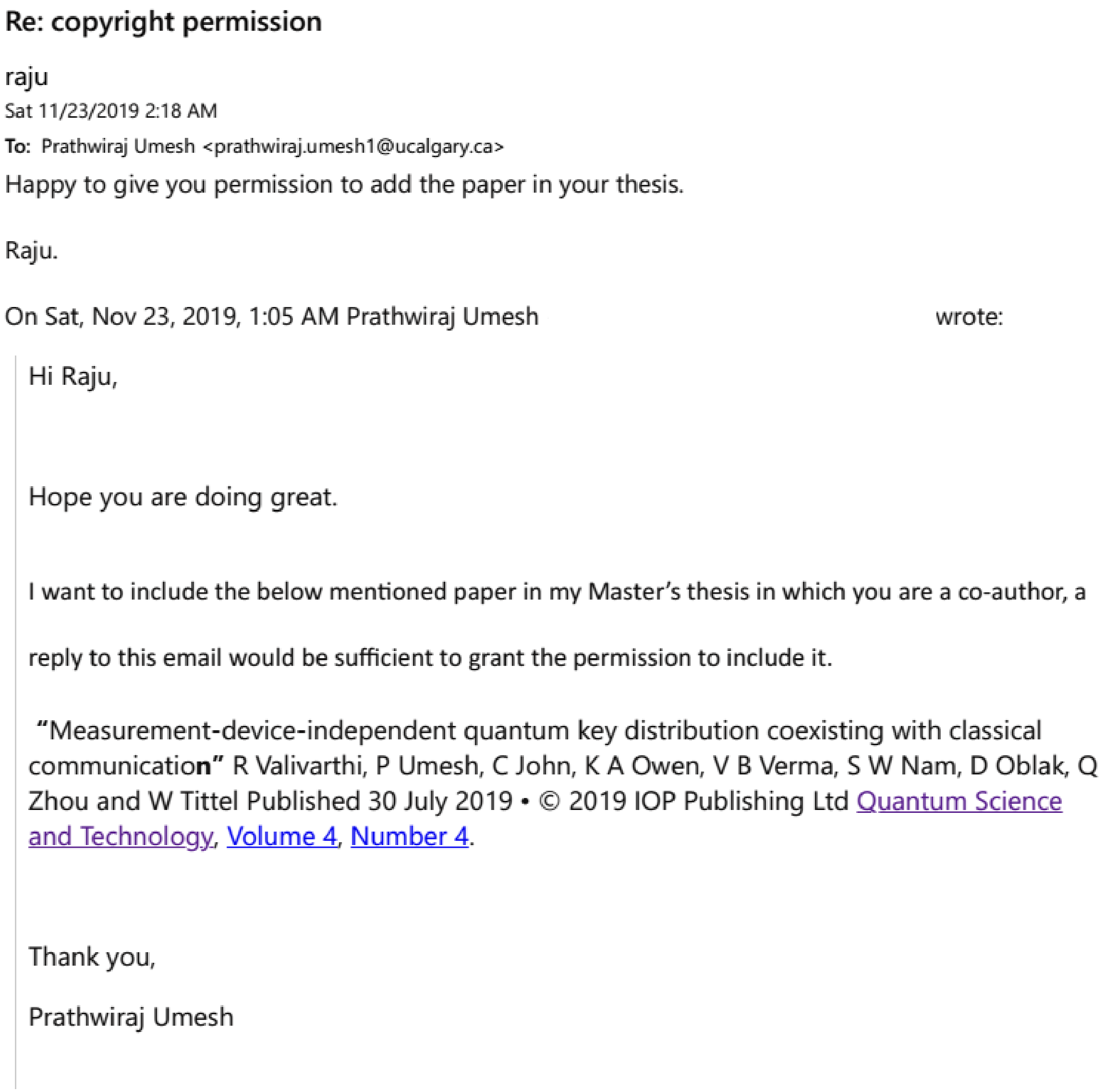
Appendix A

Copyright permissions

A.1 List of co-authors

This section of the appendix states the permission from the co-authors of the paper "Measurement-device-independent quantum key distribution coexisting with classical communication" to include the paper in my thesis.

- Raju Valivarthi
- Caleb Johm
- Kim Owen
- Varun Verma
- Sae Woo Nam
- Daniel Oblak
- Qiang Chou
- Wolfgang Tittel



Re: copyright permission

raju
Sat 11/23/2019 2:18 AM
To: Prathwiraj Umesh <prathwiraj.umesh1@ucalgary.ca>

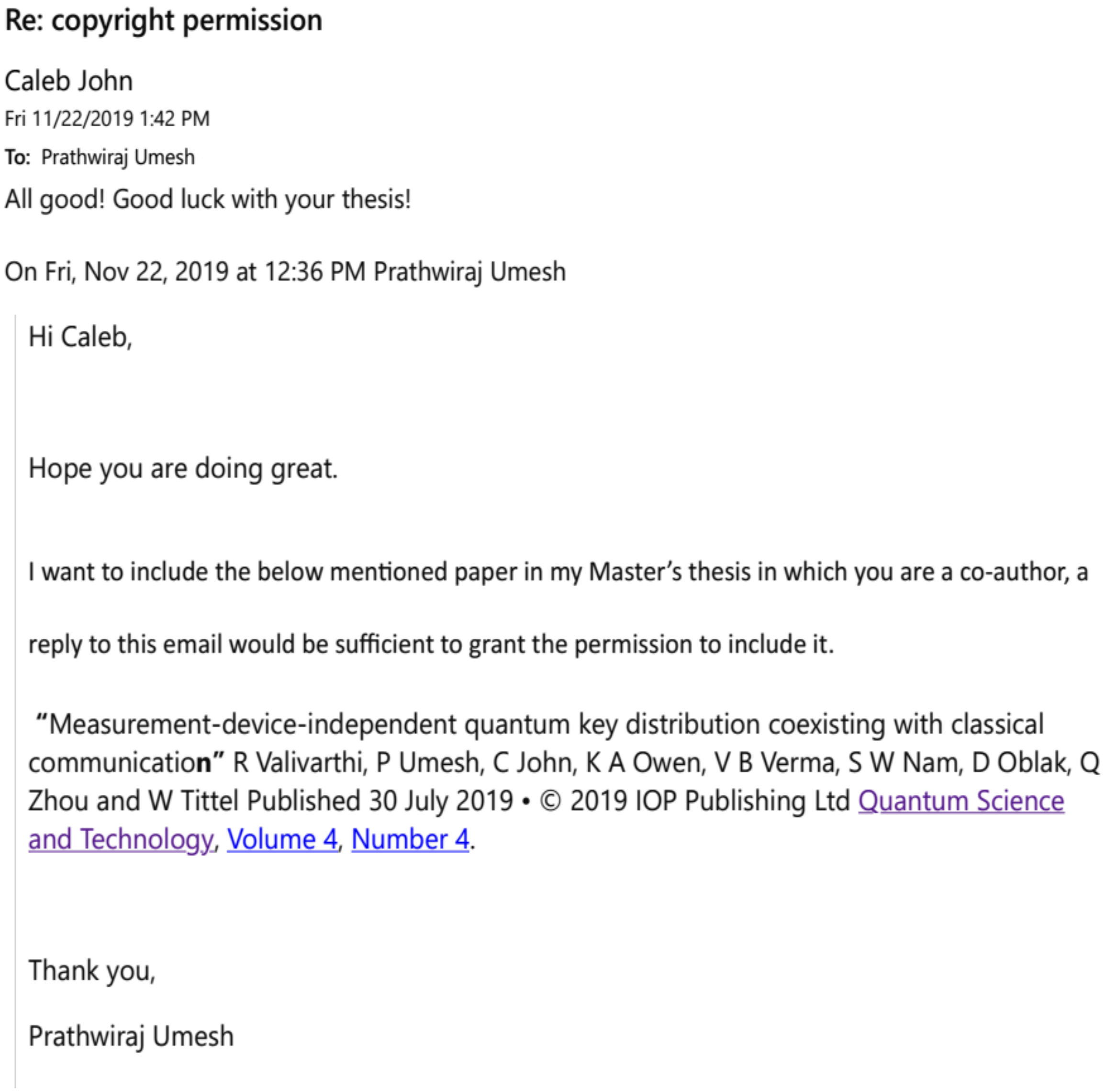
Happy to give you permission to add the paper in your thesis.

Raju.

On Sat, Nov 23, 2019, 1:05 AM Prathwiraj Umesh wrote:

> Hi Raju,
>
> Hope you are doing great.
>
> I want to include the below mentioned paper in my Master’s thesis in which you are a co-author, a
>
> reply to this email would be sufficient to grant the permission to include it.
>
> **“**Measurement-device-independent quantum key distribution coexisting with classical communicatio**n”** R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.
>
> Thank you,
>
> Prathwiraj Umesh

Figure A.1: Copyright permission from Raju Valivarthi



Re: copyright permission

Caleb John

Fri 11/22/2019 1:42 PM

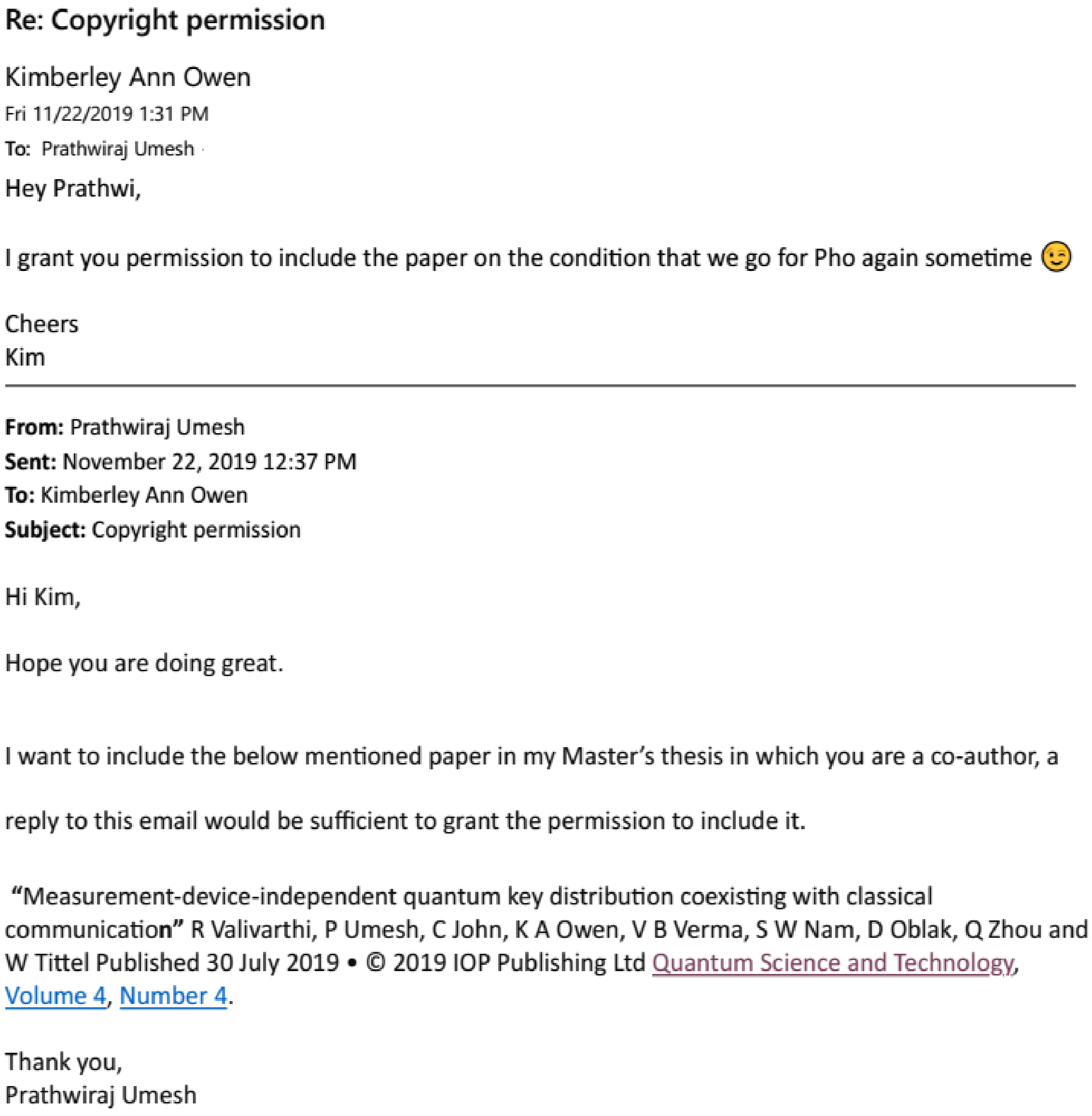
To: Prathwiraj Umesh

All good! Good luck with your thesis!

On Fri, Nov 22, 2019 at 12:36 PM Prathwiraj Umesh

> Hi Caleb,
>
> Hope you are doing great.
>
> I want to include the below mentioned paper in my Master's thesis in which you are a co-author, a
>
> reply to this email would be sufficient to grant the permission to include it.
>
> **"**Measurement-device-independent quantum key distribution coexisting with classical communicatio**n"** R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.
>
> Thank you,
>
> Prathwiraj Umesh

Figure A.2: Copyright permission from Caleb John



Re: Copyright permission

Kimberley Ann Owen

Fri 11/22/2019 1:31 PM

To: Prathwiraj Umesh

Hey Prathwi,

I grant you permission to include the paper on the condition that we go for Pho again sometime 😉

Cheers
Kim

From: Prathwiraj Umesh
Sent: November 22, 2019 12:37 PM
To: Kimberley Ann Owen
Subject: Copyright permission

Hi Kim,

Hope you are doing great.

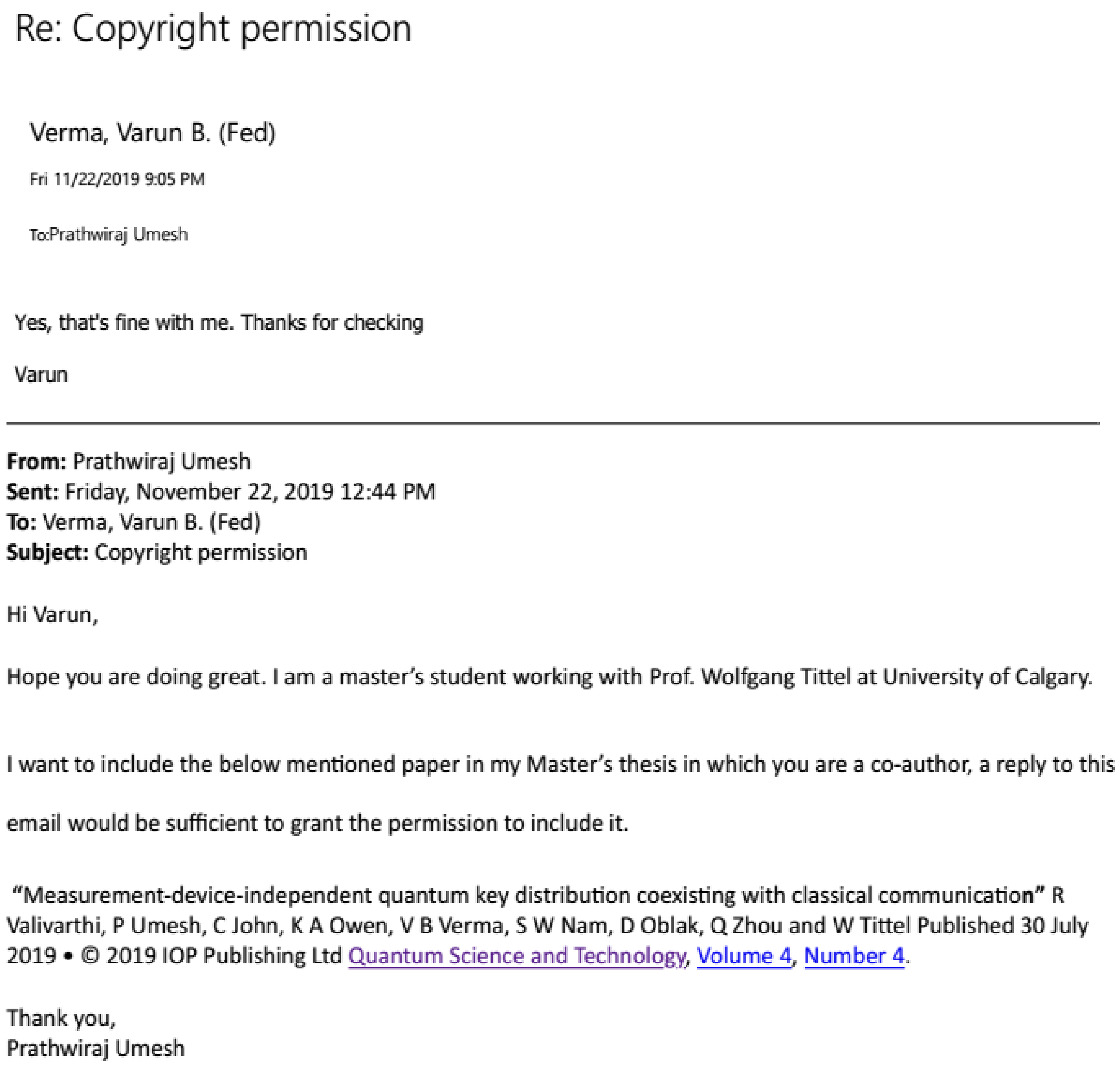
I want to include the below mentioned paper in my Master's thesis in which you are a co-author, a

reply to this email would be sufficient to grant the permission to include it.

"Measurement-device-independent quantum key distribution coexisting with classical communication**"** R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.

Thank you,
Prathwiraj Umesh

Figure A.3: Copyright permission from Kim Owen



Re: Copyright permission

Verma, Varun B. (Fed)

Fri 11/22/2019 9:05 PM

To:Prathwiraj Umesh

Yes, that's fine with me. Thanks for checking

Varun

From: Prathwiraj Umesh
Sent: Friday, November 22, 2019 12:44 PM
To: Verma, Varun B. (Fed)
Subject: Copyright permission

Hi Varun,

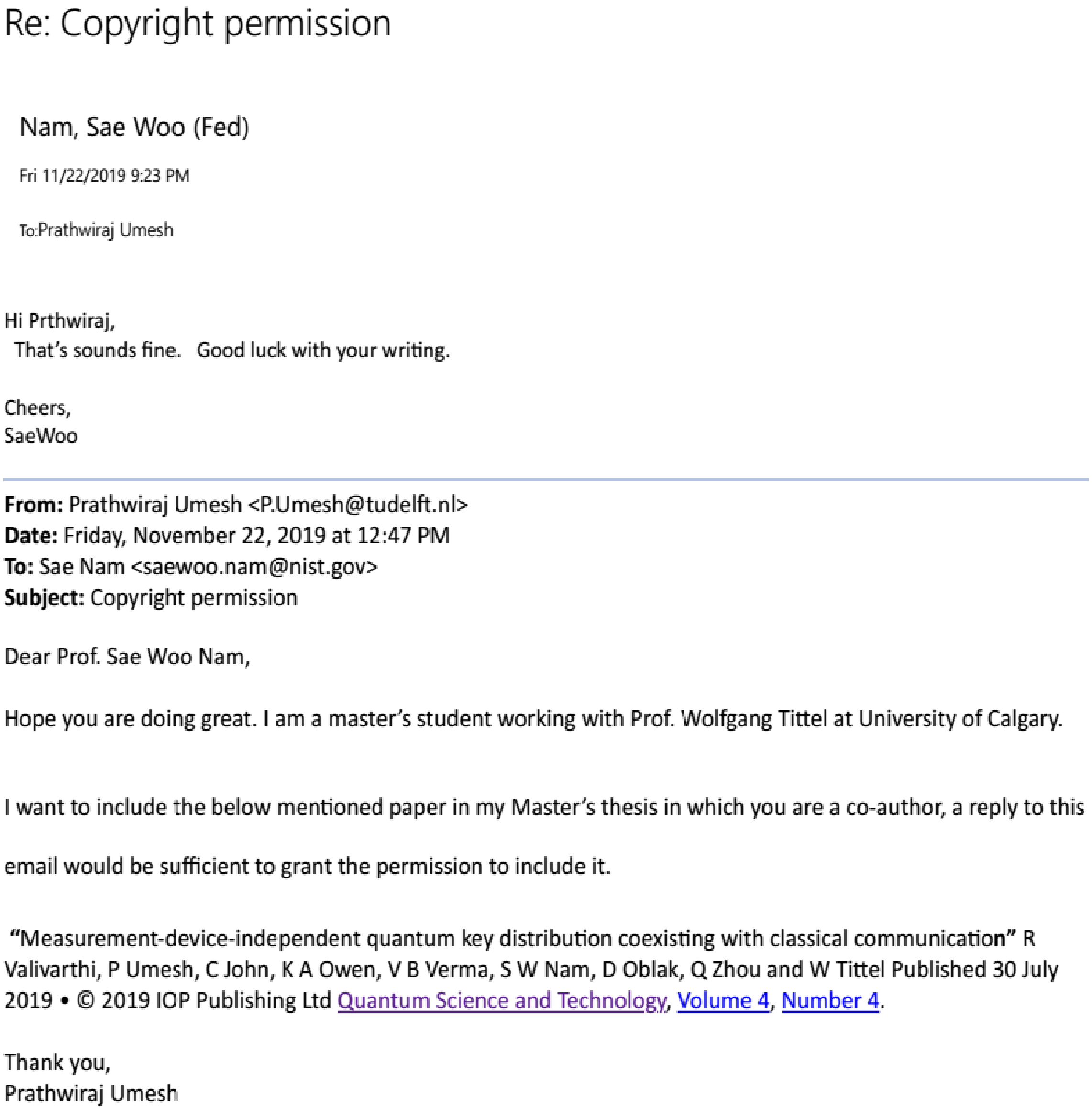
Hope you are doing great. I am a master's student working with Prof. Wolfgang Tittel at University of Calgary.

I want to include the below mentioned paper in my Master's thesis in which you are a co-author, a reply to this email would be sufficient to grant the permission to include it.

"Measurement-device-independent quantum key distribution coexisting with classical communication" R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.

Thank you,
Prathwiraj Umesh

Figure A.4: Copyright permission from Varun Verma



Re: Copyright permission

Nam, Sae Woo (Fed)

Fri 11/22/2019 9:23 PM

To:Prathwiraj Umesh

Hi Prthwiraj,
That's sounds fine.   Good luck with your writing.

Cheers,
SaeWoo

From: Prathwiraj Umesh <P.Umesh@tudelft.nl>
Date: Friday, November 22, 2019 at 12:47 PM
To: Sae Nam <saewoo.nam@nist.gov>
Subject: Copyright permission

Dear Prof. Sae Woo Nam,

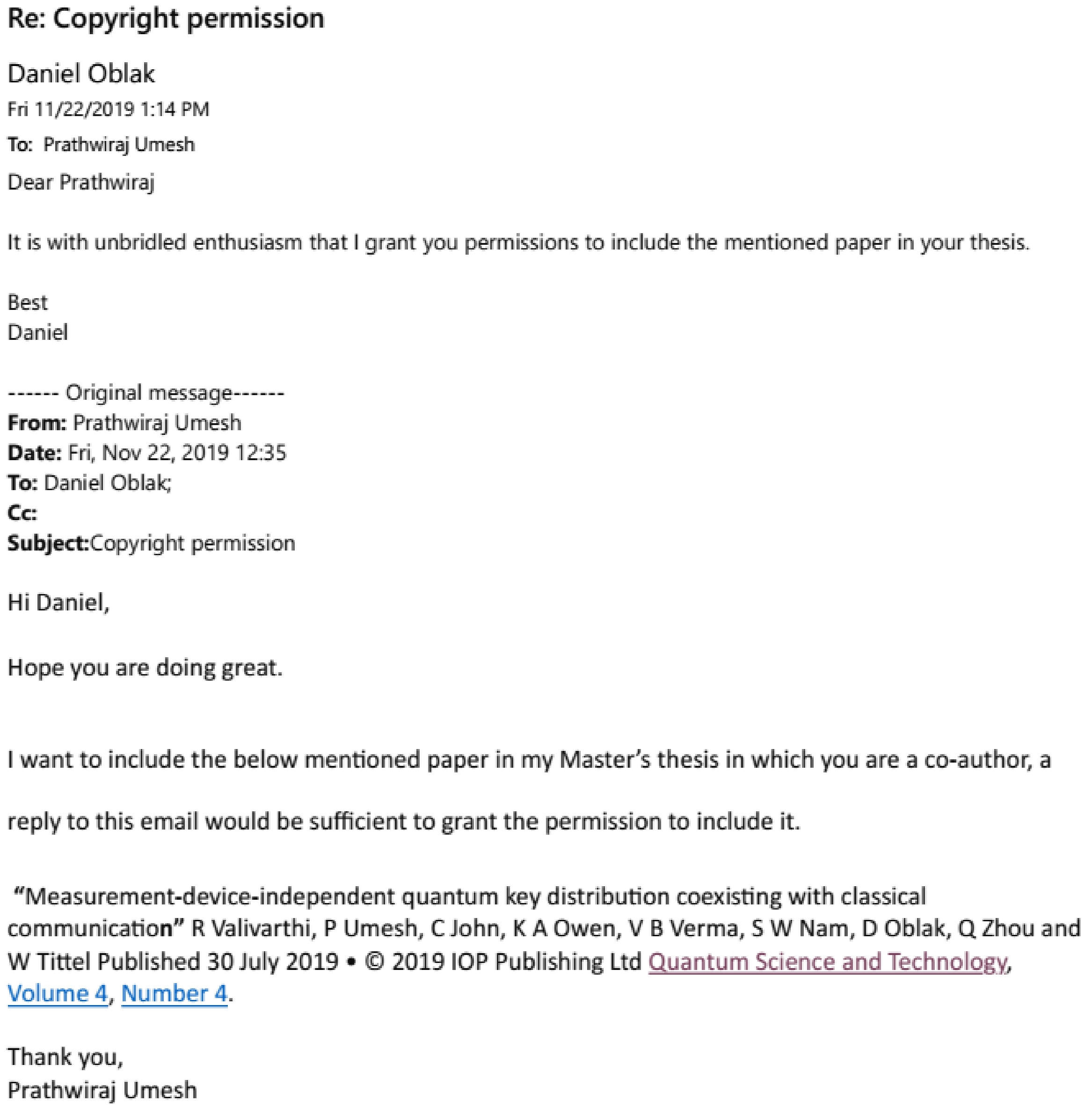
Hope you are doing great. I am a master's student working with Prof. Wolfgang Tittel at University of Calgary.

I want to include the below mentioned paper in my Master's thesis in which you are a co-author, a reply to this email would be sufficient to grant the permission to include it.

"Measurement-device-independent quantum key distribution coexisting with classical communicatio**n"** R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.

Thank you,
Prathwiraj Umesh

Figure A.5: Copyright permission from Prof. Sae Woo Nam



Re: Copyright permission

Daniel Oblak
Fri 11/22/2019 1:14 PM
To: Prathwiraj Umesh

Dear Prathwiraj

It is with unbridled enthusiasm that I grant you permissions to include the mentioned paper in your thesis.

Best
Daniel

------ Original message------
From: Prathwiraj Umesh
Date: Fri, Nov 22, 2019 12:35
To: Daniel Oblak;
Cc:
Subject: Copyright permission

Hi Daniel,

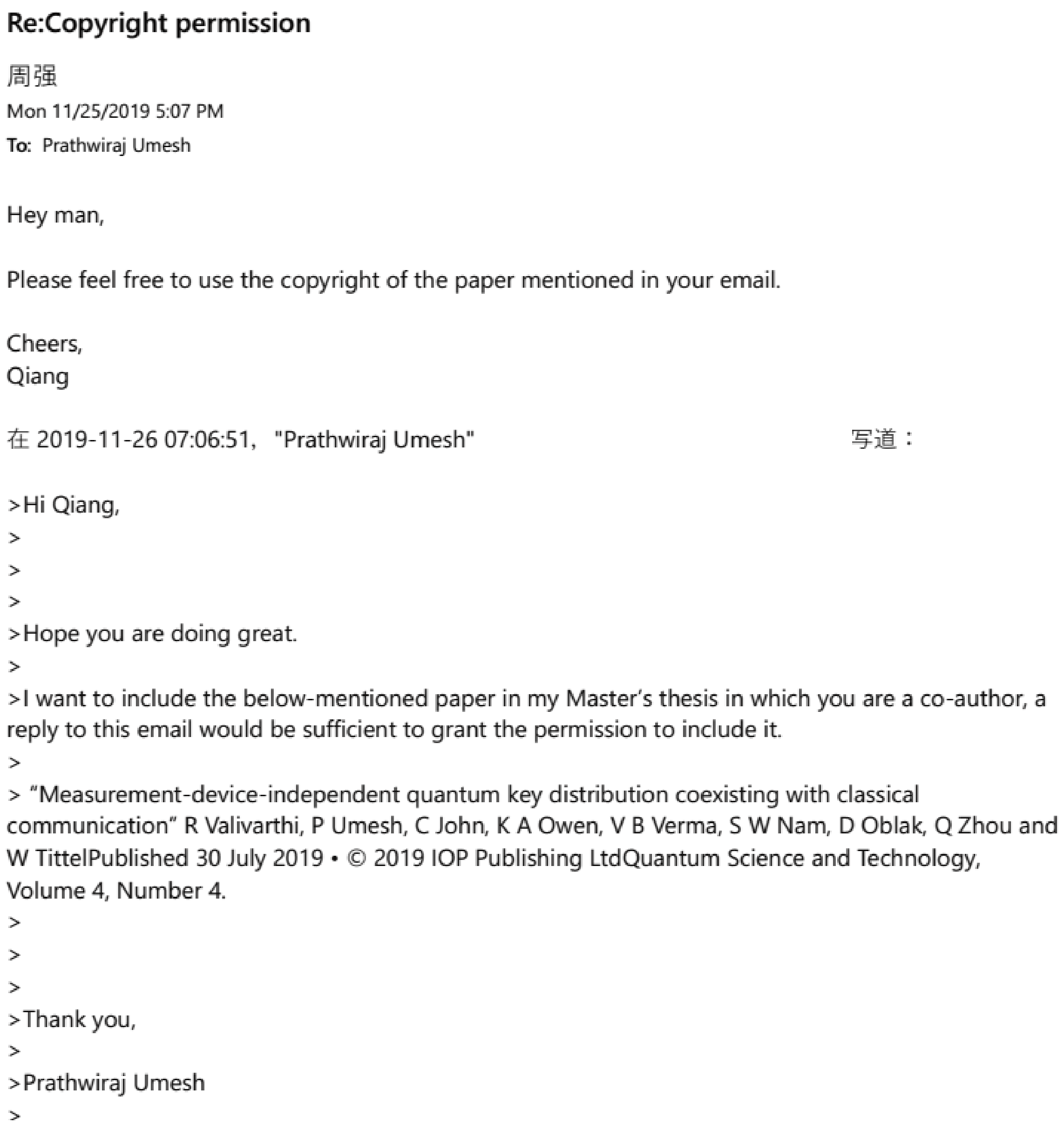
Hope you are doing great.

I want to include the below mentioned paper in my Master's thesis in which you are a co-author, a reply to this email would be sufficient to grant the permission to include it.

"Measurement-device-independent quantum key distribution coexisting with classical communication" R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.

Thank you,
Prathwiraj Umesh

Figure A.6: Copyright permission from Daniel Oblak



Re:Copyright permission

周强

Mon 11/25/2019 5:07 PM

To: Prathwiraj Umesh

Hey man,

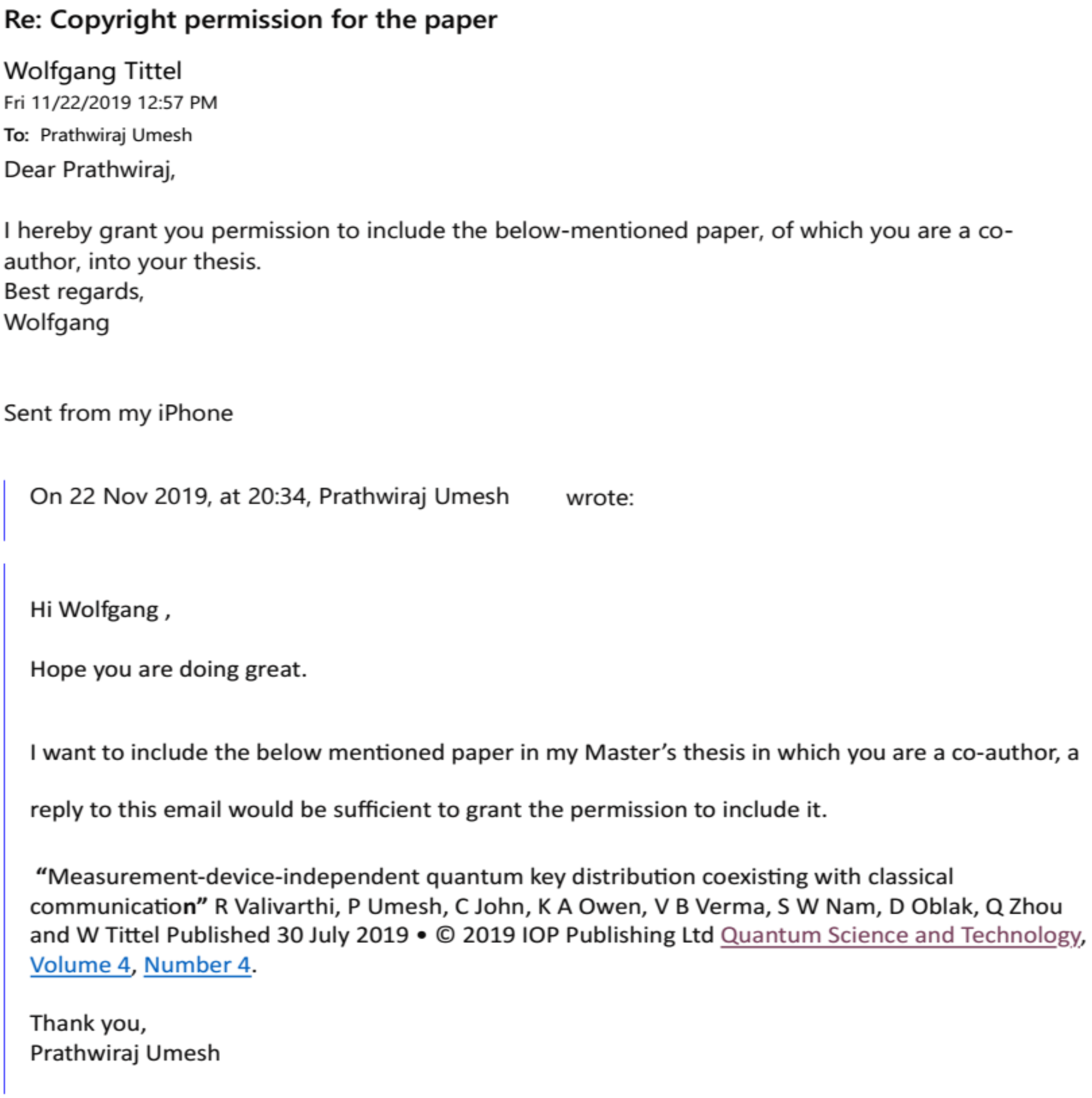
Please feel free to use the copyright of the paper mentioned in your email.

Cheers,
Qiang

在 2019-11-26 07:06:51，"Prathwiraj Umesh" 写道：

>Hi Qiang,
>
>
>
>Hope you are doing great.
>
>I want to include the below-mentioned paper in my Master’s thesis in which you are a co-author, a reply to this email would be sufficient to grant the permission to include it.
>
> “Measurement-device-independent quantum key distribution coexisting with classical communication” R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W TittelPublished 30 July 2019 • © 2019 IOP Publishing LtdQuantum Science and Technology, Volume 4, Number 4.
>
>
>
>Thank you,
>
>Prathwiraj Umesh
>

Figure A.7: Copyright permission from Qiang Zhou



Re: Copyright permission for the paper

Wolfgang Tittel
Fri 11/22/2019 12:57 PM
To: Prathwiraj Umesh

Dear Prathwiraj,

I hereby grant you permission to include the below-mentioned paper, of which you are a co-author, into your thesis.
Best regards,
Wolfgang

Sent from my iPhone

> On 22 Nov 2019, at 20:34, Prathwiraj Umesh wrote:

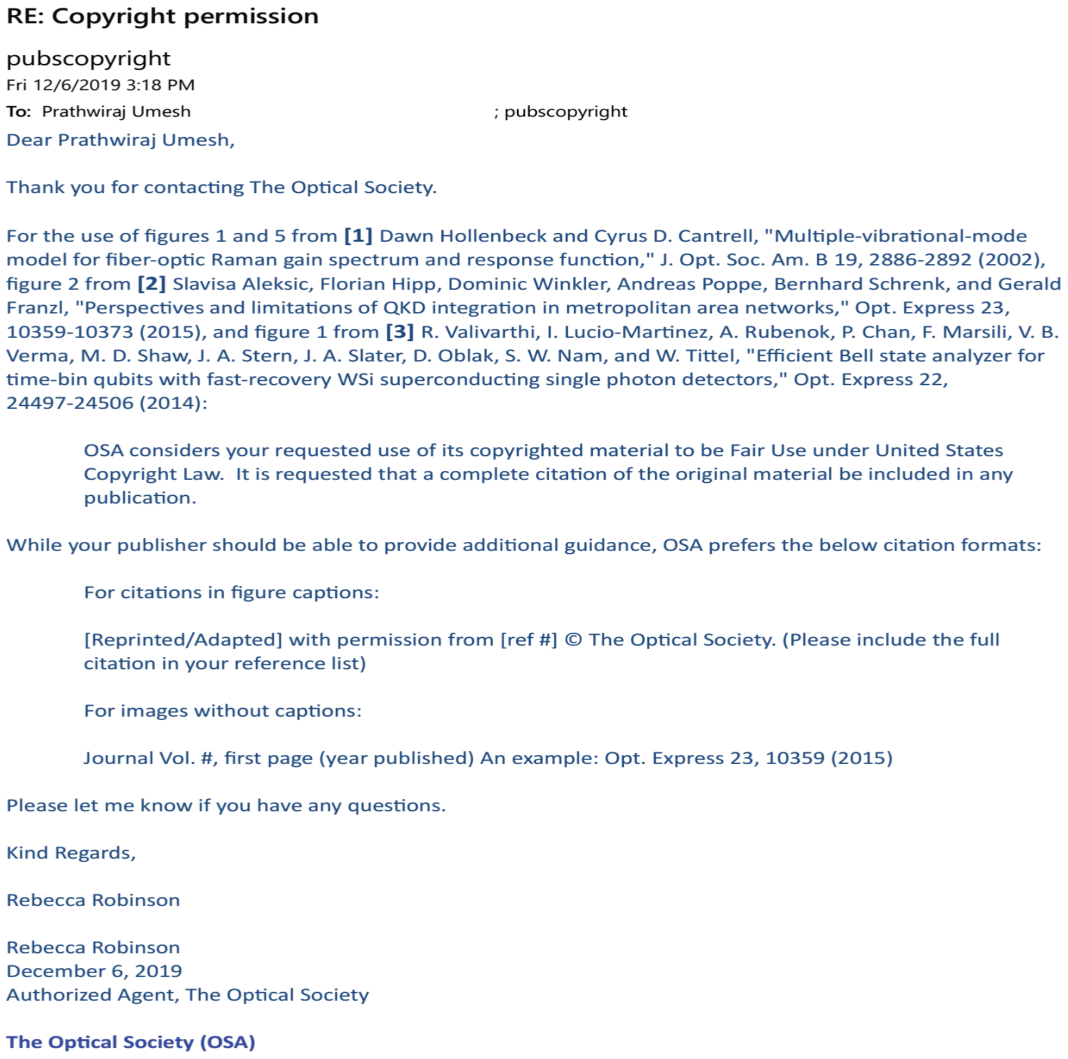
> Hi Wolfgang ,
>
> Hope you are doing great.
>
> I want to include the below mentioned paper in my Master’s thesis in which you are a co-author, a
>
> reply to this email would be sufficient to grant the permission to include it.
>
> **“**Measurement-device-independent quantum key distribution coexisting with classical communicatio**n”** R Valivarthi, P Umesh, C John, K A Owen, V B Verma, S W Nam, D Oblak, Q Zhou and W Tittel Published 30 July 2019 • © 2019 IOP Publishing Ltd Quantum Science and Technology, Volume 4, Number 4.
>
> Thank you,
> Prathwiraj Umesh

Figure A.8: Copyright permission from Prof. Wolfgang Tittel

A.2 Copyright permission to include figures

This section of the appendix states the permission to include the following figures in my thesis from various research papers.

- The figure 2.2 is take from [1].



RE: Copyright permission

pubscopyright
Fri 12/6/2019 3:18 PM
To: Prathwiraj Umesh ; pubscopyright

Dear Prathwiraj Umesh,

Thank you for contacting The Optical Society.

For the use of figures 1 and 5 from **[1]** Dawn Hollenbeck and Cyrus D. Cantrell, "Multiple-vibrational-mode model for fiber-optic Raman gain spectrum and response function," J. Opt. Soc. Am. B 19, 2886-2892 (2002), figure 2 from **[2]** Slavisa Aleksic, Florian Hipp, Dominic Winkler, Andreas Poppe, Bernhard Schrenk, and Gerald Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," Opt. Express 23, 10359-10373 (2015), and figure 1 from **[3]** R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, and W. Tittel, "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," Opt. Express 22, 24497-24506 (2014):

> OSA considers your requested use of its copyrighted material to be Fair Use under United States Copyright Law. It is requested that a complete citation of the original material be included in any publication.

While your publisher should be able to provide additional guidance, OSA prefers the below citation formats:

> For citations in figure captions:
>
> [Reprinted/Adapted] with permission from [ref #] © The Optical Society. (Please include the full citation in your reference list)
>
> For images without captions:
>
> Journal Vol. #, first page (year published) An example: Opt. Express 23, 10359 (2015)

Please let me know if you have any questions.

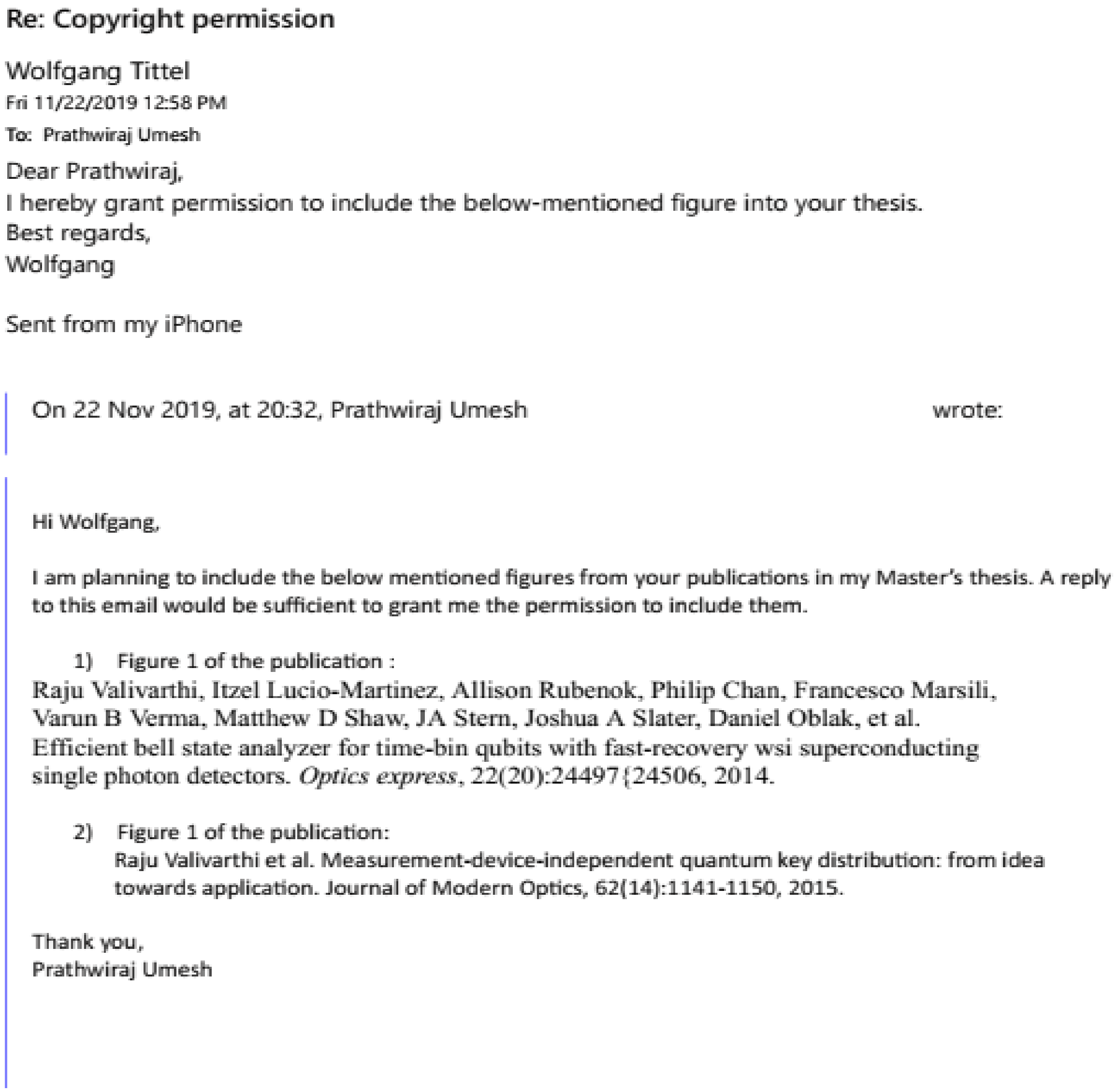
Kind Regards,

Rebecca Robinson

Rebecca Robinson
December 6, 2019
Authorized Agent, The Optical Society

The Optical Society (OSA)

Figure A.9: Copyright permission from OSA.



Re: Copyright permission

Wolfgang Tittel
Fri 11/22/2019 12:58 PM
To: Prathwiraj Umesh

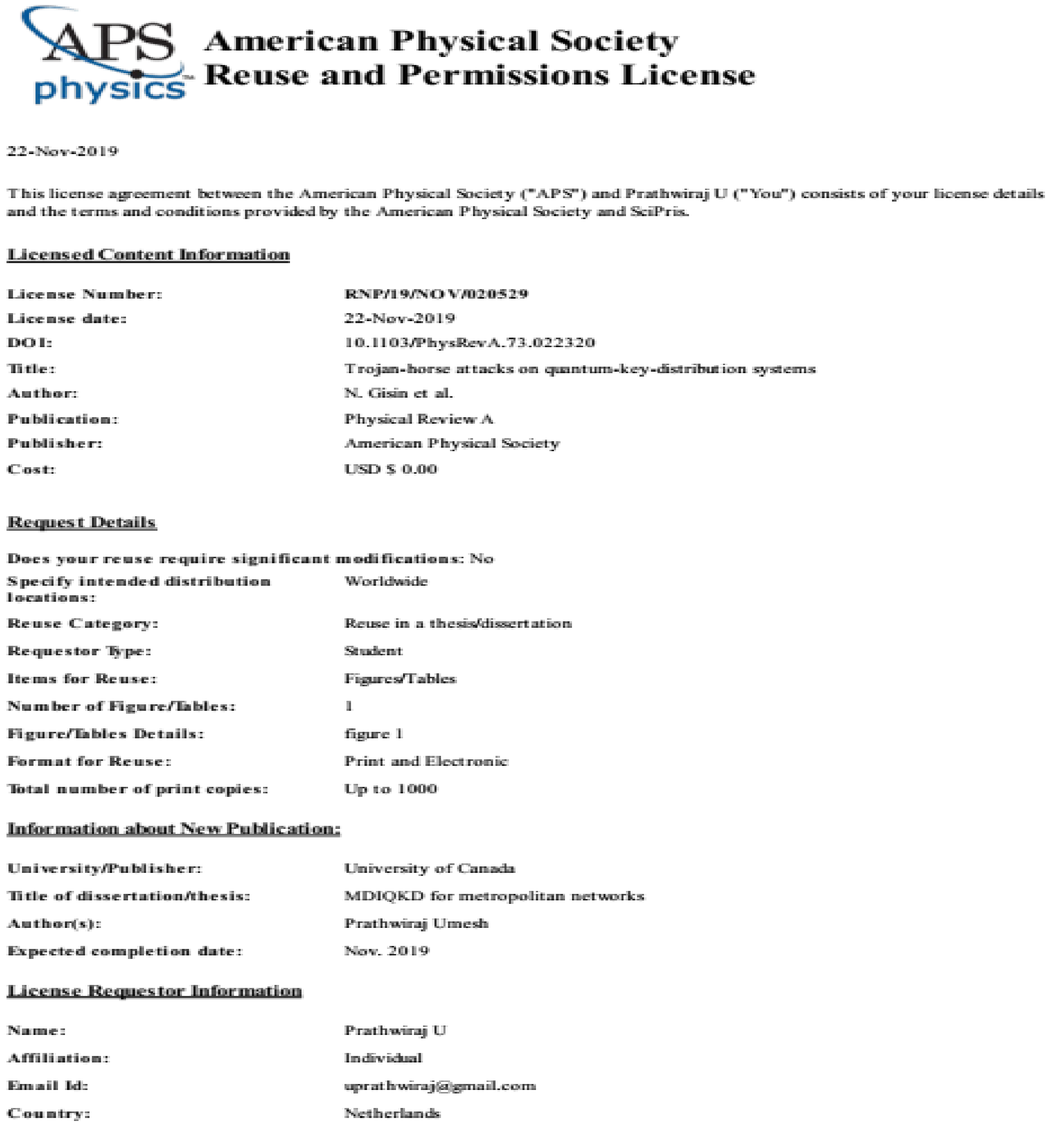
Dear Prathwiraj,
I hereby grant permission to include the below-mentioned figure into your thesis.
Best regards,
Wolfgang

Sent from my iPhone

> On 22 Nov 2019, at 20:32, Prathwiraj Umesh wrote:
>
> Hi Wolfgang,
>
> I am planning to include the below mentioned figures from your publications in my Master's thesis. A reply to this email would be sufficient to grant me the permission to include them.
>
> 1) Figure 1 of the publication :
> Raju Valivarthi, Itzel Lucio-Martinez, Allison Rubenok, Philip Chan, Francesco Marsili, Varun B Verma, Matthew D Shaw, JA Stern, Joshua A Slater, Daniel Oblak, et al. Efficient bell state analyzer for time-bin qubits with fast-recovery wsi superconducting single photon detectors. *Optics express*, 22(20):24497{24506, 2014.
>
> 2) Figure 1 of the publication:
> Raju Valivarthi et al. Measurement-device-independent quantum key distribution: from idea towards application. Journal of Modern Optics, 62(14):1141-1150, 2015.
>
> Thank you,
> Prathwiraj Umesh

Figure A.10: Copyright permission from Prof. Wolfgang Tittel

- The figure 2.4 is take from [2].



American Physical Society Reuse and Permissions License

22-Nov-2019

This license agreement between the American Physical Society ("APS") and Prathwiraj U ("You") consists of your license details and the terms and conditions provided by the American Physical Society and SciPris.

Licensed Content Information

License Number:	RNP/19/NOV/020529
License date:	22-Nov-2019
DOI:	10.1103/PhysRevA.73.022320
Title:	Trojan-horse attacks on quantum-key-distribution systems
Author:	N. Gisin et al.
Publication:	Physical Review A
Publisher:	American Physical Society
Cost:	USD $ 0.00

Request Details

Does your reuse require significant modifications: No

Specify intended distribution locations:	Worldwide
Reuse Category:	Reuse in a thesis/dissertation
Requestor Type:	Student
Items for Reuse:	Figures/Tables
Number of Figure/Tables:	1
Figure/Tables Details:	figure 1
Format for Reuse:	Print and Electronic
Total number of print copies:	Up to 1000

Information about New Publication:

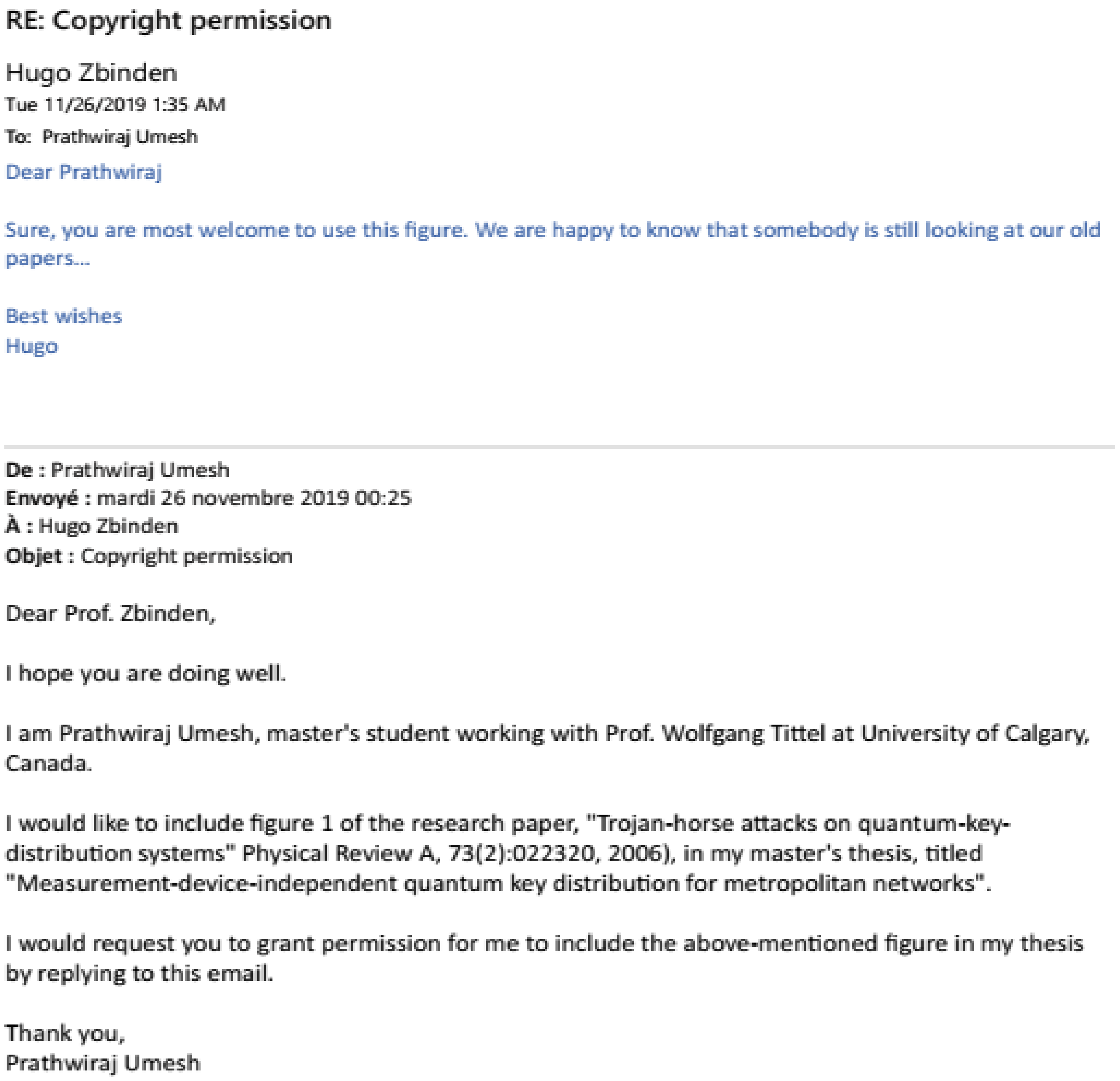
University/Publisher:	University of Canada
Title of dissertation/thesis:	MDIQKD for metropolitan networks
Author(s):	Prathwiraj Umesh
Expected completion date:	Nov. 2019

License Requestor Information

Name:	Prathwiraj U
Affiliation:	Individual
Email Id:	uprathwiraj@gmail.com
Country:	Netherlands

Figure A.11: Copyright permission from APS.

- The figure 2.5 is taken from [3].



RE: Copyright permission

Hugo Zbinden
Tue 11/26/2019 1:35 AM
To: Prathwiraj Umesh

Dear Prathwiraj

Sure, you are most welcome to use this figure. We are happy to know that somebody is still looking at our old papers...

Best wishes
Hugo

De : Prathwiraj Umesh
Envoyé : mardi 26 novembre 2019 00:25
À : Hugo Zbinden
Objet : Copyright permission

Dear Prof. Zbinden,

I hope you are doing well.

I am Prathwiraj Umesh, master's student working with Prof. Wolfgang Tittel at University of Calgary, Canada.

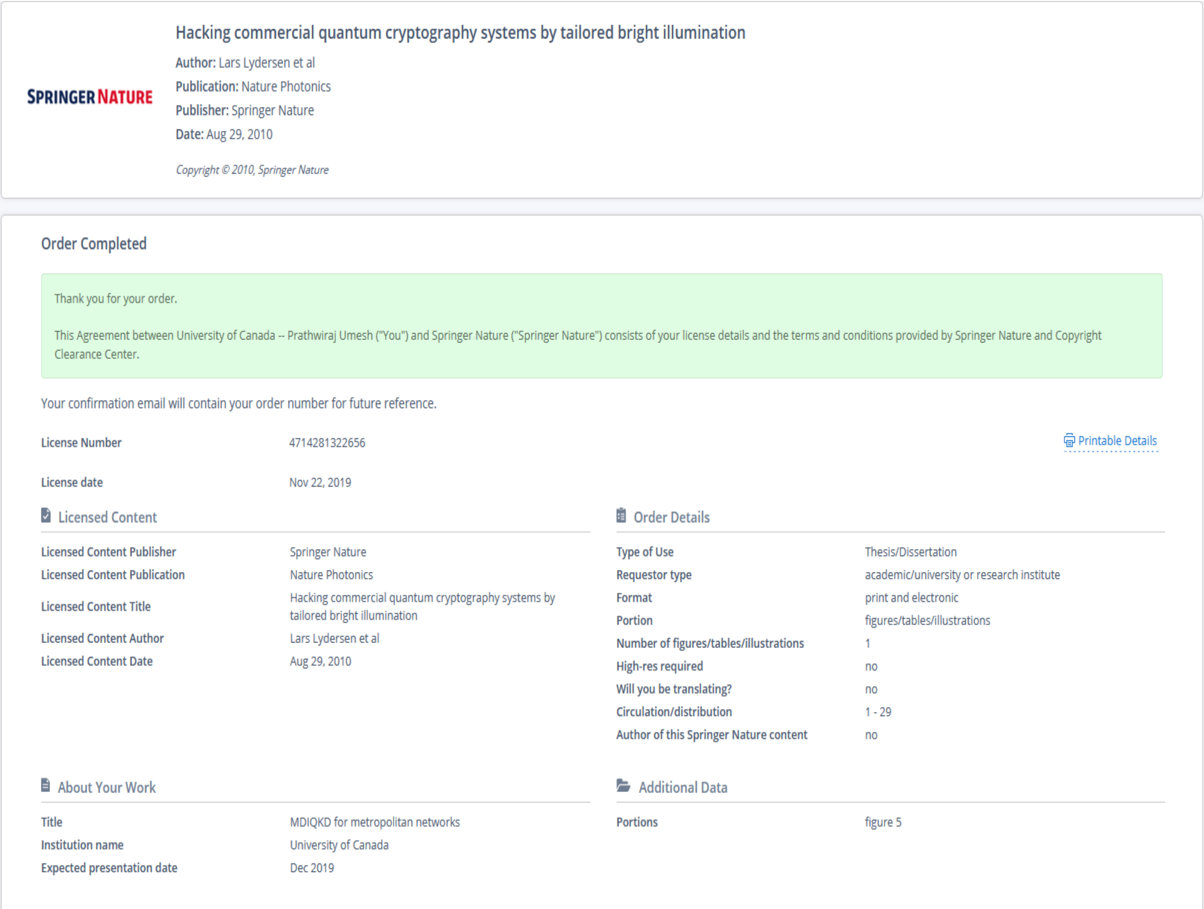
I would like to include figure 1 of the research paper, "Trojan-horse attacks on quantum-key-distribution systems" Physical Review A, 73(2):022320, 2006), in my master's thesis, titled "Measurement-device-independent quantum key distribution for metropolitan networks".

I would request you to grant permission for me to include the above-mentioned figure in my thesis by replying to this email.

Thank you,
Prathwiraj Umesh

Figure A.12: Copyright permission from Prof. Hugo Zbinden.

- The figure 2.6 is taken from [4].



SPRINGER NATURE

Hacking commercial quantum cryptography systems by tailored bright illumination

Author: Lars Lydersen et al

Publication: Nature Photonics

Publisher: Springer Nature

Date: Aug 29, 2010

Copyright © 2010, Springer Nature

Order Completed

Thank you for your order.

This Agreement between University of Canada -- Prathwiraj Umesh ("You") and Springer Nature ("Springer Nature") consists of your license details and the terms and conditions provided by Springer Nature and Copyright Clearance Center.

Your confirmation email will contain your order number for future reference.

License Number	4714281322656
License date	Nov 22, 2019

Printable Details

Licensed Content

Licensed Content Publisher	Springer Nature
Licensed Content Publication	Nature Photonics
Licensed Content Title	Hacking commercial quantum cryptography systems by tailored bright illumination
Licensed Content Author	Lars Lydersen et al
Licensed Content Date	Aug 29, 2010

Order Details

Type of Use	Thesis/Dissertation
Requestor type	academic/university or research institute
Format	print and electronic
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	1
High-res required	no
Will you be translating?	no
Circulation/distribution	1 - 29
Author of this Springer Nature content	no

About Your Work

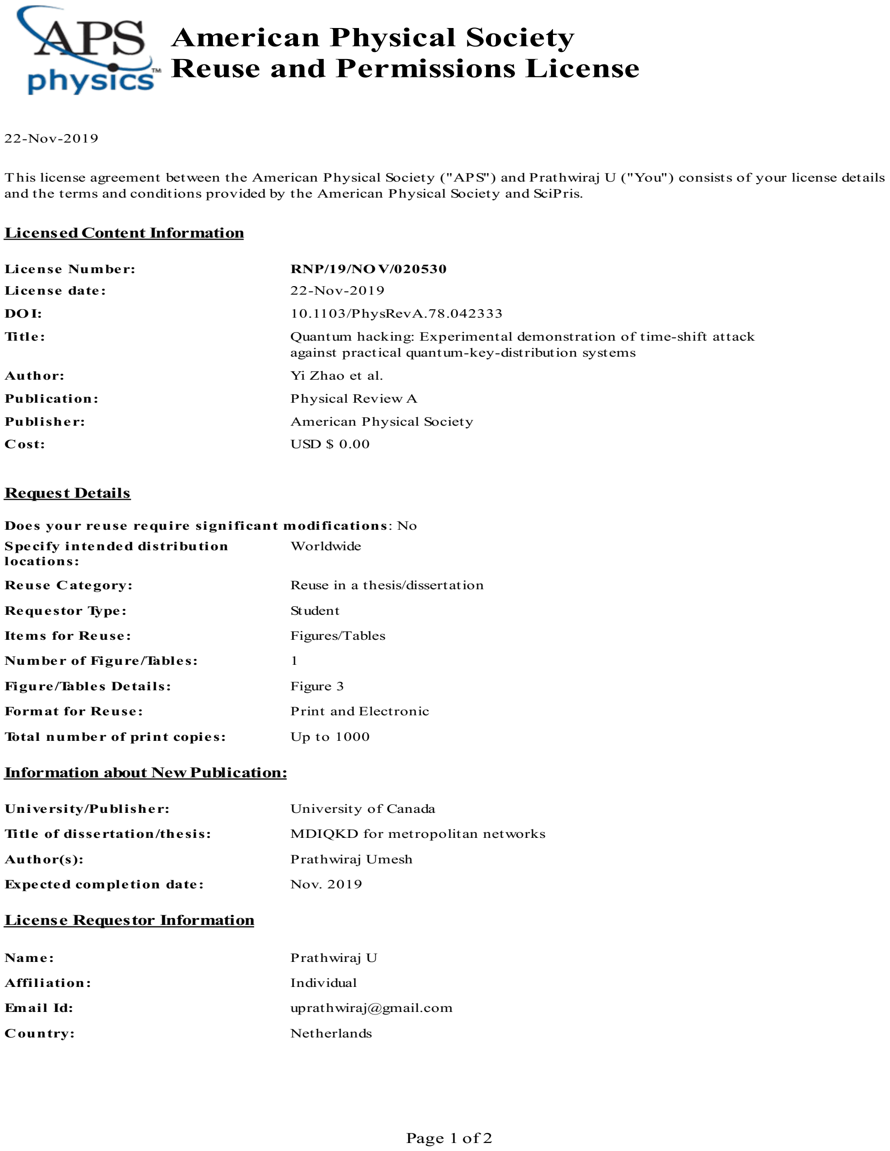
Title	MDIQKD for metropolitan networks
Institution name	University of Canada
Expected presentation date	Dec 2019

Additional Data

Portions	figure 5

Figure A.13: Copyright permission from Springer Nature.

- The figure 2.7 is taken from [5].



American Physical Society Reuse and Permissions License

22-Nov-2019

This license agreement between the American Physical Society ("APS") and Prathwiraj U ("You") consists of your license details and the terms and conditions provided by the American Physical Society and SciPris.

Licensed Content Information

License Number:	**RNP/19/NOV/020530**
License date:	22-Nov-2019
DOI:	10.1103/PhysRevA.78.042333
Title:	Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems
Author:	Yi Zhao et al.
Publication:	Physical Review A
Publisher:	American Physical Society
Cost:	USD $ 0.00

Request Details

Does your reuse require significant modifications: No

Specify intended distribution locations:	Worldwide
Reuse Category:	Reuse in a thesis/dissertation
Requestor Type:	Student
Items for Reuse:	Figures/Tables
Number of Figure/Tables:	1
Figure/Tables Details:	Figure 3
Format for Reuse:	Print and Electronic
Total number of print copies:	Up to 1000

Information about New Publication:

University/Publisher:	University of Canada
Title of dissertation/thesis:	MDIQKD for metropolitan networks
Author(s):	Prathwiraj Umesh
Expected completion date:	Nov. 2019

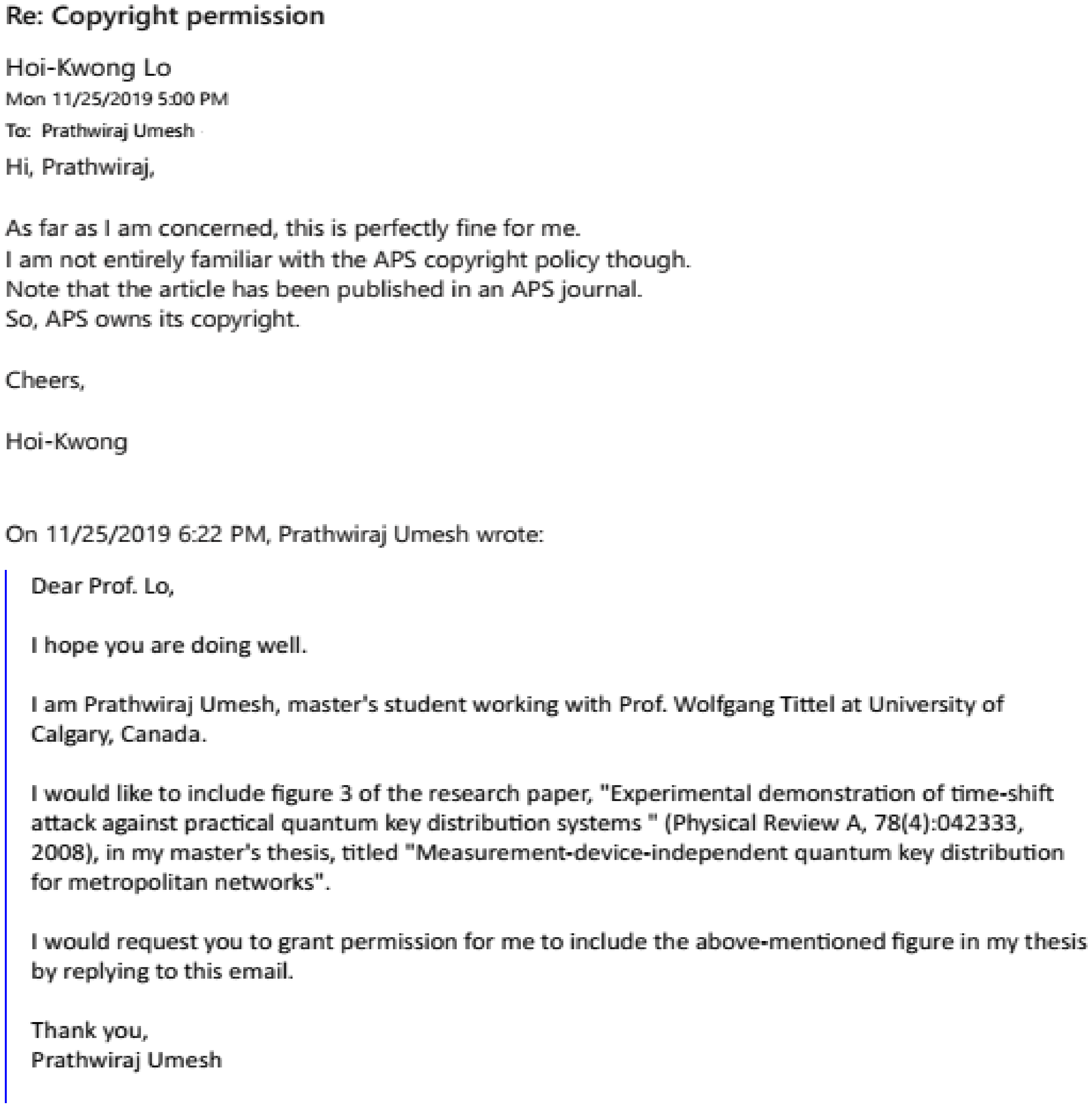
License Requestor Information

Name:	Prathwiraj U
Affiliation:	Individual
Email Id:	uprathwiraj@gmail.com
Country:	Netherlands

Page 1 of 2

Figure A.14: Copyright permission from APS physics.

- The figure 2.8 is taken from [7].



Re: Copyright permission

Hoi-Kwong Lo
Mon 11/25/2019 5:00 PM
To: Prathwiraj Umesh

Hi, Prathwiraj,

As far as I am concerned, this is perfectly fine for me.
I am not entirely familiar with the APS copyright policy though.
Note that the article has been published in an APS journal.
So, APS owns its copyright.

Cheers,

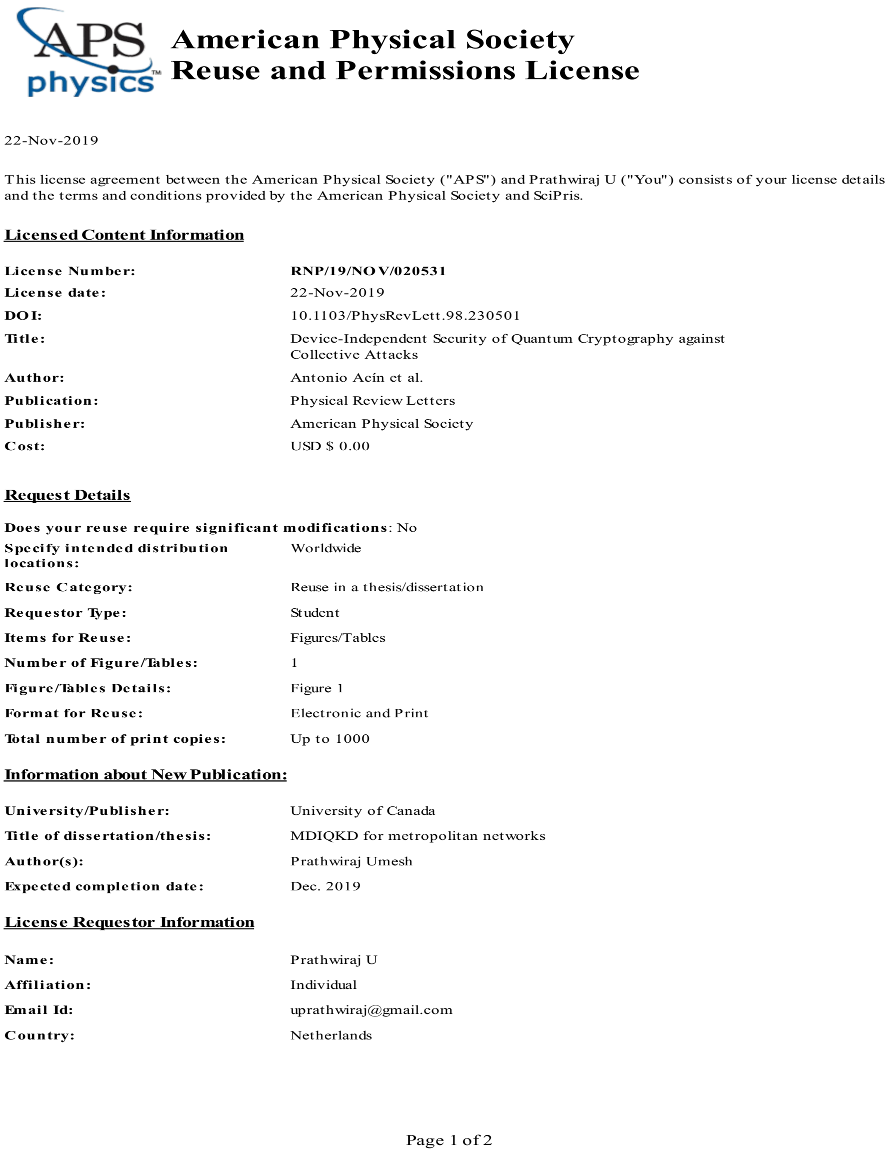
Hoi-Kwong

On 11/25/2019 6:22 PM, Prathwiraj Umesh wrote:

> Dear Prof. Lo,
>
> I hope you are doing well.
>
> I am Prathwiraj Umesh, master's student working with Prof. Wolfgang Tittel at University of Calgary, Canada.
>
> I would like to include figure 3 of the research paper, "Experimental demonstration of time-shift attack against practical quantum key distribution systems " (Physical Review A, 78(4):042333, 2008), in my master's thesis, titled "Measurement-device-independent quantum key distribution for metropolitan networks".
>
> I would request you to grant permission for me to include the above-mentioned figure in my thesis by replying to this email.
>
> Thank you,
> Prathwiraj Umesh

Figure A.15: Copyright permission from Prof. Hoi Kwong Lo.

- The figure 3.1 is taken from [8].



American Physical Society
Reuse and Permissions License

22-Nov-2019

This license agreement between the American Physical Society ("APS") and Prathwiraj U ("You") consists of your license details and the terms and conditions provided by the American Physical Society and SciPris.

Licensed Content Information

License Number:	**RNP/19/NOV/020531**
License date:	22-Nov-2019
DOI:	10.1103/PhysRevLett.98.230501
Title:	Device-Independent Security of Quantum Cryptography against Collective Attacks
Author:	Antonio Acín et al.
Publication:	Physical Review Letters
Publisher:	American Physical Society
Cost:	USD $ 0.00

Request Details

Does your reuse require significant modifications: No

Specify intended distribution locations:	Worldwide
Reuse Category:	Reuse in a thesis/dissertation
Requestor Type:	Student
Items for Reuse:	Figures/Tables
Number of Figure/Tables:	1
Figure/Tables Details:	Figure 1
Format for Reuse:	Electronic and Print
Total number of print copies:	Up to 1000

Information about New Publication:

University/Publisher:	University of Canada
Title of dissertation/thesis:	MDIQKD for metropolitan networks
Author(s):	Prathwiraj Umesh
Expected completion date:	Dec. 2019

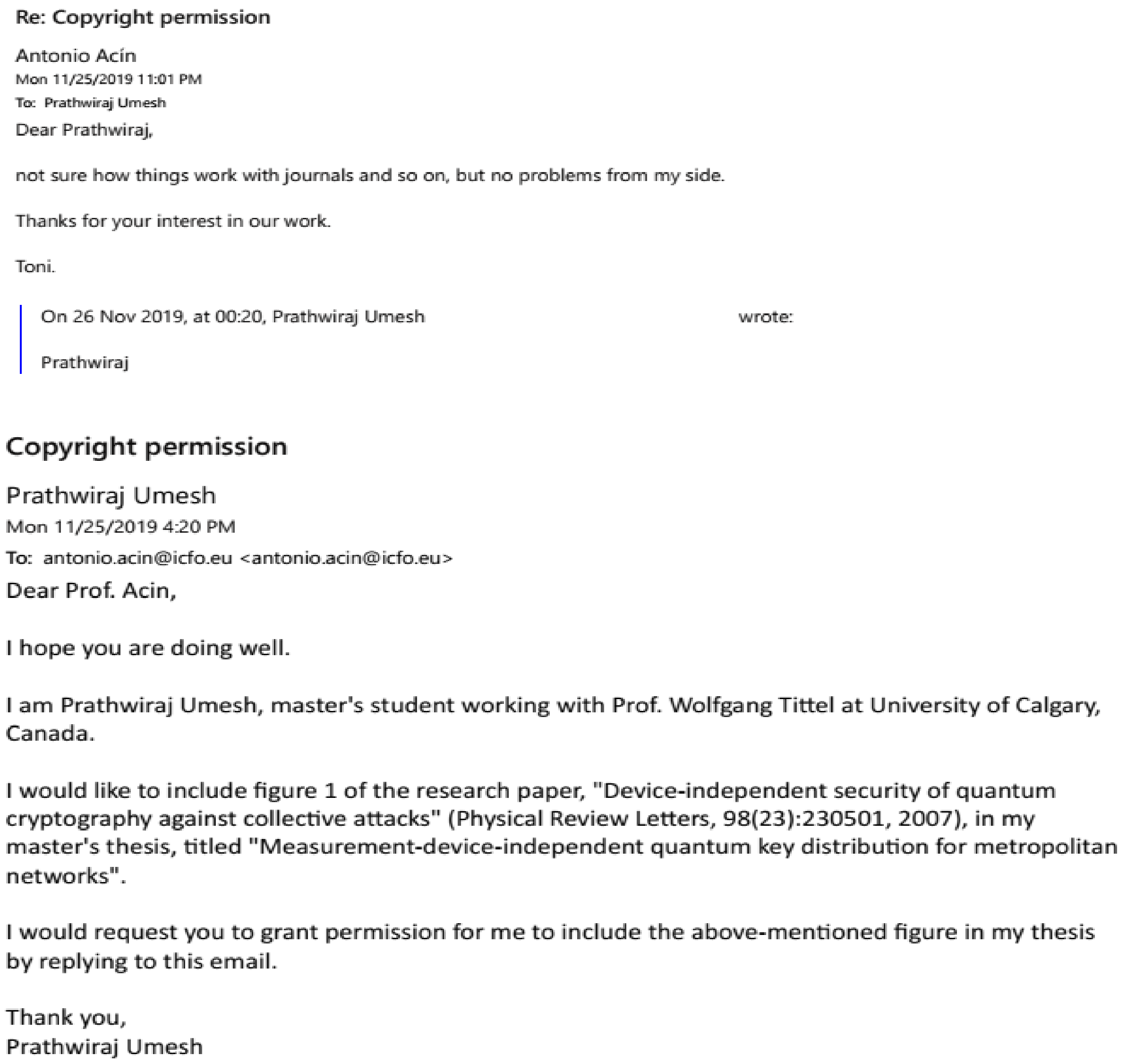
License Requestor Information

Name:	Prathwiraj U
Affiliation:	Individual
Email Id:	uprathwiraj@gmail.com
Country:	Netherlands

Page 1 of 2

Figure A.16: Copyright permission from APS physics.

- The figure 4.1 is taken from [9].
- The figure 4.8 is taken from [11]. The article is under Creative Commons Attribution 3.0 License. Therefore, the figure can be used without permissions.



Re: Copyright permission

Antonio Acín
Mon 11/25/2019 11:01 PM
To: Prathwiraj Umesh

Dear Prathwiraj,

not sure how things work with journals and so on, but no problems from my side.

Thanks for your interest in our work.

Toni.

> On 26 Nov 2019, at 00:20, Prathwiraj Umesh wrote:
>
> Prathwiraj

Copyright permission

Prathwiraj Umesh
Mon 11/25/2019 4:20 PM
To: antonio.acin@icfo.eu <antonio.acin@icfo.eu>

Dear Prof. Acin,

I hope you are doing well.

I am Prathwiraj Umesh, master's student working with Prof. Wolfgang Tittel at University of Calgary, Canada.

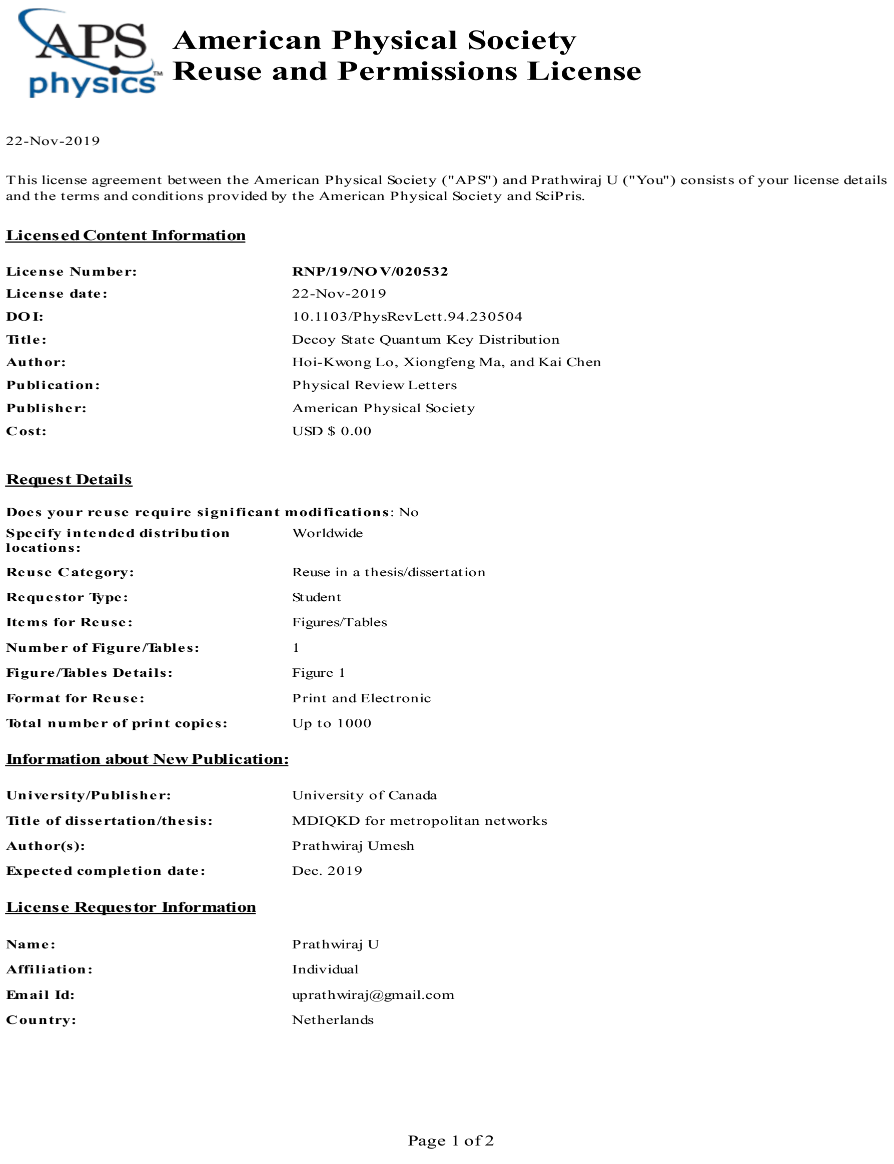
I would like to include figure 1 of the research paper, "Device-independent security of quantum cryptography against collective attacks" (Physical Review Letters, 98(23):230501, 2007), in my master's thesis, titled "Measurement-device-independent quantum key distribution for metropolitan networks".

I would request you to grant permission for me to include the above-mentioned figure in my thesis by replying to this email.

Thank you,
Prathwiraj Umesh

Figure A.17: Copyright permission from Prof. Antonio Acin.

- The figure is taken from [12]. The figures 4.3 and 4.4 are taken from [10].



American Physical Society Reuse and Permissions License

22-Nov-2019

This license agreement between the American Physical Society ("APS") and Prathwiraj U ("You") consists of your license details and the terms and conditions provided by the American Physical Society and SciPris.

Licensed Content Information

License Number:	**RNP/19/NOV/020532**
License date:	22-Nov-2019
DOI:	10.1103/PhysRevLett.94.230504
Title:	Decoy State Quantum Key Distribution
Author:	Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen
Publication:	Physical Review Letters
Publisher:	American Physical Society
Cost:	USD $ 0.00

Request Details

Does your reuse require significant modifications: No

Specify intended distribution locations:	Worldwide
Reuse Category:	Reuse in a thesis/dissertation
Requestor Type:	Student
Items for Reuse:	Figures/Tables
Number of Figure/Tables:	1
Figure/Tables Details:	Figure 1
Format for Reuse:	Print and Electronic
Total number of print copies:	Up to 1000

Information about New Publication:

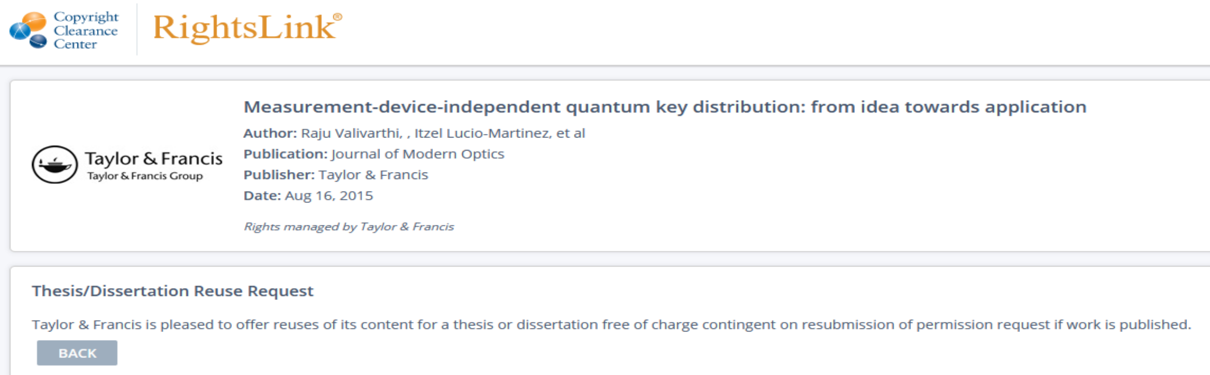
University/Publisher:	University of Canada
Title of dissertation/thesis:	MDIQKD for metropolitan networks
Author(s):	Prathwiraj Umesh
Expected completion date:	Dec. 2019

License Requestor Information

Name:	Prathwiraj U
Affiliation:	Individual
Email Id:	uprathwiraj@gmail.com
Country:	Netherlands

Page 1 of 2

Figure A.18: Copyright permission from APS physics.



Measurement-device-independent quantum key distribution: from idea towards application

Author: Raju Valivarthi, , Itzel Lucio-Martinez, et al

Publication: Journal of Modern Optics

Publisher: Taylor & Francis

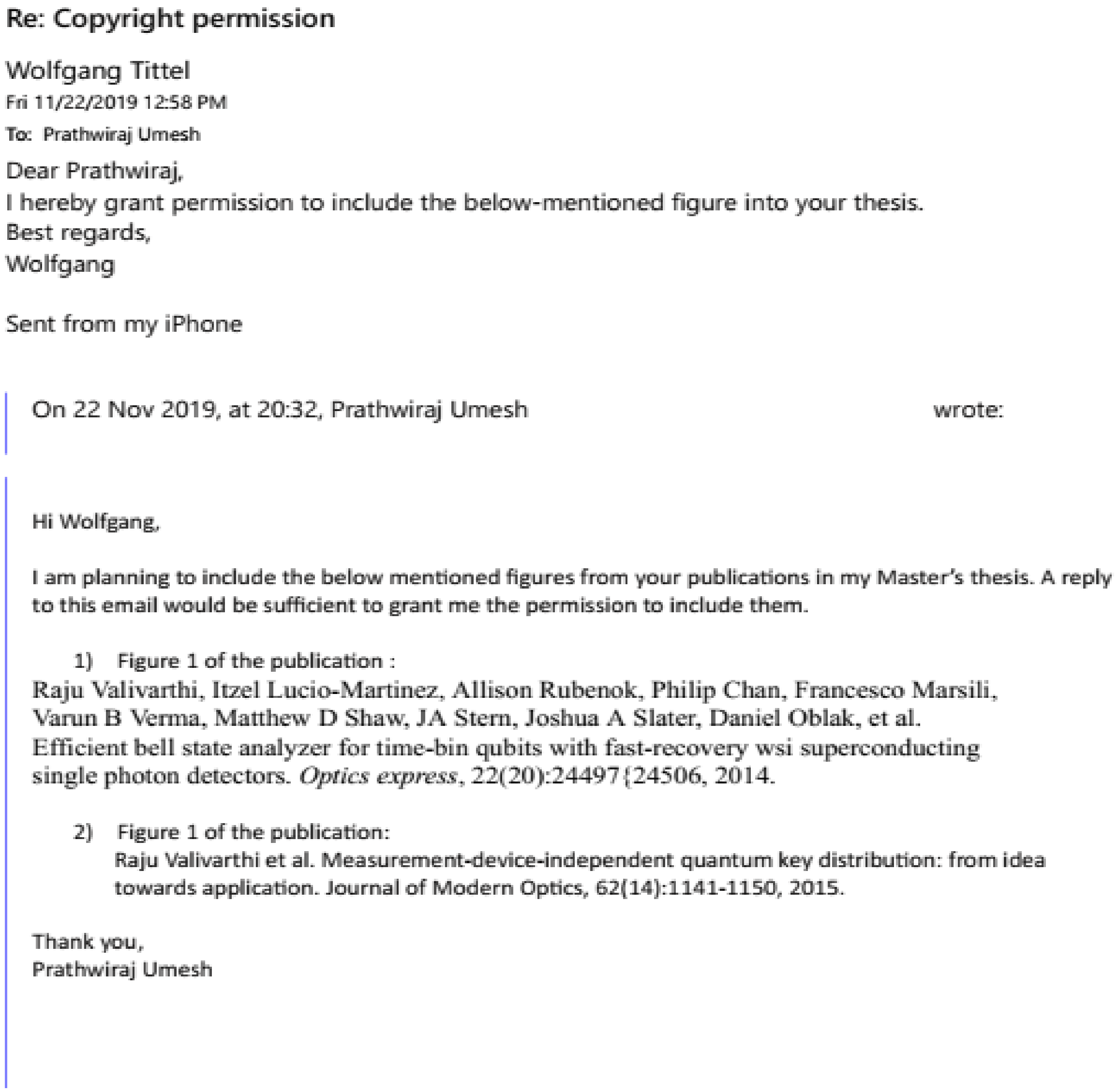
Date: Aug 16, 2015

Rights managed by Taylor & Francis

Thesis/Dissertation Reuse Request

Taylor & Francis is pleased to offer reuses of its content for a thesis or dissertation free of charge contingent on resubmission of permission request if work is published.

Figure A.19: Copyright permission from Journal of modern optics.



Re: Copyright permission

Wolfgang Tittel
Fri 11/22/2019 12:58 PM
To: Prathwiraj Umesh

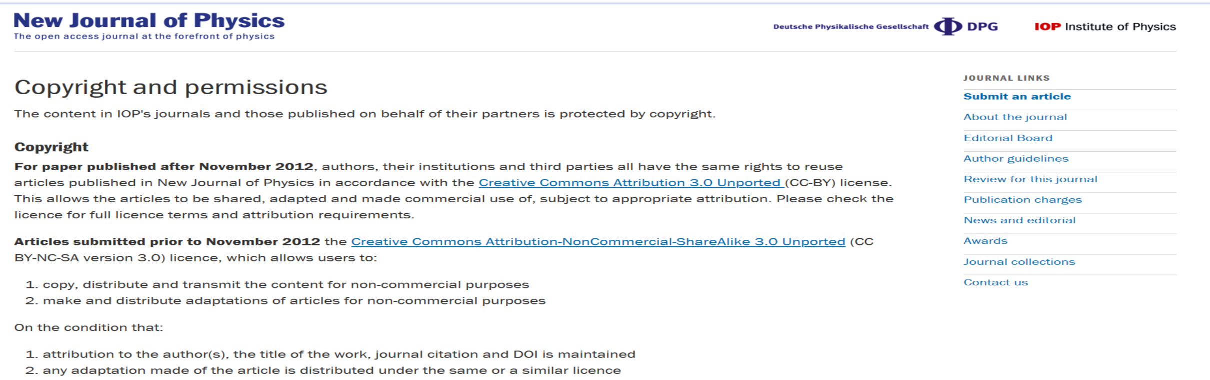
Dear Prathwiraj,
I hereby grant permission to include the below-mentioned figure into your thesis.
Best regards,
Wolfgang

Sent from my iPhone

> On 22 Nov 2019, at 20:32, Prathwiraj Umesh wrote:

> Hi Wolfgang,
>
> I am planning to include the below mentioned figures from your publications in my Master's thesis. A reply to this email would be sufficient to grant me the permission to include them.
>
> 1) Figure 1 of the publication :
> Raju Valivarthi, Itzel Lucio-Martinez, Allison Rubenok, Philip Chan, Francesco Marsili, Varun B Verma, Matthew D Shaw, JA Stern, Joshua A Slater, Daniel Oblak, et al. Efficient bell state analyzer for time-bin qubits with fast-recovery wsi superconducting single photon detectors. *Optics express*, 22(20):24497{24506, 2014.
>
> 2) Figure 1 of the publication:
> Raju Valivarthi et al. Measurement-device-independent quantum key distribution: from idea towards application. Journal of Modern Optics, 62(14):1141-1150, 2015.
>
> Thank you,
> Prathwiraj Umesh

Figure A.20: Copyright permission from Prof. Wolfgang Tittel



Copyright and permissions

The content in IOP's journals and those published on behalf of their partners is protected by copyright.

Copyright

For paper published after November 2012, authors, their institutions and third parties all have the same rights to reuse articles published in New Journal of Physics in accordance with the Creative Commons Attribution 3.0 Unported (CC-BY) license. This allows the articles to be shared, adapted and made commercial use of, subject to appropriate attribution. Please check the licence for full licence terms and attribution requirements.

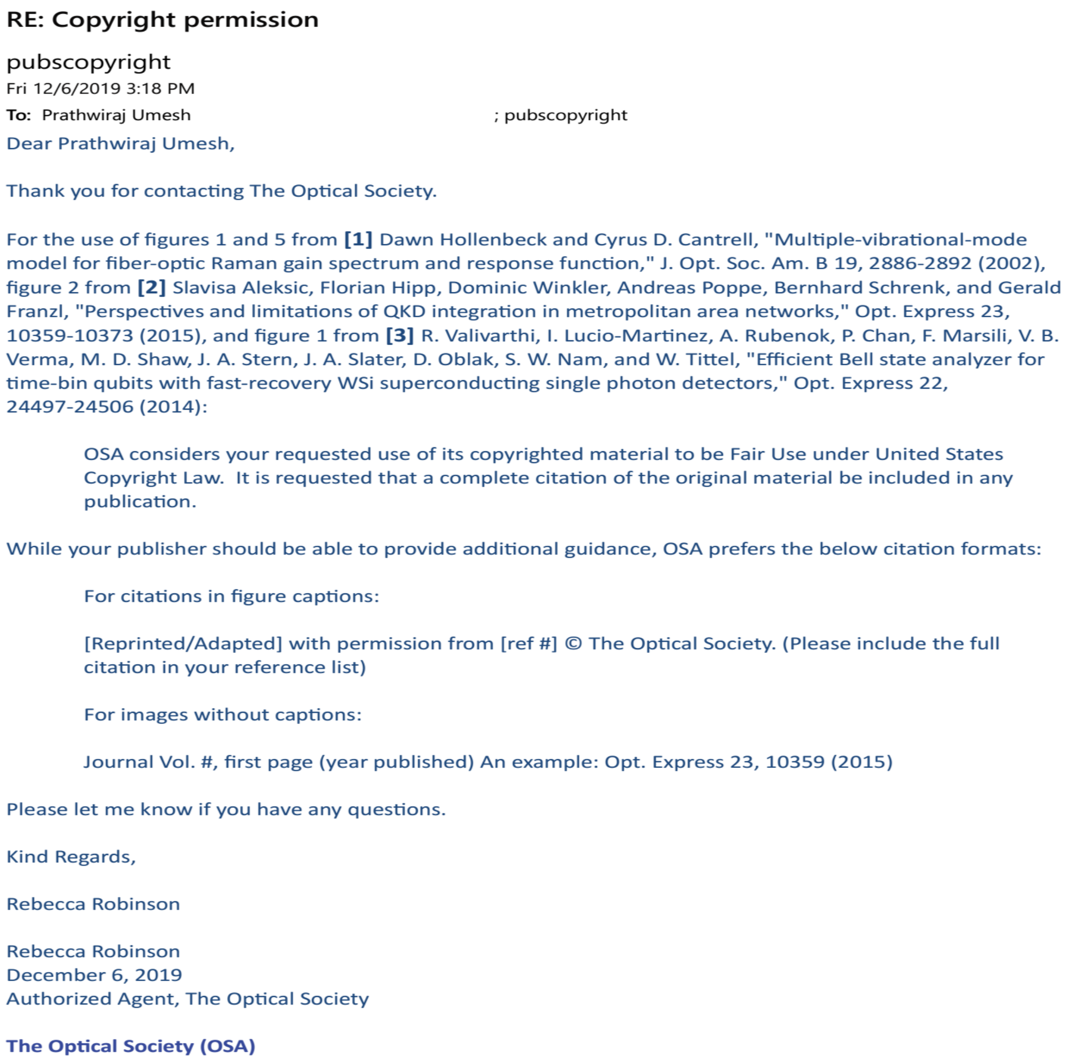
Articles submitted prior to November 2012 the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported (CC BY-NC-SA version 3.0) licence, which allows users to:

1. copy, distribute and transmit the content for non-commercial purposes
2. make and distribute adaptations of articles for non-commercial purposes

On the condition that:

1. attribution to the author(s), the title of the work, journal citation and DOI is maintained
2. any adaptation made of the article is distributed under the same or a similar licence

Figure A.21: Copyright permission from New Journal Physics.



RE: Copyright permission

pubscopyright
Fri 12/6/2019 3:18 PM
To: Prathwiraj Umesh ; pubscopyright

Dear Prathwiraj Umesh,

Thank you for contacting The Optical Society.

For the use of figures 1 and 5 from **[1]** Dawn Hollenbeck and Cyrus D. Cantrell, "Multiple-vibrational-mode model for fiber-optic Raman gain spectrum and response function," J. Opt. Soc. Am. B 19, 2886-2892 (2002), figure 2 from **[2]** Slavisa Aleksic, Florian Hipp, Dominic Winkler, Andreas Poppe, Bernhard Schrenk, and Gerald Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," Opt. Express 23, 10359-10373 (2015), and figure 1 from **[3]** R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, and W. Tittel, "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," Opt. Express 22, 24497-24506 (2014):

> OSA considers your requested use of its copyrighted material to be Fair Use under United States Copyright Law. It is requested that a complete citation of the original material be included in any publication.

While your publisher should be able to provide additional guidance, OSA prefers the below citation formats:

> For citations in figure captions:
>
> [Reprinted/Adapted] with permission from [ref #] © The Optical Society. (Please include the full citation in your reference list)
>
> For images without captions:
>
> Journal Vol. #, first page (year published) An example: Opt. Express 23, 10359 (2015)

Please let me know if you have any questions.

Kind Regards,

Rebecca Robinson

Rebecca Robinson
December 6, 2019
Authorized Agent, The Optical Society

The Optical Society (OSA)

Figure A.22: Copyright permission from OSA.